Security White Paper for
Streamline NX Secure Print Manager
Version 1.2

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

Document version
SLNXSPMV1.2.0-1.0

Notice:
This document may not be reproduced or distributed in whole or in part, for any purpose or in any fashion without the prior written consent of Ricoh Company Limited. Ricoh Company Limited retains the sole discretion to grant or deny consent to any person or party.

All product names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

Although best efforts were made to prepare this document, Ricoh Company Limited makes no representation or warranties of any kind with regards to the completeness or accuracy of the contents and accepts no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this document.

Document version history:

Version	Date of Issue	Revision
1.0	August, 2011	・ Initial Release This document applies to the following products: Secure Print Manager v1.2.0.0
		・

1. INTRODUCTION 4

2. SYSTEM 5

2.1 SYSTEM OVERVIEW 6
2.1.1 PRINT DATA FLOW FOR SECURE PRINT MANAGER (SERVER). 6
2.1.2 PRINT DATA FLOW FOR SECURE PRINT MANAGER (EMBEDDED). 7
2.1.3 PRINT DATA FLOW FOR DIRECT PRINT (WITHOUT SPM). 7
2.2 SERVICES 8

3. NETWORK PROTOCOLS 9

3.1 PROTOCOLS AND PORTS 9
3.2 RECOMMENDED PRECAUTIONS 9
3.3 SECURITY 10

4. DATA FLOW & STORAGE 12

4.1 STORED DATA - SECURE PRINT MANAGER (SERVER) 12
4.2 DATA ACCESS PERMISSION - SECURE PRINT MANAGER (SERVER) 13
4.3 TO INCREASE THE NUMBER OF LOGS RETAINED/THE MAX SIZE OF A LOG FILE 14
4.4 STORED DATA – SECURE PRINT MANAGER (EMBEDDED) 15
4.5 DATA ACCESS PERMISSION – SECURE PRINT MANAGER (EMBEDDED) 15
4.6 STORED DATA – DIRECT PRINT (WITHOUT SPM) 16
4.7 DATA ACCESS PERMISSIONS – DIRECT PRINT (WITHOUT SPM) 16

