February 2017
Version: 1.0

Xerox® App Studio 4.0
Information Assurance Disclosure

Contents

Introduction

Xerox® App Studio is a Xerox workflow solution that allows the creation of Xerox® ConnectKey® device Apps and the placement of the Apps on the devices themselves. There are several App types: Information Apps, Scan To E-Mail Apps, Scan To FTP Apps, Scan To SMB Apps, Scan To USB Apps, Scan To Multiple Destinations Apps, Scan To Office 365 SharePoint Online Apps, Scan To Dropbox, Print From URL Apps, Print From Office 365 SharePoint Online Apps, and Print From Dropbox.

Purpose

The purpose of this document is to disclose information for the Xerox® App Studio with respect to system security. System Security, for this paper, is defined as follows:

1. How scan and print jobs are created and submitted
2. How user information is stored and transmitted
3. How the product behaves in a networked environment
4. How the product may be accessed, both locally and remotely

NOTE: The customer must be responsible for the security of their network and the Xerox® App Studio product does not establish security for any network environment.

The purpose of this document is to inform Xerox customers of the design, functions, and features of Xerox® App Studio relative to Information Assurance (IA).

This document does not provide tutorial level information about security, connectivity, PDLs, or Xerox® App Studio features and functions. This information is readily available elsewhere. We assume that the reader has a prior knowledge of these types of topics.

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever as a result of user's use or disregard of the information provided in this document which includes direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages.

System Workflows

Reseller Account Creation and Activation Workflow

Step 1: Account user logs into Xerox® App Studio.

Step 2: Account user selects option to create a Reseller account by invitation.

Step 3: Account user enters reseller e-mail, first name, last name and company name.

Step 4: Invitation e-mail is sent and reseller account is created.

Step 5: Reseller receives e-mail with link to activate the Reseller account.

Step 6: Reseller clicks on activation link in the e-mail which activates the Reseller account.

Developer Account Creation and Activation Workflow

Step 1: User connects to the developer Xerox® App Studio login web page.

Step 2: User selects option to create a Xerox® App Studio account.

Step 3: User enters required information to create an account and submits the request.

Step 4: User receives e-mail with link to activate the Xerox® App Studio account

Step 5: User clicks on activation link in the e-mail which gives user access to the Xerox® App Studio

Reseller Managed Customer Account Creation and Activation Workflow

Step 1: Reseller connects to the reseller Xerox® App Studio login web page.

Step 2: Reseller navigates to Accounts tab.

Step 3: Reseller selects create account and enters required information to create a customer account.

Step 4: Account is created and is instantly activated.

Step 5: Customer account is now ready to be managed by reseller.

Customer Account Creation and Activation by Invitation Workflow

Step 1: Reseller connects to the Xerox® App Studio login web page.

Step 2: Reseller selects option to create a customer account by invitation.

Step 3: Reseller enters customer e-mail, first name, last name and company name.

Step 4: Invitation e-mail is sent and customer account is created.

Step 5: Customer receives e-mail with link to activate the customer account

Step 6: Customer clicks on activation link in the e-mail which activates the customer account.

Create ConnectKey® Info App Workflow

Step 1: User logs in to Xerox® App Studio.

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

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

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

Step 5: User selects Done and app is added to list of apps available.

Create ConnectKey® Scan Apps Workflow

Step 1: User logs into Xerox® App Studio.

Step 2: User selects the option to create a new application

Step 3: User selects to create a Xerox® ConnectKey® Scan App type (i.e. e-mail, ftp, smb, usb, multi-destination, or Office 365 SharePoint online).

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

Step 5: User sets which scan options will be displayed.

Step 6: User enters the information required and sets up layout of the app and customizes the app to meet user's needs.

Step 7: User selects Done and the app is added to list of apps available.

Create ConnectKey® Print Apps Workflow

Step 1: User logs into Xerox® App Studio.

Step 2: User selects the option to create a new application

Step 3: User selects to create a Xerox® ConnectKey® Print App type, i.e. from url or from Office 365 SharePoint online.

