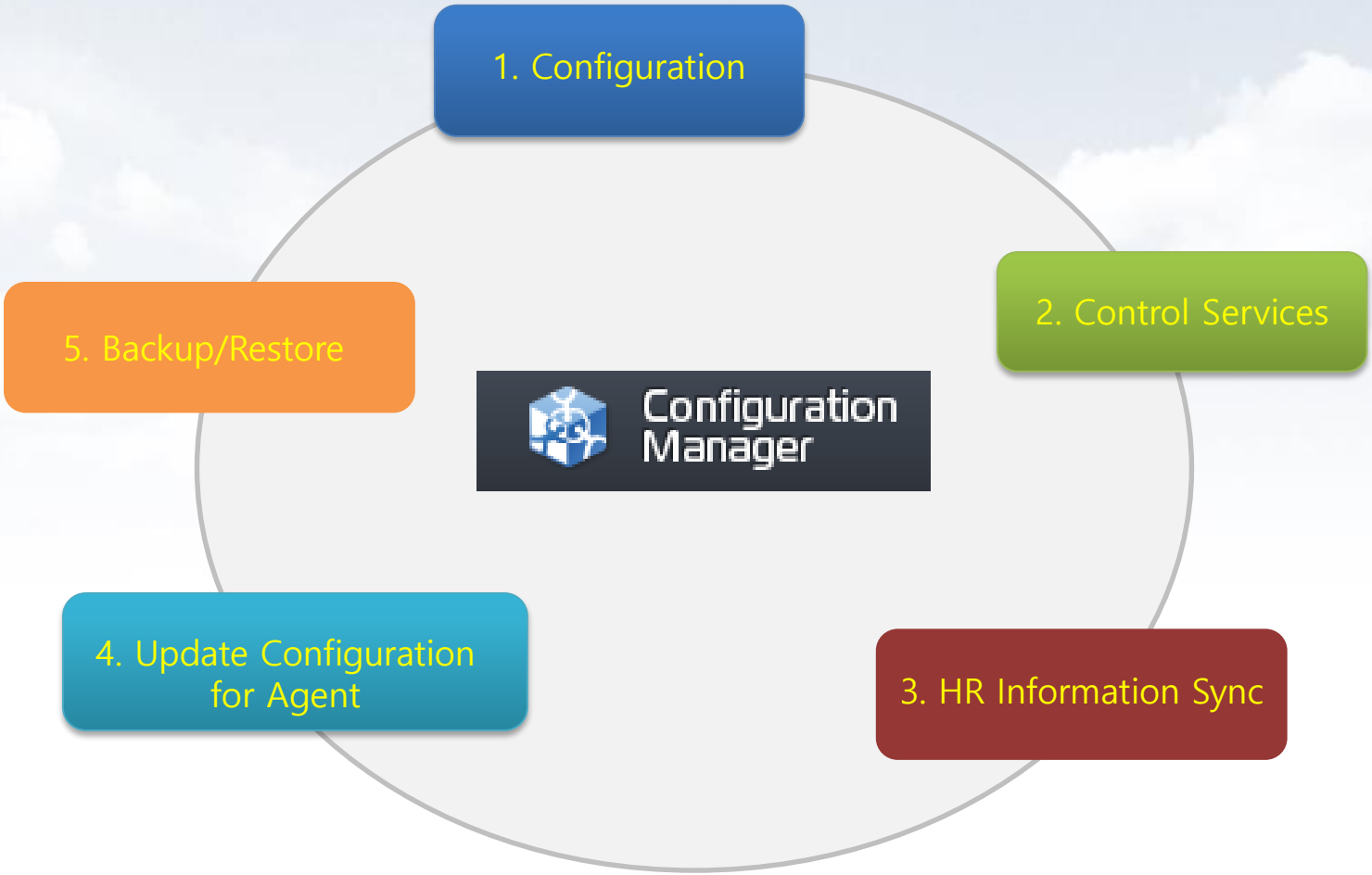
SOMANSA

Data Loss Prevention


1. Configuration
2. Control Services
3. HR Information Sync
4. Update Configuration for Agent
5. Backup/Restore
Configuration Manager

