

Realize your vision



Samsung SDS **EMM**

Installation Guide



Solution version 2.2.5

Published: January 2023

Before using this information and the product it supports, be sure to read the general information on this page.

Publisher Samsung SDS Co., Ltd
Address 125, 35-Gil, Olympic-Ro, Songpa-Gu, Seoul, South Korea.
Email ems.support@samsung.com
Website www.samsungsds.com

Samsung SDS Co., Ltd. has credence in the information contained in this document. However, Samsung SDS is not responsible for any circumstances which arise from inaccurate content or typographical errors.

The content and specifications in this document are subject to change without notice.

Samsung SDS Co., Ltd. holds all intellectual property rights, including the copyrights, to this document. Using, copying, disclosing to a third party or distributing this document without explicit permission from Samsung SDS is strictly prohibited. These activities constitute an infringement of the intellectual property rights of this company.

Any reproduction or redistribution of part or all of these materials is strictly prohibited except as permitted by the license or by the express permission of Samsung SDS Co., Ltd. Samsung SDS Co., Ltd. owns the intellectual property rights in and to this document. Other product and company names referenced in this document are trademarks and / or registered trademarks of their respective owners.

DFARS Limited Rights Notice

LIMITED RIGHTS

Contractor Name: Samsung SDS Co. Ltd., *via its distributor in the U.S.*, Samsung SDS America, Inc.

Contractor Address: Samsung SDS America, Inc.: 100 Challenger Road, 6th Fl., Ridgefield Park, NJ 07660 U.S.A.

The US Government's rights to use, modify, reproduce, release, perform, display, or disclose these technical data are restricted by paragraph (b)(3) of the Rights in Technical Data--Noncommercial Items clause contained in the US Government contract under which the US Government has obtained a license to use this computer software. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings. Any person, other than the US Government, who has been provided access to such data must promptly notify the above named Contractor.

(End of legend)

FAR Limited Rights Notice

Limited Rights Notice (Dec 2007)

(a) These data are submitted with limited rights under the US Government contract under which the US Government has obtained a license to use these data. These data may be reproduced and used by the US Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the US Government, except that the US Government may disclose these data outside the US Government for the following purposes, if any; provided that the US Government makes such disclosure subject to prohibition against further use and disclosure (if any).

(b) This notice shall be marked on any reproduction of these data, in whole or in part.

(End of notice)

Copyright 2022 Samsung SDS Co., Ltd. All rights reserved.

Preface

Users of this guide

This guide is written for system administrators who install Samsung SDS EMM (hereinafter “EMM”) solution, which provides an integrated security service. It also covers for users who manage the EMM system such as stop, start, and update the EMM.

In order to use this solution effectively, the administrator must have the understanding and experience of the following:

- General knowledge on how to operate systems
- General knowledge on how to set network systems
- General knowledge on security activities
- General knowledge on how to use web servers

Summary of this guide

This guide consists of the following chapters:

- **Chapter 1. Samsung SDS EMM installation overview**
Provides an overview of EMM and installation environment.
- **Chapter 2. Pre-installation**
Covers basic system and computer requirements needed for installing EMM.
- **Chapter 3. Installation**
Explains how to install EMM.
- **Chapter 4. Post-installation**
Explains an environment's setup after installation.
- **Chapter 5. Updating**
Explains how to use the patch installer to update EMM.
- **Chapter 6. Configuring EMM High Availability**
Explains how to configure the system to increase the availability of EMM.
- **Appendix**
Explains other integration services and configuration files.

Conventions

This document uses the following conventions:

Convention	Description
Boldface	Boldface is used to graphical user interface elements, menus, navigation trees and directories within the main text.
" "	" " double quotation marks using as below: <ul style="list-style-type: none"> • Graphical user interface pages, portals, windows • Referring to other booklets, white papers, etc., mention the author or publisher of the publication and mark the title of the book in double quotation marks
"Cross-reference"	"Cross-reference" is used to reference documents or other chapters in a document. If click the cross reference, it moves to the specified location.
Monospace	Monospace is used to commands, parameters, file names and codes. Also, the monospace font uses Courier New.
Picture	The picture is used to graphics, illustrations, screen captures, etc. to help understand documents.
Table	The table is used to easily identify and display large amounts of information in the document.

Notes

The Note is used to additional information such as tips, recommendations, exceptions, and limitations.

Note: To reflect filtered data again, click Refresh Data on the Add Common Group window.

Revision history

Solution version	Manual version	Manual revised date	Revised details
1.0.0	1.0.0	November 2014	Version 1.0.0 published.
1.0.1	1.0.1	December 2014	Version 1.0.1 published.
1.0.3	1.0.3	February 2015	Version 1.0.3 published.
1.1.0	1.1.0	March 2015	Version 1.1.0 published.
1.1.1	1.1.1	June 2015	Version 1.1.1 published.
1.1.2	1.1.2	June 2015	Version 1.1.2 published.
1.1.3	1.2.0	September 2015	High security package installation
1.2.0	1.2.2	October 2015	Updated on Samsung SDS EMM for iOS
1.2.2	1.2.3a	December 2015	Multi-server installation
1.2.3	1.3.0a	April 2016	Added Windows authentication method and SQL Server certificate installation.
1.3.0	1.4.0a	July 2016	Added hostname settings in the installer and the chapters of Configuration HA, Installing SEG.
1.4.0	1.4.1a	August 2016	Added configuring a certificate for HTTPS.
1.4.1	1.5.0a	October 2016	Added configuring Push Certificate Key Types for high security installer and installing Cloud Connector.
1.5.0	1.5.1a	December 2016	Add setting AppTunnel URLmapping for Android N and changing the RSA modules after updating. Supported the ECC P256 certificate.
1.6.0	1.6.0a	March 2017	• Changed the Apache tomcat version.
1.6.1	1.6.1a	May 2017	Added the list of open ports in the firewall to Tizen Push.
2.0	2.0a	October 2017	• Edited the firewall port opening for Tizen Push domains. • Added installation and settings for SecuCamera.
2.0	2.0b	January 2018	Updated supporting iOS APNs
2.0.2	2.0.2a	February 2018	Changed how iOS APNs certificate is generated
2.1	2.1.0a	April 2018	• Updated Cloud Connector • Changed SecuCamera mail sender setting
2.2.0	2.2.0a	March 2019	Updated Cloud Connector
2.2.4	2.2.4a	November 2019	Updated cipher suite

Solution version	Manual version	Manual revised date	Revised details
2.2.5	2.2.5a	January 2020	Updated EMM Admin Portal UX/UI Removed mMail, Secure Email Gateway Updated supporting JDK
2.2.5.1	2.2.5b	March 2020	Added installation and update instructions
2.2.5.2	2.2.5c	December 2020	Changed how licenses are searched and registered Support for token-based APNs authentication
2.2.5.3	2.2.5d	March 2021	Updated SecuCamera INI file setting contents
2.2.5.4	2.2.5e	June 2021	Updated Using EMM on iOS
2.2.5.5	2.2.5f	November 2021	DB script modification for token-based iOS APNs certificate registration Added Tomcat Upgrade Guide
2.2.5.6	2.2.5g	March 2022	Support MS SQL Server 2019
2.2.5.8	2.2.5i	December 2022	- Version 2.2.5.8 published. - Added Open JDK Verification environment

Table of Contents

Preface	iii
Users of this guide	iii
Summary of this guide	iv
Conventions	v
Notes	v
Revision history	vi
1 Overview of EMM installation	1
1.1 EMM installation component	2
1.2 EMM installation architecture	3
1.2.1 Single server architecture	4
1.2.2 Multi server architecture	5
1.3 EMM installation environment	6
2 Pre-installation	8
2.1 Installing JDK	8
2.2 Preparing certificates	10
2.2.1 Preparing server certificate	10
2.2.2 Preparing device certificate	14
2.3 Installing SQL Server	17
2.3.1 Downloading SQL Server	17
2.3.2 Installing SQL Server	17
2.3.3 Reference for installing SQL Server 2012	17
2.3.4 Adding a Windows account and privilege	19
2.4 Pre-installation checklist	21
2.4.1 Single server environment	21
2.4.2 Multi server environment	22
2.4.3 Notes on post	25
3 Installation	27
3.1 Installing EMM in a single-server environment	27
3.2 Installing EMM in a multi-server environment	37
3.2.1 Installing EMM	38
3.2.2 Installing web server	47
3.2.3 Installing Push Proxy	47
3.2.4 Installing AppTunnel Relay	48
3.3 Notes on post - Installation phase	50

4	Post-installation	52
4.1	Starting EMM	53
4.1.1	Single-server environment	53
4.1.2	Multi-server environment	55
4.2	Checking EMM status.....	57
4.3	Confirming the EMM license.....	58
4.4	Setting the service profile.....	59
4.4.1	Single-server environment	59
4.4.2	Multi-server environment	61
4.5	Registering certificate authority	64
4.6	Configuring a certificate for HTTPS	64
4.7	Registering users and devices.....	65
4.8	Registering EMM apps.....	65
4.9	Test.....	66
5	Updating EMM	67
5.1	Stopping services.....	67
5.1.1	Single-server environment	68
5.1.2	Multi-server environment	68
5.2	Installing EMM patch	70
5.2.1	Checking digital signature	70
5.2.2	Installing the patch in a single-server environment	71
5.2.3	Installing a patch in a multi-server environment	73
5.2.4	Uploading APK file	75
5.3	Changing RSA modules.....	75
5.4	Starting services	75
5.4.1	Single-server environment	75
5.4.2	Multi-server environment	76
5.5	Retrieving the EMM patch.....	78
5.6	Tomcat Upgrade	78
6	Configuring EMM High Availability	81
6.1	System configurations	81
6.1.1	Installation architecture	81
6.1.2	Installation components	82
6.1.3	Prerequisites	82
6.2	Installing the servers.....	84
6.3	Configuring the settings.....	92
6.3.1	Configuring the EMM settings	92
6.3.2	Configuring the Push settings	94
6.3.3	Configuring the AppTunnel settings	96

6.4	Testing.....	97
6.4.1	Mobile device test scenarios	97
6.4.2	Admin Portal test scenarios	100
Appendix A	Installing or changing a certificate.....	103
Appendix B	Configuring allowable Cipher.....	106
Appendix C	Audit Remote Logging.....	110
Appendix D	Using EMM on iOS	122
Appendix E	Installation Environment File.....	154
Appendix F	Installing SQL Server certificate	162
Appendix G	SecuCamera	169

1 Overview of EMM installation

Samsung SDS Enterprise Mobility Management (hereinafter "EMM") is a solution designed to support comprehensive security management across multiple layers, ranging from user devices and applications to data. A single, integrated Admin Portal, regardless of OS, enables more efficient mobile security management. It also offers security policies and a UI to satisfy customer needs and provide a user-friendly experience and improves system stability and work productivity.

This guide describes how to install and update EMM software with 6 chapters:

- Installation overview
- Pre-installation (prerequisites)
- EMM installation
- Post-installation
- Updating EMM
- Configuring EMM High Availability

Details on the process of installation are below.

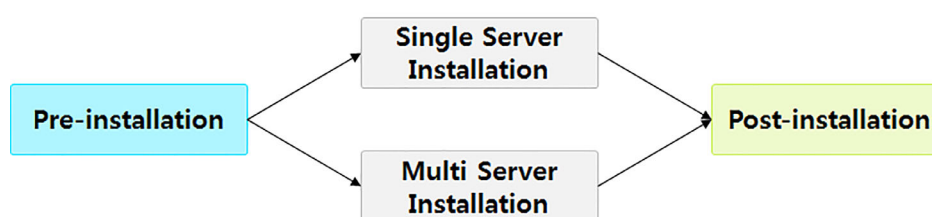


Figure 1-1. EMM installation process

Please refer to a EMM Security Target written by Gossamer for the details of security functions that have been subject to Common Criteria evaluation.

1.1 EMM installation component

The followings are modules for server and device required to install EMM:

EMM server module

Module	Roles	Notes	
EMM	Management of device and policies, communication with server modules		
LTS	A server that collects logs from the device.		
Push	DCM	Keeps the communication channel unimpeded and transfers messages between Device Agent on a device and Push server	
	PS	Register the user's device on the device side and check the data channel from DCM	
	SCM	Keeps the communication channel open between the Service Agent on the EMM and Push server	
	ECM	Keeps the communication channel open between a 3 rd party platform (FCM or APNs) and the Push server	
ICM	Provides a TLS channel for message exchange between physically separated servers.		
AppTunnel	Establish a secured channel for each app to transfer information without a risk of leak		
Push Proxy	DPP	Message relay between device agent and DCM	Multi-server only
	PPP	Message relay between device agent and PS	
	EPP	Message relay between device agent and ECM	
AppTunnel Relay	Packet relay between device and AppTunnel server		

EMM device module

Platform	Module	Roles
Android	EMM Agent	Device control and monitoring
	Push Agent	Communication with a server
iOS	EMM Client	Device control and monitoring
Windows	EMM Client	Device control and monitoring
Tizen Push	EMM Client	Device control and monitoring

Note: If you have installed and are currently using a version which separates the EMM Client from the EMM Agent, and want to update it to the integrated EMM Agent, then you need to deactivate the EMM on your device, and then re-install the integrated EMM Agent.

1.2 EMM installation architecture

EMM is installed with either a single server or multiple servers depending on the number of users and security level.

- *Note that communication between the EMM Agent and EMM Server are secured through TLS channels by default. The communication path from the Admin Portal to the EMM server channels also creates an encrypted communication channel by supporting HTTPS (over TLS). The communication path from the EMM to its certificate authority (MC ADCS), supporting MS SQL and Syslog Server are protected using Windows Server provided IPsec – instructions can be found in Samsung SDS EMM Configuration Guide for IPsec settings in Microsoft Windows Server 2016/2019 for Common Criteria Evaluation*
- *Please refer to the EMM system architecture diagrams below. Note that the ports identified in the following figures are only examples – the actual ports can be configured during installation. Note also that while the diagrams identify the MS ADCS, MS SQL and Syslog Server connections as HTTPS or TLS, in the evaluated configuration they are protected using IPsec as identified above*

1.2.1 Single server architecture

In single server architecture, EMM, Samsung SDS Push (hereinafter "Push"), Samsung SDS AppTunnel (hereinafter "AppTunnel"), and the database are installed on one single server. The single-server system is appropriate where there are few users or the server is used for demo.

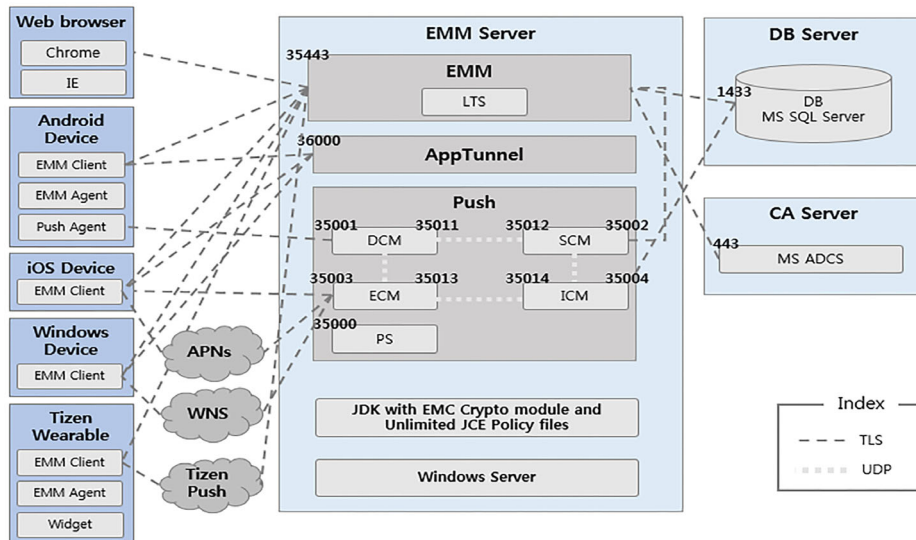


Figure 1-2. Single server architecture for EMM

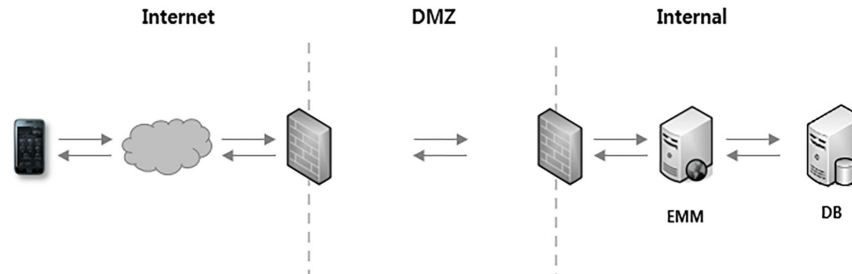


Figure 1-3. Single server network composition for EMM

1.2.2 Multi server architecture

For multi server architecture, EMM, Push, App Tunnel, Web server, Push Proxy, App Tunnel Relay, and the database are installed in a number of different servers, or the modules are grouped by area and installed on separate servers. CPU usage for the Log Transfer Server (LTS) used in EMM may increase due to multiple log processing times for many users. To accommodate a large number of users, the LTS are installed on separate servers. Multi server architecture is recommended for the case where you have a large number of users or the system requires a high level of security.

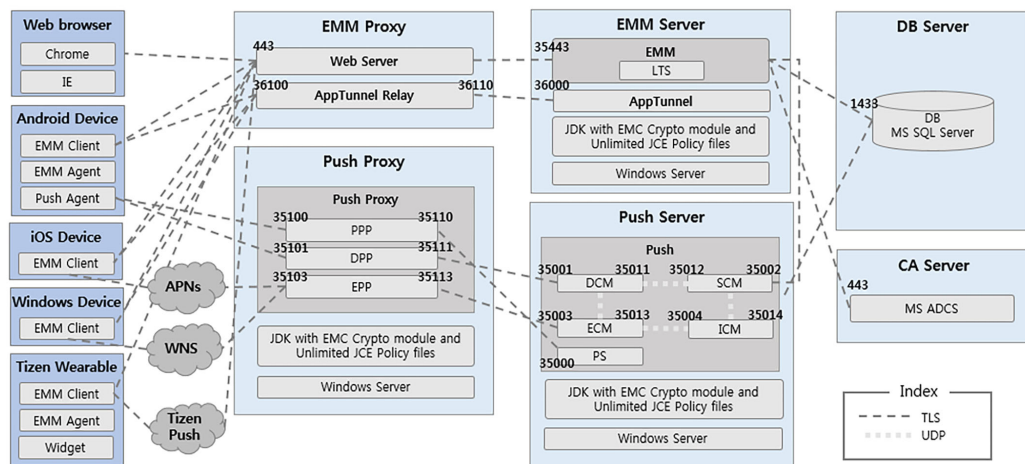


Figure 1-4. Multi server architecture for EMM

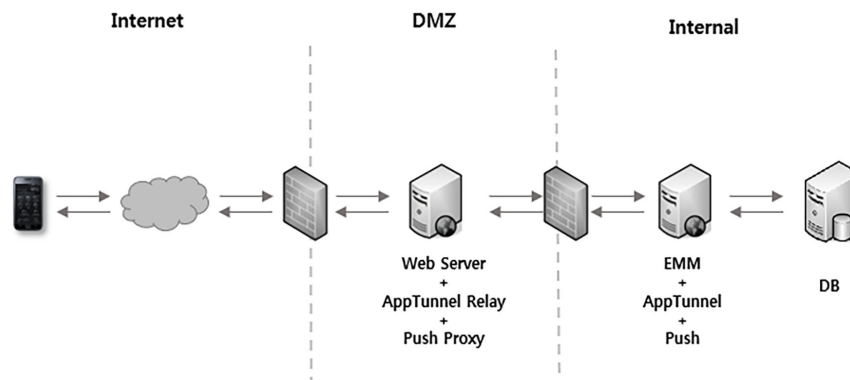


Figure 1-5. Multi server network composition 1 for EMM

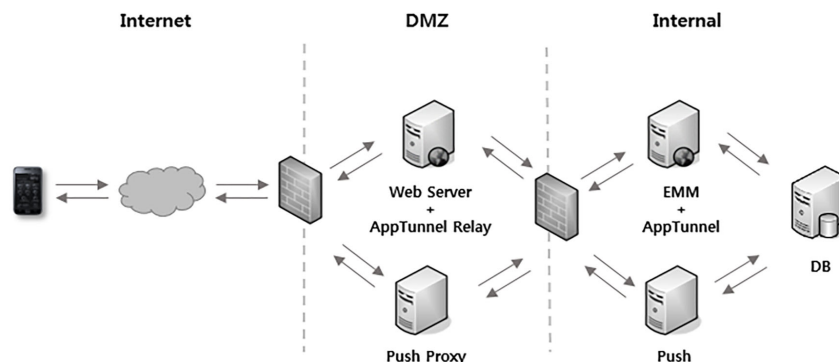


Figure 1-6. Multi server network composition 2 for EMM

1.3 EMM installation environment

The minimum hardware and software requirements that must be met to install and run EMM are listed below.

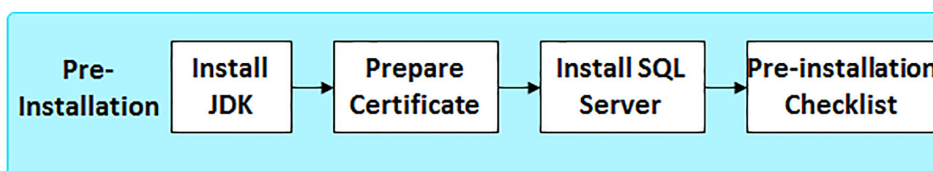
Item	Requirements
CPU	x86 quad-core processor
Memory	16GB RAM
Storage	100GB hard-disk space
Operating System	<ul style="list-style-type: none"> Windows Server 2012 R2, 2016 (the evaluated platform for CC evaluation) Windows Server 2019
Java Development Kit	Java Development Kit 1.8 (64bit, the evaluated for CC evaluation) <ul style="list-style-type: none"> Oracle JDK 1.8 (64bit) Open JDK 1.8 (Verification environment: Open JDK Azul zulu 8.31.0.1) <p>Note:</p> <ul style="list-style-type: none"> An Oracle JDK license is not provided. For Open JDK, you're recommended to use Azul Systems' Zulu module. https://www.azul.com/downloads/zulu/zulu-windows/ Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files 7 or 8
DBMS	MS SQL Server 2008-2016, 2019 (the evaluated for CC evaluation)
Browser	<ul style="list-style-type: none"> Chrome 41 Firefox 37 Internet Explorer 11

Item	Requirements
Certificate	<p data-bbox="639 253 1230 360">EMM, Push certificate APNs certificate, iOS cert certificate MS SQL Server certificate (when applying JDK 1.8)</p> <p data-bbox="639 376 1401 517">Note: • When using JDK 1.8, it is necessary to install RSA Key Size 2048bit certificate due to the limitation of commercial encryption module.</p>

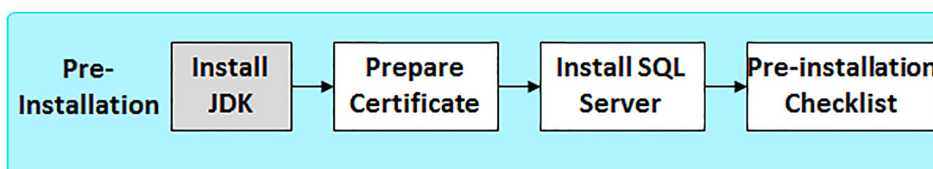
Note: After installing EMM for the first time, Tomcat upgrade and security patch must be performed by the client itself.

2 Pre-installation

This chapter describes prerequisites for the Samsung SDS EMM (hereinafter "EMM") installation. Here are the steps for pre-installation:



2.1 Installing JDK



The servers on which JDK should be installed are:

Category	Servers requiring JDK
Single server environment	EMM
Multi server environment	<ul style="list-style-type: none"> • EMM • Push • Push Proxy

1. Download Java SE Development Kit(64bit). See the Oracle or Open JDK web page for more details.
2. Install JDK.
 - If the newly installed JDK version is 1.8.0_151-b12 or later, you do not need Java patch and the security attribute must be configured. For more information, see step 6.
 - If you install Open JDK, JCE settings are not required.
3. Install EMC Crypto module certified by officially-released FIPS 140-2.
 - a. Decompress the `tomcat_rsa_module.zip` file.
 - b. Copy the files under `{tomcat_rsa_module.zip unzip location}` to `{JDK Home location}\jre\lib\ext`.
 - `cryptojce-6.2.5.jar`
 - `cryptojcommon-6.2.5.jar`
 - `jcmFIPS-6.2.5.jar`
 - `sslj-6.2.6.jar`

- `cryptojtestwriter.jar`

4. Edit the contents of `%JAVA_HOME%\jre\lib\security\java.security` file as below (Red fonts should be updated).

```

security.provider.1=com.rsa.jsse.JsseProvider
security.provider.2=com.rsa.jsafe.provider.JsafeJCE
security.provider.3=sun.security.provider.Sun
security.provider.4=sun.security.rsa.SunRsaSign
security.provider.5=sun.security.ec.SunEC
security.provider.6=com.sun.net.ssl.internal.ssl.Provider
security.provider.7=com.sun.crypto.provider.SunJCE
security.provider.8=sun.security.jgss.SunProvider
security.provider.9=com.sun.security.sasl.Provider
security.provider.10=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.11=sun.security.smartcardio.SunPCSC
security.provider.12=sun.security.mscapi.SunMSCAPI

com.rsa.ssl.compatibility.layeredsocket.useavailable=enabled

```

Note: When using a Tizen Wearable device, delete the "SHA1 jdkCA & usage TLSServer" from the "jdk.certpath.disabledAlgorithms" value in the setting key.
 Example) `jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, DSA keySize < 1024, EC keySize < 224`

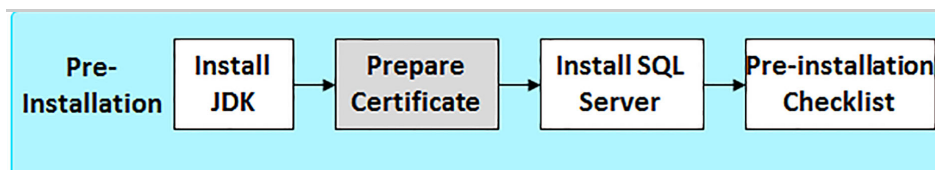
5. Copy the Java Cryptography Extension (JCE) policy file that matches the JDK version.

- Download the unlimited strength JCE policy files.
For the detailed information, see Oracle web page.
- Unzip the downloaded file to create a sub-folder named `UnlimitedJCEPolicy`. This directory contains the following files.
 - `README.txt`
 - `local_policy.jar`: Unlimited strength local policy file
 - `US_export_policy.jar`: Unlimited strength US export policy file
- Copy the 2 JAR files (`local_policy.jar`, `US_export_policy.jar`) to the directory `{JDK Home location}\jre\lib\security`.

6. If the patched JDK version is later or equal to the target version, configure the security attribute for the encryption policy.

- Target version
 - JRE 8: `1.8.0_151-b12`
- How to set up
 - Uncomment or add `crypto.policy=unlimited` in the `%JAVA_HOME%\jre\lib\security\java.security` file.

2.2 Preparing certificates



To establish the TLS connection, KeyStore needs to be created using a certificate. For this, a certificate needs to be prepared beforehand.

Certificates required for each installation architecture

Category	Certificate
Single server	<ul style="list-style-type: none"> • EMM server certificate • APNs certificate • iOS sign certificate
Multi server	<ul style="list-style-type: none"> • EMM server certificate • Push server certificate • APNs certificate • iOS sign certificate

Note: Hereinafter, the EMM certificate is the PKCS#12 certificate for servers used by EMM, and the push certificate is the PKCS#12 certificate for servers used by Push.

2.2.1 Preparing server certificate

The requirements and considerations for issuing a server certificate are as below.

Server certificate requirements

The certificate for the EMM server and Push server must satisfy the requirements below and "[Considerations for issuing a server certificate](#)" on page 11. The certificates should also be issued by PKI system in PKCS #12 format.

Available Certificate	Constraints	Requirements
RSA certificate	When ECC certificate is used, the EC Key Curves of the Root certificate and all chain certificates must be same. And their key sizes must be same as P256 or P384.	<ul style="list-style-type: none"> • Hash algorithm: SHA256 orSHA384 • Signing: ECDSA certificate • FIPS 140-2 Compliant certificate
P256 key ECC certificate		
P384 key ECC certificate		

-
- Note:**
- A general certificate converts to FIP 140-2 mode with the converter provided.
 - The Extended Key Usage item for the RSA certificate must contain Key Encipherment. For more information, see ["Notes for issuing the RSA certificates" on page 12](#).
 - A certificate for the EMM server needs to be issued by a recognized certificate authority. As for self-signed certificates, a device is provisioned only when a self-signed root certificate is stored into a device.
 - You can create a self-signed certificate for demonstration purposes by using Java Keytool or OpenSSL. The self-signed server certificates are not allowed for CC certification.
 - You can find more information on issuing APNs certificate and iOS sign certificate in ["Appendix D, Using EMM on iOS" on page 122](#).
-

Installing and registering Certificate Authority

For information on how to install Certificate Authority (CA) with Microsoft ADCS(Active Directory Certificate Services), see Microsoft official document.

Considerations for issuing a server certificate

To provide a secure communication channel, EMM establishes TLS between servers or between a server and devices. A secure communication channel requires a certificate and PKI system. A certificate is issued by CA included in PKI system.

The certificate used on EMM must meet the following requirements.

- Expiration date
- Extended key usage (ClientAuth, ServerAuth)
- Basic constraints
- Validation of root chain
- Distinguished name (DN)
- Revoked certificate (CRL)

The top 4 items are automatically verified when the server and device check mutual certificate information.

Verifying certificate distinguished name (DN)

The distinct names for certificates are verified through the EMM sever. The followings are verification points.

- Device checks the DN of EMM server certificate:
Device checks matching EMM server information (IP or domain name) and common name (CN) of the certificate.

- Push and AppTunnel server check the DN of the device certificate:
Push and AppTunnel server check the device certificate whether it has been issued from EMM server.

To verify the certificate DN, the configuration constraints for Push and AppTunnel are the following:

- Configuration Constraints for Push:
 - Push Server certificate CN matches server information on a device.
For Example, If IP is used to issue a certificate, IP should be entered when server information is needed.
 - When running Push on non-proxy mode, CN of Push server (PS, DCM) certificate must correspond with EHOST of execution script.
For Example, java-ehost = "CN of your certificate"...-jar...
 - When running Push on proxy mode, CN of Push Proxy (PPP, DPP) certificate must match EHOST field of Push_ProxyInstanceInfo Table that Push server refers to.
 - When accessing Push Proxy(PPP, DPP) or Push Server (PS, DCM) with L4 equipment, Push Proxy and Push server certificates exclusively for L4 must be installed.
- Configuration Constraints for AppTunnel
 - AppTunnel Server certificate CN matches server information on a device.
For Example, If ATR certificate is issued with IP, enter IP when ATR information is requested.
 - When accessing AppTunnel Relay and AppTunnel Server with L4 equipment, certificate of AppTunnel Relay and AppTunnel Server exclusively for L4 must be installed.
For Example, CN of ATR certificate must correspond with Domain Name of L4.

Verifying certificate CRL

Certificate CRL verification is to identify if the other party's certificate has been revoked during TLS. For information about the OCSP configuration, see "Configuring OCSP" provided separately.

Notes for issuing the RSA certificates

If you are using an RSA algorithm certificate for TSL communication, Extended Key Usage items must contain Key Encipherment. Server certificates in the Extended Key Usage item that is included Server Authentication and Client Authentication are generally issued. However, for some CAs, you may not add Key Encipherment to Extended Key Usage items if they have both Server Authentication and Client Authentication. In that case, add only Server Authentication to the Extended Key Usage item when issuing a certificate, and change the set values as follows:

In push proxy mode or in AppTunnel relay mode, change the settings in the following file.

Service	File path	Set value
Push Proxy	{EMM Installation path}/PushProxy/{Version}/resources/general/properties/general.properties	Change IN_EXTENDED_KEY_USAGE =1.3.6.1.5.5.7.3.2 to IN_EXTENDED_KEY_USAGE =1.3.6.1.5.5.7.3.1
AT Relay	{EMM Installation path}/AT/{Version}/at-relay/resources/general/properties/general.properties	

Notes for issuing the ECC certificates

To call EMM Base URL as HTTPS when Push and App Tunnel is separated from the EMM server with using a ECC algorithm P256 certificate for TLS communication, you must change (`general.properties` | `BASE_URL=https://...`), ciphers value as below.

- Configuration file: `{Tomcat_HOME}/conf/server.xml` of EMM server
- Delete below cipher suite from connector:
 - `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`
 - `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384`

Note: Please be aware of vulnerabilities of Windows CryptoAPI used in ECC certificates authentication, and download the Windows server security patch from following URL:
<https://portal.msrc.microsoft.com/en-US/securityguidance/advisory/CVE-2020-0601>

2.2.2 Preparing device certificate

To establish the TLS connection between a server and a device, a device certificate needs to be prepared to install the certificate. The requirements and Setting the device certificate template are as below.

Server certificate requirements

The device certificate requirement is same as the server certificate. The algorithm of the device certificate should be the same algorithm of the server certificate.

Available Certificate	Constraints	Requirements
RSA certificate		<ul style="list-style-type: none"> • Hash algorithm: SHA256 orSHA384 • Signing: ECDSA certificate • FIPS 140-2 Compliant certificate
P256 key ECC certificate	<ul style="list-style-type: none"> • EMM certificate is supported on iOS 9 and iOS 10. • When you use the ECC certificate, the EC key curves of the root certificate and all chain certificates must be the same and the key size must be unified in either P256 or P384. • Do not include Key Agreement in Key Usage. 	
P384 key ECC certificate		

Note: To use the certificate of the P384 key, you must upgrade to Android 7.1.1 or later on the Android N OS.

Considerations for issuing a device certificate

The certificate used on EMM must meet the following requirements.

- Expiration date
- Extended key usage (ClientAuth)
- Basic constraints
- Validation of root chain
- Distinguished name (DN)
- Revoked certificate (CRL, OCSP)

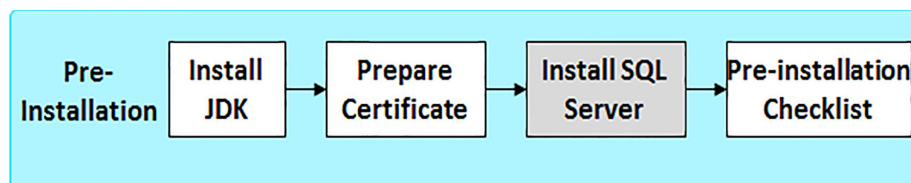
Setting the device certificate template

To set up a certificate template by CA, enter the value as below.

CA	Supported algorithm	Item
ADCS	<ul style="list-style-type: none"> • RSA 2048 • RSA 3072 • RSA 4096 • ECDSA P-256 • ECDSA P-384 	<ul style="list-style-type: none"> • Enter the device certificate name in Template display name, Template name area on General tab. • Select Supply in the request check box on Subject Name tab. • Select server information in Certification Authority, Certificate recipient area on Compatibility tab. • Select as below in Purpose area on Request Handling tab. <ul style="list-style-type: none"> - RSA algorithm:: Signature and Encryption - EC algorithm:: Signature • Select algorithm in Algorithm name area and enter minimum key size in Minimum key size on Cryptography tab. For example, Algorithm name: ECDSA_P384, Minimum key size: 384. • Select Application Policies on Extension tab and click Edit. Choose Client Authentication and click Add. • Select Key Usage on Extension tab and click Edit. Select the settings as below depending on the certificate algorithm. <ul style="list-style-type: none"> - RSA algorithm: Digital signature, Allow key exchange only with key encryption (key encipherment), Make this extension critical - EC algorithm: Digital signature, Make this extension critical
Generic SCEP	<ul style="list-style-type: none"> • RSA 2048 • RSA 3072 • RSA 4096 	See the setting guide depending on the vendor.

CA	Supported algorithm	Item
NDES	<ul style="list-style-type: none"> • RSA 2048 • RSA 3072 • RSA 4096 	Set the template in ADCS, and then register the created template name to Windows registry (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP). For detail values, see the value for ADCS.
CertAgent	<ul style="list-style-type: none"> • RSA 2048 • RSA 3072 • RSA 4096 • ECDSA P-256 • ECDSA P-384 	<p>Set the below item on Certificate Issuance menu in CertAgent Admin.</p> <p>In Extension Tab,</p> <ul style="list-style-type: none"> • select CA OCSP and enter the OCSP address on URL in Authority Information Access area. • enter CDP address on URL/DN in CRL Distribution Points area. • Select Server authentication and Client authentication check box in Extended Key Usage area. • select digital signature, key encipherment, key agreement check box in Key Usage area. <p>In Filter Tab,</p> <ul style="list-style-type: none"> • select Allow on Action in Subject Alternative Names area.

2.3 Installing SQL Server



2.3.1 Downloading SQL Server

See www.microsoft.com/en-us/evalcenter/evaluate-sql-server-2012-sp1.

2.3.2 Installing SQL Server

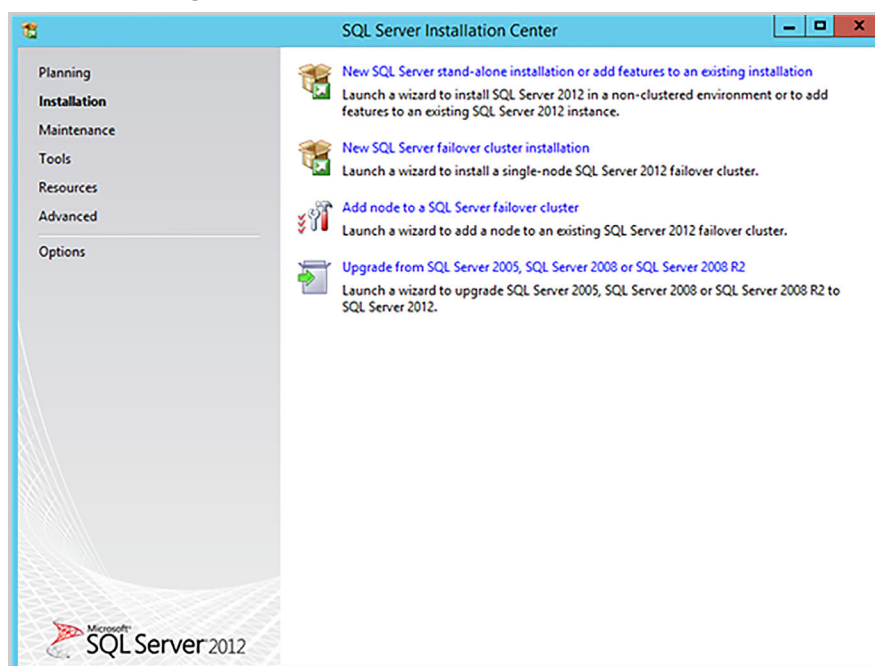
See [msdn.microsoft.com/en-us/library/bb500469\(v=sql.110\).aspx](http://msdn.microsoft.com/en-us/library/bb500469(v=sql.110).aspx).

-
- Note:**
- **File System Permissions Related to Unusual Disk Locations:**
The default path for installation is a system drive, normally drive C. When you install a temporary database or a user database, keep the followings in mind.
 - **Non-default Drive:** When a database is installed in a non-default drive, the per-service SID must have access to the database directory. SQL Server Setup enables the access.
 - **Network Share:** When you install a shared database on a network, a service account must have access to user's files and the shared database directory. SQL Server Setup does not provide database sharing on a network.
 - **Choose an Authentication Mode:**
You must select **Mixed Mode** authentication during setup. A password for sa, the administrator account for the built-in SQL server system, should be set. The sa account connects to the database by using SQL Server Authentication.
-

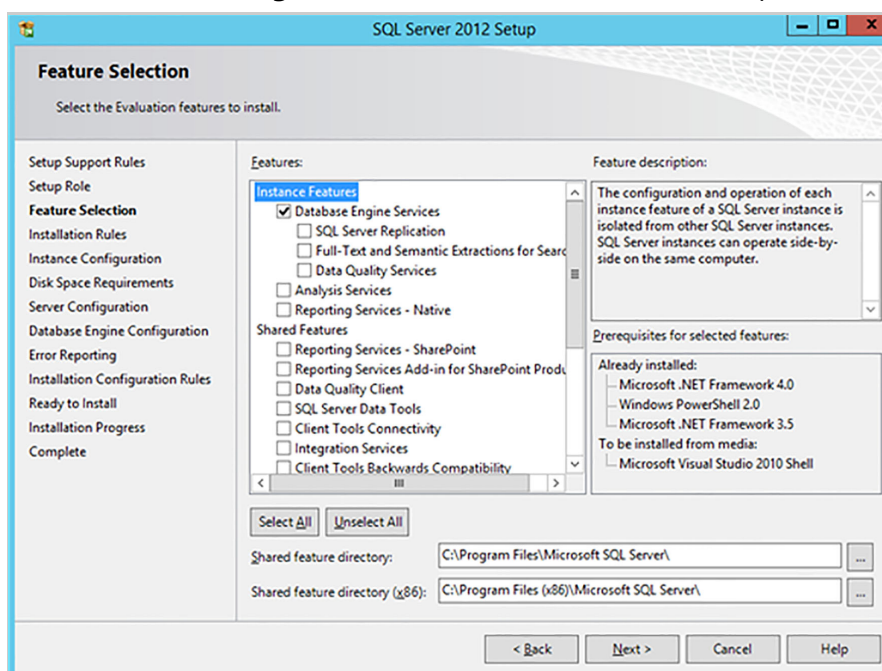
2.3.3 Reference for installing SQL Server 2012

For detailed information regarding hardware and software requirements for install of SQL Server 2012, see technet.microsoft.com/en-us/library/bb500469%28v=sql.110%29.aspx. To install SQL Server 2012, complete the following steps:

1. Select an option **New SQL Server stand-alone installation or add features to an existing installation.**

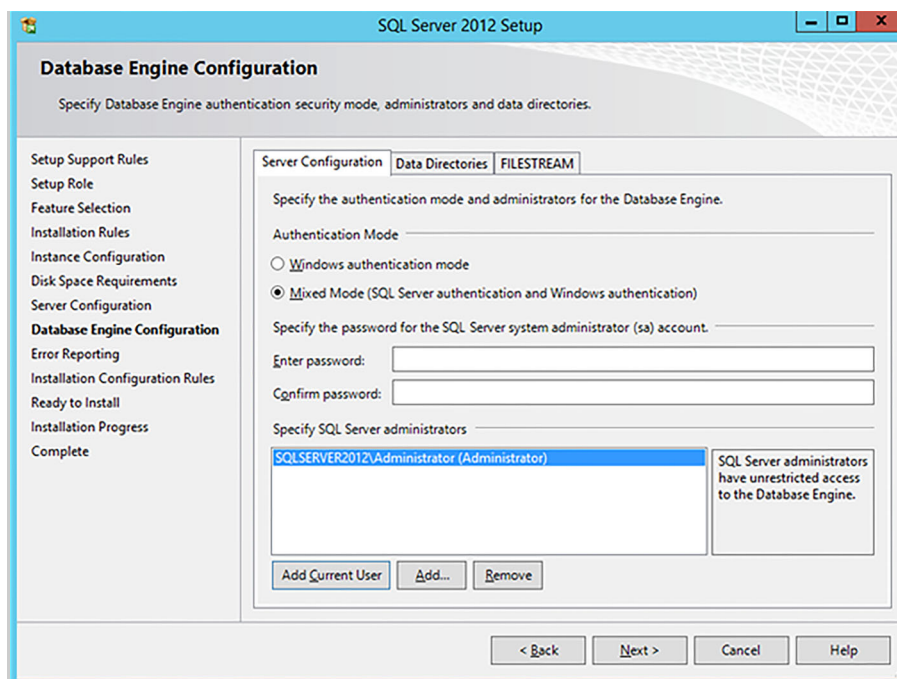


2. Select **Database Engine Services** in Feature Selection step.



3. Specify **Database Engine authentication security mode** in the Database Engine Configuration step.

- a. Select **Mixed Mode** in the **Authentication Mode** area on the Server Configuration tab.
 - Mixed Mode authenticates both the SQL account and Windows. Account authentication is required to access the database from EMM server. For account authentication, choose Mixed Mode.
- b. Enter a password in the **Enter password** field.
- c. Confirm the password in the **Confirm password** field.

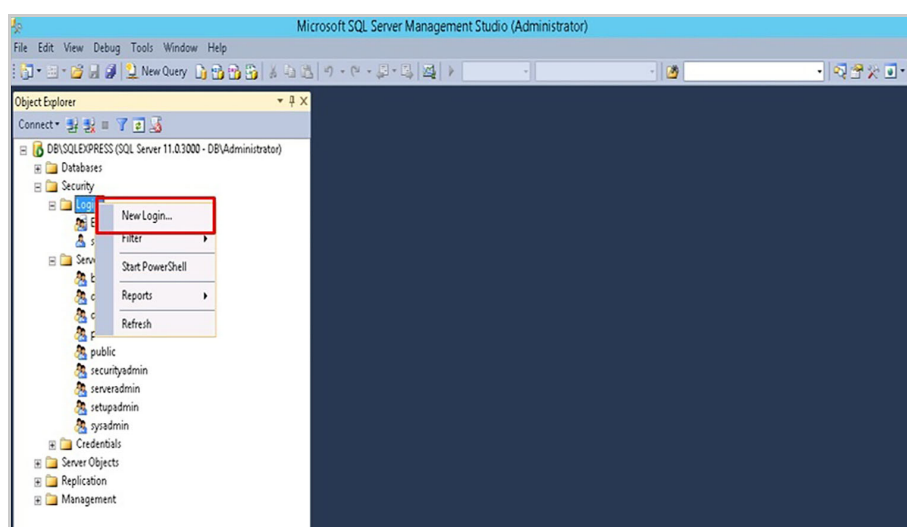
d. Click **Add Current User**.

