Software Version 4.0.2xx
Version 1.1
September 2017
702P04855

Xerox® Print Management and Mobility Suite

Information Assurance Disclosure

Document Version: 1.0

BR14700

[This page intentionally left blank.]

Contents

1. Introduction

Xerox® Print Management and Mobility Suite is a workflow solution that connects a corporation mobile workforce to new productive ways of printing, and controls user access to Xerox Multifunction Printers (MFP). Printing is easy and convenient from any mobile device without needing standard drivers and cables. This solution also supports Desktop Printing, allowing printing to a common queue with the ability to release jobs to any printer. This reduces waste from uncollected jobs and provides security for sensitive information, since jobs are only printed when the user is standing at the printer.

1.1. Purpose

The purpose of the IAD is to disclose information for the Xerox Print Management and Mobility Suite 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 Suite 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 Suite 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 Mobility Suite relative to Information Assurance (IA).

This document does not provide tutorial level information about security, connectivity or Xerox Print Management and Mobility Suite 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 Mobility Suite 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 Xerox Print Management and Mobility Suite provides two primary workflows:

- PrintSafe Workflow
- Mobile Print Workflow

2.1.1. PrintSafe Workflow

There are two parts to the PrintSafe workflow: Printer Authentication and Desktop Printing and Release.

2.1.1.1. Authentication

Defined as customers who require validation of user access to MFPs before device usage is allowed at the "All Services" screen. Card-based is the most widely used authentication method. User name and PIN-based login at the device is an alternate method of login when card readers are not installed, or are not functional. Authentication as a standalone option provides device security access only, for the customer who does not require print jobs associated with their network login.

2.1.1.2. Desktop Printing

The Mobility Suite supports the Desktop Print / Release feature using two print server models. One is a traditional printer server model, where jobs are printed to a network print queue and held there until the user authenticates themselves at a printer and releases their job(s). The other is a server "light" printer model, where jobs will be held / retained on the user's client PC, until the issuer identifies themselves at a printer and releases their jobs, at which time the jobs are sent from the user's PC directly to the printer.

2.1.2. Mobile Print Workflow

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 Suite. 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.

2.1.2.1. Submission methods:

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

2.1.2.2. Release methods:

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

2.1.2.3. 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)

2.2. Diagram

The below diagram shows a couple of example system component / architecture diagrams for different sized customers using the Mobility Suite for both the PrintSafe and Mobile Print Workflows. These diagrams and their components will be discussed in greater detail in the following sections of this document.

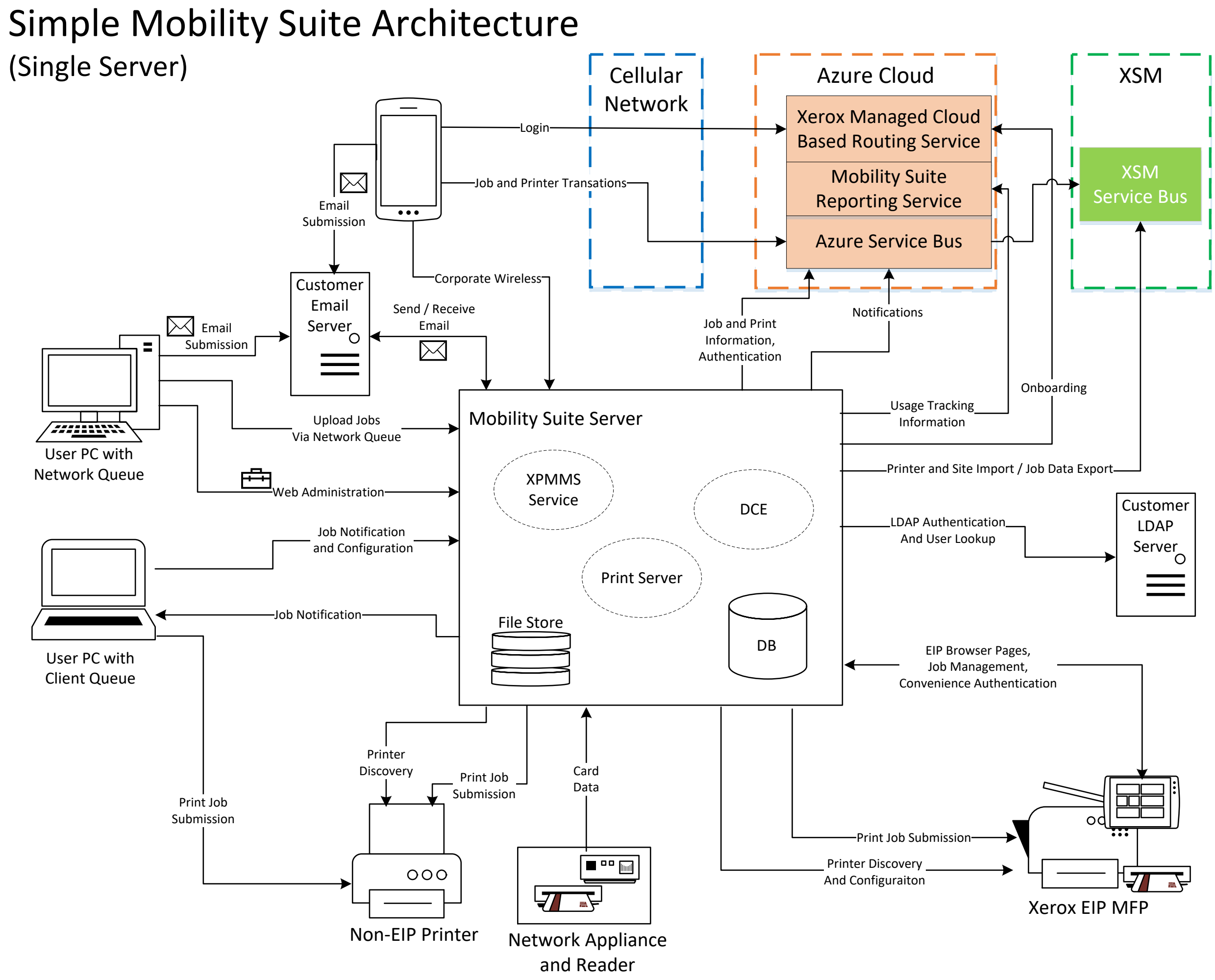
Simple Mobility Suite Architecture
(Single Server)
Cellular Network
Azure Cloud
Xerox Managed Cloud Based Routing Service
Mobility Suite Reporting Service
Azure Service Bus
XSM
XSM Service Bus
Login
Job and Printer Transations
Email Submission
Corporate Wireless
Customer Email Server
Send / Receive Email
Email Submission
User PC with Network Queue
Upload Jobs Via Network Queue
Web Administration
Job and Print Information, Authentication
Notifications
Usage Tracking Information
Onboarding
Printer and Site Import / Job Data Export
Mobility Suite Server
XPMMS Service
DCE
Print Server
File Store
DB
LDAP Authentication And User Lookup
Customer LDAP Server
Job Notification and Configuration
Job Notification
User PC with Client Queue
EIP Browser Pages, Job Management, Convenience Authentication
Print Job Submission
Printer Discovery
Print Job Submission
Card Data
Print Job Submission
Printer Discovery And Configuraiton
Non-EIP Printer
Network Appliance and Reader
Xerox EIP MFP

