Security White Paper for
Streamline NX Administration Manager
Version 1.2.0.0

Solution Value proposition Section
Global Technology Support Department
Service and Support Center
Global Marketing Group

Document version
SLNXADMV1.2.0-1.1

Document version history:

Version	Date of Issue	Revision
1.0	September, 2011	・ Initial Release
1.1	October, 2011	・ Section 3 “Network Protocols” is revised.

1. Introduction

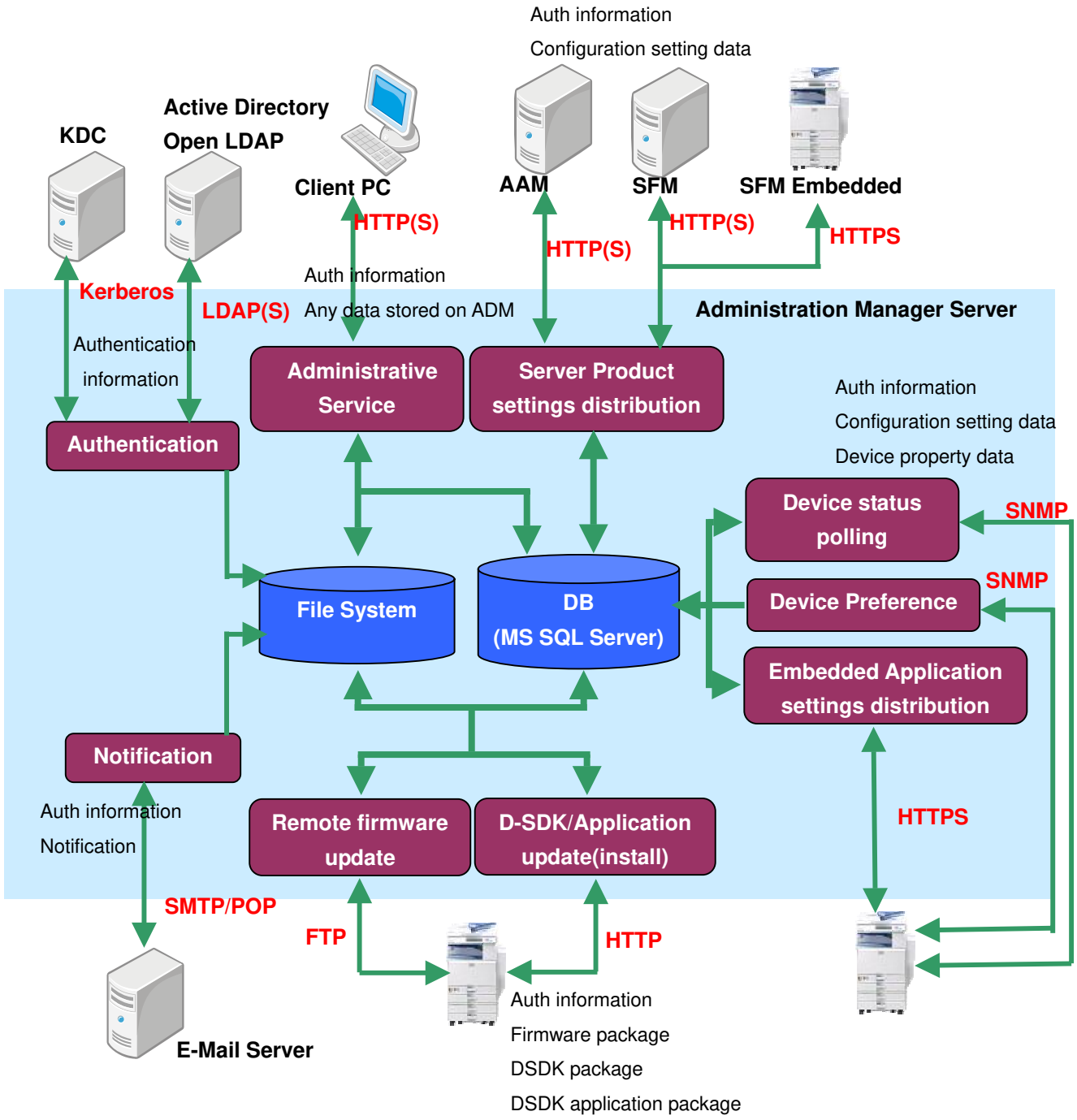
This document provides security information about Administration Manager (ADM).

