Xerox® Security Guide

Xerox® Note Converter

xerox™

Document Version: 1.0 (October 2019).

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. 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 and the files produced 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 and Azure SQL 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/updates/newly-created-azure-sql-databases-encrypted-by-default/

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 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® solution 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.

With the exception of creating an administration account, the Xerox® apps require 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.

3. Xerox® Note Converter – ConnectKey App

Description

Overview

This Xerox® solution delivers two separate software offerings, each aligning to meet specific user goals. This section applies to the ConnectKey App.

The ConnectKey App is a simple document conversion solution for your Xerox® device that assists the user with converting a handwritten document into digital files, which are delivered via an email message sent to the provided recipient.

Table 1. ConnectKey App user benefits

Application	What can I do?
ConnectKey App	Login
	Scan a paper document, which will email the digitized original and editable results to the intended recipient

App Hosting

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

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.

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

Google Cloud Vision API
The solution depends on the Google Cloud Vision API to convert digitized handwritten documents into document files that are editable. All requests are made over HTTPS.

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® Note Converter – ConnectKey App
This is an EIP capable device that can scan and execute ConnectKey Apps installed from the Xerox® App Gallery. In this case, the device has the Xerox® Note Converter installed.

Xerox® Note Converter – Web App
The Web App is responsible for hosting the web pages, which are displayed on the UI of the printer.

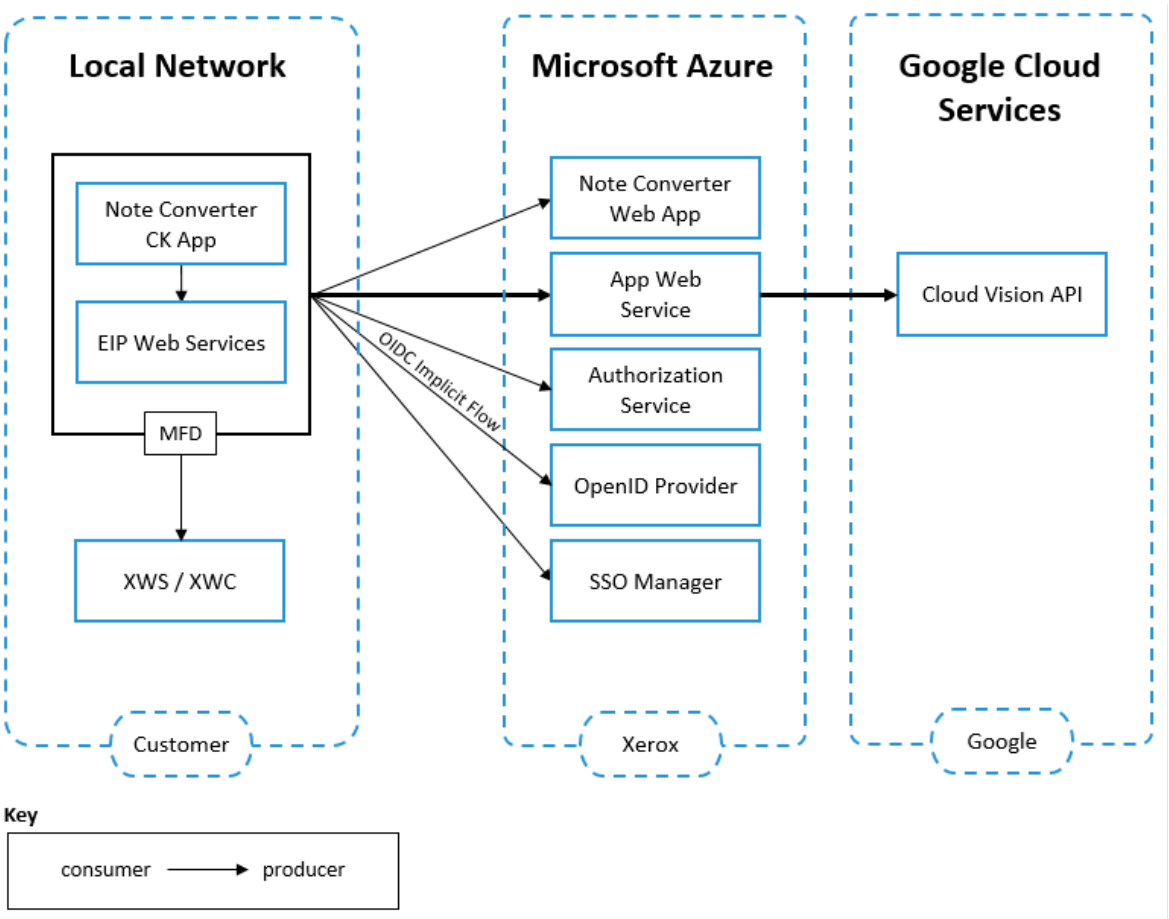
Xerox® Note Converter – Web Service
The Web Service is a service hosted on the Microsoft Azure Cloud System. The service provides the web API support for Xerox® apps. The web service interacts with Google Cloud using the Cloud Vision APIs and Microsoft services using the Azure APIs.

