Xerox® Workplace Suite 5.8.0

Security Guide

Document Version: 1.0 (May 2024). BR32554

Table of Contents

1. Introduction

Xerox® Workplace Suite (WS) is a workflow solution that connects a corporation mobile workforce to new productive ways of printing, and controls user access to Xerox® Multifunction Printers (MFP). 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.

WS has been extended in version 5.0, providing a single sign-on (SSO) infrastructure. Apps in the Xerox App Gallery which have been modified to support this new infrastructure may use WS as a storage vault for user login information (e.g., credentials or tokens). After logging into WS, a user may select an SSO enabled Gallery App, which queries WS to obtain the user's login information for that app. If available (and valid…e.g., not expired), the app uses that information to log the user into the Gallery App without the need to provide additional login credentials.

Purpose

The purpose of the Security Guide is to disclose information for Xerox® Workplace Suite 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 Suite 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 Suite 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

The Xerox® Workplace Suite provides three primary workflows:

- Print Management Workflow (which includes Single Sign-On for supported Gallery Apps)
- Mobile Print Workflow
- Content Security Workflow

Print Management Workflow

There are two parts to the Print Management workflow: Printer Authentication and Desktop Printing and Release.

Authentication

Defined as customers who require validation of user access to MFPs before device usage is allowed at the “All Services” screen. Card-based is the most widely used authentication method. User name and PIN-based login at the device is an alternate method of login when card readers are not installed or are not functional. Authentication as a standalone option provides device security access only, for the customer who does not require print jobs associated with their network login. Supported authentication mechanisms include:

- Cards (e.g., HID Prox)
- Alternate Login
  - Email and Confirmation Number
  - PIN (card number)
  - LDAP/AD
- Mobile Phone Unlock using the Xerox® Workplace App: supporting NFC, QR Codes and Unlock Code Entry
- NFC Unlock with a support USB Card Reader (Android Only using Elatec TWN4 Reader with NFC unique programming)

Single Sign-On

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

The Single Sign-On feature allows WS to store user access information for Xerox® Gallery Apps that have been designed to support the single sign-on feature. The Authentication solution now becomes an SSO vault. The SSO vault acts as a storage vault, where login information for each supported/enabled Gallery App is stored.

As an analogy, you can think of the SSO vault (e.g., XWC) as a security vault with a collection of safety deposit boxes. Each user is given a safety deposit box that is unique for that user and a specific App (e.g., the File and Print Dropbox App). To access the safety deposit box, the user provides their identity (i.e. they log into the printer) and then indicates which safety deposit box they wish to access by selecting an App on the User Interface of the printer. The App then views the contents of the safety deposit box from the security vault or they may update or delete the contents.

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

Desktop Printing

The Workplace Suite supports the Desktop Print feature using two different print queue types.

1. Network Queues – where jobs are printed to a shared Windows network print queue and can then be routed or processed appropriately according to the print workflow (Direct or Pull-Print).
2. Client Queues – where jobs are retained locally on the user's client PC until they are routed and processed, again based on the print workflow (Direct or Pull-Print). This method requires the installation of a desktop client on the user's workstation.

For either of the above print server models, the administrator may configure the type of print workflow that they would like to use. The two supported workflows:

1. Pull Print – where jobs are held until the user authenticates themselves at a printer and releases.
2. Direct Print – where jobs are sent immediately to the printer that is associated with the queue.

Rules and Quotas can also be applied to desktop jobs, which allows control over who is able to print, to which devices and at what time as well as controlling how many pages can be printed. Rules can also be used to control which print features (color or 2-sided) are available to users.

Mobile Print Workflow

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 Xerox® Workplace Suite. Depending on the submission method, the job is either printed without any further user action or the user manually releases the job to print. Rules can also be applied to mobile print jobs, which allow control over who is able to print, to which devices and at what time. Rules can also be used to control which print features (color or 2-sided) are available to users.

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

Submission Methods

- E-mail
- Xerox® Workplace App (formerly Print Portal)
- Simple Desktop Print Service (upload)

Release Methods

- Printing device UI (via EIP)
- Xerox® Workplace App (formerly Print Portal)

Combined Submission / Release Methods

(Note: jobs print without any explicit user action after submission):

- E-mail
- Xerox® Workplace App (formerly Print Portal)

Content Security Workflow

The Content Security Workflow allows an administrator to create Content Profiles and define search strings which are used to track documents processed by WS. The administrator can define actions that will be taken when a document is searched and found to match a Content Profile. The possible actions include:

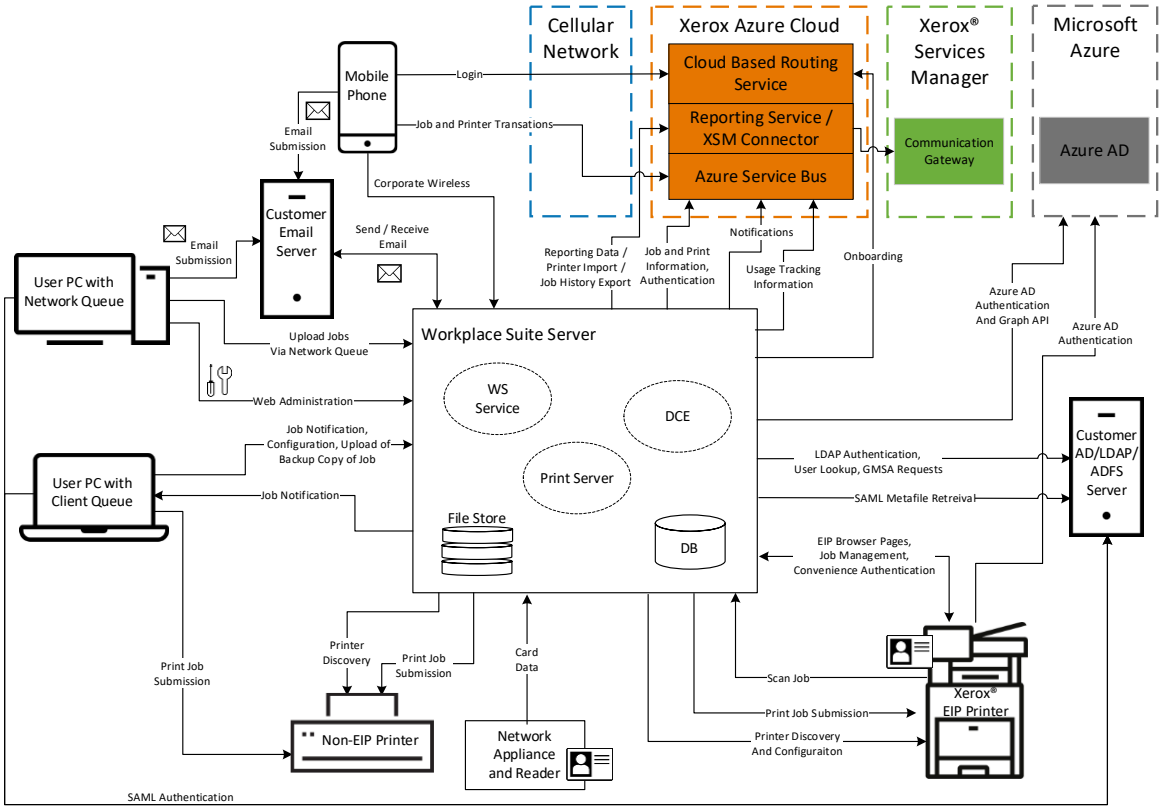
- Logging the matching Content Profile name in the Job History.
- Emailing (notifying) a list of recipients with details on the job (e.g., who printed it, name of the job, the device it was printed to, the time and date it was printed and the matching Content Profile name.
- Storing a copy of the job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

Diagrams

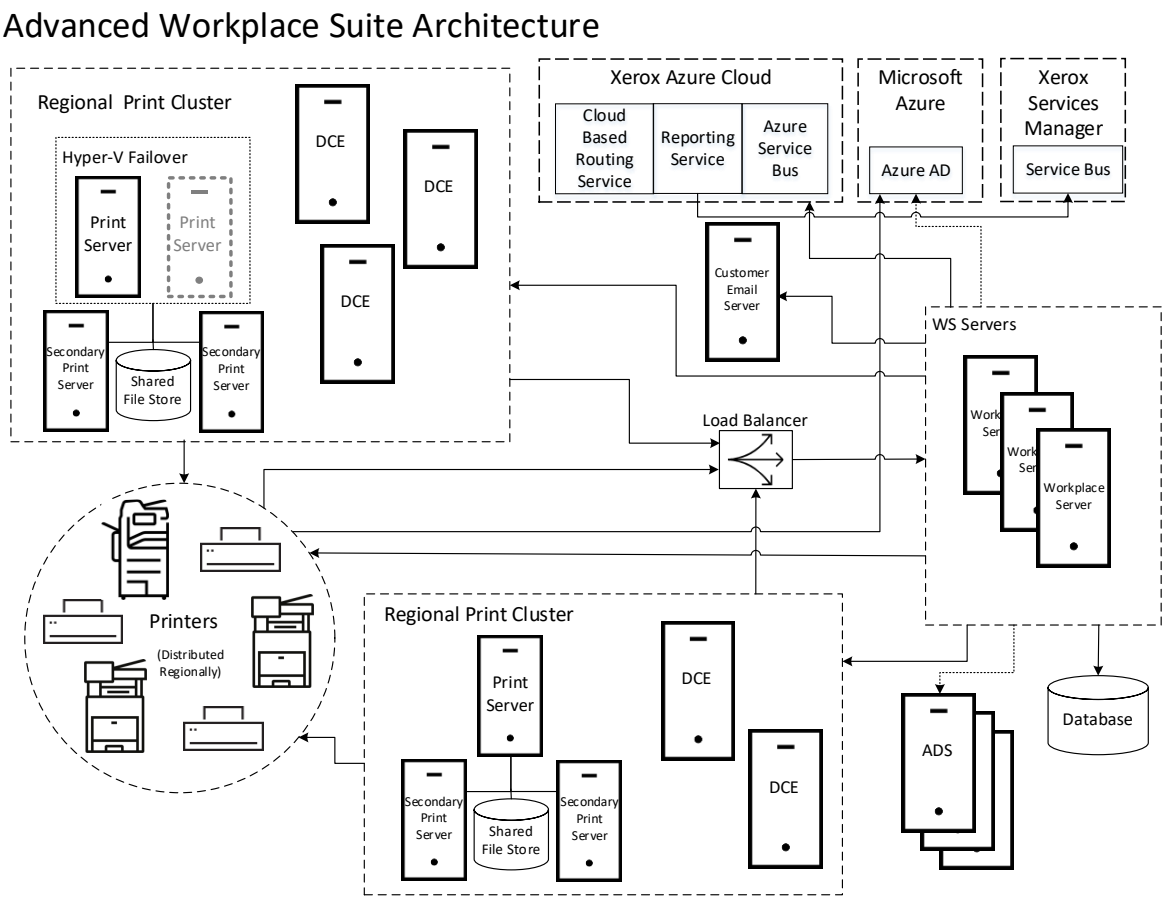
The below diagram shows a couple of example system component / architecture diagrams for different sized customers using the Workplace Suite for both the Print Management and Mobile Print Workflows. These diagrams and their components will be discussed in greater detail in the following sections of this document.

Simple Workplace Suite Components

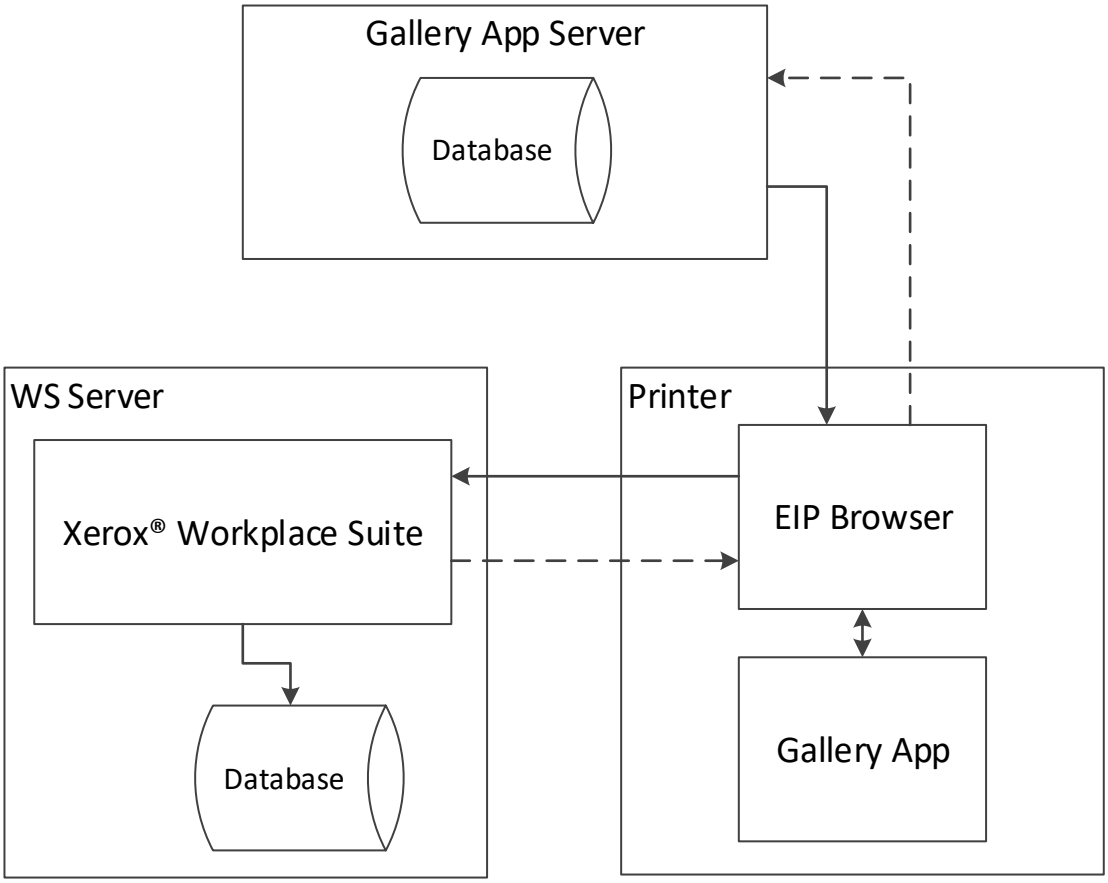
Simple Workplace Suite Architecture (Single Server)



