Security Guide

Xerox App Gallery 5.7.1

xerox™

Document Version: 1.5.1 (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. 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 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.

The Xerox App Gallery Database is hosted in the EU. Database backups are maintained in the US for up to one year. The Xerox App Gallery System Administrator is located in the US.

These Security highlights are relevant to the App Gallery system:

General Azure security

- Azure Security Center
- Azure Key Vault
- Log Analytics

Storage security

- Azure Storage Service Encryption
- Azure Storage Account Keys
- Azure Storage Analytics

Database security

- Azure SQL Firewall
- Azure SQL Connection Encryption
- Azure SQL Always Encryption
- Azure SQL Transparent Data Encryption
- Azure SQL Database Auditing

Identity and access management

- Azure Role Based Access Control
- Azure Active Directory
- Azure Active Directory Domain Services
- Azure Multi-Factor Authentication

Networking

- Network Security Groups
- Azure Traffic Manager

Please visit the Microsoft Azure Security web site for more information:
https://www.microsoft.com/en-us/trustcenter/security/azure-security

SENDGRID SERVICE

The solution provides for an email service, hosted by SendGrid. The email service sends Xerox App Gallery email notices to Xerox App Account owners using SMTP. These emails are generally confirmations of user actions, or admin actions affecting the user.

The App Gallery connects to SendGrid via a secured connection, using an API key. SendGrid servers are located in the US. For further details on SendGrid security, see: https://sendgrid.com/policies/security/. SendGrid relies on Standard Contractual Clauses (SCCs) to achieve GDPR. SendGrid retains email activity/history for 7 days. For further details on SendGrid privacy, see: https://www.twilio.com/legal/privacy.

2CHECKOUT/VERIFONE SERVICE

Xerox has partnered with 2Checkout/Verifone, (https://www.2checkout.com/) to act as Merchant of Record for Xerox App Gallery e-commerce transactions. The 2Checkout platform provides the e-commerce solution with a scalable multi-tenant SaaS eCommerce, payments and subscription management capability:

- PCI (Payment Card Industry Data Security Standard) compliance
- Security Certifications
- International Banking relationships
- Tax and VAT compliance
- Fraud and Risk management

The 2Checkout Service is accessed via 40+ globally distributed proxies hosted by a third-party service provider, providing DDoS mitigation, load balancing, failover, and security services.

- There are two 2Checkout Datacenters located within the European Union:
  - Eastern Europe (Romania)
  - Western Europe (Netherlands)
- One 2Checkout Datacenter is located within North America
  - Eastern United States
- There is an additional server in Russia for transactions made by shoppers with country='RU'.
- 2Checkout utilizes one Cloud storage provider for offsite storage of data backups, protected using industry standard strong encryption.
- 2Checkout utilizes multiple payment networks located in North America, Asia, and the European Union

For a 2Checkout GDPR statement go to: https://www.2checkout.com/policies/gdpr-compliance-statement . For further IAD concerning 2Checkout, contact: http://www.avangate.com/legal.php .

PAYMENT PROCESSORS

2Checkout/Verifone interacts with several different Payment Processors to debit customer (i.e., App Gallery user) credit card accounts. Payment Processors are located in various geographies; and specialize in transactions denominated in one or more currencies. The Xerox App Gallery has

no direct interaction with Payment Processors. For further IAD concerning 2Checkout and its interactions with Payment Processors, contact: http://www.avangate.com/legal.php.

MOODYS CORPORATION

The Xerox Sanctions service utilizes Moodys Analytics / Bureau Van Dijk “Orbis” and “Compliance Catalyst” products to provide corporate intelligence for purposes of denied parties screening and ongoing monitoring. Servers are located at several sites near Brussels, Belgium for fallover/redundancy purposes. One site is active while the other site is in standby mode. The sites are connected via protected optical links. Each site is protected by a denial of service layer and dedicated firewall. Daily backups are transferred to a special server containing enough disk space to keep three daily backups and three weekly backups at the same time. The backups on this server are transferred to tape on a weekly basis and stored off site. In 2022 Moodys will migrate the service to AWS hosting in Frankfurt with planned SOC II compliance.

A Moody’s Corporation GDPR Statement is available on request from privacy@moodys.com.

MICROSOFT AZURE AD

The Xerox App Gallery integrates with Microsoft Azure Active Directory. Azure AD acts as an Identity Provider for certain Enterprise Customer accounts within the App Gallery.

A Microsoft Privacy Statement may be found at: https://privacy.microsoft.com/en-us/privacystatement .

OKTA INC.

The Xerox App Gallery integrates with Okta Incorporated. Okta acts as an Identity Provider for certain Enterprise Customer accounts within the App Gallery.

An Okta Privacy Policy may be found at: https://www.okta.com/privacy-policy/ .

User Data in transit

WEB BROWSER AND THE APP GALLERY

App Gallery software executing on Azure servers uses the HTTPS protocol for all communication with App Gallery Web Pages. The minimum TLS version used is 1.2. The protocol establishes an HTTPS secure connection with the App Gallery Service, which relies on the web page OS to validate the security certificate as part of creation of the TLS connection. The TLS certificate is issued by Comodo (a trusted certificate authority) and ensures that the App Gallery webserver is in communication with the user's web browser, and no third party can pretend to be that webserver or intercept traffic between the web browser and the webserver.

The App Gallery requires users to authenticate before they can access features involving personal information. Basic authentication is performed with the Xerox App Gallery that transmits username and password information over the HTTPS protocol.

Once authentication is complete, data is passed between the Xerox App Gallery executing on Azure servers and the Xerox App Gallery Web Pages, to enable the features of the service within the Xerox App Gallery. This includes all data for apps, information for registered devices, and user data. App Gallery users are only able to access apps they created or purchased; and MFDs to which they have been granted access; and registered.

WEB BROWSER EXTENSIONS AND DEVICES

The Xerox App Gallery web browser extensions use SOAP messages, transmitted using the HTTP protocol on port 80, to find and add devices to a user's account. To add a device, a user must provide device administrator credentials and the SNMPv2 read/write community name string. The credentials and community string are securely stored as part of the device record in Xerox App Gallery database.

The Xerox App Gallery web browser extensions also use SOAP messages, transmitted using the HTTP protocol on port 80, to communicate with devices in order to accomplish app installation and uninstallation. The WSSE standard for SOAP messages is used to transmit nonce-protected hashes of device administrator credentials to the device to provide authorization.

GALLERY BROWSER AGENT AND THE APP GALLERY

Communication between the Gallery Browser Agent running on the user's PC and the App Gallery is done via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

GALLERY BROWSER AGENT AND THE DEVICE

Communication between the Gallery Browser Agent running on the user's PC and the Device is via EIP SDK methods. Messages are transmitted via HTTPS to devices supporting HTTPS; and messages are transmitted via HTTP to devices supporting only HTTP.

APP GALLERY AND SENDGRID

The Xerox App Gallery communicates with SendGrid to send emails using the SendGrid API defined at: https://sendgrid.com/docs/api-reference/. This communication is done via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

APP GALLERY APP AND APP GALLERY

The Xerox® App Gallery App, running on a device, communicates with the Xerox App Gallery using HTTPS. Data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

APP GALLERY APP AND DEVICE

The Xerox® App Gallery App, running on a device, communicates with the device to get a list of apps currently installed on the device and to install/upgrade apps on the device. The communication is via HTTPS and data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

APP GALLERY AND CLOUD REPOSITORY MIDDLEWARE

The Xerox App Gallery communicates with the Cloud Repository Middleware when a cloud repository app is installed on one or more devices. Xerox App Gallery registers the App and the Device Serial Numbers, where the App is being installed. This communication is done using a web service calls via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

CLOUD REPOSITORY DESIGNER APPS AND CLOUD RESIDENT REPOSITORIES

The Cloud Repository Middleware facilitates communication between the Xerox App Gallery Cloud Repository Apps and the Cloud Resident Repositories. This section describes the communication that occur between the Cloud Repository Designer Apps and the Cloud Repository Middleware as well as the communications between the Cloud Repository Middleware and the Cloud Resident Repositories.