ADM-S is a device management and integrated management server.
The main functions are as follows.

- Device List Management
- Device Discovery
- Device Monitoring
- Device Configuration
- Server Management
- SDK Application Management
- Log Management
- Job Management

2. System

2.1 System overview



All passwords that are stored on the ADM server are encrypted with Blowfish encryption, on communication path and while stored in the database.

2.2 Services

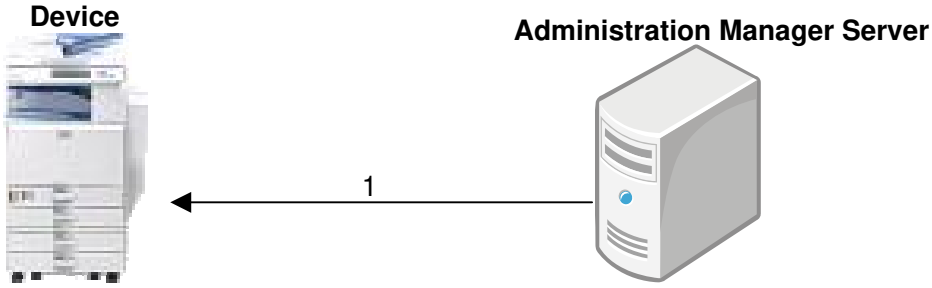
Services installed or used by ADM-S:

Service Name	Description
Streamline NX Administration Manger	The ADM service. This service is installed by ADM.

3. Network Protocols

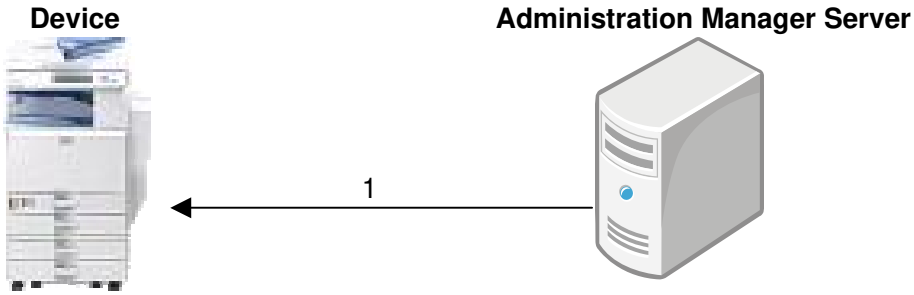
3.1 Ports and Protocols

- Discovery



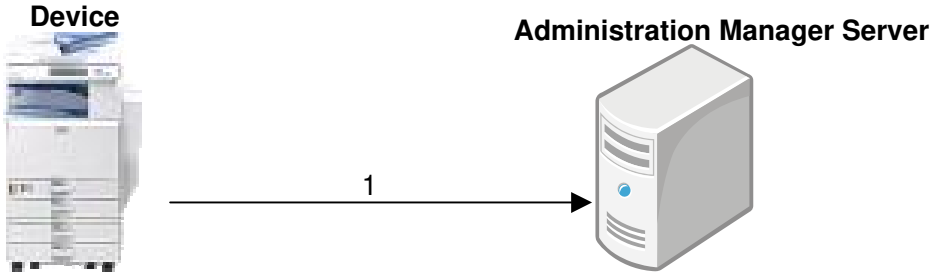
Features	Service	Protocol	Port No	Destination	Description
Discovery	SNMP v1/v2	UDP	161	Device	Retrieval of device information (IP address, Mac address, etc.)
	SNMP v3	UDP	161		

- Device Polling



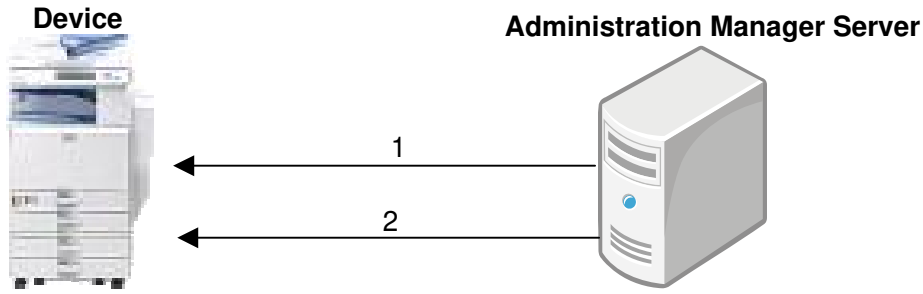
Features	Service	Protocol	Port No	Destination	Description
Device Polling	SNMP v1/v2 SNMP v3	UDP	161	Device	The following information is retrieved. - Serial number of device - Manufacturer ID - Model Name - System version - Printer Version - PPM - Comment - Printer Status - Paper Tray - Toner/Ink - Output Tray

