Xerox® Mobile Print Solution

Information Assurance Disclosure

Software Version 3.6
May 2016
702P03992

BR 15144

Contents

[This page left intentionally blank]

1 Introduction

Xerox® Mobile Print is a workflow solution that connects a corporation mobile workforce to new productive ways of printing. Printing is easy and convenient from any mobile device without needing standard drivers and cables.

1.1 Purpose

The purpose of this document is to disclose information for the Xerox® Mobile Print Solution 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 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 Solution relative to Information Assurance (IA).

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

1.2 Target Audience

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

It is assumed that the reader is familiar with the Xerox® Mobile Print workflows; as such, some user actions are not described in detail.

1.3 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.

2 System Workflows

2.1 Overview

The workflow of mobile printing is quite simple. A user using a mobile device such as a smart phone, tablet, or laptop sends a document to the Xerox® Mobile Print Server. Depending on the submission method, the job is either printed without any further user action or the user manually releases the job to print.

There are several methods for a mobile user to submit or release a job to print. The Submission method is technically decoupled from the release method. However, certain submission/release pairs make more sense than other pairs.

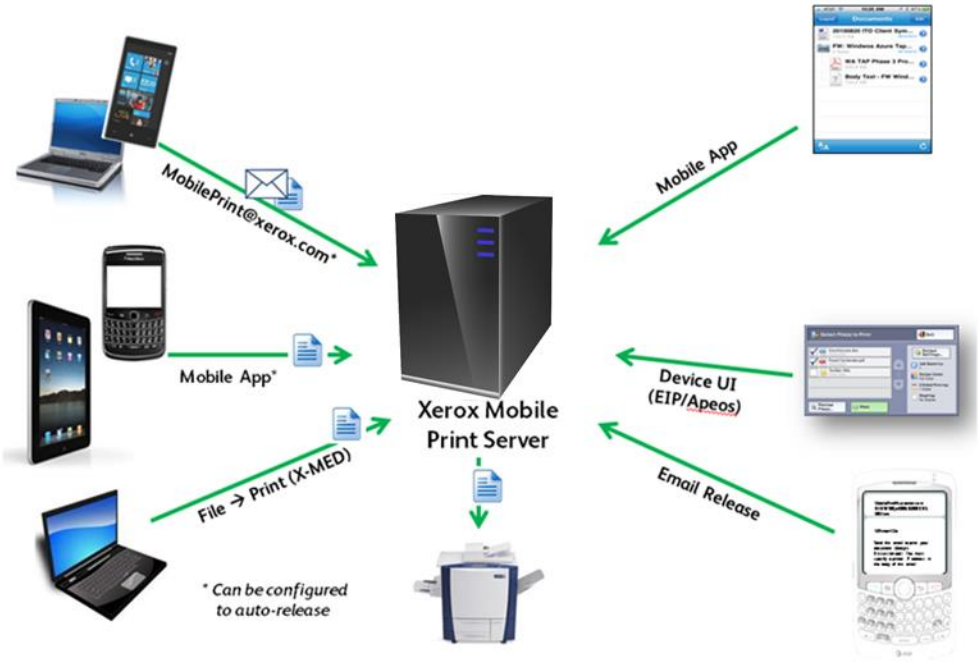

Figure 1.2-1 Mobile Print Submission Methods

Submission methods:

1. Email
2. Print Portal Application (i.e., an app on a mobile device)
3. Xerox® Mobile Express Driver® (aka File → Print)†
4. Windows PC with v4 Driver (aka File → Print)†

Release methods:

1. Email
2. Printing device UI (via EIP/Apeos)
3. Print Portal Application (i.e., an app on a mobile device)

Combined methods (i.e., job will print without any explicit user action after submission):

1. Email
2. Native App (i.e., an app on a mobile device)

The common link between all submission and release methods is the Xerox® Mobile Print Server. Documents are stored in the solution until they are deleted or until an administrative time-out has passed.

Installation, setup, and configuration of all tools are assumed to be similar to installing and configuring any other application and are not addressed in this document. Please refer to the Deployment Guide for details.

Subsequent sections will detail the methods of submission, release, and document storage in the Xerox® Mobile Print Server.

2.2 Submission Methods

2.2.1 Email Submission Workflow

Step 1: User selects document to print and creates an email with that document as an attachment, sending it to the Xerox® Mobile Print email address.

Step 2: The Mobile Print Solution monitors the email inbox and retrieves incoming submissions. The documents are held in the Mobile Print Solution for later release at the Xerox® MFP.

Step 3: The Mobile Print Solution will send the User an email with a confirmation code.

2.2.2 Mobile Print Portal Application Submission Workflow

Step 1: User selects document to upload and opens with the Xerox® Mobile Print Portal application. Using the Mobile Print Portal Application the user selects the upload option.

Step 2:

The document is uploaded to the Xerox® Mobile Print Solution.

2.2.3 Xerox® Mobile Express Driver® Submission Workflow†

Step 1: From within a PC application, the user selects File → Print and then chooses the Xerox® Mobile Express Driver® (XMED) Printer and selects Print. This opens the XMED Driver interface. The user then selects the Xerox® Mobile Print icon and then Print.

Step 2:

The document is uploaded to the Xerox® Mobile Print Solution.

2.2.4 Windows PC with v4 Driver Submission Workflow†

Step 1: From within a PC application, the user selects File → Print and then chooses a Printer that is configured to use a Mobile Print v4 Filter. The user then selects the desired attributes and submits the job.

Step 2:

The document is uploaded to the Xerox® Mobile Print Solution.

2.3 Release Methods

2.3.1 Email Release Workflow†

Step 1: After receiving the email with the confirmation number, the user opens the email, and selects the "release" link. This will generate a new pre-formatted email that is ready to be sent to the Xerox® Mobile Print Solution. The user enters the IP address of the printer or the printer's alias and sends the email. The subject of the email contains a message key as a method of ensure that the user who submitted the file is the one who is releasing it.

Step 2: The Xerox® Mobile Print Solution monitors the email inbox and retrieves incoming submissions.

Step 3: The email is processed, and based on its content, the MPS will convert the associated document using the default job attributes configured for the user into a print ready document. The Xerox® Mobile Print Solution routes the print-ready document to the desired printer.

Step 4: User receives their printed document.

2.3.2 Print Device UI Release Workflow

Step 1: User enters their Confirmation code at the MFP, selects which documents to print, selects their desired print attributes (Duplex, Stapling, Copies, B&W vs. Color), may optionally choose to preview, and selects Print.

Step 2: The Mobile Print Solution processes the original file, converting it to a print-ready document. If accounting information is required and the user has cached data for the printer or print queue, the system automatically supplies the cached data. The Xerox® Mobile Print Solution routes the print-ready document to the MFP.

Step 3: User receives their printed document.

2.3.3 Print Portal Application Release Workflow

Step 1: User opens the Xerox® Mobile Print Portal application. They then select the uploaded document from within the app. Then then modify any print job attributes desired (e.g. Duplex, Stapling, # of Copies, B&W vs. Color). The user then selects Print.

Step 2: The Xerox® Mobile Print Solution converts the original document to a print ready format and routes it to the selected printer.

Step 3: User picks up their printed document.

