Issued August 26th, 2011

Security White Paper
for
GlobalScan NX Version 1.5

Solution Value Proposition Section
Global Technology Support Department
Service and Support Center
Global Marketing Group
Ricoh Company, Ltd.

Document version
GSNXV1.5.0-1.0

Document version history:

Version	Date of Issue	Revision
1.0	August, 2011	1st Release

1. Introduction

This document describes potential network weak points and recommended precautions for them.
Ricoh products use network services to provide a variety of features for network clients, such as file sharing, printer sharing, HTTP services and also client services for accessing network servers running outside our products, such as an LDAP server or E-mail server.

As Ricoh products are designed for use inside an Intranet where network clients and servers are protected by firewalls, they rely on the Intranet's security policy, like the security provided by other network servers and clients. However, some customers require more strict security levels for network devices. This document focuses on providing the information necessary to protect against potential threats from external security risks and help customers to fit the Ricoh product into their security system.

Ricoh products interact with non-Ricoh products, such as the operating system. If you are interested in learning about vulnerabilities in non-Ricoh products, please contact the vendor of that product.

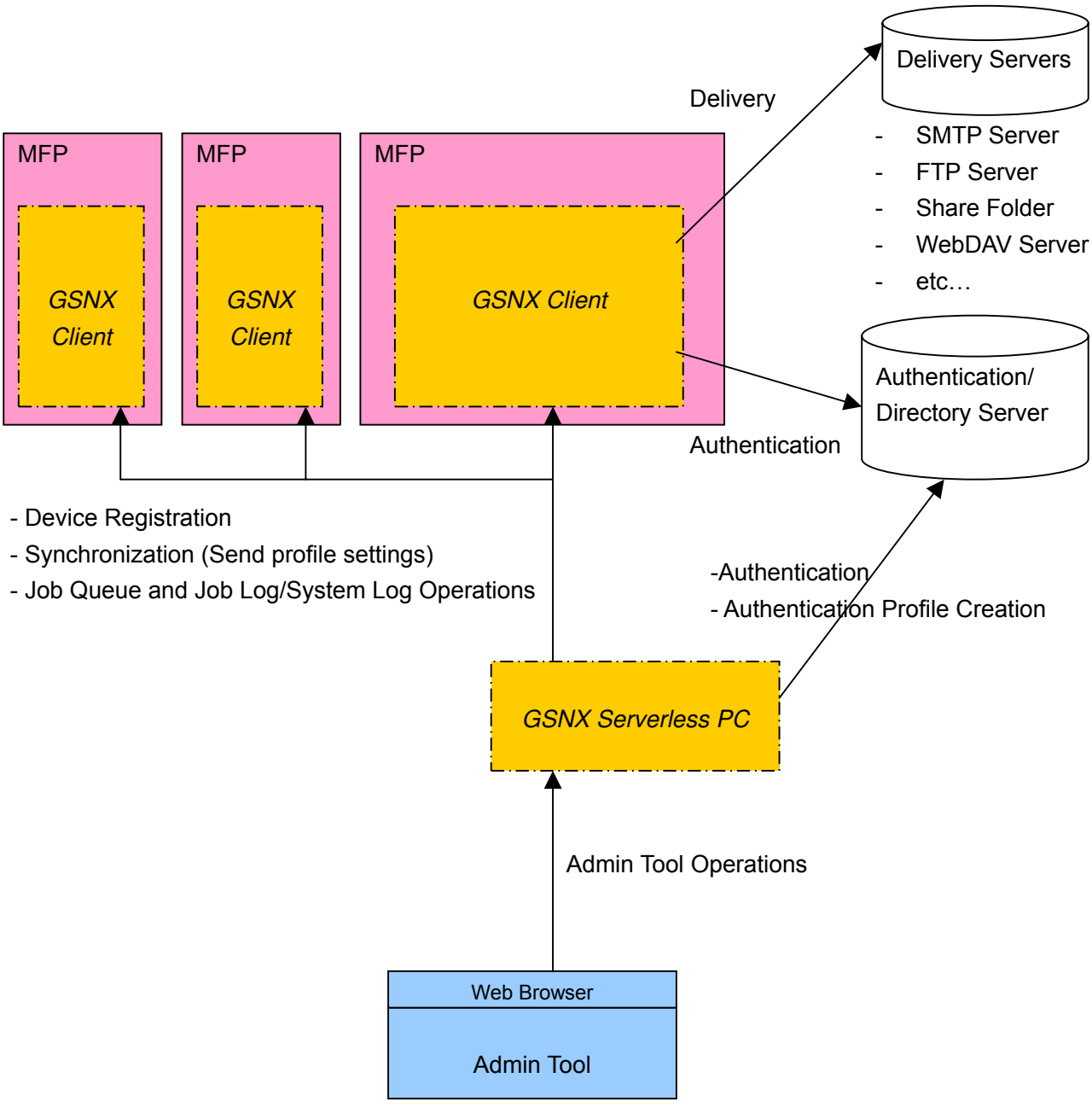
Products and versions covered by this document:

