Xerox® Workplace Cloud 5.9.1

Security Guide

Document Version: 1.0 (September 2024). BR32181

Conventions in this Document

Throughout this document, you will find tags that will indicate when the content is unique to a specific solution of the platform. These tags will include:

- [PMM] Content applies **only** to Print Management and Mobility
- [FM] Content applies **only** to Fleet Management

These tags will typically be found on section titles; however, they may be found at other points in the documentation.

NOTE: Any section not showing a tag should be assumed to follow the tags of any higher-level sections. If there are no tags on the section or on the higher-level sections then the section applies to **all** solutions.

For example, if you are implementing just Fleet Management, you will want to read sections tagged [FM] **and all untagged sections** (but you can skip the [PMM] tagged sections)

Table of Contents

1. Introduction

Xerox® Workplace Cloud (WC) is a workflow solution that connects a corporation mobile workforce to new productive ways of printer management, printing, and controlling user access to Xerox® Multifunction Printers (MFP). Customers can manage the configuration of their printers and ensure settings are consistent across their fleet of devices. Printing is easy and convenient from any mobile device without needing standard drivers and cables. This solution also supports Desktop Printing, allowing printing to a common queue with the ability to release jobs to any printer. This reduces waste from uncollected jobs and provides security for sensitive information, since jobs are only printed when the user is standing at the printer.

Purpose

The purpose of the Security Guide is to disclose information for Xerox® Workplace Cloud with respect to application security. Application security, in this context, is defined as how data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. This document describes design, functions, and features of the Xerox® Workplace Cloud relative to Information Assurance (IA) and the protection of customer sensitive information. Please note that the customer is responsible for the security of their network and the Xerox® Workplace Cloud does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Xerox® Workplace Suite 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 solution; 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

Workplace Cloud supports two different cloud solutions:

1. Printing and Print Management – Includes mobile and desktop printing, printer authentication / access and reporting.
2. Fleet Management – Which includes the ability to configure and manage settings on a set of devices.

Printing and Print Management

This workflow can be limited to just mobile printing, or it can be extended to include desktop printing, printer authentication (such as badge access) and advanced reporting.

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.

For desktop printing, the user installs the Workplace Cloud Client. The client will help with printer install and also manages communication with the Workplace Cloud solution. With this service in place, users can submit pull-print jobs as well as direct print jobs.

Workplace Cloud provides a Single Sign-On (SSO) infrastructure. The Apps in the Xerox App Gallery, which were 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 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 App
- Desktop Print Client (upload)

RELEASE METHODS

- Printing device UI (using EIP)
- Workplace App
- 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 App
- 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 simple or PIN) [Note: OKTA and HelloID only support the PIN option for manual credential entry. PINs can either be Card Numbers, values imported from LDAP / Azure AD / SAML, administrator managed values, or auto-generated PINs created by Workplace Cloud].
- Mobile Phone Unlock (using the Xerox® Workplace App for iOS or Android: NFC, QR Code, or Manual Code Entry)

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

Xerox® Workplace Cloud added the ability to support a Workplace Cloud Direct method of Printer Authentication. This feature makes use of the Azure IoT Hub capability to provide this functionality and is supported by Xerox AltaLink devices (A special firmware release is required).

XEROX® @PRINTBYXEROX

The Xerox® @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 Xerox® @PrintByXerox App. Below is a diagram outlining the different components used as part of this workflow.

COMPANY ACCOUNT IDENTITY PROVIDERS

The Xerox® Workplace Cloud solution allows the company account administrator to choose the identity provider that will be used by the users of that company when they need to identify and authenticate themselves to the solution. The supported identity providers are:

- Workplace Cloud Authentication – Email address and Workplace Cloud Password
- LDAP Authentication – Authentication against an Active Directory server using the LDAP protocol. Users enter their email, domain/user and password for LDAP.
- Azure AD – Authentication using Microsoft Azure Directory Services. Users enter their email address and their Azure AD password. This method may direct the user from Azure AD to an on-premise federated AD/LDAP server. [Based on OAUTH]
- OKTA – Authentication against OKTA. Users enter their email followed by OKTA credentials. [Based on OAUTH/OpenID]
- HelloID – Authentication using HelloID. Users enter their email, followed by HelloID credentials. [Based on OAUTH/OpenID]

Workplace Cloud supports the ability to enable two authentication methods for the same cloud company account. The supported identity providers are limited the combination of LDAP and Azure AD. One of these methods is designated as the primary method and the other the secondary. Users will authenticate to one or the other based on the administrator having mapped email addresses or email domains to the secondary method. If a user’s email address/domain is not mapped, they will use the primary authentication method. If their email address/domain is mapped, they will use the secondary authentication method.

Customers that are using an Identify Provider (IDP) that supports SAML 2.0, such as ADFS, may optionally use that provider to simplify the login process for the desktop client and the web portal. If the user is logged into their workstation, the solution will attempt to log the user into Workplace Cloud using that same identity. You must configure your IDP to trust the Workplace Cloud application as well as provide information for the solution to communicate with the IDP.

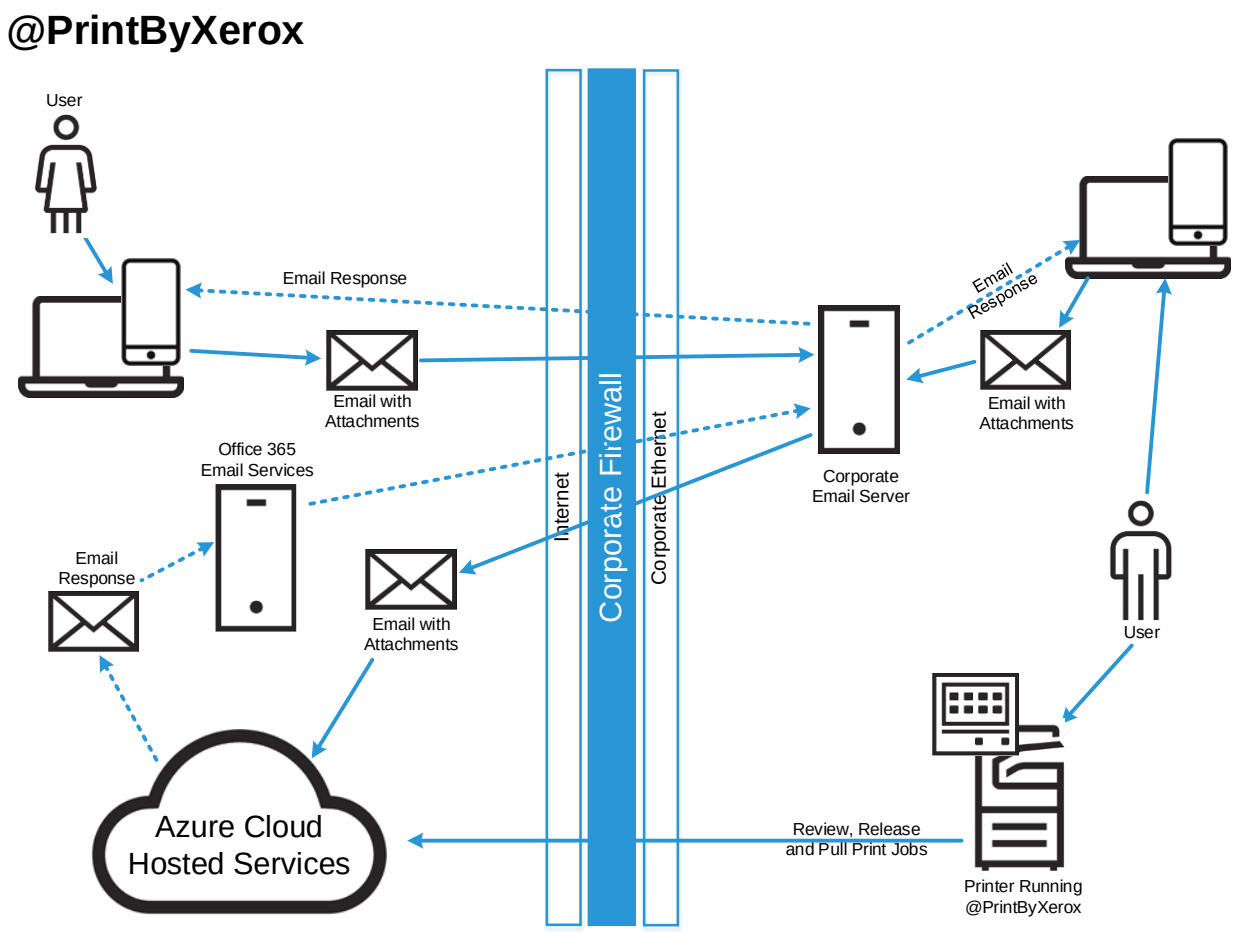


Figure 2–1: @PrintByXerox

Xerox® Workplace Cloud (with an Agent) [PMM]

The following diagram shows the system components used for the full Xerox® Workplace Cloud for Printing and Print Management solution using an Agent.

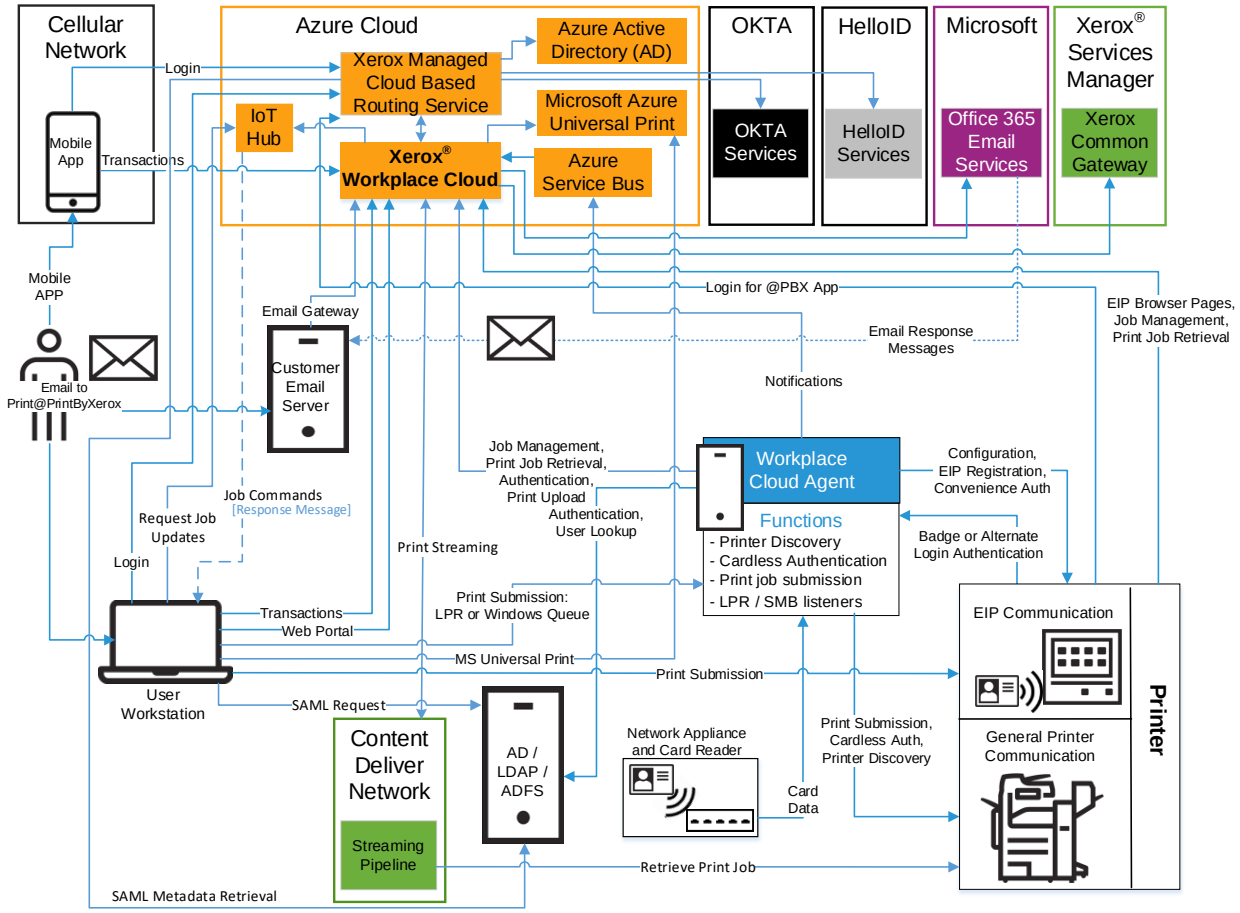


Figure 2–2: Xerox® Workplace Cloud with an Agent

XEROX® WORKPLACE CLOUD (WORKPLACE CLOUD DIRECT) [PMM]

The following diagram shows the system components used for the full Xerox® Workplace Cloud (Printing and Print Management) without an Agent.

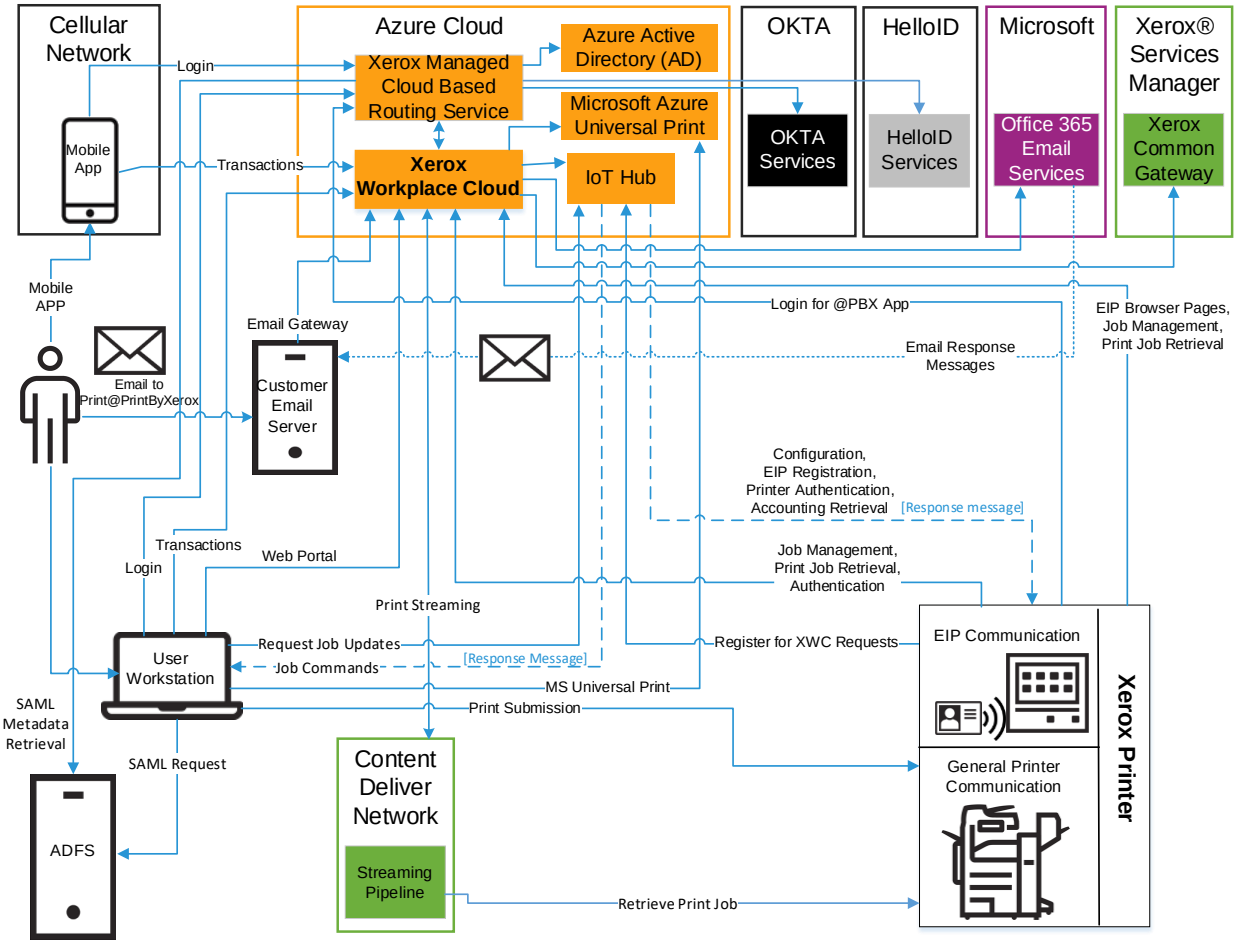


Figure 2–3: Xerox® Workplace Cloud (Workplace Cloud Direct)

DESCRIPTION OF SYSTEM COMPONENTS [PMM]

Component	Description
User	A user of the Xerox® Workplace Cloud.
Xerox® Workplace App	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.
Azure Service Bus	Used by Agent and Workplace Cloud to communicate through the customer's firewall. This is an outbound connection from the Agent to Azure. Workplace Cloud will use this path to send requests to the agent to perform actions (e.g., printer discovery).
Customer AD/LDAP/ADFS 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.
Azure IoT Hub	[Optional] Is used for the desktop client "Local Print Optimization" feature and for Workplace Cloud Direct Authentication and device management.
OKTA	[Optional] May be used for user authentication.
HelloID	[Optional] May be used for user authentication
Third-Party Public Print Provider	Allows print jobs to be submitted to Third-Party Providers.
Workplace Cloud Agent	On-premise application that runs on customer provided hardware, which supports Printer Discovery, Print transmission, Convenience Authentication and Network Accounting. Also provides LPR and Windows printer listening ports for systems that do not support a desktop client (e.g., Linux).
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 Workplace Cloud Client can be installed, which allows print jobs to be submitted to Workplace Cloud Printers from a PC or Mac. Also supports the Home Worker Print Tracker feature which monitors a user's print history, even when printing to printers not enabled in Workplace Cloud.
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.
Content Delivery Network (CDN)	Enabled high-bandwidth print job streaming from Azure to local printers in the customer environment.
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.
Microsoft Azure Universal Print	Microsoft's Universal Print infrastructure hosted in Azure.

