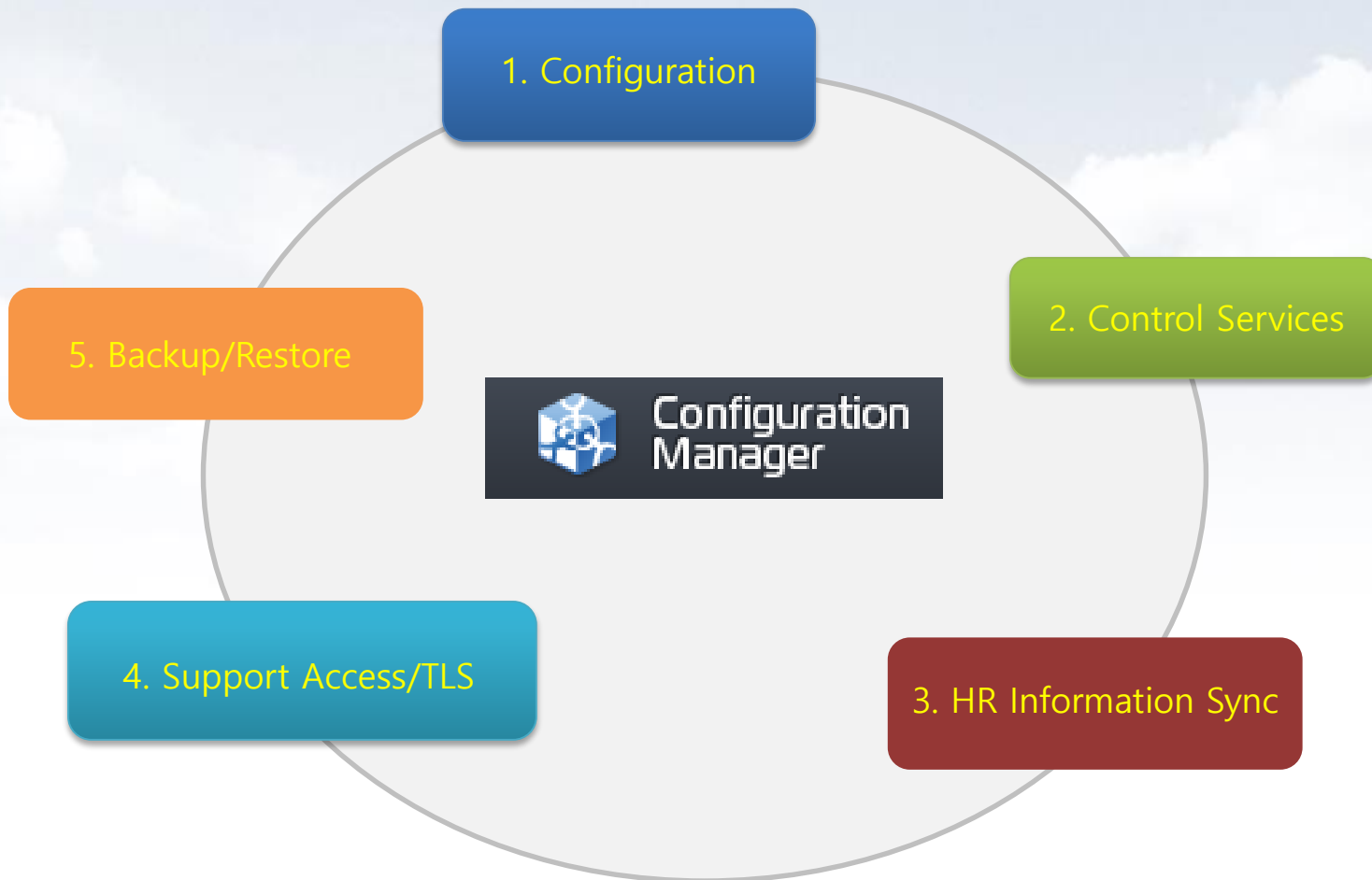




# Data Loss Prevention





## CONTENTS

- I. Structure
- II. General Setup the Server
- III. Specific Setup the Server
- IV. CM Access
- V. License
- VI. Common
- VII. Mail-i
- VIII. Proxy
- IX. Common
- X. System Setting



## I. Structure

- Main Module, flow chart and port information used by Mail-i

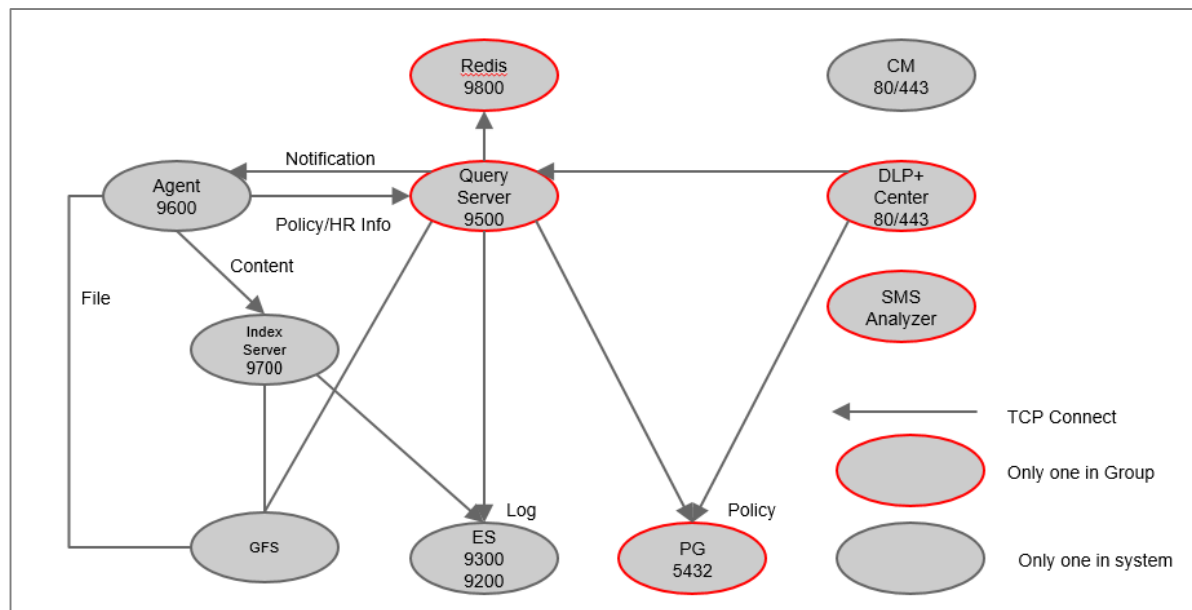
- **Agent (NDLP-Agent)** : refers to Traffic-Agent processing network traffic and Content-Agent processing protocols.

- **CM(Configuration Manager)** : provides web based user interface for the operation and control of the product such as database configuration, Agent execution and termination.

