

Xerox Security Guide

Xerox® Connect for DocuShare® Go App



© 2020 Xerox Corporation. All rights reserved. Xerox®, ConnectKey®, and DocuShare® Go are trademarks of Xerox Corporation in the United States and/or other countries. BR32318

Other company trademarks are also acknowledged.

Document Version: 1.0 (October 2020).

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.

Contents

Purpose	i
Target Audience	i
Disclaimer	i
1. General Security Protection.....	1-1
User Data Protection within the products.....	1-1
Document and File Security	1-1
Hosting - Microsoft Azure.....	1-1
Cloud Storage – Microsoft Azure	1-1
Xerox® Workplace Suite/Cloud and Single Sign-On Services	1-1
User Data in transit	1-2
Secure Network Communications.....	1-2
Xerox Workplace Suite/Cloud and Single Sign-On Services.....	1-2
User Data Protection.....	1-3
Application data stored in the Xerox cloud.....	1-3
Local Environment	1-3
2. Xerox® Connect for DocuShare® Go App – ConnectKey App Product Description	2-4
Overview	2-4
App Hosting.....	2-4
Components	2-5
Architecture and Workflows	2-6
3. Additional Information & Resources.....	3-9
Security @ Xerox	3-9
Responses to Known Vulnerabilities.....	3-9
Additional Resources	3-9

1. 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, 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.

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 both in the US and Europe. Users will be routed to the closest server geographically based on server load and network speed.

CLOUD STORAGE – MICROSOFT AZURE

All Azure Storage data is secured when at rest using AES-256 encryption.

For a full description, please follow these links:

Azure SQL

<https://azure.microsoft.com/en-us/blog/announcing-default-encryption-for-azure-blobs-files-table-and-queue-storage/>

Azure Storage

<https://azure.microsoft.com/en-us/blog/announcing-default-encryption-for-azure-blobs-files-table-and-queue-storage/>

XEROX® WORKPLACE SUITE/CLOUD AND SINGLE SIGN-ON SERVICES

The Xerox® ConnectKey App 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 as 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/>

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 ConnectKey App 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. 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 SUITE/CLOUD AND SINGLE SIGN-ON SERVICES

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

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

User data related to the categories below are stored in cloud persistent storage until a user session ends.

- Login to DocuShare account
- Scanned image preview
- Print preview image

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.

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 Xerox® Connect for DocuShare® Go app does not store any data locally on the device.

HTTP Cookies

The ConnectKey App does not store any cookies on the device.

2. Xerox® Connect for DocuShare® Go App – ConnectKey® App Product Description

OVERVIEW

ConnectKey App

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

1. Print files from the DocuShare Go online repository
2. Scan files to the DocuShare Go online repository

Application	What can I do?
ConnectKey App	<ul style="list-style-type: none">• Login to my DocuShare Go account• Select Print or Scan workflow• Navigate to a folder in my DocuShare Go account• Scan a hard copy document to DocuShare Go with standard scan settings• Select a file in DocuShare Go and Print a hard copy document with standard print settings

Table 1 ConnectKey App user benefits

APP HOSTING

The ConnectKey App depends heavily on cloud hosted components. A brief description of each can be found below.

ConnectKey App

The ConnectKey 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 enables the following behavior on a Xerox device:

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

DocuShare Go 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 DocuShare Go 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 DocuShare Go API is utilized to access the DocuShare Go repository.

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 ConnectKey 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® Web Services

During standard usage of the ConnectKey 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 Xerox® Connect for DocuShare® Go App – ConnectKey App

This is an EIP capable device that can print, scan and execute ConnectKey Apps installed from the Xerox® App Gallery. In this case, the device has the Xerox® Connect for DocuShare® Go App installed.

Xerox® Connect for DocuShare® Go App – Web UI

The Web UI component is a service hosted on the Microsoft Azure Cloud System. The Web UI component is responsible for hosting the web pages, which display on the UI of the printer.

Xerox® Connect for DocuShare® Go App – Service Interface

The Service Interface component is a service hosted on the Microsoft Azure Cloud System. The Service Interface provides the business logic service and interfaces with the Xerox® Cloud Repository Middleware.