- Note:**
- If information in database is not correct, EMM cannot be installed.
 - Confirm your DBA account and password when the message when the message " Please enter DBA account and Password to install DB" appears.

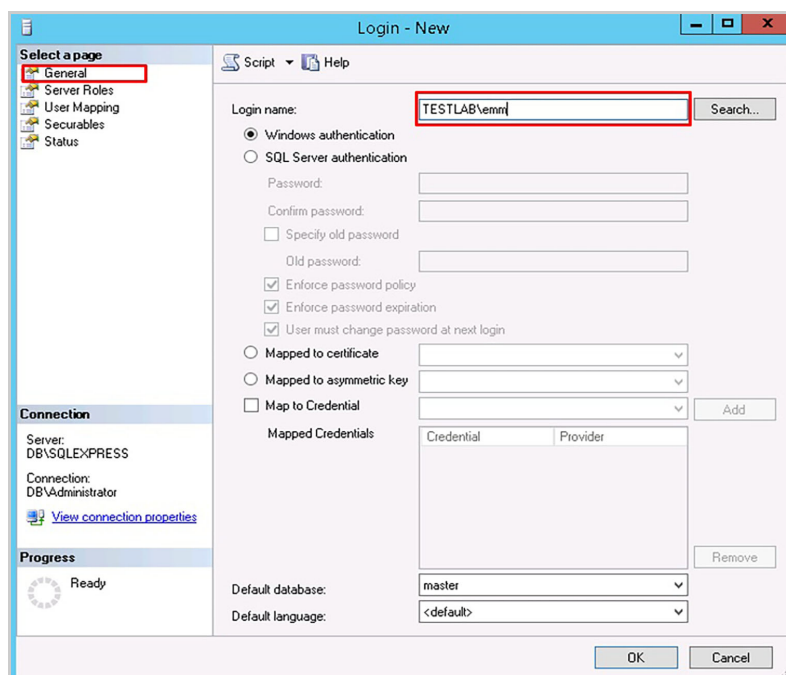
2.3.4 Adding a Windows account and privilege

The following procedure should be performed to create an EMM database using a Windows account as a database authentication method, when installing EMM.

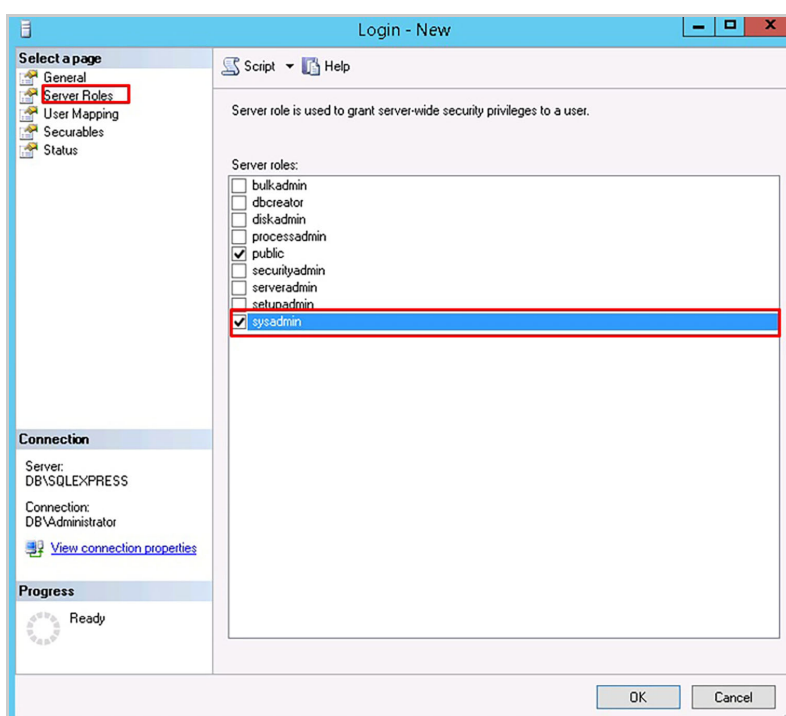
1. Run SQL Server Management Studio and go to **Security > Login** and then, right-click the mouse button and select **New Login**.



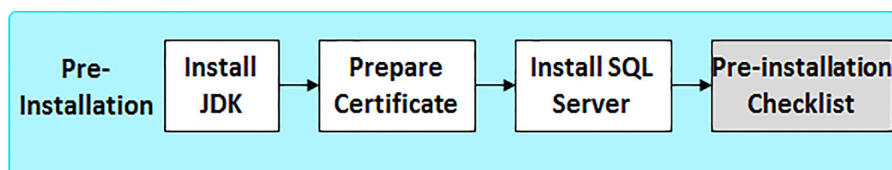
2. Select **General** and input {Domain name}\{account name} in **Login name**.



3. Click **Server Roles** and select the **sysadmin** privilege in the **Server roles** area and then, click **OK**.



2.4 Pre-installation checklist



This chapter specifies what needs to be checked before installing EMM. Before installing the EMM, you must have a domain and certificate and make sure that the firewall access and installation environment files are properly set up. You can find the details of the checklist in the following section.

2.4.1 Single server environment

No	Items to be verified
1	Public domain or URL A domain or URL needs to be accessible on the Internet.
2	EMM server certificate required to have a certificate, in P12 format, with domain name set as common name.
3	APNs certificate required to have APNs certificate issued by Apple to support iOS devices.
4	iOS sign certificate required to have iOS sign certificate to support iOS devices.
5	Java Development Kit required to install JDK in EMM server.
6	Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files required to install JCE policy file in EMM server.
7	Installation environment See " chapter 1.3, EMM installation environment " on page 6.
8	Firewall access rules Inbound traffic from network to EMM should be allowed on port 35443.
9	Firewall access rules Inbound traffic from network to Push should be allowed on port 35000 and 35001.
10	Firewall access rules Inbound traffic from network to EMM should be allowed on port 36000.
11	Firewall access rules Outbound traffic from EMM to CA server should be allowed on port 443.
12	Firewall access rules Outbound traffic from EMM to database should be allowed over TCP/IP (example port 1433).

No	Items to be verified
13	Firewall access rules Outbound traffic from Push to database should be allowed over TCP/IP (example port 1433).
14	Firewall access rules to 3rd party Push <ul style="list-style-type: none"> • Outbound traffic from EMM to gateway.push.apple.com should be allowed over port 2195. • Outbound traffic from Push to android.googleapis.com should be allowed over the port 443,5228, 5229, 5230. • Outbound traffic from Push to login.live.com, *.notify.windows.com, *.wns.windows.com should be allowed over port 443. • Outbound traffic from EMM to Tizen Push should be allowed over port 5223, 8090. For more detail server information, see "List of firewalls to open for Tizen Push" on page 24.
15	Enabling Multi-tenancy Change false for ENABLE of MULTI_TENANCY in the installation environment file (EMM{Version}_H_SETUP.ini).
16	Using features of iOS device Change DOMAIN_NAME in the installation environment file (EMM{Version}_H_SETUP.ini) into the domain of EMM.
17	Using features of Kiosk Wizard Change DOMAIN_NAME in the installation environment file (EMM{Version}_H_SETUP.ini) into the domain of EMM.
18	SQL Server certificate (when installing JDK 1.8) A server certificate for SQL Server is required.

2.4.2 Multi server environment

No	Items to be verified
1	Public domain or URL A domain or URL needs to be accessible on the Internet.
2	EMM server certificate required to have a certificate, in P12 format, with domain name set as common name.
3	Push server certificate required to have a certificate, in P12 format, with domain name set as common name.
4	APNs certificate required to have APNs certificate issued by Apple to support iOS devices.
5	iOS sign certificate required to have iOS sign certificate to support iOS devices.
6	Java Development Kit required to install JDK in servers for EMM, Push, and Push Pproxy.

No	Items to be verified
7	Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files required to install JCE policy file in servers for EMM, Push, and Push Proxy.
8	Installation environment See "chapter 1.3, EMM installation environment" on page 6.
9	Firewall access rules Inbound traffic from network to Web server should be allowed on port 443.
10	Firewall access rules Inbound traffic from network to Push Proxy should be allowed on port 35100 and 35101.
11	Firewall access rules Inbound traffic from network to AppTunnel Relay should be allowed on port 36100.
12	Firewall access rules Inbound traffic from Web server to EMM should be allowed on port 35443.
13	Firewall access rules Outbound traffic from EMM to CA server should be allowed on port 443.
14	Firewall access rules Outbound traffic from Push to Push Proxy should be allowed on port 35110, 35111, and 35113.
15	Firewall access rules Outbound traffic from AppTunnel to AppTunnel Relay should be allowed on port 36110.
16	Firewall access rules Outbound traffic from EMM to database should be allowed over TCP/IP (example port 1433).
17	Firewall access rules Outbound traffic from Push to database should be allowed over TCP/IP (example port 1433).
18	Firewall access rules to 3rd party Push <ul style="list-style-type: none"> • Outbound traffic from Push Proxy to gateway.push.apple.com should be allowed on port 2195. • Outbound traffic from Push Proxy to android.googleapis.com should be allowed over the port 443,5228, 5229, 5230. • Outbound traffic from Push Proxy to login.live.com, *.notify.windows.com, *.wns.windows.com should be allowed over port 443. • Outbound traffic from EMM to Tizen Push should be allowed over port 5223, 8090. For more detail server information, see "List of firewalls to open for Tizen Push" on page 24.
19	Enabling Multi-tenancy Change TRUE for ENABLE of MULTI_TENANCY in the installation environment file (EMM{Version}_H_SETUP.ini).
20	Using features of iOS device Change DOMAIN_NAME in the installation environment file (EMM{Version}_H_SETUP.ini) into the domain of EMM.

No	Items to be verified
21	Using features of Kiosk Wizard Change DOMAIN_NAME in the installation environment file (EMM{Version}_H_SETUP.ini) into the domain of EMM.
23	SQL Server certificate A SQL server certificate (RSA 2048bit) is required.

List of firewalls to open for Tizen Push

When you use Wearable EMM, notification is delivered via Tizen Push. You should open the ports in the EMM server to the following Tizen Push servers to use Tizen Push. You can limit the service area by opening the ports for the applicable region using the corresponding domain or IP addresses.

It is recommended that you open port 5223 in the EMM and Tizen Push server firewall for all open internet networks. If you can only open firewall ports for certain networks, please contact the technical support team.

Note: Please contact the technical support team for a service in the China region.

- Firewalls between EMM and Tizen Push server

Region	Domain	Port	IP List
Europe Americas Southeast Asia	euwest.gateway.push.samsungosp.com useast.gateway.push.samsungosp.com apsoutheast.gateway.push.samsungosp.com	8090	54.77.219.225 54.76.143.44 34.252.157.16 52.30.192.102 52.50.94.13 54.194.121.30
Northeast Asia - Korea - Japan	apkorea.gateway.push.samsungosp.com apnortheast.gateway.push.samsungosp.com	8090	13.112.147.144 52.197.148.5 13.112.185.8 13.113.78.161 52.192.187.3 52.199.246.13
China	apchina.gateway.push.samsungosp.com.cn	8090	52.19.208.212 54.77.55.213 52.16.204.91 52.209.1.80 52.48.132.73 54.154.122.99
Europe Americas Southeast Asia	euwest.gateway.push.samsungosp.com useast.gateway.push.samsungosp.com apsoutheast.gateway.push.samsungosp.com	8090	54.77.219.225 54.76.143.44 34.252.157.16 52.30.192.102 52.50.94.13 54.194.121.30

2.4.3 Notes on post

Checking EMM port

Open the command prompt and enter **netstat** command (`netstat -no | findstr port`) to check the available port.

- For the default port used by EMM, see ["chapter 2.4, Pre-installation checklist" on page 21](#).
- If the default port of EMM has been used for other services, change the value of the port in `EMM{Version}_H_SETUP.ini` before installing. For more details about `EMM{Version}_H_SETUP.ini`, see ["Appendix E, Installation Environment File" on page 154](#).

Checking MS SQL TCP/IP port

To check MS SQL port and set the TCP/IP port, complete the following steps:

1. Check if MS SQL Server is accessible.
 - a. Enter **telnet** command to check whether MS SQL Server is running.

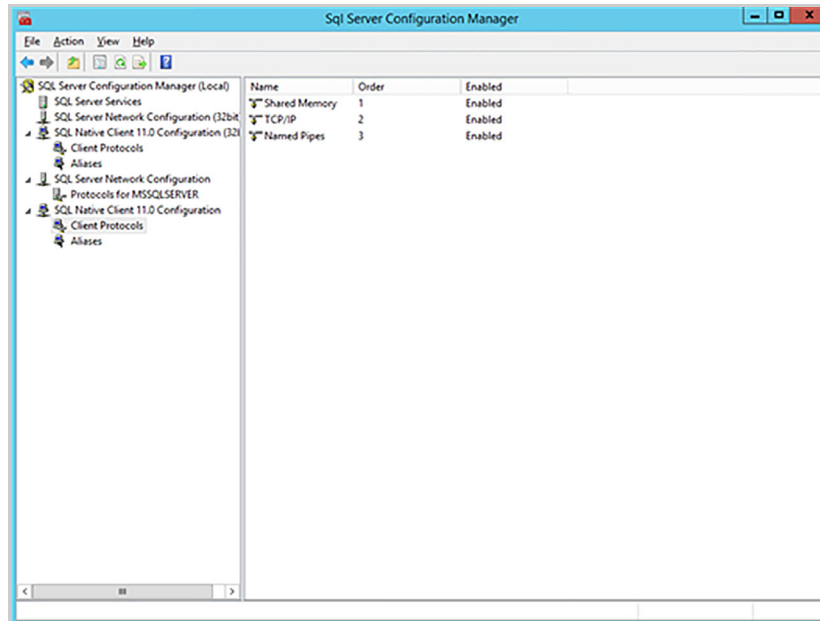
Note: If **telnet** command fails, do as follows.

1. Go to **Server Manager > Dashboard**
 2. Click on **Add roles and features** on Configure this local server tab and there appears "Add Roles and Features Wizard" window.
 3. Check **Telnet Client** in Features stage.
 4. Click on **Install** for Confirmation.
 5. When the installation is completed, click **Close** in Results stage.
-

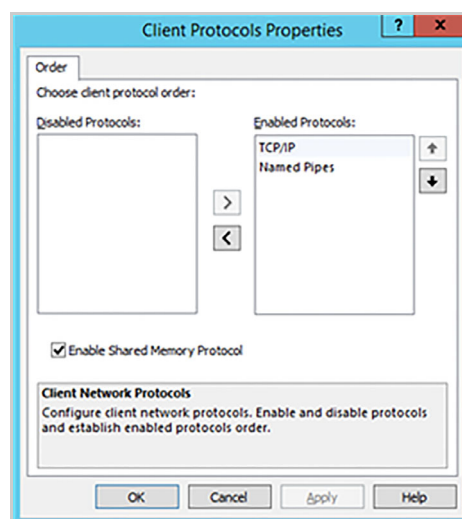
- b. Enter **telnet localhost 1433** command in the command prompt window.
 - If a server is used through localhost or a different port, instead enter following the format `telnet SQL_Server_IP SQL_Server_Port` command.
- c. If a command does not run, check as follows.
 - Check if SQL server is working properly with a person in charge of the server.
 - Contact security person to change firewall settings to add SQL server port.

2. Configure a client to use TCP/IP.
 - a. Expand **SQL Native Client 11.0 Configuration** in the "SQL Server Configuration Manager" window.

b. Right click on **Client Protocols** and click **Properties**.



- c. In the **Enabled Protocols** area, set TCP/IP as the default protocol to access the SQL Server.
- The first one on the list of Enabled Protocols is the default protocol.



3 Installation

This chapter describes how to install Samsung SDS EMM (hereinafter "EMM") in a single-server or multi-server environment. Hereinafter Push is Samsung SDS Push and AppTunnel is Samsung SDS AppTunnel. s

3.1 Installing EMM in a single-server environment

This chapter provides instructions on using EMM installer to install EMM, Push, and AppTunnel. The following descriptions are based on the content of "[chapter 1.2.1, Single server architecture](#)" on page 4.

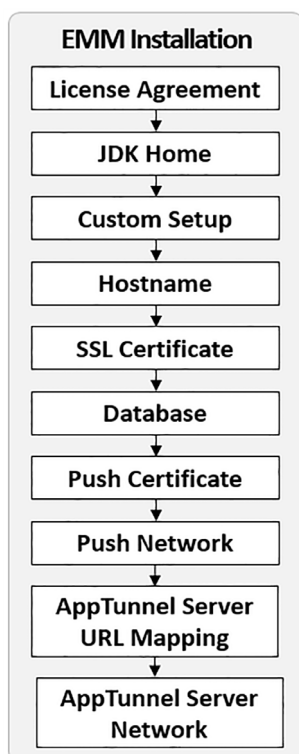
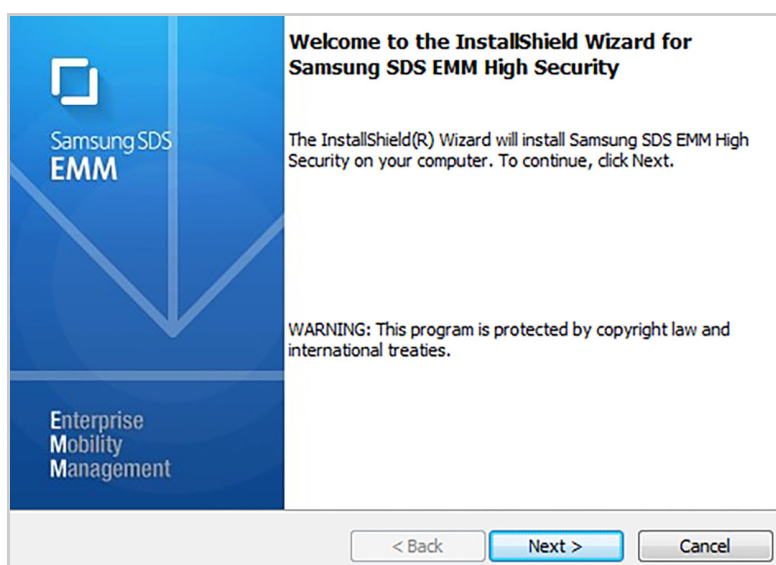


Figure 3-1. Installation steps in a single-server environment

Start EMM installer

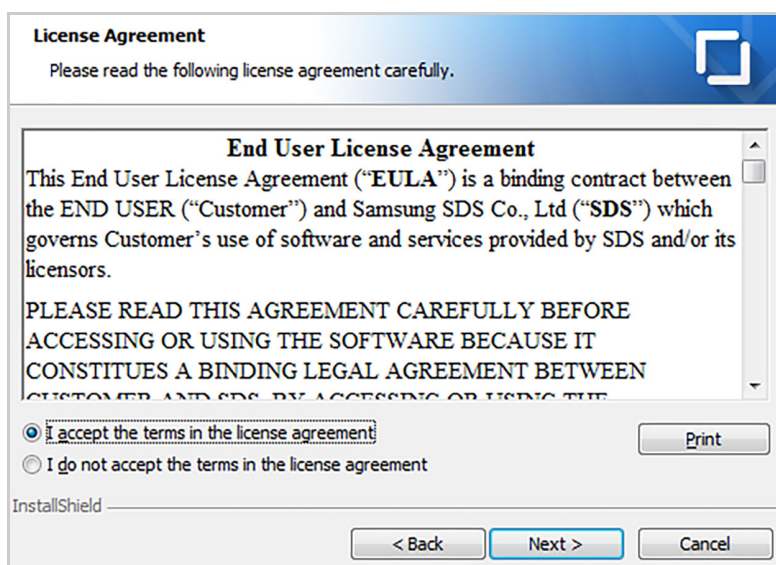
To install EMM, complete the following steps. To stop the installation process, click **Cancel**.

1. Download EMM_Setup_{Version}_H_{Builddate}.zip.
2. Decompress EMM_Setup_{Version}_H_{Builddate}.zip.
3. Run EMM_Setup_{Version}_H_{Builddate}.exe.
 - EMM must be installed using an administrator account.
4. Select a language, then click **OK**.
5. When InstallShield Wizard starts, click **Next** to continue.



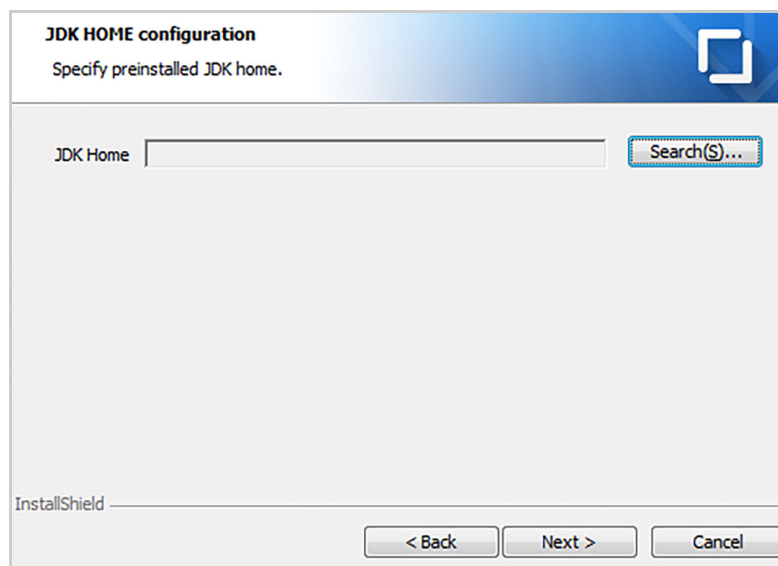
License agreement

6. Read this end user license agreement carefully and check **I accept the terms in the license agreement**. Then, click **Next**.



JDK Home configuration

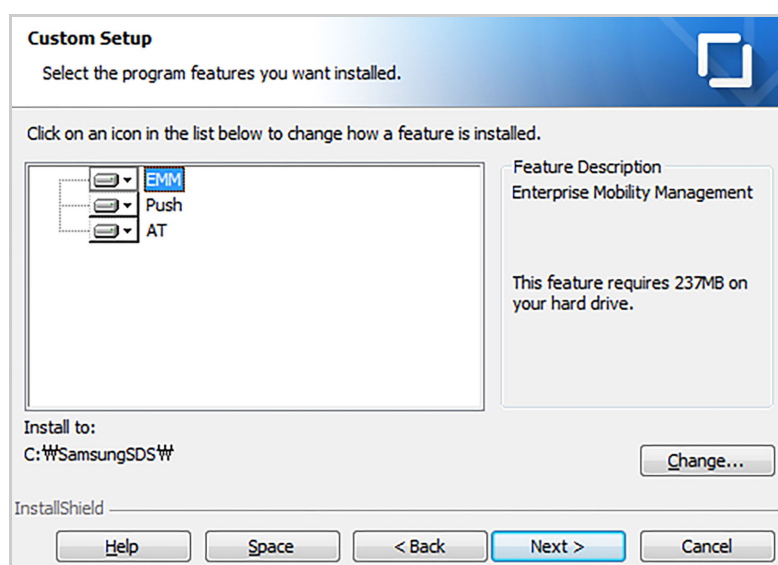
- Set the directory for JDK Home. Click **Search**, and then choose a JDK home directory. Click **Next** to continue.



Note: When the message “The directory is not JAVA directory,” appears, change it to the directory where JDK is installed.

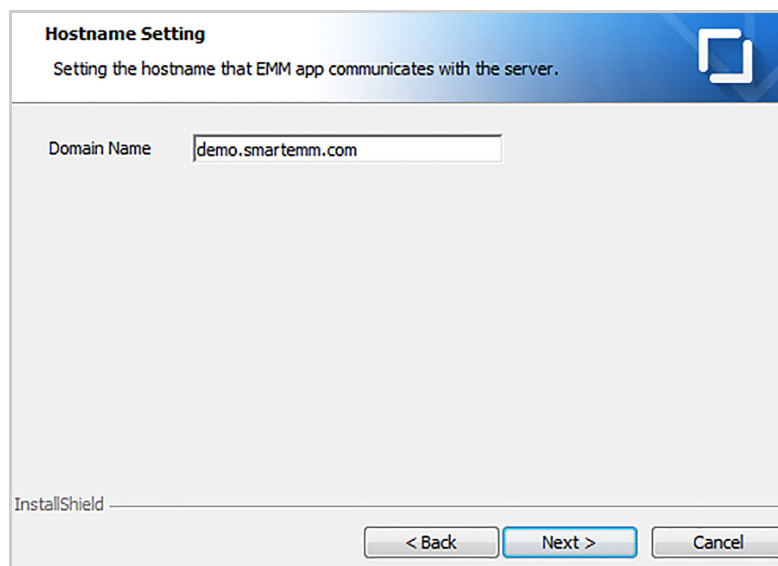
Custom setup

- Choose the directory into which install EMM, and then click **Next** to continue.
 - The default path is C:\SamsungSDS\, and it can be changed.



Hostname setting

9. Enter the domain name to be used by the EMM application to communicate with the EMM server, and then click **Next**.



Hostname Setting
Setting the hostname that EMM app communicates with the server.

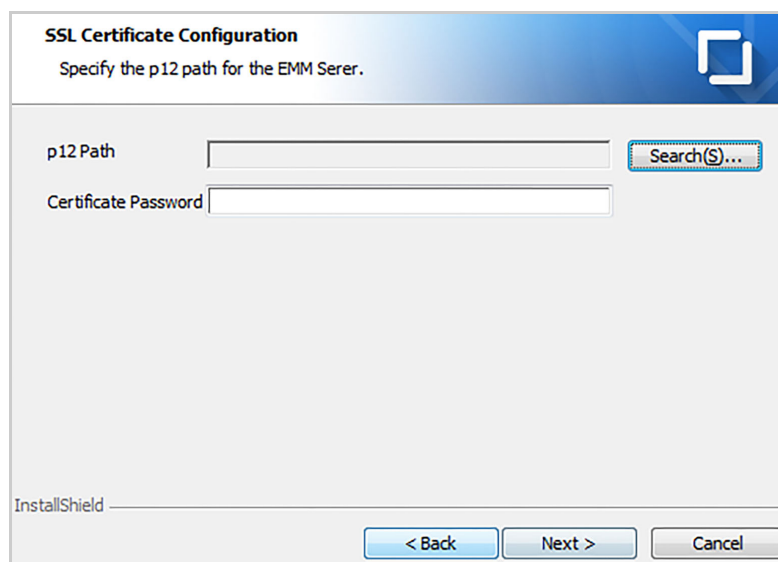
Domain Name

InstallShield

< Back Next > Cancel

SSL Certificate configuration

10. Click **Search**, and then choose the EMM server certificate, issued in "[chapter 2.2, Preparing certificates](#)" on page 10, for the server (P12 file) prepared.
11. Enter the **Certificate password**.
12. Click **Next** to continue.



SSL Certificate Configuration
Specify the p12 path for the EMM Server.

p12 Path Search(S)...

Certificate Password

InstallShield

< Back Next > Cancel

Note: If the extension for the EMM server certificate issued by CA is .PFX, it should be changed to .P12 to install EMM.

Database configuration

13. Select a database type (MSSQL) and an authentication method. The screen capture below shows the settings screen when the MSSQL type Windows authentication method is selected.

Samsung SDS EMM Enterprise Security

Database Configuration
Specify the database settings used by EMM.

Database Type: MSSQL

Authentication: SQL Server Windows

Host: localhost Port: 1433

Instance Name:

DB(Service) Name: EMM230EDB

User: EMM230E

Password: Confirm Password:

***Duplicate User or DB Name could cause errors during installation. So you need to check it out before clicking Next.**

InstallShield

< Back Next > Cancel

14. Enter information requested to use EMM, Push, and AppTunnel database.

Properties	Descriptions
Host	The server address where EMM database will be installed
Port	The TCP/IP port of server where EMM database will be installed
DB(Service) Name	The name of database
User	The ID of users who will access EMM database
Password	The password of users who will access EMM database

15. Click **Next** to continue.

Samsung SDS EMM Enterprise Security

Database Configuration
Specify the database settings used by EMM.

Database Type: MSSQL

Authentication: SQL Server Windows

Host: localhost Port: 1433

Instance Name:

DB(Service) Name: EMM230EDB

User: EMM230E

Password: Confirm Password:

***Duplicate User or DB Name could cause errors during installation. So you need to check it out before clicking Next.**

InstallShield

< Back Next > Cancel

- Note:**
- If Windows authentication has been selected, the administrator account and password input will be disabled.
 - Instance is optional.
 - Since EMM stores operating information after the installation is completed, you must remember users and password.

16. Enter the DB settings configuration information, and the click Next.

- MSSQL settings configuration
 - Select a DB install option.
New Install: install new EMM DB.
No Install: Do not install EMM DB. You can find more details in "[For database installation — Select No Install](#)" on page 50.
 - Enter the database administrator account password in DBA Password. If Windows authentication has been selected, the administrator account and password input will be disabled.
 - If you want to manage the database file and log file separately, check Separate management of DB/Log files.
 - The default destination of database file and log file is C:\Program Files\Microsoft SQL Server\{SQL Version}\MSSQL\DATA\.
 - If SQL server has not been installed, the path should be modified.

MSSQL DB Setting Configuration
Specify the MSSQL DBMS File/DBA settings.

DB Installation: New Install

DBA Account: [Empty text box]

DBA Password: [Empty text box]

Seperate management of DB/Log files

DB File Destination: C:\SamsungSDS\DATAFILES\WEMM\DB.mdf

Log File Destination: C:\SamsungSDS\DATAFILES\WEMM\DB.ldf

* If you do not check for this condition, DB / Log files are created in the default directory of MSSQL DB. If you create a file in a separate folder, please enter the present inputs.

InstallShield

< Back Next > Cancel

17. Click **Next** to continue.

Push Cert configuration

18. Click **Search**, then choose the Push server certificate (P12 file) issued in "chapter 2.2, Preparing certificates" on page 10.
19. Select EC or RSA key algorithm of the certificate from **Push Certificate Key Type** list which Push server uses.
20. Enter the information for the Push certificate.

Properties	Descriptions
Entity Alias	The Alias for the Samsung SDS Push certificate
DN_List	<ul style="list-style-type: none"> • The Common Name (CN) for the Samsung SDS Push certificate. • If the SAN information is set in the certificate, enter the SAN information only. • For the multiple DNs, enter IP address or domain using comma (",") separator without space.
Entity Password	The password for the Samsung SDS Push certificate
Store Password	The password for the Samsung SDS Push certificate key storage

21. Click **Next** to continue.

Note: If the extension of Push server certificate issued by CA is .PEX, it should be changed to .P12 to install EMM.

Push Network configuration

22. Enter the Public IP address or domain of the Push server in **Push External Host** field. For **Push Internal Host**, enter Private IP address of the Push server.
 - **Push External Host** must match the CN on certificate.
 - If the CN of the certificate is domain, enter the domain. If it is IP, enter the IP address.

23. **Proxy Mode** needs to be disabled.
24. Click **Next** to continue.

AppTunnel server URL mapping

25. Enter the URL Mapping information for the AppTunnel server.
 - For **Source URL**, enter the EMM HTTP address accessible from the outside.
 - For **Destination URL**, enter the EMM HTTP address used by the AppTunnel server.
26. Click **Next**.

Note: If users are using an Android N device and setting the source URL, Additional settings are required for the `/config/spring/spring-data-config.xml` file. For more information, see ["Setting the URL Mapping for AppTunnel Servers" on page 47](#).

AppTunnel server network configuration

27. Enter the Public IP or the domain for AppTunnel server in **Server External Host** field.
 - **Server External Host** must match the CN on the certificate.
 - If the certificate CN is the domain, enter the domain. If it is IP, enter the IP address.
28. Disable **Relay Mode**.
29. Click **Install**.

AppTunnel Server Network Configuration
Configure the network variables for the AT-Server component.

Server External Host

Relay Mode

Relay Internal Host

Relay Internal Port

Configure the Host of the AT-Server module for access from the external network, and for communication between AT components. (IP or Domain Name)
For Relay mode, make sure check box is selected and enter IP and Port which will be con...

InstallShield

< Back Install Cancel

Finish EMM installation

30. EMM, Push, and AppTunnel service are automatically registered in the background when **Register for Windows Service** is checked.
31. When the installation process is completed, click **Finish**.

Note: When the message “Some information is missing. Fill in all the blanks.” appears, input the value for all empty fields.

3.2 Installing EMM in a multi-server environment

This chapter illustrates how to use EMM, Push, and AppTunnel installer to install EMM, Push, AppTunnel, Push Proxy, and AppTunnel Relay. The following descriptions are based on the content of "[chapter 1.2.2, Multi server architecture](#)" on page 5.

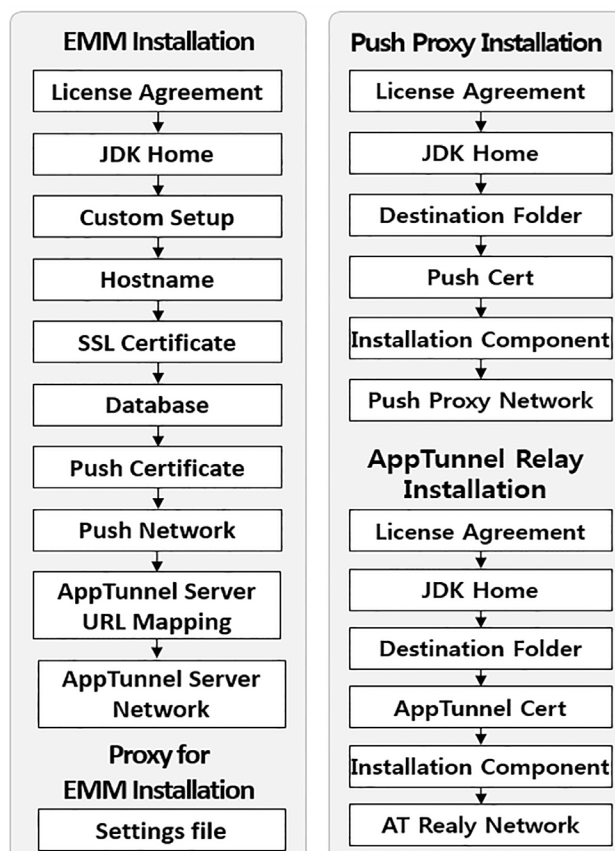


Figure 3-2. Installation steps in a multi-server environment

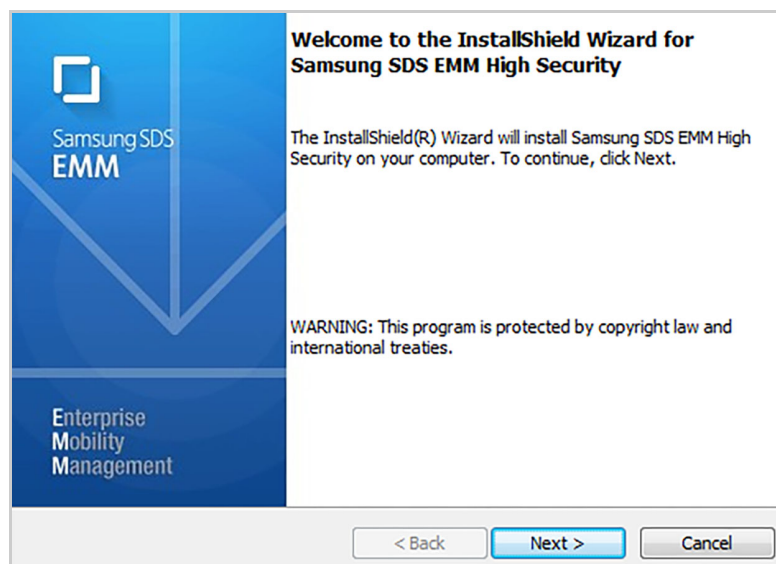
3.2.1 Installing EMM

This chapter provides instructions on using EMM installer to install EMM, Push, and AppTunnel.

Start EMM installer

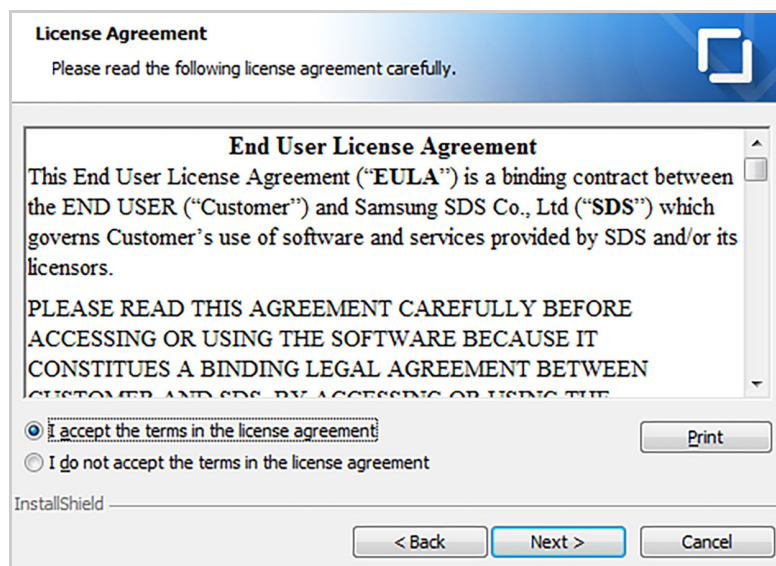
To install EMM, complete the following steps. To stop the installation process, click **Cancel**.

1. Download `EMM_Setup_{Version}_H_{Builddate}.zip`.
2. Decompress `EMM_Setup_{Version}_H_{Builddate}.zip`.
3. Run `EMM_Setup_{Version}_H_{Builddate}.exe`.
 - EMM must be installed using an administrator account.
4. Select a language, then click **OK**.
5. When InstallShield Wizard starts, click **Next** to continue.



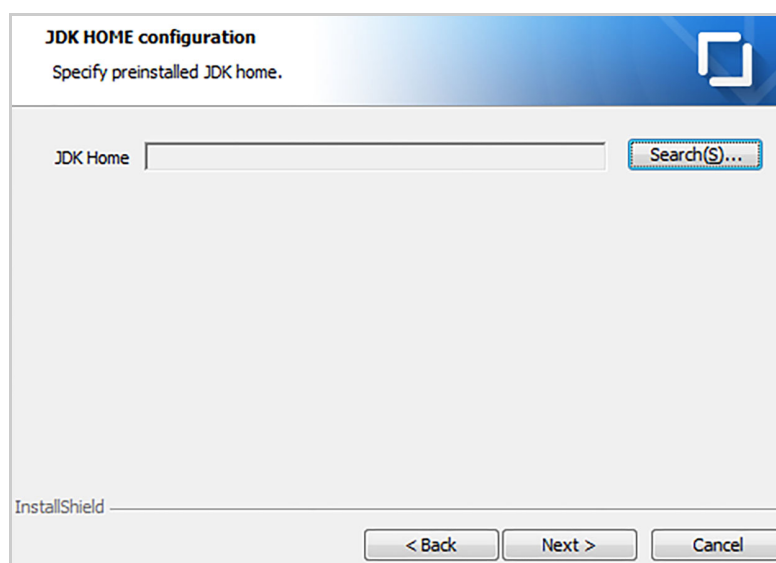
License agreement

6. Read this end user license agreement carefully and check **I accept the terms in the license agreement**. Then, click **Next**.



JDK Home configuration

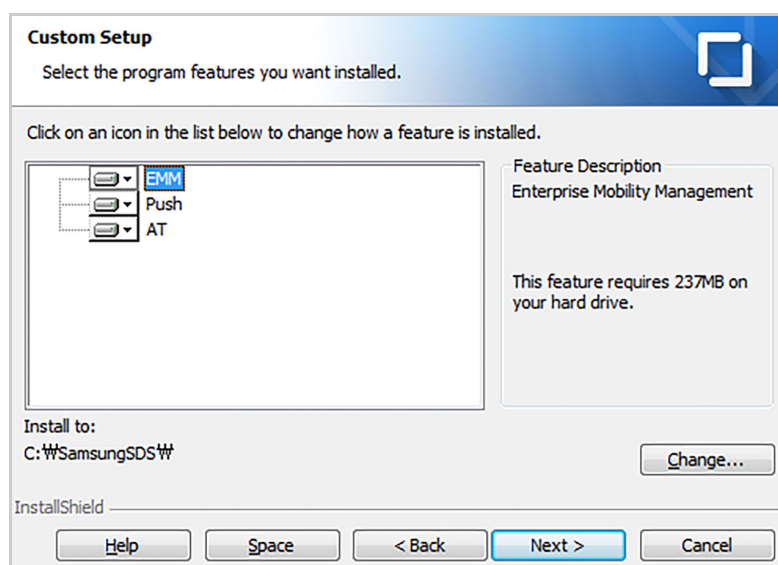
7. Set the directory for JDK Home. Click **Search**, and then choose a JDK home directory. Click **Next** to continue.



Note: When the message “The directory is not JAVA directory,” appears, change it to the directory where JDK is installed.

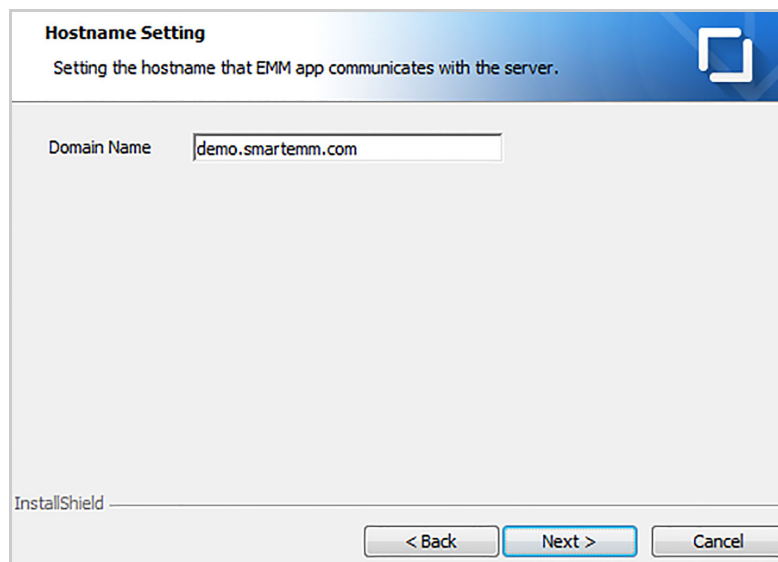
Custom setup

8. Choose the directory into which install EMM, and then click **Next** to continue.
 - The default path is C:\SamsungSDS\, and it can be changed.



Hostname setting

9. Enter the domain name to be used by the EMM application to communicate with the EMM server, and then click **Next**.



SSL Certificate configuration

10. Click **Search**, and then choose the EMM server certificate, issued in "[chapter 2.2, Preparing certificates](#)" on page 10, for the server (.P12 file) prepared.
11. Enter the **Certificate password**.
12. Click **Next** to continue.

SSL Certificate Configuration
Specify the p12 path for the EMM Server.

p12 Path Search(S)...

Certificate Password

InstallShield

< Back Next > Cancel

Note: If the extension of the EMM server certificate issued by CA is .PFX, it should be changed to .P12 to install EMM.

Database configuration

13. Select a database type (MSSQL) and an authentication method. The screen capture below shows the settings screen when the MSSQL type Windows authentication method is selected.

Database Configuration
Specify the database settings used by EMM.

Database Type: MSSQL

Authentication: SQL Server Windows

Host: localhost Port: 1433

Instance Name:

DB(Service) Name: EMM230EDB

User: EMM230E

Password: Confirm Password:

***Duplicate User or DB Name could cause errors during installation. So you need to check it out before clicking Next.**

InstallShield

< Back Next > Cancel

14. Enter information requested to use EMM, Push, and AppTunnel database.

Properties	Descriptions
Host	The server address where EMM database will be installed
Port	The TCP/IP port of server where EMM database will be installed
DB(Service) Name	The name of database
User	The ID of users who will access EMM database
Password	The password of users who will access EMM database

15. Click **Next** to continue.

- Note:**
- If Windows authentication has been selected, the administrator account and password input will be disabled.
 - Instance is optional.
 - Since EMM stores operating information after the installation is completed, you must remember users and password.

16. Enter the DB settings configuration information, and the click Next.

- MSSQL settings configuration
 - Select a DB install option.
 - New Install: install new EMM DB.
 - No Install: Do not install EMM DB. You can find more details in "[For database installation — Select No Install](#)" on page 50.
 - Enter the database administrator account password in DBA Password. If Windows authentication has been selected, the administrator account and password input will be disabled.
 - If you want to manage the database file and log file separately, check Separate management of DB/Log files.

- The default destination of database file and log file is C:\Program Files\Microsoft SQL Server\{SQL Version}\MSSQL\DATA\.
- If SQL server has not been installed, the path should be modified.

17. Click **Next** to continue.

Push Cert configuration

18. Click **Search**, then choose the Push server certificate (P12 file) issued in "[chapter 2.2, Preparing certificates](#)" on page 10.
19. Select EC or RSA key algorithm of the certificate from **Push Certificate Key Type** list which Push server uses.
20. Enter the information for the Push certificate.

Properties	Descriptions
Entity Alias	The Alias of the Samsung SDS Push certificate.
DN_List	<ul style="list-style-type: none"> • The Common Name (CN) of the Samsung SDS Push certificate. • If the SAN information is set in the certificate, enter the SAN information only. • If you are using multi-domain names, separate them by a comma (,) without spaces to enter multiple IP addresses or domains.
Entity Password	The password of the Samsung SDS Push certificate.
Store Password	The password of the Samsung SDS Push certificate key storage.

21. Click **Next** to continue.

Note: If the extension of Push server certificate issued by CA is .PEX, it should be changed to .P12 to install EMM.