GlobalScan NX Serverless version 1.5
GlobalScan NX Business Server version 1.5
GlobalScan NX Enterprise Server version 1.5

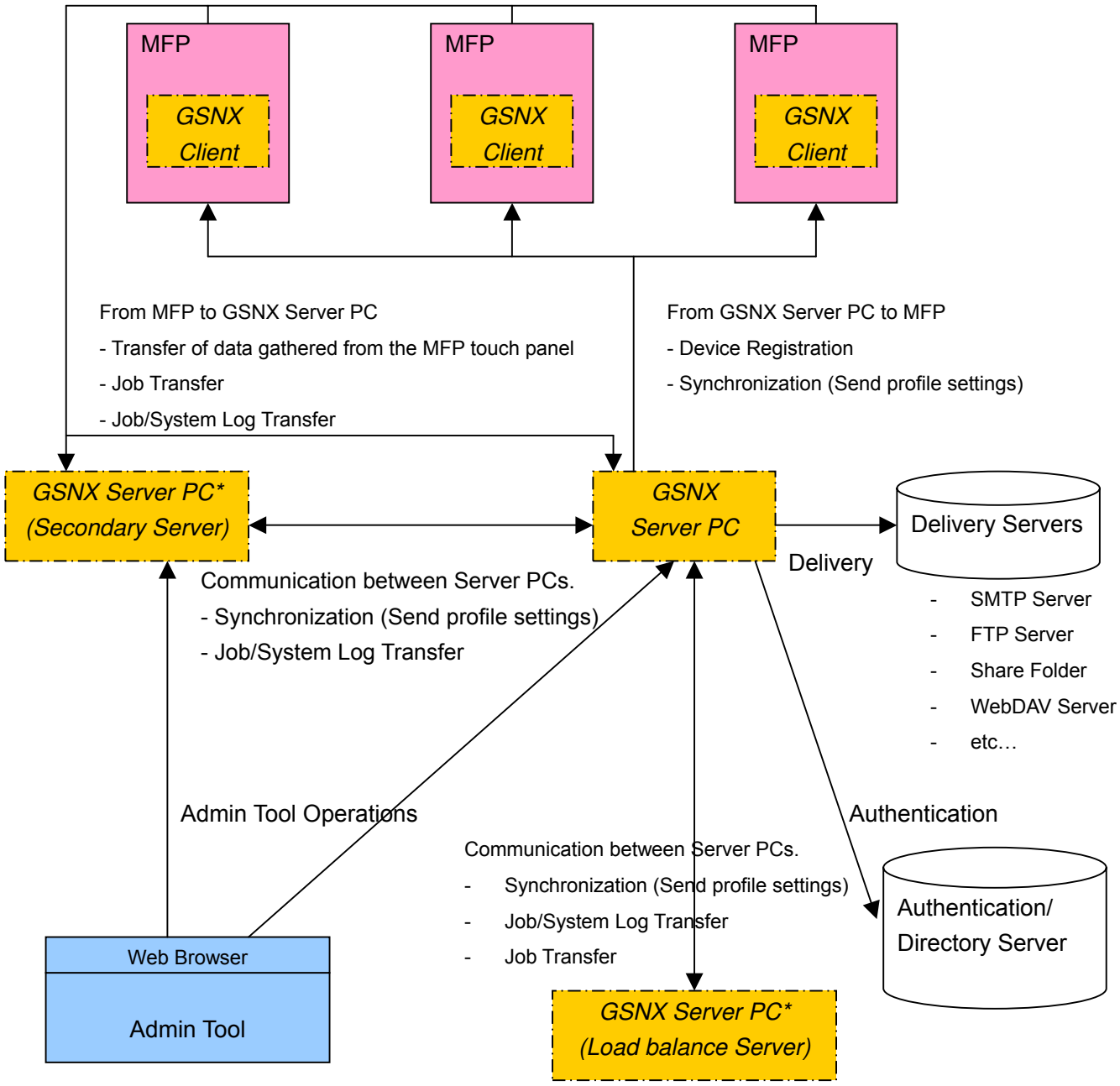
2. System

These diagrams show the general data flow within GlobalScan NX.

2.1 GlobalScan NX Serverless



2.2 GlobalScan NX Business/Enterprise Server



* Load Balance and Secondary servers perform authentication and delivery according to the synchronized settings.

3. Network Protocols

3.1 Ports and Protocols

The tables below describe the ports and protocols used for communication between the various parts of the GlobalScan NX system.

SSL On/Off indicates the current GSNX SSL configuration, as set by the SSL Setting Tool.

General Operations

Function	SSL Off		SSL On		Remarks
	Port	Protocol	Port	Protocol	
Admin Tool -> GSNX Server/Serverless PC MFP -> GSNX Server/Serverless PC	Set during install. (TCP)	HTTP	Set during install. (TCP)	HTTP	SSL Off: Default port is 8080. SSL On: Default port is 8443.
GSNX Server/PC -> MFP	8080(MFP) (TCP)	HTTP	51443(MFP) (TCP)	HTTP	Unable to change.

Device Search

Function	Port	Protocol	Remarks
Device Search	161 (UDP)	SNMP	The port number is inherent to the SNMP protocol, and cannot be changed.

Load Balance Server / Secondary Delivery Server

Function	Port	Protocol	Remarks
Server Browsing GSNX Server PC -> GSNX Server PC	5353 (UDP)	Bonjour	Communication from the Main (Primary) Server to other GSNX Server PCs.

Authentication

Both TCP and UDP are used except where indicated.

