Security Guide

Xerox® Connect App for Microsoft® OneDrive – FedRAMP Authorized

Document Version: 1.0 (March 2024).

Contents

1. Introduction

Purpose

The purpose of the Security Guide is to disclose information for Xerox® Apps 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® Apps 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® Apps do not establish security for any network environment.

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

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 apps; 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.

2. Product Description

Overview

The Xerox® Connect App for Microsoft® OneDrive – FedRAMP Authorized consists of a single workflow:

- Scan files to a Microsoft® OneDrive repository

The app and workflow facilitate a combination of the following steps:

- Single Sign-On
- Authentication
- App Hosting
- Repository Navigation
- Scanning
- Document Format Conversion
- SNMP & Device Webservice Calls

Application	What can I do?
Xerox® Connect App for Microsoft® OneDrive – FedRAMP Authorized	• Login to my OneDrive account • Navigate to a folder in my OneDrive repository • Scan a hard copy document to OneDrive using basic configurable scan settings

Table 1 Xerox® App user benefits

APP HOSTING

The Xerox® Connect App for Microsoft® OneDrive **–** FedRAMP Authorized depends heavily on cloud hosted components. A brief description of each can be found below.

Xerox® Connect App for Microsoft® OneDrive – FedRAMP Authorized

The Xerox® App consists of two key components, the device weblet and the cloud-hosted web service. The device weblet is a Xerox® App/EIP web app that enables the following behavior on a Xerox® Device:

- Presents the user with an application UI that executes functionality in the cloud.
- Interfaces with the EIP API, which delegates work when document scanning.

The weblet communicates with the cloud-hosted web service, which executes the business logic of the app.

Microsoft® OneDrive Storage Service

In order for the Xerox® App to communicate and interact with the correct storage location, the user needs to establish a connection with their OneDrive repository. This connection process utilizes the sign-in dialog provided by a customer's chosen identity provider. By default, the primary identity authority is

the Microsoft Online Identity Service. It's also possible for a customer to choose to configure their MSOL tenant so that the Microsoft identity authority delegates to a customer's federated identity provider. In either case, the customer tenant's identity authority requests the username and password needed to access OneDrive content.

Single Sign-On via Kerberos

To improve user experience, Xerox offers an optional on-premises Single Sign-On (SSO) capability that removes the need for a user to sign-in to the Xerox® App each time. When this option is enabled, users can log into the printer and are then able to launch the app without the need to provide additional credentials.

Xerox Extensible Interface Platform®

App script executes device web service calls internally to initiate and monitor scan functions and to pull relevant details related to device properties and capabilities.

COMPONENTS

MFD with Xerox® Connect App for Microsoft® OneDrive – FedRAMP Authorized

This is an EIP capable device that can print, scan and execute a Xerox® ConnectKey® App typically installed from the Xerox App Gallery. In this case, the device has the Xerox® Connect App for Microsoft® OneDrive – FedRAMP Authorized installed without involving Xerox App Gallery during the installation process.

The MFD communicates with the App Service, Middleware Service, Microsoft Online Identity Service, and optionally a customer's AD FS cluster when App SSO using Kerberos is enabled.

Cloud App Service

The App Service component is a web service hosted on the Microsoft Azure Cloud System. This component is responsible for hosting the web pages that display on the UI of the Xerox® Device. Additionally, this component provides the business logic service.

The App Service accepts requests from the MFD and communicates with Xerox Cloud Repository Middleware and File Conversion Services.

Cloud Repository Middleware

The Cloud Repository Middleware component is a service hosted on the Microsoft Azure Cloud System. The primary function of this middleware is to serve as the cloud storage interface adapter for current and future products and services.

The Cloud Repository Middleware accepts requests from the MFD and the App Service and communicates with the Microsoft Online Identity Service and Microsoft Graph.