CONTENTS

I. Structure

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

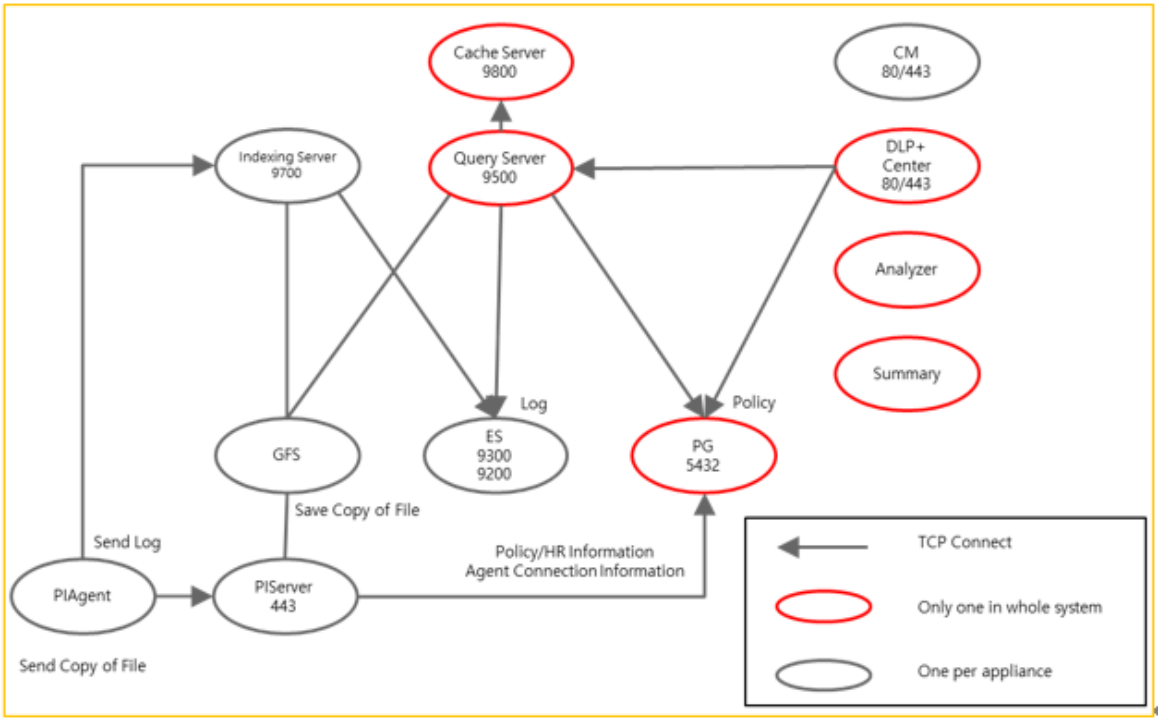
• **PIServer (Privacy-i Server)** : Existing fuctions of version 5.0 except incident log process, such as login / policy / HR(Human Reasource) information / decide information / remote command, etc. , are provide to PIServer

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

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



I. Structure

- **Cache Server (Redis)** : works as a temporary storage for viewed incidents.

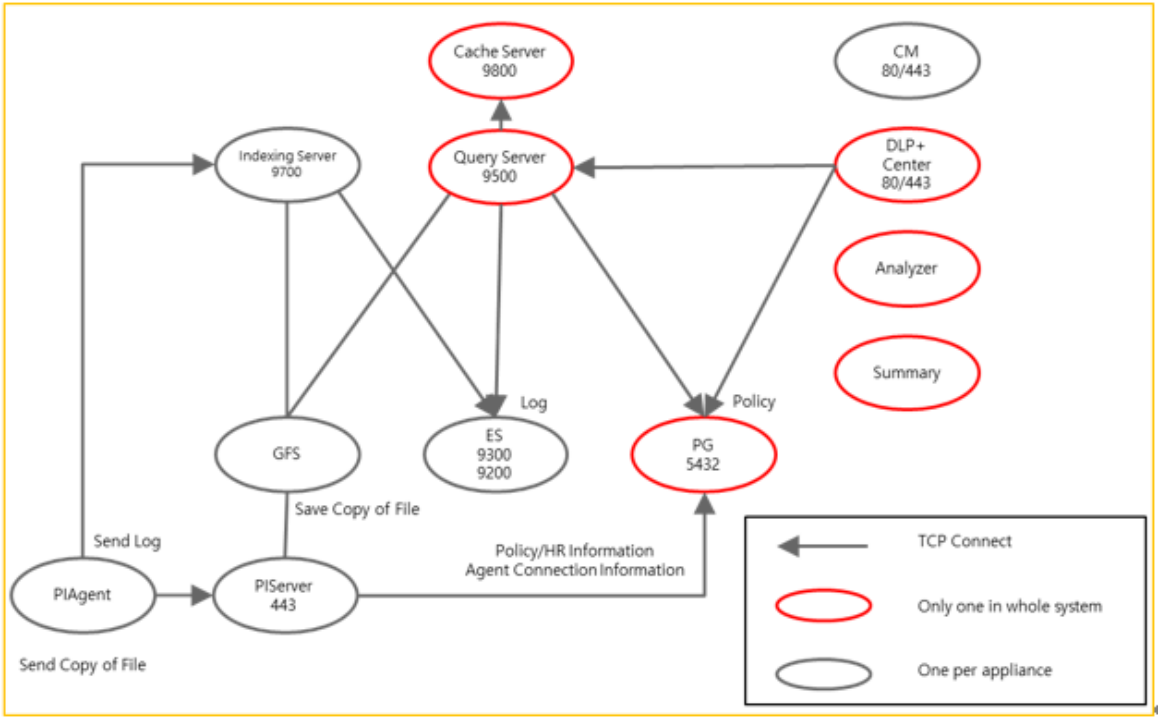
- **SMSAnalyzer :** detects data patterns such as resident registration numbers from the saved incidents (Content/Attachment files).

