Privacy-i

V6.0 for DLP+ HyBoost

[Admin Manual V1.0]

Introduction

The contents of this manual may be changed without prior notice to improve the product and enhance performances. The companies, organizations, products, people and events illustrated in the examples of the manual are fictitious, and are not actual entities. Any part of this manual shall not be replicated or stored to search systems, or introduced or transferred to the system, in any form or by any means (electronic, mechanical, copy machine, disk copy or otherwise), or for any purpose without the explicit approval from Somansa Co., Ltd.

Somansa Co., Ltd. holds patents, trademark rights, copyrights and other intellectual property rights related to the subject matter described 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 with any license regarding the patents, trademark rights, copyrights and 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.comInquirieson Function/ On-Line Remote Assistance/ Off-Line Maintenance Support Requests/User Training Requests

[Remark]
The resident registration numbers shown on the UI screens included in the manual are manipulated numbers with actual validity.

Contents

1. Personal Information Retention Control Solution: Privacy-i

1.1 Overview

1.1.1 What is personal information retention control solution Privacy-i?

Privacy-i, a personal information retention control solution, is a tool that automatically scans and locates personal information stored in PCs which has been designated to be deleted by the governing laws so that staffs of a company can delete it in person. The laws stipulate that personal information be strictly controlled as described below, and, if violated, corresponding personnel and the company shall be subject to punishment by the law.

[TABLE 1-1] REGULATIONS RELATED TO PERSONAL INFORMATION

Related regulations	Articles	Contents
[Notification by Korea Communications Commission Standards of measures for technical/administrative protection of personal information]	Article 3	Only the personnel in charge of treating personal information can retain personal information in PC, and the personnel information retained in PC by the personnel must be **removed** after use.
	Article 6-4	The personal information retained in PC by authorized personnel for treating personal information should be **encrypted** for saving.
Act on Information and Communication Network	Article 29	When the period of use of personal information expires (meaning termination of the purpose of use), the corresponding information should be **removed** immediately.

1.2 System Recommendation

Please refer to [Table 1-2] for the correct operating system version on which to install the Server, Management Console and Agent.

[TABLE 1-2] OPERATING SYSTEM IDENTIFICATION

Category	Operating System
Privacy-i Server DLP+ Center Configurator Manager	CentOS6.4_x64 or above (Kernel 2.6.x or above)
Privacy-i Agent (Windows)	Windows 7 (x86/x64), following editions: - Home Premium - Professional - Ultimate - Enterprise Windows 8.1 (x86/x64) Windows 8.1 Pro (x86/x64) Windows 8.1 Enterprise (x86/x64) Windows 10 (x86/x64) Windows 10 Pro (x86/x64) Windows 10 Enterprise (x86/x64)

Below are the hardware requirements to install the Server, Management Console and Agent.

[TABLE 1-3] MINIMUM HARDWARE REQUIREMENTS TO INSTALL PRIVACY-i

Category	Hardware and Software Requirements	
Privacy-i Server DLP+ Center Configurator Manager	CPU	Intel Quad Xeon 3.1GHz * 1 or higher
	HDD	500GB * 2 (raid1) or more
	MEM	8GB or more
Privacy-i Agent	CPU	Intel Core 2 1.6Ghz
	HDD	3 GB or more of free space
	MEM	1GB or more
※ Number of simultaneous users of Privacy-i Agent: Recommended to limit to 3000 users per server. Distributed operations to multiple servers are required when there are more than 3000 users.		

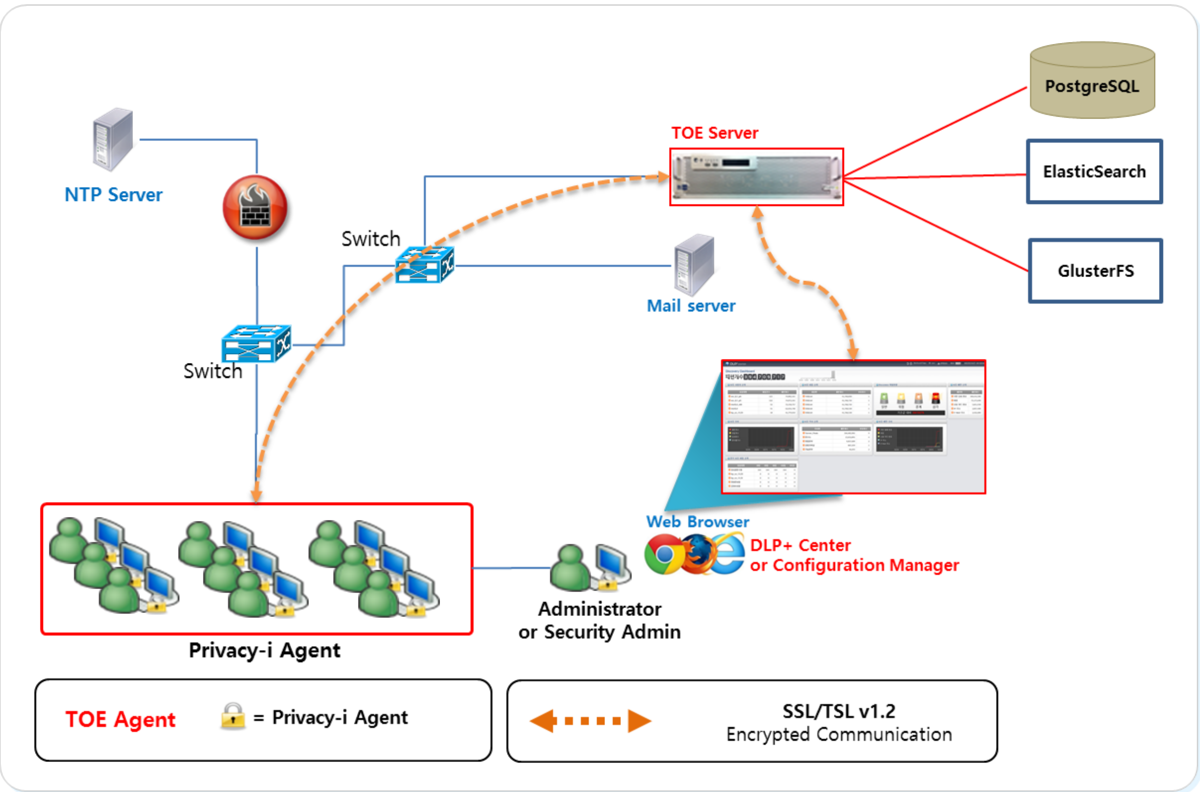
1.3 Package Configurations

Privacy-i V6.0 for DLP+ HyBoost package is configured as shown in [Table 1-4].

[TABLE 1-4] PRIVACY-I PACKAGE CONFIGURATION TABLE

Category	Qty.	Note
TOE Server package	1	Server application
TOE Agent package	1	Agent Application to be installed on a user's computer
Admin / User manual	1	Admin Guide
Software License Certificate	1	License Certificate to allow the use of the software

1.4 Privacy-i Configuration Diagram



(FIGURE 1-1) PRIVACY-I SYSTEM CONFIGURATION DIAGRAM

☞ **"Privacy-i V6.0 for DLP+ HyBoost" runs tasks according to the following procedures.**

① Install the Agent on a PC to inspect whether it contains personal information or not.
② Agent inspects personal information periodically on the local disk of a host.
③ Agent sends a inspection result to the server, and the result is saved on the HDD for log storage.
④ Users can run a user inspection on Agent to check whether the PC retains any personal information in the PC.
⑤ Agent controls external interfaces of a host (USB, Print, CD/DVD, Bluetooth, Wired/Wireless LAN, etc.) or checks the data that is transmitted according to the Admin Policy in order to run the function of controlling personal information data.

☞ **Administrator runs the following tasks through the Configuration Manager.**

① Connect to a database to save logs and policies.
② PostgreSQL 9.3 is used as a database for storing data such as logs and policies. And, use TCP/IP-based data communication when the Privacy-i Server and DLP+ Center communicate with the database.
③ Set the HDD capacity on the DB logs to prevent losing logs when they become full.
④ Register the Privacy-i license.

☞ **Administrator runs the following tasks through DLP+ Center.**

① Set the data pattern for reference to inspect of personal information in a user PC when Agent inspects for personal information in a user PC.
② Generates or edits other administrator or user account.
③ Query searched personal information to analyze the trends of retaining personal information in the company, and warns to each user or performs the task of file deletion or encryption.

(Figure 1-1) SSL3.0/TLS1.2 is provided for communication channel between component modules of the system. Detailed information on the encryption algorithm used for encrypted communication is shown in

[TABLE 1-5].

[TABLE 1-5] DETAILS OF ENCRYPTION CHANNEL FOR EACH COMPONENT

Encryption library	Privacy-i Server DLP+ Center Configuration Manager	OpenSSL 1.0.1s
	Privacy-i Agent	SChannel (Windows 7/8/10)
Protocol	SSL3.0 / TLS_v1.2	
Subject	All data channel transmitted or received between Privacy-i Server ↔ Privacy-i Agent, DLP+ Center / Configuration Manager ↔ Management console	
Cipher Suites	TLS_RSA_WITH_AES_128_CBC_SHA256	
	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	
	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	
	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	
	TLS_RSA_WITH_AES_256_CBC_SHA256	
	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	
	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	

Also, the Tomcat Server operated in the server is composed of 3 units, with ports configured as follows.

[TABLE1-6] SERVICE PORTS FOR EACH COMPONENT MODULE

Components	Port	Note
DLP+ Center	443	
Privacy-i Server		
Configurator Manager		

1.5 Encryption / Decryption Algorithm

The encryption algorithm used by Privacy-i product for encrypting/encoding uses SEED-128. The library for the algorithm uses **Klib** (developed by Korea University, and has been approved by National Intelligence Service in 2014). See [TABLE 1-7] for detailed information.

[TABLE1-7] KLIB DETAILED INFORMATION

Category	Contents
Encryption algorithm	Klib v2.1 -> SEED(128bit) + CBC block encryption
Safe key induction	Standards of PKCS#5 password-based encryption (RFC2898 applied) Encryption Key induction algorithm = PBKDF2_HMAC-SHA1 (Password, Salt, Iteration Count)

1.6 Product Information

1.6.1 First Release Date: October 1, 2016

1.6.2 Structure of Manual

The manual consists of two parts, the Administrator's Manual and the User's Manual. The Administrator's manual includes instructions and descriptions of configuration, installation and usage of the server. The User's Manual includes instructions and descriptions of configuration, installation and usage of Agent.

- Administrator's Manual: Privacy-i V6.0 for DLP+ HyBoost Administrator's Manual V1.0.docx
- User's Manual: Privacy-i V6.0 for DLP+ HyBoost User's Manual V1.0.docx

2. Installation

2.1 Environmental Conditions

The process described in this section requires programs to install Privacy-i V6.0 for DLP+ HyBoost product.

[TABLE 2-1] ENVIRONMENTAL CONDITIONS FOR INSTALLING PROGRAMS

Program	Version	Note
PostgreSQL	9.3	Database
gcc-c++	4.4.7	Compiler
Java Runtime Environment (JRE)	1.8	Running environment

Recommendations

✓ When creating a PostgreSQL account, it is recommended to create and add a Database Administrator account, rather than using the Default account.

2.2 Installing Product

2.2.1 Installing TOE Server Package

To run Privacy-i V6.0 for DLP+ HyBoost TOE server package, execute the '**Privacy-i_V6.0_for_DLP+_HyBoost_Install.BIN**' Installation file. (※ PostgreSQL must be installed before installing the product. Be noted that the package cannot be installed if PostgreSQL is not installed.) Run the Package as follows. (Check the file permissions when running the Package.)

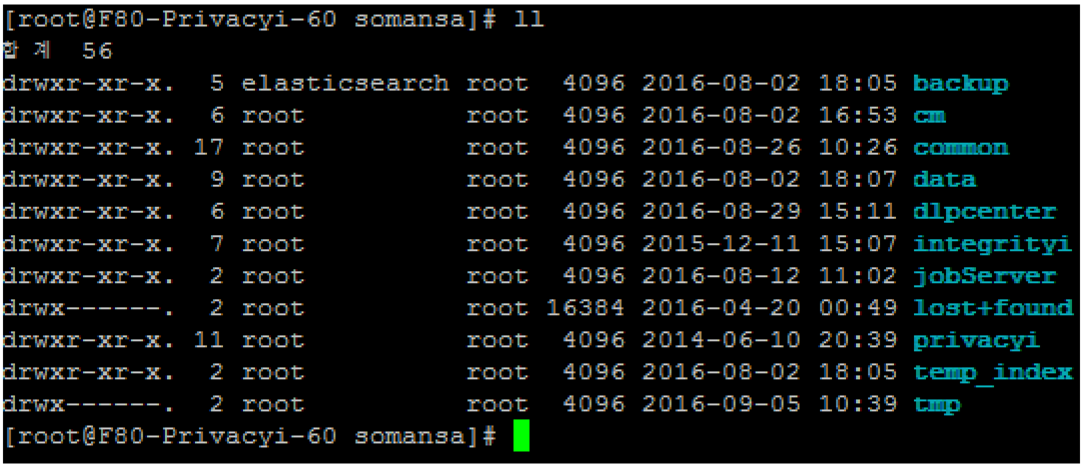
#sh Privacy-i_V6.0_for_DLP+_HyBoost_Install.BIN

If following message is shown during installation, enter the IP of a PC where the Security administrator 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 desktop to connect Configuration Manager
192.168.10.171 (contents that user should input)

2.2.2 Installation Path

When installation of Privacy-i 6.0 for DLP+ HyBoost package is completed, the product will be installed in /somansa path as shown below (Figure 2-1).



```
[root@F80-Privacyi-60 somansa]# ll
합 계  56
drwxr-xr-x.  5 elasticsearch root   4096 2016-08-02 18:05 backup
drwxr-xr-x.  6 root          root   4096 2016-08-02 16:53 cm
drwxr-xr-x. 17 root          root   4096 2016-08-26 10:26 common
drwxr-xr-x.  9 root          root   4096 2016-08-02 18:07 data
drwxr-xr-x.  6 root          root   4096 2016-08-29 15:11 dlpcenter
drwxr-xr-x.  7 root          root   4096 2015-12-11 15:07 integrityi
drwxr-xr-x.  2 root          root   4096 2016-08-12 11:02 jobServer
drwx------.  2 root          root  16384 2016-04-20 00:49 lost+found
drwxr-xr-x. 11 root          root   4096 2014-06-10 20:39 privacyi
drwxr-xr-x.  2 root          root   4096 2016-08-02 18:05 temp_index
drwx------.  2 root          root   4096 2016-09-05 10:39 tmp
[root@F80-Privacyi-60 somansa]#
```

(FIGURE 2-1) INSTALLATION PATH SET-UP SCREEN

When installation of TOE server terminates, i Server is complete, connect to the Configuration Manager, extract the UID of the Server, and apply for issuance of a License by contacting Somansa License Center (http://license.somansa.com/). The connecting address for the Configuration Manager is as follows:

https://IP_ADDR/cm

2.3 License

2.3.1 Issuance Procedure

STEP
Copy the two license files (privacyi.license, privacyi.license.serial) received via e-mail to '/somansa/common/license' folder, and copy encryption key (cm_piencrypt.dat) to '/somansa/privacyi/data' folder.

STEP 2
Registered license can be confirmed from Configuration Manager > Privacy-i > license tab.

2.3.2 Disadvantages of not renewing licenses

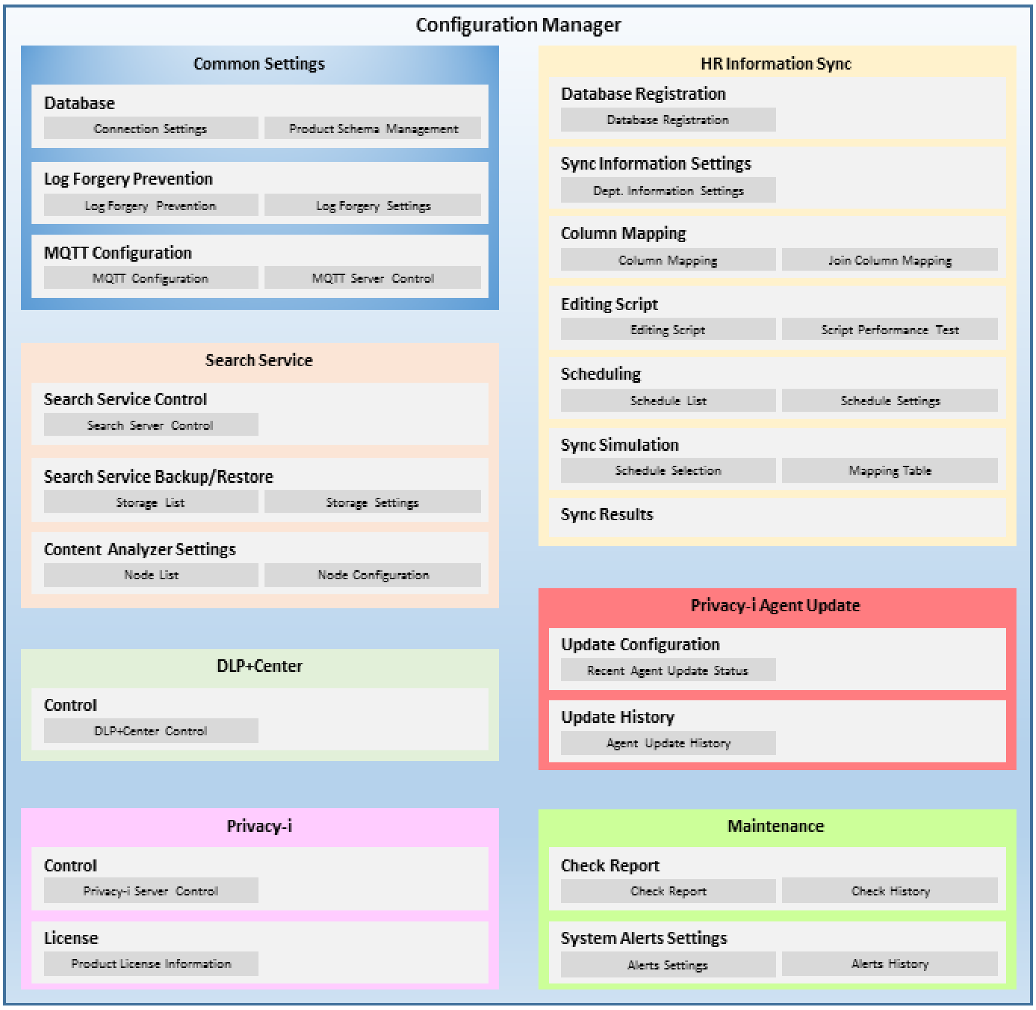
If a product license agreement has expired and not renewed, the product will not update. In addition, the latest security patch files cannot be received, and server operation cannot be controlled when Privacy-i Server is down. Therefore, please renew the license when it has expired.

3. Configuration Manager

3.1 Running Configuration Manager

Run the Configuration Manager through a web browser. The initial Security Administrator password is provided by UI, and should be changed after login. If the password is forgotten, please contact the person at SOMANSA in charge of the business.

3.2 Configuration Manager Setup



Configuration Manager

Common Settings
- Database: Connection Settings, Product Schema Management
- Log Forgery Prevention: Log Forgery Prevention, Log Forgery Settings
- MQTT Configuration: MQTT Configuration, MQTT Server Control

Search Service
- Search Service Control: Search Server Control
- Search Service Backup/Restore: Storage List, Storage Settings
- Content Analyzer Settings: Node List, Node Configuration

DLP+Center
- Control: DLP+Center Control

Privacy-i
- Control: Privacy-i Server Control
- License: Product License Information

HR Information Sync
- Database Registration: Database Registration
- Sync Information Settings: Dept. Information Settings
- Column Mapping: Column Mapping, Join Column Mapping
- Editing Script: Editing Script, Script Performance Test
- Scheduling: Schedule List, Schedule Settings
- Sync Simulation: Schedule Selection, Mapping Table
- Sync Results

Privacy-i Agent Update
- Update Configuration: Recent Agent Update Status
- Update History: Agent Update History

Maintenance
- Check Report: Check Report, Check History
- System Alerts Settings: Alerts Settings, Alerts History

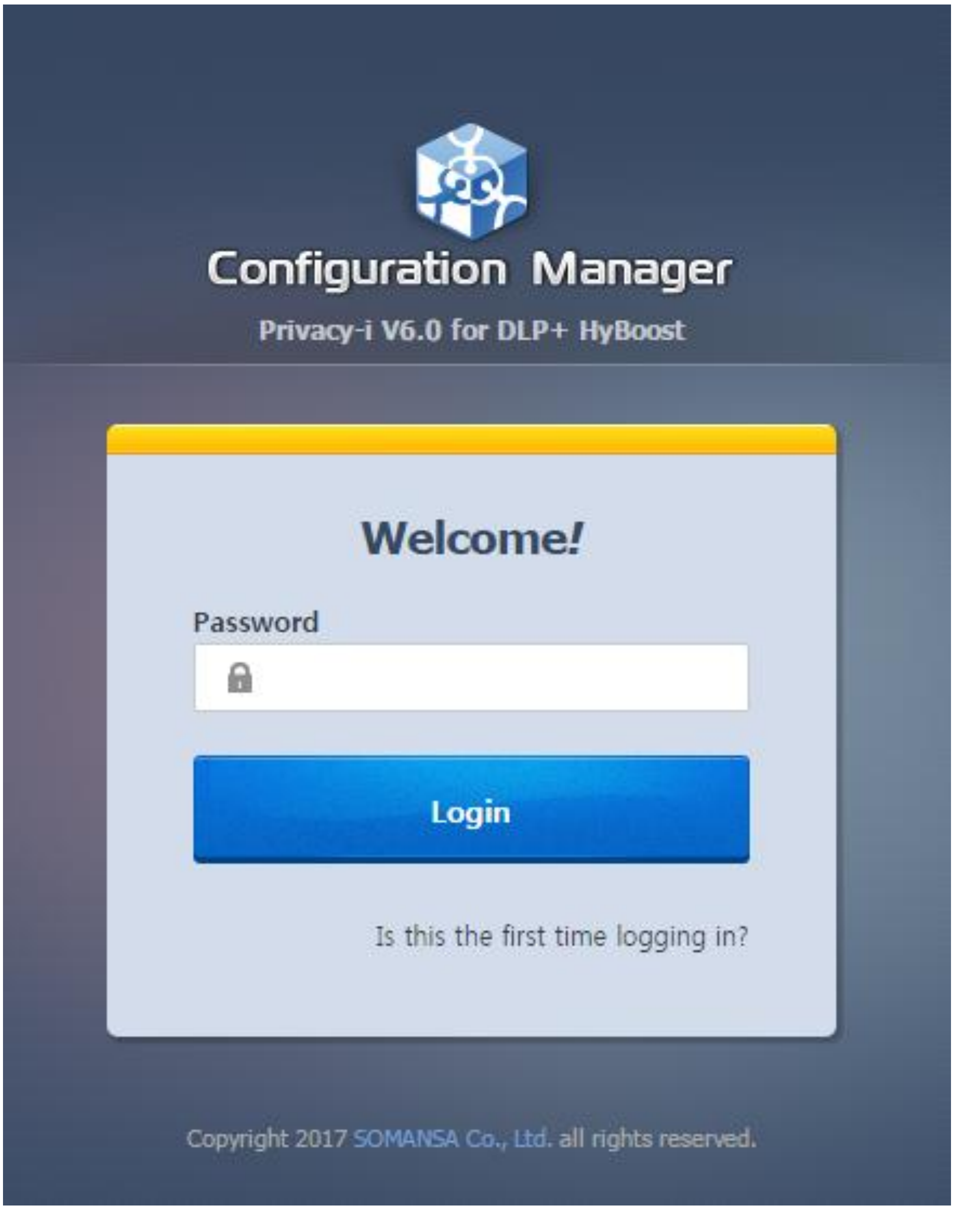
(FIGURE 3-1) CONFIGURATION MANAGER CONFIGURATION DIAGRAM

Configurator Manager is configured as in (Figure 3-1). Configuration Manager provides configuration of common areas, DLP+ Center, Privacy-i, Maintenance, environmental settings.

3.3 Initial Connection Settings

3.3.1 Enter Password in the First Connection

When logged in to Configuration Manager, a login page will appear as below (Figure 3-2). The administrator account in Configuration Manager is “Security Admin”, and only one account is available. Therefore, additional separate ID needs to be entered. Enter the default password upon initial connection, and log in with the "Security Admin".


Configuration Manager
Privacy-i V6.0 for DLP+ HyBoost
Welcome!
Password
Login
Is this the first time logging in?
Copyright 2017 SOMANSA Co., Ltd. all rights reserved.

(FIGURE 3-2) CONFIGURATION MANAGER LOGIN SCREEN

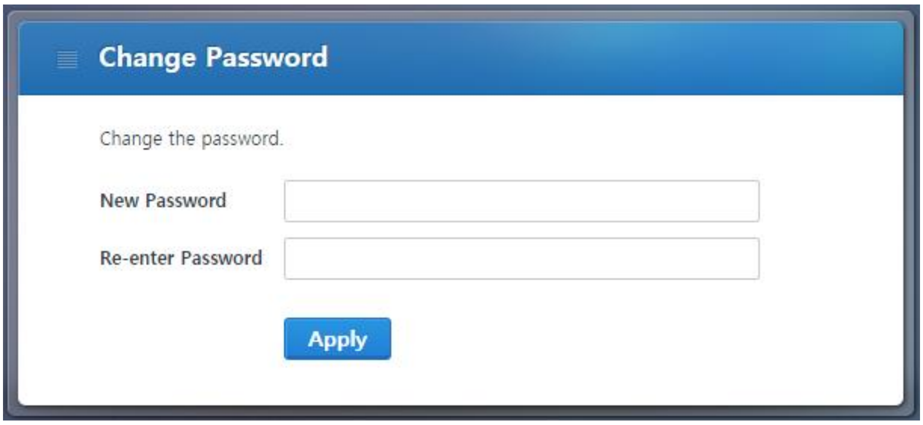
☞ Effective Input Field Range

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

Item	Effective range	Character	Failure message
Password	9~41	Numbers, upper and lower case letters, special characters	Enter password.

3.3.2 Setting Up a New Password

The screen appears after entering a default password. Set up a new password for the Security Admin in the Configuration Manager.



Change Password

Change the password.

New Password

Re-enter Password

(FIGURE 3-3) CONFIGURATION MANAGER NEW PASSWORD SETTING SCREEN

☞ EFFECTIVE INPUT FIELD RANGE UPON LOGIN

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

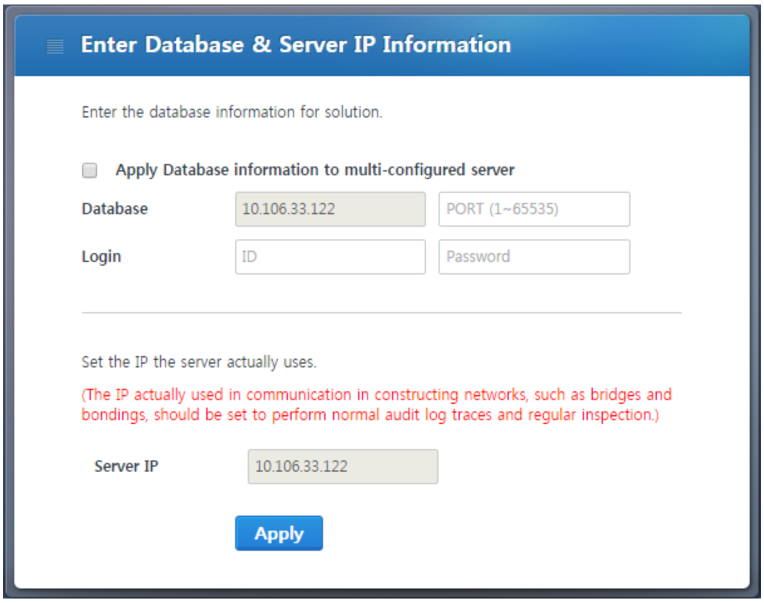
Item	Effective range	Character	Failure message
New password	9~41	Numbers, upper and lower case letters, special characters	Enter password.
Confirm the new password	9~41	Numbers, upper and lower case letters, special characters	Enter password again.

Recommendations

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

3.3.3 Enter Database Information

Enter database information for "Privacy-i V6.0 for DLP+ HyBoost" on this screen. Enter the database accessible IP / Port / Account.



Enter Database & Server IP Information

Enter the database information for solution.

□ Apply Database information to multi-configured server

Database: 10.106.33.122 | PORT (1~65535)

Login: ID | Password

Set the IP the server actually uses.

(The IP actually used in communication in constructing networks, such as bridges and bondings, should be set to perform normal audit log traces and regular inspection.)

Server IP: 10.106.33.122

(FIGURE 3-4) ENTER CONFIGURATION MANAGER DATABASE INFORMATION

☞ Descriptions on items

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.

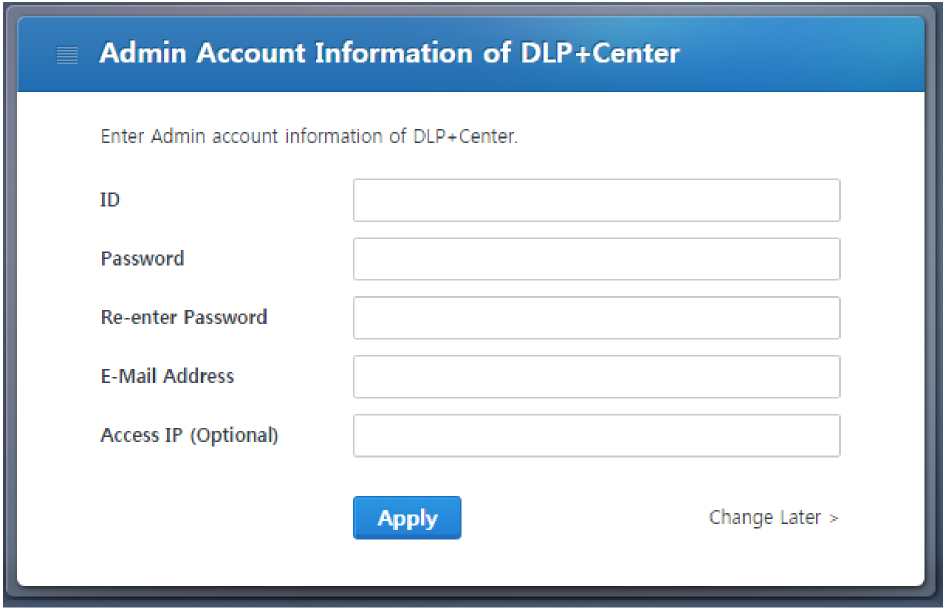
☞ EFFECTIVE INPUT FIELD RANGE UPON LOGIN

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

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

3.3.4 DLP+Center Admin Account Information Settings

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 can only access. In the 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.)



Admin Account Information of DLP+Center

Enter Admin account information of DLP+Center.

ID

Password

Re-enter Password

E-Mail Address

Access IP (Optional)

(FIGURE 3-5) ENTER DLP+ CENTER SECURITY ADMIN ACCOUNT INFORMATION

☞ EFFECTIVE INPUT FIELD RANGE UPON LOGIN

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

Item	Effective range	Character	Failure message
ID	5~100	Letters	Enter ID of DLP+ Center Admin.
Password	9~41	Numbers, upper and lower case letters, special characters	Enter Admin password of DLP+ Center.
Password	9~41	Numbers, upper and lower case letters, special characters	Enter Admin password of DLP+ Center again.
Access IP	15	Numbers, special character (.)	Enter effective Admin IP of DLP+ Center.

Recommendations

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

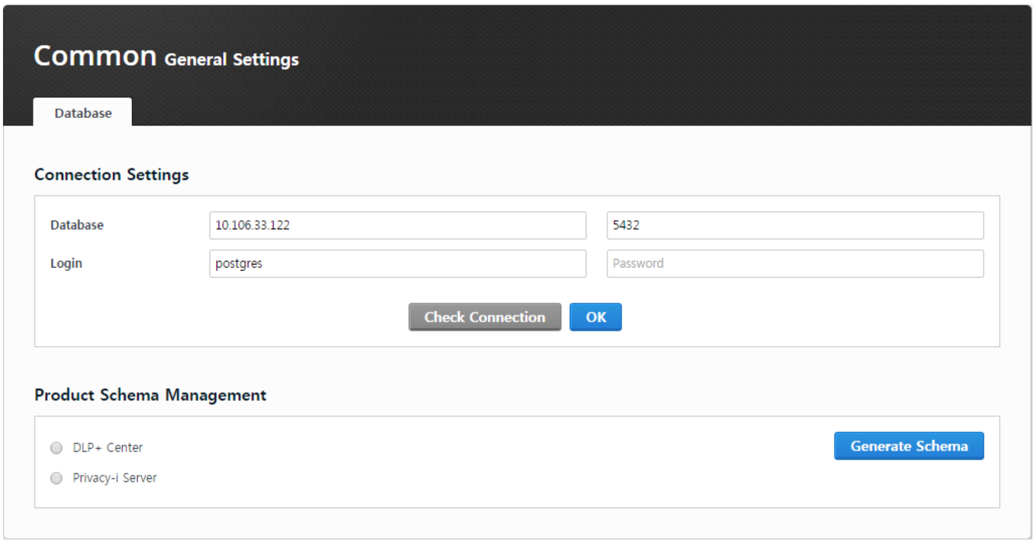
3.4 COMMON

3.4.1 Common Area Settings

Once the initial Configuration Manager setup is complete, the "Common Area Settings" menu appears. The page is the screen of the first page appearing upon re-login to the Configuration Manager. The Common Items provide the Default Database Settings, and Log manipulation Prevention for "Privacy-i V6.0 for DLP+ HyBoost" product.

3.4.1.1 Default Database Connection Settings

(Figure 3-6) 6) is a screen where a common database connection can be setup. The common database shows input information in the "3.3.3 Enter Database Information" during initial installation. If the "Privacy-i V6.0 for DLP+ HyBoost" database information is modified, the user can update the information through "Default Database Connection Settings".



Common General Settings

Database

Connection Settings

Database 10.106.33.122 5432

Login postgres Password

Product Schema Management

○ DLP+ Center

○ Privacy-i Server

(FIGURE 3-6) COMMON AREA SETTINGS SCREEN

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

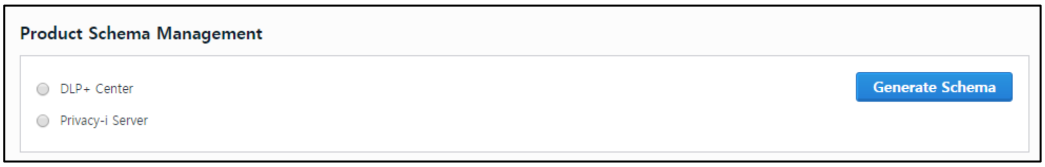
☞ Effective Input Field Range

[TABLE 3-5] EFFECTIVE INPUT FIELD RANGE UPON THE DEFAULT DATABASE CONNECTION

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

3.4.1.2 Product Schema Management

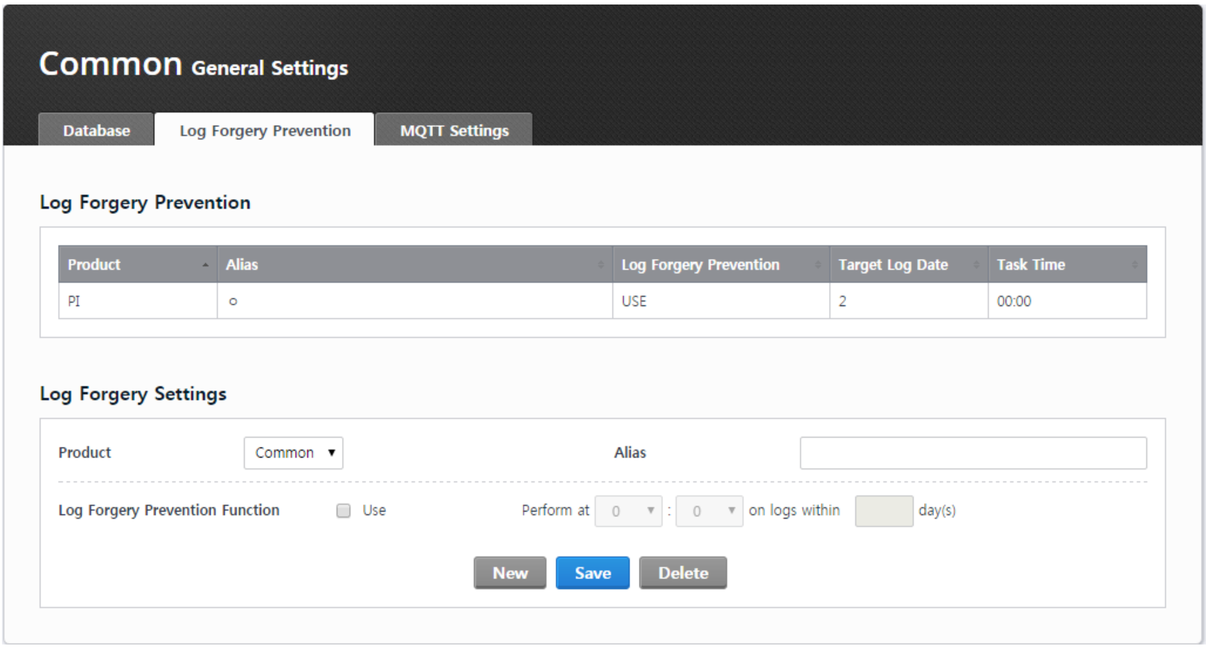
After the initial preference task, a task must be run through "Create Schema". This creates a database that is needed to run Privacy-i Server, DLP+ Center, and the Schema is created in the database entered in the "Default Database Connection Settings". When "Create Schema" is clicked, a notification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



(FIGURE 3-7) PRODUCT SCHEMA MANAGEMENT SCREEN

3.4.1.3 Log Manipulation Settings

In order to prevent sensitive contents logs of saved personal information from being manipulated, “Log Manipulation Settings” function is provided. For the function of setting the log manipulation, log database of the Privacy-i Server should have been generated in advance (See 3.5 Privacy-i Server). Since only reading authority is provided and delete/modify is not available when using the function of preventing log manipulation, the function of protecting personal information sensitive contents log is being provided.



Log Forgery Prevention

Product	Alias	Log Forgery Prevention	Target Log Date	Task Time
PI	○	USE	2	00:00

Log Forgery Settings

Product: Common ▾ Alias:

Log Forgery Prevention Function ☐ Use Perform at 0 ▾ : 0 ▾ on logs within day(s)

(FIGURE 3-8) COMMON AREA SETTING SCREEN

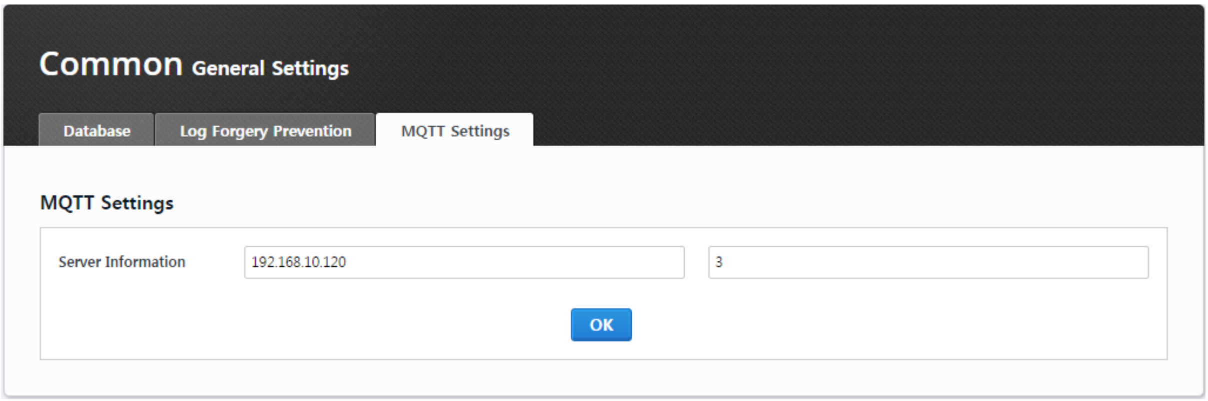
☞ Effective Input Field Range

[TABLE 3-6] EFFECTIVE INPUT FIELD RANGE OF WORM MANAGEMENT

Item	Effective range	Character	Failure message
Log manipulation prevention function (Date)	1~9999	Numbers	Enter the log date for prevention.

3.4.1.1 MQTT Settings

After entering the information of MQTT server, the state can be checked and controlled. It is possible to start, stop and refreshing the MQTT server.



MQTT Settings

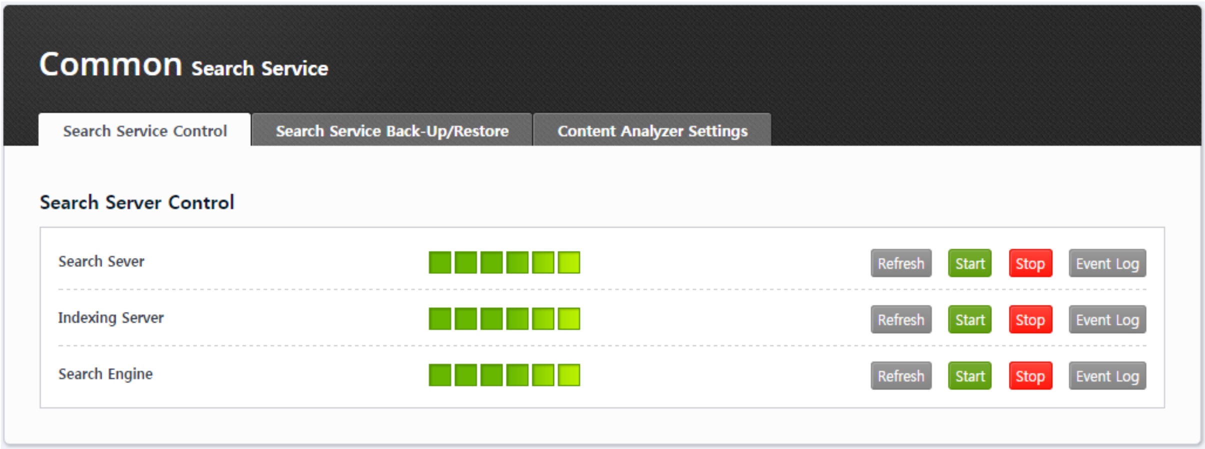
Server Information: 192.168.10.120 | 3

(FIGURE 3-9) COMMON – COMMON AREA SETTINGS – MQTT SETTINGS

3.4.2 Search Server

3.4.2.1 Search Server Control

The state of the search server can be checked and controlled. Normal operation is possible only when start, stop and refreshing can be checked and run for the query server, indexing server and the search.

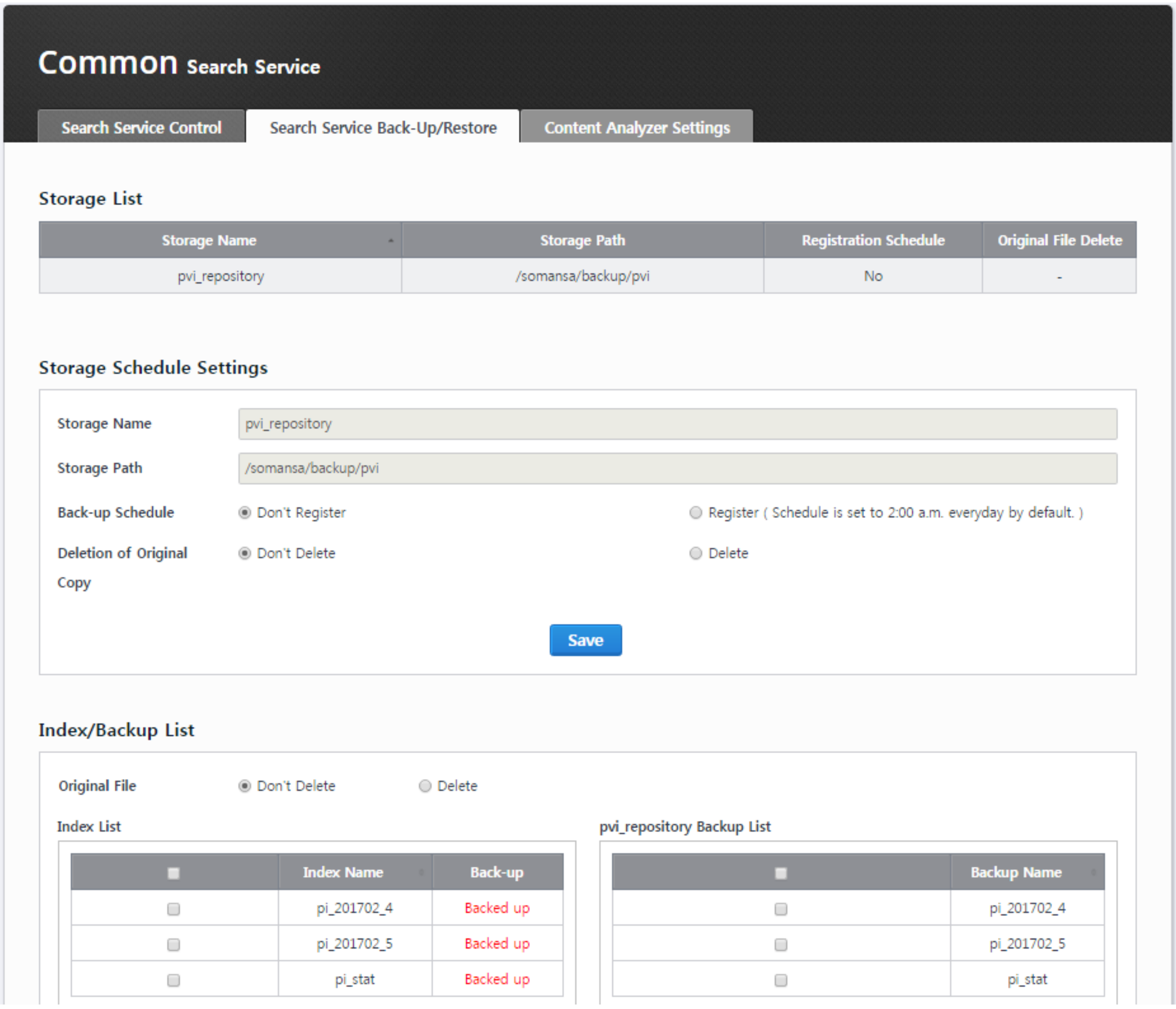


Search Sever	🟩🟩🟩🟩🟩🟩	Refresh	Start	Stop	Event Log
Indexing Server	🟩🟩🟩🟩🟩🟩	Refresh	Start	Stop	Event Log
Search Engine	🟩🟩🟩🟩🟩🟩	Refresh	Start	Stop	Event Log

(FIGURE 3-10) COMMON – SEARCHSERVER – SEARCH SERVER CONTROL

3.4.2.2 Search Server Backup / Restoration

Search server can be backed up and restored. Repository can be set and schedules can be registered to perform. Backup and restoration functions are provided for ElasticSearch where logs are saved and GlusterFS where file is saved. Index / backup list will be enabled when mi_repository is selected in the repository list.



Storage List

Storage Name	Storage Path	Registration Schedule	Original File Delete
pvi_repository	/somansa/backup/pvi	No	-

Storage Schedule Settings

Storage Name	pvi_repository
Storage Path	/somansa/backup/pvi
Back-up Schedule	● Don't Register ○ Register (Schedule is set to 2:00 a.m. everyday by default.)
Deletion of Original Copy	● Don't Delete ○ Delete

Index/Backup List

Original File ● Don't Delete ○ Delete

Index List

□	Index Name	Back-up
□	pi_201702_4	Backed up
□	pi_201702_5	Backed up
□	pi_stat	Backed up

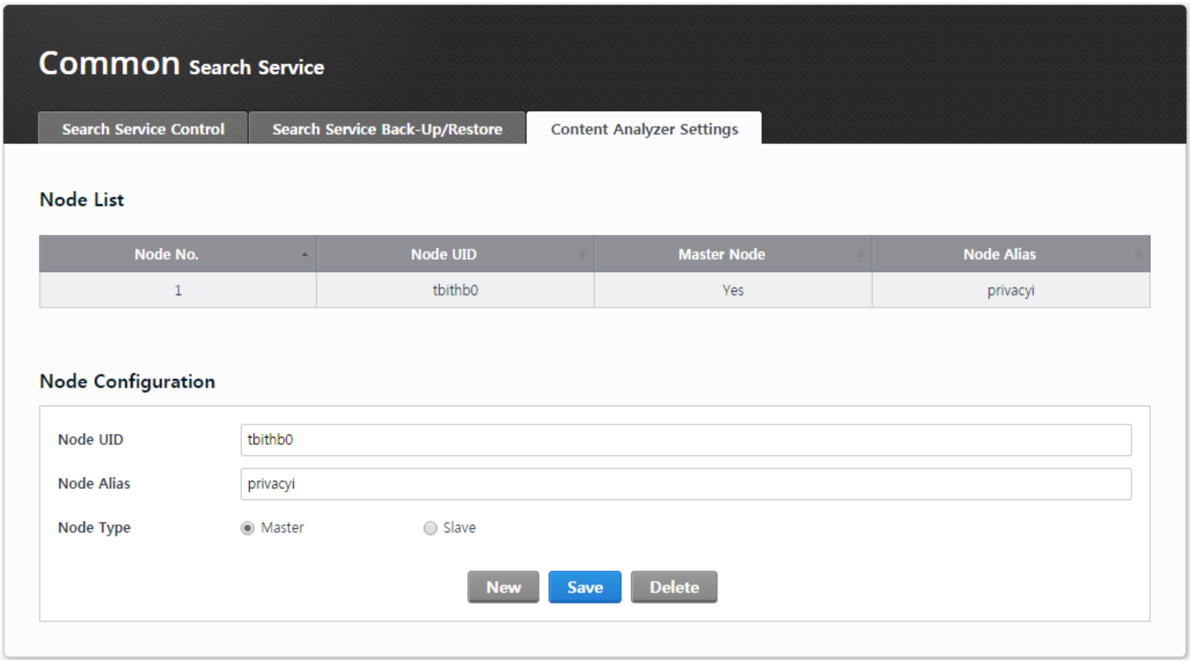
pvi_repository Backup List

□	Backup Name
□	pi_201702_4
□	pi_201702_5
□	pi_stat

(FIGURE 3-11) COMMON – SEARCH SERVER BACKUP / RESTORATION – REPOSITORY LIST

3.4.2.3 Setting Contents Analyzer

Text of logs, personal information pattern of files can be analyzed by setting the contents analyzer.