- **DLP+Center** : provides web based user interface for tasks such as incident (log) view, policy management and reports and so on.

- **Query Server** : views the incidents and deliver the policies and HR data to the Agent.

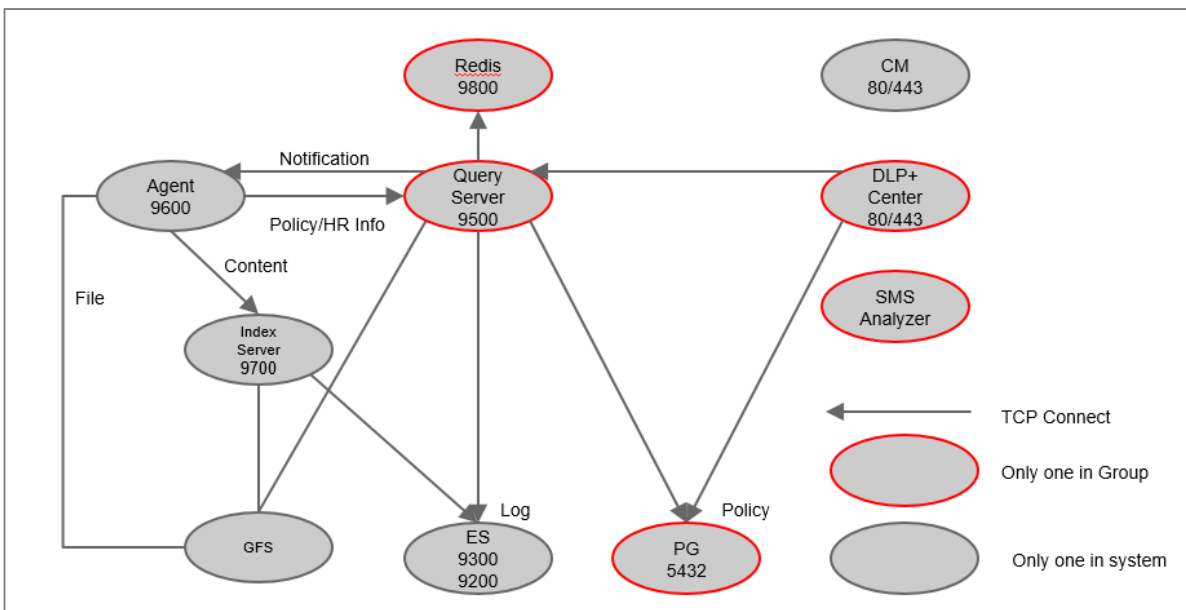
- **Indexing Server (Indexer)** : saves the incident an Agent has created in ElasticSearch.





## I. Structure

- **Cache Server (Redis)** : works as a temporary storage for viewed incidents.
- **SMSAnalyzer** : detects data patterns such as resident registration numbers from the saved incidents (Content/Attachment files).
- **SMSSummary** : performs scheduled summary task for incidents with patterns.
- **ElasticSearch (henceforth ES)** : saves the incidents in the form of an index.
- **GlusterFS (henceforth GFS)** : saves the attachment file of the incidents.
- **PostgreSQL** : saves system configuration, HR data, policies, data mining (reports) and audit logs.





## I. Structure

All-in-one
CM (Configuration Manager)
Indexer (Tomcat_indexer)
Agent
Elasticsearch
GlusterFS
Queryserver (Tomcat_queryserver)
DLP+Center
Redis
Postgresql
SMSAnalyzer
SMSSummary

Agent
CM (Configuration Manager)
Indexer (Tomcat_indexer)
Agent
Elasticsearch
GlusterFS
Storage
CM (Configuration Manager)
Queryserver (Tomcat_queryserver)
Elasticsearch
GlusterFS
DLP+Center
Redis
Postgresql
SMSAnalyzer
SMSSummary

Agent
CM (Configuration Manager)
Indexer (Tomcat_indexer)
Agent
Elasticsearch
GlusterFS
Main Storage
CM (Configuration Manager)
Queryserver (Tomcat_queryserver)
Elasticsearch
GlusterFS
DLP+Center
Redis
Postgresql
SMSAnalyzer
SMSSummary
Sub Storage
Elasticsearch
GlusterFS



## II. General Setup the Server

### 1. Configuration Manage IP

- recommend manage IP set up for eth0

- 1) Connect server
- 2) Edit for vi editor : vi  
*/etc/sysconfig/network-scripts/ifcfg-eth0*
- 3) Change the IPADDR, NETMASK,  
GATEWAY, ETC

### 2. Change Server Local Time

- 1) *cp /usr/share/zoneinfo/"YOUR TIME"  
/etc/localtime*

### 3. Change Hostname

- hostname must be unique

- 1) Move to path : *cd /hyboost/init*
- 2) Execute script : *./all.init.sh*

```
DEVICE=eth0
HWADDR=08:00:27:07:0F:09
TYPE=Ethernet
UUID=71ade838-0cff-424f-91eb-acf9eb620724
NM_CONTROLLED=yes
ONBOOT=yes
BOOTPROTO=none
IPADDR=192.168.1.111
GATEWAY=192.168.1.1
DNS1=8.8.8.8
DNS2=8.8.8.8
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

```
[root@hello sysadmin]# date
Thu Jul 20 14:38:44 PDT 2017
[root@hello sysadmin]# cp /usr/share/zoneinfo/Asia/Seoul /etc/localtime
cp: overwrite `/etc/localtime'? y
[root@hello sysadmin]# date
Fri Jul 21 06:38:50 KST 2017
[root@hello sysadmin]#
```



## III. Specific Setup the Server

### 1. All-in-one

- If you run the *all-init.sh*, no further configuration is required.

```
Changing hostname must be done before serviced in site.
We don't have any responsibility for changing hostname when it is on service.
There will be problem with those type of hostname. Type the new hostname to use.
- Don't use _ or space inside the hostname.

hostname : sky

===== Check HostName =====
The hostname you entered is [ sky ]
Do you want to continue?
y. yes
n. no
>> y

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4 sky
192.168.1.116 sky

===== Restarting Postgresql =====
Stopping postgresql-9.3 service: [ OK ]
Starting postgresql-9.3 service: [ OK ]

===== QueryServer Reconfigure =====
Check QueryServer : ip=https://sky

===== ES/GFS Reconfigure =====
>>>>> WARNING <<<<<<
ES/GFS Reconfigure is only required for All-in-One System.
If it's multi-node(storage) system or system that agent and storage is separated,
check for the elasticsearch/glusterfs guide.
Have you understand the warning and going to continue reconfiguration ? (y/n)
>> y

===== Elasticsearch Reconfigure =====
Stopping elasticsearch: [ OK ]
node.name: 'sky'
discovery.zen.ping.unicast.hosts: ['sky:9300']
network.host: ['sky','localhost']
Starting elasticsearch: [ OK ]