- **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)
PIServer
Elasticsearch
GlusterFS
Queryserver (Tomcat_queryserver)
DLP+Center
Redis
Postgresql
SMSAnalyzer
SMSSummary

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

PIServer
CM (Configuration Manager)
Indexer (Tomcat_indexer)
PIServer
Elasticsearch
GlusterFS
Main Storage
CM (Configuration Manager)
Queryserver (Tomcat_queryserver)
Elasitcsearch
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

```
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
```

2. Change Server Local Time

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

```
[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]#
```

3. Change Hostname

- hostname must be unique

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

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 responsiblity for chaning 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 seperated,
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. PIServer 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)

```
127.0.0.1   localhost localhost.localdomain
192.168.1.112   PIServer
192.168.1.113   storageserver
```

2.2 ES of PIServer

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:['*PIServerhost:9300*','*storagehost:9300*'])

```
node.name: 'PIServer'
discovery.zen.ping.unicast.hosts: ['PIServer:9300','storageserver:9300']
network.host: ['PIServer','localhost']
path.repo: ['/somansa/backup/maili','/somansa/backup/wk','/somansa/backup
index.max_result_window: 2147483647
index.query.bool.max_clause_count: 4096
node.master: true
node.data: false
```

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:['*PIServerhost:9300*','*storagehost:9300*'])
4) ES service of PIServer and Storage Server restart

```
node.name: 'storageserver'
discovery.zen.ping.unicast.hosts: ['PIServer:9300','storageserver:9300']
network.host: ['storageserver','localhost']
path.repo: ['/somansa/backup/maili','/somansa/backup/wk','/somansa/backup
index.max_result_window: 2147483647
index.query.bool.max_clause_count: 4096
node.master: true
node.data: true
```

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**

```
===== 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
```

2.5 GFS of Agent Server

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

```
===== 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.
192.168.1.8 Mainstorage
192.168.1.9 Substorage
192.168.1.10 PIServer1
192.168.1.11 PIServer2
```

3.2 ES of PIServers

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:[‘*PIServerhost1:9300*’, ‘*PIServerhost2:9300*’,’*storagehost1:9300*’, ’*storagehost2:9300*’])

```
node.name: 'PIServer1'
discovery.zen.ping.unicast.hosts: ['PIServer1:9300','PIServer2:9300,','Mainstorage:9300','Substorage:9300']
network.host: ['PIServer1','localhost']
path.repo: ['/somansa/backup/maili','/somansa/backup/wk','/somansa/backup/pvi']
index.max_result_window: 2147483647
index.query.bool.max_clause_count: 4096
node.master: true
node.data: false
```

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:['*PIServerhost1:9300*', '*PIServerhost2:9300*','*storagehost1:9300*', '*storagehost2:9300*','localhost'])
4) ES service of PIServer and Storage Server restart

```
node.name: 'Mainstorage'
discovery.zen.ping.unicast.hosts: ['PIServer1:9300','PIServer2:9300,','Mainstorage:9300','Substorage:9300']
network.host: ['Mainstorage','localhost']
path.repo: ['/somansa/backup/maili','/somansa/backup/wk','/somansa/backup/pvi']
index.max_result_window: 2147483647
index.query.bool.max_clause_count: 4096
node.master: true
node.data: true
```

