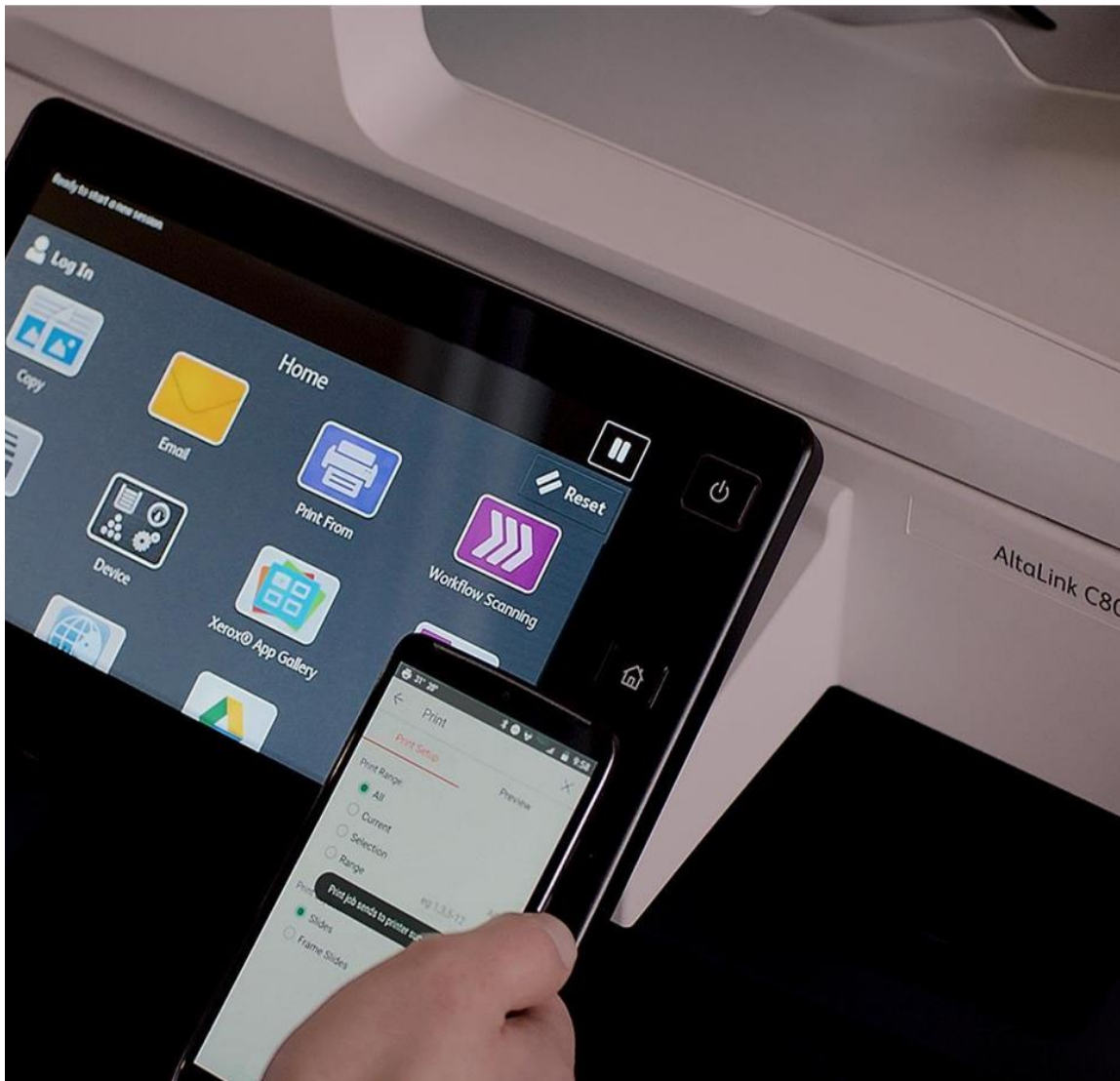


Xerox® Security Guide

Connect for SignNow App



© 2020 Xerox Corporation. All rights reserved. Xerox® is a trademark of Xerox Corporation in the United States and/or other countries. BR29909

Other company trademarks are also acknowledged.