Cloud Repository Designer App and Cloud Repository Middleware

At launch, the app must get an authentication/session token from the Cloud Repository Middleware Service in order to be given permission to access the cloud repository thru the Cloud Repository Middleware Service. The app requests the authentication/session token by transmission of the device serial number and the app id. The token is used for that session of the app. The app can then authenticate with the Cloud Resident Repository and then browse for folders and files. For Cloud Repository Designer Apps that do NOT use OAuth 2.0 for authentication, the app encrypts any user credentials sent to the Cloud Repository Middleware service as a URL query parameter.

All communication is done via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2. Xerox App Gallery supplies a link to a Certificate Authority root certificate for validation with Cloud Repository Middleware service. It is the responsibility of the customer to install the certificate on their devices and to enable server certificate validation on the devices.

Based on the type of app, either a print or scan job is initiated with the device. Once the job has been submitted, the device communicates with the Cloud Repository Middleware (See the section **Device and Cloud Repository Middleware** for details).

Device and Cloud Repository Middleware

The Scan and Print jobs submitted to a device communicate with the Cloud Repository Middleware via HTTPS and the data is transmitted securely and is protected by TLS security for both Upload and Download of documents. The minimum TLS version used is 1.2. All web service calls by the device, to the Cloud Repository Middleware, use the same authentication/session token acquired by the Cloud Repository Designer App.

Cloud Repository Middleware and Cloud Resident Repositories

The Cloud Repository Middleware routes incoming requests to the Cloud Resident Repository specified in the request (i.e. GoogleDrive, Dropbox, etc.). The Cloud Repository Middleware will decrypt any credentials before using them to access a Cloud Resident Repository.

The Cloud Repository Middleware uses a published API to communicate with each of the supported Cloud Resident Repositories. All communication is via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

MIDDLEWARE AZURE CLOUD SERVICE AND THE MIDDLEWARE AZURE CLOUD STORAGE

The Middleware Azure Cloud Service communicates with the Middleware Azure Cloud Storage via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2. Cloud Repository Middleware Service does a look up for a device serial number and app id pair in the Cloud Repository Middleware's Azure Cloud Storage when an app requests an authentication/session token.

CUSTOMER REPOSITORY DESIGNER APP AND CUSTOMER REPOSITORY SERVER

The Xerox App Gallery does not guarantee secure communications for the Print From URL app and the Scan to Multi-Destination app with the Customer Repository Server. It is the responsibility of the customer to install certificates on the device and repository server which would ensure secure communication.

MIDDLEWARE AZURE CLOUD SERVICE AND DOCUMENT CONVERSION

The Middleware Azure Cloud Service communicates with the Azure VM Document Conversion Engine via HTTPS and is protected by TLS security. The minimum TLS version used is 1.2.

APP WRAPPER AND APP GALLERY

Communication between the App Wrapper executing on the Device and the App Gallery software is via the Xerox e-commerce API. The communication is over HTTPS - and is hashed; but not encrypted. Hashing problems are detected at the receiving end, so that data tampering will be detected. The usage reported via the e-commerce API is not considered to be personal data; and is therefore not further encrypted.

The App Wrapper executing on the Device communicates with App Gallery software via the check app update API using HTTPS. Data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

APP GALLERY AND THE 2CHECKOUT/VERIFONE SYSTEM

Communication between the Xerox App Gallery and the 2Checkout/Verifone system is via the 2Checkout API 4.0 defined at: https://knowledgecenter.avangate.com/Integration/01JSON-RPC_API. Communication involves passing user data between the two systems. The user data includes user email address, company, and physical address. *NOTE: user physical address is stored by the Gallery while a transaction is in progress; but is not permanently stored in the App Gallery database.* Once the transaction has completed, the user physical address is permanently stored in the 2Checkout system. The following user Credit Card information is exchanged between the two systems: 1) last 4 digits, 2) expiration date, 3) card vendor.

The App Gallery utilizes the same URLs (described below) regardless of the Gallery User's country. This means that the physical locale of data processing and storage are the responsibility of the 2Checkout system for GDPR purposes.

Instant Payment Notification

When the details of an order change, the 2Checkout server will send to a predefined App Gallery URL an HTTP POST which encapsulates a data structure containing the information about the modified order. That information will be assigned a signature for authentication. The signature is realized using an HMAC_MD5 signature and a common secret key established between 2Checkout and the Xerox App Gallery. The HMAC algorithm is applied to all data sent. RFC 2104).

License Change Notification

When the details of a license change, the 2Checkout server will send to a predefined App Gallery URL an HTTP POST which encapsulates a data structure containing the information about the modified license. That information will be assigned a signature for authentication. The signature is realized using an HMAC_MD5 signature and a common secret key established between 2Checkout and the Xerox App Gallery. The HMAC algorithm is applied to all data sent. RFC 2104).

Buy/Renew Link

The App Gallery issues requests to 2Checkout on behalf of the Gallery user to Purchase or Renew a subscription in the 2Checkout system. Communication is via secure HTTP using a common secret key established between 2Checkout and the Xerox App Gallery.

2CHECKOUT SYSTEM AND PAYMENT PROCESSORS

For information on the interface between 2Checkout and the Payment Processors, contact 2Checkout at http://www.avangate.com/legal.php.

APP GALLERY AND APP CLOUD SERVICES

Communication between the App Gallery and selected Xerox App Cloud Services is via the following mechanisms:

Account API

The Account API allows selected Xerox App Cloud Services and the Xerox App Gallery to share Common Xerox Accounts. API methods are secured by passing the user's session token. The Xerox® Workflow Central App is an example of an app's cloud service that invokes the Account API.

Access List API

The Access List API allows selected Xerox App Cloud Services to specify which Common Xerox Accounts are entitled to manage and/or execute the App. API methods are secured by passing the user's session token. The Xerox® Workflow Central App is an example of an app's cloud service that invokes the Access List API.

License API

The License API allows selected Xerox App Cloud Services to interrogate the Xerox App Gallery for unexpired licenses associated with an Account. The API method is secured by passing the user's session token. The Xerox® Workflow Central App is an example of an app's cloud service that invokes the License API.

Landing Pages

The Xerox App Gallery implements landing pages that may be invoked by selected Xerox App Cloud Services for common app functions. Landing pages are secured by passing the user's session token. The Xerox® Workflow Central App is an example of an app's cloud service that invokes the gallery landing pages.

All of the above communication uses HTTPS. Data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

APP GALLERY AND SANCTIONS SERVICE

The App gallery communicates with the Sanctions Service to perform denied parties screening of Xerox App Accounts that are created or edited. The API is secured with an API Subscription Key, the individual functions are secured by Function Key, and a Client Key secures communication to known clients. Communication is done via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

XEROX SANCTIONS SERVICE AND MOODYS ANALYTICS / BUREAU VAN DIJK

The Xerox Sanctions Service communicates with Moodys Analytics / Bureau Van Dijk “Orbis” and “Compliance Catalyst” products to obtain corporate intelligence and add entities to a portfolio that Compliance Catalyst monitors for sanctions changes. The interface is secured via an API Token and credentials assigned to Xerox by BVD.

Documentation for the API may be found at https://documenter.getpostman.com/view/8532867/SWLh4mG7?version=latest .

APP GALLERY AND XEROX-BRANDED DEVELOPER APPS OR CLOUD REPOSITORY DESIGNER APPS

The App Gallery communicates with Xerox-branded Developer Apps or Cloud Repository Designer Apps via gallery API. The App uses the API to set and get a person’s “privacy preference”. These methods are secured with the app creator’s ID. The App utilizes this mechanism only when the person has authenticated with the Device to prevent the app from presenting the Xerox Corporate Privacy Statement to a person who has opted to not see it again. The App identifies the person to the Xerox App Gallery with a one-way hash of the person’s ID on the Device.

