Xerox® Connect for RMail® App

Security Guide

Xerox® Connect for RMail®

Copyright © 2020 Xerox Corporation. BR26610 Document

Version: 1.0 (May 2020).

Contents

Preface

Xerox® Connect for RMail App provides seamless integration with the RMail service secure Email platform. Key features include transmission as an encrypted email, automatic transition to secure file share mode for large documents and tracking with proof of content delivered via Registered Email™ service to provide a robust audit record.

For customers needing a comprehensive and secure email solution, the RMail service delivers HIPAA and GDPR compliant security integrated with the popular email systems. The Xerox® Connect for RMail App compliments this, providing a seamless and efficient workflow for capturing paper documents and sending via the RMail service.

Purpose

The purpose of the Security Guide is to disclose information for the Xerox® Connect for RMail App with respect to Xerox® 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® Connect for RMail App 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® Connect for RMail App does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Xerox® Connect for RMail App features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

Note: A guide for the secure installation and operation of most Xerox® office equipment is available at www.xerox.com/security. Once there, find your device on the list, and select the “Secure Installation and Operation Guides for Xerox® Products” link.

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® Connect for RMail App; as such, some user actions are not described in detail.

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.

Description and Details

Overview

The Xerox Connect for RMail App is compatible with Xerox® AltaLink, VersaLink and ConnectKey® i-Series devices.

The Xerox® Connect for RMail App supports the RMail service secure Email workflows – users may scan documents and send them via the RMail service. Users will be allowed to select the recipients, subject and message content, define registered email settings and, scanning parameters.

App Hosting

The Xerox® Connect for RMail App consists of two key components, the device weblet and the cloud-hosted web service. The device weblet is a ConnectKey / EIP[1] web app that 1) presents the device user a view of the functionality that is executed in the cloud, and 2) interfaces with the device via the EIP API to initiate device functionality such as document scanning.

The weblet (running in a browser on the device) communicates with the cloud-hosted web service, which executes the business logic of the app, including the selection of message recipients and sending the scanned documents through the RMail service.

RMail Service

The RMail service serves as a communications proxy, enabling email sending.

In order for the app to communicate with the RMail service, it utilizes the authentication provided by RMail, which prompts the user for their RMail service login credentials.

Once authorization has been established, a token is returned from the RMail service. This token is used for further interactions and, it is encrypted on the web service using AES 256. The device does not store the token nor account credentials.

Single Sign On via Xerox® Workplace Suite/Cloud and SSO Manager

In order to improve user experience by removing the need to log in to the RMail service each time, Xerox® offers an optional Single Sign-On (SSO) capability. Users can log into the multi-function printer and are then able to launch the app without the need to provide additional credentials.

The Single Sign-On feature integrates with the Xerox® Workplace Suite/Cloud (XWS/C) authentication solution to store user access information for SSO-compatible Xerox® Gallery Apps. After the user enters their storage service credentials the first time, the XWS/C solution acts as a storage vault where the login information is securely stored.

[1] EIP – The Xerox Extensible Interface Platform. Available on all ConnectKey enabled Xerox MFPs. For more information please refer to https://www.xerox.com/en-us/office/eip

All content to be stored in the vault is encrypted with AES 256 by the SSO Manager server before being given to the SSO vault that resides on the Xerox® Workplace Suite/Cloud solution. This ensures that the SSO vault can never view or use the contents being stored in the vault. Only the SSO Manager infrastructure knows how to decrypt the content stored in the vault and only the App knows how to use it.

The SSO Manager Service manages the encryption key exchange required for secure communications and encrypts/decrypts the content saved in the vault.

For a full description, please review the Xerox® Workplace Suite/Cloud Information Assurance Disclosure: https://security.business.xerox.com/en-us/products/xerox-workplace-suite/

Device Web Service Calls

During standard usage of the Connect for RMail App, calls to the device web services are used to initiate and monitor scan functions and retrieve device information using the EIP interface.