Figure 2.2-1: Simple Mobility Suite Components

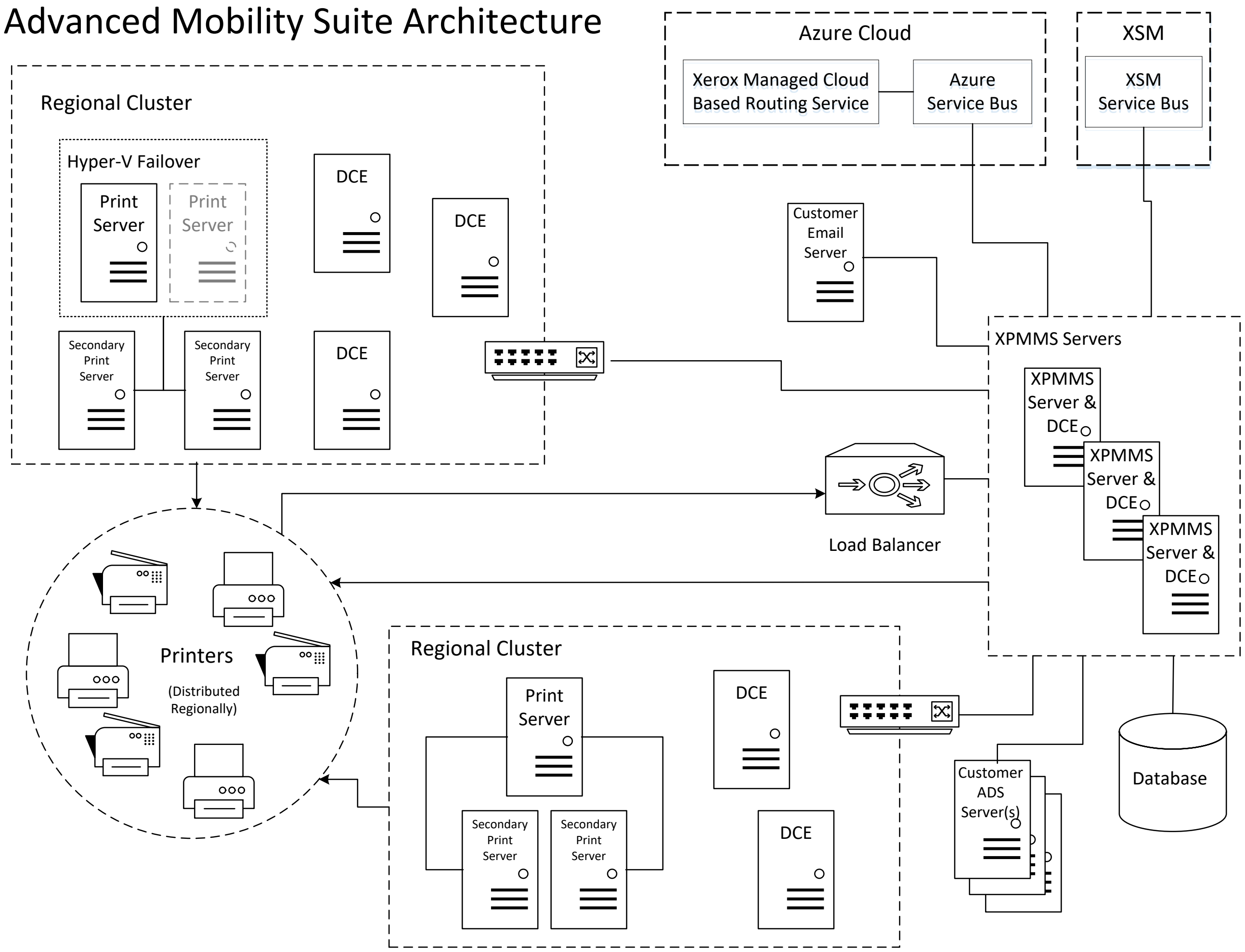

Figure 2.2-2: Advanced Mobility Suite Architecture

2.3. Description of System Components

Component	Description
User	A user of the XPMMS system.
Xerox Print Management and Mobility Server	On premise application that runs on customer provided hardware, which supports Printer Discovery, Printer Management, Print Routing, EIP Web Page Host, Administration Host, and Convenience Authentication.
Xerox® Mobile Print Portal Application	Mobile Phone application that allows the user to find printers and upload / send print jobs to XPMMS.
Xerox Cloud Azure Services	Xerox Services hosted on Microsoft Azure that support Mobile Phone authentication, printer discovery and print submission.
Customer ADS/LDAP Server	Used for user authentication.
Print Server with Network Queues	Windows PC hosting Shared Network Print Queues running the Xerox Job Agent Service. Handles job routing, notifying the XPMMS of new jobs, parses jobs, modifies job for selected attributes, and transmits jobs to the printer on release.
Document Conversion Engine (DCE)	Converts mobile jobs to print ready format upon release and transmits jobs to the printer.
SQL Database	Storage of XPMMS configuration, user info, job info, job history.
File Storage	Storage of print jobs.
Printer	Any printing device (Xerox or Non-Xerox) that is enabled to support XPMMS.
Customer Email Server	The Customer Email Server is used to get print jobs to the Xerox Print Management and Mobility Suite.
User PC with Network Queue and/or Client Queue	User's system on which the Virtual Print Driver can be installed, which allows print jobs to be submitted to Cloud Printers from the PC.
Xerox Email Service	Used to send email responses back to users of XPMMS.
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.
Mobility Suite Reporting Service	Collects usage information used to improve future performance and functionality of the solution.

Table 2.3-1: System Components

3. System Architecture

3.1. Sub-Systems

3.1.1. Xerox Print Management and Mobility Suite Server

The Xerox Print Management and Mobility Suite Server is the primary server for this Xerox solution. It is responsible for handling administration and configuration of the system, orchestration of all components and services, performing authentication and serving EIP browser pages, performing usage tracking and job management. XPMMS runs on a Windows based server or PC.

