

VERSION 5.9.1XX
SEPT 2024
702P09322

Xerox® Workplace Cloud

Administrator Guide

© 2024 Xerox Corporation. All Rights Reserved. Xerox®, Xerox and Design®, VersaLink®, AltaLink®, and Xerox Secure Access Unified ID System® are trademarks of Xerox Corporation in the United States and/or other countries.

Android™ and Chrome™ are trademarks of Google, Inc. in the United States and/or other countries.

Apple®, Mac®, Safari® and Bonjour® are registered trademarks of Apple, Inc. registered in the United States and/or other countries.

Microsoft® Azure AD is a trademark of Microsoft Corporation.

Firefox® is a registered trademark of Mozilla Corporation.

Follow-You Printing® is a registered trademark of Equitrac Corporation.

iOS® is a trademark or registered trademark of Cisco Systems Inc. in the United States and/or other countries.

Adobe® and Acrobat® are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

JavaScript® is a trademark of Oracle Corporation.

Microsoft®, Microsoft® .NET, Windows®, Windows Server®, Windows 10®, Windows Server® 2012 R2, Windows Server® 2016, and Internet Explorer® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Opera® is a trademark of Opera Software ASA.

This product includes software developed by Aspose: <https://www.aspose.com>

Contents

Overview	13
Xerox® Workplace Cloud Overview	14
Xerox® Workplace Cloud Configurations.....	17
Xerox® Workplace Cloud Experience With an Agent	17
Xerox® Workplace Cloud Experience Without an Agent	17
Basic Xerox® Workplace Cloud Experience	17
Xerox® Workplace Cloud Configurations Comparison Chart	18
Xerox® Workplace Cloud Supported Printers	25
Xerox® Workplace Cloud Help	27
Supported Windows PC Browsers for Accessing the Xerox® Workplace Cloud Web Portal.....	28
Supported Macintosh Browsers for Accessing the Xerox® Workplace Cloud Web Portal	29
Supported Operating Systems for Mobile Applications.....	30
Using Xerox® Workplace Cloud	31
Creating a Xerox® Workplace Cloud Company Account	32
Creating a User Account for Xerox® Workplace Cloud.....	34
Verifying Registration of Your Company.....	35
Logging in to Xerox® Workplace Cloud Web Portal With a Different Company Code	36
Viewing the Company You are Logged in to	37
Finding the Company Codes You Have Logged In	38
Changing Your Password on the Xerox® Workplace Cloud Web Portal.....	39
Print	41
Print: Web	42
Printing a Document From the Xerox® Workplace Cloud Web Portal.....	42
Using the Print Options.....	42
Finding the Status of a Printer Using an Agent.....	42
Submitting a Job Using a Web Portal	43
Printing Using a Print Queue on the Web Portal.....	43
Print: Desktop	44
Installing the Xerox® Workplace Cloud Windows Client	44
Installation of the Workplace Cloud Macintosh Client.....	45
Desktop Printing Using Windows Cloud Client.....	46
Desktop Printing Using MAC Cloud Client.....	48
Adding Favorite Printers	49
Print: Email.....	50
Print: Mobile	51
Printing a Document From a Mobile Device.....	51
Reprinting a Document From the Xerox® Workplace Mobile App	51
Jobs	53
Jobs: History.....	54

Viewing the Job Status of the History and Print Tracker.....	54
Jobs: Processing	57
Viewing the Processing Job Status	57
Jobs: Available	58
Viewing the Available Jobs	58
Delete the Uploaded Jobs	58
Jobs: Print Tracker.....	59
Printers	61
Printer Tabs	62
Adding a New Printer	63
Recommended Steps to Add New Printers when using Printer Cloning	63
Enabling a Home Printer on an Existing Company Account When Using an Agent.....	64
Printers Action Menu and Edit Printer Settings Descriptions	65
Change Site.....	65
Print Welcome Page	65
Generate Labels	66
Enable or Disable Printer	66
Enable or Disable Direct Printing.....	66
Making a Printer Private or Public.....	67
Set Accounting Mode	67
Set Client Application Installation Mode	68
Set Authentication Mode	69
Set Direct Email Mode	69
Set Auto Release Mode.....	70
Set Usage Tracking Mode.....	70
Set File Decryption Mode	71
Cloud direct (Manage Printer without an Agent).....	72
Manage Printer using an Agent.....	72
Removing Selected Printers from the Printer List	73
Repair.....	73
Remove	74
Changing the Printer Name	74
Printer Details	74
Editing the IP Address of a Printers.....	75
Serial Number	75
Supported Printer Languages.....	75
Supported Finishers for Desktop Direct Print	75
Setting Protocols	76
Enabling Secure Print.....	77
Printing to Alternate IP Address.....	77
SNMP Settings	78
Printer Groups.....	79
Creating Printer Groups.....	79
Deployment Groups.....	80
General Steps to Deploy Direct Printers on Client Computers Using Deployment Groups.....	80
General Steps to Deploy Pull Print Queues on Client Computers Using Deployment Groups	80

Create Deployment Groups	81
Viewing and Editing the Deployment Group	83
Supported Languages	84
Xerox® Global Print Driver	85
Print Queues	87
Print Queue Enablement	88
Server-Based Print Queues	88
Creating Print Queues	88
Testing the Communication Between Xerox® Workplace Cloud and the Print Queue	88
Changing a Site Associated With a Print Queue	89
Enabling or Disabling a Print Queue	90
Setting Up Accounting for a Print Queue	91
Assigning an Agent to a Print Queue	92
Printing a Welcome Page for a Print Queue	93
Removing a Print Queue	94
Sites	95
Adding a Site	96
Changing the GPS Coordinates of a Site	97
Removing a Site	98
Agents	99
Xerox® Workplace Cloud Agent	100
Agent Description	100
Agents - Best Practices	100
Workplace Cloud Direct	100
System Requirements for the Cloud Agent Software	100
Required Agent Ports	101
Using a Load Balancer With your Agent	102
Failover for Authentication	102
Load Balancer Requirements	103
Installation of an Agent	104
Setting Up a New Agent	104
Configuration and Settings of an Agent	105
Logging the Agent in to the Xerox® Workplace Cloud	105
Agent Settings on Agent Computer	105
Agent Settings on the Cloud Portal	110
User Management	117
Agent Management	119
Upgrading an Agent Manually	119
Knowing When an Agent Needs an Upgrade	119
Updating the Agent on the Web Portal	119
Checking the Version of Your Agent	120
Finding the Agent Code	120

Removing an Agent Affects Printers	120
Switching from Using an Agent to Agentless	120
Users	123
Users	124
User: Details	124
User Actions Menu Options	127
Analyzing Print Quotas - Actions Menu	128
Changing the User Roles	129
Change Department	129
Remove User	130
Generate New PIN	130
User Import	130
Delete Users from File	132
Job Deletion when a User Changes their Home Account	133
User Groups	134
Creating User Groups	134
Account	137
Account: Company Profile	138
Company Profile: Details	138
Company Profile: Contact Information	139
Company Profile: Company Authentication Type	140
Account: Settings	154
Settings: Desktop Printing	154
Settings: Feature Defaults	176
Settings: Home Worker Print Tracker	176
Settings: LDAP Connections	178
Settings: Azure AD Connections	179
Settings: HelloID Connection	185
Settings: SAML Connection	186
Settings: Network Appliances	191
Settings: Performance	197
Settings: Print Defaults	199
Settings: XSM Export	199
Settings: Single Sign-On	201
Settings: Microsoft Universal Print	203
Account: Policies	208
Policies: Print Controls	208
Policies: Data Retention Policy	209
Policies: Encryption	210
Policies: Public Printing	214
Policies: Agent Upgrades	214
Policies: Access Controls	215
Policies: Printer Authentication	216
Policies: Security	225
Policies: Rules	226

Policies: Printer Selection	236
Policies: Offline Mode	237
Policies: Content Security	238
Policies: Client Application	240
Account: Accounting	242
Accounting: Accounting Options	242
Accounting: Accounting Prompts	244
Accounting: Administrative Defaults	246
Accounting: Job Reporting	246
Account: Licensing	249
License Options	249
Activating Xerox® Workplace Cloud Licenses	249
Purchasing More Print Jobs or More Device Licenses	252
Changing a License Type	252
License History	253
Reports	259
Dashboard	260
Summary of the Dashboard Reports	260
Modifying Estimated Cost	261
Job Reporting	262
Viewing Job Reporting Data	262
Exporting Job Reporting Data	262
Schedule the email delivery of Job Reporting Data export	262
Job Reporting Report Field Descriptions	263
User Audit	269
User Activity	270
Export User Activity	270
Troubleshooting	271
Software Installation Issue (Unable to Install Program that is blocked by Windows)	272
Account Issues	273
User Cannot Print to Company Private Printers	273
User Cannot Print to Company Printers	273
Unwanted or Unauthorized Users Print to Company Printers	273
Prompted to Create New Account When Your Account Already Exists	274
Communication Error When Using a Wireless Adapter on a VersaLink Product	274
Why Would a Company Code Need to be Reset?	274
User Type is Blank on the Users Page	274
User List is not Updated When an Account Administrator Removes a User From a Company	
Account	274
User Access Rights Not Updated	274
Account Settings are not Being Saved	274
Windows Messages Display in Mixed Languages	275
Messages Display With Question Marks or Nonrecognizable Characters	275
Agent Issues	276

Agent Communication Issues	276
Agent Icon Not in System Tray.....	276
Received a Print Agent Not Responding Message	276
Unable to Install or Register Agent Software	276
Unable to Upgrade or Uninstall the Agent.....	277
Agent Does Not Upgrade Automatically	277
Printer Search Status Shows “Unable to Communicate with Agent”	277
Received a Print Agent is Not Installed for This Printer Message	277
Xerox® Workplace Cloud Agent Shows as Not Connected on Agent PC	278
Print Agent Installation Failed	278
Discovery on a Subnet Range Takes Too Long	278
Printer is Not Discovered by Agent	279
What Last Discovered Means.....	279
Printers Are Not Discovered After Printer Search Was Initiated on the Web Portal	279
Unable to Delete a Site.....	279
Printer Issues.....	280
Printing Issues.....	280
Unable to Enable Printer	282
Unable to add the Printer Client on a Xerox® AltaLink Printer	282
Company Printers Do Not Display on the Account	282
Documents Do Not Display on the Account.....	283
When Using Open in Function in Apple iOS, Workplace Mobile App Does Not Display as an Option	283
Printer Search Status Shows “Unable to Communicate with Agent”	283
The GPS Coordinates of the Printer Changed.....	283
Job is Not Displayed in the History.....	283
Job Did Not Print as Expected	283
Job Printed 2-Sided Instead of 1-Sided	284
Job Printed in Black and White Instead of Color	284
Unable to Select Color Printing.....	284
Charged For a Blank Email or Blank Attachment.....	284
Printer is Requesting for Paper to be Loaded When it can Substitute	284
Missing Images in Printed Output.....	284
Job Did Not Print With Correct Font	284
Unable to Find Printed Output	285
Direct Email Print Job Fails.....	285
Unable to Find the Printer When Adding the Printer Using the Mobile App.....	285
Unable to See Printer or Print Queue	286
Unable to Print Using Print Queues	286
Job Did Not Print When Accounting is Enabled.....	286
Did Not Receive Job Submission or Job Completion Notification.....	286
Unable to View and Print to Printers That Are Outside the Company.....	287
Printer Model Name Contains Special Characters.....	287
Unable to Find My Public Printers	287
MFP Client Application (@PrintByXerox) Installation Error.....	287
Checking all Available Printers are Discovered	288
@PrintByXerox Icon is not Visible or Displays Question Marks (?) on Printer	288
@PrintByXerox Icon Does Nothing	288
Error When Resetting Password or User ID on the @PrintByXerox App Using an Agent	288

Message States “For Administration, your Home Company Should be set to the Company to Which this Printer is Registered. This Printer is Registered in a Different Company.”	288
Message States “Maximum Number of Printers that you can Enable has Been Reached. To Enable the Printer, Disable a Different Printer or Purchase Additional Printer Licenses.”	289
Unable to Unlock MFP from the Workplace Mobile App Using Cardless or Card Based Authentication	289
Unable to Unlock a Printer Using Alternate Login.....	289
Administration Button Does Not Display in @PrintByXerox App.....	290
@PrintByXerox Print Job Does Not Print.....	290
Authentication Issues.....	291
User Interface Gives me a Message that MFP is not Set Up for Card Authentication	291
Card Authentication is Not Working Correctly	291
I am not Prompted to Swipe My ID Badge	291
I Get an Error Message When I Swipe my ID Badge.....	291
Nothing Happens When I Swipe my ID Badge.....	291
Local User Database is Deleted on Versalink Devices	291
OKTA Authentication on VersaLink devices	291
iOS Native Printing Issues	292
Unable to See the Xerox® Workplace Cloud When Using iOS Native Printing.....	292
User Authorization Fails When Printing Through iOS Native Print.....	292
User Does Not Receive Push Notifications When Printing Through iOS Native Printing.....	293
User Print Job Not Uploading When Printing Through iOS Native Printing	293
Document Printed in a Format That was Not Expected When Printing Through iOS Native Printing.....	293
Printer Appears Offline When Using iOS Native Printing.....	293
New Features Overview	295
New Features for Xerox Workplace Cloud Version 5.9.1	296
New Features for Xerox Workplace Cloud Version 5.8.3.....	297
New Features for Xerox Workplace Cloud Version 5.8.2.....	298
New Features for Xerox Workplace Cloud Version 5.8.1	299
New Features for Xerox® Workplace Cloud Version 5.8.0	300
New Features for Xerox® Workplace Cloud Version 5.7.3.....	301
New Features for Xerox Workplace Cloud Version 5.7	302
New Features for Xerox® Workplace Cloud Version 5.6.1	303
New Features for Xerox® Workplace Cloud Versions 5.5 and 5.6	304
New Features for Xerox® Workplace Cloud Version 5.4.....	305
New Features for Xerox® Workplace Cloud Version 5.3.....	307
Workplace Cloud Direct (Manage Printer without an Agent).....	309
Introduction	310
Printers Supported and Firmware Requirements	311
Methods to Enable the Cloud Direct Feature on a Printer	312
Auto Enablement of Remote Management	312
Manual Enablement of Cloud Direct feature of the Printers on the Workplace Cloud Portal.....	314

Enabling Workplace Cloud Direct Printer using the @PrintByXerox Gallery App (Without using Agent)	316
Enable the VersaLink® Printers as Cloud Direct	317
Switch Cloud Direct Printer to be Managed by an Agent	319
Workplace Cloud Direct Authentication	320
Capabilities of Workplace Cloud Direct Authentication	320
Enable Authentication for Cloud Direct Printers	320
Configuring Workplace Cloud Direct Authentication for Xerox AltaLink B80XX or C80XX Printers	321
Troubleshooting the Workplace Cloud Direct Capability	323
Xerox® Driver Configuration File	325
Xerox Print Driver Configuration Tool	326
Downloading the Xerox Print Driver Configuration Tool User Guide	326
Preparing Xerox® Driver Configuration File	326
Workplace Clients	329
Workplace Client Overview	330
Installation	330
Securing the Xerox® Workplace Cloud Client to an Account	330
Health Check	330
Workplace Windows Client	332
Workplace Macintosh Client	333
Xerox® Workplace Cloud for Mac	333
Xerox® Workplace App for Chrome	335
Workplace App Settings for Google Chrome	336
Uploading the Xerox® Mobile Print Portal App Chrome Configuration File	337
Example 1: Complete Configuration	337
Example 2: A Configuration that Removes Standard and Network Accounting	338
EFI Fiery® Controller	343
Xerox® Workplace Cloud for Xerox® Printers with an EFI Fiery Controller	344
Direct Configuration Setup	344
Network Hub Configuration Setup	345
Setting up the EFI fiery Custom Drivers for Mac Client	347
Enabling the Workplace Cloud Mac Client with the Fiery Controller	347
Setting up the EFI Fiery Custom Drivers for Windows Desktop Client	349
Preparing the Fiery Custom Driver	349
Login Methods Using the Xerox® Workplace Mobile App	351
Logging in to a Printer Using a QR Code	352
Unlocking the Printer Using Native Camera	353
Logging in to a Printer Using Manual Code Entry	354

Logging into the @PrintByXerox App using a QR Code.....	355
Logging in to a Printer Using NFC.....	356
Enabling NFC on Altalink® Devices	356
Enabling NFC on Versalink® Devices	356
Deleting Registered NFC Capable Mobile Devices From My User Profile	357
Configuring Authentication.....	359
Enabling Cardless Authentication and Card Authentication.....	360
Using an ID Card to Unlock a Printer.....	362
Deleting ID Card Information for My User Profile Using the Xerox® Workplace Cloud Web Portal	363
Setting Up the DNS-SD for iOS Native Printing	365
Setting Up the DNS-SD for iOS Native Printing.....	366
Introduction to DNS-SD for iOS Native Printing	366
Configuring the Microsoft® Windows® DNS Server	366
Configuring a BIND Server	370
Configuring a DHCP Server	371
Frequently Asked Questions.....	372
User Profile	373
User Profile: User Profile.....	374
Viewing and Deleting your Registered Cards.....	374
Resetting your Generated PIN.....	375
User Profile: User Preferences.....	376
Configuring Your Email Notification Policy	376
Configuring Your Retention Policy	376
Configuring Your Print Preferences	376
Setting Your Document Release Order	377
User Profile: Single Sign-On	378
Resetting Single Sign-On Settings	378
Remove Workplace Cloud from your Environment	379
Remove Workplace Cloud from your Environment	380

Overview

This chapter contains:

- Xerox® Workplace Cloud Overview..... 14
- Xerox® Workplace Cloud Configurations 17
- Xerox® Workplace Cloud Configurations Comparison Chart..... 18
- Xerox® Workplace Cloud Supported Printers 25
- Xerox® Workplace Cloud Help..... 27
- Supported Windows PC Browsers for Accessing the Xerox® Workplace Cloud Web Portal 28
- Supported Macintosh Browsers for Accessing the Xerox® Workplace Cloud Web Portal..... 29
- Supported Operating Systems for Mobile Applications 30

Xerox® Workplace Cloud Overview

Xerox® Workplace Cloud is a versatile cloud-based virtual print solution designed to accommodate customers with mobile and desktop printing needs. Because it is a cloud-based virtual print solution, Workplace Cloud works across multiple networks, giving you complete control of every printer at every location.

Xerox® Workplace Cloud boosts productivity and control costs, which is easy-to-set-up and use because it is hosted in the cloud, all updates and patches are managed by Xerox. This frees up your IT resources allowing them to concentrate on your core business.

- Workplace Cloud supports the following printing methods:
 - **Desktop**
 - Desktop Printing is a offering that replaces the traditional print infrastructure with a virtualized technology. It includes a common end-user solution that incorporates Desktop Printing Direct Print with immediate release and Follow you Pull printing models in a new modern approach to printing.
 - Provides native desktop printing (**File > Print**) with Windows® and Mac® OS. Our desktop clients enable job submission over the internet or local network and can be optimized for print speed.
 - Pull printing allows you to submit your jobs to a secure queue from any PC or mobile device. Once you have authenticated at a networked printer of your choice, you can then view, select, print, modify job settings, and delete jobs.
 - Desktop printing supports using the Xerox GPD, Xerox and third party printer Drivers by using the Custom Driver and Print Queue Conductor (Composer Files) features.
 - **Mobile App**
 - Xerox® Workplace Mobile App enables printing for iOS and Android™.
 - Once you have authenticated on the Mobile App, you can then view, select, print, modify job settings, and delete jobs.
 - Mobile App supports printer unlocking and authentication using Mobile unlock: QR Code, NFC Tap, and Unlock Code.
 - Mobile App supports logging into the @PrintByXerox App using a QR Code.
 - **Web**
 - Print from a Cloud Web Portal at <https://xwc.services.xerox.com/>.
 - Once you have authenticated on the Cloud Web Portal, you can then view, select, print, modify job settings, and delete jobs.
 - **Email**
 - Use email direct printing by forwarding an email and attachments directly to the specific Cloud email address of a Cloud enabled printer. Contact your administrator for the email address of your printer.
 - Forward an email with attachments to print@printbyxerox.com. The email and attachments are available to print from the @PrintByXerox printer App of your Xerox® Workplace Cloud-enabled multifunction printer, where you can select and print your documents.
- **Authentication and Access Control**

- Xerox® Workplace Cloud provides flexible authentication options to unlock your printer, securely release your pull print jobs, and access your multifunction printer (MFP) Apps.
- Supports PIN-only, express code, or user name and password authentication as an alternate login.
- Supports a card-based reader authentication option that is compatible with a wide range of industry-standard secure readers and cards.
- Integrates with Microsoft® Active Directory LDAP, Azure AD, OKTA, SAML, and HelloID authentication.
- Single sign-on capability allows access to SSO-enabled Xerox® AltaLink and VersaLink device Apps. Conveniently authenticate at the printer once, then securely access all your MFP SSO-enabled Apps without having to remember long passwords or perform any additional time-consuming login steps.
- Workplace Cloud supports various types of rules such as:
 - **Print Controls:** Controls printer access for Users and User Groups, Printer and Printer Groups including Printing Attributes.
 - **Print Quotas:** Controls and restricts the total number of pages that a User can print over a defined period.
 - **Print Limits:** Restricts the number of pages that all Users or User Groups can print in a single job.

Reporting: When Job Reporting is enabled, the Xerox® Workplace Cloud solution will report on job activity of the printers which have been enabled in Workplace Cloud. If a Xerox printer is enabled for Usage Tracking (Network Accounting), the solution will collect job reporting data directly from the Printer and combine the data into one report.

- Support Xerox Network Accounting: Workplace Cloud collects Usage Tracking (Networking Accounting) data directly from the Printer for job types supported by network accounting.
- Dashboard: The Xerox® Workplace Cloud job reporting dashboard provides predefined summary information for customers who use the reporting capability of Workplace Cloud.

The Dashboard provides the following reports:

- ◆ Print Summary
- ◆ Cost Savings
- ◆ Paper Summary
- ◆ Most Used Printers
- ◆ Least Used Printers
- ◆ Top Users
- ◆ Top Departments
- Job Reporting: The Job report contains combined data from Workplace Cloud job data and Network Accounting data retrieved from the printer. The Usage tracking feature must be enabled on the Cloud printer to retrieve Network Accounting data.
- Workplace Analytics: The four levels of Workplace Analytics are device, user, document and process. It reveals the insights available for each one and how they can be used to make your employees more productive and your workplace more efficient and secure.
- User Audits and User Activity: User Audit tracks Web portal login, Client login, Mobile App login, Web Portal New User Registration, and Alternate login with credentials whereas, User Activity tracks and update the

status of print authentication, new card registrations, custom email onboarding message, scheduled job reporting export and license activation.

- The Content security feature safeguards against data or intellectual property loss by searching all documents printed either in the office or home location using a specific administrator-defined term or text string (for example, confidential or internal use only and so on). If a match is found, an alert along with the job details and content will be sent to the administrator for follow-up.

Xerox® Workplace Cloud Configurations

Xerox® Workplace Cloud has three configurations to fit requirements of the users.

- The full Xerox® Workplace Cloud experience enables all features of the solution, including the @PrintByXerox app on Xerox® AltaLink® and VersaLink® multifunction printers. The features are available with or without an Agent. How you set up your account determines what functionality is available to you. Some features, such as printing to non-Xerox devices, require an agent.
- The Basic Xerox® Workplace Cloud experience enables an email to the Xerox® Workplace Cloud with pull-print workflow from the app on Xerox® AltaLink® and VersaLink® multifunction printers.

The details on each configuration are as follows:

XEROX® WORKPLACE CLOUD EXPERIENCE WITH AN AGENT

The presence of the agent enables discovery of printers so there is central management of your printers. Since the Agent communicates to the Xerox® Workplace Cloud, your printers do not need to be exposed outside of your company. There is no need to set the printer proxy when discovering printers with an agent. Setting the Agent proxy, however, is required.

To enable the pull-print workflow, the @PrintByXerox printer app is installed remotely by the Agent using the Xerox® Workplace Cloud Web Portal, or using the Xerox® App Gallery, if available.

For more details, refer to [Xerox® Workplace Cloud Configurations Comparison Chart](#). For more information on Installation and Configuration of the Agent, refer to [Agents](#). To add an agentless printer, refer to [Workplace Cloud Direct \(Manage Printer without an Agent\)](#).

XEROX® WORKPLACE CLOUD EXPERIENCE WITHOUT AN AGENT

For users who desire a solution with less infrastructure, and are using the latest generation of Xerox® AltaLink® and VersaLink® devices only, there is an option to run entirely in the cloud.

For more details, refer to [Xerox® Workplace Cloud Configurations Comparison Chart](#) and refer to [Workplace Cloud Direct \(Manage Printer without an Agent\)](#).

BASIC XEROX® WORKPLACE CLOUD EXPERIENCE

For companies with the latest generation of Xerox MFPs who have no need for anything other than simple, email-based submission, an @PrintByXerox AltaLink® and VersaLink® printer app is available via the Xerox® App Gallery.

There is no company account to create or manage, and no license necessary. The single workflow is email submission to cloud with pull-print from the AltaLink® and VersaLink® App. The user enters their email address or login ID, followed by a password to access the @PrintByXerox app.

For more details, refer to [Xerox® Workplace Cloud Configurations Comparison Chart](#).

Xerox® Workplace Cloud Configurations Comparison Chart

FUNCTIONS	LICENSED ACCOUNTS THAT USE AGENT	LICENSED ACCOUNTS THAT DO NOT USE AGENTS	UNLICENSED ACCOUNTS USING THE XEROX® ALTALINK® AND VERSALINK® APP. AGENT NOT SUPPORTED
Must create a company account	Yes	Yes	No
Licensed	Yes	Yes	No
Company account management	Xerox® Workplace Cloud Web Portal	Xerox® Workplace Cloud Web Portal	No
Xerox Technical Support by telephone	Yes	Yes	No




CONFIGURATION	LICENSED ACCOUNTS THAT USE AGENT	LICENSED ACCOUNTS THAT DO NOT USE AGENTS	UNLICENSED ACCOUNTS USING THE XEROX® ALTALINK® AND VERSALINK® APP. AGENT NOT SUPPORTED
Workplace Cloud Agent needed and installed within the company network	Yes	No	No
Printer management enabling and configuration	Xerox® Workplace Cloud Web Portal	Initially, connect to a company at each Xerox® @PrintByXerox app multifunction device. Subsequent management can be performed at the Xerox device or Xerox® Workplace Cloud Web Portal. Refer to Workplace Cloud Direct (Manage Printer without an Agent) .	No
Printers can be made public	Yes	Yes	No
Xerox Standard Accounting or Xerox Network Accounting	Yes. If Xerox Standard Accounting or Xerox Network Accounting are enabled at the printer, before accessing the	Yes. If Xerox Standard Accounting or Xerox Network Accounting is enabled at the printer, before accessing the	Yes. If Xerox Standard Accounting or Xerox Network Accounting is enabled at the printer, before accessing the app,



CONFIGURATION	LICENSED ACCOUNTS THAT USE AGENT	LICENSED ACCOUNTS THAT DO NOT USE AGENTS	UNLICENSED ACCOUNTS USING THE XEROX® ALTALINK® AND VERSALINK® APP. AGENT NOT SUPPORTED
	app, users are required to enter login credentials. The credentials are used for any job submitted from the app.	app, users are required to enter login credentials. The credentials are used for any job submitted from the app.	users are required to enter login credentials. The credentials are used for any job submitted from the app.
Third-party print queues, for example, Equitrac	Yes	No	No
User management, can restrict access	Yes	Yes	No
Workplace Cloud client for Windows	Yes	Yes	No
Workplace Cloud client for Mac	Yes	Yes	No
Network Queues, LPR	Yes	No	No
Xerox printers @PrintByXerox application installation	Xerox® Workplace Cloud web portal	Xerox App Gallery	Xerox App Gallery
Printer connectivity	Internet: Company network only if not using EIP at the Xerox® device	Internet*	Internet*



FEATURE	LICENSED ACCOUNTS THAT USE AGENT	LICENSED ACCOUNTS THAT DO NOT USE AGENTS	UNLICENSED ACCOUNTS USING THE XEROX® ALTALINK® AND VERSALINK® APP. AGENT NOT SUPPORTED
Secure Print	Yes	Yes, refer to Workplace Cloud Direct (Manage Printer without an Agent) .	No. Secure Print is not needed. To print your jobs, log in to the Xerox® VersaLink®, Primelink or AltaLink® app.
Print Quotas	Yes	Yes	No


FEATURE	LICENSED ACCOUNTS THAT USE AGENT	LICENSED ACCOUNTS THAT DO NOT USE AGENTS	UNLICENSED ACCOUNTS USING THE XEROX® ALTALINK® AND VERSALINK® APP. AGENT NOT SUPPORTED
Content Security	Yes	Yes	No
Single Sign-On	Yes	No	No
Home Worker	Yes	Yes	No
Print later using email or from an upload to the Workplace Mobile App	Xerox® EIP-enabled printers	Xerox® VersaLink®, Primelink, and AltaLink® printers	Xerox® VersaLink®, Primelink, and AltaLink® printers
File Encryption/Decryption	Yes	Only Altalink® printers with latest Firmware	No
Job Order	Yes	Yes	No
Alternate IP printing Fiery Support.	Yes	No	No

AUTHENTICATION	LICENSED ACCOUNTS THAT USE AGENT	LICENSED ACCOUNTS THAT DO NOT USE AGENTS	UNLICENSED ACCOUNTS USING THE XEROX® ALTALINK® AND VERSALINK® APP. AGENT NOT SUPPORTED
Convenience Authentication using the Workplace App	Xerox® EIP-enabled printers	No.	No
Convenience Authentication using the Alternate Login, Cloud authentication, or LDAP Credentials	Xerox® EIP-enabled printers	Yes, refer to Workplace Cloud Direct (Manage Printer without an Agent) .	No

AUTHENTICATION	LICENSED ACCOUNTS THAT USE AGENT	LICENSED ACCOUNTS THAT DO NOT USE AGENTS	UNLICENSED ACCOUNTS USING THE XEROX® ALTALINK® AND VERSALINK® APP. AGENT NOT SUPPORTED
		 Note: Only Altalink® printers with latest Firmware supports agentless authentication	
Card Authentication	Xerox® EIP-enabled printers	Yes, refer to Workplace Cloud Direct (Manage Printer without an Agent) .  Note: Only Altalink® printers with latest Firmware supports agentless authentication	No
Auto Release using Authentication	Xerox® EIP-enabled printers	Yes, refer to Workplace Cloud Direct (Manage Printer without an Agent) .  Note: Only Altalink® printers with latest Firmware supports agentless authentication	No
Auto Release using a network appliance	Only works with an Agent and requires a special license	No	No
LDAP synchronization	Yes	No	No
PIN authentication	Yes	Yes, refer to Workplace Cloud Direct (Manage Printer without an Agent) .	No

AUTHENTICATION	LICENSED ACCOUNTS THAT USE AGENT	LICENSED ACCOUNTS THAT DO NOT USE AGENTS	UNLICENSED ACCOUNTS USING THE XEROX® ALTALINK® AND VERSALINK® APP. AGENT NOT SUPPORTED
		 Note: Only Altalink® printers with latest Firmware supports agentless authentication	
QR Code Authentication	Yes	No	No
Blocking Machine Access	Yes	Yes, refer to Workplace Cloud Direct (Manage Printer without an Agent) .	No
On boarding – Alternate Login and Badge registration	Yes	 Note: Only Altalink® printers with latest Firmware supports agentless authentication	No

PRINTING CAPABILITIES	LICENSED ACCOUNTS THAT USE AGENT	LICENSED ACCOUNTS THAT DO NOT USE AGENTS	UNLICENSED ACCOUNTS USING THE XEROX® ALTALINK® AND VERSALINK® APP. AGENT NOT SUPPORTED
Print now using the Workplace Mobile App	Xerox® and non-Xerox	<p>For VersaLink® or AltaLink® printers with older firmware the printer has to support Gallery App. The job is held and not sent directly to the device. To print the job, log in to the @PrintByXerox EIP App.</p> <p> Note: Only Atalink® printers with latest firmware supports direct printing.</p>	No
Print from the Xerox® Workplace Cloud Web portal	Xerox® and non-Xerox	<p>For VersaLink® or AltaLink® printers with older firmware the printer has to support Gallery App. The job is held and not sent directly to the device. To print the job, log in to the @PrintByXerox EIP App.</p> <p> Note: Only Atalink® printers with latest firmware supports direct printing.</p>	No
Direct to your Xerox® device Workplace Cloud email address	Xerox® and non-Xerox	<p>For VersaLink® or AltaLink® printers with older firmware the printer has to support Gallery App. The job is held and not sent directly to the device. To print the job, log in to the @PrintByXerox EIP App.</p>	No

PRINTING CAPABILITIES	LICENSED ACCOUNTS THAT USE AGENT	LICENSED ACCOUNTS THAT DO NOT USE AGENTS	UNLICENSED ACCOUNTS USING THE XEROX® ALTALINK® AND VERSALINK® APP. AGENT NOT SUPPORTED
		 Note: Only Atalink® printers with latest firmware supports direct printing.	