Node List

Node No.	Node UID	Master Node	Node Alias
1	tbithb0	Yes	privacyi

Node Configuration

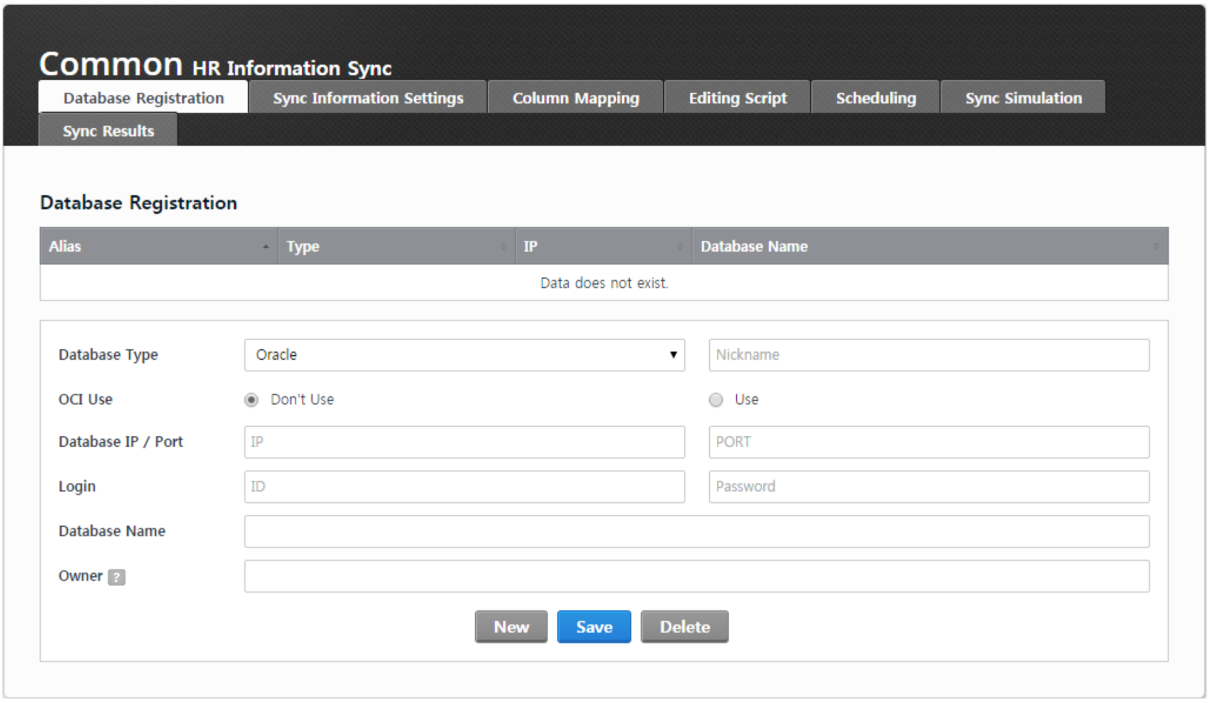
Node UID	tbithb0
Node Alias	privacyi
Node Type	● Master ○ Slave

(FIGURE 3-12) COMMON – CONTENTSANALYZER SETTINGS – NODE INFORMATION AND SETTINGS

3.4.3 Association of Human Resource (HR) Information

3.4.3.1 Database Registration

DB information for synchronization human resource information can be registered.



Database Registration

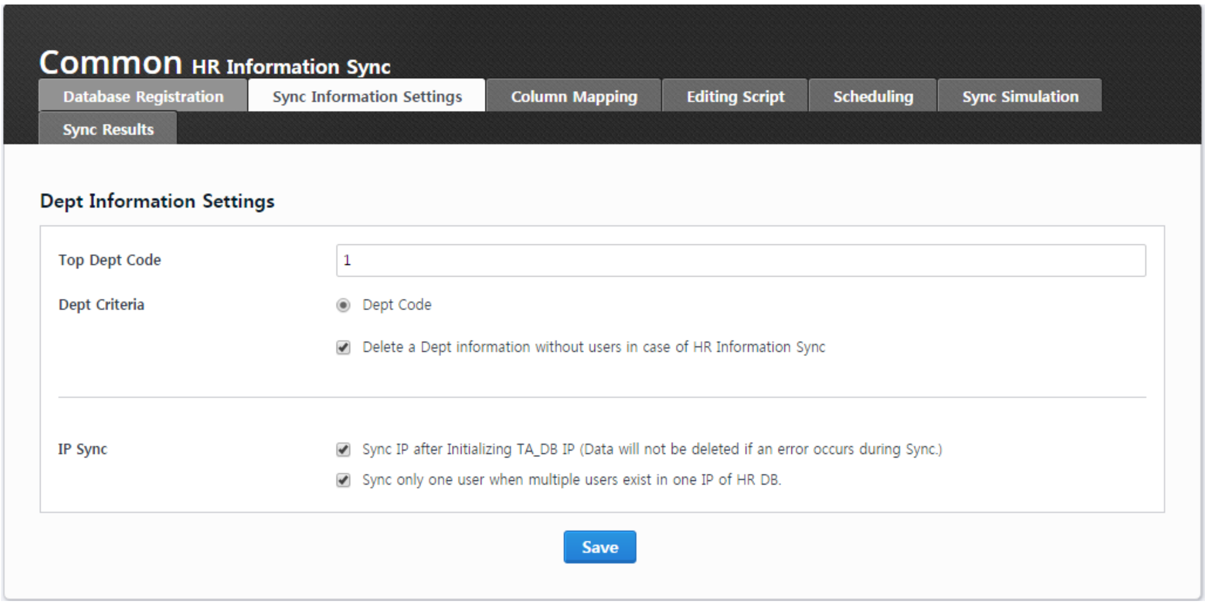
Alias	Type	IP	Database Name
Data does not exist.			

Database Type	Oracle ▾	Nickname
OCI Use	● Don't Use	○ Use
Database IP / Port	IP	PORT
Login	ID	Password
Database Name		
Owner ?		

(FIGURE 3-13) HR INFROMATION REGISTRATION SCREEN

3.4.3.2 Synchronization Information Settings

Department information can be set.



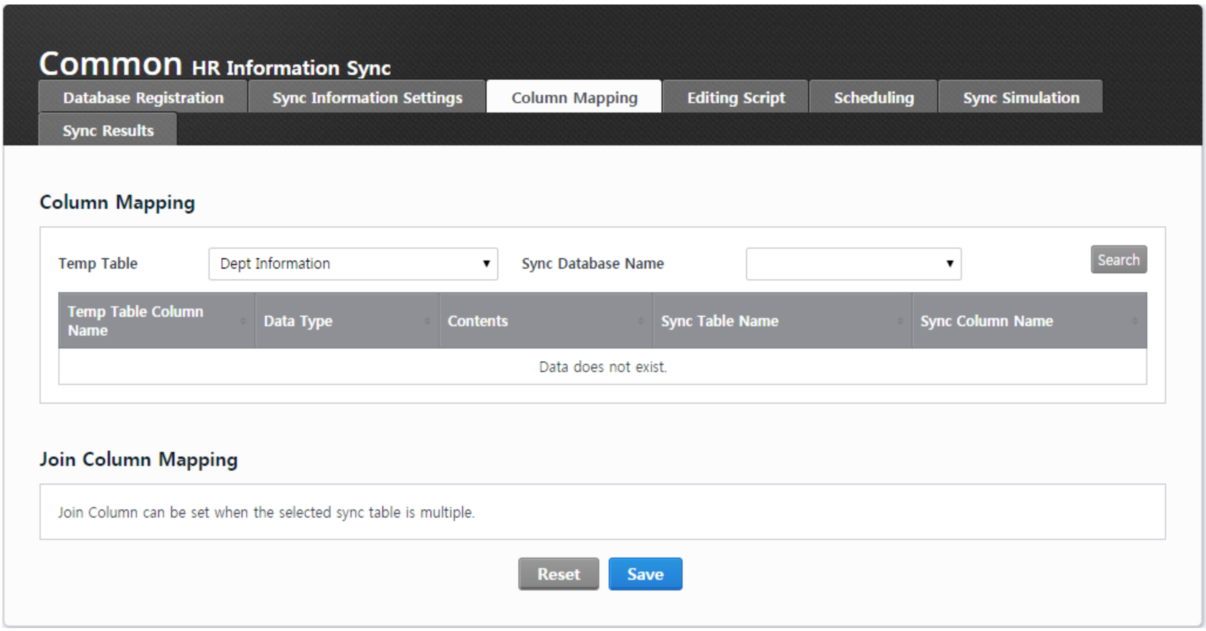
Dept Information Settings

Top Dept Code	1
Dept Criteria	● Dept Code ☑ Delete a Dept information without users in case of HR Information Sync
IP Sync	☑ Sync IP after Initializing TA_DB IP (Data will not be deleted if an error occurs during Sync.) ☑ Sync only one user when multiple users exist in one IP of HR DB.

(FIGURE 3-14) SYNCHRONIZATION INFORMATION SETTING SCREEN

3.4.3.3 Column Mapping

The user information to be used in DLP+Center and the user information present in HR information DB are mapped.



Temp Table: Dept Information ▾

Sync Database Name: ▾

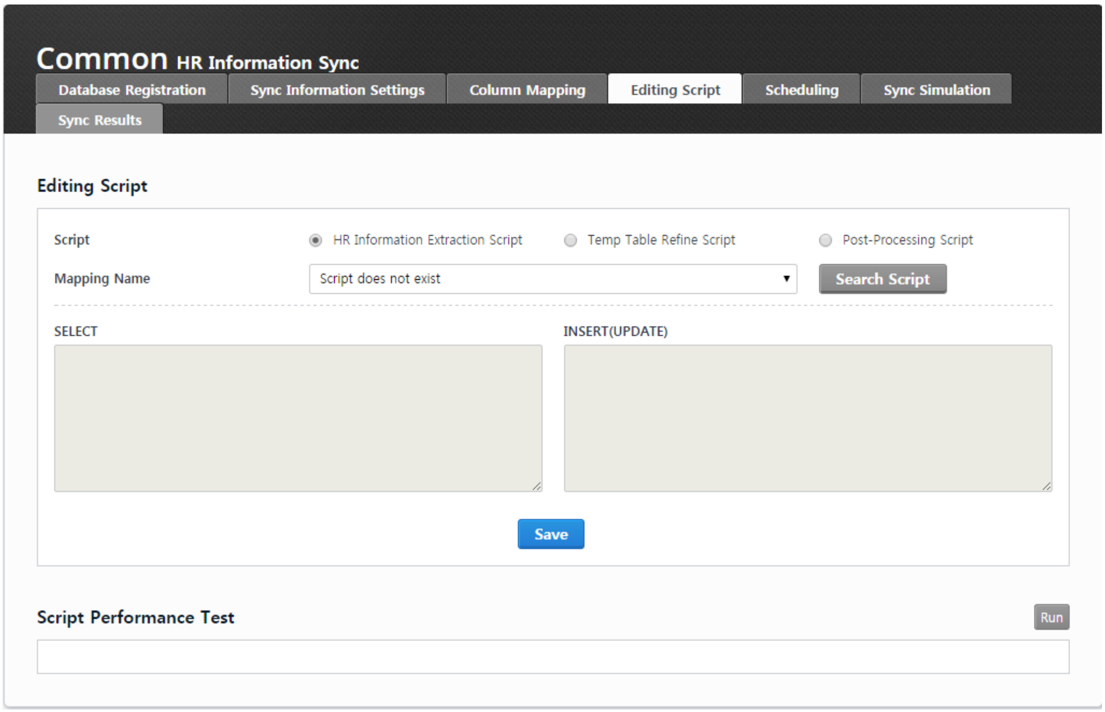
Temp Table Column Name	Data Type	Contents	Sync Table Name	Sync Column Name
Data does not exist.				

Join Column can be set when the selected sync table is multiple.

(FIGURE 3-15) COLUMN MAPPING SCREEN

3.4.3.4 Editing Script

It can be saved by viewing HR information extraction script or temporary table refinement script. The results of executions can be previewed through the results of script execution test.



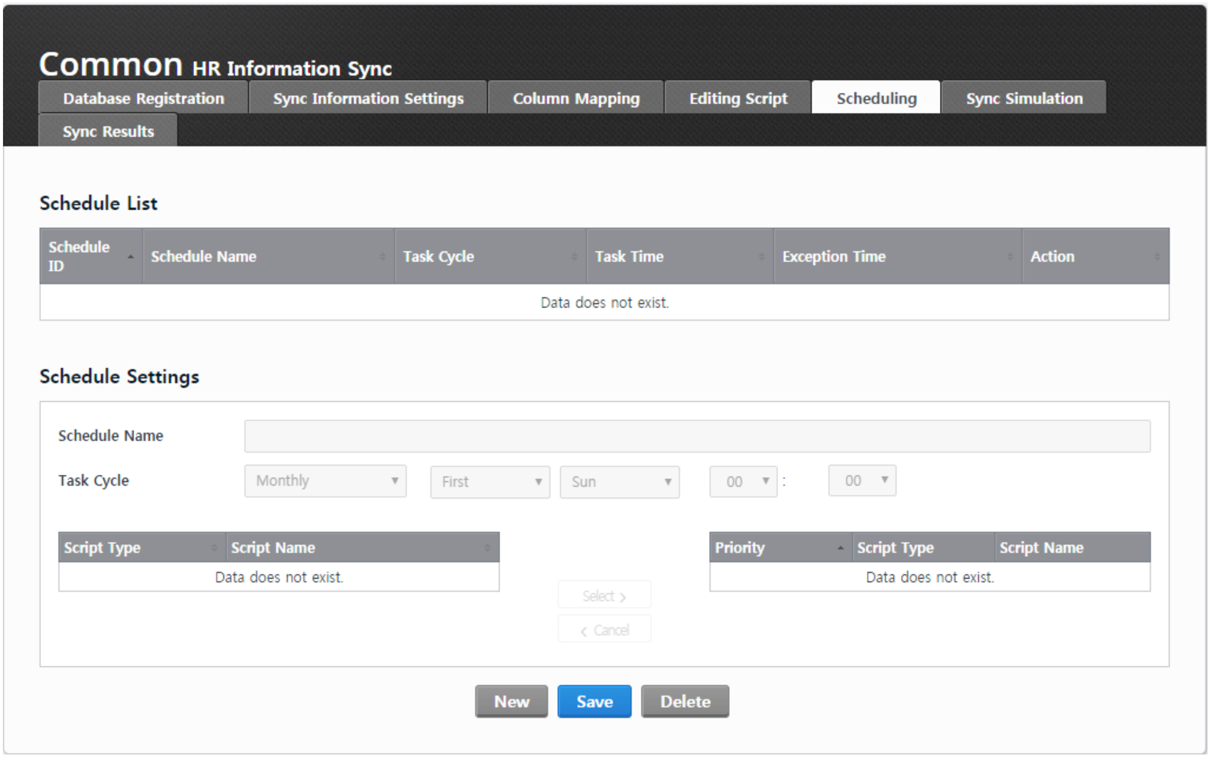
Script: ● HR Information Extraction Script ○ Temp Table Refine Script ○ Post-Processing Script

Mapping Name: Script does not exist ▾

(FIGURE 3-16) SCRIPT EDIT SCREEN

3.4.3.5 Scheduling

Synchronization with HR information DB is performed for every predefined period by registering to the scheduling. Association is possible in the unit of day, week and month.



Schedule List

Schedule ID	Schedule Name	Task Cycle	Task Time	Exception Time	Action
Data does not exist.					

Schedule Settings

Schedule Name	
Task Cycle	Monthly, First, Sun, 00 : 00

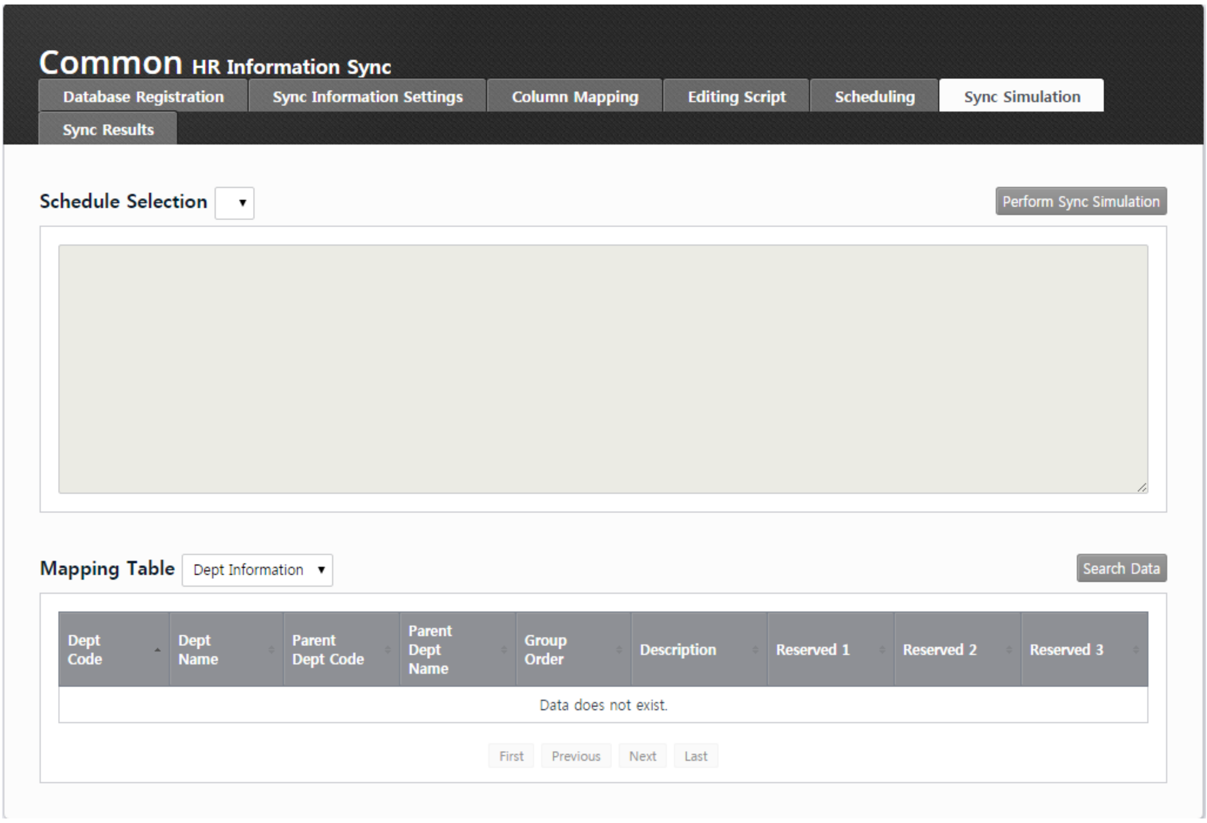
Script Type	Script Name
Data does not exist.	

Priority	Script Type	Script Name
Data does not exist.		

(FIGURE 3-17) SCHEDULING SCREEN

3.4.3.6 Synchronization Simulation

HR information DB association registered to the scheduling can be performed through the Synchronization simulation. The results of performance can be viewed through a mapping table.

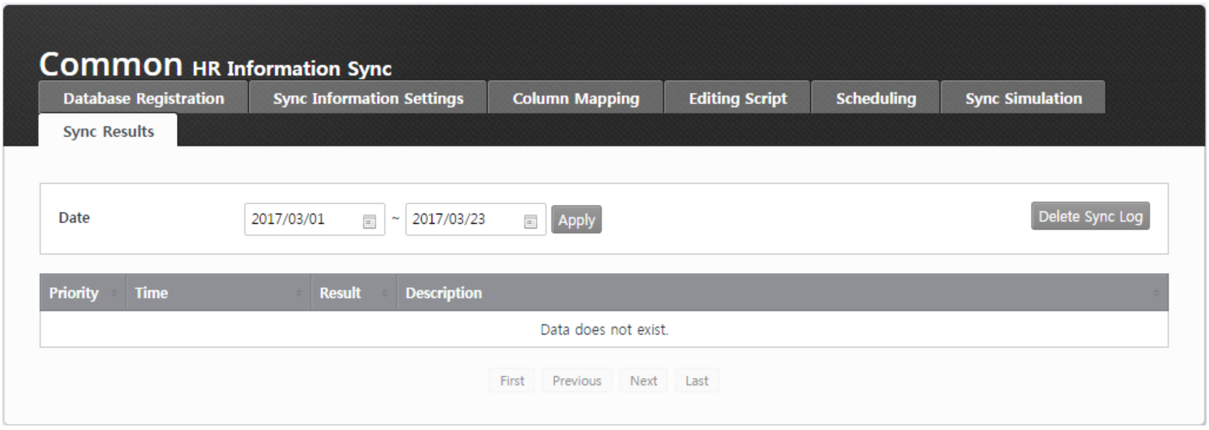


Dept Code	Dept Name	Parent Dept Code	Parent Dept Name	Group Order	Description	Reserved 1	Reserved 2	Reserved 3
Data does not exist.								

(FIGURE 3-18) SYNCRONIZATION SIMULATION SCREEN

3.4.3.7 View Results of Synchronization

Results of performing the synchronization can be checked.



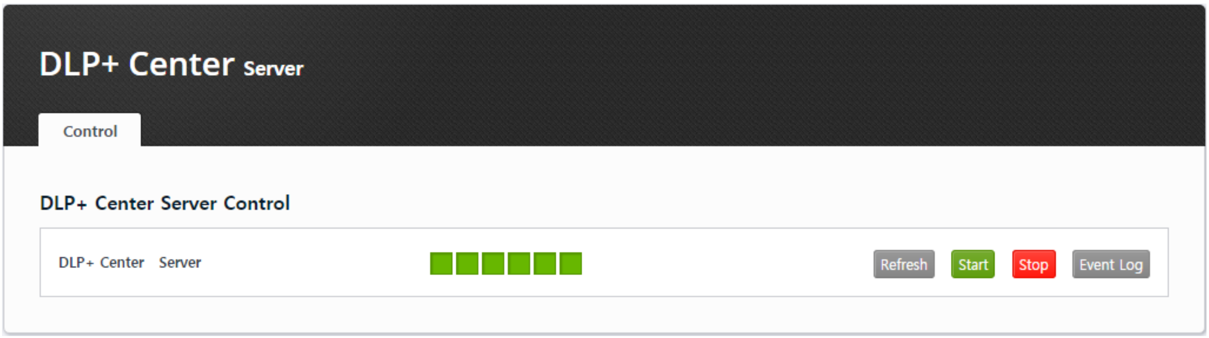
Date 2017/03/01 ~ 2017/03/23

Priority	Time	Result	Description
Data does not exist.			

(FIGURE 3-19) SCREEN FOR VIEWING SYNCHRONIZATION RESULTS

3.5 DLP+Center

The state of DLP+ Center server can be checked and controlled. It is possible to start, stop and refresh for the DLP+ Center server.

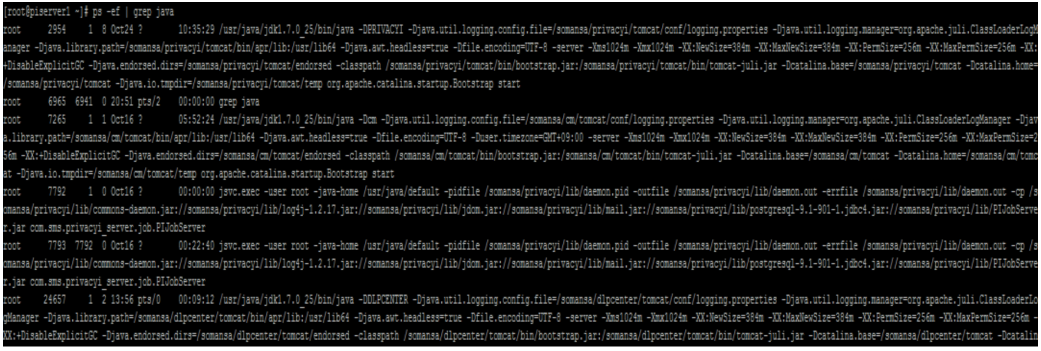


(FIGURE 3-20) DLP+ CENTER – SERVER CONTROL

✓ Method of checking the service again at system console after running all services

It is possible to check on the information of Demon process in which following components (Privacy-I Server, DLP+Center, Configuration Manager, Job Server, Privacy-I Agent Update Server) are executed.

# ps –ef | grep java

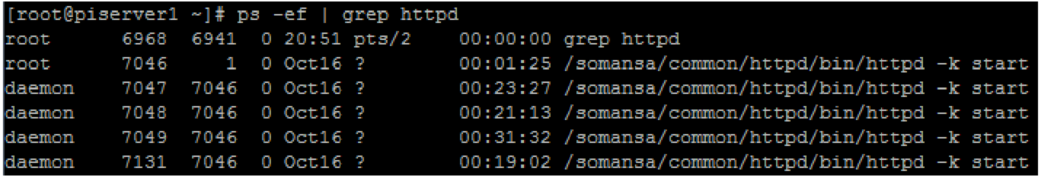


```
[root@piserver1 ~]# ps -ef | grep java
root      2954     1  8 Oct24 ?        10:35:29 /usr/java/jdk1.7.0_25/bin/java -DPRIVACYI -Djava.util.logging.config.file=/somansa/privacyi/tomcat/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogM
anager -Djava.library.path=/somansa/privacyi/tomcat/bin/apr/lib:/usr/lib64 -Djava.awt.headless=true -Dfile.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:NewSize=384m -XX:MaxNewSize=384m -XX:PermSize=256m -XX:MaxPermSize=256m -XX:
+DisableExplicitGC -Djava.endorsed.dirs=/somansa/privacyi/tomcat/endorsed -classpath /somansa/privacyi/tomcat/bin/bootstrap.jar:/somansa/privacyi/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/somansa/privacyi/tomcat -Dcatalina.home=
/somansa/privacyi/tomcat -Djava.io.tmpdir=/somansa/privacyi/tomcat/temp org.apache.catalina.startup.Bootstrap start
root      6965  6941  0 20:51 pts/2    00:00:00 grep java
root      7265     1  1 Oct16 ?        05:52:24 /usr/java/jdk1.7.0_25/bin/java -Dcm -Djava.util.logging.config.file=/somansa/cm/tomcat/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djav
a.library.path=/somansa/cm/tomcat/bin/apr/lib:/usr/lib64 -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Duser.timezone=GMT+09:00 -server -Xms1024m -Xmx1024m -XX:NewSize=384m -XX:MaxNewSize=384m -XX:PermSize=256m -XX:MaxPermSize=2
56m -XX:+DisableExplicitGC -Djava.endorsed.dirs=/somansa/cm/tomcat/endorsed -classpath /somansa/cm/tomcat/bin/bootstrap.jar:/somansa/cm/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/somansa/cm/tomcat -Dcatalina.home=/somansa/cm/tomc
at -Djava.io.tmpdir=/somansa/cm/tomcat/temp org.apache.catalina.startup.Bootstrap start
root      7792     1  0 Oct16 ?        00:00:00 jsvc.exec -user root -java-home /usr/java/default -pidfile /somansa/privacyi/lib/daemon.pid -outfile /somansa/privacyi/lib/daemon.out -errfile /somansa/privacyi/lib/daemon.out -cp /s
omansa/privacyi/lib/commons-daemon.jar://somansa/privacyi/lib/log4j-1.2.17.jar://somansa/privacyi/lib/jdom.jar://somansa/privacyi/lib/mail.jar://somansa/privacyi/lib/postgresql-9.1-901-1.jdbc4.jar://somansa/privacyi/lib/PIJobServe
r.jar com.sms.privacyi_server.job.PIJobServer
root      7793  7792  0 Oct16 ?        00:22:40 jsvc.exec -user root -java-home /usr/java/default -pidfile /somansa/privacyi/lib/daemon.pid -outfile /somansa/privacyi/lib/daemon.out -errfile /somansa/privacyi/lib/daemon.out -cp /s
omansa/privacyi/lib/commons-daemon.jar://somansa/privacyi/lib/log4j-1.2.17.jar://somansa/privacyi/lib/jdom.jar://somansa/privacyi/lib/mail.jar://somansa/privacyi/lib/postgresql-9.1-901-1.jdbc4.jar://somansa/privacyi/lib/PIJobServe
r.jar com.sms.privacyi_server.job.PIJobServer
root     24657     1  2 13:56 pts/0    00:09:12 /usr/java/jdk1.7.0_25/bin/java -DDLPCENTER -Djava.util.logging.config.file=/somansa/dlpcenter/tomcat/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLo
gManager -Djava.library.path=/somansa/dlpcenter/tomcat/bin/apr/lib:/usr/lib64 -Djava.awt.headless=true -Dfile.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:NewSize=384m -XX:MaxNewSize=384m -XX:PermSize=256m -XX:MaxPermSize=256m -
XX:+DisableExplicitGC -Djava.endorsed.dirs=/somansa/dlpcenter/tomcat/endorsed -classpath /somansa/dlpcenter/tomcat/bin/bootstrap.jar:/somansa/dlpcenter/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/somansa/dlpcenter/tomcat -Dcatalin
```

(FIGURE 3-21) JAVA SERWICE CHECK SCREEN

The state of Apache server can be checked for the components to communicate with outside as shown in the Figure below.

# ps –ef | grep httpd (Check Apache server)



```
[root@piserver1 ~]# ps -ef | grep httpd
root      6968  6941  0 20:51 pts/2    00:00:00 grep httpd
root      7046     1  0 Oct16 ?        00:01:25 /somansa/common/httpd/bin/httpd -k start
daemon    7047  7046  0 Oct16 ?        00:23:27 /somansa/common/httpd/bin/httpd -k start
daemon    7048  7046  0 Oct16 ?        00:21:13 /somansa/common/httpd/bin/httpd -k start
daemon    7049  7046  0 Oct16 ?        00:31:32 /somansa/common/httpd/bin/httpd -k start
daemon    7131  7046  0 Oct16 ?        00:19:02 /somansa/common/httpd/bin/httpd -k start
```

(FIGURE 3-22) APACHE SERVICE CHECKING SCREEN

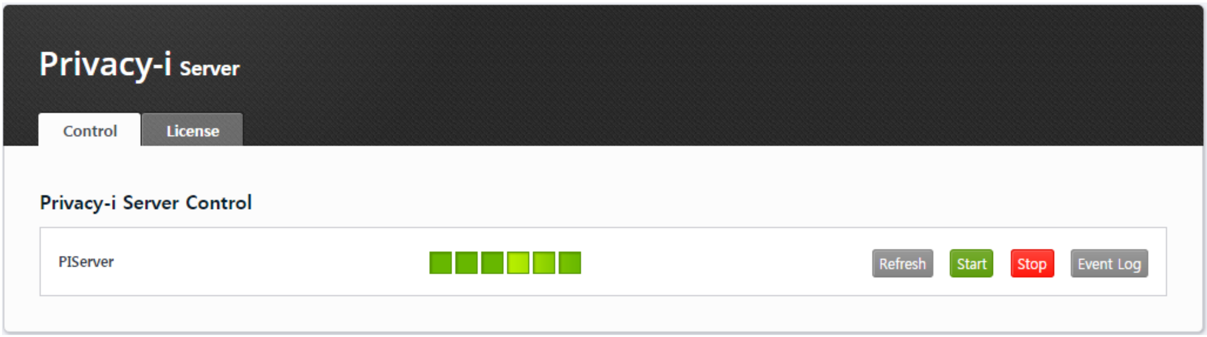
3.6 Privacy-i Settings

Privacy-i server management, and license are provided.

3.6.1 Privacy-i Server

3.6.1.1 Server Management

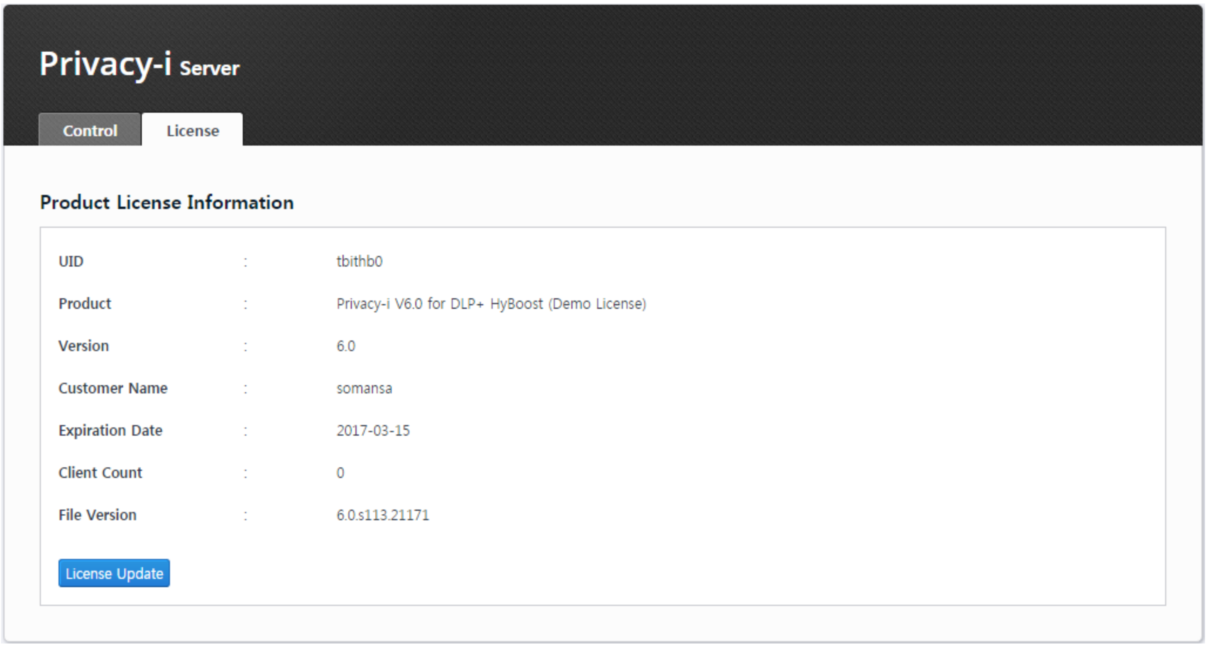
The status of the Privacy-i Server and its operation can be set. As shown in the Figure below, Restart, Start and Stop functions for the Privacy-i Server are provided.



(FIGURE 3-23) PRIVACY-I SERVER CONTROL

3.6.1.2 License

UID / License expiration date / number of users, etc. are displayed (see Receive License Issuance). Place the License received from the SOMANSA 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	:	tbithb0
Product	:	Privacy-i V6.0 for DLP+ HyBoost (Demo License)
Version	:	6.0
Customer Name	:	somansa
Expiration Date	:	2017-03-15
Client Count	:	0
File Version	:	6.0.s113.21171

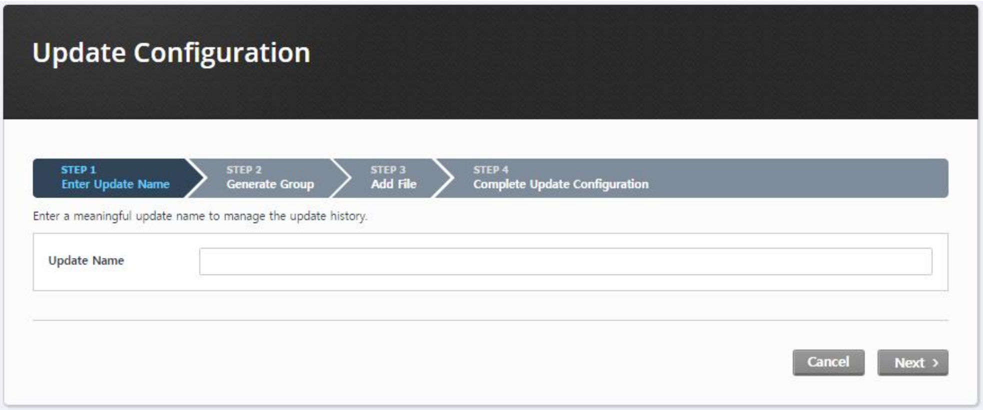
(FIGURE 3-24) PRIVACY-I LICENSE SCREEN

3.6.2 Privacy-i Agent Update

3.6.2.1 Agent Update Configuration

Step 1. Enter update name

Name of the update to be proceeded should be input. (Ex: Regular release, 3 Q, 2014)



Update Configuration

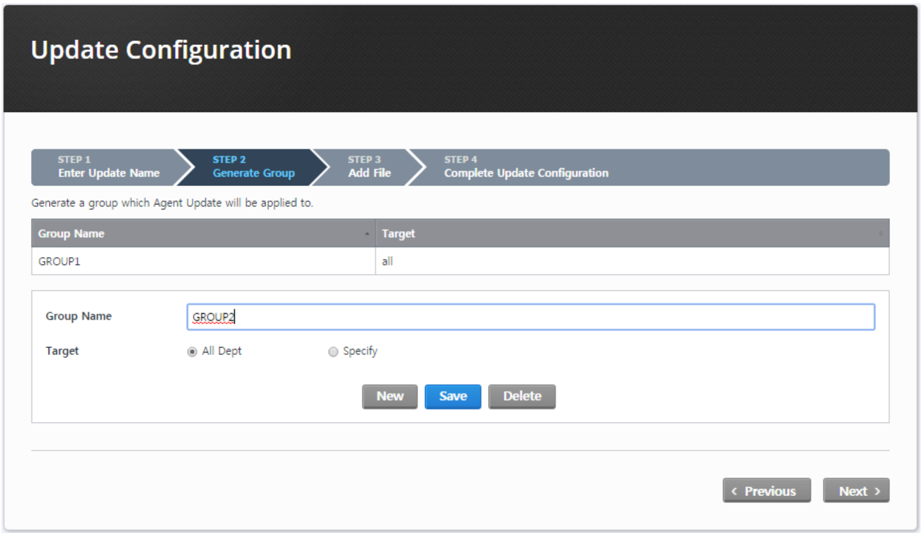
Enter a meaningful update name to manage the update history.

Update Name

(FIGURE 3-25) UPDATE NAME ENTER SCREEN

Step 2. Generate Group

Generate an update group. One or more group(s) must be specified, and can be categorized according to the characteristics of the module. In addition, the target to be applied to the group can be specified as a whole or selectively based on HR information.



Update Configuration

Generate a group which Agent Update will be applied to.

Group Name	Target
GROUP1	all

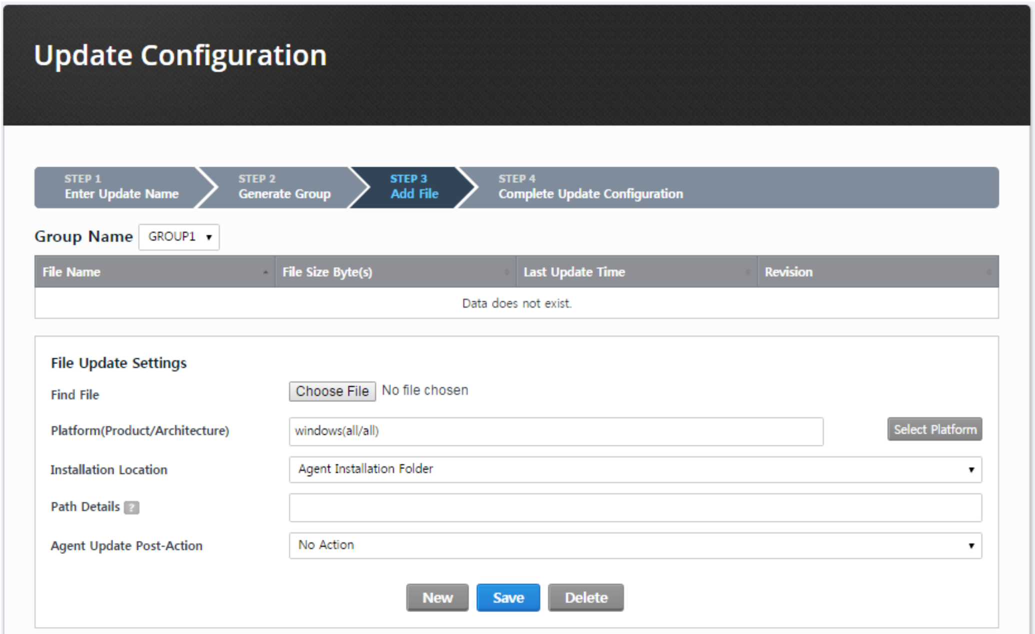
Group Name: GROUP2

Target: ● All Dept ○ Specify

(FIGURE 3-26) GROUP CREATING SCREEN

Step 3. Add files

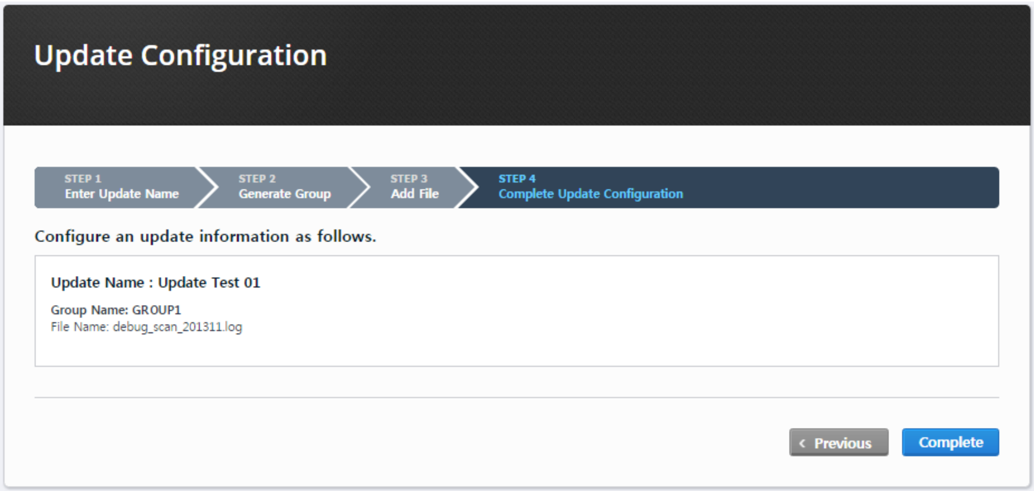
Add a file to update. On a platform, OS type and architecture name (x86. x64) can be selected. Installation location can be selected to the Privacy-i Agent installation folder, Privacy-i Data folder, Windows folder and System32 folder; and a specific path can be entered. (Omit ‘/’ before and after the entered path) 'No Action', 'Create Service', 'Run', 'Register Registry' and 'Restart Privacy-i Agent' can be selected for the following action.



(FIGURE 3-27) FILE ADD SCREEN

Step 4 Complete update configuration

Configured update information can be checked.



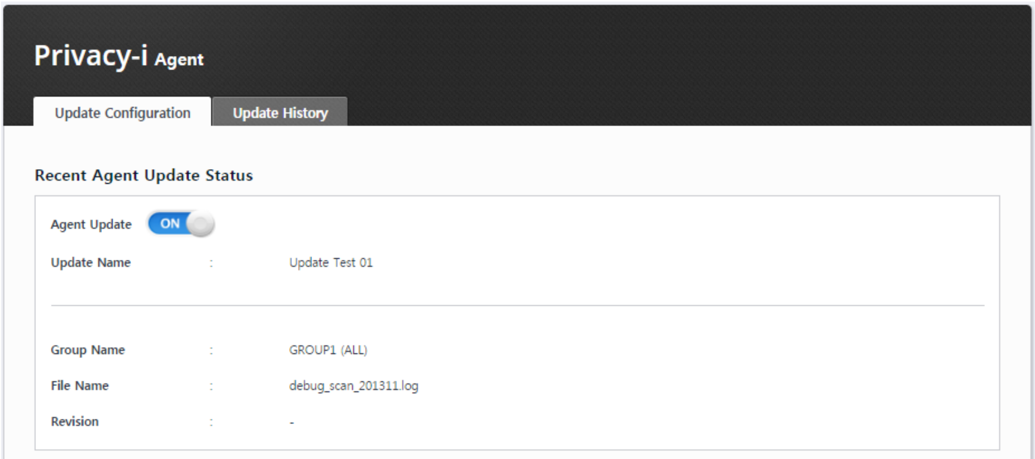
Configure an update information as follows.

Update Name : Update Test 01

Group Name: GROUP1
File Name: debug_scan_201311.log

(FIGURE 3-28) COMPLETED UPDATE CONFIGURATION SCREEN

When update configuration is complete, the updated information is saved as an xml file. When existing xml or xml to be configured needs to be checked for the xml file saved, it can be compared using the 'Diff' button.



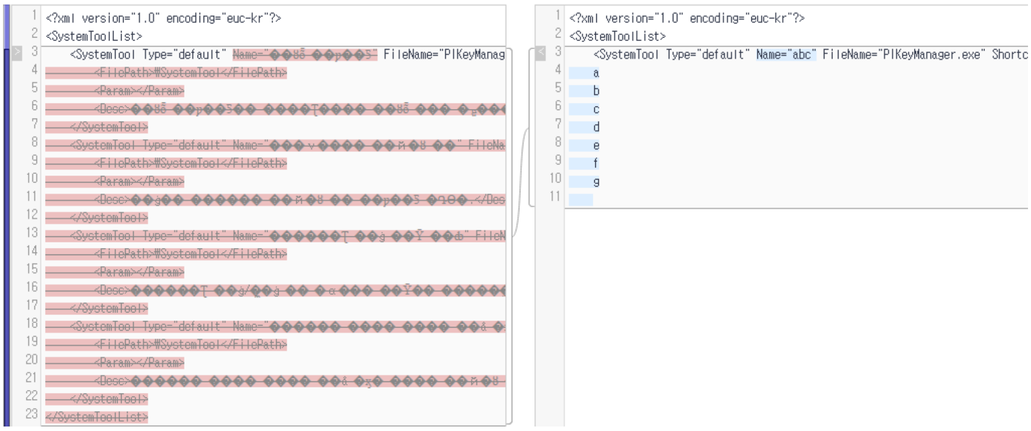
Privacy-i Agent

Recent Agent Update Status

Agent Update ON

Update Name	:	Update Test 01
Group Name	:	GROUP1 (ALL)
File Name	:	debug_scan_201311.log
Revision	:	-

(FIGURE 3-29) DIFF BUTTON



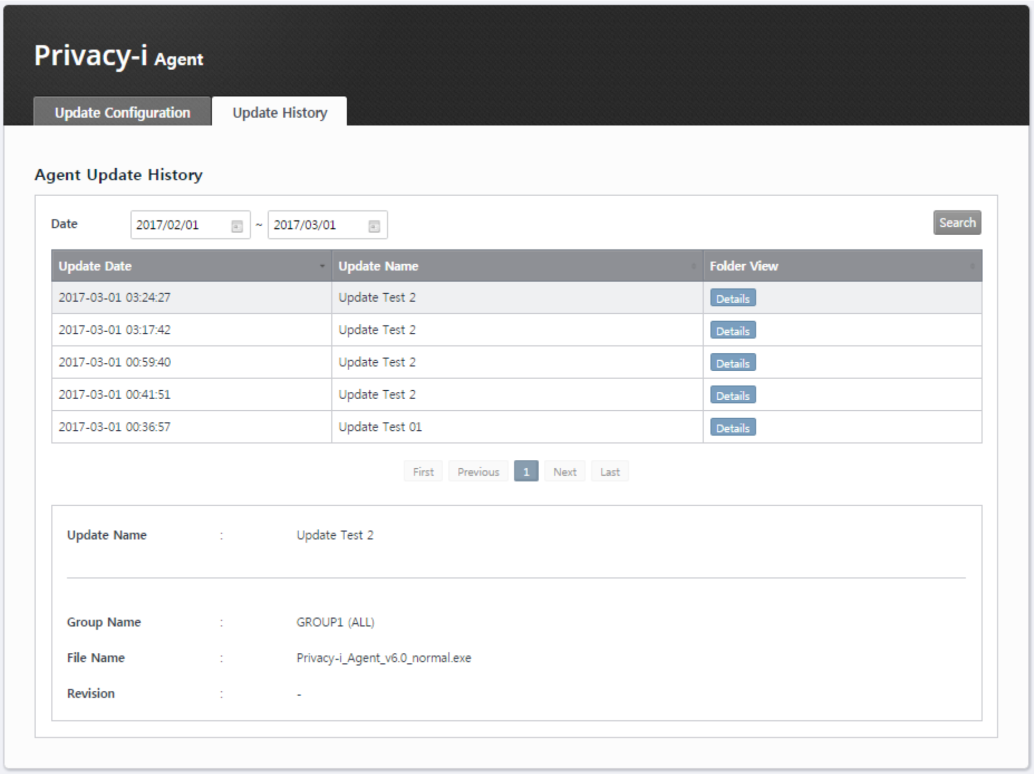
```
<?xml version="1.0" encoding="euc-kr"?>
<SystemToolList>
    <SystemTool Type="default" Name="��ué ��p��5" FileName="PIKeyManag
        <FilePath>#SystemTool</FilePath>
        <Param></Param>
        <Desc>��ué ��p��5�� ����T���� ��ué ��� �g��
    </SystemTool>
    <SystemTool Type="default" Name="��� v���� ��ň�ö ��" FileNa
        <FilePath>#SystemTool</FilePath>
        <Param></Param>
        <Desc>��ġ�� ������ ��ň�ö �� ��p��5 �ᄀ��.</Des
    </SystemTool>
    <SystemTool Type="default" Name="������T ��ġ ��Ÿ ��ф" FileN
        <FilePath>#SystemTool</FilePath>
        <Param></Param>
        <Desc>������T ��ġ/��ġ �� �α��� ��Ÿ�� �����
    </SystemTool>
    <SystemTool Type="default" Name="������ ���� ���� ��å �
        <FilePath>#SystemTool</FilePath>
        <Param></Param>
        <Desc>������ ���� ���� ��å �x� ���� ��ň�ö
    </SystemTool>
</SystemToolList>
```

```
<?xml version="1.0" encoding="euc-kr"?>
<SystemToolList>
    <SystemTool Type="default" Name="abc" FileName="PIKeyManager.exe" Shortc
    a
    b
    c
    d
    e
    f
    g
```

(FIGURE 3-30) XML CONTENT COMPARISON SCREEN

3.6.2.2 View Agent Update History

History of agent update can be viewed.



