Issued September 21st, 2012

Security White Paper
for
Device Manager NX Lite

Solution Support Department
Service and Support Center
Global Marketing Group
Ricoh Company, Ltd.

Document version: 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	September, 2012	1st Release

1. Introduction

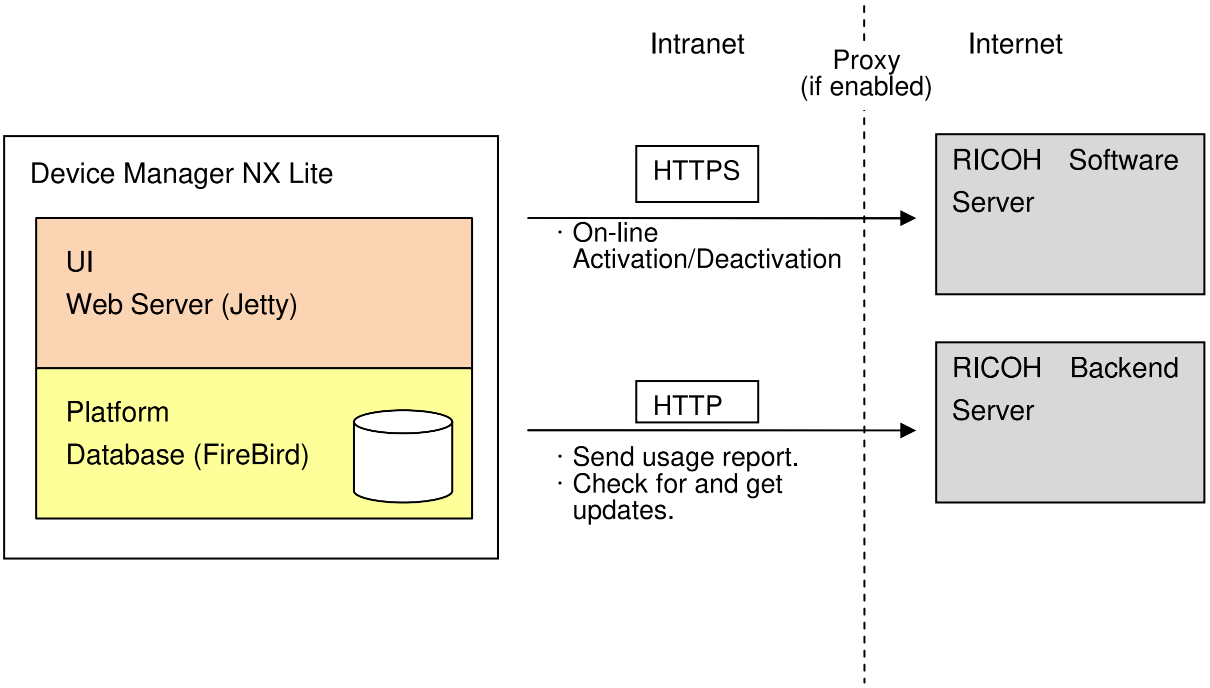
Device Manager NX Lite is device management software which provides basic remote device management functions, such as batch configuration and device monitoring, from the comfort of the administrator’s desktop. Even though it is free software, it can still be used to manage up to 250 devices.

This document is designed to describe the product’s functioning with regards to network and data security. As Ricoh products are designed for use inside an intranet where network clients are protected by firewalls, they rely heavily on the intranet’s security policies. This document focuses on providing the information necessary to protect against potential threats from external security risks and help customers to securely incorporate the Ricoh product into their system.