Xerox® Workplace Cloud Supported Printers

Xerox Multifunction / All-in-One Laser Printers

- AltaLink® B8000 Series
- AltaLink® B8100 Series
- AltaLink® B8245/B8255/B8270
- AltaLink® C8000 Series
- AltaLink® C8100 Series
- AltaLink® C8230/C8235/C8245/C8255/C8270
- VersaLink® B405
- VersaLink® B415/C415
- VersaLink® B605/B615
- VersaLink® B620
- VersaLink® B625
- VersaLink® B7000 Series
- VersaLink® B7100 Series
- VersaLink® C405
- VersaLink® C505
- VersaLink® C605
- VersaLink® C620
- VersaLink® C625
- VersaLink® C7000 Series
- VersaLink® C7100 Series
- WorkCentre® 3655i
- WorkCentre® 5800i Series
- WorkCentre® 5900i Series
- WorkCentre® 6655i
- WorkCentre® 7200i Series
- WorkCentre® 7800i Series
- WorkCentre® 7970i
- WorkCentre® EC7800 Series
- Xerox® Color C60/C70
- Xerox® EC8000 Series
- Xerox® PrimeLink® B9100 Series
- Xerox® PrimeLink® C9065/C9070 Printer

Office Printers

- VersaLink® B400
- VersaLink® B600/B610
- VersaLink® C400
- VersaLink® C500
- VersaLink® C600
- VersaLink® C7000
- VersaLink® C8000
- VersaLink® C8000W
- VersaLink® C9000

Xerox Digital Printing Press Portfolio

- Xerox® Color C60/C70
- Xerox® PrimeLink® B9100 Series
- Xerox® PrimeLink® C9065/C9070 Printer

For a current list of Xerox® AltaLink® and VersaLink® MFPs, refer to <http://www.office.xerox.com/software-solutions/xerox-workplace-cloud/enus.html>.

Proxy must be set at the Multifunction Printer if it is behind a firewall.



Note: If you plan to install the EIP App, enable and configure the Extensible Services Proxy settings on the printer. The @PrintByXerox app requires access to the Internet. This can mean the user needs to configure proxy access. It depends on your environment.

Xerox® Workplace Cloud Help

For more help and information using the Xerox® Workplace Cloud:

1. Workplace Cloud Announcements: [Workplace Cloud - Announcements](#).
2. Workplace Cloud forum: [Workplace Cloud - Customer Support Forum](#).
3. Workplace Mobile App forum: [Workplace Cloud - Customer Support Forum](#).
4. To access Cloud Knowledge base, type in your question, go to [Workplace Cloud - Product Support](#).
5. To access Cloud Documentation, all Guides, go to [Workplace Cloud - Documentation Download](#).

Supported Windows PC Browsers for Accessing the Xerox® Workplace Cloud Web Portal

Supported PC browsers include:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox



Note: JavaScript must be installed.



Note: Web Portal access is not supported on mobile devices.

Supported Macintosh Browsers for Accessing the Xerox® Workplace Cloud Web Portal

Supported Macintosh browsers include:

- Google Chrome
- Mozilla Firefox



Note: JavaScript must be installed.



Note: Web Portal access is not supported on mobile devices.

Unsupported Macintosh browsers include:

- Apple Safari
- Opera

Supported Operating Systems for Mobile Applications

- iOS version 13.0 and higher
- Android version 6.0 and higher



Note: Web Portal access is not supported on mobile devices.

Using Xerox® Workplace Cloud

This chapter contains:

- Creating a Xerox® Workplace Cloud Company Account.....32
- Creating a User Account for Xerox® Workplace Cloud34
- Verifying Registration of Your Company35
- Logging in to Xerox® Workplace Cloud Web Portal With a Different Company Code36
- Viewing the Company You are Logged in to.....37
- Finding the Company Codes You Have Logged In38
- Changing Your Password on the Xerox® Workplace Cloud Web Portal.....39

Creating a Xerox® Workplace Cloud Company Account



Note: Ensure that you create a company account using the Workplace Cloud web application. It cannot be created using mobile device.

Guidelines:

- A user can Change Company using **Change Company** option on the login page of the Workplace Cloud portal and re-home themselves to another company.
- A user can only be homed or active in one Cloud Company.
- A printer can only be enabled in one Cloud Company.
- If a user is logged into the workplace Cloud and clicks on their email address in the upper right corner of the website, the **My Companies** section will list all the associated companies for that user.

1. Go to <https://xwc.services.xerox.com>.
2. Click **Create Company Account**.
3. If you have an existing Workplace Cloud User Account, enter the email address of that account. If not, enter an email address and click **Submit**.
4. Enter your email password. If you are a new user, reset the password, a verification mail will be sent with the verification code, enter the code and reset the password and click **Submit**.

Get Started page appears.

5. Select the storage location for your Company information. Company information includes details regarding users, printers, sites, configuration settings, and reporting data. Choose the location which makes the most sense for your business. Be sure to consider any data residency policies that your company or government may require when deciding between the provided options.



Important: This choice is permanent and can not be modified in future.

- **European Union (EU)** (Default).
 - **United Kingdom (UK)**.
6. Click **Next**.
 7. Select the storage location for your documents. If your print jobs contain sensitive information and you have concerns about where that data will be stored, then select the storage location that aligns with your company information storage location. This could impact performance when releasing jobs if the storage location is geographically far from the printer.

If you do not have concerns about where your documents are stored, or if performance is more important than the storage location, then select **Optimized for Performance** option. This uses the location of the end user to decide where a document will be stored. The documents will reside in one of following locations: EU, UK, or US. Be sure to consider any data residency policies that your company or government may require when deciding between the provided options.

- **Optimized for Performance (based on location)**
 - **Always use the European Union (EU) or United Kingdom (UK)**
8. Click **Next**.

9. Provide the following information about your Company and click **Submit**.



Note: You can also add these information after creating your Company account.

- Company Name
- Country
- Address:
 - Country
 - City
 - State/Province
- Postal Code
- Contact Email
- Contact Email Language

Xerox Workplace Cloud Terms of Service Agreement page appears.

10. Read the **Xerox Workplace Cloud Terms of Service Agreement** and click **I Agree**.

A Workplace Cloud Company account is created.



Note: After you create a company account, the existing or new user with the entered email address is the account administrator.

11. Follow the instructions provided on the landing page to set up your Workplace Cloud Company account.
12. Download and install the Xerox® Workplace Cloud Agent. Printers on the same subnet as the Agent PC are identified, and one site is created, automatically.
As needed, you can add more subnets and sites later.
13. Enable one or more printers.

The system is now ready for users to print.



Note: If you are a service provider, or an administrator who creates multiple Xerox® Workplace Cloud companies, it is highly recommended that you use a service account and service email address specific to each company that you created.

Creating a User Account for Xerox® Workplace Cloud

This section describes creating a user account for a company that already exists.

- Go to <https://xwc.services.xerox.com>.
- Click **Create User Account**, then follow the instructions on screen.
- Enter an email address where you can receive email, and click **Submit**.
- Follow the rest of the instructions on the screen and in any emails you receive from the progress.



Note: To complete these steps, you need to acquire a company code from your account administrator. When you complete, as all users are created with General User permissions.

- If the users need an elevated permissions, it is recommended to contact an account administrator.

Verifying Registration of Your Company

1. Go to <https://xwc.services.xerox.com>, and log in as a user who created the Workplace Cloud Company Account
2. Select the **Account** tab and then select **Company Profile**.
3. Verify the **Details** correctly list your Company Name, Company Code, and Contact Information.
4. Record the Company Code for the account. This code is required to onboard more users.

Logging in to Xerox® Workplace Cloud Web Portal With a Different Company Code

1. Log out from the Xerox® Workplace Cloud Web Portal.
2. Go to the login page at <https://xwc.services.xerox.com> and select the **Change Company** check box.
This will prompt for the company code when you log in. You will receive a verification email that includes an authorization code.
3. Log in to the Xerox® Workplace Cloud Web Portal and enter the authorization code to complete the company change process.

Viewing the Company You are Logged in to

The company you are logged into is shown in the upper right corner of the Xerox® Workplace Cloud Web Portal.

Finding the Company Codes You Have Logged In



Note: Finding the company code is not available in the Workplace Mobile App. For more information, refer to [Login Methods Using the Xerox® Workplace Mobile App](#).

1. From the Xerox® Workplace Cloud Web Portal, click your email address in the upper right corner of the screen.
2. Select **User Profile** under User Options. The company codes you have used are listed under **My Companies**.

Changing Your Password on the Xerox® Workplace Cloud Web Portal



Note: This applies only to the accounts with Cloud Authentication enabled.

1. From the login screen of the Xerox® Workplace Cloud Web Portal, enter your email address and click **Submit**.
2. On the password page, select **Reset Password**.
3. Check your email for a temporary password.
4. Enter the temporary password on the Web Portal.



Note: The temporary password that is issued is valid for 24 hours after it is requested.

5. Create a new password and select **Submit**.



Note: Ensure that the passwords contains at least eight characters and have one uppercase alpha character and one numeric character.

Print

This chapter contains:

Print: Web.....	42
Print: Desktop.....	44
Print: Email	50
Print: Mobile.....	51

Print: Web

PRINTING A DOCUMENT FROM THE XEROX® WORKPLACE CLOUD WEB PORTAL

1. Log in to Xerox® Workplace Cloud using credentials.
2. Click **Print > Web > Print Document > Select File**.
3. Browse to the desired file.
4. Select a printer or print queue and job options.
5. If required, enter accounting information or a Secure Print passcode.
6. Select **Print**.

USING THE PRINT OPTIONS

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.

Page Range

You can select a page range for some file types. An example of the page range options is given for the selected file type.



Note: When printing from a mobile device, selecting a small page range from a large document does not save data charges.

Media Size

Xerox® Workplace Cloud supports scaling of documents to fit an available paper size. The page size is determined by the first page of the document. This is the paper size that will be used for printing. Specific paper sizes are listed according to the capabilities of the selected printer. Selecting a specific paper size will scale your document to fit on that paper size.

Auto Scale: The document will be scaled to fit on the available paper size that is closest to the size specified in the document file. This option is available only if Paper Substitution is enabled in the company account you are connected to.

Original File Size: No scaling. The document will print on the paper size that corresponds to the size specified in the file.



Note: The Original Size selection overrides scaling. If the printer does not have the proper size paper loaded, the job will be held until the paper is replenished.

FINDING THE STATUS OF A PRINTER USING AN AGENT

To see the status of a printer:

1. From the Web Portal, select the **Print** tab.

2. Select a printer from the list.

The printer status is indicated by a small colored icon at the bottom of the icon representing the selected printer.

- Red: The printer may not be available, for example paper jam. Check the printer.
- Yellow: The printer is available, but may need intervention soon, for example low supplies.
- Green: The printer is available and ready.
- Grey: The status of the printer is unknown.

3. Move the cursor over the status icon for more information.

4. Printer status also displays in the mobile app for favorite printers such as iOS and Android only:



Note: The printer status is available on the **Printers** tab:

- Select **Edit** for the printer you wish to see. The printer status is in the upper left of the Web Portal below the IP address of the printer.
- Move the cursor over the status icon for more information.

SUBMITTING A JOB USING A WEB PORTAL

To push a job directly to the device through a Web portal, perform the following steps:

1. Log in as an administrator.
2. Select **Print > Web**.
3. Choose a file, then select a printer.
4. Click **Print**.

Your job is submitted to the device through the Web portal.

PRINTING USING A PRINT QUEUE ON THE WEB PORTAL

1. From the Web Portal, select the **Print** tab.
2. Select **Browse** and navigate to your file.
3. Select a print queue.
Unique icons are used to differentiate Printer icons from Print Queue icons.
4. Select your print options and click **Print**.

Print: Desktop

Desktop printing allows you to download and install the Xerox Workplace Cloud Client to enable sending print jobs from your computer using the native **File > Print** workflow within desktop applications. Once the client is installed, you can add both pull print and direct printers to your desktop. You can then submit print jobs from anywhere, even outside the company firewall.

Guidelines:

- You can manually install Direct Printers and Pull Print Queues on your Windows or Mac Client Computer using **Print > Desktop** section.
- If a Pull Print Queue is set as a **Default Printer** during creation, the Queue will be automatically installed on your Windows or Mac Client Computer using Workplace Cloud Client.
- To automatically deploy Direct Printers and Pull Print Queues on your Windows Computer, refer to [Deployment Groups](#) section.
- To automatically deploy Pull Print Queues on your Windows and Mac Client Computer, refer to [Deployment Groups](#) section.



Note: You cannot Deploy Direct Printers to Mac Client using Deployment Groups.

INSTALLING THE XEROX® WORKPLACE CLOUD WINDOWS CLIENT

Before you can install a generic printer, install the Xerox® Workplace Cloud Client. The installation allows users to enable printers for Desktop Printing, without administrator access. Refer to the notification area.

1. Select **Account > Settings > Desktop Printing**.
2. Select **Xerox® Workplace Cloud**. A message appears asking if you want to Run or Save the `XPMMSClientInstaller.exe`. Click **Run**. The system runs a security scan. When prompted with a message asking if you give the system permission to access your PC, click **Yes**.
3. If the Wizard does not appear, on your PC, click **View Downloads**.
4. The Xerox® Setup Wizard appears.
5. Select the language you want to use during installation, then click **Ok**.
6. The splash screen appears.
7. The Welcome screen appears. Click **Next**.
8. The License agreement screen appears. Review the license agreement, then click **I accept the terms in the license agreement**. Click **Next**.
9. The Ready to Install screen appears. Click **Install**. The Installation begins.
10. When the wizard is complete, select **Finish**.
11. An icon appears in the notification tray. To view the name, hover the mouse cursor over the icon.

12. To view the options, right-click the icon. The options appear:

- **Sign In**
- **Sign Out**
- **Add Printer**
- **About**
- **Exit**



Note: Users are required to log in every 24 hours.

13. Click **Login to Xerox® Workplace Cloud**. A login screen appears. Enter your email address and password. Use the same login credentials that you used for your initial login.



Note: To view the version number of the Xerox® Workplace Cloud Client, click **About**.

14. Click **Add Printer**.

15. To return to the Print Desktop page, select **Print > Desktop**. For information about adding a generic printer, refer to [Enabling the Install Xerox® Generic Printer by Default..](#)

INSTALLATION OF THE WORKPLACE CLOUD MACINTOSH CLIENT



Note: Before you install Macintosh Workplace Cloud Client, ensure that the Xerox Macintosh Print and Scan driver or third-party driver is installed on all the Macintosh workstations. The Cloud Mac Client does not automatically install drivers. After installation, the Mac Client is operated from the Macintosh status bar.

To download and run the Mac Client installation package:

1. Log in to the Xerox Workplace Cloud Web Portal at <https://xwc.services.xerox.com>.
2. To obtain to the required installation package, choose one of the following options:
 - For a version of the Client that is pre-configured with user credentials for the logged in user, select **Print > Desktop**. Then, to download the installation package to your browser default download location, in the Install the Workplace Client section, click **Mac**.
 - For a version of the Client that is not pre-configured with user credentials, select **Account > Settings > Desktop Printing > General** tab. To download the installation package to your browser default download location, in the Install the Workplace Client section, click **Xerox Workplace Cloud Client..**

The **XeroxWorkplaceCloudClient.pkg** file downloads automatically to your browser default download location.

3. To run the installer, locate the file and click it.

The Xerox Workplace Cloud Client Installer window appears.

4. To continue the installation process, click **Continue**.

The Readme window appears, displaying additional information about the Mac Client.



Note: To print the Readme, click **Print**, or to save the Readme as a .txt file, click **Save**.

5. To continue the installation, click **Continue**.

The Software License Agreement window appears.

6. Read the license terms. To accept the terms and continue the installation, click **Continue**, then click **Agree**.

The Destination Select window appears, and the default installation location displays.



Note: To change the location of the installation, click **Change Install Location**, then select the required destination.

7. To continue the installation process, click **Install**.

A security dialog box appears.

8. To begin the installation, enter the Macintosh administrator password, then click **Install Software**.

A status progress bar appears.



Note: It can take several minutes for the installation to complete.

9. When the installation finishes successfully, a message appears confirming that the installation was successful. To finish the installation and exit the installer, Click **Close**.

A dialog box appears asking if you want to keep the installer file or move it to the Trash.

10. To keep the installation package in the current location, click **Keep**, or to move the file to the Trask, click **Move to Trash**.

The Xerox Workplace Mac Client is installed and ready to use.

DESKTOP PRINTING USING WINDOWS CLOUD CLIENT

Generic Printer (Follow Print)

Add the Xerox Generic Printer (Follow Print)



Note: You can add Xerox Generic Printer only to the Windows Client.

To submit jobs and release later, add the Generic Print driver which will be named "<Email Prefix>@printbyxerox.com", to download and install the Generic Printer:

1. Log in to the Xerox® Workplace Cloud Web Portal.
2. Select **Print > Desktop**.
3. From Add the Xerox Generic Printer (Follow Print) section, click on the **Generic Printer**.

The file named **XeroxWorkplaceCloudClient.xwcdp** is downloaded on your local folder.



Note: If the Add the Xerox Generic Printer (Follow Print) is not visible, or if the required driver is not available, contact your system administrator.

4. Double click on the downloaded **XeroxWorkplaceCloudClient.xwcdp** file to install the Generic Print Driver on your Windows Client Computer.

The Generic Print Driver is installed on your Windows Client Computer.

Printing From the Generic Printer

1. Open a Microsoft Word or other Microsoft Office or print ready document.

2. Select **File > Print**, select the **print@printbyxerox** printer, and click **Print**.
3. Go to a printer and open the **@PrintByXerox** app from the printer Local User Interface (LUI).
4. Log in to the **@PrintByXerox** app with the credentials you use for the Web portal.
5. The job you submitted displays in the print job list.
6. Click **Print** to release the job.

Add Custom Driver Printers (Follow Print) for Windows Client

To submit jobs and release later using a Windows Custom Print Driver, add a Windows Custom Print Driver to your Client Computer. When submitting to Custom Driver Printers, document conversion occurs on your desktop which reduces the duration of job processing at time of print release.



Note: An unprinted job is held for a maximum of 3 days. To set up Data Retention Policy, refer to [Data Retention Policy](#).



Note: To create a Custom Driver Printers (Follow Print), refer to [Queues](#) section.

To install a Follow You printer queue on your Windows Computer, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal.
2. Install the Windows Client, refer to [Installing the Xerox® Workplace Cloud Windows Client](#).
3. Follow you print Queues will be automatically installed if they are set as **Default Printer** when creating the Queues.
4. To manually install a Windows Custom Driver Printers (Follow Print).
 - a. Select **Print > Desktop**.
 - b. From Add Custom Driver Printers (Follow Print), click on the required Windows Custom Driver Printers (Follow Print) of the Printers that you need to install.



Note: If the Add Custom Driver Printers (Follow Print) section is not visible, or if the required driver is not available, contact your system administrator.

The file named **XeroxWorkplaceCloudClient.xwcdp** is downloaded on your local folder.

- c. Double click on the downloaded **XeroxWorkplaceCloudClient.xwcdp** file to install the Print Driver on your Windows Client Computer.

The Custom Driver Printer (Follow Print) queue and driver is installed on your Windows Cloud Client Computer.

Add Direct Printers (Windows)

To install a Direct Printer driver on your Windows Computer, do the following:



Note: To set up Drivers to a Printer in Workplace Cloud, refer to [Drivers](#) section.

1. Install the Windows Client, refer to [Installing the Xerox® Workplace Cloud Windows Client](#).
2. Click **Print > Desktop > All Printers**.


A list of enabled Direct Printer appears.


3. Click on the required printer for which you need to download the driver.
A file named **XeroxWorkplaceCloudClient.xwcdp** is downloaded for the selected printer.
4. Double click on the downloaded **XeroxWorkplaceCloudClient.xwcdp** file to install the Direct Print Driver on your Windows Client Computer.
The driver of the Direct printer is installed on your Windows Client Computer.

DESKTOP PRINTING USING MAC CLOUD CLIENT

Add a Mac PPD Definition (Follow Print)

To install a Follow You printer queue on your Mac Computer, do the following:

1. Install the Mac Client, refer to [Installation of the Workplace Cloud Macintosh Client](#).
 2. Download and install the Mac Print Drivers on your Mac Client Computer.
 3. Follow you print Queues will be automatically installed if they are set as **Default Printer** when creating the Queues.
 4. To manually install a Mac Custom Driver Printers (Follow Print).
 - a. Select **Print > Desktop**.
 - b. From **Add Custom Driver Printers (Follow Print)**, click on the required Mac Custom Driver Printers (Follow Print) of the printers that you need to install.
 - c. The file named **XeroxWorkplaceCloudClient.xwcdp** is downloaded on your local folder.
-  Note: If the **Add Custom Driver Printers (Follow Print)** section is not visible, or if the required driver is not available, contact your system administrator.
- d. Double click on the **XeroxWorkplaceCloudClient.xwcdp** file to install the Mac Custom Driver Printers (Follow Print) on your Mac Client Computer.
 - e. The Custom Driver Printers (Follow Print) of the printer is installed on your Mac Client Computer.

 Note: : If you get a driver not installed error, install the matching printer driver then re-install the **Custom Driver Printers (Follow Print)** queue.

Add Direct Printers (Mac)

To install a Direct Printer driver Job on your Mac Computer, do the following:

1. Install the Mac Client, refer to [Installation of the Workplace Cloud Macintosh Client](#).
2. Download and install the Mac Print Drivers on your Mac Client Computer.
3. To install direct printers on your Mac Client Computer:
 - a. Select **Print > Desktop > All Printers**.
A list of Direct Printer appears.
 - b. Click on the required printer for which you need to download the driver.
A file named **XeroxWorkplaceCloudClient.xwcdp** is downloaded for the selected printer.

- c. Double click on **XeroxWorkplaceCloudClient.xwcdp** file to install the Direct Printers on your Mac Client Computer.

A message appears that the printer is installed on your Mac Client Computer.

ADDING FAVORITE PRINTERS

To add Printers to the **Favorite Printers** list do the following action:

1. Click **Print > Desktop > All Printers**.

The list of Direct Printers appears.

2. Click on the **Star** icon of the required printers.

The required printers are added to the **Favorite Printers** tab.

Print: Email

Upload your documents by sending an email and optional attachments to print@printbyxerox.com or alias address (<EmailPrefix>@printbyxerox.com), refer to [Company Profile: Details](#). When you are ready, use the Xerox Workplace Cloud Portal App to select a printer, choose your print options and release your print job.

Print immediately by sending an email to a specific printer email address (yourprinter@printbyxerox.com). The email and attachments are printed automatically for you.

Email

- **Print now** (Direct Print): Send or forward an email (and attachments) directly to a Xerox® Workplace Cloud-enabled printer's email address (<Email Prefix>.<Friendly name of printer>@printbyxerox.com). To find the email address for a specific printer, check the mobile app.
- **Upload for printing later** (Follow You Pull Print): Send or forward an email (and attachments) to print@printbyxerox.com or alias address (<Email Prefix>@printbyxerox.com) and perform one of the following:
 - Go to your **Documents** in the Xerox® Workplace Mobile App, where it can be retrieved printed when you are ready to release it.

Print jobs may be retained up to 3 days, depending on the company Retention Policy.



Note: If you frequently use the upload for printing later feature, you may want to add print@printbyxerox.com to your contacts.

- Go to a supported Multifunction Printer and release the job using the @PrintByXerox printer app.

Print: Mobile

PRINTING 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 Xerox® Workplace Mobile App. This will enable you to choose a printer and print options or upload for printing later.

To access documents stored on your mobile device, use the following to locate them:

- Android users: My Library
- iOS users: Photos or File Library



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.



Note: 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.



Note: Printing a small page range from a large document does not save data charges.

REPRINTING A DOCUMENT FROM THE XEROX® WORKPLACE MOBILE APP

Go to **Documents** in the Xerox® Workplace Mobile App and follow the printing procedures.

This applies only if the Retention Policy is set to 3 days. The default behavior is for the document to be deleted immediately after printing. The Account Administrator can modify this setting to save documents for 3 days after submission so that they are available for reprint.

Jobs sent to public printers outside of Xerox® Workplace Cloud always display in the job history for 3 days. The Retention Policy settings only apply to your printer, private or public, from company.

Jobs

This chapter contains:

Jobs: History	54
Jobs: Processing	57
Jobs: Available	58
Jobs: Print Tracker	59

The Jobs tab allows you to view available, processing, pending and completed jobs.

The tabs in the Jobs tab are as follows:



Note: For each of the tabs in the Jobs tab, there is an option that allows the administrator to list company jobs. Users can only view the list of their own jobs.

History

List of all jobs processed through the Xerox® Workplace Cloud account.



Note: The list displays jobs for up to one year.

Processing

List of Jobs that are released and in the process of spooling to the printer. The status of these jobs moves to the History tab.

Available

List of Jobs that are available to be released or deleted by the user before processing. The status of these jobs moves to the Processing tab.

Print Tracker

A list of your jobs or the company jobs that were printed through the Print Tracker feature. These jobs are not listed on the History tab.



Note: The list displays jobs for up to one year.

Jobs: History

VIEWING THE JOB STATUS OF THE HISTORY AND PRINT TRACKER

To view the History and Print Tracker job status, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal using your credentials.
2. Select the **Jobs** tab.
3. Select the radio button for **My Jobs** or **Company Printer Jobs**.
The My Jobs option displays all the jobs that you have sent to the printers. The Company Printer Jobs option displays all the jobs that are sent to the printers that are enabled through the company account.
4. Do the following:
 - To view the history, click **History**.
 - To view the Home Worker Print Tracker status, click **Print Tracker**.

The following information is displayed:

- Document Name
- Device Name
- Completion Date: The completion date and time of the job.
- Status: The status of the job. The statuses are as follows:
 - **Conversion**: The job is being converted to a print-ready format in Xerox® Workplace Cloud.
 - **Rejected**: The job did not print. For example, the file type was not supported, or the license is not available.
 - **Failed**: The job did not print. For example, an error occurred during the conversion of the job, or the agent was unable to process the job.
 - **Expired**: The system was unable to process the job within a specified time period. Resend the job.
- Content Security: If **Content Security** is enabled, this field displays the content security status. For more information, refer to [Policies: Content Security](#). The statuses are as follows:
 - **No Match**: This status appears when no search strings are found in the job.
 - **Match**: This status appears when search strings are found in the job. For more information, refer to [Content Security Failure Details](#).
 - **Unknown**: This status appears when the file is not processed for search strings. For example, if the jobs are released when **Content Security** is disabled.

5. To export the information from the History or Print Tracker tabs, from the Actions menu, do the following:

- To export the current page, select **Export This Page**.
- To export all data in the table, select **Export All Pages**.

A .csv file is downloaded to your computer. The .csv file includes the following fields:

- Company
- Submitter
- Document Name
- Device Name
- Submission Date
- Completion Date
- Status
- Serial Number
- Copies
- Stapled
- Duplex
- Color pages
- Black & White Pages
- License Serial Number
- Accounting
- Content Security Status
- Found Search Strings

Jobs History Export

1. Select the **Jobs** tab.
2. Select the radio button for **Company Printer Jobs**.
3. Click **History**, then apply any filters, as needed.
4. From the Actions menu, select **Export This Page**.
The .csv file is downloaded to your computer. The default file name for the report is `XeroxCloudPrintCompanyJobsHistory.Workplace._CurrentPages.csv`.



Note: From the Actions menu, to export all data in the table, select **Export All Pages**. The default file name for the report is `XeroxCloudPrintCompanyJobsHistory.Workplace_AllPages.csv`.

Content Security Failure Details

When you select the **Failed** option, the Content Security Details window appears. You can view the following information:

Jobs

- Job Name: The name of the released job
- User: The name of the user who released the job
- Completion Time: The completion date and time of the job
- The search strings that are identified.

Jobs: Processing

VIEWING THE PROCESSING JOB STATUS

To view the Processing job status, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal using your credentials.
2. Select the **Jobs** tab.
3. Select the radio button for **My Jobs** or **Company Printer Jobs**.
The **My Jobs** option displays all the jobs that you have sent to the printers. The **Company Printer Jobs** option displays all the jobs that are sent to the printers that are enabled through the company account.
4. Click **Processing** tab.

The following information is displayed:

- User Email: The email address of the user who sent the job.
- Document Name: This option displays the name of the document.
- Device Name: This option displays the name of the device.
- Submission Date: This option displays the submission date and time of the job.
- Status: This option displays the status of the job. The different statuses are as follows:
 - Upload: (only shows in the app) The job is being sent to Xerox® Workplace Cloud.
 - Conversion: The job is being converted to print-ready format in Xerox® Workplace Cloud.
 - Pending: The job is converted and is waiting to print.
 - Processing: The job is being sent to the printer.



Note: The **Processing** job status is temporary and is moved to **History** tab once the job is released from the printer.

Jobs: Available

The **Available** tab allows users to view and delete their uploaded jobs that are ready to be released.

