

Security White Paper

Enhanced Locked Print NX 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 following product. <ul style="list-style-type: none">• Enhanced Locked Print NX v2.0
1.1.0	March, 2012	This document applies to following product. <ul style="list-style-type: none">• Enhanced Locked Print NX v2.1

1. OVERVIEW 4

2. DOCUMENT WORKFLOW SECURITY 4

3. SECURITY DATA SHEET 5

3.1. OVERVIEW 5

3.2. NETWORK 6

PROTOCOLS AND PORTS 6

RECOMMENDED PRECAUTIONS 6

3.3. STORED DATA AND PROCESSES 7

STORED DATA 7

PROCESSES 8

RECOMMENDED PRECAUTIONS 8

DATA TYPE AND ENCRYPTION 9

1. Overview

This document describes the security information for Enhanced Locked Print NX (ELP-NX).

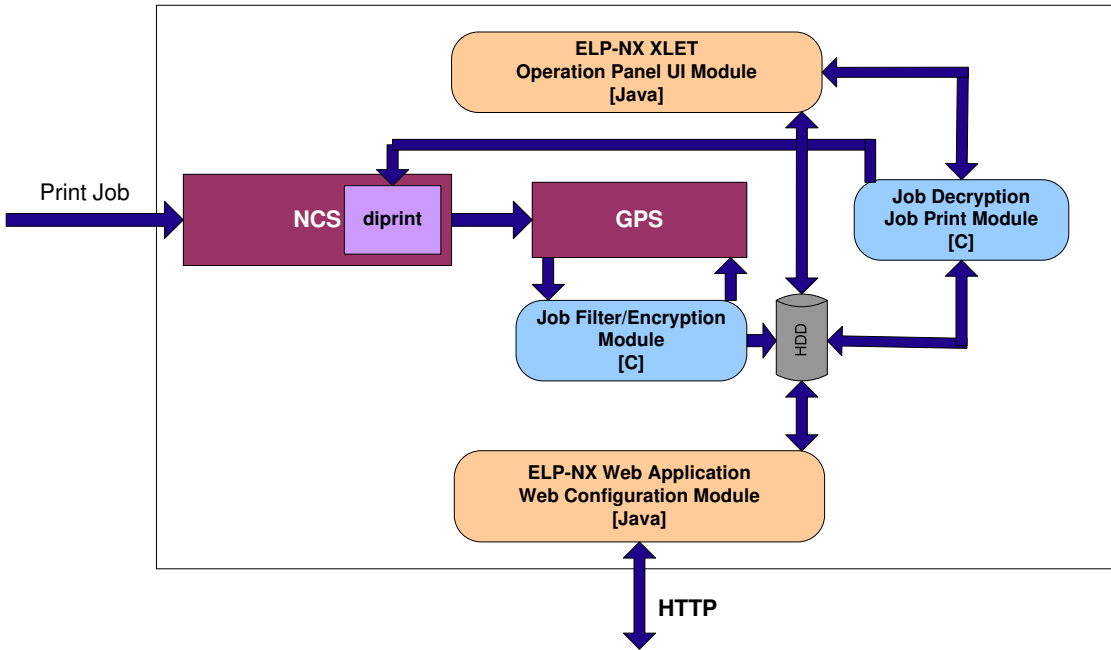
2. Document Workflow Security

If a user leaves a confidential document on a shared MFP, an unauthorized user may see it and print it. ELP-NX prevents such unauthorized access. ELP-NX forces users to be authenticated before printing stored jobs. Traditional manual entry and IC card-based authentication are both supported. Stored jobs can be retained for later access, or deleted after printing for security.

3. Security Data Sheet

This section describes the details of print data flow and network protocol and port used in ELP-NX.