===== GlusterFS Reconfigure =====
```





## III. Specific Setup the Server

### 2. Agent 1 + Storage 1

#### 2.1 Hostname

- 1) Edit for vi editor : `vi /etc/hosts`
- 2) At the bottom, enter IP and hostname of each server (Applies to all servers)

#### 2.2 ES of Agent Server

- 1) Edit for vi editor : `vi /etc/elasticsearch/elasticsearch.yml`
- 2) At the bottom, change value (node.master:true, node.data:false)
- 3) Add Storage server host (discovery.zen.ping.unicast.hosts:['agenthost:9300','storagehost:9300'])

#### 2.3 ES of Storage Server

- 1) Edit for vi editor : `vi /etc/elasticsearch/elasticsearch.yml`
- 2) At the bottom, change value (node.master:true, node.data:true)
- 3) Add Storage server host (discovery.zen.ping.unicast.hosts:['agenthost:9300','storagehost:9300'])
- 4) ES service of Agent and Storage Server restart

```
127.0.0.1 localhost localhost.localdomain localhost4 lo
calhost4.localdomain4 agentserver
::1 localhost6.localdomain6 localhost6
agentserver
192.168.1.112 agentserver
192.168.1.114 storageserver
```

```
node.master: true
node.data: false
node.name: 'agentserver'
discovery.zen.ping.unicast.hosts: ['agentserver:9300', 'st
orageserver:9300']
network.host: ['agentserver', 'localhost']
```

```
node.master: true
node.data: true
node.name: 'storageserver'
discovery.zen.ping.unicast.hosts: ['storageserver:9300', '
agentserver:9300']
network.host: ['storageserver', 'localhost']
```



## III. Specific Setup the Server

### 2.4 GFS of Storage Server

- 1) Move to path : `cd /hyboost/init`
- 2) Execute script : `/gfs.setting.sh`
  - a. Select **1.GlusterFS All-in-one System**

### 2.5 GFS of Agent Server

- 1) Move to path : `cd /hyboost/init`
- 2) Execute script : `/gfs.connect.sh`
  - a. Insert Storage Server hostname

```
==== GlusterFS Setting Service ====
!!!!After the script starts, the data is initialized!!!!
1. GlusterFS All-in-one System
2. GlusterFS Multi System ( Multi System )
3. GlusterFS Add Brick
4. Stop
>> 1
```

```
==== GFS linked Storage Server ====
Please enter Hostname for Storage Server
hostname: Mainstorage
Storage Hostname is [ Mainstorage ]
Do you want to continue?
y.Yes
n.No
>>y
```



## III. Specific Setup the Server

### 3. Agent 2 + Storage 2

#### 3.1 Hostname

- 1) Edit for vi editor : `vi /etc/hosts`
- 2) At the bottom, enter IP and hostname of each server (Applies to all servers)

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4 Mainstorage
192.168.3.8 Mainstorage
192.168.3.10 Subsotrage
192.168.3.11 Agent1
192.168.3.12 Agent2
```

#### 3.2 ES of Agent Servers

- 1) Edit for vi editor : `vi /etc/elasticsearch/elasticsearch.yml`
- 2) At the bottom, change value (node.master:true , node.data:false)
- 3) Add Storage server host (network.host:['agenthost1:9300', 'agenthost2:9300', storagehost1:9300', storagehost2:9300'])

```
node.name: 'Agent1'
discovery.zen.ping.unicast.hosts: ['Agent1:9300','Agent2:9300','Mainstorage:9300','Substorage:9300']
network.host: ['Agent1','localhost']
path.repo: ['/somansa/backup/maili','/somansa/backup/wk','/somansa/backup/pvi']
index.max_result_window: 2147483647
node.master: true
node.data: false
indices.fielddata.cache.size: 5GB
```



## III. Specific Setup the Server

### 3.3 ES of Storage Servers

- 1) Edit for vi editor : `vi /etc/elasticsearch/elasticsearch.yml`
- 2) At the bottom, change value (node.master:true , node.data:true)
- 3) Add Storage server host (discovery.zen.ping.unicast.hosts:[agent host1:9300, agenthost2:9300, storagehost1:9300, storagehost2:9300, localhost'])
- 4) ES service of Agent and Storage Server restart

```
node.name: 'Mainstorage'  
discovery.zen.ping.unicast.hosts: ['Agent1:9300', 'Agent2:9300', 'Mainstorage:9300', 'Substorage:9300']  
network.host: ['Mainstorage', 'localhost']  
path.repo: ['/somansa/backup/maili', '/somansa/backup/wk', '/somansa/backup/pvi']  
index.max_result_window: 2147483647  
node.master: true  
node.data: true  
indices.fielddata.cache.size: 5GB
```



## III. Specific Setup the Server

### 3.4 GFS of Main Storage Server

- 1) Service glusterd start
- 2) Move to path : `cd /hyboost/init`
- 3) Execute script : `/gfs.init.sh`
- 4) Execute script : `/gfs.setting.sh`
  - a. Select **2. GlusterFS Multi System**
  - b. Select **y. Add Brick Service Start**
  - c. Insert Storage Count 1
  - d. Insert Sub Storage hostname and IP

※ If more storage server exist, please add the below step
- 5) Execute script : `/gfs.setting.sh`
  - 1) Select **3. GlusterFS Add Brick**
  - 2) Insert Storage Count 1 or more
  - 3) Insert Sub Storage hostname and IP
- 6) How to check
  - 1) Gluster volume info
  - 2) Gluster volume status
  - 3) Gluster peer status

```
[root@Mainstorage init]# ./gfs.init.sh
umount: /somansa/data/gfs_data: not mounted
Stopping volume will make its data inaccessible. Do you want to continue? (y/n) y
volume stop: gfs_volume: failed: Volume gfs_volume does not exist
Deleting volume will erase all information about the volume. Do you want to continue? (y/n) y
```

```
==== GlusterFS Setting Service ====
!!!!After the script starts, the data is initialized!!!!
1. GlusterFS All-in-one System
2. GlusterFS Multi System ( Multi System )
3. GlusterFS Add Brick
4. Stop
>> 3

==== GlusterFS Add Brick ====
Do you want to add a brick to the volume?
y. Add Brick Service Start
n. stop
>> y

How many additional storage would you like to add?
Storage Count >> 1

Please enter the hostname of the additional storage.
Hostname : Substorage
Please enter the IP of the hostname.
IPADDR : 192.168.3.10
```



## III. Specific Setup the Server

### 3.5 GFS of other Storage Server

- 1) Service glusterd start

```
[root@Substorage ~]# service glusterd restart
Starting glusterd: [ OK ]
```

### 3.6 GFS of Agent Servers

- 1) Move to path : `cd /hyboost/init`
- 2) Execute script : `/gfs.connect.sh`

```
==== GFS linked Storage Server ====
Please enter Hostname for Storage Server
hostname: Mainstorage
Storage Hostname is [ Mainstorage ]
Do you want to continue?
y.Yes
n.No
>>y
```

