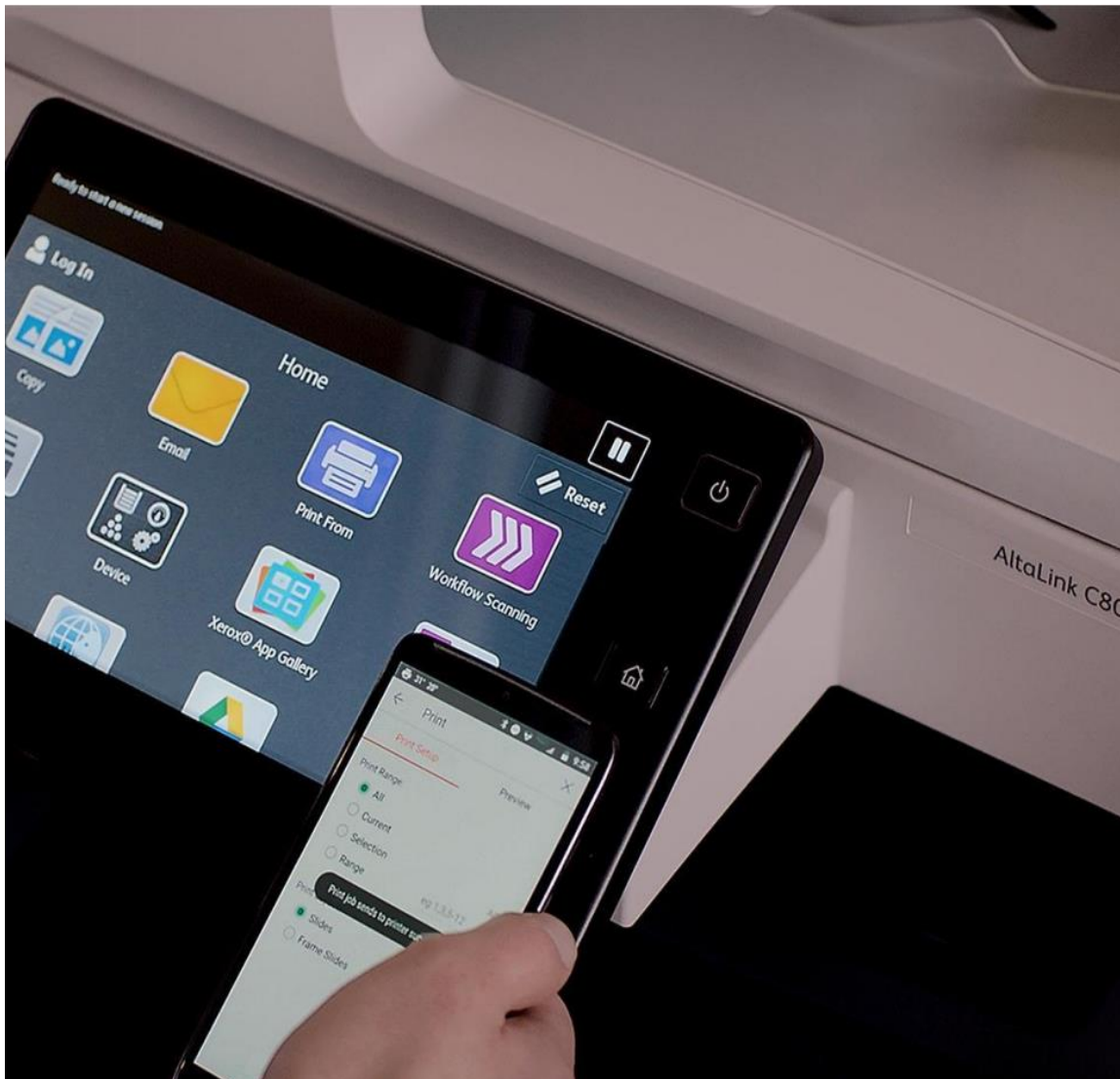


Security Guide

Xerox® Connect App for Moodle



© 2021 Xerox Corporation. All rights reserved. Xerox®, Xerox Extensible Interface Platform® and ConnectKey® are trademarks of Xerox Corporation in the United States and/or other countries. BR34378

Document Version: 1.1 (September 2021).