Step 4: User can enter default credentials.

Step 5: User sets print options.

Step 6: User sets up layout of the app and customizes the app to meet the user's needs.

Step 7: User selects Done and the app is added to list of apps available.

Manual Install of App Workflow

Step 1: User logs into Xerox® App Studio.

Step 2: User selects the save icon for the app they want to manually install. This option is not available for Xerox® App Studio 2.0 apps.

Step 3: App Studio saves the app file to the local disc.

Step 4: User copies app file to a usb stick, or they can install via the Device CWIS Web Page.

Step 5: User walks to Xerox® ConnectKey® device and manually installs app from the usb stick.

Automatic Install of App Workflow

Step 1: User logs into Xerox® App Studio.

Step 2: User selects the install icon for the app they want to automatically install.

Step 3: User selects the device they wish to install the app to and selects install.

Step 4: Xerox® App Studio installs the app to the chosen device.

Step 5: If the app is a cloud repository app, the app and device are registered with the cloud middleware.

License Workflow

Step 1: Reseller logs into Xerox® App Studio.

Step 2: Reseller selects the Licenses tab.

Step 3: Reseller selects the Purchase button.

Step 4: Reseller is instructed where to purchase licenses or they can click the link to go to the eCommerce site to purchase licenses. Once purchased the user will receive an activation key via e-mail. Note: This step is purposely outside of App Studio control. It is not the responsibility of App Studio to provide security for this step.

Step 5: Reseller selects the Add button.

Step 6: Reseller enters activation key to activate the licenses purchased for App Studio.

Step 7: Reseller can see the licenses purchased, the total and remainder of the license's count.

Step 8: Reseller selects the Customer Account to get a list of licenses allocated to that customer.

Step 9: Reseller selects Edit for a particular license.

Step 10: Reseller adjusts totals for the license.

Security Description

The security considerations are three-fold:

1. The security of the apps created by the Xerox® App Studio
2. The security of the user account information required by the Xerox® App Studio system
3. The security of the devices registered within the system by the user

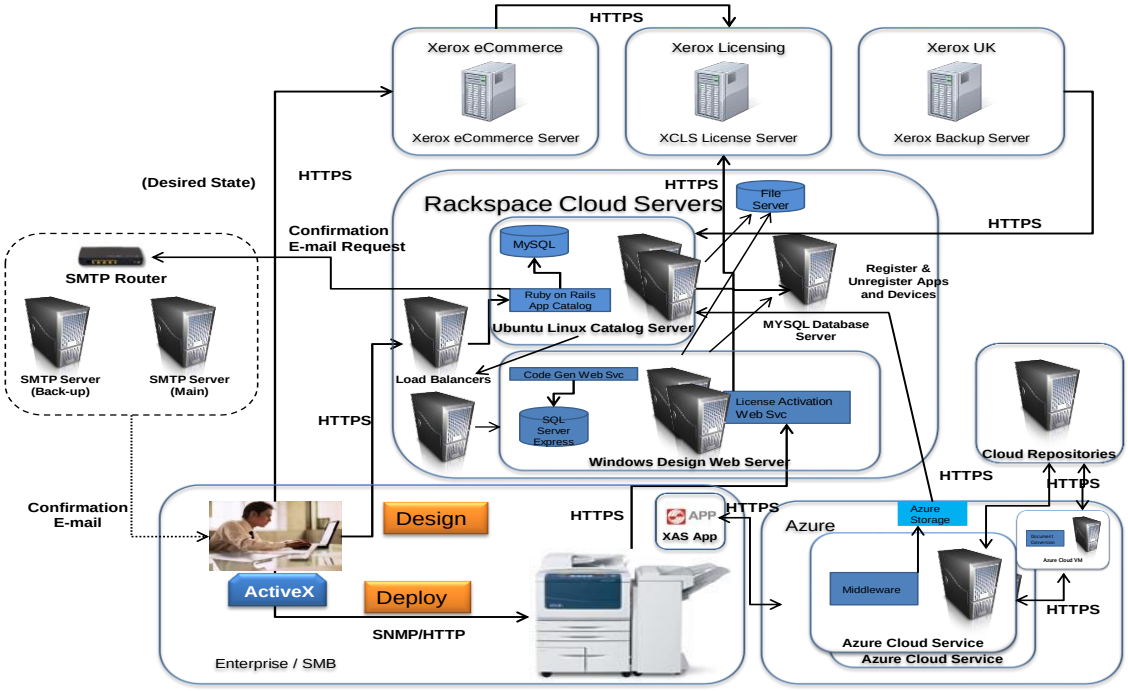
As one can see from the below diagram, information travels through multiple system components over a combination of wired and wireless networks. All use normal, industry-standard technologies and built-in security capabilities. These capabilities do need to be enabled, and the choice of which are used at each point in the system varies. This section captures the security considerations of Xerox® App Studio in the areas shown below:

1. Protocols and Port numbers used by the system
2. Individual system components
    a. Xerox® App Studio – Rackspace Catalog server (2)
    b. Xerox® App Studio – Rackspace Designer server (2)
    c. Xerox eCommerce server
    d. Xerox Corporate Licensing System
    e. Xerox® App Studio – User Web Pages
    f. Devices
    g. Rackspace Load Balancer servers
    h. Xerox Backup server
    i. Middleware Azure Cloud Service
    j. Middleware Azure Cloud Storage
    k. Cloud Resident Repositories
    l. Repository servers used by Print From URL app
    m. MYSQL Database server
    n. Cloud File storage
    o. Document Conversion Engine

3. Communication between system components
    a. Communication between Xerox® App Studio – User Web Pages and Rackspace Catalog server, Rackspace Designer server and Rackspace Load Balancer servers
    b. Communication between Rackspace Design server and Xerox Corporate Licensing System
    c. Communication between Rackspace Catalog server, Rackspace Design Server and Devices
    d. Communication between the Xerox Backup Server and the Rackspace Catalog server
    e. Communication between Xerox® App Studio and Middleware Azure Cloud Storage
    f. Communication between Xerox® App Studio Cloud Repository apps and Cloud Resident Repositories thru the Middleware Azure Cloud Service
    g. Communication between Middleware Azure Cloud Service and the Middleware Azure Cloud Storage
    h. Communication between Print From URL app on a device and a repository server
    i. Communication between Rackspace Catalog servers, Rackspace Design servers and the Rackspace MYSQL Database server
    j. Communication between Rackspace Catalog servers, Rackspace Design servers and the Rackspace Cloud Files storage
    k. Communication between Middleware Azure Cloud Service and the Azure VM Document Conversion Engine

Xerox® App Studio Network Protocols and Port Numbers Diagram

This diagram shows the protocols used in the system. Port numbers are not configurable. For non-secure connection, port number 80 is used. For secure connection, port number 443 is used. For the SMTP server port 25 is used.



Individual System Components

Xerox® App Studio – Rackspace Catalog Servers, Design Servers, Load Balancers

The Xerox® App Studio Servers, which are located in the United Kingdom, run in the Rackspace Platform. There are 2 considerations for security based on this architecture as follows:

1. Rackspace specific security information
2. Xerox® App Studio Servers specific security information

Each consideration is covered below.

Rackspace Platform Specific

Rackspace is an open source cloud company which offers various degrees of security options. Xerox® App Studio have opted to use the security option that comes with the Managed Service level for cloud servers.

