VERSION 5.8
MAY 2024
702P09255

Xerox® Workplace Suite

Administration and Configuration Guide

xerox™

Contents

Overview

This chapter contains:

Xerox® Workplace Suite Mobile Print Workflow Software Overview

The Xerox® Workplace Suite Mobile Print Workflow Basic and Premium Software allows users to print office documents, photos, and print-ready files such as PDF, TIFF, and more, using a mobile device. Users can submit documents using either email or the Xerox® Workplace Mobile App, with the ability to select various printing options. You can print documents immediately, or for sensitive content, you can release documents at the printer using a system-generated code. These abilities are accomplished without the need for print drivers or special software.

The Xerox® Workplace Suite Mobile Print Workflow Software works with Xerox printers, both EIP-enabled and non-EIP enabled, and non-Xerox Printers. You can use various methods to submit and upload files, and print documents. Xerox® Extensible Interface Platform® (EIP) is a software platform inside many Xerox multifunction printers. The EIP software enables personalized and customized solutions that are accessible from a printer touch screen.

Print documents immediately:

- Using your mobile device, select a document. Use the Open-With or Open-In Xerox® Workplace Mobile App. Select your printer and print options, then select **Print**.
- Using the name or IP address of your printer in the subject line, send an email to the Xerox® Workplace Suite Mobile Print Workflow Software. Your document and email body prints automatically.

Mobile Print Workflow Document Conversion Options:

- **Built In Document Conversion print engine** - The default conversion engine when Microsoft® Office is not installed.
- **User-Supplied Copy of Microsoft® Office 2016** - You can use Microsoft® Office 2016 as your document conversion engine by installing your own licensed version of Microsoft® Office 2016 Professional.

Upload documents to print later:

- Send an email with your office documents or photos to the Xerox® Workplace Suite Mobile Print Workflow Software incoming email address.
- Use the Document upload feature in the Xerox® Workplace Mobile App.
- Send documents from your workstation to the Mobile Print Incoming Print Queue.

Print uploaded documents:

- From the Xerox® Workplace Mobile App.
- From a Workplace Suite Print Client-EIP-enabled device.

Xerox® Print Management Workflow Overview

The Xerox® Workplace Suite Print Management Workflow allows access control to Xerox multifunction printers that have Convenience Authentication (CA) capability. Users can gain access to the multifunction printer through card swipe or the following alternate login methods:

- Primary PIN Number and an Access Card Number
- Personal, random Confirmation Number that is emailed to the user
- LDAP credentials

The Xerox® Workplace Suite Print Management Workflow supports immediate printing to a device and submitting documents to a print queue for later release at a device.

Print Management supports the following print architectures:

- A centralized printer server where print jobs are held on a Workplace Suite server while awaiting release.
- A local client based print model where jobs are held on your computer while awaiting release.
- A Direct Print path where jobs are submitted directly to a printer for immediate release.

The Print Management Workflow incorporates a Direct Print feature for desktop printing direct to a printer. Direct Print supports Network Queues and Workplace Client queues. For further information, refer to Direct Print.

The Xerox® Workplace Suite Print Management Workflow works with both Xerox and non-Xerox devices. For Xerox devices with Extensible Interface Platform (EIP) capability, Print Management supports card-based authentication, and an EIP application. This combination of features allows you to authenticate and choose which jobs you want to print.

The Secure Print feature means that print jobs sent through the Xerox® Workplace Suite Print Management Workflow are not released until the user releases the job at the printer control panel. You can release print jobs on Xerox multifunction printers using the Convenience Authentication feature, or on Xerox or non-Xerox devices using a network appliance that permits card swipes.

Xerox® Workplace Suite Print Management Workflow runs on a Windows server and expects to interface with several network components: A database, either on the same server or on an external server, and optionally, an email server and LDAP user directory, and one or more print servers. The database contains all the data associated with the Workplace Suite software installation. When the choice for alternate login is Confirmation Number, an email server is required .

The LDAP user directory contains a master list of users that the Workplace Suite synchronizes, allowing the list of users to be maintained in a single place. You can configure the Workplace Suite in many different print server variations. The primary Workplace Suite server can host the print server by itself, or with one or more secondary print servers, to distribute the print job load. The primary Workplace Suite server allows each workstation to act as a client print server with client software. Print jobs are held on the workstation until a print release causes the job to spool directly to the requesting printer.

Xerox® Workplace Suite Print Management Workflow has certain conventions for printer management and organization. The administrator finds tabs dedicated to Printers, Print Queues, and Pull Groups.

- A Printer is the physical definition of the IP Address, printer model, installed Xerox® Print Management Workflow features, and other relevant information used by the Xerox® Workplace Suite Print Management Workflow, or by the system administrator.
- A Print Queue is the Windows Printer definition for the print driver, appropriate print settings, and user-facing printer name.
- A Pull Group is the logical grouping of Printers and Print Queues, in a many-to-many relationship. When a user chooses a Print Queue when printing from an application, users can use the Print Release feature from any Printer grouped with that Print Queue.

Printers used within a Workplace Suite Server network can be Xerox multifunction printers with theConvenience Authentication feature, Xerox multifunction printers, printers without Convenience Authentication, or non-Xerox devices. The Print Release feature for devices that do not support Convenience Authentication is managed by the use of network appliances. When a user swipes a card at a network appliance or card reader, the print jobs for that user are released automatically at the associated printer.

There are various reasons why different Print Queues are used. Print Queues are available in two basic types: Pull Print Network Queues, which reside on the print servers and are shared to the workstations, and Pull Print Client Queues, which get pushed from the print server to the workstation client. A given Print Queue can be defined only with a single print driver. If multiple device types are incorporated into the system, a Print Queue with a compatible driver is required for each device type, or types that could be grouped. You can create multiple queues to distribute the print job load across multiple servers.

Pull Groups are used to group logically the printers and print queues. Printers can be grouped for many reasons. For example, the printers all use a compatible print driver based on printer features. You can group printers that have the same attached finisher. When printers are in the same building, you can group printers based on physical location. Printers from different manufacturers or in different geographical locations are not typically grouped.

Users are added to the database through LDAP synchronization, manually by the system administrator, imported using CSV files, or onboarded by each user through LDAP look-up as they begin to use the system. If LDAP synchronization is used, additions, deletions, and modifications to the LDAP directory can be scheduled regularly to keep the Workplace Suite database up to date.

Xerox® Content Security Workflow Overview

The Xerox® Content Security Workflow identifies business documents that contain information in electronic or paper form. These documents are labeled to restrict distribution and use.

Some business documents are labeled and maintained for operational, legal, financial, or historical purposes. Labels for these documents can include strings to track, such as For Internal Use Only, Business Confidential, or other terms. Tracked documents can include intellectual property, company secrets, details of business decisions or transactions, future product information, competitive information, or other objectionable content.

With the Content Security Workflow enabled, an administrator can create global content profiles and set search strings to track identified documents processed at printers. These documents, are searched to see if they match an existing Content Profile. When a match is found, email alerts are sent to a list of recipients. Content Profiles consist of one or more user-defined search strings. For example, search strings can include words like “private data”, “internal use only,” or the name of a future product.

For more information, refer to the *The Xerox® Workplace Suite Content Security Workflow Guide*.

Setting Up your Installation for the Xerox® Print Management Workflow

SETTING UP THE USER LIST

Create the user database for the Workplace Suite installation in one of the following ways:

- **Lightweight Directory Access Protocol (LDAP) Synchronization**: Users can be added all at once through synchronization, or one at a time through onboarding, a means of self-registration in the system. In either situation, user account information is loaded into the Workplace Suite database from an LDAP server. Onboarding takes place the first time that a user logs in at a print-management-controlled Xerox multifunction device. The process is used typically when some LDAP directory users do not need regular access to the printers.
- **CSV file import**: To add users to the user database, system administrators can import user data from a formatted CSV file.
- **Manual creation**: System administrators add users to the system manually.

For more information, refer to the Users chapter.

PULL GROUPS AND PRINTER ORGANIZATION

Printers and Print Queues are organized through the creation of Pull Groups. When a user sends a print job to a print queue, they can release only the print job on a printer available in the same pull group as the print queue. For detailed information on how to create and associate printers and print queues in pull groups, refer to the sections on *Printers, Print Queues and Pull Groups* in the *Xerox® Workplace Suite Administration and Configuration Guide*.

USER WORKFLOW CONSIDERATIONS

AUTHENTICATION

The typical means of authentication for a Xerox multifunction printer is to swipe a card at a card reader. If necessary, the system can be configured to allow authentication at the printer using the Alternate Login feature. You can use the Alternate Login feature with the Card Swipe authentication feature.

To configure authentication settings, access the Workplace Suite webpage. Select **Administration**, then select **Policies > Security > Printer Authentication**.

Authentication Modes

Access Card

When authentication is enabled on a printer, the default mode is Access Card swipe. This default mode is always enabled. For a printer with an attached USB Card reader, users swipe a card at the reader. If the Auto Registration setting is enabled from the Workplace Suite webpage, and a user swipes a non-registered Access Card Number, the user is prompted for the network username and password. If the user authenticates successfully, the Access Card Number is added to the user Primary PIN Access Card Number field. View the Access Card Number value on the user profile page.

Alternate Login Methods

Primary PIN and Access Card Number: The Primary PIN is the number of the card a user swipes at the card

reader. If the system administrator provides an Access Card Number to a user, the user enters the number on the printer control panel as an alternate login method. Sometimes the Primary PIN is too complex to remember easily, or, for security reasons, the system administrator can choose not to share the Primary PIN.

Confirmation Number

The confirmation number is system-generated, then emailed to the user at the email address specified for the user in the User Account. The system administrator sets the number of digits in the Confirmation Number. The Confirmation Number can be set to non-expiring or to expire after a set period of time. After the Confirmation Number expires, a new Confirmation Number is sent to the user. The system administrator cannot view the Confirmation Number. If a user forgets a Confirmation Number, there are two ways to reset it, the user can click on **Forgot Confirmation Number** on the Workplace User Portal login page or they can request the system administrator to reset their Confirmation Number.

LDAP Authentication

The Workplace Suite software synchronizes users with one or more LDAP servers. The Administrator can set the Alternate Login so that users provide LDAP credentials, including network username and network password.

Workplace Mobile App

QR Code, **NFC Unlock**, or **Unlock Code**

Note: To use the Xerox Workplace Mobile App QR Code and NFC Unlock feature, a Mobile Printing license is required. Refer to Unlocking a Printer Using the Xerox Workplace Mobile App®.

Card Authentication Usage Guidelines

The Xerox Workplace Suite offers users easy access to Xerox printers with Multiple Access Cards, Multiple Primary PINs, or Access Card Numbers. Follow the *Workplace Suite Authentication and Usage Guidelines*.

General Guidelines

- Primary PINs or Access Card Numbers must be unique for all users. Duplicate numbers are not permitted.
- There is support for Multiple Primary PINs or Access Card Numbers for each user. To allow users to authenticate with multiple Access Card Numbers, select **Policies: Security > Printer Authentication > Advanced**. To enable, select **Allow Multiple Primary PINs or Access Cards**.
- One way to assign Primary PIN or Access Card Numbers from a user LDAP record requires LDAP Connections. To configure, select **Advanced** or **Advanced with User Import Usage Mode**. Configure the field mapping for the Primary PIN or Access Card Number entry to the corresponding field in the LDAP user record. When a user logs in using the LDAP credentials Alternate Login, Print Portal, or User Portal, the Workplace Suite database user entry is updated automatically.
- Another way to assign Multiple or Single Primary PINs or Access Card Numbers is using the User Import feature with a .csv file.
- Commas are not supported as Primary PIN or Access Card Number characters.
- When a Primary PIN or Access Card Number is imported using LDAP Import, and the LDAP field is blank, the current Access Card Number is not cleared for use. If you use the User Import feature with a .csv file to enter end-user data, and the LDAP field is blank, the current Access Card Number is not cleared.

Using the setting Multiple Primary PINs or Access Cards

- The Multiple Primary PINs or Access Cards setting is Disabled by default. To enable the setting, select **Policies: Security > Printer Authentication > Advanced**.
- When assigning a Primary PIN or Access Card Numbers using the AD LDAP Import feature, the Access Card Numbers are added to the existing Access Card Numbers in the user profile.
- When a user Auto Registers an Access Card Number, the Card Number is added to the existing Access Card Numbers in the user profile.
- You can enter Multiple Access Card Numbers or PINs manually in the Workplace Suite user profile.
- When the Allow Multiple Primary PINs or Access Cards setting is disabled, a user can have only one Primary PIN or Access Card Number.
- If you disable the Allow Multiple Primary PINs or Access Cards setting after it was enabled, all user PINs are deleted.
- To assign Multiple Primary PINs or Access Card Numbers, use the User Import feature with a .csv file. To add multiple PINs for a user, separate each PIN using comma.

Options to reassign a Primary PIN or Access Card Number to a new user

- Remove the Primary PINs or Access Card Numbers from the former user, then assign the numbers to the new user.
- Remove the badge that belonged to the former user. When onboarded, the badge is assigned to the new user.
- When using the LDAP User Import feature, the Alternate Login feature, or the User CSV File Import feature, the Primary PIN or Access Card Number updates.

SECONDARY PIN

If necessary for greater security, the System Administrator can set the Workplace Suite configuration to use a Secondary PIN. The Secondary PIN is not visible to the System Administrator in the User Account. If the Workplace Suite configuration uses a Secondary PIN, each user is prompted to supply a required Secondary PIN when they Authenticate into the Xerox multifunction device. Each time after that, before being allowed to use a device for the first time, users are prompted to supply the Secondary PIN.

For users who forget their Secondary PIN, they can request that the System Administrator clears their Secondary PIN. The next time that the user logs in at the device, a prompt appears to create a new Secondary PIN.

The Secondary PIN feature works with the following authentication mechanisms: Card swipe and the Alternate Login methods of Primary PIN and Confirmation Number. The Secondary PIN feature is ignored when used with the Alternate Login methods of LDAP Authentication.

JOB RELEASE

After a job has been submitted, it can be released for printing using the following methods:

- **Printer Client App**: A user can log in to the Workplace Suite Client application on a Xerox multifunction printer. Then the user can select and print any number of submitted jobs. This mode of release works on most full panel touch screen multifunction devices that support EIP.
- **Auto Release**: All user jobs can be released automatically using:

  - Authentication with USB card readers or alternate login
  - An External Network Card Reader, Network Appliance, on a non-Xerox printer
  - An External Network Card Reader, Network Appliance, on Xerox printers that do not support Convenience Authentication
  - Mobile Phone Unlock, requires a Mobile Print Workflow
- **Mobile App**: A user can log in to the Workplace Mobile App to select and print any number of submitted jobs. Requires a Mobile Print Workflow

For more information, refer to Network Appliances (External Card Readers) or Mobile Phone Unlock.

NETWORK APPLIANCES (EXTERNAL CARD READERS)

Print Release for devices that are not locked using Xerox® Convenience Authentication can be completed using an external card reader plugged into a network appliance. Three different network appliances are supported by the Xerox® Workplace Suite Print Management Workflow:

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

The network appliances and external card readers are available in two basic types:

- Network Address Translation (NAT) appliances
- Independent network appliances.

A NAT appliance will sit between the printer and the network and takes on the printer's IP address. The printer will take on a private IP address behind the card reader. The card reader will be plugged into the network appliance rather than into the printer. The NAT appliance has very low administrative overhead as the combination of appliance and device will be mapped to the Xerox® Workplace Suite administration page as a printer.

Note: The Elatec TCP Conv2 is a NAT appliance.

The Elatec TCP Conv and RF Ideas Ethernet 241 are independent network appliances and will have a separate IP address from the printer they control for Print Release. Both the network appliance and the printer will be added individually to the Xerox® Workplace Suite administration page where they can be associated together.

Note: These readers are only recommended in networks with stable IP addresses.

The RF ID Ethernet 241 is the only network appliance that supports transport encryption.

Xerox® Workplace Suite Support

The following document is included on your Xerox® Workplace Suite Solution download:

- *Xerox® Workplace Suite Installation Guide*: Contains pre-installation requirements and software install procedures.
- *Xerox® Workplace Suite Major Upgrade Guide*: Use this guide for Xerox Workplace Suite SQL Configuration changes and upgrades from Print Management and Mobility Suite.
- *Xerox® Workplace Suite Minor Upgrade Guide*: Use this guide if you are upgrading from a previous release of Xerox Workplace Suite.

The following documents are available online:

- *Xerox® Workplace Suite Administration and Configuration Guide*: Contains information on configuration settings, licensing, and security.
- *Xerox® Workplace Suite Printer Client User Guide*: Contains information on how to send, retrieve, and print a job and use the enhanced Mobile Print email submission features. These features are available with select Xerox EIP-enabled devices only.
- *Xerox® Workplace Mobile App Quick Start Guide*: Contains information on how to start using the Xerox® Workplace Mobile App.
- *Xerox® Workplace Suite Troubleshooting Guide*: This guide can assist troubleshooting issues.
- *Xerox® Workplace Suite Print Management Workflow User Guide*: Contains information on how to use Print Management Authentication, Print Release, the Workplace Suite Client, and the Printer Client.
- *Xerox® Workplace Suite Content Security Workflow Guide*: Contains information on how to enable and use the security-related features of Xerox® Workplace Suite Content Security Workflow.

The most up-to-date documentation and software downloads are available at: www.support.xerox.com/support/xerox-workplace-suite.

To access the Xerox® Workplace Suite customer support forum, refer to: Workplace Suite - Customer Support Forum.

To access the Xerox® Workplace Suite customer support announcements, refer to: Workplace Suite Announcements - Customer Support Forum.

Xerox Global Print Driver

Xerox® Workplace Suite uses the Xerox Global Print Driver (GPD). The GPD natively supports many Xerox devices and will support others and non-Xerox devices in Basic Mode. In Basic Mode, some features, such as accounting or staple, may not be supported. For more information, search for Global Print Driver at www.xerox.com/XGPDdrivers. Select the **Documentation** tab for a list of supported products.

Workplace Suite Admin Tool User Interface

Accessing the Workplace Suite Admin Tool

The Workplace Suite Admin Tool is web-based and can be accessed remotely. Access is available through a supported Web browser, or at the Web server where the Xerox® Workplace Suite Software is installed. Logging in to an account with administrative privileges is required.

The default URLs are:

- Remote access: https://<webserver address>/login/
- Local access:https://localhost/login

You can access the user interface at the Workplace Suite server. Select **Start > All Programs > Xerox > Xerox Workplace Suite Administrator**

Note: To see context-sensitive help, move your pointer over the information icons on the user interface.

Logging in to the Workplace Suite Admin Tool

After you access the Workplace Suite Admin Tool, a login window opens. To configure the login method, select **Policies > Security > User Portal**. If you cannot access the Administration webpage, refer to Administration Recovery Procedure.

Logging out of the Workplace Suite Admin Tool

To log out of the Workplace Suite Admin Tool, select your user name in the upper right, then select **Logout**. You can use an alternate logout method: close the browser window.

Workplace Suite Admin Tool Layout

The layout tabs are:

1. **Company:** Contains settings for system operation, including the following subtabs:
   - **Company Profile**: Manage or edit your company profile.
   - **Settings**: Manage LDAP servers.
   - **Polices**: Manage data retention, EIP application, security, and workstation client settings.
   - **Workflows**: Manage Email, Mobile Application, iOS Native Printing, Desktop Clients, and Printer Clients settings.
   - **Licensing**: Manage a site base license and printer licenses.
   - **Maintenance**: Export system log files, view system health, and update printer models.
2. **Jobs:** Includes the following status subtabs:
   - **History**: List of printed jobs
   - **Current**: List of jobs currently printing or processing
   - **Content**: List of jobs currently registered available for printing from the workstations
   - **Unregistered**: List of jobs submitted by unknown users

Individual jobs or all jobs in the list can be deleted at any time.

3. **Printers:** Includes the following subtabs:
   - **Printers**: Manage the printers in your Workplace Suite Software. Printers can be added individually or in bulk using a .csv file.
   - **Printer Groups**: Provides ways to assign printers to groups.
4. **Print Queues**: Manage the print queues in your Workplace Suite Software deployment. You can add, remove, and edit the print queues in your environment.
   - **Print Servers**: Add or Delete secondary Print Management Print Servers
   - **Incoming Queues**: Display Incoming Queues
   - **Outgoing Queues**: Display Outgoing Queues
5. **Pull Groups:** Manage print pull groups by adding new groups, and editing or deleting existing ones.
6. **Discovery:** Used to add Discovery profiles for the Workplace Suite Software to scan the network periodically, to import printers into the system.
7. **Users**:
   - **Users**: Manage users of Workplace Suite Software and User Groups.
   - **User Groups**: Provides ways to assign users to groups.
8. **Reports**:
   - **Dashboard**: The dashboard provides predefined summary information for customers who use the Reporting capability of the Workplace Suite.
   - **User Audit**: Report on User access
   - **Job Reporting**: Report on usage by Users. If a printer is enabled for Usage Tracking on Workplace Suite, the report contains Network Accounting data. If Job Reporting is not enabled, the report contains only Workplace Suite job data.
9. **Permissions**: You can delegate print responsibilities for your jobs to other users.

License Options

Licenses may be offered in varying quantities and configurations. Contact your Xerox representative. For further information, refer to Licensing.

Company

This chapter contains:

Company: Company Profile

To add or update Company Profile information:

1. Click **Company > Company Profile**.

   The Company Profile appears.

2. Enter the **Details** information:
   - Company Name
   - Country
   - Address 1
   - Address 2
   - City
   - State/Province
   - Postal Code
   - Time Zone
3. Enter the **Administrator Information**:
   - First Name
   - Last Name
   - Email
   - Email Language
4. Enter the **Contact Information**:
   - Support Email
   - Contact link
   - FAQ link
5. Select **Save**.

Company: Settings

The Settings section contains information for the following features:

SETTINGS: FEATURE DEFAULTS

This section is used to configure default values for the main features and their options. These defaults are applied to any new printers which are added manually, and to any new discovery profiles that are created. It is possible that defaults will be overridden during printer or profile creation, or after creation by editing an existing printer or profile.

For detailed descriptions of Feature Defaults, refer to the Printers chapter.

SETTINGS: INCOMING MAIL AND OUTGOING MAIL

Note: The Incoming Mail feature is available with a Mobile Print Workflow license only.

Incoming Mail

The Incoming Mail server settings are used to configure the Xerox® Workplace Suite server, so that it can connect to the site mail server and retrieve sent emails from the end users.
The Mobile Print Workflow uses incoming email for the following purposes:

- You can attach your office documents or photos to an email, which can be released at the Xerox® Workplace Suite enabled printer.
- You can insert the name or IP address of the printer in the subject line and send an email to Xerox® Workplace Suite. Your document and email body prints at the printer automatically.

Outgoing Mail

The Outgoing Mail server settings are used to configure the Xerox® Workplace Suite server, so that it can connect to the site mail server and send emails to the end users. Depending on the workflows enabled, the

outgoing mail is used in different ways, as follows:

- Mobile Print Workflow: Used to send confirmation number to users.
- Content Security: When matched strings are found in a job, the content security feature uses the outgoing mail settings to send an email notification to the list of recipients.
- Print Management Workflow: Used to email a personal and random confirmation number to each user.
- Used to send email notifications to users, such as job printing status.

Incoming Mail and Outgoing Mail Server Types

Xerox® Workplace Suite supports the following email server types:

- Microsoft Exchange Web Services Settings
- Internet Message Access Protocol (IMAP) Settings
- Post Office Protocol 3 (POP3) Settings
- Microsoft Graph API Settings
- Simple Message Transfer Protocol (SMTP) Settings
- Notes Remote Procedure Call (Lotus Notes) Settings

Guidelines for Email Addresses

Receiving Email Address:

Note: Do not use your personal email address. Ensure that you use new email address for Mobile Print Jobs.

- The receiving email address is the email account that the server monitors for incoming jobs by email. Ensure that this email address is unique to the Xerox® Mobile Print Workflow.
- When you use the Mobile Print Workflow, the receiving email address is required.
- Ensure that receiving email address is associated with the incoming mail server user name and password.

From Email Address:

- The from email address is the address that end users see in the From area when they receive a confirmation email from the Xerox® Workplace Suite server.

Reply-to Email Address:

- The reply-to email address is the email address that end users see and use when they select **Reply-to** in response to the confirmation email.
- Customer service or technical support purposes use the reply-to email address.

Display Name:

- The name that users see as the originator of their confirmation email.

Settings for Incoming Mail

To configure the Incoming Mail settings, do the following:

1. Click **Company > Settings > Incoming Mail**.

   The Incoming Mail Server Settings window appears.

2. In the Server Type section, select one of the following options:

   - **Internet Message Access Protocol (IMAP)**: For more information, refer to Internet Message Access Protocol (IMAP) Settings.
   - **Microsoft Exchange Web Services**: For more information, refer to Microsoft Exchange Web Services Settings.
   - **Post Office Protocol 3 (POP3)**: For more information, refer to Post Office Protocol 3 (POP3) Settings.
   - **Notes Remote Procedure Call (Lotus Notes)**: For more information, refer to Notes Remote Procedure Call (Lotus Notes) Settings.
   - **Microsoft Graph API** For more information, refer to Microsoft Graph API Settings.

3. In the Server Information section, enter the required information in the fields.
4. If the Login Information section appears, enter the required information in the fields. For more information, refer to Login Information.
5. To verify that the test connection is successful, click **Test Connection**.
6. Click **Save**.

Settings for Outgoing Mail

To configure the Outgoing Mail settings, do the following:

1. Select **Company > Settings > Outgoing Mail**.

   The Outgoing Mail Server Settings screen appears.

2. In the Server Type section, select one of the following options:

   - **Simple Message Transfer Protocol**: For more information, refer to Simple Message Transfer Protocol (SMTP) Settings.
   - **Microsoft Exchange Web Services**: For more information, refer to Microsoft Exchange Web Services Settings.
   - **Notes Remote Procedure Call (Lotus Notes)**: For more information, refer to Notes Remote Procedure Call (Lotus Notes) Settings.
   - **Microsoft Graph API** For more information, refer to Microsoft Graph API Settings.

3. In the Server Information section, enter the required information in the fields.
4. If the Login Information section appears, enter the required information in the fields. For more information, refer to Login Information.
5. In the Test section, in the Email address field, enter an email address, then select **Send Test Email**.

   Verify that the test email is received in the associated mailbox.

6. Click **Save**.

Microsoft Exchange Web Services Settings

The software can connect to a Microsoft Exchange Server 2007 or later using Exchange Web Services (EWS). This connection is made over the HTTPS protocol. The software can authenticate using either Basic Authentication or Impersonation. With Basic Authentication, the username and password are sent securely to the Exchange Web Services server for authentication. When Impersonation is used, the software logs in as the impersonated user for the duration of the EWS connection. Login credentials for the software system are required for the impersonated user.

Incoming Mail Settings

- Server Address: Use this area to manually override and specify a URL for the EWS server. This value is given to you by the company IT department. It is recommended that you use the Auto-Discover option.

  Note: If you specify a manual URL and it later changes, all email capabilities stop functioning.

- Receiving Email Address: The email address to be used by Mobile Printing.
- Polling Rate: The rate at which to poll for emails. For more information, refer to Polling Rate for Incoming Email.
- Domain Name: The domain that is used by the software.
- User Name: The user name that is used to connect to Exchange Web Services.
- Password: The password that is used to connect to Exchange Web Services.

Outgoing Mail Settings

- Server Address: The name or IP address of the outgoing email server
- From Email Address: The email address which the users see as the originator of their confirmation email
- Reply-to Email Address: The email address which the users can reply to when responding back.
- Domain Name: The domain that is used by the software.
- User Name: The user name that is used to connect to Exchange Web Services.
- Password: The password that is used to connect to Exchange Web Services.

Internet Message Access Protocol (IMAP) Settings

Incoming Mail Settings

- Server Address: The name or IP address of the incoming email server, for example, `imap.adomain.com`, or `pop3.adomain.com`, or `xxx.xxx.xxx.xxx`.
- Port: The default port number is `143`.
- Receiving Email Address: The email address that is used by Mobile Print Workflow.
- Watch Folder: If the **IMAP Protocol** server type is enabled, the Watch Folder field appears. You can enter the location for Xerox® Workplace Suite to check for Email submissions from users periodically, for example, `inbox`.
- Use Secure Connection: To establish an encrypted link between a web server and a browser, SSL (Secure Sockets Layer) is the standard security technology used. For more information, refer to Using a Secure Connection.

- Authentication Mode: To indicate the type of server authentication used, from the Authentication Mode menu, select one of the options. The recommended setting is **Auto**.
- Polling Rate: The rate at which to poll for emails. For more information, refer to Polling Rate for Incoming Email.
- User Name: The user name that is used to connect to Exchange Web Services.
- Password: The password that is used to connect to Exchange Web Services.

Post Office Protocol 3 (POP3) Settings

Incoming Mail Settings

- Server Address: The name or IP address of the incoming email server, for example, `imap.adomain.com`, or `pop3.adomain.com`, or `xxx.xxx.xxx.xxx`.
- Port: The default port number is `110`.
- Receiving Email Address: The email address that is used by Mobile Print Workflow.
- Use Secure Connection: To establish an encrypted link between a web server and a browser, SSL (Secure Sockets Layer) is the standard security technology used. For more information, refer to Using a Secure Connection.
- Authentication Mode: To indicate the type of server authentication used, from the Authentication Mode menu, select one of the options. The recommended setting is **Auto**.
- Polling Rate: The rate at which to poll for emails. For more information, refer to Polling Rate for Incoming Email.
- User Name: The user name that is used to connect to Exchange Web Services.
- Password: The password that is used to connect to Exchange Web Services.

Simple Message Transfer Protocol (SMTP) Settings

Outgoing Mail Settings

- Server Address: The name or IP address of the outgoing email server
- Port: The default port number for SMTP is `25`.
- Use Secure Connection: To establish an encrypted link between a web server and a browser, SSL (Secure Sockets Layer) is the standard security technology used. For more information, refer to Using a Secure Connection.
- Authentication Mode: To indicate the type of server authentication used, from the Authentication Mode menu, select one of the options. The recommended setting is **Auto**.
- From Email Address: The email address which the users see as the originator of their confirmation email.
- Reply-to Email Address: The email address which the user use to respond.
- Display Name: The name which the users see as the originator of their confirmation email.

Microsoft Graph API Settings

Note: Before you configure Azure AD authentication, you can create the receiving, from, and reply-to email addresses in the Office 365 Web portal. For more information, refer to Creating Email Address in Office 365 Web Portal.

Incoming Mail Settings

- Tenant ID: The ID of the Azure AD tenant.
- Client ID: The ID of the registered application client in the Azure portal.
- Client Secret: A secret string that the application uses to prove its identity when the application requests a token. The client secret can be an application password.
- Receiving Email Address: The email address of the user added to the group

Outgoing Mail Settings

- Tenant ID: The ID of the Azure AD tenant.
- Client ID: The ID of the registered application client in the Azure portal.
- Client Secret: A secret string that the application uses to prove its identity when the application requests a token. The client secret can be an application password.
- From Email Address: The email address of the user added to the group
- Reply-to Email Address: The email address that users use in response to the confirmation email.

Configuring the Incoming Mail Server Information Values for Microsoft Graph API

To set the values in the Server Information section, do the following:

1. To set the Tenant ID value, do the following:
   a. Go to your Azure Active Directory Tenant in the Azure Portal.
   b. On the Overview page, from Directory (tenant) ID, copy the tenant ID.
      It is recommended that you paste the tenant ID in Notepad, because the same value is used to configure outgoing mail server information.
   c. From the Xerox® Workplace Suite portal, do the following:
      - Select **Company > Settings > Incoming Mail**.
      - In the Server Type section, from the menu, select **Microsoft Graph Api**.
      - In the Server Information section, in the Tenant Name field, paste the copied tenant ID.
2. To register a new application, do the following:
   a. Go to your Azure Active Directory Tenant in the Azure Portal.
   b. On the Overview page, select **App registrations > New registration**.

      The Register an application window appears
   c. Enter a name for the application.
   d. Select the radio button for **Accounts in this organization directory only (AD Name only – Single Tenant)**.
   e. Click **Register**.
   f. From the Azure portal, copy the Application (client) ID.
      It is recommended that you paste the tenant ID in Notepad, because the same value is used to configure outgoing mail server information.

g. Go to the Xerox® Workplace Suite Web portal, in the Client ID field, paste the copied ID.

3. To create and copy the client secret value, do the following:
   a. In the navigation pane, click **Certificates & secrets**.
   b. In the Client secrets area, click **New client secret**.

      The Add a client secret dialog appears.
   c. In the Description field, type the required description.
   d. In the Expired field, select one of the following:
      - **in 1 year**
      - **in 2 years**
      - **Never**
   e. Click **Add**.

      The following fields appear in the grid:
      - Description
      - Expires
      - Value
      - ID
   f. From the Value grid, copy the value.
      It is recommended that you paste the value in Notepad, because the same value is used to configure outgoing mail server information.
   g. Go to the Xerox® Workplace Suite Web portal, in the Client Secret field, paste the copied value.
4. Grant the new application the following permissions:
   a. Go to the Azure portal, then do the following:
   b. Click **API Permissions**.
   c. If the delegated Microsoft Graph default permission is set, delete the delegated permission.
   d. Click **Assign**.

      The Request API Permissions page appears.
   e. Click **Application Permission**.
   f. Enable the following check boxes:
      - **Mail.Read**
      - **Mail.ReadBasic.All**
      - **Mail.ReadWrite**
      - **Mail.Send**
   g. In the Configured permissions area, click **Grant admin consent for**.
      Ensure that the printer status is green.
5. In the navigation pane, do the following:

a. Click **Licenses**.

   The Licensed features page appears.

b. In the Manage section, click **All products**.

c. Click **Office 365**, and ensure that the licenses are present.

6. To continue the process, refer to Creating Email Address in Office 365 Web Portal.

Configuring the Outgoing Mail Server Information Values for Microsoft Graph API

To set the values in the Server Information section, do the following:

1. Select **Company > Settings > Incoming Mail**.
2. In the Server Type section, from the menu, select **Microsoft Graph Api**.
3. In the Server Information section, do the following:
   a. In the Tenant Name field, copy the tenant ID from Notepad, and paste the copied ID.
   b. In the Client ID field, copy the Application (client) ID from Notepad, and paste the copied ID.
   c. In the Client Secret field, copy the value from Notepad and paste the copied value.
   d. In the From Email Address field, enter the required email address.
   e. In the Reply-to Email Address field, enter the required email address.
4. In the Test section, in the Email address field, enter an email address, then select **Send Test Email**.

   Verify that the test email is received in the associated mailbox.
5. Click **Save**.

Creating Email Address in Office 365 Web Portal

To create the receiving, from, and reply to email addresses, do the following:

1. Go to the Office 365 Web portal.
2. Log in as an administrator.
3. Click the grid icon.
4. Click **Admin**.

   The Microsoft 365 admin center page appears.
5. In the navigation pane, click **Groups > Active Groups**.
6. Click **Add a group**.

   The Add a group page appears.
7. In the Choose a group type section, select the radio button for **Mail-enabled security**, then click **Next**.

   The Set up the basics page appears.
8. Enter a name for the group.
9. If required, in the Description field, enter the required description, then click **Next**.

   The Edit settings page appears.

10. In the Group email address field, enter an email address.

    The Review and finish adding group page appears.

11. Click **Create group**.
    It can take up to an hour for the group email address to appear on the Active Groups page, or to be available to use in the Xerox® Workplace Suite Web portal.

12. Go to the Xerox® Workplace Suite Web portal. In the Receiving Email Address field, enter the group email address that you created.

13. To restrict access to the O365 group, use Powershell and follow the instructions at https://docs.microsoft.com/en-us/graph/auth-limit-mailbox-access .
    This change can take 30 minutes to take effect and show in the Microsoft Graph API.

14. Click **Test Connection**.

    A confirmation message appears.

Notes Remote Procedure Call (Lotus Notes) Settings

Lotus Domino Email Connection Support

To connect the software to a Lotus Domino server, the Lotus client libraries must be installed on the server. These libraries should be installed on the host server by the company's IT department. Assist the IT department in getting the correct libraries to connect to their Lotus Domino mail server. Configure and run the Lotus client library using the receiving email address in order to create the adaptor file (mail file) that is pointed to during setup.

Lotus Notes Client 8.5.1 and 9.0.1 are supported.

Incoming Tab

- Server Address: The name or IP address of the incoming email server, for example, `imap.adomain.com`, or `pop3.adomain.com`, or `xxx.xxx.xxx.xxx`
- Receiving Email Address: The email address to be used by Mobile Print Workflow.
- Watch Folder: The folder to watch in the email account, for example, `inbox`.
- Polling Rate: The rate at which to poll for emails.
- MailFile: The domino mail file (i.e. mail\User)
- Password: The password to use to make the connection

Outgoing Tab

- Server Address: The name or IP address of the outgoing email server
- From Email Address: The email address which the users see as the originator of their confirmation email
- Display Name: The name which the users see as the originator of their confirmation email.
- MailFile: The domino mail file (i.e. mail\User)
- Password: The password to use to make the connection

Using a Secure Connection

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser.

1. Locate your email and printer information form to see what type of secure connection your incoming mail server requires, such as SSL.
2. If the mail server you are connecting to requires an SSL link, make a selection from the **Use Secure Connection** menu:
   - SSL Off
   - SSL On Connect
   - SSL On Start TLS

Note: Your email provider will specify which type of SSL connection you require.

Polling Rate for Incoming Email

The Polling Rate for Incoming Email setting dictates how often the system will check for incoming emails that contain jobs from users.

1. Select **Company > Settings > Incoming Mail**.

   The Incoming Mail Server Settings screen displays.
2. Change the number of seconds in the **Polling Rate** field to the new value. The default is 10 seconds. The minimum rate is 1 second and the maximum rate is 300 seconds.

Note: Only whole seconds are accepted. You cannot enter a value that is a fraction of a second.

3. If you have finished making changes on this page, select **Save**.

Login Information

Supply an email address where a test email message can be sent for confirmation that the server settings are correct. This user name and password must match the user name in the Receiving Email Address area.

1. In the **User Name** box, type the user name for the applicable mail server account.
2. In the **Password** box, type the password associated with the user name account.
3. To verify that the test connection is successful, click **Test Connection**.

SETTINGS: JOB REPORTING

Before you use this feature, install the Job Reporting module. For more information, refer to the *Xerox® Workplace Suite Installation Guide*.

Job Reporting Database Details

Use this section to enable and set up rules for importing Usage Tracking (Network Accounting) data. To view the output use **Reports > Job Reporting**.

- Job Reporting: When the Enabled box is checked, the Xerox® Workplace Suite server collects Job data from the server for all printers which have been enabled for either Desktop Print or Mobile Printing. Also, if a Xerox device has been enabled for Usage Tracking (Network Accounting) in **Printer > Features > Usage Tracking**, the server collects Network Accounting data directly from the printer for all job types supported by network accounting. The Data is Merged with the Server data and available in the Job Reporting output, Which can be accessed here, **Reports > Job Reporting**. For more details, refer to Job Reporting Guidelines.
- Database Details: Job Reporting information is stored in its own database on the Xerox® Workplace Suite server. For this reason, the database server and the name of the database must be provided.
  - Database Server - Enter the name of the database server
  - Database Name - The name of an existing database instance to which the Workplace Suite server connects and stores Job Reporting information.
- The Default Database Names: Used from installation of the Job Reporting Module local database mode. If you used an external database, these names do not apply.
  - Database Server: <Server Name>\XeroxMobility
  - Database Name: WorkplaceSuiteReporting
- Test Connection: Tests connectivity to the Database.
- Data Retention Policy: Jobs are removed from the Job Reporting database after the configured time period. To retain the job details in the database, the administrator can select the time period from 6–36 months.