Guidelines:

- The **Available** tab appears only in the **My Jobs** section and not in the **Company Printer Jobs** section.
- An administrator can only view and delete their own uploaded jobs and not the jobs of other users in a company account.
- Direct jobs are not listed in the **Available** tab as these are auto released at the printer.

VIEWING THE AVAILABLE JOBS



Note: The User can only view the **Available** tab only when the selection is **My Jobs** on the Jobs tab.

To view your Uploaded Jobs, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal using your credentials.
2. Select the **Jobs** tab.

The My Jobs option displays all the jobs that you have submitted to the printers.



Note: If you are an Administrator or Super User, select the radio button for **My Jobs** to display all the jobs that you have submitted to the printers.

3. Click **Available** tab.

The Available tab displays the user's uploaded jobs that have not yet been released on the web portal.

4. The following information is displayed:
 - User Email: Displays the email address of the user who have submitted the job.
 - Document Name: Displays the document name of the submitted job.
 - Submission Date: Displays the job submission date and time.

DELETE THE UPLOADED JOBS

1. Log in to the Xerox® Workplace Cloud Web Portal using your credentials.
2. Select the **Jobs** tab.
3. Select the radio button for **My Jobs**.

The My Jobs option displays all the jobs that you have submitted to the printers.

4. Click **Available** tab.

The Available tab displays the user's uploaded jobs that have not yet been released on the web portal.

5. Select the required Uploaded jobs and click on **Actions > Delete**.

The delete job dialogue box appears, to confirm the deletion click **Ok**. The selected jobs are deleted from the Available tab.

Jobs: Print Tracker

For detailed information, refer to [Viewing the Job Status of the History and Print Tracker](#).

Printers

This chapter contains:

- Printer Tabs..... 62
- Adding a New Printer..... 63
- Printers Action Menu and Edit Printer Settings Descriptions..... 65
- Printer Groups 79
- Deployment Groups 80
- Supported Languages..... 84
- Xerox® Global Print Driver 85

The Printers tab is where you can register and maintain the list of printers available to be used by Xerox® Workplace Cloud. A list of registered printers is displayed in a table. Mouse over the icons on the right to indicate the printer capabilities.

Printer Tabs

All

This is a list of all the printers the registered to your cloud account. This includes enabled, non enabled , discovered by agent and agentless printers.

Enabled

This is list of the printers that is enabled for users to print to.

Printer Groups

This is where you can group printers together based on common associations. For example, by location, capabilities, access, etc. Printer Groups can then be associated with print Rules and Fleet Management.

Deployment Groups

Deployment groups are used for deploying direct printers to client computers. Xerox® Workplace Cloud will act as a Print Queue Conductor and automatically deploy printers to client computers. You should select the IP range(s) of the target computers along with the printers that you wish to deploy.

Adding a New Printer



Note: If you are using Cloning to configure your printers setup, refer to [Recommended Steps to Add New Printers when using Printer Cloning](#).

There are multiple ways to add a new printer, first you have to register the printer and enable the printer.

Registering a Printer:

1. Register the printer using one of the following methods:
 - Discover the printer using an Cloud Agent, refer to [Agents](#).
 - To add a agentless printer, refer to [Workplace Cloud Direct \(Manage Printer without an Agent\)](#).
 - To manage and configure the printers after adding them to a Workplace Cloud account, refer to [Printers Action Menu and Edit Printer Settings Descriptions](#).

Enabling the Printer:

2. To enable a printer, ensure that the printer is listed in the All printers tab.
If this printer is not listed , refer to [Printer Issues](#).
3. After the printer is registered with your cloud account, the printer is listed in the **Printers > All**.
4. Select the check box next to the printer you want to enable, then select **Enable**.
The enabled printer is located on the Enabled tab.
5. Select the **Enabled** tab.
6. To enable features on multiple printers, from the Actions menu, select the required printers then, select the required features you want to enable.
7. To edit a printer and enable features select the printer name from the printer tab.
8. Refresh the printer page and check the printer status.

RECOMMENDED STEPS TO ADD NEW PRINTERS WHEN USING PRINTER CLONING

Cloning allows you to save your current printer configuration and app settings to a file that you can copy to other printers and to use as a backup. For more information about Cloning Printers, search with keyword `Clone` in [Product Support and Drivers – Xerox](#) website.

Recommended steps in Workplace Cloud for Printer Cloning

1. Clone the Printers.
2. Discover the Printers with an Agent.
3. Enable the Printers.
4. Configure settings such as authentication, Printer Client and Usage Tracking.



Note: If cloning is done after adding the printers to Workplace Cloud, you should perform a repair action on **Printers > Action > Repair** to update the printer settings in Workplace Cloud.

When you add a printer to Workplace Cloud, the following setting values are unique to each printer, if the Clone File is applied to the printers after they have been added to Workplace Cloud, you must do a repair action of the printers on Workplace Cloud to update any settings which are unique to each printer.



Note: If you follow the [Recommended steps in Workplace Cloud for Printer Cloning](#), the repair of printers on Workplace Cloud is not necessary.

- EIP App Registration for the Printer Client @PBX app
- Convenience Authentication and Workplace Cloud Authentication which use the following unique settings:
 - SSO Path Value
 - QR Code on the Blocking Screen
 - Blocking screen unlock code (4 character code)
- Usage Tracking: The Cloud **Capture Usage with Pre-Authorization** setting is unique for each Workplace Cloud Company account.

ENABLING A HOME PRINTER ON AN EXISTING COMPANY ACCOUNT WHEN USING AN AGENT

1. The user should log in at <https://xwc.services.xerox.com>.
Ensure that the user is homed in the account that they want to add the printer to. If they are not adding the printer to the same account, they need to logout and log in using the change the company code function.
2. If the account administrator has not logged in ,then the administrator should:
 - a. Log in at <https://xwc.services.xerox.com>.
 - b. Select the **Users** tab.
 - c. Grant the user either the **Agent Administrator** or **Account Administrator** role.
3. The user should:
 - a. Log out and log in at <https://xwc.services.xerox.com>.
 - b. Select the **Agents** tab.
 - c. Select **New** from the **Actions** menu.
 - d. Complete the Agent setup wizard, then click the **Download the Xerox Workplace Cloud Agent Installer** link.
 - e. Install the Agent on the home computer.
 - f. After the Agent installation is complete, log in to the Agent and it will search for all available printers. If necessary, click **Printer Search**.
 - g. Select **Enable Printers**.
The Xerox® Workplace Cloud Web Portal opens.
 - h. Select a printer to enable.
 - i. Select **Enable Printer** from the **Actions** menu.



Note: Documents printed on a home printer will be included in the total job count for the company license and user prints will be billed to their company.

Printers Action Menu and Edit Printer Settings Descriptions

Below is a description of the Printer settings that are found on Printer Edit Page or accessible using the Printer Actions menu.



Note: The Action menu settings allows you to apply settings on multiple printers at one time. Not all of the setting are Actions menu settings.

CHANGE SITE



Note: This setting can be found in the **Printers > Actions** menu and on the **Edit Printer** setting.

Use this option when your printer is moved to a new building or to show the printer in a different location on the map.

The agent is associated with a site, and any printers discovered with that agent are automatically assigned to that site.



Note: If multiple agents are set to discover the same IP address and if these agents are associated with different sites, then the printer will be associated with whatever agent's site is set by the first agent to discover the printer.

To change the site associated with a printer:

1. Go to the Cloud Web Portal and select the **Printers** tab.
2. Select the printers you wish to change.
3. Select **Edit > Location > Change Site**.



Note: Select the check box next to the printers you wish to change. From the **Actions** menu, select **Change Site**.

4. Select a different site, then click **OK**.

PRINT WELCOME PAGE



Note: This setting can be found in the **Printers > Action** menu.

The **Actions** menu will print the Welcome Page for the selected printer or printers, if you want to preview the Welcome Page, then select the glasses document icon that is located below the check-box. The Welcome Page can also be used as a test print. The Welcome Page contains user instructions and QR Codes for obtaining the Xerox® Workplace Mobile App and adding the printer to the Workplace App.

1. From the Xerox® Workplace Cloud Web Portal, select the **Printers** tab.
2. Select the check boxes next to the printers you want to print a Welcome Page for.
Ensure that the printer is enabled.
3. Select **Print Welcome Page** from the **Actions** menu.
4. Select a language and click **OK**.

GENERATE LABELS

The basic generated QR Code label can be used to unlock the printer from the Mobile App. If you want the QR Code to install the Workplace App and unlock the printer, enable the **Allow Mobile Unlock Using Native Camera** setting.

For more details on the QR Code capabilities, refer to [Unlocking the Printer Using Native Camera](#).



Note: This setting can be found in the **Printers > Action** menu.

1. From the Xerox® Workplace Cloud Web Portal, select the **Printers** tab.
2. Select the check boxes next to the printers you want to generate a label.

Ensure that the printer is enabled.

3. Select **Generate Labels** from the **Actions** menu.

The QR Code of the printer will be generated in the PDF format.

ENABLE OR DISABLE PRINTER



Note: This setting can be found in the **Printers > Actions** menu and on the **Edit Printer** setting.

Enable Printer: Makes a printer usable by the Xerox® Workplace system. If you are licensing Xerox® Workplace by devices, this option requires a license.

Disable Printer: Makes a printer unusable by the Xerox® Workplace system, but leaves it in the discovered list. This process frees any device license used by the printer.

To enable a printer, do the following:

1. From the Xerox® Workplace Cloud Web Portal, select the **Printers** tab.
2. Select the check boxes next to the printers you want to enable or disable.
3. From the **Actions** menu, select **Enable Printer**.
4. To disable the printer, From the Actions menu, select **Disable Printer**.

ENABLE OR DISABLE DIRECT PRINTING



Note: This setting can be found in the **Printers > Actions** menu and on the **Printers > Edit Printer > Details** tab.



Note: By default all the printers are enabled for Direct Printing.

Guidelines:

- When Direct Printing is enabled:
 - Displays the printers Direct Printing email address on the printers grid on the Printers tab.



Note: The direct printing email address is automatically created. The email address is made of the Company email prefix followed by printer name. The Domain Name is always @printbyxerox.com. For changing Printer email address, refer to [Change the Direct Printing Email Address](#).

- Users can see the printers on the **Print > Web** or **Desktop** tab for direct printing.

- Users can see the printers on Workplace Mobile application Favorite printers.
- Users can direct email the print jobs.
- When Direct Printing is disabled:
 - Removes the printers Direct Printing email address from the printers grid on the Printers tab.
 - Removes the printers from the **Print > Web** or **Desktop** tab.
 - Removes the printers from the Workplace Mobile application Favorite printers.
 - Users cannot direct email the print jobs, even if they have the printer email address information.

To Enable or Disable the Printers for Direct Printing do the following action:

1. From the Xerox® Workplace Cloud Web Portal, select the **Printers > All** tab.
2. Select the check boxes next to the printers that you want to enable or disable Direct Printing.
3. To enable the Direct Printing, from the **Actions** menu, select **Enable Direct Printing**.

This will enable the printers for Direct Printing.

4. To disable the Direct Printing, from the **Actions** menu, select **Disable Direct Printing**.

This will disable the printers for Direct Printing.



Note: Alternatively, click on the Printer name, on the **Details** tab, select or deselect the check box near to **Enable Direct Printing** for Direct Printer management.

MAKING A PRINTER PRIVATE OR PUBLIC



Note: This setting can be found in the **Printers > Actions** menu and on the **Edit Printer** setting.

Only a secure-print capable Xerox® printer can be set to public printer.

1. From the Xerox® Workplace Cloud Web Portal, select a printer on the **Printers** tab.
2. Do one of the following:
 - Select **Edit > Access Settings** and select **Private** or **Public**.
 - From the **Actions** menu, select multiple printer check boxes and select **Mark as Public** or **Mark as Private**.

SET ACCOUNTING MODE



Note: This setting can be found in the **Printers > Actions** menu and on the **Edit Printer** setting.

Selects the accounting mode that is set on the printer. The accounting mode should only be set in environments where Xerox® Network Accounting or Xerox® Standard Accounting is used. When this mode is set in Xerox® Workplace Cloud, the user accounting information is sent with the job.

1. From the Web Portal, select the **Printers** tab.
2. Select one or more printers from the list.
3. Select **Set Accounting Mode** from the **Actions** menu.

4. Select one of the following:

- **Xerox Network Accounting**
- **Xerox Standard Accounting**

When you enable Xerox® Network Accounting or Xerox® Standard Accounting, make sure it is for Xerox printers only. Non-Xerox printers are not compatible with these accounting methods.

5. Select **Set Accounting Mode** and then select **OK**.

Users are prompted for their accounting information when they print through the Web Portal or the Workplace Mobile App.



Note: The accounting mode selected must match the accounting mode that is set at the printer. Setting the accounting mode on the Xerox® Workplace Cloud Web Portal does not affect any printer settings.

Set Accounting Mode for Non-Xerox® Printers



Note: This setting can be found in the **Printers > Actions** menu and on the **Edit Printer** setting.

When you enable Xerox® Network Accounting or Xerox® Standard Accounting, make sure it is for Xerox® printers only. Non-Xerox printers are not compatible with these accounting methods.

For non-Xerox printers, it is recommended not to set Xerox® Accounting as a default for your company. This option should only be used with Xerox® devices that support the accounting mode selected. Refer to the documentation that came with the printer for specific accounting information.

When Xerox® Network Accounting or Xerox® Standard Accounting is the default accounting mode for Xerox® Workplace Cloud accounts, and a non-Xerox® printer is automatically enabled at discovery, ensure that you manually remove accounting from that printer separately.

1. From the Xerox® Workplace Cloud Web Portal, select the **Printers** tab.
2. Select the printer name to **Edit Printer**.
3. Select **Accounting** tab.
4. Select the radio button for **No Accounting** under **Accounting Mode** and click **Save**.

SET CLIENT APPLICATION INSTALLATION MODE



Note: This setting can be found in the **Printers > Actions** menu and on the **Edit Printer** setting.

Installs or uninstalls the @PrintByXerox app on the selected printers.

1. Select the check box next to the printers from the list.
2. From the Actions menu, select **Set Client Application Installation Mode**.

This operation takes time, so feedback on its success or failure cannot be immediate.

You can also install the Client Application on the **Printers > Features** tab.

3. To install it, select the **Install the client application on the device** check box. To remove it, deselect the check box.

SET AUTHENTICATION MODE



Note: This setting can be found in the **Printers > Actions** menu and on the **Edit Printer** setting.

Enables or disables the ability to lock or unlock the printer user interface. When enabled, credentials are required to access the console on the printer. The options are

- **Disabled:** Credentials are not required to access the console on the printer.
- **Enabled:** Credentials are required to access the console on the printer.

As operation takes time, please come back later to see if it has succeeded or failed.

For more information, refer to [Configuring Authentication](#).

SET DIRECT EMAIL MODE



Note: This setting can be found in the Printers Actions menu and in the Edit Printer setting.

You may configure one or more public or private printers in the printer list to allow unregistered (anonymous) users to submit print jobs by direct email. In this mode Xerox® Workplace Cloud will accept an email from an unregistered email address, as long as the printer email is valid and the user's email or domain is not on the Blocked Users List.



Note: An unregistered user does not need to be on the Allowed Users list to print to private printers that allow anonymous direct email print.

1. From the Xerox® Workplace Cloud Web Portal, select the **Printers** tab.
2. Click on the printer for which you would like to enable anonymous direct email print.
3. Check the box next to **Allow Direct Email Print for Anonymous Users**.
4. Select **Save**.



Note: You can also select a printer from the list on the **Printers** tab, from the Actions menu, and select **Set Direct Email Mode > Allow direct email printing for unregistered users**.



Note: Requiring Secure Print on printers that allow Direct Email Print for Anonymous Users adds a level of security to the printer. This ensures that random users cannot start the printer without being present to receive the print job.

Change the Direct Printing Email Address



Note: By default, the direct printing email address is automatically created. If you need to change the direct printing email address do the following steps.

To change your direct printing email address:

1. Select **Account > Company Profile**.
2. Under Details, email Prefix field, enter the new email Prefix value and click **Save**.



Note: The email prefix is used to create a unique email address for each printer enabled by Xerox® Workplace Cloud. All printers within the same company account will have the same email prefix. If you choose to change this setting Xerox Workplace Cloud will verify that the value you choose is not already in use.

3. Select **Printers > All** tab.
4. Click on the required Printer Name.
5. On the Name (ex: Local printer), provide the required Printer friendly name.
6. Click **Save**.
7. A new email address is displayed under the printer on the Printer grid for Direct Printing.



Note: The email address is made of the Company email prefix followed by printer name. The Domain Name is always @printbyxerox.com.



Note: Direct Printing feature must be enabled for the Printer to display the Printer email address.

SET AUTO RELEASE MODE



Note: This setting can be found in the **Printers > Actions** menu and on the **Edit Printer** setting.

To enable the Auto Release feature, perform the following steps:

1. Log in as an administrator to Xerox® Workplace Cloud.
2. Select the **Printers** tab.
3. Select the check box next to your printer.
4. You can set auto release from the Actions menu, select **Set Auto release Mode**.
5. Or, select your printer.
6. Select the **Features** tab, then select **Auto release all jobs**. For Auto Release All Jobs, select an option:
 - **Never:** If this option is enabled, the Auto Release feature is disabled. You can release the jobs manually.
 - **Using Network Appliance:** If this option is enabled, after you have authenticated from an external network, you can release the jobs.
 - **Using Access card or Alternate login:** If this option is enabled, after you have authenticated, jobs are released automatically.

SET USAGE TRACKING MODE



Note: This setting can be found in the **Printers > Actions** menu and on the **Edit Printer** setting.

When enabled, allows Job-Based Accounting data to be retrieved from the printers and used for Job Reporting.

When a printer has Usage Tracking enabled, refer to [Reporting](#).

Set Usage Tracking Mode allows you to restrict the Copy jobs, refer to [Capture Usage with Pre-Authorization](#).

Guidelines:

- If the printer does not support Set Usage Tracking Mode, the failure message is displayed on the Workplace Cloud web portal.
- If you disable Usage Tracking, when **Capture Usage with Pre-Authorization > Copy Jobs** is enabled, then Workplace Cloud will clear the Job Limits Server URL and disable the Copy Job Limits for the respective printers.

Enable or Disable Set Usage Tracking Mode

To enable or disable the Set Usage Tracking Mode, do the following steps:

1. Log in as an administrator to Xerox® Workplace Cloud.
2. Click **Printers** tab.
3. Click on **Enabled** tab, select the required printers from the list, use the filter options if necessary.
4. Select the check box of the required printers.
5. Click on **Actions > Set Usage Tracking Mode**.

The Set Usage Tracking Model (Network Accounting) dialogue box appears.

6. Select **Enabled** and click **Apply**.

The Set Usage Tracking Mode is applied to the selected printers.

7. To disable the **Set Usage Tracking Mode**, deselect the **Enabled** check box and click **Apply**.

Capture Usage with Pre-Authorization

Enabling the **Copy Jobs** option will hold all the copy jobs and require pre-approval by Workplace Cloud in order for the job to be printed. This option is used in conjunction with Rules based on Print Quotas. If a job will cause the user to exceed their Quota, then the job will be rejected by the solution.

The Capture Usage with Pre-Authorization option is supported by Xerox® AltaLink and Xerox® VersaLink devices.

Enable Capture Usage with Pre-Authorization



Note: This option is available when **Set Usage Tracking Mode** is enabled for the printers.

To enable the Capture Usage with Pre-Authorization:

1. Log in as an administrator to Xerox® Workplace Cloud.
2. Click **Printers** tab.
3. Click on **Enabled** tab, select the required printers from the list, use the filter options if necessary.
4. Select the check box of the required printers.
5. Click on **Actions > Set Usage Tracking Mode**.

The Set Usage Tracking Mode (Network Accounting) dialogue box appears.

6. Select the check box of **Copy Jobs** under **Capture Usage with Pre-Authorization**.
7. Click **Apply**.

The Capture Usage with Pre-Authorization is applied to the printers.

SET FILE DECRYPTION MODE



Note: This setting can be found in the **Printers > Action** menu.

The File Decryption Mode feature is applicable only if the customer is using their own certificate with a public key to encrypt desktop custom driver print jobs. If the certificate with the corresponding private key is installed on the

printer, some Xerox printers support the ability to decrypt these jobs. Before you enable printer decryption, ensure that you upload the certificate with the public key to Xerox® Workplace Cloud and install the certificate with the private key on the printer. File Decryption Mode can improve print performance and it helps to reduce the number of agents that are required for a given customer.

To set the file decryption mode, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select the **Printers** tab.
3. Select the required printer.
The Edit Printer page appears.
4. In the File Decryption Mode area, select one of the following radio buttons:
 - **Use the Agent to decrypt jobs**
 - **Use the Printer to decrypt jobs**
5. Select **Save**.
In the Printers tab, from the list, select the check box next to the printer, then from the Actions menu, select **Set File Decryption Mode**.

CLOUD DIRECT (MANAGE PRINTER WITHOUT AN AGENT)



Note: This setting can be found in the Printers Actions menu and in the Edit Printer setting.

For more information, refer to [Workplace Cloud Direct \(Manage Printer without an Agent\)](#).

MANAGE PRINTER USING AN AGENT



Note: This setting can be found in the Printers Actions menu and in the Edit Printer setting.

For more information, refer to [Agents](#).


Determining the Agents that are Managing a Printer

To determine the agents that are managing a printer, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select the **Printers** tab.
3. Select the required printer.
The Edit Printer page appears.
4. Select the **Agents** tab.
A grid appears that displays the agents that are managing that printer.
To remove an agent from the printer, refer to [Removing an Agent from a Printer](#).

Removing an Agent from a Printer

To remove an agent that is managing a printer, do the following:

 Note: The delete agent action can be used for a printer that was removed from an Agent Discovery profile, but the printer still has an association to that agent on the grid.

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select the **Printers** tab.
3. Select the required printer.
The Edit Printer page appears.
4. Select the **Agents** tab.
The Printer Management section appears.
5. Select the check box next to the agent that you want to remove.
6. From the Actions menu, select **Delete**.


REMOVING SELECTED PRINTERS FROM THE PRINTER LIST

 Note: This setting can be found in the **Printers > Action** menu.

Removes the printer from the discovered printers list. This option does not remove the IP address from the scan for the Agent.

Do the following to remove the printer so it is not visible to users or to remove the printer from the system entirely.

1. From the Xerox® Workplace Cloud Web Portal, select the **Printers** tab.
2. Select the check boxes next to the printers you want to disable or remove.
3. Select **Remove** in the **Actions** menu.

 Note: Removing a printer from the list does not remove it from discovery. The next time discovery is run, the printer will reappear as disabled with the default properties, unless it has been added to the Exclusions. Refer to [Excluding Printers or Subnets From Discovery by the Print Agent](#).

REPAIR

 Note: This setting can be found in the **Printers > Action** menu.

The repair operation re-applies settings to the printer to assure that the settings and the printer match.

If a printer had a maintenance issue or if the Company Workflow has been modified, settings may have been changed that require the printer to be reinstalled. If a printer, that was previously registered, is no longer operating properly in the Workplace Cloud application, you can do repair action on Workplace Cloud.

The repair process will attempt to reset the printer to the settings needed for proper communication.

Repair the Printers

1. On the **Printers** tab, select the checkbox of the printers that requires repair.
2. Select **Actions > Repair**.

A confirmation alert appears.

3. Click on **Repair**.



Note: This operation may take some time to complete, check after few minutes to see if the repair action is succeeded or failed.

REMOVE



Note: This setting can be found in the **Printers > Action** menu.

This setting removes the selected Printers from Workplace Cloud company account.

To Remove the Printer from the Workplace Cloud company account:

1. Login to the Workplace Cloud Web Portal as an administrator.
2. Select **Printers > All** tab.
3. Select the check box of required Printers from the list.
4. Click **Actions > Remove**.

The selected printers are removed from the list.

CHANGING THE PRINTER NAME



Note: This setting can be found in the Edit Printer setting.

You can change the name of the printer by:

1. From the Xerox® Workplace Cloud Web Portal, select the **Printers** tab.
2. Select a printer.



Note: If you change the printer name, the printer email address also changes. If a contact was created for the printer, delete the contact and create a new contact.

The Edit Printer page appears.

3. In the **Details** tab, in the Name field, edit the name.
4. To save the update, click **Save**.

If a Welcome Page was printed and displayed on your printer, replace it with an updated Welcome Page with the new printer name. For information on printing a Welcome Page, refer to [Print Welcome Page](#).

PRINTER DETAILS

These values are automatically detected from the printer as follows:

- Manufacturer
- Model

- MAC Address

EDITING THE IP ADDRESS OF A PRINTERS



Note: This setting can be found in the Edit Printer setting.

An account administrator can edit the IP address of the printer.

1. Login to the Workplace Cloud Web Portal.
2. From the Printers tab, select a printer.
3. Click **Details**.
4. Edit the IP address of the printer, then click **Save**.

SERIAL NUMBER



Note: This setting can be found in the Edit Printer setting.

The Serial number is detected from the printer automatically and it can be edited.

SUPPORTED PRINTER LANGUAGES

PostScript, PCL 5, PCL 6, and PDF are supported. The default language is PostScript, but the administrator can change it if necessary.

For printers that support native PDF, the advantages are faster transfer, smaller file sizes, and less network traffic.

Setting the Order of Preferences for the Printer Language



Note: This setting can be found in the Edit Printer setting.

Supported printer languages are PostScript, PCL5, PCL6, and PDF. To modify the order, the supported printer languages are used:

1. Log in as an administrator to the Xerox® Workplace Cloud Web Portal.
2. Select the **Printers** tab.
3. Select the printer you want to change.
The Edit Printer page appears.
4. In the **Details** tab, in the Printer Language menu, change the order of the language using the arrow to send to the printer.
5. To update the settings, click **Save**.

SUPPORTED FINISHERS FOR DESKTOP DIRECT PRINT

From the **Printers** tab, the administrator can assign the available finishers to a printer. Workplace Cloud supports the following finishers for Xerox® printers:

- Integrated Office Finisher
- Office Finisher LX
- Office Finisher LX with Booklet Maker
- BR Finisher
- BR Booklet Maker Finisher
- Offset Catch Tray (OCT)
- Office Finisher
- Office Finisher with Booklet Maker



Note: This configuration option is supported only for the Desktop Client with the Direct Print. It uses the default Global Print Driver (GPD) that comes with the Workplace Cloud solution. Custom drivers are not supported.

SETTING PROTOCOLS



Note: This setting can be found in the Edit Printer setting.

Xerox® Workplace Cloud supports printing with Raw, Line Printer Remote (LPR), or IPP over SSL for each printer.

1. From the Xerox® Workplace Cloud Web Portal, select the **Printers** tab.
2. Select a printer and click the IP address, then select the **Details** tab.
3. From the **Protocols** menu, select one of the following:
 - Auto Detect
 - Raw
 - LPR/LPD
 - IPP over SSL

If you choose:

- Auto Detect, Xerox® Workplace Cloud defaults to Raw.
- Raw, you can enter the Raw TCP Port.

If you leave the Raw TCP Port field blank, the default port is 9100.

- LPR/LPD, the LPR Queue Name is optional.

It is recommended that you leave the LPR Queue Name blank, unless you know the specific queue name needed to send to a specific printer.

If the queue name is blank, Xerox® Workplace Cloud tries to auto-detect the queue name.

- IPP over SSL, this option attempts to print with IPPS. This protocol sends encrypted SSL data over port 443 to the printer.

You can select the port number for each protocol.



Note: These queue names refer to print queues on the **printer**, not to server-based print queues configured on the **Print Queues** tab. For more information on print queues, refer to [Server-Based Print Queues](#).

4. To save the setting, click **Save**.

Supported Printer Protocols

Workplace Cloud supports the following printer Protocols:

- Auto Detect
- RAW (Port 9100)
- LPR/LPD (Line Printer Remote/Line Printer Daemon)
- IPP over SSL (Internet Printing Protocol over Secure Sockets Layer)

The administrator can set the options as per the requirement.

ENABLING SECURE PRINT



Note: This setting can be found in the Edit Printer setting.

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.

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

To add security to a Xerox® Secure Print capable printer you may configure Xerox® Workplace Cloud to require that Secure Print be used for all jobs sent via Xerox® Workplace Cloud to that printer.

1. From the Xerox® Workplace Cloud Web Portal, select the **Printers** tab.
2. Select a Secure Print capable printer.
3. Select the name of the printer.
4. On the **Details** tab, select the check box next to **Secure Print Capable**.
5. Select **Save**.



Note: Users will know if a printer requires a Secure Print passcode when printing with Xerox® Workplace Cloud because they will see a required field (represented by a blue bar in the field), which they must fill in before submitting a print job.

For print jobs submitted via direct email print, users will receive an email containing an auto-generated passcode, which must be entered at the printer to release the job for printing.



Note: Requiring Secure Print on printers that allow Direct Email Print for Anonymous Users adds a level of security to the printer. Only a secure-print capable Xerox printer can be set to public printer.

PRINTING TO ALTERNATE IP ADDRESS



Note: This setting can be found in the Edit Printer setting.

When enabled, Jobs released from the Printer Client Application or Auto Release All Jobs, are printed to the alternate IP address entered. Typically this feature is used for Jobs to be release to a Fiery Controller setup in a dual IP mode, instead of the printer the Fiery is connected to.

SNMP SETTINGS



Note: This setting can be found in the Edit Printer setting.

The SNMP Settings can be entered in Multiple places in Workplace Cloud, if the SNMP Setting is blank on the **Printers** tab, then the Agent or Cloud Direct SNMP setting is used. The SNMP setting entered on the **Printers > SNMP Settings** tab is the priority setting which will override the SNMP settings entered on the Agent or Cloud Direct tab.

There are two options in Set SNMP Settings: SNMP v1/2 and SNMPv3. Users can select one of the SNMP options, for more information on setting up the SNMP settings, refer to [Manage SNMP settings](#).

Printer Groups

The Xerox® Workplace Cloud provides an option to assign Printer Groups to a group of printers based on their common association. The Printer Groups are used when the account administrator associates printers with a Rule. The administrator can create or delete Printer Groups based on requirement.

CREATING PRINTER GROUPS

1. Go to <https://xwc.services.xerox.com> and log in as an administrator.
2. Click the **Printers** tab.
3. Click **Printer Groups**.
4. Create a Printer Group:
 - a. Select **Actions > New**.
 - b. Complete the Details with Name and Description fields.
 - c. Select the type of access you want with Associated Machines. Options include:
 - **Allow access to all printers except blocked list:** You can select all printers to be part of the Printer Group, except the ones specified in the list of Blocked Printers.
 - **Allow access to specified printers only:** You can select any printers from the list of Allowed Printers to be part of the Printer Group.
 - d. Click **Save**.



Note: To delete a Printer Group, click the check box of an existing Printer Group, then select **Delete** from the Actions menu.

Deployment Groups

Deployment groups are used for deploying Direct Printers or Pull Print Queues to client computers. Xerox® Workplace Cloud will act as a Print Queue Conductor and automatically deploy Printers or Pull Print Queues to client computers. You should select the IP range(s) of the target computers or User Groups along with the printers that you wish to deploy.



