Contents

Introduction ................................................................................................................................. 5
   Purpose ........................................................................................................................................ 5
   Target Audience ....................................................................................................................... 5
   Disclaimer ................................................................................................................................. 5
System Workflows .................................................................................................................... 7
   Mobile Application User Workflow ....................................................................................... 7
   Email User Workflow .............................................................................................................. 8
   Website User Workflow .......................................................................................................... 9
   Administrator Workflow ........................................................................................................... 10
Security Description .................................................................................................................. 11
   Xerox Mobile Print Cloud Network Protocols and Port Numbers Diagram ............................ 12
   Individual System Components .............................................................................................. 12
      Xerox Mobile Print Portal – Mobile Application ................................................................. 12
      Xerox Mobile Print Cloud Service ....................................................................................... 13
      Xerox Mobile Print Cloud Agent .......................................................................................... 14
      Xerox Mobile Print Cloud – User Web Pages ..................................................................... 15
      Xerox Mobile Print Cloud – Customer Administrator Web Pages ......................................... 15
      Printer .................................................................................................................................... 16
Communication between System Components ........................................................................ 17
      Communication between Xerox Mobile Print Portal Mobile Application and Xerox Mobile
      Print Cloud Service ............................................................................................................... 17
      Communication between Mobile Device and Email Server .................................................. 17
      Communication between Email Server and Xerox Mobile Print Cloud Service .................. 17
      Communication between Xerox Mobile Print Cloud Service and Xerox Mobile Print Cloud
      Agent ......................................................................................................................................... 18
      Communication between Xerox Mobile Print Cloud Agent and Printer .............................. 18
The Role of Xerox ....................................................................................................................... 19
Introduction

A Xerox Workflow Solution that connects a mobile workforce to new productive ways of printing. Printing is easy and convenient from a mobile device without needing drivers and cables.

Purpose

The purpose of this document is to disclose information for the Xerox Mobile Print Cloud with respect to system security. System Security, for this paper, is defined as follows:

1. How print jobs are received, accessed, and transmitted
2. How user information is stored and transmitted
3. How the product behaves in a networked environment
4. How the product may be accessed, both locally and remotely

Please note that the customer is responsible for the security of their network and the Xerox Mobile Print Cloud product does not establish security for any network environment.

The purpose of this document is to inform Xerox customers of the design, functions, and features of the Xerox Mobile Print Cloud relative to Information Assurance (IA).

This document does NOT provide tutorial level information about security, connectivity, PDLs, or Xerox Mobile Print Cloud features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user’s use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages.
System Workflows

Mobile Application User Workflow

Step 1: User selects document to print and opens with the Xerox Mobile Print Portal application. Using the Mobile application the user selects desired printer and print attributes (e.g. Duplex, Stapling, # of Copies, B&W vs. Color). The user then selects Print.

Step 2: The document is uploaded to the Xerox Mobile Print Cloud service for conversion to a print-ready document.

Step 3: The Xerox Mobile Print Cloud Agent retrieves the print-ready document.

Step 4: The Xerox Mobile Print Cloud Agent routes the print-ready document to the selected printer.

Step 5: User picks up their printed document.
Email User Workflow

**Step 1:** User selects document to print and forwards to the Xerox Mobile Print Cloud email address.

**Step 2:** The Xerox Mobile Print Cloud service monitors the email inbox and retrieves incoming submissions. The documents are imported to the Xerox Mobile Print Cloud service for conversion and printing. Depending on the email address sent to, the documents are printed to the specified printer, or held in the Xerox Mobile Print Cloud service for later release via the Xerox Mobile Print Portal application.

**Step 3:** The Xerox Mobile Print Cloud Agent retrieves the print-ready document.

**Step 4:** The Xerox Mobile Print Cloud Agent routes the print-ready document to the selected printer.

**Step 5:** User picks up their printed document.
Website User Workflow

**Step 1:** User logs in to the Xerox Mobile Print Cloud Website, browses their PC for a document to print, selects a printer and print options, and then prints the document.