Push Network configuration

22. Enter Private IP address of the Push server in **Push External Host** and **Push Internal Host** field.
23. **Proxy Mode** needs to be enabled.
24. Enter Private IP address of the Push Proxy server in **Proxy Internal Host** field. For **Proxy External Host**, enter Public IP or domain of Push Proxy server.
 - **Proxy External Host** must match the CN on certificate.
 - If certificate CN is domain, enter the domain. If it is IP, enter the IP address.
25. Click **Next**.

Note: When you select the **Proxy Mode** check box, you should install Push Proxy with the Push installer. For more detail, see ["chapter 3.2.3, Installing Push Proxy"](#) on page 47.

AppTunnel server URL mapping

26. Enter URL Mapping information for the AppTunnel server.

- For **Source URL**, enter an EMM HTTP address that accessible from outside.
- For **Destination URL**, enter an EMM HTTP address used by the AppTunnel server.

27. Click **Next**.

Note: If users are using an Android N device and setting the source URL, Additional settings are required for the `/config/spring/spring-data-config.xml` file. For more information, see ["Setting the URL Mapping for AppTunnel Servers"](#) on page 47.

AppTunnel server network configuration

28. Enter Public IP or domain of AppTunnel server in **Sever External Host** field.

- **Server External Host** must match the CN on certificate.
- If certificate CN is domain, enter the domain. If it is IP, enter the IP address.

29. **Relay Mode** needs to be enabled.

30. Enter Private IP of AppTunnel server in **Relay Internal Host** field. For **Relay Internal Port** field, enter 36110.

31. Click **Install**.

App Tunnel Server Network Configuration
Configure the network variables for the AT-Server component.

Server External Host

* Configure the host of the AT-Server module for access from the external network (IP or Domain Name).

Relay Mode

Relay Internal Host

Relay Internal Port

* For Relay mode, make sure check box is selected and enter Host(IP or Domain Name) and Port which will be connected for AT service.

InstallShield

< Back Install Cancel

Note: When you select the **Relay Mode** check box, you should install AT Relay with the AppTunnel installer. For more detail, see "[chapter 3.2.4, Installing AppTunnel Relay](#)" on page 48.

Finish EMM installation

32. EMM, Push, and AppTunnel service are automatically registered in the background when **Register for Windows Service** is checked.

33. When the installation process is completed, click **Finish**.

Note: When the message "Some information is missing. Fill in all the blanks." appears, input the value for all empty fields.

Setting the URL Mapping for AppTunnel Servers

If you are using an Android N device, the uppercase letters change to lowercase in the source URL address of the AppTunnel server when called by a client device. In addition, port 80 is removed at the time of URL mapping. Additional settings are required for the `/config/spring/spring-data-config.xml` file as follows:

<p>For example, if the source URL for <code>http://ABC.com</code> includes uppercase letters, add an additional URL in lowercase.</p>	<pre><bean class="com.sds.emm.at.ats.data.vo.UrlMapping"> <property name="sourceUrl" value="http://ABC.com"/> <property name="destinationUrl" value="http://www.bbb.com"/> </bean> <bean class="com.sds.emm.at.ats.data.vo.UrlMapping"> <property name="sourceUrl" value="http://abc.com"/> <property name="destinationUrl" value="http://www.bbb.com"/> </bean></pre>
<p>For example, if the source URL for <code>http://aaa.com:80</code> includes port 80, enter the URL after removing the port. Do not remove any other port except for port 80</p>	<pre><bean class="com.sds.emm.at.ats.data.vo.UrlMapping"> <property name="sourceUrl" value="http://www.aaa.com"/> <property name="destinationUrl" value="http://www.bbb.com"/> </bean></pre>
<p>For example, if the source URL for <code>http://www.ABC.com:80</code> includes both uppercase letters and port 80, add an additional URL in lowercase without port 80.</p>	<pre><bean class="com.sds.emm.at.ats.data.vo.UrlMapping"> <property name="sourceUrl" value="http://www.ABC.Com"/> <property name="destinationUrl" value="http://www.bbb.com"/> </bean> <bean class="com.sds.emm.at.ats.data.vo.UrlMapping"> <property name="sourceUrl" value="http://www.abc.Com"/> <property name="destinationUrl" value="http://www.bbb.com"/> </bean></pre>

3.2.2 Installing web server

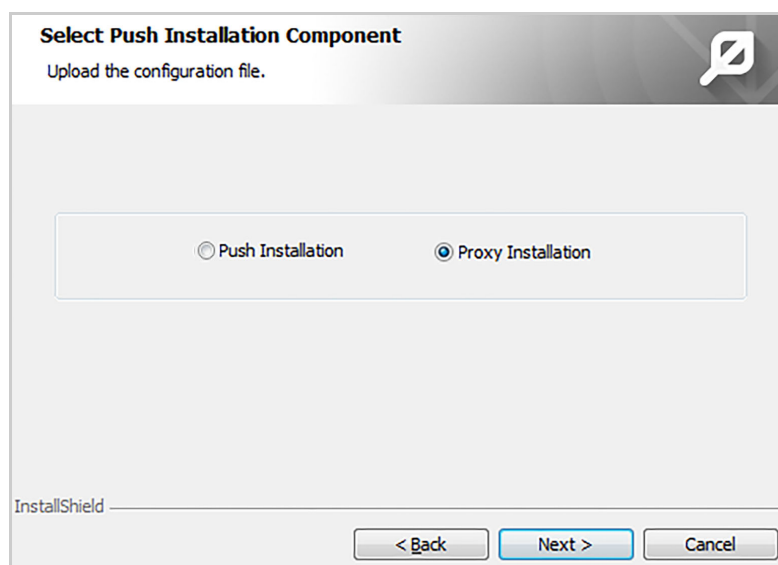
EMM can be linked with the both web servers, Apache or IIS (Internet Information Services) created by Microsoft. But the Apache and IIS products have not been evaluated by SDS for CC certification.

3.2.3 Installing Push Proxy

Install Push Proxy using Push installer. Please see the information about the process except for the steps below in the chapter that explain Installing of Push in the *Samsung SDS Push Installation Guide*.

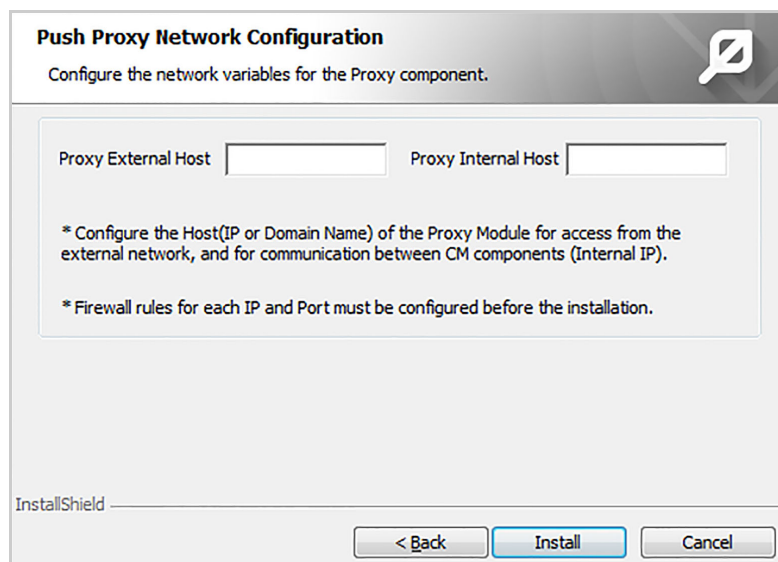
Push Installation Component

1. Select **Proxy Installation**.
2. Click **Next**.



Push Proxy Network configuration

3. Enter Public IP address or domain of Push Proxy for **Proxy External Host** and enter Private IP address of Push Proxy for **Proxy Internal Host**.
4. Click **Install**.

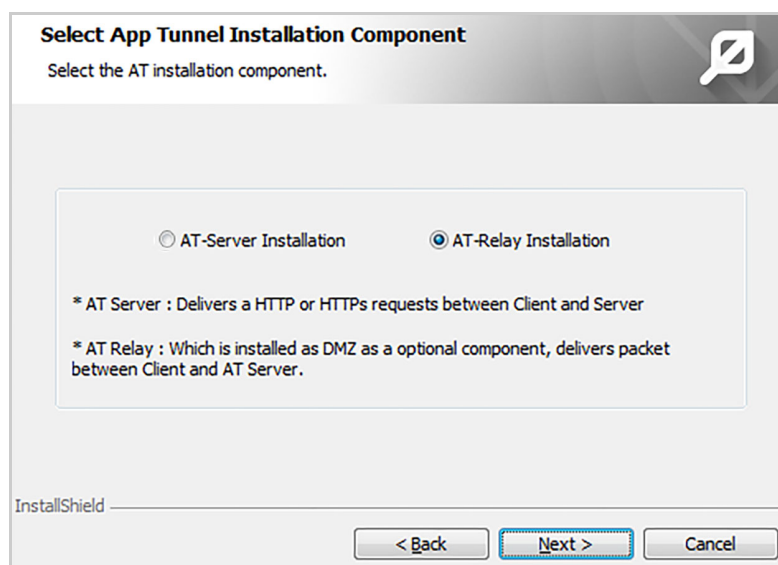


3.2.4 Installing AppTunnel Relay

Install AppTunnel Relay using AppTunnel installer. Please see the information about the process except for the steps below in the chapter that explain Installing AppTunnel in the *Samsung SDS AppTunnel Installation Guide*.

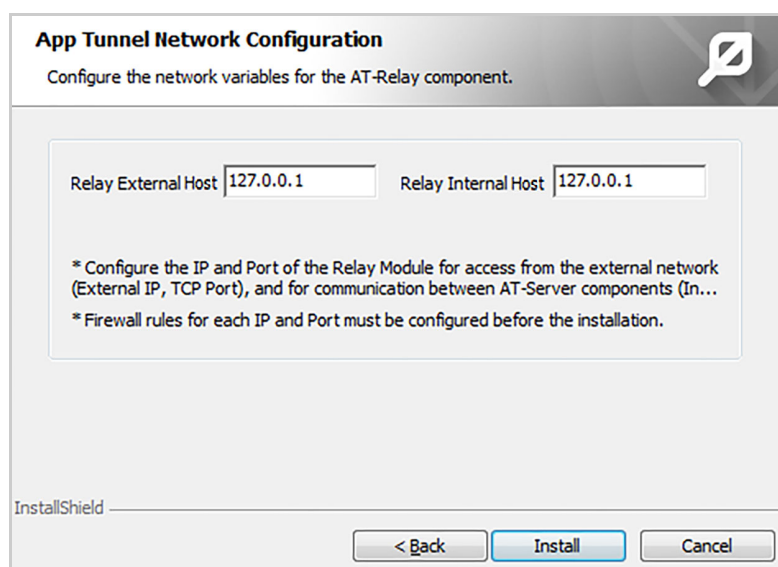
AppTunnel Installation Component

1. Select **AT-Relay Installation**.
2. Click **Next**.



AppTunnel Relay Network configuration

3. Enter the Public IP address or domain of the AppTunnel server for **Relay External Host** and enter Private IP address for the AppTunnel server for **Relay Internal Host**.
4. Click **Install**.



3.3 Notes on post - Installation phase

This chapter describes items that need to be manually set, as needed, before starting EMM installation.

For database installation — Select No Install

When you select **No Install**, Only EMM applications are installed. In this case, EMM DB should be installed manually following the steps below.

- Execution directory: {EMM installation location}
`\EMM\{Version}\war\db\script\{DBMS}`
- Run scripts in the following order:
 - 01.emm_user_script.sql
 - 02.emm_db_schema_metadata_script.sql
 - If Korean or Chinese are used, run the following scripts.
 - Korean: 02-1.emm_meta_data_ko.sql
 - Chinese: 02-2.emm_meta_data_zh.sql
 - If EMM system is on-premise (single tenant), run the following scripts.
 - 02-3.emm_single_tenant_data.sql
 - 02-4.emm_single_tenant_proc_script.sql

Execute the Push script below to install the database manually.

- Execution directory: {EMM installation location}
`\Push\PushConfig\PushQuery\{DBMS}\CREATE`
- Run these scripts:
 - 03.push_core.sql
 - 04.push_sa.sql
- Execution directory: {EMM installation location}
`\Push\PushConfig\PushQuery\{DBMS}\CREATE`
- Run these scripts:
 - 01.CORE_INIT.SQL
 - 02.SA_INIT.SQL

Setting interval between Push SA registration monitoring

To manually set an interval for when Push SA registration monitoring recurs, complete the following steps. The EMM server checks a new tenant based on the time interval specified.

1. Go to {EMM installation location}\EMM\{Version}\war\WEB-INF\classes\spring.
2. Use an editor to implement `context-task.xml`

3. Go to `periodforRegister` properties to change **value**.

```
<property name = "periodForResigter"><value>30</value></property>
```

- The interval is set to 30 minutes by default. If you want to change this, note that it should be more than 1 minute.

Note: A tenant newly registered during the specified time for Push SA registration monitoring is not registered on the EMM server.

4 Post-installation

This chapter guides you in checking the running status for Samsung SDS EMM (hereinafter "EMM") after installation is finished. Here are the steps That should be followed after installation. Push is Samsung SDS Push and AppTunnel is Samsung SDS AppTunnel.

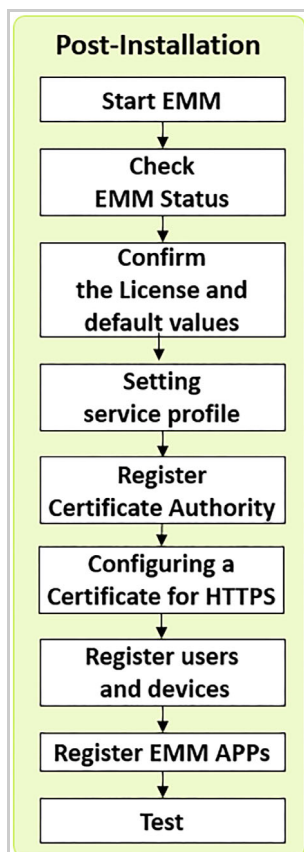


Figure 4-1. EMM Post-Installation Steps

4.1 Starting EMM

EMM runs in 2 different ways: Foreground and Background.

Note: The Push ICM module provides a TLS channel for message exchange between physically separated servers. This service runs when the Push is installed on a separate server to provide high availability.

4.1.1 Single-server environment

Running EMM as foreground service

1. Go to **Apps > Samsung SDS**.
2. Execute the following services in the order.
 - a. Push DCM Start
 - b. Push ECM Start
 - c. Push PS Start
 - d. Push SCM Start
 - e. Push ICM Start
 - f. AT Server Start
 - g. EMM Server Start

Running EMM as background service

If **Register for Windows service** is checked after EMM installation is completed, skip 1 to 4 steps.

1. Go to the {EMM installation location}
\EMM\{Version}\apache-tomcat-8.0.39\bin directory.
2. Run `emm_service_install.bat`.
 - `emm_service_install.bat` must be run using an administrator.
3. Go to the {EMM installation location}\AT\{Version}\bin directory.
4. Run `install_at_server_win_service.bat`.
 - `install_at_server_win_service.bat` must be run using administrator account.
5. Go to **Start > Administrative Tools > Services**, and then check the following services.
 - Samsung SDS AT{Version} Server Background Service (AppTunnel Server)
 - Samsung SDS EMM{Version} Server Background Service (EMM Server)
 - Samsung SDS Push{Version} DCM(1) Background Service (Push DCM)
 - Samsung SDS Push{Version} ECM(1) Background Service (Push ECM)
 - Samsung SDS Push{Version} PS(1) Background Service (Push PS)

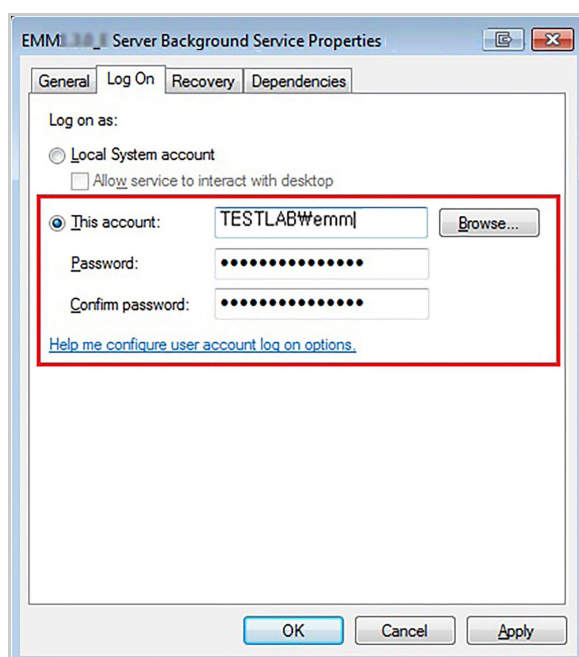
- Samsung SDS Push{Version} SCM(1) Background Service (Push SCM)
 - Samsung SDS Push{Version} ICM(1) Background Service (Push ICM)
6. The log on information should be set in the upper Windows service list, if a Windows account is set as a database authentication method, when installing EMM. For more information, see "[Setting the Windows service log on](#)" on [page 54](#).
 7. Select the service and right click, then click **Start**.
 - Execute the services in order.

- Note:**
- Depending on the level of authority given to the service account, EMM server should be operated as a Windows background service.
 - EMM service is automatically (delay start) registered. The minimum delay time for service startup is 3 minutes.

Setting the Windows service log on

The log on information for each Windows service should be set when installing EMM, if the EMM DB is set with the Windows privilege.


1. Select **Start > Administrative Tools > Services** menu and the EMM-related Windows service. Right click the mouse button and select **Properties**.
 - Samsung SDS AT{Version} Server Background Service (AppTunnel Server)
 - Samsung SDS EMM{Version} Server Background Service (EMM Server)
 - Samsung SDS Push{Version} DCM(1) Background Service (Push DCM)
 - Samsung SDS Push{Version} ECM(1) Background Service (Push ECM)
 - Samsung SDS Push{Version} PS(1) Background Service (Push PS)
 - Samsung SDS Push{Version} SCM(1) Background Service (Push SCM)
 - Samsung SDS Push{Version} ICM(1) Background Service (Push ICM)
2. Select **This account** and input the domain account and password and then, click **OK**.



4.1.2 Multi-server environment

The explanation below is based on figure 1-5 in "[chapter 1.2.2, Multi server architecture](#)" on page 5.

Running EMM as foreground service

1. Go to the server on which EMM was installed.
2. Go to **Apps > Samsung SDS** to run the following services in order.
 - a. Push DCM Start
 - b. Push ECM Start
 - c. Push PS Start
 - d. Push SCM Start
 - e. Push ICM Start
 - f. AT Server Start
 - g. EMM Server Start
3. Go to the web server.
4. Register for Apache service.
 - a. Open a command prompt with the `{Apache24forEMM installation location}\bin\` directory.
 - b. Enter `httpd -k install {Web server name}` command.
5. Click `ApacheMonitor.exe` in bin directory and click  on the right side of taskbar to check the status.
6. Go to `{Push Proxy installation location}\PushProxy\{Version}\bin` and run the following files in order.
 - a. `push_dpp_1_start.bat`
 - b. `push_epp_1_start.bat`
 - c. `push_ppp_1_start.bat`
7. Go to `{AppTunnel Relay installation location}\AT\{Version}\at-relay\bin` to run `at_realay_start.bat` file.

Running EMM as background service

If **Register for Windows service** is checked after EMM installation is completed, skip 1 to 5 steps.

1. Go to the server in which EMM was installed.
2. Go to the `{EMM installation location}\EMM\{Version}\apache-tomcat-8.0.39\bin` directory.
3. Run `emm_service_install.bat` file.
 - `emm_service_install.bat` must be run using an administrator.
4. Go to the `{EMM installation location}\AT\{Version}\bin` directory.
5. Run `install_at_server_win_service.bat` file.

- `install_at_server_win_service.bat` file must be run using administrator account.
6. Go to the web server and register for Apache service.
 - a. Open a command prompt with the `{Apache24forEMM installation location}\bin\` directory.
 - b. Enter `httpd -k install {Web server name}` command.
 7. Go to `{Push Proxy installation location}\PushProxy\{Version}\bin` directory.
 8. Run `install_push_proxy_win_service.bat` file.
 - `install_push_proxy_win_service.bat` must be run using administrator account.
 9. Go to `{AppTunnel Relay installation location}\AT\{Version}\at-relay\bin` directory.
 10. Run `install_at_relay_win_service.bat` file.
 - `install_at_relay_win_service.bat` file must be run using administrator account.
 11. Go to **Start > Administrative Tools > Services**, and then check the following services.

Server	Service
Server with EMM	Samsung SDS Push{Version} DCM(1) Background Service
	Samsung SDS Push{Version} ECM(1) Background Service
	Samsung SDS Push{Version} PS(1) Background Service
	Samsung SDS Push{Version} SCM(1) Background Service
	Samsung SDS Push{Version} ICM(1) Background Service
	Samsung SDS AT{Version} Server Background Service
	Samsung SDS EMM{Version} Server Background Service
Web server	Samsung SDS PushProxy{Version} DPP(1) Background Service
	Samsung SDS PushProxy{Version} EPP(1) Background Service
	Samsung SDS PushProxy{Version} PPP(1) Background Service
	Samsung SDS AT{Version} Relay Background Service

12. The log on information should be set in the upper Windows service list, if a Windows account is set as a database authentication method, when installing EMM. For more information, see ["Setting the Windows service log on" on page 54](#).
13. Select the service and right click, then click **Start**.
 - Execute the services in the order.

Note:

- Depending on the level of authority given to service account, the EMM server should operate as Windows background service.
- EMM service is automatically (delay start) registered. The minimum delay time for the service startup is 3 minutes.

4.2 Checking EMM status

This chapter describes how to check if the port and firewall used by EMM are open after installation.

Checking EMM ports

Check whether the port is used with `netstat` commands (`netstat -no | findstr port number`) in the command prompt. If the `netstat` command is not working, check the log of the server not responding in the `{Installation location}\{Service}\{Version}\log` directory.

- For the port used for EMM, see the "[chapter 2.4, Pre-installation checklist](#)" on [page 21](#).

Server	Service	Log	Notes
Server with EMM	EMM	emm.log	
	Push PS	ps_{Service start date}.log	
	Push DCM	dcm_{Service start date}.log	
	Push SCM	scm_{Service start date}.log	
	Push ECM	ecm_{Service start date}.log	
	Push ICM	icm_{Service start date}.log	
	AppTunnel	at_{Service start date}.log	
Web server	Push Proxy PPP	ppp_{Service start date}.log	Multi-server environment only
	Push Proxy DPP	dpp_{Service start date}.log	
	Push Proxy EPP	epp_{Service start date}.log	
	AppTunnel Relay	at_{Service start date}.log	

Check if firewall is open

Check if other PCs can use telnet commands to access the inbound release port. See "[chapter 2.4, Pre-installation checklist](#)" on [page 21](#) for firewall access rule.

For example, telnet **{EMM Server IP}** 35080

- Contact the person in charge of the firewall If there is no response to the command.

4.3 Confirming the EMM license

Since EMM works with a demo license at first, only limited functions are available. Before using EMM, the issued license must be registered. To register the license, complete the follow steps. For more information about confirming the EMM license in the chapter that explain Registering license in the *Samsung SDS EMM Administrator's Guide*.

License Detail

EMM_LICENSE	Company Name	EMM (Demo)	Maximum numbers of devices	100 (Registered Devices : 42)
Product Key -	License Version	v1.5.1	Maximum number of API Client	10
EMM -	Security Level	HIGH	SecuCamera Count	10 (Activated SecuCameras : 2)
	Access Period	2020-10-23~2021-12-31	Visitor	Do not use
	Single Product	UMP,APPTUNNEL	Knox Portal for Mobile	Do not use
	Connector	DB,REST,WS	Samsung Group	Do not use

- Log in to EMM Admin Portal.
 - The address of EMM Admin Portal:
 - Single-server: https://EMM server IP address or domain:port/emm
 - Multi-server: https://IP address or domain of Web server:port/emm
 - The default user ID and password are admin.
- Go to **Setting > License** and click the license to see the details.
- Check **Access Period**, **Security Level**, and **Single Product** of the license that appears at the top of the "License Detail" page.
 - If the license validity terms and product options do not match, contact the license issuer.
- Select the EMM license from the list, click the **Modify** button, enter the License key value, and click **Save**.

- Note:**
- TMS manages license in Multi-Tenant mode; therefore, EMM does not show the menu in Multi-Tenant mode. In Multi-Tenant mode, TMS manages license registration and management in the TMS server. For more information, see the *Samsung SDS TMS Administrator's Guide*.
 - If you use KPE-Premium, go to **Setting > License**, click the **Add** button, and enter the value of license in the **License Key** field. For the Knox license, contact the sales manager.

4.4 Setting the service profile

The service profile is service information downloaded from the EMM server to the user device when the device is provisioned. The service profile manages values such as EMM Server, EMM Client, Push server, AppTunnel server, App store, Audit Server, Log Server and MDM Server.

4.4.1 Single-server environment

To set the service profile for single-server, complete the following steps.

1. Go to **Setting > Server > Configuration** in the EMM Admin Portal.
2. Click **Service profile**.
3. Change the following values according to the installation environment.
 - EMM server domain: Public IP or domain
 - HTTPS/HTTP port of EMM server: e.g. 35080
 - Push server domain: Public IP or domain.
 - TCP port of Push server: e.g. 35000
 - AppTunnel server domain: Public IP or domain.
 - HTTP port of AppTunnel server: e.g. 36000
 - See the ["Appendix C, Audit Remote Logging"](#) on page 110 for transferring Audit logs to the remote log server or for sending the audit log files to an external server.

Profile category	Item	The value to be changed
EMM Server	Protocol Type to Access EMM Server	http
	EMM Server Host	EMM server domain
	EMM Server Port	35080
	EMM Server Context	emm
	Request Timeout(ms)	30000
	Compression upon request (TRUE/FALSE)	FALSE
	Request Data Type	XML
	Protocol Type to Access Cert Server	https
	Cert Server Host	EMM server domain
	Cert Server Port	35443
	Cert Server Context	emm
	Protocol Type to Access Provision Server	https
	Provision Server Host	EMM server domain
	Provision Server Port	35443

Profile category	Item	The value to be changed
EMM Client	URL for EMM packages distribution	https://EMM server domain:35443/emm/ws/appFileDown/getEMMInstallJson
Push	AppTunnel Host	EMM server domain
	AppTunnel Port	36000
	Push Master PS Host	EMM server domain
	Push Master PS Port	35000
	Push Slave PS Host	EMM server domain
	Push Slave PS Port	35000
App Store	App Store Access URL	https://EMM server domain:35443/emm/mobile/bas.do
Audit Server	Protocol Type to Access Audit Server	https
	Audit Server Host	EMM server domain
	Audit Server Port	35443
	Audit Server Context	Its
	Audit Server Access Timeout(ms)	30000
	AuditLog File Size for Automatic Upload (unit:byte)	10240 The size of the log file automatically uploaded to the server from the device
Log Server	Protocol Type to Access Log Server	https
	Log Server Host	EMM server domain
	Log Server Port	35443
	Log Server Context	Its
	Log Server Access Timeout(ms)	30000
	Log File Storage Period(unit:day)	7
	Log File Size Limit(unit:byte)	10485760

Profile category	Item	The value to be changed
MDM	EMM Agent Download URL	https://EMM server domain :35443/emm/down/file/EMMAgent.apk
	Push Agent Download URL	https://EMM server domain :35443/emm/down/file/Samsung SDS-Push-Agent.apk
	MDM Enrollment URL for iOS	https://EMM server domain :35443/emm
	Client Download URL after Factory Reset	https://EMM server domain :35443/emm/down/file/EMMClient.apk
	Client-signature for validation after factory reset	Signature value that are extracted from the EMM Client.
	Client package name for validating installation after factory reset	com.sds.emm.client

4.4.2 Multi-server environment

To set the service profile for multi-server, complete the following steps.

1. Go to **Setting > Service > Configuration**.
2. Click **Service profile**.
3. Change the following values according to the installation environment.
 - Domain of EMM server: Public IP or domain of Web server
 - HTTPS/HTTP port of EMM server: e.g. 443
 - Domain of Push Proxy server: Public IP or domain of Push Proxy server.
 - TCP port of Push Proxy PPP: e.g. 35100
 - Domain of AppTunnel Relay server: Public IP or domain of Push Proxy server.
 - TCP port of AppTunnel Relay server: e.g. 36110
 - See the "[Appendix C, Audit Remote Logging](#)" on page 110 for transferring Audit logs to the remote log server or for sending the audit log files to an external server.

Profile category	Item	The value to be changed
EMM Server	Protocol Type to Access EMM Server	http
	EMM Server Host	EMM server domain
	EMM Server Port	443
	EMM Server Context	emm
	Request Timeout(ms)	30000
	Compression upon request(TRUE/FALSE)	FALSE
	Request Data Type	XML
	Protocol Type to Access Cert Server	https
	Cert Server Host	EMM server domain
	Cert Server Port	443
	Cert Server Context	emm
	Protocol Type to Access Provision Server	https
	Provision Server Host	EMM server domain
Provision Server Port	443	
EMM Client	URL for EMM packages distribution	https://EMM server domain :443/emm/ws/appFileDown/get EMMInstallJson
Push	AppTunnel Host	EMM server domain
	AppTunnel Port	36000
	Push Master PS Host	EMM server domain
	Push Master PS Port	35000
	Push Slave PS Host	EMM server domain
	Push Slave PS Port	35000
App Store	App Store Access URL	https://EMM server domain:443/emm/mobile/bas.do
Audit Server	Protocol Type to Access Audit Server	https
	Audit Server Host	EMM server domain
	Audit Server Port	443
	Audit Server Context	Its
	Audit Server Access Timeout(ms)	30000
	AuditLog File Size for Automatic Upload (unit:byte)	10240 The size of the log file automatically uploaded to the server from the device

Profile category	Item	The value to be changed
Log Server	Protocol Type to Access Log Server	https
	Log Server Host	EMM server domain
	Log Server Port	35443
	Log Server Context	Its
	Log Server Access Timeout(ms)	30000
	Log File Storage Period(unit:day)	3
	Log File Size Limit(unit:byte)	1048576
MDM	EMM Agent Download URL	https://EMM server domain:443 /emm/down/file/EMMAgent.apk
	Push Agent Download URL	https://EMM server domain :443/emm/down/file/Samsung SDS-Push-Agent.apk
	MDM Enrollment URL for iOS	https://EMM server domain :443/emm
	Client Download URL after Factory Reset	https://EMM server domain :443/emm/down/file/EMMClient. apk
	Client-signature for validation after factory reset	
	Client package name for validating installation after factory reset	com.sds.emm.client

Note: The domain name of server URL is automatically entered as the Public IP of EMM server in installation setup file (EMM{Version}_H_SETUP.ini). For more details, see "[Appendix E, Installation Environment File](#)" on page 154.

4.5 Registering certificate authority

The CA server information needs to be registered in the EMM Admin Portal to implement TLS communication between the EMM server and the device. For more information about registering CA, see the chapter that explains Managing certificate in the *Samsung SDS EMM Administrator's Guide*.

4.6 Configuring a certificate for HTTPS

When the EMM is enrolled on a device, the device connects the EMM server by HTTPS or HTTP communications for DN (Distinguish Name) authentication of the device certificate. For connection by HTTPS, the Root CA and DN of EMM server must be authenticated. To authenticate a certificate, DN information must be configured. The instruction to configure a certificate is as below.

Adding or changing a Root certificate of the EMM server

When HTTPS communications are done by a self-signed certificate on the Push, AppTunnel, or EMM servers, or the certificates unregistered on the JAVA cacerts are used, you must add a Root certificate. Also when the certificate of Trust Store expired or was reissued, you must change the Root certificate. The cacerts file provided by JAVA is formed by JKS. So you must convert it into a P12 file and then convert into FIPS Compliant certificate.

The essential prerequisites of the certificate are as below:

- Trust Store requires P12 file format and FIPS Compliant.
- Password for P12 file in Trust Store should be "changeit."

You must set the following server certificates that communicate with devices:

Service	Configuration	Target certificate
Push	Proxy mode	a certificate of each Push Proxy server
	Non-Proxy mode	a certificate of each Push server
AppTunnel	Relay mode	a certificate of each AppTunnel Relay server
	Non-Relay mode	a certificate of each AppTunnel server

To add or change a root certificate, complete the following steps.

1. Backup `{PUSH_HOME}\resources\cacerts180.p12` file:
The `cacerts180.p12` is the converted file from the `cacerts` file into a P12 type and FIPS compliant certificate.
2. Import the Root certificate of EMM server into `{JAVA_HOME}\jre\lib\security\cacerts`. At command window, enter as below. Password should be "changeit."

- **YYY**: Any alias unduplicated with an alias of the existing cacerts certificate
- **XXX.cer**: The Root certificate of EMM server

```
keytool -import -alias YYY -file XXX.cer -keystore
{JAVA_HOME}\jre\lib\security\cacerts
```

3. Copy {JAVA_HOME}\jre\lib\security\cacerts file into {PUSH_HOME}\resources\cacerts.
4. Convert {PUSH_HOME}\resources\cacerts file as type of JKS into PKCS12 type. The conversion scripts are as below.

```
keytool -importkeystore -srckeystore
{PUSH_HOME}/resources/cacerts
-srcstoretype JKS -deststoretype PKCS12 -destkeystore
{PUSH_HOME}/resources/cacerts.p12
```

5. Convert {PUSH_HOME}\resources\cacerts.p12 file into the FIPS compliant certificate with the converter provided.

-
- Note:**
- The provided FIPS conversion tool was changed. You must convert a certificate by using the changed conversion tool. The `Fips140Converter.jar` file date of the latest conversion tool is July 24, 2015.
 - The FIPS conversion tool must be run in a JAVA environment where the EMC Crypto module (Tomcat RSA patch) is patched.
-

6. Modify a file name `cacerts.p12` in {PUSH_HOME}\resources directory into `cacerts180.p12`.
7. Copy a `cacerts180.p12` certificate to each server directory based on EMM configuration.
 - Push Proxy: {PushProxy_HOME}\resources
 - AppTunnel: {ATS_HOME}\resources
 - AppTunnel Relay: {ATR_HOME}\resources

4.7 Registering users and devices

Register the users and devices to use EMM in the Admin Portal. For more information, see *Samsung SDS EMM Administrator's Guide*.

4.8 Registering EMM apps

The EMM service is available on a device only with the EMM application registered in the EMM Admin Portal. For more information about registering EMM applications, see *Samsung SDS EMM Administrator's Guide*.

1. Download APK files (EMM Agent, EMM Client, and Push) and IPA files (EMM Client for iOS) officially released.
2. Log in to EMM Admin Portal.
3. Go to **Setting > EMM Application and Policy > EMM Application**.
4. Click **Add** on the top of the page.
5. Add APK files and IPA files according to the category.
 - **Agent:** Samsung SDS EMM Agent.apk
 - **Client:** Samsung SDS EMM Client.ipa
 - In case of using separate packages for EMM Client and Agent, Samsung SDS EMM Client.apk for Android should be registered.
 - **Push Agent:** Samsung SDS Push Agent.apk
 - In case of using Private Push, add the apk file.
 - For automatic updating, check **Automatic Update**.

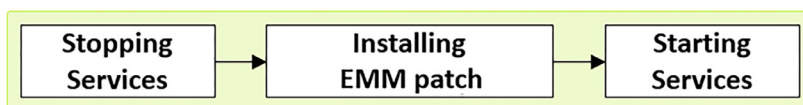
4.9 Test

Start the test when installation of EMM Client, EMM Agent, and Push Agent are completed on the device. See the information about how to install and test the EMM application on the device in the chapter that explains Checking device policies and Using applications in *the Samsung SDS EMM User's Guide*.

-
- Note:**
- See "[Appendix C, Audit Remote Logging](#)" on page 110 for using remote log server.
 - For TLS communication between the EMM server and a device, the root certificate for the CA server should be installed on a device.
-

5 Updating EMM

This chapter describes how to update Samsung SDS EMM (hereinafter “EMM”) to the latest version. See the following steps to apply the EMM patch.



Administrator can only update to the new release version from the latest version of the existing versions. e.g., 1.6.1 -> 2.0

Exceptionally, the EMM 1.5.1 patch installer can be installed from 1.3 or 1.4 version. The patch is supported in an environment using Windows OS and MS SQL database.

Note: Please be aware of vulnerabilities of Windows CryptoAPI used in ECC certificates authentication, and download the Windows server security patch from following URL:
<https://portal.msrc.microsoft.com/en-US/securityguidance/advisory/CVE-2020-0601>

Please note the following when you update the EMM.

- You must use the existing license information (ticket, ticket index, and key table file) when updating the EMM.
- When you update EMM from 1.3 or 1.4 version with Push being installed on the separated server constructed with HA, run the database script after updating EMM. For more detail about how to run the script, see “Samsung SDS Push Installation Guide”.
- To use iOS 12, you need to add ciphers to the Tomcat configuration file. To learn more, see "[Support for iOS 12](#)" on page 108

Note: The Push ICM module provides a TLS channel for message exchange between physically separated servers. This service runs when the Push is installed on a separate server to provide high availability.

5.1 Stopping services

The two services can stop by stopping either the foreground or background service depending on service implementation method.

5.1.1 Single-server environment

Before installing the EMM patch, EMM, Push, and AppTunnel services should be stopped.

Stopping foreground services

To stop EMM, Push, and AppTunnel services, complete the following steps.

1. Go to {EMM installation location}\EMM\{Version}\apache-tomcat-{Version}\bin\.
2. Execute `shutdown.bat` file. This will shut down Tomcat, terminating EMM.
3. Close the following Push service windows:
 - Push ({Version}) DCM(1) 35001,35011
 - Push ({Version}) PS(1) 35000,35010
 - Push ({Version}) SCM(1) 35002,35012
 - Push ({Version}) ECM(1) 35003,35013
 - Push {Version} ICM(1) 35004,35014
4. Close the following AppTunnel service window:
 - AT Server ({Version}) 36000

Stopping background services

Go to **Start > Administrative Tools > Services** and stop the following background services. Select a service with a right click, and then click **Stop**.

- Samsung SDS Push{Version} DCM(1) Background Service
- Samsung SDS Push{Version} PS(1) Background Service
- Samsung SDS Push{Version} SCM(1) Background Service
- Samsung SDS Push{Version} ECM(1) Background Service
- Samsung SDS Push{Version} ICM(1) Background Service
- Samsung SDS AT{Version} Server Background Service
- Samsung SDS EMM{Version} Server Background Service

5.1.2 Multi-server environment

Before installing EMM patch, EMM, Push, AppTunnel, Push Proxy, and AppTunnel Relay services should be stopped. The explanation below is based on "[chapter 1.2.2, Multi server architecture](#)" on page 5.

Stopping foreground services

To stop EMM patch, EMM, Push, AppTunnel, Push Proxy, and AppTunnel Relay services, complete the following steps.

1. Go to the server in which EMM was installed.

2. Go to {EMM installation location}\EMM\{Version}\apache-tomcat-{Version}\bin\.
3. Execute shutdown.bat file. This will shut down Tomcat, terminating EMM.
4. Close the following Push and AppTunnel service windows:
 - Push ({Version}) DCM(1) 35001,35011
 - Push ({Version}) PS(1) 35000,35010
 - Push ({Version}) SCM(1) 35002,35012
 - Push ({Version}) ECM(1) 35003,35013
 - Push {Version} ICM(1) 35004,35014
 - AT Server ({Version}) 36000
5. Go to the server in which Proxy for EMM was installed.
6. Close the following Push Proxy and AppTunnel Relay service windows:
 - PushProxy ({Version}) DPP(1) 35100,35110
 - PushProxy ({Version}) PPP(1) 35101,35111
 - PushProxy ({Version}) EPP(1) 35103,35113
 - AT Relay ({Version}) 36110

Stopping background services

Go to **Start > Administrative Tools > Services** and stop the following background services. Select a service with right click, and then click **Stop**.

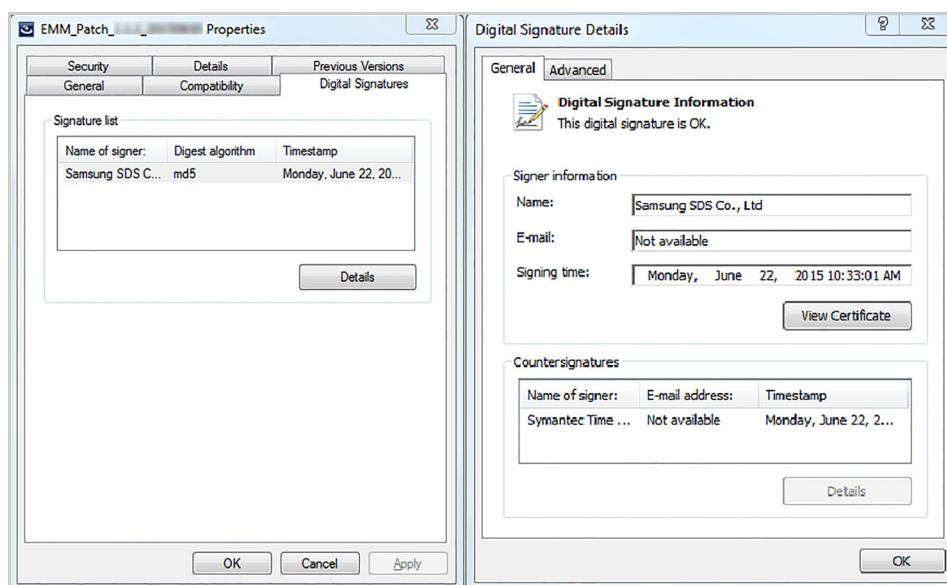
Server	Service
Server with EMM	Samsung SDS Push{Version} DCM(1) Background Service
	Samsung SDS Push{Version} ECM(1) Background Service
	Samsung SDS Push{Version} PS(1) Background Service
	Samsung SDS Push{Version} SCM(1) Background Service
	Samsung SDS Push{Version} ICM(1) Background Service
	Samsung SDS AT{Version} Server Background Service
	Samsung SDS EMM{Version} Server Background Service
Server with Proxy for EMM	Samsung SDS PushProxy{Version} DPP(1) Background Service
	Samsung SDS PushProxy{Version} EPP(1) Background Service
	Samsung SDS PushProxy{Version} PPP(1) Background Service
	Samsung SDS AT{Version} Relay Background Service

5.2 Installing EMM patch

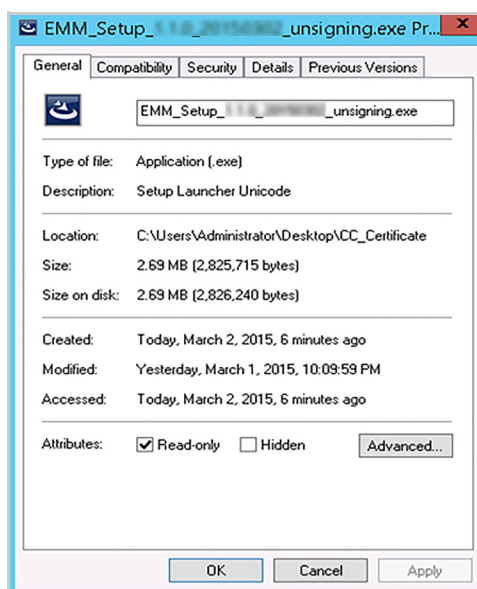
5.2.1 Checking digital signature

Samsung SDS provides an EMM patch installer, with a Samsung SDS certificate included in it, on a CD or by a downloadable link. You can check the digital signature of the installer, before installing the EMM patch.

1. Right-click `EMM_Patch_{Version}_H_{Builddate}.exe`, and then go to **Properties**.
2. Click **Details** button in Digital Signature tab.
3. Click **View Certificate** button to see the details of the digital signature.



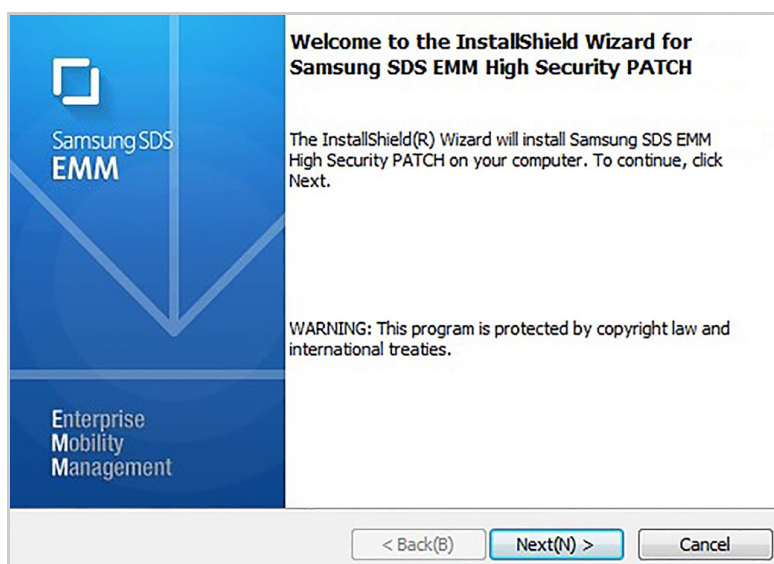
Note: An installation file not digitally signed does not have a Digital Signatures tab as below.



