

Xerox® Security Guide

Audio Documents Apps



© 2019 Xerox Corporation. All rights reserved. Xerox® is a trademark of Xerox Corporation in the United States and/or other countries. BR26398

Other company trademarks are also acknowledged.

Document Version: 1.0 (April 2019).

Preface

Purpose

The purpose of the Security Guide is to disclose information for Xerox® apps with respect to device security. Device security, in this context, is defined as how data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. This document describes design, functions, and features of the Xerox® apps relative to Information Assurance (IA) and the protection of customer sensitive information. Please note that the customer is responsible for the security of their network and the Xerox® apps do not establish security for any network environment.

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

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security. It is assumed that the reader is familiar with the apps; as such, some user actions are not described in detail.

Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox® Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox® Corporation and any third party.

Contents

1. General Security Protection.....	1-1
User Data Protection within the products.....	1-1
Document and File Security	1-1
Hosting - Microsoft Azure.....	1-1
Cloud Storage – Microsoft Azure	1-1
Xerox® Workplace Suite/Cloud and Single Sign-On Services	1-1
User Data in transit	1-2
Secure Network Communications.....	1-2
Xerox Workplace Suite/Cloud and Single Sign-On Services.....	1-2
2. Xerox® Audio Documents App – ConnectKey App	2-3
Description	2-3
Overview	2-3
App Hosting.....	2-3
Components	2-4
Architecture and Workflows	2-4
User Data Protection.....	2-6
Application data stored in the Xerox cloud.....	2-6
Local Environment	2-7
3. Xerox® Audio Documents App – App for iOS and Android	3-8
Description	3-8
Overview	3-8
App Hosting.....	3-8
Components	3-8
Architecture and Workflows	3-9
User Data Protection.....	3-11
Application data stored in the Xerox cloud.....	3-11
Local Environment	3-12
4. Xerox® Audio Documents App – Web Portal.....	4-14
Description	4-14
Overview	4-14
App Hosting.....	4-14

Components	4-14
Architecture and Workflows	4-15
User Data Protection	4-19
Application data stored in the Xerox cloud.....	4-19
Local Environment	4-19
5. Additional Information & Resources.....	5-21
Security @ Xerox	5-21
Responses to Known Vulnerabilities.....	5-21
Additional Resources	5-21

1. General Security Protection

User Data Protection within the products

Document and File Security

File content is protected during transmission by standard secure network protocols at the channel level. Since document source content and audio files 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 as a storage vault where the login information is securely stored.

All content to be stored in the vault is encrypted with AES 256 by the SSO Manager server before being given to the SSO vault that resides on the XWS/C solution. This ensures that the SSO vault can never view or use the contents being stored in the vault. Only the SSO Manager infrastructure knows how to decrypt the content stored in the vault and only the App knows how to use it.

The SSO Manager service manages the encryption key exchange required for secure communications and encrypts/decrypts the content saved in the vault.

For a full description, please review the Xerox® Workplace Suite/Cloud Information Assurance Disclosure: <https://security.business.xerox.com/en-us/products/xerox-workplace-suite/>

User Data in transit

Secure Network Communications

The web pages and app services that constitute the Xerox® 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.

2. Xerox® Audio Documents App – ConnectKey App

Description

Overview

This Xerox® solution delivers 3 separate software offerings, each aligning to meet specific user goals. This section applies to the ConnectKey App.

ConnectKey App

The ConnectKey App is a simple document conversion solution for your Xerox® device that assists the user with:

1. Creating an app administration account for managing user accounts.
2. Converting a paper document into an audio file, which is delivered through an email link.

Table 1. ConnectKey App user benefits

Application	What can I do?
ConnectKey App	<ul style="list-style-type: none">• Create the administrator account• Login• Create an audio file from a paper document• Download my converted audio file

App Hosting

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

ConnectKey App

The ConnectKey App consists of two key components, the device weblet and the cloud-hosted web service. The device weblet is a ConnectKey/EIP web app that enables the following behavior on a Xerox device:

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

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

Zamzar™ File Conversion Web Service

The solution depends on the Zamzar™ File Conversion API to convert digital documents into text-to-speech audio files. 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® Audio Documents App – 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® Audio Documents App installed.