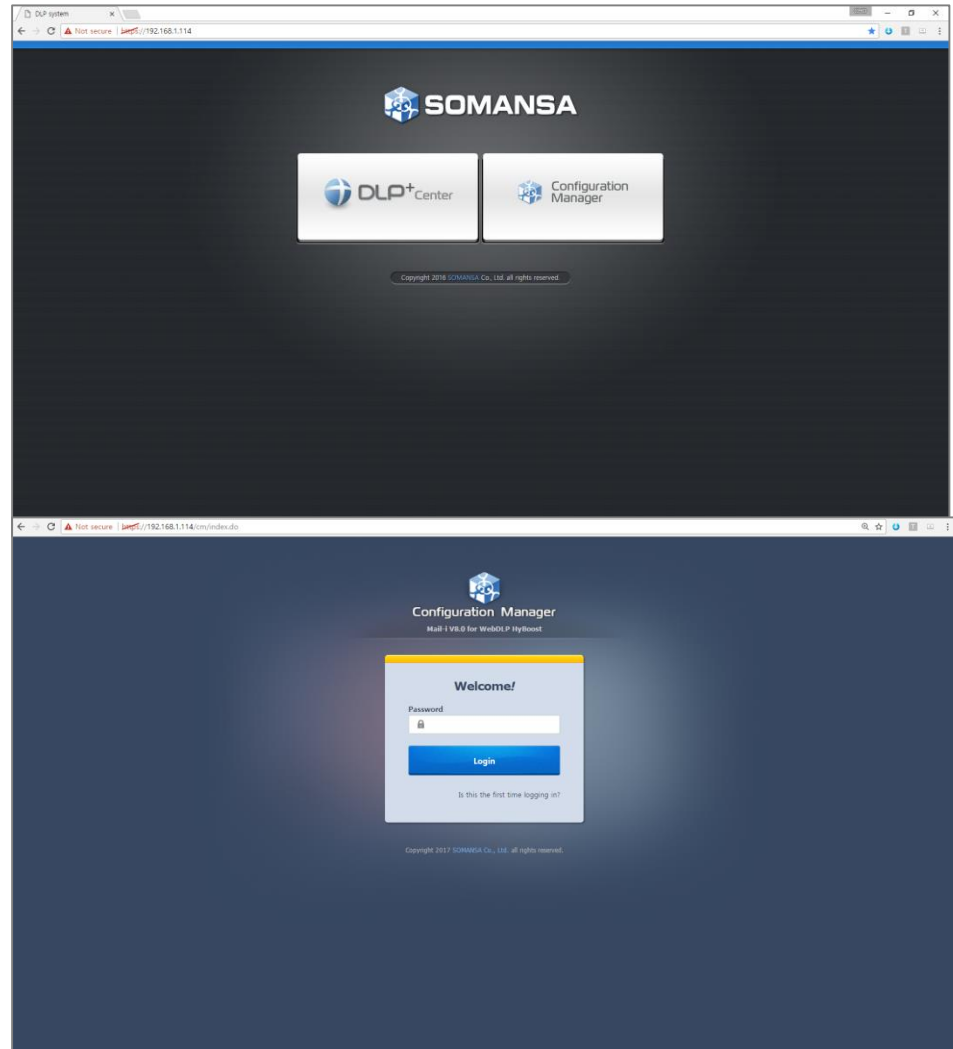


## IV. CM (Configuration Manager) Access

### 1. Access the CM

- 1) The management console.
- 2) Enter the <https://IPAddress> in web browser
- 3) Click the **Configuration Manager**

### 2. Login





## V. License

### 1. License Update

- Without a license, CM can't be set-up

- 1) Select **Setting button**
- 2) Click **Choose File** and Select **License File**
- 3) Click **Choose File** and Select **Serial File**
- 4) Click **Update**
- 5) Restart CM

#### License Update

License File	<input type="button" value="Choose File"/> No file chosen
Serial File	<input type="button" value="Choose File"/> No file chosen
Memo (Optional)	<input type="text"/> <input type="button" value="Update"/>

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





## VI. Common

### 1. DB Connection

- Postgresql default Port is 5432.
- All-in-one structure. If you have separate DB Storage, connection to DB Storage.

- 1) Select **Common > General Settings > Database**
- 2) Enter Connection Settings
- 3) Click **Check Connection**
- 4) Click **OK**

### 2. Generate Schema

- 1) Check DLP+ Center and click **Generate**
- 2) Check Mail-i and click **Generate**

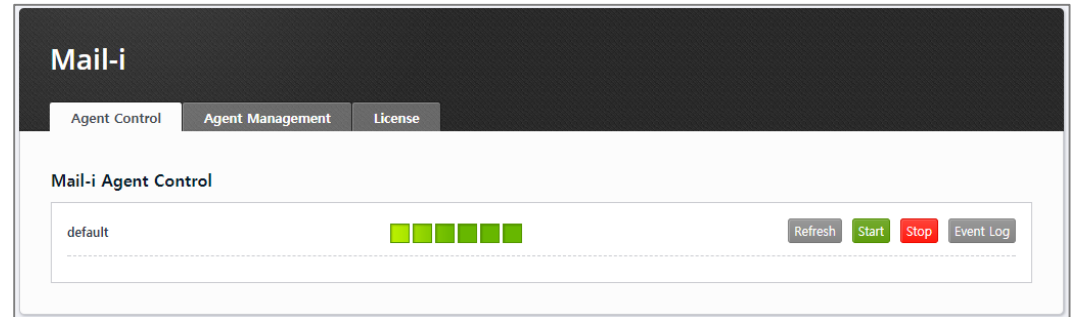
The screenshot displays the 'Common General Settings' interface. It features two tabs: 'Database' (selected) and 'MQTT Settings'. Under the 'Database' tab, there is a 'Connection Settings' section with four input fields: 'Database' (192.168.1.114), 'Port' (5432), 'Login' (postgres), and 'Password'. Below these fields are two buttons: 'Check Connection' and 'OK'. The 'Product Schema Management' section below has two radio buttons: 'DLP+ Center' (selected) and 'Mail-i'. A 'Generate Schema' button is located to the right of these options.



