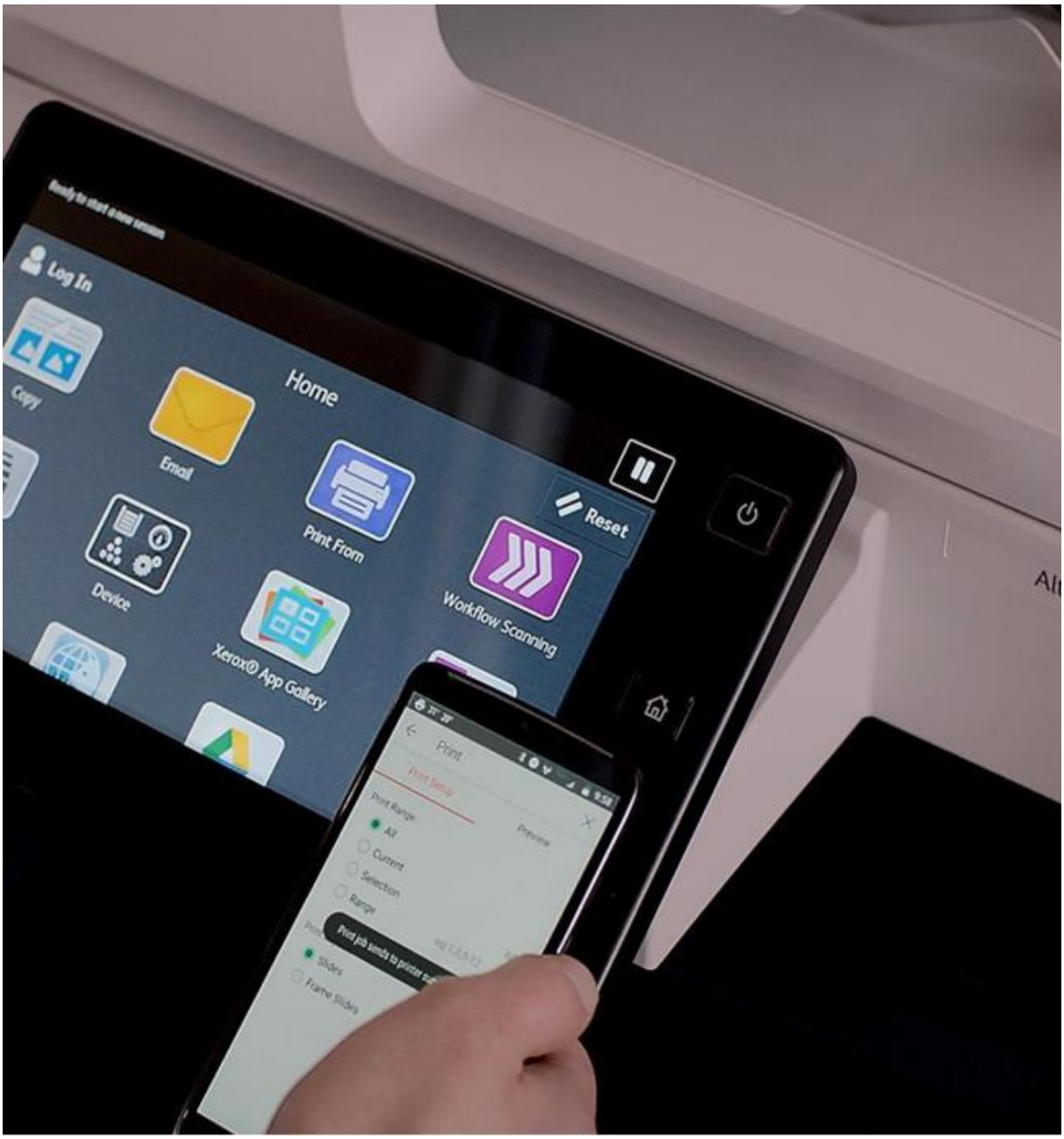
Security Guide

Xerox® Capture & Content App



xerox™

Document Version: 2.3 (Aug 2021).