All of the above communication uses HTTPS. Data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

APP GALLERY AND OKTA INCORPORATED

The App Gallery communicates with Okta Incorporated via an Okta API. The gallery invokes an auth2 method on Okta, supplying a gallery user’s “email” address as a login hint. Okta interacts with the person to authenticate them. This may involve requesting a 2Factor code if the person’s Okta account is setup with Multi Factor Authentication. Okta then returns a token for the user, which the Xerox App Gallery uses to authorize subsequent activity during that gallery session. The gallery stores Okta’s “subject identifier” to link the person’s gallery account with the Okta account. The interface is secured with a “Client ID” and a “Client Secret” stored in an Azure Key Vault.

Documentation for the Okta API may be found at: https://developer.okta.com/docs/reference/.

APP GALLERY AND MICROSOFT AZURE AD

The App Gallery communicates with Microsoft Azure AD via a Microsoft API. The gallery invokes an auth2 method on Azure AD, supplying a gallery user’s “email” address as a login hint. Azure AD interacts with the person to authenticate them. This may involve requesting a 2Factor code if the person’s Okta account is setup with Multi Factor Authentication. Azure AD then returns a token for the user, which the Xerox App Gallery uses to authorize subsequent activity during that gallery session. The gallery stores Azure AD’s “subject identifier” to link the person’s gallery account with the Okta account. The interface is secured with a “Client ID” and a “Client Secret” stored in an Azure Key vault.

Documentation for the Azure AD API may be found at: https://docs.microsoft.com/en-us/azure/active-directory/authentication/overview-authentication

3. Xerox App Gallery – Xerox® ConnectKey® App

Description

OVERVIEW

This Xerox® Solution delivers 3 separate software offerings, each aligning to meet specific user goals. This section applies to the ConnectKey App.

ConnectKey App

The Xerox® App Gallery App is an application that comes pre-installed on Xerox® Devices. The purpose of the App is to provide access to the Xerox App gallery at the device. The App allows users, at the device, to Browse the Apps available in the Gallery, login to their account and install/upgrade one or more Apps. Users login to their account by supplying their email address and password. Or if their account is setup to authenticate with an Identity provider, the credentials required by the Identity Provider.

When a user who is currently logged into the device (with “device admin” privileges) executes the App and logs into their Xerox App Account, the App will give the user the option to have the Xerox App Account credentials “remembered” at the device. If the user chooses to have the credentials “remembered”, then any user who executes the Gallery App will automatically be logged into the first gallery user’s Account. A user who is currently logged into the device (with “device admin” privileges) also has the option to “clear” the “remembered” credentials from the device. The remembered gallery name and password token credentials are stored in the device browser’s internal storage and can only be retrieved by the Xerox® App Gallery App.

Table 1. ConnectKey App user benefits

Application	What can I do?
ConnectKey App	• Browse Gallery Apps • Login • Install an App from the App Gallery

APP HOSTING

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

ConnectKey App

The ConnectKey App consists of two key components, the device weblet and the cloud-hosted web service. The device weblet is a ConnectKey/EIP web app that enables the following behavior on a Xerox device:

1. Presents the user with an application UI that executes functionality in the cloud.
2. Interfaces with the EIP API to install gallery Apps on the Device.

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

Xerox Extensible Interface Platform®

During standard usage of the ConnectKey App, calls to the device web services are used to install and update Apps on the device.

COMPONENTS

MFD with Xerox App Gallery – ConnectKey App

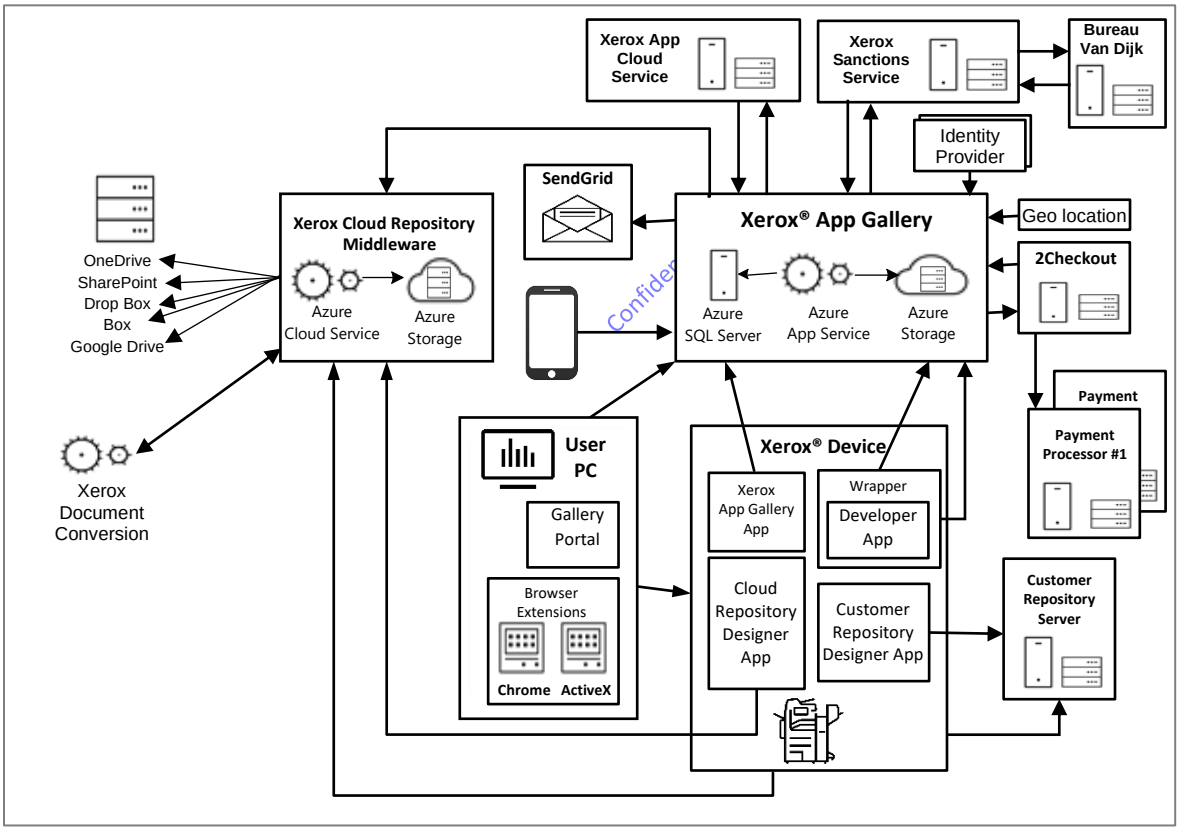
This is an EIP capable device that can execute ConnectKey Apps installed from the Xerox App Gallery.

Xerox App Gallery – Web Services

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.

ARCHITECTURE AND WORKFLOWS

Architecture Diagram



Workflows – ConnectKey App

Browse Gallery Apps

Step 1: Launch the App Gallery App at the MFD

Step 2: Browse “All Apps” in the app gallery.

Step 3: Select an App to view its “App Details" including: License Agreement, Privacy Statement and Software Disclosure.

Login

Step 1: Launch the App Gallery App on the MFD.

Step 2: Select the “Login” widget in the Action Bar

Step 3: Enter email of your Xerox App Account.

Step 4: Click on the Next button.

Step 5: Enter your password and MFA code if required by the IDP.

Step 6: Click on the OK button.

Install an App from the App Gallery

Step 1: Prerequisite – Log in to the App Gallery App
Prerequisite - for Ecommerce Apps, the App must have an active trial, or a license purchased for the App.

Step 2: Select an App to Install.

Step 3: Click on the “Install” button.

Step 4: Accept the End User License Agreement (EULA) for the App; and the system installs the selected App on the MFD.

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

User data related to the categories below are stored in cloud persistent storage to support the App Gallery App’s operation; or as a result of operations performed using the App Gallery App.

- Account data, including credentials, and ‘subject parameter’ – if authenticated by an IDP.
- Security Audit Log data, including UserId and MFD IP address.
- App data (to create installation weblets)
- App installation records

LOCAL ENVIRONMENT

Application data transmitted

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

- Account data
- Session 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.