## VII. Mail-i

### 1. Agent Service Control

- 1) Select **Mail-I > Agent Control**
- 2) Click **Start** or **Stop** you want to control Service





## VII. Mail-i

### 2. Agent Management

#### 2.1 All-in-one structure

- 1) Select **Mail-i > Agent Management**
- 2) Click **Agent Name 'default'**
- 3) Enter Description
- 4) Enter 127.0.0.1 in Search Server IP & Indexing Server IP
- 5) Enter default port information
  - ※ Default port information : Agent Port 9600 , Search Server Port 9500 , Indexing Server Port 9700
- 6) Select protocol you want Agent to analyze in the default Agent Function
  - ※ If this functions is unchecked, it does not analyze any policies in DLP+Center.
- 7) Click **Save**

### Mail-i

Agent Control | **Agent Management** | License

#### Agent Management

Agent Name	Agent UID	Agent Description	Agent IP:Port	Search Server IP:Port	Search Engine IP:Port
default	wy6vza0	default	192.168.1.114:9600	127.0.0.1:9500	127.0.0.1:9700

Agent Name	default	Agent UID	wy6vza0
Description	default		
Agent IP	192.168.1.114	Agent Port	9600
Search Server IP	127.0.0.1	Search Server Port	9500
Indexing Server IP	127.0.0.1	Indexing Server Port	9700

#### default Agent Function

Unfold All | Fold All

Electronic Mail

Select All | Dismiss All

SMTP  POP3  IMAP

Web Mail

Instant Messaging

Remote Access

Networking

Social Network Service

File Storage and Sharing

Personal File Sharing

Anonymizer



## VII. Mail-i

### 2. Agent Management

#### 2.2 Agent and Separate DB structure

- Storage DB Server doesn't have agent configuration. Only Agent Server has this configuration.

- 1) Select **Mail-i > Agent Management**
- 2) Click **Agent Name 'default'**
- 3) Enter Description
- 4) Enter Main Storage Server IP in Search Server IP
- 5) Enter 127.0.0.1 in Indexing Server IP
- 6) Enter default port information
  - ※ Default port information : Agent Port 9600 , Search Server Port 9500 , Indexing Server Port 9700
- 7) Select protocol you want to Agent to analyze in default Agent Function
  - ※ If this functions is unchecked, it does not analyze any policies in DLP+Center.
- 8) Click **Save**

The screenshot shows the 'Mail-i' interface with three tabs: 'Agent Control', 'Agent Management', and 'License'. The 'Agent Management' tab is active, displaying a table with one agent entry and a form below it.

Agent Name	Agent UID	Agent Description	Agent IP:Port	Search Server IP:Port	Search Engine IP:Port
default	wy6vza0	default	192.168.1.114:9600	192.168.1.112:9500	127.0.0.1:9700

The form below the table contains the following fields:

- Agent Name: default
- Agent UID: wy6vza0
- Description: default
- Agent IP: 192.168.1.114
- Agent Port: 9600
- Search Server IP: 192.168.1.112
- Search Server Port: 9500
- Indexing Server IP: 127.0.0.1
- Indexing Server Port: 9700

Buttons for 'New' and 'Save' are located at the bottom right of the form.

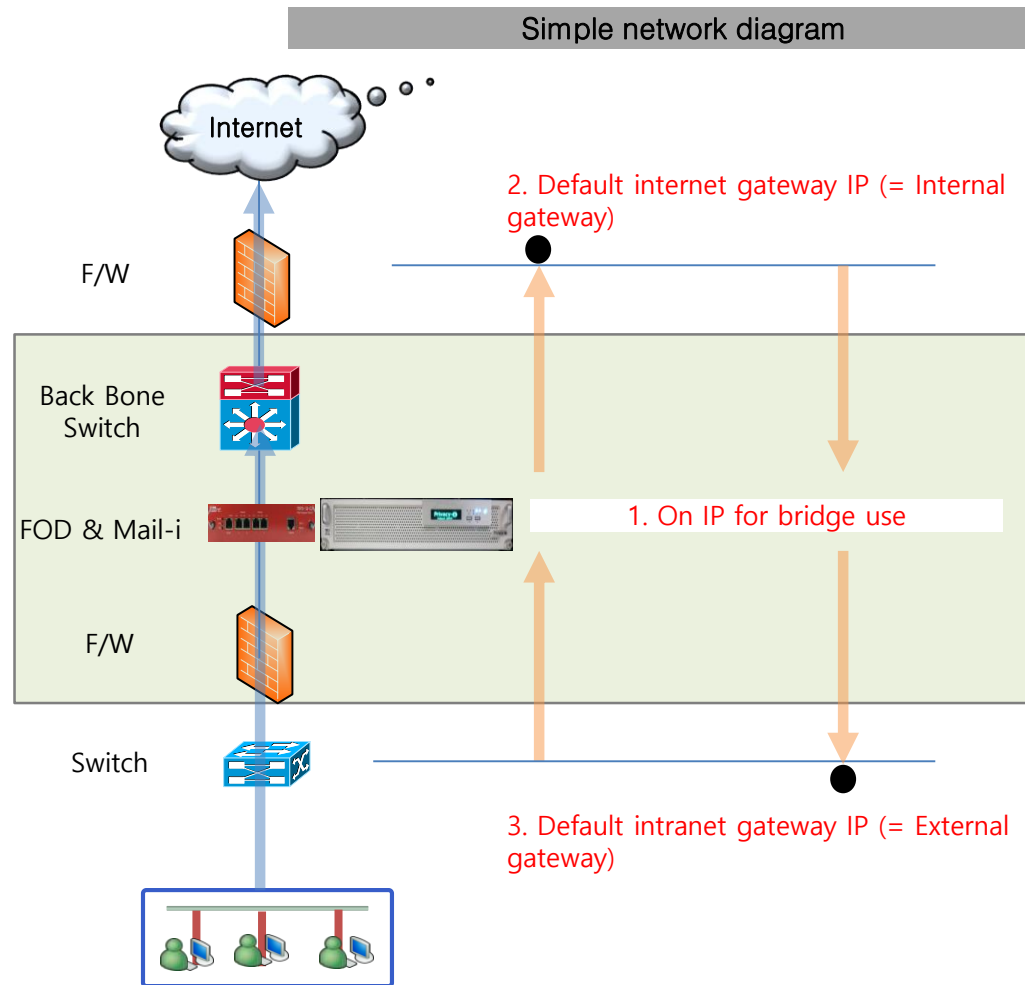


## VIII. Proxy

### 1. Transparent Proxy

- To establish Transparent Proxy, user must provide network information.
- When the type of switches are L2 or L3, the following information is required.
- If the type of switch is L4, Contact us with a detailed network diagram.

1. **One IP (include subnetmask) for bridge use.** Must exist between S/W, IPS or F/W
2. **Default internet gateway IP and subnetmask from S/W to F/W (= Internal gateway)**
3. **Default intranet gateway IP and subnetmask from F/W to S/W. (= External gateway)** When the type of switch is L2, maybe not be available. If this is the case, you do not need to enter.



