Software Version 2.0
October 2016
708P91382

Xerox® Healthcare MFP Solution

Information Assurance Disclosure

Contents

(This page Intentionally blank.)

1. Introduction

The Xerox® Healthcare MFP Solution is a workflow solution that allows a user to scan documents and send messages using their Kno2 account. The Xerox® Healthcare MFP Solution is designed to work on ConnectKey devices and is available in the Xerox App Gallery. (Look for "Share Patient Information" in the Gallery, the display name for the Xerox® Healthcare MFP App).

1.1. Purpose

The purpose of the Information Assurance Disclosure is to disclose information for the Xerox® Healthcare MFP 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® Healthcare MFP relative to Information Assurance (IA) and the protection of customer service information. Please note that the customer is responsible for the security of their network, and the Xerox® Healthcare MFP 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® Healthcare MFP relative to IA.

This document does not provide tutorial level information about security, connectivity or Xerox® Healthcare MFP features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these 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® Healthcare MFP 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® Healthcare MFP is an accessory that can be added to some Xerox ConnectKey devices. The purchase of the accessory includes a Kno2 license, allowing the MFP to be enabled in the Kno2 system. When combined with the Xerox® Healthcare MFP App, users are able to scan documents and send them via the Kno2 system to other providers or organizations that are part of the Kno2 system.

The Xerox® Healthcare MFP supports a single primary workflow.

- **Message Creation and Send** – User's identify themselves by logging into the Share Patient Information App using their Kno2 credentials. They may then create messages, which can be sent to recipients within Kno2 based upon their organization. Users will be allowed to select the recipient(s) of a message, enter patient information, attach documents (scanned files), review and send messages.

2.2. System Diagram

The architecture of the Xerox® Healthcare MFP Solution incorporates technical controls to eliminate, where possible, information security risks from all information assets including software components, connected system components, and information owners. The figure below illustrates the relationship between the Xerox® Healthcare MFP and these other system components. The base of the arrows indicate the system or touch point that initiates the contact.