**Step 2:** The Xerox Mobile Print Cloud service uploads the document for conversion and printing.

**Step 3:** The Xerox Mobile Print Cloud Agent retrieves the print-ready document.

**Step 4:** The Xerox Mobile Print Cloud Agent routes the print-ready document to the selected printer.

**Step 5:** User picks up their printed document.
Administrator Workflow

Step 1: Customer administrator logs in to the Xerox Mobile Print Cloud Website. Administrators can configure account behaviors and manage users, agents and printers.

Administrator functions:
- Manage Account Settings
- Manage Agents
- Manage Printers
- Manage Users
- Manage Licenses
- View History
The security considerations are three-fold:

1. The security of the user's documents during transport and storage
2. The security of the customer and end user account information required by the Xerox Mobile Print Cloud system
3. The security of the printers enabled within the system by the customer

As one can see from the above diagrams, documents and information travel through multiple system components over a combination of cellular, wired and wireless networks. All use normal, industry-standard technologies and built-in security capabilities. Of course these capabilities do need to be enabled, and the choice of which are used at each point in the system varies. This section captures the security considerations of Xerox Mobile Print Cloud in the following areas:

1. Protocols and Port numbers used by the system
2. Individual system components
   a. Xerox Mobile Print Portal – Mobile Application
   b. Xerox Mobile Cloud Print Service
      i. Microsoft® Windows Azure Platform Specific
      ii. Microsoft® Windows SQL Azure Database Specific
      iii. Xerox Mobile Cloud Print Service Specific
   c. Xerox Mobile Print Cloud Agent
   d. Xerox Mobile Print Cloud – User Web Pages
   e. Xerox Mobile Print Cloud – Customer Administrator Web Pages
   f. Printer
3. Communication between system components
   a. Communication between Xerox Mobile Print Portal Mobile Application and Xerox Mobile Print Cloud Service
   b. Communication between Mobile Device and Email Server
   c. Communication between Email Server and Xerox Mobile Print Cloud Service
   d. Communication between Xerox Mobile Print Cloud Service and Xerox Mobile Print Cloud Agent
   e. Communication between Xerox Mobile Print Cloud Agent and Printer
Xerox Mobile Print Cloud Network Protocols and Port Numbers Diagram

This diagram shows the protocols and typical port numbers used in the system. Port numbers are not configurable.

---

Individual System Components

**Xerox Mobile Print Portal – Mobile Application**

The Xerox Mobile Print Portal Mobile Application is the main user interface to the Xerox Mobile Print Cloud system.

The application requires users to authenticate with the Xerox Mobile Print Cloud Service before using the application. Once authenticated, the user’s credentials and authentication token are stored in the application until they log out (Please refer to the section titled “Communication between Xerox Mobile Print Cloud Mobile Application and Xerox Mobile Print Cloud Service” for more information about authentication and communications related security information).

Users can access their print jobs for preview and printing, locate printers, and only access documents they submitted and printers to which they have been granted access.

The Xerox Mobile Print Portal Mobile Application does not provide the capability to remotely wipe the mobile device.
It is ultimately the user’s responsibility to secure their mobile device. Users can enable device level passwords and manage physical access to the device. If the mobile device is lost or stolen, the user can access the web portal to change their password making the device unable to access the Xerox Mobile Print Cloud system.

**Xerox Mobile Print Cloud Service**

The Xerox Mobile Print Cloud Service runs in the Microsoft® Windows Azure Platform and utilizes the SQL Azure Database for storage. There are 3 considerations for security based on this architecture as follows:

1. Windows Azure Platform specific security information
2. SQL Azure Database specific security information
3. Xerox Mobile Print Cloud Service specific security information

Each consideration is covered below.

**Windows Azure Platform Specific**

The Windows Azure Platform operates in the Microsoft® Global Foundation Services (GFS) infrastructure, portions of which are ISO27001-certified.

