# Security Guide

Xerox® Support Assistant App


xerox™

Document Version: 1.3 (August 2023).

# Contents

# 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

The Xerox® Support Assistant App consists of several workflows. The workflows supported are:

- View service incidents
- View supply incidents
- Create a service incident report
- Create a supply incident report
- Submit meters read from device
- Change App Settings

Completing a workflow involves a combination of the following aspects described in detail below.

- App Hosting
- Device Authentication
- App Startup
- View Service Incidents
- View Supply Incidents
- Provide New Service Incident Data
- Provide Contact Information
- Provide New Supply Incident Data
- Submit New Incident Report
- Read Device Meters
- Submit Device Meters
- Change App Settings

### APP HOSTING

The Xerox® Support Assistant App depends heavily on cloud hosted components. A brief description of each can be found below.

**Xerox® Support Assistant App**

The Xerox® App consists of two key components, the device weblet and the cloud-hosted web service. The device weblet is a Xerox® 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 querying device details.

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

**Xerox Extensible Interface Platform®**

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

## COMPONENTS

**MFD with Xerox® Support Assistant App – a 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® Support Assistant App installed.

**Xerox® Support Assistant App Service – UI & App API**

The UI and App API are hosted on the Microsoft Azure Cloud System. The UI aspect produces resources rendered by the embedded EIP browser. The App API is a facade wrapper accessed by the App client, which orchestrates downstream web communication.

**Xerox® Support Assistant App Service – Support Assistant API (SA-API)**

The SA-API aspect is hosted on the Microsoft Azure Cloud System. This aspect provides the business logic service and communicates with the Xerox Integration Service middleware component.

**Xerox® Integration as a Service**

The Xerox® Integration as a Service component is a service hosted on Xerox servers. This is middleware that enables integration at scale with the Xerox Services Manager system, orchestrating work on the App's behalf.

**Xerox Services Manager**

Xerox Services Manager is a web-based asset tracking and management application that provides a single point of management for all service-related incidents and helps organizations better understand and manage output costs. Its incident management component enables Xerox Authorized Managed Print Services Partners to track all service and support-related activities, improving output/performance and increasing device and end-user productivity.

**Xerox App Gallery**

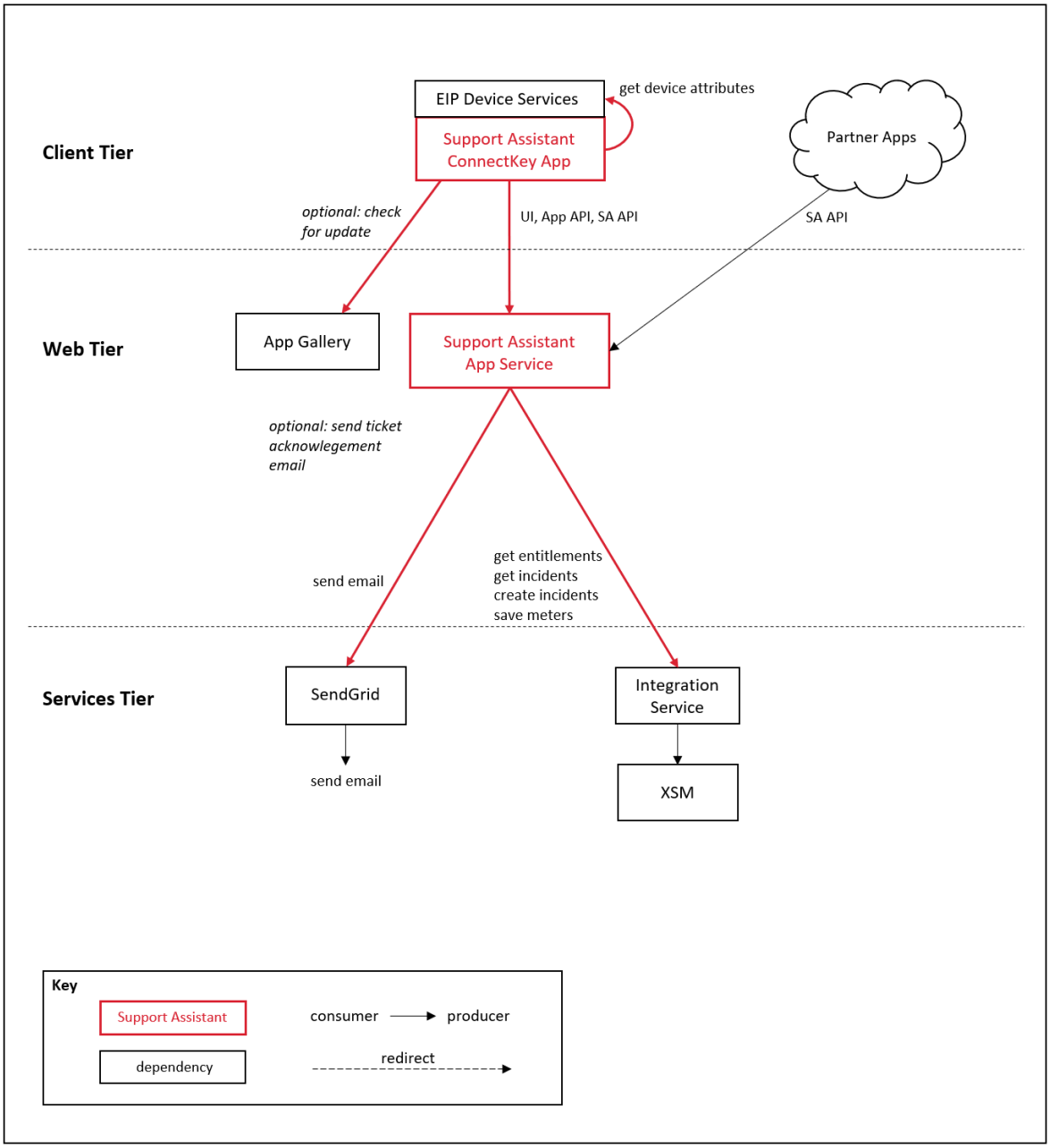
The App Gallery component is a web application, with services, hosted on the Microsoft Azure Cloud System. The App Gallery is accessed to ensure the App is entitled to run and is used when upgrading the App whenever the auto-update conditions apply.