2.4 Combined Methods

2.4.1 Email Combined Workflow

Step 1: User selects document to print and creates an email with that document as an attachment, sending it to the Mobile Print email address with the printer IP Address in the subject.

Step 2: The Xerox® Mobile Print Solution monitors the email inbox and retrieves incoming submissions.

Step 3: The Xerox® Mobile Print Solution processes the email and attachments, converting them to a print-ready document.

Step 4: The Xerox® Mobile Print Solution routes the print-ready document to the specified printer.

Step 5: User receives their printed document.

2.4.2 Print Portal Application Combined Workflow

Step 1: User selects document to print and opens with the Xerox® Mobile Print Portal application. Using the Mobile Print Portal 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 Solution for conversion to a print-ready document.

Step 3: The Xerox® Mobile Print Solution converts the original document to a print ready format and routes it to the selected printer.

Step 4: User picks up their printed document.

2.5 Administrative Workflow

Step 1: Administrator logs into the Xerox® Mobile Print Solution website. Administrators can configure solution behaviors and manage devices, users, and jobs.

Administrator functions:

- Configure Solution
- Manage Printers
- Manage Users
- Manage Jobs
- Manage Licenses
- View Reports

2.6 Email Workflow Details

Users send an email with the documents they wish to print as attachments to a specified email address.

The XMPS Server monitors the email address' inbox and reads the entire email with all attachments. The original email is then deleted from the email server. At this point, the only copy of the email (and attachments) resides on the Mobile Print Server.

The Mobile Print Service will then authenticate the user to verify he is allowed access to printing resources. Xerox® Mobile Print Services uses Active Directory Services (ADS) as a starting point to establish a user base. Xerox® Mobile Print can be configured to automatically authenticate against users in ADS and reject users not authenticated in the ADS. It can also force unauthenticated users through a different workflow that requires the administrator to validate their email address before they can use the mobile print services. While new unauthorized users can exist in the system, these users' documents are not stored in the system to mitigate resource usage by such users.

Next, the system will respond to the user by sending him or her an email with a confirmation number and various other print options dependent on configuration. The system must be connected and have access to an SMTP, Exchange Web Service (EWS) server, or Lotus Domino server to send reply messages to the user. The system supports SMTP / EWS / Notes Remote Procedure Call, SSL, username, and password. The server does not need to be the same server used for the POP, IMAP, or Domino email account used as the inbox. The receiving and sending accounts cannot be the same to prevent email loops.

The confirmation number is used in the release methods, which are described later. It is a unique number, randomly generated when the user is created. Note that the confirmation number is unique per user. Users can also request a new confirmation number through the email workflow links if they believe their confirmation number has been compromised. The

length of the confirmation number can be customized in the configuration tool to accommodate the security needs of your enterprise.

The above process repeats each time the user sends an email to the mobile printing system.

Additionally, the system can be configured so that if the IP address of the printer is specified in the email that contains the documents to be printed, the documents will print automatically. That is, there is no explicit user action to release the jobs to print.

2.7 Authentication via Xerox® Mobile Print Cloud Service

Xerox® Mobile Print Cloud Service is an optionally configured component that helps facilitate availability of Xerox® Mobile Print on the Print Portal app. It is used to route users to the internal corporate endpoint. If configured, the user's email is sent to Xerox® Mobile Print Cloud Service, and the cloud service inspects a user's provided email address (domain) to determine if it can automatically decide what enterprise to associate the email with. If Xerox® Mobile Print Cloud Service cannot determine the appropriate enterprise; the user is prompted to enter a six-digit alphanumeric Company Code which needs to be provided to the user by their administrator. Once the user is associated with the correct enterprise, the user's account creation will follow the rules described in the email section. If the user is enabled, the user will be prompted to check their email for their confirmation number and enter it, or to enter their username and password, depending on the authentication method (determined by the XMPS Server). The user remains logged in to the application until choosing to logout. Upon login, a token is created and passed to the server with every call. If the token is expired, based on the expiration timing policy set on the server, the mobile device will attempt to use the credentials stored in the mobile devices secure storage to automatically re-authenticate the user. If the re-authentication fails, the user is prompted to login to the application.

2.8 DMZ Configuration

The Azure service bus public endpoint is the typical configuration when a customer wants to allow users outside the network to access Mobile Print. However, there are some customers who wish to allow users outside the company network to access the Mobile Print system, yet they do not want to allow documents to be passed through the Microsoft owned cloud.

Mobile Print supports a configuration where the customer can set up a satellite pass-through server in a DMZ, which is accessible from outside the network. This server is configured as the external endpoint in a private configuration, and all data sent to it is forwarded to the internal server. The communication between DMZ servers and internal servers is secured. Before a DMZ server can communicate with an internal server, the DMZ server must authenticate with a valid username/password for the internal server. Once this authentication is successful, the DMZ server receives a token that is used for all further communication. This token is required for all communication to the internal server.

2.9 Xerox® Mobile Express Driver®†

Xerox® Mobile Express Driver® (X-MED) is part of mobile print and can be installed and configured separately. X-MED is only available on a PC or laptop and can submit jobs directly to a printer or to the Xerox® Mobile Print Server.

X-MED can submit a job to the Xerox® Mobile Print Server, at which point one of the release methods must be used to print the document. This method essentially bypasses the email server. As such, this submission method uses the corporate network.

Submitting a job directly to a printer is identical to any File>Print action and the user must have access to the printer, so it is assumed the user is within the corporate firewall. Security considerations for this method are not in the scope of this document.

2.10 Document Preview

Once a document has been submitted, a user (after being authenticated so that the document queue is listed to the user) may be able to view a thumbnail of the document (i.e., preview the document). This section describes any document transfer actions that occur for each viewing method.

2.10.1 Printing Device UI (via EIP)

When a preview is requested, the XMPS sends a set of jpeg images to the printing device UI. The actual document is not transferred. The jpeg is stored in RAM is and is deleted when the Xerox® EIP screen is exited.

2.10.2 Printing Device UI (via Apeos)

When a preview is requested, the XMPS sends a set of jpeg images to the printing device UI. The actual document is not transferred. The jpeg is stored in RAM is and is deleted when the Apeos screen is exited.

2.10.3 Native App (An App on a Mobile Device)

When a preview is requested, the XMPS sends the document back to the authenticated user and mobile device requesting the preview. Generation of the preview relies on the mobile devices ability to render and display the document. Secure HTTPS is leveraged for the preview data exchange. Once a user navigates away from the preview, the data is deleted until requested in the future.

For document types not supported by the mobile OS or a third party viewer but are supported by the mobile print server for printing, when a preview is requested, the XMPS sends a set of jpeg images to the mobile device UI. The actual document is not transferred. The images are stored in memory and deleted when the user leaves the screen.

2.10.4 Email

Preview is not supported for the email release method.

2.11 Public Printing

Once public printing is enabled for mobile print by the mobile print administrator, the Xerox® Public Print Cloud Service is authorized to retrieve the document using the standard mobile print API and the user's token. Once the file is retrieved from the mobile print server, it is sent to the public print provider chosen by the user. The document retrieval and transmission is done over SSL Port 443 by the cloud service. In order to use public print providers outside of the Xerox network, the user is prompted to agree to the terms if service prior to submitting the job via the Print Portal application.

