Kony Management

Windows Install Guide

On-Premises

Release V8

Document Relevance and Accuracy

This document is considered relevant to the Release stated on this title page and the document version stated on the Revision History page. Remember to always view and download the latest document version relevant to the software release you are using.

January, 2018

Revision History

Date	Document Version	Description of Modifications/Release
01/30/2018	2.0	Document published for V8 SP1 Updated EMM Installation - Enabling High Availability section. Added a note underInstalling Kony EMM for Windows > Multi-node Installation Added a note in the Installing Kony EMM for Windows section.
10/09/2017	1.0	Document published for V8 GA

Table of Contents

1. Preface

Kony Management Suite software is a policy configuration and management tool for mobile handheld devices and corresponding applications on smartphones and tablets. Kony Management Suite helps enterprises to manage complex communications between mobile devices by supporting security, network services, and software and hardware management across multiple OS platforms. Kony Management Suite also supports bring your own device (BYOD) initiatives that have become the focus of many enterprises. Kony Management Suite supports corporate and personal devices and a more complex and heterogeneous environment.

The primary purpose of Kony Management Suite is to ensure that all devices, corresponding applications, and device users comply with a company's IT policies. You can achieve this goal in different ways.

1.1 Purpose

This document is targeted at the developers who want to install Kony Management Suite on Windows platform.

1.2 Intended Audience

This document is intended for engineers or system administrators who install and configure Kony Management Suite Console and Kony Enterprise Store.

1.3 Formatting Conventions

The following are the formatting conventions used throughout the document:

:

Convention	Explanation
`Monospace`	• User input text, system prompts, and responses • File path • Commands • Program code • File names
Italic	• Emphasis • Names of books and documents • New terminology
Bold	• Windows • Menus • Buttons • Icons • Fields • Tabs
URL	Active link to a URL
Note:	Provides helpful hints or additional information
Import-ant:	Highlights actions or information that might cause problems to systems or data

1.4 Supported Platforms

Supported Platforms are iOS, iPad, Android, Android Tablet, and Windows Phone 8.1. Other Device Operating Systems are not supported.

1.5 Contact Us

We welcome your feedback on our documentation. Write to us at techpubs@kony.com.For technical questions, suggestions, comments, or to report problems on Kony's product line, contact support@kony.com.

2. Introduction

Enterprise mobility management (EMM) software is a policy configuration and management tool for mobile handheld devices and corresponding applications on smartphones and tablets. EMM helps enterprises to manage complex communications between mobile devices by supporting security, network services, and software and hardware management across multiple OS platforms. EMM also supports bring your own device (BYOD) initiatives that have become the focus of many enterprises. It can support corporate and personal devices and helps to support a more complex and heterogeneous environment.

The primary purpose of EMM is to ensure that all devices, corresponding applications, and device users are in compliance with the IT Policies set by the company. This goal can be achieved in different ways.

The following is a scenario in which the Kony EMM approaches and handles the problem:

To manage any device, it must be enrolled. The management can choose to manage only a few employee devices or all of them. The employee database can be imported from enterprise systems like Microsoft Active Directory. Once it is enrolled successfully, the EMM Administrator has complete control over the devices.

These devices are grouped together into Device Sets based on rules. Device Sets are usually dynamic, which means all the devices satisfying the rules are part of the set. Device Sets can be created on the basis of several Attribute Types including its location, ownership, OS, hardware, apps installed and much more. To keep the devices in check, device policies are created, which are applied to the device sets. These device policies and settings cover the entire scope of a device functionality. For example, enforcing a passcode policy, removing camera access at certain locations.

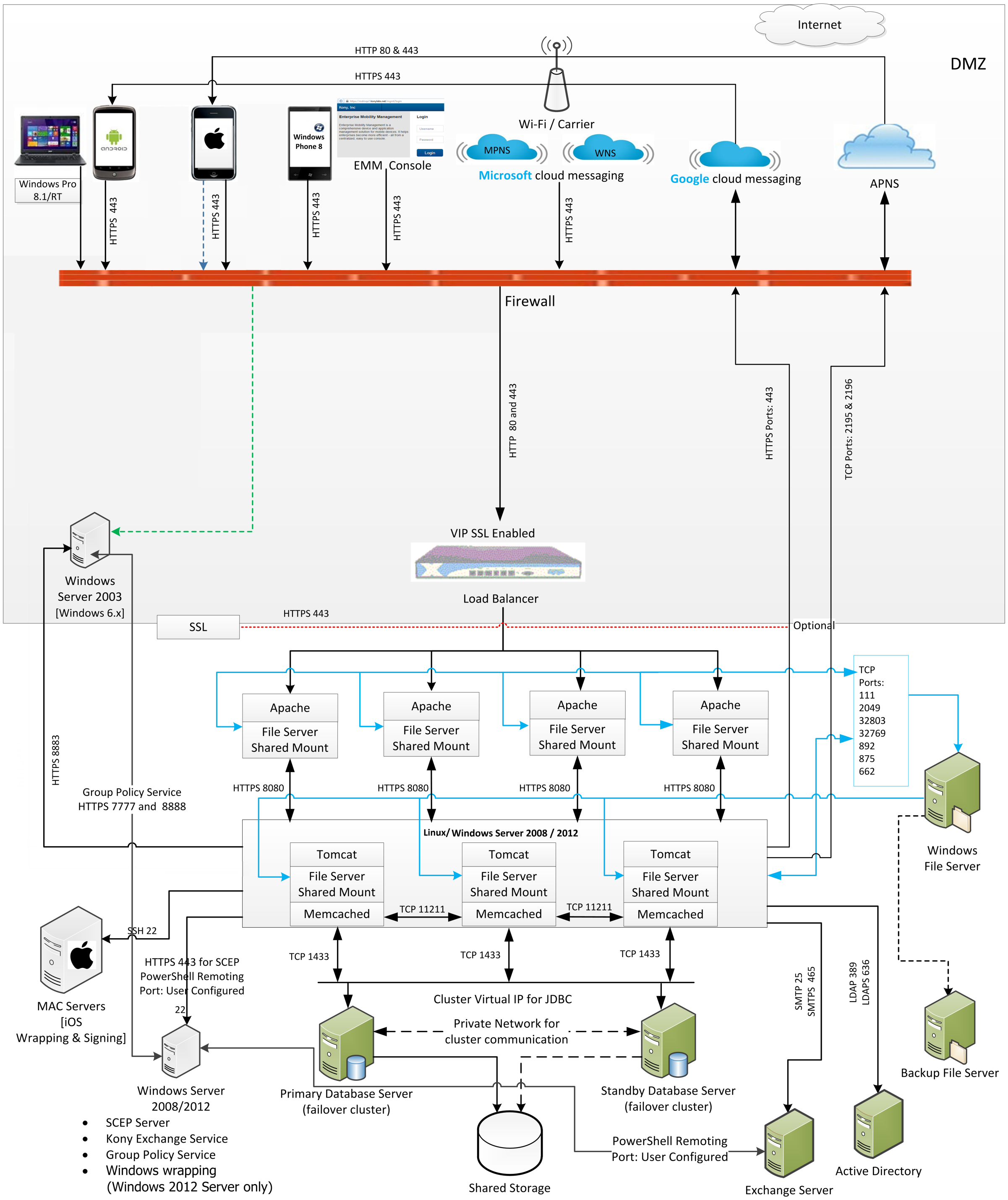
A device may belong to multiple groups and hence it can have several policies applicable to it. But, only one policy should be applied to a device. To resolve this, each policy has a Priority associated with it. The policy with the highest priority is loaded first on the device. As part of the policy, the administrator also defines Compliance Actions. If devices do not comply with the rules, the administrator can perform the required action. The administrator can prescribe a set of actions such as, sending alerts to administrator and/or the user, Blocking Email, Resetting Passcode, Locking Device, Enterprise Wipe, and a Complete Wipe. Once returning to a compliant state, the EMM server automatically restores the settings and access the device as per the policy is applied.

Similarly, application level policies can also be applied to users and groups. These differ from device level policies because they apply at the application level. For example, you can prevent cut, copy and paste for one particular application. Similarly, you can prevent application access during holidays.

All the EMM policies are dynamic and location specific. It is possible to set policies between different office locations, home and so on.

3. Kony Management Enterprise Mobile Management (EMM) Architecture and Components

An overview of the Kony Management EMM Architecture and Components is shown below:



The following table describes components in more detail.

Component	Description
Mobile Devices and Tablets	Mobile Devices with Launchpad application installed communicate with EMM server over HTTPS. Also EMM console can be accessed on HTTPS port which is meant for Administrator use. Currently EMM supports iPhones, iPads, Android devices, Windows 6.x and Windows Phone 8 devices.
Load Balancer and SSL	SSL certificate needs to be installed on Load Balancer VIP for SSL offload. It is recommended to install “VeriSign Secure Site Pro” SSL which has the maximum device compatibility.
Apache Server	Apache servers will host static content, rewrite rules, maintain session affinity for backend Tomcat server based on cookies. Optionally, additional SSL certificates can be installed on Apache servers for an end to end SSL solution. Apache server allows to download binaries from device/web based on secure/encrypted URL. Encrypted URL is valid for particular amount of time (e.g. 3 minutes)
Network File Server & File Server Shared mount	NFS server is required to provide common mount solution. Common mount will host app binaries and other static data. Common mount is attached to both Apache servers and Tomcat servers for multi-node environments. For high availability backup NFS server can be configured.
Tomcat and Memcached	Tomcat is the web server on which EMM is deployed. EMM app is a J2EE Web archive. Memcached is used for caching database queries.
MAC Server	MAC server is required to wrap and sign iOS apps. EMM server moves iOS apps on NFS mount to MAC on port 22 via SSH and performs wrap and sign /sign only actions. Signed apps are then placed on NFS mount and available for download via Apache server. This is mandatory to support App Management on iOS devices.

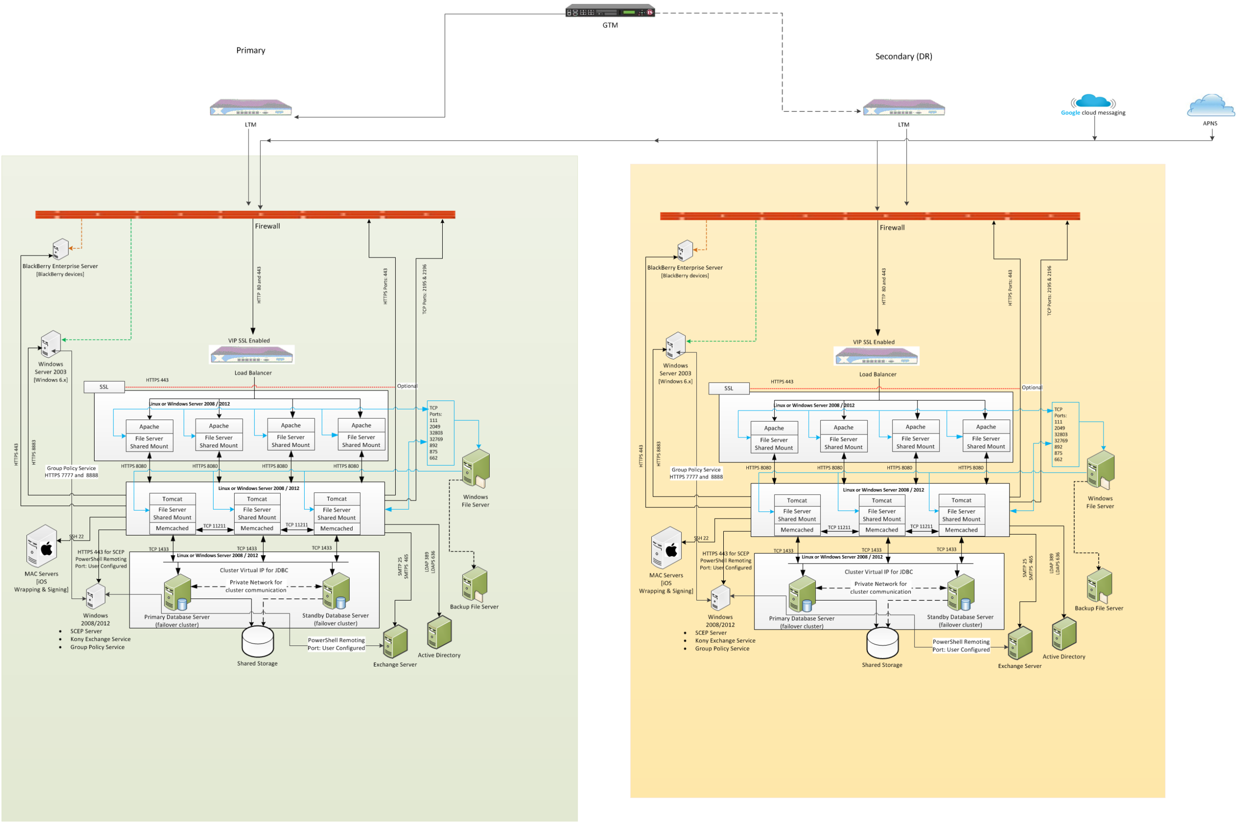
Component	Description
Exchange / Email Server	Exchange server is required to send notification emails to users. EMM has the ability to use both SMTP port 25 and SMTPS port 465 over SMTP authentication. These ports need to be opened accordingly in the firewall. Using Kony Exchange service, you can block or unblock emails (clients). Blacklisted email clients cannot communicate with the Exchange server from your device
Active Directory Server	EMM has the ability to import users and groups. User authentication is performed on Active Directory only. Note that EMM just imports users but not their passwords. LDAP port 389 or LDAPS port 636 can be used for EMM server to connect AD server. These ports need to be opened accordingly in the firewall.
Windows Server 2003	Windows Mobile 6.x devices communicate with Windows Server 2003 on HTTP/HTTPS using ports 80, 443, 8443. EMM server also connects to Window Server 2003 to get device information. Windows 2003 server will also connect to the Windows Server 2008/2012 for Group policy management service.
Windows Server 2008/2012 • SCEP Server • Kony Exchange Service • Windows 6.x MDM Group Policy	SCEP server must be installed on Windows Server 2008/2012. Interaction with SCEP server is mandatory in order to enroll iOS devices to EMM. Devices communicate SCEP over 443 port and EMM server will also communicate the SCEP server on the same port. Using Kony Exchange service, you can block or unblock emails (accounts).The blacklisted email clients cannot communicate with the Exchange server from your device. In order to support Windows 6.x devices, Group Policy Management component must be installed. The Windows Server 2003 [mobile device manager component] and Windows Server 2008/2012 both reside in the same network and the communication is carried over HTTP(S) on port 7777

Component	Description
GCM	EMM uses Google messaging cloud to send push notifications to Android devices. Respective ports and host names need to be opened in the firewall from EMM server. If the devices are behind corporate networks / Wi-Fi's, the required URL's ports need to be allowed in inbound rules. For more details, refer Push notification firewall prerequisites.
Apple Push Notification Service (APNS)	EMM also uses APNS cloud to send push notifications to iOS devices. Respective ports and Apple host names need to be opened in the firewall from EMM server. If the devices are behind corporate networks / Wi-Fi's, the required URL's ports need to be allowed in inbound rules. For more details, refer Push notification firewall prerequisites.
Failover cluster	For production EMM environments any of this database Failover cluster can be integrated for EMM database Server, which will have active and passive nodes along with heartbeat service and SAN as a database shared mount. This will have a cluster IP on top of DB services and all EMM Tomcat nodes can use the same for JDBC.

4. EMM Disaster Recovery (DR) Architecture

Global Traffic Manager (GTM) can be configured and used as Active Passive load balancing. Currently EMM is not supported with Active-Active setup. Apart from using GTM, you can also manage primary and DR sites by changing DNS record.

An overview of the EMM DR Architecture is shown below:



4.1 DR Setup

Secondary data center (DR) must contain the following components which are part of the Primary data center. We recommend that you take initial replica along with file system backups from the running state from primary data center.

- Windows Server 2008 / 2012 (SCEP, Exchange Service, Group Policy Service and Windows wrapping)
- Windows Server 2003
- MAC server
- Firewall and Load balancer rules
- NFS server
- EMM tomcat and memcached instances

Take a back up of your Windows Server 2003 and recover your system by following Microsoft Technet documentation. More details are available at - http://technet.microsoft.com/en-us/library/dd261892.aspx

4.2 DR Synchronization

The secondary data center must have the content replica from Microsoft Active Directory server domain, email server connectivity, GCM, and APNS cloud connectivity similar to the primary data center.

- All tomcat contents, including emm_config application contents
- Konyemmmaster database full backup - We recommend that you take a backup and restore these sql files manually on DR setup on a daily basis.
- docroot contents from any one NFS mount need to be synchronized in DR at least one time whenever a new app is added and wrapped.
- Apache server configuration and static contents.

5. System Requirements

Kony Management Suite has specific system requirements for installation and operation. Before installing Kony Management Suite, verify that you meet the following requirements:

- Hardware Requirements
- Software Requirements
- Database Requirements
- Android SDK Download
- User Requirements
- Network Related Prerequisites
- Exchange Server Prerequisites

> ***Note:*** You need a valid Kony license key from your sales representative or partner. Without a valid license, you cannot install EMM.

5.1 Hardware Requirements

The following sections explain the hardware requirements for an application server, an Apple server, and a database server.

5.1.1 Application Server for each Instance

Component	Requirement
Processor	Quad-Core 3.6 GHz
Memory	16 GB

Component	Requirement
Internal Storage	300 GB (15K SAS 3.5") with 2 Drives (Raid 1)
Network	2 Gigabit Ethernet Ports
Operating System	Windows Server 2008 R2 Enterprise or Windows server 2012 R2 Standard Edition and above

5.1.2 Database Server(MySQL, Oracle and Microsoft SQL Server)

Component	Requirement
Processor	Quad-Core 3.6 GHz
Memory	32 GB
Internal Storage	300 GB (15K SAS 3.5") with 3 Drives (Raid 5)
Network	2 Gigabit Ethernet Ports
Operating System	Windows Server 2008 Enterprise or Datacenter Edition

5.1.3 Windows 2008/2012 Server

SCEP Server (iOS MDM enrollment), Windows 6.x MDM group policy and Kony Exchange Service (block and unblock email clients from devices) use Windows 2008/2012 Server.

> ***Note:*** For Windows app wrapping, to manage Windows Phone 8.1 enterprise apps, deploy Windows Srver 2012 (x64).

Component	Requirement
Processor	1.6 GHz (x86 processor)
Memory	4 GB
Internal Storage	40 GB

5.1.4 Apple Server

The Apple Server (for example, Mac Mini server) dynamically wraps the policy framework on iOS applications.

> ***Important:*** Ensure before installation that an Apple Server setup is available with a valid SSH username and password with connection details.

> ***Note:*** The following hardware requirements are needed only, if iOS devices are targeted within your project.

Component	Requirement
Processor	2.5 GHz Dual-Core Intel Core i5 (Turbo Boost up to 3.1 GHz) with 3 MB L3 cache
Memory	4 GB (two 2 GB) of 1600 MHz DDR3 memory
Internal Storage	500 GB (5400-RPM) hard drive
Network	10/100/1000 BASE-T Ethernet (RJ-45 connector)
Operating System	Apple OS X Version: 10.9.4 (13E28)

5.1.5 Windows 2003 server

These requirements are applicable only if you have Windows 6.x devices.

Component	Requirement
Processor	1.4 GHz (64- bit)
Memory	1 GB. For computers with more than 4 GB of RAM, be sure to confirm hardware compatibility by clicking the appropriate link in Support resources
Internal Storage	40 GB
Operating System	Windows Server 2003 Standard x64 Edition with SP2

5.2 Software Requirements

Requirement	Device OS				Operating System	
	iOS	Android	Windows 6.x	Windows Phone 8.x	Windows	Linux
Java Runtime Environment	Yes	Yes	Yes	Yes	Yes	Yes
Database Oracle 11g	Yes	Yes	Yes	Yes	Yes	Yes
Database Microsoft SQL Server 2008 R2 / 2012	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Device OS				Operating System	
	iOS	Android	Windows 6.x	Windows Phone 8.x	Windows	Linux
Database MySQL 5.5	Yes	Yes	Yes	Yes	Yes	Yes
Linux 64-bit	Yes	Yes	Yes	Yes	No	Yes
Android SDK TAR file	No	Yes	No	No	No	No
Mac OS	Yes	No	No	No	No	No
Xcode	Yes	No	No	No	No	No
Windows Server 2008	Yes	No	No	No	Yes	No
Windows Server 2012	Yes	No	No	No	Yes	No
Windows Server 2003	Yes	No	Yes	No	No	No
Exchange Server	Yes	Yes	No	Yes	No	No
Exchange Service	Yes	Yes	No	No	No	No
SCEP Server	Yes	No	No	No	No	No
CA Server	Yes	No	No	No	No	No

Requirement	Device OS				Operating System	
	iOS	Android	Windows 6.x	Windows Phone 8.x	Windows	Linux
Windows Mobile 6.x Group Policy Service	No	No	Yes	No	No	No
Verisign Secure SSL	Yes	No	No	Yes	No	No
GoDaddy Secure SSL	Yes	No	No	No	No	No
Wildcard Distribution Certificate	Yes	No	No	No	No	No
Wildcard Mobile Provisioning Profile	Yes	No	No	No	No	No
Launchpad Push Certificate	Yes	No	No	No	No	No
Launchpad Provisioning Profile	Yes	No	No	No	No	No
Apple Push Certificate for MDM	Yes	No	No	No	No	No
Keystore certificate	No	Yes	No	No	No	No
GCM Key	No	Yes	No	No	No	No

Requirement	Device OS				Operating System	
	iOS	Android	Windows 6.x	Windows Phone 8.x	Windows	Linux
Google MAPSv2 Key	No	Yes	No	No	No	No
Google Maps API	No	Yes	No	No	No	No
Symantec Enterprise Mobile Code Signing Certificate	No	No	No	Yes	No	No
Package Family Name	No	No	No	Yes	No	No

The following are the software requirements for installing Kony Management Suite management console:

Software	Requirement
Java Runtime Environment	Oracle Enterprise License JDK 1.8.0_xx *Important:* From V8 GA release, Kony Management does not support Java 7. Java 8 is the supported version.

Software	Requirement
Database	Oracle 11g Microsoft SQL 2008 R2 / 2012 MySQL 5.5 For MySQL database, you need to set event_scheduler = ON, socket =/var/lib/mysql/mysql.sock in /etc/my.cnf (or) /etc/mysql/my.cnf under the "[mysqld]" section. The global event_scheduler = ON System variable determines whether the Event Scheduler is enabled and running on the server, which is required for scheduling EMM jobs.
Operating System	Windows Server 2008 R2 Enterprise or Windows server 2012 R2 Standard Edition and above
Mac OS	OS X Version: Yosemite (10.10)
Xcode	XCODE Version: 6.1 (6A1052d) If you upgraded Xcode, open Xcode at least once after the upgrade to install all dependent components. Install iOS simulator 7.1 if you have not installed it previously.
Windows 2008/2012	Windows Server 2008 or 2012 operating system
Visual Studio	Visual Studio 2013 express edition with update 3 (pre-requisite for Windows app wrapping)
Microsof Silverlight Runtime	Microsoft Silverlight Runtime 5.0 (pre-requisite for Windows app wrapping)
Microsoft Silverlight	Microsoft Silverlight SDK 5.0 (pre-requisite for Windows app wrapping)

Software	Requirement
Cygwin	Cygwin (32 bit) 2.850 (pre-requisite for Windows app wrapping)
Windows 2003	Windows Server 2003 operating system
OpenSSL	Can be downloaded from : http://www.indyproject.org/Sockets/fpc/AMD64-Win64OpenSSL-0_9_8g.zip
Curl	Can be downloaded from : http://curl.askapache.com/download/curl-7.33.0-win64-ssl-sspi.zip
Public SSL Certificates	PEM format
Google Maps Key	Based on customer requirements, it can be Business Key or Free Key
Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package ATL Security Update	Can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=11895 file: `vcredist_x64`
msvcr110.dll,msvcr100.dll	Can be downloaded from http://www.dll-files.com/dllindex/dll-files.shtml?msvcr110 http://www.dll-files.com/dllindex/dll-files.shtml?msvcr100 Place under `C:\Windows\System32`
EMM Installation	Installation user should have Admin rights to install EMM as a service.

Software	Requirement
Android SDK zip file	Follow the steps given below under the **Android SDK Download** section to download Android SDK zip file.

> *Important:* If a user wants to upgrade EMM from older version to the latest EMM version, then a user needs to upgrade latest versions of Mac OS Version 10.9.4 (13E 28) and Xcode version 5.1.1(5B 1008).

5.3 Database Requirements

The following are the database requirements for Kony Management.

- MySQL requirements
- Oracle requirements
- MSSQL Requirements

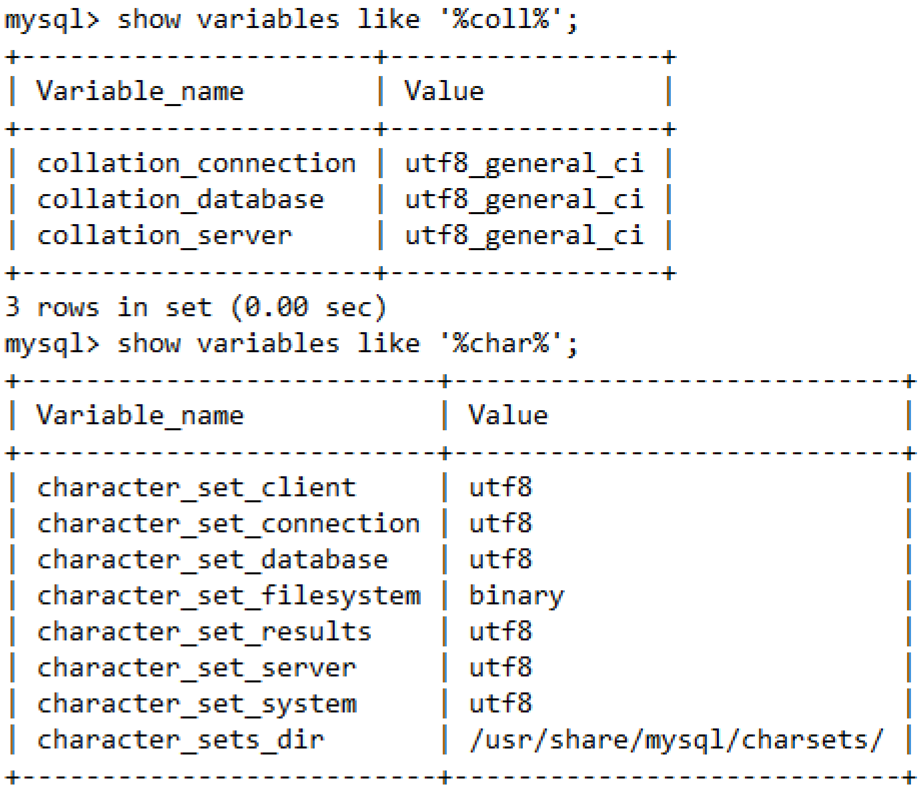
5.3.1 MySQL Requirements

- Only a qualified MySQL database administrator should handle the MySQL database setup.
- Supported versions are MySQL 5.5 and MySQL 5.6
- Configure your database with unicode character set as UTF8
- Modify **my.cnf** or **my.ini** files with the following parameters:

```
[client]
default-character-set = utf8
[mysql]
default-character-set = utf8
[mysqld]
character-set-client-handshake = FALSE
character_set_server='utf8'
```

- Restart your MySQL service

- To verify that your changes are applied correctly, verify the database variables by running the following query:



```
mysql> show variables like '%coll%';
+----------------------+-----------------+
| Variable_name        | Value           |
+----------------------+-----------------+
| collation_connection | utf8_general_ci |
| collation_database   | utf8_general_ci |
| collation_server     | utf8_general_ci |
+----------------------+-----------------+
3 rows in set (0.00 sec)
mysql> show variables like '%char%';
+--------------------------+----------------------------+
| Variable_name            | Value                      |
+--------------------------+----------------------------+
| character_set_client     | utf8                       |
| character_set_connection | utf8                       |
| character_set_database   | utf8                       |
| character_set_filesystem | binary                     |
| character_set_results    | utf8                       |
| character_set_server     | utf8                       |
| character_set_system     | utf8                       |
| character_sets_dir       | /usr/share/mysql/charsets/ |
+--------------------------+----------------------------+
```

5.3.2 Oracle Requirements

- Only a qualified Oracle database administrator should handle the Oracle database setup.

- Supported versions is Oracle 11g

- While creating the Oracle database, configure your database with unicode character set. **AL32UTF8** for Database characterset and **AL16UTF16** for National characterset.

- Create the following three tablespaces. These tablespaces will be used to create EMM database objects.

  - Tables and data tablespace: emm_data
  - Index tablespace: emm_index
  - Lob tablespace: emm_lob_data
- Create a database user with default tablespaces (emm_data) and grant quota to two other tablespaces (emm_index and emm_lob_data tablespaces).
  - If the Oracle database is of version 11gwithout pdb, then you can use the normal user for JDBC authentication.
- Grant the following permissions to the user.
  - **For versions below Oracle 11g without pdb option**: Grant connect, resource, create view, create procedure.
- Usage of the database service name.
  - **For versions below Oracle 11g without pdb option**: Use ORACLE_SID in the JDBC URL.

5.3.3 MSSQL Requirements

Prerequisites for Kony Management with SQL Server

- **Database User security role**: Create a database login `dbclient` using `SQL server authentication` with server roles as `sysadmin` and `public`
- **Database and schema access**: Installer will make use of the above login to create necessary databases and schemas required for the selected Kony Management components.
- **Database Growth sizing**: Refer to Kony Fabric Deployment Guide > Database Growth Sizing
- **Database Transaction log size**: Allocate sufficient space for the Transaction log file based on all the transactions activity of all the Kony Management components installed and as per your database backup policy. Because transaction log sizing is linked to database backup. If

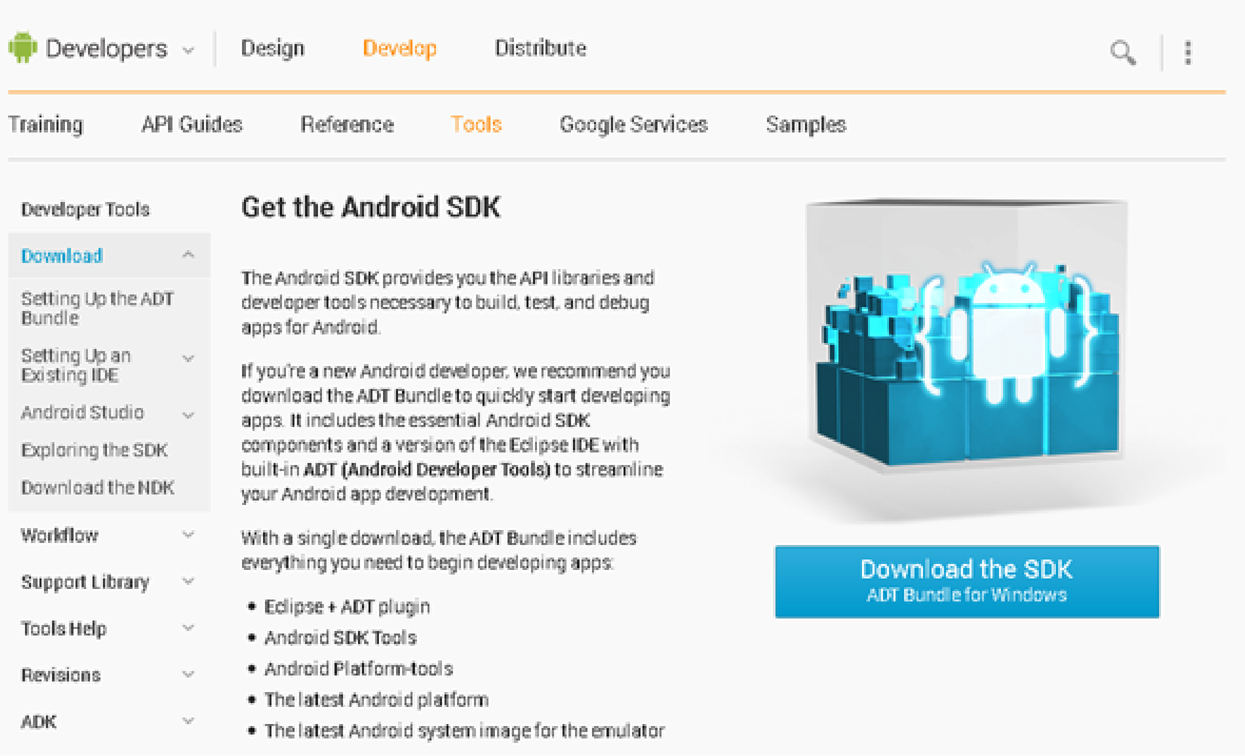
additional application logging/events are enabled in multiple components of Kony Management , then you may need to consider additional size for the transaction log.

- **Temp Database and temp log**: This is based on usage of all the databases on the server instance, by all applications connecting to these databases. In case of Kony Management, for sizing of the temp database, consider auto growth with increment size should be of 100MB and with maximum size to 10GB. But if application logging/events are enabled in multiple components of Kony Management, then the maximum size should be increased upto 20GB. This size will get reclaimed as and when the DB is restarted.
- **Database versions**: You can use **SQL Server Standard Edition** or **SQL Server Enterprise Edition** database for installing Kony Management. Kony Management is compatible with these editions. There are no prerequisites specific to these editions as Kony Management uses features common to both editions.
- **Backup plan**: You must use your organization's defined backup and retention policies for Backup strategies for your database.

5.4 Android SDK Download

The Android SDK provides you the API libraries and developer tools to build test and debug apps for Android.

For Windows , you may go to: http://developer.android.com/sdk/index.html?hl=sk



Get the Android SDK

The Android SDK provides you the API libraries and developer tools necessary to build, test, and debug apps for Android.

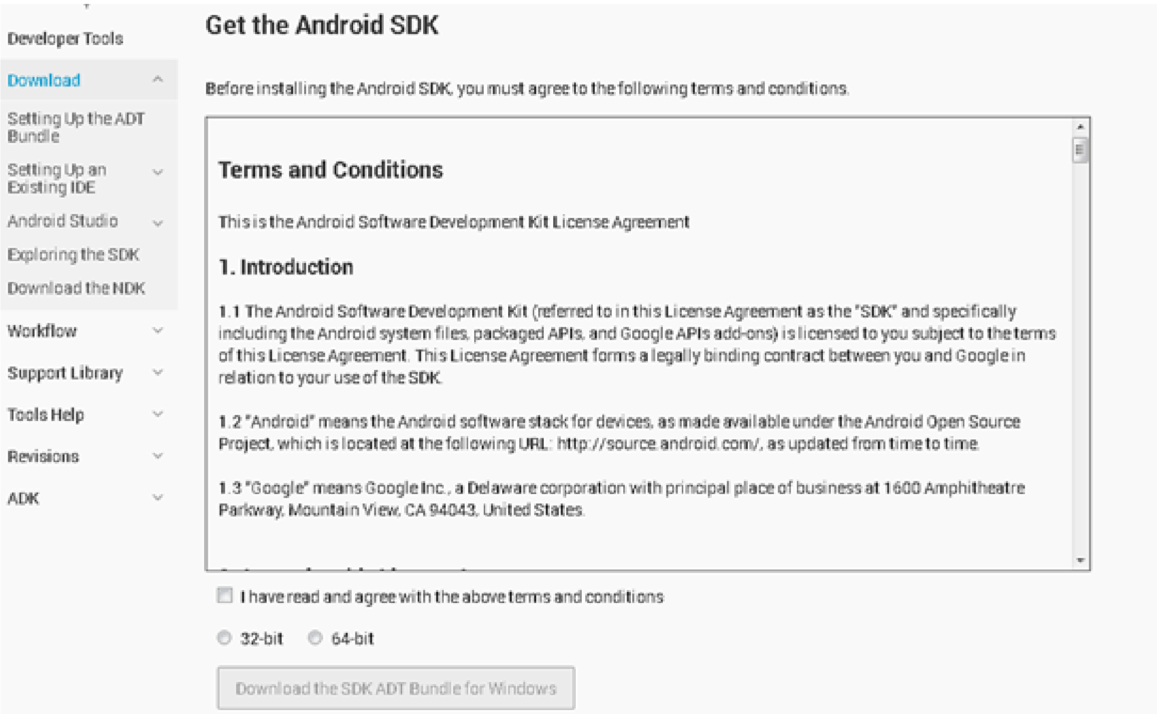
If you're a new Android developer, we recommend you download the ADT Bundle to quickly start developing apps. It includes the essential Android SDK components and a version of the Eclipse IDE with built-in **ADT (Android Developer Tools)** to streamline your Android app development.

With a single download, the ADT Bundle includes everything you need to begin developing apps:

- Eclipse + ADT plugin
- Android SDK Tools
- Android Platform-tools
- The latest Android platform
- The latest Android system image for the emulator

1. Click the **Download the SDK ADT Bundle for Windows** button.

   The **Get the Android SDK** window displays the Terms and Conditions.



Get the Android SDK

Before installing the Android SDK, you must agree to the following terms and conditions.

Terms and Conditions

This is the Android Software Development Kit License Agreement

1. Introduction

1.1 The Android Software Development Kit (referred to in this License Agreement as the "SDK" and specifically including the Android system files, packaged APIs, and Google APIs add-ons) is licensed to you subject to the terms of this License Agreement. This License Agreement forms a legally binding contract between you and Google in relation to your use of the SDK.

1.2 "Android" means the Android software stack for devices, as made available under the Android Open Source Project, which is located at the following URL: http://source.android.com/, as updated from time to time.

1.3 "Google" means Google Inc., a Delaware corporation with principal place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.

□ I have read and agree with the above terms and conditions

○ 32-bit ○ 64-bit

Download the SDK ADT Bundle for Windows

2. Accept the **Terms and Conditions**.

3. Choose 64-bit. EMM only supports Android SDK 64-bit.

4. You need to download the Android SDK 64-bit to your server, for example `D:\android.`

5. Extract the bundle, and traverse to:`D:\<EMM home folder>\adt-bundle-windows-x86_64-20140321\adt-bundle-windows-x86_64-20140321`

6. Click `SDK Manager.exe` in this folder and the entire Android SDK is downloaded directly from Google.

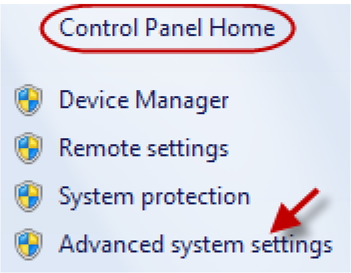
7. Rename the folder `adt-bundle-windows-x86_64-20140321 to android-sdk-windows`

8. When you download the SDK, by default the aapt tool is in the build-tools folder. You must copy it to the platform-tools folder.

> ***Note:*** Android SDK folder sholud be copied in EMM Home folder. The path sholud be as given below: D:\<EMM home folder>\android-sdk-windows

5.4.1 Environment Variables

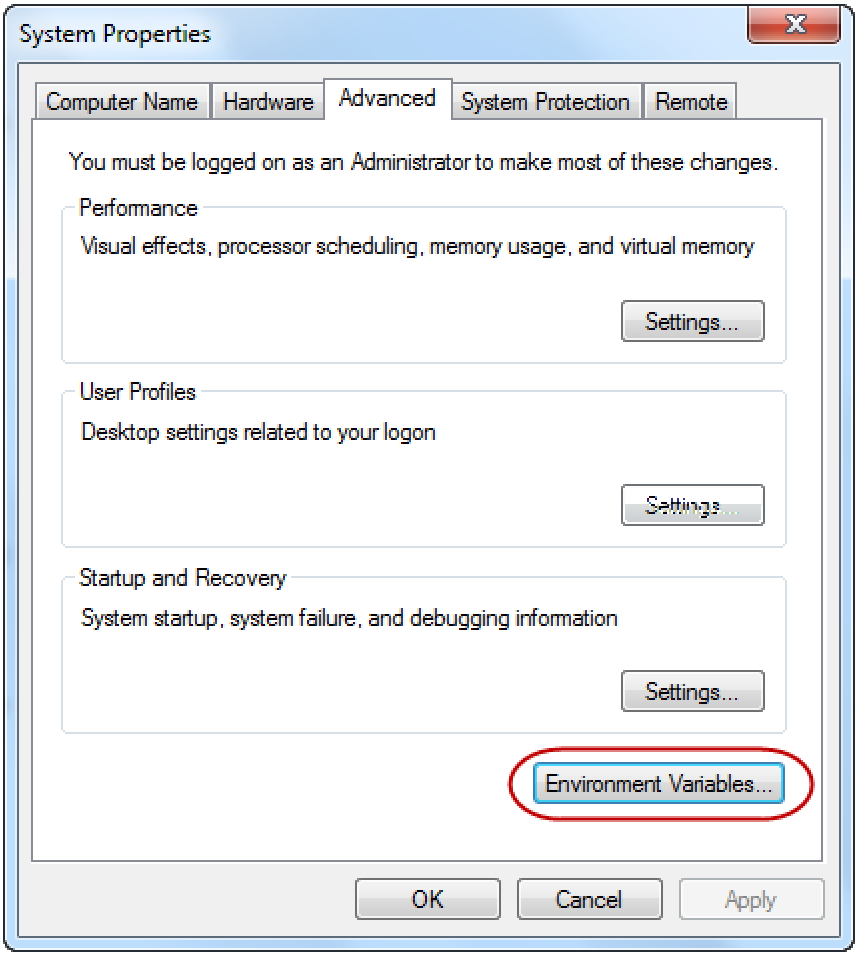
1. Right click My **Computer** > **Properties**.



2. Click **Advanced System Settings**.

   The **System Properties** window appears.

3. Click **Environment Variables**.



System Properties

You must be logged on as an Administrator to make most of these changes.

Performance
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles
Desktop settings related to your logon

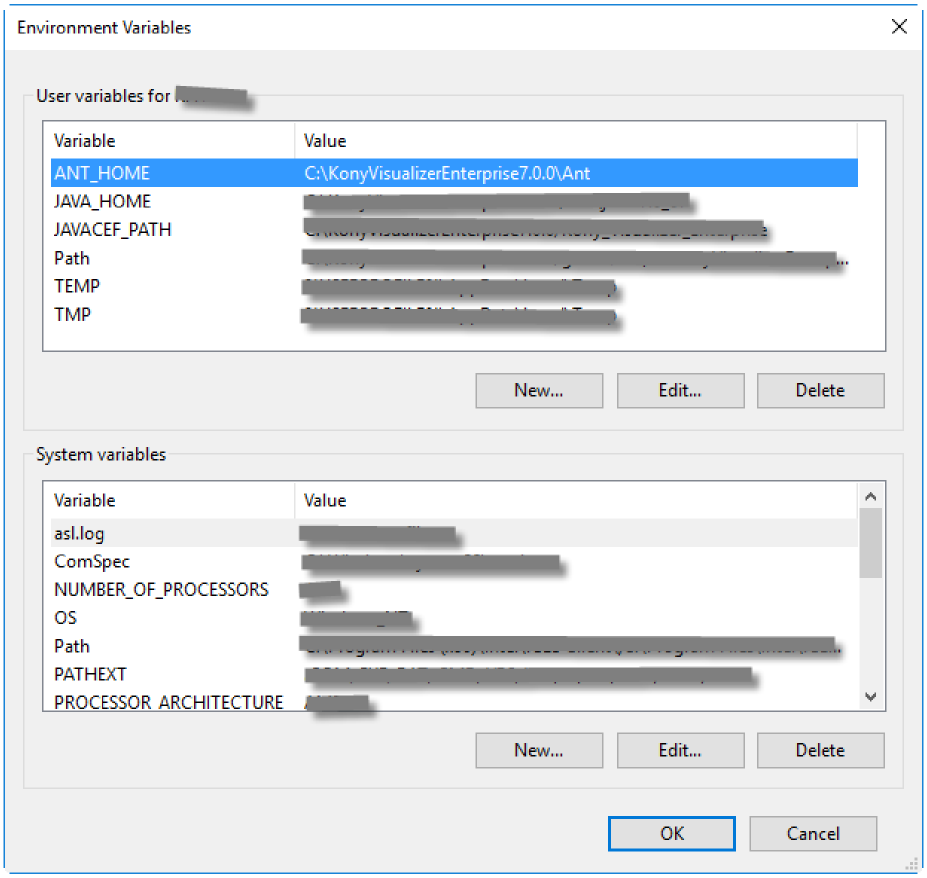
Startup and Recovery
System startup, system failure, and debugging information

4. In **Environment Variables**, the System Variables portion has a variable - Path. You need to edit the variable - Path of platform-tools and tools.

5. Define the paths for Curl and OpenSSL.

6. You need to give the absolute paths separated by semi-colons.
   If your drive is D, see the following example. You can replace D with your drive name.

```
 D:\ EMMConfig\android-sdk-windows\platform-tools ;
D:\EMMConfig\android-sdk-windows\ tools; <Path of the Curl folder>
 \curl-7.33.0-win64-ssl-sspi; <Path of the OpenSSL folder>
```



Environment Variables

User variables for [redacted]

Variable	Value
ANT_HOME	C:\KonyVisualizerEnterprise7.0.0\Ant
JAVA_HOME	[redacted]
JAVACEF_PATH	[redacted]
Path	[redacted]
TEMP	[redacted]
TMP	[redacted]

System variables

Variable	Value
asl.log	[redacted]
ComSpec	[redacted]
NUMBER_OF_PROCESSORS	[redacted]
OS	[redacted]
Path	[redacted]
PATHEXT	[redacted]
PROCESSOR_ARCHITECTURE	[redacted]

7. Add the variables and save.

8. Go to the command prompt at `C:\Users\<Username>\`

9. Verify the details.

10. Run the command `- echo %path%`

    In this scenario the newly updated paths must be present. If it is not present, set the environment variables again and ensure that it is done and saved properly.

5.4.2 Upgrading Android SDK

If you need to upgrade Android SDK, you need to:

1. Double- click `android.bat` in `D:\<EMM home folder>\android-sdk-windows\tools`
   This will upgrade the Android SDK on the system.
2. Delete the `1.apk` file in User home directory, for example, `C:\Users\<USER>\apktool\framework\`
3. Restart Tomcat.

> ***Note:*** Make sure that <Android SDK>/Platform-tools is added to the path variable.

To add the path variables, follow these steps:

1. Go to control panel > **System** >**Advanced** > **Environmental variable**, then add the required Classpath ...
2. To specify the path variables, refer the below link.

   http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/path.mspx?mfr=true

5.5 User Requirements

A database user should exist with DBA privileges for your Database (MySQL/Oracle/Microsoft SQL). Provide user the privilege to create another user. You can revoke this privilege once the installation is done.

For more information on how to create DB users and how to provide privileges to them, contact your database administrator.

- MySQL
- Microsoft SQL
- Oracle

5.5.1 MySQL Database

This user is leveraged by the installer to run scripts relating to EMM. After a successful EMM installation, you may revoke these super user privileges.

To create a MySQL database user for installer, follow these steps:

1. Use MySQL client tool to create a database user (for your reference we term it as `DB Client`. Use this username while providing inputs for the JDBC installer) with `MySQL root user`. For example, on a linux shell, invoke mysql client tool with following command:

   ```
   mysql -h localhost -u root -p
   ```

   Example output:

   ```
   # mysql -h localhost -u root -p
   Enter password:
   Welcome to the MySQL monitor. Commands end with ; or \g.
   Your MySQL connection id is 3
   Server version: 5.5.32 MySQL Community Server (GPL)
   ```

2. Grant all the privileges to create EMM databases and its respective objects (Tables, Indexes, Views,Procedures, Sequences, and Triggers).

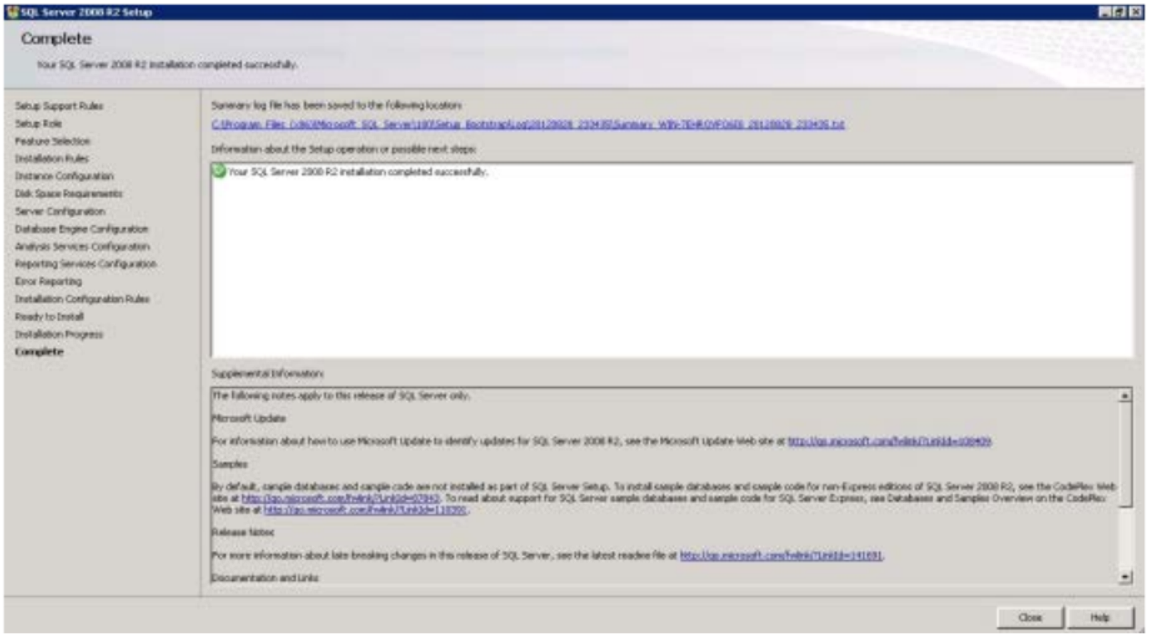
   ```
   CREATE USER 'dbclient'@'<EMM-installer-machine-ip>' IDENTIFIED
   BY '<password>';
   grant all on *.* to 'dbclient'@'<EMM-installer-machine-ip>'
   identified by
   '<password>';
   ```

   > ***Note:*** The <password> should be based on your standards. Installer machine IP has to be granted access to MySQL server with above statements.

5.5.2 Microsoft SQL Database

The steps to follow before running the database scripts packaged along with the installer for EMM are mentioned below:

1. Microsoft SQL Server database version 2008 or above needs to be installed with basic setup on the intended machine (use this machine's IP address while providing inputs for the JDBC installer).



Complete

Your SQL Server 2008 R2 installation completed successfully.

Summary log file has been saved to the following location:

C:\Program Files (x86)\Microsoft SQL Server\100\Setup Bootstrap\Log\20120828_233435\Summary_WIN-7E4R0VF0608_20120828_233435.txt

Information about the Setup operation or possible next steps:

Your SQL Server 2008 R2 installation completed successfully.

Supplemental Information:

The following notes apply to this release of SQL Server only.

Microsoft Update

For information about how to use Microsoft Update to identify updates for SQL Server 2008 R2, see the Microsoft Update Web site at http://go.microsoft.com/fwlink/?LinkId=108409.

Samples

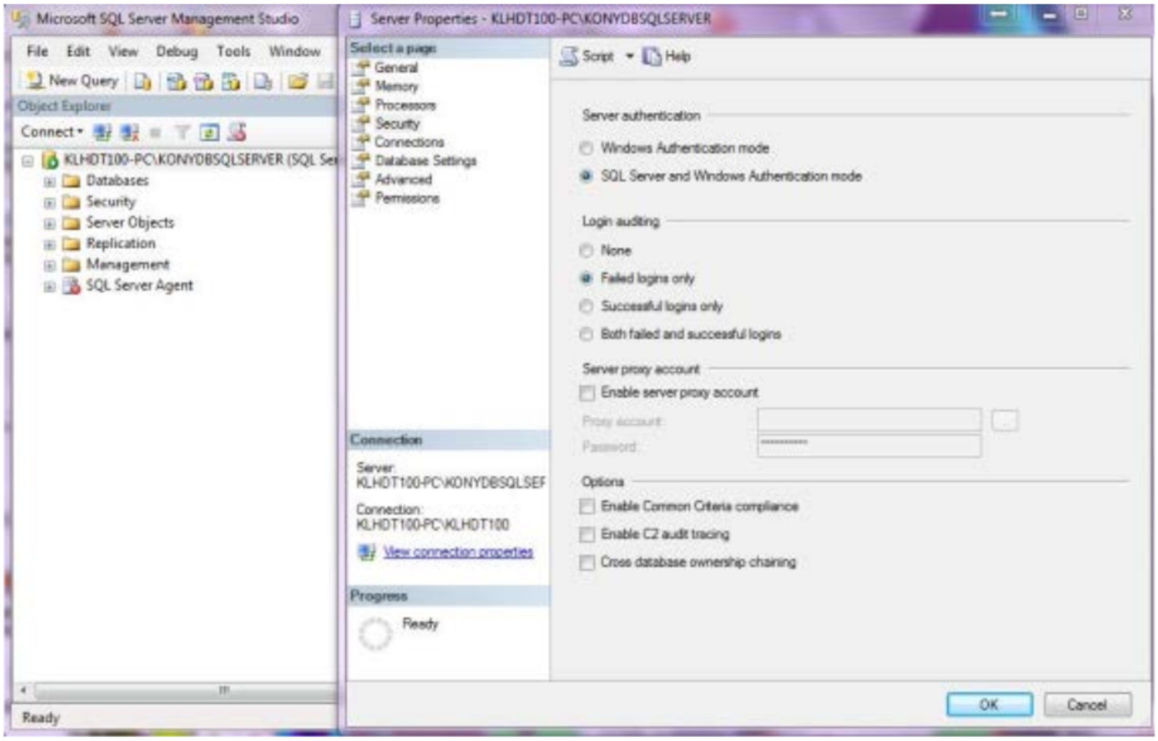
By default, sample databases and sample code are not installed as part of SQL Server Setup. To install sample databases and sample code for non-Express editions of SQL Server 2008 R2, see the CodePlex Web site at http://go.microsoft.com/fwlink/?LinkId=87843. To read about support for SQL Server sample databases and sample code for SQL Server Express, see Databases and Samples Overview on the CodePlex Web site at http://go.microsoft.com/fwlink/?LinkId=110391.

Release Notes

For more information about late breaking changes in this release of SQL Server, see the latest readme file at http://go.microsoft.com/fwlink/?LinkId=141691.

Documentation and Links

2. Use SQL Server Management Studio to enable database server authentication to SQL Server and Windows authentication mode.



Server:
KLHDT100-PC\KONYDBSQLSEF

Connection:
KLHDT100-PC\KLHDT100

View connection properties

Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Login auditing

○ None

● Failed logins only

○ Successful logins only

○ Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: **********

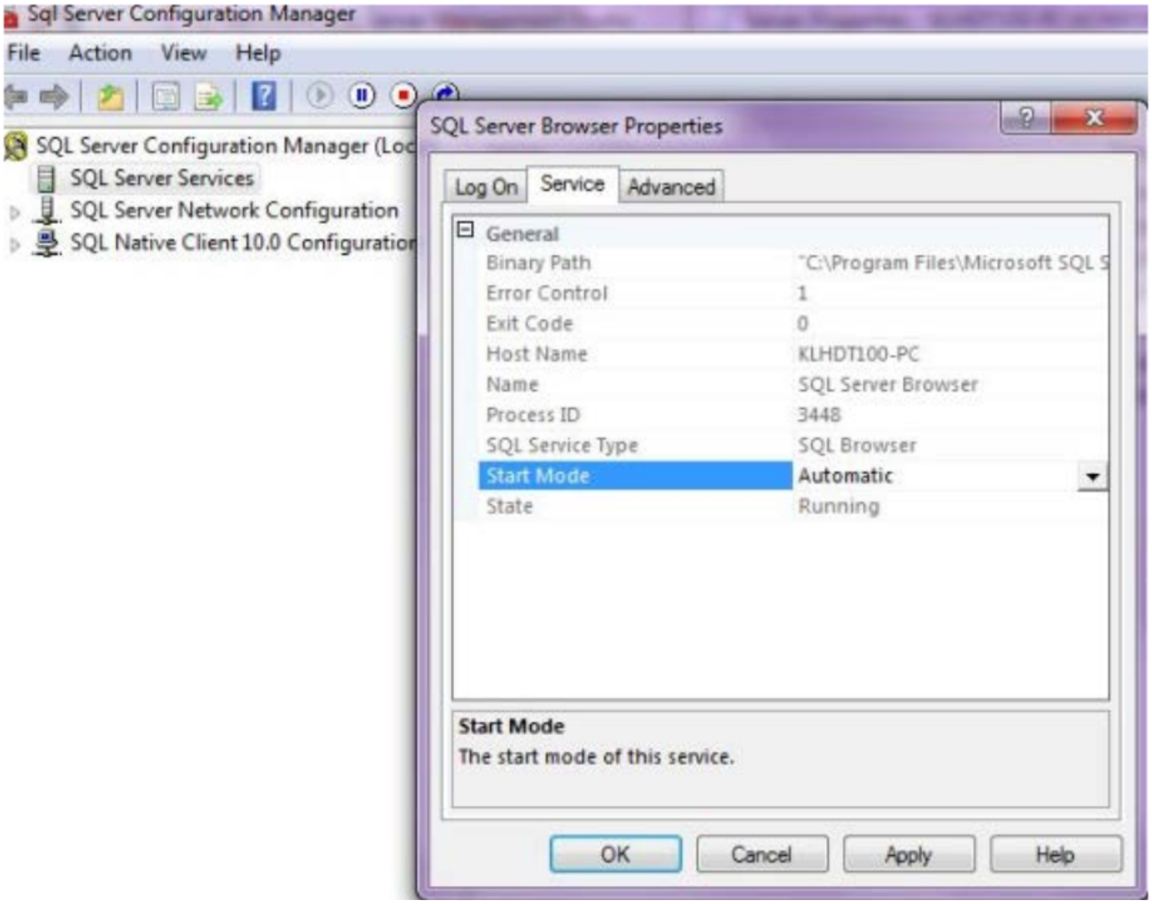
Options

□ Enable Common Criteria compliance

□ Enable C2 audit tracing

□ Cross database ownership chaining

3. Use SQL Server Configuration Manager and set the SQL Browser service start mode to automatic or manual, and then start the service.

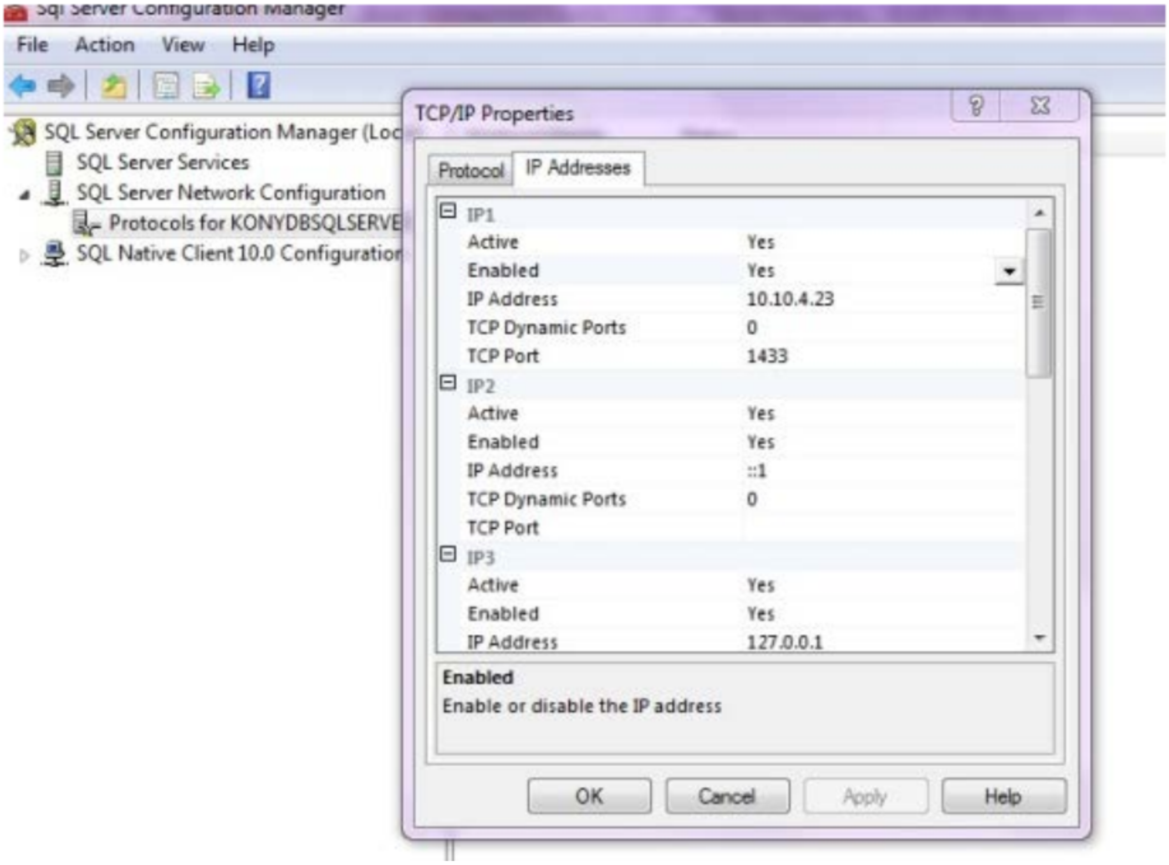

Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Loc
SQL Server Services
SQL Server Network Configuration
SQL Native Client 10.0 Configuratio
SQL Server Browser Properties
Log On
Service
Advanced
OK
Cancel
Apply
Help

General	
Binary Path	"C:\Program Files\Microsoft SQL S
Error Control	1
Exit Code	0
Host Name	KLHDT100-PC
Name	SQL Server Browser
Process ID	3448
SQL Service Type	SQL Browser
Start Mode	Automatic
State	Running

Start Mode
The start mode of this service.

4. In TCP/IP properties, enable TCP/IP protocols for a port in both Protocol/IP Addresses tabs (use this port on the installer while providing inputs for the JDBC installer) of the database server to accept the database connections.

> ***Note:*** For installer, it is suggested that the database should be on a remote server or separated from Middleware server (also installer machine). Middleware should be able to communicate to database through TCP/IP.

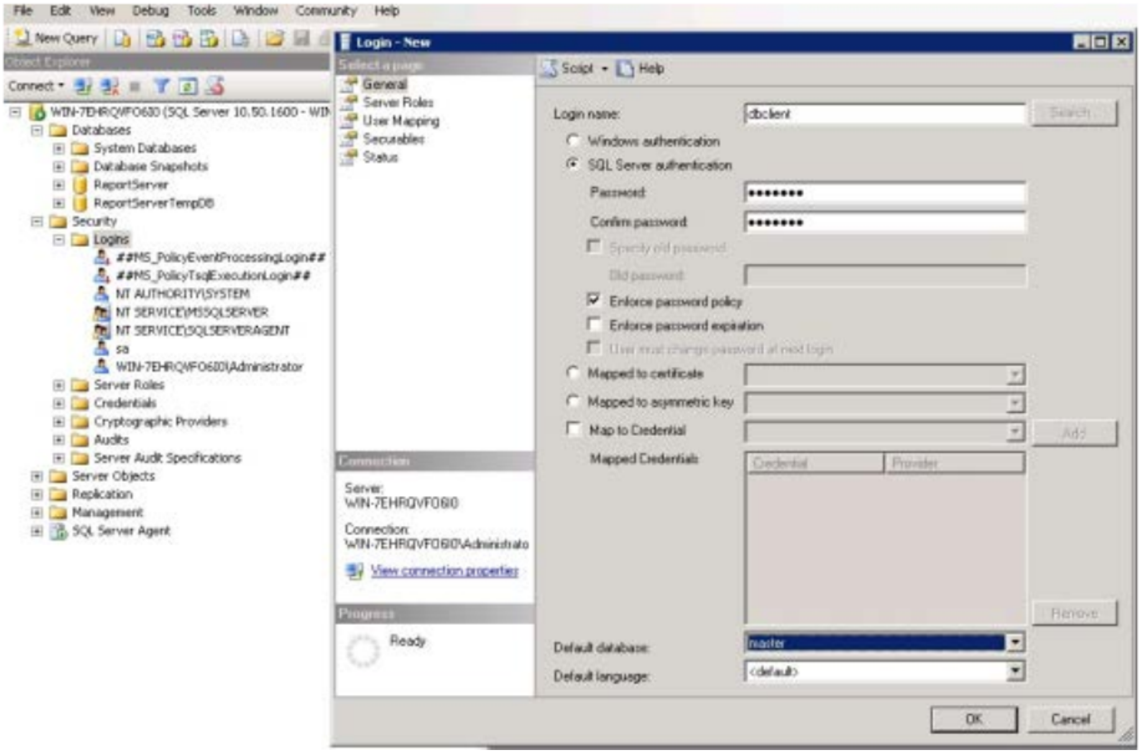

Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Loc
SQL Server Services
SQL Server Network Configuration
Protocols for KONYDBSQLSERVE
SQL Native Client 10.0 Configuratior
TCP/IP Properties
Protocol
IP Addresses
OK
Cancel
Apply
Help

IP1	
Active	Yes
Enabled	Yes
IP Address	10.10.4.23
TCP Dynamic Ports	0
TCP Port	1433
IP2	
Active	Yes
Enabled	Yes
IP Address	::1
TCP Dynamic Ports	0
TCP Port	
IP3	
Active	Yes
Enabled	Yes
IP Address	127.0.0.1

Enabled
Enable or disable the IP address

5. Use SQL Server Management Studio to create a database user with SQL server authentication to connect to SQL Server instance with server role as dbcreator,public. At this point of time no databases are created and installer will create necessary databases, schemas and all other objects. The created user owns all of KonyOne databases and schemas. The user is privileged to create databases and schemas, Tables, Indexes, Views, Procedures, Sequences, Trigger and can also provide the respective grants. For example: dbclient. Use this user while providing inputs for the JDBC installer.

> *Note:* The <password> can be as per your standards.



Login name: dbclient

○ Windows authentication

● SQL Server authentication

Password: •••••••

Confirm password: •••••••

☐ Specify old password

Old password:

☑ Enforce password policy

☐ Enforce password expiration

☐ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

☐ Map to Credential

Mapped Credentials:

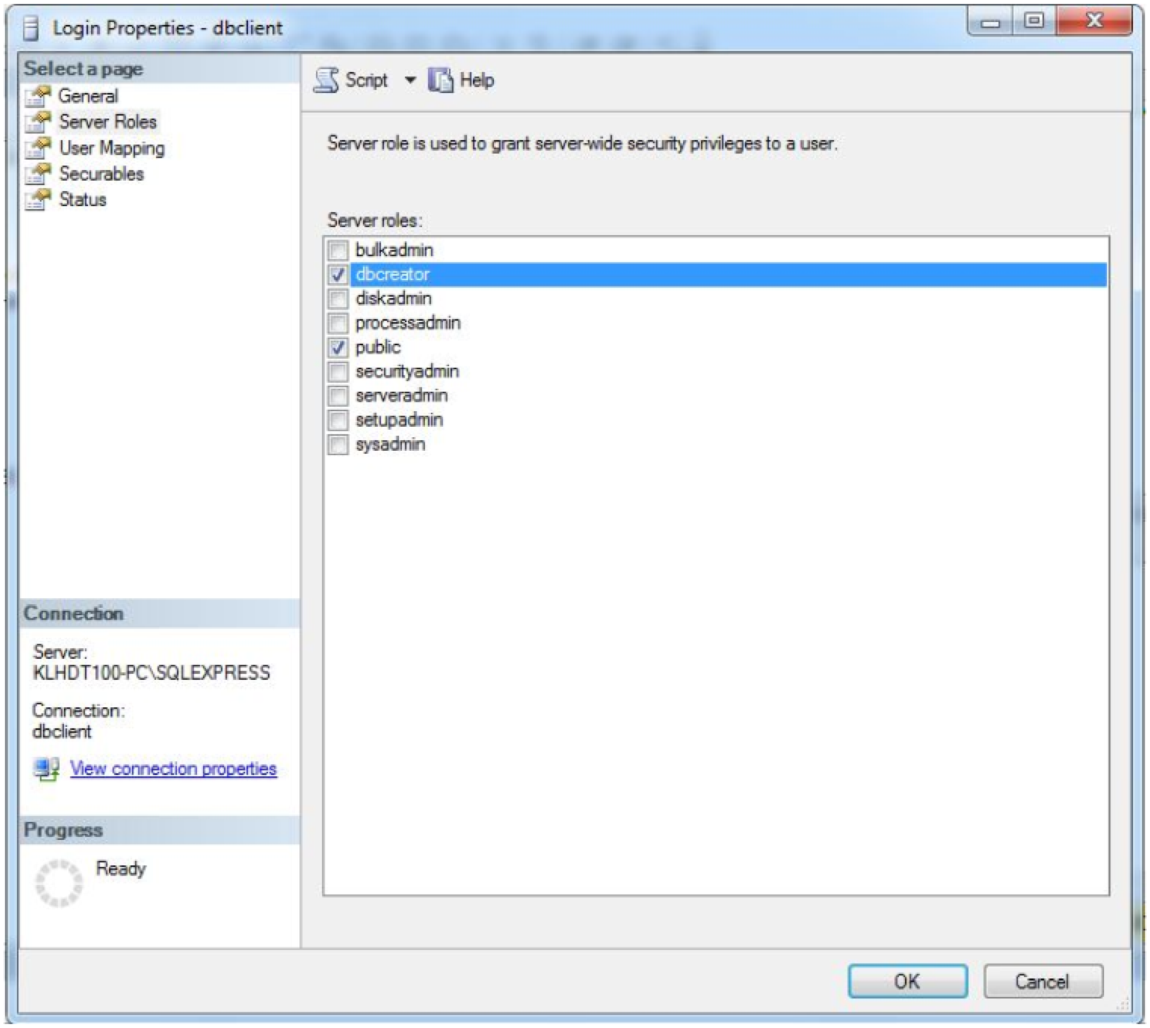
Credential	Provider

Default database: master

Default language: <default>

Server:
WIN-7EHRQVF06I0

Connection:
WIN-7EHRQVF06I0\Administrato



Server role is used to grant server-wide security privileges to a user.

Server roles:

- □ bulkadmin
- ☑ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- □ sysadmin

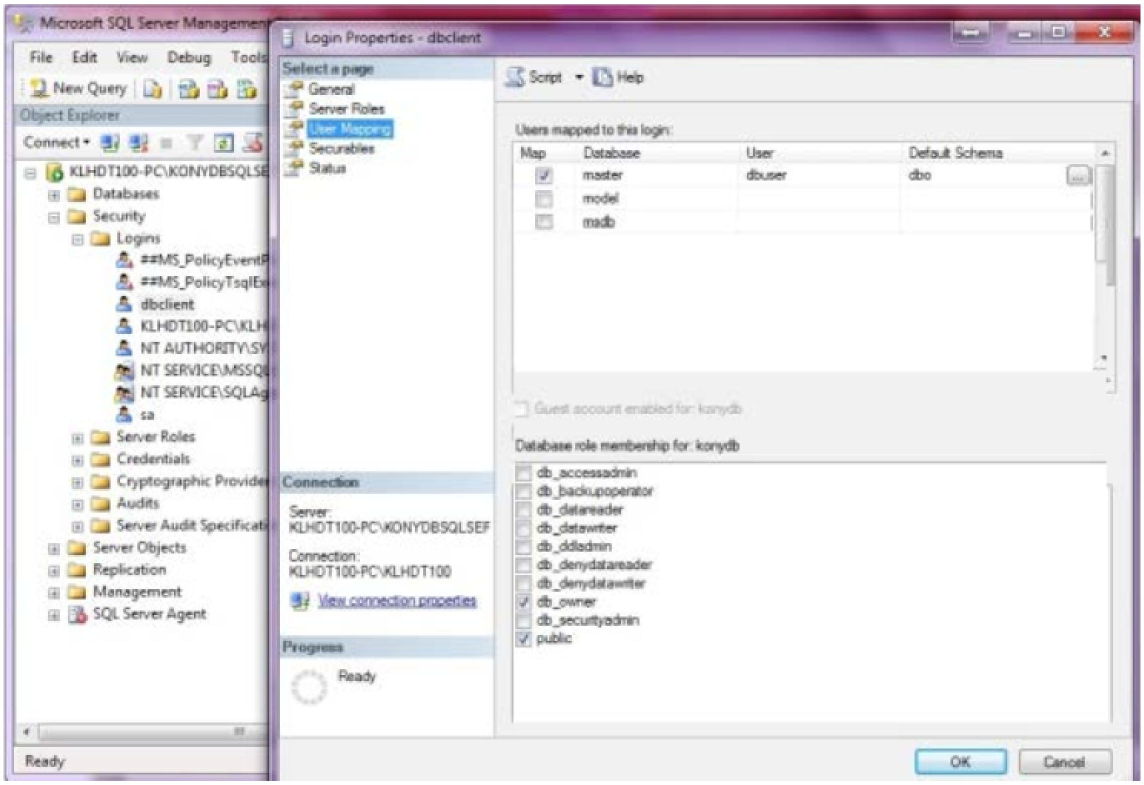
Connection

Server:
KLHDT100-PC\SQLEXPRESS

Connection:
dbclient

Progress

Ready



Users mapped to this login:

Map	Database	User	Default Schema
☑	master	dbuser	dbo
☐	model		
☐	msdb		

☐ Guest account enabled for: konydb

Database role membership for: konydb

☐ db_accessadmin
☐ db_backupoperator
☐ db_datareader
☐ db_datawriter
☐ db_ddladmin
☐ db_denydatareader
☐ db_denydatawriter
☑ db_owner
☐ db_securityadmin
☑ public

Connection

Server:
KLHDT100-PC\KONYDBSQLSEF

Connection:
KLHDT100-PC\KLHDT100

View connection properties

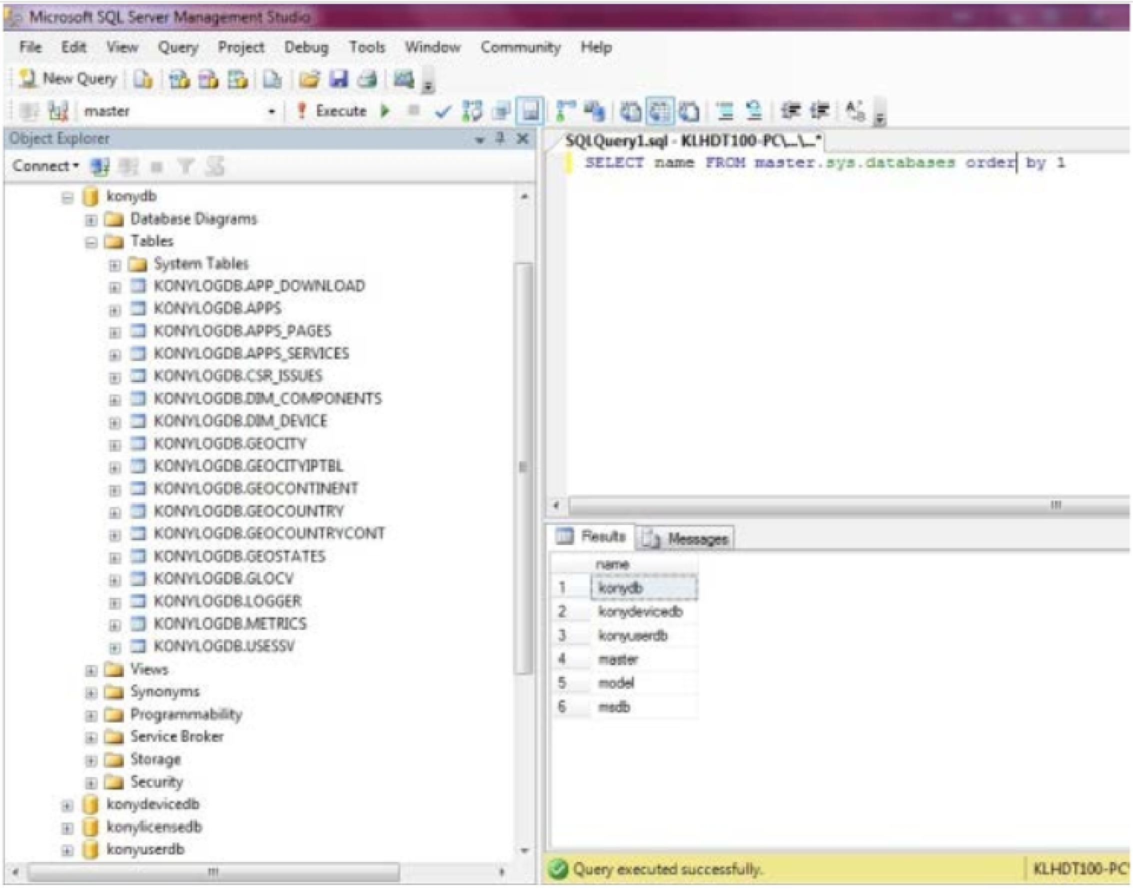
Make sure to provide all the above values in the respective parameters of the installer.

5.5.2.1 Microsoft SQL Server Database Post-installation Steps

To verify the successful database configuration, follow these steps:

1. Use SQL Server Management Studio to check if the deployment is successful, and to check if all objects are created successfully.
2. Run the following query:

```
select name FROM master.sys.databases

go
```



```
SELECT name FROM master.sys.databases order by 1
```

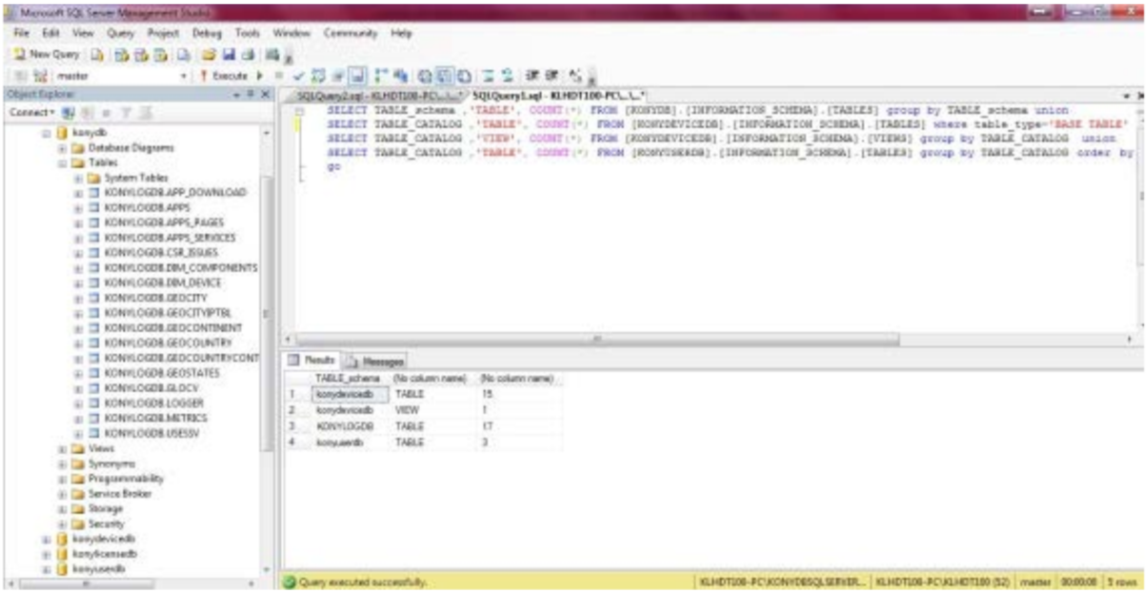
	name
1	konydb
2	konydevicedb
3	konyuserdb
4	master
5	model
6	msdb

Query executed successfully.