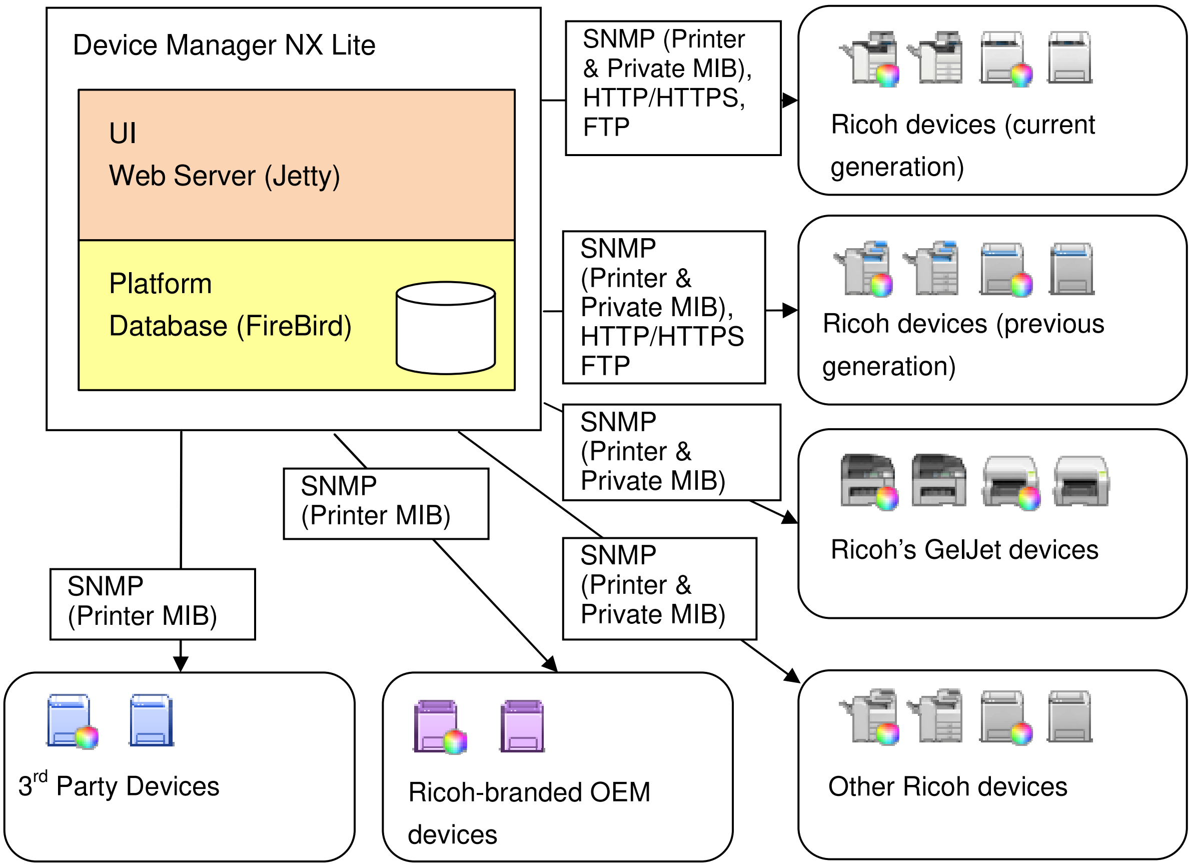
2. System

These diagrams show the general data flow for Device Manager NX Lite.

2.1. Internet communication diagram



2.2. Intranet communication diagram


Device Manager NX Lite
UI
Web Server (Jetty)
Platform
Database (FireBird)
SNMP (Printer & Private MIB), HTTP/HTTPS, FTP
Ricoh devices (current generation)
SNMP (Printer & Private MIB), HTTP/HTTPS FTP
Ricoh devices (previous generation)
SNMP (Printer & Private MIB)
Ricoh's GelJet devices
SNMP (Printer MIB)
SNMP (Printer & Private MIB)
SNMP (Printer MIB)
3rd Party Devices
Ricoh-branded OEM devices
Other Ricoh devices

The icons shown here for each device category are identical to the icons used by the Device Manager NX Lite UI.

3. Data Flow

3.1. Internet communication data flow

Data Flow	Functions	Data
Device Manager NX Lite -> RICOH Software Server	Activation/Deactivation	Product Key, Lock Code, License File
Device Manager NX Lite -> RICOH Backend Server	Usage Report	Country GUID (Product code + lock code) OS Report Date & Time Installed Date Product Name Product Version Product Option Number of devices per vendor Breakdown of Ricoh devices by generation, model type, etc. Serial numbers for up to 3 devices (Ricoh devices only, same model*)
	Software Update Notification	Product Version

*The target model is selected by choosing the device with the largest number of devices. If multiple devices of that model exist, the models with the 1st, 2nd, and 3rd largest total counters are selected for inclusion in the Usage Report.

3.2. Intranet communication data flow

Data Flow	Functions	Data
Device Manager NX Lite -> 3rd Party Devices	Collect device information.	Device's status, supply, and counter information. No user counter.
Device Manager NX Lite -> Ricoh-branded OEM devices	Collect device information.	Device's status, supply, and counter information. No user counter.
Device Manager NX Lite -> Ricoh GelJet devices	Collect device information.	Device's status, toner/supply, and counter information. No user counter.
Device Manager NX Lite -> Other Ricoh devices	Collect device information.	Device's status, toner/supply, and counter information. No user counter.
Device Manager NX Lite -> Ricoh previous generation devices	Collect device information.	Device's status, toner/supply, and counter information. With user counter.
	Basic Device Preferences	Basic device configuration.
	Address book preference	Address book configuration.
	Energy saving setting	Power status changes.
Device Manager NX Lite -> Ricoh current generation devices	Collect the device's information.	Device's status, toner/supply, and counter information. With user counter.
	Basic Device Preferences	Basic device configuration.
	Advanced Device	Advanced device configuration.