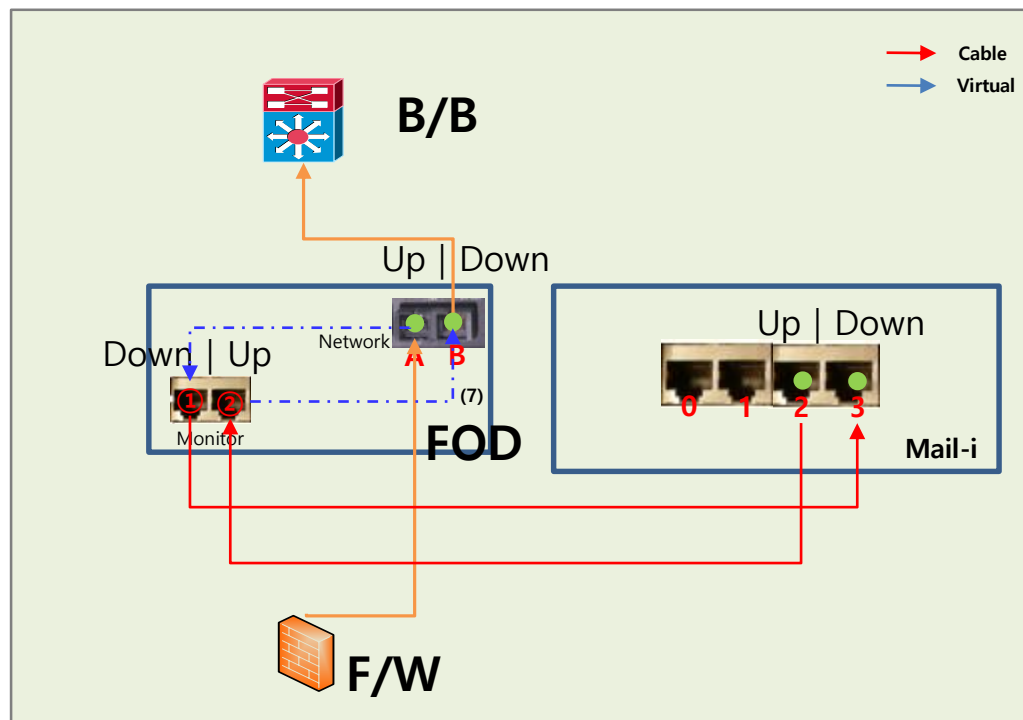


## VIII. Proxy

Detail Line

### 1. Transparent Proxy

- 1) Select **T-Proxy > Networks Settings**
- 2) Click **New**
- 3) Enter NetworkName
- 4) Enter 1.One IP (include subnetmask) for bridge use
- 5) Select Network Type **Bridge** (Reflector for L4)
- 6) Enter 2.Internal gateway
- 7) Enter 3.External gateway
- 8) Select Interface (If configured as shown in the picture, set as eth2 check Internet , eth3 check Intranet )
- 9) Enter Subnet settings(Network , Internal gateway, Extenal gateway)
- 10) Click **Save**





## VIII. Proxy

### 1. Transparent Proxy

- 1) Select **T-Proxy > Networks Settings**
- 2) Click **New**
- 3) Enter NetworkName
- 4) Enter 1.One IP (include subnetmask) for bridge use
- 5) Select Network Type **Bridge** (Reflector for L4)
- 6) Enter 2.Internal gateway
- 7) Enter 3.External gateway
- 8) Select Interface (If configured as shown in the picture, set as eth2 check Internet , eth3 check Intranet )
- 9) Enter Subnet settings(Network , Internal gateway, External gateway)
- 10) Click **Save**

**T-Proxy NetworkAgent**

Policies Settings Networks Settings

#### Network Information

Network Type	Name	IP	Intranet Gateway	Internet Gateway	Block access to internal network	Use internal gateway	Internal NIC	External NIC
Bridge	somansa	192.168.1.155/24	192.168.1.1	192.168.1.254	Not Block	Use	eth3	eth2

First Previous 1 Next Last

#### Network Settings

Network Name: somansa

IP: 192.168.1.155/24

Network Type:  Bridge  Reflector

Internal gateway:  192.168.1.1

External gateway: 192.168.1.254

The Blocking of Access to the Internal Network:  Block  Not Block

#### Interface settings

Device	Status	Intranet	Internet	Reflector
eth0	Available for use	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eth1	Available for use	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eth2	somansa Use	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
eth3	somansa Use	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Subnet settings

Network	Intranet Gateway	Internet Gateway	Use internal gateway
192.168.1.0/24	192.168.1.1	192.168.1.254	Use

First Previous 1 Next Last

Network: 192.168.1.0/24

Internal gateway:  192.168.1.1

External gateway: 192.168.1.254

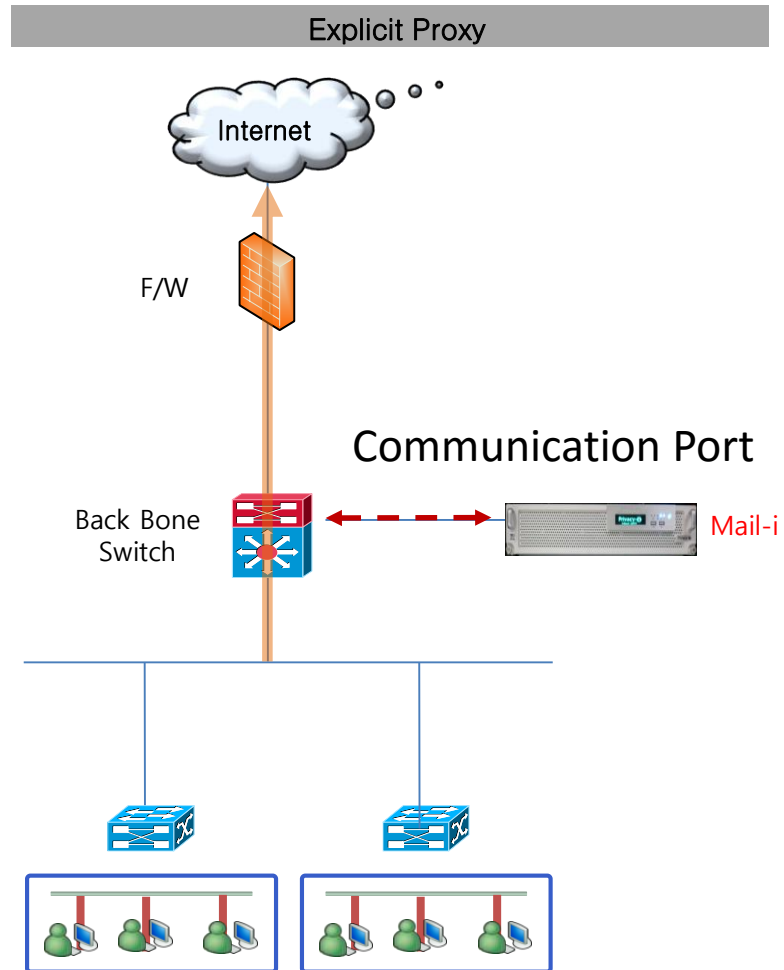
New Save Delete



## VIII. Proxy

### 2. Explicit Proxy

- Explicit Proxy doesn't have another setting. Management IP must be connected to the internet.