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  ]
```

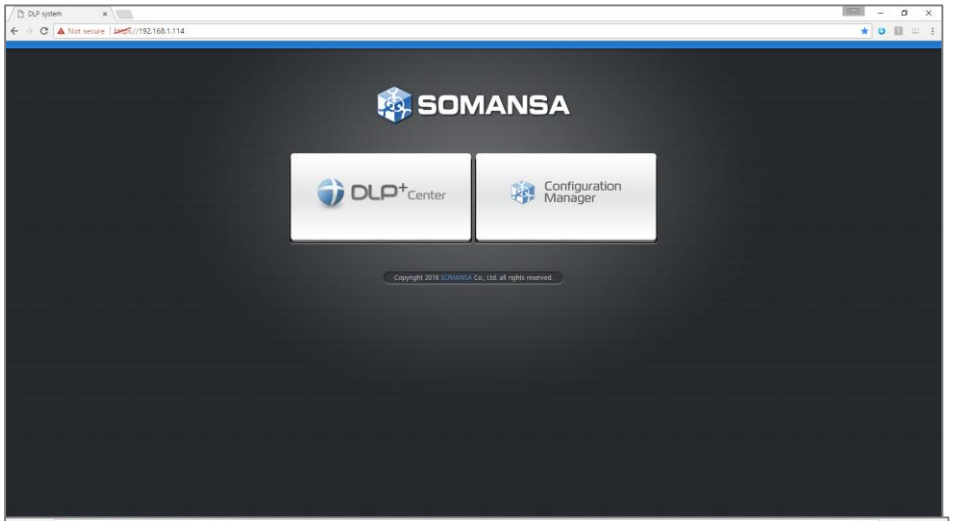
3.6 GFS of PIServers

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

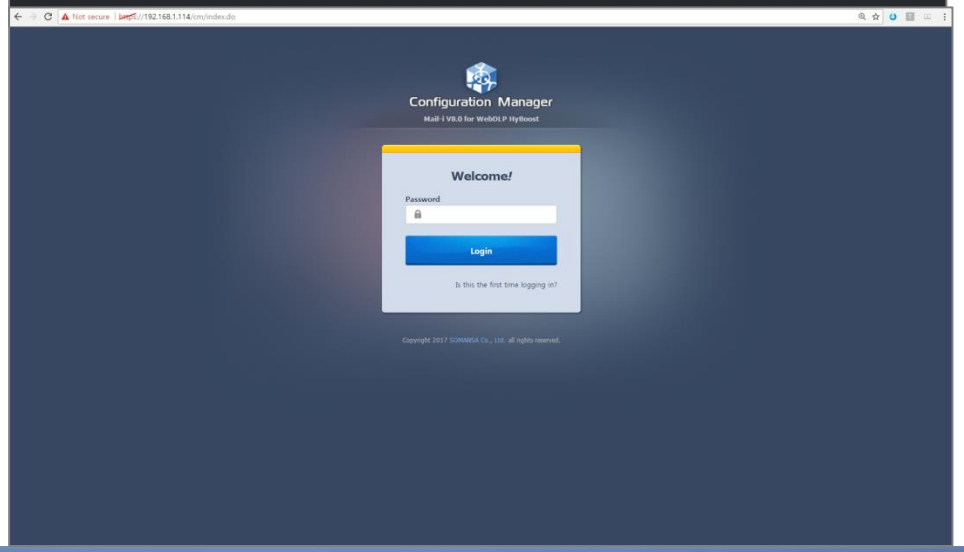
```
===== GFS linked Storage Server ====
Please enter Hostname for Storage Server
hostname: Mainstorage
Storage Hostname is [  Mainstorage ]
Do you want to continue?
y.Yes
n.No
>>y
```

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

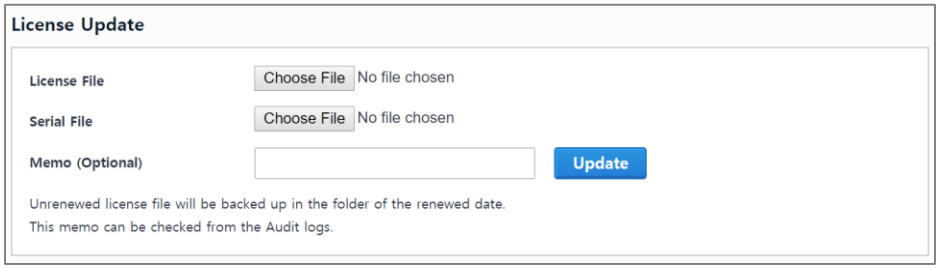


V. License

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

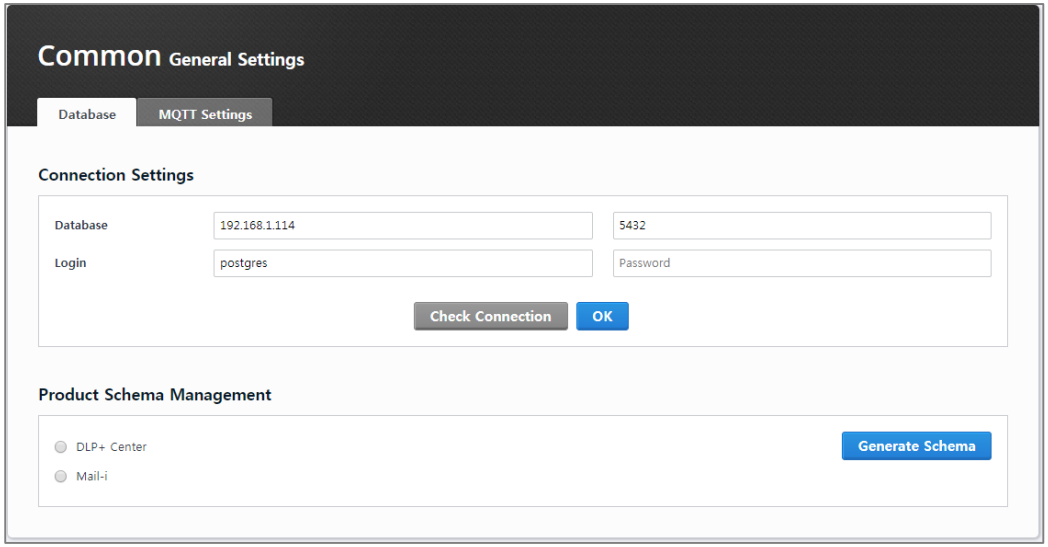


VI. Common