	Preferences	
	Address book preference	Address book configuration.
	Power Mode preference	Power status changes.

4. Access account

Device Manager NX Lite uses 3 types of access accounts to communicate with devices.

4.1. SNMP Access Account

The following access account is used for SNMP communication:

[Using SNMP V1/V2]
Read community (default value is “public”)
Write community (default value is “admin”)

[Using SNMP V3]
Username (default value is “admin”)
Password (default value is none)
Authentication algorithm [MD5/SHA1] (default value is “MD5”)
Encryption password (default value is none)
Encryption algorithm [DES/AES128] (default value is “DES”)
Context Name (default value is “GWNCS”)

Note: The account must have full device administrator privileges (User Administrator, Machine Administrator, Network Administrator, and File Administrator)

4.2. Web Access Account

This access account is used for web service (HTTP/HTTPS) communication:

Username (the default value is “admin”)
Password (the default value is blank)

Note: The account must have full device administrator privileges (User Administrator, Machine Administrator, Network Administrator, and File Administrator)

4.3. SDK access account

This access account is used for collecting SDK application information from the device.

Password (the default value is encrypted, and this is not editable.)

5. Protocols and Ports

5.1. Discovery

	Operation	Protocol	Port	Access Account	Notes
1	Collecting device information. (Device Manager NX Lite -> Device)	SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	Devices with one of the following MIBs can be registered: · sysObjectID · prtGeneralConfig Changes · Ricoh Search Function
2	Confirming the web access account. (Device Manager NX Lite -> Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Web access account	
3	Collecting SDK information. (Device Manager NX Lite -> Device)	FTP and HTTPS	TCP/21 TCP/51443	Web access account SDK access account	FTP is used to check for the SDK Platform. Disabling FTP on the device does not affect this process.

5.2. Device Polling (Status)

	Operation	Protocol	Port	Access Account	Notes
1	Collecting device status information. (Device Manager NX Lite -> Device)	SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	

5.3. Device Polling (Tray/Toner Ink)

	Operation	Protocol	Port	Access Account	Notes
1	Collecting device Tray/Toner Ink information. (Device Manager NX Lite -> Device)	SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	

5.4. Device Polling (Counter)

	Operation	Protocol	Port	Access Account	Notes
1	Collecting device Counter	SNMP	UDP/161	SNMP V1/V2:	

	information. (Device Manager NX Lite -> Device)			Read Community Or SNMP V3 access account	

5.5. Device Polling (Other)

	Operation	Protocol	Port	Access Account	Notes
1	Collecting device Other information, such as MAC address, etc. (Device Manager NX Lite -> Device)	SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	
2	Collecting SDK information (Device Manager NX Lite -> Device)	FTP and HTTPS	TCP/21 TCP/51443	Web access account & SDK access account	FTP is used to check for the SDK Platform. Disabling FTP on the device does not affect this process.

5.6. Device Polling (User Counter)

	Operation	Protocol	Port	Access Account	Notes
1	Confirming the device’s response. (Device Manager NX Lite -> Device)	SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	
2	Collecting User Counter information. (Device Manager NX Lite -> Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Web access account	

5.7. Advanced Device Preferences

	Operations	Protocol	Port	Access Account	Notes
1	Confirming the device’s response. (Device Manager NX Lite -> Device)	SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	
2	Collecting preference information. (Device Manager NX Lite -> Device)	HTTP/SOAP or HTTPS/	TCP/80 or TCP/443	Web access account	

		SOAP			
3	Configuring device preferences. (Device Manager NX Lite -> Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Web access account	

5.8. Basic Device Preferences

	Operation	Protocol	Port	Access Account	Notes
1	Confirming the device's response. (Device Manager NX Lite -> Device)	SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	
2	Collecting preference information. (Device Manager NX Lite -> Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Web access account	
		SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	
3	Configuring device preferences. (Device Manager NX Lite -> Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Web access account	
		SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	
4	Restarting the device. (Device Manager NX Lite -> Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Web access account	

5.9. Address Book Preferences

	Operation	Protocol	Port	Access Account	Notes
1	Confirming the device's	SNMP	UDP/161	SNMP V1/V2:	

	response. (Device Manager NX Lite -> Device)			Read Community Or SNMP V3 access account	
2	Collecting Address Book information. (Device Manager NX Lite -> Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Web access account	
3	Configuring the Address Book. (Device Manager NX Lite -> Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Web access account	

5.10. Power Mode

	Operation	Protocol	Port	Access Account	Notes
1	Confirming the device's response. (Device Manager NX Lite -> Device)	SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	
2	Configuring the power mode. (Device Manager NX Lite -> Device)	SNMP	UDP/161	SNMP V1/V2: Read Community Or SNMP V3 access account	

5.11. Activation/Deactivation

Activation/deactivation is internet-based, so this communication must pass through the proxy server, if one is in use.