## VIII. Proxy

### 3. Access policy

- Mail-i support reject & bypass is based on IP & Port

- 1) Select **T-Proxy > Policies Settings**
- 2) Click **Access Policy Settings > New**
- 3) Enter Client & Server IP and select Action
- 4) Click Save
- 5) Click Apply Policy

### 4. TLS policy

- Mail-i support reject & bypass is based on CN(Common Name in packet)

- 1) Select **T-Proxy > Policies Settings**
- 2) Click **TLS Policy Settings > New**
- 3) Enter Client & Server IP and select Action
- 4) Click Save
- 5) Click Apply Policy

**T-Proxy NetworkAgent**

Policies Settings    Networks Settings

**Access policy**

Priority	Client	Server	Access Action	SSL2 Action	Description
0 1	-	192.168.1.114-443/24	BYPASS	-	-
0 2	-	210.103.240.0/24	BYPASS	-	Kakao Talk(1)
0 3	-	110.76.140.0/22	BYPASS	-	Kakao Talk(2)
0 4	-	103.246.57.52/24	BYPASS	-	Daum Kakao(Kakao Talk)
0 5	-	139.150.1.74/32	BYPASS	-	Knix Kakao talk PDF Download
0 6	-	1.201.0.62/24	BYPASS	-	Kakao Talk File Server
0 7	-	31.216.147.0/24	ANALYZE	-	Mega Async(Windows Program)
0 8	-	110.76.141.23	BYPASS	-	Kakao Talk(Open Chatting)

**Access Policy Settings**

Client: IP  Port  Prefix

Server: IP  Port  Prefix

Action:

Description:

**TLS policy**

Priority	Client	Server	CN	TLS Action	Certificate	Self-signed Authentication Action	Description
0 1	-	-	- CN > *.update.microsoft.com	bypass	-	RAW	Windows Update Server
0 2	-	-	- CN > *.itunes.apple.com	bypass	-	RAW	-
0 3	-	-	- CN > *.sls.microsoft.com	RAW	-	RAW	Windows Store
0 4	-	-	- CN > *.kakao.com	bypass	-	RAW	Kakao Talk Login
0 5	-	-	- CN > *.talk.kakao.com	bypass	-	RAW	Kakao Talk
0 6	-	-	- CN > *.googleusercontent.com	bypass	-	RAW	Google Play Store

**TLS Policy Settings**

Client: IP  Port  Prefix

Server: IP  Port  Prefix

Type:   (Category Database Update date : 2017-07-21)

CN:

TLS Action:

Self-signed Certificate Operation:

Description:



## IX. Common

### 1. Search Service Control

- 1) Select **Common > Search Service Control**
- 2) Click **Start** or **Stop** to control Service

### 2. Search Service Back-up/Restore

- 1) Select **Common > Search Service > Search Service Back-up/Restore**
- 2) To schedule back-up, select Storage Schedule Settings
- 3) Click the **Save**

- To back-up and restore immediately,

- 1) Select **Common > Search Service Back-up/Restore**
- 2) Check Box you want to back-up or restore index
- 3) Click the **Backup** or **Restore**
- 4) Click the **OK**

**Common Search Service**

Search Service Control | Search Service Back-Up/Restore | Content Analyzer Settings

**Search Server Control**

Search Sever	Status	Refresh	Start	Stop	Event Log
	■ ■ ■ ■ ■				
Indexing Server	■ ■ ■ ■ ■				
Search Engine	■ ■ ■ ■ ■				

**Common Search Service**

Search Service Control | Search Service Back-Up/Restore | Content Analyzer Settings

**Storage List**

Storage Name	Storage Path	Registration Schedule	Original File Delete
mi_repository	/somanza/backup/maili	No	-

**Storage Schedule Settings**

Storage Name: mi\_repository  
Storage Path: /somanza/backup/maili

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

**Save**

**Index/Backup List**

Original File:  Don't Delete  Delete

Index List			mi_repository Backup List	
Index Name	Back-up	Backup Name	Backup Name	
mi_201706_4	Backed up	mi_201706_1	mi_201706_1	
mi_201707_3	Backed up	mi_201706_4	mi_201706_4	
mi_201707_4	Not Backed up	mi_201707_3	mi_201707_3	



## IX. Common

### 3. MQTT advanced option

※ This is an advanced option for using Response Message function of DLP + Center.

The screenshot displays the Configuration Manager web interface. The top navigation bar includes 'Configuration Manager' and tabs for 'Common', 'DLP+ Center', 'Mail-i', and 'T-Proxy'. The 'Common' tab is active, showing 'Common General Settings'. Underneath, there are two sub-tabs: 'Database' and 'MQTT Settings', with 'MQTT Settings' selected. The 'MQTT Settings' section contains a 'Server Information' label and two input fields: the first contains '192.168.1.1' and the second contains '1883'. A blue 'OK' button is positioned below the input fields. On the left side of the interface, there is a sidebar menu with sections: 'General Settings' (Database, MQTT Settings), 'Search Service' (Search Service Control, Search Service Back-Up/Restore, Content Analyzer Settings), and 'HR Information Sync' (Database Registration, Sync Information Settings).



## IX. Common

### 4. HR Information Sync

- Import customer HR (human resource) Information. The target is DB (database) and AD (Active Directory).

※ The type of data must be organized in a tree. If not, you need to edit it in tree form via 'Editing Script'.

- 1) Select **Common > HR Information Sync > Database Registration**.
- 2) Enter information about the server where the customer information is located and click **Save**
- 3) Select **Sync Information Settings**
- 4) Enter information about **Top Dept Code** and click **Save**

※ The Top Dept Code must be unique.

- 5) Select **Column Mapping**
- 6) Select Temp Table, Sync Database Name and Default Table and click **Save**
- 7) Click **OK**

The screenshot shows the 'Common HR Information Sync' interface with the 'Database Registration' tab selected. The interface includes a navigation bar with tabs: Database Registration, Sync Information Settings, Column Mapping, Editing Script, Scheduling, and Sync Simulation. Below the navigation bar is a table with the following data:

Alias	Type	IP	Database Name
test_somansa	POSTGRESQL	192.168.1.113	somansa

Below the table are input fields for Database Type (Postgresql), Database IP / Port (192.168.1.113), Login (postgres), Password, and Database Name (somansa). There are 'New', 'Save', and 'Delete' buttons at the bottom.

The screenshot shows the 'Common HR Information Sync' interface with the 'Dept Information Settings' tab selected. The interface includes a navigation bar with tabs: Database Registration, Sync Information Settings, Column Mapping, Editing Script, Scheduling, and Sync Simulation. Below the navigation bar is a form with the following fields and options:

Top Dept Code: [Input field]

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.

There is a 'Save' button at the bottom.



