V8.0 for DLP+ HyBoost

[Admin Manual V1.2]

Introduction

The contents of this Manual may be changed without prior notice to improve products and performance. The example companies, organizations, products, people and events depicted herein are fictitious. Any part of this Manual shall not be replicated, saved in a search system, introduced or transferred in any form or by any means (electronic, mechanical, copy machine, disk copy or otherwise), or for any purpose without the express approval of Somansa Co., Ltd..

Somansa Co., Ltd. holds patents, trademark rights, copyrights or other intellectual property rights covering subject matter in this Manual. Other than the rights provided to you by Somansa Co., Ltd. in accordance with any written license agreement, the provisions of this Manual shall not provide you any license regarding the patents, trademark rights, copyrights or other intellectual property rights.

- Manufacturer (Supplier) Name: SOMANSA Co., Ltd.
- Address: 3003 N. First St., Suite 301, San Jose, California 95134
- Website Address: http://www.somansatech.com/
- Technical Support: Somansa Technical Support Team / (408) 701-1302 / support@somansatech.com
  Inquiries on Function/ On-Line Remote Assistance/ Off-Line Maintenance Support Requests / User Training Requests

[Remark]
The social security numbers on the UI screens included in the Manual are fabricated numbers for the purpose of providing realistic examples.

Contents

1. Network DLP: Mail-i

1.1 Outline

1.1.1 What is Network DLP, Mail-i?

Somansa Mail-i is a Network DLP solution to monitor, discover, and protect data in motion. Using its superior packet and protocol analysis technology, Somansa Mail-i monitors outbound network traffic including Email, IM, FTP, HTTP/HTTPS, Cloud Services to protect sensitive company data and meet regulatory compliance requirements.

1.2 System Requirements

Please refer to the below for the operating system version requirements on which to install the Administration Console and Server.

[TABLE 1-1] MINIMUM REQUIREMENTS TO INSTALL ADMINISTRATION CONSOLE

Category	Hardware and Software Requirements	
Administration Console	CPU	Intel Core 2 1.6Ghz
	RAM	2 GB
	HDD	1 GB +
	NIC	10/100/1000 Ethernet
	Operating System	Windows 7 Professional (x86/x64) SP1
	Web Browser	-Internet Explorer 10 -Chrome 38.0.2125.104
	Software	Adobe Flash Player 15 Active X

Below are the hardware and software requirements to install the Server.

[TABLE 1-2] MINIMUM REQUIREMENTS TO INSTALL MAIL-I SERVER

Category	Hardware and Software Requirements	
Mail-i Server	CPU	Intel Xeon Quad 3.1Ghz
	RAM	8GB

	HDD	500GB * 2 (raid 1)
	NIC	10/100/1000 Ethernet * 3EA (In/Out-Bound, Communication)
	Operating System	CentOS 6.4 (kernel 2.6.32)
	Software	PostgreSQL 9.3

1.3 Package Configurations

Mail-i V8.0 for DLP+ HyBoost package is configured as the below.

- Configuration Manager: Web-based management interface for basic settings and other security settings required to start, stop, and run Mail-i V8.0. An authentication which is different from the initial authentication of admin and the password (at least 9 characters and including English letters, numbers and special characters) are required.

- DLP+ Center: Web-based interface managed by the authenticated admin. Functions to identify and authenticate the admin account, set up a policy and view the audit logs of Mail-i Agent are performed.

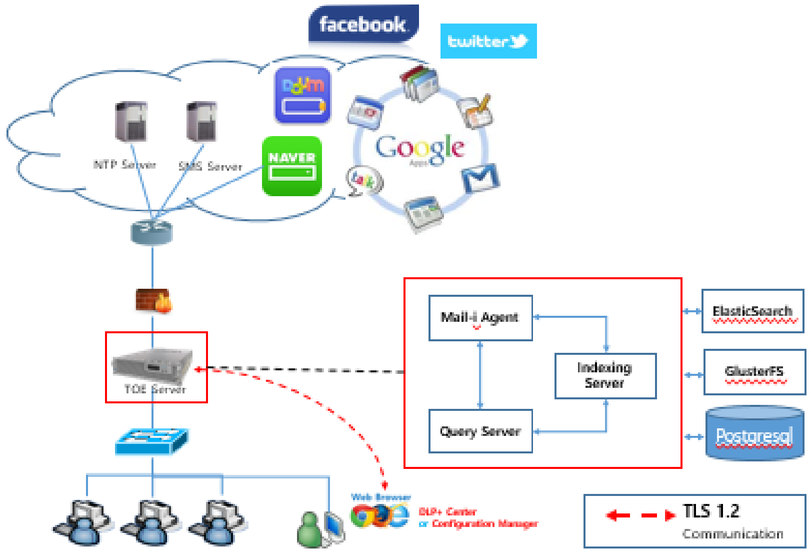
- Mail-i Agent: Performs the packet analysis about Network Applications such as email, web mail, instant messaging service and remote access. All activities through the Mail-i Agent are saved as audit logs and packets are analyzed by the policy from DLP+ Center for Mail-i V8.0 HyBoost. Based on the analysis, Audit Logs about activities related to emails of each user are also sent to Indexing Server_M and attached files are traced to GFS.

- Indexing Server_M: Traces audit logs to ElasticSearch by converting the packet analyzed by Mail-i Agent to json format.

- Referral Server_M: A package to be used to view audit logs of Mail-i Agent in DLP+Center for Mail-i V8.0 HyBoost and provide the necessary information for matching audit logs of Mail-i Agent. The information provided to Mail-i Agent consists of Policy, HR Information, and Pattern.

1.4 Mail-i Configuration Diagram

The operating environment of Mail-i is configured with T-Proxy which is installed in the traffic communication section and includes information on how Router, Switch, IPS and Firewall are configured. All bidirectional traffic passes across a product because T-Proxy is installed in the network section.



Administrator can view logs and apply policies through DLP+ Center by setting up the product operation environment in Configuration Manger. Please refer to to [2.1 Program Requirements] for the detailed requirements of Admin PC, Server Hardware and Software to run the security management function of Mail-i V8.0 for DLP+ HyBoost.

2. Installation

2.1 Program Requirements

To install Mail-i V8.0 for DLP+ HyBoost product, the programs below are required.

[TABLE 2-1] ENVIRONMENTAL CONDITIONS

Program	Version	Remark
PostgreSQL	9.3	Database
gcc-c++	4.4.7	Compiler
Java Runtime Environment (JRE)	1.7	Runtime Environment
Rdate	1.4	Time Synchronization
Elasticsearch	1.4.3	Search Engine
Glusterfs	3.6.3	Storage System
Redis	2.8.5	Key-value store

2.2 Installing Required Programs

Installation Packages of required programs which are provided by elasticsearch and glusterfs should be run before installing the server package of Mail-i v8.0 for DLP+ Hyboost. Installation File is divided into elasticsearch_143_install.bin and glusterfs_363_install.bin respectively. Please refer to the below for the package installation.

```
#sh elasticsearch_143_install.bin
#sh glusterfs_363_install.bin
```

Enter the Server IP when the message below is displayed while installing each installation file.

Please, input the IP Address of Elasticsearch, Please, input the IP Address of Glusterfs 192.168.10.67 (Content which user should enter)

2.3 Installing Product

2.3.1 Installing Mail-i Server Package

To run the Mail-i Server Package of Mail-i V8.0 for DLP+ HyBoost, run the 'Mail-i_V8.0_for_DLP+_HyBoost_Install.BIN' installation file. (※before installing the product, PostgreSQL must be installed. Please note that the package cannot be installed if PostgreSQL is not installed.) Run the Package as follows. (Please check the file permissions when running the Package.)

```
#sh Mail-i_V8.0_for_DLP+_HyBoost_Install.BIN
```

During installation, when the following message is received, enter the IP of a PC where the Security Admin can connect to the Configuration Manager. Please note that the Configuration Manager can be only connected from one registered PC.

Please, input the IP Address of the desktop to connect Configuration Manager

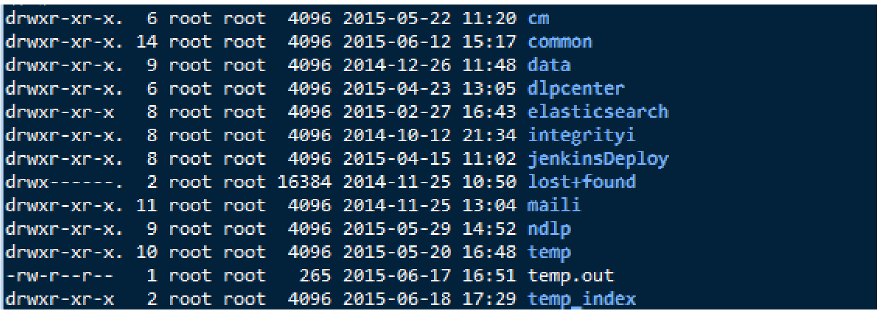
192.168.10.171 (Information that the User must enter)

The admin of Mail-i V8.0 HyBoost consists of System Admin, Admin, Operator, and Viewer. Admin, Operator, and Viewer can view the information by the type of case and time and output the information with various charts and graphs. System Admin is the unique administrator of Configuration Manager and has the right to view the logs which are necessary to run and operate Mail-i V8.0 HyBoost.

Catogory	Description
System Admin	Admin with the right to run and stop Mail-i V8.0 HyBoost and configure DB and specify the DB Path from Configuration Manager
Admin	Admin with the right to add and delete a user and admin account and view logs and edit policies
Operator	Admin with the right to view logs and policy (limited view)
Viewer	Admin with the right to view logs only

2.3.2 Installation Path

When installation of Mail-i 8.0 for DLP+ HyBoost Package is complete, the product is installed on the /somansa path as shown below figure.



```
drwxr-xr-x.  6 root root  4096 2015-05-22 11:20 cm
drwxr-xr-x. 14 root root  4096 2015-06-12 15:17 common
drwxr-xr-x.  9 root root  4096 2014-12-26 11:48 data
drwxr-xr-x.  6 root root  4096 2015-04-23 13:05 dlpcenter
drwxr-xr-x   8 root root  4096 2015-02-27 16:43 elasticsearch
drwxr-xr-x.  8 root root  4096 2014-10-12 21:34 integrityi
drwxr-xr-x.  8 root root  4096 2015-04-15 11:02 jenkinsDeploy
drwx------.  2 root root 16384 2014-11-25 10:50 lost+found
drwxr-xr-x. 11 root root  4096 2014-11-25 13:04 maili
drwxr-xr-x.  9 root root  4096 2015-05-29 14:52 ndlp
drwxr-xr-x. 10 root root  4096 2015-05-20 16:48 temp
-rw-r--r--   1 root root   265 2015-06-17 16:51 temp.out
drwxr-xr-x   2 root root  4096 2015-06-18 17:29 temp_index
```

When installation of the Mail-i Server is complete, connect to the Configuration Manager, extract the UID of the Server, and apply for issuance of a License at the SOMANSA License Center (http://license.somansa.com/). The connecting address to the Configuration Manager is as follows.

Comment [D1]: Somansa License Center in Korean.

https://IP_ADDR/cm

2.3.3 Running Mail-i V8.0 HyBoost Server

Mail-i V8.0 HyBoost Server can be run by the License Issue (Refer to 2.4 License) and Common Area Settings (Refer to 4.1 Common Area Settings).

2.3.4 Check Mail-i V8.0 HyBoost Version

Category	Version	How to check the version
Mail-i Agent	8.0.1.64	Access Console > Confirm /somansa/ndlp/env/default/scripts/ ndlp-agent version
Indexing Sever_M	18270	Access Console > Confirm /somansa/common/tomcat_indexer/ webapps/SMSIndexerWeb_Spring/META-INF/MANIFEST.MF > SVN-Revision in File
Referral Server	18275	Access Console > Confirm /somansa/common/ tomcat_queryserver/webapps/DLPQueryServer/META-INF/MANIFEST.MF > SVN-Revision in File
DLP+ Center	13690	Login DLP+ Center after running Mail-i > Click the info in the

		right upper side of DLP+ Center
Configuration Manager	13455	Login Configuration Manager after running Mail-i > Click the ‘!” image in the right upper side of Configuration Manager

2.3.5 Uninstalling Mail-i V8.0 HyBoost Server

If Mail-i V8.0 HyBoost needs to be uninstalled, please contact a SOMANSA Support Team Member.

2.3.6 System Firewall Allow/Block Settings

After Mail-i server is installed, the Port Information should be allowed in the firewall to access the web management console and login into agents of 4 programs as the below table.

[TABLE 2-2] PORT INFORMATION TO BE ALLOWED

No	Program	Port
1	DLP+ Center	443
2	Configuration Manager	
3	PostgreSQL	5432
4	ElasticSearch	9200
5		9300
6	GlusterFS	111
7		2049
8		24007~24008
9		45152~45156
10	Redis	9800
11	Mail-i Agent	9600
12		45123
13		3128

15	Indexing Server_M	9700
16	Referral Server_M	9500
17	Time Synchronization	37
18		123

2.4 License

2.4.1 Issuance Procedure

STEP 1

Connect to the Configuration Manager through a web browser and check the UID preferences. With the extracted UID, please send to support@somansatech.com. When, the receipt is complete, a License Key will be sent by E-mail.

STEP 2

Copy the two License files (privacyi.license, privacyi.license.serial) sent by E-mail to the '/somansa/common/license' folder; and copy the Encryption Key (cm_piencrypt.dat) to the '/somansa/privacyi/data' folder.

STEP 3

The Registered License can be checked in the Configuration Manager > Mail-i > License tab.

2.4.2 What happens if the license is not renewed?

If a product license agreement has expired and not renewed, the product will not update. In addition, the latest security patch files cannot be received, and server operation cannot be controlled when Mail-i Server is down. Therefore, please renew a license when it has expired.

3. Configuration Manager

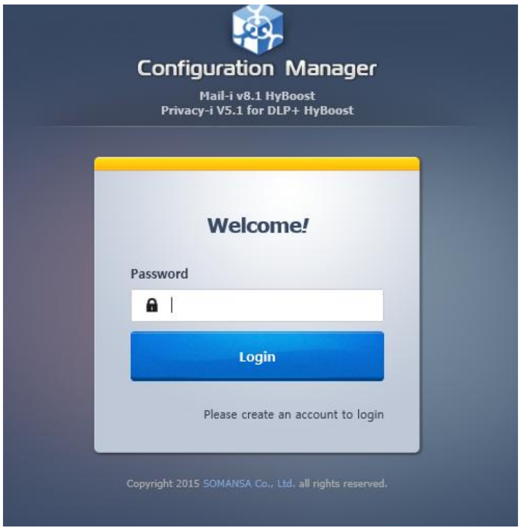
3.1 Running Configuration Manager

Configuration Manager consisting of Common Area Settings, DLP + Center, Mail-i, Maintenance, provides administrators with functionalities to configure, maintain and manage the system. Run the Configuration Manager through a web browser. The first Security Admin password is provided, and should be changed after login. If the password is forgotten, please contact the SOMANSA Support Team.

3.2 Initial Connection Settings

3.2.1 Enter Password upon Initial Connection

When logged in to Configuration Manager, the login page will appear as below (Figure 3-2). The admin account in Configuration Manager is “Security Admin”, and only one account is available. Therefore, do not enter a separate ID. Enter the default password upon initial connection, and log in with the "Security Admin".


Configuration Manager
Mail-i v8.1 HyBoost
Privacy-i V5.1 for DLP+ HyBoost
Welcome!
Password
Login
Please create an account to login
Copyright 2015 SOMANSA Co., Ltd. all rights reserved.

(FIGURE 3-1) CONFIGURATION MANAGER LOGIN SCREEN

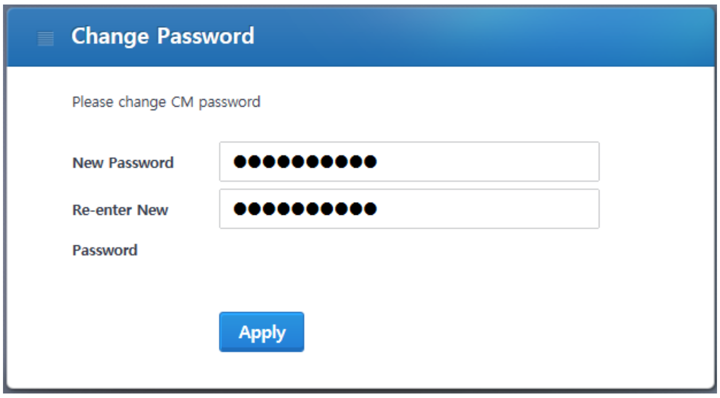
☞ Effective Input Field Range

[TABLE 3-1] EFFECTIVE INPUT FIELD RANGE UPON LOGIN

Item	Effective Range	Character	Failure Message
Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter password.

3.2.2 Setting Up a New Password

After entering the password, the Change Password screen will appear (Figure 3-3). Set up a new password for the Security Admin in the Configuration Manager.



Change Password

Please change CM password

New Password: ●●●●●●●●●●

Re-enter New Password: ●●●●●●●●●●

(FIGURE 3-2) SETTING UP A NEW PASSWORD IN THE CONFIGURATION MANAGER SCREEN

☞ Effective Input Field Range

[TABLE 3-2] EFFECTIVE INPUT FIELD RANGE UPON LOGIN

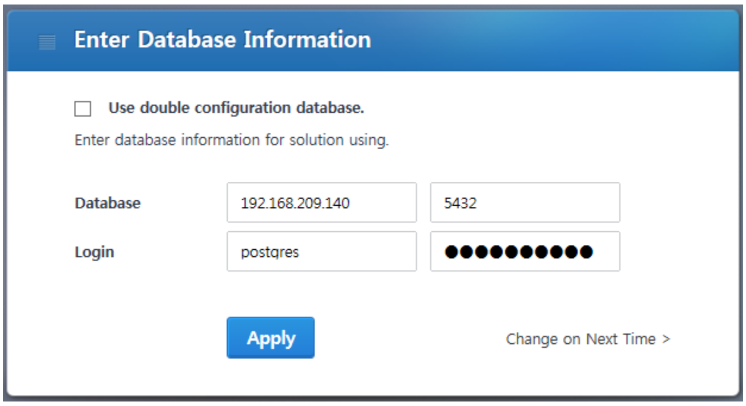
Item	Effective Range	Character	Failure Message
New Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter new password.
Confirm a New Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter password again.

Recommendations

- ✓ Password should have at least 9 characters and include English letters, numbers and special characters.
- ✓

3.2.3 Enter Database Information

Enter database information for “Mail-i V8.0 for DLP+ HyBoost” on this screen. Enter the database accessible IP/ Port/ Account.



Enter Database Information

□ Use double configuration database.

Enter database information for solution using.

Database: 192.168.209.140 | 5432

Login: postgres | ●●●●●●●●●●

(FIGURE 3-3) ENTER DATABASE INFORMATION IN THE CONFIGURATION MANAGER

☞ Item Description

① Enter Database Information: Enter the default database information of the server. If a database with a redundancy configuration is used, enter the information for an existing configured server where the database is installed.

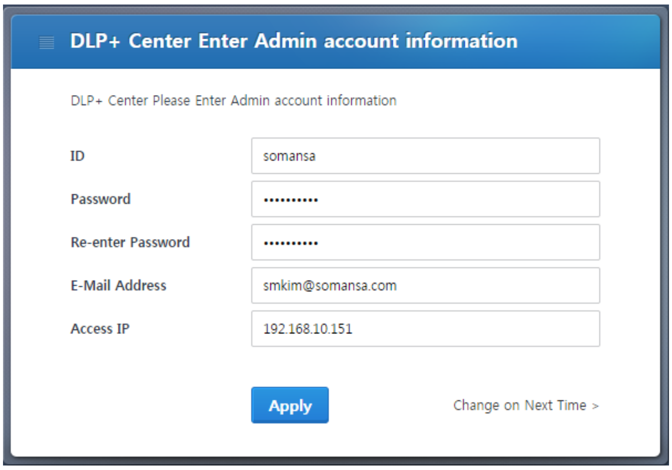
☞ Effective Input Field Range

[TABLE 3-3] EFFECTIVE INPUT FIELD RANGE UPON CONNECTION TO THE DEFAULT DATABASE

Item	Effective Range	Character	Failure Message
Database (IP)	15	Numbers, special characters (.)	Enter the IP of the default DB.
Database (Port)	1~65536	Numbers	Enter the port of the default DB.
Login (ID)	5~256	Letters	Enter the login ID of the default DB.
Login (Password)	9~70	Numbers, letters, special characters	Enter the password of the default DB.

3.2.4 Enter Admin Account Information

Set the admin account information for the DLP+ Center on this screen. Specify the admin account ID and password of the DLP+ Center, and configure the "Access IP" with the IP that the admin account has access to. In an environment with IP other than the Access IP, connection is not possible. (※please note that it should be reinstalled or contact a SOMANSA Support Team Member if Access IP is lost.)



DLP+ Center Enter Admin account information

DLP+ Center Please Enter Admin account information

ID: somansa

Password: ••••••••••

Re-enter Password: ••••••••••

E-Mail Address: smkim@somansa.com

Access IP: 192.168.10.151

(FIGURE 3-4) ENTER SECURITY ADMIN ACCOUNT INFORMATION

☞ Effective Input Field Range

[TABLE 3-4] EFFECTIVE INPUT FIELD RANGE UPON LOGIN

Item	Effective Range	Character	Failure Message
ID	5~100	Letters	Enter the DLP+ Center admin ID.
Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter the DLP+ Center admin password.
Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter the DLP+ Center admin password again.
Access IP	15	Numbers, special characters (.)	Enter the valid IP of the DLP+ Center admin.

Recommendations

- ✓ Password should have at least 9 characters and include English letters, numbers and special characters.
- ✓ .

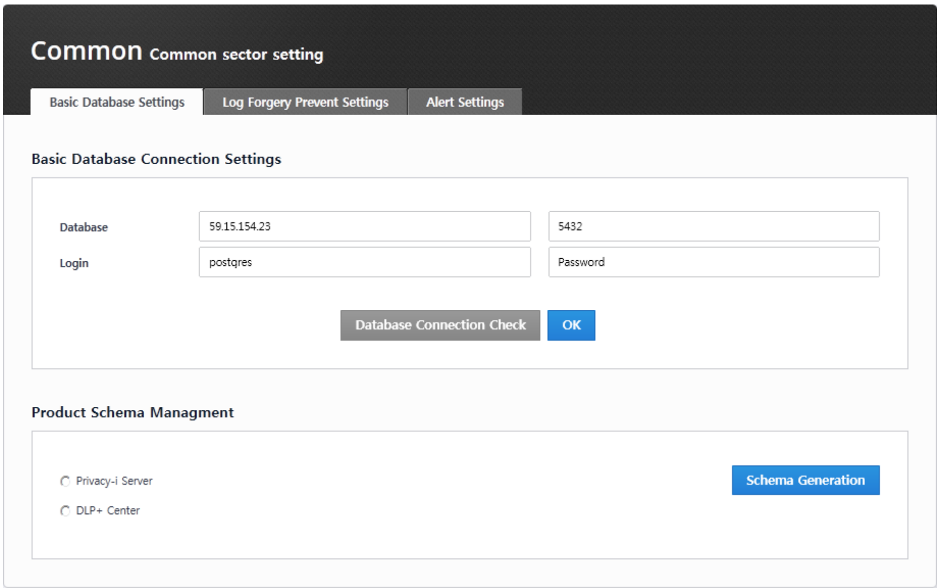
3.3 COMMON

3.3.1 Common Area Settings

Once the initial Configuration Manager setup is complete, the "Common Area Settings" menu appears. This initial page appears upon re-login to the Configuration Manager. The Common Items provide the Default Database Settings, Log Forgery/ Falsification Prevention, and Search Server Control of "Mail-i V8.0 for DLP+ Hyboost".