Agent Update History

Date 2017/02/01 ~ 2017/03/01 Search

Update Date	Update Name	Folder View
2017-03-01 03:24:27	Update Test 2	Details
2017-03-01 03:17:42	Update Test 2	Details
2017-03-01 00:59:40	Update Test 2	Details
2017-03-01 00:41:51	Update Test 2	Details
2017-03-01 00:36:57	Update Test 01	Details

First Previous 1 Next Last

Update Name	:	Update Test 2
Group Name	:	GROUP1 (ALL)
File Name	:	Privacy-i_Agent_v6.0_normal.exe
Revision	:	-

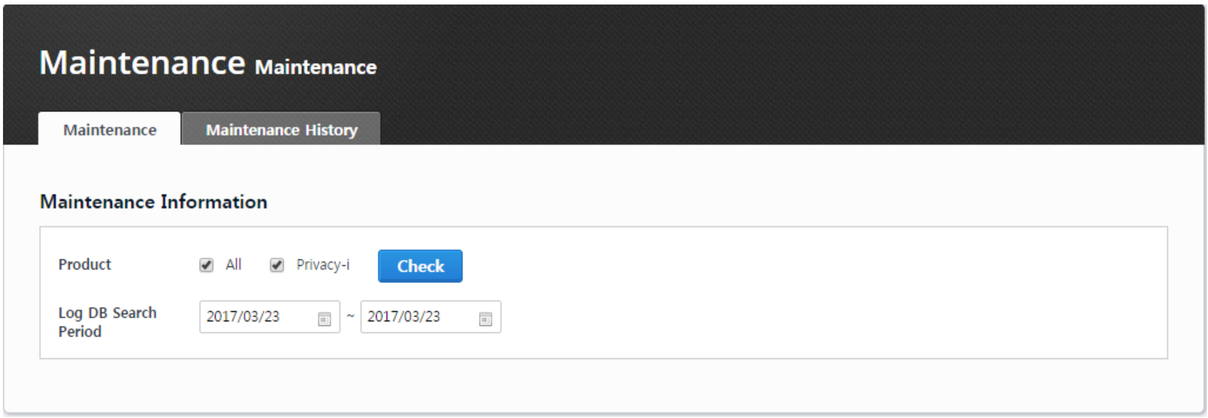
(FIGURE 3-31) VIEW AGENT UPDATE HISTORY SCREEN

3.7 Maintenance

3.7.1 Check Report

3.7.1.1 Check Report

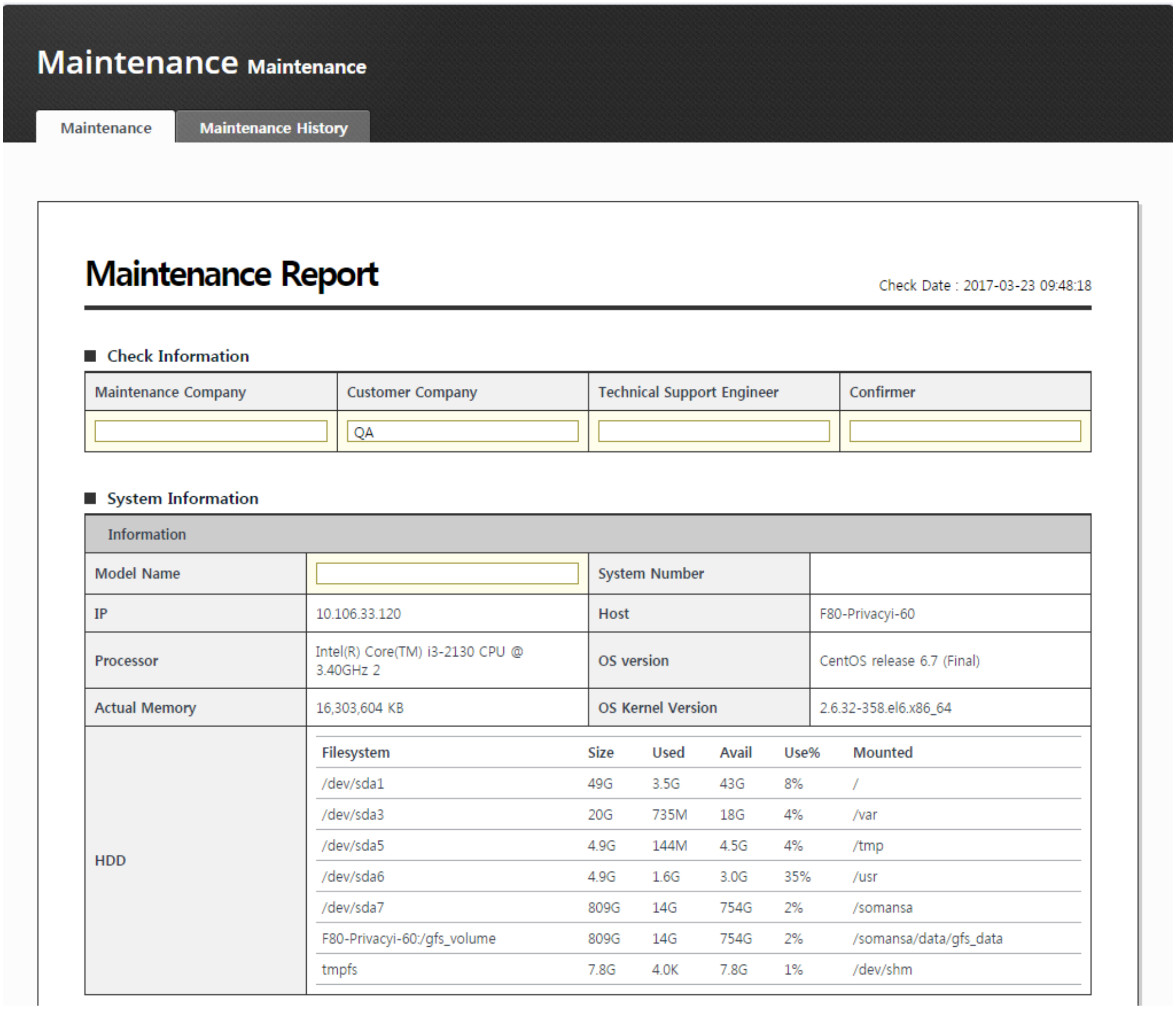
The current status of Privacy-i V6.0 system can be checked by using a Check Report tool. Select the product to be checked with Privacy-i, and then set the period for viewing log DB and click the check button to output the results of regular inspections as shown below.



Product ☑ All ☑ Privacy-i

Log DB Search Period 2017/03/23 ~ 2017/03/23

(FIGURE 3-32) CHECK REPORT SCREEN



Maintenance Report

Check Date : 2017-03-23 09:48:18

■ Check Information

Maintenance Company	Customer Company	Technical Support Engineer	Confirmer
	QA		

■ System Information

Information			
Model Name		System Number	
IP	10.106.33.120	Host	F80-Privacyi-60
Processor	Intel(R) Core(TM) i3-2130 CPU @ 3.40GHz 2	OS version	CentOS release 6.7 (Final)
Actual Memory	16,303,604 KB	OS Kernel Version	2.6.32-358.el6.x86_64

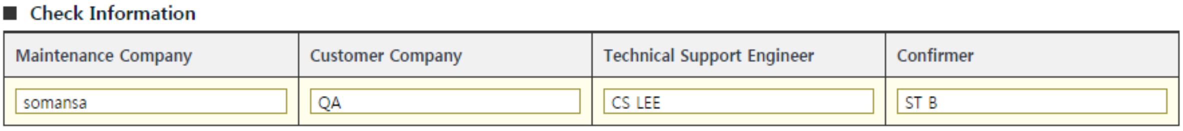
HDD

Filesystem	Size	Used	Avail	Use%	Mounted
/dev/sda1	49G	3.5G	43G	8%	/
/dev/sda3	20G	735M	18G	4%	/var
/dev/sda5	4.9G	144M	4.5G	4%	/tmp
/dev/sda6	4.9G	1.6G	3.0G	35%	/usr
/dev/sda7	809G	14G	754G	2%	/somansa
F80-Privacyi-60:/gfs_volume	809G	14G	754G	2%	/somansa/data/gfs_data
tmpfs	7.8G	4.0K	7.8G	1%	/dev/shm

(FIGURE 3-33) FULL SCREEN OF INSPECTION RESULTS

- ➢ Inspection information

  Information on related companies, client companies, inspectors, confirming persons is input manually.



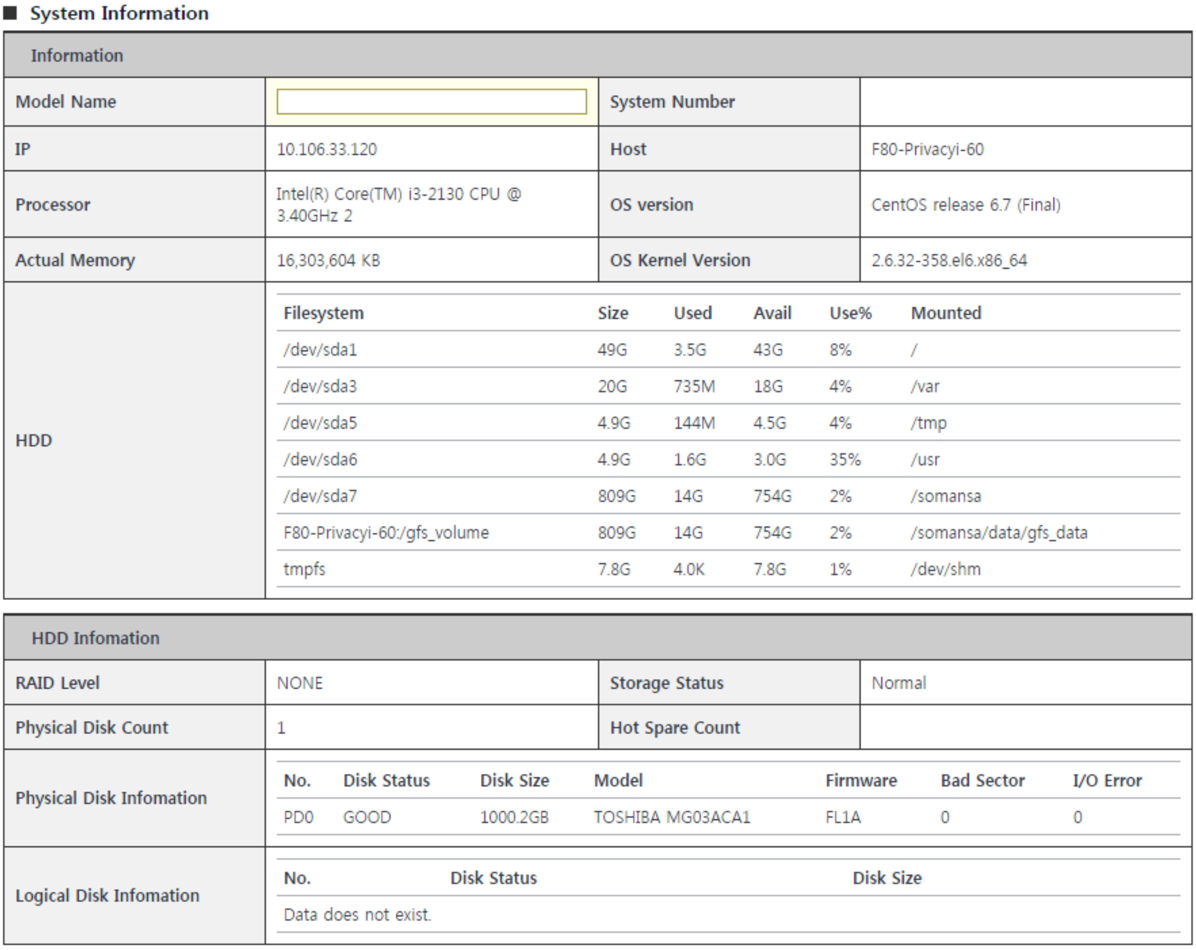
■ Check Information

Maintenance Company	Customer Company	Technical Support Engineer	Confirmer
somansa	QA	CS LEE	ST B

(FIGURE 3-34) INSPECTION INFORMATION SCREEN

- ➢ System information

  Model names are input manually. IP, host, processor, OS version, HDD, OS kernel version, DB version, and actual memory information are automatically imported.



■ System Information

Information			
Model Name		System Number	
IP	10.106.33.120	Host	F80-Privacyi-60
Processor	Intel(R) Core(TM) i3-2130 CPU @ 3.40GHz 2	OS version	CentOS release 6.7 (Final)
Actual Memory	16,303,604 KB	OS Kernel Version	2.6.32-358.el6.x86_64

HDD

Filesystem	Size	Used	Avail	Use%	Mounted
/dev/sda1	49G	3.5G	43G	8%	/
/dev/sda3	20G	735M	18G	4%	/var
/dev/sda5	4.9G	144M	4.5G	4%	/tmp
/dev/sda6	4.9G	1.6G	3.0G	35%	/usr
/dev/sda7	809G	14G	754G	2%	/somansa
F80-Privacyi-60:/gfs_volume	809G	14G	754G	2%	/somansa/data/gfs_data
tmpfs	7.8G	4.0K	7.8G	1%	/dev/shm

HDD Infomation			
RAID Level	NONE	Storage Status	Normal
Physical Disk Count	1	Hot Spare Count	

Physical Disk Infomation

No.	Disk Status	Disk Size	Model	Firmware	Bad Sector	I/O Error
PD0	GOOD	1000.2GB	TOSHIBA MG03ACA1	FL1A	0	0

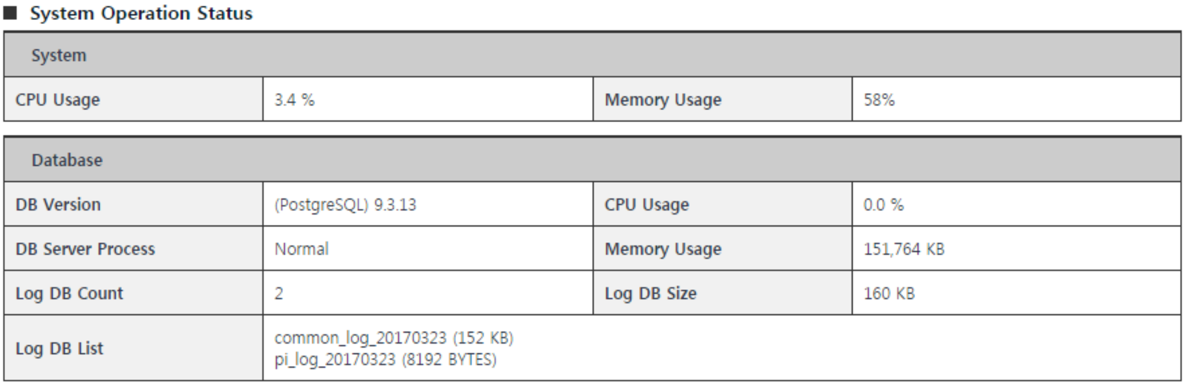
Logical Disk Infomation

No.	Disk Status	Disk Size
Data does not exist.		

(FIGURE 3-35) SYSTEM INFORMATION SCREEN

- ➢ System operation status

CPU use and memory use of the system, CPU use and memory use of database, DBServer process state, and DBAgent process state information can be viewed.



■ System Operation Status

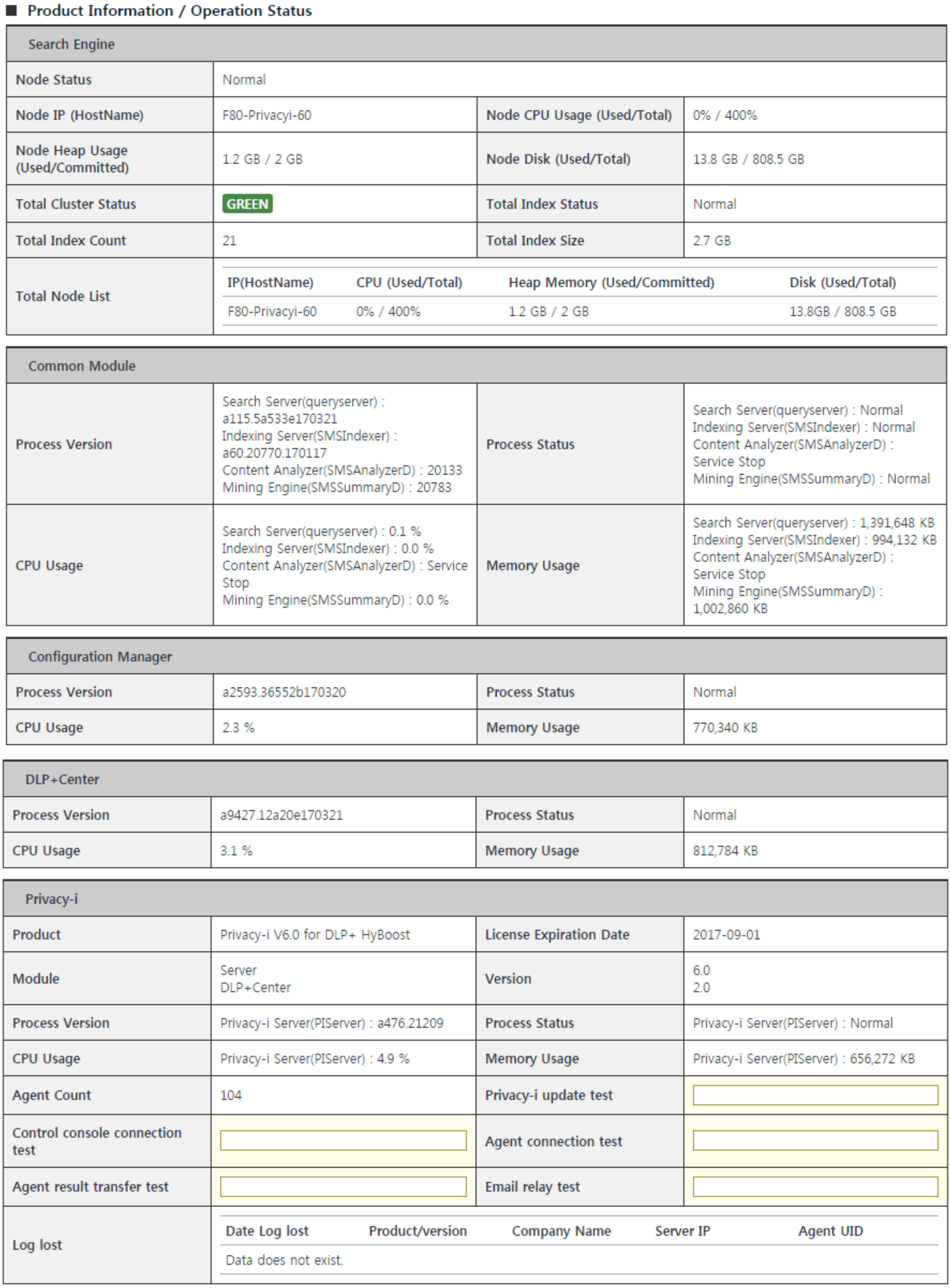
System			
CPU Usage	3.4 %	Memory Usage	58%

Database			
DB Version	(PostgreSQL) 9.3.13	CPU Usage	0.0 %
DB Server Process	Normal	Memory Usage	151,764 KB
Log DB Count	2	Log DB Size	160 KB
Log DB List	common_log_20170323 (152 KB) pi_log_20170323 (8192 BYTES)		

(FIGURE 3-36) SYSTEM OPERATION STATUS SCREEN

- Product information / Operation status

  Process version, process operation, CPU usage, memory usage, spare space of disks, average size of log DB, maximum size of log DB, data input time, data view time, the number of log DBs, log DB list information are automatically shown.



■ Product Information / Operation Status

Search Engine			
Node Status	Normal		
Node IP (HostName)	F80-Privacyi-60	Node CPU Usage (Used/Total)	0% / 400%
Node Heap Usage (Used/Committed)	1.2 GB / 2 GB	Node Disk (Used/Total)	13.8 GB / 808.5 GB
Total Cluster Status	GREEN	Total Index Status	Normal
Total Index Count	21	Total Index Size	2.7 GB
Total Node List			

IP(HostName)	CPU (Used/Total)	Heap Memory (Used/Committed)	Disk (Used/Total)
F80-Privacyi-60	0% / 400%	1.2 GB / 2 GB	13.8GB / 808.5 GB

Common Module			
Process Version	Search Server(queryserver) : a115.5a533e170321 Indexing Server(SMSIndexer) : a60.20770.170117 Content Analyzer(SMSAnalyzerD) : 20133 Mining Engine(SMSSummaryD) : 20783	Process Status	Search Server(queryserver) : Normal Indexing Server(SMSIndexer) : Normal Content Analyzer(SMSAnalyzerD) : Service Stop Mining Engine(SMSSummaryD) : Normal
CPU Usage	Search Server(queryserver) : 0.1 % Indexing Server(SMSIndexer) : 0.0 % Content Analyzer(SMSAnalyzerD) : Service Stop Mining Engine(SMSSummaryD) : 0.0 %	Memory Usage	Search Server(queryserver) : 1,391,648 KB Indexing Server(SMSIndexer) : 994,132 KB Content Analyzer(SMSAnalyzerD) : Service Stop Mining Engine(SMSSummaryD) : 1,002,860 KB

Configuration Manager			
Process Version	a2593.36552b170320	Process Status	Normal
CPU Usage	2.3 %	Memory Usage	770,340 KB

DLP+Center			
Process Version	a9427.12a20e170321	Process Status	Normal
CPU Usage	3.1 %	Memory Usage	812,784 KB

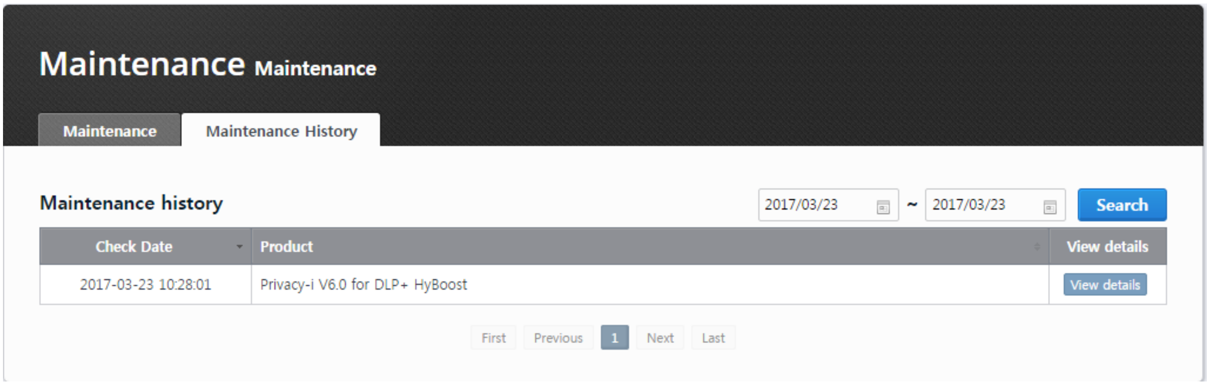
Privacy-i			
Product	Privacy-i V6.0 for DLP+ HyBoost	License Expiration Date	2017-09-01
Module	Server DLP+Center	Version	6.0 2.0
Process Version	Privacy-i Server(PIServer) : a476.21209	Process Status	Privacy-i Server(PIServer) : Normal
CPU Usage	Privacy-i Server(PIServer) : 4.9 %	Memory Usage	Privacy-i Server(PIServer) : 656,272 KB
Agent Count	104	Privacy-i update test	
Control console connection test		Agent connection test	
Agent result transfer test		Email relay test	
Log lost			

Date Log lost	Product/version	Company Name	Server IP	Agent UID
Data does not exist.				

(FIGURE 3-37) PRODUCT DEVICES / OPERATION STATUS SCREEN

3.7.1.2 View Check History

The history of inspections can be viewed through 'View Check History' for each period. Reports can be checked by clicking 'View Details'.



Maintenance history

2017/03/23 ~ 2017/03/23

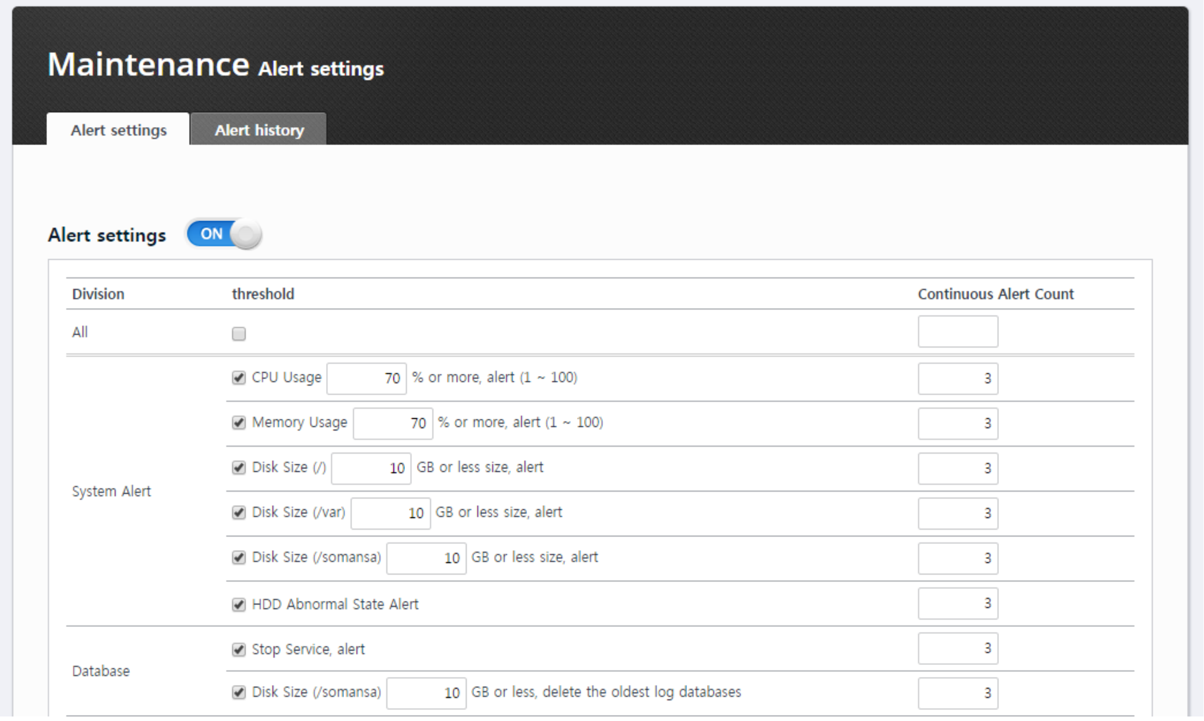
Check Date	Product	View details
2017-03-23 10:28:01	Privacy-i V6.0 for DLP+ HyBoost	View details

(FIGURE 3-38) VIEW INSPECTION HISTORY SCREEN

3.7.2 System Alerts Settings

3.7.2.1 Alerts Settings

Alerts settings intend to check and protect disks. When the space of disks saving the logs of sensitive contents is generated, mail is sent according to the information configured as in (Figure 3-40). Disk check sends the mail notifying insufficient disk space to the security administrator. Disk protection deletes the oldest logs of sensitive contents when the capacity of the configured disk becomes smaller than the reference value (Default: 512MB), and sends the deleted information to the security administrator. Alerts settings are operated through system scheduling functions, and disk check is made for every one hour and disk protection for every 10 minutes.



Maintenance Alert settings

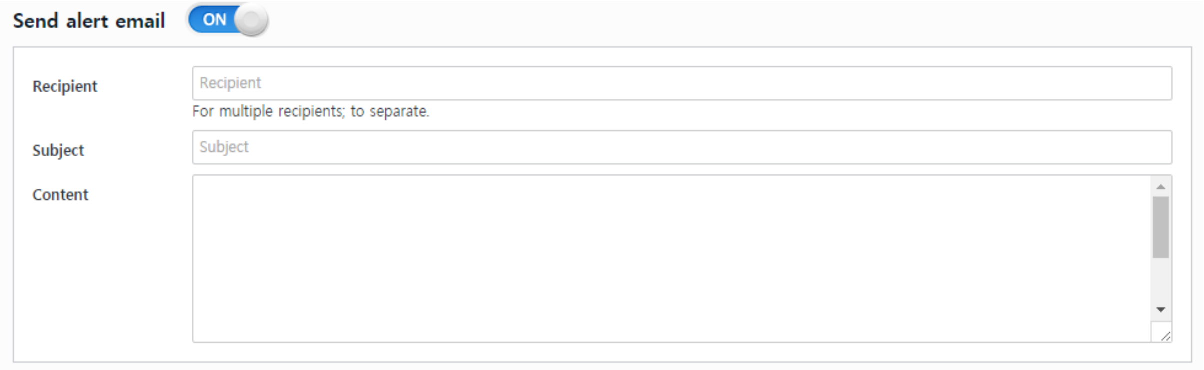
Alert settings | Alert history

Alert settings ON

Division	threshold	Continuous Alert Count
All	☐	
System Alert	☑ CPU Usage 70 % or more, alert (1 ~ 100)	3
	☑ Memory Usage 70 % or more, alert (1 ~ 100)	3
	☑ Disk Size (/) 10 GB or less size, alert	3
	☑ Disk Size (/var) 10 GB or less size, alert	3
	☑ Disk Size (/somansa) 10 GB or less size, alert	3
	☑ HDD Abnormal State Alert	3
Database	☑ Stop Service, alert	3
	☑ Disk Size (/somansa) 10 GB or less, delete the oldest log databases	3

(FIGURE 3-39) EXAMPLE OF WARNING SETTINGS SCREEN

3.7.2.2 Alerts Mail Settings



Send alert email ON

Recipient: Recipient
For multiple recipients; to separate.

Subject: Subject

Content:

(FIGURE 3-40) EXAMPLE OF WARNING MAIL SETTINGS SCREEN

☞ Effective Input Field Range

[TABLE 3-7] Effective Input Field Range for Alerts Settings

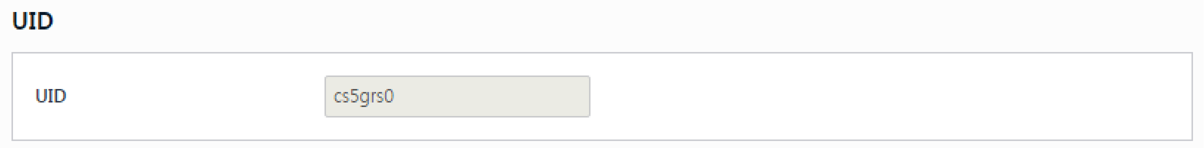
Item	Effective range	Character	Failure message
Size of database disk (Warning mail)	1~102400	Numbers	-.
Size of database disk (Delete)	1~51200	Numbers	-
Receiver (Warning mail, delete)	1~50	Numbers, letters, special characters	Enter the receiver.
Title of mail (Warning mail, delete)	1~100	Numbers, letters, special characters	-

Contents of mail (Warning 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, upper and lower case letters, special characters	Enter password.
Sender	1~50	Numbers, letters, special characters	Enter the sender.

3.8 Environmental Settings

3.8.1 UID

UID information of the server can be checked for issuing license.



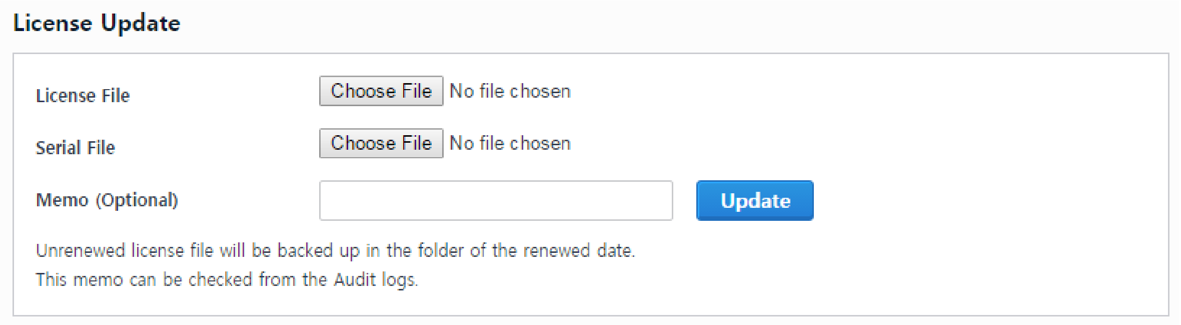
UID

UID: cs5grs0

(FIGURE 3-41) UID

3.8.2 License Update

Generated license can be updated through Control Panel.



License Update

License File: Choose File No file chosen

Serial File: Choose File No file chosen

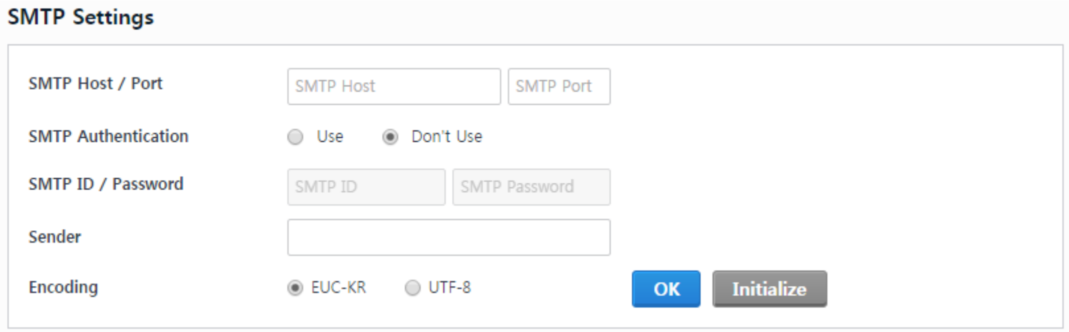
Memo (Optional):

Unrenewed license file will be backed up in the folder of the renewed date.
This memo can be checked from the Audit logs.

(FIGURE 3-42) LICENSE UPDATE

3.8.3 SMTP Settings

The log information can be sent by email at DLP+Center through SMTP settings.



SMTP Settings

SMTP Host / Port: SMTP Host | SMTP Port

SMTP Authentication: ○ Use ● Don't Use

SMTP ID / Password: SMTP ID | SMTP Password

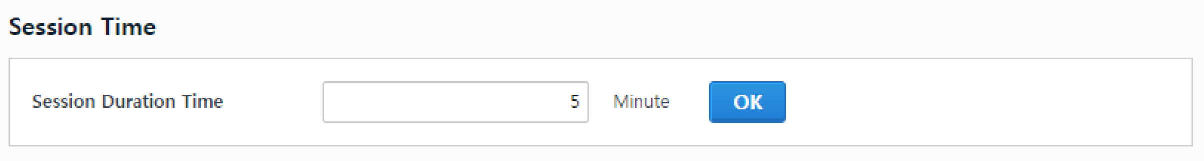
Sender:

Encoding: ● EUC-KR ○ UTF-8

(FIGURE 3-43) SMTP SETTINGS

3.8.4 Session Time Settings

Set the Session Duration of the Configuration Manager.



Session Time

Session Duration Time: 5 Minute

(FIGURE 3-44) SESSION TIME SETTINGS

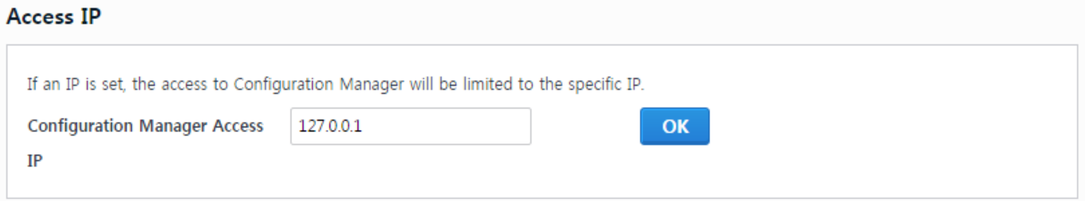
☞ Effective Input Field Range

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

Item	Effective range	Character	Failure message
Session duration	1~10	Numbers	Enter session duration.

3.8.5 Connection IP Settings

When IP is set, connection to Control Panel is limited from only the IP.



Access IP

If an IP is set, the access to Configuration Manager will be limited to the specific IP.

Configuration Manager Access IP: 127.0.0.1

(FIGURE 3-45) CONNECTION IP SETTINGS

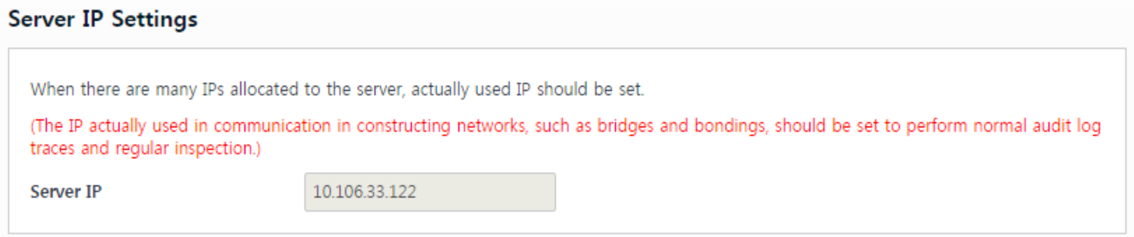
Effective Input Field Range

[TABLE 3-9] EFFECTIVE INPUT FIELD RANGE FOR CONNECTION IP SETTINGS

Item	Effective range	Character	Failure message
Control panel connection IP	15	Numbers, special character (.)	Input control panel connection IP.

3.8.6 Server IP Settings

When multiple IPs are allocated to a server, the IP actually used is configured.



Server IP Settings

When there are many IPs allocated to the server, actually used IP should be set.

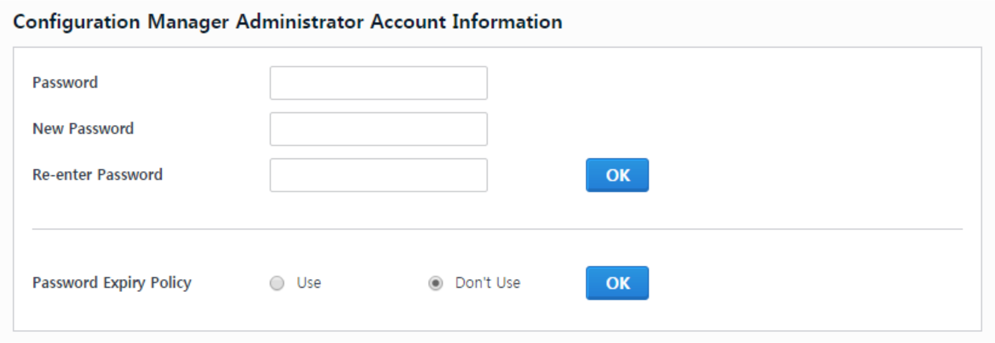
(The IP actually used in communication in constructing networks, such as bridges and bondings, should be set to perform normal audit log traces and regular inspection.)

Server IP: 10.106.33.122

(FIGURE 3-46) SERVER IP SETTINGS

3.8.7 Control Panel Administrator Account Information

Password of the administrator of Control Panel 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	

Password Expiry Policy ○ Use ● Don't Use

(FIGURE 3-47) CONTROL PANEL ADMINISTRATOR ACCOUNT INFORMATION

☞ Effective Input Field Range

[TABLE 3-10] ACCOUNT INFORMATION EFFECTIVE INPUT FIELD RANGE FOR 3.8.7 CONTROL PANEL ADMINISTRATOR

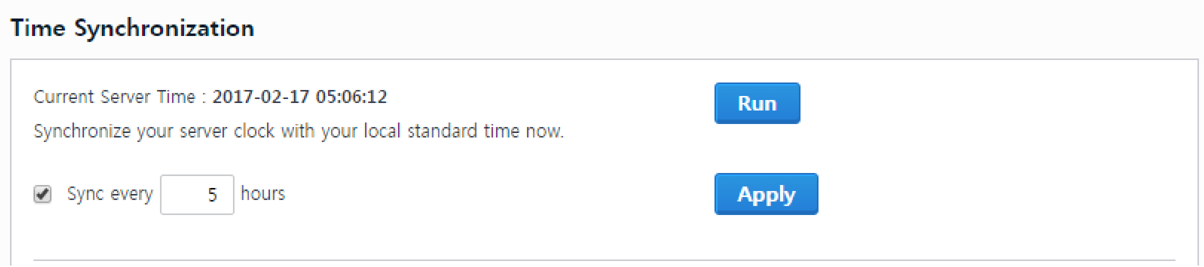
Item	Effective range	Character	Failure message
Current password	9~12	Numbers, upper or lower case letters, special characters	Enter the current password of Admin account.
New password	9~12	Numbers, upper or lower case letters, special characters	Enter the new password of the Admin account.
Confirm password	9~12	Numbers, upper or lower case letters, special characters	Enter the new password of the Admin account once again.

Recommendations

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

3.8.8 Time Synchronization

The time between product modules are synchronized as the standard time with reference to NTP server.



Time Synchronization

Current Server Time : 2017-02-17 05:06:12

Synchronize your server clock with your local standard time now.

☑ Sync every 5 hours

(FIGURE 3-48) TIME SYNCHRONIZATION

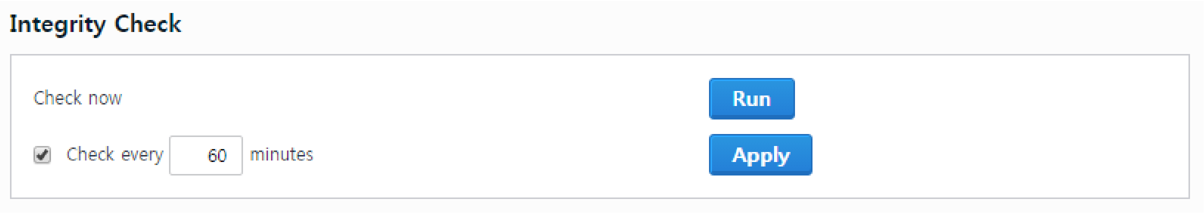
☞ Effective Input Field Range

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

Item	Effective range	Character	Failure message
Synchronization period	1~99	Numbers	Enter synchronization period.

3.8.9 Integrity Function 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" button. This function is not activated by default, but can be used after checking 'Integrity Check Period'.



Integrity Check

Check now

☑ Check every 60 minutes

(FIGURE 3-49) INTEGRITY FUNCTION CHECK

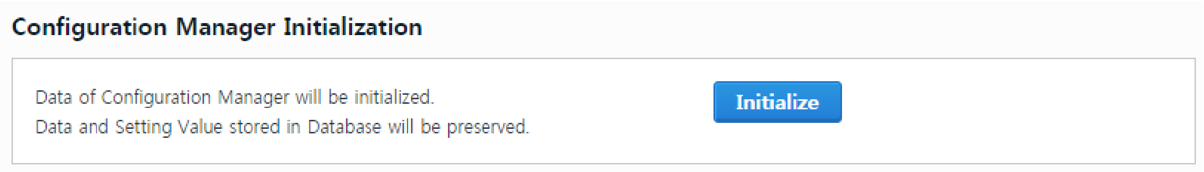
☞ Effective Input Field Range

[TABLE 3-12] EFFECTIVE INPUT FIELD RANGE FOR SETTING INTEGRITY FUNCTIONS

Item	Effective range	Character	Failure message
Integrity period	99	Numbers	Enter period of performing integrity function.

3.8.10 Reset Control Panel

Control panel settings are reset. Product settings information is reset and the system is restored to the state after installation. The data and settings values saved in database are preserved.



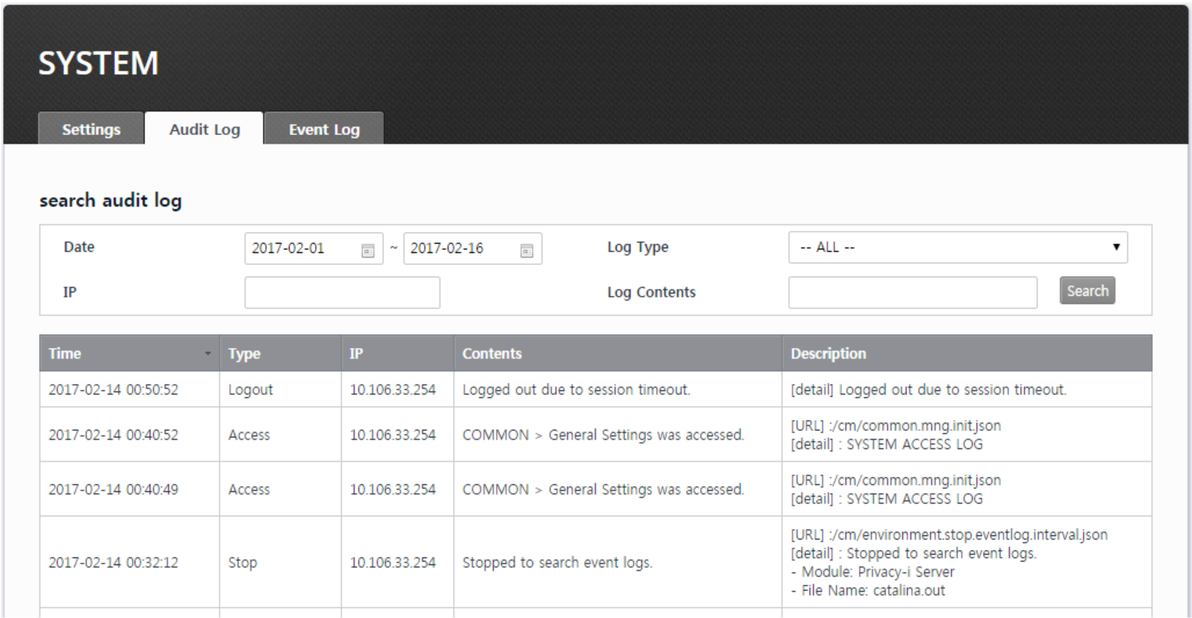
Configuration Manager Initialization

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

(FIGURE 3-50) RESET CONTROL PANEL

3.9 SYSTEM Audit Logs

This screen shows audit logs of the system for checking. 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 period. The audit logs are displayed by categorizing Date, Type, IP, Contents and Description.



search audit log

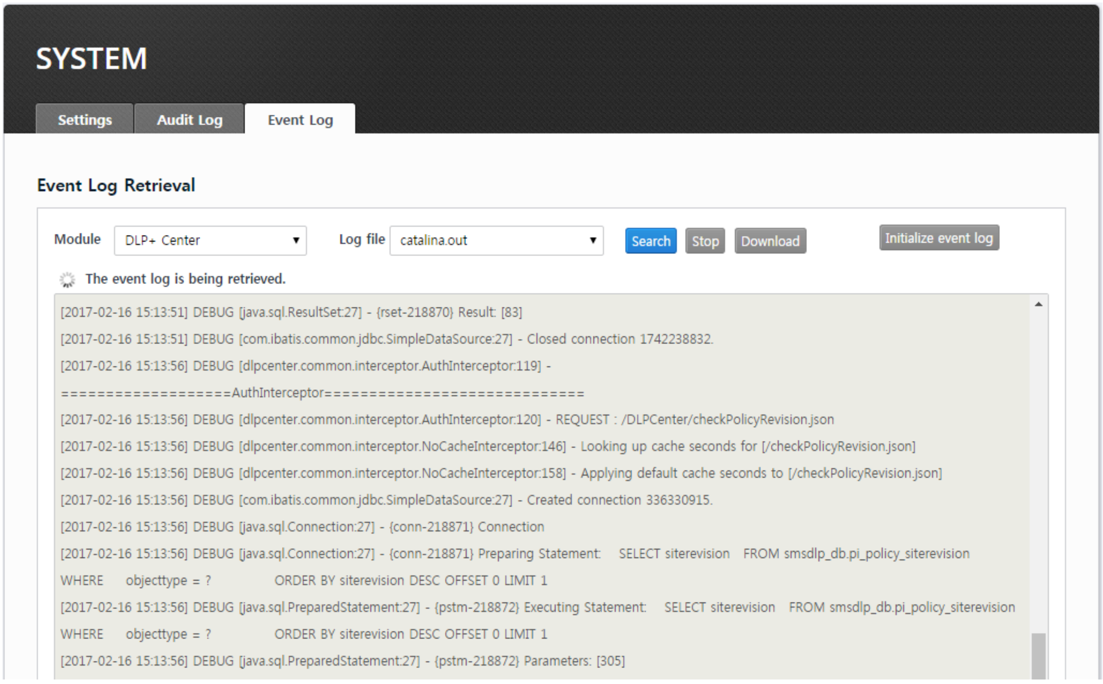
Date: 2017-02-01 ~ 2017-02-16
Log Type: -- ALL --
IP:
Log Contents:

Time	Type	IP	Contents	Description
2017-02-14 00:50:52	Logout	10.106.33.254	Logged out due to session timeout.	[detail] Logged out due to session timeout.
2017-02-14 00:40:52	Access	10.106.33.254	COMMON > General Settings was accessed.	[URL] :/cm/common.mng.init.json [detail] : SYSTEM ACCESS LOG
2017-02-14 00:40:49	Access	10.106.33.254	COMMON > General Settings was accessed.	[URL] :/cm/common.mng.init.json [detail] : SYSTEM ACCESS LOG
2017-02-14 00:32:12	Stop	10.106.33.254	Stopped to search event logs.	[URL] :/cm/environment.stop.eventlog.interval.json [detail] : Stopped to search event logs. - Module: Privacy-i Server - File Name: catalina.out

(FIGURE 3-51) VIEW SYSTEMAUDIT LOGS

3.10 SYSTEM Event Logs

Event logs for each module can be viewed to operate Privacy-i.



