Issued July 6th, 2012

Security White Paper

for

FlexRelease CX Ver1.x

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

Document version
FRCXV1.0

Notice:

Document version history:

Version	Date of Issue	Revision
1.x	June, 2012	1st Release

Table of Contents

1. Introduction

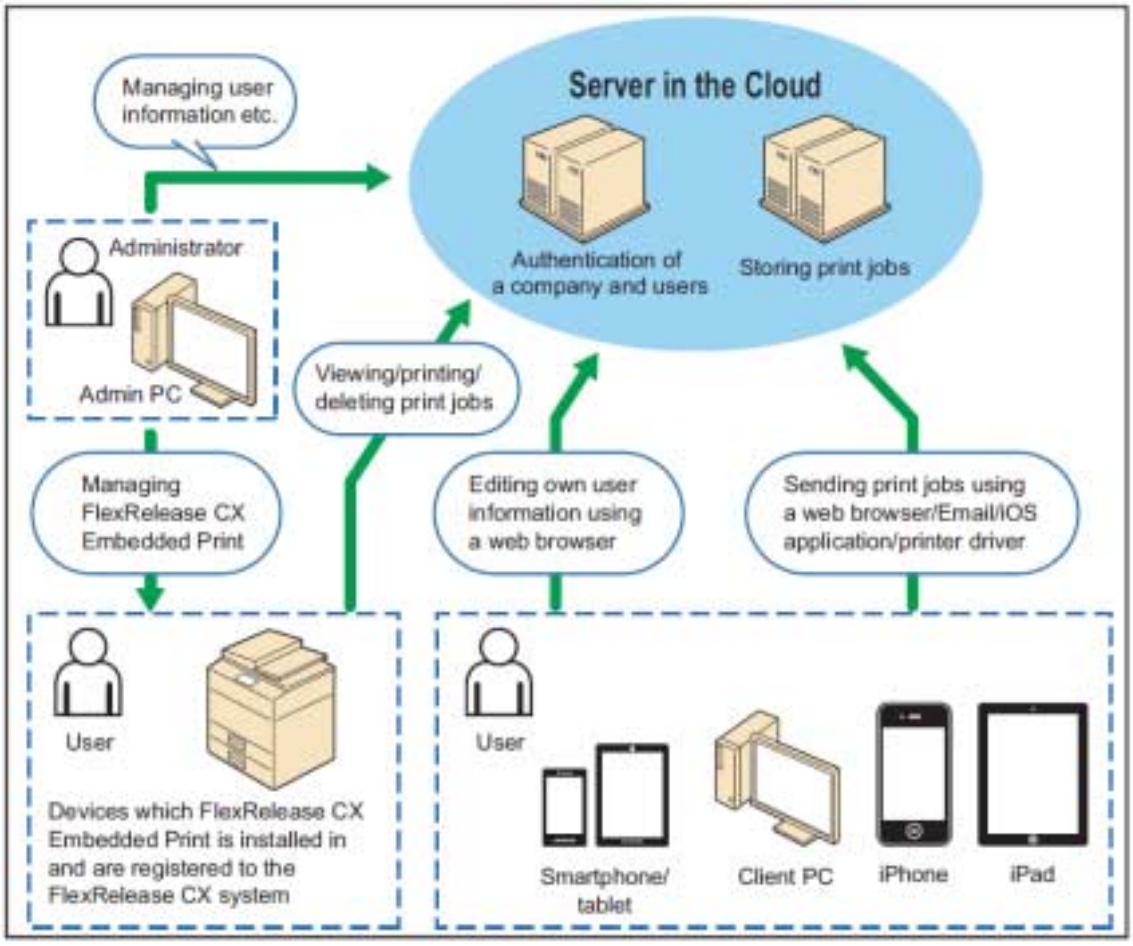
This document attempts to address any security concerns users of FlexRelease CX may have. This document covers how Ricoh has protected its servers against potential threats from external security risks and provides information that customers can use to fit the Ricoh product into their security policies.

Ricoh products do 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:
FlexRelease CX Version 1.x

2. About FlexRelease CX Version 1.x

The diagram below shows the general data flow within the FlexRelease CX system.



- Users submit print jobs to the cloud server using a client PC or a smartphone/tablet. The server converts the submitted job into print data and stores it.
- Print jobs can be submitted via either a web browser, email or the FlexRelease CX iOS application.
- The server is located in a data center. The FlexRelease CX Server is accessed as a web application.
- Users print jobs stored in the FlexRelease CX Server using FlexRelease CX Embedded Print, which is installed on a device.

3. Network Protocols

The table below describes the ports and protocols used for communication between different components of the FlexRelease CX system.

