Software Version 5.1
January 2019
702P07461

Xerox® Workplace Cloud Information Assurance Disclosure

Contents

1. Introduction

A Workflow Solution that connects a mobile workforce to new productive ways of printing. Printing is easy and convenient from a mobile device or by sending an email with attachments to print@printbyxerox.com, without needing drivers and cables.

Purpose

The purpose of the Information Assurance Disclosure (IAD) is to disclose information for the Xerox® Workplace Cloud 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 Workplace Cloud relative to Information Assurance (IA) and the protection of customer sensitive information. Note that the customer is responsible for the security of their network and the Workplace Cloud 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 the Workplace Cloud relative to Information Assurance (IA).

This document does not provide tutorial level information about security, connectivity or Workplace Cloud 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 Workplace Cloud workflow; as such, some user actions are not described in detail.

Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

2. Product Description

Overview

The workflow of mobile printing is quite simple. A user using a mobile device such as a smart phone, tablet, or laptop sends a document to the Workplace Cloud. Depending on the submission method, the job is either printed without any further user action or the user manually releases the job to print.

Workplace Cloud is extended in version 5.1, providing a Single Sign-On (SSO) infrastructure. The Apps in the Xerox® App Gallery, which is modified to support this new infrastructure, can use Workplace Cloud as a storage vault for user login information. User login information can be user credentials or tokens. After logging into the Workplace Cloud, a user can select an SSO enabled Gallery App, which queries Workplace Cloud to obtain the login information of the user for that app. If the login information is available and valid, the app uses that information to log in the user into the Gallery App without the need to provide additional login credentials.

There are several methods for a mobile user to submit or release a job to print. The Submission method is technically decoupled from the release method. However, certain submission/release pairs make more sense than other pairs.

Submission Methods

- Email
- Workplace Mobile App (Print Portal)
- Desktop Print Client (upload)

Release Methods

- Printing device UI (using EIP)
- Workplace Mobile App (Print Portal)
- Auto Release using Authentication
- Auto Release using Network Appliance

Combined Submission/Release Methods

Note: Job will print without any explicit user action after submission.

- Email
- Workplace Mobile App (Print Portal)
- Web Portal (Web browser interface to Workplace Cloud)
- Desktop Print Client (upload and print)
- Desktop Print Client (direct print)

Printer Authentication Methods

- Card Access (Proximity Cards, Magnetic Stripe Cards, NFC on Android)
- Alternate Login (Cloud Authentication, LDAP, Azure AD, or PIN)
- Mobile Phone Unlock (using the Xerox® Workplace Mobile App for iOS or Android: NFC, QR Code, or Manual Code Entry)

The common link between all submission and release methods is the Xerox® Mobility Cloud Solution. Documents are stored in the cloud until they are deleted or until an administrative timeout has passed.

@PrintByXerox

The @PrintByXerox App, available using the Xerox® App Gallery and included as an "In-Box" App on some devices is designed to give customers an introduction to the Workplace Cloud system. Users are able to submit jobs using Email, by sending them to print@printbyxerox.com, and then release them using the @PrintByXerox App. Below is a diagram outlining the different components used as part of this workflow.

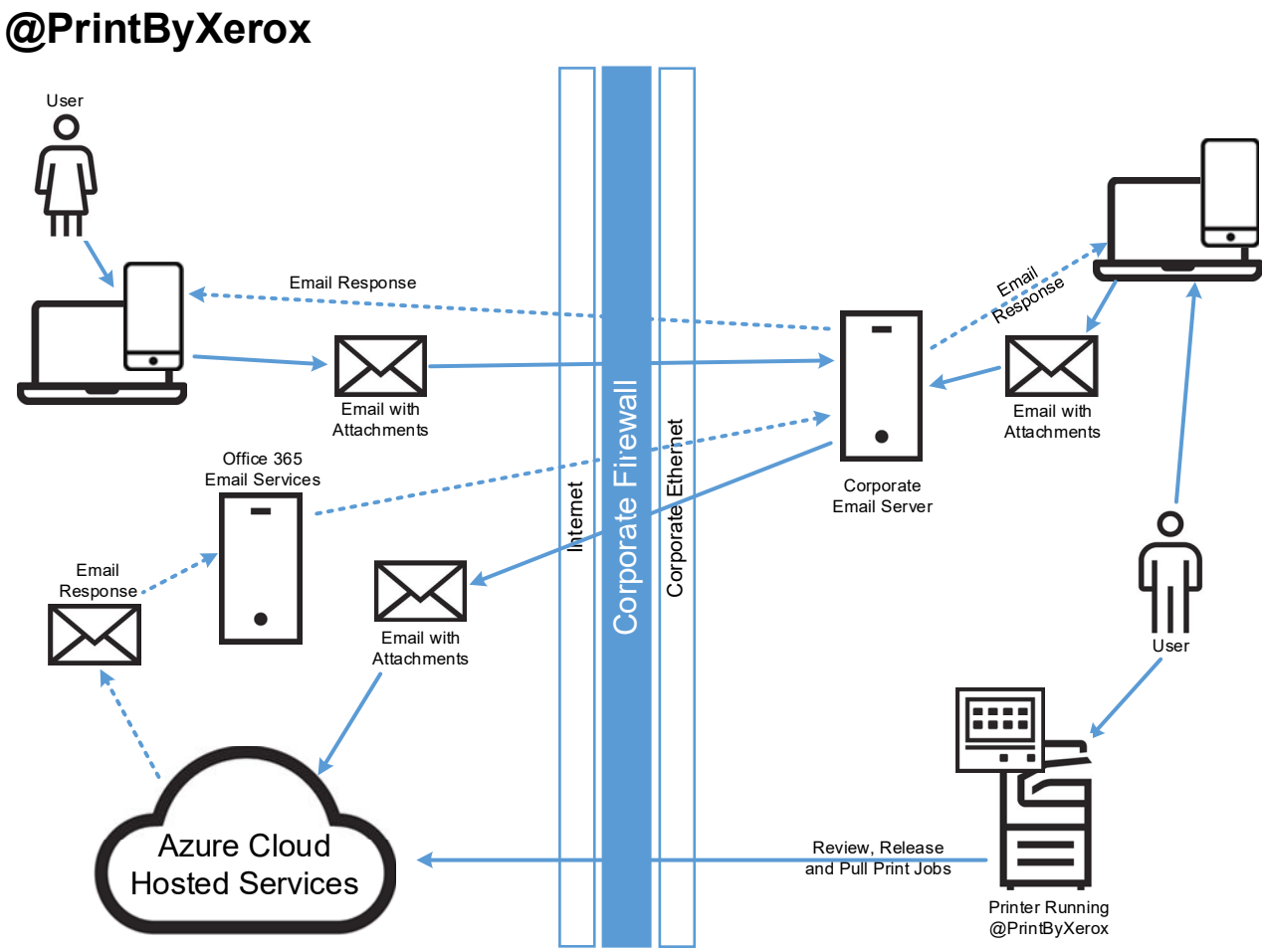

Figure 2–1: @PrintByXerox

Xerox® Workplace Cloud

The following diagram shows the system components used for the full Xerox® Workplace Cloud.

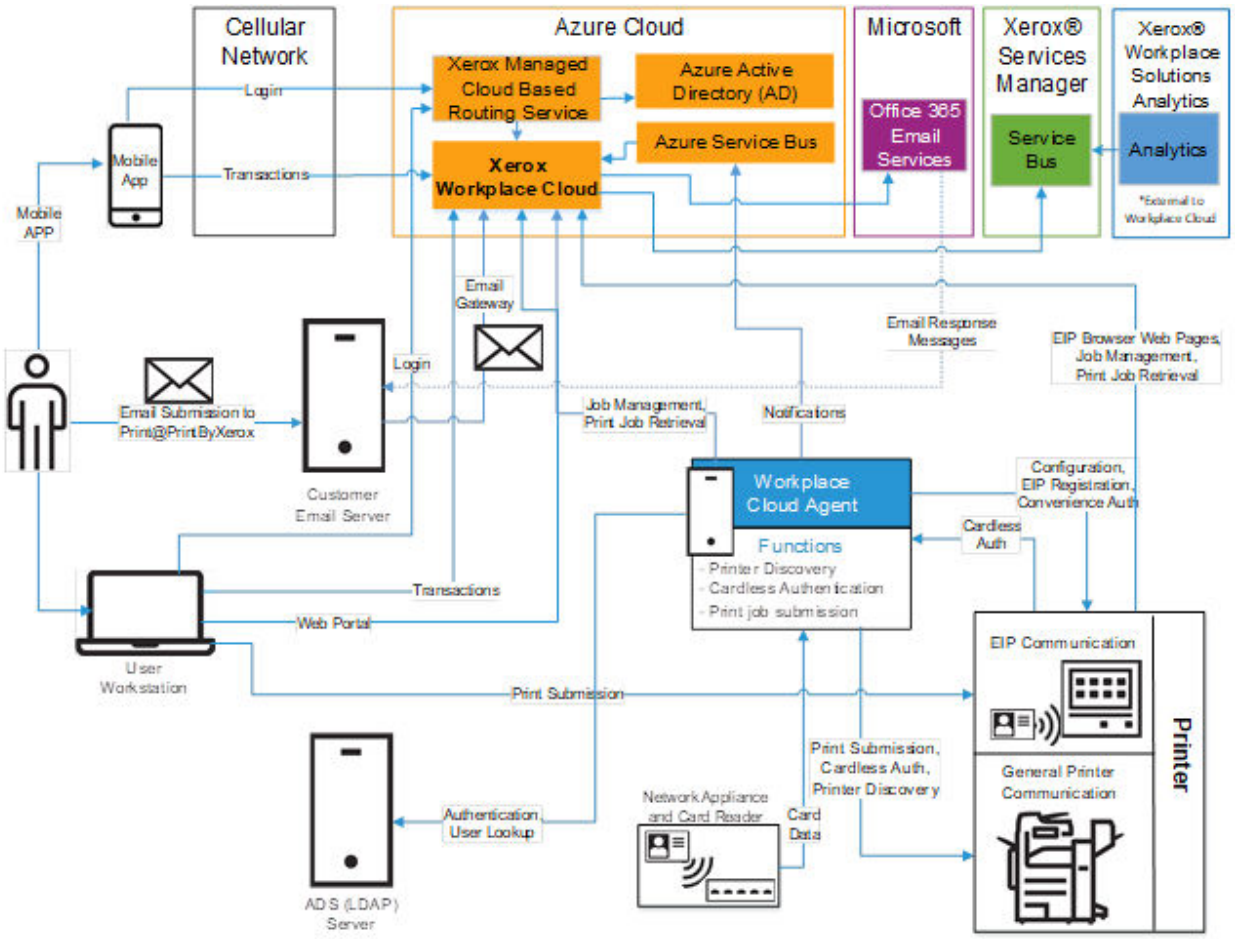

Figure 2–2: Xerox® Workplace Cloud

Single Sign-On

Xerox® and its partners offer different types of Apps in the Xerox® App Gallery, many of which require some type of user authentication. These Apps typically require unique login credentials for each one. In order to improve the user experience, Workplace Cloud offers a Single Sign-On (SSO) capability. With Single Sign-On, the users log in to the printer and able to select one of the supporting Gallery Apps without the need to provide additional credentials.