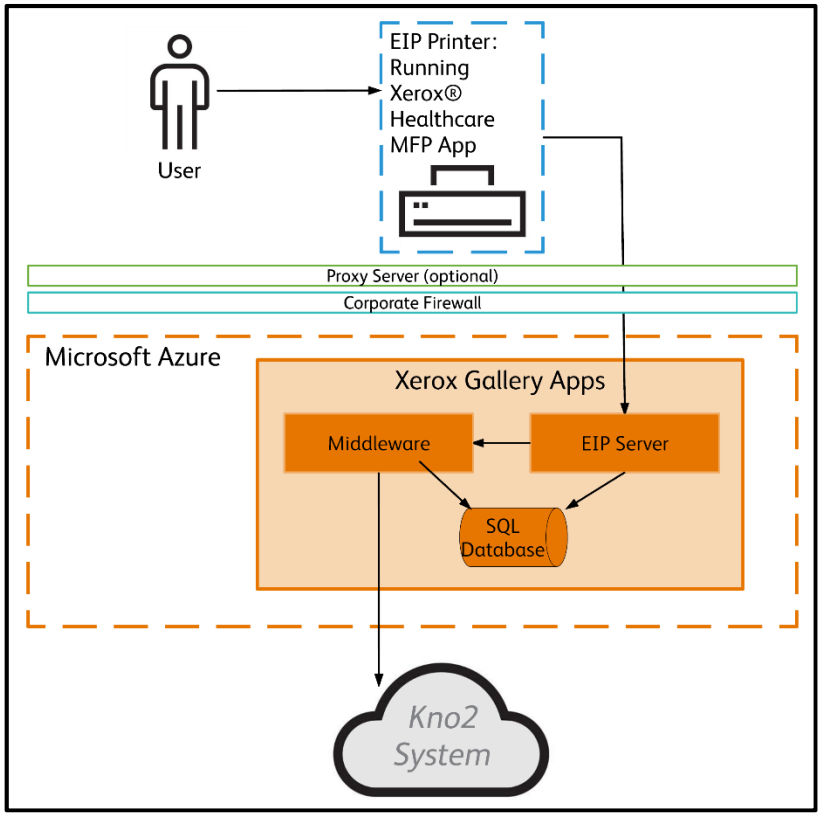

Figure 2.2-1: Xerox® Healthcare MFP Architecture

2.3. Description of System Component

Component	Description
User	A user of the Kno2 system. They user must have login credentials for the Kno2 system, and they must be associated with 1 or more Kno2 accounts.
Xerox MFP (Multi-Function Printer) running the Xerox® Healthcare MFP App	A Xerox® device that supports multiple functions (e.g. Copy, Printing, Scanning, Faxing, etc.). The devices must support EIP (Extensible Interface Platform) and have the ability to load and run ConnectKey Apps from the Xerox App Gallery.
Xerox Gallery Apps EIP Server	Serves up the EIP Web Page content displayed in the EIP browser of the MFP.
Xerox Gallery Apps Middleware	Acts as an interface/intermediary for all information and requests to Kno2.
Xerox Gallery Apps SQL Database	SQL database used to store state information related to the App (no customer/patient info is stored).
Kno2 System	The cloud hosted Kno2 system. This is the backend system used for all web service communication with the Xerox® Healthcare MFP Solution.

Table 2.3-1: System Components

3. System Architecture

3.1. Sub-Systems

3.1.1. Xerox Gallery Apps EIP Server

The Gallery Apps EIP Server runs on a Microsoft Azure Web Role. The production system runs with a minimum of 2 Azure Web Roles. Each role runs in its own Azure Virtual Machine (VM), which consist of a 1 core CPU, with 3.5GB RAM and 40GB HDD. The number of VMs may scale up/down based on demand.

Volatile Memory				
Type (SRAM, DRAM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Process to Clear**
Azure storage – System Memory	3.5GB	N	Executable code, temporary storage for messages processing related data, variables, state information, etc.	Power Off or Exit of the Service

Table 3.1-1: Volatile Memory Information Statement of Volatility (SoV)

Non-Volatile Solid State Memory				
Type (Flash, EEPROM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Process to Clear**
HDD	40GB	N	**Azure Web Roles:** Storage of binaries, libraries, graphic images, HTML pages and Javascript pages **Table Storage:** Usage Logging **SQL DB:** Session data	**Azure Web Roles:** Requires removal of Xerox roles **Table Storage:** Entries purged based on date **SQL DB:** Entries can be marked as deleted during normal system processing and will be reclaimed by the OS

Table 3.1-2: Non-Volatile Memory Information SoV

3.1.2. Xerox Gallery Apps Middleware

The Gallery Apps EIP Server runs on a Microsoft Azure Web Role. The production system runs with a minimum of 2 Azure Web Roles. Each role runs in its own Azure VM, which consist of a 1 core CPU, with 3.5GB RAM and 40GB HDD. The number of VMs may scale up/down based on demand.

Volatile Memory				
Type (SRAM, DRAM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Process to Clear**
Azure storage – System Memory	3.5GB	N	Executable code, temporary storage for messages processing related data, variables, state information, etc.	Power Off or Exit of the Service

Table 3.1.2-1: Volatile Memory Information SoV

Non-Volatile Solid State Memory				
Type (Flash, EEPROM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Process to Clear**
HDD	40GB	N	**Azure Web Roles:** Storage of binaries and libraries **Table Storage:** Usage Logging **SQL DB:** Session data	**Azure Web Roles:** Requires removal of Xerox roles **Table Storage:** Entries purged based on date **SQL DB:** Entries can be marked as deleted during normal system processing and will be reclaimed by the OS

Table 3.1.2-2: Non-Volatile Memory Information SoV

3.1.3. Kno2 System

The Kno2 system and its hardware/architecture is outside the scope of this document. Kno2 provides a cloud accessible service that is used by the Xerox® Healthcare MFP Solution. Please contact Kno2 if additional details related to the system are required.