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**



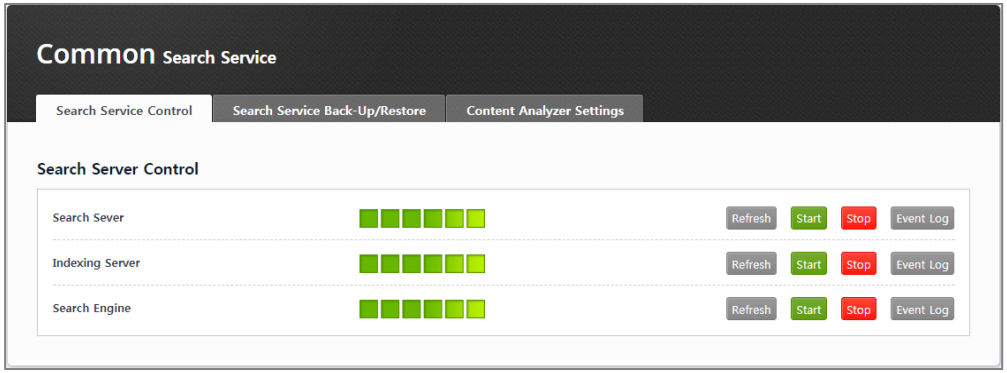
2. Generate Schema

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

IX. Common

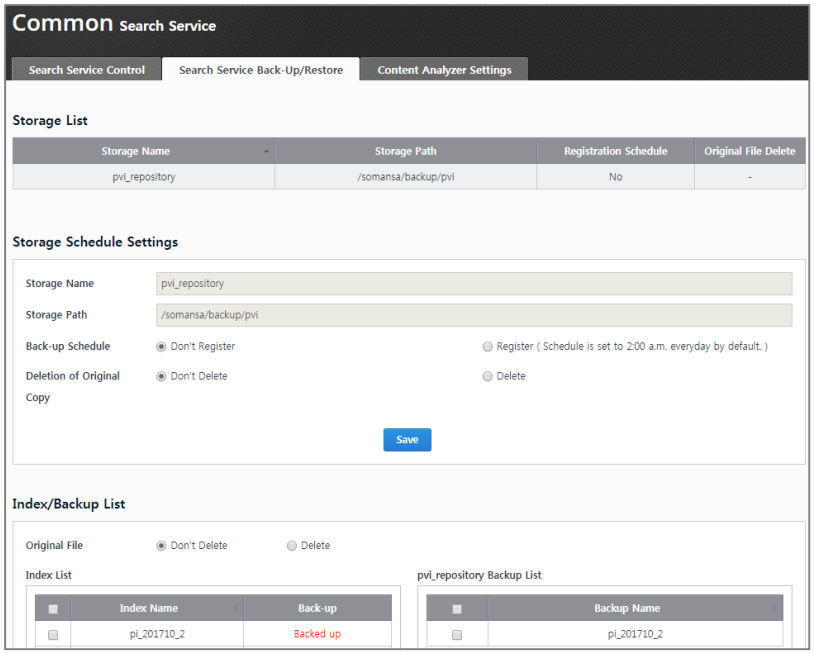
1. Search Service Control

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**



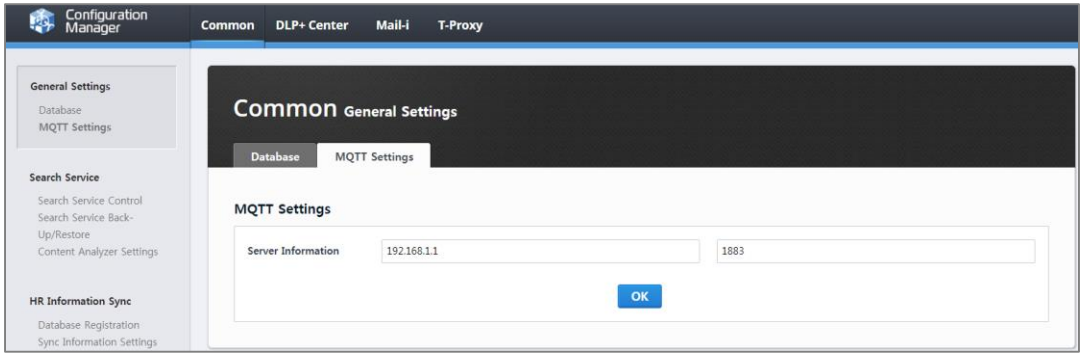
• To back-up and restore immediately,

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**

IX. Common

3. MQTT advanced option

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



IX. Common

4. HR Information Sync

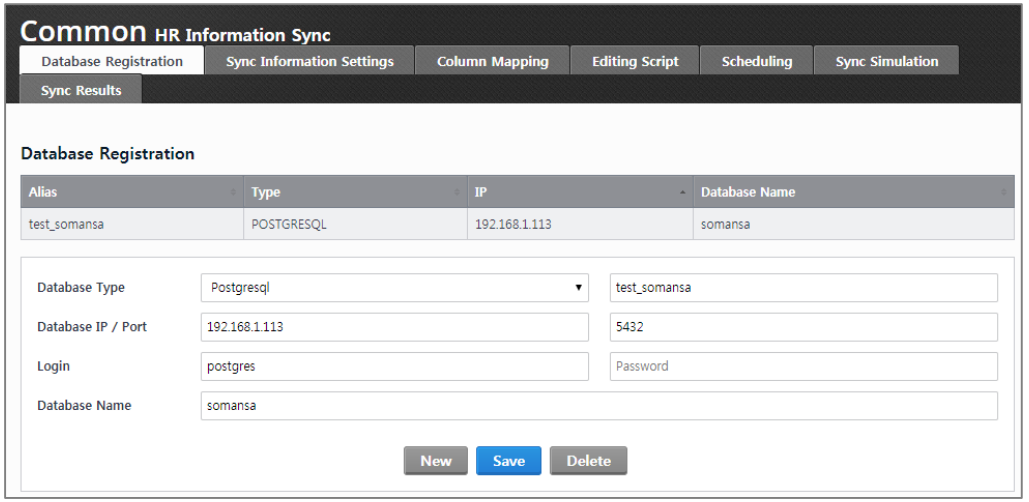