Fleet Management

The Fleet Management functionality allows the administrator to define configuration sets, push these to a printer and monitor the configuration of devices to ensure settings do not change. Different configurations can be defined for different sets of printers. Customers that use the Fleet Management feature can link their account to Xerox® Services Manager. This allows the same set of devices being monitored using Xerox® Device Agent(s) to also be managed using Workplace Cloud Fleet Management.

XEROX® WORKPLACE CLOUD FLEET MANAGEMENT (WITH AN AGENT) [FM]

The following diagram shows the system components used for the Xerox® Workplace Cloud Fleet Management only functionality using an Agent.

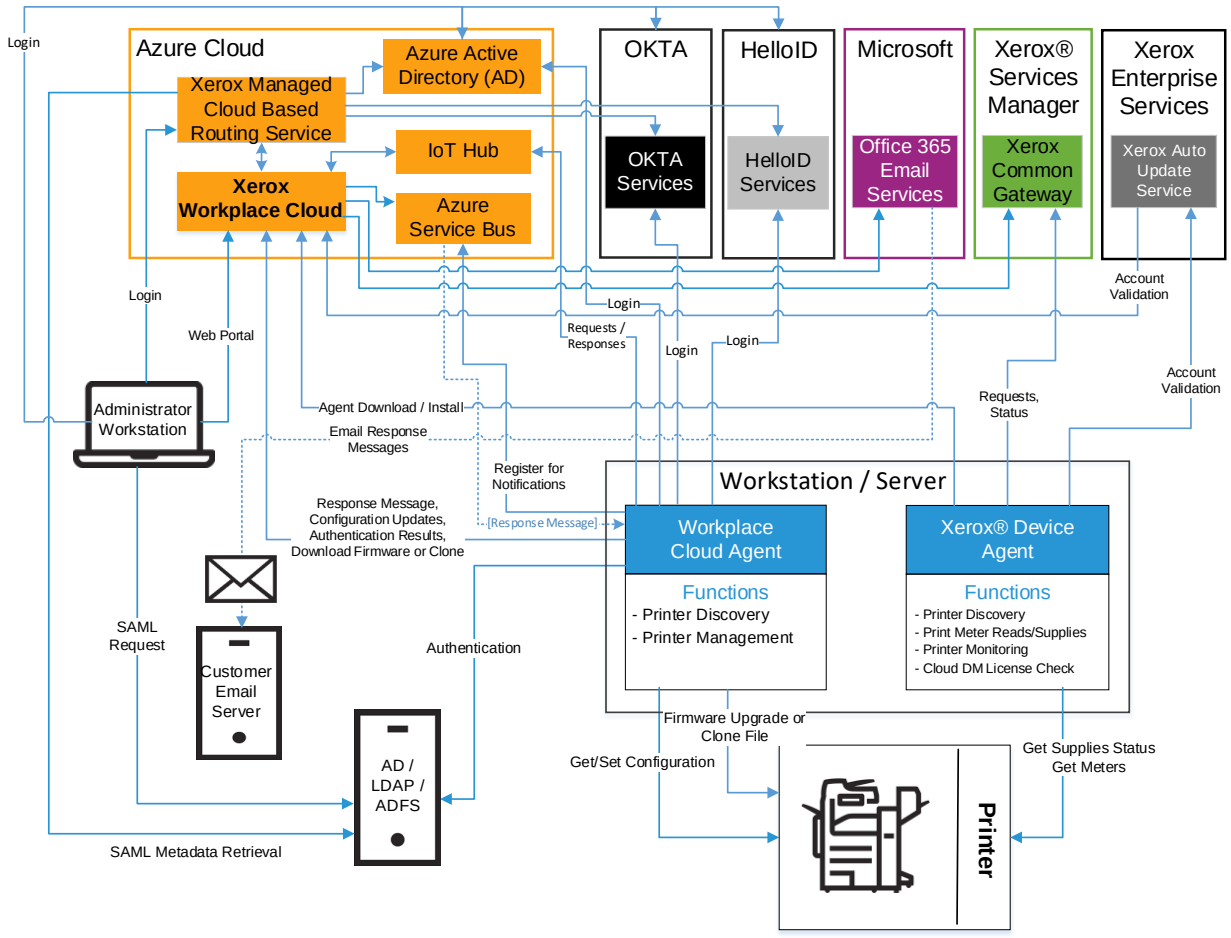


Figure 2–4: Xerox® Workplace Cloud Fleet Management – With an Agent

XEROX® WORKPLACE CLOUD FLEET MANAGEMENT (WORKPLACE CLOUD DIRECT) [FM]

The following diagram shows the system components used for the Xerox® Workplace Cloud Fleet Management only functionality without an Agent.

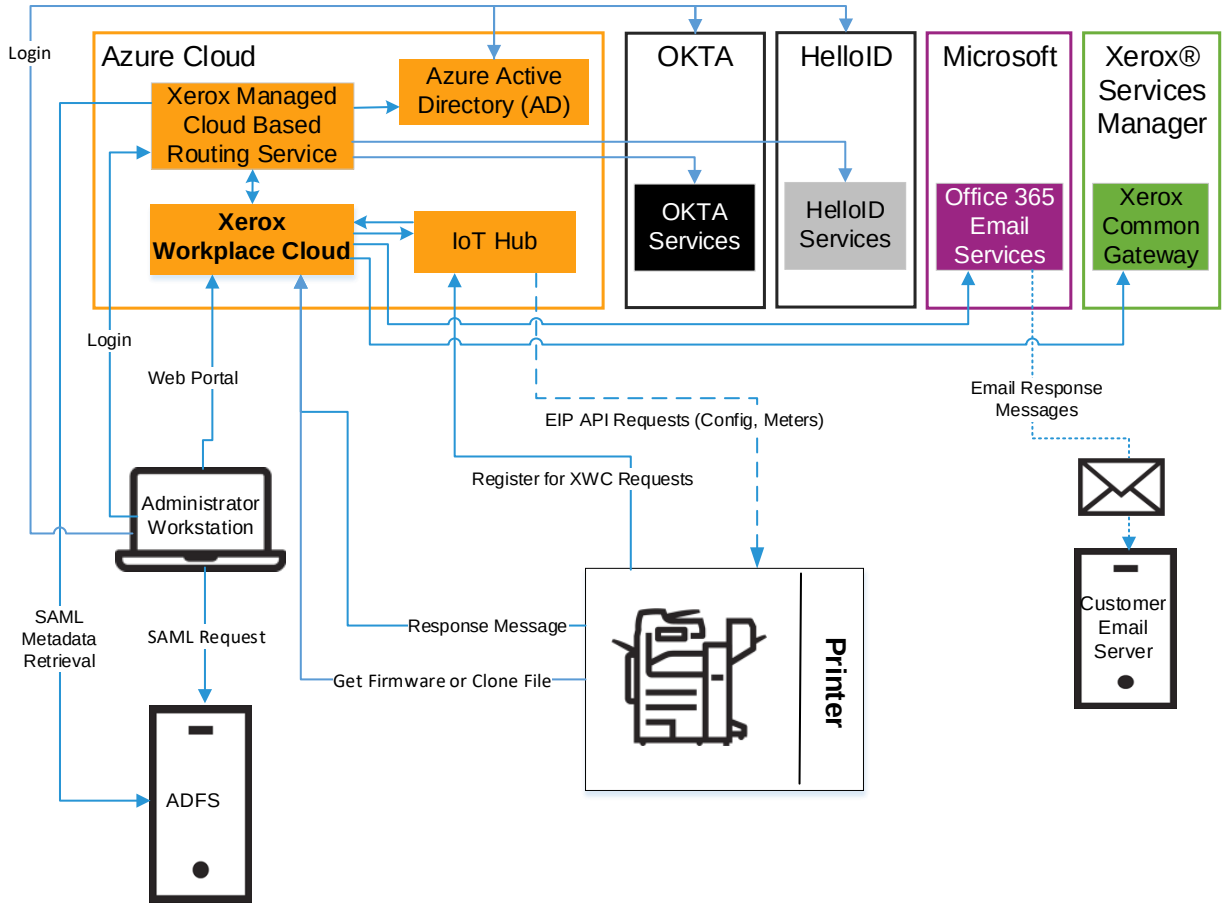


Figure 2–5: Xerox® Workplace Cloud Fleet Management – Workplace Cloud Direct

DESCRIPTION OF SYSTEM COMPONENTS [FM]

Component	Description
User	A user of the Xerox® Workplace Cloud.
Xerox® Workplace Cloud	The Azure hosted cloud service that provides the Workplace Cloud functionality.
Azure Service Bus	Used by Agent and Workplace Cloud to communicate through the customer's firewall. This is an outbound connection from the Agent to Azure. Workplace Cloud will use this path to send requests to the agent to perform actions (e.g., printer discovery).
Azure IoT Hub	Is used for Fleet Management requests sent to the Agent.
Workplace Cloud Agent	On-premise application that runs on customer provided hardware, which supports Printer Discovery, and Fleet Management.
Printer	Any printing device (Xerox or Non-Xerox) that is enabled to support Workplace Cloud.
Microsoft Office 365 Email Service	Used to send email responses back to users of Workplace Cloud.
Xerox® Services Manager	External Xerox application used in managed service accounts.
Xerox® Device Agent	External Xerox application for device monitoring that has been extended to support the installation of the WC Agent for managed print service environments using Xerox® Services Manager.
Xerox Auto Update Service	External Xerox application hosted by Xerox (internet accessible). Used to update the Device Agent.

3. System Architecture

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.

XEROX® WORKPLACE CLOUD VOLATILE MEMORY

Type (SRAM, DRAM, etc.)	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

XEROX® WORKPLACE CLOUD NON-VOLATILE MEMORY

Type (Flash, EEPROM, etc.)	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

Workplace Cloud Agent

WORKPLACE CLOUD AGENT VOLATILE MEMORY

Type (SRAM, DRAM, etc.)	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

WORKPLACE CLOUD AGENT NON-VOLATILE MEMORY

Type (Flash, EEPROM, etc.)	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 [PMM]

DESKTOP PRINT CLIENT VOLATILE MEMORY

Type (SRAM, DRAM, etc.)	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

DESKTOP PRINT CLIENT NON-VOLATILE MEMORY

Type (Flash, EEPROM, etc.)	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.

Xerox® Workplace App [PMM]

WORKPLACE APP VOLATILE MEMORY

Type (SRAM, DRAM, etc.)	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

WORKPLACE APP NON-VOLATILE MEMORY

Type (Flash, EEPROM, etc.)	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 APP [PMM]

The Xerox® Workplace App 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 Workplace App and Workplace Cloud.

The Xerox® Workplace 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 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. The entire SQL database is then encrypted using Microsoft Azure Transparent encryption.

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 stored in an encrypted format. Files stored in the cloud are encrypted using an AES encryption method. A symmetric key is generated to encrypt the file, and then the key is asymmetrically encrypted using a public certificate. Files uploaded from the Desktop Client are always encrypted using this method. File received from the Workplace App, Web Portal or via email, are encrypted upon receipt before being stored in the Cloud. More details on File Encryption can be found in the section titled “Document Encryption Summary”. This is found under the heading of “Additional Security Items”. This includes options for customers to provide their own keys used for encryption.

Access to these documents is only available to the following:

- The owner of the documents using the Xerox® Workplace App for preview.
- The owner of the documents using the Xerox® Workplace 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 3 days. If set to immediate, the document is deleted immediately after printing. If the document retention policy is set to 1 or 3 days, then after printing, the document is removed after once its total lifetime reaches the number of configured days. Therefore, documents stored in the solution shall never exceed 3 days.

Accounting information may be stored within 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 are 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.

Files encrypted using the Workplace Cloud default public certificate will be decrypted when they are retrieved by either the Agent or by the Printer if it using the EIP Pull Print API. The actual decryption is done by the Workplace Cloud backend system on the print file as it is streamed by the receiving endpoint. The actual decrypted file will never reside on any physical storage media in the cloud.

Files encrypted using a customer provided public certificate will always remain in an encrypted format when in the Cloud, including during upload and download. They can only be decrypted by the Agent that has the matching private certificate in its Windows certificate store. If you have a Xerox® AltaLink product (C80xx / B80xx) running release 103.xxx.020.23120 or later, the printer itself supports the ability to decrypt these print jobs without needing to be routed to the Agent. Both the private certificate and the CA root used to sign it must be installed on the printer in order to use the native decryption feature.

For the default file encryption method, the certificates used for encryption/decryption of documents are stored in the Azure storage account for the respective Azure site and are password protected.

Xerox® Workplace Cloud Printer Client Application Specific [PMM]

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 or use:

- The Print tab, allowing access to all printers enabled by the customer account administrator inclusive of printer name, printer location, and the printer's direct email submission email address.
- The Jobs tab, allowing the user to view uploaded documents (available for release), jobs that have been released and are being processed, jobs completed (transferred to the printer). For completed jobs, the information available includes document names, date of completion, and printer name of printer used to print the job.
- The user's profile – allowing them to view their email address, LDAP Username and Domain if applicable, User Groups to which they are a member, their badge/card number, their company code, user preferences (notifications, retention policy and print preferences). If SSO is enabled, the user can view which the Apps that they have stored login information, as well as having the ability to clear their stored SSO data.

Note: User Access does not apply when using the Fleet Management license, as only administrators would access the system in this scenario.

Xerox® Workplace Cloud Web Portal Administrator Access

All 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.
6. For the Fleet Management workflow, the administrator can view and manage the configuration profiles, configuration policies and compliance reports for their printers.

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 [PMM]

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. In addition, the entire SQL Azure database itself is encrypted using Microsoft Azure Transparent Encryption.

Xerox® Workplace Cloud – Workplace Cloud Authentication

The Workplace Cloud solution supports its own authentication mechanism called "Workplace Cloud Authentication". This authentication method is based on the user supplying their email address and then a Workplace Cloud password. User's must prove they own the email address and can set their own passwords. The password requirements are a minimum length of 8 characters with at least one uppercase and one numeric character. After authentication, the user is granted an

access token. For interfaces that store the access token (Workplace Cloud Client and Workplace App), the token lifetime can be configured for 1 to 365 days. Once the token expires, the user would be prompted to re-authenticate if they attempt to make use of the solution once the token has expired. Additionally, if the user changes their password (e.g., they forgot their password and set a new one), any existing tokens granted prior the password change would become invalid and the user would be required to re-authenticate through the given interface.

If a user incorrectly enters their Workplace Cloud Authentication password 4 times in a row, their user account will be locked. An email notification will be sent to all administrators of the cloud company when this occurs. The administrator may unlock the user account when this occurs. Alternatively, the user can use the "Reset Password" option on the Workplace Cloud web portal or on in the Xerox Workplace mobile app to reset their password, which will also unlock the user account.

LDAP/ADS/ADFS 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 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.

In addition to LDAP authentication, the Workplace Cloud solution supports the ability to use SAML to authentication users when using the Desktop Client and the Web Portal. This configuration is supported if using ADFS. For more details, refer to the SAML Connection section in the chapter titled "Additional Security Items".

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.

Authentication Methods

Workplace Cloud supports two different Azure AD authentication methods:

- **Simple** – Uses a multi-tenant Workplace Cloud application. This method requires no setup in the customer's Azure tenant. However, it does require that each user grant permission to the Xerox® Workplace Cloud application, allowing it to access the user's basic profile. It is possible for an Azure AD administrator to grant the same permission on behalf of all users of the Azure AD, allowing the Workplace Cloud to have access to their basic profile. Individual users will not be prompted. Users must be in the same Azure AD as the administrator. If more than one Azure AD is used, this step will need to be repeated for each Azure AD.
- **Advanced** – The customer may configure Azure domains which Xerox® Workplace Cloud would use as valid authentication domains for this solution. The advance method requires the administrator to create the following:

    1. Create an Azure Active Directory Web App in their Azure AD Tenant.
    2. Create an Azure Active Directory Native App in their Azure AD Tenant.
    3. Create an Azure AD Connection in Workplace Cloud:
        a. Specify the key information from the Azure AD Apps in steps #1 and #2.
        b. Define the email domains or addresses what will use this Azure AD Connection.
        c. Configure field mappings that will be retrieved from the user's profile and mapped to corresponding fields the User entry for Workplace Cloud.