Note: This feature requires version 5.8.111 or higher of the Xerox® Windows Workplace Cloud Client. However if you use Deploy printers based on User Groups setting, this setting requires version 5.8.200 or higher of the Xerox® Windows Workplace Cloud Client



Note: The user can also manually install a Printer using the Web Portal, refer to [Print: Desktop](#) section for details.

Guidelines:

- A Deployment Group can deploy a maximum of 25 printers.
- When a Deployment Group is defined, the Xerox® Workplace Cloud Desktop Client will automatically download and install printers on the client computers defined in this Deployment Group.
- Xerox® Workplace Cloud Desktop Client checks for the new printers when launching the application, during a User login and during every 24 hours.
- If you remove the printer from Deployment Groups, it is not automatically removed from the Workplace Cloud Desktop Client. The users can delete printers using the built in Operating System tools.
- The User can check for new printers manually through refreshing the printers.
- You cannot deploy a Direct Printer using Deployment Group with Mac Client.

GENERAL STEPS TO DEPLOY DIRECT PRINTERS ON CLIENT COMPUTERS USING DEPLOYMENT GROUPS

1. Add the Printer to the Workplace Cloud Company account, refer to [Adding a New Printer](#).
2. Enable the Printer, refer to [Enable or Disable Printer](#).
3. Create the Custom Driver or a Composer File that you want to associate with the Printer, refer to [Custom Drivers](#) or [Composer Files](#) section.
4. Associate the Printers to the Custom Driver or Composer File, refer to [Select the Driver Type for Direct Printers](#).



Note: If a Custom Driver or Composer File is not associated with the printer, by default the printer will use the Xerox Global Print Driver.

5. Create and Enable the Deployment Group, refer to [Create Deployment Groups](#).

GENERAL STEPS TO DEPLOY PULL PRINT QUEUES ON CLIENT COMPUTERS USING DEPLOYMENT GROUPS

1. Create the Custom Driver or a Composer File that you want to associate with the Printer, refer to [Custom Drivers](#) or [Composer Files](#) section.
2. Create Pull Print Queues, refer to [Queues](#) section and assign the Driver.

3. Enable the Pull Print Queue, refer to [Enable or Disable Pull Print Queues](#).
4. Create and Enable the Deployment Group, refer to [Create Deployment Groups](#).

CREATE DEPLOYMENT GROUPS

Deployment groups have the following four fields:

- Name
- Clients
- Printers
- Summary

To Create Deployment Group:

1. Login to the Xerox® Workplace Cloud application.
2. Click the **Printers** tab.
3. Click **Actions > Add**.
4. On the Details section, enter the Name and Description and click **Next**.
5. Select which user desktop computers running the Workplace Cloud Client that the printers will be deployed to.
 - a. **Deploy on all Client computers:** This option will install all printers associated with this Deployment Group to every client computer in the environment.
 - b. **Deploy printers to specific IP ranges of Client computers:** This option will install all the printers associated with this Deployment Group to all the clients in the specified IP ranges added to this Deployment Group.
 - To add specific IP ranges:
 - Click **Actions > Add**.
 - On the Details section, enter Name, Start Address, and End Address of the Client Computers and click **Save**.

The specific Client Computers are added.
 - To remove the Client Computers from the Deployment Group:
 - Select the required IP Range, click **Actions > Delete**.

The selected Client Computers are removed from the list.

- c. **Deploy printers based on User Groups:** This option will install all the printers associated with this Deployment Group to all the Client Computers of the Users in the User Groups.



Note: Use of this feature requires version 5.8.200 or higher of the Xerox® Workplace Cloud Client.

- To add the User Groups to this Deployment Group:
 - Click **Actions > Add**.
 - Select the check box of the required **User Groups** from the list and click **Save**.

The selected User Groups are added.



Note: If no User Groups are available for selection, refer to **User Groups** section to create a User Group.

- To remove the User Groups from the Deployment Group:
 - Select the check box of the required User Group, click **Actions > Remove**.

The selected User Groups are removed from the list.

- d. Click **Next**.

6. Select the Printers or Pull Print Queues to be used by this Deployment Group.

- a. **All Printers:** This will install all printers associated with this deployment group to every Client machine in the environment.
- b. **Printer Groups (Direct Printers):** This will install selected printer groups associated with this deployment group to every Client machine in the environment.



Note: The number of printers that can be installed per Deployment Group is limited to 25.

- To add the Printer Groups to the Deployment Group:
 - Click **Actions > Add**.
 - Select the required groups from the list and click **Save**.



Note: If no Printer Groups are available for selection, refer to **Creating Printer Groups** section to create a Printer Group.

- c. **Pull Print Queues:** This will install selected **Pull Print Queues** associated with this deployment group to every Client machine in the environment.

- To add the Pull Print Queues to this Deployment Group:
 - Click **Actions > Add**.
 - Select the check box of the **Pull Print Queues** from the list and click **Save**.

The selected Pull Print Queues are added to the Deployment Group.



Note: If no Pull Print Queues are available for selection, refer to **Queues** section to create a Pull Print Queues.

- To remove the Print Queues from this Deployment Group:
 - Select the check box of the required Pull Print Queues from the list, click **Actions > Remove**.

The selected Pull Print Queues are removed from the list.

- d. Click **Next**.

7. On the Summary, select the check box for **Enable Deployment Group** and click **Finish**.
A new Deployment Group is created and saved in the Deployment Groups.

VIEWING AND EDITING THE DEPLOYMENT GROUP

To view and edit the Deployment Group:

1. Click **Printers > Deployment Groups**.
2. Click on the required **Deployment Group** name.
3. The following tab appears:
 - **Details:** On the **Details** tab you can select the **Enable Automatic Deployment** and click **Save** to automatically download the Virtual Print Client application and install printers on the user desktop machines in this Deployment Group.

In this tab you can enable the Deployment Group, change Name and Description of the Deployment Group.
 - **Clients:** **Clients** tab allows you to change the Clients to **Deploy on all Client computers**, **Deploy printers to specific IP ranges of Client computers** or **Deploy printers based on User Groups** of the Deployment group.

In this tab you can change the Clients, add, or remove Client Computers or User Groups based on your Client selection for the Deployment Group.
 - **Printers:** **Printers** tab allows you to change the Printers to **All Printers**, **Printer Groups** or **Pull Print Queues**.

In this tab you can change the Printers, add or remove Printer Groups or Pull Print Queues based on your Printer selection for the Deployment Group.



Note: The number of printers per Deployment Group is limited to 25.

Supported Languages

- Arabic
- Catalan
- Czech
- Danish
- Dutch
- US English
- UK English
- Finnish
- French
- German
- Greek
- Hungarian
- Italian
- Japanese
- Norwegian
- Polish
- Portuguese
- Romanian
- Spanish
- Swedish
- Turkish

Xerox® Global Print Driver

Xerox® Workplace Cloud uses the 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 job programming attributes, such as 2-sided or staple, may not be supported. For more information on the GPD search for Global Print Driver on www.xerox.com. Select the **Compatible Products** tab for a list of compatible products.

Print Queues

This chapter contains:

- Print Queue Enablement 88
- Changing a Site Associated With a Print Queue 89
- Enabling or Disabling a Print Queue..... 90
- Setting Up Accounting for a Print Queue 91
- Assigning an Agent to a Print Queue 92
- Printing a Welcome Page for a Print Queue 93
- Removing a Print Queue..... 94

Print Queue Enablement

Print queues are not discovered in the same way as printers. To set up and enable a print queue, administrator credentials are required. Administrators can use the Add New Print Queue feature and enter the new queue information.

SERVER-BASED PRINT QUEUES

If your environment uses accounting packages that print through server-based queues, you will need to identify those print queue(s) on the **Print Queues** tab. They are also used by companies that print through queues, but do not use accounting. A company can use print queues with Xerox® Workplace Cloud, with or without an accounting package.



Note: Setting up the print queues properly is all that is required in order for a third party solution to work.

CREATING PRINT QUEUES

To create print queues:

1. From the Xerox® Workplace Cloud Web portal, select the **Print Queues** tab.
2. From the **Actions** menu, select **Add New Print Queue**.
3. Enter the queue information on the available tabs.



Note: Hover the cursor over the fields on the tabs to view a description of the fields.

4. To save the settings, click **Save**.

TESTING THE COMMUNICATION BETWEEN XEROX® WORKPLACE CLOUD AND THE PRINT QUEUE

Print queues are not automatically discovered by agents like printers are. You must manually add a print queue on the **Print Queues** tab. Once you enter the print queue information and save it, the print queue is added in an enabled state. It does not indicate that there is communication with the print queue. Print a welcome page to the print queue to validate that the information you entered is correct and the printer is working properly.

If you are unable to print using print queues, do the following:

1. From the Xerox® Workplace Cloud Web Portal, select a print queue from the **Print Queues** tab and click the print queue name.
2. Make sure the:
 - a. Print queue has an Assigned Agent on the **Agents** tab.
 - b. Agent is on the network and available.
 - c. Line Printer Daemon (LPD) Server, LPR/LPD Port, and Line Printer Remote (LPR) Queue Name are correct.
3. If the print queue is being used with an accounting package, make sure you have **Server-based Accounting** selected on the **Accounting** tab.
4. Verify that your agent PC can communicate with the print queue.

Changing a Site Associated With a Print Queue

To change the site:

1. From the Xerox® Workplace Cloud Web Portal, select the **Print Queues** tab.
2. Select one or more print queues.
3. Select **Change Site** from the **Actions** menu.
4. Select a site and select **OK**.

From the Edit Print Queue menu, do the following:

5. From the Xerox® Workplace Cloud Web Portal, select the **Print Queues** tab.
6. To change the site information, click the name of the queue.
7. Select the **Location** tab.
8. Change the site.
9. To update the queue, click **Save**.

Enabling or Disabling a Print Queue

Enabling a print queue will make it display for users on the **Print Queues** tab. The print queues also display with the printers on the **Print** tab for the user to select when printing. Disabling a print queue will remove it from the **Print Queues** and **Print** tab.

1. From the Web Portal, select the **Print Queues** tab.
2. Select one or more print queues.
3. Select **Enable Queue** or **Disable Queue** from the **Actions** menu.

From the Edit Print Queue menu, do the following:

4. From the Xerox® Workplace Cloud Web Portal, select the **Print Queues** tab.
5. Click the name of the queue.
6. To enable, select the check box for **Enable LPR Print Queue**.
7. To disable, deselect the check box for **Enable LPR Print Queue**.
8. To save the settings, click **Save**.

Setting Up Accounting for a Print Queue

To set the accounting mode:

1. From the Workplace Cloud Web Portal, select the **Print Queues** tab.
2. Select the required print queue name.
3. Select the **Accounting** tab.
4. In the **Set Accounting Mode** field, select one of the following modes:
 - **No Accounting**
 - **Server-based Accounting (User name only)**
 - **Server-based Accounting (User name and password)**
5. Select **Save**. Or,
6. From the Workplace Cloud Web Portal, select the **Print Queues** tab.
7. Select the required print queue name.
8. From the Actions menu, select **Set Accounting Mode**.
9. Select the required mode, and to update, click **Set Accounting Mode**.

Assigning an Agent to a Print Queue

Each print queue should be serviced by at least two agents for failover protection and load balancing. In large deployments, it is not recommended to have all print queues discovered by all agents. This increases network traffic.

To assign an agent:

1. From the Workplace Cloud Web Portal, select the **Print Queues** tab.
2. Select the required print queue.
3. Select **Agents**.
4. Select from the **Available Agents** list and use the arrows to add your selections to the **Assigned Agents** list.
5. Select **Save**.

Make sure the agent that you assign is on the network and available.

Printing a Welcome Page for a Print Queue

To print the welcome page:

1. From the Workplace Cloud Web Portal, select the **Print Queues** tab.
2. Select one or more print queues.
3. Select **Print Welcome Page** from the **Actions** menu.
4. Select a language and select **OK**.

Removing a Print Queue

To remove a print queue:

1. From the Workplace Cloud Web Portal, select the **Print Queues** tab.
2. Select one or more print queues.
3. Select **Remove** from the **Actions** menu.

Sites

This chapter contains:

- Adding a Site 96
- Changing the GPS Coordinates of a Site..... 97
- Removing a Site..... 98

A site is a logical group of printers that are usually at the same physical location. A site is displayed in the Xerox Workplace Cloud Portal app as a Push Pin in the Printer Map View or an entry in the Printer List View.

Adding a Site

To add a site, do the following:

1. From the Workplace Cloud Web Portal, select **Sites**.
2. From the Actions menu, click **New**.

The Add Site page appears.

3. In the Details area, type the required fields.

The following fields are:

- Name
- Country
- Address 1
- Address 2
- City
- County
- Time Zone
- Latitude
- Longitude
- Description

4. To save the setting, click **Save**.

Changing the GPS Coordinates of a Site

You can change a site to pinpoint a printer more specifically by changing the Latitude and Longitude settings.

To change a site, do the following:

1. From the Workplace Cloud Web Portal, select **Sites**.
2. From the list of sites, click the site name.

The Edit Site page appears.

3. In the Longitude and Latitude fields, update the values.
4. To update the site, click **Save**.

Removing a Site

To remove a site, do the following:

1. From the Workplace Cloud Web Portal, select **Sites**.
2. Select the check box next to the site from the list.
3. From the Actions menu, select **Remove**.

Agents

This chapter contains:

- Xerox® Workplace Cloud Agent..... 100
- Installation of an Agent 104
- Configuration and Settings of an Agent 105
- User Management 117
- Agent Management 119

Xerox® Workplace Cloud Agent

AGENT DESCRIPTION

An Agent is software running on a PC within the customer network that discovers print devices eligible to be used with the Xerox® Workplace Cloud, routes print jobs from the Cloud to printers, and provides general communication for other services, such as Authentication.



Note: Agent settings can be edited on both the Agent Computer and the Cloud Portal. The configuration setting may differ, refer to [Agent Settings on Agent Computer](#) and [Agent Settings on the Cloud Portal](#).

AGENTS - BEST PRACTICES

Printers and print queues can be serviced by more than one agent. Companies with a large number of printers and print queues should have multiple agents. Any agent that has a printer's IP address discovered and enabled will be used to print to that printer.

It is recommended that each printer or print queue is serviced by at least two agents for failover protection and load balancing.

In large deployments, it is not recommended to have all printers or print queues serviced by all agents. This increases network traffic. Using specific IP addresses or narrow IP Address ranges will decrease network traffic.

Any agent installed on a PC connected to a Lightweight Directory Access Protocol (LDAP) domain will report all available LDAP domains back to the Xerox® Workplace Cloud. In environments where LDAP domains are discovered by the agent, LDAP authentication may be enabled by the administrator.

WORKPLACE CLOUD DIRECT

You can auto enable the Workplace Cloud Direct setting on the printer during the printer discovery process using an Agent. For more information on enabling this setting, refer to [Auto Enablement of Remote Management](#).

SYSTEM REQUIREMENTS FOR THE CLOUD AGENT SOFTWARE

The following lists the minimum system requirements required to install the Workplace Cloud Agent software:



Note: Installation on a dedicated computer or virtual machine (VM) is required for the Xerox® Workplace Cloud agent software. Do not install the Agent on a Windows Domain Controller, because it is not supported.



Note: If you are using a Load Balancer, refer to [Using a Load Balancer With your Agent](#).

Supported Operating Systems and Configuration

- Ensure that the software is installed on the client computer using the Administrator account or an account with administrative privileges. Ensure that the software is configured for your organization.
- Microsoft.NET Framework 4.7.1
- Internet connection

Minimum:

- OS: Windows 10 or Windows 11 or Windows Server, 2016, 2019 or 2022
- CPU: Intel Core Duo CPU at 2.0GHz
- RAM: 4GB

Recommended:

- OS: Windows Server, 2016, 2019 or 2022
- CPU: Intel Core Quad CPU at 3.0GHz
- RAM: 8GB

Large Deployments: (200+ Printers)

- Supported Windows Server OS
- CPU: Dual (2) Intel Core Quad CPUs at 3.0GHz
- RAM: 16GB

REQUIRED AGENT PORTS

PROTOCOL	PORT	DESCRIPTION	CONFIGURATION	PATH
HTTPS using TLS	TCP 443	Retrieval of configuration, sending printer information, retrieval of print jobs, authentication	Non-configurable	Agent to Workplace Cloud
Raw IP	TCP 9100	Print Submission	Configurable	Agent to Printer
HTTPS	TCP 443	Azure Service Bus, with application-level encryption	Non-configurable	Agent to Workplace Cloud
LPR	TCP 515	Print Submission	Configurable	Agent to Printer or to Print Queue
IPP over SSL	TCP 443	Print Submission	Non-configurable	Agent to Printer
LDAP	TCP 389	Authentication	Non-configurable	Agent to ADS Server
LDAP over SSL	TCP 636	Authentication	Non-configurable	Agent to ADS Server
HTTPS using TLS	TCP 443	Convenience Authentication, EIP Registration, Accounting Data Configuration and Retrieval	Non-configurable	Agent to Printer
HTTPS using TLS	TCP 443	Authentication	Non-configurable	Agent to Azure AD

PROTOCOL	PORT	DESCRIPTION	CONFIGURATION	PATH
SNMP	UDP 161	Printer Discovery, Configuration	Non-configurable	Agent to Printer
LPR	TCP 515	Incoming Print Queue receives prints from LPR Clients	Configurable	LPR Client to Agent
HTTPS using TLS	TCP 443	Single Sign-On Requests or Responses	Non-configurable	Printer <--> Agent

USING A LOAD BALANCER WITH YOUR AGENT

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 Agents servicing the same printers, it is common to put the Agents behind an HTTP/HTTPS load balancer for authentication. The Load Balancer needs to be able to probe the Agent to determine if it is available and can handle an incoming request. This probe should specifically exercise the Agent web services endpoint and not perform a simple ICMP PING of the OS.

- The Xerox Workplace Cloud Agent support a single HTTPS based Load Balancer probe endpoint.

```
XWC Endpoint: https://<server>:443/ping
```



Note: No authentication is required to access this endpoint.

- After defining an Endpoint, the Workplace Cloud Agent 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.

FAILOVER FOR AUTHENTICATION

When a device is enabled for authentication, the device must have an IP address or Hostname to contact for verifying badge or manual authentication credentials. This authentication server target is sent to the device when configured by the agent and is normally the configuring agent's IP address.

This can be changed to be a load balanced IP address or Hostname when configuring an Agent on the **Details** tab under Authentication server address. In this case the agent will push the configured target IP or Hostname for the printer to authenticate against.

Multiple agents can be configured to discover the same printer and all of these multiple agents can push out to the printer the same configured IP address or Hostname. When the printer attempts to authenticate the load balancer will route to either agent that discovered the printer and process authentication requests.

LOAD BALANCER REQUIREMENTS

A load balancer for agent authentication has the following requirements:

1. The load balancer must have some degree of stickiness for a session. A user might swipe a badge, enter an email address then a Hostname. All these actions must be performed on the same agent meaning an agent should have at least the expected duration of the user's session in terms of stickiness. Setting 5 minute stickiness is a good average number that is expected to be appropriate in virtually all workflows.
2. The agent must have the ability to determine the IP address or the printer requesting to authenticate. Some load balancers replace the IP address of the client on a networking level. In this case the original client IP must be provided in the X-Forwarded-For header (refer to <https://en.wikipedia.org/wiki/X-Forwarded-For>).
3. Alternatively, some load balancers might work simply on the DNS level and simply redirect to the appropriate agent. In this case if the client IP on the network connection is still the printer, no additional work needs to be done.

Installation of an Agent

SETTING UP A NEW AGENT

1. Access the Web portal. Log in as an administrator or an agent.
2. From the Web Portal, click the **Agents** tab, then select **Local > Actions > New**.

The Agent Setup page appears.

3. In the Details section, in the Friendly Name field, type the required name. Click **Next**.
4. In the Site section, select one of the following sites:
 - **Select an Existing Site:** This option allows you to select an existing site that appears in the list.
 - **Create a new Site:** This option allows you to create a new site.



Note: After you set the site of the agent, you cannot modify it.

5. In the Discovery Settings area, select the **Discovery Settings** tab.
6. To add the discovery setting, refer to [Adding a Printer Using an Agent](#). Click **Next**.
7. In the **SNMP Settings** tab to manage SNMP settings, refer to [Manage SNMP settings](#). Click **Next**.
8. In the **Exclusions** tab, to add the exclusions, refer to [Excluding Printers or Subnets From Discovery by the Print Agent](#). Click **Next**.
9. In the iOS Native Printing, to enable the settings, refer to [iOS Native Printing](#). Click **Next**.
10. In the Incoming Print Queue, in the Print Queue Information area, select one of the following required option:
 - **Enable LPR Print Queue**
 - **Enable Windows Shared Print Queue**
11. Click **Next**.

The Create Print Agent page appears.

12. In the Verify section, verify the information and click **Next**.

The Download page appears. You can view the following information:

- Agent Name
- Site
- Agent Code

13. To download the agent installer, click **Download the Xerox Workplace Cloud Agent Installer**. Click **Finish**.
14. To obtain the agent activation code, complete the **Agent Wizard**.
15. On your local PC or server, download and install the agent software.
16. Provide login information and the Agent Code. The agent searches for available printers in the same subnet.

When you register the agent, ensure that you log in to the Xerox® Workplace Cloud using the company code of the account that belongs to that agent.

Configuration and Settings of an Agent

LOGGING THE AGENT IN TO THE XEROX® WORKPLACE CLOUD

1. Verify the Xerox® Workplace Cloud Agent displays in the notification tray area. It is called Xerox® Workplace Cloud.
2. Move the mouse cursor over the icon and right-click the icon to open the menu.
3. Select Login to Xerox® Workplace Cloud, and login using the credentials you used when you set up your user account.

AGENT SETTINGS ON AGENT COMPUTER

Discovered Printers

The Discovered Printers Options

There are three options in the **Discovered Printers** tab, as follows:

- **+**: This option allows you to enter the IP address of a printer and add it.
- **Enable Printers**: This option allows you to enable the printers.
- **Printers Search**: This option allows you to initiate a manual printer discovery. For more information, refer to [Updating Discovered Printers](#).

Updating Discovered Printers

Printer discovery is automatically run by each agent every 7 hours. To initiate a manual printer discovery, do one of the following:

- Go to the Agent:
 - a. Select the **Discovered Printers** tab.
 - b. Select **Printer Search**.
- Go to the Workplace Cloud Web Portal:
 - a. Select **Agents > Local**.
 - b. Select an Agent.
 - c. Select **Start Printer Search**.

Configuration Settings

Auto Update

To enable or disable this setting, refer to [Policies: Agent Upgrades](#).

iOS Native Printing

When you enable **iOS Native Printing**, Xerox® Workplace Cloud printers use the built-in printing capability on iOS

13.0 and later devices. You can submit print jobs to the Xerox® Workplace Cloud solution using the built-in printing capability of your iOS device. Later, you can release the jobs to any Xerox® Workplace Cloud-enabled printer using the Xerox® Workplace Mobile App application. You can release the jobs using the @PrintByXerox App on Xerox EIP capable printers. A printer named Xerox® Workplace Cloud, including the name of the servicing agent, appears on your iOS device printers list.

To enable iOS Native Printing with Auto Discovery:

1. Install the print services software on the Agent PC:
 - a. Go to <http://support.apple.com/kb/DL999>, then download and install Bonjour Print Services for Windows®.
 - b. After you install the printing software, restart the Agent.
2. Set up iOS Native Printing on the Xerox® Workplace Cloud Web Portal:
 - a. Select **Agents > Local**.
 - b. Select a specific print agent.
 - c. Select the **iOS Native Printing** tab.
 - d. Select the **Enabled** and **Automatic Discovery** check boxes.
The **Automatic Discovery** setting is optional
 - e. Click **Save**.

For the iOS device to find Xerox® Workplace Cloud in native iOS apps, place the print agent and the iOS device on the same subnet. To enable iOS Native Printing across different subnets, refer to [Setting Up the DNS-SD for iOS Native Printing](#).

Proxy Settings for the Agent

By default, the browsers proxy settings are picked up when the agent is installed. They may be updated in the Xerox® Workplace Cloud Agent on the **Configuration Settings** tab.

Discovery Settings

After you set up Xerox® Workplace Cloud Agent, you can modify the discovery settings for the Agent. You can export discovery settings from an existing Agent and import them to another Agent, using IPv4 or a Fully Qualified Domain Name (FQDN).

For more information, refer to [Discovery Settings Tab](#).

LDAP Support

There are two methods for adding LDAP Domains to your Agent:

- [Automatic LDAP Listing](#)
- [LDAP Domain Override](#)

Automatic LDAP Listing

An agent installed on a PC joined to a domain will display available domains. When using Lightweight Directory Access Protocol (LDAP) Authentication it is recommended that you have at least two agents on the domain for failover protection.

1. On the Agent PC, open the Agent and select the **Configuration Settings** tab.

2. In the **LDAP Support** section, select **View LDAP domains**.

A list of available domains displays.



Note: To enable LDAP Authentication by an Agent, you must login to the Agent PC with a domain account. This must be done on each agent PC in order for it to discover domains.



Note: If LDAP domains are not shown in the Agent UI, try the following:

- Log out of the Agent, then log in with your workplace credentials (domain\username and password).
- Manually restart the Xerox® Workplace Cloud Agent service.
- Restart the Agent PC.

LDAP Domain Override

LDAP Domain Override method allows you to add Domains manually to ensure that all the client Domains are included for LDAP authentication.

Guidelines:

- This functionality is supported in Workplace Cloud agent versions 5.7.309 or higher.
- When using the Domain Override setting, network Domains will not be added automatically.

Setting up the LDAP Domain Override

To set up the Agent LDAP Domain Override do the following:

Guidelines:

- The two files ldapdomainoverride and ldapdomains.info which you need to edit are created automatically when the Agent is run for the first time.
 - All the discovered Domains will be listed in the ldapdomains.info file, and you will need to edit this file to add the required Domains.
 - When you add your Domains to the ldapdomains.info file keep the Scanning Date after the last domain name.
1. Navigate to C:\ProgramData\Xerox\xmpcagent.
 2. Open the file named "ldapdomainoverride".
 3. Change {"overrideLDAP": FALSE} to {"overrideLDAP": TRUE} and click **Save**.
 4. Browse to \ProgramData\Xerox\xmpcagent.
 5. Open the file named "ldapdomains.info".
 6. Add all required Domains and click **Save** and restart the Workplace Cloud Agent service.



Note: Enter the Domain Name in the following format separated with comma (,), you should not manually update the Scanning Date.

Example: {"Short Domain Name1": "Full Domain Name1", "Short Domain Name2": "Full Domain Name2", "ScanningDate": "MM:DD:YYYY hh:mm:ss AM/PM" }

The Agent LDAP Override functionality is settled up successfully.

LDAP Connectivity Issues

The Xerox® Workplace Cloud Agent will report available domains.

To see all available domains:

1. Make sure the Agent PC is joined to a domain.
2. Open the agent on the Agent PC to display the Agent UI.
3. Select the **Configuration Settings** tab.
4. Under **LDAP Support**, select **View LDAP domains**.

If your domain is not displayed in the Available LDAP Domains, try the following:

- Log out, then log in with your workplace credentials (domain\username and password).
- Manually restart the Xerox® Workplace Cloud Agent service.
- Restart the Agent PC.
- Try the Domain Override configuration file method.

To enable Lightweight Directory Access Protocol (LDAP) Authentication by an Agent, you must log in to the Agent PC with a domain account. This must be done on each agent PC to enable domain discovery.

If LDAP connectivity is not available, administrators will be able to log in with Xerox® Workplace Cloud account credentials.



Note: This login procedure is available for administrators only.

Incoming Print Queue

You can view the status of the Incoming Print Queue feature. An Incoming Print Queue allows the Agent to accept print submission requests from external third party clients. For more information, refer to [Enabling Incoming Print Queue](#).

Agent Offline Mode

Agent Offline Mode is a feature of the Xerox® Workplace Cloud Agent that is installed on the computer. Agent Offline Mode provides the information about Xerox® Workplace Cloud connectivity issues and the status of Xerox® Workplace Cloud. When the Xerox® Workplace Cloud Agent cannot connect to Xerox® Workplace Cloud, Agent Offline Mode enables you to release the Follow-You print jobs and to access the home screen of the printer.

There are two ways that you can set Agent Offline Mode:

- **Automatically:** Offline mode activates automatically when Xerox® Workplace Cloud is offline or unresponsive. When Offline mode is activated, in the Configuration Settings tab, the Offline mode status appears as `Offline`, and the Modify option is disabled. When the Xerox® Workplace Cloud connection is restored, the Modify option is enabled, and the status appears as `Automatic`. Automatic is the default option for new and existing users.
- **Manually:** When there are intermittent connectivity issues or planned outage events, the agent administrator can activate Agent Offline Mode manually. If you enable Offline mode manually, the `Offline` status is in place until you disable Offline mode. When Xerox® Workplace Cloud is offline, it enables Offline mode automatically. When Xerox® Workplace Cloud is restored or online, it disables Offline mode automatically.



Note: When Offline mode is enabled automatically, it is not possible to disable it manually.

Determining if the Agent is Manually Set to in Offline Mode

To determine if a Xerox® Workplace Cloud Agent is set to Offline Mode, do the following:

1. Go to the computer where the Xerox® Workplace Cloud Agent is installed.
2. Log in to the Xerox® Workplace Cloud Agent user interface.
3. Click the **Configuration Settings** tab. If Offline mode is enabled, in the Offline Mode area, the status `Offline` appears.

Enabling Agent Offline Mode Manually

If you experience issues with Xerox® Workplace Cloud, an administrator can force the Xerox® Workplace Cloud Agent into Offline mode. To enable Agent Offline Mode, access to the Xerox® Workplace Cloud Agent computer is required. Do the following:

1. Log in to the Xerox® Workplace Cloud Agent user interface.
2. Select the **Configuration Settings** tab.
3. In the Offline Mode area, do the following:
 - a. Click **Modify**.

The Modify Configuration window appears

 - b. For Agent Offline Mode, select **Offline**.
4. To confirm the changes, click **OK**, or to cancel your changes, click **Cancel**.

In the Configuration Settings tab, the Offline Mode status appears as `Offline`, and the Modify option is enabled.

Disabling Agent Offline Mode Manually



Note: You can disable Agent Offline Mode manually, if it was enabled manually. Ensure that the Offline Mode status appears as `Offline` and the Modify option is enabled.

To disable Agent Offline Mode manually, access to the Xerox® Workplace Cloud Agent computer is required. Do the following:

1. Log in to the Xerox® Workplace Cloud Agent user interface.
2. Select the **Configuration Settings** tab.
3. In the Offline Mode area, do the following:
 - a. Click **Modify**.

The Modify Configuration window appears

 - b. For Agent Offline Mode, select **Automatic**.
4. To confirm the changes, click **OK**, or to cancel your changes, click **Cancel**.

In the Configuration Settings tab, the Offline Mode status appears as `Automatic`, and the Modify option is enabled.

