Software Version 4.0.2xx
Version 1.2
702P04728

Xerox® Print Management and Mobility Service

Information Assurance Disclosure

BR14700

Contents

1. 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 or by sending an email with attachments to print@printbyxerox.com, without needing drivers and cables.

1.1. Purpose

The purpose of the IAD is to disclose information for the Xerox® Print Management and Mobility Service with respect to device security. Device security, in this context, is defined as how data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. This document describes design, functions, and features of the Xerox® Print Management and Mobility Service relative to Information Assurance (IA) and the protection of customer sensitive information. Please note that the customer is responsible for the security of their network and the Xerox® Print Management and Mobility Service 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® Print Management and Mobility Service relative to Information Assurance (IA).

This document does not provide tutorial level information about security, connectivity or Xerox® Print Management and Mobility Service 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® Print Management and Mobility Service workflow; as such, some user actions are not described in detail.

1.3. Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

2. Product Description

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® Print Management and Mobility Service. 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.

2.1.1. Submission methods:

- E-mail
- Print Portal Application (i.e., an App on a mobile device)
- Desktop Print Client (upload)

2.1.2. Release methods:

- Printing device UI (via EIP)
- Print Portal Application (i.e., an App on a mobile device)
- Auto Release via Authentication
- Auto Release via Network Appliance

2.1.3. Combined Submission / Release methods

(Note: job will print without any explicit user action after submission):

- E-mail
- Print Portal App (i.e., an App on a mobile device)
- Web Portal (web browser interface to Xerox® Print Management and Mobility Service)
- Desktop Print Client (upload and print)
- Desktop Print Client (direct print)

2.1.4. Printer Authentication Methods

- Card Access (Proximity Cards, Magnetic Stripe Cards, NFC on Android)
- Alternate Login
- Print Portal Unlock

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

2.1.5. @PrintByXerox Solution

The @PrintByXerox ConnectKey App, available via the Xerox App Gallery and included as an “In-Box” App on some devices is designed to give customers an introduction to the Xerox® Print Management and Mobility Service system. Users are able to submit jobs via Email, by sending them to print@printbyxerox.com, and then release them using the @PrintByXerox App. Below is a diagram outlining the different components used as part of this workflow.

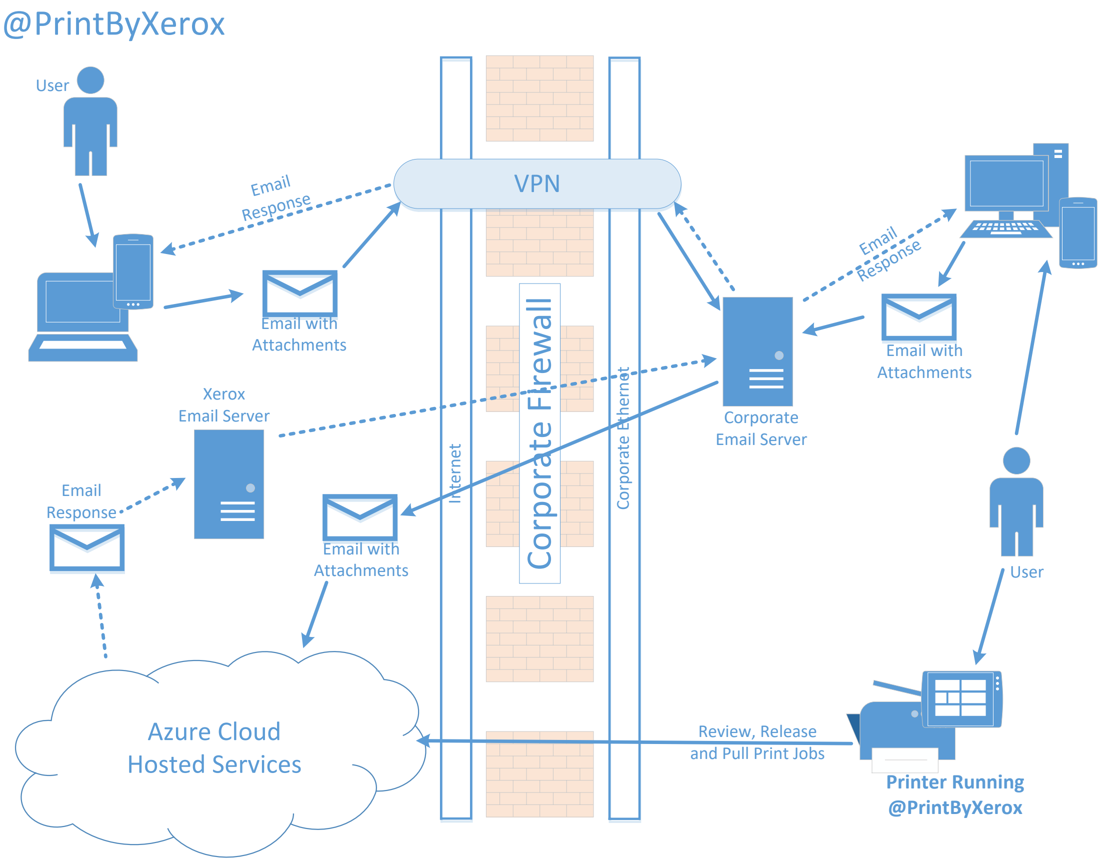

Figure 2.2.1-1: @PrintByXerox

2.1.6. Xerox® Print Management and Mobility Service

The below diagram shows the system components used for the full Xerox® Print Management and Mobility Service.