For details on the creation of the Web and Native Apps, please see the Xerox Workplace Cloud Administration Guide.

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 Access Token and Refresh Token. Workplace Cloud will validate the Azure access token authenticity. The Azure AD Graph API is used to retrieve the fields from the user's profile when using advance mode only. The fields retrieved will be based on the mappings defined for the given Azure AD connection. The userPrincipalName (UPN) field for Simple Mode and the mapped Email field for Advanced mode are used to validate that the original email address passed into the Workplace Cloud system matches the value 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.

In most customer Azure tenants, the user's Email matches their UPN. However, this is not always true. The solution supports the scenario where a user can enter their UPN in the OAUTH screen instead of their Email (on the OAUTH login screen). In this scenario, the solution will examine the returned UPN from the token, and compare it to the initial email. If they differ, the solution will block the authentication request and it will send an email verification message to the Email that was provided. This is done to validate that the user owns the Email. The User must click on the

validation link in the email. The link is only valid for 15 minutes. If the user completes this process within that time, the UPN is linked to the Email address. In subsequent logins, the user will skip this validation step assuming they use the same Email and UPN values during login. The solution will pre-fill the stored UPN in the initial OAUTH screen so that the user does not need to re-type this each time.

When a user initially on-boards to Xerox Workplace Cloud for the first time, the solution will use the email address supplied as a hint to Azure AD when triggering the OAUTH login screen. This means the user's email will be pre-populated in the Azure AD login screen. There are cases where this email hint can prevent the user from successfully logging into Azure AD, such as the UPN sequence note in the previous paragraph. The administrator of the cloud company has the option to disable the hint during the first login attempt. Azure AD will then force the user to supply both the username and password options during the first login attempt when a user is on-boarding to Xerox Workplace Cloud. This option is only available for Azure AD simple mode. Once the user successfully logs in the first time, the solution will save off the UPN that was used for authentication against Azure and use this as a hint to pre-fill subsequent login attempts to the solution. This will simplify the login process for the end user.

Azure Token Details

The Workplace Cloud solution will store both the WC 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 App on the users' mobile device
- On the PC or Mac running the desktop Client

Note: Users can also log in to Workplace Cloud using the Web Portal (browser), the Agent, and the Printer Client (Xerox® @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 access token lifetime is 60-90 minutes and the Azure refresh token lifetime is 90 days. These access token lifetimes can 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 valid within the Azure AD system before updating the Workplace Cloud authentication token.

Channel Encryption

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

Alternate Login

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 (Email or UPN) and password. This information is passed from

the printer, to the Agent. Based on a customer cloud company configuration, the authentication request will either be handled by the Agent direct (meaning the Agent will call Azure AD to validate the credentials) or the Agent will pass the credentials to the Workplace Cloud which in turn will make the Azure AD validation request. The Alternate Login method with Azure AD uses the Resource Owner Password Credentials grant method in Microsoft Azure to authenticate the user. 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.

If the authentication request is coming from the Workplace Cloud solution hosted in Azure to Microsoft's Azure AD system, then this request will be treated as an external authentication request (a request originating outside the customer's internal network). The authentication request will always originate from one of the following IP addresses in Workplace Cloud:

- 51.132.11.42 (UK South)
- 20.77.169.0 (UK South)
- 20.254.146.7 (UK West)
- 20.254.160.214 (UK West)
- 20.107.195.73 (North Europe - Ireland)
- 4.245.240.91 (North Europe - Ireland)
- 104.47.154.99 (West Europe - Netherlands)
- 40.118.22.244 (West Europe - Netherlands)
- 52.171.33.21 (US South Central – Texas)
- 52.171.32.65 (US South Central – Texas)
- 40.116.98.63 (US North Central – Illinois)
- 172.214.183.129 (US North Central – Illinois)

Some customer's Azure tenant may impose restrictions or extra security requirements on such requests. A common requirement is to require the use of multi-factor authentication on all such external requests. The Microsoft API being used by Workplace Cloud to perform these non-OAUTH authentication requests does not support multi-factor authentication. If your customer environment enforces multi-factor authentication, then you should consider:

- Not enabling the "Allow Credential Access" function found under the Azure AD Simple and Advanced authentication methods.
- Bypass multi-factor authentication. The customer can add an exception for authentication requests coming from the small set of fixed IP addresses used by Workplace Cloud. [See previous paragraph].
- The authentication request can be forced to come from the Agent instead of the Workplace Cloud backend in Azure. This means the request is coming from an entity inside their customer network. Often times, this is enough to bypass the multi-factor authentication requirement. In some environments, an additional step may be needed, requiring the inclusion of the Agent IP Address to their Azure tenant bypass list for multi-factor authentication. The option to use the Agent to handle the authentication request can be configured from the Company Profile page of the Web Portal.
  [Note: if you are not able to isolate the IP Address of the Agent, the authentication request will appear to originate from the customer's internet gateway address. The gateway IP Address could then be added to the exception list. This would have the side effect of disabling multi-factor authentication from any request originating inside their corporate network.]

Badge / Card Auto-Registration

For those customers that have enabled the auto-registration process, the Workplace Cloud will use an email-based user validation process to register an unknown card. When a user scans an unknown card number, the solution will ask the user to supply their email address. An email will be sent to the user with a link. If the user selects the link, they will be taken to a login page where they must login to Azure AD using an OAUTH login page. If they successfully log in, their badge will be associated with their user account in Workplace Cloud. The badge registration link in the received email has a configurable lifetime of 10 to 240 minutes, with a default of 30 minutes. The administrator of the cloud company can set the link lifetime for their users. Once the lifetime is exceeded, the user may not use the link to complete the badge registration process. They will need to repeat the registration process again, starting by scanning their badge at an enabled printer.

Login Simplification

When using Azure AD authentication in conjunction with an on-premise ADFS (Active Directory Federated Services) system, it may be possible to simplify the logon process for the end user when using the Workplace Cloud desktop client and/or Web Portal interface.

For the desktop Client, the administrator must supply an email domain mapping specified in a configuration file used by the Workplace Cloud client. More information on this configuration can be found in the Xerox® Workplace Cloud Administration Guide.

For the Web Portal, the user must include the domain hint as part of the URL when accessing Workplace Cloud. The format is: *https://xwc.services.xerox.com/<email-domain>*

The solution uses the domain mapping to skip the email prompt and will route the authentication request directly to Azure using the provided domain as a hint to Azure AD. Azure will in turn redirect the request to the ADFS system. The ADFS system will check if the user is logged in locally and will communicate with the AD/Kerberos system to grant access.

This simplification also requires the client workstation to trust the account federation server. This can be done manually or using a Group Policy. Details can be found here.

This option is highly dependent upon the ADFS and Azure AD configuration. It requires the user to be logged into their Windows workstation with the same identity that is used to log into Workplace Cloud configured for Azure AD authentication. This option may not work in all environments.

OKTA

OKTA is an external identity management system and is not a deliverable of Workplace Cloud. It is possible to configure Workplace Cloud to use OKTA 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.

OKTA Setup

OKTA authentication can be enabled from the Company Profile page. To use OKTA with Workplace Cloud, the administrator will need to log into the OKTA web interface and add the Workplace Cloud application. There is a Wizard interface for Workplace Cloud that will step the administrator through this process.

Step 1: The administrator must set the Server Issuer URI:

e.g., https://{oktadomain}/oauth2/{authorizationserverid}

This value can be found on the OKTA web interface. In addition to the URI, the Workplace Cloud will require the following scopes, which should be listed under the OKTA authorization server:

- OpenID (Default = No; Metadata Publish = Yes)
- Profile (Default = No; Metadata Publish = Yes)
- Offline Access (Default = No; Metadata Publish = Yes)

Step 2: Create a '*Web Application'* within OKTA. Follow the instructions as outline in the Web Portal of Workplace Cloud.

Step 3: Create a '*Native Application* within OKTA*'*. Follow the instructions as outline in the Web Portal of Workplace Cloud.

Step 4: Create a '*Single Page Application* within OKTA*'*. Follow the instructions as outline in the Web Portal of Workplace Cloud.

OKTA User Login

When using OKTA, the user will supply their email address to Workplace Cloud, which is then used to look up the account to which they belong as well as the authentication mechanism used by that account. If using OKTA, the authentication mechanism relies upon OAUTH when entering credentials. 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 OKTA. The user will actually authenticate with the OKTA site. 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 OKTA Authentication Token and Refresh Token. Workplace Cloud will validate the OKTA authentication token authenticity. The solution will also attempt to validate the email address provided to XWC during the logon sequence using information obtained from OKTA. If it's not able to do that, then it will use an email validation step to confirm that the authenticated user owns the provided email. The User must click on the validation link in the email. The link is only valid for 15 minutes. If the user completes this process within that time, the OKTA Username is linked to the Email address. In subsequent logins, the user will skip this validation step assuming they use the same Email and OKTA Username values during login. The solution will pre-fill the stored Username in the initial OAUTH screen so that the user does not need to re-type this each time. After the authentication token and email are 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 OKTA Authentication token.

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

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

Note: Users can also log in to Workplace Cloud using the Web Portal (browser), the Agent and the Xerox® @PrintByXerox EIP App, however, the Workplace Cloud Authentication Token and OKTA 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 OKTA using the OKTA refresh token (assuming it has not expired). If successful, this results in a new OKTA authentication token and refresh token, which is then used to generate a new Workplace Cloud authentication token.

The OKTA authentication token lifetime and the refresh token lifetime come from OKTA, and is not something that is set or defined by Workplace Cloud. In general, the authentication token lifetime is very short, and therefore the Xerox authentication token lifetime is short. This forces the Workplace Cloud interfaces to frequently re-validate that the user is still valid within OKTA before updating the Workplace Cloud authentication token.

All OKTA communication between the given Workplace Cloud interface (Web Portal, Workplace Cloud Mobile App, Desktop Client, or Xerox® @PrintByXerox App) is done using HTTPS over port 443.

In order to support badge/card auto-registration, the Workplace Cloud will use an email-based user validation process to register an unknown card. When a user scans an unknown card number, the solution will ask the user to supply their email address. An email will be sent to the user with a link. If the user selects the link, they will be taken to a login page where they must login to OKTA using an OAUTH login page. If they successfully log in, their badge will be associated with their user account in Workplace Cloud. The badge registration link in the received email has a configurable lifetime of 10 to 240 minutes, with a default of 30 minutes. The administrator of the cloud company can set the link lifetime for their users. Once the lifetime is exceeded, the user may not use the link to complete the badge registration process. They will need to repeat the registration process again, starting by scanning their badge at an enabled printer.

HELLOID

HelloID is an external identity management system and is not a deliverable of Workplace Cloud. It is possible to configure Workplace Cloud to use HelloID 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.

HelloID Setup

HelloID authentication can be enabled from the Company Profile page. To use HelloID with Workplace Cloud, the administrator will need to log into the HelloID web interface and add the Workplace Cloud application. There is a pre-configured template for "Xerox Workplace Cloud" in the application catalog. No other changes are necessary by the user when creating the application. Once saved, the administrator will need to:

Step 1: Enter application details into Xerox Workplace Cloud

These values can be found on the HelloID web interface for the given application:

- Client ID
- Client Secret

Step 2: Enter the URL of the applications discovery document. The format of this is: *https://{tenant}.helloid.com/oauth2/v2/{Client ID}/.well-known/openid-configuration/*

HelloID User Login

When using HelloID, the user will supply their email address to Workplace Cloud, which is then used to look up the account to which they belong as well as the authentication mechanism used by that account. If using HelloID, the authentication mechanism relies upon OAUTH when entering credentials. 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 HelloID. The user will actually authenticate with the HelloID site. When using OAUTH, the 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 HelloID Authentication Token and Refresh Token. Workplace Cloud will validate the HelloID authentication token authenticity. The solution will also attempt to validate the email address provided to XWC during the logon sequence using information obtained from HelloID. If it's not able to do that, then it will use an email validation step to confirm that the authenticated user owns the provided email. The User must click on the validation link in the email. The link is only valid for 15 minutes. If the user completes this process within that time, the HelloID Username is linked to the Email address. In subsequent logins, the user will skip this validation step assuming they use the same Email and HelloID Username values during login. The solution will pre-fill the stored Username in the initial OAUTH screen so that the user does not need to re-type this each time. After the authentication token and email are 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 HelloID Authentication token.

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

- On the PC running the Workplace Cloud Client (Mac is not supported)

Note: Users can also log in to Workplace Cloud using the Web Portal (browser), the Agent and the Xerox® @PrintByXerox EIP App, however, the Workplace Cloud Authentication Token and HelloID 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 HelloID using the HelloID refresh token (assuming it has not expired). If successful, this results in a new HelloID authentication token and refresh token, which is then used to generate a new Workplace Cloud authentication token.

The HelloID authentication token lifetime and the refresh token lifetime come from HelloID, and is not something that is set or defined by Workplace Cloud. In general, the authentication token lifetime is very short, and therefore the Xerox authentication token lifetime is short. This forces the Workplace Cloud interfaces to frequently re-validate that the user is still valid within HelloID before updating the Workplace Cloud authentication token.

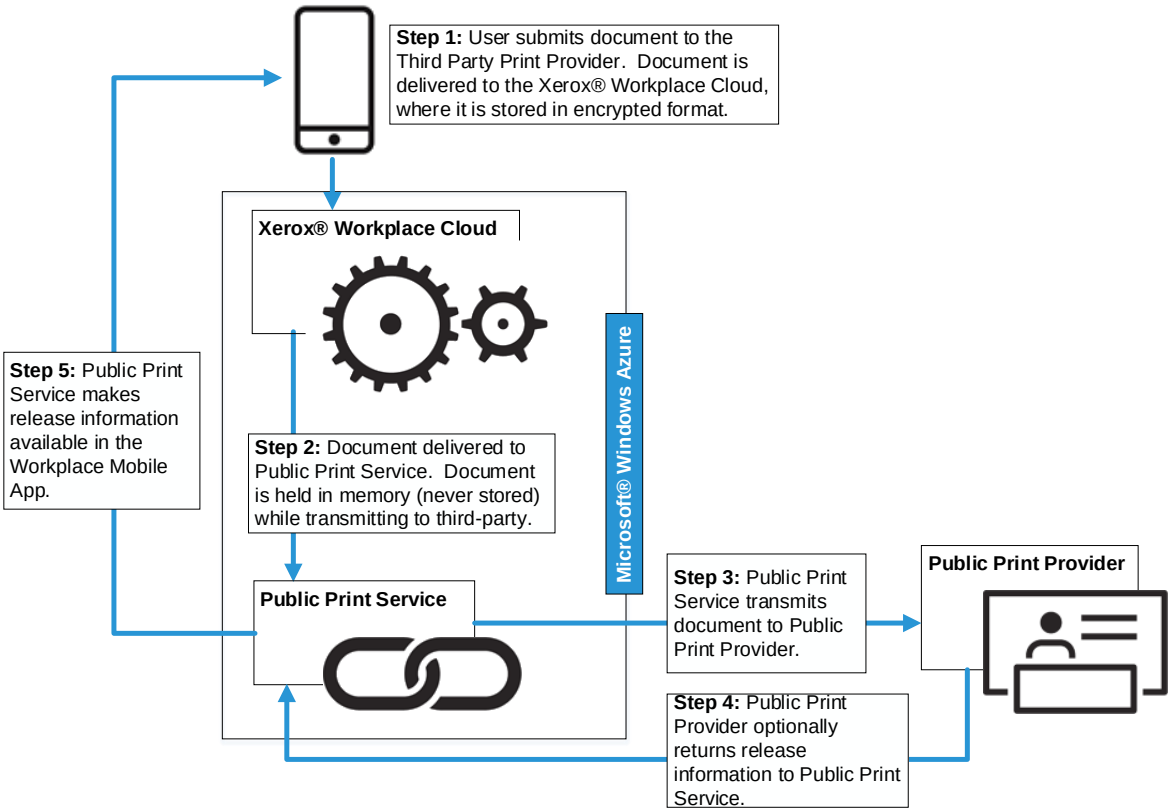
All HelloID communication between the given Workplace Cloud interface (Web Portal, Workplace Cloud Mobile App, Desktop Client, or Xerox® @PrintByXerox App) is done using HTTPS over port 443.

In order to support badge/card auto-registration, the Workplace Cloud will use an email-based user validation process to register an unknown card. When a user scans an unknown card number, the solution will ask the user to supply their email address. An email will be sent to the user with a link. If the user selects the link, they will be taken to a login page where they must login to HelloID using an OAUTH login page. If they successfully log in, their badge will be associated with their user account in Workplace Cloud. The badge registration link in the received email has a configurable

lifetime of 10 to 240 minutes, with a default of 30 minutes. The administrator of the cloud company can set the link lifetime for their users. Once the lifetime is exceeded, the user may not use the link to complete the badge registration process. They will need to repeat the registration process again, starting by scanning their badge at an enabled printer.