AGENT SETTINGS ON THE CLOUD PORTAL

Icons in the Agent Settings

There are four icons in the **Agents** section, as follows:

- **Pencil Icon:** This option allows you to edit the agent settings. For more information, refer to [Editing Agent Details](#).
- **Printer Search Icon:** This option allows you to run a printer search manually. For more information, refer to [Updating Discovered Printers](#).
- **Remove Icon:** This option allows you to remove the agent. For more information, refer to [Deleting an Agent](#).
- **Update Icon:** This option allows you to download the latest version of the agent software. If you see this icon, it means that your agent software is in earlier version and an update is available

Editing Agent Details

To edit an existing agent, do the following:

1. Log in to the Xerox® Workplace Cloud Web portal as an administrator or an agent.
2. Select **Agents > Local**, then select the check box next to the agent that you want to edit.
The Print Agent Details page appears.
3. In the Details section, do the following:
 - a. To edit the name, in the Friendly Name field, edit the required name.
 - b. In the Authentication Server field, select one of the following:
 - **Automatic:** By default, the selection is **Automatic**.
 - **Manual (IPv4 address or Host Name):** Select this option if you use a load balancer for the agents. If you select this option, enter the IP address or host name of the load balancer, then repair the printers that are connected with agent. For more information on setting up an agent load balancer, contact your Xerox representative.
 - c. Click **Save**.
4. To modify Discovery Settings, select the **Discovery Settings** tab. For more information, refer to [Discovery Settings Tab](#).
5. To modify SNMP Settings, select the **SNMP settings** tab. For more information, refer to [Manage SNMP settings](#).
6. To modify Exclusions, select the **Exclusions** tab. For more information, refer to [Excluding Printers or Subnets From Discovery by the Print Agent](#).
7. To modify iOS Native Printing, select the **iOS Native Printing** tab, refer to [iOS Native Printing](#). Click **Save**.
8. To modify incoming print queue, select the **Incoming Print Queue** tab. In the Print Queue Information area, select one of the following required options:
 - **Enable LPR Print Queue**
 - **Enable Windows Shared Print Queue:** For more information, refer to [Enable Windows Shared Print Queue](#).

9. To modify User Management, select the **User Management** tab. For more information, refer to [User Management](#).
10. Click **Save**.

Deleting an Agent

To delete or remove an agent, do the following:

1. Access the Web portal. Log in as an administrator or an agent.
2. Select **Agents > Local**, then select the check box next to the agent that you want to delete.
3. From the Actions menu, click **Remove**.

The Xerox® Workplace Cloud dialog box appears.

4. At the confirmation message, to delete the file, click **OK**, or to cancel the deletion, click **Cancel**.

Discovery Settings Tab

The Discovery Settings of a Xerox® Workplace Cloud Agent feature provides options that enable you to define the IP Addresses to use to search for printers, and to export discovery profiles:

- **Add Settings:** This option allows you to add printer settings.
- **Import Profile:** This option allows you to import a discovery profile from another agent. For more information, refer to [Importing a Discovery Settings Profile](#).
- **Export Profile:** This option allows you to export a discovery profile. For more information, refer to [Exporting a Discovery Settings Profile](#).

If the Discovery settings are not defined, the Xerox® Workplace Cloud Agent discovers the printers in the same subnet as the Agent computer.

Adding a Printer Using an Agent

To add a new printer, the IP address of the printer is added to the discovery settings of at least one agent. To direct jobs to a printer, an agent needs to be able to discover the printer. To add the necessary IP addresses to the agents in the account, do the following:

1. From the Workplace Cloud Web Portal, select the **Agents > Local** tab.
2. Select the check box next to the agent that you want to edit.
3. Select **Discovery Settings**.
4. Select **Add Setting**.
5. Add the printers.
Options for adding printers are:
 - Description
 - IPv4 Address
 - IPv4 Range
 - IPv6 Address
 - DNS Name

6. Select **Save**.



Note: Once you add the printer on the **Agents** tab, you enable it on the **Printers** tab.

Exporting a Discovery Settings Profile



Note: The exported discovery settings have a type, which is either IPv4 Address or DNS Name.

To export a discovery profile, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an agent administrator or account administrator.
2. Click the **Agents > Local** tab.

The Print Agents window appears.

3. Select the required agent.
4. Click the **Discovery Settings** tab.
5. In the Settings area, click the **Actions** menu, then select **Export Profile**.
The settings are exported to a .csv file, which has the following columns:

- Description: The description of the setting.
- Type: The setting type, which is either IPv4 Address or DNS Name.
- Value: The IPv4 address of the Fully Qualified Domain Name (FQDN).

The .csv file is downloaded to the computer. The format of the file name is AgentDiscoveryFile_MMDDYYYY.csv.

6. To exit the window, click **Close**.

Importing a Discovery Settings Profile

To import a discovery profile, do the following:

1. Log in to the Xerox® Workplace Cloud Web portal as an agent administrator or account administrator.
2. Select **Agents > Local**.
The Print Agents window appears.
3. Select the required agent.
4. Click the **Discovery Settings** tab.
5. To import the discovery settings, in the Settings area, click the **Actions** menu, then select **Import Profile**.

The Import Discovery Settings window appears.

- To upload a file, click **Choose File** or **Browse...**, then browse to the location of the .csv import file on your computer. Click **Open**.

The supported file format for importing discovery settings is .csv. Ensure that the file has the following columns and that there is one row for each import item:

- Description: The description of the setting.
- Type: The type is either IPv4 Address or DNS Name.



Note: If you do not specify IPv4 or DNS Name as the type for an entry, that row does not import and the entry is flagged as a line with errors.

- Value: The IPv4 address of the Fully Qualified Domain Name (FQDN).

- To continue, click **Confirm**, or to cancel the import, click **Cancel**.

After you import the .csv file, the Import Discovery Settings window appears, which shows the following information:

- Total Lines in Import File
- Total Lines Imported Successfully
- Total Lines with Errors

- To view the results and any status or error messages, click **Download Status File**, or to complete the import, click **Finish**.

Editing Printer Discovery Settings for an Agent

- From the Workplace Cloud Web Portal, select **Agents > Edit > Discovery Settings**.
- Select **Edit** for the discovery setting you want to change.
- Make the required changes, then select **Save**.

Deleting a Printer From an Agent

- From the Workplace Cloud Web Portal, select the **Agent** tab.
- Select the Agent from which you wish to delete the printers.
- Click **Edit**.
- Select **Discovery Settings**.
- Locate the discovery parameter, range, or setting that applies to the printer.
- Select **Delete**.



Note: To make sure the printer is no longer seen, you will need to remove the printer from each Agent that has the printer in its discovery parameters.

Determining the Agent to Which a Printer is Connected

A printer can be discovered by multiple agents, which enables failover and load balancing. To determine which agents are discovering a particular printer, verify the discovery settings of each agent. From the Web Portal, select **Agents > Local > Edit > Discovery Settings**.

Entering a Range of Printers for my Agent

Perform a printer discovery on your agent:

1. From the Workplace Cloud Web Portal, select **Agents > Local > Edit Agent > Discovery Settings > Add Setting > IPv4 range**.
2. Enter a **Start Address** and **End Address** and click **Save**.

You can enter individual IP addresses 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 by Xerox® Workplace Cloud, it can create unnecessary network traffic because the solution attempts to communicate with each IP address. This IP discovery scan is run multiple times each day.

Recreating an Agent When You Replace the Hard Drive

If your hard drive is replaced, you cannot restore the agent from a backup disk image, because Xerox® Workplace Cloud uses the hard drive ID to uniquely identify an agent. To recreate and Agent, do the following:

1. From the Xerox Workplace Cloud Web Portal, select the **Agents** tab and click the Agent associated with the replaced drive.
2. Click **Edit > Discovery Settings** and record:
 - Discovery Settings
 - SNMP Settings
 - Exclusions
3. Uninstall the agent from the PC.
4. Go to the **Agents** tab and select **New** from the **Actions** menu. Follow the Wizard to create a new agent.



Note: Use the settings that you recorded from the original agent for the new agent.

5. Go to the **Agents** tab and remove the original agent that is no longer used.

Manage SNMP settings



Note: Ensure that the SNMP setting is enabled on the printers before managing the SNMP settings on the Workplace Cloud.

SNMP settings update the SNMP version and credentials used by the Xerox® Workplace Cloud on all selected printers in the printers grid.

There are two options in Set SNMP Settings: SNMP v1/2 and SNMPv3, users can select one of the SNMP options.

Workplace Cloud supports SNMP configuration in the following places:



Note: The SNMP Setting can be entered in Multiple places in Workplace Cloud, if the SNMP Setting is blank on the **Printers** tab, then the Agent or Cloud Direct SNMP setting is used. The SNMP setting entered on each **Printers > SNMP Settings** tab is used as the priority setting, which will override the SNMP settings entered on the Agent or Cloud Direct tab.

- For configuring SNMP settings for each printer, select **Printers > All**, edit printer **SNMP Settings** tab.
- For configuring SNMP settings for multiple printers during the addition of a new Agent, select **Agent > Local > Action > New > Discovery > SNMP Settings** tab.
- For Configuring the SNMP settings for an existing **Agent**, select **Agent** edit agent **SNMP Settings** tab.
- For configuring SNMP settings for Cloud Direct printers, select **Agent > Workplace Cloud Direct > SNMP Settings**.

Guidelines:

- Each printer can have only one SET and GET Community Name.
- The SNMP v1/v2 Community String can be changed other than the default value on your devices to decrease the security risk.
- If you have changed the printer SNMP Community Names, ensure that the updated Community names are listed on the Agent SNMP settings for proper communication.
- SNMP V3 is not supported when printers are functioning with Workplace Cloud Direct mode (managed without an agent).

Setting Up the SNMP setting:

To set up the SNMP setting do the following steps:

1. On the Administration Settings, provide the `Username` and `Password`, leave blank if you want the system to use the default settings.
2. Select the required SNMP version.
3. If you select **SNMP v1/v2**, leave blank if you want the system to use the default settings or provide the **SET Community Name** and **GET Community Names** as follows:
 - For SET Community Name, `private` is the default value, if you decide to set other names ensure that the SET Community name is identical between Xerox® Workplace Cloud and the printer SNMP setting.
 - For GET Community Name `public` is the default value, if you decide to set other names ensure that the GET Community name is identical between Xerox® Workplace Cloud and the printer SNMP setting.



Note: You can enter multiple GET Community Names on the Agents SNMP section for sorting and discovering the printers based on GET Community Names.

4. If you select **SNMP V3** do the following:
 - a. On the User Name section enter the `Username` of the administrator account.
 - b. On Context Name provide the collection of management information that will be accessed on the printer.



Note: It is not mandatory to provide the Context Name.

- c. Select the Encryption as **MD5 / DES** or **SHA1 / AES-128**.
- d. In the **Access Method** section provide the `Authentication Password` and `Privacy Password`.

Excluding Printers or Subnets From Discovery by the Print Agent

1. From the Web Portal, select the **Agent** tab.
2. Select the Agent from which you wish to exclude printer(s).

3. Click **Edit**.
4. Select **Exclusions** and then select **Add Setting**.
5. Add the IP address or range you wish to exclude and select **Save**.

Enabling Incoming Print Queue

To enable **Incoming Print Queue**, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an agent administrator or account administrator.
2. Click the **Agents** tab.
The Print Agents window appears.
3. Select the required agent.
4. Click the **Incoming Print Queue** tab.
5. In the Print Queue Information area, select the check box for one of the following options:
 - **Enable LPR Print Queue:** This option allows you to enter the LPR/LPD Port number. For more information, refer to [Enable LPR Print Queue](#).
 - **Enable Windows Shared Print Queue:** For more information, refer to [Enable Windows Shared Print Queue](#).
6. Click **Save**.

Enable LPR Print Queue

It is expected that the when you submit client, it sends both the user identification of the job and the queue name of the printer (-Q option) to which the job is sent as a part of the LPR protocol, If queue name is not included, or an unknown name, for example LPQ is used, the job is uploaded to the cloud for release at a later time.

Enable Windows Shared Print Queue

Because the Xerox® Workplace Cloud software solution does not have a client for Linux currently, jobs from Linux operating systems are sent to a Windows network shared queue through the Xerox® Workplace Cloud Agent. When jobs are queued to the Agent, for an additional security, it is essential to incorporate an authentication mechanism.

An administrator creates a network shared queue and attaches the Xerox® Workplace Cloud port monitor, which is available on the Agent computer.

When you enable the **Enable Windows Shared Print Queue** setting, jobs received from this network shared print queue are uploaded to Xerox® Workplace Cloud. When the authenticated mechanism is set to LDAP, the Enable Windows Shared Print Queue setting is the best suited. Ensure that the users authenticate with this network shared queue. The user credentials are sent to Xerox® Workplace Cloud along with the job data.

User Management

The **User Management** feature enables user accounts in Xerox® Workplace Cloud to be deleted, updated, or added using a CSV file imported by the agent.

Guidelines for User Management Feature:

- The **User Management** feature will not be available when you add a new agent, it is accessible when you edit an agent.
- The User template files are accessed by configuring a UNC path that the agent will use to monitor for the User CSV files.
- To download the template file for importing Users, go to the **Users** tab and select **Actions** menu, then select **Import Users from File** option and select Download Import Template.
- To download the template file for deleting Users, go to the **Users** tab and select **Actions** menu, then select **Delete Users from File** option and select Download Delete from File Template.
- How does the system know whether to import/update or delete users: The process consuming the import file looks at the fields in the file. Use the template files to ensure correct updates.
- The agent will check the UNC path every minute for a User CSV file.
- The import files will be deleted upon completion and will not be stored.
- The UNC path must be unique for every agent.
- An email will be sent to the Administrators after the User CSV file is processed, this will include a status file.
- The **History** section provides the details on the Agent Last Run in the Xerox Workplace Cloud portal.

The Last Run details are as follows:

- Total Users in the file.
- Total Users imported or deleted.
- Total Users failed.

Steps to configure:

1. Check the **Enable** box.
If disabled, the UNC path and notes section will not be shown.
2. Specify a UNC path that the agent has access to read or write.



Note: If the UNC path is blank or invalid, the User will get an error message to be addressed.



Note: If the UNC path folder is on a remote server file share, in order for the Agent to fully access the UNC folder ensure that the Agent computer identity "**domain\machine name\$**" is assigned as the full control of the folder.

3. To add or update Users, download the template file, go to the **Users** tab and select **Actions** menu, then select **Import Users from File**, then select Download Import Template.
4. To delete Users, download the template file, go to the **Users** tab and select **Actions** menu, then select **Delete Users from File**, then select Download Delete from File Template.
5. Edit the User CSV template file accordingly.

6. Copy the updated User CSV file to the folder pointed to by the UNC path.



Note: An example for a UNC Path: **\\server\path\file**. The import file specified must be based on the templates outlined above. The agent must have access to read or write the UNC path. By default, the Xerox® Workplace Cloud Agent Service runs as Local System. To access remote shares requiring authentication, the identity (log on as) of the service can be updated. When populated, the agent will check the UNC path every minute.



Note: This feature requires version 5.8.300 or higher of the Xerox® Workplace Cloud Agent.

The History section provides the details on last run.

Additional information will be sent by email to Users with the **Administrator** role.

7. To save the settings click **Save**.

Agent Management

UPGRADING AN AGENT MANUALLY

When agents become eligible for upgrade, you will receive an email notification in the following cases:

- If you have disabled automatic upgrade of your agents
- If an agent is not eligible for auto-upgrade


This email notice indicates that an upgrade is available for the agent and provides a download link to the new agent software. Download and install the newer version. It will automatically perform an uninstall of the old Agent software before installing the new Agent. During this uninstall, the shutdown of the old Agent services may take a while, so you may receive some Windows messages. Each agent must be upgraded individually.


A message may display that indicates the setup was unable to automatically close all requested applications. Click **OK** to this message.

A message may display that indicates the Xerox® Workplace Cloud should be automatically closed. Ensure the radio button for **Automatically close applications** is selected then click **OK**.

A Xerox® Workplace Cloud Agent message may display with an Error 1306. Click **Retry**. Due to the amount of time needed for the service to shut down, this may need to be done more than once.


During the upgrade process, the Agent service is shut down for a short time. To provide uninterrupted access to printers by Xerox® Workplace Cloud users, make sure that the printers in the Discovery Settings of that agent are also covered in the Discovery Settings of another agent, or those printers will be unavailable during the agent installation and registration.

 Note: The Xerox® Workplace Cloud Agent icon is normally available in the system tray of the agent PC. If the icon is not present, manually start the agent user interface from the PC's Start menu.

 Note: If you have created multiple accounts and receive an upgrade message, please ensure you are logged into the company that uses the agent with the correct Company Code before attempting to upgrade the agent.

KNOWING WHEN AN AGENT NEEDS AN UPGRADE

On the **Agents** tab of the Web Portal, in the Agent detail area, a yellow triangle displays next to the version number. This indicates that agent software version is no longer supported and should be upgraded. If this agent was upgraded prior to the Xerox® Workplace Cloud version 1.5 release, it must be upgraded manually even if you have automatic upgrade enabled. In some cases, the existing version of agent software may no longer be supported and must be upgraded in order for Xerox® Workplace Cloud to continue working as expected.

 Note: Agent software version 2.2 and newer supports auto-upgrade.

UPDATING THE AGENT ON THE WEB PORTAL

Perform the following on the computer on which the Agent is installed:

1. To uninstall the old Agent from your computer, go to: **Control Panels > Programs > Uninstall a Program** and select **Xerox Workplace Cloud Agent**.

2. Go to <https://xwc.services.xerox.com>.
3. Select the **Agents** tab, scroll down to the bottom the page and click **Download Agent Installer**.
4. Save the installer file to your computer.
5. Open the installer and follow the on screen instructions.
6. Once it is installed, open the Xerox® Workplace Cloud Agent. If required, login with your existing credentials.
7. On your computer, go to the **Start** menu and type **Services** in the **Search** field. Select **Services** to open it.
8. From the Services window, scroll down to **Xerox Workplace Cloud**, right-click, and select **Restart** or **Start**.
9. Log in to your Agent as an administrator at <https://xwc.services.xerox.com>.
10. Click the **Agents** tab, click your Agent name to open the Agent, then select the **Discovery Settings** tab and add or verify the IP range for your printers.
11. Click the **Agents** tab and select the small printer icon to **Start Printer Search** on your agent.
12. When the printer search is complete, you may print to the Agent.

CHECKING THE VERSION OF YOUR AGENT

If you are running an older version of the Xerox® Workplace Cloud Agent and are experiencing connectivity issues, you may need to update to the latest version of the Agent and/or restart the Agent services.

1. Open the Agent software installed on your computer.
2. From the Xerox® Workplace Cloud window, in the lower right corner, click the “i” icon.
3. Check the Agent Version on the Xerox® Workplace Cloud pop-up window.

FINDING THE AGENT CODE

Select the **Agents** tab on the Web Portal. The Agent Code is listed with the details for your agent. It was also emailed to you when you created the agent. The Agent Code is used when registering an agent after an installation or upgrade.

REMOVING AN AGENT AFFECTS PRINTERS

If you remove an agent, make sure that any printers that are discovered by it are also discovered by another agent or you will not be able to print to that printer any more.

SWITCHING FROM USING AN AGENT TO AGENTLESS

This capability is only available for Xerox® AltaLink® and VersaLink® devices. Follow these steps to switch from using a Xerox® Workplace Cloud Agent to using no Agent:

1. Log in to the Xerox Workplace Cloud Web portal at <https://xwc.services.xerox.com>.
2. Select **Printers**.
3. Select the check box for the printer you want to use for Agentless printing.
4. Select **Actions > Set Client Application Installation Mode**.

5. Deselect the **Install the client application on the device** check box, and select the **Set Client Application Installation Mode** button.
6. Select **Actions > Disable Printer**.
7. Select the check box for the printer again, and then select **Actions > Remove > OK**.
8. Select the **Agents** tab.
9. Click the name of the agent that was discovering the printer to view the printer details, then do one of the following options:
 - a. If it is a single device, select the **Discovery Settings** tab and delete the printer. -or-
 - b. Click **Exclusions > Add Setting** and create an exception for the agent to ignore DNS Name of a specific printer or IPv4 Range (IP address range). Click **Save** when finished.
10. Use the Xerox App Gallery to install the Xerox® Workplace Cloud AltaLink® and VersaLink® app on your Multifunction Printer.
11. From the UI of the printer:
 - a. Log in to the printer as an administrator.
 - a. Log in to the @PrintByXerox printer app.
12. Select the **Administrator** button and register and enable the printer.

If you have multiple agents, repeat these steps for each agent or account that has discovered the printer.

If you skip step 12, the printer runs in **Basic** mode.

If you get the error message that reads “Sorry, You Are not authorized to use this printer,” you have another agent running that has discovered the same printer, so repeat the steps above for each agent.

Users

This chapter contains:

Users 124

User Groups 134

Users

The **Users** tab is where you can manage the list of users who can access Workplace Cloud.

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 displayed per page.

The **Search Fields** allows you to enter information to find the specific users from the Users list.

The **Default Search Fields** allows you to search the following user fields:

- Email
- Username
- Alternate Access

The **Cards/Managed PINs** allows you to search the following user fields:

- Card Numbers
- Managed PINs



Note: The Auto Generated Pin number cannot be searched using the search options.

USER: DETAILS

To edit user details, do the following:



Note: Some of the editing capability of the User is done on the **Actions** menu on the **Users** tab. See below for details.

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select the **Users** tab.
3. Select the user's email from the list.

The Edit User page appears.

4. Click **Details** tab. Edit the following fields as required:
 - Email Address: Displays the email address of the user.
 - Username: Displays the user name of the user.
 - Domain Name: Displays the domain name of the user account.
 - User Principal Name: Displays the User Principal name. This is a read-only value and applicable to Azure AD, OKTA, and HelloID Authentication. If using LDAP or Cloud Authentication the value appears blank.
 - Alternate Access Card User: Displays the name of alternate access card user. For more information, refer to [Alternate Access Card User](#).
 - Role: Displays the role of the user
 - Department: By default, the Department text field is blank. In the text field, type the department name, if needed.
 - Default Card: By default, the Default Card text field is blank. In the text field, type the card number.
 - Registered Cards/PINs: This option appears when you enable the Allow Multiple Primary PINs or Access Cards feature. To enable Allow Multiple Primary PINs or Access Cards, refer to [Enabling Allow Multiple Primary PINs or Access Cards](#). The Registered Cards/PINs option has two text fields with the arrow options. After you save the details, you can view the registered cards.
 - User devices: Displays the number of devices associated with the user.
 - Override Print Quota Rules: For more information, refer to [Setting Override Print Quota Rules for Individual Users](#).
5. To view the user information, click **Groups** tab.
The following information appears in the grid:
 - Name
 - Association Type
 - Description
6. To view the rules associated with the user, click **Rules** tab.
The following tabs are available:
 - **Print Controls:** For more information, refer to [Print Controls](#).
 - **Print Quotas:** For more information, refer to [Print Quotas](#).
 - **Print Limits:** For more information refer to [Print Limits](#).
7. To add or edit delegates, click **Delegates** tab. For more information, refer to [Delegates](#).
8. To save the settings, click **Save**.

Alternate Access Card User

The Alternate Access Card User field is used to store an alternate user name value for the user. LDAP or Azure AD field mappings are not available for this field. The Alternate Access Card User field is imported using the existing .csv import mechanism for new and existing users.

The Alternate Access Card User field is used to resolve jobs from the LPR queue job submission path to the correct user account. When the user is authenticated, the Alternate Access Card User field is used to allow LPR submitted

jobs which are tied to the alternate access card user to appear in the EIP application in the LPR submitted jobs show in the job history against the matched-up user email address.

When the user views their user information, they can see the current value of the Alternate Access Card User field. The Alternate Access Card User value is read only.

Alternate Access Card User Field for New and Rehomed Users

When the user onboards using any other mechanism except .csv file import, the Alternate Access Card User field is blank. When the user onboards using .csv file import, the Alternate Access Card User value is not required. If the value exists, ensure that the value must be unique with respect to all existing Alternate Access Card values and Domain and Username values in the account. When an existing user is homed to a new company account, by default, the Alternate Access Card User value for that account is blank.

Delegates

Xerox® Workplace Cloud enables the assignment of delegates for a user. The account administrator can delegate print responsibilities for the jobs of a user to other users. These delegates can release jobs of that user using the @PrintByXerox app.

Printer Client Document Release Permissions

The Printer Client Document Release Permissions section is used to manage document release permissions that you have given to others or that are granted to you. When a user is assigned as a delegate for another user, the delegate can see the job list of that user in the printer client. The delegate can manage the print jobs of the user, including deleting or printing any job submitted by that user.

Adding Document Release Permissions for Delegates

To add document release permissions for Delegates, do the following:

1. Log in to the Xerox® Workplace Cloud Web portal using your credentials.
2. Click **Users**.
3. Select a user from the list.
The Edit User page appears.
4. Click **Delegates**.
5. From the Actions menu, click **Add**.
The Add delegates screen appears.
6. In the search field, type the required name of the user that you want to grant permissions to, then click the refresh icon.
7. Select the check box next to the user, then click **OK**.

Email notifications are sent to the delegate and the user for which the delegate was added.

Removing Document Release Permissions for Delegates

To remove document release permissions for Delegates, do the following:

1. Log in to the Xerox® Workplace Cloud Web portal using your credentials.

2. Click **Users**.
 3. Select a user from the list.
- The Edit User page appears.

4. Click **Delegates**.
 5. Select the check box next to the user.
 6. From the Actions menu, click **Remove**.
- The Remove Delegates screen appears.
7. At the confirmation message, to confirm, click **Yes**, or to cancel the removal, click **No**.
- Email notifications are sent to the delegate and to the user for which the delegate was removed.

Printing Jobs of Other Users from the Printer Client

1. At a Xerox® Workplace Cloud enabled printer, from the control panel, touch the **Workplace Cloud** icon.
 2. Log in to the printer client with your user name and confirmation number, or your company login credentials.
 3. To access jobs that they are submitted by other users, next to the Exit option, click the user icon.
 4. Select the user whose jobs you want to print.
- The list of jobs appears in the printer client.
5. To print, select the jobs. Select the output settings, then click **OK**.
- Before you print, you can preview the selected jobs.
6. Click **Print**.
 7. Collect the prints.
 8. To select a different user, click the **Person** icon. Repeat the steps as needed.



Note: Before you repeat the steps, you are required to log out of the EIP app.

9. When you finish, click **Exit**.

Resetting a Password or User ID From the @PrintByXerox App

1. On the MFP UI, press **Forgot Password**.
 2. Type a valid email address.
- A message displays that an email has been sent to the email address provided.
3. To reset your password, click the password link.
 4. To reset your ID, click the ID link.

USER ACTIONS MENU OPTIONS

The **Actions** menu on the **Users** tab has the following options:

- Analyze Print Quota
- Change Role
- Change Department
- Remove
- Generate New Pin
- Import Users from File
- Delete Users from File



Note: A user can also edit some of their own information, refer to the [User Profile](#) section for more details.

ANALYZING PRINT QUOTAS - ACTIONS MENU

You can view an overview of an individual user print quota, as well as any enforced rules that affect the user.

To show user Print Quota information:


1. Click **Users**, then select a user from the list.
2. Select **Actions > Analyze Print Quota**.
Print quota information for the user displays.
3. To exit the Analyze Print Quota dialog box, click **Close**.

User Roles

A User can be assigned to the following roles:

- **Account Administrator:** When the User is assigned as an Account Administrator, they will have full access to the Workplace Cloud features. They can view and access the following tabs:
 - **Print**
 - **Jobs**
 - **Printers**
 - **Print Queues**
 - **Sites**
 - **Agents**
 - **Users**
 - **Account**
 - **Reports**
- **Agent Administrator:** When the User is assigned as an Agent Administrator, they will have partial access to the Workplace Cloud features. They can view and access the following tabs:
 - **Print**
 - **Jobs**
 - **Printers**

- **Print Queues**
- **Sites**
- **Agents**
- **Compliance Manager:** When the User is assigned as the Compliance Manager, they will have access to review reports and request the reporting data. They can view and access the following tabs:
 - **Print**
 - **Jobs**
 - **Reports.**

 Important: If the reporting section is not accessible, the user has to request administrator to enable the job reporting. For more information about reports refer to [Reports](#).
- **General User:** When the User is assigned as the General User, they will have limited access to the Workplace Cloud features. They can view and access the following tabs:
 - **Print**
 - **Jobs**

CHANGING THE USER ROLES

To change the role of the user, do the following:

1. Click **Users**.
2. In the User Management section, click **Users**.
3. Select the check box next to the email address of the user that you want to change the role.
4. From the Actions menu, select **Change Role**.

CHANGE DEPARTMENT

Change Department allows you to change the Users Department.

To change or add a User to a department:

1. Select the **Users** tab.
 2. Select a user from the list.
 3. Select **Actions > Change Department**.
- Change Department Dialogue box appears.
4. Enter the required Department of the User.
 5. Click **Save**.

The User is assigned to the required Department.



Note: You can also click on the User email and enter the required Department in the Department field to change the User's Department.

REMOVE USER

Workplace Cloud allows you to remove the selected User from the Company account.

To remove a User from the Cloud Company do the following:

1. Select **Users** tab.
2. Under User Management, click on **Users** tab.
3. Select the required User from the list.
4. Click **Actions > Remove**.
A Remove User dialogue box appears for confirmation.
5. Click **OK**.
6. The Selected User is removed from the Workplace Cloud Company account.



Note: To delete multiple Users at a time, refer to [Delete Users from File](#).

GENERATE NEW PIN

When **Generate New PIN** action is selected, an email be sent to the users indicating that they have a new PIN along with a link to their profile in Xerox Workplace Cloud.

To generate a new PIN for the user do the following:

1. Log in to the Xerox® Workplace Cloud Web portal using your credentials.
2. Select the **Users** tab.
3. Select the user(s) from the list.
4. Click **Actions > Generate New PIN**.

An email will be sent to the user(s) containing a link to their profile in Xerox Workplace Cloud. The Auto-Generated PIN can only be viewed by the end user.

USER IMPORT

Workplace Cloud has a user import process that allows the system administrator to import a file in .csv format. Each company account allows only one user at a time.

The account administrator can initiate the user import.

1. Log in as Administrator.
2. Select **Users > Actions > Import from file**.

Requirements for User Import

Before you import your users, you are required to map the email domain of your users. To map your work domain, send a request to your Xerox Representative.

Xerox Workplace Cloud software now supports adding or updating the user list using a .csv file. Results of the import are sent in an email.

CSV file

The .csv file includes the following fields:

- Email Address: An email address format.
- 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 semicolon.
- Domain: Name of the domain.
- User Name: User name of the user.
- Alternate Access Card User: Name of the Alternate access card user.
- User Groups: You can define multiple user groups in the User Groups column. Separate each user group with a semicolon.
- Department: To assign a user to a department, enter the information string in the Department field. You can use department information in JBA reporting.

Running User Import



Note: Only one user import process is allowed for each company account.

If an account administrator attempts to select the Import From File feature in the Actions menu while a user import is running, users receive an error message The user import file was accepted. All account administrators receive an email notification with the user import process completion message and a warning message, because a user import process is already running. When the import process completes, all account administrators receive an email notification with the user import results.