2.12 Push Notifications

Xerox® Mobile Print supports the ability to send push notifications to the Print Portal Application on a user's phone. Push notifications are used to notify the user of the status of print jobs submitted via the Print Portal Application. This feature must be enabled by the Mobile Print administrator, and each user must agree to receive notifications from Xerox when logging into the Print Portal App. Typically, this is done the first time the user logs into the app, but they have the option to change this setting at a later time via the phone settings. When enabled by the user, the Print Portal App will register itself with Apple or Google to receive push notifications for this particular application. Correspondingly, the Xerox® Mobile Print Server will send events to the Xerox® Mobile Print Windows Azure server, which will forward the notification to Apple (using the Apple Push Notification Server API) and/or Google when a job is transferred to a printer (success / failure). The results are forwarded to the respective mobile device.

3 Security Description

The architecture of the Xerox® Mobile Print Solution incorporates technical controls to eliminate, where possible, information security risk from all information assets including software components, connected system components, and information owners. Figure 3-1 below illustrates the relationship between the Xerox® Mobile Print system and these other system components. The base of the arrows indicates the system or touch point that initiates the contact.

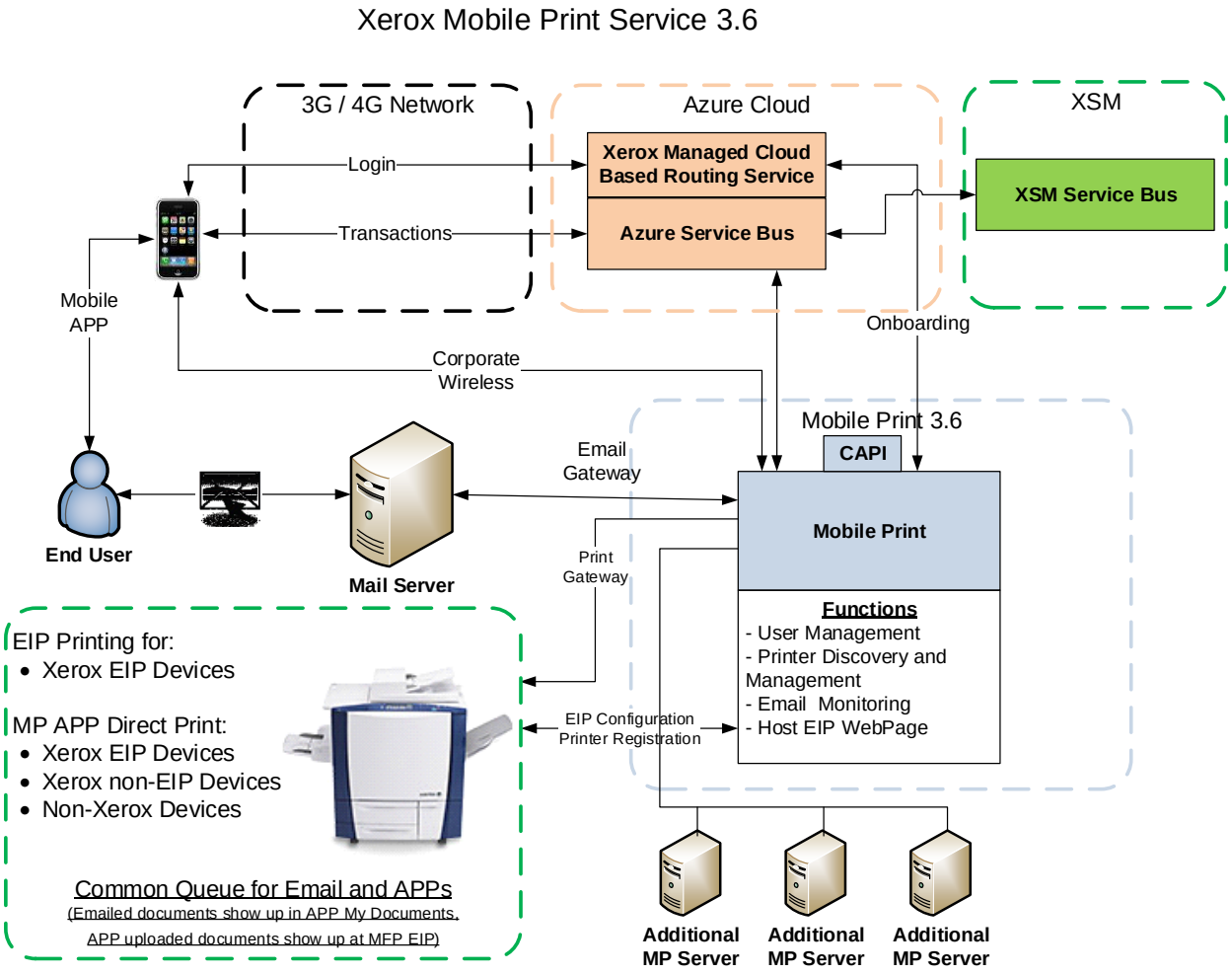

Figure 3-1: Xerox® Mobile Print Architecture

The following sections describe the components in the system and then the interfaces between the components.

Please note that this solution has been designed to offer flexibility and tailored account configuration while still maintaining a secure baseline configuration. Items that are configurable are reviewed in this document, while the methods regarding how to configure these items are not discussed in this document. From a system point of view, the administrator has control over which printers support mobile printing and which users are enabled to use mobile print.

All communication between components is SSL encrypted with the following exceptions:

Communication	Encryption Details
Xerox® Mobile Print Server to Printer	LPR and port 9100 (RAW) printing do not support encryption. If Xerox® Mobile Print is configured to print only using IPP over SSL, all communication to the printer is encrypted.
Xerox® Mobile Print Portal to Xerox® Mobile Print Server	Uses SSL over port 443 Uses mDNS (Multicast DNS) over port 5353 to locate the server on the local subnet for AirPrint. Uses IPP over SSL (Port 631) for AirPrint submission.
Xerox® Mobile Print Portal to Customer DNS Server	Uses DNS-SD (Service Discovery) to locate the server for AirPrint.
Xerox® Mobile Print Server to Customer Email Server	Email servers can be configured for both secured and unsecured connections. If the server supports secure connections, Mobile Print can be configured for secure communication.
User to Customer Email Server	If the email server supports secure connections, the Print Portal application can connect securely.
User PC via v4 Driver to Xerox® Mobile Print Server†	Uses Microsoft SMB File Sharing and Printing. Encryption depends on Microsoft file and print sharing settings.
Xerox® Mobile Print Server to Printer	SNMPv1 and v2 are used by default and do not support encryption. SNMPv3 is optional and all data is encrypted.
Xerox® Mobile Print Server to Document Conversion Engine	Not encrypted
Xerox® Mobile Print Server to Xerox Corporate Licensing System	Uses SSL over port 8443
Xerox® Mobile Print Server to Windows Azure™ †	Secured and encrypted using proprietary Microsoft technology

[† - Not needed in all configurations. Consult the Administrators Guide for information on available options.]