Event Log Retrieval

Module: DLP+ Center

Log file: catalina.out

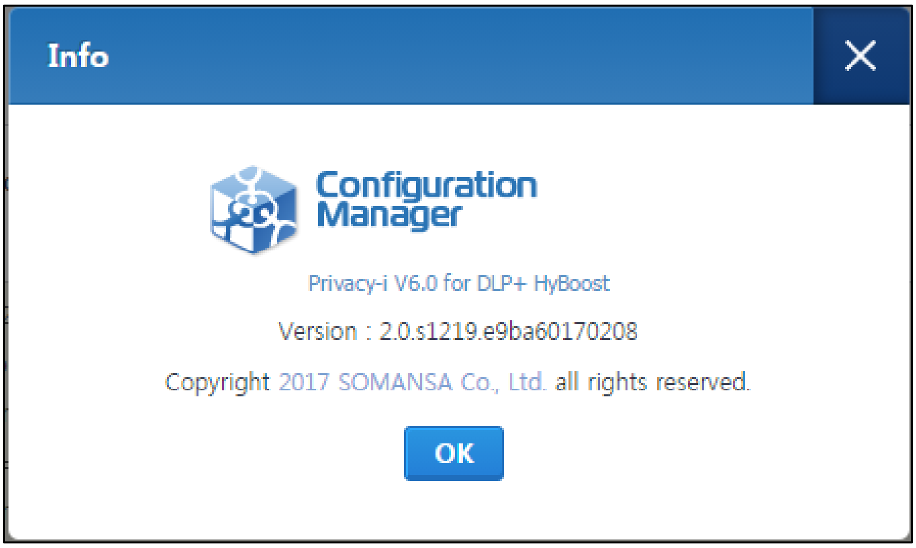
The event log is being retrieved.

```
[2017-02-16 15:13:51] DEBUG [java.sql.ResultSet:27] - {rset-218870} Result: [83]
[2017-02-16 15:13:51] DEBUG [com.ibatis.common.jdbc.SimpleDataSource:27] - Closed connection 1742238832.
[2017-02-16 15:13:56] DEBUG [dlpcenter.common.interceptor.AuthInterceptor:119] -
==================AuthInterceptor===========================
[2017-02-16 15:13:56] DEBUG [dlpcenter.common.interceptor.AuthInterceptor:120] - REQUEST : /DLPCenter/checkPolicyRevision.json
[2017-02-16 15:13:56] DEBUG [dlpcenter.common.interceptor.NoCacheInterceptor:146] - Looking up cache seconds for [/checkPolicyRevision.json]
[2017-02-16 15:13:56] DEBUG [dlpcenter.common.interceptor.NoCacheInterceptor:158] - Applying default cache seconds to [/checkPolicyRevision.json]
[2017-02-16 15:13:56] DEBUG [com.ibatis.common.jdbc.SimpleDataSource:27] - Created connection 336330915.
[2017-02-16 15:13:56] DEBUG [java.sql.Connection:27] - {conn-218871} Connection
[2017-02-16 15:13:56] DEBUG [java.sql.Connection:27] - {conn-218871} Preparing Statement:    SELECT siterevision    FROM smsdlp_db.pi_policy_siterevision
WHERE     objecttype = ?            ORDER BY siterevision DESC OFFSET 0 LIMIT 1
[2017-02-16 15:13:56] DEBUG [java.sql.PreparedStatement:27] - {pstm-218872} Executing Statement:    SELECT siterevision    FROM smsdlp_db.pi_policy_siterevision
WHERE     objecttype = ?            ORDER BY siterevision DESC OFFSET 0 LIMIT 1
[2017-02-16 15:13:56] DEBUG [java.sql.PreparedStatement:27] - {pstm-218872} Parameters: [305]
```

(FIGURE 3-52) EVENT LOG

3.11 Check TOE Version

Version of Configuration Manager can be checked in the screen. A screen for checking the version appears when clicking ⓘ button on the top right portion of the screen.



Privacy-i V6.0 for DLP+ HyBoost

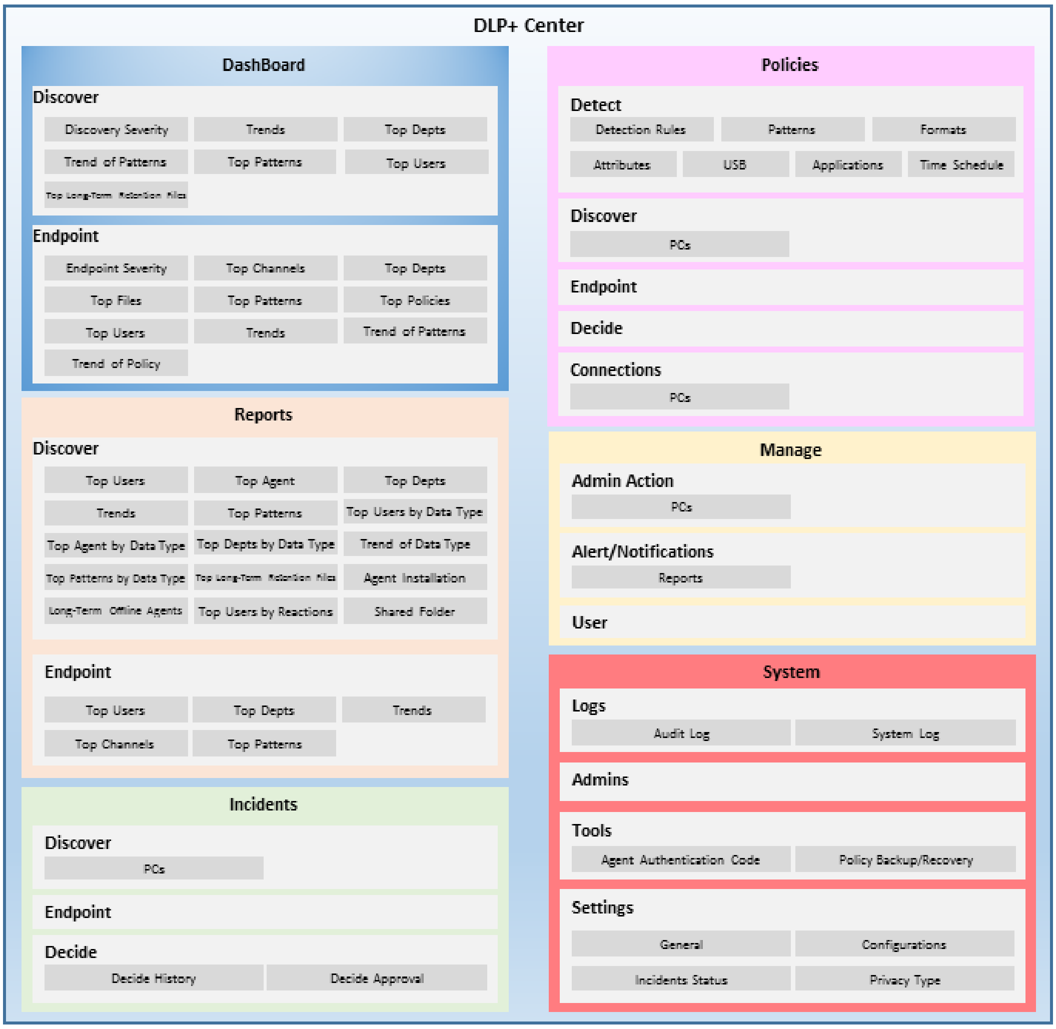
Version : 2.0.s1219.e9ba60170208

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

(FIGURE 3-53) CHECK CONFIGURATION MANAGER VERSION

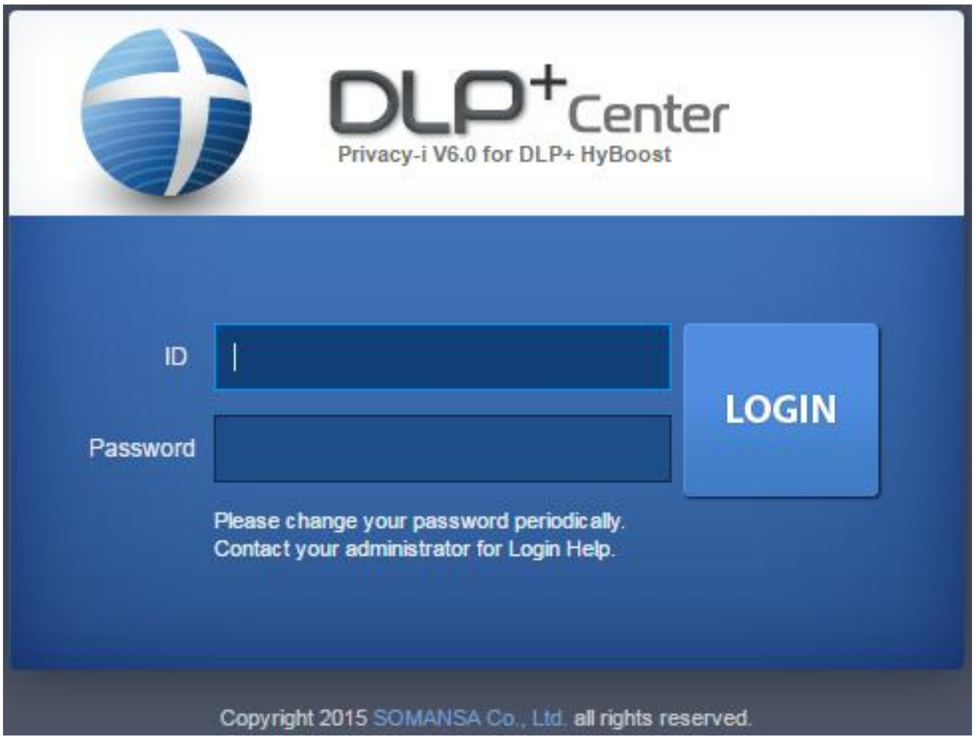
4. DLP+ Center

Privacy-i is a product that provides personal information protection and host data loss prevention, which searches and identifies personal and confidential data stored on a company PC and provides technological and managerial protection measures such as deletion or encryption, and provides Endpoint Data Loss Prevention solution, which controls dataflow from a user PC to external channels. The Privacy-i is operated and managed by the DLP+ Center. Since the DLP+ Center is operated as a web server, the authorized administrator can connect to the DLP+ Center through the company intranet anytime and anywhere for a convenient operating environment.



(FIGURE 4-1) FUNCTIONS PROVIDED BY THE DLP+ CENTER

The DLP+ Center is categorized into Dashboard, Report, Policy, Incidents, Manage and System as follows (see Figure 4-1). Dashboard updates the personal information status and sensitive information dataflow in real time to allow the administrator to view information on the main issues. Also, Report provides a variety of reports for each condition through the detected logs in a PC, and Policy allows for the management of the confidential data inspection policy that is specified to a user PC. In addition, Incidents provide information on detected confidential data and allowed / blocked log in detail. In Manage, the additional functions for the server and Agent can be set. Through System, the Audit Logs, Event and Account Authorization Settings of the DLP+ Center administrator can be viewed.



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

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

(FIGURE 4-2) DLP+ CENTER LOGIN SCREEN

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

☞ Effective Input Field Range

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

Item	Effective range	Character	Failure message
ID	5~100	Letters	Enter ID.
Password	9~41	Numbers, upper or lower case letters, special characters	Enter password.

Recommendations

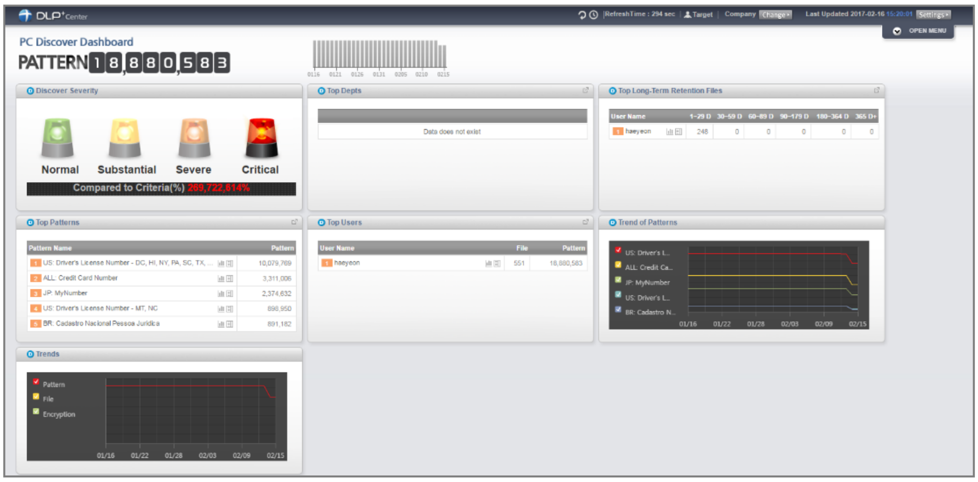
✓ Password should have at least 9 characters and include English letters, numbers and special characters.

4.1 Dashboard

Dashboard is categorized into Discover and Endpoint, and provides the status of data retention for each department or user-specific, path and data of leakage in real time. Such data are composed of components, and are displayed in the order based on the most recent, or most confidential data retained. It has the advantage of rapidly identifying the severity of retained personal information and retaining status by selecting the component and pattern and setting the department for intensive monitoring.

4.1.1 Discover

Discover Dashboard collects inspection information on the status of confidential data retained in a user PC, and provides information. Discover includes 8 components, comprising '(D) Status of Severity', '(D) Top Departments', '(D) Top Patterns', '(D) Top Users', '(D) Trends', '(D) Top Files Retained', '(D) Top Patterns Retained' and '(D) Top Files by Long-Term Retention'.



Top Long-Term Retention Files

User Name	1~29 D	30~59 D	60~89 D	90~179 D	180~364 D	365 D+
1 haeyeon	248	0	0	0	0	0

Top Patterns

Pattern Name	Pattern
1 US: Driver's License Number - DC, HI, NY, PA, SC, TX, ...	10,079,769
2 ALL: Credit Card Number	3,311,006
3 JP: MyNumber	2,374,632
4 US: Driver's License Number - MT, NC	898,950
5 BR: Cadastro Nacional Pessoa Juridica	891,182

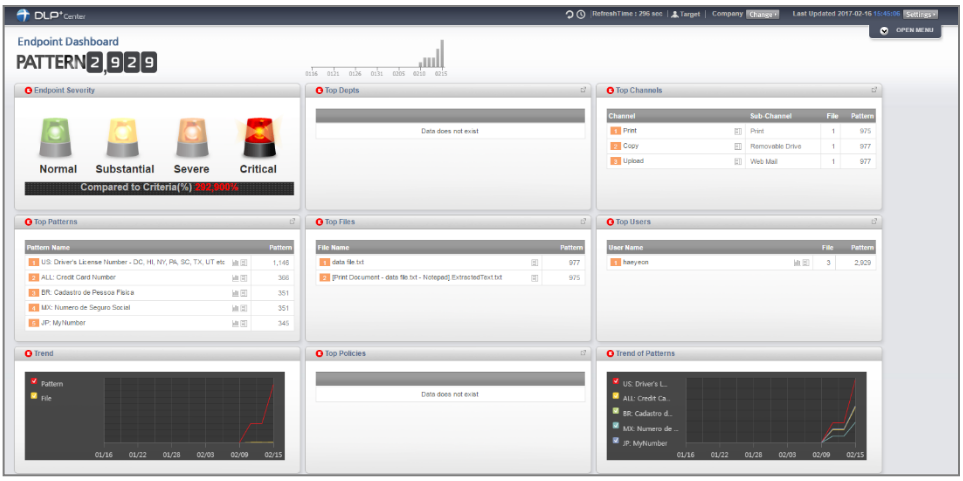
Top Users

User Name	File	Pattern
1 haeyeon	551	18,880,583

(FIGURE 4-3) DASHBOARD: DISCOVER INFORMATION

4.1.2 Endpoint

Endpoint Dashboard collects inspection information on the status of confidential data retained in a user PC, and provides information. Discover includes 8 components, comprising ‘(E) Status of Severity', ‘(E) Top Departments Exported', ‘(E) Top Patterns Exported', ‘(E) Top Users Exported', ‘(E) Trends of Carrying out', ‘(E) Top Files Exported', ‘(E) Top Patterns Exported', and ‘(E) Top Policies'.



Top Depts: Data does not exist

Channel	Sub-Channel	File	Pattern
1 Print	Print	1	975
2 Copy	Removable Drive	1	977
3 Upload	Web Mail	1	977

Pattern Name	Pattern
1 US: Driver's License Number - DC, HI, NY, PA, SC, TX, UT etc	1,146
2 ALL: Credit Card Number	366
3 BR: Cadastro de Pessoa Fisica	351
4 MX: Numero de Seguro Social	351
5 JP: MyNumber	345

File Name	Pattern
1 data file.txt	977
2 [Print Document - data file.txt - Notepad] ExtractedText.txt	975

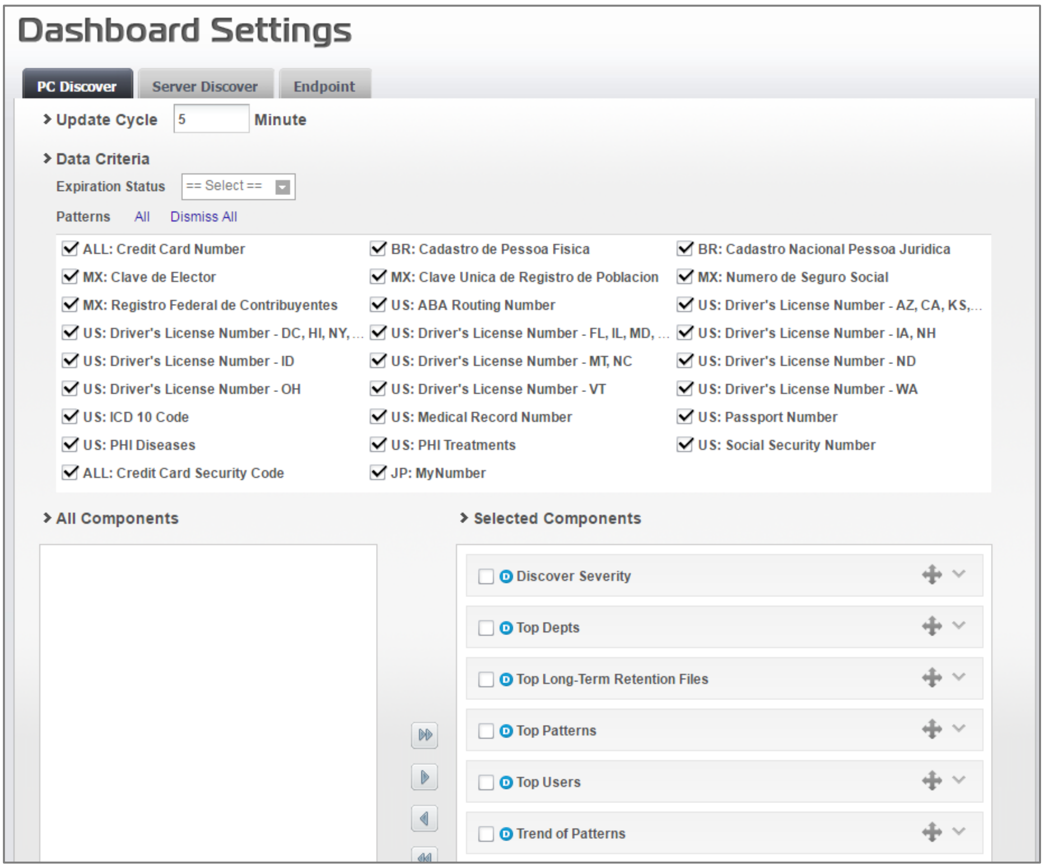
User Name	File	Pattern
1 haeyeon	3	2,929

Top Policies: Data does not exist

(FIGURE 4-4) DASHBOARD: ENDPOINT INFORMATION

4.1.3 Settings

(Figure 4-5) shows the Environmental Settings 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. The data applied to the Dashboard is shown according to the settings values.



Dashboard Settings

› Update Cycle 5 Minute

› Data Criteria

Expiration Status == Select ==

Patterns All Dismiss All

☑ ALL: Credit Card Number
☑ BR: Cadastro de Pessoa Fisica
☑ BR: Cadastro Nacional Pessoa Juridica
☑ MX: Clave de Elector
☑ MX: Clave Unica de Registro de Poblacion
☑ MX: Numero de Seguro Social
☑ MX: Registro Federal de Contribuyentes
☑ US: ABA Routing Number
☑ US: Driver's License Number - AZ, CA, KS,...
☑ US: Driver's License Number - DC, HI, NY, ...
☑ US: Driver's License Number - FL, IL, MD, ...
☑ US: Driver's License Number - IA, NH
☑ US: Driver's License Number - ID
☑ US: Driver's License Number - MT, NC
☑ US: Driver's License Number - ND
☑ US: Driver's License Number - OH
☑ US: Driver's License Number - VT
☑ US: Driver's License Number - WA
☑ US: ICD 10 Code
☑ US: Medical Record Number
☑ US: Passport Number
☑ US: PHI Diseases
☑ US: PHI Treatments
☑ US: Social Security Number
☑ ALL: Credit Card Security Code
☑ JP: MyNumber

› All Components

› Selected Components

□ Discover Severity
□ Top Depts
□ Top Long-Term Retention Files
□ Top Patterns
□ Top Users
□ Trend of Patterns

(FIGURE 4-5) DASHBOARD: SETTINGS

4.2 Reports

Reports perform outputting the analysis results for each condition about the confidential data retained (Discover) in a user PC within the network and the exported / blocked logs of Endpoint. Since Reports display various graphs, lists and main result items of the detected results, the administrator has the advantage of being able to quickly analyze according to the selected criteria.

[TABLE 4-2] REPORTS PROVIDED FROM DLP+ CENTER

		Type	Contents
Discover	PC	Top Users	Displays data by top users in the order that retains the most confidential data based on the selected department
		Top Departments	Displays data by top departments in the order that retains the most confidential data based on the selected department
		Trends	Displays results for confidential data retained in a user PC for the date logs inspected
		Top Long-Term Retention Files	Displays data by top PCs which have retained confidential data files for a long time
		Top Patterns	Displays data by top patterns for retained confidential data based on the selected department or user
		Long-Term Offline Agents	Searches the Agents with no connection for a long time
		Agent Installation	Identifies the status of Privacy-i Installation by users
		Top Users by Reactions	Displays ‘Details of Measures Taken’ (Encryption, delete, separate) for detected files and checks in the order
		Top Users by Data Type	Rankings of personal information ‘classification performance’ and ‘classification contents’ are checked for each ‘User’
		Top Departments by Data Type	Rankings of personal information ‘classification performance’ and ‘classification contents’ are checked for each ‘Department’
		Trends of Data Type	Checks the change rate of personal information pattern and file for each date
		Top Patterns by Data Type	‘Total number of patterns’ and ‘Classification performance’ are checked for each type of personal information
		Top Agents by Data Type	Rankings of personal information classification can be checked for each Agent
Endpoint	Top Users		Displays data by top users in the order that allowed / blocked the most confidential data based on the selected department
	Top Departments		Displays data by top departments in the order that allowed / blocked the most confidential data based on the selected department
	Trends of Incidents		Show the results of trends of allowed / blocked logs
	Top Channels		Displays data by top channels based on allowed / blocked incidents
	Top Patterns		Displays data by top patterns based on allowed / blocked incidents

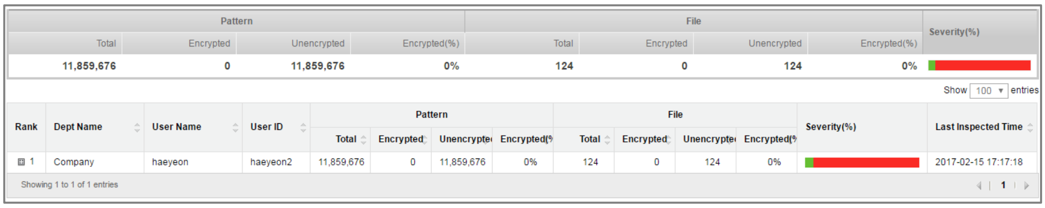
4.2.1 Discovery

4.2.1.1 PC

By using the results of status for retained confidential data inspection on a PC, Reports include 'Top Users', 'Top Departments', 'Trends of Retention', 'Top Files with Long Term Retention' and 'Top Patterns' based on the detected number of confidential data patterns or files for a specific department or user, and 'Long Term Offline Agents', 'Agent Distribution' for the Agent status.

- Top users

Displays the top users who retain the most files with confidential data information detected from a user PC in the order contents and the number of detected files. The number of detected files, and the state of encryption/non-encryption are shown based on the patterns and files, and the list of top users who retain the most confidential data by selected department is displayed at the bottom.



Pattern				File				Severity(%)
Total	Encrypted	Unencrypted	Encrypted(%)	Total	Encrypted	Unencrypted	Encrypted(%)	
11,859,676	0	11,859,676	0%	124	0	124	0%	🟩🟥

Show 100 ▾ entries

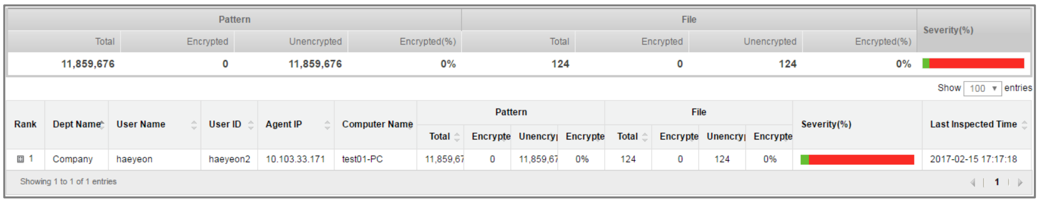
Rank	Dept Name	User Name	User ID	Pattern				File				Severity(%)	Last Inspected Time
				Total	Encrypted	Unencrypte	Encrypted(%	Total	Encrypted	Unencrypte	Encrypted(%		
⊞ 1	Company	haeyeon	haeyeon2	11,859,676	0	11,859,676	0%	124	0	124	0%	🟩🟥	2017-02-15 17:17:18

Showing 1 to 1 of 1 entries

(FIGURE 4-6) REPORTS-PC: RESULTS ON TOP USERS

- Top agents

Displays the top severity ratio of confidential data information detected from a user PC in the order, and the top list of detected severity results based on a user IP.



Pattern				File				Severity(%)
Total	Encrypted	Unencrypted	Encrypted(%)	Total	Encrypted	Unencrypted	Encrypted(%)	
11,859,676	0	11,859,676	0%	124	0	124	0%	🟩🟥

Show 100 ▾ entries

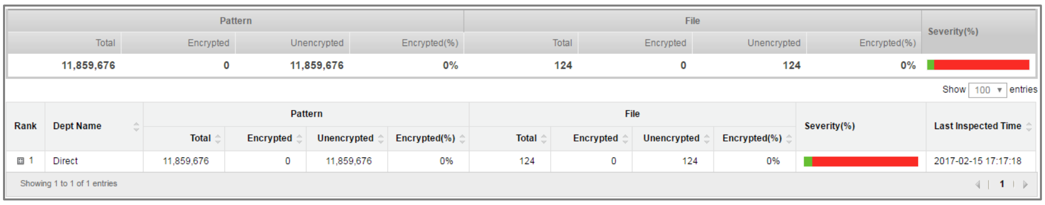
Rank	Dept Name	User Name	User ID	Agent IP	Computer Name	Pattern				File				Severity(%)	Last Inspected Time
						Total	Encrypte	Unencry|	Encrypte	Total	Encrypte	Unencry|	Encrypte		
⊞ 1	Company	haeyeon	haeyeon2	10.103.33.171	test01-PC	11,859,67	0	11,859,67	0%	124	0	124	0%	🟩🟥	2017-02-15 17:17:18

Showing 1 to 1 of 1 entries

(FIGURE 4-7) REPORTS-PC: RESULTS ON TOP OWNING AGENTS

- Top departments

Data is output based on "Department" as in the data of "Top Users" above.



Pattern				File				Severity(%)
Total	Encrypted	Unencrypted	Encrypted(%)	Total	Encrypted	Unencrypted	Encrypted(%)	
11,859,676	0	11,859,676	0%	124	0	124	0%	🟩🟥

Show 100 ▾ entries

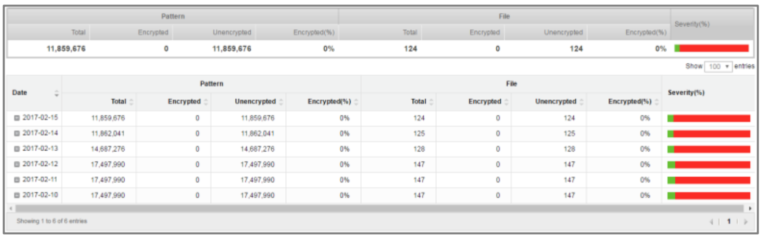
Rank	Dept Name	Pattern				File				Severity(%)	Last Inspected Time
		Total	Encrypted	Unencrypted	Encrypted(%)	Total	Encrypted	Unencrypted	Encrypted(%)		
⊞ 1	Direct	11,859,676	0	11,859,676	0%	124	0	124	0%	🟩🟥	2017-02-15 17:17:18

Showing 1 to 1 of 1 entries

(FIGURE 4-8) REPORTS-PC: RESULTS ON TOP OWNING DEPARTMENTS

- Trends

Display the trends of patterns, files and severity ratio of departments and users that retain confidential data. Also, it is possible to identify the indices on the confidential data which has been retained per period.



Pattern				File				Severity(%)
Total	Encrypted	Unencrypted	Encrypted(%)	Total	Encrypted	Unencrypted	Encrypted(%)	
11,859,676	0	11,859,676	0%	124	0	124	0%	🟩🟥

Show 100 ▾ entries

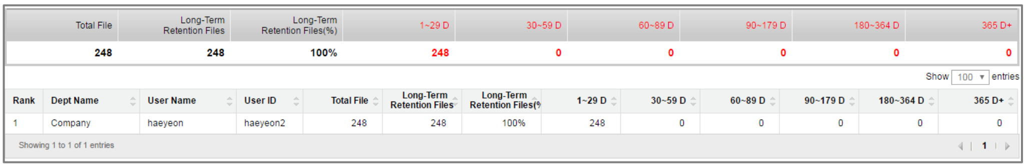
Date	Pattern				File				Severity(%)
	Total	Encrypted	Unencrypted	Encrypted(%)	Total	Encrypted	Unencrypted	Encrypted(%)	
⊞ 2017-02-15	11,859,676	0	11,859,676	0%	124	0	124	0%	🟩🟥
⊞ 2017-02-14	11,862,041	0	11,862,041	0%	125	0	125	0%	🟩🟥
⊞ 2017-02-13	14,687,276	0	14,687,276	0%	128	0	128	0%	🟩🟥
⊞ 2017-02-12	17,497,990	0	17,497,990	0%	147	0	147	0%	🟩🟥
⊞ 2017-02-11	17,497,990	0	17,497,990	0%	147	0	147	0%	🟩🟥
⊞ 2017-02-10	17,497,990	0	17,497,990	0%	147	0	147	0%	🟩🟥

Showing 1 to 6 of 6 entries

(FIGURE 4-9) REPORTS-PC: RESULTS ON TOP OWINING TRENDS SCREEN

- Top long-term retention files

Displays data for files which include confidential data for an extended period of time. The retention period of a detected file and saved confidential data (client information, personal usage) can be checked.



Total File	Long-Term Retention Files	Long-Term Retention Files(%)	1~29 D	30~59 D	60~89 D	90~179 D	180~364 D	365 D+
248	248	100%	248	0	0	0	0	0

Show 100 ▾ entries

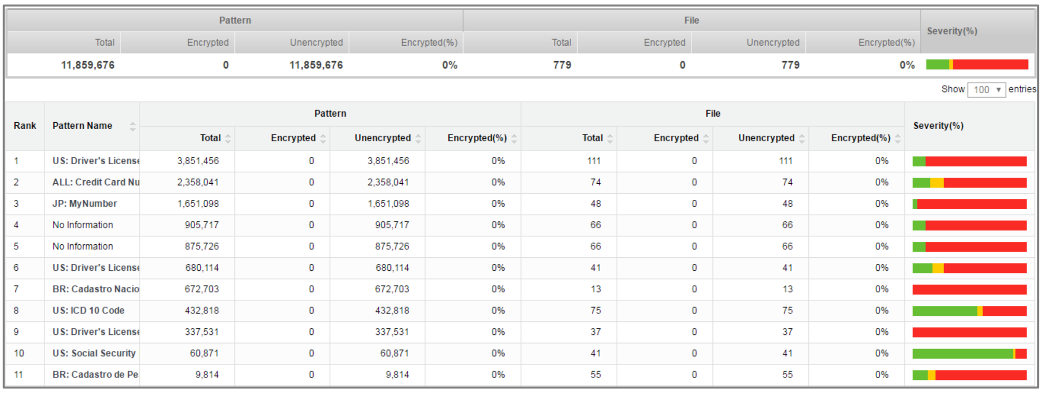
Rank	Dept Name	User Name	User ID	Total File	Long-Term Retention Files	Long-Term Retention Files(%	1~29 D	30~59 D	60~89 D	90~179 D	180~364 D	365 D+
1	Company	haeyeon	haeyeon2	248	248	100%	248	0	0	0	0	0

Showing 1 to 1 of 1 entries

(FIGURE 4-10) REPORTS-PC: RESULTS ON TOP OWNED FILE FOR LONG PERIODS

- Top patterns

Data is output based on "Pattern" as in the data of "Top Users" above.



Pattern				File				Severity(%)
Total	Encrypted	Unencrypted	Encrypted(%)	Total	Encrypted	Unencrypted	Encrypted(%)	
11,859,676	0	11,859,676	0%	779	0	779	0%	🟩🟨🟥

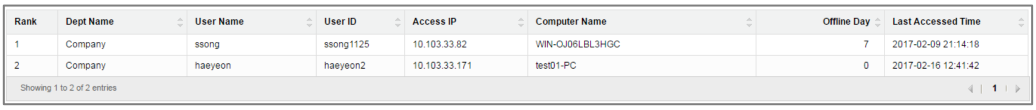
Show 100 ▾ entries

Rank	Pattern Name	Pattern				File				Severity(%)
		Total	Encrypted	Unencrypted	Encrypted(%)	Total	Encrypted	Unencrypted	Encrypted(%)	
1	US: Driver's License	3,851,456	0	3,851,456	0%	111	0	111	0%	🟩🟥
2	ALL: Credit Card Nu	2,358,041	0	2,358,041	0%	74	0	74	0%	🟩🟨🟥
3	JP: MyNumber	1,651,098	0	1,651,098	0%	48	0	48	0%	🟩🟥
4	No Information	905,717	0	905,717	0%	66	0	66	0%	🟩🟥
5	No Information	875,726	0	875,726	0%	66	0	66	0%	🟩🟥
6	US: Driver's License	680,114	0	680,114	0%	41	0	41	0%	🟩🟨🟥
7	BR: Cadastro Nacio	672,703	0	672,703	0%	13	0	13	0%	🟥
8	US: ICD 10 Code	432,818	0	432,818	0%	75	0	75	0%	🟩🟨🟥
9	US: Driver's License	337,531	0	337,531	0%	37	0	37	0%	🟥
10	US: Social Security	60,871	0	60,871	0%	41	0	41	0%	🟩🟨🟥
11	BR: Cadastro de Pe	9,814	0	9,814	0%	55	0	55	0%	🟩🟨🟥

(FIGURE 4-11) REPORTS-PC: RESULTS OF TOP PATTERNS

- Long-term offline agents

Displays data based on agents which have been offline on the server for an extended period of time.



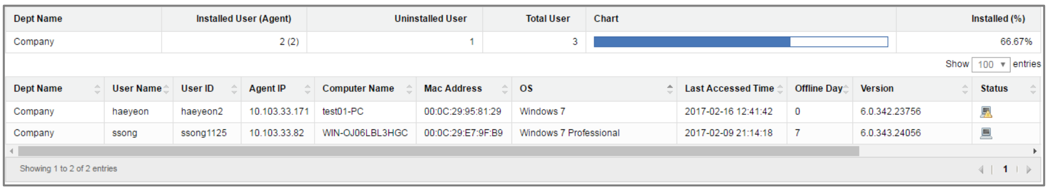
Rank	Dept Name	User Name	User ID	Access IP	Computer Name	Offline Day	Last Accessed Time
1	Company	ssong	ssong1125	10.103.33.82	WIN-OJ06LBL3HGC	7	2017-02-09 21:14:18
2	Company	haeyeon	haeyeon2	10.103.33.171	test01-PC	0	2017-02-16 12:41:42

Showing 1 to 2 of 2 entries

(FIGURE 4-12) REPORTS-PC: LONG-TERM OFFLINE AGENTS

- Agent installations

Displays user data with Agent installed based on the associated HR Information. The agent installation status in a company can be checked in output Report.



Dept Name	Installed User (Agent)	Uninstalled User	Total User	Chart	Installed (%)
Company	2 (2)	1	3		66.67%

Show 100 entries

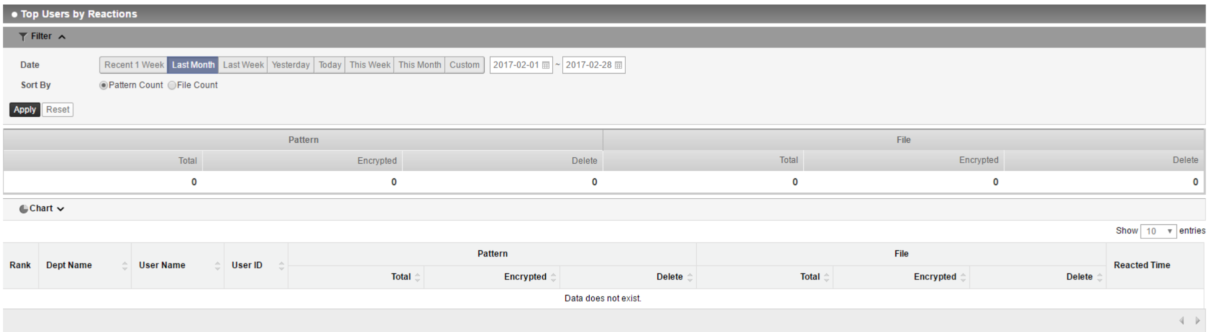
Dept Name	User Name	User ID	Agent IP	Computer Name	Mac Address	OS	Last Accessed Time	Offline Day	Version	Status
Company	haeyeon	haeyeon2	10.103.33.171	test01-PC	00:0C:29:95:81:29	Windows 7	2017-02-16 12:41:42	0	6.0.342.23756	
Company	ssong	ssong1125	10.103.33.82	WIN-OJ06LBL3HGC	00:0C:29:E7:9F:B9	Windows 7 Professional	2017-02-09 21:14:18	7	6.0.343.24056	

Showing 1 to 2 of 2 entries

(FIGURE 4-13) REPORTS-PC: AGENT INSTALLATIONS

- Top users by reactions

'Reactions' (encryption, delete, separation) on files detected by [User inspection] or [Admin inspection] are displayed so that they can be checked by ranking. For the measures (encryption, delete, separation) taken on the files detected in the initial inspection, information on the changes of the file in re-inspection is displayed through user inspection or admin inspection.



● Top Users by Reactions

Filter

Date: Recent 1 Week | Last Month | Last Week | Yesterday | Today | This Week | This Month | Custom | 2017-02-01 ~ 2017-02-28

Sort By: ● Pattern Count ○ File Count

Pattern			File		
Total	Encrypted	Delete	Total	Encrypted	Delete
0	0	0	0	0	0

Show 10 entries

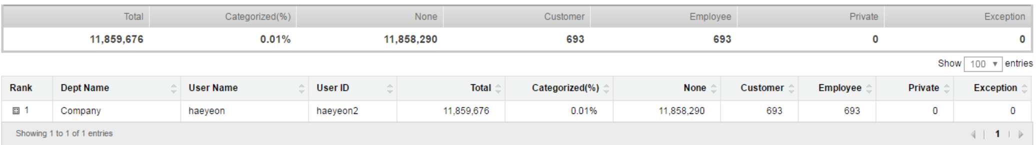
Rank	Dept Name	User Name	User ID	Pattern			File			Reacted Time
				Total	Encrypted	Delete	Total	Encrypted	Delete	

Data does not exist.

(FIGURE 4-14) REPORTS-PC: TOP USERS BY REARCIONS

- Top users by data type

The ranking of 'Classification rate' and 'Classified contents' can be checked by the 'user'. The number of patterns and the classification rate for Not Categorized, Client, Employee, Personal and Exception can be checked for each user by rankings.



Total	Categorized(%)	None	Customer	Employee	Private	Exception
11,859,676	0.01%	11,858,290	693	693	0	0

Show 100 entries

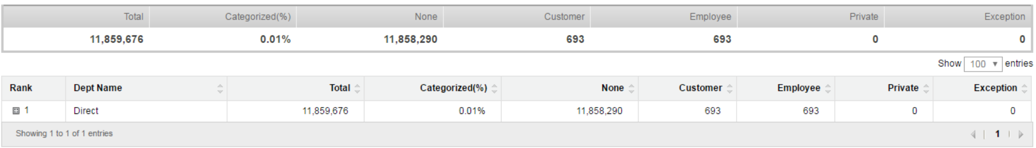
Rank	Dept Name	User Name	User ID	Total	Categorized(%)	None	Customer	Employee	Private	Exception
⊞ 1	Company	haeyeon	haeyeon2	11,859,676	0.01%	11,858,290	693	693	0	0

Showing 1 to 1 of 1 entries

(FIGURE 4-15) REPORTS-PC: TOP USERS WITH PERSONAL INFORMATION CLASSIFIED

- Top departments by type

The ranking of 'Classification rate' and 'Classified contents' can be checked by the 'department'. The number of patterns and the classification rate for Not Categorized, Client, Employee, Personal and Exception can be checked for each department by rankings.



Total	Categorized(%)	None	Customer	Employee	Private	Exception
11,859,676	**0.01%**	**11,858,290**	**693**	**693**	**0**	**0**

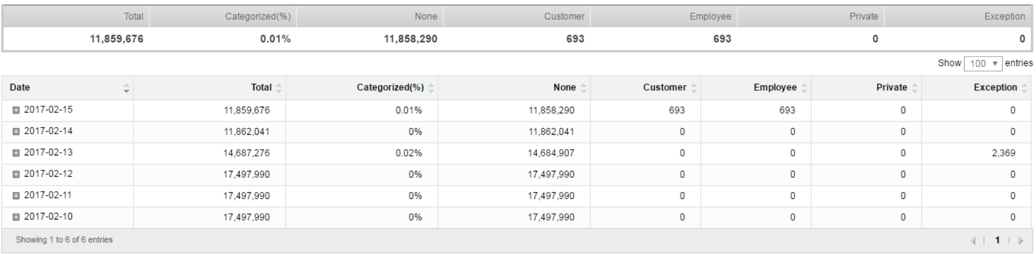
Rank	Dept Name	Total	Categorized(%)	None	Customer	Employee	Private	Exception
⊞ 1	Direct	11,859,676	0.01%	11,858,290	693	693	0	0

Showing 1 to 1 of 1 entries

(FIGURE 4-16) REPORTS-PC: TOP DEPARTMENTS WITH PERSONAL INFORMATION CLASSIFIED

- Trends for data types

The personal information pattern and the rate of changes of file a day can be checked. The trends for each pattern and file can be checked through graphs and tables.



Total	Categorized(%)	None	Customer	Employee	Private	Exception
11,859,676	**0.01%**	**11,858,290**	**693**	**693**	**0**	**0**

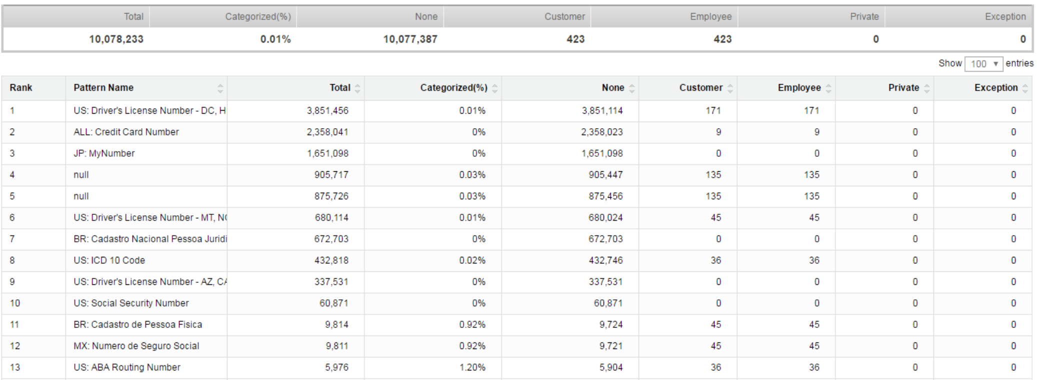
Date	Total	Categorized(%)	None	Customer	Employee	Private	Exception
⊞ 2017-02-15	11,859,676	0.01%	11,858,290	693	693	0	0
⊞ 2017-02-14	11,862,041	0%	11,862,041	0	0	0	0
⊞ 2017-02-13	14,687,276	0.02%	14,684,907	0	0	0	2,369
⊞ 2017-02-12	17,497,990	0%	17,497,990	0	0	0	0
⊞ 2017-02-11	17,497,990	0%	17,497,990	0	0	0	0
⊞ 2017-02-10	17,497,990	0%	17,497,990	0	0	0	0

Showing 1 to 6 of 6 entries

(FIGURE 4-17) REPORTS-PC: TRENDS OF PERSONAL INFORMATION CLASSIFICATION

- Top patterns by type

The ranking of 'Classification rate' and 'Classified contents' can be checked by the 'type of personal information'. The number of patterns and the classification rate for Not Categorized, Client, Employee, Personal and Exception can be checked for each type of personal information by rankings.



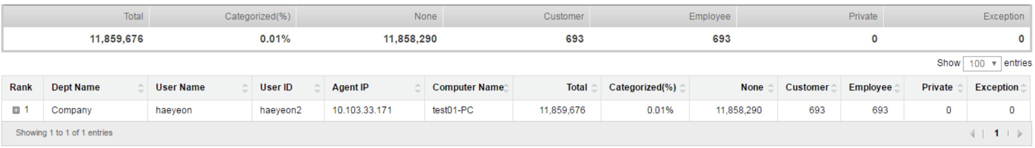
Total	Categorized(%)	None	Customer	Employee	Private	Exception
10,078,233	**0.01%**	**10,077,387**	**423**	**423**	**0**	**0**

Rank	Pattern Name	Total	Categorized(%)	None	Customer	Employee	Private	Exception
1	US: Driver's License Number - DC, H	3,851,456	0.01%	3,851,114	171	171	0	0
2	ALL: Credit Card Number	2,358,041	0%	2,358,023	9	9	0	0
3	JP: MyNumber	1,651,098	0%	1,651,098	0	0	0	0
4	null	905,717	0.03%	905,447	135	135	0	0
5	null	875,726	0.03%	875,456	135	135	0	0
6	US: Driver's License Number - MT, N(	680,114	0.01%	680,024	45	45	0	0
7	BR: Cadastro Nacional Pessoa Juridi	672,703	0%	672,703	0	0	0	0
8	US: ICD 10 Code	432,818	0.02%	432,746	36	36	0	0
9	US: Driver's License Number - AZ, C/	337,531	0%	337,531	0	0	0	0
10	US: Social Security Number	60,871	0%	60,871	0	0	0	0
11	BR: Cadastro de Pessoa Fisica	9,814	0.92%	9,724	45	45	0	0
12	MX: Numero de Seguro Social	9,811	0.92%	9,721	45	45	0	0
13	US: ABA Routing Number	5,976	1.20%	5,904	36	36	0	0

(FIGURE 4-18) REPORTS-PC: TOP PATTERNS OF PERSONAL INFORMATION CLASSIFICATION

- Top Agents by data type

Rankings of personal information classification can be checked for each Agent. The number of patterns and the classification rate for Not Categorized, Client, Employee, Personal and Exception can be checked by rankings.



Total	Categorized(%)	None	Customer	Employee	Private	Exception
11,859,676	0.01%	11,858,290	693	693	0	0

Show 100 entries

Rank	Dept Name	User Name	User ID	Agent IP	Computer Name	Total	Categorized(%)	None	Customer	Employee	Private	Exception
⊞ 1	Company	haeyeon	haeyeon2	10.103.33.171	test01-PC	11,859,676	0.01%	11,858,290	693	693	0	0

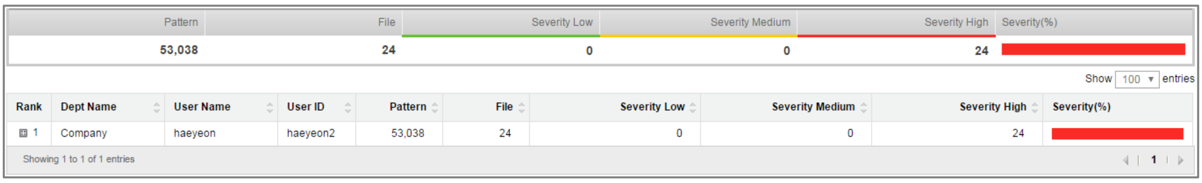
Showing 1 to 1 of 1 entries

(FIGURE 4-19) REPORTS-PC: TOP AGENTS OF PERSONAL INFORMATION CLASSIFICATION

4.2.2 Endpoint

- Top users

Displays data including allowed / blocked patterns by policy, file and severity rate in the order of the user. Through Report, top users who exported the most confidential data can be viewed.



Pattern	File	Severity Low	Severity Medium	Severity High	Severity(%)
53,038	24	0	0	24	🟥

Show 100 entries

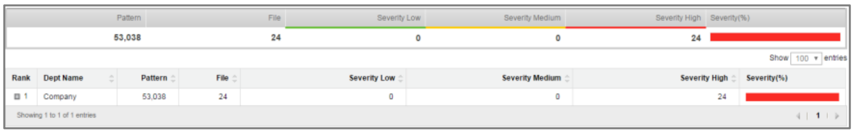
Rank	Dept Name	User Name	User ID	Pattern	File	Severity Low	Severity Medium	Severity High	Severity(%)
⊞ 1	Company	haeyeon	haeyeon2	53,038	24	0	0	24	🟥

Showing 1 to 1 of 1 entries

(FIGURE 4-20) TOP USERS

- Top departments

Displays data including allowed / blocked patterns by policy, file and severity rate in the order of the department. Through Report, top departments who exported the most confidential data can be viewed.



Pattern	File	Severity Low	Severity Medium	Severity High	Severity(%)
53,038	24	0	0	24	🟥

Show 100 entries

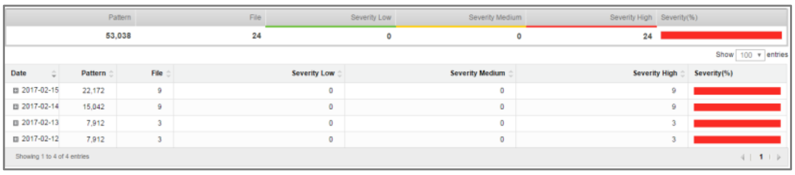
Rank	Dept Name	Pattern	File	Severity Low	Severity Medium	Severity High	Severity(%)
⊞ 1	Company	53,038	24	0	0	24	🟥

Showing 1 to 1 of 1 entries

(FIGURE 4-21) TOP DEPARTMENTS

- Trends of Incidents

Allowed/blocked patterns, file and severity rate trends according to the policy are shown. Trends of departments and users with the most exported or blocked files containing confidential data are represented as graphs and lists.