- The App Gallery App weblet
- Xerox App Account parameters (excepting “password” which is replaced by a token)
- Scratchpad data storage

HTTP Cookies

The ConnectKey App does not store any cookies on the device.

4. Cloud Repository Designer Apps

Description

OVERVIEW

This Xerox® Solution delivers 3 separate software offerings, each aligning to meet specific user goals. This section applies to the operation of Cloud Repository Designer Apps hosted by the Xerox App gallery.

Cloud Repository Designer Apps

Xerox App Gallery allows users with a Channel Partner role to generate applications that interface with multiple commercial cloud resident repositories. These “Designer Apps” are connect-key apps which allow device users to scan documents to a supported cloud repository or print documents from a supported repository.

Table 2. Cloud Repository Designer App user benefits

Application	What can I do?
Cloud Repository Designer App	• Login to the Designer App • Scan to Cloud Repository • Print from Cloud Repository

APP HOSTING

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

Cloud Repository Designer App

The Designer App consists of two key components, the app that is installed on a MFD and the cloud-hosted web service. The Designer app:

1. Presents the user with an application UI that executes functionality in the cloud.
2. Interfaces with the EIP API, which delegates work to the Device, such as document scanning and printing.

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

Xerox Document Conversion Web Service

Xerox Document Conversion is a proprietary service used to convert non-print ready documents to a print ready a format. All requests are made over HTTPS.

COMPONENTS

Xerox Cloud Repository Designer Apps

Xerox App Gallery currently generates applications that interface with multiple commercial cloud resident repositories. These apps allow users to scan documents to a supported cloud repository or print documents from a supported repository.

Office 365 SharePoint Online – this cloud repository requires users to have an account with them. The Xerox® App Gallery App requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for Office 365 include a user ID and e-mail address which contains the Office 365 domain the user has permission to access. A password is also part of the credentials. With valid credentials, the Xerox® App Gallery App can browse the repository main site or team site, the libraries contained within and the folders in the libraries. The Xerox App Gallery can generate an app to scan to Office 365 and an app to print from Office 365.

DropBox – this cloud repository requires users to have an account with them. It supports password grant authentication. The DropBox repository requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for DropBox include a user ID which is the user's e-mail address and a password. Middleware requests these credentials and passes them to DropBox. With valid credentials, the DropBox repository asks for the user to give permission for the app to access the repository. Once given, the Xerox® App Gallery App can browse the repository's folders. The Xerox App Gallery can generate and app to scan to DropBox and an app to print from DropBox.

Box – this cloud repository requires users to have an account with them. It supports OAuth 2.0 authentication. The Box repository requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for Box include a user ID which is the user's e-mail address and a password. With valid credentials, the Box repository asks for the user to give permission for the app to access the repository. Once given, the Xerox® App Gallery App can browse the repository's folders. The Xerox App Gallery can generate an app to scan to Box and an app to print from Box.

Google Drive – this cloud repository requires users to have an account with them. It supports OAuth 2.0 authentication. The Google Drive repository requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for Google Drive include a user ID which is the user's e-mail address and a password. With valid credentials, the Google Drive repository asks for the user to give permission for the app to access the repository. Once given, the Xerox® App Gallery App can browse the repository's folders. The Xerox App Gallery can generate an app to scan to Google Drive and an app to print from Google Drive.

OneDrive – this cloud repository requires users to have an account with them. There are two account types, personal and business. Personal accounts support OAuth 2.0 authentication. The OneDrive repository requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for OneDrive include a user ID which is the user's e-mail address and a password. With valid credentials, the OneDrive repository asks for the user to give permission for the app to access the repository. Once given, the Xerox® App Gallery App can browse the repository's folders. For business accounts, the user must provide a user id and password, which the app uses to authenticate the user. The Xerox App Gallery can generate an app to scan to OneDrive and an app to print from OneDrive.

Cloud Repository Middleware

The Xerox® Cloud Repository Middleware is a web application hosted in the Microsoft Azure Cloud Computing Platform. The web application consists of Web Service API's (Azure Cloud Service) and table storage (Azure Storage). The Azure data centers used by the Cloud Repository Middleware are located in the European Union and the United States. Azure "Traffic Manager" routes incoming requests to an instance, running in an Azure data center, based on the geographic location the DNS query originates from.

Azure Cloud Service

The Azure Cloud Service, in the Cloud Repository Middleware, contains the Web Service APIs used to interface with the supported Cloud Resident Repositories and the proprietary Xerox Document Conversion service.

Azure Cloud Storage

The Azure Storage Tables, in the Cloud Repository Middleware, are used to store the list of authorized apps and devices that can access the Cloud Repository Middleware API. Azure Storage is also used to store diagnostic logs generated by the Azure Cloud Service. Access requires an Account Name and Access Key, which are stored and encrypted in each Azure Cloud Service instance.

Document Conversion

Xerox Document Conversion is a proprietary service used to convert non-print ready documents to a print ready a format. The service is hosted in an Azure VM Server. It is utilized for print jobs generated from the Xerox App Gallery print apps for the third party cloud repositories.

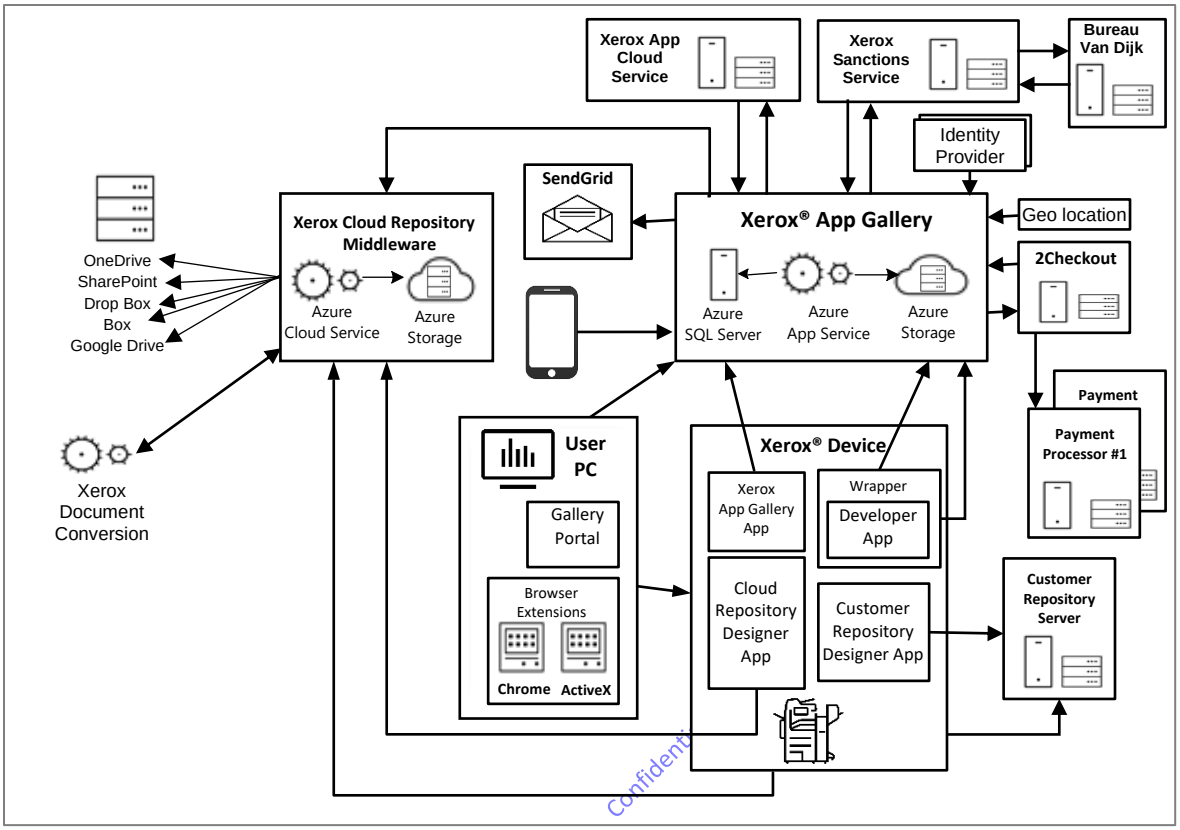
Customer Repository Designer Apps

Xerox App Gallery currently generates applications that interface with a customer hosted repository server using a variety of supported protocols. These generated apps can scan documents using FTP or SMB as well as print documents using HTTP/HTTPS.