Windows Azure Security Highlights:

- Built-in Identity Management for administrator access
- Dedicated hardware firewall
- Stateful packet inspection technology employed
- Application-layer firewalls
- Hypervisor firewalls
- Host-based firewalls
- SSL termination/ load balancing / application layer content switching
- Each deployed hosted service is segmented in own VLAN, preventing compromised node access

Please visit the Microsoft web site for more information: [http://www.windowsazure.com/en-us/develop/net/other-resources/white-papers/](http://www.windowsazure.com/en-us/develop/net/other-resources/white-papers/)

Select “Windows Azure Security Overview”.

**SQL Azure Database Specific**

The application data is stored in a SQL Azure database. This database contains information about the printers, jobs etc.

SQL Azure is protected by 2 levels of security. In addition to username and password to access the database, Microsoft protects access to SQL Azure databases by allowing configuration of a whitelist of IP Addresses that can connect to the database.

Only internal Xerox IP Addresses have been configured on the whitelist for this database. Only authorized Xerox personnel have access to this data.
Passwords, Printer MAC Address and Printer Serial Number are stored in an encrypted format in the database.

**Xerox Mobile Print Cloud Service Specific**

Original documents and printable documents are stored within Azure Storage. Both the original and printable documents are in an encrypted format.

Access to these documents is only available to the following

1. The owner of the documents via the Xerox Mobile Print Portal Mobile Application for preview.
2. Authorized Xerox personnel responsible for deployment and maintenance of the system. Since the documents are encrypted even the authorized personnel cannot open the document to view its contents

Each document printed follows a document retention policy which is applied to the document at the time of printing. The document retention policy is either immediate or 7 days. If set to immediate, the document is deleted immediately after printing. If the document retention policy is set to 7 days, the document is removed 7 days after printing. Therefore, documents are stored in the system for a maximum of 7 days.

All communications to and from the Xerox Mobile Print Cloud Service are over HTTPS. Documents are always transmitted securely and are protected by SSL security during upload and download.

Certificates used for encryption/decryption of documents are stored in the Windows Azure Certificate store as per Microsoft guidelines. This is a highly secure area protected by Microsoft. Account administrators can only upload certificates to this store. Download are not allowed. Only applications running within the same Windows Azure subscription can access the certificate.

**Xerox Mobile Print Cloud Service Virtual Machines**

Xerox will monitor vendor security bulletins and product update announcements, and assess what actions are required on the Azure virtual machines. These bulletins and announcements can come from Microsoft and other external vendors, as well as internal partners supplying components used in the product system. Xerox will update the virtual machines to maintain the health and integrity of the product system.

As anti-virus definition files are released more frequently than application and operating system patches, these updates will occur on a more frequent basis. Virtual machines are configured to perform full scans weekly, and update the anti-virus definition files before the full scan.

**Xerox Mobile Print Cloud Agent**

The Xerox Mobile Print Cloud Agent has two primary functions. First, the agent is responsible for discovering printers within the customer’s network, determining the printer capabilities, and relaying that information to the Xerox Mobile Print Cloud Service. Second, the Xerox Mobile Print Cloud Agent is responsible for routing print jobs to target printers.

The Xerox Mobile Print Cloud Agent is installed on a PC. The installing user must have administrator privileges since the Xerox Mobile Print Cloud Agent software is installed as a Windows service. The Xerox Mobile Print Cloud Agent cannot be connected to the Xerox Mobile Print Cloud Service unless the Xerox Mobile Print Cloud Service has been configured to accept the agent.
The Xerox Mobile Print Cloud Agent user interface is available to all users who can log on to the agent PC. It displays the printers discovered by the agent and allows only the proxy server address for that agent to be changed. It does not present any user or customer specific information.

A local database is maintained on the Xerox Mobile Print Cloud Agent PC. This database stores printer discovery settings and printer information for each printer discovered. Access to the database is restricted to user’s who have permission to log into the agent PC.

