



Samsung LYNK Server Installation Guide

for Hotel TV

Samsung SDS Co., Ltd.

Revision History			
Document Name		Samsung LYNK Server Installation Guide for Hotel TV	
Version	Date	Comment	Writer
0.1	2013-06-27	Initial Version	Kihyang Kim
0.2	2013-08-09	Updated for all	Kihyang Kim
0.3	2013-11-13	Updated for all	Kihyang Kim
0.4	2014-07-30	Updated for all	Kihyang Kim
0.5	2015-03-30	Updated for all	Kihyang Kim
0.6	2015-11-03	Updated for chapter 4	Kihyang Kim
0.7	2016-05-18	Updated for chapter 2.2 and 2.3	Kihyang Kim
0.8	2016-08-17	Updated for all	Kihyang Kim
0.9	2016-09-23	Updated for chapter 2	Kihyang Kim

Table of Contents

1. Environment Setup	2
1.1. Installing JRE (Java Runtime Environment)	2
1.2. Installing Tomcat.....	2
2. LYNK Setup	3
2.1. Configuring Tomcat.....	3
2.2. Installing LYNK.....	4
2.3. Configuring LYNK - Server Configuration	5
2.4. Configuring LYNK – ECMG Configuration(For Live Service).....	7
2.5. Configuring LYNK – EMMG Configuration(For Live Service)	9
2.6. Changing logging level of LYNK.....	10
3. Scrambler Setup(For Live Service)	11
3.1. Configuring scrambler in regard to LYNK	11
4. Check your system that LYNK server is installed	11

1. Environment Setup

1.1. Installing JRE (Java Runtime Environment)

See below reference link.

<http://java.sun.com/javase/6/webnotes/install/index.html>

※ JRE version 6.0 or later required.

1.2. Installing Tomcat

See below reference link.

<http://tomcat.apache.org/tomcat-6.0-doc/setup.html>

※ Tomcat version 6.0 or later required.

2. LYNK Setup

2.1. Configuring Tomcat

i. Setting TLS/SSL on server.xml file

"\$TOMCAT_HOME" means the directory of tomcat installed in your system.

Edit "\$TOMCAT_HOME/conf/server.xml" file.

Refer to the below configuration.

If you are using tomcat6, replace the original configuration for Connector port "8443" with below statements.

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    keystoreFile="keystore" keystorePass="changeit"
    keyAlias="tomcat"
    truststoreFile="truststore" truststorePass="changeit"
    clientAuth="true" sslProtocol="TLS"/>
```

If you are using tomcat7 or tomcat8, replace the original configuration for Connector port "8443" with below statements.

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
    SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    keystoreFile="keystore" keystorePass="changeit"
    keyAlias="tomcat"
    truststoreFile="truststore" truststorePass="changeit"
    clientAuth="true" sslProtocol="TLS"
    ciphers="TLS_RSA_WITH_AES_128_CBC_SHA"/>
```

ii. Remove tomcat native library file

Remove or rename tomcat native library file(tcnative-1.dll) to use https connection if that file exists.

The tcnative-1.dll file exists in "\$TOMCAT_HOME/bin" directory.

2.2. Installing LYNK

i. Installing WAR

1. Copy `CasServer.war` file into directory "`$(TOMCAT_HOME)/webapps/`".
2. Start tomcat service.

("`$(TOMCAT_HOME)`" means the directory of tomcat installed in your system.)

※ *The directory `$(TOMCAT_HOME)/webapps/CasServer` will be shown after the first server starting.*

ii. Reinstalling WAR(on linux systems)

1. Shutdown tomcat.
2. Delete the `/tomcat/webapps/CasServer.war` file
3. Delete the `/tomcat/webapps/CasServer` folder
4. Delete the `/tomcat/work/catalina/localhost` folder. (This directory is Tomcat cache folder.)
5. Sync filesystem. (use `sync` command)
6. Reboot system
7. Start tomcat
8. To make sure CasServer is uninstalled, Open CasServer Web page. It should not be connected.
9. Copy new `CasServer.war` file into `/tomcat/webapps/` directory.
10. Start tomcat

iii. Reinstalling WAR(on windows systems)

1. Shutdown tomcat.
2. Delete the `/tomcat/webapps/CasServer.war` file
3. Delete the `/tomcat/webapps/CasServer` folder
4. Delete the `/tomcat/work/catalina/localhost` folder. (This directory is Tomcat cache folder.)
5. Copy new `CasServer.war` file into `/tomcat/webapps/` directory.
6. Start tomcat

2.3. Configuring LYNK - Server Configuration

i. Server Status

You can check the status of LYNK Server using web UI.