Volatile Memory					
Type (SRAM, DRAM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear:**
RAM	Varies Based on Customer System	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 Suite Volatile Memory

Non-Volatile Memory					
Type (Flash, EEPROM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear:**
HDD	Varies Based on Customer System	Y	Storage of binaries, libraries, graphic images, HTML pages, JavaScript pages, certs, configuration, logs, user documents, print drivers, installers, templates, job metadata	Y	Requires uninstall of software and then manual removal of remaining files (e.g. logs and database file)

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

3.1.2. Print Server running Xerox Job Agent Service

Print Servers for XPMMS are Windows Servers running the Xerox Job Agent Service (XJAS). Print Server can run as standalone systems, separate from the XPMMS main server, or the XJAS can run on the same system as the XPMMS server software. The XJAS is responsible for accepting incoming jobs, storing them to the designated location, parsing jobs to detect user and accounting information as well as job attributes, notifying the XPMMS system of the job, updating job attributes and transmitting released jobs to the printer.

Volatile Memory					
Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear:
RAM	Varies Based on Customer System	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: Print Server and Xerox Job Agent 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 Customer System	Y	Storage job and related info, configuration, logs.	Y	Removal / Un-install of the XJAC. Manual removal of some files after uninstall is required (e.g. job information).

Table 3.1.2-2: Print Server and Xerox Job Agent Service Non-Volatile Memory

3.1.3. Document Conversion Engine

Volatile Memory					
Type (SRAM, DRAM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear:**
RAM	Varies Based on Customer System	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: Document Conversion Engine 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 Customer System	N	Storage of binaries, libraries, logs, printer information, print job data.	Y	Removal / Un-install of the DCE. Manual removal of some files after uninstall is required (e.g. job information).

Table 3.1.3-2: Document Conversion Engine Non-Volatile Memory

3.1.4. Client PC running Xerox Job Agent Client

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

Table 3.1.4-1: Client PC and Xerox Job Agent 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 / SSD	Varies Based on Customer System	N	Storage of binaries, libraries, printer information, print job data	Y	Removal / Un-install of the DCE. Manual removal of some files after uninstall is required (e.g. job information).

Table 3.1.4-2: Client PC and Xerox Job Agent Client Non-Volatile Memory

3.2. Open Source Components

Xerox Print Management and Mobility Suite does make use of Open Source software modules in its different components (e.g. the Mobility Suite Server, DCE, XJAS/XJACK, 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® Print Management and Mobility Suite Server

The Xerox® Print Management and Mobile Suite Server is the foundational component of the Xerox® Mobile Suite Solution, used to manage the system's behavior and user's interaction within the system from authentication, document submission, and printing. The Xerox® Mobile Suite Server (XMSS) is a Windows® application running on a Windows® Server. XMSS 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.

Users authenticate themselves at a printer using the XMSS. In addition, user's documents are received and either stored for secure release or directly printed at a printer. The Xerox® Mobility Suite Server will monitor and work in conjunction with the available Conversion Servers for document conversion and print processing, as well as the Xerox Job Agent Clients and Print Servers on receiving and releasing desktop print jobs.

There are a number of sub-functions of the Xerox Mobility Suite Server, which are discussed in greater details below:

4.1.1.1. Administration Services:

The XMSS administration services provide configuration, user, printer and job management.

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 features. Connection to the Administration Services is supported via HTTP (port 80) or HTTPS (port 443). By default the Mobility Suite 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 certificate authority on the Xerox Mobility Suite Server.

Accessing the Mobility Suite Admin webpage uses the standard browser based NTLM protocol for web authentication. This access protocol requires a user name and password for client authentication and is supported by most browsers.

During installation of the Xerox® Mobility Suite Software, the 'MPAdmin' user group is created. Windows user accounts that are members of the 'Administrator' and / or 'MPAdmin' groups on the Mobility Suite Server have access to the Admin webpage, but not to user accounts.

4.1.1.2. User Portal Services:

The XMSS User Portal provides the ability for a user to manage settings and configuration specific to themselves. At this time, this is limited to being able to view and manage Release

Permissions for the Printer Client (EIP App). Refer to section "*7.5 – Printer Client Release Permissions*" for further details on this feature.

Users interact with the User Portal via a web browser interface. Connection to the User Portal is supported via HTTPS (port 443). By default the Mobility Suite 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 certificate authority on the Xerox Mobility Suite Server.

Refer to section "*6.5 – User Portal*" for details on how to access and log into the User Portal.

4.1.1.3. Mobile Print Workflow Details:

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

However, the system 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 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 Mobility Suite 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 Third Party Print Queues in addition to printers. Sending documents to a Third Party Print Queue is equivalent to the print command in the Mobile Print Workflow. 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 the Mobility Suite will be sent to the default print queue and immediately deleted from the system.

4.1.1.4. PrintSafe Workflow Details:

By default, the PrintSafe Workflow supports auto-registration. If the customer site uses LDAP or Domain controllers, then auto-registration allows the user to can scan their badge via a connected USB card reader at a PrintSafe-enabled printer. The user would then provide their LDAP authentication credentials to validate their identity, resulting in the addition of that user and their relevant LDAP information (name, email, network user name) in the Mobility Suite user database. If auto-registration is not used, there are other options to create and manage users, including: Manual Updates, CSV Import, and LDAP Import.

All submitted jobs are stored and referenced based on the user's network user name and email address. The user's jobs are stored in the print server's Windows file system, or on the client with a randomized file name.

Unprinted jobs are deleted based on an administrator configured retention period. The default retention period is one day.

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 Suite Server. Once authenticated, the user's credentials and authentication token are stored in the application until they log out.

The Mobility Suite 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. This includes PrintSafe Workflow jobs as well. 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 Mobility Suite 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 Mobility Suite Server, the result of which is a "company code." The Mobility Suite administrator must distribute this code to authorized users. [**Note**: An administrator may request a new company code at any time.]
2. During initial log-in a user must enter their email address and company code.
3. The Mobility Suite system will generate a confirmation code and will send the confirmation number to the user at the supplied email address.
4. The user must then enter the confirmation code into the Mobile Print Portal Application.

The Mobile Print Workflow 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® Print Management and Mobility Service (Cloud Hosted) itself.

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® Mobility Suite Server, and the standard Bonjour ports must be opened on the server's firewall. The Xerox® Mobility Suite Server responds to mDNS queries and advertises itself as a printer, thereby allowing Print Portal Application users to submit print jobs to Mobility Suite using iOS native printing. Alternatively, the IT administration at a customer site can configure their DNS servers to advertise the Xerox® Mobility Suite Server as a printer. This allows client applications such as Print Portal Application to use DNS-SD (service discovery), to discover the Mobility Suite Server as a printer. Regardless of the type of discovery method, once found, the Print Portal Application can submit (upload) jobs to the Xerox® Mobility Suite Server using IPP (port 631).

Jobs are then available for release using the Print Portal Application to a printer, or the Printer Client (EIP) Application.

There is a version of the Print Portal Application that supports Google Chromebooks as well as an extension to the Google Chrome browser. When run in these environments, the Print Portal app supports "single sign-on" using your Google credentials to validate the user in place of manually entering credentials.

