

Xerox Security Guide

Xerox® Connect App for Google Drive™



© 2026 Xerox Corporation. All rights reserved. Xerox®, Xerox Extensible Interface Platform® and ConnectKey® are trademarks of Xerox Corporation in the United States and/or other countries.
BR42549

Other company trademarks are also acknowledged.

Document Version: 1.3 (April 2026).

Contents

1. Introduction	1-1
Purpose	1-1
Target Audience	1-1
Disclaimer	1-1
2. Product Description	2-2
Overview	2-2
CONFIGURING APP SETTINGS	2-2
App Hosting	2-3
Components	2-3
Architecture and Workflows	2-5
Data flow Diagram	2-5
User Data Protection	2-9
Authentication and Cloud Repository Access	2-9
Application data stored in the Xerox cloud	2-9
Delete Events	2-10
Local Environment	2-10
3. Network Information	3-11
Protocol, Ports and URLs	3-11
Use of SNMP when operating the App (Xerox Models Only)	3-12
Use of SNMP when installing the App (Xerox Models only)	3-12
4. General Security Protection	4-13
User Data Protection within the products	4-13
Document and File Security	4-13
Hosting - Microsoft Azure	4-13
Cloud Storage – Microsoft Azure	4-13
Xerox® Workplace Suite/Cloud and Single Sign-On Services (Xerox models only)	4-13
User Data in transit	4-14
Secure Network Communications	4-14
Xerox Workplace Suite/Cloud and Single Sign-On Services (Xerox models only)	4-14
5. Additional Information & Resources	5-15
Security @ Xerox	5-15
Responses to Known Vulnerabilities	5-15

Additional Resources 5-15

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 Google Drive™ consists of two primary workflows. The two workflows are:

- Print files from a Google Drive account
- Scan files to a Google Drive account

The app and two workflows facilitate a combination of the following steps:

- Single Sign-On – Only on Xerox Models
- Authentication
- App Hosting
- Repository Navigation
- Scanning
- Printing
- Document Format Conversion
- Emailing
- SNMP & Device Webservice Calls

Application	What can I do?
Xerox® Connect App for Google Drive™	<ul style="list-style-type: none">• Login to my Google account• Select Print or Scan workflow• Navigate to a folder in my Google Drive account• Scan a hard copy document to a folder in my Google Drive account with standard scan settings along with option to email the scanned document• Select one or more files in my Google Drive account and Print hard copies with standard print settings

Table 1 Xerox® App user benefits

CONFIGURING APP SETTINGS

Xerox® Connect App for Google Drive™ provides the following set of configurable settings to customize before installation. If unmodified, the app will use the default setting.

Searchable PDF: Defines the default PDF settings to be searchable, converting the scanned document into selectable text.

SNMP V1/V2 Community Name: The string used to identify which group of users can access SNMP data on a device. This is applicable to Xerox models only.

Enable Mobile Login: If enabled, the app will provide the user with the option of choosing a device or mobile login method. For Lexmark models only mobile login method is applicable.

Enable Print Workflow: If enabled, the app will provide the user with the option of choosing a Scan or Print workflow.

APP HOSTING

The Xerox® Connect App for Google Drive™ depends heavily on cloud hosted components. A brief description of each can be found below.

The Xerox® Connect App for Google Drive™

The Xerox® App consists of two key components, the device weblet and/or a flash file and the cloud-hosted web service. The device weblet is an EIP web app on Xerox models and the flash file is an eSF app on the Lexmark models that enable the following behavior on a Xerox or a Lexmark device:

- Presents the user with an application UI that executes functionality in the cloud.
- Interfaces with the Xerox® Extensible Interface Platform (EIP) API and/or Lexmark Embedded Solutions Framework (eSF) API, which delegate work, such as document scanning and printing.

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

Google Drive Storage Service

For the app to communicate and interact with the correct storage location, the user needs to establish a connection with their Google Drive repository. This connection process utilizes the authentication dialog provided by the storage service. The authentication dialog requests the username and password needed to access Google Drive content.

Single Sign-On via Xerox® Workplace Suite/Cloud and SSO Manager (Xerox models only)

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.

Lexmark Embedded Solutions Framework® (eSF) (Lexmark models only)

During standard usage of the Xerox® App on a Lexmark device, eSF calls to services and workflow managers are made to initiate and monitor print and scan functions and to identify device configuration and capabilities.

COMPONENTS

MFD with Xerox® Connect App for Google Drive™ – ConnectKey App

This is an EIP and or eSF 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 App for Google Drive installed.

The MFD communicates with the App Service, Middleware Service, App Gallery Service, and Google Authentication Service.

Xerox® Connect App for Google Drive™ – 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® or a Lexmark 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.

Xerox 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 Google Authentication Service and Google Drive API.

The Cloud Repository Middleware also interfaces with the Document Conversion Engine from Xerox, which converts non-printable document formats into printable document formats.

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® or Lexmark Devices.

Xerox App Gallery

The App Gallery component is a web application, with services hosted on the Microsoft Azure Cloud System. The App Gallery is accessed to ensure the Application is entitled to run. The application can only be run when a “Trial” license has not expired OR a “Purchased” license has not expired.

After an entitled weblet is installed on a device, App initialization will contact App Gallery:

- to ensure the Application is entitled to run on the device.
- to retrieve App Gallery App Configuration parameter values set by an App Gallery user.

File Conversion Service

The File Conversion API component is a VM 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 accepts requests from the App Service.

Twilio SendGrid API

The Twilio SendGrid API is a, 3rd Party, cloud hosted service. The Twilio SendGrid API is used to email scanned documents as attachments.

Xerox Mobile Login Service

The Mobile Login component is a service hosted on the Microsoft Azure Cloud System. It is responsible for interfacing with the Connect App API and the User’s mobile phone browser. It provides a path for user login at the MFD utilizing the authentication dialog provided by Google, displayed on the user’s mobile phone.

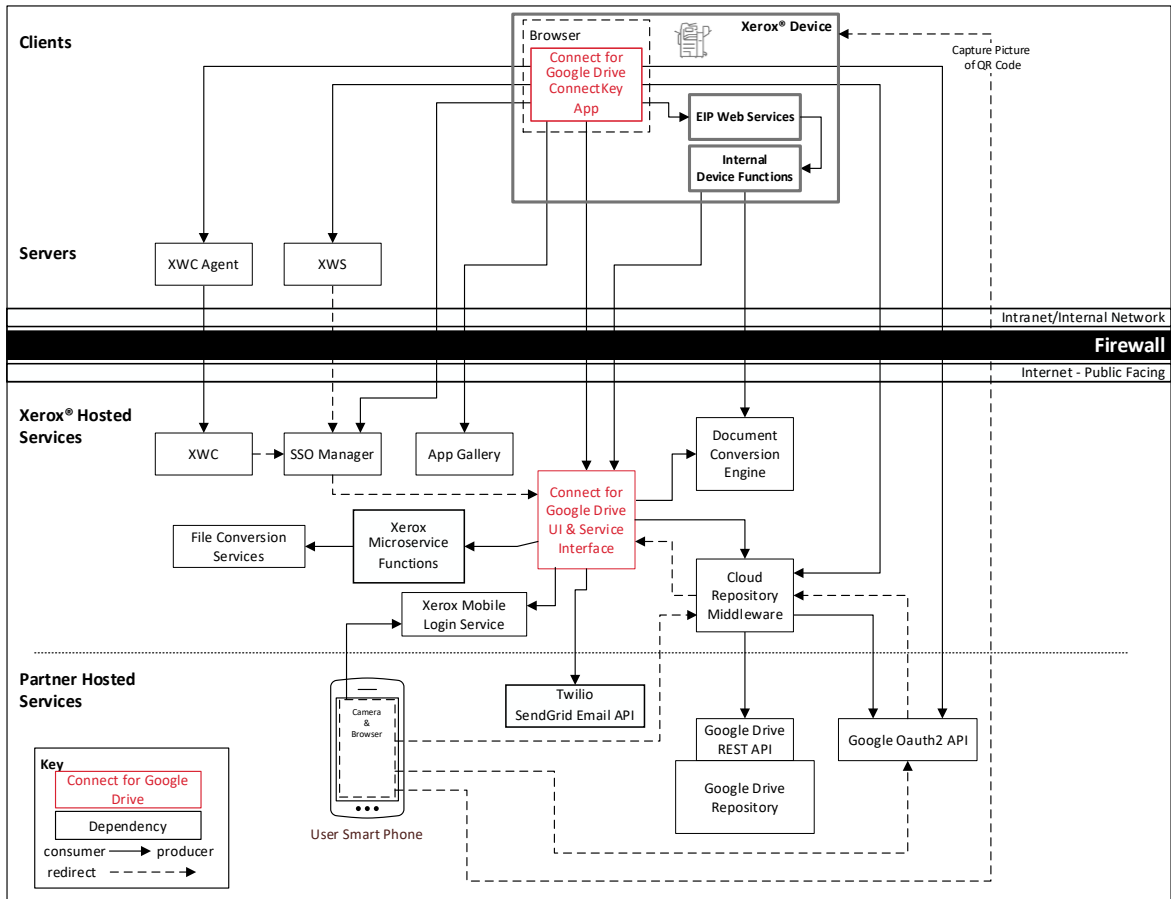
User’s mobile phone browser

A QR Code displayed on the MFD’s screen will retrieve and display the login URL from the Xerox Mobile Login service, The user’s browser displays the Google authentication dialog and interfaces with the Google OAuth2 API, providing the login result redirect.

Architecture and Workflows

DATA FLOW DIAGRAM

Xerox® Workplace Suite & Workplace Cloud Single Sign On Architecture (Xerox models only)



Workflows

Authentication Workflow – Local Authentication (Xerox models only)

- Step 1:** User selects local authentication.

- Step 2:** User authenticates to the Google Drive repository directly on the device.

Authentication Workflow – Mobile Login

- Step 1:** User selects Mobile Login.

- Step 2:** QR Code is displayed on the device.

- Step 3:** User scans QR Code with their mobile phone.

- Step 4:** User completes Google Drive repository authentication process on their mobile phone.

App Printing Workflow

- Step 1:** User Launches the App on the Xerox® or Lexmark Device.

- Step 2:**
 - Xerox Models:** User authenticates to the Google Drive repository using local or mobile login authentication. (If first login, user can agree to save credentials to Xerox® Workplace Suite/Cloud storage for future use. On subsequent logins, credentials are automatically retrieved and applied.)
 - Lexmark Models:** User authenticates to the Google Drive repository using mobile login authentication.

- 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 a Xerox® or Lexmark Device.

Step 2: **Xerox Models:** User authenticates to the Google Drive repository local or mobile login authentication. (If first login, user can agree to save credentials to Xerox® Workplace Suite/Cloud storage for future use. On subsequent logins, credentials are automatically retrieved and applied.)

Lexmark Models: User authenticates to the Google Drive repository mobile login authentication

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, email, 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: If the Email option was selected in Step 4, the scanned document is emailed to the specified recipients.

Step 8: The document is saved to the selected destination folder.

Build Job Workflow

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

- Xerox Models:** User authenticates to the Google Drive repository using either Local Authentication or Mobile Login workflow. (If first login, 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 2:** **Lexmark Models:** User authenticates to the Google Drive repository using the Mobile Login workflow.
- 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, email, etc...).
- Step 5:** User selects the Scan button to scan the document to the selected folder.
- Step 6:** If the Build Job option was selected in Step 4, the user may choose to scan another batch, process all batches as a single file, or cancel the build job and start over.
- Step 7:** After processing all batches, 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 Google repository, the user is required to authenticate with their Google login credentials. The protocol used to authenticate is OAuth 2.0. The authentication process is hosted and controlled by Google. An authentication dialog provided by Google, requests the username and password. Additional data may be required if 2-Factor authentication is enabled.

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 Google. 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 Google API with a valid Access token to access the user's data in the Google repository.

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

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 Google Drive account
- Scan preview images
- Print preview images
- Scan documents converted to MS Office formats

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.
- A delete occurs when the system detects that a document conversion job has completed, and the converted document has been downloaded.

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 activities will trigger a delete event, for the original digital document files and the converted document file.

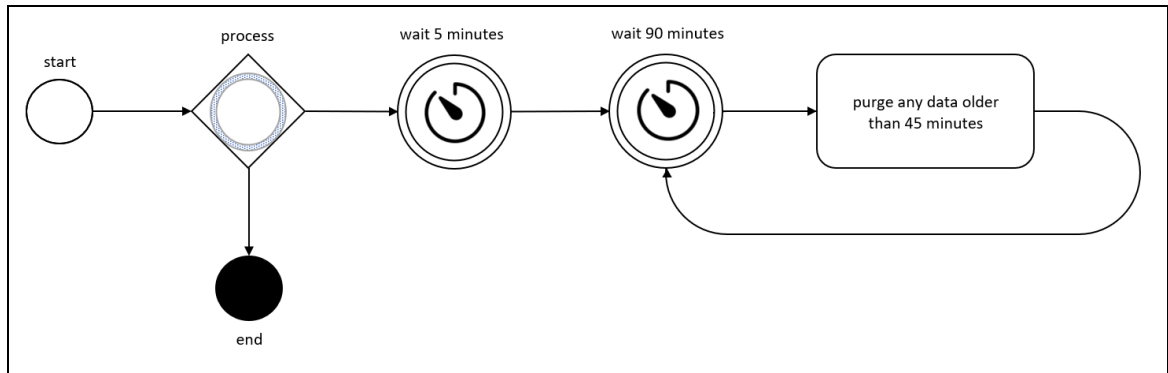
- A delete occurs when the system detects that the document conversion job has completed, and the converted document has been downloaded.

DELETE EVENTS

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

Purge documents timer job

The timer host is an Azure Function App trigger. 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.



LOCAL ENVIRONMENT

Application data transmitted

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

- Account data
- Session data
- Job data

Application data stored on the Xerox® Device

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

- Device's SNMP V2 public community string

HTTP Cookies

The Xerox® Connect App for Google Drive™ 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 for Google Drive™ App 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 Google Drive App Service	c2a-o365-web.services.xerox.com
HTTPS using TLS	TCP 443	App Configuration	ConnectKey App to App Gallery	appgallery.services.xerox.com
HTTPS using TLS	TCP 443	Subscription Entitlement	ConnectKey App to App Gallery	entitlements-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 Google OAuth2 API	accounts.google.com
HTTPS using TLS	TCP 443	Single Sign On (SSO)	ConnectKey App to SSO Manager	ssomanager.services.xerox.com
HTTPS using TLS	TCP 443	Printing Converted Documents	Xerox® Device to Document Conversion Engine	xmpcws.services.xerox.com

Protocol	Transport and Port Value	Use	Component	URL
SNMP (Xerox models only)		Device capability discovery Public read Internal pathway use only Complies with the SNMP v2 data model	ConnectKey App initialization	localhost

Use of SNMP when operating the App (Xerox Models Only)

The App does not use the SNMP protocol while in use, so it is perfectly fine to disable SNMP connectivity if that protocol is not otherwise required by another app or service.

IMPORTANT: The App does interrogate MFD SNMP OIDs over an internal channel. That internal channel is independent and unrelated to the SNMP network connectivity protocol setting. Consequently, the SNMP V1/V2 Community READ String must be set.

The default SNMP V1/V2 Community READ String value is “public”.

The internal SNMP channel is enabled when the EIP SNMP Web Service setting is enabled. This setting must be enabled to operate the App as it was designed. The V1/V2 READ string setting is still required by the EIP SNMP Web Service even when the V1/V2 protocols are disabled by the MFD administrator.

Presuming the EIP SNMP Web Service setting is enabled, and the SNMP V1/V2 Community READ Name matches the App’s SNMP V1/V2 Community Name, then the SNMP queries executed by the App over the internal channel will be successful.

Use of SNMP when installing the App (Xerox Models only)

App Gallery and potentially other deployment tools may use the SNMP protocol when discovering MFDs on the network during device discovery. If SNMP dependent tools are not used when deploying the App across a fleet, then it is not required to enable any version of the SNMP protocol after the MFD administrator sets the V1/V2 READ string using supported device configuration methods.

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 Microsoft Azure data centers located in Ireland and the United States. For users located in North America, Central America and the Caribbean the documents are temporarily held in the storage account hosted in the United States. For users located in the rest of the world, the documents are temporarily held in the storage account hosted in Ireland.

For a full description, please follow these links:

Azure Storage

<https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>
<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 (XEROX MODELS ONLY)

The Xerox® ConnectKey App 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 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 Xerox® Connect App for Google Drive™ 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 (XEROX MODELS ONLY)

The Xerox® Workplace Suite/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 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.

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/
Xerox Trust Center	https://trust.corp.xerox.com/

Table 2 Additional Resources