Security White Paper

Enhanced Locked Print NX FlexRelease Server V2

Document Version 1.1.0

Solution Support Department
Service and Support Center
Global Marketing Group

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.

Copyright © 2012 by Ricoh Company Ltd.

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
1.0.0	August, 2011	Initial release This document applies to the following products: ・ ELP-NX FS v2.0
1.1.0	March, 2012	This document applies to the following products: ・ ELP-NX FS v2.1

1. Overview

This document contains security information relating to "Enhanced Locked Print NX FlexRelease server (ELP-NX FS)".

ELP-NX FS is a print server that can be accessed by the SDK/J application "Enhanced Locked Print NX (ELP-NX)". Jobs can be submitted to the ELP-NX FS server and stored there. These jobs can then be accessed via any MFP running ELP-NX v1.3 or later, and printed.

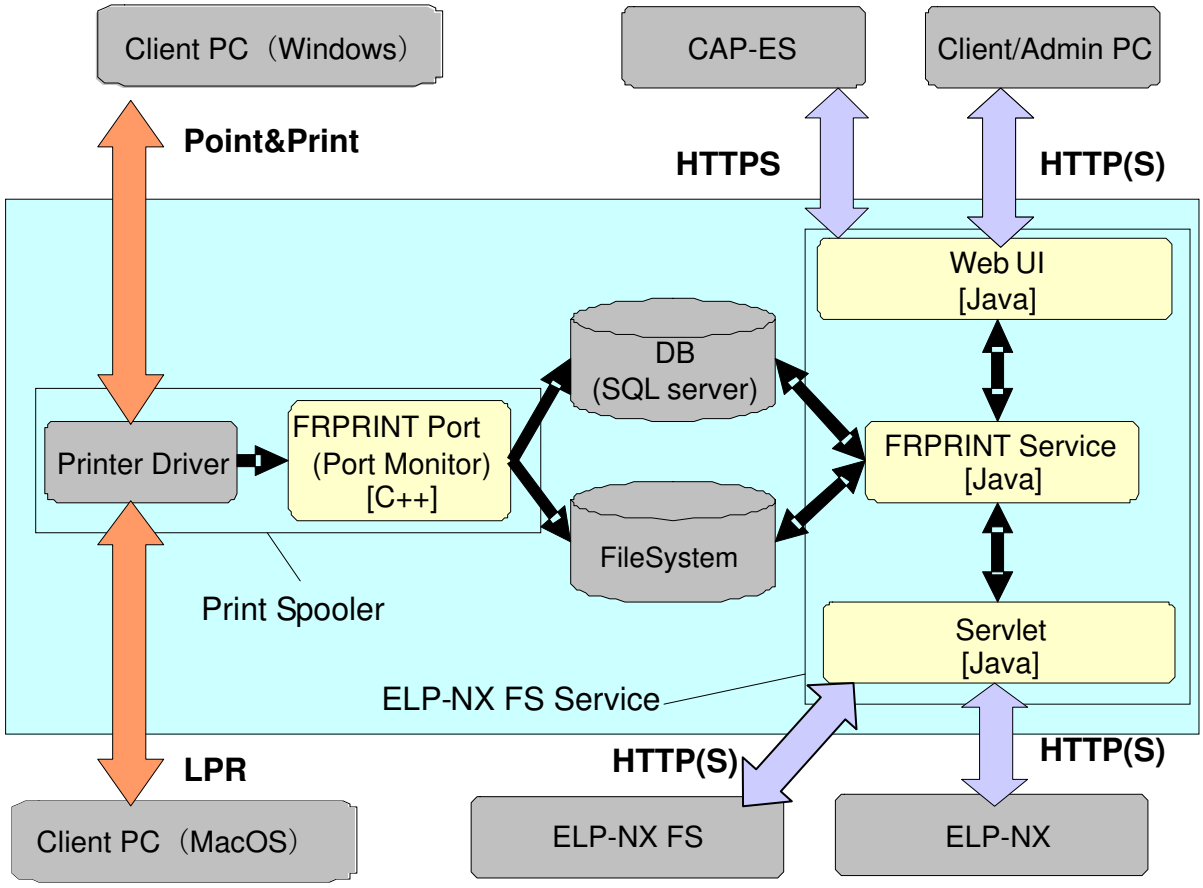
Other points:

- Users can decide whether to delete or save their job data after printing directly from the device's operation panel.
- Alternatively, administrators can delete any stored jobs manually. Users are able to delete only their own stored jobs.
- Point & Print must be used to distribute drivers from the ELP-NX FS server to users.