Contents

1. Introduction	1-1
Purpose	1-1
Target Audience	1-1
Disclaimer	1-1
2. Product Description.....	2-2
Overview	2-2
ConnectKey App	2-2
App Hosting.....	2-2
Components.....	2-3
Architecture	2-4
Architecture Diagram	2-4
User Data Protection.....	2-5
Application data stored in the Xerox cloud.....	2-5
Local Environment	2-5
PII Data Management	2-5
Clearing Device Browser Cache	2-6
3. General Security Protection.....	3-7
User Data Protection within Products	3-7
Document and File Security	3-7
Hosting - Microsoft Azure.....	3-7
Cloud Storage – Microsoft Azure	3-7
Xerox® Workplace Suite/Cloud and Single Sign-On Services	3-7
User Data in Transit	3-8
Secure Network Communications.....	3-8
Xerox Workplace Suite/Cloud and Single Sign-On Services.....	3-8
4. Additional Information & Resources.....	4-9
Security Xerox	4-9
Responses to Known Vulnerabilities.....	4-9
Additional Resources	4-9

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

CONNECTKEY APP

The Xerox® Connect App for Moodle enables users to access their Moodle storage account when scanning and printing documents. The app assists the user with:

- Browsing Moodle documents and folders.
- Selecting and optionally customizing print or scan settings.
- Submit print and scan jobs on the Xerox® Device.

Application	What can I do?
ConnectKey App	<ul style="list-style-type: none">• Login to my Moodle account and select print or scan• Browse Moodle folders and files• Select a document or destination• Customize the job settings (optional)• Submit the job to the Xerox® Device

Table 1 ConnectKey App user benefits

The Xerox® App is compatible with Xerox printers when the Xerox Extensible Interface Platform® version 3.5.0 or higher is enabled.

App Hosting

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

Xerox® Connect App for Moodle

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:

- 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.

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

Xerox® Connect for Moodle Service

The solution depends on the Moodle Cloud/Server service, which hosts the Moodle web service API. All requests are made over HTTPS using HTTP Basic authentication. A Moodle web service access token is required to access to the service. The Moodle web service access token is acquired during login, is unique to the authenticated user's account and is unique to the Xerox® Connect for Moodle app. When Single Sign-On (SSO) is being used, the Moodle web service

authorization token is securely stored in the Xerox® Workplace Suite/Cloud vault. All requests are made over HTTPS port 443.

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. The user security tokens are stored and secured by Xerox® Workplace Suite/Cloud.

Xerox Extensible Interface Platform®

During standard usage of the ConnectKey App, calls to the device web services are used to initiate and monitor scan and print functions and to pull relevant details related to device properties and capabilities.

Components

MFD with Xerox® Connect App for Moodle – 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® Connect App for Moodle installed. The Xerox® Connect for Moodle App is installed via the App Gallery.

Xerox® App Gallery

The App Gallery component is a web application, with services, hosted on the Microsoft Azure Cloud System. The App Gallery is accessed to ensure the Application is entitled to run and is used when upgrading the App whenever the auto-update conditions apply.

Xerox® Connect App for Moodle – Web UI

The Web UI component is a service hosted on the Microsoft Azure Cloud System. The Web UI component is responsible for hosting the web pages, which display on the UI of the printer.