Google Cloud Vision API

The Google Cloud hosted service provides a web API that is used by the file conversion process. The API accepts image input for processing and returns a response, which contains text content and its associated metadata.

Architecture and Workflows

Architecture Diagram



Workflows

Prerequisite – Create a Xerox Apps administrator account by activating the subscription

See Section 4: Workflows – Activate my App subscription.

Login

Step 1: Launch the App on the Xerox device.

Step 2: Complete and submit the Login form.

Step 3: When the SSO configuration is enabled, optionally agree to save the credentials for future use.

Scan a paper document

Step 1: Launch the App on the Xerox device.

Step 2: Login to view the Main page.

Step 3: Provide and confirm the workflow recipient's email address.

Step 4: Optionally modify the document file title.

Step 5: Optionally change the scan settings.

Step 6: Submit the job using the Scan button.

Retrieve my document files

Step 1: Open the Note Converter email message received, which is associated with your job.

Step 2: Open the document file attachments provided in the email message.

The OS will handle the document file content using the application associated with the file extension.

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 delete event occurs.

- Session data
- Job data
- Document data

The following activities will trigger a delete event, for all data that is classified to contain Personally Identifiable Information (PII).

- The App Subscription Administrator visits the Web Portal and deletes their own account.
- The App User visits the Web Portal and deletes their own account.

The following activities will trigger a delete event, for cloud 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 PII, 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
- Document 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 data
- Configuration data

HTTP Cookies
The ConnectKey App stores a combination of persistent and non-persistent cookies on the device. The cookies are secure, which will only be communicated over a TLS channel.

Table 2. ConnectKey App related cookies

Secure Cookie Name Domain	Persistent	Purpose
x-ms-cpim-csrf b2clogin.com	No	Cross-Site Request Forgery token used for CRSF protection.
x-ms-cpim-cache:{id}_n b2clogin.com	No	Used for maintaining the request state.
x-ms-cpim-trans b2clogin.com	No	Used for tracking the transactions (number of authentication requests to Azure AD B2C) and the current transaction.
x-ms-cpim-sso:{id} b2clogin.com	No	Used for maintaining the SSO session.
Identity.External *.services.xerox.com	No	Used for maintaining the external authentication claims state.
.AspNetCore.OpenIdConnect.Nonce.* *.services.xerox.com	Yes valid 1 hour	Provides protection against replay attacks.
.AspNetCore.Correlation.DeviceApps.* *.services.xerox.com	Yes valid 1 hour	Used to identify authenticated users by tracking the current login event.

4. Xerox® Note Converter – Web Portal

Description

Overview

This Xerox® solution delivers two separate software offerings, each aligning to meet specific user goals. This section applies to the Note Converter web portal.

The web portal is an account administration solution for customers that supports:

1. User profile management
2. Subscription accounts management

Table 3. Web Portal user benefits

Application	What can I do?	Notes
Web Portal	Activate my App subscription	Via an email link
	Create my Apps account	Via an email link
	Login	
	Update my Apps account profile information	
	Reset my password	
	Change my password	
	Delete my Apps account	
	Invite a user to enroll as an App user	An Admin-only feature
	Grant or revoke subscription admin privileges	An Admin-only feature
	Remove a member user account	An Admin-only feature

App Hosting

The web portal is a cloud hosted website. A brief description can be found below.

The solution supports linking any Apps account to an App's subscription license. The subscription activation step creates the first link between an Apps account and its subscription license. Afterwards, the account used to activate the subscription becomes the first subscription administrator and may use the portal to invite others, delegate subscription administration, revoke application access, maintain their account profile, and permanently delete their Apps account when they no longer need it.

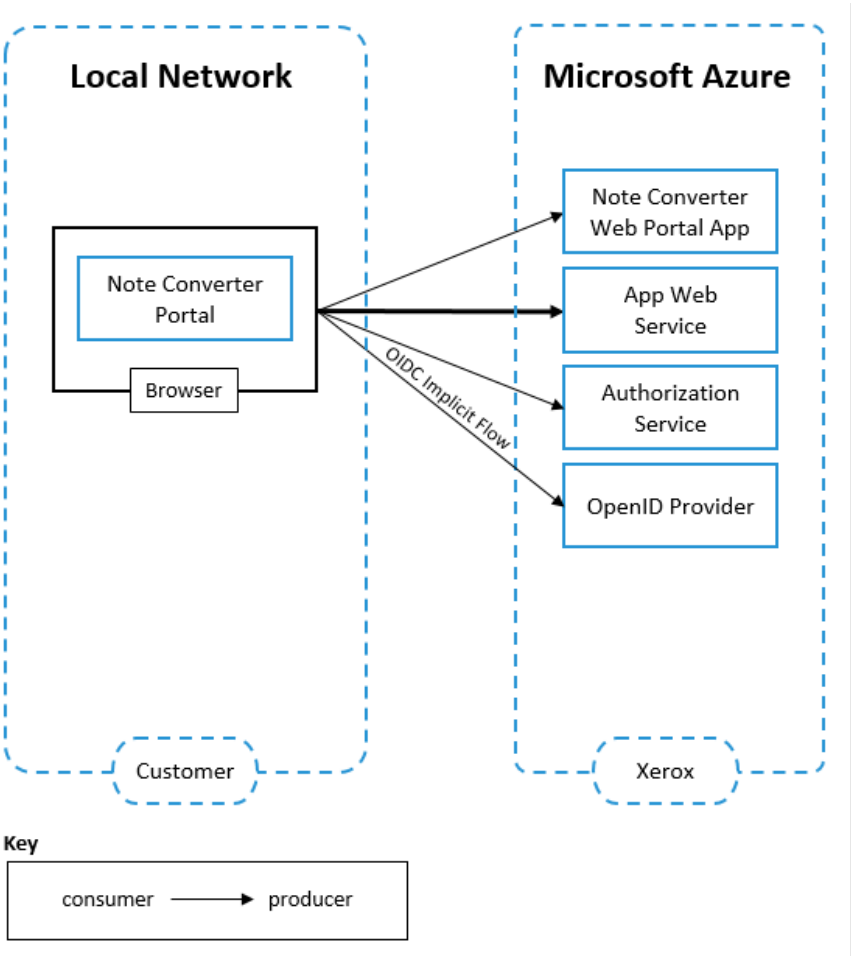
Components

Xerox® Note Converter – Portal Web App
The Web Portal provides support for maintaining sub-accounts linked to the App subscription. The portal is a browser based app that presents to the user functionality that is executed in the cloud.

Xerox® Note Converter – Portal Web Services
The Portal Web Services are hosted on Microsoft® Azure. The services are responsible for processing administrative requests sent from the web app.

Architecture and Workflows

Architecture Diagram



Workflows

Activate my App subscription (Via an email link)

Step 1: Open the App Product Key email received.

Step 2: Activate the Administrator Account Setup button link provided in the email message to navigate to the App account sign-up page.

The OS will handle the link content using the application associated with the handling web links.

Step 3: Verify your email address and complete your profile details.

Step 4: Activate the Create button to create your account and transition to your account's home page.

Create my Apps account (Via an email link)

Step 1: Open the App account invitation email received, which is linked to the App administrator's subscription.

Step 2: Activate the Create Account button link provided in the email message to navigate to the App account sign-up page.

The OS will handle the link content using the application associated with the handling web links.

Step 3: Verify your email address and complete your profile details.

Step 4: Activate the Create button to create your account and transition to your account's home page.

Login

Step 1: Find your Product Key email or your Account Invitation email and use the contained button link to sign up if you have not created an account.

Step 2: When you have your account credentials available, open a web browser and navigate to the web portal URL.

Step 3: Complete and submit the Login form to reveal your account home page.

Update my Apps account profile information

Step 1: Open a web browser and navigate to the web portal URL.

Step 2: Login to reveal your account's home page.

Step 3: Modify your profile details.

Step 4: Activate the Save button to save your changes.

Reset my password

Step 1: Open a web browser and navigate to the web portal URL.

Step 2: Activate the Forgot Password link so you can begin the password reset process.

Step 3: Verify your email address and complete the password reset form.

Step 4: Complete and submit the Reset Password form and transition to your account's home page.

Change my password

Step 1: Open a web browser and navigate to the web portal URL.

Step 2: Login to reveal your account's home page.

Step 3: Activate the Account Profile menu to reveal the action menu.

Step 4: Activate the Change Password link so you can begin the password reset process.

Step 5: Verify your email address and complete the password reset form.

Step 6: Complete and submit the Reset Password form and transition to your account's home page.

Delete my Apps account

Step 1: Open a web browser and navigate to the web portal URL.

Step 2: Login to reveal your account home page.

Step 3: As a basic user, activate the Delete button found on your account home page to remove your account and navigate back to the Login page.

As an admin user, activate the Account Details link under your Profile menu to reveal your profile information. Then activate the Delete button to remove your account and navigate back to the Login page.

All personal cloud data associated with the deleted account will be permanently destroyed.

Invite a user to enroll as an App user (Admin-only)

Step 1: Open a web browser and navigate to the web portal URL.

Step 2: Login to reveal your account's home page.

Step 3: Activate the Invite button so you can provide and submit the invitation recipient's email address.

An invitation containing an account setup link will be sent to the email address provided.

Grant or revoke subscription admin privileges (Admin-only)

Step 1: Open a web browser and navigate to the web portal URL.

Step 2: Login to reveal your account home page.

Step 3: Select the account you want to modify and activate the Edit Role button.

Step 4: Select the new role and accept the changes.

Remove a member user account (Admin-only)

Step 1: Open a web browser and navigate to the web portal URL.

Step 2: Login to reveal your account home page.

Step 3: Select the accounts you want to remove and activate the Delete button.

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 delete event occurs.

- Account data

The following activities will trigger a delete event, for all data that is classified to contain Personally Identifiable Information (PII).

- The app user visits the web portal and deletes their account.

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

Local Environment

Application data transmitted
The following app data is transmitted to/from the host device.

- Account data
- Session data
- Feature related data

Application data stored on the host file system
The web portal does not store any data on the host device.

HTTP Cookies

The Web Portal stores a combination of persistent and non-persistent cookies on the PC. The cookies are secure, which will only be communicated over a TLS channel.

Table 4. Web Portal related cookies

Secure Cookie Name Domain	**Persistent**	**Purpose**
x-ms-cpim-csrf b2clogin.com	No	Cross-Site Request Forgery token used for CRSF protection.
x-ms-cpim-cache:{id}_n b2clogin.com	No	Used for maintaining the request state.
x-ms-cpim-trans b2clogin.com	No	Used for tracking the transactions (number of authentication requests to Azure AD B2C) and the current transaction.
x-ms-cpim-sso:{id} b2clogin.com	No	Used for maintaining the SSO session.
Identity.External *.services.xerox.com	No	Used for maintaining the external authentication claims state.
.AspNetCore.OpenIdConnect.Nonce.* *.services.xerox.com	Yes valid 1 hour	Provides protection against replay attacks.
.AspNetCore.Correlation.DeviceApps.* *.services.xerox.com	Yes valid 1 hour	Used to identify authenticated users by tracking the current login event.

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

Table 4. Below are 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/