Rackspace managed service security highlights:

- System installation to a hardened patched OS
- System patches are configured by Rackspace to provide continued protection from exploits in the extent that this is offered and accomplished by Microsoft Server and Ubuntu Linux
- Dedicated firewall and VPN services to help block unauthorized system access
- Data protection with Rackspace managed backup solutions
- Dedicated intrusion detection devices to provide an additional layer of protection against unauthorized system access
- Distributed Denial of Service (DDoS) mitigation services based on proprietary Rackspace PrevenTier system
- Risk assessment and security consultation by Rackspace professional services teams
- ISO17799-based policies and procedures regularly reviewed as part of SAS70 Type II audit process
- All passwords encrypted in transit and while in storage at Rackspace

Please visit the Rackspace web site for more information:
http://www.rackspace.com/managed_hosting/services/security/

Xerox® App Studio Cloud Service Specific

All communications to and from the Xerox® App Studio Cloud Service are over https, with the exception of communication between the devices and the Rackspace Design server license activation service. Data is transmitted securely and is protected by TLS security for both upload and download.

Xerox eCommerce Server

The Xerox eCommerce Server is purposely left outside of the Xerox® App Studio workflows. When the button to purchase licenses is pushed a message is displayed to the user to go to the eCommerce web site to purchase licenses for App Studio. Xerox® App Studio is not responsible for the security of communication with the eCommerce server.

Xerox Corporate Licensing system

The Xerox Corporate Licensing System is accessed with https (Hyper Text Transfer Protocol) from the license activation service in the Rackspace – Design server.

Xerox® App Studio User Web Pages

All user web pages are accessed with https from a Web Browser.

Xerox® App Studio users have to authenticate with the Xerox® App Studio Service to access the user web pages. Once authenticated the user can view:

1. All apps created by the user through the App Studio system.
2. All devices registered by the user in the App Studio system.

Devices

Xerox 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:

1. Xerox Image Overwrite electronically shreds information stored on the hard drive of devices as part of the routine job process.
2. 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 Studio only supports Xerox® ConnectKey® devices. It is the customer's responsibility to understand the security features of these Xerox devices which are used in the Xerox® App Studio system.

Communication between the device and the License Activation Web Service uses http for Xerox® App Studio 2.0 and previous versions. Starting with Xerox® App Studio 2.0.3 this communication has been changed to use https.

Xerox Backup Server

The Xerox Backup Server uses https to access the Rackspace – Catalog server. Xerox® App Studio backup files are copied from the Catalog server to the backup server which is located in a Xerox facility.

Middleware Azure Cloud Service

The Middleware Server uses https to communicate with Xerox® App Studio scan and print apps which are associated with cloud repositories (i.e. Office 365 SharePoint Online, Dropbox, and Google Drive). The Middleware server also uses https for communication with the cloud repositories. Data is transmitted securely and is protected by TLS security for both upload and download. For extra security, when a cloud repository app is installed on a device, Xerox® App Studio stores the device serial number and the app id pair with the Middleware Azure Cloud Storage. The app can then get a session token from the Middleware based on a valid device serial number and app id pair to be used for subsequent calls to the Middleware

at run-time. All cloud repository apps encrypt any user credentials sent to the Middleware Cloud service as a URL query parameter. Middleware decrypts before they are sent to the cloud repository.

The Windows Azure Platform operates in the Microsoft® Global Foundation Services (GFS) infrastructure, portions of which are ISO27001-certified.

Windows Azure Security Highlights:

- Built-in Identity Management for administrator access
- Dedicated hardware firewall
- Stateful packet inspection technology employed
- Application-layer firewalls
- Hypervisor firewalls
- Host-based firewalls
- TLS termination/ load balanced / application layer content switched
- Each deployed hosted service is segmented in own VLAN, to prevent compromised node access

Middleware Azure Cloud Storage

Both the Azure Middleware Cloud Service and the Xerox® App Studio communicate with the Azure Cloud Storage and the use of https. A valid storage account name and storage account key pair is required for authentication. Xerox® App Studio stores a device serial number and app id pair in the Middleware Azure Cloud Storage. System diagnostic logs and activity logs are stored in the Azure Cloud Storage as well.

Cloud Resident Repositories

Xerox® App Studio currently supports two cloud resident repositories. Office 365 SharePoint Online is supported and DropBox is supported.

Office 365 SharePoint Online – this cloud repository requires users to have an account with them. The Xerox® App Studio 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 Studio app can browse the repository main site or team site, the libraries contained within and the folders in the libraries. There is a Xerox® App Studio app to scan to Office 365 and print from Office 365.