Pattern	File	Severity Low	Severity Medium	Severity High	Severity(%)
53,038	24	0	0	24	🟥

Show 100 entries

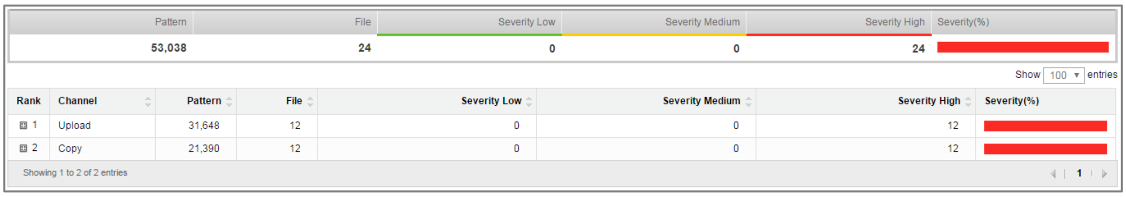
Date	Pattern	File	Severity Low	Severity Medium	Severity High	Severity(%)
⊞ 2017-02-15	22,172	9	0	0	9	🟥
⊞ 2017-02-14	15,042	9	0	0	9	🟥
⊞ 2017-02-13	7,912	3	0	0	3	🟥
⊞ 2017-02-12	7,912	3	0	0	3	🟥

Showing 1 to 4 of 4 entries

(FIGURE 4-22) TRENDS OF INCIDENTS

- Top channels

The pattern, file and severity rate on the allowed/blocked leakage path are shown in the order of channels.



Pattern	File	Severity Low	Severity Medium	Severity High	Severity(%)
53,038	24	0	0	24	🟥

Show 100 entries

Rank	Channel	Pattern	File	Severity Low	Severity Medium	Severity High	Severity(%)
⊞ 1	Upload	31,648	12	0	0	12	🟥
⊞ 2	Copy	21,390	12	0	0	12	🟥

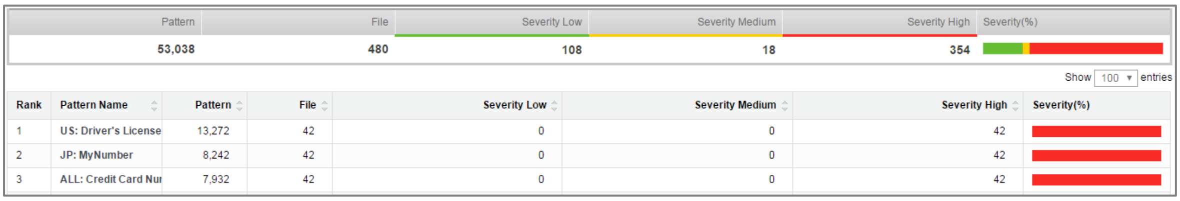
Showing 1 to 2 of 2 entries

1

(FIGURE 4-23) TOP CHANNELS

- Top patterns

Allowed/blocked data is shown based on the patterns.



Pattern	File	Severity Low	Severity Medium	Severity High	Severity(%)
53,038	480	108	18	354	🟩🟨🟥

Show 100 entries

Rank	Pattern Name	Pattern	File	Severity Low	Severity Medium	Severity High	Severity(%)
1	US: Driver's License	13,272	42	0	0	42	🟥
2	JP: MyNumber	8,242	42	0	0	42	🟥
3	ALL: Credit Card Nur	7,932	42	0	0	42	🟥

(FIGURE 4-24) TOP PATTERNS

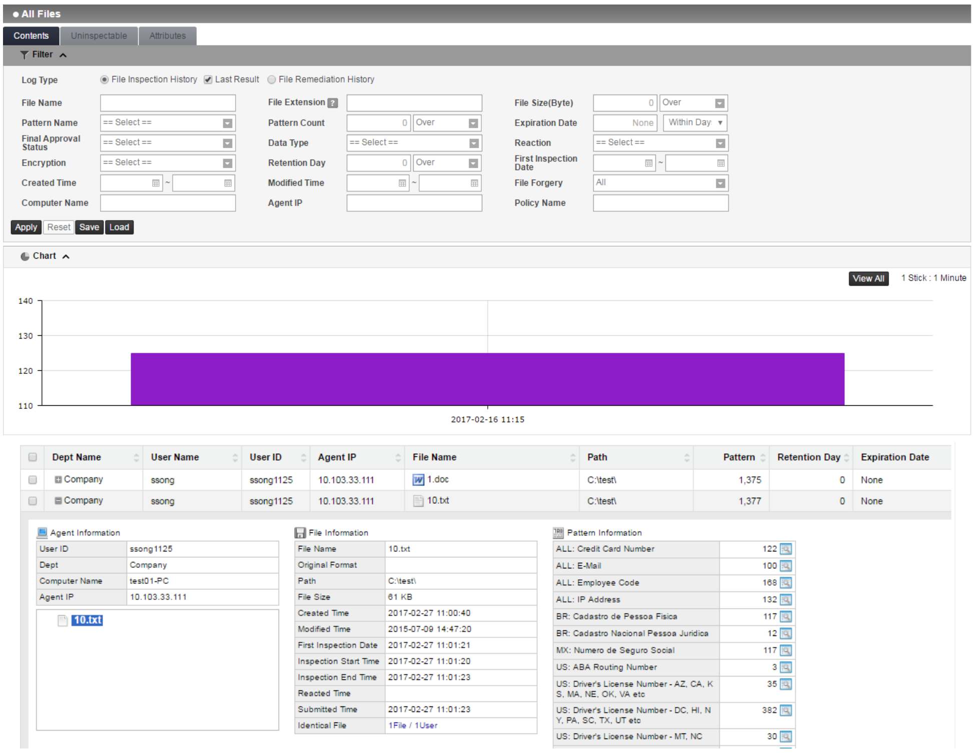
4.3 Incidents

4.3.1 Discover

4.3.1.1 PCs

- Recently Inspected Files

The data file details of departments and users that were most recently inspected can be viewed.



● All Files

Contents | Uninspectable | Attributes

Filter

Log Type: ● File Inspection History ☑ Last Result ○ File Remediation History

File Name		File Extension		File Size(Byte)	0 Over
Pattern Name	== Select ==	Pattern Count	0 Over	Expiration Date	None Within Day
Final Approval Status	== Select ==	Data Type	== Select ==	Reaction	== Select ==
Encryption	== Select ==	Retention Day	0 Over	First Inspection Date	~
Created Time	~	Modified Time	~	File Forgery	All
Computer Name		Agent IP		Policy Name	

Apply Reset Save Load

Chart

View All 1 Stick : 1 Minute

□	Dept Name	User Name	User ID	Agent IP	File Name	Path	Pattern	Retention Day	Expiration Date
□	Company	ssong	ssong1125	10.103.33.111	1.doc	C:\test\	1,375	0	None
□	Company	ssong	ssong1125	10.103.33.111	10.txt	C:\test\	1,377	0	None

Agent Information

User ID	ssong1125
Dept	Company
Computer Name	test01-PC
Agent IP	10.103.33.111

10.txt

File Information

File Name	10.txt
Original Format	
Path	C:\test\
File Size	61 KB
Created Time	2017-02-27 11:00:40
Modified Time	2015-07-09 14:47:20
First Inspection Date	2017-02-27 11:01:21
Inspection Start Time	2017-02-27 11:01:20
Inspection End Time	2017-02-27 11:01:23
Reacted Time	
Submitted Time	2017-02-27 11:01:23
Identical File	1File / 1User

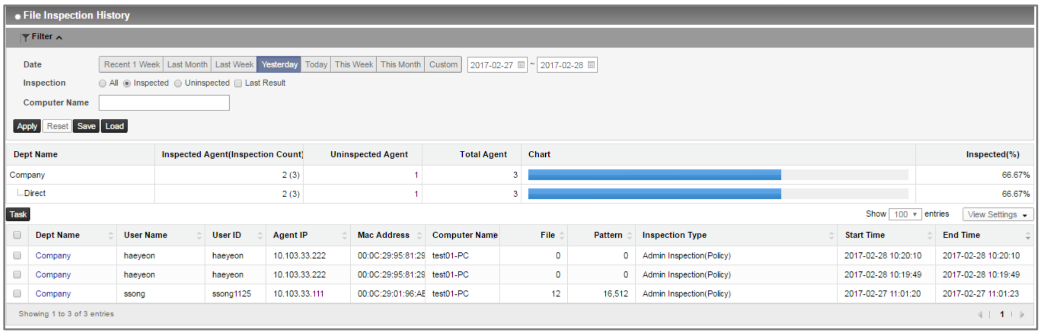
Pattern Information

ALL: Credit Card Number	122
ALL: E-Mail	100
ALL: Employee Code	168
ALL: IP Address	132
BR: Cadastro de Pessoa Fisica	117
BR: Cadastro Nacional Pessoa Juridica	12
MX: Numero de Seguro Social	117
US: ABA Routing Number	3
US: Driver's License Number - AZ, CA, KS, MA, NE, OK, VA etc	35
US: Driver's License Number - DC, HI, NY, PA, SC, TX, UT etc	382
US: Driver's License Number - MT, NC	30

(FIGURE 4-25) PERSONAL INFORMATION DETECTION RESULTS SCREEN

- File inspection

The data file details of departments and users that were previously inspected can be viewed.



● File Inspection History

Filter

Date: Recent 1 Week | Last Month | Last Week | Yesterday | Today | This Week | This Month | Custom 2017-02-27 ~ 2017-02-28

Inspection: ○ All ● Inspected ○ Uninspected □ Last Result

Computer Name:

Apply Reset Save Load

Dept Name	Inspected Agent(Inspection Count)	Uninspected Agent	Total Agent	Chart	Inspected(%)
Company	2 (3)	1	3		66.67%
Direct	2 (3)	1	3		66.67%

Task — Show 100 entries — View Settings

□	Dept Name	User Name	User ID	Agent IP	Mac Address	Computer Name	File	Pattern	Inspection Type	Start Time	End Time
□	Company	haeyeon	haeyeon	10.103.33.222	00:0C:29:95:81:29	test01-PC	0	0	Admin Inspection(Policy)	2017-02-28 10:20:10	2017-02-28 10:20:10
□	Company	haeyeon	haeyeon	10.103.33.222	00:0C:29:95:81:29	test01-PC	0	0	Admin Inspection(Policy)	2017-02-28 10:19:49	2017-02-28 10:19:49
□	Company	ssong	ssong1125	10.103.33.111	00:0C:29:01:96:AE	test01-PC	12	16,512	Admin Inspection(Policy)	2017-02-27 11:01:20	2017-02-27 11:01:23

Showing 1 to 3 of 3 entries

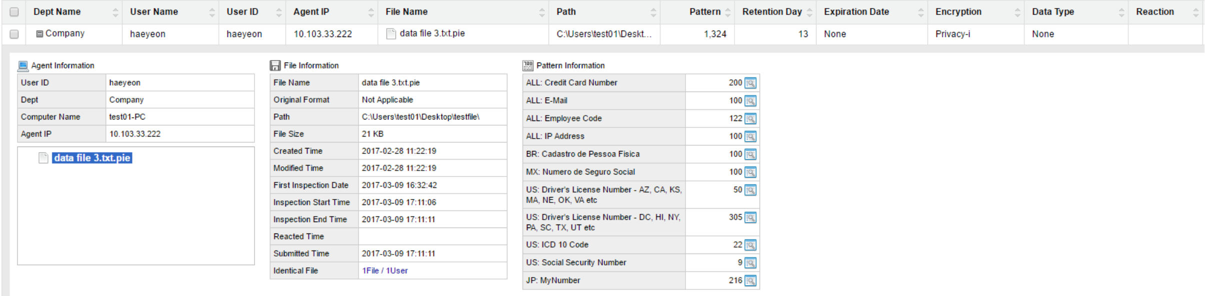
(FIGURE 4-26) FILE INSPECTION HISTORY SCREEN

[TABLE 4-3] ITEMS PROVIDED BY DISCOVER

Item	Description
Department name/User name	Name of configured department and the user belonging to the department
Agent IP	IP of user
File name	Name of detected file
Number of patterns	The number of personal information patterns in detected file
Days of retention	Days of retaining the detected file by the user
Expiring date	Expiring date detected file
Encryption	Encryption of detected file
Information type	Information type of detected file
Protective measures	Measures of encryption on detected file
Date of inspection	Date when the inspection was performed

- Measures on files

After measures on the detected file (encryption, deletion, quarantine) in the initial inspection, the information for the changes in the next inspection is displayed through user-inspection or admin inspection.



□	Dept Name	User Name	User ID	Agent IP	File Name	Path	Pattern	Retention Day	Expiration Date	Encryption	Data Type	Reaction
□	Company	haeyeon	haeyeon	10.103.33.222	data file 3.txt.pie	C:\Users\test01\Deskt...	1,324	13	None	Privacy-i	None	

Agent Information

User ID	haeyeon
Dept	Company
Computer Name	test01-PC
Agent IP	10.103.33.222

data file 3.txt.pie

File Information

File Name	data file 3.txt.pie
Original Format	Not Applicable
Path	C:\Users\test01\Desktop\testfile\
File Size	21 KB
Created Time	2017-02-28 11:22:19
Modified Time	2017-02-28 11:22:19
First Inspection Date	2017-03-09 16:32:42
Inspection Start Time	2017-03-09 17:11:06
Inspection End Time	2017-03-09 17:11:11
Reacted Time	
Submitted Time	2017-03-09 17:11:11
Identical File	1File / 1User

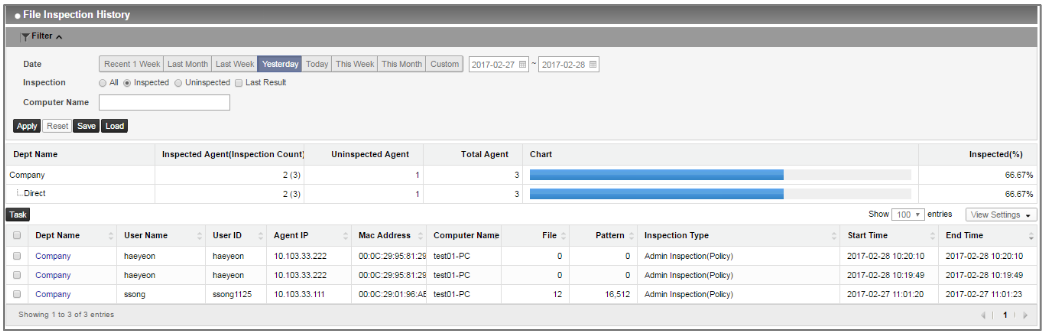
Pattern Information

ALL: Credit Card Number	200
ALL: E-Mail	100
ALL: Employee Code	122
ALL: IP Address	100
BR: Cadastro de Pessoa Fisica	100
MX: Numero de Seguro Social	100
US: Driver's License Number - AZ, CA, KS, MA, NE, OK, VA etc	50
US: Driver's License Number - DC, HI, NY, PA, SC, TX, UT etc	305
US: ICD 10 Code	22
US: Social Security Number	9
JP: MyNumber	216

(FIGURE 4-27) MEASURES ON FILE HISTORY SCREEN

- File Inspection History

File inspection history and inspection rate can be checked. Use the View Results button on the right end to check the inspection results.



● File Inspection History

Date: Yesterday, 2017-02-27 ~ 2017-02-28

Inspection: ○ All ● Inspected ○ Uninspected □ Last Result

Computer Name:

Dept Name	Inspected Agent(Inspection Count)	Uninspected Agent	Total Agent	Chart	Inspected(%)
Company	2 (3)	1	3		66.67%
└Direct	2 (3)	1	3		66.67%

Show 100 entries

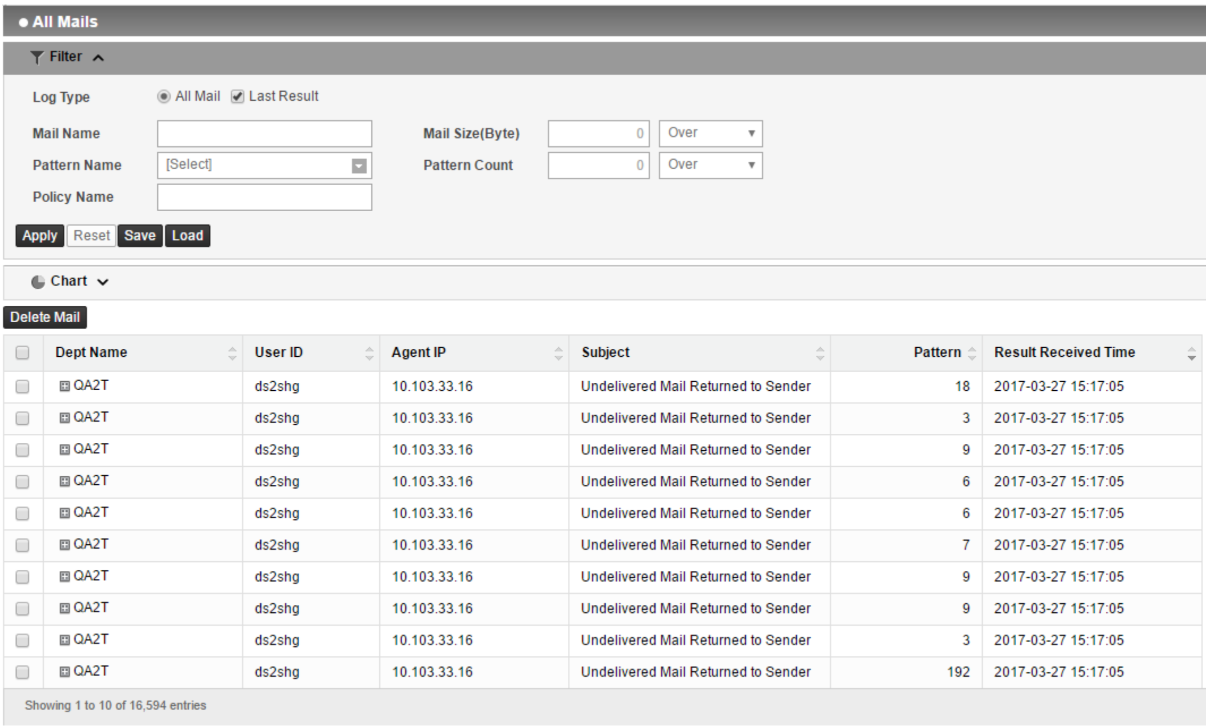
□	Dept Name	User Name	User ID	Agent IP	Mac Address	Computer Name	File	Pattern	Inspection Type	Start Time	End Time
□	Company	haeyeon	haeyeon	10.103.33.222	00:0C:29:95:81:29	test01-PC	0	0	Admin Inspection(Policy)	2017-02-28 10:20:10	2017-02-28 10:20:10
□	Company	haeyeon	haeyeon	10.103.33.222	00:0C:29:95:81:29	test01-PC	0	0	Admin Inspection(Policy)	2017-02-28 10:19:49	2017-02-28 10:19:49
□	Company	ssong	ssong1125	10.103.33.111	00:0C:29:01:96:AE	test01-PC	12	16,512	Admin Inspection(Policy)	2017-02-27 11:01:20	2017-02-27 11:01:23

Showing 1 to 3 of 3 entries

(FIGURE 4-28) FILE INSPECTION HISTORY SCREEN

- Final mail inspection

Detailed information on personal information mail can be viewed for the most recently inspected departments and users.



● All Mails

Log Type: ● All Mail ☑ Last Result

Mail Name:

Mail Size(Byte): 0 Over

Pattern Name: [Select]

Pattern Count: 0 Over

Policy Name:

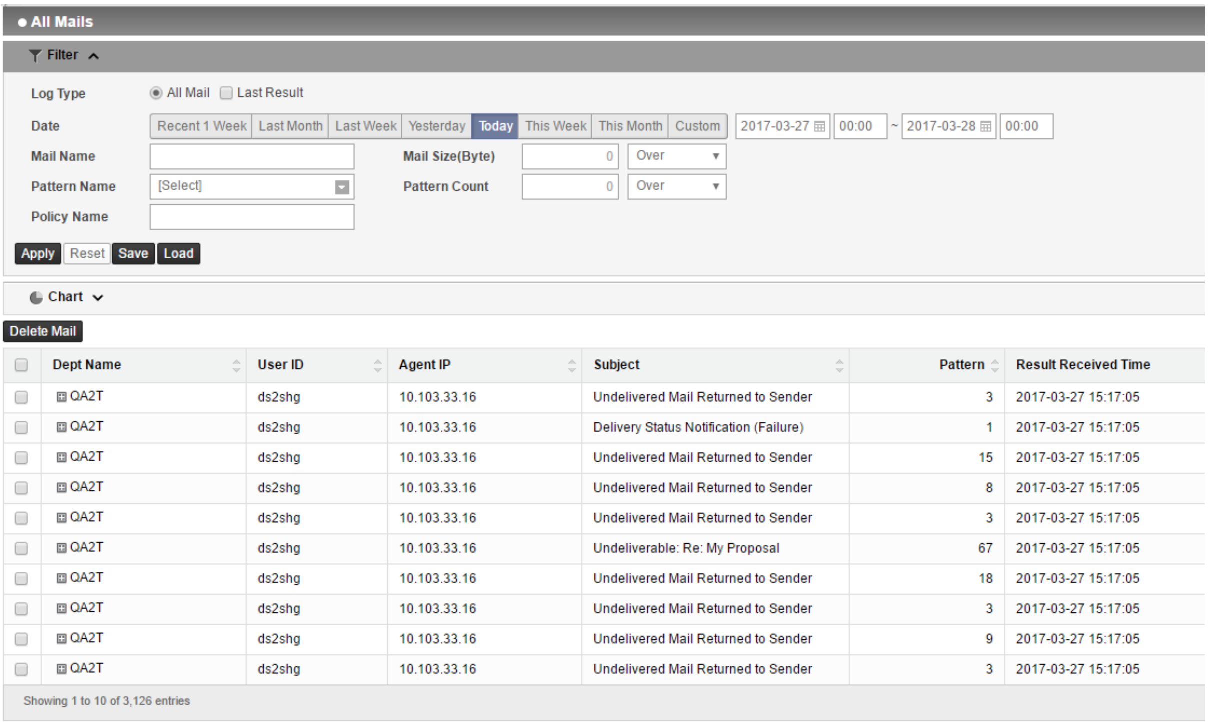
□	Dept Name	User ID	Agent IP	Subject	Pattern	Result Received Time
□	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	18	2017-03-27 15:17:05
□	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	3	2017-03-27 15:17:05
□	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	9	2017-03-27 15:17:05
□	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	6	2017-03-27 15:17:05
□	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	6	2017-03-27 15:17:05
□	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	7	2017-03-27 15:17:05
□	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	9	2017-03-27 15:17:05
□	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	9	2017-03-27 15:17:05
□	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	3	2017-03-27 15:17:05
□	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	192	2017-03-27 15:17:05

Showing 1 to 10 of 16,594 entries

(FIGURE 4-29) FINAL MAIL INSPECTION SCREEN

- Mail inspection

Detailed information of personal information files for the previously inspected departments and users can be viewed.



● All Mails

Filter

Log Type: ● All Mail ☐ Last Result

Date: Recent 1 Week | Last Month | Last Week | Yesterday | Today | This Week | This Month | Custom | 2017-03-27 | 00:00 ~ 2017-03-28 | 00:00

Mail Name:

Mail Size(Byte): 0 Over

Pattern Name: [Select]

Pattern Count: 0 Over

Policy Name:

Apply | Reset | Save | Load

Chart

Delete Mail

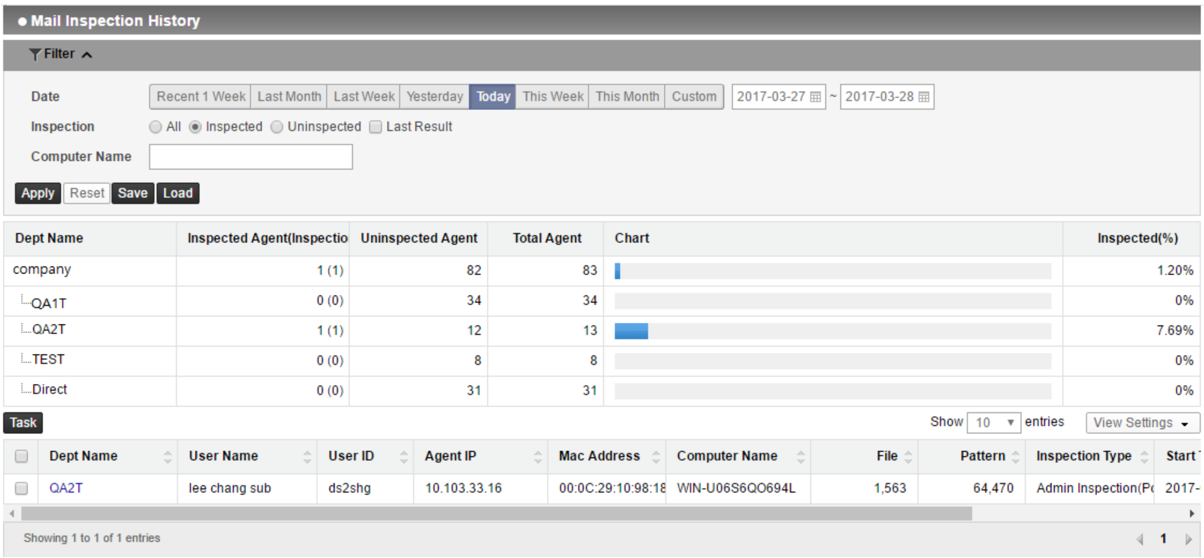
☐	Dept Name	User ID	Agent IP	Subject	Pattern	Result Received Time
☐	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	3	2017-03-27 15:17:05
☐	⊞ QA2T	ds2shg	10.103.33.16	Delivery Status Notification (Failure)	1	2017-03-27 15:17:05
☐	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	15	2017-03-27 15:17:05
☐	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	8	2017-03-27 15:17:05
☐	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	3	2017-03-27 15:17:05
☐	⊞ QA2T	ds2shg	10.103.33.16	Undeliverable: Re: My Proposal	67	2017-03-27 15:17:05
☐	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	18	2017-03-27 15:17:05
☐	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	3	2017-03-27 15:17:05
☐	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	9	2017-03-27 15:17:05
☐	⊞ QA2T	ds2shg	10.103.33.16	Undelivered Mail Returned to Sender	3	2017-03-27 15:17:05

Showing 1 to 10 of 3,126 entries

(FIGURE 4-30) MAIL INSPECTION SCREEN

- Mail inspection history

Mail inspection history and inspection rate can be checked. Inspected results can be viewed by using 'View results' button at the right end.



● Mail Inspection History

Filter

Date: Recent 1 Week | Last Month | Last Week | Yesterday | Today | This Week | This Month | Custom | 2017-03-27 ~ 2017-03-28

Inspection: ○ All ● Inspected ○ Uninspected ☐ Last Result

Computer Name:

Apply | Reset | Save | Load

Dept Name	Inspected Agent(Inspectio	Uninspected Agent	Total Agent	Chart	Inspected(%)
company	1 (1)	82	83		1.20%
QA1T	0 (0)	34	34		0%
QA2T	1 (1)	12	13		7.69%
TEST	0 (0)	8	8		0%
Direct	0 (0)	31	31		0%

Task

Show 10 entries | View Settings

☐	Dept Name	User Name	User ID	Agent IP	Mac Address	Computer Name	File	Pattern	Inspection Type	Start
☐	QA2T	lee chang sub	ds2shg	10.103.33.16	00:0C:29:10:98:18	WIN-U06S6QO694L	1,563	64,470	Admin Inspection(P	2017-

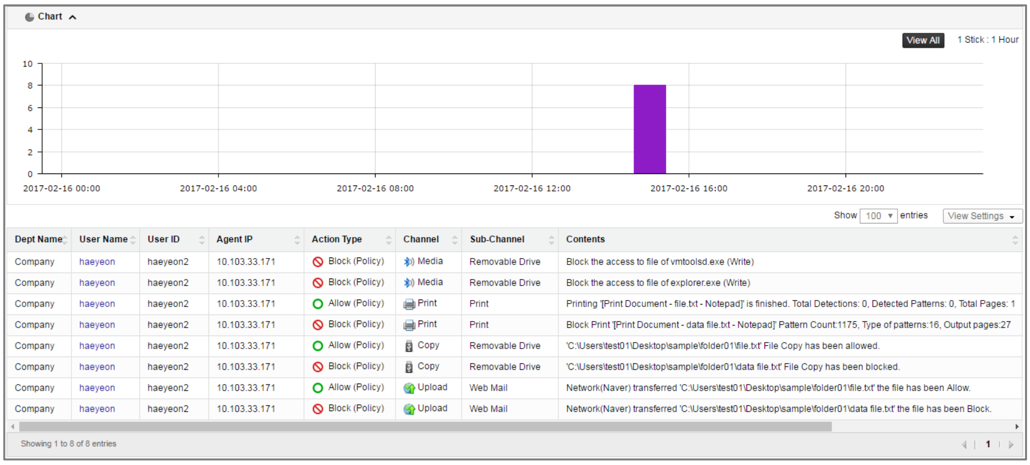
Showing 1 to 1 of 1 entries

1

(FIGURE 4-31) MAIL INSPECTION HISTORY SCREEN

4.3.2 Endpoint

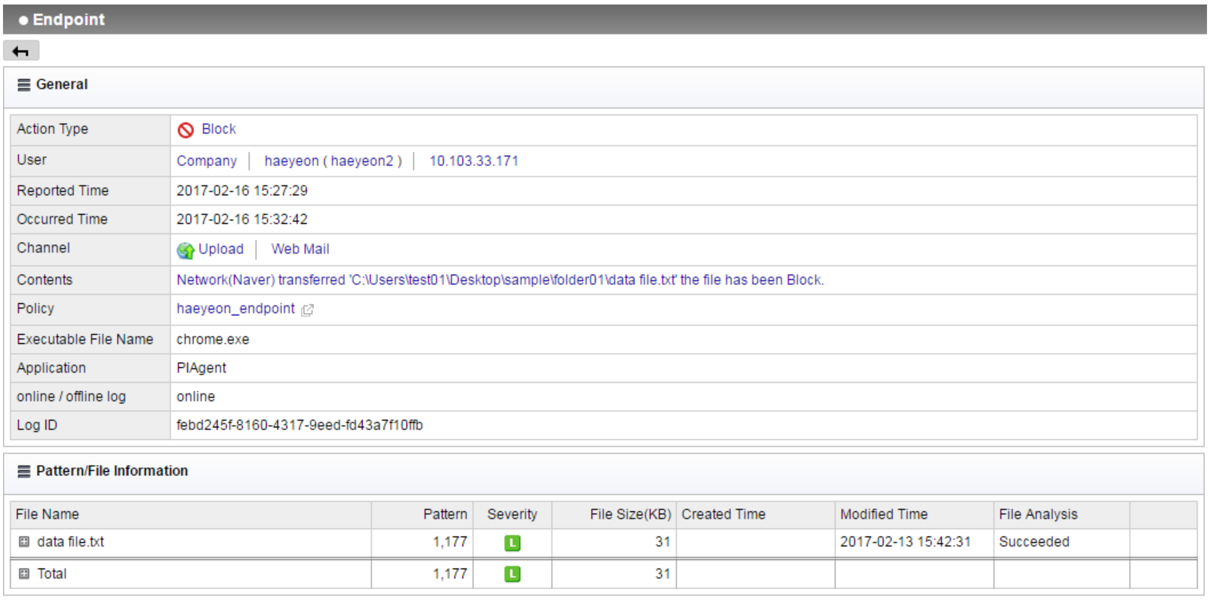
Displays an allowed or blocked file according to the channel and pattern conditions by a user or department. Through View Information, details of an exported file (Figure 4-21 above) can be viewed. By searching a similar file, files with the same confidential data based on a user can be viewed (Figure 4-32 below).



Dept Name	User Name	User ID	Agent IP	Action Type	Channel	Sub-Channel	Contents
Company	haeyeon	haeyeon2	10.103.33.171	Block (Policy)	Media	Removable Drive	Block the access to file of vmtoolsd.exe (Write)
Company	haeyeon	haeyeon2	10.103.33.171	Block (Policy)	Media	Removable Drive	Block the access to file of explorer.exe (Write)
Company	haeyeon	haeyeon2	10.103.33.171	Allow (Policy)	Print	Print	Printing '[Print Document - file.txt - Notepad]' is finished. Total Detections: 0, Detected Patterns: 0, Total Pages: 1
Company	haeyeon	haeyeon2	10.103.33.171	Block (Policy)	Print	Print	Block Print '[Print Document - data file.txt - Notepad]' Pattern Count:1175, Type of patterns:16, Output pages:27
Company	haeyeon	haeyeon2	10.103.33.171	Allow (Policy)	Copy	Removable Drive	'C:\Users\test01\Desktop\sample\folder01\file.txt' File Copy has been allowed.
Company	haeyeon	haeyeon2	10.103.33.171	Block (Policy)	Copy	Removable Drive	'C:\Users\test01\Desktop\sample\folder01\data file.txt' File Copy has been blocked.
Company	haeyeon	haeyeon2	10.103.33.171	Allow (Policy)	Upload	Web Mail	Network(Naver) transferred 'C:\Users\test01\Desktop\sample\folder01\file.txt' the file has been Allow.
Company	haeyeon	haeyeon2	10.103.33.171	Block (Policy)	Upload	Web Mail	Network(Naver) transferred 'C:\Users\test01\Desktop\sample\folder01\data file.txt' the file has been Block.

Showing 1 to 8 of 8 entries

(FIGURE 4-32) ENDPOINT DETAIL SCREEN



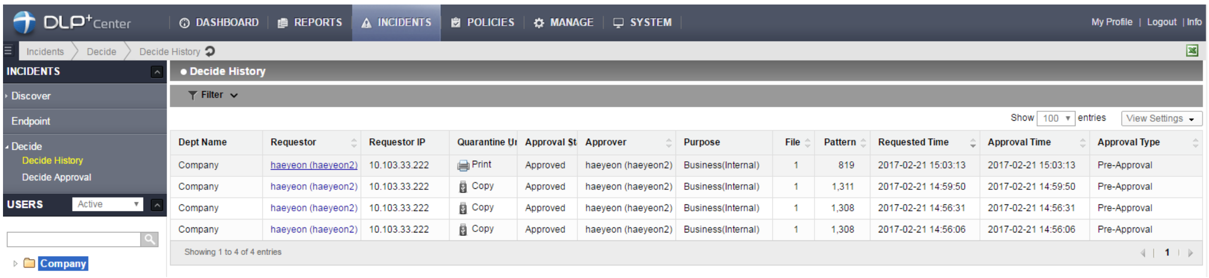
Action Type	Block
User	Company | haeyeon (haeyeon2) | 10.103.33.171
Reported Time	2017-02-16 15:27:29
Occurred Time	2017-02-16 15:32:42
Channel	Upload | Web Mail
Contents	Network(Naver) transferred 'C:\Users\test01\Desktop\sample\folder01\data file.txt' the file has been Block.
Policy	haeyeon_endpoint
Executable File Name	chrome.exe
Application	PIAgent
online / offline log	online
Log ID	febd245f-8160-4317-9eed-fd43a7f10ffb

File Name	Pattern	Severity	File Size(KB)	Created Time	Modified Time	File Analysis	
data file.txt	1,177	L	31		2017-02-13 15:42:31	Succeeded	
Total	1,177	L	31				

(FIGURE 4-33) SCREEN OF RESULTS OF ALLOWED FILES (ABOVE) AND DETAILED INFORMATION (BELOW)

4.3.3 Decide

Details of approvals such copy, upload, print, forced decoding, period extension, file save, release of separation, etc. can be checked by applying filters. Also, it is possible to check the information on delegation of decides.



Dept Name	Requestor	Requestor IP	Quarantine Ur	Approval St	Approver	Purpose	File	Pattern	Requested Time	Approval Time	Approval Type
Company	haeyeon (haeyeon2)	10.103.33.222	Print	Approved	haeyeon (haeyeon2)	Business(Internal)	1	819	2017-02-21 15:03:13	2017-02-21 15:03:13	Pre-Approval
Company	haeyeon (haeyeon2)	10.103.33.222	Copy	Approved	haeyeon (haeyeon2)	Business(Internal)	1	1,311	2017-02-21 14:59:50	2017-02-21 14:59:50	Pre-Approval
Company	haeyeon (haeyeon2)	10.103.33.222	Copy	Approved	haeyeon (haeyeon2)	Business(Internal)	1	1,308	2017-02-21 14:56:31	2017-02-21 14:56:31	Pre-Approval
Company	haeyeon (haeyeon2)	10.103.33.222	Copy	Approved	haeyeon (haeyeon2)	Business(Internal)	1	1,308	2017-02-21 14:56:06	2017-02-21 14:56:06	Pre-Approval

Showing 1 to 4 of 4 entries

(FIGURE 4-34) DECIDE SCREEN

4.4 Policy

Policy Management is divided into Discover and Endpoint. Discover manages the policy to inspect the status of retaining confidential data in the PC, and Endpoint manages the policy to control the flow of confidential data in the PC to external channels.

4.4.1 Default Policy

After the initial Installation and before the login, default policy is configured, and all activities with configured policy are blocked and audit logs are recorded. [TABLE 4-5] below shows the list of processes blocked by default.

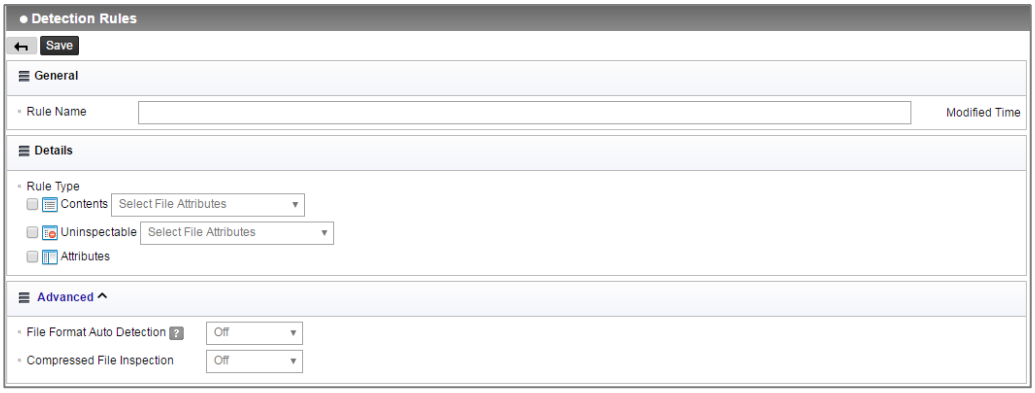
[TABLE 4-4] DEFAULT POLICY

Category	State	Target	Note
Copy Prevent+	Block	All files	Not context-aware blocking
Upload Prevent+	Block	All files	Not context-aware blocking
Print Prevent+	Block	All files	Not context-aware blocking
Clipboard Control	Block files with personal information detected Allow files with personal information not detected	NateOn, Kakao Talk	Context-aware blocking (5 patterns or more by default)
Application Control	Block	Anti-Rootkit, etc.	Block / allow based
Media Control	Block	All channels	Block / allow based

4.4.2 Detect

4.4.2.1 Detection Rules

Detection Rule to be used in Discover, Prevent+ Policy can be set. To create a Detection Rule, "File Attribute" policy is required, and can be set based on Content, Uninspectable and Attribute. Attribute Policy can be viewed in the "Policies > Detect > File Attribute".



Rule Name
Modified Time

Rule Type
□ Contents Select File Attributes ▾
□ Uninspectable Select File Attributes ▾
□ Attributes

File Format Auto Detection ? Off ▾
Compressed File Inspection Off ▾

(FIGURE 4-35) DETECTION RULE SETTINGS SCREEN

☞ Descriptions on policy items

① Contents: Detects based on the selected "File Attribute", Data Pattern and Number of Detection. During admin inspection, the results are shown in "Contents".

② Uninspectable: "Unapproved Encryption File" can be selected. During admin inspection, the results are shown in "Uninspectable" for an encrypted document or a compressed file.

③ Attribute: Detects based on the selected Policy in "File Attribute", not personal information inspection. During admin inspection, the results are shown in "Attribute".

④ Auto-detection of file type: All files except the “File Format” defined in Privacy-i are inspected, and, for manipulated files, detection and manipulation of files are informed. It should be noted that, if the corresponding options are run, it takes longer than the conventional inspections.

⑤ Compressed file inspection: Compressed files can be inspected, and it is possible to configure multi-staged compressed files and the size of compressed files.

⑥ Security drive area inspection: When security area has been set to a specific drive (e.g. S:\) in the network drive connected to the user PC, it is possible to decide whether to inspect the area for personal information.

⑦ Cloud area inspection: Used when inspecting files in the drive connected to a network.

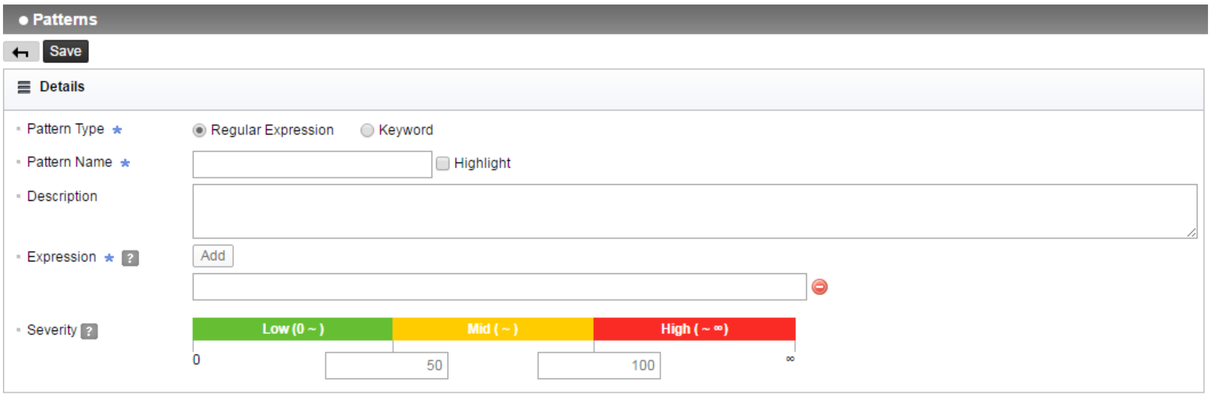
☞ Effective Input Field Range

[TABLE 4-5] DETECTION RULES EFFECTIVE INPUT FIELD RANGE

Item	Effective range	Character
Rule name	1~120	Numbers, upper or lower case letters, special characters

4.4.2.2 Patterns

Default pattern of confidential data provided by Somansa can be checked in ‘Patterns’. There are total of 13 types, which are resident registration number, foreigner registration number, driver’s license number, credit card number, social security number, passport, account number, mobile phone number, telephone number, IP address, E-mail address, corporate registration number, business registration number. When detecting for phrases or specific patterns, user defined patterns can be generated. Default pattern cannot be deleted, and the expressions cannot be modified or deleted. Patterns are used when generating inspection policies in Policy Management in Discover.



Pattern Type ★ ● Regular Expression ○ Keyword

Pattern Name ★ □ Highlight

Description

Expression ★

Severity: Low (0 ~) | Mid (~) | High (~ ∞) — 0, 50, 100, ∞

(FIGURE 4-36) PATTERN REGULAR EXPRESSION DETAILS SCREEN

☞ Descriptions on policy items

① Pattern type: Configures with regular expressions and keyword inspection method.

② Pattern name: Names can be designated in generating patterns.

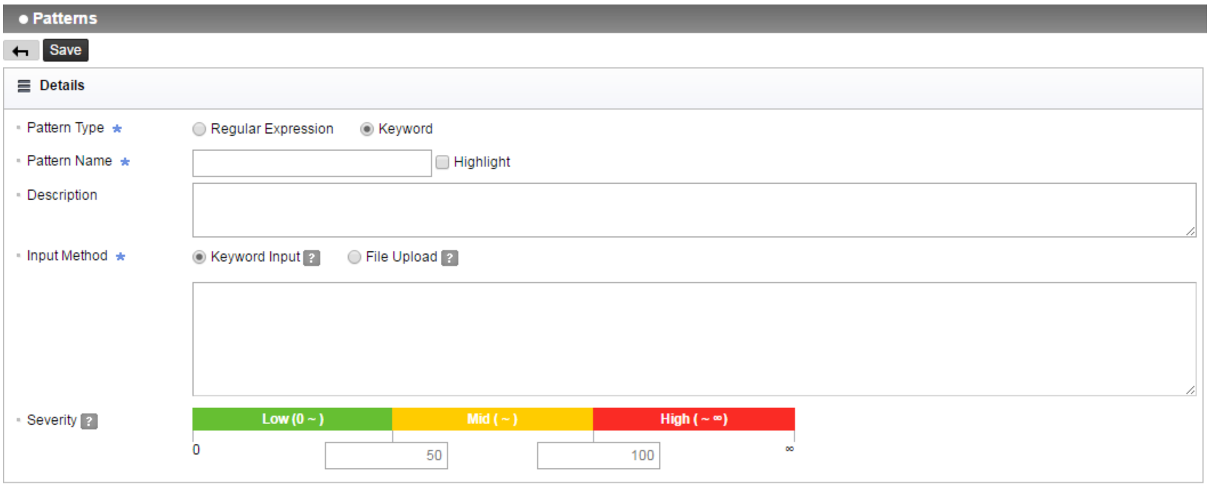
③ Description: Additional descriptions on the pattern can be recorded.

④ Expression: Configures the patterns to be detected through general keywords or regular expressions.

⑤ Effectiveness inspection: Default effectiveness inspection and additional effectiveness inspection can be designated for regular expressions.

⑥ Pattern count: Sets whether duplicated patterns will be included.

⑦ Severity rate settings: Sets severity rate in detecting patterns.



Pattern Type ★ ○ Regular Expression ● Keyword

Pattern Name ★ □ Highlight

Description

Input Method ★ ● Keyword Input ? ○ File Upload ?

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

0 50 100 ∞

(FIGURE 4-37) PATTERN REGULAR EXPRESSION DETAILS SCREEN

① Input method: Configures keyword input and file upload methods.

☞ Effective Input Field Range

[TABLE 4-6] PATTERN EFFECTIVE INPUT FIELD RANGE

Item	Effective range	Character	Failure message
Pattern name	3~225	Numbers, upper or lower case letters, special characters	Pattern name should include 3 or more characters.
Description	1~225	Numbers, upper or lower case letters, special characters	-
Expression	1~200	Numbers, upper or lower case letters, special characters	EXPRESSION cannot include spaces.
Set degree of danger	0~999,999,999	Numbers	0 cannot be input to setting degree of danger.

4.4.2.3 File Format

The formats to be used in the file attribute can be managed.

* Note that unsupported file formats are not detected, and no logs are retained.

[TABLE 4-7] DEFAULT INSPECTION FORMAT FILE

No.	File type	Format	Format name	Extensions
1	Text	Default format	Copy of Print 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 value	csv
7			General text	txt
8	Word processor	Default format	iWork Pages	pages
9			Corel WordPerfect	wpd;wp;wp4;wp5;wp6;wp7
10			OpenOffice Writer	odt;sxw
11			Hangul and Computer Hangul	hwp
12			HandySoft Arirang	hwd
13			Microsoft Word	doc;docx
14	Spreadsheet	Default format	iWork Numbers	numbers
15			OpenOffice Calc	ods;sxc
16			Microsoft Excel	xls;xlsx;xlsm
17	Presentation	Default format	Hancom Office HanShow	show
18			iWork Keynote	key
19			OpenOffice Impression	odp;sxi
20			Microsoft PowerPoint	ppt;pptx;pps
21	E-mail	Default format	Microsoft Outlook Express	eml;mht
22			Microsoft Outlook	msg;oft
23	Database	Default format	Microsoft Access	mdb;accdb
24	Others	Default format	XML Paper Specification	xps
25			Microsoft Compiled HTML	chm
26			Adobe Portable Document Format	pdf

☞ Descriptions on policy items

① File type: Expressed file types can be selected, and, if direct adding the type is required, it is possible to input the file type a user wants.

② File extension: Desired file extension can be input when detecting files. The extensions provided by default are described in [TABLE 4-7].

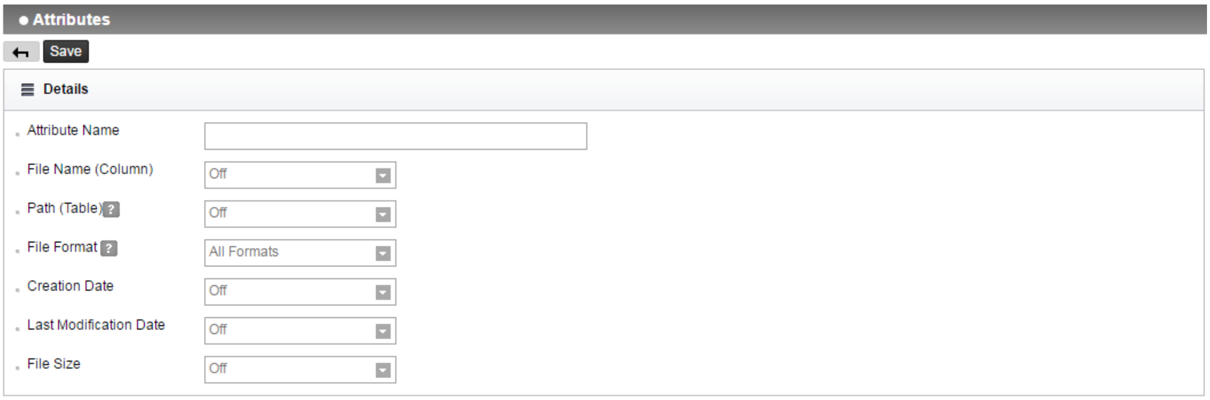
☞ Effective Input Field Range

[TABLE 4-8] FILE FORMAT EFFECTIVE INPUT FIELD RANGE

Item	Effective range	Character	Failure message
Format name	1~225	Numbers, upper or lower case letters, special characters	Input format name.
Extensions	1~20	Letters	Space cannot be registered to the file type.