Xerox® Audio Documents App – Web Services

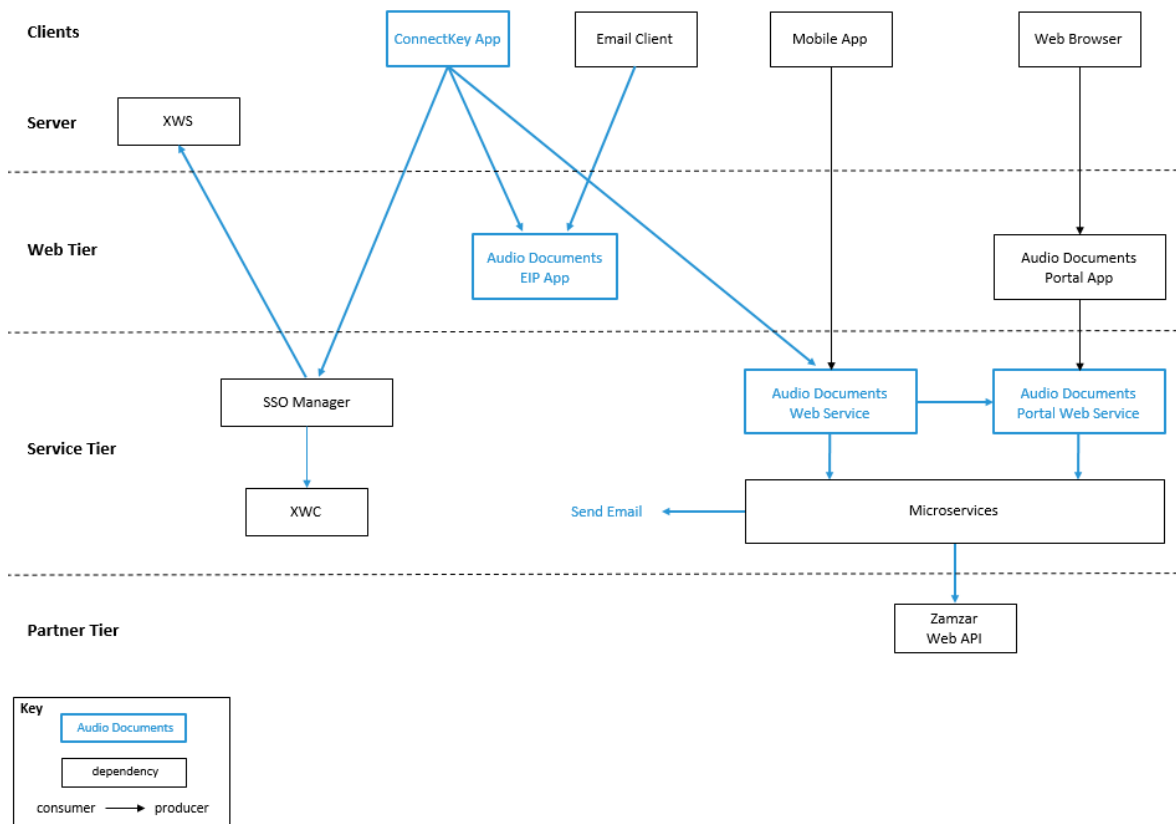
The Web Service is a service hosted on the Microsoft Azure Cloud System. The service is responsible for hosting the web pages which are displayed on the UI of the printer and provide the services support for the Xerox® apps. The web service interacts with the Zamzar services using the Zamzar APIs and Microsoft services using the Azure APIs.

Zamzar™ File Conversion Web Service

The Zamzar cloud hosted service provides a web API that is used for the file conversion process, which supports the creation and downloading of spoken word audio files.

Architecture and Workflows

Architecture Diagram



Workflows

ConnectKey App

Prerequisite – Create the administrator account



Step 1: Launch the App at the device after purchasing a new subscription.



Step 2: Complete and submit the Create Administrator Account form.

Part 1 – Login



Step 1: Prerequisite – Create the administrator account.



Step 2: Launch the App on the Xerox device.



Step 3: Complete and submit the Login form.



Step 4: When the SSO configuration is enabled, optionally agree to save the credentials to XWS/C storage for future use.

Part 2 – Create an audio file from 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 audio file title.



Step 5: Optionally change the scan settings.



Step 6: Submit the job using the Scan button.

Part 3 – Download my converted audio file



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



Step 2: Activate the audio file link provided in the email message.
The OS will handle the audio file content using the application associated with the MP3 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.

- Create the administrator account
- Login
- Create an audio file from a paper document
- Download my converted audio file

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 account and/or other users' sub-accounts.
- The App User visits the Web Portal and deletes their account.

The following activities will trigger a delete event, for cloud audio files that meet the associated criteria.

- A delete occurs when the system detects audio files that are greater than 7 days old.
- 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

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 does not store any cookies on the device.