Customer Repository Server

This server is configured and controlled by Xerox customers. It is the customer's responsibility to secure access to the server. A Customer Repository Server can be configured to allow for FTP, SMB and HTTP/HTTPS communications to allow for scanning and printing of documents.

Architecture Diagram



Workflows – Cloud Repository App

Login to the Designer App

Step 1: Prerequisite – the user has an Account on the Repository.

Step 2: Launch the Designer App on the MFD.

Step 3: Provide your repository account credentials.

Step 4: Complete the Login process.

Scan to Cloud Repository

Step 1: Select a Location on the repository on which to place the scanned images.

Step 2: Specify the name of the file and the file type to be created.

Step 3: Optionally change the scan settings.

Step 4: Submit the job using the Scan button.

Print from Cloud Repository

Step 1: Select a file on the repository to print.

Step 2: Optionally specify Quantity and other print settings.

Step 3: Submit the job using the Print button.

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

User data related to the categories below are stored in cloud persistent storage.

- Account Name and Access Key

LOCAL ENVIRONMENT

Application data transmitted

Application data related to the categories below are transmitted to/from the cloud repository designer app.

- Account data on the repository
- Session data
- Job data
- Job files

Application data stored on the Xerox device

The following app data is stored on the device, in persistent storage, until the Designer App is uninstalled from the device.

- The designer app weblet
- Configuration data (for Info Apps)
- Repository Certificate Bundle
- OAUTH tokens for Repository access
- Scratchpad data storage

HTTP Cookies

The Cloud Repository Designer App does not store any cookies on the device.

5. Xerox App Gallery – Web Portal

Description

OVERVIEW

This Xerox® Solution delivers 3 separate software offerings, each aligning to meet specific user goals. This section applies to the App Gallery web portal.

Web Portal

The Xerox App Gallery is a:

1. Marketplace that allows Gallery users to browse Xerox® ConnectKey® Device Apps and purchase and/or install the Apps on the devices themselves.
2. Xerox Workflow Solution that allows the creation of Xerox® ConnectKey® Device Apps, by Channel Partners, and the placement of the Apps on the devices themselves. There are several App types:

    - Information,
    - Scan To E-Mail,
    - Scan To Multiple Destinations,
    - Scan To Office 365 SharePoint Online,
    - Scan To Dropbox,
    - Scan To OneDrive,
    - Scan to Box,
    - Scan to GoogleDrive,
    - Print From URL,
    - Print From Office 365 SharePoint Online,
    - Print From Dropbox,
    - Print From OneDrive,
    - Print From Box, and
    - Print From GoogleDrive

Table 3. Web portal user benefits

Application	What can I do?
Web portal	Web Portal Account Creation and Login Workflows • Create and Validate an Account • Create and Validate a Developer Account • Create and Validate an Associated Account • Login Web Portal Designer App Creation Workflows • Create ConnectKey Info App • Create ConnectKey Scan Apps • Create ConnectKey Print Apps Web Portal Browse the App Gallery Workflows • Browse gallery Apps (not logged in) • Browse gallery Apps (with login) Web Portal Device Workflows • Add a Device to the Account • Discover Devices for the Account Web Portal Purchase and Installation Workflows • Install an App from the App Gallery • Activate a Trial • Purchase a “Per Device” App • Purchase an “Unlimited Devices” App Web Portal App Management Workflows • Configure App • Download App Executed by Xerox, upon request. • Request that my account be deleted

APP HOSTING

The web portal is a cloud hosted website. A brief description can be found below.

Web Portal

The solution supports gallery accounts which allow access to gallery functionality. The portal provides support for features related to accounts, app management, and device management.

COMPONENTS

Xerox App Gallery – Portal Web App

Access to the Xerox App Gallery is allowed through the following list of supported Web Browsers: Microsoft Edge v79 or higher, Microsoft Internet Explorer v11.0 or higher and Google Chrome v60.0 or higher.

Browser Extensions

In addition, each supported browser requires the installation of a Browser Add-On/Extension. The Browser Add-On/Extension is required to access the Xerox® Device for adding/removing devices in a user's account as well as the install/update/uninstall of Apps. The Microsoft Internet Explorer Browser uses an ActiveX control. The Google Chrome Browser and the Microsoft Edge Browser uses a standard Chrome Extension. The ActiveX control is hosted in the App Gallery web portal for download and installation by the IE Browser. The Chrome Extension is hosted in Google's Chrome web store for download and installation by the Edge Browser or Chrome Browser.

The Gallery also requires an extension (such as Meta4 ClickOnce Launcher) for the Chrome Browser to launch the Microsoft ClickOnce installer. ClickOnce is used to install the Gallery Browser Agent on the user's PC. Note that Microsoft Internet Explorer is able to natively launch the Microsoft ClickOnce installer.

Gallery Browser Agent

The Gallery Browser Agent is temporarily installed on the user's PC whenever the gallery user initiates a Discovery Session to find Xerox multi-function devices on the network segment the PC is connected to. The GBA is a Full Trust Application for the Microsoft .NET 4.7.2 framework. The user must allow the GBA to be installed on the PC and the user must have installation permissions for the PC.

The App Gallery initiates a Gallery Browser Agent session and supplies the GBA with IP addresses (provided by the user) to discover. Based on a user setting, the GBA communicates with the device to prepare it to be added to the user's Account. The Gallery Browser Agent periodically informs the App Gallery of the discovered Xerox MFDs.

All communication between the GBA and the App Gallery uses REST methods and is via HTTPS. Communication between the GBA and the Device is via EIP SDK methods. Messages are transmitted via HTTPS to devices supporting HTTPS; and messages are transmitted via HTTP to devices supporting only HTTP.

Xerox App Gallery – Portal Web Services

The Xerox App Gallery is a web application hosted in the Microsoft Azure Cloud Computing Platform. The web application consists of web pages (Azure App Service), functions (Azure Functions), file storage (Azure Storage) and a database (Azure SQL Server). The Azure data centers used by the App Gallery are located in the European Union and the United States. Azure "Traffic Manager" routes incoming requests to an instance, running in an Azure data center, based on the geographic location the DNS query originates from.

Azure App Services

The web pages, for the Xerox App Gallery, are deployed in a Microsoft Azure App Service. All web pages are accessed via HTTPS from a Web Browser. All communications to and from the Xerox® App Gallery App Service are over HTTPS. Data is transmitted securely and is protected by TLS security for both upload and download. The minimum TLS version used is 1.2.

Xerox App Gallery users must authenticate with the Xerox App Gallery Service to access the web pages that contain personal information. Authentication with the Xerox App Gallery Service requires the entry of an email address and password known by the system. Passwords are required to be a minimum of 8 characters and contain at least one character that meets 3 out of 4 of the following character restrictions: Upper Case Alpha, Lower Case Alpha, Numeric, Punctuation.

Once authenticated, the user can view and modify:

1. Account profile
2. All apps created by the user through the App Gallery system
3. All app configuration data created by the user through the App Gallery system
4. All devices registered by the user in the App Gallery system

Non-authenticated users may access the non-restricted Xerox App Gallery web pages. This includes viewing:

1. All Publicly available Apps
2. Details for a Publicly available App

Azure SQL Server

Azure SQL server stores and protects the data used by the Xerox App Gallery. Both “Advanced Threat Protection” and “Transparent data encryption” are enabled. In addition, the database is encrypted. Communications to the Azure SQL Server are only by the Azure App Services using TCP over Port 1433.