- Import customer HR (human resource) Information. The target is DB (database) and AD (Active Directory).

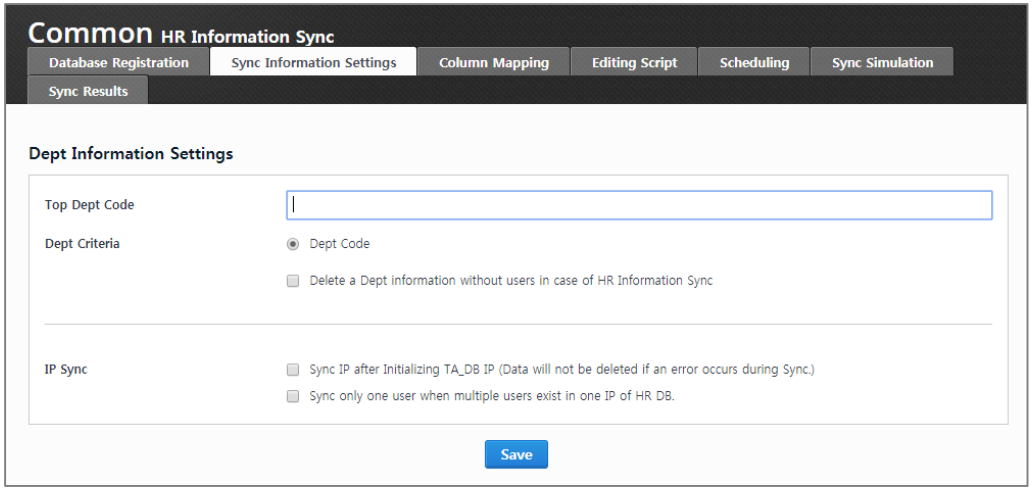
※ The type of data must be organized in a tree. If not, you need to edit it in tree form via 'Editing Script'.

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.

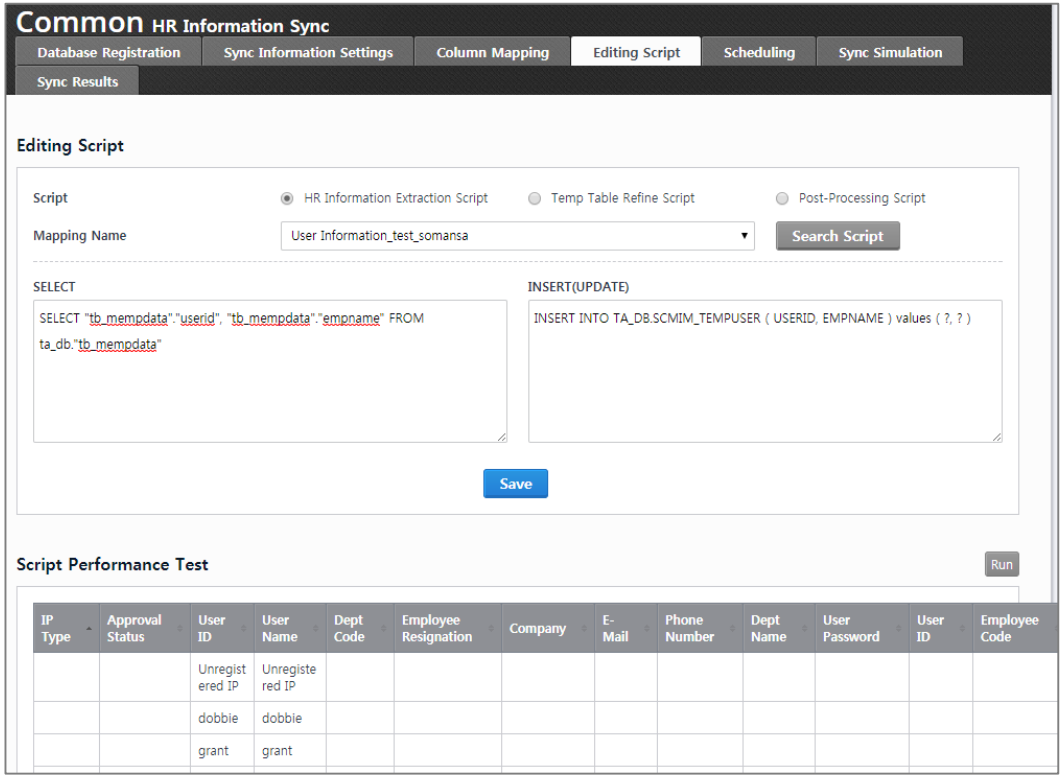
5) Select **Column Mapping**
6) Select Temp Table, Sync Database Name and Default Table and click **Save**
7) Click **OK**





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



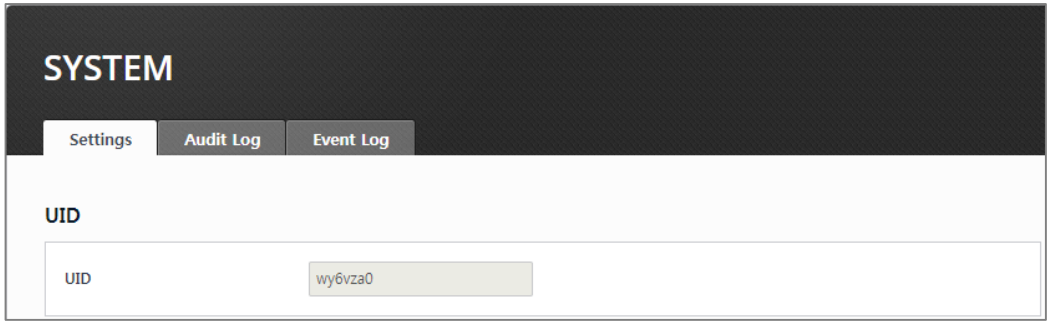
X. SYSTEM

• System default setting possible

1. Check UID