Table 3-1: SSL Component Communication

This section captures the security considerations and implementation of Xerox® Mobile Print Solution in the following areas:

- Protocols and Port numbers used by the system
- Individual system components
- Communication between system components
  - User and Email Server Communication
  - Email Server and Mobile Print Server Communication
  - Mobile Print Portal Application to Mobile Print Server Communication
  - Mobile Print Server and the Multifunction Devices Communication
  - Mobile Print Server Administration
  - Microsoft SQL Server Express database deployment
  - Mobile Print Server Windows NTFS file structure permissions
  - Conversion Server Communication

3.1 Protocols and Port numbers used by the system

The following table lists the standard default ports used for many of the protocols with Mobile Print. Some port numbers are configurable in Mobile Print such as the POP and IMAP ports. Other port numbers are non-configurable and cannot be changed. You may need to change some port numbers depending on the server you are communicating with or use the default ports if they cannot be changed. All ports used must be unblocked in the firewall that is being used on the solution server.

Protocol	Default Use Port Value	Use	Option
Web Communication Ports:			
HTTP	80	Hypertext Transfer Protocol.	Non-configurable
HTTP/SSL	443	HTTP over SSL. If a certificate is already configured on the IIS default website, it will be used by Xerox® Mobile Print. If no certificate is configured, Xerox® Mobile Print will create a self-signed cert. The administrator has the option to load a certificate from a trusted authority later if desired.	Non-configurable
Licensing Ports:			
HTTPS/SSL	8443	HTTP over SSL. Used to activate or validate a license. If the customer is using off-line activation, then this port is not needed.	Non-configurable
Email Communication Ports:			
POP3	110	Post Office Protocol version 3 enables "standards- based" clients such as Outlook Express or Netscape Communicator to access the email server.	Configurable
POP3/SSL	995	POP3 over SSL uses TCP port 995 to securely retrieve encrypted email messages via POP3.	Configurable
Exchange Web Services	443	Exchange Web Services uses this port.	Configurable
IMAP	143	Internet Message Access Protocol version 4, may be used by "standards-based" clients such as Microsoft Outlook Express or Netscape Communicator to access the email server.	Configurable
IMAP4/SSL	993	IMAP4 over SSL uses TCP port 993 to securely retrieve encrypted email messages via IMAP4.	Configurable

Protocol	Default Use Port Value	Use	Option
Secure IMAP4	585	Originally used for IMAP4 protocol to receive in- formation from email servers. It is typically switched to 993. Some implementations of IMAP4 may still use port 585 to handle incoming messages.	Configurable
SMTP	25	Simple Mail Transfer Protocol is the foundation for all email transport in Exchange 2000.	Configurable
SMTP/SSL (Secure SMTP)	465	SMTP over SSL. TCP port 465 is reserved by common industry practice for secure SMTP communication using the SSL protocol.	Configurable
NRPC (Domino)	1352	Lotus Notes RPC. This is the API used between Lotus Notes and the Lotus Domino server. Communication between XMPC and Lotus Notes is via a local API on the same PC.	Non-configurable
Printer/Printing Communication Ports:			
LPR	515	Fallback printing port if port 9100 not accessible.	Non-configurable
AppSocket RAW or Windows TCP-mon	9100	Common communications port used for RAW printing.	Non-configurable
IPP over SSL	443	Internet Printing Protocol over SSL. Mobile Print will send print jobs to the printers using this encrypted protocol.	Non-configurable
SNMP	161	Printer configuration	Non-configurable
Authentication / User Import Ports:			
LDAP	389	Lightweight Directory Access Protocol uses this port.	Configurable
LDAP with SSL	636	Lightweight Directory Access Protocol with Secure Sockets Layer uses this port. This service does not support a TLS configuration.	Configurable
Mobile Print Internally Used Ports:			
Mobile Print DCE	8801, 8802	Mobile Print uses this port to communicate to the Document Conversion Engine (DCE).	Configurable
Mobile Print Server to Server	8800	Mobile Print uses this port to communicate with other Mobile Print servers.	Configurable
iOS Native Printing:			

Protocol	Default Use Port Value	Use	Option
DNS-SD	53	Print Portal Mobile App printer discovery using DNS.	Not-configurable
mDNS	5353	Print Portal Mobile App printer discovery on the local subnet using mDNS.	Not-configurable
IPP	631	IPP Print submission to Xerox® Mobile Print. Always uses SSL.	Not-configurable

Table 3.1-1: XMPS Network Ports

The default port for hosting application web pages is 443 using HTTPS. If HTTPS cannot be used (for example, it is prohibited in a specific region), HTTP over port 80 can also be configured. Both ports can run simultaneously.

---

† Some features and capabilities noted above are only available with select deployments (e.g., managed service accounts or advanced professional services).

3.2 System Components

3.2.1 Xerox® Mobile Print Solution Services

The Xerox® Mobile Print Server is the foundational component of the Xerox® Mobile Print Solution used to manage the system's behavior and user's interaction within the system from document submission to print. Xerox® Mobile Print Server is a Windows® application running on a Windows® Server. XMPS will conform to the customer's existing security policies, using Windows® based authentication to access this application. Access to the server should be limited to Systems Administrators and authorized Xerox personnel.

User's documents are received and stored for secure release on the Xerox® Mobile Print Server. The Xerox® Mobile Print Server will monitor and work in conjunction with the available Conversion Servers for document conversion and print processing.

3.2.1.1 Mobile Print Solution Administration Services

The Mobile Print Solution administration services run on the Mobile Print Server to provide configuration, user, printer and job management. In addition, user's documents can be converted to a printable format using a Conversion Server (see below).

The administrator interacts with the Administration Services via a web browser interface to perform tasks such as creating an incoming email account to receive jobs upon, managing users, registering printers, and enabling the Mobile Print Portal Application usage. Connection to the Administration Services is supported via HTTP (port 80) or HTTPS (port 443). By default, the Mobile Print Server uses a self-signed certificate for HTTPS communication. [Please note that most web browsers will generate a warning when using the self-signed certificate as it was not generated by a trusted authority]. The administrator has the option to load and use a certificate from a trusted authority on the Mobile Print server.

By default, the Mobile Print Solution will accept any user to create an account within the system. Accounts are created whenever an email submission is received or when the Mobile Print Portal Application is first used to access the system.

However, Mobile Print can be configured to only allow a specific set of users (an allowed-list) or to not allow a specific set of users (a block-list).

When an account is created, the user will receive a system generated confirmation code. The confirmation code is used to access their jobs at the MFP or to connect the Mobile Print Portal Application to the server.

All users jobs are stored and referenced based upon the users email address. User's jobs are stored in the Mobile Print Server Windows file system with a randomized file name. By default they are not encrypted, however, an Encrypted File System (EFS) may be configured manually.

Unprinted jobs are deleted based upon an administrator configured retention period. The default retention period is 1 day. The Retention Settings apply to Print Queues in addition to printers. Sending documents to a print queue is equivalent to the print command in the Mobile Print system. This means that if the system is configured to delete documents after printing, documents will also be deleted after sending them to a print queue. Based on this same example, if a default print queue is set on the system, all emails sent to Mobile Print will be sent to the default print queue and immediately deleted from the system.

4 System

4.1 System Components

4.1.1 Document Storage

Documents are stored unencrypted in the XMPS Server. The documents are stored in a configurable location†, which can be any location that the Xerox® Mobile Print Service has access to. For performance and configuration reasons, on-box storage is recommended. Access to the documents is protected by Windows and Server access on the client's domain. As a layer of protection, actual documents are stored with an obfuscated file name and extension.