1. Run the user import command. Default information is stored as follows:
 - The User Role option is set to General User.
 - The Xerox Workplace Cloud Authentication Password is set to a random value that is unknown to users.
 - The Print Job Submission and Print Job Completion notifications for users are set to Receive Failure Notification Only.
2. Ensure that the email and card data are unique. The user import feature does not create duplicate records.
 - If possible, the import inserts the user names, then associates the users with a group.
 - Update the card data and groups for existing users, if appropriate.
 - Before inserting the file in the .csv file for importing, the import verifies that the user does not exist.
3. An email is sent to all account administrators with the following information:
 - Total number of failed user imports
 - Total number of successful user imports
 - Email attachment in .csv format with a list of failed users and failure descriptions

If the user import fails, failure descriptions are included in the email:

- PIN string is not unique in the import file
- User is transferred to another Workplace Cloud company account

- The company account owns the domain account and the Workplace Cloud development team has not performed a Genesis mapping

DELETE USERS FROM FILE

Workplace Cloud has a User Deletion process that allows the System Administrators to import a file in .csv format and delete the Users.

You can navigate to the Users section and Delete the required users by importing a .csv file which consist of Users Email information.

User Deletion Guidelines

- You can only import one .csv file at a time, if you attempt to upload another file during the deletion process, the error message appears as “A Delete Users from file process is already running.”
- If the email column does not exist in .csv file, then the error message appears as “The selected file is not in the correct format. The file must contain the “email” column.”
- All Account Administrators will receive an email notification with the User Deletion results upon deletion process completion.
- If user is not in existing company, the error message displayed in the Deletion Results mail that “The user is not part of the Company Account.”
- The user who has been assigned to multiple Cloud Companies will be assigned to the previous Cloud Company when he is deleted.
- Deleted users who are not associated with any other Workplace Cloud Company will be deleted from the whole Xerox Workplace Cloud Company Account.

Download and Edit the Delete from File Template

To download and edit the `Delete from File Template.csv` file do the following action:

1. Click **Users** tab.
2. Under **User Management** section, select **Users** tab.
3. Click **Actions > Delete Users from File**.

Xerox Workplace Cloud Dialogue box appears.

4. Click on the **Download Delete from File Template**.

The `Delete from File Template.csv` is downloaded in your local folder.

5. Open the downloaded `Delete from File Template.csv` file and add the required Users email under email column and save the .csv file.



Note: Validate the email column entries to ensure that they are correct. If the email entries are not valid, during deletion you will receive a mail stating that the email column must contain valid email addresses.

Delete Users from File

To delete the Users from file, do the following action:



Note: To download and configure the Delete from file Template.csv file refer to [Download and Edit the Delete from File Template](#).

1. Click **Users** tab.
2. Under **User Management** section, select **Users** tab.
3. Click **Actions > Delete Users from File**.

Xerox Workplace Cloud Dialogue box appears.

4. Click on **Choose File** and select the Delete from File Template.csv file that contains the users that are to be removed from the Xerox® Workplace Cloud Company.



Note: You can click on **Choose File** again to change the uploaded .csv file.

5. Click on **Import**.

A notification displayed as the user delete file was accepted. All Account Administrators will receive an email notification with the user delete results upon import process completion.



Note: If there is a service issue the error message is displayed as Error Occurred while deleting the Users.

6. Click **OK**.

The Users are successfully deleted from the Workplace Cloud Company.

JOB DELETION WHEN A USER CHANGES THEIR HOME ACCOUNT

If a user has access to multiple company accounts, when they are logged in using one company account, they can access and release jobs that they submitted using that account only. So that users cannot access jobs that they submitted from a different company account, if their home account changes, all existing jobs stored for that user in Xerox® Workplace Cloud are deleted. Jobs are deleted whether they are stored locally or in the cloud. All information about the jobs is deleted, including original jobs, convert jobs, and job metadata.



Note: Users can have access to multiple company accounts. The home account of a user is the company account that the user last logged into in the Web Portal.

Additionally, jobs are deleted when the account administrator removes the user from their current home account using the Xerox® Workplace Cloud Web Portal.

User Groups

Xerox® Workplace Cloud provides three different options for assigning users to user groups. To associate the users with a group, select one of the following user association types:

- **Include all users except blocked list:** This option adds all users except the users specified in the blocked users list. Users who are assigned to the Blocked List have no printing permissions.
- **Include only specified users:** This option allows you to add users to a group manually.
- **Include LDAP / Azure AD Groups:** This option adds users listed in the LDAP or Azure AD groups.

CREATING USER GROUPS

To create a user group:

1. Log in to the Xerox® Workplace Cloud Web portal as an administrator.
2. Click the **Users** tab, then select **User Groups > Actions > New**.
3. For Details, in the Name field, type a user group name.
4. In the Description field, type a brief description for the new user group.
5. In the Associated Users field, select one of the following user association types:
 - **Include all users except blocked list:** This option includes all users except the users in the blocked list.
 - **Include only specified users:** This option allows you to add users to a group manually.
 - **Include LDAP / Azure AD Groups:** This option includes users specified in the list of LDAP or Azure AD Groups.
6. Click **Save**.

A menu appears with an Actions tab.
7. Select **Actions > Add**.

The Add User window appears.
8. In the Details section, do the following:
 - a. From the Type menu, select **Email Address** or **Email Domain**.
 - b. In the Value field, type the email address or the email domain of the user. Depending on the value, you can add a user with an email address or with an email domain.
 - c. Click **Save**.
9. Add users in one of two ways.
 - To select existing users from the list, select **Actions > Select Users**, then select the users that you want to add.
 - To search for users, click **Search**, then add users to the group.
10. You can associate the new user group with LDAP / Azure AD Groups. For Associated Users, click **Include LDAP / Azure AD Groups**.

11. Click **Actions**, then click **Add**.

A new window appears for Associated LDAP / Azure AD Group.

12. In the Associated LDAP / Azure AD Group field, type an LDAP / Azure AD group name, then click **Save**.
13. After you assign users to the LDAP / Azure AD group, click **Save**.

The new user group appears on the Users tab.

Account

This chapter contains:

- Account: Company Profile..... 138
- Account: Settings..... 154
- Account: Policies 208
- Account: Accounting..... 242
- Account: Licensing 249

Account: Company Profile

- [Company Profile: Details](#)
- [Company Profile: Contact Information](#)
- [Company Profile: Company Authentication Type](#)

COMPANY PROFILE: DETAILS

Company Profile

After you log in to the Web portal, select **Account > Company Profile**. You can edit the following details:

- Company name
- Company code: Allows you to reset your company code. Specify whether the company code appears on the Welcome Page
- Email prefix: Allows you to create a unique email address for each printer enabled in Xerox® Workplace Cloud.
- Use as alias: Allows you to define an custom email alias to be used in place of print@printbyxerox.com for submitting jobs via email.



Note: When you initially set up a company, you can select **Use as alias** in the Details area of the Web UI and use a unique email address instead of **print@printbyxerox**. When Use as alias is selected, the **Enable Express Code for [email address]** check box becomes available. When this check box code is selected, the user will get an email upon successful submission of documents to the cloud, and that email will contain a 6 digit number. The user may then walk up to any printer in their company, and type in the 6 digit number on the @PrintByXerox app. The @PrintByXerox app will log them in and display the documents they submitted. If the express code is not enabled, the user would have to log into @PrintByXerox app with their email address and password in order to print their documents.



Note: The email prefix is used to create a unique email address for each printer enabled by Xerox Workplace Cloud. All printers within the same company account will have the same email prefix. If you choose to change this settings Xerox Workplace Cloud will verify that the value you choose is not already in use.

When **Use as alias** is selected, the **Enable Express Code for your Email Prefix** entered above becomes available.

Enable Express Code

If enabled, the User receives the express codes for Email jobs and for Desktop Job submission.

Limit Express Codes for email job submission only

- If enabled, the User receives the express codes for Email jobs and not for Desktop Job submission.
- If disabled, the Express code is sent for both Email jobs and Desktop jobs.
- Contact information
- Contact email address
- Language: Language in which the system sends notification emails

- Company authentication type

Changing the Company Name

1. From the Web Portal, select **Account > Company Profile**.
2. Enter a new **Company Name**.

Setting a Default Time Zone

To set the default time zone, do the following:

1. Log in to Xerox® Workplace Cloud Web Portal as an administrator.
2. Select **Account > Company Profile**.
3. In the Details section, from the Default time zone menu, select the required time zone option.



Note: When you create Sites, the time zone is configured.

Changing the Printer Email Prefix

The email prefix is combined with the printer name to form a unique printer email address.

1. From the Web Portal, select **Account > Company Profile**.
2. Enter a short, unique prefix.



Note: The prefix must be short and unique. If you select a prefix that is already used, you will receive an error message.

Resetting a Company Code for Account Administrators Only

1. From the Web Portal, select **Account > Company Profile**.
2. Click **Reset Code** next to 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 new Welcome Pages to display with each printer. For more information, refer to [Print Welcome Page](#).

COMPANY PROFILE: CONTACT INFORMATION

In the Contact Information section, you can edit the following fields:

- Contact First Name
- Contact Last Name
- Contact Email
- Contact Email Language



Note: Multiple email addresses can be entered in the Contact Email section separated by commas. This facilitates the management of the workplace cloud account by multiple administrators.

COMPANY PROFILE: COMPANY AUTHENTICATION TYPE

The following is a list of authentication methods supported by Xerox® Workplace Cloud:



Note: Before you change from Xerox Workplace Cloud Authentication to a different authentication setting, it is recommended that you open two different browsers. Use one window to log in using Xerox® Workplace Cloud authentication and the other browser window to test the new authentication change. If there are authentication issues, you can use the Xerox® Workplace Cloud authentication browser to fix authentication issues and return to Workplace cloud authentication, if necessary.

- **Xerox Workplace Cloud Authentication:** Users log in using the email and password that are registered with Xerox® Workplace Cloud.
- **LDAP Authentication:** After the agents run the printer search, to route LDAP requests to the correct agents, domain names are sent to Xerox® Workplace Cloud.
 - **Secondary Authentication:** Secondary authentication selection is supported using Azure AD.
- **Azure AD Authentication:** To access the system, users registered to the company code of an account can validate their identity using Azure AD.
 - **Secondary Authentication:** Secondary authentication selection is supported using LDAP.
- **OKTA Authentication:** To access the system, users registered to the company code of an account can validate their identity using OKTA authentication.
- **HelloID Authentication:** To access the system, users registered to the company code of this account may access the system by validating their identity using HelloID credentials.



Note: Enabling this authentication method will disable Alternate Login support.

Alternate Login Methods Table

This table details about the type of alternate login supported depending on the authentication method you have selected for Workplace Cloud Authentication.

PRINTER AUTHENTICATION TYPE	ALTERNATE LOGIN WITH PIN AUTHENTICATION OFF	ALTERNATE LOGIN WITH PIN AUTHENTICATION ON
OKTA	Feature Disabled	Enter PIN
Azure AD Advanced (Allow Credential access disabled)	Feature Disabled	Enter PIN
Azure AD Advanced (Allow Credential access enabled)	Enter email or ID	Enter email or PIN
Azure AD Simple (Allow Credential access disabled)	Feature Disabled	Enter PIN
Azure AD Simple (Allow Credential access enabled)	Enter email or ID	Enter email or PIN

PRINTER AUTHENTICATION TYPE	ALTERNATE LOGIN WITH PIN AUTHENTICATION OFF	ALTERNATE LOGIN WITH PIN AUTHENTICATION ON
LDAP	Enter email or ID	Enter email or PIN
Cloud Auth	Enter email or ID	Enter email or PIN
Hello ID	Feature Disabled	Enter PIN



Note: To enable or disable PIN Authentication, refer to [Disable PIN Authentication](#).

Secondary Authentication



Note: Xerox® Workplace Cloud Agent version 5.7 or greater supports Secondary authentication.

When you enable LDAP and Azure AD authentication for an account, you can enable a Secondary authentication method.

Xerox® Workplace Cloud supports Primary and Secondary authentication types as follows:

PRIMARY AUTHENTICATION TYPE	SECONDARY AUTHENTICATION TYPE
Xerox® Workplace Cloud authentication	No secondary authentication
LDAP authentication	Azure AD authentication
Azure AD authentication	LDAP authentication
OKTA authentication	No secondary authentication

Ensure that you specify at least one email domain or email address that is used for the Secondary authentication method. Workplace Cloud with an Agent and Workplace Cloud Direct supports Secondary authentication. If the user email address or email domain is found in the list of email addresses or email domains for the Secondary authentication type, only Secondary authentication is attempted for that user.

Configuring Xerox® Workplace Cloud Authentication

The Access Token Lifetime determines how long the user is allowed to remain logged in before they are required to reenter their credentials, for example, in the Desktop Client. For accounts that use Xerox® Workplace Cloud authentication or LDAP authentication, this time is configurable.

To configure the account-level access token, do the following:

1. Log in as an administrator.
2. Click **Account > Company Profile > Company Authentication Type**.
3. Select the radio button for **Xerox Workplace Cloud Authentication configuration**.
4. In the Access Token Lifetime text field, type the number of days, from 1–365 days.
5. Click **Save**.

LDAP Authentication

LDAP (Lightweight Directory Access Protocol) is an open and cross-platform protocol used for directory services authentication. To configure LDAP Authentication, register at least one Xerox® Workplace Cloud Agent that is installed on a computer that is connected to a domain. When the agent is activated, it attempts to discover available domains. When one or more domains are discovered, the LDAP Authentication feature becomes available in Xerox® Workplace Cloud. When you log in, any one of the LDAP domains shown is used for authentication. When you log in to Xerox® Workplace Cloud, you are prompted for the Xerox® Workplace Cloud credentials, such as domain\username and password.

 Note: LDAP Authentication cannot be enabled unless an agent reports that LDAP domains are available.

To route LDAP requests to the correct agents, when agents run the printer search, agents send the domain names to the cloud. To enable a secure connection (LDAPS), select the check box for Use SSL.

 Note: If you change the **Use SSL** setting, all LDAP servers are updated.

Enabling LDAP Authentication

LDAP Authentication supports secondary authentication.

To enable LDAP Authentication, do the following steps:

1. Log in to Xerox® Workplace Cloud as an administrator.
2. Select **Account > Company Profile**.
3. In the Company Authentication Type section, select the radio button for **LDAP Authentication**.
The Primary and Secondary tabs appear.
4. On the **Primary** tab, to enable secure connection (LDAPS), select the check box for **Use SSL**.

 Note: If you change the **Use SSL** setting, all LDAP servers are updated.

5. In the Access Token Lifetime field, type the required days.
The Access Token Lifetime determines how long users can remain logged in before they are required to reenter their credentials, for example, in the Desktop Client. For accounts using Cloud authentication or LDAP authentication, you can set the time from 1–365 days.
6. To save the settings, click **Save**.


A notification displays that the account information has been successfully updated.

7. Follow these steps to enable the optional Secondary authentication:

 Note:

- Only Simple **Azure AD Authentication** is supported for Secondary authentication.
- Follow the steps in this section to enable the Secondary authentication and to add the Email Domains / Addresses, then follow the steps in the **Azure AD Authentication** section to complete the setup.

8. Select the **Secondary** tab.
9. Select the radio button for **Azure AD Authentication**.
10. To add or remove Email Domain / Addresses do the following steps:

 Note: Secondary authentication will only be applicable for users specified within the Email Domain / Addresses.

- a. In the Email Domain / Addresses, click **Actions** and then select **Add**.
A dialog box appears.
- b. Enter the specific email address or email domain that should be authenticated through Azure AD Authentication and then click **Save**.

The email domain or email address is added to the Assigned Email Domains / Addresses section.

 Note: You can add email addresses and email domains in combination.

- c. To remove the Email Domains / Addresses, select the required Email Domains / Addresses, click **Actions** and then select **Remove**.
- d. Click on **Save**.

A notification displays confirming that the account information has been successfully updated.

11. To complete the Azure AD Authentication setup, refer to [Azure AD Authentication](#) section.

 Note: You must do the steps applicable only to Simple Azure AD Authentication.

12. To disable the secondary authentication, select the **Secondary** tab and then select the radio button for **None**.
13. To save the settings, click **Save**.

A notification displays that the account information has been successfully updated.

Azure AD Authentication

When Azure AD Authentication is enabled, users registered to the company code of this account can validate their identity using Azure AD to access the system.

Azure AD Authentication Guidelines:

- Before you deploy Azure AD authentication, it is recommended that you verify that Azure AD authentication is functioning correctly. First, enable and validate the Workplace Cloud Web Portal Azure Authentication login.
- To help with debugging Azure AD 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.
- When a user authenticates with Azure AD, and the user exists in Xerox® Workplace Cloud, the local profile of the user is updated based on the Azure AD user information. If the user name field has a value and the corresponding Azure AD field is blank, the user name is retained.
- If a user supplies an email address that maps to a domain that does not exist or is not enabled, the authentication request is rejected.
- Simple and Advanced Azure AD Authentication supports PIN Authentication as an Alternate Login.
- For more details, refer to [Azure AD Authentication Methods](#) section.

Azure AD Authentication can be configured in two ways: **Simple** and **Advanced**.

Simple Azure AD Authentication Configuration



Note: Azure AD Simple supports login with UPNs in addition to email addresses.

The Simple configuration provides a multi-tenant solution. Users are maintained using fixed field mapping. Azure AD group information for users is not supported.

During software upgrade, all existing accounts with the Azure AD Authentication type are converted to the Simple Azure AD authentication type.

When any new or existing account is changed to the Azure AD Authentication type, the account defaults to the Simple Azure AD authentication type.

If Simple Azure AD Authentication is selected the following options are available for selection under Global Permission:

- **Grant Access Permission** option is available for selection. This option grants Xerox® Workplace Cloud access to the basic profile of all users of the Azure Active Directory. Individual users are not prompted for credentials. Ensure that users are in the same Azure Active Directory as the administrator. If more than one Azure Active Directory is used, repeat this step for each Azure AD authentication.

During the initial login, ensure that each user is granted permission to the Xerox® Workplace Cloud, that allows access to their basic profile. To restrict access to the system, use the **Account > Policies > Access Controls** page.

- **Allow Credential Access** option is available for selection. This option allows Xerox® Workplace Cloud to handle the login credentials of a user, including their password. This is needed when authenticating a user using the Alternate Login option on a Xerox printer. Refer to the [Alternate Login Methods Table](#).



Note: This method does not support Azure Multi-factor Authentication.



Note: To configure Alternate Login, refer to [Policies: Printer Authentication](#).

- **Source of Authentication**

Source of Authentication is only available when **Allow Credential Access** is enabled, the following are the Source of Authentication options for Azure AD Simple authentication:

- **Xerox Workplace Cloud:** The authentication request is made from the Workplace Cloud solution in the Azure cloud.
- **Xerox Workplace Cloud Agent:** The Authentication requests will be handled by the Workplace Cloud Agent. Use this option if your Azure AD system requires the use of Multi-Factor Authentication. Using the Agent for authentication requests, you can add an exception for the IP address of the Agent to your Azure AD configuration to bypass Multi-Factor Authentication.
- **Provide email domain hint for new users:**
 - Some environments allow the user to override the email hint provided to Azure AD so that they can enter their Universal Principle Name as an alternative. If your tenant does not allow you to override the hint, then you may disable this option for your users. This will force a brand new user to enter their initial login credential the first time they attempt to log into Xerox Workplace Cloud using Azure AD. This credential will be cached for future login attempts if the user is successfully validated.

Troubleshooting Alternate Login for Azure AD Simple Mode

If you are using Azure AD Simple mode with the Source of Authentication set to Xerox Workplace Cloud, and Alternate Login is failing, this may be caused by the customer requiring Multi-Factor Authentication (MFA).

Adding an exception to the customers Azure AD Conditional Access configuration for the following static IP addresses will allow them to bypass Multi-Factor Authentication (MFA) with this login method at the printer:

LOCATION	IP ADDRESS
UK South	51.132.11.42
UK South	20.77.169.0
UK West	20.254.146.7
UK West	20.254.160.214
Europe North	20.107.195.73
Europe North	4.245.240.91
Europe West	104.47.154.99
Europe West	40.118.22.244

Advanced Azure AD Authentication Configuration

The Advanced configuration supports multiple Azure AD domains. Users are maintained using custom field mappings for each connection. Azure AD group information for users is supported. A single tenant App is required for each domain.

You must add at least one Azure AD Connection to enable the Advanced Azure AD Authentication option. To add the Azure AD connections, refer to [Settings: Azure AD Connections](#), you can also click on **Configure Connections** to define an Azure AD Connection.

To set the Field Mapping values for Azure AD Connections, refer to [Setting the Field Mapping Values](#).

Advanced Azure AD Guidelines:

- A new Azure AD application must be created for every Azure AD tenant and must be configured for the Workplace Cloud and the Azure AD tenant.
- Advanced Azure AD supports card registration only by using Azure credentials.
- 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 Cloud, as an email address is required to log in.
- Specific Cloud user fields can be mapped to Azure AD fields (e.g., badge number).

Allow Credential Access:

This option allows Xerox® Workplace Cloud to handle the login credentials of a user, including their password. This is needed when authenticating a user using the Alternate Login option on a Xerox printer. Refer to the [Alternate Login Methods Table](#).



Note: This method does not support Azure Multi-factor Authentication.



Note: To configure Alternate Login, refer to [Policies: Printer Authentication](#).

• Source of Authentication

Source of Authentication is only available when **Allow Credential Access** is enabled, the following are the Source of Authentication options for Azure AD Advanced authentication:

- **Xerox Workplace Cloud:** The authentication request is made from the Workplace Cloud solution in the Azure cloud.
- **Xerox Workplace Cloud Agent:** The Authentication requests will be handled by the Workplace Cloud Agent. Use this option if your Azure AD system requires the use of Multi-Factor Authentication. Using the Agent for authentication requests, you can add an exception for the IP address of the Agent to your Azure AD configuration to bypass Multi-Factor Authentication.
- **Provide email domain hint for new users:**
 - Some environments allow the user to override the email hint provided to Azure AD so that they can enter their Universal Principle Name as an alternative. If your tenant does not allow you to override the hint, then you may disable this option for your users. This will force a brand new user to enter their initial login credential the first time they attempt to log into Xerox Workplace Cloud using Azure AD. This credential will be cached for future login attempts if the user is successfully validated.

Enabling Azure AD Authentication

To enable Azure AD Authentication, do the following:

1. Log in to Xerox® Workplace Cloud as an administrator.
2. Select **Account > Company Profile**.
3. In the Company Authentication Type section, select the radio button for **Azure AD Authentication**.
The Primary and Secondary tabs appear.
4. On the Primary tab, select one of the following radio buttons:
 - **Simple:** Authentication is performed using a multitenant application. Users are maintained using a fixed field mapping. Azure AD group information for users is not available.
 - **Advanced:** Authentication is performed using your configured Azure AD connections. Users are maintained using custom field mapping per connection. Azure AD group information for users is available.



Note: Azure AD Simple and Advanced supports PIN Authentication.

5. If you select the radio button for **Simple** do the following steps:
 - a. Click **Save**.
A notification appears confirming the account information has been successfully updated.
 - b. In the Global Permission section, click **Grant Access Permission**.
Azure AD pop-up window appears.
 - c. Click on administrator account and click **Accept** to grant permission.
A notification displays confirming that the access permission has been granted successfully by an Azure AD administrator.
 - d. To exit and return to Company Authentication Type click **Close**.

- e. If you want to enable the alternate login for the users, select **Allow Credential Access** check box and select the required Source of Authentication:

Source of Authentications are:

- **Xerox Workplace Cloud:** with this option the authentication request is made from the Workplace Cloud solution in the Azure cloud.
- **Xerox Workplace Cloud Agent:** with this option the Authentication requests will be handled by the Workplace Cloud Agent. Use this option if your Azure AD system requires the use of Multi-Factor Authentication. By using the Agent for authentication requests, you can add an exception for the IP address of the Agent to your Azure AD configuration to bypass Multi-Factor Authentication.



Note: **Allow Credential Access** allows the users to login to the printer using Administrator Login credentials. To configure and enable Alternate Login, refer to [Policies: Printer Authentication](#).

- f. Click on **Provide email domain hint for new users** check box to allow your users to override the email hint provided to Azure AD, so that they can enter their Universal Principle Name as an alternative. This setting is enabled by default.



Note: If your tenant does not allow you to override the hint, then you may disable this option for your users. This will force a brand new user to enter their initial login credential the first time they attempt to log into Xerox Workplace Cloud using Azure AD. This credential will be cached for future login attempts if the user is successfully validated.

- g. To save the settings, click **Save**.

A notification displays that the account information has been successfully updated.

6. If you select the radio button for **Advanced**, do the following steps:



Note: To enable Advanced Azure AD Authentication option you must add one or more Azure AD connections. To add the connections, refer to [Settings: Azure AD Connections](#).

- a. Click **Configure Connections**.

You are redirected to Azure portal.

- b. If you want to enable the alternate login for the users, select **Allow Credential Access** check box and select the required Source of Authentication:

Source of Authentications are:

- **Xerox Workplace Cloud:** with this option the authentication request is made from the Workplace Cloud solution in the Azure cloud.
- **Xerox Workplace Cloud Agent:** with this option the Authentication requests will be handled by the Workplace Cloud Agent. Use this option if your Azure AD system requires the use of Multi-Factor Authentication. By using the Agent for authentication requests, you can add an exception for the IP address of the Agent to your Azure AD configuration to bypass Multi-Factor Authentication.



Note: **Allow Credential Access** allows the users to login to the printer using Administrator Login credentials. To configure and enable Alternate Login, refer to [Policies: Printer Authentication](#).

- c. Click on **Provide email domain hint for new users** check box to allow your users to override the email hint provided to Azure AD, so that they enter their Universal Principle Name as an alternative.



Note: If your tenant does not allow you to override the hint, then you may disable this option for your users. This will force a brand new user to enter their initial login credential the first time they attempt to log into Xerox Workplace Cloud using Azure AD. This credential will be cached for future login attempts if the user is successfully validated.

- d. Click **Save**.

A notification appears confirming the account information has been successfully updated.

7. Follow these steps to enable the optional Secondary authentication:



Note: Follow the steps in this section to enable the Secondary authentication and to add the Email Domains / Addresses, then follow the steps in the **LDAP Authentication** section to complete the setup.

8. Select the **Secondary** tab.

9. Select the radio button for **LDAP Authentication**.

10. To add or remove Email Domain / Addresses do the following steps:



Note: Secondary authentication will only be applicable for users specified within the Email Domain / Addresses.

- a. In the Email Domain / Addresses, click **Actions** and then select **Add**.

A dialog box appears.

- b. Enter the specific email address or email domain that should be authenticated through LDAP Authentication and then click **Save**.

The email domain or email address is added to the Assigned Email Domains / Addresses section.



Note: You can add email addresses and email domains in combination.

- c. To remove the Email Domains / Addresses, select the required Email Domains / Addresses, click **Actions** and then select **Remove**.
- d. Click on **Save**.

A notification displays confirming that the account information has been successfully updated.

11. To complete the LDAP Authentication setup, refer to **LDAP Authentication** section.
12. To disable the secondary authentication, select the **Secondary** tab and then select the radio button for **None**.
13. To save the settings, click **Save**.

A notification displays that the account information has been successfully updated.

Azure AD Authentication Methods

Badge User Registration with Azure AD Credentials



Note:

- To register as a new user, the user needs an Azure AD account.
- Azure AD authentication supports login with UPNs in addition to email addresses.

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

1. Enter 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. Click 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 them to enter their Azure login credentials.

3. Log in using their Azure login credentials.

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



Note: 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 the Allow Multiple Primary PINs or Access Cards feature disabled, when a user swipes a new card, an error message does not appear.

Printer Client Login with Azure AD Credentials

When you enable the Azure AD authentication feature for the Printer Client, when a user logs in, they are redirected to the Azure AD login page to provide credentials. If their machine has a valid Azure AD token, for example if they are logged in to Office 365, they are not prompted to provide Azure AD credentials.

Mobile Application Login with Azure AD Credentials

When you enable the Azure AD authentication feature for the mobile application, when a user logs in, they are redirected to the Azure AD login page to provide credentials. If their machine has a valid Azure AD token, for example if they are logged in to Office 365, they are not prompted to provide Azure AD credentials. The supported operating systems are Android, iOS, and Chrome OS.

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 Cloud login page, they are redirected to the Azure AD login page to provide credentials. If their machine has a valid Azure AD token, for example if they are logged in to Office 365, they are not prompted to provide Azure AD credentials.



Note: An Azure AD administrator can grant permission on behalf of all users of the Azure Active Directory, which allows Workplace Cloud access to their basic profile. Ensure that the users are in the same Azure AD account as the administrator. If the user has more than one Azure AD account, repeat this step for each Azure Active Directory.

Advanced Azure AD Authentication

Advanced Azure AD connection supports multiple single-tenant applications.

On the Add Azure AD Connection page, if you enable **Use only for specified email domains** or **Use for any email domain**, users can authenticate Azure AD connections using their Azure AD credentials. After a user authenticates, the user is added to the Workplace Cloud database with the current Azure AD entry using current mappings for the connection. If the user cannot authenticate, an error message appears that states *Your email domain is not valid for this company code.*

You can authenticate Azure AD connections from the following:

- Web portal
- Windows client
- Mac client
- iOS application
- Android application
- Chrome extension
- Printer Client

OKTA Authentication

Administrators can configure OKTA Authentication to allow users to access the following components of the Xerox® Workplace Cloud environment using a single set of credentials:

- @PrintByXerox printer client
- Xerox® Workplace Cloud Client
- Xerox® Workplace Cloud Web portal
- Xerox® Workplace Cloud Google Chrome browser extension



Note:

- To enable and configure OKTA Authentication, an OKTA admin account and sufficient knowledge of the OKTA API are required.
- OKTA Authentication supports PIN Authentication.
- OKTA Authentication supports login with UPNs in addition to email addresses.

Enabling and Configuring OKTA Authentication

To enable and configure OKTA Authentication:

1. Log in as administrator to the Xerox® Workplace Cloud Web Portal.
2. Select **Account > Company Profile**.
3. In the Company Authentication Type section, select **OKTA Authentication**.

The OKTA Configuration Wizard window appears automatically.



Note: If the OKTA Configuration Wizard window does not appear automatically, click **Configure OKTA**.

4. In the Authorization Server section, enter the Server Issuer URI (Uniform Resource Identifier), then click **Next**.



Note: To obtain an OKTA authorization server, visit the OKTA website. For further information, contact your OKTA representative.

5. In the OKTA web user interface, create a web application using the configuration options that are listed in the Application and Login sections of the OKTA Configuration Wizard.

For more information on creating applications in the OKTA web user interface, contact your OKTA representative.

