Xerox®
Connect for Microsoft®
OneDrive App

Information Assurance Disclosure

BR25649
Document Version: 1.0 (December 2018).

Preface

Xerox® Connect for Microsoft® OneDrive app is a simple repository connection solution for your Xerox® device that supports:

1) retrieving and printing files from a OneDrive repository,
2) scanning files into a OneDrive repository.

1. Purpose

The purpose of the Information Assurance Disclosure (IAD) is to disclose information for Xerox® Connect for Microsoft® OneDrive app 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® Connect for Microsoft® OneDrive 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 Microsoft® OneDrive app does not establish security for any network environment.

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

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 Connect for Microsoft® OneDrive app; as such, some user actions are not described in detail.

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.

.

Contents

1. Description and Details

Overview

The Xerox® Connect for Microsoft® OneDrive app provides two primary workflows for the logged in customer (see section 3 for workflow and data flow overview):

- Print files from a OneDrive repository
- Scan files to a OneDrive repository

Each workflow facilitates a combination of steps:

- App hosting
- Integration with the third-party storage service: Microsoft® OneDrive
- Printing files
- Scanning files
- Device web service calls

App Hosting

The Xerox® Connect for Microsoft® OneDrive app consists of two key components, the device weblet and the cloud-hosted web service. The device weblet is a ConnectKey / EIP web app that 1) presents the device user a view to 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 printing and scanning.

The weblet communicates with the cloud-hosted web service, which executes the business logic of the app, including the printing and scanning of files.

Microsoft® OneDrive Storage Service

In order for the 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 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.

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 storage service 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.

The Single Sign-On feature integrates with the Xerox® Workplace Suite/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 XWS/C 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 XWS/C 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/

Printing Files

When a user wants to print a document, they will navigate their online repository, locate and select the file from the storage service, optionally modify the print settings, and print out the file. The Xerox® Connect for Microsoft® OneDrive app's web service will retrieve the file from the storage service and print it.

Scanning Files

A user can scan a file to a select folder in their repository by navigating to folder, selecting their scan options and pressing the Scan button in the app UI. The scanned file is uploaded to the app's web service, which transfers the file to the user selected folder within their repository.

Device Webservice Calls

During standard usage of the Xerox® Connect for Microsoft® OneDrive app, calls to the device web services are used to initiate scan and print functions using the EIP interface.

2. Security

Hosting

The Xerox® Connect for Microsoft® OneDrive 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 ISO27001-certified. 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 Security Center
- Azure Key Vault
- Log Analytics

Storage security

- Azure Storage Service Encryption
- Azure Storage Account Keys
- Azure Storage Analytics

Database security

- Azure SQL Firewall
- Azure SQL Connection Encryption
- Azure SQL Always Encryption
- Azure SQL Transparent Data Encryption
- Azure SQL Database Auditing

Identity and access management

- Azure Role Based Access Control
- Azure Active Directory
- Azure Active Directory Domain Services
- Azure Multi-Factor Authentication

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 Microsoft® OneDrive app, are deployed in a Microsoft Azure App Service. All web pages are accessed via HTTPS from a Web Browser. All communications to and

from the Xerox® App Service 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 Microsoft® OneDrive app requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for OneDrive include an e-mail address and a password. With valid credentials, the Xerox® Connect for Microsoft® OneDrive app can browse the repository main site or team site, the libraries contained within and the folders in the libraries. Authenticated users are allowed to scan and print documents using HTTPS.

At launch, the app must get an authentication/session token from the Cloud Repository Middleware Service in order to be given permission to access the cloud repository thru the Cloud Repository Middleware Service. The app requests the authentication/session token by transmission of the device serial number and the app id. The token is used for that session of the app. The app can then authenticate with the Cloud Resident Repository and then browse for folders and files.

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. Xerox® App Gallery supplies a link to a Certificate Authority root certificate for validation with Cloud Repository Middleware service. It is the responsibility of the customer to install the certificate on their devices and to enable server certificate validation on the devices.

Based on the user actions, either a print or scan job is initiated with the device. Once the job has been submitted, the device communicates with the Xerox Cloud Repository Middleware (See the section **Device and Xerox Cloud Repository Middleware** for details).

Device and Xerox Cloud Repository Middleware

The Scan and Print jobs submitted to a device communicate with the Cloud Repository Middleware via HTTPS and the data is transmitted securely and is protected by TLS security for both Upload and Download of documents. The default TLS version used is 1.2. All web service calls by the device, to the Cloud Repository Middleware, use the same authentication/session token acquired by the Cloud Repository App.

Cloud Repository Middleware and Cloud Resident Repositories

The Cloud Repository Middleware routes incoming requests to the Cloud Resident Repository specified in the request (i.e. OneDrive). The Cloud Repository Middleware will decrypt any credentials before using them to access a Cloud Resident Repository.

The Cloud Repository Middleware uses the Microsoft® Graph API to communicate with each of the OneDrive Cloud Resident Repository. 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.

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 calls the SSO Manager and the SSO Manager calls the XWS/C 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 XWS vault are encrypted using AES 256.

Local Encryption Storage

The Xerox® Connect for Microsoft® OneDrive app does not store any data locally on the device.

Devices

Xerox® devices have a variety of security features that can be employed to increase security. Availability of these features depends based on model. It is the customer's responsibility to understand and implement appropriate controls for devices behavior.