The documents are retained until either:

1. The user deletes them via the printing device UI or the Mobile App, or
2. The Xerox® Mobile Print Service deletes them after a configurable timeout.

As with any Microsoft server OS, the deleted documents follow traditional Microsoft Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself but are overwritten as the system reclaims the disk space. The Mobile Print Admin UI does provide the ability to delete documents if needed.

Note: Encryption is available using the Microsoft built-in Encrypted File System (EFS) feature.

Mobile Print limits the maximum size of a submitted file to 1GB or smaller. A utility may be used to modify this value if necessary.

4.1.2 Xerox® Mobile Print Portal Application

The application uses a Xerox® managed cloud based routing service to direct the user to the appropriate Xerox® Mobile Print Server. Once authenticated, the user's credentials and authentication token are stored in the application until they log out.

The Mobile Print Admin has control over how often a user will need to re-supply their credentials when using the Mobile Print Portal App. An option exists to retain the logged on users credentials within the app, such that any subsequent logon will not require the user to re-supply their credentials. The Admin may also control the length of time that the user will remain logged into the account when using the Print Portal App. Users will be required to re-supply their credentials once the once the timeout is reached. If the Admin has enabled the "Retain Login Credentials" feature, then the user would automatically be logged back into the system after the expiration time period.

Users can only access jobs that they have submitted. With the Mobile Print Portal Application, users can preview their jobs, see a list of available printers, select print options and submit their job for printing.

For security reasons, enabling and accessing the Mobile Print Server using the Mobile Print Portal Application is a multi-step process:

1. An administrator must enable the use of the Mobile Print Portal Application via Administration Services at the Mobile Print Server, the result of which is a “company code.” The Mobile Print administrator must distribute this code to authorized users.

   Note: An administrator may request a new company code at any time.
2. During initial login, a user must enter their email address and company code.
3. The Mobile Print system will generate a confirmation code and to insure a valid email address, will send the confirmation number to the user at the supplied email address.
4. The user must enter the confirmation code.

Mobile Print also supports both an allowed-list and a block-list capability. An allowed-list would restrict access to only a specified set of user email addresses; a block-list would disallow these email accounts.

Lastly, if a user needs to reconfigure the Mobile Print Portal Application from one company code to another, an action verification code is sent to the user by the Xerox® Mobile Print Cloud Service itself. The email will come from noreply@PrintbyXerox.com.

The Print Portal Application supports iOS native printing. This print mechanism uses a combination of printer discovery, via either mDNS or DNS-SD to locate a compatible printer. If using mDNS, the Apple Bonjour Service must be installed on the Xerox® Mobile Print Server, and the standard Bonjour ports must be opened on the server’s firewall. The Xerox® Mobile Print Server responds to mDNS queries and advertises itself as a printer, thereby allowing Print Portal Application users to submit print jobs to Mobile Print using iOS native printing. Alternatively, the IT administration at a customer site can configure their DNS servers to advertise the Xerox® Mobile Print Server as a printer. This allows client applications such as Print Portal Application to use DNS-SD (service discovery), to discover the Mobile Print Server as a printer. Regardless of the type of discovery method, once found, the Print Portal Application can submit (upload) jobs to Xerox® Mobile Print using IPP (port 631). Jobs are then available for release using the Print Portal Application to a printer, or the Printer Client (EIP) Application.

4.1.3 Xerox® Managed Cloud Based Routing Service

The Xerox® managed cloud based routing service provides a “routing” capability between the Mobile Print Portal Application, running on a customer’s smart device, and the Mobile Print Solution Server running within the customer’s network. Messages are sent from the Mobile Print Portal Application to the Cloud Service.

The Xerox® managed cloud based routing service runs on the Microsoft Windows Azure Platform (see below). All communication is handled using Industry standard HTTPS protocols. The SSL certificate is issued by Comodo (a trusted certificate authority) and ensures that the application has been verified and validated.

For more information on Windows Azure Security, please visit http://azure.microsoft.com/en-us/support/trust-center/.

4.1.4 Xerox® Mobile Print Conversion Servers

The Xerox® Mobile Print Solution is modular in design, leveraging a core Mobile Print Server component as well as one or more additional components referred to as Conversion Server. The Conversion Server converts documents from their native format (e.g., .doc, .ppt) to a print ready file (e.g., postscript, pcl) that the destination printer understands. A Conversion Server may reside on the same server as the Xerox® Mobile Print Server, or it may reside on a separate server. Only one Conversion Server may reside on each server.

4.1.4.1 Document Storage

Both the native format document and the print ready file are temporarily stored to the Conversion Server system disk while the files are active. Once the Conversion Server has completed the document conversion, the print ready document returns to the Xerox® Mobile Print Server and the files are deleted from the Conversion Server disk and memory.

As with any Microsoft server OS, the deleted documents follow traditional Microsoft Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself, but are overwritten as the system reclaims the disk space. The Mobile Print Service provides no facilities to erase the documents themselves. In this sense, the Conversion Server should be treated as any other document server within the corporate firewall.

4.1.5 Xerox® Mobile Print Database

Microsoft SQL CE 4 database is used by Xerox® Mobile Print as the default relational data store. However, XMP can be configured to work with an external Microsoft SQL database.

4.1.6 Xerox® Mobile Print Express Driver®†

Xerox® Mobile Print Solution leverages this X-MED driver to add the flexibility for users to find and print directly to a printer of their choice or to leverage the Mobile Pull Print solution by selecting Xerox® Mobile Print. Users open their document, select file print, select the Xerox® Mobile Express Driver®, select to use Xerox® Mobile Print, and their document is processed, sent, and waiting for their secure release at whatever printer they choose.

4.1.7 Email Server

The email server is used to receive emails from and send emails to the mobile user. The preferred implementation is to leverage the client's established email infrastructure and email security in place; however, the mail server can be an internally or externally managed server. The email infrastructure will act as the path to transport user's documents from the user's mobile device into the Xerox® Mobile Print infrastructure. The user's documents will temporarily

reside on your mail server until the email message and its attachments are retrieved by the Xerox® Mobile Print Solution.

4.1.8 Printer

The printer can represent any printing device connected to your network. In the figure above and throughout this document, we will use a Xerox® MFD with an EIP/Apeos control panel interface.

4.1.8.1 Xerox Extensible Interface Platform® (EIP)

Xerox® multifunction devices introduce a flexible Xerox® proprietary platform called EIP. This platform acts as a secure embedded web service that other applications can leverage to expose functionality and services to the user through the local control panel interface. Xerox® Mobile Print uses this platform to secure access and present users with the Xerox® Mobile Print Solution.

4.1.8.2 Xerox Apeos

Fuji Xerox® multifunction devices introduce a flexible proprietary platform called Apeos. This platform acts as a secure embedded web service that other applications can leverage to expose functionality and services to the user through the local control panel interface. Xerox Mobile Print uses this platform to secure access and present users with the Xerox® Mobile Print Solution.

4.1.9 Mobile Print User

The mobile print user is an end-user attempting to print a document using the Xerox® Mobile Print Service from a mobile device, laptop, or desktop PC to a printing device on the corporate network. It is assumed that the client's security policy and systems have already authorized the user to use corporate facilities.