The Xerox Mobile Print Cloud Agent installs by default in the following location:

**Program Files(x86)->Xerox->Mobile Print Cloud Agent**

Access to this folder and sub-folders is limited to users logged on to the agent PC. It contains the agent executable file, its database, and language libraries.

Threats include physical damage to the system, attacks over the network, as well as damage caused by viruses. The goal is to minimize the security risks as much as possible, and have policies in place to detect and reduce the negative impact of a security incident. Examples of things that can be done to reduce risks include proper use of logins and passwords, restricting network access, applying security related operating system updates, and the use of virus detection software.

The customer is ultimately responsible for securing their environment to meet their specific security needs. Depending on the customer needs, the customer can increase security by installing a firewall, and/or physically securing the hardware to a limited access area. The customer, depending on their needs, should use tools to monitor and log physical and network access to the Xerox Mobile Print Cloud Agent hardware and software to determine if and when a security incident has occurred. The customer should also back-up their data to ensure that it may be recovered in case of deletion or corruption.

Please refer to the section titled “Communication between Xerox Mobile Print Cloud Service and Xerox Mobile Print Cloud Agent” and the section titled “Communication between Xerox Mobile Print Cloud Agent and Printer” for more information about authentication and communications related security information.

**Xerox Mobile Print Cloud – User Web Pages**

All user web pages are accessed using HTTPS from a browser.

Xerox Mobile Print Cloud customer account users have to authentication with the Xerox Mobile Print Cloud Service to access the user web pages. Once authenticated the user can view:

1. All printers enabled by the customer account administrator inclusive of printer name, printer location, and the printer's direct email submission email address.
2. Only jobs submitted by the user inclusive of document names, date of completion, and printer name of printer used to print the job.

**Xerox Mobile Print Cloud – Customer Administrator Web Pages**

All user customer administrator web pages are accessed using HTTPS from a browser.
Xerox Mobile Print Cloud customer account administrators have to authenticate with the Xerox Mobile Print Cloud Service to access the administrator user web pages. Once authenticated the administrator user can view everything that users can in addition to the following:

1. Users associated with their customer account via a listing that includes email addresses.
2. All jobs processed for the account inclusive of document names, date of completion, email address of user that submitted the document, and printer name of printer used to print the job. This includes documents submitted by users who are not members of the customer account, but have seen and printed to one of the account printers.
3. Licensing information that includes license activation keys and associated serial numbers. Once a license is installed for a customer account, the license activation keys and associated serial numbers cannot be re-used to install in other customer accounts.
4. IP addresses for all printers discovered by the customer account’s Xerox Mobile Print Cloud Agents.
5. The addresses of sites where printers are located.
6. Xerox Mobile Print Cloud Agents that have been created and registered with the customer account. This includes the agents Activation Codes which are tied to the customer account and cannot be used to register a Xerox Mobile Print Cloud agent in another customer account. This information is displayed for the customer account administrators only. It is the responsibility of the administrator in sharing Activation Codes with others.

**Printer**

Xerox printers have a variety of security features that can be employed to increase security. Availability of these features will vary depending on model. It is the customer’s responsibility to understand and implement appropriate controls for printer behavior.

Some examples are as follows:

1. Xerox Image Overwrite electronically shreds information stored on the hard drive of devices as part of routine job processing.
2. Data Encryption uses state of the art encryption technology on data stored within the device as well as for data in motion in and out of the device.


The Xerox Mobile Print Cloud Service supports printers from a variety of manufacturers. It is the customer’s responsibility to understand the security features of any non-Xerox printers configured for use in the system.
Communication between System Components

Communication between Xerox Mobile Print Portal Mobile Application and Xerox Mobile Print Cloud Service

The Xerox Mobile Print Portal Mobile Application uses the HTTPS protocol for all communication with the Xerox Mobile Print Cloud Service. It establishes an HTTPS secure connection with the Xerox Mobile Print Cloud Service relying on the mobile device operating system to validate the security certificate as part of establishing the SSL connection. The SSL certificate is issued by Comodo (a trusted certificate authority) and ensures that the application has been verified and validated.