  Note: The Job Reporting database can grow quickly. It is recommended that you use the lowest setting. If you are using the default database that is supplied with the software, the maximum database size is 10 Gbytes.
- Schedule: Configure the frequency in which the Workplace Suite server retrieves accounting data from all enabled printers.
  - Disabled
  - Hourly
  - Every Day
  - On (Specify which day to run)
- Run Now

Job Reporting Guidelines

Job Reporting Installation overview:

- Requires a MS SQL Database, can be an external customer provided Database or one is provided.
- If you are not using an external database, an optional package installs Microsoft SQL Express 2017 Database and automatically sets the Database Server name and Database Name on the Job Reporting Screen.
- If you want to connect to remote Database Server see the Installation guide for details.
- Job Reporting can be enabled with Mobile Printing and Print Management workflows, and utilizes a single workflow connector.

Job Reporting Process:

- The Job Reporting process can be scheduled or run immediately.
- The process can be run or scheduled from this section on the Admin web page, **Settings > Job Reporting**
- When the process runs, The Job Reporting report and dashboard is updated with the latest information from the Server and Printers that have Usage Tracking enabled.
- Printers that have Workplace Suite Usage Tracking enabled successfully will be queried for their current Network Accounting Records.
- If the Network Accounting Records are successfully downloaded from the printer, then they are purged from the printer.
- It is recommended to schedule Job Reporting to run more often like every evening or hourly in the following scenarios:

  Note: It is assumed that you have enabled Usage Tracking Network Accounting on the printers. This means the JBA logs includes all the printer activity.

  – You have over 100 printers and an average or number of jobs printing.

  – You have less than 100 printers and there are a lot of jobs being printed.

When a Printer has Usage Tracking enabled:

For printers that support Xerox Network Accounting:

- Network accounting is automatically is turned on at the Printer with accounting prompts turned off.
- Refer to Workplace Suite online Knowledge base for which printers that Network Accounting has to manually be turned on.
- The server will collect Usage Tracking (Networking Accounting) data directly from the Printer for job types supported by network accounting. This includes Print, Copy, Scan, Fax, and all job types.
- The Network Accounting data from the printer is the source of record and are augmented with Data from Workplace Suite server data, such as user name and email address. User data is prioritized from Workplace Suite Server information. Print date is prioritized from the printer.
- For Workplace Suite Server jobs that don't match with a Network Accounting record for the same printer are not included in the report.

Job Reporting Data Overview:

- When Usage Tracking is enabled on a Printer that does not have Print Management Authentication or third party Authentication enabled the job owner field in the report will be set to unknown in the report for Copy, Scan, and Fax Jobs. There may be a job owner value for print jobs depending on how the print job was sent to the printer.
- When Usage Tracking is NOT enabled on a Printer or the Printer does not support Network Accounting, the Job Reporting Report will contain job history information for job data from the Workplace Suite server. The report will contain only the Mobile Printing and Print Management workflow print job history for that printer.
- The Job Reporting report may contain missing or inconsistent data if the Printer's Network Accounting data is also being downloaded and purged from a 3rd party accounting package on the same printer.

About the Job Reporting Report:

- The Job Reporting Report is updated after the Job Reporting Process is run, **Settings > Job Reporting**.
- The data retention for the Job Reporting database goes according to the Job Reporting Data Retention Policy. For more information, refer to Job Reporting Database Details.
- The device is the source of data for Job Reporting enabled devices, the times from the printer is what the printer reports but converted, by the server, to UTC time format (Coordinated Universal Time) no other modification. For example:
  - The raw device completion time is: 20161122131518
  - The report column DeviceJobCompletionUTC will contain 2016-11-22 18:15:18.000 since the printer has a time zone of -05:00:00
- Refer to the Reports section for detail table of the Job Reporting report fields.

SETTINGS: CONTENT STORAGE

The Content Storage Settings window is where you configure the location for temporary files, used by the Xerox® Workplace Suite system. In a deployment with multiple servers, all servers must have access to this location.

Content Partition Settings

The Content Storage Settings window is used to configure the document storage location Xerox® Workplace Suite uses to store all Mobile Print Workflow submissions. In a deployment with multiple servers, all servers must have access to this location. The Content Storage Settings are set automatically during the application installation.

Caution: Use this feature with caution and only for a custom configuration. For example, changing the server drive letter, and so on. Edit the Content Storage Settings with the assistance of your Xerox Analyst.

1. Select **Company > Settings > Content Storage**.

   The Content Storage Settings window displays.

2. For the **Content Partition Settings**, enter the location of the document storage directory.

   Important:

   - If you change the location of the storage directory, do the following:
     - Manually move the content files from the current location to the new location.
     - Restart the Mobile Printing Service.
   - If the storage location does not exist, the server attempts to create any missing directories.

3. To test the document storage directory, select **Validate Directory**.

   Note: Testing the document storage directory results in the creation of any directories that do not currently exist.

   If the Success icon appears, the directory is valid.

4. To store the Content Storage Settings, select **Save**.

Content Security Storage

For details about Content Security Storage, refer to the *Xerox® Workplace Suite Content Security Workflow Guide*.

SETTINGS: CONVERSION SERVERS

Note: This feature is only available with a Mobile Print Workflow license.

For customer supplied Microsoft Office 2016 Conversion Server options, refer to the *Xerox® Workplace Suite Upgrade Guide for Print Management and Mobility Suite, Mobile Print, and PrintSafe* at www.xerox.com/XWSsupport.

The DCE (Document Conversion Engine Servers) is a feature within the Mobile Print Workflow. The server is used to convert documents (such as TIFF, JPEG, TXT, Word DOCX, PDF and PPT file formats) to PS or PCL for concurrent Mobile Printing requests.

Mobile Printing is enabled to support and install multiple DCE server configurations for large, busy implementations where users are submitting multiple jobs simultaneously. To configure your Mobile Print Workflow for these types of advanced configurations, please contact authorized Xerox personnel for further details.

Important: Please be aware that adding a DCE to an existing implementation which uses multiple DCEs, will require all DCEs to be updated.

SETTINGS: PRINT DEFAULTS

To access the Default Print Settings screen, select **Company > Settings > Print Defaults**.

Print Options

Note: This feature is only available with a Mobile Print Workflow license.

The installation default print settings are:

- Color - **Full Color**
- Duplex - **One Sided**
- Staple - **Enabled**

- Media Size - **Auto Scale**

PRINT OPTIONS	FEATURE
Color	• When enabled, this option defaults to color printing • When disabled, this option defaults to black and white printing
Duplex	• One Sided - printing • Two Sided, Head to Head - printing • Auto Scale - printing
Staple	• When enabled this option defaults to stapled output • When disabled this option defaults to non-stapled output
Media Size	• Auto Scale • Original File Size

Banner Page: The banner page is printed with the actual Mobile Printing job and displays either the document name or a custom message.

- Print Banner Page: When enabled, the banner page is printed.
- File Name:
  - Document Name
  - Custom Message
- Custom Message text field

Banner Page

The banner page is printed with the actual Workplace Suite job and displays either the document name or a custom message.

- Print Banner Page: When enabled, the banner page is printed.
- File Name:
  - Document Name
  - Custom Message
- Custom Message text field

Job Owner

Job Owner configures which user attribute will be used as the job owner when the Workplace Suite sends a job to the printer. This value is displayed in the device UI to help the user identify the jobs and is used when sending jobs to third-party print queues.

From the **Use The Value Of** menu the following selections are available:

- Domain\User Name
- User Email Address
- User Name
- Xerox® Workplace Suite - Selecting this will use the text "Xerox® Workplace Suite" as the job owner.

To change one or all of these settings.

1. Select **Company > Settings > Print Defaults**.

   The Default Print Settings screen displays.

2. Select the desired print settings.
3. Select **Save**.

Note: Users will only see the printer features you make available.

Job Owner Override

When enabled, any job released using the Printer Client will have the job owner field overwritten with the user name of the logged on user.

SETTINGS: LDAP CONNECTIONS

LDAP administrators are specialized network administrators who provide information such as: domain names, server names, ports the LDAPs connect on, and so on. There is no standard or commonality in LDAP setup. Each company will be set up differently.

LDAP Connections allow you to configure valid authentication domains for the Xerox® Workplace Suite. You may change the LDAP ports and enforce the SSL Connection in the details of the LDAP server.

There are two LDAP Usage Modes that provide different LDAP connection capabilities:

- Simple Mode
  - Add LDAP Servers
  - Test LDAP connection
- Advanced Mode
  - Supports import of users, refer to Setting: LDAP Import.
  - Field Mapping supports which LDAP field is used to populate each field in the local user database.
  - User Deletion customizes LDAP filter used to locate users that should be removed from the user database when performing an LDAP Import, which is enabled for deletions.
  - Changes LDAP connection to communicate using generic LDAP commands.

- Specify and prioritize the container(s) that will be searched when on-boarding new users or importing users.
- Used for looking up group membership (e.g. Rules).

Select **Company > Settings > LDAP Connections** to manage LDAP connections.

The **Actions** menu provides a list of tasks that can be performed:

- New
- Delete
- Enable
- Disable

Adding a New LDAP Connections

To add and enable a LDAP connection:

1. Select **Company > Settings > LDAP Connections**.

   The LDAP Connections list appears.

2. From the Actions menu, select **New**.

   The New LDAP Connection window appears.

3. In the Details section, enter the required information or select an option, as needed.
   - **Enabled**: To enable the LDAP connection, select the check box for **Enabled**.

   Note: Only enabled servers are used for authentication or user import.

   - **Default**: To make the current LDAP connection as a default setting, select **Default**.
   - **Domain Name**: Enter the Domain Name that you want to appear in the LDAP Connections list.
   - **Server Name**: Enter the server address where the domain is hosted.
   - **Use SSL**: To use SSL, select the check box for **SSL**.
   - **Port**: Enter the port value for the LDAP connection.
4. Select a Usage Mode:
   - **Simple**: This mode is for standard field management, for simple usage.
   - **Advanced**: This mode is for specialized field management, customized field settings, and user import based on the defined LDAP Container list. See Advanced Mode instructions below.
5. For **Simple** mode, select **Test Connection**. To verify the connection, enter the following information:
   - **User Name**
   - **Password**

   The test attempts to log in to the LDAP server.

6. Select **Run test**.

   The run test results appear:

   - If the run test is successful, the Success icon appears.
   - If the run test is unsuccessful, the Test connection failed icon appears.

7. Select **Save**.
8. Select **Advanced** Usage mode.
9. Select LDAP Connection.

   Note: By default, Workplace Suite will assume all connections are to a Microsoft Active Directory Server. Select the check box option **Enable Generic LDAP Connection** if you wish to communicate using generic LDAP commands in the LDAP Connection field.

10. Enter the following information in the LDAP Credentials fields:
    Credentials are required to customize the field mappings or to specify the container list used for scheduled imports.

    - **User Name**
    - **Password**

    Note: To access the Advanced tab, authenticate in the LDAP Credentials fields.

    LDAP uses Containers to hold information and map users. Use this setting to specify the container(s) that will be searched when on-boarding new users or importing users from Active Directory. If no containers are specified, the solution will use the root container as the default. The solution will search for users in the defined containers, starting with the first listed container and working down the list.

11. To add a container, select **Add Container**. The **Add Container** setting allows you to scan and authenticate against a LDAP server. You can change the priority of an item by selecting a container and using the arrows on the right to move it up or down in the list.
12. Select **Test Connection**. To verify the connection, enter the following information:

    - **User Name**
    - **Password**

    The test attempts to log in to the LDAP server.

13. Select **Run test**.

    The run test results appear:

    - If the run test is successful, the Success icon appears.
    - If the run test is unsuccessful, the Test connection failed icon appears.

14. Select **Save**.

    The message `Your changes have been saved` appears, and the Advanced tab is selected.

    Note: To avoid misconfiguration, you must understand the structure. It is important to understand how the user data structure was created, be able to log in, and administer the LDAP system.

15. Enter the custom User Deletion Filter.

    Note: The User Deletion Filter is needed only when the **Import Settings** is enabled.

    Note: When performing an LDAP Import, a customized LDAP filter is used to locate users that are selected for removal from the Workplace Suite software database. If a user matches the User Deletion Filter, the user is removed from the Workplace Suite software database.

16. You can modify the following Field Mapping settings:
    - **Email Address**
    - **User Name**
    - **Alternate Access Card Use**
    - **Primary PIN or Access Card Number**
    - **First Name**
    - **Last Name**
    - **Network Accounting User ID**
    - **Network Accounting Account ID**
    - **Department**
    - **Groups**
    - **User Object Class**
    - **Use Import Filter**
17. To store the LDAP configuration, select **Save**.

To Change Look up Priority for an LDAP Server

When doing authentication or user lookup, the Workplace Suite System will search the LDAP Connections list from first LDAP Server to last LDAP Server, the default server is at the top of the list. The order of the LDAP servers can be modified. If you move the mouse over a server in the LDAP Connections list, it will turn yellow. Press down on the left mouse button and drag the server up or down to change the order of the list. This is useful to organizer you commonly used servers at the top.

Editing the Settings of an LDAP Connection

To edit the settings of an existing LDAP connection:

1. Select **Company > Settings > LDAP Connections**.

   The LDAP Connections list displays.

2. In the Connection table, select the name of the LDAP connection you want to edit. The Edit LDAP Connection screen displays.
3. On the Server tab, you can edit the Details, Usage Mode, and LDAP Credentials information.

   To view the status of the LDAP connection, select **Test Connection**. The system tests the LDAP and displays an indicator with a status of verified or failed.

4. Select **Save**.

Disabling an LDAP Connection

To disable an LDAP Connection and make it unavailable:

1. Select **Company > Settings > LDAP Connections**.

   The LDAP Connection list displays.

2. Select the checkbox next to the connections you want to disable.
3. Select **Disable** from the Actions menu.

   The connection remains in the list, but is disabled.

4. When the confirmation message displays, select **OK**.

   The window closes and the system updates the LDAP connection table.

Deleting an LDAP Connection

To remove an LDAP Connection from the list:

1. Select **Company > Settings > LDAP Connections**.

   The LDAP Connections list displays.

2. Select checkbox next to the connections you wish to delete.
3. Select **Delete** from the Actions menu.
4. When the confirmation message displays, select **OK**.

   The window closes and the system updates the LDAP connection table.

Enabling SSL for an LDAP Domain

1. Select **Company > Settings > LDAP Connections**.
2. Select the name of the LDAP domain connection where you want to enable SSL.
3. On the Enable LDAP Connection screen, select the **Use SSL** check box.
4. Select **Save**.

SETTINGS: LDAP IMPORT

LDAP Import is similar to Discovery. You can set up a schedule to periodically run an LDAP Import or you have the ability to run it immediately. LDAP syncs with Xerox® Workplace Suite Software so if employees join or leave the company, they are added or marked as deleted in the LDAP system and then when you run an import, it updates the users in the Workplace Suite User Database. This eliminates the need to manually manage the users in the Workplace Suite System. After you run an LDAP Import for the first time, you need to decide what you want the import process to do the next time you run it.

To set up and run an LDAP Import:

1. Select **Company > Settings > LDAP Import**.

   The LDAP Import Schedule screen appears.

2. From the Changes to Apply section, determine which of the following you want to apply the next time LDAP Import is run:

   - **Additions**: New users in LDAP will be added to the Workplace Suite system.
   - **Modifications**: The current user records are compared to the existing user records and any changes are brought over to the Workplace Suite system.
   - **Deletions**: Users who are deleted from LDAP will be marked as deleted in the Workplace Suite User Database.

3. In the Schedule section, select when you want LDAP Import to run:

   - **Disabled**: There is no schedule.
   - **Every Day**: Run LDAP Import once a day at a set time.
   - **On**: Run LDAP Import on selected days at a set time.

     (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday)

   - **At approximate time** (Hour \ Minute): Used daily or on set days.

4. Select **Save**.

   The LDAP Changes to Apply and Schedule settings are saved.

Note: You can also select:

- **Run Now** to immediately start an LDAP import, which uses the last saved settings in the Changes to Apply section.
- The **History** refresh icon to get the status details of the last LDAP import.
- **Success** to view the status details including the Import Details and Counts.

Note: A Processing... indicator may display until the import process is complete.

Importing a List of Users with LDAP Synchronization

1. To enable User Import, for one or more LDAP connections:

   a. In the Usage Mode area, select **Advanced**.

   b. In the LDAP Credentials area, type the administrator User Name and Password.

      The Advanced tab appears.

   c. Select the **Advanced** tab.

   d. In the Import Settings area, select **Enabled**.

   e. Click **Save**.

2. For LDAP Import, select the following options:

a. Changes to apply - Select which type of changes in the AD\LDAP to effect in the Print Management Server User database:

   Additions to the database

   Modifications to the database and/or

   Deletions from the database

b. Select the scheduled time (if you want) for regular synchronization and/or select **Run Now** for immediate synchronization.

c. Select **Save**.

   Synchronization may take several minutes, depending on the changes requested and the size of the database.

SETTINGS: AZURE AD CONNECTION

Introduction

When you enable the Azure AD Connection feature, users can authenticate to the Web Portal, Printer Client application, and Workplace Mobile App using their Azure AD credentials. The following authentication settings are available for the administrator to enable:

- New card registration with Azure AD credentials
- Mobile Application with Azure AD credentials
- Printer Client login with Azure AD credentials
- Web Portal login with Azure AD credentials

Azure AD Connection Guidelines

Note: The Alternate login feature does not support Azure AD authentication at the printers.

- Before you deploy Azure AD authentication, it is recommended that you validate that Azure is functioning correctly. It is recommended that you enable and validate Xerox® Workplace Suite Web Portal Azure Authentication login first.
- To help with debugging Azure authentication issues, keep a browser tab open that is logged in to the Web administration webpage already. If there are Azure AD authentication issues, to make changes, you can use this logged-in browser window.
- If you are locked out of the Web administration page, to recover your account, refer to Administration Recovery Procedure.
- Ensure that the Field Mapping setting for the **Email Address** field is mapped to a user email address. If you do not follow this process, the user cannot receive email notifications or log in to Xerox® Workplace Suite, when an email address is required to log in.
- When a user authenticates with Azure AD, and the user exists in Xerox® Workplace Suite, the local profile of the user is updated based on the Azure AD user information. If the user field has a value and corresponding Azure field side is blank, the user value is not updated as a blank value.

Enabling Azure AD Connection

To enable Azure AD Connection, do the following:

1. Select **Company > Settings > Azure AD Connection**.
2. Select the check box for **Enable Azure AD Authentication**.

   The following tabs appear:

   - **Server**: In the Xerox® Workplace Suite area, by default, the host name appears in the Host name field automatically.
   - **Web Application**
   - **Native Application**
   - **Advanced**
3. In the Server tab, set the Tenant ID value. To set this value, refer to Setting the Server Values.
4. In the **Web Application** tab, to set the required values, refer to Setting the Web Application Values.
5. In the **Native Application** tab, to set the required values, refer to Setting the Native Application Values.
6. In the **Advanced** tab, to set the required values, refer to Setting the Advanced Values.
7. After you have completed the Azure AD connection setup, refer to Completing the Azure AD Connection Setup.

Setting the Server Values

To set the values in the **Server** tab, do the following:

1. Go to your Azure Active Directory Tenant in the Azure Portal.
2. On the Overview page, from Directory (tenant) ID, copy the tenant ID.
3. From the Workplace Suite portal, do the following:
   a. Select the **Server** tab.
   b. In the Azure AD Tenant Information area, in the Tenant ID field, paste the copied tenant ID.
4. After you set the values in the Server tab, set the values in the Web Application tab. Refer to Setting the Web Application Values.

Setting the Web Application Values

To set the Web Application values, do the following:

1. Go to your Azure Active Directory Tenant in the Azure Portal.
2. On the Overview page, select **App registrations > New registration**.

   The Register an application window appears
3. Enter a name for the application.
4. Select the radio button for **Accounts in this organization directory only (AD Name only – Single Tenant)**.
5. Click **Register**.
6. From the Azure portal, copy the Application (client) ID.
7. Go to the Xerox® Workplace Suite Web portal, then select the **Web Application** tab.

8. In the Register the new application area, in the Client ID field, paste the copied ID.
9. Go to Azure portal page, then do the following:
    a. Click **API Permissions**.
    b. In the Configured permissions area, select **Microsoft Graph**.

       The Request API Permissions page appears.
    c. Click **Delegated Permission** and then do the following:
        - From the OpenId Permissions section, select the check box for **openid**.
        - From the User section, select the check box for **User.Read**.
        - From the Group section, select the check box for **Group.Read.All**.
        - Click **Update Permissions**.
    d. .Click **Grant admin consent for**.

       A confirmation message appears.
    e. Click **Yes**.
10. Go to the Azure portal, then from the navigation pane, do the following:
    a. Click **Authentication**.

       The Platform configurations page appears.
    b. From the Implicit grant and hybrid flows section, select the check box for **Access tokens (used for implicit flows)**.
11. In the navigation pane, click **Certificates & secrets**.
12. In the Client secrets area, click **New client secret**.

    The Add a client secret dialog appears.
13. In the Description field, type the required description.
14. In the Expired field, select one of the following:
    - **in 1 year**
    - **in 2 years**
    - **Never**
15. Click **Add**.

    The following fields appear in the grid:
    - Description
    - Expires
    - Value
    - ID
16. In the Client secrets grid, from the Value field, copy the value.
    If the Value field has asterisk you are required to create a new client secret.

17. Go to the Xerox® Workplace Suite Web portal, then do the following:
    a. Select the **Web Application** tab.
    b. In the Create a client secret area, in the Client Secret field, paste the copied value.
18. Go to the Azure portal, then from the navigation pane, click **Authentication**.

    The Platform configurations page appears.
19. Click **Add a platform**.

    The Configure Platforms dialog appears.
20. Click **Web**.

    The Redirect URIs field appears in the window.
21. Go to the Xerox® Workplace Suite Web portal, then do the following:
    a. Select the **Web Application** tab.
    b. In the Set Redirect URIs on the new application as follows: area, copy the first URL.
22. Go to the Azure portal, then in the Redirect URIs field, paste the copied URL.
23. Click **Configure**.

    The Platform configurations page appears.
24. In the Redirect URIs area, click **Add URI**.
25. On the Xerox® Workplace Suite Azure AD Connection screen, from the Set Redirect URIs on the new application as follows: area, for Redirect URIs copy each of the remaining values.
26. Go to the Azure portal. In the Redirect URIs area, click **Add URI**, then paste the URIs.
27. On the Xerox® Workplace Suite Azure AD Connection screen, from the Set Logout URL on the new application as follows: area, copy the logout URL.
28. In the Azure portal, in the Logout URL section, paste the copied URL, then click **Save**.

Setting the Native Application Values

To set the Native Application values, do the following:

1. Go to your Azure Active Directory Tenant in the Azure Portal.
2. On the Overview page, select **App registrations > New registration**.

   The Register an application window appears
3. Enter the required name.
4. Select the radio button for **Accounts in this organization directory only (AD Name only – Single Tenant)**.
5. Click **Register**.
6. From the Azure portal, copy the Application (client) ID.
7. Go to the Xerox® Workplace Suite Web portal, do the following:
   a. Select the Native Application tab.
   b. In the Register the new application area, in the Client ID field, paste the copied client ID.

8. Go to the Azure portal page, then do the following:
   a. Click **API Permissions**.
   b. In the Configured permissions area, select **Microsoft Graph**.

      The Request API Permissions page appears.
   c. Click **Delegated Permission** and then do the following:
      - From the OpenId Permissions section, select the check box for **openid**.
      - From the User section, select the check box for **User.Read**.
      - From the Group section, select the check box for **Group.Read.All**.
      - Click **Update Permissions**.

      A confirmation message appears.
   d. Click **Yes**.
   e. From the navigation pane, click **Authentication**.
      In the Implicit grant and hybrid flows section, do the following:
      - Select the check box for **Access tokens (used for implicit flows)**.
      - Select the check box for **ID tokens (used for implicit and hybrid flows)**.
9. Go to the Azure portal, then from the navigation pane, click **Authentication**.

   The Platform configurations page appears.
10. Click **Add a platform**.

    The Configure Platforms dialog appears.
11. Click **Web**.

    The Redirect URIs field appears in the window.
12. Go to the Xerox® Workplace Suite Web portal, then do the following:
    a. Select the **Native Application** tab.
    b. In the Set Redirect URIs on the new application as follows: area, copy the Web URI.
13. Go to the Azure portal, then in the Redirect URIs field, paste the copied URI.
    a. Select the check box for **Access tokens (used for implicit flows)**.
    b. Select the check box for **ID tokens (used for implicit and hybrid flows)**.

       The access token and ID token are enabled.
    c. Click **Configure**.
14. Click **Add a platform**.

    The Configure Platforms dialog appears.
15. Click **Mobile and desktop applications**.

    The Redirect URIs field appears in the window.
16. Go to the Xerox® Workplace Suite Web portal, then do the following:

a. Select the **Native Application** tab.

b. In the Set Redirect URIs on the new application as follows: area, copy the first Mobile and desktop applications URI.

17. Go to the Azure portal, then in the Custom redirect URIs field, paste the copied URI.
18. In the Redirect URIs area, click **Add URI**.
19. On the Xerox® Workplace Suite Azure AD connection screen, from the Set Redirect URIs on the new application as follows: area, copy the second mobile and desktop application Redirect URIs value.
20. Go to the Azure portal, then in the Redirect URIs area, click **Add URI**.
21. In the Custom redirect URIs field, paste the copied URI.
22. Click **Save**.

Setting the Advanced Values

To set the advanced values, do the following:

1. In the Field Mapping area, complete the following fields:

   Note: For all the Field Mapping fields, you can enter the value, or from the menu, select the required value.

   - Email Address
   - User Name
   - Alternate Access Card User
   - Primary PIN or Access Card Number
   - First Name
   - Last Name
   - Network Accounting User ID
   - Network Accounting Account ID
   - Department
2. Click **Save**.

Completing the Azure AD Connection Setup

It is mandatory to perform the following steps to complete the Azure AD connection setup:

1. To enable Azure AD Authentication for the Web portal, do the following:

   a. Select **Company > Policies > Security**.

   The Security Settings page appears.

   b. Select the **User Portal** tab.

   c. Select the radio button for **Azure AD Authentication**.

   d. Click **Save**.
2. To enable Azure AD authentication for the printer client, do the following:

a. Select **Company > Policies > Security**.

   The Security Settings page appears.

b. Select the **Printer Client** tab.

c. Select the check box for **Prompt the User to Supply Credentials**.

d. Select the radio button for **Azure AD Authentication**.

e. Click **Save**.

3. To enable Azure AD authentication for automatic registration at the printer, do the following:

   a. Select **Company > Policies > Security**.

      The Security Settings page appears.

   b. Select the **Printer Authentication** tab.

   c. In the Auto Registration section, select the check box for **Azure AD Authentication**

   d. Click **Save**.

4. To enable Azure AD authentication for auto registration at the printer, do the following:

   a. Select **Company > Policies > Security**.

      The Security Settings page appears.

   b. Select the **Mobile Application** tab.

   c. Select the radio button for **Azure AD Authentication**.

   d. Click **Save**.

Azure AD Authentication Methods

New Card Registration with Azure AD Credentials

Provides the ability for a user to register a new card using Azure AD Authentication. If the user does not exist they we be created, if they already exist the card will be assigned to them. Once the card is registered to that user any subsequent card logon would then use the users registered information.

Note: To register as a new card, the user needs an Azure AD account.

After you enable the Azure AD authentication feature at **Company > Security > Print Authentication > Auto Registration**, and the user swipes a new card at the printer, they are required to do the following:

1. The user enters an email address.

   At the user interface, a message appears that states `To complete registration, follow instructions in email sent to (<email_address>).`. An email with a link to complete the registration is sent to the user.

2. The user clicks the link in the email.
   The link in the email expires after 30 minutes.

   If the user attempts to access the link after it expires, an error message appears that states `The link has expired and is no longer valid. Please attempt to register your access card again at an enabled printer.`.

   To confirm the identity of the user, a window prompts the user to enter their Azure login credentials.

3. The user logs in using their Azure login credentials.
   After confirmation, if necessary based on the current Azure AD, the user local database record gets updated.

   The badge is registered to the user. A window appears that states `Your card has successfully been registered to your account.`.

Note: Ensure that the badge number is new. If you enable the Allow Multiple Primary PINs or Access Cards feature for the account, you can add any new badge to the account. If you disable the Allow Multiple Primary PINs or Access Cards feature for the account, the latest card number replaces the existing card number in the user profile. With this feature disabled, when a user swipes a new card, an error message does not appear.

Mobile Application Login with Azure AD Credentials

When you enable the Azure AD authentication feature for the Mobile Application, when the user logs in, they are redirected to the Azure AD login page to provide credentials. To enable the feature, select **Company > Policies > Security > Mobile Application**. The supported mobile operating systems are Android, iOS, and Chrome.

Printer Client Login with Azure AD Credentials

When you enable the Azure AD authentication feature for the Printer Client, when the user logs in, they are redirected to the Azure AD login page to provide credentials. To enable the feature, refer to Xerox® Printer Client.

Web Portal Login with Azure AD Credentials

When you enable the Azure AD authentication feature for the Web portal, and the user opens the Xerox® Workplace Suite login page, they are redirected to the Azure AD login page to provide credentials.

To enable the feature for the Web portal, select **Company > Policies > Security > User Portal**.

SETTINGS: SAML CONNECTION

Customers who use an Identify Provider (IdP) that supports SAML, such as ADFS, can use it to simplify the login process for the Web portal. If the user is logged in to their workstation, the solution attempts to log the user in to Xerox® Workplace Suite using that same identity. Configure your IdP to trust the Xerox® Workplace Suite application, and provide information for the Xerox® Workplace Suite solution to communicate with the IdP. This capability is supported for workstations that run Microsoft Windows.

Note: When you use an LDAP Authentication with ADFS, the SAML connection capability is validated. Multiple SAML Connection definitions are not supported.

IdP and Xerox® Workplace Suite Configuration

To use SAML, the administrator is required to supply information to the IdP about Xerox® Workplace Suite, so that it can trust communication coming from the Xerox® Workplace Suite solution. Similarly, the administrator needs to

configure Xerox®Workplace Suite with information about the IdP so that it knows how to connect to the provider. The required information includes the following:

- Service provider information to be entered in the IdP
  - Workplace Suite identifier: `urn:xerox:services:000C29D34DAFFBB3DE869C2FC`
  - SAML assertion endpoints: For the Web portal https://xws.services.xerox.org/login/home/ProcessSaml.
  - Binding: HTTP-POST
  - Field mappings: Ensure that you map the associated fields in your identity provider to the provided Xerox® Workplace Suite attribute values. The following table shows the importance required vs optional values and the recommended mapping of attributes in ADFS/LDAP to Workplace Suite:

IDENTITY PROVIDERATTRIBUTE RECOMMENDATION, BASED ON ADFS	WORKPLACE SUITE ATTRIBUTES	IMPORTANCE
Source: LDAP Attribute: Email Address	Email	Required, if username is blank
Source: ADFS Claim Attribute: Windows account name	Username	Required, if email is blank
Source: LDAP Attribute: Department	Department	optional
Source: LDAP Attribute: Given-Name	Firstname	optional
Source: LDAP Attribute: Surname	Lastname	optional

Note: The username attribute value in Workplace Suite must conform to the format of domain or username. The ADFS claim value of Windows account name returns a value of this format. Use the ADFS claim mapping instead of using the LDAP field of SAM-Account-Name.

- Identity provider information to be entered in Workplace Suite.
  - Metadata URL: Location of IdP configuration file, which is retrieved using HTTPS. Typically, the port is 443, but can be a non-standard port such as 8443, as defined by the IdP.

Note: Ensure that the metadata URL configured in the SAML Connection page of the Web portal has Internet access. To retrieve the configuration file, the Xerox® Workplace Suite solution hosted in Azure needs to access this URL. To use the SAML capability, the customer is required to ensure that the configuration file is publicly available and accessible.

The Xerox® Workplace Suite solution retrieves the IdP configuration file from the supplied metadata URL location. The key information retrieved in the configuration file includes the following:

- Identifier: Entity ID
- Single Sign-On URL: Connections use HTTPS. Typically, the port is 443, but can be a non-standard port such as 8443, as defined in the retrieved metadata file.
- Single Sign-On binding: HTTP-Redirect

Intranet Zone Configuration

For SAML to work, the Web portal login method require the Federation Server DNS name to be added to the Intranet zone. To configure this trust, refer to https://docs.microsoft.com, *Configure Client Computers to Trust the Account Federation Server*.

Configuring SAML Connection

To use the SAML Connection option, do the following:

1. Update the Intranet Zone on the user workstation. For more information, refer to Updating the Intranet Zone
2. Configure the IDP and Workplace Suite for trusted communication. For more information, refer to Configuring the IdP and Xerox® Workplace Suite for Trusted Communication
3. Configure the Administrator or user portal to use SAML. To configure, do the following:
   a. In the Web portal, select **Company > Policies > Security > User Portal**.
   b. Select the radio button for **SAML Authentication**.

Updating the Intranet Zone

You can update the intranet zone through group policy or on a user-by-user basis. For more information, refer to https://docs.microsoft.com, *Configure Client Computers to Trust the Account Federation Server*.

To update the intranet zone on the Windows 10 system, do the following:

1. In the search box, type the `Internet Options` option. Run the Control Panel option
2. Select the **Internet Options** options.
3. Select the **Security** tab.
4. Select the **Local Intranet** settings.
5. Click **Sites**.
6. Click **Advanced**.
7. In the Add this website to the zone:, add the URL `https://<ADFS-FQDN>`.
8. Click **Add**.

In Chrome or Firefox browser, SAML Connection required additional configuration. For more information, refer to https://docs.microsoft.com, *Configure Client Computers to Trust the Account Federation Server*.

- For Chrome, you have to add the WIASupportedUserAgents on the ADFS system.
- For Firefox you have to add the WIASupportedUserAgents on the ADFS system and add the ADFS server to the Firefox network.automatic-ntlm-auth.trusted-uris setting. For more information, refer to https://docs.microsoft.com, *Integrated authentication with Firefox in Update Rollup 12*.

Configuring the IdP and Xerox® Workplace Suite for Trusted Communication

To configure the IdP and Xerox® Workplace Suite for trusted communication, do the following:

1. In the Web portal, Select **Company > Settings > SAML Connection**.
2. In the Enablement section, select the check box for **Enable SAML Support**.

   The Service Provider Information and Identity Provider Information sections appear.
3. In the Metadata URL field, type IdP Metadata URL.

   The Metadata URL allows Xerox® Workplace Suite to communicate with the IDP for authentication requests.
4. Click **Save**.
   The Workplace Suite solution retrieves the IdP configuration from the supplied Metadata URL location. The key information retrieved in the configuration file appears in the Retrieved Configuration section as follows:
   - Identifier
   - Single Sign-On Binding
   - Single Sign-On URL
   - Metadata XML
   - Last Retrieved
5. Use the service provider information from the Web portal, and log in to the ADFS system.
6. Open the `Relying Party Trusts` folder.
7. Add a new trust for Xerox® Workplace Suite .
8. Select the **Identifier** tab.
9. In the Relying Party Trusts field, add the identifier information from the Web portal.
10. Click **OK**.
11. Select the **Endpoints** tab, then add the endpoints.
12. Click **OK**.

SETTINGS: NETWORK APPLIANCES

Note: This feature is available only with a Print Management Workflow license.

Network appliances are small network boxes that attach to the network. Network appliances permit the Xerox® Workflow Suite Print Management Workflow software connector to control the release of user documents to printers that do not support the Xerox® Secure Access or Convenience Authentication. A network appliance is configured on the network by the administrator. The appliance is associated with the particular printer in the Workplace Suite Admin Tool. To release jobs at the printer, users can swipe their card through the card reader associated with the printer. One network appliance is required for each printer.

Note:

- This is a Print Management Workflow feature. If the Mobile Print Workflow is enabled for the printer connected to the Network Appliance, you can print Mobile Print Workflow jobs.
- The Jobs that are released automatically correspond to the Workflow Device Connector that is enabled for that printer. This includes Mobile Print and Print Management (Client Queue and Network Queue). For Print Management jobs to release the Incoming Printer automatically, queues must be in the same Printer Group as the printer where they are releasing the Jobs.

Settings: Network Appliances > Models

The Xerox® Print Management Workflow supports three network appliance models: RF Ideas Ethernet 241, Elatec TCP Conv2/3, and Elatec TCP Conv. By default, each of these models is available on the Workplace Suite software at **Company > Settings > Network Appliances > Models**. If any or all of these models are not going to be part of your site installation, you can disable the listeners on the server.

The default ports that the listeners use are:

- RF Ideas Ethernet 241-2001
- Elatec TCP Conv2/3-7777
- Elatec TCP Conv-7778

If the network appliances on your system are configured to use a different port, an administrator can change these default ports. Ensure that any firewall on the Workplace Suite server is configured to allow communication through the ports.

Settings: Network Appliances > Appliances

There are three possible actions that can be taken with respect to network appliances.

- New
- Remove Printer Association
- Delete

Adding a New Network Appliance

To add a new network appliance to the system, the device must first be configured on the network using the installation instructions provided by the manufacturer. Once the device has a valid IP address, you can add the network appliance to the system.

1. On the Network Appliances screen, go to the Appliances tab and select **New** from the Actions list.
2. Enter a Display Name that will be meaningful to the administrator.
3. Enter the network appliance IP address.
4. Select the appropriate Network Appliance Model from the list.
5. Select **Select Printer** to make the association between the network appliance and the printer that the appliance will control.
6. Select **OK**.
7. Select **Save**.

Remove Printer Association

1. On the Network Appliances screen, go to the Appliances tab.
2. Select the network appliance and select **Remove Printer Association** from the Actions list and confirm when prompted.

Deleting a Network Appliance

1. On the Network Appliances screen, go to the Appliances tab.
2. Select the network appliance and select **Delete** from the Actions list and confirm when prompted.

SETTINGS: SITES

A site is a logical group of printers that are usually at the same physical location.

The **Actions** menu provides a list of tasks that can be performed.

The **Page** indicator shows which page is being viewed of the total number of pages.

The **Items Per Page** indicator lets you set the number of sites that are displayed per page.

The **Sort By** menu lets you sort the list by:

- Name A-Z
- Name Z-A

The **Search** field lets you quickly find specific sites in long lists.

Adding a New Site

1. Select the **Sites** tab. From the Actions menu, select **New**.

   The Add New Site window appears.

2. Enter the **Details**:
   - **Name**
   - **Country**
   - **Address 1**
   - **Address 2**
   - **City**
   - **Postal Code**
   - **County**
   - **Latitude**
   - **Longitude**

   Note: The Mobile Printing App uses Latitude and Longitude to locate nearby printers.

   - **Time Zone**

   Note: The server Time Zone setting is used for print Rules time restrictions.

   - **Description**
3. Select **Save**.