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 Mobility Suite 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 security 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. Document Conversion Servers

The Xerox® Mobility Suite is modular in design, leveraging a core Mobility Suite Server component as well as one or more additional Mobile Print Workflow components referred to as Conversion Servers. 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® Mobility Suite Server, or it may reside on a separate server. Only one Conversion Server may reside on any given 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 process, the print ready document is stored in the configured Content Storage location, which could be local to the DCE or a shared network resources (e.g. RAID system). Any temporary files created during the conversion process are deleted from the Conversion Server disk and memory after storing the print ready document.

The print ready file will be deleted from the system once the original is deleted.

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 Mobility Suite 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 Job Agent Service / PrintSafe Client

The Xerox® PrintSafe Workflow is modular in design, leveraging the core Mobility Suite Server, as well as one or more additional components referred to as the Job Agent Service and the PrintSafe Client. The Job Agent Service runs on the print server and is included as part of the install of the Xerox® Mobility Suite Software. For customers who want to use an external print server, they can install the Job Agent Service on one or more external servers to create a distributed or regional system of print servers. For environments that want to forego a traditional print server, they can instead install the PrintSafe Client on each user's workstation.

4.1.5.1. Job Agent Service

The Job Agent Service is a Windows service installed on a print server used in conjunction with the Xerox® Mobility Suite software with the PrintSafe Workflow license. The service can run on the same server running the Xerox® Mobility Suite, or it can run on one or more external print servers. When installed on an external server, the Job Agent Service starts a listening service and waits for the Mobility Suite Server to enable it to perform job management. The Xerox® Mobility Suite administrator must add the print server IP Address to the list of print servers, effectively enabling the Job Agent Service to begin communicating with the Mobility Suite Server. The messaging between the Mobility Suite Server and PrintSafe Client consists of:

- Reporting of available printers (Queues)
- Enablement of printers (Queues)
- Job Information – Reporting of new jobs and their details
- Notification of job release to an enabled printer
- Results of job transfer to a printer
- Periodic job synchronization

4.1.5.2. PrintSafe Client

The PrintSafe Client is a Windows service installed on a client workstation used in conjunction with Xerox® Mobility Suite Software with the PrintSafe Workflow license. When installed a user workstation, the PrintSafe Client must be pointed to the Mobility Suite Server via the inclusion of a configuration file or via a Service Registry setting which can be pushed to the workstation by the customer IT organization. The PrintSafe Client is responsible for managing print queues and print jobs on the client workstation. The messaging between the Mobility Suite Server and PrintSafe Client consists of:

- Querying the server for configuration (e.g., polling intervals, timeouts, etc.)
- Querying the server for the list of printers (Queues)
- Installing or removing printers (Queues)
- Job Information – Reporting of new jobs and their details
- Polling or notification for job release to an enabled printer
- Reporting of job transfer to a printer
- Periodic job synchronization

4.1.6. Document Storage

4.1.6.1. Mobile Print Workflow

Documents are stored unencrypted in the Xerox Mobility Suite Server. The documents are stored in a configurable location†, which can be any location to which the Xerox® Mobility Suite Server has access. 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:

- The user deletes them via the Print Client App at the device UI or the Print Portal App.
- The Xerox® Mobility Suite 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 Suite Web Administration UI does provide the ability to delete documents if needed.

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

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

4.1.6.2. PrintSafe Workflow

All printers (queues) configured for the PrintSafe Workflow use the Mobility Suite Port Monitor. Part of the Windows print path, this monitor accepts a print ready file (e.g., Postscript of PCL) and writes it to disk. The location where the file is written is configured using the Mobility Suite Web Admin tool. The print ready file and some descriptor files are temporarily stored on the print server or client workstation system disk while the files are active. Upon release to a printer, the Job Agent Service or Client removes the associated files.

As with any Microsoft server OS, the deleted documents follow traditional MS 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 Xerox® PrintSafe Software provides no facilities to erase the documents.

4.1.7. Xerox® Mobility Suite Database

Microsoft SQL CE 4 database is used by Xerox® Mobility Suite as the default relational data store. However, XMS can be configured to work with an external Microsoft SQL database. In order to create this database, the user who installs Xerox® Mobility Suite must have permissions to create databases and database logins, and grant permissions. During the installation, Xerox® Mobility Suite grants the system account “Domain\ComputerName$”, the rights to update the created database.

4.1.8. LDAP/ADS Server

The Xerox Mobility Suite Server retrieves and stores a list of available active directory domains based on the context of the domain to which the XMMS server belongs. The administrator may also manually add domains if desired. The administrator may then enable or disable domains which can be used for authentication and user import.

4.1.8.1. LDAP Authentication

The LDAP/ADS Server is part of the customer’s network and is not a deliverable of the Xerox Mobility Suite. Therefore the security and maintenance of the LDAP/ADS Server is outside of the responsibility of XMMS.

When the Authentication Type for the Print Portal App or the EIP Printer Client App is enabled for LDAP Authentication, or Convenience Authentication is configure for LDAP when using Alternate Login or Auto Enrollment of Cards, the Mobility Suite Server will verify user credentials against Active Directory. The workplace credentials consist of Domain Name, Domain Username and Domain Password. The Mobility Suite Server performs an LDAP login using the supplied credentials. Passwords are never stored. By default, the system uses SASL when doing an LDAP bind.

In order to communicate with Active Directory, Xerox® Mobility Suite uses the Active Directory Services Interfaces (ADSI) technology available in all Windows operating systems supported by Xerox® Mobility Suite. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if TLS is being used.

4.1.8.2. LDAP Import

Xerox® Mobility Suite can be configured to import users from Active Directory. This capability is an extension of the setup used for LDAP/ADS Authentication. The administrator 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 instructs the Mobility Suite Server to use SASL when doing an LDAP bind.

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

As part of the import, the administrator can define the LDAP containers that are queried as part of the import and map the fields within those contains to fields within the Mobility Suite user database.

As part of the import, the administrator may configure the type of LDAP records that they wish to import: Additions (new LDAP records), Modifications (updated LDAP records) or Deletions (users that have been removed or marked as deleted in LDAP). As part of the “Deletions” option, the administrator may configure an LDAP Filter specific to each LDAP server to be used when looking for deleted records to be removed from the XPMMS database.

In order to communicate with Active Directory, Xerox® Mobility Suite uses the Active Directory Services Interfaces (ADSI) technology available in all Windows operating systems supported by Xerox® Mobility Suite. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if TLS is being used.

4.1.9. 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.

4.1.9.1. Secure Print

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 system to require that Secure Print be used for all jobs sent via the Mobile Print Workflow to that printer.

Secure Print passcodes are never stored on the mobile App or in the Mobility Suite Server. 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.

4.1.9.2. Printer Authentication

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® Mobility Suite uses this platform to secure access to the printer.