Advanced Workplace Suite Architecture



Single Sign-On Components



Description of System Components

Component	Description
User	A user of the WS system.
Xerox® Workplace Suite	On premise application that runs on customer provided hardware/server, which supports Printer Discovery, Printer Management, Print Routing, EIP Web Page Host, Administration Host, and Convenience Authentication.
Xerox® Workplace App (print portal)	Mobile Phone application that allows the user to find printers and upload / send print jobs to WS.
Xerox Cloud Services	Xerox Cloud Services hosted on Microsoft Azure that support Mobile Phone authentication, printer discovery and print submission.
Customer ADS/LDAP Server	Used for user authentication.
Microsoft Azure AD	Used for user authentication.
Identity Provider	Used for SAML authentication with the web administration (user portal) interface.
Print Server with Network Queues	Windows PC hosting Shared Network Print Queues running the Job Agent Service. Handles job routing, notifying the WS of new jobs, parses jobs, modifies job for selected attributes, and transmits jobs to the printer on release.
Document Conversion Engine (DCE)	Converts mobile jobs to print ready format upon release and transmits jobs to the printer.
SQL Database	Storage of WS configuration, user info, job info, job history.
File Storage	Storage of print jobs.
Printer	Any printing device (Xerox® or Non-Xerox®) that is enabled to support WS.
Customer Email Server	The Customer Email Server is used to get print jobs to the Xerox® Workplace Suite.
User PC with Network Queue and/or Client Queue	User's system on which network print queues or client queues (using the desktop client) are installed.
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.
Reporting Service / Xerox Service Manager Connector	Azure hosted interface between the Workplace Suite server and Xerox Service Manager.
App from App Gallery	An App found in the Xerox App Gallery that has been modified to support SSO.
App Server	A backend system that handles the browser-based calls and processing needed by the App. Maintains knowledge and information about the SSO server.

3. System Interaction

This section describes the system components and their interfaces.

Xerox® Workplace Suite Server

The Workplace Suite server is the foundational component of the Xerox® Workplace Suite solution, used to manage the system's behavior and user's interaction within the system from authentication, document submission, and printing. The Xerox® Workplace Suite Server (WSS) is a Windows® application running on a Windows® Server. WSS will conform to the customer's existing security policies, using Windows® based authentication to access this application. It is recommended that access to the server be limited to Systems Administrators and authorized Xerox® personnel.

Users authenticate themselves at a printer using the WSS. In addition, user's documents are received and either stored for secure release or directly printed at a printer. The Xerox® Workplace Suite server monitors and works in conjunction with the available Conversion Servers for document conversion and print processing, as well as the Job Agent Clients and Print Servers on receiving and releasing desktop print jobs. The XWSS provides Single Sign-On functionality for supported Gallery Apps.

For network communication using HTTPS, the WSS supports TLS versions 1.0, 1.1 and 1.2. Support for SSL v2/v3 has been deprecated.

There are a number of sub-functions of the Xerox® Workplace Suite server, which are discussed in greater details below.

Administration Services

The WSS administration services provide configuration, user, printer and job management.

The administrator interacts with the Administration Services via a web browser interface to perform tasks such as creating an incoming email account to receive jobs upon, managing users, registering printers, and enabling features. Connection to the Administration Services is supported via HTTP (port 80) or HTTPS (port 443). By default, the Workplace Suite Server uses a self-signed certificate for HTTPS communication.

[Please note that most web browsers will generate a warning when using the self-signed certificate as it was not generated by a trusted authority].

The administrator has the option to load and use a certificate from a trusted certificate authority on the Xerox® Workplace Suite server.

The Workplace Suite Admin webpage is accessed via a web browser. By default, the system uses an email address and confirmation number to access the administration interface the first time. From there, there administrator may select the desired authentication mechanism for both web administration and user portal (see next section) access. The supported authentication mechanisms are:

- Email and Confirmation Number – User can login using their email and a system generated Confirmation Number. Confirmation numbers are not visible to the administrator and are stored as hashed values in the DB.
- LDAP Authentication – User can login using their LDAP credentials. At least one LDAP Connection must be enabled to select this option.

- Windows Integrated Authentication - When this option is enabled, users will not be required to log into the User Portal. Workplace Suite will use the identity of the current Microsoft Windows session to log the user into the portal.
- Azure AD Authentication – Users can login using their email address and their Azure AD password. This mechanism requires that the system has access to the internet.
- SAML Authentication - Customers that are using an Identify Provider (IDP) that supports SAML 2.0, such as ADFS, may optionally use that provider to log into the web administrative interface. If the user is logged into their workstation, the solution will attempt to log the user into Workplace Suite using that same identity. You must configure your IDP to trust the Workplace Suite application as well as provide information for the solution to communicate with the IDP.

User Portal Services

The WSS User Portal provides the ability for a user to manage settings and configuration specific to themselves. At this time, this is limited to being able to view and manage Release Permissions for the Printer Client (EIP App). Refer to section “7.5 – Printer Client Release Permissions” for further details on this feature.

Users interact with the User Portal via a web browser interface. Connection to the User Portal is supported via HTTPS (port 443). By default, the Workplace Suite Server uses a self-signed certificate for HTTPS communication.

Mobile Print Workflow Details

By default, the Mobile Print Workflow allows any user to create an account within the system. Accounts are created whenever an email submission is received or when the Xerox® Workplace App (print portal) is first used to access the system.

However, the system can be configured to only allow a specific set of users (an allowed-list) or to not allow a specific set of users (a block-list).

When an account is created the user receives a system generated confirmation code. The confirmation code is used to access their jobs at the MFP or to connect the Workplace App to the server.

All users’ jobs are stored and referenced based upon the user’s email address. User’s jobs are stored in the Workplace Suite Server Windows file system with a randomized file name. Jobs stored on disk are encrypted using AES-256. Additionally, an Encrypted File System (EFS) may be configured as well.

Unprinted jobs are deleted based upon an administrator configured retention period. The default retention period is 1 day. The Retention Settings apply to Third Party Print Queues in addition to printers. Sending documents to a Third-Party Print Queue is equivalent to the print command in the Mobile Print Workflow. This means that if the system is configured to delete documents after printing, documents are deleted after sending them to a print queue. Based on this same example, if a default print queue is set on the system, all emails sent to Workplace Suite are in turn sent to the default print queue and immediately deleted from the system.

Print Management Workflow Details

By default, the Print Management Workflow supports auto-registration. If the customer site uses LDAP or Domain controllers, then auto-registration allows the user to scan their badge (or Android phone with NFC) via a connected USB card reader at a Print Management (authentication) enabled printer. The user would then provide their LDAP authentication credentials to validate their identity, resulting in the addition of that user and their relevant LDAP information (name, email, network

user name) in the Workplace Suite user database. The solution can support multiple badges per user if desired. If auto-registration is not used, there are other options to create and manage users, including: Manual Updates, CSV Import, and LDAP Import.

All submitted jobs are stored and referenced based on the user's network user name and email address. The user's jobs are stored in the print server's Windows file system, or on the client with a randomized file name. Jobs received and stored by the print server are encrypted using AES-256. Jobs on the client workstation are not encrypted.

Unprinted jobs are deleted based on an administrator configured retention period. The default retention period is one day.

Rules Processing

The WS system allows the administrator to define rules which are applied at print release time (applies to copy jobs as well). There are 2 types of Rules available in WS.

1. Print Controls – are used to determine which printers are available, the time and day when they can be accessed and what attributes may be used when processing jobs for any given user.
2. Print Quotas – are used to set a page limit per user that they are allowed to print during a given time period (daily, weekly, monthly).

By default, no rules are defined. Users may access any printer, at any time, and all print attributes are available. In addition, there are no print quotas defined, so users can print an unlimited number of pages. When one or more rules have been defined and enabled, the system switches to a permission access mode. In order to print, the user must be granted permission to print to a given device using a rule. The administrator can control which devices, which time of day and which attributes are available to the users of the system. If there are no rules allowing a user to print, based on the device being used and the time of day, then the user's job is blocked from printing after release.

If a user exists in multiple rules, then all rules are checked at the time of print release. If there is at least one rule allowing the user to print to the given device based on the time of day, then the jobs are allowed to complete. If there are multiple rules that map the current printer and time of day, which have conflicting print feature access (e.g., color and single-sided), the rule(s) granting access to these features take precedence).

Rule processing always occurs on the WS server. This processing determines if a user is allowed to release a print job on a given printer, at the current time and if any job attributes need to be modified (e.g., change to black & white or duplex). The actual job attribute changes occur in different components based on the location of the job: JAS/JAC for desktop jobs and the DCE for mobile jobs.

Content Security Processing

The processing of jobs for Content Security occurs at the time the job is uploaded into the WS system. This implies that the processing occurs in different components based on entry into the solution. For desktop submitted jobs using the Print Management Workflow, the JAS/JAC components handle content security processing. For Mobile Print jobs and Copy and Scan jobs, the WS server handles the processing. The WS server handles the coordination of the results of the content security processing and ensuring the configured options for a matching profile is applied: Logging, Email Notification and Storing.

In the case of Content Storing of a job, the administrator defines the location of where the data will be stored using the web admin as well as the retention period of the stored files. The maximum allowed retention period is one year. Once the retention period is reached, the stored file(s) are deleted. As with any Microsoft server OS, the deleted documents follow traditional Microsoft

Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself, but are overwritten as the system reclaims the disk space. The Workplace Suite provides no facilities to erase the documents themselves. The stored files are encrypted using AES-256 by WS. Additionally, file Encryption is available using the Microsoft built-in Encrypted File System (EFS) feature.

Copy and Scan Job Processing

The WS solution supports the ability to perform Scan and Copy jobs. Both job types result in the scan job being sent or pulled to the server. The job is stored temporarily in the Content Partition Storage location until it is printed or emailed. The job is deleted after it is transferred to the final destination. If Content Security is enabled and the job matches a Content Profile that is configured with the content storage option, the original PDF received from the scan is then stored in the configured content storage location. If Rules are enabled, then they are applied to Copy jobs, as copies result in printed / marked pages.

Single Sign-On

The WS Server provides the SSO functionality that can be called or access from supported Apps in the 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 WS. 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 (SHA256) within the SQL database.

Xerox® Workplace App (formerly Print Portal)

The application uses a Xerox managed cloud-based routing service to direct the user to the appropriate Xerox® Workplace Suite server. Once authenticated, the user's credentials and authentication token are stored in the application until they log out.

The Workplace Suite Admin has control over how often a user will need to re-supply their credentials when using the Workplace App. An option exists to retain the logged-on user's credentials within the app, such that any subsequent logon will not require the user to re-supply their credentials. The Admin may also control the length of time that the user will remain logged into the account when using the Workplace App. Users will be required to re-supply their credentials once the once the timeout is reached. If the Admin has enabled the "Retain Login Credentials" feature, then the user would automatically be logged back into the system after the expiration time period.

Users can only access jobs that they have submitted. This includes Print Management Workflow (Pull-Print) jobs as well. With the Workplace App, users can preview their jobs, see a list of available printers, select print options and submit their job for printing.

For security reasons, enabling and accessing the Workplace Suite server using the Workplace App is a multi-step process:

1. An administrator must enable the use of the Workplace App via Administration Services at the Workplace Suite Server, the result of which is a "company code." The Workplace Suite administrator must distribute this code to authorized users. [Note: An administrator may request a new company code at any time.]
2. During initial log-in a user must enter their email address and company code.

3. The Workplace Suite system generates a confirmation code and sends the confirmation number to the user at the supplied email address.
4. The user must then enter the confirmation code into the Workplace App.

The Mobile Print Workflow supports both an allowed-list and a block-list capability. An allowed-list would restrict access to only a specified set of user email addresses; a block-list would disallow these email accounts.

Lastly, if a user needs to reconfigure the Workplace App from one company code to another, an action verification code is sent to the user by the Xerox® Workplace Cloud (Cloud Hosted) itself.

For customers that have installed both the Mobile Print Workflow and the Print Management Workflow, the Workplace App supports the ability to authenticate with an enabled printer. There is an option in the menu of the app called “Unlock Printer”. This option allows you to use your phone to authenticate with a device in place of a card or using Alternate Login. The supported logon methods for mobile phone unlock include:

- NFC (Android and iOS, where your iOS device must be an iPhone 7 or newer running iOS 11 or later). [Feature requires a Xerox® VersaLink or Xerox® AltaLink series printer]
- QR Code – You may scan the QR code found on the welcome page or on the blocking screen of the printer user interface panel.
- Unlock Code – You may enter the 4-character code found on the authentication blocking screen of the printer.