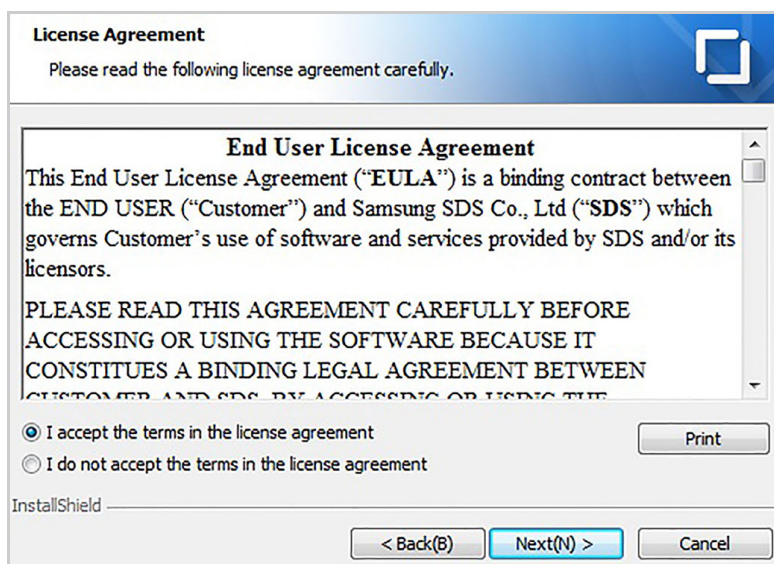
5.2.2 Installing the patch in a single-server environment

Install the patch to the server in which EMM has been installed.

1. Run `EMM_Patch_{Version}_H_{Builddate}.exe`.
 - The patch file should be installed using an administrator account.
2. Select a desired language, then click **OK**.
3. When InstallShield Wizard starts, click **Next** to continue.

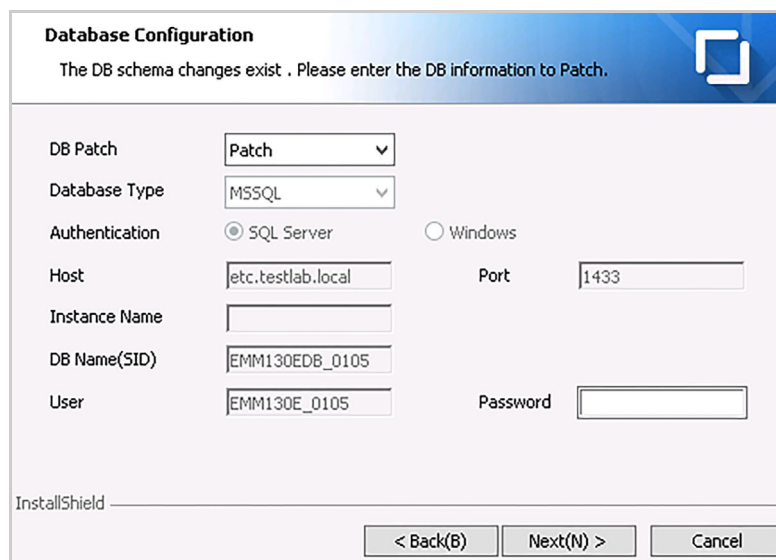


4. Read this end user license agreement carefully and check **I accept the terms in the license agreement**. Then click **Next**.



5. Enter the database information used to install the previous version and click **Next**.

- **DB Patch:** Set whether or not to update the database. The default value is **Patch**. In the HA server environment, only the primary server's database needs to be updated. Select **No Patch** for the rest of servers.

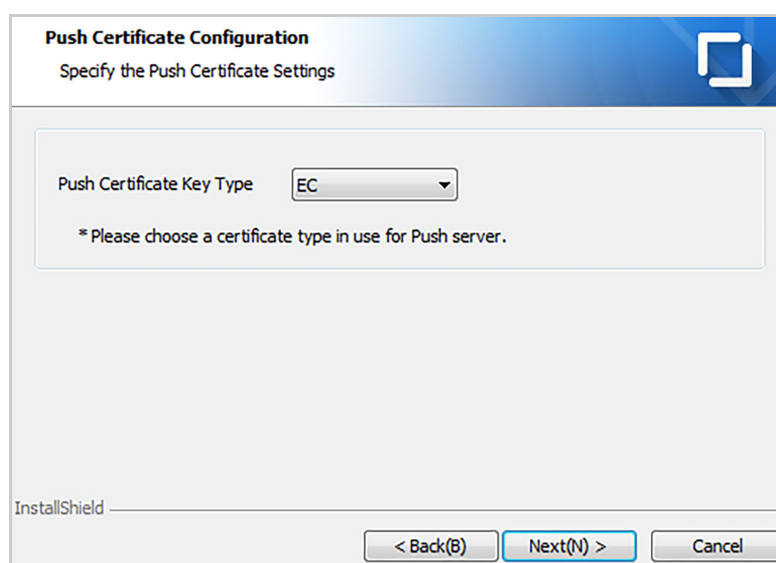


The screenshot shows the 'Database Configuration' dialog box. The title bar reads 'Database Configuration' and the subtitle is 'The DB schema changes exist . Please enter the DB information to Patch.' The dialog contains the following fields and options:

- DB Patch:** A dropdown menu set to 'Patch'.
- Database Type:** A dropdown menu set to 'MSSQL'.
- Authentication:** Two radio buttons: 'SQL Server' (selected) and 'Windows'.
- Host:** A text box containing 'etc.testlab.local'.
- Port:** A text box containing '1433'.
- Instance Name:** An empty text box.
- DB Name(SID):** A text box containing 'EMM130EDB_0105'.
- User:** A text box containing 'EMM130E_0105'.
- Password:** An empty password field.

At the bottom, there are three buttons: '< Back(B)', 'Next(N) >', and 'Cancel'. The 'Next(N) >' button is highlighted in blue. The 'InstallShield' logo is visible in the bottom left corner.

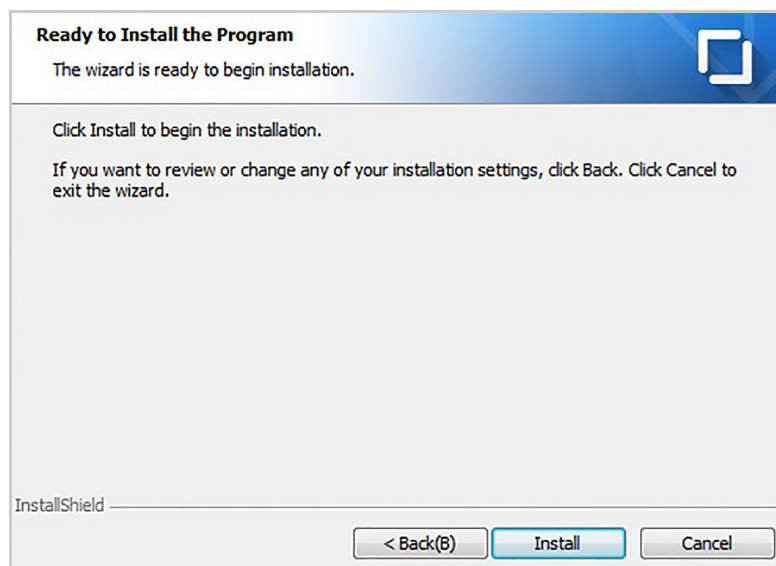
6. Select EC or RSA from the **Push Certificate Key Type** as the certificate key algorithm for the push server, and then click **Next**.



The screenshot shows the 'Push Certificate Configuration' dialog box. The title bar reads 'Push Certificate Configuration' and the subtitle is 'Specify the Push Certificate Settings'. The dialog contains the following field and options:

- Push Certificate Key Type:** A dropdown menu set to 'EC'.

Below the dropdown, there is a note: '* Please choose a certificate type in use for Push server.' At the bottom, there are three buttons: '< Back(B)', 'Next(N) >', and 'Cancel'. The 'Next(N) >' button is highlighted in blue. The 'InstallShield' logo is visible in the bottom left corner.

7. Click **Install**.8. Click **Finish**.

- After updating EMM 1.5.1, follow the step for the additional settings.

Note: Below are directories to back up the previous versions and to save new files created during patch installation.

- Backup files:
 - {EMM installation location}\EMM\{Version}\backup\{Patch Version}
 - {EMM installation location}\Push\{Version}\backup\{Patch Version}
 - {EMM installation location}\AT\{Version}\backup\{Patch Version}
- Patch files:
 - {EMM installation location}\EMM\PATCH\{Patch Version}
 - {EMM installation location}\Push\PATCH\{Patch Version}
 - {EMM installation location}\AT\PATCH\{Patch Version}

5.2.3 Installing a patch in a multi-server environment

For patch installation in a multi-server environment, see "[chapter 1.2.2, Multi server architecture](#)" on page 5.

Installing an EMM patch

Run EMM patch in the server in which EMM was installed, Push, and AppTunnel patches will also be installed at the same time. The installation process is the same as "[chapter 5.2.2, Installing the patch in a single-server environment](#)" on page 71

Installing the Push Proxy patch

Run Push patch on the server in which Push Proxy was installed. For more details on installation, see the chapter that explains Installing Push Proxy in the *Samsung SDS Push Installation Guide*.

Installing AppTunnel Relay patch

Run AppTunnel patch on the server in which AppTunnel Relay has been installed. For more information, see the Chapter 5 of "Samsung SDS AppTunnel Installation Guide".

Configuring a EMM certificate

When Push and AppTunnel connect with the EMM server by HTTPS communication, you need to configure a EMM certificate.

Note: Below are directories to back up the previous versions and to save new files created during patch installation.

- Backup files:

- {EMM installation location}\EMM\{Version}\backup\{Patch Version}
- {EMM installation location}\Push\{Version}\backup\{Patch Version}
- {EMM installation location}\AT\{Version}at-server\backup\{Patch Version}
- {Push Proxy installation location}\PushProxy\{Version}\backup\{Patch Version}
- {AppTunnel Relay installation location}\AT\{Version}\at-relay\backup\{Patch Version}

- Patch files:

- {EMM installation location}\EMM\PATCH\{Patch Version}
 - {EMM installation location}\Push\PATCH\{Patch Version}
 - {EMM installation location}\AT\PATCH\{Patch Version}
 - {Push Proxy installation location}\PushProxy\PATCH\{Patch Version}
 - {AppTunnel Relay installation location}\AT\PATCH\{Patch Version}_Relay
-

5.2.4 Uploading APK file

You should upload the EMM Client, Agent, and Push Agent to update to in the EMM Admin Portal.

5.3 Changing RSA modules

After updating by EMM 1.5.1, you need to change the below RSA modules. Install EMC Crypto module certified by officially-released FIPS 140-2.

1. Back up the below files in the existed `{JDK_HOME path}\jre\lib\ext` directory.
 - `certj.jar`
 - `cryptojce-*.jar`
 - `cryptojcommon-*.jar`
 - `jcmFIPS-*.jar`
 - `sslj-*.jar`
2. Decompress the `tomcat_rsa_module.zip` file to the any directory.
3. Copy the files, `{decompressed tomcat_rsa_module.zip path}` to `{JDK_HOME path}\jre\lib\ext`.
 - `cryptojce-6.2.5.jar`
 - `cryptojcommon-6.2.5.jar`
 - `jcmFIPS-6.2.5.jar`
 - `sslj-6.2.6.jar`
 - `cryptojtestwriter.jar`

5.4 Starting services

After completing the patch installation, start EMM, Push, and AppTunnel services again by starting either the foreground or background service. If updates were done successfully, the service runs normally.

5.4.1 Single-server environment

Starting foreground services

To run EMM, Push, and AppTunnel by starting the foreground service, complete the following steps:

1. Go to `{EMM installation location}\EMM\{Version}\apache-tomcat-{Version}\bin\`.

2. Execute `startup.bat` file. That will start Tomcat, starting EMM.
3. Access the directory, `{EMM installation location}\Push\{Version}\bin`, to run the following Push batch files:
 - `push_dcm_1_start.bat`
 - `push_ps_1_start.bat`
 - `push_scm_1_start.bat`
 - `push_ecm_1_start.bat`
 - `push_icm_1_start.bat`
4. Access the directory, `{EMM installation location}\AT\{Version}\at-server\bin`, to run the AppTunnel batch file.
 - `AT_Server_Start.bat`

Starting background services

Go to **Start > Administrative Tools > Services** and start the following background services. Select a service with a right click, and then click **Start**.

- Samsung SDS Push{Version} DCM(1) Background Service
- Samsung SDS Push{Version} PS(1) Background Service
- Samsung SDS Push{Version} SCM(1) Background Service
- Samsung SDS Push{Version} ECM(1) Background Service
- Samsung SDS Push{Version} ICM(1) Background Service
- Samsung SDS AT{Version} Server Background Service
- Samsung SDS EMM{Version} Server Background Service

-
- Note:**
- If a Windows account is set as a database authentication method when EMM is first installed, additional setting is required. The log on information should be set in the upper Windows service list after updating EMM. For more information, see ["Setting the Windows service log on in chapter 4" on page 54](#).
 - Run the file, `EMM_Patch_{Version}_H_{Builddate}.exe`, again after the patch is installed to uninstall the patch and restore the earlier version.
-

5.4.2 Multi-server environment

Starting foreground services

To run EMM, Push, AppTunnel, Push Proxy, and AppTunnel Relay by starting foreground service, complete the following steps:

1. Go to the server in which EMM has been installed.
2. Go to `{EMM installation location}\EMM\{Version}\apache-tomcat-{Version}\bin\`.
3. Execute `startup.bat` file. That will start Tomcat, starting EMM.

4. Access the directory, {EMM installation location} \Push\{Version}\bin, to run the following Push batch files:
 - push_dcm_1_start.bat
 - push_ps_1_start.bat
 - push_scm_1_start.bat
 - push_ecm_1_start.bat
 - push_icm_1_start.bat
5. Access the directory, {EMM installation location}\AT\{Version}\at-server\bin, to run the AppTunnel batch file.
 - AT_Server_Start.bat
6. Go to the server in which Proxy for EMM has been installed.
7. Access the directory, {Push Proxy installation location}\PushProxy\{Version}\bin, to run the following Push Proxy batch files:
 - push_dpp_1_start.bat
 - push_epp_1_start.bat
 - push_ppp_1_start.bat
8. Access the directory, {AppTunnel Relay installation location}\{Version}\at-relay\bin, to run at_relay_start.bat file.

Starting background services

Go to **Start > Administrative Tools > Services** and start the following background services. Select a service with right click, and then click **Start**.

Server	Service
Server with EMM	Samsung SDS Push{Version} DCM(1) Background Service
	Samsung SDS Push{Version} ECM(1) Background Service
	Samsung SDS Push{Version} PS(1) Background Service
	Samsung SDS Push{Version} SCM(1) Background Service
	Samsung SDS Push{Version} ICM(1) Background Service
	Samsung SDS AT{Version} Server Background Service
	Samsung SDS EMM{Version} Server Background Service
Server with Proxy for EMM	Samsung SDS PushProxy{Version} DPP(1) Background Service
	Samsung SDS PushProxy{Version} EPP(1) Background Service
	Samsung SDS PushProxy{Version} PPP(1) Background Service
	Samsung SDS AT{Version} Relay Background Service

- Note:**
- If a Windows account is set as a database authentication method when EMM is first installed, additional setting is required. The log on information should be set in the upper Windows service list after updating EMM. For more information, see "[Setting the Windows service log on in chapter 4](#)" on page 54 .
 - Run the file, `EMM_Patch_{Version}_H_{Builddate}.exe`, again after the patch is installed to uninstall the patch and restore the earlier version.

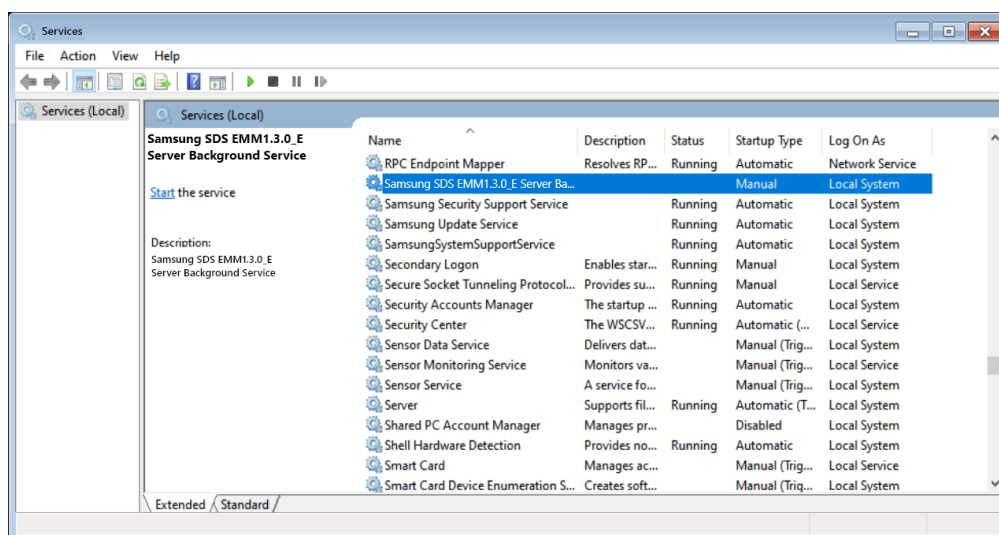
5.5 Retrieving the EMM patch

To return to the previous version by deleting the installed patch, navigate to **Control Panel > Program > Programs and Features** and delete the installed patch, or run `EMM_Patch_{Version}_H_{Builddate}.exe`. The installed patch will be deleted and EMM will return to the previous version.

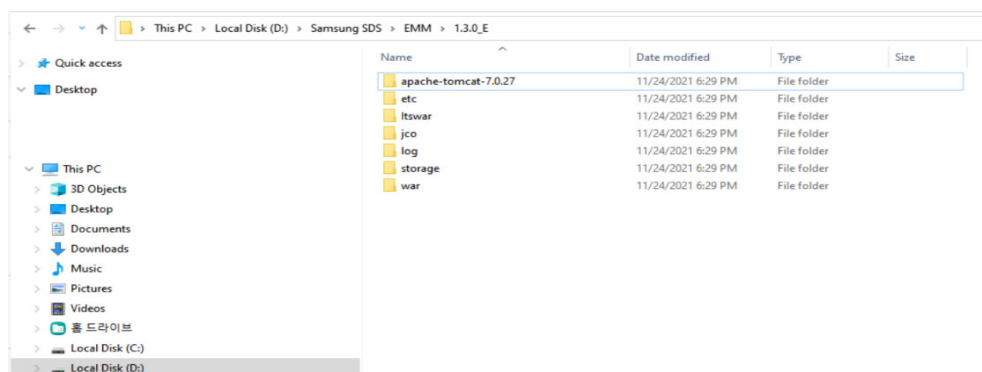
5.6 Tomcat Upgrade

To upgrade Tomcat, complete the following steps.

1. Stop the EMM/Push/AT (if available) services from the Windows Services app.



2. Run `emm_service_uninstall.bat` from `{EMM}\apache-tomcat-{Version}\bin` folder.
Skip this step if the EMM is not running as a Windows service.
3. Backup installed Tomcat folder.
Change the folder name from `apache-tomcat-{Version}` to `apache-tomcat-{Version}_bak`.



4. Unzip new Tomcat.

Download the new Tomcat from <http://tomcat.apache.org/download-80.cgi> and unzip the file to the {EMM installation location}.

5. Copy bat files.

Copy following files from the {EMM installation location}\apache-tomcat-{Version}\bin folder, and then paste it to {new Tomcat folder}\bin folder.

- emm_service_install.bat
- emm_service_uninstall.bat
- emm_start_all.bat
- service.bat
- startup.bat
- catalina.bat

6. Edit bat files.

Edit below things from the bat files that are copied to the new Tomcat folder.

- emm_service_install.bat, emm_service_uninstall.bat, emm_start_all.bat
 - BEFORE:


```
cd D:\SamsungSDS\EMM\{Version}\apache-tomcat-{Version}\bin
```
 - AFTER:


```
cd D:\SamsungSDS\EMM\{Version}\apache-tomcat-{New Version}\bin
```
- service.bat
 - BEFORE:


```
Set "CATALINA_HOME=D:\SamsungSDS\EMM\{Version}\apache-tomcat-\{Version}"
```
 - AFTER:


```
Set "CATALINA_HOME=D:\SamsungSDS\EMM\{Version}\apache-tomcat-{New Version}"
```

Note: If Tomcat's major version is changed, below must be edited as well. (Below change is from 7 to 8.)

1. Find the **tomcat7.exe** and switch to the **tomcat8.exe** (5 total).
2. Edit **PR_DESCRIPTION**.

- BEFORE: Set PR_DESCRIPTION=Apache Tomcat {Version} Server - <http://tomcat.apache.org/>
- AFTER: Set PR_DESCRIPTION=Apache Tomcat {New Version} Server - <http://tomcat.apache.org/>

3. Modify **gc_log** location.

- BEFORE:
"%EXECUTABLE%" //US//%SERVICE_NAME% --JvmOptions "-
Dcatalina.base=%CATALINA_BASE%;-Dcatalina.home=%CATALINA_HOME%;-
Djava.endorsed.dirs=%CATALINA_HOME%\endorsed;-XX:MaxPermSize=512m;-
XX:+PrintGCTimeStamps;-XX:+PrintHeapAtGC;-verbosegc;-Xloggc:D:
\SamsungSDS\EMM\{Version}\apache-tomcat-{Version}\logs\gclog.log;" --
StartMode jvm --StopMode jvm --JvmMs 512m --JvmMx 512m
- AFTER:
"%EXECUTABLE%" //US//%SERVICE_NAME% --JvmOptions "-
Dcatalina.base=%CATALINA_BASE%;-Dcatalina.home=%CATALINA_HOME%;-
Djava.endorsed.dirs=%CATALINA_HOME%\endorsed;-XX:MaxPermSize=512m;-
XX:+PrintGCTimeStamps;-XX:+PrintHeapAtGC;-verbosegc;-Xloggc:D:
\SamsungSDS\EMM\{Version}\apache-tomcat-{New Version}\logs\gclog.log;" --
StartMode jvm --StopMode jvm --JvmMs 512m --JvmMx 512m

- **startup.bat**

- BEFORE:
Set "CATALINA_HOME=D:\SamsungSDS\EMM\{Version}\apache-tomcat-\{Version}"
- AFTER:
Set "CATALINA_HOME=D:\SamsungSDS\EMM\{Version}\apache-tomcat-{New Version}"

7. Copy and Paste xml file.

Copy the `server.xml` file from {EMM installation location}\apache-tomcat-{Version}\conf folder and paste it to {new Tomcat folder}\tomcat\conf folder.

8. Modify xml file.

From the `server.xml` find

```
<ListenerclassName="org.apache.catalina.core.JasperListener"></Listener>
```

and delete it.

9. Register new Tomcat as a Windows service.

Move to new Tomcat's bin folder (`apache-tomcat-{New Version}\bin`), and run the `emm_service_install.bat` file as administrator.

10. Run the Tomcat service.

The EMM must be running as a background service.

6 Configuring EMM High Availability

This chapter describes how to configure the system to increase the availability of Samsung SDS EMM (hereinafter "EMM") to perform required services without fail.

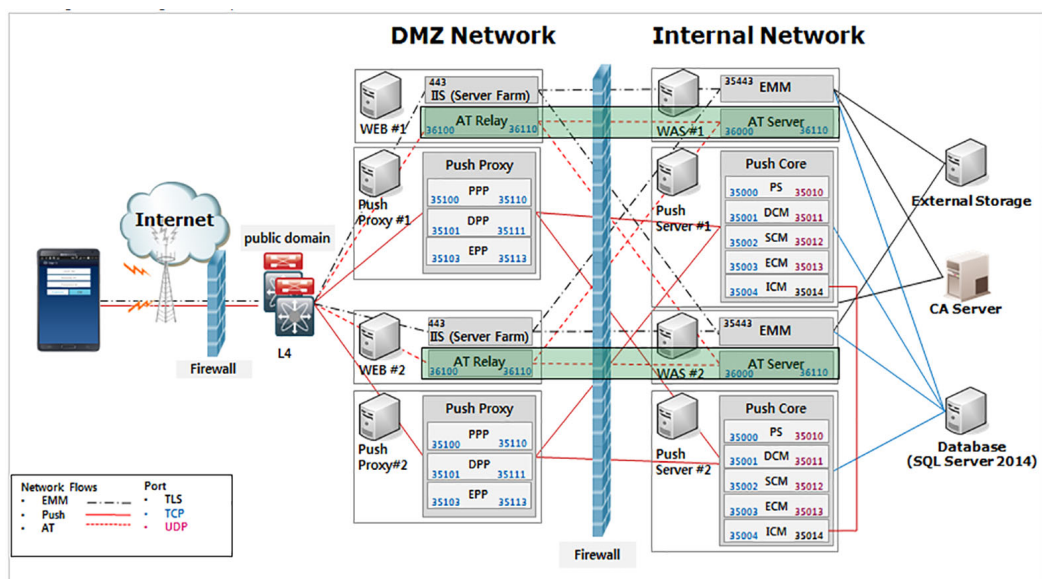


6.1 System configurations

Components required to configure the EMM HA (High Availability) are described in the following. For information about the EMM installation environment, see ["chapter 1.3, EMM installation environment" on page 6](#)

6.1.1 Installation architecture

When configuring HA, install the EMM server, Web server, database server, and external storage on separate servers. Connect the two servers (Web server and EMM server) on the front-end L4 switch to provide high availability and scalability. To access the EMM server from the EMM Client, call the public domain linked to the L4 switch.



6.1.2 Installation components

To configure the HA, you need external storage and L4 equipment.

Component	Description
L4 switch	This is used for load balancing and failover purposes, and it must meet the following requirements. <ul style="list-style-type: none"> • Load balancing: HTTP, HTTPS, VPN, and TCP/IP protocols are available via a specific port. • Failover: Active/Standby or Active/Active policy can apply. The public domain is required to be matched with the IP of L4. You need the public certificate for the public domain when you install the EMM server.
WEB server	A web server that can be configured with IIS 8.5.
EMM server	A server consisting of Apache Tomcat. The Tomcat is installed by default by the EMM Installer.
External Storage	A storage device for sharing files, such as images and APK files registered by the EMM server. This storage device should be present in a separate, third place, and can be configured as an NAS server.
Database	All EMM servers configured for high availability must use the same database. For example, the EMM1 and EMM2 servers must use the same EMM DB connection address. Note: As DB redundancy and EMM redundancy are separate matters, this guide does not cover DB redundancy (Clustering).

6.1.3 Prerequisites

You must have the following to configure EMM HA.

Item	Description
L4 domain	An L4 domain is a single, external domain that is used to communicate with the EMM Client and the EMM servers configured for high availability. When you install the EMM and Push, make sure to enter an L4 domain name for the external domain.
L4 domain certificate	Since the L4 domain certificate should be set to the server during the EMM installation, you must prepare the certificate in advance.

Item		Description
Firewall	RMI port	RMI port is used to synchronize scheduling and transferring of device log files between EMM1 and EMM2 servers. You must open the RMI port between the two servers. The RMI port is defined as follows in the {EMM Installation path}/war/WEB-INF/classes/config/default-config.xml and {EMM Installation path}/ltsvar/WEB-INF/classes/config/default-config.xml. The default port is 11029 and 11409. For other information, such as the policy regarding turning off the firewall, see "chapter 2.4, Pre-installation checklist" on page 21 .
	Push UDP port	You must open the Push UDP port between the EMM1 and EMM2 servers. This is used to perform a health check from the Push server and to open 35010, 35011, 35012, 35013, and 35014 UDP ports between the two servers.

6.2 Installing the servers

This section describes how to install the Web server and EMM server. The following examples will help you understand the setting information.

Server	Domain examples	IP examples
L4 switch	test8.testlab.local	192.168.0.78
WEB1 server	test3.testlab.local	192.168.0.73
EMM1 server	test4.testlab.local	192.168.0.74
WEB2 server	test5.testlab.local	192.168.0.75
EMM2 server	test6.testlab.local	192.168.0.76
Database	etc.testlab.local	

Installing the EMM1 server

Run the EMM installer to install the EMM1 server. For more information about installation procedures other than the HA configuration below, see "[chapter 3.2.1, Installing EMM](#)" on page 38.

- SSL certificate settings: You must enter the L4 certificate for the SSL certificate.
- Database settings: In the **Host** field, enter the domain name (etc.testlab.local). Set the relevant database on the etc.testlab.local server where MS SQL is installed.

Database Configuration
Specify the database settings used by EMM.

Database Type:

Authentication: SQL Server Windows

Host: Port:

Instance Name:

DB Name(SID):

User:

Password: Confirm Password:

***Duplicate User or DB Name could cause errors during installation. So you need to check it out before clicking Next.**

InstallShield

< Back Next > Cancel

- Push network configuration: Enter the settings information for starting the Push server. Select the **Proxy Mode** checkbox and enter the proxy server information.

Item	Description
Push External Host	Enter the domain or IP address of the EMM1 server where Push is installed.
Push Internal Host	Enter the domain or IP address of the EMM1 server where Push is installed.
Proxy External Host	You must enter the L4 domain because the address is used to connect to the Push proxy server from your device.
Proxy Internal Host	Enter the domain or IP address of the Web1 server where Push Proxy is installed.

Push Network Configuration
Configure the server external host and internal host.

Push External Host Push Internal Host

Proxy Mode

Proxy External Host Proxy Internal Host

Configure the Host of the Push Module for access from the external network, and for communication between Push components. (IP or Domain Name)
Firewall rules for each Host and Port must be configured before the installation.

InstallShield

< Back Install Cancel

Installing the Web1 server

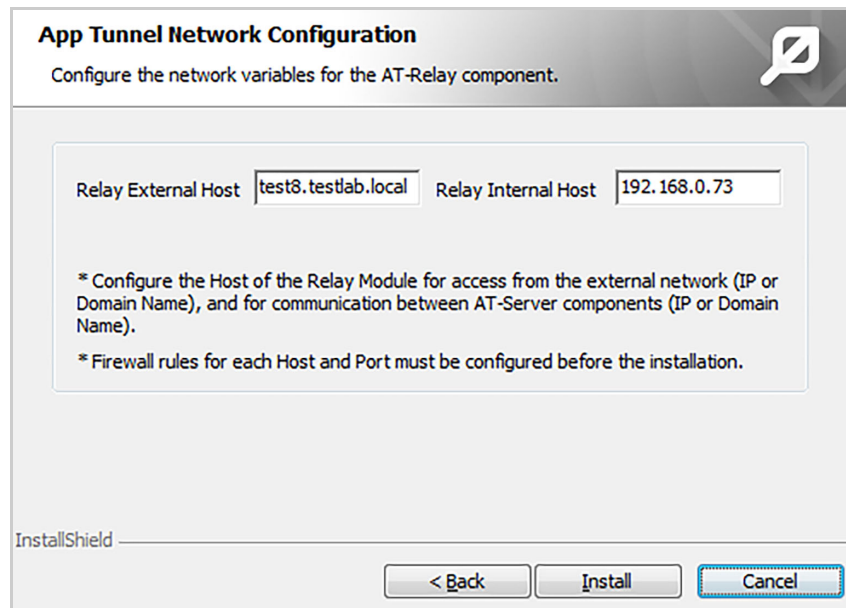
Run the Push and AppTunnel installer to install the Web1 server. For more information about setup procedures other than the following HA configuration, see ["chapter 3.2.3, Installing Push Proxy" on page 47](#) and ["chapter 3.2.4, Installing AppTunnel Relay" on page 48](#).

- Push Proxy network configuration: Enter the settings information for starting the Push Proxy server. Select the Proxy component and enter the proxy server information.

item	Description
Proxy External Host	You must enter the L4 domain because the address is used to connect to the Push proxy server from your device.
Proxy Internal Host	Enter the domain or IP address of the Web1 server where Push Proxy is installed.

- AppTunnel Relay network settings: Enter the settings information for starting the AppTunnel Relay server. Select the AT-Relay installation component and enter the relay server information.

item	Description
Relay External Host	You must enter the L4 domain because the address is used to connect to the AT Relay server from your device.
Relay Internal Host	Enter the domain or IP address of the Web1 server where AT Relay is installed.



App Tunnel Network Configuration
Configure the network variables for the AT-Relay component.

Relay External Host Relay Internal Host

* Configure the Host of the Relay Module for access from the external network (IP or Domain Name), and for communication between AT-Server components (IP or Domain Name).
* Firewall rules for each Host and Port must be configured before the installation.

InstallShield

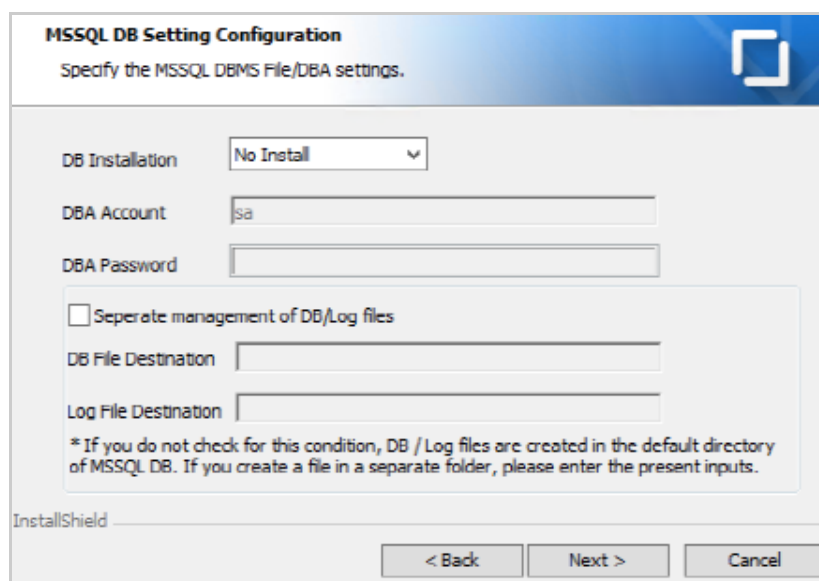
< Back Install Cancel

- For details about the Web server settings, see ["Additional settings for IIS" on page 91.](#)

Installing the EMM2 server

Run the EMM installer to install the EMM2 server. For more information about setup procedures other than the following HA configuration, see ["chapter 3.2.1, Installing EMM" on page 38.](#)

- SSL certificate settings: You must enter the L4 certificate for the SSL certificate.
- Database settings: In the Host area, enter the domain name (etc.testlab.local). Set the relevant database on the etc.testlab.local server where MS SQL is installed. The database information you enter during the EMM2 server installation must be the same as that of the EMM1 server installation. Select **No Install** so that the EMM database is not created again.



MSSQL DB Setting Configuration
Specify the MSSQL DBMS File/DBA settings.

DB Installation

DBA Account

DBA Password

Separate management of DB/Log files

DB File Destination

Log File Destination

* If you do not check for this condition, DB / Log files are created in the default directory of MSSQL DB. If you create a file in a separate folder, please enter the present inputs.


InstallShield

< Back Next > Cancel

- Push network configuration: Enter the settings information for starting the Push server. Select the **Proxy Mode** check box, and enter the proxy server information.

item	Description
Push External Host	Enter the domain or IP address of the EMM2 server where Push is installed.
Push Internal Host	Enter the domain or IP address of the EMM2 server where Push is installed.
Proxy External Host	You must enter the L4 domain because the address is used to connect to the Push proxy server from your device.
Proxy Internal Host	Enter the domain or IP address of the Web2 server where Push Proxy is installed.

Push Network Configuration



Configure the server external host and internal host.

Push External Host

Push Internal Host

Proxy Mode

Proxy External Host

Proxy Internal Host

Configure the Host of the Push Module for access from the external network, and for communication between Push components. (IP or Domain Name)

Firewall rules for each Host and Port must be configured before the installation.

InstallShield

Installing the Web2 server

Run the Push and AppTunnel installers to install the Web2 server. For more information about setup procedures other than the following HA configuration, see ["chapter 3.2.3, Installing Push Proxy" on page 47](#) and ["chapter 3.2.4, Installing AppTunnel Relay" on page 48](#).

- Push proxy network configuration: Enter the settings information for starting the Push Proxy server. Select the **Proxy Mode** check box and enter the proxy server information.

item	Description
Proxy External Host	You must enter the L4 domain because the address is used to connect to the Push proxy server from your device.
Proxy Internal Host	Enter the domain or IP address of the Web2 server where Push Proxy is installed.

- AppTunnel relay configuration: Enter the settings information for starting the AppTunnel Relay server. Select the AT-Relay installation component and enter the relay server information.

item	Description
Relay External Host	You must enter the L4 domain because the address is used to connect to the AT Relay server from your device.
Relay Internal Host	Enter the domain or IP address of the Web2 server where AT Relay is installed.

App Tunnel Network Configuration

Configure the network variables for the AT-Relay component.

Relay External Host Relay Internal Host

* Configure the Host of the Relay Module for access from the external network (IP or Domain Name), and for communication between AT-Server components (IP or Domain Name).

* Firewall rules for each Host and Port must be configured before the installation.

InstallShield

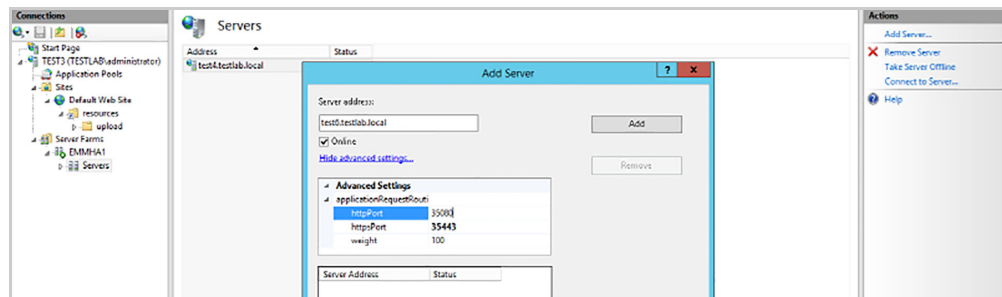
- For details about the Web server settings, see ["Additional settings for IIS"](#) on page 91.

Additional settings for IIS

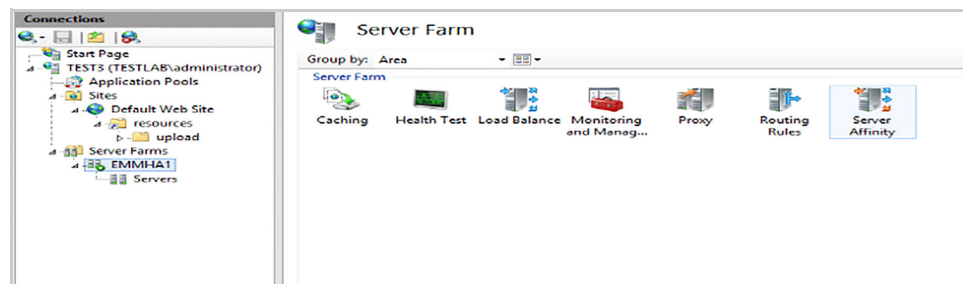
Install Internet Information Services (IIS) on the Web server, and then install the relevant components of Application Request Routing (ARR) as follows. To set up a Server Farm for the HA configuration through IIS, complete the following steps:

- URL rewrite
- Web Farm Framework
- Application Request Routing
- External Cache

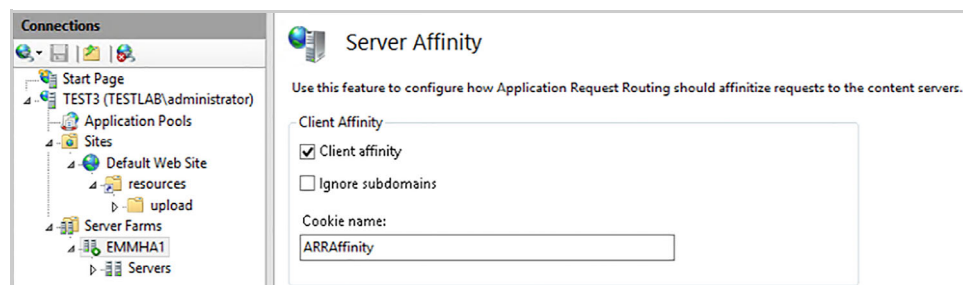
1. In the Internet Information Services (IIS) Manager, go to **Connections > Server Farms**, and click Servers. On the Server Farm screen, go to **Actions > Add Server**, and add a server to be configured for HA.
2. On the "Add Server" pop-up window, type the domain and IP information of the EMM Server to link with the Server address, and click **Add**.
The following is an example of linking servers: The newly added EMM1 server with the domain test4.testlab.local and the EMM2 server at test6.testlab.local. The two EMM servers are configured for HA through IIS.



3. Click the Server Farm that is configured for HA, and select **Server Affinity**.



4. Select the Client affinity check box.



6.3 Configuring the settings

This section describes how to change the EMM settings to configure it for high availability after installing the EMM.

You should configure the settings for resource sharing or for calling a domain. After you have finished configuring all the settings, run all the modules that are installed on the EMM Server and Push proxy server to verify that the servers start normally.

Modifying the service profile

In the EMM Admin Portal, enter the information in the EMM service profile for accessing the EMM server from the EMM client. After completing the installation of the EMM1 and EMM2 servers, modify the EMM and Push server addresses in the service profile to the L4 domain address.

- For Single-Tenant mode, in the Admin Portal, go to **Setting > > Configuration**, and then click the **Service profile** to modify it.
- For Multi-Tenant mode, in the TMS Admin Portal, go to **Management > Service profile** to modify it.

6.3.1 Configuring the EMM settings

Check the following settings in the `default-config.xml` file on the EMM1 and EMM2 servers, and then change the path to the external storage. The path to the file is as follows:

- `{EMM Install Location}\{Version}\war\WEB-INF\classes\config\default-config.xml`

Changing the EMM host information

The three values, hostname, httpsPort, and url must be configured as the L4 address and https address of L4.

- The following is an example of an L4 address: test8.testlab.local:443.

```
<emm>
  <hostname>test8.testlab.local</hostname>
  <httpsPort>443</httpsPort>
</emm>

<download>
  <url>https://test8.testlab.local:443</url>
</download>
```

Changing the storage path

Change the storage path to an external storage device. The external storage path settings for the EMM1 and EMM2 servers must be the same as that of the External Storage.

- When the External Storage path is {EXTERNAL_STORAGE_PATH}:

```
<rootPath>{EXTERNAL_STORAGE_PATH}\storage</rootPath>
<tempPath>{EXTERNAL_STORAGE_PATH}\storage\temp</tempPath>
<fileUploadPath>{EXTERNAL_STORAGE_PATH}\storage\fileUpload</file
UploadPath>
<addPath>{EXTERNAL_STORAGE_PATH}\storage\qrcode</addPath>
<qrcodeImagePath>{EXTERNAL_STORAGE_PATH}\storage\qrcode</qrcodeI
magePath>

<profileBasicUploadPath>{EXTERNAL_STORAGE_PATH}\storage\mdm\uploa
d</profileBasicUploadPath>
<webClipUploadPath>{EXTERNAL_STORAGE_PATH}\storage\mdm\upload\we
bClip</webClipUploadPath>
<fontUploadPath>{EXTERNAL_STORAGE_PATH}\storage\mdm\upload\font<
/fontUploadPath>
<knoxSSOConfigUploadPath>{EXTERNAL_STORAGE_PATH}\storage\mdm\upl
oad\sso\conf</knoxSSOConfigUploadPath>
<knoxSSOLogoUploadPath>{EXTERNAL_STORAGE_PATH}\storage\mdm\uploa
d\sso\logo</knoxSSOLogoUploadPath>
<knoxGenVPNConfigUploadPath>{EXTERNAL_STORAGE_PATH}\storage\mdm\
upload\knoxGenVPN\profile</knoxGenVPNConfigUploadPath>
<genVPNConfigUploadPath>{EXTERNAL_STORAGE_PATH}\storage\mdm\uploa
d\genVPN\profile</genVPNConfigUploadPath>
```

6.3.2 Configuring the Push settings

This section describes how to change the Push settings to configure it for high availability.

Configuring the Push proxy components

When the Push Proxy mode is set on the EMM installer, the information of Push Proxy modules is inserted to database automatically.

Currently, you do not have the EMM2 Push proxy information in the EMM database management because you chose the **No Install** option when you installed the EMM2.

To enter the information of the DPP, PPP, and EPP modules for the EMM2 Push proxy, run MS SQL Studio to access the database, and then run the following script.

- The following shows an example of a DB script when the external and internal IP addresses of the EMM2 Push proxy are "test8.testlab.local" and "192.168.0.75" respectively. INSTANCEID should be set as {COMPONENTID}.002.

```
INSERT INTO PUSH_PROXYINSTANCEINFO (COMPONENTID, INSTANCEID,
EXHOST, EXPORT, INHOST, INPORT, STATUS, LAST_MODIFIED) VALUES
('0012','0012.002','test8.testlab.local','35101','192.168.0.75',
'35111','1',getdate());

INSERT INTO PUSH_PROXYINSTANCEINFO (COMPONENTID, INSTANCEID,
EXHOST, EXPORT, INHOST, INPORT, STATUS, LAST_MODIFIED) VALUES
('0013','0013.002','test8.testlab.local','35100','192.168.0.75',
'35110','1',getdate());

INSERT INTO PUSH_PROXYINSTANCEINFO (COMPONENTID, INSTANCEID,
EXHOST, EXPORT, INHOST, INPORT, STATUS, LAST_MODIFIED) VALUES
('0014','0014.002','test8.testlab.local','35103','192.168.0.75',
'35113','1',getdate());
```

Configuring Multi SCM

Configure a Multi SCM IP address in the `sa.properties` file located in the following directory to configure the Push SCM module of the EMM server for high availability.

- {EMM Install Location}\{Version}\war\WEB-INF\classes\sa\properties\sa.properties
- Enter the IP instance information of the SCM_IP items as follows. Below is an example of the SCM information that is installed in test4.testlab.local (EMM1 server), test6.testlab.local (EMM2 server).

```
SCM_IP=test6.testlab.local:35002,test4.testlab.local:35002
```


Applying Push licenses

To change Push licenses, you must apply the same information and files to the EMM1 and EMM2 servers as shown below:

- Change SAGID, TICKET, and TICKET_KEY_INDEX in the `sa.properties` file:
`{EMM Install Location}\{Version}\war\WEB-INF\classes\sa\properties\sa.properties`
- `{EMM Install Location}\{Version}\resources\PushKeyTable.ser`

L4 settings

To use L4, change the USE_L4 settings to TRUE in the `ps.properties` file in the following directory: You must set the L4 IP and port in PUSH_EXTRACCESSINFO database.