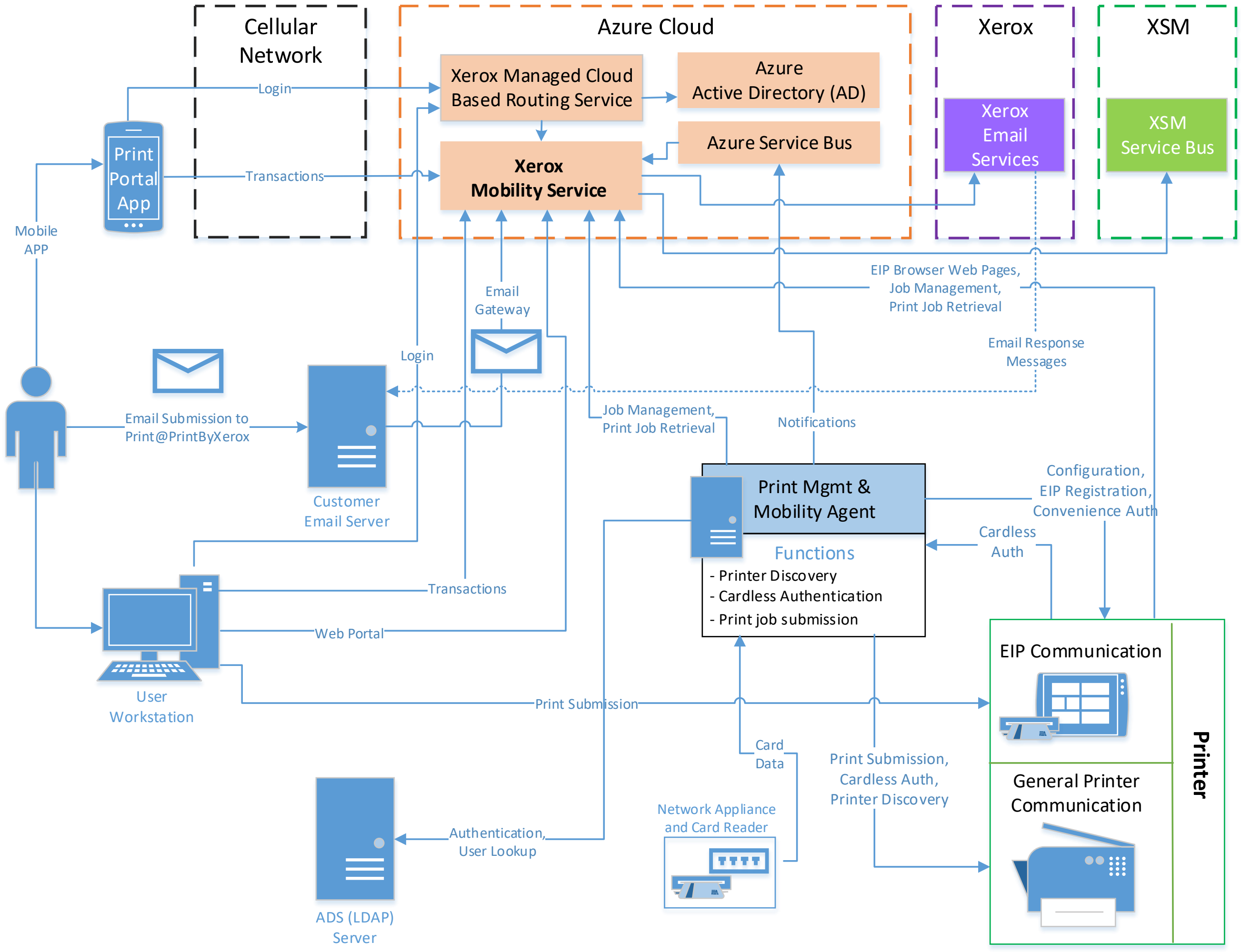
Cellular Network
Azure Cloud
Xerox
XSM
Xerox Managed Cloud Based Routing Service
Azure Active Directory (AD)
Azure Service Bus
Xerox Mobility Service
Xerox Email Services
XSM Service Bus
Login
Transactions
Print Portal App
Mobile APP
Email Gateway
Login
EIP Browser Web Pages, Job Management, Print Job Retrieval
Email Response Messages
Email Submission to Print@PrintByXerox
Customer Email Server
Job Management, Print Job Retrieval
Notifications
Print Mgmt & Mobility Agent
Functions
- Printer Discovery
- Cardless Authentication
- Print job submission
Configuration, EIP Registration, Convenience Auth
Cardless Auth
Transactions
Web Portal
User Workstation
Print Submission
EIP Communication
General Printer Communication
Printer
Card Data
Print Submission, Cardless Auth, Printer Discovery
Network Appliance and Card Reader
Authentication, User Lookup
ADS (LDAP) Server

Figure 2.2.2-1: Xerox® Print Management and Mobility Service

2.2. Description of System Components

Component	Description
User	A user of the Xerox® Print Management and Mobility Service.
Xerox® Mobile Print Portal Application	Mobile Phone application that allows the user to find printers and upload / send print jobs to Xerox® Print Management and Mobility Service.
Xerox® Print Management and Mobility Service	The Azure hosted cloud service that provides the Xerox® Print Management and Mobility Service functionality.
Customer ADS/LDAP Server	Used for user authentication.
Azure AD	[Optional] May be used for user authentication. Microsoft's Azure AD may in turn forward authentication requests to the customer's hosted AD system.
Third Party Public Print Provider	Allows print jobs to be submitted to 3rd Party Providers.
Xerox® Print Management and Mobility Agent	On premise application that runs on customer provided hardware, which supports Printer Discovery, Print transmission, and Convenience Authentication.
Server Based Print Queues	Allows print jobs to be forwarded to other 3rd Party Solutions for added job tracking, accounting, etc.
Printer	Any printing device (Xerox or Non-Xerox) that is enabled to support Xerox® Print Management and Mobility Service.
Customer Email Server	The Customer Email Server is used to get print jobs to the Xerox® Print Management and Mobility Service.
User Workstation	User's system on which the Desktop Print Client can be installed, which allows print jobs to be submitted to Xerox® Mobility Service Printers from the PC.
Xerox Email Service	Used to send email responses back to users of Xerox® Print Management and Mobility Service.
Network Appliance	External hardware device that supports card based document release at Non-Xerox or Non-EIP Devices.
XSM (Xerox Services Manager)	External Xerox application used in managed service accounts.

Table 2.3-1: System Components

3. System Architecture

3.1. Sub-Systems

3.1.1. Xerox® Print Management and Mobility Service

The Xerox® Print Management and Mobility Service consists of number of different services that run as an Azure role (Web Role or Worker Role). The type of role used depends upon the function of the service. If the service is interfacing externally via some type of API or interface, it's typically a Web Role and if the service performs internal processing, then it's typically a Worker Role. Each role runs on its own Azure VM instance, and the number of such instances will vary based on the system load. Each service is assigned a fixed size set of RAM and HDD for the given VM, which varies based on the service and its needs.

	Volatile Memory				
Type (SRAM, DRAM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
Azure storage – System Memory	Varies Based on Service	N	Executable code, temporary storage for messages processing related data, variables, state information, etc.	Y	Power Off or Exit of the Service

Table 3.1.1-1: Xerox® Print Management and Mobility Service Volatile Memory

	Non-Volatile Solid State Memory				
Type (Flash, EEPROM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
HDD	Varies Based on Service	N	Storage of binaries, libraries, graphic images, HTML pages, JavaScript pages, certs, configuration, logs, user documents, print drivers, installers, templates, job metadata	Y	Requires removal of Xerox roles

Table 3.1.1-2: Xerox® Print Management and Mobility Service Non-Volatile Memory

3.1.2. Xerox® Print Management and Mobility Agent

	Volatile Memory				
Type (SRAM, DRAM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
RAM	Customer Provided	N	Executable code, temporary storage for processing related data, variables, state information, etc.	Y	Power Off or Exit of the Service

Table 3.1.2-1: Xerox® Print Management and Mobility Agent Volatile Memory

	Non-Volatile Solid State Memory				
Type (Flash, EEPROM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
HDD	Customer Provided	N	Storage of binaries, libraries, logs, printer information	N	Removal / Un-install of the Agent. Data may be manually deleted by users with access rights to the PC on which the Agent is running. Periodic removal of some data based on time.

Table 3.1.2-2: Xerox® Print Management and Mobility Agent Non-Volatile Memory

3.1.3. Desktop Print Client

	Volatile Memory				
Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear
RAM	Customer Provided	N	Executable code, temporary storage for processing related data, variables, state information, etc.	Y	Power Off or Exit of the Service

Table 3.1.3-1: Desktop Print Client Volatile Memory

	Non-Volatile Solid State Memory				
Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear
HDD	Customer Provided	N	Storage of binaries, libraries, logs, printer information, print job data	Y	Removal / Un-install of the Client. Data may be manually deleted by users with access rights to the PC on which the Client is running. Periodic removal of some data based on time.

Table 3.1.3-2: Desktop Print Client Non-Volatile Memory

3.1.4. Print Portal Application

	Volatile Memory				
Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear
RAM	Customer Provided	N	Executable code, temporary storage for processing related data, variables, state information, etc.	Y	Power Off

Table 3.1.4-1: Print Portal Application Volatile Memory

	Non-Volatile Solid State Memory				
Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear
ROM	Customer Provided	N	Storage of binaries, libraries, printer information, print job data	Y	Removal / Un-install of the App.

Table 3.1.4-2: Print Portal Application Non-Volatile Memory

3.2. Open Source Components

Xerox® Print Management and Mobility Service does make use of Open Source software modules in its different components (e.g. the Cloud hosted Xerox® Mobility Service, the Desktop Client, etc.). An up to date bill of materials for this solution is available upon request from Xerox.