3.2. Open Source Components

3.2.1. Cloud Hosted Components

Component	Version
Bootstrap	3.3.5
MS Entity Framework	6.1.3
jquery	2.1.4
Microsoft ASP.NET Web API Client Libraries	5.2.3
Microsoft ASP.NET Web API Core Libraries	5.2.3
Microsoft ASP.NET Web API OWIN	5.2.3
Microsoft ASP.NET Web API Web Host	5.2.3
Modernizr	2.8.3
WebGrease	1.6.0
jQuery UI - jquery/jquery-ui on GitHub	1.11.4
stringencoders	trunk-20110712-svn
Antlr	3.5.0.2
Microsoft ASP.NET MVC 4	5.2.3
Microsoft ASP.NET Web Optimization Framework	1.1.3
Microsoft ASP.NET Web Pages 2	3.2.3
Microsoft jQuery Unobtrusive Validation	3.2.3
Microsoft.Web.Infrastructure	1.0.0.0
jQuery Corner Plugin	2.13
jQuery BlockUI Plugin	2.59.0
Respond JS	1.4.2
Visual Studio Autogenerated Code	VS2013
Microsoft Azure Key Vault Core Library	1.0.0
Microsoft.Owin.Host.HttpListener	3.0.1
Microsoft.Owin.Hosting	3.0.1
Microsoft.Owin	3.0.1
RAZOR - Microsoft.NET Application Suite	3.2.3
CodeDOM Providers for .NET Compiler Platform ("Roslyn") 1.0.1	Unspecified
jquery-tmpl	vBeta1.0.0
angular.js	1.4.7
Aspose.Total for .NET	Unspecified
Microsoft ASP.NET Identity Core	2.2.1
Microsoft ASP.NET Identity EntityFramework	2.2.1

jQuery.Form	3.51
Aes Class Sample Code	Unspecified
iscroll	5.1.3
angular.js	1.4.8
Visual Studio Autogenerated Code	2015
Microsoft Exchange Web Services Managed API 2.0	Unspecified
Bootstrap	3.3.6
DeveloperForce.Force	1.2.3
SharpZipLib	0.86.0
Microsoft HTTP Client Libraries	2.2.29
Microsoft BCL Portability Pack	1.1.10
Microsoft BCL Build Components	1.0.21
EdmLib	5.7.0
System.Spatial	5.7.0
WCF Data Services Client	5.7.0
Microsoft Async 1.0.168	Unspecified
Microsoft Compression	3.9.85
JSBase64 1.0	Unspecified
Json.NET	8.0.3
EIP Nextgen Widgets g9 04152016	Unspecified
Paul Johnson's JavaScript Message Digest Hash Function Library	2.2alpha
Windows Azure Storage	7.0.0
Windows Azure Configuration Manager	3.2.1
Sample for polyfill of find method in JavaScript	Unspecified
jquery-validation	1.15.0
ODataLib	5.7.0

Table 3.2.1-1: Cloud Hosted Components

3.2.2. ConnectKey App Components

Component	Version
jquery	2.1.4

Table 3.2.2-1: ConnectKey App Components

3.3. Operating System

The VMs in Azure run Windows Server 2012 R2.

4. System Interaction

4.1. Component Communication

Communication	Encryption Details
Printer and Xerox Gallery Apps EIP Server	Printer communicates via HTTPS with the EIP Server to retrieve EIP page contents (browser pages) to be displayed at the printer. Printer sends scan jobs to the Gallery Apps Middleware via HTTPS.
Xerox Gallery Apps EIP Server and Xerox Gallery Apps Middleware	The EIP Server communicates with the Middleware via HTTPS for any and all Kno2 related requests. The Middleware layer acts as an interface/intermediary for all information and requests to Kno2.
Xerox Gallery Apps Middleware and Kno2 System	Xerox Gallery Apps Middleware communicates with Kno2 via HTTPS for Login, Draft Creation/Modification, sending attachments and initiating Messages.
Xerox Gallery Apps Middleware and XGA SQL Database	Retrieval and storage of state information related to the App (no customer/patient info is stored).
Xerox Gallery Apps EIP Server and XGA SQL Database	Retrieval and storage of state information related to the App (no customer/patient info is stored).