4.4.2.4 File Attributes

Conditional values of attributes of files to be inspected can be designated in 'File Attribute'. Inspection can be performed according to the name, path, type, creation date and size of the file, and at least one condition should be selected to generate a policy. Each condition satisfies AND condition, and files are detected according to the settings of each item. Generated file attributes are used in Discover of Policy Management to generate inspection policies.


● Attributes

Save

Details

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

(FIGURE 4-38) DETIALS OF FILE ATTRIBUTES

☞ Descriptions on policy items

① File name designation: Space for inputting file name is enabled when selected as 'Use', and targets for inclusion and exclusion can be selected. The name of the file to be detected (excluded) can be input. The file name should be input including the extension.

② Path designation: Space for inputting path name is enabled when selected as 'Use', and targets for inclusion and exclusion can be selected. The name of the path to be detected (excluded) can be input.

③ File format designation: All formats can be selected or directly designated. If direct designation is selected, the formats listed in [TABLE 4-21] can be selected.

④ Designation of creation date: Space for inputting date is enabled when selected as 'Use', and the creation date to be detected can be selected.

⑤ Finally modified date: Space for inputting date is enabled when selected as 'Use', and the modified creation date to be detected can be selected.

⑥ Designation of size: Space for inputting size is enabled when selected as 'Use', and the size of the file to be detected can be selected. The sizes are divided into minimum and maximum, and can be selected.

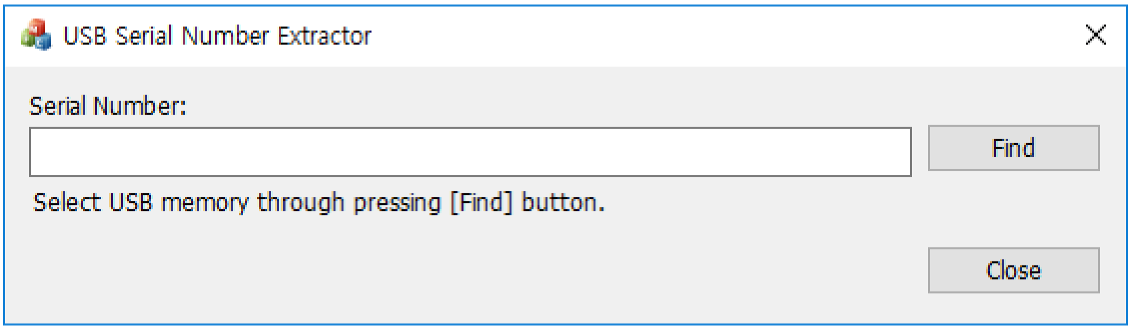
☞ Effective Input Field Range

[TABLE 4-8] FILE ATTRIBUTE EFFECTIVE INPUT FIELD RANGE

Item	Effective range	Character	Failure message
Name	3~225	Numbers, upper or lower case letters, special characters	The name should include 3 or more characters.

4.4.2.5 USB Management

USB registration management provides the function of registering the usable media such as portable disks or USB that are allowed to use in the company. USB Serial number is extracted by using a USB Serial number extractor, and the serial number can be registered in USB Management screen.

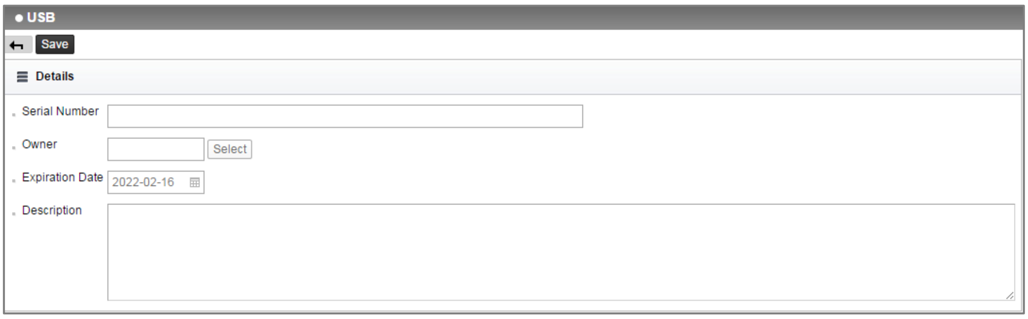


USB Serial Number Extractor

Serial Number:

Select USB memory through pressing [Find] button.

(FIGURE 4-39) USB SERIEAL NUMBER EXTRACTOR



Serial Number

Owner

Expiration Date 2022-02-16

Description

(FIGURE 4-40) USB REGISTRATION SCREEN

☞ Descriptions on policy items

① Serial number: Input the USB Serial number extracted by using a USB Serial number extractor.

② Administrator: The person to manage the USB to be registered can be selected, and the person should be registered in “MANAGE > Users” for selection.

③ Purpose: The purpose of USB to be registered for business or personal use can be selected.

④ Expiring date: Expiration date of USB to be registered can be selected.

☞ Effective Input Field Range

[TABLE 4-9] USB MANAGEMENT EFFECTIVE INPUT FIELD RANGE

Item	Effective range	Character	Failure message
Serial number	5~60	upper or lower case letters, special characters	Serial number should include 5 or more characters.
Description	1~1024	Numbers, upper or lower case letters, special characters	-

4.4.2.6 Applications

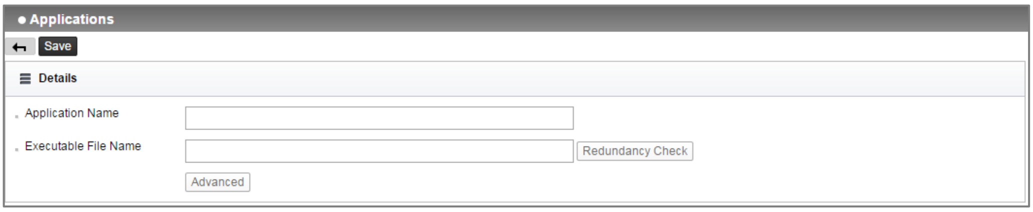
Applications are managed. Privacy-i provides, by default, blocking of executions of processes that can abnormally change the operations of Agent or the processes that can lead to leakage to outside in a user PC such as Anti-RootKit, Sysinternal, etc. When operating the product, the programs that should not be executed are prevented from running through the corresponding functions. [TABLE 4-12] below shows the list of processes to be blocked from execution by default.

[TABLE 4-10] DEFAULT APPLICATIONS

Name	Execution file name
ucloud2	ucloud2.exe
(AnalysisTools) ProcessHacker	ProcessHacker.exe
(RootKit) aswMBR	aswMBR.exe
(RootKit) autoruns	autoruns.exe
(RootKit) CheatEngine 32bit	cheatengine-i386.exe
(RootKit) CheatEngine 64bit	cheatengine-x86_64.exe
(RootKit) cureit	cureit.exe
(RootKit) Directory Snoop FAT	DS_FAT.exe
(RootKit) Directory Snoop NTFS	DS_NTFS.EXE
(RootKit) gmer	gmer.exe
(RootKit) IceSword	IceSword.EXE
(RootKit) KernelDetective	KernelDetective.exe
(RootKit) mstsc 32bit	mstsc.exe
(RootKit) Pchunter 32bit	PCHunter32.exe

(RootKit) Pchunter 64bit	PCHunter64.exe
(RootKit) RootkitRevealer	RootkitRevealer.exe
(RootKit) Spy Hunter	SpyHunter4.exe
(RootKit) SystemExplorer	SystemExplorer.exe
(RootKit) TDSSKiller	TDSSKiller.exe
(RootKit) Tuluka_v1.0.394.77.exe	Tuluka_v1.0.394.77.exe
(RootKit) Unhackme	Unhackme.exe
(RootKit) Unlocker	Unlocker.exe
Sophos Anti-Rootkit	sargui.exe
HitmanPro	HitmanPro.exe
Malwarebytes Anti-Rootkit	mbar.exe
McAfee Rootkit Remover	rootkitremover.exe
Norton Power Eraser	NPE.exe
Trend Micro RootkitBuster	Trend_Micro_RootkitBusterV5.0-1180.exe Trend_Micro_RootkitBusterV5.0-1180x64.exe
Vba32 AntiRootkit	Vba32arkit.exe
Bitdefender Rootkit Remover	bitdefender_BootkitRemoval_x86.exe bitdefender_BootkitRemoval_x64.exe
Powertool	PowerTool.exe PowerTool32.exe PowerTool64.exe
RogueKiller	RogueKiller.exe
RogueKillerCMD	RogueKillerCMD.exe
Radix Anti-Rookit	radixgui.exe
Comodo Cleaning Essentials	CCE.exe
Comodo Autorun Analyzer	Autoruns.exe
Comodo KillSwitch	KillSwitch.exe
OSHI Unhooker	OSHI Unhooker.exe
Tizer Rootkit Razor	RootkitRazor.exe
Panda Free Antivirus	PSUAMain.exe
KillProcess	KillProcess.exe
Ultimate Process Killer	Ultimate_Process_Killer_2.0.2.exe
Daphne v2.04	Daphne.exe
(Sysinternals) procexp	procexp.exe
(Sysinternals) procmon	procmon.exe
(Sysinternals) pskill	pkill.exe
(Sysinternals) pslist	pslist.exe
(Sysinternals) VirtualBox	VirtualBox.exe
(Sysinternals) Vitual PC 2007	Vitual PC.exe
(Sysinternals) Vitual PC 2007	geek.exe
(Sysinternals) vmrun	vmrun.exe

(Sysinternals) vmware	vmware.exe
(Sysinternals) vmware tray	vmware-tray.exe
(Sysinternals) vmware vmx	vmware-vmx.exe
MicorSoft WORD	WINWORD.EXE
N Drove Explorer	ndrive.exe
Tor Browser	vidalia.exe
ucloud2-2	ucloudUpload.exe
UltraSurf	ultrasurf.exe
NateOn	NateOnMain.exe
NotePad	notepad.exe
Samsung Kies	kies.exe
Apple iTunes	itunes.exe
Kakao Talk PC Messenger	KakaoTalk.exe
File Guri	fileguri.exe



(FIGURE 4-41) PROGRAM NAME REGISTRATION SCREEN

☞ Descriptions on policy items

① Execution file name: Execution files that a user wants to execute in addition to basic applications can be input.

② Designation of binary search words: Appears when 'Advanced Settings' is clicked, and allows inputting binary of the execution file.

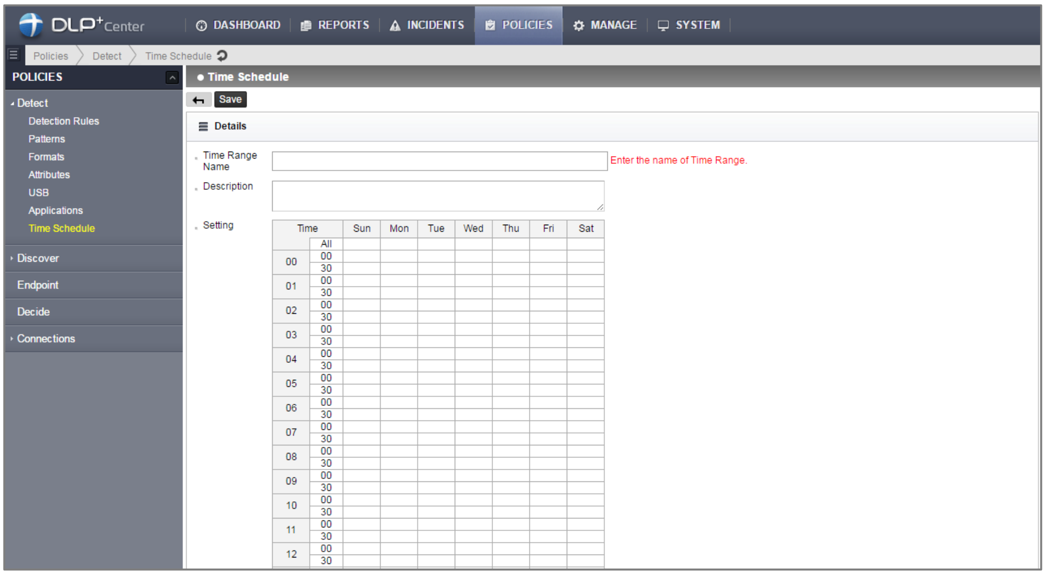
☞ Effective Input Field Range

[TABLE 4-11] EFFECTIVE INPUT FIELD RANGE OF APPLICATIONS

Item	Effective range	Character	Failure message
Name	3~255	Numbers, upper or lower case letters, special characters	The name should include 3 or more characters.
Description	1~255	Numbers, upper or lower case letters, special characters	-

4.4.2.7 Time Range

When adding a server Discover policy, the time frames used for 'Exceptional Time Range Settings' function can be added, modified or deleted.



Time Range Name: Enter the name of Time Range.

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							

(FIGURE 4-42) ADD TIME FRAME SCREEN

☞ Descriptions on policy items

① Time range name: The name of the time range to be added can be designated.

② Description: Descriptions on the time range can be input.

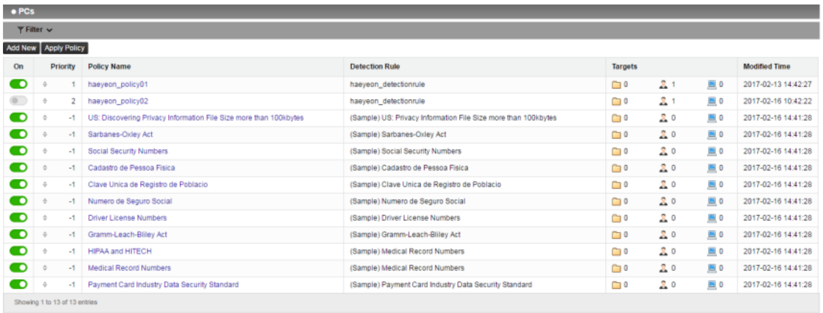
③ Time range settings: The time frame to be set can be configured by dragging a mouse. Settings can be made for every 30 minutes. If the entire day of week (column), or all day of the week in designated time frame (row) are to be selected, select the front area of the column or row.

4.4.3 Discover

Discover provides the function to manage the policy to be used for inspecting confidential data retained in a PC.

4.4.3.1 PC

The policy used when inspecting confidential data retained in a user PC. Confidential Data Inspection Policy is categorized into a part to create a policy and a part to set a pattern. In the part to set a policy, a basic pattern and policy name can be set. In the part to set a pattern, a user-defined pattern other than the basic pattern can be added, or an expiration date of pattern can be added or modified. Click the policy on the list to see Policy Name / Modified Time / Number of Set Data Patterns at the bottom of the window. Please refer to below tables for a description of each setting.



● PCs

On	Priority	Policy Name	Detection Rule	Targets			Modified Time
●	1	haeyeon_policy01	haeyeon_detectionrule	0	1	0	2017-02-13 14:42:27
○	2	haeyeon_policy02	haeyeon_detectionrule	0	1	0	2017-02-16 10:42:22
●	-1	US: Discovering Privacy Information File Size more than 100kbytes	(Sample) US: Privacy Information File Size more than 100kbytes	0	0	0	2017-02-16 14:41:28
●	-1	Sarbanes-Oxley Act	(Sample) Sarbanes-Oxley Act	0	0	0	2017-02-16 14:41:28
●	-1	Social Security Numbers	(Sample) Social Security Numbers	0	0	0	2017-02-16 14:41:28
●	-1	Cadastro de Pessoa Fisica	(Sample) Cadastro de Pessoa Fisica	0	0	0	2017-02-16 14:41:28
●	-1	Clave Unica de Registro de Poblacio	(Sample) Clave Unica de Registro de Poblacio	0	0	0	2017-02-16 14:41:28
●	-1	Numero de Seguro Social	(Sample) Numero de Seguro Social	0	0	0	2017-02-16 14:41:28
●	-1	Driver License Numbers	(Sample) Driver License Numbers	0	0	0	2017-02-16 14:41:28
●	-1	Gramm-Leach-Bliley Act	(Sample) Gramm-Leach-Bliley Act	0	0	0	2017-02-16 14:41:28
●	-1	HIPAA and HITECH	(Sample) Medical Record Numbers	0	0	0	2017-02-16 14:41:28
●	-1	Medical Record Numbers	(Sample) Medical Record Numbers	0	0	0	2017-02-16 14:41:28
●	-1	Payment Card Industry Data Security Standard	(Sample) Payment Card Industry Data Security Standard	0	0	0	2017-02-16 14:41:28

Showing 1 to 13 of 13 entries

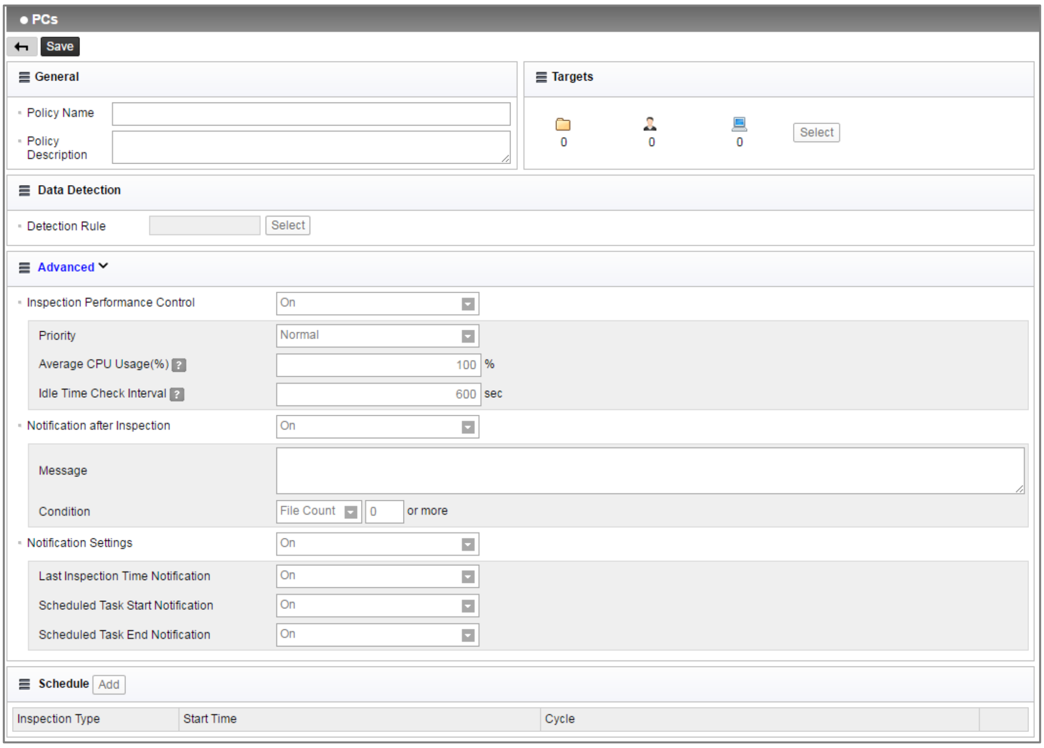
(FIGURE 4-43) DISCOVER POLICY LIST

☞ Descriptions on policy items

[TABLE 4-12] CONFIDENTIAL DATA INSPECTION OPTION SETTINGS

Category	Target	Description
Inspection speed settings	Inspection speed settings	Whether to set inspection speed
	Priority of inspection tasks	High, Medium, Low
	Average CPU use rate (%)	Sets CPU resources for inspection
	Idle time check interval (sec)	Uses maximum CPU resource in inspection when there is no mouse or keyboard input
Actions when inspection terminates	Automatic encryption	After inspection results, encryption is performed for all detected files. Type of encryption is Privacy-i encryption
	Guide message	When inspection terminates, the person with authority sets the guide message in person
	Criteria for exposing messages	The number of detected patterns/files is set as the settings option of the guide message
Notification settings	Auto-notification of last inspection time	Uses notification message when the last inspection terminates among multiple central inspections
	Notification of start of scheduled task	Uses notification message when scheduled inspection starts
	Notification of end of scheduled task	Uses notification message when scheduled inspection ends
Use masking for detection results	-	Whether to use masking for detection results
Use real time inspection	-	Whether to use real time inspection by the person with authority
Schedule settings	Inspection type	Inspection type, whose type is file inspection

	Starting date	Inspection starting date
	Starting time	Inspection starting time
	Interval	Inspection interval, the type being perform once, every day, every week, every month



● PCs

Save

General
- Policy Name
- Policy Description

Targets
0 0 0 Select

Data Detection
- Detection Rule Select

Advanced
- Inspection Performance Control: On
  - Priority: Normal
  - Average CPU Usage(%): 100 %
  - Idle Time Check Interval: 600 sec
- Notification after Inspection: On
  - Message
  - Condition: File Count 0 or more
- Notification Settings: On
  - Last Inspection Time Notification: On
  - Scheduled Task Start Notification: On
  - Scheduled Task End Notification: On

Schedule Add

Inspection Type	Start Time	Cycle

(FIGURE 4-44) DISCOVER POLICY DETAILS SCREEN

☞ Descriptions on the items

① Detection Rule: Runs a personal information inspection, based on the registered policy in the "Detection Rules".

② Inspection Speed Control Function: The resource of the system can be specified for the process running inspection on the Agent PC during remote inspection. The setting for details is available when this function is set to 'Use'.

- Inspection Task Priority: Priority for the running process can be specified.
- Average CPU utilization allocated to inspection: CPU utilization of the running process can be set when running an inspection.
- Idle Time Check Interval: If an idle time set by a user PC has passed, the CPU utilization of the process becomes 100%. Inspection speed is improved through resources of the system that are not used during idle time.

③ Automatic encryption when an inspection terminates: After performing a remote inspection, Privacy-i encryption is performed for all detected files (contents, uninspectable). Encrypted files are encoded to .pia extension.

④ Guide message when terminating inspection: A guide message can be provided to a user PC when remote inspection is completed. The message is displayed according to a set pattern or number of files.

⑤ Notification settings: Provides a notification window in the lower right corner when remote inspection is completed. The settings for detailed items are available when this function is set to 'Use'.

- Notification for last inspection date: Displays the last inspection date.
- Notification for starting inspection date: Notifies start of inspection to the Agent PC when scheduled task starts.
- Notification for terminating inspection date: Notifies termination of inspection to the Agent PC when scheduled task terminates.

⑥ Use of masking to detection results: Masking is applied to detected personal information pattern in 'View Detail' for detected personal information, and displayed on UI.

⑦ Use of real time inspection: When the phrases saved in a user PC is created or saved after changing, the personal information is notified to a user through a notification message.

☞ Effective Input Field Range

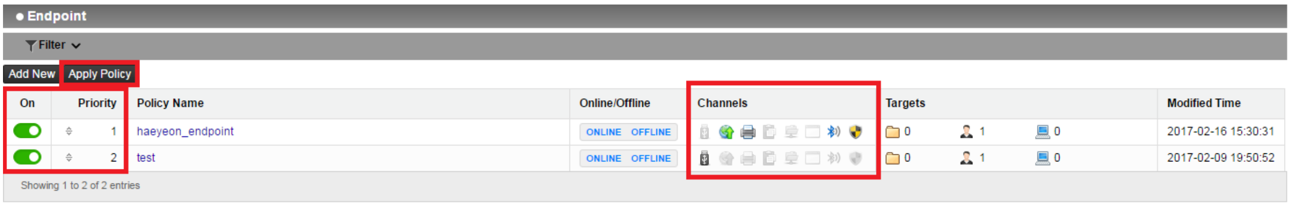
[TABLE 4-13] EFFECTIVE INPUT FIELD RANGE OF POLICY PC

Item	Effective range	Character	Failure message
Policy name	1~120	Numbers, upper or lower case letters, special characters	Enter policy name.
Average CPU use allocated for inspection	0~100	Numbers	Only numbers between 10 and 100 can be entered.
Period of checking idle times	0~999	Numbers	Number less than 1 cannot be entered.

4.4.4 Endpoint

In the Endpoint, a policy can be defined for controlling channels that can communicate externally, such as removable storage devices, communication media, printers, application programs, networks, etc. A policy that logs or blocks when a user transfers a confidential file externally can be specified. A leak of important company information can be prevented in advance.

Policy can be added in Policies > Endpoint.



● Endpoint

Filter

Add New | Apply Policy

On	Priority	Policy Name	Online/Offline	Channels	Targets			Modified Time
●	1	haeyeon_endpoint	ONLINE OFFLINE		0	1	0	2017-02-16 15:30:31
●	2	test	ONLINE OFFLINE		0	1	0	2017-02-09 19:50:52

Showing 1 to 2 of 2 entries

(FIGURE 4-45) ENDPOINT POLICY SETTINGS

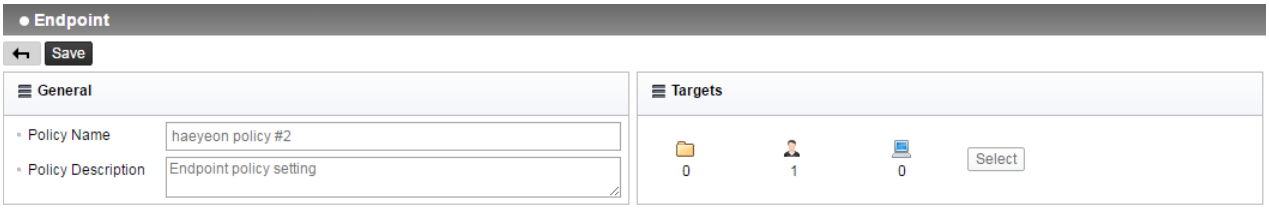
There are three parts in general.

A. The policy will be applied only when "Apply Policy" button is clicked after completing the generation of the policy.

B. Generated policies can be managed through on / off functions, and multiple policy settings are possible to one Agent depending on the policy priority.

C. For the target channel designated for each Endpoint policy, user convenience is provided by setting to disable in the case of "Pass", and to enable in the case of "Control".

1) Add New
Policy name and policy description can be designated, and the designation is possible by classifying into department, user and PC in the target.



● Endpoint

Save

General

- Policy Name: haeyeon policy #2
- Policy Description: Endpoint policy setting

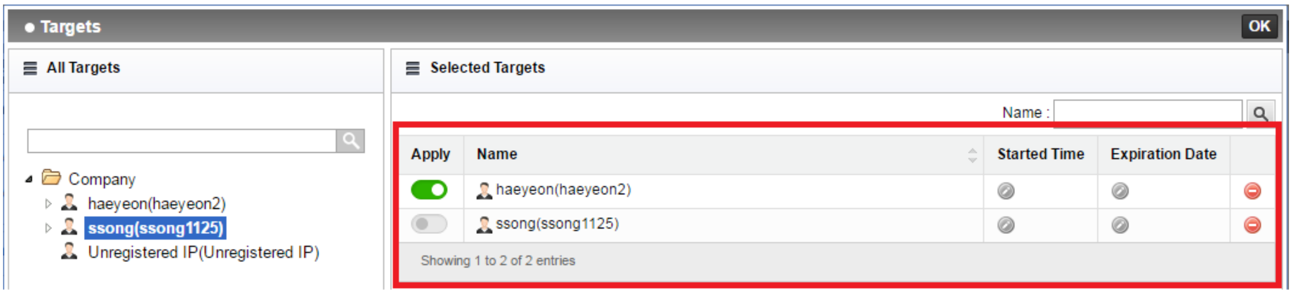
Targets

0 1 0

Select

(FIGURE 4-46) ENDPOINT POLICY GENERATION GENERAL AND APPLICATION TARGET SCREEN

Also, in the case of application targets, the function of application can be set to on/off so that on/off function can be provided when those using the policy can release the policies without deleting them.



- Company
  - haeyeon(haeyeon2)
  - ssong(ssong1125)
  - Unregistered IP(Unregistered IP)

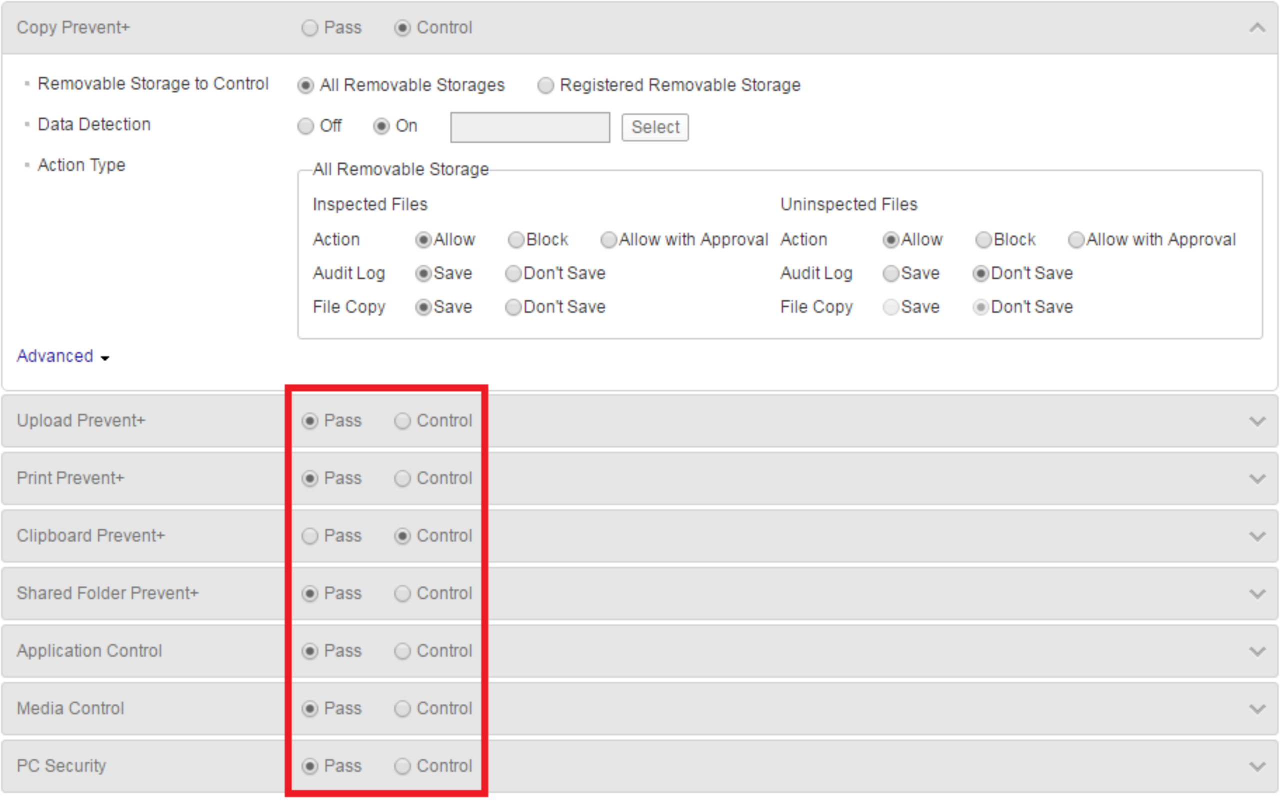
Apply	Name	Started Time	Expiration Date	
On	haeyeon(haeyeon2)			
Off	ssong(ssong1125)			

Showing 1 to 2 of 2 entries

(FIGURE 4-47) ON/OFF FUNCTION FOR APPLICATION TARGET

2) Control target channel

The control target channel can generate all policies in one policy as shown in Figure. The policy settings screen is the same as the above Privacy-i V6.0. The option of "Pass" in Details Settings means it is excluded in the policy, and selecting the option of "Control" enables generation of policy.



Copy Prevent+ ○ Pass ● Control

- Removable Storage to Control: ● All Removable Storages ○ Registered Removable Storage
- Data Detection: ○ Off ● On [Select]
- Action Type

All Removable Storage

Inspected Files				Uninspected Files			
Action	● Allow	○ Block	○ Allow with Approval	Action	● Allow	○ Block	○ Allow with Approval
Audit Log	● Save	○ Don't Save		Audit Log	○ Save	● Don't Save	
File Copy	● Save	○ Don't Save		File Copy	○ Save	● Don't Save	

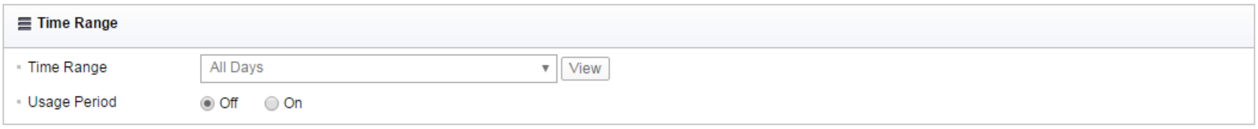
Advanced ▾

Upload Prevent+	● Pass	○ Control
Print Prevent+	● Pass	○ Control
Clipboard Prevent+	○ Pass	● Control
Shared Folder Prevent+	● Pass	○ Control
Application Control	● Pass	○ Control
Media Control	● Pass	○ Control
PC Security	● Pass	○ Control

(FIGURE 4-48) CONTROL TARGET CHANNEL

3) Time Range settings

Time Range policy settings are possible according to the policy generated at Policies > Detect > Time Range policy.



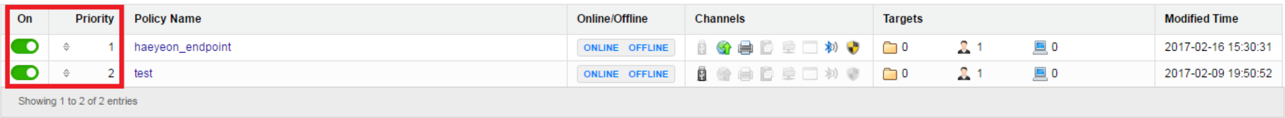
Time Range

- Time Range: All Days ▾ View
- Usage Period: ● Off ○ On

(FIGURE 4-49) TIME RANGE SETTINGS

When term of use is set, the policy will be reflected to the policy of the Agent at the set date and time as shown in Figure.

4) Policy priorities

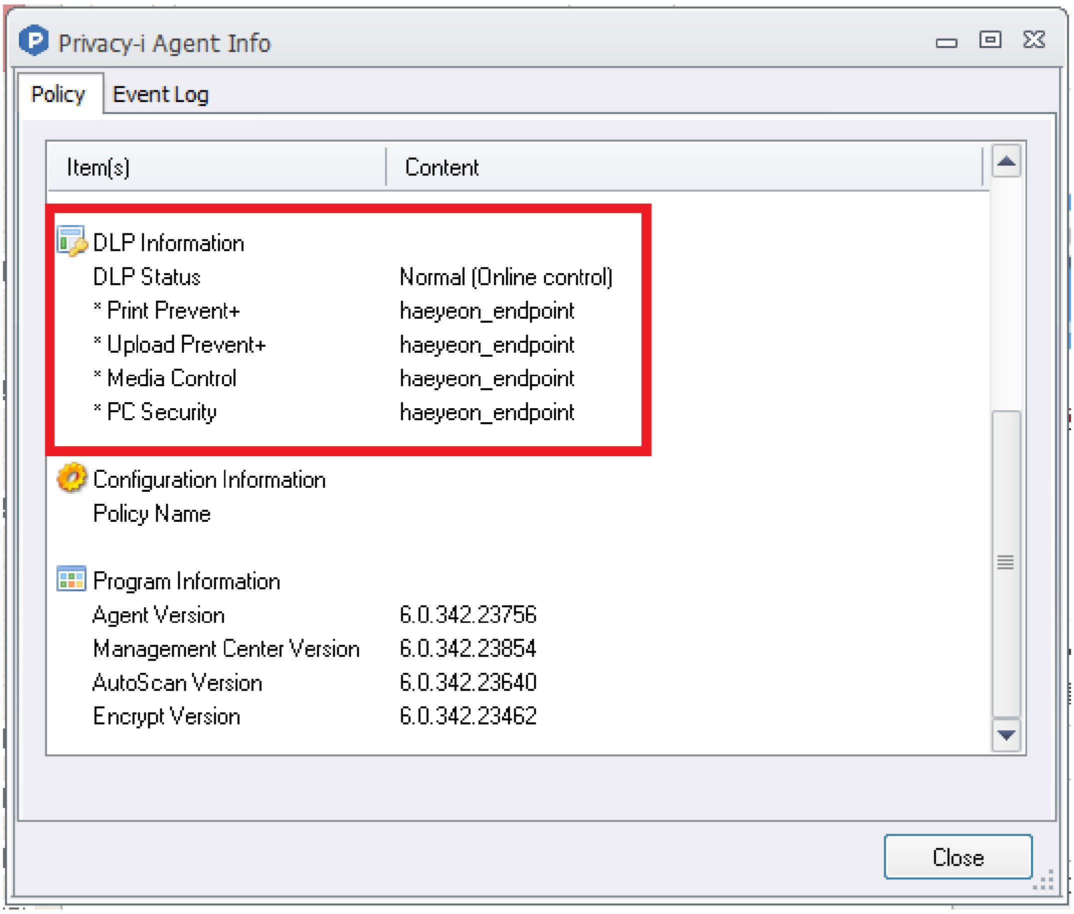


On	Priority	Policy Name	Online/Offline	Channels	Targets	Modified Time
●	1	haeyeon_endpoint	ONLINE OFFLINE		0 1 0	2017-02-16 15:30:31
●	2	test	ONLINE OFFLINE		0 1 0	2017-02-09 19:50:52

Showing 1 to 2 of 2 entries

(FIGURE 4-50) POLICY PRIORITIES

As shown in Figure, users with the same targets are designated with the policy with priority 1 and the policy with priority 3. When the policy is updated in Agent, multiple policies are applied.



Privacy-i Agent Info

Policy | Event Log

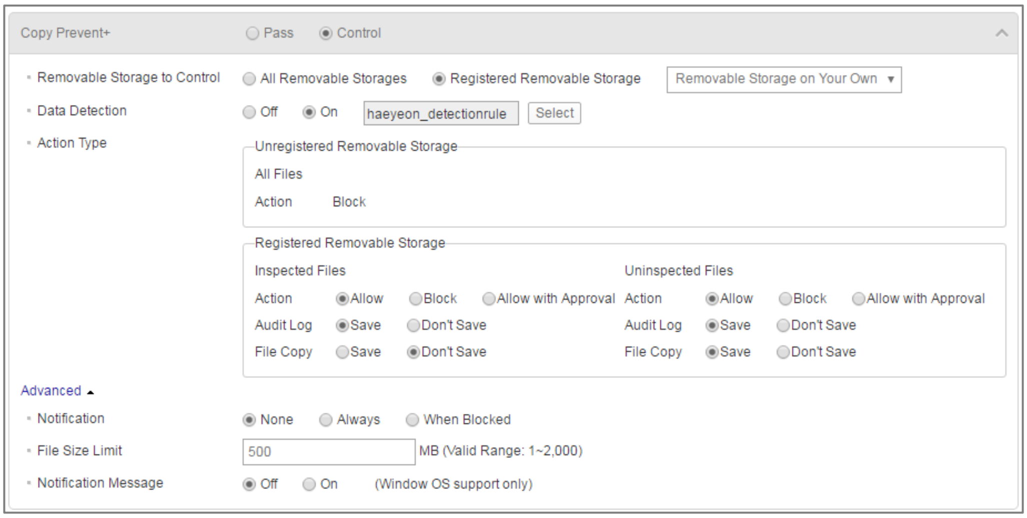
Item(s)	Content
DLP Information	
DLP Status	Normal (Online control)
* Print Prevent+	haeyeon_endpoint
* Upload Prevent+	haeyeon_endpoint
* Media Control	haeyeon_endpoint
* PC Security	haeyeon_endpoint
Configuration Information	
Policy Name	
Program Information	
Agent Version	6.0.342.23756
Management Center Version	6.0.342.23854
AutoScan Version	6.0.342.23640
Encrypt Version	6.0.342.23462

(FIGURE 4-51) AGENT POLICY INFORMATION

Multiple policies can be applied since the policy with priority is applied first in Agent as shown in Figure.

4.4.4.1 Copy Prevent+

A policy can be set for portable storage media such as USB memories and external disks. The other data leakage control policies below are configured with the same process. Since a wide range of USBs are used in an organization, it is often difficult to manually apply and allow or block policy for available USB drive restriction. In this case, the policy allows using selective types of USB by allowing only the USB devices registered in the organization.



Copy Prevent+ ○ Pass ● Control

- Removable Storage to Control: ○ All Removable Storages ● Registered Removable Storage | Removable Storage on Your Own ▾
- Data Detection: ○ Off ● On | haeyeon_detectionrule | Select
- Action Type:

Unregistered Removable Storage
All Files
Action Block

Registered Removable Storage

Inspected Files				Uninspected Files			
Action	● Allow	○ Block	○ Allow with Approval	Action	● Allow	○ Block	○ Allow with Approval
Audit Log	● Save	○ Don't Save		Audit Log	● Save	○ Don't Save	
File Copy	○ Save	● Don't Save		File Copy	● Save	○ Don't Save	

Advanced ▴

- Notification: ● None ○ Always ○ When Blocked
- File Size Limit: 500 MB (Valid Range: 1~2,000)
- Notification Message: ● Off ○ On (Window OS support only)

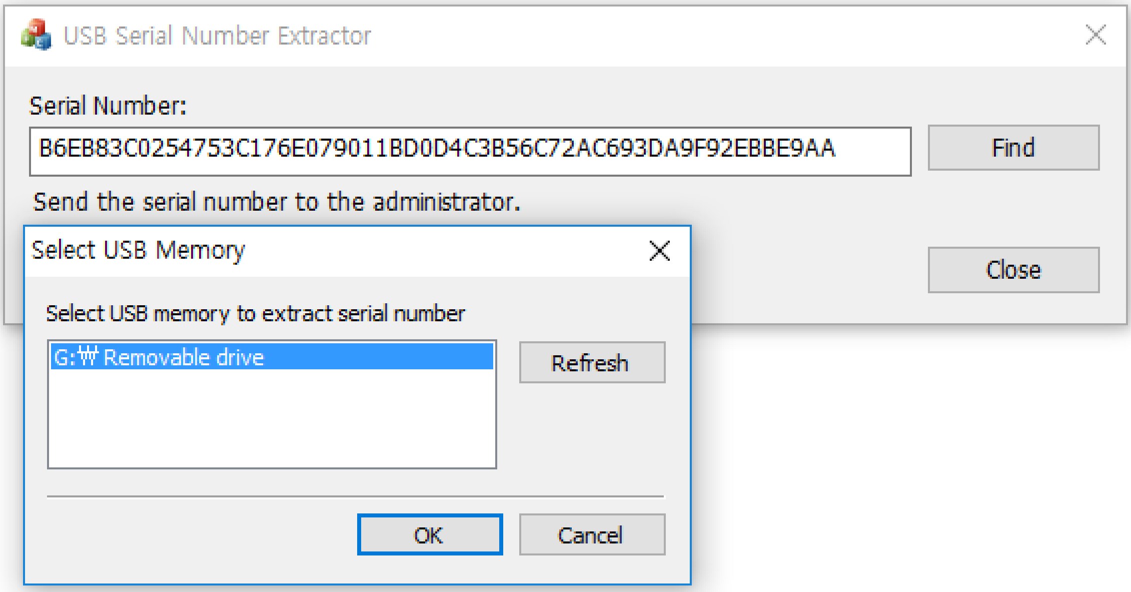
(FIGURE 4-52) COPY PREVENT POLICY DETAILS SCREEN

- Register portable storage media

  The function provides advanced settings of Copy Prevent+, by which only USB allowed in the client company can be used for security policy application. The user can only use USB registered from Admin of DLP+ Center, and personal or unregistered USB are applied to be blocked from using.

4.4.4.2 Registration of Portable Storage Media and Use of Registered Media

1) Issuance of USB Serial number through PIUSBSerial program
   The administrator of DLP+ Center can extract serial information of USB to be used in the company through PIUSBSerial program installed in a PC.



Serial Number:
B6EB83C0254753C176E079011BD0D4C3B56C72AC693DA9F92EBBE9AA

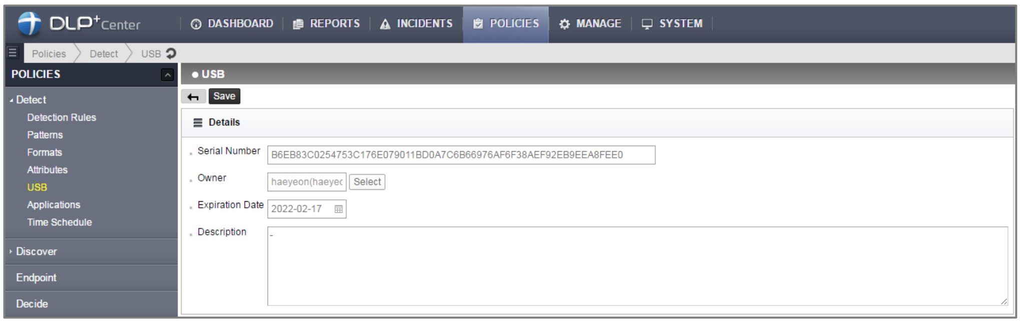
Send the serial number to the administrator.

Select USB memory to extract serial number

G:₩ Removable drive

(FIGURE 4-53) REGISTER SERIAL INFORMATION OF USB THROUGH PIUSBSERIAL PROGRAM

2) Register USB Serial number to DLP+ Center
When extraction of USB serial information is completed, the administrator of DLP+ Center registers the extracted serial information to DLP+ Center. The registration can be proceeded in the item of “MANAGE > USB” in DLP+ Center menu, and the serial number, person with Admin authority, purposes, expiration date, and description information are input to register the “Registered portable storage media”.



Serial Number: B6EB83C0254753C176E079011BD0A7C6B66976AF6F38AEF92EB9EEA8FEE0

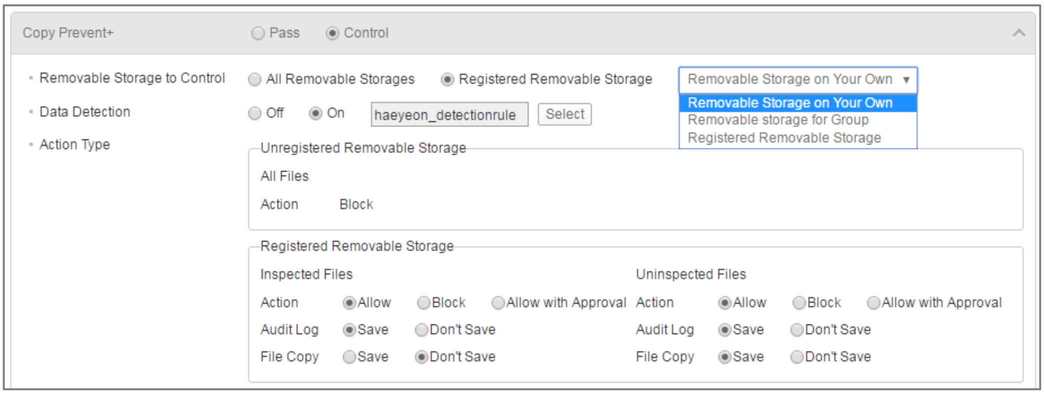
Owner: haeyeon(haeyec

Expiration Date: 2022-02-17

Description: -

(FIGURE 4-54) USB SERIAL NUMBER REGISTRATION SCREEN

3) Policy application: Endpoint > Copy Prevent+



Copy Prevent+ ○ Pass ● Control

- Removable Storage to Control ○ All Removable Storages ● Registered Removable Storage [Removable Storage on Your Own ▾]
- Data Detection ○ Off ● On haeyeon_detectionrule [Select]
- Action Type

Removable Storage on Your Own
Removable storage for Group
Registered Removable Storage

Unregistered Removable Storage

All Files

Action Block

Registered Removable Storage

Inspected Files				Uninspected Files			
Action	● Allow	○ Block	○ Allow with Approval	Action	● Allow	○ Block	○ Allow with Approval
Audit Log	● Save	○ Don't Save		Audit Log	● Save	○ Don't Save	
File Copy	○ Save	● Don't Save		File Copy	● Save	○ Don't Save	

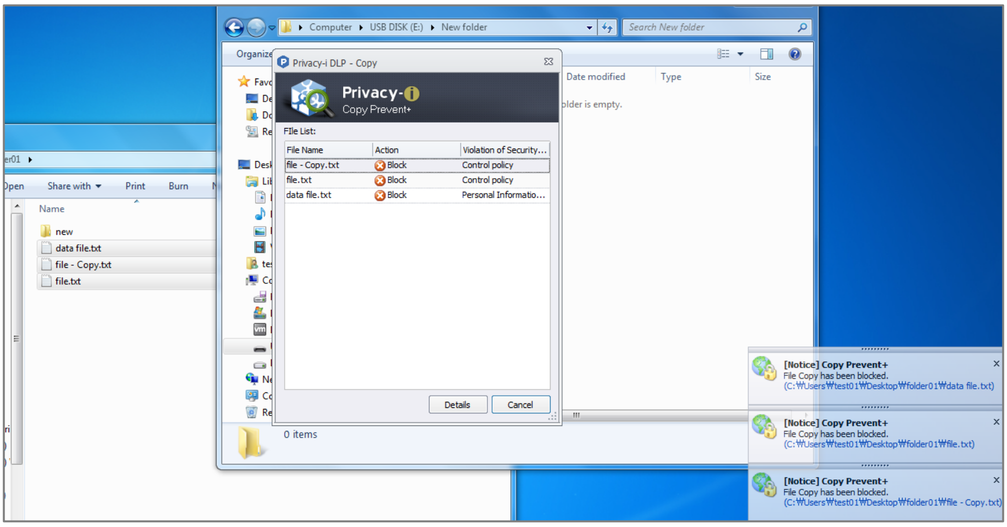
(FIGURE 4-55) COPY PREVENT+ PORTABLE STORAGE MEDIA SETTINGS SCREEN

“Registered portable storage media” is applied in Copy Prevent+. As shown in the Figure above, ‘All portable storage media’, or ‘Registered portable storage media’ can be selected from “Control target portable storage media”. For the department or Agent user with ‘Registered portable storage media’ registered, applied policy can be used for the registered USB, and copy of all files will be blocked for unregistered USB. “Designate portable storage media” is classified for use as shown in the TABLE below, and, for USB registered in DLP+ Center, use of not relevant user or department will be always blacked.

[TABLE 4-14] Confidential data inspection options settings

Category	Description
Portable storage media of owner	The **user** designated as the ‘Administrator’ can only be applied context-aware policy for the registered USB.
Portable storage media owned by the department of the user	The **department** designated as the ‘Administrator’ can only be applied context-aware policy for the registered USB.
Select registered portable storage media	The USB designated by the administrator can only be applied context-aware policy for the registered USB.