Contents

1. Introduction

Purpose

Xerox® Capture & Content is a Xerox Gallery App that allows users to scan and submit documents from their Xerox Multifunction device to the Xerox® Global Capture Platform (GCP) where a Customer-aligned Capture & Content Service will automatically extract critical data, classify and catalog key information from the document and enable automation and streamlining of complex data-intensive business processes.

With the ability to persist metadata values and scan settings, completing a workflow and submitting documents to the Global Capture Platform is fast and efficient. Users can preview their scanned document, receive printed confirmations, and even receive an email confirmation at a later time, once the GCP workflow has fully processed the scanned document and data.

The purpose of the Security Guide is to disclose information for Xerox® Capture & Content App 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® Capture & Content App 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® Capture & Content App does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity, or Xerox® Capture & Content 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

Xerox® Capture & Content App consists of one primary workflow:

- Scan and submit documents

The app and workflow facilitate a combination of the following steps:

- App components and hosting
- Configuration
- Scan and submission to the GCP API
- Print
- Email
- Logging
- SNMP & Device Webservice Calls

App components and hosting

Xerox® Capture & Content App consists of five key components: the EIP web app, the EIP weblet, the REST API, the database, and encrypted blob storage.

The user installs the EIP weblet from the App Gallery onto a Xerox device. When a user runs the weblet, the EIP web app launches.

All components except for the EIP weblet are hosted in Microsoft Azure.

Configuration

Before you can run Capture & Content on your Xerox device, you must configure the app using App Gallery configuration. When you install the app for the first time, you'll be prompted to enter your Global Capture Platform client ID and server URL.

Scan and submission to the GCP API

Once the user has chosen a workflow and entered workflow metadata, a single or multi-page document can be scanned. The scanned document, along with the workflow name and workflow metadata values are then submitted to the Xerox GCP API over TLS. Once the data has been submitted, the user can receive a print and/or email confirmation (see **Print** and **Email** sections below).

To generate thumbnails for scan preview, the scanned document is temporarily stored in Azure encrypted blob storage for no more than 15 minutes.

Print

Users can enable Print confirmations in the app. If enabled, a confirmation sheet will print on the Xerox device when the document and data has been submitted to GCP for processing. Print confirmations may contain the serial number and user ID from the device.

Print jobs are retrieved via the REST API using a unique, time sensitive, complex identifier.

Email

Users can enable Email confirmations in the app. If enabled, an email will be sent to the specified email address at a later time, once the GCP workflow has fully processed the scanned document and data. Email confirmations may contain the serial number and user ID from the device.

No email configuration is required. The email will be sent from a noreply Xerox email address.

Logging

Logging is persisted on the server to aid with support and application scaling. Logging is transmitted over TLS and no personally identifiable information is stored.