3. Run the entire statement as one full query as shown below:

```
SELECT TABLE_schema ,'TABLE', COUNT(*) FROM [KONYDB].
[INFORMATION_SCHEMA].[TABLES] group by TABLE_schema union
SELECT TABLE_CATALOG ,'TABLE', COUNT(*) FROM [KONYDEVICEDB].
[INFORMATION_SCHEMA].[TABLES] where table_type='BASE TABLE'
group by TABLE_CATALOG union
SELECT TABLE_CATALOG ,'VIEW', COUNT(*) FROM [KONYDEVICEDB].
[INFORMATION_SCHEMA].[VIEWS] group by TABLE_CATALOG union
SELECT TABLE_CATALOG ,'TABLE', COUNT(*) FROM [KONYUSERDB].
[INFORMATION_SCHEMA].[TABLES] group by TABLE_CATALOG order by 1
go
```

If the above query is broken and run individually, you will receive unintended outputs.



```
SELECT TABLE_schema ,'TABLE', COUNT(*) FROM [KONYDB].[INFORMATION_SCHEMA].[TABLES] group by TABLE_schema union
SELECT TABLE_CATALOG ,'TABLE', COUNT(*) FROM [KONYDEVICEDB].[INFORMATION_SCHEMA].[TABLES] where table_type='BASE TABLE'
SELECT TABLE_CATALOG ,'VIEW', COUNT(*) FROM [KONYDEVICEDB].[INFORMATION_SCHEMA].[VIEWS] group by TABLE_CATALOG  union
SELECT TABLE_CATALOG ,'TABLE', COUNT(*) FROM [KONYUSERDB].[INFORMATION_SCHEMA].[TABLES] group by TABLE_CATALOG order by
go
```

	TABLE_schema	(No column name)	(No column name)
1	konydevicedb	TABLE	15
2	konydevicedb	VIEW	1
3	KONYLOGDB	TABLE	17
4	konyusedb	TABLE	3

Query executed successfully. | KLHDT100-PC\KONYDBSQLSERVER... | KLHDT100-PC\KLHDT100 (52) | master | 00:00:00 | 5 rows

5.5.3 Oracle Database

As part of prerequisites for Oracle database, you need to create tablescape, create a user with some privileges and map the created user with the tablespace.

To perform Oracle prerequsites, do the following:

1. Using a SQLPlus or another Database client, connect to your Oracle database as Sysdba.
2. Create three tablescape `(emm_data, emm_index, and emm_lob_data)` by executing the command given below

```
CREATE TABLESPACE EMM_DATA DATAFILE '<DATA_FILE_PATH>/emm_
data.dbf'
SIZE 2048M AUTOEXTEND ON NEXT 100M MAXSIZE 5120M;
CREATE TABLESPACE EMM_INDEX DATAFILE '<DATA_FILE_PATH>/emm_
```

```
index.dbf'
SIZE 2048M AUTOEXTEND ON NEXT 100M MAXSIZE 5120M;
CREATE TABLESPACE EMM_LOB_DATA DATAFILE '<DATA_FILE_PATH>/emm_lob_
data.dbf' SIZE 2048M AUTOEXTEND ON NEXT 100M MAXSIZE 5120M;
```

3. Create a new user with DBA privilages by executing the command given below:

```
CREATE USER <install-user>
IDENTIFIED BY <password>
DEFAULT TABLESPACE EMM_DATA
TEMPORARY TABLESPACE TEMP
PROFILE DEFAULT;
GRANT CREATE SESSION,RESOURCE,CREATE USER TO <install-user> with
admin option;
```

> ***Note:*** If your organization does not want to provide DB privilages to this user, provide the user, Create Session, Connect (a role), and Create User privilages.

4. Map the user with tablespaces by execuitng the command given below:

```
ALTER USER <install-user> QUOTA UNLIMITED ON EMM_DATA;
ALTER USER <install-user> QUOTA UNLIMITED ON EMM_INDEX;
ALTER USER <install-user> QUOTA UNLIMITED ON EMM_LOB_DATA;
```

5.6 Network-Related Prerequisites

A firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network that is not assumed to be secure and trusted. Firewall permits traffic for the ports that are required for the communication. The purpose of ports is to uniquely identify different applications or processes running on a single computer and thus enable them to share a single physical connection to a packet-switched network.We recommend the following firewall settings for a successful EMM installation.

5.6.1 Port Configurations

We recommend the following firewall settings for a successful EMM installation.

Firewall Settings required for EMM Server

The firewall settings of EMM Server are defined in the table below:

Source	Destination	Port	Protocol	Direction	Action	Description
EMM Server	Your SMTP Server hostname Example: relay.appriver.com	25	TCP	Outbound	Allow	The EMM Server communicates with the SMTP Server through the SMTP Port. It sends emails to both administrators and users based on action or workflow triggers.
EMM Server	Database Server	For MySQL 3306	TCP	Both	Allow	For establishing EMM Server JDBC connectivity.
EMM Server	dl-ssl.google.com	443	TCP	Both	Allow	To connect and update Android SDK software.

Source	Destination	Port	Protocol	Direction	Action	Description
EMM Server or Load Balancer VIP	For Internet or Intranet (If external access is required for Intranet, then it is done through VPN)	HTTP 80 (Optional), HTTP 443	TCP	Both	Allow	For establishing communication among devices/browsers and the EMM server.
EMM Server	Microsoft Active Directory Server (ADS)	389	TCP	Both	Allow	To import Users and Groups from ADS, which helps users to login into EMM with Active Directory Server credentials.

Source	Destination	Port	Protocol	Direction	Action	Description
EMM Server	Microsoft Active Directory Services through secure channels. (Optional)	636	TCP	Both	Allow	To import Users and Groups from ADS, which helps users to login into EMM with Active Directory Server credentials over secure port with Microsoft Active Directory Services through secure channels.
EMM Server	SCEP Server	80, 443	TCP	Both	Allow	EMM Server will interact with the SCEP server for iOS device enrolment. Installer will validate the SCEP server connection.

Source	Destination	Port	Protocol	Direction	Action	Description
EMM Server	Mac Server	22	TCP	Both	Allow	For establishing SSH connectivity to the Mac build Server from the EMM Server. The Mac build Server is used for binary wrapping and dynamic policy injection for iOS.
EMM Server	Windows Server 2012	22	TCP	Both	Allow	For establishing SSH connection to the Windows build server from the EMM Server. The Windows build

Source	Destination	Port	Protocol	Direction	Action	Description
EMM Server and Devices	itunes.apple.com	443	HTTPS	Both	Allow	Kony EMM Server searches the apps from the iTunes for the given keyword on HTTPS using ports 443. Similarly, devices also need to access the iTunes store to download apps through the same port.
EMM Server	www.apple.com	443	HTTPS	Both	Allow	Kony EMM Server obtains the Apple Root certificate hosted on the domain to generate the APNS certificate.

Source	Destination	Port	Protocol	Direction	Action	Description
EMM Server	developer.apple.com	443	HTTPS	Both	Allow	Kony EMM Server obtains the Apple WWDR certificate hosted on the domain to generate the APNS certificate.
EMM Server	play.google.com	443	HTTPS	Both	Allow	Kony EMM Server searches the apps from the Google Store for the given key word on HTTPS using 443. Similarly, devices also need to access the Google Play Store to download apps through the same ports.

Source	Destination	Port	Protocol	Direction	Action	Description
Devices	Google Cloud	5228, 5229, 5230	TCP, HTTP, HTTPS, UDP	Both	Allow	When a device is on corporate WiFi network, ensure that 5228. 5229, 5230 ports are open to recover push notifications from Google Cloud

Note: Verify that all required ports are open by using the command telnet `<domain name> <port>`.

5.6.2 Push Notification - Firewall Change

Source	Destination	Service	Protocol	Direction	Action	Description
EMM Server	android.apis.google.com, android.googleapis.com/gcm/send	443	TCP	Both	Allow	Allow the EMM Server to access Google's cloud Messaging service.
EMM Server	gateway.push.apple.com, gateway.sandbox.push.apple.com	2195	TCP	Both	Allow	Allow the EMM Server to access Apple's APNs service.

Source	Destination	Service	Protocol	Direction	Action	Description
EMM Server	feedback.push.apple.com, feedback.sandbox.push.apple.co	2196	TCP	Both	Allow	Allow the EMM Server to access Apple's APNs service
Internal Corporate WiFi router for Mobile Devices	You must accept outgoing connections to all IP addresses contained in the IP blocks listed in Google’s ASN of 15169. For IP Addresses and Firewall Settings, refer https://developer.android.com/google/gcm/http.html	5228, 5229, 5230	TCP	Both	Allow	Apple devices connect to APNs servers through this port.

Source	Destination	Service	Protocol	Direction	Action	Description
Internal Corporate WiFi router for Mobile Devices	ax.init.itunes.apple.com, ocsp.apple.com	80, 443	TCP	Both	Allow	Apple devices connect to public Apple OCSP and iTunes service through this port.
EMM Server	gateway.push.apple.com gateway.sandbox.push.apple.com	2195	TCP	Both	Allow	Allow the KPNS server to access Apple's APNs service.

Source	Destination	Service	Protocol	Direction	Action	Description
EMM Server	feedback.sandbox.push.apple.com feedback.push.apple.com	2196	TCP	Both	Allow	Allow the KPNS server to access Apple's APNs service.
Internal Corporate WiFi router for Mobile Devices	android.apis.google.com android.googleapis.com	443	TCP	Both	Allow	Android devices will connect to GCM through this port.

Note: Verify that all required ports are open by using the command telnet `<domain name> <port>`.

Important: Do not attempt to route traffic directly from Load Balancer to EM Tomcat Server (runs on 8080 port). Make sure that all traffic goes through EMM Apache HTTP Server.

Note:

iOS Certificate validation: The first time a user opens an app, the distribution certificate is validated

> by contacting Apple’s OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server isn’t interpreted as a revocation. To verify the status, the device must be able to reach ocsp.apple.com. The OCSP response is cached on the device for the period of time specified the OCSP server—currently, between three and seven days. The validity of the certificate is not checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app is prevented from running. Revoking a distribution certificate invalidates all of the apps you have signed with it. You should revoke a certificate only as a last resort—if you are sure the private key is lost or the certificate is believed to be compromised.

To complete the EMM installation successfully, it is essential that the chosen domain name should be resolved to the proper IP address. This is based on the mapped DNS record either with nslookup or dig from the EMM installation server.

For example, if your chosen domain name is www.example.com and it is mapped in the DNS to the load balancer VIP - 93.184.216.119. The same has to be resolved, when you issue the following command as displayed below:

```
nslookup www.example.com
```

or

```
dig www.example.com
```

```
C:\Users\TEMP>nslookup www.example.com

Server: kitspl.com

Address: 10.10.19.11

Non-authoritative answer:

Name: www.example.com

Addresses: 2606:2800:220:6d:26bf:1447:1097:aa7

93.184.216.119
```

This is also applicable for intranet based domains.

5.6.3 Reverse Proxy Settings

If your EMM server will be behind reverse proxies like IIS or iPlanet etc, ensure that the query string limit is enhanced from 2048 to 4096 as MDM enrollment process requires it. iOS builtin MDM agent passes the certificate to EMM Servers as a query string in GET request. Depending on the key strength, the query string length varies. For example, 2048 key strength will generate certificate with a length of 4000 characters (base64 encoded string).

In case of an IIS server, you should change the values for maxUrlLength maxQueryLength in web.config of the website (for example,emm.company.com) used for EMM.

```
<system.web>
<httpRuntime maxUrlLength="4096" maxQueryStringLength="16384" />
</system.web>
```

If this setting for reverse proxy servers does not work, contact Microsoft support for further help to enhance the values for maxUrlLength, and maxQueryLength.

If the IIS Server is installed on a 64-bit machine, the web.config file where the **httpruntime** rule needs to be added would be located in the path **%systemdrive%/Microsoft.NET/Framework64/<.NET Version>/config/**.

Here, the **%systemdrive% = Windows installation folder** and **<.NET Version> = The latest version of .NET framework installed on the machine**.

> ***Note:*** For EMM web application, ensure that the HTTP method PUT is enabled for the endpoint /devicemanager/ota/checkin. This is mandatory for iOS enrollment.

5.6.4 Windows Mobile 6.x Firewall Settings

To support Windows Mobile 6.x devices, ports should be configured properly to ensure there is no conflict.

Source	Destination	Port	Protocol	Direction	Action	Description
Windows Mobile 6.x Device	Windows Server 2003	80, 443, 8443	HTTP / HTTPS	Both	Allow	Windows Mobile 6.x device will communicate with Windows Server 2003 on HTTP/HTTPS using ports 80,443,8443
EMM Server	Windows Server 2003	8883	HTTPS	Both	Allow	Kony EMM Server pulls data from Windows Server 2003 via the KonyWin6MDMService using HTTPS on Port 8883
Windows Server 2003	Windows Server 2008/2012	7777	HTTP (S)	Both	Allow	The Windows Server 2003 [Mobile Device Manager component] and Windows Server 2008/2012 [Group Policy component] both reside in the same network and the communication is carried over HTTP(S) on Port 7777.

Source	Destination	Port	Protocol	Direction	Action	Description
Windows Server 2008/2012	Windows Server 2003	8888	HTTP (S)	Both	Allow	The Windows Server 2008/2012 and Windows Server 2003 both reside in the same network and the communication is carried over HTTP(S) on Port 8888.

> ***Note:*** Verify that all required ports are open by using the command telnet `<domain name> <port>`.

These need to be configured during installation. If no changes are provided, the defaults are kept. It is advised to change these defaults as there are several applications and OS processes that capture these ports. This may result in a broken pipe and loss of communication. Ports above 1024 are preferred as they are less prone to capture from any system resources or third-party applications.

5.6.5 Exchange Server Firewall Changes

Exchange Server is required by EMM to send mails to EMM Users and Administrators. Additionally, if you wish to configure Email and Calendar settings on devices, you must open these ports.These settings should be configured only if Exchange Server is installed.

Source	Destination	Port	Description
EMM Server	Exchange Server	Default SMTP Port: 25 SMTPS Port: 465 Any available port can be choosen.	EMM Server needs to communicate with Exchange mail Service to send notification emails.
Kony Exchange Service	Exchange Server	HTTPS Port: 443 User configured.	Kony Exchange Service needs to perform Powershell remoting with the Exchange Server
EMM Server	Kony Exchange Service	User configured	EMM Server needs to communicate with Kony Exchange Service to block or unblock emails for the device

Note: Verify that all required ports are open by using the command telnet `<domain name> <port>`.

Note: The port number you provided while setting Exchange service should be provided for EMM Server .

5.7 Exchange Server Prerequisites

This section describes the configuration steps to be performed on the Windows instance where your corporate Exchange Server is installed. Usually Exchange server settings are taken care by the enterprise hosting your exchange server.

1. Enable powershell remoting using the "Enable-PSRemoting" cmdlet. Ensure that you have admin privileges before you execute this command. For more information, refer http://technet.microsoft.com/en-us/library/hh849694.aspx

2. Set trusted hosts. This includes a list of ip addresses or DNS names from which you need to entertain powershell remoting.

   Powershell console commands are:

   `cd WSMan:\localhost\Client:` This will move to the WSMan Client policy directory.
   `Set-Item .\TrustedHosts *: "*"` will allow all. If specific IPs or DNS addresses are present;
   add the values separated by commas.

3. Allowing/Disallowing unencrypted traffic:

   Unencrypted traffic means using HTTP. If remoting has to work over HTTP, use the following commands:

   ```
   cd WSMan:\localhost\Client: This will move to the WSMan Client
   policy directory
   .Set-Item .\AllowUnencryptedTraffic $true: This will allow the
   session to work without encryption.
   ```

   After executing the above mentioned commands on powershell, open **IIS Server Manager>Sites>Default Web Site>Powershell** and disable SSL. Disable Basic authentication.

   Disallowing unencrypted means using HTTPS. The commands are as follows:

   ```
   cd WSMan:\localhost\Client
   Set-Item .\AllowUnencryptedTraffic $false
   ```

   After executing the above mentioned commands on powershell, open **IIS Server Manager>Sites>Default Web Site>Powershell** and enable SSL. Enable Basic authentication.

4. Restart the IIS Server.

5. Restart the WinRM Service. Powershell cmdlet for this is `Restart-Service WinRM`

   For more information, refer Kony Exchange Service Document.

6. Windows 2008 2012 Server setup

> *Important:* Steps in this section must be executed by a Windows server administrator. If you have any questions, contact your Windows Server Administrator.
>
> Kony Management server requires Windows Server 2012, in order to manage enterprise apps for Windows Phone 8.1.

Windows 2008/2012 server setup includes the following components. The following can be implemented on a single Windows 2008/2012 server or on different servers.

> *Note:* Make sure that all Windows Servers are in one domain.
>
> If you want to install SCEP components using Kony EMM Windows components installer, click here.

- Setting SCEP server
- Setting Exchange Service
- Setting Group Policy Service
- Setting Visual Studio
- Setting Microsoft Silverlight runtime
- Setting Microsoft Silevrlight SDK
- Setting Cygwin

6.1 Setup SCEP and CA Server

To enable EMM to support iOS devices, certificate distribution through Simple Certificate Enrollment Protocol (SCEP) server is mandatory.This must be done before the EMM installation process begins. A certificate authority (CA) must also be set to sign certificates distributed by the SCEP server.

> ***Note:*** SCEP setup is not required in case of SA Mode (or MAM only license).

6.1.1 Supported Operating Systems

- Windows Server 2008 data center Edition R2 with Service Pack 2
- Windows Server 2008 Enterprise Edition

For more information, refer Windows Server 2012 video tutorial and Active Directory Certificate Services

> ***Important:*** SCEP can also be installed on the same Windows server on which EMM is installed using multiple IP addresses. However, this is not a recommended approach for production environment.

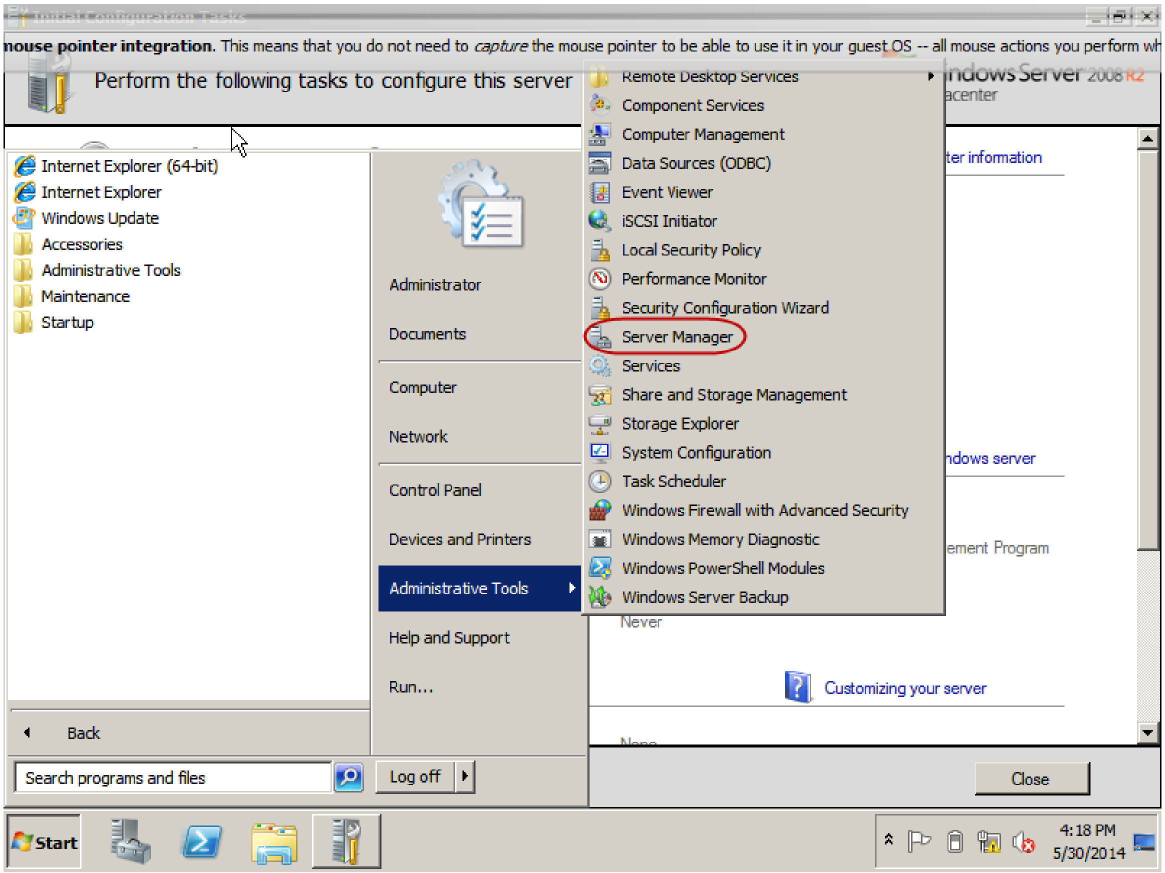
6.1.2 SCEP Server Setup on Windows Server 2008

This section covers the basics of setting up a SCEP server.

To setup SCEP server, follow these steps:

> ***Note:*** Note that you can also setup SCEP Server on Windows Server 2012.

1. Click the **Server Manager** icon on the task bar.

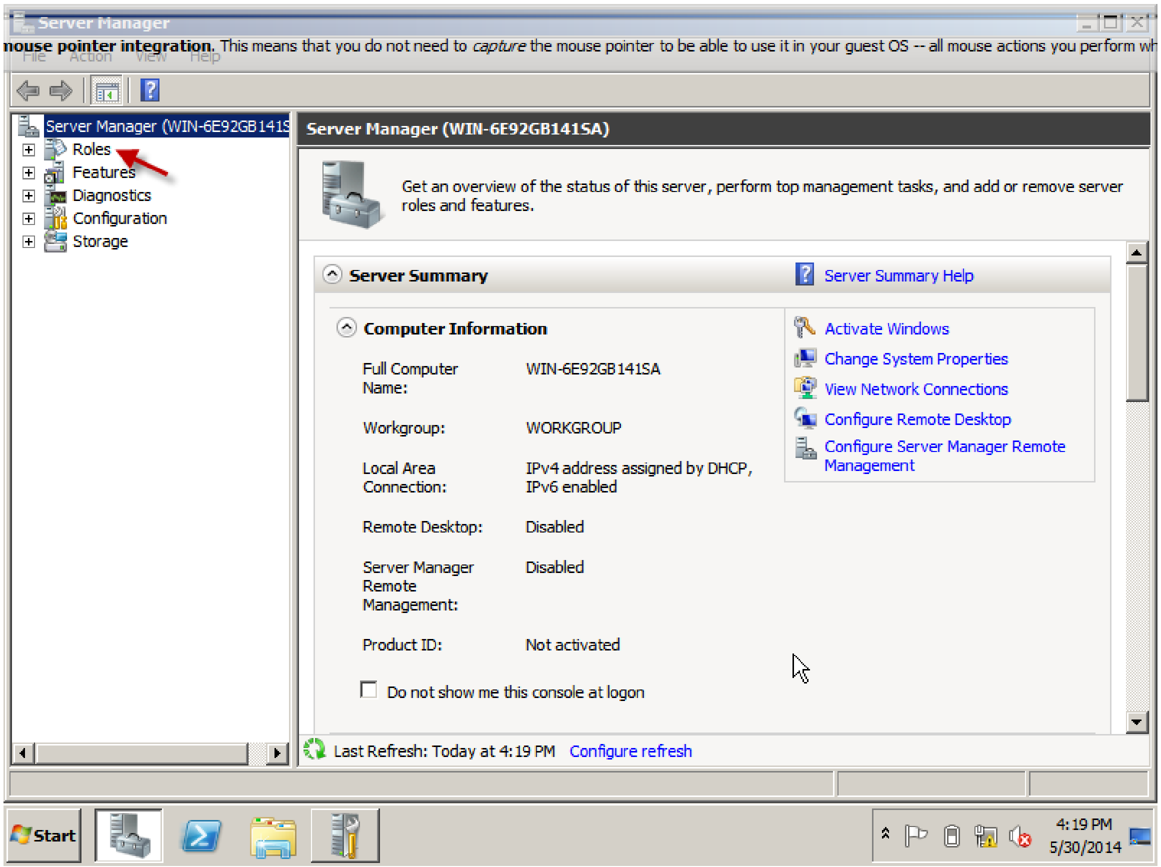


mouse pointer integration. This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform wh

The **Server Manager** window appears.

2. On the left panel, click **Roles**. The **Roles** window appears in the right panel.

> ***Important:*** If Active Directory Certificate Services is already installed, you can skip steps until Step no. 23



nouse pointer integration. This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform wh

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Full Computer Name: WIN-6E92GB141SA

Workgroup: WORKGROUP

Local Area Connection: IPv4 address assigned by DHCP, IPv6 enabled

Remote Desktop: Disabled

Server Manager Remote Management: Disabled

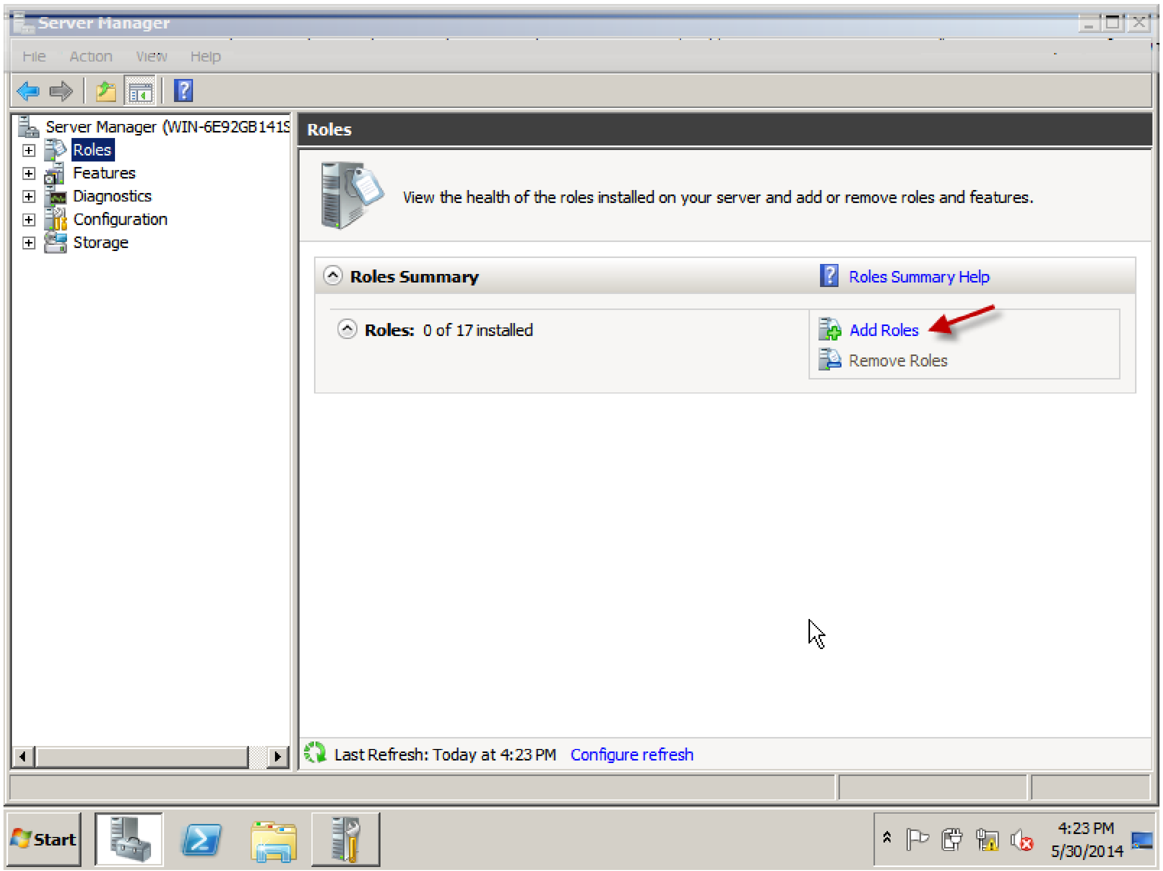
Product ID: Not activated

☐ Do not show me this console at logon

Last Refresh: Today at 4:19 PM

3. Click the **Server Summary** label.

   The **Roles Summary** menu appears.

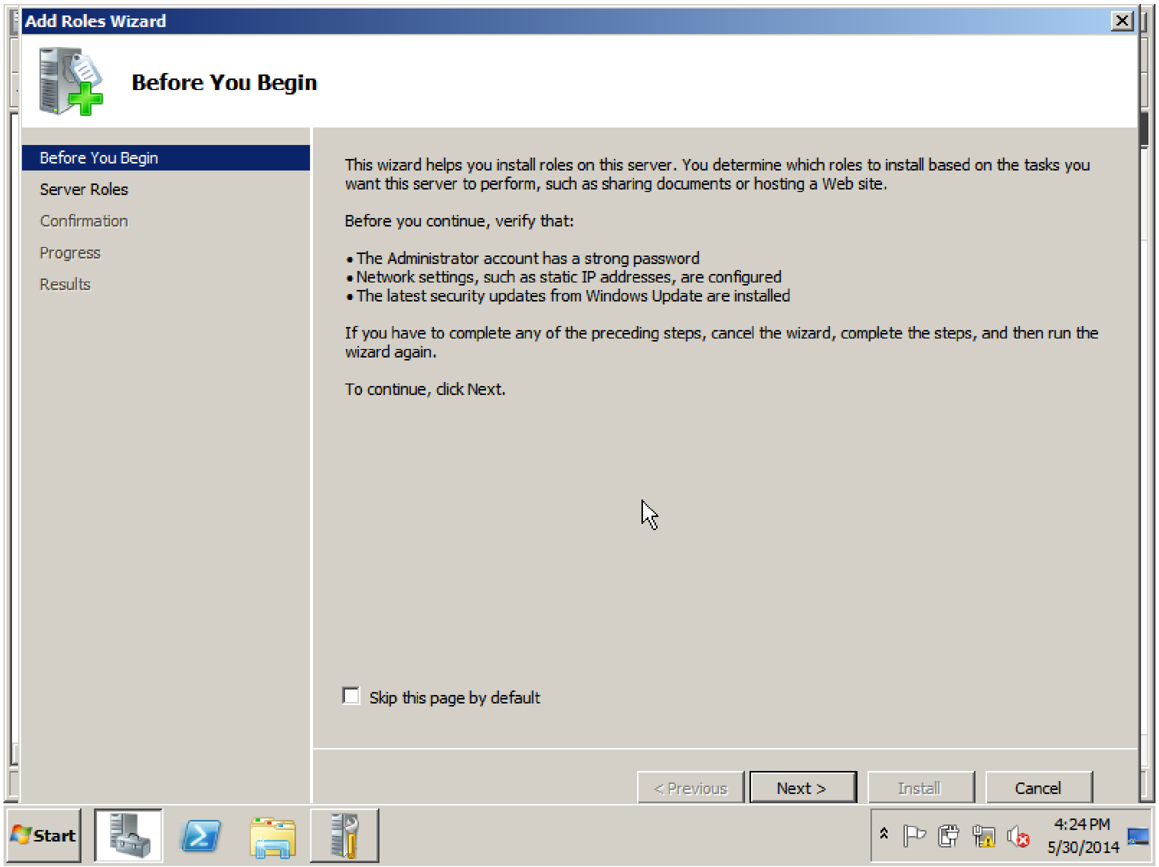


View the health of the roles installed on your server and add or remove roles and features.

Roles: 0 of 17 installed

Last Refresh: Today at 4:23 PM

4. Under Role Summary, click **Add Roles**. The **Add Roles** Wizard appears.



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

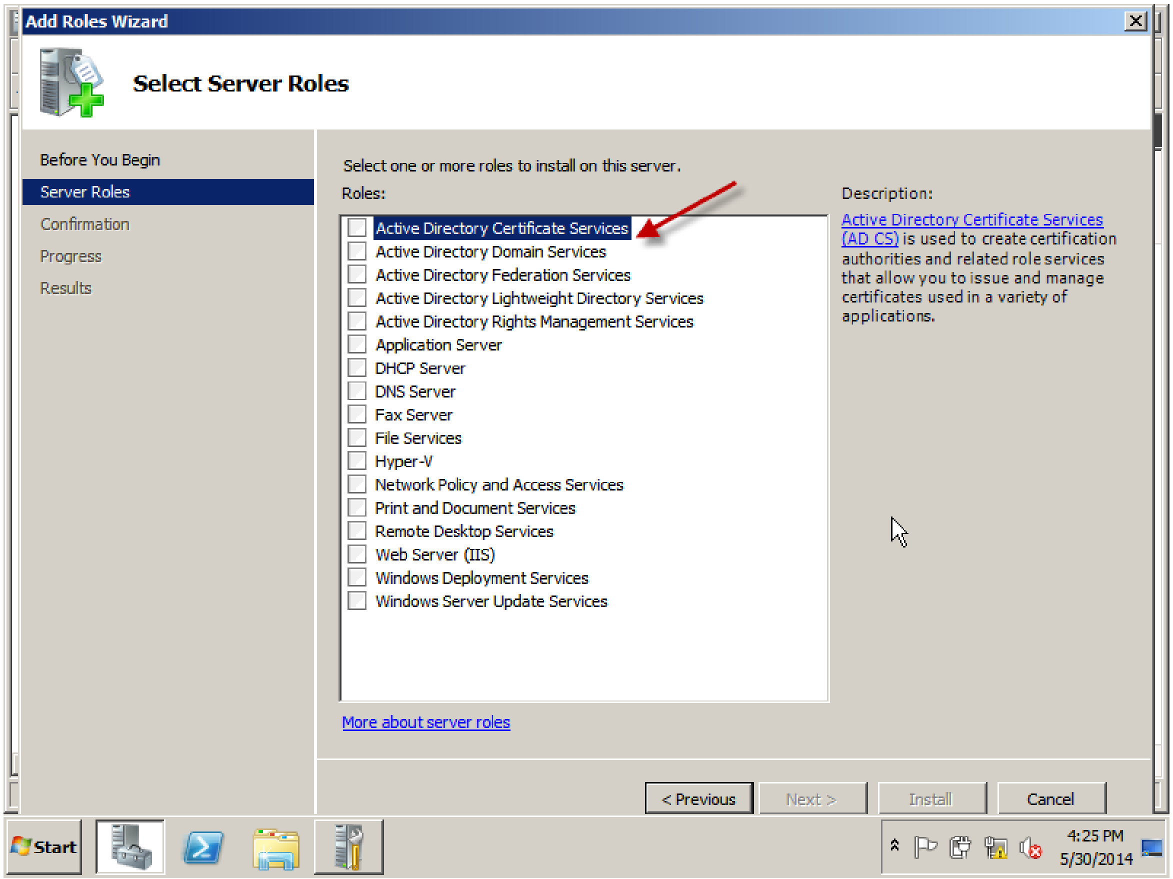
To continue, click Next.

☐ Skip this page by default

5. Click **Next** to continue.

   The **Select Sever Roles** window appears.

6. Select the **Active Directory Certificate Services** checkbox, and click **Next**.



Select one or more roles to install on this server.

Roles:

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

More about server roles

Description:

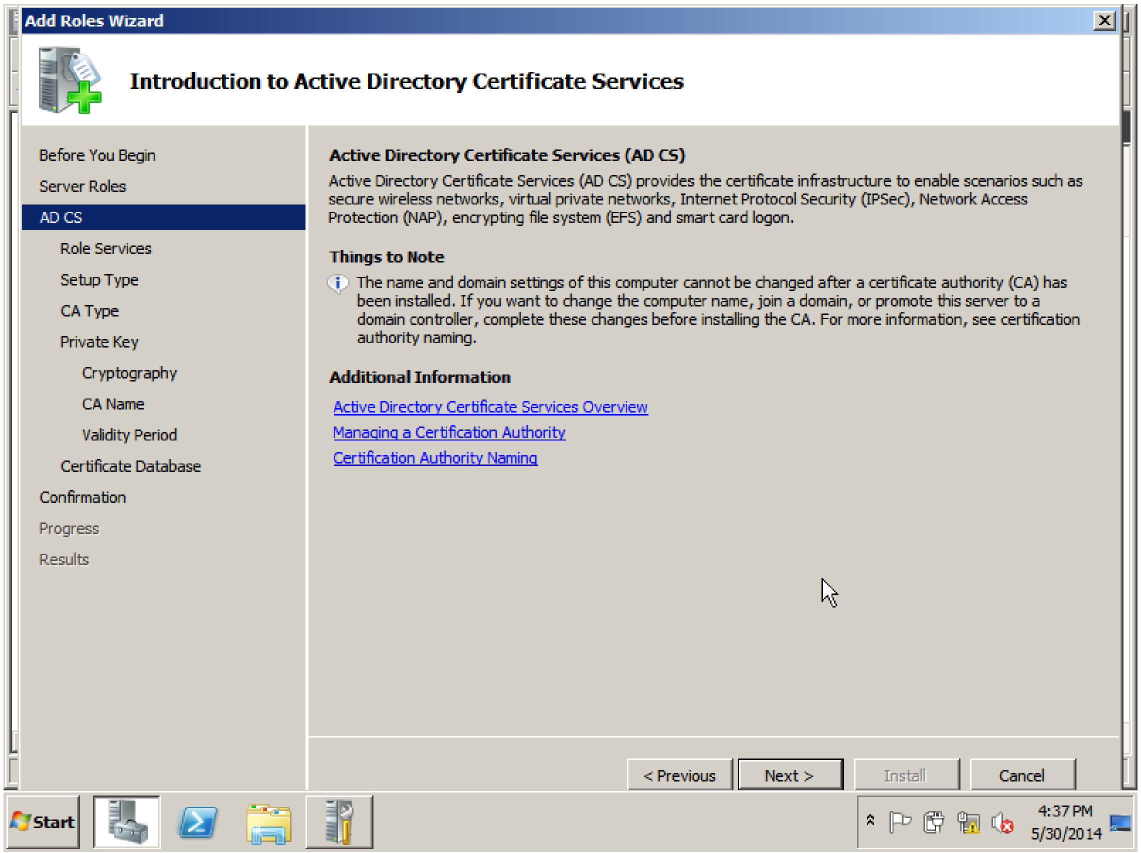
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Following links are available on the **Select Server Roles** window:

- **More about server roles**: Click this link to open the Adding Server Roles and Features window that informs about how to manage and secure multiple server roles in an enterprise with the Server Manager console.
- **Active Directory Certificate Services (AD CS)**: Click this link to open Active Directory Services Overview window that informs about how to deploy AD CS.

The **Introduction to Active Directory Certificate Services** window appears.

7. Select the **Active Directory Certificate Services** checkbox, and click **Next**.



Active Directory Certificate Services (AD CS)

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card logon.

Things to Note

The name and domain settings of this computer cannot be changed after a certificate authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

Additional Information

Active Directory Certificate Services Overview
Managing a Certification Authority
Certification Authority Naming

Following links are available on the **Introduction to Active Directory Services** window:

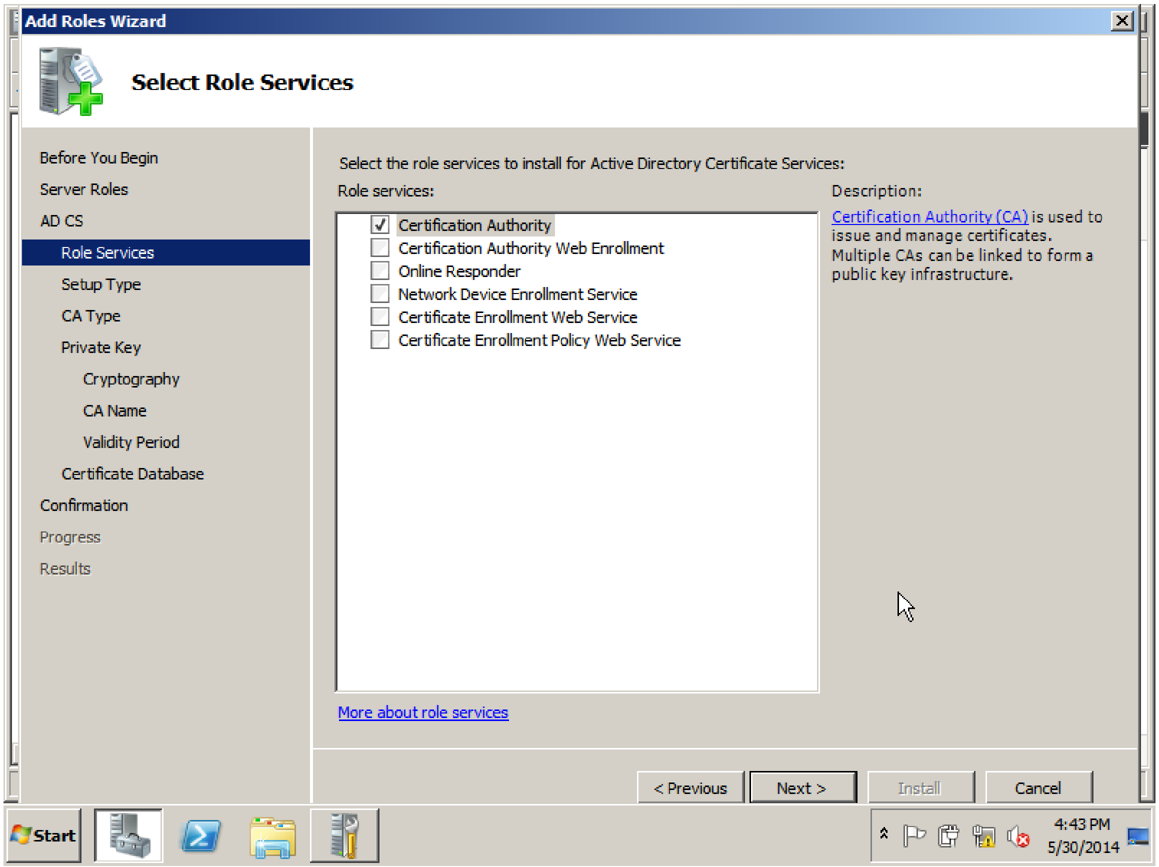
- **Active Directory Certificate Services Overview**: Click this link to open Active Directory Certificate Services Overview help window that informs about how to set up Active Directory Certificate Services.
- **Managing a Certificate Authority**: Click this link to open Managing a Certificate Authority help window that informs about two broad categories of tasks: infrequent management tasks and the recurring management tasks.
- **Certificate Authority Naming**: Click this link to open Certification Authority Naming help window that informs about how to establish a CA naming convention before you configure certification authority (CAs)

8. Click **Next**.

   The **Select Roles Services window** appears

9. Click **Certificate Authority** checkbox if it is not selected.

10. Click **Next**.



Add Roles Wizard

Select Role Services

Select the role services to install for Active Directory Certificate Services:

Role services:

☑ Certification Authority
□ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

Description:

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

More about role services

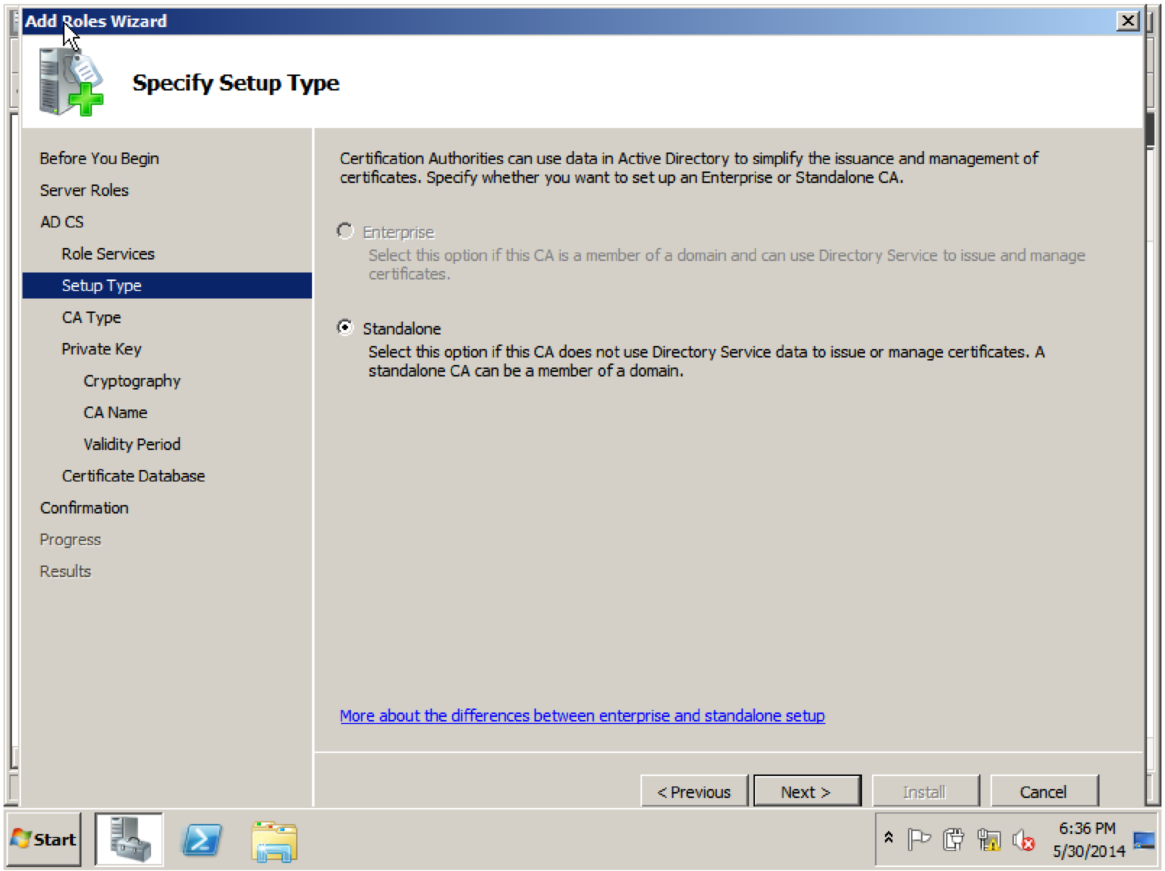
11. Following links are available on the **Select Role Services** window:

   - **Certification Authority (CA)**: Click this link to open the Types of Certification Authorities window that informs about the types of certification authorities.

- **More about role services**: Click this link to open the Roles, Role Services, and Features window that informs about what roles, role services and features are, and how they are integrated in your enterprise.

The **Specify Setup Type** window appears.

12. By default the **Standalone** option is selected. Click **Next** to continue.



Add Roles Wizard

Specify Setup Type

Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

○ Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

● Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

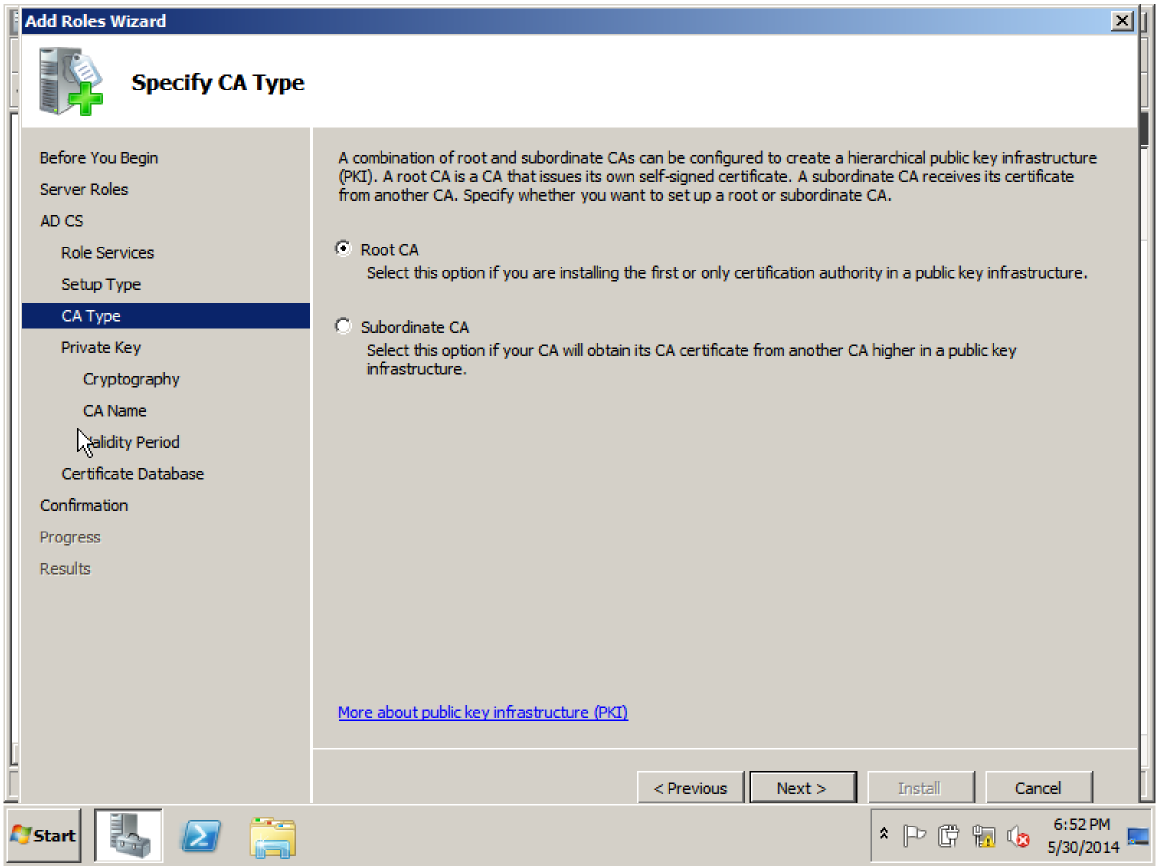
More about the differences between enterprise and standalone setup

Following links are available on the **Specify Setup Type** window:

- **More about the difference between enterprise and standalone setup**: Click this link to open the **Types of Certification Authorities** window that informs about the types of the certification authorities.

  The **Specify CA Type** window appears.

13. By default the **Root CA** option is selected. Click **Next** to continue.



Add Roles Wizard

Specify CA Type

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

● Root CA
Select this option if you are installing the first or only certification authority in a public key infrastructure.

○ Subordinate CA
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

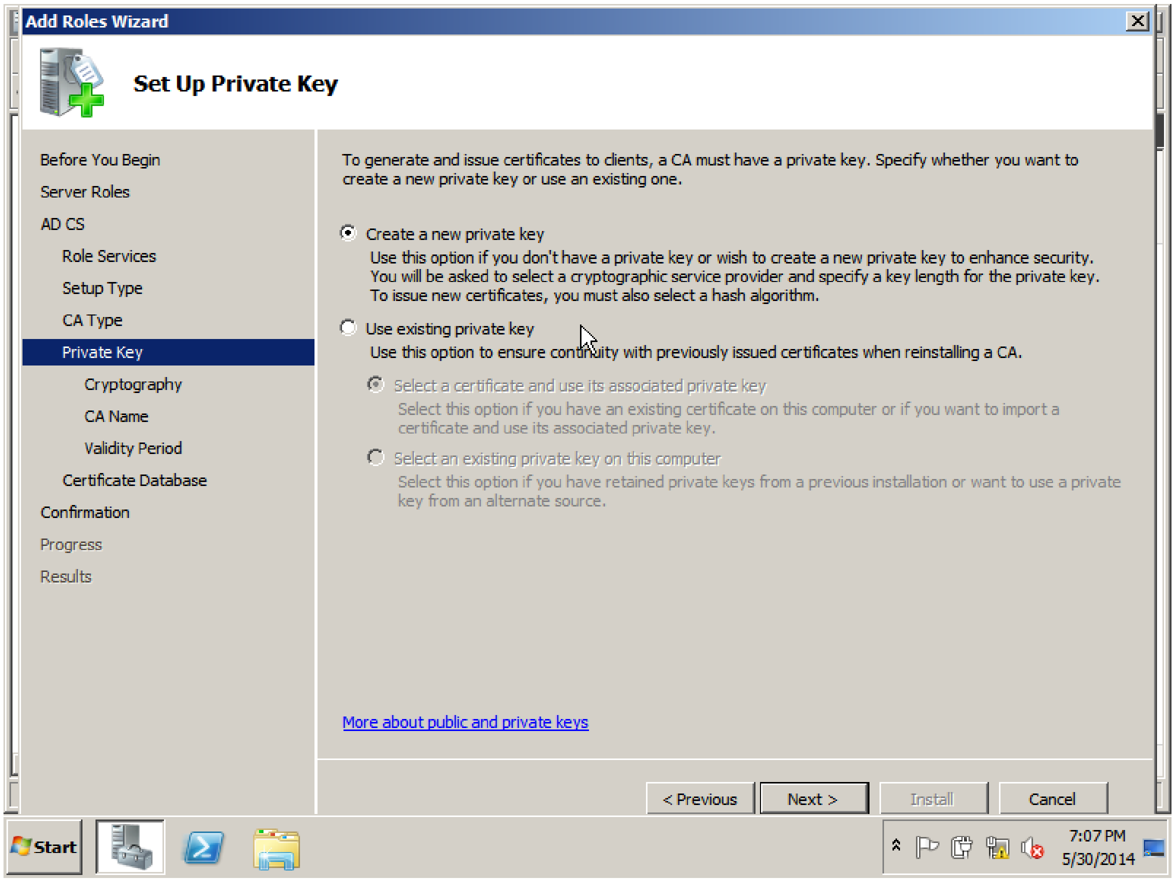
More about public key infrastructure (PKI)

Following links are available on the **Specify CA Type** window:

- **More about public key infrastructure (PKT)**: Click this link to open the Public Key Infrastructure window that informs about the use of digital certificates, certificate authorities and registration authorities that verify and authenticate the validity of each entity that is involved in an electronic transaction that involves the use of public key cryptography.

The **Setup Private Key** window appears.

14. By default the **Create a new private key** option is selected. Click **Next** to continue.



Set Up Private Key

To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

● Create a new private key

Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

○ Use existing private key

Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

● Select a certificate and use its associated private key

Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about public and private keys

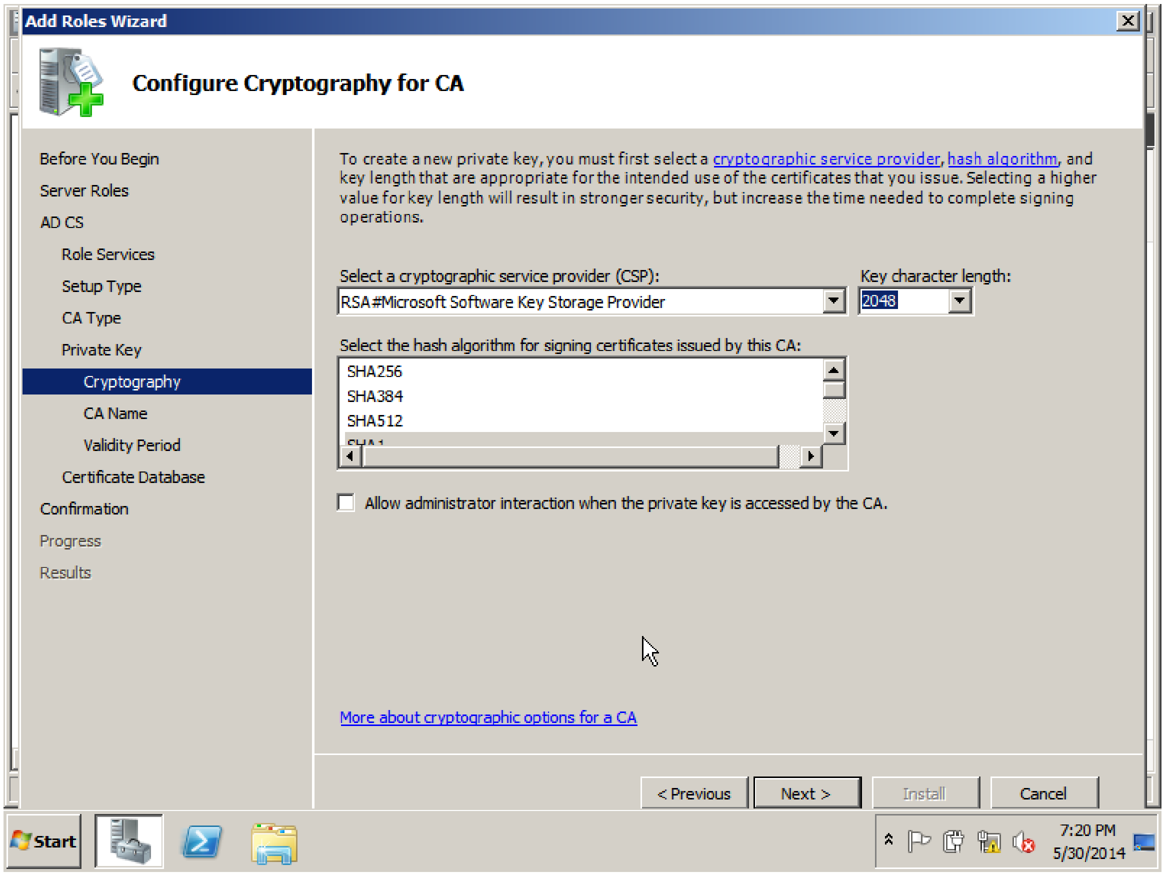
Following links are available on the **Setup Private Key** window:

- **More about public and private key**: Click this link to open the **Public and Private Keys** window that informs about how to encrypt and decrypt the information.

The **Configure Cryptography for CA** window appears.

15. Ensure Key character length value is **2048** This is used to define -DSCEP_KEY_SIZE while configuring SCEP settings in EMM Server. refer section 5.1.4

16. Click **Next** to continue.



Add Roles Wizard

Configure Cryptography for CA

To create a new private key, you must first select a cryptographic service provider, hash algorithm, and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

Select a cryptographic service provider (CSP): RSA#Microsoft Software Key Storage Provider

Key character length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1

□ Allow administrator interaction when the private key is accessed by the CA.

More about cryptographic options for a CA

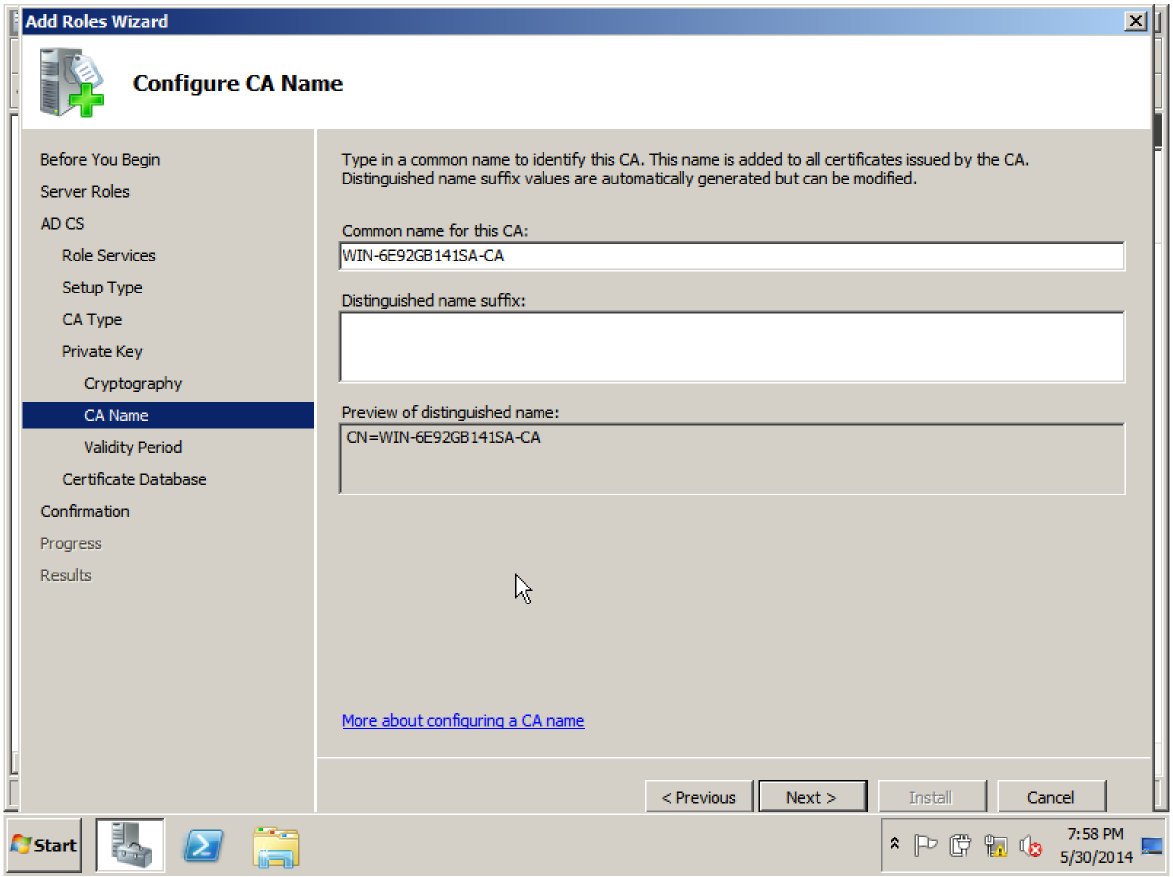
Following links are available on the **Configure Cryptography for CA** window:

- **Cryptographic service provider**, hash algorithm: Click this link to open the Cryptographic Service Providers help window that informs about cryptographic service providers.
- **More about cryptographic options for CA**: Click this link to open the Cryptographic Options for CAs window that informs about how to implement the cryptographic options.

The **Configure CA Name** window appears.

17. Copy text from the Common name for this CA field. This is used to define -DSCEP_COMMON_NAME, -DSCEP_CA_DOMAIN and -DSCEP_CA_INSTANCE_NAME, while configuring SCEP settings in EMM server. For more details, refer section 5.1.4

18. Click **Next** to continue.



Add Roles Wizard

Configure CA Name

Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:
WIN-6E92GB141SA-CA

Distinguished name suffix:

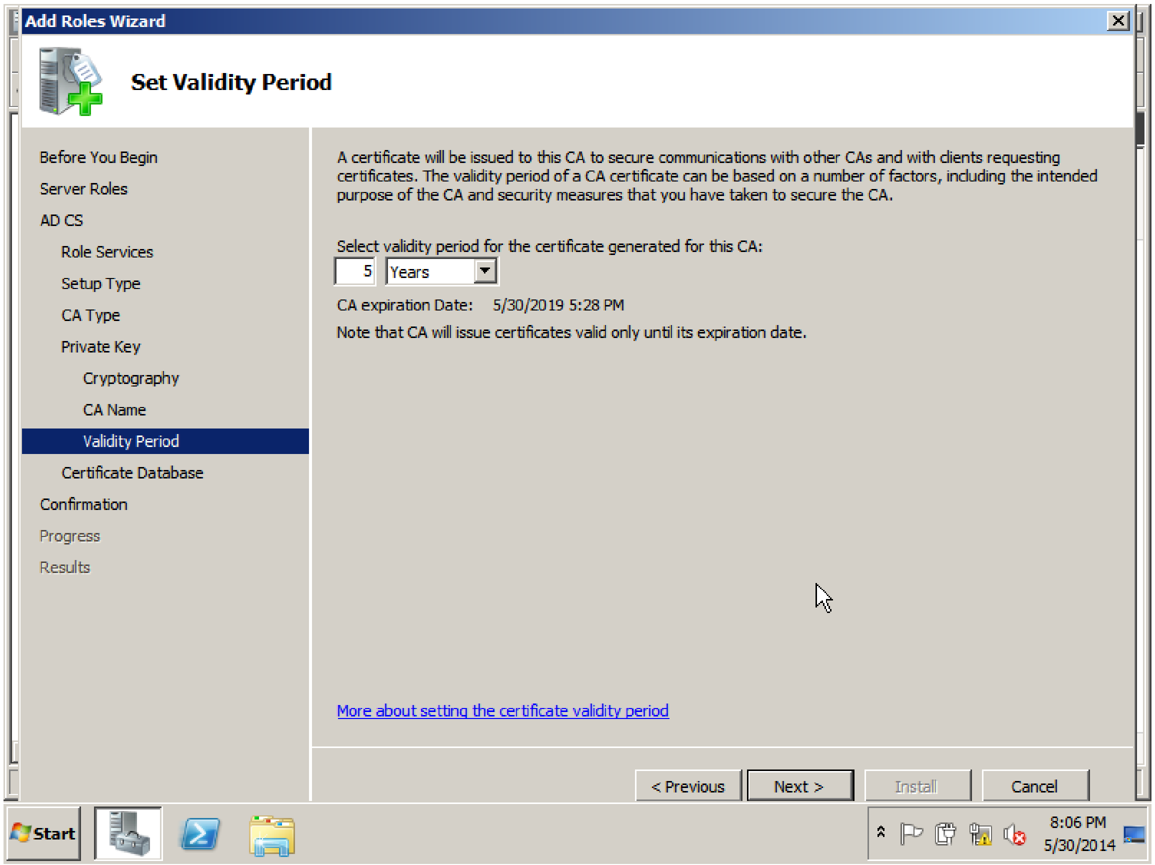
Preview of distinguished name:
CN=WIN-6E92GB141SA-CA

Following links are available on the **Configure CA Name** window:

- **More about configuring a CA Name**: Click this link to open the Certification Authority Naming help window that informs about how to create a name.

  The **Set Validity Period** window appears.

19. Click **Next** to continue.



A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.

Select validity period for the certificate generated for this CA:

5 Years

CA expiration Date: 5/30/2019 5:28 PM

Note that CA will issue certificates valid only until its expiration date.

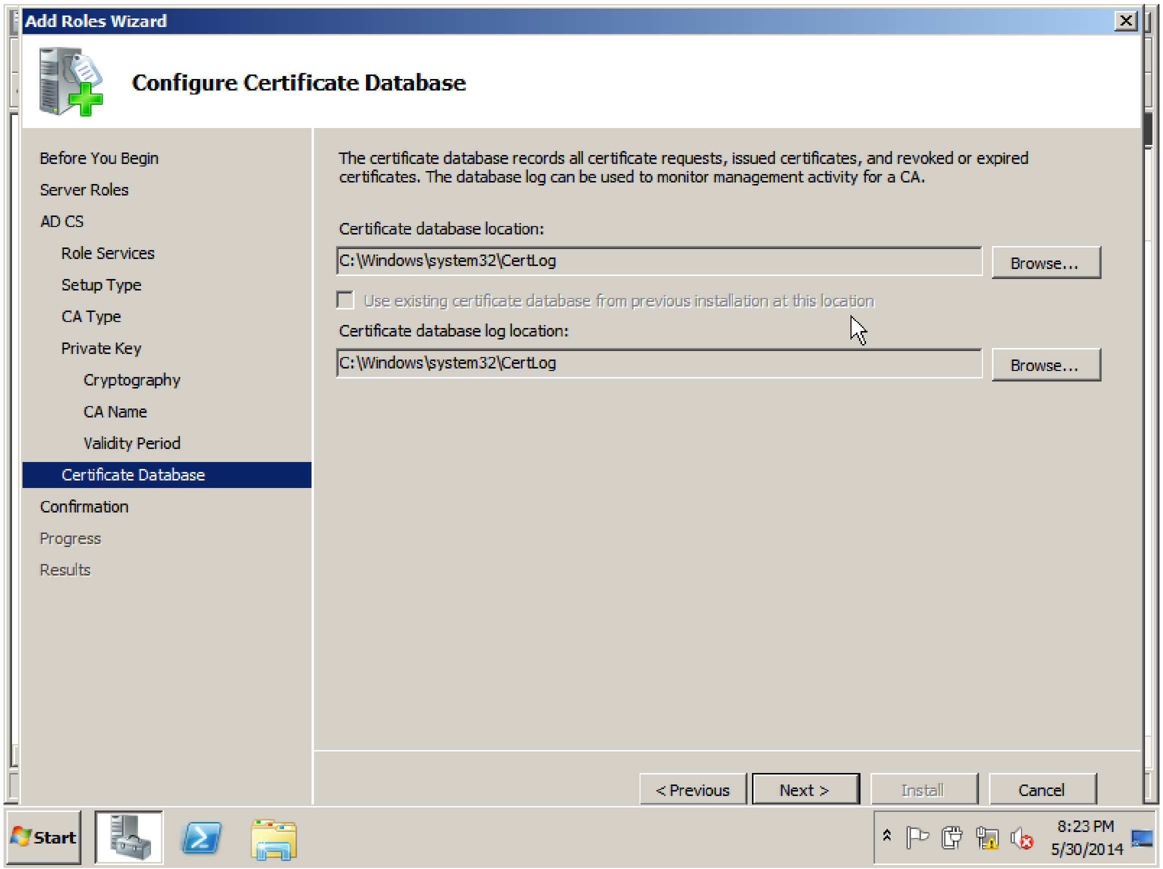
More about setting the certificate validity period

Following links are available on the **Setup Validity Period** window:

- **More about setting the certificate validity period**: Click this link to open the **Certificate Validity Periods** help window that informs about how to renew a certificate issued from a Windows based enterprise certification authority (CA).

The **Configure Certificate Database** window appears.

20. Click **Next** to continue.



Add Roles Wizard

Configure Certificate Database

The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.

Certificate database location:

C:\Windows\system32\CertLog

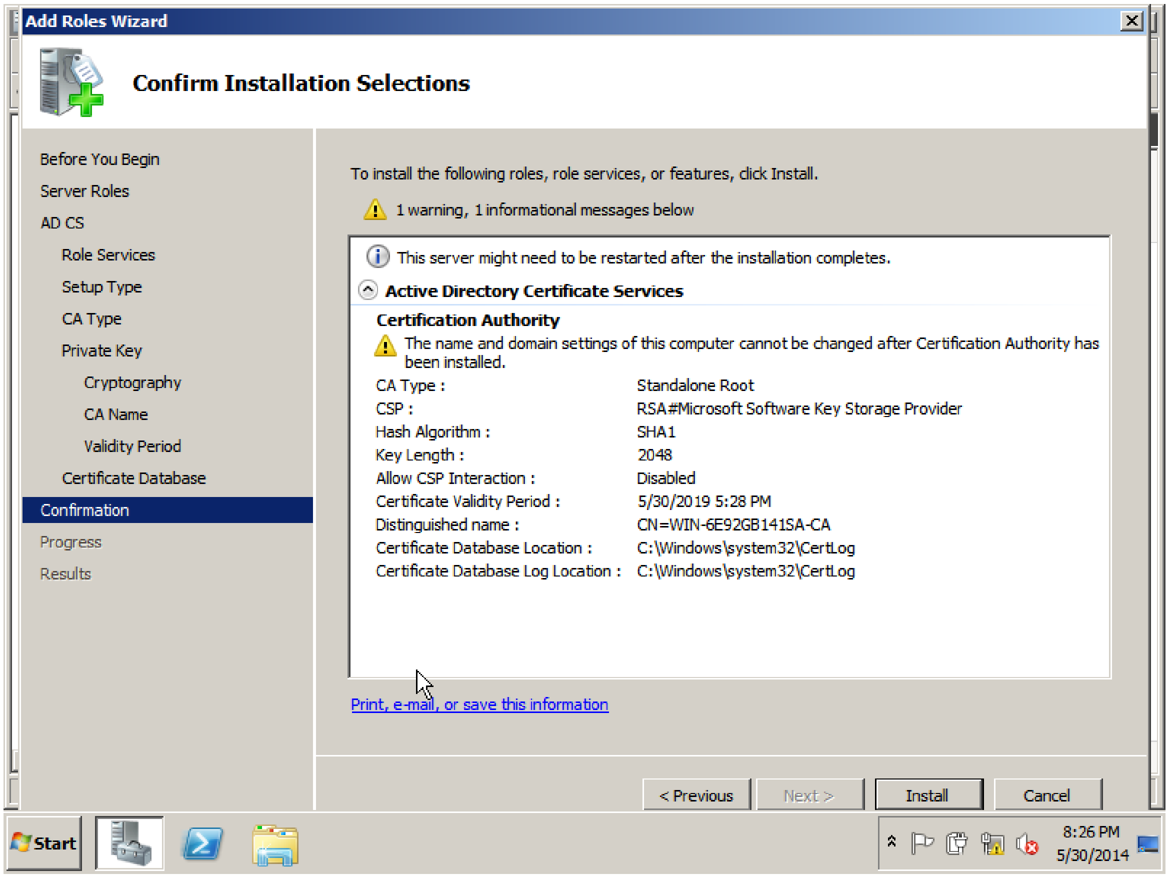
□ Use existing certificate database from previous installation at this location

Certificate database log location:

C:\Windows\system32\CertLog

The **Confirm Installation Selections** window appears.

21. Click **Install**.



To install the following roles, role services, or features, click Install.

⚠ 1 warning, 1 informational messages below

ⓘ This server might need to be restarted after the installation completes.

Active Directory Certificate Services

Certification Authority

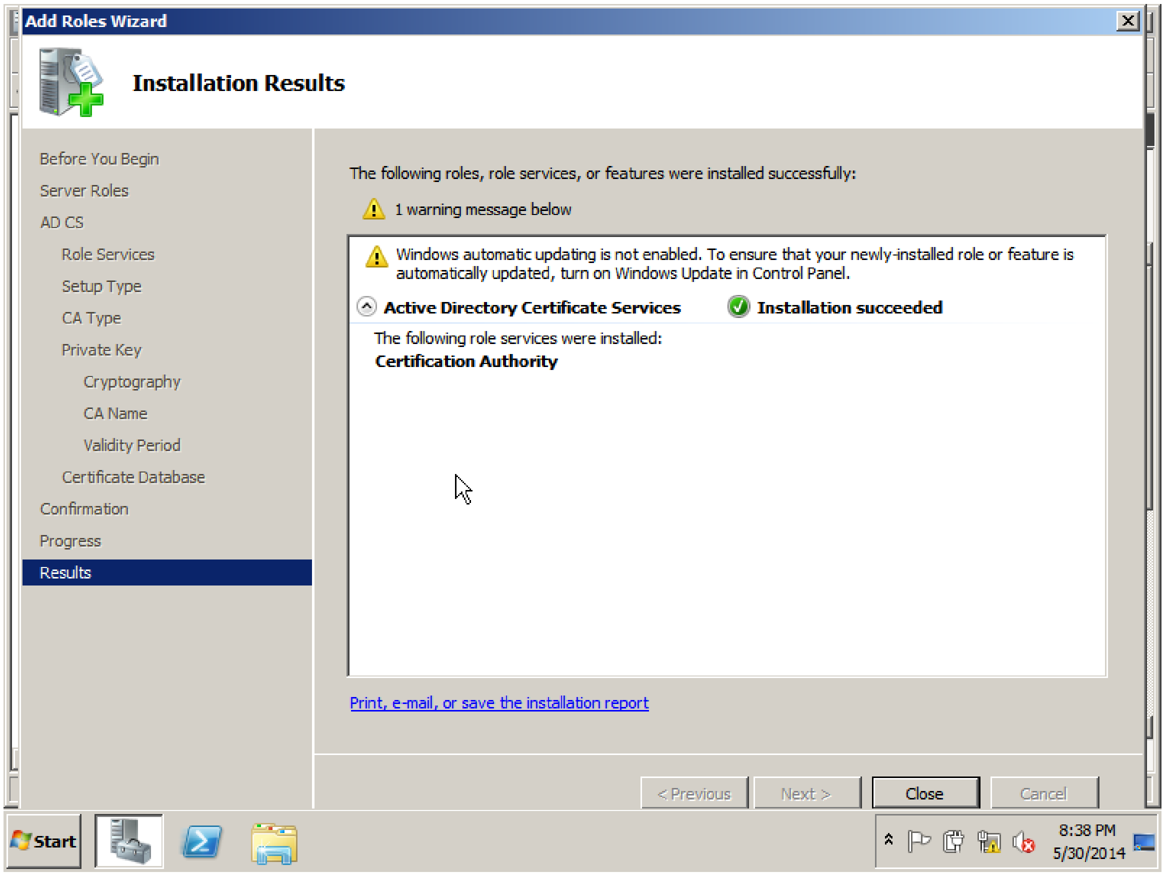
⚠ The name and domain settings of this computer cannot be changed after Certification Authority has been installed.

CA Type :	Standalone Root
CSP :	RSA#Microsoft Software Key Storage Provider
Hash Algorithm :	SHA1
Key Length :	2048
Allow CSP Interaction :	Disabled
Certificate Validity Period :	5/30/2019 5:28 PM
Distinguished name :	CN=WIN-6E92GB141SA-CA
Certificate Database Location :	C:\Windows\system32\CertLog
Certificate Database Log Location :	C:\Windows\system32\CertLog

Following links are available on the **Confirm Installation Selections** window:

- **Print, e-mail, or save the information**: Click this link to open the C:\\Windows\Logs\ServerManagerInstallationLog.html

The **Installation Results** window appears with the confirmation message, stating that following roles, role services, or features are installed successfully.



The following roles, role services, or features were installed successfully:

⚠ 1 warning message below

⚠ Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel.

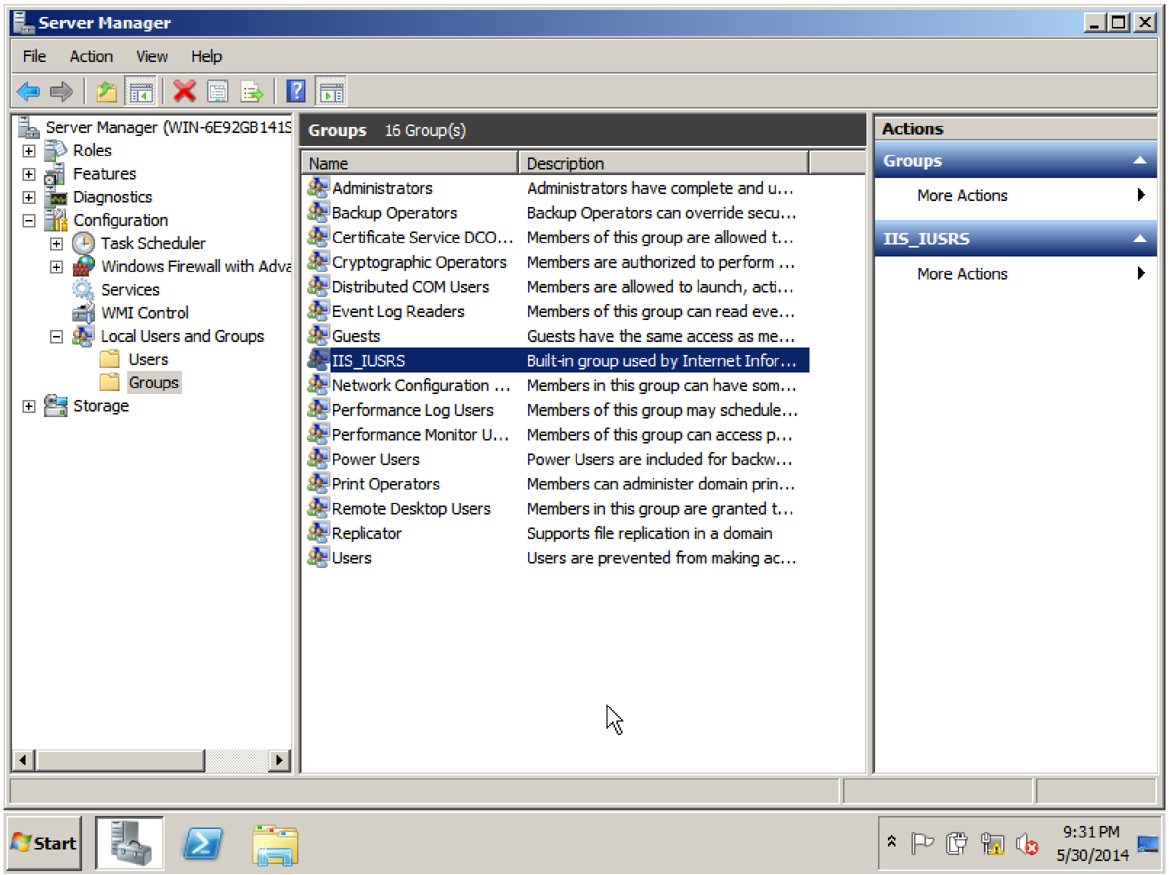
Active Directory Certificate Services ✓ **Installation succeeded**

The following role services were installed:
Certification Authority

22. Click **Close**.

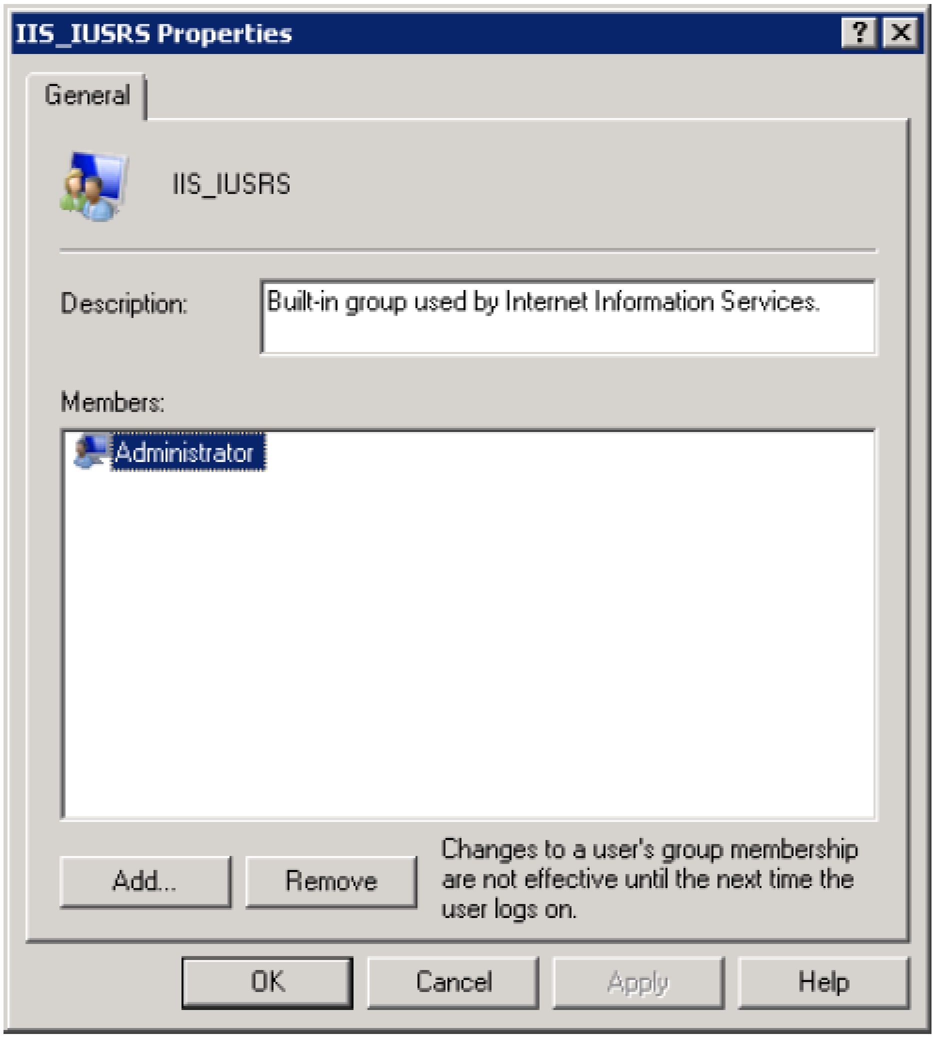
23. Click **Server Manager** > **Configuration** > **Groups**.