3. Xerox® Audio Documents App – App for iOS and Android

Description

Overview

This Xerox® solution delivers 3 separate software offerings, each aligning to meet specific user goals. This section applies to the mobile app.

Mobile App

The mobile app is a document conversion solution for your mobile phone.

Table 2. Mobile app user benefits

Application	What can I do?
Mobile App	<ul style="list-style-type: none">• Login• Create an audio file from a digital document• Download and listen to my converted audio file• Delete my converted audio file from my device

App Hosting

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

Mobile App

The mobile app consists of two key components, the mobile app that is installed on a phone and the cloud-hosted web service. The mobile app is a native Android or iOS app that:

1. Presents the user with an application UI that executes functionality in the cloud.
2. Interfaces with OS platform APIs on various devices to manage personal application data.

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

Zamzar™ File Conversion Web Service

The solution depends on the Zamzar™ File Conversion API, hosted by Zamzar Ltd, to convert digital documents into audio files. All requests are made over HTTPS.

Components

Xerox® Audio Documents App – App for iOS and Android

The mobile app is capable of converting digital documents into personal audio files that can be played within the app. The Xerox® Audio Documents App is installed using the Google Play Store for Android or the Apple App Store for iOS.

Xerox® Audio Documents App – Web Services

The Audio Documents web services are hosted on Microsoft® Azure. The services are responsible for hosting the web pages which are displayed on the printer user interface and provide services

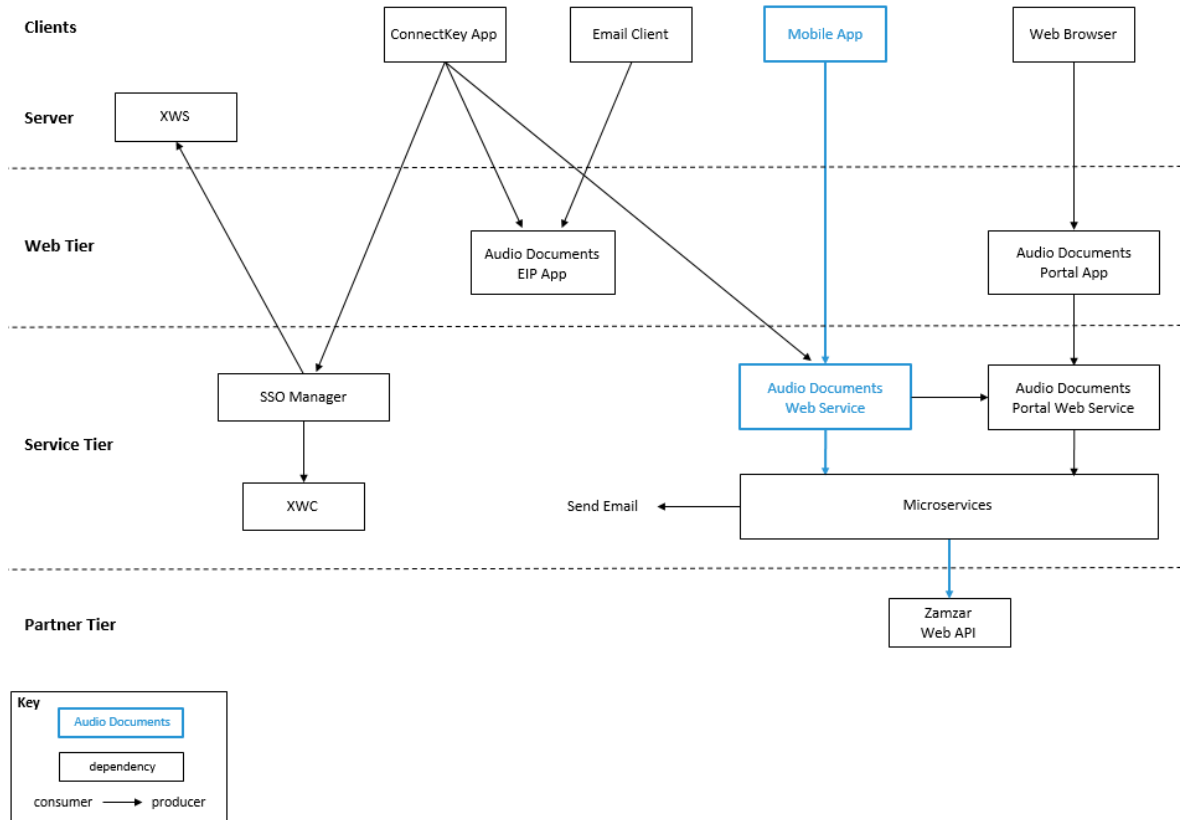
support for each of the Audio Documents apps. The web service interacts with Zamzar services using the public APIs and interacts with Microsoft services using the Microsoft® Azure APIs.