Go to `http://[ip_address]:[port]/CasServer > Login > Configuration > Server'`

※ Use the default account to login. (ID: admin, Password: 12345)

Check below items.

- License Status : Displays type and valid period of LYNK license
- SK Update Period : Displays SK Update period
- M/W Server Connection : Displays status of M/W connection
- Recent Error : Displays recent server errors

Server Status Item	Values	Description
License Status	Ex)Period Limited License (20130418 ~ 20131018)	Period limited license
	Ex)52CFEDD6E9883555AC33D156BDC 57501 (20130101 ~ 20151230)	Formal license
	No License	Has no license
SK Update Period	Ex)24 hour(s)	Format : Number + Unit(minute/hour/day/month)
M/W Server Connection	N/A	Not available This means M/W Server URL is not defined. This is not an error because you don't need to connect M/W Server.
	OK	Has no connection error
	In Error	Has M/W server connection error
Recent Error	MW_SERVER_CONNECTION_ERROR	Has M/W server connection error
	SERVER_LICENSEPATH_INVALID	License Path has invalid directory
	SERVER_PERIODLICENSE_EXPIERD	Period license has expired
	SERVER_TLS_KEYFILE_COPY_FAILED	The keystore and truststore file(key files for TLS/SSL) have not been copied into \$TOMCAT_HOME directory for any reason
	SERVER_WIDGET_FILE_COPY_FAILED	The files for client widget have not been copied into \$TOMCAT_HOME/webapps directory for any reason.

To solve the above server errors written in red, check below items.

- **MW_SERVER_CONNECTION_ERROR**
 - ✓ Check if the connection of M/W Server URL is normal.
 - ✓ If the M/W Server URL is wrong, modify the value refer to following 'Server Configuration'.
- **SERVER_LICENSEPATH_INVALID**
 - ✓ Check if the path exists.
 - ✓ If the path is wrong, modify the value refer to following 'Server Configuration'.
- **SERVER_PERIODLICENSE_EXPIERD**
 - ✓ Check if the path exists.
 - ✓ If the license path is valid, you should request a formal license on the License menu. The License Menu is located in Admin > License. You should request a license and import the license file received from License Manager. Refer to the chapters "3.2.2 Reuest License" and "3.2.3 Import License File" in "Samsung_LYNK_Server_Administrator_Guide.doc"

- **SERVER_TLS_KEYFILE_COPY_FAILED**
 - ✓ Check if \$TOMCAT_HOME directory has the right to write.
 - ✓ If the \$TOMCAT_HOME directory has no right to write, modify the property.
 - ✓ If the right has no problem, copy keystore and truststore file from \$TOMCAT_HOME/webapps/CasServer directory to \$TOMCAT_HOME directory.
- **SERVER_WIDGET_FILE_COPY_FAILED**
 - ✓ Check disk capacity.
- **No License**
 - ✓ Check if the license path is valid.
 - ✓ If the license path is valid, you should request a formal license on the License menu. The License Menu is located in Admin > License. You should request a license and import the license file received from License Manager. Refer to the chapters "3.2.2 Reuest License" and "3.2.3 Import License File" in "Samsung_LYNK_Server_Administrator_Guide.doc"

ii. Server Configuration

Some configurations can be configured when it is needed. Usually you don't need to modify the configurations. But if you want to modify the value, you can do that using web UI.

Go to `http://[ip_address]:[port]/CasServer > Login > Configuration > Server'`

Check below configurations.

Configuration Name	Default Value	Explanation
KeyServerURL	http://127.0.0.1:8080/CasServer/RequestSK.do	The URL of M/W server which provides key to LYNK. The sample value is 'http://127.0.0.1:8080/CasServer/RequestSK.do'. You should modify this value as your key server url containing page url for requesting SK.
SkPeriod	24 hours	The period for updating SK value.
NeedMKProvisioning	no	Determine whether or not to need for provisioning master key to share master key with Key Server. The default value is 'no'.
UseWatermark	no	Determine whether or not to insert watermark into EMM. The default value is 'no'.
DeviceType	TV	Determine the type of devices that LYNK Server manages. The default device type is "TV".

2.4. Configuring LYNK – ECMG Configuration(For Live Service)

i. ECMG Status

You can check the ECMG status of LYNK Server using web UI.

Go to `http://[ip_address]:[port]/CasServer > Login > Configuration > ECMG`

Check below items.