   The window closes and the system updates the list of sites.

Editing a Site

1. On the **Sites** tab, select the name of the site you want to edit.

   The Edit Site window displays.
2. Enter the **Details**:
3. Select **Save**.

Deleting a Site

1. Select the **Sites** tab.
2. Select the checkbox for one or more sites that you wish to delete.
3. Select **Delete** from the **Actions** menu.
4. When the confirmation message displays, select **Yes**.

   The window closes and the system updates the list of sites.

Importing a Site

To import a site from a file:

1. Select the **Sites** tab.

2. Select **Import From File...** from the **Actions** menu.

   The Import Sites window appears.

3. Select **Browse** and navigate to the file you want to import, then select **Open**.

   Select **Download Example**, edit this file as your base import file.

4. Select **Next** and review the import data.

   The Import Data Validation Details window appears.

5. Select **Import**.

   The window closes and the system updates the list of sites.

Exporting Sites

You can export the entire site list to a CSV file.

1. Select the **Sites** tab.
2. Select **Export All Pages** from the **Actions** menu.

   Note: To export the current page from the printers list, choose **Export This Page** from the Actions menu.

3. Locate the download location and open the file.

   The exported list of sites opens in Microsoft Excel.

SETTINGS: SINGLE SIGN-ON

Single Sign-On is an authentication method that enables users to securely authenticate with multiple applications from the Xerox App Gallery.

When the user access the Single Sign-On enabled Gallery App for the first time, they must login to the printer using Xerox Workplace Suite and then enter their credentials for the app, the user will be asked to store their authentication data at the end of the authentication sequence, when they agree to store their information with Workplace Suite, subsequent access to the same App will not require the credentials. Each Gallery App installed on the printer that supports Single Sign-On has this option.

Note:

- For SSO login to work, users need to sign into each app once and agree to let their information be stored.
- This feature is available only with a Print Management Workflow license.
- For more information, refer to *Xerox® Workplace Suite Single Sign-On for Apps Quick Start Guide*.

Load Balancer Server Address

For some Load Balancer configurations, multiple IP addresses can be used as a pass-through address. Workplace Suite Administrator can enter one or more Load Balancer Server Address to allow the user to use the Single Sign-On credentials on the printer.

Note: This setting is only required in configurations where a load balancer has multiple IP addresses. Single Sign-On will not allow the user to log into the printer until multiple IP addresses have been added on the Load Balancer Server Address.

Adding the Load balancer Server Address

To add the Load Balancer Server Address:

1. Select **Company > Settings > Single Sign-ON**.

   A Single Sign-On window appears.

2. Under the Load Balancer Server Address section, add the necessary Load balancer Server Addresses.

   Note: Use a semicolon (;) to separate each Load Balancer Server Address.

3. Click **Save**.

   A notification displayed that your changes have been saved.

SETTINGS: PROXY SETTINGS

The proxy server settings are found under **Company > Settings > Proxy Settings**.

This section configures Xerox® Workplace Suite so it can reach external resources on the Internet.

When the Mobile Print Workflow is enabled it requires a valid outgoing internet connection. If the Mobile Print Workflow is not enabled, then doing this procedure is optional, but strongly recommended because email containing external content (such as images) will be printed correctly by Mobile Printing and licensing can be performed without a manual import of the license file.

To configure Workplace Suite Software to reach external resources on the Internet:

1. Select **Company > Settings > Proxy Settings**.

   The Proxy Settings screen displays.

2. Under Details, select the checkbox for **Enable Proxy Server**.
3. Enter an address in the **Web Proxy Address** field.
4. Enter Bypass Proxy settings for these addresses.
5. Select the checkbox for **Bypass proxy setting for local (intranet) address**.
6. Under Authentication, select the checkbox for Authentication Required if authentication is required for the proxy server:
   a. Select an **Authentication Mode**.
   b. Enter a **Domain Name**.
   c. Enter a **User Name**.
   d. Enter a **Password**.
7. Select **Test Proxy Server** to verify the configuration.
8. Select **Save**.

Company: Policies

This chapter contains the configuration information for the following topics:

POLICIES: SECURITY

Policies: Security > General

Confirmation Number

You can use the Confirmation Number for Printer Authentication and Printer Client Authentication.

Confirmation number is used by the guests to log into the Xerox Workplace Suite Printer Client (EIP App) and release email jobs.

Details

- **Confirmation Number Length:** 1–10 digits are required for the confirmation number.
  - **Enable Confirmation Number Expiration:** Expiration based on the numbers of days configured.
- **Confirmation Number Generation After Expiration**: This setting allows you to configure when new confirmation numbers will be generated after they expire.

  Note: This setting is only visible when **Enable Confirmation Number Expiration** is toggled on (enabled).

  The supported options are:

  - **Generate after expiration** (default): When the confirmation number is expired, the solution will auto-generate a new value for each enabled user and send them an email notification containing the new confirmation number.
  - **Generate after email job is received**: When an email job is received, the system will check if the user's confirmation number is expired. If expired, a new one will be created and an email notification will be sent, which contains the new confirmation number.

    Important: It is recommended to not use this option if you have enabled confirmation number login for Printer Authentication, the Mobile App, or the User Portal.

> **Caution:** When this setting is enabled, the XWS server will not automatically send out a new confirmation number after they expire. The user will have to send an email job to XWS server to receive a new confirmation number.

Note: When this setting is enabled, the expiration time will allow values of 1–365 days (Normally 30–365).

- **Maximum Failed Login Attempts:** The number of failed login attempts allowed before the user account is disabled is 3–5.

  Note: When the maximum number of failed login attempts is reached, the user and Workplace Suite Administrator both receive an email when a user is locked out. The email contains a link to unlock the user account.

To store the Security settings, select **Save**.

To restore the Security settings to the previous saved settings, select **Reset**.

Policies: Security > Printer Authentication

Note: This feature is only available with a Print Management Workflow license.

This section is used to control access to the printer. The administrator can control and configure the authentication mechanism, locking screen details, user registration, and card details.

If you are using a USB Card Reader for authentication, a USB Card Reader plug-in is required on VersaLink NW and PrimeLink devices.

Policies: Security > Printer Authentication > Basic

Alternate Login

Note: The Alternate login feature does not support Azure AD authentication at the printers.

Alternate login is a mechanism that controls how a user can log in without using the USB card reader attached to the multifunction printer.

- **Disabled**: Ensure that the user uses an identification card to log in.
- **Primary PIN**: Users can enter an assigned primary PIN, which can be the number that is read from the card. Alternatively, if the site does not use identification cards or card readers, the Primary PIN can be an assigned number.

  Note: This feature is only available with a Print Management Workflow license.
- **Confirmation Number**: The server creates a system-generated confirmation number and emails it to the user. Optionally, the user can log in to the printer using the confirmation number.

  Guidelines:

- When you select Confirmation Number as the alternate login mechanism, the user is required to log in with their LDAP credentials at the printer. After logging in, the user receives their confirmation number. The confirmation number is generated by the server and emailed to the user.
- If a user forgets a Confirmation Number, there are two ways to reset it, the user can click on Forgot Confirmation Number on the Workplace User Portal login page or they can request the system administrator to reset their Confirmation Number, For more information, refer to Forgot Confirmation Number and Resetting Confirmation Number.
- For information about the policies for the confirmation numbers, refer to Policies: Security > General.
- If the confirmation number of a user expires, they receive a new confirmation number by email.
- If your server is configured with a Mobile Print Workflow license, the confirmation number is received from the server, when the user emails a job. The same confirmation number is used for the printer authentication for Alternate Login.

- **LDAP Authentication**: The user can enter LDAP credentials for LDAP lookup by the Print Management server.

Printer Control Panel Administrator Login

Enabling Administrator Login allows a user to log in at the printer control panel using the Alternate Login feature. This log in feature provides a user access to administrator functions. To use this feature, on the first Alternate Login screen the user must enter the user name “admin”, then enter the configured password.

To enable and configure the Administrator Login feature:

1. For Administrator Login, click Enable.
2. In the Password field, enter an alternate Administrator Login password.

Auto Registration

The Auto Registration specifies whether the user can register their card themselves through on-boarding, or whether the system administrator has preregistered their card.

Auto Registration happens when you swipe an unknown card and they are prompted to supply their credentials. The credentials include email and password, LDAP user name and password, Azure AD user name and password, or SAML user name and password. If valid, the card number is added to the database for that user and works by doing a card swipe.

- **Disabled**: If you select this option, the user cannot register their own card themselves.
- **LDAP Authentication**: If you select this option, the print management server is configured to access an LDAP server for user information. When a user swipes their card for the first time at the multifunction printer, they can provide LDAP credentials, and the card is associated with their print management workflow account.
- **Azure AD Authentication**: If you select this option, ensure that you have enabled the Azure AD Connection feature. For more information, refer to Azure AD Authentication Methods.
- **SAML Authentication**: If you select this option, ensure that you have enabled the SAML Connection feature. For more information, refer to Settings: SAML Connection.

Note:

- The Azure AD or SAML Authentication selection have an option to **Include card number in auto registration email**. If you want to enable this setting, select the check box: **Include card number in auto registration email**.
- This setting is useful if you are using Primary PIN or Access Card Number as the Alternate Login method on the device.

Machine Access

These settings control whether the Print Management server or the Device System Admin will configure the device access.

- **Manage Machine Access at the Device** - The MFP access settings are handled by the Device System Admin. This is typically done through the web interface of the printer.
- **Manage Machine Access** using Print Management Workflow - The MFP access settings are set automatically by the Print Management server.
  - **Service Pathway** – Controls whether the Services pathway is locked automatically if Machine Access is managed by the Print Management server.

Policies: Security > Printer Authentication > Advanced

Use the Allow Multiple Primary PINs or Access Cards setting to enable users with multiple Access Cards or Primary PINs associated with their user record. The Default setting is Disabled.

Note: If you enable the Allow Multiple Primary PINs or Access Cards setting, then later disable the setting, all user PINs and Access Card Numbers are deleted.

Domain Qualification

Use this setting to enable or disable the use of Domain Qualification when providing user credentials at the device.

If enabled, when credential information is sent to the printer, the system prepends the user domain to the network user name. For example: DOMAIN\USERNAME.

Custom Blocking Screen Message

If enabled, the blocking screen can be customized on the device to display the Title and Message defined in the appropriate language section.

If you enable Mobile Phone Unlock and are using a Custom Message, edit the Message and add the Mobile Unlock code. For details, refer to Mobile Phone Unlock.

Secondary PIN

- Prompt the user to supply a PIN in addition to their card or Alternate Login credentials. If the user does not have a configured Secondary PIN, they will be allowed to create one.

Details

- Never
- Always: requires a Minimum PIN Length

Selecting **Save** stores the Security settings.

Selecting **Reset** restores the Security settings to the previous saved settings.

Card Setup

If proximity card readers are used in the Print Management Workflow environment, a contiguous subset of the characters read from the card can be specified to be used as the PIN for validation.

- Proximity Cards - Control which characters read from the card are used as the ID Number of the card. Selections include: **Use all Characters** or **Use Required Range of Characters**.
- Magnetic Stripe Cards - Control whether track 1 or track 2 data is used as the ID Number of the card. For magnetic stripe cards, the administrator can choose which data track is used as the card number.

Policies: Security > Printer Client

Xerox® Printer Client

You can configure security settings related to the Printer Client application.

1. To access the Printer Client feature, do the following:
   a. Select **Company > Policies > Security > Printer Client**.
   b. Select the features required for your environment.

2. To configure security settings, do the following:

   - **Logged on Users (Access Card)**: Use the logged-in user credentials when you access the printer client. If the logged-in user matches a user in the local database, the printer client does not prompt the user to provide more credentials.

Note: The Printer Client feature is available only with a Print Management Workflow license.

   - **External Printer Authentication** : The Printer Client trusts external third-party authentication providers. The Printer Client matches the logged-in user name to the Workplace Suite user database. If a match exists, the Printer Client shows jobs that are available for that user.

Note: For details about configuring the Printer Client for card access, refer to Configuring for Alternate Access Card Users with CAC/PIV Environments.

   - **Prompt the User to Supply Credentials**: The user is prompted to supply credentials when they select the Printer Client feature.
     - **LDAP Authentication**: If you select this option, the user is prompted to supply their LDAP user name and password.
     - **Azure AD Authentication**: For more information, refer to Azure AD Authentication Methods.
     - **Confirmation Number**: This feature has the following options.
       - **Email Address Required**: The user is prompted to supply their Email Address followed by their Confirmation Number.
       - **Mask Confirmation Number**: Obscure the Confirmation Number when entered in the Printer Client application.

Note: The Mask Confirmation Number feature is available only with a Print Management Workflow license.

     - **Primary PIN**: Optionally, users can log in to the device using their PIN. This value maps to a user card number. To add PINs manually, you can import the numbers using LDAP, or add them during the auto registration of a card.

Mask Confirmation Number

In Workplace Suite, Mask Confirmation Number is now a setting (default setting is Off) that affects the confirmation number for both:

- Email and Confirmation Number
- Confirmation Number

Policies: Security > Mobile Application

Note: This feature is only available with a Mobile Print Workflow license.

Mobile Application

You can find the Security section in **Company > Policies > Security**. You can configure the security settings related to the mobile application. This setting controls the authentication mechanism to access the mobile application.

- **Mobile Application**
  - **LDAP Authentication**: Users enter LDAP credentials when they log in to the mobile app. To configure LDAP connections, select: **Company > Settings > LDAP Connections**. The LDAP Authentication feature supports Print Portal App Login Retention.
  - **Azure AD Authentication**: The Azure AD authentication does not support the Print Portal App Login Retention setting. Microsoft Azure determines the login retention policy.
  - **Email and Confirmation Number**: Users receive a unique number by email that is required to use the mobile app. The Email and Confirmation Number feature supports Print Portal App Login Retention.
- **Print Portal App Login Retention** Users are required to provide their credentials when they access the Xerox® Workplace Mobile App. This setting controls when the user is required to reenter their credentials.
  - **Retain Login Credentials** check box: To enable this option, select the check box. User credentials are retained and used for subsequent login attempts.
  - Retain Login Credentials field: In the text field, you can enter the number of days to retain the login. When you use the mobile application, this option controls the length of time the user remains logged in to their account. When the expiration time is reached, the user is logged-out of the mobile application and is required to reenter their credentials. If the **Retain Login Credentials** feature is enabled, the user logs in using their retained credentials automatically.

Policies: Security > User Portal

User Portal Login

This section is where the administrator configures the authentication mechanism for user access to their personal Web portal. Authentication is required to use the permissions feature, which grants access to other users to manage your jobs.

To configure your authentication mechanism, select one of the following authentication types:

- **Email and Confirmation Number**: When this option is enabled, the user logs in with an email address and a system-generated confirmation number.
- **LDAP Authentication**: When this option is enabled, the user logs in with LDAP credentials. To select this option, ensure that at least one LDAP Connection is enabled.

  Note: An LDAP Connection is required to use LDAP Authentication. To configure an LDAP Connection, select **Company > Settings > LDAP Connections**. Ensure that an LDAP connection is configured and functional. To test the connection, in the Test section, type the user credentials, then click **Test Connection**.
- **Azure AD Authentication**: Users can log in using their Azure AD credentials. To select this option, ensure that the Azure AD Connection is enabled.
- **Windows Integrated Authentication**: When this option is enabled, the user is not required to log into the User Portal. Xerox® Workplace Suite uses the identity of the current Microsoft Windows session to log in the user to the portal. If the user does not exist in the Xerox® Workplace Suite user database, the user cannot access the Web portal.

- **SAML Connection**: Before you select this option, enable the SAML Connection feature.

If the administrator cannot log in, refer to Administration Recovery Procedure.

POLICIES: CONTENT PROFILES

Note: For details on Content Profiles, refer to the *Xerox® Workplace Suite Content Security Workflow Guide*.

POLICIES: RULES

Print Controls

Rules are created to customize printer access. Rules can control printer access by User Groups, Printer Groups, Print Release Time, and Printing Attributes.

Print Controls Guidelines

- Rules apply only when you release a job to a printer.
- Rules do not apply to Printer Client Scan jobs, or with Mobile Print Workflow Outgoing Queues.
- When an administrator implements rules for printing, users are assigned to a user group. The user group is associated to a rule. Any user not assigned to a rule cannot use the print feature.
- Before you create rules for printing, establish User Groups and Printer Groups.
- Rules allow administrators to specify which user groups can access the print features, including the use of color and 1-sided printing.
- When you attempt to use a print feature that you do not have permission to use, you receive an email warning. The system uses permitted features only to print the job.
- When you are assigned to multiple rules, the rule that enables the most permissions takes precedence over rules that are more restrictive.

Creating Rules

To create a rule:

1. Select **Company > Policies > Rules**.

   The Rule Details tab appears.

2. Select **Actions > New**.

   The Rules Wizard guides you through the rule creation process.

3. Type the Name and a brief Description of the new rule, then click **Next**.

User Association

To assign users or groups to the new rule:

1. To add users:
   - To add all users to the rule, click **All Users**.
   - To add multiple users to the rule, click **Select User Groups**.
2. From the Available User Groups list, select user groups to add to the rule.
3. To move the selected groups to the Associated User Groups list, click the right arrow button.
4. Click **Next**.

Device Association

Use this procedure to associate devices to a new rule.

1. To associate all devices to the new rule:
   a. Click **All Devices**.
   b. To continue to time-based rule options, select **All Devices > Next**.
2. To associate one or more device groups to the new rule:
   a. Click **Select Device Groups**.
   b. To move groups from the Available Device Groups list to the Associated Device Groups, click the group, then click the right arrow button. To move more device groups, for each group, repeat this step.
   c. Click **Next**.

Allowing a Print Job Release Based on Time

To add the specific day and time printing guidelines to the new rule:

1. Click **Enabled**.
2. Select the specific days and times that users can print, then click **Next**.

Allowing Color Access

To allow users to print in both color and black and white, for Allow Color Access, click **Enabled**.

Allowing Single-Sided Access

To allow users to process jobs 1-sided, select the **Enabled** check box.

Note: When 1-sided printing is disabled, all jobs are printed 2-sided.

Reviewing the Rule Settings

To review and save the rules settings:

1. To make the new rule effective, from the Rule Summary, select the **Enable Rule** check box.
2. To edit the new rule, click **Back**.
3. To save the rule, click **Finish**.

Editing an Existing Rule

To edit an existing rule:

1. Select **Company > Policies > Rules**.

   A list of rules appears.

2. Click a Rule Name.
3. Select each subtab, then enter required information as necessary. When you are finished, click **Save**. The subtabs are **Details**, **Users**, **Devices**, **Time**, and **Print**.

Rule Actions

To enable, disable, or delete a rule:

1. Select **Company > Policies > Rules**.

   A list of rules appears.

2. To change the status of a rule, select a rule from the list. Select **Actions > Enable**,**Actions > Disable**, or **Actions > Delete**.

   A confirmation message appears.

3. Click **OK**.

Implementing Rules

Use the following steps when you move from an open printing environment to one driven by rules. Use these steps to test the rules and determine if they function as intended.

1. Create a User Group called "allButAdmin" for all users, but exclude the administrator.
2. Create another User Group called "AdminOnly" that contains the administrator only.
3. To allow current users to print continue to print while validating your new rule, create a rule for the “allButAdmin” group. Include rule options that allow printing to all devices and have access to all print features.
4. Create a test rule for the “AdminOnly” user group, containing the Rule Options which you want to validate.
5. Validate the new rule and test the configured rule options.
6. When rule validation is complete, edit the rule to include everyone you want to apply to the Rule to.
7. Disable the rule created in step 3.

Rule Examples

Scenario 1

Establish rules for the Faculty and Staff on a college campus. Faculty members want to print any time, on any device, 1-sided or 2-sided, and in color. Students are permitted to print between 8:00 AM and 9:00 PM, and only 1-sided, in black and white.

One possible solution for Scenario 1 requires creation of two Rules, two Access Groups, and one Printer Group.

1. Create a Faculty and Student User Group.
2. Create a Printer Group that contains Student Printers.
3. Create a Faculty Rule. Add the Faculty User Group, then enable full access to all devices and print features.

4. Create a Student Rule. Add the Student User Group, then enable access to the Students printer group. Set the print release time to between 8:00 AM and 9:00 PM daily. Do not enable Allow Color Access and Allow Single-Sided settings. This setting allows students to print 2-sided and in black and white only.

Scenario 2

Establish rules for printing and copying for company employees. A Human Resource team requests exclusive use of a group of printers.

One possible solution for Scenario 2 requires creation of two Rules, one Access Group, and two Printer Groups.

1. Create a Human Resource User Group.
2. Create a Human Resource Printer Group that contains the Human Resource printers.
3. Create a Rule, then add the Human Resource User Group and the Human Resource Printer Group.
4. Create a Non-Human Resource Printer Group that contains all printers expect the Human Resource printers.
5. Create a second Rule, then add all users and add the Non-Human Resource Printer Group.

Determining Rules Assigned to a User

To view assigned rules for an existing user:

1. Select the **Users** tab.

   A list of current users appears on the Users subtab.
2. To view account details, find and select the user, then click **User Email**.
3. To view the enabled rules assigned to the user, click the **Rules** subtab.

Print Quotas

Print Quotas Overview

Print Quotas provide administrators with the ability to control and restrict the number of pages that an individual user can print. Print Quotas allow administrators to limit how many pages a user or group of users can print in a specified period, and prevent users from exceeding set limits. Print quota rules also apply to copy jobs.

This section describes the features of Print Quotas, and provides instructions for creating, adjusting, analyzing, and overriding Print Quota rules.

Note:

- Print Quota Rules are designed to allow a print job to be completed when it falls outside of the maximum quota for the period. For example, if a rule restricts users from printing more than 50 pages per day, the user can still print a single print job with more than 50 pages.
- The Pages per Job Estimation parameter is used when Print Management Workflow Desktop Print queues have the Conversion Mode option set to None, or when the page count cannot be determined.
- Various Print Quota settings and actions are located on the Users tab.

Print Quota Notifications

EIP Error Messages

Users that exceed the enforced Print Quota limit receive an error message in the Printer Client app if they attempt to release a job. This prevents the user from printing the job.

Email Notifications

Users receive an email notification when they print a job or make a copy that results in them being within 25% of their Print Quota threshold for the current period.

Users receive an email notification when they print a job or make a copy that results in them exceeding their Print Quota threshold for the current period.

Setting Print Quota Parameters

1. Click **Company** > **Policies** > **Rules** > **Print Controls**.
2. To set the print quota period, select one of the following options:
   - **Daily** – Select this option to set the allocated print quota period to every 24 hours at 00:00 local time.
   - **Weekly** – Select this option to set the allocated print quota period to start on Monday and end on Sunday at 00:00 local.
   - **Monthly** – Select this option to set the allocated print quota period to start on the first day of the month and end on the last day of the month at 00:00 local time.
   - **Yearly** – Select this option to set the allocated print quota period to start on the first day of the current year until the last day of the year. (January 1st to December 31st).

   Note: The Users Print Quota is replenished when a new quota period begins.
3. To set the estimated pages for print jobs that cannot be parsed to determine the number of pages in the job, in the Pages field, enter the required number.
4. To save the settings, click **Save**.

   A notification appears confirming that the changes have been saved.

Creating a New Print Quota Rule

Note: When more than one Print Quota rule is enabled, the more restrictive rule is enforced. For example, if rule 1 enforces a maximum quota of 30 pages per day, and rule 2 enforces a maximum quota of 50 pages per day, rule 1 is always enforced first.

1. Click **Company** > **Policies** > **Rules**, then select the **Print Quotas** tab.
2. To create a new rule, click **Actions**, then select **New**.
3. In the name field, enter the required name for the rule.

   Note: Use a unique name for the new rule. If you enter a name that is already in use, an error message appears preventing you from saving the rule.
4. If required, enter a description for the rule, then click **Next**.
5. To apply the rule to all users, click the **All Users** option.

6. To apply the rule only to specific user groups, click the **Select User Groups** option:
   a. A pop-up window appears. To add a User Group to the Associated User Groups, locate the required group in the Available User Groups list, then click the Plus (+) icon.
   b. To remove a User Group from the Associated User Groups, locate the required group, then click the trash can icon.
   c. To create a new User Group, click **New User Group**, then follow the on-screen instructions. For further information on creating and managing User Groups, refer to User Groups.
   d. To add the Associated User Groups to the new rule, click **OK**.
7. To confirm the settings, click **Next**.
8. To set the print quota for the new rule, type the required number of pages, then click **Next**.

Note:

- The default setting for the print quota pages is 50.
- The default setting for the print quota period is Daily. To change the print quota period, refer to Setting Print Quota Parameters.

9. To save and enable the new rule, ensure that Enable Rule is selected, then click **Finish**.

   The new rule appears in the list of Print Quota rules.

Enabling or Disabling a Print Quota Rule

1. Click **Company** > **Policies** > **Rules**, then select the **Print Quotas** tab.
2. To select the rule that you want to enable or disable, locate the required rule, then click the associated check box.
3. To enable or disable the selected rule, click **Actions**, then select the required option.

   The settings are saved automatically.

Deleting a Print Quota Rule

1. Click **Company** > **Policies** > **Rules**, then select the **Print Quotas** tab.
2. To select the rule that you want to delete, locate the required rule, then click the associated check box.
3. To delete the selected rule, click **Actions**, then select **Delete**.

   A dialog box appears.
4. To confirm your selection, click **OK**.

   The settings are saved automatically.

Displaying the User Print Quota Analysis

You can view usage information for a user by accessing the user Print Quota Analysis page.

To show user Print Quota information:

1. On the Xerox Workplace Suite home page, click **User**, then select the check box next to the user you require.

2. Select **Actions** > **Analyze Print Quota**.

   The following print quota analysis information displays:

   - **Enforced Quota** – The most restrictive Print Quota Rule that applies to the user or, if enabled, the Override Print Quota Rules configuration for the user.
   - **Remaining** – The total number of pages that remain in the user print quota for the current period.
   - **Consumed** – The total number of pages the user has consumed in the current period.

Viewing Assigned User Print Quota Rules

You can view the print quota rules that have been assigned to a user by the system administrator.

To view pint quota rules assigned to a user:

1. On the Xerox Workplace Suite home page, click **User**, then select the check box next to the user you require.
2. Select **Actions** > **Analyze Print Quota**.

   The following user print quota rules information is displayed:

   - **Override Print Quota Rules**: If Override Print Quota rules is enabled, the user is not restricted by any Print Quota rules. Instead, user specific print quota rules can be assigned. For further details, refer to Overriding Print Quota Rules for Individual Users.
   - **Pages**: This indicates the number of pages the user can print within the given period. You can adjust the Pages value as required.
   - **Period**: This indicates the refresh rate of the user Print Quota. For information on adjusting the Print Quota Period, refer to Setting Print Quota Parameters
   - **Enforced Print Quota Rule**: This displays the current enforced Print Quota rule.

Overriding Print Quota Rules for Individual Users

You can define rules for specific users that override any general Print Quota rules that apply to all users or any groups of users that contain the specific user.

To override Print Quota for a User:

1. On the Xerox Workplace Suite home page, click **User**, then select the check box next to the user you require.
2. On the User Details page, select **Override Print Quota Rules**.
3. For Pages, enter the required Print Quota value or select **Unlimited**.

Viewing the User Print Quota Status

You can access information about Print Quota rules that apply to your user account

To view your Print Quota status:

1. Log in to the Xerox Workplace Suite web page.
2. In the upper right corner of the screen, click your user name.
3. To access your user profile, click **Profile**.

   Your Print Quota status displays.

Print Limits

Print Limits Overview

The Print Limits feature provides administrators the ability to restrict the number of pages that an associated user or user group can print in a single job.

Print Limits Guidelines

- You can apply Print Limits to a User or to User Groups.
- The Print Limits calculation includes counts of the copies when a user prints a job. For example, if the print limit for a job is set to 10 pages and a user wants to print two copies of a 9 page job, the job gets blocked from printing.
- When a user exceeds their Print Limits for Print Management Workflow Desktop jobs, Workplace Suite removes the job.
- When a user exceeds their Print Limits for Mobile Print jobs, the Print Job Retention Policy decides the removal of the job.
- The Print Limits rules also apply to Workplace Suite copy jobs that are initiated from the Workplace Suite Printer Client Copy feature.

Notification Settings in Print Limits

- When a user exceeds their print limit, an email notification is sent to the user.
- When the user releases a job from the printer client that exceeds their print limit, the job fails and a message appears.
- The administrator can modify the Notification Message in the Print Limits message section.
- To track the jobs that have failed because a user exceeded their print limit, refer to the Workplace Suite Administration Job History page.

Modifying the Notification Settings Message

The notification message appears in available languages.

1. To modify the notification message, click **Company > Policies > Rules**, then select the **Print Limits** tab.
2. In the Notification Settings area, click **Message**.

   The default notification message appears.
3. To update or change the default notification message, click any of the following options that are available in the Message field:
   - **Reset to default**: This option modifies the notification message and resets the message to the default message.
   - **Insert Rule**: This option inserts in the notification message the printing limit rule that your system administrator configured.
   - **Insert Page Count**: This message inserts in the notification message the page count for your print job.
4. To discard the changes that you selected, click **Reset**.The Reset option returns the notification message to the default settings.

5. To save the changes, click **Save**.

Creating a Print Limits Rule

1. To create a rule for Print Limits, click **Company > Policies > Rules**, then select the **Print Limits** tab.
2. Click **Actions**, then select **New**.
3. In the Name field, enter the required name for the rule.
4. If required, enter a description for the rule, then click **Next**.
5. For User Association, select the needed features:
   - To apply the rule to all users, click **All Users**.
   - To apply the rule only to specific user groups, click **Select User Groups**.
6. A pop-up window appears. Select the needed features:
   - To add a user group to the Associated User Groups, in the Available User Groups list, locate the required group, then click the **Plus** (**+**) icon.
   - To remove a user group from the Associated User Groups area, locate the required group, then click the trash icon.
   - To create a user group, click **New User Group**, then follow the onscreen instructions. For more information on creating and managing user groups, refer to User Groups.
7. After you select the available or new user group, to add the Associated User Groups to the new rule, click **OK**.
8. To manage the user groups, click **Manage**, then repeat Step 6 as needed.
9. To confirm the settings, click **Next**.
10. To set the total print limits for the new rule, in the Set Page Count Limits area, select one of the following:
    - **Unlimited**: This option allows unlimited page counts.
    - **Page Limit**: This option lets you enter the number of pages for a job.
11. In the Color area, select one of the following:
    - **Unlimited**: This option allows unlimited print colors.
    - **Page Limit**: This option sets the limit for the number of pages that are printed in color.
12. To confirm the Set Page Count Limits settings, click **Next**. The Rule Summary for the new rule appears.
    - To enable the new rule, from the Rule Summary window, click the check box for **Enable Rule**.
    - To save the new rule, click **Finish**. The new rule appears in the list of Print Limits Rules.

Enabling or Disabling a Print Limits Rule

1. To enable or disable a printing limit rule, click **Company > Policies > Rules**, then select the **Print Limits** tab.
2. To select the rule that you want to enable or disable, locate the required rule in the Rules list, then select the associated check box.
3. To enable or disable the selected rule, click **Actions**, then select **Enable** or **Disable**.

   The settings are saved automatically.

Deleting a Print Limits Rule

1. To delete a rule from the Rules list, click **Company > Policies > Rules**, then select the **Print Limits** tab.
2. To select the rule that you want to delete, locate the required rule in the Rules list, then select the associated check box.
3. To delete the selected rule, click **Actions**, then click **Delete**.

   A dialog box appears.
4. To confirm your selection, click **OK**.

   The settings are saved automatically.

Viewing the User Print Limits Summary

You can access information about Print Limits rules that apply to your user account.

To view your print limits:

1. Log in to the Xerox Workplace Suite webpage.
2. In the upper-right corner of the screen, click your user name.
3. To access your user profile, click **Profile**.

   Your print limits status appears.

POLICIES: NOTIFICATIONS

Email Notification Settings

This section is used to determine what email notifications will be received by the user.

To configure email notifications:

1. Select **Company > Policies > Notifications**.

   The Notification Settings screen appears.
2. Select from the following options:
   - Receive All Notifications
   - Receive Failure Notifications Only
   - None
3. Select **Save**.

Note: Notifications could be delivered to your junk mail. Check your junk mail for email notifications and configure your junk mail to allow emails from Xerox® Workplace Suite.

Push Notification Settings

Use this feature to control the ability to send Push Notifications to the user's mobile device. For Push notifications, the user must install the Xerox® Workplace Mobile App on their mobile device, they must agree to receive push notifications, and they must have logged into the mobile app at least once.

To configure the Push Notification option:

1. Select **Company > Policies > Notifications**.

   The Notification screen appears.

2. Select a Push Notification option:
   - Receive All Notifications
   - Receive Failure Notifications Only
   - None
3. Select **Save**.

Note: Notifications could be delivered to your junk mail. Check your junk mail for email notifications and configure your junk mail to allow emails from Xerox Workplace Suite.

POLICIES: DATA RETENTION

Retention Policy

The Retention Policy determines how long your print job remains in the Xerox® Workplace Suite system. There are three options:

- Immediately: This option deletes Jobs from the system after printing.
- Allow User to Retain Jobs: This option allows users to save content immediately after a job prints.
- Periodically: This option deletes Jobs from the system at a set interval: 1, 3, 7, 14 or 30 days after job submission.

Note: When the Periodically option is selected, jobs are deleted from the system after the set day interval passes. If the jobs printed or did not print, the jobs are deleted.

To configure the Data Retention settings:

1. Select **Company > Policies > Data Retention**.
2. Select the check box for the required Retention Policy:
   - Immediately: This option deletes Jobs after printing.
   - Allow User to Retain Jobs: This option allows users to save content immediately after a job prints.
   - Periodically: This option deletes jobs after a set number of days, if the jobs printed or did not print.
3. Select **Save**.

Archived Content Retention Policy

The Archived Content Retention Policy determines how long your stored job remains in the Xerox® Workplace Suite system after the configured time period.

Note: For archiving jobs for longer than 30 days, use an external file storage location. For example, use an external file storage location such as a network share or high-availability storage array network (SAN) for archived jobs.

To configure the Data Retention settings:

1. Select **Company > Policies > Data Retention**.
2. For the Archived Content Retention Policy, enter the **Days after submission**.
3. Select **Save**.

POLICIES: PRINTER

Details

The Printer Client uses this address for communicating with Xerox® Workplace Suite.

1. Select **Company > Policies > Printer**.
2. Enter the **Details** of the address that the Printer Client is to use when communicating with Xerox® Workplace Suite. Once set, do not change this address.
   - Server Address

Print Protocol

The protocol used to transfer print jobs to the printer. This setting is used as a default when adding new printers to the server. Changes to this setting have no impact on the configuration of existing printers. [Applies to the Mobile Print Workflow].

1. Select **Company > Policies > Printer**.
2. Enter the **Details**:
   - Raw or LPR (Default)
   - IPP over SSL

Documents Release Order

Use this option to control the order in which jobs are processed and printed.

1. Select **Company > Policies > Printer**.
2. Enter the **Documents Release Order**:
   - Maximize Performance (Default)
   - Enforce Job Order

Display Name

When using the Discovery feature to add printers, or manually adding them and leaving the display name blank, the server uses one of the following fields to assign the printer's display name. From the top of the list to the bottom, the first non-blank value available for the Printer is used.

1. Select **Company > Policies > Printer**.
2. Choose a **Display Name**, using the up/down arrows to reorder items in the list.
   - System Name
   - Printer IP Address
   - Serial Number
   - Xerox Asset Number
   - Customer Asset Number
3. Select **Save**.

POLICIES: MOBILE USER ACCESS

Note: This feature is only available with a Mobile Print Workflow license.

Mobile User Access

The **Mobile User Access** area is where you specify who is allowed access to the Mobile Print Workflow.

- The **Actions** menu provides a list of tasks that can be performed.
- The **Page** indicator shows which page is being viewed of the total number of pages.
- The **Users per page** indicator lets you set the number of users that are displayed per page.
- The **Search** field lets you quickly find specific users in long lists.

1. Select **Company > Policies > Mobile User Access**.
2. Select an option:
   - **Allow All Users Except Blocked List**: This option lets everyone have access to the Mobile Print Workflow except for the users you specify.

     You can Add, Import or Delete email addresses from the **Blocked Users** list.
   - **Allow Only Specified**: This option lets only users that you specify have access to the Mobile Print Workflow.

     You can Add, Import or Delete email addresses from the **Allowed Users** list.

3. If you are using the **Blocked Users** list or the **Allowed Users** list, select one of the following options to add or remove users from the list:
   - Add
   - Delete
   - Import
   - Export This Page
   - Export All Pages
4. Select **Save**.

Guest Onboarding Using Email

Note: To use this feature, access to the Mobile Print Workflow is required.

Guidelines for onboarding users

- For the feature to work properly, you are required to configure both the incoming and outgoing email settings.
- When you create users using LDAP Import setting , this feature does not apply. This feature applies only when you create new users or guest users using an email.
- To configure guest users, in the Xerox® Workplace Suite Web portal, select **Company > Policies > Mobile User Access**, then select the radio button for **Allow Only Specified**.
- If the administrator attempts to enter an email address or domain that matches an existing entry, an error appears and the new entry is not saved.
- The user is onboarded as either a guest or a normal user, based on the user type value.
  - For a user type of Guest User, the user is added as a guest and their expiration period is set to the configured value.
  - For a user type of normal user, the guest flag is not set and no expiration period is assigned.
- If the default guest expiration value changes, the expiration date of users that are already created is not impacted.
- When the expiration period is reached, the guest user is removed automatically. Alternatively, you can delete the guest user from the Users tab.
- The guest user receives an email response, which provides their guest account details.

Usage Guidelines

When a user submits an email to the incoming email address of the Xerox® Workplace Suite system, the email address is compared to the email and domain entries in the Allow Only Specified field. The following logic is used for onboarding the user:

- If the users match an email address, they are onboarded. The Department, Network Accounting User ID, and Network Accounting Account ID are added to the user profile.
- If the users match a domain, they are onboarded. The Department, Network Accounting User ID, and Network Accounting Account ID are added to the user profile.

- If the user matches both a domain and email address, the email address takes precedence.

Note: When the guest user is onboarded, the system generates a confirmation number or password automatically, and an email notification is sent to the guest user.

Caution: If you use your company domain, all new users are assigned to the department, network accounting user ID, and network accounting account ID of the company.

Adding a User with Guest User Enabled

1. Select **Company > Policies > Mobile User Access**.
2. Select the radio button for **Allow Only Specified**.
3. From the Allowed Users list, click **New**.

   The Add User dialog box appears.
4. In the Details section, do the following:
   a. From the Allowed Type menu, select one of the following:
      - **Email Domain**
      - **Email Address**
   b. In the Value text field, type the required value.
   c. In the Department text field, type the required department.
   d. In the Network Accounting User ID text field, type the required user ID.
   e. In the Network Accounting Account ID text field, type the required account ID.
5. In the Guest User section, select the check box for **Enabled**.
   The system generates a confirmation number or password automatically and emails it to the guest user using the email address.

   The Expiration Time (days) option appears.
6. In Days after creation, select the number of days.
7. To save the settings, click **Save**.

POLICIES: ACCOUNTING

Note: This feature is only available with a Mobile Print Workflow license.