Zamzar™ File Conversion Web Service

The Zamzar cloud hosted service provides a public web API that is used for the file conversion process, which supports the creation and downloading of spoken word audio files.

Architecture and Workflows

Architecture Diagram



Workflows

Mobile App

Part 1 – Login



Step 1: Prerequisite – Create the administrator account using the ConnectKey App on the Xerox device.



Step 2: Launch the App on the mobile device.



Step 3: On the first run, read and accept the EULA.



Step 4: Complete and submit the Login form.

Part 2 – Create an audio file from a digital document



Step 1: Launch the App on the mobile device.



Step 2: Login to view the document list.



Step 3: Tap the Convert File button.



Step 4: Locate and select a file to convert to audio to transition to view the conversion settings.



Step 5: Optionally change the document language setting.



Step 6: Submit the job using the Convert button.

Part 3 – Download and listen to my converted audio file



Step 1: Launch the App on the mobile device.



Step 2: Login to view the document list.



Step 3: Optionally locate and tap the Download control for a document in the list.



Step 4: Tap a document in the list to reveal the playback controls.



Step 5: Tap the Play control to begin downloading the file if needed and playback the audio.



Step 6: Optionally use the Back and Forward controls to adjust the playback position.

Part 4 – Delete my converted audio file



Step 1: Launch the App on the mobile device.



Step 2: Login to view the document list.



Step 3: Locate a downloaded document in the list and tap the Delete control.

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
- Session data
- Job data
- Personal audio files

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 account and/or other users' sub-accounts.
- The app user visits the web portal and deletes their account.

The following activities will trigger a delete event, for cloud audio files that meet the associated criteria.

- A delete occurs when the system detects audio files that are greater than 7 days old.
- 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 mobile device.

- Account data
- Session data
- Job data
- Personal audio files

Application data stored on the mobile device

The following app data is stored on the mobile device, in device storage, until the app is uninstalled from the device or removed by the user.

- Account data
- Session data
- Job data
- Personal audio files

Provided the mobile device shipped with Android 6.0 from the factory, device encryption is enforced. For more information, please follow these links:

Android encryption overview

<https://source.android.com/security/encryption/>

Android full-disk encryption

<https://source.android.com/security/encryption/full-disk>

Android file-based encryption

<https://source.android.com/security/encryption/file-based>

Apple iOS mobile devices use device encryption, which is not configurable. For more information, please follow this link:

iOS Security

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

HTTP Cookies

The mobile app does not store any cookies on the device.

4. Xerox® Audio Documents App – Web Portal

Description

Overview

This Xerox® solution delivers 3 separate software offerings, each aligning to meet specific user goals. This section applies to the Audio Documents web portal.

Web Portal

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

1. Modifying personal profile information.
2. Inviting others to enroll so they can use the apps.

Table 3. Web portal user benefits

Application	What can I do?
Web portal	<ul style="list-style-type: none">• Login• Update my account profile information• Invite a user to enroll as an app user• Create my sub-account• Reset my password• Delete my sub-account <p>Executed by Xerox, upon request.</p> <ul style="list-style-type: none">• Delete my administrator account

App Hosting

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

Web Portal

The solution supports application sub-accounts linked to a subscription bundle. The portal provides support for features related to administering accounts and profiles.