The Single Sign-On feature allows Workplace Cloud to store user access information for Xerox® App Gallery applications that are designed to support the Single Sign-On feature. The Authentication solution now becomes a SSO vault. The SSO vault acts as a storage vault, where login information for each supported and enabled Gallery App is stored.

As an analogy, you can think of the SSO vault of Workplace Cloud as a security vault with a collection of safety deposit boxes. Each user is given a safety deposit box that is unique for that user and a specific App, for example; the File and the Print Dropbox App. To access the safety deposit box, the user provides their identity by logging in to the printer, then indicates which safety deposit box they wish to access by selecting an App on the User Interface of the printer. The App then views the contents of the safety deposit box from the security vault, or they can update or delete the contents.

All content to be stored in the vault is encrypted by the App or its backend hosted system, before it is given to the SSO vault. This ensures that the SSO vault can never view or use the contents that are stored in the vault. Only the App infrastructure knows how to decrypt and use the contents of the vault.

The following diagram shows the main system components used for the Single Sign-On capability.

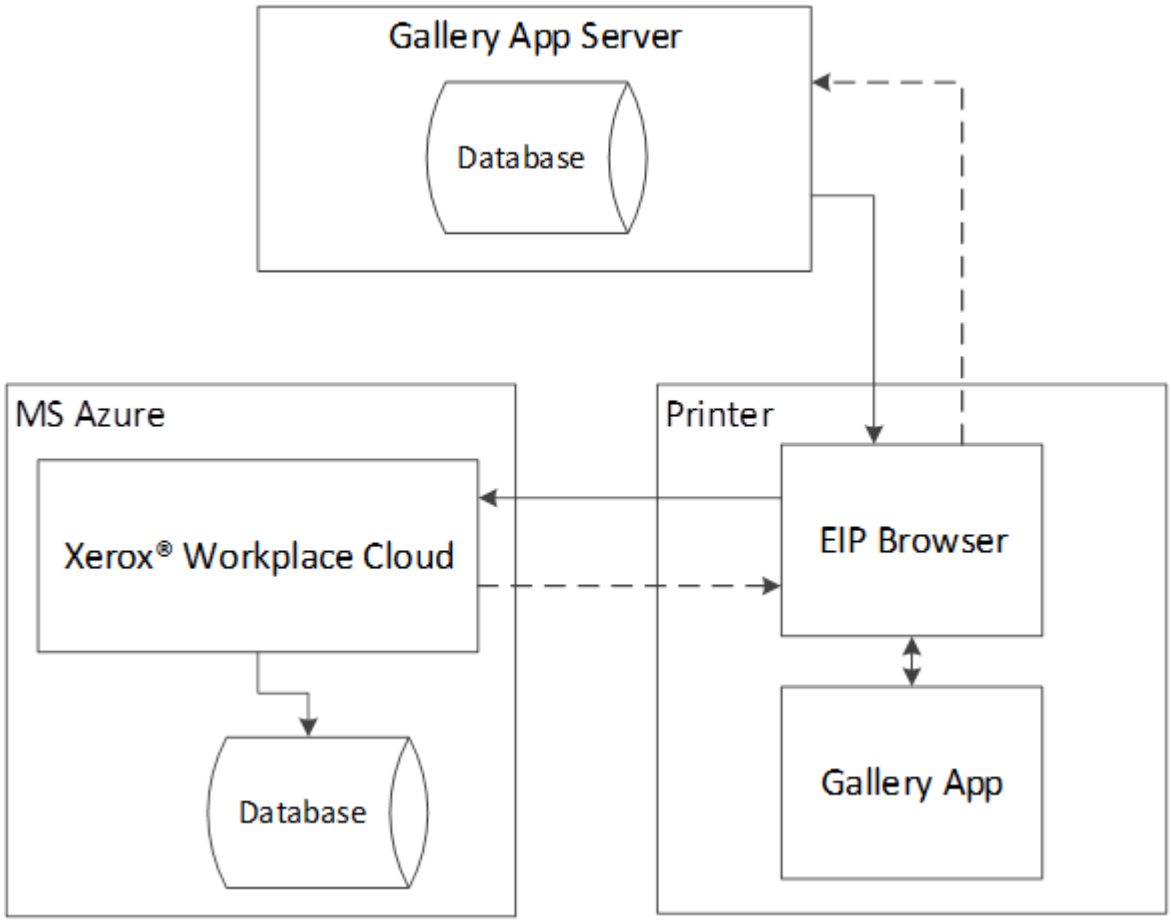

Figure 2–3: Single Sign-On Components

Description of System Components

Table 2-1: System Components

Component	Description
User	A user of the Xerox® Workplace Cloud.
Xerox® Workplace Mobile App (Print Portal)	Mobile application for iOS, Android, and Chrome that allows the user to find printers and upload / send print jobs to Workplace Cloud.
Xerox® Workplace Cloud	The Azure hosted cloud service that provides the Workplace Cloud functionality.
Customer ADS/LDAP Server	Used for user authentication.
Azure AD	[Optional] May be used for user authentication. Microsoft's Azure AD may in turn forward authentication requests to the customer's hosted AD system.
Third-Party Public Print Provider	Allows print jobs to be submitted to 3rd Party Providers.
Xerox® Workplace Cloud Agent	On-premise application that runs on customer provided hardware, which supports Printer Discovery, Print transmission, and Convenience Authentication.
Server Based Print Queues	Allows print jobs to be forwarded to other 3rd Party Solutions for added job tracking, accounting, and so on.
Printer	Any printing device (Xerox or Non-Xerox) that is enabled to support Workplace Cloud.
Customer Email Server	The Customer Email Server is used to get print jobs to the Workplace Cloud.
User Workstation	User's system on which the Desktop Print Client can be installed, which allows print jobs to be submitted to Workplace Cloud Printers from the PC.
Microsoft Office 365 Email Service	Used to send email responses back to users of Workplace Cloud.
Network Appliance	External hardware device that supports card-based document release at Non-Xerox or Non-EIP Devices.
Xerox® Services Manager	External Xerox application used in managed service accounts.

Component	Description
App from Gallery	An App found in the Xerox® App Gallery that is modified to support SSO.
App Server	A backend system that handles the browser based calls and processing needed by the App. Maintains knowledge and information about the SSO server.

3. System Architecture

Sub-Systems

Xerox® Workplace Cloud

The Xerox® Workplace Cloud consists of number of different services that run as an Azure role (Web Role or Worker Role). The type of role used depends upon the function of the service. If the service is interfacing externally using some type of API or interface, it's typically a Web Role and if the service performs internal processing, then it's typically a Worker Role. Each role runs on its own Azure VM instance, and the number of such instances will vary based on the system load. Each service is assigned a fixed size set of RAM and HDD for the given VM, which varies based on the service and its needs.

Table 3-1: Xerox® Workplace Cloud Volatile Memory

Volatile Memory					
Type (SRAM, DRAM, and so on.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
Azure storage – System Memory	Varies Based on Service	N	Executable code, temporary storage for messages processing related data, variables, state information, and so on.	Y	Power Off or Exit of the Service

Table 3-2: Xerox® Workplace Cloud Non-Volatile Memory

Non-Volatile Solid-State Memory					
Type (Flash, EEPROM, and so on.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
HDD	Varies Based on Service	N	Storage of binaries, libraries, graphic images, HTML pages, JavaScript pages, certs, configuration, logs, user documents, print drivers, installers, templates, job metadata	Y	Requires removal of Xerox roles

Xerox® Workplace Cloud Agent

Table 3-3: Xerox® Workplace Cloud Agent Volatile Memory

Volatile Memory					
Type (SRAM, DRAM, and so on.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
RAM	Customer Provided	N	Executable code, temporary storage for processing related data, variables, state information, and so on.	Y	Power Off or Exit of the Service

Table 3-4: Xerox® Workplace Cloud Agent Non-Volatile Memory

Non-Volatile Solid-State Memory					
Type (Flash, EEPROM, and so on.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
HDD	Customer Provided	N	Storage of binaries, libraries, logs, printer information	N	Removal / Un-install of the Agent. Data may be manually deleted by users with access rights to the PC on which the Agent is running. Periodic removal of some data based on time.

Desktop Print Client

Table 3-5: Desktop Print Client Volatile Memory

Volatile Memory					
Type (SRAM, DRAM, and so on.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
RAM	Customer Provided	N	Executable code, temporary storage for processing related data, variables, state information, and so on.	Y	Power Off or Exit of the Service

Table 3-6: Desktop Print Client Non-Volatile Memory

Non-Volatile Solid State Memory					
Type (Flash, EEPROM, and so on.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
HDD	Customer Provided	N	Storage of binaries, libraries, logs, printer information, print job data	Y	Removal / Un-install of the Client. Data may be manually deleted by users with access rights to the PC on which the Client is running. Periodic removal of some data based on time.

Xerox® Workplace Mobile App (Print Portal)

Table 3-7: Workplace Mobile App Volatile Memory

Volatile Memory					
Type (SRAM, DRAM, and so on.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
RAM	Customer Provided	N	Executable code, temporary storage for processing related data, variables, state information, and so on.	Y	Power Off

Table 3-8: Workplace Mobile App Non-Volatile Memory

Non-Volatile Solid-State Memory					
Type (Flash, EEPROM, and so on.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Contains Customer Data**	**Process to Clear**
ROM	Customer Provided	N	Storage of binaries, libraries, printer information, print job data	Y	Removal / Un-install of the App.

Open Source Components

Xerox® Workplace Cloud uses Open Source software modules in its different components, such as the Cloud hosted Workplace Cloud, the Desktop Client, and so on. An up-to-date bill of materials for this solution is available upon request from Xerox.

4. System Interaction

System Components

Xerox® Workplace Mobile App (Print Portal)

The Xerox® Workplace Mobile App (Print Portal) is the main user interface to the Xerox® Workplace Cloud.

The application requires users to authenticate with the Workplace Cloud before using the application. When authenticated, the user's credentials and authentication token are stored in the application until they log out. For more information about authentication and communications-related security information, refer to *Communication between the Xerox® Workplace Mobile App and Xerox® Workplace Cloud*.

The Xerox® Workplace Mobile App does not provide the capability to remotely wipe the mobile device.