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 Suite 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 themselves:

1. The user may supply their Xerox Mobility Suite user credentials (username / password or LDAP 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 Print Client 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, the Xerox Mobility Suite supports a feature called Auto-Release. This feature is disabled by default, but may be enabled by the Administrator. Upon successfully completing the authentication step at a printer, if the Auto-Release feature is enabled, any print jobs uploaded to the system will automatically be released and printed at the device.

4.1.9.3. Xerox Mobility Suite: Printer Client App

Devices which are EIP capable have the ability to support the Xerox Mobility Suite Printer Client App. This App allows users to identify themselves, view and manage their print jobs.

The Mobility Suite Server will install the EIP App on the printer using the EIP Registration API, which is done using HTTP/HTTPS. Communication between the EIP App and the Mobility Suite Server is done using HTTP over port 80 or HTTPS over port 443. If Alternate Login is configured for LDAP or Auto Registration is enabled, then the communication of the app will be encrypted (HTTPS over 443). Otherwise the App will using HTTP over port 80.

4.1.9.4. 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. The Xerox Mobility Suite uses this platform to secure access and present users with the Xerox® Mobility Suite solution for the Mobile Print Workflow. [The PrintSafe Workflow does not support Apeos].

4.1.10. Customer Email Server(s)

The email server is used to receive emails from and send emails to users of the Mobility Suite solution. 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 into the Xerox® Mobility Suite infrastructure. The user's documents will temporarily reside on your mail server until the email message and its attachments are retrieved by the Xerox® Mobility Suite Server.

The Xerox Mobility Suite administrator will need to configure both the incoming mail server as well as the outgoing mail server. Both connections require credentials (e.g. username / password) to access the mail servers. The setup, maintenance, and security of the customer email server is outside the scope of Xerox Mobility Suite.

4.1.11. 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.

4.1.12. XSM

The Xerox® Mobile Suite 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® Mobility Suite has a license for "Xerox® Mobility Suite - Managed Print Services."

4.1.12.1. Export Jobs to XSM

Only the account ID is needed in order to export jobs to XSM. 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 and User Name

NUp
- This only applies when printing using the FX Apeos workflow

Job ID

Job Type

Copies

Page Count B/W

Page Count Color

Total Page Count

Plex

Submission Date Time

Completed Date Time

Content Size

Color
- If the document contains color

Duplex

Document Name

Document Type
- If the document is Word, PPT, etc.

Media Size

Printer Name

Printer MAC Address

Server Name
- Always Mobility Suite Server Name

Server MAC Address
- Always Mobility Suite Server MAC address

PDL Type

Fax Destination Number

Fax Duration

Scan Recipient Description

Scan Recipient Type

Device Job Completion Time

4.1.12.2. Import Printers / Sites from XSM

When the Xerox Mobile Suite is configured to import printers and sites from XSM, then XSM is treated as the source of record. As such, the administrator has several limitations on what can be modified 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, Xerox Mobility Suite will perform an SNMP discovery to add the printers to the printer list. If the discovery fails, printers will not be added to the system.

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 Xerox Mobility Suite.

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

4.2. System Component Interfaces

4.2.1. 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 than 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 email domain.

The Mobility Suite 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 Mobility Suite 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.

4.2.2. Mobile Print Portal App and Xerox Mobility Suite Service

In order for a smart device application, running on a service provider's 3G/4G/LTE network to "talk" to a server behind a corporate firewall, an intermediate cloud-based service is used. Xerox uses the Microsoft Azure Service Bus Relay to create this cloud endpoint between the mobile device and the Mobility Suite Service.

The HTTPS protocol is used for all communications between the Mobile Print Portal Application, the Xerox® managed cloud based routing service, and the Mobility Suite Service. 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 TLS connection. Likewise, the Xerox® managed cloud based routing service relies on the Mobility Suite Service to validate the security certificate as part of establishing a TLS connection.

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

If using the Chromebook or Chrome browser Print Portal extension with the single sign-on feature, when a user attempts to log in, the app will pre-populate the email field with the logged on users email address. When this is submitted to the server, the app will also include the Google authentication token of the logged on user as well as the AppID of the Print Portal App. The server will validate the email, token and AppID with Google using HTTPS over port 443. If these are valid, the user is considered authenticated. The server then creates a Mobile Print authentication token and returns that to the Print Portal App. The user then remains logged into the App until the Mobile Print token expires. At this time, the app will attempt to repeat the process.

Once authentication is complete, data is passed directly between the Mobile Print Portal App and the Mobility Suite Server or from outside the corporate network by routing through the Azure Service Bus Relay. 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 Mobility Suite Server. All communication between the mobile phone and the DMZ server, as well as the DMZ server and the Mobility Suite 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® Mobility Suite Server). When iOS Native Printing is enabled, the Mobility Suite 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 Mobility Suite Server.

4.2.3. Customer Email Server and Xerox Mobility Suite Service Communication

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

For security:

- The Mobility Suite 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 TLS.

The Mobility Suite Server 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® Mobility Suite Server supports connectivity to the following:

- SMTP (port 25 or 587),

- IMAP (143 or 993 (TLS)) and
- POP (110 or 995 (TLS))
- Microsoft Exchange Web Services (80 or 443 (TLS))
- Lotus Domino NRPC (Port 1352)

Using the protocols above, the Mobility Suite 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. Mobility Suite 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 XMSS communicates using a local API with Lotus Notes Client installed on the same PC as XMSS, which in turn uses Note RPC to communicate with the Domino server.

The Mobility Suite Server 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, the Mobility Suite will Log On as the impersonated user for the duration of the EWS connection. The impersonated user must have Log On credentials to the Mobility Suite system.

4.2.4. Mobility Suite Server and Printer Communication

The Mobility Suite Server communicates with the Printer for a number of different reasons using various protocols. These are outlined below:

4.2.4.1. Discovery

Discovery applies to all printers that are enabled to work with Xerox® Mobility Suite. The Mobility Suite Server connects to the printer via SNMP (Port 161) to retrieve printer configuration, capabilities, paper tray information (paper size and availability). The SNMP communication is done either via SNMPv1/v2 (no encryption) or SNMPv3 (encryption) using port 161.

4.2.4.2. Printer Client (EIP App)

The Mobility Suite connects to the printer's web services to install the Printer Client EIP/Apeos application on Xerox® printers via port 80 (HTTP) or 443 (HTTPS) based on the configuration of the printer. The Server will also make use of the EIP Session API and Device Configuration APIs using these same ports.

The Mobility Suite 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.

Based on the configuration of the system, users may need to identify themselves using the Printer Client. This done by entering their confirmation number, primary PIN, 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. The primary PIN is always displayed.

4.2.4.3. Print Authentication

Authentication is only supported by Xerox® multifunction devices that support the EIP Convenience Authentication API.

The server configures the authentication feature on the printer via SNMP (Port 161). The SNMP communication is done via SNMPv1/v2 (no encryption) or SNMPv3 (encryption).