THIRD PARTY PUBLIC PRINT PROVIDER [PMM]

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



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 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 3-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 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 Public Print Service, which is co-located with the Workplace Cloud in Microsoft® Windows Azure.

Original documents are transmitted from the Public Print Service to the third-party public print provider in a secure manner. All communications to and from the Workplace Cloud and 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 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.

WORKPLACE CLOUD AGENT

The Workplace Cloud Agent has multiple functions based on the licensing and configuration of the account:

Print Management (Mobile Printing, Desktop Printing, Printer Authentication, Accounting):

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. If the customer is using the Desktop Enhanced Encryption feature with their own public and private keys using certificates, the Agent will decrypt the job after retrieving from Workplace Cloud and then send it to the printer via the configured print protocol for that device.
3. The Agent is responsible for performing 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.
7. The Agent can optionally cancel jobs that have been sent to a device and not yet printed when a user logs out of the printer or their session ends.
8. The Agent can support both an LPR and a Windows Shared Network (SMB) printer listening port to accept jobs from platforms not supported via the desktop client (Windows and Mac). In particular the primary client would be Linux, both other platforms could leverage this capability as well.

Fleet Management:

- The Agent is responsible for executing configuration policies on enabled printers. This includes querying the printer configuration based on the associated configuration profiles for various settings and if needed modifying the configuration to match the policy. It also includes checking firmware levels and applying necessary upgrades to the devices. The Agent can also push clone files to the device.
- The Agent performs device monitoring and alerting, such as when consumable like paper are needed.

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 users 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.

Agents may be 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.

Agents may be installed in a Load Balancer (LB) configuration where 2 or more Agents sit behind an HTTP/HTTPS load balancer. Printers that need to communicate with the Agent, can instead communicate with the configured LB name/address, and the LB will in turn pass this along to the one of the configured agents (testing to ensure the Agent is up). The Xerox Workplace Cloud Agent supports a LB probe / test endpoint that can be used by the LB to determine if the Agent system as well as the Agent application is up and running. The endpoint used for this testing is:

https://<agent-system>/ping

The LB should send an HTTP GET request to the above URL. If the response back is an HTTP 200 (ok), the LB can assume the Agent is available and requests can be directed to it. If any other response is received, such as an HTTP 500 (internal server error), then the LB should not treat the associated Agent as being available.

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 Workplace Cloud and the Workplace Cloud Agent, Communication between the Workplace Cloud Agent and the Printer, or Communication between LPR Clients and the Workplace Cloud Agent.

For details regarding Document Encryption using Desktop Enhanced Keys, refer to the section titled “Additional Security Items”.

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.

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. More details on printer authentication can be found in the “System Access” section of this document.

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® @PRINTBYXEROX APP [PMM]

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

1. Xerox® ConnectKey® 2.0i, Xerox® AltaLink®, and Xerox® VersaLink® Products – Support the Xerox® @PrintByXerox 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. Workplace Cloud Agent – The Workplace Cloud Agent installs the Xerox® @PrintByXerox 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 Xerox® @PrintByXerox App. 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 Xerox® @PrintByXerox 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 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 Xerox® @PrintByXerox App is the traditional Workplace Cloud environment, with a license and one or more Agents. The Agent will install the @PrintByXerox App 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 CLIENT) [PMM]

Users may install the Workplace Cloud Client on their Windows PC or Apple Mac. This application will install the administrator defined default print queues on the user's workstation. If using a PC, the client will install either the Xerox® Global Print Driver® (GPD) or an administrator uploaded custom driver for any Workplace Cloud enabled printers, as well as install and start a background service and a sys tray utility. If the Home Worker Print Tracker feature is enabled, the Workplace Cloud Client will install a print tracker v3 port monitor to all printers on the user's local workstation that are using v3 print drivers and which are not a Workplace Cloud enabled printer. The port

monitor is actually hidden (not visible in the Windows Printer Properties port page), and acts like shim, allowing the solution to intercept the job and collect information such as username, job name, print attributes like number of pages or color and if enabled it will also prompt for accounting information. This allows tracking of print jobs to printers not enabled in Workplace Cloud. The primary intent of this feature is to track print use on company owned workstations, even if the user is printing to devices that are outside of the normal solution workflows. The supported printer port types include:

- Standard TCPIP Port
- Local Port
- USB Port
- WSD Port

The background service is used to monitor for new job submissions using the installed Workplace Cloud Client and send these up to the cloud server. All communication between the Workplace Cloud 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 Workplace Cloud 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 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 workstation for future use. The expiration period of the authentication token is configurable by the cloud account administrator if using Workplace Cloud Authentication or LDAP, with a range of 1-365 days. When the authentication token expires or becomes invalid, the user will be re-prompted to supply their credentials. If using Azure AD, OKTA or HelloID, the token lifetime is typically very short, but the solution will attempt to refresh the token, if possible, when needed.

The Workplace Cloud Client makes use of the following locations to store user-based information:

- **%LOCALAPPDATA%\Xerox\XMPC** – This area is used to temporarily store jobs submitted to XWC that are being processed (e.g., job metadata collection) prior to notifying the cloud backend of the new job. This is also where locally stored follow-you jobs are retained while waiting for release at a printer and where jobs are temporarily stored during in order to be parsed if the Content Security feature is enabled.
- %**APPDATA%\Xerox\XMPC** – Contains data related to the specific user that should be persistent across reboots. This would include items such as the user's current access token, client configuration, account information and cached printer information for fallback printing.

Linked Company

By default, users are able to log in and out of the client using any registered cloud user account. This includes logging in with accounts from different Workplace Cloud companies. If the administrator for a Cloud company would like to restrict the client installed on a given workstation to only be used by users in that same company, they may supply a configuration option when installing the client on the user's workstation. It is assumed that the Desktop Client is being installed via an IT push mechanism such as SCCM. As part of that managed installation, the

appropriate configuration file can be included with the client installation package. Details on how to link a client can be found in the administration guide.

Print Job Path (for Workplace Cloud Printers)

Pull Print Jobs

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. Administrators may also provide an optional flag in the local configuration of the client which will allows them to override the account Local Print Optimization feature on a workstation-by-workstation basis. This gives the customer the flexibility to establish a company default for the majority of users, while using a different setting for a select few (e.g., a small branch office). To modify the configuration file, the user must have administrator rights on the workstation.

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.

Direct Print Jobs

When using the Desktop Client to submit jobs to a direct printer, the client will attempt to send the job directly to the printer. If the Desktop Client detects that the printer is reachable on the network it will push the job to the device using Raw IP (Port 9100), LPR (Port 515) or IPP over TLS (Port 443) based on the printer configuration. If the workstation is not able to reach the printer on the local network, the client will check the “Local Print Optimization” setting, and if it’s configured for local with cloud backup or cloud only, then the job will be transferred to the cloud and will be processed by an Agent in order to get it to the printer. The Agent will either directly pull down the job (via an HTTPS channel) and push it to the printer using the configured print protocol, or it will make a request to the printer using the EIP Pull Print API, instructing it to pull down the job (over an HTTPS channel). In the event that the printer cannot be reached locally, and the “Local Print Optimization” setting is set for local storage only, the client will fail the job as the solution will not be able transfer the job to the printer.

Print Job Encryption

The Desktop Client always encrypts print jobs that are uploaded to the Cloud. By default, the file is encrypted using a key from a public cert that is generated by Workplace Cloud. This is a common certificate across all tenants of the solution. If the customer prefers, they can upload their own certificate, which will be retrieved by the client application during it’s normal 24 configuration synch. The client will use the key from the public certificate, either the customer uploaded version (if available) or the default Workplace Cloud certificate, to encrypt the job before it is uploaded to Workplace Cloud. For additional details on Document Encryption using Keys, please refer to the section titled “Additional Security Items”.

Failover Support

In order to improve the user experience of the Workplace Cloud 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 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\Roaming\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 auto-detected 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 to 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.

Customers have the option to enable the ability for the desktop client to periodically check for an enforced offline mode based on querying DNS for a specific entry. Details on this capability are documented in the administration guide.

MICROSOFT OFFICE 365 – EMAIL SERVICE

Email responses sent to the end user are handled by 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).

All emails originating from Xerox® Workplace Cloud will come from one of the following email addresses:

- xmpc2@xerox.com
- XeroxMobilePrintCloud@xerox.com
- XeroxWorkplaceCloud@xerox.com
- XeroxWorkplaceCloud2@xerox.com
- XeroxWorkplaceCloud3@xerox.com
- XeroxWorkplaceCloud4@xerox.com
- XeroxWorkplaceCloud5@xerox.com
- XeroxWorkplaceCloud6@xerox.com

NETWORK APPLIANCE [PMM]

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/Conv3 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 optionally 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.) [PMM]
- Import Printers, Sites, and Printer/Site Mappings
- Export Printer Configuration, Meters, Supply Information and Status [FM]

Each of these actions with SM can be configured by the Administrator. There could be device specific limitations on the system for the respective action.

Export Job Data

- Requires the SM Account ID

Import Printers and Sites

- Requires the administrator to configure a SM Username and Password. (For a Xerox SM - connected account setup only, in standalone mode, once Xerox SM Export is enabled, Workplace Cloud does not get the respective data from SM)
- The SM user, at a minimum, must have Account Entity View and CustomerChargebackEntry Entity View permissions for successful import.

Exporting Printer Data

- Requires the SM Account ID

All communication between SM and Workplace Cloud will be over HTTPS (port 443) and occurs in the cloud. The production Xerox® Services Manager is hosted in the US. This is the default SM used by Xerox® Workplace Cloud for connected cloud accounts.

CONTENT DELIVERY NETWORK (CDN) [PMM]

Microsoft Azure supports the use of CDN as a mechanism to improve the distribution of data, enabling fast and localized downloads. Microsoft partners with different CDN providers, which have many geographically distributed servers with high-speed connections to Azure. Xerox makes use of Microsoft's Azure Front Door service to provide CDN functionality to Xerox Workplace

Cloud. When print ready jobs are made available for release at a printer, and that printer supports the EIP Pull Print API (e.g., ConnectKey, AltaLink and VersaLink devices), the @PBX app and the Agent can tell the printer to retrieve the print job from the Cloud (pulling the job down to the printer over HTTPS on port 443 and submitting it to print). The CDN endpoint is also supported by the Agent and Agent retrieved jobs. This print retrieval supports the CDN path to stream the job data from Azure blob storage in the Workplace Cloud through the Azure Front Door CDN server that is closest to the printer and then down to the printer. Caching is disabled on the Azure Front Door servers, however, while transitioning from the Azure<->Azure Front Door TLS connection to the Azure Front Door<->Customer TLS connection, the content needs to be decrypted and re-encrypted in memory due to the different certificates involved in the transfer. Customers who may be concerned with this data transfer can use the Desktop Enhanced Encryption feature under policies to ensure desktop jobs remain encrypted throughout the transfer or leave the feature disabled.

All communication between the printer and the CDN will be over HTTPS (port 443).

APP IN THE GALLERY [PMM]

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 [PMM]

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.

XEROX® DEVICE AGENT [FM]

The Xerox® Device Agent is not part of the Workplace Cloud solution. It's an application designed for managed print environments that wish to collect printer information such as configuration and meters and report them to Xerox® Services Manager (SM). The Device Agent has been modified to support easy installation of the Xerox® Workplace Cloud Agent. The Device Agent includes a small background service which will query the Workplace Cloud backend system to see if the Device Agent's associated SM account has been linked to a Workplace Cloud account. If the Workplace Cloud account exists and is linked to SM, the service will pull over and install the Workplace Cloud Agent on the same workstation / server, and will register it to use the linked WC/SM account. Communication between the Device Agent and the Workplace Cloud backend is via HTTPS (port 443).

Full details on the Device Agent and all of these features and functionality are not included in this document. Please refer to the Security & Evaluation Guide for the Xerox® Device Agent.

XEROX AUTO UPDATE SERVICE [FM]

The Xerox Auto Update Service is not part of the Workplace Cloud solution. It's a service hosted by Xerox on the internet that is used by the Device Agent for doing upgrades of the Device Agent. This service has been extended to support a specific request by the Device Agent to check if its associated SM account has been linked to a Workplace Cloud account. If the account is not linked, the Device Agent will not communicate with Workplace Cloud.

System Component Interfaces

COMMUNICATION BETWEEN THE WORKPLACE APP AND WORKPLACE CLOUD [PMM]

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

After authentication is complete, data is passed between the Xerox® Workplace App and the Workplace Cloud to enable the features of the service within the Xerox® Workplace 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 THE WORKPLACE APP AND THE CUSTOMER EMAIL SERVER [PMM]

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 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 WORKPLACE CLOUD AND THE 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, requests or notifications from Workplace Cloud to the Agent to perform certain functions are sent as response messages via the Azure Service Bus (used for both the Print Management and Fleet Management workflows) as well as via the Azure

IoT Hub interface (used for Fleet Management). Upon receiving notification of a new action, the Agent will call back to Workplace Cloud for the details of the request.

Requests might include discovering a printer, getting the current configuration of the printer, or modifying settings, sending a print job, performing an authentication request or retrieving accounting data from the printer.

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 CDN feature is enabled, the Agent will retrieve print jobs that are ready to be sent to a printer using the Azure Front Door endpoints. This helps speed up the download of large print jobs.

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 Cloud, 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 Xerox® @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 auto-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.

For scenarios where the XWC backend may be partially up, but not responding correctly, the administrator has the option to manually enable or force the agent into failover authentication mode. This can be done on the UI of the Agent itself. The resulting behavior would mimic that of auto failover method, however, there would be no 24-hour timeout period.

When using the Agent for Cloud Fleet Management, the Agent is responsible for downloading firmware releases and/or clone files and pushing these to the printer. All downloads are done

using HTTPS over TLS 1.2. These downloads make use of the Azure Front Door Content Delivery Network in order to maximize the download speed.

COMMUNICATION BETWEEN THE 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.

For newer Xerox devices that support the EIP Pull Print API, and which have access to the internet, the Agent will direct the printer (via the Pull Print API) to retrieve print jobs directly from the cloud. Otherwise, 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 Xerox® @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.

In conjunction with the Convenience Authentication feature, Workplace Cloud supports an optional security mode that will cancel any pending jobs released to the printer which have not yet completed printing. The assumption being that if the user session has ended, then the user is likely not at the printer. The feature is off by default, but when enabled, includes a configurable time period after logout or session termination is detected before any unfinished jobs will be cancelled. The time period is 30 to 3600 seconds. To use this capability, the Local Print Optimization setting must be disabled. This feature is only supported for desktop follow-you jobs submitted using a custom driver, and released using the Xerox® @PrintByXerox App to a VersaLink or AltaLink printer

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 the Workplace Cloud Administrator Guide.

COMMUNICATION BETWEEN THE WORKPLACE CLOUD AGENT AND A THIRD-PARTY PRINT QUEUE [PMM]

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 CLIENT AND WORKPLACE CLOUD [PMM]

When a user sends a job to a Xerox® Workplace Cloud enabled printer using the Desktop Client, the file is converted to Postscript and stored temporarily on the hard disk of the workstation. Similarly, if the Home Worker Print Tracker feature is enabled, the port monitor will intercept the job and store it temporarily on the hard disk of the workstation. The location of the stored files is dependent upon the user:

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

The Workplace Cloud 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 type of printer: Workplace Cloud or Home Worker Print Tracker. For a Workplace Cloud enable printer, the job will be processed 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\RetainedJobs

For a Home Worker Print Tracker job, the client will parse the job to determine the following set of information:

- Email Address of the user logged into the Workplace Cloud Client.
- Job Name
- Submission Time
- Printer Name
- Number of Copies
- Simplex or Duplex
- Number of Color Pages
- Number of Black & White Pages
- [OPTIONAL] Accounting Data (User ID / Account ID)
- Network User Name of the person logged onto the workstation (Domain\Username or Device\Username)
- [OPTIONAL] Matching Content Security Strings

This information will be uploaded to the Workplace Cloud and included in the Reporting data accessible by the account administrator.

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

The Workplace Cloud 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 workstation 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.

The Workplace Cloud Client will report a small set of information to the Workplace Cloud. This information is used for customer support as well as for planning purposes for future changes to the client functionality and supported operating systems. The set of information includes:

- Client ID
- Client Version

- Operating System Version
- .NET Version
- Email address of last logged in user
- Account ID of last logged in user
- IoT Hub Device ID
- Last Communication Date

COMMUNICATION BETWEEN THE WORKPLACE CLOUD CLIENT AND THE PRINTER [PMM]

If a workstation 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 when sending the print job. 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).

If the workstation is not able to reach the printer on the local network, the job will be transferred to the cloud and will be processed by an Agent in order to get it to the printer.