1. Introduction

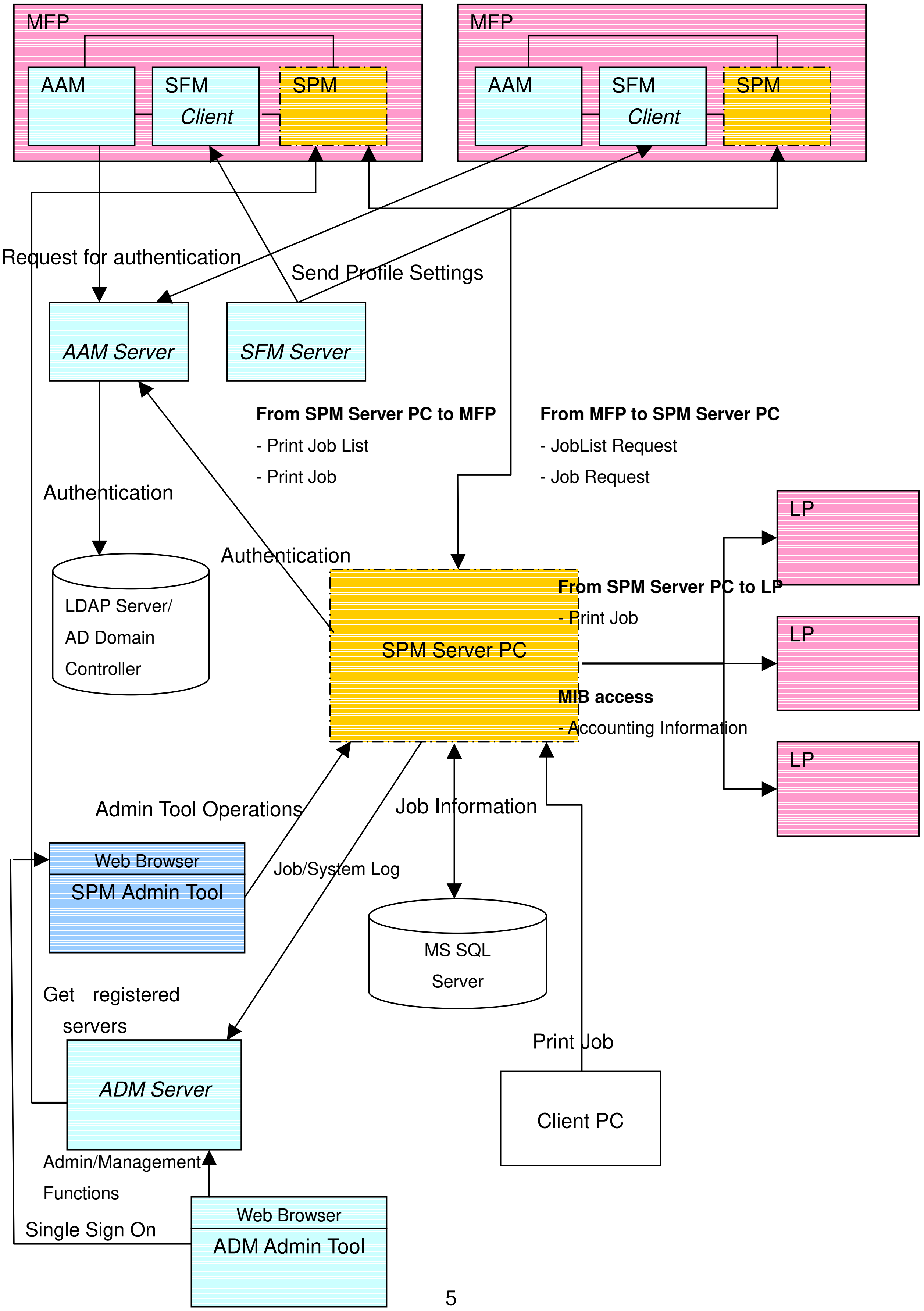
This document provides security information about Streamline NX Secure Print Manager (Server) (SPM-S), Secure Print Manager (Embedded) (SPM-E), and Streamline NX Direct Print.

Secure Print Manager (Server) (SPM-S) is a print server that can be accessed by the SDK/J application Secure Print Manager (Embedded) (SPM-E). Jobs can be submitted to the SPM (Server) and stored there. The jobs can then be accessed and printed via any MFP with the SPM (Embedded) installed. Also, the direct printing for LPs is supported via the Point & Print feature.

Other points:

- Administrators can configure Secure Print Manager (Server) to automatically delete jobs after printing.
- Alternatively, administrators can delete stored jobs manually. Users are able to delete only their own stored jobs.
- Point & Print must be used to distribute drivers from the SPM-S server to users.

