October 2013
702P00860

Xerox® App Studio

Information Assurance Disclosure

Version 2.0

Contents

Introduction

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 currently two App types, Information Apps and Scan Apps.

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 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 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.

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 resulting from user's use or disregard of the information provided in this document including 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: User connects to the 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 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 3: Invitation e-mail is sent and customer account is created.

Step 4: Customer receives e-mail with link to activate the customer account

Step 5: 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 App Workflow

Step 1: User logs into Xerox App Studio.

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

Step 3: User selects Xerox® ConnectKey™ Scan App type of to create (i.e. e-mail, ftp, multi-destination, smb or usb).

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.

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.

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.

.

Licensing 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. 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:

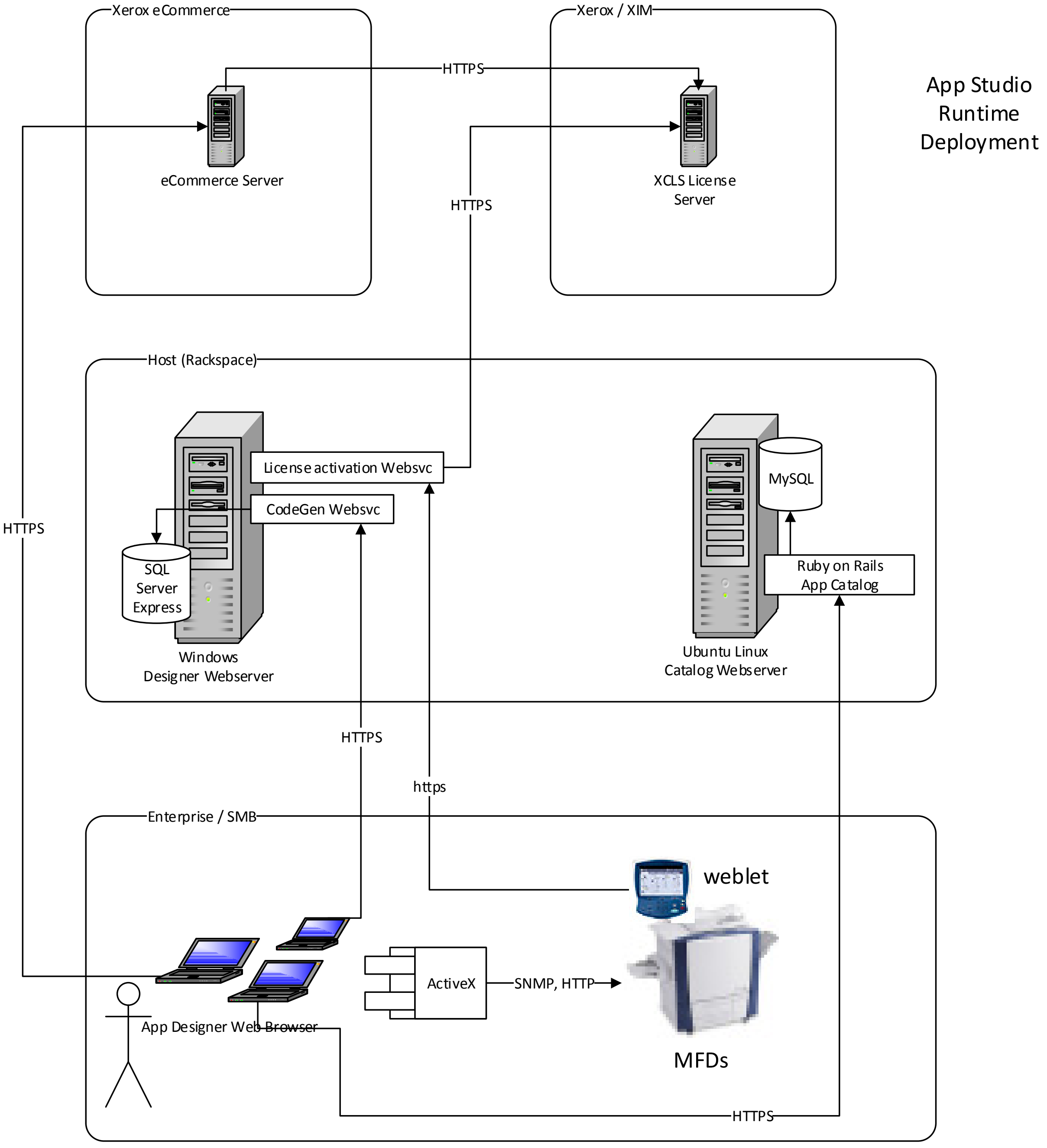
1. The security of the apps created by the Xerox App Studio
2. The security of the user account information required by the Xerox App Studio system
3. The security of the devices registered within the system by the user

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. Of course 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 following areas:

1. Protocols and Port numbers used by the system
2. Individual system components
    a. Xerox App Studio – Rackspace Catalog server
    b. Xerox App Studio – Rackspace Designer server
    c. Xerox eCommerce server
    d. Xerox XCLS license server
    e. Xerox App Studio – User Web Pages
    f. Devices
3. Communication between system components
    a. Communication between Xerox App Studio – User Web Pages and Rackspace Catalog server and Rackspace Designer server
    b. Communication between Rackspace Catalog server and Xerox XCLS license server
    c. Communication between Rackspace Catalog server and Devices

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.



Individual System Components

Xerox App Studio – Rackspace Catalog Server and Design Server

The Xerox App Studio Servers runs 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 varying degrees of security options. Xerox App Studio has opted to use the security option that comes with the Managed Service level for cloud servers.

Rackspace managed service security highlights:

- System installation using hardened patched OS
- System patching configured by Rackspace to provide ongoing protection from exploits in so far as 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 during transmission 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. Data is always transmitted securely and is protected by SSL security during 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 XCLS License Server

The XCLS License Server is accessed using HTTPS from the Rackspace – Catalog server.

Xerox App Studio – User Web Pages

All user web pages are accessed using HTTPS from a 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 will vary depending 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 routine job processing.
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 supports devices from a variety of manufacturers. It is the customer's responsibility to understand the security features of any non-Xerox devices configured for use in the system.

Communication between System Components

Communication between Xerox App Studio –Rackspace Catalog Server and Design Server and Xerox App Studio Web Pages

The Xerox App Studio servers use the HTTPS protocol for all communication with the Xerox App Stdio Web Pages. It establishes an HTTPS secure connection with the Xerox App Studio Service relying on the web page operating system to validate the security certificate as part of establishing the SSL connection. The SSL certificate is issued by Comodo (a trusted certificate authority) and ensures that the Xerox App Studio websever 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 using any of its features. Basic authentication is performed with the Xerox App Studio providing 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. 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 Catalog Server and Xerox XCLS License Server

The Xerox App Studio – Rackspace License Activation Service uses the HTTPS protocol for all communication with the Xerox XCLS License Server. It establishes an HTTPS secure connection with XCLS relying on the certificate authority configuration of the Windows server on which it resides to validate the security certificate as part of establishing the SSL connection with XCLS.

Communication between Xerox App Studio – Rackspace Catalog Server 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 Role of Xerox

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

Xerox will:

- Run industry standard security diagnostics tests during development to determine vulnerabilities. If found, the vulnerabilities will either be fixed, minimized, or documented
- Monitor, notify, and supply (when necessary) security patches provided by third party software vendors used with the App Studio software.