**Twilio SendGrid® Email API**

The SendGrid Email API is a cloud API service produced by Twilio. The SendGrid Email API is used to send incident confirmation email notifications to users that create service or supply tickets.

# Diagrams

## DATA FLOW DIAGRAM



## Workflows

### DEVICE AUTHENTICATION

**Device login:** Prior to starting the Xerox® Support Assistant App, a device administrator authenticates using their device credentials. The device administrator can perform this step so that the Support Assistant App configuration settings can be viewed or changed.

The device login interaction uses the device login workflow, and sensitive tokens, cookies, or passwords related to the device login session are not accessible to the Support Assistant App.

### APP STARTUP

During startup of the Support Assistant App, the EIP browser runs the CK App HTML and JavaScript hosted on the device which fetches the App's UI content using Support Assistant App Service endpoints hosted in the Azure App Service.

The main page initialization script reads and decrypts the App Configuration data entered in the Xerox App Gallery prior to installation. The App Configuration data contains the SNMP Community String, an optional Logo URL, and access permissions for the creation of Supply Incidents, Service Incidents and submission of Meters.

Next, the main page initialization script executes local HTTP calls to device EIP web services in order to obtain relevant details associated with the device and its capabilities (i.e., Device Serial Number, MAC Address, Supplies List, etc.).

Finally, the main page initialization script calls the Support Assistant App API to get the Entitlements for the device upon which the App is executing. Entitlements specify whether a device is under contract for Service and/or Supplies.

### VIEW SERVICE INCIDENTS

When a user wants to view Service Incidents for the device, they will navigate to the Services tab in the Support Assistant App. The Support Assistant App calls the Support Assistant App API to retrieve Service Incidents, created within the last 30 days, for the device in use.

### VIEW SUPPLY INCIDENTS

When a user wants to view Supply Incidents for the device, they will navigate to the Supplies tab in the Support Assistant App. The Support Assistant App calls the Support Assistant App API to retrieve Supply Incidents, created within the last 30 days, for the device in use.

### CREATE A NEW SERVICE INCIDENT

When a user wants to create a new Service Incident for the device, they will navigate to the Services tab in the Support Assistant App. On the Services tab, the user will then click on the "Request Service" button.

The first step in creating a new Service Incident is to provide data for the Incident Report. The App will first display a list of common device issues. The user will then select the issue that best describes the service problem they wish to report. Next, the user will have an option to enter free form text to describe the service problem in more detail. Once the Service Incident Data is provided, the user selects "Next" to continue with the workflow.

### CREATE A NEW SUPPLY INCIDENT

When a user wants to create a new Supply Incident for the device, they will navigate to the Supplies tab in the Support Assistant App. On the Supplies tab, the user will then click on the "Request Supplies" button.

The first step in creating a new Supply Incident is to provide data for the Incident Report. The App will make local HTTP calls to device EIP web services to read the list of Supplies unique to the device. The App then displays the list of Supplies read from the device. The user will then select one or more supply items they wish to report as needing replacement. Once all the Supply Incident Data are provided, the user selects "Next" to continue with the workflow.

### PROVIDE CONTACT INFORMATION

The second step in creating either a new Service Incident or Supply Incident is for the user running the App to provide their contact information. The App will require the user to provide their Name, Email Address and Phone number. This information is used to send a confirmation email when the incident has been created. In addition, the information is used by Xerox in case they need to contact the user to gather additional information about the incident report. Once all of Contact information is provided, the user selects "Next" to continue with the workflow.