2. System

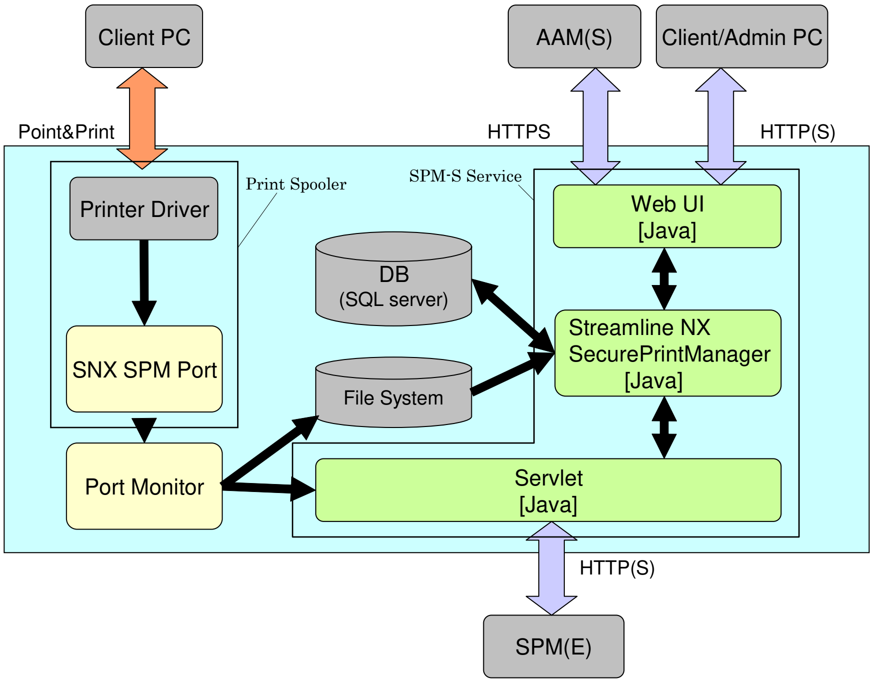

MFP
AAM
SFM Client
SPM
MFP
AAM
SFM Client
SPM
Request for authentication
Send Profile Settings
AAM Server
SFM Server
From SPM Server PC to MFP
- Print Job List
- Print Job
From MFP to SPM Server PC
- JobList Request
- Job Request
Authentication
LDAP Server/
AD Domain
Controller
Authentication
LP
LP
LP
SPM Server PC
From SPM Server PC to LP
- Print Job
MIB access
- Accounting Information
Admin Tool Operations
Job Information
Web Browser
SPM Admin Tool
Job/System Log
MS SQL
Server
Get registered
servers
Print Job
ADM Server
Client PC
Admin/Management
Functions
Single Sign On
Web Browser
ADM Admin Tool

2.1 System overview

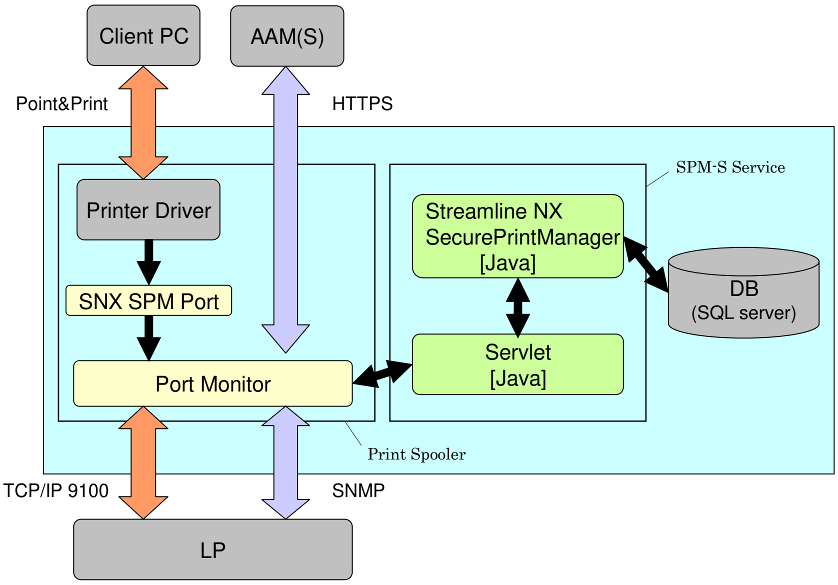
Note: Information about AAM, SFM, and ADM are described in the corresponding Security White Papers.

2.1.1 Print data flow for Secure Print Manager (Server).

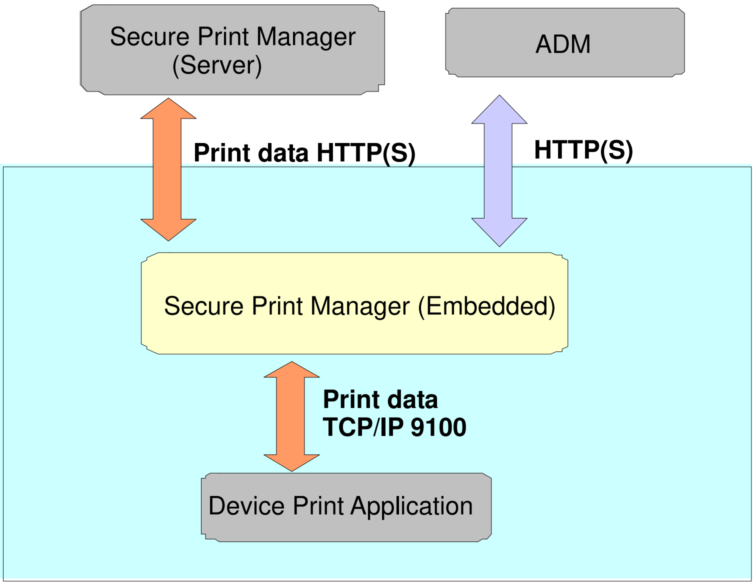
Secure Print with SPM (embedded SDK app):