4. System Interaction

4.1. System Components

4.1.1. Xerox® Mobile Print Portal Application

The Xerox® Mobile Print Portal Application is the main user interface to the Xerox® Print Management and Mobility Service.

The application requires users to authenticate with the Xerox® Print Management and Mobility 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 Portal Application and Xerox® Print Management and Mobility Service" for more information about authentication and communications related security information).

The Xerox® Mobile Print Portal 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 webpage to change their password making the device unable to access the Xerox® Print Management and Mobility system.

4.1.2. Xerox® Print Management and Mobility Service

The Xerox® Print Management and Mobility Service runs in the Microsoft® Windows Azure Platform and utilizes the SQL Azure Database for storage. There are a number of considerations for security based on this architecture as follows:

- Windows Azure Platform specific security information
- SQL Azure Database specific security information
- Xerox® Print Management and Mobility Service specific security
- Xerox® Print Management and Mobility EIP App specific security
- Xerox® Print Management and Mobility Service Virtual Machines
- Xerox® Print Management and Mobility Web Portal
- Xerox® Print Management and Mobility Email Service

Each consideration is covered below.

4.1.2.1. 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 its own VLAN, preventing compromised node access

Please visit the following Microsoft web sites for more information:

1. Windows Azure Security Overview

   http://azure.microsoft.com/blog/2010/08/10/new-windows-azure-security-overview-white-paper-now-available/

   Select Windows Azure Security Overview.

2. Microsoft Azure Trust Center:

   https://azure.microsoft.com/en-us/support/trust-center/

4.1.2.2. SQL Azure Database Specific

The application data is stored in a SQL Azure database. This database contains information about the printers, print queues, 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 Addresses and Printer Serial Numbers are stored in an encrypted format in the database.

4.1.2.3. Xerox® Print Management and Mobility 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:

- The owner of the documents via the Xerox® Mobile Print Portal Mobile Application for preview.
- The owner of the documents via the Xerox® Mobile Print Portal Mobile Application or the Xerox® Print Management and Mobility EIP App for Print Release.
- 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, 1 day or 7 days. If set to immediate, the document is deleted immediately after printing. If the document retention policy is set to 1 or 7 days, then after printing, the document is removed after the number of configured days. Therefore, documents are stored in the system for a maximum of 7 days.

Accounting information may be stored within the Azure Storage. It is stored in an encrypted format. Accounting information that can be saved is:

- Default accounting information to be used when printing Welcome Pages to printers and print queues that require accounting information. If the administrator chooses to enter this information, it will be saved within Azure.
- User accounting information that is entered by the user when they print a job to a printer is identified with having Xerox® Network Accounting or Xerox® Standard Accounting, or a print queue that is set with server-based accounting. The administrator can configure the software to allow user accounting data to be saved. The default is to not save user accounting data.

All communications to and from the Xerox® Print Management and Mobility Service is over HTTPS using TLS (SSLv2 and v3 are not used). Documents are always transmitted securely and are protected by TLS 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. Downloads are not allowed. Only applications running within the same Windows Azure subscription can access the certificate.

4.1.2.4. Xerox® Print Management and Mobility EIP App Specific

When accessing the Xerox® Print Management and Mobility EIP App, web pages (HTML, JavaScript, icons, etc.) are served up by the Xerox® Print Management and Mobility Service. This pathway includes the ability to provide login credentials to view and manage a user's list of jobs, including print job deletion or print initiation. This pathway also includes the ability for a Xerox® Mobility Service Admin / System Administrator to manage some of the settings of the printer, including: Printer Enablement, Public Print Enablement, Site and Friendly Name.

All communications between the Xerox® Print Management and Mobility EIP App and the Xerox® Print Management and Mobility Service are over HTTPS using TLS. Certificates used for this communication path are stored in the Windows Azure Certificate store as per Microsoft guidelines.

4.1.2.5. Xerox® Print Management and Mobility Service Virtual Machines

Xerox will monitor vendor security bulletins and products 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.

4.1.2.6. Xerox® Print Management and Mobility Web Portal

4.1.2.6.1. User Access

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

Xerox® Print Management and Mobility customer account users must authenticate with the Xerox Print Management and Mobility Service to access the Web Portal. Once authenticated the user can view:

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

4.1.2.6.2. Administrator Access

All user customer administrator web pages are accessed using HTTPS over TLS from a browser.

Xerox® Print Management and Mobility customer account administrators have to authenticate with the Xerox® Print Management and Mobility 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 and the user's authentication / access card / badge number.
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® Print Management and Mobility Agents. For each printer, the administrator can view and manage the enablement for Xerox® Print Management and Mobility, as well as the enablement for Convenience Authentication and whether the printer has the Xerox® Print Management and Mobility EIP App installed.
5. The addresses of sites where printers are located.

Xerox® Print Management and Mobility 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® Print Management and Mobility 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.

4.1.2.7. Xerox® Print Management and Mobility Email Service

The Xerox® Print Management and Mobility Service hosts its own Email SMTP service in Azure. This is used to receive all incoming email transmissions. Email receipt is accepted using SMTP port 25. No credentials are needed to send email to this server. Support for encryption is available via the STARTTLS mechanism.

4.1.3. LDAP/ADS Server

The LDAP/ADS Server is part of the customer's network and is not a deliverable of Xerox® Print Management and Mobility Service. Therefore the security and maintenance of the LDAP/ADS Server is outside of the responsibility of Xerox® Print Management and Mobility Service.

When Company Authentication Type is enabled for LDAP Authentication, or Convenience Authentication is configure for LDAP when using Alternate Login or Auto Enrollment of Cards, Xerox® Print Management and Mobility will verify user credentials against Active Directory. The workplace credentials consist of Domain Name, Domain Username and Domain Password.

The Xerox® Print Management and Mobility Agent retrieves and stores a list of available active directory domains based on the context of the logged in user on the Agent computer.

4.1.4. Azure AD

The Microsoft Azure AD system is part of the Microsoft Azure backend system and is not a deliverable of Xerox® Print Management and Mobility Service. However, it is possible to configure XPMMS to use Azure AD as a user authentication mechanism. This is a company specific setting, and when enabled applies to all interfaces of XPMMS that require authentication credentials.

When using Azure AD, the user will supply their email address, which is then used to lookup which account they are in and which authentication mechanism to use for that account. In the case of Azure AD, the authentication mechanism with Azure uses OAUTH. This is an open standard, commonly used on the internet to delegate authorization decisions across a network of web enabled applications. When using OAUTH, the XPMMS system will turn control for user validation over to Azure AD. The user will actually authenticate with the Azure AD site and then delegate permission to use the XPMMS solution. The XPMMS solution never sees the user's credentials. What is returned to the XPMMS solution is the result of the authentication request as well as an Azure Authentication Token and Refresh Token. XPMMS will validate the Azure authentication token, and if valid will grant the user an XPMMS authentication token. The expiration time of the XPMMS authentication token matches that of the Azure Authentication token.

The XPPMS solution will store both the XPMMS authentication token and Azure refresh token on the specific device and interface to which the user logged in. In this case either:

- The Xerox Print Portal App on the users mobile device
- On the PC running the desktop Client

[Note: users can also log into XPMMS via the Web Portal (browser), the Agent and the Printer Client (@PrintByXerox app), however, the XPMMS Authentication Token and Azure Refresh Token are never stored in these scenarios].

If a user tries to access the given interface above and the XPMMS authentication token has expired, then the system will attempt to re-authenticate with Azure using the Azure refresh token (assuming it hasn't expired). If successful, this results in a new Azure authentication token and refresh token, which is then used to generate a new XPMMS authentication token.