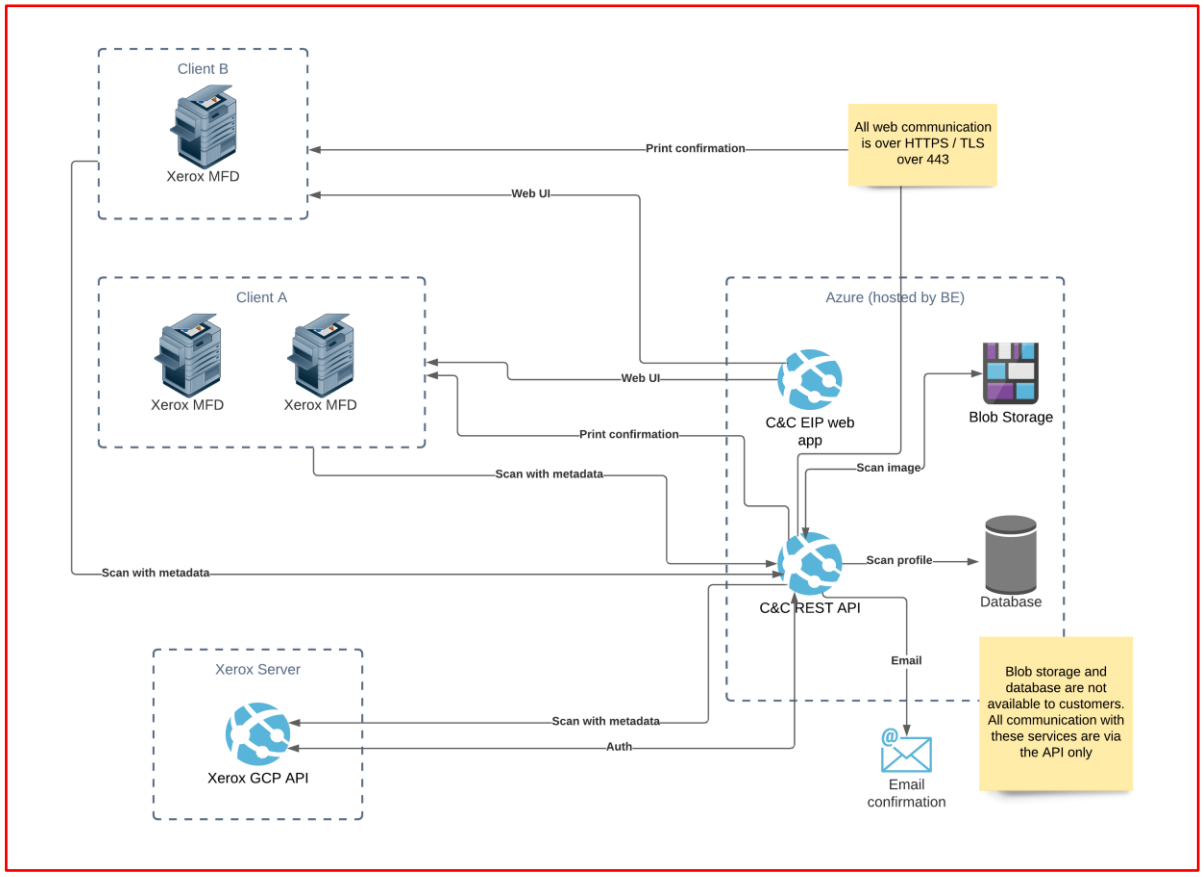
SNMP & Device Webservice Calls

During standard usage of Capture & Content, local calls to SNMP are initiated to pull relevant details such as device language. The initiation of scan and the usage of internal graphical components are also handled through these device level web service calls.

Architecture and Workflows

Architecture Diagram

Below is a diagram that outlines what's being transmitted between each service.



3. User Data Protection

User Data Protection within the Product

The Xerox® Capture & Content EIP web app, REST API, database, and encrypted blob storage are hosted on the Microsoft Azure Network. The EIP weblet is hosted in the Xerox App Gallery. 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.

For more information regarding user data protection provided by the Xerox® Multifunction Device, please reference your specific model's Security Guide.

User Data at Rest

Data Persistence

Scanned documents and print confirmations are temporarily persisted in encrypted blob storage for a maximum of 15 minutes. Azure blob storage is encrypted using 256-bit AES encryption and is FIPS 140-2 compliant.

The user's client ID, app ID, and device serial number are stored and encrypted in the database's session table for a maximum of 15 minutes. They may be needed to get a new session token while polling the status of the submitted document.

Local storage on the Xerox device is used to persist scan settings, which could include an email address.

The scan profile, which includes the workflow metadata and server URL, is stored for the duration of the user's session.

Logging is also persisted on the server to aid with support and application scaling.

User Data in Transit

Secure Network Communications

The Xerox® Capture & Content web app and API require that the device can communicate over port 443 outside the client's network. All communication between all aspects of the application are encrypted using HTTP Secure (TLS).

The selected workflow, the workflow metadata, and the scanned document are all transmitted to Xerox GCP API.

4. Additional Information and 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 the 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 1 Security Resources