Xerox® Cloud Repository Middleware

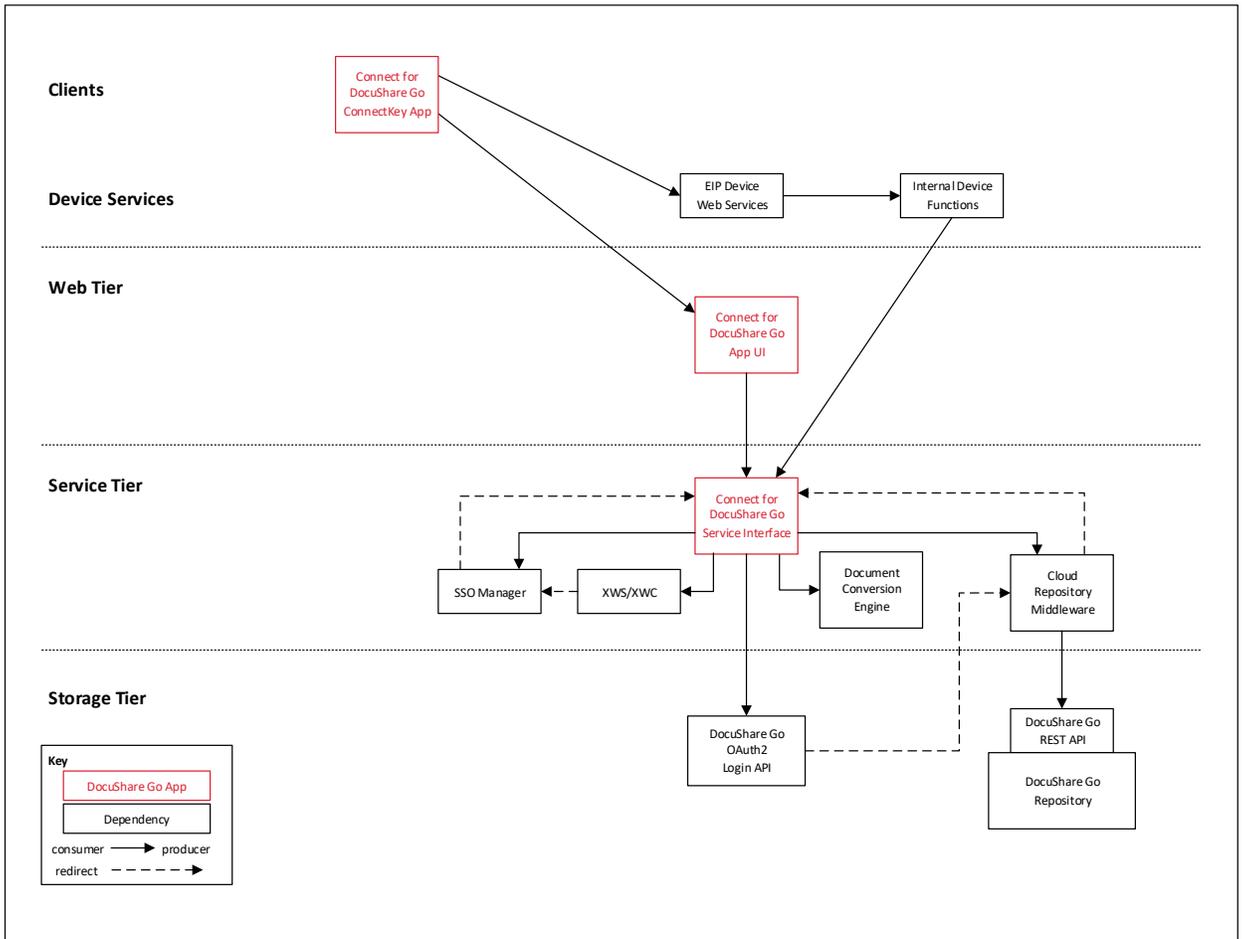
The Cloud Repository Middleware component is a service hosted on the Microsoft Azure Cloud System. The Cloud Repository Middleware interfaces with the DocuShare Go REST APIs to access the DocuShare Go repository. The Cloud Repository Middleware also interfaces with the Xerox® Document Conversion Engine, which converts non-printable document formats into printable document formats.

Xerox® Document Conversion Engine

The Document Conversion Engine component is a service hosted on the Microsoft Azure Cloud System. The Document Conversion Engine converts a variety of document formats to a format that is printable by Xerox® devices.

ARCHITECTURE AND WORKFLOWS

Architecture Diagram



Workflows

App Printing Workflow



Step 1: Launch the App on the Xerox device.



Step 2: User authenticates to the DocuShare Go 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.)



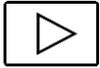
Step 3: User navigates the folder structure to locate the file to be printed.



Step 4: User optionally selects to Preview the document to be printed.



Step 5: User selects a file and modifies the print options (ie; single sided, etc...).



Step 6: User selects the Print button to print their file at the device.

App Scanning Workflow



Step 1: User Launches the App on the Xerox device.



Step 2: User authenticates to the DocuShare Go 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 destination folder for the scanned document.



Step 4: User modifies the scanning options (ie; 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 Scan 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.

3. 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