- `{EMM Install Location}\PUSH\{Version}\resources\ps\properties\ps.properties`
- Below is a DB script example of entering the IP and port to the L4 address:
`test8.testlab.local`.

```
INSERT INTO PUSH_EXTACCESSINFO
      (COMPONENTID,HOST,TCPPORT,LAST_MODIFIED)      VALUES ('0012',
'test8.testlab.local', {L4 port linked to DPP,getdate()});

INSERT INTO PUSH_EXTACCESSINFO
      (COMPONENTID,HOST,TCPPORT,LAST_MODIFIED)      VALUES ('0013',
'test8.testlab.local', {L4 port linked to PPP},getdate());
```

6.3.3 Configuring the AppTunnel settings

Install AppTunnel Server (ATS) and AppTunnel Relay Server (ATR) according to the deployment mode, and then set the details as follows.

Configuring the Relay server settings

Configure the AppTunnel Relay server information in the EMM1 and EMM2 servers as shown below. The path to the file is as follows:

- {EMM Install Location}\AT\{Version}\resources\config\spring\spring-data-config.xml
- Below is an example of using two Relay servers: 70.30.183.127:36100 and 70.30.183.127:36100.

```
<property name="relays">
  <list>
    <bean class="com.sds.emm.at.ats.data.vo.Relay">
      <property name="relayInstancelId" value="relay1"/>
      <property name="relayHost" value="70.30.183.127"/>
      <property name="relayPort" value="36100"/>
      <property name="status" value="1"/>
    </bean>
    <bean class="com.sds.emm.at.ats.data.vo.Relay">
      <property name="relayInstancelId" value="relay2"/>
      <property name="relayHost" value="70.30.183.128"/>
      <property name="relayPort" value="36100"/>
      <property name="status" value="1"/>
    </bean>
  </list>
</property>
```

Configuring the certificate information

Set the CN value of SubjectDN for ATS and ATR in the IN_DN_LIST in the `general.properties` file in the EMM1 and EMM2 servers. The path to the file is as follows:

- {EMM Install Location}\AT\{Version}\resources\general\properties\general.properties

6.4 Testing

This section describes how to conduct the test after configuring high availability for the Samsung SDS EMM. A high availability test is used to determine whether the automatic server switching and continuous services are provided by randomly creating fault conditions.

In other words, the testing checks the Failover connection between the two servers redundantly configured. This manual describes only the EMM and Push servers and the test procedure is as follows.

1. Pre-Test: Introduces the preliminary work to prepare for the test.
2. Test: Causes a failure condition on the server being connected to a mobile device or the Admin Portal. Stop the server in communication with a Client for a definite test.
3. Check Service: Make sure that the service is switched to a normal server from the failed server.

6.4.1 Mobile device test scenarios

This section describes how to test the following three cases: Activating mobile devices, downloading an app from the App Store, and uploading log files from devices.

Activating mobile devices

Enable the EMM and then disable it on the mobile device to proceed with the Failover testing.

- Pre-Test
 1. Register the information of the test subjects (i.e. the user ID, Password, and mobile ID) in advance.
 2. Remotely access each server where EMM is installed, and monitor both of the EMM server log files by using a program, such as a tail program. Restrict the use of the EMM server to checking the logs only for the test purposes.

```

C:\SamsungSDS\EMM\1.3.0_E_Vo\log\emmlog [3.7 MB]
2016-05-31 20:15:05 DEBUG [A.selectProfileCompValueList:43] <== Row: EMM, effcd4e382e
2016-05-31 20:15:05 DEBUG [A.selectProfileCompValueList:43] <== Row: EMM, effcd4e382e
2016-05-31 20:15:05 DEBUG [A.selectProfileCompValueList:43] <== Row: EMM, effcd4e382e
2016-05-31 20:15:05 DEBUG [c.s.m.b.c.MobileController:506] ##### ProfileAPI Success xelatc
2016-05-31 20:15:05 DEBUG [c.s.m.b.c.MobileController:514] ##### authorityInternalApp : [
2016-05-31 20:15:05 DEBUG [c.s.m.b.c.MobileController:515] ##### STEP2 : END ProfileAPI C
2016-05-31 20:15:05 DEBUG [A.applstCount:43] ==> Parameters: EMM(Stcing), Android(Sttring), F
2016-05-31 20:15:05 DEBUG [A.applstCount:43] ooo Using Connection [857994944, URL+jdbc:sqlse
2016-05-31 20:15:05 DEBUG [A.applstCount:43] ==> Preparing: SELECT COUNT(*) FROM ( SELECT C
2016-05-31 20:15:05 DEBUG [A.applstCount:43] <== Columns:
2016-05-31 20:15:05 DEBUG [A.applstCount:43] <== Row: 1
2016-05-31 20:15:05 DEBUG [c.s.m.b.c.MobileController:519] ##### Applst Count Search Don
2016-05-31 20:15:05 DEBUG [c.s.m.b.c.MobileController:500] ##### STEP3 : END APPLISTCOUNT
2016-05-31 20:15:05 DEBUG [c.s.m.b.c.MobileController:550] ##### JSON ABRAY1 #####
2016-05-31 20:15:05 DEBUG [c.s.m.b.c.MobileController:561] ##### JSON ABRAY2 #####
2016-05-31 20:15:05 DEBUG [c.s.m.b.c.MobileController:566] ##### STEP4 : START UPDATCOUNT
2016-05-31 20:15:05 DEBUG [A.updateCount:43] ooo Using Connection [685325501, URL+jdbc:sqlse
2016-05-31 20:15:05 DEBUG [A.updateCount:43] ==> Preparing: SELECT count(*) FROM ( SELECT A.

C:\SamsungSDS\EMM\1.3.0_E_Vo\log\emmlog [216.5 KB]
2016-05-31 20:03:50 WARN [c.s.m.c.u.MessageDataEncryptionManager:117] Compression meth
2016-05-31 20:03:50 INFO [c.s.m.c.s.i.AppComanService:272] PHONE OR TAB CHECK
2016-05-31 20:04:00 WARN [c.s.m.c.u.MessageDataEncryptionManager:117] Compression meth
2016-05-31 20:04:10 INFO [c.s.m.c.e.n.s.i.NoticeServiceProvider:113] ##### NOTICE SERV
2016-05-31 20:04:13 INFO [c.s.m.c.e.n.s.i.NoticeServiceProvider:114] ##### 1. HEADER I
2016-05-31 20:04:13 INFO [c.s.m.c.e.n.s.i.NoticeServiceProvider:120] ##### 2. ENCERVE
2016-05-31 20:04:13 ERROR [c.s.m.c.e.n.s.i.NoticeServiceProvider:247] Compression metho
2016-05-31 20:04:13 INFO [c.s.m.c.e.n.s.i.NoticeServiceProvider:132] ##### 3. PRIVATE
2016-05-31 20:04:13 INFO [c.s.m.c.e.n.s.i.NoticeServiceProvider:136] ##### 4. ANALYZE
2016-05-31 20:04:13 INFO [c.s.m.c.e.n.s.i.NoticeServiceProvider:156] ##### 5. COMPRES
2016-05-31 20:04:13 INFO [c.s.m.c.e.n.s.i.NoticeServiceProvider:146] ##### 6. PUBLIC K
2016-05-31 20:04:13 INFO [c.s.m.c.e.n.s.i.NoticeServiceProvider:149] ##### 7. ENCRIFPTI
2016-05-31 20:04:14 WARN [c.s.m.c.u.MessageDataEncryptionManager:117] Compression meth
2016-05-31 20:04:14 INFO [c.s.m.c.s.i.AppComanService:272] PHONE OR TAB CHECK
2016-05-31 20:04:50 WARN [c.s.m.c.u.MessageDataEncryptionManager:117] Compression meth
2016-05-31 20:04:50 INFO [c.s.m.c.s.i.AppComanService:272] PHONE OR TAB CHECK
2016-05-31 20:04:55 WARN [c.s.m.c.u.MessageDataEncryptionManager:117] Compression meth
2016-05-31 20:04:55 INFO [c.s.m.c.s.i.AppComanService:272] PHONE OR TAB CHECK
  
```

- Test
 3. Perform an enrollment on a mobile device and check which EMM server the log is created on.

4. If the device enrollment is successful, perform unenrollment.
5. Remotely access the server where a log is created in Step 3, and then stop the EMM service.
 - Check Service
6. Perform enrollment on the mobile device again and check if a log is created on the server where the EMM service has not been stopped.
7. Make sure enrollment is successful from the terminal.

Downloading applications

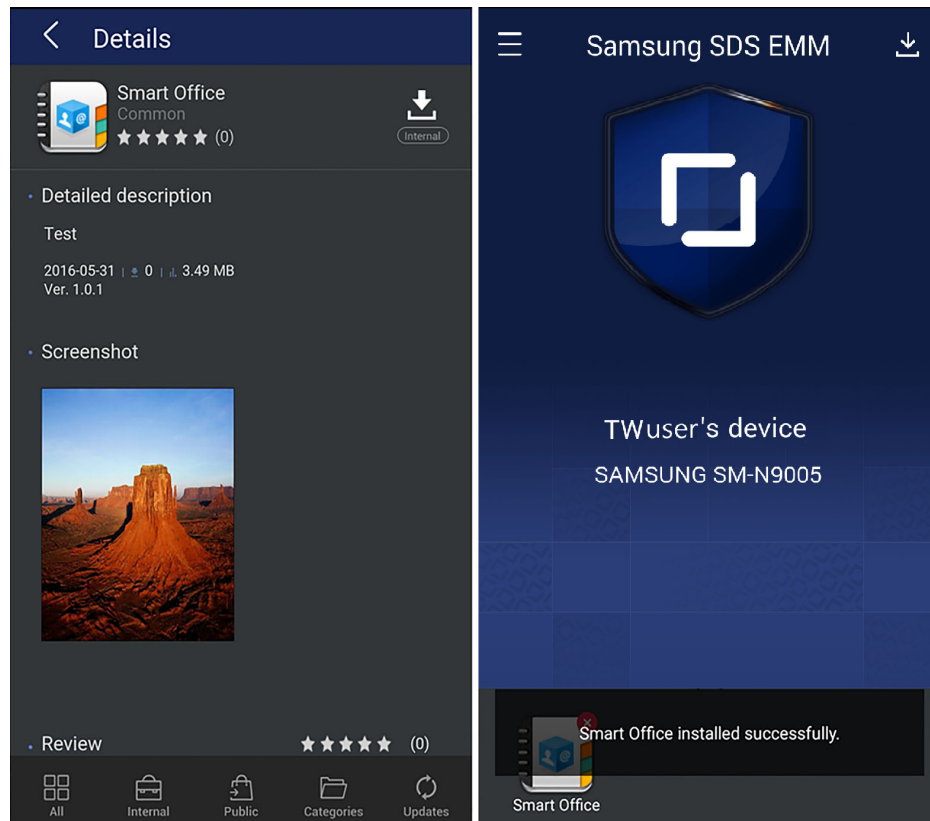
Download an application from the App Store and delete it from the terminal to proceed with the failover testing.

- Pre-Test

1. Prepare a device with the EMM service activated.
2. Remotely access each server where EMM is installed, and monitor both of the EMM server logs by using a program such as a tail program. Restrict the use of the EMM server to checking the logs only for the test purposes.

The image shows two terminal windows side-by-side, both displaying log output from a Samsung device. The left window is titled 'emmllog (3.7 MB) - BareTail' and shows logs from 2016-05-31 20:15:05 onwards. The right window is titled 'emmllog (216.5 KB) - BareTail' and shows logs from 2016-05-31 20:03:50 onwards. The logs contain various messages including 'DEBUIG', 'WARN', 'INFO', and 'ERROR' with detailed system information and error codes.

- Test
3. Run the EMM on the device, and then click the App Store menu to check which server generates the EMM logs.
 4. Select and install a random application.



5. Remotely access the server where a log is created in Step 3, and then stop the EMM service.
 - Check Service
6. After you uninstall the application from the mobile device, click on the App Store and check if the app is missing from the list.
7. Select and reinstall the application that was installed in Step 4 and check if the installation is complete.

Uploading device log files

You can conduct this test by uploading log files from a mobile device and checking whether the logs are collected from the failover Admin Portal.

- Pre-Test
 1. Prepare a mobile device with the EMM service activated.
 2. Remotely access each server where EMM is installed, and monitor both of the EMM server log files by using a program, such as a tail program. Restrict the use of the EMM server to checking the logs only for the test purposes.

- Test
 3. Run the EMM on the mobile device, and then click the App Store menu to check which server generates the EMM logs.
 4. From the device's EMM, go to **Support > Send activity Log** and send the device log to the EMM server.
 5. Access the EMM Admin Portal and check if the log was uploaded from the mobile device.
 6. Remotely access the server where the log was created in Step 3, and then stop the EMM service.
- Check Service
 7. From the device's EMM, go to **Support > Send activity Log** and send the device log to the EMM server.
 8. Access and check if the log was uploaded from the mobile device.

6.4.2 Admin Portal test scenarios

This section describes how to test for the following four cases: Accessing the Admin Portal, uploading applications, building Kiosk applications, and importing a profile.

Accessing the Admin Portal

After logging into the Admin Portal and checking the server IP address, perform the failover test.

- Pre-Test

1. Enter the EMM URL in the browser and log into the EMM Admin Portal.
2. Go to **Setting** > > **Server Information** and check the IP information of the server you are currently connected to.

COMPUTERNAME	TEST4
CRYPTOJ_VERSION	6.2.0.1
EMM Host	test4
EMM IP	192.168.0.33
EMM Version	1.3.0 (EMM Build Number: 20160404.1643)
JAVA_HOME	C:/Program Files/Java/jdk1.7.0_79
JMX PORT	

- Test

3. Remotely access the server that you confirmed the IP information of in Step 2, and then stop the EMM service.
4. Click any menu on the EMM Admin Portal that was connected.

- Check Service

5. When the login window appears on the EMM Admin Portal, log in again.
6. Go to **Setting** > > **Server Information**, check the COMPUTERNAME and EMM IP to check if the connection is switched to another server.

→ COMPUTERNAME	TEST5
CRYPTOJ_VERSION	6.2.0.1
EMM Host	test5
→ EMM IP	192.168.0.24
EMM Version	1.3.0 (EMM Build Number: 20160404.1643)
JAVA_HOME	C:/Program Files/Java/jdk1.7.0_79
JMX PORT	

Uploading applications

After uploading and assigning an internal application from the EMM Admin Portal, verify whether the application is installed on the device.

- Pre-Test

1. Prepare the applications, icons, and screenshots to upload for testing.
2. Enter the EMM URL in the browser and log in to the EMM Admin Portal. Go to **Setting** > > **Server Information** and check the IP information of the server you are currently connected to.

- Test

3. Go to **Application**, and add the application installation files, icons, and screenshots to register for the internal applications.
4. Remotely access the server that you confirmed the IP information of in Step 2, and then stop the EMM services.

- Check Service
- 5. Log back in to the Admin Portal, and go to **Settings > > Server Information**, and then check the changes in the COMPUTERNAME and EMM IP that you are currently connected to.
- 6. Go to **Application** and check the application information you added in Step 3

After adding the internal application, click Assign to deploy the application to the device. **Importing profiles**

Export the profile from the Admin Portal to the device, and then make sure the new profile file has been registered.

- Pre-Test
 1. Enter the EMM URL in the browser and log in to the EMM Admin Portal.
 2. Go to **Setting > > Server Information** and check the IP information of the server you are currently connected to.
 3. Generate a random profile, click the profile you created, and then click the **Export Policy** to download the profile file.
- Test
 4. Go to **Profile**, and click **Import Policy** to save the profile exported from Step 3 to create a profile.
 5. Remotely access the server that you confirmed the IP information of in Step 2, and then stop the EMM services.
- Check Service
 6. Log back in to the Admin Portal, and go to **Setting > > Server Information**, and then check the changes in the COMPUTERNAME and EMM IP that you are currently connected to.
 7. Go to **Profile**, and click **Import Policy** to save the profile exported from Step 3 as a different name to create a profile
 8. Compare the policies of the profiles that you created in Step 4 and Step 7 to check if they are properly registered.

Appendix A Installing or changing a certificate

A.1 Installing and changing EMM server certificate

To install or change the certificate used by Samsung SDS EMM (hereinafter "EMM") server, complete the following steps:

1. Stop the EMM server. You can get detailed instructions in the ["chapter 5.1, Stopping services" on page 67](#).
2. Back up the existing certificate. Skip this step when installing a new certificate.
 - The directory where the certificate is installed: Check with the following line in `{EMM installation location}/EMM/{version}/apache-tomcat-{Version}/conf/server.xml`.


```
<Connector port="35443" ..... keystoreFile="Path to certificate" .....></Connector>
```
3. Install the certificate.
 - Copy a new P12 certificate file to the current directory or a new directory.
 - If you copy it to a new directory, modify the certificate path for the `server.xml` file.
 - For the server certificate requirements, see the ["chapter 2.2, Preparing certificates" on page 10](#).
4. Restart EMM server. For detailed instructions, see the ["chapter 5.4, Starting services" on page 75](#).

Configuring the EMM server certificate for HTTPS

When the device connects the EMM server by HTTPS communications for DN (Distinguish Name) authentication of the device certificate, DN of EMM server must be authenticated. To authenticate a certificate, DN information must be configured. If DN or Key type of the certificate are changed, configure the certificate as below

item	Description
The file directory	<code>{Push_HOME}/resources/certserver/properties/cert.properties</code>

item	Description
DN List of the EMM server certificate	Enter Common Name (CN) of server certificate from emm.trusted.dnlist . <ul style="list-style-type: none"> Enter Subject Alternative Name (SAN) if SAN information is set up in a certificate.
EMM Certificate Key Type	Enter EC or RSA key algorithm of the certificate from emm.certificate.algorithm . If emm.certificate.algorithm is RSA, enter the cipher list as below. <ul style="list-style-type: none"> emm.certificate.rsa.cipher.suite=TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256 If emm.certificate.algorithm is EC, comment the item to be disabled as below. <ul style="list-style-type: none"> #emm.certificate.rsa.cipher.suite=TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA

A.2 Installing or changing a certificate for Push and AppTunnel server

To install or change certificates used by Samsung SDS Push (hereinafter "Push") server, Proxy, Samsung SDS AppTunnel (hereinafter "AppTunnel") Server, and AppTunnel relay, complete the following steps:

1. Stop the process. For more information, see the chapter that explains running the service of *Samsung SDS Push Administrator's Guide* and *Samsung SDS AppTunnel Administrator's Guide*.
2. Backup the existing certificate: Skip this step for installation of a new certificate.
 - Directory backup: {EMM installation location} resources/{IP}_ \${Port}
 - Config file backup: {EMM installation location}/resources/general/properties/general.properties
 - Cert file backup: STORE_FILEPATH for P12 files in {EMM installation location}/resources/general/properties/general.properties/
3. Install a certificate.
 - a. Delete the existing directory, {EMM installation location}/resources/{IP}_ \${Port}
 - b. Edit the config files: Modify below items in {EMM installation location}/resources/general/properties/general.properties file.
 - **ENTITY_ALIAS**: Alias Name for new P12 certificate
 - **ENTITY_PASSWORD**: Key Password for new P12 certificate. Make sure to enter ENTITY_PASSWORD identical to STORE_PASSWORD.
 - **STORE_FILEPATH**: File path for new P12 certificate
 - **STORE_PASSWORD**: Password for new P12 file

- **IN_DN_LIST:** CN value for new P12 file
- c. Copy new Cert File and P12 cert file.
4. Start the process. For more information, see chapter 3 of “Samsung SDS Push Administrator’s Guide” and chapter 3 of “Samsung SDS AppTunnel Administrator’s Guide.

A.3 Installing or changing a new SA certificate

To install or change certificate used by Push SA in EMM Server, complete the following steps:

1. Stop the EMM server. For detailed instructions, see the "[chapter 5.1, Stopping services](#)" on page 67.
2. Backup the existing certificate: Skip this step for Installation of a new certificate.
 - Config file backup: {EMM installation location}/EMM/{version}/war/WEB-INF/classes/sa.properties
 - Cert file backup: P12_FILE_PATH of {EMM installation location}/EMM/{version}/war/WEB-INF/classes/sa.properties for P12 files.
3. Install a certificate.
 - Copy the new cert file in P12 format: Default path is in /EMM/{version}/war/WEB-INF/classes/export.p12
4. Edit the config files. Modify the items below in {EMM installation location}/EMM/{version}/war/WEB-INF/classes/sa.properties file.
 - **P12_FILE_PATH:** file path for new P12 certificate
 - **P12_ALIAS:** alias name for new P12 certificate
 - **P12_PWD:** password for new P12 certificate
 - **SA_PRIVATEKEY_PWD:** key password for new P12 certificate. Make sure to enter SA_PRIVATEKEY_PWD identical to P12_PWD.
5. Restart the EMM server. For detailed instructions, see the "[chapter 5.4, Starting services](#)" on page 75.

Appendix B Configuring allowable Cipher

B.1 Setting Push and AppTunnel

All communication within Samsung SDS Push (hereinafter "Push") and Samsung SDS AppTunnel (hereinafter "AppTunnel") is based on TLS. The Samsung SDS EMM (hereinafter "EMM") supports high security communication with the mutual authentication and the FIPS certified cryptographic module for TLS.

The cipher module works properly only when the cc-certified module with FIPS mode on is set on both a server and a device.

- Server: FIPS certified Crypto-J module with FIPS mode on, provided by EMC
- Device: CC certified OpenSSL module with FIPS mode on, provided by Samsung Electronics

Configuration

TLS Control: TLS communication is established and works properly only when a device supports the protocol and cipher controlled by a server through TLS handshake procedures. The cipher suite and TLS version should be configured in EMM server component (In Push Proxy, Push Server, AT Relay, AT Server) before operation.

Configuration file

- AppTunnel: {EMM installation location}
/AT/resources/general/properties/general.properties
- Push: {EMM installation location}
PUSH/resources/general/properties/general.properties

TLS version control

The TLS channel is established successfully only when the device version matches that of the server.

- The default setting is set as below, the following case can be connected only with TLS 1.2.
 - PROTOCOL_LIST=TLSv1.2
- You can change the value of PROTOCOL_LIST, enter the range of TLS versions using comma(,) in PROTOCOL_LIST. If you set as below, the following case can be connected with TLS 1.2.
 - PROTOCOL_LIST=TLSv1.2
- The only TLS version 1.2 is allowed to be configured by the requirements of the Security Target.

Cipher control

The TLS channel is established successfully only when the device matches the list of the cipher suite in the server. The use of the Cipher Suite list varies depending on the Key Type settings for the certificate.

- CIPHER_SUITE_LIST= TLS_RSA_WITH_AES_128_CBC_SHA256,
 TLS_RSA_WITH_AES_256_CBC_SHA256,
 TLS_RSA_WITH_AES_256_GCM_SHA384,
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- For ECDSA, the following ciphers should be used.
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- For RSA, the following ciphers should be used.
 - TLS_RSA_WITH_AES_128_CBC_SHA256,
 TLS_RSA_WITH_AES_256_CBC_SHA256,
 TLS_RSA_WITH_AES_256_GCM_SHA384,
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- Null cipher, SSL cipher and RC4 cipher are excluded.
- All cipher system supports are available without any extra configuration.
- The administrator do not add any cipher suites except those allowed by the Security Target.
- In the list for the cipher suite, there must be no spaces between the comma and the next cipher.

B.2 Setting Tomcat

The EMM Admin Portal requires TLS on the Tomcat server. The installation package provides the default settings, but these can change if necessary.

Configuration file

- `{Tomcat_HOME}/conf/server.xml`

TLS version control

- `<connector port=35443 ... sslEnabledProtocols="TLSv1.2"`
- Support TLS v1.2

Cipher control

- `<Connector port=35443 ... sslEnabledProtocols="TLSv1.2" ciphers="`
`TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256`
`,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_CBC_S`
`HA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_AES`
`_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_EC`
`DHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_25`
`6_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH`
`E_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_S`
`HA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH`
`_AES_256_GCM_SHA384" ... />`
- Use comma(,) between Cipher Suites.
- Default Cipher Suite
 - `TLS_RSA_WITH_AES_128_CBC_SHA256,`
`TLS_RSA_WITH_AES_256_CBC_SHA256,`
`TLS_RSA_WITH_AES_256_GCM_SHA384,`
`TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,`
`TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,`
`TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,`
`TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,`
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,`
`TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,`
`TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,`
`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,`
`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,`
`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,`
`TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- The administrator do not add any cipher suites except those allowed by the Security Target.

Support for iOS 12

.If you have upgraded to version 2.1.6 and wish to use iOS 12, then you need to complete the following:

- Add cipher

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
```

```
- <Connector port=35443 ... sslEnabledProtocols="TLSv1.2"
  ciphers="TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_
  ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128
  _GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_EC
  DHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SH
  A,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_G
  CM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE
  _RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CB
  C_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA",TLS_RSA_WITH_A
  ES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384"> </Conne
  ctor>
```

- Remove the comment from the Listener

Remove the comment from the code in

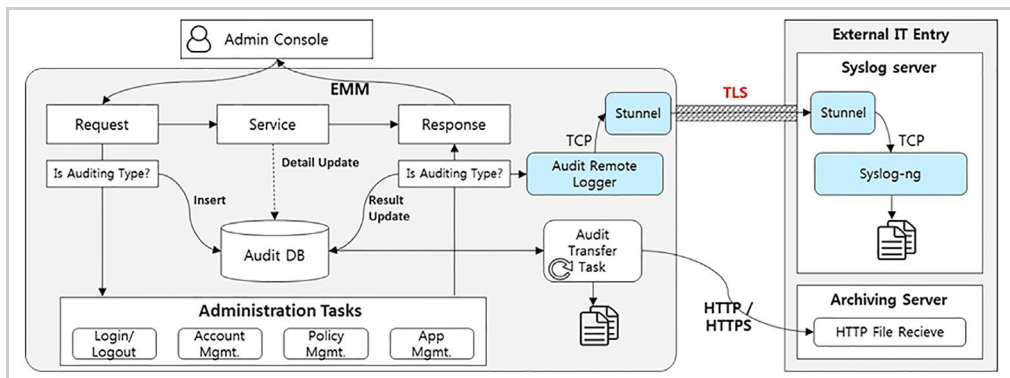
`org.apache.catalina.core.AprLifecycleListener` and leave the code as below..

```
<Listener
  className=""org.apache.catalina.core.AprLifecycleListen
  er"" SSLEngine=""on""></Listener>
```

Appendix C Audit Remote Logging

C.1 Remote logging overview

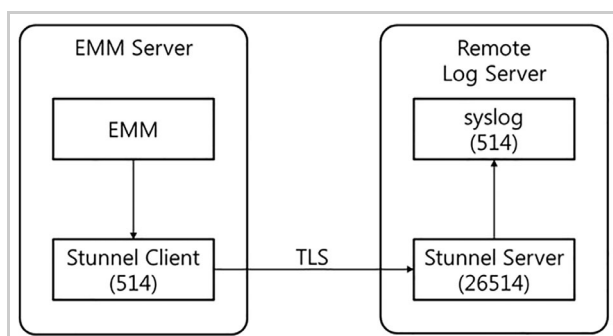
The Samsung SDS EMM (hereinafter "EMM") audit log provides Remote Logging to transfer the Audit log to the remote logging server, when necessary, for management. Communication between the EMM server and the remote log server is protected by TLS secure communication or using Windows Server provided IPsec settings. The communication path from the EMM to Syslog Server is protected using Windows Server provided IPsec – instructions can be found in Samsung SDS EMM Configuration Guide for IPsec settings in Microsoft Windows Server 2016/2019 for Common Criteria Evaluation.



This chapter describes the settings to transfer the audit log to the remote logging server and the process of installing stunnel to connect the security channel between EMM and the remote logging server.

1. Remote log server
 - Classifying and recording audit log files on syslog
 - Installing and configuring stunnel Server
2. EMM server
 - Installing and configuring stunnel Client

The software is installed on the EMM server and remote log server.



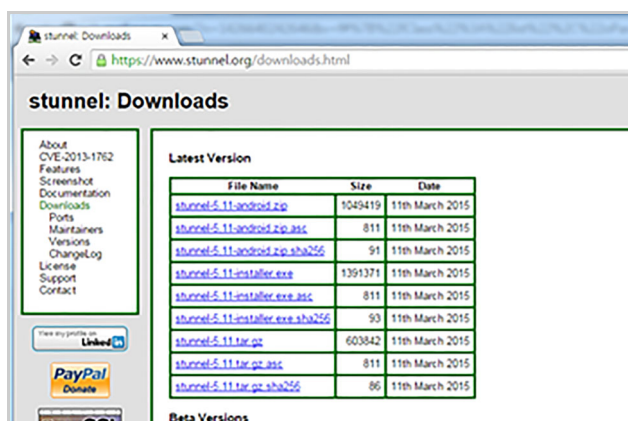
※ If IPsec is configured, it communicates directly with the EMM server without Stunnel.

- Note:**
- Remote log server is not automatically installed on EMM installation. It should be set up separately with Syslog-ng or rsyslog or other solutions supporting Syslog protocol (RFC5424) installed on it. Refer to the install guide included with the remote log server OS.
 - This appendix explains how to install and configure stunnel on Windows. The installation and configuration on Linux and other operating systems, download the install file at www.stunnel.org and refer to the following URL regarding information on operating systems, including Linux.
 - Stunnel must be installed on both the EMM server and the Remote log server. Stunnel should be set as the server on the Remote log server, and Client on the EMM server.

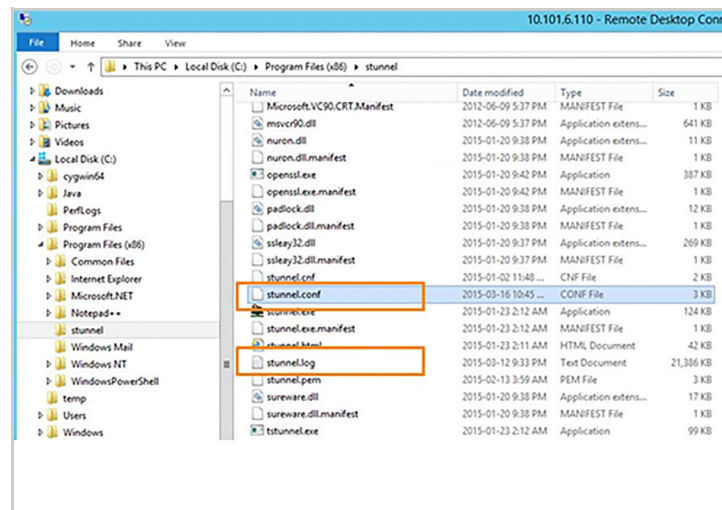
C.2 Installing stunnel in Windows

To install Stunnel in Windows, complete the following steps:

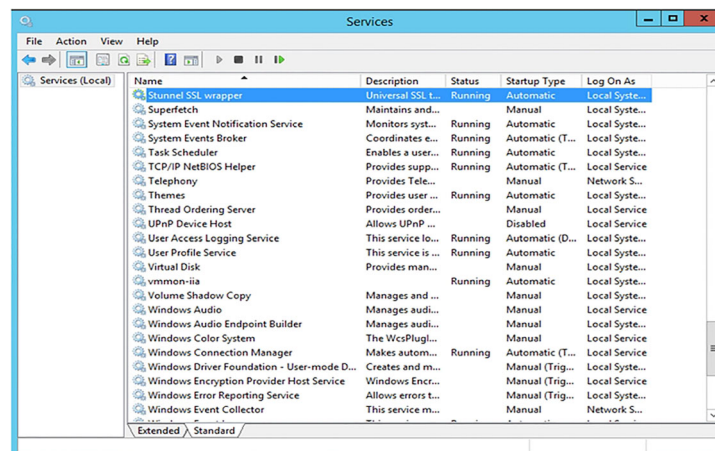
1. Download the latest version of stunnel for Windows at www.stunnel.org/downloads.html.



2. Run on the downloaded file to install stunnel.
 - The installation location of stunnel and files are:
 - Installation path: C:\Program Files (x86)\stunnel
 - Configuration file: C:\Program Files (x86)\stunnel\stunnel.conf
 - Log file: C:\Program Files (x86)\stunnel\stunnel.log



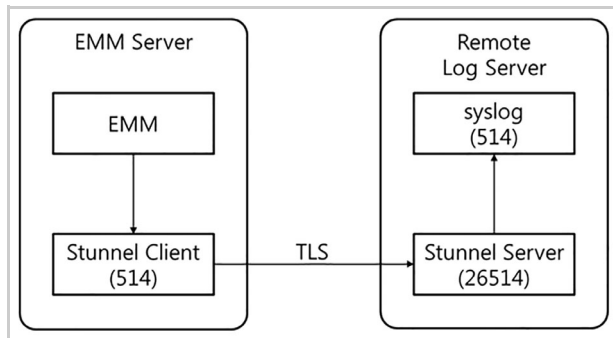
3. Go to **Start Windows > All Programs > stunnel > Edit stunnel.conf** and edit the configuration file:
 - See "[C.3.2, Configuring stunnel](#)" on page 114 for the detailed instructions.
4. Go to **Start Windows > All Programs > stunnel > stunnel Service Install** and register for the Windows Service.
5. Click **stunnel Service Start(▶)** to start stunnel.
 - Go to **Start Windows > All Programs > stunnel**, then click **Service Start**.



- Go to **Start Windows > Tools > Service**, then click **Start Service**.

C.3 Configuring the remote log server

This explains the configuration for the secure communication channel connection between the EMM server and the remote log server. Port number can be set in this way.



C.3.1 Configuring Syslog-ng for the remote log server

This configuration is to classify the transferred audit log from Syslog-ng with the following criteria and to record the log.

- Classify directories by Host name.
- Classify log files by Tenant or EMM module name with date.

Open the configuration file in the editor, then modify it according to the environment. The configuration file is located in `/etc/syslog/syslog-ng.conf`.

```

@version: 3.2
@include "scl.conf"

options {
  dir-owner("SYSTEM");
  dir-group("root");
  dir-perm(0755);
  owner("SYSTEM");
  group("root");
  perm(0644);
  keep_hostname(yes);
  time-reap(30);
  mark-freq(60);
  flush_lines(0);
  create-dirs(yes);
};
  
```

```
# EMM Audit
source s_audit_tcp {
  tcp(port(514) - Port
  flags("syslog-protocol")
  max-connections(100)
  encoding("UTF-8"));
};

template t_emm_audit_template { - Log file record Template configuration
  template("${ISODATE} ${HOST} ${SOURCEIP}
  ${.SDATA.emmAudit@18060.tenantId} ${MSG}\n");
  template_escape(no); };

destination d_emm_audit { - Log file establishing rule configuration
  file("/logs/${HOST}/emm_audit_${.SDATA.emmAudit@180
  60.tenantId}-${YEAR}-${MONTH}-${DAY}.log"
  template(t_emm_audit_template)
  );
};

log {source(s_audit_tcp); destination(d_emm_audit);};
```

-
- Note:**
- This chapter describes how to configure syslog-ng. It does not have to be syslog-ng. You can use other solutions, including Rsyslog and syslogd supporting Syslog protocol (RFC5424).
 - Since the Syslog-ng configuration file for the remote log server is located in a different directory, depending on the OS, refer to the install guide for the OS.
 - You can use different criteria to sort the audit log, depending on your environment. The tenant or EMM module name must be included in the file name.
-

C.3.2 Configuring stunnel

You have to install stunnel on both the EMM server and the remote log server for secure communication. Set the Stunnel as the server on the remote logging server and as a client on the EMM server so that EMM server can ask for secure communication to the remote log server.

Open the stunnel configuration file using the editor and edit in accordance with your site's environment.

- Go to **Start Windows > All Programs > Stunnel > Edit stunnel Configuration.**

Configuring the stunnel as a server

The configuration example below is for secure communication between the EMM server and remote log server.

- CC/MDMPP requirements are highlighted in bold.

```
(Example)
debug = 7
output = stunnel.log
fips = yes
engine = capi
Verify = 3
cert = eccert.pem
key = eckey.pem
[audit-syslog-server]
sslVersion = TLSv1.2
ciphers = AES128-SHA:AES256-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-
AES256-SHA:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-
GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-
SHA384
accept = 26514
connect = 514
```

Configuring the stunnel as a client

The following example is for secure communication between the EMM server and the remote log server. CC/MDMPP requirements are highlighted in bold.

```
(Example)
debug = 7
output = stunnel.log
fips = yes
engine = capi
[audit-syslog-client]
client = yes
ciphers = AES128-SHA:AES256-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-
AES256-SHA:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-
GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-
SHA384
cert = ecclient.pem
key = eckey.pem
CAfile = rootca-and-server-certs.pem
CRLfile = combined-CRL-file.pem
accept = 127.0.0.1:6514
connect = {remote log server} :26514
```

Note: Prepare the certificates listed below to set the options:

- Remote log server: CA file (pem), CRL file (pem), Server certificate, key file (pem)
- EMM server: CA file (pem), CRL file (pem), Client certificate, key file (pem)

Set the CC related items in accordance with CC(MDMPP) requirements.

C.3.3 Configuring stunnel options

This explains how to set important options when configuring stunnel. All the CC/MDMPP related items must be set in accordance with the requirements.

Global option

CC/MDMPP requirements are highlighted in bold.

```

stunnel.conf - Notepad
File Edit Format View Help
; Sample stunnel configuration file for Win32 by Michal Trojnara 2002-2015
; Some options used here may be inadequate for your particular configuration
; This sample file does "not" represent stunnel.conf defaults
; Please consult the manual for detailed description of available options
;
; * Global options
; *-----
; Debugging stuff (may useful for troubleshooting)
debug = 7
output = stunnel.log
; Enable FIPS 140-2 mode if needed it for compliance
fips = yes
; Initialize Microsoft CryptoAPI interface
engine = capi
; Also needs "engineID = capi" in each section using the CAPI engine
;
; * Service defaults may also be specified in individual service sections *
; *-----
; Certificate/key is needed in server mode and optional in client mode
;cert = stunnel.pem

```

(Example)

`debug = [FACILITY.]LEVEL`

debugging level

Level is a one of the syslog level names or numbers emerg (0), alert (1), crit (2), err (3), warning (4), notice (5), info (6), or debug (7).

`output = FILE`

append log messages to a file

fips = yes | no

Enable or disable FIPS 140-2 mode.

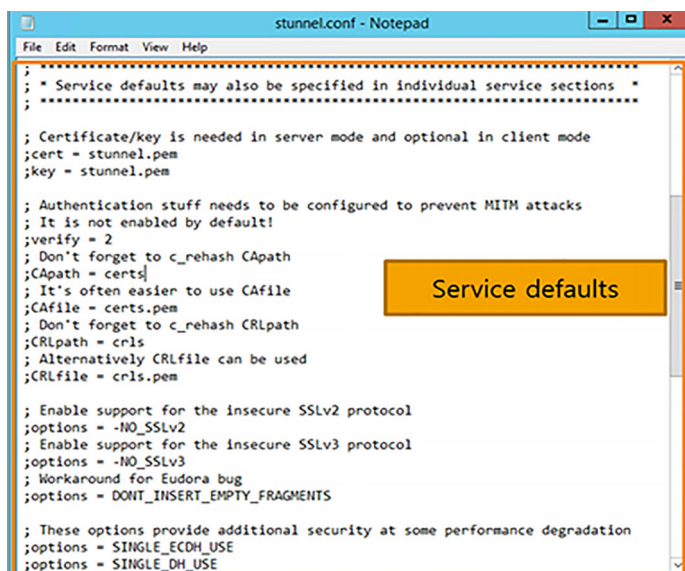
engine = capi | auto | ENGINE_ID

select hardware engine

Editing service-level options

There are two ways to set service level options: Edit Service defaults to apply it to all services in-cluding server and client, or edit Service definitions to apply it to each service.

- Service defaults

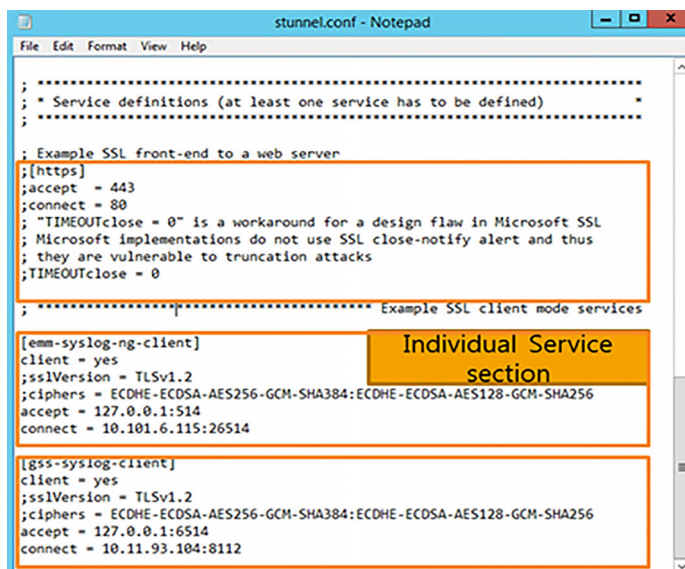


```

stunnel.conf - Notepad
File Edit Format View Help
;
; * Service defaults may also be specified in individual service sections *
;
; Certificate/key is needed in server mode and optional in client mode
;cert = stunnel.pem
;key = stunnel.pem
;
; Authentication stuff needs to be configured to prevent MITM attacks
; It is not enabled by default!
;verify = 2
; Don't forget to c_rehash Cpath
;Cpath = certs
; It's often easier to use CAfile
;CAfile = certs.pem
; Don't forget to c_rehash CRLpath
;CRLpath = crls
; Alternatively CRLfile can be used
;CRLfile = crls.pem
;
; Enable support for the insecure SSLv2 protocol
;options = -NO_SSLv2
; Enable support for the insecure SSLv3 protocol
;options = -NO_SSLv3
; Workaround for Eudora bug
;options = DONT_INSERT_EMPTY_FRAGMENTS
;
; These options provide additional security at some performance degradation
;options = SINGLE_ECDH_USE
;options = SINGLE_DH_USE

```

- Service definitions