2. System Security

2.1 System overview

Note: Information about CAP-ES is described in the Card Authentication Package/Card Authentication Package Enterprise Server Security White Paper.



The table below shows what data is transmitted over the network:

Communication Route	**Transmitted Data**
CAP-ES <-> Web UI (HTTPS)	The username and password used for logging into the Web UI
Client/AdminPC <-> WebUI（HTTP/HTTPS）	Print job information (user name, document name, etc.) My Document Folder information (user name, PIN, etc.) Configuration information (authentication settings, etc.) Debug log, Delete log. Username and password used for logging into the Web UI
ELP-NX <-> Servlet (HTTP/HTTPS)	Print job information (user name, document name, etc.) My Document Folder information (user name, PIN, etc.)
ELP-NX FS <-> Servlet (HTTP/HTTPS)	Print job information (user name, document name, etc.)

Note: Passwords transmitted between ELP-NX and ELP-NX FS are encrypted using AES128. Passwords transmitted between the client PC and the web UI are not encrypted.

2.2 Network

2.2.1 Network related services and protocols/ports used

Features	Service	Protocol	Port No	Destination	Description
Job Storage (Windows)	Print Spooler	TCP	445 (*1)	Client PC	SMB
Job Storage (Mac)	Print Spooler	TCP	515 (*1)		LPR
Administrative Tool (no encryption)	FRPRINT Service	TCP	8080 (*1)(*3)		HTTP
Administrative Tool (encryption)	FRPRINT Service	TCP	8443/TCP (*1)(*3)		HTTPS
Administrative Tool (authenticaton enabled)	FRPRINT Service	TCP	18443 (*2)(*3)	CAP-ES	HTTPS
On Demand Print(ELP-NX)	FRPRINT Service	TCP	8080 (*1)(*3)	Device (ELP-NX)	HTTP
On Demand Print(ELP-NX)	FRPRINT Service	TCP	8443 (*1)(*3)		HTTPS
RemoteDB connection	SQL Server (FRPRINT)	TCP	1024-65535 (*2)	DB Server	SQL
RemoteDB connection	SQL Server Browser	UDP	1434 (*2)		SQL

(*1) Ports opened by ELP-NX FS (on the ELP-NX FS side)

(*2) Ports opened on the server side when ELP-NX FS connects to the server as a client

(*3) Default ports that can be changed

Services

Services installed or used by ELP NX-FS:

Service Name	Description	Remarks
SQL Server (FRPRINT)	Database service	The instance name specified when the SQL server is installed.
SQL Server Browser	The service used for database name resolution.	Only used when the SQL Server is installed as a named instance.
Print Spooler	This is a spooler service in Windows printing system. This service is a part of Windows.	
Server	Job storage	
Task Scheduler	Scheduled processes	
FRPRINT Service	The ELP-NX FS Web Service	
TCP/IP Print Server	LPD service	Only used when the MacOS (LPR) client is used.

2.2.2 Security

1) Connection to the ELP-NX FS Administrative Tool

HTTP or HTTPS can be used to connect to the ELP-NX FS Administrative Tool (web interface). The administrator password can be changed using the tool, but the password is not encrypted if HTTP is used. If security is a concern, HTTPS is recommended. TLS v1.0 is used when SSL is enabled.

2) Connection between the ELP-NX FS server and an MFP/LP (initiated by the MFP)

HTTP or HTTPS can be used to connect to the ELP-NX FS server from an MFP/LP. Whether HTTP or HTTPS is used is configured in ELP-NX (SDK app).

- If HTTP is used, the username is transmitted unencrypted when viewing the job list, printing a job or deleting a job. If security is a concern, HTTPS is recommended.

Using HTTPS might decrease printing performance. The degree of this decrease (if any) depends on the job and the model.

2.3 Stored data

2.3.1 Data types

Data type	Security

Print data	- Stored in the ELP-NX FS file system.
	- Storage path is configured using the "Job Storage Path" parameter.
	- Encryption of the stored print data can be enabled or disabled using the "Encrypt Job Data" option. If enabled, the print data is encrypted using AES128.
	- The print data is sent over the network unencrypted (if stored as encrypted data, it will be decrypted before being sent to an MFP/LP).
	- Jobs are deleted in any of the below cases:
	  - Deleted/printed from the ELP-NX operation panel. *
	  - Deleted from the ELP-NX FS Administrative tool (web UI). *
	  - Deleted from the ELP-NX FS User tool (web UI). *
	  - Auto-deleted periodically. *
	* Job deletion is affected by the system configuration. Please see the Administrator's Guide for more information.