Some examples are as follows:

1. Xerox Image Overwrite electronically shreds information stored on the hard drive of devices as part of the routine job process.
2. Data Encryption uses state of the art encryption technology on data stored within the device as well as for data in motion in and out of the device.

For more information about the above examples as well as for other device security related technologies please see http://www.xerox.com/information-security/product-security.

The Xerox® Connect for Microsoft® OneDrive app is supported on Xerox® ConnectKey®, AltaLink® and VersaLink® devices. It is the customer's responsibility to understand the security features of these Xerox® devices, which are used in the Xerox® App Gallery system.

Clearing Device Browser Cache

It is recommended that users log out of the app when they have finished their task at the device. Logging out of the app will terminate the connection to the authenticated Cloud Repository.

The EIP browser will also clear the cache on all system session boundaries. System boundaries are any conditions that lead to a login/logout of the current user. The act of logging out of the app is all that is necessary to disconnect from the cloud repository.

However, if the user prefers to manually clear the device browsing history, in addition to logging out of the app, there are a couple options that can be applied to accomplish this. Users may opt to double click the Clear All button on the ConnectKey® device panel and then select Confirm in the dialog window. Or users may exit the app by logging out and then select the Reset button for AltaLink® and Versalink® devices.

The EIP browser will also clear cache when it is explicitly disabled on the system. A Device Administrator can accomplish this by following the steps outlined below.

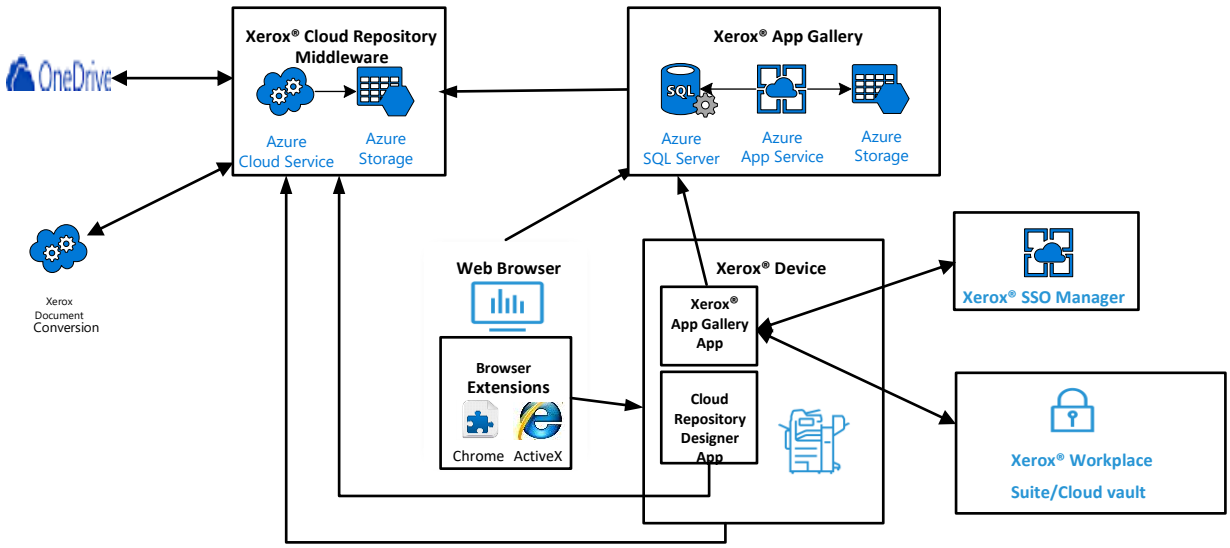
Disable the EIP Browser using CentreWare Internet Services® for ConnectKey® and AltaLink® devices;

1. Launch a web browser.
2. Enter the device IP address.
3. Log in with the device admin credentials.
4. **Select Properties -> General Setup -> Extensible Service Setup**.
5. On the Extensible Service Setup page, uncheck **Enable the Extensible Services Browser** option and select **Apply**.
6. Select **OK** to dismiss the success dialog window.
7. **Recheck** the **Enable the Extensible Services Browser** option.
8. Select **Apply**.
9. Select **OK** to dismiss the success dialog window.

Disable the EIP Browser using the Embedded Web Server for VersaLink® devices;

1. Launch a web browser.
2. Enter the device IP address.
3. Log in with the device admin credentials.
4. **Select Apps -> EIP Settings**
5. On the EIP Settings page, slide the EIP Browser switch to the left to turn it off.
6. Slide the EIP Browser switch back to the right to turn the option back on.

3. Workflow and Data Flow Overview



App Printing Workflow

Step 1: User launches the App at the Device

Step 2: User authenticates to the Microsoft® OneDrive repository. (If first login, user can agree to save credentials to XWS/C storage for future use. On subsequent logins, credentials are automatically retrieved and applied.)

Step 3: User navigates the folder structure to locate the file to be printed.

Step 4: User selects a file and modifies the print options (ie; single sided, etc…).

Step 5: User selects the Print button and their file is printed at the device.

App Scanning Workflow

Step 1: User launches the App at the Device

Step 2: User authenticates to the Microsoft® OneDrive repository. (If first login, user can agree to save credentials to XWS/C storage for future use. On subsequent logins, credentials are automatically retrieved and applied.)

Step 3: User navigates to and selects the folder that the file will be scanned into.

Step 4: User modifies the scanning options (ie; single sided, resolution, etc…).

Step 5: User selects the Scan button and the file is scanned into the selected folder.