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

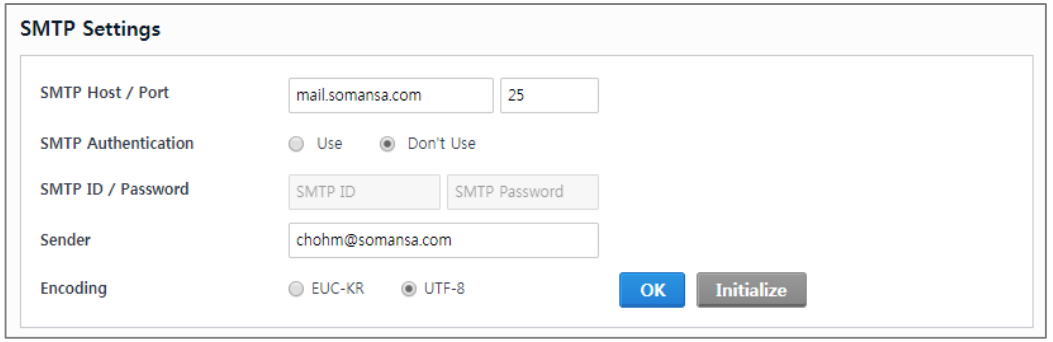
1) Select **SYSTEM > Settings.** You can check



2. SMTP Settings

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

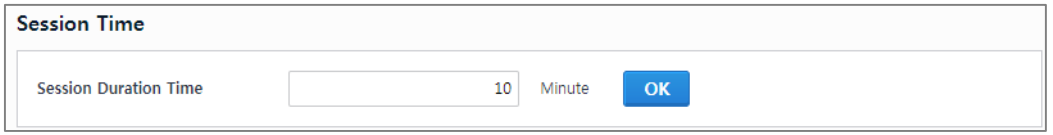
1) Select **SYSTEM > Settings**
2) Insert SMTP Host / Port and Sender and select SMTP Authentication, Encoding and SMTP ID / Password
3) Click **OK**



3. Session Time

• You can change Session Time for CM.

1) Select **SYSTEM > Settings**
2) Insert Session Duration Time you want
3) Click **OK**



X. SYSTEM

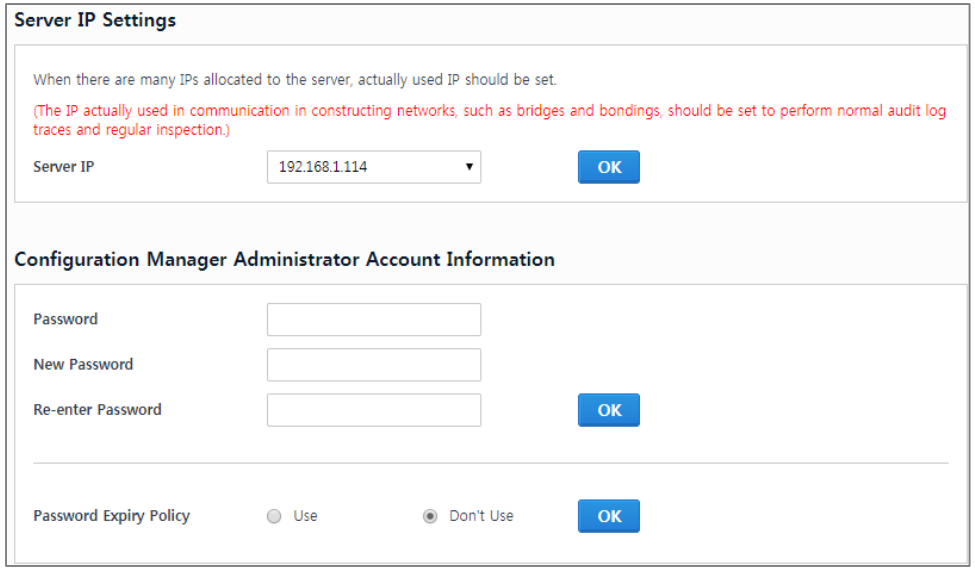
4. Server IP Settings

• 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**