- Trap



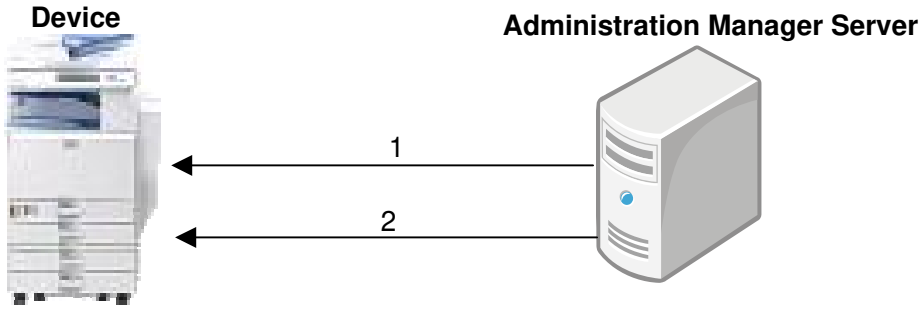
Features	Service	Protocol	Port No	Destination	Description
Trap	SNMP v1/v2	UDP	162	ADM server	Notify ADM of device event.
	SNMP v3	UDP	162		

- Device Preferences



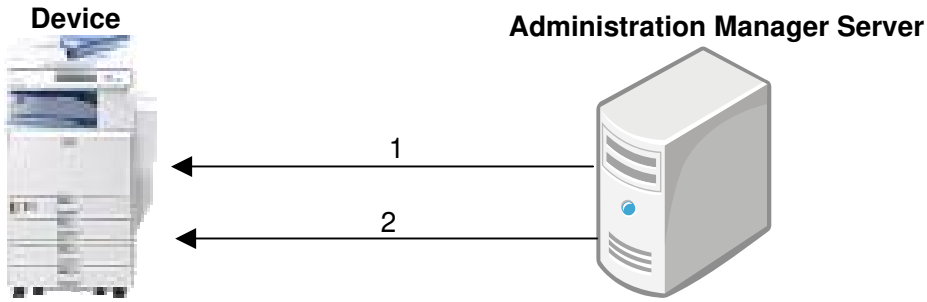
Features	Service	Protocol	Port No	Destination	Description
Retrieval of device information	SNMP v1/v2	UDP	162	ADM server	The following item is necessary: 1. Read community name
	SNMP v3	UDP	162		The following items are necessary: 1. User name 2. Password 3. Authentication Algorithm 4. Encryption password Context name
	HTTP/SOAP Or HTTPS/SOAP	TCP	80 443		The following items are necessary: 1. User name Password
Batch configuration	SNMP V1/V2	UDP	161	ADM server	The following item is necessary: 1.Write community name
	SNMP V3	UDP	161		The following items are necessary: 1. User name 2. Password 3. Authentication algorithm 4. Encryption password 5. Context name
	HTTP/SOAP or HTTPS/SOAP	TCP	80 443		The following items are necessary: 1. User name 2. Password

- Embedded Application Settings (AAM, SPM)



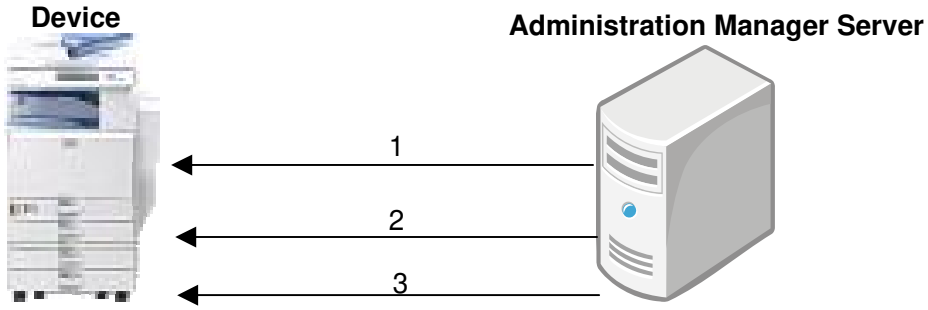
Features	Service	Protocol	Port No	Destination	Description
Retrieval of device information	SNMP v1/v2	UDP	161	Device	The following item is necessary: 1. Read community name
	SNMP v3	UDP	161		The following items are necessary: 1. User name 2. Password 3. Authentication Algorithm 4. Context name
Batch configuration	HTTPS	TCP	51443	Device	Access to AAM or SPM.