4.1.10 Xerox® Services Manager (XSM) Connectivity

The Xerox® Mobile Print system can connect to XSM in order to perform the following actions:

- Export Job Data (Page count, Plex, etc.)
- Import Printers, Sites and Printer/Site Mappings

Each of these methods of synchronizing with XSM has its own configuration as well as specific limitations on the system as a whole.

Connectivity to XSM can only be enabled if Xerox® Mobile Print has a license for "Xerox® Mobile Print - Managed Print Services."

4.1.10.1 Export Jobs to XSM

Only the account ID is needed in order to export jobs to the system. If the printer data is matched to a printer in XSM, then XSM will record the data.

If “Obscure User Data” is enabled, no identifying user information such as the username or password is sent to XSM. All identifying information is replaced by unique GUIDs such that the number of individual users reported remains the same but each unique user cannot be identified.

The following data is sent to XSM:

- Display Name
  - Printer Display Name
- Network User Name (e.g. the Domain\Username)
  - If Obscure User Data is set, a random GUID is sent
  - If Obscure User Data is not set, the Domain\Username is sent
- Email Address
  - If Obscure User Data is set, a random GUID is sent
- Network Accounting ID
  - This field will be mapped to Network Accounting User Name on XSM
- NUp
  - This only applies when printing using the FX Apeos workflow
- Copies
- Page Count B/W
- Page Count Color
- Plex
- Submission Date Time
- Completed Date Time
- Content Size
- Color
  - If the document contains color
- Document Type
  - If the document is Word, PPT, etc.
- Media Size
- Printer Name
- Printer MAC Address
- Server Name
  - Always Mobile Print Server Name
- Server MAC Address
  - Always Mobile Print Server MAC address

4.1.10.2 Import Printers / Sites from XSM

When Mobile Print is configured to import printers and sites from XSM, then XSM is treated as the source of record. As such, administrator has several limitations on what can be changed on printers and sites. The general principle is that any data that comes from XSM should be read-

only. The administrator can only change fields related to printers and sites that do not come from XSM.

When printers are imported from XSM, Mobile Print will perform an SNMP discovery to add the printers to the printer list. If the discovery fails, printers will not be added to Mobile Print.

In order to correctly discover XSM printers, discovery settings such as SNMP community names and device credentials must be set correctly on the discovery tab. The settings that the printers used to discover the printers from XDM or XDA are not used and must be specified again in Mobile Print.

If a printer is successfully imported to the Mobile Print system and then is deleted from XSM, it will remain in the Xerox® Mobile Print system until the SA disables or deletes it.

4.1.11 DMZ Configuration

The Azure service bus public endpoint is the typical configuration when a customer wants to allow users outside the network to access Mobile Print. However, there are some customers who wish to allow users outside the company network to access the Mobile Print system, yet they do not want to allow documents to be passed through the Microsoft owned cloud.

Mobile Print supports a configuration where the customer can set up a satellite pass-through server in a DMZ, which is accessible from outside the network. This server is configured as the external endpoint in a private configuration, and all data sent to it is forwarded to the internal server.

The communication between DMZ servers and internal servers is secured. Before a DMZ server can communicate with an internal server, the DMZ server must authenticate with a valid username/password for the internal server. Once this authentication is successful, the DMZ server receives a token that is used for all further communication. This token is required for all communication to the internal server.

4.1.12 Logging

The Mobile Print server uses logging to help diagnose issues and problems. User credentials (e.g., passwords or confirmation numbers) are never logged.

4.2 System Component Interfaces

4.2.1 Users and the Xerox® Mobile Print Solution

Users may be added, deleted, or modified in the Xerox® Mobile Print Solution. Refer to the Xerox® Mobile Print Solution Administration and Configuration Guide (latest version) for details.

The user interacts with the Printer to:

1. Release documents to print.
2. Retrieve the printed documents.

Note: For a description of any specific Xerox® printing device's Xerox® Security Information, Bulletins, and Advisory Responses see www.xerox.com/information-security.

4.2.2 User and Email Server Communication

The first layer of security is at the point of contact between the user and the method used to expose the email address to the end user. Although this is necessary to facilitate the use of the system, it can be controlled using various mechanisms. For example, the email address can be made available through a Xerox® printer's EIP interface and thus accessible to only people physically at the printing device.

The details on how the XMPS solution interacts with the customer email server are provided later.

Users submit their documents for printing using standard email messages from their smartphone to their company's email server. Whether the email messages are encrypted or not is a decision and responsibility of the company's IT department.

If the user is submitting the email within the internal corporate network to a corporate email server, the transmission of the document is as secure as any email sent over the corporate network. This is true for both wired and wireless connections. However, if the user submits the email from outside the corporate network, for example, sending it from a personal email account such as Gmail, security cannot be guaranteed until the email is within the corporate network.

In both cases, the security of the document is no different from any email sent to a co-worker's corporate email address.

While a public email server can be used, it is recommended that you have control over the email server and that it is within your corporate firewall. This latter configuration offers the first line of defense by giving you the ability to create and control Blocked and Allowed user lists based on domain.

The Mobile Print Server communicates to the end user via email messages sent through the customer's email server. Each time a user submits documents for printing; the Mobile Print Server will retrieve the message and respond with a confirmation email message. The confirmation email message contains a personal confirmation code. The confirmation code is later used to retrieve and print their documents at the multifunction device (MFD).

Confirmation codes are configurable in length and unique for each user. Once assigned the confirmation code will be reused for each submission from the same user. Note, this is specifically for the users convenience so that all their jobs will be shown at the MFD. Users may request that their confirmation code be changed at any time.

4.2.3 Email Server and Mobile Print Server Communication

Network communication between the email server and the Mobile Print Server is configured within the administration pages.

For security:

- The Mobile Print server will require a customer supplied username and password to access the Mail Server. The credentials are stored within the SQL database.
- The communication port is configurable.
- Network communication between the servers can be configured to be encrypted using SSL.

XMPS can send emails to the user and acts as a standard email client. It periodically polls the email server (the poll time is configurable) and retrieves any emails and attachments as needed. Once the email is retrieved, the email and attachments on the email server are deleted.

The Xerox® Mobile Print Server supports connectivity to the following:

- SMTP (port 25 or 587),
- IMAP (143 or 993 (SSL)) and
- POP (110 or 995 (SSL))
- Microsoft Exchange Web Services (80 or 443 (SSL))
- Lotus Domino NRPC (Port 1352)

Using the protocols above, Mobile Print will connect to the inbound email account to pull messages, and use the outbound email configuration for sending email. The inbound and outbound email configurations may use different protocols. Mobile Print can connect to a Microsoft Exchange Server 2007 or later using Exchange Web Services (EWS). This connection is made over the HTTPS protocol. When communicating with Domino, the XMPS communicates using a local API with Lotus Notes Client installed on the same PC as XMPS, which in turn uses Note RPC to communicate with the Domino server.

Mobile Print can authenticate either using Basic Authentication or Impersonation.

In the case of basic authentication, the username and password are sent securely to the EWS server for authentication.