The Workplace App supports iOS native printing. This print mechanism uses a combination of printer discovery, via either mDNS or DNS-SD to locate a compatible printer. If using mDNS, the Apple Bonjour Service must be installed on the Xerox® Workplace Suite server, and the standard Bonjour ports must be opened on the server’s firewall. The Xerox® Workplace Suite Server responds to mDNS queries and advertises itself as a printer, thereby allowing Workplace App users to submit print jobs to Workplace Suite using iOS native printing. Alternatively, the IT administration at a customer site can configure their DNS servers to advertise the Xerox® Workplace Suite server as a printer. This allows client applications such as Workplace App to use DNS-SD (service discovery), to discover the Workplace Suite Server as a printer. Regardless of the type of discovery method, once found, the Workplace App can submit (upload) jobs to the Xerox® Workplace Suite server using IPP (port 631). Jobs are then available for release using the Workplace App to a printer, or the Printer Client (EIP) Application.

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 supports “single sign-on” using your Google credentials to validate the user in place of manually entering credentials.

Xerox Managed Cloud Based Routing Service

The managed cloud routing service provides a “routing” capability between the Workplace App, running on a customer’s smart device, and the Workplace Suite Server running within the customer’s network. Messages are sent from the Workplace App to the Cloud Service.

The managed cloud-based routing service runs on the Microsoft Windows Azure Platform (see below). All communication is handled using Industry standard HTTPS protocols with TLS 1.2. The security certificate is issued by Comodo (a trusted certificate authority) and ensures that the application has been verified and validated.

For more information on Windows Azure Security, please visit:

http://azure.microsoft.com/en-us/support/trust-center/

Document Conversion Servers

The Xerox® Workplace Suite is modular in design, leveraging a core Workplace Suite server component as well as one or more additional Mobile Print Workflow components referred to as Conversion Servers. The Conversion Server converts documents from their native format (e.g., .doc, .ppt) to a print ready file (e.g., Postscript, PCL) that the destination printer understands. A Conversion Server may reside on the same server as the Xerox® Workplace Suite server, or it may reside on a separate server. Only one Conversion Server may reside on any given server.

Document Storage

Both the native format document and the print ready file are temporarily stored to the Conversion Server system disk while the files are active. Once the Conversion Server has completed the document conversion process, the print ready document is stored in the configured Content Storage location, which could be local to the DCE or a shared network resources (e.g., RAID system). Files are encrypted before being stored to disk using AES-256. Please note that the conversion process requires access to the unencrypted data. So there is a short period of time during conversion where an encrypted file will be temporarily stored on the disk. Any temporary files created during the conversion process are deleted from the Conversion Server disk and memory after storing the print ready document.

The print ready file is deleted from the system once the original is deleted.

As with any Microsoft server OS, the deleted documents follow traditional Microsoft Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself, but are overwritten as the system reclaims the disk space. The Workplace Suite provides no facilities to erase the documents themselves. In this sense, the Conversion Server is treated as any other document server within the corporate firewall.

Job Agent Service / Workplace Client

The Print Management Workflow is modular in design, leveraging the core Workplace Suite Server, as well as one or more additional components referred to as the Job Agent Service and the Workplace Client. The Job Agent Service runs on the print server and is included as part of the install of the Xerox® Workplace Suite software. For customers who want to use an external print server, they can install the Job Agent Service on one or more external servers to create a distributed or regional system of print servers. For environments that want to forego a traditional print server, they can instead install the Workplace Client on each user's workstation. The Job Agent Service/Client is also responsible for processing incoming print jobs for Content Security. Jobs are processed to see if they match one of the configured Content Profiles. If a match is found, the agent notifies the WS server. If the matching profile has the content storage option enabled, the agent also creates a PDF of the print job and sends this to the WS server to be T.

Job Agent Service

The Job Agent Service is a Windows service installed on a print server used in conjunction with the Xerox® Workplace Suite software with the Print Management Workflow license. The service can run on the same server running the Xerox® Workplace Suite, or it can run on one or more external print servers. When installed on an external server, the Job Agent Service starts a listening service and waits for the Workplace Suite Server to enable it to perform job management. The Xerox® Workplace Suite administrator must add the print server IP Address to the list of print servers, effectively enabling the Job Agent Service to begin communicating with the Workplace Suite server. The messaging between the Workplace Suite Server and Workplace Client consists of:

- Reporting of available printers (Queues)
- Enablement of printers (Queues)
- Job Information – Reporting of new jobs and their details
- Notification of job release to an enabled printer
- Results of job transfer to a printer
- Periodic job synchronization

Workplace Client

The Workplace Client is a Windows service installed on a client workstation used in conjunction with Xerox® Workplace Suite Software with the Print Management Workflow license. When installed on a user workstation, the Workplace Client must be pointed to the Workplace Suite Server via the inclusion of a configuration file or via a Service Registry setting which can be pushed to the workstation by the customer IT organization. The Workplace Client is responsible for managing print queues and print jobs on the client workstation. The messaging between the Workplace Suite Server and Workplace Client consists of:

- Querying the server for configuration (e.g., polling intervals, timeouts, etc.)
- Querying the server for the list of printers (Queues)
- Installing or removing printers (Queues)
- Job Information – Reporting of new jobs and their details
- Polling or notification for job release to an enabled printer
- Reporting of job transfer to a printer
- Periodic job synchronization

Document Storage

Mobile Print Workflow

Documents are stored and encrypted using AES-256 by the Xerox® Workplace Suite server. The documents are stored in a configurable location, which can be any location to which the Xerox® Workplace Suite server has access. For performance and configuration reasons, on-box storage is recommended. Access to the documents is protected by Windows and Server access on the client's domain. As a layer of protection, actual documents are stored with an obfuscated file name and extension.

The documents are retained until either:

- The user deletes them via the Print Client App at the device UI or the Workplace App.
- The Xerox® Workplace Suite deletes them after a configurable timeout.

As with any Microsoft server OS, the deleted documents follow traditional Microsoft Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself but are overwritten as the system reclaims the disk space. The Mobile Suite Web Administration UI does provide the ability to delete documents if needed.

Note: Stored documents are encrypted using AES-256. Additional encryption is also available using the Microsoft built-in Encrypted File System (EFS) feature.

Workplace Suite limits the maximum size of a submitted file to 1GB or smaller. A utility may be used to modify this value if necessary.

Print Management Workflow

All printers (queues) configured for the Print Management Workflow use the Workplace Suite Port Monitor. Part of the Windows print path, this monitor accepts a print ready file (e.g., Postscript of PCL) and writes it to disk. The location where the file is written is configured using the Workplace Suite Web Admin tool. The print ready file and some descriptor files are temporarily stored on the print server or client workstation system disk while the files are active. Upon release to a printer, the Job Agent Service or Client removes the associated files based on the configured retention settings.

Note: For jobs stored on the print server, documents are encrypted using AES-256 before storing them to disk. There is a small window of time during submission of the file where the XWS port monitor will receive the incoming job and temporarily store it to disk in an unencrypted format. The XWS server monitors the folder where these files are temporarily written by the port monitor and will process and move them to longer term storage where they are encrypted. The encryption scheme does not apply to the jobs stored locally on the user's workstation. Additional encryption is also available using the Microsoft built-in Encrypted File System (EFS) feature. With the release of version 5.6, the Desktop Client supports an optional Local Print Optimization mode that will store follow-you jobs locally as well as store a backup copy on the server in the event that the user workstation is not available at the time the document is released at a printer. By default, client queue jobs are only stored locally on the workstation. This option controlled by a combination of a global permission setting as well as enabled on an individual basis at the workstation level via a configuration file that can be deployed in managed software environment (e.g. using SCCM). The backup copy of the file will be stored on the Workplace Suite Print Server that hosts the client queue (used to download the driver to the user workstation). The backup files will be stored in the same directory as network queue jobs on the Print Server. This is a configurable location that can be uniquely defined for each Print Server. The default location is:

- C:\ProgramData\Xerox\XMP\CompatibleJobTickets\Jobs

When Local Print Optimization is enabled and a client queue job is released to a printer, the preferred print path is from the client workstation to the printer. After the job is transferred to the printer, both the client workstation copy and the server copy will be deleted (based on the configured retention settings). If the client cannot be reached to release the job, the printer server will be notified and the backup copy will be sent to the printer. The print server will delete the backup copy after transferring the job (based on the retention settings). Once the client re-connects to the server it will clean up any jobs that were printed. The cleanup process runs once per day.

As with any Microsoft server OS, the deleted documents follow traditional MS Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself, but are overwritten as the system reclaims the disk space. The Xerox® Workplace Suite provides no facilities to erase the documents.

Xerox® Workplace Suite Database

Microsoft SQL Express 2017 database is used by Xerox® Workplace Suite as the default relational data store. However, WS can be configured to work with an external Microsoft SQL database. The database must be created prior to connecting Workplace Suite.

When using an external Microsoft SQL database, the Workplace Suite solution supports three different forms of authentication:

1. **Windows Authentication** – The user account logged into the Server on which Workplace Suite is being installed must have Read/Write access to the SQL database.
2. **SQL Server Authentication** – The user credentials provided for database connection must have db_owner rights to the SQL database.
    - For the main database, the solution will construct a connection string that includes the SQL Server information and supplied credentials. This connection string will be encrypted using SHA256 and stored in a configuration file, to be used at start-up to connect to the DB.
    - For the reporting database, the solution will store the SQL Server Authentication credentials in the main SQL database. The credentials are encrypted using SHA256 prior to being stored.

3. Group Managed Service Account (gMSA) – Domain managed account that provides automatic password management
    - GMSA account must have dbowner rights to XWS database or must be assigned to a custom role with the following permissions on the XWS database: Select, Execute, Insert, Update, Delete, Alter, Alter Any Schema, References.
    - Use as a service principal, so Windows manages the password instead of relying on the administrator to manage the password. All service instances use the same principal.
    - The domain controller computes the password on the key that the Key Distribution Services provides, along with other attributes of the gMSA.
    - Unlike the SQL or NT Authentication options, the installing user / machine (domain\machine name$) are not required to have any rights on the Database Server or Database itself.

Microsoft SQL Servers always supports Windows Authentication. If the database engine is configured for 'mixed mode', then SQL Server Authentication can be used. Microsoft SQL Server 2014 and later support gMSA.LDAP / ADS Server

The Xerox® Workplace Suite server retrieves and stores a list of available active directory domains based on the context of the domain to which the WS server belongs. The administrator may also manually add domains if desired. The administrator may then enable or disable domains which can be used for authentication and user import.

LDAP Authentication

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

When the Authentication Type for the Workplace App or the EIP Printer Client App is enabled for LDAP Authentication, or Convenience Authentication is configured for LDAP when using Alternate Login or Auto Enrollment of Cards (or Android phones with NFC and a supported USB card reader), the Workplace Suite Server verifies user credentials against Active Directory. The workplace credentials consist of Domain Name, Domain Username and Domain Password. The Workplace Suite Server performs an LDAP login using the supplied credentials. Passwords are never stored. By default, the system uses SASL when doing an LDAP bind.

In order to communicate with Active Directory, Xerox® Workplace Suite uses the Active Directory Services Interfaces (ADSI) technology available in all Windows operating systems supported by Xerox® Workplace Suite. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if TLS is being used.

LDAP Import

Xerox® Workplace Suite can be configured to import users from Active Directory. This capability is an extension of the setup used for LDAP/ADS Authentication. The administrator has the ability to configure the type of LDAP access (Anonymous, Basic, Negotiate) required when connecting the LDAP server. By default, the system is configured to use the Negotiate setting, which instructs the Workplace Suite Server to use SASL when doing an LDAP bind.

The administrator must supply user credentials to be supplied to the LDAP server when performing an import, assuming they have selected either Simple or Negotiate for the Usage Mode. The credentials are stored in the Workplace Suite Server database (SQL), and encrypted using SHA256 and AES.

As part of the import, the administrator can define the LDAP containers that are queried as part of the import and map the fields within those contains to fields within the Workplace Suite user database.

As part of the import, the administrator may configure the type of LDAP records that they wish to import: Additions (new LDAP records), Modifications (updated LDAP records) or Deletions (users that have been removed or marked as deleted in LDAP). As part of the “Deletions” option, the administrator may configure an LDAP Filter specific to each LDAP server to be used when looking for deleted records to be removed from the WS database.

In order to communicate with Active Directory, Xerox® Workplace Suite uses the Active Directory Services Interfaces (ADSI) technology available in all Windows operating systems supported by Xerox® Workplace Suite. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if TLS is being used.

Microsoft Azure AD

Azure AD Authentication

Xerox® Workplace Suite has the option to support Azure AD as an authentication mechanism for user identification when logging into the User Portal, Printer Client and Print Portal Chrome extension. This mechanism is not supported for Alternate Login at the printer or the Workplace Mobile App.

When 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 Suite 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 Suite solution. When using OAUTH, Workplace Suite never sees the user’s password. What is returned to Workplace Suite is the result of the authentication request. The Workplace Suite server will retrieve the Azure Authentication Token. And will validate its authenticity. The Azure AD Graph API is used by Workplace Suite server to optionally retrieve the following default fields for the user: ‘mail’, ‘userPrincipalName’, ‘department’, ‘employeeid’, ‘givenname’, ‘surname’, ‘jobtitle’ and ‘companyname’. The administrator may choose which values are retrieved and they have the option of specifying non-default fields found in the user’s profile if desired (e.g. to populate the badge number or accounting values). After the authentication token is validated, Workplace Suite will grant the user access to Workplace Suite.

All Azure AD communication between the given Workplace Suite interface (User Portal, Printer Client and Print Portal Chrome extension) is done using HTTPS over port 443.