3.3.1.1 Default Database Connection Settings

The figure below is a screen where a common database connection can be set up. The common database shows input information in the "3.2.3 Enter Database Information" during initial installation. If the "Mail-i V8.0 for DLP+ HyBoost" database information is modified, it updates the information through "Default Database Connection Settings".



Common Common sector setting

Basic Database Connection Settings

Database	59.15.154.23	5432
Login	postgres	Password

Product Schema Managment

○ Privacy-i Server

○ DLP+ Center

(FIGURE 3-5) COMMON AREA SETTINGS SCREEN

After entering common database connection information, the session status can be checked through "Check Database Connection". If the connection failure window appears, please check if the account information is entered incorrectly, or the service status of the database.

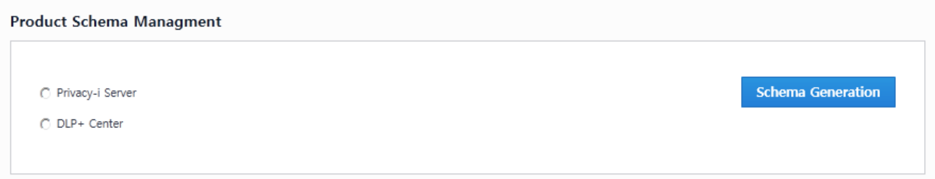
☞ Effective Input Field Range

[TABLE 1-2] EFFECTIVE INPUT FIELD RANGE UPON THE DEFAULT DATABASE CONNECTION

Item	Effective Range	Characters	Failure Message
Database (IP)	15	Numbers, special characters (.)	Enter the IP of the DB.
Database (Port)	1~65536	Numbers	Enter the port of the DB.
Login (ID)	5~256	Letters	Enter the login ID.
Login (Password)	9~70	Numbers, letters, special characters	Enter the password of the DB.

3.3.1.2 Product Schema Management

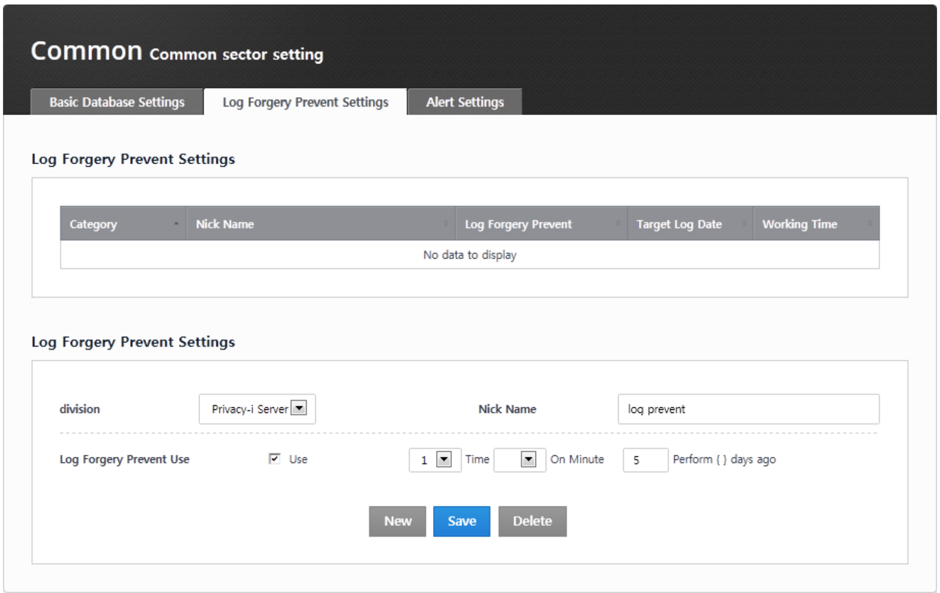
After the initial preference task, a task must be run through "Generate Schema" under Product Schema Management. This creates a database that is needed to run Mail-i Server, DLP+ Center, and the Schema is created in the database entered in the "Default Database Connection Settings". When "Generate Schema" is clicked, a notification window that displays, "If such information exists in the database, it will be removed. Do you want to continue?" is generated, and the initial data required for operating the selected Schema is created. Please note that the database information will be initialized if Generate Schema is continued while operating solutions.



(FIGURE 3-6) PRODUCT SCHEMA MANAGEMENT SCREEN

3.3.1.3 Log Forgery Prevention Settings

To prevent forgery or falsification of saved sensitive data logs, "Log Forgery Prevention" function is provided. To enable the preventive settings, the log database for Mail-i Server must be created in advance. When the Log Forgery Prevention function is enabled, logs are only viewed and deletion nor modification is not allowed, which help protect the logs of sensitive data.



Common Common sector setting

Log Forgery Prevent Settings

Category	Nick Name	Log Forgery Prevent	Target Log Date	Working Time
No data to display				

Log Forgery Prevent Settings

division: Privacy-i Server

Nick Name: log prevent

Log Forgery Prevent Use: ☑ Use 1 Time On Minute 5 Perform ( ) days ago

(FIGURE 3-7) LOG FORGERY PREVENTION SETTINGS SCREEN

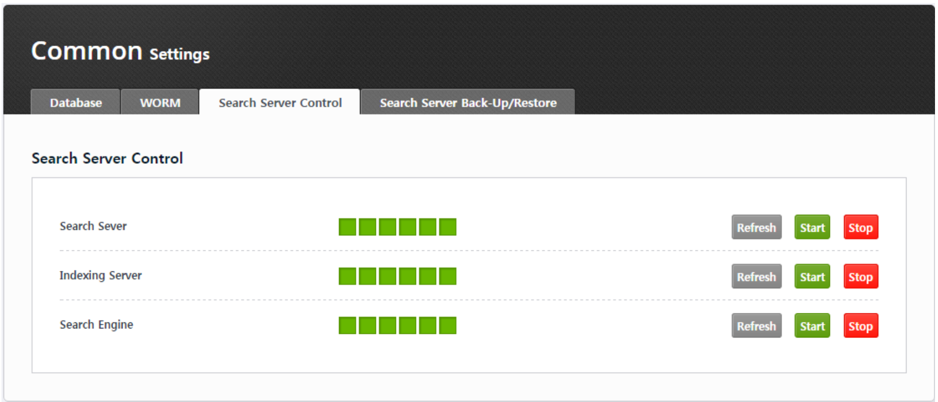
☞ Effective Input Field Range

[TABLE 3-5] EFFECTIVE INPUT FIELD RANGE OF WORM MANAGEMENT

Item	Effective Range	Character	Failure Message
Log Forgery Prevention function (Date)	1~9999	Numbers	Enter the target log date.

3.3.1.4 Search Server Control

The status of Search Server can be viewed and controlled. Specifically, Refresh, Start and Stop functions for Query Server, Indexing Server and/or Search Engine are provided.



Common Settings

Search Server Control

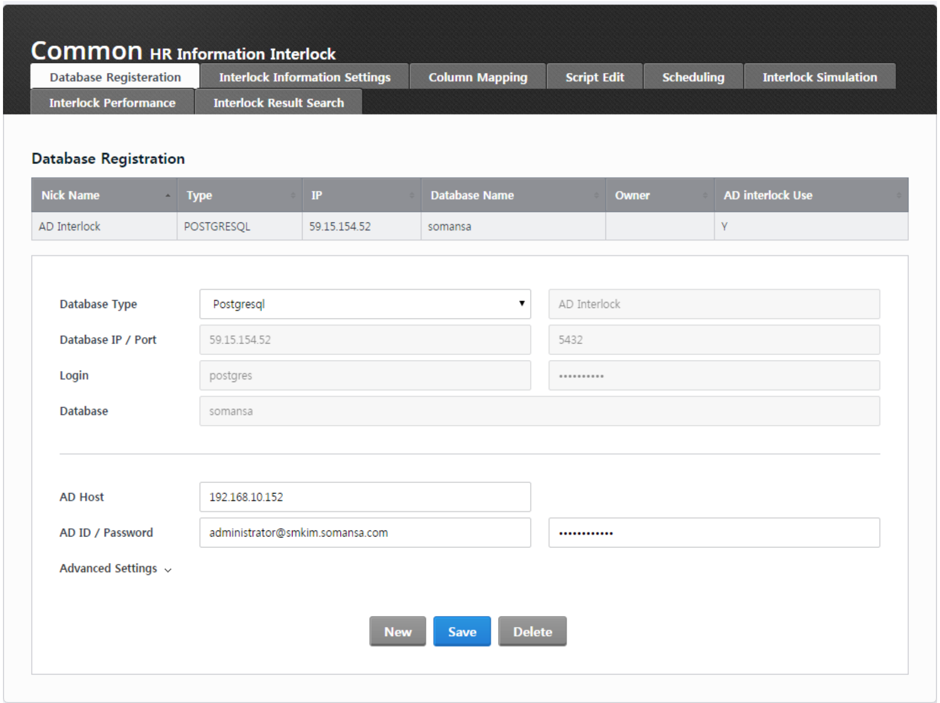
Search Sever	🟩🟩🟩🟩🟩🟩	Refresh Start Stop
Indexing Server	🟩🟩🟩🟩🟩🟩	Refresh Start Stop
Search Engine	🟩🟩🟩🟩🟩🟩	Refresh Start Stop

(FIGURE 3-8) COMMON – COMMON AREA SETTINGS – SEARCH SERVER CONTROL

3.3.2 HR Information Sync

3.3.2.1 Database Registration

Database to sync with HR information can be registered.



Common HR Information Interlock

Database Registration

Nick Name	Type	IP	Database Name	Owner	AD interlock Use
AD Interlock	POSTGRESQL	59.15.154.52	somansa		Y

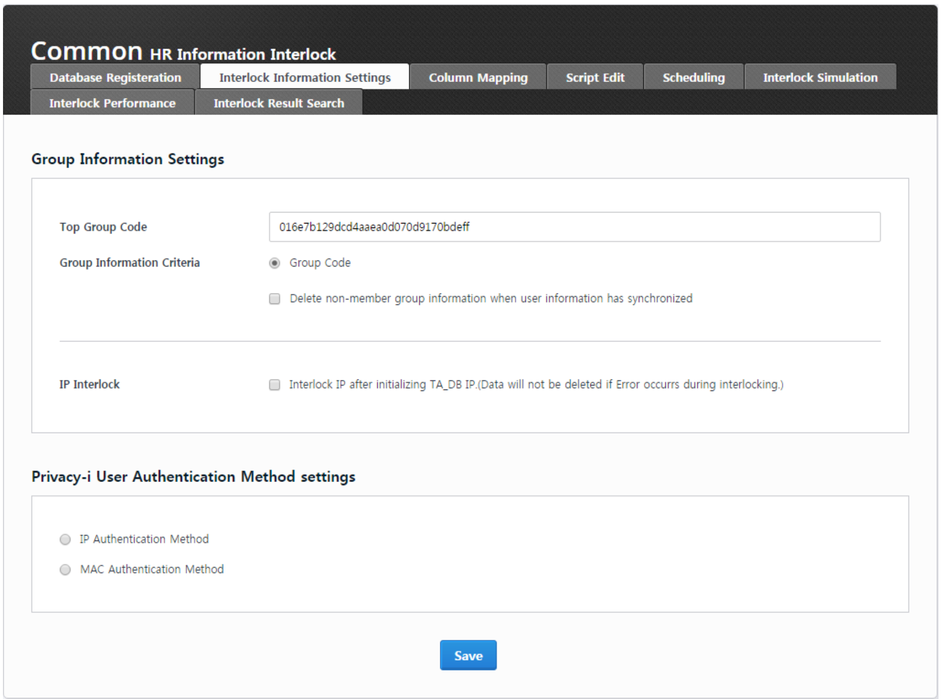
Database Type	Postgresql	AD Interlock
Database IP / Port	59.15.154.52	5432
Login	postgres	••••••••••
Database	somansa	
AD Host	192.168.10.152	
AD ID / Password	administrator@smkim.somansa.com	••••••••••••

Advanced Settings

(FIGURE 3-9) HR REGISTRATION SCREEN

3.3.2.2 Sync Information Settings

Department Information and Mail-i User Authentication can be configured.



Group Information Settings

Top Group Code: 016e7b129dcd4aaea0d070d9170bdeff

Group Information Criteria: ● Group Code

□ Delete non-member group information when user information has synchronized

IP Interlock: □ Interlock IP after initializing TA_DB IP.(Data will not be deleted if Error occurrs during interlocking.)

Privacy-i User Authentication Method settings

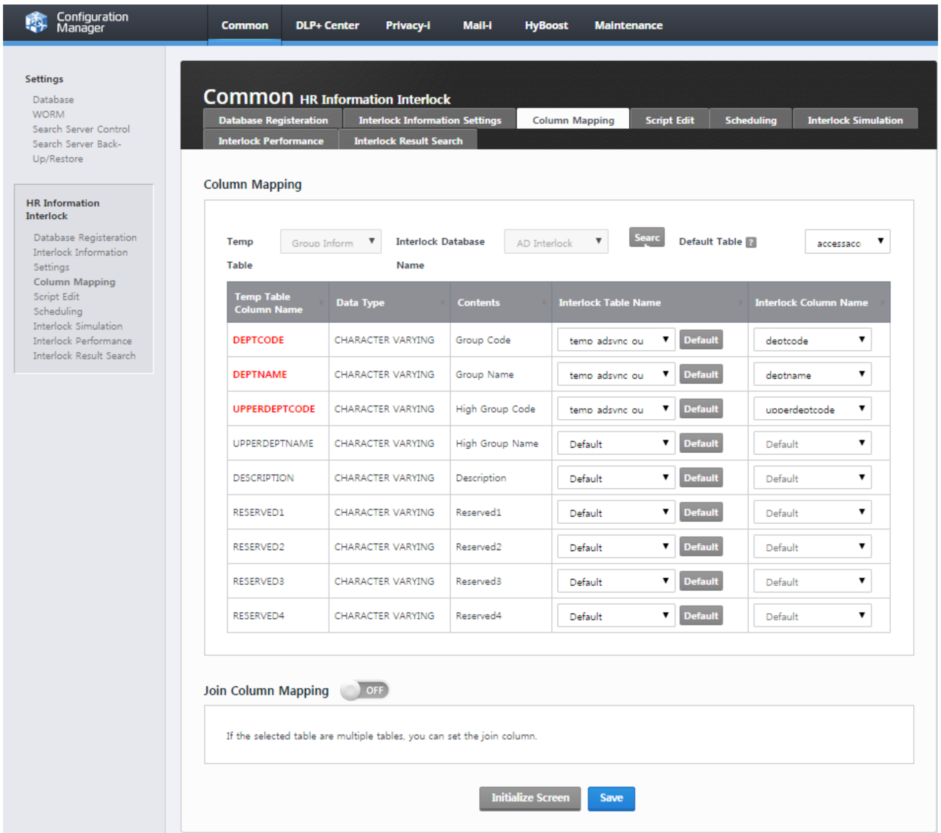
○ IP Authentication Method

○ MAC Authentication Method

(FIGURE 3-10) SYNC INFORMATION SETTING SCREEN

3.3.2.3 Column Mapping

Maps user information for the DLP+Center and user information in the HR information DB.



Column Mapping

Temp Table: Group Inform ▼ Interlock Database Name: AD Interlock ▼ Default Table ?: accessacc ▼

Temp Table Column Name	Data Type	Contents	Interlock Table Name	Interlock Column Name
DEPTCODE	CHARACTER VARYING	Group Code	temp adsvnc ou ▼ Default	deptcode ▼
DEPTNAME	CHARACTER VARYING	Group Name	temp adsvnc ou ▼ Default	deptname ▼
UPPERDEPTCODE	CHARACTER VARYING	High Group Code	temp adsvnc ou ▼ Default	upperdeptcode ▼
UPPERDEPTNAME	CHARACTER VARYING	High Group Name	Default ▼ Default	Default ▼
DESCRIPTION	CHARACTER VARYING	Description	Default ▼ Default	Default ▼
RESERVED1	CHARACTER VARYING	Reserved1	Default ▼ Default	Default ▼
RESERVED2	CHARACTER VARYING	Reserved2	Default ▼ Default	Default ▼
RESERVED3	CHARACTER VARYING	Reserved3	Default ▼ Default	Default ▼
RESERVED4	CHARACTER VARYING	Reserved4	Default ▼ Default	Default ▼

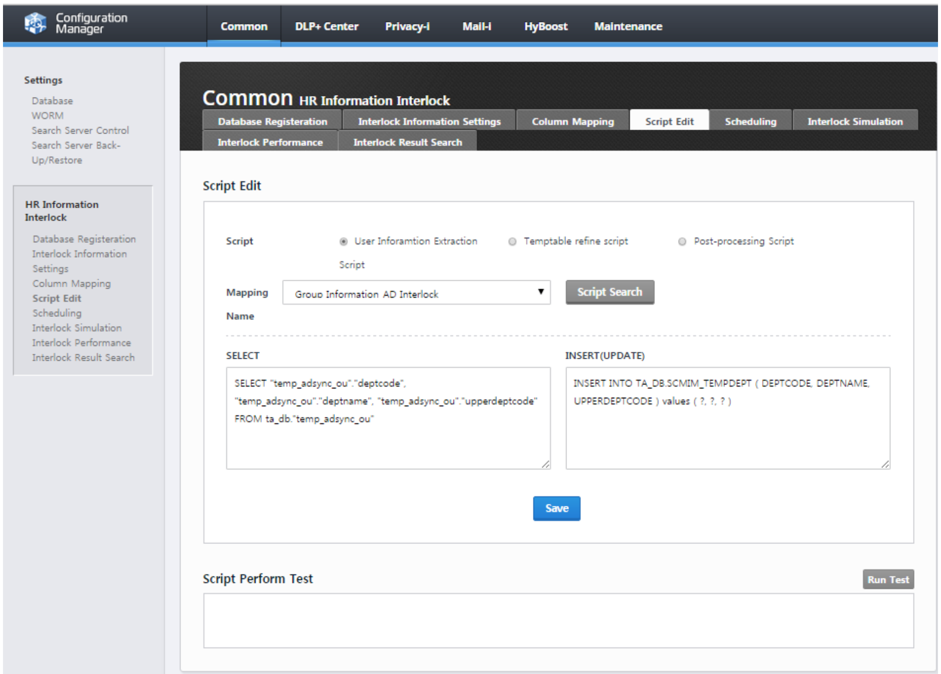
Join Column Mapping OFF

If the selected table are multiple tables, you can set the join column.

(FIGURE 3-11) COLUMN MAPPING SCREEN

3.3.2.4 Editing Script

Extracted Script of HR Information can be viewed and saved, or Refined Script of a Temporary Table can be created and saved. The results can be previewed through the Script Performance Test Results.



Script Edit

Script: ● User Inforamtion Extraction Script ○ Temptable refine script ○ Post-processing Script

Mapping Name: Group Information AD Interlock ▼

SELECT

```
SELECT "temp_adsync_ou"."deptcode",
"temp_adsync_ou"."deptname", "temp_adsync_ou"."upperdeptcode"
FROM ta_db."temp_adsync_ou"
```

INSERT(UPDATE)

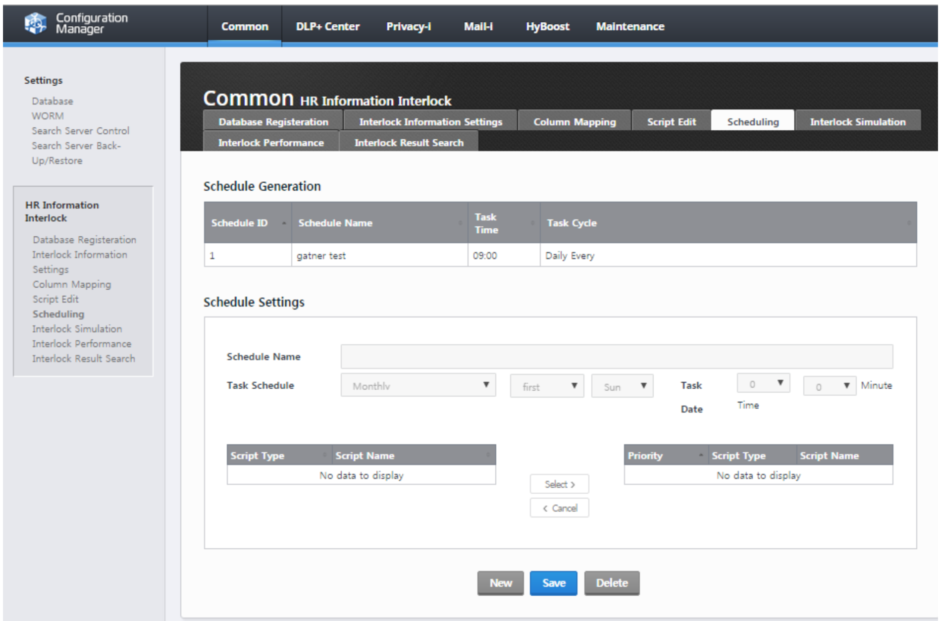
```
INSERT INTO TA_DB.SCMIM_TEMPDEPT ( DEPTCODE, DEPTNAME,
UPPERDEPTCODE ) values ( ?, ?, ? )
```

Script Perform Test

(FIGURE 3-12) EDIT SCRIPT SCREEN

3.3.2.5 Scheduling

When Scheduling is registered, it syncs with the HR information DB at regular intervals. Daily, weekly and monthly sync are available.