- Software Distribution (D-SDK, Embedded Application)



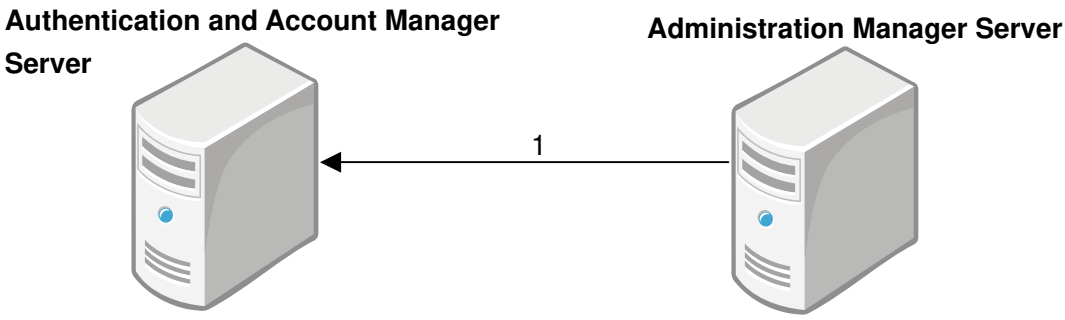
Features	Service	Protocol	Port No	Destination	Description
Retrieval of device information	SNMP v1/v2	UDP	161	Device	The following item is necessary: 1. Read community name
	SNMP v3	UDP	161		The following items are necessary: 1. User name 2. Password 3. Authentication Algorithm 4. Encryption password 5. Context name
Software Upload	HTTP	TCP	8080	Device	Uploads application to device.

- RFU



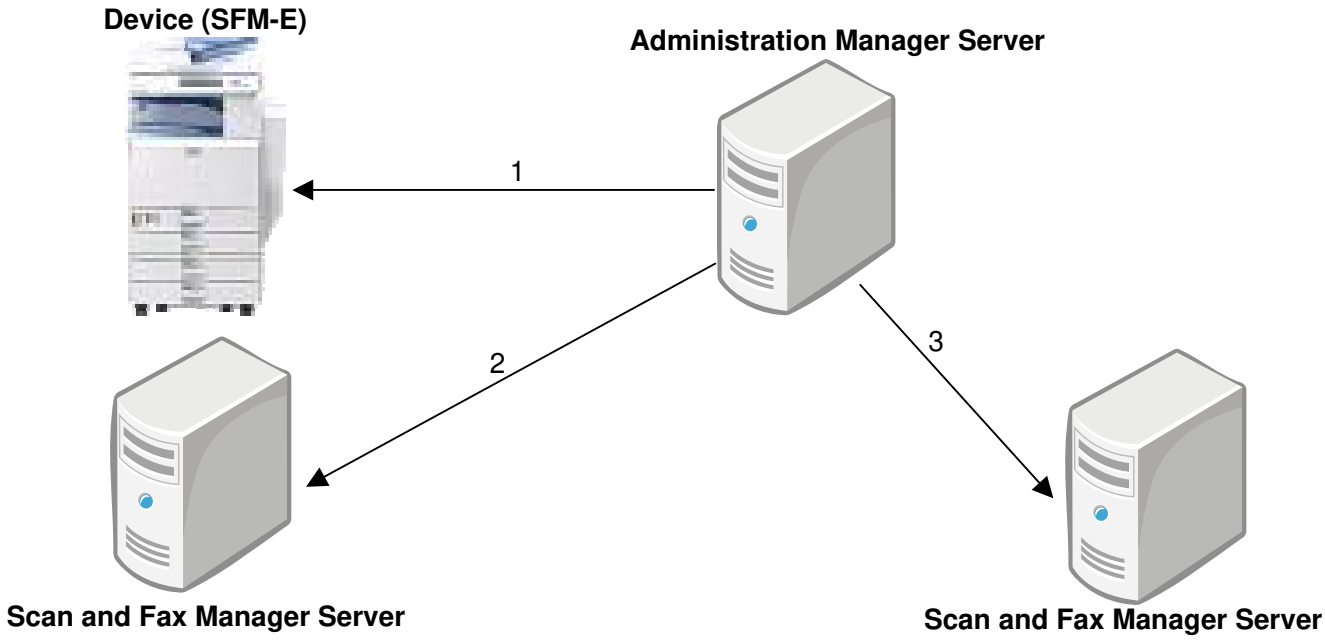
Features	Service	Protocol	Port No	Destination	Description
Decision of port used	ftp	TCP	(No.1) 10021 10020 (No.2) 21, 20	Device	Port No.2 is attempted only when Port No. 1 is unavailable. However, Port No. 2 is not used if a communication error occurs after Port No. 1 has been opened.
Upload Firmware	ftp	TCP	No. 1 or No. 2		
Check update result	ftp	TCP	No. 1 or No. 2		