24. The Groups section appears in the right panel. Add the administrator user to IIS_IUSRS group.



Name	Description
Administrators	Administrators have complete and u…
Backup Operators	Backup Operators can override secu…
Certificate Service DCO…	Members of this group are allowed t…
Cryptographic Operators	Members are authorized to perform …
Distributed COM Users	Members are allowed to launch, acti…
Event Log Readers	Members of this group can read eve…
Guests	Guests have the same access as me…
IIS_IUSRS	Built-in group used by Internet Infor…
Network Configuration …	Members in this group can have som…
Performance Log Users	Members of this group may schedule…
Performance Monitor U…	Members of this group can access p…
Power Users	Power Users are included for backw…
Print Operators	Members can administer domain prin…
Remote Desktop Users	Members in this group are granted t…
Replicator	Supports file replication in a domain
Users	Users are prevented from making ac…

25. The following image shows that the administrator is added to IIS_IUSRS group.



Description: Built-in group used by Internet Information Services.

Members:

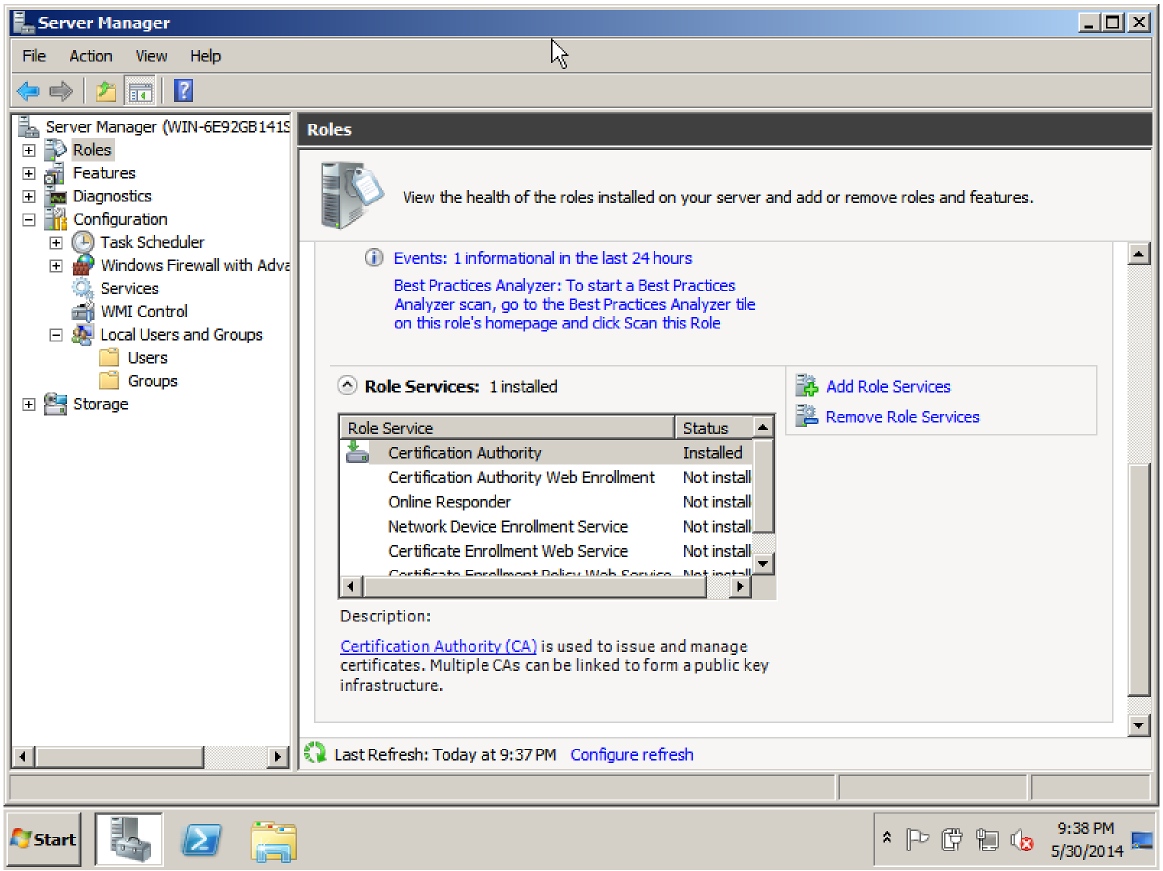
Administrator

Changes to a user's group membership are not effective until the next time the user logs on.

26. On the left panel, click **Roles**.

    The **Roles** window appears in the right panel.

27. Click the **Add Role Services** button.



View the health of the roles installed on your server and add or remove roles and features.

Events: 1 informational in the last 24 hours

Best Practices Analyzer: To start a Best Practices Analyzer scan, go to the Best Practices Analyzer tile on this role's homepage and click Scan this Role

Role Services: 1 installed

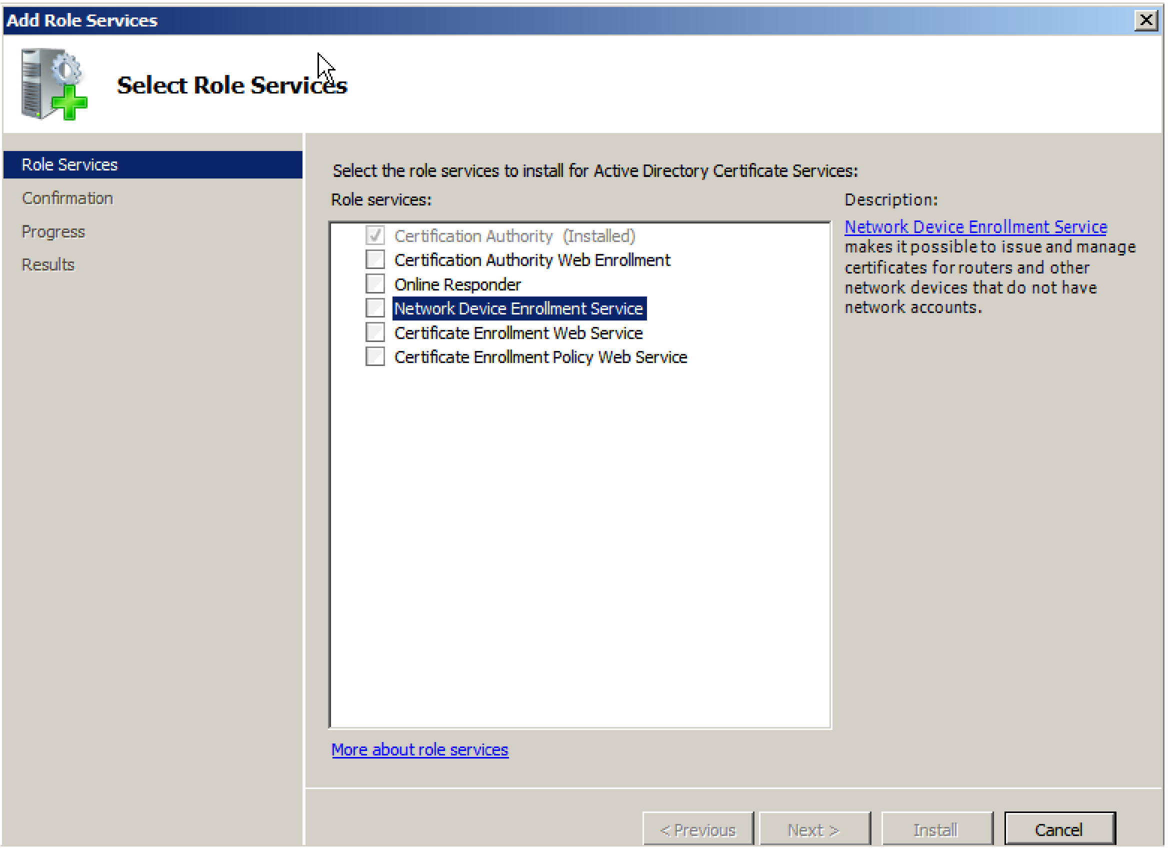
Role Service	Status
Certification Authority	Installed
Certification Authority Web Enrollment	Not install
Online Responder	Not install
Network Device Enrollment Service	Not install
Certificate Enrollment Web Service	Not install
Certificate Enrollment Policy Web Service	Not install

Description:

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

Last Refresh: Today at 9:37 PM

28. Select **Network Device Enrollment Service** checkbox. Click **Next**.



Select the role services to install for Active Directory Certificate Services:

Role services:

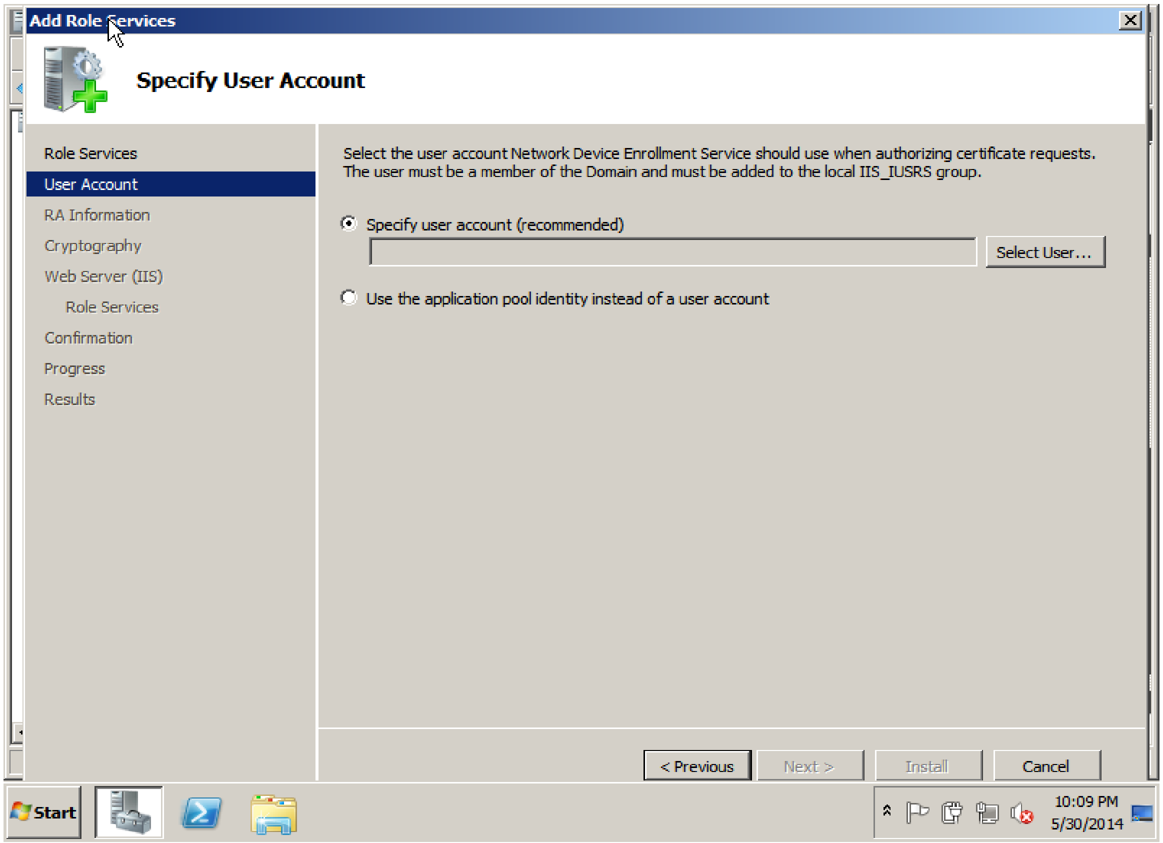
- ☑ Certification Authority (Installed)
- □ Certification Authority Web Enrollment
- □ Online Responder
- □ Network Device Enrollment Service
- □ Certificate Enrollment Web Service
- □ Certificate Enrollment Policy Web Service

Description:

Network Device Enrollment Service makes it possible to issue and manage certificates for routers and other network devices that do not have network accounts.

29. Select the **Specify user account (recommended)** option and select user account as **Administrator**. Provide the User Name and Password . This User Name -DSCEP_CA_ USERNAMEand the Password -DSCEP_CA_PASSWORD is used to configure SCEP details in EMM Server.For more details, refer section 5.1.4

30. Click **Next** to continue. The **RA Information** tab becomes active.



Add Role Services

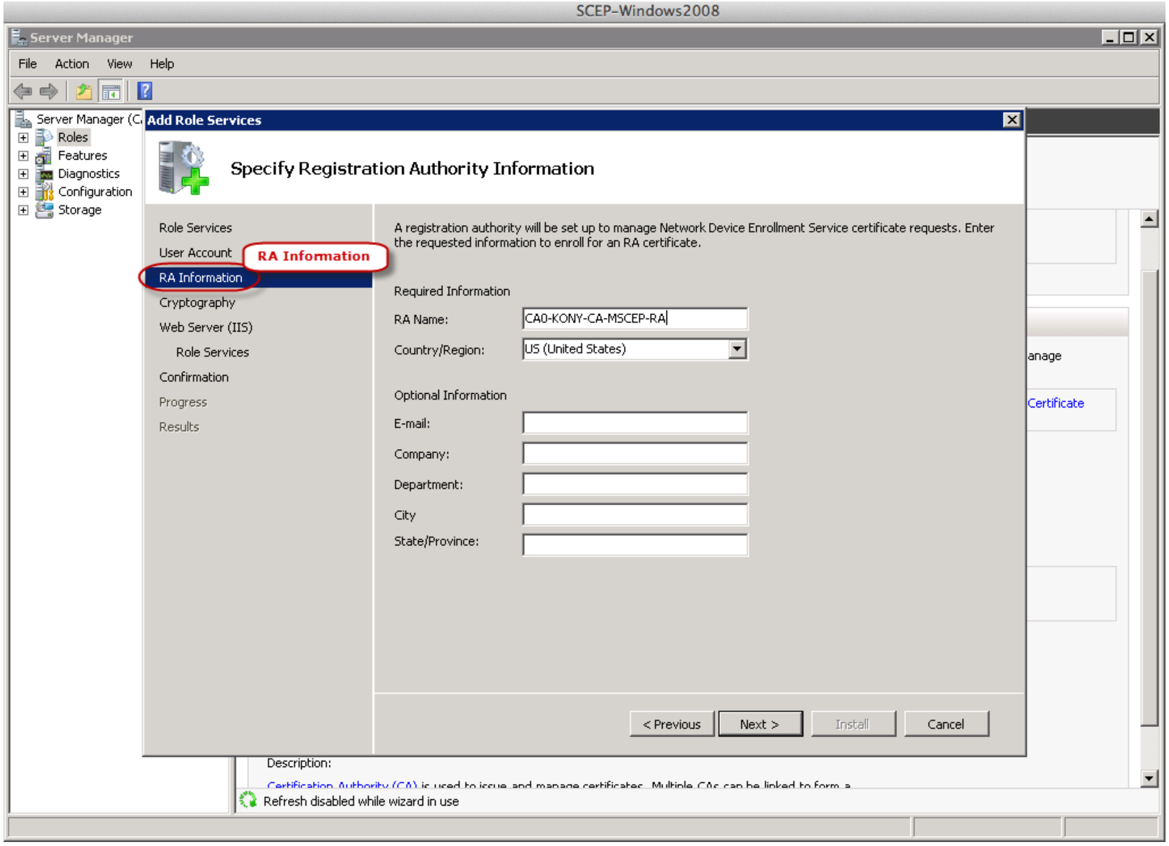
Specify User Account

Select the user account Network Device Enrollment Service should use when authorizing certificate requests. The user must be a member of the Domain and must be added to the local IIS_IUSRS group.

● Specify user account (recommended)

○ Use the application pool identity instead of a user account

31. Accept the default values for the **RA Name** and **Country/Region** fields. Click **Next** to continue.The **Cryptography** tab becomes active.



Specify Registration Authority Information

A registration authority will be set up to manage Network Device Enrollment Service certificate requests. Enter the requested information to enroll for an RA certificate.

Required Information

RA Name: CA0-KONY-CA-MSCEP-RA

Country/Region: US (United States)

Optional Information

E-mail:

Company:

Department:

City

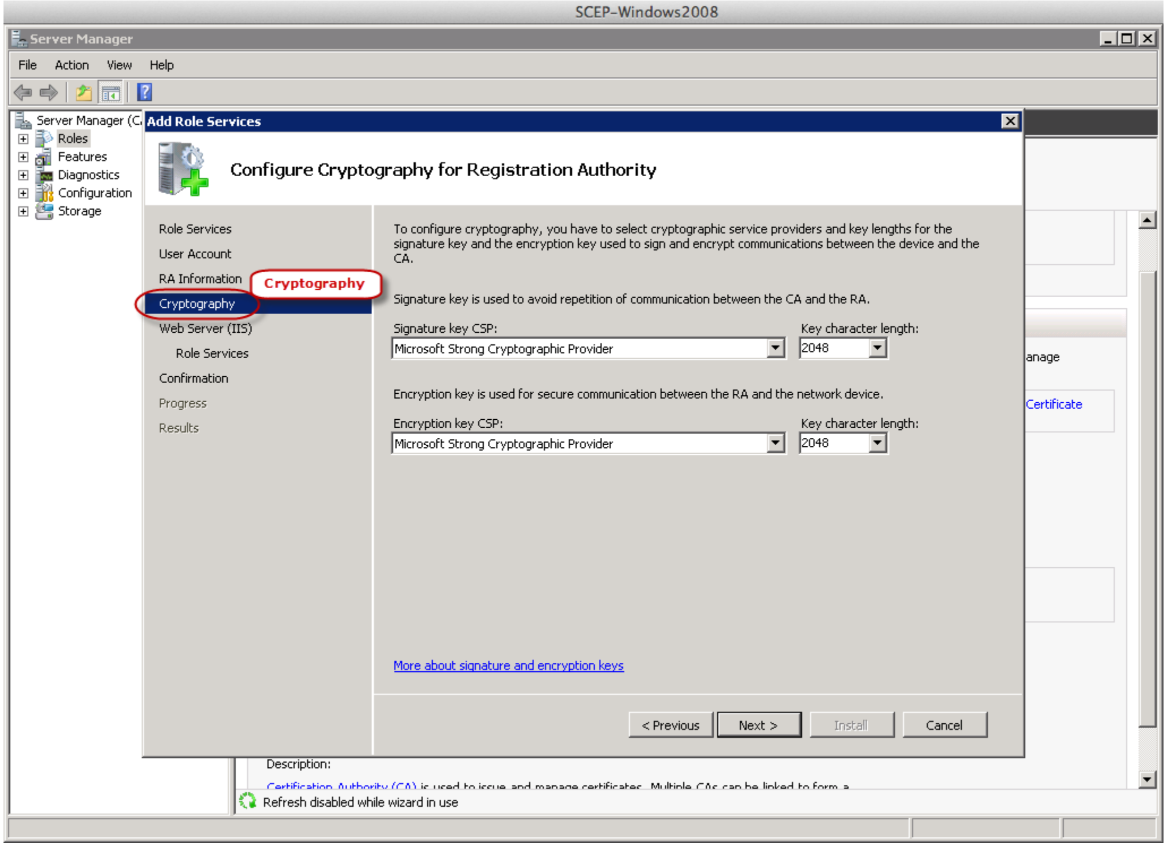
State/Province:

Description:

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a

Refresh disabled while wizard in use

32. Accept the default values for **Signature Key CSP** and **Encryption Key CSP** fields, and then click **Next** to continue. The **Web Server (IIS)** tab becomes active.



Configure Cryptography for Registration Authority

To configure cryptography, you have to select cryptographic service providers and key lengths for the signature key and the encryption key used to sign and encrypt communications between the device and the CA.

Signature key is used to avoid repetition of communication between the CA and the RA.

Signature key CSP: Microsoft Strong Cryptographic Provider

Key character length: 2048

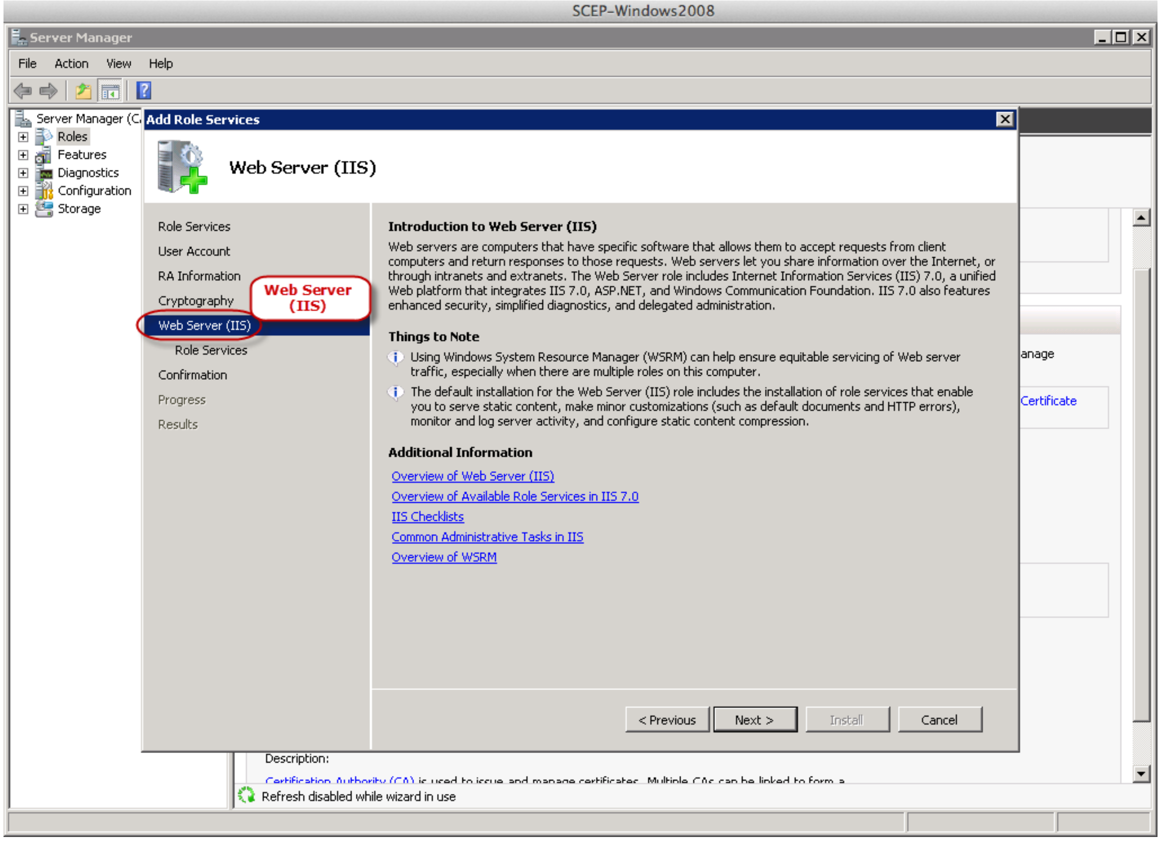
Encryption key is used for secure communication between the RA and the network device.

Encryption key CSP: Microsoft Strong Cryptographic Provider

Key character length: 2048

More about signature and encryption keys
< Previous
Next >
Install
Cancel
anage
Certificate
Description:
Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a
Refresh disabled while wizard in use

33. Click **Next** to continue. The **Role Services** tab becomes active.



Introduction to Web Server (IIS)

Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features enhanced security, simplified diagnostics, and delegated administration.

Things to Note

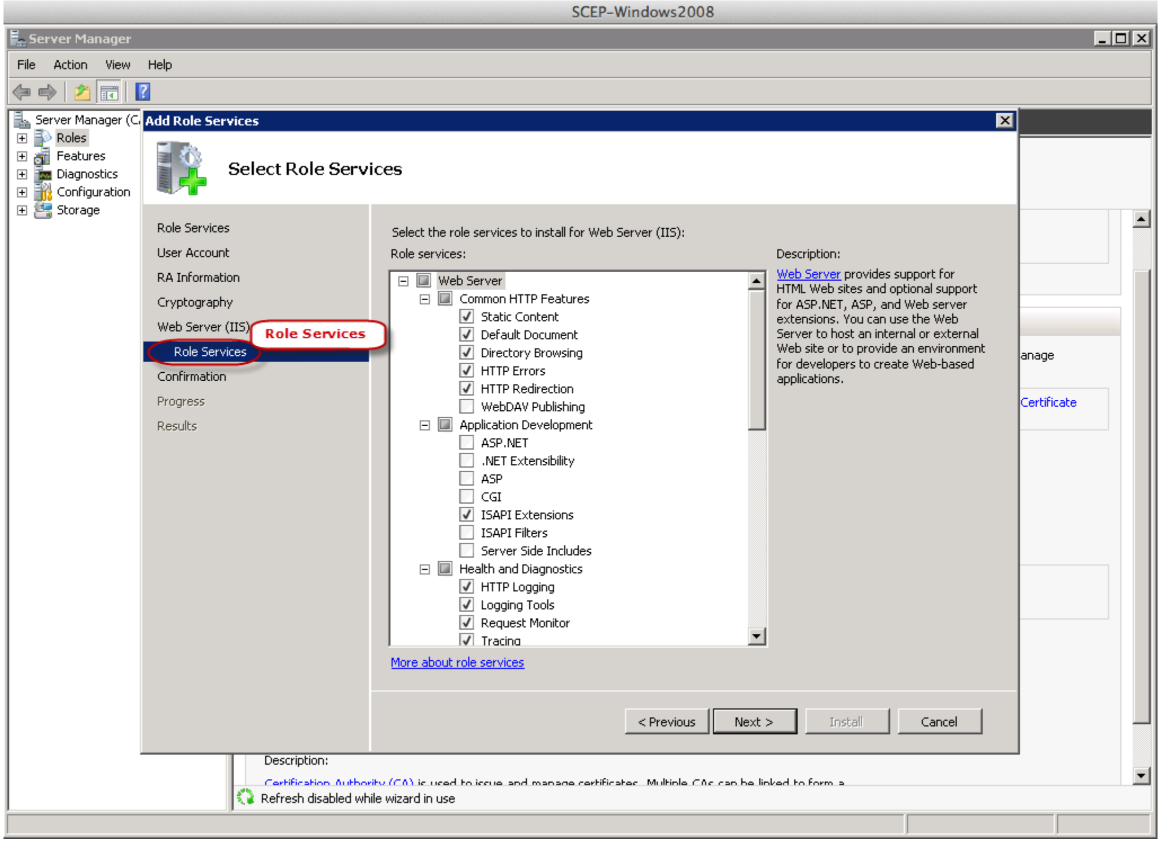
- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

Additional Information

Overview of Web Server (IIS)
Overview of Available Role Services in IIS 7.0
IIS Checklists
Common Administrative Tasks in IIS
Overview of WSRM

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a

34. Accept the default values and then click **Next** to continue. The **Confirmation** tab becomes active.



SCEP-Windows2008

Server Manager

Add Role Services

Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

- ⊟ ▣ Web Server
  - ⊟ ▣ Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ HTTP Redirection
    - ☐ WebDAV Publishing
  - ⊟ ▣ Application Development
    - ☐ ASP.NET
    - ☐ .NET Extensibility
    - ☐ ASP
    - ☐ CGI
    - ☑ ISAPI Extensions
    - ☐ ISAPI Filters
    - ☐ Server Side Includes
  - ⊟ ▣ Health and Diagnostics
    - ☑ HTTP Logging
    - ☑ Logging Tools
    - ☑ Request Monitor
    - ☑ Tracing

Description:

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

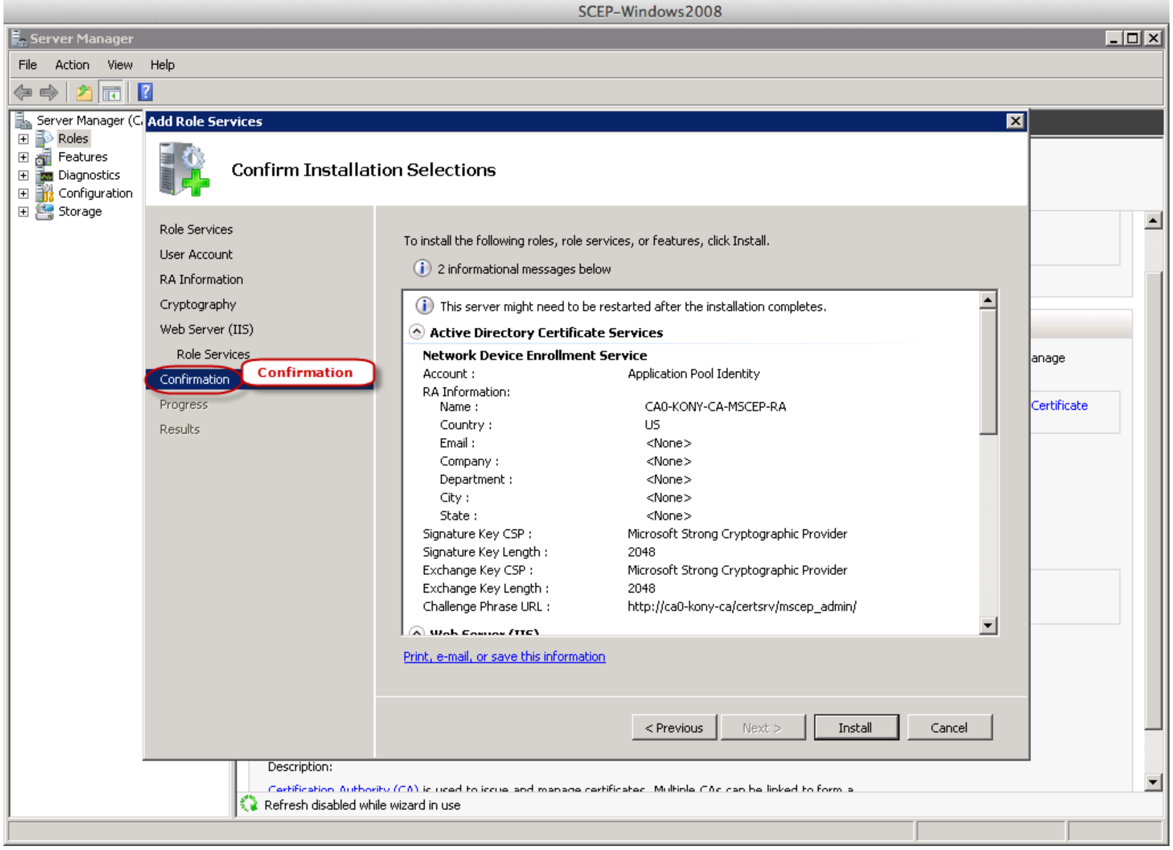
More about role services

Description:

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a

Refresh disabled while wizard in use

35. Accept the default values and then click **Next** to continue.



Confirm Installation Selections

To install the following roles, role services, or features, click Install.

2 informational messages below

This server might need to be restarted after the installation completes.

Active Directory Certificate Services

Network Device Enrollment Service

Account :	Application Pool Identity
RA Information:	
Name :	CA0-KONY-CA-MSCEP-RA
Country :	US
Email :	<None>
Company :	<None>
Department :	<None>
City :	<None>
State :	<None>
Signature Key CSP :	Microsoft Strong Cryptographic Provider
Signature Key Length :	2048
Exchange Key CSP :	Microsoft Strong Cryptographic Provider
Exchange Key Length :	2048
Challenge Phrase URL :	http://ca0-kony-ca/certsrv/mscep_admin/

Web Server (IIS)

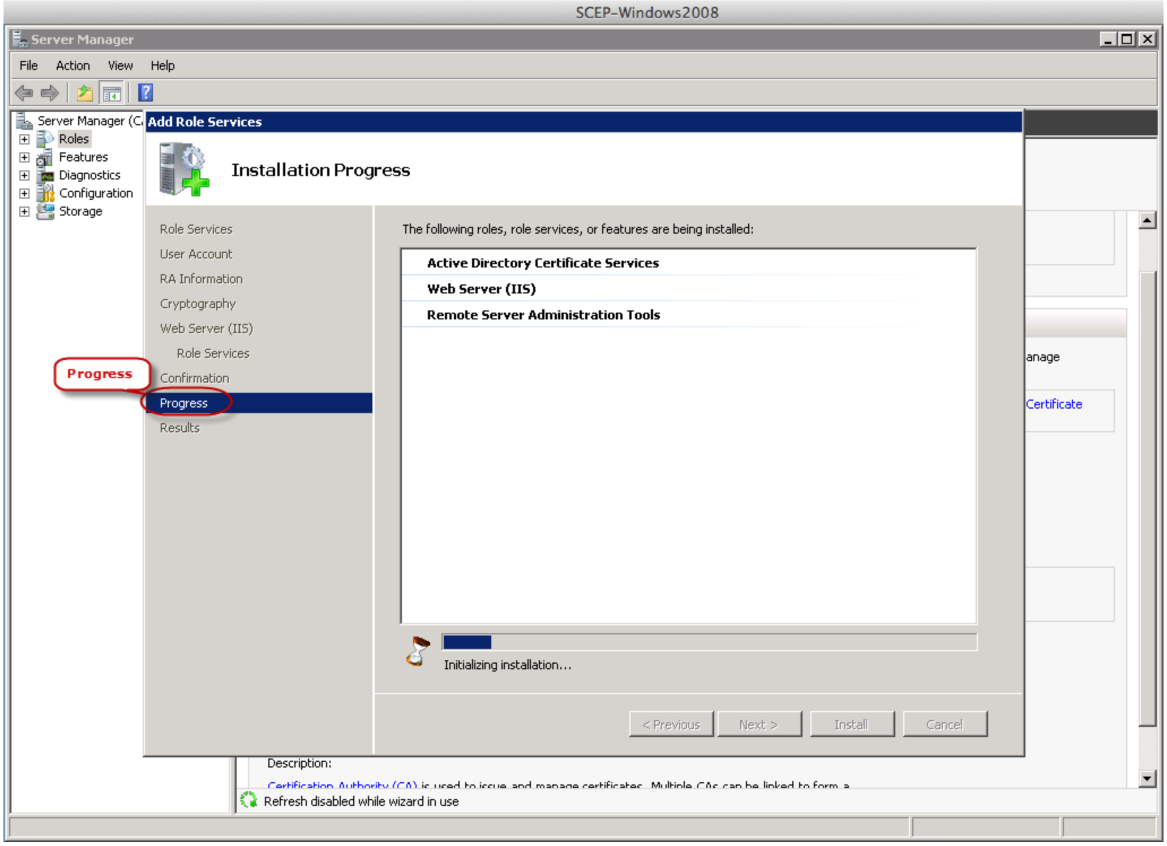
Print, e-mail, or save this information

Description:

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a

Refresh disabled while wizard in use

36. Click the **Install** button to continue.



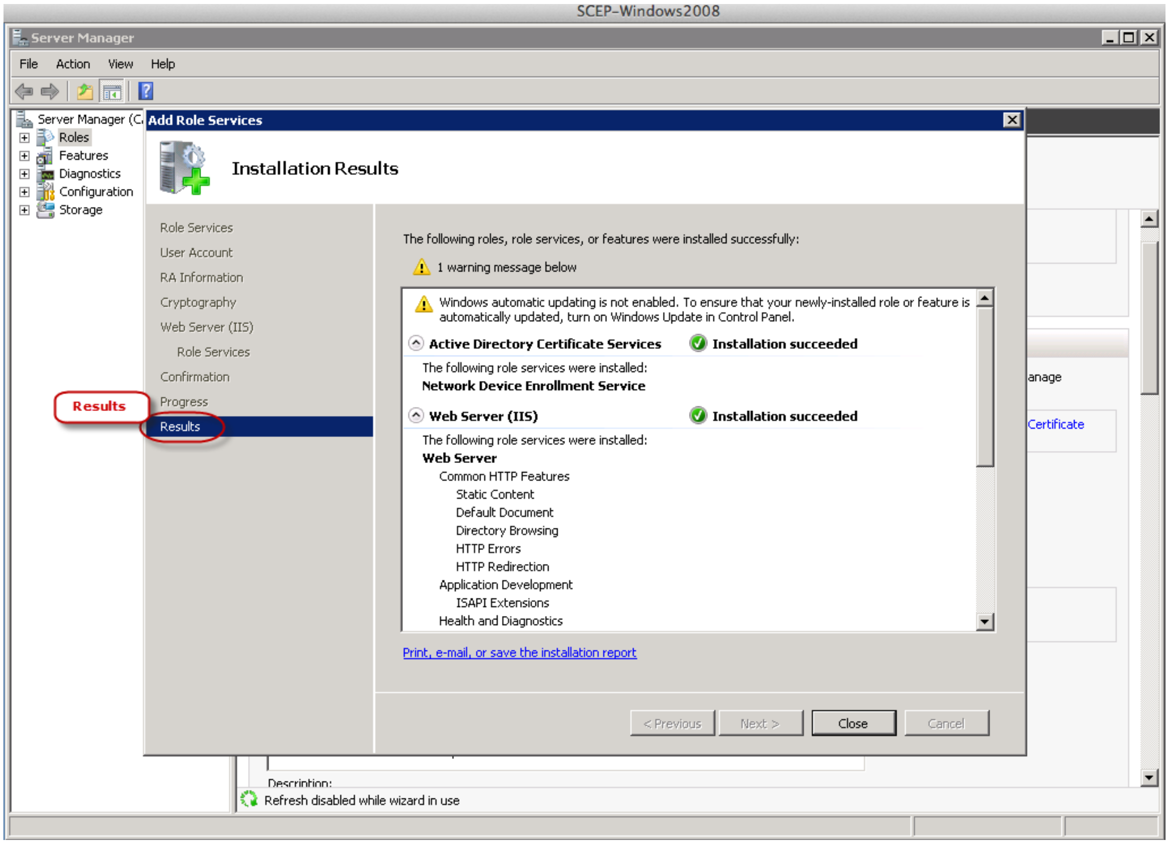
The following roles, role services, or features are being installed:

Active Directory Certificate Services
Web Server (IIS)
Remote Server Administration Tools

Initializing installation...

The above window shows the installation in progress. After the installation is complete, the Results window appears.

37. Verify the Active Directory services, and check if it is successful for the **Active Directory Certificate Services** and **Network Device Enrollment Service**. Click **Close** to continue.



Installation Results

The following roles, role services, or features were installed successfully:

1 warning message below

Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel.

Active Directory Certificate Services **Installation succeeded**

The following role services were installed:
Network Device Enrollment Service

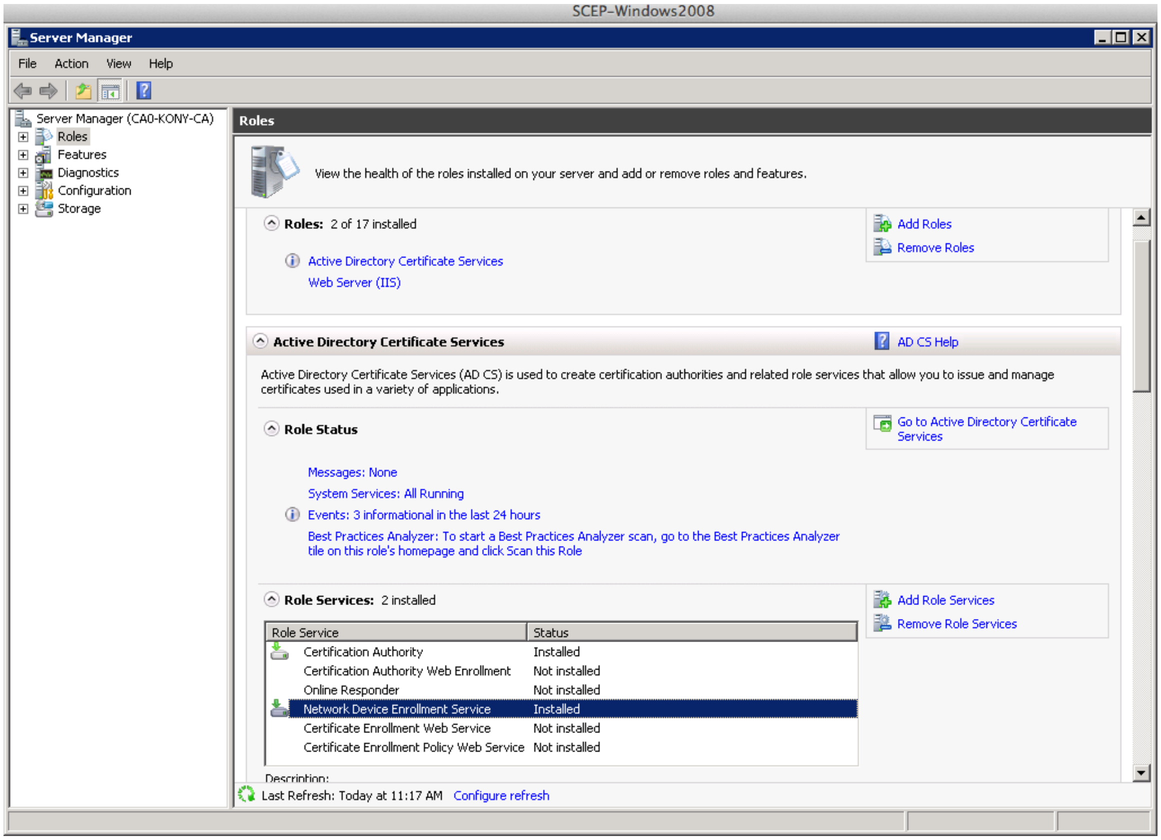
Web Server (IIS) **Installation succeeded**

The following role services were installed:
Web Server
Common HTTP Features
Static Content
Default Document
Directory Browsing
HTTP Errors
HTTP Redirection
Application Development
ISAPI Extensions
Health and Diagnostics

Print, e-mail, or save the installation report

Refresh disabled while wizard in use

38. Click the **Server Manager** icon on the task bar. On the left panel, click **Roles**. The **Roles** window appears.



View the health of the roles installed on your server and add or remove roles and features.

Roles: 2 of 17 installed

Active Directory Certificate Services
Web Server (IIS)

Active Directory Certificate Services

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Role Status

Messages: None
System Services: All Running
Events: 3 informational in the last 24 hours
Best Practices Analyzer: To start a Best Practices Analyzer scan, go to the Best Practices Analyzer tile on this role's homepage and click Scan this Role

Role Services: 2 installed

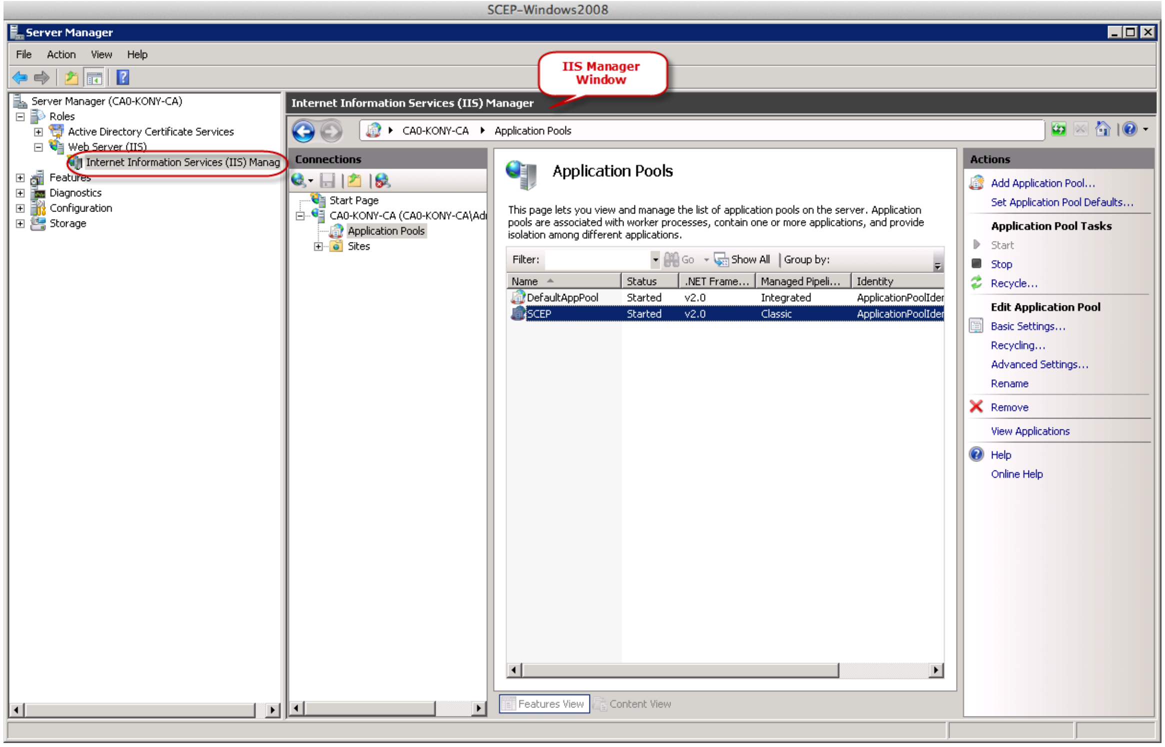
Role Service	Status
Certification Authority	Installed
Certification Authority Web Enrollment	Not installed
Online Responder	Not installed
Network Device Enrollment Service	Installed
Certificate Enrollment Web Service	Not installed
Certificate Enrollment Policy Web Service	Not installed

Last Refresh: Today at 11:17 AM

39. Under Role summary, click **Add Role Services**.

40. Open **Server Manager** and expand **Roles**. From **Web Server**, select **Internet Information Services (IIS) Manager**.

41. In the **IIS Manager** window, select **Application Pools**. Click **Application Pools** and select **SCEP** from the **Application Pools** window.



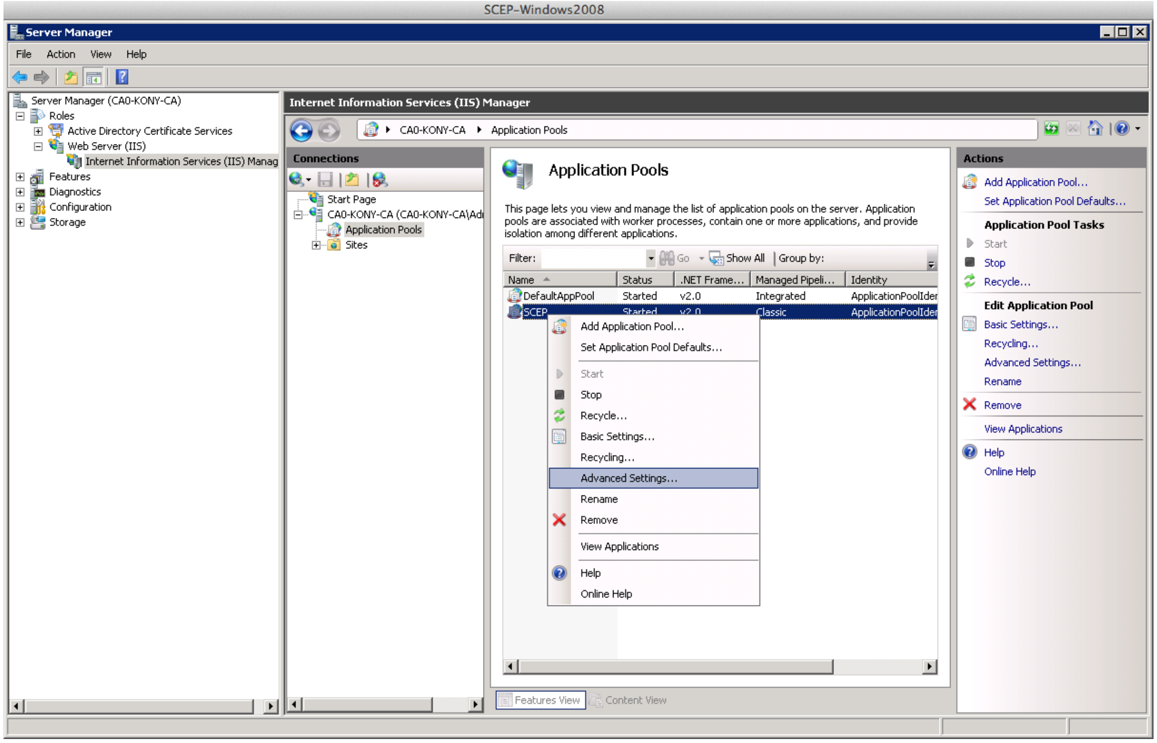
Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Filter: Go Show All | Group by:

Name	Status	.NET Frame...	Managed Pipeli...	Identity
DefaultAppPool	Started	v2.0	Integrated	ApplicationPoolIder
SCEP	Started	v2.0	Classic	ApplicationPoolIder

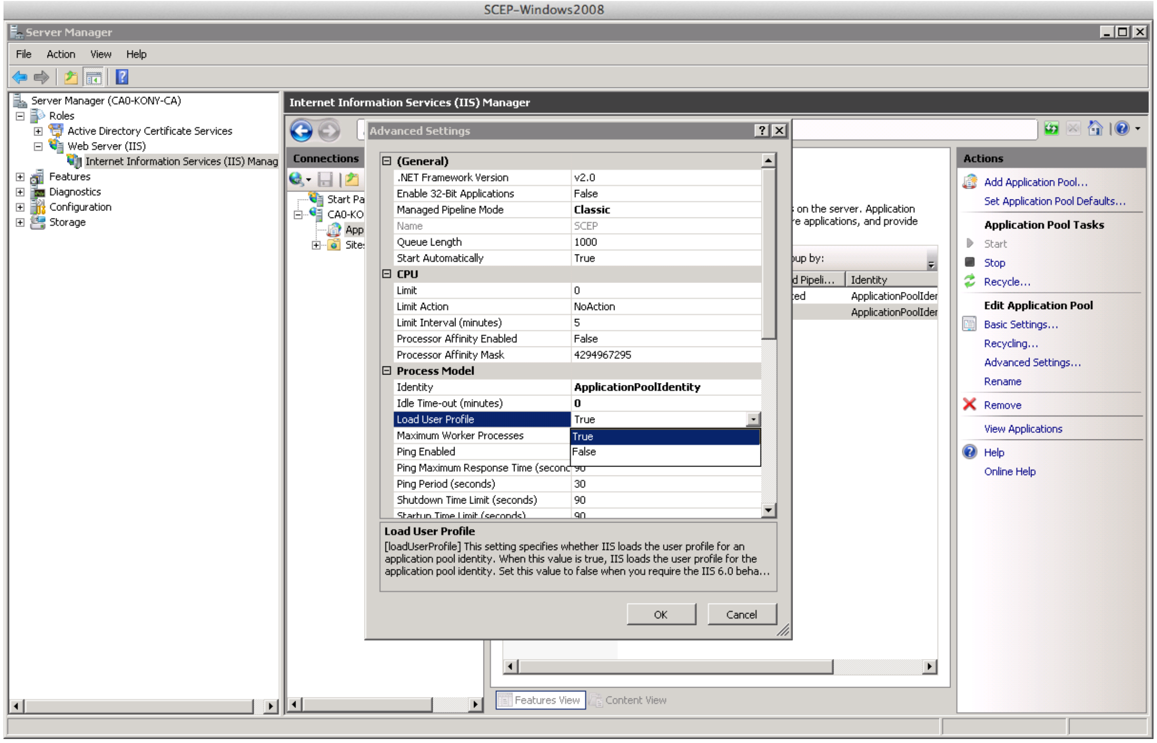
42. Right-click the **SCEP** application and click **Advanced Settings**.



This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET Frame...	Managed Pipeli...	Identity
DefaultAppPool	Started	v2.0	Integrated	ApplicationPoolIder
SCEP	Started	v2.0	Classic	ApplicationPoolIder

43. From the **Advance Settings** window, double-click **Load User Profile** to change the property from false to true. Click **OK** to continue.

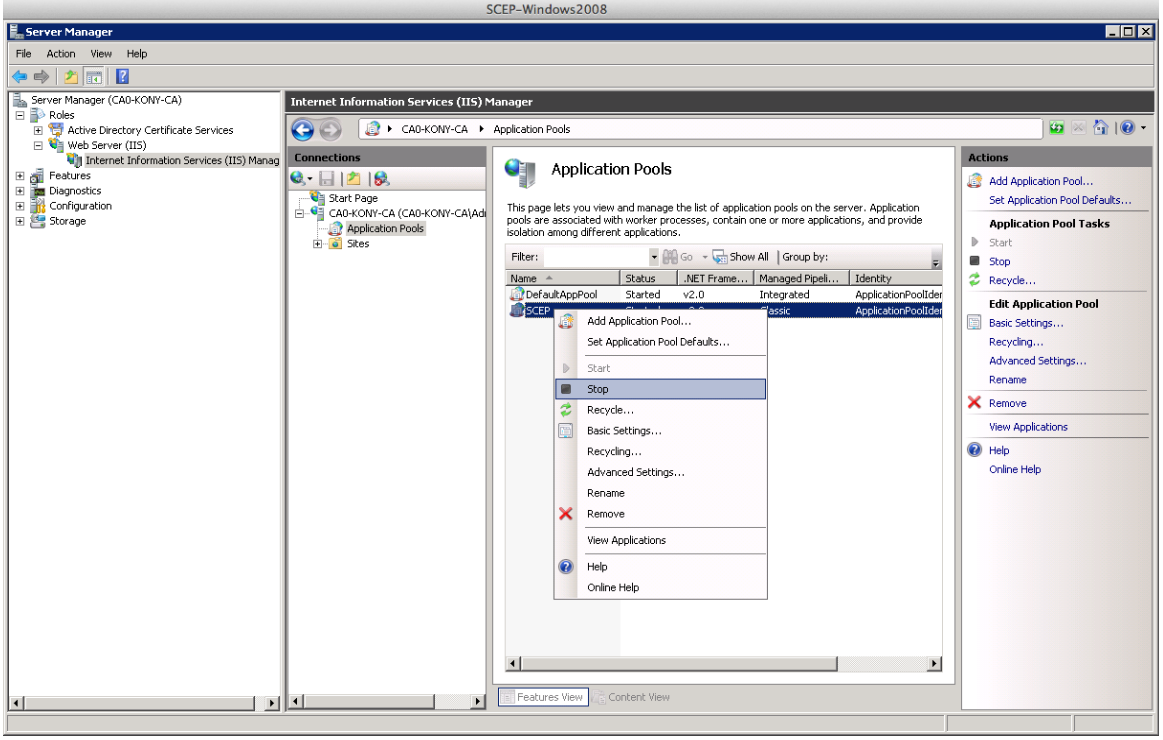


(General)	
.NET Framework Version	v2.0
Enable 32-Bit Applications	False
Managed Pipeline Mode	**Classic**
Name	SCEP
Queue Length	1000
Start Automatically	True
CPU	
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Process Model	
Identity	**ApplicationPoolIdentity**
Idle Time-out (minutes)	**0**
Load User Profile	True True False
Maximum Worker Processes	
Ping Enabled	
Ping Maximum Response Time (seconc	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90

Load User Profile

[loadUserProfile] This setting specifies whether IIS loads the user profile for an application pool identity. When this value is true, IIS loads the user profile for the application pool identity. Set this value to false when you require the IIS 6.0 beha...

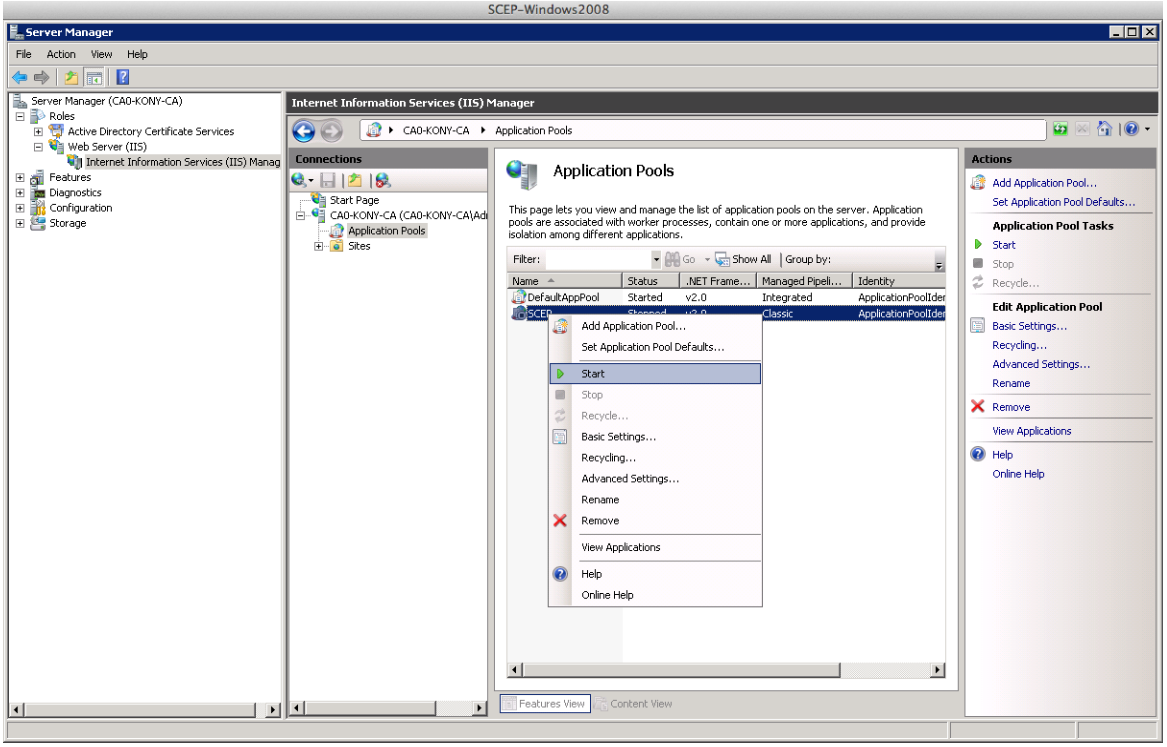
44. Right-click the **SCEP** Application pool, and click **Stop**.



This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET Frame...	Managed Pipeli...	Identity
DefaultAppPool	Started	v2.0	Integrated	ApplicationPoolIder
SCEP	[illegible]	[illegible]	Classic	ApplicationPoolIder

45. Right-click **Application Pool** and click **Start**.



This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET Frame...	Managed Pipeli...	Identity
DefaultAppPool	Started	v2.0	Integrated	ApplicationPoolIder
SCEP	Stopped	v2.0	Classic	ApplicationPoolIder

46. Open Windows Registry with the command `regedit`

47. Navigate to the location **HKEY_LOCAL_ MACHINE\Software\Microsoft\Cryptography\MSCEP**

48. Create a new registry key *UseSinglePassword.*

49. In the *UseSinglePassword key*, create a *DWORD key UseSinglePassword* and set its value to 0.

50. Create a new registry key *PasswordMax.*

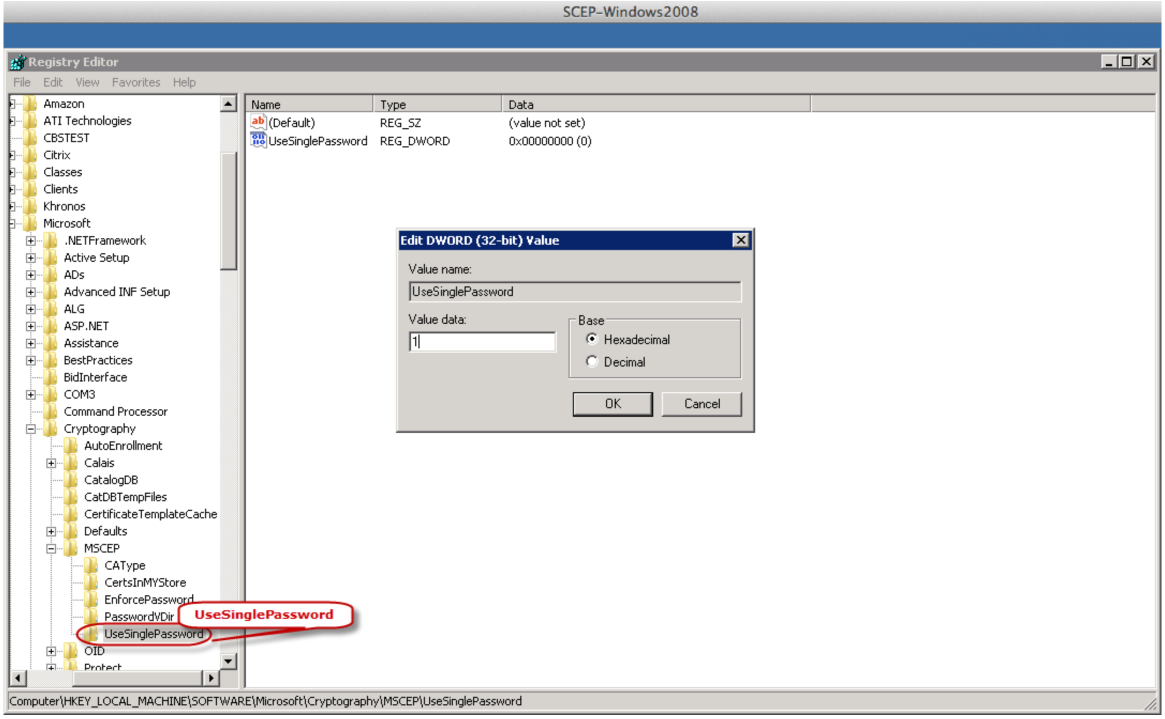
51. In the *PasswordMax* key, create a *DWORD key PasswordMax* and set its value based on your environment.

> ***Note:*** Recommended value is 50% of your total ios devices.

52. Click **UseSinglePassword** folder.

Edit DWORD (32-bit) Value window appears.

53. Find the registry key value as UseSinglePassword and modify **Value data** as 1. Click **OK** to continue.



Name	Type	Data
(Default)	REG_SZ	(value not set)
UseSinglePassword	REG_DWORD	0x00000000 (0)

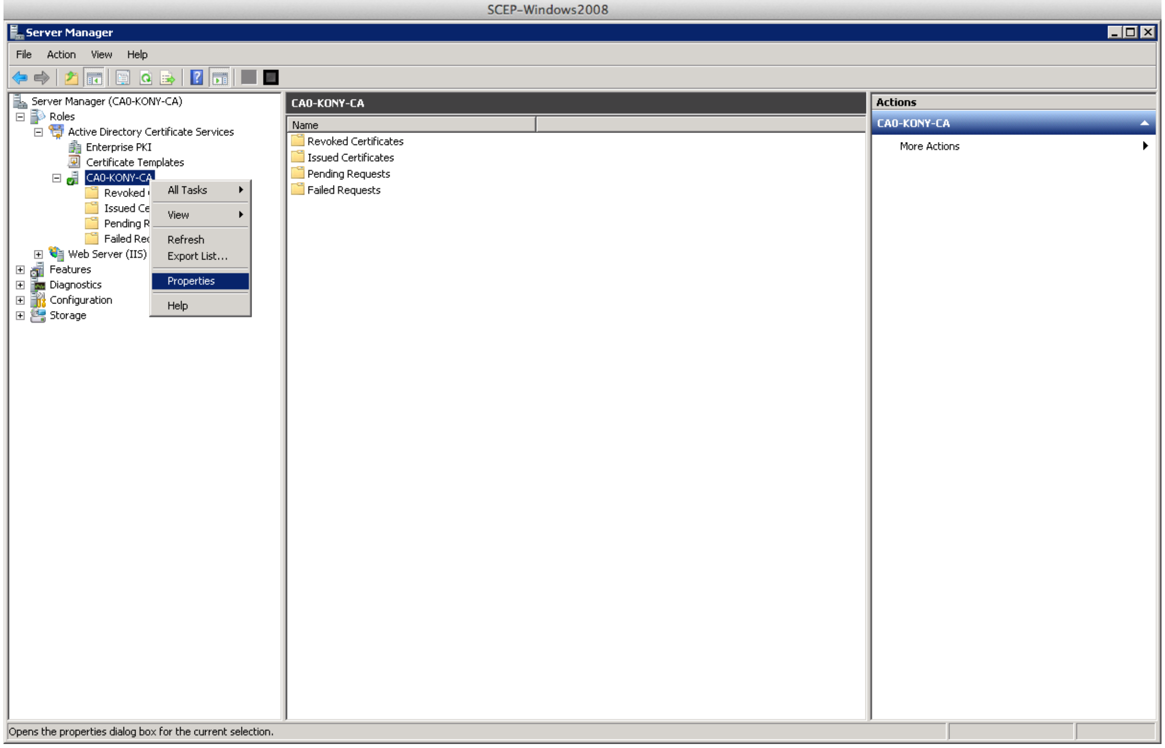
Value name: UseSinglePassword

Value data: 1

Base: ● Hexadecimal ○ Decimal

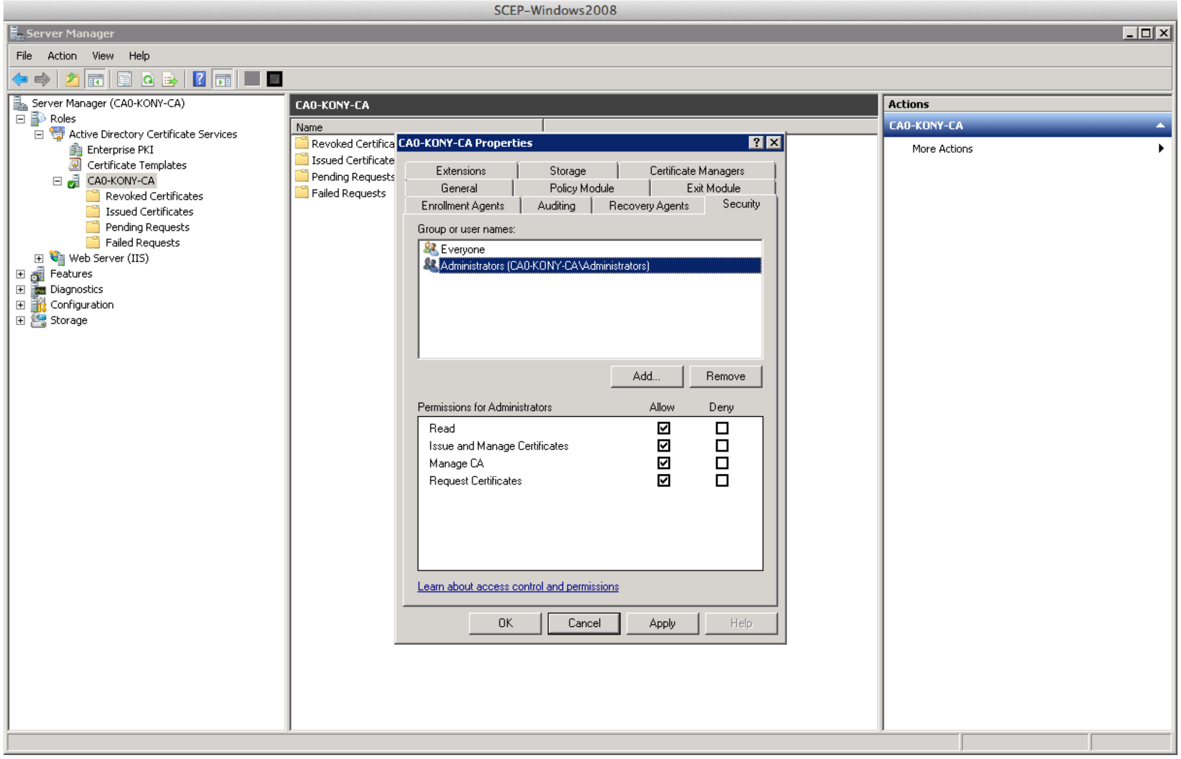
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\UseSinglePassword

54. From the Server Manager, navigate to **CA0-KONY-CA** section. Right-click to go to properties.



Opens the properties dialog box for the current selection.

55. Under the **Security** tab, select **Administrator** and allow all the permissions displayed in the image above. Accept the default values and click **Apply**. Click **OK** to continue.

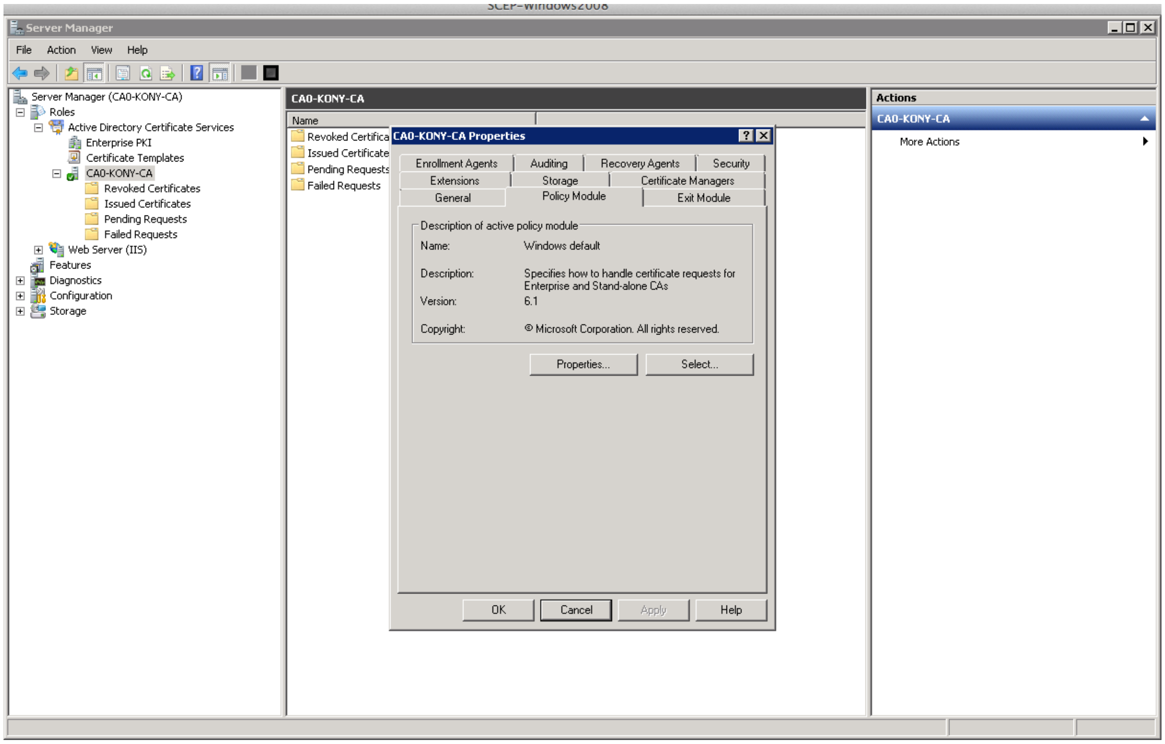


Group or user names:

- Everyone
- Administrators (CA0-KONY-CA\Administrators)

Permissions for Administrators	Allow	Deny
Read	☑	□
Issue and Manage Certificates	☑	□
Manage CA	☑	□
Request Certificates	☑	□

56. Navigate to the **Policy Module** tab, and then click **Properties**.



Description of active policy module

Name: Windows default

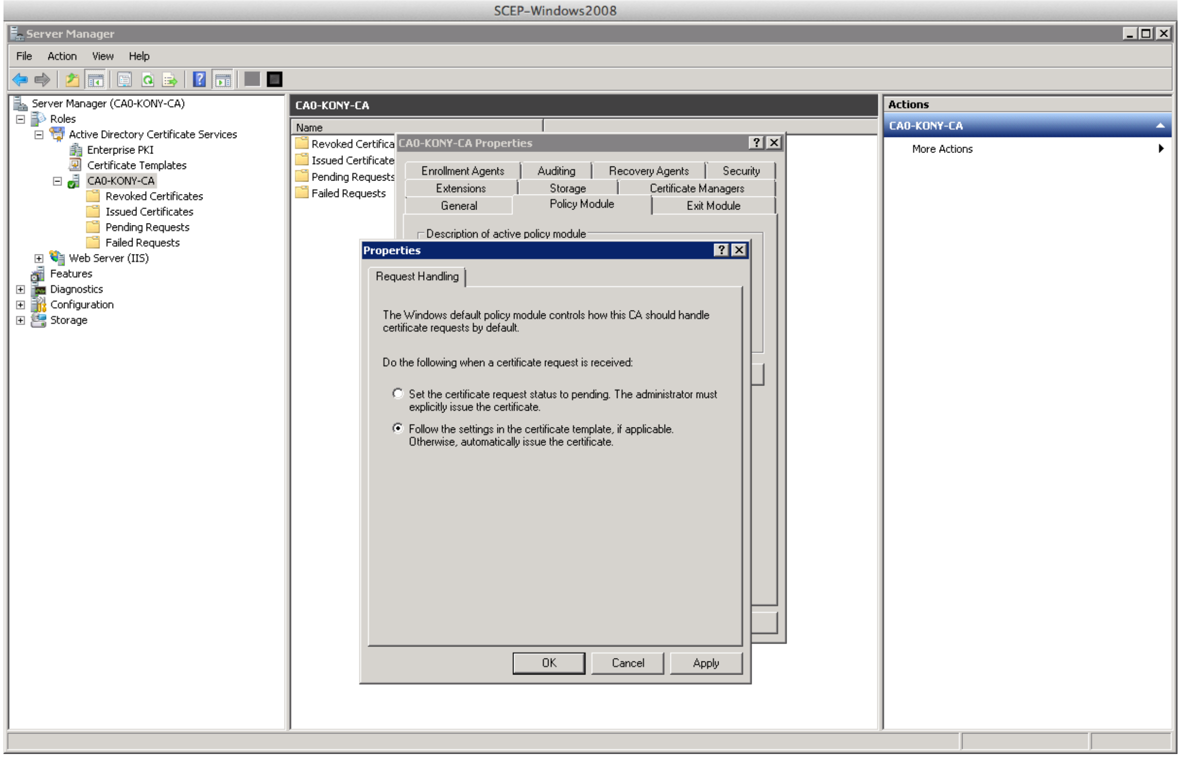
Description: Specifies how to handle certificate requests for Enterprise and Stand-alone CAs

Version: 6.1

Copyright: © Microsoft Corporation. All rights reserved.

57. Select Request Handling property as "Follow the settings in the certificate template, if applicable Otherwise, automatically issue the certificate"

58. Click the **Apply** button and then **OK** to continue.



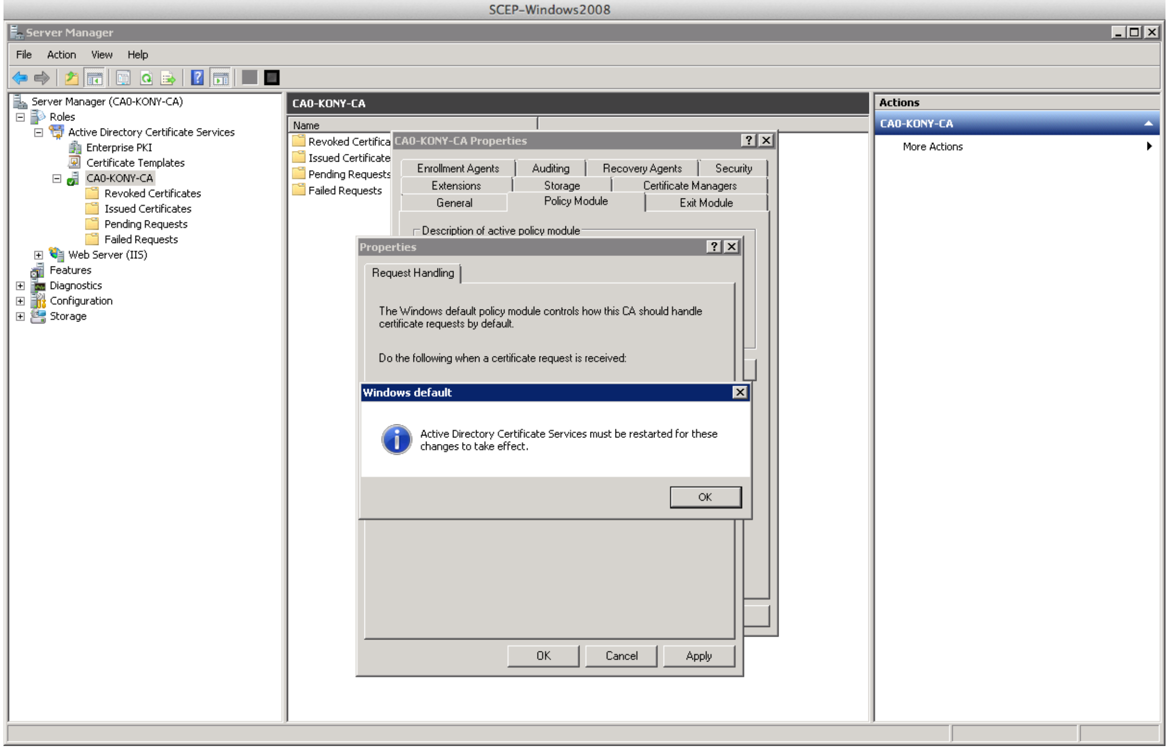
The Windows default policy module controls how this CA should handle certificate requests by default.

Do the following when a certificate request is received:

○ Set the certificate request status to pending. The administrator must explicitly issue the certificate.

● Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate.