The Accounting area allows you to enable and configure Job Reporting, as well as configuring accounting defaults and when they will be used for Mobile Print Workflow.

The Mobile Print Workflow allows you to print Mobile Printing jobs when accounting is enabled at the printer. The Mobile Print Workflow supports both Xerox Network and Standard Accounting.

Note: If a password is set for Xerox Standard Accounting on any Mobile Printing-enabled printers, a default credential must be set in the **Company > Policies > Accounting > Administrative Defaults**. As a result, all Mobile Printing jobs on all printers will be tracked with the common credentials.

Policies: Accounting > General

Printer Session Accounting Codes

When you enable the Printer Session Accounting Codes feature:

If accounting codes are available in the user session of the printer, the Printer Client (EIP) app retrieves the codes and uses them for jobs released using the app. For the desktop jobs released to a Xerox printer, if the job was submitted using a Xerox print driver, the solution attempts to add or update the accounting codes to the job. Mobile jobs always use the accounting codes from the session regardless of the Printer Session Accounting Codes setting. For the job that is modified, ensure that the associated print queue is configured with a conversion mode of **Simple**

Accounting data retention policy

When you allow user accounting to be saved, the user's last entered accounting data will be saved for each printer to which they have printed. Users will not have to re-enter the accounting information each time they print. In addition, this setting will enable direct email printing to printers when accounting is enabled at a printer, or when server-based accounting is used.

Note: **Mixed Environment for Both Accounting Methods.** If your site is using both Xerox Network and Standard Accounting on Mobile Printing-enabled printers, contact your Xerox representative.

These settings control the handling and storage of user-entered accounting information.

1. Select **Policies > Accounting > General**, select one of the following default options for: Accounting data retention policy.
   - Allow User Accounting Data to be Saved
   - Show User Accounting Data in Job History Report
2. Select **Save**.

How To Allow Direct Email Printing When Accounting is Enabled

Direct email printing is sending an email directly to a Xerox® Mobile Printing-enabled printer's IP address.

The administrator must allow user accounting data to be stored in the system to enable the email printing feature. Because there is no way to enter accounting information when using the direct email printing feature, users must have already printed to that printer through the Workplace Mobile App or Printer Client app and have entered their accounting information.

Policies: Accounting > Administrative Defaults

Note: This feature is only available with a Mobile Print Workflow license.

When you set default accounting credentials matching credentials, must be created at each printer that is enabled for Xerox Network and Standard Accounting and registered with the Xerox® Workplace Suite server.

1. From the **Company** tab, select **Policies > Accounting > Administrative Defaults**.

2. In the **Administrative Defaults** area, you may select an override setting from the list under **Override Rules**:
   - **Require User Data** - This option requires the user to enter valid credentials.
   - **Override User Data** - This option allows the system to always use the default settings below in place of values entered by the user.
   - **User default for empty credentials** - This option allows the system to use the default settings below when the credentials entered by the user are empty.
3. Under the **Network Accounting**, enter:
   - **User ID**
   - **Accounting ID**

   Note: Both IDs are required
4. Under the **Standard Accounting** section, enter:
   - **User ID**
   - **PassCode**
5. Select **Save**.

Company: Workflows

This chapter contains the configuration information for:

WORKFLOWS: PRINTER CLIENTS

The Print Client allows users to release documents uploaded to the Workplace Suite server.

1. Select **Company > Company Profile > Workflows > Printer Clients**.
2. Enter information in the Auto Exit Timer field, which determines the length of inactivity before logging out of the Printer Client App.

   Note: This setting is independent from any timeout set at the printer control panel.
3. To use a custom message for the initial Printer Client screen, for Initial Screen Message, select the **Enabled** check box.
4. Select a language.
5. Enter a custom message in the text field, or modify the existing message with your specific information.
6. Select the name to be used as the Printer Client display name on the Home screen of the printer. For Display Name, click **Workplace Suite**, or **Mobility Suite**.
7. Select **Save**.

WORKFLOWS: DESKTOP PRINT> PRINT MANAGEMENT

This feature is only available with a Print Management Workflow license.

If your site is using Client workstation print queues, management and behavior of those print queues is specified in **Company > Workflows > Desktop Clients > Print Management**.

Communications Mechanism

Desktop Clients will listen for notifications sent by the server that jobs are ready to be released to print. This setting may require the Client to allow incoming communications from the server.

- **Polling** - Job Poll Interval (seconds) - The polling rate at which the Workstation Client machines query the Workplace Suite server to determine if a print job has been released by the user at an MFP
- **TCP/IP** - This setting requires the new Desktop Client to allow incoming communications from the server, the default port number 9907 is used to communicate with the server.

When enabled with the new Desktop Client, the Client will attempt to open the Windows Firewall port 9907 automatically.

Note: This is the recommended Communication Mechanism for future and current installs.

- **Messaging**:
  - Port - Port on which the Client will listen for server notifications.
  - Allow Incoming Communications from the Server - Enabling this setting will create a Windows firewall rule on the user's workstation, allowing incoming communications over UDP on the configured port, the default port number is 9807.

Processing Intervals

Configuration Poll (hours) - The polling rate at which the Workstation Client machine queries the Workplace Suite server to determine if there are configuration updates, such as a new print queue to be added to the Workstation Client devices and printers.

Local Print Optimization

To use Local Print Optimization, the Xerox® Workplace Suite desktop client is required. When you enable the Local Print Optimization feature, the Workplace Suite Client stores a local copy and sends a backup job file to the Workplace Suite server. When jobs are released, the Workplace Suite software solution attempts to send the local copy of the job to the printer. If there is a connection issue from the local workstation to the printer, Workplace Suite sends the backup file to the printer.

The Local Print Optimization option can improve the reliability of desktop jobs that are submitted from the desktop client for later release. When the option is enabled, desktop clients are allowed to store a copy of the job on the workstation of the user and upload it to the server. When the user releases the job to a printer, the server attempts to notify the client that the job is to be released and where to send it. If the client is available to receive this request, the job is sent directly from the workstation to the printer. If the client is not available, the job is sent directly from the server to the printer.

Note: The common deployment method for the Workplace Suite Client using Local Print Optimization is automatic installation and configuration using Microsoft System Center Configuration Manager.

Enabling Local Print Optimization

To enable this feature, you are required to enable it in two places: on the server and in the desktop client.

Enabling Local Print Optimization on the Administrator Webpage

1. Select **Workflow > Desktop Print > Print Management**.
2. Select the check box for **Enabled**.

Enabling Local Print Optimization in the Workplace Suite Client

There are several methods to enable the feature on the Workplace Suite Client, see the following details:

Note: The common deployment method for the Workplace Suite Client using Local Print Optimization is automatic installation and configuration using Microsoft System Center Configuration Manager.

To enable the feature when you install or upgrade the Workplace Suite Client, do the following:

1. Copy the file `PreConfig.xml` to the same directory as the Workplace Suite Client installer.
2. Run the Workplace Suite Client installer.
3. The `PreConfig.xml` file is copied to the `Xerox Workplace Suite Client\ProgramFiles \preConfigure` folder automatically.

   Local Print Optimization is enabled on the desktop client.

To enable the feature, if the Workplace Suite Client was installed previously, do the following:

4. Copy the `PreConfig.xml` file to the following folder `C:\Program Files (x86)\Xerox\Xerox Workplace Suite Client\ProgramFiles\preConfigure`.
   A sample of the `PreConfig.xml` file is included with the Workplace Suite Software download file.

The Local Print Optimization setting is applied when the desktop client detects the server setting on the next print job, when the computer restarts, and within 24 hours of enabling the setting.

Disabling Local Print Optimization

To disable Local Print Optimization, do the following:

1. Select **Workflow > Desktop Print > Print Management**.
2. Clear the check box for **Enabled**.

   If the Local Print Optimization setting is disabled on the server, the capability is disabled on the Workplace Suite Client.

Allow Printing in Offline Mode

Note: Allow Printing in Offline Mode is supported in the Workplace Suite Client only.

Offline mode printing allows users to redirect their print jobs when the desktop client cannot connect to the server. The desktop client stores up to 10 printers that the user has printed to previously and uses those printers when it cannot connect to the server. If the user has not printed from the client, there are no stored printers for the client to redirect the jobs to. When jobs are printed in offline mode, print quotas and print rules are not applied.

Note: When the server is online again, the desktop client uploads the print history for jobs printed in offline mode.

If offline mode is enabled and the client loses connection to the Workplace Suite server, the user is prompted with a dialog box that shows a list of the stored printers and the following options:

- Ignore: If the user selects a printer then clicks **Ignore**, the print job is stored in the `Offline Jobs` folder. When the server is online again, the print job is submitted to the server.
- Print: If the user selects a printer then clicks **Print**, and the printer is accessible, the job prints to the printer directly. If the user selects a printer then clicks **Print**, and the client fails to print, an error message appears, and the print job is deleted. When the server is online again, the print job history is reported to the Workplace Suite server.

WORKFLOWS: DESKTOP PRINT > MOBILE PRINTING

This feature is only available with a Mobile Print Workflow license.

If your site is using client workstation print queues, management and behavior of those print queues is specified in

Company > Workflows > Desktop Clients > Mobile Printing.

Basic Client Printing

- Enabled - Enable occasional desktop print submission. Users may submit jobs from their PC using the standard File > Print mechanism.
- Queue Display Name - This is the display name that will be used for the shared network print queue for basic client printing.
- Select the location of the incoming print jobs - This is the location where the print driver will store the incoming print jobs.

WORKFLOWS: DESKTOP PRINT > JOB PROCESSING

Typically, this feature will be used to process print output from a specialized application that does not add the User Name in the print file in a standard way.

The Workplace Suite solution provides an administrative setting to enable Username searching. This setting is found on the **Company > Workflows > Desktop Print > Job Processing** page. The setting is called **User Name Search** and it is disabled by default.

User Name Search

User Name Search is a computational intensive feature. It is desirable to limit the number of queues which will perform this processing. It is recommended that you set up a separate queue(s) just for this feature. Refer to **Queue Association** setting below.

Some applications that submit jobs to the Workplace Suite solution may embed the job owner information in the header of the job using non-stand attributes. Typically, these are of the format of tag followed by a value. The Workplace Suite solution can be enabled to search for a customizable set of tag strings. The first match that is found will result in the solution extracting the trailing value after the tag, and assigning that as the job owner. An example might be:

@PJL SET USERNAME=“UserXYZ“

Where the tag search string would be **‘@PJL SET USERNAME=’** and the value of the tag is **‘UserXYZ’**. Workplace Suite will remove any single or double quotes, as well as parenthesis that may be around the value. If there are leading or trailing spaces around the value, those will also be removed.

Note: This feature is only supported when using Network Shared Queues.

1. Select the check box for **Enable User Name Search** to enable the feature, as it is disabled by default.
2. Add the search string in the New Value field.
3. Move the arrows in the right to slide it over in the Search Strings box.

4. The Workplace Suite solution provides an option called **Queue Association** to select which print queues will be used for the job parsing feature.

   Queue Association

   Selects the print queues which will perform job process. This is a computational intensive feature. It is desirable to limit the number of queues which will perform this processing. It is recommended that you set up a separate queue(s) just for this feature.

   Guidelines for Select Queues Feature:

   - **Select Queues** feature only supports Network queues and not Client queues.
   - If the print server that the Job Processing queue is running on is down, the job parsing will not be processed.
   - **Select Queues** will result in better performance in job parsing.

   The options are:

   - **All Queues**: This is the default option. When selected, all Workplace Suite Server queues will perform Job Parsing.
   - **Select Queues**: When selected, only the designed Workplace Suite Server queues will perform Job Processing from all available print servers.

     a. Once selected, a pop-up window appears with the available print queues. You can use the drop down menu to filter the printer queues.

     b. Use the **+** button to add the queue to the processing list.

     c. Click **OK**.

        The print queue will be listed along with the print server name.

     d. Click **Manage** to edit any changes to the settings.

5. Click **Save**.
6. The Workplace Suite solution parses the jobs submitted to the Print Queues.

   The resulting value retrieved will be used as a job owner.

7. The extracted value will be compared with the User Database based on looking for a match in the Email, User Name, or Alternate Access Card User fields.
8. The job gets mapped if it matches to any of the above fields and allows the user to release the job to a printer.

Guidelines for Conversion Mode:

- A maximum of 10 search strings will be allowed.
- Parsing is limited to the first 1000 bytes of the print job.
- The Username value extracted from the job will override any received LPR protocol Username for the job.

Note: If using Raw IP printing at release time, the retrieved Username value will not be used.

- The Workplace Suite solution will use the stored Username when a job is released to a printer, by using the LPR or IPP protocol.

Job Processing Steps:

- Add up to 10 tag strings that will be used to search.
- Workplace Suite will search the first 1000 bytes of the print job header for a set of tag strings.
- When a tag string is found, the Workplace Suite will match against the trailing value.

Note: Up to EOL or CR and will remove leading spaces and parentheses.

- Workplace Suite attempts to match against the following user fields:
  - Email Address
  - User Name: Will match against the User Name portion of the User Name field (domain and backslash are removed).
  - Alternate Access Card User
- When the first match against that is found will result in the solution.
- When the first successful match occurs, the print job will be programed with the User Name field from the User record that was matched.

WORKFLOWS: EMAIL

Note: This feature is only available with a Mobile Print Workflow license.

In the **Workflows** section, the **Email Printing Setup** area is where you enable the Mobile Print Workflow to use a custom message in the confirmation email notification.

Details

- **Show Release Documents**: The system shows Release Document Links in the email confirmation message.
- **Direct Printing Using Printer or Print Queue IP Address**: If the printer IP Address matches the email subject or email body, then the email and all attachments will be released immediately to the printer.
- **Direct Printer Using Printer or Print Queue Display Name**: If the printer display name matches the email subject, the email and all attachments will be released immediately to the printer.
- **Discard Small Image File Attachments**: Image file attachments smaller than 2 KB will be discarded.
- **Default Language**: If User has not set a preferred language, the system will use the configured default language for all email correspondence.

Custom Email Response Messages

Enabled: Enables the system to use a custom message in the confirmation email notification.

Languages: The language fields allows you to enter custom messages or modify existing messages in the available languages.

WORKFLOWS: MOBILE APP

Note: This feature is only available with a Mobile Print Workflow license.

The Mobile Print Workflow allows you to install the system's mobile app (Xerox® Workplace Mobile App) on your

mobile device for printing. This feature enables you to send your documents from the app to a network connected printer (EIP or non-EIP enabled including non-Xerox devices) or to upload them for release at a later time (e.g. using the Printer Client application).

Setup

Once you have downloaded and installed the Xerox® Workplace Mobile App onto your mobile device, you must perform the following administrative setup tasks in the order listed:

- Set the proxy settings under: **Company > Settings > Proxy Settings**
- Register your company or institution and retrieve your company code
- Set up additional printer sites for the printer devices

Proxy and Mobile App Enablement

1. Select **Company > Settings > Proxy Settings**. For information on how to enable the proxy server and addresses, refer to Settings: Proxy Settings.
2. Select **Company > Workflows > Mobile Application**.
3. To allow Xerox® Workplace Mobile App users access to the Mobile Printing feature, select **Enable mobile app printing**.
4. Select **Save**.
5. If you want to share the company code and email it to other users, click **Share Company Code**.
   - The default is to send the company code to all known users. If you select the individual user option, the To field becomes available for you to enter individual user email addresses. Select **Send**.
   - If more than 1000 users are registered in the Mobile Print Workflow, the Send Company Code to all known users feature is disabled. To share the company code in this situation, create a distribution list of all Mobile Print Workflow users, then share the company code.

   The Share Company Code email message window appears.
6. If you want to request another company code, click **Request New Company Code**.

Print the Welcome Page for the App

The Welcome Page contains a QR code that Xerox® Workplace Mobile App users are able to scan to identify the printer. The Welcome Page should be located in a convenient location near the printer. The Welcome Page also provides a convenient connectivity test between the Mobile Print Workflow and a printer.

Note: If accounting is enabled on the device, the correct administrative defaults must be configured in the **Company > Polices > Accounting** section.

The Welcome page job will appear on the **Jobs** tab. The job can be removed or it will be deleted once it has met the data retention settings.

To print the Welcome Page:

1. On the **Printers** tab, select the printer.
2. Select **Print Welcome Page** from the **Actions** menu.

3. Configure your Welcome Page settings and select **OK**.
4. A Welcome Page will be sent to that printer.
5. Place the Welcome Page in a convenient location near the printer it was printed on.

Adding an Additional Site for the Mobile App

You can add one or more sites that can be used when you add a printer device.

1. Select **Company > Settings > Sites**, click **New** from the **Actions** menu.
2. Enter the name, address and description of the site.
3. Enter the latitude and longitude of the site's location.
4. Select **Save**. If the site is added successfully, it is added to the table.

Administration

The **Mobile App Setup** area is where you configure the mobile app for use on your smart or mobile device.

Note: Apple iOS Version 9.0 or higher and Android 4.0 mobile devices are supported.

1. Select **Company > Workflows > Mobile App**.
2. Select one of the following to enable or disable Mobile App Printing:
   - **Enable Mobile App Printing (Xerox Workplace Mobile App)**
   - **Disable Mobile App Printing (Xerox Workplace Mobile App)**
3. Select one of the following for your Company Code:
   - **Share Company Code**
   - **Request New Company Code**
4. Select an Access Controls option:
   - **Private** - Users can print to your Workplace Suite server only if they are in your corporate Wi-Fi network.
   - **Public** - Users can print to your Workplace Suite server regardless of their location using either cellular or Wi-Fi connections.
5. Select **Test Connection** to verify that the mobile app setup is working correctly.
6. Select **Save**.

Security

The Security section can be found under **Company > Policies > Security**. Here security settings related to the mobile app can be configured:

- Authentication Type: Method of confirming users identity for both the Printer Client and the Workplace Mobile App.

  Xerox® Workplace Mobile App Authentication options:

  – LDAP Authentication: Users enter LDAP credentials when logging into the mobile app. To configure LDAP connections select: **Company > Settings > LDAP Connections**.

  – Confirmation Number: Users receive a unique number via email that is required to use the mobile application.
- Workplace Mobile App Login Retention: Users must provide their credentials when accessing the Workplace Mobile App. This setting controls when the user will be required to resupply their credentials.
- Set the Confirmation Number: Total number of digits required for Confirmation Number
- Set the Confirmation Number Lockout: Number of failed login attempts before user account is disabled
- Enable and set the Confirmation Number Expiration and Reset: Confirmation number will expire based on number of days set, system will send an email with a new confirmation number to the user

To configure the System Security settings:

1. Select **Company > Policies > Security**.
2. Under **Authentication Type** select a mobile app:
   - LDAP Authentication
   - Confirmation Number
3. Under **Details** enter a number for the following:
   - Confirmation Number Length
   - Maximum Failed Login Attempts

   This is the number of failed login attempts before the user account is disabled. When the user is locked out, an email is sent that contains a link to unlock the user's account.

   Note: Users can also be unlocked by:
   - Selecting the **Users** tab.
   - Selecting the locked out user.
   - Deselecting the **Locked Out** checkbox.
4. Under **Mobile App Login Retention**, if **Retain Login Credentials** is enabled, and **Expiration Time (days)** is set, when the expiration time is reached, the user will be logged out of the mobile app and will automatically log in using their retained credentials.
5. Under **Confirmation Number Expiration and Reset**, if the checkbox for enabled is selected and a number of days is set, the confirmation number will expire within that number of days.
   The expiration time is the total number of days since the confirmation number was created or last reset. When the confirmation number expires, the system will generate an email notification for enabled users containing a new confirmation number.

6. Click **Save**.

Mobile Phone Unlock

Note: Both Mobile Print Workflow and Print Management Workflow installation is required for the Mobile Phone Unlock to work. For more information, refer to Unlocking a Printer Using the Xerox Workplace Mobile App®.

1. Select **Company > Workflow > Mobile Application**.
   - Select **Mobile Phone Unlock**.
   - Select **Enable QR Code on Printer**.
2. Select **Company > Policies > Security > Printer Authentication > Basic**.
   - Select **Manage Machine Access Using Print Management**.
   - Select **Service Pathway**.
3. Select **Company > Policies > Security > Printer Authentication > Basic**. Select **Authentication**.
4. If you enable the Custom Blocking Screen, edit the Message, then add the Mobile Phone Unlock code to the Custom Message. Select **Company > Policies > Security > Printer Authentication > Advanced**.
   - Select Custom Blocking Screen Message.
   - Select each language that your devices support.
   - Add the following text to the current message: `Unlock with this Pin Number:`
   - Select **Insert Unlock Code**.

How To Use the Workplace Mobile App

1. Go to www.xerox.com/XWSsupport.
2. Select the **Documentation** tab to view the User Guide for your mobile device.

Public Printing

The Mobile Print Workflow can be configured to control the public and private access of Workplace Mobile App users to your company and outside company printers. When enabled, your mobile app users will be able to see and print their documents to your company printers and to printers that are outside your company account.

Important: To enable Public Printing, Mobile Printing must be enabled.

Do the following to enable Mobile Printing:

- Select **Company > Workflows > Mobile App**.
- Select **Enable Mobile Printing**.
- Select **Public** under **Access Controls**.

To set up Public Printing:

1. Select **Company > Workflows > Mobile App > Public Printing**.

2. Under **Details**, select one of the following options:
   - Allow users to access only your company printers
   - Allow users to access printers enabled by other companies
3. Click **Save**.

How To Find the Status or History of a Job

1. Select **Jobs > History**.
2. View the status and history information of each job.

How To Print a Document From a Mobile Device

You can print from a mobile device in the following ways:

App

When viewing a document on your mobile device, open it with the mobile app. This will enable you to choose a printer and print options or upload for printing later.

Note:

- User print preferences are initially set to match the company account, but can be changed. Some print options may not be available on certain printers.
- Selecting **Original File Size** or a specific paper size overrides scaling and paper substitution. If the printer does not have the proper paper size loaded, the job will be held for resources.
- Printing a small range from a large document does not save data charges.

Email

- **Print now**: Send or forward an email (and attachments) directly to a Xerox® Mobile Printing-enabled printer by sending the email to the Mobile Print Server email address and placing the printer's IP address as the subject of the email.

  Note: Must be setup by selecting **Company > Workflows > Email**

  Only Mobile Print Workflow jobs are forwarded to outgoing Queues.
- **Upload for printing later**: Send or forward an email (and attachments) to your company's Workplace Suite email address. It will be added to your document library in Mobile Printing where it can be retrieved with the app and printed at a later time.

  Print jobs may be retained, depending on the company Retention Policy.

  Note: If you frequently use the upload for printing later feature, you may want to add your company's Workplace Suite email address to your contacts.

How To Reprint a Document

Go to **Documents** in the mobile app and follow the printing procedures.

This applies only if the Retention Policy is not set to **Immediate**. The default behavior is for the document to be deleted immediately after printing. The Administrator can modify this setting to save documents after submission so that they are available for reprint.

How To Submit a Document to Print Later

In the mobile app, you may upload your document to save for printing later.

1. In the print window, select the option to upload the job.
2. Attach the document to an email and send to your company's Mobile Printing email address.

   It will be added to your document library in Mobile Printing, where you may retrieve it with the app and print it later. It will be retained depending on the company retention policy configuration.

How To Reset a Company Code

1. Select **Company > Workflows > Mobile App**.
2. Click **Request New Company Code** under your Company Code.
3. Communicate the new code to your users.

   Note: In the Company Profile settings you can choose to include or exclude the company code on the Welcome Page.

4. Create a new Welcome Page to display with each printer.

   Note: For more information, refer to *Print a Welcome Page for the App*.

How To Configure Mobile App Usage to Your Company's Local Wireless Network Only

Configuring the mobile app for your company's local wireless network will allow mobile app users to access stored documents and your company's printers only when they are connected to your company's local wireless network.

1. Select **Company > Workflows > Mobile App**.
2. Under **Access Controls**, select **Private**.

   Note: Changing the **Access Controls** setting to **Private** also disables Public Printing and the **Public Printing** settings (**Company > Workflows > Mobile App > Public Printing**) will change to **Private**.

How To Print Email from the Mobile App

To set up Xerox® Workplace Mobile App to configure an IMAP/POP email connection and print emails from within the application:

1. Select **Company > Workflows > Mobile App**.
2. Select the **Enable Xerox Workplace Mobile In-App Email Printing**, checkbox.
3. Select a Protocol:
   - Internet Message Access Protocol (IMAP)
   - Post Office Protocol 3 (POP3)

4. Enter a server in the **Server** field.
5. Enter a number in the **Port** field
6. Enter a folder in the **Watch** Folder field (if IMAP Protocol is selected above).
7. Select an **Authentication Mode** from the list.
8. Select an **SSL Mode** from the list.
9. Click **Save**.

Push Notifications

Mobile Print Workflow supports the built-in job notification system for iOS and Android users of the mobile app to send mobile device notifications in addition to the current email notifications. Users must have enabled push notifications when they set up the mobile app.

WORKFLOWS: IOS NATIVE PRINTING

Note: This feature is only available with a Mobile Print Workflow license.

You can submit print jobs to the Mobile Print Workflow using the built-in printing capability of your iOS device and release the jobs later to any Workplace Suite enabled printer using the Xerox® Workplace Mobile iOS app. A printer named "Xerox® Workplace Suite Mobile Printing" or name you choose to display, will be displayed on your iOS device printers list. After printing via AirPrint to a "Xerox® Workplace Suite Mobile Printing" printer, release these jobs from the mobile app or the Printer Client App. iOS users can now print documents using AirPrint. There are two ways to discover the Mobile Printing AirPrint printer:

- Local discovery - If this is enabled, the Workplace Suite Server must be on the same WiFi subnet as the iOS device.
- DNS server - If the phone is set up to connect to the DNS server, when a user opens a document and selects print, the iOS device performs a DNS search for the local WiFi network for AirPrint-enabled printers.

To utilize both methods the DNS name should match the Local Discovery Name

iOS Enable Native Printing

Server Enablement

Workplace Suite hosts an AirPrint-enabled virtual printer. When the user prints to the Mobile Printing AirPrint printer, Workplace Suite receives a pdf file, which is uploaded to the server. The pdf file can later be released using any Mobile Print Workflow release method. To enable iOS Native Printing with Auto Discovery:

- Install the Apple Bonjour Print services software on the Server
- Download and install Bonjour Print Services for Windows and install on your Mobile Printing Server: http://support.apple.com/kb/DL999
- From the Workplace Suite Administrative web page go to **Company > Workflows > iOS Native Printing** and enable it.

iOS End User Experience

When printing from AirPrint, the user selects the Workplace Suite printer and a logon window displays requesting the user's login credentials. The Credentials required are the same as the mobile app. These are set in **Company > Policies > Security > Printer Client** tab. If LDAP Authentication is enabled then the user would enter Domain Name\Username and their password. If Email and Confirmation Number is enabled the user would enter Email Address and Confirmation number as the password.

After the user successfully logs in, the credentials are cached on the device and are not required again until the user's password or confirmation number changes.

iOS Troubleshooting

No printers visible on Apple iOS devices.

Assuming Bonjour Print Services is installed on the server, iOS print feature is enabled and iOS device is on the same subnet as the server.

The following ports must be open on your firewall:

PORT	TCP OR UDP	SERVICE OR PROTOCOL NAME
631	TCP	Internet Printing Protocol (IPP)
5353	UPD	Multicast DNS (MDNS)

For support, go to https://support.apple.com/en-us/HT202944.

Company: Licensing

The **Licensing** section provides License Host Details and Server, Printer, and Print Queue summaries as well as a License Features History.

LICENSING DETAILS

The License Host Details include:

- Name
- Hardware Address
- Primary Serial Number
- Status
- Last Communication Date Time

The Workflow Summary include:

- Mobile Printing
- Print Management
- Content Security

The Microsoft® Office Conversion Servers Summary include:

- Available
- Enabled
- Remaining

The Workflow Device Connectors Summary (WDC) include:

- Available
- Mobile Printing
- Authentication/Desktop Print
- Content Security
- Printer Client/Usage Tracking
- Remaining

License Features History

The License Features History has the following options:

- Activate License
- Export License
- Export Activation Keys

To Activate a License:

1. Select **Company > Licensing**.
2. From License Features History, select **Actions > Activate License**.

3. Select one of the following Activation Options:
   - **Activate Online**: Select this option if your network allows outgoing connection to the Xerox licensing server.
     1. Enter the activation key. A default serial number exists.
     2. Select **Activate**.
   - **License File**: Select this option if your network does not allow outgoing connection to the Xerox licensing server.
     1. Choose the file.
     2. Select **Activate**.

Note: Only the activation keys that were activated online using the **Activate Online** method are listed in the exported CSV file.

To Export a License:

1. Select **Company > Licensing**.
2. From License Features History, select **Actions > Export License**.

To Export a Activation Key:

1. Select **Company > Licensing**.
2. From License Features History, select **Actions > Export Activation Keys**.

   A .csv file gets downloaded and the name of the file will be Activation_Keys_YYYY.MM.DD.csv. The .csv file lists the Activation Keys and the date it was activated on.

Maintenance

This chapter contains the configuration information for:

MAINTENANCE: BACKUP AND RESTORE

- The Backup and Restore feature is not available for new installations of Xerox® Workplace Suite and for systems that are configured for an external database.
- The new installations on Workplace Suite use a Microsoft SQL Express 2017 database. To manage that database, use the Microsoft SQL Management Studio software or a similar tool.

Important: Workplace Suite is not available while backing up the system, so this should be done during off-hours. Follow your recommended corporate best practice to backup or restore the Workplace Suite server. You should backup the server prior to any actions, such as installing an upgrade, which might result in irreversible changes to the system. This feature is only available to Workplace Suite systems that are not using an external database.

Select **Company > Maintenance > Backup and Restore**.

The **Actions** menu includes the following functions:

- **Backup** - Backs up the selected database
- **Restore** - Retrieves a previously backed up database
- **Delete** - Removes the selected database

Backup

To back up a database:

1. Select **Company > Maintenance > Backup and Restore**.

   The **Database Settings** display the Database Name and Version.

2. From the **Actions** menu, select **Backup**.

   The Backup Database window appears.

3. Select **Yes**.

   A Backup Successful message appears.

   Important: Backup files are stored locally on the server and can be found by going to **C:\PROGRAMDATA\Xerox\XMP\BackupAndRestore**. The **ProgramData** folder may be hidden on the file system. To view the **ProgramData** folder, disable file extension and folder hiding.

Restore

To restore a backup database:

1. Select **Company > Maintenance > Backup and Restore**.

   The **Database Settings** display the Database Name and Version.

2. Select the checkbox for the database you wish to restore.
3. From the **Actions** menu select **Restore**.

   The Restore Database Warning message appears.

4. Select **Yes** to restore the database.

   A Restore Successful message appears.

Delete

To delete a backup database:

1. Select **Company > Maintenance > Backup and Restore**.

   The **Database Settings** display the Database Name and Version.

2. Select the checkbox for the database you wish to remove.
3. From the Actions menu, select **Delete**.

   The Delete Files warning message appears.

4. Select **Yes**.

MAINTENANCE: LOGS

The System Logs Manager is used in conjunction with Xerox support personnel to download Logs that helps to troubleshoot and resolve issues.

To download and view the log files:

1. Select **Company > Maintenance > Logs**.
   A System Logs Manager window appears.
2. Select the tab for the type of log files you wish to download and view:
   - **Applications**
   - **Conversion Jobs**
3. The System Logs Manager has the following filter options:
   - The **Files** indicator shows the total number of Log files available in the System Logs Manager of the selected tab.
   - The **Page** indicator shows which page is being viewed of the total number of pages.
   - The **Items Per Page** indicator lets you set the number of Logs displayed per page.
   - The **Search** option lets you to filter the Logs by Log Name.

4. Apply the required filters and click **Actions** and select:
   - For **Applications** tab:
     - **Export All Logs**: Exports the Logs from all the pages.
     - **Export Displayed Logs**: Exports the Logs displayed on the page.
     - **Log File Collection Assistant**: Exports the Logs based on the user requirement with specific issue type, for more information refer to Log File Collection Assistant.
   - For **Conversion Jobs** tab:
     - **Export All Logs**: Exports the Logs from all the pages.
     - **Export Displayed Logs**: Exports the Logs displayed on the page.

Note: For **Export All Logs** and **Export Displayed Logs** actions, a zip file named "Xerox Workplace Suite_ Suite Version Number_Date" is downloaded in your downloads folder of your local machine.

Log File Collection Assistant

The Xerox® Workplace Suite allows the user to download the log files from the Workplace Suite environment. The **Log File Collection Assistant** at the Maintenance section helps the user to download the log files based on a specific issue type. The user will drive a wizard that generates a zip file of the required log files.

Guidelines to Download the Log Files

- File Name should be entered for Log file collection, if you have not entered the file name you will get an error message "File Name is required.".
- If the File Name entered has a non-standard character you will get an error message "File Name is invalid.".
- At least one Issue Type must be selected before downloading the log files, if you have not selected the Issue Type, you will get an error message "At least one issue type is required.".

Downloading the Log Files

To download the specific Log Files:

1. Select **Company > Maintenance > Logs**.

   The System Logs Manager window appears.

2. Select **Actions > Log File Download Assistant**.

   A log file collection wizard appears.

3. On the File Name enter the required `File Name` for your Log File Collection zip file and Click **Next**.

   The Issue Type section appears.

4. Select the type of issue that occurred from the following list with the problem associated with specific section:

   Configuration

   - Licensing
   - Printer Client Application Installation
   - Printer Authentication Enablement
   - Usage Tracking Enablement
   - Data Import/Export (e.g. LDAP, printers, users, sites, etc.)
   - Printer Discovery
   - Confirmation Number Reset
   - Record Retention Manager

   Printing

   - Printer Client (print, copy, and scan)
   - Network Print Queue

   Note: Additional log files from the Print Server are required. These log files can be retrieved via **Print Queues > Print Servers > Actions > Select Print Server > Download Log File**.

   - Desktop Client Print Queue

   Note: Additional log files from the user's computer are required. These log files can be retrieved via **Print Queues > Desktop Clients > Actions > Select Desktop Client > Download Log File**.

   - Email Workflow
   - Print Portal (Chrome Extension)

   Note: Additional log files from the Chrome Extension application are required. In the Chrome app, click on **Export Log** to obtain log file.

   - Print Portal (iOS/Android)

   Note: Additional log files from the Print Portal application are required. In the mobile application, select **Settings > Application Logs** to obtain log file.

   - Auto Release Job
   - Job Accounting
   - Print Rules
   - Job Content Security

   Authentication

   - Printer Client Logon
   - Printer Authentication

- Single Sign-On Application

Reporting

- Usage Tracking - Data Import
- Usage Tracking - Dashboard Manager
- Job Reporting Export

Others

- Other general log files will be collected.

5. After selecting the required logs, Click **Next**.

   The Date Occurred section appears.

6. On the Date Occurred section select the required filed from the below list and click **Next**.
   - Today
   - This Week
   - This Month

   The Summary Page appears.

7. Review the Log File Collection summary. Click **Finish**.

   Note: You can also click back to make changes on any of the previous section.

8. Once the specific issue log files are obtained from all the servers, they will be available as zip file on downloads folder on your local machine.

MAINTENANCE: PRINTER MODEL UPDATE

After completing a Printer Model Update, printers with an incorrect model in the Printers list can be selected for a repair action.

Select **Company > Maintenance > Printer Model Update**.

Update from File

1. Select **Company > Maintenance > Printer Model Update**.
2. Select **Browse** and then select a Printer Model Update zip file.
3. Select **Apply**.
4. After the Printer Model Update is complete, repair the printers with an incorrect model in the Printers list:
   a. Select the checkbox next to each printer with an incorrect model.
   b. From the Actions menu, select **Repair**.

For more information, see: Printer Model Update Installation Guide

MAINTENANCE: SYSTEM HEALTH DASHBOARD

The system provides the administrator with a comprehensive summary of the health of each of the Workplace Suite components.

Select **Company > Maintenance > System Health Dashboard**.

The System Health Dashboard provides the following information:

- Database Details
  - Server Name
  - Database Name
  - Database Version
  - Application Version
- Usage Tracking Details
- Service Components Details
- Conversion Service Print Driver Details
- Settings Details
- System Utilization

Jobs

This chapter contains:

Print jobs are submitted on Workstation Clients and are held until released by the user on login at the device. Jobs that have been submitted but not yet released will be found listed in the **Jobs** tab under **Content**. Jobs that have been released and are in the process of spooling to the MFP will be found listed in the **Jobs** tab under **Current**. Jobs that have finished spooling to the MFP will be found listed in the **Jobs** tab under **History**.

Note: Jobs submitted to the system by a user who is not currently in the user list will be listed in the Unregistered list. Jobs submitted by an unregistered user will appear in the Content list once the user is registered.

Unregistered

Jobs submitted to the system by a user who is not currently in the user list will not be listed in the Content list. Jobs submitted by an unregistered user will appear in the Content list once the user is registered.

1. Select **Jobs > Unregistered**.

   All jobs submitted by an unregistered user appear.

History: Export

1. Select the **Jobs** tab.
2. From the **History** tab, apply any desired filters.
3. Select **Export This Page** from the Actions menu.
4. Locate the download location and open the file.

   The default filename for the export is: JobHistory_CurrentPage.csv

Note: To export all data in the table, select **Export All Pages** from the Actions menu. The default filename for the export of all data is: JobHistory_AllPages.csv

Current: Export

1. Select the **Jobs** tab.
2. From the **Current** tab, apply any desired filters.
3. Select **Export This Page** from the Actions menu.
4. Locate the download location and open the file.

   The default filename for the export is: JobsCurrent_CurrentPage.csv

Note: To export all data in the table, select **Export All Pages** from the Actions menu. The default filename for the export of all data is: JobsCurrent_AllPages.csv

Content: Delete

You can manually delete stored jobs from the Content jobs list.

1. Select the **Content** list from the **Jobs** tab.

   The list of jobs that have been processed by the system within the time period set by the administrator.

2. To delete a job from the list:
   a. Select the checkbox for the job you wish to delete.
   b. Select **Delete** from the Actions menu.

Printers

This chapter contains:

Workflows

Primary Workflow settings are established for selected printers. Enabling one or more items under each Workflow requires the use of a Workflow Device connector. The Workflow settings are applied when a printer is added as a New printer, is Repaired, or when settings change.

To access the Workflows window, click the **Printers** tab, **Printers** subtab, select a printer, then click **Features**.

Mobile Printing (Connections: 1)

Note: To support workflows, a Xerox® Mobile Print Workflow License is required.

The following features are available when Mobile Printing is enabled:

- Email Workflow
- Workplace Mobile App (Submit and Release)
- Printer Client Support
- Desktop Print: this feature lets you send a job to a Mobile Printing incoming print queue
- Only printers with Mobile Printing enabled can print Mobile Print Jobs.

Print Management (Enable either one or both features utilizes one Workflow Connector)

Note: Authentication and Desktop Printing require a Xerox® Workplace Suite Print Management Workflow License.

Authentication

- Authentication controls the use of the Xerox printers. Users are required to identify themselves before accessing the device.
- The Authentication workflow configures the Convenience Authentication capability of the Xerox multifunction printers.

Desktop Printing

- Desktop Printing enables the submission and secure release of print jobs. Users are required to identify themselves before the job is printed on a particular device.
- If enabled, users can request that print jobs are released from a given device. The request is made using the Printer Client App, or automatically when users authenticate or scan their badge or ID. This type of authentication is accomplished using a network appliance.
- Only Printers with the Print Management Workflow connector enabled can release the secure Jobs.
- The Print Management Workflow supports Printer Client functionality.