- ECMG Server Status : Displays the status of ECMG Server socket
- Channel Count : Displays the count of channel connected with ECMG Server of LYNK
- Stream Count : Displays the count of stream connected with ECMG Server of LYNK
- Recent Error : Displays recent ECMG errors

ECMG Status Item	Values	Description
ECMG Server Status	Ex) Running (10.240.48.192:9999)	ECMG Server is running and accepts client request.
	Not Running	ECMG Server is not running because of some problem. For example ECMG Server port defined for ECMGPort in configuration was bound already by another application.
Channel Count	Ex)5	The number means count of channels connected with ECMG Server socket.
Stream Count	Ex)5	The number means count of streams connected with ECMG Server socket.
Recent Error	ECMG_PORT_ALREADY_IN_USE	ECMG Port is already in use.
	ECMG_CW_ENCRYPTION_KEY_NOT_DEFINED	The CW from SCS is encrypted, but there is no CW encryption key is not set in LYNK in case that. If the CW from SCS is not encrypted, CW encryption key don't need to be set.
	ECMG_CW_ENCRYPTION_METHOD_NOT_DEFINED	The CW from SCS is encrypted, but there is no CW encryption method is not set in LYNK in case that. If the CW from SCS is not encrypted, CW encryption method don't need to be set.
	ECMG_CW_DECRYPT_ERROR	When the CW Encryption key has illegal hexadecimal character or odd number of characters.

To solve the above ECMG errors written in red, check below items.

- **ECMG_PORT_ALREADY_IN_USE**
 - ✓ Check if the ECMGPort defined in configuration is bound already.
 - ✓ If the port is used, modify the 'ECMGPort' value refer to following 'ECMG Configuration' and restart tomcat.
- **ECMG_CW_ENCRYPTION_KEY_NOT_DEFINED**
 - ✓ This error will occur only when the CW from SCS is encrypted.
 - ✓ If the CWEncryptionKey is blank, modify that value refer to following 'ECMG Configuration'.
- **ECMG_CW_ENCRYPTION_METHOD_NOT_DEFINED**
 - ✓ This error will occur only when the CW from SCS is encrypted.
 - ✓ If the CWEncryptionMethod is blank, modify that value refer to following 'ECMG

Configuration’.

- **ECMG_CW_DECRYPT_ERROR**

- ✓ This error will occur when the CW Encryption key has illegal hexadecimal character or odd number of characters.
- ✓ Check if the CWEncryptionKey or CWEncryptionMethod is wrong, modify that value refer to following ‘ECMG Configuration’.

ii. ECMG Configuration

Go to `http://[ip_address]:[port]/CasServer > Login > Configuration > ECMG’`

Check below configurations.

Configuration Name	Default Value	Explanation
ECMGPort	9999	The listening port number of ECMG Server in LYNK.
DelayStart	-500	The amount of time between the start of a Crypto Period and the start of the broadcasting of the ECM attached to this period. The unit is ms.
DelayStop	-500	The amount of time between the start of a Crypto Period and the end of the broadcasting of the ECM attached to this period. The unit is ms.
RepPeriod	300	The period in milliseconds for the repetition of data. The unit is ms.
MinCpDuration	50	Parameter is communicated at channel setup by the ECMG to the SCS to indicate the minimum supported amount of time a control word shall be active before it can be changed. The unit is 100ms.
MaxCompTime	30	Parameter is communicated by the ECMG to the SCS during channel setup. The unit is ms.
CWEncryptionKey		CW Encryption Key. During provisioning CW, SCS can encrypt CW and send that encrypted value. The ECMG Server of LYNK receives the encrypted CW and decrypts CW using CWEncryptionKey and CWEncryptionMethod. If you don't encrypt CW, you don't need to set this value.
CWEncryptionMethod		CW Encryption method. During provisioning CW, SCS can encrypt CW and send that encrypted value. The ECMG Server of LYNK receives the encrypted CW and decrypts CW using CWEncryptionKey and CWEncryptionMethod. If you don't encrypt CW, you don't need to set this value.

※ *DelayStart, DelayStop, RepPeriod, MinCpDuration and MaxCompTime are used in ecm_channel_status message in response of ecm_channel_setup message on simulcrypt protocol.*

2.5. Configuring LYNK – EMMG Configuration(For Live Service)

i. EMMG Status

You can check the EMMG status of LYNK Server using web UI.

Go to `http://[ip_address]:[port]/CasServer > Login > Configuration > EMMG`

Check below items.