Security

Hosting

As outlined above, the Xerox® Connect for RMail App consists of two parts; a weblet installed on the Xerox device and the cloud-based web service with which the weblet communicates. The web service is hosted on the Microsoft Azure Network. The Microsoft Azure Cloud Computing Platform operates in the Microsoft Global Foundation Services (GFS) infrastructure, portions of which are ISO27001certified. Microsoft has also adopted the new international cloud privacy standard, ISO 27018. Azure safeguards customer data in the cloud and provides support for companies that are bound by extensive regulations regarding the use, transmission, and storage of customer data.

Microsoft Azure Security Highlights

These Security highlights are relevant to the App Gallery system.

General Azure security

- Azure Log Analytics

Networking

- Network Security Groups
- Azure Traffic Manager

For a full description, please follow the link: https://docs.microsoft.com/en-us/azure/security/azure-network-security

Secure Web Communications

The web pages for the Xerox® Connect for RMail App are deployed in a Microsoft Azure Virtual Machine. All web pages are accessed via HTTPS from a Web Browser. All communications to and from the Virtual Machine are over HTTPS. Data is transmitted securely and is protected by TLS security for both upload and download. The default TLS version used is 1.2.

The Xerox® Connect for RMail App requires the user to provide proper/valid credentials in order to gain access to the RMail service. Authenticated users can scan and send documents using HTTPS.

At launch, the app must get an authentication token from the RMail service authentication process. The token is used for that session of the app.

If the customer environment includes an Authentication solution (e.g., Xerox® Workplace Suite/Cloud) with Single Sign On functionality enabled, the user can agree to have their user credentials securely stored and automatically applied during subsequent app launches.

All communication is done via HTTPS and the data is transmitted securely and is protected by TLS security. The default TLS version used is 1.2.

Local and Cloud Storage

The following items are stored locally on the device:

- Recently used usernames are stored in order to simplify the non-SSO user login process.
- Recently used recipient email addresses are stored in order to simplify the addressing workflow.
- Specific user configurations like Registered Email settings and scanning parameters are stored locally on the device as a user convenience.

To use the Xerox® Connect for RMail App, a user must log in to their RMail service account. The app invokes the RMail service, which requires the user to enter their existing username and password and returns an authentication token that can be used for future access.

If the customer environment includes an Authentication solution (e.g., Xerox® Workplace Suite/Cloud) with Single Sign On functionality enabled, the user can agree to have their user credentials securely stored and automatically applied during subsequent app launches.

Once logged in, the user proceeds with specifying the recipients to whom the message will be sent, along with Registered Email settings and scanning parameters, including document OCR. After scanning is completed, the Xerox® Device uploads the scanned files to the cloud-based web service. The uploaded content is encrypted using AES 256. After transmission to the RMail service, all cloud-based stored documents and RMail service credentials are deleted.

The content is protected during transmission by standard secure network protocols at the channel level.

Xerox® Workplace Suite/Cloud and Single Sign On

The Xerox® Workplace Suite/Cloud server accepts credential storage requests from the App via the SSO Manager Service (the App retrieves a vault key from the SSO Manager and uses it to retrieve login credentials from the Xerox® Workplace Suite/Cloud service). All communication is via HTTPS and the data is transmitted securely and is protected by TLS security. The default TLS version used is 1.2. The credentials stored in the Xerox® Workplace Suite vault are encrypted using AES 256.

Components

Xerox® Multi-Function Printer (MFP)

This is an EIP capable device capable of running ConnectKey Apps from the Xerox App Gallery. In this case, the MFP has the Connect for RMail App installed. The Xerox Connect for RMail App is installed via the Gallery either as a paid or trial App.

Web Service

The web service is hosted on the Microsoft Azure Cloud System. The service is responsible for hosting the web pages, which are displayed on the UI of the printer, storage of the scanned documents and a message queue to send emails through the RMail service. The service is hosted in Europe.