The default Azure authentication token lifetime is 2 hours and the default Azure refresh token lifetime is 2 weeks. These can of course be modified through Azure by the customer, but this is outside the scope of XPMMS. The relevant point here is that the authentication token lifetime is very short, and therefore the Xerox authentication token lifetime is short. This forces the XPMMS interfaces to frequently re-validate that the user is still in valid within the Azure AD system before updating the XPMMS authentication token.

All Azure AD communication between the give XPMMS interface (Web Portal, Print Portal, Desktop Client or @PrintByXerox app) is done using HTTPS over port 443.

4.1.5. Third Party Public Print Provider

This diagram shows the flow between Xerox® Print Management and Mobility components and a third party public print provider. All communication is over HTTPS using TLS.

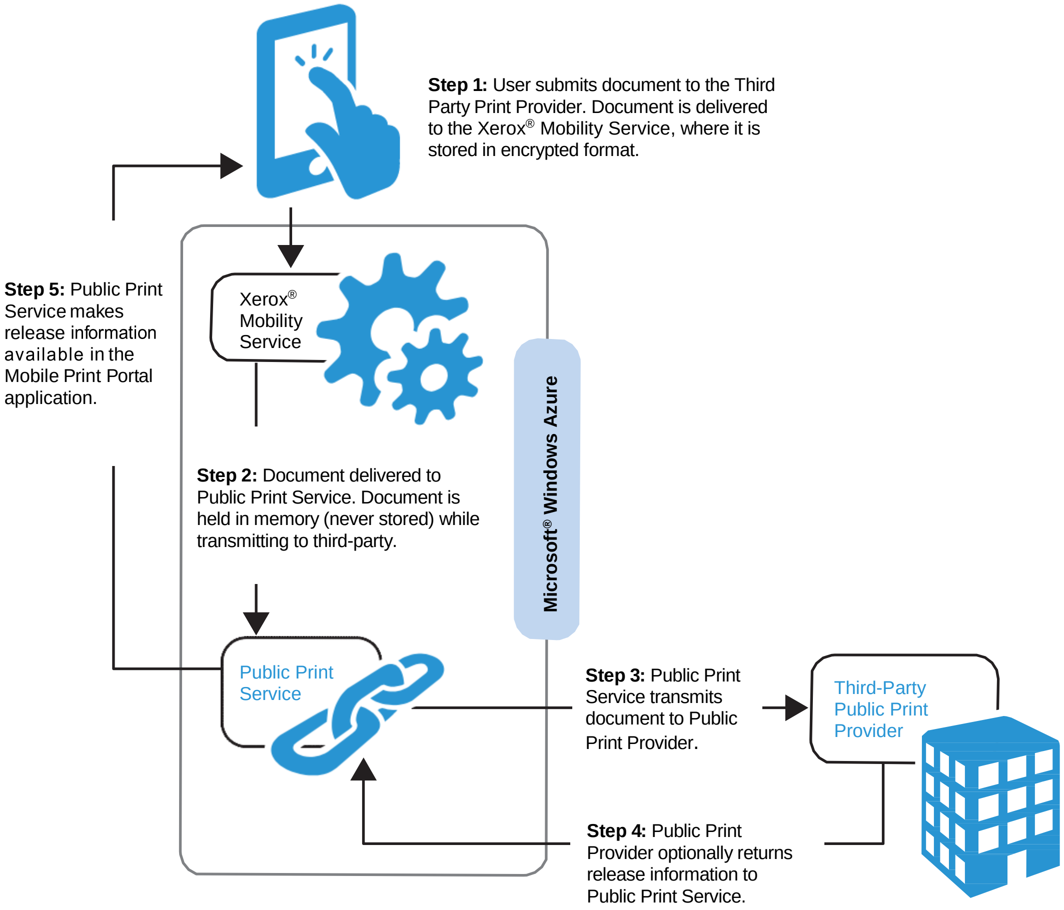
Step 1: User submits document to the Third Party Print Provider. Document is delivered to the Xerox® Mobility Service, where it is stored in encrypted format.
Step 5: Public Print Service makes release information available in the Mobile Print Portal application.
Xerox® Mobility Service
Step 2: Document delivered to Public Print Service. Document is held in memory (never stored) while transmitting to third-party.
Microsoft® Windows Azure
Public Print Service
Step 3: Public Print Service transmits document to Public Print Provider.
Third-Party Public Print Provider
Step 4: Public Print Provider optionally returns release information to Public Print Service.

Figure 4.1.4-1: Third Party Public Print Provider

Xerox® Print Management and Mobility, when configured to do so, offers the capability to a user of printing to a third party public print provider from the Xerox® Mobile Print Portal application. These third party networks provide access to printers at hotels, airport lounges and other public locations.

When printing to a third party public print provider, the user is alerted that they are sending their document outside of the Xerox® Print Management and Mobility Service. Each document printed to a third party public print provider is stored within Azure Storage. It follows a 7 day document retention policy, which is applied to the document at the time of printing. The original document is stored within Azure Storage in an encrypted format.

Access to these documents is only available to the following:

- The owner of the documents via the Xerox® Mobile Print Portal Mobile application for preview.
- 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.

Original documents printed to a third party print provider are delivered to the Xerox® Mobile Print Public Print Service, which is co-located with the Xerox® Print Management and Mobility Service in Microsoft® Windows Azure.

Original documents are transmitted from the Xerox® Mobile Print Public Print Service to the third party public print provider in a secure manner. All communications to and from the Xerox® Mobile Print Public Print Service are over HTTPS using TLS. Documents are always transmitted securely and are protected by TLS security during transmission to the third party public print provider.

The third party public print provider may respond with a release code or other information the user would need to retrieve their printed output. It is delivered securely over HTTPS. This information is available via the Xerox® Mobile Print Portal application only by the user who printed the document.

Xerox maintains the security and integrity of the document up until the point that it is transmitted to the third party. Xerox cannot assume responsibility for the security of any content of the document that is transferred.

4.1.6. Xerox® Print Management and Mobility Agent

The Xerox® Print Management and Mobility Agent has multiple functions.

1. The agent is responsible for discovering printers within the customer's network, determining the printer capabilities, and relaying that information to the Xerox® Print Management and Mobility Service.
2. The Xerox® Print Management and Mobility Agent is responsible for routing print jobs to target printers and print queues.
3. The Agent is responsible for performing any printer configuration. This includes the following feature areas:
   - Convenience Authentication – The agent will make SNMP queries and modifications to the following device settings: enable/disable for Convenience Authentication / Xerox Secure Access, Blocking Screen strings, Alternate Login, and Service Locking.
   - Xerox® Print Management and Mobility EIP App – The agent will register the Xerox Print Management and Mobility EIP App on the printer.
4. The Agent will implement the EIP Convenience Authentication API, acting as the authentication server, which allows users to authenticate their identity and unlock the printer.
5. The Agent is responsible for domain authentication lookups of users.
6. The Agent will listen for Network Appliance card data, and will release any pending jobs to the associated printer.

The Xerox® Print Management and Mobility Agent is installed on a PC. The installing user must have administrator privileges since the Xerox® Print Management and Mobility Agent software is installed as a Windows service. The Xerox® Print Management and Mobility Agent cannot be connected to the Xerox® Print Management and Mobility Service unless the Xerox® Print Management and Mobility Service has been configured to accept the agent.

The Xerox® Print Management and Mobility 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 print queues served by the agent. It allows only the proxy server address for that agent to be changed. It does not present any user or customer specific information.