4) Privacy-i Agent operation method according to Copy Prevent+ policy
When using the “Registered portable storage media”, context-aware policy will be applied according to the policy. When using unregistered portable storage media, however, it is always blocked with the popup message, “Not approved portable media”.



Privacy-i DLP - Copy

Privacy-i
Copy Prevent+

FIle List:

File Name	Action	Violation of Security...
file - Copy.txt	Block	Control policy
file.txt	Block	Control policy
data file.txt	Block	Personal Informatio...

[Notice] Copy Prevent+
File Copy has been blocked.
(C:₩Users₩test01₩Desktop₩folder01₩data file.txt)

[Notice] Copy Prevent+
File Copy has been blocked.
(C:₩Users₩test01₩Desktop₩folder01₩file.txt)

[Notice] Copy Prevent+
File Copy has been blocked.
(C:₩Users₩test01₩Desktop₩folder01₩file - Copy.txt)

(FIGURE 4-56) CONFIDENTIAL INFORMATION CONTEXT-AWARE BLOCKING SCREEN FOR REGISTERED PORTABLE STORAGE MEDIA

☞ Descriptions on policy items

① Control target portable storage media: All portable storage media or registered portable storage media can be selected, policy is registered for the selected portable storage media.

② Data inspection: Off' or 'On' can be selected, and, when 'On' is selected, the policy registered in "Detection Rules" can be selected, and the policy is set by the specified rule.

③ Counter measures: Storage media that are not registered are blocked, and registered portable storage media or all portable storage media can be set to allow / block. In addition, 'Save / Do Not Save' can be set for a copied file when allowed.

④ Notification message: 'No Notification', 'Always Notify', and 'Notify When Blocked' can be selected. Notification can be shown on Privacy-i Agent when it is set.

⑤ Limit in the size of a copy: When saving copies, only copies for configured values can be saved.

⑥ Warning message: 'Off' or 'On' can be selected, and, when 'On' is selected, warning messages can be sent to Privacy-i Agent.

☞ Effective Input Field Range

[TABLE 4-15] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING PORTABLE STORAGE MEDIA

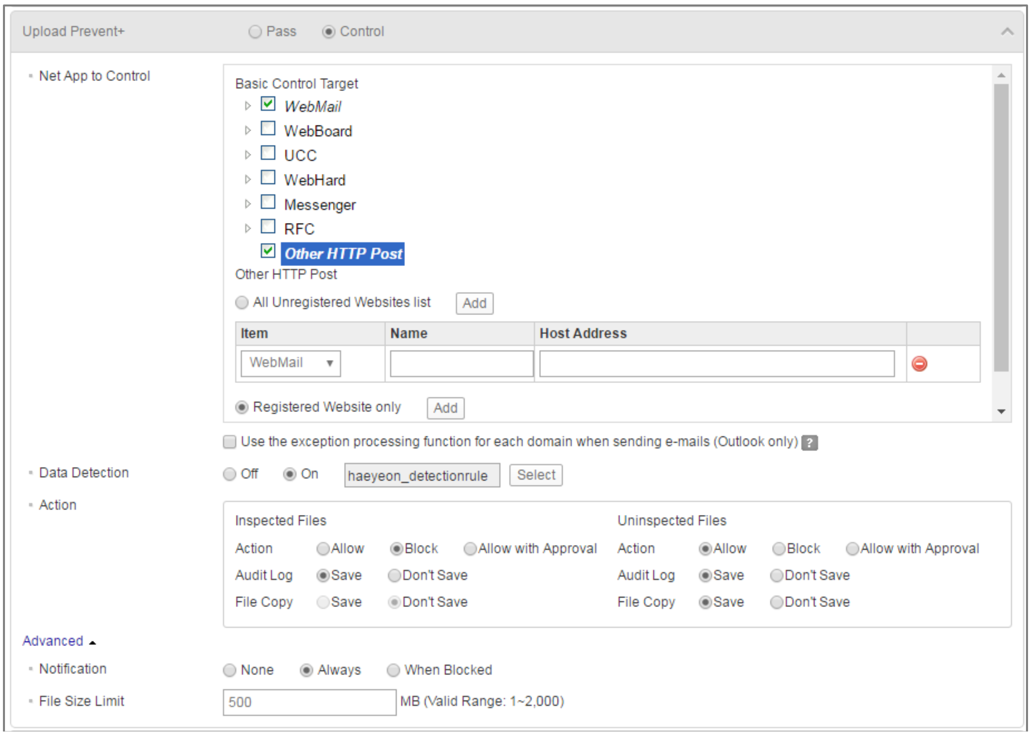
Item	Effective range	Character	Failure message
Policy name	1~120	Numbers, upper or lower case letters, special characters	Enter policy name.
Limit in size of copy	1~2000	Numbers	The size of the copy file should be input in the range of 1~2000 MByte(s).

4.4.4.3 Upload Prevent+

The policy on file attachment or upload such as Web mail, Web board, Web hard, etc. is configured. The other data leakage control policy below also consists of the same processes.

[TABLE 4-16] OBJECTS OF NETWORK SUPPORT

Category	Target	Category	Target
Web mail	Naver	UCC	Youtube
	Daum	Web hard	DacomHard
	Nate		NDrive
	Hotmail		Daum Cloud
	Yahoo	Messenger	Skype
	Gmail		NateOn
Web board	Naver Blog		MissLee
	Daum Blog		Yahoo Messenger
	Cyworld	RFC	SMTP
	Facebook		FTP



Upload Prevent+ ○ Pass ● Control

- Net App to Control

Basic Control Target
☑ WebMail
□ WebBoard
□ UCC
□ WebHard
□ Messenger
□ RFC
☑ Other HTTP Post

Other HTTP Post
○ All Unregistered Websites list Add

Item	Name	Host Address	
WebMail ▾			⊖

● Registered Website only Add

□ Use the exception processing function for each domain when sending e-mails (Outlook only) ?

- Data Detection ○ Off ● On haeyeon_detectionrule Select
- Action

Inspected Files				Uninspected Files			
Action	○ Allow	● Block	○ Allow with Approval	Action	● Allow	○ Block	○ Allow with Approval
Audit Log	● Save	○ Don't Save		Audit Log	● Save	○ Don't Save	
File Copy	○ Save	● Don't Save		File Copy	● Save	○ Don't Save	

Advanced ▴
- Notification ○ None ● Always ○ When Blocked
- File Size Limit 500 MB (Valid Range: 1~2,000)

(FIGURE 4-57) UPLOAD PREVENT POLICY DETAILS SCREEN

☞ Descriptions on policy items

① Control target NetApps: Default control target in [TABLE 4-18] can be selected, and, when selecting other HTTP Post, desired control target can be set.

② Data inspection: Off' or 'On' can be selected, and, when 'On' is selected, the policy registered in "Detection Rules" can be selected, and the policy is set by the specified rule.

③ Counter measures: All files that are uploaded can be set to allow/ block. In addition, 'Save/ Do Not Save' can be set for a copied file when allowed.

④ Notification message: 'No Notification', 'Always Notify', and 'Notify When Blocked' can be selected. Notification can be shown on Privacy-i Agent when it is set.

⑤ Limit in the size of a copy: When saving copies, only copies for configured values can be saved.

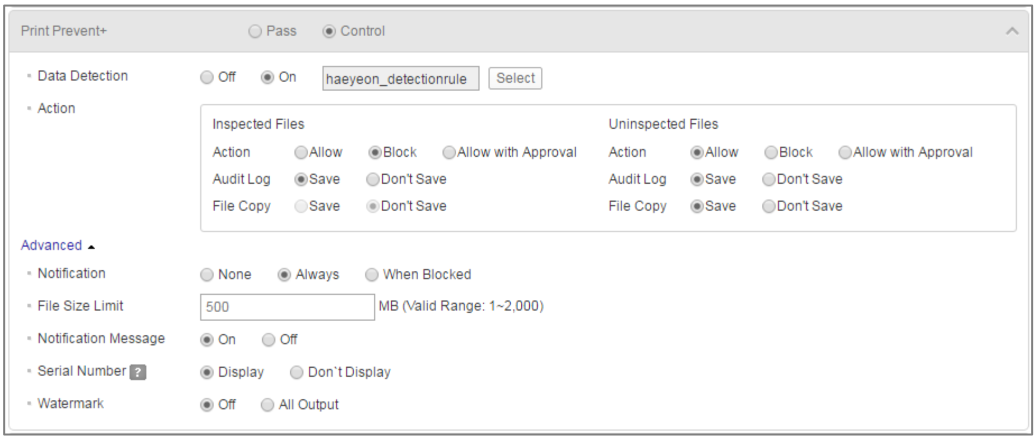
☞ Effective Input Field Range

[TABLE 4-1917] UPLOAD PREVENT EFFECTIVE INPUT FIELD RANGE

Item	Effective range	Character	Failure message
Policy name	1~120	Numbers, upper or lower case letters, special characters	Input policy name.
Other HTTP Post (name)	1~120	Numbers, upper or lower case letters, special characters	-
Other HTTP Post (Host address)	1~1024	Numbers, upper or lower case letters, special characters	-
Limit in size of copy	1~2000	Numbers	The size of the copy file should be entered in the range of 1~2000 MByte(s).

4.4.4.4 Print Prevent+

The policy for printing a document through a printer is configured. The other data leakage control policy below also consists of the same processes.



Print Prevent+ ○ Pass ● Control

- Data Detection ○ Off ● On haeyeon_detectionrule Select
- Action

Inspected Files

Action	○Allow	●Block	○Allow with Approval
Audit Log	●Save	○Don't Save	
File Copy	○Save	●Don't Save	

Uninspected Files

Action	●Allow	○Block	○Allow with Approval
Audit Log	●Save	○Don't Save	
File Copy	●Save	○Don't Save	

Advanced ▲

- Notification ○ None ● Always ○ When Blocked
- File Size Limit 500 MB (Valid Range: 1~2,000)
- Notification Message ● On ○ Off
- Serial Number ? ● Display ○ Don`t Display
- Watermark ● Off ○ All Output

(FIGURE 4-58) PRINT PREVENT DETAILS SCREEN

☞ Descriptions on policy items

① Data inspection: 'Off' or 'On' can be selected, and, when 'On' is selected, the policy registered in "Detection Rules" can be selected, and the policy is set by the specified rule.

② Counter measures: All files that are uploaded can be set to allow / block. In addition, 'Save / Do Not Save' can be set for a copied file when allowed.

③ Notification message: 'No Notification', 'Always Notify', and 'Notify When Blocked' can be selected. Notification can be shown on Privacy-i Agent when it is set.

④ Limit in the size of a copy: When saving copies, only copies for configured values can be saved.

⑤ Warning message: 'Off' or 'On' can be selected, and, when 'On' is selected, warning messages can be sent to Privacy-i Agent.

⑥ Serial number: When selected to 'Display', the serial number of output page is displayed.

⑦ Watermark: When all outputs or outputs including data are selected, watermarks are printed on the output pages.

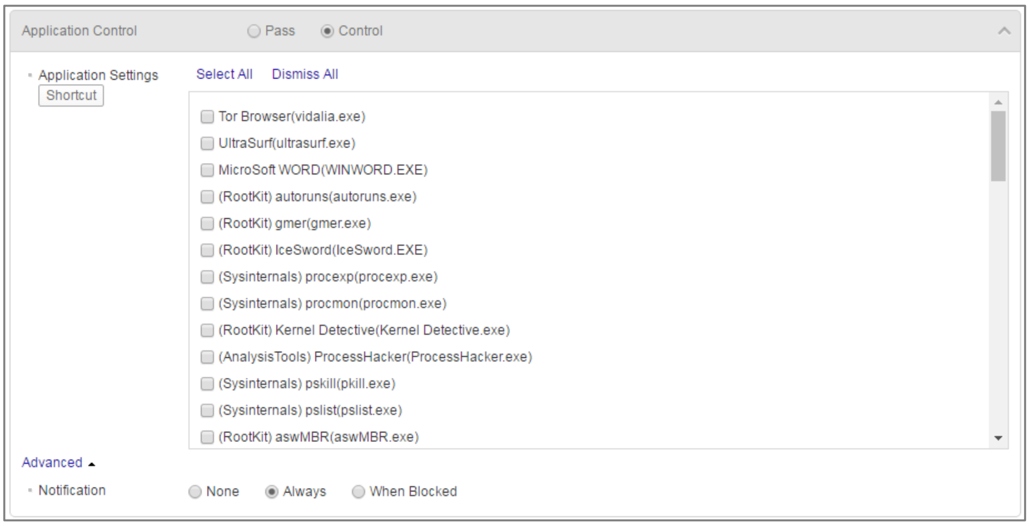
☞ Effective Input Field Range

[TABLE 4-180] PRINT PREVENT EFFECTIVE INPUT FIELD RANGE

Item	Effective range	Character	Failure message
Policy name	1~120	Numbers, upper or lower case letters, special characters	Enter policy name.
Limit in size of copy	1~2000	Numbers	The size of the copy file should be input in the range of 1~2000 MByte(s).

4.4.4.5 Application Control+

Control of program execution provides allow or block of operations of specific programs in a PC. When block is made by inputting program names or binary search word in 'Add', the program will not be executed.



Application Control ○ Pass ● Control

Application Settings

Shortcut

Select All Dismiss All

- □ Tor Browser(vidalia.exe)
- □ UltraSurf(ultrasurf.exe)
- □ MicroSoft WORD(WINWORD.EXE)
- □ (RootKit) autoruns(autoruns.exe)
- □ (RootKit) gmer(gmer.exe)
- □ (RootKit) IceSword(IceSword.EXE)
- □ (Sysinternals) procexp(procexp.exe)
- □ (Sysinternals) procmon(procmon.exe)
- □ (RootKit) Kernel Detective(Kernel Detective.exe)
- □ (AnalysisTools) ProcessHacker(ProcessHacker.exe)
- □ (Sysinternals) pskill(pkill.exe)
- □ (Sysinternals) pslist(pslist.exe)
- □ (RootKit) aswMBR(aswMBR.exe)

Advanced ▴

Notification ○ None ● Always ○ When Blocked

(FIGURE 4-59) APPLICATION CONTROL DETAILS SCREEN

① Block execution: Applications provided in [TABLE 4-12] default applications can be selected.

② Notification message: 'No Notification', 'Always Notify', and 'Notify When Blocked' can be selected. Notification can be shown on Privacy-i Agent when it is set.

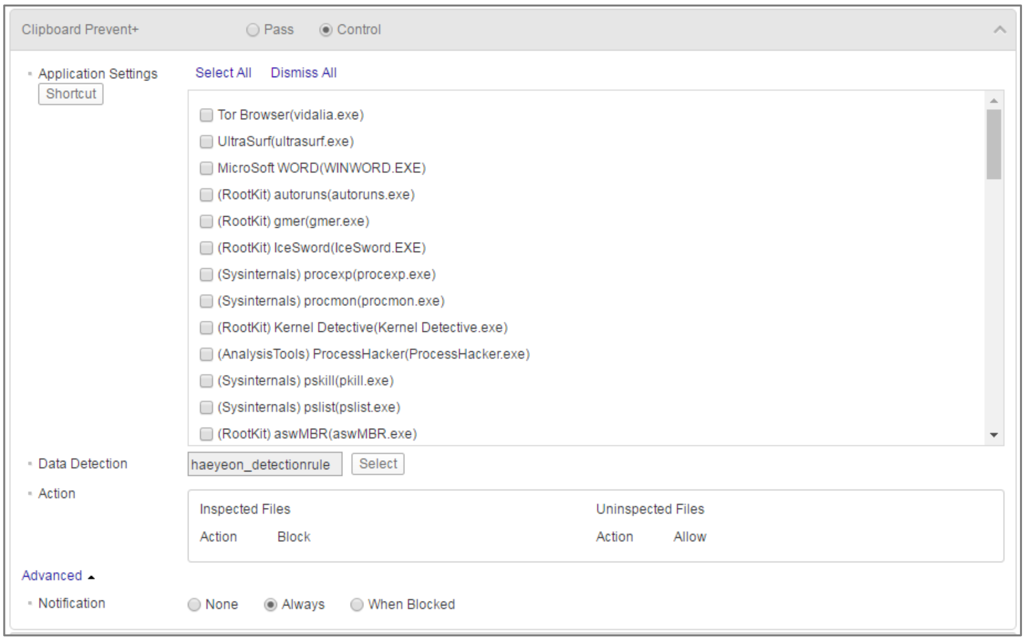
☞ Effective Input Field Range

[TABLE 4-191] APPLICATION CONTROL EFFECTIVE INPUT FIELD RANGE

Item	Effective range	Character	Failure message
Policy name	1~120	Numbers, upper or lower case letters, special characters	Enter policy name.

4.4.4.6 Clipboard Prevent+

Clipboard execution control determines whether to allow or block the operations of files stored in clipboard. As in the program execution control, program name can be input in 'Add' to block the operation so that copying from the copied to the clipboard can be blocked.



Clipboard Prevent+ ○ Pass ● Control

Application Settings Shortcut — Select All Dismiss All

- □ Tor Browser(vidalia.exe)
- □ UltraSurf(ultrasurf.exe)
- □ MicroSoft WORD(WINWORD.EXE)
- □ (RootKit) autoruns(autoruns.exe)
- □ (RootKit) gmer(gmer.exe)
- □ (RootKit) IceSword(IceSword.EXE)
- □ (Sysinternals) procexp(procexp.exe)
- □ (Sysinternals) procmon(procmon.exe)
- □ (RootKit) Kernel Detective(Kernel Detective.exe)
- □ (AnalysisTools) ProcessHacker(ProcessHacker.exe)
- □ (Sysinternals) pskill(pkill.exe)
- □ (Sysinternals) pslist(pslist.exe)
- □ (RootKit) aswMBR(aswMBR.exe)

Data Detection: haeyeon_detectionrule Select

Action:

Inspected Files		Uninspected Files	
Action	Block	Action	Allow

Advanced ▴

Notification: ○ None ● Always ○ When Blocked

(FIGURE 4-60) CLIPBOARDPREVENT DETAILS SCREEN

☞ Descriptions on policy items

① Clipboard block: Applications provided in [TABLE 4-29] default applications can be selected. In the case of "Detection Rules", the policy registered in "Detection Rules" can be selected, and the policy is set according to the selected rules.

② Counter measures: All files can be set to allow/ block. In addition, 'Save/ Do Not Save' can be set for a copied file when allowed.

③ Notification message: 'No Notification', 'Always Notify', and 'Notify When Blocked' can be selected. Notification can be shown on Privacy-i Agent when it is set.

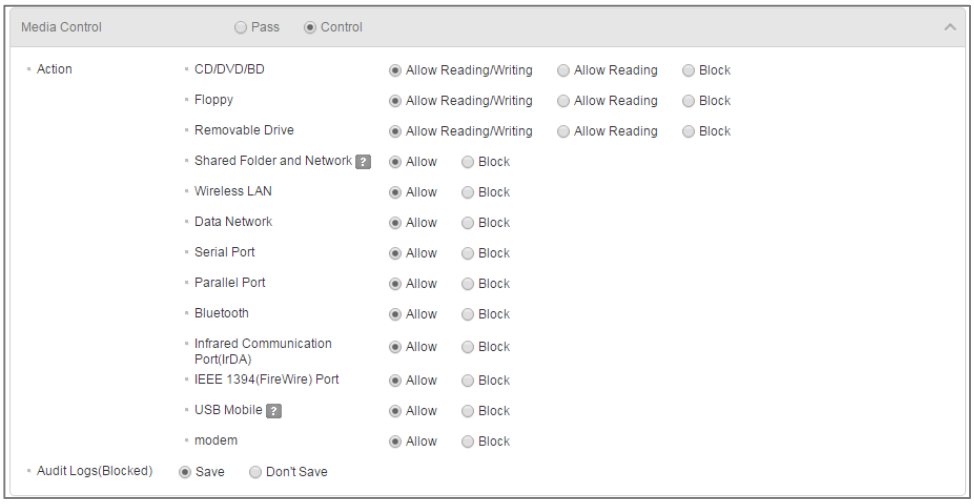
☞ Effective Input Field Range

[TABLE 4-202] CLIPBOARD PREVENT EFFECTIVE INPUT FIELD RANGE

Item	Effective range	Character	Failure message
Policy name	1~120	Numbers, upper or lower case letters, special characters	Enter policy name.

4.4.4.7 Media Control

Privacy-i provides a Control function to allow or block data from moving to external channels, such as CD/DVDs and floppy disk reading/writing, external shared folder and network drive connections, wireless LAN, data networks (tethering, Wibro), serial/parallel ports, Bluetooth, infrared communication (IrDA), IEEE 1394 (Firewire), USB portable devices (USB Mobile), etc.



Media Control ○ Pass ● Control

- Action
  - CD/DVD/BD ● Allow Reading/Writing ○ Allow Reading ○ Block
  - Floppy ● Allow Reading/Writing ○ Allow Reading ○ Block
  - Removable Drive ● Allow Reading/Writing ○ Allow Reading ○ Block
  - Shared Folder and Network ? ● Allow ○ Block
  - Wireless LAN ● Allow ○ Block
  - Data Network ● Allow ○ Block
  - Serial Port ● Allow ○ Block
  - Parallel Port ● Allow ○ Block
  - Bluetooth ● Allow ○ Block
  - Infrared Communication Port(IrDA) ● Allow ○ Block
  - IEEE 1394(FireWire) Port ● Allow ○ Block
  - USB Mobile ? ● Allow ○ Block
  - modem ● Allow ○ Block
- Audit Logs(Blocked) ● Save ○ Don't Save

(FIGURE 4-61) MEDIA CONTROL DETAILS SCREEN

☞ Descriptions on policy items

① Control Settings: CDs/DVDs, floppy disks and USBs can be divided into reading and writing, and set to be allowed/blocked. Reading other specified media is blocked/allowed.

☞ Effective Input Field Range

[TABLE 4-213] MEDIA EFFECTIVE INPUT FIELD RANGE

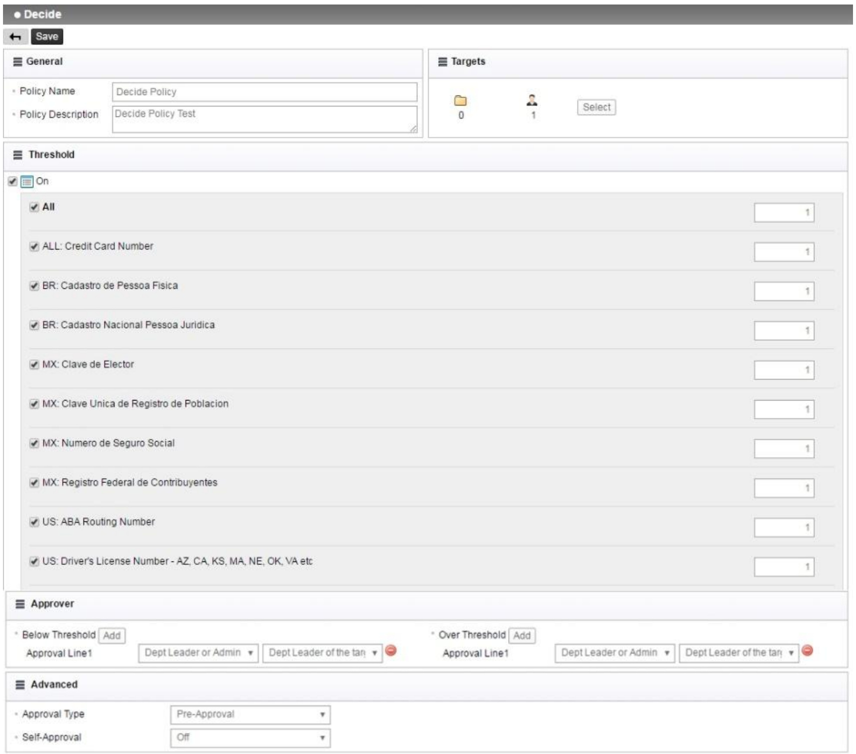
Item	Effective range	Character	Failure message
Policy name	1~120	Numbers, upper or lower case letters, special characters	Enter policy name.

4.4.4.8 Time of Applying Policies

The function sets a time frame to apply online or offline policies.

4.4.5 Decide

Approval policy can be configured.


● Decide

General

- Policy Name: Decide Policy
- Policy Description: Decide Policy Test

Targets

Threshold

☑ On

☑ All	1
☑ ALL: Credit Card Number	1
☑ BR: Cadastro de Pessoa Fisica	1
☑ BR: Cadastro Nacional Pessoa Juridica	1
☑ MX: Clave de Elector	1
☑ MX: Clave Unica de Registro de Poblacion	1
☑ MX: Numero de Seguro Social	1
☑ MX: Registro Federal de Contribuyentes	1
☑ US: ABA Routing Number	1
☑ US: Driver's License Number - AZ, CA, KS, MA, NE, OK, VA etc	1

Approver

- Below Threshold [Add]
  Approval Line1: Dept Leader or Admin ▾ | Dept Leader of the tar ▾
- Over Threshold [Add]
  Approval Line1: Dept Leader or Admin ▾ | Dept Leader of the tar ▾

Advanced

- Approval Type: Pre-Approval ▾
- Self-Approval: Off ▾

(FIGURE 4-62) DECIDE DETAILS SCREEN

☞ Description of detailed items of policy

① Policy name: Decides policy name.

② Target: Select the department or user to apply. When shortcut is selected, it moves to Apply to targets > PCs.

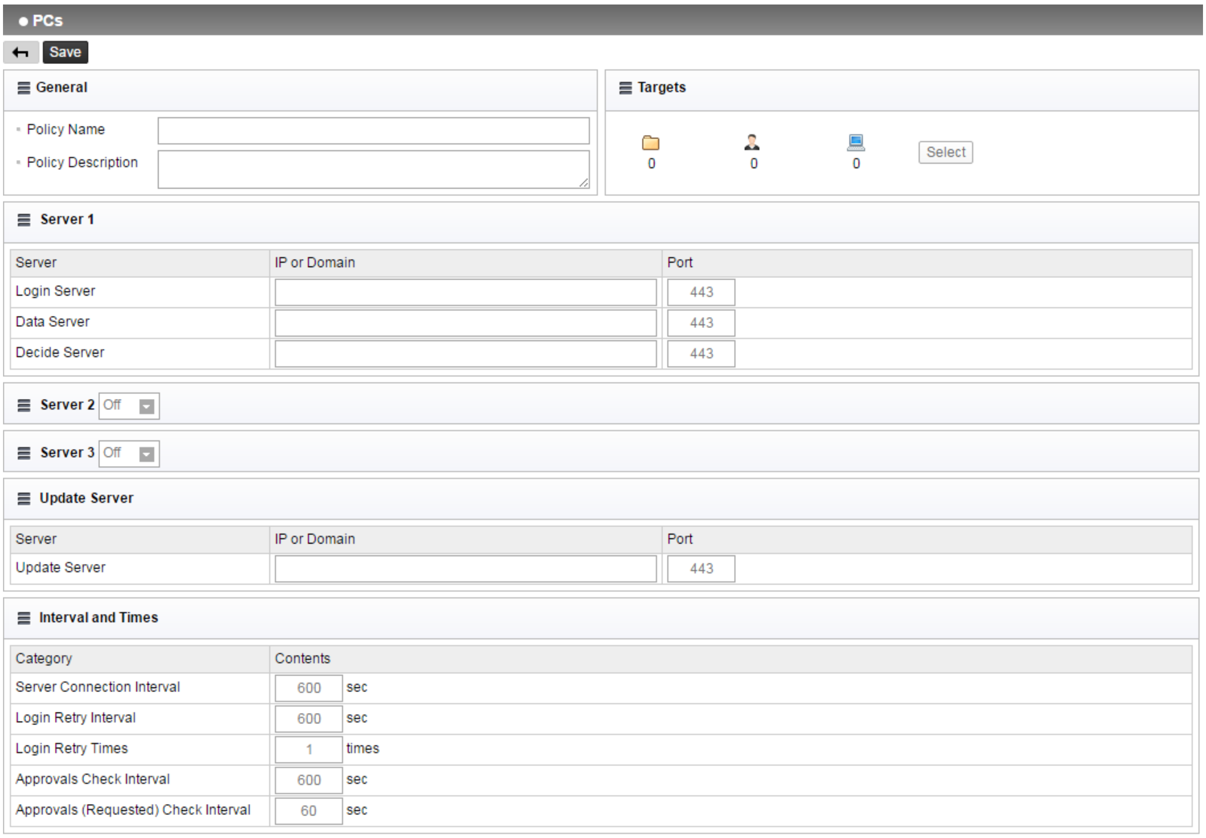
③ Threshold setting: Setting is made for each pattern so that approval can be obtained in the case of exceeding configured figures.

④ Approver setting: Those with authority of approval can be set on the basis of designated threshold.

⑤ Approval options: Prior approval, post approval, prior/post approval method, and users themselves can be designated as those with authority of approval.

4.4.6 Connections

Connection settings for the sever to be connected by Agent can be configured.



● PCs

Save

General

Policy Name	
Policy Description	

Targets

0	0	0	Select

Server 1

Server	IP or Domain	Port
Login Server		443
Data Server		443
Decide Server		443

Server 2 Off

Server 3 Off

Update Server

Server	IP or Domain	Port
Update Server		443

Interval and Times

Category	Contents
Server Connection Interval	600 sec
Login Retry Interval	600 sec
Login Retry Times	1 times
Approvals Check Interval	600 sec
Approvals (Requested) Check Interval	60 sec

(FIGURE 4-63) PC CONNECTION SETTINGS SCREEN

☞ Descriptions on policy items

① Connection server 1: Connection server of Privacy-i Agent is configured.

- Connection server 2 (3): When selected for use, it can be configured in the same way as in connection server 1, which is necessary in duplicate or triplicate settings.

② Server connection period: The time of period for connecting the server is set.

③ Login retrial period: Re-login period is set when there is no response from Privacy-i Agent Installed PC.

④ Number of login retrials: The number of login retrials in the case of failing in account is set.

☞ Effective Input Field Range

[TABLE 4-24] CONNECTIONS EFFECTIVE INPUT FIELD RANGE

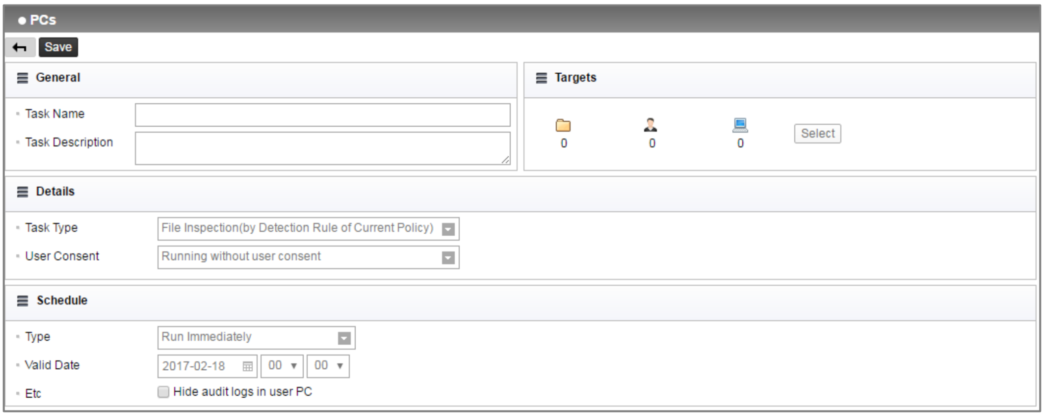
Item	Effective range	Character	Failure message
Setting name	1~120	Numbers, upper or lower case letters, special characters	Enter setting name.
IP	15	Numbers, special characters (.) (However, 0.0.0.0 and 255.255.255.255 cannot be entered)	Incorrect IP has been inserted to the connection server 1. Check and try again.
Server connection period	1~99999	Numbers	Space cannot be entered.
Login re-trial period	1~99999	Numbers	Space cannot be entered.
Number of login re-trial	1~99999	Numbers	Space cannot be entered.

4.5 Manage

4.5.1 Admin Action

4.5.1.1 PC

It is used for managing confidential data information on a user PC and Agent environment control for users or departments. Types provided with a remote command include Remote inspection, Delete file, Encryption, Server Connection Policy Update and Agent Update. Schedule settings are available to run a task temporarily or repeatedly. Forced execution without user consent or executing a task with user consent can be set.



General
- Task Name
- Task Description

Details
- Task Type: File Inspection(by Detection Rule of Current Policy)
- User Consent: Running without user consent

Schedule
- Type: Run Immediately
- Valid Date: 2017-02-18 00 00
- Etc: □ Hide audit logs in user PC

(FIGURE 4-64) REMOTE TASK SETTINGS SCREEN

[TABLE 4-4] below shows detailed information on the types of remote commands.

[TABLE 4-225] TYPES AND FUNCTIONS OF REMOTE COMMANDS

Types of remote commands	Description
File inspection (current policy)	Performs confidential data inspection with the inspection policy allocated to a department or user
File inspection (temporary policy)	Performs confidential data inspection with the inspection policy other than the policy allocated to a department or user
Mail inspection (current policy)	Performs confidential data inspection with the inspection policy allocated to a department or user
Mail inspection (temporary policy)	Performs confidential data inspection with the inspection policy other than the policy allocated to a department or user
Cancel running inspection	Cancels running central inspection
Pause running inspection	Pauses currently running central inspection current
Resume paused inspection	Resumes temporally paused inspection
File separate	Separates file by the recently performed inspection results
File delete	Deletes file by the recently performed inspection results
File encode	Encrypts file by the recently performed inspection results
Server connection	Tasks performed on the Agent when server connection policy has been changed

policy update	
Agent update	Transfers update command to a user when Agent update module is configured to a server
Delete Agent package	Deletes Agent packages

☞ Descriptions on policy items

① Task Type: Specified in Remote Command Types and Functions in [Table 4-37], and runs the selected task.

- File Inspection (Use the detection rule designated to current policy): Sets a remote task with a policy specified for a user in POLICIES > Apply to Targets
- File Inspection (Select the detection rule to be used temporarily): Sets a remote task with a rule specified in "Detection Rules" item, which appears when selecting.
- File Delete: Sets a remote task that selects the detected file of a user (department) chosen in "Target" and deletes the file through the "Add File" button, which appears when selecting.
- Encrypt file: Sets a remote task that selects the detected file of a user (department) chosen in "Target" and encodes the file through the "Add File" button, which appears when selecting.
- Update server connection policy: Server policy can be update through selecting desired settings in “Update Target”, which appears when selecting.
- Cancel running inspection: The policy cancelling currently running remote inspection can be registered.

② Task Settings: A remote task for a user or department can be specified. Execution without user consent or a user consent request can be selected. When selecting a user consent request, a message for a consent request can be entered.

③ Temporary setting of task: Running methods include an immediate execution or scheduled execution.
In the scheduled execution, the remote task is performed on a scheduled date and time. When selecting audit logs to be hidden in a user PC, the audit logs do not remain in the agent.

☞ Effective Input Field Range

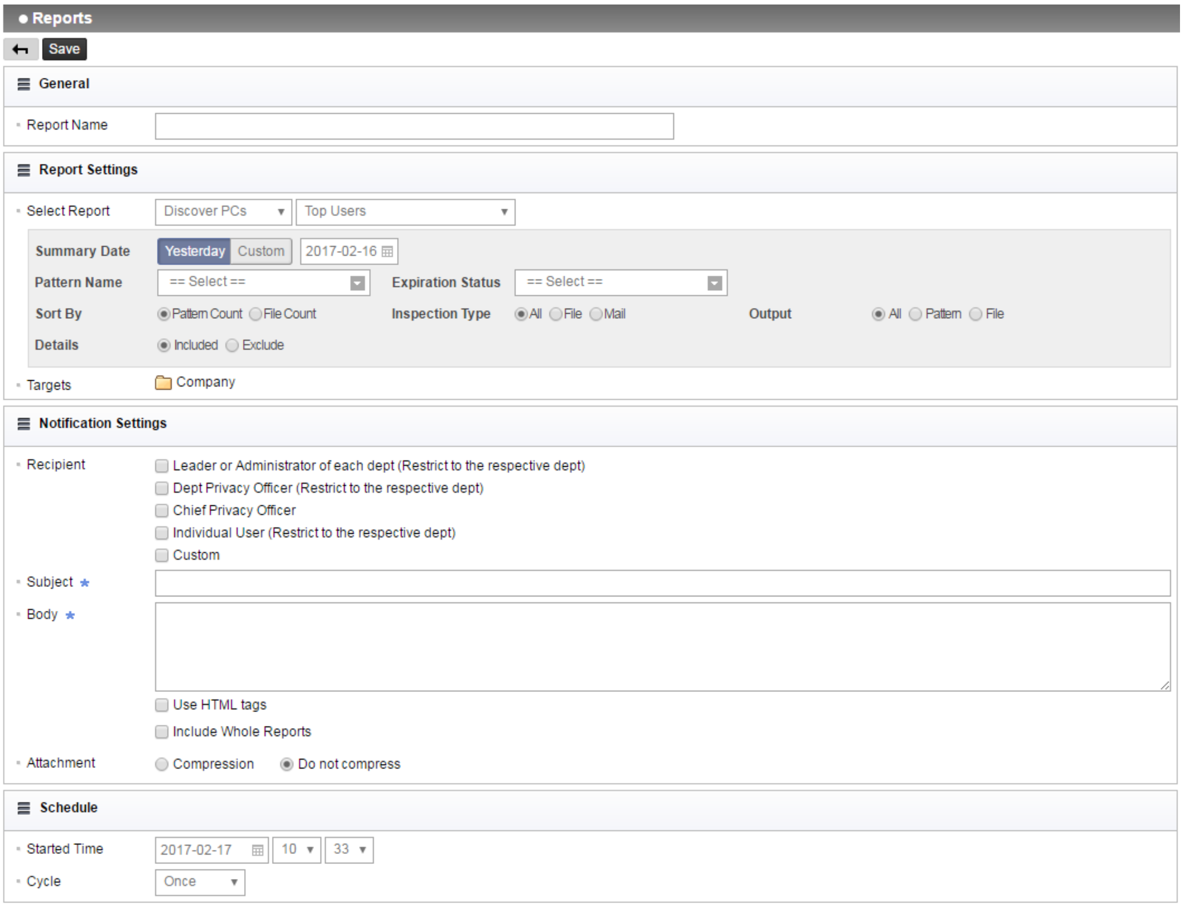
[TABLE 4-236] EFFECTIVE INPUT FIELD RANGE OF REMOTE CONTROL

Item	Effective range	Character	Failure message
Policy name	1~120	Numbers, upper or lower case letters, special characters	Enter task name.
Message	1~4000	Numbers, upper or lower case letters, special characters	-

4.5.2 Alerts / Notification

4.5.2.1 Notify Reports

Statistics of Discover and Endpoint can be received through the E-mail registered in user information.



● Reports

General

Report Name:

Report Settings

Select Report: Discover PCs ▾ | Top Users ▾

Summary Date: [✓ Yesterday] Custom | 2017-02-16

Pattern Name: == Select == | Expiration Status: == Select ==

Sort By: ● Pattern Count ○ File Count | Inspection Type: ● All ○ File ○ Mail | Output: ● All ○ Pattern ○ File

Details: ● Included ○ Exclude

Targets: Company

Notification Settings

Recipient:
□ Leader or Administrator of each dept (Restrict to the respective dept)
□ Dept Privacy Officer (Restrict to the respective dept)
□ Chief Privacy Officer
□ Individual User (Restrict to the respective dept)
□ Custom

Subject *:

Body *:

□ Use HTML tags
□ Include Whole Reports

Attachment: ○ Compression ● Do not compress

Schedule

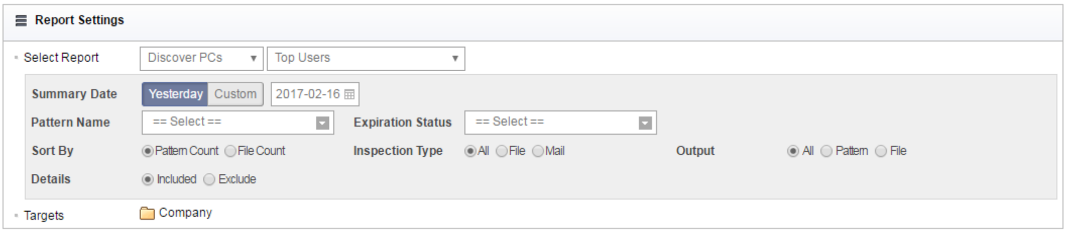
Started Time: 2017-02-17 | 10 ▾ | 33 ▾

Cycle: Once ▾

(FIGURE 4-65) REPORT NOTIFICATION DETAILS SCREEN

☞ Report Notification Details

- Report settings: One of report details of Discover PCs, Discover Servers and Endpoint can be selected.
- Filter settings: Recent Inspection Date, Ranking Criteria and Pattern can be selected so that the filter can be applied.



Report Settings

Select Report: Discover PCs ▾ | Top Users ▾

Summary Date: [✓ Yesterday] Custom | 2017-02-16

Pattern Name: == Select == | Expiration Status: == Select ==

Sort By: ● Pattern Count ○ File Count | Inspection Type: ● All ○ File ○ Mail | Output: ● All ○ Pattern ○ File

Details: ● Included ○ Exclude

Targets: Company

(FIGURE 4-66) REPORT SETTINGS SCREEN

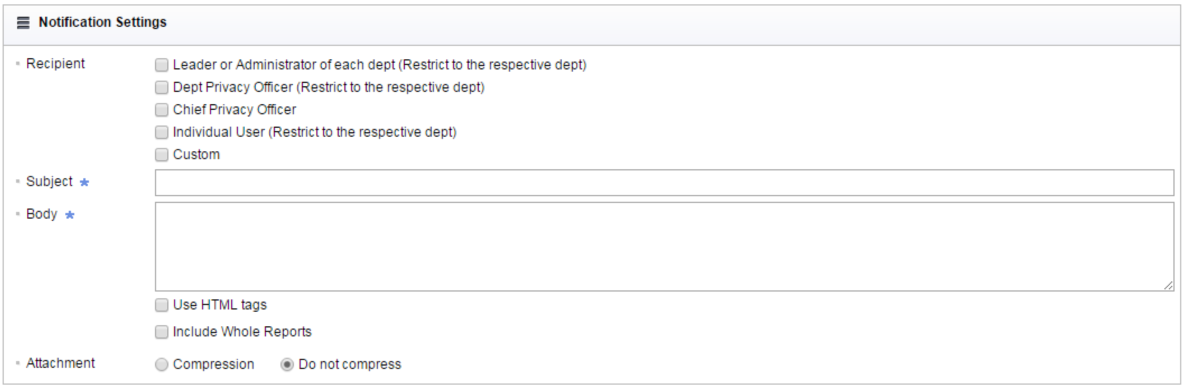
- Inspection summary target: Inspection summary target can be selected to the department, and the user.

▪ Targets

Company

(FIGURE 4-67) INSPECTION SUMMARY TARGET SCREEN

- Notification settings: Receiving person and mail contents can be made.



Notification Settings

Recipient
□ Leader or Administrator of each dept (Restrict to the respective dept)
□ Dept Privacy Officer (Restrict to the respective dept)
□ Chief Privacy Officer
□ Individual User (Restrict to the respective dept)
□ Custom

Subject *

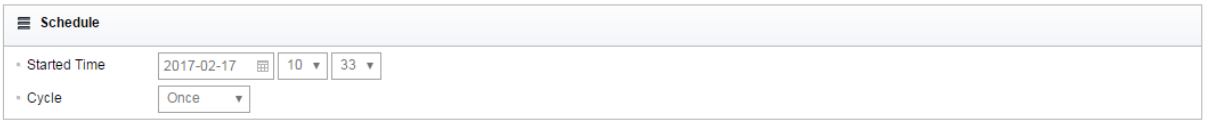
Body *

□ Use HTML tags
□ Include Whole Reports

Attachment ○ Compression ● Do not compress

(FIGURE 4-68) NOTIFICATION TRANSFER TARGET SCREEN

- Period settings: Notification period can be set in the unit of day, week and month.



Schedule

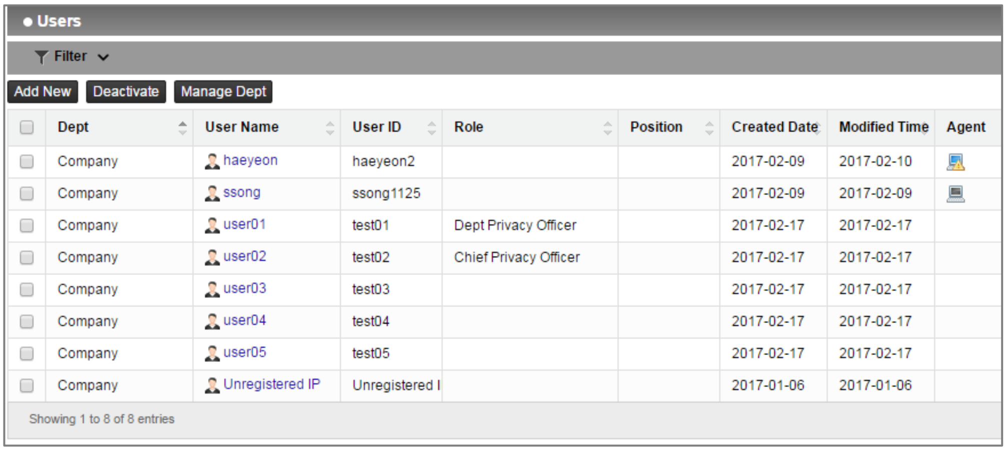
Started Time 2017-02-17 10 33

Cycle Once

(FIGURE 4-69) NOTIFICATION PERIOD SETTINGS SCREEN

4.5.3 Users

Users can be added, modified and deleted. The number of Agents retained and the connection status can be viewed through the agent column on the list.



● Users

Filter

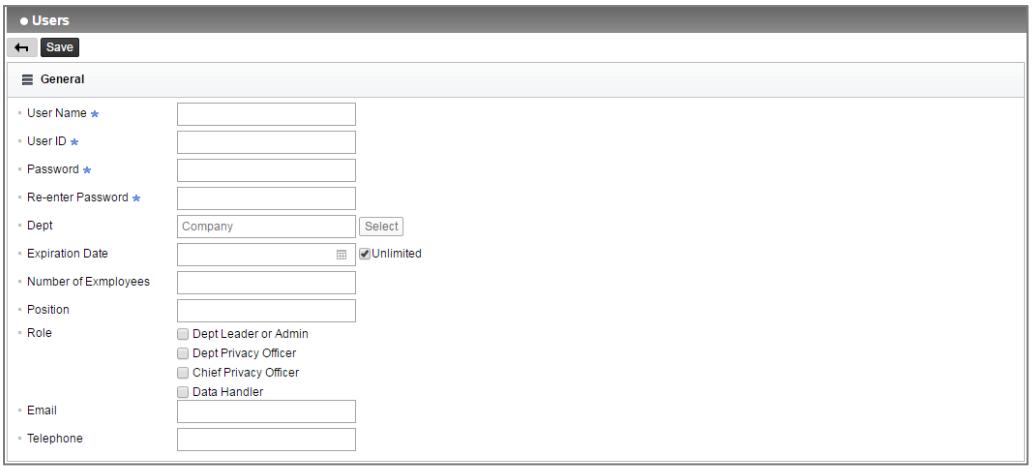
☐	Dept	User Name	User ID	Role	Position	Created Date	Modified Time	Agent
☐	Company	haeyeon	haeyeon2			2017-02-09	2017-02-10	🖥
☐	Company	ssong	ssong1125			2017-02-09	2017-02-09	🖥
☐	Company	user01	test01	Dept Privacy Officer		2017-02-17	2017-02-17	
☐	Company	user02	test02	Chief Privacy Officer		2017-02-17	2017-02-17	
☐	Company	user03	test03			2017-02-17	2017-02-17	
☐	Company	user04	test04			2017-02-17	2017-02-17	
☐	Company	user05	test05			2017-02-17	2017-02-17	
☐	Company	Unregistered IP	Unregistered I			2017-01-06	2017-01-06	

Showing 1 to 8 of 8 entries

(FIGURE 4-70) USER ACCOUNT MANAGEMENT SCREEN

- User management

User management shows the agent information on the user PC that is registered to HR information. For HR information, functions including adding, deleting a user, and changing a password are provided.



● Users

General

User Name *	
User ID *	
Password *	
Re-enter Password *	
Dept	Company Select
Expiration Date	☑ Unlimited
Number of Exmployees	
Position	
Role	☐ Dept Leader or Admin ☐ Dept Privacy Officer ☐ Chief Privacy Officer ☐ Data Handler
Email	
Telephone	

(FIGURE 4-71) USER MANAGEMENT DETAILS

☞ Descriptions on policy items

① Department: The department registered in "Manager > Users > Department management" can be selected, and the user is registered to the selected department.

② Account Starting Date: The available starting date of the account to be registered can be entered.

③ Account Ending Date: The available ending date of the account to be registered can be entered.

④ Staff Number: The staff number of the account user to be registered can be entered.

⑤ Mail: Email of the account user to be registered can be entered.

⑥ Telephone: Phone number of the account user to be registered can be entered.

☞ Effective Input Field Range

[TABLE 4-27] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING USERS

Item	Effective range	Character	Failure message
User name	1~225	Numbers, upper and lower case letters, special characters	Enter user name.
User ID	4~20	Numbers, upper and lower case letters, special characters	Enter user ID.
Password	9~35	Numbers, upper and lower case letters, special characters	Enter password.
Check password	9~35	Numbers, upper and lower case letters, special characters	There is no password confirmation.
Staff No.	1~20	Numbers, upper and lower case letters, special characters	-
Mail	1~50	Numbers, upper and lower case letters, special characters	-
Phone number	1~15	Numbers	-

Recommendations

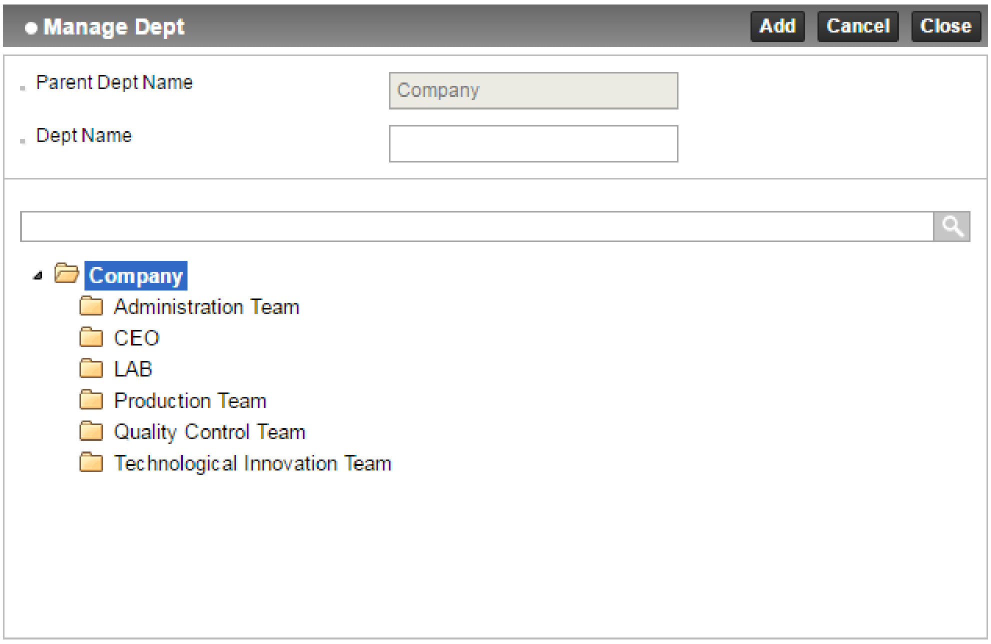
✓ Password should have at least 9 characters including English letters, numbers and special characters.