When a Workplace Suite interface is configured for Azure AD authentication, the individual interfaces (User Portal, Printer Client and Print Portal Chrome extension) handle the credential access via OAUTH. For Web based interfaces (User Portal and Printer Client) the final results of the authentication request are returned to the Workplace Suite server by doing a post-back through the browser to the WS server using one of the following redirect URIs:

- https://<SERVER-NAME>/login/home/ProcessAzureAD
- https://<SERVER-NAME>/xeroxmobileprint/home/ProcessAzureAD
- https://<SERVER-NAME>/xeroxmobileprintnextgen/home/ProcessAzureAD
- https://<SERVER-NAME>/login/api/azure/logout

The Workplace Suite server is the entity that will query the user's profile and will request tokens. This communication is done via HTTPS over port 443. The endpoints used by the Workplace Suite server are:

- https://login.microsoftonline.com (retrieve access token)
- https://graph.microsoft.com (query user profile for configured fields)

For Native Apps, such as the Chrome extension, the results of the authentication request are returned directly to the caller. The Native App will then retrieve the access token and send it to the Workplace Suite server (via HTTPS). The WS server will make the call to the Graph API to query the user profile for the configured fields and update the user record in the DB if necessary.

Auto-Registration of Badges using Azure AD

For those customers that have enabled the auto-registration process, Workplace Suite 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 Suite. If the user does not exist in the WS database, then a new user record will be added for that user.

Configuration of Azure AD

In order to use Azure AD authentication, the customer must create an application in their Azure AD domain found under their O365 subscription. This must be done for the following:

- Web Applications – Workplace Suite User Portal and Printer Client
- Native Applications – Print Portal Chrome Extension

Details on this configuration can be found in the Workplace Suite Administration Guide. Of special note are the permissions that must be granted.

- API Permissions for Microsoft Graph – allow 'openid' (allows user sign-in)
- API Permissions for User Read – Select 'Remove permission' (allows sign-in and read access)
- Web Applications must be given Implicit Grant rights for Access Tokens (allows requesting of a token directly from the authorization endpoint)
- Native Applications must be given Implicit Grant rights for Access Tokens and ID Tokens (allows requesting of a token directly from the authorization endpoint)

Identify Provider and SAML Authentication

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

[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 Suite so that it can trust communication coming from the solution. Similarly, the Workplace Suite 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 Suite Identifier (*XWS-<GUID>*)
- SAML Assertion Endpoints (always use HTTPS on port 443)
  - *https://<XWS-Server>/login/home/ProcessSaml*
- Binding (*HTTP-Post*)
- Field Mappings

Identity Provider Information (to be entered into Workplace Suite)

- 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 Suite 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"

Intranet Zone Configuration

Both the User Portal login method with SAML requires 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

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 Suite solution will need to access this URL to retrieve the configuration file. Customers must ensure this file is available and accessible to the Workplace Suite server in order to use the SAML capability.

SAML Authentication Process

SAML authentication is supported for the user 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 user portal in the user's browser. The user would enter their credentials which are sent back to the IDP. The Workplace Suite 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. In this case they are sent to the SAML Assertion Endpoint (*https://<XWS-Server>/login/home/ProcessSaml*). 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 user will be denied access to the Web

Administration / User Portal. [Please note that the Workplace Suite 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].

Printer

Xerox printers have a variety of security features that can be employed to increase security. Availability of these features will vary depending on model. It is the customer's responsibility to understand and implement appropriate controls for printer behavior.

Secure Print

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

Users may choose to use Secure Print with Secure Print enabled printers, or the administrator may configure their system to require that Secure Print be used for all jobs sent via the Mobile Print Workflow to that printer.

Secure Print passcodes are never stored on the mobile App or in the Workplace Suite Server. 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's documentation.

Printer Authentication

Xerox® multifunction devices introduce a flexible Xerox Extensible Interface Platform® (EIP). This platform acts as a secure embedded web service that other applications can leverage to expose functionality and services to the user through the local control panel interface. Xerox® Workplace Suite uses this platform to secure access to the 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 Xerox® Workplace Suite 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 themselves:

1. The user may supply their Xerox® Workplace Suite user credentials (username / password or LDAP credentials depending upon the Company/Account configuration) at the printer.
2. The user can identify themselves using their access card (e.g., employee badge), or an NFC capable Android phone with a supported USB card reader. [Note: The system can support multiple badges for each user if desired].
3. The user may use the Xerox® Workplace App, using any of the following methods:
    a. Supplying the 4-character code found on the local user interface of the machine into the Workplace App. This identifies the printer in the App and the user can confirm that they wish to unlock the device.

b. Tapping the NFC tag of the printer using their mobile phone (Android or iPhone 7 or newer with iOS 11).
c. Scanning a QR Code (found on the Welcome Page or on the blocking page for AltaLink devices).

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

In conjunction with authentication feature, the Xerox® Workplace Suite supports a feature called Auto-Release. This feature is disabled by default but may be enabled by the Administrator. Upon successfully completing the authentication step at a printer, if the Auto-Release feature is enabled, any print jobs uploaded to the system are automatically be released and printed at the device.

Workplace Suite 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 user name of “admin” on the first Alternate Login screen, and then enter the password configured by the WS administrator. The password is common across all devices which have been enabled for printer authentication by Workplace Suite. This feature is disabled by default.

Xerox® Workplace Suite: Printer Client App

Devices which are EIP capable have the ability to support the Xerox® Workplace Suite App Authentication Solution. This App allows users to identify themselves, view and manage their print jobs.

The Workplace Suite Server installs the EIP App on the printer using the EIP Registration API, which is done using HTTP/HTTPS. Communication between the EIP App and the Workplace Suite Server is done using HTTPS over port 443. For older legacy devices that do not support HTTPS or are not able to handle the encryption keys used by the WS server, the option exists to enable the App to use HTTP over port 80 on a printer by printer basis.

If Azure AD is enabled as the authentication system for the Printer Client, then the EIP App will directly communicate with Microsoft Azure AD using the OAUTH interface via HTTPS port 443. The initial Azure AD request will be directed to: https://login.microsoftonline.com.

Xerox Apeos

Fuji Xerox® multifunction devices introduce a flexible proprietary platform called Apeos. This platform acts as a secure embedded web service that other applications can leverage to expose functionality and services to the user through the local control panel interface. The Xerox® Workplace Suite uses this platform to secure access and present users with the Xerox® Workplace Suite solution for the Mobile Print Workflow. [The Print Management Workflow does not support Apeos].

Customer Email Server(s)

The email server is used to receive emails from and send emails to users of the Workplace Suite solution. The preferred implementation is to leverage the client’s established email infrastructure and email security in place; however, the mail server can be an internally or externally managed server. The email infrastructure acts as the path to transport user’s documents into the Xerox®

Workplace Suite infrastructure. The user's documents temporarily reside on the mail server until the email message and its attachments are retrieved by the Xerox® Workplace Suite server.

The Xerox® Workplace Suite administrator will need to configure both the incoming mail server as well as the outgoing mail server. Both connections require credentials (e.g., username / password) to access the mail servers. The setup, maintenance, and security of the customer email server is outside the scope of Xerox® Workplace Suite.

Network Appliance

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

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

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

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

Xerox® Services Manager

The Xerox® Workplace Suite can connect to Xerox® Services Manager (SM) in order to perform the following actions:

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

Each of these methods of synchronizing with SM has its own configuration as well as specific limitations on the system as a whole.

Connectivity to SM can only be enabled if Xerox® Workplace Suite has a license for "Xerox® Workplace Suite – Managed Print Services."

Export Jobs to Xerox® Services Manager

Only the account ID is needed in order to export jobs to SM. If the printer data is matched to a printer in SM, then SM records the data.

If "Obscure User Data" is enabled, no identifying user information such as the username or password is sent to SM. All identifying information is replaced by unique GUIDs such that the number of individual users reported remains the same but each unique user cannot be identified.

The following data is sent to SM:

Display Name

- Printer Display Name

Network User Name (e.g., the Domain\Username)

- If Obscure User Data is set, a random GUID is sent

- If Obscure User Data is not set, the Domain\Username is sent

Email Address

- If Obscure User Data is set, a random GUID is sent
  - Network Accounting ID and User Name
  - NUp
- This only applies when printing using the FX Apeos workflow
  - Job ID
  - Job Type
  - Copies
  - Page Count B/W
  - Page Count Color
  - Total Page Count
  - Plex
  - Submission Date Time
  - Completed Date Time
  - Content Size
  - Color
- If the document contains color
  - Duplex
  - Document Name
  - Document Type
- If the document is Word, PPT, etc.
  - Media Size
  - Printer Name
  - Printer MAC Address
  - Server Name
- Always Workplace Suite Server Name
  - Server MAC Address
- Always Workplace Suite Server MAC address
  - PDL Type
  - Fax Destination Number
  - Fax Duration
  - Scan Recipient Description
  - Scan Recipient Type
  - Device Job Completion Time

Import Printers / Sites from Xerox® Services Manager

When the Xerox® Workflow Suite is configured to import printers and sites from SM, then SM is treated as the source of record. As such, the administrator has several limitations on what can be modified on printers and sites. The general principle is that any data that comes from SM will be

read-only. The administrator can only change fields related to printers and sites that do not come from SM.

When printers are imported from SM, Xerox® Workplace Suite performs an SNMP discovery to add the printers to the printer list. If the discovery fails, printers are not added to the system.

In order to correctly discover SM printers, discovery settings such as SNMP community names and device credentials must be set correctly on the discovery tab. The settings that the printers used to discover the printers from Xerox® Device Manager or Xerox® Device Agent are not used and must be specified again in Xerox® Workplace Suite.

If a printer is successfully imported in Xerox® Workplace Suite and is then deleted from SM, it remains in the Xerox® Workplace Suite until the system administrator disables or deletes it.

App in the Gallery

This item refers to an App in the Xerox App Gallery that has been modified to use the Single Sign-On feature provided by WS 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 WS server. The App and EIP browser act as an intermediary between the App Server (usually outside the corporate firewall) and the WS server, which is typically on the internal customer network. All communication between the App, the App Server and the WS server uses TLS. [Note: the App is not written by or controlled by the WS solution. It is an external component to the system that is making use of functionality provided by the WS.]

App Server

The server hosting the functionality supplied by an App in the Gallery. This may be a Xerox hosted server or a third-party server, depending upon who created the App. The App Server never directly communicates with the WS. 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 WS solution. It is an external component to the system that is making use of functionality provided by the WS.]

User and Email Server Communication

The first layer of security is at the point of contact between the user and the method used to expose the email address to the end user. Although this is necessary to facilitate the use of the system, it can be controlled using various mechanisms. For example, the email address can be made available through a Xerox printer’s EIP interface and thus accessible to only people physically at the printing device.

The details on how the XMPS solution interacts with the customer email server are provided later.

Users submit their documents for printing using standard email messages from their smartphone to their company’s email server. Whether the email messages are encrypted or not is a decision and responsibility of the company’s IT department.

If the user is submitting the email within the internal corporate network to a corporate email server, the transmission of the document is as secure as any email sent over the corporate network. This is true for both wired and wireless connections. However, if the user submits the email from outside the corporate network, for example, sending it from a personal email account such as Gmail, security cannot be guaranteed until the email is within the corporate network.

In both cases, the security of the document is no different than any email sent to a co-worker's corporate email address.

While a public email server can be used, it is recommended that you have control over the email server and that it is within your corporate firewall. This latter configuration offers the first line of defense by giving you the ability to create and control Blocked and Allowed user lists based on email domain.

The Workplace Suite Server communicates to the end user via email messages sent through the customer's email server. Each time a user submits documents for printing; the Workplace Suite Server retrieves the message and responds with a confirmation email message. The confirmation email message contains a personal confirmation code. The confirmation code is later used to retrieve and print their documents at the multifunction device (MFD).

Confirmation codes are configurable in length and unique for each user. Once assigned the confirmation code will be reused for each submission from the same user. Note, this is specifically for the user's convenience so that all their jobs will be shown at the MFD. Users may request that their confirmation code be changed at any time.

Xerox® Workplace App and Xerox® Workplace Suite Service

In order for a smart device application, running on a service provider's 3G/4G/LTE network to "talk" to a server behind a corporate firewall, an intermediate cloud-based service is used. Xerox uses the Microsoft Azure Service Bus Relay to create this cloud endpoint between the mobile device and the Workplace Suite Service.

The HTTPS protocol is used for all communications between the Workplace App, the Xerox managed cloud-based routing service, and the Workplace Suite Service. Validation of the certificate is done by the receiving system. Therefore, the Xerox managed cloud-based routing service relies on the mobile device operating system to validate the security certificate as part of establishing the TLS connection. Likewise, the Xerox managed cloud-based routing service relies on the Workplace Suite Service to validate the security certificate as part of establishing a TLS connection.

The Workplace App requires users to authenticate before using any of its features. Basic authentication is performed with the Mobile Workplace App providing email and confirmation number or using LDAP credentials over the HTTPS (TLS) protocol.

If using the Chromebook or Chrome browser Workplace Mobile (Print Portal) extension with the single sign-on feature, when a user attempts to log in, the app pre-populates the email field with the logged-on user's email address. When this is submitted to the server, the app also includes the Google authentication token of the logged-on user as well as the AppID of the Workplace App. The server validates the email, token and AppID with Google using HTTPS over port 443. If these are valid, the user is considered authenticated. The server then creates a Mobile Print authentication token and returns that to the Workplace App. The user then remains logged into the App until the Mobile Print token expires. At this time, the app attempts to repeat the process.

Once authentication is complete, data is passed directly between the Workplace App and the Workplace Suite Server or from outside the corporate network by routing through the Azure Service Bus Relay. 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. Again, all communication is using the HTTPS protocol.

In a DMZ Configuration, the intermediate cloud-based service is hosted by the customer. The Workplace App communicates with the customer hosted cloud service, which in turn communicates with the Workplace Suite Server. All communication between the mobile phone and the DMZ

server, as well as the DMZ server and the Workplace Suite Server is done using HTTPS. All other details in the above section apply to a DMZ setup except for the replacement of the Xerox hosted cloud service with the customer hosted DMZ server.