- Server Configuration (AAM-S)



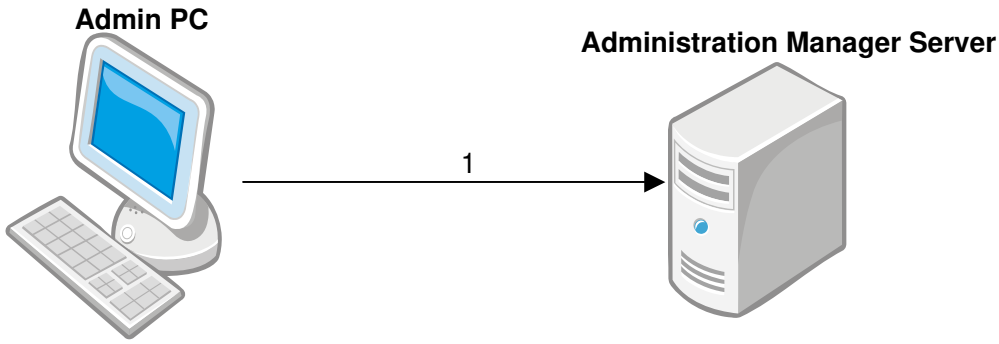
Features	Service	Protocol	Port No	Destination	Description
Batch configuration	HTTP or HTTPS	TCP	Port of AAM-S	AAM Server	Configures the authentication settings for AAM-S.

- Device Assignment (SFM-S)



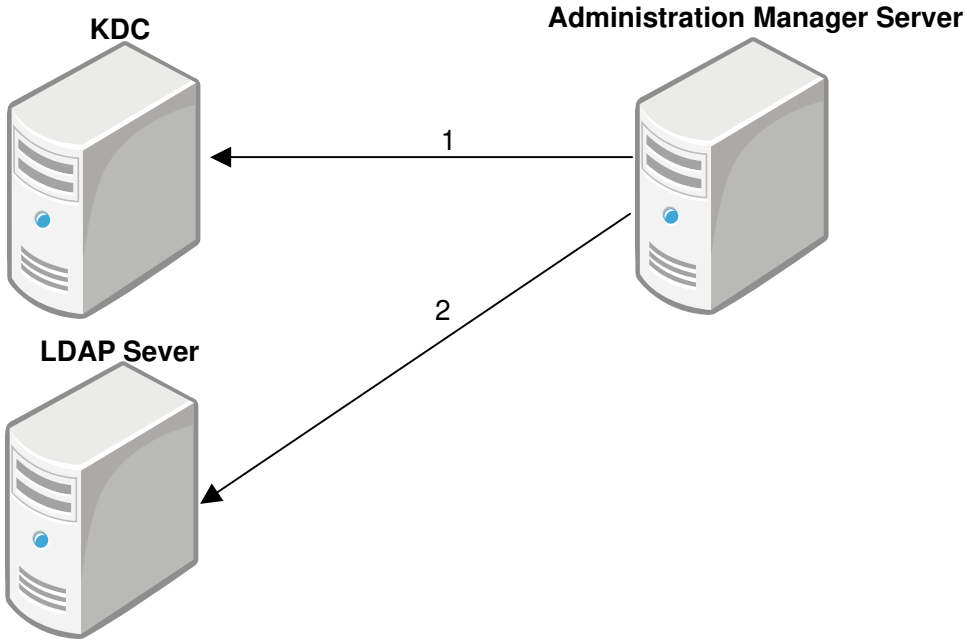
Features	Service	Protocol	Port No	Destination	Description
Update registered SFM-S	HTTPS	TCP	51443	Device	Checks the SFM-S assigned to the device. Updates the SFM-S information if the device is assigned to a different SFM-S.
Remove Device	HTTP or HTTPS	TCP	Port of SFM-S	SFM Server	Deletes the device from the previous SFM-S.
Register Device/Batch configuration	HTTP or HTTPS	TCP	Port of SFM-S	SFM Server	1. Registers the device with the new SFM-S 2. Updates SFM-S settings.