File Conversion Service

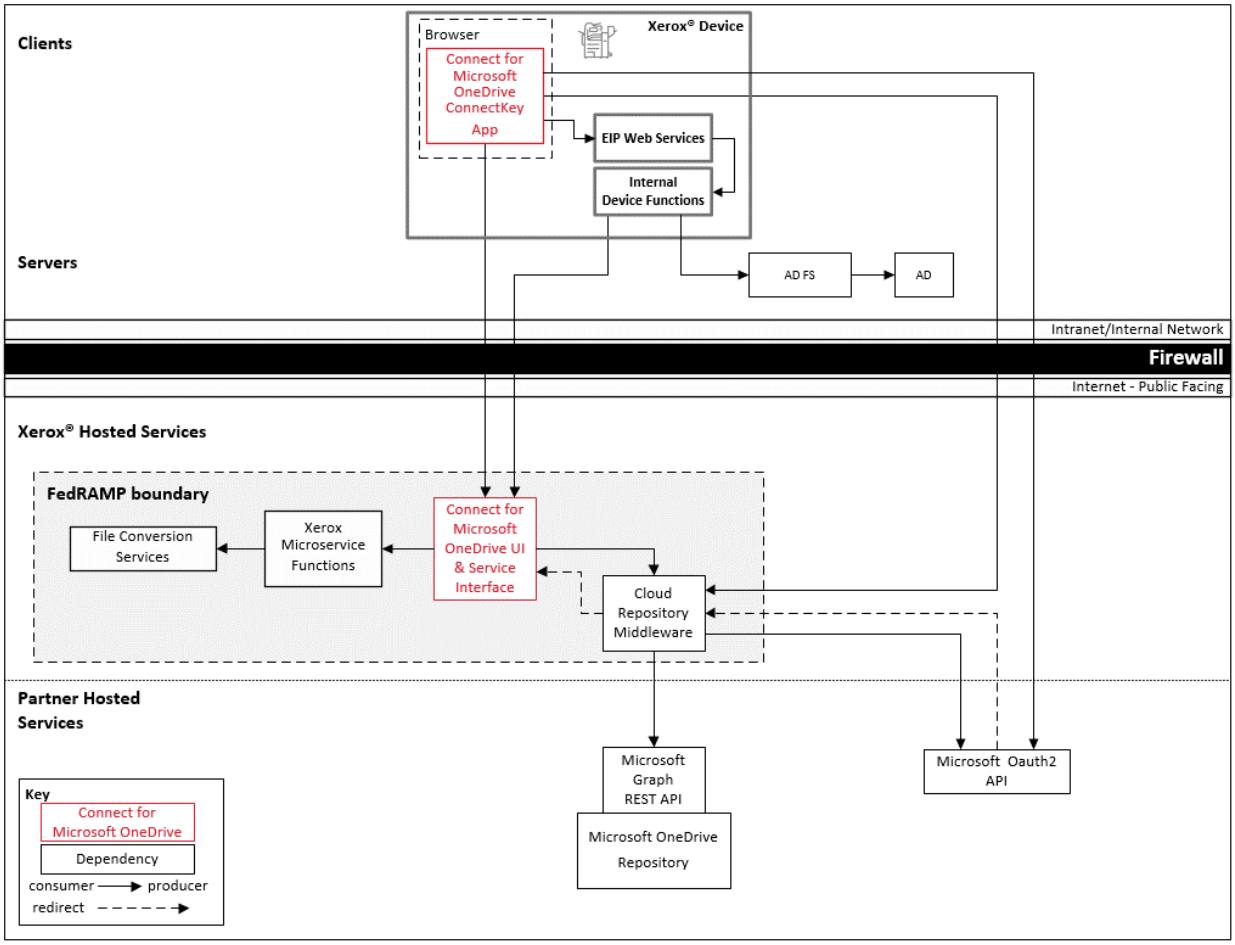
The File Conversion Service component is a service hosted on the Microsoft Azure Cloud System. This component converts a variety of original or scan document formats into formats supported by the App. It is primarily used for cloud-based OCR workloads when converting a scanned document into one of the following Microsoft® Office document formats: Word (DOCX), Excel (XLSX), PowerPoint (PPTX).

The File Conversion Service may accept requests from the App Service.

Architecture and Workflows

DATA FLOW DIAGRAM

App Architecture



Workflows

App Scanning Workflow

Step 1:	User Launches the App on the Xerox® Device.
Step 2:	User authenticates to the OneDrive repository. User authenticates to the OneDrive repository. (If SSO using Kerberos is enabled, the user is signed in automatically.)
Step 3:	User navigates to and selects the destination folder for the scanned document.
Step 4:	User modifies the scanning options (i.e., single sided, resolution, output format, preview, etc.).
Step 5:	User selects the Scan button to scan the document to the selected folder.
Step 6:	If the Preview option was selected in Step 4, the user views the scanned document before deciding to allow the document to be saved to the selected destination folder.
Step 7:	The document is saved to the selected destination folder.