Document Version: 1.0 (August 2020).

Introduction

Purpose

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

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

Target Audience

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

Disclaimer

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

Contents

Purpose	i
Target Audience	i
Disclaimer	i
1. General Security Protection.....	1-1
User Data Protection within the products.....	1-1
Document and File Security	1-1
Hosting - Microsoft Azure.....	1-1
Cloud Storage – Microsoft Azure	1-1
Xerox® Workplace Suite/Cloud and Single Sign-On Services	1-1
User Data in transit	1-2
Secure Network Communications.....	1-2
Xerox Workplace Suite/Cloud and Single Sign-On Services.....	1-2
2. Product Description.....	2-3
Overview	2-3
App Hosting.....	2-3
Components	2-4
Architecture and Workflows	2-5
User Data Protection.....	2-10
Application data stored in the Xerox cloud.....	2-10
Local Environment	2-10
3. Additional Information & Resources.....	3-11
SignNow Security.....	3-11
Security @ Xerox	3-11
Responses to Known Vulnerabilities.....	3-11
Additional Resources	3-11

1. General Security Protection

User Data Protection within the products

DOCUMENT AND FILE SECURITY

File content is protected during transmission by standard secure network protocols at the channel level. Since document source content may contain Personally Identifiable Information (PII) or other sensitive content, it is the responsibility of the user to handle the digital information in accordance with information protection best practices.

HOSTING - MICROSOFT AZURE

The cloud services are hosted on the Microsoft Azure Network. The Microsoft Azure Cloud Computing Platform operates in the Microsoft® Global Foundation Services (GFS) infrastructure, portions of which are ISO27001-certified. Microsoft has also adopted the new international cloud privacy standard, ISO 27018. Azure safeguards customer data in the cloud and provides support for companies that are bound by extensive regulations regarding the use, transmission, and storage of customer data.

The Apps hosted in the cloud are scalable so that multiple instances may be spun up/down as needed to handle user demand. The service is hosted both in the US and Europe. Users will be routed to the closest server geographically based on server load and network speed.

CLOUD STORAGE – MICROSOFT AZURE

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

For a full description, please follow these links:

Azure Storage

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

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

The Xerox® ConnectKey App Single Sign-On feature integrates with the Xerox® Workplace Suite/Cloud authentication solution to store user access information for SSO-compatible Xerox Gallery Apps. After the user enters their storage service credentials the first time, the XWS/C solution acts as a storage vault where the login information is securely stored.

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

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

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

User Data in transit

SECURE NETWORK COMMUNICATIONS

The web pages and app services that constitute the Xerox® Solutions are deployed to Microsoft Azure App Services. All web pages are accessed via HTTPS from a web browser. All communications are over HTTPS. Data is transmitted securely and is protected by TLS security for both upload and download. The default TLS version used is 1.2.

The Xerox® App requires the user to provide proper/valid credentials in order to gain access to the application's features. Authenticated users are allowed to access the features and data using HTTPS.

At launch, the apps must get an authentication/session token through the solution's authentication process. The access token acquired is used for that session of the app.

When using the ConnectKey App installed on a Xerox® Device, if the customer environment includes an Authentication solution (e.g., Xerox® Workplace Suite/Cloud) with Single Sign-On functionality enabled, the user can agree to have their user credentials securely stored and automatically applied during subsequent app launches.

All communication is done via HTTPS and the data is transmitted securely and is protected by TLS security. The default TLS version used is 1.2. Xerox® App Gallery supplies a link to a Certificate Authority root certificate for validation with the cloud web service. It is the responsibility of the customer to install the certificate on their devices and to enable server certificate validation on the devices.

For more information related to Azure network security, please follow the link: <https://docs.microsoft.com/en-us/azure/security/azure-network-security>

XEROX WORKPLACE SUITE/CLOUD AND SINGLE SIGN-ON SERVICES

The Xerox® Workplace Suite/Cloud server accepts credential storage requests from the App via the SSO Manager service (the ConnectKey App retrieves a vault key from the SSO Manager and uses it to retrieve login credentials from the XWS/C service). All communication is via HTTPS and the data is transmitted securely and is protected by TLS security. The default TLS version used is 1.2.