It is ultimately the responsibility of the user to secure their mobile device. Users can enable device level passwords and manage physical access to the device. If the mobile device is lost or stolen, the user can access the webpage to change their password making the device unable to access the Workplace Cloud solution.

Xerox® Workplace Cloud

The Workplace Cloud runs in the Microsoft® Windows Azure Platform and utilizes the SQL Azure Database for storage. There are a number of considerations for security based on this architecture as follows:

- Windows Azure Platform specific security information
- SQL Azure Database specific security information
- Workplace Cloud specific security
- Workplace Cloud Printer Client Application specific security
- Workplace Cloud Desktop Client
- Workplace Cloud Web Portal
- Workplace Cloud Email Service

Each consideration is covered below.

Windows Azure Platform Specific

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
- SSL termination / load balancing / application layer content switching
- Each deployed hosted service is segmented in its own VLAN, preventing compromised node access

Go to the following Microsoft website for more information:

- Windows Azure Security Overview: https://docs.microsoft.com/en-us/azure/security/#
- Microsoft Azure Trust Center: https://www.microsoft.com/en-us/trustcenter/cloudservices/azure

SQL Azure Database Specific

The application data is stored in a SQL Azure database. This database contains information about the printers, print queues, jobs and so on. The SSO Vault data is also stored in the SQL Azure Database and entries are encrypted using AES.

SQL Azure is protected by two levels of security. In addition to username and password to access the database, Microsoft protects access to SQL Azure databases by allowing configuration of a whitelist of IP Addresses that can connect to the database.

Only internal Xerox IP Addresses have been configured on the whitelist for this database. Only authorized Xerox personnel have access to this data.

Passwords, Printer MAC Addresses and Printer Serial Numbers are stored in an encrypted format in the database.

Xerox® Workplace Cloud Specific

Original documents and printable documents are stored within Azure Storage. Both the original and printable documents are in an encrypted format.

Access to these documents is only available to the following:

- The owner of the documents using the Xerox® Workplace Mobile App for preview.
- The owner of the documents using the Xerox® Workplace Mobile App or the Xerox® Workplace Cloud Printer Client Application for Print Release.
- Authorized Xerox personnel who are responsible for deployment and maintenance of the system. Since the documents are encrypted even the authorized personnel cannot open the document to view its contents.

Each document printed follows a document retention policy which is applied to the document at the time of printing. The document retention policy is either immediate, 1 day or 7 days. If set to immediate, the document is deleted immediately after printing. If the document retention policy is set to 1 or 7 days, then after printing, the document is removed after the number of configured days. Therefore, documents are stored in the system for a maximum of 7 days.

Accounting information may be stored within the Azure Storage. It is stored in an encrypted format. Accounting information that can be saved is:

- Default accounting information to be used when printing Welcome Pages to printers and print queues that require accounting information. If the administrator chooses to enter this information, it will be saved within Azure.

- User accounting information that is entered by the user when they print a job to a printer is identified with having Xerox Network Accounting or Xerox® Standard Accounting, or a print queue that is set with server-based accounting. The administrator can configure the software to allow user accounting data to be saved. The default is to not save user accounting data.

All communications to and from the Workplace Cloud is over HTTPS using TLS (SSLv2 and v3 are not used). Documents are transmitted securely always and are protected by TLS security during upload and download.

Certificates used for encryption/decryption of documents are stored in the Windows Azure Certificate store as per Microsoft guidelines. This is a highly secure area protected by Microsoft. Account administrators can only upload certificates to this store. Downloads are not allowed. Only applications running within the same Windows Azure subscription can access the certificate.

Xerox® Workplace Cloud Printer Client Application Specific

When accessing the Xerox® Workplace Cloud Printer Client Application, webpages (HTML, JavaScript, icons, and so on.) are served up by the Workplace Cloud. This pathway includes the ability to provide login credentials to view and manage a user's list of jobs, including print job deletion or print initiation. This pathway also includes the ability for a Workplace Cloud Admin/System Administrator to manage some of the settings of the printer, including: Printer Enablement, Public Print Enablement, Site and Friendly Name.

All communications between the Xerox® Workplace Cloud Printer Client Application and the Workplace Cloud are over HTTPS using TLS. Certificates used for this communication path are stored in the Windows Azure Certificate store as per Microsoft guidelines.

Xerox® Workplace Cloud Virtual Machines

Xerox will monitor vendor security bulletins and products update announcements, and assess what actions are required on the Azure virtual machines. These bulletins and announcements can come from Microsoft and other external vendors, as well as internal partners supplying components used in the product system. Xerox will update the virtual machines to maintain the health and integrity of the product system.

As anti-virus definition files are released more frequently than application and operating system patches, these updates will occur on a more frequent basis. Virtual machines are configured to perform full scans weekly, and update the anti-virus definition files before the full scan.

Xerox® Workplace Cloud Web Portal

User Access

All user web pages are accessed using HTTPS over TLS from a browser.
Workplace Cloud customer account users must authenticate with the Workplace Cloud to access the Web Portal. Once authenticated the user can view:

- All printers enabled by the customer account administrator inclusive of printer name, printer location, and the printer's direct email submission email address.
- Only jobs submitted by the user inclusive of document names, date of completion, and printer name of printer used to print the job.

Administrator Access

All user customer administrator web pages are accessed using HTTPS over TLS from a browser.

Workplace Cloud customer account administrators have to authenticate with the Workplace Cloud to access the administrator user web pages. When authenticated, the administrator user can view everything that users can in addition to the following:

1. Users associated with their customer account using a listing that includes email addresses and the user's authentication / access card / badge number.
2. All jobs processed for the account inclusive of document names, date of completion, email address of user that submitted the document, and printer name of printer used to print the job. This includes documents submitted by users who are not members of the customer account, but have seen and printed to one of the account printers.
3. Licensing information that includes license activation keys and associated serial numbers. After a license is installed for a customer account, the license activation keys and associated serial numbers cannot be reused to install in other customer accounts.
4. IP addresses for all printers discovered by the customer account's Workplace Cloud Agents. For each printer, the administrator can view and manage the enablement for Workplace Cloud, as well as the enablement for Convenience Authentication and if the printer has the Workplace Cloud Printer Client Application installed.
5. The addresses of sites where printers are located.

Xerox® Workplace Cloud Agents that have been created and registered with the customer account. This includes the agents Activation Codes which are tied to the customer account and cannot be used to register an Agent in another customer account. This information is displayed for the customer account administrators only. It is the responsibility of the administrator in sharing Activation Codes with others.

Xerox® Workplace Cloud - Email Service

The Workplace Cloud hosts its own Email SMTP service in Azure. This is used to receive all incoming email transmissions. Email receipt is accepted using SMTP port 25. No credentials are needed to send email to this server. Support for encryption is available using the STARTTLS mechanism.

Xerox® Workplace Cloud – Single Sign-On

The Workplace Cloud solution provides the SSO functionality that can be called or accessed from supported Apps in the Xerox® App Gallery. The server acts as the network interface accepting and responding to requests to store or retrieve authentication information, as well as the keeper of that information. All SSO related information is stored in the SQL database used by Workplace Cloud. Sensitive information such as the actual stored authentication data, the private key used to decrypt the SSO requests sent by an App, and the public key used to validate signed requests from an App are all stored in encrypted format within the SQL Azure database.

LDAP/ADS Server

The LDAP/ADS Server is part of the customer's network and is not a deliverable of Workplace Cloud. Therefore, the security and maintenance of the LDAP/ADS Server is outside of the responsibility of Workplace Cloud.

When Company Authentication Type is enabled for LDAP Authentication, or Convenience Authentication is configured for LDAP when using Alternate Login or Auto Enrollment of Cards, Workplace Cloud will verify user credentials against Active Directory. The workplace credentials consist of Domain Name, Domain Username and Domain Password. The communication path uses either LDAP (Port 389) or LDAP over SSL (Port 636). Once a user is verified, the following LDAP fields will be retrieved and written to the Workplace Cloud user record:

- Email Address: mail
- Username: sAMAccountName
- Department: department
- Groups: memberof

By default, the Workplace Cloud runs in automatic configuration mode, where the Xerox® Workplace Cloud Agent retrieves and stores a list of available active directory domains based on the context of the logged in user on the Agent computer. Standard LDAP/AD fields are used to retrieve information about the user. The administrator has the option to enable a manual LDAP configuration mode, allowing them to control which LDAP domains will be used for authentication as well as configuring which LDAP fields will be read and used to populate the user fields in Workplace Cloud user record. Besides the normal fields of Email Address, Username, Department and Groups, the administrator can also define a field to retrieve the Primary PIN of the user (Access Card Number).

The manual LDAP configuration mode also supports the ability to store LDAP system credentials for each LDAP server. These are stored in the SQL Azure database, and the password is encrypted. The system credentials allow the solution to support card on-boarding, by looking up unknown card access numbers in LDAP and importing a matching user into Workplace Cloud. The credentials also support the ability to validate that a user attempting to log into a printer through an access card is still a user in the LDAP/AD system, and is not deleted.

Azure AD

The Microsoft Azure AD system is part of the Microsoft Azure backend system and is not a deliverable of Workplace Cloud. However, it is possible to configure Workplace Cloud to use Azure AD as a user authentication mechanism. This is a company-specific setting, and when enabled applies to all interfaces of Workplace Cloud that require authentication credentials.

When using Azure AD, the user will supply their email address, which is then used to look up which account they are in and which authentication mechanism to use for that account. If using Azure AD, the authentication mechanism with Azure uses OAUTH. This is an open standard, commonly used on the Internet to delegate authorization decisions across a network of web enabled applications. When using OAUTH, the Workplace Cloud system will turn control for user validation over to Azure AD. The user will actually authenticate with the Azure AD site and then delegate permission to use the Workplace Cloud solution. When using OAUTH, Workplace Cloud solution never sees the user's password. What is returned to the Workplace Cloud solution is the result of the authentication request as well as an Azure Authentication Token and Refresh Token. Workplace Cloud will validate the Azure authentication token authenticity. The Azure AD Graph API is used to retrieve the following fields for the user: mail, userPrincipalName & department. The mail and userPrincipalName fields are used to

validate that the original email address passed into the Workplace Cloud system matches at least one of those fields in the user's basic profile. After the authentication token is validated, the Workplace Cloud solution will grant the user a Workplace Cloud authentication token. The expiration time of the Workplace Cloud authentication token matches that of the Azure Authentication token.

The XPPMS solution will store both the Workplace Cloud authentication token and Azure refresh token on the specific device and interface to which the user logged in. In this case either:

- The Xerox® Workplace Cloud Mobile App on the users' mobile device
- On the PC running the desktop Client

Note: Users can also log in to Workplace Cloud using the Web Portal (browser), the Agent, and the Printer Client (@PrintByXerox app), however, the Workplace Cloud Authentication Token and Azure Refresh Token are never stored in these scenarios.