Schedule Generation

Schedule ID	Schedule Name	Task Time	Task Cycle
1	gatner test	09:00	Daily Every

Schedule Settings

Schedule Name

Task Schedule: Monthlv ▼ first ▼ Sun ▼ Task Date 0 ▼ 0 ▼ Minute Time

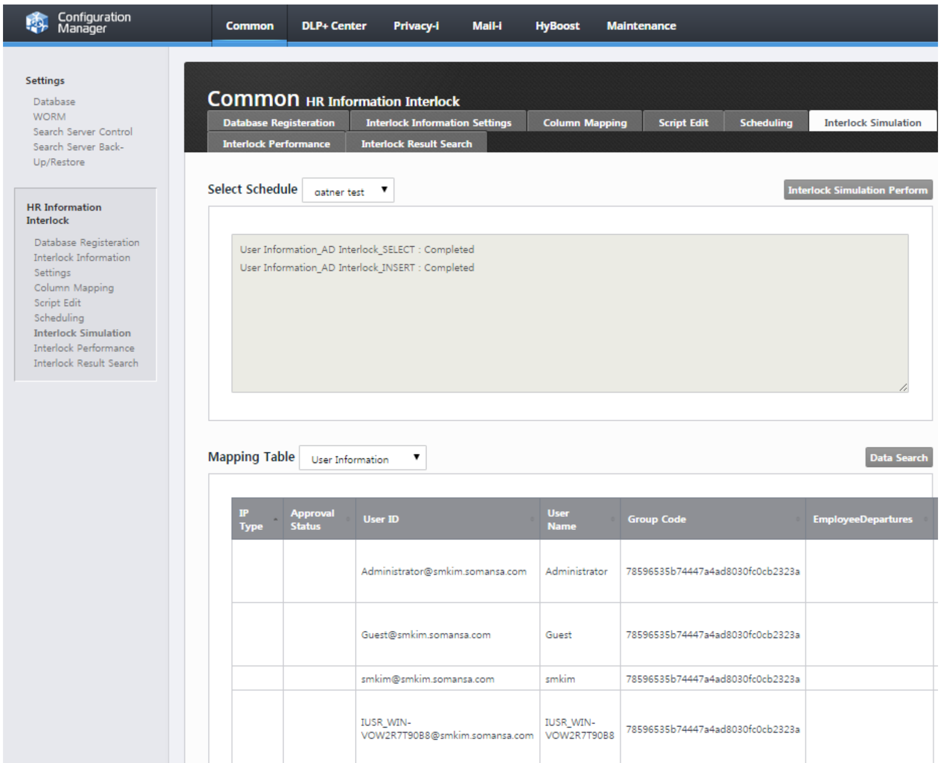
Script Type	Script Name
No data to display	

Priority	Script Type	Script Name
No data to display		

(FIGURE 3-13) SCHEDULING SCREEN

3.3.2.6 Sync Simulation

With Sync Simulation, HR information DB Sync that is registered for scheduling can be run. The results can be viewed through the mapping table.



Select Schedule: oatner test

```
User Information_AD Interlock_SELECT : Completed
User Information_AD Interlock_INSERT : Completed
```

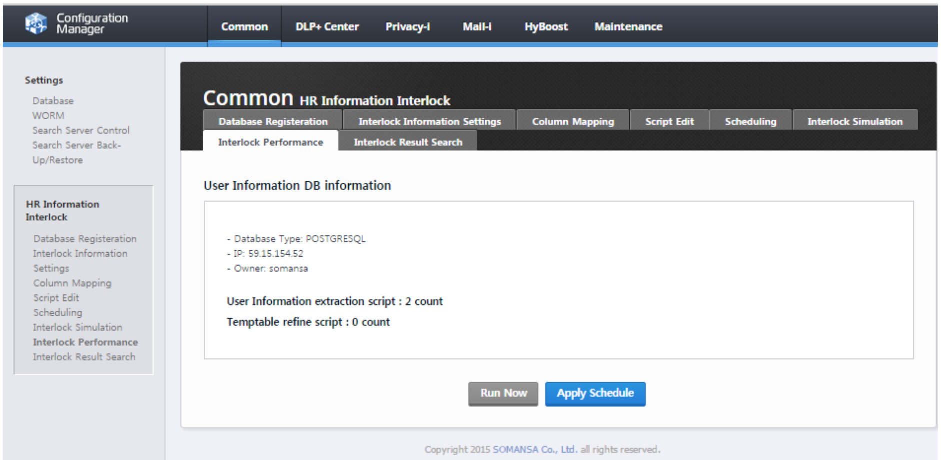
Mapping Table: User Information

IP Type	Approval Status	User ID	User Name	Group Code	EmployeeDepartures
		Administrator@smkim.somansa.com	Administrator	78596535b74447a4ad8030fc0cb2323a	
		Guest@smkim.somansa.com	Guest	78596535b74447a4ad8030fc0cb2323a	
		smkim@smkim.somansa.com	smkim	78596535b74447a4ad8030fc0cb2323a	
		IUSR_WIN-VOW2R7T90B8@smkim.somansa.com	IUSR_WIN-VOW2R7T90B8	78596535b74447a4ad8030fc0cb2323a	

(FIGURE 3-14) SYNC SIMULATION SCREEN

3.3.2.7 Running Sync

Runs the actual sync by applying schedules.



User Information DB information

- Database Type: POSTGRESQL
- IP: 59.15.154.52
- Owner: somansa

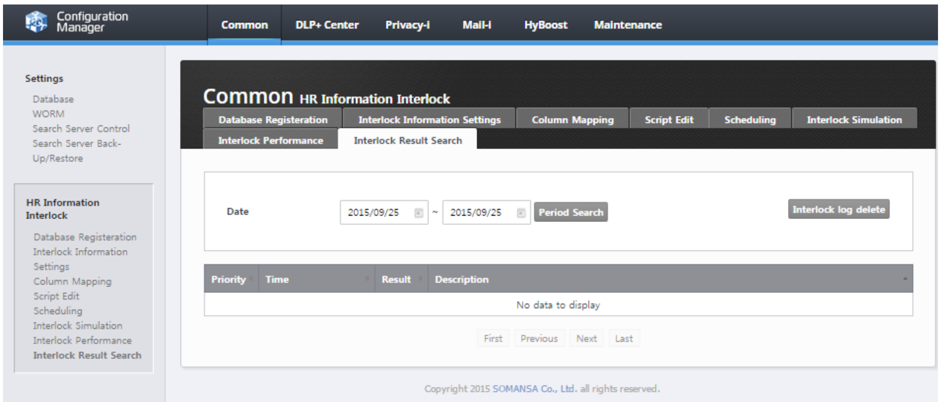
User Information extraction script : 2 count

Temptable refine script : 0 count

(FIGURE 3-15) RUNNING SYNC SCRREN

3.3.2.8 Sync Results

The Sync Results can be viewed.



Date 2015/09/25 ~ 2015/09/25

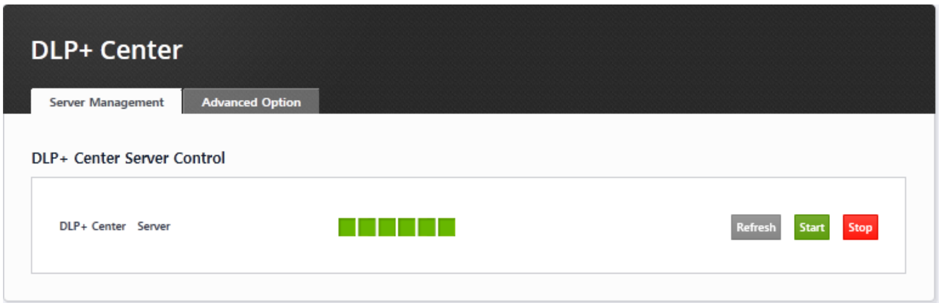
Priority	Time	Result	Description
No data to display			

(FIGURE 3-16) VIEW SYNC RESULTS SCREEN

3.4 DLP+ Center Settings

3.4.1 Server Management

The status of the DLP+ Center Server and its operation can be set. Restart, Start and Stop functions for the DLP+ Center Server are provided.



DLP+ Center

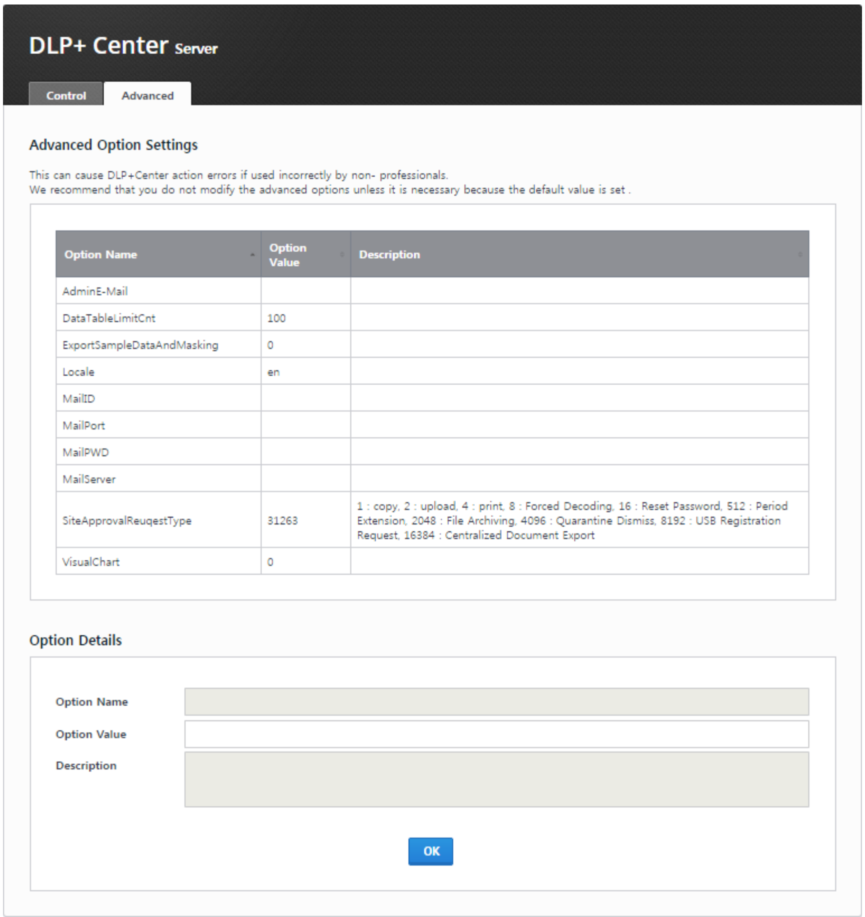
DLP+ Center Server Control

DLP+ Center Server 🟩🟩🟩🟩🟩🟩

(FIGURE 3-17) DLP+CENTER SERVER MANAGEMENT SCREEN

3.4.2 Advanced Options

Options for operating DLP+ Center can be selected.



Advanced Option Settings

This can cause DLP+Center action errors if used incorrectly by non- professionals.
We recommend that you do not modify the advanced options unless it is necessary because the default value is set .

Option Name	Option Value	Description
AdminE-Mail		
DataTableLimitCnt	100	
ExportSampleDataAndMasking	0	
Locale	en	
MailID		
MailPort		
MailPWD		
MailServer		
SiteApprovalReuqestType	31263	1 : copy, 2 : upload, 4 : print, 8 : Forced Decoding, 16 : Reset Password, 512 : Period Extension, 2048 : File Archiving, 4096 : Quarantine Dismiss, 8192 : USB Registration Request, 16384 : Centralized Document Export
VisualChart	0	

Option Details

Option Name
Option Value
Description

(FIGURE 3-18) DLP+CENTER ADVANCED OPTIONS

The options are provided by the DLP+ Center. However, the advanced functions can lead to errors in the DLP+ Center operation when used incorrectly by a non-experienced user. We recommend not modifying Advanced Options unless modification is absolutely necessary since default values are set. Please contact the Somansa Support Team if option changes must be checked. For the definitions of each option, please refer to the table below.

[TABLE 3-6] DEFINITION OF ADVANCED OPTIONS

Option	Definition
VisualChart	Whether to display chart in a report or not (0/1)
Locale	Set a locale for localization (ko/en)

DataTableLimitCnt	Number of table outputs (default 100)
AdmnE-mail	Email address of Security Admin
MailServer	Address for SMTP Mail Server
MailPWD	Password for SMTP Mail Server
MailID	ID for SMTP Mail Server
MailPort	Port for SMTP Mail Server
ExportSampleDataMasking	Options for exporting Incidents Excel 0 – Exclude sample data (include pattern name and number only) 1 – Include sample data + Masking 2 – Include sample data (Plain Text)

☞Effective Input Field Range

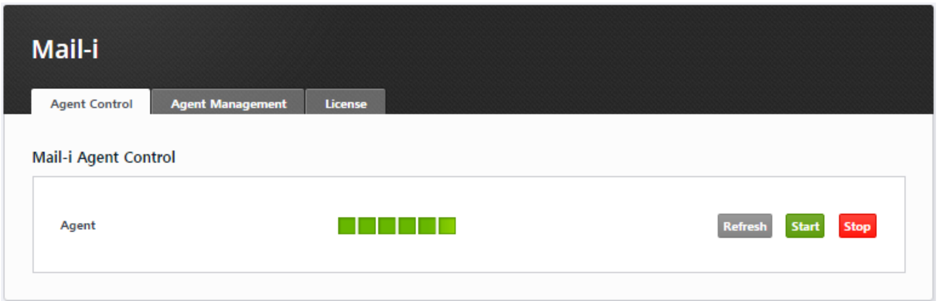
[TABLE 3-7] EFFECTIVE INPUT FIELD RANGE FOR ADVANCED OPTIONS

Item	Effective Range	Character	Failure Message
Values for Option	0~50	Numbers	Select an option

3.5 Mail-i Settings

3.5.1 Agent Control

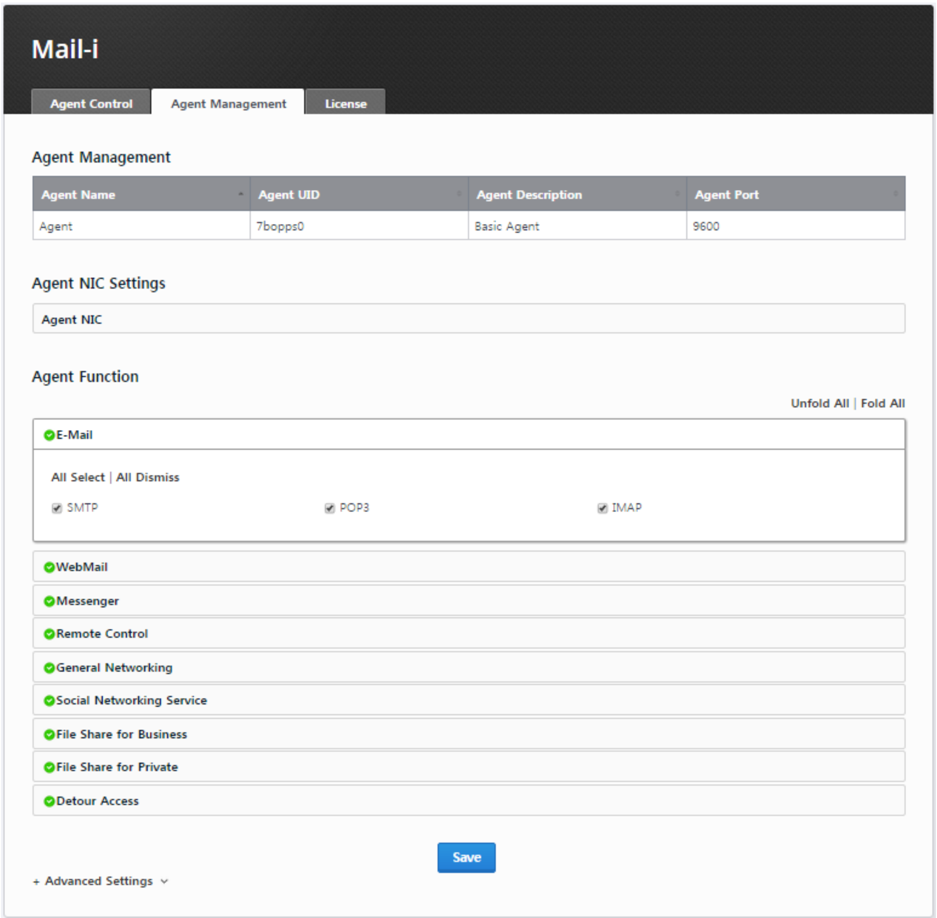
The status of Mail-i agents can be viewed and controlled. Restart, Start and Stop functions for agents are provided.



(FIGURE 3-19) MAIL-I SETTINGS – AGENT CONTROL

3.5.2 Agent Management

Mail-i Agents can be managed and controlled. Specifically, Agent NIC Settings, Functional Options, and Advanced Options are provided.



Mail-i

Agent Management

Agent Name	Agent UID	Agent Description	Agent Port
Agent	7bopps0	Basic Agent	9600

Agent NIC Settings

Agent NIC

Agent Function

E-Mail

☑ SMTP ☑ POP3 ☑ IMAP

WebMail

Messenger

Remote Control

General Networking

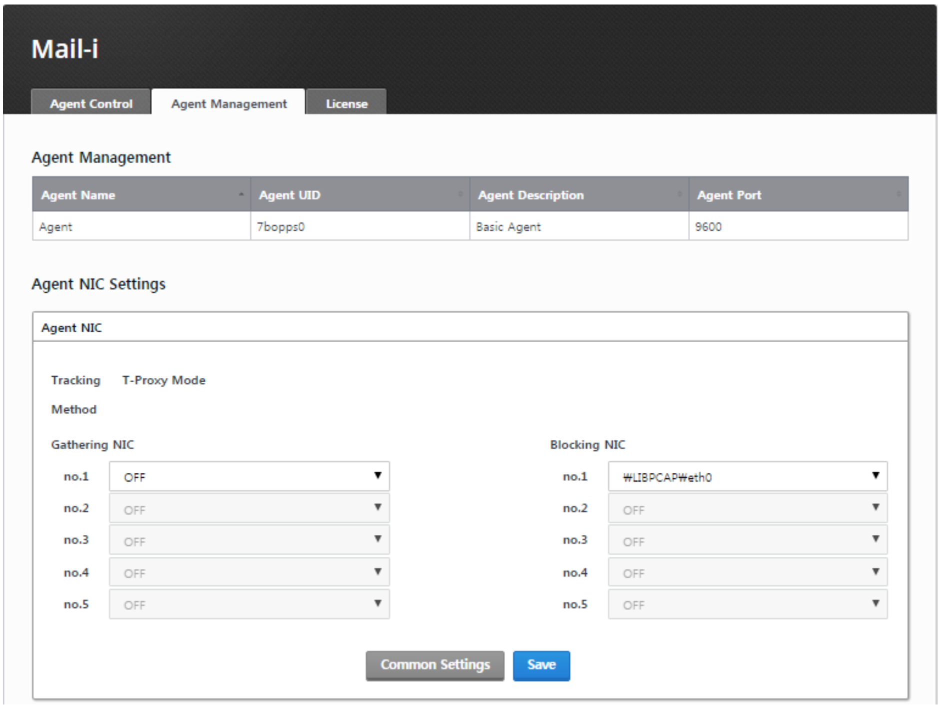
Social Networking Service

File Share for Business

File Share for Private

Detour Access

(FIGURE 3-20) MAIL-I SETTINGS – AGENT MANAGEMENT



Agent Management

Agent Name	Agent UID	Agent Description	Agent Port
Agent	7bopps0	Basic Agent	9600

Agent NIC Settings

Agent NIC

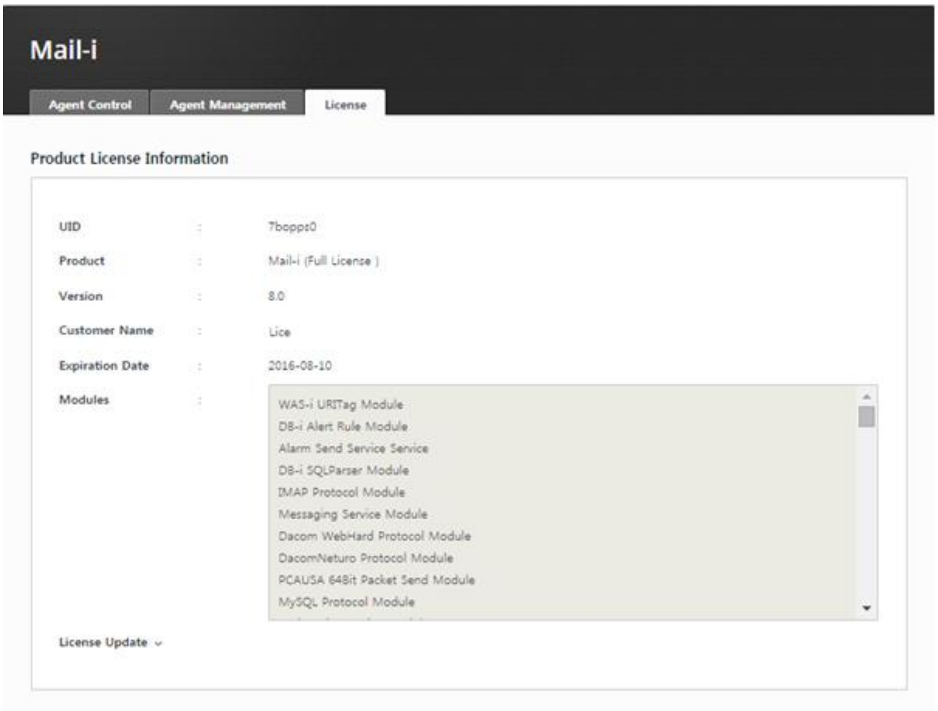
Tracking Method: T-Proxy Mode

Gathering NIC		Blocking NIC	
no.1	OFF	no.1	₩LIBPCAP₩eth0
no.2	OFF	no.2	OFF
no.3	OFF	no.3	OFF
no.4	OFF	no.4	OFF
no.5	OFF	no.5	OFF

(FIGURE 3-21) MAIL-I SETTINGS – AGENT MANAGEMENT - ADVANCED

3.5.3 License

UID/License expiration date/ number of users, etc. are displayed (see Receive License Issuance). Place the License received from the SOMANSA License Center in the /somansa/common/license folder to register the license as above. If the valid date of the License is expired or a License from another server is copied, main functions such as Data Pattern Update will not work. (See License Issuance)



Product License Information

UID : 7bopps0

Product : Mail-i (Full License)

Version : 8.0

Customer Name : Lice

Expiration Date : 2016-08-10

Modules :

WAS-i URITag Module
DB-i Alert Rule Module
Alarm Send Service Service
DB-i SQLParser Module
IMAP Protocol Module
Messaging Service Module
Dacom WebHard Protocol Module
DacomNeturo Protocol Module
PCAUSA 64Bit Packet Send Module
MySQL Protocol Module

License Update

(FIGURE 3-22) MAIL-I LICENSE

3.6 Maintenance

3.6.1 Regular Check

3.6.1.1 Regular Check

The current system status of Mail-i can be checked by Regular Check. The regular check result like the below figure will be displayed by selecting the product to check as Mail-i, setting the period of viewing Log DB and clicking the Regular Check button.