59. Accept the message, and click **OK** to continue.

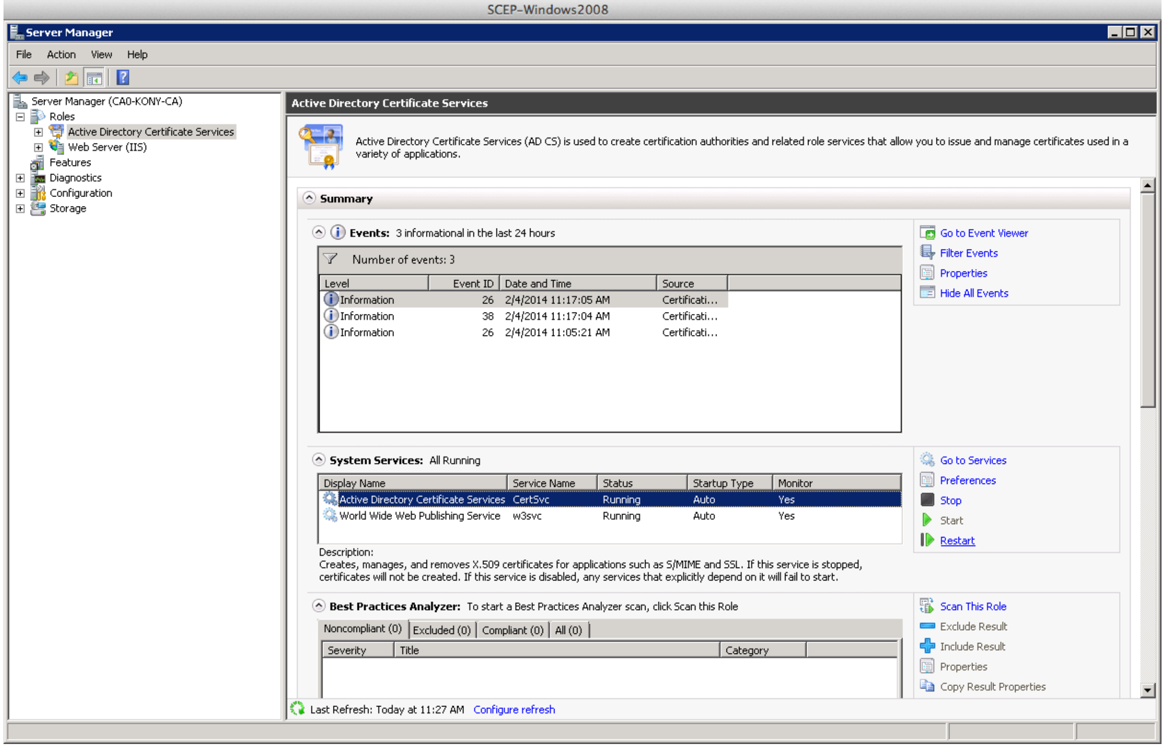


The Windows default policy module controls how this CA should handle certificate requests by default.

Do the following when a certificate request is received:

Active Directory Certificate Services must be restarted for these changes to take effect.

60. Go to **Server Manager** and select Active Directory Certificate Services (ADCS).



Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Events: 3 informational in the last 24 hours

Number of events: 3

Level	Event ID	Date and Time	Source
Information	26	2/4/2014 11:17:05 AM	Certificati...
Information	38	2/4/2014 11:17:04 AM	Certificati...
Information	26	2/4/2014 11:05:21 AM	Certificati...

System Services: All Running

Display Name	Service Name	Status	Startup Type	Monitor
Active Directory Certificate Services	CertSvc	Running	Auto	Yes
World Wide Web Publishing Service	w3svc	Running	Auto	Yes

Description:
Creates, manages, and removes X.509 certificates for applications such as S/MIME and SSL. If this service is stopped, certificates will not be created. If this service is disabled, any services that explicitly depend on it will fail to start.

Best Practices Analyzer: To start a Best Practices Analyzer scan, click Scan this Role

Noncompliant (0) | Excluded (0) | Compliant (0) | All (0)

Severity	Title	Category

Last Refresh: Today at 11:27 AM

61. Click the **Restart** button to restart this service.

6.1.3 Installing SSL Certificate on IIS Web Server

The Secure Socket Layer protocol ensures secure transactions between web servers and browsers. The protocol uses a third party, a Certificate Authority (CA), to identify one end or both end of the transactions for HTTPS communication.

To set up SSL on an Internet Information Services (IIS) computer, follow these steps:

1. You need the certificates for HTTPS communication.To procure any SSL certificate, follow these steps (applicable to all SSL vendors):

   i. Generate CSR (Certificate Signing Request).

   ii. Submit CSR to CA (Certificate Authority).

   iii. Get/download a Signed SSL provided by CA.

   iv. Sign the Certificate with private key and other supporting associated ROOT and intermediate certificates.

   > ***Note:*** Self Signed Certificates are not supported.

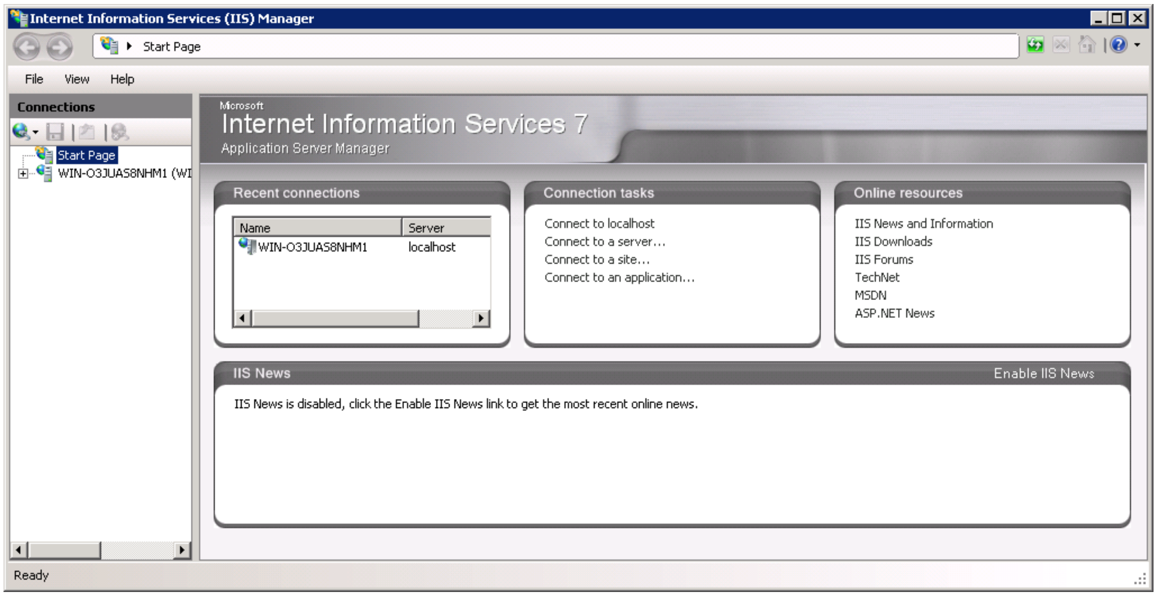
2. You need to procure these certificates from any of the CA vendors, preferably:

   - Verisign - Verisign Secure SSL
   - GoDaddy - GoDaddy Secure SSL

> ***Note:*** We have tested with Verisign or GoDaddy only in DEV/QA and production as these certificates have maximum mobile device compatibility.
>
> These certificates require 600 octal file permission so that the SSL keys can be read.

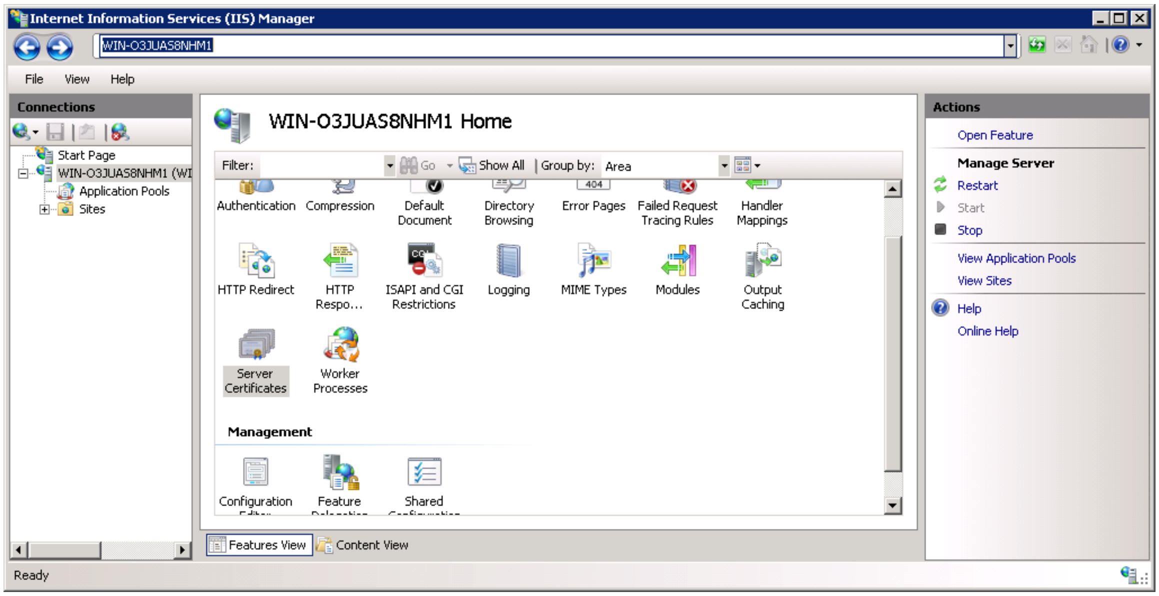
The server instance that will be installed should have a valid DNS name that matches the common name. SSL should be a trusted certificate issued by a valid certificate authority (as listed above) and it should be compatible on mobile devices.

1. Go to Start > Run, enter the command `inetmgr`, and then press Enter key.

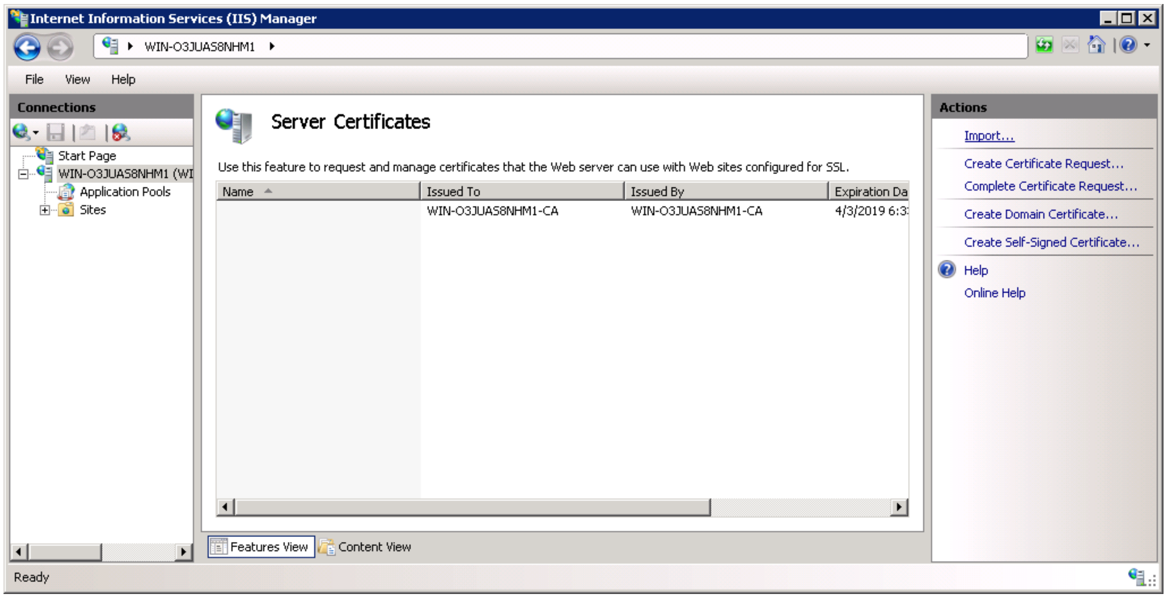


IIS News is disabled, click the Enable IIS News link to get the most recent online news.

2. Double-click **Server Certificates**.



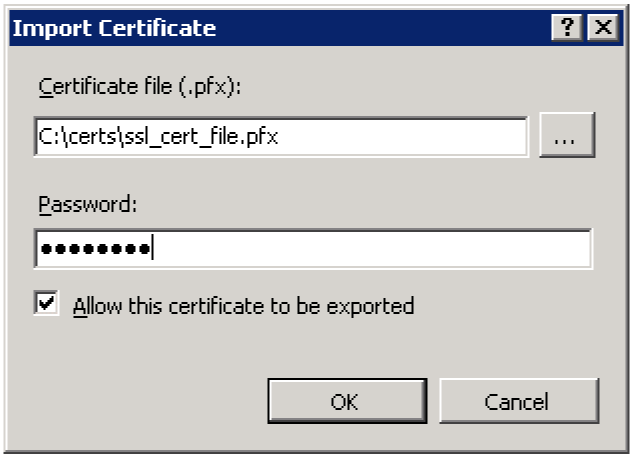
3. On the right pane click on **Import**.



Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Da
	WIN-O3JUAS8NHM1-CA	WIN-O3JUAS8NHM1-CA	4/3/2019 6:3

4. Select SSL certificate in .PFX format, enter certificate password if any, and then click **OK**.



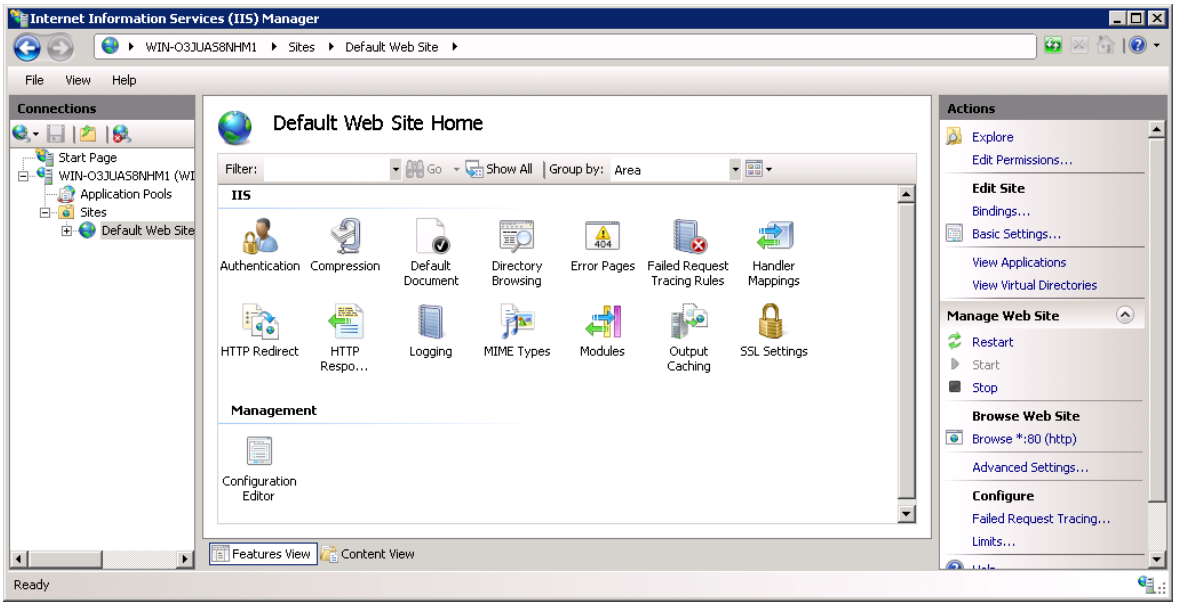
Import Certificate

Certificate file (.pfx): C:\certs\ssl_cert_file.pfx

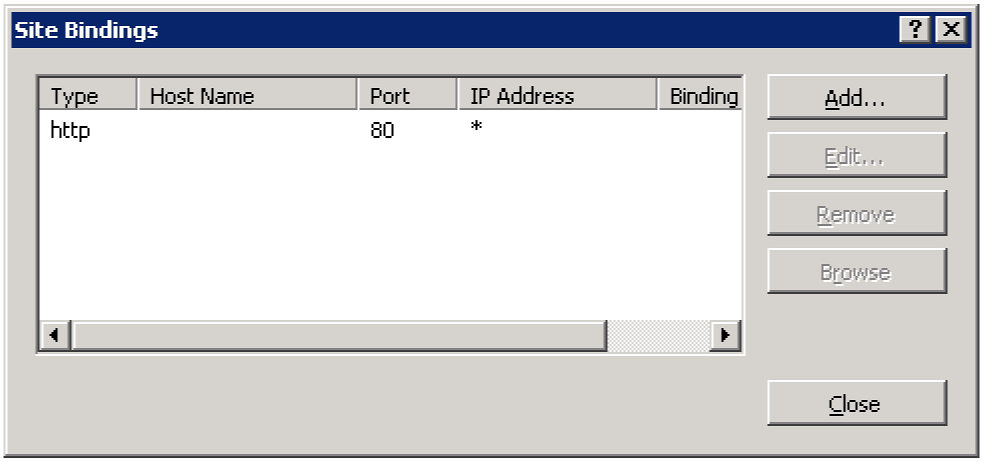
Password: ●●●●●●●●●

☑ Allow this certificate to be exported

5. On the right pane, click **Bindings**.



6. Click **Add**.

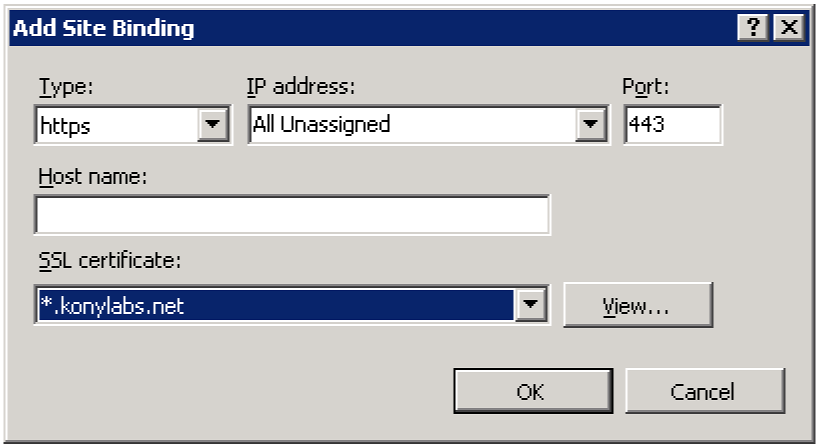


Site Bindings

Type	Host Name	Port	IP Address	Binding
http		80	*	

7. Select https from Type drop-down list, All Unassigned as IP address, and then select SSL certificate from the drop-down list.

> ***Note:*** In case if you are using specific domain SSL please also mention hostname as well. In case multiple IP addresses available on the system please select one from the IP address drop-down list instead of selecting All Unassigned.



Add Site Binding

Type: https

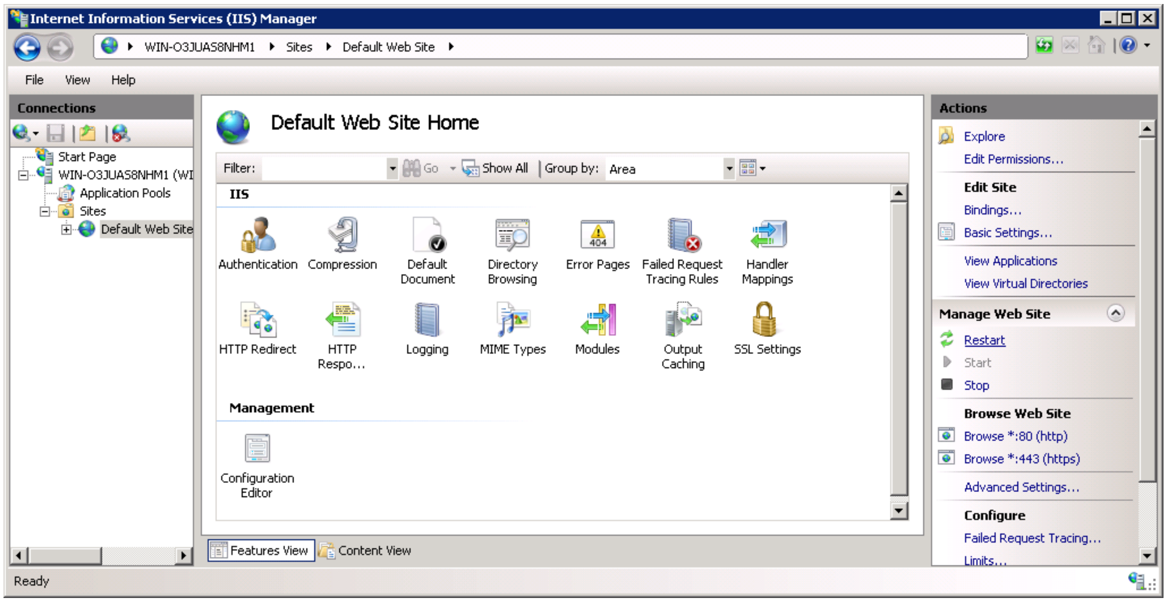
IP address: All Unassigned

Port: 443

Host name:

SSL certificate: *.konylabs.net

8. Click Restart from the right pane to restart IIS service.



9. Once service is restarted, reboot Windows server.

6.1.4 Configuring EMM Server with SCEP values

During EMM installation, if iOS device enrollment is supported, Installer may ask for SCEP server details. Based on SCEP copy of installation, provide SCEP values. The details given below can be obtained from the SCEP Server.

SCEP Values	Description
-DSCEP_CHALLENGE	SCEP Password challenge (Refer Step no 12 under section 2.2.3)
-DSCEP_SERVER_URL =<your SCEP server>	SCEP Service URL(Refer Step no 10 under section 2.2.3)
-DSCEP_KEY_SIZE=2048	RSA key size in bits either 1024 or 2048 (Refer Step no 10 under section 2.2.2)
-DSCEP_CA_INSTANCE_ NAME=<your SCEP instance name>	Certificate authority name used in SCEP installation.(Refer Step no 12 under section 2.2.2)
-DSCEP_COMMON_NAME=<your SCEP instance common name>	Representation of X.500 name for example, O=Company Name,CN=Foo (Refer Step no 12 under section 2.2.2)
-DSCEP_CHALLENGE_URL =<your SCEP server challenge URL>	Preshared secret for automatic enrolment (Refer Step no 11 under section 2.2.3)
-DSCEP_CA_DOMAIN =<your SCEP server domain name>	Domain name of the user account used while installing SCEP.(Refer Step no 12 under section 2.2.2)
-DSCEP_CA_USERNAME=<your NDES usename>	Account user name used while installing SCEP service. (Refer Step no 21 under section 2.2.2)
-DSCEP_CA_ PASSWORD=xxxxxxxxxx	Password of the user account.(Refer Step no 21 under section 2.2.2)

6.1.4.1 SCEP Configuration Example

Replace XXXX with the values used during your installation.

```
-DSCEP_SERVER_URL=https://ca.XXXXXXXX.com/CertSrv/mscep/

-DSCEP_KEY_SIZE=2048

-DSCEP_CA_INSTANCE_NAME=CA0-XXXXXXXX-CA

-DSCEP_COMMON_NAME=CA0-XXXXXXXX-CA

-DSCEP_CHALLENGE_URL=https://ca.XXXXXXXX.com/CertSrv/mscep_admin

-DSCEP_CA_DOMAIN=CA0-XXXXXXXX-CA

-DSCEP_CA_USERNAME=administrator

-DSCEP_CA_PASSWORD=XXXXXXXXXXXX
```

6.2 Kony Exchange Service Setup

To allow communication between the Windows Server 2008/2012 and your corporate email exchange server (to enable block and unblock email access on enrolled devices), Kony Exchange service should be configured. Using this service, you can also restrict email clients that can be used on enrolled devices.

To set Kony Exchange service,

1. Enable powershell remoting using the "Enable-PSRemoting" cmdlet. Ensure that you have admin privileges before you execute this command. For more information, refer http://technet.microsoft.com/en-us/library/hh849694.aspx

2. **Set trusted hosts**. This includes a list of ip addresses or DNS names from which you need to entertain powershell remoting.

   Powershell console commands are:

   ```
   cd WSMan:\localhost\Client : This will move to the WSMan Client
   policy
   directory.
   Set-Item .\TrustedHosts * : "*" will allow all. Incase Exchange
   Servers
   IP/DNS is supposed to be trusted add it inplace of "*"
   ```

   > ***Note:*** If there are multiple trusted hosts, seperate them by commas.

3. Allowing/Disallowing unencrypted traffic:
   Unencrypted traffic means using HTTP. If remoting has to work over HTTP, use the following commands:

```
cd WSMan:\localhost\Client: This will move to the WSMan Client
policy directory.
Set-Item .\AllowUnencryptedTraffic $true: This will allow the
session to work without encryption
```

After executing the above mentioned commands on powershell, open **IIS Server Manager>Sites>Default Web Site>Powershell** and enable SSL.

Disallowing unencrypted means using HTTPS. The commands are as follows:

```
cd WSMan:\localhost\Client
Set-Item .\AllowUnencryptedTraffic $false
```

After executing the above mentioned commands on powershell, open **IIS Server Manager> Sites>Default Web Site>Powershell** and disable SSL.

4. Install the Kony Exchange Service. During the service installation, feed in appropriate values. If powershell is enabled to work on HTTPS in the server configuration, give the Exchange Server URL like `https://<hostname>/powershell/` else it appears like `http://<hostname>/powershell/`

> ***Note:*** **Execute the following command in the Powershell console as an administrator to confirm that Powershell remoting is successful.** `New-Possession -Configuration Name Microsoft.Exchange -Connectionless <your exchange server Cockleshell URIC> -Credential <your user logo> -Authentication Basic -Allow Redirection`
> **Enter password when prompted. Session details will appear on the console**

For more information, refer Kony Exchange Service Document.
Kony Exchange Service Document

6.3 Kony Windows Mobile 6.x Group Policy service installation

As mentioned in http://technet.microsoft.com/en-us/library/dd261866.aspx a machine that supports GPMC has to be in the domain in which SCMDM 2008 server is installed. To support Windows Mobile 6.x devices on EMM, Group Policy service must be installed.

> *Important:* This service has to be installed on the machine that supports group policy management. This machine should be accessible to SCMDM 2008 machine. It need not have a public IP and can remain with in the corporate domain.

The Installation file can be downloaded from the developer portal.

1. Enable PowerShell scripts to run on Group policy machine. For more information visit the page.
2. Install `InstallerGPMCMDM.msi` on the machine as per below section:

   Service Configuration: This section defines the parameters for GP service with which it will be started.

   a. **(URL):** Address on which service will listen to the requests.

   b. **User Name and Password** : Valid credentials are required to install the MDM service.

   Kony Server Configuration:

   This section defines the credentials of Kony Server User that is used to generate the HashKey to validate the requests.

   - Once Install button is pressed, installer will install the GPMC service along with its `Config.xml file`. Install it in the machine and start the service.
   - Once the service is started, it will serve the request on URL configured during installation.

- To validate the request, once the request reaches to the GPMC service, service uses the Kony Server User credentials defined in `config.xml` and generate the hash key at its end. Once hash key is generated by MDM service, it matches it with hash key received in request. That is the process of authentication under the hood

3. Go to the installation directory on the machine on which GP Server 2008 was installed. A "`Config.xml`" file is found with a layout similar to:-

```
<Config>
<UserName>KonyServerUser</UserName>
<Password>Password</Password>
<ServiceUserName>KH1446</ServiceUserName>
<ServicePassword>Password#123</ServicePassword>
<QueueSize>200</QueueSize>
<Logging>true</Logging>
<MDMInstance>mdm1</MDMInstance>
<MDMServerUrl>https://*:8878/</MDMServerUrl>
<PolicyServerUrl>http://gpmc.pftest.local:8883/</PolicyServerUrl>
<PolicyServerCallbackUrl>http://winmdm.pftest.local:8585/</PolicyServerCallbackUrl>
</Config>
```

Explanation for the configuration parameters values:

- **UserName and Password:** These parameters get configured with the value provided during installation. Refer Step number 4 for more information.

- **ServiceUserName and ServicePassword:** These parameters are configured with the value provided during installation. Refer Step number 4 for more information.

- **Queue Size:** This is the size of the queue maintained by this service for asynchronous processing. Enter a convenient value. If the queue gets full, the service is denied to the clients.

- **Logging:** Make it **true** if windows event logging is needed, else **false**.
- **MDMInstance:** During the MDM Server installation, a MDM Instance name is given. Give that instance name here.
- **MDMServerUrl:** Enter the server DNS or IP here along with port on which this service is supposed to listen. If **https** is used, refer to the step number 5 for binding SSL port with a certificate.
- **PolicyServerCallbackUrl**: This is the same machine as MDMServerUrl except that it must listen on a different port. Choose a different port.
- **PolicyServerUrl**: This is the DNS/IP of the machine on which group policy execution is enabled. Give the DNS/IP and Port on which the group policy will be launched.

Open the windows logs and check for any errors. If no errors, the service will start listening incoming connections on PolicyServerUrl. If any error is found, the service will not work as desired. It may even stop.

> ***Note:*** Ensure that the port given is proper and also the DNS/IP is accessible in the domain.

> ***Important:*** If `Config.xml` needs to be changed for any reason, before making the changes, stop the service using ***stopService.ps1***. Make the changes and use ***restartService.ps1*** to restart the service.

4. The Kony MDM Console requires the **PolicyServerUrl** as mentioned in the `Config.xml` files in installation path. Note this URL and use it in Kony MDM Console.
5. To bind a port with a SSL certificate for secure communication (https):

   a. For windows 2003 download "Windows 2003 SP1 Support Tools" from this page.

      These tools contain a tool called "`httpcfg.exe`" which allows to bind a port with a SSL Certificate. Information about this tool is mentioned on this page.

For newer OS "`httpcfg.exe`" is obsolete and replaced with "`netsh.exe`" as given on this page.

b. For newer OSes (2008, Vista) powershell command can be used to bind a port with SSL Certificate. More information is given on this page.

6.4 Windows Server for Windows Phone App Wrapping

6.4.1 Software Requirements

Component	Version
Visual Studio	Visual studio 2013 express edition with update 3 (Prerequisite for Windows app wrapping)
Microsoft Silverlight Runtime	Microsoft Silverlight Runtime 5.0 (Prerequisite for Windows app wrapping)
Microsoft Silverlight	Microsoft Silverlight SDK 5.0 (Prerequisite for Windows app wrapping)
Cygwin	Latest Cygwin (32 bit) version. (Prerequisite for Windows app wrapping)

6.4.2 How to Install Visual Studio

Windows Phone Enterprise apps must be signed for app management and app wrapping. You must install Visual Studio to manage Windows phone app wrapping.

See the Visual Studio website for more information on how to install and configure Visual Studio.

6.4.3 How to Install Microsoft Silverlight Runtime

To manage enterprise apps, you need the Windows phone app wrapping feature to function. You must install Microsoft Silverlight Runtime to manage Windows phone app wrapping.

See the Microsoft Silverlight Runtime website for more information on how to install Microsoft Silverlight Runtime.

6.4.4 How to Install Microsoft Silverlight SDK

To manage enterprise apps, you need Windows phone app wrapping feature to function. You must install Microsoft Silverlight SDK to manage Windows phone app wrapping.

See the Microsoft Silverlight SDK website for more information on how to install and configure Microsoft Silverlight SDK.

6.4.5 How to Install Cygwin

Cygwin is a large collection of GNU and Open Source tools that provide features similar to a Linux distribution on Windows. To manage Windows phone app wrapping, install Cygwin. With Cygwin, user binaries are copied to the Windows machine. To manage enterprise apps, you need Windows phone app wrapping feature to function.

> *Important:* You should be familiar with Linux commands to work with Cygwin.

See the Cygwin website for more information on how to install and setup Cygwin.

> *Important:* You must install Cygwin along with openSSH, openSSL, Dos2Unix, Winzip, Unzip, and Curl components.

6.4.5.1 How to Configure Cygwin Properties

To configure Cygwin for enterprise application wrapping based on your system settings, follow these steps:

1. Right click on **Computer**, and select **Properties**. The system window appears.

2. Select the **Advanced System Settings** link from the **Control Panel Home** pane. The **System Properties** window appears.

3. Select **Environment Variables**.

4. In the **Environment Variables** window, go to **User Variables** and select **New**.
   1. Enter **CYGWIN_HOME** in the Variable Name field.
   2. Enter `C:\cygwin64\bin` in the Variable Value field.
   3. Click **OK**.
5. Select **Path** from **User Variables** and click **Edit**.
   1. Add `C:\cygwin64\bin` in the Variable Value field.
   2. Click **OK**.

> ***Important:*** For Windows wrapping, directory path should be less than 260 characters. If the path is more than 260 characters, the signing process will fail during application wrapping

6.4.5.2 How to Configure SSH Server

To configure the SSH server, follow these steps:

1. Navigate to your Cygwin installation folder (for example, c/cygwin).
2. Select **Cygwin.bat**, right click, and select **Run as administrator**. The Command prompt appears.
3. In the command prompt, type `ssh-host-config`, and press enter. An alert `Should StrictModes be used? (yes/no)` appears.
4. Type `Yes` and press enter. An alert `Should privilege separation be used? (yes/no)` appears.
5. Type `Yes` and press enter. An alert `you want to install sshd as a service. (yes/no)` appears.

6. Type `Yes` and press enter. The system prompt `Enter the value of CYGWIN for the daemon: []` appears.

7. Type `ntsec tty` and press enter. An alert `Do you want to use a different name? (yes/no)` appears.

8. Type `No` and press enter. The system prompt `Please enter the password for user <username>)` appears.

9. Type the password and press enter.The `Reenter:` prompt appears.

10. Type the password again and press enter. A confirmation message on SSHD configuration appears.

11. Execute the following commands:

    - `chmod +r /etc/passwd`: Provides read permissions to password file.
    - `chmod u+w /etc/passwd`: Provides write permissions to user.
    - `chmod +r /etc/group`: Provides read permissions to a group file.
    - `chmod u+w /etc/group`: Provides write permissions to user.
    - `chmod 755 /var`: Provides all permissions to var folder.
    - `touch /var/log/sshd.log`: Creates a new empty file sshd.log.
    - `chmod 644 /var/log/sshd.log`: Owner can write and other users can only read the log file.
    - `chown system /etc/ssh*`: Changes owner for ssh* files to system.
    - `chown system /var/empty`: Changes owner for /car/empty folder to system.
    - `mkgroup -l > ..\etc\empty`: This will print /etc/group file to /etc/empty file.

- `mkpasswd -l > ..\etc\passwd`: This will print /etc/passwd file to /etc/passwd.
- `chmod a+x /etc/sshd_config`: This will provide read and write permission to the sshd_config file.

> ***Important:*** If the openssh you are using is version 6.7, perform the following steps:
>
> Open /etc/sshd_config
> Add the following line towards the end of the file:
> **KexAlgorithms diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1**

12. To start SSHD, open command prompt and enter `net start sshd`. The SSHD service will start successfully.
13. To change passwords, in the command prompt, enter `passwd <username>`.
14. To verify test connection, open an ssh client tool, enter localhost in connection type text box, and click open. The SSH terminal opens, and a success message appears.

7. EMM Windows Components

This section explains how to install EMM Windows Components using Kony EMM Windows Components installer. Go to the next section if you manually installed EMM Windows components.

For Kony Management Suite to work on the Windows platform, you must install the following:

- Kony Exchange Service
- Windows Mobile 6.x Group Policy
- CA Role
- NDES (SCEP)
- Windows App Wrapping

The EMM Windows Components installer installs all the above components except the Windows App Wrapping.

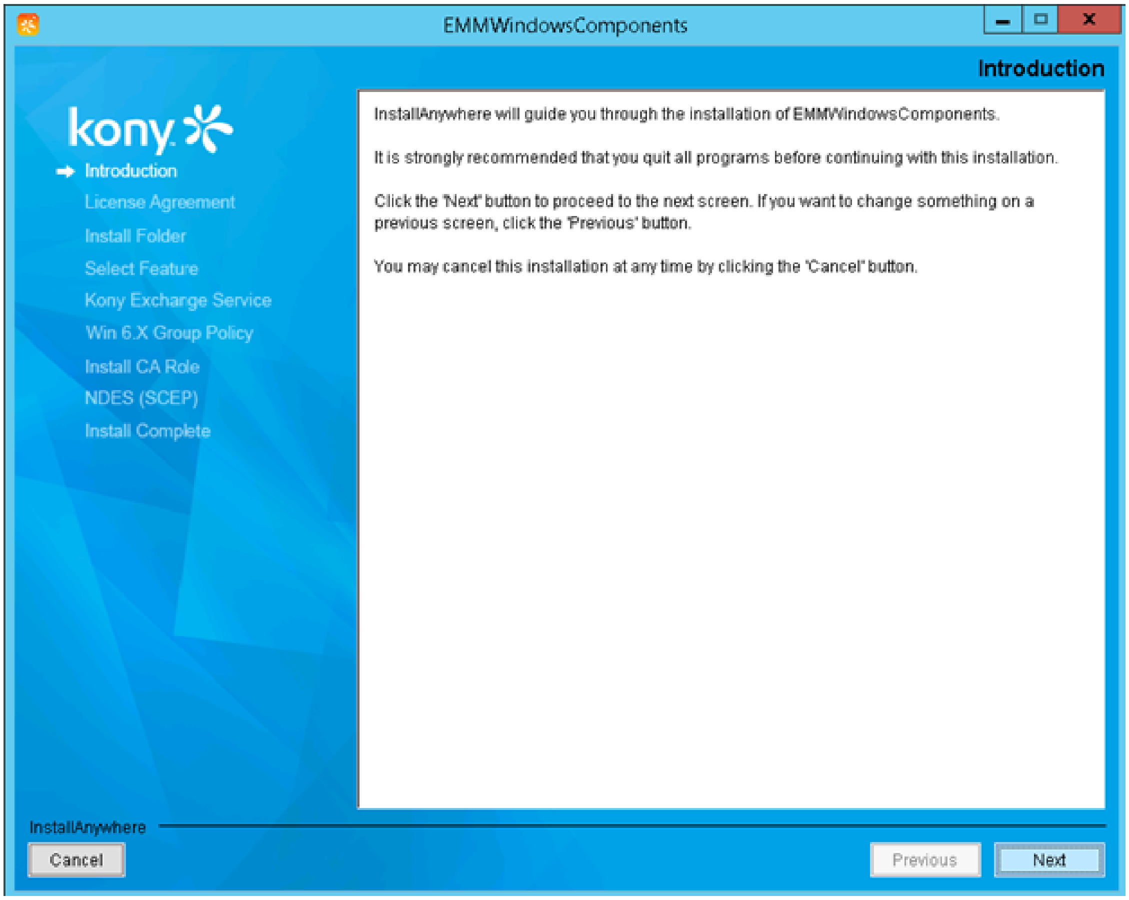
7.1 Prerequisites

- Kony Exchange Service - Powershell 3.0 and above, .Net 3.5 and above.
- Group Policy Service - Windows 7 and above, .Net version 4.0
- CA Role and NDES - Windows Server 2012 (enterprise edition recommended).
- EMM Windows Components executable file.

7.2 Installing EMM Windows Components

To install the required components for the Windows Server for the Kony Management Suite, follow these steps:

1. Click the downloaded **EMMWindowsComponents.exe**. The InstallAnywhere page appears.



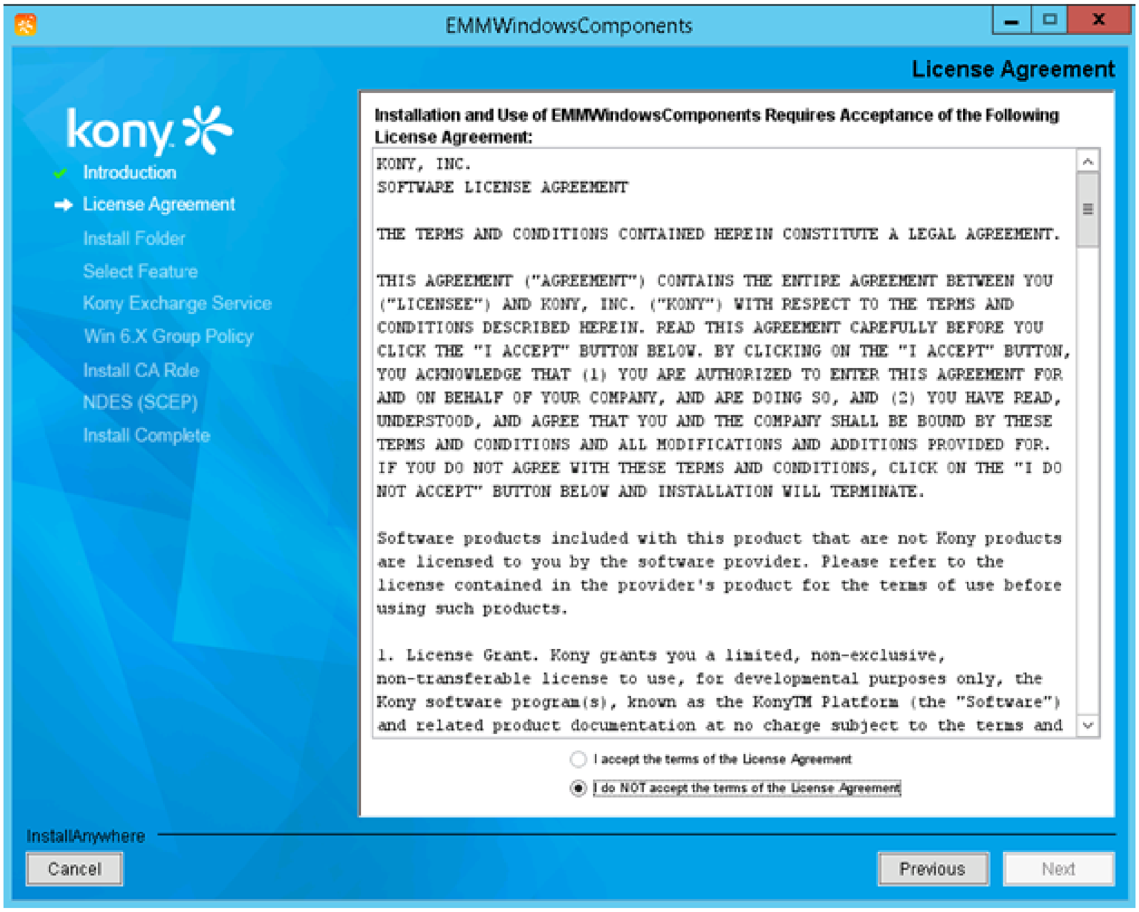
InstallAnywhere will guide you through the installation of EMMWindowsComponents.

It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

2. Click **Next**. The License Agreement appears.



Installation and Use of EMMWindowsComponents Requires Acceptance of the Following License Agreement:

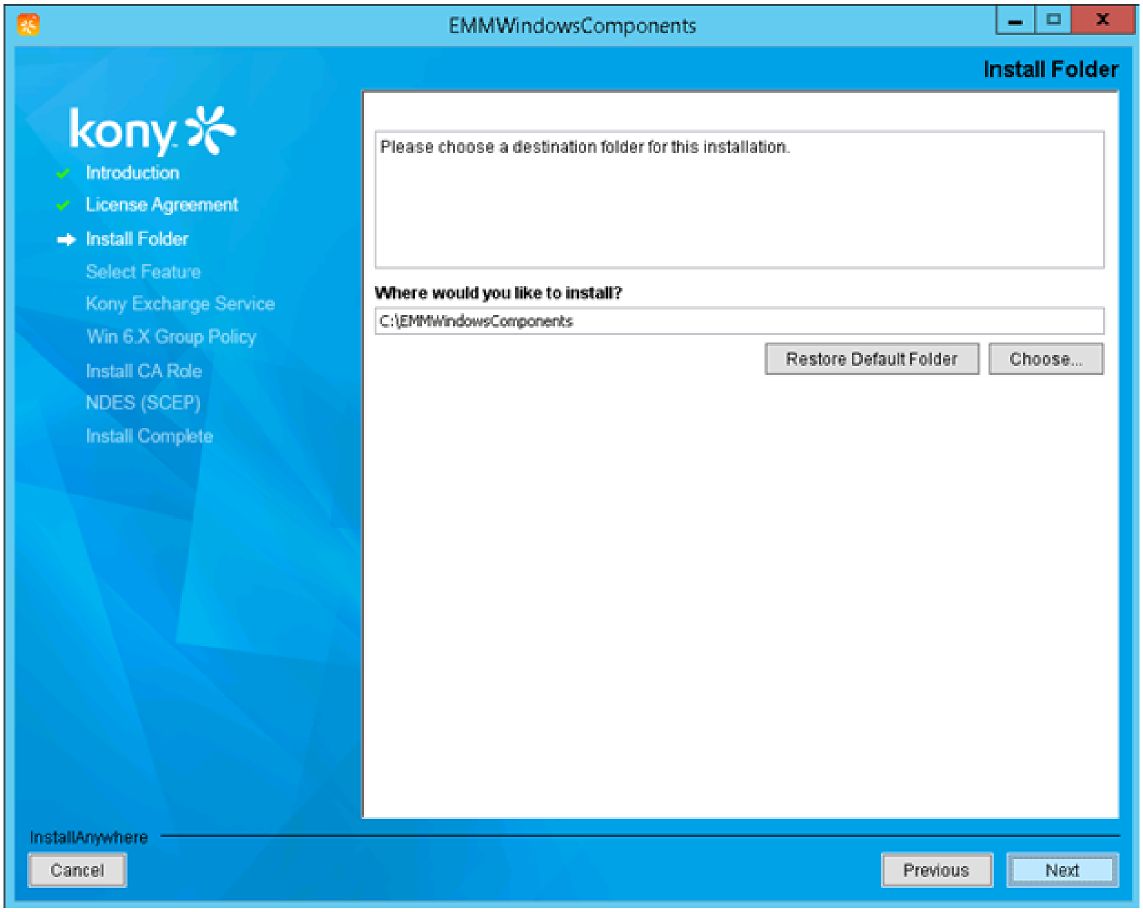
```
KONY, INC.
SOFTWARE LICENSE AGREEMENT

THE TERMS AND CONDITIONS CONTAINED HEREIN CONSTITUTE A LEGAL AGREEMENT.

THIS AGREEMENT ("AGREEMENT") CONTAINS THE ENTIRE AGREEMENT BETWEEN YOU
("LICENSEE") AND KONY, INC. ("KONY") WITH RESPECT TO THE TERMS AND
CONDITIONS DESCRIBED HEREIN. READ THIS AGREEMENT CAREFULLY BEFORE YOU
CLICK THE "I ACCEPT" BUTTON BELOW. BY CLICKING ON THE "I ACCEPT" BUTTON,
YOU ACKNOWLEDGE THAT (1) YOU ARE AUTHORIZED TO ENTER THIS AGREEMENT FOR
AND ON BEHALF OF YOUR COMPANY, AND ARE DOING SO, AND (2) YOU HAVE READ,
UNDERSTOOD, AND AGREE THAT YOU AND THE COMPANY SHALL BE BOUND BY THESE
TERMS AND CONDITIONS AND ALL MODIFICATIONS AND ADDITIONS PROVIDED FOR.
IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, CLICK ON THE "I DO
NOT ACCEPT" BUTTON BELOW AND INSTALLATION WILL TERMINATE.

Software products included with this product that are not Kony products
are licensed to you by the software provider. Please refer to the
license contained in the provider's product for the terms of use before
using such products.

1. License Grant. Kony grants you a limited, non-exclusive,
non-transferable license to use, for developmental purposes only, the
Kony software program(s), known as the KonyTM Platform (the "Software")
and related product documentation at no charge subject to the terms and
```

○ I accept the terms of the License Agreement

● I do NOT accept the terms of the License Agreement

3. Scroll down through the license agreement page. The **I accept the terms of the License Agreement** option is enabled.

4. Select the **I accept the terms of the License Agreement** option, and then click **Next**. The Install Folder appears.

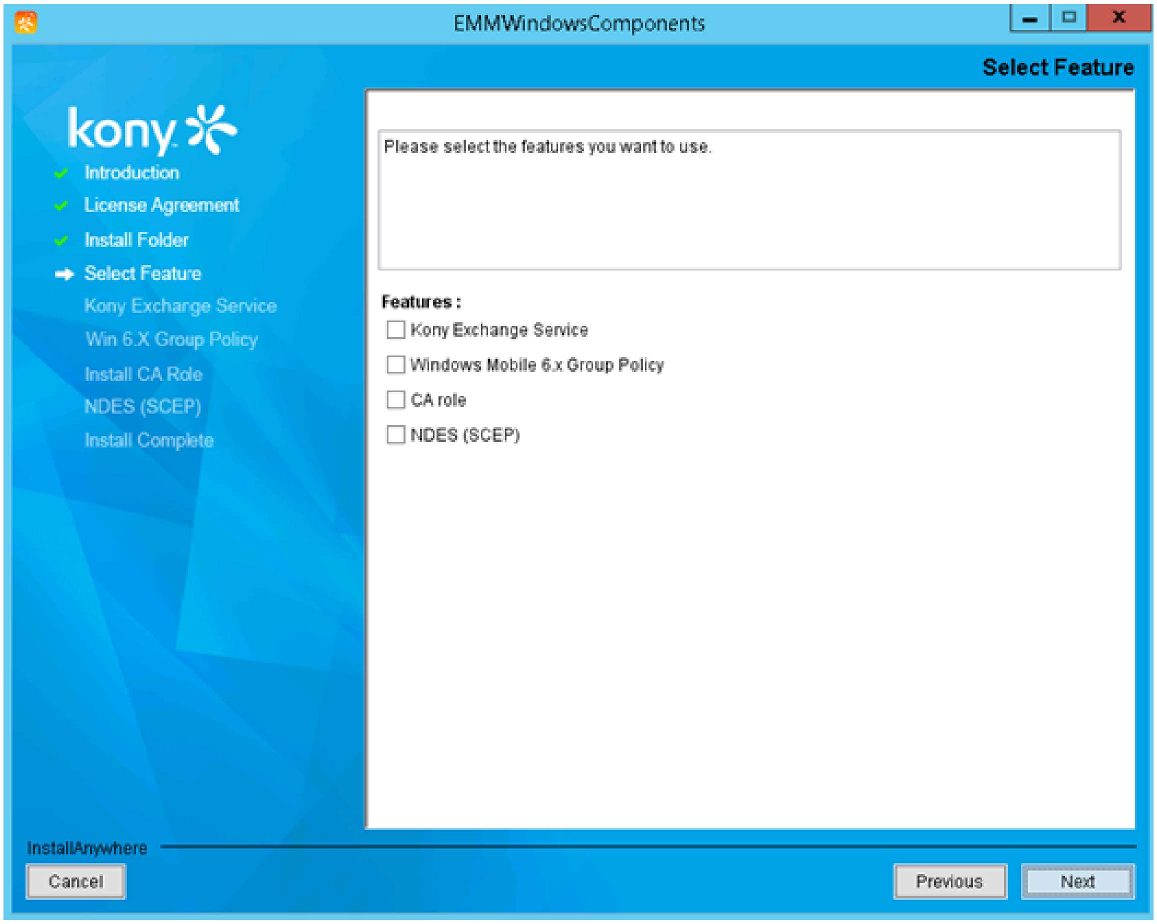


Please choose a destination folder for this installation.

Where would you like to install?

C:\EMMWindowsComponents

5. If you want to install EMM components in any specific folder, click **Choose**, and select the folder. Otherwise, leave the default options, and click **Next**. The Select Feature page appears.



Please select the features you want to use.

Features :

□ Kony Exchange Service

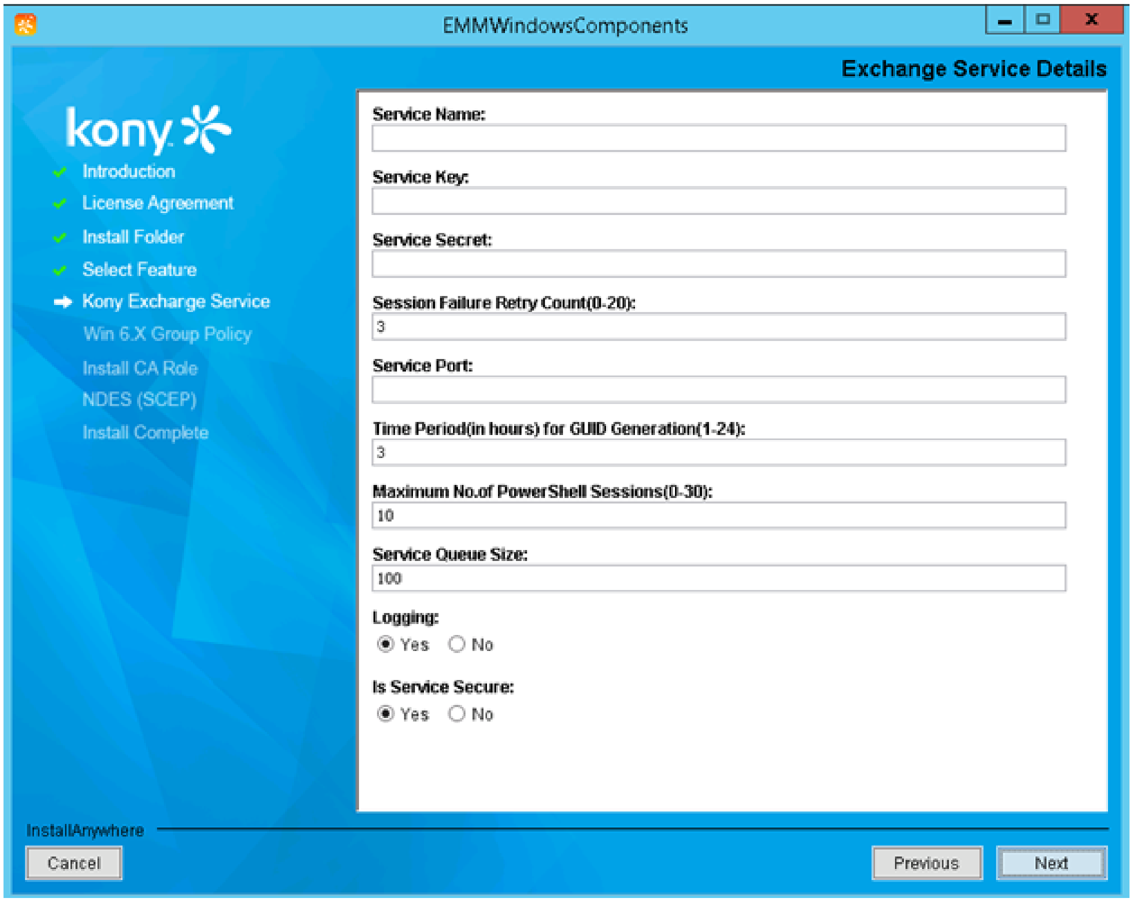
□ Windows Mobile 6.x Group Policy

□ CA role

□ NDES (SCEP)

6. Select all features, and then click **Next**. The Exchange Service Details page appears.

> ***Note:*** To allow communication between the Windows Server 2008/2012 and your corporate email exchange server (to enable block and unblock email access on enrolled devices), Kony Exchange service should be configured. Using this service, you can also restrict email clients that can be used on enrolled devices.



Exchange Service Details

Service Name:

Service Key:

Service Secret:

Session Failure Retry Count(0-20): 3

Service Port:

Time Period(in hours) for GUID Generation(1-24): 3

Maximum No.of PowerShell Sessions(0-30): 10

Service Queue Size: 100

Logging: ● Yes ○ No

Is Service Secure: ● Yes ○ No

7. Enter the following details:

   1. **Service Name**: Enter the exchange service name.

   2. **Service Key**: Enter the exchange service key.

   3. **Service Secret**: Enter the exchange service secret.

   4. **Session Failure Retry Count (0-20)**: Enter the number of times the session should retry after session failure.

   5. **Service Port**: Enter service port details.

   6. **Time Period (in hours) for GUID Generation (1-24)**: Enter the time period for the GUID

generation.

7. **Maximum No. of PowerShell Sessions (0-30)**: Enter the maximum number of poweshell sessions allowed.

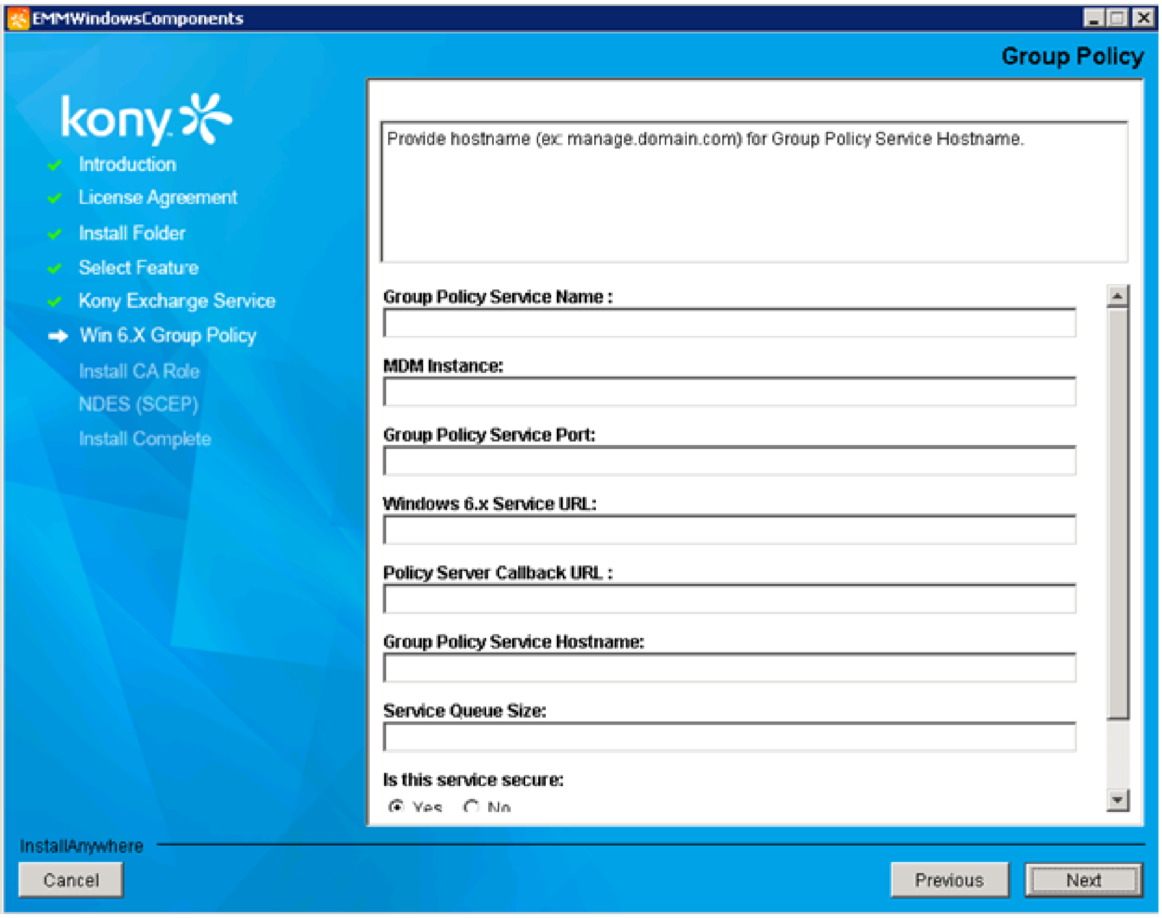
8. **Service Queue Size**: Enter the size of allowed queue service.

9. **Logging**: Select **Yes** if logging is required.

10. **Is Service Secure**: Select **Yes**, if the service is secure.

8. Click **Next**. The Group Policy Page appears.

> ***Note:*** As mentioned in http://technet.microsoft.com/en-us/library/dd261866.aspx, a machine that supports GPMC must be in the domain in which SCMDM 2008 server is installed.
> To support Windows Mobile 6.x devices on EMM, the Group Policy service must be installed on the machine that supports group policy management. This machine should be accessible to the SCMDM 2008 machine. It need not have a public IP and can remain within the corporate domain.



Provide hostname (ex: manage.domain.com) for Group Policy Service Hostname.

Group Policy Service Name :

MDM Instance:

Group Policy Service Port:

Windows 6.x Service URL:

Policy Server Callback URL :

Group Policy Service Hostname:

Service Queue Size:

Is this service secure:

● Yes ○ No

9. Complete these fields:

   1. **Group Policy Service Name**: Enter the group policy service name.
   2. **MDM Instance**: Enter details of the MDM instance.
   3. **Group Policy Service Port**: Enter the group policy service port details.
   4. **Windows 6.x Service URL**: Enter the Windows 6.x service URL details.
   5. **Policy Server Callback URL**: Enter the policy server callback URL details.
   6. **Group Policy Service Hostname**: Enter the group policy service hostname details.
   7. **Service Queue Size**: Enter the size of allowed queue service.

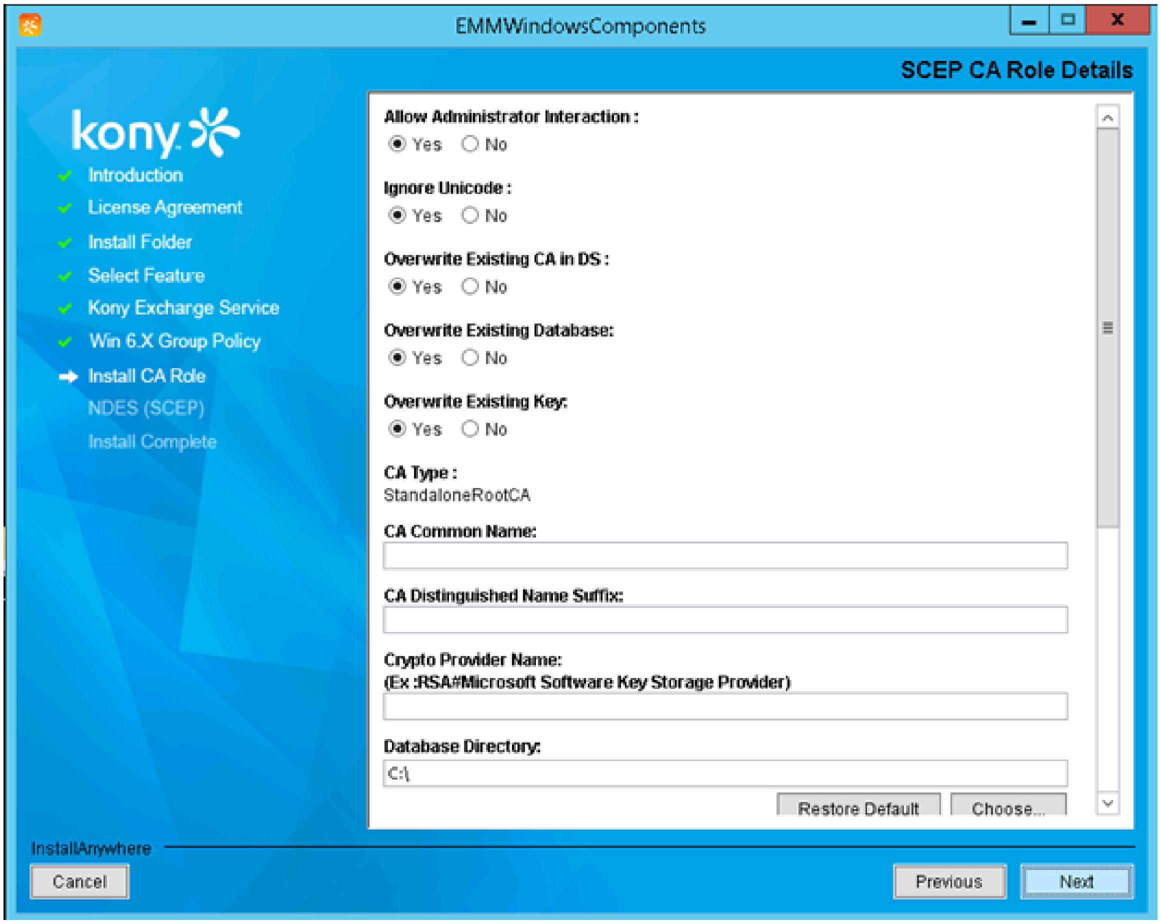
8. **Is This Service Secure**: Select **Yes** if the service is secure.

   > *Note:* If the service is secure (https), select Yes. Select No if the service is not secure (http).

9. **Logging**: Select **Yes** if logging is required.

10. After entering all the details in the Group Policy page, click **Next**. The SCEP CA Role Details Page appears.

    > *Note:* To enable EMM to support iOS devices, certificate distribution through, Simple Certificate Enrollment Protocol (SCEP) Server is mandatory.This must be done before the EMM installation begins. A certificate authority (CA) must also be set to sign certificates distributed by the SCEP Server.



SCEP CA Role Details

Allow Administrator Interaction :
● Yes ○ No

Ignore Unicode :
● Yes ○ No

Overwrite Existing CA in DS :
● Yes ○ No

Overwrite Existing Database:
● Yes ○ No

Overwrite Existing Key:
● Yes ○ No

CA Type :
StandaloneRootCA

CA Common Name:

CA Distinguished Name Suffix:

Crypto Provider Name:
(Ex :RSA#Microsoft Software Key Storage Provider)

Database Directory:
C:\

11. Enter the following details:

    1. **Allow Administrator Interaction**: Select **Yes** to allow administrator interaction.
    2. **Ignore Unicode**: Select **Yes** to ignore unicode.
    3. **Overwrite Existing CA in DS**: Select **Yes** to overwrite existing CA in DS.
    4. **Overwrite Existing Database**: Select **Yes** to overwrite the existing database.
    5. **Overwrite Existing Key**: Select **Yes** to overwrite the existing key.
    6. **CA Type**: Details of the CA type appear.
    7. **CA Common Name:** Enter the CA common name.

    8. **CA Distinguished Name Suffix**: Enter the distinguished name suffix of the CA.

    9. **Crypto Provider Name**: Enter the name of the crypto provider.

    10. **Database Directory**: Select the database directory.
        Ensure that the database directory you provide is not used by any other service. Once the CA role is installed, the directory will be locked by the Active Directory Certificate Services.

    11. **Hash Algorithm Name**: Enter the hash algorithm function name.

    12. **Key Length**: Enter the length of the hash algorithm key.

    13. **Log Directory**: Select the location for the log directory.
        Ensure that the database log directory you provide is not used by any other service. Once the CA role is installed, the directory will be locked by the Active Directory Certificate Services.

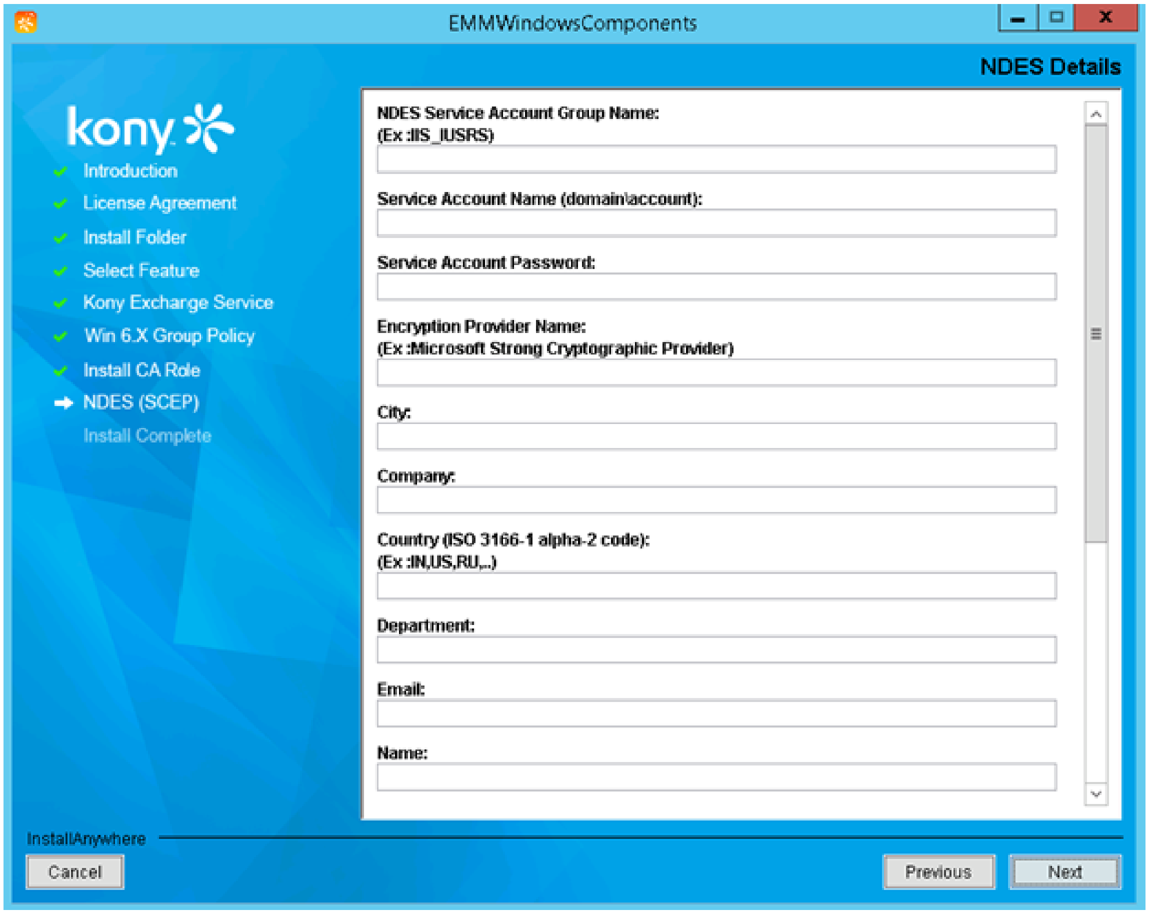
    14. **Validity Period Units**: Select the validity period unit of the CA. Options are **Years**, **Months**, **Weeks**, and **Days**.

    15. **Validity Period**: Enter the validity period of the CA.

    16. **Username**: Enter your username for your CA type provider account.

    17. **Password**: Enter your password for your CA type provider account.

12. Once you have entered all the details in the SCEP CA Role Details Page, click **Next**. The NDES Details page appears.



NDES Service Account Group Name:
(Ex :IIS_IUSRS)

Service Account Name (domain\account):

Service Account Password:

Encryption Provider Name:
(Ex :Microsoft Strong Cryptographic Provider)

City:

Company:

Country (ISO 3166-1 alpha-2 code):
(Ex :IN,US,RU,..)

Department:

Email:

Name:

13. Enter the following details:

    1. **NDES Service Account Group Name**: Enter the NDES service account group name.

    2. **Service Account Name (domain/account)**: Enter the service account name.

       > ***Note:*** In case the server is a standalone computer, enter the computer name.

    3. **Service Account Password**: Enter your NDES service account password.

    4. **Encryption Provider Name**: Enter your NDES encryption provider name.

    5. **City**: Enter your city.

6. **Country (ISO 3166-1 alpha-2-code)**: Enter your country.
7. **Department**: Enter your department details.
8. **Email**: Enter your email address.
9. **Name**: Enter your name.
10. **State**: Enter the state name.
11. **Signing Provider Name**: Enter the signing provider name.
12. **Maximum Numbr of Passwords to Cache**: Enter the maximum number of issued passwords to be stored in the password cache.
13. **Log in Username**: Enter your log in username.
14. **Log in User Password**: Enter your log in password.
15. **Encryption Key Length**: Enter the length of the encryption key.
16. **Signing Key Length**: Enter the length of the signing key.

14. After entering all the details in the NDES Details page, click **Next**. The Pre-Installation Summary page appears.

15. Click **Install**. The Install Complete page appears.

> *Note:* All components are installed one by one. You might see several notifications before the final install complete page.

> *Note:* If a Status confirmation page appears, click Yes to open the SCEP URL in a browser.

16. Click **Done**.

7.3 Windows App Wrapping

7.3.1 Software Requirements

Component	Version
Visual Studio	Visual studio 2013 express edition with update 3 (Prerequisite for Windows app wrapping)
Microsoft Silverlight Runtime	Microsoft Silverlight Runtime 5.0 (Prerequisite for Windows app wrapping)
Microsoft Silverlight	Microsoft Silverlight SDK 5.0 (Prerequisite for Windows app wrapping)
Cygwin	Latest Cygwin (32 bit) version. (Prerequisite for Windows app wrapping)

7.4 How to Install Visual Studio

Windows Phone Enterprise apps must be signed for app management and app wrapping. You must install Visual Studio to manage Windows phone app wrapping.

See the Visual Studio website for more information on how to install and configure Visual Studio.

7.5 How to Install Microsoft Silverlight Runtime

To manage enterprise apps, you need the Windows phone app wrapping feature to function. You must install Microsoft Silverlight Runtime to manage Windows phone app wrapping.

See the Microsoft Silverlight Runtime website for more information on how to install Microsoft Silverlight Runtime.

7.6 How to Install Microsoft Silverlight SDK

To manage enterprise apps, you need Windows phone app wrapping feature to function. You must install Microsoft Silverlight SDK to manage Windows phone app wrapping.

See the Microsoft Silverlight SDK website for more information on how to install and configure Microsoft Silverlight SDK.

7.7 How to Install Cygwin

Cygwin is a large collection of GNU and Open Source tools that provide features similar to a Linux distribution on Windows. To manage Windows phone app wrapping, install Cygwin. With Cygwin, user binaries are copied to the Windows machine. To manage enterprise apps, you need Windows phone app wrapping feature to function.

> ***Important:*** You should be familiar with Linux commands to work with Cygwin.

See the Cygwin website for more information on how to install and setup Cygwin.

> ***Important:*** You must install Cygwin along with openSSH, openSSL, Dos2Unix, Winzip, Unzip, and Curl components.

7.7.1 How to Configure Cygwin Properties

To configure Cygwin for enterprise application wrapping based on your system settings, follow these steps:

1. Right click on **Computer**, and select **Properties**. The system window appears.
2. Select the **Advanced System Settings** link from the **Control Panel Home** pane. The **System Properties** window appears.
3. Select **Environment Variables**.
4. In the **Environment Variables** window, go to **User Variables** and select **New**.
    i. Enter **CYGWIN_HOME** in the Variable Name field.
    ii. Enter `C:\cygwin64\bin` in the Variable Value field.

iii. Click **OK**.

5. Select **Path** from **User Variables** and click **Edit**.
   1. Add `C:\cygwin64\bin` in the Variable Value field.
   2. Click **OK**.

> ***Important:*** For Windows wrapping, directory path should be less than 260 characters. If the path is more than 260 characters, the signing process will fail during application wrapping

7.7.2 How to Configure SSH Server

To configure the SSH server, follow these steps:

1. Navigate to your Cygwin installation folder (for example, c/cygwin).
2. Select **Cygwin.bat**, right click, and select **Run as administrator**. The Command prompt appears.
3. In the command prompt, type `ssh-host-config`, and press enter. An alert `Should StrictModes be used? (yes/no)` appears.
4. Type `Yes` and press enter. An alert `Should privilege separation be used? (yes/no)` appears.
5. Type `Yes` and press enter. An alert `you want to install sshd as a service. (yes/no)` appears.
6. Type `Yes` and press enter. The system prompt `Enter the value of CYGWIN for the daemon: []` appears.
7. Type `ntsec tty` and press enter. An alert `Do you want to use a different name? (yes/no)` appears.

8. Type `No` and press enter. The system prompt `Please enter the password for user <username>)` appears.

9. Type the password and press enter.The `Reenter:` prompt appears.

10. Type the password again and press enter. A confirmation message on SSHD configuration appears.

11. Execute the following commands:

    - `chmod +r /etc/passwd`: Provides read permissions to password file.
    - `chmod u+w /etc/passwd`: Provides write permissions to user.
    - `chmod +r /etc/group`: Provides read permissions to a group file.
    - `chmod u+w /etc/group`: Provides write permissions to user.
    - `chmod 755 /var`: Provides all permissions to var folder.
    - `touch /var/log/sshd.log`: Creates a new empty file sshd.log.
    - `chmod 644 /var/log/sshd.log`: Owner can write and other users can only read the log file.
    - `chown system /etc/ssh*`: Changes owner for ssh* files to system.
    - `chown system /var/empty`: Changes owner for /car/empty folder to system.
    - `mkgroup -l > ..\etc\empty`: This will print /etc/group file to /etc/empty file.
    - `mkpasswd -l > ..\etc\passwd`: This will print /etc/passwd file to /etc/passwd.
    - `chmod a+x /etc/sshd_config`: This will provide read and write permission to the sshd_config file.

> *Important:* If the openssh you are using is version 6.7, perform the following steps:
>
> Open /etc/sshd_config
> Add the following line towards the end of the file:
> **KexAlgorithms diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1**

12. To start SSHD, open command prompt and enter `net start sshd`. The SSHD service will start successfully.

13. To change passwords, in the command prompt, enter `passwd <username>`.

14. To verify test connection, open an ssh client tool, enter localhost in connection type text box, and click open. The SSH terminal opens, and a success message appears.

8. Apple Server for App Wrapping

8.1 Software Requirements

Component	Version
Mac OS	OS X Version: Yosemite (10.10)
Xcode	XCODE Version: 6.1 (6A1052d)
Dos2Unix	5.3.3

> ***Note:*** If you upgraded Xcode, open Xcode at least once after the upgrade to install all dependent components. Install iOS simulator 7.1 if you have not installed it previously.

> ***Important:*** If you are on older version of the MAC OS and Xcode than the one mentioned in the software requirements, please update them, For more information on how to update, see Mac OS X Upgrade and Xcode Upgrade for more information.

8.2 Install Xcode and iOS Simulators

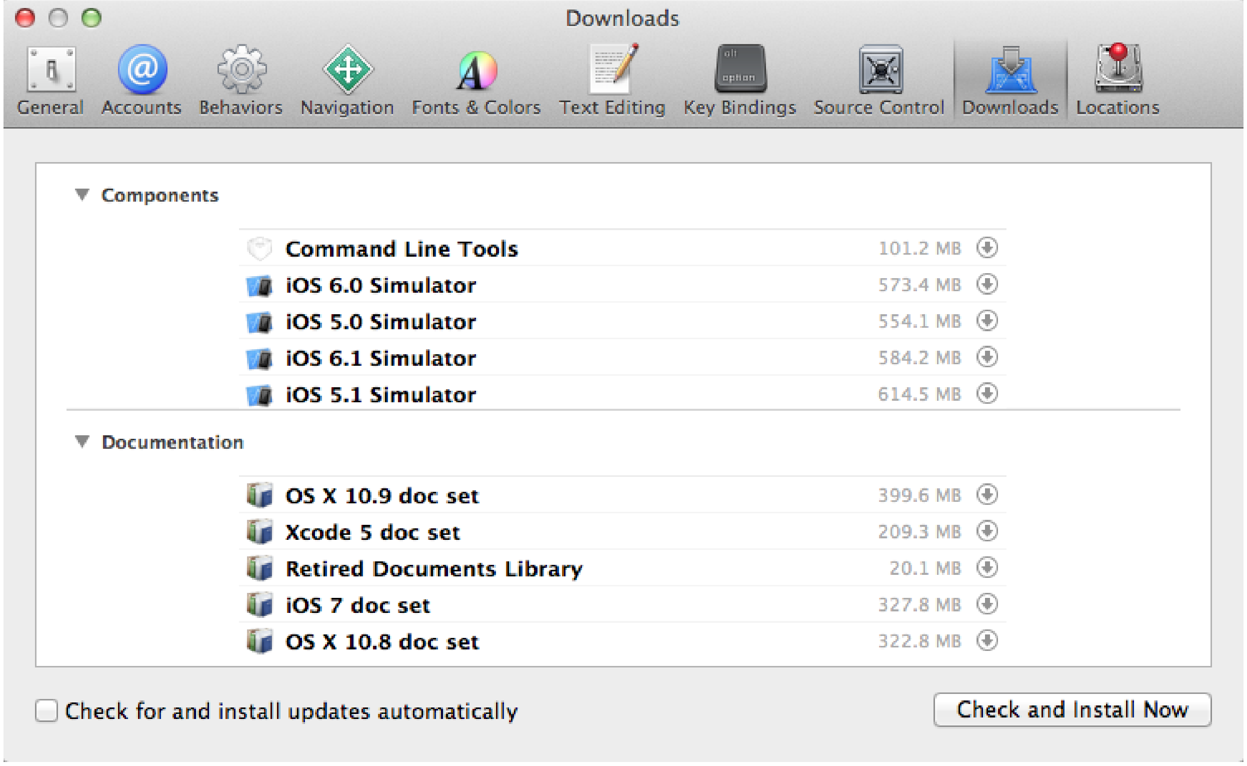
On the Apple Server, install Xcode command line tools and iOS simulators. Xcode provides an interface for downloading and installing the latest command line tools, such as Apple LLVM compiler and system headers.

1. Install Xcode
   - Navigate to App Store, search for **Xcode** and install it.

2. Install the iOS simulators

    1. In Xcode navigate to **Preferences** menu > **Downloads** tab > **Components** tab

    2. Click **Install** next to the version 5.x and higher simulators.



▼ Components

Command Line Tools	101.2 MB
iOS 6.0 Simulator	573.4 MB
iOS 5.0 Simulator	554.1 MB
iOS 6.1 Simulator	584.2 MB
iOS 5.1 Simulator	614.5 MB

▼ Documentation

OS X 10.9 doc set	399.6 MB
Xcode 5 doc set	209.3 MB
Retired Documents Library	20.1 MB
iOS 7 doc set	327.8 MB
OS X 10.8 doc set	322.8 MB

□ Check for and install updates automatically

> *Important:* If you have multiple EMM environments (for example, Production environment, QA environment, Development environment), you must have a single MAC user assigned to each one of the environment. For example, Production environment should be mapped to MAC User 1, QA environment should be mapped to MAC User 2 etc. For more information on how to create a MAC user, click here.