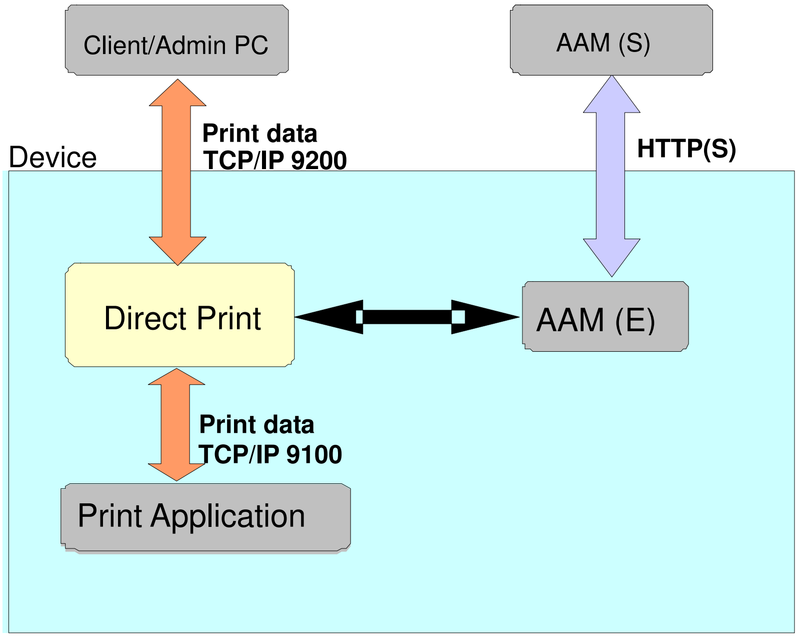
Direct Print (with SPM):



2.1.2 Print data flow for Secure Print Manager (Embedded).



2.1.3 Print data flow for Direct Print (without SPM).



2.2 Services

Services installed or used by SPM-S:

Service Name	Description
Streamline NX Secure Print Manger	The main SPM-S service. This service is installed by SPM-S.
Print Spooler	Spooler service in Windows printing system. This service is a part of Windows.

3. Network Protocols

3.1 Protocols and Ports

Secure Print Manager (Server)

Features	Service	Protocol	Port No	Purpose
PrintSpooler	NetBIOS Session Service	TCP	139	Spooling the job
	SMB	TCP	445	
SPM-S Service	http	TCP	8080（*1）	Administrative Tool/User Job Tool
	https	TCP	8443（*1）	
	http	TCP	8080（*1）	Connection from an MFP/LP
	https	TCP	8443(*1）	
SQL Server（StreamlineNX）	http	TCP	1024 - 65535 (*2)	DB

(*1) Default values: These can only be changed during installation of SPM-S.

(*2) The SQL Server automatically finds a free port to use. The port being used by SQL Server can be found in the SQL Server Configuration Manager:

Secure Print Manager (Embedded)

Features	Service	Protocol	Port No	Destination	Description
Administrative Tool	http	TCP	8080	From Client PC/ADM to SPM (Embedded)	SPM-E configuration web page.
	https	TCP	51443		
Remote Print	http	TCP	8080 (*1)	Secure Print Manager -Server	Job lists and print data transferred from the Secure Print Manager (Server) to the printer that actually prints the job.
	https	TCP	8443 (*1)		Job lists and print data transferred from the SPM-S to the printer via TLS.
Direct Print (diprint)	PDL Data Stream	TCP	9100 (*1)	MFP/LP Print application	

(*1) Default values: These can only be changed during installation of SPM-S.