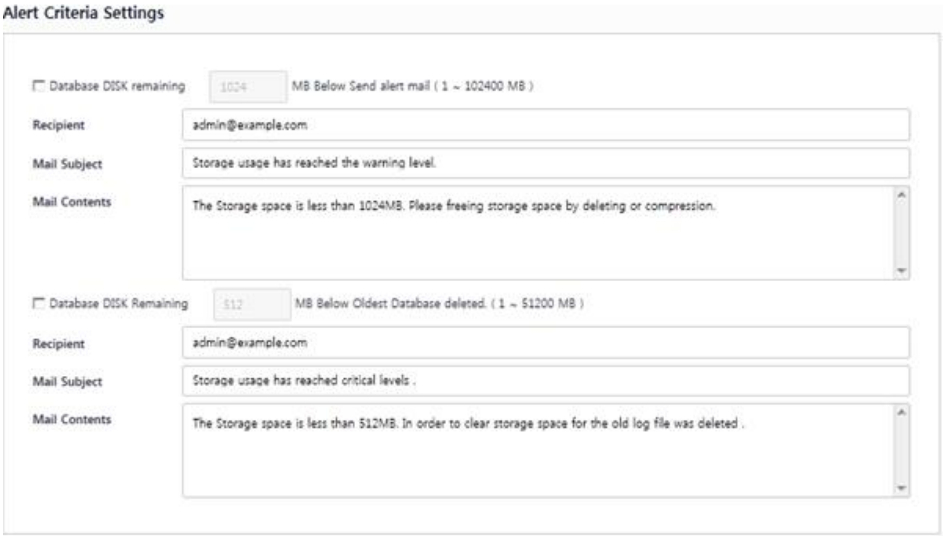
3.6.1.2 Check Histories

The histories of checks which has been performed per period can be viewed. The check reports also are provided by clicking the details.

3.6.2 System Alert Settings

3.6.2.1 Alert Settings

Mail-i system automatically alert any abnormalities through email if a threshold previously defined is reached. Specifically, thresholds for automatic alert for CPU occupancy, memory occupancy, available disk space, database operation, Mail-i query server, agent operation, license expiration, search engine status, indexing server status, and loss of logs can be set.



Alert Criteria Settings

□ Database DISK remaining 1024 MB Below Send alert mail (1 ~ 102400 MB)

Recipient: admin@example.com

Mail Subject: Storage usage has reached the warning level.

Mail Contents: The Storage space is less than 1024MB. Please freeing storage space by deleting or compression.

□ Database DISK Remaining 512 MB Below Oldest Database deleted. (1 ~ 51200 MB)

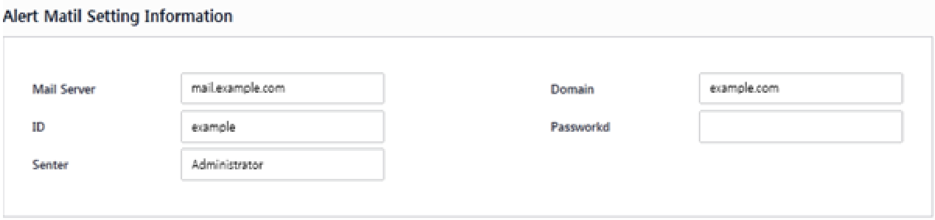
Recipient: admin@example.com

Mail Subject: Storage usage has reached critical levels .

Mail Contents: The Storage space is less than 512MB. In order to clear storage space for the old log file was deleted .

(FIGURE 3-23) ALERT SETTINGS SCREEN EXAMPLE

3.6.2.2 Alert Mail Settings



Alert Matil Setting Information

Mail Server	mail.example.com	Domain	example.com
ID	example	Passworkd	
Senter	Administrator		

(FIGURE 3-24) ALERT MAIL SETTINGS SCREEN EXAMPLE

☞ Effective Input Field Range

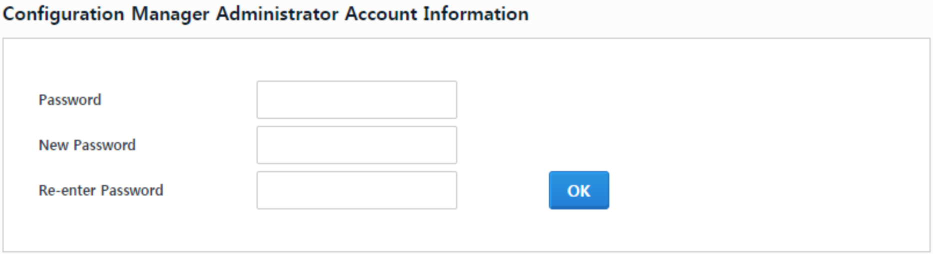
[TABLE 3-8] EFFECTIVE INPUT FIELD RANGE FOR ALERT SETTINGS

Item	Effective Range	Character	Failure Message
Database Disk Size (Alert Mail)	1~102400	Numbers	-.
Database Disk Size (Delete)	1~51200	Numbers	-
Recipient (Alert Mail, Delete)	1~50	Numbers, letters, special characters	Enter the recipient.
Mail Subject (Alert Mail, Delete)	1~100	Numbers, letters, special characters	-
Mail Content (Alert Mail, Delete)	1~2000	Numbers, letters, special characters	-.
Mail Server	1~30	Numbers, special characters	Enter the mail server.
Domain	1~30	Numbers, special characters	Enter the domain.
ID	5~30	Numbers, special characters	Enter ID.
Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter password.
Sender	1~50	Numbers, letters, special characters	Enter the sender.

3.7 Preferences

3.7.1 Configuration Manger Administrator Account Information

Password for the Security Admin can be changed. To change the password, enter the current password, a new password and new password confirmation. We recommend changing passwords regularly for security purposes.



Configuration Manager Administrator Account Information

Password

New Password

Re-enter Password

(FIGURE 3-25) CONFIGURATION MANAGER ADMINISTRATOR ACCOUNT INFORMATION

☞ Effective Input Field Range

[TABLE 3-9] EFFECTIVE INPUT FIELD RANGE FOR CONFIGURATION MANAGER ADMIN ACCOUNT

Item	Effective Range	Character	Failure Message
Current Password	9~12	Numbers, uppercase/ lowercase letters, special characters	Enter the password for the current admin account.
New Password	9~12	Numbers, uppercase/ lowercase letters, special characters	Enter the new password for the admin account.
Confirm Password	9~12	Numbers, uppercase/ lowercase letters, special characters	Enter the new password for the admin account again.

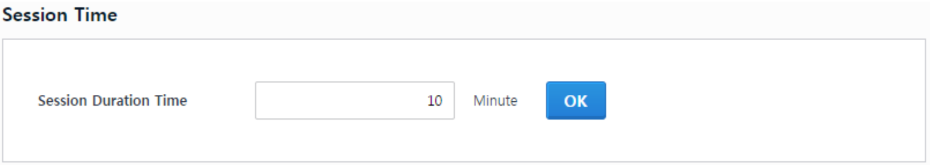
Recommendations

✓ Password should have at least 9 characters and include English letters, numbers and special characters.

✓

3.7.2 Session Time

Set the Session Duration of the Configuration Manager.



Session Time

Session Duration Time 10 Minute

(FIGURE 3-26) SESSION TIME

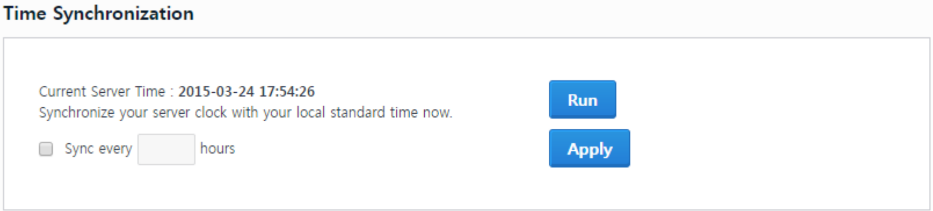
☞ Effective Input Field Range

[TABLE 3-10] EFFECTIVE INPUT FIELD RANGE FOR SESSION TIME SETTINGS

Item	Effective Range	Character	Failure Message
Session Duration	1~10	Numbers	Enter the session duration.

3.7.3 Time Synchronization

Synchronizes the time between product modules in standard time based on the NTP Server.



Time Synchronization

Current Server Time : 2015-03-24 17:54:26

Synchronize your server clock with your local standard time now.

□ Sync every [ ] hours

(FIGURE 3-27) TIME SYNCHRONIZATION

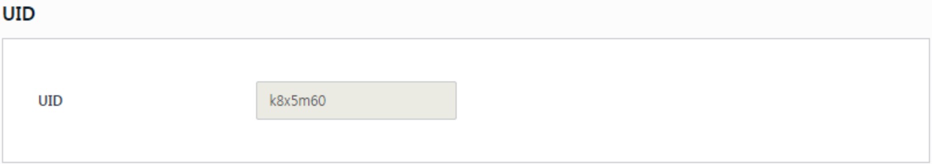
☞ Effective Input Field Range

[TABLE 3-11] EFFECTIVE INPUT FIELD RANGE FOR TIME SYNCHRONIZATION

Item	Effective Range	Character	Failure Message
Synchronization Cycle	1~99	Numbers	Enter a synchronization cycle.

3.7.4 UID

The server UID information can be viewed for license issuance.



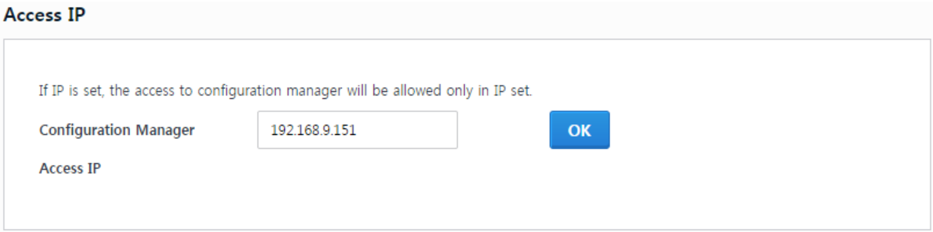
UID

UID: k8x5m60

(FIGURE 3-28) UID

3.7.5 Access IP

Configures Access IP to the Configuration Manager. The Configuration Manger can be connected from a total of 2 IPs, including a local IP and a set IP.



Access IP

If IP is set, the access to configuration manager will be allowed only in IP set.

Configuration Manager Access IP: 192.168.9.151

(FIGURE 3-29) ACCESS IP SETTINGS

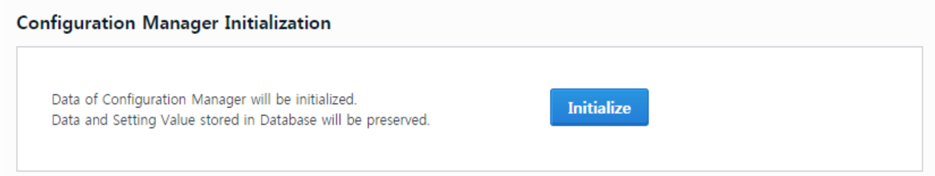
☞ Effective Input Field Range

[TABLE 3-12] EFFECTIVE INPUT FIELD RANGE FOR ACCESS IP SETTINGS

Item	Effective Range	Character	Failure Message
Control Panel Access IP	15	Numbers, special characters (.)	Enter the Control Panel Access IP.

3.7.6 Configuration Manger Initialization

Initializes Configuration Manager settings. Initializes the product setting information and returns to status after installation. Data and setting value that are stored in the database will be preserved.



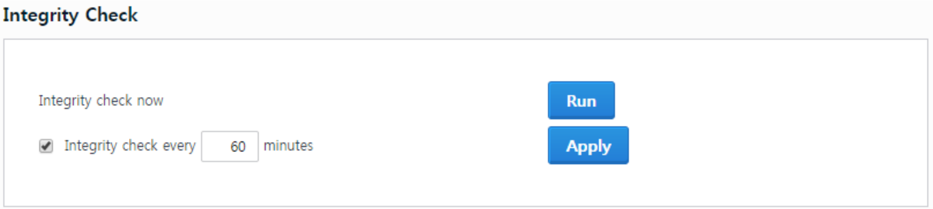
Configuration Manager Initialization

Data of Configuration Manager will be initialized.
Data and Setting Value stored in Database will be preserved.

(FIGURE 3-30) CONFIGURATION MANAGER INITIALIZATION

3.7.7 Integrity Check

Sets the Integrity function of the product. The Integrity Inspection provides two methods, which include running a scheduled task, and a Security Admin clicking the "Run Now" button. This function is not activated by default, but can be used after checking 'Integrity Cycle'.



Integrity Check

Integrity check now

☑ Integrity check every 60 minutes

(FIGURE 3-31) INTEGRITY CHECK

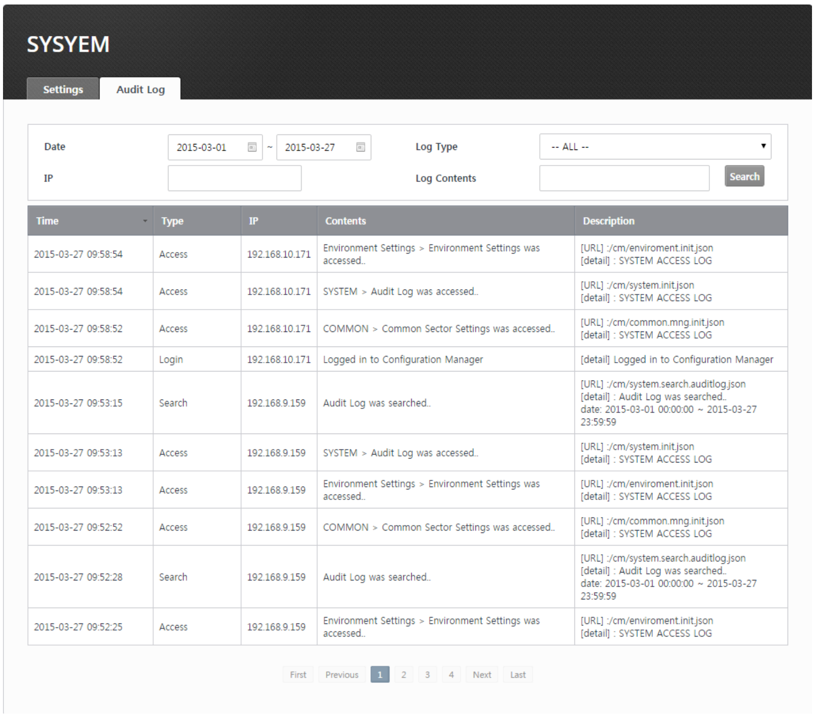
☞ Effective Input Field Range

[TABLE 3-13] EFFECTIVE INPUT FIELD RANGE FOR INTEGRITY CHECK

Item	Effective Range	Character	Failure Message
Integrity Cycle	99	Numbers	Enter the integrity function cycle.

3.8 SYSTEM Audit Logs

This screen shows Audit Logs of the SYSTEM. All events of the Security Admin from the initial installation to operation are saved. In addition, Audit Logs can be viewed by setting the desired time period. The Audit Logs are displayed by categorizing Date, Type, IP, Content and Description.



Date 2015-03-01 ~ 2015-03-27

Log Type -- ALL --

IP

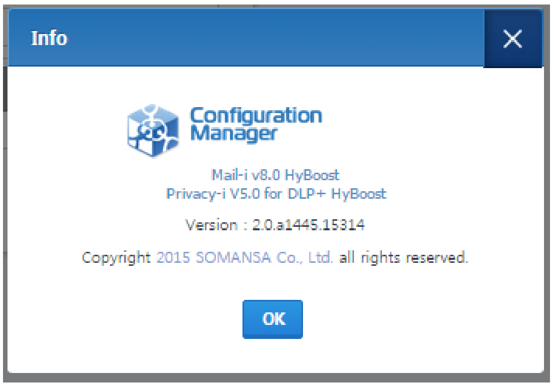
Log Contents

Time	Type	IP	Contents	Description
2015-03-27 09:58:54	Access	192.168.10.171	Environment Settings > Environment Settings was accessed..	[URL] :/cm/enviroment.init.json [detail] : SYSTEM ACCESS LOG
2015-03-27 09:58:54	Access	192.168.10.171	SYSTEM > Audit Log was accessed..	[URL] :/cm/system.init.json [detail] : SYSTEM ACCESS LOG
2015-03-27 09:58:52	Access	192.168.10.171	COMMON > Common Sector Settings was accessed..	[URL] :/cm/common.mng.init.json [detail] : SYSTEM ACCESS LOG
2015-03-27 09:58:52	Login	192.168.10.171	Logged in to Configuration Manager	[detail] Logged in to Configuration Manager
2015-03-27 09:53:15	Search	192.168.9.159	Audit Log was searched..	[URL] :/cm/system.search.auditlog.json [detail] : Audit Log was searched.. date: 2015-03-01 00:00:00 ~ 2015-03-27 23:59:59
2015-03-27 09:53:13	Access	192.168.9.159	SYSTEM > Audit Log was accessed..	[URL] :/cm/system.init.json [detail] : SYSTEM ACCESS LOG
2015-03-27 09:53:13	Access	192.168.9.159	Environment Settings > Environment Settings was accessed..	[URL] :/cm/enviroment.init.json [detail] : SYSTEM ACCESS LOG
2015-03-27 09:52:52	Access	192.168.9.159	COMMON > Common Sector Settings was accessed..	[URL] :/cm/common.mng.init.json [detail] : SYSTEM ACCESS LOG
2015-03-27 09:52:28	Search	192.168.9.159	Audit Log was searched..	[URL] :/cm/system.search.auditlog.json [detail] : Audit Log was searched.. date: 2015-03-01 00:00:00 ~ 2015-03-27 23:59:59
2015-03-27 09:52:25	Access	192.168.9.159	Environment Settings > Environment Settings was accessed..	[URL] :/cm/enviroment.init.json [detail] : SYSTEM ACCESS LOG

(FIGURE 3-32) VIEW SYSTEM AUDIT LOGS

3.9 Check Configuration Manager Version

The version of the Configuration Manager can be checked on this screen. Click the ⓘ button at the top right to check the version.



Mail-i v8.0 HyBoost
Privacy-i V5.0 for DLP+ HyBoost

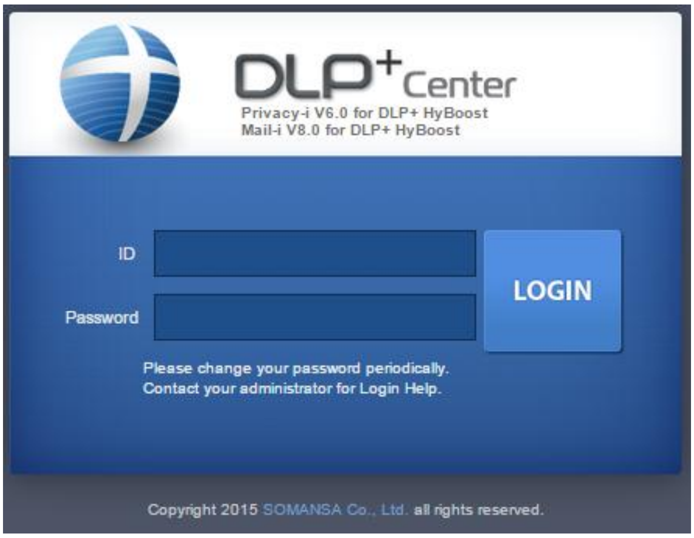
Version : 2.0.a1445.15314

Copyright 2015 SOMANSA Co., Ltd. all rights reserved.

(FIGURE 3-33) CHECK CONFIGURATION MANAGER VERSION

4. DLP+ Center

Mail-i is a solution for data loss prevention that allows organizations to prevent users from accessing internal information and leaking it outside. In addition, Mail-i provides a Network Data Loss Prevention solution, which logs, monitors and controls outgoing email, instant messages, attachments and other application information in real time. Mail-i is operated and managed by the DLP+ Center, a central management console. Since the DLP+ Center is operated as a web server, the authorized admin can connect to the DLP+ Center through the company intranet anytime and anywhere for a convenient operating environment.


DLP+ Center
Privacy-i V6.0 for DLP+ HyBoost
Mail-i V8.0 for DLP+ HyBoost
ID
Password
LOGIN
Please change your password periodically.
Contact your administrator for Login Help.
Copyright 2015 SOMANSA Co., Ltd. all rights reserved.

(FIGURE 4-1) DLP+ CENTER LOGIN

When the DLP+ Center URL address is entered into a web browser, a login screen appears as shown in (Figure 4-2). When the account information set in Configuration Manager is entered, the DLP+ Center can be successfully logged in. Please note that the session becomes locked if the wrong password is entered more than 3 times.

☞ Effective Input Field Range

[TABLE 4-1] EFFECTIVE INPUT FIELD RANGE UPON DLP+ CENTER LOGIN

Items	Effective Range	Character	Failure Message

ID	5~100	Letters	Enter the ID.
Password	9~41	Numbers, Uppercase/ Lowercase Letters, Special Characters	Enter the password.

Recommendation

- ✓ Password should have at least 9 characters and include English letters, numbers and special characters.
- ✓

4.1 Dashboard

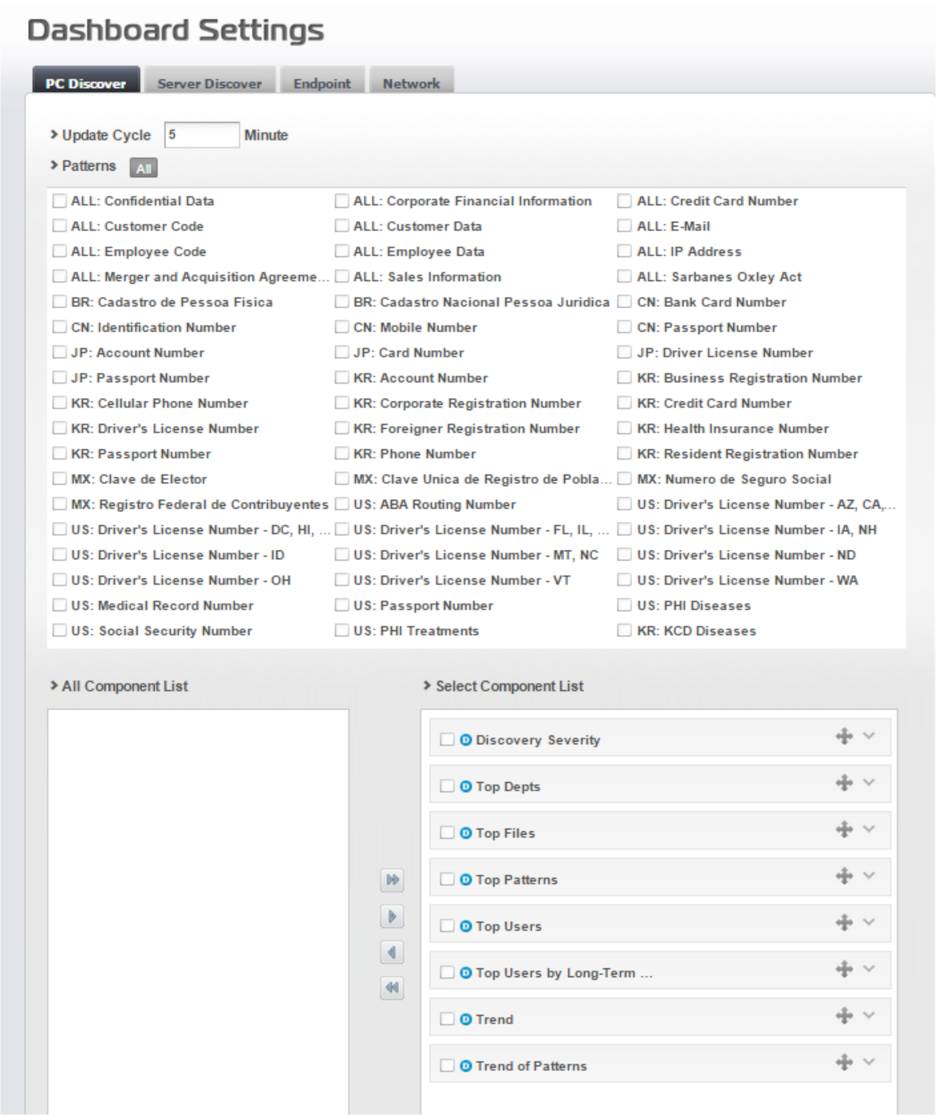
Dashboard provides department or user-specific data retained, leakage path and data in real time. Such data are composed of components, and are displayed in order based on the most recent, or retained sensitive data. It has the advantage of quickly identifying the severity of retained data and retaining status by selecting the component and pattern and setting specific users/groups for intensive monitoring.