Authentication Method	Function	Port	Protocol	Remarks
Active Directory / Active Directory (Passwordless)	Authentication Process	88	KRB5	When UDP connection is failed, TCP is used.
		389/636	LDAP/LDAPS	Port and protocol determined when Authentication Profile created.
	Creation of Authentication Profile	137	NBNS	
		445	SMB	
		389/636	LDAP/LDAPS	When 389/LDAP is unavailable, 636/LDAPS is used.
	Generation of User List	88	KRB5	
		389/636	LDAP/LDAPS	Port and protocol determined when Authentication Profile created.
NT	Authentication Process	88	KRB5	
		137	NBNS	
		138 (UDP)	SMB_NETLOGON	
		139	SAMR	
		445 (TCP)	SMB DCERPC SAMR	
	Creation of Authentication Profile	137	NBNS	
	Generation of User List	137 (UDP)	NBNSS	
		139 (TCP)	NBNSS SMB DCERPC SAMR	
		445 (TCP)	SMB DCERPC SAMR	
LDAP / LDAP (Passwordless)	Authentication Process	389 (TCP)	LDAP/LDAPS	Port and protocol determined when Authentication Profile created. Defaults are 389/LDAP.
	Creation of Authentication Profile	389 (TCP)	LDAP/LDAPS	Port and protocol determined when Authentication Profile created. Defaults are 389/LDAP.
	Generation of User List	389 (TCP)	LDAP/LDAPS	Port and protocol determined when Authentication Profile created. Defaults are 389/LDAP.
Send to Home Folder/Send to Me Settings (AD or LDAP)	Obtains server as a home folder/mail address from the specified LDAP server.	389 (TCP)	LDAP/LDAPS	Port and protocol determined when Authentication Profile created. Defaults are 389/LDAP.