6. After you create the web application, in the Client Credentials section, enter the client ID and client secret information from the OKTA web user interface. Click **Next**.
7. In the OKTA web user interface, create a native application using the configuration options that is listed in the Application and Login sections of the OKTA Configuration Wizard.
8. After you create the native application, in the Client Credentials section, enter the client ID from the OKTA web user interface, then click **Next**.
9. In the OKTA web user interface, create a single page application using the configuration options that are listed in the Application and Login sections of the OKTA Configuration Wizard.
10. After you create the single page application, in the Client Credentials section, enter the client ID from the OKTA web user interface. Click **Finish**.
11. To save the settings, click **Save**.

A notification appears that confirms your saved settings.

Logging In Using OKTA Authentication



Note: OKTA Authentication supports login with UPNs in addition to email addresses.

1. At the Xerox® Workplace Cloud login screen, type your email address, then click **Submit**.

You are redirected to the OKTA login screen.

2. Enter your OKTA user name and password, then click **Sign In**.

You are redirected to the Xerox® Workplace Cloud Web Portal home screen.

HelloID Authentication

When HelloID Authentication is enabled, users registered to the company code of this account can access the system by validating their identity using HelloID credentials. HelloID connection must be set up before enabling HelloID Authentication. To set up HelloID connection, refer to [Settings: HelloID Connection](#).



Note: This authentication method only supports Alternate Login via PIN. Users are not allowed to enter their HelloID credentials when using Alternate Login.

Administrators can configure HelloID Authentication to allow users to access the following components of the Xerox® Workplace Cloud environment using a HelloID Credentials:

- @PrintByXerox Printer Client
- Xerox® Workplace Cloud Client
- Xerox® Workplace Cloud Agent

- Xerox® Workplace Cloud Web portal
- Workplace Mobile Application
- Xerox® Workplace Cloud Google Chrome browser extension

Guidelines

- When changing the authentication type to HelloID Authentication, ensure you have configured HelloID Connections. If the HelloID connections are not configured and you try to enable HelloID Authentication, you get an error that there is no HelloID connection configured.
- HelloID credentials cannot be used as Alternate login credentials.
- PIN Authentication can be used as an Alternate login method for HelloID Authentication.
- After changing the authentication type to HelloID Authentication, you should do the repair action on all the printers which are enabled for authentication.

Enabling HelloID Authentication



Note: This authentication method only supports Alternate Login via PIN. Users are not allowed to enter their HelloID credentials when using Alternate Login.

To enable and configure Hello ID Authentication:

1. Log in as administrator to the Xerox® Workplace Cloud Web Portal.
2. Select **Account > Company Profile**.
3. In the Company Authentication Type section, select **HelloID Authentication**.



Note: Before changing the Company Authentication type to **HelloID Authentication**, ensure that you have set up a **HelloID Connection**. Click on **HelloID Connection** to set up HelloID connection, refer to [Settings: HelloID Connection](#).

4. Click **Save**.

HelloID is now set as the Company Authentication Type for your Workplace Cloud Company account.



Note: After saving your changes, please repair all existing printers which are enabled to use Authentication.

Logging in Using HelloID Authentication

1. For a user not associated with a Company account, do the following steps:
 - a. In the Workplace Cloud Web Portal, click on the **Create User Account**.
 - b. On the login screen, type your company email address, click **Submit**.
 - c. Enter the Company Code of the Workplace Cloud account, click **Submit**, you will receive the verification email to your Workplace Cloud email.



Note: You need to acquire a Company Code from your account administrator.

- d. Enter the verification code, click **Submit**, you are redirected to HelloID Login.
- e. Enter your HelloID username and password.



Note: If your Workplace Cloud email address and HelloID username are same, you will not receive the verification email.

- f. Workplace Cloud will send a confirmation email to your Workplace Cloud email address. Click on the confirmation link in the email, this associates your HelloID UPN to your Cloud email address.

Your Workplace Cloud account is now associated with the HelloID account and you are now successfully logged in to the Workplace Cloud account using HelloID Authentication.

2. For a user associated with a Company Account, the Workplace Cloud solution will skip the Workplace Cloud email validation step and the user is prompted to the HelloID authentication page with the email ID populated.



Note: If a user logged in once using HelloID, the solution will validate the HelloID username with the email address provided to the Workplace Cloud, When they don't match, the solution will perform an email validation step to establish the linkage between the email and the username and save it in the database.

Unlocking a Printer Using Alternate Login

Users can unlock the Multifunction Printer directly from the device, if you are using Cloud Authentication or LDAP. Be sure to connect to the same company account as the printer.

1. From the control panel of the printer, in the keyboard, press **Alternate Login**.
2. To unlock the printer, enter your User Name or User ID, followed by your Password.

First-time users have to register at the Xerox® Workplace Cloud Web Portal.

If Lightweight Directory Access Protocol (LDAP) authentication is enabled, enter your email address, and then your user name and password. LDAP authentication is enabled on the Web Portal on the **Account > Company Profile** page.



Caution: When your printing is complete, to ensure that other users cannot access your documents, always log out.

Unlocking a Printer Using Card Authentication

Users can unlock the Multifunction Printer directly from the device. Ensure that you are connected to the same company account as the printer. The Printer Essentials Bundle license is needed for the Card authentication. Go to the printer and swipe your ID badge at the card reader device.

Account: Settings

The Settings section contains the information for the following features:

- [Settings: Desktop Printing](#)
- [Settings: Feature Defaults](#)
- [Settings: Home Worker Print Tracker](#)
- [Settings: LDAP Connections](#)
- [Settings: Azure AD Connections](#)
- [Settings: HelloID Connection](#)
- [Settings: SAML Connection](#)
- [Settings: Network Appliances](#)
- [Settings: Performance](#)
- [Settings: Print Defaults](#)
- [Settings: XSM Export](#)
- [Settings: Single Sign-On](#)
- [Settings: Microsoft Universal Print](#)

SETTINGS: DESKTOP PRINTING

Desktop printing allows you to download and install the **Xerox Workplace Cloud Client** to enable sending print jobs from your computer using the native **File > Print** workflow within desktop applications. Once the client is installed, you can add both follow print and direct printers to your desktop. You can then submit print jobs from anywhere, even outside the company firewall.

The following sections contain instructions on creating a Generic, Custom Driver and Composer File and how to associate them with a direct printer and creating a Pull Print Queue.

- [General](#)
- [Configuration](#)
- [Drivers](#)
 - [Custom Drivers](#)
 - [Composer Files](#)
 - [Mac PPD](#)
- [Direct Print](#)
- [Queues](#)

Ways to Deploy Direct Printers or Pull Printers to the Desktop Client:

You can deploy the Direct Printers or Pull Printers on the Desktop Client through following methods:

- You can manually install the printers using Workplace Cloud Web Portal, refer to **Print: Desktop** section.
- You can use Deployment Groups by which you can automatically install the Printers, refer to **Deployment Groups** section.



Note: The number of printers that can be installed per Deployment Group is limited to 25.

General

The General tab allows you to install Windows or Mac Xerox Workplace Client to your computer which is used to add printers for Desktop Printing without administrator access.

When deploying the Mac version of the client, you must ensure that the accountid.json file in the client package download is in the same directory as the client installer when you deploy the client to your users.

Select the Xerox Generic Printer if you would like to have it installed automatically once the Xerox® Workplace Cloud Client is installed. The client will check once per day to see if there is a new printer that needs to be installed. Deselecting the Xerox Generic Printer will not remove it once installed by the client.

Workplace Cloud Client Installation Packages

There are three different installation packages for the Workplace Cloud Client see below for details:

Workplace Cloud Client Non-Configured Version



Note: This is the standard package an administrator can download, then configure and distribute. This version is not pre-configured.

From Xerox® Workplace Cloud Web Portal, click **Account > Settings > Desktop Printing > General** to download the Workplace Cloud Client installer only Version for Windows or Mac. After installation of this version do the following:

- User is logged in and linked to their company.
- Automatically installs the default print queue setup by the Administrator.

Workplace Cloud Client Pre-Configured Version



Note: This is the standard package an end user would normally use, and is can be downloaded by a general user.

From Xerox® Workplace Cloud Web Portal, click **Print > Desktop** tab to download the Workplace Cloud Client Pre-Configured Version for Windows or Mac. After installation of this version do the following:

- User is logged in and linked to their company.
- Automatically installs the default print queue setup by the Administrator.

Workplace Cloud Client MSI Deployment Version



Note: To customize and distribute, an administrator can download the MSI package.

You can download the Xerox® Workplace Cloud desktop client as a non-executable installation Package and install the package onto a Windows PC without requiring administrator privileges. To download the Xerox Workplace Cloud Client MSI, for IT Managed Deployment only, go to this link: <https://www.support.xerox.com/en-us/product/xerox-workplace-cloud/downloads>.

Installation of the Xerox® Workplace Cloud Client

Installation of the Workplace Cloud Windows Client



Note: After installation, the Windows Client is operated from the Windows system tray.

To download and run the Windows non-executable installation package:

1. Log in to the Xerox® Workplace Cloud Web Portal at <https://xwc.services.xerox.com>.
2. To obtain the required installation package, choose one of the following options:
 - For a version of the Client that is pre-configured with user credentials for the logged in user, select **Print > Desktop**. Then, to download the installation package to your browser default download location, in the Install the Workplace Client section, click **Windows**.
 - For a version of the Client that is not pre-configured with user credentials, select **Account > Settings > Desktop Printing**, then click **Desktop Client**. Then, to download the installation package to your browser default download location, in the Install the Workplace Client section, click **Xerox® Workplace Cloud Client**.

The `XeroxWorkplaceCloudClient.exe` file downloads automatically to your browser default download location.

3. To run the setup wizard, locate the file and double click it.

The Xerox Setup Wizard window appears.

4. From the drop-down menu, select the required language from the list, then click **Ok**.

A splash screen appears and the Install window updates while installation files are unpacked. After a short while, the Xerox Setup Wizard window opens and a Welcome message appears.

5. To see any additional information about the software, click **View Readme**.
6. To continue the installation, click **Next**.

The License Agreement window appears.

7. Read the license terms. To accept the terms and continue the installation, select the check box for **I accept the terms in the license agreement**, then click **Next**.

The Ready To Install window appears

8. To begin the installation, click **Install**.

A status progress bar appears.



Note: It can take several minutes for the installation to complete.

9. When the installation finishes successfully, the Setup Complete window appears. To finish the installation and exit the wizard, click **Finish**.

The Xerox Workplace Cloud Client is installed and ready to use.

Installation of the Workplace Cloud Macintosh Client



Note: Before you install Macintosh Workplace Cloud Client, ensure that the Xerox Macintosh Print and Scan driver or third-party driver is installed on all the Macintosh workstations. The Cloud Mac Client does not automatically install drivers. After installation, the Mac Client is operated from the Macintosh status bar.

To download and run the Mac Client installation package:

1. Log in to the Xerox Workplace Cloud Web Portal at <https://xwc.services.xerox.com>.
2. To obtain the required installation package, choose one of the following options:
 - For a version of the Client that is pre-configured with user credentials for the logged in user, select **Print > Desktop**. Then, to download the installation package to your browser default download location, in the Install the Workplace Client section, click **Mac**.
 - For a version of the Client that is not pre-configured with user credentials, select **Account > Settings > Desktop Printing > General** tab. To download the installation package to your browser default download location, in the Install the Workplace Client section, click **Xerox Workplace Cloud Client..**

The **XeroxWorkplaceCloudClient.pkg** file downloads automatically to your browser default download location.

3. To run the installer, locate the file and click it.

The Xerox Workplace Cloud Client Installer window appears.

4. To continue the installation process, click **Continue**.

The Readme window appears, displaying additional information about the Mac Client.



Note: To print the Readme, click **Print**, or to save the Readme as a .txt file, click **Save**.

5. To continue the installation, click **Continue**.

The Software License Agreement window appears.

6. Read the license terms. To accept the terms and continue the installation, click **Continue**, then click **Agree**.

The Destination Select window appears, and the default installation location displays.



Note: To change the location of the installation, click **Change Install Location**, then select the required destination.

7. To continue the installation process, click **Install**.

A security dialog box appears.

8. To begin the installation, enter the Macintosh administrator password, then click **Install Software**.

A status progress bar appears.



Note: It can take several minutes for the installation to complete.

9. When the installation finishes successfully, a message appears confirming that the installation was successful. To finish the installation and exit the installer, Click **Close**.

A dialog box appears asking if you want to keep the installer file or move it to the Trash.

10. To keep the installation package in the current location, click **Keep**, or to move the file to the Trask, click **Move to Trash**.

The Xerox Workplace Mac Client is installed and ready to use.

Enabling the Install Xerox® Generic Printer by Default

Once the Xerox® Workplace Cloud Client is installed, you may add a Xerox® Generic Printer. When you print to the generic printer, the document is sent to the cloud. When you go to the device later and log in to Xerox® Workplace Cloud you may release the job to print. The job may also be released using the Workplace Mobile App.

1. Select **Account > Settings > Desktop Printing > General** tab.
2. In Xerox® Workplace Cloud Client, select the check box next to **Install Xerox® Generic Printer by Default**.
3. To install the Xerox® Workplace Cloud Client with the Xerox® Generic Printer, click the **Xerox® Workplace Cloud Client** link .

Showing and Hiding Features in Desktop Printing for Windows

Administrators can show and hide features of the Desktop Printing for Windows section of the Xerox® Workplace Cloud Web Portal to manage user access to certain desktop printing features.

To show and hide Desktop Printing for Windows features:

1. Log in as administrator to the Xerox® Workplace Cloud Web Portal.
2. Select **Account > Settings > Desktop Printing > General** tab.
3. To hide a section, select the corresponding check box:
 - **Hide the Workplace Client:** This option prevents users from accessing a link to download the Xerox® Workplace Cloud desktop client installation package.
 - **Hide the Xerox Generic Printer:** This option prevents users from submitting jobs for later release using the Generic Printer driver.
 - **Hide Custom Driver Printers:** This option prevents users from submitting jobs for later release using a custom print driver.
 - **Hide Direct Printers:** This option prevents users from printing directly to a specific printer from a list of connected printers.
4. To save the settings, click **Save**.

A notification appears confirming that the settings are saved.

Local Print Optimization

The Local Print Optimization feature can improve the print performance of desktop jobs that are submitted to a custom generic printer for later release. You can set the Local Print Optimization feature at the account level and override the setting for each client, as needed. To override the setting for the account, ensure that Local Print Optimization is set to **Enabled without Cloud Backup** or **Enabled with Cloud Backup**.



Note: For more information about the Local Print Optimization feature, access the Desktop Printing Web Portal, then click the **Information (i)** button.

There are several options for the Local Print Optimization feature.

- **Disabled:** All custom driver jobs will convert to print ready file format and then upload to the cloud. No local copy will be stored on the desktop. The primary user case for this is for clients that are on separate networks from the printers.
- **Enabled without Cloud Backup:** The desktop client stores all jobs locally. When the jobs are released, they transition from the user workstation to the local printer. If there is a connection issue to either the workstation or the printer, the job does not print, and is deleted. All custom driver jobs convert to print ready file format and is stored in a folder on the user computer. Copy is not uploaded to the cloud. When a user releases the print job at a printer, the Azure IoT Hub sends a notification to the Workplace Cloud Client to release the job directly to the printer. Ensure that the client is online and have network connectivity to the printer at the time the document is release or else the document fails to print. Select this configuration option for customers who have extremely low bandwidth throughout their company network and for desktop clients which are likely to always be
- **Enabled with Cloud Backup:** The desktop client stores a local copy of the job and sends a backup job file to the Cloud service. When jobs are released, the 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, the Cloud sends the backup file to the printer. There are two options as follows:
 - **Enabled with Cloud Backup – Maximum File Size Disabled:** All custom driver jobs will convert to print ready file format and will be stored in a folder on the user’s computer and a copy will upload to the cloud. When a user releases the job at a printer, the Azure IoT Hub will notify the client to release the job directly to the printer. However, if the client is offline, the printer will pull the file from the cloud. Unless a company has bandwidth concerns, this is the most optimal configuration for the majority of customers. Before you use the **Enabled without Cloud Backup** option, If some bandwidth concerns are present, ensure that the customers use the **Enabled with Cloud Backup – Maximum File Size Enabled** option. When their client or computer happens to be offline, the **Enabled without Cloud Backup** option does not provide a failover mechanism for end users.
 - **Enabled with Cloud Backup – Maximum File Size Enabled:** All custom driver jobs convert to print ready file format and is stored in a folder on the user computer and some jobs have a copy uploaded to the cloud. The Maximum File Size configured value is used to determine which documents are stored locally as there is no copy is uploaded to cloud. For example, if the maximum file size is 10 MB, when a converted print ready file is over 10 MB, it is stored locally to reduce the bandwidth required by the company network to transmit files over 10 MB. For files over the configured Maximum File Size, when a user releases the print job at a printer, to release the job directly to the printer, the Azure IoT Hub sends a notification to the Workplace Cloud Client. Ensure that the client is online and have internet connectivity to the printer at the time the document is release or else the document will fail to print. For files under the configured Maximum File Size, when a user releases the job at a printer, the Azure IoT Hub will notify the client to release the job directly to the printer. However, if the client is offline, the printer will pull and download the file from the cloud. This configuration option is recommended if there are bandwidth concerns with large print jobs. The recommended configuration option for Local Print Optimization is **Enabled with Cloud Backup – Maximum File Size Disabled**. It is optimal to select this setting because it always uploads a backup file to cloud which provides the best end user experience in cases where the client or user’s computer where the client resides happens to be offline.



Note: You can define the maximum file size for the backup job. The file size can range from 1–9999 Mbytes. Jobs larger than the configured maximum size result in no backup job sent to the Cloud. The job is stored locally on the user workstation.

Enabling Local Print Optimization



Note: By default, for Xerox® Workplace Cloud, Local Print Optimization is disabled.

1. Log in to Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Settings**, then select **Desktop Printing**.

The Desktop Printing page appears.



Note: To change the settings, follow the instructions in the screen.

After you enable the feature, jobs that are submitted to a custom generic printer for later release are stored locally and optionally sent to the Xerox® Workplace Cloud.

Disabling Local Print Optimization



Note: When Local Print Optimization feature is disabled at the account level, the feature is disabled for all Clients, and any Client override settings do not apply.

To disable local print optimization for an account, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Settings > Desktop Printing > General** tab.
3. In the Local Print Optimization area, select **Disabled**.
4. To confirm your changes, click **Save**, or to cancel the changes, click **Cancel**.

After you disable the feature, jobs submitted to a custom generic printer for later release are sent to the Cloud. Copies are not stored locally.

Overriding the Local Print Optimization Account Setting for Xerox® Workplace Cloud Clients



Note: Client override is supported only when Local Print Optimization for the account is set to Enabled with Cloud Backup or Enabled without Cloud Backup.

For individual Xerox® Workplace Cloud Clients, you can override the Local Print Optimization setting that is enabled at the account level. The use of the override setting optimizes jobs that are released in sites that have a lower bandwidth.

To override the local print optimization setting of the account, you are required to place a file that contains the necessary settings in the installation path for the Xerox® Workplace Cloud Client.

For more information on overriding the account local print optimization settings, contact a Xerox representative.

Configuration

The Configuration tab allows you to manage the Xerox® Driver Configuration files created using the Xerox® Print Driver Configuration Tool. You can deploy the XML Driver Configuration file to all Users or select User Groups. There is a **Actions** menu to add, delete, enable, disable, and set deployment priority of the XML Driver Configuration files.

Xerox® Driver Configuration

When you configure the Desktop Printing settings for the account, you can specify an Xerox® Driver Configuration file for the Xerox® Workplace Cloud Client for Windows to use. When the Xerox® Workplace Cloud Client is installed, it checks for and installs the Xerox® Driver Configuration file. Xerox® Workplace Cloud Client checks for and retrieves

any updates to the file once a day. You can install one Xerox® Driver Configuration file at a time only. The file applies to Xerox® print drivers only and can support multiple print drivers. The Configuration file allows you to set the print defaults and enforce print attributes for the account.



Note: The Xerox® Workplace Cloud Client for Mac does not use, install, or update the XML Driver Configuration File.

Xerox Print Driver Configuration Tool is used to create the Xerox Drive Configuration XML file, for more information on the Xerox® Print Driver Configuration Tool, refer to [Xerox® Driver Configuration File](#).

Add Xerox XML Driver Configuration File

To add Xerox® XML Driver Configuration File, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Settings > Desktop Printing > Configuration** tab.
3. Click **Actions > Add**.
4. On the Details provide the Name and Description of the XML Driver Configuration file.
5. On XML File, in the Select File field, click **Choose File**.
6. Browse to the location of the `CommonConfiguration.xml` file on your computer, click **Open**.

The file name appears in the Choose File field.



Note: The name of the file should be `CommonConfiguration.xml`.

7. Click **Save**.
The User Association section appears.
8. In the User Association section, select the set of users to which the configuration file will apply:
 - **All Users:** Selecting this option installs configuration file to all users.
 - **Select User Groups:** If you select this option, click on **Action > Add** to add User Group to which the Configuration files will be installed.

To remove User Groups, click **Actions > Remove**.

9. Select **Enable** check box and click **Save** to enable and install the XML Driver Configuration file.

The XML Driver Configuration file is successfully created and installed to the required users.

Enable or Disable Xerox XML Driver Configuration File

To enable or disable the Xerox® XML Driver Configuration File, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Settings > Desktop Printing > Configuration** tab.
3. Select the check box of required Xerox® XML Driver Configuration File.
4. Click **Actions > Enable**.

The XML Driver Configuration File is enabled.

5. To disable the XML Driver Configuration File, click **Actions > Disable**.

The XML Driver Configuration File is disabled.

6. Click **Save**.

Delete Xerox XML Driver Configuration File

To delete the Xerox® XML Driver Configuration File, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Settings > Desktop Printing > Configuration** tab.
3. Select the check box of required Xerox® XML Driver Configuration Files.
4. Click **Actions > Delete**.

The XML Driver Configuration Files are deleted.

5. Click **Save**.



Note: When the daily check and update cycle happens, the Driver Configuration File is removed from the installed Xerox® Workplace Cloud Clients.

Setting Priority Order to Xerox XML Driver Configuration

The priority order is used to determine the order of the **XML Driver Configuration** file that get installed on the users computer. If there is more than one XML Driver Configuration file associated to the given user, use the **Move Up** and **Move Down** options on **Actions** menu to change the priority order.

To change the Priority order of the XML Driver Configuration:

1. Click **Account > Settings > Desktop Printing > Configuration**.
2. To move the Xerox Driver Configuration file to the highest priority or move up the priority order, select the **Xerox Driver Configuration** file, click **Actions > Move Up**, repeat the step to move up the priority order to the required number.
3. To move the Xerox Driver Configuration file to the least priority or move down the priority order, select the **Xerox Driver Configuration** file, click **Actions > Move Down**, repeat the step to move down the priority order to the required number.

Drivers


Drivers tab provides the ability to create specific print drivers for your Cloud enabled devices. You can create, configure, and manage drivers that can be assigned to your printers.

In Workplace Cloud, you can create the following drivers for your printers based on the requirements, for more details on each drivers refer to the below sections:

- Custom Drivers
- Composer Files
- Mac PPD

General Steps for Setting up and Using the Drivers

For Windows Custom Drivers

1. Create and prepare your Custom Driver, refer to [Preparing the Driver for Upload](#).
 2. Prepare the optional DriverMetaData.xml file, refer to [Preparing the DriverMetaData.xml file](#).
-  Note: You can skip the attachment of DriverMetaData.xml file if there are no errors when uploading the drivers. If you are adding Finishers to the Custom Driver then the DriverMetaData.xml is required.
3. Package your Custom driver and upload it, refer to [Upload Custom Print Driver in Workplace Cloud](#).
 4. You can associate a Custom Driver to a Direct Printer or Pull Print Queue.
 - a. To associate a Custom Driver to a Direct Printer, refer to [Associate Printers to a Custom Driver](#) or [Select the Driver Type for Direct Printers](#).
 - b. To set up a Pull Print Queue and associate a Custom Driver to it, refer to the [Queues](#) section.

For Windows Composer Files

1. [Download and Extract the Xerox® Workplace Solutions Print Queue Composer Tool](#).
2. Install the Printer Drivers on the server where you want to create the Composer file.
3. Set the required Printer Defaults for the Print Driver.
4. Launch the Xerox® Workplace Solutions Print Queue Composer Tool and follow the steps listed on the user interface to export the Composer File.
5. Import the exported Composer File into Workplace Cloud, refer to [Import the Composer File into Workplace Cloud](#).
6. You can associate a Composer File to a Direct Printer or Pull Print Queue.
 - a. To associate the direct Printers to the Composer File, refer to [Associate Printers to a Composer File](#) or [Select the Driver Type for Direct Printers](#).
 - b. To set up a Pull Print Queue and associate a Composer File to it, refer to the [Queues](#) section.


For Mac PPD

1. Create a Custom Mac PPD, refer to [Creating a Custom Mac PPD](#).
2. To set up Pull Print Queue and associate a Mac PPD to it, refer to [Queues](#) section.

Custom Drivers

Provides the ability to use specific print drivers for your Cloud-enabled printers. Custom drivers can be assigned to [Direct Print](#) or [Pull Print Queue](#). Only Windows v3 drivers are supported. The driver should be in ZIP format and must contain the x86 and x64 drivers.

By default, the **Xerox PullPrint PS Driver 5.887.3.0** and **PullPrint PCL6 Driver 5.887.3.0** drivers are pre-installed. Custom drivers, you can associate a Direct Printer or Pull Print Queues to these drivers. You cannot update or delete these pre-installed drivers.

 Note: If you need to create the Fiery Custom Driver, refer to [Setting up the EFI Fiery Custom Drivers for Windows Desktop Client](#) section.

Custom Drivers for Windows

Preparing the Driver for Upload

The Custom Driver upload feature in Workplace Cloud requires both the 32-bit (86x) and 64-bit (64x) versions of a V3 driver that are bundled up into one zip file.



Note: V4 drivers are not supported by the Custom Driver feature in Workplace Cloud, only V3 drivers, or drivers that include the full set of driver files as opposed to some type of application or installer are supported.

Assuming that you have already downloaded the 32-bit (86x) and 64-bit (64x) versions of a V3 driver to your desktop, follow the steps below to bundle up a Custom Driver for use with the Workplace Cloud Client.

1. Navigate into the directory where the 32-bit (x86) driver package is downloaded. This should contain all of the files for the driver including the .ini file.
2. Right click the Driver file and click **Extract All**, select a destination and extract files, for example C:\Users\<user>\Desktop\Pullprint_5.617.7.0_PCL6_x86\Pullprint_5.617.7.0_PCL6_x86_Driver.inf.
3. Navigate into the directory where the files are extracted.
4. Select all the files, right click and click on **Send to Compressed (Zipped) folder**.
5. Rename the zipped 32 bit driver file with required driver name, for example PullPrint32.zip
6. Repeat the same procedure for the 64-bit (x64) driver.
7. If you are adding Finishers to the Custom Driver then the **DriverMetaData.xml** is required. Refer to [Preparing the DriverMetaData.xml file](#).
8. Select the zipped 32-bit (86x) driver file, 64-bit (64x) driver file and **DriverMetaData.xml** file from your Desktop, right click and click on **Send to Compressed (Zipped) folder**.
9. Rename the resulting zip file to something descriptive, for example PullPrintPS.zip.
10. Inspect the contents of the zip file by clicking on the zipped driver file and ensure there are no sub folders.



Note:

- Each driver zip file must have all file files at root level with no sub folders.
- Ensure each driver zip file contains only one .ini file.

The Custom Driver is prepared and ready to upload.

11. To upload the custom driver to Workplace Cloud, refer to [Upload Custom Print Driver in Workplace Cloud](#).
12. If there is an error when uploading the Custom Driver you may need to add the **DriverMetaData.xml**. Refer to [Preparing the DriverMetaData.xml file](#).

Preparing the DriverMetaData.xml file




Note: To add Installable Options such as Finishers to your Xerox Global Printer Drivers as a Custom driver, refer to [Set the Printer Model and Finisher in the DriverMetaData.xml Configuration File](#). This is optional.

1. Login to the Xerox® Workplace Cloud as an administrator.

2. Click **Account > Settings > Desktop Printing > Drivers > Custom Drivers**.


New Custom Driver section appears.

3. Click **Actions > Add**.
4. Under New Custom Driver field, click on the **DriverMetaData.xml** to download the sample **DriverMetaData.xml** file.
5. Copy the **DriverMetaData.xml** file and paste it in the Driver folder which is created on your computer.
6. Open the **DriverMetaData.xml** file, and do the following action:
7. Rename the Manufacturer name as required at `<Manufacturer>Manufacturer Name</Manufacturer>`.
8. Rename Driver Model name to the Driver Model you are using between the `<Model>` tag.


 Note: To get the Driver Model name, open the **.inf** file located in your downloaded driver folder. The **.inf** file name and location can be different based on the driver you are using. For example, the Xerox GPD **.inf** file is called **x3UNIX.inf**. An example for the Driver Model name line that was extracted from that file is: **Xerox_UPD_0="Xerox Global Print Driver PCL6"** where, Xerox Global Print Driver PCL6 is the Driver Model Name that you would use.

 Note: To add Installable Options such as Finishers to your Xerox Global Printer Drivers as a Custom driver, refer to [Set the Printer Model and Finisher in the DriverMetaData.xml Configuration File](#). This is optional.

9. Rename the Zip file Name as x64.zip at `<ZipFile>ZipFile Name</ZipFile>`.
10. Rename the InfFile Name at `<InfFile>InfFile Name</InfFile>` with the .inf file name present in your x64 zip folder.
11. Rename the CatalogFile Name at `<CatalogFile>CatalogFile Name</CatalogFile>` with the .cat file name present in your x64 zip folder.
12. Do the steps from 9–11 for x86 driver.
13. Save the **DriverMetaData.xml** file.
14. The created DriverMetaData.xml file needs to be placed in the root of the custom driver.zip file before you upload it, refer to [Preparing the Driver for Upload](#).

 Note: DriverMetaData.xml file helps the user to upload the Custom Driver successfully on Xerox Workplace Cloud application. You can skip the attachment of DriverMetaData.xml file if there are no errors in uploading the drivers.

Set the Printer Model and Finisher in the DriverMetaData.xml Configuration File

 Note: This option is only supported when using the Xerox Global Printer Driver as a custom driver.

To add a Finisher details to the **DriverMetaData.xml** Configuration File.

1. Open the **DriverMetaData.xml** Configuration File for editing.

2. Add the following XML tags below the existing <Model> tag.

```
<XeroxGlobalPrintDriver>
<PrinterModel>Model Name</PrinterModel>
<Finisher>Finisher API Value</Finisher>
</XeroxGlobalPrintDriver>
```

3. Next to the <PrinterModel> tag add the Printer Model.



Note: To get the Printer Model name, select the printer that was installed using Xerox GPD Driver and go to the **Control Panel > Devices and Printers**. Right click on the printer and click on the **Printer Properties > Administration > Configuration**. On the **Configuration** drop down you will get the list of Printer Model names.

4. Enter the Finisher API values between the <Finisher> tag. For Finisher API value name, refer to [Printer Finishers API Values](#) tables below. Ensure that you select the correct table for your printer family.
5. After defining the Finisher, continue with step 8 of [Preparing the DriverMetaData.xml file](#) task.
6. Refer to [Validating the Configuration of the Custom Printer Driver](#) to check whether the driver is configured correctly.