Note: Only jobs associated with the Workflow connector enabled on the printer can be released to that printer.

Content Security (utilizes one Workflow Connector)

When Content Security is enabled on a printer, an administrator can create global content profiles and set search strings to track identified documents processed at printers. The documents are searched for matches to an existing Content Profile.

Printer Client / Usage Tracking (Enabling either one or both features utilizes one Workflow Connector)

Printer Client (Print Anywhere)

- Printer Client enables the Printer Client App on supported Xerox Printers.
- You can use the Printer Client feature to release both Print Management or Mobile Printing Jobs, depending on enabled Workflows for that printer.
- Copy and Scan functionality is available on Xerox® AltaLink® printers and Xerox® VersaLink® printers only.
  - When you use the Scan To Email feature, the Xerox® Workplace Suite Server User List appears. Select email recipients from the list. Use LDAP Import for a comprehensive list.
  - Copy and Scan job data is stored in the Job History. You can track Copy and Scan jobs in Job Reporting, when it is enabled.
  - For more information about enabling and using Copy or Scan, refer to the *Xerox® Workplace Suite Troubleshooting Guide*.

Usage Tracking (Network Accounting)

Note: For more information, refer to Settings: Job Reporting.

- Usage Tracking (Network Accounting) enablement. When enabled, accounting data can be retrieved from Xerox printers that support Network Accounting and is used for detailed Job Reporting.
- Each printer that is enabled for this workflow is queried for all Job data including Print, Copy, Scan, Fax jobs.
- Data is merged with the server data and is available in the Job Reporting output.
- Printers enabled for Usage Tracking (Network Accounting) reports include all applicable jobs types: Print, Fax, Copy, and Scan. Printers that are not enabled for Usage Tracking report only Print jobs submitted through the Xerox® Workplace Suite, with a reduced set of attributes.
- If Usage Tracking (Network Accounting) is enabled for a printer, only Printer Network Accounting jobs are listed in the Usage Report. If Usage Tracking is not enabled, only Workplace Suite jobs are added to the Job Reporting Report.

Accounting Credentials

Note: This feature is only available with a Mobile Print Workflow license.

To access the Workflows window, click the **Printers** tab, **Printers** subtab, select a printer, then click **Features**.

Select the accounting credential type for supporting all Mobile Print Workflow jobs. When using Authentication and Usage Tracking, Network Accounting is applied to Copy, Scan, and Fax jobs. The Network Accounting feature is unavailable for Xerox printers that do not support accounting.

For Accounting Credentials, select one of the following default options:

- **No Accounting**: No accounting credentials are supplied when using the mobile app, or when using Authentication.
- **Network Accounting**: User must supply their Network Accounting User Name and ID when using the mobile app. Stored credentials are passed to the printer when using Authentication.
- **Standard Accounting**: User must supply their Standard Accounting User Name and Password when using the mobile app.

Note: The accounting mode selected must match the accounting mode that is set at the printer.

TERMS USED IN THE ACCOUNTING SECTION

- **Accounting Credentials:** Account ID, User ID, and Password sent with the job
- **Default Accounting Credentials:** The accounting data entered in Mobile Printing
- **Standard Accounting:** The system is designed to validate the accounting credentials against a database stored internally on the printer
- **Network Accounting (also known as Job Based Accounting):** The system can be configured to validate the accounting credentials against a database stored internally on the printer, or an external database hosted on the accounting system
- **Validation**: The printer checks that it has accounting credentials stored

Secure Printing

This feature is only available with a Mobile Print Workflow license.

To access the Workflows window, click the **Printers** tab, **Printers** subtab, select a printer, then click **Features**.

The Xerox® Secure Print feature allows you to control the print timing of your documents. When the user submits a document, they enter a passcode and then must enter the same passcode when retrieving the job, at the printer.

By default, users have the option to use Secure Print when printing to Xerox® Secure Print capable printers. This option requires no action on the part of the administrator.

For extra security for a Xerox® Secure Print capable printer, you can configure Mobile Printing to require that Secure Print must be used for all jobs sent using Mobile Printing to that printer.

Under **Secure Printing**, select or deselect **Secure Print Required** .

Important: When using the Printer Client App on Secure Print enabled printers, users enter their Mobile Printing Confirmation Number to release jobs, not a Secure Print Release code.

Auto Release All Jobs

Note: This feature is only available with a Print Management Workflow license.

To access the Workflows window, click the **Printers** tab, **Printers** subtab, select a printer, then click **Features**.

Auto Release All Jobs controls if the print jobs are sent to the printer immediately upon authentication, either by card swipe / alternate login, or by swiping a card at a network appliance. If this setting is enabled, the printers typically do not have the Printer Client Application installed.

Auto Release All Jobs

- **Never**: If jobs are released on this device, it will be only through the Printer Client Application after the user logs in.
- **Using Access Card or Alternate Login**: Held print jobs are released automatically when the user completes the login sequence with card or alternate login. Optionally, the administrator can enable the capability to prompt the user to determine if they would like to release their jobs or not.
- **Using Network Appliance**: Held print jobs are released automatically when the user scans a card at a mapped network appliance associated with this printer.

Printers

The Printers tab is where you can register and maintain the list of printers available to be used by Xerox® Workplace Suite.

A list of registered printers is displayed in a table. Mouse over the icons on the right to indicate the printer capabilities:

- **Features**: Mobile Printing enabled, Authentication enabled, Desktop Print enabled, and Content Security enabled.
- **Options**: Printer Client Application, Auto Release All Jobs, Usage Tracking, Secure Printing, and Accounting Credentials.

Mouse over the icons to indicate Preview Welcome Page, Printer Status, Color Capable, 2-sided, and Stapling capabilities.

The **Actions** menu provides a list of tasks that can be performed:

- **New**: Create a printer for use with Workplace Suite.
- **Import**: Creates printers based on information contained in a CSV file. Use the Import template for assistance with file format.
- **Export This Page**: Creates a CSV file that includes all the printer device information for the printers displayed on the page.
- **Export All Pages**: Creates a CSV file that includes all printer device information with enforced filter.
- **Change Site**: Use this option when your printer is moved to a new building or to make the printer show up in a different location on the Xerox® Workplace Mobile App map.
- **Enable Printer**: Make a printer usable by Workplace Suite.
- **Disable Printer**: Make a printer unusable by Workplace Suite, but leave it in the discovered list.
- **Modify Features**: Apply settings to multiple printers at one time.
- **Print Welcome Page**: Display the Welcome Page for the printer. It can also be used as a test page. There is no charge for this feature; it does consume any job credits. It contains user instructions for obtaining the mobile app.
- **Repair**: Attempts to reset the print device to the settings needed for proper communication.
- **Delete**: Removes the printer from the discovered printers list. This feature does not remove the IP address from the Discovery Profile scan.

The **Page** indicator shows the specific page in the table of printers that is being viewed from the total number of pages.

The **Items Per Page** indicator lets you set the number of printers that are displayed per page.

The **Sort By** menu lets you sort the list by:

- Name A-Z
- Name Z-A
- IP V4 Address ASC (ascending)
- IP V4 Address DSC (descending)

- Model A-Z
- Model Z-A
- Site A-Z
- Site Z-A
- Last Communication Date ASC
- Last Communication Date DSC

The **Filter By** menu lets you filter the list by:

- Added in last 24 hours - shows newly discovered printers
- Last 14 days
- Last month
- Added in last 3 months
- Enabled with errors - printer is enabled, but there was a problem with one or more of the enabled features
- Enabled
- Usage Tracking: Enabled
- Usage Tracking: Enabled with errors
- Disabled by administrator
- Insufficient licenses
- Pending Discovery - device is in the process of being added
- Unable to communicate with the device - indicates an error requiring administrator intervention
- Not Enabled - device found by discovery profile, but is not enabled yet

The **Search** field lets you quickly find specific printers in long lists.

ADDING A NEW PRINTER

To add a printer, use an IPV4 address. If DHCP is in use, add the printers using the Discovery method. For more information, refer to the *Discovery* section.

1. Select the **Printers** tab.

   The Printers list appears.

2. Select **Actions > New**.

   The Create New Printer window appears.

3. On the Details tab, enter the IP Address of an EIP-enabled, non-EIP, or non-Xerox device that resides within your firewall.
4. Enter the Display Name that you want to use for the printer.

5. Select the Printer Language that you want to use for the printer.
   - PCL 6
   - PostScript: The default language is PostScript.
6. From the list, select the Protocol that you want to use for the printer.
   - **Raw or LPR**: The protocol used is auto-detected. The Raw protocol uses port 9100.
   - **IPP over SSL**: This protocol uses port 443 and is not configurable.
   - **Raw TCP Port**: For this protocol, type the port number to be used. Defaults to Port 9100 and can be changed after you add the printer.
   - **LPR**: The LPR protocol uses port 515 and is not configurable. LPR Protocol is recommended if you use Accounting.
7. To select an encoding scheme, on the **Details** tab, select the **Character Encoding** used by the printer. Character encoding is used to display the Job Name and User Name on the Banner Page, and displayed on the printer. To use this feature, the printer must also be configured to support your selected encoding scheme.
8. To release jobs from the printer to the Fiery® Device for the users with devices set up to the Dual IP Fiery® configuration, enable the check box, **Print to Alternate IP Address**. Once enabled, all print paths will direct print jobs to the alternate IP address instead of the printer IP Address.

   Note: For details on using the setting **Print to Alternate IP Address**, refer to Enabling the Printer to Release the Job to the Fiery Controller section.
9. The Pull Groups feature is available only with a Print Management Workflow license. On the Pull Groups tab, ensure that the Groups are in the appropriate field, either Unassociated Groups or Associated Groups. To move a group, select it, then click the arrow buttons.
10. On the Features tab, select the appropriate Workflows. For more information, refer to Workflows.
    - **Mobile Printing**
    - For the **Print Management** workflow, select
      - **Authentication**
        - **Xerox Secure Access Reader Support**
      - **Desktop Print**
    - **Printer Client/Usage Tracking**
      - **Install Printer Client**
        - **Enable Copy**
        - **Enable Scan**

    Note: Enable Copy and Enable Scan does not enable all the required printer features.

    For details, refer to Enabling Copy and Scan.

    - **Usage Tracking (Network Accounting)**

11. Select the appropriate **Accounting Credentials**. For more information, refer to Accounting Credentials .
    - No Accounting
    - Network Accounting
    - Standard Accounting
12. If necessary, select **Secure Printing > Secure Print Required**.
    - **Secure Print Required**
13. Select the appropriate Auto Release All Jobs option. For more information, refer to Auto Release All Jobs.
    - Never
    - Using Access Card or Alternate Login
    - Using Network Appliance

> **Caution:** When you select Never and disable the Printer Client Application option, you cannot release held print jobs on the device.

14. On the Site tab, select **Change**.
15. Select the appropriate Site, then select **OK**.
16. On the Administration tab:
    - Select **Administration Settings**, then provide the required information:
      - Username
      - Password
    - Device Management
      - SNMP v1/v2
        - Set Community Name
        - Get Community Name
      - SNMP v3

Note:

- If you select SNMP v1/v2, use the **Get Community Names** and **Set Community Names** as defined on the device in the Xerox® CentreWare Internet Services software.
- Mobile Print Workflow supports manual printer addition and discovery using SNMP v3. You cannot enable SNMP v3 using the CSV import method for adding printers.

17. To enable the printer, from the top right section of the screen, select the **Enable Printer** check box.

18. Select **Save**.

    The Create New Printer window closes. The Printer List appears with your printer at the top, and a status of pending discovery. When the device discovery completes successfully, the status appears as enabled with a green icon and check mark.

Note:

- If you want to see status changes as they occur, enable **Automatic Refresh** at the top of the printer list.
- If the device status appears as a red X, select the printer. To view the error message, hover over the icon.
- To correct the device registration settings, select the printer. Retype the IP address, Username, and Password, then ensure that the device that you are trying to add is within your firewall.
- To sort the list of printers, use the Sort by and Filter by options. You can search by model, IP address, or location. Type text in the **Search** field, then select the **Search** button. The search results display in the table.

IMPORT

Before importing a CSV file, it is highly recommended to first run an export to preview the layout and use as a template. See Creating a .csv File for Importing Printers for details

To import a list of printers:

1. On the **Printers** tab, select **Import** from the **Actions** menu.

   The Import Printers window appears.

2. Select **Choose File** and navigate to the CSV file you want to import, and select **Open**.
3. Select **Next** and review the import data.

   The Import Data Validation Details window appears.

4. Select **Import**.

   The printer CSV file is imported to the list of printers and imported printers are automatically enabled.

Note: CSV files used with a given version of Print Management Workflow may not be compatible with later versions of Workplace Suite. Always refer to the current Administration guide for information.

Note: For best results when using .csv import, ensure that your browser language is set to the same language as the server on which Workplace Suite is installed.

CREATING A .CSV FILE FOR IMPORTING PRINTERS

The CSV Columns are not order specific. Each column has an index number, which represents the column value. For details, refer to the following guidelines.

Important: The CSV file from Mobile Printing Solution 3.x, Workplace Software 1.x, and older versions of the software are not compatible with the newer release of Workplace Suite software.

Guidelines

- When you add a printer, by default the **Company > Settings > Feature Defaults** settings are used. When you use the CSV method to import the data, values that exist override these default settings.
- Row one is the Index row and is mandatory, and remains unchanged.
- Row two is the Description row and is mandatory, and remains unchanged.
- Columns can be in any order as long as the appropriate index is set.
- When you import, to add or change the data on that row, you edit the Change Column Index # 999 number from a 0 to a 1.
- Change Column Index #: 999, where 0=no change 1=Change.
- When you export the .csv file, the change column defaults to 0. If you do not change it to a 1, then any rows that are updated are not processed.

The key required fields or columns are as follows:

- Printers: IP Address
- Sites: Site Name

Note: If this field does not exist, the record is not created or updated.

CSV Read Only Fields

New read only fields have been added to CSV export. These fields can be viewed for reporting purposes but are ignored on import. These include the following fields:

- Manufacturer
- Model
- Serial Number
- MAC Address
- Protocol
- Port Number
- Last Discovered
- Printer Status (Enabled, Enabled with errors, Unable to Communicate, etc.)
- Printer Client Application Install status (Installed, Unable to connect to printer, etc.)

Add/Change Printer Using Import

To load or import a list of EIP-enabled, non-EIP and non-Xerox Printer devices in a batch by adding device information to a CSV (Comma Separated Value) file. You must download a CSV template file and add the list of print devices.

Another use of this CSV import feature is to change existing printer information. To do this, export your current printer information, change any non-read only values (except IP Address, which is a key field), such as display names, and re-import the file.

1. To download the sample Printer Template CSV file:
   a. Select the **Printers** tab. The Printers list displays.
   b. Select **Actions > Import**.
   c. Select **Download Example**
   d. Save the Printers_CurrentPage.csv file. The template file can be edited with any text editor, such as Notepad. Note the location of the file in case you need to edit it in the future.
2. To add devices to the Printer Template CSV file:
   a. Open in Excel and make sure to save the file as CSV (Comma delimited) (*.csv).

Note: For all devices, the IP Address is required. For Xerox® EIP devices, the Username and Password are required. Refer below to the requirements for the field names in these columns. For non-Xerox devices, the following fields are used: IP Address, Display Name, Site Name, Protocol, Printer Language, and GET Community Name. All other fields are ignored.

When editing the template, keep the index row (row 1) and the description row (row 2) and add one row for each device to be added.

To create an example printer template file, add devices using the manual method. Then use the Export All Pages feature on the Printers page to download a sample.

b. Fill in the printer values using one row for each device starting at row 3 (keep the header and description row intact). The requirements for the Field Number and Name columns are:

- 999 – Change – Change the 0 in this field to a 1 if any values are changed
- 100 – IP Address – Required for Xerox® EIP, Xerox non-EIP and non-Xerox devices
- 201 – Manufacturer (Read Only)
- 200 – Model (Read Only)
- 202 – Serial Number (Read Only)
- 203 – MAC Address (Read Only)
- 204 – Port Number (Read Only)
- 205 – Last Discovered (Read Only)
- 206 – Status (Read Only)
- 207 – App Install (Read Only)
- 101 – Display Name
- 102 – Site Name
- 150 – Install Printer Client – 1 = Install Printer Client on Printer, 0 = Don't install
- 300 – Protocol – Enter one of the following to set printer protocol:
  - RAW-LPR
  - IPPS

Note: IPPS represents iIPP over SSL.

- 301 – Printer Language – Optional for Xerox EIP, Xerox non-EIP and non-Xerox devices. The default is PostScript®. Enter PostScript or PCL 6.
- 400 – GET Community Name – Required if printer has non-default SNMP GET string for Xerox EIP devices; enter the non-default SNMP GET string from printer.
- 401 – SET Community Name – Required if printer has non-default SNMP SET string for Xerox EIP devices; enter the non-default SNMP SET string.
- 402 – Printer Login User Name
- 403 – Printer Login Password
- 500 – Pull Groups

3. After editing the CSV file:
   a. Browse for the file.
   b. Select the file.
   c. Select **Next**.
4. Go to the Summary area and verify the information is correct.

5. If the Summary area does not meet your expectations, re-edit the file and re-import it. If it shows what you expected, click Import.

   Note: If there are errors, click Download Status File to view the errors. The file displays a new Message field that describes the errors.

6. Select **Close**.

EXPORTING A LIST OF PRINTERS

You can export the entire printer list to a CSV file.

1. On the **Printers** tab, select **Export All Pages** from the Actions menu.

   Note: To export the current page from the printer list, select **Export This Page** from the **Actions** menu. A file named Printers_CurrentPage.csv is saved.

   A file named Printers_AllPages.csv is saved.

2. Locate the download location and open the file.

   The exported list of devices displays.

   Note: For best results when using .csv export, ensure that your browser language is set to the same language as the server on which Workplace Suite is installed.

CHANGE SITE

The discovery profile is associated with a site, and any printers discovered with that discovery profile are automatically assigned to that site.

Note: If multiple discovery profiles (associated with different sites) discover the same IP address, the printer will be associated with the site that is set by the first discovery profile to discover the printer.

To change the site associated with a printer:

1. Select the **Printers** tab.
2. Select the checkbox for the printers you wish to change.
3. From the **Action** menu, select **Change Site**.

   The Change Site caution message appears.

4. Select **OK** if you are sure you want to change the site for the selected printer(s).
5. Select a different site, then select **OK**.

ENABLE PRINTER

1. On the **Printers** tab, select the checkbox for the printer you wish to enable.
2. Select **Enable** from the Actions menu to enable the selected printer.

   A confirmation message displays.

3. Select **Yes** to enable the printer.

Note: These steps only apply if a printer has been added or discovered, and is in the list of printers.

DISABLE PRINTER

Disabling a printer makes it unusable for Mobile Printing and frees up any device license which may be in use by that printer. Disabled printers are also removed from the mobile app.

1. On the **Printers** tab, select the checkbox for the printer you wish to disable.
2. Select **Disable** from the Actions menu to disable the selected printer.

   A confirmation message displays.
3. Select **Yes** to disable the printer.

DIRECT PRINTING

Direct Print is a Workflow feature that allows desktop printing directly to a printer. Direct Print provides a Direct Print submission path using either the Workplace Suite Client or a shared windows network queue. For further information, and instructions for configuring, enabling, and disabling Direct Print, refer to Direct Print.

MODIFY FEATURES

To modify features for the selected printers:

1. Select the **Printers** tab.

   The Printers window appears.
2. Select the check box for each printer whose features you want to modify.
3. From the Actions menu, select **Modify Features**.

   The Modify Features window appears.
4. Select the features that you want to modify:
   - **Authentication**
     - **Do not change device configuration**: Current settings are maintained on the device.
     - **Disabled**: Remove authentication settings from the device. All users can walk up to the multifunction printer and use the available features.
     - **Enabled**: Install authentication settings on the device as configured in the **Policies > Security > Authentication**.
   - **Desktop Print**
     - **Do not change device configuration**: Current settings are maintained on the device.
     - **Disabled**: Users can print from their personal computer, but cannot release print jobs from this printer device.

    - **Enabled**: Users can print from their personal computer, jobs are held, and users can release print jobs from this printer device. Release print jobs through the Printer Client Application, or through auto-release of all jobs.
- **Mobile Printing**
    - **Do not change device configuration**: Current settings are maintained on the device.
    - **Disabled**: Users cannot print from their mobile device and cannot use email to print.
    - **Enabled**: Users can print from their mobile device or use email to print.
- **Content Security**
    - **Do not change device configuration**: Current settings are maintained on the device.
    - **Disabled**: Jobs are not tracked for security content.
    - **Enabled**: Jobs are processed and tracked for security content.
- **Printer Client**
    - **Do not change device configuration**: Current settings are maintained on the device.
    - **Remove**: Removes the printer client application from the printer. Held jobs cannot be released on this device from the printer client application.
    - **Install**: If the printer is enabled, install the printer client application on the printer. Held documents can be released on this device using the printer client application.
    - **Enable Scan**
    - **Enable Copy**
- **Usage Tracking (Network Accounting)**
    - **Do not change device configuration**: Current settings are maintained on the device.
    - **Disabled**: No Accounting.
    - **Enabled**: Network Accounting.
- **Accounting Credentials**
    - **Do not change device configuration**: Current settings are maintained on the device.
    - **Disabled**: No Accounting.
    - **Enabled**: Network Accounting.
    - **Enabled**: Standard Accounting.
- **Secure Printing**
    - **Do not change device configuration**: Current settings are maintained on the device.
    - **Disabled**: A Secure Print passcode is not required for job release.

    - **Enabled**: A Secure Print passcode is required for job release.
- **Auto Release All Jobs**
    - **Do not change device configuration**: Current settings are maintained on the device.
    - **Never**: Jobs can be released on this device only through the Printer Client Application, after a user logs in.
    - **Using Access Card or Alternate Login**: Held print jobs are released automatically when a user completes the login sequence with the card or alternate login.
    - **Using Network Appliance**: Held print jobs are released automatically when a user scans a card at a mapped network appliance associated with this printer.
- **Enable Printer(s)**: Select the check box to make the printer available to users.

5. After you modify the features, select the **Enable Printer** check box.
6. To apply the changes to the selected printer, select **Save**.

PRINT WELCOME PAGE

Welcome pages provide a convenient way to on-board new users to the Xerox® Workplace Suite when using the Xerox® Workplace Mobile Print Workflow.

The Welcome Page contains a QR code that mobile app users are able to scan to identify the printer. The Welcome Page should be located in a convenient location near the printer. The Welcome Page also provides a convenient connectivity test between the Mobile Print Server and a printer.

Note: If accounting is enabled on the device, the correct administrative defaults must be configured in the **Company > Polices > Accounting** section.

1. On the **Printers** tab, select the printer.
2. Select **Print Welcome Page** from the **Actions** menu.
3. Configure your Welcome Page settings and select **OK**.
4. A Welcome Page will be sent to that printer.
5. Place the Welcome Page in a convenient location near the printer it was printed on.

REPAIR

If a printer has had maintenance or if the Company Workflow has been modified, settings may have been changed that require the printer to be reinstalled with the Xerox® Workplace Suite Software. If a device, that was previously registered, is no longer operating properly with the software, you can attempt to repair it from within Workplace Suite. The repair process will attempt to reset the printer to the settings needed for proper communication.

1. On the **Printers** tab, select the checkbox for the printer that requires repair.
2. Select **Repair** from the Actions menu.

   A confirmation alert appears.

3. Select **Yes** to proceed.

   If the printer status is Not Registered, select the printer and hover over the printer icon for the error message. To correct the printer registration settings, select the printer and then retype the IP address, Username, and Password.

   Refer to the *Troubleshooting* chapter for more information on device registration problems.

4. If the printer was not able to be repaired, the printer settings will have to be checked directly by accessing the printer from the CentreWare Web Internet Services user interface.

DELETE

Deleting a printer will remove it from the list of printers.

1. On the **Printers** tab, select the checkbox for the printer you wish to delete.
2. Select **Delete** from the Actions menu to remove the selected printer.

   A confirmation message displays.

3. Select **Yes** to delete the printer.

Note: Deleting a printer will remove the printer from the list of printers, but if the printer is being discovered by a Discovery Profile, the printer will be re-added to the list. To permanently remove the printer, the Discovery Profile must be configured to not include the printer when discovery is run. See the *Discovery* section for more information.

Printer Groups

This section explains how to create printer groups.

CREATING A PRINTER GROUP

To create a printer group:

1. From the Printers tab, click the **Printer Groups** subtab.
2. From the Printer Groups subtab, select **Actions > New**.
3. Type the Name and Description.
4. To select how printers are assigned to the Printer Group, click one of the following:
   - **All printers except blocked list**: All printers are in the Printer Group, except devices in the Blocked Printers list.
   - **Specified printers only**: All printers in the Allowed Printers list are included in the same Printer Group.
5. To find printers that do not appear in the Allowed Printers list, use the **Search** feature.
6. To update the list of Blocked Printers, select **Actions > Add** or **Actions > Delete**, then click **Save**.

EDITING A PRINTER GROUP

To edit a printer group:

1. From the Printers tab, click the **Printer Groups** subtab.
2. To assign printers to a printer group, click the **Printer Group** name, then select one of the following:
   - **All printers except blocked list**: All printers are in the Printer Group except devices in the Blocked Printers list.
   - **Specified printers only**: All printers in the Allowed Printers list are included in the same Printer Group.
3. To find printers that do not appear in the Allowed Printers list, use the **Search** feature.
4. To update the list of Blocked Printers, select **Actions > Add** or **Actions > Delete**, then click **Save**.

VIEWING PRINTER GROUPS

To view Printer Groups:

1. Select the **Printers** tab, then select the **Printer Groups** subtab.
2. To view group details for the Printer Access Groups, click **Printer Group**.

Direct Print

DIRECT PRINT OVERVIEW

Direct Print is a Print Management Workflow feature that allows desktop printing directly to a printer. Direct Print provides a Direct Print submission path using either the Workplace Suite Client or a shared windows network queue. Direct Printers can be created on the main server or any connected external print server.

This section describes the features of Direct Printing, and provides instructions for configuring, enabling, and disabling Direct Printing.

Note:

- Any Workplace Suite printer can be configured for a Direct Print queue. Additional Direct Print queues for that printer can be created on external print servers.
- Direct Printing is only available with a Print Management Workflow license.
- To enable Direct Print queues, you must enable the Desktop Print feature on the printer. Direct Printers are enabled and managed on the Printer Grid.
- Direct Print queues are shared Windows Printers monitored by Workplace Suite
- Once the Direct Print Windows Print driver is installed, do not change the outgoing Port.
- Direct Print jobs are tracked by Xerox Workplace Suite, and are included in the Reports page of the Xerox Workplace Suite webpage.

DIRECT PRINT CONFIGURATION OPTIONS

Direct Printer Types

Direct Printing is configurable for the following types of printers:

- **Network Printer**: A network printer is a Windows network shared printer hosted on a print server. End Users must connect to Direct Printer using the Windows Add a Printer interface.
- **Client Printer**: A client printer is designed to be installed by the Workplace Suite Client. They are still defined on a printer server, as the Workplace Client will need to connect to the server in order to pull over and install the correct driver on the user's workstation.

Direct Printer Network Accounting

When Network Accounting is enabled, the following settings are automatically set to enabled in the Xerox GPD:

- Xerox Network Accounting
- Always Prompt
- Mask User ID / Account ID
- Remember Last Codes

Note:

- If Network Accounting Is enabled, when submitting a job to a Direct Print queue, the user is prompted to enter their User ID and Account ID.
- Network Accounting is only available for configurations using the Xerox GPD.
- The Xerox GPD is configured with Network Accounting enabled for the associated Direct Printer queue.
- For Direct Printers, to retrieve the codes associated with Direct Print jobs, enable Xerox Workplace Suite Job Reporting Usage Tracking. This downloads the printer JBA log to the Xerox Workplace Suite server, and adds the required codes to the report.

Direct Print Driver Configuration

Direct Print drivers are configurable using one of the following two options:

- **Auto:** This mode automatically configures Xerox Workplace Suite to use the preinstalled Xerox GPD installed by the Xerox Workplace Suite prerequisites. This mode is recommended for both Xerox and Fuji Xerox branded printers.

  Note:

  - The specific printer model will be programmed on the Xerox GPD based on printer model. If the printer model is not supported by the Xerox GPD, set the GPD to **Basic Mode**, and set the Model to **Other**.
  - The PDL is taken from the printer details and determines which GPD is used.
- **Manual:** This mode enables manual configuration of available advanced finishing options. This mode is recommended for non-Xerox branded printers, and Xerox branded printers where a model-specific driver is required.

  Note:

  - Manual mode allows the printing solution to query the selected server for its current list of print drivers and allows the system administrator to select the required queue.
  - For Manual configurations that do not use the Xerox GPD, to enable Direct Print, first install the v3 type print driver for your printer.
  - After selecting a driver, the service will use the display name of the printer as the direct shared printer name.
  - Third-party drivers are not compatible with Network Accounting. If you select a third-party driver and enable Network Accounting, you will receive an error message.
  - For Manual mode, if the printer is not supported by the Xerox GPD, if you select the Xerox GPD, the Printer Model is not automatically programmed and the driver will stay in Basic Mode.

Direct Print Job Conversion Mode

Direct Print jobs can be converted using the following methods:

- **None:** Print jobs are not parsed and cannot be modified. This mode gives the best performance when printing but does not support other features that require the job to be parsed and modified. For example, Job will not be

processed for Content Security keyword search. Print rules will not modify print attributes like Color and Sides. User Print Quotas will use the Pages per Job Estimation value.

- **Simple:** Print jobs are parsed and modified by the printing solution. Jobs can be modified at time of release if print rules are applied.

Note: This conversion method can result in slower printing performance.

CONFIGURING AND ENABLING A NEW DIRECT PRINT QUEUE

Note:

- Direct Printers are enabled and managed on the Printer Grid.
- For each printer, you can only add one Direct Printer per print server.
- To enable Direct Print queues, you must enable the Desktop Print feature on your printer.
- The Direct Printer queue name is created using the printers Display Name. This is a user configurable field.
- Deleting a Printer that is configured with a Direct Print queue will delete the Windows Direct Print queue when the printer is next synchronized from the client.

Before you begin, perform these steps:

- Add the required printer to your Xerox Workplace Suite environment.
- Verify that Desktop Printing is enabled. To verify, click **Printers > Features**, then ensure that the **Desktop Print** check box is selected.

To configure and enable a new Direct Print queue:

1. Click **Printers > Printers**From the list of available printers, select the check box for the printer you want to configure.

   Note: You can select one or more printers from the list.

2. Click **Actions > Enable Direct Printing**.

   The Enable Direct Printing dialog box displays.

3. Select the required print server, then click **Next**.
4. For Printer Type, select the required option, then click **Next**.
   - **Network Printer**: Select this option if the printer is a shared network device hosted on a print server. For further details, refer to Direct Printer Types.
   - **Client Printer**: Select this option if the printer was installed by the Workplace Suite Client. For further details, refer to Direct Print Configuration Options.
5. To set up the printer with network accounting enabled, select the **Enable Network Accounting** check box.

   Note: This option is only supported for Xerox printers using the Xerox Global Print Driver.

6. For Driver Selection, select the required option, then click **Next**.
   - **Auto**: Select this option to automatically use the Xerox Global Print Driver. For further details, refer to Direct Print Driver Configuration.
   - **Manual**: Select this option to display a list of compatible print drivers on the print server, then elect the required driver from the list. For further details, refer to Direct Print Driver Configuration.
7. For Conversion Mode, select the required option, then click **Next**.
   - **None**: Select this option to disable print job parsing and print attribute modification after job submission. For further details, refer to Direct Print Job Conversion Mode.
   - **Simple**: Select this option to enable print job parsing and print attribute modification after job submission. For further details, refer to Direct Print Job Conversion Mode.
8. Ensure that the settings are correct for your required configuration, then, to create and enable the Direct Print queue, click **Finish**.

DISABLING AN EXISTING DIRECT PRINT QUEUE

Once a Direct Print queue has been created, it can be disabled from the list of added printers.

Note:

- Disabling a Direct Print queue will remove the queue and the associated driver from the Workplace Suite webpage and the Workplace Suite Client, as well as any other locations where the printer was added.
- Disabling a printer that is configured with an enabled Direct Print queue prevents users from printing to the Direct Print queue, but it does not disable the Direct Print queue. The Direct Printing settings are retained when you re-enable the printer.
- If a Direct Print queue is disabled, the configuration is not saved.

To disable a Direct Print queue:

1. Click **Printers > Printers**. From the list of printers, select one or more printers for the Direct Print queues you wish to disable.
2. To disable the Direct Print queue for the selected printers, click **Actions**, then select **Disable Direct Printing**.

   The Disable Direct Printing dialog box appears.
3. Select the server for the Direct Print queues you want to disable, then click **Apply**.

   The associated Direct Print queues are disabled, and the settings are saved automatically.

VIEWING AND MODIFYING SETTINGS FOR AN EXISTING DIRECT PRINT QUEUE

Once a Direct Print queue has been created, it can no longer be edited in Xerox Workplace Suite. To modify the settings for an existing Direct Print queue, disable and then re-enable the queue with updated settings as required. For details, refer to Disabling an Existing Direct Print Queue and Configuring and Enabling a New Direct Print Queue.

To view the configuration for an existing Direct Print queue:

1. Click **Printer > Printers**.
2. From the list of printers, click the name of the printer you want to view.

3. Select the **Direct Print** tab.

   The configuration details for all Direct Print queues associated with the printer are displayed.

ADDING A DIRECT PRINTER TO THE XEROX WORKPLACE SUITE CLIENT

Note: To use the new Direct Print Client feature in Xerox Workplace Suite version 5.3 or greater, the client must be upgraded to the version that is packaged with Xerox Workplace Client 5.3 or greater.

To add a Direct Printer to the Xerox Workplace Suite client:

1. Run the Xerox Workplace Suite Client, then select **Printers & Queues**.
2. Click **Add Printer**.

   The Add Printer dialog box appears.
3. From the list of available Direct Printers, select the required printer, then click **Add**.

   The Direct Printer is added to the Printers/Queues list.

Note:

- If you receive a driver installation error, install the driver manually.
- The only changes that are transferred to the Workplace client driver are the server driver changes that are made in the **Installable Options** section of the Xerox GPD driver. If you update the Windows Printer configuration on the server, the Workplace Client printers are updated according to the Configuration Poll Interval. To view the configuration settings in the Xerox Workplace Suite client, select **Company > Workflows > Desktop Print > Processing Intervals**.

ADDING A NETWORK QUEUE DIRECT PRINTER USING A CLIENT

For adding a network queue Direct Printer, your system administrator can provide one or more shared network print queue names.

Note: For information and instructions on how to install a specific print queue, contact your system administrator.

To add a network queue Direct Printer using the Windows Add a Printer wizard:

1. On your Windows PC, access the Windows Control Panel.
2. Click **Devices and Printers**, then select **Add a Printer**.
3. Click **The printer that I want isn't listed**.
4. Select **Add a Bluetooth, wireless or network discoverable printer**, then click **Next**.
5. 5. Select the required shared printer from the list and enter the name provided by your ystem administrator in the format `\\<server name>\<printqueuename>`.
6. To finish installing the print queue, follow the on-screen instructions.

Note: If you receive a Driver install error, install the driver manually.

Print Queues

This chapter contains:

Incoming Queues and Print Servers

Note: This feature is only available with a Print Management Workflow license.

Print queues for the Workplace Suite server are Microsoft Windows printers. These printers define the drivers used on the Print Management Workflow workstation client machines for the print queues shown in Devices and Printers. On the Workplace Suite server, in Devices and Printers or in Printer Management, create Windows Printers using the Global Print Driver, the Pull Print Driver, and/or specific Device Print Drivers, as appropriate for your environment.

Note: If your environment is mixed between x86 and x64 machines, you must create the Windows printers on the Workplace Suite server using the appropriate driver for the server. Then add the other version of the driver by entering Control Panel and selecting **Printer Properties > Sharing > Additional Drivers**.

The Incoming Queues section displays all Windows printers defined on the Workplace Suite server. Any Windows printer used by the Print Management Workflow workstation clients should be enabled here.

XEROX PRINT DRIVERS

Workplace Suite server uses the Xerox Global Print Driver (GPD), the Xerox® Pull Print Driver (PPD), and Device Drivers.

If all the printers using this print queue are of the same model, use the device specific print driver. For Xerox® devices, you can also use the Global Print Driver configured for that specific device. For non-Xerox devices, use the manufacturer's print driver.

If all printers using this print queue are Xerox Printers that support XCPT (Xerox® Common Print Ticket), use the Xerox® Pull Print driver. ConnectKey devices and most Xerox MFDs support XCPT. The complete list of supported devices is available at www.xerox.com/Ppdrivers.

When using the Xerox Global Print Driver on a print queue that will be used with non-Xerox devices, the driver will need to be configured in Basic Print Mode. Basic Print Mode will limit the features that can be used with these printers. The recommended approach would be to have separate print queues for Xerox and non-Xerox devices, and to use the device specific drivers.

ADMINISTRATOR SETUP FOR PULL PRINT QUEUES

Printers can be local to the Print Management server, or remote (external print server).

- **Local Server** - By default, the installed Print Management server assumes you are going to use the local server for setting up your print queues. This is the simple model and the Admin is not required to set up an external device.
- **Print Servers** - External servers may be used to offload the print job spooling and processing to one or more external devices. Job processing can be computer intensive, so if you have some large environments, the customer may want to offload this work to an external server. To install an external server, run the Workplace Suite server install package, including the Prerequisites on the print server, but don't license the software. On the main Workplace Suite server, add the external print server to the configuration. This will establish the communication path between the Workplace Suite server and the Print Server. When adding Incoming Print Queues to the remote server, follow the same setup guidelines for incoming Queues as the main server which is documented in this section. The external Print Servers incoming Queues will be listed and managed on the main server incoming queues list.

PRINT QUEUE TYPES

There are two types of print queues.

- **Pull Print Network Queue**: A traditional network printing queue, where jobs are sent to an off-box server which could be the Print Management server (local), or the external print server.
- **Pull Print Client Queue**: This queue provides a mode of printing where jobs are held on the personal computer of a user until they are released to a printer. This queue requires the Xerox® Workplace Suite Client.

NETWORK QUEUE SETUP - SERVER

Note: Before adding new Print Queues, it is important to view the latest queue list. To refresh the list of Print Queues, select the relevant Print Server, then select **Action** > **Refresh Queue List**.

1. Set up a local printer on the server using the Xerox XMP v3 Port Monitor.
2. Select an appropriate driver based on printer models, capabilities, manufacturers, and so on.
3. Configure the printer the way you want, for example, model, finisher, and so on.
4. On the Sharing tab, enable client-side rendering (all rendering should be done client-side).
5. On the Sharing tab, make sure 32-bit and 64-bit drivers are both installed if this appropriate for your network.
6. Share the printer.
7. Pick a share name that makes sense and will be understood by users.
8. Enable the queue in the Workplace Suite Admin Tool and ensure the Queue Type is set to **Network**.
9. Select **None** or **Simple** as the Conversion Mode for the queue.