## IX. Common

- 8) Select Editing Script and click **Save**. Editing Script can be used to modify additional or insufficient information
- 9) Select **Scheduling**
- 10) Click **New**
- 11) Enter Schedule Name and select Task Cycle you want to time
- 12) Set the Script order and click **Save**
- 13) Select **Sync Simulation**
- 14) Select Schedule Selection and click **Perform Sync Simulation**
- 15) Select Mapping Table and click **Search Data**
- 16) Select **Sync Results**. You can check logs for Sync results

Common HR Information Sync

[Database Registration](#)
[Sync Information Settings](#)
[Column Mapping](#)
[Editing Script](#)
[Scheduling](#)
[Sync Simulation](#)

Sync Results

### Editing Script

Script  HR Information Extraction Script  Temp Table Refine Script  Post-Processing Script

Mapping Name User Information\_test\_somansa Search Script

---

**SELECT**

```
SELECT "tb_mempdata"."userid", "tb_mempdata"."empname" FROM
ta_db."tb_mempdata"
```

**INSERT(UPDATE)**

```
INSERT INTO TA_DB.SCMIM_TEMPUSER ( USERID, EMPNAME) values ( ?, ? )
```

Save

Run

### Script Performance Test

IP Type	Approval Status	User ID	User Name	Dept Code	Employee Resignation	Company	E-Mail	Phone Number	Dept Name	User Password	User ID	Employee Code
		Unregistered IP	Unregistered IP									
		dobbie	dobbie									
		grant	grant									



## X. SYSTEM

- System default setting possible



### 1. Check UID

- UID is used as a unique key in the system and required for license renewal requests.

1) Select **SYSTEM > Settings**. You can check

The screenshot shows the 'SYSTEM' settings page with tabs for 'Settings', 'Audit Log', and 'Event Log'. The 'UID' field is highlighted, showing the value 'wy6vza0'.

### 2. SMTP Settings

- The SMTP Settings is required before using mail related functions in DLP+Center.

1) Select **SYSTEM > Settings**

2) Insert SMTP Host / Port and Sender and select SMTP Authentication, Encoding and SMTP ID / Password

3) Click **OK**

The screenshot shows the 'SMTP Settings' page with the following fields and options:

SMTP Host / Port	mail.somansa.com	25
SMTP Authentication	<input type="radio"/> Use <input checked="" type="radio"/> Don't Use	
SMTP ID / Password	SMTP ID	SMTP Password
Sender	chohm@somansa.com	
Encoding	<input type="radio"/> EUC-KR <input checked="" type="radio"/> UTF-8	

Buttons: **OK**, **Initialize**

### 3. Session Time

- You can change Session Time for CM.

1) Select **SYSTEM > Settings**

2) Insert Session Duration Time you want

3) Click **OK**

The screenshot shows the 'Session Time' page with the following field:

Session Duration Time	10	Minute	<b>OK</b>
-----------------------	----	--------	-----------



## X. SYSTEM

### 4. Server IP Settings

- Server IP is automatically set.

1) Select **SYSTEM > Settings**. You can check Server IP.

- If the IP is different from the actual IP, change the information below.

1) Connect SSH  
2) Edit for vi editor : vi  
/somansa/common/conf/common.properties  
3) Change the UseIP

### 5. Configuration Manager Administrator Information

- Set administrator password change.

1) Select **SYSTEM > Settings**  
2) Insert current Password and New Password  
3) Click **OK**

- Set administrator password policy.

1) Select **SYSTEM > Settings**  
2) Select Password Expiry Policy  
3) Click **OK**

#### 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

---

#### Configuration Manager Administrator Account Information

Password

New Password

Re-enter Password

---

Password Expiry Policy  Use  Don't Use



## X. SYSTEM

### 6. Time Synchronization

- Synchronize system time.

- 1) Select **SYSTEM > Settings**
- 2) Check Sync time cycle you want
- 3) Click **Apply**
- 4) Insert **Time Server**
- 5) Click **OK**

### 7. Integrity Check

- Set the system Integrity check.

- 1) Select **SYSTEM > Settings**
- 2) Check Integrity time cycle you want
- 3) Click **Apply**

※ Configuration Manager Initialization is advanced option.

#### Time Synchronization

Current Server Time : 2017-07-22 04:27:19 Run

Synchronize your server clock with your local standard time now.

Sync every  hours Apply

---

Your server clock will be synchronized with Time Server.

Time Server  OK

#### Integrity Check

Check now Run

Check every  minutes Apply

#### Configuration Manager Initialization

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





## X. SYSTEM

### 8. Audit Log

- Search audit log

- 1) Select **SYSTEM > Audit Log**
- 2) Select Date
- 3) Click **Search**

### 9. Event Log

- Retrieve event log

- 1) Select **SYSTEM > Event Log**
- 2) Select Module
- 3) Select Log file
- 4) Click **Search** or **Download**

The screenshot shows the 'SYSTEM' interface with the 'Audit Log' tab selected. It features a search area with fields for 'Date' (2017-08-01 to 2017-08-31), 'IP', 'Log Type' (set to '-- ALL --'), and 'Log Contents'. Below the search area is a table with the following data:

Time	Type	IP	Contents	Description
2017-08-30 05:18:47	Access	96.64.237.21	System > Settings was accessed.	[URL] :/cm/evnrioment.lnit.json [detail] : SYSTEM ACCESS LOG
2017-08-30 05:18:45	Access	96.64.237.21	COMMON > General Settings was accessed.	[URL] :/cm/common.mng.init.json [detail] : SYSTEM ACCESS LOG
2017-08-30 05:18:44	Login	96.64.237.21	Logged in to Configuration Manager	[detail] Logged in to Configuration Manager
2017-08-30 04:19:09	Logout	35.167.83.225	Logged off from Configuration Manager	[detail] Logged off from Configuration Manager
2017-08-30 04:18:37	Access	35.167.83.225	COMMON > HR Information Sync was accessed.	[URL] :/cm/m.mng.init.json [detail] : SYSTEM ACCESS LOG
2017-08-30 04:18:20	Access	35.167.83.225	COMMON > General Settings was accessed.	[URL] :/cm/common.mng.init.json [detail] : SYSTEM ACCESS LOG

The screenshot shows the 'SYSTEM' interface with the 'Event Log' tab selected. It features an 'Event Log Retrieval' section with a 'Module' dropdown (DLP+ Center), a 'Log file' dropdown (catalina.out), and buttons for 'Search', 'Stop', 'Download', and 'Initialize event log'. Below the search area, a message states 'The event log is being retrieved.' followed by a log snippet:

```
[2017-09-06 06:21:05] DEBUG [java.sql.ResultSet:27] - {reset-531284} Result: [93]
[2017-09-06 06:21:05] DEBUG [com.ibatis.common.jdbc.SimpleDataSource:27] - Closed connection 1894701205.
[2017-09-06 06:21:10] DEBUG [dlpcenter.common.interceptor.AuthInterceptor:125] -
=====AuthInterceptor=====
```



**SOMANSA**

[www.somansatech.com](http://www.somansatech.com)