> *Important:* After installing EMM instances, each MAC user must manually configure **wrap-ios.zip** file. For more information, click here. You do not need to perform this step if EMM installer has the an appropriate MAC user and the MAC is configured successfully with EMM configuration.

8.3 Active SSH Access for Users after MAC OS Upgrade

Since the Mac OS update removes or modifies the existing “ssh” user access privileges, so it is recommended to update or modify the access once you upgrade the current Mac OS version.

To update or modify the access, run the following commands:

1. Login into the Mac system as a root/admin user.
2. Run the following commands.

   i.
   ```
   sudo dscl . append /Groups/com.apple.access_ssh user <username>
   ```

   ii.
   ```
   sudo dscl . append /Groups/com.apple.access_ssh groupmembers `dscl . read /Users/<username> GeneratedUID | cut -d " " -f 2`
   ```

> ***Note:*** Repeat the same commands for all users that are configured for EMM instances.

> ***Important:*** : Above steps are not applicable for new Mac OS installation with the latest version.

8.4 Installing dos2Unix

To install dos2Unix on your MAC server, do the following:

> ***Important:*** Modify administrator restrictions on your MAC **Allow apps downloaded from** value to **Anywhere** to proceed with the installation. If you do not modify the restriction, dos2unix will not be installed. After you installed the software, you can revert administrator restrictions .

1. Download and install the dos2unix software on MAC. Download link: https://code.google.com/p/rudix/downloads/detail?name=dos2unix-5.3.3-0.pkg

   As installation is done on Mac machines, the files and commands must be compatible with the Unix environment. The dos2unix command ensures that this is done, eliminating any compatibility issues.

9. Certificate Requirements

EMM requires two types of certificates.

- SSL Certificates
- Device Certificates

Device Certificates:Device certificates are required post-installation. You will not be using these certificates in the steps detailed in this document. Further steps on how to use certificates are provided in the Quick Start Guide

9.1 SSL Certificates

SSL certificates are used for secure communication between the device and EMM server. Usually, SSL certificates are installed on Load balancer. SSL certificates must be procured from trusted Certificate Authorities, GoDaddy or VeriSign.

You can configure end to end SSL from device to App server. For SSL communication between Load balancer and Web server, Web server and App server, you can also use self signed SSL certificates.

Load balancer SSL certificates, including private key should be provided to the EMM Server during installation. A check is performed on iOS devices to ensure no tampering has been done.

For iOS devices, EMM server sends payload (enrollment or policy push) along with a message digest. Private key is used to encrypt the message digest creating a digitally signed message digest. This is sent along with the payload to the device.

At the device end, the device in-built MDM agent uses the payload to create the message digest. Using its public key, it decrypts the digitally signed message digest sent by the server and compares these two. If the message digest is not signed with a private key, a Not verified message displays on the device.

1. To procure any SSL certificate, follow these steps (applicable to all SSL vendors):
    i. Generate CSR (Certificate Signing Request).
    ii. Submit CSR to CA (Certificate Authority).
    iii. Get/download a Signed SSL provided by CA.
    iv. Sign the Certificate with private key and other supporting associated ROOT and intermediate certificates.

> ***Note:*** Self Signed Certificates are not supported.

2. You need to procure these certificates from any of the CA vendors, preferably:
    - Verisign - Verisign Secure SSL
    - GoDaddy - GoDaddy Secure SSL

> ***Note:*** We have tested with Verisign or GoDaddy only in DEV/QA and production as these certificates have maximum mobile device compatibility.
>
> These certificates require 600 octal file permission so that the SSL keys can be read.
>
> The server instance that will be installed should have a valid DNS name that matches the common name. SSL should be a trusted certificate issued by a valid certificate authority (as listed above) and it should be compatible on mobile devices.

9.2 Device Certificates

You should create several Device certificates as part of prerequisites for EMM server. You will require these certificates as part of the installation process so it is recommended that you create these certificates and keep them ready.

- iOS Certs
  - Wildcard Distribution Certificate
  - Wildcard Mobile Provisioning Profile
  - Launchpad Push Certificate
  - Launchpad Provisioning Profile
  - Apple Push Certificate for MDM (Not required for SA Mode or MAM Only License)
- Android
  - Keystore certificate
  - GCM Key
  - Google MAPSv2 Key
- Windows Phone 8.1
  - Symantec Enterprise Mobile Code Signing Certificate: You must procure a Symantec Enterprise Mobile Code Signing Certificate which will be used to sign your Windows phone 8.1 enterprise apps. EMM uses this certificate during the wrapping and signing process of your Windows phone 8.1 Enterprise apps.

> ***Note:*** For more information on why you need to procure Symantec Enterprise certificate, and the process of distributing enterprise apps to windows phone, see Microsoft Company app distribution for Windows Phone.

You need to create an Enterprise Apple Account and an enterprise Account for Google (can be same as developer account).

10. Third Party Systems

There are several third-party systems that are required to be in place for a successful installation. The ones given below should ideally be there to use most of the EMM functionality. None of these are mandatory, they are only highly recommended.

10.1 Google Maps API

There are two types of Google Maps APIs namely:

- **Free Google Maps API**: To use Free Google Maps API, you do not require a key.
- **Business Google Maps API**: To use Business Google Maps API, you require a client ID.

These APIs shall be required in case you wish to locate devices or use Geo-fences while applying policies.

10.2 Admin Email Settings

Create an email address for the EMM server communication. The EMM Server sends an email notification based on user activities such as app publishing, un-publishing, and more. For this purpose, a new email address or email group (for example, EMMadmin@company.com) should be created.

10.3 Active Directory Integration

Active Directory integration is achieved using an LDAP(S) connector. AD is configured post EMM installation. Obtain your enterprise Domain Controller Host Name or IP address, domain name, port, and context information prior to installation.

Ensure that the below attributes are configured in your AD before importing any Groups or Users to EMM. If these attributes are not present in your AD, Users and Groups import will fail.

- ADS_COMMON_NAME="**cn**";
- ADS_NAME="**name**";

- ADS_EMAIL="**mail**";
- ADS_MOBILE="**telephoneNumber**";
- ADS_GROUP_MAPPED_ID="**sAMAccountName**";
- ADS_USER_MAPPED_ID="**userPrincipalName**";
- ADS_MEMBER_OF="**memberOf**";
- ADS_FIRST_NAME="**givenName**";
- ADS_LAST_NAME="**sn**";
- ADS_DESCRIPTION="**description**";
- ADS_DISPLAY_NAME = "**displayName**";
- ADS_OBJECT_CLASS = " **objectClass**";
- ADS_USER_OBJECT_CATEGORY = "**objectCategory**"

10.4 Package Family Name (PFN) for Windows Notification Service (WNS)

Package Family Name (PFN) for Windows Notification Service (WNS)

Package Family Name (PFN) enables you to sync windows devices with EMM to apply policies and issue commands to devices on demand. If you do not use PFN, devices interact with EMM Server on scheduled sync intervals.

For PFN to work, you should have a Windows Store developer account, and must submit an app to the store. Note that registering an app name is valid only for an year and you must renew it every year.

Once you have a Package Name, you must associate it in Visual studio with your enterprise app store and app. Further steps on how to create and use PFN are provided in the Quick Start Guide.

11. Windows Mobile 6.x - MS System Center 2008

These items are needed only if managing Windows Mobile 6.x - MS System Center 2008 server if supporting WM 6.x

- Learn more about SCMDM 2008 Installation System Requirements.
- Ensure that all the machines (MDM 2008 Server machine, Group Policy machine, Cert. Authority Machine) are part of the domain in which the Kony MDM solution is installed. Procure the Administrator credentials of the domain.
- Follow instructions to install MDM 2008 Server through the following links:
    i. System Center Mobile Device Manager 2008 - Install Guide (No Gateway) - Part 1

    ii. System Center Mobile Device Manager 2008 - Install Guide (No Gateway) - Part 2

    iii. System Center Mobile Device Manager 2008 - Install Guide (No Gateway) - Part 3
- Enable PowerShell scripts to run on MDM 2008 Server machine and Group policy machine.

For more information, refer Windows Mobile 6.x .

12. Installing Kony EMM for Windows

The user interface for Kony EMM Installer displays information to a user, and prompts a user for information needed to install and configure EMM on the system. Kony EMM Installer user interface also displays information about the progress of system changes as they are installed.This section explains the installation on the Windows platform. You can upgrade Kony EMM on your system after installation.

- EMM - New Installation
- EMM - Upgrade Installation
- EMM Installation - Enabling High Availability

12.1 EMM - New Installation

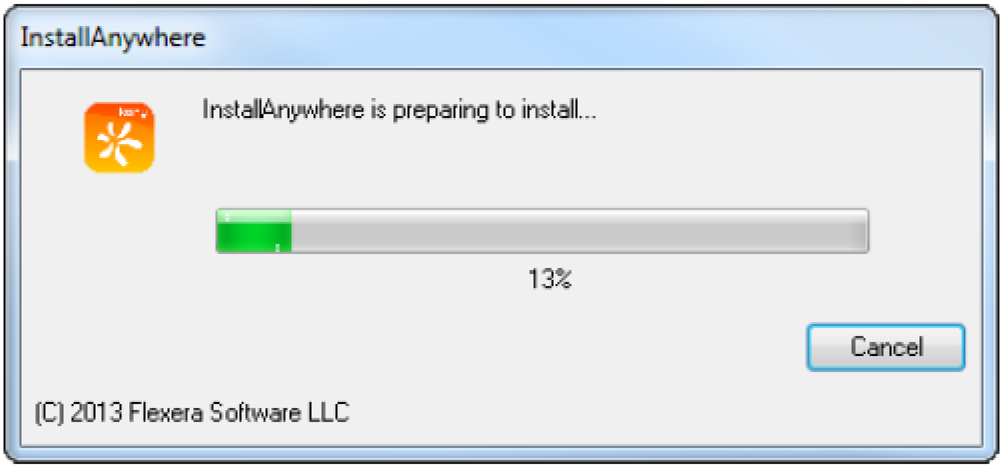
To install Kony EMM for Windows, follow these steps:

1. Click `KonyEMM.exe` file as an administrator.

> ***Note:*** Ensure that firewall and antivirus software allows the `KonyEMM.exe` file to launch.

> ***Note:*** If you are unable to open the `.exe. file`, then follow the instructions given below:
> Start `KonyEMM-X.X.X.X_GA.exe LAX_VM "<Java installed folder>\jre7\bin\java.exe"` from the command prompt.

The **InstallAnywhere** dialog appears. **InstallAnywhere** extracts the installer resources.

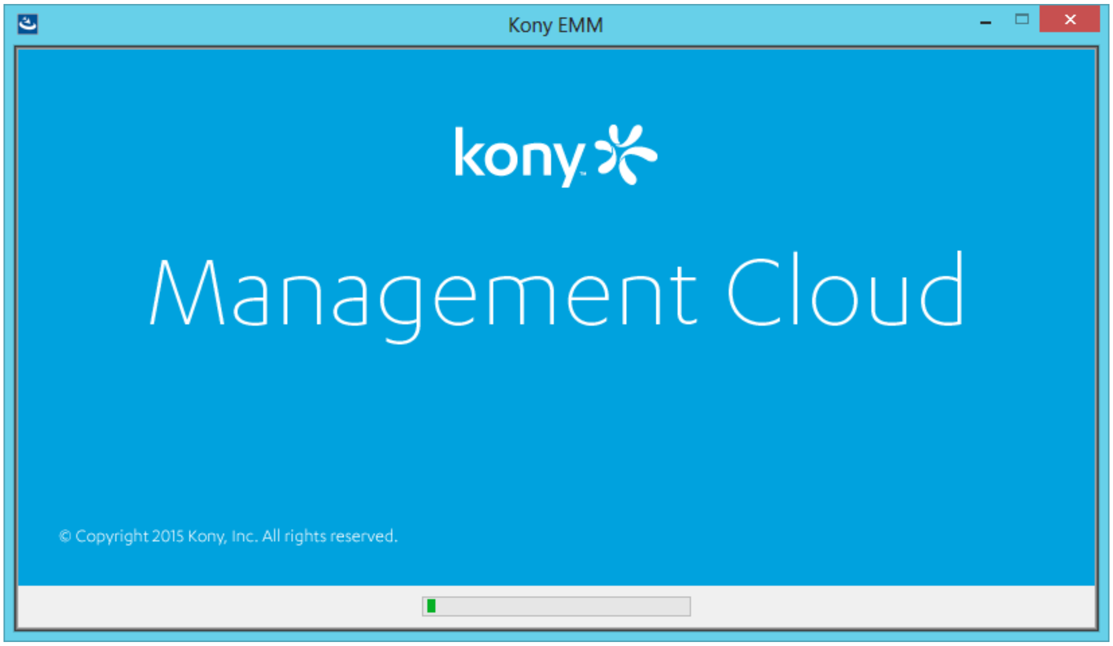

InstallAnywhere

InstallAnywhere is preparing to install...

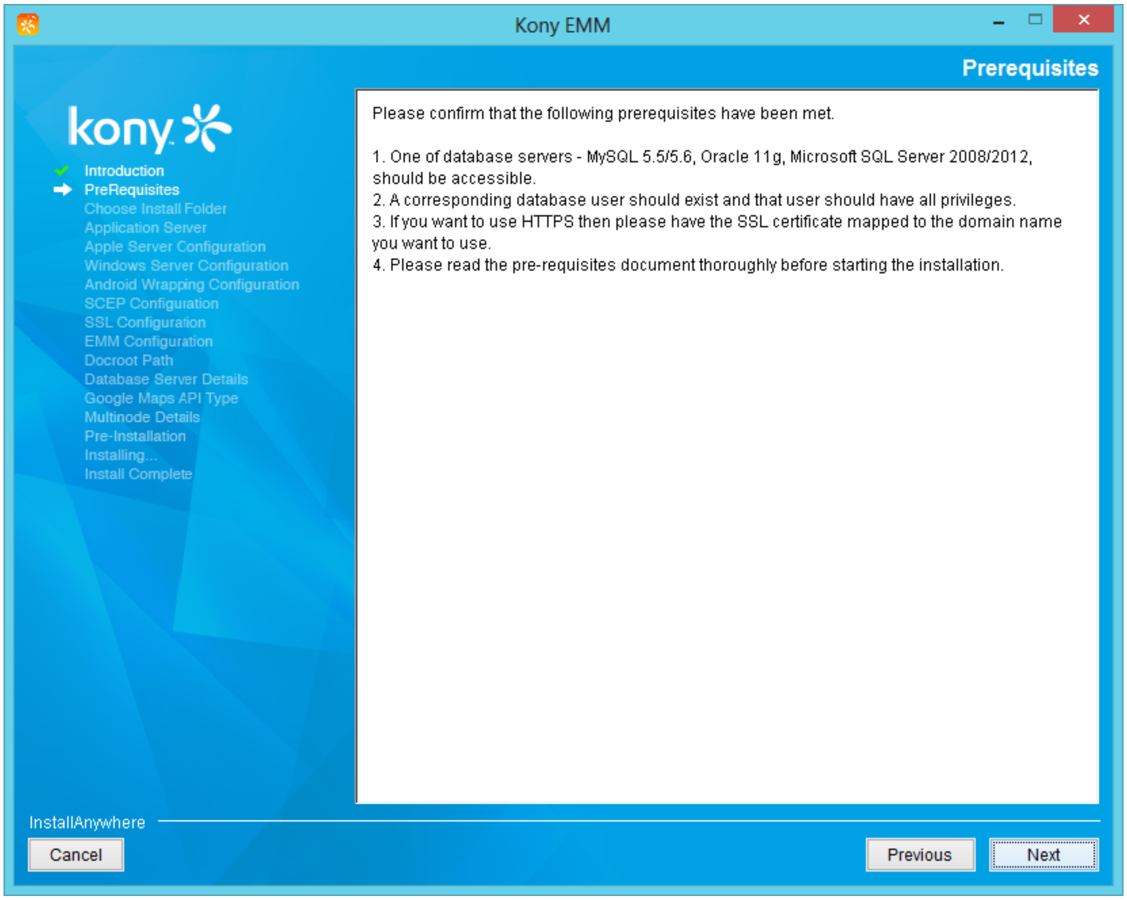
13%

(C) 2013 Flexera Software LLC

A dialog with the Kony logo appears.



2. Read the instructions carefully before installing Kony EMM.



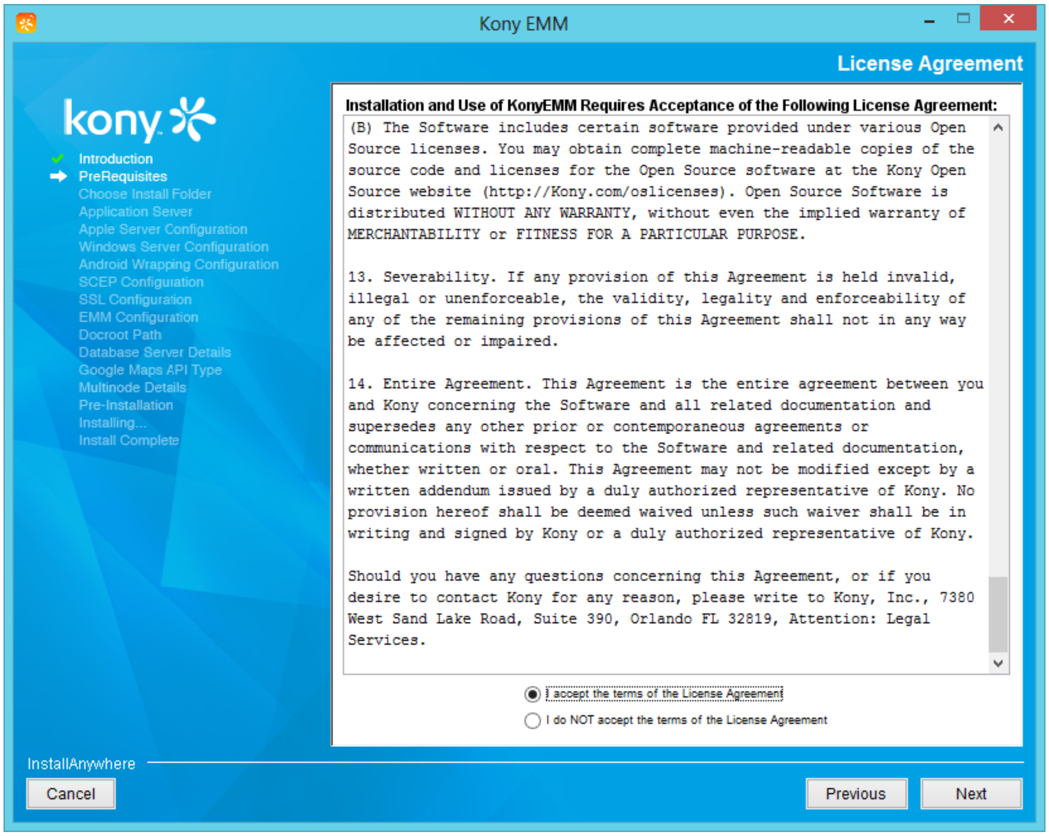
Please confirm that the following prerequisites have been met.

1. One of database servers - MySQL 5.5/5.6, Oracle 11g, Microsoft SQL Server 2008/2012, should be accessible.
2. A corresponding database user should exist and that user should have all privileges.
3. If you want to use HTTPS then please have the SSL certificate mapped to the domain name you want to use.
4. Please read the pre-requisites document thoroughly before starting the installation.

3. Click **Next** to continue.

   The **License Agreement** window appears.

4. Select the **"I accept the terms of the License Agreement"** option after carefully reading the text.



Installation and Use of KonyEMM Requires Acceptance of the Following License Agreement:

```
(B) The Software includes certain software provided under various Open
Source licenses. You may obtain complete machine-readable copies of the
source code and licenses for the Open Source software at the Kony Open
Source website (http://Kony.com/oslicenses). Open Source Software is
distributed WITHOUT ANY WARRANTY, without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

13. Severability. If any provision of this Agreement is held invalid,
illegal or unenforceable, the validity, legality and enforceability of
any of the remaining provisions of this Agreement shall not in any way
be affected or impaired.

14. Entire Agreement. This Agreement is the entire agreement between you
and Kony concerning the Software and all related documentation and
supersedes any other prior or contemporaneous agreements or
communications with respect to the Software and related documentation,
whether written or oral. This Agreement may not be modified except by a
written addendum issued by a duly authorized representative of Kony. No
provision hereof shall be deemed waived unless such waiver shall be in
writing and signed by Kony or a duly authorized representative of Kony.

Should you have any questions concerning this Agreement, or if you
desire to contact Kony for any reason, please write to Kony, Inc., 7380
West Sand Lake Road, Suite 390, Orlando FL 32819, Attention: Legal
Services.
```

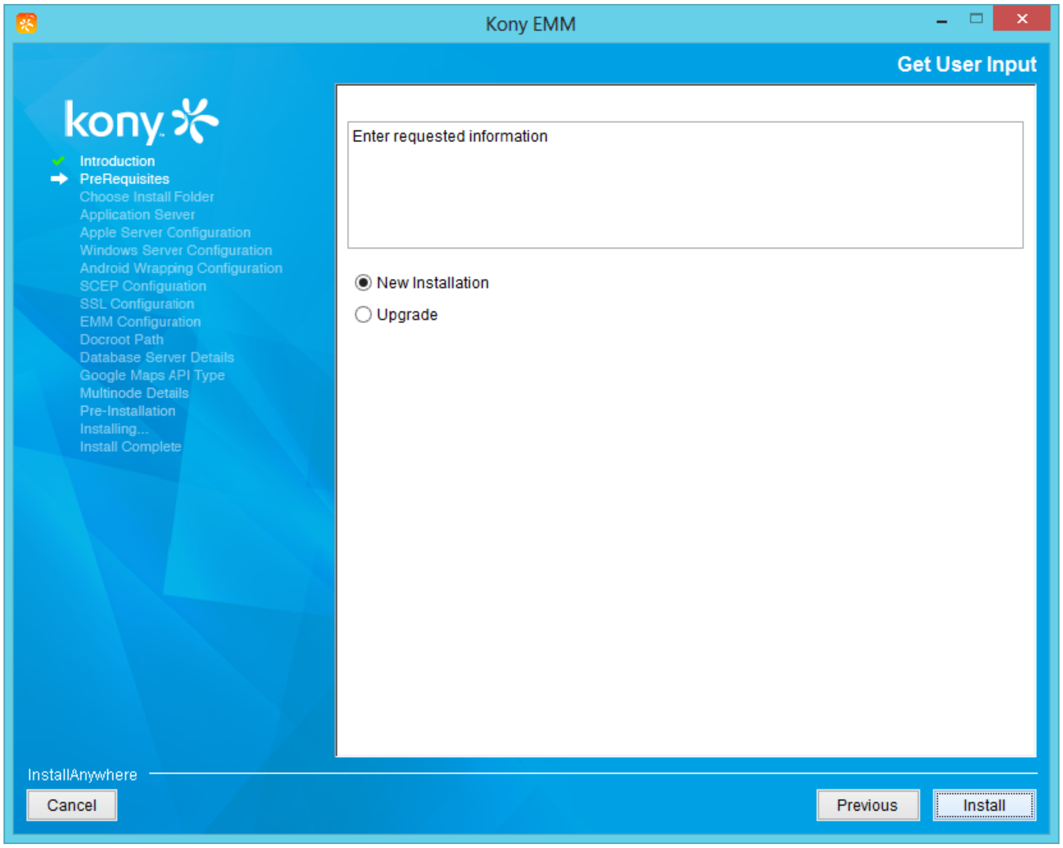
● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

5. Click **Next** to continue.

   The **Get User Input** window appears.

6. Select the installation option. By default, it is set to **New Installation**.

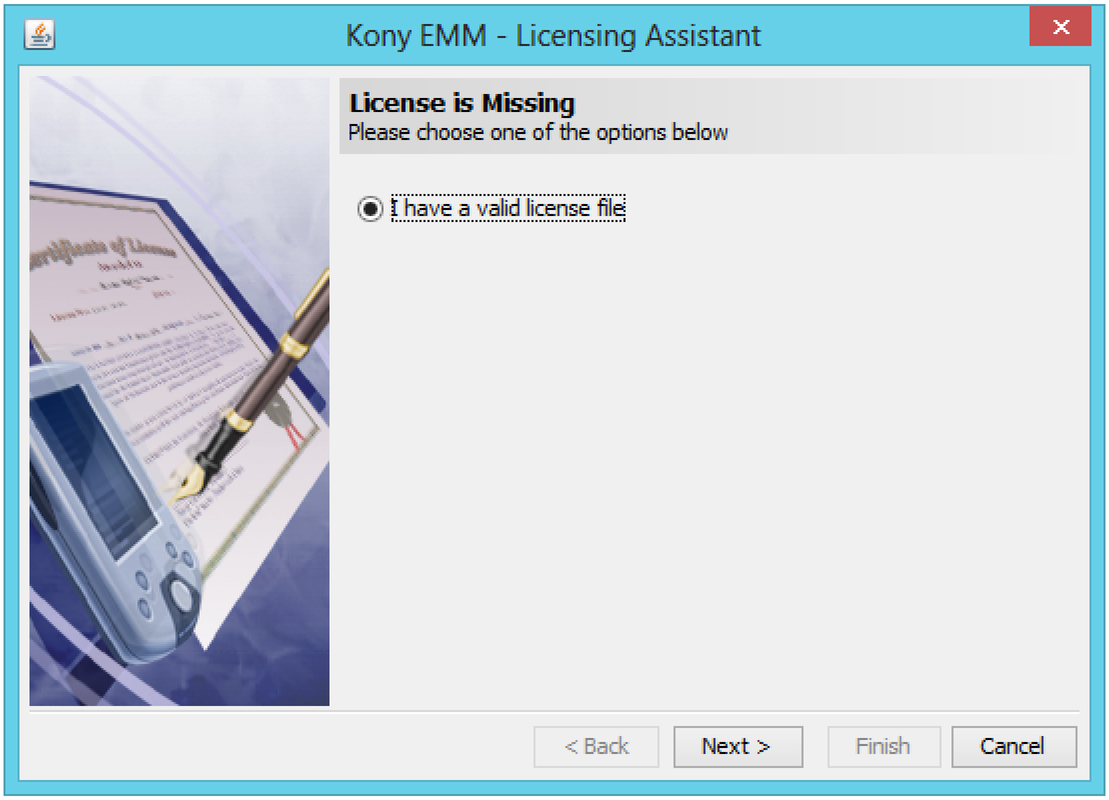


Enter requested information

● New Installation
○ Upgrade

7. Click **Next** to continue. The **Please Wait** window appears.

   The **Kony EMM-Licensing Assistant** window then appears.


Kony EMM - Licensing Assistant

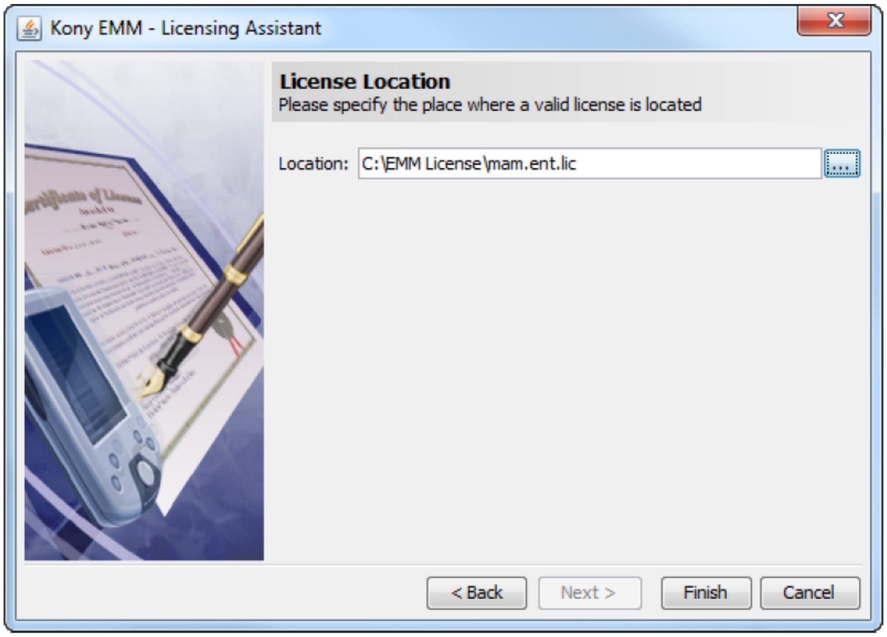
License is Missing
Please choose one of the options below

● I have a valid license file

> ***Note:*** If you use a MAM Only or Store Only license, then you cannot use the SCEP services.

8. Click **Next** to continue.

   The **Kony EMM-Licensing Assistant** window displays the Location search field.


Kony EMM - Licensing Assistant

License Location
Please specify the place where a valid license is located

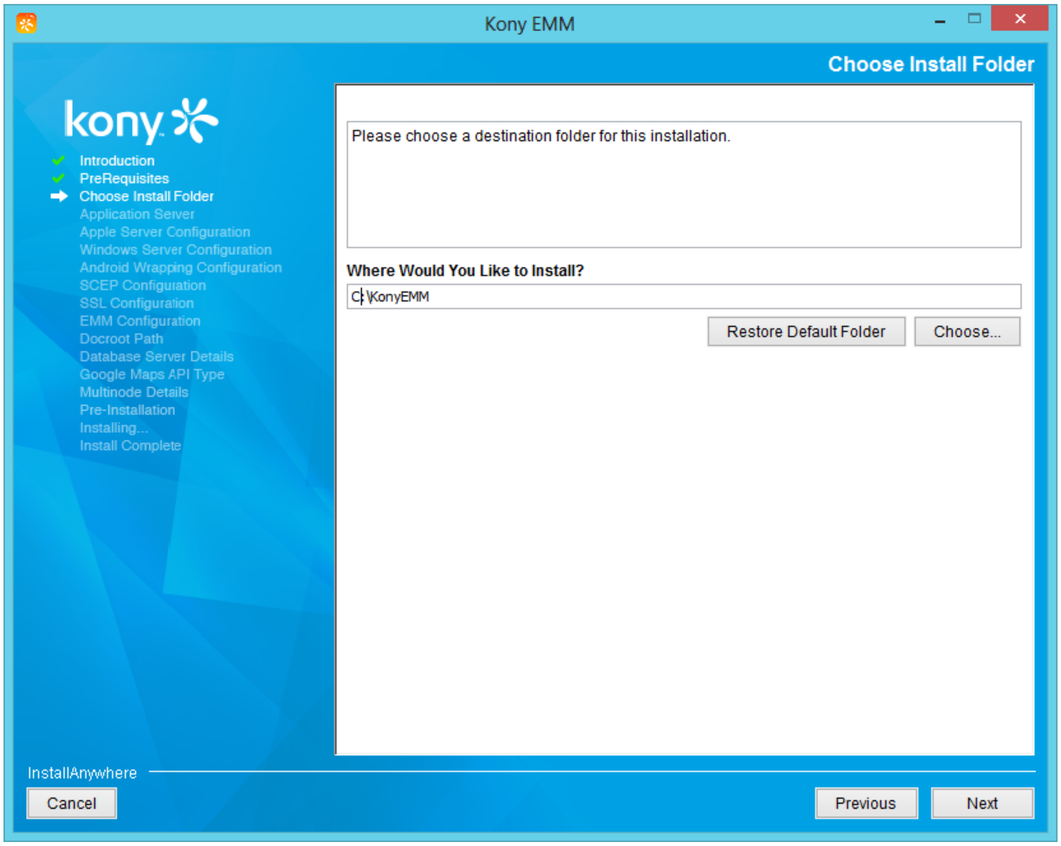
Location: C:\EMM License\mam.ent.lic

9. Click **Browse**, select the license location, and click **Finish**.

   The **Please Wait** window appears and informs a user that Kony EMM configuration is in progress.

   > *Note:* Kony EMM runs only with a valid license, which you must supply. The License File activates the installation, identifying which products you can run.Store the license file in an accessible location, such as in the default Downloads folder on your computer.

10. Click **Choose** to browse the required folder from your system.



Please choose a destination folder for this installation.

Where Would You Like to Install?

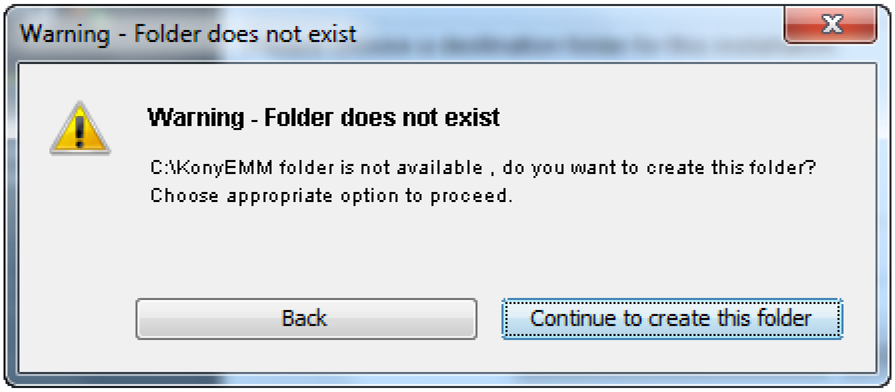
C:\KonyEMM

> ***Note:*** Do not use spaces in the Install Folder name. If you use spaces, then the system displays an error message that the installation path is invalid.

> ***Note:*** By default, the install location is in the C drive. However, a non-OS installed partition is recommended.

11. If the selected folder is not available, then the warning message - **Folder does not exist** appears. The alert also asks if you want to create the folder.

12. Click **Continue to create this folder**.



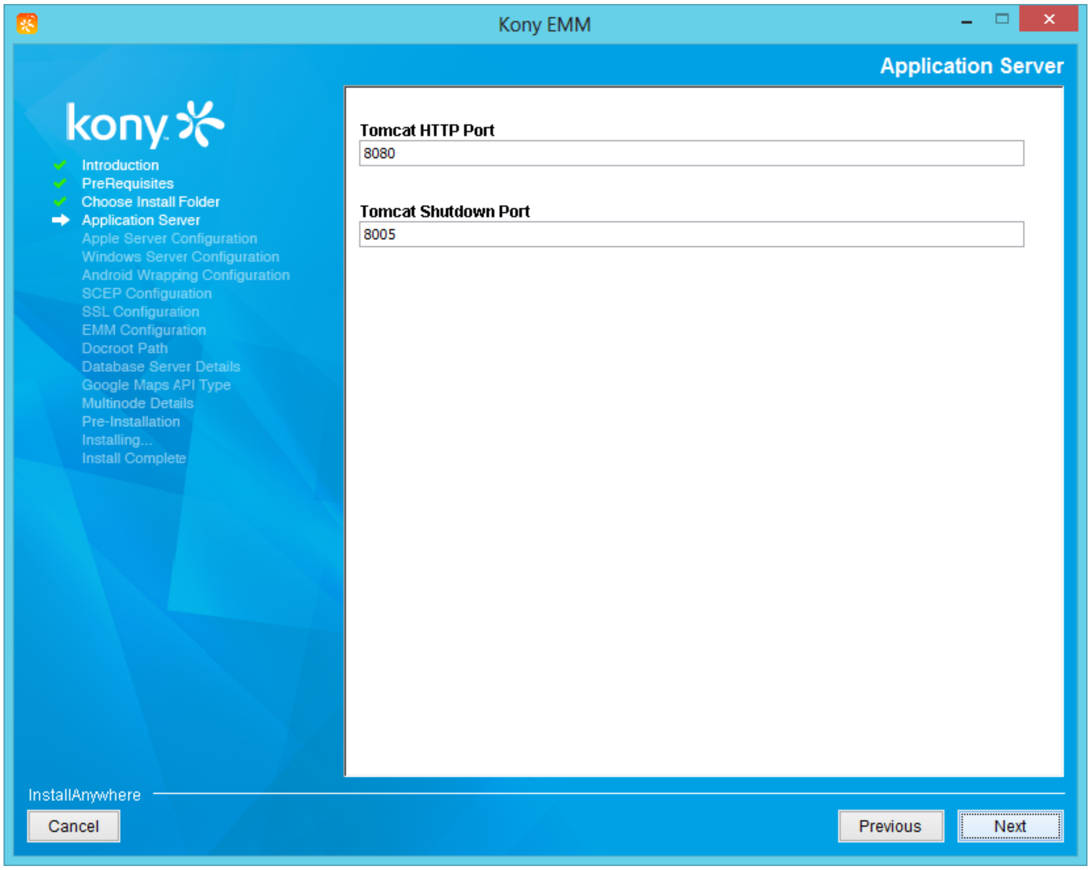
Warning - Folder does not exist

C:\KonyEMM folder is not available , do you want to create this folder?
Choose appropriate option to proceed.

Warning - Folder does not exist
Back
Continue to create this folder

13. Click **Next** to continue.

The **Application Server** window with default **Tomcat HTTP Port** number and default **Tomcat Shutdown Port** number appears.



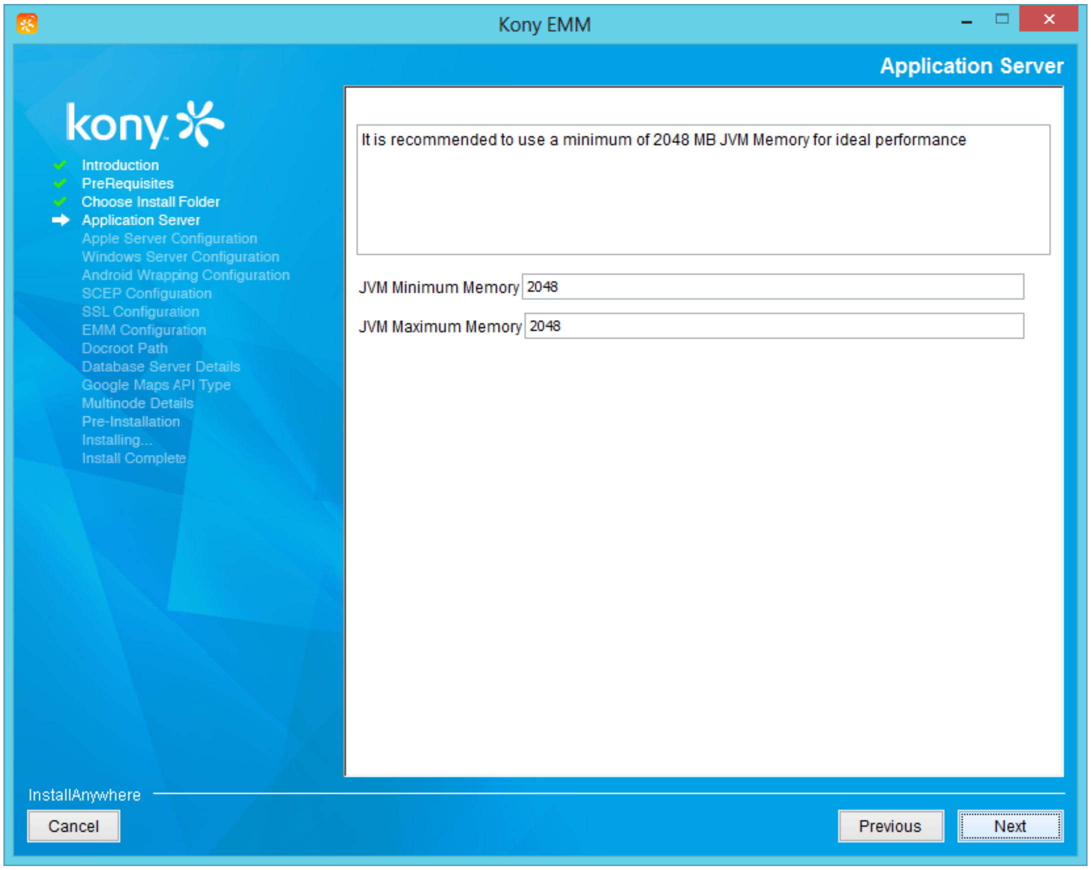
Tomcat HTTP Port: 8080

Tomcat Shutdown Port: 8005

> *Note:* A user can define customer, specific valid ports. Ensure that Tomcat HTTP Port and Tomcat Shutdown Port are different and not in use.

14. Click **Next** to continue.

The Application Server window displays **JVM Maximum Memory** and **JVM Minimum Memory** fields.



It is recommended to use a minimum of 2048 MB JVM Memory for ideal performance

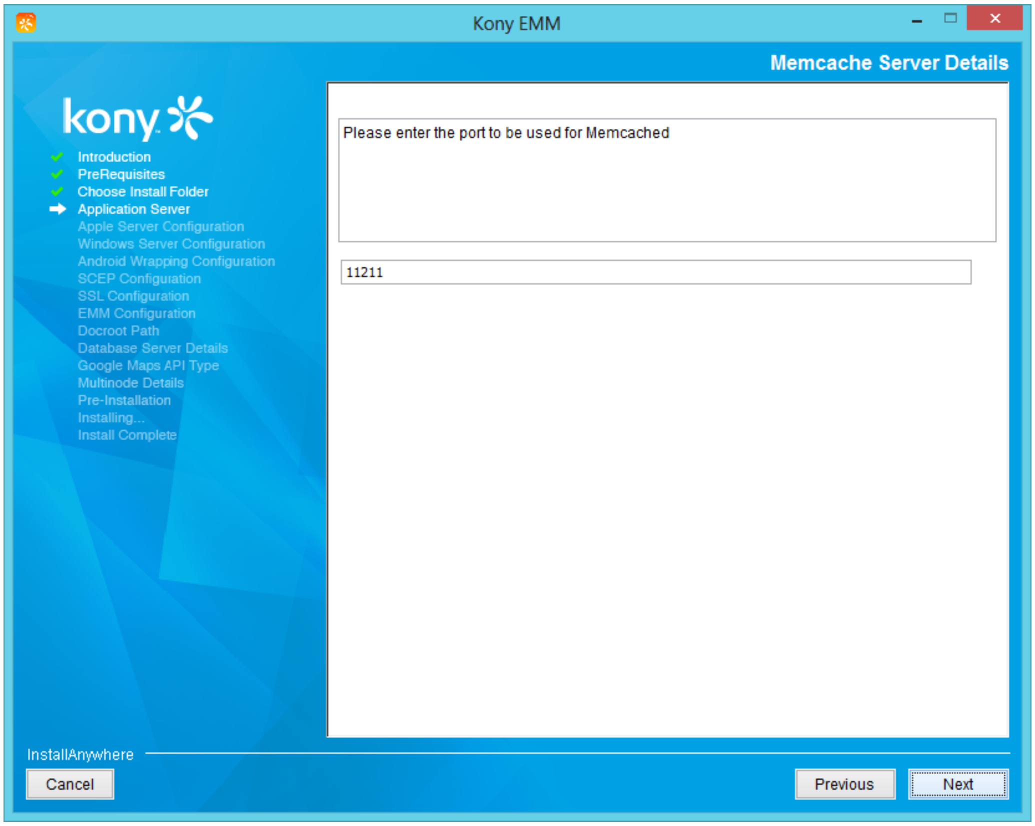
JVM Minimum Memory 2048

JVM Maximum Memory 2048

> *Note:* Use a minimum of 2048 MB JVM memory for an ideal performance. This is the memory that EMM Server requires.

The **Memcache Server Details** window appears.

15. Enter the **Port Number** to be used for Memcached.



Please enter the port to be used for Memcached

11211

16. Click **Next** to continue.

    The **Host name and IP address** window appears.

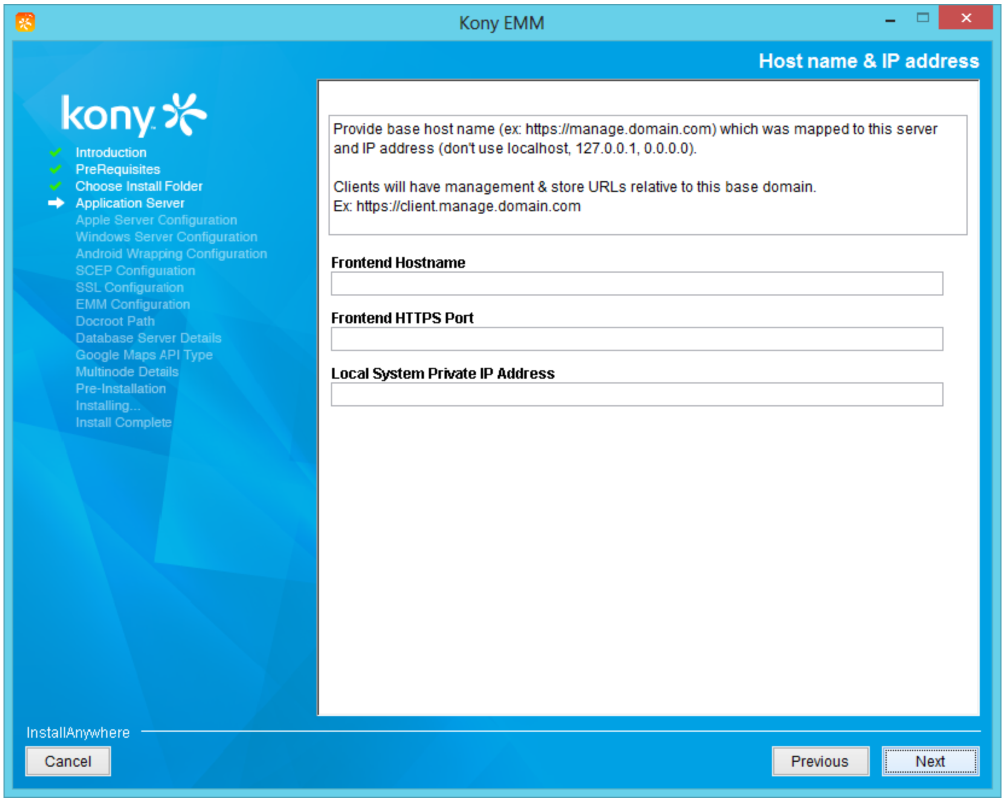
17. Enter details for the following fields:

    a. **Frontend Hostname**: Enter the host name URL that is mapped to this server. For multinode installation, enter the Load Balancer URL.

    b. **Frontend HTTPS Port**: Enter the Load Balancer HTTPS port number.

    > ***Note:*** The Frontend HTTPS port is the same as the Apache HTTPS port, if there is no load balancer. If a load balancer is present, it should be the load balancer's HTTPS port.

c. **Local System Private IP Address**: Enter the local/private IP mapped to the server where installation is in progress.



Host name & IP address

Provide base host name (ex: https://manage.domain.com) which was mapped to this server and IP address (don't use localhost, 127.0.0.1, 0.0.0.0).

Clients will have management & store URLs relative to this base domain.
Ex: https://client.manage.domain.com

Frontend Hostname

Frontend HTTPS Port

Local System Private IP Address

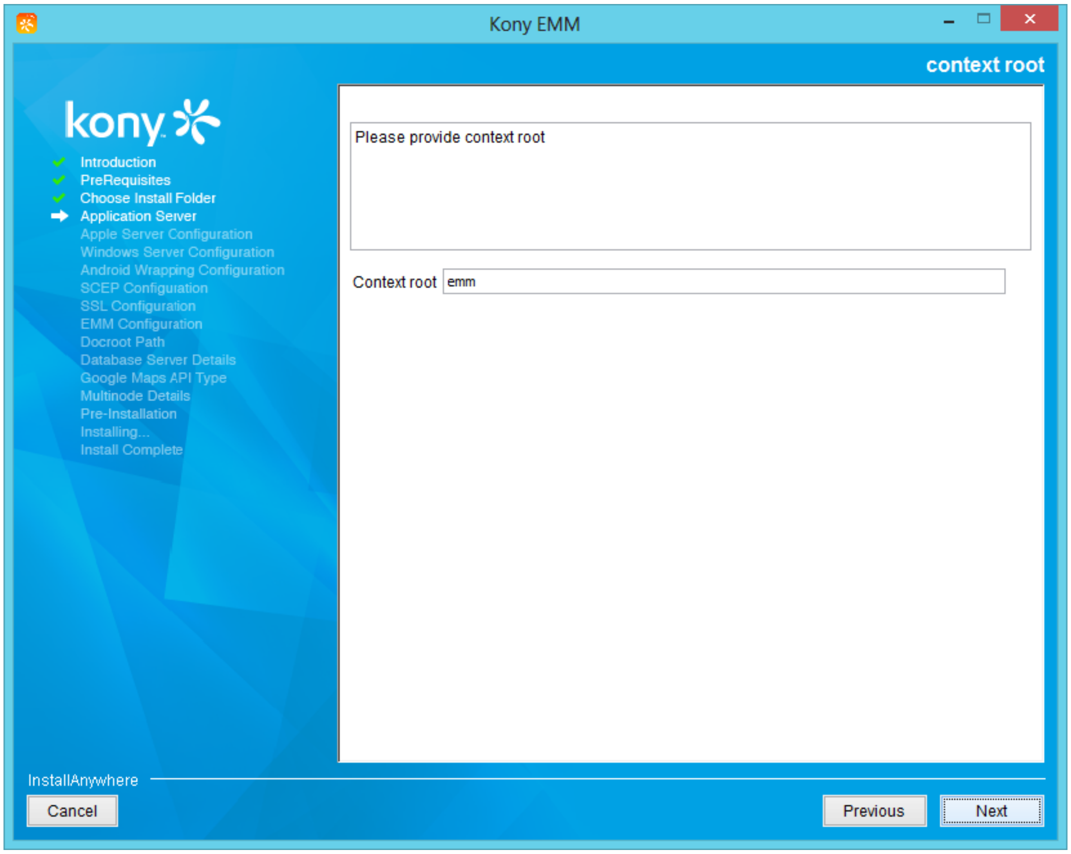
> *Note:* The installation of Kony EMM might fail if there are network configuration and connectivity problems. Ensure that the IP address is valid (do not provide the public IP address of the server), and the Hostname URL is correct.

18. Click **Next** to continue.

The **Context root** window appears.

> *Note:* The Context element represents a web application, which is run within a particular virtual host. Each web application is based on a Web Application Archive (WAR) file, or a corresponding directory containing the corresponding unpacked contents.
> You may define as many Context elements as you want. Each such Context must have a

> unique context path within a virtual host. In addition, a Context must be present with a context path equal to a zero-length string. This Context becomes the default web application for this virtual host, and processes all requests that do not match any other Context's context path. For example, if the context root is given as EMM, then the war file will be named as EMM and all the requests will be processed to EMM.



Please provide context root

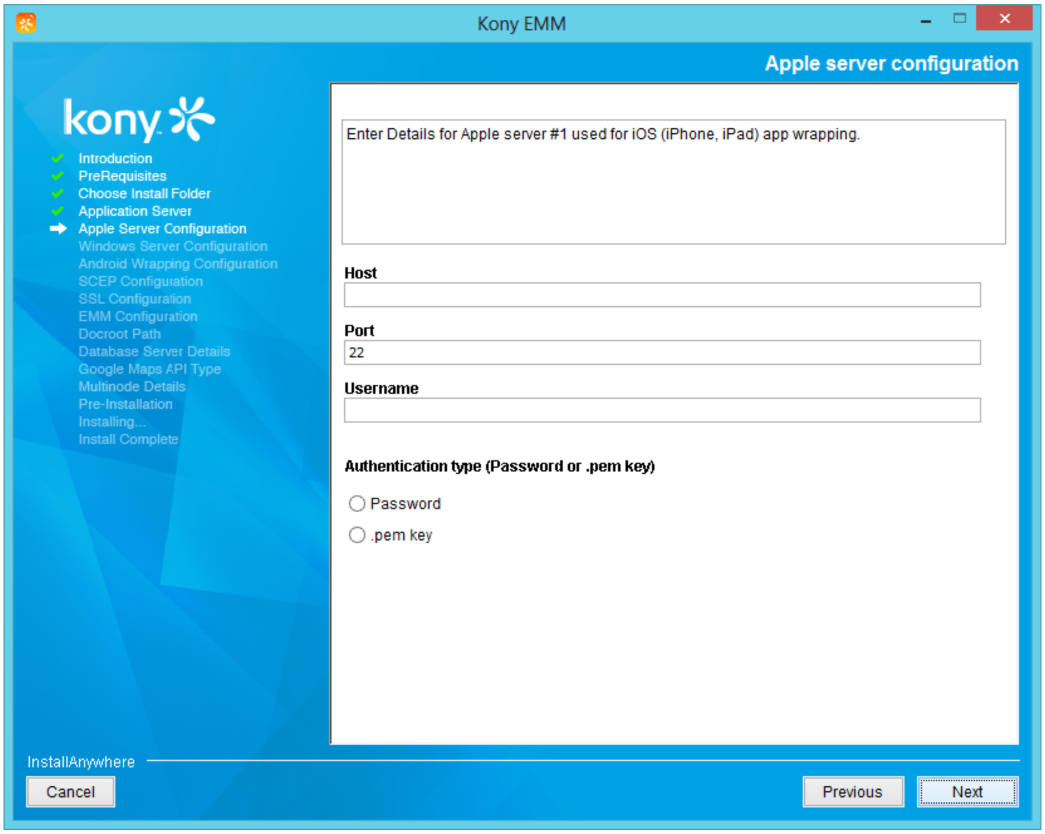
Context root: emm

19. Define your **Context root**.

20. Click **Next** to continue.

    The **Apple server configuration** window appears. You can configure a maximum of four Apple servers.The **Apple server configuration window** displays **Host**, **Port**, and **Username** fields.

21. Enter **Host** details, **Port** number and **Username** for Apple server used for iOS wrapping.



Enter Details for Apple server #1 used for iOS (iPhone, iPad) app wrapping.

Host

Port: 22

Username

Authentication type (Password or .pem key)

○ Password

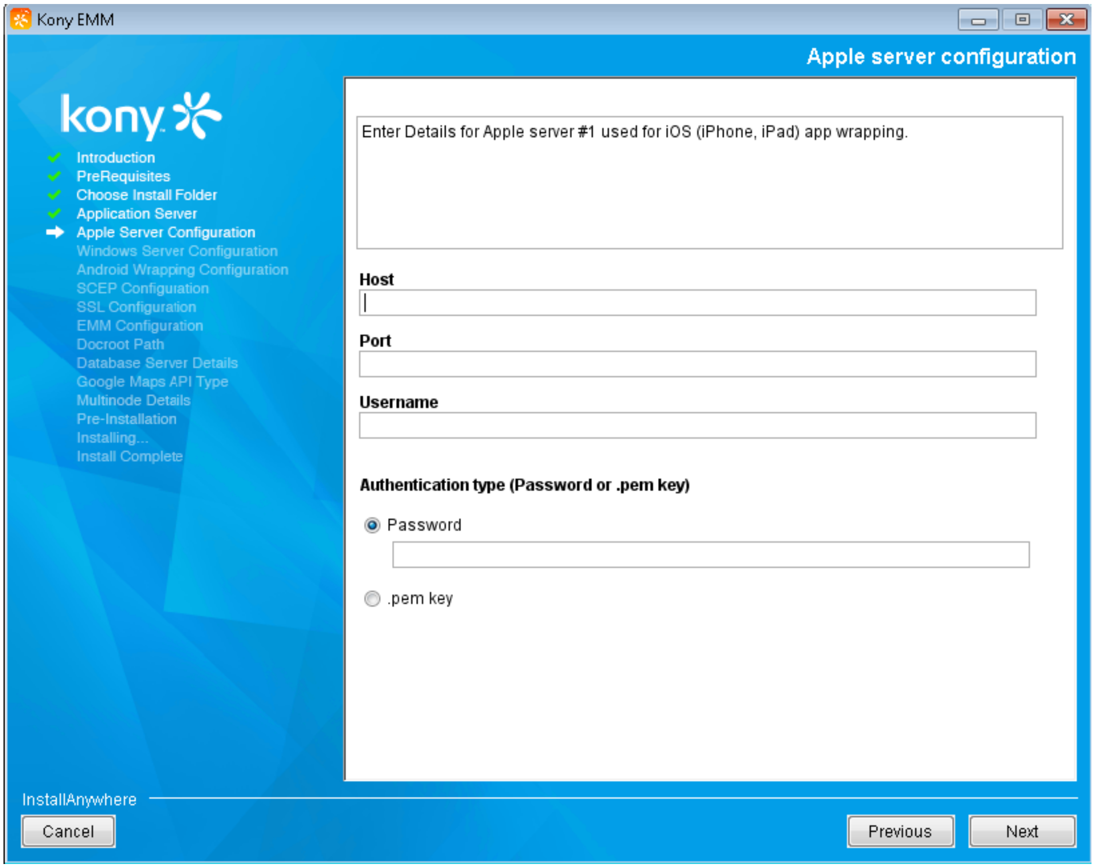
○ .pem key

22. Based on your requirement, choose the user authentication type as:

- Password
- .pem key

12.1.0.1 Password

23. If you select the **Password** option, enter a password in the **Password** field.



Enter Details for Apple server #1 used for iOS (iPhone, iPad) app wrapping.

Host

Port

Username

Authentication type (Password or .pem key)

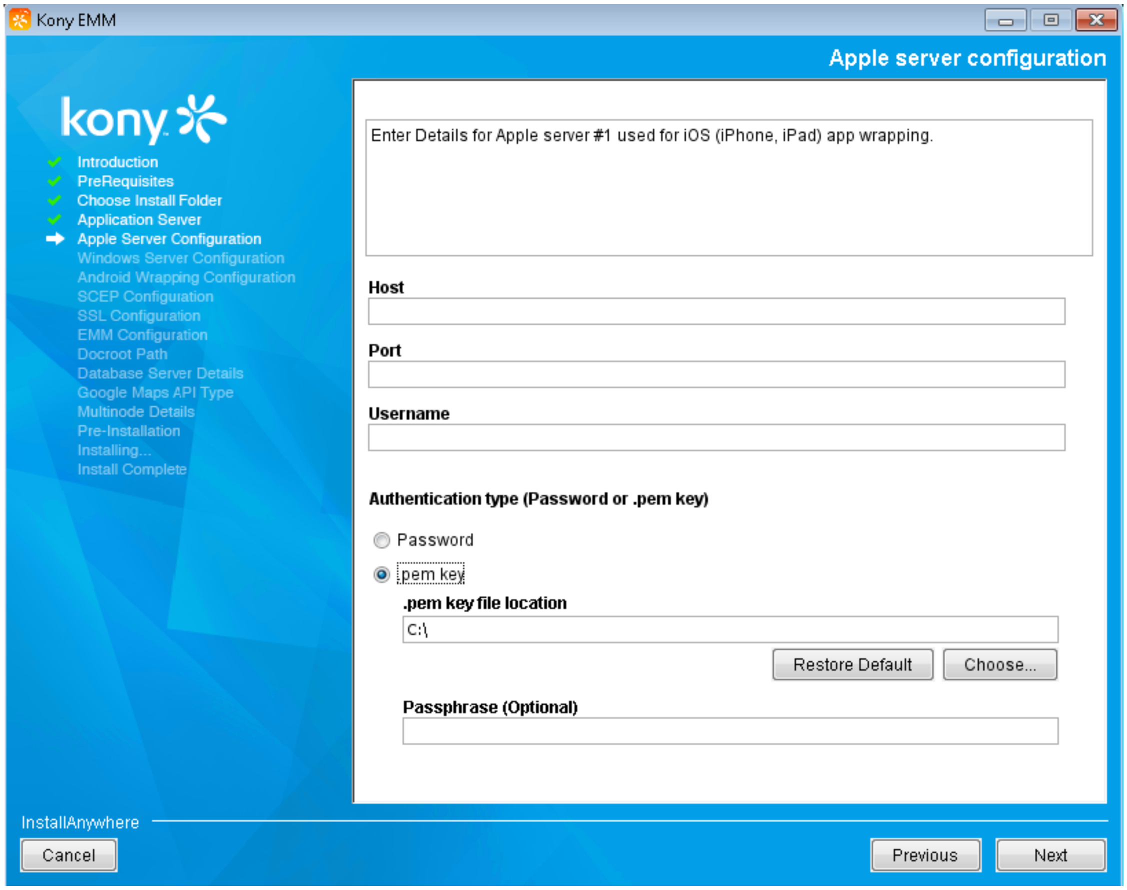
● Password

○ .pem key

12.1.0.2 .pem key

24. If you select the **.pem key** option, click **Choose** to browse the .pem key from your system.

> ***Note:*** If your .pem key is associated with a passphrase, then you are prompted for the passphrase details.



Enter Details for Apple server #1 used for iOS (iPhone, iPad) app wrapping.

Host

Port

Username

Authentication type (Password or .pem key)

○ Password

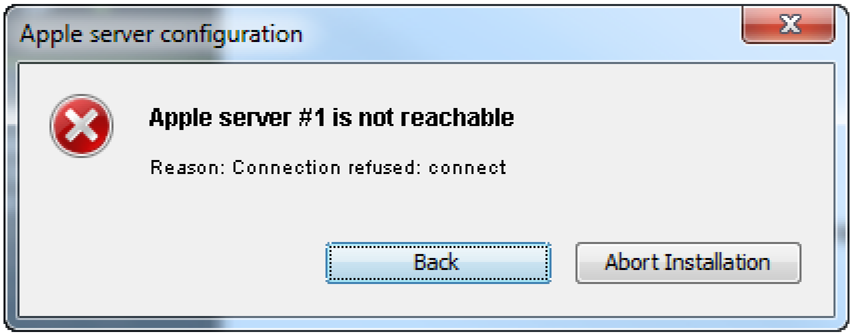
● pem key

.pem key file location

C:\

Passphrase (Optional)

25. If the Apple Server is not reachable, the following warning message appears:



Apple server #1 is not reachable

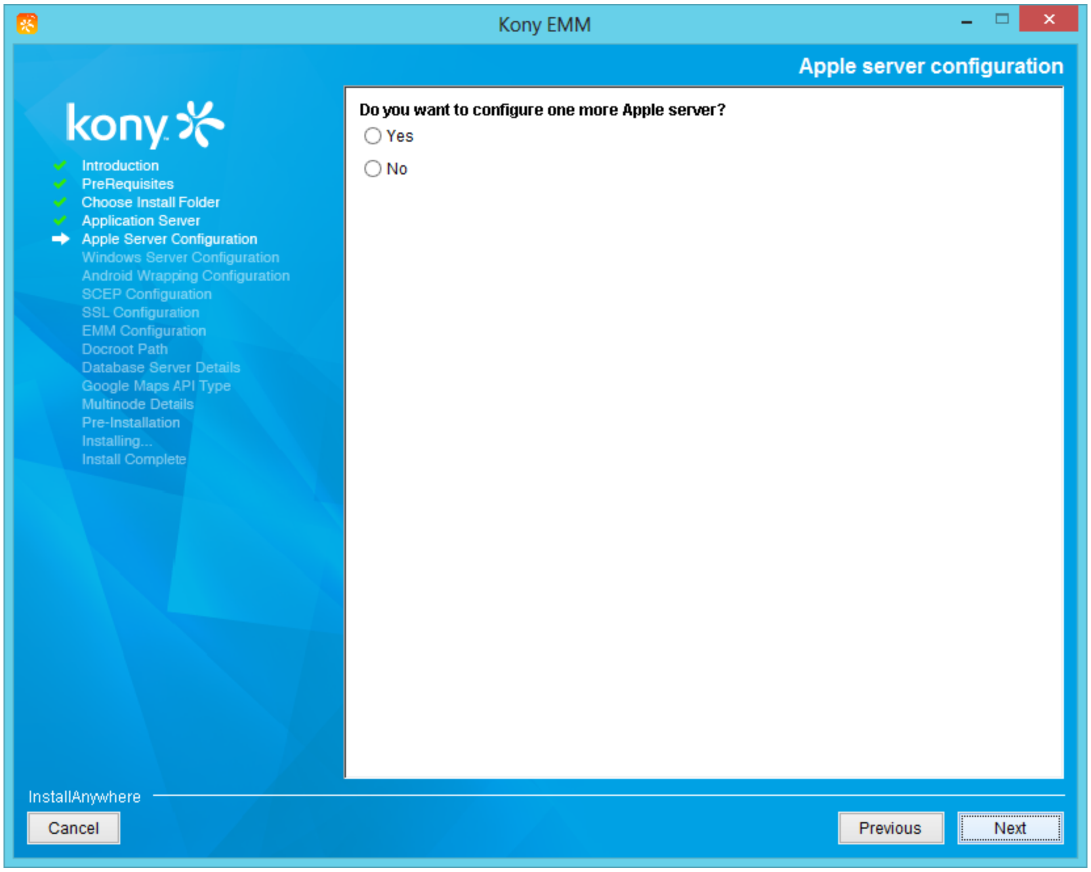
Reason: Connection refused: connect

26. Click **Back** to reset the server connection.

27. Click **Next** to continue.

The **Do you want to configure one more Apple server?** query appears.

28. Based on your requirement, select Yes or No.



Do you want to configure one more Apple server?

○ Yes

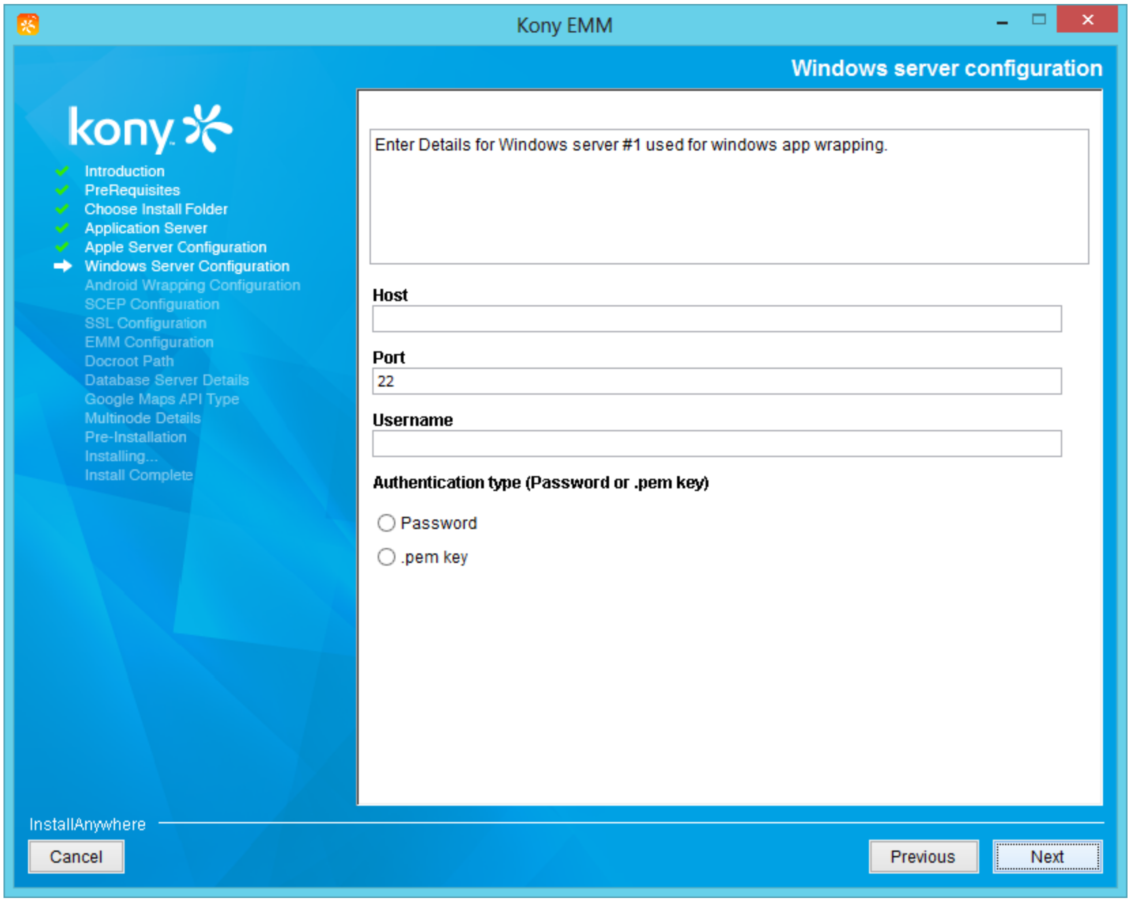
○ No

> ***Note:*** If you select **Yes**, then Apple Server window #2 appears and prompts you to enter the appropriate details.You can configure four Apple Servers. If you click **No**, the **Windows Server Configuration** panel appears

29. Select the option, and click **Next** to continue.

    The **Windows Server Configuration** window appears.

30. Enter **Host** details, **Port** number and **Username** for Windows server used for app wrapping.



Enter Details for Windows server #1 used for windows app wrapping.

Host

Port: 22

Username

Authentication type (Password or .pem key)

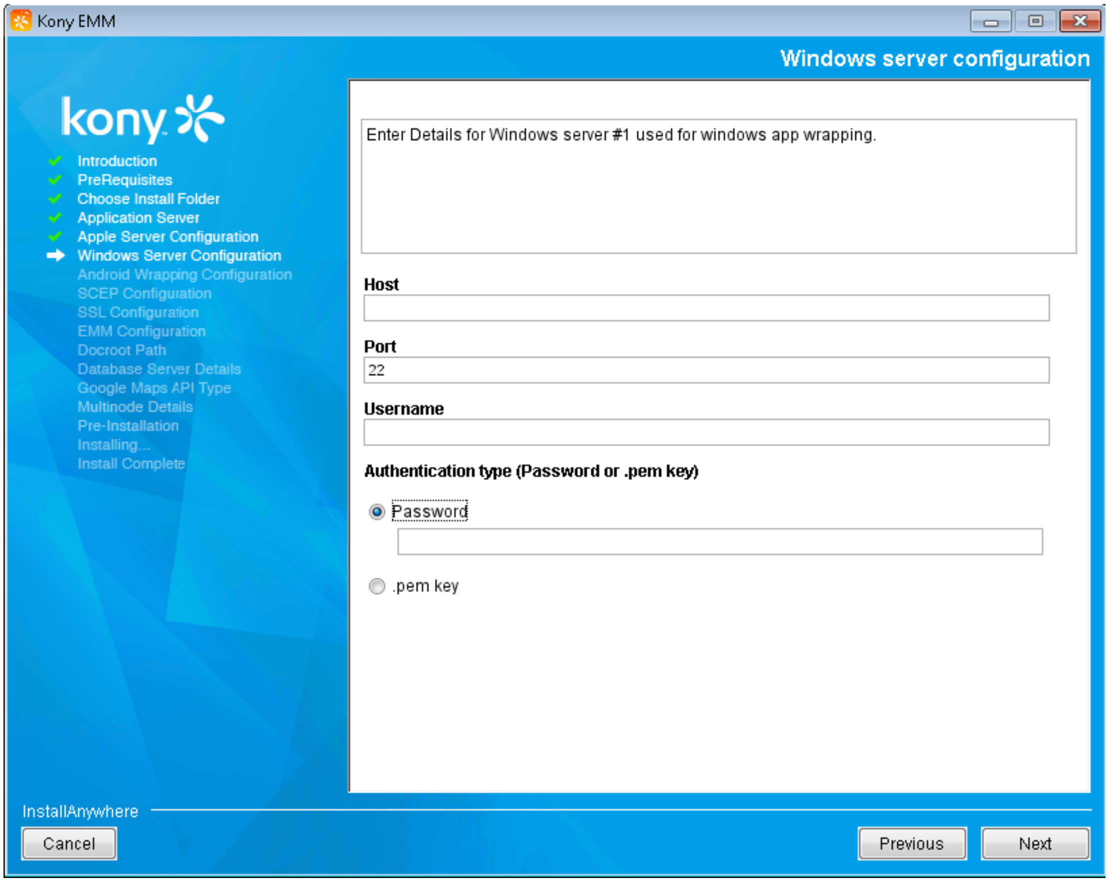
○ Password

○ .pem key

31. Based on your requirement, choose the user authentication type as:
    - Password
    - .pem key

12.1.0.3 Password for Windows Server Configuration

32. If you select the Password option, then enter a password in the **Password** field.



Enter Details for Windows server #1 used for windows app wrapping.

Host

Port
22

Username

Authentication type (Password or .pem key)

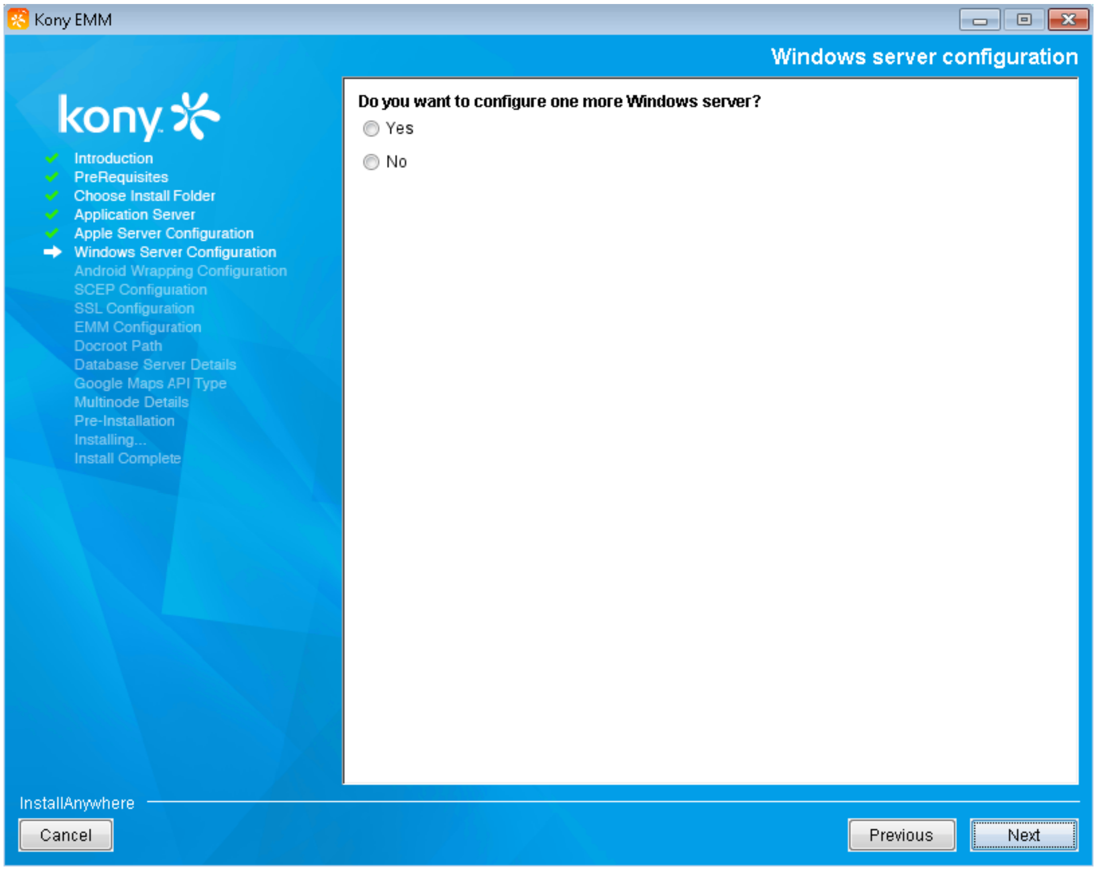
● Password

○ .pem key

12.1.0.4 .pem key for Windows Server Configuration

33. If you select the .pem key option, then click **Choose** to browse the .pem key from your system.

    The **Do you want to configure one more Windows server?** query appears.



Do you want to configure one more Windows server?

○ Yes

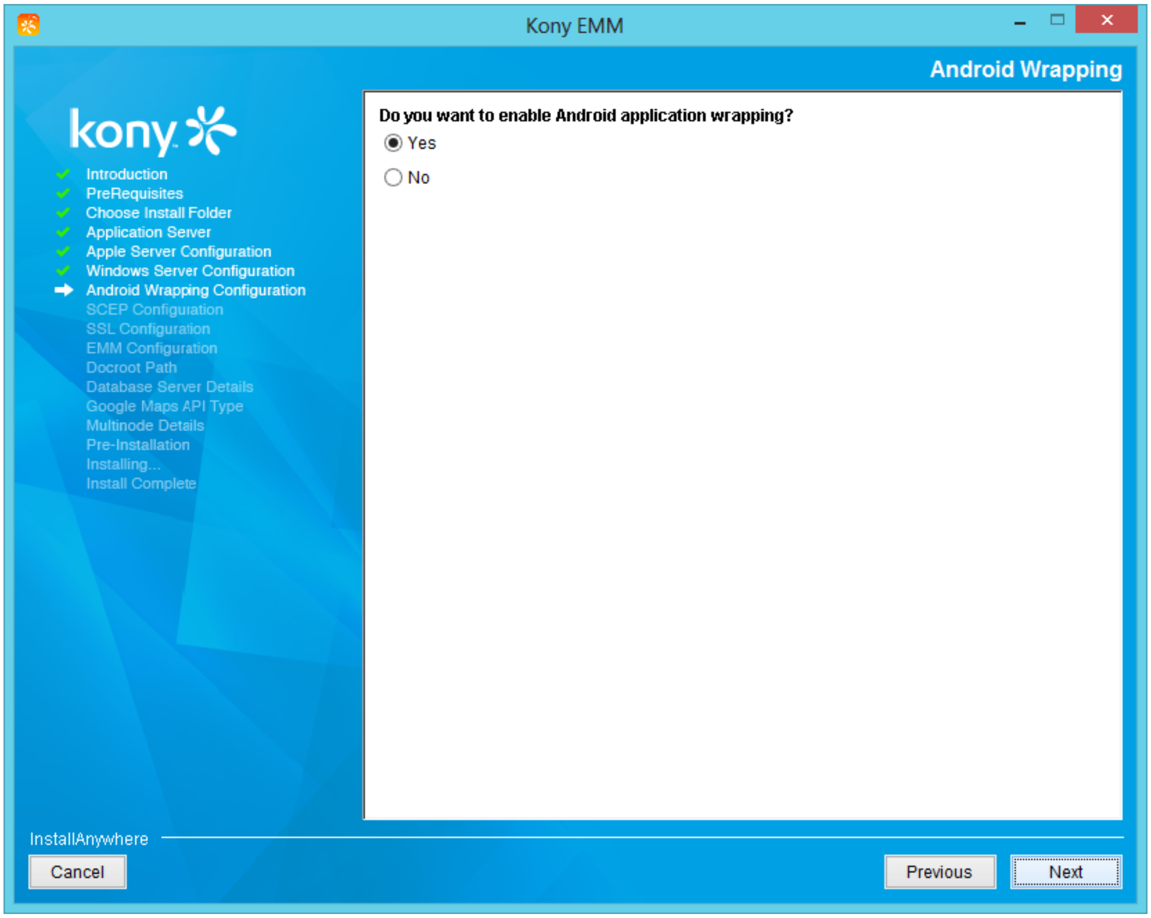
○ No

> ***Note:*** If you select **yes**, then Windows Server window #2 appears and prompts you to enter the appropriate details.

34. If you select No, click **Next** to continue.

    The **Android Wrapping** window appears.

35. Select the **yes** option to continue.



Do you want to enable Android application wrapping?

