Web Application Security Guide

Xerox® FreeFlow® Vision Connect Software

Document Version: 1.1 (March 2024).

BR40076

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

Overview

The Xerox® FreeFlow® Vision Connect is a cloud-based solution to intelligently monitor and control production devices. Xerox® FreeFlow® Vision Connect provides workflows that operates easily, adapts effortlessly, scales quickly, and delivers consistently.

The Xerox® FreeFlow® Vision Connect facilitates a combination of the following steps:

- Dashboard view of Xerox production devices
- Manage and monitor device events and metadata
- Analytics

Table 1.1 Xerox® FreeFlow® Vision Connect User Benefits

Application	What can I do?
Xerox® FreeFlow® Vision Connect	Onboard Xerox production devices Dashboard view of devices and its events Monitor and manage devices events

APP HOSTING

The Xerox® FreeFlow® Vision Connect depends heavily on cloud hosted components. 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 in US.

The Security highlights that are relevant to the Xerox® FreeFlow® Vision Connect are:

General Azure security

- Azure Security Center
- Azure Key Vault
- Log Analytics

Storage security

- Azure Storage Service Encryption
- Azure Storage Account Keys
- Azure Storage Analytics

Database security

- Azure SQL Firewall
- Azure SQL Connection Encryption

- Azure SQL Always Encryption
- Azure SQL Transparent Data Encryption
- Azure SQL Database Auditing

Identity and access management

- Azure Role Based Access Control
- Azure Active Directory
- Azure Active Directory Domain Services
- Azure Multi-Factor Authentication

Networking

- Azure Traffic Manager

Xerox® FreeFlow® Vision Connect

The Xerox® FreeFlow® Vision Connect consists of two key components:

- Printer Agent for FreeFlow Vision Connect
- Cloud Server for Vision Connect

COMPONENTS

Printer Agent for FreeFlow Vision Connect

The Printer Agent for FreeFlow Vision Connect is an on-prem application installed on DFE. This application forwards the engine events, consumables, and job information to the cloud hosted web app. Agent maintains the connection between the command center app service and the DFE.

FreeFlow Vision Connect Dashboard Portal – FreeFlow Vision Connect Cloud Server

The App 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 Mobile. The web service interacts with the Printer Agent for FreeFlow Vision Connect and Microsoft services using the Azure APIs.

The PWA cloud hosted service provides a dashboard view of devices and its events.

User can monitor and look at the details of the printer, based on the device entitlement.

The Printer events and metadata are presented to user.

The app allows to add users to the solution.

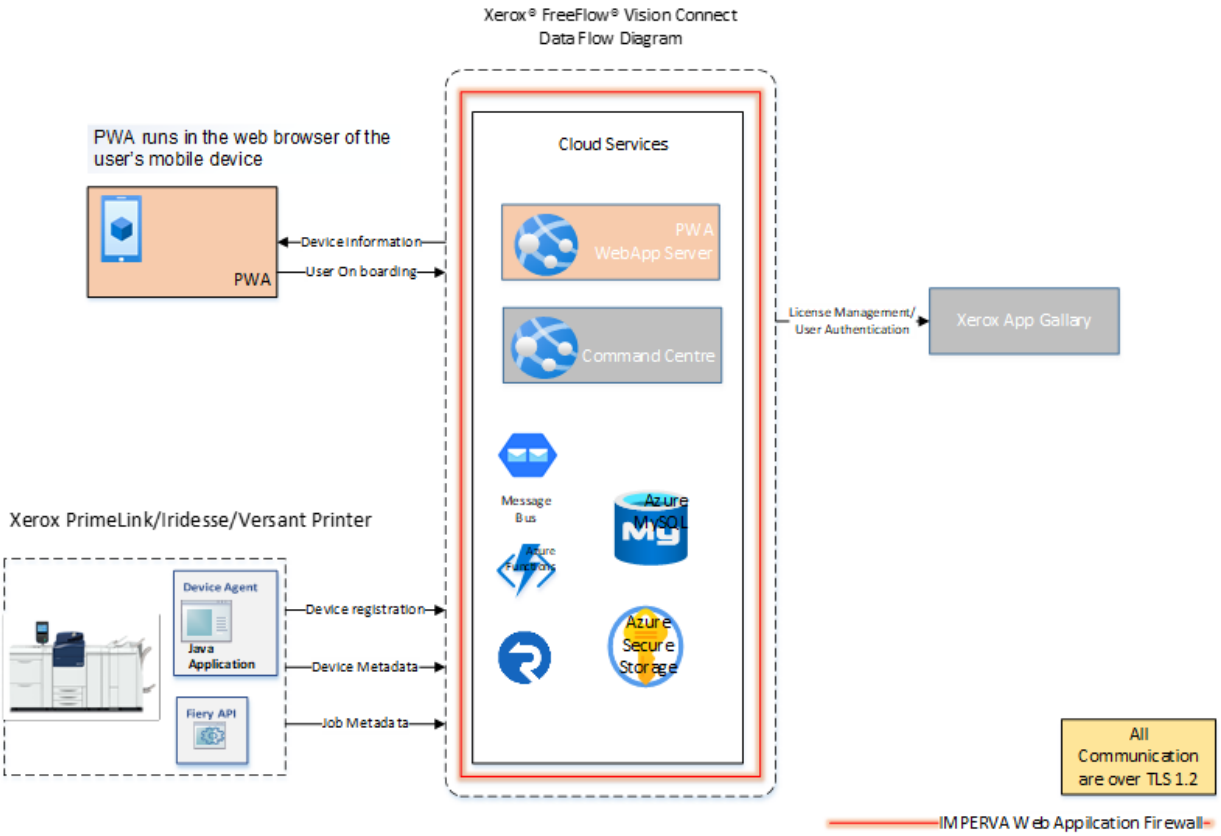
The app authenticates the user by username and password.