User Data Protection

AUTHENTICATION AND CLOUD REPOSITORY ACCESS

For the Xerox® App to access data stored in the cloud repository, the user is required to authenticate with their Microsoft Online login credentials. The protocol used to authenticate is OAuth 2.0. The authentication process is hosted and controlled by Microsoft. An authentication dialog provided by Microsoft, requests the username and password. Additional data may be required if 2-Factor authentication is enabled.

It's also possible for a customer to choose to configure their MSOL tenant so that the Microsoft identity authority delegates to a customer's federated identity provider. In either case, the customer tenant's identity authority requests the username and password needed to access OneDrive content.

Upon successful login, an authentication code is returned to the device browser, via an HTTP redirect to the Cloud Repository Middleware. The Cloud Repository Middleware then uses the authentication code to obtain an Access and Refresh Token from Microsoft. The Access and Refresh Tokens are returned to the device browser via an HTTP redirect to the Xerox® App. The Cloud Repository Middleware utilizes the Microsoft® Graph API with a valid Access token to access the user's data in the Microsoft repository.

The account credentials provided by the user are accessible to only Microsoft. The App script operating within the EIP browser does not store usernames and passwords. Usernames and passwords are secured using Microsoft's implementation of the OAuth2 protocol. That data is protected during transmission to Microsoft servers using the TLS 1.2 network security protocol.

Once the user completes the authorization challenge, the MSOL identity service returns Graph API access security tokens to the device. Those tokens are then delivered to the App Service and used when accessing the user's files via the Microsoft® Graph API.

The user's access security tokens may be persisted to Xerox managed cloud storage temporarily during the duration of the user's app session.

APPLICATION DATA STORED IN THE XEROX CLOUD

User data related to the categories below are stored in cloud persistent storage until a delete event occurs.

- Login to OneDrive account
- Scanned image preview

The following activities will trigger a delete event, for digital document files that meet the associated criteria.

- A delete occurs when the system detects intermediate processing files exist after a job has completed.

The balance of data stored in the cloud, that is unrelated to user Personally Identifiable Information, may be stored indefinitely for event reporting purposes.

User documents that have been requested to be converted to a Microsoft® Office format are stored in cloud persistent storage until a delete event occurs.

The following delete events occur.

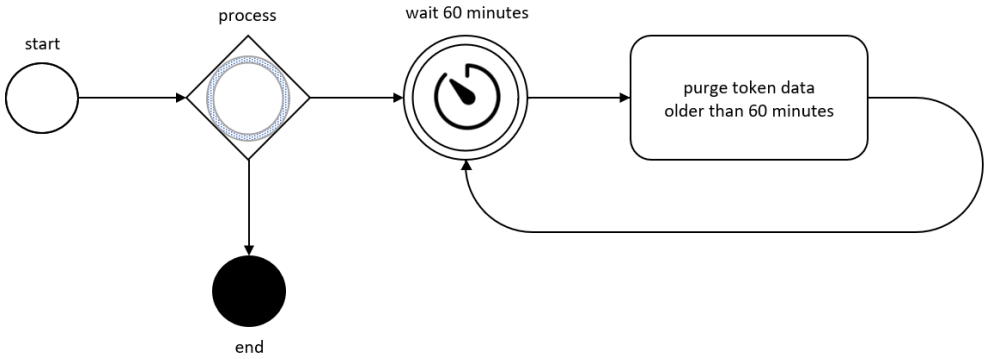
- A delete event occurs when the system detects it is the first day of the month.
- A delete event occurs at least once every 24 hours.

DELETE EVENTS

Delete events are triggered by background timer jobs running in the Xerox cloud.

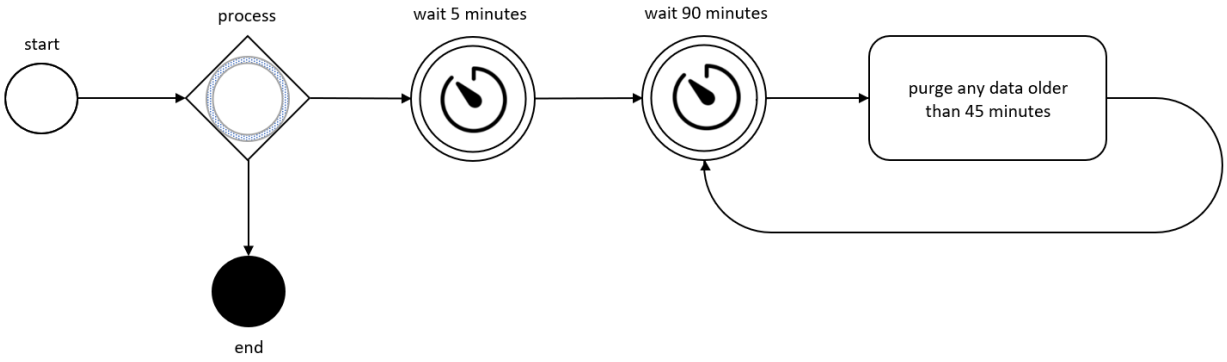
Purge tokens timer job

The timer host is Azure Function App initiated. The trigger event fires shortly after the Function App host is instantiated and subsequent trigger events stop when the timer host process terminates. The purge logic executes in-process.



Purge print and scan preview documents timer job

The timer host is Azure App Service initiated. The timer event fires shortly after the Connector App Service host is instantiated and subsequent timer events stop when the timer host process terminates. The purge logic executes in-process.



Purge converted documents and job parameters timer job

The timer host is Azure App Service initiated. The timer event fires once a day. The purge logic executes in-process.

LOCAL ENVIRONMENT

Application data transmitted

Application data related to the categories below are transmitted to/from the Xerox® Device.

- Account data
- Session data
- Job data

Application data stored on the Xerox® Device

The following app data is stored on the device, encrypted in Browser internal storage, until the App is uninstalled from the device.

- Device's SNMP V2 public community string

HTTP Cookies

The Xerox® Connect for Microsoft® OneDrive App does not store any cookies on the device.

3. Network Information

Protocol, Ports and URLs

The following table lists the protocol, ports and URLs used by the Xerox® Connect App for Microsoft® OneDrive when executing within a customer's private network. All connections are outbound to Cloud hosted components.

Protocol	Transport and Port Value	Use	Component	URL
HTTPS using TLS	TCP 443	App UI, Folder Navigation, Document Scanning	ConnectKey App to Connect for Microsoft OneDrive UI & Services Interface	Available upon request
HTTPS using TLS	TCP 443	Facilitate Authentication Flow	ConnectKey App to Cloud Repository Middleware	Available upon request
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	ConnectKey App to Microsoft OAuth2 API	login.microsoftonline.com

4. General Security Protection

User Data Protection within the products

DOCUMENT AND FILE SECURITY

File content is protected during transmission by standard secure network protocols at the channel level. Since document source content may contain Personally Identifiable Information (PII) or other sensitive content, it is the responsibility of the user to handle the digital information in accordance with information protection best practices.

HOSTING - MICROSOFT AZURE

The cloud services are hosted on the Microsoft Azure Network. The Microsoft Azure Cloud Computing Platform operates in the Microsoft® Global Foundation Services (GFS) infrastructure. 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.

The Apps hosted in the cloud are scalable so that multiple instances may be spun up/down as needed to handle user demand. The service is hosted in Microsoft Azure data centers located in the US and Ireland. Users will be automatically routed to the closest server based on their geographical location.

For full details on Microsoft Azure's standards and certifications, please follow this link:

https://docs.microsoft.com/en-us/azure/compliance/

CLOUD STORAGE – MICROSOFT AZURE

All Azure Storage data is secured when at rest using AES-256 encryption. Any documents, held temporarily, are contained in an Azure Storage account hosted in the Microsoft Azure data center located in Ireland.

For a full description, please follow these links:

Azure Storage

https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

User Data in transit

SECURE NETWORK COMMUNICATIONS

The web pages and app services that constitute the Xerox® Solutions are deployed to Microsoft Azure App Services. All web pages are accessed via HTTPS from a web browser. All communications 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® App requires the user to provide proper/valid credentials in order to gain access to the application's features. Authenticated users are allowed to access the features and data using HTTPS.

At launch, the apps must get an authentication/session token through the solution's authentication process. The access token acquired is used for that session of the app.

When using the Xerox® Connect App for Microsoft® OneDrive – FedRAMP Authorized installed on a Xerox® Device, 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. It is the responsibility of the customer to install the TLS CA certificates on their devices and to enable server certificate validation on all devices.

For more information related to Azure network security, please follow the link:
https://docs.microsoft.com/en-us/azure/security/azure-network-security

5. Additional Information & Resources

Security @ Xerox

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see https://www.xerox.com/security.

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

Additional Security Resources

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/
Xerox Trust Center	https://trust.corp.xerox.com

Table 2 Additional Resources