- EMMG Client Status : Displays the status of EMMG Client
- EMMG Period : Displays the EMM transmission period
- EMMG Server Count : Displays the total count of EMMG Server registered in LYNK
- Recent Error : Displays recent EMMG errors

EMMG Status Item	Values	Description
EMMG Client Status	Running	EMMG Client thread is running and sends EMMs to EMMG server registered in LYNK.
	Not Running	EMMG Client thread is not running because user stopped the EMMG Client Service by clicking 'Stop EMMG Service' button.
EMMG Period	Ex)200ms	This means EMM transmission period from LYNK to SCS. The unit of value is ms.
EMMG Server Count	Ex)2	The number means count of EMMG Server registered in LYNK.
Recent Error	EMMG_SERVER_CONNECTION_ERROR	This means there is one or more connection error to EMMG server.

To solve the above EMMG errors written in red, check below items.

- **EMMG_SERVER_CONNECTION_ERROR**
 - ✓ Check if the EMMG Server information registered in LYNK is correct.
 - ✓ If the EMMG Server information is wrong, delete the wrong EMMG Server and add EMMG Server from the EMMG Server List. Before deleting EMMG Server, you should stop the EMMG Service by clicking 'Stop EMMG Service' button. After adding new EMMG Server, you should start the EMMG Service by clicking 'Start EMMG Service' button.
- **Not Running**
 - ✓ Check if the EMMG Service was stopped and then start the EMMG Service by clicking 'Start EMMG Service' button

ii. EMMG Configuration

Go to `http://[ip_address]:[port]/CasServer > Login > Configuration > EMMG`

Configuration Name	Default Value	Explanation
EMMGPeriod	200	The EMM transmission period from LYNK to EMMG Server. The unit is ms.(Min. : 200ms)

iii. EMMG Server Configuration

You should set the values of emmg server ip, port, channel id and stream id.

Go to `http://[ip_address]:[port]/CasServer > Login > Configuration > EMMG`.

Add or delete EMMG Server from the EMMG Server List in that page.

2.6. Changing logging level of LYNK

You can change logging option by change configure file.

The configure file for logging is "\$TOMCAT_HOME/webapps/CasServer/WEB-INF/classes/log4j.xml"

You can change the logging level by changing value in red as following.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE configuration >
<configuration debug="true" xmlns='http://logging.apache.org/'>
  <appender name="dailyRollingFile"
    class="com.samsung.icecop.admin.service.CustomDailyRollingFileAppender">
    <param name="File" value="{catalina.home}/logs/CasServer" />
    <param name="Append" value="true" />
    <param name="DatePattern" value="'.yyyy-MM-dd'.log" />
    <param name="MaxNumberOfDays" value="14"/>
    <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="[%d{ISO8601}] %-
5p:[%t]%x(%C:%M) - %m%n" />
    </layout>
  </appender>
  <root>
    <level value="info" />
    <appender-ref ref="dailyRollingFile" />
  </root>
</configuration>
```

Default value of level is "info".

The log levels are debug (most detailed log level), info, warn, error and fatal(most simple log level).

If you want to see the detailed log, you should set the value of level as debug.

You should restart tomcat to apply above modification.

3. Scrambler Setup(For Live Service)

3.1. Configuring scrambler in regard to LYNK

- i. ECMG Server(in LYNK) Configuration
You should set the value of ecmg server ip address and port number to get ECM data from LYNK.
Refer to ECMGPort value of LYNK Server Configuration menu.The default value of ecmg port is 9999.
- ii. ECMG Channel and Stream Configuration
You should set the values of channel, stream and ecm used in ecm_channel_setup and ecm_stream_setup message of Simulcrypt. Whatever you set channel, stream and ecm, LYNK accept that without setting in LYNK.
- iii. LYNK's CLIENT_ID Configuration
The value of LYNK's CLIENT_ID in Simulcrypt is 0x112. The CLIENT_ID value is used in EMM_CHANNEL_SETUP message.

4. Check your system that LYNK server is installed

- i. Check windows update settings (**only Windows**)
If you use automatic updating option in Windows, you should disable this option. Otherwise your system will be restarted whenever windows updating works.
- ii. Check firewall settings
If you cannot access the LYNK web page from any remote computer, you should check firewall settings of the system that LYNK Server is installed. You can enable HTTP and HTTPS to allow connection to your website by setting firewall.
- iii. Check hard disk capacity
LYNK and tomcat server creates log files everyday. Therefore it needs some hard disk volume. In normal condition, it needs 7 MB per one day.

LYNK backups the watermark data file whenever the capacity of watermark file is greater than 1024bytes. The backedup files are saved in "\$TOMCAT_HOME/logs/LYNK_Backup/" directory.

Therefore, you need to check the capacity of your LYNK system periodically.