Components

Xerox® Audio Documents App – Portal Web App

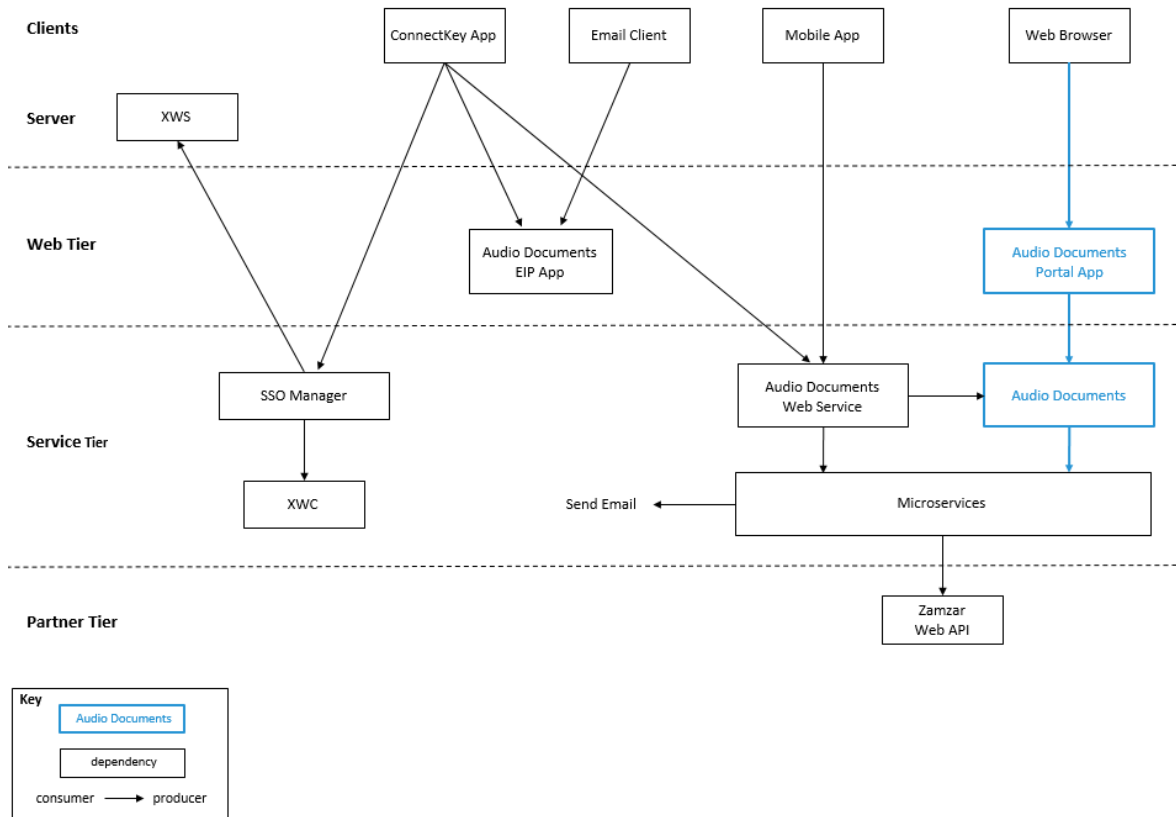
The Web Portal provides support for maintaining sub-accounts linked to the App subscription. The portal is a browser based app that presents to the user functionality that is executed in the cloud.

Xerox® Audio Documents App – 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
Web Portal

Optional – Complete Admin Account Setup (Admin only)



Step 1: Prerequisite – Create the administrator account using the ConnectKey App on the Xerox device.



Step 2: Open the Audio Documents administrator authorization email message received, which is associated with your subscription.



Step 3: Activate the Complete Account Setup button link provided in the email message to navigate to the Administrator Account Setup form.

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



Step 4: Optionally modify the admin profile details.



Step 5: Activate the Complete Setup button to navigate to the Manage Sub-Accounts page.

Login



- Step 1:** Prerequisite – Create the administrator account using the ConnectKey App on the Xerox device.
- (a) Optional – Invite a user to create a sub-account.
 - (1) Optional – Create my sub-account.



- Step 2:** Open a web browser and navigate to the web portal URL.



- Step 3:** Complete and submit the Login form to reveal the app home page.

Update my account profile information



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



- Step 2:** Login to reveal your account home page.
- (a) App administrators will also need to activate the profile menu and select the Account Details item.



- Step 3:** Modify your profile details.



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

Part 1 – Invite a user to create a sub-account (Admin only)



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



- Step 2:** Login to reveal the Admin account 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.

Part 2 – Create my sub-account



Step 1: Open to view the Audio Documents sub-account invitation email message received, which is associated with the administrator's subscription.



Step 2: Activate the Complete Account button link provided in the email message to navigate to the Create Account page.

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



Step 3: Optionally modify the account profile details.



Step 4: Activate the Create My Account button to activate your account and navigate to the account home page.

Reset my password



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



Step 2: Activate the Forgot Password control so you can provide and submit your account email address.

An invitation containing a Reset Password link will be sent to the email address provided.



Step 3: Open to view the Reset Password email message received, which is associated with your account's subscription.



Step 3: Activate the Password Reset button link provided in the email message to navigate to the Reset Password page.

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



Step 4: Complete and submit the Reset Password form to navigate to the Login page.

Delete my sub-account (Non-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: 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.

Delete my administrator account (Admin only)



Step 1: Contact Xerox for assistance.

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 subscription administrator visits the web portal and deletes their account and/or other users' sub-accounts.
- 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 does not store any cookies on the host device.

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 <http://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: <http://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	http://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/