4.1.1 Network

Network Dashboard provides number of data and patterns by channels and users in real time. Network has 7 components, including 'Network Severity', 'Top Depts', 'Top Users', 'Top Channels', 'Trend', 'Trend of Patterns' and 'Top Patterns'.

4.1.2 Settings

The Figure below is the Preferences screen where Dashboard data information can be configured. The options that can be selected in the Settings are Select Component, Select Pattern to be used for each component, and Renewal Cycle and displays the data applied to the Dashboard according to this set value.



Dashboard Settings

› Update Cycle 5 Minute

› Patterns All

☐ ALL: Confidential Data
☐ ALL: Customer Code
☐ ALL: Employee Code
☐ ALL: Merger and Acquisition Agreeme...
☐ BR: Cadastro de Pessoa Fisica
☐ CN: Identification Number
☐ JP: Account Number
☐ JP: Passport Number
☐ KR: Cellular Phone Number
☐ KR: Driver's License Number
☐ KR: Passport Number
☐ MX: Clave de Elector
☐ MX: Registro Federal de Contribuyentes
☐ US: Driver's License Number - DC, HI, ...
☐ US: Driver's License Number - ID
☐ US: Driver's License Number - OH
☐ US: Medical Record Number
☐ US: Social Security Number
☐ ALL: Corporate Financial Information
☐ ALL: Customer Data
☐ ALL: Employee Data
☐ ALL: Sales Information
☐ BR: Cadastro Nacional Pessoa Juridica
☐ CN: Mobile Number
☐ JP: Card Number
☐ KR: Account Number
☐ KR: Corporate Registration Number
☐ KR: Foreigner Registration Number
☐ KR: Phone Number
☐ MX: Clave Unica de Registro de Pobla...
☐ US: ABA Routing Number
☐ US: Driver's License Number - FL, IL, ...
☐ US: Driver's License Number - MT, NC
☐ US: Driver's License Number - VT
☐ US: Passport Number
☐ US: PHI Treatments
☐ ALL: Credit Card Number
☐ ALL: E-Mail
☐ ALL: IP Address
☐ ALL: Sarbanes Oxley Act
☐ CN: Bank Card Number
☐ CN: Passport Number
☐ JP: Driver License Number
☐ KR: Business Registration Number
☐ KR: Credit Card Number
☐ KR: Health Insurance Number
☐ KR: Resident Registration Number
☐ MX: Numero de Seguro Social
☐ US: Driver's License Number - AZ, CA,...
☐ US: Driver's License Number - IA, NH
☐ US: Driver's License Number - ND
☐ US: Driver's License Number - WA
☐ US: PHI Diseases
☐ KR: KCD Diseases

› All Component List

› Select Component List

☐ Discovery Severity
☐ Top Depts
☐ Top Files
☐ Top Patterns
☐ Top Users
☐ Top Users by Long-Term ...
☐ Trend
☐ Trend of Patterns

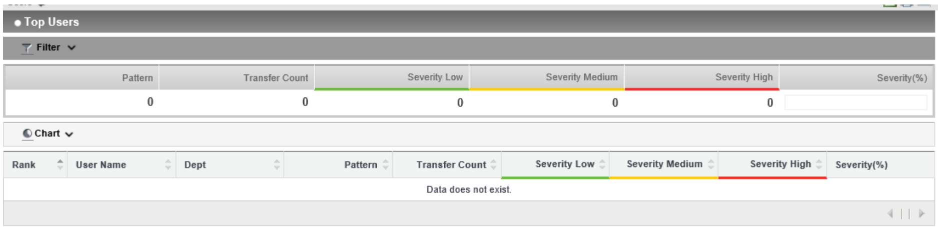
(FIGURE 4-2) DASHBOARD SETTINGS

4.2 Reports

Reports shows the results of conditional analysis performed about confidential data transmitted by departments and users. Since Reports display a variety of graphs, lists and main result items of the detected results, the Admin has the advantage of being able to quickly analyze according to the selected criteria. Reports consists of five components; Top Users, Top Depts, Trends, Top Categories and Top Patterns.

4.2.1 Top Users

Display the top users who transmitted data patterns in order. The number of patterns and transmissions is shown by users. The details of types and number of patterns and the number of transmissions are also shown below the user when selected.



● Top Users

Filter

Pattern	Transfer Count	Severity Low	Severity Medium	Severity High	Severity(%)
0	0	0	0	0	

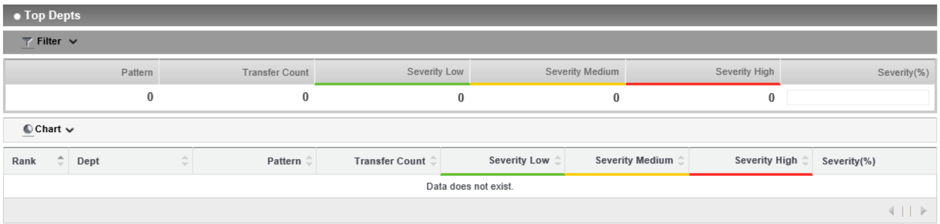
Chart

Rank	User Name	Dept	Pattern	Transfer Count	Severity Low	Severity Medium	Severity High	Severity(%)
Data does not exist.								

(FIGURE 4-3) REPORT – TOP USERS

4.2.2 Top Depts

Displays the departments in the order of data patterns transmitted. The number of patterns and transmissions is shown by departments. The details of types and number of patterns and the number of transmissions are also shown below the department when selected.



● Top Depts

Filter

Pattern	Transfer Count	Severity Low	Severity Medium	Severity High	Severity(%)
0	0	0	0	0	

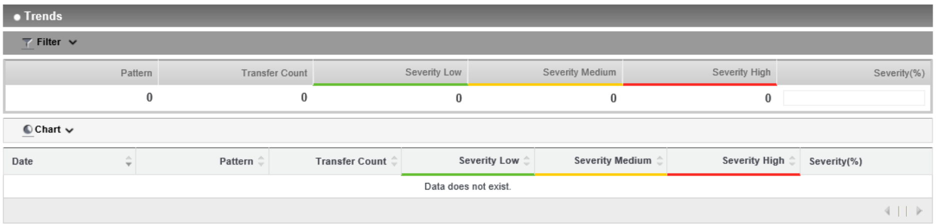
Chart

Rank	Dept	Pattern	Transfer Count	Severity Low	Severity Medium	Severity High	Severity(%)
Data does not exist.							

(FIGURE 4-4) REPORT – TOP DEPTS

4.2.3 Trends

Displays the trends of data patterns transmitted. The number of patterns and transmissions is shown by dates. The details of types and number of patterns and the number of transmissions for the selected date are also shown below the date when selected.



● Trends

Filter

Pattern	Transfer Count	Severity Low	Severity Medium	Severity High	Severity(%)
0	0	0	0	0	

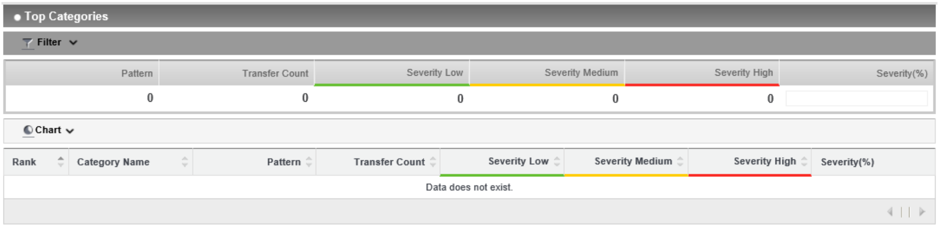
Chart

Date	Pattern	Transfer Count	Severity Low	Severity Medium	Severity High	Severity(%)
Data does not exist.						

(FIGURE 4-5) REPORT – TRENDS

4.2.4 Top Categories

Shows categories of data patterns transmitted. The number of patterns and transmissions is shown by categories.



● Top Categories

Filter

Pattern	Transfer Count	Severity Low	Severity Medium	Severity High	Severity(%)
0	0	0	0	0	

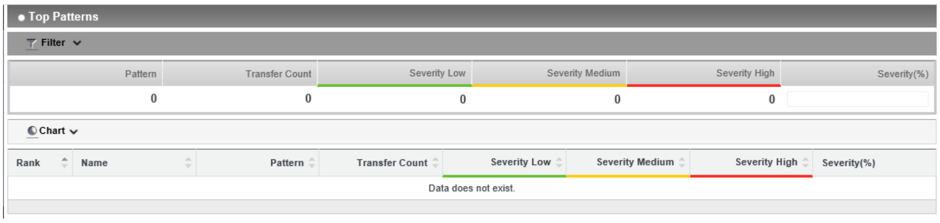
Chart

Rank	Category Name	Pattern	Transfer Count	Severity Low	Severity Medium	Severity High	Severity(%)
Data does not exist.							

(FIGURE 4-6) REPORT – TOP CATEGORIES

4.2.5 Top Patterns

Displays confidential data patterns in the order of transmission. The number of patterns and transmissions is shown by the type of patterns.



● Top Patterns

Filter

Pattern	Transfer Count	Severity Low	Severity Medium	Severity High	Severity(%)
0	0	0	0	0	

Chart

Rank	Name	Pattern	Transfer Count	Severity Low	Severity Medium	Severity High	Severity(%)
Data does not exist.							

(FIGURE 4-7) REPORT – TOP PATTERNS

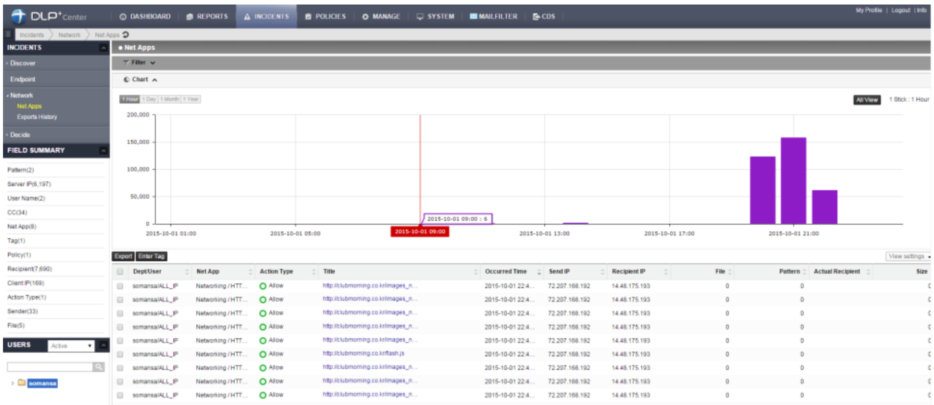
4.3 Incidents

4.3.1 Network

Networkpplications that are outgoing through Internet can be logged and viewed. The types of NetworkApplications include email, web mail, messenger, generic networking, social networking service, business file share, personal file share, alternate routing and media share. Also, logs for Network Applications retaining confidential data can be monitored. The types of data supported include; resident registration number, foreigner registration number, driver license number, passport number, bank account number, credit card number, cell phone number, phone number, email address, IP address, corporate registration number, business registration number and healthcare insurance number.

4.3.2 Net Apps

The data of users and departments, Net Apps, actions, subjects, number of files/patterns and dates can be viewed.



□	Dept/User	Net App	Action Type	Title	Occurred Time	Send IP	Recipient IP	File	Pattern	Actual Recipient	Size
□	somansa/ALL_IP	Networking / HTT...	○ Allow	http://clubmorning.co.kr/images_n...	2015-10-01 22:4...	72.207.168.192	14.48.175.193	0	0		0
□	somansa/ALL_IP	Networking / HTT...	○ Allow	http://clubmorning.co.kr/images_n...	2015-10-01 22:4...	72.207.168.192	14.48.175.193	0	0		0
□	somansa/ALL_IP	Networking / HTT...	○ Allow	http://clubmorning.co.kr/images_n...	2015-10-01 22:4...	72.207.168.192	14.48.175.193	0	0		0
□	somansa/ALL_IP	Networking / HTT...	○ Allow	http://clubmorning.co.kr/images_n...	2015-10-01 22:4...	72.207.168.192	14.48.175.193	0	0		0
□	somansa/ALL_IP	Networking / HTT...	○ Allow	http://clubmorning.co.kr/images_n...	2015-10-01 22:4...	72.207.168.192	14.48.175.193	0	0		0
□	somansa/ALL_IP	Networking / HTT...	○ Allow	http://clubmorning.co.kr/flash.js	2015-10-01 22:4...	72.207.168.192	14.48.175.193	0	0		0
□	somansa/ALL_IP	Networking / HTT...	○ Allow	http://clubmorning.co.kr/images_n...	2015-10-01 22:4...	72.207.168.192	14.48.175.193	0	0		0
□	somansa/ALL_IP	Networking / HTT...	○ Allow	http://clubmorning.co.kr/images_n...	2015-10-01 22:4...	72.207.168.192	14.48.175.193	0	0		0
□	somansa/ALL_IP	Networking / HTT...	○ Allow	http://clubmorning.co.kr/images_n...	2015-10-01 22:4...	72.207.168.192	14.48.175.193	0	0		0

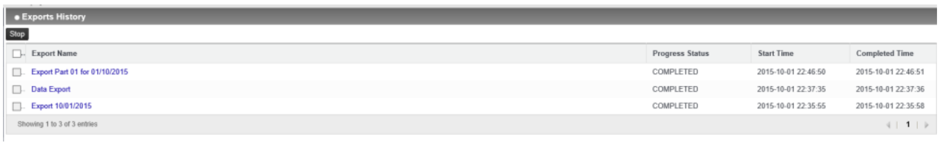
(FIGURE 4-8) INCIDENTS – NETWORK – NET APPS

4.3.3 Export

The details of specific and all logs can be exported and viewed by including or excluding the information of attached file and file analysis results. The items to export can be selected and selectable items include content, transmitted date, Net App, recipients, CC, user ID, user department, sender IP, recipient IP, Agent ID, size, actions, tag, personal information, and the number of attached files. The results of all exports are viewed under INCIDENTS – Network – Export History.

4.3.4 Export History

View the results of exports under INCIDENTS – Network – Net Apps



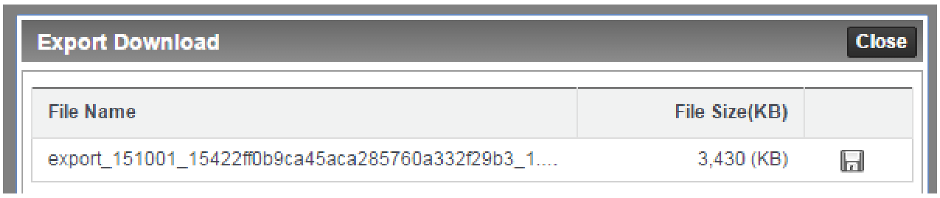
● Exports History

Stop

□ Export Name	Progress Status	Start Time	Completed Time
□ Export Part 01 for 01/10/2015	COMPLETED	2015-10-01 22:46:50	2015-10-01 22:46:51
□ Data Export	COMPLETED	2015-10-01 22:37:35	2015-10-01 22:37:36
□ Export 10/01/2015	COMPLETED	2015-10-01 22:35:55	2015-10-01 22:35:58

Showing 1 to 3 of 3 entries

(FIGURE 4-9) INCIDENTS – NETWORK – NET APPS – EXPORT HISTORY



Export Download

Close

File Name	File Size(KB)	
export_151001_15422ff0b9ca45aca285760a332f29b3_1....	3,430 (KB)	💾

(FIGURE 4-10) INCIDENTS – NETWORK – NET APPS – EXPORT HISTORY – DOWNLOAD

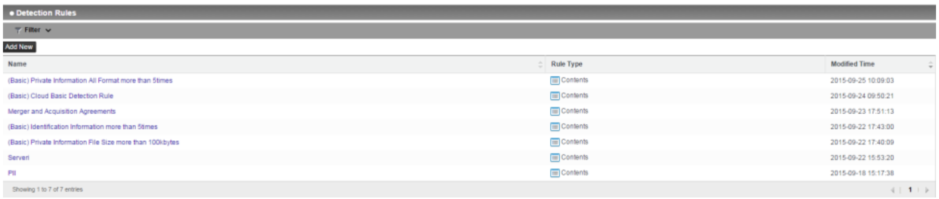
All details about the log saved as HTML file can be viewed after files are downloaded and decompressed.

4.4 Policies

4.4.1 Detect

4.4.1.1 Detection Rules

Detection Rules for specific conditions can be configured. Patterns of sensitive data and user-defined patterns and properties are selected for the conditions. The policy for each country can be easily set by using a pre-defined detection rule template and selecting Sensitive Data Protection, Regulatory Compliance, and Confidential Data Protection.

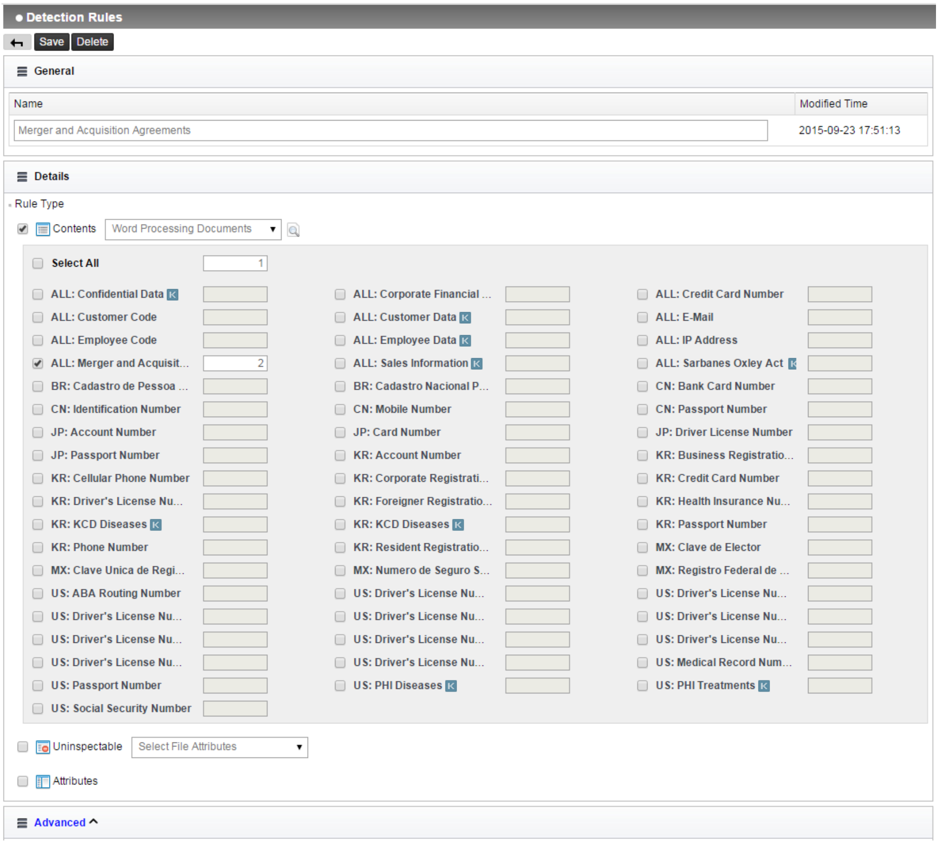


● Detection Rules

Name	Rule Type	Modified Time
(Basic) Private Information All Format more than 5times	Contents	2015-09-25 10:09:03
(Basic) Cloud Basic Detection Rule	Contents	2015-09-24 09:50:21
Merger and Acquisition Agreements	Contents	2015-09-23 17:51:13
(Basic) Identification Information more than 5times	Contents	2015-09-22 17:43:00
(Basic) Private Information File Size more than 100kbytes	Contents	2015-09-22 17:40:09
Serveri	Contents	2015-09-22 15:53:20
PII	Contents	2015-09-18 15:17:38

Showing 1 to 7 of 7 entries

(FIGURE 4-11) POLICIES – DETECT – DETECTION RULES



● Detection Rules

General

Name	Modified Time
Merger and Acquisition Agreements	2015-09-23 17:51:13

Details

Rule Type

☑ Contents: Word Processing Documents

□ Select All	1				
□ ALL: Confidential Data		□ ALL: Corporate Financial ...		□ ALL: Credit Card Number	
□ ALL: Customer Code		□ ALL: Customer Data		□ ALL: E-Mail	
□ ALL: Employee Code		□ ALL: Employee Data		□ ALL: IP Address	
☑ ALL: Merger and Acquisit...	2	□ ALL: Sales Information		□ ALL: Sarbanes Oxley Act	
□ BR: Cadastro de Pessoa ...		□ BR: Cadastro Nacional P...		□ CN: Bank Card Number	
□ CN: Identification Number		□ CN: Mobile Number		□ CN: Passport Number	
□ JP: Account Number		□ JP: Card Number		□ JP: Driver License Number	
□ JP: Passport Number		□ KR: Account Number		□ KR: Business Registratio...	
□ KR: Cellular Phone Number		□ KR: Corporate Registrati...		□ KR: Credit Card Number	
□ KR: Driver's License Nu...		□ KR: Foreigner Registratio...		□ KR: Health Insurance Nu...	
□ KR: KCD Diseases		□ KR: KCD Diseases		□ KR: Passport Number	
□ KR: Phone Number		□ KR: Resident Registratio...		□ MX: Clave de Elector	
□ MX: Clave Unica de Regi...		□ MX: Numero de Seguro S...		□ MX: Registro Federal de ...	
□ US: ABA Routing Number		□ US: Driver's License Nu...		□ US: Driver's License Nu...	
□ US: Driver's License Nu...		□ US: Driver's License Nu...		□ US: Driver's License Nu...	
□ US: Driver's License Nu...		□ US: Driver's License Nu...		□ US: Driver's License Nu...	
□ US: Driver's License Nu...		□ US: Driver's License Nu...		□ US: Medical Record Num...	
□ US: Passport Number		□ US: PHI Diseases		□ US: PHI Treatments	
□ US: Social Security Number					

□ Uninspectable: Select File Attributes

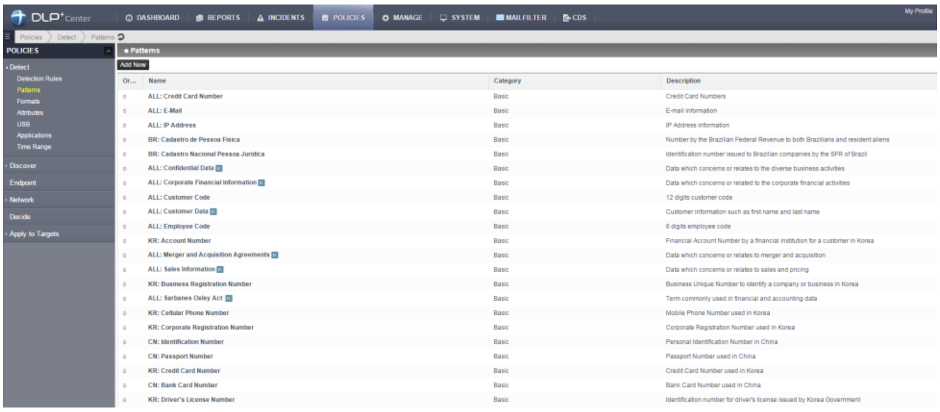
□ Attributes

Advanced

(FIGURE 4-12) POLICIES – DETECT – DETECTION RULES - DETAILS

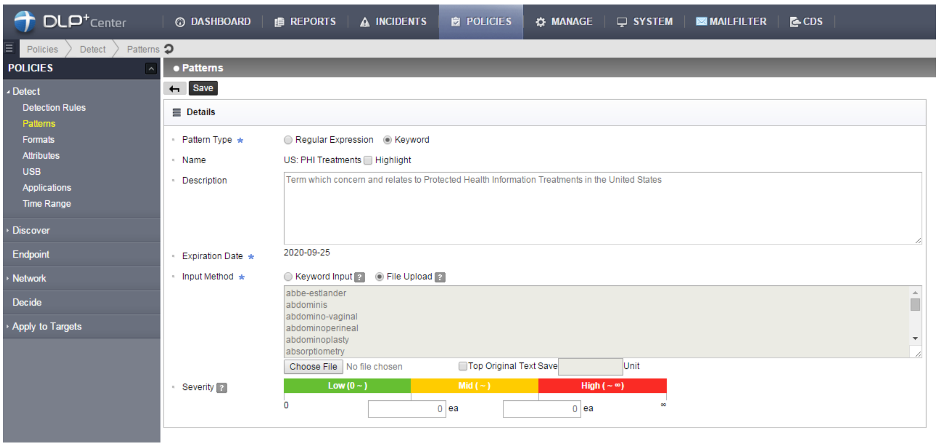
4.4.1.2 Pattern

In Pattern, basic patterns of confidential data provided by SOMANSA can be viewed. Provided patterns include social security number, driver's license number, credit card number, health insurance card number, passport number, account number, cell phone number, phone number, IP address, and E-mail address, and more. To detect a specific phrase or pattern, a user-defined pattern can be created. Basic patterns cannot be deleted, and expressions cannot be modified or deleted. Pattern is used when creating Detection Rule.



