Xerox®
Connect for Moodle App

Security Guide

Document Version: 1.0 (April 2019).

Table of Contents

1. Introduction

Purpose

The purpose of the Security Guide is to disclose information for Xerox® App Gallery 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® App Gallery 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® App Gallery apps do not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Xerox® App Gallery apps 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 is a solution for your Xerox® device that integrates with Moodle. This solution assists the user with the following:

1. Scanning documents to Moodle.
2. Printing documents from Moodle.

The table below describes what the application can do to benefit the user.

Application	What can I do?
ConnectKey App	• Login • Select Scan or Print workflow • Browse Moodle for a Scan destination or a file(s) to Print • Define Scan or Print Job settings • Submit Scan or Print Job to device for processing

App Hosting

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

ConnectKey App

The ConnectKeyApp consists of two key components, the device weblet and the cloud-hosted web service. The device weblet is a ConnectKey / EIP web app that:

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

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

Moodle Cloud/Server Service

The solution depends on the Moodle Cloud/Server service, which hosts the Moodle webservice API. All requests are made over HTTPS using HTTP Basic authentication. A Moodle webservice access token is required to access to the service. The Moodle webservice 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 webservice access token is securely stored in the Xerox® Workplace Suite/Cloud vault.

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 Device EIP Web Services

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

Components

MFD with Xerox® Connect for Moodle ConnectKey App

This is an EIP capable device capable of scanning and running ConnectKey Apps from the Xerox App Gallery. In this case, the device has the Xerox® Connect for Moodle App installed. The Xerox® Connect for Moodle App is installed via the Gallery.

Xerox® Connect for Moodle Web Service

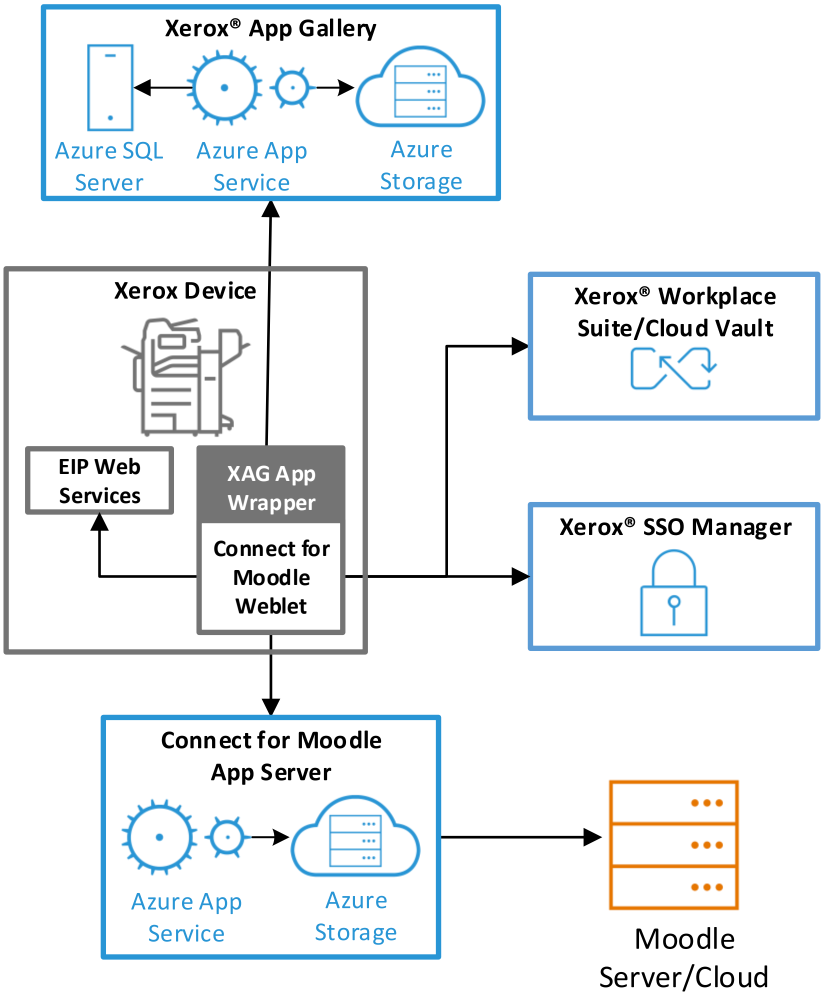
The Web Service is a service hosted on the Microsoft Azure Cloud System. The service is responsible for hosting the web pages which are displayed on the UI of the printer and provide the services support for the Xerox® apps. The web service interacts with the Moodle Cloud/Server service using the Moodle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

Moodle Cloud/Server Service

The Moodle Cloud/Server hosted service provides a Webservice API, which supports logging to a user account, accessing user account content, accessing site configuration, accessing courses, accessing course contents, accessing course assignments, uploading files and downloading files.

Architecture and Workflows

Architecture Diagram



Workflows

Login

Step 1: Launch the App on the Xerox device.

Step 2: Complete and submit the Login form.

Step 3: When the SSO configuration is enabled, optionally agree to save the credentials to XWS/C storage for future use.

Scan Documents to Moodle

Step 1: Launch the App on the Xerox device.

Step 2: Login to view the Main page.

Step 3: Select Scan Workflow option.

Step 4: Browse to destination for Scanned document

Step 5: Optionally change the scan settings.

Step 6: Submit the job using the Scan button.

Part 3 – Print Documents from Moodle

Step 1: Launch the App on the Xerox device.

Step 2: Login to view the Main page.

Step 3: Select Print Workflow option.

Step 4: Browse to document(s) to be printed.

Step 5: Optionally change the print settings.

Step 6: Submit the job using the Print button.

3. User Data 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 U.S. and Europe. Users will be routed to the closest server geographically based on server load and network speed.

Local Storage - ConnectKey App

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.

Cloud Storage - Microsoft Azure

Application data stored in the Xerox cloud

No Personally Identifiable Information (PII) is stored in the Xerox cloud.

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 ConnectKey App Single Sign-On feature integrates with the Xerox® Workplace Suite/Cloud Authentication Solution to store user access information for SSO-compatible Xerox® App 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® Connect for Moodle App and the Xerox® App Gallery are deployed to Microsoft Azure App Services. All web pages are accessed via HTTPS from a web browser. All communications to and from the Xerox® Connnect for Moodle App services 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® Connect for Moodle app 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 Authentication Solution) 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.

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 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

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/