If using iOS native printing, the Workplace App may use mDNS (Port 5353) to discover printers (e.g., the Xerox® Workplace Suite server). When iOS Native Printing is enabled, the Workplace Suite Server is listening for and responding to mDNS queries. Alternatively, the Workplace App may use DNS-SD (Service Discovery) to locate printers. Once found, the Workplace App uses the iOS native print submission mechanism (IPP over port 631) to upload jobs to the Workplace Suite Server.

Customer Email Server and Xerox® Workplace Suite Service Communication

Network communication between the email server and the Mobile Suite Server is configured within the administration pages.

For security:

- The Workplace Suite server requires a customer supplied username and password to access the Mail Server. The credentials are stored within the SQL database.
- The communication port is configurable.
- Network communication between the servers can be configured to be encrypted using TLS.

The Workplace Suite server can send emails to the user and acts as a standard email client. It periodically polls the email server (the poll time is configurable) and retrieves any emails and attachments as needed. Once the email is retrieved, the email and attachments on the email server are deleted.

The Xerox® Workplace Suite server supports connectivity to the following:

- SMTP (port 25 or 587),
- IMAP (143 or 993 (TLS)) and
- POP (110 or 995 (TLS))
- Microsoft Exchange Web Services (80 or 443 (TLS))
- Lotus Domino NRPC (Port 1352)
- Microsoft Graph API (Port 443)

Using the protocols above, the Workplace Suite connects to the inbound email account to pull messages and use the outbound email configuration for sending email. The inbound and outbound email configurations may use different protocols. Workplace Suite can connect to a Microsoft Exchange Server 2007 or later using Exchange Web Services (EWS). This connection is made over the HTTPS protocol. When communicating with Domino, the WSS communicates using a local API with Lotus Notes Client installed on the same PC as WSS, which in turn uses Note RPC to communicate with the Domino server. Communication using the MS Graph API uses HTTPS over port 443.

The Workplace Suite Server can authenticate either using Basic Authentication or Impersonation.

In the case of basic authentication, the username and password are sent securely to the EWS server for authentication.

When impersonation is used, the Workplace Suite will Log On as the impersonated user for the duration of the EWS connection. The impersonated user must have Log On credentials to the Workplace Suite system.

When using the MS Graph API, a shared secret is used for authentication. All communication is over a secure HTTPS channel using TLS.

Workplace Suite Server and Printer Communication

The Workplace Suite server communicates with the Printer for a number of different reasons using various protocols. These are outlined below:

Discovery

Discovery applies to all printers that are enabled to work with Xerox® Workplace Suite. The Workplace Suite Server connects to the printer via SNMP (Port 161) to retrieve printer configuration, capabilities, paper tray information (paper size and availability). The SNMP communication is done either via SNMPv1/v2 (no encryption) or SNMPv3 (encryption) using port 161.

Printer Client (EIP App)

The Workplace Suite connects to the printer's web services to install the Printer Client EIP/Apeos application on Xerox printers via port 80 (HTTP) or 443 (HTTPS) based on the configuration of the printer. The Server makes use of the EIP Session API and Device Configuration APIs using these same ports.

The Workplace Suite can host web pages to the printing device's User Interface commonly referred to as Xerox Extensible Interface Platform® (EIP) and Apeos. The device must be enabled to display these web pages and the web pages do not have any access to documents or any data residing on the printing device. All data exchanged is over port 80 via HTTP (default). HTTPS (port 443) unless the printer is specifically configured to use HTTP (port 80).

Based on the configuration of the system, users may need to identify themselves using the Printer Client. This done by entering their confirmation number, primary PIN, email and confirmation number, their LDAP credentials, or their Azure credentials based on the system configuration. The LDAP password is always obscured (hidden) when entered in the application. The confirmation number is shown by default, but the option to obscure the confirmation number may be enabled by the administrator if necessary. The primary PIN is always displayed. If Azure AD is enabled as the authentication system for the Printer Client, then the EIP App will directly communicate with Microsoft Azure AD using the OAUTH interface via HTTPS port 443. The initial Azure AD request will be directed to: https://login.microsoftonline.com.

Print Authentication

Authentication is only supported by Xerox® multifunction devices that support the EIP Convenience Authentication API.

The server configures the authentication feature on the printer via SNMP (Port 161). The SNMP communication is done via SNMPv1/v2 (no encryption) or SNMPv3 (encryption).

During user authentication, the Workplace Suite Server and the printer communicate using web service calls to initiate an authentication session, supply card data, and / or prompt the user to supply credentials or other data, and unlock the device for user access. All data exchanged is over port 443 via HTTPS.

Scan and Copy

For Scan and Copy jobs processed by WS, the scan job is transferred from the printer to the server using HTTPS (or HTTP if HTTPS is not available). The server initiates this transaction, so the job is pulled to the server. In the case of Copy jobs, the WS server sends the job back to the printer using the configured print protocol for that device (LPR / RawIP / IPP over SSL).

Administrator Configuration and the Workplace Suite Server

In order to administer the Workplace Suite server, users connect to the server using a web browser. When the system is first installed and not yet configured, the system will be in an open state, allowing any user to connect and configure the basic system using the Install Wizard. This process also requires the configuration of an initial starting administrator by supplying their email address and assigning them a confirmation number. Once the Install Wizard is complete, users log into the system using the configured authentication mechanism for the User Portal. The supported methods for authentication include:

- Email and Confirmation Number
- LDAP/AD User Credentials
- Windows Integrated Authentication
- Azure AD

For Windows Integrated Authentication, Workplace Suite will use the identity of the current Microsoft Windows session to look up the user in the SQL database. If the user exists, then they are logged into the User Portal without having to provide credentials. If the user does not exist, then they will be blocked from accessing the web interface. [Note: If IIS web server on the XWS system is unable to validate the identity of the logged-on user, then they may be prompted to supply Windows credentials.]

If Azure AD is enabled as the authentication system for the portal, then the browser will directly communicate with Microsoft Azure AD using the OAUTH interface via HTTPS port 443. The initial Azure AD request will be directed to: https://login.microsoftonline.com.

The administrator may assign roles to the users of the system, such as “General User”, “Power User” or “System Administrator”.

Document Conversion Server and Workplace Suite Service Communication

The Workplace Suite service stores the user’s Mobile Print Workflow documents in the configure Content Storage Location and then notifies the Document Conversion Server using a named pipe (net.pipe) over the localhost interface. The connection can be configured to use other bindings if desired. User documents are only temporarily stored within the external Conversion Server and only to the extent of network communication and conversion.

When the Workplace Suite Service and the Conversion Server(s) are on separate machines, they communicate via HTTPS over port 443.

Document Conversion Server and the Printer

The Conversion Server which hosts the Document Conversion Engine (whether running on the same server as the Workplace Suite Service or on a separate server) is responsible for submitting the converted Mobile Print job to the printer. The default submission method for Mobile Jobs is Raw IP (Port 9100) over TCP/IP. Other ports that can be used are 2501, 2000, 515 (LPR), and 443 (IPP over TLS).

User Workstation and Print Server Communication

The user workstation communicates with the print server in two ways:

- Print queue and driver install
- Print submission

Print queue install can be initiated via the Workplace Client, or via the Windows print install wizard if print queues are added manually. Printing is done via traditional shared Windows network printers. These capabilities use DCE/RPC communication over port 1058 and SMB communication via port 445.

Job Agent Service/Client and Xerox® Workplace Suite Server Communication

The Job Agent runs either on the user's workstation (Job Agent Client as part of the Workplace Client) or on a Print Server (Job Agent Service).

Job Agent Service Start Up

When the Job Agent Service is first installed, the software listens on port 443 using HTTPS for initial configuration information from the Workplace Suite Server. Once the administrator adds the IP address of the external print server to its list of supported servers, the Workplace Suite Server pushes the communication endpoint to the Job Agent Service. This endpoint is used for all communication between the Job Agent Service and the Workplace Suite Server. The JAS processes incoming jobs if Content Security is enabled, looking for matches to any of the Content Profiles. If a matching profile has content storage enabled, the JAS creates a PDF copy of the job. The results of content matching and any PDF copies are transferred to the WS server.

Job Agent Client Configuration

The Workplace Client periodically polls the Workplace Suite Server using the configure endpoint with HTTPS on port 443. This includes the retrieval of timers for job polling, configuration polling, Content Profiles, and maintenance polling. For Job Release, the client supports 3 options:

1. Polling – Client polls the Workplace Suite Server using the configured interval to check for new jobs. This connection is based on TCP using port 443.
2. TCP/IP – Client will listen for TCP connections on port 9907 for notifications to release a pending job.
3. Messaging - The Workplace Client will listen for message notification being sent from the Workplace Suite Server. When running in the messaging mode, the Job Agent Client (JAC) listens on port 9807 using UDP by default. If this port is not available, the client tries 3 other ports to find one that is not in use, adding 10 each time (e.g., 9807, 9817, 9827 and 9837). This port can also be manually configured if desired. If the client fails to obtain a port, then it defaults to using polling mode when querying for pending jobs.

The JAC processes incoming jobs if Content Security is enabled, looking for matches to any of the Content Profiles. If a matching profile has content storage enabled, the JAC creates a PDF copy of the job. The results of content matching and any PDF copies are transferred to the WS server.

Job Management

Both the Workplace Client and the Job Agent Service communicate with the Workplace Suite Server to communicate new jobs being added to the system, to know when jobs are to be released, to update job status, and job synchronization. This is done via web service calls using HTTPS over port 443. The Job Agent Service listens for notifications from the server about jobs to be released. The Workplace Client either polls for this information or if messaging is enabled it listens on port 443. The reporting of new jobs and job status is always initiated by the Workplace Client. For the Job Agent Service, communication is two-way.

Primary Print Server and Secondary Print Server

In the event that a customer has configured the use of 1 or more Secondary Print Servers to be used in conjunction with a Primary Print Server, the servers communicate together using port 443 and HTTPS for the purpose of facilitating workload distribution.

Job Agent Client and Job Agent Service

When Local Print Optimization is enabled and a client queue job is submitted by the user, the Job Agent Client will store a copy of the job locally, but will also send a copy of the job to the Job Agent Service that hosts the shared client queue (used for driver download). The job is sent via a web service call from the client to the print server using HTTS (port 443). The backup files will be stored in the same directory as network queue jobs on the Print Server. This is a configurable location that can be uniquely defined for each Print Server. The default location is:

C:\ProgramData\Xerox\XMP\CompatibleJobTickets\Jobs

When Local Print Optimization is enabled and a client queue job is released to a printer, the preferred print path is from the client workstation to the printer. If the client cannot be reached to release the job, the Workplace Suite server will notify the printer server and the backup copy will be sent to the printer.

Job Agent Service/Client and Printer Communication

When a job is released for printing, the Job Agent Service / Client submits a print ready file to the printer. The default submission method is Port 515 (LPR). Raw IP (Port 9100) over TCP/IP can also be used as well as IPP over SSL (Port 443). For Raw IP printing, the port is configurable.

External Communication Between Xerox® Workplace Suite Service and Xerox® Cloud Services

Except for incoming email, by default Xerox® Workplace Suite cannot be accessed from outside the company network. The administrator enables this workflow and may choose to limit it to only users which are operating within the company network.

The Windows Azure Service Bus is a Microsoft Cloud based messaging system that Xerox leverages to establish a secure application to application connection allowing select communication between approved clients outside a company's network to leverage services within a company's solution. While the Windows Azure and Xerox hosted service provide the secure connection path to the service, access to the Xerox® Workplace Suite continues to be controlled by the local Workplace Suite solution.

Xerox® Workplace Suite and the Windows Azure Service Bus

Xerox® Workplace Suite will only connect to the Windows Azure Service Bus if the mobile print option is enabled. During the provisioning process at set-up time an external URL is provisioned on the service bus then Xerox® Workplace Suite is configured to facilitate communication through that URL using an encrypted key. Workplace Suite initiates and maintains a connection to Azure service bus over HTTPS so that users using their mobile device over a public cellular or Internet connection can use the Mobile Print Workflow. The URL endpoint assigned is what various end clients (i.e., mobile devices) connect to.

Mobile Devices and the Windows Azure Service Bus

When the mobile device communicates with Workplace Suite through the Azure service bus, communication is always over HTTPS with a secure trusted certificate over the service bus URL allocated in the provisioning process. To mitigate the need for the user to type in the URL, a routing mechanism was created to allow URL discovery based on the user's email address domain. Users may be prompted for a company code if the login service is unable to determine which company they are associated with using the domain. Company code is used as a deciding factor to which account/service the user will authenticate/route against. Users have an option to always prompt for company code inside the settings view during login. This gives greater flexibility for a user to specify a certain company to be routed to upon login. The discovery and routing are facilitated through a Xerox® managed cloud-based routing service, which is discussed in the next section.

Mobile Devices and the Managed Cloud Based Routing Service

Mobile devices or other user interfaces may connect to the Managed Cloud Based Routing Service to determine what cloud endpoint is used for the remainder of the mobile print session. The routing service determines the cloud endpoint by the user's email address. If this service cannot resolve the external endpoint it may prompt the user for their company code to further resolve the cloud external endpoint. All communication between the mobile devices and managed cloud-based routing service is secure over HTTPS using TLS 1.2 (port 443) with a trusted certificate.

Xerox® Workplace Suite and LDAP / Active Directory Communication

LDAP / Active Directory Authentication

When configured for Enterprise Authentication, Workplace Suite verifies user credentials against Active Directory. Workplace Suite also queries Active Directory for information regarding trusted domains.

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

Active Directory Import

Xerox® Workplace Suite can be configured to import users from Active Directory. This capability is an extension of the setup used for LDAP / ADS Authentication. The Admin has the ability to configure the type of LDAP access (Anonymous, Basic, Negotiate) required when connecting the LDAP server. By default, the system is configured to use the Negotiate setting, which in turn instructs the Workplace Suite Server to use SASL when doing an LDAP Bind.