```

stunnel.conf - Notepad
File Edit Format View Help
;
; * Service definitions (at least one service has to be defined) *
;
; Example SSL front-end to a web server
;[https]
;accept = 443
;connect = 80
; "TIMEOUTclose = 0" is a workaround for a design flaw in Microsoft SSL
; Microsoft implementations do not use SSL close-notify alert and thus
; they are vulnerable to truncation attacks
;TIMEOUTclose = 0
;
; ***** Example SSL client mode services *****
;
;[emm-syslog-ng-client]
client = yes
;sslVersion = TLSv1.2
;ciphers = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256
accept = 127.0.0.1:514
connect = 10.101.6.115:26514
;
;[gss-syslog-client]
client = yes
;sslVersion = TLSv1.2
;ciphers = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256
accept = 127.0.0.1:6514
connect = 10.11.93.104:8112

```

Editing cipher suites

Cipher suites, a service-level option, can be set in both Service defaults and individual service. The administrator must set cipher suites to operate in a CCMDMPP Complaint manner.

- **ciphers** = CIPHER_LIST
 - Select permitted SSL ciphers.

– A code with a colon list given for SSL connection. (e.g. DES-CBC3-SHA:IDEA-CBC-MD5.).

– CC/MDMPP requirements are highlighted in bold.

ciphers = AES128-SHA:AES256-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384

- **options** = SSL_OPTIONS

– OpenSSL library options.

– Except for SSL_OP_prefix.Stunnel, options are derived by combining Stunnel and open SSL library. Several options can be used to specify multiple options. A **dash(-)** should be added to option name to disable the option:

- For example, for compatibility with the erroneous Eudora SSL implementation, the following options can be used:

options = DONT_INSERT_EMPTY_FRAGMENTS

default:

options = NO_SSLv2

options = NO_SSLv3

Editing certificate options

Certificate options are service-level options and can be set in both Service defaults and individual services. EMM Server components act as clients in order to securely connect to the remote syslog server. If the remote syslog server requires mutual authentication, the administrator must configure only the certificates for the EMM Server components.

- **cert** = PEM_File

– The name of certificate chain PEM file.

– The certificates must be in PEM format, and must be delivered from the actual server/client certificate to the self-signed root CA certificate.

– A certificate is required in server mode, and optional in client mode.

- **key** = KEY_File

– The Private key for the certificate is specified as cert option.

– The Private key is needed to authenticate the certificate owner. For security reasons, only the owner of the file can view its contents. On Unix systems you can use the **chmod 600 keyfile** command.

– Default: value of cert option

Editing CA & CRL options

CA & CRL options, service level options, can be set in both Service defaults and individual service. To run it in CC MDMPP Compliant manner, the administrator must make sure that Stunnel includes both the audit server certificate and the audit server root certificate. The administrator may include these two certificates in the stunnel configuration by using either the **CPath** or the **CAfile** options specified below.

- **CPath** = DIRECTORY
 - Certificate Authority directory.
 - This is the directory used by stunnel when using **verify**. Note that the certificates in this directory should be named XXXXXXXX.0 where XXXXXXXX is the hash value of the certificate encoded with DER.
 - The hash algorithm has been changed in OpenSSL 1.0.0. It is required to `c_rehash` the directory When OpenSSL 0.x.x. is upgraded to OpenSSL 1.x.x.
 - **CPath** path is relative to **chroot** directory.
- **CAfile** = CERT_FILE
 - Certificate Authority file.
 - This file contains multiple CA certificates, used with **verify**.

The administrator may include these two certificates in the stunnel configuration by using either **CRLpath** or **CRLfile**.

- **CRLpath** = DIRECTORY
 - Certificate Revocation Lists directory.
 - This is the directory used by stunnel to find CRLs when using the **verify**. Note that the CRLs in this directory should be named XXXXXXXX.r0 where XXXXXXXX is the CRL hash value of certificate encoded with DER.
 - The hash algorithm has been changed in OpenSSL 1.0.0. It is required for `c_rehash` the directory when OpenSSL 0.x.x. is upgraded to OpenSSL 1.x.x.
 - **CRLpath** path is relative to **chroot** directory.
- **CRLfile** = CERT_FILE:
 - Certificate Revocation Lists file
 - This file contains multiple CRLs, used with the **verify**.

Editing verify certificate

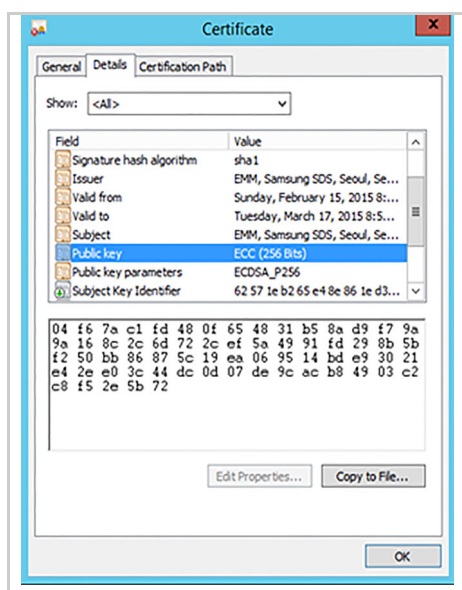
Stunnel has methods for checking certificates, which are controlled by the **verify** option. In order to operate in a CC MDMPP Compliant manner, the administrator must configure the system to use **verify=3**.

- **verify** = LEVEL
 - verify peer certificate
 - level 0: Request and ignore peer certificate.
 - level 1: Verify peer certificate if present.
 - level 2: Verify peer certificate.
 - level 3: Verify peer with locally installed certificate.
 - level 4: Ignore CA chain and only verify peer certificate.
 - Default: No verify.

It is important to understand that this option is for access control, not for authorization. The level 2 certificates that have not been revoked are allowed, regardless of the Common Name. For this reason an assigned CA should be used with level 2, not with the general CA commonly used in the web server. Level 3 is preferred for point-to-point connections.

Certificate key exchange algorithm

The cipher suite key exchange algorithm for TLS connections is determined by the certificate key exchange algorithm. If a certificate issued with RSA open key is used, TLS is connected to the RSA key exchange algorithm. If support for the EC key exchange algorithm is needed, a certificate issued with the EC key exchange algorithm must be used.



- Note:**
- According to (tools.ietf.org/html/rfc2818#section-3), FQDN is a standard for HTTP over TLS between the web site and browser. Stunnel requires the administrator to register the server certificate file on the client manually. The certificate validity check should be performed by the administrator prior to using the certificate.
 - This chapter only handles the minimum options for secure connections. See www.stunnel.org/static/stunnel.html for more details.

C.4 Using Audit Remote Logging

When configuration between the remote log server and the EMM server is completed, configure the remote log server on the EMM Admin Portal. Then, all the audit logs are sent to the remote log server and recorded. These are the steps:

1. Log into EMM Admin Portal.
2. Go to **Setting** > > **Configuration**.
3. Click **Audit**.
4. Check **Connect to Audit Log to Remote Server (SYSLOG)** on "Audit" window.
5. Enter **IP/Host** and **Port**.
6. Click **OK**.
7. Get remote logging started.

Appendix D Using EMM on iOS

To use Samsung SDS EMM on iOS devices, issue the following certificates and then register on the EMM server, or use it for building the EMM Client.

1. Issue and register APNs certificates
 - On the iOS system, the client and the server communicate through APNs, Apple's public push server, by default.
 - APNs certificates are used to encrypt and authenticate messages communicated through the APNs server. There are two certificates under APNs certificates and each one can be issued or registered using separate procedures.
 - a. MDM APNs certificate: Used for device control through iOS embedded MDM module.
 - b. App APNs token/certificate: Used for communication with the SDS EMM Client.
2. Issue and register iOS Sign Certificate
The certificate is used for the encryption and authentication of the profile message between the EMM server and the client. It can be issued or registered using the Java Keytool.
3. Issue iOS Client Distribution Certificate and build EMM Client
According to iOS regulations, a certificate for encryption of the EMM Client must be issued and used for building the EMM Client.

The processes above should be done with the client certificates, but it might be very complicated. Therefore, starting from SDS EMM v2.4.1, it is first recommended to use a simplified method that uses given certificates built by SDS. In this case, you need to issue MDM APNs certificate only out of certificates listed above. The others will be automatically pre-loaded on SDS EMM server.

If you are using EMM with a version below v.2.4.1 or already using an iOS certificates for your other work apps, refer to ["D.2, Using iOS Client with your certificate" on page 127](#) and proceed with issuance and registration with the client certificate.

D.1 Using Generic iOS Client

Previously, clients had to build the EMM Client for themselves due to Apple's policy and the fact that APP (Client) Certificate requires annual update. However, as token method with unlimited period is now supported, EMM Client built by Samsung SDS's certificate can now be provided. Clients do not need to create a paid ADEP account nor need a MAC Book because they do not need to build the EMM Client. However, to modify applications or share data with the client's other work app, you must build and deploy iOS applications using the client's existing certificate as was done before. No updates are available if the build certificate is different.

Note: iOS Client Distribution Certificate which is created based on the SDS ADEP is valid for 2 years only, so you should update the iOS version before the expiration period is over.

D.1.1 Checking Prerequisites

If you newly install v2.4.1 or don't have registered iOS certificates on the server, required certificates will be automatically registered during the version upgrade.

1. Client APNs token
On the EMM Admin Portal, go to **Setting > Server > Configuration**, and click Public Push button to check that the client token is registered.
2. iOS Sign Certificate
On the EMM Admin Portal, go to **Advanced > Certificate > External Certificate** and check that the iOS Sign Cert and iOS Signing Root CA Cert are registered.

D.1.2 Generating and registering an MDM APNs certificate

To generate the MDM APNs certificate, you should download the certificate from the EMM Admin Portal and send it to SDS EMM technical support team to get vendor signed. After then, follow the steps below to issue the certificate on the Apple Push Certificates Portal.

Downloading the request file for MDM APNs

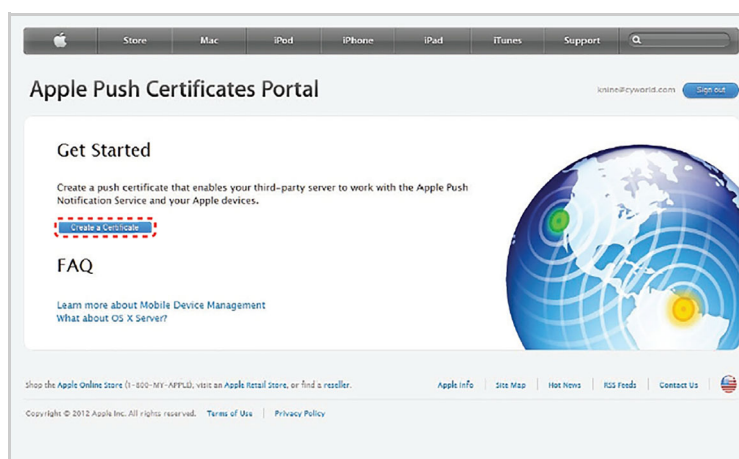
To generate a certificate, the CSR (Certificate Signing Request) file is a prerequisite. CSR file should include the information of the EMM Admin Portal such as the domain name, key value, etc. and require a vendor signature. Therefore, download the CSR file by following the steps below and send the CSR file to EMM technical support team for getting a vendor signature.

1. Go to **Setting > Server > Configuration** in the EMM Admin Portal.
2. Click **Public Push** on the top of the window and click **APNs** tab.
3. Click **Generate Request** in the **Agent** area then the Certificate Signing Request (CSR) file is downloaded to the administrator's PC.
4. The generated MDM APNs certificate as the Agent certificate is not added the vendor signature. Send the generated csr file to the EMM technical support team and get the csr file with the vendor signature added.
 - Without the vendor signature added, the CSR file will not correctly perform APNs communication.

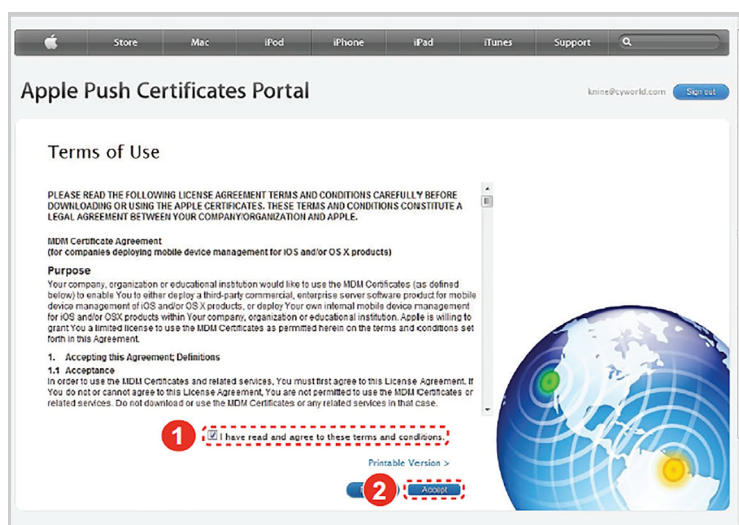
Issuing MDM APNs certificate

You must register the `csr` file, which you have received from the EMM technical support team, on the Apple Push Certificates Portal.

1. Log into the Apple Push certificate portal (<https://identity.apple.com/pushcert>).
2. Click **Create a Certificate**.



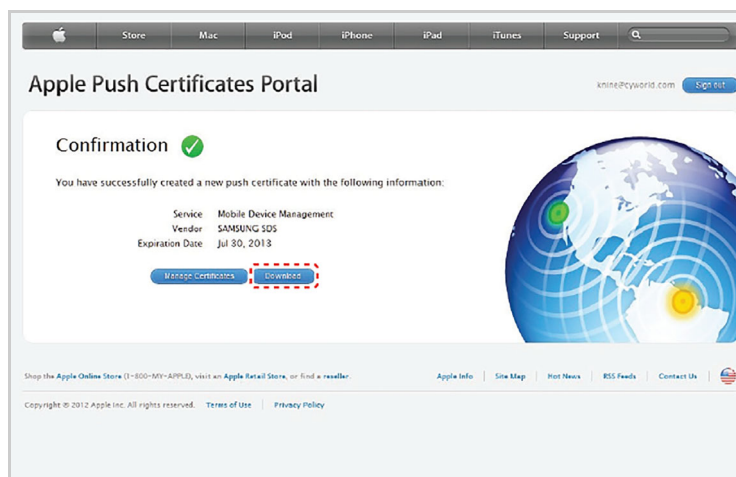
3. Read Terms of Use and check **I have read and agree to these terms and conditions**, then click **Accept**.



4. Click **Choose File**, then select `csr` file.
5. Click **Upload**.



6. Click **Download** in order to download `MDM_SAMSUNG_SDS_Certificate.pem` file.



Uploading the MDM APNs certificate

To upload the downloaded `MDM_SAMSUNG_SDS_Certificate.pem` to Admin Portal, follow the steps below:

1. Go to **Setting > Server > Configuration** in the EMM Admin Portal.
2. Click **Public Push** on the top of the window and click **APNs** tab.
3. Click **Upload APNs Certificate** in the **Agent** area, select the `MDM_SAMSUNG_SDS_Certificate.pem` file, and click **OK**.
4. The uploaded subject information of certificate and the expiration date appear on the top of the window.
The MDM APNs certificate registered can be checked in **Certificate > External Certificate** as `APNs_MDM_Certificate`.

MDM APNs certificate generation is completed. If you use Samsung SDS Push service, register the certificate information into Push DBMS by referring "[D.1.3, Registering an iOS APNs certificate directly in Push database](#)" on page 126. If you use Public Push service, complete "[D.1.4, Registering the iOS Client](#)" on page 127 step.

D.1.3 Registering an iOS APNs certificate directly in Push database

If you use Samsung SDS Private Push service, you must register the MDM APNs certificate and the App token information into a Push DBMS for communicating between the iOS devices and the server.

To register certificate information on Push DBMS by running a DBMS query, complete the following steps (this instruction is based on MSSQL DBMS):

1. Connect to the database through a tool, MS SQL Server Management Studio etc.
 - An BULK insert authority must be granted to the DB connection account. If the authority is not granted, you must grant it or connect by a SA (System Administrator) account.
2. Copy the MDM APNs certificate generated by your company to the MS SQL server, and register the certificate information by running the DB script below. The red values below must be replaced with the your company's information.
 - APID: An ID for the Push Service. For the MDM APNs certificate, enter EMMA/0/\$Tenant_ID\$.
 - SUBAPPLICATIONTYPE: The value to distinguish certificates using APID. For an MDM APNs certificate, enter 0. For an APP APNs certificate, enter 1.
 - CERTIFICATE_PASS: The password for the certificate
 - EXPIRATIONDATE: Certificate expiration date (YYYY-MM-DD)
 - Directory where the certificate file is installed

```
INSERT INTO PUSH_APNS_CERTIFICATE (APID, SUBAPPLICATIONTYPE,
CERTIFICATE_PASS, CERTIFICATE, EXPIRATIONDATE, STATUS,
LAST_MODIFIED)
SELECT 'EMMA/0/$TenantID$', 0, '$CERTIFICATE_PASSWORD$', *,
'$EXPIRATION_DATE$', '1', GETDATE() FROM OPENROWSET( BULK
N'D:\SamsungSDS\0.installFiles\APNs_Agent.p12', SINGLE_BLOB) rs;
GO
```

3. Copy the App APNs token file (.p8), which is automatically registered on the EMM Admin Portal (Setting > Server > Configuration > Public Push > Client), to the MS SQL server. Register the token information by running the below DB script. The values marked in red below must be replaced with the client's information.
 - APID: ID for Push Service. Enter EMMC/0/\$Tenant_ID\$.
 - SUBAPPLICATIONTYPE: The value to distinguish certificates. Enter 0 except for the MDM APNs certificate.
 - Bundle ID: The unique identifier of your EMM client
 - Team ID: ID given to the development team by Apple
 - Key ID: Authentication key ID

- Directory where the certificate file is installed

```
INSERT INTO PUSH_APNS_TOKENBASED_INFO (APID,
SUBAPPLICATIONTYPE, BUNDLE_ID, SIGNING_KEY, TEAM_ID, KEY_ID,
STATUS, LAST_MODIFIED)
  SELECT 'EMMC/0/$Tenant_ID$', 1, 'com.sds.emm.client', *,
'LLVDH2GU5H', 'PS879B66B6', '1', GETDATE() FROM OPENROWSET(
BULK N'D:\SamsungSDS\0.installFiles\ADEP_APNs_AuthKey_K1237JGH
I.p8', SINGLE_BLOB) rs;
GO
```

When the APNS certificate is updated from the Apple Developer site, you must make the same updates to the Push service. Updating process for the Push Service is the same as the initial registration method indicated above. If you already have a certificate for the same APID and SUB_APP_TYPE, the certificate information should be updated.

D.1.4 Registering the iOS Client

The iOS Generic Client can be distributed through a download URL. Only the version registered to the EMM Admin Portal can be installed to user devices. You must register the version you want to install.

To register the iOS EMM app, complete the following steps:

1. Go to **Setting > EMM Application and Policy > EMM Application**.
2. Click **Add > Newly Register**.
3. On the "Add EMM Application" window, enter the following information. Displayed fields may vary depending on the category and platform.
 - **Category:** Client
 - **Platform:** iOS
 - **Application Name:** It is automatically entered according to the category selection, and the application name can also be modified.
4. Click **Save**.

D.2 Using iOS Client with your certificate

To build iOS Client using your certificate, complete the following steps.

1. Checking prerequisites
["D.2.1, Checking prerequisites" on page 128](#)
2. Setting Apple Push Notification Service (APNs) certificate
["D.2.2, Generating APNs certificates" on page 128](#)
3. Building EMM Client
["D.2.3, Building the EMM Client" on page 137](#)

4. Registering APNs certificate
"D.2.4, Registering APNs certificates" on page 144
5. Setting iOS Sign certificate
"D.2.5, Setting the iOS Sign Certificate" on page 150

D.2.1 Checking prerequisites

The following items are required in order to use EMM on iOS:

- Sign up for ADEP Site: Sign up for the Apple Developer Enterprise Program at <https://developer.apple.com/programs/enterprise/> to build and distribute iOS apps for the enterprise.
- MAC Book: Since EMM is provided to customers in the form of source code, a device based on iOS, MAC is needed.

D.2.2 Generating APNs certificates

EMM requires Apple Push Notification Service (APNs) certificate or APNs token-based information in order to send a Samsung SDS push message to an iOS device. There are two types of iOS APNs certificates. The iOS embedded MDM module only supports MDM APNs certificate type and EMM Client supports both APP APNs certificate and token types.

- MDM APNs certificate: A certificate to use MDM APNs, which sends Push messages from the EMM server to the iOS EMM module.
 - Create the MDM APNs certificate as an Agent certificate in the Admin Portal.
- App APNs certificate: A certificate to use App APNs, which sends Push messages from the EMM server to the EMM application.
 - Create the App APNs certificate as an Client certificate in the Admin Portal.
- APP APNs token: Token-based information to use App APNs, which sends Push messages from the EMM server to the EMM application.
 - You can select either App APNs certificate or App APNs token-based information to set it in Samsung SDS EMM.

D.2.2.1 Generating MDM APNs certificate

To generate a MDM APNs certificate, complete the following steps:

Downloading the request file for MDM APNs

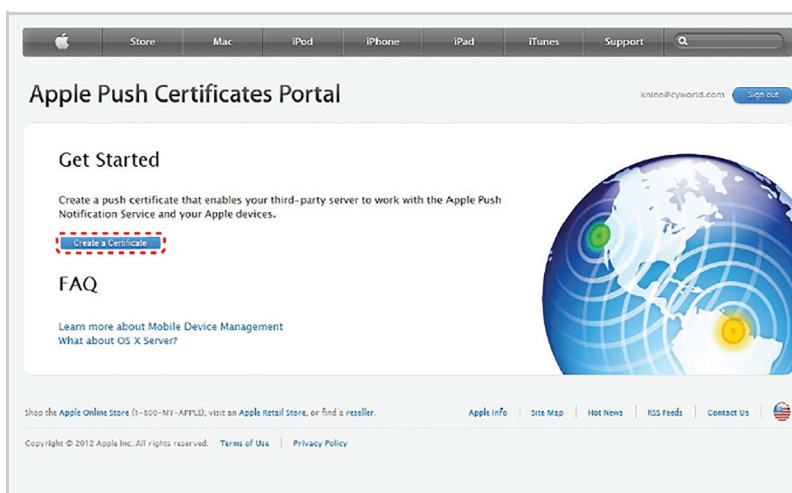
To generate a certificate, the CSR (Certificate Signing Request) file is a prerequisite. CSR file should include the information of the EMM Admin Portal such as the domain name, key value, etc. and require a vendor signature. Therefore, download the CSR file by following the steps below and send the CSR file to EMM technical support team for getting a vendor signature.

1. Go to **Setting > Server > Configuration** in the EMM Admin Portal.
2. Click **Public Push** on the top of the window and click **APNs** tab.
3. Click **Generate Request** in the **Agent** area then the Certificate Signing Request (CSR) file is downloaded to the administrator's PC.
4. The generated MDM APNs certificate as the Agent certificate is not added the vendor signature. Send the generated csr file to the EMM technical support team and get the csr file with the vendor signature added.
 - Without the vendor signature added, the CSR file will not correctly perform APNs communication.

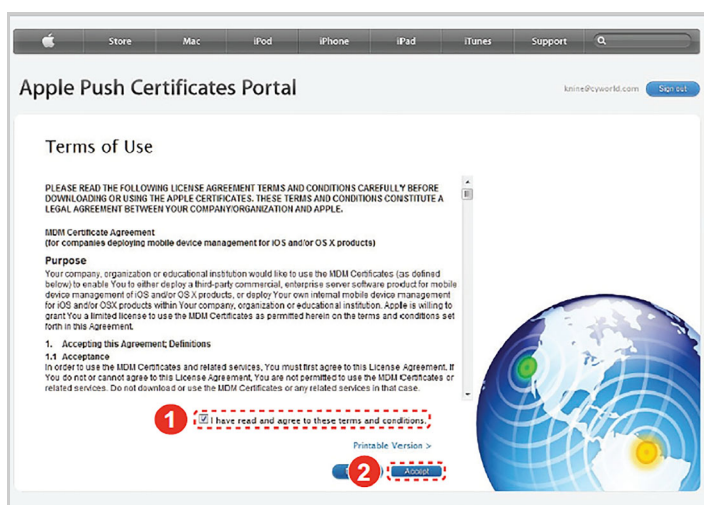
Issuing MDM APNs certificate

You must register the `csr` file, which you have received from the EMM technical support team, on the Apple Push Certificates Portal.

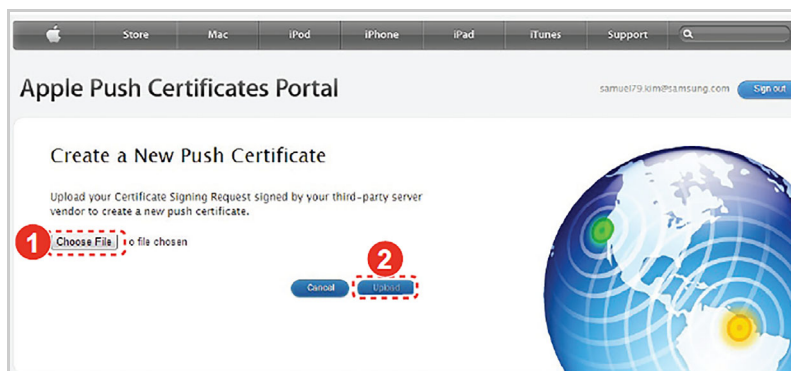
1. Log into the Apple Push certificate portal (<https://identity.apple.com/pushcert>).
2. Click **Create a Certificate**.



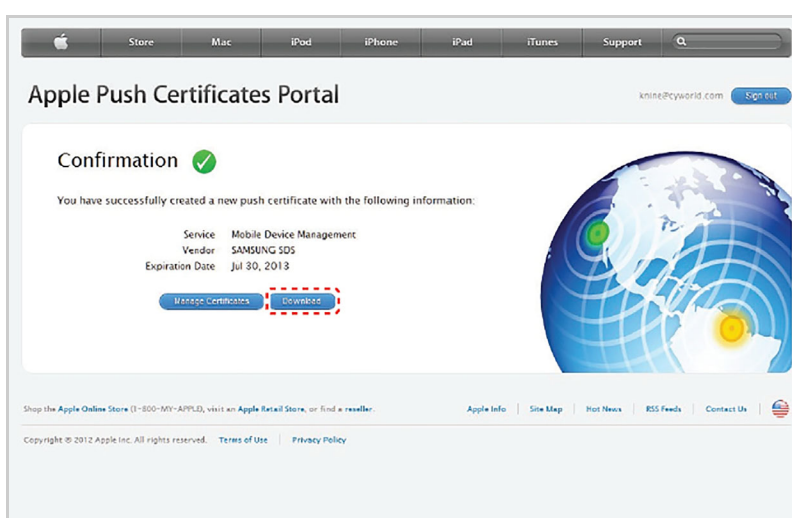
3. Read Terms of Use and check **I have read and agree to these terms and conditions**, then click **Accept**.



4. Click **Choose File**, then select `csr` file.
5. Click **Upload**.



6. Click **Download** in order to download `MDM_SAMSUNG_SDS_Certificate.pem` file.



Uploading the MDM APNs certificate

To upload the downloaded `MDM_SAMSUNG_SDS_Certificate.pem` to Admin Portal, follow the steps below:

1. Go to **Setting > Server > Configuration** in the EMM Admin Portal.
2. Click **Public Push** on the top of the window and click **APNs** tab.
3. Click **Upload APNs Certificate** in the **Agent** area, select the `MDM_SAMSUNG_SDS_Certificate.pem` file, and click **OK**
4. The uploaded subject information of certificate and the expiration date appear on the top of the window.
The MDM APNs certificate registered can be checked in **Certificate > External Certificate** as `APNs_MDM_Certificate`.

MDM APNs certificate generation is completed. Next step is to issue App APNs token/certificate.

D.2.2.2 Generating App APNs certificate

In order to generate an App APNs certificate, you must be registered on ADEP with a company name. Follow the steps below to generate an App APNs certificate. If you want to issue the non-expiring token instead of App APNs certificate, refer ["D.2.2.3, Issuing App APNs token-based information" on page 136](#). If you want to issue the certificate, start from ["Downloading the request file for App APNs" on page 131](#) step.

Downloading the request file for App APNs

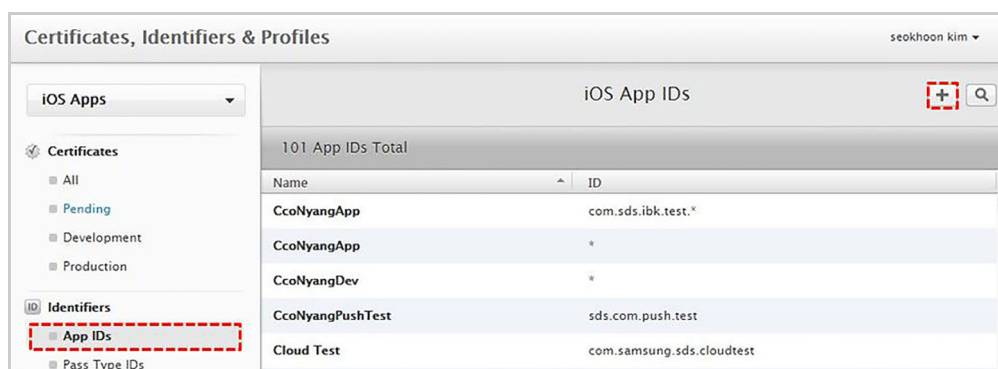
To generate a certificate, the CSR (Certificate Signing Request) file is a prerequisite. CSR file should include the information of the EMM Admin Portal such as the domain name, key value, etc. The CSR file downloaded by following the steps below will be used in step 4 of the ["Issuing MDM APNs certificate" on page 129](#).

1. Go to **Setting > Server > Configuration** in the EMM Admin Portal.
2. Click **Public Push** on the top of the window and click **APNs** tab.
3. Click **Generate Request** in the **Client** area then the Certificate Signing Request (CSR) file is downloaded to the administrator's PC.

Creating App ID

App ID consists of a Team ID and a Bundle ID. Team ID is an ID assigned by ADEP and Bundle ID is to identify a single EMM app and is used when building EMM Client.

1. Go to **Identifiers > App IDs**.
2. Click **+**.



3. Enter App ID information.
 - a. Enter a **Name**.
 - b. Select a **Team ID** for App ID Prefix
 - c. Select **Explicit App ID** and enter **Bundle ID** for App ID Suffix, then click **Continue**.
e.g. com.{Company name}.emm.client

App ID Description

Name:
You cannot use special characters such as @, &, %, ', "

App ID Prefix

Value:

App ID Suffix

Explicit App ID

If you plan to incorporate app services such as Game Center, In-App Purchase, Data Protection, and iCloud, or want a provisioning profile unique to a single app, you must register an explicit App ID for your app.

To create an explicit App ID, enter a unique string in the Bundle ID field. This string should match the Bundle ID of your app.

Bundle ID:

We recommend using a reverse-domain name style string (i.e., com.domainname.appname). It cannot contain an asterisk (*).

d. Select **Push Notifications** among the listed items for App Services.

App Services

Select the services you would like to enable in your app. You can edit your choices after this App ID has been registered.

Enable Services:

- App Groups
- Associated Domains
- Data Protection
 - Complete Protection
 - Protected Unless Open
 - Protected Until First User Authentication
- Game Center
- HealthKit
- HomeKit
- Wireless Accessory Configuration
- iCloud
 - Compatible with Xcode 5
 - Include CloudKit support (requires Xcode 6)
- In-App Purchase
- Inter-App Audio
- Passbook
- Push Notifications
- VPN Configuration & Control

4. Check the entered information, then click **Submit**.

To complete the registration of this App ID, make sure your App ID information is correct, and click the submit button.

App ID Description: **CellWe EMM Client**

Identifier: **LLVDH2GUSH.com.sds.cellweemm.client**

App Groups: Disabled

Associated Domains: Disabled

Data Protection: Disabled

Game Center: **Enabled**

HealthKit: Disabled

HomeKit: Disabled

Wireless Accessory Configuration: Disabled

iCloud: Disabled

In-App Purchase: **Enabled**

Inter-App Audio: Disabled

Wallet: Disabled

Push Notifications: **Configurable**

VPN Configuration & Control: Disabled

5. Click **Done**.

Note: For more information regarding App ID, see <https://developer.apple.com/library/archive/documentation/General/Conceptual/DevPedia-CocoaCore/AppID.html>

Issuing App APNs certificate

To issue app APNs certificates, complete the following steps:

1. Click an App ID created on "Creating App ID" on page 131, then click **Edit**.

CellWe EMM Client com.sds.cellweemm.client

ID

Name: CellWe EMM Client
Prefix: LLVDH2GUSH
ID: com.sds.cellweemm.client

Application Services:

Service	Development	Distribution
App Group	<input type="radio"/> Disabled	<input type="radio"/> Disabled
Associated Domains	<input type="radio"/> Disabled	<input type="radio"/> Disabled
Data Protection	<input type="radio"/> Disabled	<input type="radio"/> Disabled
Game Center	<input checked="" type="radio"/> Enabled	<input checked="" type="radio"/> Enabled
HealthKit	<input type="radio"/> Disabled	<input type="radio"/> Disabled
HomeKit	<input type="radio"/> Disabled	<input type="radio"/> Disabled
Wireless Accessory Configuration	<input type="radio"/> Disabled	<input type="radio"/> Disabled
iCloud	<input type="radio"/> Disabled	<input type="radio"/> Disabled
In-App Purchase	<input checked="" type="radio"/> Enabled	<input checked="" type="radio"/> Enabled
Inter-App Audio	<input type="radio"/> Disabled	<input type="radio"/> Disabled
Wallet	<input type="radio"/> Disabled	<input type="radio"/> Disabled
Push Notifications	<input checked="" type="radio"/> Configurable	<input checked="" type="radio"/> Configurable
VPN Configuration & Control	<input type="radio"/> Disabled	<input type="radio"/> Disabled

2. On "iOS App ID Settings" window, click **Create Certificate** of Production SSL Certificate.

Push Notifications
● Configurable

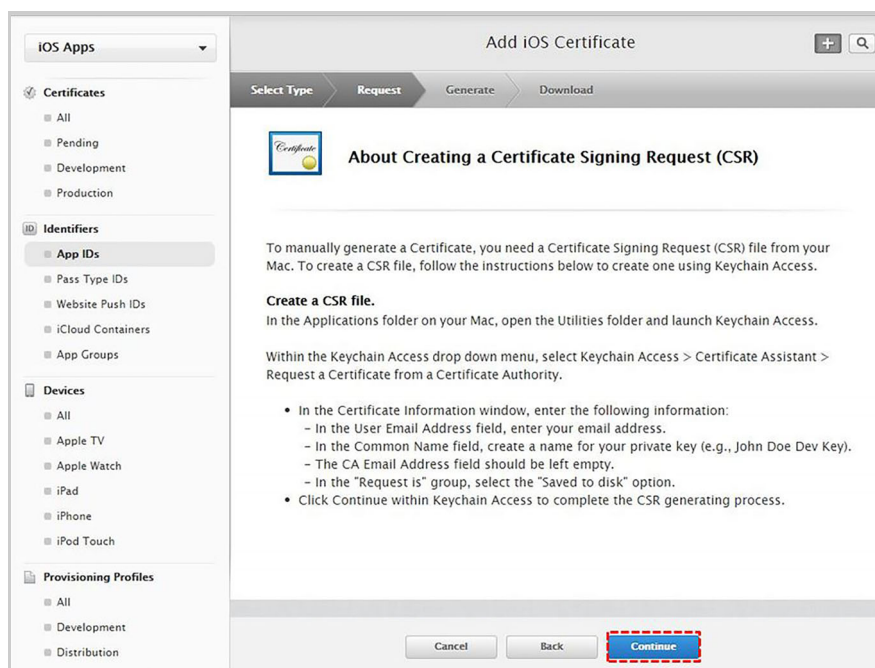
Apple Push Notification service SSL Certificates
To configure push notifications for this iOS App ID, a Client SSL Certificate that allows your notification server to connect to the Apple Push Notification Service is required. Each iOS App ID requires its own Client SSL Certificate. Manage and generate your certificates below.

Development SSL Certificate
Create certificate to use for this App ID.

Production SSL Certificate
Create certificate to use for this App ID.

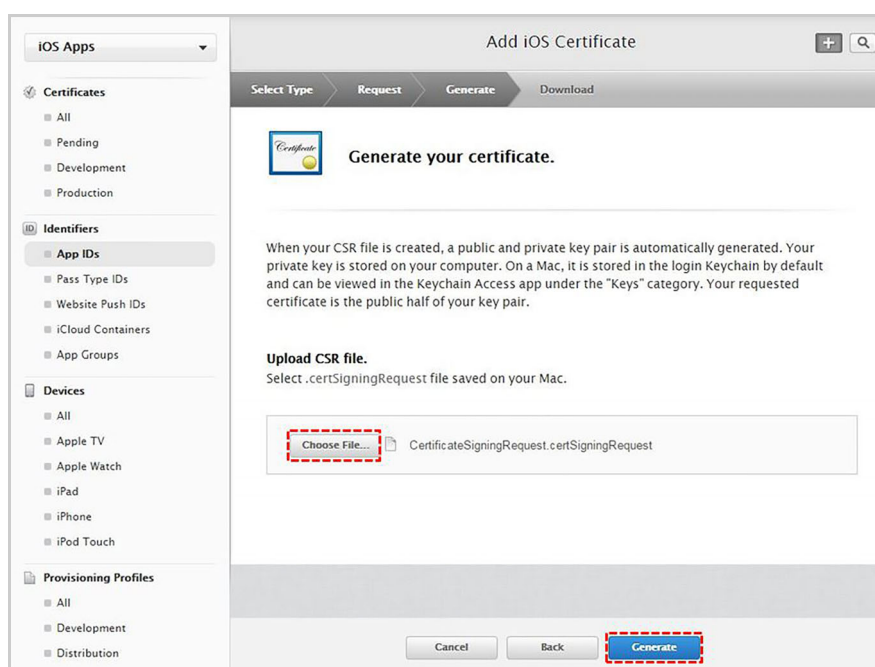
VPN Configuration & Control
 Disabled

3. On About Creating a Certificate Signing Request (CSR) step, click **Continue**.

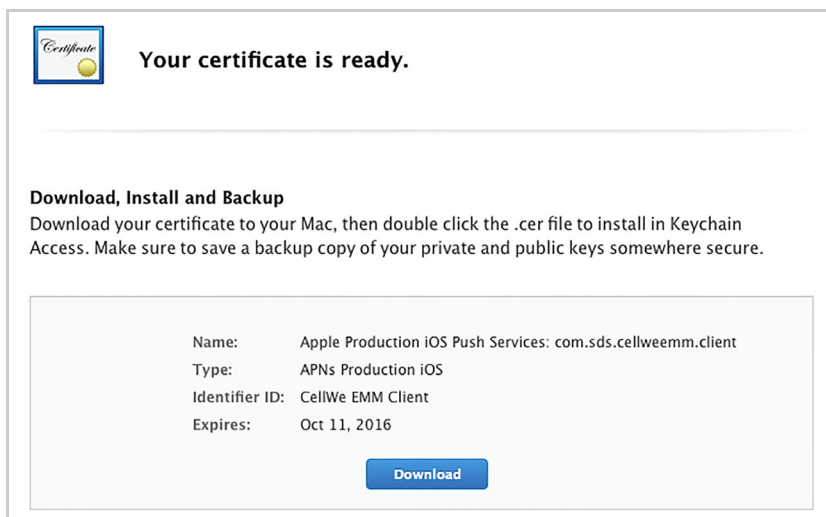


4. On Generate your certificate step, click **Choose File**, then select the CSR file created under the "Downloading the request file for App APNs" on page 131 section.

5. Click **Generate**.



6. Click **Download** and download `aps_production.cer` file.



Uploading the App APNs certificate

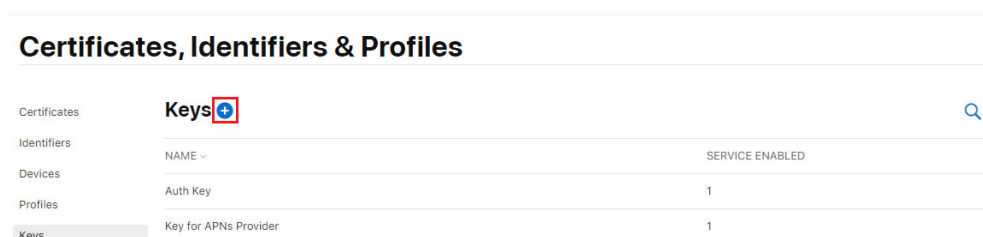
To upload the downloaded `aps_production.cer` file to Admin Portal, follow the steps below:

1. Go to **Setting > Server > Configuration** in the EMM Admin Portal.
2. Click **Public Push** on the top of the window and click **APNs** tab.
3. Click **Upload APNs Certificate** in the **Client** area, select the `aps_production.cer` file, and click **OK**
4. The uploaded subject information of certificate and the expiration date appear on the top of the window.
The MDM APNs certificate registered can be checked in **Certificate > External Certificate** as `APNs_Client_Certificate`.

D.2.2.3 Issuing App APNs token-based information

You can select either using App APNs certificate or using the token type. Using the certificate requires annual renewal, but the token does not expire, which makes it easy to manage. To issue App APNs token-based information, complete the following steps:

1. Click the  button next to the **Keys** category of Certificates, Identifiers & Profiles.



- Fill in the Key Name field, select the **Apple Push Notifications service (APNs)** check box, and then click the **Continue** button.

Certificates, Identifiers & Profiles

< All Keys

Register a New Key Continue

Key Name

You cannot use special characters such as @, &, *, ' , / , - , .


ENABLE	NAME	SERVICE	
<input type="checkbox"/>	Apple Push Notifications service (APNs)	Establish connectivity between your notification server and the Apple Push Notification service. One key is used for all of your apps. Learn more <small>ⓘ You have already reached the maximum allowed number of keys for this service</small>	
<input type="checkbox"/>	MapKit JS	Use Apple Maps on your websites. Show a map, display search results, provide directions, and more. Learn more <small>ⓘ There are no identifiers available that can be associated with the key</small>	Configure
<input type="checkbox"/>	MusicKit	Access the Apple Music catalog and make personalized requests for authorized users. Learn more <small>ⓘ There are no identifiers available that can be associated with the key</small>	Configure

- Click the **Register** button.
- Click the Download button to download the issued Auth key and check the Key ID. The issued Auth key can only be downloaded once. Store it in a safe location.
- Check the Team ID in **Account > Membership**.

Program Resources

- Overview
- Membership**
- People
- Certificates, IDs & Profiles
- CloudKit Dashboard
- Servers
- Code-Level Support

Additional Resources



Membership Details

Your team's membership information and legal agreements.

Membership Information

Program Type	Apple Developer Enterprise Program
Team Name	
Team ID	
Entity Type	In-House / Enterprise

After completing App APNs certificate, you have completed issuing all needed two certificates for APNs communication. As a next step, you must complete "Building the EMM Client" step to distribute to users. After building the EMM Client, you are ready to distribute EMM App to the users.

D.2.3 Building the EMM Client

In order to distribute EMM on an iOS device without Apple's App store, you must build an EMM Client using the Bundle ID created through "Creating App ID" on page 131 and the profile created under "Generating the Distribution Provisioning profile" on page 140. This describes the process of building the `EMM Client.ipa` application for an iOS device.

Note: Customers who have already been using ADEP accounts should skip "Generating the iOS Distribution certificate" on page 138.

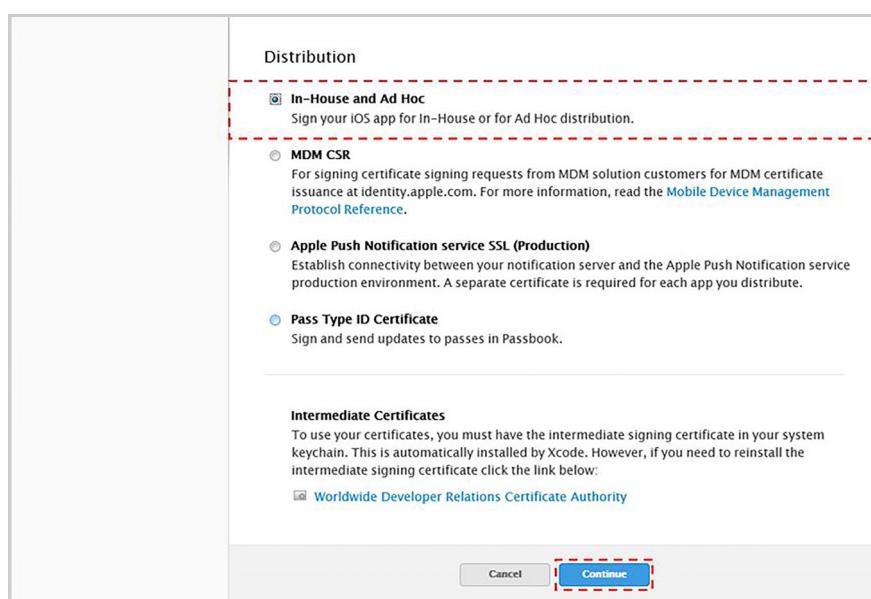
Generating the iOS Distribution certificate

An iOS Distribution certificate is required to distribute the iOS application. ADEP account information is included with the iOS Distribution certificate. The ADEP account information will be included in the Distribution Provisioning profile upon the EMM Client build. To generate the iOS Distribution certificate, complete the following steps:

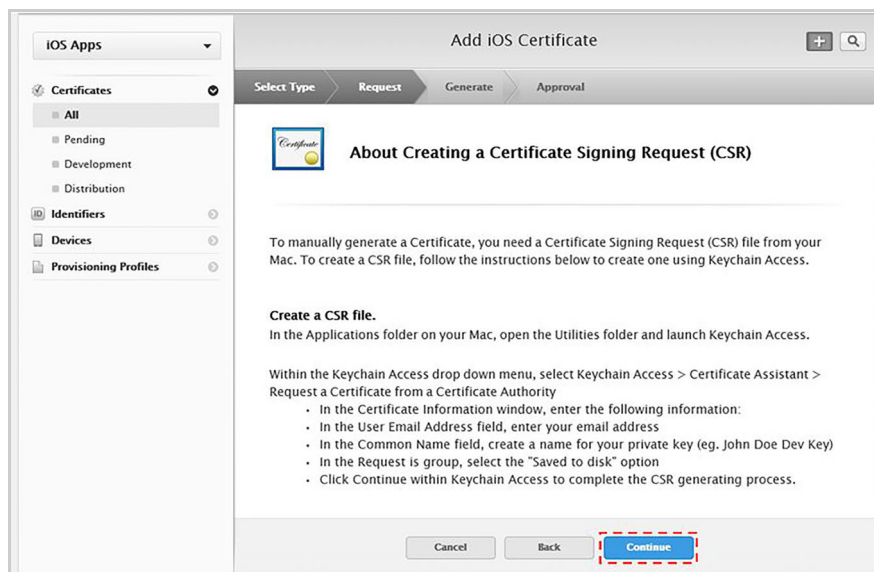
1. Log into Apple Dev Center(<https://developer.apple.com/account/>).
2. Go to **Certificates > Production**.
3. Click + on the upper right side of the window.



4. Select **In-House and Ad Hoc** and click **Continue**.

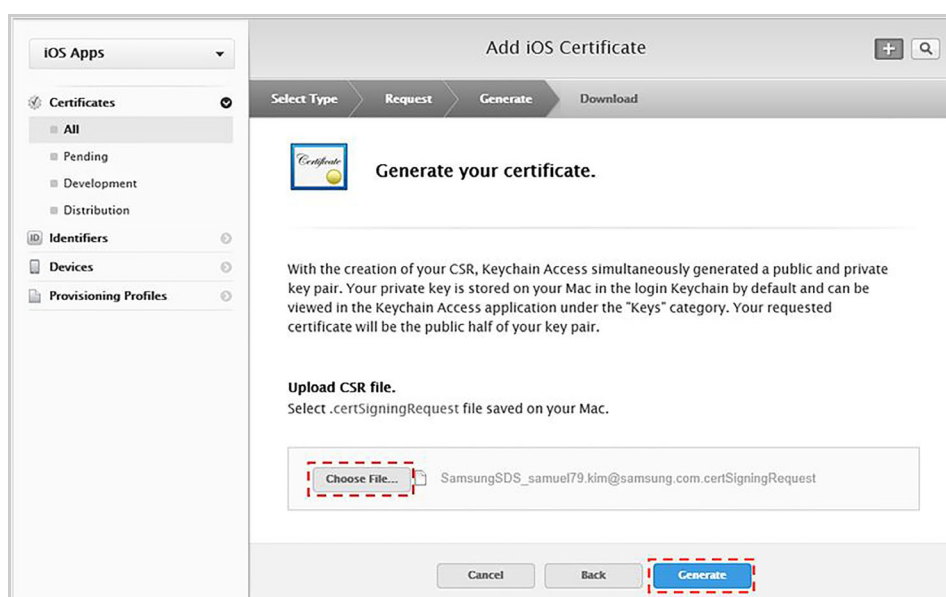


5. On About Creating a Certificate Signing Request (CSR) step, click **Continue**.



6. With Generate your certificate step, click **Choose File**, then select CSR file created on ["Downloading the request file for MDM APNs"](#) on page 128 section.

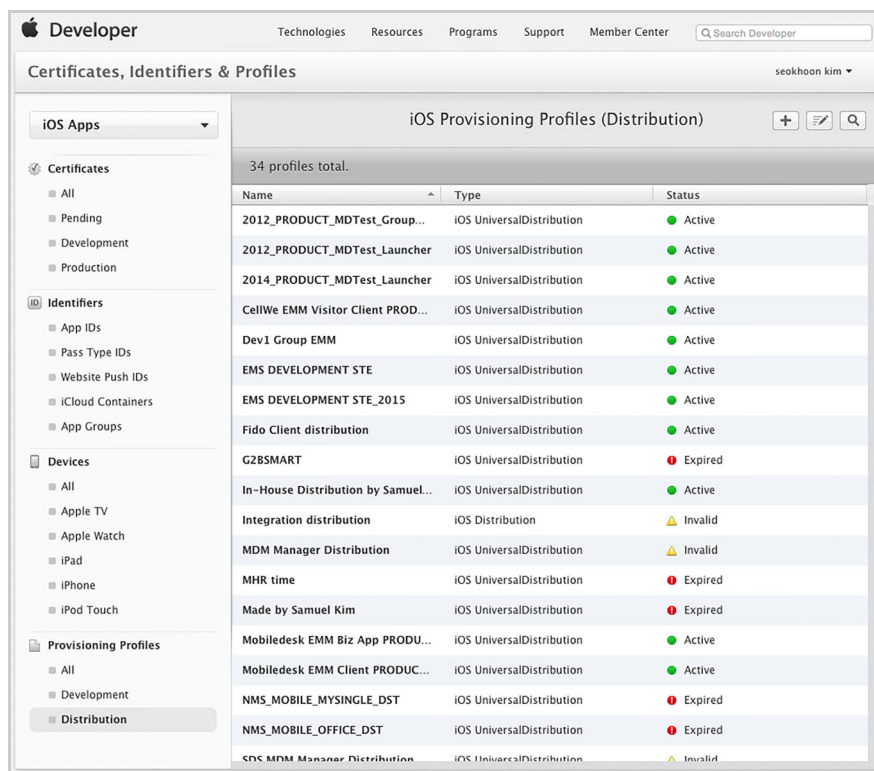
7. Click **Generate**.



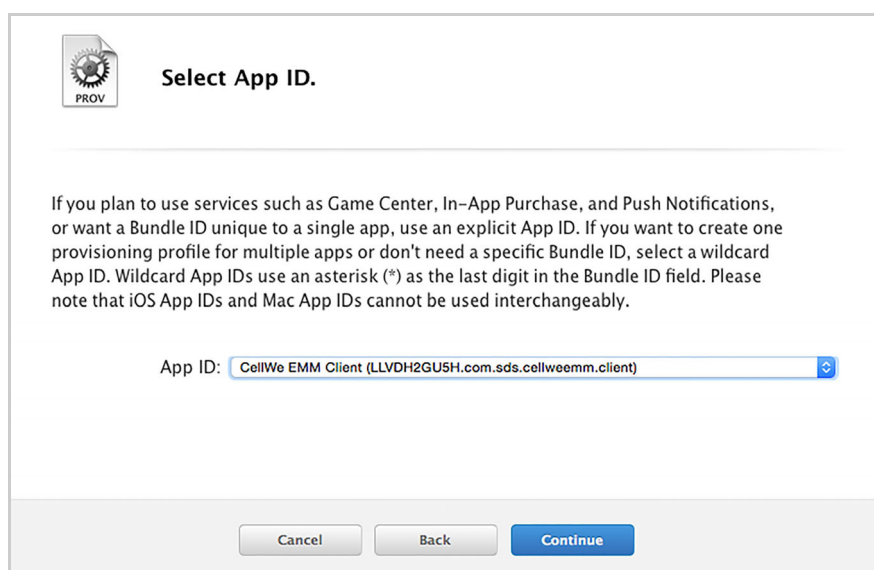
Note: You must be careful not to revoke the distributed certificate. Once the distribution certificate is deleted, you are required to rebuild both the Distribution Provisioning profile and EMM Client.

Generating the Distribution Provisioning profile

1. Log into Apple Dev Center(<https://developer.apple.com/account/>).
2. Go to **Provisioning Profiles > Distribution**.
3. Click + on the upper right side of the window.

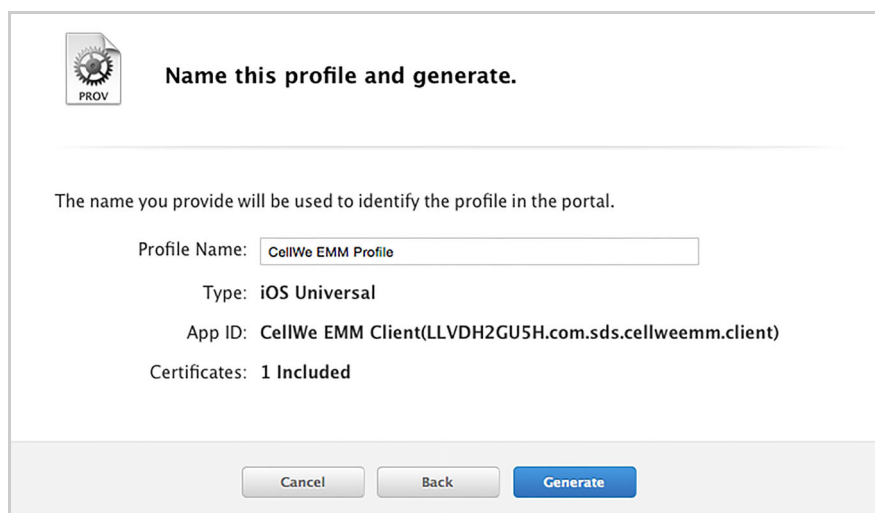



4. Create the Distribution Provisioning profile.
 - a. For Distribution Method, select **In House** and click **Continue**.
 - b. For App ID, select an App ID created on "[Creating App ID](#)" on page 131 .



- c. Select the Distribution certificate established under "[Generating the iOS Distribution certificate](#)" on page 138, then click **Continue**.

d. Enter a **Profile Name** and click **Generate**.



 **Name this profile and generate.**

The name you provide will be used to identify the profile in the portal.

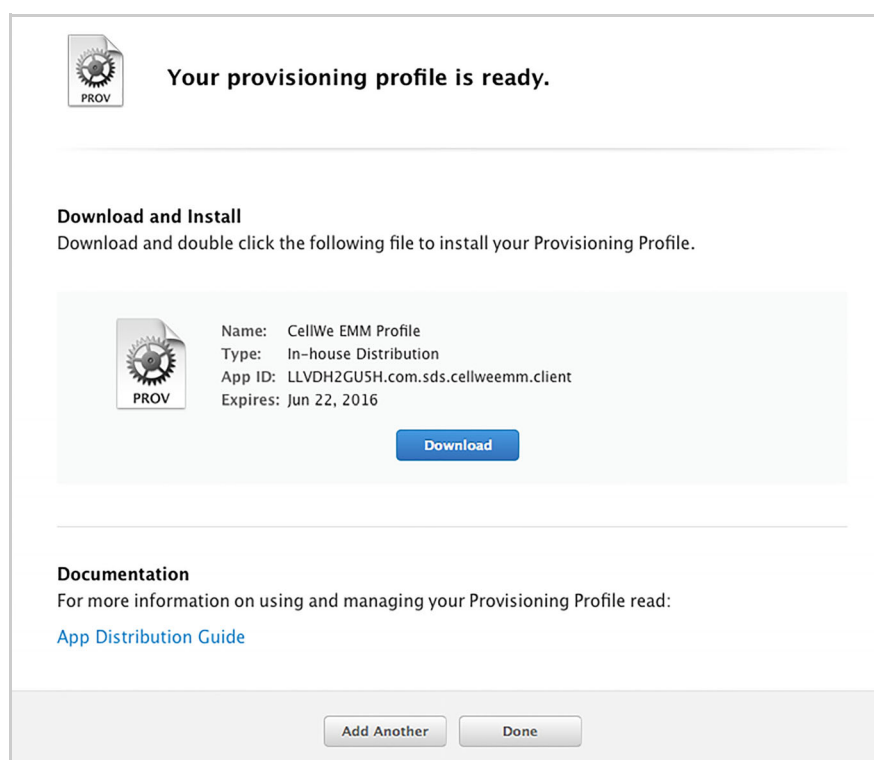
Profile Name:


Type: iOS Universal

App ID: CellWe EMM Client(LLVDH2GU5H.com.sds.cellweemm.client)


Certificates: 1 Included

e. Click **Download**.



 **Your provisioning profile is ready.**

Download and Install
Download and double click the following file to install your Provisioning Profile.

 Name: CellWe EMM Profile
Type: In-house Distribution
App ID: LLVDH2GU5H.com.sds.cellweemm.client
Expires: Jun 22, 2016

Documentation
For more information on using and managing your Provisioning Profile read:
[App Distribution Guide](#)

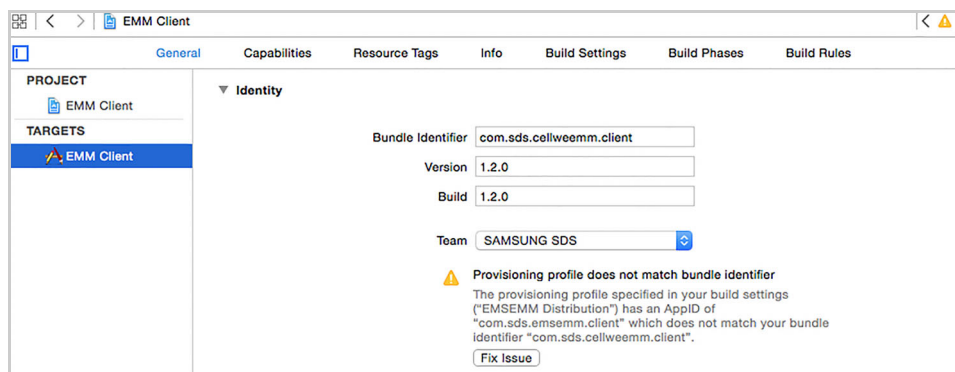
5. Double click the Distribution Provisioning profile (.mobileprovision) to add to Xcode Organizer. Xcode Organizer is a screen where you can view documentation such as device and repository management.

- Note:**
- If Xcode Organizer does not work properly, right click on the file and go to **Open with > Xcode.app**.
 - You must install Xcode individually.

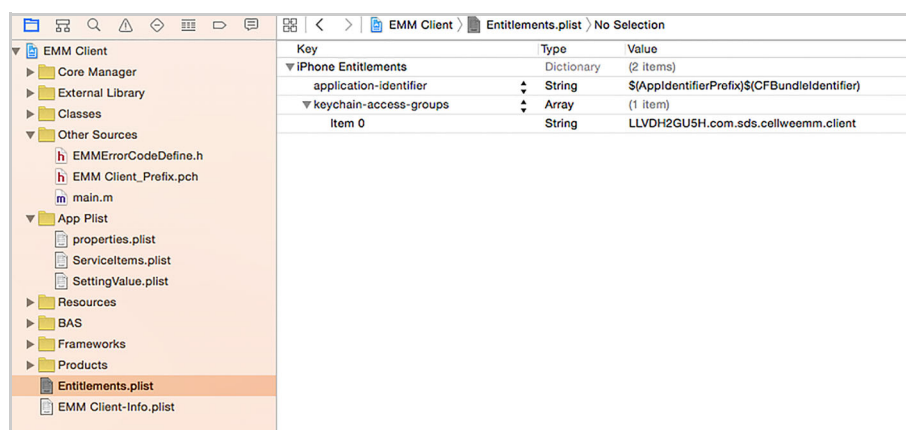
Setting the Bundle ID

1. Start Xcode. Xcode is an integrated development environment used to develop software for Apple products, such as macOS, iOS, and iPadOS.

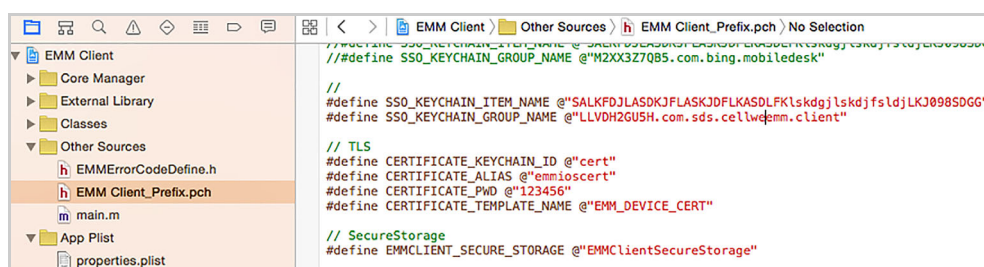
2. Execute the officially-released EMM Client project.
3. On Project Navigator, select an EMM Client project, then click EMM Client under **TARGETS**.
4. For **Bundle Identifier** on the General tab, enter the Bundle ID, created on "Creating App ID" on page 131.



5. Change the **keychain-access-groups** value.
 - a. Go to **EMM Client > Products**.
 - b. Click `Entitlements.plist` file.
 - c. Change **keychain-access-groups** value to **{Team ID}.{Bundle ID}**.



6. Change **SSO_KEYCHAIN_GROUP_NAME** value.
 - a. Go to **EMM Client > Other Sources**.
 - b. Click `EMM_Client_Prefix.pch` file.
 - c. Change **SSO_KEYCHAIN_GROUP_NAME** to **keychain-access-groups** value.

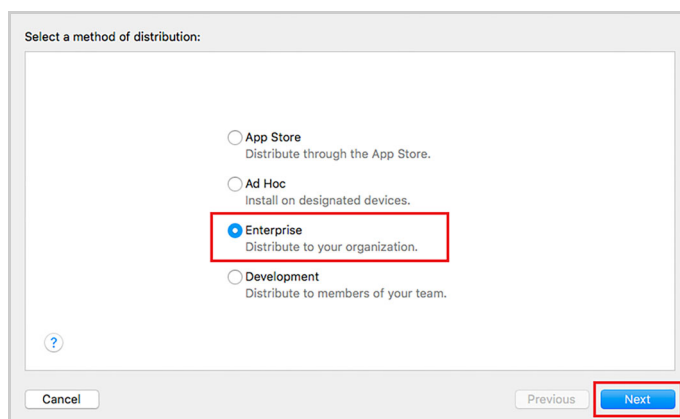


Modifying the EMM Client setting

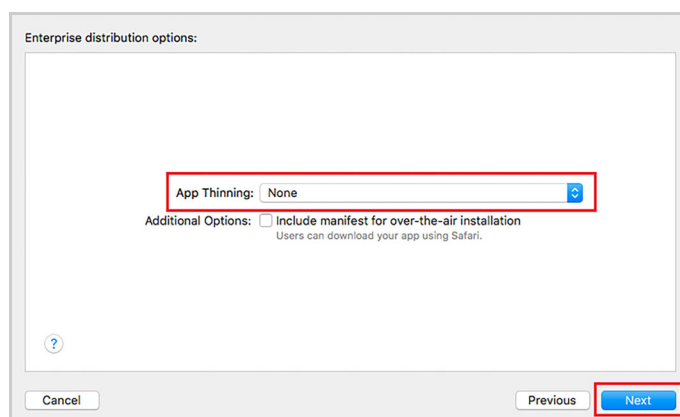
For more details regarding EMM Client settings, see the chapter 5 that explains EMM Client Development for iOS in the *Samsung SDS EMM Developer's Guide*.

Building the EMM Client

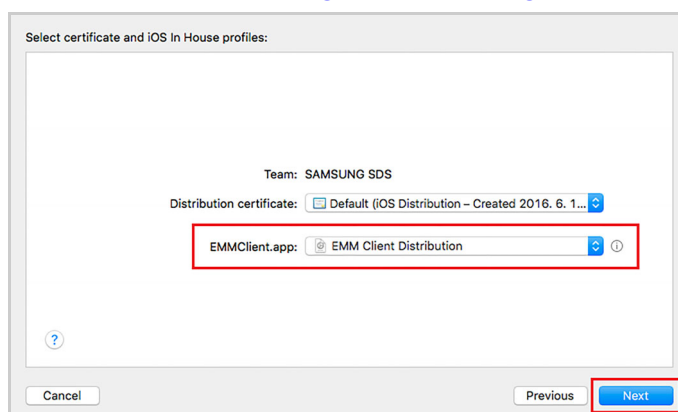
1. Start Xcode. Xcode is an integrated development environment used to develop software for Apple products, such as macOS, iOS, and iPadOS.
2. Go to **Product > Archive**.
3. From the Archive list, select EMM Client and click **Export** at the right **Archive Information**.
4. Under Select a method for distribute step, select **Enterprise** and click **Next**.



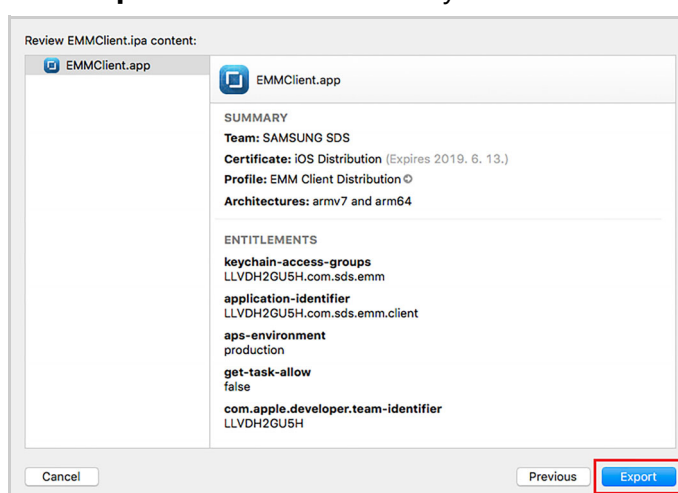
5. Select the **None** in the App Thinning and click **Next**.



6. Select Distribution Provisioning profile created in ["Generating the Distribution Provisioning profile"](#) on page 140 and click **Next**.



7. Click **Export** and select a directory which to save the `EMM Client.ipa` file.



After building the EMM Client, you are ready to distribute EMM App to the users. If you use Samsung SDS Push service, register the certificate information into Push DBMS by referring ["D.2.4, Registering APNs certificates"](#) on page 144. If you use Public Push service, complete ["D.2.5, Setting the iOS Sign Certificate"](#) on page 150 step.

D.2.4 Registering APNs certificates

If you use Samsung SDS Private Push service, you must register information of MDM APNs certificate and App Token into Push DBMS by using Public Push Tool or entering MSSQL query directly. Downloading iOS APNs certificate.

To copy the iOS APNs certificate, you should download the APNs certificate from ["D.2.2, Generating APNs certificates"](#) on page 128. To download the APNs certificate, complete the following steps:

1. Go to **Setting > Server > Configuration** in the EMM Admin Portal.
2. Click **Public Push** on the top of the window and click **APNs** tab.
3. Click **Download Cert** in the **Agent** and **Client** field.

4. Enter the password to set the password for the certificate, then click **OK**.

- For MDM APNs: APNs_MDM_Certificate.p12
 - For App APNs: APNs_Client_Certificate.p12
- If you use an App token, prepare the token file to upload.

D.2.4.1 Registering an iOS APNs certificate directly in Push database

After copying the APNs certificate to the Push server, the APNs certificate information must be registered on the Push DBMS. Use the Public Push Tool provided or run MSSQL DBMS query manually for the registration.

Using Public Push Tool

To enter the APNs certificate, run the Public Push tool provided after Push installation. How to run the tool and the input values:

- The file to run: PublicPush/publicPush.jar
- How to run the tool:
Depending on the authentication method, enter the parameters as shown below and press the Enter key.

i) Certificate-based authentication, using the Public Push tool with .p12 file