If the Agent Proxy setting is configured by a user, the Agent will in turn set the system level proxy of the PC on which the Agent is running. The system level proxy settings would then be usable by other applications running on the same PC.

A local database is maintained on the Xerox® Print Management and Mobility Agent PC. This database stores printer discovery settings and printer information for each printer discovered, and print queue information as entered by the administrator. Access to the database is restricted to user's who have permission to log into the agent PC.

The Xerox® Print Management and Mobility Agent installs by default in the following location:

Program Files(x86) > Xerox > XeroxPrintManagementandMobilityServiceAgent

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.

By default, agents are set to upgrade automatically when a new version of the agent software is available. Agents connect to the Xerox® Print Management and Mobility Service and, if a newer version is available, it is automatically downloaded over HTTPS using TLS and installed. The administrator can disable this feature if desired.

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® Print Management and Mobility 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® Print Management and Mobility Service and Xerox® Print Management and Mobility Agent" and the section titled "Communication between Xerox® Print Management and Mobility Agent and Printer" for more information about authentication and communications related security information.

4.1.7. Server-Based Print Queues

For a server that hosts third party print queues used by Xerox® Print Management and Mobility, nothing special is required. To minimize security risks, leverage any security features of print control software. Incorporate standard security measures, apply security related operating system updates, use anti-virus software and add hard disk encryption.

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 should back up their data to ensure that it may be recovered in case of deletion or corruption.

4.1.8. 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.

Xerox® Secure Print allows you to control the print timing of your documents. When using Secure Print during print job submission, users enter a passcode, and then must enter the same passcode to retrieve the job at the printer.

Users may choose to use Secure Print with Secure Print enabled printers, or the administrator may configure their Xerox® Print Management and Mobility Service account to require that Secure Print be used for all jobs sent via Xerox® Print Management and Mobility Service to that printer.

Secure Print passcodes are never stored on the mobile App or in the Xerox® Print Management and Mobility Service. They are transferred securely over TLS. Passcodes are never stored externally to the job on the printer.

Passcodes are numeric and conform to the requirements of the printer model. Auto-generated passcodes are a minimum of 6 digits for all printers whose maximum is at least 6 digits.

For information on the security of a job while it is stored on the printer, refer to your printer's documentation.

Additional security can be enforced at the printer if the printer is EIP Capable and/or supports the EIP Convenience Authentication API. For those printers which support this capability, the Xerox® Print Management and Mobility Service provides the capability to lock the printer's local user interface, and require the user to authenticate themselves at the printer in order to gain access to any of the services / features of the printer. There are three ways in which a user can authenticate:

1. The user may supply their Xerox® Print Management and Mobility Service user credentials (username / password, LDAP, or Azure AD credentials depending upon the Company/Account configuration) at the printer.
2. The user can identify themselves using their access card (e.g. employee badge).
3. The user may use the Xerox® Print Portal App, by supplying the 4 character code found on the local user interface of the machine into the Print Portal App. This will identify the printer in the App and the user can confirm that they wish to unlock the device.

In each of the above scenarios, upon supplying valid credentials or making the unlock request, the printer will remove the blocking screen and the user will have access to the services / features of the printer. If the printer is an EIP capable device and the Xerox® Print Management and Mobility EIP App is installed, then the user may select the App and view their list of jobs without providing additional login credentials for the app.

In conjunction with authentication feature, Xerox® Print Management and Mobility supports a feature called Auto-Release. This feature is disabled by default, but may be enabled by the Administrator for the given account. Upon successfully completing the authentication step at a printer, if the Auto-Release feature is enabled, any print jobs uploaded to the Cloud system will automatically be released and printed at the device.

Other examples of printer security features are as follows:

- Xerox Image Overwrite electronically shreds information stored on the hard drive of devices as part of routine job processing.
- 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.
- Certificate Validation forces the printer to validate all certificates used for HTTPS communication to ensure that they originate from a trusted certificate authority.

For more information about the above examples as well as for other printer security-related technologies please see:

http://www.xerox.com/information-security/product-security

The Xerox® Print Management and Mobility 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.

4.1.9. Xerox® Print Management and Mobility EIP App

Devices which are EIP capable have the ability to support the Xerox® Print Management and Mobility EIP App. This App allows users to log into their account, view and manage their print jobs. There are two methods of adding / using the Xerox® Print Management and Mobility application with EIP:

1. ConnectKey App – sometimes referred to as a "weblet". This form of App is installed by the customer, typically a system administrator, or it may come pre-installed (in-box App).
2. Xerox® Print Management and Mobility Agent – The Agent installed the EIP App directly on the printer based on configuration settings made using the Xerox® Print Management and Mobility Web Portal.

There are 3 modes of execution for the Xerox® Print Management and Mobility EIP App. The first of which is the unlicensed mode. This mode is only supported with the ConnectKey App, and the user is limited to the basic workflow of email submission and EIP print release. When using this mode, there is no Agent installed on the customer's network. Print jobs are retrieved from the Xerox® Print Management and Mobility Service by the printer using HTTPS over TLS with port 443.

The second mode of execution for the EIP App is a licensed mode, without an Agent. This mode is only supported with the ConnectKey App. In this mode, the user has access to most of the features of Xerox® Print Management and Mobility, including use of the Print Portal App. Print jobs are retrieved from the Xerox® Print Management and Mobility Service by the printer using HTTPS over TLS with port 443.

The third mode of execution for the EIP App is the traditional Xerox® Print Management and Mobility Service environment, with a license and one or more Agents. The Agent will install EIP in this mode, using the EIP Registration API, which is done using HTTP/HTTPS. Print jobs are received via the Agent using LPR (port 515) or Raw IP (port 9100).

4.1.10. Customer Email Server

The Customer Email Server is used to get print jobs to the Xerox® Print Management and Mobility Service. It acts as a mail relay system to route jobs to the mail service hosted in Azure. The setup, maintenance, and security of the customer email server is outside the scope of Xerox® Print Management and Mobility Service.

4.1.11. User Workstation

Users may install the Xerox® Print Management and Mobility Service Desktop Client on their Windows PC. This application will install a printer on the user's PC, using the Xerox GPD as the driver, as well as install and start a background service and a sys tray utility. The background service is used to monitor for new job submissions via the installed Desktop Client and send these up to the cloud server. All communication between the Desktop Client and the Xerox® Print Management and Mobility Service hosted in Azure is done using HTTPS over port 443.

The Mobility Service Desktop Client can be downloaded and installed by the user using the Web Portal, or it may be pushed by the IT department of the customer to the end user. If installed via the Web

Portal, Xerox® Print Management and Mobility Service will create an install package for the printer based on the logged on users authentication token. This means the login token will be included in the installer. If the driver package is pushed by the IT department of the customer, then no token is included.

To use the Desktop Client, users must provide their credentials. Once validated, the user's authentication is maintained on the PC for future use. The expiration period of the authentication token is based on the license of the account, with a maximum of up to 7 days. Once the authentication token expires, the user will be re-prompted to supply their credentials.

4.1.12. Xerox Email Service

Email responses sent to the end user are handled by the Xerox Email Service. This service is hosted by Xerox (not an Azure Server). Access to this email server requires a username and password. Xerox® Print Management and Mobility Service has its own assigned credentials for this purpose. Access to this account is limited to a few key personal on the Xerox® Print Management and Mobility Service team. Email transmission is done using Exchange Web Services over port 443 (HTTPS).

4.1.13. Network Appliance

The network appliance, sometimes referred to as an ID Controller, is an external hardware device that supports the ability to plug in a USB keyboard mode card reader and transfer card information to a configured application. In this case, the Network Appliance is configured to send card data to the PrintSafe Server.