COMMUNICATION BETWEEN THE WORKPLACE CLOUD CLIENT AND THE AZURE IOT HUB [PMM]

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 through the IoT Hub and 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 Web Sockets 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 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 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 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 OR SHARED WINDOWS PRINT (SMB) CLIENTS AND THE WORKPLACE CLOUD AGENT [PMM]

The Agent supports the ability to enable both an LPR listening port and a Network Shared Printer (SMB) port, which can accept incoming print jobs from LPR Clients and SMB based Clients (e.g., Linux) that may not support the ability to print to the shared network pull queues used by Microsoft Windows workstations. This feature might be used by Linux workstations or possibly even mainframes. By default, this interface uses LPR over port 515, but the port is configurable and SMB is over port 445. [Note: jobs submitted to the Agent via LPR or a Shared Windows Queue are never stored locally on the Agent. They are always uploaded to the Workplace Cloud. This applies to both follow-you jobs as well as LPR "direct" jobs (where the queue name in the LPR protocol matches the IP Address or Friendly name of a printer enabled in XWC). The *Local Print Optimization* feature does NOT apply to jobs received by the Agent over LPR or a Shared Windows Network Printer.]

COMMUNICATION BETWEEN THE APP FROM THE GALLERY, THE APP SERVER, AND WORKPLACE CLOUD [PMM]

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 a key size of 1024. Additional details on SSO can be found in Chapter 7 Single Sign-On of this document.

COMMUNICATION BETWEEN WORKPLACE CLOUD AND THE PRINTER

@PrintByXerox App [PMM]

For Xerox devices that support the EIP browser and EIP Apps, the Xerox® @PrintByXerox App will pull page content to be displayed in the browser of the printer UI panel from Workplace Cloud. This includes all page content, authentication, available jobs, job selection and job status. All communication is via HTTPS over Port 443.

Printing [PMM]

For newer Xerox devices that support the EIP Pull Print API (ConnectKey, AltaLink & VersaLink), the printer can be directed to retrieve print jobs directly from the cloud (either from Azure blob storage or if CDN is enabled, then through an Azure Front Door server). Job release from the Xerox® @PrintByXerox App always uses this method to get print jobs to devices which support this API. It is also possible to enable the Agent to support this print path (again for printers supporting this API). The Agent would direct the printer to pull the print job instead of routing the job through an Agent and then to the printer. This will decrease network load as well as load on the Agent itself.

Establish IoT Hub Connection

Workplace Cloud Direct Authentication and/or Device Management is supported primarily via the Azure IoT Hub. The establishment of the IoT Hub connection requires the printer to call the Workplace Cloud backend in Azure to get the IoT Hub connection string. This connection string is specific for each device based on printer unique information. The printer must pass this information to WC using a proprietary API, which is protected via certificate validation. This call is over HTTPS using port 443.

Workplace Cloud Direct Authentication [PMM]

In regards to Workplace Cloud Direct Authentication, the EIP Convenience Authentication API requires the printer to make some of the authentication API requests directly from the Printer to the Workplace Cloud backend system hosted in Azure. These calls are initiated from the printer (e.g., initiate a new session as a result of a card swipe or selecting the Alternate Login button). This communication path uses HTTPS over port 443.

EIP Response Messages

Response messages to EIP API requests coming through the IoT Hub are sent directly from the printer to Workplace Cloud via web service APIs. These message use HTTPS over port 443.

Firmware Updates and Clone Files [FM]

For devices using the Cloud Direct feature, the cloud backend can instruct the printer to pull down and submit both firmware releases and/or clone files using the EIP Pull Print API. These files are always pulled down from a Workplace Storage account located in one of the supported regions (EU, UK, US) using and HTTPS request over port 443. These storage accounts always use the Azure Front Door CDN interface to maximize file download speed.

COMMUNICATION BETWEEN THE PRINTER AND THE IOT HUB

After the printer receives the IoT Hub connection string for Workplace Cloud, the printer directly calls the Azure IoT Hub APIs to create an IoT Hub connection. This call is over AMPQ using port 5671 (with HTTPS over 443 as a fallback). The IoT Hub channel is an out-bound connection from the printer to the IoT Hub, which then allows responses (new requests) to be send back down through this channel. These are response messages from a networking perspective, not new inbound connections. The WC will use this connection path to the printer for authentication, configuration, accounting and device management in a Workplace Cloud Direct environment.

COMMUNICATION BETWEEN THE XEROX® DEVICE AGENT AND WORKPLACE CLOUD [FM]

The Device Agent includes a small background service which will query the Auto Update Service to see if the Device Agent's associated SM account has been linked to a Workplace Cloud account. If the account exists and is linked, the service will pull over and install the Workplace Cloud Agent on the same workstation / server, and will register it to use the linked WC/SM account. Communication between the Device Agent and the Workplace Cloud backend is via HTTPS (port 443).

COMMUNICATION BETWEEN THE XEROX® DEVICE AGENT AND THE XEROX AUTO UPDATE SERVICE [FM]

The Device Agent includes a small background service which will query the Auto Update Service hosted by Xerox to see if the Device Agent's associated SM account has been linked to a Workplace Cloud account. If the account is linked, then the Device Manager will then call the Workplace Cloud to download the Cloud Agent installer. Communication between the Device Agent and the Auto Update Service is via HTTPS (port 443).

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.

XEROX® WORKPLACE APP PORTS [PMM]

Protocol	Transport and Port Value	Use	Option	Component	Direction
HTTPS using TLS	TCP 443	Authentication, Job / Printer Listing, Initiate Print Conversion	Non-configurable	App to WS Service	Out
HTTPS using TLS	TCP 443	Authentication	Non-configurable	App to Azure AD, OKTA or HelloID	Out
IPP	TCP 631	iOS Native Print Submission	Non-configurable	App to Agent	Out
HTTPS using TLS	TCP 443	Authentication (for Chrome SSO)	Non-configurable	App to Google	Out

WORKPLACE CLOUD AGENT PORTS

Protocol	Transport and Port Value	Use	Option	Component	Direction
HTTPS using TLS	TCP 443	Retrieval of configuration, sending printer info, retrieval of print jobs, retrieval of firmware releases or clone files, authentication, print job upload for LPR/SMB listener ports.	Non-configurable	Agent to Workplace Cloud	Out
Raw IP	TCP 9100	[PMM] Print Submission [FM] Firmware Update	Configurable	Agent to Printer	Out
HTTPS	TCP 443	Azure Service Bus (with application-level encryption)	Non-configurable	Agent to Workplace Cloud	Out
LPR	TCP 515	[PMM] Print Submission [FM] Firmware Update	Configurable	Agent to Printer or to Print Queue	Out
HTTPS using TLS	TCP 443	[PMM] Retrieval of print job from CDN	Non-configurable	Agent to CDN (Azure Front Door)	Out

IPP over SSL	TCP 443	[PMM] Print Submission	Non-configurable	Agent to Printer	Out
LDAP	TCP 389	[PMM] Authentication	Non-configurable	Agent to ADS Server	Out
LDAP over SSL	TCP 636	[PMM] Authentication	Non-configurable	Agent to ADS Server	Out
HTTPS using TLS	TCP 443	[PMM] Printer Authentication, EIP Registration, Accounting Data Configuration and Retrieval, Pull Print Request, Job Management, Clone File Install	Non-configurable	Agent to Printer	Out
HTTP	TCP 80	Printer capabilities, configuration [FM] Clone File Install (fallback if HTTPS not available)	Non-configurable	Agent to Printer	Out
HTTPS using TLS	TCP 443	[PMM] Printer Authentication	Non-configurable	Printer to Agent	In
HTTPS using TLS	TCP 443	[PMM] Authentication	Non-configurable	Agent to Azure AD, OKTA or HelloID	Out
SNMP	UDP 161	Printer Discovery, Configuration	Non-configurable	Agent to Printer	Out
LPR	TCP 515	[PMM] Incoming Print Queue – Receive prints from LPR Clients	Configurable	LPR Client to Agent	In
Windows Shared Printer (SMB)	TCP 445	[PMM] Incoming Print Queue – Receive prints from SMB Clients Note: there may be additional ports needed for MS Printing. Refer to: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements	Configurable	SMB Client to Agent	In
HTTPS using TLS	TCP 443	[PMM] Single Sign-On Requests / Responses	Non-configurable	Printer ←→ Agent	In/Out
AMQP Web Sockets	TCP 443	[FM] Azure IoT Hub connection for Fleet Management requests	Non-configurable	Agent to Azure IoT Hub	Out
IPP	TCP 631	[PMM] iOS Native Print Submission	Non-configurable	iOS device to Agent	In
HTTPS using TLS	TCP 443	Agent Load Balancer Query / Test	Non-configurable	Load Balancer	In
Windows File Sharing (SMB)	TCP 445	Agent import from Windows Share of CSV for user import and deletion. Note: there may be additional ports needed for Windows File Sharing. Refer to: https://docs.microsoft.com/en-	Non-configurable	Agent to File Share	Out

		us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements			

XEROX® @PRINTBYXEROX APP PORTS [PMM]

Protocol	Transport and Port Value	Use	Option	Component	Direction
HTTPS using TLS	TCP 443	Retrieval of EIP Browser pages for display on the UI. Authentication, Job Listing, Initiate Print Conversion	Non-configurable	@PBX to Workplace Cloud	Out
HTTPS using TLS	TCP 443	Authentication	Non-configurable	@PBX to Azure AD, OKTA or HelloID	Out
HTTPS using TLS	TCP 443	QR Code icon retrieval	Non-configurable	@PBX to Azure Blob Storage	Out

PRINTER PORTS

Protocol	Transport and Port Value	Use	Option	Component	Direction
SNMP	UDP 161	Printer Discovery, Configuration	Non-configurable	Cloud Agent to Printer	In
LPR	TCP 515	[PMM] Incoming Print Queue – Receive prints from LPR Clients [FM] Firmware updates	Configurable	LPR Client to Cloud Agent	In
Raw IP	TCP 9100	[PMM] Print Submission [FM] Firmware updates	Configurable	Cloud Agent to Printer	In
IPP over SSL	TCP 443	[PMM] Print Submission	Non-configurable	Cloud Agent to Printer	In
HTTPS using TLS	TCP 443	EIP Registration, Initiate Pull Print, Configuration, Job Management, Clone File Install	Non-configurable	Cloud Agent to Printer	In
HTTP	TCP 80	Printer capabilities, configuration [FM] Clone file install (fallback if	Non-configurable	Agent to Printer	In

		HTTPS not available)			
HTTPS using TLS	TCP 443	Pull Print Request, (Azure) IoT Hub Connection Request and Response Messages to requests sent over the IoT Hub, Firmware and Clone file download	Non-configurable	Printer to Workplace Cloud	Out
HTTPS using TLS	TCP 443	[PMM] Pull Print Request to CDN	Non-configurable	Printer to CDN (Azure Front Door)	Out
HTTPS using TLS	TCP 443	[PMM] Printer Authentication (Agent)	Non-configurable	Printer to/from Cloud Agent	In/Out
AMQP (with HTTPS using TLS as a fallback)	TCP 5671 (TCP 443 fallback)	Azure IoT Hub connection for Workplace Cloud Direct requests.	Non-configurable	Printer to Azure IoT Hub	Out
SNMP	UDP 161	[FM] Printer Discovery, Meter Reads, Monitoring	Non-configurable	Device Agent to Printer	In
HTTPS using TLS	TCP 443	[PPM] Single Sign-On for Gallery Apps	Non-configurable	Print to Workplace Cloud portal	Out

WORKPLACE CLOUD CLIENT PORTS [PMM]

Protocol	Transport and Port Value	Use	Option	Component	Direction
HTTPS using TLS	TCP 443	Printer Configuration, Driver Download, Print Submission, Home Worker Print Tracker job details	Non-configurable	Client to Workplace Cloud	Out
HTTPS using TLS	TCP 443	Authentication	Non-configurable	Client to Azure AD, OKTA or HelloID	Out
AMQP Web Sockets	TCP 443	Print job release notification	Non-configurable	Client (Windows PC) to Azure IoT Hub	Out

LPR	TCP 515	Print Submission	Configurable	Client (Windows PC) to Printer	Out
Raw IP	TCP 9100	Print Submission	Configurable	Client (Windows PC) to Printer	Out
IPP over SSL	TCP 443	Print Submission	Non-configurable	Client (Windows PC) to Printer	Out
SAML	TCP 443	SAML 2.0 Authentication	Non-configurable	Client (Windows PC) to IDP (ADFS)	Out

NETWORK APPLIANCE PORTS [PMM]

Protocol	Transport and Port Value	Use	Option	Component	Direction
Raw	TCP 7778	Receive Card Swipe Data from Elatec TCPConv	Configurable	Network Appliance to Agent	Out
Raw	TCP 7777	Receive Card Swipe Data from Elatec TCPConv2 / Conv3	Configurable	Network Appliance to Agent	Out
Raw	TCP 2001	Receive Card Swipe Data from RFIdeas Ethernet 241	Configurable	Network Appliance to Agent	Out

XEROX® DEVICE AGENT PORTS [FM]

Protocol	Transport and Port Value	Use	Option	Component	Direction
HTTPS using TLS	TCP 443	Agent Installer Download	Non-configurable	Device Agent to Workplace Cloud	Out
SNMP	UDP 161	Printer Discovery, Meter Reads, Monitoring	Non-configurable	Device Agent to Printer	Out
HTTPS using TLS	TCP 443	Command Requests, Printer Configuration and Monitoring Information, Configuration, Status	Non-configurable	Device Agent to Services Manager	Out

HTTPS using TLS	TCP 443	Account Validation	Non-configurable	Device Agent to Xerox Auto Update Service	Out

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.

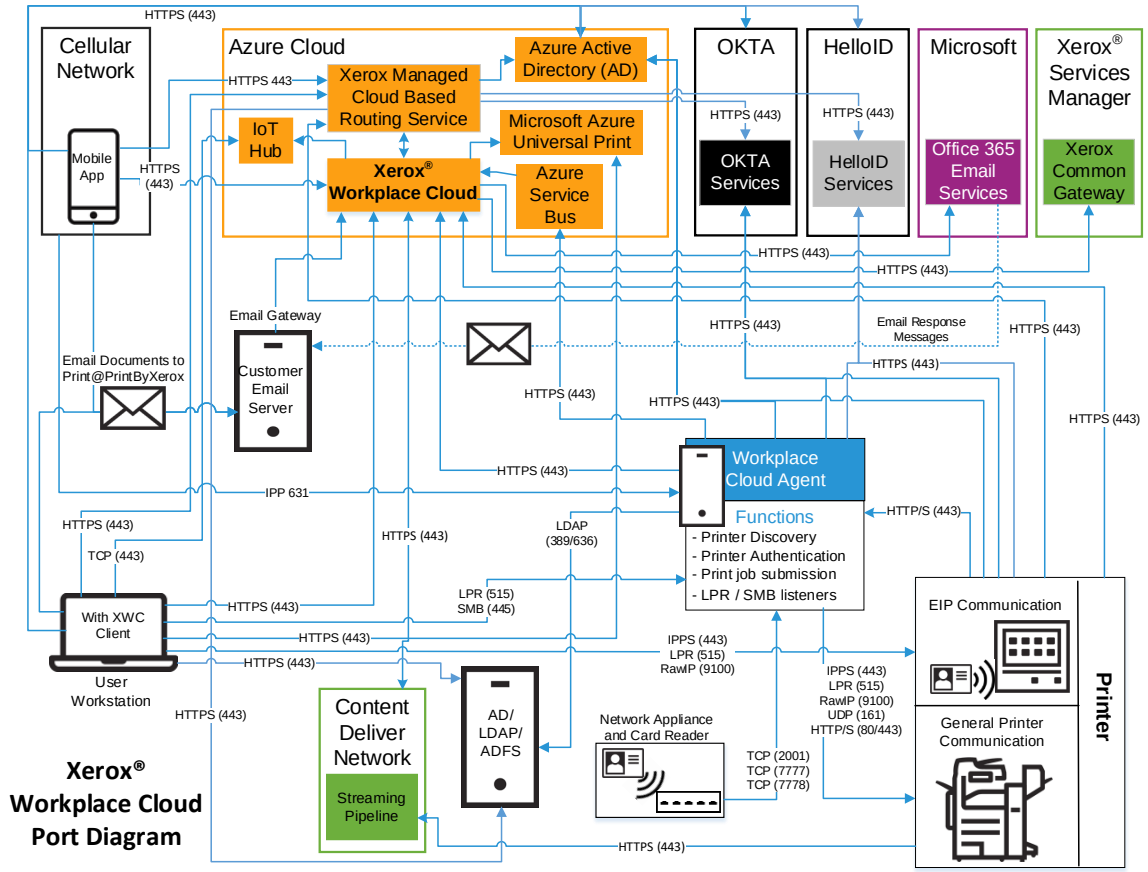
Protocol	Default Use Port Value	Use	Direction
HTTPS	TCP 443	Authentication	In
Raw	TCP 7778	Receive Card Swipe Data from Elatec TCP Conv	In
Raw	TCP 7777	Receive Card Swipe Data from Elatec TCP Conv2 / Conv3	In
Raw	TCP 2001	Receive Card Swipe Data from RFIdeas Ethernet 241	In

