

UNCLASSIFIED



# **SAMSUNG SDS EMM v1.5.x SUPPLEMENTAL PROCEDURES**

**Version 1, Release 1**

**20 January 2017**

**Developed by Samsung SDS and DISA for the DoD**

UNCLASSIFIED

### **Trademark Information**

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

---

**TABLE OF CONTENTS**

	<b>Page</b>
<b>1. SECURITY READINESS REVIEW .....</b>	<b>1</b>
1.1 General .....	1
1.2 Mobile Policy Review .....	1
<b>2. SAMSUNG SDS EMM SERVER SOFTWARE SECURITY AND CONFIGURATION INFORMATION.....</b>	<b>2</b>
2.1 Samsung SDS EMM Server Architecture .....	2
2.2 MDM Software Components .....	3
2.3 Samsung SDS EMM Server MDM Required Firewall Ports.....	3

## LIST OF TABLES

	<b>Page</b>
Table 2-1: Samsung SDS EMM Server Core Components .....	3
Table 2-2: Required Ports and Services.....	3

## LIST OF FIGURES

	<b>Page</b>
Figure 2-1: Samsung SDS EMM Server Single Server Architecture .....	2
Figure 2-2: Samsung SDS EMM Server Multi-Server Architecture .....	2



## **1. SECURITY READINESS REVIEW**

### **1.1 General**

When conducting a Samsung SDS Enterprise Mobility Management (EMM) server security review, the reviewer or auditor will identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with the Samsung SDS EMM.

### **1.2 Mobile Policy Review**

Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website located at <http://iase.disa.mil/stigs/mobility/Pages/policies.aspx>.

Use the Mobile Policy STIG and the MDM Server Policy STIG to review the Samsung SDS MDM asset.

## 2. SAMSUNG SDS EMM SERVER SOFTWARE SECURITY AND CONFIGURATION INFORMATION

Instructions to properly install the Samsung SDS EMM Server are provided in the following documents:

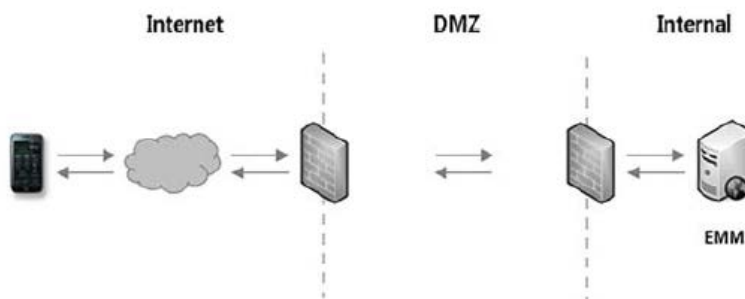
- Samsung SDS EMM Installation Guide, Version 1.5.1, December 2016
- Samsung SDS Push Installation Guide, Version 1.5.1, December 2016
- Samsung SDS AppTunnel Installation Guide, Version 1.5.1, December 2016
- Samsung SDS EMM Administrator's Guide, Version 1.5.1, December 2016

### 2.1 Samsung SDS EMM Server Architecture

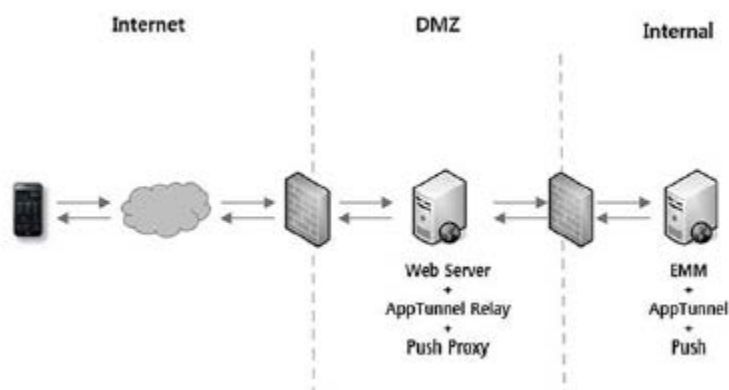
The Samsung SDS EMM Server can be deployed with or without proxy servers in a DMZ. The following two diagrams depict these architectures.

Refer to Section 1.2.2 of the Samsung SDS EMM Installation Guide, Version 1.5.1, December 2016, for more details.

**Figure 2-1: Samsung SDS EMM Server Single Server Architecture**



**Figure 2-2: Samsung SDS EMM Server Multi-Server Architecture**





## 2.2 MDM Software Components

**Table 2-1: Samsung SDS EMM Server Core Components**

Component	Description
EMM Agent	Software installed within an Android mobile device.
EMM Server	The main server running to which remote administrators connect. The EMM Server bears responsibility for all logic needed to manage mobile devices.
Push Server	The Push Server accepts connections from mobile devices and then relays the messages to and from the EMM Server (for example, to send policies to an agent or to send back a reply from an agent). One can install multiple Push Servers in order to allow the overall solution to scale the supported number of mobile devices (a single Push Server configuration was used during testing).
AppTunnel Server	The AppTunnel server accepts connections from the EMM Client (one of the three portions of the agent software on Android) and allows the Client to upload log files or download mobile applications to be installed by the agent.
AppTunnel Relay (multi-server architecture only)	A proxy to forward communication to an AppTunnel Server.
Push Proxy (multi-server architecture only)	A proxy to forward communication to a Push Server.
Web Server (multi-server architecture only)	A proxy to forward communication to an EMM Server.

## 2.3 Samsung SDS EMM Server MDM Required Firewall Ports

The ports listed in Table 2-2 are examples and can be adjusted during product installation as needed to meet a customer's specific network.

**Table 2-2: Required Ports and Services**

From	To	Port	Description
Web Browser or MD Agents	EMM Server	35443	Offers remote administration interface.
MD Agents	AppTunnel Server	36000	Supports MAS functions.
MD Agents	Push Server	35000, 35001, 35003	Supports communication between Agents and EMM Server.

From	To	Port	Description
EMM Server	Apple APNS	2195/2196	Communication between EMM and Apple APNS for iOS Support.
EMM Server	Microsoft SQL Database Server	1433	Communication to and from the Database.
iOS MD Agents	Apple APNS	5223 / 443	Supports communication between iOS Agent and Apple APNS.
Knox Agent	Knox Licensing Server	443	Allows for license validation for Samsung Knox devices.
EMM	Knox Licensing Server	443	Allows for license validation for Samsung Knox devices.