● Yes

○ No

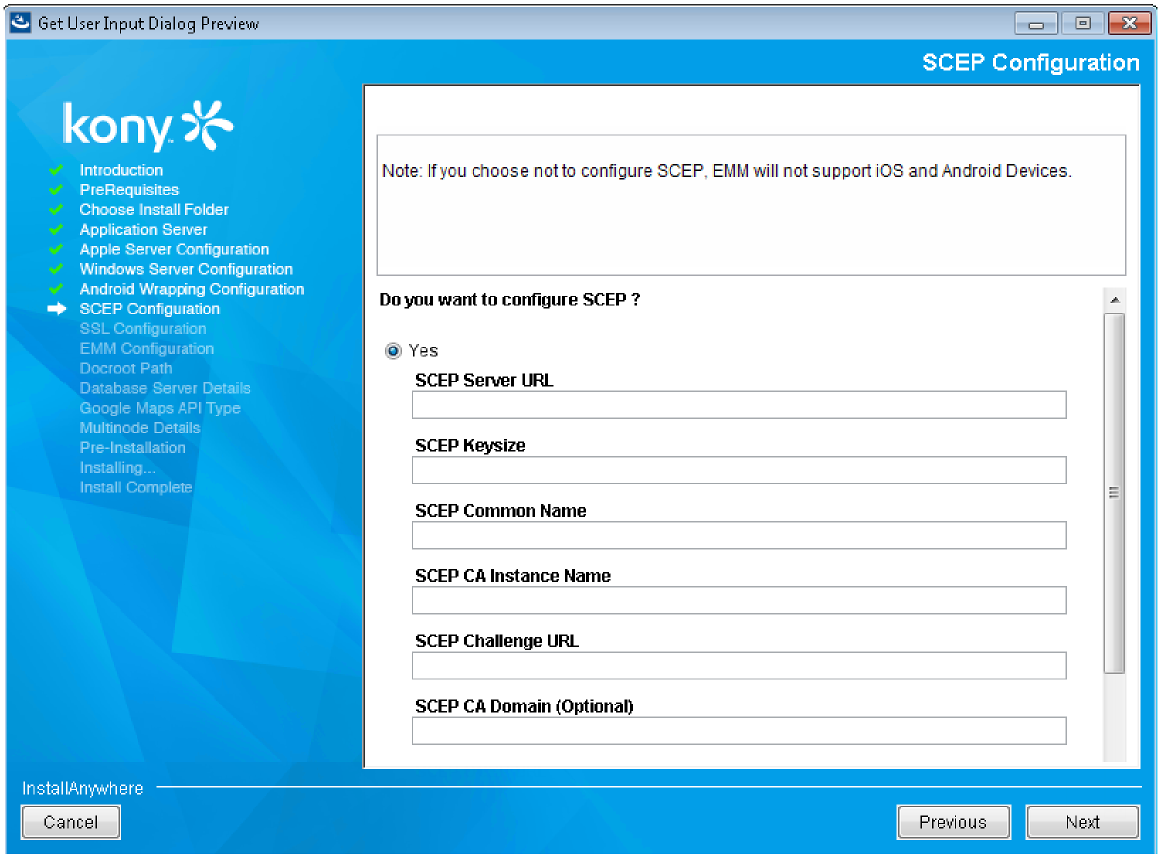
The **SCEP Configuration** window appears. All the certificates required by iOS devices during enrollment are distributed through the **SCEP** server. If you select the No option,, then you will not be able to enroll any iOS devices.

> *Note:* The SCEP configuration option appears only when the user has enabled the iOS wrapping and or Android wrapping.

> *Note:* If you do not select Enable Android Wrapping, then EMM cannot provide support to Android devices.

36. Select the **yes** option to continue.

    The **SCEP Configuration** window appears with the entry fields.



Note: If you choose not to configure SCEP, EMM will not support iOS and Android Devices.

Do you want to configure SCEP ?

● Yes

SCEP Server URL

SCEP Keysize

SCEP Common Name

SCEP CA Instance Name

SCEP Challenge URL

SCEP CA Domain (Optional)

37. Enter details for the following fields:
    a. SCEP Server URL
    b. SCEP Keysize
    c. SCEP Common Name
    d. SCEP CA Instance Name
    e. SCEP Challenge URL
    f. SCEP CA Domain (Optional)

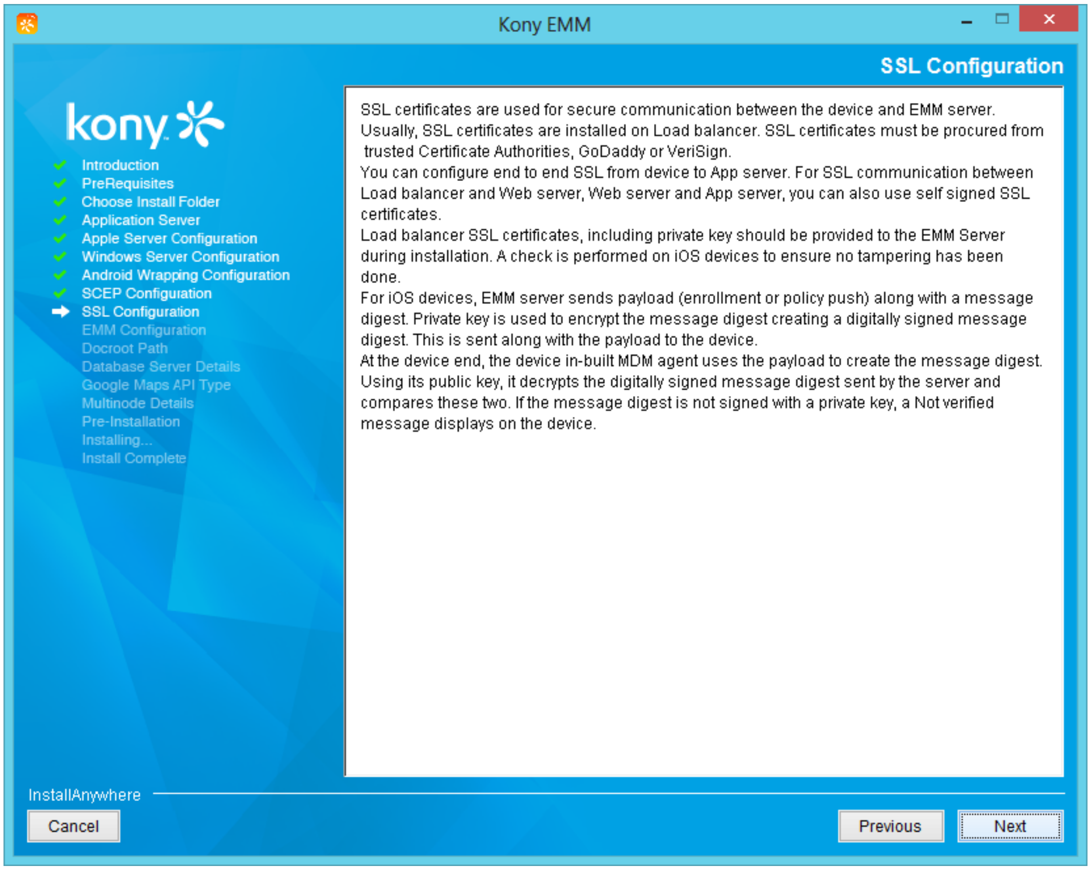
    g. SCEP CA Username

    h. SCEP CA Password

38. Click **Next** to continue.

    The **Please Wait window** appears, alerting the user that KonyEMM configuration is in progress.

    The **SSL Configuration** statement window appears.

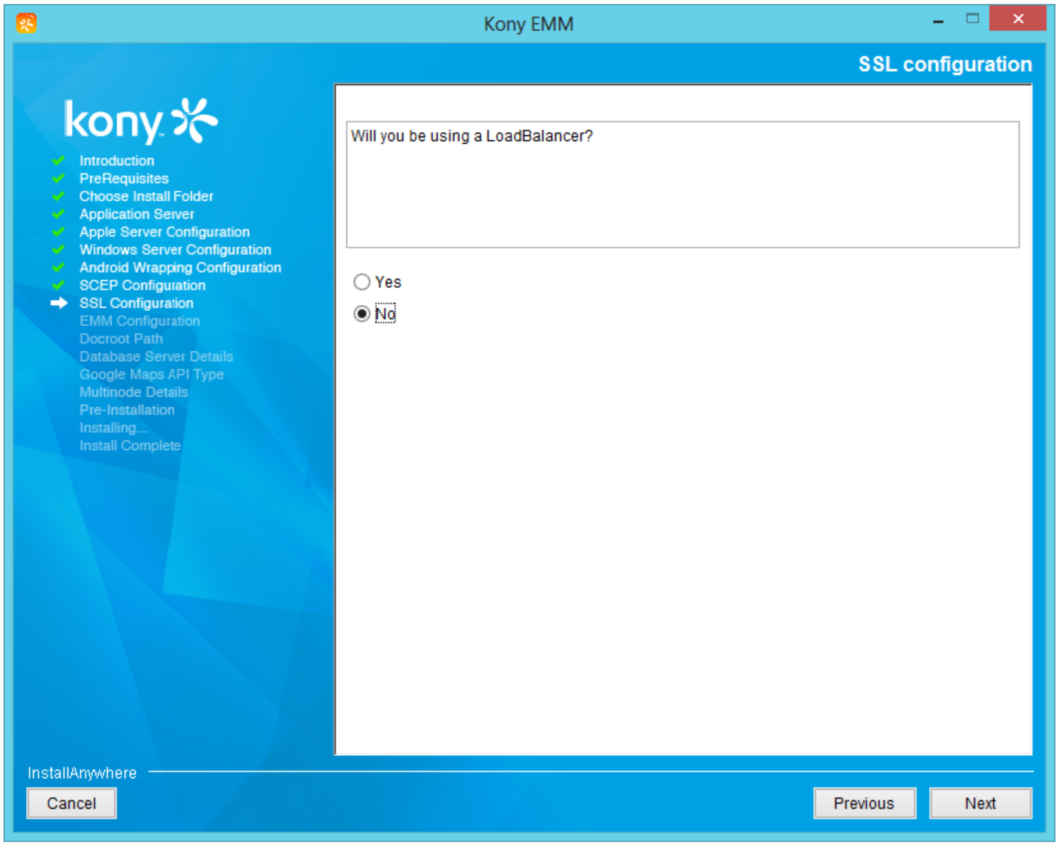


SSL certificates are used for secure communication between the device and EMM server. Usually, SSL certificates are installed on Load balancer. SSL certificates must be procured from trusted Certificate Authorities, GoDaddy or VeriSign.
You can configure end to end SSL from device to App server. For SSL communication between Load balancer and Web server, Web server and App server, you can also use self signed SSL certificates.
Load balancer SSL certificates, including private key should be provided to the EMM Server during installation. A check is performed on iOS devices to ensure no tampering has been done.
For iOS devices, EMM server sends payload (enrollment or policy push) along with a message digest. Private key is used to encrypt the message digest creating a digitally signed message digest. This is sent along with the payload to the device.
At the device end, the device in-built MDM agent uses the payload to create the message digest. Using its public key, it decrypts the digitally signed message digest sent by the server and compares these two. If the message digest is not signed with a private key, a Not verified message displays on the device.

39. Click **Next** to continue.

    The **SSL Configuration** window appears.

40. To use LoadBalancer, select the option as **Yes**. By default, the option is set to **No**.



Will you be using a LoadBalancer?

○ Yes

● No

41. You need **LoadBalancer Certificates** to enroll iOS devices. Click **Choose** to browse the following files from their location. Ensure that you select the appropriate certificates.

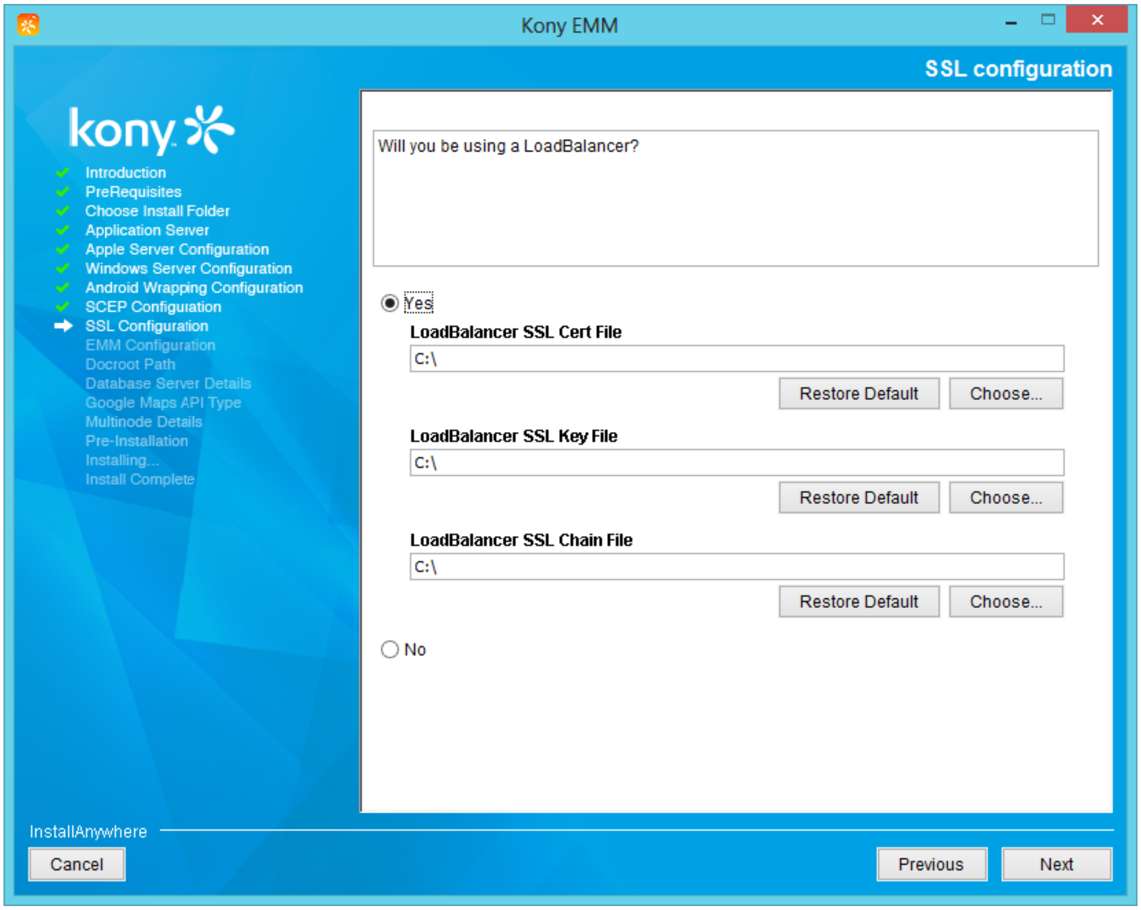
    a. LoadBalancer SSL Cert File

    b. LoadBalancer SSL Key File

    c. LoadBalancer SSL Chain File

> ***Note:*** LoadBalancer SSL certificates, including private key, should be provided to EMM Server during installation. A check is performed on iOS devices to ensure no tampering has occured.For iOS devices, EMM Server sends payload (enrollment or policy push) along with a message digest. Private key encrypts the message digest creating a digitally signed

> message digest, which is sent along with the payload to the device.
>
> At the device end, the device built-in MDM agent uses the payload to create the message digest. Using its public key, it decrypts the digitally signed message digest sent by the server and compares these two. If the message digest is not signed with a private key, a Not verified message is displayed on the device.



Will you be using a LoadBalancer?

● Yes

LoadBalancer SSL Cert File: C:\

LoadBalancer SSL Key File: C:\

LoadBalancer SSL Chain File: C:\

○ No

42. Select the **No** option, if you do not want to use LoadBalancer.

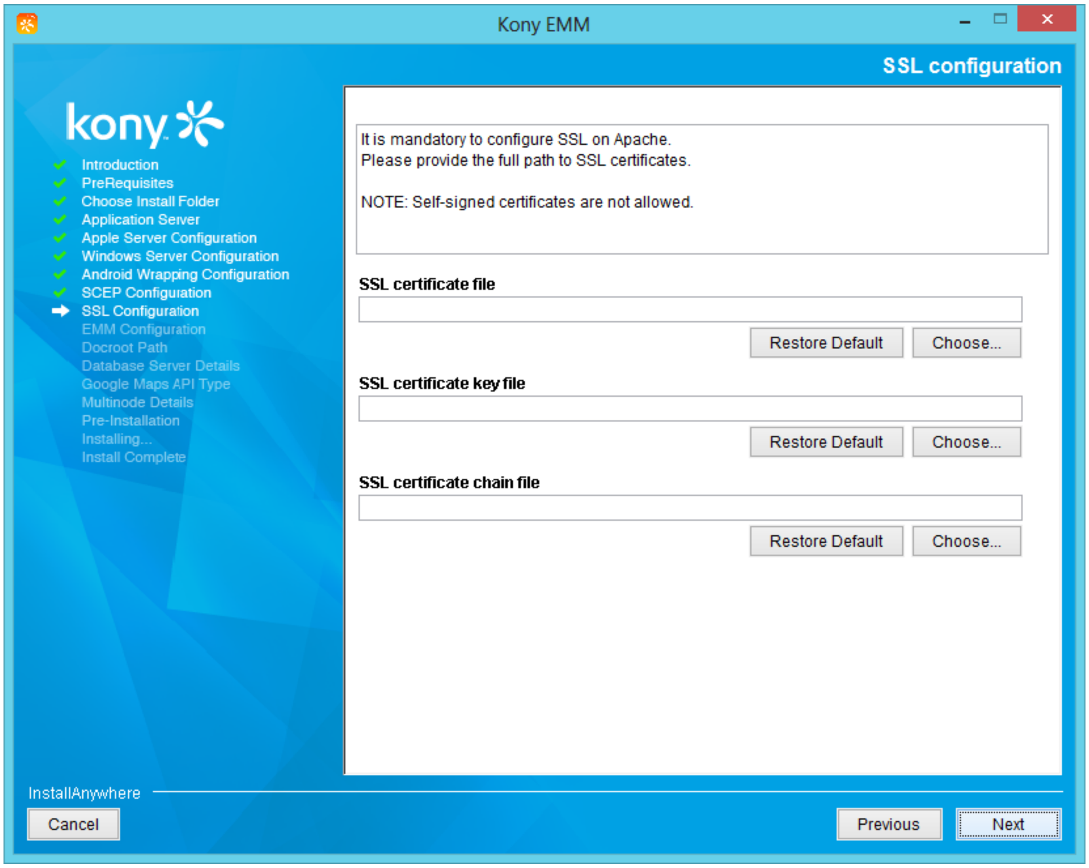
43. To configure SSL on Apache, click **Choose** to browse the following files from their location. Ensure that you select the appropriate certificates.

a. SSL certificate file

b. SSL certificate key file

c. SSL certificate chain file

> ***Note:*** A publicly signed SSL certificate must be available for import during the installation. Self-signed certificates are not allowed.



It is mandatory to configure SSL on Apache.
Please provide the full path to SSL certificates.

NOTE: Self-signed certificates are not allowed.

SSL certificate file

SSL certificate key file

SSL certificate chain file

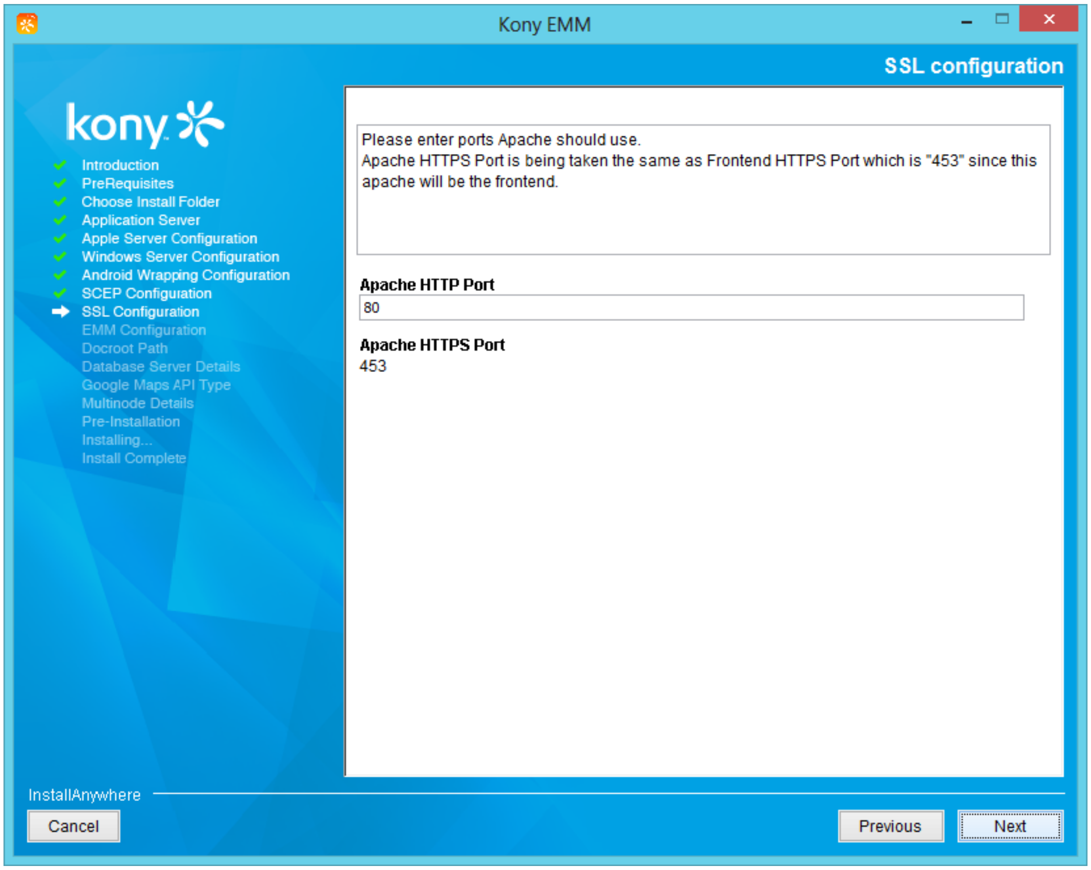
44. Click **Next** to continue.

The **SSL Configuration** window appears with default values for the Apache **HTTP Port** and the Apache **HTTPS Port**.

45. Based on your requirement, you can enter the values for the following fields:

    a. **Apache HTTP Port**: Enter the HTTP Port number.

    b. **Apache HTTPS Port**: HTTPS.This port number will be same as the Frontend HTTPS port, if you do not want to configure LoadBalancer.



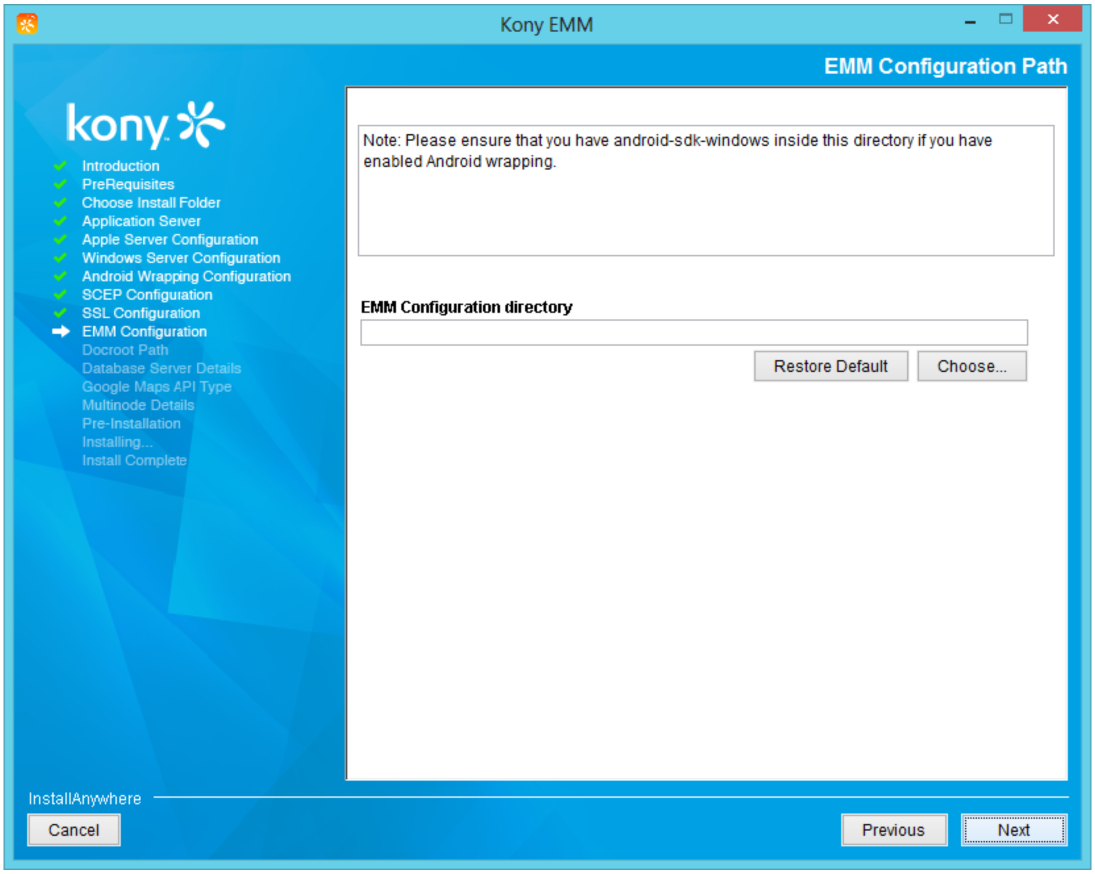
Please enter ports Apache should use.
Apache HTTPS Port is being taken the same as Frontend HTTPS Port which is "453" since this apache will be the frontend.

Apache HTTP Port
80

Apache HTTPS Port
453

46. Click **Next** to continue.

    The **EMM Configuration Path** window appears.



Note: Please ensure that you have android-sdk-windows inside this directory if you have enabled Android wrapping.

EMM Configuration directory

> *Important:* Ensure that you have android-sdk-windows in this directory if you have enabled Android wrapping.

47. If the Android SDK is not found, then the warning message **Error -android -sdk- windows** dialog appears. The alert also asks you to go back or abort the installation.

48. Click **Choose** to browse the **EMM Configuration directory**.The path you define stores all dynamic content created in EMM application, such as device details, device sets, app details,categories, and settings.

> *Important:* Do not include spaces in the name of EMM Configuration Directory. If you include spaces, an error message will appear to warn that the installation path is invalid.

The **Docroot Path** window appears.

49. Click **Choose** to select the desired path - for example <installation folder>/docroot.For multinode installation, enter the UNC path of your docroot folder in common mount, for example \\10.11.11.53\EMM_FS\docroot

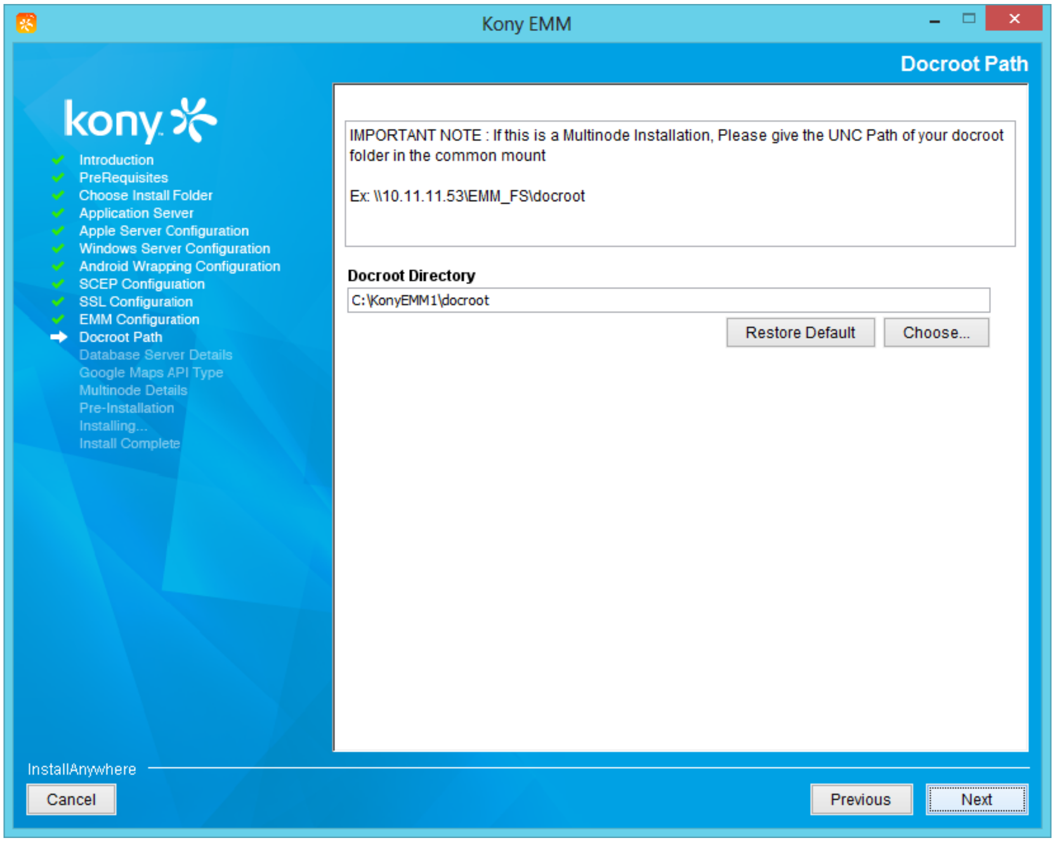
The selected path will appear in the **Docroot Directory** field.

The docroot or docbase is the storage location which EMM uses to store all admin or user uploaded content. For on-premises installations, the docroot is a hard-mounted location within the application server; a local file-system or an SAN mounted device. The docroot can be hosted on an Amazon Simple Storage Service.

The docroot comprises of four separate directories for the EMM modules: Store, MAM, MDM, MCM, MDM., and emm_common.

For local file systems, Static resources like screen shots or header images or icons are navigable if one is familiar with directory structure and the generated file names. There are no access regulations. Access to secure assets like binaries are restricted via Apache through secure URLs over web. Ensure that unintended users do not have file system read/write permissions. Access to critical assets like certificates are completely blocked. They may only be accessed internally and never by a client.

For Amazon Simple Storage Service, access to static resources is through static URLs available publicly. For secure assets like binaries, access is restricted through secure URLs generated with an expiring schedule. Links to critical assets like certificates are never generated. These are only used internally via secure Amazon APIs.



IMPORTANT NOTE : If this is a Multinode Installation, Please give the UNC Path of your docroot folder in the common mount

Ex: \\10.11.11.53\EMM_FS\docroot

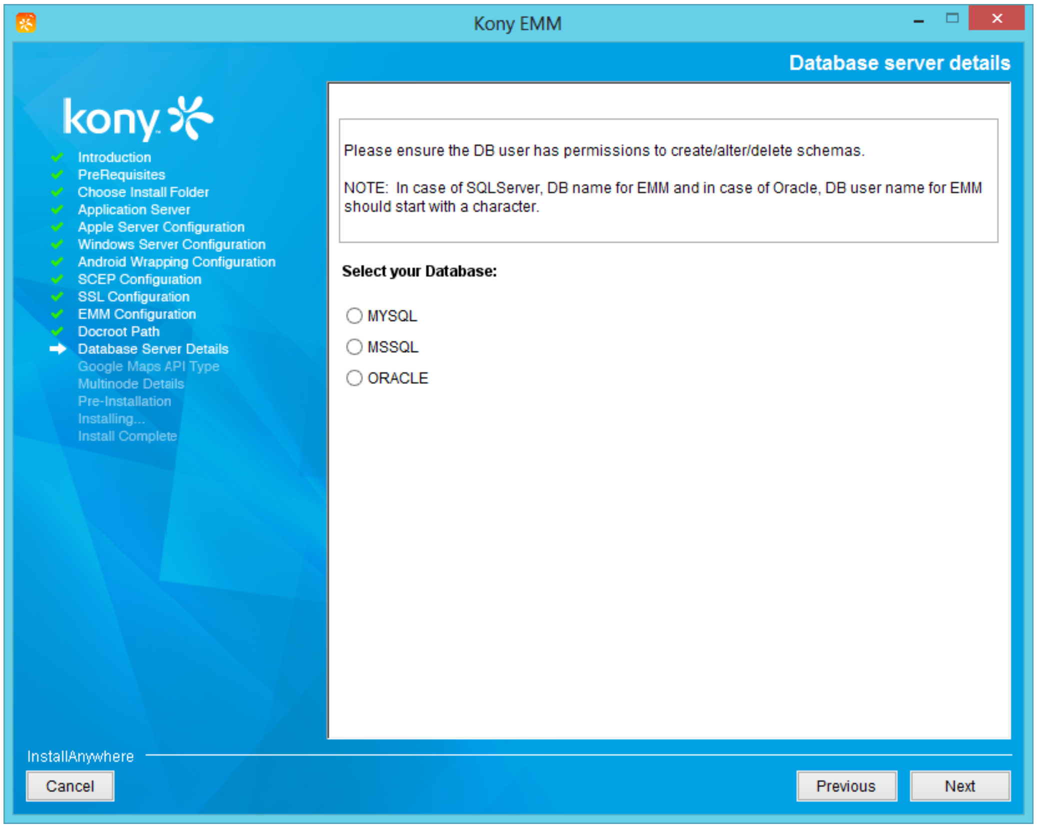
Docroot Directory

C:\KonyEMM1\docroot

50. Click **Next** to continue.

    The **Database server details** window appears.

51. Select the required database.



Please ensure the DB user has permissions to create/alter/delete schemas.

NOTE: In case of SQLServer, DB name for EMM and in case of Oracle, DB user name for EMM should start with a character.

Select your Database:

○ MYSQL
○ MSSQL
○ ORACLE

52. Based on your requirement, choose the database as:

- MySQL
- Microsoft SQL
- ORACLE

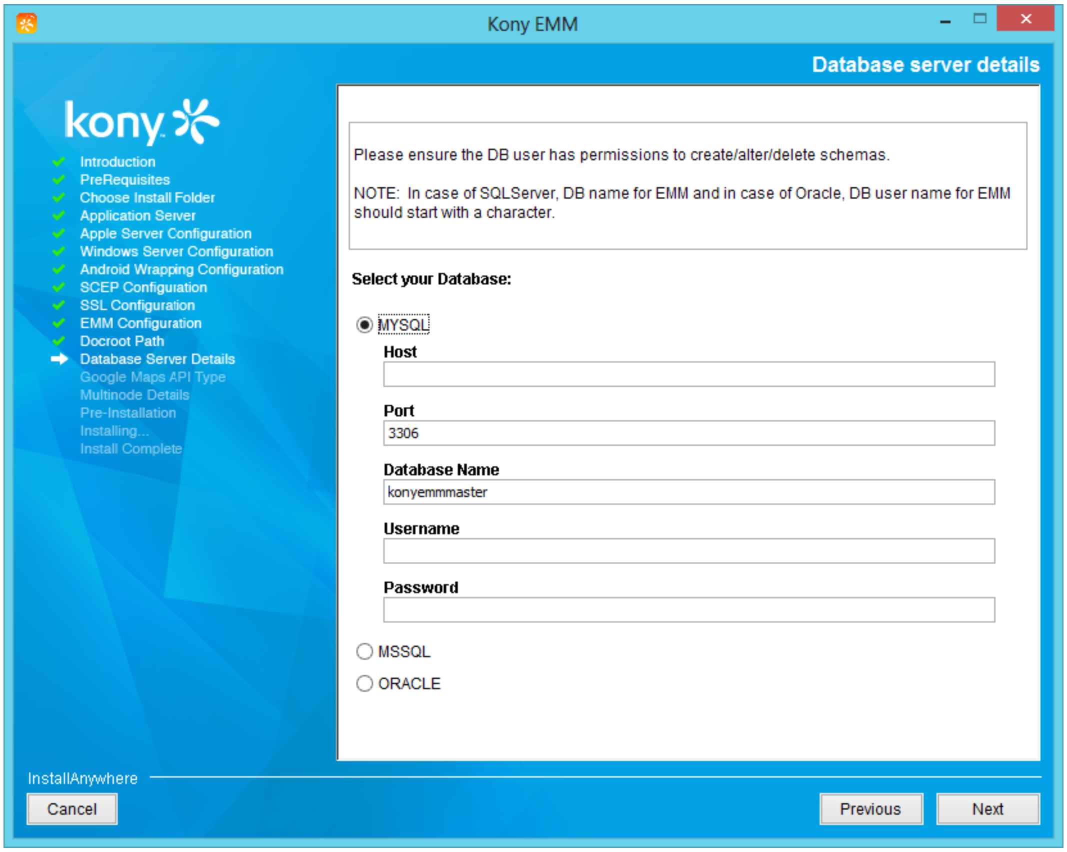
12.1.0.5 MySQL

53. If you select database **MySQL**, enter details for the following fields:

- **Host**: Enter the host name used while creating the database user. By default, the host name is set as localhost.
- **Port**: Enter the Port number. By default, it is set as 3306.

- **Database Name**: By default, the Database Name is set as konyemmmaster. The name konyemmmaster was created during preinstallation.
- **Username**: Enter the Database Administrator (DBA).
- **Password**: Enter the database password of Database Administrator.

> ***Note:*** You might receive warning messages regarding database connection failures while using existing databases. Ensure your MySQL version is greater than 5.5.



Please ensure the DB user has permissions to create/alter/delete schemas.

NOTE: In case of SQLServer, DB name for EMM and in case of Oracle, DB user name for EMM should start with a character.

Select your Database:

● MYSQL

Host:

Port: 3306

Database Name: konyemmmaster

Username:

Password:

○ MSSQL

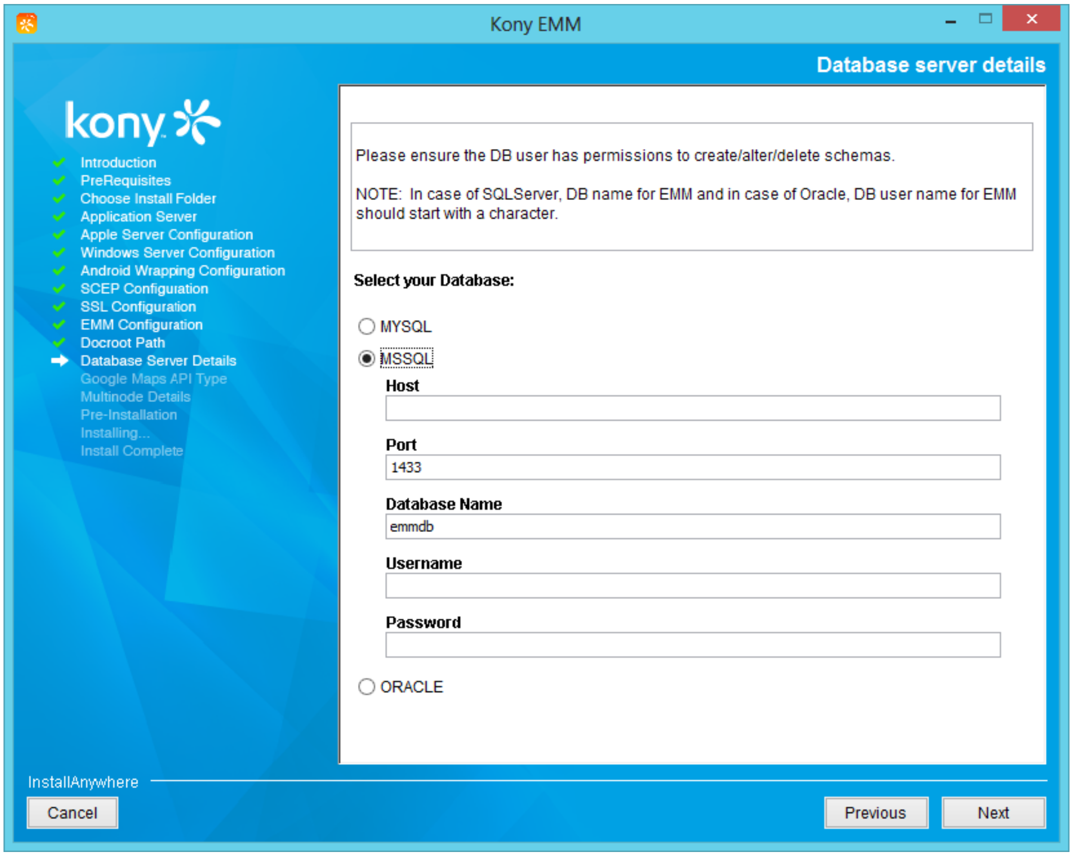
○ ORACLE

12.1.0.6 Microsoft SQL

54. If you select the **database** as **Microsoft SQL**, then enter details for the following fields:

    - **Host**: Enter the host name used while creating the database user. By default, the host name is set as localhost.
    - **Port**: Enter the Port number. By default, the Port number is set as 1433.
    - **Database Name**: By default, the database name is set as emmdb.Emmdb was created during preinstallation.
    - **Username**: Enter the user name of the DBA.
    - **Password**: Enter the database password of the DBA.

    > ***Note:*** You might receive warning messages regarding database connection failures and using existing database. Ensure that an instance of the SQL Server is running on the host and accepting TCP/IP connection at the port.



Database server details

Please ensure the DB user has permissions to create/alter/delete schemas.

NOTE: In case of SQLServer, DB name for EMM and in case of Oracle, DB user name for EMM should start with a character.

Select your Database:

○ MYSQL

● MSSQL

Host

Port
1433

Database Name
emmdb

Username

Password

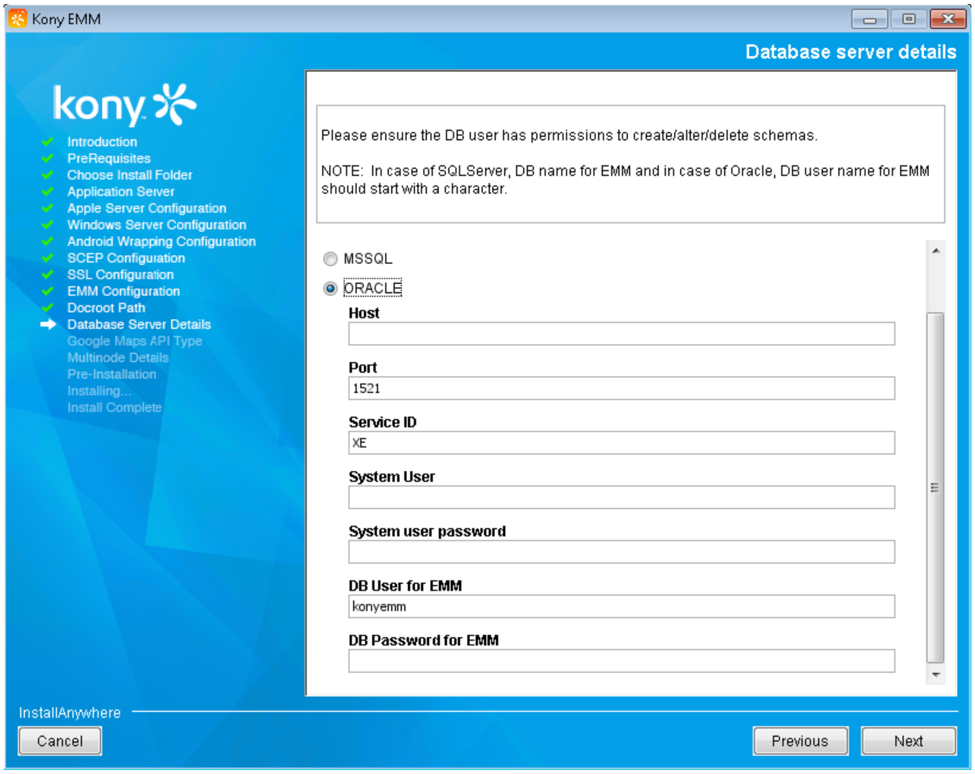
○ ORACLE

12.1.0.7 ORACLE

55. If you select the database as **Oracle**, enter details for the following fields:

- **Host**: Enter the host name used while creating the database user. By default, the host is set as localhost.
- **Port**: Enter the Port number. By default, the port number is set as 1521.
- **Service ID**: By default, the Service ID is set as XE.
- **System User**: Enter the user name of the DBA.
- **System User Password:** Enter the database password of DBA.

- **DB User for EMM**: Enter your desired databse user name for EMM. By default, the user name will be set as *konyemm*.
- **DB Password for EMM**: Enter your desired databse password for the user you created.



Please ensure the DB user has permissions to create/alter/delete schemas.

NOTE: In case of SQLServer, DB name for EMM and in case of Oracle, DB user name for EMM should start with a character.

○ MSSQL
● ORACLE

Host:

Port: 1521

Service ID: XE

System User:

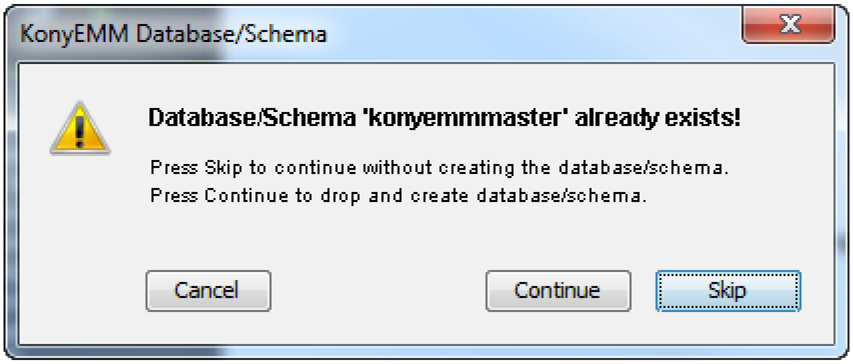
System user password:

DB User for EMM: konyemm

DB Password for EMM:

> *Important:* Before installing the Oracle database, the following Database Tablespaces should be created.
>
> EMM_DATA
>
> EMM_INDEX
>
> EMM_LOB_DATA

If database/schema already exists, the system will display the following warning.



Database/Schema 'konyemmmaster' already exists!

Press Skip to continue without creating the database/schema.
Press Continue to drop and create database/schema.

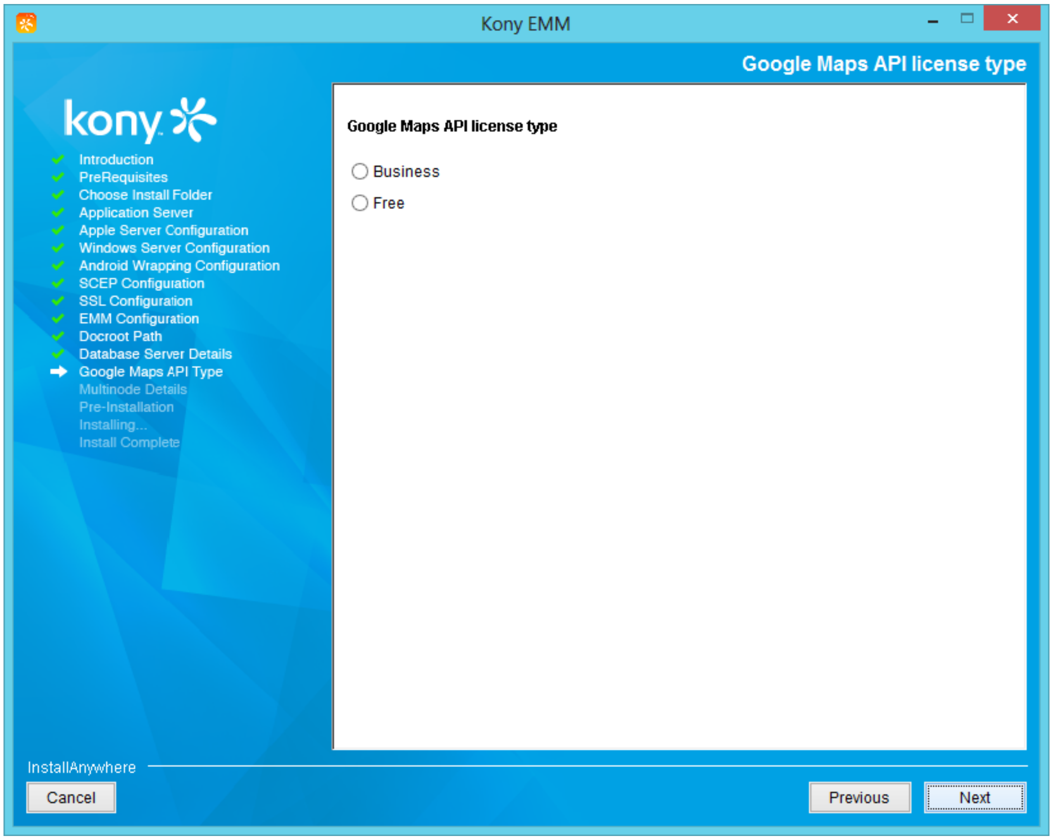
> *Note:* Based on your requirement, you can click **Skip** without creating the database/schema. You can click **Continue** to drop and create database/schema.

> *Note:* You might receive warning messages regarding database connection failures using existing database. To ensure database connectivity, follow these steps:
> The TCP/IP connection to the local host and port fails. Ensure to enter correct credentials to ensure database server connectivity.
> Make sure that the TCP connection to the port is not blocked by a firewall..

The **Please Wait** window appears, advising a user that KonyEMM configuration is in progress.

56. Click **Next** to continue.

    The **Google Maps API license type** window appears.



Google Maps API license type

○ Business

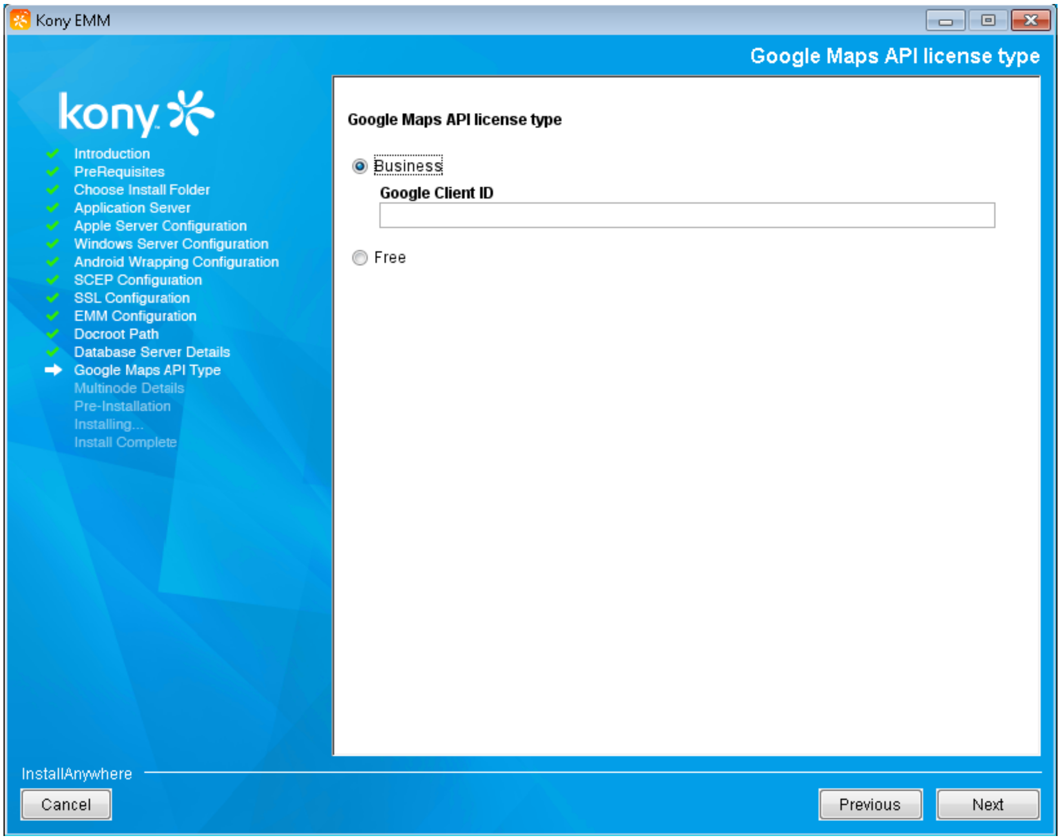
○ Free

> ***Note:*** Google Maps application is essential to provide features, such as the identification ofi device location and geo-fences. If you want to have these features, you must provide an appropriate license and client ID details.
>
> Refer to the following tutorial to generate the maps key
> https://developers.google.com/maps/documentation/javascript/tutorial
>
> Based on a customer account, use the business key or free key.
>
> For the business option,enter the client ID. For the Free option, enter the Maps key.

57. Based on your requirement, choose the **Google Maps API License type** as:
    a. Business
    b. Free

12.1.0.8 Business

58. If you select the **Business** option, then enter the client ID in **Google Client ID**.



Google Maps API license type

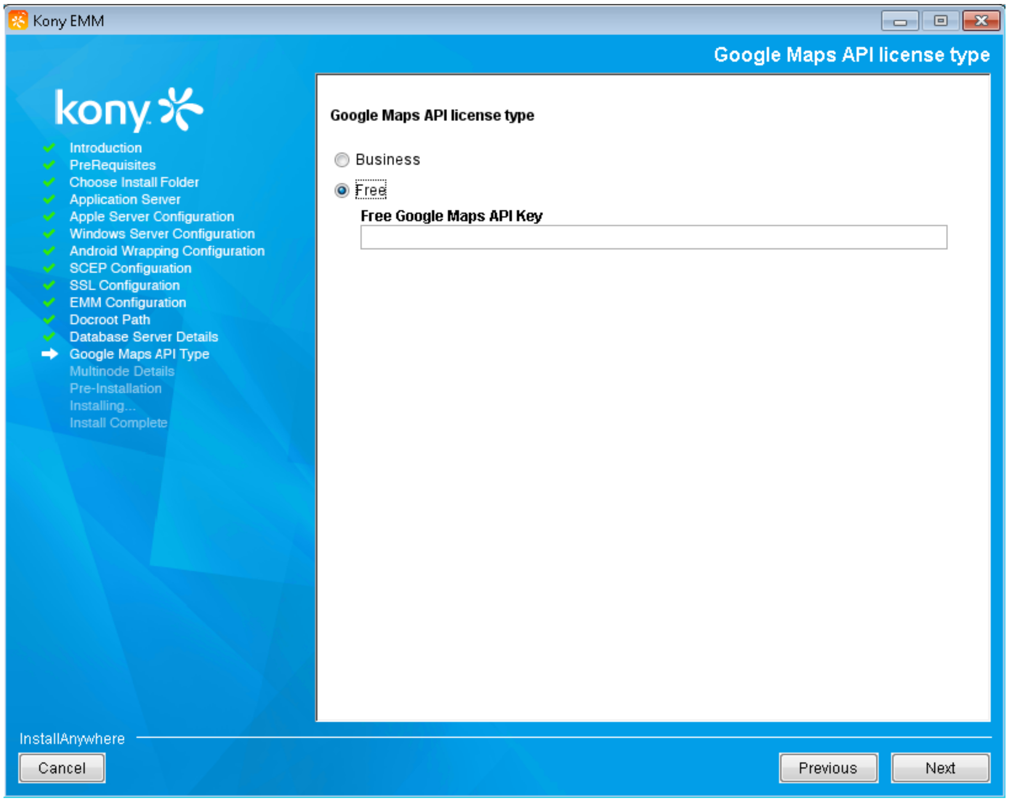
● Business

Google Client ID

○ Free

12.1.0.9 Free

59. If you select the **Free** option, then enter the API key of Free Google maps in **Free Google Maps API Key**.



Google Maps API license type

○ Business

● Free

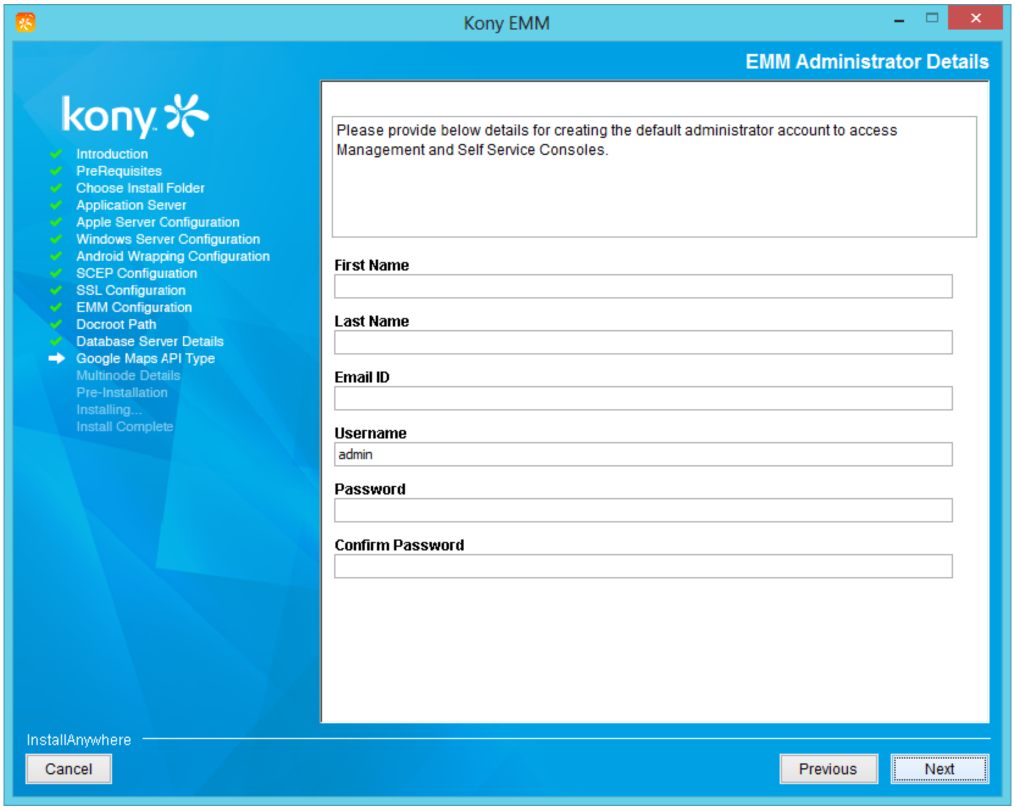
Free Google Maps API Key

60. Click **Next** to continue.

    The **EMM Administrator Details** window appears.

61. Enter details for the following fields:
    a. **First Name**: Enter your first name.
    b. **Last Name**: Enter your last name.
    c. **Email ID**: Enter your email-ID.
    d. **Username**: Enter your desired EMM console user name. By default, it is set as admin.
    e. **Password**: Enter your desired EMM console user password for the user you want to create.

> ***Note:*** The user name and the password provided are the admin login credentials of the EMM Management Console.



Please provide below details for creating the default administrator account to access Management and Self Service Consoles.

First Name

Last Name

Email ID

Username: admin

Password

Confirm Password

62. Click **Next** to continue.

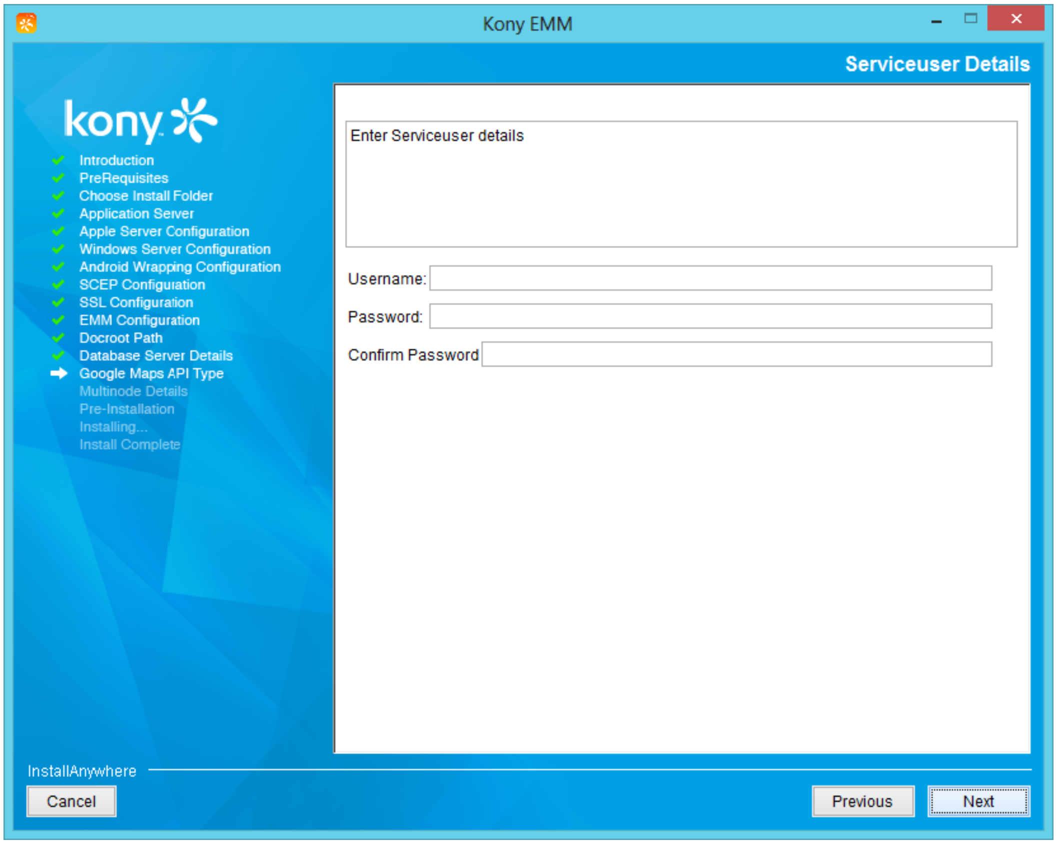
    The **Serviceuser Details** window appears.

63. Enter details for the following fields:

    - **Username**: Enter the service user name.
    - **Password**: Enter a password.

- **Confirm Password**: Reenter the password to confirm it.

> *Important:* A service user manages the services. The service user should be present on system. The EMM Installer will not create the service user.



Enter Serviceuser details

Username:

Password:

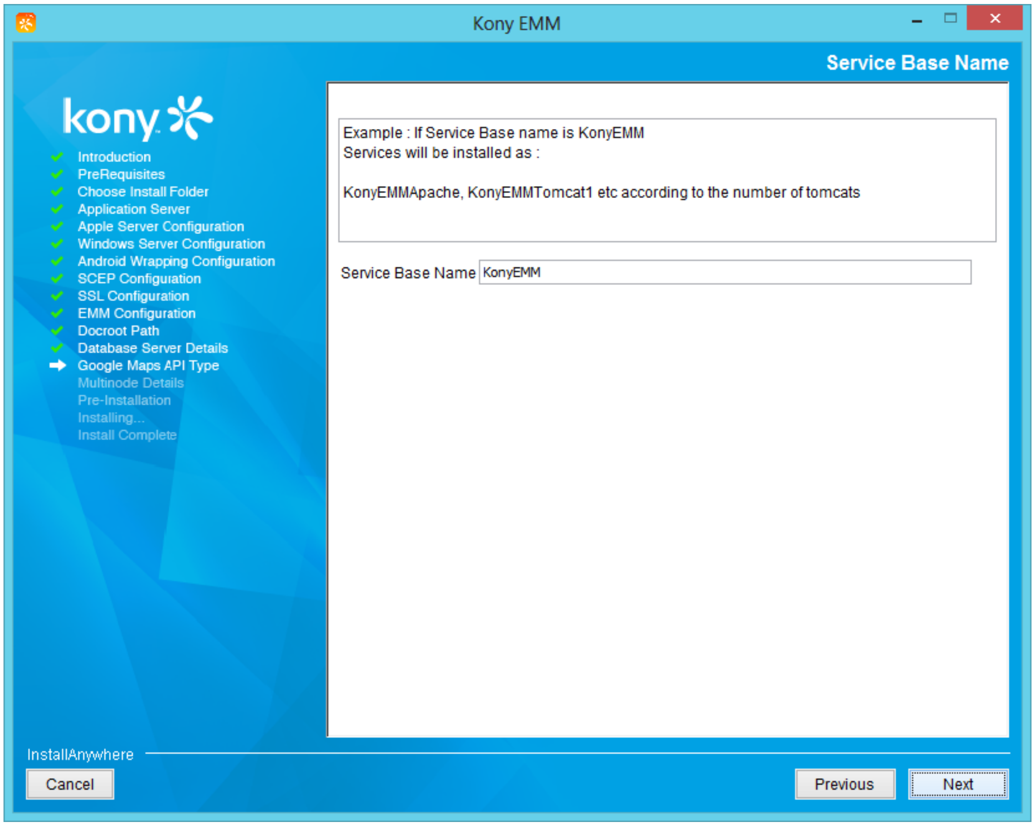
Confirm Password

64. Click **Next** to continue.

    The **Please Wait** window appears, alerting the user that Kony EMM configuration is in progres.

    The **Service Base Name** window appears.

> *Note:* Based on the service base name, services are installed. For example, if the service base name is KonyEMM , then services are installed as KonyEMMApache or KonyEMMTomcat1 and so on according to the number of Tomcat servers.



Example : If Service Base name is KonyEMM
Services will be installed as :

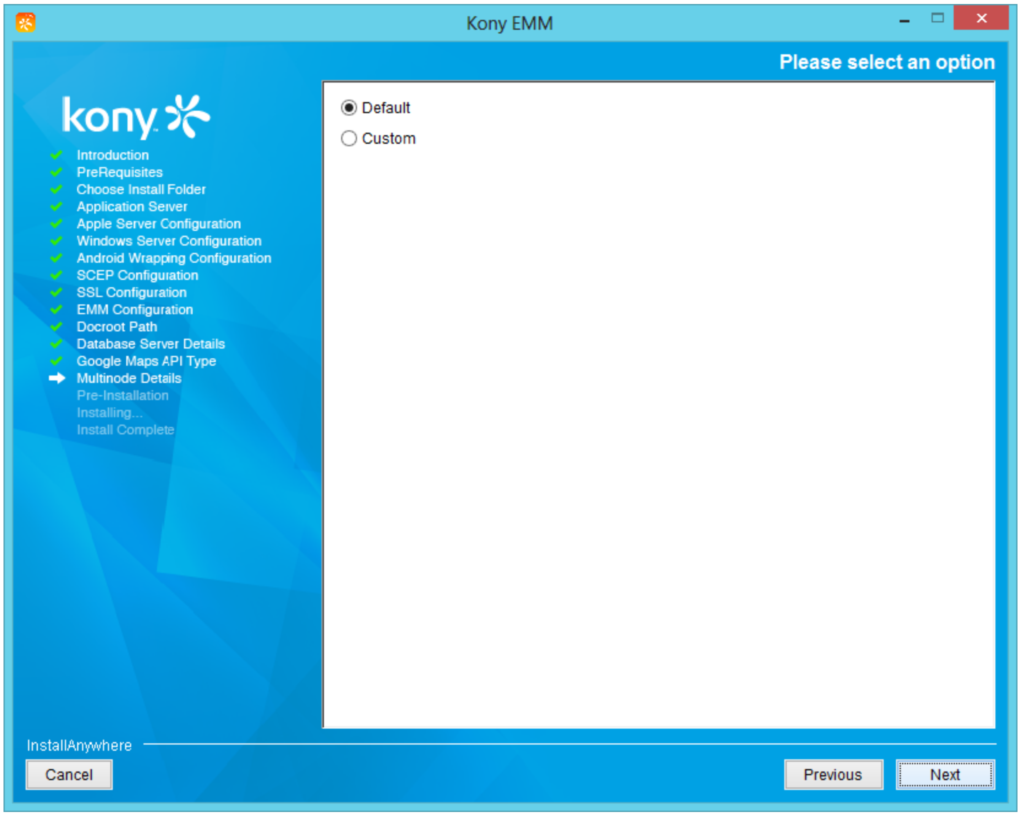
KonyEMMApache, KonyEMMTomcat1 etc according to the number of tomcats

Service Base Name: KonyEMM

65. Click **Next** to continue.

    The **Please select an option** window appears

66. For single node installation, select the **Default** option. To customize the default setup, select the **Custom** option for multinode installation.



● Default
○ Custom

67. Click **Next** to continue.

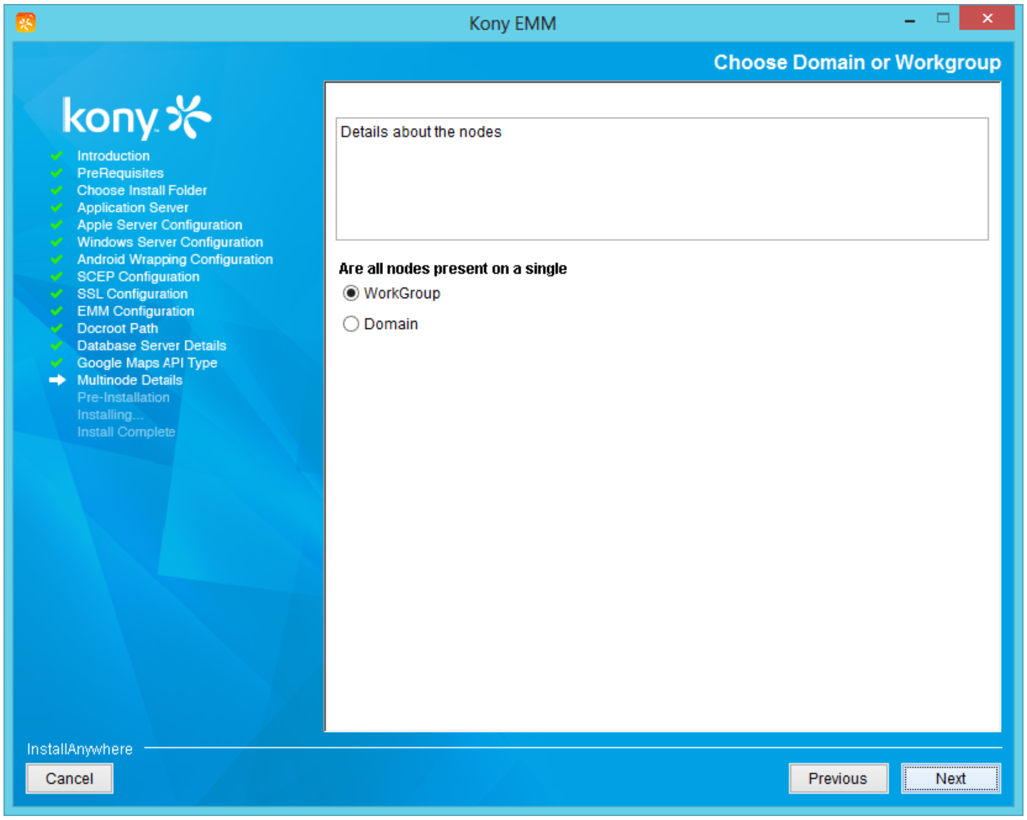
12.1.1 Multinode Installation

> ***Important:*** Before you go ahead with multi-node installation, ensure that User Account Control (UAC) is disabled on all the nodes you want to install Kony Management suite on. If you do not disable UAC, you may encounter UAC validation error. For information on how to disable UAC, see Microsoft documentation or see opensource documentation.

> *Important:* Windows multi-node installation needs Powershell Remoting to be set up to communicate with other Windows instances. The Powershell Remoting topic is covered under the header about_Remote_Troubleshooting in Microsoft help topics. Users need to enable Powershell Remoting before using the EMM installer for multi-node installation on Windows.

The **Choose Domain or WorkGroup** window appears.

68. Based on the availability of all nodes in a single **WorkGroup** or **Domain**, select the **WorkGroup** or **Domain** option.By default the option is set to **WorkGroup**.



Details about the nodes

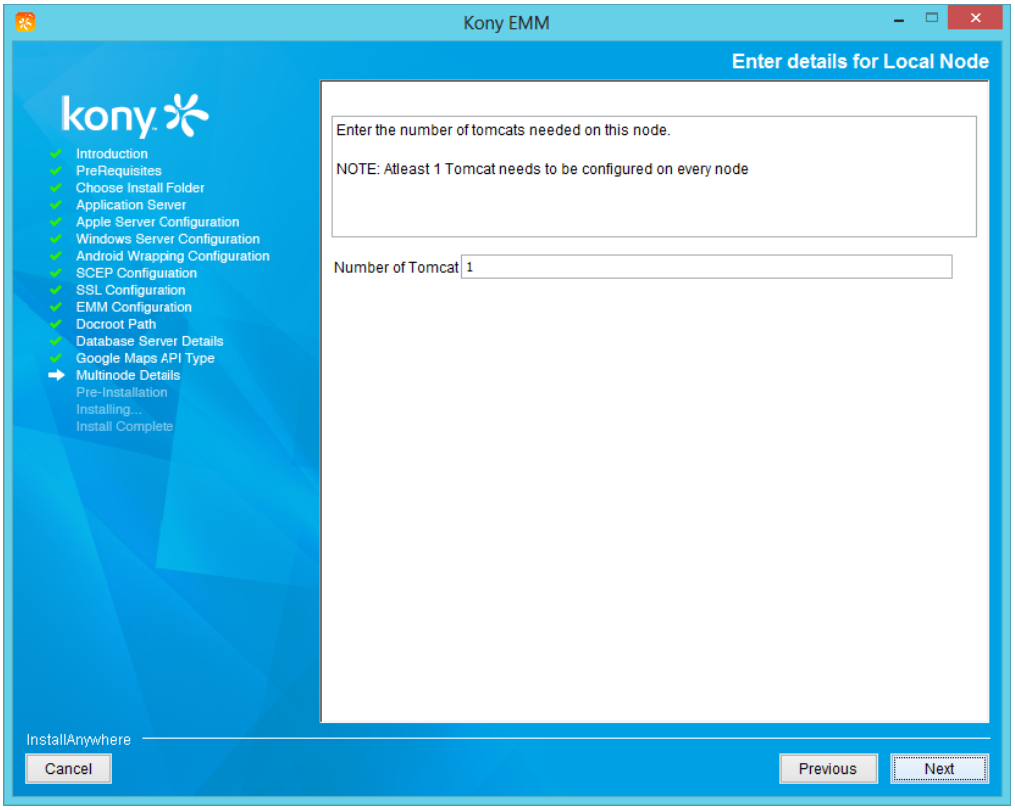
Are all nodes present on a single

● WorkGroup

○ Domain

The **Enter details for Local Node** window appears.

69. Enter the number of Tomcat servers you need to configure on local box in **Number of Tomcat**.



Enter the number of tomcats needed on this node.

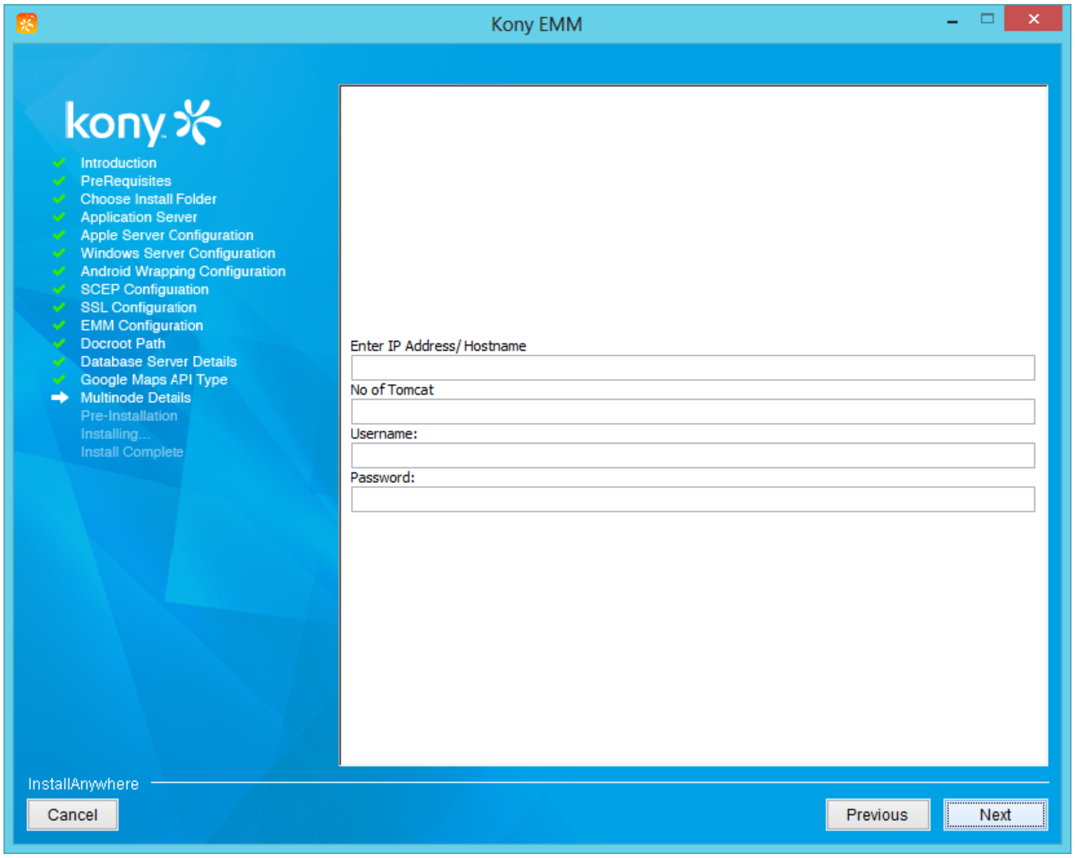
NOTE: Atleast 1 Tomcat needs to be configured on every node

Number of Tomcat 1

70. Click **Next** to continue.

71. Enter the details for the following fields:

- **Enter IP Address**: Enter the private IP address of the remote node.
- **Number of Tomcat**: Enter the number of Tomcat servers servers that you need to configure on specific node.
- **Username**: Enter the user name of the remote systems.
- **Password**: Enter user password of the remote systems.



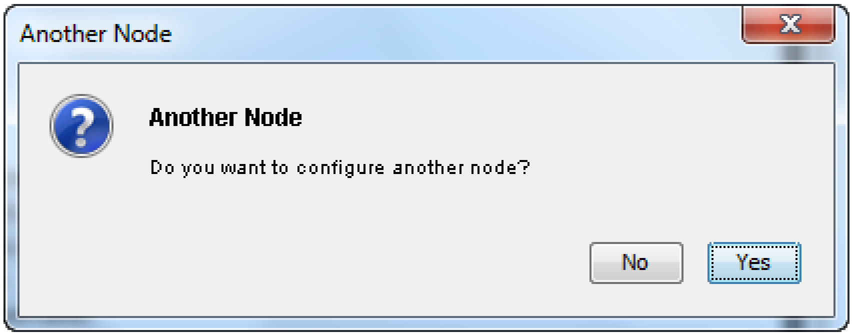
Enter IP Address/ Hostname

No of Tomcat

Username:

Password:

Once the configuration is complete, system displays the **Another Node** dialog, asking if the administrator wants to configure an additional node.



Another Node

Do you want to configure another node?

72. If you want to configure an additional node, click **Yes** to continue.

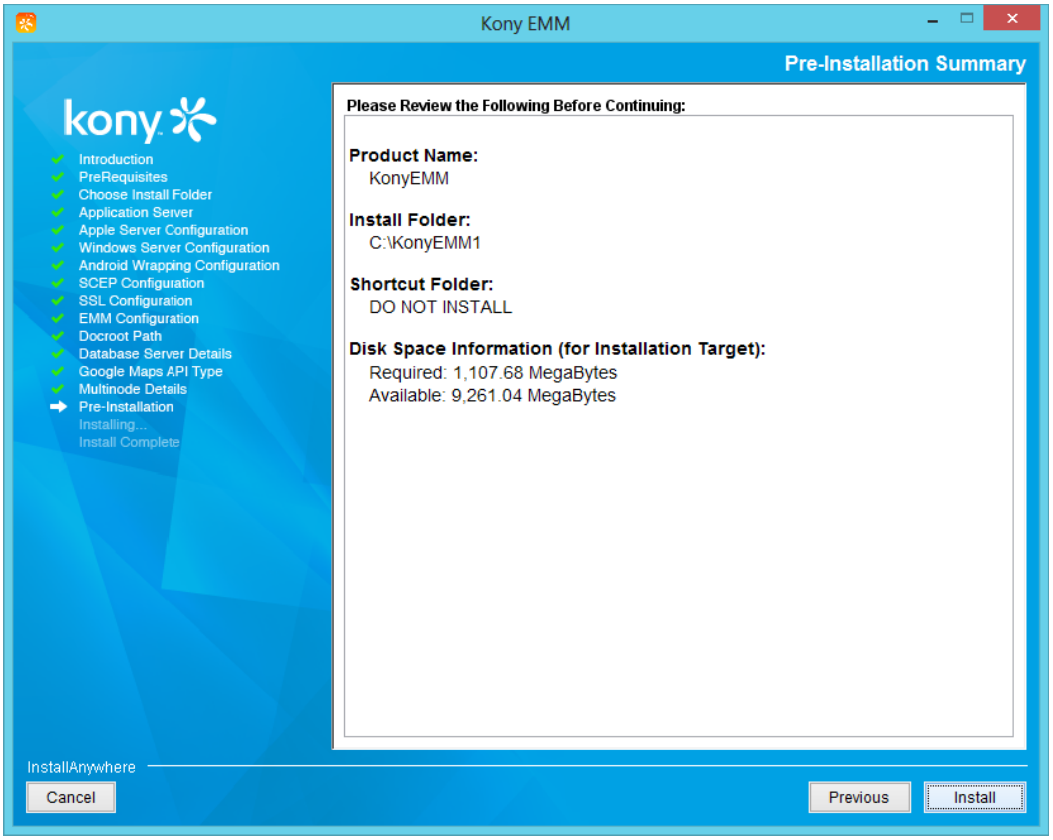
    The system displays the entry fields to enter details for the additional Tomcat Server configuration. Once the configuration is complete, the system again displays the **Another Node** dialog, asking if the administrator wants to configure an additional node.

73. Select **No** if the multinode configuration is complete.

74. Click **Next** to continue.

    The **Pre-Installation Summary** window appears.

75. Review the details provided for installing the EMM Server. If you want to change other settings, you can click **Previous**, to navigate to the window, where the modification is required.



Please Review the Following Before Continuing:

Product Name:
KonyEMM

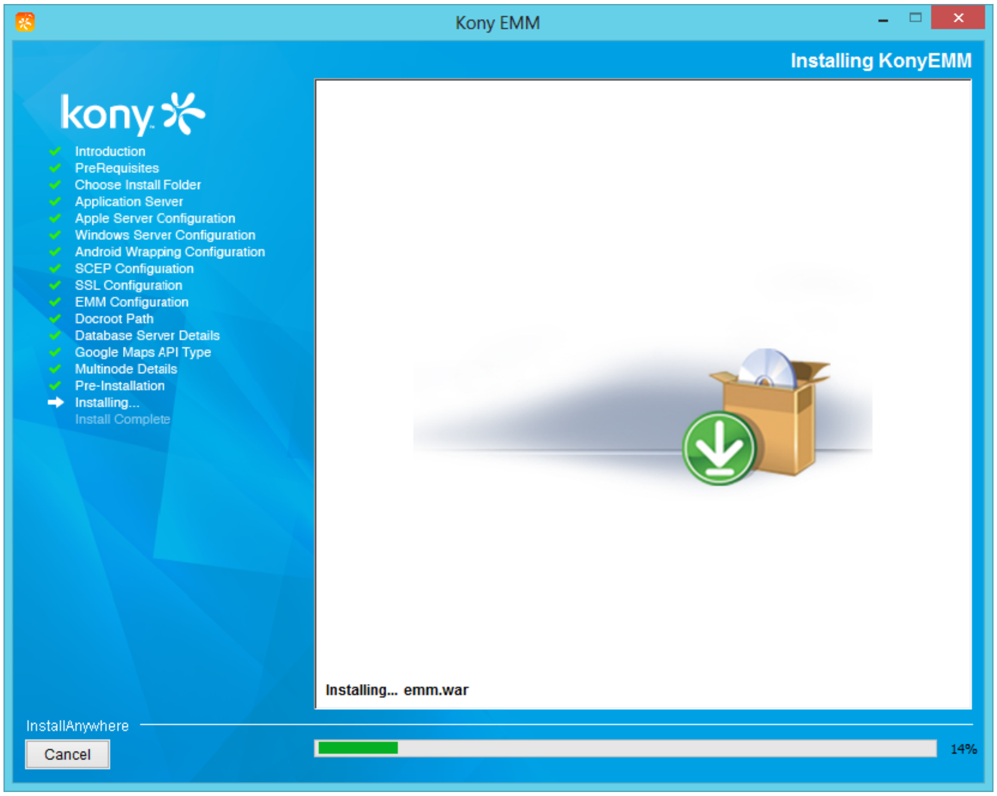
Install Folder:
C:\KonyEMM1

Shortcut Folder:
DO NOT INSTALL

Disk Space Information (for Installation Target):
Required: 1,107.68 MegaBytes
Available: 9,261.04 MegaBytes

76. Click **Install** to continue.

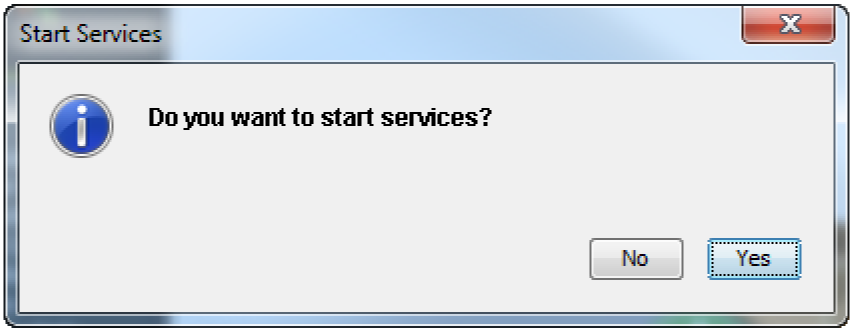
    The **Installing Kony EMM** window appears. It displays the installation in progress message.



Installing... emm.war

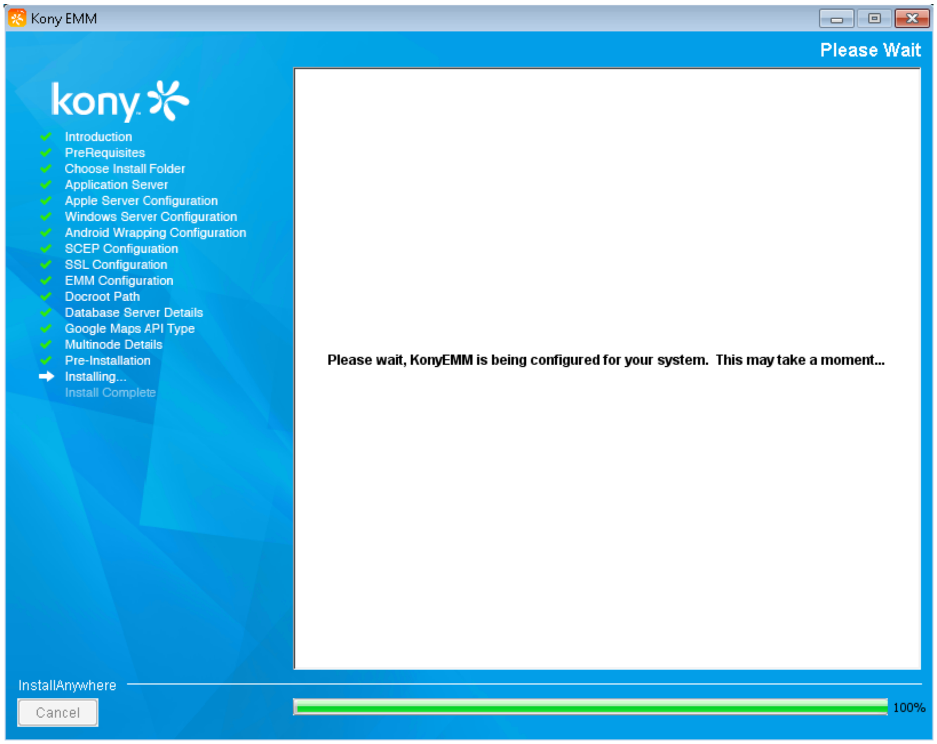
77. After installation, the **Start Services** dialog appears, asking to start services.

78. Click **Yes** to continue.



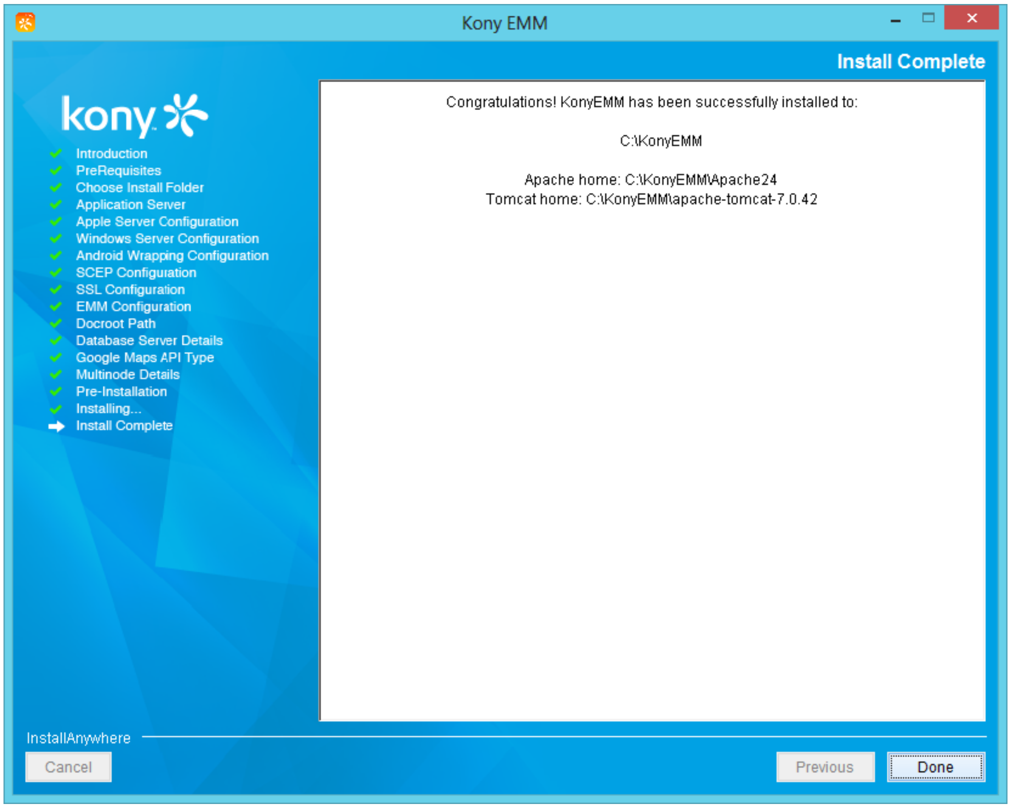
Do you want to start services?

The **Please Wait** window appears. It displays the installation in progress message.



Please wait, KonyEMM is being configured for your system. This may take a moment...

79. Once the installation completes, the **Install Complete** window appears with the confirmation message.



Congratulations! KonyEMM has been successfully installed to:

C:\KonyEMM

Apache home: C:\KonyEMM\Apache24
Tomcat home: C:\KonyEMM\apache-tomcat-7.0.42

80. Click **Done** to close the window.

12.2 EMM - Upgrade Installation

This section explains the upgrade procedure on a Windows platform.

Based upon the type of installation you have, the upgrade procedure is two types.

- Automated Installation (Single node, multi-node)
- Manual Multi-node Installation

> *Important:* After upgrading from one version of Kony Management Suite to another version of Kony Management Suite, ensure that all Enterprise Apps (that launch directly from the springboard) are re-wrapped and updated on user devices. If you do not re-wrap, app will not launch.

Follow these steps to upgrade your Kony Management Suite for Windows. It ensures service interruption is kept to a minimum and safeguards all the tools to restore your original installation in case of a failure.

> *Important:* You need to upgrade Kony Management suite (EMM) installation from the master node.

> *Important:* Before you go ahead with multi-node upgrade, ensure that User Account Control (UAC) is disabled on all the nodes you want to upgrade Kony Management suite on. If you do not disable UAC, you may encounter UAC validation error. For information on how to disable UAC, see Microsoft documentation or see opensource documentation.

> *Important:* Windows multi-node installation needs Powershell Remoting to be set up to communicate with other Windows instances. The Powershell Remoting topic is covered under the header about_Remote_Troubleshooting in Microsoft help topics. Users need to enable Powershell Remoting before using the EMM installer for multi-node installation on Windows.

12.2.1 Automated Installation (Single node, multi-node)

Prerequisites

- You can download the EMM Installer from http://community.kony.com/downloads/manual with your credentials. Navigate to the Kony Management section and click on the specific release related files you want to download. For example, if you want to download Kony Management 3.0, click on the Kony v3.0 GA tab.

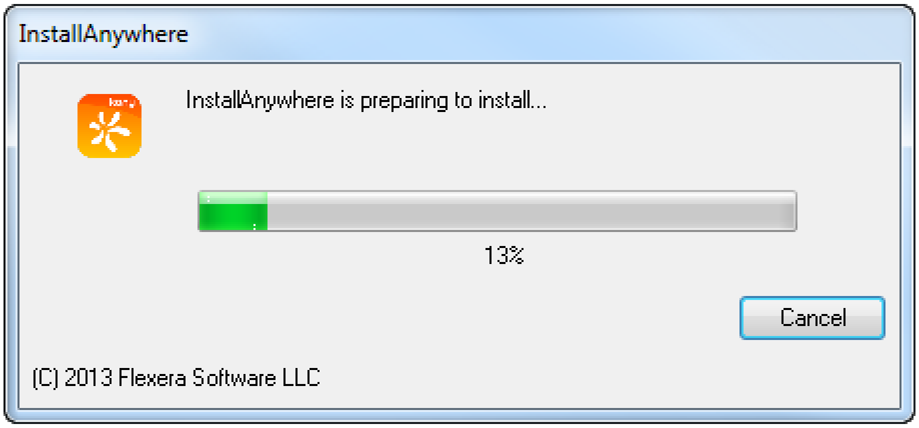
- Ensure that you have a previous version of EMM installed.
- Ensure that `KonyEMM.exe (x.x)` file has execute permission.

To upgrade Kony EMM for Windows, follow these steps:

1. Execute the KonyEMM.exe file as an administrator.Files required for the EMM Console installation are extracted.

   > ***Note:*** Ensure that firewall /anti-virus allows to execute the file.

2. The **InstallAnywhere** dialog appears.The **InstallAnyWhere** dialog displays information about the progress of the software installation at run time.

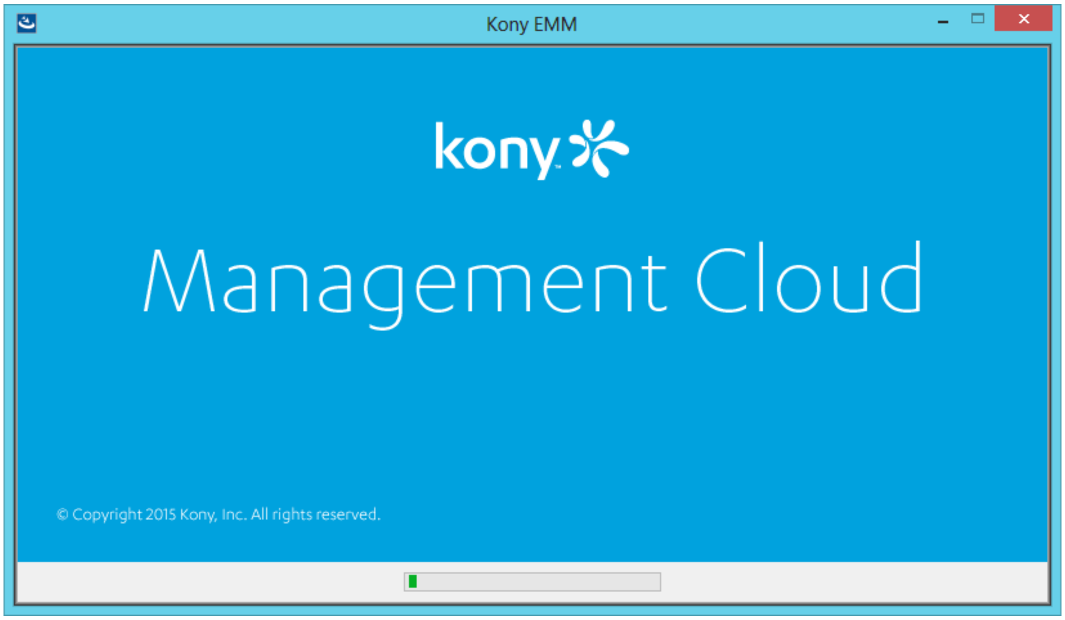
   InstallAnywhere

   InstallAnywhere is preparing to install...

   13%

   (C) 2013 Flexera Software LLC

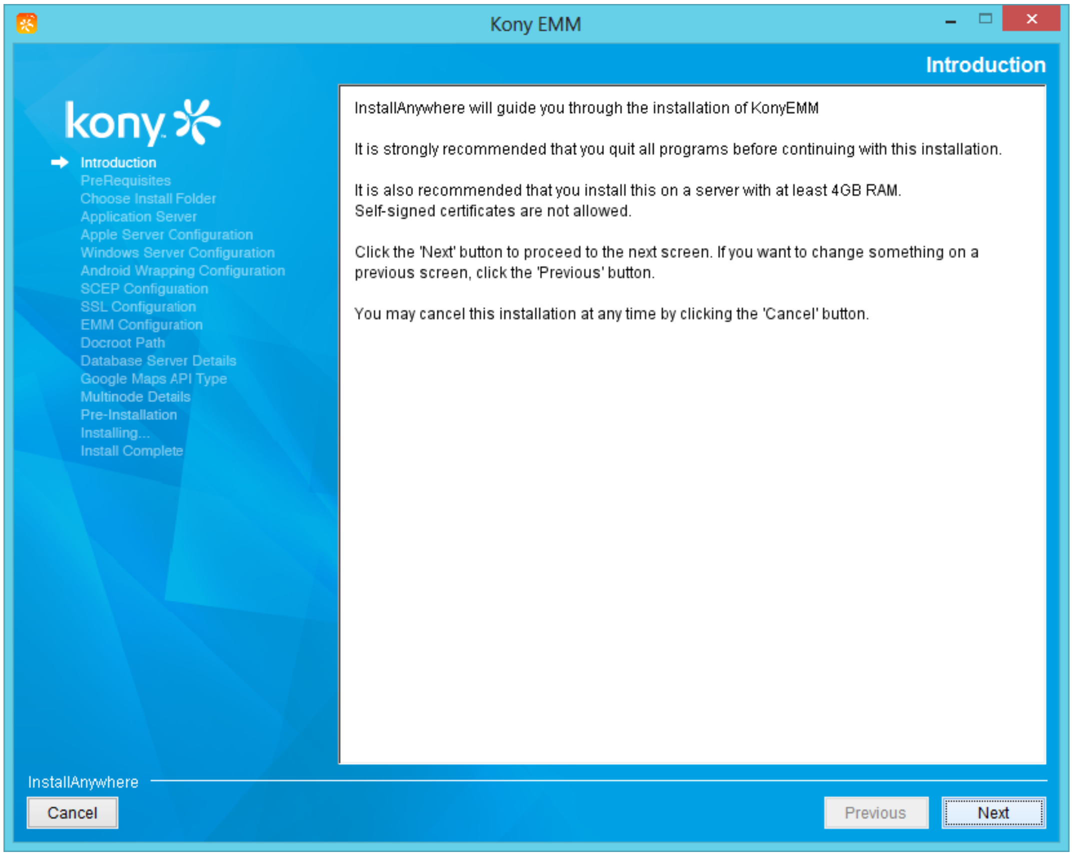
   A dialog with Kony logo appears.



© Copyright 2015 Kony, Inc. All rights reserved.

3. Click **Next** to continue.

4. Read the instructions carefully before installing Kony EMM.



InstallAnywhere will guide you through the installation of KonyEMM

It is strongly recommended that you quit all programs before continuing with this installation.

It is also recommended that you install this on a server with at least 4GB RAM.
Self-signed certificates are not allowed.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

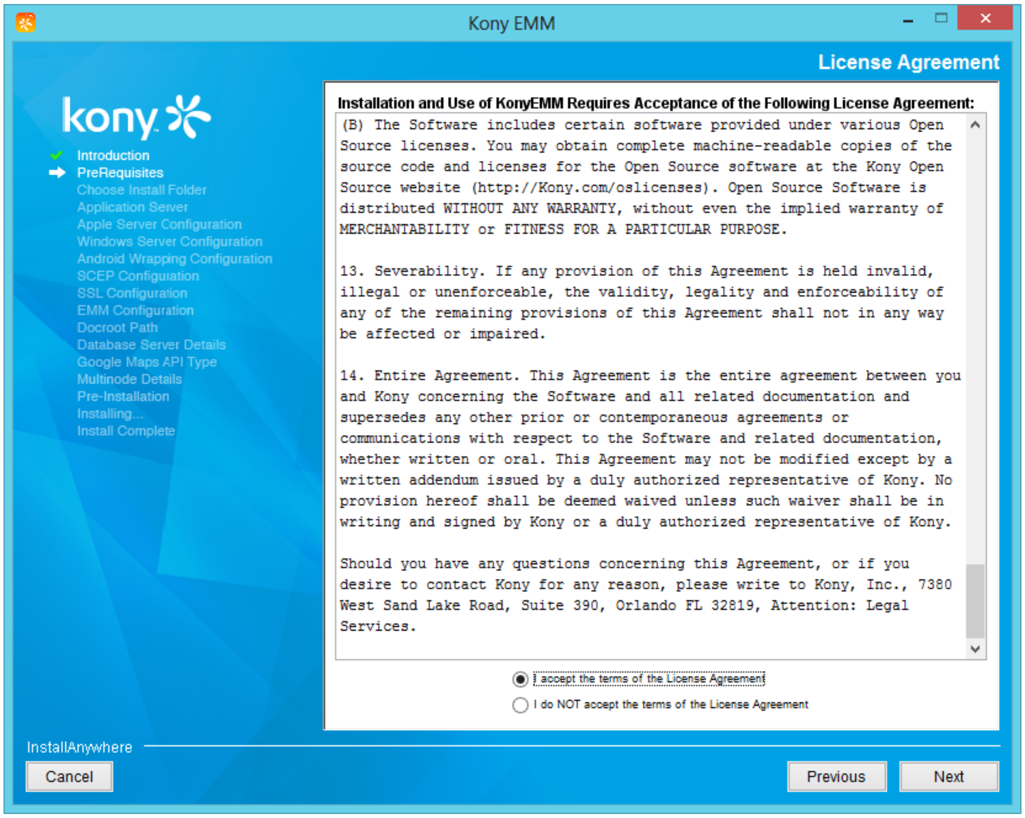
You may cancel this installation at any time by clicking the 'Cancel' button.

5. Click **Next** to continue.

   The **License Agreement** window appears.

6. Select the **I accept the terms of the License Agreement** option.

> ***Note:*** To activate the License Agreement option, carefully read the entire text.



Installation and Use of KonyEMM Requires Acceptance of the Following License Agreement:

(B) The Software includes certain software provided under various Open Source licenses. You may obtain complete machine-readable copies of the source code and licenses for the Open Source software at the Kony Open Source website (http://Kony.com/oslicenses). Open Source Software is distributed WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

13. Severability. If any provision of this Agreement is held invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions of this Agreement shall not in any way be affected or impaired.

14. Entire Agreement. This Agreement is the entire agreement between you and Kony concerning the Software and all related documentation and supersedes any other prior or contemporaneous agreements or communications with respect to the Software and related documentation, whether written or oral. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of Kony. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by Kony or a duly authorized representative of Kony.

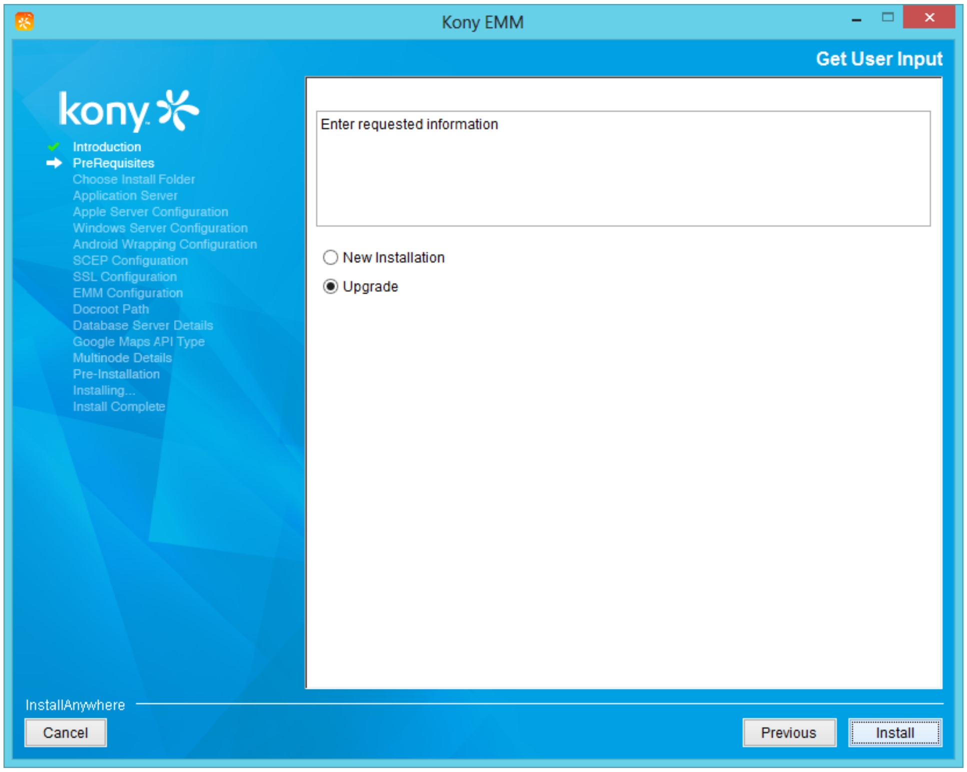
Should you have any questions concerning this Agreement, or if you desire to contact Kony for any reason, please write to Kony, Inc., 7380 West Sand Lake Road, Suite 390, Orlando FL 32819, Attention: Legal Services.

● I accept the terms of the License Agreement
○ I do NOT accept the terms of the License Agreement

7. Click **Next** to continue.

   The **Get User Input** window appears.

8. Select the **Upgrade** option. By default, it is set to **New** Installation.



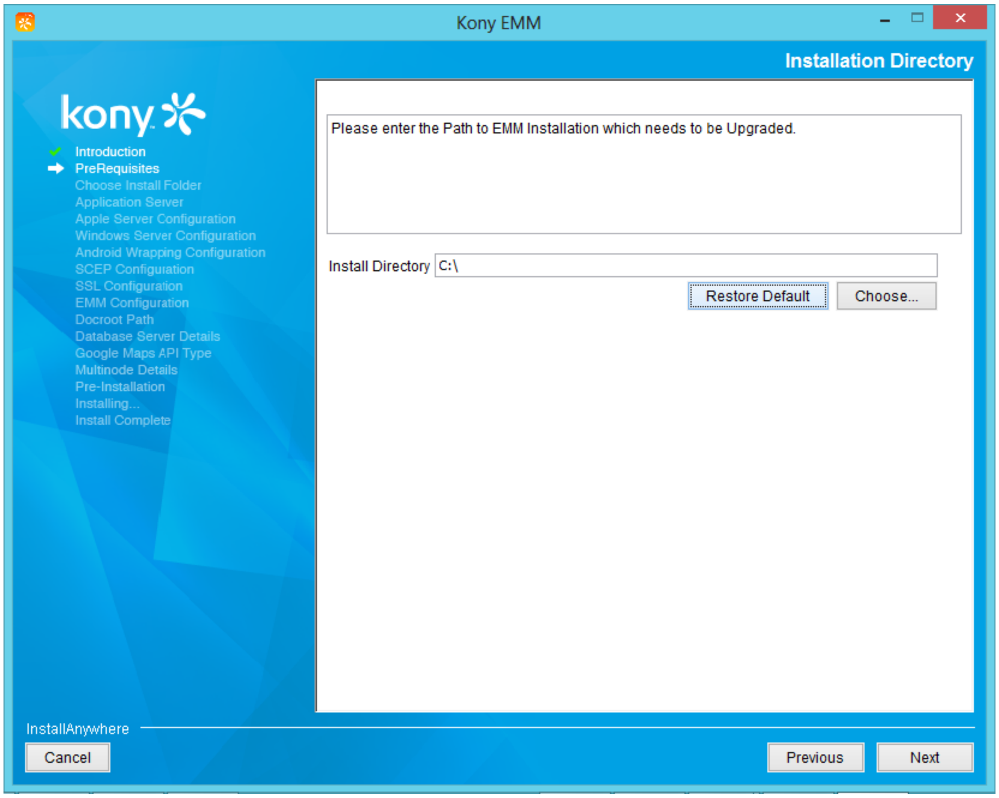
Enter requested information

○ New Installation
● Upgrade

9. Click **Next** to continue.

   The **Installation Directory** window appears.

10. Click **Choose** to browse the required folder from your system, or enter the path for the EMM Installation that needs to be upgraded.

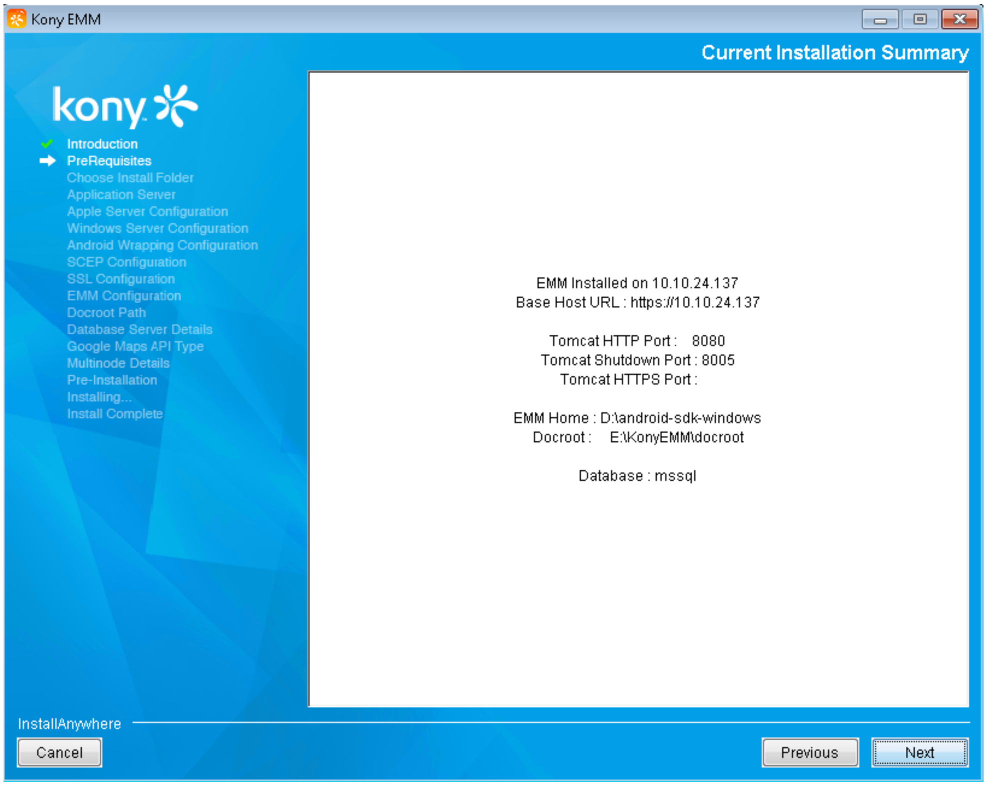


Please enter the Path to EMM Installation which needs to be Upgraded.

Install Directory C:\

11. Click **Next** to continue.

    The **Current Installation Summary** window appears.



EMM Installed on 10.10.24.137
Base Host URL : https://10.10.24.137

Tomcat HTTP Port : 8080
Tomcat Shutdown Port : 8005
Tomcat HTTPS Port :

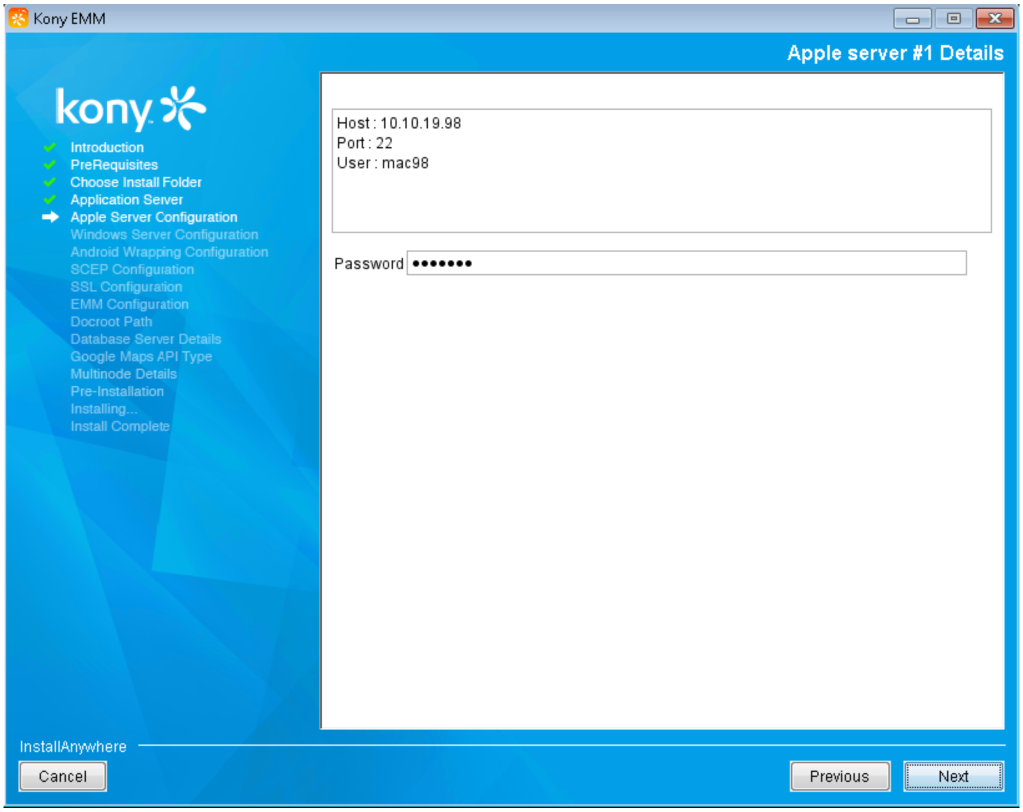
EMM Home : D:\android-sdk-windows
Docroot : E:\KonyEMM\docroot

Database : mssql

12. Click **Next** to continue.

The **Please Wait** window appears, informing a user that KonyEMM configuration is in progress

The **Apple server #1 Details** window appears.



Host : 10.10.19.98
Port : 22
User : mac98

Password •••••••

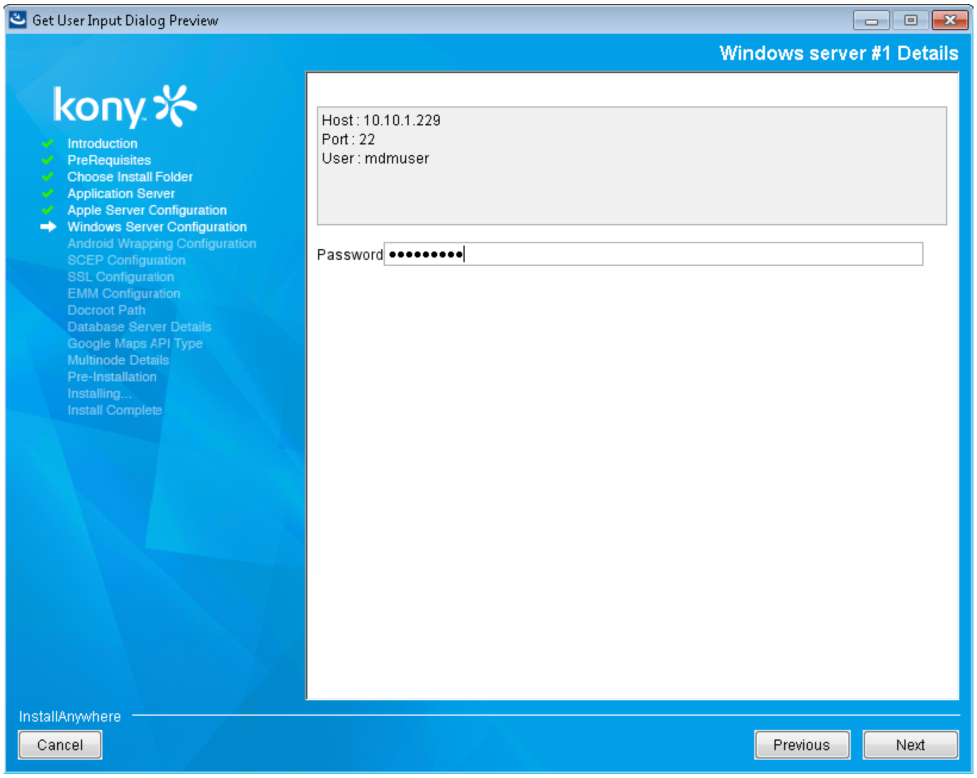
13. Enter the password.

14. Click **Next** to continue.

    The **Please Wait** window appears, informing a user that KonyEMM configuration is in progress.

    The **Windows Server #1 Details** window appears.

15. Enter the password.



Host : 10.10.1.229
Port : 22
User : mdmuser

Password •••••••••

16. Click **Next** to continue.

The SCEP Configuration window appears. All the certificates required by iOS devices during enrollment are distributed through the SCEP server. If you select the No option,, then you will not be able to enroll any iOS devices.

> ***Note:*** The SCEP configuration option appears only when the user has enabled the iOS wrapping and or Android wrapping.

> ***Note:*** If you do not select Enable Android Wrapping, then EMM cannot provide support to Android devices.If Android wrapping is supported, then choose the parent directory of Android SDK.

17. Enter details for the following fields:

a. SCEP Server URL

b. SCEP Keysize

c. SCEP Common Name

d. SCEP CA Instance Name

e. SCEP Challenge URL

f. SCEP CA Domain (Optional)

g. SCEP CA Username

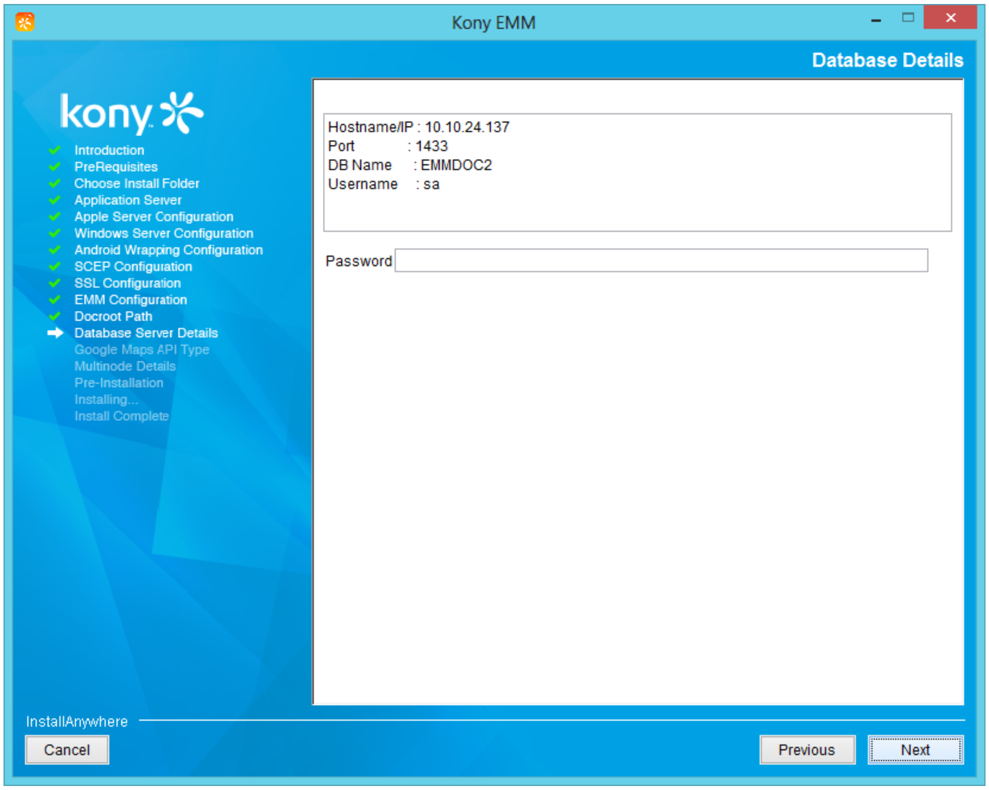
h. SCEP CA Password

18. Click **Next** to continue.

    The **Please Wait** window appears, informing a user that KonyEMM configuration is in progress.

    The **Database Details** window appears.

19. Enter the password.



Hostname/IP : 10.10.24.137
Port : 1433
DB Name : EMMDOC2
Username : sa

Password

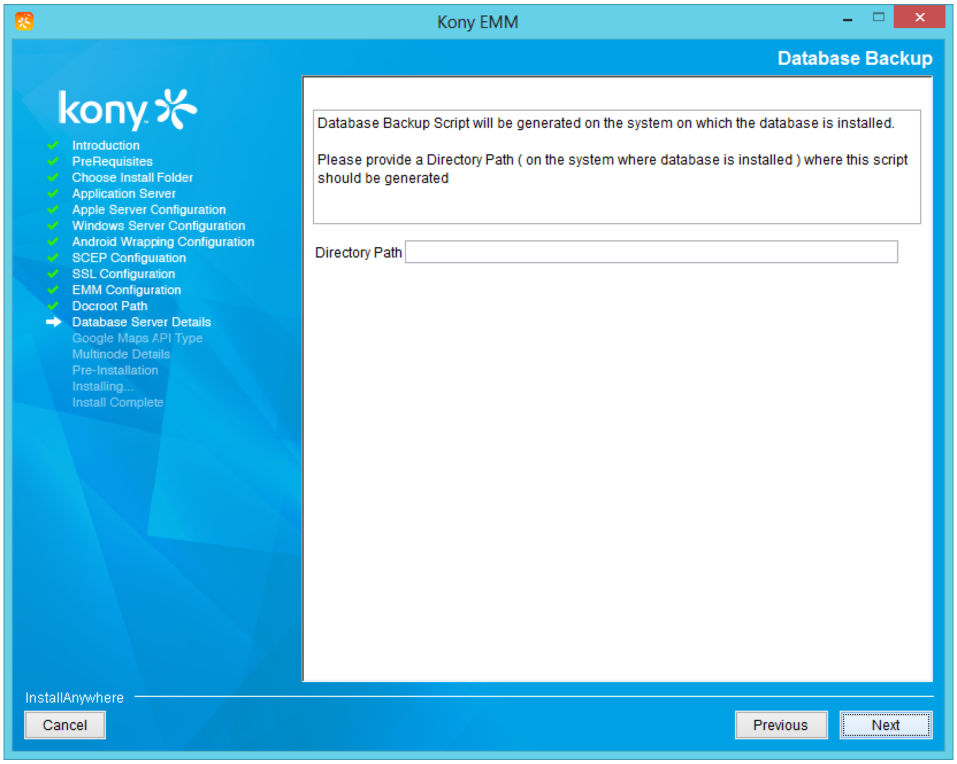
20. Click **Next** to continue.

> ***Important:*** System initiates the database backup process. Dump command is mandatory for taking backup of database(s) through installer. If database dump command is not found, restart the upgrade process with this command in path or take database backup manually.

The **Please Wait** window appears, informing a user that KonyEMM configuration is in progress.

The **Database backup** window appears.

21. Enter the directory path.



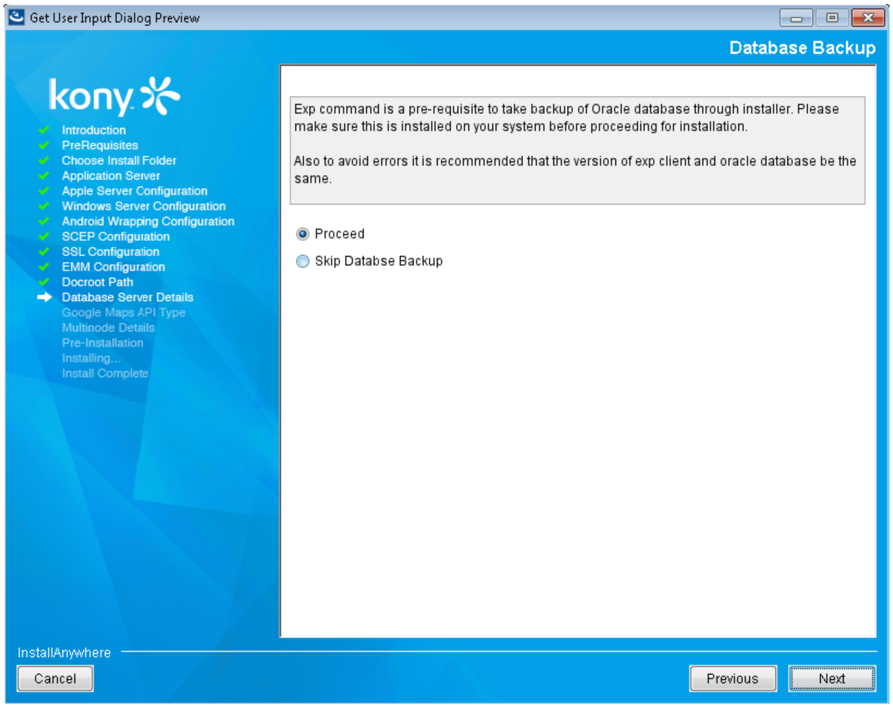
Database Backup Script will be generated on the system on which the database is installed.

Please provide a Directory Path (on the system where database is installed) where this script should be generated

Directory Path

22. Click **Next** to continue.

23. The **Database Backup** window appears asking if to proceed or stop the backup process.



Exp command is a pre-requisite to take backup of Oracle database through installer. Please make sure this is installed on your system before proceeding for installation.

Also to avoid errors it is recommended that the version of exp client and oracle database be the same.

● Proceed

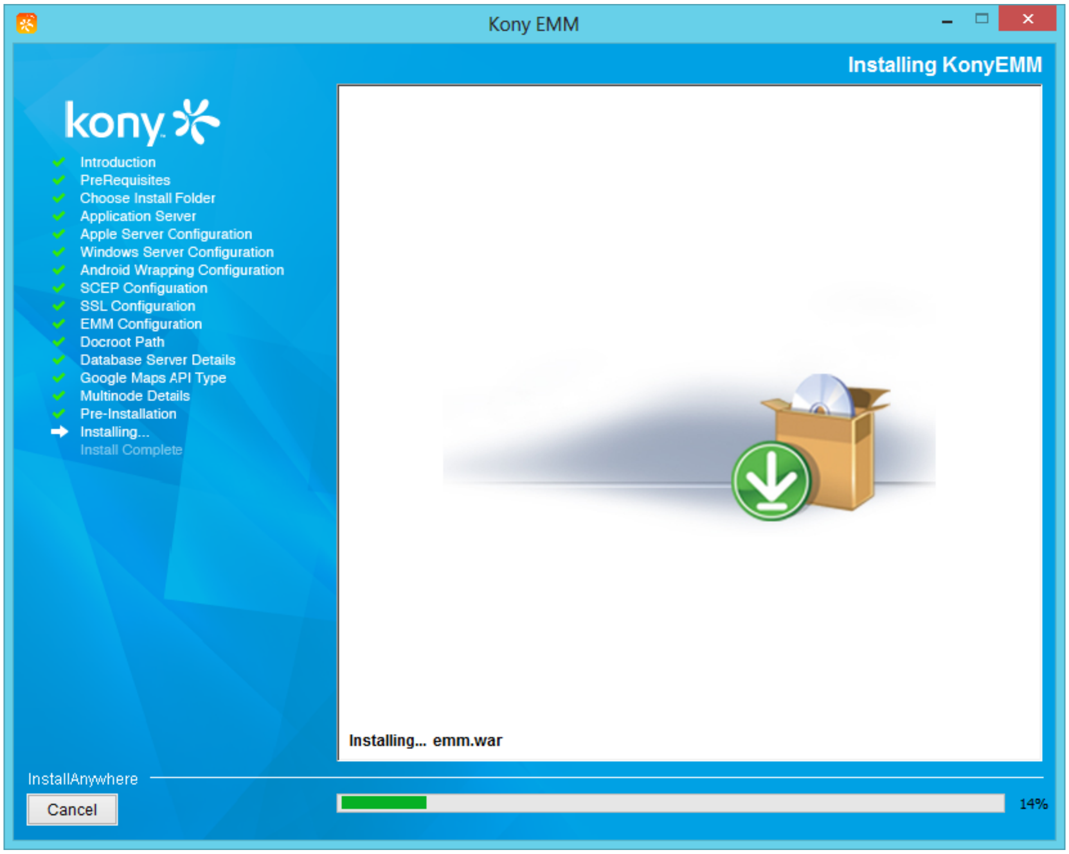
○ Skip Databse Backup

24. Click **Next** to continue.

    The **Please Wait** window appears, informing a user that KonyEMM configuration is in progress.

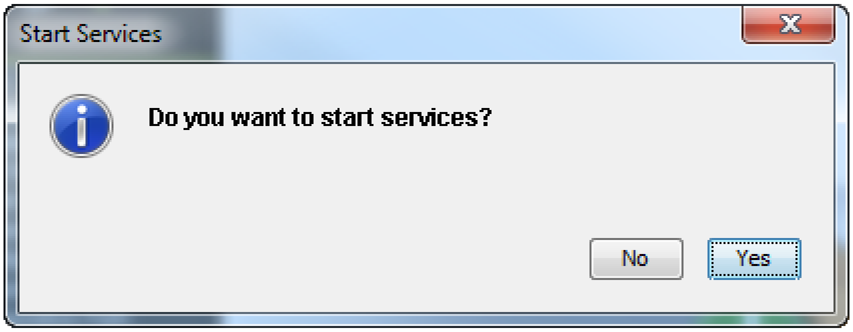
25. Click **Install** to continue.

    The **Installing Kony EMM** window appears.



Installing... emm.war

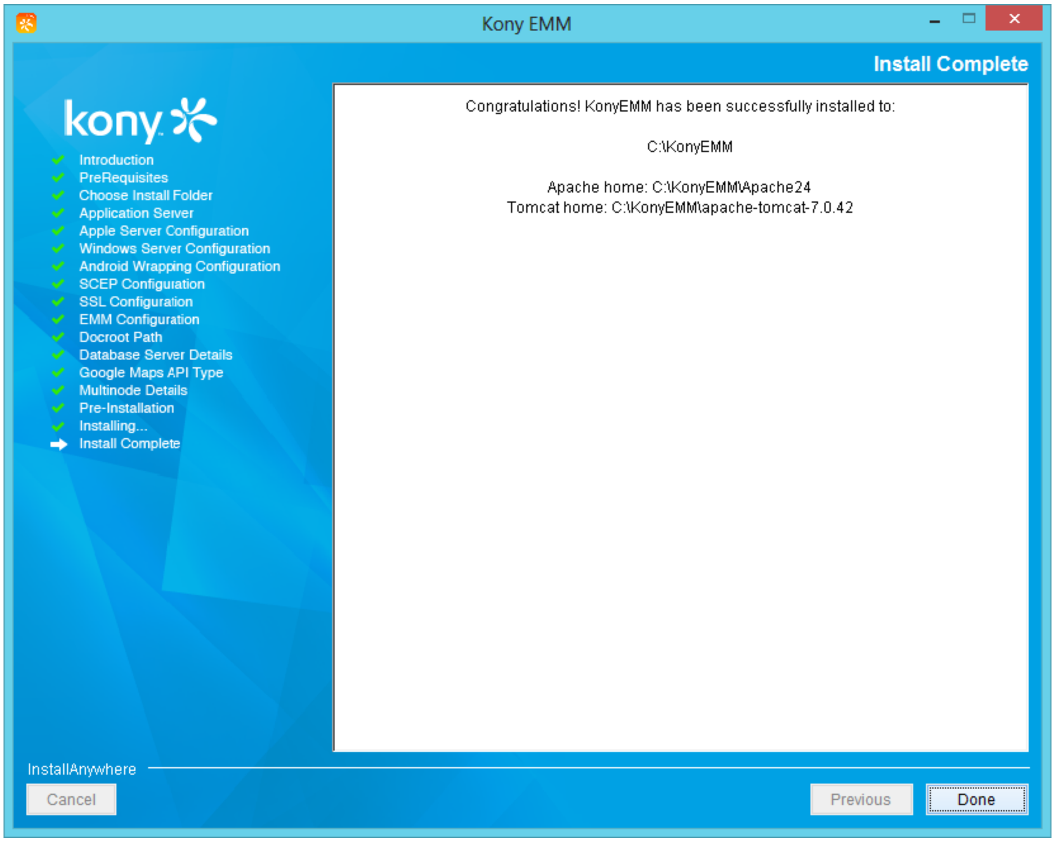
The **Start Services** dialog appears, asking, if you want to start services?



Do you want to start services?

26. Click **Yes** to continue.

27. Once the installation completes, the **Install Complete** window appears with the confirmation message.



Congratulations! KonyEMM has been successfully installed to:

C:\KonyEMM

Apache home: C:\KonyEMM\Apache24
Tomcat home: C:\KonyEMM\apache-tomcat-7.0.42

28. Click **Done** to close the window.

> ***Important:*** If you are upgrading to 3.5 and DB is MSSQL, replace the entry below in the catalina.properties file.
>
> Old: HIBERNATE.DIALECT=org.hibernate.dialect.SQLServer2008Dialect
>
> New: HIBERNATE.DIALECT=com.kony.persistence.hibernate.core.EMMSQLServerDialect

Once you have upgraded the EMM server, upgrade the Launchpad app in the EMM management console. For more information, see Post Upgrade Tasks.

12.2.2 Manual Multi-node Installation

Upgrading Multi-node installation/instance involves six different steps.

- Download artifacts
- Stop Services
- Backup files
- Place downloaded files in appropriate folders
- Run DB scripts
- Restart Servers

> *Important:* To add the Windows App management feature, you need to setup Windows 2012 Server. See the Windows 2008 2012 Server setup section for more details.

> *Important:* For Windows multi-node installation, systems are recommended to be present in the same network.

12.2.2.1 Download artifacts

Download the artifacts below in a zip format from Kony.You may have to login using your kony developer portal login credentials. You can find all artifacts under **EMM multi-node upgrade artifacts** section.

- emm.war
- emm_static.zip
- wrap-android.zip
- wrap-ios.zip
- dbscripts.zip
- apps.zip

12.2.2.2 Stop services

You need to stop the following servers that are relevant for this upgrade.

- Tomcat Service
- Apache Service
- Memcached Service

The preferred sequence is to stop Apache first, followed by Tomcat and Memcached.

12.2.2.3 Backup of all relevant files and folders

Back up your files before replacing them, in case errors occur during the upgrade. Rename all files and folders with an extension **upgrade_backup**.

Navigate to `/<Installation Folder>`, make another copy of the **docroot** folder and rename it as **docroot_upgrade_backup**.

> ***Important:*** You will not be able to rollback the upgrade if you do not backup your files and folders.

12.2.2.4 Placing files and folder at appropriate locations

> ***Important:*** You should replace files and folders in all your nodes (individual servers)

You must place all downloaded files in their appropriate locations.

- emm.war (`/<Installation Folder>/apache-tomcat-7.0.42/webapps`)
- emm_static.zip (`/<Installation Folder>/emm-static`)
- Wrap-android.zip (`<EMM_HOME>/emm_config/`)
- wrap-ios.zip (`<User_HOME>/wrap-ios folder`)

- dbscripts.zip
- apps.zip

Replace emm.war, emm_static.zip,wrap-android.zip, and wrap-ios.zip files in their respective locations.

For emm.war

1. Copy the **emm.war** file from the location you have downloaded the files.
2. Navigate to `/<Installation Folder>/apache-tomcat-7.0.42/webapps` folder.
3. Place the **emm.war** file in it.

For emm_static.zip

1. Copy the **emm_static.zip** file from the location you have downloaded the files.
2. Unzip **emm_static.zip** in the `/<Installation Folder>/emm-static` folder

For wrap-android.zip

1. Extract the **wrap-android.zip** file
2. Copy **KONY_POLICYINJECT_ANDROID**, **tools**, and **tools-mac** folders from the extracted files.
3. Navigate to `<EMM_HOME>/emm_config/`, and place all copied files in the *emm_config* folder.You must not modify any other files or folders in the *emm_config* folder.

For Wrap-ios.zip

On your MAC machine,

1. Copy the **wrap-ios.zip** file from the location you have downloaded the files.
2. Navigate to `<User_HOME>/wrap-ios` folder and unzip the **wrap-ios.zip** in it.

3. After unzip, the folder path will be as `<User_HOME>/wrap-ios/EMM-GA-2.5.5`

4. Navigate to `<User_HOME>/wrap-ios/EMM-GA-2.5.5/scripts` and execute the commands below to provide u+x permissions and to convert `.sh files` and make them compatible with linux using dos2unix tool.

   `Chmod u+x scriptsInitiation.sh`

   `dos2unix scriptsInitiation.sh`

   `./scriptsInitiation.sh`

For wrap-win.zip

On your Windows 2012 server machine,

1. Copy the wrap-win.zip file from the location where you downloaded the files.

2. Navigate to <User_HOME>/folder and extract files from wrap-win.zip. The folder path of extracted files is <User_HOME>/wrap-win/EMM-GA-x.x.

3. From your list of installed programs, open Cygwin terminal.

4. Navigate to `<User_HOME>/wrap-win/EMM-GA-x.x/scripts`. Run the following commands to provide u+x permissions and to convert .sh files and make them compatible with linux using dos2unix tool.

   ```
   Chmod u+x scriptsInitiation.sh
   dos2unix scriptsInitiation.sh
   ./scriptsInitiation.sh
   ```

To Run DB scripts

- Copy **dbscript.zip** file from the location you have downloaded the files.

- Navigate to a folder and unzip the folder.

- Execute .sql files as instructions provided in readme.txt file.

> *Note:* You must execute these .sql files on the schema that was created at the time of previous installation.

> *Important:* If you are upgrading with several releases in between, execute all the .sql files in the order of the releases. For example, if you are upgrading from 2.0 to 2.5.5, then, execute 2.1.1, 2.5, 2.5.1, 2.5.2, 2.5.3, 2.5.4 and 2.5.5.

> *Note:* If your existing installation version is prior to 3.5 release, do not start services from installer, do the following:
>
> In the **catalina.sh** and **catalina.bat** files, add **-D parameter -DMAX_ACTIVE_DBC=100** and **-Dfile.encoding=UTF-8** parameters.
> In the **catalina.properties** file, add **java.security.egd=file:/dev/./urandom**

> *Important:* If you are upgrading to 3.5 and DB is MSSQL, replace the entry below in the catalina.properties file.
> Old: HIBERNATE.DIALECT=org.hibernate.dialect.SQLServer2008Dialect
> New: HIBERNATE.DIALECT=com.kony.persistence.hibernate.core.EMMSQLServerDialect

Update Proxyname

After updating artifacts, you must update proxy name in server.xml and catalina.properties files.

To update proxyname, do the following:

1. Navigate to **<tomcat>/conf/** and open **server.xml** file.
2. Before the **proxyPort** key, add **proxyName="${TOMCAT_PROXY_NAME}".**
3. Save server.xml and close it.

4. Open **catalina.properties** file.

5. Add the key **TOMCAT_PROXY_NAME =<DOCROOT.URL>.**

> ***Important:*** Remove /<webContext>/download from you docroot.url before you provide it to TOMCAT_PROXY_NAME. For example, if your docroot.url is https://yourcompany.net/emm/download. Provide https://yourcompany.net.

To Restart all servers

Once you have completed all the steps as described above, restart all the services that you have stopped. The preferred sequence is Memcached first, then Tomcat and then Apache service/server.

To Upgrade Launchpad

Once all other steps are done, you must upgrade Launchpad to ensure smooth functioning on the device.

Unzip the **apps.zip** folder that you downloaded. It contains binaries of Launchpad in all platforms. Upgrade Launchpad in the Enterprise Store across all platforms. For more information, see EMM user guide. The request to upgrade Launchpad shall be sent to all enrolled devices.

12.3 EMM Installation - Enabling High Availability

The EMM application is already installed on a single node Windows Server. All the pre-requisites are met and the system is tested and certified to be completely functional. The EMM application must be highly available and a single node is not sufficient. The following steps define how to enable high availability of EMM using multi node setup.

12.3.1 Database

There are no changes to the SQL Server DB.

12.3.2 Android

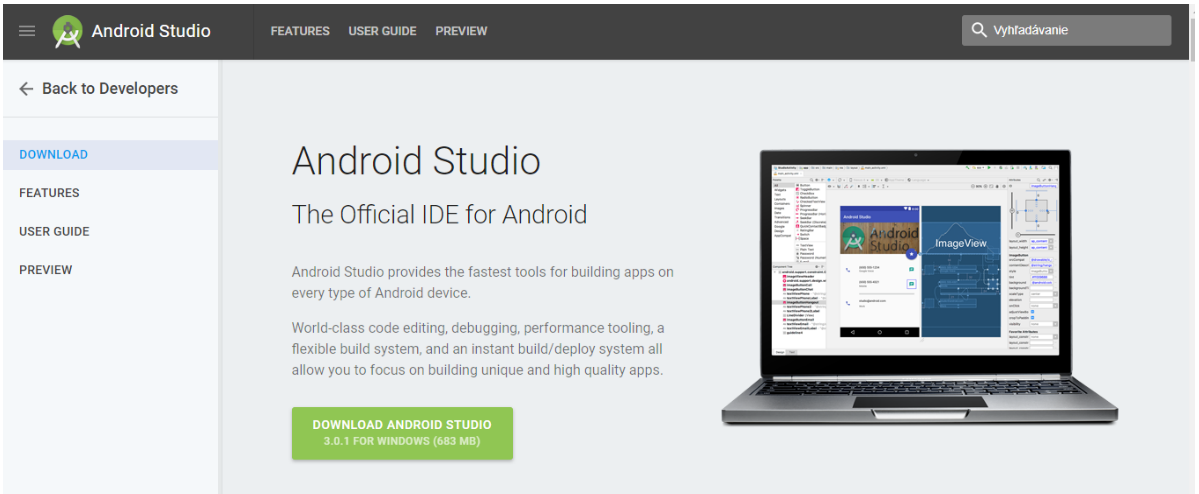
The following procedure explains how to download Android SDK.

12.3.2.1 Windows

To download Android SDK for Windows, follow these steps:

1. Click the link Androd SDK for Windows.

   The Android Studio page appears.



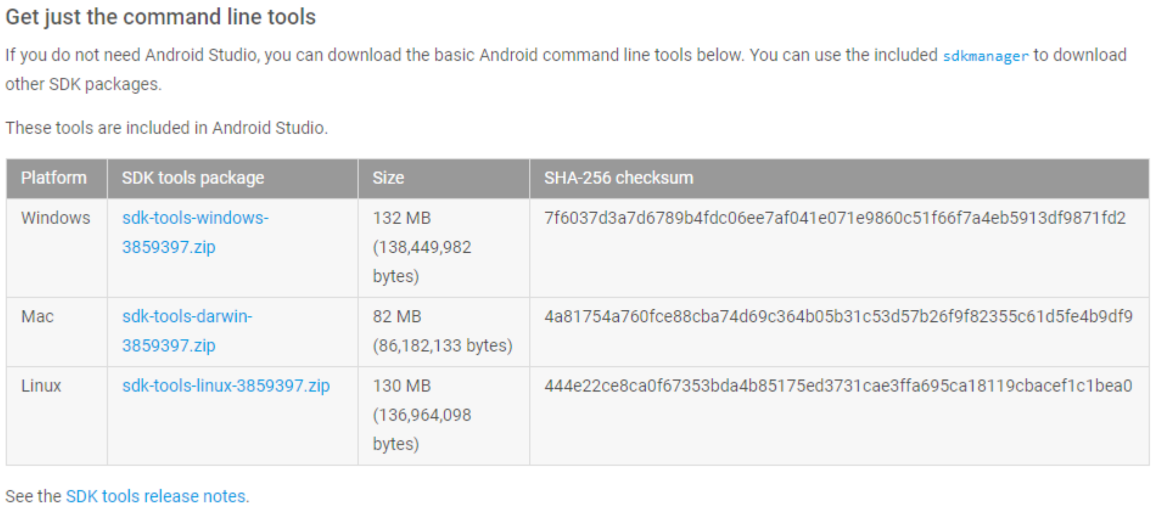
Android Studio

The Official IDE for Android

Android Studio provides the fastest tools for building apps on every type of Android device.

World-class code editing, debugging, performance tooling, a flexible build system, and an instant build/deploy system all allow you to focus on building unique and high quality apps.

2. Navigate down on the page to the header **Get just the command line tools**.



Get just the command line tools

If you do not need Android Studio, you can download the basic Android command line tools below. You can use the included `sdkmanager` to download other SDK packages.

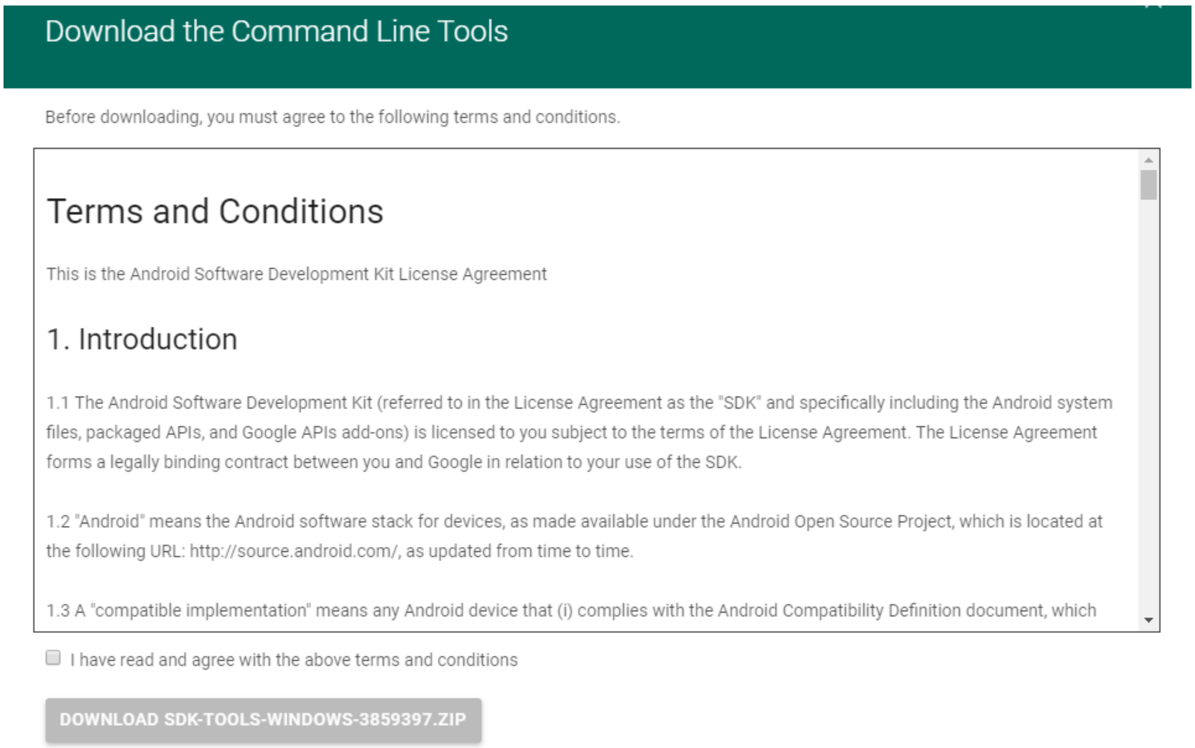
These tools are included in Android Studio.

Platform	SDK tools package	Size	SHA-256 checksum
Windows	sdk-tools-windows-3859397.zip	132 MB (138,449,982 bytes)	7f6037d3a7d6789b4fdc06ee7af041e071e9860c51f66f7a4eb5913df9871fd2
Mac	sdk-tools-darwin-3859397.zip	82 MB (86,182,133 bytes)	4a81754a760fce88cba74d69c364b05b31c53d57b26f9f82355c61d5fe4b9df9
Linux	sdk-tools-linux-3859397.zip	130 MB (136,964,098 bytes)	444e22ce8ca0f67353bda4b85175ed3731cae3ffa695ca18119cbacef1c1bea0

See the SDK tools release notes.

The **Download the Command Line Tools** window appears.

3. Select the checkbox **I have read and agree with the above Terms and Conditions**.



Download the Command Line Tools

Before downloading, you must agree to the following terms and conditions.

Terms and Conditions

This is the Android Software Development Kit License Agreement

1. Introduction

1.1 The Android Software Development Kit (referred to in the License Agreement as the "SDK" and specifically including the Android system files, packaged APIs, and Google APIs add-ons) is licensed to you subject to the terms of the License Agreement. The License Agreement forms a legally binding contract between you and Google in relation to your use of the SDK.

1.2 "Android" means the Android software stack for devices, as made available under the Android Open Source Project, which is located at the following URL: http://source.android.com/, as updated from time to time.

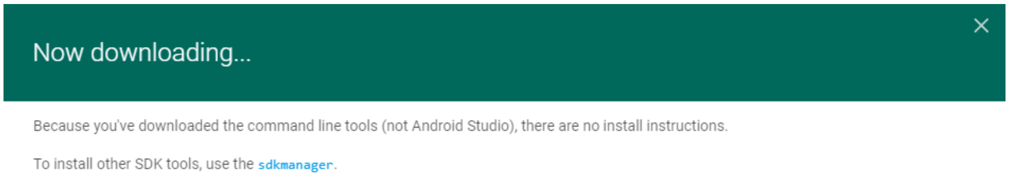
1.3 A "compatible implementation" means any Android device that (i) complies with the Android Compatibility Definition document, which

□ I have read and agree with the above terms and conditions

The **Download SDK- Tools Windows** button becomes active.

4. Click the **Download the SDK ADT Bundle for Windows** button.

   The **Now downloading** window appears.

   Now downloading...

   Because you've downloaded the command line tools (not Android Studio), there are no install instructions.

   To install other SDK tools, use the `sdkmanager`.

5. Download the SDK to your server, for example, D:\android. Unzip the bundle.
6. Next, traverse to: `D:\android\adt-bundle-windows-x86_64-20140321\adt-bundle-windows-x86_64-20140321`
7. Click `SDK Manager.exe` in the folder to download the entire Android SDK from Google.

   The folder that contains Android SDK folder is your Kony EMM Home folder. You need to move the Android SDK folder accordingly.

12.3.3 Manual Steps to configure multi node setup

The Installer is required to run on all nodes only if you wish to setup new EMM with multi node setup through manual steps. If already EMM with a single node is running and you want to enable more nodes or setup multi node for the high availability installer, then installer should run only on new nodes. Thus, for the existing single node setup to enable with multi node requires some configuration changes in the primary node and new nodes.

If you already run EMM on multi- node setup and have uploaded any images or certificates, take a backup of the docroot folder. Create an empty docroot folder with the same name. The following steps explains how to setup manually a multi-node setup.

1. Ensure that the pre-requisites for installation are met accordingly.
2. Run the Single Node installer.
    i. Provide **Docroot** with **UNC** path.
3. Ensure that the UNC paths are updated.
4. Check that the following details are in place:

    `D:\<InstallFolder>\Apache24\cgi-bin\appserver`

    i. The appserver file must be modified on line number 32

    ii. My $fileRoot = //10.10.4.1/emm_fs/emm/

    iii. Provide the UNC path of the emm folder.

    iv. In Tomcat conf folder update the `catalina.properties file` param :

    `DOCROOT.DIR=//10.10.4.1/emm_fs/emm`

    v. Navigate to path `D:\<InstallFolder>\Apache24\conf\httpd.conf and check the httpd.conf, lines 1074-1079`, and verify the following details:

    - Alias ${KONYEMM_WEBCONTEXT} download “//10.10.4.1/emm_fs/emm”
    - <Directory “//10.10.4.1/emm_fs/emm”>
    - Options - Index
    - AllowOverride None
    - Require all granted
    - </Directory>

    The emm folder path is provided in UNC path as above.

5. Edit the `httpd.conf` file.

```
ProxyPassMatch ^${KONYEMM_WEBCONTEXT}(.*)$ balancer://emmcluster

${KONYEMM_WEBCONTEXT}$1

ProxyPassReverse ^${KONYEMM_WEBCONTEXT_ONE} balancer://emmcluster/

<Proxy balancer://emmcluster>

##Load Balancer list

BalancerMember http://10.11.11.53:8080 route=emm1 retry=1 max=25
timeout=600

BalancerMember http://10.11.11.55:8080 route=emm2 retry=1 max=25
timeout=600

ProxySet stickysession=SESSIONID|sessionid

</Proxy>
```

> ***Note:*** The BalancerMember sequence is also important. Ensure that the URLs are provided in the same order.

6. Install Memcached.

   i. If the system is Windows, admin needs to update the system environment variable named with `MEMCACHE_CLUSTER` as well with same details of `IP1:Port1 IP2:Port2`

   > ***Note:*** Do not use any quotes

   ii. To reflect the new changes, all services need to be restarted. To start the memcache service follow the step no. iii.

   iii. Open the **Start Menu** and run `service.msc`. Right Click on **Memcached Service** and start. `<IMAGE HeRE>`

7. In the Tomcat conf directory, edit `server.xm`l,

   ```
   <Engine name =”Catalina” defaultHost=”localhost”
   jvmRoute=”emm1”>
   ```

   The `jvmRoute` must be changed to the node name provided in the `Apache httpd.conf` file.

8. Ensure Pre-requisites are met in the new node to be installed.

9. Run the Installer on the second node. Provide the same details as the first node.

10. Let the installer create a dummy database (DB) and EMM home as well for new node.

11. Next the admin needs to point to the first node DB details for the new node.It can be done updating the details in catlina.properties file of the second node.

12. Copy the `httpd.conf` file from the initial installation.

    > *Note:* The **BalancerMember** sequence is also important. Ensure that the URLs are provided in the same order.

13. Let the installer create a dummy database (DB) and EMM home as well, but the system uses the DB of the first node. Thus, next you need to point to the first node DB details and updating the catlina.properties file in the second node.

14. Follow the same steps for setting up Memecached and starting services. (i.e. Do step 2 for this node).

15. In the Tomcat conf directory, edit the `server.xml`,

    ```
    <Engine name =”Catalina” defaultHost=localhost”
    jvmRoute=emm2>
    ```

    The `jvmRoute` must be changed to the node name provided in Apache httpd.conf file.

16. To add more nodes, repeat steps 8-12 again for each node.

17. Restart Tomcat and Apache in all nodes installed.

13. Post-Installation Tasks

This section describes how to complete post-installation tasks after you have installed the software. It includes information about the following topics:

- Tomcat Services
- Manually start the EMM service
- Login
- How to Reset a User Account Password for Network Device Enrollment Service (NDES)
- How to encrypt Database Password (EMM On-Premise build)

13.1 Tomcat Services

1. Stop the service `<TOMCAT_SERVICE_NAME>` from the Services window.
2. Go to `<TOMCAT_HOME>/bin` and run the following command

```
tomcat7.exe //US//<TOMCAT_SERVICE_NAME> ++JvmOptions "<JVM_
OPTIONS>" --JvmMs 2048 --JvmMx 2048
```

> ***Note:*** In Production environments, recommended heap size is 3584. Specify this value instead of 2048 in the above command

> ***Note:*** Below placeholders should be filled in with proper values before executing the above command..

- `TOMCAT_SERVICE_NAME` : This pertains to Service name of EMM Tomcat. You can find it in the services window

- `JVM_OPTIONS` : Open `<TOMCAT_HOME>/bin/service.bat` and search for string `"%SERVICE_NAME% ++JvmOptions".` Copy all the `jvm` options inside double quotes.

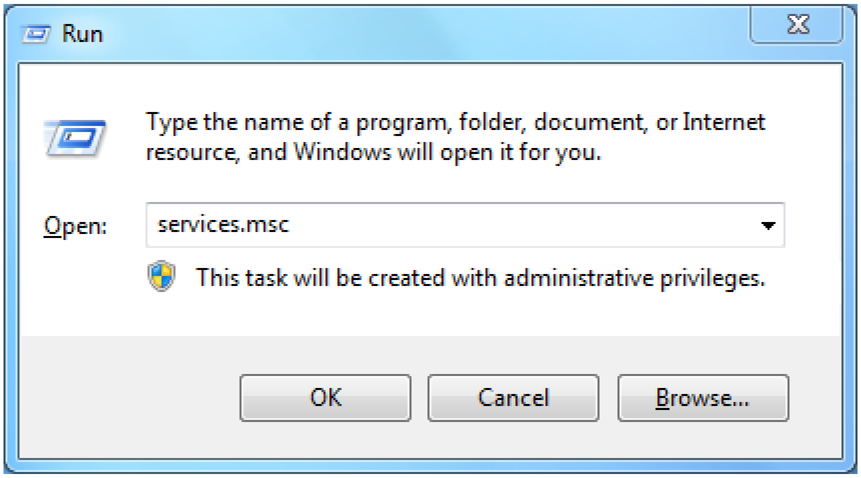
3. Start the service `<TOMCAT_SERVICE_NAME>` from the services window.

13.2 Manually start the EMM service

The Kony EMM Login screen appears.

If a user wants to start the services manually, then follow these steps:

1. Press **Windows + R** to open the **Run** window.

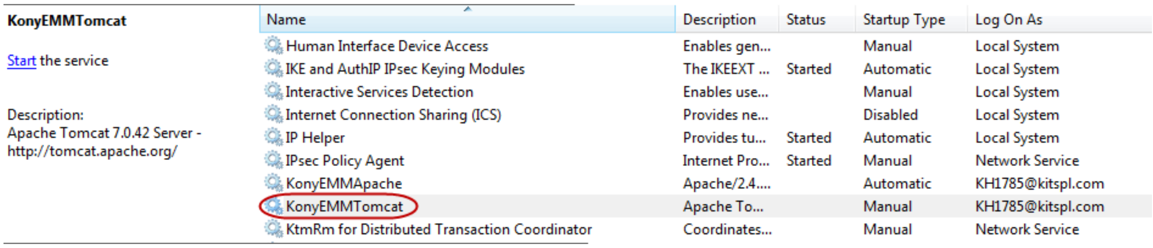

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
services.msc
This task will be created with administrative privileges.
OK
Cancel
Browse...

2. Enter services.msc in **Open**. Click **OK** to continue.

   The **Service** window appears on screen.

3. Click the installed services **Kony EMM Tomca**t, and **Kony EMM Apache**.

4. Click **Start** in the left panel.



KonyEMMTomcat

Start the service

Description:
Apache Tomcat 7.0.42 Server - http://tomcat.apache.org/

Name	Description	Status	Startup Type	Log On As
Human Interface Device Access	Enables gen...		Manual	Local System
IKE and AuthIP IPsec Keying Modules	The IKEEXT ...	Started	Automatic	Local System
Interactive Services Detection	Enables use...		Manual	Local System
Internet Connection Sharing (ICS)	Provides ne...		Disabled	Local System
IP Helper	Provides tu...	Started	Automatic	Local System
IPsec Policy Agent	Internet Pro...	Started	Manual	Network Service
KonyEMMApache	Apache/2.4....		Automatic	KH1785@kitspl.com
KonyEMMTomcat	Apache To...		Manual	KH1785@kitspl.com
KtmRm for Distributed Transaction Coordinator	Coordinates...		Manual	Network Service

The service starts.

5. Open an Internet browser.

6. Enter the EMM URL in the Address field of the browser. The EMM Console Login screen appears.

7. **User Name**: Enter the user name in the User name text field.

8. **Password**: Enter the password in the Password text field.

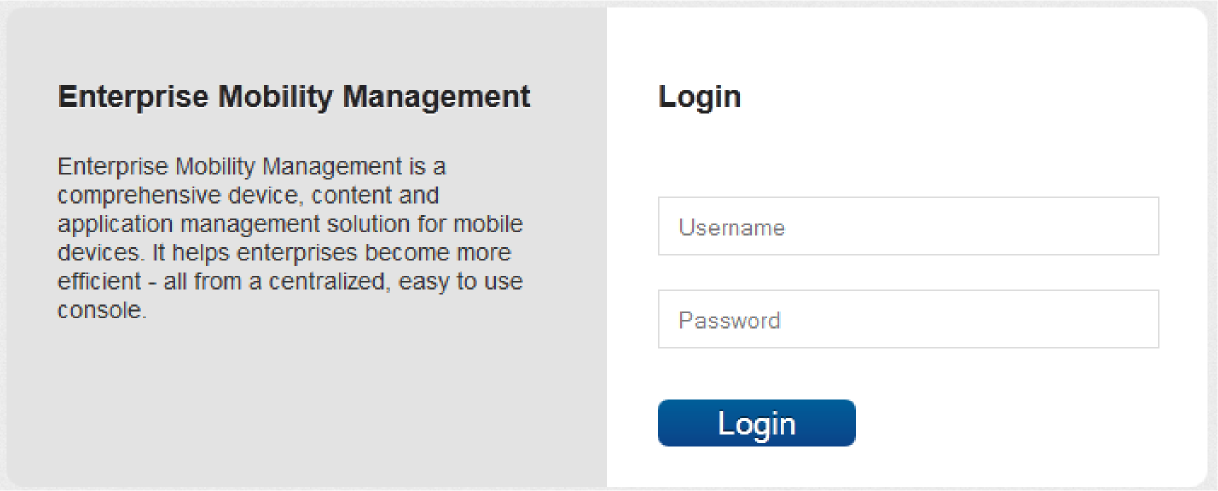
9. Click the **Login** button. After successful authentication,the Dashboard screen appears.

13.3 Login

The Administrator must logi in to set up the EMM for the organization.The Administrator needs to login with the credentials provided at installation.

The Kony EMM Console authentication window allows its users to log in to the system. The users with appropriate privileges can log in to the EMM Console and perform various operations.

To log in to the EMM Console, follow these steps:



Enterprise Mobility Management

Enterprise Mobility Management is a comprehensive device, content and application management solution for mobile devices. It helps enterprises become more efficient - all from a centralized, easy to use console.

Login

1. Open an Internet browser.
2. Enter the EMM URL in the address field of the browser. The EMM Console Login screen appears.
3. **Username**: Enter the user name in the username text field.
4. **Password**: Enter the password in the password text field.
5. Click the **Login** button. After successful authentication, the Dashboard screen appears.

> ***Note:*** It is recommended that the same User as Administrator should not login from multiple browsers or computers at the same time. Modifying the same page simultaneously may result into an unexpected behavior.

13.4 How to Reset a User Account Password for Network Device Enrollment Service (NDES)

All NDES service accounts are provided with a password during the installation. To change the password given during installation, follow these steps:

> ***Note:*** Download required artifacts from Kony Portal under Password Encryption Artifacts section.

1. In the windows server, open your server manager.

   The Server Manager window appears.

2. In the Server Manager, click on the Active Directory Domain Services Dashboard on the left.

   The Active Directory Console appears.The console displays the SCEP server details.

3. Right-click on the SCEP server name and then click **Active Directory Users and Computers**.

   The Active Directory Users and Computers window appears.

4. In the Active Directory Users and Computers window, click **Domain Controllers**.

   Details of users and computers in the domain console appear.

5. Right-click on the user whose password is being reset, and then select **Reset Password**.

   The Reset Password window appears.

6. Enter a new password in the **Password** text box.
7. Enter the password again in the **Confirm Password** text box.
8. Click **OK** to save the password.

   A message appears confirming that the password has been changed.

9. Click **OK**.

13.5 How to encrypt an NDES User Account Password

An NDES user account password must be encrypted for increased security. To encrypt an NDES user account password, follow these steps:

> ***Note:*** Download required artifacts from Kony Portal under Password Encryption Artifacts section.

1. Navigate to the folder where you have downloaded **emm-tomcat7-propertysource.zip** and extract the folder contents.
2. In the command prompt, navigate to the extracted folder and run the following command `java-jar emm-tomcat7-propertysource.jar`.

   A window appears.
3. Enter the new password you have set for the NDES service user account.
4. The console displays encrypted password in the format below.

   ```
   Encrypted Password: xxxxxxxxxxxxxxx
   ```
5. Copy the encrypted text.

   > ***Note:*** Make sure that you are not copying any blank spaces.
6. Navigate to **<TOMCAT_HOME>/conf**.
7. Open the `catalina.properties` file.
8. Search for a key value **SCEP_CA_PASSWORD**.
9. Replace the existing password in the **SCEP_CA_PASSWORD** key with the new encrypted password.

10. Set the value for **SCEP_PASSWORD_ENCRYPTED** key to **True**.

11. Restart the EMM server.

> ***Important:*** Enroll an iOS device to verify that the NDES service user account password reset is successful.

13.6 How to encrypt Database Password (EMM On-Premise build)

Database passwords can be encrypted to prevent unauthorized users from accessing password information from server logs. To encrypt database user account password, follow the steps below.

1. Navigate to the folder where you have downloaded **emm--tomcat7--propertysource.zip** and extract the folder contents.
2. From the extracted folder, copy **emm-tomcat7-propertysource.jar**.
3. Navigate to **<TOMCAT_HOME>/lib** and paste the copied **emm-tomcat7-propertysource.jar** in it.
4. Navigate to **<TOMCAT_HOME>/conf**.
5. Open `catalina.properties` file.
6. Add the following details at the end of the file.
   ```
   org.apache.tomcat.util.digester.PROPERTY_
   SOURCE=com.kony.emm.tomcat7.EMMTomcat7PropertySource
   ```
7. Open your database console and navigate to **<TOMCAT_HOME/lib** directory.
8. Run the command `java-jar emm-tomcat7-propertysource.jar.`
9. The system prompts you to enter your database password.
10. The console displays the encrypted password.

    ```
    Encrypted Password: xxxxxxxxxxxxxxx
    ```
11. Copy the encrypted text.

    > ***Note:*** Make sure that you do not copy any blank spaces.

12. Navigate to **<TOMCAT_HOME>/conf**.
13. Open the `catalina.properties` file.
14. Search for a key value **RDS_PASSWORD**.
15. Replace the existing password next to **RDS_PASSWORD** with the copied encrypted password text.
16. Restart the EMM Tomcat server.

14. Post Upgrade Tasks

14.1 Renaming Enterprise Store App for Android

After you upgrade the EMM server, you must replace a file in the Apache install folder for Renaming the Enterprise store feature to work for Android.

To replace the a file in Apache install folder, follow these steps:

1. Navigate to the Apache folder in your Kony Management suite installer folder, such as `/home/user1/KonyEMM/InstallationFolder/Utilities/EMM-GA-x.x/apache/cgi-bin/`.
2. Copy the Appserver file.
3. Navigate to the Apache folder in your Kony Management suite installer folder, such as `/home/user1/KonyEMM/InstallationFolder/apache/cgi-bin/`.
4. Paste the Appserver file.
5. Restart the Apache server.

14.2 Upgrading Launchpad Details

After you upgrade the Kony Management server, you must upgrade Launchpad details in your Kony Management Suite management console.

To upgrade Launchpad, follow these steps:

1. In your management console, navigate to **App Management** > **Enterprise Apps** > and click **Launchpad** app. Launchpad details appear.
2. Click **Upgrade Application**. Upgrade App screen displays.
3. In the App Basics section, select the platform to upgrade and then click **Next Step>>**.

4. Enter version number in the App Version text box.

5. Click **+ Add** to add binary files. Windows explorer opens.

6. Navigate to the EMM installation folder (for example, `<installation folder>\Utilities\EMM-GA-2.5.1\Docroot\mam\7433678379351539713\iphone\1.0.0`) and select required files. For example, 7433678379351539713.plist, appicon.png and store_iphone.ipa.

7. Click **Upload**. Files will be uploaded.

8. Click **Next Step>>**. Repeat click **Next Step>>** in Step 3 and Step 4 pages.

9. In Step 5 page, click **Upgrade App**.

10. A Success dialog box appears.

11. Click **OK**. Workflow State changes to **In Review**. Change the status to **Approved**. Launchpad State Change page appears.

12. Enter your comments in **Comments** text box and click **Change State**. Success dialog box appears.

13. Click **OK**. Workflow State changes to **Approved**.

14. In the **Publish Status** column, Select **Publish** from the drop down list. Launchpad State Publish page appears.

15. Enter your comments in **Comments** text box and click **Publish**. Success dialog box appears.

16. Click **OK**. Status in **Publish Status** column changes to **Published**. Upgrade process is complete and the user gets push notifications on the device.

14.3 Updating Tomcat Configuration

A new encryption key is introduced to enhance a secure assets download. To securely download an asset to the device, you must update the existing Tomcat configuration.

To update the Tomcat configuration, follow these steps:

1. Navigate to your Kony Management suite uninstaller folder, such as `/home/user1/KonyEMM/uninstaller`.
2. Open the **installvariables.properties** file.
3. Search for the **DOWNLOAD_ENCRYPTION_KEY** variable, and copy the variable along with its key value.
4. Navigate to `<Tomcat>/conf`.
5. Open the **catalina.properties** file.
6. At the end of the file, paste the **DOWNLOAD_ENCRYPTION_KEY** variable along with its key value.
7. Rename the key name to **DOWNLOAD.ENCRYPTION.KEY**
8. Save and close the file.

14.4 Replacing Apache Files

When you upgrade to the latest version of EMM, you need to copy files for the Apache service to run.

To replace Apache files, follow these steps:

1. Navigate to `<EMM Installation Folder>/Utilities/<version>/apache/cgi-bin`
2. Copy **appserver**,and **mcmdownload** files from the folder.

3. Navigate to `<EMM Installation Folder>/apache/cg-bin`

4. Paste the copied appserver and mcmdownload files.

14.5 Updating Tomcat Services for i18N

When you upgrade from any previous version of Kony Management suite to 4.1 GA, you must update your Tomcat services for the internationalization feature to work. This task is required only if you want to use the internationalization feature. If you do not perform this task, you may have iOS device enrollment issues.

1. In your windows instance, open services (services.msc). Find your Tomcat service name. For example, KonyEMMTomcat.

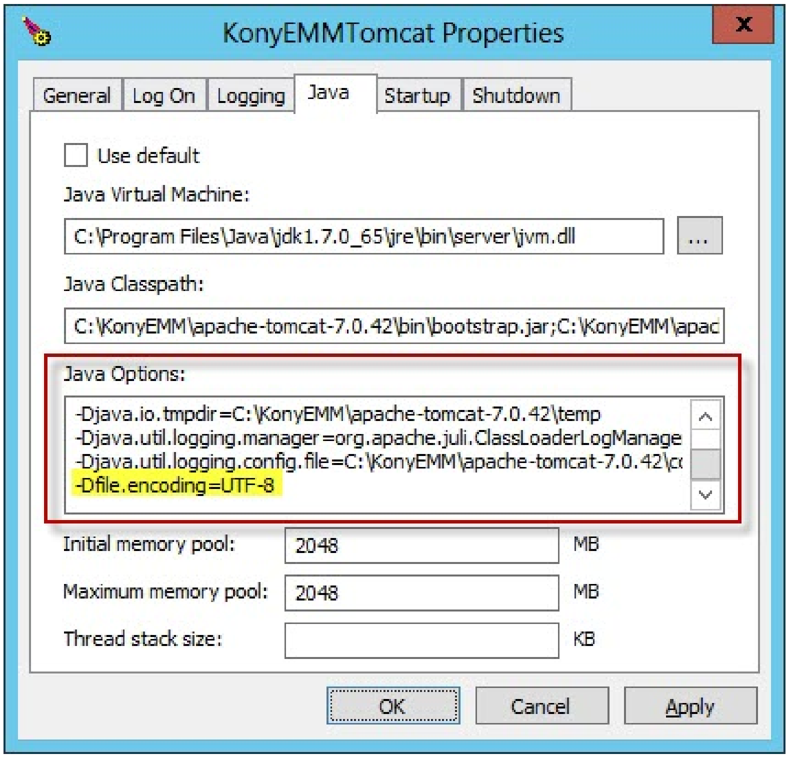
2. Open command prompt as administrator.

3. Navigate (cd) to the Tomcat bin directory.

4. Run the command below.
   `tomcat7w //ES//<Service name from Step #1>`The Tomcat properties window appears.

5. Click the **Java** tab.

6. In the Java Options section, add the following as a new line.
   -Dfile.encoding=UTF-8



☐ Use default

Java Virtual Machine:

```
C:\Program Files\Java\jdk1.7.0_65\jre\bin\server\jvm.dll
```

Java Classpath:

```
C:\KonyEMM\apache-tomcat-7.0.42\bin\bootstrap.jar;C:\KonyEMM\apac
```

Java Options:

```
-Djava.io.tmpdir=C:\KonyEMM\apache-tomcat-7.0.42\temp
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManage
-Djava.util.logging.config.file=C:\KonyEMM\apache-tomcat-7.0.42\c
-Dfile.encoding=UTF-8
```

Initial memory pool: 2048 MB

Maximum memory pool: 2048 MB

Thread stack size: KB

7. Click **Apply**.

8. Click the **General** tab.

9. Click **stop+start** to stop and start the service.

14.6 Updating Apache Files

In Kony Management 4.2.5.2, to enhance the security of encrypted EMM binary and content URLs, a new encryption mechanism is implemented. When you upgrade to Kony Management 4.2.5.2 from any previous version, you must perform the following steps.

> ***Note:*** Perform all the steps below in your EMM install folder. For example, **EMMInstalledFolder**.

1. Navigate to the following folder in your EMM install folder.
   EMMInstalledFolder/Utilities/EMMInstalledFolder/apache/conf/

2. Open **httpd.conf** file. Find the variable for **PassEnv MEMCACHE_CLUSTER** and copy the variable (key and its value).
3. Navigate to the following folder in your EMM install folder.
   EMMInstalledFolder/apache/conf/
4. Open the **httpd.conf** file.
5. Paste the copied key and value of **PassEnv MEMCACHE_CLUSTER** in the **httpd.conf** file.
6. Restart the Apache server.

15. Archiving MSSQL Database

You must archive MSSQL database to improve the performance of the database. This is done by archiving any unnecessary data from mdm_request, mdm_request_correlation, and mdm_request_correlation_status tables. If data in these tables crosses over 200000 rows, the database performance might be affected.

To find the row count, perform the following query in your MSSql.

```
select count(1) from emm.mdm_request_correlation_status
go
```

You must run the procedure mentioned below whenever the data crosses 200000 rows or whenever performance degradation observed.

You must stop the Kony Management Suite server before running the following procedure. The archiving procedure performs multiple operations on tables and their indexes. If you do not stop the Kony Management server, if the application keeps on updating status, this can interfere with the archiving process and it may even result in critical dead lock issues.

> ***Important:*** Please run this procedure in Restricted maintenance window with EMM application downtime window.

Once you are done executing the procedure, you can view complete auditing of the archiving process archive_audit. Run the following query to verify details of archiving:

```
select * from emm.archive_audit
go
```

If the procedure encounters any errors during the archive process, data of the corresponding table will not be deleted. Rest of the tables will continue to be archived.

If the archive process fails, the error code is published in the status column of emm.archive_audit.

This archive process is applicable from Kony Management 4.0 GA onwards. If your EMM is a previous version than 4.0 GA, upgrade to Kony Management 4.0 GA before you start the archiving process.

To archive MSSQL database, do the following:

1. Through your SQL management studio or any other compatible SAL server client, run the following query to verify rows count:

   ```
   select count(1) from emm.mdm_request_correlation_status
   go
   ```

2. If the row count is more than 200000, stop EMM application along with app server.

3. Execute the following query:

   ```
   USE <DB_name>
   GO
   DECLARE @return_value int
   EXEC @return_value = [emm].[proc_archive_tables]
   SELECT 'Return Value' = @return_value
   GO
   ```

4. Verify the archiving execution by running the following query.

   ```
   select * from emm.archive_audit
   go
   ```

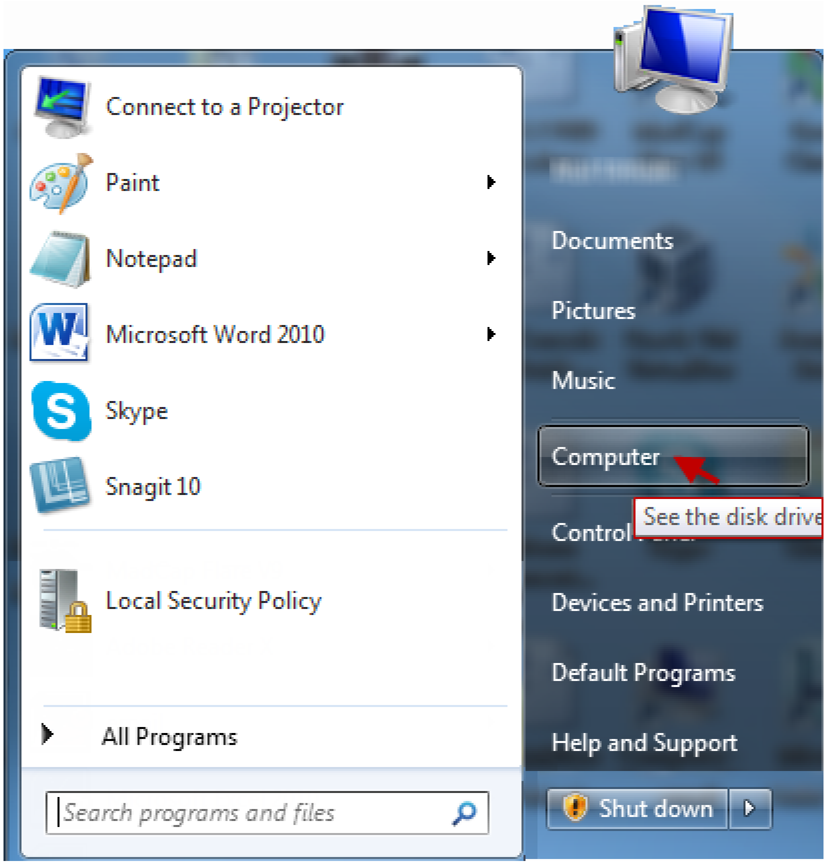
   > *Important:* Restart your memcache and Tomcat servers.

16. Uninstalling EMM

For one or other reason, you may need to uninstall Kony EMM from your system. The instructions given below explain in detail about how to uninstall Kony EMM.

To uninstall Kony EMM from your system, follow these steps:

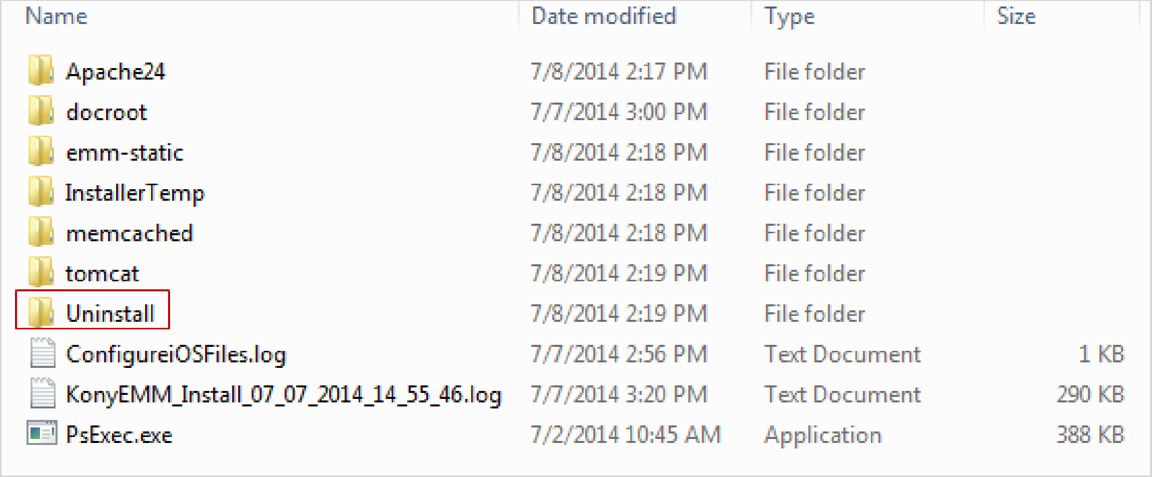
1. Click **Start** menu and then select **Computer**.



2. Find and click Hard Disk Drive, where Kony EMM is installed.

3. Click the **Kony EMM** Install folder.

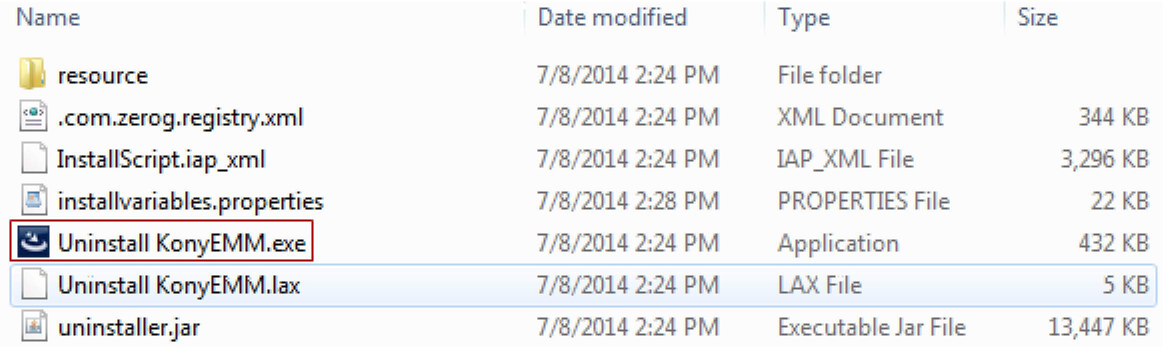
4. Install folder opens and displays the inner **Uninstall** folder.



Name	Date modified	Type	Size
Apache24	7/8/2014 2:17 PM	File folder	
docroot	7/7/2014 3:00 PM	File folder	
emm-static	7/8/2014 2:18 PM	File folder	
InstallerTemp	7/8/2014 2:18 PM	File folder	
memcached	7/8/2014 2:18 PM	File folder	
tomcat	7/8/2014 2:19 PM	File folder	
Uninstall	7/8/2014 2:19 PM	File folder	
ConfigureiOSFiles.log	7/7/2014 2:56 PM	Text Document	1 KB
KonyEMM_Install_07_07_2014_14_55_46.log	7/7/2014 3:20 PM	Text Document	290 KB
PsExec.exe	7/2/2014 10:45 AM	Application	388 KB

5. Click the **Uninstall** folder.

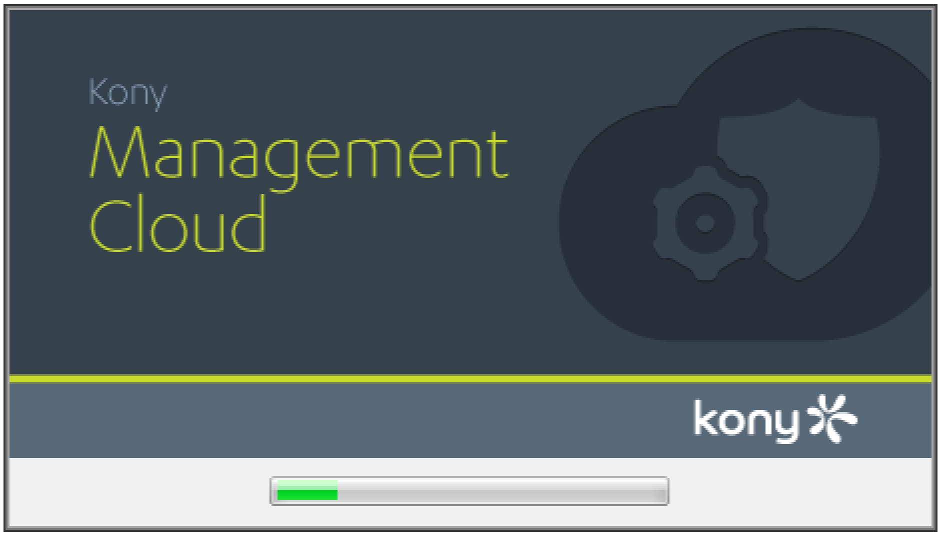
The Uninstall folder opens and displays **Uninstall KonyEMM**.exe.



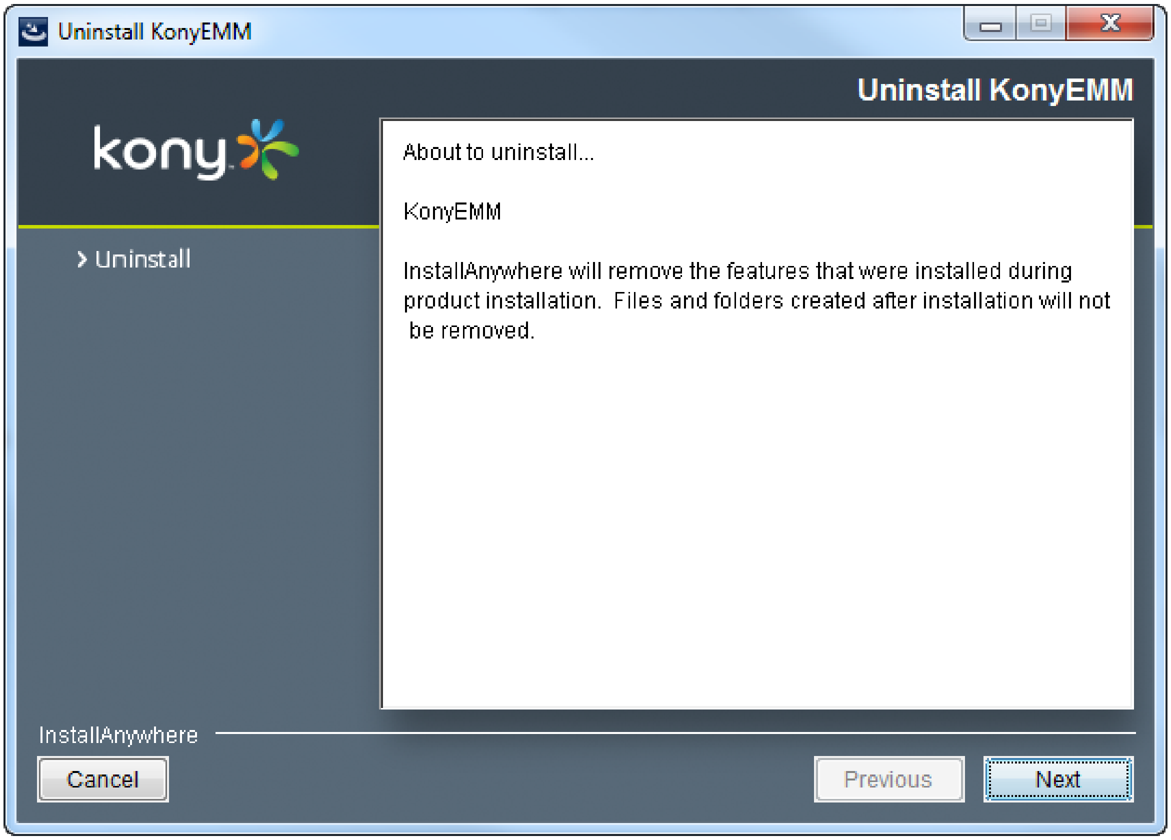
Name	Date modified	Type	Size
resource	7/8/2014 2:24 PM	File folder	
.com.zerog.registry.xml	7/8/2014 2:24 PM	XML Document	344 KB
InstallScript.iap_xml	7/8/2014 2:24 PM	IAP_XML File	3,296 KB
installvariables.properties	7/8/2014 2:28 PM	PROPERTIES File	22 KB
Uninstall KonyEMM.exe	7/8/2014 2:24 PM	Application	432 KB
Uninstall KonyEMM.lax	7/8/2014 2:24 PM	LAX File	5 KB
uninstaller.jar	7/8/2014 2:24 PM	Executable Jar File	13,447 KB

6. Click the **Uninstall KonyEMM**.exe.

A dialog with Kony logo appears



The **Uninstall KonyEMM** window appears.



About to uninstall...

KonyEMM

InstallAnywhere will remove the features that were installed during product installation. Files and folders created after installation will not be removed.

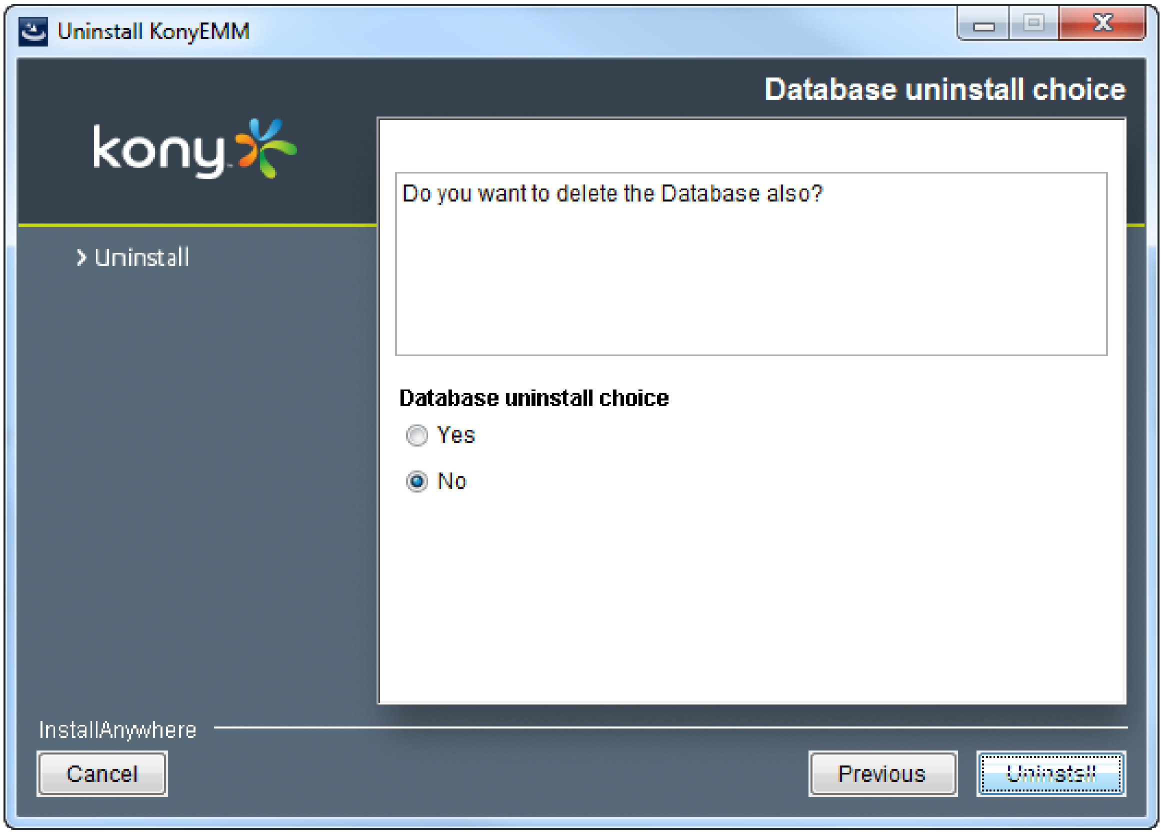
Uninstall KonyEMM window informs a user that InstallAnywhere will remove the features that were installed during product installation. Files and folders created after installation are not removed.

7. Click **Next** to continue.

8. The **Database uninstall choice** window appears.

   The **Database uninstall choice** window displays the alert message asking if you want to delete the database.

9. Select the option button as **Yes** or **No**. By default, it is set to No.



Do you want to delete the Database also?

Database uninstall choice

○ Yes

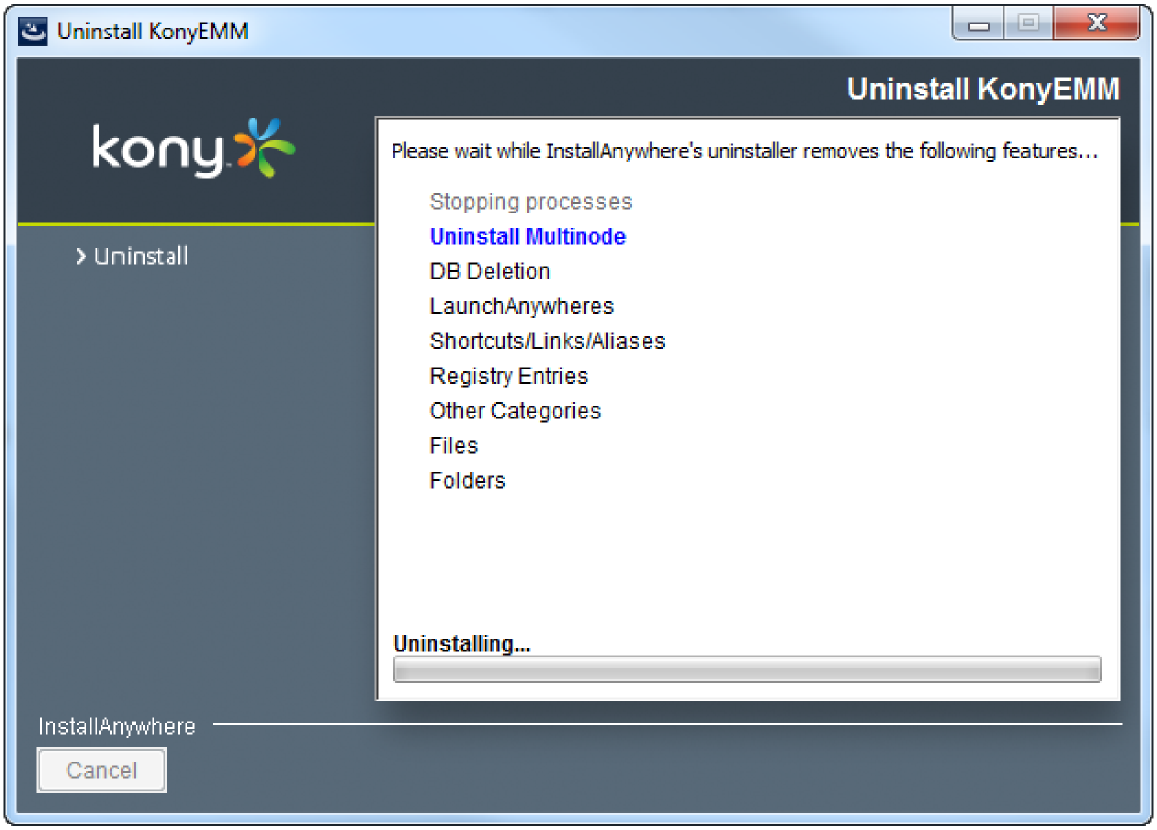
● No

> ***Note:*** If you select the Yes option, the database is deleted from your system. If you select the No option, then database is not deleted and you can access it for future use.

10. Click **Uninstall** to continue.

    The **Uninstall Kony EMM** window appears.

    The **Uninstall Kony EMM** window displays a list of features and informs a user that the uninstaller removes the following features.



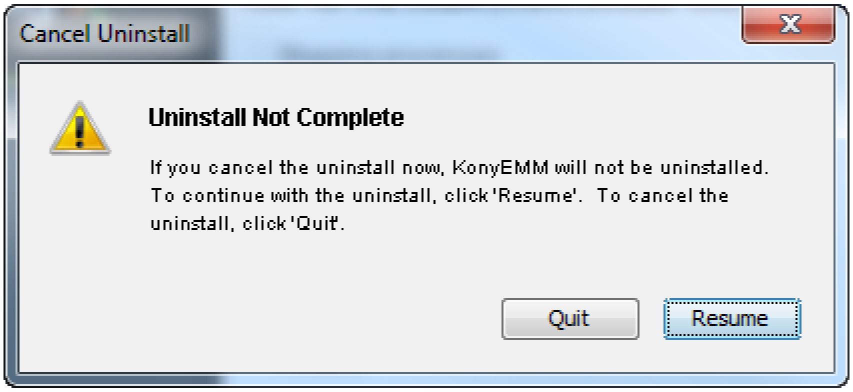
Uninstall KonyEMM

Please wait while InstallAnywhere's uninstaller removes the following features...

Stopping processes
Uninstall Multinode
DB Deletion
LaunchAnywheres
Shortcuts/Links/Aliases
Registry Entries
Other Categories
Files
Folders

Uninstalling...

11. If you click **Cancel** during uninstallation, then The **Cancel Uninstall** warning dialog appears. It informs a user that uninstallation is not complete and, Kony EMM will not be uninstalled.



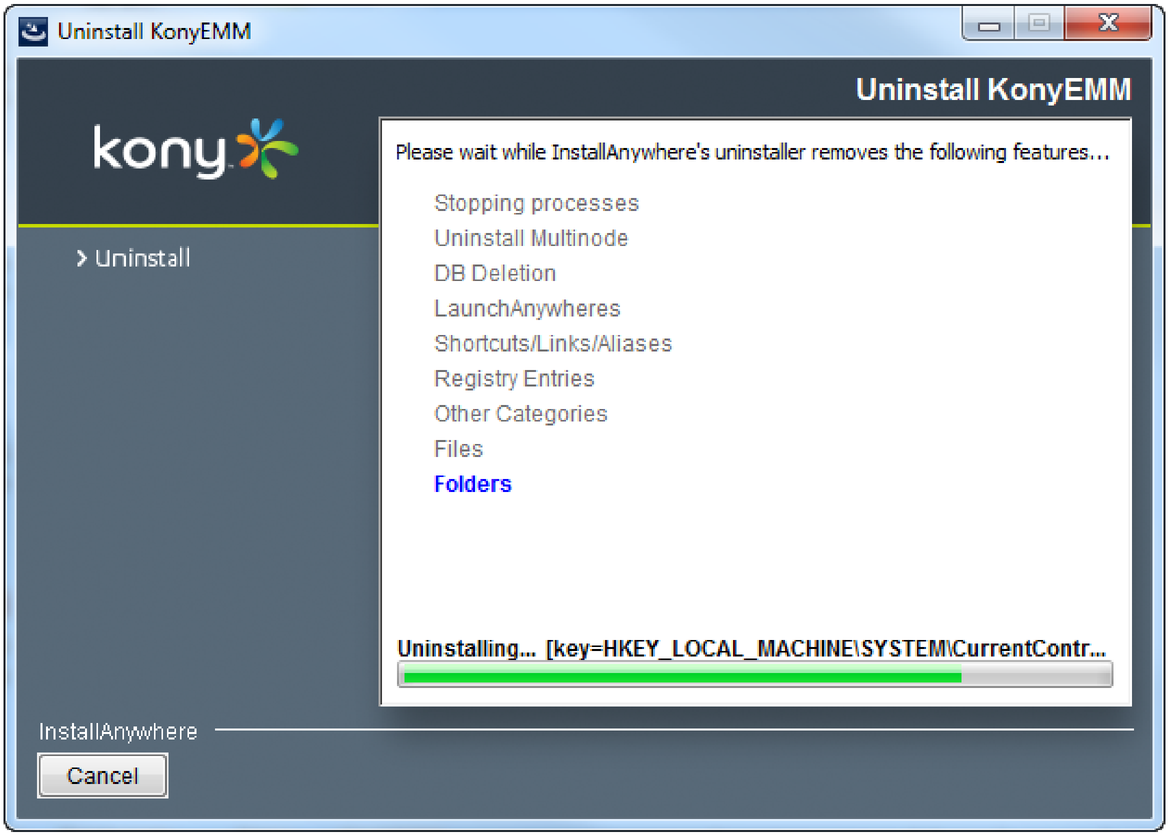
Uninstall Not Complete

If you cancel the uninstall now, KonyEMM will not be uninstalled. To continue with the uninstall, click 'Resume'. To cancel the uninstall, click 'Quit'.

12. To cancel the uninstall EMM, click **Quit.**

13. To resume the uninstall EMM, click **Resume**.

    The **Uninstall Kony EMM** window displays that the uninstalling is in progress.

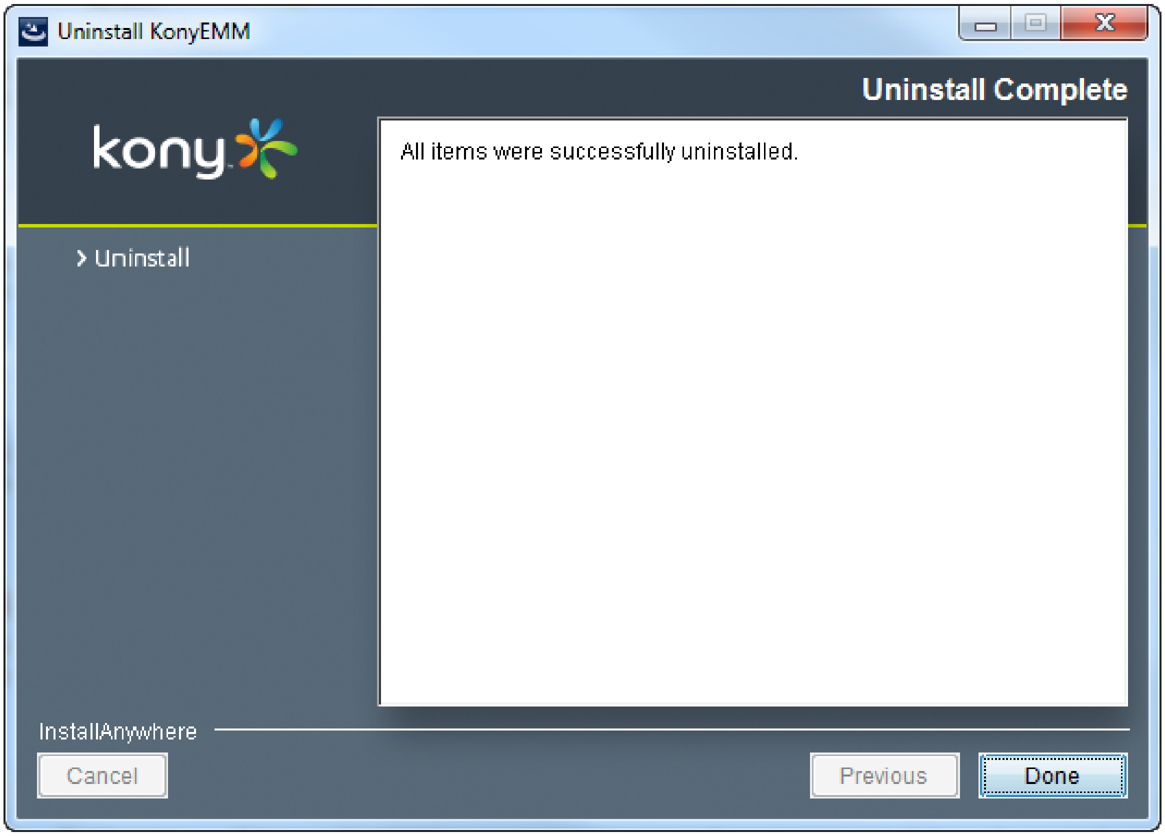


Please wait while InstallAnywhere's uninstaller removes the following features...

Stopping processes
Uninstall Multinode
DB Deletion
LaunchAnywheres
Shortcuts/Links/Aliases
Registry Entries
Other Categories
Files
Folders

Uninstalling... [key=HKEY_LOCAL_MACHINE\SYSTEM\CurrentContr...

Once the uninstallation is complete, the **Uninstall Complete** window appears.It informs that all items are successfully uninstalled.



All items were successfully uninstalled.

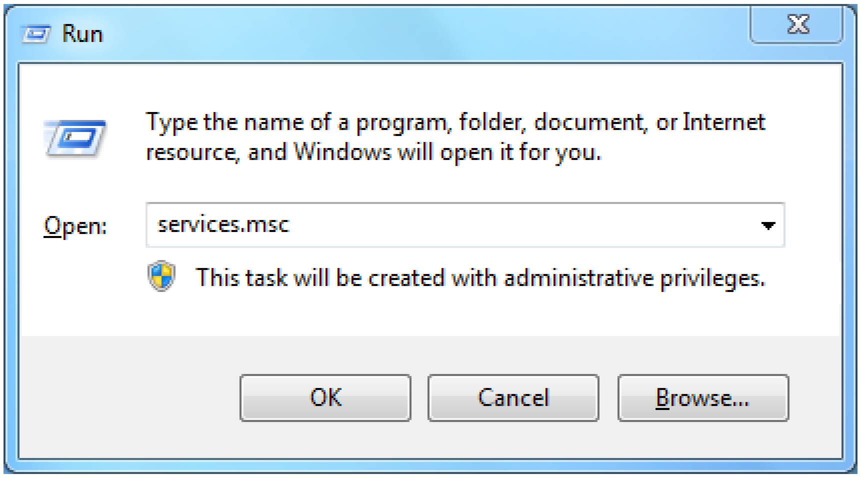
14. Click **Done** to close the window.

17. Troubleshooting Windows Service Installation

When you install Windows Service, you may receive an error message. In such a situation, the installation process does not finish. This section contains information that instructs you how to troubleshoot Windows Service installation.

To troubleshoot for Windows Service installation, follow these steps:

1. Press **Windows + R** to open the **Run** window.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

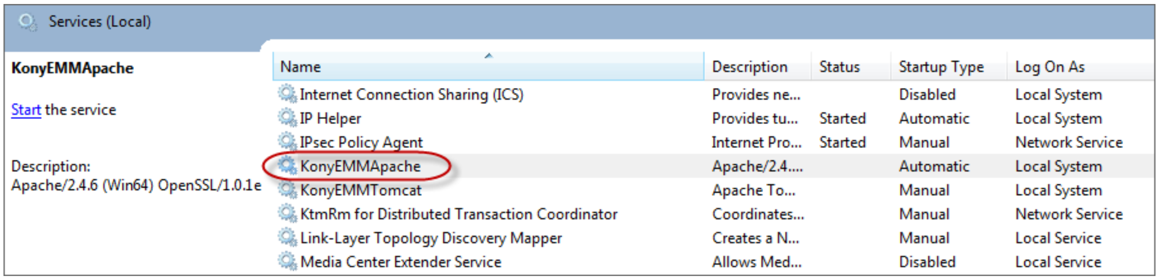
Open: services.msc

This task will be created with administrative privileges.

2. Enter **services.msc** in **Open**. Click **OK** to continue.

   The **Service** window appears on screen.

3. Double-click the installed Service.



KonyEMMApache

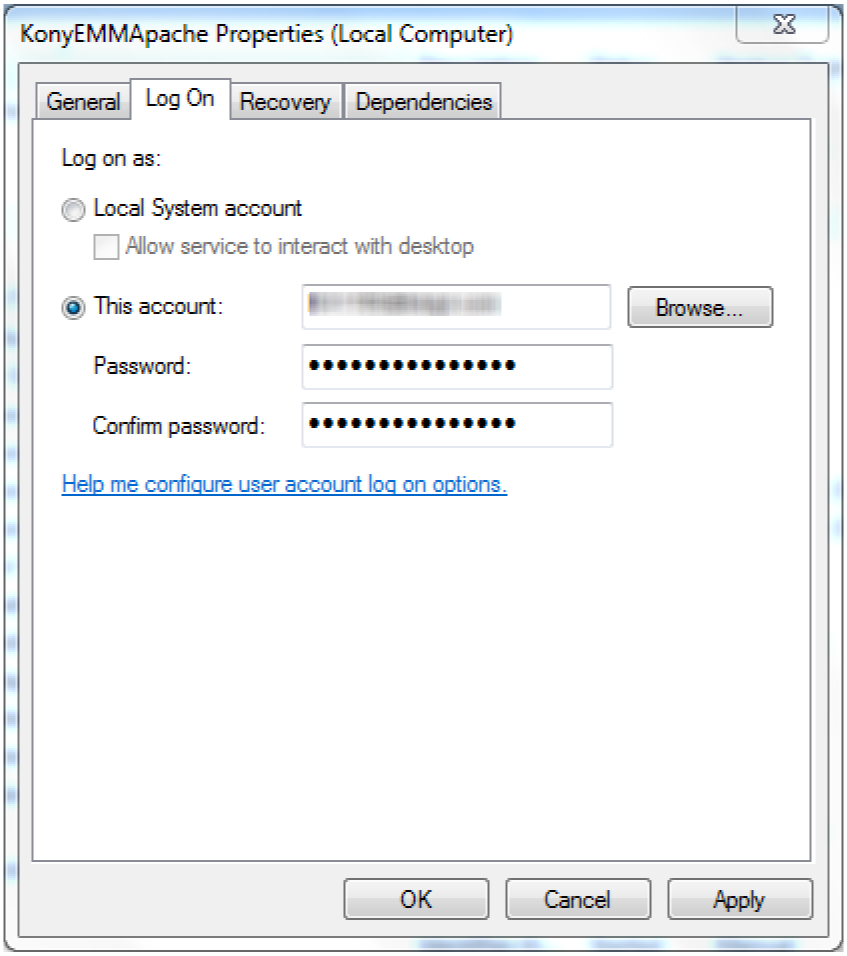
Start the service

Description:
Apache/2.4.6 (Win64) OpenSSL/1.0.1e

Name	Description	Status	Startup Type	Log On As
Internet Connection Sharing (ICS)	Provides ne...		Disabled	Local System
IP Helper	Provides tu...	Started	Automatic	Local System
IPsec Policy Agent	Internet Pro...	Started	Manual	Network Service
KonyEMMApache	Apache/2.4....		Automatic	Local System
KonyEMMTomcat	Apache To...		Manual	Local System
KtmRm for Distributed Transaction Coordinator	Coordinates...		Manual	Network Service
Link-Layer Topology Discovery Mapper	Creates a N...		Manual	Local Service
Media Center Extender Service	Allows Med...		Disabled	Local Service

The **KonyEMMApache Properties** window appears.

4. Click the **Log On** Tab. Enter the following details:



KonyEMMApache Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: [redacted]

Password: •••••••••••••••

Confirm password: •••••••••••••••

Help me configure user account log on options.

   a. **The Account**: Browse the account details. The selected account details appears in the text field.

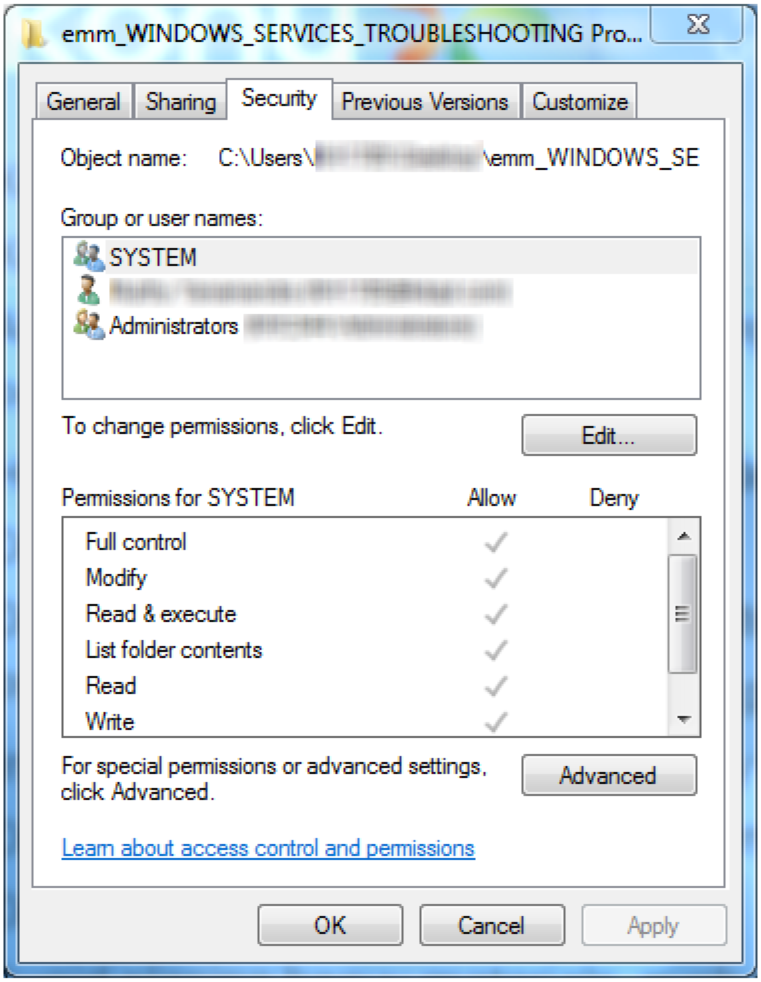
   b. **Password:** Enter your password.

   c. **Confirm password**: Re-enter your password to confirm it.

   d. Click **Apply** to continue. When you click Apply, you should receive a confirmation message stating that the user has been given the Log On as Service right.

5. Make sure that the user has full control permissions on the Install Directory and its subfolders.This means that the user should have full control of all files/folders within the install

directory. To verify this details, click the **Security** tab to know permission details.



Object name: C:\Users\[redacted]\emm_WINDOWS_SE

Group or user names:

SYSTEM
[redacted]
Administrators [redacted]

To change permissions, click Edit.

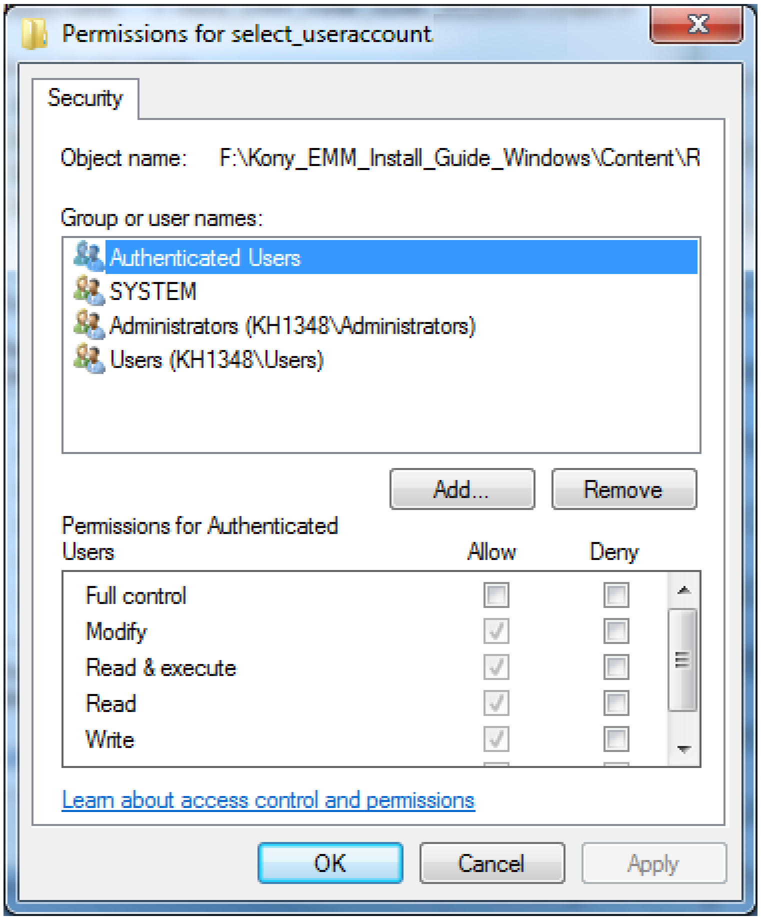
Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

6. If the user does not have the required permissions,click **Edit**.

   The **Permissions for select_useraccount** window appears


Permissions for select_useraccount
Security
Add...
Remove
Learn about access control and permissions
OK
Cancel
Apply

Object name: F:\Kony_EMM_Install_Guide_Windows\Content\R

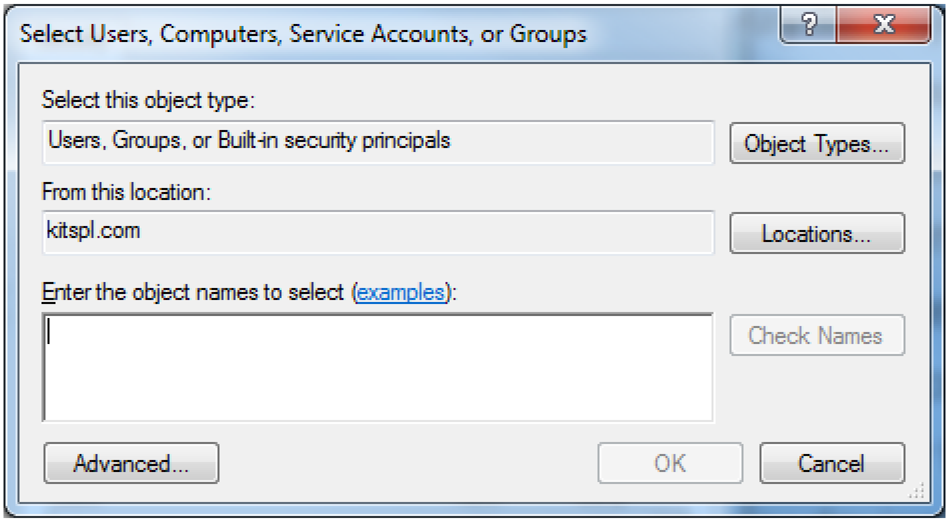
Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (KH1348\Administrators)
- Users (KH1348\Users)

Permissions for Authenticated Users	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
Read	☑	□
Write	☑	□

7. Click **Add**.

   The **Select Users, Computers, Service Accounts, or Groups** window appears.



Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Groups, or Built-in security principals

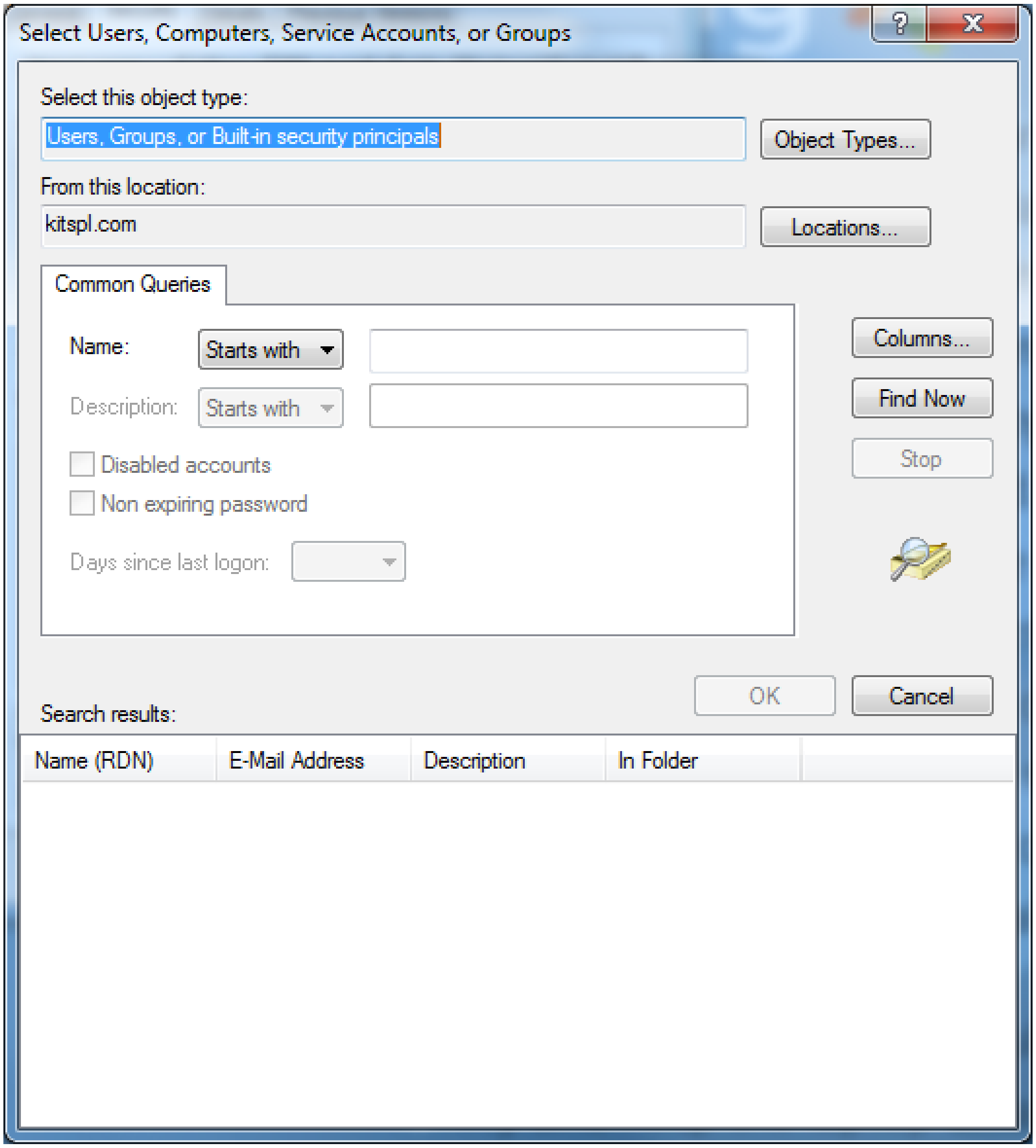
From this location:
kitspl.com

Enter the object names to select (examples):

8. Click **Advanced**.

   The **Common Queries** section appears.

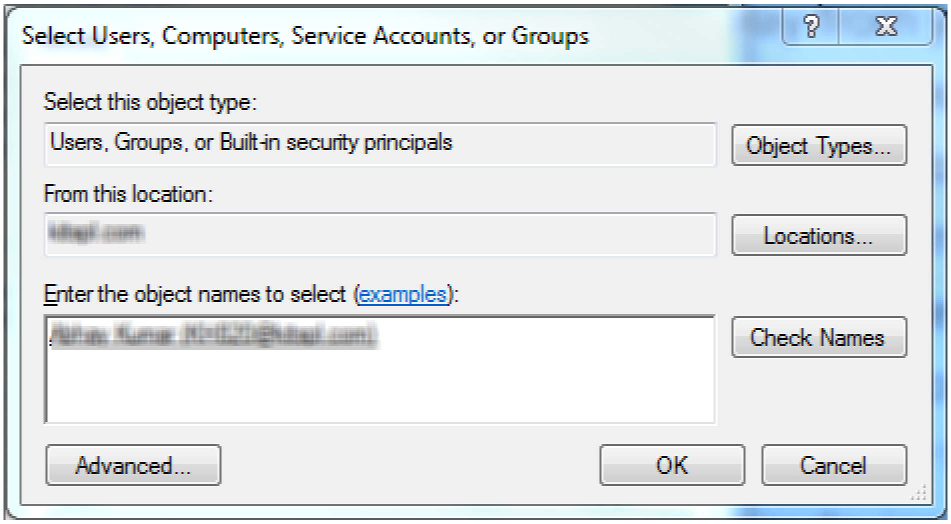
9. Add the name of the user, if not already present.



10. Enter the initial letter in **Name**. Click **Find Now**.

    The **Search Result** displays a list of all the users with the entered initial letter.

11. Select the name. The selected name appears in the **Select Users, Computers, Service Accounts, or Groups** window in the **Enter the Object names to select** field.



Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Groups, or Built-in security principals

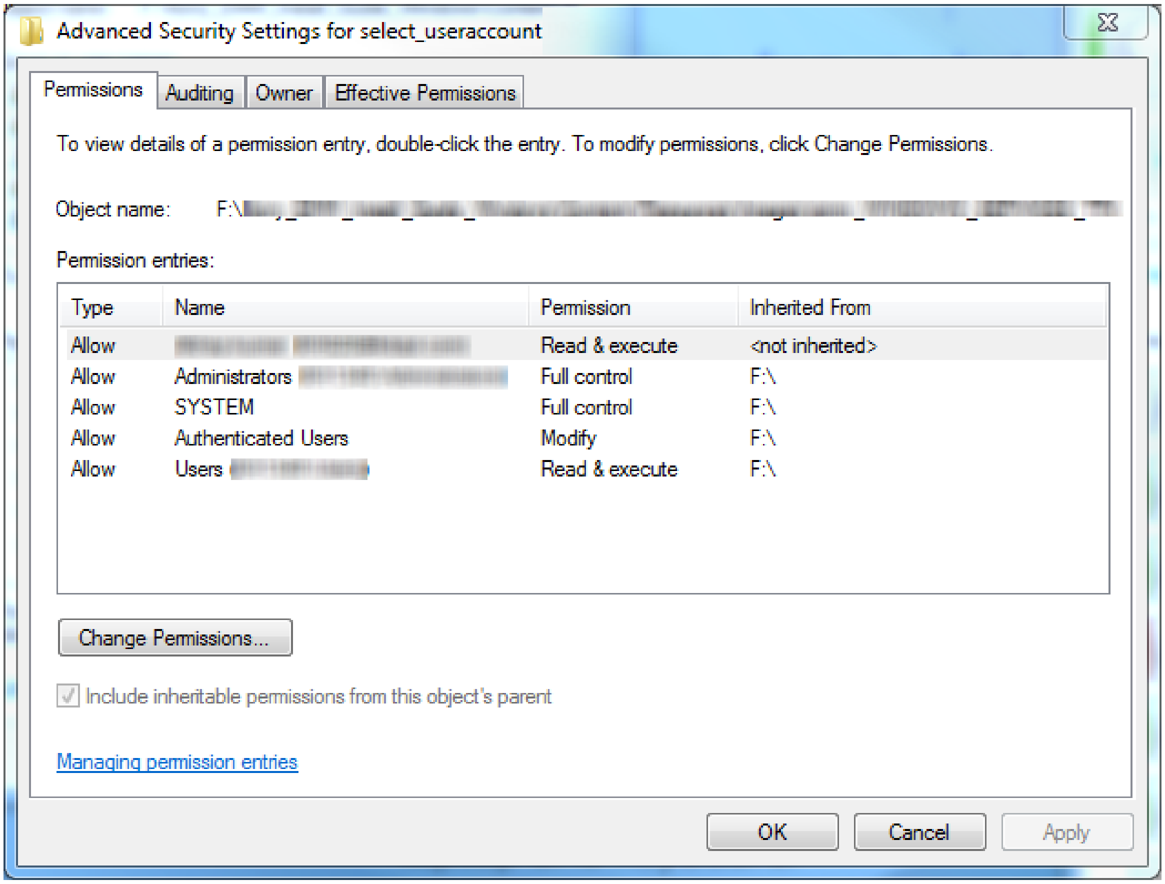
From this location:
[redacted]

Enter the object names to select (examples):
[redacted]

12. Click **OK** to continue.

13. Click **Advanced.**

    The **Advanced Security Settings for select_useraccoun**t window appears.


Advanced Security Settings for select_useraccount
Permissions
Auditing
Owner
Effective Permissions
Change Permissions...
Include inheritable permissions from this object's parent
Managing permission entries
OK
Cancel
Apply

To view details of a permission entry, double-click the entry. To modify permissions, click Change Permissions.

Object name: F:\[redacted]

Permission entries:

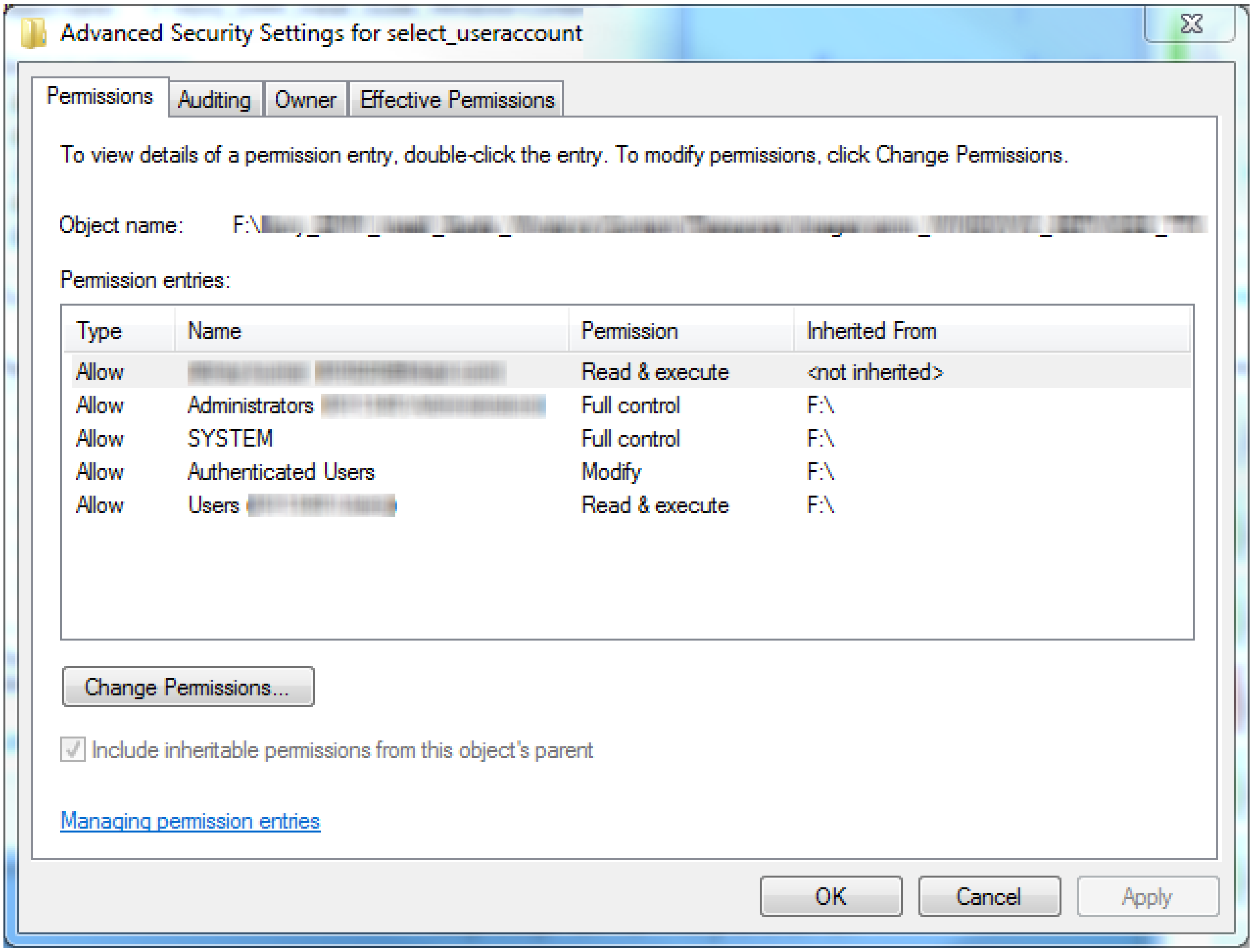
Type	Name	Permission	Inherited From
Allow	[redacted]	Read & execute	<not inherited>
Allow	Administrators [redacted]	Full control	F:\
Allow	SYSTEM	Full control	F:\
Allow	Authenticated Users	Modify	F:\
Allow	Users [redacted]	Read & execute	F:\

☑ Include inheritable permissions from this object's parent

14. Click **Change Permissions**.

    Advanced Security Settings for select-useraccount window appears.

15. Double click a name in the **Permission entries** list.



To view details of a permission entry, double-click the entry. To modify permissions, click Change Permissions.

Object name: F:\[redacted]

Permission entries:

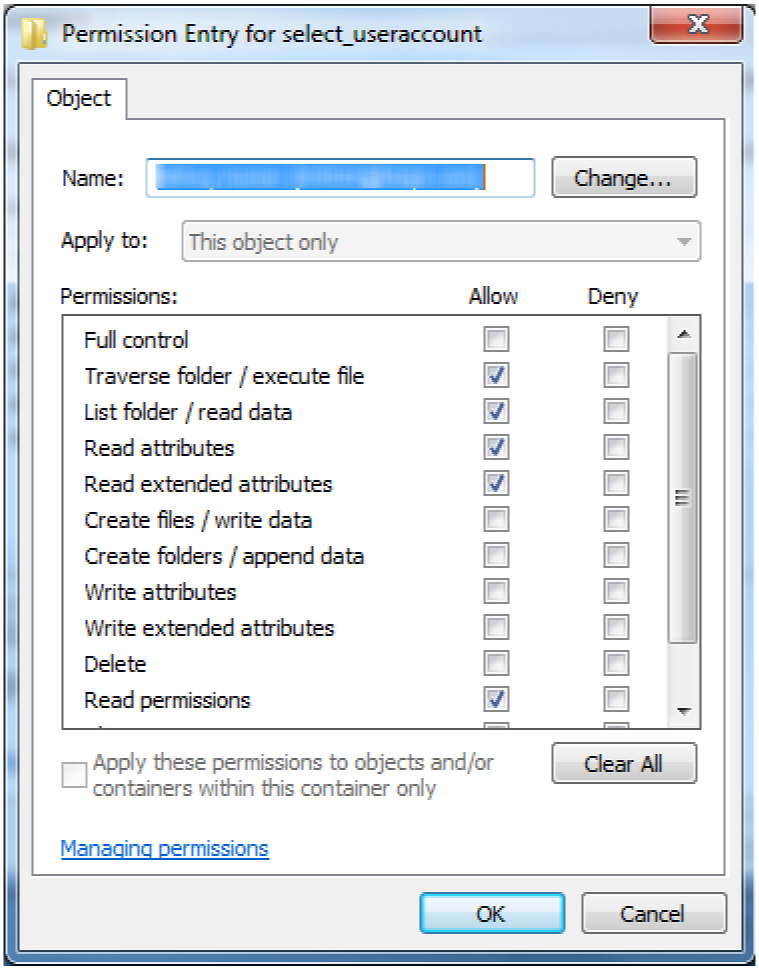
Type	Name	Permission	Inherited From
Allow	[redacted]	Read & execute	<not inherited>
Allow	Administrators [redacted]	Full control	F:\
Allow	SYSTEM	Full control	F:\
Allow	Authenticated Users	Modify	F:\
Allow	Users [redacted]	Read & execute	F:\

☑ Include inheritable permissions from this object's parent

.

The **Permission Entry for select_useraccount** window displays the Permissions list view.

16. Grant full control. Select the **Replace all child object permissions with inheritable permissions from this object** check box and then click **Apply**.



Permission Entry for select_useraccount

Object

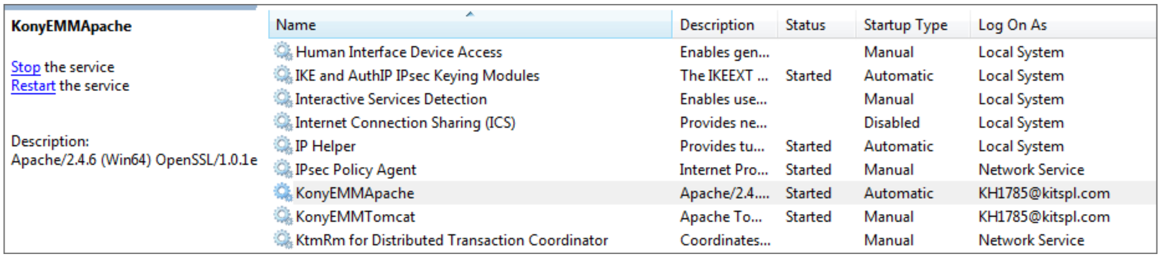
Name: [redacted]

Apply to: This object only

Permissions:	Allow	Deny
Full control	□	□
Traverse folder / execute file	☑	□
List folder / read data	☑	□
Read attributes	☑	□
Read extended attributes	☑	□
Create files / write data	□	□
Create folders / append data	□	□
Write attributes	□	□
Write extended attributes	□	□
Delete	□	□
Read permissions	☑	□

□ Apply these permissions to objects and/or containers within this container only

17. After following these steps, start the Service from services.msc



KonyEMMApache

Stop the service
Restart the service

Description:
Apache/2.4.6 (Win64) OpenSSL/1.0.1e

Name	Description	Status	Startup Type	Log On As
Human Interface Device Access	Enables gen...		Manual	Local System
IKE and AuthIP IPsec Keying Modules	The IKEEXT ...	Started	Automatic	Local System
Interactive Services Detection	Enables use...		Manual	Local System
Internet Connection Sharing (ICS)	Provides ne...		Disabled	Local System
IP Helper	Provides tu...	Started	Automatic	Local System
IPsec Policy Agent	Internet Pro...	Started	Manual	Network Service
KonyEMMApache	Apache/2.4....	Started	Automatic	KH1785@kitspl.com
KonyEMMTomcat	Apache To...	Started	Manual	KH1785@kitspl.com
KtmRm for Distributed Transaction Coordinator	Coordinates...		Manual	Network Service

18. The installed service starts.

17.1 Troubleshooting ADS Integration

Issue: If EMM server needs to connect AD server, which is under another firewall, then user cannot save the directory settings details in EMM portal.

To resolve this issue, follow these steps:

1. Log on as the **Domain Administrator** on the **Active Directory** domain server.
2. Install the **Certificate Authority (CA)** on the Microsoft Windows server(which installs the **Server Certificate** on the Active Directory server). To do so, follow these steps:
   i. Click **Start** > **Control Panel** > **Administrative Tools** > **Certificate Authority** to open the CA Microsoft Management Console (MMC) GUI.

   ii. Expand the CA, computer and then right-click it to select the **CA Propertie**s. (Certificate should be related to your server domain name, For Example, *manage.domain.com* or related to your domain SSL)

   iii. From **General** menu, click **View Certificate**.

   iv. Select the **Details** view, and click **Copy to File** on the lower-right corner of the window.

   v. Use the **Certificate Export** wizard to save the CA certificate in a file.

   vi. Provide file name as `LdapCert.cer` and move it to EMM Server (You can save the CA certificate in either `DER Encoded Binary X-509` format or `Based-64 Encoded X-509` format)

3. Login to EMM Server and take backup of cacerts from location `Java\jdk1.7.0_51\jre\lib\security.`
4. Execute the following command:

```
keytool -keystore cacerts -importcert -alias ldapCert -file
LdapCert.cer
```

5. Execute the step given below from EMM server command prompt:

```
keytool -keystore <Java\jdk1.7.0_51>\jre\lib\security cacerts -
importcert -alias ldapCert -file LdapCert.cer
```

6. Place `LdapCert.cer` file at a valid location that was generated at *step no 2>sub step no v.*

   System displays the success message informing that the certificate is imported successfully.

18. Troubleshooting SQLCipher Issues

18.1 What is SQLCipher and how does Kony Management Suite use SQLCipher?

SQLCipher is an open source library that provides secure encryption of SQLite database files. SQLCipher is ideal for protecting embedded application databases and is well suited for mobile development.

When an application (Android/IOS) creates a database, the database is saved in the application's private space in plain text. These plain text database (unprotected) files can be pulled from applications. The database info can be viewed using SQlite viewer apps like SqliteBrowser and these apps can leak important in the databases to unauthorized users.

Sqlcipher provides APIs to protect application created databases with a password so that even if the databases are pulled from mobile, the SQLite viewer apps cannot open the pulled databases and will show that databases are either corrupted or password protected.

Kony Management Suite makes use of SQLCipher to protect application databases for the enterprise apps submitted for wrap and sign mode on Kony Management Suite administrator console.

Kony Management Suite provides a secure way of managing the password for SQLCipher databases where the password is not kept in the apps.

App developers must write their application database logic using the native android SQLite APIs and Kony Management Suite will automatically make those APIs secure using SQLCipher APIs once the app is submitted on Kony Management Suite administrator console for wrapping and signing.

18.2 Troubleshooting SQLCipher files on Android Apps

Kony Management Suite provides app databases protection using SQLCipher integration with dynamic password management for the enterprise apps.

This Kony Management Suite feature will automatically convert databases created by an app to much-secured databases which will be protected by Kony Management Suite dynamic password management module. So a developer does not have to use SQLCipher files to protect app databases. If the app already contains SQLCipher files and submitted on Kony Management Suite administrator console for wrap and sign mode, Kony Management Suite specific files which are fips compliant and relatively more secure version won’t be replaced in the apps. The resultant wrapped enterprise app may crash during run time with some methods missing which are present in Kony Management Suite SQLCipher files.

18.2.1 Native developer

You must look for following files in the your project location mainly in libs and assets and delete those and regenerate the apk.

- Delete sqlcipher.jar from libs folder
- Delete following .so files from libs/armeabi, libs/armeabi-v7a,libs/x86 or any other locations if found
    - libdatabase_sqlcipher.so
    - libsqlcipher_android.so
    - libstlport_shared.so
- Delete following files from assets or any other locations if found
    - libcrypto.mp3
    - libssl.so.1.0.0
    - libxcrypto.mp3
    - libxssl.so.1.0.0
    - icudt46l.zip

For final confirmation, apk to be submitted on Kony Management suite administrator console can be open with zip utility (like winzip > open archive) and lib and assets dir can be checked for presence of above mentioned files.

19. Frequently Asked Questions

My Android app is crashing after wrapping. What do I do?

- You may have unnecessary .jar or SQL files in your .apk file. For information on SQL files, click here.

Not enough space in the Temp directory, what should I do?

- If you (Kony Management Administrator) do not have enough space in the temp directory of the computer you are installing Kony Management Suite on, you might face some issues. To avoid this problem, before running the installer, an administrator should create the following new environment variable and point the variable to a folder/directory which contains enough space (>1 GB).
  `Export IATEMPDIR=<Directory_having_proper_permission_and_enough_space>`

Can I move Apache logs temporary folder?

- No, do not change the path to temp directory. It should reside at its default location after post EMM installation. By default, it is located at: `/home/user1/KonyEMM/apache-tomcat-7.0.42/temp`.

Can an admin configure wrapping server later (i.e. post installation)?

- Yes. For iOS, you can configure the wrapping server by modifying the hosts.properties. For Windows, you can configure by modifying the hosts_win.properties file. For Android, the setup used for SDK will be used.

Why should an administrator configure upto four Apple Mac servers?

- An administrator needs to configure upto four Apple MAC servers for fail-safe.

What are the properties used for Google Maps?

- If you have a client ID, you can use googlemaps.client.id property. If you have a free API key, you can use googlemaps.free.api.key property.

How to display Google Maps in Child apps?

- To display Google Maps in an enterprise app wrapped with Kony Management Suite, you must add Kony Management Keystore SHA1 fingerprint entry against the child app package name in the Google API console page for the generated MAP v2 key. For more information, see the Setting Certificates section of the Kony Management User guide.

My MAC server is not connecting to the Kony Management Console.

- When you are able to telnet to MAC server from EMM server, but still shows Connection FAILED in health check status. If we observe Algorithm error then we need to add the below line in **/etc/sshd_config** in MAC server.

  KexAlgorithms diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1