NETWORK QUEUE SETUP - USER

1. The user adds a network printer to their PC.

   For example:

   - \\<server name or IP address>\<Print Queue Name>
   - \\Jean\JeanRemoteOne

PULL PRINT NETWORK QUEUE DETAILED INSTRUCTIONS - SERVER SETUP

Adding a Network Printer (Server Installation)

You can use the following method to add multiple printers. In this example, a single printer is added.

1. Go to the Control Panel and choose **Devices** and **Printers**. Click **Add Printer**.

   The Add Printer dialog displays.

2. Choose **The Printer that I want isn't listed** option.
3. In the Find a printer by other options screen, choose **Add a printer using a TCP/IP address or hostname**, and then click **Next**.

4. In the Type a printer hostname or IP address screen, enter the multifunction printer IP address or hostname, and then click **Next**.
5. In the Type a printer name screen, enter an easy-to-remember printer name, and then click **Next**.
6. In the Printer Sharing screen, choose **Share this printer so that others on your network can find and use it** option.
7. Enter an easy-to-remember Share name and location (Comment is optional), and then click **Next**
8. Click **Finish** to complete the installation.

Configuring a Network Printer (Server Installation)

1. Go to the Control Panel and choose **Devices** and **Printers**.
2. Right-click the printer listed in the Printers list.
3. Choose **Printer Properties** from the selection menu.
4. On the Printer Properties window, go to the **Ports** tab. Select the server using the **Xerox XMP v3 Port Monitor**.
5. Select an appropriate driver based on printer models, capabilities, manufacturers, and so on.
6. Configure the printer, e.g., Model, Finisher, and so on.
7. Configure the printer for client-side rendering.
8. Install both 32-bit and 64-bit drivers.
   a. On the Printer Properties window, go to the Sharing tab and click **Additional Drivers**.
   b. Make sure both Processor boxes, x64 and x86, are checked and click **OK**.
   c. Click **Browse** and locate the directory where **ntprint_inf.inf** file is located.
   The default Xerox Print Prerequisites location is `C:\Program Files(x86 for 32-bit)\Xerox\Xerox Print Prerequisites\InstallerSupport\X-GPD\Windows <Printer Language>\<32-bit or 64-bit>`.
   d. Click **OK** to return to the Printer Properties dialog window.
9. Pick a Share name that makes sense and is understandable by the users, and then click **OK** to share the printer.
10. Enable the queue on the **Workplace Suite Admin Tool** and ensure that the Queue Type is set to **Pull Print Network Queue**.
11. Select the Conversion Mode for the queue: **None** or **Simple**.
    - **None** – Print jobs will not be parsed and cannot be modified. This mode gives the best printing performance, but does not support other features that require the job to be parsed and modified. For example, a job will not be processed for Content Security keyword search. Print rules will not modify print attributes such as Color and Sides. User Print Quotas will use the Pages per Job Estimation value.
    - **Simple** – The user can modify quantity, color, and simplex/duplex. This selection is only supported by Xerox printers.
12. Add the Incoming Queue to a Pull Group.

WORKPLACE SUITE CLIENT QUEUE - SERVER SETUP

1. The system admin should set up a local printer on the server using the standard TCP/IP port monitor.

2. Select an appropriate drive based on printer models, capabilities, manufacturers, and so on.
3. Configure the printer the way you want, for example, model, finisher, and so on.
4. Install the 32-bit and 64-bit drivers.
5. Share the printer.
6. Pick a share name that makes sense and will be understood by users.
7. Enable the queue in the Workplace Suite Admin Tool and ensure the Queue Type is set to **Client**.
8. Select **None** or **Simple** as the Conversion Mode for the queue.
   - **None** - The user cannot modify and job attributes. This setting is typically used for non-Xerox drivers.
   - **Simple** - The user can modify quantity, color, and plex. This setting is only supported by Xerox printers.

WORKPLACE SUITE CLIENT - USER SETUP

1. The user places the Xerox® Workplace Suite Client installer and config file on their PC.
2. The user runs the Xerox® Workplace Suite Client installer.

   Note: The config file must be in the same directory.

3. The Xerox® Workplace Suite Client communicates with the Workplace Suite server and installs the configured Client print queues.

WORKPLACE SUITE CLIENT DETAILED INSTRUCTIONS - SERVER SETUP

Note: Print Management Workflow supports multiple printers.

Workplace Suite Client Queue Detailed Instructions - Server Setup

You can use the following method to add multiple printers. In this example, a single printer is added.

1. Go to the Control Panel and choose **Devices** and **Printers**. Click **Add Printer**.

   The Add Printer dialog displays.

2. Choose **The Printer that I want isn't listed** option.
3. In the Find a printer by other options screen, choose **Add a printer using a TCP/IP address or hostname**, and then click **Next**.
4. In the Type a printer hostname or IP address screen, enter the multifunction printer IP address or hostname, and then click **Next**.
5. In the Type a printer name screen, enter an easy-to-remember printer name, and then click **Next**.
6. In the Printer Sharing screen, choose **Share this printer so that others on your network can find and use it** option.
7. Enter an easy-to-remember Share name and location (Comment is optional), and then click **Next**.
8. Click **Finish** to complete the installation.

Workplace Suite Client Detailed Instructions - User Setup

1. Go to the Control Panel and choose **Devices** and **Printers**.
2. Right-click the printer listed in the Printers list.
3. Choose **Printer Properties** from the selection menu.
4. On the Printer Properties window, go to the **Ports** tab.
   The System Administrator should set up a local printer on the server using either the standard TCP/IP port monitor, or a local port monitor.
5. Select an appropriate driver based on printer models, capabilities, manufacturers, and so on.
6. Configure the printer, e.g., Model, Finisher, and so on.
7. Install both 32-bit and 64-bit drivers.
   a. On the Printer Properties window, go to the Sharing tab and click **Additional Drivers**.
   b. Make sure both Processor boxes, x64 and x86, are checked and click **OK**.
   c. Click **Browse** and locate the directory where **ntprint_inf.inf** file is located.
   The default Xerox Print Prerequisites location is `C:\Program Files(x86 for 32-bit)\Xerox\Xerox Print Prerequisites\InstallerSupport\X-GPD\Windows <Printer Language>\<32-bit or 64-bit>`.
   d. Click **OK** to return to the Printer Properties dialog window.
8. Pick a Share name that makes sense and is understandable by the users, and then click **OK** to share the printer.
9. Enable the queue on the **Print Management Admin Tool** and ensure that the Queue Type is set to **Client**.
10. Select the Conversion Mode for the queue: **None** or **Simple**.
    - **None** – The user cannot modify any job attributes. This selection is typically used for non-Xerox drivers.
    - **Simple** – The user can modify quantity, color, and simplex/duplex. This selection is only supported by Xerox printers.

ENABLE AN INCOMING QUEUE

1. On the **Print Queues** tab, select **Incoming Queues**.
2. From the list, select the name of the print queue you want to enable.
3. On the Edit Print Queue screen Details tab, select the **Enable** checkbox.
4. Click **Save**.

DISABLE AN INCOMING QUEUE

1. On the **Print Queues** tab, select **Incoming Queues**.
2. From the list, select the name of the print queue you want to disable.
3. In the Details section, remove the check mark from the **Enable** checkbox.
4. Click **Save**.

ADD AN INCOMING PRINT QUEUE TO A PULL GROUP

1. On the **Print Queues** tab, select the **Incoming Queues** tab.
2. Select the name of the print queue that you want to add to a printer group.
3. On the Edit Print Queue window, select the Pull Groups tab and move one or more Pull Groups from the Unassociated side to the Associated side.

EDITING THE PRINTER AND ASSOCIATED PULL GROUPS

You can change which pull groups a printer is associated with by adding a printer to a pull group or removing it from a pull group.

1. On the **Printers** tab, select the name of the printer whose pull group association you want to edit.
2. On the Edit Printer screen, select the **Pull Groups** tab.

   The lists of unassociated pull groups and associated pull groups display.
3. To associate the printer with a pull group, select a pull group from the Unassociated Groups list and select the right-facing arrow.

   The pull group moves to the Associated Groups list.
4. To remove the printer from a pull group, select a printer from the Associated Groups list and select the left-facing arrow.

   The pull group moves to the Unassociated Groups list.
5. Select **Save**.

Outgoing Queues

Note:

- This feature is only available with a Mobile Print Workflow license.
- Only Mobile Print Workflow jobs are forwarded to Outgoing Queues. This includes jobs received from Mobile Print Desktop Client.

ADDING A NEW PRINT QUEUE

1. Select **Print Queues > Outgoing Queues**, then select **New** from the Actions menu.

   The Add New Print Queue screen displays.
2. Enter the **Details**:
   - Display Name
   - Manufacturer (Xerox, Other, Fuji Xerox)
   - Model
   - Printer Language (PCL 6 or PostScript®)
   - LPD Server
   - LPR/LPD Port
   - LPR Queue Name
   - Default checkbox - If enabled, any content sent to the Mobile Print Workflow incoming email address will be automatically forwarded to the default print queue as a print job. There can only be one default print queue (the last print queue selected is the default).
3. Enter the **Device Capabilities**:
   - Color Mode (Color or Black and White)
   - Stapling (No staple or 1 Staple)
   - 2-Sided Printing (1-Sided Print or 2-Sided Print)
   - Available Paper Trays (Letter, A3, A4 or Ledger/Tabloid)
4. Click **Save**, then click **Next**.
5. Select the **Location** tab and enter the **Location Details**:
   - Actions: Add Site or Remove Site
6. Select the **Accounting** tab.

7. Select an **Accounting Mode**:
   Selecting Network Accounting or Standard Accounting requires users to enter accounting information when printing to this print queue. The information that they enter is passed through the print queue to the printer's Network or Standard accounting setup. These credentials are not used for authentication at the print queue itself. For more information on sending print queue authentication credentials, see How to Choose User and Domain Information to be Sent to Third-Party Accounting Queues .
   - No Accounting
   - Network Accounting
   - Standard Accounting

   Note: For more information, see the *Accounting* section.
8. Click **Save**.

OUTGOING QUEUES: DETAILS

In addition to the information in the table on the Print Queues tab, you can view more details, such as error codes and their descriptions, about an individual device. For example, you can check the device details for an explanation of why a print queue did not register successfully.

1. On the**Print Queues > Outgoing Queues**, select the print queue you wish to edit.

   The **Details** window opens.

   You can edit the following **Device Information**:
   - Display Name
   - Manufacturer
   - Model
   - Printer Language (PCL 6 or PostScript®)
   - LPD Server
   - LPR/LPD Port
   - LPR Queue Name
   - Default checkbox - If enabled, any content sent to the Mobile Print Workflow incoming email address (or via AirPrint) will be automatically forwarded to the default print queue as a print job. There can only be one default print queue (the last print queue selected is the default).

   You can edit the following **Device Capabilities**:
   - Color Mode
   - Stapling
   - 2-Sided Printing
   - Available Paper Trays
2. Select the **Accounting** tab.

3. Select an **Accounting Mode**:

   Selecting Network Accounting or Standard Accounting requires users to enter accounting information when printing to this print queue. The information that they enter is passed through the print queue to the printer's Network or Standard accounting setup. These credentials are not used for authentication at the print queue itself. For more information on sending print queue authentication credentials, see How to Choose User and Domain Information to be Sent to Third-Party Accounting Queues.

   - No Accounting
   - Network Accounting
   - Standard Accounting

4. Select the **Location** tab and enter the **Location Details**:
   - Add Site
5. Review the information and select **Save**.

HOW TO CHOOSE USER AND DOMAIN INFORMATION TO BE SENT TO THIRD-PARTY ACCOUNTING QUEUES

Some accounting systems require that the user domain be provided when submitting jobs to print queues. If your accounting system requires this, set the accounting options as follows:

1. Select **Company > Settings > Print Defaults**.
2. Under **Job Owner**, choose the correct domain information to be included.

   Note: When using a pull printing workflow with a third-party print queue, the job owner must match the username in the third-party print queue solution. If the usernames don't match the user will not see their jobs in the pull printing client.

3. Select **Save**.

Pull Groups

This chapter contains:

Note: This feature is only available with a Print Management Workflow license.

This chapter contains the information to add, edit, and delete Pull Groups.

How to Associate Printers and Print Queues Using Pull Groups

In a Print Management Workflow environment, print jobs are printed by the users to the Print Management Workflow print queues just as the user might print to any other Windows printer. If the Print Management Workflow environment is configured with client queues (workstations that have the Workplace Suite Client installed), then the job is held on the workstation client machine until the user logs in at the MFP to release the job for printing. The Workplace Suite Admin will create device Pull Groups that link the Printers and Print Queues in logical groupings based on print drivers that are compatible with the printers, features that are available on the printers, and physical locations of the printers.

Pull Groups are typically defined to allow the user the flexibility to print out their document at any nearby printer. Therefore, if a printer is down or is busy, the user can go to another nearby printer. All printers placed in the same group must use a compatible print driver and that driver must be the one defined for any print queue added to that Pull Group. If you place print queues using different print drivers in the same group, you must be sure that all printers in that group support all of those print drivers.

Guidelines for creating pull groups:

Do

- Place printers of the same type/model in a group that is geographically nearby.
- Use a print driver that is designed to work with all printers in that group.
- If printers from different manufacturers are to be in the same Pull Group, use the Xerox Global Print Driver in Basic Print Mode.

Don't

- Place a printer into the same Pull Group that contains a print queue using an incompatible driver.
- Place printers with different printing and/or finishing capabilities together if you think users will be unable to identify which devices can meet the printing and/or finishing requirements for their job. (For example, if the user prints a color job and a B&W printer is in the group, the user may release the job to a device that cannot print color.)

Create a New Pull Group

1. On the Pull Groups tab, select **Create New Group**.
2. Enter a Name and a Description for the group and select **Save**.

Editing the Printer and Associated Pull Groups

You can change which pull groups a printer is associated with by adding a printer to a pull group or removing it from a pull group.

1. On the **Printers** tab, select the name of the printer whose pull group association you want to edit.
2. On the Edit Printer screen, select the **Pull Groups** tab.

   The lists of unassociated pull groups and associated pull groups display.
3. To associate the printer with a pull group, select a pull group from the Unassociated Groups list and select the right-facing arrow.

   The pull group moves to the Associated Groups list.
4. To remove the printer from a pull group, select a printer from the Associated Groups list and select the left-facing arrow.

   The pull group moves to the Unassociated Groups list.
5. Select **Save**.

Add a Print Queue to a Pull Group

1. On the **Printer Groups** tab, select the pull group you want to add the print queue to.
2. Select **Print Queues**.
3. From the Actions menu, select **Add**.
4. From the **Select Print Queues** window, select the print queue to add to the pull group and select **Save**.

Remove a Print Queue from a Pull Group

1. On the **Printer Groups** tab, select the pull group you want to remove the print queue from.
2. Select **Print Queues**.
3. Select the print queue to be removed from the pull group.
4. From the **Actions** menu, select **Remove** and confirm when prompted.

Add a Printer to a Pull Group

1. On the **Printer Groups** tab, select the pull group you want to add the printer to.
2. Select **Printers**.
3. From the **Actions** menu, select **Add**.
4. From the **Select Printers** window, select the printer to add to the pull group and select **Save**.

Remove a Printer from a Pull Group

1. On the **Printer Groups** tab, select the pull group you want to remove the printer from.
2. Select **Printers**.
3. Select the printer to be removed from the pull group.
4. From the **Actions** menu, select **Remove** and confirm when prompted.

Discovery

This chapter contains:

This chapter contains the information for setup and configuration of automated printer Discovery.

Discovery Profiles

Discovery profiles are used to periodically scan the network to import printers into the system. Printers created with Discovery are not automatically enabled and the printer client is not registered on the printer. Default Workflows and Features can be assigned to the newly discovered printers. To enable printer(s), refer to Printers Tab. To understand the Workflows refer the Printer section in this manual.

Note: If a device is defined in Printers, it has an IP address. If an IP address changes, running discovery detects any changes to the IP address. It will be done usually on a once-a-day basis, so it will take a little while but it will fix itself if discovery is turned on. Recommended to be used in an environment where printers are using DHCP addressing in order to refresh printers when IP leases expire. Each Discovery profile will be able to be run once a day. For more frequent updates of the addressing, multiple profiles can be created.

The number of profiles indicates the total number of discovered profiles.

The **Actions** menu provides a list of tasks that can be performed.

The **Page** indicator shows which page is being viewed of the total number of pages.

The **Items Per Page** indicator lets you set the number of profiles that are displayed per page.

The **Sort by** menu lets you sort the list by:

- Name A-Z
- Name Z-A
- Last Communication Date ASC
- Last Communication Date DESC

The **Filter By** menu lets you filter the list by:

- Added in last 24 hours
- Last 14 days
- Last month
- Added in last 3 months

The **Search** field lets you quickly find specific profiles in long lists.

Setting Up a Discovery Schedule

The administrator can schedule when Discovery will run.

1. Select the **Discovery** tab.
2. Select **New** from the **Actions** menu to create a new discovery profile.
   Name
3. Under **Details**:
   - Enter a Name
   - Select a Printer Language

   Site
4. Select **Next** and select one of the following:
   - **Existing Site**: Select the check-box next to an existing site.
   - **New Site**: Enter the Details and Location.

   Discovery
5. Select **Next** and enter the following optional information, otherwise select **Next** 3 times to go to the next step.
   a. From the **Discovery Settings** tab, select **New** from the **Actions** menu and enter the IP Address or range in which it will search for new printers. Complete the information, Display Name, Discovery Scan Type, IP Address AND optional Authentication (Printer Login User Name and Printer Login Password), select **Save** and then select **Next**.
   b. From the **SNMP Settings** tab, Complete the information, SNMP v1/v2, Set Community Name, Get Community Name, SNMP v3, and select **Next**.
   c. From the **Exclusions** tab, select **New** from the **Actions** menu and enter the IP address or range in which it will exclude when searching for new devices. Complete the information, Display Name, Discovery Scan Type, and IP Addres and select **Save** and then select **Next**.

   Features
6. Please refer to Workflows for detailed description of the features. Complete the information and select **Next**.
   - Workflows
   - Accounting Credentials
   - Secure Printing
   - Auto Release All Jobs

   Schedule
7. Select the appropriate check-box and select **Next**.
   - **Disabled**
   - **Every Day**
   - **On** a day of the week at an approximate time.

   Verify
8. Verify the information, then select **Finish** to create the new discovery profile.

Entering a Range of Printers for my Discovery Profiles

1. Select **Discovery** and select a printer to edit.
2. Select **Discovery Settings**
3. From the **Actions** menu, select **New**.
4. From the **Discovery Scan Type** menu, select **IP Address Range**.
5. Enter a **Start IP Address** and **End IP Address**.

   You can enter individual or a range of IP addresses to include more printers. Discovery of large ranges is slower. If the range includes many IP addresses that are not printers to be used, it may create unnecessary network traffic because the solution attempts to communicate with each IP address. You can run this IP Discovery scan multiple times each day depending on the schedule.
6. If necessary, enter the printer credentials for and select **Save**.
   - Printer Login User Name
   - Printer Login Password
7. To set the printer defaults, select **Features > Workflows**. For a detailed description of the features, refer to Printers.

Discovery Profiles are Associated With a Site

When a discovery profile is created, it is associated with a site. This site is used as a default printer site when a printer is discovered for the first time.

Note: A Discovery Profile's site cannot be changed.

Manual Discovery

To initiate a manual printer discovery:

1. Select the **Discovery** tab.
2. Select the check-box for the Discovery profile.
3. From the **Actions** menu, select **Run Discovery Now**.

How To Change the Site Associated With a Discovery Profile

A Discovery Profile's site cannot be changed.

Users

This chapter contains:

User Administration

Users are added to the database through LDAP synchronization, manually by the system administrator, imported via CSV files, or on-boarded by each user through LDAP look-up as they begin to use the system. If LDAP synchronization is used, additions, deletions, and modifications to the LDAP directory can be done on a regularly scheduled basis to keep the Workplace Suite database up to date.

Users

The **Users** tab is where you can manage the list of users who can access Workplace Suite.

The **Actions** menu provides a list of tasks:

- New
- Reset Confirmation Number
- Clear Secondary PIN (This feature is only available with a Print Management Workflow license.)
- Analyze Print Quota
- Import From File
- Export This Page
- Export All Pages
- Delete

The **Page** indicator shows which page is being viewed of the total number of pages.

The **Items per page** indicator lets you set the number of users displayed per page.

The **Filter By** menu allows you to filter the list by:

Time:

- Added in last 24 hours
- Last 14 days
- Last 30 days
- Added in last 3 months

User Roles:

- General User
- Power User
- System Administrator

The **Search** field allows you to enter any of the following user information to find the specific users from the **Users** list:

- Email Address
- User Name
- Alternate Access Card User
- First Name
- Last Name
- Department
- Primary PINs and Access Card Numbers

ADDING A NEW USER

To manually add a new user:

1. Select the **Users** tab.
2. Select **Actions > New**.
3. Enter the required information on the following section:
   - Details
   - User Quota
   - Primary PINs and Access Card Numbers
   - Guest User
   - Roles
   - Account Settings
4. Once the required User Information is entered, Click **Save**.

Note: It is mandatory to enter at least one User role to add the User in the Workplace Suite, for more information on User Role refer to User Roles section.

User Roles

A User can be assigned to the following roles:

1. System Administrator
2. Power User
3. General User

System Administrator: When the User is assigned as a **System Administrator**, they will have full access to the Workplace Suite features.

Power User: When the User is assigned as a **Power User**, they will have partial access to the Workplace Suite features.

Note: Power Users have access to all the tabs except the **Company** tab.

General User: When the User is assigned as the **General User**, they will have limited access to the Workplace Suite features.

For more details on the General User capabilities, refer to Xerox® Workplace Suite User Portal section.

User Role Access to Workplace Suite Features

The following table shows the User Roles and their access to Workplace Suite features:

FEATURES	SYSTEM ADMINISTRATOR	POWER USER	GENERAL USER
Company/Settings	Yes	No	No
Jobs	Yes	Yes	No

FEATURES	SYSTEM ADMINISTRATOR	POWER USER	GENERAL USER
Printers	Yes	Yes	No
Print Queues	Yes	Yes	No
Pull Groups	Yes	Yes	No
Discovery	Yes	Yes	No
Users	Yes	Yes	No
Reports	Yes	Yes	No
Delegation	Yes	Yes	Yes

Guidelines:

The following are the features of a Power User:

- Power User cannot access the **Company** and **Settings** tab.
- The landing page for a Power User will be the **Jobs** tab.
- Power User cannot assign or remove any Roles for a User.
- Power User functions as a General User when using Mobile App, Workplace App, and Chrome extension.
- Power User cannot view the documents submitted by a User on the **Jobs** tab.
- Power User cannot add, edit, or delete an existing Administrator or Power User.
- Power User can add and edit General Users.

ASSIGNING A USER ROLE TO THE USERS

The following User Roles are available in Unassigned Roles field to assign to a User:

1. **System Administrator**
2. **Power User**
3. **General User**

To assign a user with any one of the above Roles, do the following:

1. Open the Users window, click **Users** tab.
2. Click on the User's email for which you want to assign with **System Administrator**, **Power User**, or **General User** Role.
3. From the Unassigned Roles field, select the required Roles.
4. Click the **right arrow** button to move the selected User Role to the Assigned Roles field.
5. Click **Save**.

   The User is assigned to the required Roles.

ASSIGNING USERS TO A DEPARTMENT

1. Click the **Users** tab.
2. To edit user data fields, click the associated user Email address.
3. Add a value to the Department field.
   - As an alternate method of assigning a user department, you can use the Users CSV Import file, which has the Department field.
   - It is common for LDAP mapping to populate automatically the Department field.

USER HAS NO EMAIL ADDRESS SETTING

To create a user without an email address, create the user manually using the **User has no email address** setting. If you enable the **User has no email address** setting, ensure that the user performs the administrator functions. Ensure that this user is not a general end user who prints.

Note: The **User has no email address** setting is not supported when users are imported from LDAP.

To add a user that does not have email address, do the following:

1. Select the **Users** tab.
2. From the Actions menu, click **New**.
3. Select the check box for **User has no email address**.

   The User Name field is mandatory in these cases.
4. In the Email Address text field, type the required user name.
5. Enter information in the other fields, as required.
6. To save the setting, click **Save**.

GUEST USER ACCESS USING EMAIL

For more information, refer to Guest Onboarding Using Email.

TEMPORARY GUEST ACCESS

The administrator can now create temporary guest user accounts that expire after 1, 3, 7, 14, 30, 60, 90 or 180 days. This user is enabled for both confirmation number and LDAP logins. When the user is created, a confirmation code is created and emailed to the user. This confirmation code is also used as the password for LDAP login.

Temporary Guest Access Enable

This is an important feature when LDAP is enabled and you want to create a guest user.

1. From the Administration web page, click the **Users** tab.
2. Select **Action > New** .
3. Enter the user's Email Address.

4. Enter the User Name. It is recommended that you use the user's email address. This field is required if LDAP authentication is on.
5. The First Name and Last Name are optional
6. Select the **Guest User** check box.
7. An **Expiration Time (days)** will appear, select an expiration time for how long you want the user to be active.

   The password is always the confirmation number emailed to the user. When the user expires, the account is removed from the system automatically.
8. Select **Save**.

ASSIGNING PRINT QUOTA FOR INDIVIDUAL USERS

You can define the Print Quota rules for specific User that override any general Print Quota rules that apply to all users or any groups of users that contain the specific User.

1. Select the **Users** tab, click on the required **User**.
2. On the **User Details > Print Quota**, select **Override Print Quota Rules**.
3. For Pages, select **Unlimited** for the User to print Unlimited pages or select **Limited** and enter the required Print Quota value.
4. Click **Save**.

ADDING PRIMARY PINS AND ACCESS CARD NUMBERS

For Guidelines, refer to Authentication>**Card Authentication Usage Guidelines**.

1. Select the **Users** tab, click on the required **User**.
2. On the Primary PINs and Access Card Numbers , New Value field enter the applicable values and Click on the **right arrow** button.
3. Click **Save**.

RESETTING CONFIRMATION NUMBER

To reset a Users existing Confirmation Number:

1. Select the **Users** tab.
2. Select a User (or Users) from the list.
3. Select **Actions > Reset Confirmation Number**.
4. Select **Yes**.
5. After **Successfully reset user(s) confirmation number** appears, select **Close**.

   After completing the above steps, the Workplace Suite server will generate new confirmation number(s) and will email them to the user(s).

Note: The User can also reset the Confirmation Number by selecting **Forgot Confirmation Number** at User Portal Login Page, for more information refer to Forgot Confirmation Number.

CLEARING A SECONDARY PIN

Note: Feature enablement is required before an administrator can clear the Secondary PIN for a user. Refer to the Secondary PIN topic in this guide.

To clear a Secondary PIN, follow this procedure:

1. Click the **Users** tab.
2. From the list, click a user name.
3. Click **Actions > Clear Secondary PIN**.
4. Click **Yes**.
5. After you clear the Secondary PIN, click **Close**.

   The next time that the specified users log in to the printer, the users are required to create a new Secondary PIN.

GUIDELINES TO IMPORT A LIST OF USERS FROM A .CSV FILE

When you import from a .csv file, the following information applies:

- When you use the CSV method to import the data, the .csv data override the existing data.
- Row one is the Index row and is mandatory, and remains unchanged.
- Row two is the Description row and is mandatory, and remains unchanged.
- Columns can be in any order as long as the appropriate index is set.
- When you import, to add or change the data on that row, you edit the Change Column Index # 999 number from a 0 to a 1.
- Change Column Index #: 999, where 0=no change 1=Change.
- When you export the .csv file, the change column defaults to 0. If you do not change it to a 1, then any rows that are updated are not processed.
- Primary PIN: A card data string or a personal identification number that the system administrator assigns to each user. When you enable the **Allow Multiple Primary PINs or Access Cards** feature, to import multiple pins, separate each PIN with a comma.

The key required field or column is Users: Email Address and Username.

Note: If this field does not exist, the record is not created or updated.

IMPORTING A LIST OF USERS FROM A .CSV FILE

The Users area lets you upload a list of users in a batch from a CSV (Comma-Separated Value) file. Download the CSV file, then add the list of users.

1. Select the **Users** tab.
2. Select **Actions > Import From File…**.

   The Import Users window opens.

3. Select **Download Example**, then choose where you want to save the template file.
   a. You can edit the template file with any text editor, such as Notepad. Note the location of the file in case you want to edit it in the future.
   b. You can use Microsoft Excel to edit the file.
      - From Excel, select the **Office Button**, then select **Open**.
      - From the All Excel Files menu, select **All Files**.
      - Locate and open the template file.
      - When the Text Import Wizard appears, select **Delimited** and specify a comma as the delimiter.
      - When you finish editing the file, ensure that you select **Save as Type** and select **CSV (Comma delimited)(*.csv)**.
4. Select **Choose File**.
5. Locate your edited file, then select **Open**.
6. Select **Next**.

   The file is read and any errors are displayed.
7. Select **Import**.

   The users are imported.

EXPORTING A LIST OF USERS

You can export the entire user list to a CSV file.

1. Select **Users > Actions > Export All Pages**.

   Note: To export the current page from the users list, select **Export This Page** from the **Actions** menu. A file named User_CurrentPage.csv is saved.

   A file named User_AllPages.csv is saved.
2. Locate the download location and open the file.

   The exported list of users displays.

Note: For best results when using .csv export, ensure that your browser language is set to the same language as the server on which Workplace Suite is installed on.

DELETING USERS

1. On the **Users** tab, select the checkbox for the user you want to delete.
2. Select **Actions > Delete**.

   A deletion confirmation alert appears.
3. Select **Yes** to confirm.

DETECTING THE END-USER LANGUAGE AUTOMATICALLY

The Mobile Print Workflow can detect the end user language, so email responses are in the correct end user language. The default language is utilized for the end user email responses, like Confirmation Email, Job Status Email etc.

To define the default language, Workplace Suite can leverage the device language set for EIP and mobile apps as the user language. If the user does not have a language set, on the first login through mobile apps or EIP, the system will use the device language to set the base user language going forward. This language is only set once per user.

How the end user's default language is set:

- The first login through mobile apps or Printer Client Application, the system will use the device language to set the base user language.
- The system sets the user's default language from email headers. If this language is available, Mobile Printing uses it to set the user's default language and first email response.
- The administrator can view the user's default language when viewing the user's details on the administrative web page.

The end user can change their default email language by sending an email to the server. When a confirmation email is sent, they select the Change Email Language link at the bottom of the email.

User Groups

The Xerox® Workplace Suite software provides three ways to assign users to groups. To associate the users with a group, you can select only one User Association Type.

- **All Users Except Blocked List**: To create a group of all users with print permissions, click **Save**. Users who are assigned to the Blocked List have no printing permissions.
- **Manually Add Users**: To add users to a group manually, select **Actions > New**. Select users from the list or use the **Search** feature to find users, then add them to the group. Click **Save**.
- **LDAP Groups**: To create user groups from existing LDAP user groups, select this option.

Note: An LDAP Connection is required to use LDAP groups. To configure an LDAP Connection, select **Company > Settings > LDAP Connections**. Click **Advanced**, then verify the credentials for the LDAP group. The IMPORT setting is not required.

CREATING A USER GROUP

To create a User Group:

1. Select the **Users** tab, then select **Actions > New**.
2. Type a Name and a brief Description of the new User Group, then select **Save > Next**.
3. Select a User Association Type. Refer to the User Association Type descriptions.
   - Allow All Users Except Blocked List
   - Manually Defined Users
   - LDAP Groups
4. After you assign users to the new User Group, click **Save**.
5. From the Users tab, click **User Groups**.

   The new User Group appears.

Reports

This chapter contains:

Dashboard

Note: Before you can use the Dashboard, install, then enable the Job Reporting add-on. For instructions on installing the add-on, refer to the *Xerox® Workplace Suite Installation Guide*.

The Xerox® Workplace Suite Dashboard provides predefined summary information for customers who use the Reporting capability of Workplace Suite. To update the Dashboard information, it is required to run the Job Reporting task on a regular schedule. For more information, refer to the Job Reporting section in Settings: Job Reporting.

The Dashboard section of the Reports tab provides the following reports:

- Job Summary
- Cost Savings
- Most Used Printers
- Least Used Printers
- Top Users
- Top Departments
- Daily Summary
- Hourly Summary

The Dashboard menu includes the following options:

- Dashboard Report: This menu allows users to select different dashboard reports.
- Time Period: This menu allows users to select the time period for the data reported. Options include Monthly, Quarterly, and Yearly.
- Job Type: This menu allows users to select the source of the job data.
  - Workplace Suite Print and Copy Jobs: This option displays data on the Dashboard for Workplace Suite print and copy jobs.
  - All Print and Copy Jobs: This option shows data from printers that have the Workplace Suite Usage Tracking (Network Accounting) feature enabled. The report shows data from Workplace Suite jobs. The job data includes copies, received faxes, or any page marked by the printer.
  - Print Jobs: This option displays data for all print jobs. Print jobs include delayed print jobs, proof print jobs, Secure Print jobs, reports, scan-to-print jobs, and received faxes, embedded-faxes, and Internet faxes.
  - Copy Jobs: This option displays data for Workplace Suite jobs and copy jobs done at the printer using the Copy function.
  - Scan Jobs: This option displays the data for Workplace Suite Scans and scan jobs done at the printer using the Scan-to function, scan-to-email jobs, embedded-fax-send jobs, fax-send jobs, internet-fax jobs, scan-to-fax jobs, and scan-to-ifax jobs.
- Actions: This menu has three options:

- Refresh: This option allows you to refresh the page.
- PDF Export: This option allows you to export the Dashboard reports in PDF format.
- Modify Cost: This option allows you to configure the cost parameters of a printed page for Dashboard reports.

The following are the views in the Dashboard summary:

- Paging view: This toggle button allows you to view the different pages using the navigation and arrow buttons.
- List view: This toggle button allows you to view the output on one page. You can scroll to view all the data.

MODIFY COST

To configure the cost of a printed page, use the Modify Cost feature. Modify Cost is used in the Reporting Dashboard to give an approximated cost or savings for certain displayed items based on the selected dashboard view. You can set the following Cost parameters individually:

Note: Modify Cost allows you to enter values up to four decimal places.

- Currency Symbol: Select the currency symbol that will be displayed on the dashboard screen for the Cost column. This can be set to a blank value. The symbols of the country currencies are Dollar, Euro, British Pounds, and Japanese Yen.
- Sheet Cost:
  - Hardware Cost: A fixed cost applied to each printed page that maps to machine expenses, such as customer replaceable units, hardware cost, and maintenance cost.
  - Paper Cost: The cost of a single piece of paper. This cost should be an average if different page sizes are used.
- Marking Cost:
  - Black and White: This is the average toner cost per black and white image.
  - Color: This is the average toner cost per color image.
- Scanning Cost:
  - Black and White: This is the average toner cost per black and white image.
  - Color: This is the average toner cost per color image.
- Estimated Default Cost: The estimated costs are for a full printing job, not printed sheets.

Note: Cost cannot be determined for jobs printed to a Queue, which has been configured to use a Conversion Mode of None. To make the cost estimation more accurate, a default cost for an average job can be configured and will be used if the job details can not be obtained for any given job.

REFRESHING THE DASHBOARD REPORTS

To ensure that the most recent job information appears in the Dashboard and Summary sections, refresh the dashboards regularly. To refresh the dashboard reports, do the following:

1. Click **Company > Settings > Job Reporting**.
2. Click **Run Now**.

EXPORTING REPORTS TO PDF

To export Dashboard reports in PDF format, do the following:

1. Click **Reports**.
2. Click **Dashboard**.
3. From the Actions menu, select **PDF Export**.

The default format of the Dashboard file name is `DashboardNameDashboard_YYYYMMDDHHMM.PDF`.

The cover page of an exported PDF report shows the Name, Date, Job type, and Description of the report. Each page has a heading and a page number. The PDF file shows details of the dashboard report and followed by applicable graphs.

SUMMARY OF DASHBOARD REPORTS

Note: The Dashboard reports on jobs only from the date that the Xerox® Print Management and Mobility Suite 4.0.2 is installed.

- Job Summary: This Dashboard report provides the printed sheet count, cost calculation, and graphs for the specified period.
  - Estimated Job Count: The Estimated Job Count increments by one for jobs that meet both of the following criteria:
    - Jobs that cannot be parsed because the Incoming Queues for the Workplace Suite print queues are configured with a Conversion Mode of None.
    - Jobs that the Usage Tracking (Network Accounting) feature does not track.
- Cost Savings: This Dashboard report calculates the estimated cost savings on jobs not printed.
  - This report applies to Workplace Suite jobs. The report does not include jobs submitted outside of this solution, such as copies, scans, emails, and faxes.
  - This table shows the cost saved for jobs that a user submitted for printing but that were not released or that were deleted before printing.
  - When jobs are deleted or expired, and when the system cannot determine the page count, the report shows estimated cost savings.
- Most Used Printers: This Dashboard report lists the top 10 printers that are used most, based on the number of sheets printed. The printer data includes the number of black and white and color images, and the cost for the specified period.
- Least Used Printers: This Dashboard report lists the top 10 printers that are used least, based on the number of sheets printed. The printer data includes the number of black and white and color images printed.
- Top Users: This Dashboard report lists the top 10 users who print the most sheets. Each entry in the list includes the number of black and white and color images, and the cost for the specified period.
- Top Departments: This Dashboard report lists the names of the departments that frequently use the printers. To obtain results for this dashboard report, ensure that users are assigned to a department.
- Daily Summary: This Dashboard report lists the jobs processed by Workplace Suite Usage Tracking (Network Accounting) feature or Mobility Suite server. The report shows the total number of 1-sided and 2-sided sheets and images printed for each day over the selected period. The report includes the following job types:

  - Jobs that cannot be parsed because the Incoming Queues for the Workplace Suite print queues are configured with a Conversion Mode of None.
  - Jobs that the Usage Tracking (Network Accounting) feature does not track.
- Hourly Summary: This Dashboard report lists the jobs processed by Workplace Suite Usage Tracking (Network Accounting) feature or Mobility Suite server processed jobs. The report shows the total number of 1-sided and 2-sided sheets and images printed for each hour over the selected period. The report includes the following job types:
  - Jobs that cannot be parsed because the Incoming Queues for the Workplace Suite print queues are configured with a Conversion Mode of None.
  - Jobs that the Usage Tracking (Network Accounting) feature does not track.

Summary

The Xerox® Workplace Suite Summary section provides predefined summary information for customers who use the reporting capability of Workplace Suite. The Summary section of the Reports tab provides the following reports:

- User Summary
- Printer Summary
- Department Summary
- Account ID Summary
- Accounting Summary

The Summary section includes the following options:

- Summary Tables: This menu allows users to select different Summary tables.
- Job Type: This menu allows users to select the source of the job data for the summary table.
  - Print and Copy: This option displays data for all print and copy jobs that generate printed output.
  - Print: This option displays data for all print jobs. Print jobs include delayed-print jobs, proof-print jobs, Secure-Print jobs, reports, scan-to-print jobs, embedded faxes, received faxes, and Internet-faxes.
  - Copy: This option displays data for the Workplace Suite jobs and copy jobs done at the printer using the Copy function.
  - Scan: This option displays the data for the Workplace Suite scans, scan jobs done at the printer using the Scan-to function, scan-to-email jobs, embedded-fax-send jobs, fax-send jobs, internet-fax jobs, scan-to-fax jobs, and scan-to-ifax jobs.
- Time Period: This menu allows users to select the time period for the data reported. Options include Last 7 days, Last 14 days, Last 30 days, and Added in Last 3 months, and Specify Date.
- Actions: This menu has four options:
  - Refresh: This option refreshes the page.
  - CSV Export: This option allows you to export Summary reports in .csv format.
  - PDF Export: This option allows you to export the Summary reports in PDF format.
  - Modify Cost: This option configures the cost of a printed page Summary reports.