Printer Finishers API Values



Note: The finishers listed below are not supported by all printer models. Refer to your printer documentation for finisher's that are supported by your printer.

The tag name for the Installable Option Finisher is <Finisher>.

Altalink

FINISHERS	API VALUES
Offset Catch Tray (OCT)	offset-catch-tray
Office Finisher	office-finisher
Office Finisher LX	type-sb
Integrated Office Finisher	a-type-finisher
Office Finisher with Booklet Maker	officer-finisher-booklet-maker
Office Finisher LX with Booklet Maker	type-sb-booklet-maker
BR Finisher	br-finisher
BR Booklet Maker Finisher	br-finisher-booklet-maker
High Volume Finisher	hvf
High Volume Finisher with Booklet Maker	hvf-bm
Global Integrated Office Finisher	ga-type-finisher

Versa Link

FINISHERS	API VALUES
Not Installed	not-installed
Mailbox	sct-mailbox
Finisher Tray	a4-type-finisher
Offset Catch Tray (OCT)	Not supported
Office Finisher	office-finisher
Office Finisher LX	type-sb
Integrated Office Finisher	a-type-finisher
Office Finisher with Booklet Maker	office-finisher-booklet-maker
Office Finisher LX with Booklet Maker	type-sb-booklet-maker
BR Finisher	Not supported
BR Booklet Maker Finisher	br-finisher-booklet-maker
High Volume Finisher	Not supported
High Volume Finisher with Booklet Maker	Not supported
Global Integrated Office Finisher	ga-type-finisher

Prime Link

FINISHERS	API VALUES
Offset Catch Tray (OCT)	offset-catch-tray
Simple Catch Tray (SCT)	simple-catch-tray
BR Finisher	br-finisher
BR Booklet Maker Finisher	br-finisher-booklet-maker
PR Finisher	pr-finisher
PR Finisher Plus	pr-finisher-ftm
PR Booklet Maker Finisher	pr-finisher-booklet-maker
High Capacity Stacker	hcs
HCS + PR Finisher	hcs-pr-finisher
HCS + PR Booklet Maker Finisher	cs-pr-finisher-booklet-maker
HCS + PR Finisher Plus	hcs-pr-finisher-ftm

Upload Custom Print Driver in Workplace Cloud

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select **Account > Settings > Desktop Printing > Drivers > Custom Drivers**.
The Custom Drivers section appears.
3. To create a new Custom Driver, click **Action > Add**.
The New Custom Driver page appears.
4. On the Name field, enter the name of the Custom Driver.
5. In the New Custom Driver section, click **Choose File**.
6. Browse to the location of the Custom Driver zip file on your computer, click Open.
The file name appears in the Choose File field.



Note: Ensure that the driver is in .zip format, and supports both x86 and x64 systems. If you are getting errors when uploading the custom driver, you can include a .xml file (DriverMetaData.xml) in the .zip file to describe the driver that you are uploading, refer to [Preparing the DriverMetaData.xml file](#).

7. Click **Save**.
The new Custom Driver appears in the Custom Drivers list.

Associate Printers to a Custom Driver



Note: A Custom Driver must be added before associating the printers to it, to add a new Custom Driver, refer to [Upload Custom Print Driver in Workplace Cloud](#).

To associate Printers to a Custom Driver:

1. Click on **Account > Settings > Desktop Printing > Drivers > Custom Drivers**.
2. Click on the Custom Driver name to which you want to associate the printers.
3. Click **Printers** tab.
4. Click **Actions > Add**.
List of Enabled Printers appears.
5. Select the required printers that you need to associate and click **Save**.
The selected printers are associated with the Custom Driver.

Remove Printers from a Custom Driver

To remove Printers from a Custom Driver:

1. Click on **Account > Settings > Desktop Printing > Drivers > Custom Drivers**.
2. Click on the Custom Driver name from which you want to remove the Printers.
3. Click **Printers** tab.
4. Select the required Printers from the list.

5. Click **Actions > Remove**.

The selected printers are removed from the Custom Driver Printers list.

Delete a Custom Driver

Before deleting the Custom Drivers, remove the Printers that are associated with that Custom Drivers, refer to [Remove Printers from a Custom Driver](#).

To delete the Custom Drivers:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select **Account > Settings > Desktop Printing > Drivers > Custom Drivers**.

The Custom Drivers section appears.

3. Select the required Custom Drivers from the list of Custom Drivers.
4. Click **Actions > Delete**.

The selected Custom Drivers are deleted from a Workplace Cloud account.

Validating the Configuration of the Custom Printer Driver

To validate the configuration of a **Custom Driver** that you created, you are instructed below to install the **Custom Driver** using Cloud Client and then checking the printer configuration settings are correct.

1. Associate a **Custom Driver** or **Composer File** with a Direct Printer, refer to [Select the Driver Type for Direct Printers](#).
2. Associate a **Custom Driver** or **Composer File** to a Pull Printer, refer to [Adding Pull Print Queue](#).
3. Install the Workplace Cloud Client, refer to [Installing the Xerox® Workplace Cloud Windows Client](#).
4. Install the Printers or Pull Print Queues on your client Computers, refer to [Deployment Groups](#).
5. Go to Windows **Control Panel > All Control Panel Items > Devices and Printers > Printers**.
6. Select the required print driver, right click and select **Printer Properties**.

The **Properties** dialogue box appears.

7. Click the **Administration** tab and ensure that the Model name of the printer is correct.
8. Click the **Configuration** tab and ensure the that Installable Options, Finishers is correct.

Composer Files

The **Xerox® Workplace Solutions Print Queue Composer** tool that can be downloaded from Xerox® Workplace Cloud, captures print drivers and preconfigured driver settings and zips them into a file called a Composer file. The Composer zip file can be uploaded into Xerox® Workplace Cloud and associated with a Direct Printer. Once the Composer File is associated with a Direct Printer, the Workplace Cloud Client will download the Composer File and install the driver and add the print queue.

The printer can be installed by using printer Deployment Groups or manually installed by the user.



Note: This feature requires version 5.8.111 or higher of the Xerox® Workplace Cloud Client.

Guidelines:

- When a Composer File is associated with a Direct Printer, make sure the Composer File is compatible with that printer.
- Workplace Cloud only supports Composer files which are extracted from a Windows x64 bit Operating system.
- Composer files can only be created and uploaded to Xerox® Workplace Cloud using the Xerox® Workplace Solution Print Queue Composer tool.
- If a user tries to upload a non-Composer File, the following error message is displayed:
 - This Composer File is not valid. Use the Xerox® Print Queue Composer tool to generate a new one and try again.
- If a Composer File has not been uploaded and a user selects save, the following error message is displayed:
 - Composer file is required.
- Direct printers that are linked to a Composer File will use the Xerox® Global Print Drivers if the Composer File is deleted.

Setting Up the Composer File

Xerox Print Queue Composer Tool

Xerox® Workplace Solutions Print Queue Composer tool is used to export and create a Composer File of the Printers from a server.

Download and Extract the Xerox® Workplace Solutions Print Queue Composer Tool

To download and extract the Xerox Print Queue Composer Tool:

1. Click on **Account > Settings > Desktop Printing > Drivers > Composer Files**.
2. Click on the **Xerox® Print Queue Composer** link.
3. Once the **Xerox® Print Queue Composer** file is downloaded, unzip the downloaded file to a local directory.
4. Run the **Xerox.Workplace.PrintQueueComposer.exe** file to launch the application.

Export the Composer files of the Printer



Note: You must have an administrator access on your local machine to run the Xerox® Workplace Solutions Print Queue Composer tool.

1. Open the folder where you have extracted the files of **XeroxWorkplacePrintQueueComposer** tool.
2. Right click on the **Xerox.Workplace.PrintQueueComposer.exe** file and click **Run as administrator**.
3. The Xerox® Workplace Solutions Print Queue Composer tool is opened.
4. Click on **Get local Printers** to fetch the local printers list.
5. Select the required printers from the list for which you need to generate the composer files.
6. Select the file path by clicking on **Choose Path**.
7. Click on **Export printer**.

8. The Printer composer files are generated and placed in the defined file path.

Import the Composer File into Workplace Cloud

Only Composer files generated by the Xerox® Print Queue Composer tool can be uploaded into Xerox® Workplace Cloud.



Note: You can only upload the Composer File extracted from Windows x64 bit Operating System.

1. Click on **Account > Settings > Desktop Printing > Drivers > Composer Files**.
2. Click on **Actions > Add**.

A Composer File wizard is opened.

3. On the **Details** section, enter the Name and Description.
4. On New Composer File, select **Choose File** option.
5. Select the required extracted Composer File from your local disk.



Note: To extract the Composer File, refer to [Export the Composer files of the Printer](#).

6. Click **Save**.

Settings have been saved successfully message appears and the Composer File is successfully uploaded into Workplace Cloud account.

Associate Printers to a Composer File



Note: A Composer File must be set up before associating the Printers, to set up Composer File, refer to [Setting Up the Composer File](#).

To associate Printers to a Composer File:

1. Click on **Account > Settings > Desktop Printing > Drivers > Composer Files**.
2. Click on the Composer File name to which you want to associate the printers.
3. Click **Printers** tab.
4. Click **Actions > Add**.

List of Enabled Printers appears.

5. Select the required printers that you need to associate and click **Save**.

The selected printers are associated with the Composer File.

Remove Printers from a Composer File

To remove Printers from a Composer File:

1. Click on **Account > Settings > Desktop Printing > Drivers > Composer Files**.
2. Click on the Composer File name from which you want to remove the Printers.
3. Click **Printers** tab.
4. Select the required Printers from the list.

5. Click **Actions > Remove**.

The selected printers are removed from the list.

Delete a Composer File

Before deleting the Composer Files, remove the Printers that are associated with that Composer Files, refer to [Remove Printers from a Composer File](#).

To delete the Composer Files:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select **Account > Settings > Desktop Printing > Drivers > Composer Files**.

The Composer Files section appears.

3. Select the required Composer Files from the list of Composer Files.
4. Click **Actions > Delete**.

The selected Composer Files are deleted from a Workplace Cloud account.

Mac PPD

Custom Print Drivers for Mac

When you create a custom driver in the Xerox® Workplace Cloud Web Portal, you can specify the Mac Postscript Printer Description (PPD) to include in the print driver package. After you enable the Mac PPD option, you can type a PPD name manually or select from a predefined list of names based on the Xerox® PPD print driver file.



Note: Before you install Macintosh Workplace Cloud Client, ensure that the Xerox Macintosh Print and Scan driver or third-party driver is installed on all the Macintosh workstations. The Cloud Mac Client does not automatically install drivers. After installation, the Mac Client is operated from the Macintosh status bar.

Creating a Custom Mac PPD

To create a Custom Mac PPD and specify the Mac PPD, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Settings > Desktop Printing > Drivers > Mac PPD**.
3. Click **Actions > Add**.

The New Custom Mac PPD screen appears.

4. On the Details, Name field, provide the MAC PPD Name.
5. On the Driver Selection, select any one of the following option to define the MAC PPD:
 - Select from List: This option allows you to select from the pre-populated driver list from the drop down.
 - Specify Manually: This option allows you to manually enter the Mac PPD Name, and it should match the PPD installed on your MAC device.
6. Click **Save**.

The new Mac PPD is created and added to the MAC PPD list.

Delete a Custom Mac PPD

To delete a Custom Mac PPD:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Settings > Desktop Printing > Drivers > Mac PPD**.
3. Select the required MAC PPDs from the list.
4. Click **Actions > Delete..**

The selected MAC PPDs are deleted from the list..

Direct Print

For Workplace Cloud, the Direct Print option is introduced with a generic print driver. You can configure the print driver used for the Direct Print path with any printer in your company.

Select the type of driver to be used with the direct printer. By default, all printers use the Xerox Global Print Driver. You can change the print driver to a Windows Custom Driver or Composer File and optionally add a Mac PPD.

1. To access Direct Print from the Cloud, log in to Workplace Cloud as a system administrator.
2. Select **Account > Settings > Desktop Printing**. Click **Direct Print**.
3. To select the Driver Type, refer to [Select the Driver Type for Direct Printers](#).

When a new Driver is added and enabled, the driver appears in the **Print > Desktop** menu.

Select the Driver Type for Direct Printers

By default, all printers use the Xerox Global Print Driver. You may change the print driver to a Custom Driver, Composer File, or a Mac PPD.

To set the Driver Type for the Direct Printer:

1. Select **Account > Settings > Desktop Printing > Direct Print**.
2. Select the required printers from the list.
3. Click on **Actions > Select Driver Type**.
4. Select the required Driver type:
Driver Selection: **Windows**

- Default: Xerox® Global Print Driver
- Composer Files



Note: If you choose Composer File, select the required Composer File from the Available Composer File list.

- Custom Drivers



Note: If you choose Custom Drivers, select the required Custom Drivers from the Available Custom Drivers list.

- Driver Selection: **Mac**



Note: If you choose Mac, select the required Mac PPD you would like to assign to the direct print device (s) from the Available Mac PPDs.

5. Click **OK**.

The required Driver Type is set for the Direct Printers.

6. Click **Save**.



Note: The driver type selected is displayed on the Direct Print listing page to the right of the Direct Printer, if there is no driver associated with direct printer, Default is displayed.

Queues

Queues tab provides the ability to create Pull Print Queues that use specific print drivers for your Workplace Cloud enabled printers.

You can do the following action on Queues Tab:

- Add Pull Print Queues
- Enable Pull Print Queues
- Disable Pull Print Queues
- Enable as Default Printer
- Disable as Default Printer
- Delete Pull Print Queues



Note: You can associate a **Pull Print Queues** to a **Deployment Group**, refer to [Deployment Groups](#) section.

Add Pull Print Queue

To add a Pull Print Queue, do the following action:

1. Click **Account > Settings > Desktop Printing > Queues** tab.
2. Click **Actions > Add**.

Pull Print Queue: New page appears.

3. On the Details Section:
 - Select the check box for **Enable**, if you need users to install this pull print queue on their desktop client and upload print jobs to a generic printer using the driver assigned to this Pull Print Queue.
 - Enter the required **Printer Name** and **Description** of your new Pull Print Queue.
 - Select the check box for **Default Printer** to install the printer automatically once Xerox® Workplace Cloud Client is installed.

4. On the **Driver Selection**:

For Windows:

- If your Driver selection is **Composer Files** for your Pull Print Queue:
 - Click **Change**, select the required **Composer File** from the Available Composer Files list that you like to assign to this pull print Queue.
- If your Driver selection is **Custom Drivers** for your Pull Print Queue:
 - Click **Change**, select the required **Custom Driver** from the Available Custom Drivers list that you like to assign to this pull print Queue.

For Mac:

- Click **Change**, select the required **MAC PPD** from the Available MAC Drivers list that you like to assign to this pull print Queue.

5. Click **Save**.

The Pull Print Queue is created and saved on the Pull Print Queue list.

Enable or Disable Pull Print Queues

To enable or disable the Pull Print Queues, do the following action:



Note: Enabling Pull Print Queues allows users to install the Pull Print Queue on their desktop client and upload print jobs to a generic printer using the drivers associated with the Pull Print Queue.

1. Click **Account > Settings > Desktop Printing > Queues** tab.
2. To enable the Pull Print Queues, select the required Pull Print Queues from the list, click **Actions > Enable**.
3. To disable the Pull Print Queues, select the required Pull Print Queues from the list, click **Actions > Disable**.



Note: You can also enable or disable a Pull Print Queue on editing the Pull Print Queue.

4. Click **Save**.

The required Pull Print Queues are enabled or disabled.

Enable or Disable Default Printer on the Pull Print Queue

To enable or disable the Default Printer on the Pull Print Queue, do the following action:



Note: Enabling the Pull Print Queue as Default Printer will install the Printer automatically once Xerox® Workplace Cloud Client is installed.

1. Click **Account > Settings > Desktop Printing > Queues** tab.
2. To enable the Pull Print Queue as a **Default Printer**, select the required Pull Print Queues from the list, click **Actions > Enable as Default Printer**.
3. To disable the Pull Print Queues as a **Default Printer**, select the required Pull Print Queues from the list, click **Actions > Disable as Default Printer**.



Note: You can also edit the Pull Print Queue to enable or disable the Default Printer for the Pull Print Queue.

4. Click **Save**.

The required Pull Print Queue are enabled or disabled as the Default Printer.

Delete the Pull Print Queue

To delete the Pull Print Queue, do the following action:



Note: Deleting the Pull Print Queue disassociates the Pull Print Queue from any existing Deployment Groups.

1. Click **Account > Settings > Desktop Printing > Queues** tab.
2. Select the check box of the required Pull Print Queue from the list.
3. Click **Actions > Delete**.

The selected Pull Print Queue is removed from the Pull Print Queues list.

SETTINGS: FEATURE DEFAULTS

Configuring the Auto Release All Jobs Setting

The Auto Release All Jobs feature allows you to control when the jobs are released to the printer. When the jobs are printed using the auto release feature, after they are printed, they are deleted from the system.

1. Select **Account > Settings > Feature Defaults**.
2. In the Auto Release All Jobs area, select one of the following radio buttons:
 - **Never:** Jobs are not released automatically. The user has to select the jobs to release using the Printer Client application.
 - **Using Access Card or Alternate Login:** After the user completes the login sequence, this option releases all the jobs of the user.
 - **Prompt:** When you select the radio button for **Using Access Card or Alternate Login**, the **Prompt** option appears. During the login sequence, users are prompted to release their jobs.
 - **Using Network Appliance:** When users scan a card at a mapped network appliance, such as RF Ideas Ethernet 241, Elatec TCPConv, or Elatec TCPConv2/3, this option releases all the jobs of the user.

SETTINGS: HOME WORKER PRINT TRACKER



Note: The Home Worker Print Tracker feature is supported on the Windows version of the Xerox® Workplace Cloud Client only.

The Home Worker Print Tracker feature of the Xerox® Workplace Cloud solution enables you to monitor and track printing from company-owned workstations. The Home Worker Print Tracker feature allows users to print to their home printers and Xerox® Workplace Cloud tracks their print history. The Home Worker Print Tracker print history is included in the company reporting data. The reporting data allows the administrator to monitor the employee usage of company-owned home printers, and track company prints on user-owned printers or printers not enabled in Xerox® Workplace Cloud. The information can be used for supplies ordering and reimbursement. The solution tracks information such as job names, number of pages printed, color or black white pages, time of submission, number of copies, 1-sided or 2-sided, and accounting information. The data is reflected in the Job Reporting Dashboard. For more information, refer to [Dashboard](#).

For more information on the Workplace Client, refer to [Workplace Client Overview](#).

Enabling Home Worker Print Tracker

When the Home Worker Print Tracker feature is enabled, the desktop client application installs a port monitor shim for printers using Windows v3 print drivers. The following port types are supported for this feature:

- Standard TCP/IP port
- LPR port
- USB port
- WSD Port

Other port types are not supported. When a printer is shimmed with the Home Worker Print Tracker module, the client collects metadata about the jobs submitted to these shimmed devices, and reports the data to Xerox® Workplace Cloud.

To enable the Home Worker Print Tracker feature, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select the **Account** tab.
3. Click **Settings > Home Worker Print Tracker**.
4. Select the check box for **Enabled**.

The Accounting Prompts section appears. For more information, refer to [Home Worker Print Tracking Accounting Prompts](#).

5. To enable the following options, select one of the following check boxes:
 - **Prompt for Accounting User ID**
 - **Prompt for Accounting Account ID**
6. To save the setting, click **Save**.

Home Worker Print Tracking Accounting Prompts

If the Accounting prompts option is enabled, in the Xerox® Workplace Cloud Client, a pop-up window prompts you to enter the accounting information for the print job. If you do not enter the values, the job is deleted. It is recommended that you provide the accounting information to the user. The accounting information is added to the job information in the job reports.

When Home Worker Print Tracker is enabled, an option to enable accounting prompts appears. The two accounting prompts options are:

- **Prompt for Accounting User ID**
- **Prompt for Accounting Account ID**

If you do not select one of these options, the user is not prompted to enter any accounting codes at print submission time. If either or both fields are selected, when the user submits a print job, they are required to enter a value for each enabled field. If the user selects **Cancel** or **Close** in the pop-up window, the print job is deleted.

SETTINGS: LDAP CONNECTIONS

LDAP Synchronization

All Xerox® Workplace Cloud Agents identify the established LDAP connections on the Windows system where they are installed, and report those connections back to the Cloud.

LDAP Connections are available as a User Association type in the creation of User Groups for Rules. System administrators can set up deletion filters that check each time existing users log in with a badge. The Cloud lets the user log in, but validates asynchronously that the user is not in the configured deletion filters. If users are in one of the filters, they are logged out forcibly. System administrators can set up a custom set of LDAP containers. If system administrators do not customize LDAP containers, the Cloud defaults to the LDAP root node.

LDAP credentials are listed for each user, on the Users tab, under User Information. LDAP connections synchronize users with the Cloud User Database in real time, as users authenticate with the Cloud. System administrators can delete LDAP connections reported to the Cloud by Agents.

The Xerox® Workplace Cloud obeys a deletion of LDAP connections made by system administrators and reported by Agents. The next time that the Agent communicates with the Cloud, the Cloud ensures that LDAP connections do not appear in the Web Portal automatically.

LDAP Configuration Modes

All LDAP connections are auto-enabled by default. When a system administrator modifies one auto-enabled LDAP connection, all subsequent LDAP connections that are newly identified and reported to the Cloud are disabled by default. System administrators that require a controlled, secure system that does not auto-enable LDAP connections by default, and switches the Configuration Mode to **Manual**. After switching the Configuration Mode from **Manual** to **Automatic** mode, all manual LDAP configurations are lost. The Cloud resumes the reporting and enablement of all LDAP domains in Automatic mode from the Agent.

- **Automatic:** All domains reported by Agents are enabled always, and are not configured. When the modes are switched from Manual mode to Automatic mode, all configurations made in Manual mode are lost.
- **Manual:** System administrators can enable or disable domains, and access advanced configuration options. When Manual mode is enabled, and when a user clicks Save, the LDAP Connections grid appears.

Editing LDAP Configuration Modes

1. Log in as an administrator to Xerox® Workplace Cloud version 5.1.
2. Select **Account > Settings > LDAP Connections**.
3. Select the check box for **Automatic** or **Manual**.
4. Click **Save**.

Enabling or Disabling an LDAP Connection

1. Log in as an administrator to Xerox® Workplace Cloud.
2. Select **Account > Settings > LDAP Connections**.
3. Click **Actions**. For the LDAP connections, select **Enable** or **Disable**.
4. Click **Save**.

Editing LDAP Connections

The LDAP server is used to authenticate and synchronize users with the Xerox® Workplace Cloud user database.

1. Log in as an administrator to Xerox® Workplace Cloud version 5.1.
2. Select **Account > Settings > LDAP Connections**.
3. To edit an LDAP connection, from the list, click an existing LDAP connection.

An Edit LDAP Connection window appears. The Server tab shows Details, Test Connection, and Usage Mode.

4. To test a connection, on the Server tab, type a user name and password, then click the **Test Connection** button.

The Test Connection results appear. The results can be any of the following:

- Green check icon: A green check icon indicates that the test connection is successful.
- Red cross icon: A red cross icon indicates that the test connection is unsuccessful. Verify the settings, then try the test connection again, using the correct LDAP credentials.



Note: Ensure that LDAP credentials are accurate. Multiple trials with the wrong password can block the account from the Cloud system.

5. For Usage Mode, select **Simple** or **Advanced**.
 - **Simple:** This mode uses standard field mappings.
 - **Advanced:** This mode is for customized field mappings.
 - a. When you select Advanced mode, a new LDAP Credentials section and an **Advanced** tab appear. On the Server tab, type the user name and password for a saved LDAP Credentials user.



Note: To activate the Advanced tab, customize field mappings, and deletion containers, the saved LDAP credentials are required.

- b. On the Advanced tab, Field Mapping and User Synchronization sections appear. To customize the Field Mapping information, enter the user details, as required.
- c. For User Synchronization, set up the Deletion Filter. To locate the users who should no longer use their badges to log in to the account, click Deletion Filter.
- d. From the list, click LADP Containers. To create an LADP Container, select **Actions > New**. Type the name of the new LADP Container, then click **Save**.
- e. To delete an LADP Container, select the LADP Container, then select **Actions > Delete**.



Note: The Cloud default is to scan the entire LDAP root node. To prevent the Cloud from scanning the entire LDAP root node, you can customize the LDAP Containers.

6. Click the Agents tab. In the LDAP domain, verify the list of Associated Agents installed on the workstation.
7. Click **Save**.

SETTINGS: AZURE AD CONNECTIONS

Use the Azure AD connections page to configure the Azure AD tenants that you want in Xerox® Workplace Cloud for Advanced Azure AD Authentication.



Note: When you have added Azure AD connections, refer to [Azure AD Authentication](#) section to enable Advanced Azure AD Authentication.

Adding an Azure AD Connection

To add an Azure AD connection, do the following:

1. Select **Account > Settings > Azure AD Connection**.
2. From the Actions menu, click **Add**.

The Add Azure AD Connection page appears.

3. Configure the settings in the following tabs:
 - **Details:** For more information, refer to [Configuring the Azure AD Connection Information](#).
 - **Web Application:** For more information, refer to [Setting the Web Application Values](#)
 - **Native Application:** For more information, refer to [Setting the Native Application Values](#)
 - **Field Mappings:** For more information, refer to [Setting the Field Mapping Values](#)
4. Click **Save**.

Configuring the Azure AD Connection Information

To configure the Azure AD connection information, do the following:

1. Click the **Details** tab.
By default, the **Enabled** check box is selected.
2. In the Name field, type a name for the connection.
3. Go to your Azure Active Directory Tenant in the Azure portal.
4. On the Overview page, from Directory (tenant) ID, copy the tenant ID.
5. Go to the Workplace Cloud Web portal.
6. In the Tenant ID field, paste the copied value.
7. In the Email domain(s) section, select one of the following radio buttons:
 - **Use for any email domain:** If any existing connection has this option selected already, deselect this radio button. Only one connection can have this option enabled.
 - **Use only for specified email domains:** If you select this radio button, add at least one email domain as follows:
 - In the Email Domains field, type the required email domain.
 - Click **Add**. In the Assigned Email Domains field, the added email domain appears.
8. Click **Save**.

Setting the Web Application Values

To set the Web Application values, do the following:

1. In the Azure portal, go to your Azure Active Directory Tenant.

2. On the Overview page, do the following:
 - a. Select **App registrations > New registration**.
The Register an application window appears
 - b. Type a name for the application.
 - c. Select the radio button for **Accounts in this organization directory only (AD Name only – Single Tenant)**.
 - d. Click **Register**.
 - e. From the Azure portal, copy the Application (client) ID.
3. Go to the Xerox® Workplace Cloud Web portal. On the Add Azure AD Connection screen, do the following:
 - a. Select the **Web Application** tab.
 - b. In the Register the new application area, in the Client ID field, paste the copied ID.
4. 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**, 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 GroupMember section, select the check box for **GroupMember.Read.All**.
 - Click **Update Permissions**.
 - d. Click **Grant admin consent for**.
A confirmation message appears.
 - e. Click **Yes**.
5. Go to the Azure portal, then from the navigation pane, do the following:
 - a. Click **Authentication**.
The Platform configurations page appears.
 - b. In the Implicit grant and hybrid flows section, select the check box for **Access tokens (used for implicit flows)**.
The access token is enabled.
6. In the navigation pane, click **Certificates & secrets**.
 - a. In the Client secrets area, click **New client secret**.
The Add a client secret dialog appears.
 - b. In the Description field, type the required description.
 - c. In the Expires field, select one of the options.

- d. Click **Add**.
The Client secrets grid appears.
- e. In the Client secrets grid, copy the Value.
If the Value field has asterisked, you are required to create a client secret.
7. Go to the Xerox® Workplace Cloud Web portal, then do the following:
 - a. Select the **Web Application** tab.
 - b. In the Create a client secret area, paste the copied value.
8. Go to the Azure portal, then do the following:
 - a. From the navigation pane, Click **Authentication**.
The Platform configurations page appears.
 - b. Click **Add a platform**.
The Configure Platforms dialog appears.
 - c. Click **Web**.
The Redirect URIs field appears in the window.
9. Go to the Xerox® Workplace Cloud 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 URI.
10. Go to the Azure portal, then in the Redirect URIs field, paste the copied URI.
11. Click **Configure**.
The Platform configurations page appears.
12. In the Redirect URIs area, click **Add URI**.
13. On the Xerox® Workplace Cloud Add Azure AD Connection screen, from the Set Redirect URIs on the new application as follows: area, for Redirect URIs copy the second value.
14. Go to the Azure portal. In the Redirect URIs area, click **Add URI**, then paste the URIs.
15. Click **Save**.

Setting the Native Application Values

To set the Native Application values, do the following:

1. In the Azure portal, go to your Azure Active Directory Tenant.
2. On the Overview page, do the following:
 - a. Select **App registrations > New registration**.
The Register an application window appears
 - b. Type a name for the application.
 - c. Select the radio button for **Accounts in this organization directory only (AD Name only – Single Tenant)**.

- d. Click **Register**.
 - e. From the Azure portal, copy the Application (client) ID.
3. Go to the Xerox® Workplace Cloud Web portal. On the Add Azure AD Connection screen, 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.
4. 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**, 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 GroupMember section, select the check box for **GroupMember.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)**.
5. Go to the Azure portal, then from the navigation pane, do the following:
 - a. Click **Authentication**.
The Platform configurations page appears.
 - b. Click **Add a platform**.
The Configure Platforms dialog appears.
 - c. Click **Web**.
The Redirect URIs field appears in the window.
6. Go to the Xerox® Workplace Cloud 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.
7. Go to the Azure portal, then in the Redirect URIs field, paste the copied URI.
8. Click **Configure**.
9. Click **Add a platform**.
The Configure Platforms dialog appears.

10. Click **Mobile and desktop applications**.

The Redirect URIs field appears in the window.

11. Go to the Xerox® Workplace Cloud 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.

12. Go to the Azure portal, then do the following:

- a. In the Custom redirect URIs field, paste the copied URI.
- b. In the Redirect URIs area, click **Add URI**.

13. On the Xerox® Workplace Cloud Add 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.

14. Go to the Azure portal, then do the following:

- a. In the Redirect URIs area, click **Add URI**.
- b. In the Custom redirect URIs field, paste the copied URI.

15. On the Xerox® Workplace Cloud Add Azure AD connection screen, from the Set Redirect URIs on the new application as follows: area, copy the third mobile and desktop application Redirect URIs value.

16. Go to the Azure portal, do the following:

- a. In the Redirect URIs area, click **Add URI**.
- b. In the Custom redirect URIs field, paste the copied URI.

17. Click **Save**.

Setting the Field Mapping Values

The Field Mappings tab allows you to customize which Azure AD fields are used to populate the user fields in the Xerox® Workplace Cloud user database.

To set the field-mapping values, do the following:

1. Click the Field Mapping tab, complete the following fields:



Note: For all the Field Mapping fields, type a value or select a value from the menu.

- