Security Guide

Xerox® Workflow Central Platform

Document Version: 3.0 (September 2023).

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 – Web Application

Overview

This solution delivers 2 separate software offerings, each aligning to meet specific user goals. This section applies to the Web App which is run from a compatible web browser on a PC, Tablet, Laptop computer or Mobile phone.

The Xerox® Workflow Central Platform provides multiple workflows for the logged in customer based on their account privileges.

Application	What can I do?
Web App	• Create an account • Login to my account • Purchase a subscription • Manage user access to a subscription • Customize workflow settings • View available document workflows • Execute a document workflow • Save a customized document workflow • Create automated workflows • View and manage automated workflows • View and manage protected documents • Execute a document workflow from the Xerox® Print and Scan Experience App.

Table 1 Web App user benefits

APP HOSTING

The Web App consists completely of cloud hosted components that are accessed via a web browser. A brief description of each can be found below.

Web App

The Web App consists of three key components, the Web App User Interface, the Workflow Central Platform User Interface and Service Interface, the Workflow Central Platform Microservices Interface and the App Cloud Connector. These components enable the following behavior in a web browser:

1. Provides the user with the application UI that executes functionality in the cloud.
2. Executes Microservices, which delegates work such as document format conversion and language translation.
3. Provides interfaces, for Automated Workflows, with 3rd party cloud repository and Email services

Xerox App Gallery

The App Gallery component is a web application hosted on the Microsoft Azure Cloud System. The App Gallery Component implements the following functions for the Xerox® Workflow Central Platform Web App: Authentication, Account Creation, Account Management, Access List Management, Access Authorization, App Subscription Purchase, App Subscription Management, and CK App Installation on Xerox® Devices.

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 following commercial cloud repository providers: Xerox® DocuShare® Go Content Management Platform, Microsoft (OneDrive and O365 SharePoint), Google Drive, Dropbox, and Box.

For the Xerox® Workflow Central Platform to communicate and interact with a specific cloud repository provider, the user needs to establish a connection. This connection process utilizes an OAuth 2.0 login workflow provided by the cloud repository provider, which requests the username and password. Upon successful authentication, an OAuth access token is returned to the browser from the cloud repository. The access token is passed to the Cloud Repository Middleware for use when calling a cloud repository provider's API. The access token is never stored.

NOTE: *For security purposes, some Microsoft Azure AD Tenants may be configured to require an Azure AD administrator to grant access to any application before it can be used by any of their users. The following URL can be accessed by an Azure AD Administrator to grant access within their Azure AD Tenant: https://cloudmiddleware.services.xerox.com/azuread/adminconsent.aspx*

Xerox® Translates Service

The Xerox® Translates Service component is a set of translation APIs hosted in the Microsoft Azure Cloud System. The Web App uses the API to translate documents into a different language while maintaining the layout and format of the original document.

Xerox® Auto-Redaction App

The Xerox® Auto-Redaction App component contains a set of document redaction APIs hosted in the Microsoft Azure Cloud System. The Workflow Central Platform uses the API to generate a document with a set of specified data redacted from the original document.

Xerox OCR Service

The Xerox OCR Service component is a set of document format conversion APIs hosted in the Microsoft Azure Cloud System. The Workflow Central Platform uses the API to convert documents into one of the following Microsoft formats: DOCX, PPTX or XLXS.

ABBYY Cloud OCR Service

The ABBYY Cloud OCR Service component is a set of partner, cloud hosted Optical Character Recognition (OCR) and document format conversion APIs.

Microsoft Translator Service

The Microsoft Translator Service component is a set of partner, cloud hosted language translation APIs.

Zamzar Audio Service

The Zamzar Audio Service component is a set of partner, cloud hosted audio file conversion APIs. The Workflow Central Platform uses the Zamzar Audio API to convert a document into an Audio file.

Google Vision Service

The Google Vision Service component is a set of partner, cloud hosted OCR APIs. The Workflow Central Platform uses the API to generate editable text documents from an image of a handwritten document.

Google DLP Service

The Google DLP (Data Loss Prevention) Service component is a set of partner, cloud hosted document analysis and redaction APIs.

SummarizeBot Service

The SummarizeBot Service component is a set of partner, cloud hosted document summarization APIs. The Workflow Central Platform uses the API to generate summarized documents.

RPost RMail Service

The RPost RMail Service component is a partner, cloud hosted email services platform. The Workflow Central Platform uses the RMail API to send Registered and Encrypted email when it is specified in a document workflow.

RPost RDocs Service

The RPost RDocs Service component is a partner, cloud hosted document protection platform. The Workflow Central Platform uses the RDocs API to create and send protected (encrypted) documents. The RDocs API is also used for the viewing and controlling access to the protected documents (via the Active Documents feature) created by a Workflow Central Platform user.

OpenText XM Fax Service

The OpenText XM Fax Service component is a partner, cloud hosted Fax service platform. The Workflow Central Platform uses the Cloud Fax API to send a document as a Fax.

Twilio SendGrid Email Service

The Twilio SendGrid Email Service component is a partner, cloud hosted email services platform. The Workflow Central Platform uses the SendGrid API to send email when it is specified in a document workflow.

COMPONENTS

Xerox® Workflow Central Platform – UI & Services Interface

The UI & Service Interface component is a service hosted on the Microsoft Azure Cloud System. The component is responsible for hosting the web pages, which are displayed in the User's web browser on their PC. Additionally, the component provides user access and management, business logic services, workflow management and execution, and the Workflow Central Platform APIs.

Xerox® Workflow Central Platform – Microservices

The Microservices component is a set of Microsoft Azure Functions hosted on the Microsoft Azure Cloud System. The various microservices interface with a host of third-party APIs to perform specific operations like Audio Conversion, Translation, Format Conversion, OCR, Summarization and Email.

Xerox App Cloud Connector

The App Cloud Connector component is a service hosted on the Microsoft Azure Cloud System. The App Cloud Connector interfaces with the following commercial cloud repository providers: Microsoft (OneDrive and O365 SharePoint) and Google Drive.   The App Cloud Connector also interfaces with Microsoft Exchange Online.

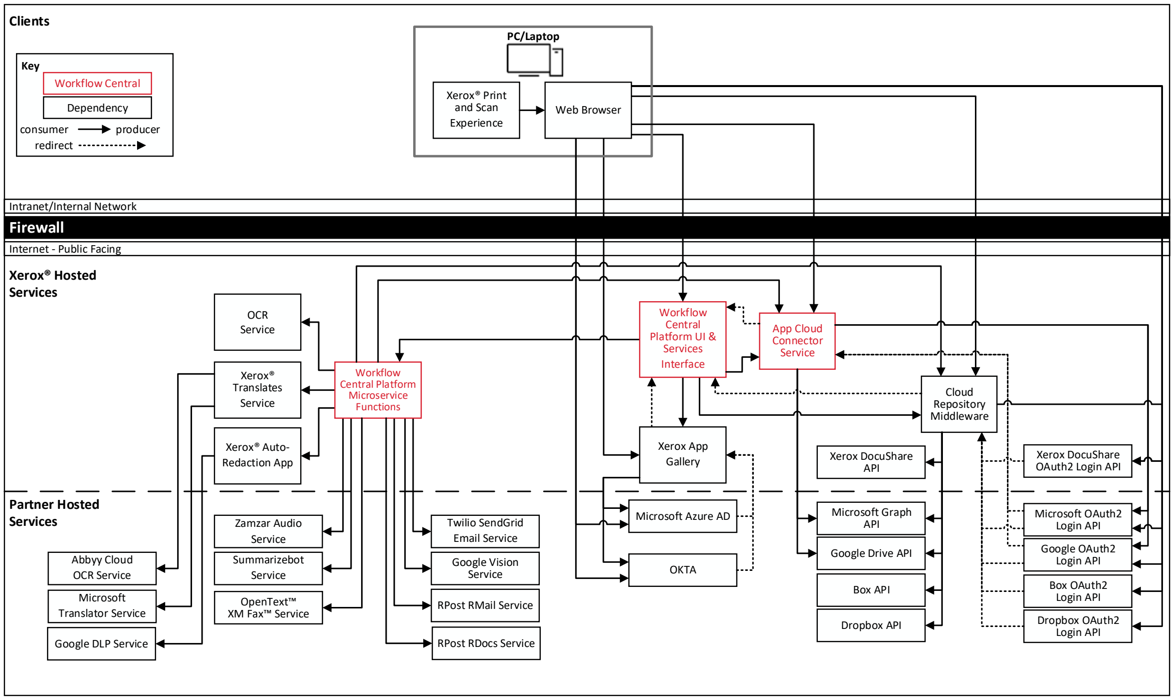
When creating an automated workflow, the user needs to authenticate with a supported commercial cloud service. This authentication process utilizes an OAuth 2.0 login workflow provided by the commercial cloud service, which requests the username and password. Upon successful authentication, an OAuth access token and refresh token are returned to the App Cloud Connector. The App Cloud Connector encrypts and stores the tokens in Microsoft Azure Cloud Storage using unique encryption keys stored in a Microsoft Azure Key Vault. An App Cloud Connector access token is returned to the browser which is used to access the configured commercial cloud service while creating or updating an automated workflow.

When an automated workflow is saved by the user, the associated App Cloud Connector's access token is stored in encrypted Microsoft Azure Cloud Storage. The App Cloud Connector access token is then used to access the configured commercial cloud service whenever the automated workflow executes.

NOTE: *For security purposes, some Microsoft Azure AD Tenants may be configured to require an Azure AD administrator to grant access to any application before it can be used by any of their users. The following URL can be accessed by an Azure AD Administrator to grant access within their Azure AD Tenant:*
https://xeroxappcloudconnector.services.xerox.com/MSGraph/AdminConsent

Architecture and Workflows

DATA FLOW DIAGRAM



WORKFLOWS

Create Account

Step 1: User enters the URL for the Web App in a web browser on their PC/Laptop/Tablet.

Step 2: User selects the “Try or Buy from the Xerox App Gallery” button.

Step 3: User selects the “Login” button.

Step 4: User selects the “Create Account” link in the Login dialog.

Step 5: User enters required information for Account Creation and selects OK button.

Step 6: User receives an email with instructions on how to complete the creation of their account.

Step 7: User opens the email and clicks on a link to complete the creation of their account from the web browser on their PC/Laptop/Tablet or Mobile Phone.

Purchase Subscription

Step 1: User enters the URL for the Web App in a web browser on their PC/Laptop/Tablet or Mobile Phone.

Step 2: User selects the “Log In” button and enters their account username and password.

Step 3: User selects the “Try or Buy from the Xerox App Gallery” button.

Step 4: User selects the Plan they wish to purchase.

Step 5: User chooses the “Subscription Duration” and “Subscription Plan” and then selects the “Checkout” button.

Step 6: User enters Payment information and selects the “Place Order” button.

Step 7: An order confirmation with order number is displayed.

Step 8: User receives an email with a payment receipt.

Add User Access to Subscription

Step 1: User enters the URL for the Web App in a web browser on their PC/Laptop/Tablet or Mobile Phone.

Step 2: User selects the “Log In” button and enters their account username and password.

Step 3: User navigates to the “Users” page and selects the “Invite” button to provide access to the subscription for another user.

Step 4: User enters the email address of the user whom they wish to grant access to the App subscription.

Step 5: The invited User receives an email informing them that they have been granted access to the App subscription along with a link to create an account.

Step 6: Invited User opens the email and clicks on a link to complete the creation of their account from the web browser on their PC/Laptop/Tablet or Mobile Phone.

Customize workflow settings

Step 1: User enters the URL for the Web App in a web browser on their PC/Laptop/Tablet or Mobile Phone.

Step 2: User selects the “Log In” button and enters their account username and password.

Step 3: User selects the “Workflow Settings” icon in the Workflows page.

Step 4: User chooses which workflows are to be hidden or displayed, in the Workflows tab of the “Workflow Settings” dialog box,

Step 5: User selects “Features” tab, in “Workflow Settings” dialog box and chooses which features to enable or disable for all workflows.

Step 6: User selects “OK” button to save the “Workflow Settings”.

Execute a Document Workflow

Step 1: User enters the URL for the Web App in a web browser on their PC/Laptop/Tablet or Mobile Phone.

Step 2: User selects the “Log In” button and enters their account username and password.

Step 3: The Web App displays the “Single” document workflows available for execution by the user.

Step 4: User either selects a document workflow to execute or navigates to the “Combination” document workflows and selects a document workflow to execute.

Step 5A: If “Local Drive” is chosen as the location for input file selection, the User navigates to and selects the input file(s) for the document workflow.

Step 5B: If a “Cloud Repository” is chosen as the location for input file selection, the User first authenticates with the chosen “Cloud Repository” then navigates to and selects the input file(s) for the document workflow.

Step 6: User modifies the settings for each operation defined in the document workflow

Step 7: User defines one or more output destinations to specify where the output from the document workflow will be sent. (Download, Email, Cloud Repository, and/or Print). *NOTE: Some workflows do NOT support Print as an output destination.*

Step 7A: If a “Cloud Repository” is chosen as an output destination, the User is required to authenticate with the chosen “Cloud Repository” and select a destination folder.

Step 8: User selects Run button to start the execution of the document workflow.

Step 9A: If Email was defined as an output destination, for the document workflow, then an email is sent to the specified recipients with a link to download the generated output file.

Step 9B: If Download was defined as an output destination, for the document workflow, then the generated output file is saved to user’s local file system.

Step 9C: If a Cloud Repository was defined as an output destination, for the document workflow, then the generated output file is saved to the specified Cloud Repository location.

Step 9D: If Print was defined as an output destination, for the document workflow, then the user must login to the Workflow Central application at a Xerox® Device, to have the generated output file printed.

Save Customized Document Workflow

Step 1: User enters the URL for the Web App in a web browser on their PC/Laptop/Tablet or Mobile Phone.

Step 2: User selects the “Log In” button and enters their account username and password.

Step 3: The Web App displays the “Single” document workflows available for execution by the user.

Step 4: User either selects a document workflow to execute or navigates to the “Combination” document workflows and selects a document workflow to execute.

Step 5: User navigates to and selects the input file for the document workflow.

Step 6: User modifies the settings for each operation defined in the document workflow

Step 7: User defines one or more output destinations to specify where the output from the document workflow will be sent. (Download, Email, Cloud Repository, and/or Print). *NOTE: Some workflows do NOT support Print as an output destination.*

Step 8: User selects “Save as New” button to create a new customized document workflow.

Step 9: User enters a document workflow name, selects an icons and chooses whether the document workflow will be private or public.

Step 10: User selects the “Save” button to create the customized document workflow.

Step 10: User navigates to the “Saved” document workflows to view and execute a customized document workflow.

Create automated workflows

Step 1: User enters the URL for the Web App in a web browser on their PC/Laptop/Tablet or Mobile Phone.

Step 2: User selects the “Log In” button and enters their account username and password.

Step 3: The Web App displays the “Single” document workflows available for execution by the user.

Step 4: User selects “Automated” then selects “Create”.

Step 5: User defines either an Input folder, from a Cloud Repository) or an Email account as the location where to look for documents to be processed by the automated workflow. *NOTE: The supported Cloud Repositories are Google Drive, Microsoft OneDrive and Microsoft SharePoint. Only Microsoft Email is supported currently*.

Step 6: User defines the “Conditions” for the execution of the automated workflow.

Step 7: User selects a document workflow (i.e., Translate, Redact, etc.) to be used by the automated workflow.

Step 8: User modifies the settings for each operation defined in the selected document workflow.

Step 9: User defines the output destination where the output from the automated workflow will be sent. (Email or Cloud Repository).

Step 9: User enters an automated workflow name, selects an icon and chooses whether the “Activate” the automated workflow.

Step 10: User selects the “Save” button to create the automated workflow.

View and manage automated workflows

Step 1: User enters the URL for the Web App in a web browser on their PC/Laptop/Tablet or Mobile Phone.

Step 2: User selects the “Log In” button and enters their account username and password.

Step 3: The Web App displays the “Single” document workflows available for execution by the user.

Step 4: User selects “Automated” and a list of automated workflows, created by the authenticated user, is displayed.

Step 5: User can “Activate” or “Deactivate” an automated workflow displayed in the list.

Step 6: User can Delete, Edit or View the execution history of an automated workflow displayed in the list.

View and manage protected documents

Step 1: User enters the URL for the Web App in a web browser on their PC/Laptop/Tablet or Mobile Phone.

Step 2: User selects the “Log In” button and enters their account username and password.

Step 3: The Web App displays the “Single” document workflows available for execution by the user.

Step 4: User runs the Protect document workflow to generate a “Protected” document.

Step 5: Upon completion of the “Protect” document workflow, the user navigates to the “Active Documents” tab.

Step 6: A list of “Active Documents”, generated by the “Protect” document workflow, is displayed.

Step 7: User can Delete or View the details of any “Active Document” displayed in the list.

Execute a document workflow from the Xerox® Print and Scan Experience desktop application

Step 1: User runs the Xerox® Print and Scan Experience App from their PC/Laptop.

Step 2: User initiates a scan from the Xerox® Print and Scan Experience App.

Step 3: User chooses Xerox® Workflow Central Platform as the destination for the scanned document.

Step 4: The Xerox® Print and Scan Experience App uploads the scanned document to Xerox® Workflow Central Platform and then launches Xerox® Workflow Central Platform in the user's default web browser.

Step 5A: If "Trial Usage" has NOT been exhausted, the Web App is automatically "Logged In" as a Guest.

Step 5B: If "Trial Usage" has been exhausted, the Web App displays the "Log In" screen and User enters their account username and password to "Log In".

Step 6: The Web App displays the document workflows available for execution by the user.

Step 7: User selects a document workflow to execute.

Step 8: The scanned document uploaded by the Xerox® Print and Scan Experience App is automatically selected as the input file for the document workflow.

Step 9: User modifies the settings for each operation defined in the document workflow

Step 10: User defines one or more output destinations to specify where the output from the document workflow will be sent. (Download, Email, Cloud Repository, and/or Print). *NOTE: Some workflows do NOT support Print as an output destination.*

Step 10A: If a “Cloud Repository” is chosen as an output destination, the User is required to authenticate with the chosen “Cloud Repository” and select a destination folder.

Step 11: User selects Run button to start the execution of the document workflow.

Step 12A: If Email was defined as an output destination, for the document workflow, then an email is sent to the specified recipients with a link to download the generated output file.

Step 12B: If Download was defined as an output destination, for the document workflow, then the generated output file is saved to the user’s local file system.

Step 12C: If a Cloud Repository was defined as an output destination, for the document workflow, then the generated output file is saved to the specified Cloud Repository location.

Step 12D: If Print was defined as an output destination, for the document workflow, then the user must login to the Workflow Central App at a Xerox® Device, to have the generated output file printed.

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

User data related to the categories below are stored in cloud persistent storage.

- Customized workflows explicitly saved by the user.
- Workflow data, including intermediate processing files and output files, for workflow jobs that are processing or pending completion due to required user interaction.
- Logs of completed and cancelled workflow jobs.
- Automated workflows created by the user.
- Encrypted access and refresh tokens used by an automated workflow.
- History of automated workflow jobs.

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 for workflow output files, where the user has chosen to have an email sent with a download link, on the 7th day after the output file was created.

The following activities will trigger a delete event, for encrypted access and refresh tokens associated with an automated workflow.

- Deletion of an automated workflow by the user.
- Deactivation of an automated workflow by the user.
- Deactivation of an automated workflow caused by either non-entitlement or an error accessing the configured cloud service(s).
- Disabling of the automated workflow feature or of workflows configured in an automated workflow.

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

APPLICATION DATA STORED IN THE ABBYY CLOUD OCR SERVICE

User documents that need OCR and/or format conversion 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.

For detailed information on User Data Protection and Security for the Abbyy Cloud OCR Service, please follow this link: https://www.abbyy.com/cloud-ocr-sdk/legal/dpa/

APPLICATION DATA STORED IN THE ZAMZAR AUDIO SERVICE

User documents that have been requested to be converted to an Audio 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 audio file.

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

For detailed information on User Data Protection and Security for the Zamzar Audio Service, please follow this link: https://developers.zamzar.com/dpa

APPLICATION DATA STORED IN THE GOOGLE VISION SERVICE

User handwritten documents that have been requested to be converted to text are stored in cloud persistent storage until a delete event occurs.

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

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

For detailed information on User Data Protection and Security for the Google Vision Service, please follow this link: https://cloud.google.com/vision/docs/data-usage

APPLICATION DATA STORED IN THE GOOGLE DLP SERVICE

User documents that have been requested to be redacted 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.

- A delete occurs when the system detects that the document redaction inspection job has completed and the locations of the redacted data fields, within the document, has been downloaded.

For detailed information on User Data Protection and Security for the Google DLP Service, please follow this link: https://cloud.google.com/dlp/docs/support/data-security

APPLICATION DATA STORED IN THE MICROSOFT TRANSLATOR SERVICE

User documents that have been requested to be translated to a different language 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 translated document file.

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

For detailed information on User Data Protection and Security for the Microsoft Translator Service, please follow this link: https://www.microsoft.com/en-us/translator/business/notrace/

APPLICATION DATA STORED IN THE SUMMARIZEBOT SERVICE

User documents that have been requested to be summarized 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 summarized document file.

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

For detailed information on User Data Protection and Security for the SummarizeBot Service, please follow this link: https://www.summarizebot.com/privacy_policy.html

APPLICATION DATA STORED IN THE RPOST RMAIL SERVICE

User data related to the categories below are stored in cloud persistent storage.

- User documents that have been requested to be sent in a Registered and Encrypted email
- Sender's email address
- Recipient's email address

The following activities will trigger a delete event, for the document files sent in the email. The documents are stored so that the recipient can download them from links contained in the email.

- A delete occurs on the 7th day after the Registered and Encrypted email has been sent.

The following activities will trigger a delete event, of the Sender's email address.

- A delete can only occur by sending a request to WorkflowCentralSupport@xerox.com to have the email address permanently removed from the RPost RMail system.

The following activities will trigger a delete event, of the Recipient's email address.

- A delete occurs on the 7th day after the Registered and Encrypted email has been sent.

For detailed information on User Data Protection and Security for the RPost RMail Service, please follow this link: https://rpost.com/legal-notices/privacy-notice/

APPLICATION DATA STORED IN THE RPOST RDOCS SERVICE

Metadata related to a Protected document is stored in cloud persistent storage.

- Document name, Created Date, Expires Date, Security Level, and Status.
- Number of pages, Max views per user, Identify screen capture state, respond to email address, Timestamp state, Printing state, disclose user list state, limit domains state.
- Number of Views, Total Viewing time.
- Authorized users list: user email, timestamp of first view, number of views, total view time, active state.

NOTE: The actual Protected document is not stored in cloud persistent storage by the service. Instead, the Protected document remains in possession of the document owner and the persons the Protected document has been distributed to. These persons may persistently store the Protected document wherever they wish.

The following activities will trigger adding a person to the Protected document's Authorized Users list in the RPost RDocs service:

- The document owner adding an email to the Authorized Users list at the time the workflow is executed.
- A person requesting a passcode to access a "Track Viewers" security Protected document.

Deleting the Protected document from Workflow Central Active Documents will remove its metadata from cloud persistent storage. The Document Owner's email is not removed from persistent storage; and may be removed only by special request.

NOTE: The expiration of a Protected document does not delete any metadata associated with the protected document. Expired documents are automatically deleted 30 days after expiration or 1 year after creation, whichever occurs first.

NOTE: Deleting the Protected document from Workflow Central Active Documents does NOT delete the Protected document file - which remains in the possession of the document owner and *recipients. That said, the content of the Protected document file is inaccessible once the document has been deleted from Workflow Central Active Documents*.

For detailed information on User Data Protection and Security for the RPost RDocs Service, please follow this link: https://rpost.com/legal-notices/privacy-notice/

APPLICATION DATA STORED IN THE OPENTEXT XM FAX SERVICE

User data related to the categories below are stored in cloud persistent storage.

- User documents that have been requested to be sent in as a Fax.
- Recipient's Fax number
- If "Cover Sheet" is enabled:
  - Subject
  - Recipient Name

The following activities will trigger a delete event for documents and optional cover sheet data sent in a Fax.

- A delete occurs on the 7th day after the Fax has been sent.

For detailed information on User Data Protection and Security for the OpenText XM Fax service, please follow this link: https://www.opentext.com/about/privacy/

LOCAL ENVIRONMENT

Application data transmitted

Application data related to the categories below are transmitted to/from a User's PC/Laptop/Tablet or Mobile Phone.

- Account Login data
- App Access/Entitlement data
- Workflow Input, Output and Control Parameters
- Workflow Execution Status data
- Protected Document's status and configuration parameters
- Automated workflow configuration parameters
- Automated workflow execution history data

Application data stored on the User's PC/Laptop/Tablet or Mobile Phone

- The application stores both the user's "access token" and "refresh token", for Workflow Central, in Browser Local Storage. The "access token" has limited lifespan of 2 hours and the "refresh token" is single use with a life span of 100 days.
  - The "access token" and "refresh token" are deleted from Browser Local Storage when a user "Logs Out" of Workflow Central.
- The application will store files, generated during the execution of a workflow, when a workflow is defined to download the workflow's output.

HTTP Cookies

The Web App only stores non-tracking, technically necessary data required by Microsoft Azure.

3. Product Description – Xerox® ConnectKey® App

Overview

This solution delivers 2 separate software offerings, each aligning to meet specific user goals. This section applies to the Xerox ConnectKey App which is executed from a Xerox® Device.

The Xerox® Workflow Central Platform provides two primary workflows for the logged in customer:

1. Execute a document workflow
2. Save a customized document workflow

Application	What can I do?
ConnectKey App	• Login to my account • View available document workflows • Execute a document workflow • Save a customized document workflow

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 four key components, the device weblet, the ConnectKey App User Interface, the Workflow Central Platform Service Interface, and the Workflow Central Platform Microservices Interface. The device weblet is a ConnectKey/EIP web app that enables the following behavior on a Xerox® device:

- Presents the user with an application UI that executes functionality in the cloud.
- Interfaces with the EIP API, which delegates work, such as document scanning and printing.
- Executes Microservices, which delegates work such as document format conversion and language translation.

Xerox App Gallery

The App Gallery component is a web application hosted on the Microsoft Azure Cloud System. The App Gallery Component implements the following functions for the ConnectKey App: Authentication and Access Authorization within the Xerox® Workflow Central Platform.

Xerox Extensible Interface Platform®

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.

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 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 following commercial cloud repository providers: Xerox DocuShare Go, Microsoft (OneDrive and O365 SharePoint), Google Drive, Dropbox, and Box.

For the ConnectKey App to communicate and interact with a specific cloud repository provider, the user needs to establish a connection. This connection process utilizes an OAuth 2.0 login workflow provided by the cloud repository provider, which requests the username and password. Upon successful authentication, an OAuth access token is returned to the device from the cloud repository. The access token is passed to the Cloud Repository Middleware for use when calling a cloud repository provider's API. The access token is never stored.

NOTE: *For security purposes, some Microsoft Azure AD Tenants may be configured to require an Azure AD administrator to grant access to any application before it can be used by any of their users. The following URL can be accessed by an Azure AD Administrator to grant access within their Azure AD Tenant: https://cloudmiddleware.services.xerox.com/azuread/adminconsent.aspx*

Xerox® Translates Service

The Xerox® Translation Service component is a set of translation APIs hosted in the Microsoft Azure Cloud System. The Web App uses the API to translate documents into a different language while maintaining the layout and format of the original document.

Xerox® Auto-Redaction App

The Xerox® Auto-Redaction App component contains a set of document redaction APIs hosted in the Microsoft Azure Cloud System. The Workflow Central Platform uses the API to generate a document with a set of specified data redacted from the original document.

Xerox OCR Service

The Xerox OCR Service component is a set of document format conversion APIs hosted in the Microsoft Azure Cloud System. The Workflow Central Platform uses the API to convert documents into one of the following Microsoft formats: DOCX, PPTX or XLXS.

ABBYY Cloud OCR Service

The ABBYY Cloud OCR Service component is a set of partner, cloud hosted Optical Character Recognition (OCR) and document format conversion APIs.

Microsoft Translator Service

The Microsoft Translator Service component is a set of partner, cloud hosted language translation APIs.

Zamzar Audio Service

The Zamzar Audio Service component is a set of partner, cloud hosted audio file conversion APIs. The Workflow Central Platform uses the Zamzar Audio API to convert a document into an Audio file.

Google Vision Service

The Google Vision Service component is a set of partner, cloud hosted OCR APIs. The Workflow Central Platform uses the API to generate editable text documents from an image of a handwritten document.

Google DLP Service

The Google DLP (Data Loss Prevention) Service component is a set of partner, cloud hosted document analysis and redaction APIs.

SummarizeBot Service

The SummarizeBot Service component is a set of partner, cloud hosted document summarization APIs. The Workflow Central Platform uses the API to generate summarized documents.

RPost RMail Service

The RPost RMail Service component is a partner, cloud hosted email services platform. The Workflow Central Platform uses the RMail API to send Registered and Encrypted email when it is specified in a document workflow.

RPost RDocs Service

The RPost RDocs Service component is a partner, cloud hosted document protection platform. The Workflow Central Platform uses the RDocs API to create and send protected (encrypted) documents. The RDocs API is also used for the viewing and controlling access to the protected documents (via the Active Documents feature) created by a Workflow Central Platform user.

OpenText XM Fax Service

The OpenText XM Fax Service component is a partner, cloud hosted Fax service platform. The Workflow Central Platform uses the Cloud Fax API to send a document as a Fax.

Twilio SendGrid Email Service

The Twilio SendGrid Email Service component is a partner, cloud hosted email services platform. The Workflow Central Platform uses the SendGrid API to send email when it is specified in a document workflow.

COMPONENTS

Xerox® Device with Xerox® Workflow Central Platform – Xerox® 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® Workflow Central Platform installed.

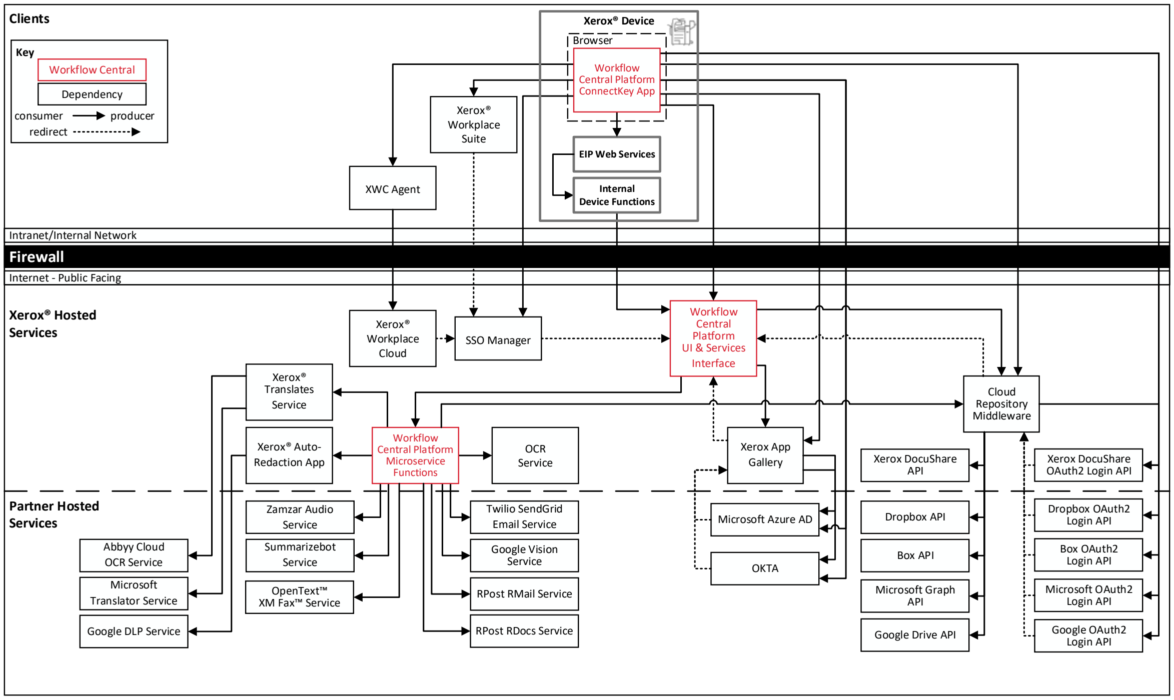
Xerox® Workflow Central Platform – UI & Services Interface

The UI & Service Interface component is a service hosted on the Microsoft Azure Cloud System. The component is responsible for hosting the web pages, which are displayed on the UI of the Xerox® Device. Additionally, the component provides user access and management, business logic services, workflow management and execution, and the Workflow Central Platform APIs.

Xerox® Workflow Central Platform – Microservices

The Microservices component is a set of Microsoft Azure Functions hosted on the Microsoft Azure Cloud System. The various microservices interface with a host of 3rd Party APIs to perform specific operations like Audio Conversion, Translation, Format Conversion, OCR, Summarization and Email.

DATA FLOW DIAGRAM



WORKFLOWS

Execute a Document Workflow

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

Step 2: User enters their account username and password. (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: The document workflows available for execution by the user are displayed.

Step 4: User selects a document workflow to execute.

Step 5: User modifies the scanning options (i.e., single sided, original size, etc.…).

Step 6: User modifies the settings for each operation defined in the document workflow

Step 7: User defines one or more output destinations to specify where the output from the document workflow will be sent. (Download, Email, Cloud Repository, and/or Print). *NOTE: Some workflows do NOT support Print as an output destination.*

Step 7A: If a “Cloud Repository” is chosen as an output destination, the User is required to authenticate with the chosen “Cloud Repository” and select a destination folder.

Step 8: User selects Run button to start the execution of the document workflow

Step 9A: If Email was specified as an output destination, for the document workflow, then an email is sent to the specified recipients with a link to download the generated output file.

Step 9B: If Download was defined as an output destination, for the document workflow, then the user must login to Workflow Central from a PC/Laptop or Mobile device, to have the generated output file saved to user’s local file system.

Step 9C: If a Cloud Repository was defined as an output destination, for the document workflow, then the generated output file is saved to the specified Cloud Repository location.

Step 9D: If Print was defined as an output destination, for the document workflow, then the output document is printed to the Xerox® Device with the defined print options.

Save Customized Document Workflow

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

Step 2: User enters their account username and password. (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: The document workflows available for execution by the user are displayed.

Step 4: User selects a document workflow to execute.

Step 5: User modifies the scanning options (i.e., single sided, original size, etc.…).

Step 6: User modifies the settings for each operation defined in the document workflow

Step 7: User defines one or more output destinations to specify where the output from the document workflow will be sent. (Download, Email, Cloud Repository, and/or Print). *NOTE: Some workflows do NOT support Print as an output destination.*

Step 8: User selects “Save as New” button to create a new customized document workflow.

Step 9: User enters a document workflow name, selects an icons and chooses whether the document workflow will be private or public.

Step 10: User selects the “Save” button to create the customized document workflow.

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

User data related to the categories below are stored in cloud persistent storage.

- Customized workflows explicitly saved by the user
- Workflow data, including intermediate processing files and output files, for workflow jobs that are processing or pending completion due to required user interaction.
- Logs of completed and cancelled workflow jobs.

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 for workflow output files, where the user has chosen to have an email sent with a download link, on the 7th day after the output file was created.

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

APPLICATION DATA STORED IN THE ABBYY CLOUD OCR SERVICE

User documents that need OCR and/or format conversion 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.

For detailed information on User Data Protection and Security for the Abbyy Cloud OCR Service, please follow this link: https://www.abbyy.com/cloud-ocr-sdk/legal/dpa/

APPLICATION DATA STORED IN THE ZAMZAR AUDIO SERVICE

User documents that have been requested to be converted to an Audio 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 audio file.

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

For detailed information on User Data Protection and Security for the Zamzar Audio Service, please follow this link: https://developers.zamzar.com/dpa

APPLICATION DATA STORED IN THE GOOGLE VISION SERVICE

User handwritten documents that have been requested to be converted to text are stored in cloud persistent storage until a delete event occurs.

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

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

For detailed information on User Data Protection and Security for the Google Vision Service, please follow this link: https://cloud.google.com/vision/docs/data-usage

APPLICATION DATA STORED IN THE GOOGLE DLP SERVICE

User documents that have been requested to be redacted 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.

- A delete occurs when the system detects that the document redaction inspection job has completed and the locations of the redacted data fields, within the document, has been downloaded.

For detailed information on User Data Protection and Security for the Google DLP Service, please follow this link: https://cloud.google.com/dlp/docs/support/data-security

APPLICATION DATA STORED IN THE MICROSOFT TRANSLATOR SERVICE

User documents that have been requested to be translated to a different language 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 translated document file.

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

For detailed information on User Data Protection and Security for the Microsoft Translator Service, please follow this link: https://www.microsoft.com/en-us/translator/business/notrace/

APPLICATION DATA STORED IN THE SUMMARIZEBOT SERVICE

User documents that have been requested to be summarized 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 summarized document file.

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

For detailed information on User Data Protection and Security for the SummarizeBot Service, please follow this link: https://www.summarizebot.com/privacy_policy.html

APPLICATION DATA STORED IN THE RPOST RMAIL SERVICE

User data related to the categories below are stored in cloud persistent storage.

- User documents that have been requested to be sent in a Registered and Encrypted email
- Sender’s email address
- Recipient’s email address

The following activities will trigger a delete event, for the document files sent in the email. The documents are stored so that the recipient can download them from links contained in the email.

- A delete occurs on the 7th day after the Registered and Encrypted email has been sent.

The following activities will trigger a delete event, of the Sender's email address.

- A delete can only occur by sending a request to WorkflowCentralSupport@xerox.com to have the email address permanently removed from the RPost RMail system.

The following activities will trigger a delete event, of the Recipient's email address.

- A delete occurs on the 7th day after the Registered and Encrypted email has been sent.

For detailed information on User Data Protection and Security for the RPost RMail Service, please follow this link: https://rpost.com/legal-notices/privacy-notice/

APPLICATION DATA STORED IN THE RPOST RDOCS SERVICE

Metadata related to a Protected document is stored in cloud persistent storage.

- Document name, Created Date, Expires Date, Security Level, and Status.
- Number of pages, Max views per user, Identify screen capture state, respond to email address, Timestamp state, Printing state, disclose user list state, limit domains state.
- Number of Views, Total Viewing time.
- Authorized users list: user email, timestamp of first view, number of views, total view time, active state.

NOTE: The actual Protected document is not stored in cloud persistent storage by the service.   Instead, the Protected document remains in possession of the document owner and the persons the Protected document has been distributed to.   These persons may persistently store the Protected document wherever they wish.

The following activities will trigger adding a person to the Protected document's Authorized Users list in the RPost RDocs service:

- The document owner adding an email to the Authorized Users list at the time the workflow is executed.
- A person requesting a passcode to access a "Track Viewers" security Protected document.

Deleting the Protected document from Workflow Central Active Documents will remove its metadata from cloud persistent storage.   The Document Owner's email is not removed from persistent storage; and may be removed only by special request.

NOTE: The expiration of a Protected document does not delete any metadata associated with the protected document. Expired documents are automatically deleted 30 days after expiration or 1 year after creation, whichever occurs first.

NOTE: Deleting the Protected document from Workflow Central Active Documents does NOT delete the Protected document file - which remains in the possession of the document owner and recipients.   That said, the content of the Protected document file is inaccessible once the document has been deleted from Workflow Central Active Documents.

For detailed information on User Data Protection and Security for the RPost RDocs Service, please follow this link: https://rpost.com/legal-notices/privacy-notice/

APPLICATION DATA STORED IN THE OPENTEXT XM FAX SERVICE

User data related to the categories below are stored in cloud persistent storage.

- User documents that have been requested to be sent in as a Fax.
- Recipient’s Fax number
- If “Cover Sheet” is enabled:
  - Subject
  - Recipient Name

The following activities will trigger a delete event for documents and optional cover sheet data sent in a Fax.

- A delete occurs on the 7th day after the Fax has been sent.

For detailed information on User Data Protection and Security for the OpenText XM Fax service, please follow this link: https://www.opentext.com/about/privacy/

LOCAL ENVIRONMENT

Application data transmitted

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

- Account Login data
- App Access/Entitlement data
- Workflow Input, Output and Control Parameters
- Workflow Execution Status data
- Device Session data
- Device Job data

Application data stored on the Xerox® Device

The following app data is stored on the device, encrypted in Browser’s internal storage, until the App is uninstalled from the device.

- Device’s SNMP V2 public community string

HTTP Cookies

The ConnectKey App only stores non-tracking, technically necessary data required by Microsoft Azure.

4. Network Information

Protocol, Ports and URLs

The following tables lists the protocol, ports and URLs used by the Web Browser or Xerox® ConnectKey app when executing within a customer's private network. All connections are outbound to Cloud hosted components.

WEB APPLICATION

Protocol	Transport and Port Value	Use	Component	URL
HTTPS using TLS	TCP 443	Authentication, Account Management, Access Management, Workflow Management, Subscription Entitlement	Browser to Workflow Central Platform UI & Services Interface	workflowcentral.services.xerox.com
HTTPS using TLS	TCP 443	Account Creation, Profile Modification, Device Management, Subscription Purchase and Management	Browser to App Gallery	appgallery.services.xerox.com
HTTPS using TLS	TCP 443	Facilitate Authentication Flow	Browser to Cloud Repository Middleware	cloudmiddleware.services.xerox.com
HTTPS using TLS	TCP 443	Facilitate Authentication Flow	Browser to App Cloud Connector	xeroxappcloudconnector.services.xerox.com
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Xerox DocuShare® Go – United States	docushare-go-prod.auth.us-east-1.amazoncognito.com d3oia8etllorh5.cloudfront.net

Protocol	Transport and Port Value	Use	Component	URL
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Xerox DocuShare® Go – Europe	docushare-go-v3-prod-eu.auth.eu-central-1.amazoncognito.com d3oia8etllorh5.cloudfront.net
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Microsoft	login.microsoftonline.com
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Google	accounts.google.com
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Dropbox	www.dropbox.com
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Box	www.box.com
HTTPS using TLS	TCP 443	Opening a Protected Document	Browser to RDocs	app2.rdocs.io

XEROX® CONNECTKEY APPLICATION

Protocol	Transport and Port Value	Use	Component	URL
HTTPS using TLS	TCP 443	Authentication, Account Management, Access Management, Workflow Management	ConnectKey App to Workflow Central Platform UI & Services Interface	workflowcentral.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	Single Sign On (SSO)	ConnectKey App to SSO Manager	ssomanager.services.xerox.com

Protocol	Transport and Port Value	Use	Component	URL
HTTPS using TLS	TCP 443	Facilitate Authentication Flow	Browser to Cloud Repository Middleware	cloudmiddleware.services.xerox.com
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Xerox DocuShare® Go – United States	docushare-go-prod.auth.us-east-1.amazoncognito.com d3oia8etllorh5.cloudfront.net
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Xerox DocuShare® Go – Europe	docushare-go-v3-prod-eu.auth.eu-central-1.amazoncognito.com d3oia8etllorh5.cloudfront.net
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Microsoft	login.microsoftonline.com
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Google	accounts.google.com
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Dropbox	www.dropbox.com
HTTPS using TLS	TCP 443	OAuth 2.0 Login Flow	Browser to Box	www.box.com

5. 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. All Workflow Central Platform persistent data and 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 this link:

https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

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

The Single Sign-On feature within the Xerox® ConnectKey App 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® 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 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® ConnectKey App installed on a Xerox® Device, in a customer environment that 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 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.

6. 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