The Admin must supply user credentials that are in turn supplied to the LDAP server when performing an import (assuming they have selected either Simple or Negotiate for the Usage Mode. The credentials are stored in the Workplace Suite Server database (SQL), and are encrypted using SHA256 and AES.

As part of the import, the Admin can define the LDAP containers that are to be queried as part of the import and, in turn, map the fields within those containers to fields within the Workplace Suite User Database.

In order to communicate with Active Directory, Workplace Suite uses the Active Directory Services Interfaces (ADSI) technology that is available in all Windows Operating Systems supported by Workplace Suite. The communication with the Active Directory servers occurs via the standard LDAP port 389 or via 636, if TLS is being used.

Active Directory On-Boarding Using Email

When a new user sends an email, Workplace Suite checks all of the domains configured for "Advanced" or "Advanced with Import" for the user entry matching the user's email address. If the user is found in Active Directory, Workplace Suite populates the user database with the data found in Active Directory.

Xerox® Workplace Suite and Microsoft Azure AD

Azure AD Authentication

When a Workplace Suite interface is configured for Azure AD authentication, the individual interfaces (User Portal, Printer Client and Print Portal Chrome extension) handle the credential access via OAUTH. For Web based interfaces (User Portal and Printer Client) the final results of the authentication request are returned to the Workplace Suite server by doing a post-back through the browser to the WS server using one of the following redirect URIs:

- https://<SERVER-NAME>/login/home/ProcessAzureAD
- https://<SERVER-NAME>/xeroxmobileprint/home/ProcessAzureAD
- https://<SERVER-NAME>/xeroxmobileprintnextgen/home/ProcessAzureAD
- https://<SERVER-NAME>/login/api/azure/logout

The Workplace Suite server is the entity that will query the user's profile and will request tokens. This communication is done via HTTPS over port 443. The endpoints used by the Workplace Suite server are:

- https://login.microsoftonline.com (retrieve access token)
- https://graph.microsoft.com (query user profile for configured fields)

For Native Apps, such as the Chrome extension, the results of the authentication request are returned directly to the caller. The Native App will then retrieve the access token and send it to the Workplace Suite server (via HTTPS). The WS server will make the call to the Graph API to query the user profile for the configured fields and update the user record in the DB if necessary.

Xerox® Workplace Suite and Identity Provider (SAML) Communication

SAML Authentication

SAML 2.0 authentication is supported as an authentication mechanism for the user 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 user portal in the user's browser. The user would enter their credentials which are sent back to the IDP. The Workplace Suite 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. In this case they are sent to the SAML Assertion Endpoint (*https://<XWS-Server>/login/home/ProcessSaml*). If the results are successful, the user is granted an access token. If the results are not successful, the user will be denied access to the Web Administration / User Portal. SAML communication is typically over TCP port 443 using TLS. Non-standard ports (e.g. 8443) are possible.

Communication Between Xerox® Workplace Suite and Xerox® Service Manager Connector

The Workplace Suite system can be configured to connect to the Xerox® Service Manager Connector in Azure in order to perform the following actions:

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

The connector is an intermediate between the Workplace Suite server and Xerox® Services Manager. The Workplace Suite sever never directly connects to the Service Manager. Each of these methods of synchronizing with Service Manager has its own configuration as well as specific limitations on the system as a whole. Connectivity to Service Manager can only be enabled if Workplace Suite has a license for "Managed Print Services". The Importing of Printers and Sites requires the SA to configure an Account ID as well as a Username and Password. Optionally, a Chargeback Code may be specified. For the Exporting of Job Data, the Admin need only configure the Account ID. They may optionally enable the "Obscure User Data" setting, which when enabled obfuscate all user data (e.g., User Name, Email Address, Accounting User Name before sending any data to the Service Manager server.

All communication between Xerox® Workplace Suite, the Xerox® Service Manager Connector and Xerox® Services Manager is over HTTPS (port 443).

Communication Between Xerox® Workplace Suite and Workplace Suite Reporting Service in Azure

The Workplace Suite Server collects system usage information on a daily basis and report this to the Reporting Service in Azure, an online Xerox service. The type of information being collected includes, but is not limited to, items such as:

- Version of Workplace Suite Software
- Type of SQL Database
- Associated Licenses
- Printer Details:
  - Number of Printers
  - Features that are enabled (Mobile Print, Authentication, Desktop Print, Printer Client, etc)
  - Xerox vs Non-Xerox

- Server Details
  - Operating System
  - Size of Memory
  - 32 vs 64 Bit
  - Microsoft Office: Installed, Activation State, Version
- Print Queues:
  - Number and Type (Outgoing, Incoming, Client, Network, Conversion Mode)
- Prints:
  - Number Succeeded, Failed, Deleted or Expired.
  - Release Mechanism: Email, Printer Client, Mobile App, Auto Release.
  - Print Job Summary: Number of Color Pages, Number Black & White Pages.
  - Document Types: Word, Excel, Power Point, etc.

Information is used to improve Xerox customer support as well as the performance and functionality of the product in future releases. No personal or customer sensitive information is collected.

This feature is enabled by default but may be disabled by the customer if desired. This setting resides on the following page: Company > Maintenance > System Health Dashboard > System Utilization.

Communication Between the App from the Gallery, the App Server, and the Xerox® Workplace Suite Server

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 / 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 the WS Server and the App Server. Data is both encrypted and signed to ensure authenticity and privacy. Encryption is done using an RSA algorithm with key size of 10240. Additional details on SSO can be found in section 7.9 Single Sign-On of this document.

4. Logical Access, Network Protocol Information

Protocols and Ports

The following table lists the standard default ports used by the Xerox® Workplace Suite. 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 and Print Portal Chrome Extension Ports

Protocol	Transport and Port Value	External URL (if applicable)	Use	Option	Component	Direction
HTTPS using TLS	TCP 443 (TLS 1.2)	https://xccsts.services.xerox.com	Authentication Routing	Non-configurable	App to WS Service	Out
HTTPS using TLS	TCP 443	https://xws-prod.servicebus.windows.net	Authentication, Job / Printer Listing, Initiate Print Conversion	Non-configurable	App to WS Service	Out
HTTPS using TLS	TCP 443	https://accounts.google.com	Authentication (for Chrome Single Sign-On)	Non-configurable	App to Google	Out
HTTPS using TLS	TCP 443	(Azure AD only) https://login.microsoftonline.com	Authentication (for Chrome)	Non-configurable	App to Azure AD	Out

Xerox® Workplace Suite Ports

Protocol	Transport and Port Value	External URL (if applicable)	Use	Option	Component	Direction
Azure Service Bus	TCP 80, 443	*.servicebus.windows.net	Handling Mobile App requests: Authentication, Submission, Job Listing, Print Release	Non-configurable	WS to ASB	Out
Cloud Routing Service	TCP 443 (TLS 1.2)	https://xccsts.services.xerox.com	Store or update mobile routing information for phone communication	Non-configurable	WS to Cloud Routing Service	Out
HTTPS	TCP 443		WS and DCE Communication	Configurable	WS to DCE	In/Out
HTTPS	TCP 443		WS uses this port to communicate with other WS servers. JAS and JAC also	Configurable	WS / JAS / JAC to WS	In/Out

Protocol	Transport and Port Value	External URL (if applicable)	Use	Option	Component	Direction
			request info using this port.			
Raw	UDP 9807		WS uses this port to notify JAC that a job is ready to be released (Messaging Mode)	Configurable	WS to JAC	Out
Raw	TCP 9907		WS uses this port to notify the desktop client (JAC) that a job is ready to be released (TCP/IP Mode)	Non-configurable	WS to JAC	Out
SQL	TCP 1433		Microsoft SQL Client to Server Communication for database queries and storing.	Non-configurable	WS to SQL Server	Out
LDAP	TCP 389		Authentication, User Look-up	Non-configurable	WS to ADS Server	Out
LDAPS	TCP 636		Authentication, User Look-up.	Configurable	WS to LDAP Server	Out
HTTPS using TLS	TCP 443	(Azure AD only) https://login.microsoftonline.com	Azure AD token retrieval	Non-configurable	WS to Azure AD	Out
HTTPS using TLS	TCP 443	(Azure AD only) https://graph.microsoft.com	Azure AD user profile attribute retrieval	Non-configurable	WS to Azure AD	Out
HTTPS using TLS	TCP 443		Azure AD authentication redirect URL	Non-configurable	Client to WS	In
HTTPS using TLS	TCP 443		EIP Registration, Configuration, Accounting, Scan Job Retrieval (Note: HTTPS preferred)	Non-configurable	WS to Printer	Out
HTTPS using TLS	TCP 443	(SAML only)	SAML Metadata file retrieval	Non-configurable	WS to IDP (e.g. ADFS)	Out
HTTPS	TCP 443		Print Authentication (Convenience Authentication)	Non-configurable	WS to/from Printer	In/Out

Protocol	Transport and Port Value	External URL (if applicable)	Use	Option	Component	Direction
HTTP	TCP 80		EIP Registration, Configuration, Accounting, Scan Job Retrieval (Note: HTTPS is used if enabled on the printer)	Non-configurable	WS to Printer	Out
SNMP	UDP 161		Printer Discovery, Configuration	Non-configurable	WS to Printer	Out
HTTPS using TLS	TCP 443	https://xsmconnector.services.xerox.com	Send Print History and Retrieve Printer List to/from Xerox® Services Manager Connector in Azure	Non-configurable	WS to Xerox Service Manager Connector	Out
HTTPS using TLS	TCP 443	https://xsmconnector.services.xerox.com	Send system utilization information to the Reporting Service in Azure	Non-configurable	WS to Reporting Service	Out
SMTP	TCP 25		Sending email responses	Non-configurable	WS to SMTP Server	Out
SMTP / TLS (Secure SMTP)	TCP 465		SMTP over TLS. TCP port 465 is reserved by common industry practice for secure SMTP communication using the TLS protocol.	Configurable	WS to SMTP Server	Out
POP3	TCP 110		Post Office Protocol version 3, enables "standards- based" clients such as Outlook to access the email server.	Configurable	WS to POP3 Server	Out
POP3 / TLS	TCP 995		POP3 over TLS uses TCP port 995 to receive encrypted email messages.	Configurable	WS to POP3 Server	Out
Exchange Web Services	TCP 443		Exchange Web Services used for receiving Email	Configurable	WS to Exchange	Out
IMAP	TCP 143		Internet Message Access Protocol version 4, may be used by "standards-	Configurable	WS to IMAP Server	Out

Protocol	Transport and Port Value	External URL (if applicable)	Use	Option	Component	Direction
			based" clients such as Microsoft Outlook Express to access the email server.			
IMAP/TLS	TCP 993		IMAP4 over TLS for securely receiving encrypted email messages.	Configurable	WS to IMAP Server	Out
NRPC	TCP 1352		Lotus Notes RPC. This is the API used between Lotus Notes and the Lotus Domino server. Communication between WS and Lotus Notes is via a local API on the same PC.	Non-configurable	WS (running Lotus Notes) to Domino Server	Out
HTTPS using TLS	TCP 443	https://graph.microsoft.com	Email send / receive for O365.	Non-configurable	WS to O365	Out
HTTP / HTTPS	TCP 80 / TCP 443		Administration using Web Admin Tool. If a certificate is already configured on the IIS default website it is used by Xerox® Workplace Suite. If no certificate is configured, WS creates a self-signed cert. The administrator has the option to load a certificate from a trusted authority later if desired.	Non-configurable	Browser to Workplace Suite Service	In
HTTPS	TCP 8443	https://gateway.websrvs.xerox.com	HTTP over TLS. Used to activate or validate a license. If the customer is using off-line activation, then this port is not needed.	Non-configurable	Workplace Suite Service to Xerox® Licensing Server	Out
IPP	TCP 631		Receipt of Mobile Jobs on phones using the iOS Native	Non-configurable	Mobile Phone to WS	In

Protocol	Transport and Port Value	External URL (if applicable)	Use	Option	Component	Direction
			Print feature. Always uses TLS.			
HTTPS	TCP 443		HTTP over TLS. Used to validate a Chrome browser or Chromebook single sign-on user with Google.	Non-configurable	WS to Google	Out
App Socket RAW or Windows TCP-Mon	TCP 9100		Print Submission of Copy Jobs	Configurable	WS to Printer	Out
LPR	TCP 515		Print Submission of Copy Jobs	Non-configurable	WS to Printer	Out
IPP over TLS	TCP 443		Print Submission of Copy Jobs. Encrypted print transfer.	Non-configurable	WS to Printer	Out
HTTPS	TCP 443		Single Sign-On requests.	Non-configurable	WS <-> Printer	In/Out
Raw	TCP 7778		Receive Card Swipe Data from Elatec TCPConv	Configurable	Network Appliance to WS	In
Raw	TCP 7777		Receive Card Swipe Data from Elatec TCPConv2	Configurable	Network Appliance to WS	In
Raw	TCP 2001		Receive Card Swipe Data from RFIdeas Ethernet 241	Configurable	Network Appliance to WS	In
HTTPS	TCP 443		Get Access Token, Job List, Release / Delete Jobs	Non-configurable	WS <-> GABI	In/Out
HTTPS	TCP 443		Load Balancer probe test: https://<xws_server>:443/Bula/Admin/ping	Non-configurable	Load Balancer to WS	In
ADWS	TCP 9389		AD Web Services, used for GMSA	Non-configurable	WS to AD	Out