If a user tries to access the given interface above and the Workplace Cloud authentication token has expired, then the system will attempt to re-authenticate with Azure using the Azure refresh token (assuming it has not expired). If successful, this results in a new Azure authentication token and refresh token, which is then used to generate a new Workplace Cloud authentication token.

The default Azure authentication token lifetime is 2 hours and the default Azure refresh token lifetime is 2 weeks. These can of course be modified through Azure by the customer, but this is outside the scope of Workplace Cloud. The relevant point here is that the authentication token lifetime is very short, and therefore the Xerox authentication token lifetime is short. This forces the Workplace Cloud interfaces to frequently revalidate that the user is still in valid within the Azure AD system before updating the Workplace Cloud authentication token.

All Azure AD communication between the give Workplace Cloud interface (Web Portal, Workplace Cloud Mobile App, Desktop Client, or @PrintByXerox app) is done using HTTPS over port 443.

There is a login scenario for Workplace Cloud using Azure AD that does NOT use OAUTH. This case is where the printer authentication is being used, and the user manually enters user credentials using the Alternate Login feature or when trying to auto-register a card. In this scenario, the Xerox printer does not have the ability to display a browser-based screen allowing the OAUTH login page to be shown. Because of this device side limitation, the printer will use native screens to prompt for the Azure AD username and password. This information is passed from the printer, to the Agent, to the Workplace Cloud and finally to Azure for validation and authentication. The same validation is done on the returned Azure Access Token as is done in the OAUTH scenario. The user data is always encrypted using HTTPS along each path, and is never stored on any of the devices. When logging in using this method, no tokens are ever stored. The user session will end at the printer when the user logs out or a system timeout occurs.

Third-Party Public Print Provider

This diagram shows the flow between Workplace Cloud components and a third-party public print provider. All communication is over HTTPS using TLS.

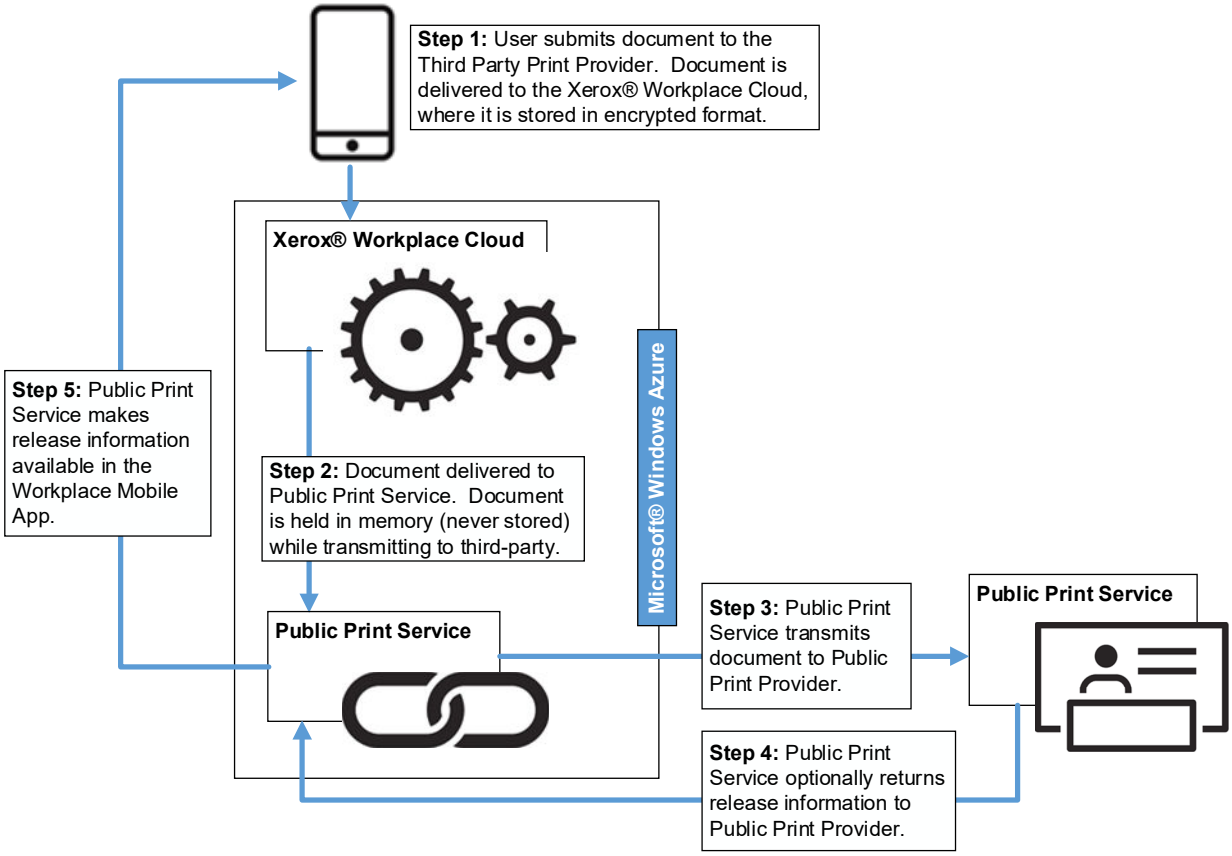

Figure 4–1: Third-Party Public Print Provider

Workplace Cloud, when configured to do so, offers the capability to a user of printing to a third-party public print provider from the Xerox® Workplace Mobile App. These third-party networks provide access to printers at hotels, airport lounges, and other public locations.

When printing to a third-party public print provider, the user is alerted that they are sending their document outside of the Workplace Cloud. Each document printed to a third-party public print provider is stored within Azure Storage. It follows a 7-day document retention policy, which is applied to the document at the time of printing. The original document is stored within Azure Storage in an encrypted format.

Access to these documents is only available to the following:

- The owner of the documents using the Xerox® Workplace Mobile App for preview.
- Authorized Xerox personnel responsible for deployment and maintenance of the system. Since the documents are encrypted, even the authorized personnel cannot open the document to view its contents.

Original documents printed to a third-party print provider are delivered to the Xerox® Workplace Mobile Public Print Service, which is co-located with the Workplace Cloud in Microsoft® Windows Azure.

Original documents are transmitted from the Workplace Cloud Public Print Service to the third-party public print provider in a secure manner. All communications to and from the Workplace Cloud Public Print Service are over HTTPS using TLS. Documents are always transmitted securely and are protected by TLS security during transmission to the third-party public print provider.

The third-party public print provider may respond with a release code or other information the user would need to retrieve their printed output. It is delivered securely over HTTPS. This information is available using the Xerox® Workplace Mobile App only by the user who printed the document.

Xerox maintains the security and integrity of the document up until the point that it is transmitted to the third party. Xerox cannot assume responsibility for the security of any content of the document that is transferred.

Xerox® Workplace Cloud Agent

The Xerox® Workplace Cloud Agent has multiple functions.

1. The agent is responsible for discovering printers within the customer's network, determining the printer capabilities, and relaying that information to the Workplace Cloud.
2. The Agent is responsible for routing print jobs to target printers and print queues.
3. The Agent is responsible for performing any printer configuration. This includes the following feature areas:

   - Convenience Authentication – The agent will make SNMP queries and modifications to the following device settings: enable/disable for Convenience Authentication/Xerox® Secure Access, Blocking Screen strings, Alternate Login, and Service Locking.
   - Workplace Cloud Printer Client Application – The agent will register the Workplace Cloud Printer Client Application on the printer.

4. The Agent will implement the EIP Convenience Authentication API, acting as the authentication server, which allows users to authenticate their identity and unlock the printer.
5. The Agent is responsible for domain authentication lookups of users.
6. The Agent will listen for Network Appliance card data, and will release any pending jobs to the associated printer.

The Agent is installed on a PC. The installing user must have administrator privileges since the Agent software is installed as a Windows service. The Agent cannot be connected to the Workplace Cloud unless the Workplace Cloud is configured to accept the Agent.

The Agent user interface is available to all users who can log on to the agent PC. It displays the printers discovered by the agent and print queues served by the agent. It allows only the proxy server address for that agent to be changed. It does not present any user or customer specific information.

If the Agent Proxy setting is configured by a user, the Agent will in turn set the system level proxy of the PC on which the Agent is running. The system level proxy settings would then be usable by other applications running on the same PC.

A local database is maintained on the Agent PC. This database stores printer discovery settings and printer information for each printer discovered, and print queue information as entered by the administrator. Access to the database is restricted to user's who have permission to log into the agent PC.

The Agent installs by default in the following location:

Program Files(x86) > XEROX > Xerox Workplace Cloud Agent

Access to this folder and sub-folders is limited to users logged on to the agent PC. It contains the agent executable file, its database, and language libraries.

By default, agents are set to upgrade automatically when a new version of the agent software is available. Agents connect to the Workplace Cloud and, if a newer version is available, it is automatically downloaded over HTTPS using TLS and installed. The administrator can disable this feature as needed..

Threats include physical damage to the system, attacks over the network, as well as damage caused by viruses. The goal is to minimize the security risks as much as possible, and have policies in place to detect and reduce the negative impact of a security incident. Examples of things that can be done to reduce risks include proper use of logins and passwords, restricting network access, applying security-related operating system updates, and the use of virus detection software.

The customer is ultimately responsible for securing their environment to meet their specific security needs. Depending on the customer needs, the customer can increase security by installing a firewall, and/or physically securing the hardware to a limited access area. The customer, depending on their needs, should use tools to monitor and log physical and network access to the Agent hardware and software to determine if and when a security incident has occurred. The customer should also back-up their data to ensure that it may be recovered in case of deletion or corruption.

For more information about authentication and communications-related security information, refer to *Communication between Xerox® Workplace Cloud and the Xerox® Workplace Cloud Agent*, *Communication between the Xerox® Workplace Cloud Agent and the Printer*, or *Communication between LPR Clients and the Xerox® Workplace Cloud Agent*.

Server-Based Print Queues

For a server that hosts third-party print queues used by Workplace Cloud, nothing special is required. To minimize security risks, leverage any security features of print control software. Incorporate standard security measures, apply security-related operating system updates, use anti-virus software and add hard disk encryption.

The customer is ultimately responsible for securing their environment to meet their specific security needs. Depending on the customer needs, the customer can increase security by installing a firewall, and/or physically securing the hardware to a limited access area. The customer should back up their data to ensure that it may be recovered if deletion or corruption occurs.

Printer

Xerox printers have various 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 printer behavior.

Xerox® Secure Print allows you to control the print timing of your documents. When using Secure Print during print job submission, users enter a passcode, and then must enter the same passcode to retrieve the job at the printer.