Or...	Name	Category	Description
	ALL: Credit Card Number	Basic	Credit Card Numbers
	ALL: E-Mail	Basic	E-mail information
	ALL: IP Address	Basic	IP Address information
	BR: Cadastro de Pessoa Fisica	Basic	Number by the Brazilian Federal Revenue to both Brazilians and resident aliens
	BR: Cadastro Nacional Pessoa Juridica	Basic	Identification number issued to Brazilian companies by the SFR of Brazil
	ALL: Confidential Data K	Basic	Data which concerns or relates to the diverse business activities
	ALL: Corporate Financial Information K	Basic	Data which concerns or related to the corporate financial activities
	ALL: Customer Code	Basic	12 digits customer code
	ALL: Customer Data K	Basic	Customer information such as first name and last name
	ALL: Employee Code	Basic	8 digits employee code
	KR: Account Number	Basic	Financial Account Number by a financial institution for a customer in Korea
	ALL: Merger and Acquisition Agreements K	Basic	Data which concerns or relates to merger and acquisition
	ALL: Sales Information K	Basic	Data which concerns or relates to sales and pricing
	KR: Business Registration Number	Basic	Business Unique Number to identify a company or business in Korea
	ALL: Sarbanes Oxley Act K	Basic	Term commonly used in financial and accounting data
	KR: Cellular Phone Number	Basic	Mobile Phone Number used in Korea
	KR: Corporate Registration Number	Basic	Corporate Registration Number used in Korea
	CN: Identification Number	Basic	Personal Identification Number in China
	CN: Passport Number	Basic	Passport Number used in China
	KR: Credit Card Number	Basic	Credit Card Number used in Korea
	CN: Bank Card Number	Basic	Bank Card Number used in China
	KR: Driver's License Number	Basic	Identification number for driver's license issued by Korea Government

(FIGURE 4-13) PATTERN LIST



Pattern Type ★ ○ Regular Expression ● Keyword

Name US: PHI Treatments □ Highlight

Description Term which concern and relates to Protected Health Information Treatments in the United States

Expiration Date ★ 2020-09-25

Input Method ★ ○ Keyword Input ? ● File Upload ?

abbe-estlander
abdominis
abdomino-vaginal
abdominoperineal
abdominoplasty
absorptiometry

Choose File No file chosen □ Top Original Text Save Unit

Severity ? Low (0 ~) Mid (~) High (~ ∞)

0 0 ea 0 ea ∞

(FIGURE 4-14) PATTERN DETAILS

☞ Policy Item Description

① Expiration Date: Sets an expiration date for the currently registered pattern.

② Expression: Sets a pattern to detect by using a general keyword or regular expression.

③ Severity: Sets a severity level when detecting a pattern.

☞ Effective Input Field Range

[TABLE 4-2] EFFECTIVE INPUT FIELD RANGE FOR PATTERN

Item	Effective Range	Character	Failure Message
Name	3~225	Numbers, uppercase/ lowercase letters, special characters	Pattern name must be at least 3 characters.
Description	1~225	Numbers, uppercase/ lowercase letters, special characters	-
Expression	1~200	Numbers, uppercase/ lowercase letters, special characters	A blank value cannot be registered in the expression.
Severity	0~999,999,999	Numbers	0 cannot be entered in Severity Settings.

4.4.1.3 File Format

Manages a format to use in file attributes

* However, unsupported formats cannot be detected, and logs cannot be stored.

[TABLE 4-3] DEFAULT INSPECTION FORMAT FILE

Order	File Type	Category	Format Name	Extension
1	Text	Basic Format	Copy of Printed Document	pvi
2			Microsoft Hypertext Archive	mht
3			Hypertext Markup Language	html;htm
4			Extensible Markup Language	xml
5			Rich Text Format	rtf
6			Comma-Separated Values	csv
7			Plain Text Format	txt
8	Word processor	Basic Format	iWork Pages	pages
9			Corel WordPerfect	wpd;wp;wp4;wp5;wp6;wp7
10			OpenOffice Writer	odt;sxw
11			Hancom HWP	hwp
12			HandySoft Arirang	hwd
13			Microsoft Word	doc;docx

14	Spreadsheet	Basic Format	iWork Numbers	numbers
15			OpenOffice Calc	ods;sxc
16			Microsoft Excel	xls;xlsx;xlsm
17	Presentation	Basic Format	Hancom Office Hanshow	show
18			iWork Keynote	key
19			OpenOffice Impression	odp;sxi
20			Microsoft PowerPoint	ppt;pptx;pps
21	E-mail	Basic Format	Microsoft Outlook Express	eml;mht
22			Microsoft Outlook	msg;oft
23	Database	Basic Format	Microsoft Access	mdb;accdb
24	Others	Basic Format	XML Paper Specification	xps
25			Microsoft Compiled HTML	chm
26			Adobe Portable Document Format	pdf

☞ Policy Item Description

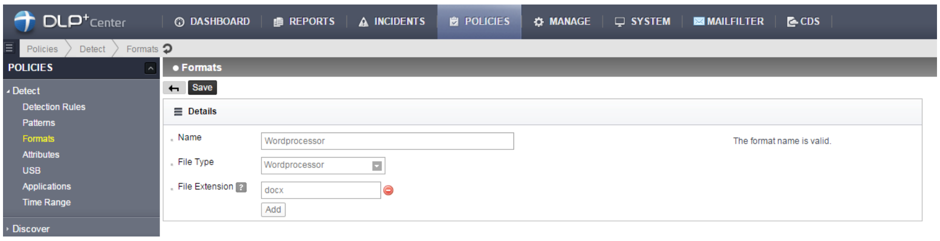
① File Type: Specified file types can be selected and entered when directly selecting 'Add'.

② File Extension: Extensions to detect can be entered. The extensions provided by default are listed in [Table 4-29].

☞ Effective Input Field Range

[TABLE 4-4] EFFECTIVE INPUT FIELD RANGE FOR FILE FORMAT

Item	Effective Range	Character	Failure Message
Format Name	1~225	Numbers, uppercase/ lowercase letters, special characters	Enter a format name.
Extension	1~20	Letters	An empty value cannot be registered for file type.



Name: Wordprocessor — The format name is valid.

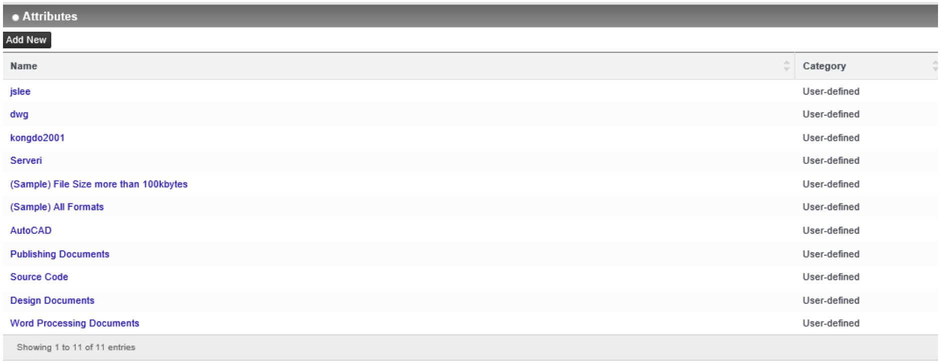
File Type: Wordprocessor

File Extension: docx

(FIGURE 4-15) FILE FORMAT DETAILS

4.4.1.4 Attributes

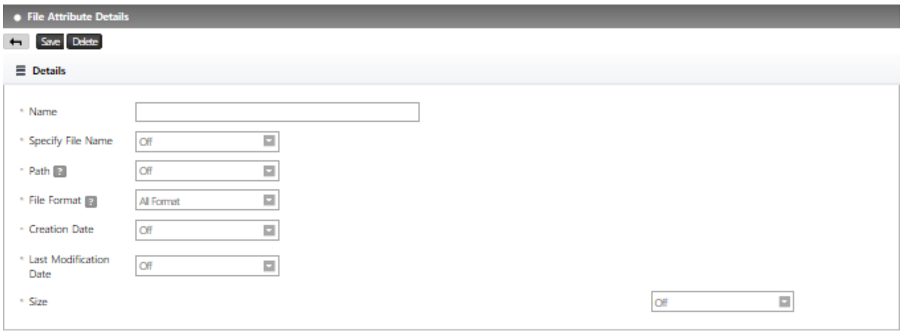
In Attributes, a condition value of a file attribute to be inspected can be specified. Inspection can be carried out according to file name, path, type, date created and size. To create a policy, one or more conditions must be selected. Each setting satisfies the AND condition, and a file is detected according to the settings for each item. A generated file attribute is used when creating Detection Rule.



Name	Category
jslee	User-defined
dwg	User-defined
kongdo2001	User-defined
Serveri	User-defined
(Sample) File Size more than 100kbytes	User-defined
(Sample) All Formats	User-defined
AutoCAD	User-defined
Publishing Documents	User-defined
Source Code	User-defined
Design Documents	User-defined
Word Processing Documents	User-defined

Showing 1 to 11 of 11 entries

(FIGURE 4-16) ATTRIBUTES LIST



Name:

Specify File Name: Off

Path: Off

File Format: All Format

Creation Date: Off

Last Modification Date: Off

Size: Off

(FIGURE 4-17) FILE ATTRIBUTE DETAILS

☞ Policy Item Description

① File Name: When selected, the file name field is activated, and Included Target and Excluded Target can be selected. A file name to detect (exclude) can be entered. A file name must be entered with its extension.

② Path: When selected, the path name field is activated, and Included Target and Excluded Target can be selected. A path to detect (exclude) can be entered.

③ File Format: All Formats or Specify Directly can be selected. When Specify Directly is selected, the desired format among formats described in [Table 4-21] can be selected.

④ File Created Date: When selected, the date field is activated, and date created to detect can be selected.

⑤ File Modified Date: When selected, the date field is activated, and date modified to detect can be selected.

⑥ File Size: When selected, the size field is activated, and file size to detect can be entered. Size is divided into a range and minimum for selection.

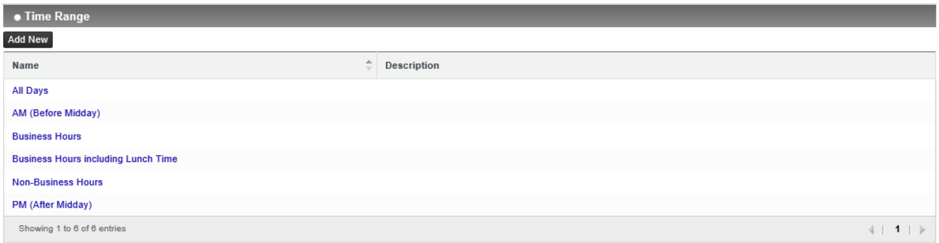
☞ Effective Input Field Range

[TABLE 4-5] EFFECTIVE INPUT FIELD RANGE FOR FILE ATTRIBUTES

Item	Effective Range	Character	Failure Message
Name	3~225	Numbers, uppercase/ lowercase letters, special characters	Name should have at least 3 characters.

4.4.1.5 Time Range

Time Range can be added, modified, deleted and is used to create the Network Policy.



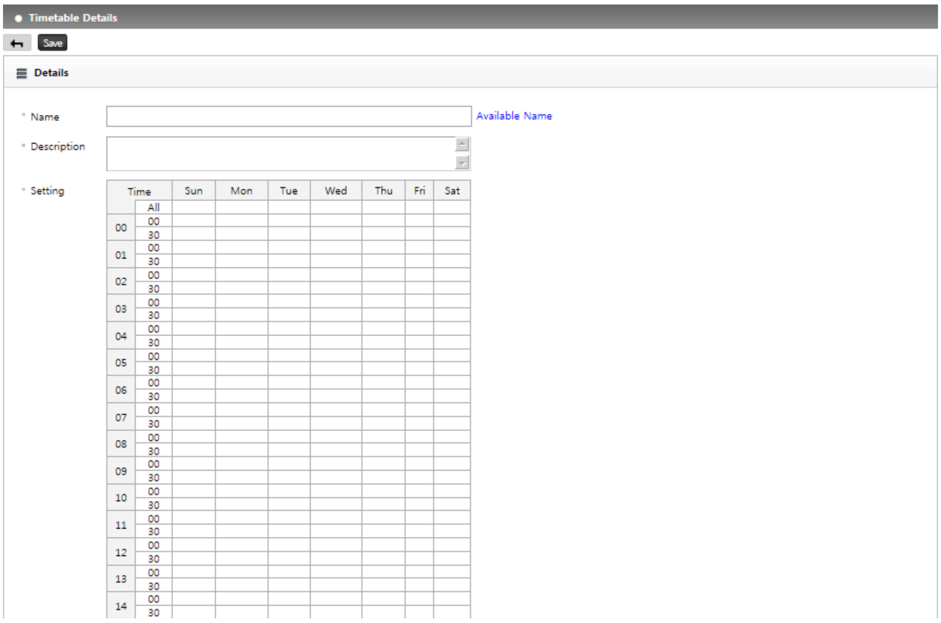
● Time Range

Add New

Name	Description
All Days	
AM (Before Midday)	
Business Hours	
Business Hours including Lunch Time	
Non-Business Hours	
PM (After Midday)	

Showing 1 to 6 of 6 entries

(FIGURE 4-18) TIME RANGE LIST



● Timetable Details

Save

Details

* Name

Available Name

* Description

* Setting

Time		Sun	Mon	Tue	Wed	Thu	Fri	Sat
	All							
00	00							
	30							
01	00							
	30							
02	00							
	30							
03	00							
	30							
04	00							
	30							
05	00							
	30							
06	00							
	30							
07	00							
	30							
08	00							
	30							
09	00							
	30							
10	00							
	30							
11	00							
	30							
12	00							
	30							
13	00							
	30							
14	00							
	30							

(FIGURE 4-19) ADDING TIME RANGE SETTINGS SCREEN

☞ Policy Item Description

① Time Range Name: Time range name to add can be specified.

② Description: A description for time range can be entered.

③ Time Range Settings: Time range can be set by dragging and dropping. It can be set in 30-minute units. To select all days (vertical) or all days in a specified time range (horizontal), select the front row or column.

4.4.2 Network

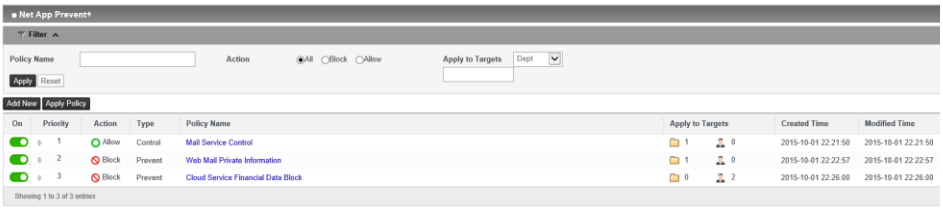
Network can be set to Allow and Block by settings. Net App Prevent policy is categorized into a part to control the access to Net Apps and a part to prevent attached files. Data Tagging policy is only available to control and the tag to logs is added. Net Apps which are applicable to each policy are as below.

Category	Protocol	Policy (Applicable)
Email	SMTP, POP3, IMAP	Control, Prevent, Tagging
Web Mail	AOL, Chollian, Daum Hanmail, Gmail, iCloud Mail, Korea.com, Korea.kr, Nate, Naver, Outlook Live, QQ Mail, Yahoo	Control, Prevent, Tagging
Instant Messaging	AOL Instant Messenger, Facebook Messenger, Google Talk, Misslee, NateOn, Yahoo Voice	Control, Prevent, Tagging
Remote Access	Dacom_Neturo, MS Remote Desktop, PCAnywhere, Radmin, TeamViewer, VNC	Control
	Telnet	Control, Prevent, Tagging
Networking	POST, Response	Control, Prevent, Tagging
Social Networking Service	Cyworld, Daum Blog, Daum Café, Egloos, Facebook, Instagram, Myspace, Naver Blog, Naver Café, Salesforce, Tumblr	Control, Prevent, Tagging
File Storage and Sharing	2nDrive, Amazon Cloud, Box, Dropbox, Evernote, FTP, Google Drive, iCloud, LG U+ Box, LG U+ Webhard, Naver Ndrive, OneDrive, SharePoint, SMB, SugarSync, T Cloud, Tencent	Control, Prevent, Tagging

	Cloud, U Cloud	
Personal File Sharing	ToToDisk,	Control ,Prevent, Tagging
	Clubbox, eDonkey, Fileguri, GNUtella	Control
Anonymizer	SOCKS	Control

4.4.2.1 Net App Prevent+

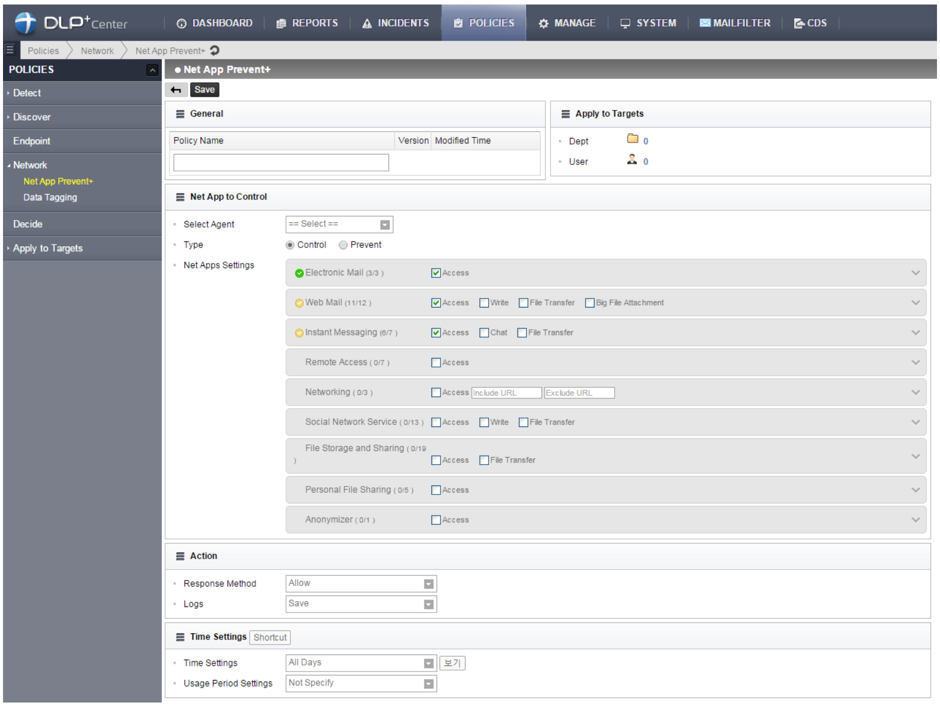
A policy that is used when allowing or blocking specific Network Applications. The supported types of Net Apps are email, web mail, instant messaging, remote access, networking, social networking service, file storage and sharing, personal file sharing and anonymizer (alternate routing). Each Net Apps is controlled by selecting the access, writing, file share function. Also, access time span and period can be set as well.