Document Conversion Engine Server Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
App Socket RAW or Windows TCP-Mon	TCP 9100	Print Submission	Configurable	DCE to Printer	Out
LPR	TCP 515	Print Submission	Non-configurable	DCE to Printer	Out
IPP over TLS	TCP 443	Print Submission. Encrypted print transfer	Non-configurable	DCE to Printer	Out
HTTPS	TCP 443	WS and DCE Communication	Configurable	WS to DCE	In/Out

Print Server Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
SMB Print	TCP 445	Print submission to a network queue. Client Workstation to print server.	Non-configurable	Workstation to Print Server	In
DCE/RPC	TCP 1058	Network Print Queue Access and Driver Download. From Workstation Print Queue to Print Server or from Workplace Client to Print Server.	Non-configurable	Workstation to Print Server	In

Printer and Printer Client (EIP App) Ports

Protocol	Transport and Port Value	External URL (if applicable)	Use	Option	Component	Direction
HTTP / HTTPS	TCP 80 / 443		Retrieval of EIP Browser pages for display on the UI. Uses HTTPS by default. Authentication, Job Listing, Initiate Print Conversion, Azure AD Redirect	Non-configurable	Printer EIP App to WS Service	Out
HTTPS	TCP 443		Printer Authentication	Non-configurable	Printer to/from WS	In/Out
LPR	TCP 515		Print Submission	Non-Configurable	JAS/JAC/WS to Printer	In

Raw IP	TCP 9100		Print Submission	Configurable	JAS/JAC/WS to Printer	In
IPP over TLS	TCP 443		Print Submission	Non-Configurable	JAS/JAC/WS to Printer	In
HTTPS using TLS	TCP 443	(Azure AD only) https://login.microsoftonline.com	Printer Client Login using Azure AD	Non-configurable	Printer EIP App to Azure AD	Out

Job Agent Service (JAS) Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
Raw IP	TCP 9100	Print Submission	Configurable	JAS to Printer	Out
LPR	TCP 515	Print Submission	Non-configurable	JAS to Printer	Out
IPP over TLS	TCP 443	Print Submission	Non-configurable	JAS to Printer	Out
HTTPS	TCP 443	Configuration, Job Information, Print Release	Configurable	WS to/from JAS	In/Out
HTTPS	TCP 443	Receipt of print job back for Local Print Optimization	Non-configurable	JAC to JAS	In

Job Agent Client (JAC) Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
Raw IP	TCP 9100	Print Submission	Configurable	JAC to Printer	Out
LPR	TCP 515	Print Submission	Non-configurable	JAC to Printer	Out
IPP over TLS	TCP 443	Print Submission	Non-configurable	JAC to Printer	Out
DCE/RPC	TCP 1058	Network Print Queue Access and Driver Download. From Workplace Client to Print Server.	Non-configurable	Workplace Client to Print Server	Out
HTTPS	TCP 443	Configuration, Job Information, Print Release	Configurable	JAC to WS	Out
HTTPS	TCP 443	Upload of print job backup for Local Print Optimization	Non-configurable	JAC to JAS	Out

Protocol	Transport and Port Value	Use	Option	Component	Direction
Raw	UDP 9807	Notification of Print Job Release (Messaging Mode)	Configurable	WS to JAC	In
Raw	TCP 9907	Notification of Print Job Release (TCP/IP Mode)	Non-configurable	WS to JAC	In

Network Appliance Ports

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

iOS Native Printing Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
DNS-SD	UDP 53	Mobile Phone printer discovery using DNS.	Not-configurable	Phone to DNS Server	Out
mDNS	UDP 5353	Mobile Phone printer discovery on the local subnet using mDNS.	Not-configurable	Phone Broadcast on Local Subnet	Out
IPP	TCP 631	IPP Print submission to Xerox® Workplace Suite. Always uses TLS.	Not-configurable	Phone to WS	Out

User / Administrator Portal Ports (Browser on user Workstation)

Protocol	Transport and Port Value	Use	Option	Component	Direction
HTTP*/HTTPS	TCP 80*/443	User portal / admin portal connection,	Configurable	Workstation to WS	Out

Protocol	Transport and Port Value	Use	Option	Component	Direction
*** Optional**	* Optional	logon, view and set configuration.			
HTTPS	TCP 443	SAML 2.0 Authentication	Not-configurable	Workstation to IDP (e.g ADFS)	Out
HTTPS	TCP 443	Azure AD Authentication	Not-configurable	Workstation to Azure AD	Out

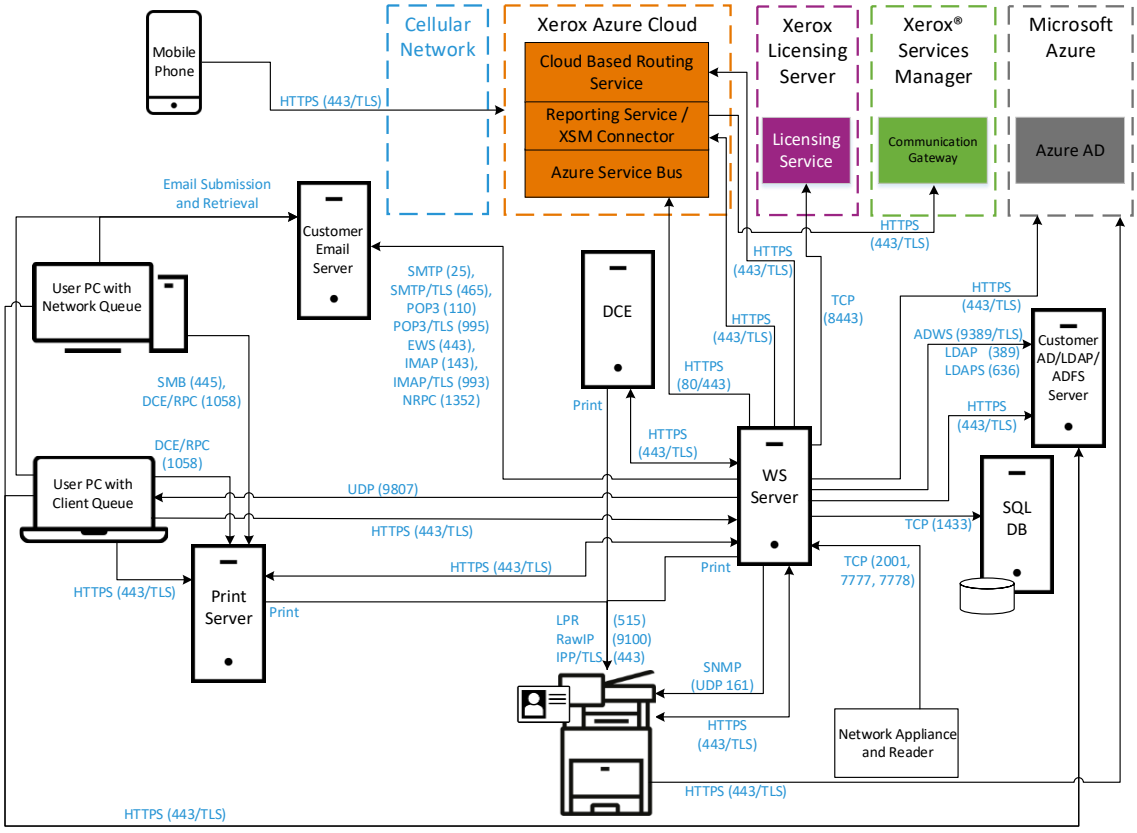
The default port for hosting application web pages is 443 using HTTPS. If HTTPS cannot be used (for example, it is prohibited in a specific region), HTTP over port 80 can also be configured. Both ports can run simultaneously.

Port Diagram

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

Network Port Diagram

Xerox® Workplace Suite – Network Port Diagram



5. System Access

Xerox® Workplace Suite (Web Administration Portal)

When accessing the Xerox® Workplace Suite directly (i.e., the User Portal for administrative access), the administrator connects to:

https://<webserver_address>/Login/

The user provides credentials to log into the User Portal based on the configurated authentication type:

- Email and Confirmation Number
- LDAP Authentication
- Windows Integrated Authentication
- Azure AD
- SAML Authentication

The user must exist in the WS user database and must be assigned either the “Administrator” role or the “Power User” role. Please note that the “Power User” role provides access to all web administrator tabs except for the “Company” tab.

For Windows Integrated Authentication, Workplace Suite will use the identity of the current Microsoft Windows session to look up the user in its SQL database. If the user exists, then they are logged into the User Portal without having to provide credentials.

If Azure AD is enabled as the authentication system for the portal, then the browser will directly communicate with Microsoft Azure AD using the OAUTH interface via HTTPS port 443. The initial Azure AD request will be directed to: https://login.microsoftonline.com.

If SAML is enabled as the authentication system for the portal, then the browser will direct the authentication to the configure SAML Single Sign-On URL for the customer Identity Provider, typically over port 443 (but could be a non-standard port).

Xerox® Workplace App (Print Portal)

When accessing the Workplace App, users need to provide their email address. WS looks 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 are prompted to enter either their Xerox® Workplace Suite Confirmation Number, or their company LDAP credentials (DOMAIN\USERNAME and PASSWORD). When using LDAP, the Domain is used to route the LDAP requests to the correct Agent, which in turn communicates with the ADS/LDAP server.

The results of successfully authenticating with WS is an access token. The token is stored on the phone and used for subsequent communication with WS. The lifetime of the access token configurable. Prior to the token expiring, the phone obtains a new token, which requires the use of the user’s login credentials. The Workplace App stores 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 deletes any saved data including the credentials when the application gets un-installed.

Some customers have security concerns about providing authentication credentials (even though they are always encrypted) on their mobile phone using the internet or through their wireless provider (3G/4G). For accounts with this concern, the WS provides a configuration option which forces Workplace App user authentication to take place only on the corporate LAN. Once authentication has taken place, users are then allowed to use the app on networks outside of their company LAN for printing. This option is disabled by default.

Workplace Client

The Workplace Client needs to access the enabled client-based queues hosted on the Print Server(s) in order to download and install the print driver for each client queue. By default, the Workplace Client runs as an NT Service on the workstation and uses the Local System Account when attempting to connect to the Print Server hosting the client queue. If these credentials are not valid, the user may supply different credentials using the Sys Tray utility installed with the Workplace Client. The supplied credentials are then used by the Workplace Client NT Service when accessing the Print Server queues to retrieve the driver. Credentials are stored in the system registry of the workstation. The password is encrypted using SHA1-AES.

Print jobs submitted via the Workplace Client always use the network username of the person logged into the workstation as the job owner.

The Workplace Client DLLs are signed to ensure the integrity of the components are runtime.

Printer Client (EIP App)

To access the Printer Client App, users either need to log into the printer via the Convenience Authentication feature and then select the Printer Client App, or they need to log into the EIP App itself. The Workplace Suite administrator also has the option of allowing an external authentication mechanism (something other than the Workplace Suite itself) as an approved authentication service. So a user can authenticate themselves at the printer with the external service, and if they then select the Workplace Suite Printer Client App, the App pulls the logged on users credentials from the session (network username and email address) and if these values map to a user in the Workplace Suite database, then the user has access to their print job(s) for release at the device. [Note: the ability to use an external authentication mechanism is off by default].

The Printer Client (EIP App) never saves the user's credentials. The user can log out of the EIP App manually but selecting the "Exit" button in the App, or by navigating out of the App (e.g., selecting the All Services, Machine Status, or Job Status buttons on the UI panel). The UI itself has a built-in inactivity timer that logs 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 EIP App itself has its own 5-minute timer. The EIP App timeout logs the user out of the App after 5 minutes of use, unless they dismiss warning pop-up, which restarts the 5-minute timer.

User Portal

When accessing the User Portal, users connect to:

https://<webserver address>/Login

The user must exist in the WS user database, and the user record must be enabled and not locked out. The administrator can configure the type of authentication that will be required to access the User Portal. The supported methods include:

- Email and Confirmation Number
- LDAP Authentication
- Windows Integrated Authentication
- Azure AD
- SAML Authentication

For Windows Integrated Authentication, Workplace Suite will use the identity of the current Microsoft Windows session to look up the user in its SQL database. If the user exists, then they are logged into the User Portal without having to provide credentials.

If Azure AD is enabled as the authentication system for the portal, then the browser will directly communicate with Microsoft Azure AD using the OAUTH interface via HTTPS port 443. The initial Azure AD request will be directed to: https://login.microsoftonline.com.

If SAML is enabled as the authentication system for the portal, then the browser will direct the authentication to the configure SAML Single Sign-On URL for the customer Identity Provider, typically over port 443 (but could be a non-standard port).

The only setting or configuration available to the user using the User Portal is the configuration of Release Permissions for the Printer Client.

Print Portal Chrome Extension

When accessing the Chrome Extension, users need to provide their email address. WS looks 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 are prompted to enter either their Xerox® Workplace Suite Confirmation Number, their company LDAP credentials (DOMAIN\USERNAME and PASSWORD), or they are redirect to Azure AD to complete the logon process. When using LDAP, the Domain is used to route the LDAP requests to the correct Agent, which in turn communicates with the ADS/LDAP server.

The results of successfully authenticating with WS is an access token. If Azure AD authentication is used, the lifetime of the WS access time will be set to match the lifetime of the Azure Access Token. Once the token expires, the user is required to provide login credentials. The access token is stored locally in the browser for that user session.

6. Additional Security Items

Auto Release via Network Appliance Workflow

Held print jobs are released automatically as soon as 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 Suite to control the release of user documents to printers that do not support the use of 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 WS 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 WS:

- RF Ideas Ethernet 241
- Elatec TCP Conv2
- Elatec TCP Conv

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

The listeners use these default ports:

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

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

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

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

Audit Log

The Xerox® Workplace Suite maintains a history of the users that have logged in WS via any of the interfaces: Workplace App, Printer Client, or Convenience Authentication. Entries are maintained for a period of 1 year. Entries older than that are purged from the log.