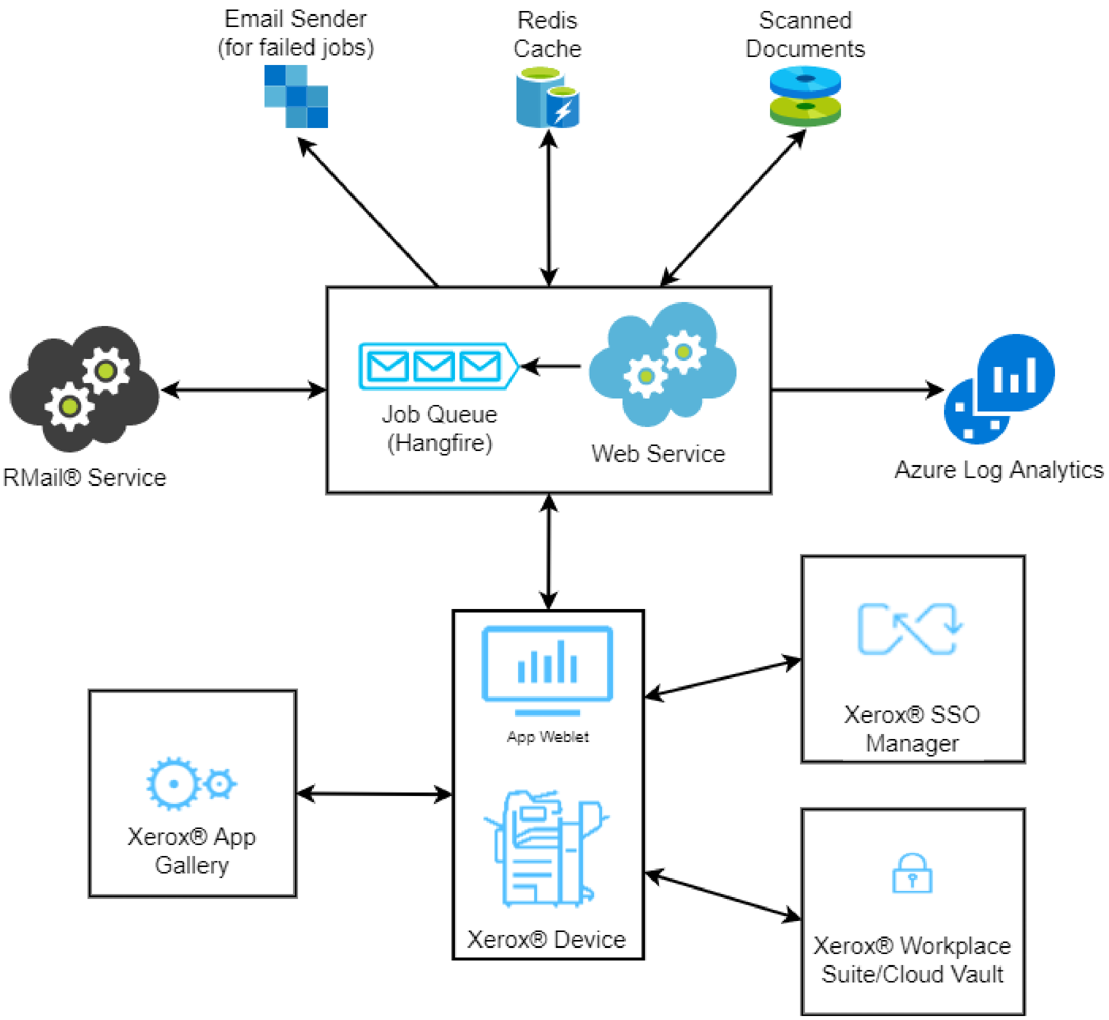
RMail Service

The RMail service provides an Application Programming Interface (API) allowing for user authentication, and the creation and sending of email messages.

Azure Log Analytics

The Azure Log Analytics is used for troubleshooting and/or metrics gathering.

Workflow and Data Flow Overview



Secure Email Workflow

Step 1: User launches Connect for RMail App at the device.

Step 2: User authenticates to the RMail service. (In the first login to an SSO enabled implementation, the user can agree to save credentials to Xerox® Workplace Suite/Cloud storage for future use. On subsequent logins, credentials are automatically retrieved and applied.)

Step 3: User starts to create an email message, selects recipients, and optionally adds a subject and a message body.

Step 4: User selects registered email settings to provide secure message delivery through the RMail service.

Step 5: User selects scanning options such as 2-sided scanning, resolution, output color, original orientation, original size and type.

Step 6: User reviews the message parameters and selects the Send button.

Step 7: The Xerox device starts scanning the document.

Step 8: The scanned document is sent to Connect for RMail App web service.

Step 9: The scanned document is attached to the message and sent to the RMail service for delivery.