Xerox®

Security Guide

for Connect App for Clio

BR25651 Document Version: 2.0 (April 2019).

Table of Contents

Table of Contents **3**
1 Introduction 4
Purpose **4**
Target Audience **4**
Disclaimer **4**
2 Product Description 5
Overview **5**
Single Sign On 5
App Hosting 5
Selection 5
Scanning 5
Printing 5
SNMP & Device Webservice Calls 5
Architecture and Workflows **6**
Architecture Diagram 6
3 User Data Protection 7
User Data Protection within the product **7**
User Data in transit **7**
Secure Network Communications 7
4 Additional Information & Resources 8
Security @ Xerox **8**
Responses to Known Vulnerabilities **8**
Additional Resources **8**

1 Introduction

Purpose

Xerox® Connect App for Clio is a Xerox Gallery App that allows users to connect into Clio, an SMB-focused Practice and Case Management service. The app provides a user the ability to scan a document into their account at a case/matter level, search for documents, and print the results. Expense data can be tracked and will be fed back into Clio for print and scan jobs.

The purpose of the Security Guide is to disclose information for Xerox Connect App for Clio 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 Xerox Connect App for Clio 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 Xerox Connect App for Clio does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Xerox Connect App for Clio 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 Xerox Connect App for Clio; 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

Xerox Connect App for Clio consists of two primary workflows. The two workflows are:

- Scan a document
- Print a document

The app and two workflows facilitate a combination of the following steps:

- Single Sign On
- App Hosting
- Selection
- Scanning
- Printing
- SNMP & Device Webservice Calls

Single Sign On
If a user is leveraging Xerox Workplace Suite/Cloud, the user can use Single Sign On to sign into the app. This works by storing the user's Clio sign in token within Workplace Suite/Cloud.

App Hosting
Xerox Connect App for Clio consists of three key components; the device app, the API, and the associated database. The device app is a ConnectKey®/EIP web app and the API is a REST API.

Selection
At various steps in the application, the user may be prompted to make selections. These selections include document metadata (Category), files to print, scan settings, and print settings. They are dynamic and are driven by API calls.

Scanning
When scanning, documents are scanned and submitted to the Clio API for upload. Due to the nature of the Xerox EIP scanning workflow design, the user's scan is temporarily persisted so document thumbnails can be pulled.

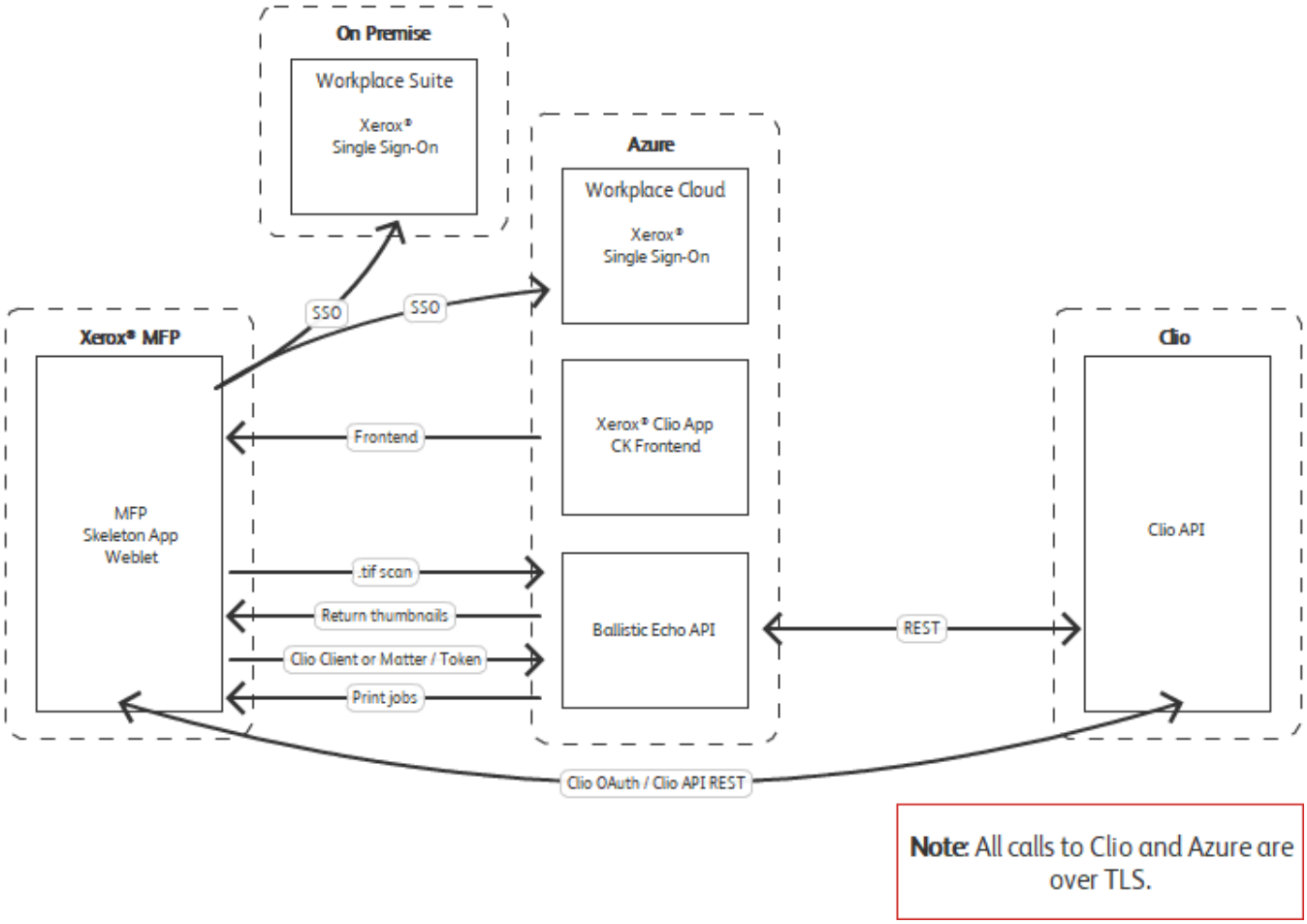
Printing
When printing, the selected document is pulled from Clio's API. Much like scanning, the document is temporarily persisted so document thumbnails can be retrieved.

SNMP & Device Webservice Calls
During standard usage of Xerox Connect App for Clio, local calls to SNMP are initiated to pull relevant details such as device language. The initiation of scan, print, and the usage of internal graphical components are also handled through these local web service calls.

Architecture and Workflows

Architecture Diagram

Below is a diagram that outlines what data is being processed and transmitted between each service.



3 User Data Protection

User Data Protection within the product

Xerox Connect App for Clio API and EIP app are hosted on the Microsoft Azure Network. Microsoft's Azure data center operations feature comprehensive information security policies and processes using standardized industry control frameworks, including ISO 27001, SOC 1, and SOC 2.

For a full description, please follow the link: https://docs.microsoft.com/en-us/azure/security/azure-network-security

User Data in transit

Secure Network Communications

Xerox Connect App for Clio and the API require that the device can communicate over port 443 outside the client's network. All web communications between the API, Clio, and Xerox devices are encrypted using HTTP Secure (HTTPS).

Documents that are scanned are temporarily stored as Azure blobs (raw image, thumbnails, etc.). The raw image is not accessible from anything other than the server-side code.

The thumbnails are stored using short live Secure Access Signature (SAS) URLs. Once the user is finished processing, the thumbnails are removed.

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

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