The network appliance and the Agent communicate via raw TCP sockets with proprietary data exchange based on the manufacturer of the appliance.

Elatec: The Elatec TCP Conv and TCP Conv2 use ports 7778 and 7777 respectively. The card data is sent in plain text.

RF Ideas: The RF Ideas Ethernet 241 uses port 2001. By default, the card data is not encrypted, but the option to use encryption is available.

4.1.14. XSM (Xerox Services Manager)

Xerox® Print Management and Mobility Service 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 is achieved using a special connection URL and creating a new account that is linked to XSM. The Administrator will need to provide an XSM Account ID at the time the Xerox® Mobility Service account is created. The Importing of Printers and Sites requires the SA to configure an XSM Username and Password.

All communication between XSM and Xerox® Print Management and Mobility Service will be over HTTPS (port 443).

4.2. System Component Interfaces

4.2.1. Communication between Xerox® Mobile Print Portal and Xerox Print Management and Mobility Service

The Xerox® Mobile Print Portal Mobile Application uses the HTTPS over TLS protocol for all communication with the Xerox® Print Management and Mobility Service. It establishes an HTTPS secure connection with the Xerox® Print Management and Mobility Service relying on the mobile device operating system to validate the security certificate as part of establishing the TLS connection. The security 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 (using TLS).

Once authentication is complete, data is passed between the Xerox® Mobile Print Portal Mobile Application and the Xerox® Print Management and Mobility 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 cellular (3G/4G/LTE) communications on their mobile devices.

4.2.2. Communication between Xerox Mobile Print Portal and the Customer Email Server

Emails submitted to the Xerox® Print Management and Mobility 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® Print Management and Mobility Service. It is the user's responsibility to ensure appropriate email security controls are in place.

4.2.3. Communication between the Customer Email Server and Xerox® Print Management and Mobility Service

Emails are processed and consumed immediately upon receipt by the Xerox® Print Management and Mobility service. Emails are not stored in any repository or inbox.

4.2.4. Communication between Xerox® Print Management and Mobility Service and the Xerox® Print Management and Mobility Agent

The Xerox® Print Management and Mobility Agent uses the HTTPS protocol over TLS for all communication with the Xerox® Print Management and Mobility Service. It establishes an HTTPS over TLS secure connection with the Xerox® Print Management and Mobility Service relying on the PC's operating system to validate the security certificate as part of establishing the TLS connection.

After successful installation of the Xerox® Print Management and Mobility Agent software, it will attempt to register itself with the Xerox® Print Management and Mobility Service. The Xerox® Print Management and Mobility Agent's registration process provides the Xerox Print Management and Mobility Service with the Xerox® Print Management and Mobility account's administrator credentials, the Xerox® Print Management and Mobility Agent Activation Code, and a machine hash code. The Xerox® Print Management and Mobility Service returns a Xerox® Print Management and Mobility Agent registration identifier to complete the registration process. The Xerox® Print Management and Mobility 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® Print Management and Mobility Agent, print job data is transmitted between the Xerox® Print Management and Mobility Service and the Xerox® Print Management and Mobility 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.

If the Convenience Authentication feature is enabled, the Agent will facilitate communications acting as a middleman between the printer and the Xerox Print Management and Mobility Service, receiving authentication requests from either entity and converting them to the appropriate response and passing that onto the recipient. All such communication is done using HTTPS.

4.2.5. Communication between the Xerox® Print Management and Mobility Agent and the Printer

The Xerox® Print Management and Mobility 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® Print Management and Mobility Agent will route print jobs to the target printer using either Raw Port 9100 or LPR/LPD Port 515. These ports are both configurable.

Customers can further secure the print path by enabling IPSec between their Xerox® Print Management and Mobility Agent PC and their printers provided the printers support IPSec. When configuring IPsec, ensure that the communication between the Xerox® Print Management and Mobility Agent and Xerox® Print Management and Mobility Service does not employ IPsec.

When a printer is enabled, the Agent may register the Xerox® Print Management and Mobility EIP App, or it may enable the Convenience Authentication feature based on the printer configuration settings supplied by the administrator. The EIP App will be registered using the EIP Registration API, which requires the printer's administration credentials. The Convenience Authentication feature enabled and configuration is done via SNMP using the SET Community string and administration credentials for the printer.

If the Convenience Authentication feature is enabled, the Xerox® Print Management and Mobility Agent will play a role in authenticating a user at the printer. The Agent will facilitate communications between the printer and the Xerox® Print Management and Mobility Service, receiving authentication requests from either entity and converting them to the appropriate response and passing that onto the recipient. All such communication is done using HTTPS.

The Xerox® Print Management and Mobility Agent may be enabled to support iOS Native printing. When enabled, devices running iOS may locate and send print jobs directly to the Agent. This is done using the IPP protocol using port 631. For further details on this capability, please review the Xerox® Print Management and Mobility Administration Guide.

4.2.6. Communication between the Xerox® Print Management and Mobility Agent and a 3rd Part Print Queue

Customers identify their print queues to Xerox® Print Management and Mobility Agent by providing information on the server, port and queue name.

The Xerox® Print Management and Mobility Agent will route print jobs to the print queue using LPR/LPD Port 515. This port is configurable.

Customers can further secure the print path by enabling IPSec between the Xerox® Print Management and Mobility Agent PC and the servers. When configuring IPsec, ensure that the communication between the Xerox® Print Management and Mobility Agent and Xerox® Print Management and Mobility Service does not employ IPsec.

4.2.7. Communication between the Mobility Service Desktop Client and Xerox® Print Management and Mobility Service

When a user sends a job to the Xerox® Print Management and Mobility Service using the Desktop Client, the file is converted to Postscript and stored temporarily on the hard disk of the PC. The location of the stored files is dependent upon the user:

```
C:\Users\<USERNAME>\AppData\Local\Xerox\XPMMS\VirtualPrint\Jobs
```

The Mobility Service Desktop Client runs in the background and monitors this folder for any new files. When one is detected, it then uploads the file to the Xerox® Print Management and Mobility Service using HTTPS (TLS) over port 443. After the upload completes (success or failure), the temporary file(s) are deleted from the hard disk.

4.2.8. Communication between the Mobility Service Desktop Client and the Printer

If a PC running the Desktop Client and the Printer to which a job are to be released are on the same network, the Desktop Client will send the job directly to the printer, avoiding the need to send the job to the Xerox® Print Management and Mobility Service. The Desktop Client detects that the printer is on the same network using an ICMP ping request. The print job itself will be sent via either Raw IP (Port 9100) or LPR (Port 515) to the printer based on the printer configuration.

4.2.9. Communication between the Xerox® Print Management and Mobility Agent and the Customer ADS (LDAP) Server

When Company Authentication Type is enabled for LDAP Authentication, Xerox® Print Management and Mobility will verify user credentials against Active Directory. The workplace credentials consist of Domain Name, Domain Username and Domain Password.

Workplace Credentials are not stored on the Agent computer or in the Cloud database. The Print Portal App stores the Workplace Credentials encrypted on the mobile device. Xerox® Print Management and Mobility agent will query Active Directory for available domains.

In order to communicate with Active Directory, Xerox® Print Management and Mobility uses the Active Directory Services Interfaces (ADSI) technology that is available in all Windows Operating Systems supported by Xerox® Print Management and Mobility. The communication with the Active Directory servers occurs via the standard LDAP port 389. Communication is secured via SASL bind usually using the GSSAPI mechanism.

4.2.10. Communication between the Xerox® Print Management and Mobility Service and XSM

All communication between XSM and Xerox® Mobility Service will be over HTTPS (port 443).