2. Product Description

OVERVIEW

ConnectKey App

The ConnectKey App is a simple document signing solution for your Xerox® Device that integrates with SignNow eSignature workflows. The app assists the user with:

1. Browsing SignNow documents for previewing and printing.
2. Scanning a document into their SignNow account.
3. Scanning a document to create a new SignNow document based on a SignNow template.
4. Electronically signing documents sent to their SignNow account.

Application	What can I do?
ConnectKey App	<ul style="list-style-type: none">• Login to my SignNow account.• Browse, preview, and print SignNow documents.• Scan a document into your SignNow documents folder.• Scan a document and create a new SignNow document that is based on a selected SignNow template.• Sign documents sent to my SignNow Account.

Table 1 ConnectKey App user benefits

APP HOSTING

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

ConnectKey App

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

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

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

SignNow eSignature Web Service

The solution depends on the SignNow eSignature REST API to retrieve the user's folders, templates, and documents and to download and/or upload digital documents. 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® Connect for SignNow 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® Connect for SignNow App installed.

Xerox® Connect for SignNow App – Web Services

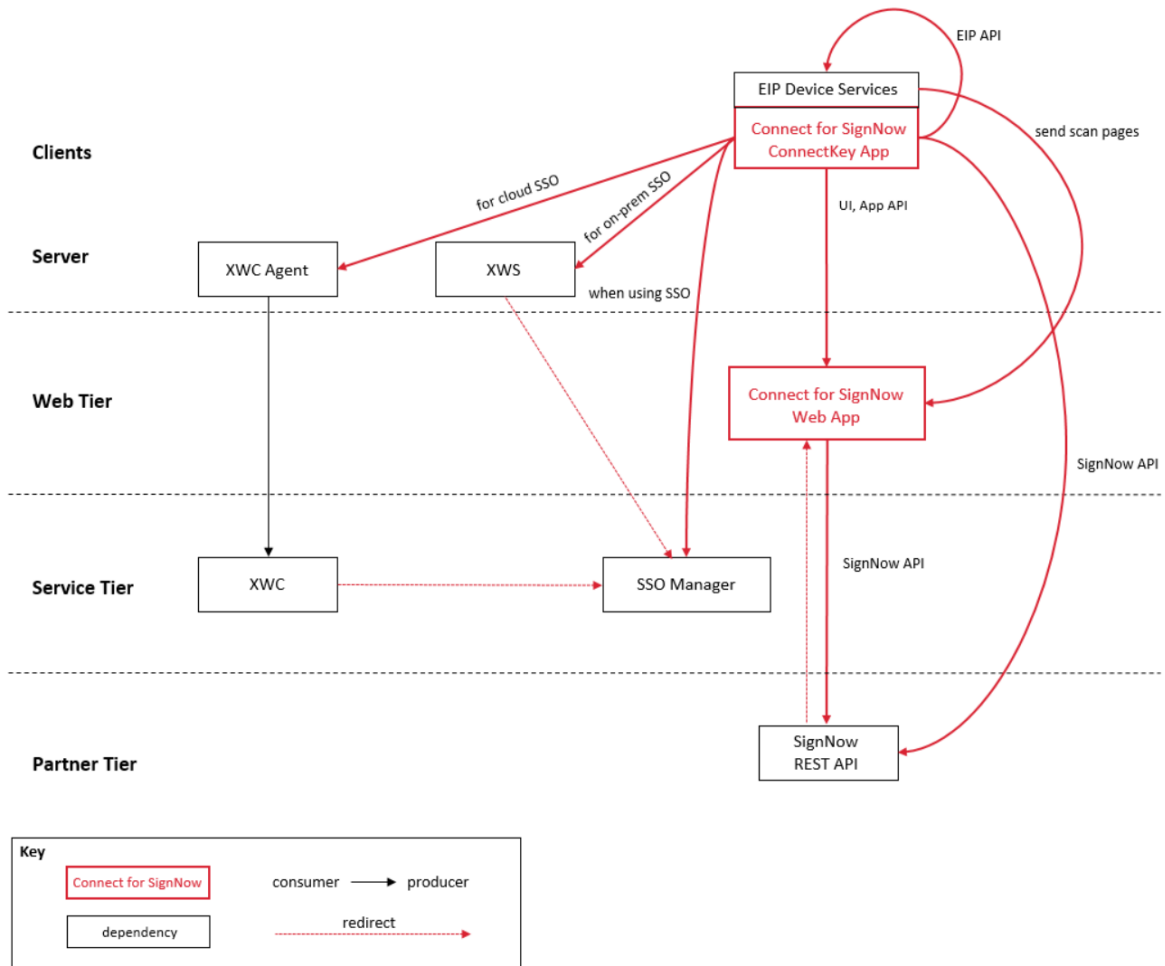
The Web Service is a service hosted on the Microsoft Azure Cloud System. The service is responsible for hosting the web pages which are displayed on the UI of the printer and provide the services support for the Xerox® Apps. The web service interacts with the SignNow services using the SignNow eSignature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