Users are automatically locked out of their account after 5 failed attempts.

The web app shall maintain an inactivity timer to automatically end user sessions.

Architecture and Workflows

DATA FLOW DIAGRAM



Workflows

For App onboarding Workflows, refer to the Workflows section in *Xerox® FreeFlow® Vision Connect Web Application User Guide.*

3. 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 your responsibility 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 your demand. The service is hosted both in the US and Europe. You are 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 detailed description, go to:

Azure Storage

https://azure.microsoft.com/en-us/blog/announcing-default-encryption-for-azure-blobs-files-table-and-queuestorage/

XAG AUTHENTICATION

The FreeFlow Vision Connect Single Sign-On feature integrates with the Xerox® App Gallery authentication solution to store user access information for SSO-compatible Xerox Gallery Apps. When you enter the storage service credentials for the first time, the Xerox® Workplace Suite/Cloud 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 Xerox® Workplace Suite/Cloud 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 detailed description, refer to the Xerox® Workplace Suite/Cloud Information Assurance Disclosure: https://security.business.xerox.com/en-us/products/xerox-workplace-suite/.

Xerox® FreeFlow® Vision Connect supports Azure AD and OKTA Authentication which is supported by XAG.

APPLICATION DATA STORED IN THE XEROX CLOUD

User data and device metadata are stored in the Azure SQL Database with Transparent Data Encryption
• Device data (Device Serial number)
• Configuration data (Device metadata and Job metadata)
• User details (User ID and Password)
Note:
• Ensure that the password contains alphanumeric and special characters.
• Do not use the User ID as password.
• Do not repeat the password which was previously used.

Application Data Stored on the Xerox Device Agent
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 Xerox® FreeFlow® Vision Connect stores cookies to complete the user session.
Note:
• User will be prompted to remain logged in on every combination of user, device, or browser after logging in.
• User will be prompted again if they explicitly logout.
• Users will be automatically logged out after a period of 7 days without any activity. Ensure that user request to stay logged in on every device or browser combination.

Audit Log
User and Administrator actions are logged in Audit log and stored securely.

User Data in Transit

SECURE NETWORK COMMUNICATIONS

The Imperva Web Application Firewall monitors the Azure App Service endpoints and secures the inbound traffic.
https://www.imperva.com/products/web-application-firewall-waf.

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® FreeFlow® Vision Connect requires you 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.

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. The app 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, follow the link, https://docs.microsoft.com/en-us/azure/security/azure-network-security.

XEROX APP GALLERY SERVICES

Communication between the App Gallery and selected Xerox App Cloud Services is using the following mechanisms:

Account API
The Account API allows selected Xerox App Cloud services and the Xerox App Gallery to share Common Xerox Accounts. API methods are secured by passing the user's session token.

Access List API
The Access List API allows selected Xerox App Cloud Services to specify which Common Xerox Accounts are entitled to manage and/or execute the app. API methods are secured by passing the user's session token.

License API
The License API allows selected Xerox App Cloud Services to interrogate the Xerox App Gallery for unexpired licenses associated with an Account. The API methods are secured by passing the user's session token.

Landing Pages
The Xerox App Gallery implements landing pages that may be invoked by selected Xerox App Cloud Services for common app functions. Landing pages are secured by passing the user's session token.

All the above communication uses HTTPS. Data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

4. Additional Information and Resource

Xerox® FreeFlow® Vision Connect Security

SECURITY @ XEROX

We maintain an up-to-date public webpage that contains the latest security information that pertains to its products. Refer to https://www.xerox.com/security.

RESPONSES TO KNOWN VULNERABILITIES

We have created a document that gives details of the Xerox Vulnerability Management and Disclosure Policy, which is used in the discovery and remediation of vulnerabilities in the Xerox® software and hardware. You can download this document from 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/