	Operations	Protocol	Port	Access privileges	Note
1	Confirm the request for Activation/Deactivation. (Device Manager NX Lite -> Ricoh Software Server)	HTTPS	TCP/443	Retained in Device Manager NX Lite	

5.12. Usage Report/Update Notification

Usage Reports and Update Notifications are internet-based, so th

	Operations	Protocol	Port	Access privileges	Note
1	Transmit usage reports & check for updates. (Device Manager NX Lite ->	HTTP	TCP/80	Retained in Device Manager NX Lite	Device Manager NX Lite does not support direct

	Ricoh Backend Server)				downloading of update data.

Note
-The port number cannot be changed.
-Device Manager NX Lite initiates all network communication. Also, Device Manager NX Lite has no open ports in order to prevent an unauthorized external connection.

6. General Security Considerations

6.1. Security Considerations

As devices do not have secure communication enabled by default, communication between Device Manager NX Lite and devices is not encrypted by default. Please configure HTTPS and SNMPv3 settings if secure protocols are required.
When Device Manager NX Lite communicates with a device via SSL/TLS communication (depends on device configuration), Device Manager NX Lite uses a certificate to encrypt the communication, but does not check the validity of the certificate. Also, importing a device certificate to the PC where Device Manager NX Lite is installed has no effect, as Device Manager NX Lite does not support custom certificates.

If a device has both HTTP and HTTPS enabled, HTTPS is used.

Device Manager NX Lite supports the following ciphers/encryption protocols:
-Hash- SHA-2 (SHA-256)
-Public Key- RSA2048
-Common Key- AES256, AES128, or 3TDEA

7. Stored Data

7.1 Stored Data

Data	Item	Detail
Device Data	Encryption	Not encrypted. Device Data is stored in a DB. The DB has no encryption or other protection. However, it has no ports in order to prevent external connections. The DB is created in the following directory: <Install Folder>¥data¥database¥firebird¥ Device Manager NX Lite uses a special account and password to access that DB. The account and password are encrypted using Blowfish (128-bit) and are stored in gc.properties: <install folder>¥configuration¥gc.properties
	Back-up	Included in the System Back-up.
	Log Entry	None.
	Remarks	None.
Device Access Account Data	Encryption	Not encrypted. Access Account Data is stored in the same DB as Device Data.
	Back-up	Included in the System Back-up.
	Log Entry	None.
	Remarks	None.
Configuration Data (Template/Task)	Encryption	Not encrypted. Configuration Data is stored in the same DB as Device Data. In addition, Address Book Preferences and Advanced Device Preferences are encrypted using AES (256-bit) and are stored in the repository: <install folder>¥data¥repository¥
	Back-up	Included in the System Back-up.
	Log Entry	Task results are recorded in the Task Logs.
	Remarks	None.
System Settings	Encryption	Not encrypted. System Settings are stored in the same DB as Device Data. In addition, some information is also stored in gc.properties: <install folder>¥configuration¥gc.properties The license code, authentication credentials for the eDC Server, and the password of the Proxy Server account are encrypted using Blowfish (128-bit). The other settings are stored in plain text. Information stored in only the DB file: -Custom Properties

		-System Data Settings Information stored in both the DB file and settings file: -Activation and Usage Report Settings -Proxy Settings -Display Settings
	Back-up	Included in the System Back-up.
	Log Entry	Configuration of system settings are not recorded in System Logs.
	Remarks	None.
System Password	Encryption	Not encrypted. The System Password is stored in the same DB as Device Data.
	Back-up	Included in the System Back-up.
	Log Entry	Changes to the system password are not recorded in the System Logs.
	Remarks	Use of a blank password is supported.
Logs (Task, System, Notification)	Encryption	Not encrypted. The Logs are stored in the same DB as Device Data.
	Back-up	Included in the System Back-up.
	Log Entry	-
	Remarks	None.
Back-up Data	Encryption	None. The Back-up Data is just a copy of the DB file.
	Back-up	-
	Log Entry	The result of the back-up process is recorded in the System Logs.
	Remarks	None.
Debug Log	Encryption	Plain text. Not Masked.
	Back-up	Not included in the System Back-up.
	Log Entry	-
	Remarks	None.