- Administrative Tool



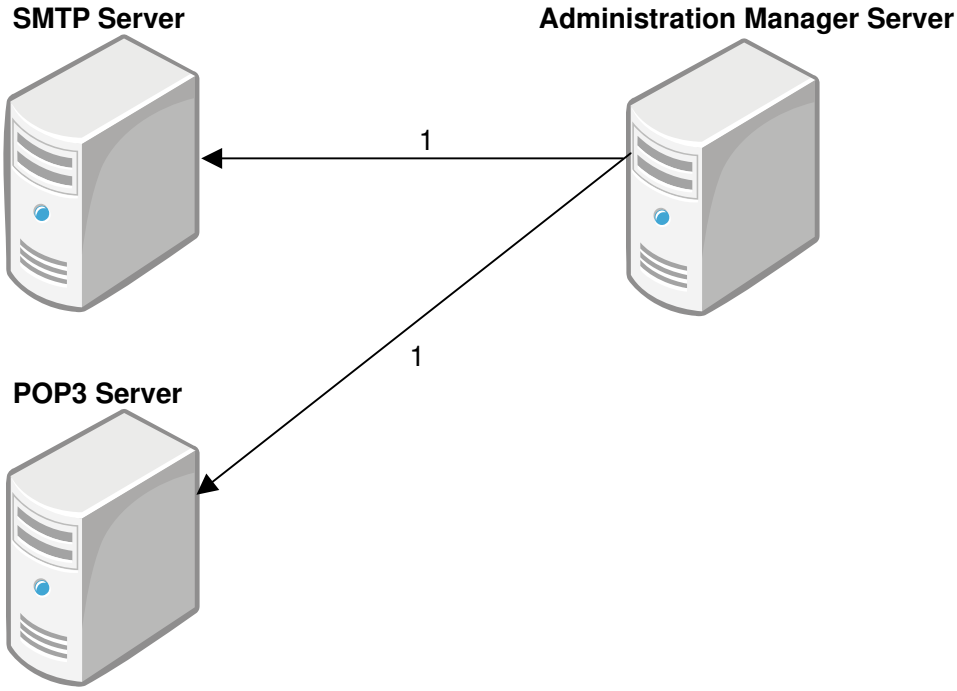
Features	Service	Protocol	Port No	Destination	Description
ADM Server Management	HTTP or HTTPS	TCP	Set during install.	ADM Server	Browser -> Jetty

- Authentication



Features	Services	Protocol	Port No	Destination	Description
Active Directory Authentication	KRB5	TCP	88	KDC Server	
LDAP Authentication	LDAP LDAPS	TCP	389 636	LDAP Server	

- Notification



Features	Service	Protocol	Port No	Destination	Description
Send E-mail1	SMTP	TCP	Port of SMTP Server (default:25)	SMTP Server	This port should match the settings of the SMTP server.
	POP3	TCP	Port of POP3 Server (default:110)	POP3 Server	(optional)To authenticate with POP before SMTP.

4. Data Flow & Storage

4.1 Data types/Location

Data type	Security
Device Data	All device data is stored in the MS SQL Server.
Device Preference Data	All device preferences are stored in the MS SQL Server.
Embedded Application settings	All SDK application data is stored in the MS SQL Server.
Device Software (Firmware, D-SDK, Embedded Application)	Policy and template information is stored in the MS SQL Server. The data (ZIP file) is stored in the local file system. Path: <Install folder>\data\repository
Server Configuration	All data is stored in the MS SQL Server
Log Data	The job log data is stored in the MS SQL Server. The system log is stored in the local file system. Path: <Install folder>\data\logs The debug log and launch log are stored in the local file system. Path: <Install folder>\logs
System Configuration	All data is stored in the MS SQL Server.