3.1. Overview



3.2. Network

Protocols and Ports

Features	Service	Protocol	Port No	Destination	Purpose
DNS Setup	DNS	UDP	53 (*1)	DNS Server	Name resolution
P2P (ELP-NX to ELP-NX)	FRPRINT (ELP-NX)	TCP	8080 (*4)	ELP-NX	User/Job List acquisition, User information editing, Delete print request
ELP-NX FS connection (Default)	FRPRINT (ELP-NX FS)	TCP	8080 (*1)(*3)	ELP-NX FS	User/Job List acquisition, User information editing, Delete print request
ELP-NX FS connection (SSL)	FRPRINT (ELP-NX FS)	TCP	8443 (*1)(*3)	ELP-NX FS	User/Job List acquisition, User information editing, Delete print request
Print via Standard TCP/IP	Standard TCP/IP	TCP	9100/ (*2)	Client PC	Spool
LPR Print	LPR	TCP	515 (*2)		Spool
IPP Print	IPP	TCP	631 (*2)		Spool
IPPS Print	IPPS	TCP	433 (*2)		Spool
Job Deletion Tool	FRPRINT (ELP-NX)	TCP	8080 (*2)		Job Deletion Tool (HTTP)
Web Image Monitor	HTTP	TCP	80 (*2)		WebImageMonitor
Web Image Monitor (SSL)	HTTPS	TCP	443 (*2)		WebImageMonitor
Configuration Tool	FRPRINT (ELP-NX)	TCP	8080 (*2)	Management Client PC	Configuration Tool (HTTP)
Configuration Tool (SSL)	FRPRINT (ELP-NX)	TCP	51443 (*2)		Configuration Tool (HTTPS)
Configuration Tool	FRPRINT (ELP-NX)	UDP	50007 (*2)		Device search (Discovery)

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

(*2) Ports opened by ELP-NX

(*3) Port can be changed.

(*4) ELP-NX acts as both a client and a server.

Recommended precautions

Configuration Tool

HTTP or HTTPS can be used to connect from ELP-NX to the Configuration Tool. When changing the administrator's password, using HTTPS is recommended because the password is not encrypted if HTTP is used. ELP-NX uses TLS v1.0 when HTTPS is enabled.

3.3. Stored Data and Processes

Stored Data

Data Type	Specifications
Print Job	Print jobs are stored on the device HDD with blowfish encryption.
Job DB	This database manages the stored print jobs for each user. This database is encrypted.
System Configuration	The settings for ELP-NX are stored on the device HDD. In addition, the password is encrypted using AES 128-bit. The configuration file can be imported only by administrator. The configuration file is always encrypted.
Log	Administrator can import and export the logs via Configuration Tool. The log files are not encrypted. The following logs are available: - Delete Log - Analyze Log

Processes

Data Type	Account Type	Action	Description
Print Job DB	System	Add Delete	System stores the print job in the local HDD and encrypts it. System deletes the stored job(s) after a certain period, if the “Auto delete timer” function is enabled.
	Administrator	Read Delete	Used for administrator actions (check job list, delete stored jobs).
	User	Delete	User reads and deletes job(s) via the operation panel.
System Configuration	System	Add	System creates the configurations after installed.
	Administrator (*)	Read Modify	System downloads and modifies the configurations via administrative tool.
Log	System	Add Delete	System adds and deletes the logs.
	Services Engineer (*)	Read	Service Engineer downloads the log files via administrative tool.

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

Recommended Precautions

If all delete options are disabled, the device’s HDD may become full due to the number of stored jobs. If the automatic deletion functions are not used, please manage the stored jobs to ensure that the device HDD does not become full.

Data Type and Encryption

●: AES 128-bit Encryption

○: Plain Text or AES 128-bit Encryption, depending on the settings

△: Plain text only

—: Data not stored/transmitted

Data Type	System Log (*1)	Delete Log	Network Communication (*2)				HDD Storage (*3)
			Administrator PC to ELP-NX	User PC to ELP-NX	P2P	ELP-NX FS	
User Name/User ID	△	△	○	○	△	○	○
Password	—	—	●	—	●	●	●
Display Name	△	△	○	—	△	○	○
Job info (e.g. job's name)	△	△	○	○	△	○	● (*4)
Host Name/IP (Print Client)	△	△	○	—	△	—	○
Host Name/IP (ELP-NX FS)	△	△	○	—	—	○	○
Configuration Tool password	—	—	●	—	—	—	●

(*1) Some log information can be masked using the Log Masking Tool.

(*2) The items marked with ○ can be encrypted through HTTPS connection.

(*3) Encryption is only available through the HDD encryption option.

(*4) If the [Encrypt Stored Document] option setting is enabled. This encryption will stack with the HDD encryption option for extra security.