```
java -jar publicPush.jar {AUTH_TYPE} {DB_PASSWORD} {APID}
{SUB_APP_TYPE} {CERT_FILE_PATH} {CERT_PASSWD}
{CERT_EXPIRATION_DATE} {PUSH_HOME}
```

Item	Description
AUTH_TYPE	When using the certificate as an authentication type, enter 0.
DB_PASSWORD	Password for the account of the Push server database. If you connect to the MSSQL server via Windows authentication, this password will be ignored.
APID	The unique application ID used by the Push services <ul style="list-style-type: none"> • For an MDM APNs certificate, enter EMMA/0/\$Tenant_ID\$, • For an APP APNs certificate, enter EMMC/0/\$Tenant_ID\$
SUB_APP_TYPE	When using multiple APNs certificates for a single APID, the item values are used to distinguish certificates. <ul style="list-style-type: none"> • 0: If you register an MDM Agent certificate • 1: If you register another certificate
CERT_FILE_PATH	The path to the APNs certificate file
CERT_PASSWD	The password for the APNs certificate
CERT_EXPIRATION_DATE	APNs certificate expiration date (YYYY-MM-DD)
PUSH_HOME	Directory where the Push server is installed EX) C:\SamsungSDS\Push\{Version}

ii) Token-based authentication, using the Public Push tool with .p8 file

```
java -jar publicPush.jar {AUTH_TYPE} {DB_PASSWORD} {APID}
{SUB_APP_TYPE} {KEY_FILE_PATH} {BUNDLE_ID} {TEAM_ID} {KEY_ID}
{PUSH_HOME}
```

Item	Description
AUTH_TYPE	When using the token as an authentication type, enter 1.
DB_PASSWORD	The password for the account of the Push server database. If you connect to the MSSQL server via Windows authentication, this password will be ignored.
APID	The unique application ID used by the Push services
SUB_APP_TYPE	When using multiple APNs certificates for a single APID, the item values are used to distinguish certificates. <ul style="list-style-type: none"> • 0: If you register MDM Agent certificate • 1: If you register other certificate
KEY_FILE_PATH	The path to the authentication token signature key (p8) file
BUNDLE_ID	The unique identifier of your EMM client (Topic)
TEAM_ID	The ID given to the development team by Apple
KEY_ID	Key ID of the authentication token signature key (p8) file
PUSH_HOME	Directory where the Push server is installed EX) C:\SamsungSDS\Push\{Version}

When the APNs certificate is updated from the Apple Developer site, you must make the same updates to the Push service. Updating the certificate used for the Push Service is the same as the initial registration method indicated above. If you already have a certificate for the same APID and SUB_APP_TYPE, an update confirmation message is displayed. Enter **Yes** to update the certificate.

Error Messages the Public Push tool

This section describes how to troubleshoot error messages that occur when using the Public Push tool.

Error message	Cause	Solution
APNs certification loading failed. See below detail messages	The tool cannot read the {CERT_FILE_PATH/KEY_FILE_PATH} file.	Refer to the message content and make sure the certificate path is correct and you have the necessary file read permissions.
Cannot read DB information from jdbc.properties file. See below detail messages	The Push installation directory cannot read the jdbc.properties file	Enter information registered at the Apple: APNs certificate, the password for the certificate, and the certificate validity period.
JDBC driver loading failed. See below detail messages	Cannot load the JDBC driver.	Make sure that the {oracle/mssql/mysql}-connector.jar file is in the Push installation directory.

Error message	Cause	Solution
DB connection failed. See below detail messages	Cannot connect to the DB.	Confirm the message content and make sure your name and the DB information is configured correctly, or the firewall connection to the DB server is required.
SubApplicationType should be Number	If the SUB_APP_TYPE, entered during the program execution, is not a number	Enter the required number value for SUB_APP_TYPE.

Running MSSQL Query directly

To register certificate information on Push DBMS by running a DBMS query, complete the following steps (this instruction is based on MSSQL DBMS):

1. Connect to the database through a tool, MS SQL Server Management Studio etc.
 - An BULK insert authority must be granted to the DB connection account. If the authority is not granted, you must grant it or connect by a SA (System Administrator) account.
2. Copy a certificate file on the MS SQL server.
 - Certificate-based information: A certificate with the p12 file extension and converted to FIPS-140 mode
 - Token-based information: A signing key with the p8 file extension
- 3-1. If you use certificate-based information for APNs authentication information, run the following DB scripts to register the MDM (EMMA) and App (EMMC) APNs certificate information.

The bolded APID, Certificate Password, Certificate expiration date, and Certificate location can be changed according to the system.

 - **APID**: An ID for the Push Service. For the MDM APNs certificate, enter EMMA/0/\$Tenant_ID\$. For the APP APNs certificate, enter EMMC/0/\$Tenant_ID\$.
 - **SUBAPPLICATIONTYPE**: The value to distinguish certificates using APID. For an MDM APNs certificate, enter 0. For an APP APNs certificate, enter 1.
 - **CERTIFICATE_PASS**: The password for the certificate

- EXPIRATIONDATE: Certificate expiration date (YYYY-MM-DD)
Directory where the certificate file is installed

```

INSERT INTO PUSH_APNS_CERTIFICATE
(APID, SUBAPPLICATIONTYPE, CERTIFICATE_PASS, CERTIFICATE, EXPIRATION
DATE, STATUS, LAST_MODIFIED)
    SELECT '$APID_FOR_EMMA$', 0, '$CERT_PASSWORD$', *, '2017-07-
28', '1',
getdate() FROM OPENROWSET( BULK N'C:\Program Files\Microsoft SQL
Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\APNs_MDM_Certificate.p12',
SINGLE_BLOB) rs;

INSERT INTO PUSH_APNS_CERTIFICATE
(APID, SUBAPPLICATIONTYPE, CERTIFICATE_PASS, CERTIFICATE, EXPIRATION
DATE, STATUS, LAST_MODIFIED)
    SELECT 'APID_FOR_EMMC', 1, 'CERT_PASSWORD', *, '2017-07-28', '1',
getdate() FROM OPENROWSET( BULK N'C:\Program Files\Microsoft SQL
Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\APNs_Client_Certificate.p12
',
, SINGLE_BLOB) rs;

go

```

- 3-2. If you use token-based information for APNs authentication information for the App APNs, run the following DB scripts to register the token-based EMM Client information. The bolded APID, the EMMC App's BundleID (Topic), TeamID, KeyID, and the SigningKey's location can be changed according to the system.
- APID: ID for Push Service. Enter EMMC/0/\$Tenant_ID\$.
 - SUBAPPLICATIONTYPE: The value to distinguish certificates. Enter 0 except for the MDM APNs certificate.
 - Bundle ID: The unique identifier of your EMM client
 - Team ID: ID given to the development team by Apple
 - Key ID: Authentication key ID

- Directory where the certificate file is installed

```

INSERT INTO PUSH_APNS_TOKENBASED_INFO
(
  APID,
  SUBAPPLICATIONTYPE,
  BUNDLE_ID,
  SIGNING_KEY,
  TEAM_ID,
  KEY_ID,
  STATUS,
  LAST_MODIFIED
)
SELECT
  '$APID_FOR_EMMC$',
  1,
  '$BUNDLE_ID_FOR_EMMC$',
  *,
  '$TEAM_ID_OF_APP_ACCOUNT$',
  '$KEY_ID_OF_SIGNING_KEY$',
  '1',
  getdate ()
FROM OPENROWSET( BULK N'C:\Program Files\Microsoft SQL
Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\ADEP_APNs_AuthKey_K1237J
GHI.p8', SINGLE_BLOB) rs;

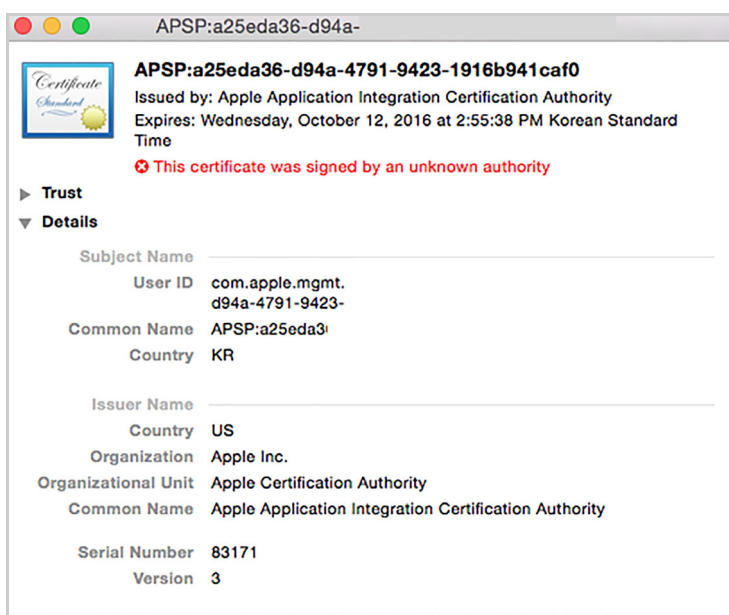
```


Configuring APNs Topic

When the MDM APNs certificate is registered to the Admin Portal, the APNs Topic value is exported and automatically set. If APNs Topic value is changed, you need to match this with the user ID.

To change the APNs Topic value, complete the following steps:

1. Double click the MDM APNs certificate generated under "[D.2.2.1, Generating MDM APNs certificate](#)" on page 128.
2. Check the **User ID** in the pop-up window.



3. Set the User ID for the MDM APNs certificate as the APNs Topic value on the EMM Admin Portal.
 - a. Log in to the EMM Admin Portal.
 - b. Go to **Setting > Server > Configuration**.
 - c. In the **Category: MDM**, Change the **APNs Topic** to the User ID of the MDM APNs certificate.
 - d. Click  on the upper side of the window and apply the changes.

Configuration

Options	Value
Category: MDM (20)	
39 APNs Topic for iOS	com.apple.mgmt.External.61c3238d-4b19-4646-af888711c32d
40 Attestation Api Key	4F509BC98750-4B19-4646-af888711c32d
41 Attestation Server URL	https://attest-api.mdm.com
42 Daily retries for device commands in request	0
43 Direct boot command polling interval for Android (min)	0
44 Camera Option from Lock Screen for iOS	TRUE
45 Keepalive Interval Period (hr, Android Only)	6
46 Reminder to Go Off Before Keepalive Expiration (hr, Android Only)	1
47 Keepalive Duration (days, set 0 to disable, Android Only)	0

D.2.5 Setting the iOS Sign Certificate

The iOS Sign Certificate (`iOSSigningCert.p12`) is a server certificate necessary for communication between the EMM server and iOS devices. Apple MDM specifications require a digital signature with iOS Sign Certificate when the EMM server sends data to iOS devices.

D.2.5.1 Generating iOS Sign Certificate

The default public key for iOS Sign Certificate is RSA (2048bit) and the signature algorithm is Sha256RSA. The examples below shown in bold should be modified according to the installation environment. If you need multiple certificates, repeat steps 3 through 6 after the first certificate is issued.

Note: For more information on Java keytool, see docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

1. Create the directory iOS Sign Certificate in a specific location you want.
2. Open a command prompt and go to iOS Sign Cert directory.
3. Generate the self-signed Root key storage.
 - a. Enter the followings in the command prompt.


```
keytool -genkeypair -v -alias RootCA_alias -keystore RootCA.jks -keyalg RSA -keysize 2048 -validity 36500 -ext KeyUsage:critical="keyCertSign" -ext BasicConstraints:critical="ca:true"
```

 - Enter Alias of Root certificate in **RootCA_alias**.
 - **RootCA.jks** is Root CA Keystore file.
 - b. Enter the Root key storage password which should have at least 6 letters.
 - c. Enter the Root key storage password again.
 - d. Enter the answers to the questions shown in the command prompt:
 - What is your first and last name?
 - What is the name of your organizational unit?
 - What is the name of your organization?
 - What is the name of your City or Locality?
 - What is the name of your State or Province?
 - What is the two-letter country code for this unit?
 - e. If the confirmation appears and if there is nothing wrong with it, enter Y.
 - f. Enter the key password for RootCA_alias.
 - g. Enter the key password for RootCA_alias again.
 - h. Check that the `RootCA.jks` file was created in iOS Sign Cert directory.
4. Export the self-signed Root key storage certificate.
 - a. Enter the followings in the command prompt.


```
keytool -export -v -alias RootCA_alias -file RootCA.crt -keystore RootCA.jks -rfc
```

 - **RootCA.crt** is the Root CA certificate file.
 - b. Enter the Root key storage password.
 - c. Check that `RootCA.crt` was created in the iOS Sign Cert directory.

5. Generate the server Keystore file.

- a. Enter the followings in the command prompt.

```
keytool -genkeypair -v -alias "EMM Server" -keystore
iOSSigningCert.jks -keyalg RSA -keysize 2048 -validity 36500
```

- The file, **iOSSigningCert.jks**, is server Keystore file.
- b. Enter the server key storage password which should have at least 6 letters.
- c. Enter the server key storage password again.
- d. Enter the answers to the questions shown in the command prompt:
- What is your first and last name?
 - What is the name of your organizational unit?
 - What is the name of your organization?
 - What is the name of your City or Locality?
 - What is the name of your State or Province?
 - What is the two-letter country code for this unit?
- e. If the confirmation appears and if there is nothing wrong with it, enter Y.
- f. Enter key password for EMM Server.
- g. Enter the key password for EMM Server again.
- h. Check that **iOSSigningCert.jks** was created in iOS Sign Cert directory.

6. Generate server certificate.

- a. Enter as follows in the command prompt.

```
keytool -certreq -v -alias "EMM Server" -keystore
iOSSigningCert.jks -file rsaOneCert.csr
```

- b. Enter the server key storage password.
- c. Check that **rsaOneCert.csr** was created in iOS Sign Cert directory.

```
keytool -gencert -v -alias RootCA_alias -keystore RootCA.jks
-infile rsaOneCert.csr -validity 3650 -outfile iOSSigningCert.crt
-rfc -ext KeyUsage:critical="digitalSignature" -ext
EKU="serverAuth"
```

- The file, **iOSSigningCert.crt**, is a digitally signed certificate file.
- d. Enter the server key storage password.

7. Import the Root certificate to server Keystore.

- a. Enter as follows in the command prompt.

```
keytool -import -v -alias RootCA_alias -file RootCA.crt -
keystore iOSSigningCert.jks -storetype JKS
```

- b. Enter the server key storage password.
- c. When the question asking if you trust the certificate, and if there is nothing wrong with it, enter Y.

```
keytool -import -v -alias "EMM Server" -file iOSSigningCert.crt
-keystore iOSSigningCert.jks -storetype JKS
```

- d. Enter server key storage password.
8. Generate P12 certificate file in server Keystore.
 - a. Enter as follows in the command prompt.


```
keytool -importkeystore -srkeystore iOSSigningCert.jks
-destkeystore iOSSigningCert.p12 -deststoretype PKCS12
-srcalias "EMM Server"
```


 - The file, `iOSSigningCert.p12`, is P12 server certificate file.
 - b. Enter the key storage password for the object (`iOSSigningCert.p12`).
 - c. Enter the key storage password for the object (`iOSSigningCert.p12`) again.
 - d. Enter the key storage password for source (`iOSSigningCert.jks`).
 - e. Check that `iOSSigningCert.p12` certificate was created in the iOS Sign Cert directory.
9. Convert the certificate to FIPS140 mode with the tool provided.

Note: Enter the command below to check `iOSSigningCert.p12`.