5. Logical access, network protocol information.

5.1. Protocols and Ports

The following table lists the standard default ports used by the Xerox® Print Management and Mobility solution. Some port numbers are configurable on the printer, such as the Raw IP printing port. Other port numbers are non-configurable and cannot be changed.

Protocol	Default Use Port Value	Use	Option	Direction
Xerox® Print Portal Application Ports:				
HTTPS using TLS	TCP 443	Authentication, Job / Printer Listing, Initiate Print Conversion	Non-configurable	App to Xerox® Print Management and Mobility Service
HTTPS using TLS	TCP 443	Authentication	Non-configurable	App to Azure AD
IPP	TCP 631	iOS Native Print Submission	Non-configurable	App to Agent
Xerox® Print Management and Mobility Agent Ports:				
HTTPS using TLS	TCP 443	Retrieval of configuration, sending printer info, retrieval of print jobs, authentication.	Non-configurable	Agent to Xerox® Print Management and Mobility Service
Raw IP	TCP 9100	Print Submission	Configurable	Agent to Printer
AMQP	TCP 80	Azure Service Bus (with application level encryption)	Non-configurable	Agent to Xerox® Print Management and Mobility Service
LPR	TCP 515	Print Submission	Configurable	Agent to Printer
LDAP	TCP 389	Authentication	Non-configurable	Agent to ADS Server
HTTPS using TLS	TCP 443	Convenience Authentication, EIP Registration	Non-configurable	Agent to Printer
HTTPS using TLS	TCP 443	Authentication	Non-configurable	Agent to Azure AD

Protocol	Default Use Port Value	Use	Option	Direction
SNMP	TCP 161	Printer Discovery, Configuration	Non-configurable	Agent to Printer
Print@PrintByXerox EIP App Ports:				
HTTPS using TLS	TCP 15043	EIP Single Sign On	Non-configurable	Printer to Agent
HTTPS using TLS	TCP 443	Retrieval of EIP Browser pages for display on the UI. Authentication, Job Listing, Initiate Print Conversion	Non-configurable	Printer EIP App to Xerox® Print Management and Mobility Service
HTTPS using TLS	TCP 443	Authentication	Non-configurable	Printer EIP App to Azure AD
Printer Ports:				
HTTPS using TLS	TCP 443	Initiate Pull Print Request	Non-configurable	Printer to Xerox® Print Management and Mobility Service
HTTPS using TLS	TCP 15042	Convenience Authentication	Non-configurable	Printer to Agent
Desktop Client Ports:				
HTTPS using TLS	TCP 443	Printer Configuration, Driver Download, Print Submission	Non-configurable	Desktop Client to Xerox® Print Management and Mobility Service
HTTPS using TLS	TCP 443	Authentication	Non-configurable	Desktop Client to Azure AD
Ping	ICMP Echo	Test if printer is on the local network.	Non-configurable	Desktop Client to Printer
Xerox® Print Management and Mobility Service Ports:				
SMTP	TCP 25	Receive Email Submissions	Non-configurable	Listening port for incoming email submissions

Protocol	Default Use Port Value	Use	Option	Direction
HTTPS using TLS	TCP 443	Exchange Web Services. Used to send email responses end users.	Non-configurable	Xerox® Print Management and Mobility Service to Xerox Email Service
HTTPS using TLS	TCP 443	Send Print History and Retrieve Printer List to/from XSM.	Non-configurable	Xerox® Print Management and Mobility Service to XSM
HTTPS using TLS	TCP 443	Azure AD Authentication token validation	Non-configurable	Xerox® Print Management and Mobility Service to Azure AD
HTTP	TCP 80	Used by the traffic manage to determine which Azure sites are available.	Non-configurable	Azure Traffic Manager to Xerox® Print Management and Mobility Service
Network Appliance Ports:				
Raw	TCP 7778	Receive Card Swipe Data from Elatec TCPConv	Configurable	Network Appliance to Agent
Raw	TCP 7777	Receive Card Swipe Data from Elatec TCPConv2	Configurable	Network Appliance to Agent
Raw	TCP 2001	Receive Card Swipe Data from RFIdeas Ethernet 241	Configurable	Network Appliance to Agent

Table 5.1-1: Protocols and Ports

Firewall Rules

The following table lists the standard firewall rules used by the Xerox® Print Management and Mobility solution. It is expected that the administrator will modify the firewall rules of the PC running the Agent if these features are being used at the customer site.

Protocol	Default Use Port Value	Use
HTTPS	TCP 15042	Authentication
HTTPS	TCP 15403	EIP Single Sign On
Raw	TCP 7778	Receive Card Swipe Data from Elatec TCPConv
Raw	TCP 7777	Receive Card Swipe Data from Elatec TCPConv2
Raw	TCP 2001	Receive Card Swipe Data from RFIdeas Ethernet 241

Table 5.2-1: Firewall Rules

6. System access

6.1. Xerox® Print Management and Mobility Service (Web Portal)

When accessing the Xerox® Print Management and Mobility Service directly (i.e. the Web Portal for either general user access or administrative access), the user will connect to:

https://XPMMS.services.xerox.com/Login

Users will need to provide their email address. Xerox® Print Management and Mobility Service will look up the user's email address to determine the company account to which they are homed, and then based on that company's authentication configuration, they will be prompted to enter either their Xerox® Print Management and Mobility Service password, their company LDAP credentials (DOMAIN\USERNAME and PASSWORD), or their Azure AD credentials. When using LDAP, the Domain will be used to route the LDAP requests to the correct Agent, which in turn will communicate with the ADS/LDAP server.

Credentials (either the Xerox® Mobility Service Password, the LDAP credentials or the Azure credentials) are never saved in the browser. In addition, the user's browser session will timeout after 20 minutes of inactivity.

6.2. Xerox® Print Management and Mobility Service Agent

When the Agent is initially installed, the company's Xerox® Print Management and Mobility Service administrator must provide their credentials (Mobility Service, LDAP or Azure AD) and Company Code so that the App can communicate with the Xerox® Print Management and Mobility Service and register the Agent with their account. Subsequent communication to Xerox® Print Management and Mobility Service will used computed access credentials for the Agent based on the hardware of the workstation on which the Agent is running. The Administrator credentials are not stored or used after the initial registration occurs.

6.3. Xerox® Mobile Print Portal Application

When accessing the Xerox® Mobile Print Portal App, users will need to provide their email address. Xerox® Print Management and Mobility Service will look up the user's email address to determine the company account to which they are homed, and then based on that company's authentication configuration, they will be prompted to enter their Xerox® Print Management and Mobility Service password, their company LDAP credentials (DOMAIN\USERNAME and PASSWORD), or their Azure AD credentials. When using LDAP, the Domain will be used to route the LDAP requests to the correct Agent, which in turn will communicate with the ADS/LDAP server.

The results of successfully authenticating with Xerox® Print Management and Mobility Service is an access token. The token is stored on the phone and used for subsequent communication with Xerox® Print Management and Mobility Service. The lifetime of the access token is 24 hours. Prior to the token expiring, the phone will obtain a new token, which requires the use of the user's login credentials. So the Print Portal App will store the user's access credentials on the phone in encrypted format in order to support renewing the access token. For Android devices, the credentials are encrypted and saved to internal storage of mobile device and this is only accessible by the Print Portal application. For iOS devices, the credentials are saved in a keychain which is encrypted and only accessible by the Print Portal application. The OS of the mobile device will delete any saved data including the credentials when the application gets un-installed.