Azure Cloud Storage

Azure Cloud Storage contains a file repository used by the App Gallery. Access requires an Account Name and Access Key, which are securely stored in the configuration for each Azure App Service deployment. Only authorized Xerox IT personnel have access to these keys via Microsoft’s Azure Management Portal.

Azure Functions

Azure Functions are used for the following purposes: providing gallery email (and communication with the SendGrid mail service), providing App licensing (and communication with the eCommerce provider), and App execution entitlement (and communication with an App or App Wrapper).

SendGrid Service

The solution provides for an email service, hosted by SendGrid. The email service sends Xerox App Gallery email notices to Xerox App Account owners using SMTP. These emails are generally confirmations of user actions, or admin actions affecting the user.

The App Gallery connects to SendGrid via a secured connection, using an API key. For further details on SendGrid security, see: https://sendgrid.com/policies/security/ .

2Checkout/Verifone Service

Xerox has partnered with 2Checkout, formerly known as Avangate Inc., (https://www.2checkout.com/) to act as Merchant of Record for Xerox App Gallery e-commerce transactions. The 2Checkout platform provides the e-commerce solution with a scalable multi-tenant SaaS eCommerce, payments and subscription management capability:

- PCI (Payment Card Industry Data Security Standard) compliance
- Security Certifications
- International Banking relationships
- Tax and VAT compliance
- Fraud and Risk management

This partnership allows App licenses to be sold in gallery-supported countries world-wide.

The e-commerce provider maintains an account for each it's 'customers' (i.e. Gallery users who make App purchases.) The customer account contains user data such as the customer's email address, company, and physical address. 2Checkout maintains a history of the customers' Credit Card transactions; and maintains Credit Card information on file as a convenience to the customer, and to satisfy legal requirements.

The customer has the option to prefill credit card information from the previous purchase. This option defaults to "don't prefill".

The 2Checkout Service is accessed via 40+ globally distributed proxies hosted by a 3rd party service provider, providing DDoS mitigation, load balancing, failover, and security services.

- There are two 2Checkout Datacenters located within the European Union:
  - Eastern Europe
  - Western Europe
- One 2Checkout Datacenter is located within North America
  - Eastern United States
- One 2Checkout Datacenter is located in Russia for transactions involving users with country=RU.
- 2Checkout utilizes one Cloud storage provider for offsite storage of data backups, protected using industry standard strong encryption.
- 2Checkout utilizes multiple payment networks located in North America, Asia, and the European Union

For a 2Checkout GDPR statement go to: https://www.2checkout.com/policies/gdpr-compliance-statement . For further IAD concerning 2Checkout, contact: http://www.avangate.com/legal.php.

Payment Processors

2Checkout interacts with several different Payment Processors to debit customer (i.e. App Gallery user) credit card accounts. Payment Processors are located in various geographies; and specialize in transactions denominated in one or more currencies. The Xerox App Gallery has no direct interaction with Payment Processors. For further IAD concerning 2Checkout and its interactions with Payment Processors, contact: http://www.avangate.com/legal.php.

Multifunction Devices

Xerox Multifunction Devices have a variety of security features that can be employed to increase security. Availability of these features depends based on model. It is the customer's responsibility to understand and implement appropriate controls for devices behavior.

Some examples are as follows:

- Xerox Image Overwrite electronically shreds information stored on the hard drive of devices as part of the routine job process.

- Data Encryption uses state of the art encryption technology on data stored within the device as well as for data in motion in and out of the device.

For more information about the above examples as well as for other device security related technologies please see http://www.xerox.com/information-security/product-security.

The Xerox App Gallery supports the Xerox® ConnectKey® family of devices, the Xerox® AltaLink® family of devices and the Xerox® VersaLink® family of devices. It is the customer's responsibility to understand the security features of these Xerox devices, which are used in the Xerox App Gallery system.

App Wrapper

As part of the process of uploading a new Developer App, the system wraps the App. At runtime, the Wrapper performs an initial entitlement check with the App Gallery to determine if the App is entitled to run on the Device. If not entitled, the App will be prohibited from running. All Developer Apps are wrapped prior to Publication in the gallery.

Apps that were installed prior to XAG 5.0 are not wrapped and therefore do not interact with the App Gallery. However, the App Developer may publish a new Version of such an app that includes e-commerce features; in which case the system will wrap the new App version.

Based on an Update Policy established by the Account owner, the App Wrapper will automatically update the App with the current version, configuration, and certificate bundle pulled down from the App gallery.

Xerox Sanctions Service

The Xerox App Gallery invokes the Xerox Sanctions Service whenever a Xerox App Account is created or edited. The Xerox Sanctions Service provides a means for a gallery user to search for their company in the Moodys Analytics / Bureau Van Dijk Orbis database.

Once the Xerox App Account user has selected a company, the app gallery initiates a scan operation of the selected company. This has the effect of placing the company in a portfolio to be monitored by Moodys Analytics / Bureau Van Dijk Compliance Catalyst: and executing a denied parties scan of the company. Compliance Catalyst implements an algorithm to automatically accept engagements with a low risk level (as defined by Xerox Export Control). All medium and high risk engagements are manually reviewed by Xerox Export Control personnel. An account that fails the review is barred from logging in to the Xerox App Gallery or being entitled to execute Apps implementing Xerox Access Lists.

The Sanctions service notifies the Xerox App Gallery whenever there is a change in the denied parties status of a monitored Account.

Moodys Analytics / Bureau Van Dijk

Moodys Analytics / Bureau Van Dijk is a provider of corporate intelligence. The BVD Orbis product maintains a database of companies worldwide gleaned from public records. The BVD Compliance Catalyst product scans companies (and individuals) to determine if they are denied parties – as defined by Xerox Export Control.

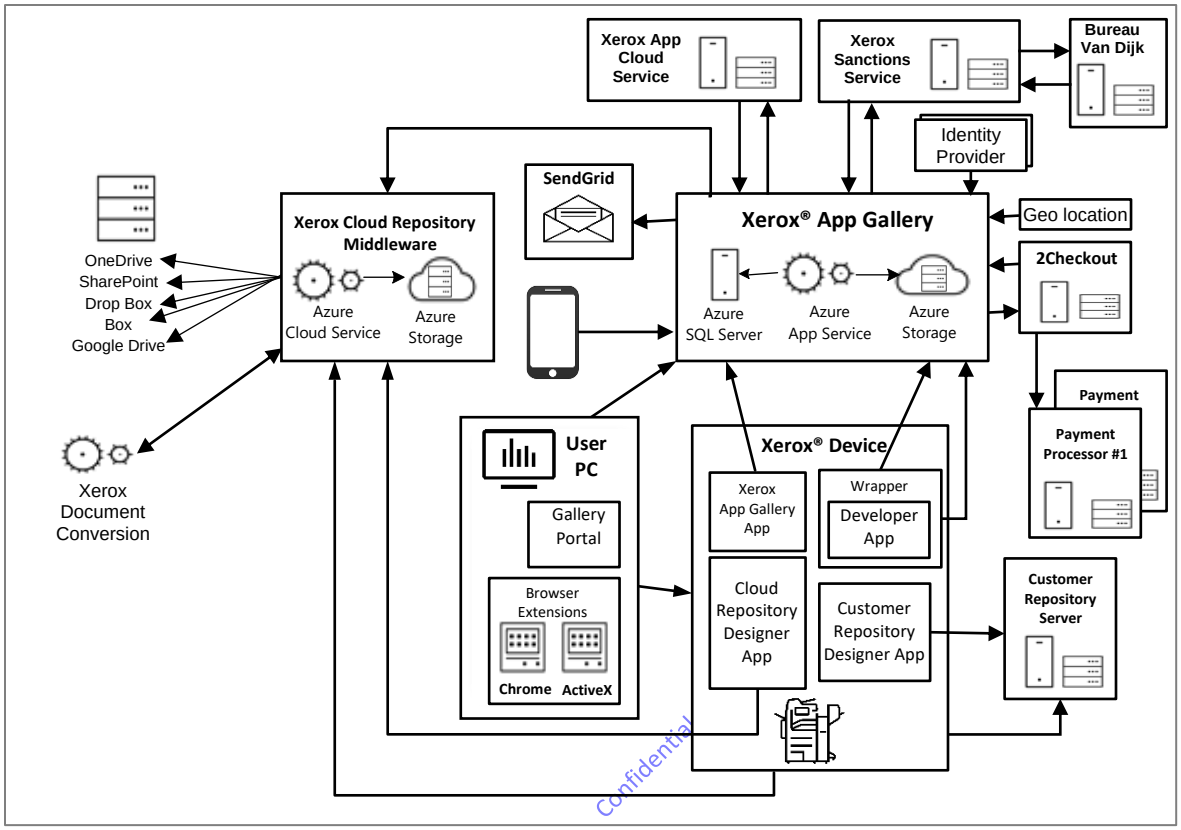
Okta Incorporated

The Xerox App Gallery invokes Okta API methods to authenticate persons whose Xerox App Accounts are configured to authenticate with the Okta Identity Provider.