(*2) SPM-E can act both as a server and as a client

Direct Print

Features	Service	Protocol	Port No	Destination	Description
Direct Print Service	PDL Data Stream	TCP	9200	From client PC to Print Service	

3.2 Recommended precautions

Secure Print Manager uses TLS v1.0 when HTTPS is enabled.

3.3 Security

Connection between the SPM-S server and an MFP/LP (initiated by the MFP)

1) Secure Print with SPM

HTTP or HTTPS can be used to connect to the SPM-S server from an MFP/LP. HTTPS can be enabled by ADM.

- If HTTP is used, the job information is not encrypted. If security is a concern, HTTPS is recommended.

Note: Passwords are not transmitted between the MFP and SPM-S.

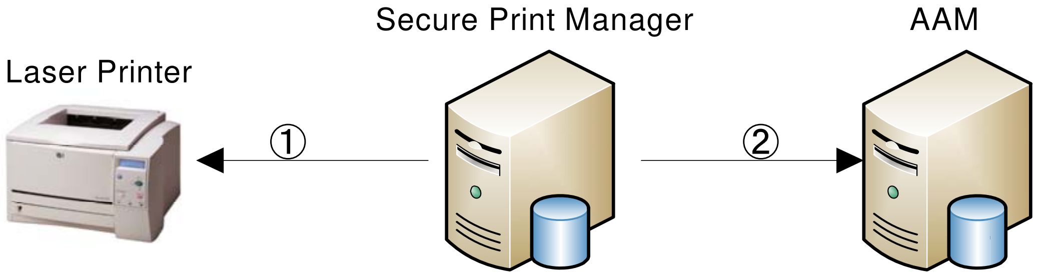
2) Direct Print (with SPM) to Laser Printer (LP)

When using Direct Print for LPs, the Secure Print Manager server (SPM-S) sends the print job data to the LP's TCP/IP port 9100.

SPM-S obtains the number of printed pages from an LP using SNMP. SPM-S continues monitoring the status of the LP through polling (SNMP) until the print job is completed. Then SPM-S registers the collected information on the number of output pages to the AAM server.

Note: The supported versions of SNMP are v1 and v2.

- Collecting and registering the Accounting information.



No.	Purpose	Protocol	Port	Remarks
1	Retrieving the accounting information	SNMP V1/V2	161	The following item is necessary: 1. Read community name
2	Registering the accounting information	HTTPS	Port on AAM-S	Access to AAM-S.

Using HTTPS may cause a decrease of printing performance. The degree of the decrease (if any) depends on the job and the model.

4. Data Flow & Storage

4.1 Stored Data - Secure Print Manager (Server)

Data type	Security
Print data	- Stored in the SPM-S file system. - Encrypted (AES 128-bit). Decrypted before being sent to an MFP/LP. - ***Delete job after printing***: A print job can be deleted automatically after printing is complete. This can be configured by administrators using the web interface's "Delete job after printing" setting. - ***Auto Delete Interval:*** Jobs are stored on the SPM-S server for a certain period of time (configurable) and then automatically deleted once that time has elapsed. This can be configured by administrators using the web interface. This can be used in conjunction with the "Delete job after printing" setting to automatically delete unprinted jobs. - Administrators can manually delete any job via the web interface. - Users can manually delete any of their own jobs via the web interface or the operation panel.
Job Attributes	- Various attributes about each job are stored in the database on the SPM-S server. - These attributes (date, user name, number of pages, etc.) are extracted from submitted jobs and stored in the database. They are then used to display the Job List on the MFP. Note: Passwords are not stored. - Job attributes are deleted when the corresponding job is deleted. Job Attributes are stored in the database unencrypted.
SPM-S System Configuration	- Stored both in the SQL database and the file system. The Web Admin Tool Administrator's password and the password for the database connection are stored encrypted (AES128).
Logs	- Stored in the Windows file system. - Access Log: Access to SNX SPM port and SPM-S service are logged. Administrators can download 2 days worth of Access log entries via the web UI. Service engineers can download the whole Access log. - Error Log: Errors affecting the services “SNX SPM Port” and “SPM-S Service” are logged. Only service engineers can download the Error log. - A new log file is created everyday and will be used for logging for the next 24 hours or until the size of the file reaches 10MB. If the

	log file reaches 10MB a new file will be created and used for the remainder of the 24 hour period or until that file reaches 10MB. - The most recent 20 log files will be retained. Older files are overwritten. Logs are not encrypted.