Port Diagrams

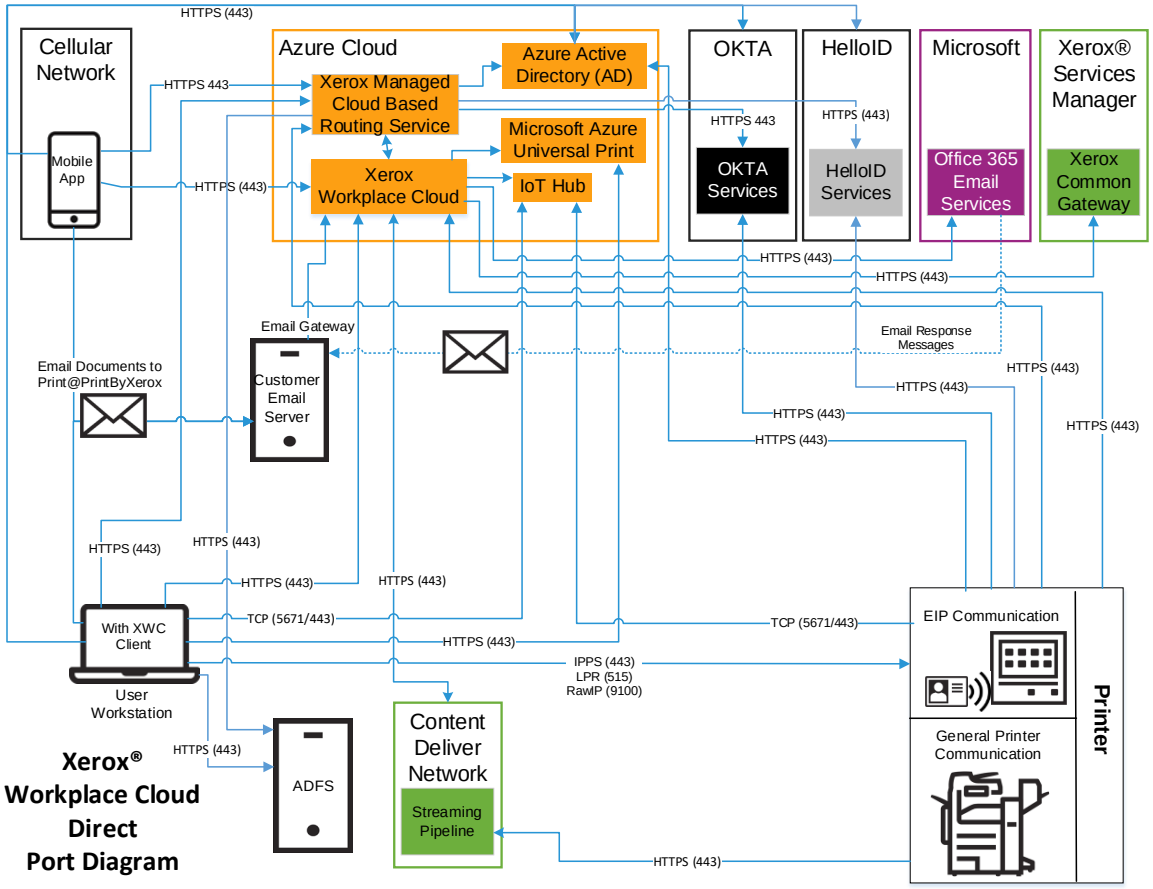
The following diagram gives a pictorial representation of the components and ports being used to facilitate communication.

PRINT MANAGEMENT PORT DIAGRAM [PMM]

Print Management Port Diagram (with an Agent)

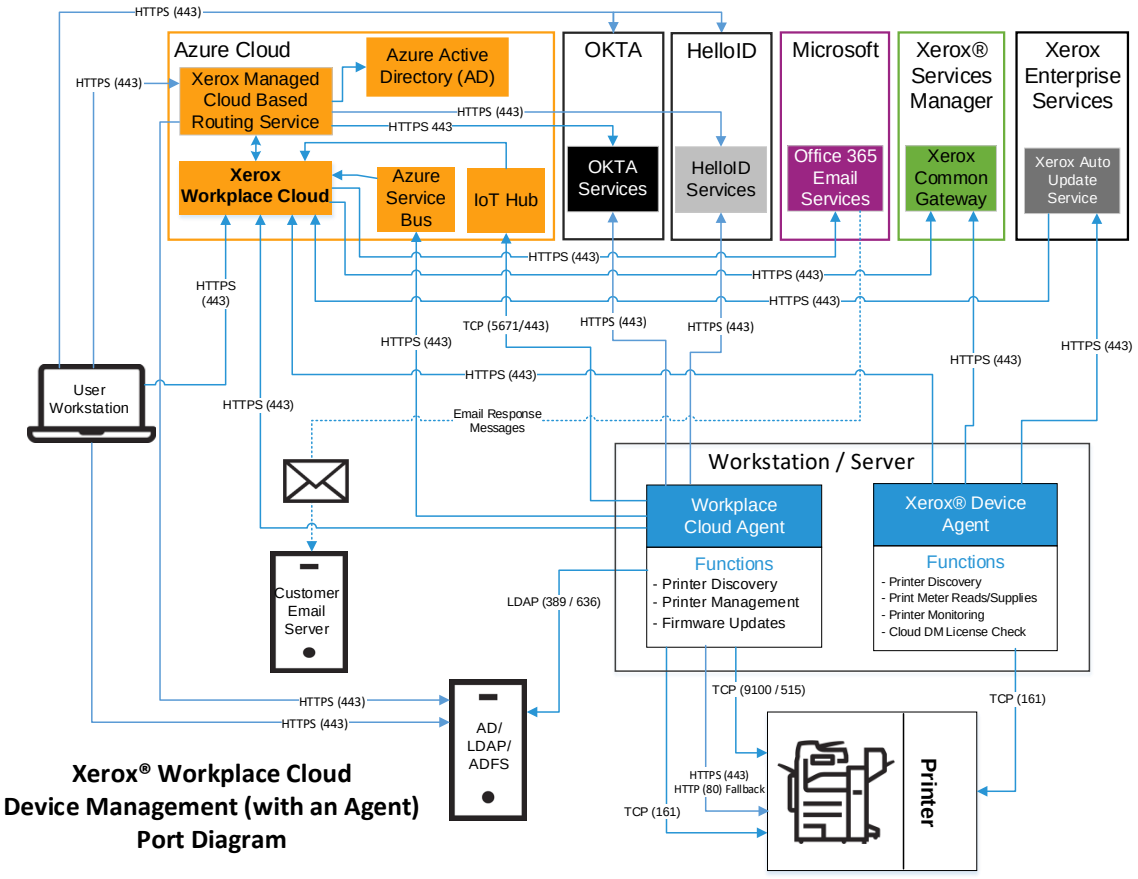


Print Management Port Diagram (Workplace Cloud Direct)

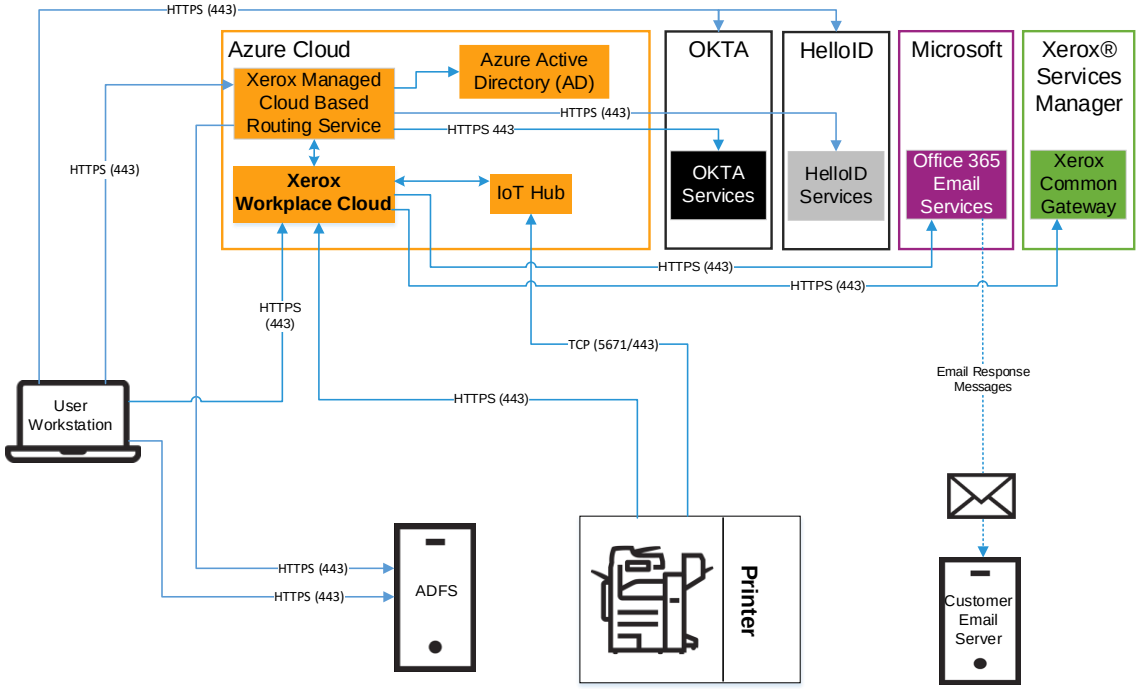


FLEET MANAGEMENT PORT DIAGRAM [FM]

Fleet Management Port Diagram (with an Agent)



Fleet Management Port Diagram (Workplace Cloud Direct)



Xerox® Workplace Cloud
Fleet Management
(Cloud Direct)
Port Diagram

6. System Access

Cloud Company

In order to use Xerox® Workplace Cloud, someone must initially create a company account. This person will become the initial administrator and owner of the solution. This is a one-time process. After creation, additional administrators may be created as well as updating the contact information for the primary person response for the solution.

During creation time of the Cloud Company, the user must select the location where their company information will be stored in the Azure SQL database. There are three different options, which align with the Azure deployment sites used for Xerox® Workplace Cloud. The choices are either:

- UK
- EU
- US

Company information in this case includes items such as company details, sites, user details, printer information, company account configuration and reporting data.

In addition to selecting the Azure deployment location for the database, the administrator must also select the storage location for submitted jobs that are stored in the cloud. The options supported are:

- Performance (based on the location of the submitter)
- EU
- UK
- US

The EU, UK or US options for document storage would limit submitted jobs to only being stored in the respective location. The choice of the Performance option will use geo-location logic to determine the location of the submitting user (based on DNS) and then store the job in the Azure deployment region aligned with that location: EU, UK or US.

Selection of the storage location for your company information and document storage are specific to data at rest within the Workplace Cloud solution. All communication, between on-site components (e.g. Print, Agent, Desktop Client) and the Workplace Cloud solution hosted in Azure, will use DNS based geo-location logic and the Azure Traffic Manager to determine which Azure site is used to handle the communication traffic for any given request. For example:

- Cloud Company X created with EU designated as the location for company information and document storage.
- A user in Company X that submits a print request while travelling in the US would have their data pass through the US compute nodes before coming to rest in the EU database/storage accounts. (Assumes the DNS server used to revolve the Workplace Cloud endpoint is located in the US).
- A user in Company X that submits a print request from within the EU would have their data pass through the EU compute nodes before coming to rest in the EU database/storage accounts. (Assumes the DNS server used to revolve the Workplace Cloud endpoint is located in the EU).

User Accounts

Xerox® Workplace Cloud is a multi-tenant solution based on a set of registered companies. Each company is assigned a unique company code. This code is used to link a user to one of these registered companies. Users of Workplace Cloud can only be actively linked (often referred to as "homed") to one company. As part of the initial user account creation, they can supply the company code to ensure they are homed to the correct company. It is also possible (upon request) to associate an email domain or list of domains to a registered company, so that user's on-boarding for the first time will not need to provide a company code and will automatically get homed to the correct company. As part of the user account creation, the user will need to authenticate via the configured mechanism of the home company (Cloud Authentication, LDAP, Azure AD, OKTA or HelloID).

Workplace Cloud does allow users to change their home account using the Web Portal or the Workplace App. The login interface provides an option to change companies, and when selected, prompts the user to supply the company code of the new company that they wish to be associated with. When a user changes companies (re-homes their account), any jobs they had previously upload to the system (which are based on the user being homed to the old company) will be deleted and no longer available to be released.

Users that on-board via email using the generic print@printbyxerox.com address will be put in the PUBLIC cloud company account. The only exception to the above is if there is an email domain mapping in place for a given cloud company, in which case the user will be put into the mapped company.

Users can also end up in the PUBLIC account via on-boarding from one of the login interfaces, Web Portal, Workplace App, and the @PrintByXerox printer client if they do not specific a company code when creating an account. Again, the only exception to the above is if there is an email domain mapping in place for a given cloud company, in which case the user will be put into the mapped company.

An end user's information for the PUBLIC account is stored in the UK data centers.

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), their OKTA credentials, their HelloID credentials or their Azure AD credentials. When using LDAP, the Domain will be used to route the LDAP requests to the correct Agent, which will then 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 4 hours of inactivity.

Workplace Cloud Agent

When the Agent is initially installed, the company's Xerox® Workplace Cloud administrator must provide their credentials (Workplace Cloud, LDAP, OKTA, HelloID 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 App [PMM]

When accessing the Xerox® Workplace 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), their OKTA credentials, their HelloID credentials 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 for Workplace Cloud Authentication or LDAP is 1-365 days based on the configuration set by the company account administrator. 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 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 App. For iOS devices, the credentials are saved in a keychain which is encrypted and only accessible by the Workplace App. The OS of the mobile device will delete any saved data including the credentials when the application gets un-installed. If using Azure AD, OKTA or HelloID, credentials are never stored. Instead, the phone will store the refresh token of the Identity Provider and will attempt to auto-refresh as needed.

There is a version of the Workplace App that supports Google Chromebooks as well as an extension to the Google Chrome browser. When run in these environments, the Workplace 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 user's 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 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 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.

Workplace Cloud Client for Windows and Mac [PMM]

When installing the Workplace Cloud 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), their OKTA credentials, HelloID Credentials (Windows only), 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 token is encrypted using AES before being stored on the local workstation. The lifetime of the access token is 1 to 365 days based on the configuration set by the company account administrator (for LDAP or Workplace Cloud Authentication). Once the access token is expired or becomes invalid, the user will be prompted to re-supply their authentication credentials, after which a new access token will be created. For Azure AD, OKTA or HelloID (Windows), the lifetime of the Workplace Cloud access token matches that of the Azure AD, OKTA or HelloID access token lifetime. When this expires, Workplace Cloud will attempt to use the Azure AD or OKTA refresh token to obtain a new Azure AD, OKTA or HelloID access and refresh token, which then will generate a new Workplace Cloud access token.

To simplify the logon process, the Desktop Client will cache the user's email address. It would then be used in subsequent login scenarios where the current Workplace Cloud access token has expired and the user is required to re-authenticate. The cached email will be stored along with other persistent data used by the Desktop Client. If the user manually logs out of the solution, the cached email address will be discarded.

Printer

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. [Note: OKTA and HelloID only support the PIN option. PINs can either be Card Numbers, values imported from LDAP / Azure AD / SAML, administrator managed values, or auto-generated PINs created by Workplace Cloud].
2. The user can identify themselves using their access card (for example, employee badge).
3. The user can use the Xerox® Workplace 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 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.

Workplace Cloud supports a special administrator logon capability for Printer Authentication. Enabling this setting allows a user to log into the printer control panel via the Alternate Login feature and access administrator functions of the printer. To use this feature, the user must enter the username of “admin” on the first Alternate Login screen, and then enter the password configured by the WC administrator. The password is common across all devices which have been enabled for printer authentication by Workplace Cloud. This feature is disabled by default.

AUTO-GENERATED PINS

The Workplace Cloud solution supports the creation of auto-generated PINs, which can be used as a printer authentication mechanism. This feature is disabled by default for your cloud company. However, an administrator may optionally enable this option if using printer authentication. Auto-generated PINs are numeric only. The starting length of the PINs is configurable, between 4-10 digits. These values are auto-generated when a user first on-boards to the company. The administrator can regenerate PINs for users if needed. The end user can also regenerate their PIN if desired. PINs are never re-used, and are always unique for all users in the Cloud Company. Only the end user can see their auto-generate PIN. An administrator is not able to view their auto-generated PIN.

Xerox® @PrintByXerox App [PMM]

To access the Xerox® @PrintByXerox 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), their OKTA credentials, their HelloID credentials, 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 Xerox® @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.