DMZ Configuration

The Azure service bus public endpoint is the typical configuration when a customer wants to allow users outside the network to access the Xerox® Workplace Suite. However, there are some customers who wish to allow users outside the company network to access the Workplace Suite, yet they do not want to allow documents to be passed through the Microsoft owned cloud.

Xerox® Workplace Suite supports a configuration where the customer can set up a satellite pass-through server in a DMZ, which is accessible from outside the network. This server is configured as the external endpoint in a private configuration, and all data sent to it is forwarded to the internal server.

The communication between DMZ servers and internal servers is secured. Before a DMZ server can communicate with an internal server, the DMZ server must authenticate with a valid username/password for the internal server. Once this authentication is successful the DMZ server receives a token that is used for all further communication. This token is required for all communication to the internal server.

DMZ Setup

In order to enable the DMZ feature, the Workplace Suite Server must be set to “Private” mode. When inside of your company firewall, Mobile App users are able to access WS via the Internal Server endpoint. When outside of the firewall, Mobile App users can access WS via the External Server endpoint.

DMZ Setup requires that a server be set up which has an external network connection to the Internet. The Workplace Suite software needs to be installed on this server and configured to support the DMZ feature. The setup entails pointing the DMZ server at your WS server and supplying administrator credentials which are used by the DMZ server when connecting to the WS server.

All DMZ configuration is done using HTTPS communication over port 443. The connection is initiated by the DMZ server, and can be trusted by the WS server based on the supplied administration credentials.

Mobile Devices and the DMZ Server

Mobile devices or other user interfaces may connect to the DMZ Server to access their Workplace Suite Server when they are external to the company’s network.

All communication between the Mobile Print App and the DMZ Server is over HTTPS (port 443).

Mobile Login using a Company Code

The mobile app can be configured to prompt for a company code at logon time. When configured to do this, the app queries the Azure Service Bus to find the DMZ Server end point. After which, all communication between the mobile app and the Workplace Suite Server is directly between the mobile phone and the DMZ server. User validation of credentials and transmission of all jobs occurs between the phone and the DMZ Server.

Mobile Login using the Private Access Control

The mobile app can be configured with using the Private Access Control feature, such that the app points to the DMZ server for all communication. With this configuration, the mobile app never accesses the Azure Service Bus. To perform this setup in the mobile app, Users can manually enter the link (as provided by their Workplace Suite Administrator), or the Admin has the ability to

push out an email to all users which includes a link that, when selected from a Mobile device, updates the configuration of the App and makes it point to the desired external URL.

Debug Logs

The Workplace Suite server uses logging to help diagnose issues and problems. User credentials (e.g., passwords or confirmation numbers) are never logged.

Workplace Suite Server Windows File Structure

The Workplace Suite Server stores files in the install location: %ProgramData%\Xerox\XMP

Smartcard (CAC/PIV) Integration

The Workplace Suite solution may be used with external authentication mechanisms, including CAC/PIV card authentication. Many Xerox advanced office products support smartcard integration, which is built into the Xerox® multifunction device (MFD) itself. Smartcard authentication is not performed directly within Xerox® Workplace Suite. Instead, the authentication of the user is performed between the printer, the smartcard and the Domain Controller at the customer site. The Xerox® Workplace Suite can be configured to allow users authenticated by an external system (i.e. something external to Workplace Suite) to access the printer client (EIP App) using the logged-on user identity. This removes the need for the user log into the Workplace Suite Printer Client. Users see their list of jobs after starting the app and may select and release them as desired.

The Workplace Suite server must be configured to allow the logged-on user (using an external authentication mechanism) to access the Printer Client. This is done using the following settings from the Web Admin Tool:

Company > Policies > Security > Printer Client

- Enable “Logged on Users (Access Card)
- Enable “External Printer Authentication”.

The Workplace Suite server must also be configured such that the “Alternate Access Card User” field for each user in the User database is populated. Typically, this field is populated from LDAP using the UPN (universalprinciplename) field. In a typical customer environment using this capability, a user logged onto the Printer would normally have an identifier something like:

- username@domain (UPN)

When that same user submits jobs from their PC, the user identity typically has a format of:

- DOMAIN\username

Enhancements to the Xerox® Workplace Suite server, allow the matching of the UPN value to the DOMAIN\username value, so that the user may be presented with their list of jobs and release them from the Printer Client (EIP App).

Printer Client Release Permissions

The Printer Client (or EIP App) provides an interface on some Xerox devices to view and release the user’s printer jobs. This includes both Mobile Print jobs and Print Management Workflow

submitted jobs. By default, only the user that submitted a job will be allowed to view and manage their jobs. However, the Xerox® Workplace Suite system allows users to grant access permission to other users in the system to view and manage their jobs. This feature is available when the User Portal interface has been enabled.

Company > Policies > Security > User Portal

Once enabled, users may log into the web portal:

https://<server>/login

After logging into the web portal, users have access to the Delegation tab, allowing them to both view the list of users which have granted them permission to access their print jobs using the “Print Theirs” tab. They may also grant permission to other user users to access their print jobs. Details on this functionality can be found in the administration guide for this solution.

Release permissions are only supported via the Printer Client. This configuration does not impact any other interface (e.g., Workplace App). Users can always view the list of users that have been granted release permission to their documents and they may revoke that ability at any time.

To help distinguish who is releasing a job versus who originally sent it, the job history (Jobs > History) and reports (Reports > Job Reporting) summary have been updated for the CSV export capability to include “Printed By Email” and “Print By User Name” fields. These fields are populated with corresponding information from the person that released the job to the printer using the Printer Client.

Administration Recovery

The Administration Recovery Procedure is used to log in to repair settings that prevent you or another

Administrator from logging in. This procedure allows you to assign a new Administrator, repair email, LDAP, and other settings. When using this feature, the User Portal authentication mechanism is reset to “Email and Confirmation Number”. If this is not the preferred login method, change the User Portal authentication method back to your desired configuration. To access the Administration Recovery Procedure, you must use Domain or Workstation local user accounts that satisfy either of the following requirements:

- The User must be in the “Administrator” group of the server.
- The User must be in the “MPAdmin” group of the server

Details on using the feature can be found in the Administration and Configuration Guide.

Single Sign-On

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

- All communication is over HTTPS.
- The WS server validates the certificate of the App Server vault. The certificate must be from a well-known and trusted provider, or it must exist in the trusted root certs on the server (e.g., if generated from a local certificate authority).
- The SSO authentication data for a given user and app is given to the WS Server in an encrypted format. The WS 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 WS for storage].

- Exchange of sensitive information between WS and the App / App Server uses public key cryptography with asymmetric keys. Each side (WS and App Server) has its own public and private keys, and shares the public key with the opposite side, but keeps its private key hidden. Data is encrypted by the public key and then sent to the owner of the private key to decrypt it.
- All message exchanges related to authentication data include digital signatures, so that the receiver can always validate that the request is coming from a trusted entity.
- Messages containing authentication data include 3 levels of encryption:
  - The channel is encrypted via HTTPS.
  - Message content is encrypted using public key cryptography with asymmetric keys. An RSA algorithm is used for encryption with a key size maximum of 16384.
  - Authentication data is encrypted by the Gallery App or its backend server prior to storing it with WS. 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 on the WS Server. 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 WS, and then encrypts that data using the public key of WS.
2. That data is then signed by the App Server using its own private key.
3. When this data is received by WS, it validates the signature using the public key of the Gallery App Server.
4. The message is then decrypted by WS using its private key.

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

Desktop Client Failover Mode

In order to improve the user experience of the Workplace Suite Client for scenarios where the solution is not able to communicate with the main server (such as networking issues or the service is temporarily down), a special offline printing mode is supported. In such cases, the user will be notified of the connection issue when they attempt to print to a Workplace Suite client queue. They will be given the option to submit the job 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 recently used printers on that workstation, and will be updated every 24 hours with the most recent set of printers. This file includes information like the name of the printer, IP Address, MAC Address, Manufacturer, Model, Site, Printer Language, 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 Workplace Server is re-established.

When printing using the Failover Mode, print Rules and Quotas will not be applied. If Content Security is enabled, the client will cache a list of the configured content profiles and search strings. This list is updated once per day with the current content profiles. Jobs processed while in failover mode would be compared against the cached profiles and matches would be stored along with the print job metadata. This information would be sent back to the Workplace Suite server once connection is re-established.

Cached printer information and content security information, as well as job metadata for failover jobs is stored by default in the following location:

- C:\ProgramData\Xerox\XMP\CompatibleJobTickets

GABI Integration

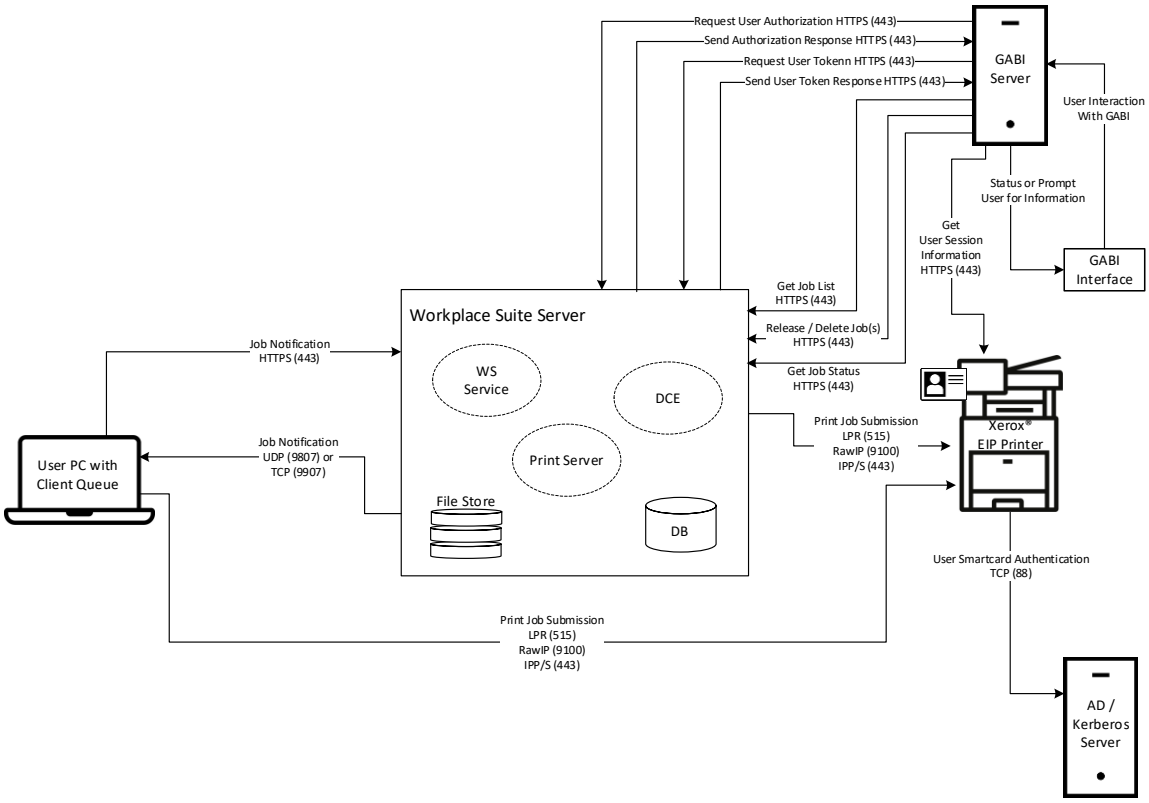
The XWS solution supports integration with GABI Solutions, which is a product commonly used to support contactless voice-to-command support to office equipment. This product is typically used in environments that require 508(c) compliance, allowing users with disabilities to easily access printers and multi-function devices. This capability is only available with a special Trusted Application license.

The Xerox® Workplace Suite solution and GABI Solutions product can be configured to allow users of an appropriately configured Xerox printer to access and release their Workplace Suite print jobs using the Gabi solution. This solution integration is based on the following points:

- Both the WS and GABI server-based solutions are hosted on-premise.
- The Xerox printers are configured for Smartcard login.
- The WS and GABI servers have been configured to create a trust relationship between the GABI solution and the WS solution, allowing a user logged on the printer to get their WS job list and release and/or delete their queued jobs using GABI.
- The trust relationship between the two systems is based on a certificate key and singed requests coming from the GABI server.
- All communication between GABI and WS server is over HTTPS.
- The GABI system will get the identity of the user logged into the given MFD and will then request a user access token for that user. The WS server will validate the requestor based on the passed in public key and signature, and grant the GABI solution a token.
- The token has a short lifetime.
- The token is return via a registered URL that was previously configured on the WS server.

Below is a diagram of the GABI and Workplace Suite system interaction when releasing a stored job(s). This assumes that the appropriate configuration between the WS solution and GABI system has already been done, which establishes the trust relationship between the two systems.

GABI and Workplace Suite Architecture (Job Release)



Workplace Suite and GABI Communication Diagram

Load Balancer HTTP Probe

In environments where there are multiple Workplace Suite servers connected to the same database, it is common to put the Workplace Suite servers behind an HTTPS load balancer. Printers, Desktop Clients, Print Servers and DCE's will all communicate through the load balancer when attempting to interface with the Workplace Suite servers. The Workplace Suite servers support the ability for the load balancer system to perform an HTTPS probe to test the state of the server (is the server up and functioning properly so that requests can be routed to that system). The probe endpoint used by the load balancer should be:

https://<server_ip_address>:443/Bula/Admin/ping

The load balancer can use either http or https for the above probe endpoint. The load balancer should send an HTTP GET request to the configured endpoint and the Workplace Suite server would return a response of 200 (ok). Anything else should be treated as the Workplace Suite server being unavailable.

7. 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/