```
keytool -list -keystore iOSSigningCert.p12 -storetype pkcs12
```

D.2.5.2 Registering iOS sign certificate

This part of the chapter describes how to register iOS sign certificate on the EMM Admin Portal.

1. Log in to the EMM Admin Portal.
2. Go to **External certificates**.
3. Click **Add**.
4. Enter the iOS sign certificate information.
 - Purpose: iOS Sign Cert
 - Type: Root
5. Click **Browse** and select iOS sign certificate.
6. Click **Save**.
7. Copy the **Certificate No** of the registered certificate.
8. Go to **Configuration**.
9. Enter the certificate number in **Communication digital signature certificate(iOS)**.
10. Click .

After registering iOS Signed Certificate on EMM Admin Portal, all steps are completed. You can manage the iOS devices through iOS profile setting and App distribution.

Appendix E Installation Environment File

This describes each section of the `EMM{Version}_H_SETUP.ini`.

MULTI_TENANCY

Properties	Description	Default Value	Location
ENABLE	Whether to use multi-tenant mode <ul style="list-style-type: none"> • true: Multi-tenant • false: Single-tenant 	false	Path to file: C:\SamsungSDS\EMM\{Version}\war\WEBINF\classes\config\default-config.xml

Server_URL

Properties	Description	Default Value	Location	Notes
HOST	IP address for EMM server installation	localhost	<ul style="list-style-type: none"> • Path to file: C:\SamsungSDS\EMM\{Version}\war\WEB-INF\classes\config\default-config.xml • The part that comes after <code>common/emm</code>: <ul style="list-style-type: none"> - hostname - httpPort - httpsPort - loopbackIp - loopbackPort 	
PORT	HTTP Port of EMM WAS	35080		
DOMAIN_NAME	Public IP or domain address with external access	demo.smartemm.com		The value must be changed.
HTTPS_PORT	HTTPS Port of EMM server	35443		
LOOPBACK_IP	Loopback IP for EMM server	127.0.0.1		
LOOPBACK_PORT	Loopback Port for EMM server	35080		
EXTERNAL_PORT	<ul style="list-style-type: none"> • Single-server: HTTPS Port with external access to EMM server • Multi-server: HTTPS Port with external access to Web server 	35443		

DATABASE

Properties	Description	Default Value	Location
TYPE	Type of database	MSSQL	<ul style="list-style-type: none"> • Path to file: C:\SamsungSDS\EMM\{Version}\war\WEB-INF\classes\config\default-config.xml • The part comes after database/type: - type
HOST	Server address for MSSQL	localhost	<ul style="list-style-type: none"> • Path to file: C:\SamsungSDS\EMM\{Version}\war\WEB-INF\classes\config\default-config.xml • The part comes after common/datasource/emm: - driver - url - username - password
PORT	TCP/IP port for MSSQL	1433	
NAME	Database name	EMM{Version}DB	
USER	Database access user ID	EMM{Version}	
PASSWORD	Database access password		
SA_USER	MS SQL admin ID	sa	
SA_PASSWORD	MS SQL admin password		

PUSH_SAGID

Properties	Description	Default Value	Location
SAGID	<p>The ID used for the SA module included in the application registered in Push server.</p> <ul style="list-style-type: none"> • Duplicate SAGIDs are not allowed in the environment with a single Push server. • A ticket for the SAGID set is needed. 	SDSEMMSA	C:\SamsungSDS\PushConfig\PushSA\resources\sa\properties\sa.properties

PUSH_APID

Push APID is the ID used for the application that provides Push service. EMM uses EMM Agent (EMMA) and EMM Client (EMMC) as default.

Properties	Description	Default Value	Location
APID	The ID used for Push service application. • Duplicate APIDs are not allowed in the environment with a single Push server.	EMMA	C:\SamsungSDS\PushConfig\PushSA\resources\sa\properties\sa.properties

GENERAL_CONFIG

Specify the basic information on the Push operating environment.

- **USE_L4:** Specify whether to implement load balancing with L4 Network equipment for multiple Push server instances (Proxy or Push CM module).
- **SMB_RUN_MODE:** Specify the operating mode for the Push server.
 - NORMAL: Install Push CM only in DMZ.
 - PROXY: Install Push Proxy in DMZ and Push CM in Intranet zone.

Properties	Description	Default Value	Properties
USE_L4	Whether to use L4. • true: Use • false: Do not use	FALSE	C:\SamsungSDS\Push\{Version}\bin\push_cm_start.bat
SMB_RUN_MODE	Whether to activate Proxy mode • true: Use • false: Do not use	NORMAL	

Properties	Description	Default Value	Properties
USE_L4	Whether to use L4. • true: Use • false: Do not use	FALSE	C:\SamsungSDS\Push\{Version}\bin\push_cm_start.bat
SMB_RUN_MODE	Whether to activate Proxy mode • true: Use • false: Do not use	NORMAL	

CM_JAVA_CONFIG

Configure environment for JAVA on which Push CM is operated.

Properties	Description	Default Value	Location
JAVA_MAX_MEMORY	Maximum memory for JAVA	1g	C:\SamsungSDS\Push\{Version}\bin\push_cm_start.bat
JAVA_MIN_MEMORY	Minimum memory for JAVA	512M	

CM_OS_TYPE

Set the OS for server platform on which Push CM is operated.

Properties	Description	Default Value	Location
OS_TYPE	OS type of Push server	WINDOWS	C:\SamsungSDS\Push\{Version}\bin\push_cm_start.bat

CM_WINDOWS_OS_TYPE

Specify the type of OS for Push CM operated on Microsoft Windows.

Properties	Description	Default Value	Location
WINDOWS_OS_TYPE	The type of Windows for Push server	64BIT	C:\SamsungSDS\Push\{Version}\bin\push_cm_start.bat

CM_CONFIG

Set the environment for the installation and operation of Push CM.

- **CM_EHOSTIP:** The IP address on the server where Push CM is installed. The external public IP address accessible on a device.
- **CM_IHOSTIP:** The internal server IP address for communication between Push CM instances.
- **XXX_INSTANCE_COUNT:** The number of Push components (DCM, SCM, PS, and ECM)
- **XXX_TCP_PORT:** Tcp Port number for communication with Push external components including Push Device Agent(DA) and Service Agent(SA).

- **XXX_UDP_PORT**: UDP Port number for communication between Push CM instances

Properties	Description	Default Value	Location
CM_EHOSTIP	External CM IP	127.0.0.1	C:\SamsungSDS\Push\{Version}\bin\push_cm_start.bat
CM_IHOSTIP	Internal CM IP	127.0.0.1	
DCM_INSTANCE_COUNT	The number of DCM instances	1	
DCM_TCP_PORT	DCM TCP Port communicating with the outside	35001	
DCM_UDP_PORT	DCM UDP Port communicating with the inside	35011	
SCM_INSTANCE_COUNT	The number of SCM instances	1	
SCM_TCP_PORT	SCM TCP Port communicating with the outside	35002	
SCM_UDP_PORT	SCM UDP Port communicating with the inside	35012	
ECM_INSTANCE_COUNT	The number of ECM instances	1	
ECM_TCP_PORT	ECM TCP Port communicating with the outside	35003	
ECM_UDP_PORT	ECM UDP Port communicating with the inside	35013	
PS_INSTANCE_COUNT	The number of PS instances	1	
PS_TCP_PORT	PS TCP Port communicating with the outside	35000	
PS_UDP_PORT	PS UDP Port communicating with the inside	35010	
ICM_INSTANCE_COUNT	The number of ICM instances	1	
ICM_TCP_PORT	ICM TCP Port communicating with the outside	35004	
ICM_UDP_PORT	ICM UDP Port communicating with the inside	35014	

PROXY_HOSTIP

Set the environment for installation and operation of Push Proxy.

- **PROXY_EHOSTIP**: The IP address on the server where Push Proxy is installed. The external public IP address accessible on a device.
- **PROXY_IHOSTIP**: The internal IP address of the server where Push Proxy is installed for Push CM access.

- **XXX_ETCP_PORT**: TCP Port number for communication between the Push external components, including the Push Device Agent (DA) and Service Agent (SA).
- **XXX_ITCP_PORT**: TCP Port number that accepts access from Push CM instances.

Properties	Description	Default Value	Location
PROXY_EHOSTIP	Proxy external IP		C:\SamsungSDS\PushProxy\ {Version}\bin\push_proxy_ start.bat
PROXY_IHOSTIP	Proxy internal IP		
DPP_ETCP_PORT	DPP external port	35101	
DPP_ITCP_PORT	DPP internal port	35111	
PPP_ETCP_PORT	PPP external port	35100	
PPP_ITCP_PORT	PPP internal port	35110	
EPP_ETCP_PORT	EPP external port	35103	
EPP_ITCP_PORT	EPP internal port	35113	

AT_SERVER_JAVA CONFIG

Set the environment for JAVA on which AppTunnel is operated.

Properties	Description	Default Value	Location
JAVA_MAX_MEMORY	Maximum memory for JAVA	1g	C:\SamsungSDS\AT\{Version} \at-server\bin\ at_server_start.bat
JAVA_MIN_MEMORY	Minimum memory for JAVA	512M	

AT_SERVER_OS_TYPE

Set the OS for server platform on which AppTunnel is operated.

Properties	Description	Default Value	Location
OS_TYPE	The OS type of AppTunnel server	WINDOWS	C:\SamsungSDS\AT\{Version}\a t-server\bin\ at_server_start.bat

AT_SERVER_WINDOWS_OS_TYPE

Specify the type of OS for AppTunnel operated on Microsoft Windows.

Properties	Description	Default Value	Location
WINDOWS_OS_TYPE	The type of Windows for AppTunnel server	64BIT	C:\SamsungSDS\AT\{Version} \at-server\bin\ at_server_start.bat

AT_SERVER_CONFIG

Set the environment for the installation and operation of AppTunnel.

- **ATS_HOSTIP:** The IP used by the external components of the AppTunnel client to communicate with the AppTunnel server.
- **ATS_TCPPORT:** TCP Port used by external components of the AppTunnel client to communicate with the AppTunnel server.

Properties	Description	Default Value	Location
ATS_HOSTIP	External IP of AppTunnel server	127.00.1	C:\SamsungSDS\AT\{Version}\at-server\bin\at_server_start.bat
ATS_TCPPORT	TCP Port used by AppTunnel server for communication with the outside	36000	

AT_RELAY_HOSTIP

Set the environment for installation and operation of AppTunnel relay server.

- **RELAY_IHOSTIP:** The internal IP allowing the AppTunnel server to connect to App Tunnel relay server.
- **RELAY_INT_PORT:** The port used by AppTunnel server to connect to App Tunnel relay server

Properties	Description	Default Value	Location
RELAY_IHOSTIP	The internal IP of AppTunnel relay	127.0.0.1	C:\SamsungSDS\AT\{Version}\at-relay\bin\at_relay_start.bat
RELAY_INT_PORT	The internal port of AppTunnel relay	36110	

SA_PROPERTIES

Set the information that is needed to allow Push SA to access and communicate with Push CM.

- **SCM information:** The information on IP and Port of SCM included in Push CM.
 - When connecting to several SCM instances from the SA, MULTI_SCM_USE property is set as TRUE, and MULTI_SCM_INFO is set as SCM_IP:SCM_PORT with colon(":"). Multiple items can be set using a comma (",") separator.
e.g.) 70.30.173.XXX:35012,70.30.183.XXX:35013

- Ticket information: The license information used to access Push CM.

Properties	Description	Default Value	Location
SCM_PORT	SCM IP Port	35002	C:\SamsungSDS\PushConfig\PushSA\resources\sa\properties\sa.properties
MULTI_SCM_USE	For multi SCM instance	FALSE	
MULTI_SCM_INFO	For multi SCM instance, SCM IP and Port • SCM_IP_1:SCM_PORT_1 ,SCM_IP_2:SCM_PORT_2		
TICKET	The value of ticket for SAGID	b5f62...0 ccb6a96a c5f65130 bc5b297 5f0b76b e3	
TICKET_KEY_INDEX	Ticket index	10	

Appendix F Installing SQL Server certificate

The database certificate should be changed due to the limitation of the EMC Crypto module. This chapter describes how to install a 2048 bit RSA certificate. To install the certificate, take the following steps.

Note: A problem can occur when installing a 2048 bit certificate, if another system uses SQL Server. Compatibility with other systems should be checked.

Creating SQL Server certificate

Create a P12 type certificate for SQL Server, and copy it to SQL Server.

- When creating a certificate, the Common Name (CN) must be the name of the computer where the database is installed.
- Set Key Size to 2048 bit.
- Input DigitalSignature as Key Usage.
- Input ServerAuth as Extended Key Usage.

The following shows an example of creating a certificate, using keytool.

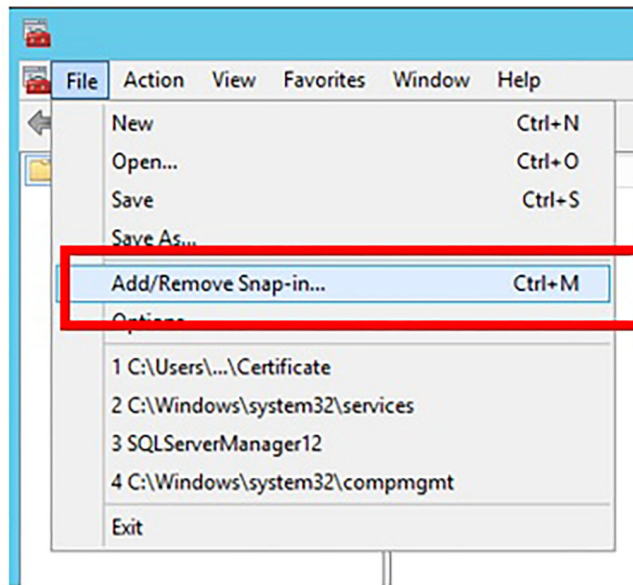
```
keytool -genkey -v -alias mssql -keystore sqlserver.p12 -storetype pkcs12 -keyalg RSA -keysize 2048 -keypass 123456 -validity 7300 -ext KeyUsage:critical="digitalSignature" -ext EKU="serverAuth" -storepass 123456 -dname CN=computer name
```

Installing SQL Server certificate

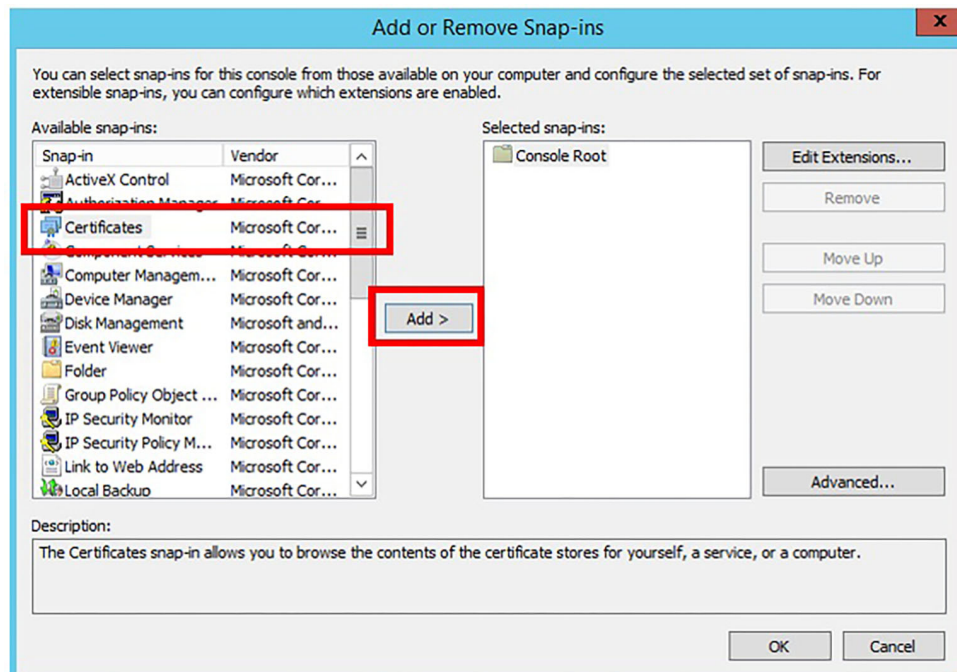
To install the certificate used in SQL Server, complete the following steps:

1. Enter **Windows > Run > mmc** in SQL Server to start Windows Management Console (MMC).

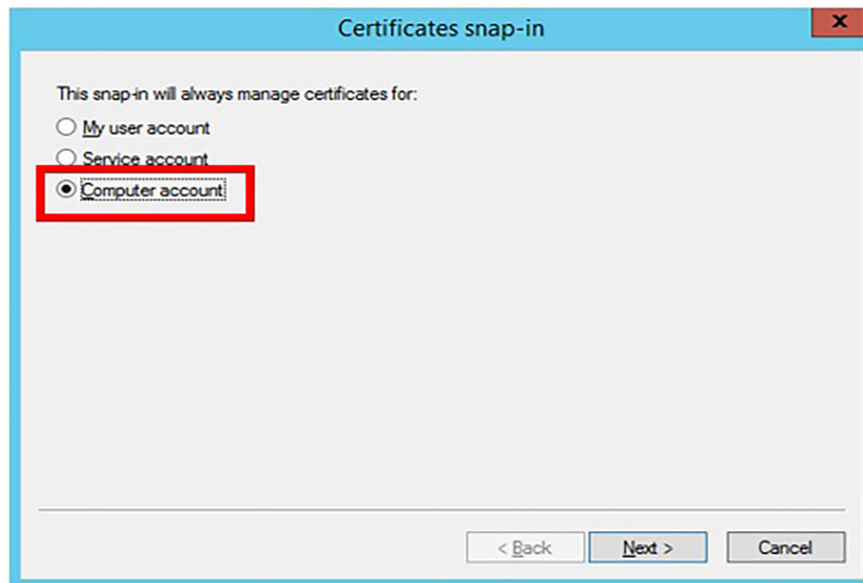
2. Select **File > Add/Remove Snap-in** in MMC.



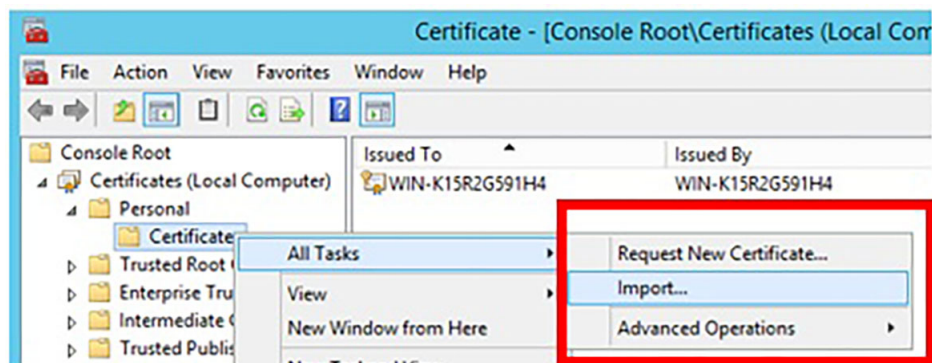
3. Select **Certificates** in **Available snap-ins** and click **Add** to open the “Certificates snap-in” window. Select **Computer account** and select a certificate target (Local Computer) that will be managed by snap-in and click **Finish**.



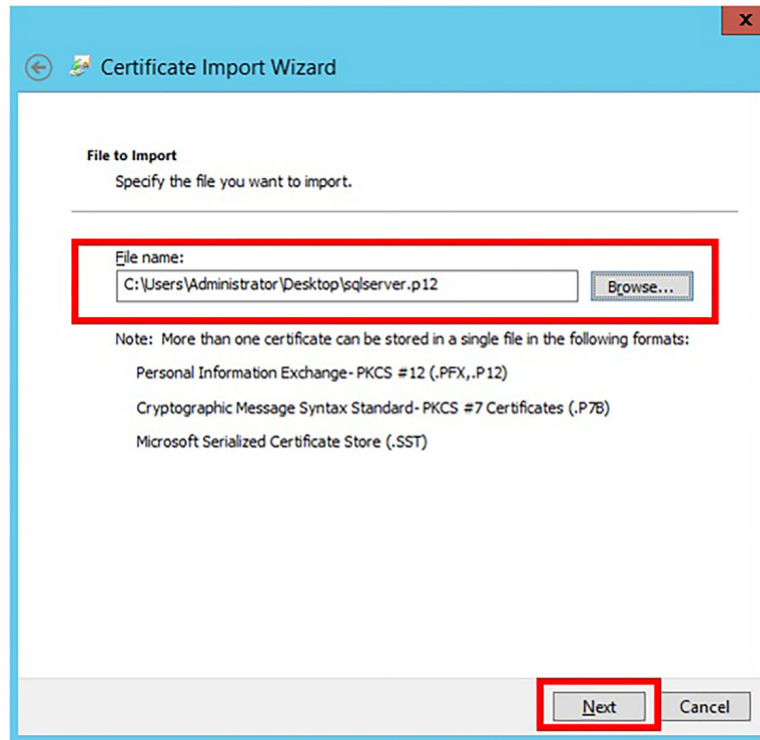
4. Check the selected snap-in and click **OK** to finish adding certificates to snap-in.



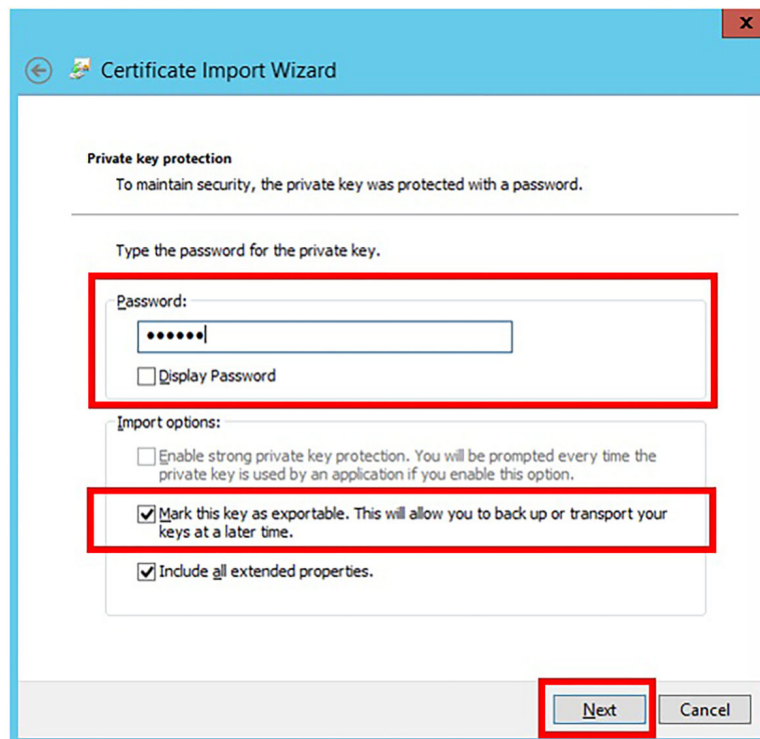
5. Extend Certificates (Local Computer) added to MMC and select **Personal > Certificates**.
6. Right click and select **All Tasks > Import**.



7. Select the certificate that was created in advance (example, sqlserver.p12) on the "File to import" window, and click **Next**.



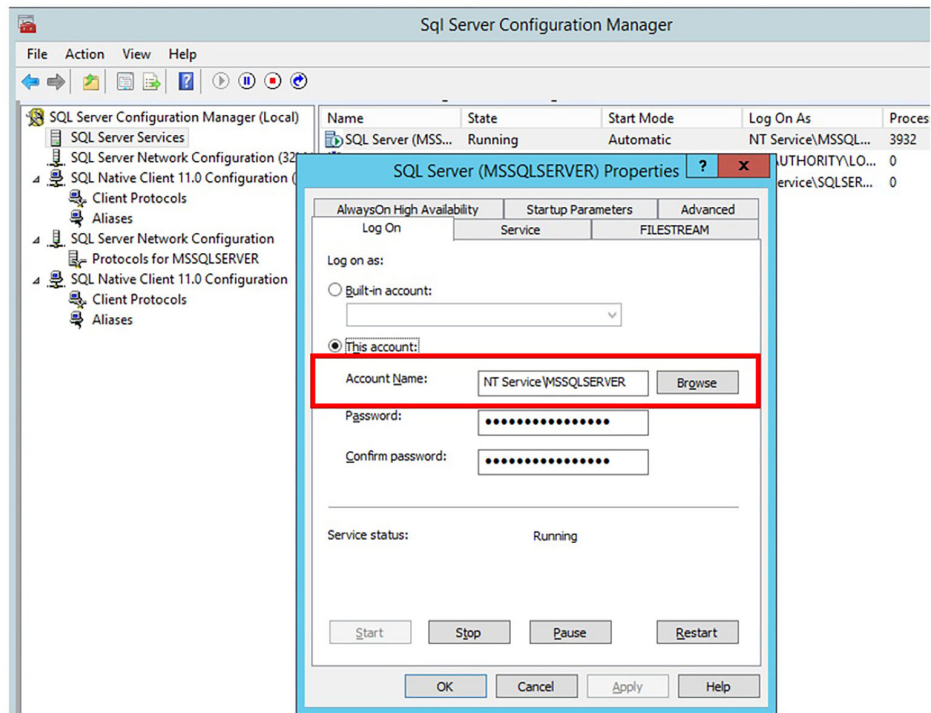
8. Input the password (example, 123456) and select the **Mark this key as exportable....** check box and click **Next**.



9. Select **Personal** as **Certificate Store** and click **Next**.
10. Check the certificate setting information and click **Finish** to install the certificate.

Checking the SQL Server execution account

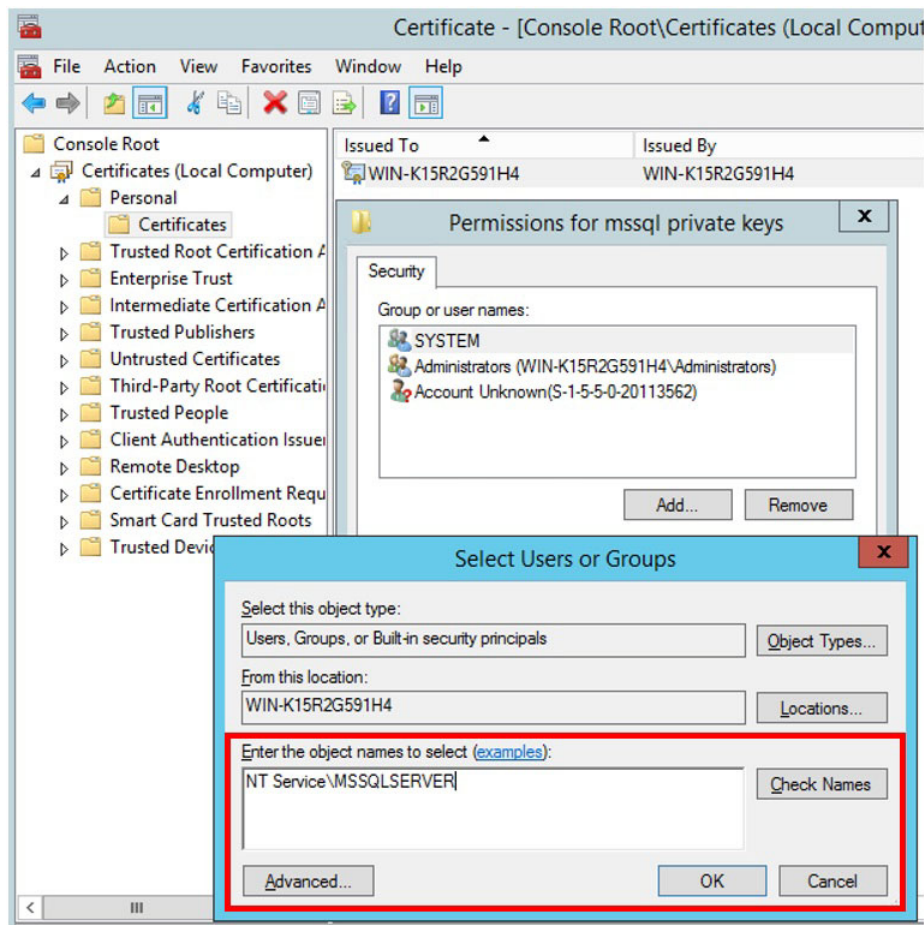
1. Run SQL Server Configuration Manager in Windows Server.
2. Select the SQL Server that currently running in **SQL Server Services** and right click. Then select Properties to open the "SQL Server (MSSQLSERVER) Properties" window.
3. Copy the content of the Account Name (example, NT Service\MSSQLSERVER) in the Log On tab. The copied Account Name is used to authorize the SQL Server certificate.



Authorizing SQL Server certificate

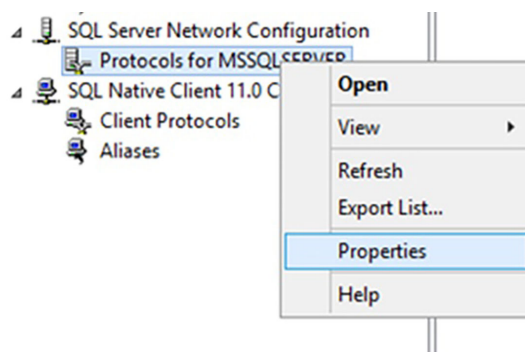
1. Extend Certificates (Local Computer) in MMC and select **Personal > Certificates**. Select an installed certificate in "[chapter , Installing SQL Server certificate](#)" on page 162 and right click the mouse button and then, select **All Tasks > Manage Private Keys...**
2. Click the **Add** button in the "Permissions for mssql private keys" window and add the account (The account copied in "Checking an SQL Server execution account", such as NT Service\MSSQLSERVER).

3. Select the check box for Full Control/Read privilege on the added account.

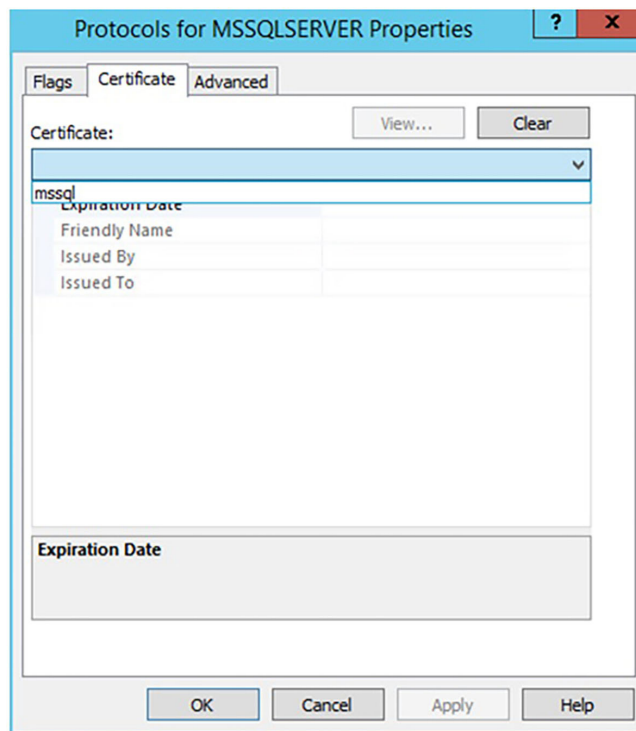


Designating SQL Server certificate

1. Select Protocol for MSSQLSERVER of the SQL Server Network Configuration item in SQL Server Configuration Manager. Then, right click and select **Properties**.



2. Select the installed MSSQL certificate in the Certificate tab and click the **OK** button.



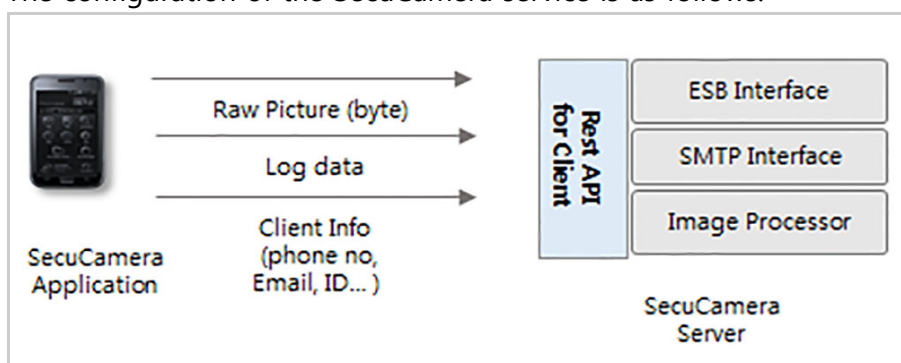
3. Select the SQL Server Instance in the SQL Server Services in SQL Server Configuration Manager. Right click and select **Restart** to restart the SQL Server.

Appendix G SecuCamera

G.1 Overview of Samsung SDS SecuCamera

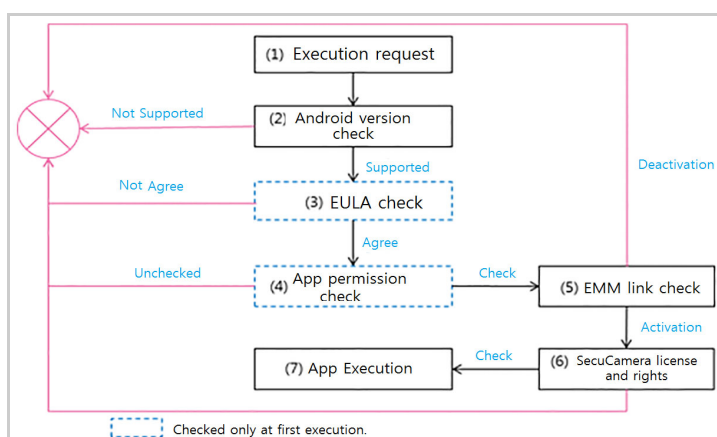
The Samsung SDS SecuCamera is an enterprise security camera application used by EMM to encrypt captured photographs without saving them on a device and send them to a user's email. The EMM administrator can distribute the SecuCamera by purchasing the license and deploying event profiles to a user's device for installation. SecuCamera is supported for on-premise type of EMM 2.0 or later only and is consisted of an application to install on devices and a server. The SecuCamera application can run only once the EMM is installed on a user's device and the user is logged in.

The configuration of the SecuCamera service is as follows:



- SecuCamera application
 - The SecuCamera application is installed when you log in to EMM for the first time on a device running on Android Lollipop or newer, or when you update the policy. Data created in the application is not saved, but encrypted and sent to the SecuCamera server.
- SecuCamera server
 - The SecuCamera server converts encrypted data to image data and sends it to an email address via the linked mail server. The email address must be registered in the EMM user information in advance.
 - The image data in the SecuCamera server is deleted according to the deletion period.
 - The SecuCamera server supports an enterprise service bus (ESB), such as Knox Portal or an SMTP email interface to link to the user's mail server.
 - An interface with the EMM server is not supported so the SecuCamera server can be used as an independent server.

SecuCamera Process flow



This figure illustrates the process for running the SecuCamera application. It shows an overview of the execution process of the SecuCamera application in EMM.

No.	Description
1	The user runs the SecuCamera application on their device.
2	The application checks the device OS version. <ul style="list-style-type: none"> Android OS Lollipop or later is supported.
3, 4	The user accepts EULA and gives permission to the SecuCamera app installation. If the user does not accept, the SecuCamera is not installed.
5	The application checks for a successful login and activation of EMM.
6	The application checks for the license and rights.
7	The application is executed.

- Note:**
- When installing the SecuCamera server, configure the server using `INI` file. For more information, see "[G.3.1, Installing the SecuCamera server](#)" on page 173.
 - Images captured by the SecuCamera are sent to the email address registered in the EMM user information. Therefore, email addresses must be registered in the user information on the EMM Admin Portal for users to receive images from the SecuCamera application.

G.2 Configuring SecuCamera

You can control devices to prohibit use of cameras according to the company security policy. However, you can allow specific users to use the SecuCamera application and to do so, you must complete the following jobs on the EMM Admin Portal:

- Check license in TMS Admin Portal.
- Register a user's email address and enable the use of the SecuCamera.

Register SecuCamera application and set SecuCamera policies.

Preparation

You need to check that you have an appropriate license on the TMS Admin Portal. Go to **Tools > Basic > License** and check the **Number of SecuCamera Users**.

Setting User Information

1. Go to User
2. Click **Add**, and register the user's information including user's Email and select Enable on Secu Camera checkbox.

Registering an application

1. Go to **Setting > EMM Application and Policy** and click **Add > Newly Register**.
2. On the "Add EMM Application" window, select **SecuCamera** from the **Classification** list and type in SecuCamera in **Application Name**.
3. Click **Browse** to upload the SecuCamera installation file. Please contact Technical support for the apk file.
4. Click **Save**.

Configuring the SecuCamera Policy

In order to use the SecuCamera application, you must first enable the SecuCamera application in the SecuCamera policy and configure the INI file.

Configuring the INI file

For each policy, you can set the SecuCamera server address, FinishTimer, mail sender, whether to use a watermark, and whether to modify the email subject using the INI file. See the example below to configure an INI file.

- Address: Set the SecuCamera server address.

- **FinishTimerSec:** If the SecuCamera application doesn't function for the specified period of time set in seconds, it closes automatically. If left unspecified, the default value of 60 seconds is used.
- **UseMark:** Whether or not to use watermarks on photographed images that are sent via email.
 - When enabled, a user's email address registered in the EMM Admin Portal is marked on the center of the image.
 - By default, watermark use is disabled and no input value is necessary.
 - When a watermark is in use, the user's email address, email send date, or text entered by the administrator is displayed in the center of images. To change the watermark, see "[Watermark settings](#)" on page 178
- **UseCustom:** Set whether to edit the subject of the e-mail to which the photographed picture is sent.
 - true: The default title can be modified.
 - No setting or false: The default title cannot be modified.

```
[Info]
Address = https://127.0.0.1
[FinishTimer]
FinishTimerSec= 60
[UseMark]
UseMark = false
[Title]
UseCustom = false
```

To configure a profile, complete the following steps:

1. Go to **Setting > EMM Application and Policy > SecuCamera**
2. On the "Policy Set" window, select **Use** for **SecuCamera App** and **Configuration File**.
3. Upload the previously configured `INI` file, and click **Save & Apply**.

G.3 Installing the SecuCamera server

The SecuCamera server can be configured independently from the EMM server without being linked. To install the SecuCamera server, first configure the Apache Tomcat server environment. You can receive the `setup.exe` file for the SecuCamera server from the technical support team for installation and set the server installation file, such as the email server linked to the SecuCamera server, watermark modification method and the deletion period of photographed images saved in the server.

Preparing for installation

You must prepare the following before installing the SecuCamera server:

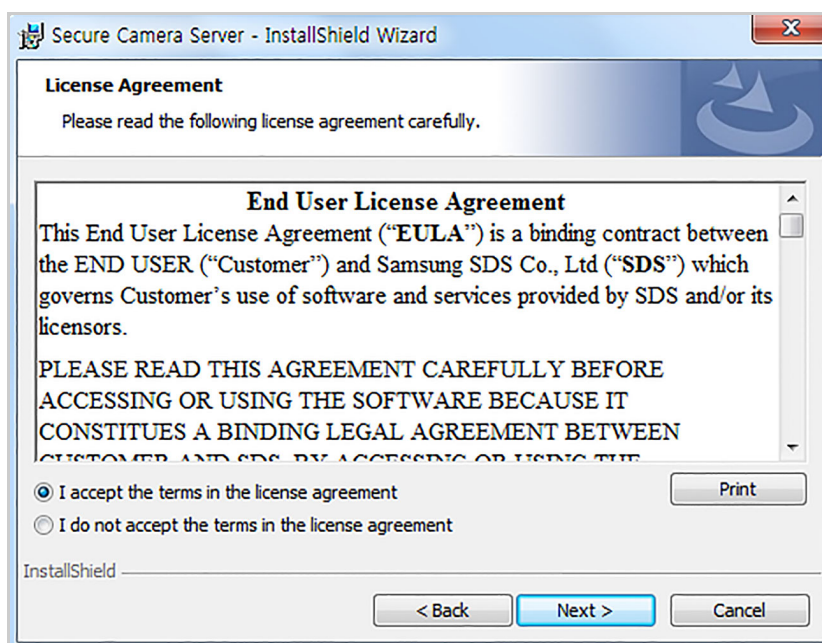
- Environment for installation
 - Check supported OS: Windows Server 2008 R2 (64bit) or 2012 (64bit)
 - Apache Tomcat installation must be installed for SecuCamera server operation.
- Java Development Kit (JDK)
 - Install Java Development Kit 1.8(bit). For more information, see ["2.1, Installing JDK" on page 8](#).
- Network environment
 - Open the firewall between the SecuCamera server and the email server.
- Request and prepare the installation and configuration files.
 - installation file for SecuCamera server

G.3.1 Installing the SecuCamera server

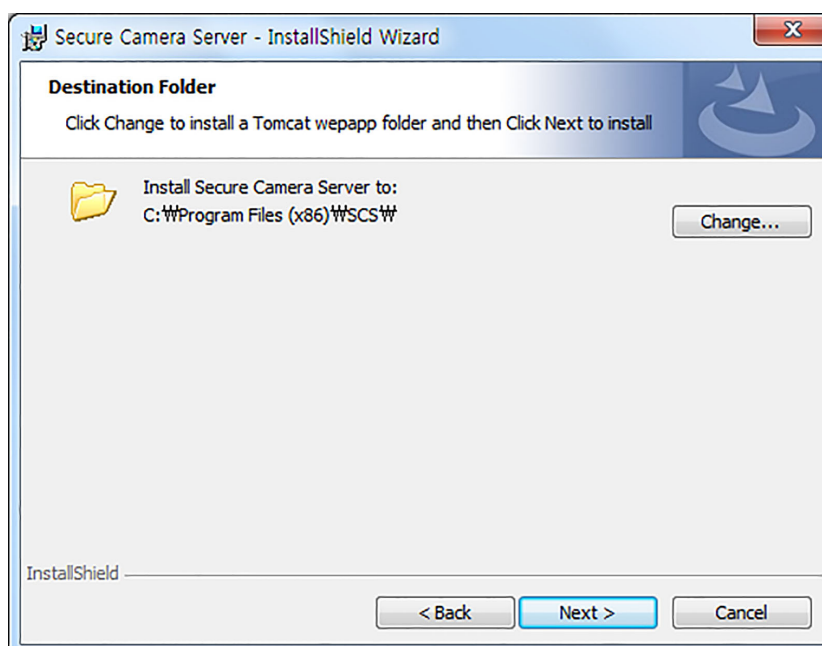
To use the received files to install the SecuCamera server in the Apache Tomcat environment, complete the following steps:

1. Open the File Explorer, navigate and run the received `setup.exe` file.
 - The file must be installed using the Windows administrator account.
2. Select the language for installation and click **OK**.
3. When the InstallShield Wizard starts, click **OK**.

4. Read the EULA carefully, select **I accept the terms in license agreement**, and click **Next**.



5. Click **Change** to change destination path for SecuCamera server installation as {Tomcat installation path}\webapp, and click **Next**.



6. Click **Install** to install the SecuCamera server.
7. When the SecuCamera server installation is complete, modify the Tomcat configuration file so the SecuCamera server runs automatically when the Tomcat server is run.

- Tomcat configuration file : {Tomcat path}\conf\server.xml

```
<Host name= "localhost" appBase="webapps"
      unpackWARs = "true" autoDeploy= "true">
  <!-- Omitted-->

  <Context docBase="SCS" path="/securecamera"
    reloadabel="true">

</Host>
```

G.3.2 Configuring the SecuCamera server

You can specify the properties that are associated with the SecuCamera server on the `config.properites` file, such as the email interface, email format, logs, image format, and the data deletion period.

Configure the default settings of the SecuCamera server and the mail sender's information sent by the server in the file shown below:

- Path to the SecuCamera server configuration file:
{Secure Camera installation path}\WEB-INF\classes\properties\config.properties file.
 - `config.properties` file: Configure the settings including the email interface linked to the SecuCamera server, mail type, log, image format, watermark modification, and data deletion cycle.
 - `mail-sender-settings.json` file: The mail sender's information sent by the SecuCamera server.

Configure the `config.properites` file as follows:

```
# 1:smtp 2:knox portal(ESB)
mail.server=2

#smtp settings
mail.smtp.host=10.10.123.54
mail.smtp.port=25
mail.smtp.sender=GilDong Hong <gdong.hong@example.com>

#on/off
mail.smtp.tls=off
mail.smtp.ssl=off

#smtp authentication
#on/off
mail.smtp.auth=off
mail.smtp.username= username
mail.smtp.pwd=password

#esb settings
mysingle.esb.cid=C60ML0000
mysingle.esb.cpw=C60ML0000111222
mysingle.esb.sender=gdong.hong@example.samsungsds.com
mysingle.esb.sender.pw=sdstest12!
mysingle.esb.mail.url=http://example.samsung.net/test/
```

```

#mail settings
mail.subject=[SecuCamera] Photographed images
mail.body.uri=/html/mail_file.html

#mail settings
#on/off
mail.sender.setting=on

#image settings
image.upload.path=c:\\SecuCam_Image
image.format=jpg

#log settings (Location to which logs sent by the device are
saved)
device.log.path=c:\\SecuCam_Log

#image/device log cleaner
#on/off
clearner.image=off
clearner.devicelog=off

#image WarterMark modification
#0:Do not use 1:email 2:send date 3:Text entered by the
administrator
WarterMark.format= 1
WarterMark.customer=[Text displays as the watermark]

#cron format
#Sec 0-59 , - * /
#Min 0-59 , - * /
#Hour 0-23 , - * /
#Day 1-31 , - * ? / L W
#Month 1-12 or JAN-DEC , - * /
#Day 1-7 or SUN-SAT , - * ? / L #
#Year (Option) 1970-2099 , - * /
clearner.image.clonetab=0 0 23 * * SUN
clearner.devicelog.clonetab=0 0 23 * * SAT

```

Email server settings

Specify the email server to be linked with the SecuCamera server.

- When sending via the SMTP server: mail.sever= 1
- When sending via the ESB (e.g., Knox Portal) server: mail.server= 2
- When sending via the Knox Portal Rest API V1 server: mail.server= 3
- When sending via the Knox Portal Rest API V2 server: mail.server= 4

SMTP server setting

If you send emails via the SMTP serve, you need to specify the SMTP server IP address, Port number, sender's email address, and set whether to enable or disable TSL/SSL.

- mail.smtp.host= IP address of the SMTP server
- mail.smtp.port= Port number of the SMTP server
- mail.smtp.sender= SMTP sender email
- mail.smtp.tls= Set TLS use as On or Off
- mail.smtp.ssl= Set SSL use as On or Off

SMTP authentication settings

Specify whether or not to use authentication when sending an SMTP email.

- mail.smtp.auth= Set authentication use as On or Off
- mail.smtp.username= Username for SMTP authentication
- mail.smtp.pwd= Password for SMTP authentication

ESB server setting

Setup the correct service environment for ESB, request for ESB use from the corresponding provider, and obtain a CID and a CPW.

- mysingle.esb.cid= Granted CID
- mysingle.esb.pwd= Granted CPW
- mysingle.esb.sender= ESB sender email
- mysingle.esb.sender.pw= ESB sender password
- mysingle.esb.mail.url= ESB sender URL

Knox Portal API V1 server settings

Set up the interface of the server that has been requested for V1 API to connect to Knox Portal. After this point (2020.12), applications for V1 API are no longer possible.

- Knoxportal.rest.sender = Knox Portal sender email
- Knoxportal.rest.mail.token= Token received to use Knox Portal V1 API
- Knoxportal.rest.mail.url= Knox Portal Mail API URL
- Knoxportal.rest.mail.attach.total.max.size = maximum number of attachments for Knox Portal Mail
- Knoxportal.rest.empsearch.cid = CID received to use Knox Portal V1 API
- Knoxportal.rest.empsearch.token = Token received to use Knox Portal V1 API
- Knoxportal.rest.empsearch.url = Knox Portal employees inquiry API URL

Knox Portal API V2 server settings

V2 Rest API for Knox Portal connection must be applied to the person in charge of Knox Portal, and the Token and CID must be received.

- Knoxportal.rest.v2.sender = Knox Portal sender email
- Knoxportal.rest.v2.mail.token= Token received to use Knox Portal V2 API
- Knoxportal.rest.v2.mail.url= KnoxPortal V2 Mail API URL
- Knoxportal.rest.v2.empsearch.cid = CID received to use Knox Portal V2 API

- `Knoxportal.rest.v2.empsearch.token` = Token received to use Knox Portal V2 API
- `Knoxportal.rest.v2.empsearch.url` = Knox Portal employees inquiry V2 API URL

Email settings

Specify the email title and html file path containing the body of the email to be sent from the SecuCamera server.

- `mail.subject`= Email title
- `mail.body.uri`= `.html` file path containing body

Enabling mail sender settings

To specify senders of emails sent by the SecuCamera server for each department, you need to decide whether the `json` file should be used or not.

- If the `mail.sender.setting` is "on," then emails are sent using the sender information specified in the `mail-sender-settings.json` file.
- If no department information for the user exists in the `mail-sender-settings.json` file, then the `mail.smtp.sender` specified in the `config.properties` file or the mail sending server specified as the `mysingle.esb.sender` is used.
- If you configure the `mail-sender-settings.json` file, see ["Mail sender settings" on page 180](#).

Image settings

Specify the file saving path and the format of images photographed by Secure Camera.

- `image.upload.path`= Image saving path
- `image.format`= Image format

Watermark settings

You can set the watermark to contain the user's email address, email send date, or specific text so that it can be added to photos taken using the SecuCamera application.

- `watermark.format`= Enter one of the following numbers depending on the watermark display format.
 - 0: Do not use
 - 1: User's email address
 - 2: Email send date
 - 3: Specific text
- `watermark.custom`= The administrator enters text that should be used as the watermark (50 bytes).

Cleaner settings

Specify the deletion period of images and logs saved on the SecuCamera server for a periodic cleanup. For more information, see ["Crontab format" on page 180](#).

- cleaner.image= Set Image deletion as On or Off
- cleaner.devicelog= Set Log deletion as On or Off
- cleaner.image.clonetab= Image deletion period
- cleaner.image.clonetab= Log deletion period

Crontab format

```

Second 0-59, - * /
Minute 0-59, - * /
Hour 0-23, - * /
Day of the Month 1-31, - * ? / L W
Month of the Year 1-12 or JAN-DEC, - * /
Day of the Week 1-7 or SUN-SAT, - * ? / L #
Year(optional) 1970-2099, - * /
* : All values
? : No specific value
- : Range of values
, : Separates values
/ : Initial value in conjunction with a step value
L : Last value in the range
W : Monday to Friday or the closest Monday/Friday
# : Day of the week in conjunction with week number of the month, 2#1
=> First Monday

```

E.g.,) Expression Meaning

```

Second Minute Hour Day Month Week(Year)
"0 0 12 * * ?": Any days of the week, monthly, daily, 12:00:00
"0 15 10 ? * *": Every days of the week, monthly, any date, 10:15:00
"0 15 10 * * ?": Any days of the week, monthly, daily, 10:15:00
"0 15 10 * * ? *": Every year, any days of the week, monthly, daily,
10:15
"0 15 10 * * ?": 2005" In year 2005, any days of the week, monthly,
daily 10:15
"0 * 14 * * ?": Any days of the week, monthly, daily, 2pm at every 0
sec of a minute
"0 0/5 14 * * ?": Any days of the week, monthly, daily, 2pm at every
0 sec with 5 minute interval
"0 0/5 14,18 * * ?": Any days of the week, monthly, daily, 2pm, 6pm,
at every 0 sec with 5 minute interval
"0 0-5 14 * * ?": Any days of the week, monthly, daily, from 2pm to
2:05pm at every 0 sec
"0 10,44 14 ? 3 WED": March, every Wednesday, any date, 14:10:00,
14:44:00
"0 15 10 ? * MON-FRI": Mon to Fri, monthly, any date 10:15:00
"0 15 10 15 * ?": Any weekday, monthly, 15th 10:15:00
"0 15 10 L * ?": Any weekday, last day of every month, 10:15:00
"0 15 10 ? * 6L": Last Friday of every month, any date, 10:15:00
"0 15 10 ? * 6L 2002-2005": From 2002 to 2005, last Friday of every
month, any date, 10:15:00
"0 15 10 ? * 6#3": Monthly, every 3rd Friday, any date, 10:15:00

```

Mail sender settings

Photos taken using SecuCamera are sent to the user who has taken them in an email through the mail server.

The sender can be selected depending on the department to which the user belongs. If the user's department is not specified in the `mail-sender-setting.json` file, then the mail sender specified in the `config.properites` file is used to send emails instead. For more information about the default settings of the SecuCamera server, see ["Configuring the SecuCamera server" on page 175](#).

- department: The department to which the user belongs.
- email: The sender's email address.
- pass: The password for the sender's email address. This value must be entered for Knox Portal.

The following is a sample `mail-sender-setting.json` file.

```
{
  "settings":
  [
    {
      "department" : "SDS Suwon",
      "email" : "seungyong.shin@emsdev2.com",
        /*sender's email */
      "pass" : "SDS" /*password for sender's email*/
    }
    {
      "department" : "SDS Jamsil",
      "email" : "marvin.moon@emsdev2.com",
      "pass" : "SDS"
    }
  ]
}
```

For instance, the sender is changed according to the specified email sending information.

- If the recipient belongs to "SDS Suwon," then the email sender becomes seungyoung.shin@emsdev2.com.
- If the recipient belongs to "SDS Jamsil," then the email sender becomes marvin.moon@emsdev2.com.
- If the recipient doesn't belong to either department, then the email sender becomes the default sender specified in the `config.properties` file.
 - When the `mail.server` value is "1 (SMTP)," the sender specified as the `mail.smtp.sender` is used to send emails.
 - When the `mail.server` value is "2 (Knox Portal)," the sender specified as the `mysingle.esb.sender` is used to send emails.

G.3.3 Running SecuCamera server

If you run the Tomcat server after installing the SecuCamera server, the SecuCamera server will run simultaneously.

To run the Tomcat server, complete the following steps:

1. Go to the `{Tomcat installation path}\bin` folder, and double-click the `startup.bat` file.
2. Check that the Tomcat server runs successfully.

- The Tomcat server will run as follows and the SecuCamera server will run simultaneously.

```

Tomcat
oyDirectory Deployment of web application directory [C:\wapache-tomcat-9.0.0.M26W
webapps\host-manager] has finished in [46] ms
05-Sep-2017 14:54:10.541 정보 [main] org.apache.catalina.startup.HostConfig.depl
oyDirectory Deploying web application directory [C:\wapache-tomcat-9.0.0.M26Wweba
pps\manager]
05-Sep-2017 14:54:10.573 정보 [main] org.apache.catalina.startup.HostConfig.depl
oyDirectory Deployment of web application directory [C:\wapache-tomcat-9.0.0.M26W
webapps\manager] has finished in [32] ms
05-Sep-2017 14:54:10.573 정보 [main] org.apache.catalina.startup.HostConfig.depl
oyDirectory Deploying web application directory [C:\wapache-tomcat-9.0.0.M26Wweba
pps\ROOT]
05-Sep-2017 14:54:10.588 정보 [main] org.apache.catalina.startup.HostConfig.depl
oyDirectory Deployment of web application directory [C:\wapache-tomcat-9.0.0.M26W
webapps\ROOT] has finished in [15] ms
05-Sep-2017 14:54:10.588 정보 [main] org.apache.catalina.startup.HostConfig.depl
oyDirectory Deploying web application directory [C:\wapache-tomcat-9.0.0.M26Wweba
pps\securecamera]
05-Sep-2017 14:54:10.619 정보 [main] org.apache.catalina.startup.HostConfig.depl
oyDirectory Deployment of web application directory [C:\wapache-tomcat-9.0.0.M26W
webapps\securecamera] has finished in [31] ms
05-Sep-2017 14:54:10.619 정보 [main] org.apache.coyote.AbstractProtocol.start St
arting ProtocolHandler ["ajp-nio-8009"]
05-Sep-2017 14:54:10.666 정보 [main] org.apache.catalina.startup.Catalina.start
Server startup in 1064 ms

```

Checking SecuCamera server logs

When the user runs the SecuCamera application on their device, they can check the SecuCamera server logs saved during communication between the device and the server.

- Log file location: The top-level folder in which the SecuCamera server is installed.
For example, if the SecuCamera application was installed in the `c:\sds\securecamera` folder, logs are saved to the `c:\` folder. You can modify the `log4j.xml` file to change the log file path.
- Log information: Fileid, Filename, Filesize, hostip, userid, email, state, insert_date, and update_date.
 - hostip: The IP address of the SecuCamera server.
 - userid: The device user's ID.
 - state: One of the following log messages is displayed about the state of the SecuCamera server.
 - Key exchanged after launching SecuCamera to send emails: Ready to key change.
 - Ready to send emails after taking photos: Ready to send mail.
 - Key deleted after closing SecuCamera: Ready to remove key.
 - Log delivery function enabled in SecuCamera: Ready to save deviceLog.

SAMSUNG SDS

Realize your vision

www.samsungds.com

Copyright 2022 Samsung SDS Co., Ltd. All rights reserved.