In the Summary section, you can type a value in the text field and filter the list to show only values that match the search string.

SUMMARY TABLES

The Summary table lists the jobs processed by the Workplace Suite Usage Tracking (Network Accounting) feature or Mobility Suite server. The report includes the total number of 1-sided and 2-sided sheets printed. The report includes the following job types:

- Jobs that cannot be parsed because the Incoming Queues for the Workplace Suite print queues are configured with a Conversion Mode of None.
- Jobs that the Usage Tracking (Network Accounting) feature does not track.

The different types of summary reports are as follows:

- User Summary: This table displays the total number of sheets and images printed for each user over the selected period.
- Printer Summary: This table displays the total number of sheets and images printed for each printer over the selected period.
- Department Summary: This table displays the total number of sheets and images printed for each department over the selected period.
- Accounting Summary: This table displays a breakdown of the total number of sheets and images printed for accounting User ID and Account ID over the selected period.

EXPORTING REPORTS TO PDF OR .CSV

You can export reports in PDF format or .csv format.

To export Summary reports, do the following:

1. Click **Reports > Summary**.
2. From the Actions menu, to export the report, select one of the following:
   - To export reports in PDF format select **PDF Export**.
   - To export reports in .csv format, select **CSV Export**.

The default PDF format of the Summary file name is `SummaryName_YYYYMMDDHHMM.PDF`.

The default .csv format of the file name is `SummaryName_YYYYMMDDHHMM.csv`.

The cover page of an exported PDF report shows the Name, Date, Job type, and Description of the report. Each page has a heading and a page number. The PDF file shows details of the dashboard report, followed by applicable graphs.

Job Reporting

Note: Before you use the Job Reporting feature, ensure that you enable **Usage Tracking (Network Accounting)**. When Usage Tracking (Network Accounting) is enabled on a printer, the report data includes the printer Job Based Accounting (JBA) data. For more information, refer to Job Reporting Guidelines.

1. Click **Reports > Job Reporting**.
2. Optionally, Filter the data using any of the predefined filters or type in the filter text field.
   Predefined filters are as follows:
   - **Filter by Status**
   - **Filter by Date**
   - **Job Type**
   - **Filter by Field**
   - **Contains**
3. From the Actions menu, select **Export This Page**.

   The .csv file is downloaded to your computer.

Note: From the Actions menu, to export all data in the table, select **Export All Pages**.

Note: The default file name for the report is `JobReport_CurrentPage.csv`. If you select Export All Pages, the file name is `JobReport_AllPages.csv`.

JOB REPORTING REPORT FIELD DESCRIPTIONS

The following table contains descriptions of the Job Reporting fields:

NAME	DESCRIPTION	SOURCE OF INFORMATION (PRIMARY/SECONDARY SOURCE)
User Email	Email address format.	Server
job-owner	Used for association of job data with the network login name. If JBA is not enabled, use the value from the database. If JBA is enabled, use the supplied value.	Printer and Server
job-owner-domain	Used to provide login domain context association of the job-owner attribute.	Printer and Server
accounting-information-avp	For association of validation field names with log data entries. If JBA is not enabled, use Null. If JBA is enabled, then use double quote enclosed comma separated UTF-8 name / value pairs.	Printer
Department	The department associated with a given user. This is a database field in the user record. It MAY be blank.	Server
User ID	Value from JBA accounting-information-avp (XRX_ USERID) takes precedence. If JBA field is Blank, the value of the field is populated with the Workplace Suite Network Accounting User ID of the user. If both JBA and DB are blank or not populated, return Null.	Printer and Server
Account ID	Value from JBA accounting-information-avp (XRX_ ACCTID) takes precedence. If JBA field is Blank, the value of the field is populated with the Workplace Suite Network Accounting Account ID of the user. If both JBA and DB are blank or not populated, return Null.	Printer and Server
device-name	Used to uniquely identify a machine from others.	Printer and Server
Printer IP	The Printer IP address, the job was submitted to.	Server
Site	Name of the Site, the printer is assigned to.	Server
job-type	Specifies the type of job recorded. Each job will have only one type. Supported Values: 'Copy', 'Delayed Print', 'Embedded Fax Receive', 'Embedded Fax Send', 'Fax Send', 'Fax Receive', 'Internet Fax', 'Internet Receive', 'Other', 'Print', 'Proof Print', 'Report', 'Scan', 'Scan to Email', 'Scan to Fax', 'Scan to Internet Fax', 'Scan to Print', 'Secure Print', 'Store Files', 'Print Files'	Printer and Server
job-type-detail	Provides job type detailing designed to supplement the regular "job-type" attribute.	Printer

NAME	DESCRIPTION	SOURCE OF INFORMATION (PRIMARY/SECONDARY SOURCE)
system-job-type	This attribute identifies the system job type for the job log entry in which it appears.	Printer
job-identifier	The TCP/IP Host Name or string "job" concatenated with machine unique number.	Printer
system-job-identifier	The string "job" concatenated with a machine unique number.	Printer
Report ID	Solution unique ID. Mapping of job details to internal data element for debugging.	Server
job-name	The alphanumeric name of the job assigned by the user, or will default to Print / Copy / Fax / Scan if not supplied by user. The job identifier may be concatenated to any system generated default job type. Job name may be the file name of the submitted job.	Printer / Server
Server Received Time UTC	Denotes the UTC time when a job was submitted to the system. Only applies to Print Management or Mobile Printing job.	Server
Transferred To Printer Time UTC	Denotes the UTC time when a print job completely transferred to a printer. Only applies to Print Management or Mobile Printing job.	Server
printer-completion-time UTC	Denotes UTC the time when a print job completes at the printer (printing, filing, emailing, faxing). Only applies to jobs tracked using JBA.	Printer
printer-completion-time	Denotes the time when a print job completes at the printer (printing, filing, emailing, faxing). Only applies to jobs tracked using JBA.	Printer
Completion Time UTC	Denotes the UTC time when a print job completes at the printer (printing, filing, emailing, faxing). Only applies to jobs tracked using JBA.	Server
Job Status	Indicates the final status (success / failure) of a job.	Server
jba-completed-reasons	The final state of a job.	Printer
job-copies-completed	The number of sets of a job that were produced. E.g: A four page document with 3 copies completed means that 3 sets of 4 pages each were produced.	Printer and Server
Color Printed	Indicates if a job had 1 or more color pages.	Server

NAME	DESCRIPTION	SOURCE OF INFORMATION (PRIMARY/SECONDARY SOURCE)
finishing-staple	If JBA is enabled, this field indicates if the job used stapling. If JBA is disabled, then this setting applies only to Print Management or Mobile Printing jobs and indicates if stapling was requested.	Printer and Server
finishing-punch	If JBA is enabled, this field indicates if the job used hole punching. If JBA is disabled, then this setting will always indicate 'No'.	Printer and Server
finishing-fold	If JBA is enabled, this field indicates if the job was folded. If JBA is disabled, then this setting will always indicate 'No'.	Printer and Server
Duplex Printed	If JBA is enabled, this field indicates if the job resulted in 1 or more duplex pages. If JBA is disabled, this setting indicates if duplex was requested.	Server
Color Pages Printed	The total number of color pages printed or total color images produced for a job. If JBA is disabled, this number wil indicate the total pages of a Print Management or Mobile Printing Job which was requested to print as color (it does not mean all pages actually print using color).	Server
Black And White Pages Printed	The total number of black & white pages printed or total black & white images produced for a job. If JBA is disabled, this number will indicate the total pages of a Print Management or Mobile Printing Job which was requested to print as black and white.	Server
media-type	The type of media (paper) used when printing a job. If JBA is disabled, then this value will be null. The supported values are machine dependent and are not part of a fixed set. So translation of this object will not be possible.	Printer
media-color	The color of the paper used when printing a job. If JBA is disabled, then this value will be null. The supported values are machine dependant and are not part of a fixed set. So translation of this object will not be possible.	Server
media-size	Media size using well known names (if available). If a mapping of the size to a name does not exist, then the value of "Unknown" will be return.	Server
media-size-in-mm	Media size in millimeters.	Server

NAME	DESCRIPTION	SOURCE OF INFORMATION (PRIMARY/SECONDARY SOURCE)
media-sheets-produced	The total number of sheets of media (paper, transparency, etc) printed. If JBA is not enabled, then null will be returned.	Server
media-tiers	Number of media tiers for the given job. If tiered billing is not supported or JBA is not enabled, then null will returned.	Server
media-tier-1-count	Number of impressions at tier level 1. Will be null if tiered billing is disabled or JBA is disabled.	Server
media-tier-2-count	Number of impressions at tier level 2. Will be null if tiered billing is disabled or JBA is disabled.	Server
media-tier-3-count	Number of impressions at tier level 3. Will be null if using 2 tiered billing, tiered billing is disabled or JBA is disabled.	Server
media-black-and-white-pages	The number of media sides to which black and white impressions are applied for the given media block. If JBA is disabled then null will be returned.	Server
media-color-pages	The number of media sides to which color impressions are applied for the given media block. If JBA is disabled then null will be returned.	Server
number-of-images	Total count of impressions including banner sheets and error sheets but excluding blank sheets if the job type is a type that prints. Also indicates the total number of impressions scanned if the job is a scan only job. If the job is a compound job that both scans and prints, the number indicated will be the number impressions that were printed.	Server
media-other-pages	Sheet count for all new media types encountered after the first 6. If JBA is disabled, null will be used.	Server
total-simplex-sheets	Total number of simplex imaged sheets output by job content including banner sheets and cover sheets (simplex imaged cover sheets). If a sheet is printed on one side or blank (no images at all), it is counted as a simplex sheet.	Server
total-duplex-sheets	Total number of duplex sheets output by job content including banner sheets and cover sheets. If a sheet is printed on both sides, it is counted as a duplex sheet. Note: Some simplex to duplex jobs will contain both duplex and simplex output sheets.	Server

NAME	DESCRIPTION	SOURCE OF INFORMATION (PRIMARY/SECONDARY SOURCE)
image-size	Image size using well known names (if available). If a mapping of the size to a name does not exist, then the value of "Unknown" will be return.	Server
image-size-in-mm	Describes the size of the image that is scanned.	Server
images-sheets-produced	Number of image sheets that were scanned.	Server
black-and-white-images	Number of B&W image sides that were scanned.	Server
color-images	Number of color image sides that were scanned.	Server
image-other-size	The count of image blocks scanned after the first 3 image blocks	Server
total-network-destinations	The total number of scan destinations to which documents were scanned and filed (up to a maximum of 6).	Server
total-scan-pages-delivered	The total number of pages scanned to the set of scan destinations.	Server
scan-other-pages	The total count of all impression sides sent to all new document paths after the first 6.	Server
total-number-of-images-filed	Total count of the number of images scanned and filed to file server(s). Counts images scanned to file, scanned to fax, scanned to email and any other scan job types filed to a network server. Does not apply to images stored only on the originating device. Counted are images scanned that are successfully filed. If an image is filed to a least one file server, it is counted once. Image totals are computed as follows: number of network destinations times number of image.	Server
number-of-phone-numbers	The total number of destination phone numbers used in the job.	Server
total-number-of-smtp-recipients	Contains the totaled number of all to, cc, and bcc attributes in a scan to email job.	Server
fax-images-completed	The total number of fax images completed for a single job (could be multiple fax calls).	Server
fax-success-calls	The total number of fax calls successfully completed for a single job.	Server

NAME	DESCRIPTION	SOURCE OF INFORMATION (PRIMARY/SECONDARY SOURCE)
fax-failed-calls	The total number of failed fax calls for a single job.	Server
Content Profile Matched	The Content Security profile that was matched.	Server

Schedule

The Schedule section shows the defined scheduled summary reports. The administrator can create, delete, or edit the scheduled reports. A schedule consists of a type of report, the creation of interval, the output format of the report, and a recipient list.

The Actions menu has the following options:

- New: This option allows you to create a schedule for the summary report.
- Delete: This option allows you to delete a schedule that appears in the list.
- Enable: This option allows you to enable a schedule that appears in the list.
- Disable: This option allows you to disable a schedule that appears in the list.
- Run Now: This option allows you to run a schedule that appears in the list.

CREATING A SCHEDULE

Note: After you schedule a report and before the report is created, to ensure that the report has the latest data, run the Job Reporting task. For more information, refer to Settings: Job Reporting.

To create a schedule for a summary report, do the following:

1. Click **Reports > Schedule**.
2. From the Actions menu, click **New**.

The New Schedule window appears.

3. In the Details section, do the following:
   a. In the Name field, type the required name.
   b. In the Description field, type the required description.
4. To set the file format for a summary report, for File Format, select one of the following radio buttons:
   - **PDF**: To export the report in PDF format, select this option.
   - **CSV**: To export the report in .csv format, select this option.
5. To set the frequency for a summary report, for Frequency, select one of the following radio buttons:
   - **Weekly**: To receive the summary report once a week on a Sunday, select this option.
   - **Monthly**: To receive the summary report on the first day of every month, select this option.
6. To define the job type for a summary report, for Job Type, select one of the following options:
   - **Print and Copy**
   - **Print**
   - **Copy**
   - **Scan**
7. Click **Next**.

   The Reports screen appears.

8. To select which summary reports to assign to the schedule, select one or more of the following toggle buttons: By default, The summary reports toggle buttons are disabled.
   - **User Summary**
   - **Printer Summary**
   - **Department Summary**
   - **Accounting Summary**
   - **Account ID Summary**
9. Click **Next**.

   The Email Settings screen appears.
10. From the Email Settings screen, do the following:
    a. In the To field, type the required email address.
    b. In the Subject field, type the required subject.
    c. In the Message field, type the required message.
11. Click **Next**.

    The Verify screen appears. Review the scheduled task summary.
12. To enable the schedule, select the check box for **Enable Schedule Task**.
13. To confirm and save the schedule, click **Finish**.

EDITING A SCHEDULE

To modify a schedule, do the following:

1. Click **Reports > Schedule**.
2. Select the name of the schedule that you want to edit. The name appears in blue.

   The Edit Schedule screen appears. This screen displays the name of the scheduled summary report.
3. Make the required changes, then click **Save**, or to cancel the changes, click **Cancel**.

DELETING A SCHEDULE

To delete a schedule, do the following:

1. Click **Reports > Schedule**.
2. Select the check box next to the schedules that you want to delete.
3. From the Actions menu, select **Delete**.

ENABLING A SCHEDULE

To enable a schedule, do the following:

1. Click **Reports > Schedule**.

2. Select the check box next to the schedules that you want to enable.
3. From the Actions menu, select **Enable**.

DISABLING A SCHEDULE

To disable a schedule, do the following:

1. Click **Reports > Schedule**.
2. Select the check box next to the schedules that you want to disable.
3. From the Actions menu, select **Disable**.

RUNNING A SCHEDULE

To run a schedule, do the following:

1. Click **Reports > Schedule**.
2. Select the check box next to the schedules that you want to run.
3. From the Actions menu, select **Run Now**.

User Audit

1. Select **Reports > User Audit**.
2. Optionally, enter a search term to refine your displayed data in the User Audit table.
3. Select **Export This Page** from the Actions menu.

   The Save As window displays.

   Note: To export all data in the table, choose **Export All Pages** from the Actions menu.

4. Navigate to where you want to save the report and select **Save**.

   Note: The default filename for the report is UserAudits_CurrentPage.csv.

   The **Actions** menu provides a list of tasks that can be performed.

   The **Page** indicator shows which page is being viewed of the total number of pages.

   The **Items Per Page** indicator lets you set the number of email addresses that are displayed per page.

   The **Search** field lets you quickly find specific email addresses in long lists.

Delegation

This chapter contains:

The Xerox® Workplace Suite provides a user portal to allow you to manage printing responsibilities. You can delegate printing responsibilities for your jobs to other users, and allows users to print your jobs from their Printer Client (EIP app).

To access jobs that belong to other users that you are delegated to print, use the Printer Client.

Xerox® Workplace Suite User Portal

To access the Workplace Suite user portal, open a Web browser, then type `https://xxx.xxx.xxx.xxx/login`, where `xxx.xxx.xxx.xxx` is the IP address or the hostname for your server.

PRINTER CLIENT DOCUMENT RELEASE PERMISSIONS

The Permissions section is used to manage document release permissions you have given to others or which have been granted to you. When a user is given permission to access other users print jobs, they can see their job list when using the Printer Client. They can also manage their print jobs, including deleting or printing any job submitted by that user.

- **Print Theirs**: Use the Print Theirs tab to manage the list of users for which you have released permission. You can request that other users grant you permission to manage their documents.
- **Print Mine**: Use the Print Mine tab to manage which users can view, delete, or print your jobs.

ADDING THE DOCUMENT RELEASE PERMISSIONS FROM THE USER PORTAL

1. Log in to the user portal with your email address and confirmation number, or LDAP credentials.
2. To request permission to manage documents that belong to other users, select **Print Theirs**.
   a. Click **Actions > Request**. Enter the email address of the user for whom you want to request document access. Click **OK**.

      An email message is sent to the user that you designated, that requests that they grant you permission to release their documents.

   b. To remove users from the permissions list, select the users, then click **Actions > Remove**.
3. To manage which users can view, delete, or print your jobs, select **Print Mine**.
   a. To add other users to your allowed list, click **Actions > Add**.

      You can add users or select users that you previously added to allow access to your documents.

   b. To remove users from the permissions list, select the users, then click **Actions > Remove**.

Printing Other User Jobs from the Printer Client

1. At a Xerox® Workplace Suite enabled printer, from the control panel, touch the **Workplace Suite** icon.
2. Log in to the Printer Client with your user name and confirmation number, or company login credentials.
3. To access jobs that belong to other users, click the **Person** icon, located next to the Exit button.

   Note: You can view only the jobs for users who have granted you permission to release their jobs.

4. Select the user whose jobs you want to print.

   The list of jobs appears in the Printer Client.

5. Select the jobs to print, select the Output Settings, then click **OK**.

   You can preview selected jobs before printing.

6. Click **Print**.
7. Collect the prints.
8. To select a different user, click the **Person** icon. Repeat the steps as needed.
9. When you are finished, click **Exit**.

Troubleshooting

If you are having a problem with the Xerox® Workplace Suite software, refer to the *Xerox® Workplace Suite Troubleshooting Guide*. To obtain the guide, and for more information, use the searchable support website at www.xerox.com/XWSsupport.

Standard Default Ports

This chapter contains:

The following table lists the standard default ports used for many of the protocols with Workplace Suite. Some port numbers are configurable in Workplace Suite such as the POP and IMAP ports. Other port numbers are non-configurable and cannot be changed. You may need to change some port numbers depending on the server you are communicating with or use the default ports if they cannot be changed. All ports used must be unblocked in the firewall that is being used on the solution server.

PROTOCOL	TRANS-PORT AND PORT VALUE	USE	OPTION	DIREC-TION
Xerox Workplace Mobile App Ports:				
HTTPS using TLS	TCP 443	Authentication, Job / Printer Listing, Initiate Print Conversion	Non-configurable	App to XWS Service
Xerox Workplace Suite:				
DCE	TCP 8801, 8802	XWS and DCE Communication	Configurable	XWS to DCE
HTTPS	TCP 443	XWS uses this port to communicate with other XWS servers. XJAS and XJAC also request info using this port.	Configurable	XWS / XJAS / XJAC to XWS
HTTP	TCP 80	XWS uses this port to notify XJAC that a job is ready to be released.	Non-configurable	XWS to XJAC
SQL	TCP 1433	Microsoft SQL Client to Server Communication for database queries and storing.	Non-configurable	XWS to SQL Server
LDAP	TCP 389	Authentication, User Look-up	Non-configurable	XWS to ADS Server
LDAPS	TCP 636	Authentication, User Look-up.	Configurable	XWS to LDAP Server
HTTPS using TLS	TCP 443	Convenience Authentication, EIP Registration, Configuration, Accounting, Scan Job Retrieval. Note: HTTPS preferred.	Non-configurable	XWS to Printer

PROTOCOL	TRANS-PORT AND PORT VALUE	USE	OPTION	DIREC-TION
HTTP	TCP 80	EIP Registration, Configuration, Accounting, Scan Job Retrieval. Note: HTTPS is used if enabled on the printer.	Non-configurable	XWS to Printer
SNMP	UDP 161	Printer Discovery, Configuration	Non-configurable	XWS to Printer
HTTPS using TLS	TCP 443	Send Print History and Retrieve Printer List to or from XMS.	Non-configurable	XWS to XSM
HTTPS using TLS	TCP 443	Send system utilization information to the Workplace Suite Reporting Service (MSRP)	Non-configurable	XWS to MSRS
SMTP	TCP 25	Sending email responses	Non-configurable	XWS to SMTP Server
SMTP/TLS (Secure SMTP)	TCP 465	SMTP over TLS. TCP port 465 is reserved by common industry practice for secure SMTP communication using the SSL protocol.	Configurable	XWS to SMTP Server
POP3	TCP 110	Post Office Protocol version 3, enables “standards-based” clients such as Outlook to access the email server.	Configurable	XWS to POP3 Server
POP3/TLS	TCP 995	POP3 over TLS uses TCP port 995 to receive encrypted email messages.	Configurable	XWS to POP3 Server
Exchange Web Services	TCP 443	Exchange Web Services used for receiving Email	Configurable	XWS to Exchange
IMAP	TCP 143	Internet Message Access Protocol version 4, may be used by“standards-based”clients such as Microsoft Outlook Express or Netscape Communicator to access the email server.	Configurable	XWS to IMAP Server
IMAP/TLS	TCP 993	IMAP4 over TLS for securely receiving encrypted email messages.	Configurable	XWS to IMAP Server
NRPC	TCP 1352	Lotus Notes RPC. This is the API used between Lotus Notes and the Lotus Domino server. Communication between XMPC and Lotus Notes is via a local API on the same PC.	Non-configurable	XWS (running Lotus Notes) to Domino Server

PROTOCOL	TRANS-PORT AND PORT VALUE	USE	OPTION	DIREC-TION
HTTP / HTTPS	TCP 80 / TCP 443	Administration using Web Admin Tool. If a certificate is already configured on the IIS default website, it will be used by Xerox® Workplace Suite. If no certificate is configured, Xerox®Workplace Suite will create a self-signed cert. The administrator has the option to load a certificate from a trusted authority later if desired.	Non-configurable	Browser to Work-place Suite Service
HTTPS	TCP 8443	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	Work-place Suite Service to Xerox Licensing Server
IPP	TCP 631	Receipt of Mobile Jobs on phones using the iOS Native Print feature. Always uses SSL.	Non-configurable	Mobile Phone to XWS
HTTPS	TCP 443	HTTP over TLS. Used to validate a Chrome browser or Chromebook single sign-on user with Google.	Non-configurable	XWS to Google
AppSocketRAW or Windows TCP-Mon	TCP 9100	Print Submission of Copy Jobs	Non-configurable	XWS to Printer
LPR	TCP 515	Print Submission of Copy Jobs	Non-configurable	XWS to Printer
IPP over TLS	TCP 443	Print Submission of Copy Jobs. Encrypted print transfer.	Non-configurable	XWS to Printer
Document Conversion Engine Server Ports:				
AppSocketRAW or Windows TCP-Mon	TCP 9100	Print Submission	Non-configurable	DCE to Printer
LPR	TCP 515	Print Submission	Non-configurable	DCE to Printer
IPP over TLS	TCP 443	Print Submission. Encrypted print transfer.	Non-configurable	DCE to Printer
DCE	TCP 8801, 8802	XWS and DCE Communication	Configurable	XWS to DCE
Print Server Ports:				

PROTOCOL	TRANS-PORT AND PORT VALUE	USE	OPTION	DIREC-TION
SMB Print	TCP 445	Print submission to a network queue. Client Workstation to print server.	Non-configurable	Worksta-tion to Print Server
DCE/RPC	TCP 1058	Network Print Queue Access and Driver Download. From Workstation Print Queue to Print Server or from Workplace Suite Client to Print Server.	Non-configurable	Worksta-tion to Print Server
Printer and Printer Client (EIP App) Ports:				
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.	Non-configurable	Printer EIP App to XWS Service
HTTPS	TCP 443	Printer Authentication	Non-configurable	Printer to XWS
Xerox Job Agent Service Ports: Note: XJAS - Xerox Job Agent Server, the Workplace Suite Print Server that is hosting the Network Queues, this can be an external Print Server or the Main Server.				
Raw IP	TCP 9100	Print Submission	Configurable	XJAS to Printer
LPR	TCP 515	Print Submission	Configurable	XJAS to Printer
IPP over TLS	TCP 443	Printer Submission	Non-configurable	XJAS to Printer
HTTPS	TCP 443	Configuration, Job Information, Print Release	Configurable	XWS to XJAS
Xerox Job Agent Client (XJAC) Ports: Note: XJAC - Xerox Job Agent Client, this is the Xerox Desktop Print Client Software.				
RAW	TCP 9907	Notification of Print Job Release (TCP/IP Mode)	Configurable	XWS to XJAC
RAW IP	TCP 9700	Communication method for the Desktop Client, called TCP/IP	Configurable	XJAC to XWS
Raw IP	TCP 9100	Print Submission	Configurable	XJAC to Printer

PROTOCOL	TRANS-PORT AND PORT VALUE	USE	OPTION	DIREC-TION
LPR	TCP 515	Print Submission	Configurable	XJAC to Printer
IPP over TLS	TCP 443	Print Submission	Non-configurable	XJAC to Printer
DCE/RPC	TCP 1058	Network Print Queue Access and Driver Download. From Workplace Suite Client to Print Server	Non-configurable	Work-place Client to Print Server
HTTPS	TCP 443	Configuration, Job Information, Print Release	Configurable	XJAC to XWS
Raw	UDP 9807	Notification of Print Job Release	Configurable	XWS to XJAC
Network Appliance Ports:				
RAW	TCP 7778	Receive Card Swipe Data from Elatec TCPConv	Configurable	Network Appliance to XWS
RAW	TCP 7777	Receive Card Swipe Data from Elatec TCPConv2	Configurable	Network Appliance to XWS
RAW	TCP 2001	Receive Card Swipe Data from RFIdeas Ethernet 241	Configurable	Network Appliance to XWS
iOS Native Printing Ports:				
DNS-SD	UDP 53	Mobile Phone printer discovery using DNS	Non-configurable	Phone to DNS Server
mDNS	UDP 5353	Mobile Phone printer discovery on the local subnet using mDNS	Non-configurable	Phone Broadcast on Local Subnet
IPP	TCP 631	IPP Print submission to Xerox® Workplace Suite. Always uses TLS.	Non-configurable	Phone to XWS

Using a Load Balancer with Workplace Suite

Load balancer is used to scale the solution by distributing requests to multiple servers. Load balancer is used to provide failover by detecting when a server is no longer operational and routing data to a different server.

When 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 Load Balancer needs to be able to probe the server to determine if it is available and can handle an incoming request. This probe should specifically exercise the Xerox Workplace Suite services and not perform a simple ICMP PING of the OS.

- The Xerox Workplace Suite server supports a single HTTPS based Load Balancer probe endpoint.

```
XWS Host Service: https://<server>:443/Bula/Admin/ping
```

Note: No authentication is required to access this endpoints.

- After defining an endpoint, the Xerox Workplace Suite server will return with:
  - An HTTP 200 (ok) response if the service is up and healthy.
  - Any other error should be considered a failure, such as HTTP 500 (internal server error), HTTP 404 (not found) or 408 (request timeout) and so on.
- The endpoint will test both the following, and if either or both fail, then a negative response will be returned (something other than 200).
  - BULA backend is up and functioning.
  - EIP browser backend is up and functioning.

Configure Alternate Access Card Users with CAC/PIV Environments

This appendix contains:

Configuring for Alternate Access Card Users with CAC/PIV Environments

This user matching algorithm applies when you use CAC/PIV cards for printer authentication and use the Workplace Suite as a Follow-You Print solution. The Workplace Suite compares the printer session data for an Authenticated user with the Workplace Suite user database. The comparison is done in the following order: User Name, then Alternate Access Card User.

- An LDAP mapping field, Alternate Access Card User, is mapped by default to userPrincipalName.
- When you import or auto-onboard LDAP users, the new Alternate Access Card User field populates with the mapped LDAP entry details.
- Alternatively, to configure the Alternate Access Card User field, you can use the Users CSV Import feature.

1. To have the printer compare the Alternate Access Card User field with the printer session data, click **Company > Policies > Security**.

   The Security Settings webpage opens.

2. On the Security Settings webpage, select **Printer Client**.
3. To enable the feature, click the **Logged on Users (Access Card) and External Printer Authentication** check box.

Administration Recovery Procedure

This appendix contains:

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.

To make changes, launch the Administration Wizard. When launched, the Getting Started Wizard runs to guide you through current system administration configurations.

Note: To complete the Administration Recovery Procedure, it is required that you complete all steps of the Getting Started Wizard. When finished using the wizard, click **Finish** on the last window. If you fail to complete the Wizard, changes are not implemented and the Getting Started Wizard remains in an open or incomplete state.

Security Requirements

To use the Administration Recovery Procedure, you must be a member of one of the following groups on the Workplace Suite server:

- Local Windows or Domain Administrator group
- Local Windows MPAdmin group

Using the Administration Recovery Procedure

To add a new Alternate Administrator with Web Portal login credentials:

1. To access your Xerox® Workplace Suite server, use the following recovery URL for the active authentication method:
   `https://<server name or IP address>/administrator`

   Note: If Windows Integrated Authentication is enabled and this URL does not result in a prompt for your user credentials, use the following URL:

   `https://<server name or IP address>/ssologin/reset`

2. Log in using your user credentials. For details, refer to Security Requirements.
3. Follow the step-by-step instructions. Change settings as necessary.
4. To update the Web User Portal and save your changes, at the Ready window, click **Finish**.

   The User Portal is reconfigured to authenticate using Email and Confirmation Number. If necessary, change the User Portal authentication method back to your required configuration.

5. To change the User Portal authentication method:
   a. Click **Company > Policies > Security**.
   b. Click the **User Portal** tab.
   c. For User Portal Login, select the required authentication method and change other settings, as needed.
   d. Click **Save**.

Rerunning the Setup Wizard

The setup wizard allows you to configure the following settings:

- Profile
- Proxy
- License
- Incoming Email
- Outgoing Email, settings are required

To rerun the setup wizard:

1. To access your Xerox® Workplace Suite server, use the following recovery URL for the active authentication method:
   `https://<server name or IP address>/administrator`

   Note: If Windows Integrated Authentication is enabled and this URL does not result in a prompt for your user credentials, use the following URL:

   `https://<server name or IP address>/ssologin/reset`
2. Log in using your user credentials. For details, refer to Security Requirements.
3. To configure the solution software, follow the step-by-step instructions in the wizard.

   Note:

   - Type the appropriate data in the fields and set options, as needed.
   - To navigate through the configuration steps, use the **Next** or **Back** buttons.
4. To confirm your settings, click **Test**.

Unlocking a Printer Using the Xerox Workplace Mobile App®

This appendix contains:

Printer Login Methods Using the Mobile App

Both Mobile Print Workflow and Print Management Workflow must be installed for Mobile Phone Unlock to work. Mobile Phone Lock must be enabled. For details, refer to Mobile Phone Unlock.

The log in methods available from the Xerox® Workplace Mobile App include:

- The ability to log in to the Printer using a QR Code.
- The ability to log in using Manual Code Entry at a Printer Login Window.
- The ability to log in using NFC on Android and iOS devices. Available for Xerox® AltaLink® printer families and Xerox® VersaLink®printer families only.

Logging in to a Printer Using a QR Code

Both Mobile Print Workflow and Print Management Workflow must be installed for Mobile Phone Unlock to work. Ensure that Mobile Phone Lock is enabled. For details, refer to Mobile Phone Unlock.

To log in to a multifunction printer using a QR Code:

1. On a Xerox® AltaLink® printer, scan the QR Code on the printer Login Screen.
2. On any supported Xerox® printer, scan the QR Code on your printed Welcome to Xerox Workplace Suite page.

Logging in to a Printer Using Manual Code Entry

Both Mobile Print Workflow and Print Management Workflow must be installed for Mobile Phone Unlock to work. Mobile Phone Lock must be enabled and an Unlock Code established. For details, refer to Mobile Phone Unlock.

To log in to a printer using Manual Code Entry, enter the Unlock Code, found on the printer Login Screen.

Logging in to a Printer Using NFC

Both Mobile Print Workflow and Print Management Workflow must be installed for Mobile Phone Unlock to work. Ensure that Mobile Phone Lock is enabled. For details, refer to Mobile Phone Unlock.

Note: For iPhones, this feature is limited to iPhone 7 and newer, with iOS 11.

To log in to a printer using Near Field Communication:

1. From Xerox® Workplace Suite, enable Mobile Phone Unlock. For details, refer to Mobile Phone Unlock.
2. On your printer, enable Near Field Communication. For details, refer to Enabling NFC on Altalink Devices or Enabling NFC on Versalink Devices.
3. Add a printer , then enable **Authentication** and enable **Features**. Click **Save**.
4. In a mobile device that supports Near Field Communication, log in to the Xerox® Workplace Mobile App.
5. Select **Menu**.
6. Select **Unlock Printer**.
7. Place the mobile device near the printer NFC area.

   After the printer is unlocked, your mobile device displays `Unlock printer is successful`.

Enabling NFC on Altalink Devices

1. Navigate to device IP web page.
2. Login as an administrator.
3. Click **Connectivity**.
4. Click **Setup**.
5. Under Protocol, locate NFC and click **Edit**.
6. Enable NFC.
7. Click **OK**.

Enabling NFC on Versalink Devices

1. Navigate to device IP web page.
2. Login as an administrator.
3. Click **Connectivity**.
4. Click **NFC**.
5. Enable NFC.
6. Click **OK**.

Xerox® Workplace Mobile App for Chrome

This appendix contains:

This section describes the administration of the Xerox® Workplace Suite Mobile App for Chrome. This information applies only when you use the Google Admin Console to manage users and settings.

Configuring Workplace Mobile App Settings for Google Chrome

SETTING	DESCRIPTION
DefaultServiceURL (String) **Default: None**	Overrides the cloud URL and takes you to a designated mobile app. Use this option to bypass the Xerox Cloud Routing Service and go to a DMZ or onsite server. Unless you connect to your own network, this setting prohibits Workplace Mobile App access.
CanChangePrinters (Yes/No) **Default: Yes**	Modifies the Workplace Mobile App Printer List. If you set up printers that users can see, but not change, select **No**. For example, at a school, select **No** when students can use only designated student printers, and cannot add printers.
PullPrint (Yes/No) **Default: Yes**	Displays the mobile app printer in the list of user devices. The mobile app printer is a device used only for uploads. Use this setting when you submit jobs that you later release to the mobile app or Xerox® EIP Printer Client for mobile printing.
Printers (List) **Default: None**	Displays a list of printers where you can select the default. For mobile app users, these printers must be valid and enabled in the mobile app or cloud print server.
StandardAccounting (Object) **Default: None**	When you configure the selected printer for standard accounting, this option sets up a default user ID and passcode. When you print, you can use the advanced options listed in the printer dialog. If you use the default user ID, it eliminates the need to remember the user ID and passcode.
NetworkAccounting (Object) **Default: None**	If you configure a selected printer for network accounting, this option sets up a default user ID and accounting ID. When you print, you can use the Advanced options in the printer dialog. If you use the default user ID, it eliminates the need to remember the user ID and passcode.
SingleSignOn (Yes/No) **Default: No**	If the Xerox® Workplace Suite server supports this feature, this option requires the client to use Google Single Sign-on.

Uploading the Xerox® Workplace Mobile App Chrome Configuration File

1. To create a configuration file, copy the configuration text from Example 2, then paste the text into a new file. Save the file and add a **.json** extension.
2. To edit the new **.json** file, use your deployment settings, then edit the new **.json** file. Click **Save**.

   Note: The revised configuration file does not function without a **.json** extension.
3. Remove the default settings from the current configuration file. Refer to *Example 2: A Configuration that Removes Standard and Networking Accounting.*
4. Access **https://admin.google.com**, then log in as the Administrator.
5. Select **Device Management > Chrome Management**.

   The Chrome Management screen appears. From the Chrome Management screen, you can configure the following features:

   - User Settings
   - Google Play Store Settings
   - Public Session Settings
   - Device Settings
   - Devices
   - App Management
6. Click **App Management**.
7. In the **Find** or the **Update Apps** field, type Xerox, then click **Search**.
8. Select **Xerox Workplace Mobile App**, then click **User Settings**.

   Note: Users are grouped by organization or business unit. You can customize the user settings or apply one configuration to all groups. For more information on Settings, refer to https://support.google.com/chrome/a/answer/1375694.
9. To upload the customized configuration file, from the Org column, select an organization. Click **Upload Configuration File**, then click **Save**.
10. To validate the contents of the uploaded configuration file, click **View**.

    Note: Policy changes take a few minutes to enable.
11. To view the latest policies for an application, or to force an immediate device reload:
    a. Use the Chrome browser, then access **chrome://policy**.
    b. To view the current configuration values for the Workplace Mobile App, scroll the page.

    Note: The configuration values for the Workplace Mobile App are set in the Google Admin Console.

Example 1: Complete Configuration

For a complete configuration:

1. Copy and paste the information from Example 2, and use the information as a template for your new configuration file.
2. Name and save the file with a **.json** extension.

Note: The file does not function without the **.json** extension.

Example 2: A Configuration that Removes Standard and Network Accounting

```
{
"DefaultServiceUrl": {
"Value": "https://<Server Hostname>/capi"
},
"PullPrint": {
"Value": "No"
},
"SingleSignOn": {
"Value": "Yes"
},
"CanChangePrinters": {
"Value": "Yes"
},
"Printers": {
"Value": [
{ "name": "Printer Name" },
]
},
"NetworkAccounting": {
"Value": [
{
"field_id": "userId",
"field_value": "grade4\\students"
},
{
"field_id": "accountingId",
"field_value": "grade4_students"
}
]
},
"StandardAccounting": {
"Value": [
{
"field_id": "userId",
"field_value": "grade4_students"
{},
"field_id": "accountingId",
"field_value": "grade4_students"
}
]
}
}
```

1. Add the following text at this location.

Note: It is important that you add this text **before** you remove the text from step 2.

```
{
"DefaultServiceUrl": {
"Value": "https://xccsts.services.xerox.com/commonloginservice.svc”
},
"PullPrint": {
"Value": "Yes"
},
"CanChangePrinters": {
"Value": "No"
},
"Printers": {
"Value": [
{ "name": "VersaLink B405" },
]
```

2. Remove the following text:

Note: It is important that you do not remove this text until you **after** you add the text from step 1.

```
},
"NetworkAccounting": {
"Value": [
{

"field_id": "userId",
"field_value": "grade4\\students"
},
{
"field_id": "accountingId",
"field_value": "grade4_students"
}
]
},
"StandardAccounting": {
"Value": [
{
"field_id": "userId",
"field_value": "grade4_students"
},
{
"field_id": "passcode",
"field_value": "print_code_123"
}
]
}
```

3. Add the following text:

```
}
}
"DefaultServiceUrl": {
"Value": "https://xccsts.services.xerox.com/commonloginservice.svc”
}
"PullPrint": {
"Value": "Yes"
},
"CanChangePrinters": {
"Value": "No"
},
"Printers": {
"Value": [
{ "name": "VersaLink B405" },
]
}
}
```

Enabling Copy and Scan

This appendix contains:

Enabling Copy and Scan on Your Xerox® AltaLink® Printer

To enable Copy and Scan features on your Xerox® AltaLink® Printer:

1. Access the Embedded Web Server page for your Xerox AltaLink printer, then log in as an administrator.
2. Select **Properties > Apps > Printing > Printing Web Services**.
3. Verify that the following settings are selected:

- For Remote System Management, select **Extensible Service Registration**, then select **Device Configuration**.
- For Print Services, select **Print Extension**, or for Job Submission, select **Print Submission**.
- For Scan Services, select **Scan Extension**, or for Job Submission, select **Scan Submission**.
- For **Job Management**, select **Job Management Extension**, then select **Allow Open Access to Job Information**.
- For Authentication & Accounting, select **Authentication & Accounting Configuration**, then select **Session Data**.