Microsoft Azure AD

The Xerox App Gallery invokes Azure AD API methods to authenticate persons whose Xerox App Accounts are configured to authenticate with the Azure AD Identity Provider.

Architecture Diagram



Workflows

Web Portal Account Creation and Login Workflows

Create and Validate an Account

Step 1: Launch the App Gallery from the browser and Select the "Login" widget in the Action Bar.

Step 2: Select the "Create Account" option.

Step 3: Enter required account information and click on OK. This includes selecting a company from a list of candidates.

Step 4: The App Gallery invokes the Sanctions Service to perform a denied parties scan of the Account.

Step 5: The App gallery emails the user a Notification which requests that the user login to the system.

Step 6: The user clicks on the link in the email notification.

Step 7: The user logs into the App Gallery web portal to complete account validation.

Create and Validate a Developer Account

Step 1: User connects to the developer specific Xerox App Gallery login web page.

Step 2: User selects option to create a Xerox App Gallery developer account.

Step 3: User enters required information to create a developer account and submits the request. This includes selecting a company from a list of candidates.

Step 4: The App Gallery invokes the Sanctions Service to perform a denied parties scan of the Account.

Step 5: Xerox App Gallery creates and activates the developer account, sets its status to "validating" and sends email notification to user.

Step 6: The user clicks on the link in the email notification.

Step 7: The user logs into the App Gallery web portal to complete account validation.

Create and Validate an Associated Account

Step 1: Channel Partner selects option to create a customer account by invitation.

Step 2: Channel Partner enters the associated account's e-mail.

Step 3: Invitation e-mail is sent to the supplied e-mail address

Step 4: Associated Account receives e-mail with link to complete account creation. The user clicks on the link in the email notification.

Step 5: Associated Account user enters required account information and clicks on OK. This includes selecting a company from a list of candidates.

Step 6: The App Gallery invokes the Sanctions Service to perform a denied parties scan of the Account.

Step 7: The App gallery emails the Associated Account user a Notification which requests that the user login to the system.

Step 8: The Associated Account user clicks on the link in the email notification.

Step 9: The Associated Account user logs into the App Gallery web portal to complete account validation.

Login

Step 1: Launch the App Gallery from the browser and select the "Login" widget in the Action Bar.

Step 2: Enter email of your Xerox App Account.

Step 3: Click on the Next button.

Step 4: Enter your password and MFA code, if required by the IDP.

Step 5: Click on the OK button.

Web Portal Designer App Creation Workflows

Create ConnectKey Info App

Step 1: Channel Partner logs in to Xerox App Gallery.

Step 2: Channel Partner selects the option to create a new application.

Step 3: Channel Partner selects Xerox® ConnectKey® Info App as the type of app to create.

Step 4: Channel Partner enters the information required, selects the layout of app, and customizes the app to meet user's needs.

Step 5: Channel Partner selects Done and app is added to list of apps available from their account.

Create ConnectKey Scan Apps

Step 1: Channel Partner logs in to Xerox App Gallery.

Step 2: Channel Partner selects the option to create a new application.

Step 3: Channel Partner selects to create a Xerox® ConnectKey® Scan App type (i.e. e-mail, multi-destination, Office 365 SharePoint online, etc.).

Step 4: Channel Partner selects if a destination can be entered or if a default value is displayed.

Step 5: Channel Partner sets which scan options will be displayed

Step 6: Channel Partner enters the information required, selects the layout of app, and customizes the app to meet user's needs.

Step 6: Channel Partner selects Done and app is added to list of apps available from their account.

Create ConnectKey Print Apps

Step 1: Channel Partner logs in to Xerox App Gallery.

Step 2: Channel Partner selects the option to create a new application.

Step 3: Channel Partner selects to create a Xerox® ConnectKey® Print App type. (i.e. from URL, Office 365 SharePoint online. Dropbox, etc.)

Step 5: Channel Partner sets which print options will be displayed

Step 6: Channel Partner enters the information required, selects the layout of app, and customizes the app to meet user's needs.

Step 6: Channel Partner selects Done and app is added to list of apps available from their account.

Web Portal Browse the App Gallery Workflows

Browse gallery Apps (not logged in)

Step 1: Launch the App Gallery App at the Browser

Step 2: Browse "All Apps" in the app gallery. The user will see all publicly published apps.

Step 3: Select an App to view its "App Details" including: License Agreement, Privacy Statement and Software Disclosure.

Step 4: User will see the detailed information for the app including description, restrictions, screenshots and legal disclosures

Browse gallery Apps (with login)

Step 1: User logs in to Xerox App Gallery.

Step 2: Launch the App Gallery App at the Browser

Step 3: Browse “All Apps” in the app gallery. The user will see all publicly published apps that are not restricted from view in the user’s country.

Step 4: Browse “My Apps” in the app gallery. The user will see all the apps that the user has installed, or has active licenses for, or has been shared with by a Channel Partner.

Step 3: Select an App to view its “App Details" including: License Agreement, Privacy Statement and Software Disclosure.

Step 4: User will see the detailed information for the app including description, restrictions, screenshots and legal disclosures

<u>Web Portal Device Workflows</u>

Add a Device to the Account

Step 1: User logs in to Xerox App Gallery.

Step 2: User presses the “Add Device” button

Step 3: User enters the device’s IP address and SNMP string.

Step 4: The system searches for that device on the accessible network segment; and displays the device’s model number.

Step 5: User enters device’s credentials, physical location and other information.

Step 6: The system adds the device to the Account’s “My Devices”.

Discover Devices for the Account

Step 1: User logs in to Xerox App Gallery.

Step 2: User presses the “Start Discovery” button

Step 3: The user selects one or more “Discovery Profiles” for the discovery session. (each Profile contains ranges of addresses to scan and ranges of addresses to ignore)

Step 4: The system searches for devices in the device range on the accessible network segment

Step 5: The system automatically adds the discovered devices to the user’s “My Devices”; for profiles specifying auto-add. For manual-add profiles, the system presents the user with a list of discovered devices.

Step 6: The user selects one or more of the discovered devices to add to the Account’s “My Devices”.

Step 7: The system adds the selected device(s) to the Account’s “My Devices”.

Web Portal Purchase and Installation Workflows

Install an App from the App Gallery

Step 1: Prerequisite – Log in to the App Gallery App
Prerequisite – for Ecommerce Apps, the App must have an active trial, or an Active license for the App.

Step 2: Select an App to Install from the web portal.

Step 3: Click on the “Install” button.

Step 4: Accept the End User License Agreement (EULA) for the App

Step 5: The system installs the selected App on the MFD.

Step 6: If the app is a cloud repository app, the app and devices are registered with the cloud middleware

Activate a Trial

Step 1: User logs into Xerox App Gallery.

Step 2: User clicks on the “Try It” button in the Gallery’s My App/ App Details View.

Step 3: Accept the End User License Agreement (EULA) for the App

Step 4: User selects the Devices where the App is to be installed for the Trial.

Step 5: The system installs the selected App on the MFD.

Activate a Subscription Capture Trial

Step 1: User logs into Xerox App Gallery.