The Workplace Cloud solution supports the ability for the administrator to define or configure a delegate or set of delegates for any given user. This allows a user that has been granted delegation rights to release or delete that users’ jobs when accessing the @PrintByXerox App. [When an administrator grants delegation rights, both the delegate and main user are sent an email notifying them of this configuration change]. Upon entry to the @PrintByXerox App, the user (delegate) can then view their own print jobs, but they have the ability to switch to viewing the jobs of a user for which they are a delegate. This is a one-way access switch within the app. Once the delegate switches from viewing their jobs to that of the other user, then cannot switch back and they cannot switch to viewing the jobs of another user. They must log out and re-logon if they wish

to view their own jobs or those of another user. When a delegate releases a job of another user, that job will be tracked as if the original user released the job in the job history and reporting data. An email notification will be sent to the original job owner, notifying them that a delegate printed their job.

EXPRESS CODES

The Express Code function is an optional feature that the Workplace Cloud administrator can enable for their cloud company. The primary use case for Express Codes is for guest printing via email submission. However, the desktop print patch can also support Express Codes. To use this feature, the administrator must first define an Emil Prefix for their company, and then enable the option to use it as an alias for print@printbyxerox.com. This setting is found on the Company Profile page. The Express Code option is then available to be enabled. Once enabled, any job emailed to the defined Email Prefix will result in the return of an Express Code. This is a six-digit numerical value. User can log into the @PrintByXerox EIP app on the printer using their confirmation number and release just the one associated email job. Each email submission to the email prefix address will result in a different express code (one per email). The administrator has an additional option to control whether or not desktop jobs will be included in the Express Code feature.

Content Delivery Network (CDN) [PMM]

Microsoft Azure supports the use of CDN as a mechanism to improve the distribution of data, enabling fast and localized downloads. Microsoft partners with different CDN providers, which have many geographically distributed servers with high-speed connections to Azure. Xerox makes use of Microsoft's Azure Front Door service to provider CDN functionality for Xerox Workplace Cloud. When print ready jobs are made available for release at a printer, and either that printer supports the EIP Pull Print API (e.g., ConnectKey, AltaLink and VersaLink devices), or the job is being downloaded by the Agent, then @PBX app and the Agent can tell the printer to retrieve the print job from the Cloud (pulling the job down to the printer over HTTPS on port 443 and submitting it to print), or the Agent will download the job directly via CDN and submit it to the printer using the configure print protocol. This print retrieval supports the CDN path to stream the job data from Azure blob storage in the Workplace Cloud through the Azure Front Door CDN server that is closest to the printer/agent and then down to the printer or agent. The path between Azure blob storage and the CDN edge server is essentially a super highway to quickly get the data from one of the Azure sites used by Workplace Cloud (US, EU or UK) to the CDN endpoint. The data is then pulled down to the printer/agent from the CDN edge server, which is physically close to the printer, minimizing the network path that the data needs to travel. The print job data is never stored in the CDN endpoint. Caching is disabled on the Azure Front Door servers, however, while transitioning from the Azure<->Azure Front Door TLS connection to the Azure Front Door<->Customer TLS connection, the content needs to be decrypted and re-encrypted in memory due to the different certificates involved in the transfer. Customers who may be concerned with this data transfer can use the Desktop Enhanced Encryption feature under policies to ensure desktop jobs remain encrypted throughout the transfer or leave the feature disabled.

The CDN feature is optional for Workplace Cloud accounts. The feature is disabled by default for new Workplace Cloud accounts. To configure CDN support, the administrator must go to the: Account > Settings > Performance page and modify the 'Enable CDN' checkbox. The URLs that need to be accessed by the printer are shown below:

- https://xwcsvccdn.services.xerox.com

The above URL is actually a DNS CNAME for an Azure Front Door endpoint that will have the base URL of:

- https://*.azurefd.net

Printers must have access to the internet (either directly or via a proxy) in order to take advantage of this feature.

The size of a print job has implications for whether or not CDN is used. For small files, the job will just be pulled directly from Azure Blob storage and CDN will not be used. There is some overhead to setting up the CDN that makes it inefficient to use for smaller jobs. Logic is built into Workplace Cloud to only use the CDN pathway when it makes sense.

The print ready files stored in Azure Blob storage are encrypted using a unique (per job) symmetric key and initialization vector. The files are decrypted by the Workplace Cloud as they are downloaded. [Note: if the customer is using their own certificates with keys for encryption, please see the section titled “Document Encryption Summary”]. The lifetime of the print ready files stored in Azure Blob storage is dependent upon the company’s retention period for downloaded jobs: Immediate, 1 day or 3 days. An unprinted job would be removed from Azure Blob storage after 3 days. The maximum time a job will be stored will never exceed 3 days, whether or not it’s printed and retained or unprinted.

The access token for the print ready file URL which is created and given to the @PBX App or the Agent to make a pull print request has a very short lifetime (15 minutes) and is a single use token (meaning you can’t download the file from the same URL more than once). If there is no request to retrieve the job during the token lifetime, the URL will expire and no longer be valid. This is done to ensure that there is only a small window of availability to retrieve the file.

For those customers that are concerned about regionalization and keeping user data (in this case the print job data) within a given region (e.g., GDPR concerns), the Azure Front Door platform relies upon many servers distributed throughout the world. When a printer or agent attempts to retrieve a job from Azure blob storage, which in turn makes use of the CDN platform, the URL of the job will consist of a base FQDN that is the same for each of the primary Azure data centers used to perform document conversion:

- xwcsvccdn.services.xerox.com

When the printer/agent attempts to resolve that URL, which contains the above FQDN value, the printer’s local DNS server will get routed to n Microsoft DNS server. Microsoft’s DNS server system will attempt to locate the closest server to the requestor (the printer). The printer or agent’s DNS server is used as a proxy for the actual location of the printer/agent.

7. Additional Security Items

Xerox® Workplace Cloud Endpoint Table

The following endpoints, provided in 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). [*Note: the IP addresses associated with these endpoints can change at any time. Xerox does not use fixed IP addresses for these endpoints. Do not attempt to resolve these DNS names to IP addresses and then add exceptions to your firewall allowed list using IP addresses.*]

CLOUD ENDPOINTS

Component	Product	Ref#	Endpoint FQDN
Xerox® Workplace Cloud Agent		1	https://xwc.services.xerox.com
		2	https://xmpcws.services.xerox.com
		4	*.servicebus.windows.net
		8	(Azure AD only) https://login.microsoftonline.com
		9	(OKTA only) customer defined URL
	[PMM]	10	[OPTIONAL] https://xwcsvccdn.services.xerox.com
	[FM]	11	(Fleet Management) https://clouddm.azure-devices.net
	[FM]	11	(Fleet Management) https://iot-cfm-weu-prd.azure-devices.net
	[FM]	11	(Fleet Management) https://iot-cfm-scus-prd.azure-devices.net
	[FM]	13	(Fleet Management) https://xwcdm.services.xerox.com
		18	(HelloID only) https://{helloiddomain}.helloid.com
	[FM]	19	https://xeroxdmprdstoragescus-fqdwgqhqehcfb4dt.a03.azurefd.net
	[FM]	19	https://xeroxdmprdstorageweu-bbf2baebhxc0gaga.z01.azurefd.net
	[FM]	19	https://sfxeroxdm-c8afdpfpcwg6b4hp.z01.azurefd.net
Xerox® EIP Printer & @PrintByXerox EIP App	[PMM]	1	https://xwc.services.xerox.com
	[PMM]	3	https://xmpceip.services.xerox.com
	[PMM]	2	https://xmpcws.services.xerox.com
	[PMM]	8	(Azure AD only) https://login.microsoftonline.com
	[PMM]	9	(OKTA only) customer defined URL
	[PMM]	10	[OPTIONAL] https://xwcsvccdn.services.xerox.com

		11	(Workplace Cloud Direct) https://clouddm.azure-devices.net
		11	(Workplace Cloud Direct) https://iot-cfm-weu-prd.azure-devices.net
		11	(Workplace Cloud Direct) https://iot-cfm-scus-prd.azure-devices.net
		12	(Workplace Cloud Direct) https://wdm.services.xerox.com
	[PMM]	18	(HelloID only) https://{helloiddomain}.helloid.com
	[FM]	19	https://xeroxdmprdstoragescus-fqdwgqhqehcfb4dt.a03.azurefd.net
	[FM]	19	https://xeroxdmprdstorageweu-bbf2baebhxc0gaga.z01.azurefd.net
	[FM]	19	https://sfxeroxdm-c8afdpfpcwg6b4hp.z01.azurefd.net
[PMM]Xerox® Workplace Application – Mobile App	[PMM]	5	https://xccsts.services.xerox.com
	[PMM]	2	https://xmpcws.services.xerox.com
	[PMM]	6	https://publicprintapi.services.xerox.com
	[PMM]	8	(Azure AD only) https://login.microsoftonline.com
	[PMM]	9	(OKTA only) customer defined URL
		18	(HelloID only) https://{helloiddomain}.helloid.com
Xerox® Workplace Cloud Web Portal – Customer Web Pages		1	https://xwc.services.xerox.com
		8	(Azure AD only) https://login.microsoftonline.com
		9	(OKTA only) customer defined URL
	[FM]	13	(Fleet Management) https://xwcdm.services.xerox.com
		15	(SAML only) IDP Single Sign-On Request
	[PMM]	17	https://app.powerbi.com
		18	(HelloID only) https://{helloiddomain}.helloid.com
[PMM]Xerox® Workplace Cloud Client	[PMM]	5	https://xccsts.services.xerox.com
	[PMM]	2	https://xmpcws.services.xerox.com
	[PMM]	1	https://xwc.services.xerox.com
	[PMM]	7	https://virtualprintiothub.azure-devices.net
	[PMM]	7	https://virtualprintiothubukw.azure-devices.net
	[PMM]	7	https://virtualprintiothubus.azure-devices.net
	[PMM]	7	https://virtualprintiothubncus.azure-devices.net
	[PMM]	7	https://virtualprintiothubneu.azure-devices.net
	[PMM]	7	https://virtualprintiothubweu.azure-devices.net
	[PMM]	8	(Azure AD only) https://login.microsoftonline.com
	[PMM]	9	(OKTA only) customer defined URL

	[PMM]	15	(SAML only) IDP Single Sign-On Request
	[PMM]	18	(HelloID only) https://{helloiddomain}.helloid.com
[FM]Xerox® Device Agent	[FM]	1	https://xwc.services.xerox.com
	[FM]	2	https://xmpcws.services.xerox.com
[PPM] Xerox® Workplace Cloud Printer Client for APEOS printers	[PMM]	2	https://xmpcws.services.xerox.com
	[PMM]	16	https://xmpcapeos.services.xerox.com

CLOUD ENDPOINT DESCRIPTIONS

Ref#	Endpoint FQDN	Description
1	https://xwc.services.xerox.com	Hosts the web portal interface used by administrators and users for configuration and web submission of print jobs. Also used for SSO and SAML Assertion.
2	https://xmpcws.services.xerox.com	Hosts the web service endpoint allowing print job submission and management as well as retrieving and setting configuration data for an account. Also used for print job retrieval by the printer when using the Xerox® @PrintByXerox App, or when the Agent retrieves jobs to be pushed to a printer.
3	https://xmpceip.services.xerox.com	[PMM] Web server used to host the Xerox® @PrintByXerox browser pages available on EIP printers.
4	*.servicebus.windows.net	Azure service bus endpoints used by the Agent to connect to the Azure service bus gateway.
5	https://xccsts.services.xerox.com	The Xerox routing service used during login. Maps the user's email to their home company and the configured authentication mechanism for that account. Performs authentication if Cloud or routes to an external authentication mechanism (LDAP, OKTA, HelloID or Azure AD). Grants access token.
6	https://publicprintapi.services.xerox.com	[PMM] Used for printing to third party providers if enabled in the company account.
7	https://virtualprintiothub.azure-devices.net https://virtualprintiothubukw.azure-devices.net https://virtualprintiothubus.azure-devices.net https:// virtualprintiothubncus.azure-devices.net https://virtualprintiothubeun.azure-devices.net https://virtualprintiothubeuw.azure-devices.net	Azure IoT Hub for print job release notifications to the Workplace Client when jobs are stored locally as a result of the Local Print Optimization feature.
8	(Azure AD only) https://login.microsoftonline.com	Azure AD login for authentication of users.
9	(OKTA only) customer defined URL	OKTA login for authentication of users.
10	[OPTIONAL] https://xwcsvccdn.services.xerox.com	[PMM] High speed Content Delivery Network endpoints hosted by Microsoft. Used for print job retrieval by the printer when using the

		Xerox® @PrintByXerox App, or when the Agent retrieves jobs to be pushed to a printer.
11	https://clouddm.azure-devices.net https://iot-cfm-weu-prd.azure-devices.net https://iot-cfm-scus-prd.azure-devices.net	[FM] Azure IoT Hub for fleet management notifications to the Workplace Cloud Agent for printer configuration and monitoring. [PMM] / [FM] (Workplace Cloud Direct) Azure IoT Hub connection endpoint for Workplace Cloud Direct Authentication, Print Release and Device Management commands.
12	https://wdm.services.xerox.com	[PMM] / [FM] (Workplace Cloud Direct) Request Azure IoT Hub connection details to be used for establishing an IoT Hub connection to be used by printers for Workplace Cloud Direct Authentication and Device Management. Return EIP response messages for requests that come through the IoT Hub.
13	https://xwcdm.services.xerox.com	[FM] Used for Web Portal when accessing Fleet Management pages.
14	(SAML only) IDP Metadata URL	Retrieval of IDP Metadata file by the Workplace Cloud Service.
15	(SAML only) IDP Single Sign-On URL	SAML 2.0 authentication request.
16	https://xmpcapeos.services.xerox.com	[PMM] Web server used to host the APEOS Printer Client browser pages.
17	https://app.powerbi.com	[PMM] Embedded Power BI Service hosted by Microsoft Azure. Used to render the Reporting Analytics pages.
18	https://{helloiddomain}.helloid.com	HelloID login for authentication of users.
19	https://xeroxdmprdstoragescus-fqdwgqhqehcfb4dt.a03.azurefd.net https://xeroxdmprdstorageweu-bbf2baebhxc0gaga.z01.azurefd.net https://sfxeroxdm-c8afdpfpcwg6b4hp.z01.azurefd.net	[FM] Storage account location for retrieval of software updates and clone files to be installed / applied to printers.

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

Following, are 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 App [PMM]

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 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 App will prevent any further communication with Workplace Cloud and therefore prevent the user from using the App.

Xerox® @PrintByXerox App [PMM]

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 Xerox® @PrintByXerox 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 Xerox® @PrintByXerox 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 Xerox® @PrintByXerox App is installed.

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

Auto Release Using Network Appliance Workflow [PMM]

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

1. Ethernet 241
2. Elatec TCP Conv2 / Conv3
3. 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 / Conv3 - 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 App, Web Portal, Xerox® @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 six different Azure data centers:

- South Central US – located in Texas
- North Central US – located in Illinois
- UK South – located in London
- UK West – located in Cardiff
- EU West – located in the Netherlands
- EU North – located in Ireland

All User and Account information is stored in the UK (both the UK South and UK West), the EU (Netherlands and Ireland), or the US (Texas and Illinois) data centers. The data is replicated across paired sites in the UK, EU or US to support failover scenarios. Print job data is stored in either the US, EU or UK explicitly or based on geo-location. Within the UK, EU and US data centers, there is full active redundancy for services and the database in that region. A UK West data center failure will fail over to the UK South data center. An EU North data center failover will fail over to the EU West. A North Central US data center failure will fail over to the South-Central US. A UK South, EU West or South Central US data center failure may cause temporary loss of service globally depending on the type of failure encountered and the time associated with the full switch over to the UK West, EU North or North Central US site respectively. Due to the centralized nature of the User and Account database being in the UK, EU or US and because of government and business privacy policies, the respective hosting locations will never failover to a different region.

Usage Tracking and Reporting [PMM]

The Xerox® Workplace Cloud supports the ability to collect network accounting information from Xerox and Fuji 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 or the Fuji APEOS Accounting API, the Workplace Cloud will supplement print job data that it collects (includes print jobs sent to Workplace Cloud enabled printers as well as print jobs submitted to a Home Worker Print Tracker supported printer) with that retrieved from Xerox Network Accounting. This is an optional feature that is disabled by default and must be enabled globally in the customer's cloud account to make it available on a printer-by-printer basis. Usage tracking data collected by Workplace Cloud is stored in Azure SQL in the UK, EU or US Azure sites. The Analytics feature in Workplace Cloud accesses the Azure SQL to generate tables and graphs. The solution supports the ability to export the raw reporting data to a CSV file, or to use the reporting dashboards, both of which use the reporting data stored in Azure SQL.

Reporting data retrieved from Xerox printers is done using the EIP Network Accounting API, which runs over port 443. The printer is server in this case, listening for external commands. Requests are made by either the WC Agent, or if using Cloud Direct technology, the request is initiate over the Azure IoT Hub from the WC backend and the printer returns the response data using a REST API call over ort 443 to WC.

For Fuji devices, the XWC Agent is used to retrieve job history from the device. The Agent queries the printer using HTTPS over port 443 to extract the job history. The printer's admin credentials are needed as part of the job history API request. This information is then uploaded in Xerox Workplace Cloud and included in the Reporting data.