Users may choose to use Secure Print with Secure Print enabled printers, or the administrator may configure their Workplace Cloud account to require that Secure Print be used for all jobs sent using Workplace Cloud to that printer.

Secure Print passcodes are never stored on the mobile App or in the Workplace Cloud. They are transferred securely over TLS. Passcodes are never stored externally to the job on the printer.

Passcodes are numeric and conform to the requirements of the printer model. Auto-generated passcodes are a minimum of 6 digits for all printers whose maximum is at least 6 digits.

For information on the security of a job while it is stored on the printer, refer to your printer documentation.

Additional security can be enforced at the printer if the printer is EIP Capable and/or supports the EIP Convenience Authentication API. For those printers which support this capability, the Workplace Cloud provides the capability to lock the printer's local user interface, and require the user to authenticate themselves at the printer in order to gain access to any of the services/features of the printer. There are three ways in which a user can authenticate:

1. The user may supply their Workplace Cloud user credentials (user name/password, LDAP, or Azure AD credentials depending upon the Company/Account configuration) at the printer, or if the PIN Authentication feature is enabled, they can enter a PIN to login to the printer.
2. The user can identify themselves using their access card (for example, employee badge).
3. The user can use the Xerox® Workplace Mobile App with its "Unlock Printer" feature. The supported methods of unlocking the printer include:

- NFC – Use your Android device or iPhone 7 or newer with iOS 11.
- QR Code – Scan the QR code found on the Welcome Sheet or for some printers on the authentication blocking screen.
- Manual Code Entry - Enter the 4-character code found on the local user interface of the machine into the Workplace Mobile App.
- Any of these methods will identify the printer in the App and the user can confirm that they wish to unlock the device.

In each of the above scenarios, upon supplying valid credentials or making the unlock request, the printer will remove the blocking screen and the user will have access to the services / features of the printer. If the printer is an EIP capable device and the Workplace Cloud Print Client Application is installed, then the user may select the App and view their list of jobs without providing additional login credentials for the app.

In conjunction with authentication feature, Workplace Cloud supports a feature called Auto-Release. This feature is disabled by default, but may be enabled by the Administrator for the given account. Upon successfully completing the authentication step at a printer, if the Auto-Release feature is

enabled, any print jobs uploaded to the Cloud system will automatically be released and printed at the device.

Other examples of printer security features are as follows:

- Image Overwrite electronically shreds information stored on the hard drive of devices as part of routine job processing.
- 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.
- Certificate Validation forces the printer to validate all certificates used for HTTPS communication to ensure that they originate from a trusted certificate authority.

For more information about the above examples as well as for other printer security-related technologies, refer to

http://www.xerox.com/information-security/product-security

The Workplace Cloud supports printers from various manufacturers. It is the customer's responsibility to understand the security features of any non-Xerox printers configured for use in the system.

Xerox® Workplace Cloud Printer Client Application

Devices which are EIP capable have the ability to support the Xerox® Workplace Cloud Printer Client Application. This App allows users to log into their account, view and manage their print jobs. There are two methods of adding / using the Workplace Cloud Printer Client Application:

1. ConnectKey® 2.0i, AltaLink®, and VersaLink® Products – Support the @PrintByXerox Gallery App. This form of App is installed by the customer, typically a system administrator using the Xerox® App Gallery, or it may come pre-installed (as an in-box App).
2. Xerox® Workplace Cloud Agent – The Agent installed the EIP App directly on the printer based on configuration settings made using the Xerox® Workplace Cloud Web Portal.

There are 3 modes of execution for the Workplace Cloud Printer Client Application. The first of which is the unlicensed mode. This mode is only supported with the ConnectKey App, and the user is limited to the basic workflow of email submission and EIP print release. When using this mode, there is no Agent installed on the customer's network. Print jobs are retrieved from the Workplace Cloud by the printer using HTTPS over TLS with port 443.

The second mode of execution for the EIP App is a licensed mode, without an Agent. This mode is only supported with the ConnectKey App. In this mode, the user has access to most of the features of Workplace Cloud, including use of the Workplace Mobile App. Print jobs are retrieved from the Workplace Cloud by the printer using HTTPS over TLS with port 443.

The third mode of execution for the EIP App is the traditional Workplace Cloud environment, with a license and one or more Agents. The Agent will install EIP in this mode, using the EIP Registration API, which is done using HTTP/HTTPS. Print jobs are received using the Agent using LPR (port 515) or Raw IP (port 9100).

Customer Email Server

The Customer Email Server is used to get print jobs to the Workplace Cloud. It acts as a mail relay system to route jobs to the mail service hosted in Azure. The setup, maintenance, and security of the customer email server is outside the scope of Workplace Cloud.

User Workstation (Workplace Cloud Desktop Client)

Users may install the Xerox® Workplace Cloud Desktop Client on their Windows PC. This application will install the administrator defined default print queues on the user's PC, using either the Xerox® Global Print Driver (GPD) or an administrator uploaded custom driver, as well as install and start a background service and a sys tray utility. The background service is used to monitor for new job submissions using the installed Desktop Client and send these up to the cloud server. All communication between the Desktop Client and the Workplace Cloud hosted in Azure is done using HTTPS over port 443.

If the user workstation is configured to use a proxy server, the Desktop Client will use the configured proxy setting when communicating with the Workplace Cloud. This includes the ability to use proxy authentication if enabled in the system-wide proxy settings.

The Workplace Cloud Desktop Client can be downloaded and installed by the user using the Web Portal, or it may be pushed by the IT department of the customer to the end user. If installed using the Web Portal, Workplace Cloud will create an install package for the printer or print queue based on the authentication token for the user who is logged in. This means the login token will be included in the installer. If the install package is pushed by the IT department of the customer, then no token is included.

To use the Desktop Client, users must provide their credentials. When validated, authentication for the user is maintained on the PC for future use. The expiration period of the authentication token is based on the license of the account, with a maximum of up to 7 days. When the authentication token expires, the user will be re-prompted to supply their credentials.

Print Job Path

When using the Desktop Client to submit jobs to a pull-print queue (where jobs are held for later release), the administrator can configure where the job will be stored while it is waiting for the user to release it. This feature is called "Local Print Optimization". By default, this is set to "Enabled with Cloud Backup", meaning that the desktop client will store a local copy of the job and send a backup to the cloud service. The administrator can also define a maximum file size to be uploaded to the cloud when using this option. If the file exceeds the configured maximum, it will not be sent to the cloud.

When jobs are released, the solution will attempt to send the local copy of the job to the printer first. If there is a connection issue from the local workstation to the printer, the cloud copy of the job will be sent to the printer. The desktop client will clean-up the local copy of the job the next time it synchronizes with the cloud backend. The administrator can also configure this setting such that jobs are never stored locally and are always sent to the cloud, or they can configure it such that jobs are only stored locally and never sent to the cloud. Locally stored jobs are saved on the hard drive of the user's workstation, at the following location:

C:\Users\<USERNAME>\AppData\Local\Xerox\XMPC\VirtualPrint\RetainedJobs

The job will be removed either after printing or based on configured retention settings.

Failover Support

In order to improve the user experience of the Workplace Cloud Desktop Client for scenarios where the solution is not able to communicate with the cloud backend system (such as networking issues or the service is temporarily down), a special offline printing mode is supported. In cases where the cloud backend system is not available, the user will be notified of the connection issue when they attempt to print. They will be given the option to continue to print and wait for the connection to be restored so the job can be processed, or they will be offered the option to print the job immediately to one of up to 10 different devices. The set of available devices is based on the user's favorite printers from the Workplace Mobile App as well as recently used printers. The Workplace Cloud system will maintain this list of devices and the Desktop Client will periodically retrieve it and store it locally at:

C:\Users\<USERNAME>\AppData\Local\Xerox\XMPC\VirtualPrint\

This file includes information like the name of the printer, IP Address, MAC Address, Manufacturer, Model, Site, Printer Language, User's Email Address, Printing Port Numbers and the Device ID of the printer. If a user opts to print to one of the available printers using the offline mode, the Desktop Client will send the job directly to the printer using the configured print protocol (LPR, RawIP, IPP/S) and will maintain some metadata about the job so that it can update the print history after connection to the cloud is re-established.

The offline printing mode is only supported for a maximum of 24 hours. After that time, users will no longer be able to print using the offline method. Jobs will be held until the client is able to establish connection with the Workplace Cloud. This is designed prevent unauthorized printing for an extended period without validation that the user still exists in the backend system. The system administrator should address any connectivity issues within that 24 hour period.

Microsoft Office 365 - Email Service

Email responses sent to the end user are handled by the Office 365. This service is hosted by Microsoft using an Office 365 email account. Login access to this Workplace Cloud email account is limited to a few key Xerox personal on the Workplace Cloud team. Email transmission is done using Exchange Web Services over port 443 (HTTPS).

Network Appliance

The network appliance, sometimes referred to as an ID Controller, is an external hardware device that supports the ability to plug in a USB keyboard mode card reader and transfer card information to a configured application. In this case, the Network Appliance is configured to send card data to the Agent.

The network appliance and the Agent communicate using raw TCP sockets with proprietary data exchange based on the manufacturer of the appliance.

Elatec: The Elatec TCP Conv and TCP Conv2 use ports 7778 and 7777 respectively. The card data is sent in plain text.

RF Ideas: The RF Ideas Ethernet 241 uses port 2001. By default, the card data is not encrypted, but the option to use encryption is available.

Xerox® Services Manager

Xerox® Workplace Cloud can be configured to connect to Xerox® Services Manager (SM) in order to perform the following actions:

- Export Job Data (Page count, Plex, and so on.)
- Import Printers, Sites, and Printer/Site Mappings

Each of these methods of synchronizing with SM has its own configuration as well as specific limitations on the system as a whole. Connectivity to SM is achieved using a special connection URL and creating a new account that is linked to SM. The Administrator will need to provide an SM Account ID at the time the Workplace Cloud account is created. The Importing of Printers and Sites requires the SA to configure an SM Username and Password.

All communication between SM and Workplace Cloud will be over HTTPS (port 443).

App in the Gallery

This item refers to an App in the Xerox® App Gallery that is modified to use the Single Sign-On feature provided by Workplace Cloud and is running on the EIP browser of the printer. The App is expected to retrieve configuration from the printer and pass this back to the App Server so that it can determine if the SSO feature is supported by the Workplace Cloud solution. The App and EIP browser act as an intermediary between the App Server and the Workplace Cloud Solution. All communication between the App, the App Server and the Workplace Cloud uses TLS.

Note: The App is not written by or controlled by the Workplace Cloud solution. It is an external component to the system that is making use of functionality provided by the Workplace Cloud.

App Server

The server hosting the functionality supplied by an App in the Gallery. This can be a Xerox® hosted server or a 3rd party server, depending upon who created the App. The App Server never directly communicates with the Workplace Cloud. All communication is funneled through the instance of the App running on a printer and the EIP browser of that device. Communication between the App Server and the App uses TLS.

Note: The App is not written by or controlled by the Workplace Cloud solution. It is an external component to the system that is making use of functionality provided by the Workplace Cloud.

System Component Interfaces

Communication between the Xerox® Workplace Mobile App and Xerox® Workplace Cloud

The Xerox® Workplace Mobile App uses the HTTPS over TLS protocol for all communication with the Xerox® Workplace Cloud. It establishes an HTTPS secure connection with the Workplace Cloud relying on the mobile device operating system to validate the security certificate as part of establishing the TLS connection. The security certificate is issued by Comodo (a trusted certificate authority) and ensures that the application has been verified and validated.

The Xerox® Workplace Mobile App requires users to authenticate before using any of its features. Basic authentication is performed with the Xerox® Workplace Mobile App providing username and password information over the HTTPS protocol, usingTLS.

After authentication is complete, data is passed between the Xerox® Workplace Mobile App and the Workplace Cloud to enable the features of the service within the Xerox® Workplace Mobile App. This includes all data for previewing and printing jobs, location of printers, and user location data as determined by the mobile device. Users are only able to access documents they submitted and printers to which they have been granted access.

Users should consult their network provider on best practices for securing their cellular (3G/4G/LTE) communications on their mobile devices.

Communication between Xerox® Workplace Mobile App and the Customer Email Server

Emails submitted to the Xerox® Workplace Cloud by a user's mobile device or computer will use the security mechanism defined by the user's email client. User documents are the primary data transmitted using email to the Workplace Cloud. It is the user's responsibility to ensure that appropriate email security controls are in place.

Communication between the Customer Email Server and Xerox® Workplace Cloud

Emails are processed and consumed immediately upon receipt by the Xerox® Workplace Cloud. Emails are not stored in any repository or inbox.

Communication between Xerox® Workplace Cloud and the Xerox® Workplace Cloud Agent

The Xerox® Workplace Cloud Agent uses the HTTPS protocol over TLS for all communication with the Workplace Cloud. It establishes an HTTPS over TLS secure connection with the Workplace Cloud relying on the PC's operating system to validate the security certificate as part of establishing the TLS connection.

After successful installation of the Agent software, it will attempt to register itself with the Workplace Cloud. The Agent's registration process provides the Workplace Cloud with the Agents account administrator credentials, the Agent Activation Code, and a machine hash code. The Workplace Cloud returns an Agent registration identifier to complete the registration process. The Workplace Cloud account's administrator credentials are only held in memory during the registration process and removed when the registration process is complete.

After successful registration of the Agent, print job data is transmitted between the Workplace Cloud and the Agent in the form of print ready files. This data may exist in memory on the agent PC while it is being spooled to the printer. In addition, data about printers discovered and printer capabilities is transmitted.

If the Convenience Authentication feature is enabled, the Agent will facilitate communications acting as a middleman between the printer and the Workplace Cloud, receiving authentication requests from either entity and converting them to the appropriate response and passing that onto the recipient. All such communication is done using HTTPS.

As part of the Convenience Authentication feature, the Agent will support a failover mode for card-based authentication. The Agent will create an SQL CE database on the hard drive of the machine on which it is running. The database is password protected using a password that is generated by the Workplace Cloud backend system. This password is shared across all Agents for any one account, but is unique across all accounts. Once per day, the Agent will retrieve from Workplace CloudS, the list of users for the account, and will store this in the local SQL CE database. The information stored for each user consists of:

- Email Address
- Network User Name
- User ID (GUID) – This is just an internal identifier
- Card Number
- NFC Number(s) – Android phone identifiers when used with the Elatec TWN 4 reader
- Legacy Card Number – For customers using Xerox® Secure Access readers.

When a user tries to authenticate with a printer, the authentication request is transmitted to the Agent. If the Agent is not able to communicate with the Workplace Cloud, it will fall back to using its local database of users. If the user is logging on with a card (or an Android Phone using the TWN 4 reader), the Agent will look up the card or NFC number and if found will allow the user to log in to the printer. Note that the auto-release jobs feature is not available in this fallback authentication mode. In addition, the Alternate Login feature and the @PrintByXerox App will not be available in this scenario. The intent of this feature is to allow users to access other services on the printer, such as Copy, Scan, Fax, even if the cloud backend cannot be reached.

The failover authentication mode is only supported for a maximum of 24 hours. After that time, users will no longer be able to authenticate with the printer. This mode is designed to prevent unauthorized

access to the device for an extended period without validation that the user still exists in the backend system. The system administrator should address any connectivity issues within that 24-hour period.

Communication between the Xerox® Workplace Cloud Agent and the Printer

The Xerox® Workplace Cloud Agent uses SNMPv1/v2 or SNMPv3 to discover printers and printer capabilities. For SNMP v1/v2, customers can configure the community name strings for the agent to use if they have configured their printers to use non-default values. For SNMPv3, customers can configure a user name for the administrator account, an encryption mechanism and passwords for authentication and privacy. These same settings must be configured on the printers in order to use SNMPv3.

The Agent will route print jobs to the target printer using either Raw Port 9100, LPR/LPD Port 515 or IPP over SSL on Port 443. The LPR and RawIP ports are both configurable.

Customers can further secure the print path by enabling IPsec between their Agent PC and their printers provided the printers support IPsec. When configuring IPsec, ensure that the communication between the Agent and Workplace Cloud does not employ IPsec.

When a printer is enabled, the Agent may register the Workplace Cloud Printer Client Application, or it may enable the Convenience Authentication feature based on the printer configuration settings supplied by the administrator. The @PrintByXerox App will be registered using the EIP Registration API, which requires the printer's administrator credentials. The Convenience Authentication feature enablement and configuration is done using SNMP using the SET Community string for SNMPv1/v2 or the SNMPv3 administrator account and passwords along with the administrator credentials for the printer.

If the Convenience Authentication feature is enabled, the Agent will play a role in authenticating a user at the printer. The Agent will facilitate communications between the printer and the Workplace Cloud, receiving authentication requests from either entity and converting them to the appropriate response and passing that onto the recipient. All such communication is done using HTTPS.

The Agent may be enabled to support iOS Native printing. When enabled, devices running iOS may locate and send print jobs directly to the Agent. This is done using the IPP protocol using port 631. For further details on this capability, refer to *Workplace Cloud Administrator Guide*.

Communication between the Xerox® Workplace Cloud Agent and a Third-Party Print Queue

Customers identify their print queues to the Agent by providing information on the server, port and queue name.

The Agent will route print jobs to the print queue using LPR/LPD Port 515. This port is configurable.

Customers can further secure the print path by enabling IPsec between the Agent PC and the server hosting the third-party queue. When configuring IPsec, ensure that the communication between the Agent and Workplace Cloud does not employ IPsec.

Communication between the Workplace Cloud Desktop Client and Xerox® Workplace Cloud

When a user sends a job to the Xerox® Workplace Cloud using the Desktop Client, the file is converted to Postscript and stored temporarily on the hard disk of the PC. The location of the stored files is dependent upon the user:

C:\Users\<USERNAME>\AppData\Local\Xerox\XMPC\VirtualPrint\Jobs

The Workplace Cloud Desktop Client runs in the background and monitors this folder for any new files. When one is detected, it then processes that job based on the configured "Local Print Optimization" feature, either storing locally, or uploading to cloud or both. For uploads to the cloud, the file is sent to Workplace Cloud using HTTPS (TLS) over port 443. For locally stored jobs, the file is moved to:

C:\Users\<USERNAME>\AppData\Local\Xerox\XMPC\VirtualPrint\RetrainedJobs

After upload to cloud and/or transfer to the "RetainedJobs" directory, any temporary files are deleted from the hard disk.

The Workplace Cloud Desktop Client will also periodically retrieve a list of the 10 most recently used/favorite printers for the user and will store this on the hard drive of the PC on which the client is running. This information is used for print failover if the cloud service is not available. The Client will also maintain job history information for any jobs printed using the failover method and will report this back to the Workplace Cloud solution when connection is re-established.

In order to support the "Local Print Optimization" feature, where jobs are stored locally, the Desktop Client makes use of Microsoft's Azure IoT Hub. This allows the Desktop Client to receive notifications about stored jobs, such as releasing the job or deleting the job. The Desktop Client opens a connection to the IoT Hub, which allows the Workplace Cloud solution to send commands back down to the client in response. The result is an open connection between the Desktop Client and the Azure IoT Hub. All communication is done using AMQP over port 5671 (with a fallback to AMQP over WebSockets using port 443). This connection is outbound from the client to the Azure IoT Hub, which allows responses to be sent back through this connection. User workstations should allow outbound traffic over port 5671 to support this feature. If this port is not open, it should fallback to using outbound port 443, which is typically allowed in most environments. If your environment is very restrictive to HTTPS traffic, you may need to review the setup of workstations, proxies and internet firewalls.

Communication between the Workplace Cloud Desktop Client and the Printer

If a PC running the Desktop Client and the Printer to which a job is to be released is on the same network, the Desktop Client will send the job directly to the printer. This process avoids the need to send the job to the Workplace Cloud. The Desktop Client detects that the printer is on the same network using an ICMP ping request. The print job itself will be sent using Raw IP (Port 9100), LPR (Port 515) or IPP over TLS (Port 443) to the printer based on the printer configuration. If the Desktop Client is running in failover printing mode, jobs will be transferred to the printer directly using the configured print protocol for that device (Raw IP, LPR or IPP/S).

Communication between the Xerox® Workplace Cloud Agent and the Customer ADS (LDAP) Server

When Company Authentication Type is enabled for LDAP Authentication, Workplace Cloud will verify user credentials against Active Directory. The workplace credentials consist of Domain Name, Domain Username and Domain Password.

Workplace Credentials are not stored on the Agent computer or in the Cloud database. The Agent will query Active Directory for available domains.

In order to communicate with Active Directory, Workplace Cloud uses the Active Directory Services Interfaces (ADSI) technology that is available in all Windows Operating Systems supported by Workplace Cloud. The communication with the Active Directory servers occurs using the standard LDAP port 389 or using LDAP over SSL with port 636. Communication is secured using SASL bind usually using the GSSAPI mechanism.

If LDAP is configured for manual configuration mode, then Workplace Cloud supports the ability to store LDAP system credentials for each LDAP server. These are stored in the SQL Azure database, and the password is encrypted. The system credentials allow the solution to support card on-boarding, by looking up unknown card access numbers in LDAP and importing a matching user into Workplace Cloud. The credentials also support the ability to validate that a user attempting to log into a printer through an access card is still a user in the LDAP/AD system and has not been deleted.