Step 2: User clicks on the “Try It” button in the Gallery’s My App/ App Details View for an app defined to capture payment information.

Step 3: Accept the End User License Agreement (EULA) for the App

Step 4: User selects the desired Price Options for a subscription the trial will renew into.

Step 5: User selects the Devices where the App is to be installed for the Trial.

Step 6: App Gallery initiates a transaction with the 2Checkout system for a trial subscription.

Step 7: User Confirms trial subscription by clicking the “Place Order” button in the 2Checkout shopping cart. For first-time purchases, 2Checkout will request personal information including: email address, physical address, Credit Card Information

Step 8: 2Checkout processes the order

Step 9: 2Checkout presents a “Thank You” page to the user detailing the transaction.

Step 10: User presses the Done button on the “Thank You” page

Step 11: Xerox App Gallery installs the app to the selected devices; and Activates a trial license for the app in the user's Account.

Purchase a "Per Device" App

Step 1: User logs into Xerox App Gallery.

Step 2: User clicks on the Buy/Subscribe button in the Gallery's My App/ App Details View.

Step 3: User selects the desired Price Option. (This step is omitted for Apps with only a single Price Option).

Step 4: User selects the Devices for which the App is being purchased. The user may also specify an "additional quantity" for future installation.

Step 5: App Gallery initiates a purchase transaction with the 2Checkout system.

Step 6: User Confirms purchase by clicking the "Place Order" button in the 2Checkout shopping cart. For first-time purchases, 2Checkout will request personal information including: email address, physical address, Credit Card Information

Step 7: 2Checkout processes the order by debiting the User's credit card account. This involves transactions with various payment processors located throughout the world

Step 8: 2Checkout presents a "Thank You" page to the user detailing the purchase just made.

Step 9: User presses the Done button on the "Thank You" page

Step 10: Xerox App Gallery installs the app to the selected devices; and Activates a license for the purchased app in the user's Account.

Purchase an "Unlimited Devices" App

Step 1: User logs into Xerox App Gallery.

Step 2: User clicks on the Buy/Subscribe button in the Gallery's My App/ App Details View.

Step 3: User selects the desired Price Option. (This step is omitted for Apps with only a single Price Option).

Step 4: App Gallery initiates a purchase transaction with the 2Checkout system.

Step 5: User Confirms purchase by clicking the “Place Order” button in the 2Checkout shopping cart. For first-time purchases, 2Checkout will request personal information including: email address, physical address, Credit Card Information

Step 6: 2Checkout processes the order by debiting the User’s credit card account. This involves transactions with various payment processors located throughout the world

Step 7: 2Checkout presents a “Thank You” page to the user detailing the purchase just made.

Step 8: User presses the Done button on the “Thank You” page

Step 9: App Gallery presents a list of Devices for the user to select for installation. The user may elect to install the App now or postpone installation until a future date.

Step 10: Xerox App Gallery installs the app to the selected devices; and Activates a license for the purchased app in the user’s Account.

Web Portal App Management Workflows

Configure App

Step 1: User logs into Xerox App Gallery.

Step 2: Authorized user selects the App's "configure" option.

Step 3: Authorized user supplies "Values" for each of the configuration elements defined by the App Developer.

Step 4: Authorized user saves the Configuration Data to the App Gallery.

Step 5: Authorized user elects to Install / Download the App.

Step 6: App Gallery creates a weblet that includes the current Configuration Data.

Step 7: App Gallery Installs / Downloads the weblet.

Step 8: User launches the App at the Device.

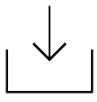
Step 9: App extracts the Configuration Data from the weblet and honors it during App execution

Download App

Step 1: User logs into Xerox App Gallery.

Step 2: Authorized user selects the App's "download" option.

Step 3: App Gallery creates a weblet that includes the current Configuration Data.



Step 4: App Gallery downloads the weblet to the user's browser.

Step 5: Gallery user installs the App weblet on devices using media.

App Entitlement Workflows

App Entitlement Check at the MFD

Step 1: User launches the app at the MFD.

Step 2: App Wrapper checks with App Gallery for entitlement to execute the app.

Step 3: If App Gallery entitlement check passes, the App is allowed to execute on the Device.

Step 4: If the App Gallery entitlement check fails, the user is informed that the app is no longer entitled to execute because 1)Trial has Expired, 2) Subscription has expired, or 3) Development period has expired.

App Usage Reporting and Entitlement Check at the MFD

Step 1: User launches the app at the MFD.

Step 2: App Wrapper checks with App Gallery for entitlement to execute, as described in the “App Entitlement Check at the MFD” section above.

Step 3: User performs an App function (i.e. Scan, Print, etc.).

Step 4: Apps defined with a Usage Based licensing model, report the usage consumed by the App function to the App Gallery.

Step 5: App rechecks with App Gallery for continued entitlement to execute. App behaves as designed by the App Developer when there is no longer entitlement.

Request that my Account be Deleted

Step 1: User logs into Xerox App Gallery and navigates to “My Account Details”.

Step 2: Authorized user selects “Delete Account” button.

Step 3: App Gallery informs the user that account history will be lost, apps will no longer be entitled to execute; and app licenses will be disabled.

Step 4: User confirms understanding.

Step 5: User clicks on the “Request Delete” button, and the gallery informs the user that the request is being processed.

Step 6: The gallery notifies the System Administrator that the user wishes the account to be deleted.

Step 7: The System Administrator navigates to the Account and presses the “Delete” account button.

Step 8: The System Administrator confirms the delete operation.

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

User data related to the categories below are stored in cloud persistent storage.

- Account data, including credentials, and ‘subject parameter’ – if authenticated by an IDP.
- Security Audit Log data, including UserId and platform IP address.
- Device-related data, including credentials
- App data (to create installation weblets)
- App configuration information

The Xerox App Gallery maintains configuration data for configurable apps at the Account level. The Names for each Configuration Element are supplied by the App Developer; and the Values are supplied by the gallery user. Personal Data may be stored in Configuration Data

- App license information, including reported App Usage
- App installation records

A gallery user may request that the System Administrator delete a gallery Account.

PERSONAL DATA MAINTAINED BY THE E-COMMERCE PROVIDER

The Xerox App Gallery acts as a passthrough for e-commerce Personal Data for the duration of the e-commerce purchase session. The Xerox App Gallery does not persistently store this Personal Data.

- Email address (which is identical to the Xerox App Account email address)
- Full Name
- City, State, Zip/Postal Code, Country
- Credit Card Details for one or more cards, each of which includes:
  - Card Number
  - Card expiration Month and Year
  - CVV2 / CVC2 Code
  - Cardholder Name

PERSONAL DATA MAINTAINED BY THE CORPORATE INTELLIGENCE PROVIDER

The Moodys Analytics / Bureau Van Dijk Compliance Catalyst product stores personal information in a “contacts portfolio” database to enable CC to monitor individuals against changes in Denied Parties lists. The sanctions service removes the entity being monitored from the Contacts Portfolio when the corresponding Xerox App Account is deleted.

- Full Name
- Address

LOCAL ENVIRONMENT

Application data transmitted

The following app data is transmitted to/from the platform on which the web browser is executing.

- Account data, including credentials
- Session data, including IP address
- Ecommerce Personal Data
- Device Data, including credentials
- App information
- App configuration information

Application data stored on the host file system

The web portal does not store any data permanently to the device on which the web browser is executing unless the authorized user elects to Download an app weblet to the host file system.

HTTP Cookies

The Xerox App Gallery web portal does not store any persistent cookies on the device on which the web browser is executing. The gallery stores an Access Token (with a lifetime of 2 hours) in local storage; and a Refresh Token in session storage with a lifetime of 100 days.

Software partners the Xerox App Gallery integrates with may create their own cookies to facilitate user interaction. If so, these software partners provide their own cookie notices and / or cookie management. For example, see the e-commerce provider’s Cookie Policy at: https://www.2checkout.com/legal/cookie-policy/ .

6. 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

Table 4. 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/