Function		Destination	Port	Protocol
Connection TO the FlexReleaseCX System		www.flex-release.ricoh.com	80 (TCP)[1] 443 (TCP)	HTTP HTTPS
Connection FROM the FlexRelease CX system		External components	123 (UDP) 53 (TCP/UDP)	NTP DNS
Uploading print jobs	From FlexRelease CX Server (via a web browser)	www.flex-release.ricoh.com	443 (TCP)	HTTPS
	By Email	mx01ricoh.co.jp mx02.ricoh.co.jp mx03.ricoh.co.jp mx04.ricoh.co.jp	25 (TCP)	SMTP
	From iOS Application	www.flex-release.ricoh.com	443 (TCP)	HTTPS
Printing the jobs		www.flex-release.ricoh.com	443 (TCP)	HTTPS
Managing FlexRelease CX Embedded Print	Using FlexRelease CX Embedded Print Manager	<device's IP address/host name>:8080/frcx/login <device's IP address/host name>:51443/frcx/login	8080 (TCP) 51443 (TCP)	HTTP HTTPS

When installing FlexRelease CX Embedded Print on a device, a connection from the managing PC to the device via both ports 8080 and 51443 (TCP) must be available.

[1] When accessing the FlexRelease CX System via HTTP, the connection is automatically redirected to use HTTPS.

4. Operation Management

4.1. Server Monitoring

The network, server, and applications are monitored 24 hours a day, 365 days a year for both security and performance issues.

4.2. Regular Vulnerability Patching

Security patches for OS and middleware are applied regularly, but only after verifying the impact on the FlexRelease CX system using a development/test environment.

4.3. Vulnerability Assessments

New versions will only be released after testing using IBM Rational AppScan. For more information about Rational AppScan, please visit IBM's website at http://www-01.ibm.com/software/awdtools/appscan/.

In addition, the system undergoes the internet server security inspection performed by an outside security consultant once a year.

5. Information Security Policy

5.1. Anti-Virus Policy

All documents submitted by customers are checked by anti-virus software. At this time, Trend Micro's Virus Buster[2] is used, and the latest definition file is always in use. In addition, spam filters are also used. If a file is identified as spam, that file will be blocked.

In addition, Trend Micro's ServerProtect anti-virus software is run on all the Windows servers to help protect the entire FlexRelease CX system from infection.

[2] Virus Buster is the Japanese version of OfficeScan.

6. Data Protection

6.1. Data Backup

Configuration data and user information provided by the customer are stored in the server and are backed-up regularly in case of equipment failure or other serious issues. However, a backup of the print data is not taken in order to help preserve customer information security.

6.2. Data Erasing

Any data submitted to the server for printing is deleted automatically after the print is completed, and no related data is left on the server.[3]

Print jobs are automatically deleted from the server at a pre-defined interval. The print job storage period is configured by the client-side administrator. Users can also delete their own jobs stored on the server.

6.3. Protection of print documents

Print jobs are stored in a multi-tenant database. The documents are retrieved using a query containing a client-specific FlexRelease ID (FlexRelease Code) and a user ID as keys, which ensures that only documents belonging to the proper user are retrieved.

[3] A slight time-lag may occur between the print completion and the data erasure.

7. Prevention of Unauthorized Access

7.1. Management of Administrator Access

Server administrators undergo maintenance every time there are personnel changes, and there is regular maintenance every six months (account validity checks & password updates are performed). Administrators also undergo training outlining acceptable data access procedures.

7.2. Access Controls

FlexRelease CX system authentication is based on the FlexRelease Code, User Name, and Password. Access is only granted if authentication succeeds.

The length of the FlexRelease Code is 9 digits. The length of the user name is up to 128 alphanumeric characters. The password lengths are from 6 to 128 characters, but the period of validity is unlimited. If a wrong password is entered 5 times is succession, the account is locked. Accounts are unlocked by administrators, or automatically after 24 hours.

System users are classified as either an administrator user or a general user. Ricoh creates the first administrator account with a default password for the customer. Once the default password is changed by the customer, the account becomes accessible only by the customer. The customer can then use this account to create other administrator or general user accounts.

Only a hashed form of the customer’s password is stored on the FlexRelease Server. The actual password is not known to Ricoh.

Printing from a particular device requires that the FlexRelease CX Embedded Print application be installed in the device, and that the device has been registered with the FlexRelease CX server. The device is registered using the input FlexRelease Code, administrator ID and administrator password. The registered device is bound to the specified FlexRelease Code, which means that documents that use a different FlexRelease Code cannot be printed.

Printing documents from a device requires the authentication of the user and password. Printing from devices that are not registered with the FlexRelease CX server is impossible.

7.3. Prevention of unauthorized access

A firewall is configured to block unauthorized connections, and no confidential information is stored in any server directly accessible from the internet.

Access to the server for maintenance purposes is performed via Ricoh's internal corporate network, not from the internet. There is also a firewall between the server and Ricoh's corporate network. Access to the back-up data is also strictly controlled and monitored.

8. Information Security Policy

8.1. Communication Encryption

HTTPS is used for communication between the web browser and server, between the FlexRelease CX iOS Application and server, and Ricoh devices and the server. The server uses a certificate with a public key length of 2048-bits that is issued by GlobalSign. The protocols used for HTTPS encryption are as follows:

- SSL v3
- TLS 1.0, TLS 1.2

SMTP is used for submission of print jobs via email. The communication path and content being submitted are not encrypted. Therefore, email submission should only be used if sending of job content in plain text is acceptable by the customer’s security policy.

Submitting print jobs via email requires registering the sender’s email address with the FlexRelease CX system. Files submitted from unregistered email addresses are not accepted.