X. SYSTEM

6. Time Synchronization

- Synchronize system time.

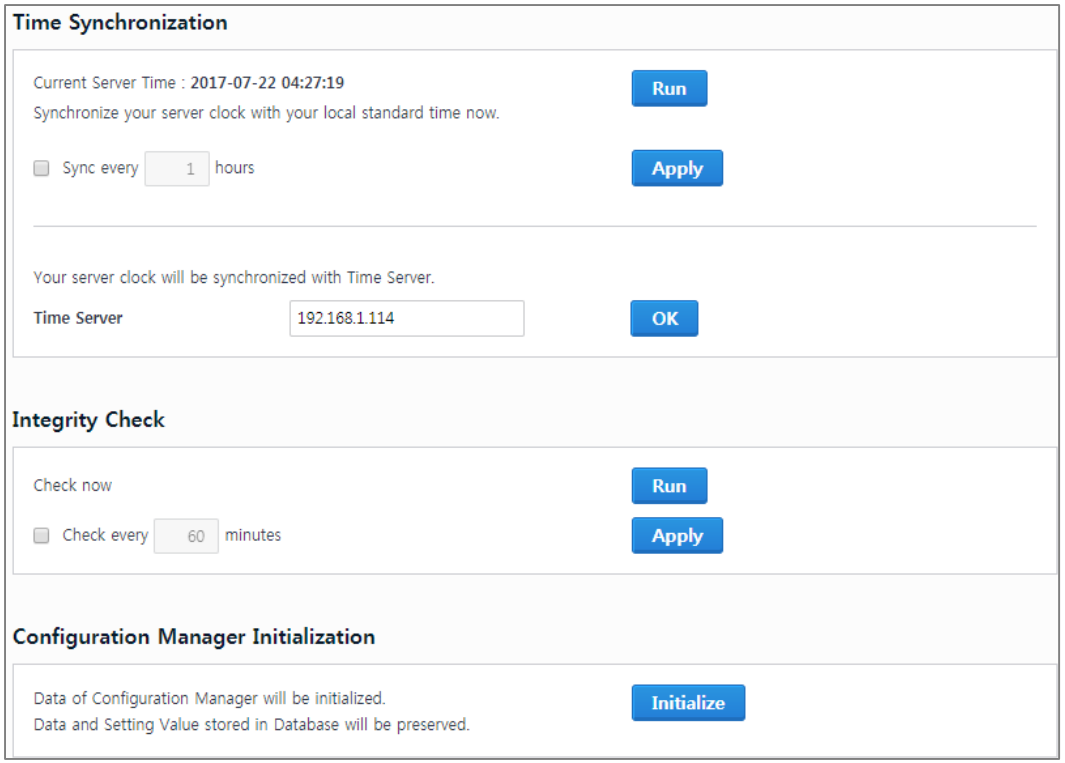
1) Select **SYSTEM > Settings**
2) Check Sync time cycle you want
3) Click **Apply**
4) Insert **Time Server**
5) Click **OK**

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.



X. SYSTEM

8. Audit Log

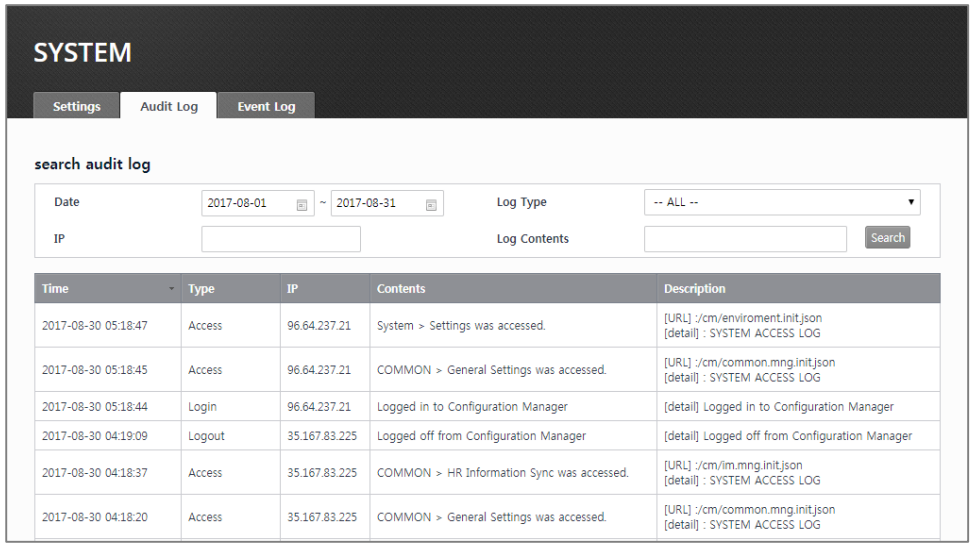
- Search audit log

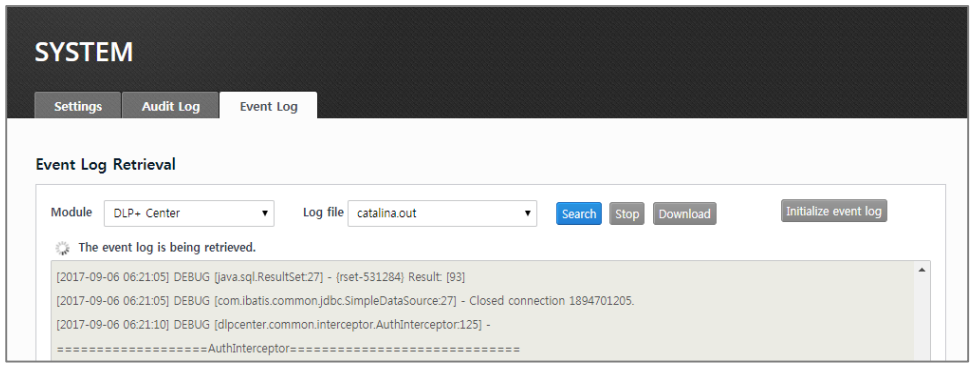
1) Select **SYSTEM > Audit Log**
2) Select Date
3) Click **Search**

9. Event Log

- Retrieve event log

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





SOMANSA

www.somansatech.com