*1) For information about changing the max size of a log file, please see section 4.3.

*2) For information about changing the number of log files retained, please see section 4.3.

4.2 Data Access Permission - Secure Print Manager (Server)

Data type	Account Type	Permissions	Process
Print data	User	Add	
	SNX SPM Port	Add	- Encrypt and store the print data on the SPM-S hard disk. - Writes job attributes to the DB.
	SPM-S Service	Delete	- "Delete job after printing" - "Auto Delete Interval"
	Administrator	Delete	- Manual deletion via web interface
	User	Delete	- Manual deletion via web interface or the operation panel
System Configuration	Administrator	Edit	- Settings changed via web interface
	SPM-S Service	Edit	- Settings changed via web interface (above) are written to the database.
Logs	SNX SPM Port	Add Delete	- Creates and manages logs.
	SPM-S Service	Add Delete	- Creates and manages logs.
	Field service engineer	Download	- Any existing logs - Both the Access and Error logs relating to the SPM-S port and service.
	Administrator	Download	- Access logs only (most recent 2 days). - Access logs relating to the SPM-S port and service.

4.3 To increase the number of logs retained/the max size of a log file

A. SNX SPM Port

1. Navigate to "Administrative Tools" > "Services" and stop the "Print Spooler" service.
2. Open <install path>\jetty\webapps\spm-s\WEB-INF\conf\port_log4j.properties and edit the values shown in **blue**:

   Access logs:

Number of logs retained	log4j.appender.**port_access**.MaxBackupIndex=**20**
Max file size	log4j.appender.**port_access**.MaxFileSize=**10**MB

   Error logs:

Number of logs retained	log4j.appender.**port_error**.MaxBackupIndex=**20**
Max file size	log4j.appender.**port_error**.MaxFileSize=**10**MB

3. Navigate to "Administrative Tools" > "Services" and start the "Print Spooler" service.

B. SPM-S Service

1. Navigate to "Administrative Tools" > "Services" and stop the "Streamline NX Secure Print manager" service.
2. Open <install path>\jetty\webapps\spm-s\WEB-INF\conf\server_log4j.properties and edit the values shown in **blue**:

Access logs:

Number of logs retained	log4j.appender.**server_access**.MaxBackupIndex=**20**
Max file size	log4j.appender.**server_access**.MaxFileSize=**10**MB

Error logs:

Number of logs retained	log4j.appender.**server_error**.MaxBackupIndex=**20**
Max file size	log4j.appender.**server_error**.MaxFileSize=**10**MB

3. Navigate to "Administrative Tools" > "Services" and start the "Streamline NX Secure Print manager" service.

4.4 Stored Data – Secure Print Manager (Embedded)

Data type	Security
System Configuration	The settings for SPM-E are stored in the device HDD. In addition, the admin password is encrypted using DES. The configuration file can be imported only by administrator. The configuration file is always encrypted.
Log	Administrator can import and export the logs via administrative tool. The log files are not encrypted. The total size for logs is 2MB.

4.5 Data Access Permission – Secure Print Manager (Embedded)

Data type	Account type	Event	Process
System Configuration	System	Add	System creates the initial configuration after installation.
	Administrator (*)	Read Modify	System downloads and modifies the configurations via the administrative tool.
Log	System	Add Delete	System adds and deletes the logs.
	Services Engineer (*)	Read	Services Engineer downloads the log files via administrative tool.

(*) The use of SSL is recommended whenever possible.

4.6 Stored Data – Direct Print (without SPM)

Data type		Security
System Configuration	Listening port number, Destination port number	The settings for Direct Print are stored in the SD card.

4.7 Data Access Permissions – Direct Print (without SPM)

Data	Account Type	Event	Process
System Configuration	System	Read	