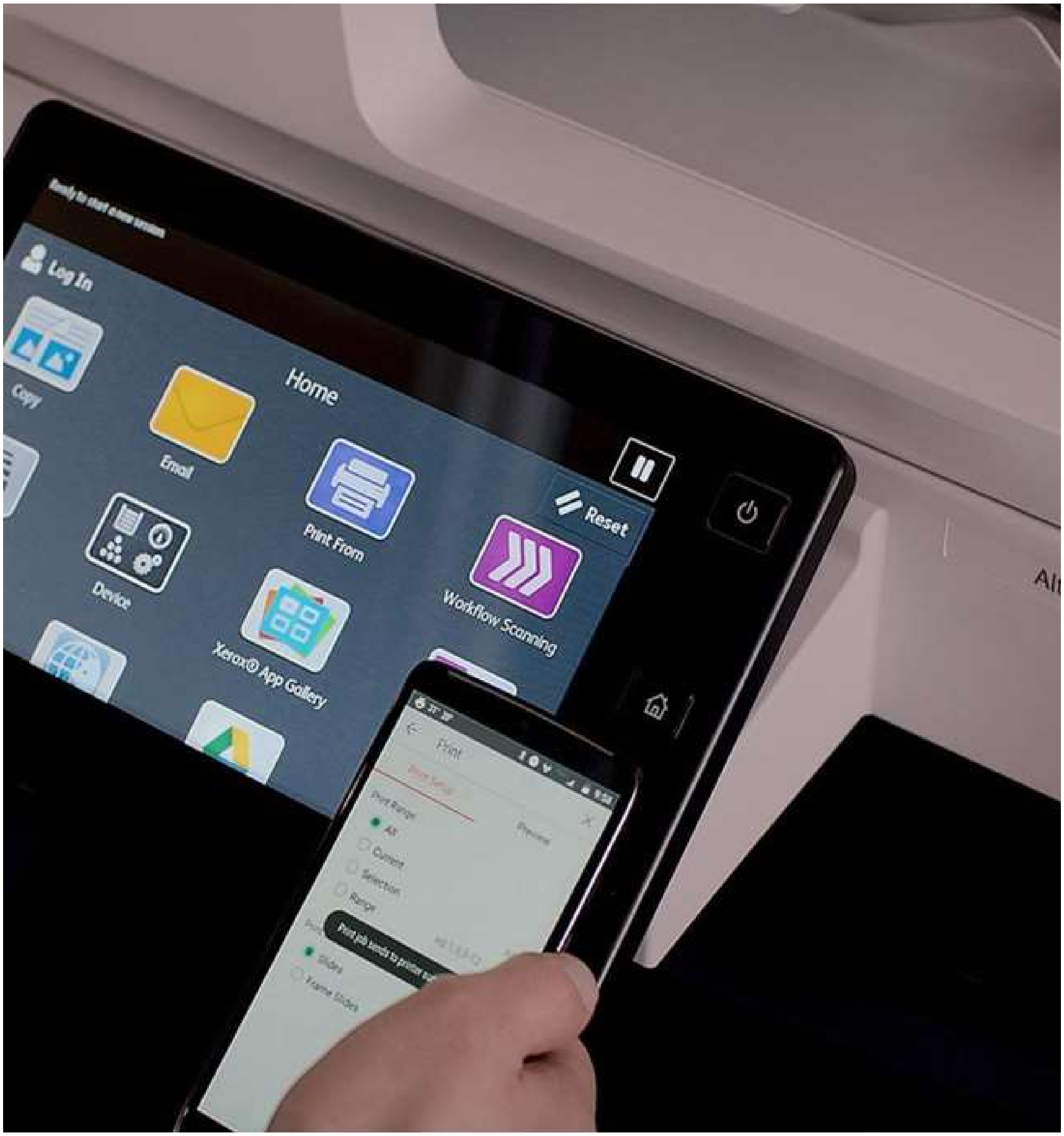
Security Guide

Xerox® Scanning App for Hyland OnBase



Document Version: 20240208

Contents

1. Introduction

Purpose

Xerox® Scanning App for Hyland OnBase (Scan to OnBase) is a Xerox Gallery App that integrates with Hyland OnBase and provides users the ability to scan and upload documents to their Hyland OnBase scan queue of choice. Scan to OnBase can be configured to work with your custom Hyland OnBase application server URL allowing any of your users to sign in and access their scan queues. Search makes it easy to find queues and Xerox SSO can be configured for a quick and efficient sign-in process.