During user authentication, the PrintSafe Server and the printer communicate using web service calls to initiate an authentication session, supply card data, and / or prompt the user to supply credentials or other data, and unlock the device for user access. All data exchanged is over port 443 via HTTPS.

4.2.5. Administrator configuration and of the Mobility Suite Server

Accessing the Mobility Suite 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 Mobility Suite Server would have access, but not user accounts.

4.2.6. Document Conversion Server and Mobility Suite Service Communication

The Mobility Suite service will send the user’s Mobile Print Workflow documents to the Document 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 Mobility Suite Service and the Conversion Server(s) are on separate machines, they communicate via TCP/IP over ports 8801 and 8802.

4.2.7. Document Conversion Server and the Printer

The Conversion Server which hosts the Document Conversion Engine (whether running on the same server as the Mobility Suite Service or on a separate server) is responsible for submitting the converted Mobile Print job to the printer. The default submission method for Mobile Jobs is Port 9100 over TCP/IP. Other ports that can be used are 2501, 2000, 515 (LPR), and 443 (IPP over TLS).

4.2.8. User Workstation and Print Server Communication

The user workstation communicates with the print server in two ways:

- Print queue and driver install
- Print submission

Print queue install can be initiated via the PrintSafe Client, or via the Windows print install wizard if print queues are added manually. Printing is done via traditional shared Windows network printers. These capabilities use DCE/RPC communication over port 1058 and SMB communication via port 445.

4.2.9. Job Agent Service/Client and Xerox Mobility Suite Server Communication

The Job Agent runs either on the users workstation (Xerox Job Agent Client as part of the PrintSafe Client) or on a Print Server (Xerox Job Agent Service).

4.2.9.1. Job Agent Service Start Up

When the Job Agent Service is first installed, the software listens on port 8800 using HTTP for initial configuration information from the Mobility Suite Server. Once the administrator adds the IP address of the external print server to its list of supported servers, the Mobility Suite Server will push the communication endpoint to the Job Agent Service. This endpoint is used for all communication between the Job Agent Service and the Mobility Suite Server.

4.2.9.2. Xerox Job Agent Client Configuration

The PrintSafe Client periodically polls the Mobility Suite Server using the configure endpoint with HTTP on port 8800. This includes the retrieval of timers for job polling, configuration polling, and maintenance polling. Optionally, the PrintSafe Client can also be configure to listen for message notification being sent from the Mobility Suite Server. This lessens the amount of network traffic generated using the PrintSafe Client. When running in the messaging mode, the Xerox Job Agent Client will listen on port 9807 using UDP by default. If this port is not available, the client will try 3 other ports to find one that is not in use, by adding 10 each time (e.g. 9807, 9817, 9827 and 9837). If the client fails to obtain a port, then it will default to using polling when querying for pending jobs.

4.2.9.3. Job Management

Both the PrintSafe Client and the Job Agent Service communicate with the Mobility Suite Server to communicate new jobs being added to the system, to know when jobs are to be released, to update job status, and job synchronization. This is done via web service calls using HTTP over port 8800. The Job Agent Service listens for notifications from the server about jobs to be released. The PrintSafe Client either polls for this information or if messaging is enabled it listens on port 8800. The reporting of new jobs and job status is always initiated by the PrintSafe Client. For the Job Agent Service, communication is two-way.

4.2.9.4. Primary Print Server and Secondary Print Server

In the event that a customer has configured the use of 1 or more Secondary Print Servers to be used in conjunction with a Primary Print Server, the servers will communicate together using port 8800 and HTTP for the purpose of facilitating workload distribution.

4.2.10. Job Agent Service and Printer Communication

When a job is released for printing, the Job Agent Service / Client submits a print ready file to the printer. The default submission method is Port 515 (LPR). Port 9100 over TCP/IP can also be used.

4.2.11. External Communication between Xerox Mobility Suite Service and Xerox Azure Services

Except for incoming email, by default Xerox Mobility Suite 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.

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 Xerox Mobility Suite continues to be controlled by the local Mobility Suite solution.

4.2.11.1. XMS and the Windows Azure Service Bus

During the provisioning process at set-up time an external URL is provisioned on the service bus then Xerox Mobility Suite is configured to facilitate communication through that URL using an encrypted key. XMS initiates and maintains a connection to Azure service bus over HTTPS to XMS services so that users using their mobile device over a public cellular or Internet connection can use the Mobile Print Workflow. 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 XMS 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 XMS endpoint is used for the remainder of the mobile print session. The routing service determines the XMS 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 XMS 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. Xerox Mobility Suite and LDAP / Active Directory Communication

4.2.12.1. LDAP / Active Directory Authentication

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

In order to communicate with Active Directory, Mobility Suite uses the Active Directory Services Interfaces (ADSI) technology that is available in all Windows Operating Systems supported by Mobility Suite. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if TLS is being used. Communication is secured via SASL bind using the GSSAPI mechanism.

4.2.12.2. Active Directory Import

Xerox Mobility Suite can be configured to import users from Active Directory. This capability is an extension of the setup used for LDAP / ADS Authentication. The 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 Mobility Suite 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 Mobility Suite Server database (SQL), and will be encrypted using DES with MD5 hashing.

As part of the import, the 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 Mobility Suite User Database.

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

4.2.12.3. Active Directory On-Boarding using Email

When a new user sends an email, Mobility Suite 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, Mobility Suite populates the user database with the data found in Active Directory.

4.2.13. Communication between the Xerox Mobility Service and XSM

The Mobility Suite 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 Mobility Suite has a license for “Managed Print Services”. The Importing of Printers 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 Mobility Suite will be over HTTPS (port 443).

4.2.14. Communication between the Xerox® Mobility Suite Server and the Mobility Suite Reporting Service in Azure

The Mobility Suite Server will collect system usage information on a daily basis and report this to the Mobility Suite Reporting Service, an online Xerox service. The type of information being collected includes, but is not limited to, items such as:

- Version of Mobility Suite Software
- Type of SQL Database
- Associated Licenses
- Printer Details:
  - Number of Printers
  - Features that are enabled (Mobile Print, Authentication, Desktop Print, Printer Client, etc)
  - Xerox vs Non-Xerox
- Server Details
  - Operating System
  - Size of Memory
  - 32 vs 64 Bit
  - Microsoft Office: Installed, Activation State, Version
- Print Queues:
  - Number and Type (Outgoing, Incoming, Client, Network, Conversion Mode)
- Prints:
  - Number Succeeded, Failed, Deleted or Expired.
  - Release Mechanism: Email, Printer Client, Mobile App, Auto Release.
  - Print Job Summary: Number of Color Pages, Number Black & White Pages.
  - Document Types: Word, Excel, Power Point, etc.

Information is used to improve Xerox customer support as well as the performance and functionality of the product in future releases. No personal or customer sensitive information is collected.