- Policy Management

Discover Inspection Policy and Endpoint DLP Policy generated in policy can be specified by a department or a user.

- Department Management

Department Management shows departments registered in User Information. For user information, functions to add, delete and move department are provided.



● Manage Dept

Parent Dept Name: Company

Dept Name:

(FIGURE 4-72) DEPARTMENT MANAGEMENT

☞ Effective Input Field Range

[TABLE 4-28] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING USER DEPTARTMENT

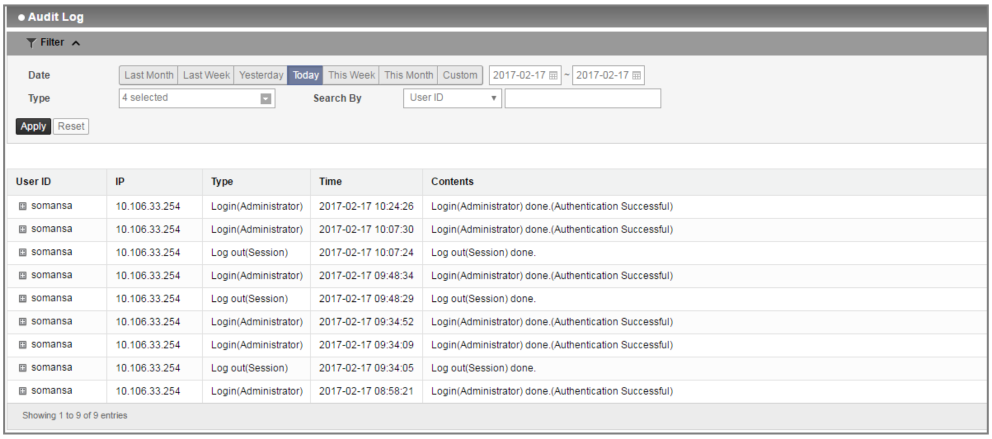
Item	Effective range	Character	Failure message
Dept.	1~100	Numbers, upper and lower case letters, special characters	Input the name of the department.
Search	1~100	Numbers, upper and lower case letters, special characters	-

4.6 System

4.6.1 Logs

- Audit log

For all activities of the administrator, Information Management Logs, Information Trace Logs, Policy Management Logs and Account Management Logs can be viewed. An audit trace is provided through the log.



Date: Last Month | Last Week | Yesterday | Today | This Week | This Month | Custom 2017-02-17 ~ 2017-02-17

Type: 4 selected Search By: User ID

User ID	IP	Type	Time	Contents
⊞ somansa	10.106.33.254	Login(Administrator)	2017-02-17 10:24:26	Login(Administrator) done.(Authentication Successful)
⊞ somansa	10.106.33.254	Login(Administrator)	2017-02-17 10:07:30	Login(Administrator) done.(Authentication Successful)
⊞ somansa	10.106.33.254	Log out(Session)	2017-02-17 10:07:24	Log out(Session) done.
⊞ somansa	10.106.33.254	Login(Administrator)	2017-02-17 09:48:34	Login(Administrator) done.(Authentication Successful)
⊞ somansa	10.106.33.254	Log out(Session)	2017-02-17 09:48:29	Log out(Session) done.
⊞ somansa	10.106.33.254	Login(Administrator)	2017-02-17 09:34:52	Login(Administrator) done.(Authentication Successful)
⊞ somansa	10.106.33.254	Login(Administrator)	2017-02-17 09:34:09	Login(Administrator) done.(Authentication Successful)
⊞ somansa	10.106.33.254	Log out(Session)	2017-02-17 09:34:05	Log out(Session) done.
⊞ somansa	10.106.33.254	Login(Administrator)	2017-02-17 08:58:21	Login(Administrator) done.(Authentication Successful)

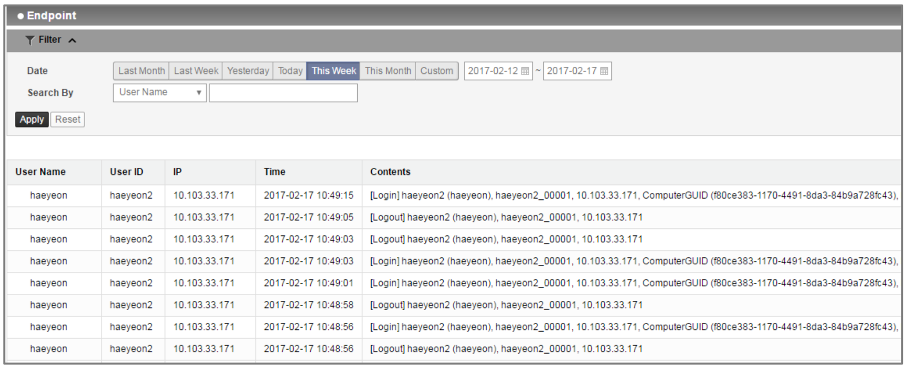
Showing 1 to 9 of 9 entries

(FIGURE 4-73) AUDITLOGS

4.6.1.1 System Logs

- Endpoint

  Records the audit logs for login, logout and policy distribution of Privacy-i Agent connected to the Privacy-i Server. In addition, logs for integrity success/failure of Privacy-i Agent can be viewed.



Date: Last Month | Last Week | Yesterday | Today | This Week | This Month | Custom 2017-02-12 ~ 2017-02-17

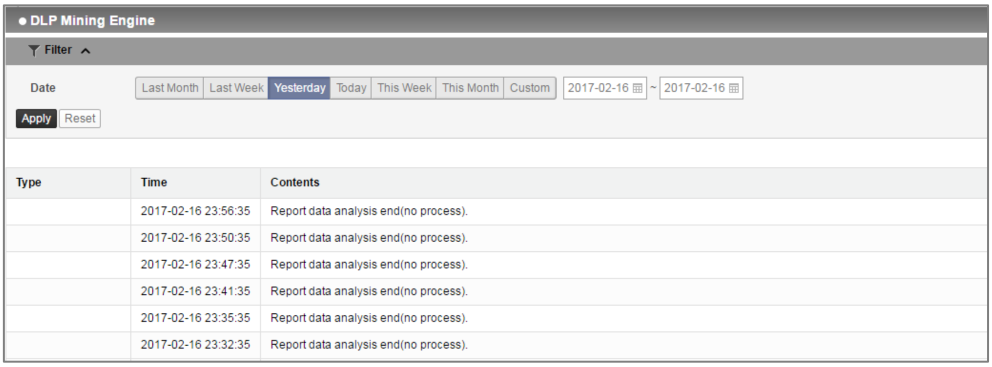
Search By: User Name

User Name	User ID	IP	Time	Contents
haeyeon	haeyeon2	10.103.33.171	2017-02-17 10:49:15	[Login] haeyeon2 (haeyeon), haeyeon2_00001, 10.103.33.171, ComputerGUID (f80ce383-1170-4491-8da3-84b9a728fc43),
haeyeon	haeyeon2	10.103.33.171	2017-02-17 10:49:05	[Logout] haeyeon2 (haeyeon), haeyeon2_00001, 10.103.33.171
haeyeon	haeyeon2	10.103.33.171	2017-02-17 10:49:03	[Logout] haeyeon2 (haeyeon), haeyeon2_00001, 10.103.33.171
haeyeon	haeyeon2	10.103.33.171	2017-02-17 10:49:03	[Login] haeyeon2 (haeyeon), haeyeon2_00001, 10.103.33.171, ComputerGUID (f80ce383-1170-4491-8da3-84b9a728fc43),
haeyeon	haeyeon2	10.103.33.171	2017-02-17 10:49:01	[Login] haeyeon2 (haeyeon), haeyeon2_00001, 10.103.33.171, ComputerGUID (f80ce383-1170-4491-8da3-84b9a728fc43),
haeyeon	haeyeon2	10.103.33.171	2017-02-17 10:48:58	[Logout] haeyeon2 (haeyeon), haeyeon2_00001, 10.103.33.171
haeyeon	haeyeon2	10.103.33.171	2017-02-17 10:48:56	[Login] haeyeon2 (haeyeon), haeyeon2_00001, 10.103.33.171, ComputerGUID (f80ce383-1170-4491-8da3-84b9a728fc43),
haeyeon	haeyeon2	10.103.33.171	2017-02-17 10:48:56	[Logout] haeyeon2 (haeyeon), haeyeon2_00001, 10.103.33.171

(FIGURE 4-74) ENDPOINT LOGS

- DLP+ Mining Engine

  Runs Mining Engine to collect Discover, Endpoint audit logs as the information for use in DLP+ Center at a specific time. Task logs for the process are saved.



Type	Time	Contents
	2017-02-16 23:56:35	Report data analysis end(no process).
	2017-02-16 23:50:35	Report data analysis end(no process).
	2017-02-16 23:47:35	Report data analysis end(no process).
	2017-02-16 23:41:35	Report data analysis end(no process).
	2017-02-16 23:35:35	Report data analysis end(no process).
	2017-02-16 23:32:35	Report data analysis end(no process).

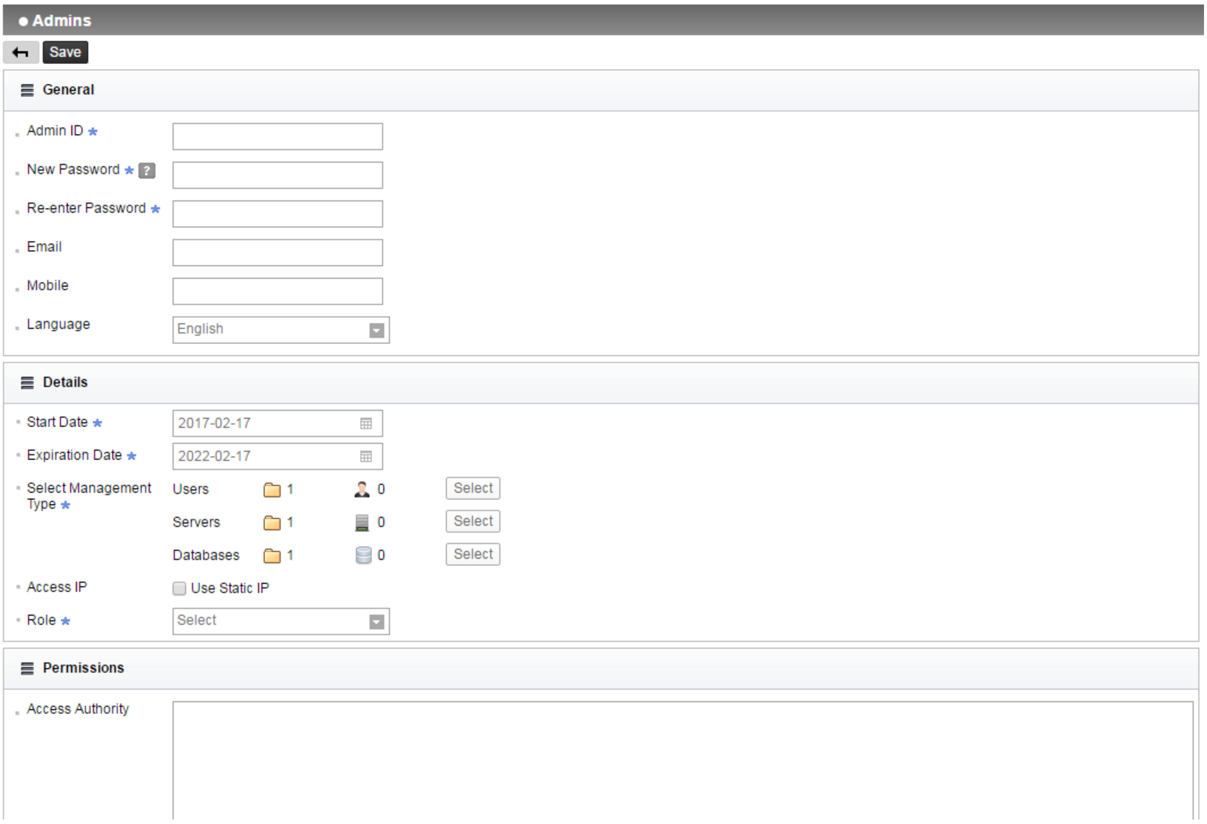
(FIGURE 4-75) DLP+ MINING ENGINE LOGS

4.6.2 Admin

The administrator account has the authority to manage and control the DLP+ Center. The administrator account is created by the administrator of the operating system when installing the product package. In addition, the administrator can create and delete an Operator or Viewer account according to the access department and view permissions. However, the administrator account created during package installation cannot be deleted. [Table 4-29] provides a description of the account permission of DLP+ Center.

[TABLE 4-2924] AUTHORITIES OF INTEGRATED ACCOUNTS

Account	Authorities	Number of accounts
Admin	Control of all authorities, operator, viewer account	1
Operator	View logs in allowed access menu and department	1
View	View logs in limited access menu and department	5



● Admins

↤ Save

General

- Admin ID *
- New Password * ?
- Re-enter Password *
- Email
- Mobile
- Language: English

Details

- Start Date *: 2017-02-17
- Expiration Date *: 2022-02-17
- Select Management Type *:

Users	1	0	Select
Servers	1	0	Select
Databases	1	0	Select

- Access IP: □ Use Static IP
- Role *: Select

Permissions

- Access Authority

(FIGURE 4-76) ADMINISTRATOR REGISTRATION SCREEN

☞ Effective Input Field Range

[TABLE 4-250] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING ADMIN

Item	Effective range	Character	Failure message
Administrator ID	5~20	English	Admin ID is 5 or more characters.
Password	9~35	Numbers, upper and lower case letters, special characters	Enter password.
Check password	9~35	Numbers, upper and lower case letters, special characters	There is no confirmation of password.
Mail	1~200	Numbers, upper and lower case letters, special characters	Enter mail correctly.
Mobile phone	1~20	Numbers	-

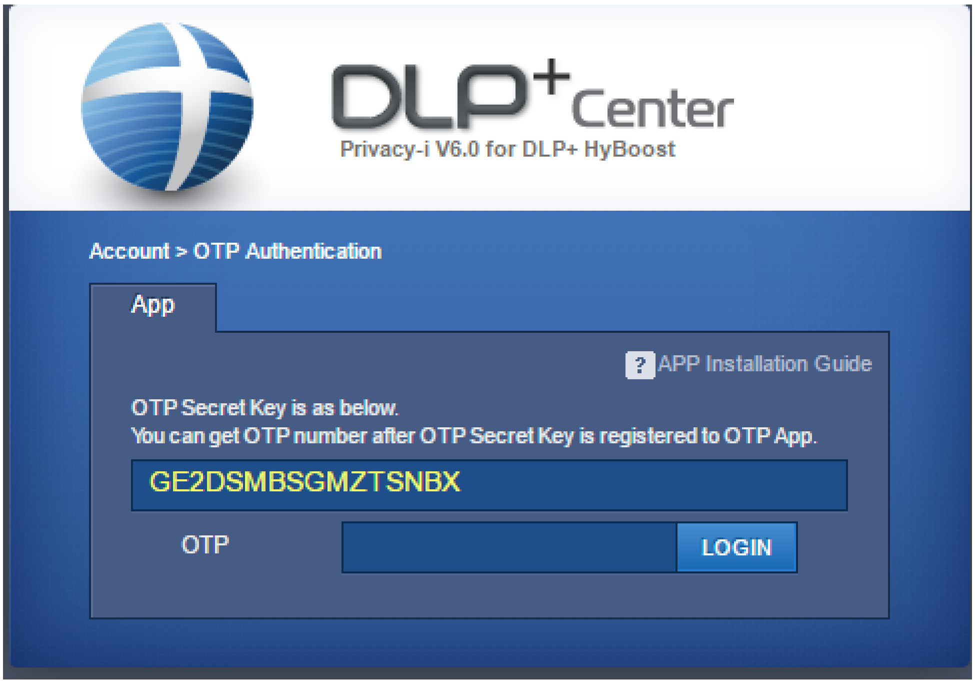
Recommendations

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

- Use of OTP

To enhance the level of security, use of Two-Factor authentication function can be configured, in which ID / PW authentication and OTP (One Time Password) authentication are available. OTP authentication methods include two types of authentications, app authentication / text message authentication. Only one of the two authentications can be selected, and, once selected, the same OTP method will be used in the process. (To change the OTP method, click [Reset OTP private key] in Modification of Admin Account)

※ If a top administrator (Super Admin) cannot receive configured OTP, it is possible to receive through the registered E-mail.



OTP Secret Key is as below.
You can get OTP number after OTP Secret Key is registered to OTP App.

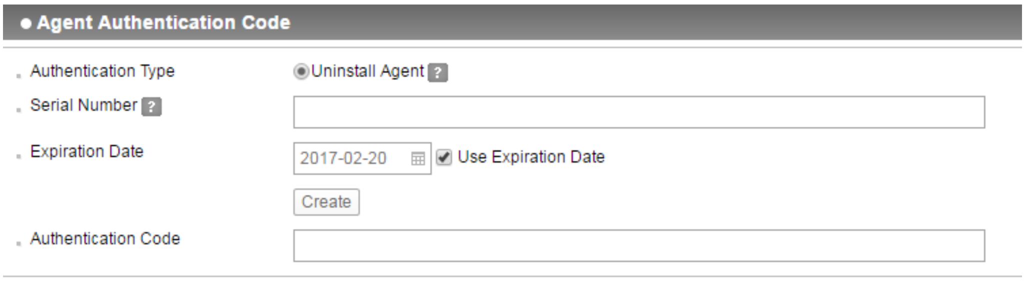
GE2DSMBSGMZTSNBX

(FIGURE 4-77) OTP AUTHENTICATION LOGIN

4.6.3 Tools

4.6.3.1 Generating Agent Delete password

Generate Agent [Delete password] by inputting the serial number transmitted from the Agent.



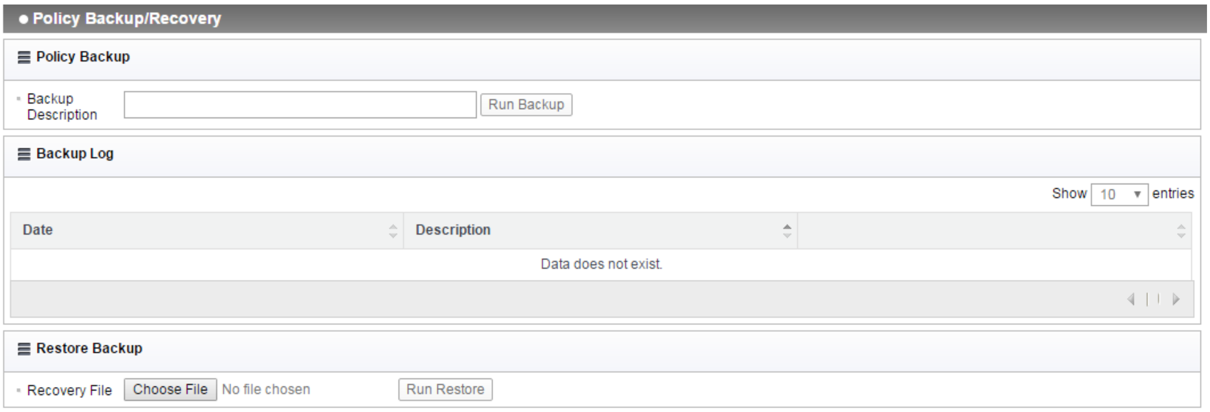
● Agent Authentication Code

Authentication Type	● Uninstall Agent ?
Serial Number ?	
Expiration Date	2017-02-20 ☑ Use Expiration Date Create
Authentication Code	

(FIGURE 4-78) GENERATING AGENT DELETE PASSWORD

4.6.3.2 Policy Backup / Restoration

Backup/restoration is performed on the policy generated in the operation.



● Policy Backup/Recovery

Policy Backup

Backup Description [ ] Run Backup

Backup Log

Show 10 ▾ entries

Date	Description	
Data does not exist.		

Restore Backup

Recovery File Choose File No file chosen Run Restore

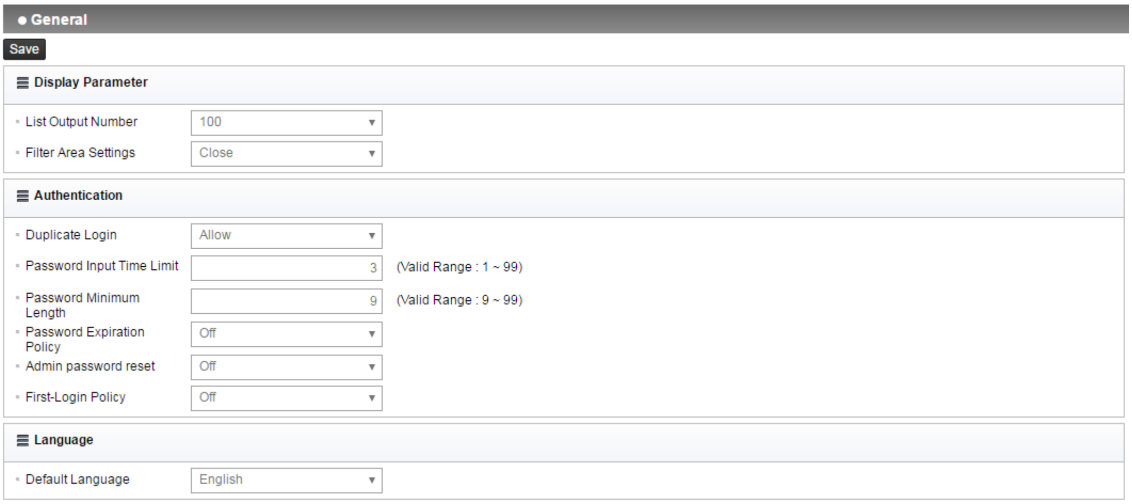
(FIGURE 4-79) SEARCHING SHARED FOLDER

Backup files can be downloaded, and backup policy information can be updated to perform restoration.

4.6.4 Settings

4.6.4.1 General

Default settings of DLP+ Center can be designated.



● General

Save

☰ Display Parameter

List Output Number	100 ▾	
Filter Area Settings	Close ▾	

☰ Authentication

Duplicate Login	Allow ▾	
Password Input Time Limit	3	(Valid Range : 1 ~ 99)
Password Minimum Length	9	(Valid Range : 9 ~ 99)
Password Expiration Policy	Off ▾	
Admin password reset	Off ▾	
First-Login Policy	Off ▾	

☰ Language

Default Language	English ▾	

(FIGURE 4-80) GENERAL

1) List settings

   Number of cases on the log information output to a screen by default and filter area can be configured.

2) Authentication settings

   Password related settings can be made, such as the number of logins and password locks of DLP+ Center, etc.

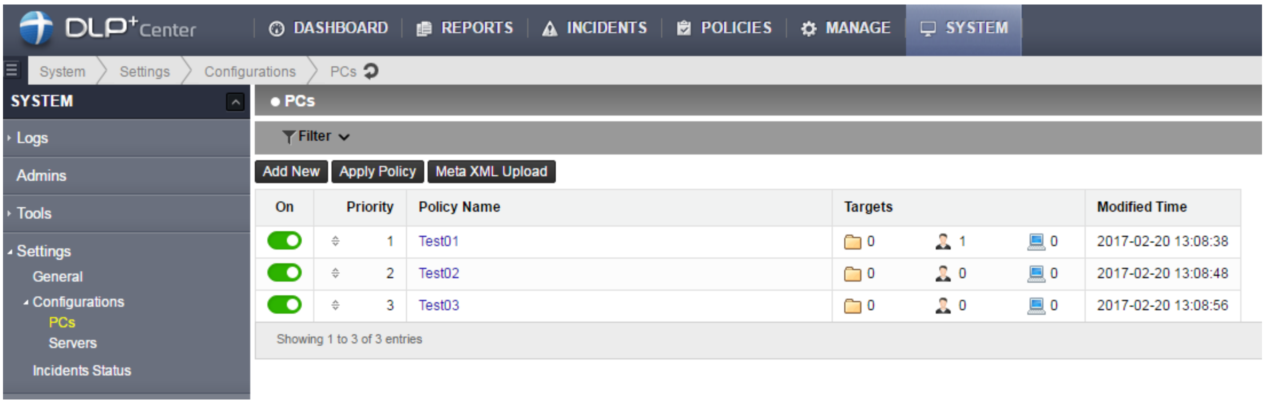
3) Internationalization settings

   The language is designated during server Installation, and the default language settings can be changed in the corresponding options.

4.6.4.2 Configurations

In order to improve the high maintenance cost due to the structure of Privacy-i V5.0 version or earlier, where Agent options are included in the package file, the function of synchronization by generating policy at DLP+Center and transferring policy to Agent when changing the setting values.

Functions are generated from System > Settings > Configurations > PCs screen.

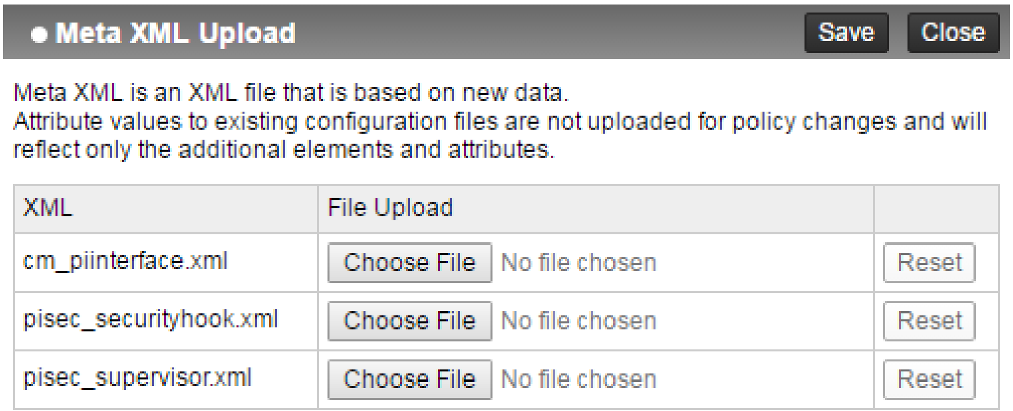


On	Priority	Policy Name	Targets			Modified Time
●	1	Test01	0	1	0	2017-02-20 13:08:38
●	2	Test02	0	0	0	2017-02-20 13:08:48
●	3	Test03	0	0	0	2017-02-20 13:08:56

Showing 1 to 3 of 3 entries

(FIGURE 4-81) CONFIGURATIONS SETTINGS SCREEN

1) Meta XML Upload
Meta XML is an XML file which is the reference when adding new ones. When uploading files, the attribute values configured to the existing Configurations policy are not changed, and only added elements and attributes are reflected. Meta XML can change cm_piinterface.xml, pisec_securityhook.xml, pisec_supervisor.xml.

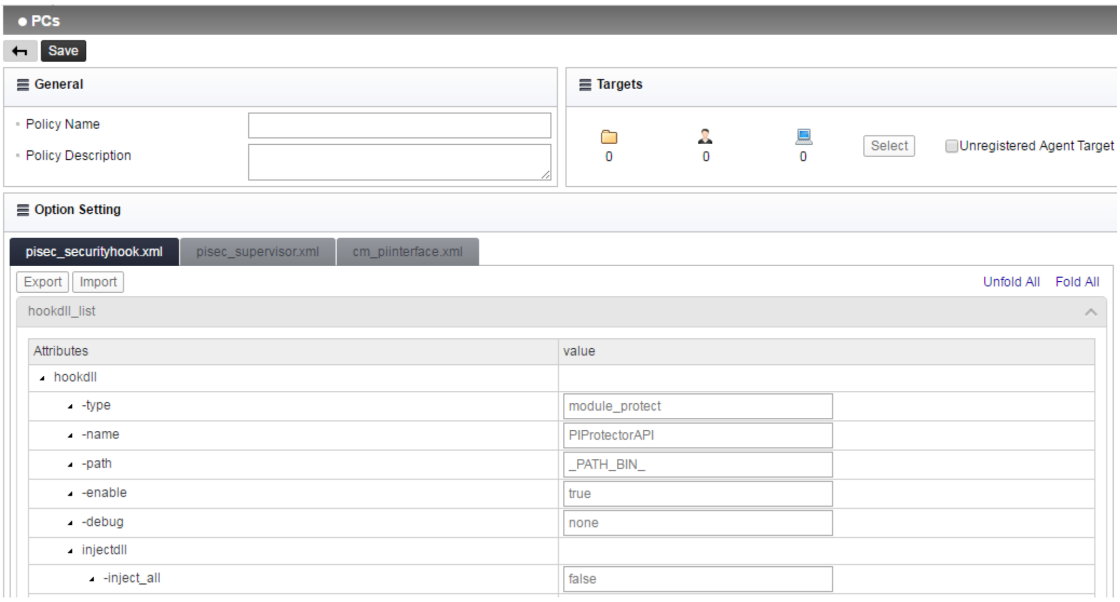


Meta XML is an XML file that is based on new data.
Attribute values to existing configuration files are not uploaded for policy changes and will reflect only the additional elements and attributes.

XML	File Upload	
cm_piinterface.xml	Choose File No file chosen	Reset
pisec_securityhook.xml	Choose File No file chosen	Reset
pisec_supervisor.xml	Choose File No file chosen	Reset

(FIGURE 4-82) META XML UPLOAD

2) Add New
Policy can be generated by changing the options to be changed and designating the object of application, as shown in the Figure. For convenience, functions of exporting and importing each xml have been added.



● PCs

Save

General

- Policy Name
- Policy Description

Targets

0 0 0 Select □Unregistered Agent Target

Option Setting

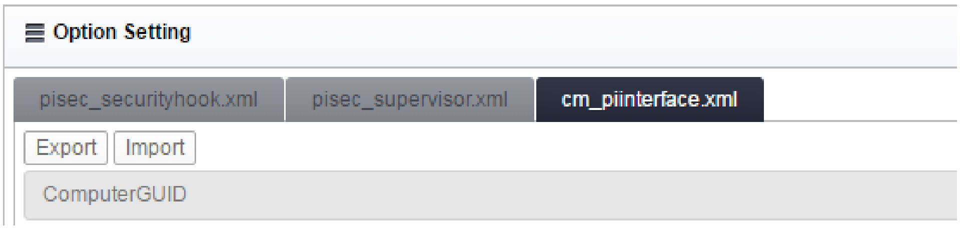
pisec_securityhook.xml | pisec_supervisor.xml | cm_piinterface.xml

Export Import   Unfold All Fold All

hookdll_list

Attributes	value
hookdll	
-type	module_protect
-name	PIProtectorAPI
-path	_PATH_BIN_
-enable	true
-debug	none
injectdll	
-inject_all	false

(FIGURE 4-83) ADD NEW SCREEN



Option Setting

pisec_securityhook.xml | pisec_supervisor.xml | cm_piinterface.xml

Export Import

ComputerGUID

(FIGURE 4-84) XML FILE * DISPLAY WITH OPTIONS CHANGED

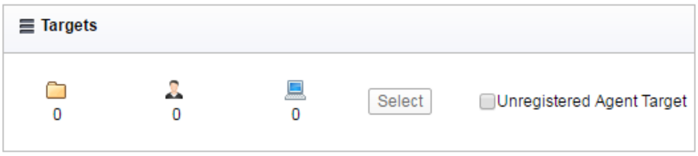
When changing the option of the XML, '*' mark is displayed as in *cm_piinterface.xml, as shown in Figure. Only the xml with * mark displayed reflects the policy. At the first time, however, 3 files are applied at the same time, and then only modified policy is reflected thereafter.

3) Applying policy
The policy is completely reflected by generating Agent option synchronization policy and clicking "Apply Policy" button.

Changed policy is received by updating policy in PIAgent.

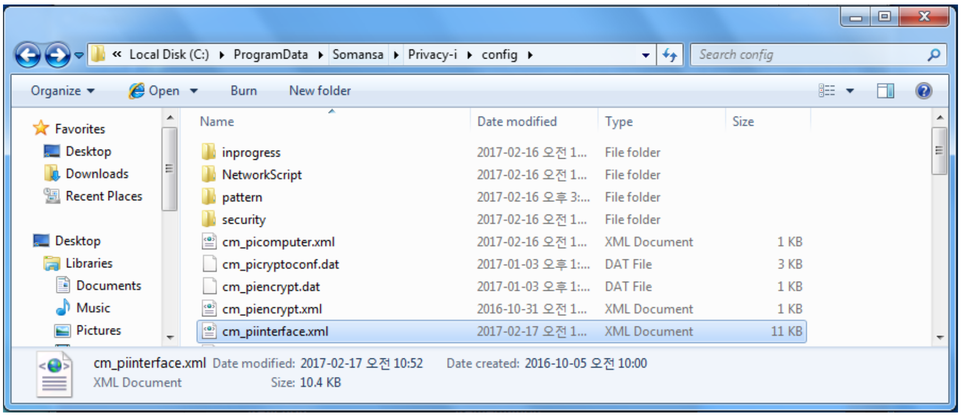
[Caution] Since there is no Policy Settings Apply to Targets in Privacy-i V6.0, "Apply Policy" button should be clicked after generating the policy to reflect the new or modified policy.

4) Unregistered Agent object
In generating policy, if policy is generated to "Unregistered Agent Object" in the object for applying the policy, download the values of cm_piinterface.xml, pisec_securityhook.xml, pisec_supervisor.xml by initially connecting the connection server after completing Agent Installation.



(FIGURE 4-85) UNREGISTERED AGENT OBJECT

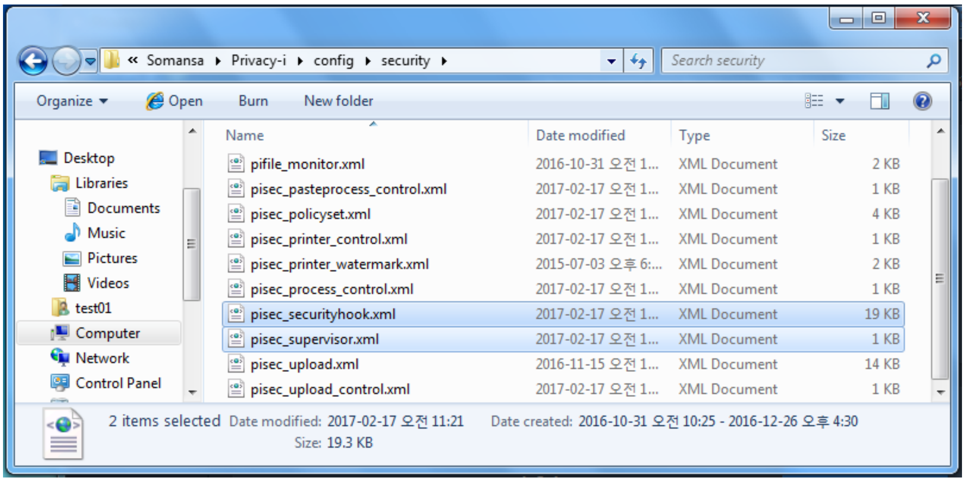
Therefore, in the case of the package with no cm_piinterface.xml, pisec_securityhook.xml, pisec_supervisor.xml files at Agent package, package generation according to the changes in options is not needed since xml can be downloaded by initially accessing the connection server after completing Agent Installation.



Name	Date modified	Type	Size
inprogress	2017-02-16 오전 1...	File folder	
NetworkScript	2017-02-16 오전 1...	File folder	
pattern	2017-02-16 오후 3:...	File folder	
security	2017-02-16 오전 1...	File folder	
cm_picomputer.xml	2017-02-16 오전 1...	XML Document	1 KB
cm_picryptoconf.dat	2017-01-03 오후 1:...	DAT File	3 KB
cm_piencrypt.dat	2017-01-03 오후 1:...	DAT File	1 KB
cm_piencrypt.xml	2016-10-31 오전 1...	XML Document	1 KB
cm_piinterface.xml	2017-02-17 오전 1...	XML Document	11 KB

cm_piinterface.xml Date modified: 2017-02-17 오전 10:52 Date created: 2016-10-05 오전 10:00
XML Document Size: 10.4 KB

(FIGURE 4-86) CM_PIINTERFACE.XML IS CHANGED IMMEDIATELY AFTER PACKAGE INSTALLATION



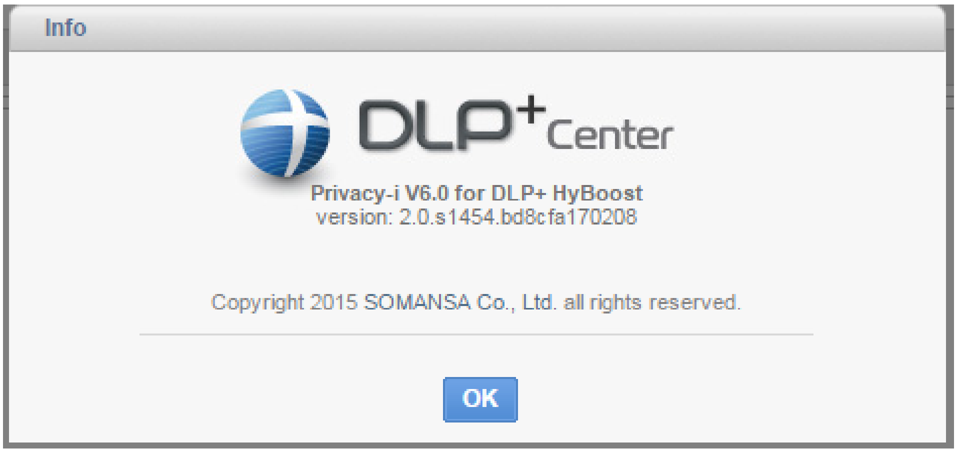
Name	Date modified	Type	Size
pifile_monitor.xml	2016-10-31 오전 1...	XML Document	2 KB
pisec_pasteprocess_control.xml	2017-02-17 오전 1...	XML Document	1 KB
pisec_policyset.xml	2017-02-17 오전 1...	XML Document	4 KB
pisec_printer_control.xml	2017-02-17 오전 1...	XML Document	1 KB
pisec_printer_watermark.xml	2015-07-03 오후 6:...	XML Document	2 KB
pisec_process_control.xml	2017-02-17 오전 1...	XML Document	1 KB
pisec_securityhook.xml	2017-02-17 오전 1...	XML Document	19 KB
pisec_supervisor.xml	2017-02-17 오전 1...	XML Document	1 KB
pisec_upload.xml	2016-11-15 오전 1...	XML Document	14 KB
pisec_upload_control.xml	2017-02-17 오전 1...	XML Document	1 KB

2 items selected Date modified: 2017-02-17 오전 11:21 Date created: 2016-10-31 오전 10:25 - 2016-12-26 오후 4:30
Size: 19.3 KB

(FIGURE 4-87) PISEC_SECURITYHOOK.XML, PISEC_SUPERVISOR.XML IS CHANGED IMMEDIATELY AFTER PACKAGE INSTALLATION

4.6.5 Check TOE version

DLP+ Center version can be checked in the screen. Click Info button on top right of the screen to see the screen for checking the version.



Info

DLP+ Center

Privacy-i V6.0 for DLP+ HyBoost
version: 2.0.s1454.bd8cfa170208

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

(FIGURE 4-88) DLP+ CENTER VERSION CHECK

5. Uninstalling TOE

Contact engineers of Somansa if Privacy-i V6.0 HyBoost needs to be uninstalled.

6. FAQ

Q) What is the confidential data retention control solution?
A) A tool that automatically detects confidential data on a PC, which is designated to be deleted according to governing laws so that personnel can delete the information personally.

Q) What are the types of information that can be detected by the confidential data retention control solution?
A) Documents including resident registration numbers, account numbers, credit card numbers, mobilel phone numbers can be detected.

Q) From what type of file can the confidential data retention control solution detect confidential data?
A) The solution detects confidential data from documents produced in MS Office/HWP/pdf/txt/html/rtf/csv/ and other text formats.

Q) What are the criteria of a confidential data document??
A) Any documents containing information that can identify individuals including customers and staffs, such as account numbers, credit card numbers, resident registration numbers and cell phone numbers.

Q) How can I search confidential data in a PC using the confidential data retention control solution?
A) Click the Privacy-i icon (confidential data detection solution) on the Desktop.

Q) Is detection available for documents with document security (DRM) applied?
A) A quick inspection window appears when the confidential data retention control solution is executed, and detection can be made by checking the DRM document inspection in the quick inspection window.

Q) What is a periodical inspection (Admin inspection)?
A) The periodical inspection is scheduled activity campaign to check whether any employees retain any confidential data that must be deleted from the PC on a monthly basis. Users can view the results through a notification message such as Start Inspection / Running / Inspection Completed.

Q) How can I process the task later when performing the periodical inspection (admin inspection)?
A) Check the ‘Perform later’ button in the notification window. However, you will see pop-up window that appears periodically.

Q) The confidential data retention control solution is not executed.
A) The solution can be executed when intra network is not connected or when the periodical inspection (admin inspection) is running.

Q) How can I check a confidential data file detected on my PC?
A) Users can check depending on whether users are running the periodical inspection (admin inspection) or Inspection by the user when checking confidential data extracted logs. Please see the relevant pages for more information.

Q) How can I stop the inspection in the periodical inspection (admin inspection)?
A) Users cannot stop the procedure of inspection when the periodical inspection (admin inspection) is in progress. When the user runs the inspection in person, however, it can be stopped through the “Stop inspection” button.

Q) How do I retrieve the specific confidential data content existing in an extracted confidential data file?
A) Users can view confidential data details through the "View File Details" menu, which appears when you select the file on the View Log List and right-click.log.

Q) I need a description of the function buttons on the View Log List screen after inspection is completed.
A) The functions include Select All, Move, Delete, Statistics and Reports. Please see the relevant pages for detailed instructions.

Q) What should I do if a confidential data file is detected?
A) ① For files needed for business, specify it as "General (Business)" in the confidential data categorization menu, and make sure to delete it when the task is completed. ② For files related to personal life, specify it as "Private (Personal)". ③ For a detection error that does not contain confidential data, specify it as "Exception File". ④ Other files must be completely deleted. When storing a confidential data file in a PC, you must encrypt the file and completely delete files specified for business after the task is completed.

Q) How do I completely delete detected files?
A) Select the files to be deleted in the View Log List, and click the "Delete" button.

Q) How can I encrypt the detected files?
A) Select the corresponding files in the View Log List, and click the "Encryption" button log. When a document security screen appears, conventional encryption methods can be used.

Q) I opened and checked the file detected to contain confidential data, but there is no confidential data in the file.
A) This may occur when detected contents are hidden, charts/graphs are linked (OLE), or there is a detection error matching the confidential data pattern. Please see the relevant pages for more information.

Q) What does "Other Detection" mean in the View Log after inspection is completed?
A) Other Detection means it is unable to check content due to an encrypted file through a self-encrypting function (ex: MS Office, ZIP password settings, etc.)

Q) I have run the periodical inspection (remote inspection). How are the results processed?
A) The results of the periodical inspection (remote inspection) can be checked by a user on the corresponding PC. In addition, the summary statistics for each team/user (number of detections) are automatically sent to the team head via E-mail. The team head needs to check the detected data content and should perform continuous management so that unnecessary confidential data can be deleted.
※When running the inspection by a user, the E-mail will not be sent and only the user can check the results.

Q) How can I re-run the user information input window when the user information was not entered during the agent installation?
A) The user information input window appears again when the PC is restarted.

Q) What is the key-shaped icon in the lower-right corner of my desktop after the final installation?
A) The information window of the agent icon is configured with 6 menus, including Running Privacy-i, View Policy, View Event Log, Policy Update, Module Update and Re-login.

Q) How can I uninstall the installed confidential data retention control solution (TOE Agent)?
A) TOE Agent cannot be uninstalled by the user. If it needs to be uninstalled, contact engineers at Somansa.

Q) Is there a function for preventing the unauthorized access of a server and client?
A) There is an xml-based command protocol which is defined by the SOMANSA product through a TCP/IP-based server service communication port. When a service communication port of the unauthorized server connects and transfers a random dummy string (using, for example, Telnet), this will be ignored by the server service. Also, for a client which is used by an administrator, the account will be automatically locked for a certain period of time when login authentication fails 5 times. In addition, if the same account is connected to the client simultaneously in two places, the prior connection will be automatically shut down with an alert message.

Q) What should I do when a server's operating system and hardware fails, other server functions fail, and server recovery is needed due to a user error?
A) Report the failure and request maintenance support at the SOMANSA Help Desk in the first. After receiving a remote or on-site inspection, please take action, such as patching the module, updating or re-installing the product depending on the inspection results of the engineer.

Q) Do you provide functions to check events regarding product errors or the causes of errors?
A) If an error such as abnormal termination of service and program termination occurs, please check the event logs of your operating system. For the detailed inspection for an error, we recommend you to receive an inspection through the SOMANSA Help Desk Request and Inquiries for On-Line/Off-Line support.

Q) Do you provide education courses for users to operate and use the product?
A) The user education courses provided after purchasing the product are listed in the following table.

[TABLE 6-1] USER EDUCATION COURSES

Item	Contents	Subject/Period	Note
Education on product	Understands the product (purposes and main functions) Introduces basic function of the product and technologies	Operators and administrators of the product / Before installing the product	Education on site 2 hr. or less
Education on operation	Methods for basic settings for operating the product Methods for setting and applying policies Methods for distributing and updating Agent Methods for managing and retrieving log	Operators and administrators of the product / After installing the product, and after completing building and before distributing Agent	Education on site 4 hr. or less
Education on advanced operation	Methods of applying and utilizing policies for each situation Methods of countering failures (analysis/measures) Cases of actual uses and other cases are shared	Operators and administrators of the product / When requested, or on the day of regular education of the company once a quarter	Limited to customers with free maintenance of one year, or with paid maintenance.

7. Definitions of Terms

Account Management Log
Added, modified and deleted logs of an administrator account and identified and approved logs of an authorized administrator

Viewer
Has permission to audit logs for modified history of the DLP+ Center (restricted access right))

Security Log
Audit logs left in MS SQL while running security functions at the DLP+ Center, which refer to Information Management Log, Policy Management Log, Account Management Log, System Log, etc.

User
Refers to anyone who uses a PC with the agent installed in a company.

User Data
Data generated for a user by the user, which does not affect product operation.

Identity
Used for identifying an authorized user

System Administrator
An authorized administrator who is in charge of product operation and environment settings in the control panel

System Log
Updated log on policies and patterns

Administrator
Person with the authority to edit policies in the DLP+ Center.

Agent
The Agent is installed on a user PC side, and operates in Windows/Linux environment. The Agent runs a scan when an agent user inspects confidential data on his/her own PC, or when an administrator forcefully scans confidential data on a user PC from the server.

DBMS
DB server where all audit logs are saved. PostgreSQL is selected and used as the DB server for this product.

External Interface
General term for various ports that can output data saved in the host, which includes USB, IDE, SATA, e-SATA, IEEE1394, PCMCIA, LAN/WLAN, Bluetooth, Serial/Parallel Port, Infrared port, etc.

Threat Agent
Unauthorized user/administrator or external IT entity that poses threats such as illegal access, modification and deletion of assets.

Authorized Administrator
Refers to the system administrators, administrators, operators and viewers.

Authentication Data
Information used to verify the identity of a user.

Operator
A person among authorized administrators, who can view all audit data, and add/delete/modify policy/pattern

Information Management Log
Edit Log / Statistic Report Output Log of a PC user in a company who uses a user PC log collected through the agent and History Log / Agent that the admin checks Policy Management

Policy Management Log
Log with pattern/policy edited by an administrator or an operator

Organizational Security Policies
Security rules, procedures, practices, guidelines, etc., which are enforced by the organization

Contents
Various information or contents that are stored in the host or provided through a network, which can be represented in a particular file format (HWP, TXT, DOC, PDF, DOCX, PPT, PPTX, XLS, XLSX, ZIP, etc.), or can be information itself

KLiB
Encryption module which made by Korea University, and has been approved by National Intelligence Service in 2014. The module includes the encryption algorithms listed in [TABLE7-1], and TOE, the subject of the evaluation, removes weaknesses by using the encryption module of KLiB (v2.1).

[TABLE 7-1] LIST OF ENCRYPTION ALGORITHMS PROVIDED BY KLIB (V2.1)

Category	Contents
Symmetric key algorithm	ARIA, SEED, AES, DES
Public key algorithm	RSAES-PKCS-v1_5, RSAES-OAEP-v2.1
Electronic signature algorithm	RSASSA-PKCS-v1_5, RSASSA-PSS, ECDSA (WTLS C-165/151/164, FIPS K-163)
Hash algorithm	SHA-2/256/384/512, MD5
MAC algorithm	HMAC (hash = MD5, SHA-2), CBC-MAC (cipher = ARIA, SEED, DES, AES)
Random number generator	FIPS PUB 186-2 PRNG, ANSI X9.62 PRNG

DLP+ Center
Administration console that an administrator/operator/viewer can log into, to set confidential data pattern policy rules, view reports, and register agent users, etc.

PKI (Public Key Infrastructure)
Public key-based structure, which guarantees integrity and confidentiality of data for various applications such as Web, network, DB and mail, based on encryption/encoding, electronic signature and user authentication, and generates the function of user non-repudiation

Protocol
Rules for communication to provide user services such as E-mail, Messenger, File Upload/Download and Web, which collectively refers to SMTP, HTTP, HTTPS, FTP, SFTP, SSH, TELNET, IMAP, IRC, RDP, etc.