6.4. Desktop Client

When installing the Desktop Client, users will need to provide their email address. Xerox® Print Management and Mobility Service will look up the user's email address to determine the company account to which they are homed, and then based on that company's authentication configuration, they will be prompted to enter their Xerox® Print Management and Mobility Service password, their company LDAP credentials (DOMAIN\USERNAME and PASSWORD), or their Azure AD credentials. When using LDAP, the Domain will be used to route the LDAP requests to the correct Agent, which in turn will communicate with the ADS/LDAP server.

The results of successfully authenticating with Xerox® Print Management and Mobility Service is an access token. The token is stored on the user's workstation and used for subsequent communication with Xerox® Print Management and Mobility Service. The lifetime of the access token is either 24 hours or 7 days based on licensing. Once the access token is expired, the user will be prompted to re-supply their authentication credentials, after which a new access token will be created.

6.5. Print@PrintByXerox EIP App

To access the Print@PrintByXerox EIP App, users will either need to log into the printer via the Convenience Authentication feature, or they will need to log into the EIP App itself. User will start by providing their email address. Xerox® Print Management and Mobility Service will look up the user's email address to determine the company account to which they are homed, and then based on that company's authentication configuration, they will be prompted to enter their Xerox® Print Management and Mobility Service password, their company LDAP credentials (DOMAIN\USERNAME and PASSWORD), or their Azure AD credentials. When using LDAP, the Domain will be used to route the LDAP requests to the correct Agent, which in turn will communicate with the ADS/LDAP server.

The Print@PrintByXerox App will never save the user's credentials. The can log out of the EIP App manually, but selecting the "Exit" button in the App, or by navigating out of the App (e.g. selecting the All Services, Machine Status, or Job Status buttons on the UI panel). The UI itself has a built in inactivity timer that will log the user out if the user is not interacting with the UI. The inactivity period is configurable by the device administrator. In addition to the device timer, the EIP App itself has its own 5 minute timer. The EIP App timeout will log the user out of the App after 5 minutes of use, unless they dismiss warning pop-up, which restarts the 5 minute timer.

7. Additional Security Items

7.1. Xerox® Print Management and Mobility Service Endpoint Table

The following endpoints, given in FQDN format, are accessed by various components of the Xerox® Print Management and Mobility Service solution that reside inside a customer's network. The customer must ensure that these components have access to the internet, and in particular these specific endpoints, in order for this solution to work properly. All endpoints are accessed via HTTPS using TLS (port 443).

Component	Endpoint FQDN
Xerox® Print Management and Mobility Agent	• https://xpmms.services.xerox.com • https://xmpcws.services.xerox.com • https://xcpagentservicebus.servicebus.windows.net • https://xcpagentservicebus01.servicebus.windows.net • https://xcpagentservicebus02.servicebus.windows.net • https://xcpagentservicebus03.servicebus.windows.net : • https://xcpagentservicebus10.servicebus.windows.net • (Azure AD only) https://login.microsoftonline.com
Xerox® Print Management and Mobility EIP App – Printer App	• https://xmpceip.services.xerox.com • https://xccsts.services.xerox.com • https://xmpcws.services.xerox.com • (Azure AD only) https://login.microsoftonline.com
Xerox® Mobile Print Portal – Mobile App	• https://xccsts.services.xerox.com • https://xmpcws.services.xerox.com • https://publicprintapi.services.xerox.com • (Azure AD only) https://login.microsoftonline.com
Xerox® Print Management and Mobility – Customer Web Pages	• https://xpmms.services.xerox.com • (Azure AD only) https://login.microsoftonline.com
Xerox® Print Management and Mobility – Desktop Client	• https://xccsts.services.xerox.com • https://xmpcws.services.xerox.com • https://xpmms.services.xerox.com • (Azure AD only) https://login.microsoftonline.com

Table 7.1-1: Cloud Endpoints

7.2. Certificate Validation

Xerox® Print Management and Mobility Service is a cloud hosted service, available to anyone that has internet access. In order to ensure that users are connecting to a known trusted entity, the cloud hosted service in Azure uses a digital certificate created by a well-known and trusted certificate authority.

7.2.1. Connection Details

Below are details on the different access methods users have available to them when connecting to the Xerox® Print Management and Mobility Service as related to certificate validation.

Web Portal

Well-known browsers which are up to date (version and security patches) such as Internet Explorer, Chrome, Firefox, Edge, Safari, include the public keys for most of the well-known certificate authorities (CA) used on the internet. This includes the CA used to generate the Xerox® Print Management and Mobility Service root certificate. As such, these browsers will test and validate the Xerox® Print Management and Mobility Service server certificate when a connection is made to the Xerox® Print Management and Mobility Service Web Portal. No special setup or configuration is needed from the user to take advantage of this capability.

Print Portal

Similar to the browser on a PC, both Android and iOS include the public keys for most of the well-known certificate authorities used on the internet. These public keys are available to applications running on the mobile phone. The Xerox® Print Portal Application is designed such that it always validates the server certificate for all communication with the Xerox® Print Management and Mobility Service. If this validation fails, the Print Portal App will prevent any further communication with Xerox® Print Management and Mobility Service and therefore prevent the user from using the App.

@PrintByXerox App

Most of the newer Xerox devices that support EIP have the capability to perform certificate validation. By default, these devices have validation turned off. It is recommended that the user enable this capability on the printer. If the @PrintByXerox EIP App has been loaded via the Xerox App Gallery or App Studio, or the App is pre-installed on the MFP, then the public root certificate is included with App and will be used when validation is enabled. If the @PrintByXerox EIP App has been loaded via the Agent, then no public root certificate will be programmatically pushed to the printer. The user will need to obtain the public root cert for the following site:

https://XPMMS.services.xerox.com/Login

Once the cert is available, it will need to be imported into the trusted root certs of each printer where the @PrintByXerox App is installed.

[Note: Not all Xerox capable EIP printers support certificate validation.]

7.3. Auto Release via Network Appliance Workflow

Held print jobs are released automatically as soon as the user scans a card at a mapped network appliance associated with the printer.

Network appliances are small network boxes that attach to the network and permit Xerox® Print Management and Mobility to control the release of user documents to printers that do not support the use of Xerox Secure Access / Convenience Authentication. A network appliance is configured on the network by the administrator, the appliance is associated with the particular printer in the Xerox® Print Management and Mobility Service Admin Web Portal, and the user can release their jobs at the printer by swiping their card using the card reader associated with the printer. One network appliance is required for each printer.

7.3.1. Models

Three network appliance models are supported by Xerox® Print Management and Mobility Service: RF Ideas Ethernet 241

- Elatec TCP Conv2
- Elatec TCP Conv

Each of these models is available by default on the Web Portal administration site at *Account* > *Settings* > *Network Appliances* > *Models*. If any or all of these models are not going to be part of your site installation, they can be disabled to turn the listeners off on the server.

The listeners use these default ports:

- RF Ideas Ethernet 241 - 2001
- Elatec TCP Conv2 - 7777
- Elatec TCP Conv - 7778

The default ports can be changed by the administrator if the network appliances on your system have been configured to use a different port. Any firewall on the Agent must be configured to allow communication through the port(s).

By default, the network appliances support communication using non-encrypted channels. Therefore, card data is sent in plain text format when transmitting the card data from the network appliance to the Agent. The RF Ideas Ethernet 241 is the only network appliance that supports encryption (using SSL) of the communication path.

Note: The Ethernet 241 supports SSLv3. It does not support TLS1.x.

7.4. Audit Log

The Xerox® Print Management and Mobility Service will maintain a history of the users that have logged in Xerox® Print Management and Mobility Service via any of the interfaces: Print Portal, Web Portal, @PrintByXerox, or Convenience Authentication. Entries are maintained for a period of 1 year. Entries older than that are purged from the log.