This feature is enabled by default, but may be disabled by the customer if desired. This setting resides on the following page: *Company > Maintenance > System Health Dashboard > System Utilization.*

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 Suite. 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.

Application Protocol	Transport and Port Value	Use	Option	Direction
Xerox Print Portal Application Ports:				
HTTPS using TLS	TCP 443	Authentication, Job / Printer Listing, Initiate Print	Non-configurable	App to XPMMS
Xerox Print Management and Mobility Service:				
DCE	TCP 8801,	XPMMS and DCE Communication	Configurable	XPMMS to DCE
HTTP	TCP 8800	XPMMS uses this port to communicate with other XPMMS servers. XJAS and XJAC also request info using this port.	Configurable	XPMMS / XJAS / XJAC to XPMMS
Raw	UDP9807	XPMMS uses this port to notify XJAC that a job is ready to be released	Non-configurable	XPMMS to XJAC
SQL	TCP 1433	Microsoft SQL Client to Server Communication for database queries and storing.	Non-configurable	XPMMS to SQL Server
LDAP	TCP 389	Authentication, User Look-up	Non-configurable	XPMMS to ADS Server
LDAP with SSL	TCP 636	Authentication, User Look-up. This service does not support a TLS configuration.	Configurable	XPMMS to LDAP Server
HTTPS using TLS	TCP 443	Convenience Authentication, EIP	Non-configurable	XPMMS to Printer
SNMP	TCP 161	Printer Discovery, Configuration	Non-configurable	XPMMS to Printer
HTTPS using TLS	TCP 443	Send Print History and Retrieve Printer List to/from XSM.	Non-configurable	XPMMS to XSM

Application Protocol	Transport and Port Value	Use	Option	Direction
HTTPS using TLS	TCP 443	Send system utilitization information to the Mobility Suite Reporting Service	Non-configurable	XPMMS to MSRS
SMTP	TCP 25	Sending email responses	Non-configurable	XPMMS to SMTP Server
SMTP/TLS (Secure SMTP)	TCP 465	SMTP over TLS. TCP port 465 is reserved by common industry practice for secure SMTP communication using the TLS protocol.	Configurable	XPMMS to SMTP Server
POP3	TCP 110	Post Office Protocol version 3, enables “standards- based” clients such as Outlook to access	Configurable	XPMMS to POP3 Server
POP3/TLS	TCP 995	POP3 over TLS uses TCP port 995 to receive encrypted email	Configurable	XPMMS to POP3 Server
Exchange Web Services	TCP 443	Exchange Web Services used for receiving Email	Configurable	XPMMS to Exchange
IMAP	TCP 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	XPMMS to IMAP Server
IMAP/TLS	TCP 993	IMAP4 over TLS for securely receiving encrypted email messages.	Configurable	XPMMS to IMAP Server
NRPC	TCP 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	XPMMS (running Lotus Notes) to Domino Server
HTTP / HTTPS	TCP 80 / TCP 443	Administration using Web Admin Tool. If a certificate is already configured on the IIS default website it will be used by Xerox® Mobility Suite. If no	Non-configurable	Browser to Mobility Suite Service

Application Protocol	Transport and Port Value	Use	Option	Direction
		certificate is configured, Xerox® Mobilty Suite will create a self-signed cert. The administrator has the option to load a certificate from a trusted authority later if desired.		
HTTPS	TCP 8443	HTTP over TLS. Used to activate or validate a license. If the customer is using off-line activation, then this port is not needed.	Non-configurable	Mobility Suite Service to Xerox Licensing Server
IPP	TCP 631	Receipt of Mobile Jobs on phones using the iOS Native Print feature. Always uses TLS.	Non-configurable	Mobile Phone to XPMMS
HTTPS	TCP 443	HTTP over TLS. Used to validate a Chrome browser or Chromebook single sign-on user with Google.	Non-configurable	XPMMS to Google
Document Conversion Engine Server Ports:				
AppSocket RAW or Windows TCP-Mon	TCP 9100	Print Submission	Non-configurable	DCE to Printer
LPR	TCP 515	Print Submission	Non-configurable	DCE to Printer
IPP over TLS	TCP 443	Print Submission. Encrypted print transfer.	Non-configurable	DCE to Printer
DCE	TCP 8801, 8802	XPMMS and DCE Communication	Configurable	XPMMS to DCE
Print Server Ports:				
SMB Print	TCP 445	Print submission to a network queue. Client Workstation to print server.	Non-configurable	Workstation to Print Server
DCE/RPC	TCP 1058	Network Print Queue Access and Driver Download. From Workstation Print Queue to Print Server or from	Non-configurable	Workstation to Print Server

Application Protocol	Transport and Port Value	Use	Option	Direction
		PrintSafe Client to Print Server.		
Print Client (EIP App) Ports:				
HTTP / HTTPS	TCP 80 / 443	Retrieval of EIP Browser pages for display on the UI. Authentication, Job Listing	Non-configurable	Printer EIP App to XPMMS Service
Xerox Job Agent Service Ports:				
Raw IP	TCP 9100	Print Submission	Configurable	XJAS to Printer
LPR	TCP 515	Print Submission	Configurable	XJAS to Printer
HTTP	TCP 8800	Configuration, Job Information, Print Release	Configurable	XPMMS to XJAS
Xerox Job Agent Client Ports:				
Raw IP	TCP 9100	Print Submission	Configurable	XJAC to Printer
LPR	TCP 515	Print Submission	Configurable	XJAC to Printer
DCE/RPC	TCP 1058	Network Print Queue Access and Driver Download. From PrintSafe Client to Print Server.	Non-configurable	PrintSafe Client to Print Server
HTTP	TCP 8800	Configuration, Job Information, Print Release	Configurable	XJAC to XPMMS
Raw	UDP 9807	Notification of Print Job Release	Configurable	XPMMS to XJAC
Network Appliance Ports:				
Raw	TCP 7778	Receive Card Swipe Data from Elatec TCPConv	Configurable	Network Appliance to XPMMS
Raw	TCP 7777	Receive Card Swipe Data from Elatec TCPConv2	Configurable	Network Appliance to XPMMS
Raw	TCP 2001	Receive Card Swipe Data from RFIdeas Ethernet 241	Configurable	Network Appliance to XPMMS
iOS Native Printing Ports:				
DNS-SD	UDP 53	Mobile Phone printer discovery using DNS.	Not-configurable	Phone to DNS Server

Application Protocol	Transport and Port Value	Use	Option	Direction
mDNS	UDP 5353	Mobile Phone printer discovery on the local subnet using mDNS.	Not-configurable	Phone Broadcast on Local Subnet
IPP	TCP 631	IPP Print submission to Xerox® Mobility Suite. Always uses TLS.	Not-configurable	Phone to XPMMS

Table 5.1-1: Protocols and 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.