When impersonation is used, Mobile Print will Log On as the impersonated user for the duration of the EWS connection. The impersonated user must have Log On credentials to the Mobile Print system.

4.2.4 Mobile Print Portal Application to Mobile Print Server Communication

In order for a smart device application, running on a service provider's 3G/4G network to "talk" to a server behind a corporate firewall, an intermediate cloud-based service is used. Effectively the cloud service is a *forwarding* service. The smart device application sends requests to the cloud service. They are queued until the appropriate server has requested to pick up any messages. The server will process these requests and return them to the forwarding service, which will send to the appropriate application.

HTTPS protocol is used for all communications between the Mobile Print Portal Application, the Xerox® managed cloud based routing service, and the Mobile Print Server. Validation of the certificate is done by the receiving system. Therefore, the Xerox® managed cloud based routing service relies on the mobile device operating system to validate the security certificate as part of establishing the SSL connection. Likewise, the Xerox® managed cloud based routing service relies on the Mobile Print Server to validate the security certificate as part of establishing an SSL connection.

The Mobile Print Portal application requires users to authenticate before using any of its features. Basic authentication is performed with the Mobile Print Portal Application providing email and confirmation number or using LDAP credentials over the HTTPS protocol.

Once authentication is complete, data is passed directly between the Mobile Print Portal Application and the Mobile Print Server or from outside the corporate network by routing through the Azure Service Bus. 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. Again, all communication is using the HTTPS protocol.

In a DMZ Configuration, the intermediate cloud-based service is hosted by the customer. The Mobile Print Portal Application communicates with the customer hosted cloud service, which in turn communicates with the Mobile Print Server. All communication between the mobile phone and the DMZ server, as well as the DMZ server and the Mobile Print Server is done using HTTPS. All other details in the above section apply to a DMZ setup accept for the replacement of the Xerox® hosted cloud service with the customer hosted DMZ server.

If using iOS native printing, the Print Portal Application may use mDNS (Port 5353) to discover printers (e.g., the Xerox® Mobile Print Server). When iOS Native Printing is enabled, the Mobile Print Server is listening for and responding to mDNS queries. Alternatively, the Print Portal Application may use DNS-SD (Service Discovery) to locate printers. Once found, the Print Portal Application uses the iOS native print submission mechanism (IPP over port 631) to upload jobs to the Mobile Print Server.

4.2.5 Mobile Print Server and Multifunction Device (MFD) Communication

When users are ready to print their documents there are two methods

1. They will go to a multifunction device (MFD), start an EIP application, and enter their confirmation code.
2. They will pick an MFD using the Mobile Print Portal Application to which the Mobile Print Server will send their job.

Based on the above user interactions, the XMPS will interact with the printer in five ways:

1. XMPS connects to the printer's web services to install the mobile print EIP/Apeos application on Xerox® printers via port 443 over HTTPS.
2. XMPS can host web pages to the printing device's User Interface commonly referred to as Xerox Extensible Interface Platform® (EIP) and Apeos. The device must be enabled to display these web pages and the web pages do not have any access to documents or any data residing on the printing device. All data exchanged is over port 80 via HTTP (default). HTTPS (port 443) is also supported.

   Users identify themselves at the Printer Client application by entering their confirmation number, email and confirmation number, or their LDAP credentials based on the system configuration. The LDAP password is always obscured (hidden) when entered in the application. The confirmation number is shown by default, but the option to obscure the confirmation number may be enabled by the administrator if necessary.
3. XMPS queries the printer when a job is released to print to obtain the printing device's latest status of the paper trays (paper size and availability).
4. XMPS submits a print ready file to the printer. The default submission method is Port 9100 over TCP/IP. Other ports that can be used are 2501, 2000, 515 (LPR), and 443 (IPP over SSL).
5. XMPS connects to the printer via SNMP (port 161) to retrieve printer configuration and determine paper availability and size for the paper substitution option.

4.2.6 Administrator configuration and usage of the Mobile Print Server

Accessing the Mobile Print server administration web pages use HTTP specification for Basic Authentication. This access protocol requires a username and password for client authentication and is supported by most browsers.

During installation, the MPAdmin group is created.

Windows user accounts that are members of the Administrator or MPAdmin groups on the Mobile Print Server would have access, but not user accounts.

4.2.7 Microsoft SQL Server Compact database deployment

During installation of the Mobile Print server, a SQL Server CE database is created in the install location. Access to this database is restricted through file permissions.

4.2.8 Microsoft SQL Server external database deployment

During installation of the Mobile Print server, a database is created in the specified SQL database instance. In order to create this database the user that installs Mobile Print must have permissions to create databases, database logins and grant permissions. During install Mobile Print grants the Mobile Print system account “<ComputerName>$” rights to update the created database.

4.2.9 Mobile Print Server Windows file structure

The Mobile Print Server stores files in the install location:

%ProgramData%\Xerox\XMP

4.2.10 Document Conversion Engine Communication

The Mobile Print Main services will send the user’s documents to the Conversion Server using a named pipe (net.pipe) protocol on port 8802. The connection can be configured to use other bindings if desired. User documents are only temporarily stored within the external Conversion Server and only to the extent of network communication and conversion.

When the XMPS and the Conversion Server(s) are on separate machines, they communicate via TCP/IP over ports 8801 and 8802.

4.2.11 External Communication to XMPS via Azure

Except for incoming email, by default XMPS cannot be accessed from outside the company network. The administrator enables this workflow and may choose to limit it to only users which are operating within the company network.

Users with mobile devices and X-MED installations operating outside of the company’s network will have secure access to the XMPS solution by connecting through the Xerox® managed cloud based routing service for the initial routing process. The X-MED driver allows the user to submit documents to XMPS from the desktop via the submission paths described above. The data is submitted via an HTTPS (port 443) connection over TCP/IP and has no access to the data stored on the XMPS server. All documents submitted are stored within the user repository along with any other jobs submitted to XMPS by any other means.

The Windows Azure Service Bus is a Microsoft Cloud based messaging system that Xerox leverages to establish a secure application-to-application connection allowing select communication between approved clients outside a company’s network to leverage services within a company’s solution. While the Windows Azure and Xerox® hosted service provide the secure connection path to the service, access to the XMP service and solution continue to be controlled by the local XMP solution.

4.2.11.1 XMPS and the Windows Azure Service Bus

During the provisioning process at set-up time, an external URL is provisioned on the service bus then mobile print is configured to facilitate communication through that URL using an encrypted key. XMPS initiates and maintains a connection to Azure service bus over HTTPS to XMPS services so that users using their mobile device over a public cellular or Internet connection can use Mobile Print. The URL endpoint assigned is what various end clients (i.e., mobile devices) will connect to.

4.2.11.2 Mobile Devices and the Windows Azure Service Bus

When the mobile device communicates with XMPS through the Azure service bus, communication is always over HTTPS with a secure trusted certificate over the service bus URL allocated in the provisioning process. To mitigate the need for the user to type in the URL, a routing mechanism was created to allow URL discovery based on the user's email address domain. Users may be prompted for a company code if the login service is unable to determine which company they are associated with using the domain. Company code is used as a deciding factor to which account/service the user will authenticate/route against. Users have an option to always prompt for company code inside the settings view during login. This gives greater flexibility for a user to specify a certain company to be routed to upon login. The discovery and routing is facilitated through a Xerox® managed cloud based routing service, which is discussed in the next section.