On	Priority	Action	Type	Policy Name	Apply to Targets		Created Time	Modified Time
●	1	Allow	Control	Mail Service Control	1	0	2015-10-01 22:21:50	2015-10-01 22:21:50
●	2	Block	Prevent	Web Mail Private Information	1	0	2015-10-01 22:22:57	2015-10-01 22:22:57
●	3	Block	Prevent	Cloud Service Financial Data Block	0	2	2015-10-01 22:26:00	2015-10-01 22:26:00

Showing 1 to 3 of 3 entries

(FIGURE 4-20) NET APP PREVENT+ POLICY



● Net App Prevent+

General

Policy Name	Version	Modified Time

Apply to Targets

- Dept 0
- User 0

Net App to Control

- Select Agent: == Select ==
- Type: ● Control ○ Prevent
- Net Apps Settings:
  - Electronic Mail (3/3) ☑ Access
  - Web Mail (11/12) ☑ Access □ Write □ File Transfer □ Big File Attachment
  - Instant Messaging (6/7) ☑ 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 □ File Transfer
  - Personal File Sharing (0/5) □ Access
  - Anonymizer (0/1) □ Access

Action

- Response Method: Allow
- Logs: Save

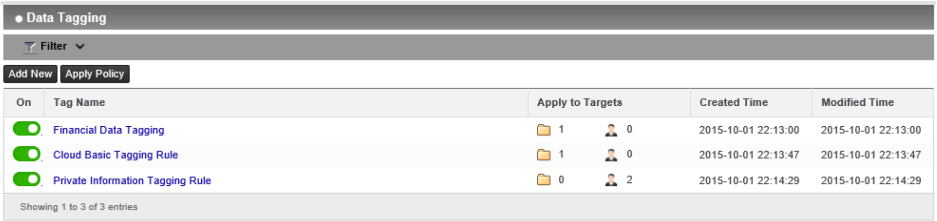
Time Settings Shortcut

- Time Settings: All Days 보기
- Usage Period Settings: Not Specify

(FIGURE 4-21) NET APP PREVENT+ POLICY DETAILS

4.4.2.2 Data Tagging

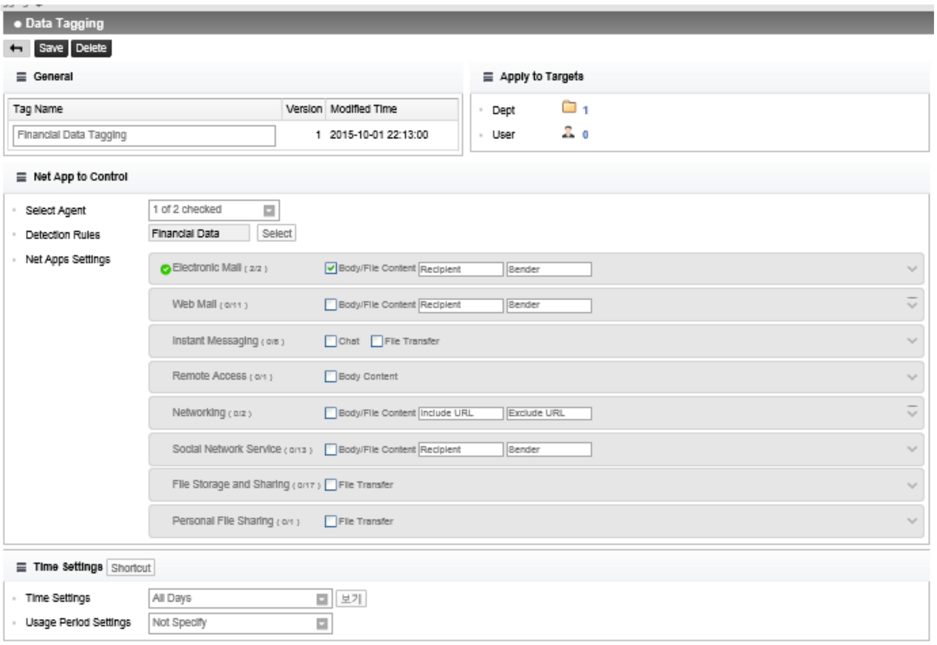
Sets a Tagging on specific Net Apps. Logs satisfying the conditions will have tag marks on their title. Supported types of Net Apps are email, web mail, instant messaging, remote access, generic networking, social network service, file storage and sharing, personal file sharing and alternate routing. Each type are controlled by selecting the access, writing, file share function. Also, access time span and period are can be set as well.



On	Tag Name	Apply to Targets		Created Time	Modified Time
●	Financial Data Tagging	1	0	2015-10-01 22:13:00	2015-10-01 22:13:00
●	Cloud Basic Tagging Rule	1	0	2015-10-01 22:13:47	2015-10-01 22:13:47
●	Private Information Tagging Rule	0	2	2015-10-01 22:14:29	2015-10-01 22:14:29

Showing 1 to 3 of 3 entries

(FIGURE 4-22) DATA TAGGING



Data Tagging

General

Tag Name	Version	Modified Time
Financial Data Tagging	1	2015-10-01 22:13:00

Apply to Targets

Dept	1
User	0

Net App to Control

- Select Agent: 1 of 2 checked
- Detection Rules: Financial Data [Select]
- Net Apps Settings:

Electronic Mail (2/2)	☑ Body/File Content	Recipient	Sender
Web Mail (0/11)	□ Body/File Content	Recipient	Sender
Instant Messaging (0/8)	□ Chat	□ File Transfer	
Remote Access (0/1)	□ Body Content		
Networking (0/2)	□ Body/File Content	Include URL	Exclude URL
Social Network Service (0/13)	□ Body/File Content	Recipient	Sender
File Storage and Sharing (0/17)	□ File Transfer		
Personal File Sharing (0/1)	□ File Transfer		

Time Settings [Shortcut]

- Time Settings: All Days [보기]
- Usage Period Settings: Not Specify

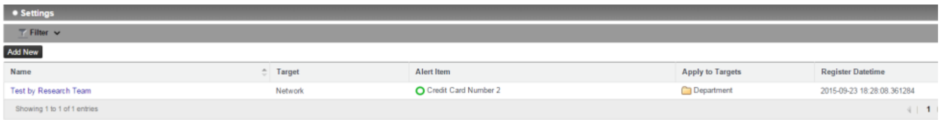
(FIGURE 4-23) DATA TAGGING DETAILS

4.5 Manage

4.5.1 Alerts/Notifications

4.5.1.1 Reports

Statistics of Network can be sent to the E-mail registered in user information. Reports (for specific user/groups or periods) on Top Users, Top Depts, Trends, Top Categories, and Top Patterns are provided.

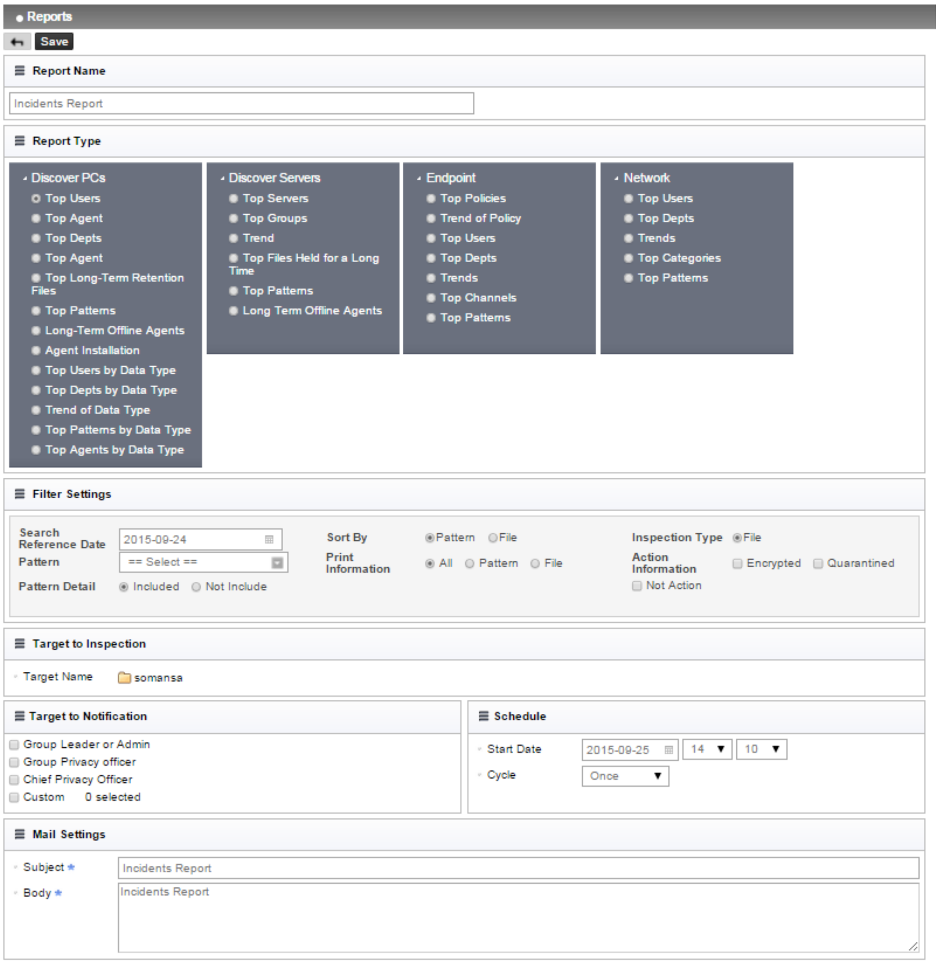


Settings

Name	Target	Alert Item	Apply to Targets	Register Datetime
Test by Research Team	Network	Credit Card Number 2	Department	2015-09-23 18:28:08.361284

Showing 1 to 1 of 1 entries

(FIGURE 4-24) ALERT/NOTIFICATIONS - REPORTS



Report Name: Incidents Report

Filter Settings

Search Reference Date: 2015-09-24
Pattern: == Select ==
Pattern Detail: ● Included ○ Not Include
Sort By: ● Pattern ○ File
Print Information: ● All ○ Pattern ○ File
Inspection Type: ● File
Action Information: □ Encrypted □ Quarantined □ Not Action

Target to Inspection

Target Name: somansa

Target to Notification

□ Group Leader or Admin
□ Group Privacy officer
□ Chief Privacy Officer
□ Custom 0 selected

Schedule

Start Date: 2015-09-25 14 ▼ 10 ▼
Cycle: Once ▼

Mail Settings

Subject *: Incidents Report
Body *: Incidents Report

(FIGURE 4-25) ALERT/NOTIFICATIONS – REPORTS DETAILS

☞ Report Notification Details

① Report Type: One of the reports details of Top Users, Top Depts, Trends, Top Categories and Top Patterns can be selected.

② Filter Settings: Recent Inspection Date, Ranking Criteria and Pattern can be selected and a filter can be applied.

③ Inspection Summary Target: A department or a user can be selected for Inspection Summary Target.

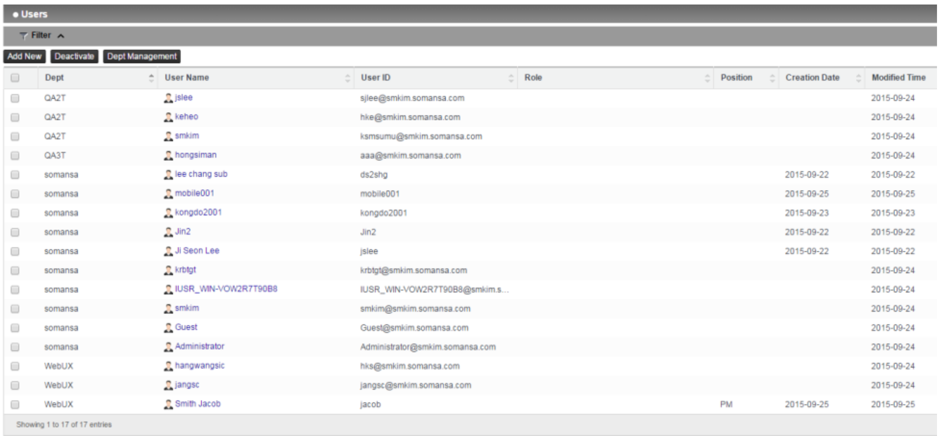
④ Notification Target: Recipients for the notification can be selected.

⑤ Schedule: Notification cycle can be set once, daily, weekly or monthly.

⑥ Mail Settings: Mail subject and body can be entered.

4.5.2 Users

A user can be added, modified and deleted.



● Users

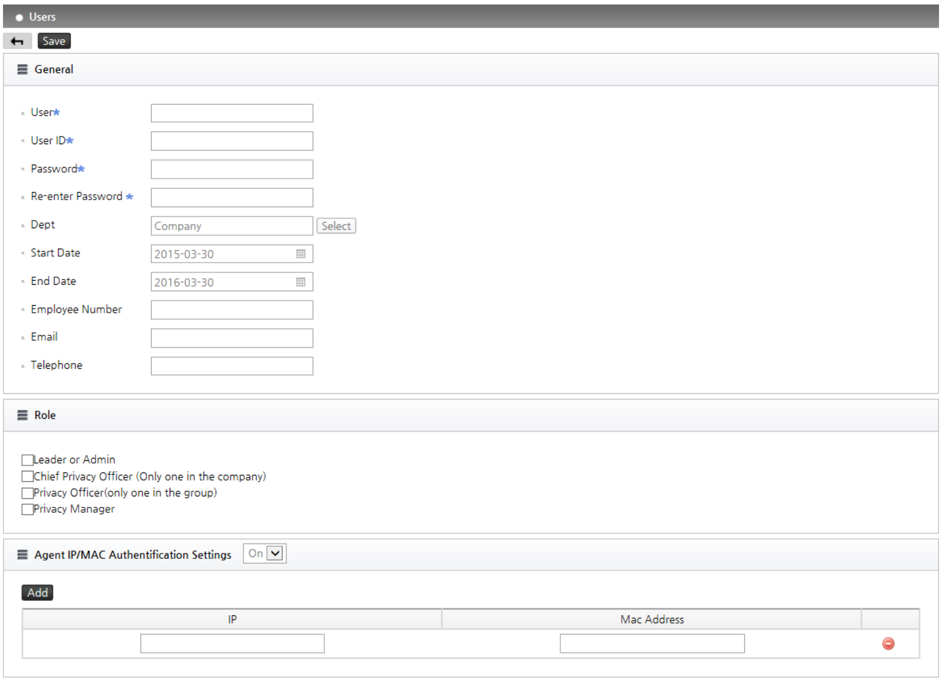
□	Dept	User Name	User ID	Role	Position	Creation Date	Modified Time
□	QA2T	jslee	sjlee@smkim.somansa.com				2015-09-24
□	QA2T	keheo	hke@smkim.somansa.com				2015-09-24
□	QA2T	smkim	ksmsumu@smkim.somansa.com				2015-09-24
□	QA3T	hongsiman	aaa@smkim.somansa.com				2015-09-24
□	somansa	lee chang sub	ds2shg			2015-09-22	2015-09-22
□	somansa	mobile001	mobile001			2015-09-25	2015-09-25
□	somansa	kongdo2001	kongdo2001			2015-09-23	2015-09-23
□	somansa	Jin2	Jin2			2015-09-22	2015-09-22
□	somansa	Ji Seon Lee	jslee			2015-09-22	2015-09-22
□	somansa	krbtgt	krbtgt@smkim.somansa.com				2015-09-24
□	somansa	IUSR_WIN-VOW2R7T90B8	IUSR_WIN-VOW2R7T90B8@smkim.s...				2015-09-24
□	somansa	smkim	smkim@smkim.somansa.com				2015-09-24
□	somansa	Guest	Guest@smkim.somansa.com				2015-09-24
□	somansa	Administrator	Administrator@smkim.somansa.com				2015-09-24
□	WebUX	hangwangsic	hks@smkim.somansa.com				2015-09-24
□	WebUX	jangsc	jangsc@smkim.somansa.com				2015-09-24
□	WebUX	Smith Jacob	jacob		PM	2015-09-25	2015-09-25

Showing 1 to 17 of 17 entries

(FIGURE 4-26) USER ACCOUNT MANAGEMENT

- User Management

User Management shows the user information that is registered to HR Information. For user information, functions including adding, deleting a user, and changing a password are provided and the detail user information such as user name, ID, status, department, account start/expiration date, IP information, employee number, email, phone, etc can be specified.



General

User*	
User ID*	
Password*	
Re-enter Password *	
Dept	Company Select
Start Date	2015-03-30
End Date	2016-03-30
Employee Number	
Email	
Telephone	

Role

□Leader or Admin
□Chief Privacy Officer (Only one in the company)
□Privacy Officer(only one in the group)
□Privacy Manager

Agent IP/MAC Authentification Settings On

IP	Mac Address	

(FIGURE 4-27) USER MANAGEMENT DETAILS

☞ Descriptions

① User Name: User name to be registered can be entered.

② User ID: User ID to be registered can be entered. ID must be unique.

③ Password: Password can be entered/modified.

④ Dept: Department registered in "MANAGER > Users > Dept Management" can be selected, and a user is registered to the selected department.

⑤ Start Date: An available start date of the account to register can be entered.

⑥ End Date: An available end date of the account to register can be entered.

⑦ Employee number of the account user to register can be entered.

⑧ Email: Email of the account user to register can be entered.

⑨ Telephone: Phone number of the account user to register can be entered.

☞ Effective Input Field Range

[TABLE 4-6] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING USERS

Items	Effective Range	Character	Failure Message
User Name	1~225	Numbers, Uppercase/ Lowercase Letters, Special Characters	Enter the user name.
User ID	4~20	Numbers, Uppercase/ Lowercase Letters, Special Characters	Enter the user ID.
Password	9~35	Numbers, Uppercase/ Lowercase Letters, Special Characters	Enter the password.
Confirm Password	9~35	Numbers, Uppercase/ Lowercase Letters, Special Characters	Confirm the password.
Employee Number	1~20	Numbers, Uppercase/ Lowercase Letters, Special Characters	-
Email	1~50	Numbers, Uppercase/ Lowercase Letters, Special Characters	-
Phone Number	1~15	Numbers	-

Recommendation

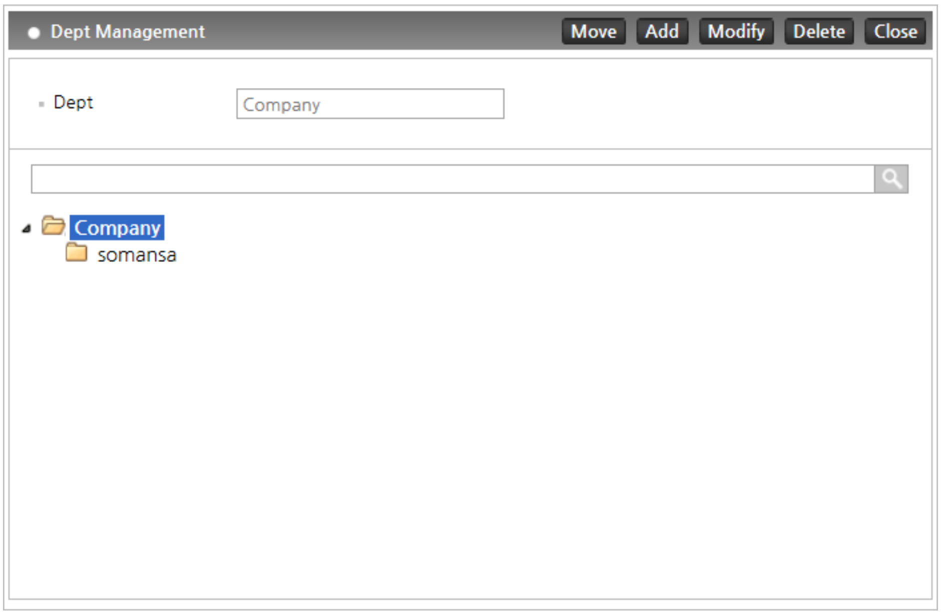
✓ Password should have at least 9 characters and include English letters, numbers and special characters.

- User Deactivation

Users can be activated or deactivated. Deactivated user accounts are not available for use.

- Dept Management

Dept Management shows departments registered in HR Information. For HR Information, functions to add, delete and move department are provided.



Dept: Company

(FIGURE 4-28) DEPT MANAGEMENT

☞Effective Input Fields Range

[TABLE 4-7] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING DEPT

Items	Effective Range	Character	Failure Message
Dept	1~100	Numbers, Uppercase/ Lowercase Letters, Special Characters	Enter the department name.
Find	1~100	Numbers, Uppercase/ Lowercase Letters, Special Characters	-

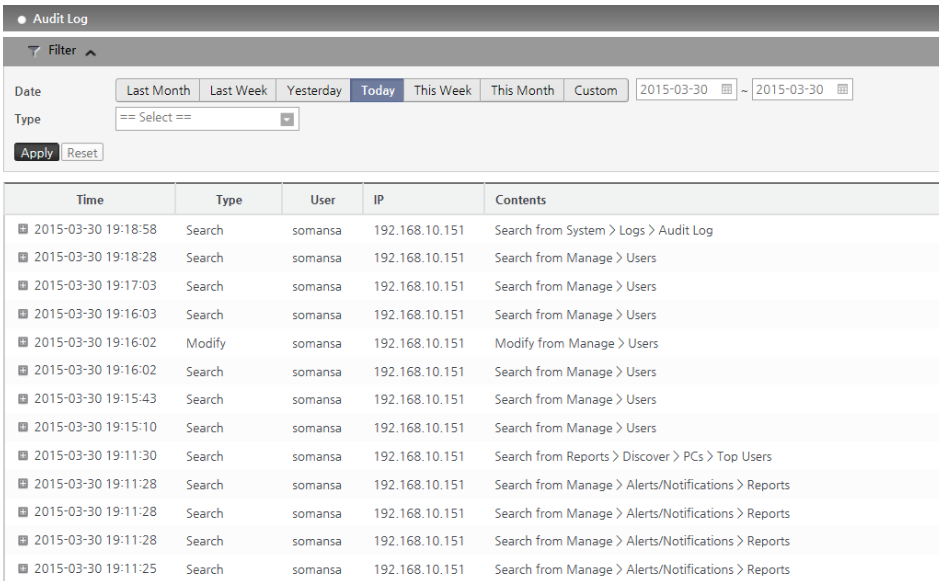
4.6 SYSTEM

4.6.1 Logs

- Audit Logs

For all activities of the admin, Information Management Logs, Information Trace Logs, Policy

Management Logs and Account Management Logs can be viewed. An Audit Trail is provided through the log.



● Audit Log

Filter

Date: Last Month | Last Week | Yesterday | Today | This Week | This Month | Custom | 2015-03-30 ~ 2015-03-30

Type: == Select ==

Apply Reset

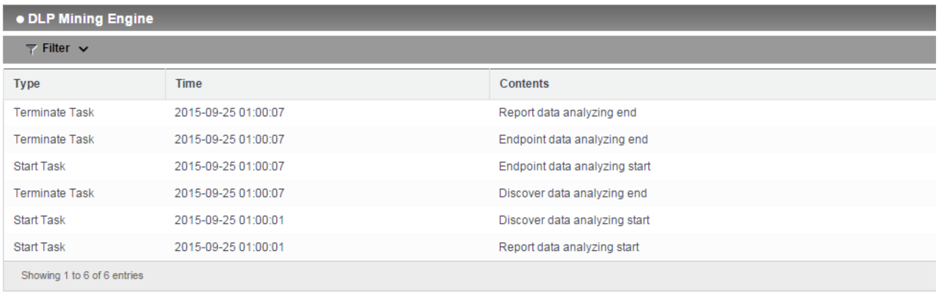
Time	Type	User	IP	Contents
2015-03-30 19:18:58	Search	somansa	192.168.10.151	Search from System > Logs > Audit Log
2015-03-30 19:18:28	Search	somansa	192.168.10.151	Search from Manage > Users
2015-03-30 19:17:03	Search	somansa	192.168.10.151	Search from Manage > Users
2015-03-30 19:16:03	Search	somansa	192.168.10.151	Search from Manage > Users
2015-03-30 19:16:02	Modify	somansa	192.168.10.151	Modify from Manage > Users
2015-03-30 19:16:02	Search	somansa	192.168.10.151	Search from Manage > Users
2015-03-30 19:15:43	Search	somansa	192.168.10.151	Search from Manage > Users
2015-03-30 19:15:10	Search	somansa	192.168.10.151	Search from Manage > Users
2015-03-30 19:11:30	Search	somansa	192.168.10.151	Search from Reports > Discover > PCs > Top Users
2015-03-30 19:11:28	Search	somansa	192.168.10.151	Search from Manage > Alerts/Notifications > Reports
2015-03-30 19:11:28	Search	somansa	192.168.10.151	Search from Manage > Alerts/Notifications > Reports
2015-03-30 19:11:28	Search	somansa	192.168.10.151	Search from Manage > Alerts/Notifications > Reports
2015-03-30 19:11:25	Search	somansa	192.168.10.151	Search from Manage > Alerts/Notifications > Reports

(FIGURE 4-29) AUDIT LOGS

4.6.1.1 System Logs

- DLP+ Mining Engine

Runs Mining Engine to collect Network audit logs as information used on DLP+ Center at a scheduled time.