4. Select **Properties > Apps > Workflow Scanning**.
5. Ensure that **Remote Start (TWAIN)** is selected.
6. For printers enabled with the Xerox® Workplace Suite, select **Repair** or **Re-add**.
7. At the printer control panel, select the Workplace Suite App, then verify that the Copy and Scan features are installed and available on the Xerox AltaLink printer.

Enabling Copy and Scan on Your Xerox® VersaLink® Printer

To enable Copy and Scan features on your Xerox® VersaLink® printer:

1. Access the Embedded Web Server page for your Xerox VersaLink printer, then log in as an administrator.
2. Select **Apps > EIP Settings > EIP Web Services**.
3. Verify that the following settings are selected:

- For Remote System Management, select **Extensible Service Registration**, then select **Device Configuration**.
- For Print Services, select **Print Extension**.
- For Scan Services, select **Scan Extension**.
- For Authentication & Accounting, select **Configuration**, **Session Data**, and **Xerox Secure Access**.

4. Select **Apps > EIP Settings**.
5. Ensure that the Start Job Using Remote Program feature is selected.
6. For printers enabled with the Xerox® Workplace Suite, select **Repair** or **Re-add**.
7. At the printer control panel, select the Workplace Suite App, then verify that the Copy and Scan features are installed and available on the Xerox® VersaLink® printer.

Xerox® Workplace Suite for Xerox® PrimeLink®, Color C60/C70 and Versant Printers with Fiery® Controller

This appendix contains:

This section provides procedures on setting up Xerox® Workplace Suite for Xerox® PrimeLink® printers, Xerox® Color C60/C70, and Versant printers with the Fiery® controller.

Fiery® Configuration Overview

The Fiery® controller is an optional print controller that you can configure for use with Xerox® PrimeLink®, C9065/C9070 printers, Xerox® Color C60/C70 printers, and Versant printers.

You can connect the Fiery® controller to the network and to the printer using one of the following configurations:

- Direct Configuration
- Network Hub Configuration

Xerox® Workplace Suite fully supports Network Hub Configuration.

- Network Hub Configuration: For this configuration, the printer and the Fiery® controller each have their own IP address. The printer and controller connect to the network independently of each other. When you use the Network Hub configuration, the printer controller works as if an Fiery® controller is not present.
- Direct Configuration **(Not Supported)**: For this configuration, only the Fiery® controller is connected to the network. The printer is connected to the Fiery® controller, but is isolated from the network.
- Xerox® Workplace Suite now supports the ability to release Jobs from the Printer EIP App to the Fiery®. This feature is called **Print to Alternate IP Address**.

Xerox® Workplace Suite and Fiery® Direct Configuration Setup Procedure

ENABLING THE PRINTER TO RELEASE THE JOB TO THE FIERY® CONTROLLER

Note: Set the Fiery® and Printer to Dual IP Mode. Ensure that both the devices are on the public network, make note of the Printer's and Fiery® IP Address. If you want to use Card Authentication, and if you are using a Versant Press you will have to add the USB Plugin.

Guidelines on Dual IP Fiery® Support:

- The Fiery® controller connects to the network and to the printer in two ways, single IP Mode and Dual IP Mode.
- The **Alternate IP address for printing** feature is designed for the Dual IP Mode configuration.
- The printer and the Fiery® controller each have their own IP address. The printer and controller connect to the network independently of each other.
- The Fiery® is not required to be added as a printer.
- The Fiery® device in some configurations is discoverable. If the Fiery® device is in the printer list, the **Administrator** should disable or remove it to conserve the licenses.
- The printer should support all the normal authentication capabilities.
- All the print paths should release the jobs to the alternate IP Address printer which can be a (Fiery®).
- **LPR** protocol is highly recommended when using the **Print to Alternate IP Address** setting.
- DNS name is not supported in the IP Address field.

1. In a Web browser, log in to Xerox® Workplace Suite.
2. Select the **Printers** tab, then select the **Printers** subtab.
3. From the Actions list, select **New**.
4. On the Details tab, for IP Address, type the IP address of the printer.
5. Go to the **Printing to Alternate IP Address** section.
6. Enable the setting, **Print to Alternate IP Address**.
7. Enter the IP address of the Fiery® Controller.
8. For Protocol, select **LPR**.
9. If required, in the Pull Groups area, associate the printer to groups.
10. If required, to add the printer to a site, in the Site Information area, click **Change**, select a site, then click **OK**.
11. Select the **Features** subtab.

    Important: If you have enabled any of the following features in Xerox® Workplace Suite, before you save the new printer in Xerox® Workplace Suite, in the Embedded Web Server, change the printer settings manually for the enabled feature.

    - Authentication for the Print Management feature
    - Alternate Login security feature

- Usage Tracking (Network Accounting) feature

To change the printer settings for these features, log in to the Embedded Web Server for the printer, then follow the steps for each of the features that you have enabled in Xerox® Workplace Suite. For details on how to log in to the Embedded Web Server, refer to the system administrator guide for the printer.

12. If you have enabled the Authentication for the Print Management feature in Xerox® Workplace Suite, before saving the new printer, perform the following steps. To access the authentication for the Print Management feature, select **Features > Workflows > Print Management > Authentication**.
    a. In the Embedded Web Server for the printer, click **Properties > Security > Authentication Configuration**.
    b. For Login Type, select **Xerox Secure Access**.
    c. Click **Apply**.
13. If you have enabled the Alternate Login security feature in Xerox® Workplace Suite, before saving the new printer, perform the following steps. To access the Alternate Login security feature, select **Company > Settings > Policies > Security > Printer Authentication > Basic > Alternate Login**.
    a. In the Embedded Web Server for the printer, click **Properties > Security > Remote Authentication Servers > Xerox Secure Access Settings**.
    b. To enable the Alternate Login Keyboard, for Local Login, select **Enabled**.
    c. Click **Apply**.
14. If you have enabled the Usage Tracking (Network Accounting) feature in Xerox® Workplace Suite, before saving the new printer, perform the following steps. To access the Usage Tracking (Network Accounting), select **Features > Workflows > Printer Client / Usage Tracking > Usage Tracking (Network Accounting)**.
    a. In the Embedded Web Server for the printer, click **Properties > Accounting > Accounting Configuration**.
    b. Enable accounting modes as needed.
    c. Click **Apply**.
15. In Xerox® Workplace Suite, on the **Features** subtab, enable other features as needed.
16. To save the new printer, click **Save**.

TROUBLESHOOTING TIPS

After you add a printer, if an enablement error appears, you can repair the printer. In the Embedded Web Server for the printer, verify that the printer settings are correct for the features that you are using in Xerox® Workplace Suite.

In the Embedded Web Server for the printer, verify that the feature settings are correct for one or more of the following features:

- Authentication for Print Management
- Alternate Login
- Usage Tracking (Network Accounting)

1. If you enabled Authentication for Print Management in Xerox® Workplace Suite, perform the following steps:
    a. Verify that Login Type is set to Xerox Secure Access. In the Embedded Web Server for the printer, click **Properties > Security > Authentication Configuration**.

b. If Login Type is not set to Xerox Secure Access, for Login Type, select **Xerox Secure Access**, then click **Apply**.

2. If you enabled Alternate Login in Xerox® Workplace Suite, perform the following steps:

   a. Verify that Local Login is enabled. In the Embedded Web Server for the printer, click **Properties > Security > Remote Authentication Servers > Xerox Secure Access Settings**.

   b. If Local Login is not enabled, to enable the Alternate Login Keyboard, for Local Login, select **Enabled**, then click **Apply**.

3. If you enabled Usage Tracking (Network Accounting) in Xerox® Workplace Suite, perform the following steps:

   a. Verify that Accounting Type is set to Network Accounting. In the Embedded Web Server for the printer, click **Properties > Accounting > Accounting Configuration**.

   b. If Accounting Type is not set to Network Accounting, for Accounting Type, select **Network Accounting**, then click **Apply**.

4. In Xerox® Workplace Suite, select the **Printers** tab, then select the **Printers** subtab.

5. From the list of printers, select the check box for your printer.

6. From the Actions list, select **Repair**.

Setting Up Desktop Printing with Xerox® PrimeLink® Printers

Note: Before you enable Direct Printing, install the Xerox® PrimeLink® v3 print driver on all servers, including external print servers. You can download the print driver from the Xerox® PrimeLink® support page at http://www.xerox./support.

For the Print Management Desktop Printing feature with Direct Print queues or Follow Print incoming queues, use the required Xerox® PrimeLink® v3 print driver.

Note: Use only the Xerox PrimeLink v3 print driver. Do not use a global print driver or a v4 driver.

Guidelines for enabling Direct Printing for Network Printer and Client Printer

- Ensure that the Xerox® PrimeLink® v3 print driver is installed on all servers, including external print servers.
- During Direct Printing enablement, when the Print Driver selection page appears, select **Manual**, then select the Xerox® PrimeLink® v3 print driver.

Guidelines for enabling Incoming Print Queues

When you create a Pull Print Network Queue or a Pull Print Client Queue, use the Xerox® PrimeLink® v3 print driver.

Server Hostname Change Instructions

This appendix contains:

When you change the Hostname of the server, it can affect many things. Before you change the server Hostname, review the instructions and guidelines. It is recommended to perform this task off hours.

When we refer to the Hostname, it can be the server Hostname for a server that is on or not on a domain. For a server that is on a domain, the Hostname is referred to as the Fully Qualified Domain Name (FQDN) that is made up of the Hostname.domain name. If any part of that name changes after an installation, the change is considered as a server name change. Some examples of server name changes are, adding a server to a domain, changing domains, and changing the server Hostname.

Changing the Hostname of the server can affect the server communication with the Workplace Suite database.

- After a Hostname change, the database connection may be broken and needs to be updated.
- The Workplace Suite database setting is located in a configuration file, this is addressed in the instructions.
- If you are using an external SQL Server Workplace Suite database, you do not need to edit the configuration file. However, the rights to the Database from the new Server Hostname maybe broken because of the identity change. Make sure the new Domain or Server Name has read and write rights to the SQL Database after the Hostname change.
- The identity of the server for database access is DomainName\ServerName$.

Steps to Change Server Name

To change server name, do the following:

1. Change the Hostname of the server. This can include changing the Domain name of the server.
2. Restart your computer.
3. Try to bring up the Workplace Suite Web page.

   If the Workplace Suite administrative Web page appears and you are able to login then you do not need to edit the configuration file.

   If the Workplace Suite administrative Web page fails to start you need to edit the database configuration file.
4. To edit the database configuration file, do the following:
   When you edit the configuration file, it allows Workplace Suite to connect the main database.

   Note: If you are using an external main database, you can skip this section.

   The Database Pointers entry name XeroxMPEntities is the main database point and should be corrected after the hostname

   change or migration to a new server.
   To edit the Main Database entry, do the following:

   a. On the server, go to `<Workplace Suite Install Directory>\Services`.
   b. Make a backup of the file `Xerox.MobilePrint.BULA.Service.exe.Config`.
      To use the new hostname, change the database connection string.
   c. To edit, open the file `Xerox.MobilePrint.BULA.Service.exe.Config`.
   d. Update the database connection string to point to use the new hostname.
   e. In the `<connectionStrings>` section of the file, do the following:
      - Locate the name `XeroxMPEntities`, then change the old Hostname string to the new Hostname.
      - Edit the following string:

```
<connectionStrings>
<add name="XeroxMPEntities"
connectionString="Server=<INSERT NEW HOSTNAME HERE>\XeroxWorkplace;
Database=WorkPlaceSuite;Integrated Security=True;
"providerName="System.Data.SqlClient" />
```

   f. Save the file.
   g. From Windows Services, restart the Xerox Mobile Print Host Service.
      If the Xerox Mobile Print Host Service does not start there is an issue with your connection string that needs to be corrected.
   h. Bring up the Workplace Suite Web administrator page.
   i. Login as an administrator in the Xerox® Workplace Suite Web portal.

   There are other settings you are required to fix in the following sections:
5. If you have enabled **Job Reporting**, fix the job reporting database connection as follows:

Note: The database settings for the job reporting database is fixed on the administrator user interface but not in the configuration file.

a. Select **Company > Settings > Job Reporting**.

b. Take a note of the values in the Database Server and Database Name fields.

c. In the Database Server field, change the value to new hostname.

d. Click **Test Connection**.

6. If Mobile Print Workflow is running, remove the old conversion server. To remove, do the following:

   a. Select **Company > Settings > Conversion Servers**.

      The new server appears automatically in the list. Remove the old conversion server which has old Hostname.

   b. To remove the old conversion server, select the check box next to the old conversion server, then from the Actions menu, click **Delete**.

Note: You should not add the external conversion servers again.

7. To remove the old server from the System Health Dashboard, do the following:

   a. Select **Company > Maintenance > System Health Dashboard**.

   b. Select the old server.

      The **Remove** option appears.

   c. Click **Remove**.

      The old server is removed.

8. If the printers communicate to the server using Hostname, fix the printers as follows:

   a. Select **Company > Policies > Printer**.

   b. In the Details section, if this address is a FQDN then we need to change it to the new FQDN.

   c. Click **Save**.

   d. Select **Printers**.

      The Printers page appears.

      It is recommended you repair one printer then test Workplace Suite features such as Authentication and Workplace Printer EIP Client.

   e. If the test is successful, select the check box at the top of the list.

      All the printers are selected.

   f. From the Actions menu, select **Repair**.

For more information on other settings that affects hostname change, refer to Other Settings that Affect Hostname Change.

Changing the server hostname can effect printer communication to the Workplace server:

- Check for the value in the Server Address field here, select **Company > Policies > Printer**.
- If the server address value is the servers Hostname, then you will have to update this field with the new hostname and repair all the printers. This is addressed in the instructions.
- If the server address value is the Servers IP address, and that is not changing, then you don't have to repair the printers.

Other Settings that Affect Hostname Change

The following features, if enabled, are effected by a host name change: If you are using a User Portal authentication method other than Confirmation Number, it is recommended to change the user portal login to Confirmation Number authentication before you change the servers host name. If you cannot login after the hostname change you can use the Admin Recovery Procedure to login to the User Portal.

- Azure AD authentication: The Azure connection will need to be updated with the new Host Name information or you have the option to remove the current AZURE connection and add it back again. Some of the items that will need to be updated, enter the new hostname and then all of the Platform URI fields need to be updated in Azure.
- SAML authentication: The SAML connection will need to updated or you have the option to remove the current SAML connection and add it back again. Refer to Settings: SAML Connection. Some of the items that will need to be updated, either update the SAML Assertion end point with the new hostname in ADFS, then download the updated Metadata URL from Workplace Cloud SAML configuration web page and apply it in ADFS.
- Mobile Application Setup in Xerox® Workplace Mobile App: Internal Workplace Suite Server Name needs to be updated.

Xerox® V4 Print Driver Support Installation and Configuration

This appendix contains:

Overview

- The V4 solution essentially leverages non-shared V3 queues and LPR port monitors to replace your current V3 Workplace port monitor queues.
- To convert over to V4 incoming print Queues you will need to recreate your current V3 incoming network queues and share the queues out with your end users. The instructions for this process is below.
- Currently only incoming Network Queues are supported using a V4 Driver.

PREREQUISITES

The prerequisites are as follows:

- Xerox V4 driver:
  - Typically, these are drivers that contain the word Class or specifically say V4 such as, Xerox Pull Print Driver V4 PS, and Xerox WorkCentre 7800 Series Class Driver.
  - It is recommended to use the Xerox Pull Print Driver V4 Postscript and PCL Version. Go to this link and search for V4 on the web page.https://www.support.xerox.com/en-us/product/xerox-pull-print-driver/downloads?platform=win10x64&language=en.
- Windows Update infrastructure to support V4 drivers: It is recommended to have the infrastructure set up in the following manner:
  - Print Queue is configured for V4 on print server
  - Clients can connect to the V4 queue and download appropriate driver using Windows Update

Note: If this functionality does not work, drivers download a generic XPS driver and use a server-side rendering. This causes both rendering and performance problems.

INSTALLATION OVERVIEW

Followings are the steps needed to support a V4 driver:

- Create or reuse your existing V3 incoming Network Print Queues.
  - If you are using your existing incoming V3 queues, you should unshared them.
  - The V3 queues will output to the XMP Port monitor.
  - For each V3 queue we recommend you output it to 2 or more XMP Port monitors.
  - Print Pooling will need to be enabled on the V3 queue.
  - We also recommend you create 2 V3 Queues for every V4 queue.
  - The V3 queue will be the LPR incoming print queue for the V4 queue so name the Queue appropriately.
- Create V4 incoming Network queues and share them.
  - The V4 queues will output via LPR printing to the V3 Queues.
  - Print Pooling will need to be enabled on the V4 queue to support output to the multiple V3 queues.
  - Basically the Jobs will be transferred from the V4 Queues to the V3 Queues then to Workplace Suite.
- There will be some configurations steps to link the V3 and V4 queues to Workplace Suite.

Configuration Instructions

The configuration instructions assume familiarity with setting up Xerox Workplace Suite for a V3 incoming Network queue.

SUPPORTED CONFIGURATION FOR V4

The following combination of settings are supported with V4 drivers:

- Follow You server Network queues are supported.
- Direct print queues are not supported.

ENABLING LPD AND LPR PRINT PORT

To support a LPR printer you will need to enable the LPD Service role and enable the LPR port:

1. Open the Service Manager.
2. From the upper-right menu, select **Manage**, then select **Add roles and features**.

   The Add roles and features wizard appears, then the Before You Begin window appears.
3. To move to the Server Roles window, click **Next**.

   The Server Roles page appears.

   By default, the File and Storage Services and the Print and Document Services check boxes are selected.
4. Click and expand Print and Document Services, and enable **LPD Service (Installed)**.
5. Click **Next**, and enable **LPR Port Monitor**.
6. Click **Install**.
7. Go to Service Manager, and verify if the LPD service is running, and it is set to **Automatic**. Ensure the first and second failure are at the very least set to **Restart the Service**. Depending on uptime requirements it is recommended to set Subsequent failures to **Restart the Service**.
8. Increase the number of threads for the LPR service. For more information, refer the following instructions https://docs.microsoft.com/.

Note: By default, the registry key is not present. This limits the number of LPR ports to 11. Setting the registry value to 1 makes the LPD use any port whose number is greater than 1024 to transmit the jobs.

Warning: If Registry Editor is used incorrectly, serious problems can occur that requires you to reinstall your operating system. Xerox cannot guarantee that you or anyone can solve problems resulting from the incorrect use of Registry Editor. Use Registry Editor at your own risk. Before you edit, back up the registry.

9. Start Registry Editor (Regedit.exe) and go to the following key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft \LPDSVC\lpr.
10. Select or Create the LPDSVC key.
11. On the Edit menu, select **Add Key**, then in the Key Name box, type `lpr`.
12. Select the created lpr key. On the Edit menu, select **New then Binary Value**, and then in the New Value dialog box, type the`UseNonRFCSourcePorts` Value Name information.

13. Double-click the name `UseNonRFCSourcePorts` then add the Value Data `01`, then click **OK**.
14. Exit Registry Editor.
15. To read the new Registry Settings, from Services Manager restart Print Spooler Service, LPD server restarts automatically.

CREATING THE V3 SUPPORTING QUEUES

Set up a local V3 printer on the server using the Xerox XMP v3 Port Monitor.

1. From the Start menu, select **Control Panel > Hardware and Sound > Devices and Printers**.
2. Select **Add a printer**.
3. Select **The Printer that I want isn't listed** option.
4. Select **Add a local printer or network printer with manual settings**.
5. Select **Create a new port, then choose in the pulldown Xerox XMP v3 Port Monitor**.
6. Enter a port name.
7. The driver is not important as long as it is a V3 driver, it is recommended to use the V3 Xerox Pull Print Driver or Global Print Driver. For more information, refer to Prerequisites.
8. Select Manufacture and Driver.
9. Name the Printer, take note of the name you will have to point the V4 driver to this printer. The name of the V3 queue is entered as the LPR printer name when you setup the V3 queue.
10. Add additional XMP v3 Port Monitor to the queue. To add an additional XMP v3 Port Monitor to the queue, do the following:
    a. For the V3 printer you just added, select **Printer Properties** on the printer.
    b. Select the **Ports** tab.
    c. Select **Enable printer pooling**.
    d. Select **Add Port** then choose in the dropdown **Xerox XMP v3 Port Monitor**.
    e. Enter a port name. The port will be named XeroxMon_ with your name appended. The Port should be automatically selected.
    f.
11. Repeat these steps and create another V3 Queue.

CREATING THE V4 QUEUE AND LINKING TO THE V3 QUEUES

Set up a local V4 printer on the server and link it to a V3 queue.

1. From the Start menu, select **Control Panel > Hardware and Sound > Devices and Printers**.
2. Select **The Printer that I want isn't listed** option.
3. Select **Add a local printer or network printer with manual settings**.
4. Select **Create a new port, then choose LPR Port in the pulldown**.

5. Enter the IP address or hostname of the local server and the name of the V3 queue created in the previous section.

   Note: 127.0.0.1 or localhost cannot be used.

6. The driver is important, it is recommended to use the V4 Xerox Pull Print Driver.
7. Select Manufacture and Driver.
8. This Queue will be shared so name it appropriately.
9. Add additional V3 LPR ports to the V4 queue. To add an additional V3 LPR ports to the V4 queue:
   a. For the V4 printer you just added, select **Printer Properties** on the printer.
   b. Select the **Ports** tab.
   c. Select **Enable printer pooling**.
   d. Select **Add Port** then choose in the dropdown **LPR Port**.
   e. Enter the IP address or hostname of the local server and the name of the second V3 queue created in the previous section.
   f. Enter the name of the second V3 printer your created.
10. Test and then share the printer.

ENABLING PRINT QUEUE IN XEROX® WORKPLACE SUITE WEB PORTAL

Note: If you make changes to the V4 and V3 Driver, ensure that you disable the Print Queue in Xerox® Workplace Suite, and add the print queue again.

To enable the Print Queue in Xerox® Workplace Suite Web Portal, do the following:

1. In the Xerox® Workplace Suite Web Portal, select the **Print Queues > Incoming Queues** tab.
2. Select the check box next to the appropriate print queue.
3. From the Actions menu, select **Refresh Queues**.
4. To enable the V4 queue, do the following:
   a. Select the check box next to the appropriate V4 queue.
   b. From the Actions menu, select **Enable**.

      The Details page appears.

   c. In the Queue Type - (V3) section, select the radio button for **Pull Print Network Queue**.
   d. In the Conversion Mode section, select the radio button for **Simple**.
   e. Select the **Pull Groups** tab.
   f. From the **Unassociated Groups** field, add the queue to the **Associated Groups** field.
5. To enable the V3 queue, do the following:
   a. Select the check box next to the appropriate V4 queue.
   b. From the Actions menu, select **Enable**.

      The Details page appears.

c. In the Queue Type - (V3) section, select the radio button for **Pull Print Network Queue**.

d. In the Conversion Mode section, select the radio button for **Simple**.

e. Select the **Pull Groups** tab.
Add to same Pull Group as the V4 Queue Pull Group.

f. From the **Unassociated Groups** field, add the queue to the **Associated Groups** field.

SETUP TESTING AND TROUBLESHOOTING

This is the path a V4 print job will take:

- User submits a Print Job to a V4 incoming Queue
- The V4 Print queue uses LPR to send data to local V3 Print queue
- The V3 Print queue uses the Xerox port monitor to intercept data to add the print job to the workplace users account

Setup Testing and Troubleshooting Guidelines

The guidelines for setup, testing and troubleshooting are following:

- Jobs coming through LPR will not contain a domain so it is important to have LDAP domains configured so that XWS can attempt to prepend existing domains to find a user match.
- The LPR queues can be tested with the built-in windows LPR command using a command such as: Lpr -S ip_address_of_server -P queue_name hello.txt, hello.txt is a simple text file.
- It is recommended to use a firewall to disable 515 (LPR) access from outside the server as the LPR communication would only be from the server itself.

Troubleshooting

PROBLEM	SOLUTIONS
Print Job is not forwarded to the V3 Queue.	To diagnose the problem: • From Control Panel, Devices and Printers page, Open the See what Printing window for the corresponding V3 and V4 Queues. • The queues (both V3 and V4) can be paused to see jobs flowing through the queue. • Submit a test job to the V4 Queue. • You should see the Print Job in the V4 Queue window, then it will move to the V3 Driver window. • Then the Job will show in Workplace Jobs Content print jobs list. • If the job is unable to move, check the Queue where the job is stuck.
Print job is not listed in the Jobs Content window.	• Look at the un-registered jobs tab. • If the Job is located there then the solution is not able to match a user name to the Job. • Jobs coming through LPR will not contain a domain so it is important to have LDAP domains configured so that XWS can attempt to prepend existing domains to find a user match.

Xerox® Workplace Suite User Portal

This appendix contains:

Workplace Suite User Portal

ACCESSING THE WORKPLACE SUITE USER PORTAL

To access the Workplace Suite User Portal:

1. Open a Web browser, then type `https://xxx.xxx.xxx.xxx/login`, where `xxx.xxx.xxx.xxx` is the IP address or the hostname for your server.
2. Login to the User Portal.

Note: Refer to Policies: Security > User Portal to set up the authentication mechanism for user to access their personal Web portal.

If Confirmation Number is selected as an authentication mechanism, the user can reset their Confirmation Number, refer to Forgot Confirmation Number to reset it.

USER PORTAL CAPABILITIES

The User Portal has the following Capabilities:

1. Delegation Setup, refer to Delegation.
2. User profile

   After you log in to the Web portal, in the upper right corner, select **User Name > Profile**. The User Profile page appears, where you can view and delete the following information:

   - Details
   - Primary PINs and Access Card Numbers
   - Print Quota
   - Print Limits
   - Single Sign-On Settings

FORGOT CONFIRMATION NUMBER

To reset your Confirmation Number, do the following steps:

1. Enter your `email address`.
2. Select **Forgot Confirmation Number**.

   A Reset Confirmation Number dialogue box appears, Click **OK**.

Note: A Verification Code will be emailed to reset your Confirmation Number. Please check your email inbox. If you do not receive the Verification Code within few minutes, please check your Spam or Junk Folder.

3. Enter the Verification Code and Click **Next**:
   - If you failed to enter the Verification Code within 5 minutes, click **Back** and redo the Forget Confirmation Number process.
   - If you have validate successfully with the Verification Code, a new Confirmation Number will be emailed to you.
4. Enter your new Confirmation Number to login.

USER PROFILE: DETAILS

After you log in to the Web portal, in the upper right corner, select **User Name > Profile**. The User Profile page appears, which shows the following information:

- Email Address
- User Name
- First Name
- Last Name

USER PROFILE: PRIMARY PINS AND ACCESS CARD NUMBERS

This section allows users to view and delete the primary PINs or access card numbers associated to the user account.

Deleting Primary PINs or Access Card Numbers

To delete an existing primary PIN or Access Card Number, do the following:

1. After you log in to the Web portal, in the upper right corner of the screen, click your user name.
2. To access your user profile, click **Profile**.

   The User Profile page appears.
3. In the Primary PINs and Access Card Numbers section, select the check box next to the PIN or access card.
4. From the Actions menu, click **Delete**.

USER PROFILE: PRINT QUOTA

You can access information about Print Quota rules that apply to your user account. For more information, refer to Viewing the User Print Quota Status.

USER PROFILE: PRINT LIMITS

You can access information about Print Limits rules that apply to your user account. For more information, refer to Viewing the User Print Limits Summary.

USER PROFILE: SINGLE SIGN-ON SETTINGS

You can manage your Single Sign-On authentication data for applications installed on your company printers. A grid appears with the following columns:

- App Description
- Single Sign-On Agreement
- Last Modified Date Time

If you click the **Reset** option from the Actions menu, you can delete the stored authentication data for the Apps and reset the Single Sign-On agreement to `Not Accepted`.

Resetting Single Sign-On Settings

To reset Single Sign-On Settings, do the following:

1. After you log in to the Web portal, in the upper right corner of the screen, click your username.
2. To access your user profile, click **Profile**.

   The User Profile page appears.
3. In the Single Sign-On Settings section, select the check box next to the application.
4. From the Actions menu, click **Reset**.

What is New in Xerox® Workplace Suite

This appendix contains:

What is New in Xerox® Workplace Suite

New Features in Version 5.8

- The Mobile and desktop application and IOS/MacOS URI links on the Azure AD connection page **Native Application** tab have been updated.
- The Workplace Suite Forum link has changed to: Workplace Suite - Customer Support Forum.
- The Workplace Suite Announcements link has changed to: Workplace Suite Announcements - Customer Support Forum.
- A new setting called **Confirmation Number Generation After Expiration** has been added under **Enable Confirmation Number Expiration** option in the **Company > Policies > Security > General** tab, which controls when a User will get a new confirmation number generated, after it expires.
- A new section called **Printing to Alternate IP Address** has been added to the **Printers > Edit Printers > Details** tab, this setting allows print jobs to be released to a alternate IP address which can be a Fiery® or another printer.
- A new feature called **Queue Association** has been added to designate which print queue will be used to perform job processing.
- A new authentication method called as **Group Managed Service Account** has been added for SQL access where the Windows operating system manages the password for the account instead of relying on the administrator to manage the password.

New Features in Version 5.7.200

- A new User Role called **Power User** has been added. This role has access privileges more than a **General User**, but not as such of an **Administrator**. The primary feature of the role is to allow users to access all tabs except the **Company** and **Settings** tab.
- New Xerox® Workplace Suite Prerequisite software that supports the Xerox® VersaLink® B625 and C625 Multifunctional Printers.
- The Dashboard **Modify Cost** setting allows you to enter values up to four decimal places.
- **Print Quota** allows you to select **Yearly** option as a quota period to set the allocated Print Quota to start on the first day of the current year until the last day of the year (January 1st to December 31st).
- Ability to **Export License Activation Keys** from **Company > Licensing > License Features History** Actions menu. Only the activation keys that were activated online through the solution web interface (**Activate Online** option) are listed in the exported file.
- Microsoft SQL Server 2022 version is now supported for the customer supplied external Database for the Main and Job Reporting Database.
- The Workplace Suite Load Balancer probe endpoint information is documented in this guide. The information can be used by a Load Balancer, which provides failover by detecting when a Workplace Suite Server is no longer available and routes call to a different Suite Server.
- You can set a LDAP connection to communicate using generic LDAP commands. Microsoft Active Directory is the recommended LDAP connection.
- Workplace Suite Solution will no longer require an external database to be set to Microsoft SQL Server 2014 Compatible Mode.

- Added a new feature called as **Job Processing**, which allows you to search the header of a print file for a customizable set of tag strings and submit the job using the Username from the first match. This feature works with incoming Network queues. Typically, this feature will be used to process print output from a specialized application.
- Workplace Suite Desktop Client has been updated to support accessibility requirements for end users that have vision and physical disabilities using third-party accessibility tools to navigate the UI elements.
- The Workplace Suite Job Reporting Installer has been updated and is only required to use on new installations.

New Features in Version 5.7.1

- Supports the ability to **Include the card number in auto registration email** for Azure AD and SAML authentication. The setting to enable this feature is located in **Company > Policies > Security > Printer Authentication > > Basic > Auto Registration > Azure AD Authentication** and **SAML Authentication**.
- Supports the ability to search the user with Primary PINs and Access Card Numbers on the **Users** tab search field.
- Critical security updates and improvements.

New Features in Version 5.7.000

- Load Balancer Server Addresses on Single Sign-On feature:
  - When a Load Balancer has multiple IP addresses, the Workplace Suite Administrator can enter the multiple IP addresses on the Load Balancer Server Address to allow the user to login with the Single Sign-On credentials.
- Log File Collection Assistant on Maintenance: Logs section:
  - The Log File Collection Assistant at the Maintenance section helps the user to download the log files based on a specific issue type. The user will drive a wizard that generates a zip file of the required log files.
- Workplace Suite Server supports Microsoft Windows® Server 2022.
- Workplace Suite Desktop Client supports Windows® 11.

New Features in Version 5.6.700

Improved security for the users Confirmation Number:

- User can no longer retrieve their Confirmation Number, they can only reset it by a two-step verification process.
- On the User Portal Login Page and Mobile Apps screen the Retrieve Confirmation Number action has changed to Forgot Confirmation Number.
- The user must verify who they are by entering a Verification Code received in their email and then they will receive a new Confirmation Number.
- The setting Custom Confirmation Messages is now called Custom Email Response Messages.
- The Custom Email Response Messages can be customized, but you cannot insert the Confirmation Number in the message.

New Features in Version 5.6.500

Xerox® Workplace Suite software version 5.6.500 has the following feature updates and changes:

- New Xerox® Workplace Suite prerequisite software that supports the Xerox® VersaLink® B71XX and C71XX Multifunction Printers.
- Support for SQL Authentication for SQL server database when installing or upgrading the Xerox® Workplace Suite software.
- Improvements for large Deployments:
  - New Desktop Client software update that supports the new Server Communication Mechanism called TCP/IP, you can find this setting on the server Administration page.
  - Print Server Communication to Xerox® Workplace Suite Server has been improved.
  - Ability to download the Print Server logs from the main Xerox® Workplace Suite server.

New Features in Version 5.6.300

Xerox® Workplace Suite software version 5.6.300 has the following feature updates and changes:

- Ability to schedule Job Reporting to run hourly.
- Support for identity provider SAML authentication.
- New prerequisite software that supports the Xerox® EC80XX Color Multifunction Printer.
- Ability for the user to delete their own PINs and Access Card Numbers.

New Features in Version 5.6.100

Xerox® Workplace Suite software version 5.6.100 has the following feature updates and changes:

- Supports Azure AD authentication.
- On new installations, SQL server 2017 Express is installed for the main database server and job reporting database server.
- Allows resetting of the hardware address in the installation wizard when needed.
- On new installations, IIS settings are enabled automatically.

New Features in Version 5.6

Xerox® Workplace Suite software version 5.6 has the following feature updates and changes:

- Addition of forum and announcements links
- Support fo Guest user onboarding using email
- Ability to add printer session accounting codes to desktop printed jobs
- Support for LDAP import mapping of the network accounting user ID
- Support for local print optimization for Xerox® Workplace Suite Client
- Support for Offline Mode for the Xerox® Workplace Suite Client
- Support for administrator users without an email address
- Support for SQL Server 2017 and SQL Server 2019
- Support for Windows Server 2008 is removed

New Features in Version 5.5

Xerox® Workplace Suite software version 5.5 has the following feature updates and changes:

- Introduction of the Print Limits Rule feature, that limits printing by number of pages in the job.
- New Incoming or Outgoing server type added with support for Microsoft Graph API to access Microsoft Exchange Online
- Job Reporting improvements and additions are as follows:
  - New Dashboards and redesigned Dashboard layout
  - Ability to export dashboard reports to a PDF or .csv file
  - More report filtering options that include filter by User, Department, Printer, Account ID, and Job type
  - Renamed Billing Code to Account ID on the job report raw data
  - New job reporting raw data fields: Printer IP, Site, and User ID
  - New Summary Reports that provide a summary by User, Printer, Department, Account ID, and Accounting: UserID or AccountID
  - Ability to schedule Summary Reports
  - Scanning Cost estimation is added for the Modify Cost reporting feature
  - New Data Retention Policy setting for the Job Reporting data
- New Workplace Suite Prerequisite software includes support for the Xerox® PrimeLink® C9065/C9070 and PrimeLink® B9100/B9110/B9125/B9136 printers, and AltaLink® B8145/B8155/B8170 and AltaLink® C8135/C8145/C8155/C8170 Multifunction Printers
- Installations and upgrades of the Xerox Workplace Suite Server and Workplace Client software now require Microsoft .NET 4.7.2
- Xerox Workplace Suite software support for Windows® Server 2019 environments
- For installations and upgrades, Workplace Suite server no longer supports Microsoft Windows® 7
- New Workplace Suite Client software release contains bug fixes

New Features in Version 5.4

- Support for Windows Integrated Authentication
- Support for Raw TCP Port printing protocol
- Ability to change the Raw TCP port number
- Updated Workplace Suite Client software
- New prerequisite software and a Printer Model update file support Xerox® PrimeLink® C9065/C9070 printers
- Support for Xerox® PrimeLink® C9065/C9070 printers with Fiery® direct configuration

  Note: For details on setup, refer to the *Xerox Workplace Suite Administration and Configuration Guide*.
- Discontinued support for PCL 5

New Features in Version 5.3

- Direct Printing, a Print Management feature that allows desktop printing directly a printer.
- The User Job Limits provide the ability to set print quota rules that control the number of pages a user is permitted to print.
- Support for customer-licensed and installed Microsoft Office 2016 with any Mobile Workflow license.

New Features in Version 5.1

- Support for Multiple Primary PINs and Access Card Numbers for the same user.
- For new installations, the default built-in database software is now MS SQL Express 2014. For existing upgrade solutions that use MS SQLCE, the SQLCE database is retained and used. MS SQL Express 2014 is not installed on existing upgrades.

New Features in Version 5.0

- Content Security Workflow, an updated licensable workflow
- Mobile Print Basic conversion option
- Rules to manage print access
- Web administration role management
- Copy and Scan additions to the Printer Client, for Xerox® AltaLink® printer families
- Copy and Scan additions to the Printer Client, for Xerox® VersaLink® printer families
- Mobile App QR Code and NFC unlock features
- Printer Authentication screen QR Code, for unlocking Xerox® AltaLink® printer families and Xerox® ConnectKey® printer families
- Support for NFC software on ELECTEC TWN4 card readers on Android devices
- Support for TLS 1.2 with any HTTPS communication protocol
- FIPS (Federal Information Processing Standard) support: Available with a new installation, but unsupported as an upgrade
- Mobile Print Opt-out Email Link
- Printer Client icon legacy name support
- Alternate Login option for printer administration
- Character Encoding default setting for each printer

For a new feature list when upgrading from Mobile Print versions 3.5 and 3.6, or PrintSafe version 1.x, refer to the Appendices of the *Upgrade Guide for Print Management and Mobility Suite, Mobile Print, and PrintSafe*, and *Release Content History* information.