SignNow eSignature Web Service

The SignNow cloud hosted service provides a web API that is used for the eSignature workflow processes, which support the creation and downloading of digital documents for electronic signing.

ARCHITECTURE AND WORKFLOWS

Architecture Diagram



Workflows

Print SignNow document – Select and print document(s) from SignNow



Step 1: Launch the App on the Xerox device.



Step 2: Login with SignNow account credentials to view the Main page.



Step 3: Select the Print workflow.



Step 4: Browse to target folder, select document(s) to print.



Step 5: Optionally change the print settings.



Step 6: Print the document(s) using the Print button.

Scan to SignNow – Scan hard copy document into SignNow



Step 1: Launch the App on the Xerox device.



Step 2: Login with SignNow account credentials to view the Main page.



Step 3: Select the Scan workflow.



Step 4: Optionally modify the document name.



Step 5: Optionally change the scan settings. Select the Preview option if you want to preview the scan before uploading to SignNow.



Step 6: Scan the document(s) using the Scan button.



Step 7: If Preview was selected, view the scanned images.



Step 8: If Preview is satisfactory, tap Upload to save the document to your SignNow account.

Scan to SignNow with Template – Scan hard copy document into SignNow applying pre-defined Template which specifies Recipients and/or Signing Fields.



Step 1: Launch the App on the Xerox device.



Step 2: Login with SignNow account credentials to view the Main page.



Step 3: Select the Scan with Template workflow.



Step 4: Browse the folder tree and select the template.



Step 5: Optionally modify the document name.



Step 6: Optionally change the scan settings. Select the Preview option if you want to preview the scan before uploading to SignNow.



Step 7: Scan the document(s) using the Scan button.



Step 8: If Preview was selected, view the scanned image.



Step 9: If Preview is satisfactory, tap Upload to save the document to your SignNow account.

Sign a document – Select and sign documents that are waiting to be signed.



Step 1: Launch the App on the Xerox device.



Step 2: Login with SignNow account credentials to view the Main page.



Step 3: Select the Digitally Sign workflow.



Step 4: Browse the document list and select a document to sign.



Step 5: Optionally print to read the document.



Step 6: Preview the document and select a page that requires your attention.



Step 7: Mark each required field and repeat for each page as needed.



Step 8: To conclude the ceremony, tap Sign to send the signed document to SignNow.



Step 9: Optionally select Print in the confirmation alert to send the signed document to the Print workflow.

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

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

- Document images for preview are temporarily stored.
- Document files created from a SignNow template are temporarily stored.

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

- Job data

LOCAL ENVIRONMENT

Application data transmitted

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

- SignNow account data
- CK App 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 does not store any cookies on the device.

3. Additional Information & Resources

SignNow Security

SignNow has a strong background in IT security and SignNow has established itself as a highly secure and efficient e-signature platform for any kind of organization. With industry leading features like Advanced Threat Protection and Link protection, SignNow keeps your documents as safe and secure as possible.

For more information about SignNow security, see <https://www.signnow.com/security>.

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