The purpose of the Security Guide is to disclose information for Scan to OnBase 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 the design, functions, and features of Scan to OnBase 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® Scan to OnBase does not establish security for any network environment.

This document does not provide tutorial-level information about security, connectivity, or Scan to OnBase 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® Scan to OnBase consists of one primary workflow:

- Scan and upload a document to a Hyland OnBase scan queue

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

- App Components
- App Gallery Configuration
- Sign-In
- Xerox Single Sign On (SSO)
- Browse Scan Queues
- Search Scan Queues
- Scan and Upload
- Logging
- SNMP & Device Webservice Calls

App Components

Xerox® Scan to OnBase consists of four key components: the EIP web app, the EIP weblet, the REST API, and the database.

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.

The REST API interacts with the EIP web app, database, and Hyland OnBase SDK.

See **User Data Protection within the Product** on page 6 for details on hosting.

App Gallery Configuration

Before you can run Scan to OnBase on your Xerox® device(s), you must configure the app using App Gallery configuration. When you install the app for the first time, you will be prompted to specify:

- Hyland OnBase application server URL (required)
- Hyland OnBase license name (optional)
- Hyland OnBase data source (required)
- SNMP community name (required)

These values are passed by the EIP weblet to the EIP web app on app startup and are stored in local storage on the Xerox device.

Sign-In

When a user signs into Scan to OnBase on a Xerox device, the EIP web app sends the REST API the user's username and password. If the credentials are valid, a session token is generated, which the EIP web app uses on subsequent calls to the REST API.

Xerox Single Sign On (SSO)

If a user is leveraging Xerox Workplace Suite (XWS) or Xerox Workplace Cloud (XWC), they can use Xerox SSO to sign into the app. This works by storing the user's login details within Xerox Workplace Suite or Xerox Workplace Cloud.

Browse Scan Queues

During the workflow, users can browse the scan queues associated with their Hyland OnBase account. The REST API fetches this information from Hyland OnBase via the Hyland OnBase SDK.

Search Scan Queues

During the Browse workflow, users can search for scan queues associated with their Hyland OnBase account.

Scan and Upload

When a user scans a document, it is uploaded to the selected scan queue in Hyland OnBase.

Logging

Logging is persisted on the server to aid with support and application scaling. Logging is transmitted over TLS.

SNMP & Device Webservice Calls

During standard usage of Scan to OnBase, local calls to SNMP are initiated to pull relevant details such as device model, serial number, and MAC address. The initiation of scan and the usage of internal graphical components are also handled through these device-level web service calls.

3. User Data Protection

User Data Protection within the Product

The Scan to OnBase EIP web app, REST API, and database are hosted on the Microsoft Azure Network in both the US and Europe.

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 of Azure's security, 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

The user's username, password, session token, device ID, device MAC, Hyland OnBase data source, Hyland OnBase server URL, and Hyland OnBase license name are stored in the database for 15 minutes. This data is required to create and maintain session tokens. It's encrypted with AES-256.

Local storage on the Xerox device is used to persist the user's most recent scan settings, Xerox SSO login state (if enabled), and values from App Gallery Configuration, which includes the Hyland OnBase server URL, Hyland OnBase data source, Hyland OnBase license name, and SNMP community name. Local storage on the Xerox device is not accessible by the user.

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

User Data in Transit

Secure Network Communications

The Scan to OnBase EIP web app and REST API require that the device can communicate over port 443 outside the client's network.

The scanned document is transferred from the Xerox device to Hyland OnBase via the REST API. The document being transmitted could contain PII.

The Hyland generated session token is transmitted after login, as well as the Hyland server routing info, which includes username, password, device ID, device MAC, Hyland OnBase data source, Hyland OnBase server URL, and Hyland OnBase license name.

If the user is leveraging Xerox SSO, the device session username is retrieved from the device and sent to Xerox Workplace Suite/Cloud.

All communication between the device, REST API, EIP web app, and Hyland OnBase are securely transmitted over HTTP Secure (TLS).

4. Additional Information and Resources

Security Xerox

We maintain an evergreen public web page that contains the latest security information pertaining to its products. Please see https://www.xerox.com/security.

We have created a document that 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