Job Attributes	- Various attributes about each job are stored in the database on the ELP-NX FS server. - Job 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 stored unencrypted. - Job attributes are sent over the network unencrypted. - Job attributes are deleted when the corresponding job is deleted.

My Document Folder Information	- Stored in the database if "Use My Document Folder" option in the "Authentication Settings" of the Administrative Tool is selected.
	- The information is created:
	  - When a user with no Folder submits a print job
	  - Manually from the ELP-NX FS Administrative tool
	- The information is modified:
	  - from the ELP-NX operation panel
	  - from the ELP-NX FS Administrative took (web UI)
	  - from the ELP-NX FS User tool (web UI)
	- The information is deleted:
	  - manually from the ELP-NX FS Administrative tool (web UI)
	  - auto-deleted periodically
	- User PINs are encrypted using AES128.
	- My Document Folder data (excluding the PIN) is transferred in unencrypted form.

ELP-NX FS System Configuration	- Configurable from the ELP-NX FS Administrative tool. - Stored in the database without encryption (authentication settings, parameter settings).

Internal User Information	- Internal Users Information includes:
	  - Default administrator password.
	  - SQL DB sa user name and password.
	- Administrator's password can be changed from the Administrative tool (web UI).
	- The sa's username and password can be changed from the Management Tool.
	- Information is stored on the server and encrypted (AES128).

Debug Logs	- Stored locally.
	- Can be downloaded from the Administrative tool.
	- Debug logs are created by the following modules:
	  - FRPRINT Port. (max. of 10MB x 30 files*)
	  - FRPRINT Service. (max. of 10MB x 30 files*)
	- Once 30 files have been created, the oldest file is overwritten.
	*default value

Delete Logs	- Stored both in the database and locally. - Can be downloaded from the Administrative tool. - Log entries older than 60 days cannot be downloaded. - Log entries older than 60 days are deleted daily at 5:30 AM.

2.3.2 Operations performed on data

Data type	Performed by	Event	Notes
Print data	User	Add	
	ELP-NX FS Port	Add	- Encrypt and store the print data on the ELP-NX FS hard disk. - Write job attributes to the DB.
	ELP-NX FS Service	Delete	- "Delete job after printing" - "Auto Delete Interval"
	Administrator	Delete	- Manual deletion via web interface - A single job or all jobs belonging to a specific user can be deleted.
	User	Delete	- Manual deletion via web interface or the operation panel - Users can delete any of their own jobs.
System Configuration	Administrator	Edit	- Settings changed via web interface
	ELP-NX FS Service	Edit	- Settings changed via web interface (above) are written to the database. - The admin password is saved on the hard disk.
Logs	ELP-NX FS Port	Add Delete	- New log file created daily and in 10MB intervals. In other words, every time the log exceeds 10MB in a single day, a new log file is created. - The most recent 20 log files are retained.

	ELP-NX FS Service	Add Delete	- New log file created daily and in 10MB intervals. In other words, every time the log exceeds 10MB in a single day, a new log file is created. - The most recent 20 log files are retained.
	Field service engineer	Download	- Any existing logs - Both the Access and Error logs relating to the ELP-NX FS port and service.
	Administrator	Download	- Access logs only (most recent 2 days). - Access logs relating to the ELP-NX FS port and service.

2.3.3 Initialization of the administrator password

If the administrator password is forgotten, the password can be re-initialized as follows:

1. Navigate to "Administrative Tools" > "Services" and stop the "Enhanced Locked Print NX Flex Release Server Service" service.
2. Delete the file "<install path>\jetty\webapps\elp-nx-fs\WEB-INF\data\admin.properties ".
3. Navigate to "Administrative Tools" > "Services" and start the "Enhanced Locked Print NX Flex Release Server Service" service.

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

The size and number of Debug Log files can be changed using the following procedure.

1. Stop the services listed below:
   - FRPRINT Service
   - Print Spooler
   - TCP/IP Print Server (if print jobs from a Mac OS device are stored)
   - Task Scheduler

2. Open the settings file and edit the values shown in **blue**:

■ FRPRINT Port

Settings file	<install path>\conf\FRPortMonitorLog.xml
File count	<entry key="LogRotation">**30**</entry>
File size (in bytes)	<entry key="LogRotationSize">**10485760**</entry>

■ FRPRINT Service

Settings file	<install path>\jetty\webapps\frprint\WEB-INF\conf\server_log4j.xml
File count	<param name="MaxBackupIndex" value="**20**"></param>
File size	<param name="MaxFileSize" value="**10**MB"></param>

3. Re-start the services stopped in step 1.