Communication between the Xerox® Workplace Cloud and Xerox® Services Manager

All communication between Xerox® Services Manager and Xerox® Workplace Cloud will be over HTTPS (port 443).

Communication between LPR Clients and the Xerox® Workplace Cloud Agent

The Agent supports the ability to enable an LPR listening port, which can accept incoming print jobs from LPR Clients that may not support the ability to print to the shared network pull queues used by Microsoft Windows workstations. This feature might be used Mac or Linux workstations or possibly even mainframes. By default, this interface uses LPR over port 515, but the port is configurable.

Communication between the App from the Gallery, the App Server and the Xerox® Workplace Cloud

All SSO related communication requests to get or set a user's authentication data uses TLS. Sensitive information in all communications is also encrypted at the message or data item level in addition to the encryption of the data stream itself using TLS. Message level encryption uses shared keys pairs (a public and private key) for exchange of data between Workplace Cloud and the App Server. Data is both encrypted and signed to ensure authenticity and privacy. Encryption is done using an RSA algorithm with key size of 10240. Additional details on SSO can be found in Chapter 7 *Single Sign-On* of this document.

5. Logical Access, Network Protocol Information

Protocols and Ports

The following table lists the standard default ports used by the Workplace Cloud solution. Some port numbers are configurable on the printer, such as the Raw IP printing port. Other port numbers are non-configurable and cannot be changed.

Table 5-1: Protocols and Ports

Protocol	Default Use Port Value	Use	Option	Direction
Xerox® Workplace Mobile App (Print Portal) Ports :				
HTTPS using TLS	TCP 443	Authentication, Job / Printer Listing, Initiate Print Conversion	Non-configurable	App to Workplace Cloud
HTTPS using TLS	TCP 443	Authentication	Non-configurable	App to Azure AD
IPP	TCP 631	iOS Native Print Submission	Non-configurable	App to Agent
HTTPS using TLS	TCP 443	Authentication (for Chrome SSO)	Non-configurable	App to Google
Xerox® Workplace Cloud Agent Ports:				
HTTPS using TLS	TCP 443	Retrieval of configuration, sending printer info, retrieval of print jobs, authentication.	Non-configurable	Agent to Workplace Cloud
Raw IP	TCP 9100	Print Submission	Configurable	Agent to Printer
HTTPS	TCP 443	Azure Service Bus (with application level encryption)	Non-configurable	Agent to Workplace Cloud

Protocol	Default Use Port Value	Use	Option	Direction
LPR	TCP 515	Print Submission	Configurable	Agent to Printer or to Print Queue
IPP over SSL	TCP 443	Print Submission	Non-configurable	Agent to Printer
LDAP	TCP 389	Authentication	Non-configurable	Agent to ADS Server
LDAP over SSL	TCP 636	Authentication	Non-configurable	Agent to ADS Server
HTTPS using TLS	TCP 443	Convenience Authentication, EIP Registration, Accounting Data Configuration and	Non-configurable	Agent to Printer
HTTPS using TLS	TCP 443	Authentication	Non-configurable	Agent to Azure AD
SNMP	TCP 161	Printer Discovery, Configuration	Non-configurable	Agent to Printer
LPR	TCP 515	Incoming Print Queue – Receive prints from LPR	Configurable	LPR Client to Agent
HTTPS using TLS	TCP 443	Single Sign-On Requests / Responses	Non-configurable	Printer ←→ Agent
@PrintByXerox EIP App Ports:				
HTTPS using TLS	TCP 443	Retrieval of EIP Browser pages for display on the UI. Authentication, Job	Non-configurable	@PBX to Workplace Cloud
HTTPS using TLS	TCP 443	Authentication	Non-configurable	@PBX to Azure AD
HTTPS using TLS	TCP 443	QR Code icon retrieval	Non-configurable	@PBX to Azure Blob Storage
Printer Ports:				
HTTPS using TLS	TCP 443	Initiate Pull Print Request	Non-configurable	Printer to Workplace Cloud
HTTPS using TLS	TCP 443	Convenience Authentication	Non-configurable	Printer to Agent

Protocol	Default Use Port Value	Use	Option	Direction
Desktop Client Ports:				
HTTPS using TLS	TCP 443	Printer Configuration, Driver Download, Print Submission	Non-configurable	Desktop Client to Workplace Cloud
HTTPS using TLS	TCP 443	Authentication	Non-configurable	Desktop Client to Azure AD
AMQP (with HTTPS using TLS as a fallback)	TCP 5671 (TCP 443 fallback)	Print job release notification	Non-configurable	Desktop Client to Azure IoT Hub
Ping	ICMP Echo	Test if printer is on the local network.	Non-configurable	Desktop Client to Printer
LPR	TCP 515	Print Submission	Configurable	Desktop Client to Printer
Raw IP	TCP 9100	Print Submission	Configurable	Desktop Client to Printer
IPP over SSL	TCP 443	Print Submission	Non-configurable	Desktop Client to Printer
Xerox® Workplace Cloud Ports:				
SMTP	TCP 25	Receive Email Submissions	Non-configurable	Listening port for incoming email submissions
HTTPS using TLS	TCP 443	Exchange Web Services. Used to send email responses end users.	Non-configurable	Workplace Cloud to O365 Email Service
HTTPS using TLS	TCP 443	Send Print History and Retrieve Printer List to/from Xerox® Services Manager.	Non-configurable	Workplace Cloud to Xerox® Services Manager
HTTPS using TLS	TCP 443	Azure AD Authentication token validation	Non-configurable	Workplace Cloud to Azure AD

Protocol	Default Use Port Value	Use	Option	Direction
HTTP	TCP 80	Used by the traffic manage to determine which Azure sites are available.	Non-configurable	Azure Traffic Manager to Workplace Cloud
HTTPS using TLS	TCP 443	Single Sign-On Requests / Responses	Non-configurable	Printer ←→ Workplace Cloud
Network Appliance Ports:				
Raw	TCP 7778	Receive Card Swipe Data from Elatec TCPConv	Configurable	Network Appliance to Agent
Raw	TCP 7777	Receive Card Swipe Data from Elatec TCPConv2	Configurable	Network Appliance to Agent
Raw	TCP 2001	Receive Card Swipe Data from RFIdeas Ethernet 241	Configurable	Network Appliance to Agent

Firewall Rules

The following table lists the standard firewall rules used by the Workplace Cloud solution. It is expected that the administrator will modify the firewall rules of the PC running the Agent if these features are being used at the customer site.

Table 5-2: Firewall Rules

Protocol	Default Use Port Value	Use
HTTPS	TCP 443	Authentication
Raw	TCP 7778	Receive Card Swipe Data from Elatec TCPConv
Raw	TCP 7777	Receive Card Swipe Data from Elatec TCPConv2
Raw	TCP 2001	Receive Card Swipe Data from RFIdeas Ethernet 241

6. System Access

Xerox® Workplace Cloud (Web Portal)

When accessing the Xerox® Workplace Cloud directly (using the Web Portal for either general user access or administrative access), the user will connect to:

https://xwc.services.xerox.com/Login

Users will need to provide their email address. Workplace Cloud will look up the user's email address to determine the company account to which they are homed, and then based on that company's authentication configuration, they will be prompted to enter either their Workplace Cloud password, their company LDAP credentials (DOMAIN\USERNAME and PASSWORD), or their Azure AD credentials. When using LDAP, the Domain will be used to route the LDAP requests to the correct Agent, which thenwill communicate with the ADS/LDAP server.

Credentials (either the Workplace Cloud Password, the LDAP credentials, or the Azure credentials) are never saved in the browser. In addition, the user's browser session will timeout after 20 minutes of inactivity.

Xerox® Workplace Cloud Agent

When the Agent is initially installed, the company's Xerox® Workplace Cloud administrator must provide their credentials (Workplace Cloud, LDAP or Azure AD) and Company Code so that the App can communicate with the Workplace Cloud and register the Agent with their account. Subsequent communication to Workplace Cloud will use computed access credentials for the Agent based on the hardware of the workstation on which the Agent is running. The Administrator credentials are not stored or used after the initial registration occurs.

Xerox® Workplace Mobile App

When accessing the Xerox® Workplace Mobile App, users will need to provide their email address. Xerox® Workplace Cloud will look up the user's email address to determine the company account to which they are homed, and then based on that company's authentication configuration, they will be prompted to enter their Workplace Cloud password, their company LDAP credentials (DOMAIN\USERNAME and PASSWORD), or their Azure AD credentials. When using LDAP, the Domain will be used to route the LDAP requests to the correct Agent, which then will communicate with the ADS/LDAP server.

The results of successfully authenticating with Workplace Cloud is an access token. The token is stored on the phone and used for subsequent communication with Workplace Cloud. The lifetime of the access token is either 24 hours or 7 days based on the license type being used for by the account. Prior to the token expiring, the phone will obtain a new token, which requires the use of the user's login credentials. So the Workplace Mobile App will store the user's access credentials on the phone in encrypted format in order to support renewing the access token. For Android devices, the credentials are encrypted and saved to internal storage of mobile device and this is only accessible by the Workplace Mobile App. For iOS devices, the credentials are saved in a keychain which is encrypted and only accessible by the Workplace Mobile App. The OS of the mobile device will delete any saved data including the credentials when the application gets un-installed.

There is a version of the Workplace Mobile App that supports Google Chromebooks as well as an extension to the Google Chrome browser. When run in these environments, the Workplace Mobile App will support authentication using the Cloud solution supported mechanisms, as well as supporting "single sign-on" using your Google credentials to validate the user in place of manually entering credentials.

For Chrome using one of the supported authentication mechanisms for Workplace Cloud, the access token will only be stored in memory. Once the token expires, the user will be required to re-authenticate with Workplace Cloud.

In the case of Chrome using the Single Sign-On (SSO) feature, when a user attempts to log in, the app will pre-populate the email field with the logged on users email address. When this is submitted to the server, the app will also include the Google authentication token of the logged on user as well as the AppID of the Workplace Mobile App. The Workplace Cloud backend system will validate the email, token and AppID with Google using HTTPS over port 443. If these are valid, the user is considered authenticated. The Workplace Cloud then creates a Mobile Print access token and returns that to the Workplace Mobile App on Chrome. The user then remains logged in to the App until the access token expires. At this time, the app will attempt to repeat the process.

Desktop Client

When installing the Desktop Client, users will need to provide their email address. Xerox® Workplace Cloud will look up the user's email address to determine the company account to which they are homed, and then based on that company's authentication configuration, they will be prompted to enter their Workplace Cloud password, their company LDAP credentials (DOMAIN\USERNAME and PASSWORD), or their Azure AD credentials. When using LDAP, the Domain will be used to route the LDAP requests to the correct Agent, which then will communicate with the ADS/LDAP server using LDAP (Port 389) or LDAP over SSL (Port 636).