Communication with Delivery Servers

Delivery Method	Port	Protocol	Remarks
E-mail Delivery GSNX Server -> Email Server MFP -> Email Server	25 (TCP)	SMTP/SMTPS	Set as part of Project properties, this port should match the settings of the SMTP server.
	110 (TCP)	POP	Used when POP before SMTP is used for authentication. Set as part of Project properties, this port should match the settings of the SMTP server. 110 is the default.
	389/636 (TCP)	LDAP/LDAPS	Set as part of Project properties, this port should match the settings of the LDAP server.
Folder Delivery GSNX Server -> Share Folder Server MFP -> Share Folder Server	445 (TCP) 139 (TCP)	SMB	As a part of the JCIFS library, this port is unchangeable. When 445 is unavailable, 139 is used.
	137 (UDP)	NBNS	As a part of the JCIFS library, this port is unchangeable.
FTP Delivery GSNX Server -> FTP Server MFP -> FTP Server	21/22 (TCP)	FTP/SFTP	This port should match the settings of the FTP server. Set as part of the Project properties, the port number is included in the URL of the Start Point Path. If a port is not specified, FTP's default is 21 and SFTP's default is 22.
	20 (TCP)	FTP	This port is automatically 1 less than the above port, and is not user-specified.
WebDAV Delivery GSNX Server -> WebDAV Server MFP -> WebDAV Server	80/443 (TCP)	HTTP/HTTPS	This port should match the settings of the WebDAV server. Set as port of the Project properties, the port number is included in the URL of the Start Point Path. If a port is not specified, the default is 80.
RightFax Plug-in GSNX Server -> FaxUtil (RightFax COM API)	-	COM	The COM API included in FaxUtil is used by the GSNX server. RCL is not responsible for the communication between FaxUtil and the RightFax server.
SharePoint Plug-in GSNX Server -> Microsoft Office SharePoint Server	80/443 (TCP)	HTTP/HTTPS	This port should match the settings of the SharePoint server. The port is set by adding the port number to the Start Point Path URL. If a port is not specified, the default is 80.
DocumentMall Plug-in Server: GSNX Server -> DocumentMall Server GSNX Server -> Proxy Server Serverless: MFP -> DocumentMall Server MFP -> Proxy Server	443 (TCP)	HTTP	This port cannot be changed.
	8080 (TCP)	HTTP	
Send to Printer Plug-in GSNX Server -> Printer Driver	-	-	GSNX sends the print data to the printer driver using the standard Windows API. Communication between the printer driver and the printer is controlled by the settings in the printer driver.

RMI (Java Remote Method Invocation API)

Function	Port	Protocol	Remarks
Batch Execution	41108 (TCP)	JRMP	Batch Execution uses this port internally.
	41109 (TCP)	JRMP	Batch Execution uses this port internally.

Server Internal (Web server and servlet container)

Function	Port	Protocol	Remarks
Internal Communication	48009 (TCP)	AJP13	The web server uses this port for internal communication.

3.2 Recommend Precautions

3.2.1 HTTP Communication

Default communication between the AdminTool and the GSNX server, and again between the GSNX server and the MFP is done in HTTP without SSL and is therefore not encrypted. The password and other sensitive data are only protected by a weak encryption method. Users sensitive to security concerns should use SSL.

3.2.2 Connecting to other servers

Data sent between a GSNX server and a resource server (FTP server, SMTP server, LDAP server, etc.), or an MFP and a resource server is also not protected by encryption. Users sensitive to security concerns should use SSL.

3.2.3 Communication with attached devices

Communication with devices occurs as follows:

(1) Device → GSNX Server PC

- Transfer of data gathered from the device touch panel
- Job Transfer
- Job/System Log Transfer

(2) GSNX Serverless/Server PC → Device

- Device Registration/Synchronization (Send profile settings)
- Job Queue and Job Log/System Log Operations (Serverless version, SSL On)

(3) AdminTool → Device

- Job Queue and Job Log/System Log Operations (Serverless version, SSL Off)

Using HTTP(S) as a base, data formats such as XML and CSV are sent and except for certain data (such as login credentials), this data is not encrypted. To maintain security, SSL is necessary. Also, when the MFP and GSNX PC (Serverless or Business/Enterprise Server) are separated and must pass through a VPN or NAT, address translation may not allow for correct operation.

3.2.4 Communication between GSNX Servers

When using Load Balance or Secondary Delivery Servers, communication between GSNX servers occurs as follows:

- Initial Load Balance or Secondary Delivery Server settings
- Server Browsing
- Server Synchronization
- Log Forwarding
- Job/Queue Operations
- Job Distribution between the Load Balance servers

Except for Server Browsing, default communication between the GSNX servers is done over HTTP without SSL, and is therefore not encrypted. Passwords and other sensitive data are only protected by a weak encryption method. Users sensitive to security concerns should use SSL.