Table 4.1-1: Component Communication

This section captures the security considerations and implementation of Xerox® Healthcare MFP in the following areas:

- Protocols and port numbers used by the system
- Individual system components
- Communication between system components

4.2. System Components

4.2.1. Printer with Xerox® Healthcare MFP

This is an EIP capable device capable of running ConnectKey Apps from the Xerox App Gallery. In this case, the printer has the Xerox® Healthcare MFP App installed. The Xerox® Healthcare MFP App is installed via the Gallery and must be licensed on the Kno2 system.

4.2.2. Xerox Gallery Apps EIP Server

The Xerox Gallery Apps EIP Server is a service hosted on the Microsoft Azure Cloud System. The EIP Server is responsible for hosting the EIP web pages which are displayed on the UI of the printer. The web pages are based on user interaction with the Xerox® Healthcare MFP App. The EIP Server interacts with the Middleware when it needs to interface with the Kno2 system. The server is scalable so that multiple instances may be spun up/down as needed to handle user demand. The service is hosted both in the US and Europe (Dublin). Users will be routed to the closest server geographically (based on network speed).

4.2.3. Xerox Gallery Apps Middleware

The Xerox Gallery Apps Middleware is a service hosted on the Microsoft Azure Cloud System. The Middleware acts as an interface to the Kno2 System. All communication related to Kno2 between the Printer and the EIP Server is directed to the Middleware. These other components never directly interact with the Kno2 System. The server is scalable so that multiple instances may be spun up/down as needed to handle user demand. The service is hosted both in the US and Europe (Dublin). Users will be routed to the closest server geographically (based on network speed).

4.2.4. Kno2 System

The Kno2 cloud hosted system provides a programmatic (API) interface to the Kno2 methods allowing for the creation and sending of Kno2 messages.

4.2.5. SQL Storage

A collection of non-sensitive information related to the Xerox® Healthcare MFP App instances are installed on the various Xerox printers. Information includes:

- Encoded Session Information
  - Access Token
  - Issue date
  - Token Expiration
  - Refresh Token
  - Token Type
  - Device License info
  - Username

- Encoded Attachment Details
  - Attachment Size
  - Name
  - Confidentiality
  - Date
  - Message ID
  - Job Status

4.3. System Component Interfaces

4.3.1. Users and Xerox® Healthcare MFP

Users must have a Kno2 account in order to use the Xerox® Healthcare MFP. Refer to the *Xerox® Healthcare MFP Quick Start Guide* (latest version), the section entitled *Associate Your MFP to Your Kno2 Account* for details.

The user interacts with the printer to:

- Authenticate and identify themselves
- Create and send Kno2 Messages (including scanned attachments)

In order to use the Xerox® Healthcare MFP App, the user must supply their Kno2 authentication credentials. These are validated before any further communication can happen with the Kno2 system. The result of the authentication request is the creation of a logon token, which is used for subsequent communication requests with Kno2. In addition to user authentication, the printer itself must be licensed in the Kno2 system. The Xerox® Healthcare MFP App will prevent use of the App if the printer is not associated with a valid license.

4.3.2. Xerox® Healthcare MFP and Xerox Gallery Apps EIP Server Communication

The Xerox® Healthcare MFP App will communicate with the Xerox Gallery Apps EIP Server to request the web page (browser) content that is to be displayed on the printer. The Xerox® Healthcare MFP App will always interact with the EIP Server and will not directly call the Middleware for any Kno2 interaction.

Scan job (attachments) are filed via HTTPS to the EIP Server, which in turn redirects them to the Middleware service. The files are never stored within the Azure Cloud system.