The results of successfully authenticating with Workplace Cloud is an access token. The token is stored on the user's workstation and used for subsequent communication with Workplace Cloud. The lifetime of the access token is either 24 hours or 7 days based on licensing. Once the access token is expired, the user will be prompted to re-supply their authentication credentials, after which a new access token will be created. For Azure AD, the lifetime of the Workplace Cloud access token matches that of the Azure AD access token lifetime. When this expires, Workplace Cloud will attempt to use the Azure AD refresh token to obtain a new Azure AD access and refresh token, which then will generate a new Workplace Cloud access token.

@PrintByXerox EIP App

To access the @PrintByXerox EIP App, users will either need to log in to the printer using the Convenience Authentication feature, or they will need to log in to the @PBX App itself. User will start by providing their email address. Xerox® Workplace Cloud will look up the user's email address to determine the company account to which they are homed, and then based on that company's authentication configuration, they will be prompted to enter their Workplace Cloud password, their company LDAP credentials (DOMAIN\USERNAME and PASSWORD), or their Azure AD credentials. When using LDAP, the Domain will be used to route the LDAP requests to the correct Agent, which then will communicate with the ADS/LDAP server.

The @PrintByXerox App will never save the user's credentials. Users can log out of the @PBX App manually, by selecting the "Exit" button in the App, or by navigating out of the App (such as selecting the All Services, Machine Status, or Job Status buttons on the UI panel). The UI itself has a built-in inactivity timer that will log the user out if the user is not interacting with the UI. The inactivity period is configurable by the device administrator. In addition to the device timer, the @PBX App itself has its own 5 minute timer. The @PBX App timeout will log the user out of the App after 5 minutes of use, unless they dismiss warning pop-up, which restarts the 5-minute timer.

7. Additional Security Items

Xerox® Workplace Cloud Endpoint Table

The following endpoints, provided FQDN format, are accessed by various components of the Xerox® Workplace Cloud solution that reside inside a customer's network. The customer must ensure that these components have access to the Internet, and in particular these specific endpoints, in order for this solution to work properly. All endpoints are accessed using HTTPS with TLS (port 443).

Table 7-1: Cloud Endpoints

Component	Endpoint FQDN
Xerox® Workplace Cloud Agent	• https://xwc.services.xerox.com • https://xmpcws.services.xerox.com • https://xcpagentservicebus.servicebus.windows.net • https://xcpagentservicebus01.servicebus.windows.net • https://xcpagentservicebus02.servicebus.windows.net • https://xcpagentservicebus03.servicebus.windows.net : • https://xcpagentservicebus10.servicebus.windows.net • (Azure AD only) https://login.microsoftonline.com
Xerox® Workplace Cloud Printer Client Application – @PrintByXerox	• https://xmpceip.services.xerox.com • https://xmpcws.services.xerox.com • https://xcpproduction.blob.core.windows.net • https://xpmmsuks.blob.core.windows.net • (Azure AD only) https://login.microsoftonline.com
Xerox® Workplace Mobile Application – Mobile App	• https://xccsts.services.xerox.com • https://xmpcws.services.xerox.com • https://publicprintapi.services.xerox.com • (Azure AD only) https://login.microsoftonline.com
Xerox® Workplace Cloud Web Portal – Customer Web Pages	• https://xwc.services.xerox.com • (Azure AD only) https://login.microsoftonline.com
Xerox® Workplace Cloud Desktop Client	• https://xccsts.services.xerox.com • https://xmpcws.services.xerox.com • https://xwc.services.xerox.com • https://virtualprintiothub.azure-devices.net

- (Azure AD only) https://login.microsoftonline.com

Certificate Validation

Xerox® Workplace Cloud is a cloud hosted service, available to anyone that has Internet access. To ensure that users are connecting to a known trusted entity, the cloud hosted service in Azure uses a digital certificate created by a well-known and trusted certificate authority.

Connection Details

Followingare details on the different access methods users have available to them when connecting to the Xerox® Workplace Cloud as related to certificate validation.

Web Portal

Well-known browsers which are up to date (version and security patches) such as Internet Explorer, Chrome, Firefox, Edge, include the public keys for most of the well-known certificate authorities (CA) used on the Internet. This includes the CA used to generate the Xerox® Workplace Cloud root certificate. As such, these browsers will test and validate the Workplace Cloud server certificate when a connection is made to the Workplace Cloud Web Portal. No special setup or configuration is needed from the user to take advantage of this capability.

Workplace Mobile App

Similar to the browser on a PC, Android, iOS and Chrome include the public keys for most of the well-known certificate authorities used on the Internet. These public keys are available to applications running on the mobile phone. The Xerox® Workplace Mobile App is designed such that it always validates the server certificate for all communication with the Xerox® Workplace Cloud. If this validation fails, the Workplace Mobile App will prevent any further communication with Workplace Cloud and therefore prevent the user from using the App.

@PrintByXerox App

Most of the newer Xerox devices that support EIP have the capability to perform certificate validation. By default, these devices have validation turned off. It is recommended that the user enable this capability on the printer. If the @PrintByXerox EIP App has been loaded using the Xerox® App Gallery or App Studio, or the App is pre-installed on the MFP, then the public root certificate is included with App and will be used when validation is enabled. If the @PrintByXerox EIP App has been loaded using the Agent, then no public root certificate will be programmatically pushed to the printer. The user will need to obtain the public root cert for the following site:

https://xwc.services.xerox.com/Login

When the cert is available, it will need to be imported into the trusted root certs of each printer where the @PrintByXerox App is installed.

Note: Not all Xerox capable EIP printers support certificate validation.

Auto Release Using Network Appliance Workflow

Held print jobs are released automatically when the user scans a card at a mapped network appliance associated with the printer.

Network appliances are small network boxes that attach to the network and permit Xerox® Workplace Cloud to control the release of user documents to printers that do not support the use of Xerox® Secure Access / Convenience Authentication. A network appliance is configured on the network by the administrator, the appliance is associated with the particular printer in the Workplace Cloud Admin Web Portal, and the user can release their jobs at the printer by swiping their card using the card reader associated with the printer. One network appliance is required for each printer.

Models

Three network appliance models are supported by Xerox® Workplace Cloud: RF Ideas Ethernet 241

- Elatec TCP Conv2
- Elatec TCP Conv

Each of these models is available by default on the Web Portal administration site at **Account > Settings > Network Appliances > Models**. If any or all of these models are not going to be part of your site installation, they can be disabled to turn the listeners off on the server.

The listeners use these default ports:

- RF Ideas Ethernet 241 - 2001
- Elatec TCP Conv2 - 7777
- Elatec TCP Conv - 7778

The default ports can be changed by the administrator if the network appliances on your system have been configured to use a different port. Any firewall on the Agent must be configured to allow communication through the port(s).

By default, the network appliances support communication using non-encrypted channels. Therefore, card data is sent in plain text format when transmitting the card data from the network appliance to the Agent. The RF Ideas Ethernet 241 is the only network appliance that supports encryption, using SSL, of the communication path.

Note: The Ethernet 241 supports SSLv3. It does not support TLS1.x.

Audit Log

The Xerox® Workplace Cloud will maintain a history of the users that have logged in Workplace Cloud using any of the interfaces: Workplace Mobile App, Web Portal, @PrintByXerox, or Convenience Authentication. Entries are maintained for a period of 1 year. Entries older than that are purged from the log.

Azure Data Centers

The Xerox® Workplace Cloud is hosted in the cloud using Microsoft Azure, which is a public cloud computing platform. The Workplace Cloud solution uses three different Azure data centers:

- South Central US – located in Texas
- UK South – located in London
- West Europe – Netherlands (Amsterdam)

All User and Account information is stored in the UK South data center. Print job data is stored in either the US or UK centers based on geo-location. Job reporting information (detailed job history and job accounting information) is stored in the West Europe center. Within the UK data center, there is full active redundancy for services and the database. A US data center failure will fail over to the UK data center. However, a UK data center failure will not automatically fail over to the US data center due to the centralized nature of the User and Account database being in London and because of EU Privacy policies.

Usage Tracking and Reporting

The Xerox® Workplace Cloud supports the ability to collect network accounting information from Xerox devices that support this feature. This includes job information for Copy, Scan and Fax jobs as well as Print jobs. For printers that don't support Xerox Network Accounting, the Workplace Cloud will supplement print job data that it collects with that retrieved from Xerox Network Accounting. This is an optional feature that is disabled by default and must be enabled globally to make it available on a printer-by-printer basis. This data is collected and stored in Azure using their Data Lakes storage mechanism. The Reporting information is stored in Microsoft's Azure Data Center located in Amsterdam. The customer may configure the data retention period for this stored information, with the maximum being 1 year.

Single Sign-On

The SSO capability is designed with a focus on security of the Gallery App authentication data (credentials, token, and so on). Below is a highlight of the main security points of this solution:

- All communication is over HTTPS.
- The Workplace Cloud validates the certificate of the App Server vault. The certificate must be from a well-known and trusted provider.
- The SSO authentication data for a given user and app is given to the Workplace Cloud in an encrypted format. The Workplace Cloud can never view the authentication data.
  Note: It is the responsibility of the App from the Gallery and/or its backend server to encrypt the authentication data before sending it to Workplace Cloud for storage.
- Exchange of sensitive information between Workplace Cloud and the App/App Server uses public key cryptography with asymmetric keys. Each side (Workplace Cloud and App Server) has its own public and private keys, and shares the public key with the opposite side, but keep its private key hidden. Data is encrypted by the public key and then sent to the owner of the private key to decrypt it.
- All message exchanges related to authentication data include digital signatures, so that the receiver can always validate that the request is coming from a trusted entity.
- Messages containing authentication data include 3 levels of encryption:
  - The channel is encrypted via HTTPS.
  - Message content is encrypted using public key cryptography with asymmetric keys. An RSA algorithm is used for encryption with a key size maximum of 16384.
  - Authentication data is encrypted by the Gallery App or its backend server prior to storing it with Workplace Cloud. The format and encryption method used are up to the Gallery APP vault.

Data sent from one entity to the other is always encrypted using the public key of the receiver. As an example, let's assume the App/Gallery App Server would like to store new authentication data in Workplace Cloud. The steps to manage the encryption of this data are as follows:

1. The Gallery App Server constructs the appropriate message data to be sent to Workplace Cloud, and then encrypts that data using the public key of Workplace Cloud.
2. That data is then signed by the App Server using its own private key.
3. When this data is received by Workplace Cloud, it validates the signature using the public key of the Gallery App Server.
4. The message is then decrypted by Workplace Cloud using its private key.

A similar exchange takes place when sending the response message from the SSO vault to the Gallery App Server.


xerox