4.2.11.3 Mobile Devices and the Xerox® Managed Cloud Based Routing Service

Mobile devices or other user interfaces may connect to the Xerox® managed cloud based routing service to determine what XMPS endpoint is used for the remainder of the mobile print session. The routing service determines the XMPS endpoint by the user's email address. If this service cannot resolve the external endpoint it may prompt the user for their company code to further resolve the XMPS external endpoint. All communication between the mobile devices and Xerox® managed cloud based routing service is secure over HTTPS (port 443) with a trusted certificate.

4.2.12 LDAP / Active Directory Authentication

When configured for Enterprise Authentication, Mobile Print will verify user credentials against Active Directory. Mobile Print will also query Active Directory for information regarding trusted domains.

In order to communicate with Active Directory, Mobile Print uses the Active Directory Services Interfaces (ADSI) technology that is available in all Windows Operating Systems supported by Mobile Print. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if SSL is being used.

Communication is secured via SASL bind using the GSSAPI mechanism. Mobile Print retrieves a list of trusted active directory domains in the context of the currently logged on user from the Enterprise Mobile Print API Configuration Utility. The configuration utility will search for trusted

domains along with their respective names and LDAP URLs in the active directory forest available to the user that is using the utility.

The Xerox® Mobile Print API service verifies active directory credentials against the specified LDAP domain. In the case of <domain username>/<domain password> authentication, standard LDAP authentication is used. In the case of <email>/<domain password> authentication, Mobile Print (in the context of the “Local System Identity”) will search for a user filtering on email in the Default Active directory domain. If it finds this user, Mobile Print will then extract the username and continue with standard <domain username>/<domain password authentication>. In order to find a user using only an email address, generally both the user and the Mobile Print system need to belong to the default domain.

4.2.13 Active Directory Import

Mobile Print can be configured to import users from Active Directory. This capability is an extension of the setup used for LDAP / ADS Authentication. The Mobile Print Admin has the ability to configure the type of LDAP access (Anonymous, Basic, Negotiate) required when connecting the LDAP server. By default, the system is configured to use the Negotiate setting, which in turn instructs the Mobile Print Server to use SASL when doing an LDAP Bind.

The Admin must supply user credentials that will be supplied to the LDAP server when performing an import (assuming they have selected either Simple or Negotiate for the Usage Mode. The credentials will be stored in the Mobile Print Server database (SQL), and will be encrypted using DES with MD5 hashing.

As part of the import, the Mobile Print Admin can define the LDAP containers that will be queried as part of the import and, in turn, map the fields within those containers to fields within the Mobile Print User Database.

In order to communicate with Active Directory, Mobile Print uses the Active Directory Services Interfaces (ADSI) technology that is available in all Windows Operating Systems supported by Mobile Print. The communication with the Active Directory servers occurs via the standard LDAP port 389 or via 636, if SSL is being used.

4.2.14 Active Directory On-Boarding using Email

When a new user sends an email, Mobile Print checks all of the domains configured for “Advanced” or “Advanced with Import” for the user entry matching the user’s email address. If the user is found in Active Directory, Mobile Print populates the Mobile Print database with the data found in Active Directory.

4.2.15 External Communication to XMPS via DMZ

Except for incoming Email, by default XMPS cannot be accessed from outside the company network. The administrator enables this workflow and may choose to limit it to only users which are operating within the company network.

Users with mobile devices and X-MED installations operating outside of the company's network will have secure access to the XMPS solution by connecting through the customer managed DMZ cloud based routing service for the initial routing process. This allows users to access XMPS outside of their customer network, but using customer controlled servers for document routing.

4.2.15.1 DMZ Setup

In order to enable the DMZ feature, the Mobile Print Server must be set to "Private" mode. When inside of your company firewall, Mobile App users will be access XMPS via the Internal Server endpoint. When outside of the firewall, Mobile App users will access XMPS via the External Server endpoint.

DMZ Setup will require that a server be set up which has an external network connection to the Internet. The XMPS software will need to be installed on this server and configured to support the DMZ feature. The setup entails pointing the DMZ server at your XMPS server and supplying administrator credentials which will be used by the DMZ server when connecting to the XMPS server.

All DMZ configuration is done using HTTPS communication over port 443. The connection is initiated by the DMZ server, and can be trusted by the XMPS server based on the supplied administration credentials.

4.2.15.2 Mobile Devices and the DMZ Server

Mobile devices or other user interfaces may connect to the DMZ Server to access their Mobile Print Server when they are external to the company's network.

All communication between the Mobile Print App and the DMZ Server will be over HTTPS (port 443).

4.2.15.2.1 Mobile Login using a Company Code

The mobile app can be configured to prompt for a company code at logon time. When configured to do this, the app will query the Xerox Azure Service Bus to find the DMZ Server end point. After which, all communication between the mobile app and the Mobile Print Server will be directly between the mobile phone and the DMZ server. User validation of credentials and transmission of all jobs occurs between the phone and the DMZ Server.

4.2.15.2.2 Mobile Login using the Private Access Control

The mobile app can be configured with using the Private Access Control feature, such that the app points to the DMZ server for all communication. With this configuration, the mobile app never accesses the Xerox® Azure Service Bus. To perform this setup in the mobile app, Users can manually enter the link (as provided by their Mobile Print Administrator), or the Admin will have the ability to push out an email to all users which includes a link that, when selected from a Mobile device, will update the configuration of the App and make it point to the desired external URL.

4.2.16 XSM Connectivity

The Mobile Print system can be configured to connect to XSM in order to perform the following actions:

- Export Job Data (Page count, Plex, etc.)
- Import Printers, Sites and Printer/Site Mappings

Each of these methods of synchronizing with XSM has its own configuration as well as specific limitations on the system as a whole. Connectivity to XSM can only be enabled if Mobile Print has a license for “Xerox® Mobile Print - Managed Print Services”. The Importing of Prints and Sites requires the SA to configure an Account ID as well as a Username and Password. Optionally, a Chargeback Code may be specified. For the Exporting of Job Data, the Admin need only configure the Account ID. They may optionally enable the “Obscure User Data” setting, which when enabled will obfuscate all user data (e.g. User Name, Email Address, Accounting User Name before sending any data to the XSM server.

All communication between XSM and Xerox Mobile Print will be over HTTPS (port 443).

5 Roles

5.1 Customer Supplied Network

Even the most secure systems are vulnerable to someone who has the right knowledge, access, and enough time. Threats include physical damage at the system, over networks, or 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, and the use of virus detection software.

5.2 Xerox Role

Xerox will strive to provide the most secure software product possible based on the information and technologies available while maintaining the products 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.

5.3 Customer Role

Although the Mobile Print product support team will try to provide software that is secure, 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, implementing a private network, 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 Mobile Print 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.

In implementing a security strategy, customers must keep in mind that they should not modify the Mobile Print product system or its environment in any way that will prevent it from functioning properly. If the customer performs such modifications, Xerox® will not be able to support the product should problems occur. The customer may be responsible for returning the Mobile Print product back to the original installed state. This may include uninstalling unsupported software, resetting configuration settings, or possibly reinstalling the Mobile Print software product.