The Xerox Mobile Print Portal Mobile Application requires users to authenticate before using any of its features. Basic authentication is performed with the Xerox Mobile Print Portal Mobile Application providing username and password information over the HTTPS protocol.

Once authentication is complete, data is passed between the Xerox Mobile Print Portal Mobile Application and the Xerox Mobile Print Cloud Service to enable the features of the service within the Xerox Mobile Print Portal Mobile Application. This includes all data for previewing and printing jobs, location of printers, and user location data as determined by the mobile device. Users are only able to access documents they submitted and printers to which they have been granted access.

Users should consult their network provider on best practices for securing their 3G/4G communications on their mobile devices.

Communication between Mobile Device and Email Server

Emails submitted to the Xerox Mobile Print Cloud Service by a user’s mobile device or computer will use the security mechanism defined by the user’s email client. User documents are the primary data transmitted via email to the Xerox Mobile Print Cloud Service. It is the user’s responsibility to ensure appropriate email security controls are in place.

Emails generated by the Xerox Mobile Print Cloud Service typically contain temporary user passwords and system messages.

Communication between Email Server and Xerox Mobile Print Cloud Service

Emails are processed and consumed immediately upon receipt by the XMPC service. Emails are not stored in any repository or inbox.
Communication between Xerox Mobile Print Cloud Service and Xerox Mobile Print Cloud Agent

The Xerox Mobile Print Cloud Agent uses the HTTPS protocol for all communication with the Xerox Mobile Print Cloud Service. It establishes an HTTPS secure connection with the Xerox Mobile Print Cloud Service relying on the PC's operating system to validate the security certificate as part of establishing the SSL connection.

After successful installation of the Xerox Mobile Print Cloud Agent software, it will attempt to register itself with the Xerox Mobile Print Cloud Service. The Xerox Mobile Print Cloud Agent’s registration process provides the Xerox Mobile Print Cloud Service with the Xerox Mobile Print Cloud account’s administrator credentials, the Xerox Mobile Print Cloud Agent Activation Code, and a machine hash code. The Xerox Mobile Print Cloud Service returns a Xerox Mobile Print Cloud Agent registration identifier to complete the registration process. The Xerox Mobile Print Cloud account’s administrator credentials are only held in memory during the registration process and removed once the registration process is complete.

After successful registration of the Xerox Mobile Print Cloud Agent, print job data is transmitted between the Xerox Mobile Print Cloud Service and the Xerox Mobile Print Cloud Agent in the form of print ready files. This data may exist in memory on the agent PC while it is being spooled to the printer. In addition, data about printers discovered and printer capabilities is transmitted.

Communication between Xerox Mobile Print Cloud Agent and Printer

The Xerox Mobile Print Cloud Agent uses SNMPv2 to discover printers and printer capabilities. Customers can configure the community name strings for the agent to use if they have configured their printers to use non-default values.

The Xerox Mobile Print Cloud Agent routes print jobs to the target printer using Raw Port 9100. These ports are not configurable.

Customers can further secure the print path by enabling IPSec between their Xerox Mobile Print Cloud Agent PC and their printers provided the printers support IPSec. If configuring IPSec, ensure that the communication between the Xerox Mobile Print Cloud Agent and Xerox Mobile Print Cloud Service does not employ IPsec.
The Role of Xerox

Xerox will strive to provide the most secure software product possible based on the information and technologies available while maintaining the product's performance, value, functionality, and productivity.

Xerox will:

• Run industry standard security diagnostics tests during development to determine vulnerabilities. If found, the vulnerabilities will either be fixed, minimized, or documented.

• Monitor, notify, and supply (when necessary) security patches provided by third party software vendors used with the Mobile Print software.