Information exchanged when Server Browsing is not encrypted because it does not contain any critical information.

4. Data Flow & Storage

4.1 Stored Data

Data	Item	Security Note
Profile Data	Access Control	Depends on Administrator Settings.
	Encryption	No Data Needing Encryption.[1]
	Back-up	Data saved in GSNX's back-up system. Back-ups are created manually or using the Scheduled Backup function.
	Log Entry	None.
	Remarks	
Project Data	Access Control	Depends on Administrator Settings.
	Encryption	No Data Needing Encryption.[1]
	Back-up	Data saved in GSNX's back-up system. Back-ups are created manually or using the Scheduled Backup function.
	Log Entry	None.
	Remarks	None.
Plug-in Data	Access Control	Depends on Administrator Settings
	Encryption	User IDs and passwords are encrypted using the 128-bit Blowfish encryption algorithm. The key used by the Blowfish algorithm is encrypted using the 1024-bit RSA encryption algorithm for communication on the network.[1]
	Back-up	Data saved in GSNX's back-up system. Back-ups are created manually or using the Scheduled Backup function.
	Log Entry	Depends on the Plug-in, but typically only failures are entered in the System Log, and both successful and failed operations are stored in the Job Log.
	Remarks	None.
System Settings	Access Control	Depends on Administrator Settings.
	Encryption	User IDs and passwords inside the Authentication Profile Settings and Administrator Settings are encrypted using the 128-bit Blowfish encryption algorithm. The key used by the Blowfish algorithm is encrypted using the 1024-bit RSA encryption algorithm for communication on the network.
	Back-up	Data saved in GSNX's back-up system. Back-ups are created manually or using the Scheduled Backup function.
	Log Entry	It depends on the setting, but typically changes are written with an access record to the System Log.
	Remarks	None.

Data	Item	Security Note
Built-in Account	Access Control	Depends on Administrator Settings
	Encryption	Password information is encrypted using the 128-bit Blowfish encryption algorithm. The key used by the Blowfish algorithm is encrypted using the 1024-bit RSA encryption algorithm for communication on the network.
	Back-up	Data saved in GSNX's back-up system. Back-ups are created manually or using the Scheduled Backup function.
	Log Entry	Nothing stored in logs.
	Remarks	None.
Delivery job	Access Control	Administrators may see all jobs, while general users may only see their own jobs.
	Encryption	The User ID and password for login to a project are encrypted using the 1024-bit RSA encryption algorithm.
	Back-up	Delivery jobs remaining in the queue are not backed up.
	Log Entry	Success or failure is stored in the Job Log.
	Remarks	None.
Job Log	Access Control	Administrators may see all job logs, while general users may only see their own job logs.
	Encryption	Nothing encrypted.
	Back-up	The Job Log is not backed up.
	Log Entry	-
	Remarks	None.
System Log	Access Control	Only Administrators may see all system logs.
	Encryption	Nothing encrypted.
	Back-up	The System Log is not backed up.
	Log Entry	-
	Remarks	None.
Back-up Data	Access Control	Depends on Administrator Settings
	Encryption	Back-up data is encrypted when saved using Java's password-based encryption (PBE). If a password is not specified, the encryption is done using null characters.
	Back-up	-
	Log Entry	This and other maintenance operations are sent to the System Log.
	Remarks	Up to 30 instances of back-up data may be saved. A password can be set for an individual back-up data when it is downloaded, and that password must be entered when that same data is uploaded.

[1]Profile, Project, and Plug-in data are all listed separately because GSNX treats each set of data differently.

4.2 Data Flow

There are many network connections involved in the GSNX system, and as those connections are done primarily in HTTP, the system is not very secure. Also, since GSNX makes use of the FTP and SMB protocols when connecting with some resource servers, there are added weak points.

Users who feel that system is too weak by default should active the SSL settings to gain acceptable levels of security.

4.3 Server/PC Data

Except for some user information, such as account passwords, the server/PC resources such as the program data, configuration, registry, and logs are stored without encryption. There are no special protections on the stored data.
Therefore, special attention should be given to the server access, such as proper user access management, physical isolation, anti-virus software, etc.

End of Document