Data stored by Workplace Cloud in Azure SQL will be archived monthly using Microsoft's long-term retention capability in Azure SQL. This includes the reporting data. The archive files will be

retained for 7 years. These will be stored in the relevant Azure sites with SQL databases used by Workplace Cloud. This equates to the UK, EU and US sites. Each quarter, the solution will purge reporting historical data as needed that is older than one year. The customer will always have access to a minimum of 1 year of reporting data.

Single Sign-On [PMM]

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:
  1. The channel is encrypted via HTTPS.
  2. 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.
  3. 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. The App then posts this data to the Workplace Cloud Agent. The Agent validates the request is coming from printer with an active user session, as well as validates the IP address of the call to ensure it's coming from an enabled printer and which has an active user session. The Agent then forwards the request to the Workplace Cloud solution in Azure.
4. When this request is received by Workplace Cloud, it validates the signature using the public key of the Gallery App Server.
5. 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.

If the customer is using the "Cloud Direct" option, where the printer it communicating directly with the Workplace Cloud solution in Azure and there is no on-premise Agent, additional safeguards are put in place to ensure the security of the user's data. The Workplace Cloud solution will create a unique client certificate for the printer and push it as well as the corresponding public root certificate to the device. When the App on the printer is attempting to access the vault, it performs an HTTPS post to the EIP browser on the printer. The browser then forwards that request to the cloud service endpoint in Azure, which is configured to require certificate authentication. The solution validates that the certificate is valid, and it matches the printer on which the user has an active authentication session. Only after these security checks are performed will the solution allow access to the user's vault data for the given App.

User Import via CSV File

Xerox® Workplace Cloud supports the ability for an administrator to import a list of users into their cloud company account, thereby avoiding the user from having to on-board themselves to the company. The primary focus of this feature is allowing both the creation of the user and the assignment of a PIN or Badge / Card number to the user. The PIN assignment is particularly important for customers with a large number of users that do not have access cards or badges, and want a single factor form of authentication at the printer to release jobs.

The import feature is constrained such that only users with pre-staged email domains for that company will be allowed to be created and linked to the account. For example, if Company XYZ owns the email domain of "@xyz.com", they can request the Workplace Cloud team to link that email domain to their company account. This process is carried out off-line and is performed by Xerox® Workplace Cloud personnel. If the administrator attempts to import a user with an email domain that has not been linked to their company (e.g., @gmail.com), that user will be ignored by the system.

The set of support fields that may be imported into the user database of Workplace Cloud are:

- Email
- Last Name
- First Name
- Middle Name
- Group [Note: Groups must exist prior to import]
- Department
- Username (e.g., DOMAIN\USERNAME for LDAP)
- PIN (Card Number)

[Note: The administrator must pre-define the PINs and ensure they are unique. The CSV imported PINs / Card Numbers are different than the Workplace Cloud auto-generated PINs. The auto-generate PINs are managed by the Workplace Cloud solution and cannot be set or altered using the CSV User import feature].

The results of importing a list of users will be emailed to the administrator that requested the import as well as the contact person for the company account.

Packet Inspection

Xerox® Workplace Cloud makes use of both the Azure Service Bus and Azure IoT Hub mechanisms for the Workplace Cloud Agent and Workplace Cloud Client to receive response messages from the cloud hosted solution. These interfaces make use of certificate validation. These Azure communication mechanisms in conjunction with the Workplace Cloud Agent and Client prevent the use of packet inspection being used to view the contents of the messages being exchanged over these interfaces. Web inspection utilities that attempt to analyze data going into or out of their company will cause Xerox® Workplace Cloud to fail for the Azure Service Bus and Azure IoT Hub communication pathways.

Document Encryption Summary [PMM]

Xerox® Workplace Cloud will always store both original documents and print ready documents in an encrypted format when in the cloud. Files are encrypted using an AES encryption method. A symmetric key is generated to encrypt the file, and then the key itself is asymmetrically encrypted

using a public certificate. The point at which a document is encrypted depends upon the submission method:

- **Desktop Client** –Files uploaded from the Desktop Client are always encrypted before being uploaded to the cloud using this method.
- **Workplace App** – A file uploaded from the Workplace App will be encrypted upon receipt by Workplace Cloud before being stored.
- **Web Portal** – A file received from the Web Portal will be encrypted upon receipt before being stored in the Cloud.
- **Email** - A file received from email will be encrypted upon receipt before being stored in the Cloud.

As noted previously, the Workplace Cloud solution will always symmetrically encrypt documents at rest in the cloud using AES with a unique key per job. The key itself is then asymmetrically encrypted using key. There are three options in Workplace Cloud regarding the source of the encryption/decryption keys:

- **Xerox Encryption** (default) – A common public certificate and private key is used to encrypt and decrypt the symmetric keys for documents at rest in the cloud. It's also used to encrypt desktop jobs before uploading them to the cloud. Documents are decrypted for conversion and when released and downloaded to a printer or agent. Decryption happens in the cloud.
- **Account Encryption** – This is a Bring Your Own Key (BYOK) option which allows the customer to create and upload their own certificate and private key pair. This option is used for documents at rest in the cloud. It's also used to encrypt desktop jobs before uploading them to the cloud. Documents are decrypted for conversion and when released and downloaded to a printer or agent. Decryption happens in the cloud.
- **Desktop Enhanced Encryption** – This option supports End-to-End encryption of desktop custom driver jobs, requiring the customer to Bring Your Own Key (BYOK). Customers must upload their own public certificate for encryption of jobs in the desktop client. The certificate with the private key must be installed on the Agent(s) and/or printers (supported on select printer models). Jobs are encrypted when not on the customer network, including while in transit (uploading / downloading).

For both the Xerox Encryption and Account Encryption options, the point at which jobs are encrypted or decrypted is the same. The only difference between the two is which keys are used for the encrypting and decrypting documents. If the customer uploads a certificate for Account Encryption, then that will always take precedence over the Xerox Encryption mechanism.

For Account Encryption, the customer must create and upload a PFX file that contains the public certificate with the public key as well as the private key use for decryption. The private key must be password protected. The keys must also be 2048-bit or larger.

For the Desktop Client submission path, the solution supports a Desktop Enhanced Encryption mode. The administrator has the option to create and use a pair of x509 certificates, one which contains a public key and the other which contains a private key, that will be used for the encryption and decryption. The customer uploads the public certificate to Workplace Cloud, and this is then pushed to all of the XWC Clients. Files encrypted using a customer provided public certificate will always remain in an encrypted format when in the Cloud, including during upload and download.

Files encrypted using the Workplace Cloud default public certificate or by the customer Account Encryption certificate will be decrypted when they are retrieved by either the Agent or by the Printer if it using the EIP Pull Print API. The actual decryption is done by the Workplace Cloud backend system as it is streamed by the receiving endpoint. The actual decrypted file will never reside on any physical storage media in the cloud.

If the customer is using the Desktop Enhanced Encryption (i.e., their own x509 certificate pair for desktop jobs), then the customer will install the private cert (used to decrypt the print jobs) on each XWC Agent deployed at the customer site. If the customer has AltaLink devices that natively support decryption, then the private certificate as well as the root CA (Certificate Authority) used to sign the private certificate can be installed on each AltaLink device. All desktop jobs that have been encrypted with a private key, upon release, will be routed to the Agent, or in the case of the AltaLink, they may directly be pulled down from the cloud to the printer. This includes print jobs released by the Xerox® @PrintByXerox App. The XWC Agent must pull the job down in its encrypted format, and then the Agent will decrypt it and sent it to the printer. Files encrypted using a customer provided public certificate will always remain in an encrypted format when in the Cloud, including during upload and download. They can only be decrypted by the Agent that has the matching private certificate in its Windows certificate store. For AltaLink devices with the appropriate release and installed certificates, the printer will decrypt and spool the job directly. Files encrypted using a customer provided public certificate will always remain in an encrypted format when in the Cloud, including during upload and download. They can only be decrypted by the Agent that has the matching private certificate in its Windows® certificate store, or by an appropriately configured printer that has the matching private certificate as well as the root CA certificate used to sign the private certificate. The print will validate the chain of trust between the private certificate and the root CA certificate. If the chain of trust cannot be made, the print will delete the encrypted print job and nothing will be printed.

Content Security [PMM]

The Content Security Workflow allows an administrator to create a Content Profile, whereby they define a set of search strings which are used to track documents processed by Workplace Cloud. The solution will then process each job (limited to desktop jobs submitted with the Windows desktop client application). The client application will parse submitted jobs.

- Logging the matching strings in the Job History.
- Emailing (notifying) a list of recipients with details on the job (e.g., who printed it, name of the job, the device it was printed to, the time and date it was printed).

Microsoft Azure Universal Print [PMM]

Workplace Cloud can be integrated with Microsoft Azure Universal Print. This feature allows a cloud company to create a single pull print queue in the Microsoft Azure Universal Print resource. Once created in the Azure tenant, the print queue can be authorized and shared out to all the users of the organization like any other Microsoft Universal Print Printer. This will allow Windows 10 Azure AD joined devices to add the printer and submit content to the queue, which in turn will cause the jobs to be pulled into the Workplace Cloud solution for later release to a printer. Details on setup of this feature can be found in the administration guide.

The Microsoft Azure Universal Print integration with Workplace Cloud requires the customer to create a new application in their Azure AD Tenant that is accessible by Workplace Cloud. The application must have the following Permissions listed below. Note that two of the below items indicate “Delegated” permissions. It is vital that the administrator configuring Microsoft Universal Print in the Workplace Cloud web portal have those permissions in their Azure AD tenant or the registration process will fail.

API	Permissions	Type	Description

Microsoft Graph	Users.Read	Delegated	Sign in and read user profile
Universal Print	Printers.Create	Delegated	Create (register) new printers
Universal Print	Printers.Read	Application	Read printers
Universal Print	PrintProperties.ReadWrite	Application	Read and write the properties and attributes of printers
Universal Print	PrinteJob.Read	Application	Read the metadata and payload of users' print jobs
Universal Print	PrinteJob.ReadWriteBasic	Application	Read and write the metadata of users' print jobs

In order for Workplace Cloud to access the created web application in the customer's tenant, the customer must create a client secret under Certificates & Secrets for the new application. In Workplace Cloud, the cloud company administrator must then supply the following information for the app:

- Tenant ID (from the Azure AD Tenant Overview)
- Application ID (from the Web Application created for Workplace Cloud)
- Client Secret (which was created as noted above)

As part of the registration process allowing Workplace Cloud to retrieve jobs submitted to the Azure tenant's Universal Print queue, the customer must also configure where the submitted jobs will be stored once retrieved by Workplace Cloud. The locations correspond to the Azure sites used in the deployment of Xerox® Workplace Cloud:

- UK South
- EU North
- South Central US

The normal retention settings for the customer company account will apply to the Universal Print jobs once retrieved by Workplace Cloud.

For more information on Microsoft Universal Print please see the latest documentation from Microsoft: https://docs.microsoft.com/universal-print/.

SAML Connection

Customers that are using an Identify Provider (IDP) that supports SAML 2.0, such as ADFS, may optionally use that provider to simplify the login process for the desktop client and the web portal. If the user is logged into their workstation, the solution will attempt to log the user into Workplace Cloud using that same identity. You must configure your IDP to trust the Workplace Cloud application as well as provide information for the solution to communicate with the IDP. This capability is only supported for workstations running Microsoft Windows.

[Note: the SAML Connection capability has only been validated when using a LDAP Authentication in conjunction with ADFS. Multiple SAML Connection definitions are not supported.]

CONFIGURING THE IDP AND WORKPLACE CLOUD

To use SAML, the administrator must supply information to the IDP about Workplace Cloud so that it can trust communication coming from the solution. Similarly, the Workplace Cloud must be

configured with information about the IDP so that it knows how to connect to the provider. The required information includes:

Service Provider Information (to be entered into the IDP)

- Workplace Cloud Identifier (*urn:xerox:services:xwc*)
- SAML Assertion Endpoints (always use HTTPS on port 443)
  - *https://xwc.services.xerox.com/login/acs* (Web Portal)
  - *https://com.xerox.services.xwc/login/acs* (Desktop Client)
- Binding (*HTTP-Post*)
- Field Mappings

Identity Provider Information (to be enabled into Workplace Cloud)

- Metadata URL – location of IDP configuration file (retrieved via HTTPS). The port is typically 443 but could be a non-standard port such 8443 as defined by the IDP.

The Workplace Cloud solution will retrieve the IDP configuration from the supplied Metadata URL location. The key information retrieved in the configuration file includes:

- Identifier (Entity ID)
- Single Sign-On URL – Connection's use HTTPS. The port is typically 443 but could be a non-standard port such 8443 as defined in the retrieved metadata file.
- Single Sign-On Binding – Must be "HTTP-Redirect"

DOMAIN HINT CONFIGURATION

In order for the desktop client and web portal to use SAML, the customer must supply an email domain hint as part of the initial connection information to Workplace Cloud in order to bypass the normal email prompt screen. The method for doing this varies for the web portal and client. The provided domain must by pre-configured in the Workplace Cloud routing service for the given company account.

Web Portal (Browser)

For browser authentication, the user must supply the domain hint in the URL. The format of the browser URL is:

- https://xwc.services.xerox.com/<domain>

Desktop Client

For the desktop client, the administrator must configure the email domain using JSON configuration file on the user's workstation. This file will be read by the desktop client application when a logon request is required. The file name is '*PdlParserSettings.json*' and is located at: *%PROGRAMDATA%\Xerox\XMPC*. The contents of the file should be:

```
{
    "CompanyLookup": {
        "Domain": "<domain>"
    }
}
```

INTRANET ZONE CONFIGURATION

Both the Web Portal and the Desktop Client login methods require the Federation Server DNS name to be added to the Intranet Zone in order for SAML to work. Details on how to configure this trust can be found here:

Configure Client Computers to Trust the Account Federation Server | Microsoft Docs

EXTRANET/INTERNET CONFIGURATION

If users will be required to log into the Desktop Client or Web Portal from the extranet/internet, then the customer must deploy a Web Application Proxy.

- For extranet access, all clients accessing the ADFS service from outside the corporate network (extranet/internet) must be able to resolve the ADFS service name to the load balancer for the Web Application Proxy servers or the Web Application Proxy server.
- The firewall located between the Web Application Proxy and the ADFS system must allow TCP inbound connections over port 443.
- The firewall between the clients and the Web Application Proxy must allow TCP inbound connections over port 443.
- If client user certificate authentication (client TLS authentication using X509 user certificates) is required and the certauth endpoint on port 443 is not enabled, AD requires TCP port 49443 to be enabled inbound on the firewall between the clients and the Web Application Proxy.

METADATA URL FILE RETRIEVAL

The Metadata URL configured in the SAML Connection page of the Web Portal must be accessible via the internet. The Workplace Cloud solution hosted in Azure will need to access this URL to retrieve the configuration file. Customers must ensure this file is publicly available and accessible in order to use the SAML capability.

SAML AUTHENTICATION PROCESS

SAML authentication is supported for both the desktop client and the web portal. This assumes the above has been configured properly. The actual authentication request will be sent by the user's workstation to the IDP Single Sign-On URL. From there, the IDP will handle the request. If the user is not currently logged into the IDP on their workstation then the IDP will post back to the requestor, displaying a logon screen (e.g., for ADFS). This is a browser-based screen being displayed by the desktop client (in a browser frame) or if using the web portal in the user's browser. The user would enter their credentials which are sent back to the IDP. The Workplace Cloud solution is not directly handling credentials in this case. The results of the logon request are returned to the caller (user workstation) via an HTTP Post. If the logon attempt was from the client, it would Post the results to the Workplace Cloud routing service. If the logon attempt was from the Web Portal, the results are sent to the SAML Assertion Endpoint (*https://xwc.services.xerox.com/login/acs*), which is then processed by the Workplace Cloud routing service. The solution will validate the signature of the SAML response. If the results are successful, the user is granted an access token. If the results are not successful, the solution will fall back to prompting the user to enter their email and appropriate credentials for their company authentication method configured for their Workplace Cloud company account. [Please note that the Workplace Cloud implementation of SAML does not support separately encrypting the request/response. All communication is over an HTTPS encrypted channel. To increase the security of the SAML connection, the solution will create and supply a Relay Session ID to the IDP. This ID must be returned in the response and has a limited lifetime of 5 minutes].

Device Cloning [FM]

The Workplace Cloud Fleet Management solution provides the ability to upload device clone files and push these to printers being managed in the company account. Some of the data items in a clone file may be considered sensitive, such as server names, IP addresses, system passwords, etc.). Clone files coming from newer Xerox devices like AltaLink, VersaLink and ConnectKey WorkCentre products encrypt the clone files at creation time. The CFM solution does not perform additional encryption of these files at rest in the cloud.

8. Additional Information and Resources

Security @ Xerox®

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see https://www.xerox.com/security.

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

Additional Security Resources

Below are additional resources.

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/
Xerox Trust Center	https://trust.corp.xerox.com