DropBox - this cloud repository requires users to have an account with them. The Xerox® App Studio app 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. With valid credentials, the Xerox® App Studio app can browse the repository's folders. There is a Xerox® App Studio app to scan to DropBox and 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 Studio app can browse the repository's folders. There is a Xerox® App Studio app to scan to Box and 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 Studio app can browse the repository's folders. There is a Xerox® App Studio app to scan to Google Drive and 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 Studio app can browse the repository's folders. For business accounts, the user must provide its user id and password, which the app uses to authenticate the user. There is a Xerox® App Studio app to scan to OneDrive and print from OneDrive.

Repository Servers Used By Print From URL

Xerox® App Studio requires users to provide proper/valid credentials if the repository server requires it. Some repository servers do not require credentials to access it, therefore the user will be granted immediate access.

MySQL Database Server

MySQL database server stores the data used by the designer server and catalog server. MySQL database server uses https to communicate with the Rackspace Catalog server and the Rackspace Designer server.

Cloud File Storage

Cloud file storage stores files used by the designer server and catalog server. The Rackspace Catalog server and the Rackspace Designer server use https to access the Cloud file storage.

Document Conversion Engine

The Document Conversion Engine is used by the middleware to convert non-print ready documents to print ready format for print jobs generated from the Xerox® App Studio print

apps for the third party cloud repositories. The middleware communicates with the Document Conversion Engine which sits on an Azure VM server via https.

Communication between System Components

Communication between Xerox® App Studio, Rackspace Catalog Servers, Design Servers and Load Balancers and Xerox® App Studio Web Pages

The Xerox® App Studio servers use the https protocol for all communication with the Xerox® App Studio Web Pages. It establishes an https secure connection with the Xerox® App Studio 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 Xerox® App Studio 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.

Xerox® App Studio requires users to authenticate before they can use any of its features. Basic authentication is performed with the Xerox® App Studio that provides username and password information over the https protocol.

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

Communication between Xerox® App Studio, Rackspace Design Server, and Xerox Corporate Licensing System

The Xerox® App Studio – Rackspace License Activation Service uses the https protocol for all communication with the Xerox Corporate Licensing System. It establishes an https secure connection when the Xerox Corporate Licensing System relies on the certificate authority configuration of the Windows server on which it resides to validate the security certificate as part of establishment of the TLS connection with the Xerox Corporate Licensing System.

Communication between Xerox® App Studio – Rackspace Catalog and Design Servers and Devices

The Xerox® App Studio uses SNMPv2 to discover printers and printer capabilities. Customers can configure the community name strings for the agent to use if they have configured their printers to use non-default values.

Xerox® App Studio also uses SOAP messages transmitted over the https protocol 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. These device administrator credentials are supplied by the user and stored as part of the device record in Xerox® App Studio.

The devices communicate directly with the Xerox® App Studio Design server when it tries to validate a license for an App that has been installed on the device. For technical reasons this communication will be done via http for the initial 1.0 release. In future releases the desired state is for this communication to be done via https.

Communication between Xerox Backup Server and Xerox® App Studio – Rackspace Catalog Server

The Xerox Backup Server is a password protected server which communicates via https with the Xerox® App Studio Rackspace Catalog server at a regularly scheduled interval to copy the backup files of Xerox® App Studio to the Xerox Backup Server. The Xerox Backup server is located at a Xerox facility in the United Kingdom.

Communication between Xerox® App Studio – Rackspace Catalog Server and Xerox® App Studio – Rackspace Catalog Slave Server

The Xerox® App Studio – Rackspace Catalog server communicates with the Xerox® App Studio – Rackspace Catalog slave server via https. Every time the Catalog server's data changes the change is mirrored to the Catalog slave server so that they are always in sync. If the Catalog server goes offline, the Catalog slave will immediately take its place so the Xerox® App Studio downtime is minimized as much as possible.

