Security Guide

Scan Apps for Microsoft Cloud Repositories

Applies to:

- Scan App for Microsoft® OneDrive
- Scan App for Microsoft® 365

Document Version: 1.0 (January 2022).

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

Scan App for Microsoft® OneDrive and Scan App for Microsoft® 365 both support a single workflow:

- Scan files to a Microsoft cloud repository

The app facilitates a combination of the following steps:

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

Application	What can I do?
Scan App for Microsoft® OneDrive Scan App for Microsoft® 365	• Login to my Microsoft account • Navigate to a folder in my repository • Scan a hard copy document to the repository using standard user specified scan settings.

Table 1 Xerox® App user benefits

APP HOSTING

Each scan App depends on cloud hosted components. A brief description of an App's components can be found below.

The Scan App

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

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

The weblet script communicates with the cloud-hosted connector web service, which executes the connector logic for the app.

Microsoft 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 repository. This connection process utilizes the authentication dialog provided by the storage service, which requests the username and password for the storage service account. An OAuth login token is returned to the device from the storage service. This token is used for further interactions. The account credentials are not stored by the Device. Once authenticated, the Microsoft® Graph API is utilized to access the Microsoft repository using the cloud-hosted connector web service.

Single Sign-On via Xerox® Workplace Cloud and SSO Manager

In order to improve user experience, by removing the need to log in to the Xerox® App each time Xerox offers an optional Single Sign-On (SSO) capability. 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®

During standard usage of the Xerox® App, calls to the device web services are used to initiate and monitor scan functions and to pull relevant details related to device properties and capabilities.

COMPONENTS

MFD with a Scan App – a Xerox® ConnectKey® App

This is an EIP capable device that can print, scan and execute ConnectKey Apps installed from the Xerox® App Gallery or other utility. In this case, the device has the Scan App for Microsoft® OneDrive or Scan App for Microsoft® 365 installed.

Scan App – UI & Service Interface Client

The UI & Service Interface Client component is embedded in the weblet. The App weblet is a container that enables in-box hosting of the App's web pages, which display on the UI of the Xerox® Device. Additionally, the component provides the business logic service and interfaces with the Xerox Cloud Repository Middleware.

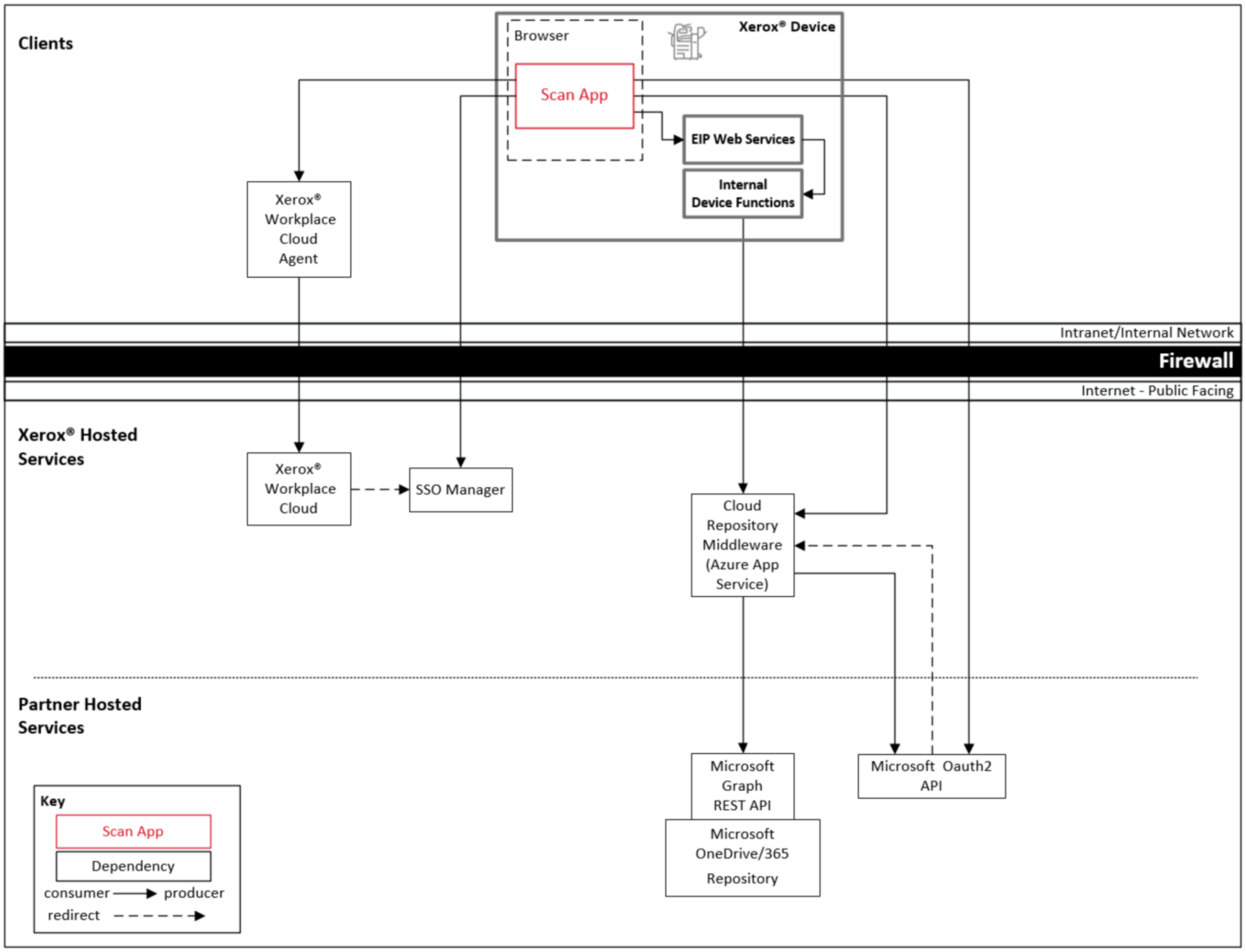
Xerox Cloud Repository Middleware

The Cloud Repository Middleware component is a service hosted on the Microsoft Azure Cloud System. The Cloud Repository Middleware interfaces with the Microsoft Graph REST APIs to access the Microsoft Online IdP and the Microsoft cloud repository.

Architecture and Workflows

DATA FLOW DIAGRAM

Single Sign-On Architecture



Workflows

App Scanning Workflow

Step 1: User Launches the App on the Xerox® Device.

Step 2: User authenticates to the Microsoft cloud repository. (If first login, user can agree to save their credentials to the SSO vault storage for future use. On subsequent logins, the user’s credentials are automatically retrieved and applied.)

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, etc…).

Step 5: User selects the Scan button to scan the document to the selected folder.

Step 6: The document is saved to the selected destination folder.

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

Scanned document data is never persisted to the Xerox cloud. The scanned document is streamed from the device to the Microsoft repository using the Xerox Cloud Repository Middleware.

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

- For Microsoft session support, the App stores the Graph API OAuth2 refresh token
    - for offline persistence, the token is stored in Xerox® Workplace Cloud
    - for online persistence, the token is stored temporarily in an Azure Table

The following activities will trigger a delete event, for data that meet the associated criteria:

- when the system detects intermediate files exist after a job has completed processing
- when the system detects a session has ended after a timer job time threshold is reached

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

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 Scan Apps do 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 Scan Apps 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 Configuration	ConnectKey App to App Gallery	appgallery.services.xerox.com
HTTPS using TLS	TCP 443	Facilitate Authentication Flow	ConnectKey App to Cloud Repository Middleware	cloudmiddleware.services.xerox.com
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	ConnectKey App to Microsoft OAuth2 API	login.microsoftonline.com
HTTPS using TLS	TCP 443	Single Sign On (SSO)	ConnectKey App to SSO Manager	ssomanager.services.xerox.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

XEROX® WORKPLACE CLOUD AND SINGLE SIGN-ON SERVICES

The Xerox® ConnectKey App Single Sign-On feature integrates with the Xerox® Workplace Cloud 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 Xerox® Workplace Cloud solution acts a storage vault where the login information is securely stored.

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 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/

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 a Scan App installed on a Xerox® Device, if the customer environment includes an Authentication solution (e.g., Xerox® Workplace 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. Xerox App Gallery supplies a link to a Certificate Authority root certificate for validation with the cloud web service. It is the responsibility of the customer to install the certificate on their devices and to enable server certificate validation on the devices.

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

XEROX WORKPLACE CLOUD AND SINGLE SIGN-ON SERVICES

The Xerox® Workplace Cloud server accepts credential storage requests from the App via the SSO Manager service (the Xerox® App retrieves a vault key from the SSO Manager and uses it to retrieve login credentials from the Xerox® Workplace 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.

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 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/

Table 2 Additional Resources