6. System access

6.1. Xerox Print Management and Mobility Suite (Web Administration Portal)

When accessing the Xerox Print Management and Mobility Suite directly (i.e. the Web Portal for administrative access), the administrator will connect to:

http://<webserver address>/MobilitySuiteAdmin/

[Note: HTTPS may also be used if desired.]

The user must provide either Administrator credentials or they must be a member of the MPAdmin Group as defined on the server upon which Xerox Mobility Suite is running (Workplace or Local credentials) or on the Domain Controller.

6.2. Xerox Mobile Print Portal Application

When accessing the Xerox Mobile Print Portal App, users will need to provide their email address. XPMMS 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 Suite Confirmation Number, or their company LDAP credentials (DOMAIN\USERNAME and PASSWORD). 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 XPMMS is an access token. The token is stored on the phone and used for subsequent communication with XPMMS. The lifetime of the access token configurable. 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.

6.3. PrintSafe Client

The PrintSafe Client will need to access the enabled client based queues hosted on the Print Server(s) in order to download and install the print driver for each client queue. By default, the PrintSafe Client runs as an NT Service on the workstation and uses the Local System Account when attempting to connect to the Print Server hosting the client queue. If these credentials are not valid, the user may supply different credentials using the Sys Tray utility installed with the PrintSafe Client. The supplied credentials will then be used by the PrintSafe Client NT Service when accessing the Print Server queues to retrieve the driver.

Print jobs submitted via the PrintSafe Client will always use the network username of the person logged into the workstation as the job owner.

6.4. Printer Client (EIP App)

To access the Printer Client App, users will either need to log into the printer via the Convenience Authentication feature and then select the Printer Client App, or they will need to log into the EIP App itself. The Mobility Suite administrator also has the option of allowing an external authentication mechanism (something other than the Mobility Suite itself) as an approved authentication service. So a user can authenticate themselves at the printer with the external service, and if they then select the

Mobility Suite Printer Client App, the App will pull the logged on users credentials from the session (network username and email address) and if these values map to a user in the Mobility Suite database, then the user will have access to their print job(s) for release at the device. [Note: the ability to use an external authentication mechanism is off by default].

The Printer Client (EIP App) will never save the user's credentials. The user 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.

6.5. User Portal

When accessing the User Portal, users will connect to:

https://<webserver address>/Login

The user must exist in the XPMMS user database, and the user record must be enabled and not locked out. The administrator can configure the type of authentication that will be required to access the User Portal. The supported methods include:

- Disabled (access is not allowed)
- Email and Primary PIN
- Email and Confirmation Number
- LDAP Authentication

The only setting or configuration available to the user using the User Portal is the configuration of Release Permissions for the Printer Client.

The user will be logged out of the User Portal after 5 minutes of inactivity.

7. Additional Security Items

7.1. 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 XPMMS 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.

7.1.1. Models

Three network appliance models are supported by XPMMS:

- RF Ideas Ethernet 241
- Elatec TCP Conv2
- Elatec TCP Conv

Each of these models is available by default on the Mobility Suite Admin webpage 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.

7.2. Audit Log

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

7.3. DMZ Configuration

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

Xerox Mobility Suite 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.

7.3.1.1. DMZ Setup

In order to enable the DMZ feature, the Mobility Suite Server must be set to "Private" mode. When inside of your company firewall, Mobile App users will be access XMS via the Internal Server endpoint. When outside of the firewall, Mobile App users will access XMS 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 XMS 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 XMS server and supplying administrator credentials which will be used by the DMZ server when connecting to the XMS 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 XMS server based on the supplied administration credentials.

7.3.1.2. Mobile Devices and the DMZ Server

Mobile devices or other user interfaces may connect to the DMZ Server to access their Mobility Suite 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).

7.3.1.2.1. 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 Mobility Suite 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.

7.3.1.2.2. 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 Mobility Suite 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.

7.4. Debug Logs

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

7.5. Mobility Suite Server Windows File Structure

The Mobility Suite Server stores files in the install location: %ProgramData%\Xerox\XMP

7.6. Smartcard (CAC/PIV) Integration

The Mobility Suite solution may be used with external authentication mechanisms, including CAC/PIV card authentication. Many Xerox advanced office products support smartcard integration, which is built into the Xerox Multi-Function device (MFD) itself. Smartcard authentication is not performed directly within Xerox Mobility Suite. Instead, the authentication of the user is performed between the printer, the smartcard and the Domain Controller at the customer site. The Xerox Mobility Suite can be configured to allow users authenticated by an external system (i.e. something external to Mobility Suite) to access the printer client (EIP App) using the logged on user identity. This removes the need for the user log into the Mobility Suite Printer Client. Users will see their list of jobs after starting the app and may select and release them as desired.

The Mobility Suite server must be configured to allow the logged on user (using an external authentication mechanism) to access the Printer Client. This is done using the following settings from the Web Admin Tool:

Company > Policies > Security > Printer Client

- Enable “Logged on Users (Access Card)

- Enable “External Printer Authentication”.

The Mobility Suite server must also be configured such that the “Alternate Access Card User” field for each user in the User database is populated. Typically, this field is populated from LDAP using the UPN (universalprinciplename) field. In a typical customer environment using this capability, a user logged onto the Printer would normally have an identifier something like:

username@domain (UPN)

When that same user submits jobs from their PC, the user identity is typically has a format of:

DOMAIN\username

Enhancements to the Xerox Mobiliy Suite server, will allow the matching of the UPN value to the DOMAIN\username value, so that the user may be presented with their list of jobs and release them from the Printer Client (EIP App).

7.7. Printer Client Release Permissions

The Printer Client (or EIP App) provides an interface on some Xerox devices to view and release the user’s printer jobs. This includes both Mobile Print jobs and PrintSafe Desktop submitted jobs. By default, only the user that submitted a job will be allowed to view and manage their jobs. However, the

Xerox Mobility Suite system allows users to grant access permission to other users in the system to view and manage their jobs. This feature is available when the User Portal interface has been enabled.

Company > Policies > Security > User Portal

Once enabled, users may log into the web portal:

https://<server>/login

After logging into the web portal, users have access to the Permission tab, allowing them to both view the list of users which have granted them permission to access their print jobs using the “Print Theirs” tab. They may also grant permission to other user users to access their print jobs. Details on this functionality can be found in the administration guide for this solution.

Release permissions are only supported via the Printer Client. This configuration does not impact any other interface (e.g. Print Portal). User’s can always view the list of users that have been granted release permission to their documents and they may revoke that ability at any time.

To help distinguish who is releasing a job versus who originally sent it, the job history (Jobs > History) and reports (Reports > Job Reporting) summary have been updated for the CSV export capability to include “Printed By Email” and “Print By User Name” fields. These fields will be populated with corresponding information from the person that released the job to the printer using the Printer Client.