Communication between Xerox® App Studio and the Middleware Cloud Storage

The Xerox® App Studio communicates with the Middleware Cloud Storage when a cloud repository app is installed on a device. Xerox® App Studio takes the device serial number and the app id and registers and stores the pair in the Middleware Cloud Storage. This communication is done via https and the data is transmitted securely and is protected by TLS security for both upload and download. A valid storage account name and storage account key pair is required for authentication and access to the Middleware Cloud Storage.

Communication between Xerox® App Studio Cloud Repository Apps and Cloud Resident Repositories thru the Middleware Azure Cloud Service

The Middleware Cloud Service acts as a router for communication between the Xerox® App Studio Cloud Repository Apps and the Cloud Resident Repositories. At app login time the app must get an authentication/session token from the Middleware Cloud Service in order to be given permission to access the cloud repository thru the Middleware Cloud 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 browse the cloud repository and based on which app can then scan to or print from the cloud repository. This communication is done via https and the data is transmitted securely and is protected by TLS security for both upload and download. XAS supplies a link to a Certificate Authority root certificate for validation with Middleware Cloud service. It is the responsibility of the customer to install the certificate on their devices and to enable server certificate validation on the devices.

All cloud repository apps encrypt any user credentials sent to the Middleware Cloud service as a URL query parameter. Middleware decrypts before they are sent to the cloud repository.

Communication between Xerox Device and Cloud Resident Repositories thru the Middleware Azure Cloud Service

The Middleware Cloud Service acts as a router for communication between the Xerox Device and the Cloud Resident Repositories. The authentication/session token is used by the device to perform a scan to or print from the cloud repository. This communication is done via https and the data is transmitted securely and is protected by TLS security for both upload and download.

Communication between 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. Middleware Cloud Service does a look up for a device serial number and app id pair in the Middleware Azure Cloud Storage when an app requests an authentication/session token.

Communication between Print From URL app and Customer Repository Server

The Xerox® App Studio does not guarantee security when the Print From URL app communicates 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.

Communication between Middleware Azure Cloud Service and the Azure VM Document Conversion Engine

The Middleware Azure Cloud Service communicates with the Azure VM Document Conversion Engine via https.

Supported MFPs/Printers

The following is a list of MFPs that support the use of the Xerox® App Studio:
• Xerox® WorkCentre® 3655 Multifunction Printer
This device is loaded with the software for 2016 ConnectKey Technology enabled MFPs / WorkCentre®
3655i.
• Xerox® WorkCentre® 5845/5855 Multifunction Printer
This device is loaded with the software for 2016 ConnectKey Technology enabled MFPs.
• Xerox® WorkCentre® 5865/5875/5890 Multifunction Printer
This device is loaded with the software for 2016 ConnectKey Technology enabled MFPs / WorkCentre®
5865i/5875i/5890i.
• Xerox® WorkCentre® 5945/5955 Multifunction Printer
This device is loaded with the software for 2016 ConnectKey Technology enabled MFPs / WorkCentre®
5945i/5955i.
• Xerox® WorkCentre® 6655 Multifunction Printer
This device is loaded with the software for 2016 ConnectKey Technology enabled MFPs / WorkCentre®
6655i.
• Xerox® WorkCentre® 7220/7225 Multifunction Printer
This device is loaded with the software for 2016 ConnectKey Technology enabled MFPs / WorkCentre®
7220i/7225i.
• Xerox® WorkCentre® 7830/7835/7845/7855 Multifunction Printer
This device is loaded with the software for 2016 ConnectKey Technology enabled MFPs / WorkCentre®
7830i/7835i/7845i/7855i.
• Xerox® WorkCentre® 7970 Multifunction Printer

The Role of Xerox

Xerox strives to provide the most secure software product possible based on the information and technologies available while maintaining the product performance, value, functionality, and productivity.

Xerox will:

- Run industry standard security diagnostics tests in development to determine vulnerabilities. If found, the vulnerabilities will either be fixed, minimized, or documented

  Monitor, notify, and supply necessary security patches provided by third party software vendors used with the App Studio software.