### SUBMIT A NEW INCIDENT

The final step in creating either a new Service Incident or Supply Incident is for the user to submit the report to Xerox for processing. The App will display the Incident Information for review by the user. The user can then select either "Send" or "Cancel".

If the user selects "Send" the App will call the Support Assistant App API to submit the new incident report to Xerox. The App will send an Email to user that contains the Incident Number, Creation Date and the Incident Data for the new incident.

If the user selects "Cancel", the workflow is terminated, and a new incident report is not submitted to Xerox.

### READ METERS

When a user wants to send the Billing Meters for the device, they will navigate to the Meters tab in the Support Assistant App. The Support Assistant App will make local HTTP calls to device EIP web services to read the meters from the device. The App will then display the Meter Names and Values read from the device.

### SUBMIT METERS

The final step in sending the Billing Meters is for the user to submit them to Xerox. To complete the workflow, the user selects the "Send Meter Reads" button. The App then calls the Support Assistant App API to submit the Meter Reads to Xerox. Finally, the App displays a confirmation screen indicating that the workflow has completed successfully.

### CHANGE APP SETTINGS

For users executing the Support Assistant App with device administrator privileges, the user can click on the Gear button to change the App's settings. The only setting available is the ability to turn "Demo Mode" either "On" or "Off". The "Demo Mode" feature of the App allows users to execute the App to see how it functions. Any data entered or retrieved is faked for demonstration purposes.

# User Data Protection

## APPLICATION DATA STORED IN THE XEROX CLOUD

No user data related to the App are stored in cloud persistent storage.

## APPLICATION DATA STORED IN THE TWILIO SENDGRID SERVICE

For detailed information on User Data Protection and Security for the Twilio SendGrid Service, please follow this link: https://www.twilio.com/legal/privacy/

## LOCAL ENVIRONMENT

**Application data transmitted**

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

- Account data
- Session data
- Xerox Services Manager incident data
- Metered supplies order data
- MFP device properties 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's SNMP V2 public community string

**HTTP Cookies**

The Xerox® Support Assistant App does not store any cookies on the device.

## PII DATA MANAGEMENT

**In Scope for this document:**

- Personal Data acquired and transmitted by the Xerox® Support Assistant App.

**Out of Scope for this document:**

- Personal Data acquired and maintained by
  - Xerox Services Manager
  - a Service Dispatch System
  - an Order Tracking System

The following personal data is acquired and transmitted by the Xerox® Support Assistant App. No personal data is stored and maintained by the Xerox® Support Assistant App.

- First Name
- Last Name
- Phone Number
- Email address

## 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. Network Information

## Protocol, Ports and URLs

The following table lists the protocol, ports and URLs used by the Xerox® Support Assistant when executing within a customer's private network. All public connections are outbound to Cloud hosted components.

| Protocol | Transport and Port Value | Use | Component | URL |
|---|---|---|---|---|
| **HTTPS using TLS** | TCP 443 | App UI | ConnectKey or EIP App to Support Assistant App Service Interface | supportassistant.services.xerox.com |
| **HTTPS using TLS** | TCP 443 | App Configuration | ConnectKey App to App Gallery | appgallery.services.xerox.com |
| **HTTPS using TLS** | TCP 443 | Subscription Entitlement | ConnectKey App to App Gallery | entitlements-appgallery.services.xerox.com |
| **SNMP** | | Device capability discovery<br><br>Public read<br><br>Internal pathway use only<br><br>Complies with the SNMP V2 data model | ConnectKey App initialization | localhost |

## Use of SNMP when operating the App

The App does not use the SNMP protocol while in use, so it is perfectly fine to disable SNMP connectivity if that protocol is not otherwise required by another app or service.

**IMPORTANT:** The App does interrogate MFD SNMP OIDs over an internal channel. That internal channel is independent and unrelated to the SNMP network connectivity protocol setting. Consequently, the SNMP V1/V2 Community READ String must be set.

The default SNMP V1/V2 Community READ String value is “public”.

The internal SNMP channel is enabled when the EIP SNMP Web Service setting is enabled. This setting must be enabled to operate the App as it was designed. The V1/V2 READ string setting is still required by the EIP SNMP Web Service even when the V1/V2 protocols are disabled by the MFD administrator.

Presuming the EIP SNMP Web Service setting is enabled, and the SNMP V1/V2 Community READ Name matches the App’s SNMP V1/V2 Community Name, then the SNMP queries executed by the App over the internal channel will be successful.

## Use of SNMP when installing the App

App Gallery and potentially other deployment tools may use the SNMP protocol when discovering MFDs on the network during device discovery. If SNMP dependent tools are not used when deploying the App across a fleet, then it is not required to enable any version of the SNMP protocol after the MFD administrator sets the V1/V2 READ string using supported device configuration methods.

# 4. General Security 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 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/

## 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.

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

# 5. 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 1 Additional Resources**