Xerox® Connect App for Moodle – Service Interface

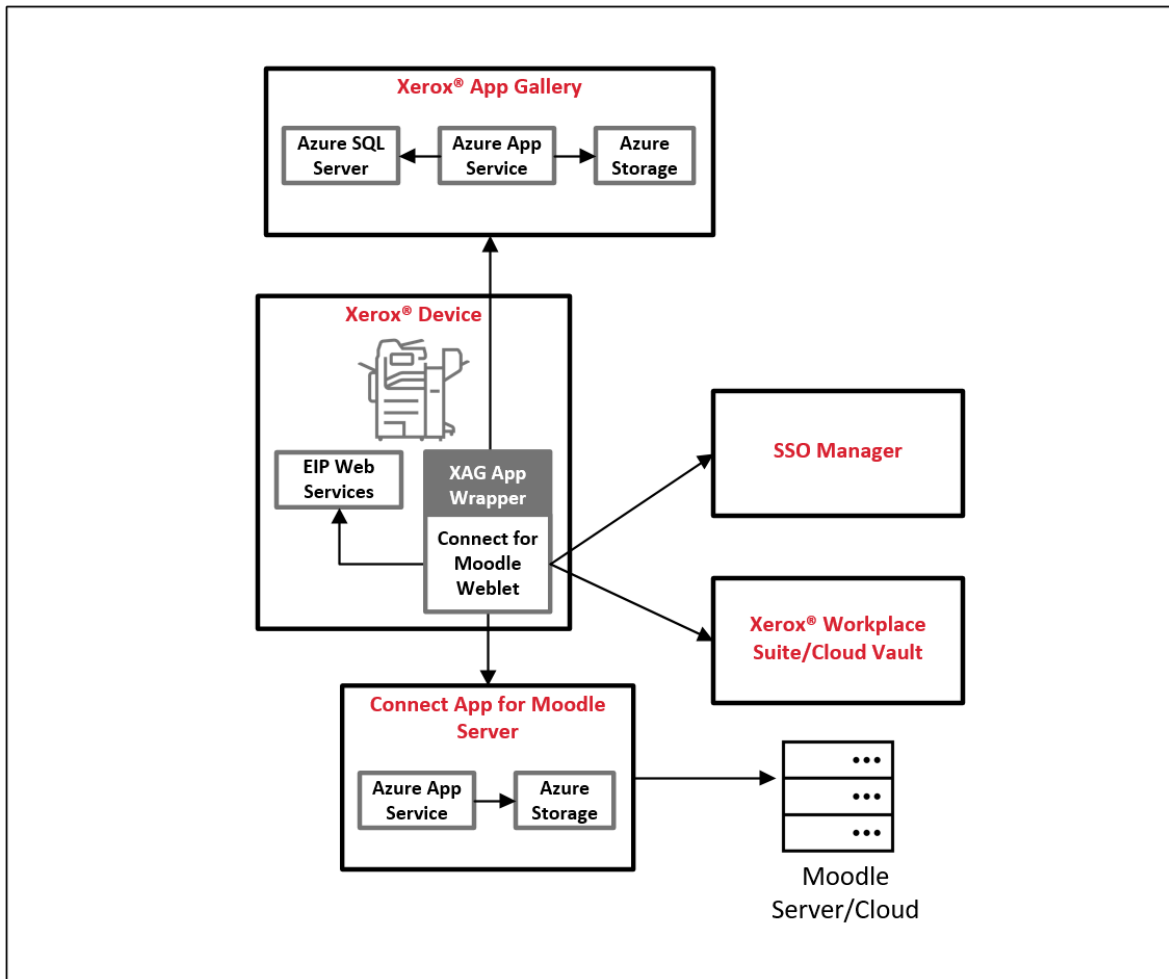
The Service Interface component is a service hosted on the Microsoft Azure Cloud System. The Service Interface provides the business logic service and interfaces using the Moodle APIs and Microsoft services using the Azure APIs.

Moodle Cloud

The Moodle cloud hosted service provides a web API that is used for retrieving repository structure, document files, and other user related data. The Moodle API consumed by the app supports authenticating the user for repository access, accessing user content, accessing site configuration, accessing courses and course content, accessing assignments, and uploading and downloading files.

Architecture

ARCHITECTURE DIAGRAM



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.

- When XWS/C SSO is enabled: Moodle authorization token

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.
- Closing the App

LOCAL ENVIRONMENT

Application data transmitted

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

- Moodle account data
- CK App session data
- Job data
- Document content

Application data stored on the Xerox device

The ConnectKey App does not store any data on the device.

HTTP Cookies

The ConnectKey App does not store any cookies on the device.

PII DATA MANAGEMENT

No Personally Identifiable Information (PII) is stored.

CLEARING DEVICE BROWSER CACHE

The Device Browser Cache is cleared when one of the following events occur.

- Device Logout
- Device Timeout
- Double Clear All
- Browser Restart
- Cycling the Browser from Disabled to Enabled

3. General Security Protection

User Data Protection within 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 Xerox® Connect App for Moodle 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 Xerox® App retrieves a vault key from the SSO Manager and uses it to retrieve the user's authorization token 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.

4. 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