All communication between the Xerox® Healthcare MFP App and the EIP Server is done using HTTPS over port 443. If the printer is configured to use a proxy server for EIP Services, then the communication will be routed first through the local proxy server of the customer. The proxy configuration is a printer setting, and is outside the scope of this solution.

State information, such as the login token for a session, is maintained in the SQL Database. Session-related information is removed upon logout. Sessions are terminated when a user logs out of the App (this includes navigation away from the App), the printer system timeout is reached or the built in 5-minute timer of the App has been exceeded.

If a user exits the Xerox® Healthcare MFP App, the App will attempt to delete any draft message that has been created. If the Xerox® Healthcare MFP App is unable to delete the draft (e.g. connectivity was lost), then the draft message will be available to the user if they log onto the Kno2 web portal. The user may then delete, modify or send the draft as desired.

4.3.3. Xerox Gallery Apps EIP Server and Xerox Gallery Apps Middleware Communication

The Xerox Gallery Apps Middleware acts as an interface between the EIP Server and Kno2. All communication between the EIP Server and the Middleware is via HTTPS using port 443. This includes Kno2 communication for user authentication, message creation, adding attachments (scan jobs) and sending messages. The Middleware is just a pass-through interface. No personal data (including scan jobs) is ever stored by the Middleware.

Similar to the EIP Server, the Middleware makes use of the SQL Database to store state information related to a job or session. This information is removed upon logout or job completion/deletion.

4.3.4. Xerox Gallery Apps Middleware and Kno2 System Communication

The Xerox Gallery Apps Middleware interfaces with the Kno2 system using APIs provided by Kno2. All communication is done via HTTPS over port 443. The Middleware provides a programmatic interface for the EIP Server to easily make Kno2 requests, while abstracting away the details of those requests as well as the handling of message parameters and responses. The interface is designed to be easily called and processed by a web server.

5. Logical access, network protocol information.

5.1. Protocols and Ports

The following table lists the standard default ports used by the Xerox® Healthcare MFP solution. Some port numbers are configurable on the printer, such as the Proxy server address. Other port numbers are non-configurable and cannot be changed.

Protocol	Default Use Port Value	Use	Option	Direction
Xerox Gallery Apps EIP Service Ports:				
HTTPS	TCP 443	EIP Application Webpage Retrieval	Non-configurable	Printer to EIP Server
HTTPS	TCP 443	HTTPS Scan Image Store	Non-configurable	Printer to EIP Server
Xerox Gallery Apps Middleware Ports:				
HTTPS	TCP 443	Kno2 Pass-through Communication	Non-configurable	EIP Server to Middleware
Kno2 Ports:				
HTTPS	TCP 443	HTTPS Scan Image Store	Non-configurable	Middleware to Kno2

Table 5.1-1: Protocols and Ports

6. System access

6.1. App Gallery Authentication

In order to access the Xerox® Healthcare MFP Solution, someone must install the App on the Multi-Function Printer. Typically, this is done by the printer administrator. To obtain a Gallery Account, go to:

https://appgallery.external.xerox.com/xerox_app_gallery/login

6.2. Kno2 Portal Authentication

Users of the Xerox® Healthcare MFP solution must have a Kno2 account. Help on creating a Kno2 account can be found at https://kno2.com.

7. Security Features of the Multi-Function Devices.

The following is a set of recommended security setting for your Xerox Multi-Function device. These settings are recommended, but are not mandatory and will not directly impact the Xerox® Healthcare MFP Solution. Because of the nature of the personal data being handled by the Xerox® Healthcare MFP App, it would be beneficial to ensure that your Xerox MFP is as secure as possible.

Details on enabling these features can be found in the *Xerox® Healthcare MFP Quick Start Guide*:

a. Enable Certificate Validation (where available)
b. Enable Image Overwrite Security
c. Turn on the Audit Log
d. Enable McAfee Embedded Control (where available)
e. Enable User Data Encryption