● DLP Mining Engine

Filter

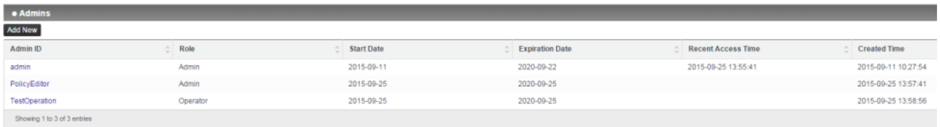
Type	Time	Contents
Terminate Task	2015-09-25 01:00:07	Report data analyzing end
Terminate Task	2015-09-25 01:00:07	Endpoint data analyzing end
Start Task	2015-09-25 01:00:07	Endpoint data analyzing start
Terminate Task	2015-09-25 01:00:07	Discover data analyzing end
Start Task	2015-09-25 01:00:01	Discover data analyzing start
Start Task	2015-09-25 01:00:01	Report data analyzing start

Showing 1 to 6 of 6 entries

(FIGURE 4-30) DLP+ MINING ENGINE LOGS

4.6.2 Admins

Admin accounts have rights to operate and manage the DLP+ Center. An admin account is created by the operating system admin when installing the product package. In addition, an admin can create and delete an Operator or Viewer Account according to the access department and view permissions. However, an admin account created during package installation cannot be deleted.



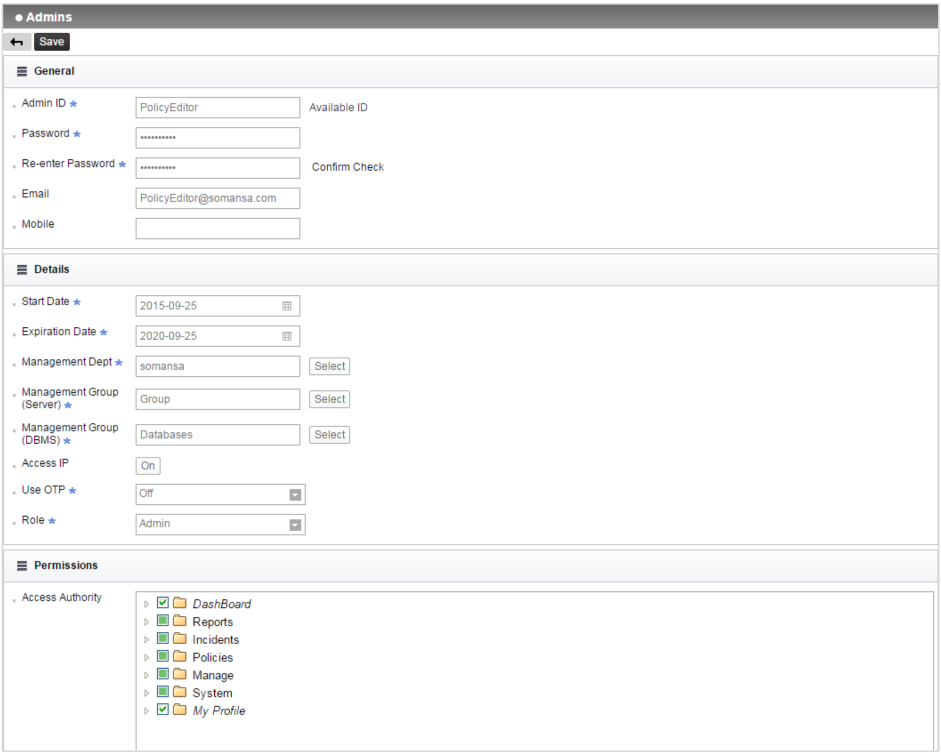
Admin ID	Role	Start Date	Expiration Date	Recent Access Time	Created Time
admin	Admin	2015-09-11	2020-09-22	2015-09-25 13:55:41	2015-09-11 10:27:54
PolicyEditor	Admin	2015-09-25	2020-09-25		2015-09-25 13:57:41
TestOperation	Operator	2015-09-25	2020-09-25		2015-09-25 13:58:56

Showing 1 to 3 of 3 entries

(FIGURE 4-31) ADMINS MANAGEMENT

[TABLE 4-8] INTEGRATED ACCOUNT RIGHTS

Accounts	Rights	Number of Accounts
Admin	All rights, Operator and viewer account management	1
Operator	Authorized access menu and log view in a department	1
View	Limited access menu and log view in a department	5



● Admins

Save

General

Admin ID *	PolicyEditor	Available ID
Password *	••••••••••	
Re-enter Password *	••••••••••	Confirm Check
Email	PolicyEditor@somansa.com	
Mobile		

Details

Start Date *	2015-09-25	
Expiration Date *	2020-09-25	
Management Dept *	somansa	Select
Management Group (Server) *	Group	Select
Management Group (DBMS) *	Databases	Select
Access IP	On	
Use OTP *	Off	
Role *	Admin	

Permissions

Access Authority

- ☑ *DashBoard*
- ▣ Reports
- ▣ Incidents
- ▣ Policies
- ▣ Manage
- ▣ System
- ☑ *My Profile*

(FIGURE 4-32) ADMINS MANAGEMENT DETAILS

☞Effective Input Field Range

[Table 4-9] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING ADMIN

Items	Effective Range	Character	Failure Message
Admin ID	5~20	Letters	An admin ID should have at least 5 characters.
Password	9~35	Numbers, Uppercase/ Lowercase Letters, Special Characters	Enter the password.
Confirm Password	9~35	Numbers, Uppercase/ Lowercase Letters, Special Characters	Confirm the password.
Email	1~200	Numbers, Uppercase/ Lowercase Letters, Special Characters	-

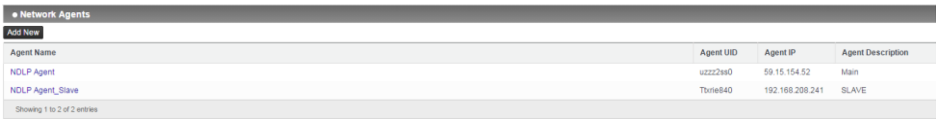
Recommendation

✓ Password must be at least 9 characters and include English letters, numbers and special characters.

4.6.3 Settings

4.6.3.1 Network Agents

Network Agents can be added, modified, deleted.

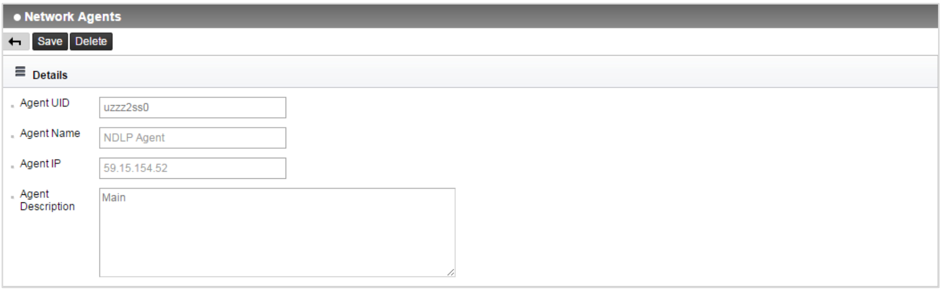


● Network Agents

Agent Name	Agent UID	Agent IP	Agent Description
NDLP Agent	uzzz2ss0	59.15.154.52	Main
NDLP Agent_Slave	Tbrie840	192.168.208.241	SLAVE

Showing 1 to 2 of 2 entries

(FIGURE 4-33) NETWORK AGENTS



● Network Agents

Agent UID: uzzz2ss0

Agent Name: NDLP Agent

Agent IP: 59.15.154.52

Agent Description: Main

(FIGURE 4-34) NETWORK AGENTS DETAILS

☞ Descriptions

① Agent UID : UID of the Agent can be entered.

② Agent Name : Name of the Agent can be specified.

③ Agent IP : IP address of the Agent can be entered.

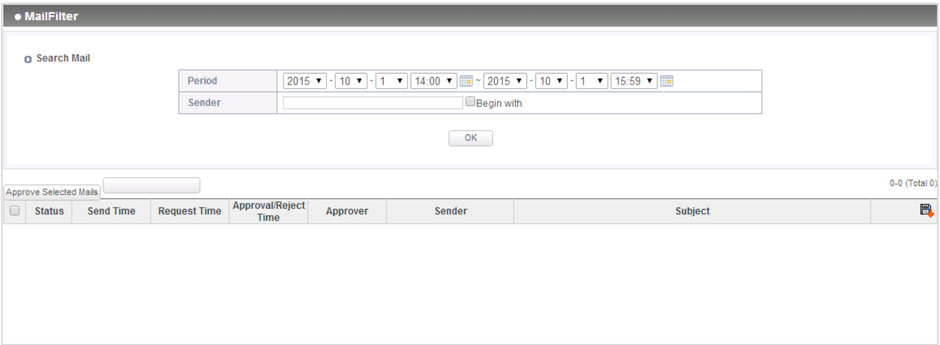
④ Agent Description: Description of the Agent can be added.

4.7 Mail-Filter

Mail-Filter is a specific module installed into Mail-i to manage all emails retaining the sensitive data. All outgoing emails can be sent by the decide process and pre-defined policy.

4.7.1 Mail List

The progress of all emails can be viewed. The status of email is categorized into Waiting, Rejected, Approved and Transmitted. Administrator can check the status by using the filters such as the email address and specified period. Administrator can also approve, block and delete emails by selecting the target email from the list.



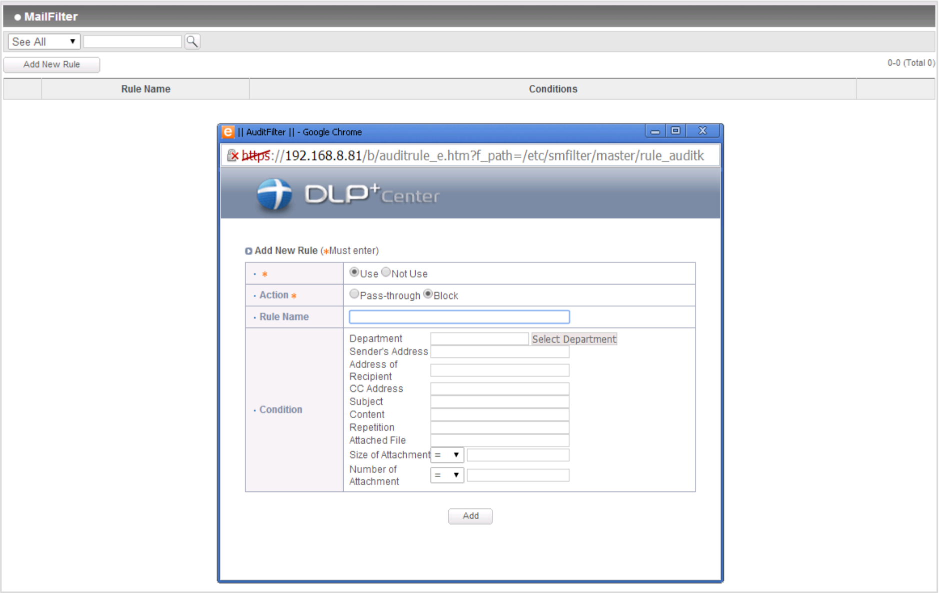
Period	2015 ▾ - 10 ▾ - 1 ▾ 14:00 ▾ ~ 2015 ▾ - 10 ▾ - 1 ▾ 15:59 ▾
Sender	□Begin with

□	Status	Send Time	Request Time	Approval/Reject Time	Approver	Sender	Subject	

(FIGURE 4-35) MAIL LIST

4.7.2 Decide Policy

Administrator can enforce policies to block outgoing email messages that violate predefined Email Security policies. Detail information on the users that attempted to send violated email messages externally such as time, user account, department and the message contents are retained and can be used for legal evidence for further investigation purposes.



● MailFilter

See All ▾ 🔍

Add New Rule — 0-0 (Total 0)

Rule Name	Conditions

|| AuditFilter || - Google Chrome

~~https~~://192.168.8.81/b/auditrule_e.htm?f_path=/etc/smfilter/master/rule_auditk

DLP⁺Center

Add New Rule (*Must enter)

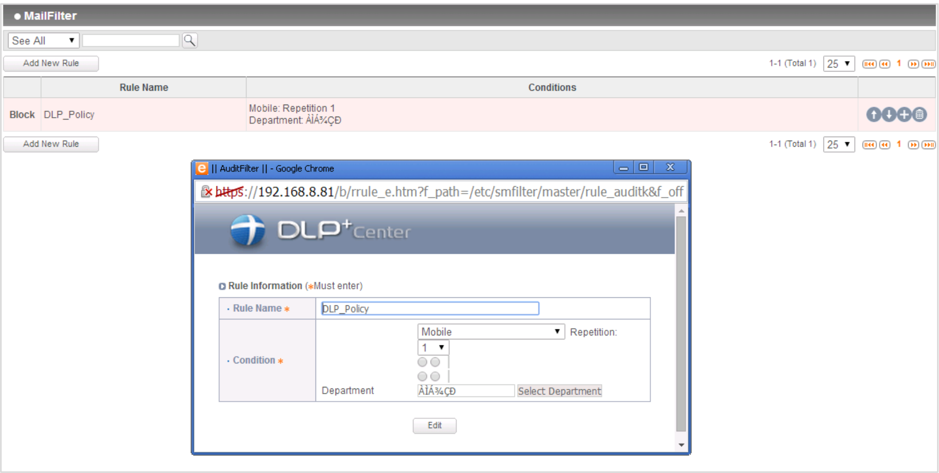
· *	● Use ○ Not Use
· Action *	○ Pass-through ● Block
· Rule Name	
· Condition	Department [Select Department] Sender's Address Address of Recipient CC Address Subject Content Repetition Attached File Size of Attachment = ▾ Number of Attachment = ▾

Add

(FIGURE 4-36) POLICY SETTINGS

4.7.3 Specify Block Policy

Apply a block policy by specifying the number of repetitions.



● MailFilter

See All ▾ 🔍

Add New Rule — 1-1 (Total 1) 25 ▾ 1

	Rule Name	Conditions
Block	DLP_Policy	Mobile: Repetition 1 Department: ÀÎÀ¾ÇÐ

Add New Rule — 1-1 (Total 1) 25 ▾ 1

|| AuditFilter || - Google Chrome

~~https~~://192.168.8.81/b/rrule_e.htm?f_path=/etc/smfilter/master/rule_auditk&f_off

DLP⁺Center

Rule Information (*Must enter)

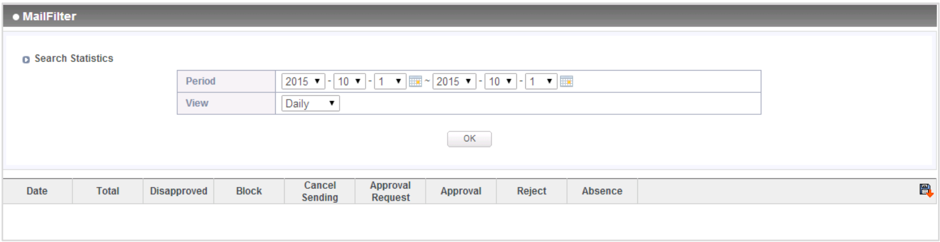
· Rule Name *	DLP_Policy
· Condition *	Mobile ▾ Repetition: 1 ▾ ○ ○ ○ ○ Department ÀÎÀ¾ÇÐ [Select Department]

Edit

(FIGURE 4-37) SPECIFY BLOCK POLICY

4.7.4 Statistics

All email messages violated the rules by dates or periods can be viewed. From the list of search results, the detail information based on the status of email such as Requested, Approved and Rejected according to the specified search period and date are provided.



Period: 2015 - 10 - 1 ~ 2015 - 10 - 1

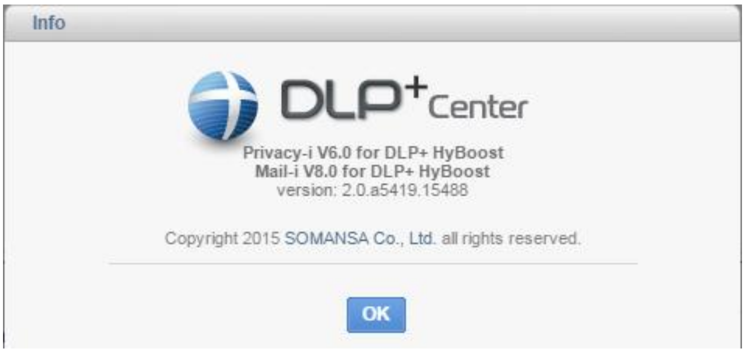
View: Daily

Date	Total	Disapproved	Block	Cancel Sending	Approval Request	Approval	Reject	Absence

(FIGURE 4-38) STATISTICS

4.8 Checking the Version of DLP+ Center

This screen shows the version of the DLP+ Center. Click the ⓘ button at the top right to check the version.



Privacy-i V6.0 for DLP+ HyBoost
Mail-i V8.0 for DLP+ HyBoost
version: 2.0.a5419.15488

Copyright 2015 SOMANSA Co., Ltd. all rights reserved.

(FIGURE 4-39) CHECK DLP+ CENTER VERSION

5. Appendix

5.1 T-Proxy

5.1.1 What is T-Proxy?

T-Proxy is a transparent proxy that disallows both the user and server to be aware of the existence of the proxy, which differentiates itself from generic proxy.

T-Proxy intercepts packets from a user and establishes a connection to the server, as if it is the user. The server also cannot be aware of the existence of the proxy, since it also understands it as a user, not a proxy.

5.1.2 Why is T-Proxy needed?

In case of SSL, communication is secured based on certificates, so it is impossible to decipher the packets intercepted in the middle of the communication. However, when a T-Proxy is used, the packets can be decrypted since it has the certificate they are encrypted upon. So the messages of the encrypted protocols that have been blocked, can be decrypted and logged if T-Proxy is used.

5.2 Net Apps Test Scenario

5.2.1 Office 365 Onedrive

- Setting a Block Policy

(1) Click [POLICIES] on DLP+Center.
(2) Click Network-Net App Prevent.
(3) Click [Add New].
(4) Select a policy and specify a target to apply the policy.
(5) Select [Prevent] for Control Type, and select a Detection Rule to apply.
(6) Select [Business File Share] – [Onedrive] from Net Apps.
(7) Select a Countermeasure [Block/Allow].
(8) Click [Apply].

- File Blocking Test

(1) Browse to https://login.microsoftonline.com/
(2) Click the [Onedrive] icon from the menu on the bottom.
(3) Click [Upload].
(4) Locate a file that violates the detection rule and select the file to upload.
(5) Check the file upload is handled (blocked or allowed) in accordance with the countermeasure you previously specified.
(6) Check that the log for the activity exists and reads as what happened (Blocked/Allowed) from DLP+ Center.

5.2.2 Office 365 Mail

- Setting a Block Policy

(1) Click [POLICIES] on DLP+ Center.
(2) Click Network-Net App Prevent.
(3) Click [Add New].
(4) Select a policy and specify a target to apply the policy.
(5) Select [Prevent] for Control Type, and select a Detection Rule to apply.
(6) Select [Webmail] - [Microsoft Outlook Live].

(7) Select a Countermeasure [Block/Allow].
(8) Specify Time Range and click [Save].
(9) Click [Apply].

- Email Content Detection Test

(1) Browse to https://login.microsoftonline.com/
(2) Click the [Mail] icon from the menu on the bottom.
(3) Click [Create New].
(4) Write an email message with some information that violate the detection rules.
(5) Click [Send].
(6) Check the email message is handled (blocked or allowed) in accordance with the countermeasure you previously specified.
(7) Check that the log for the activity exists and reads as what happened (Blocked/Allowed) from DLP+ Center.

- Attached File Detection Test

(1) Browse to https://login.microsoftonline.com/
(2) Click the [Mail] icon from the menu on the bottom.
(3) Click [Create New].
(4) Specify recipient and put some texts in the body.
(5) Click [Attach Files] on top.
(6) Click the Computer icon, and add a file that violates the predefined detection rules.
(7) Select a way to upload the file (select Upload to OneDrive & Send as Shared/Attached File).

→ Skip to the step #9, if you select Upload to OneDrive.

(8) Check the email message is handled (blocked or allowed) in accordance with the countermeasure you previously specified.
(9) Check that the log for the activity exists and reads as what happened (Blocked/Allowed) from DLP+ Center.

5.2.3 Office 365 SharePoint

- Setting a Block Policy

(1) Click [POLICIES] on DLP+ Center.
(2) Click Network-Net App Prevent.
(3) Click [Add New].
(4) Select a policy and specify a target to apply the policy.
(5) Select [Prevent] for Control Type, and select a Detection Rule to apply.
(6) From Target Net Apps, select [Business File Share] - [Sharepoint].
(7) Select a Countermeasure [Block/Allow].
(8) Specify Time Range and click [Save].
(9) Click [Apply].

- Content Detection Test

(1) Browse to https://login.microsoftonline.com/ and login.
(2) Browse to https://portal.office.com/admin/default.aspx.

(3) Click [Office 365 Management Center] – [Administrator] – [SharePoint] on the left menu.
(4) Open the URL of a SharePoint Site registered.
(5) Enter a text that violates a predefined policy in the text entry below News Feed, and click [Post].
(6) Check the post is handled (blocked or allowed) in accordance with the countermeasure you previously specified.
(7) Check that the log for the activity exists and reads as what happened (Blocked/Allowed) from DLP+ Center.

- Attached File Detection Test

(1) Browse to https://login.microsoftonline.com/ and login.
(2) Browse to https://portal.office.com/admin/default.aspx.
(3) Click [Office 365 Management Center] – [Administrator] – [SharePoint] on the left menu.
(4) Open the URL of a SharePoint Site registered.
(5) Click [Upload].
(6) Click [Choose Files] and select a file that violates the predefined detection rules.
(7) Specify the target folder path, and click [OK].
(8) Check the upload is handled (blocked or allowed) in accordance with the countermeasure you previously specified.
(9) Check that the log for the activity exists and reads as what happened (Blocked/Allowed) from DLP+ Center.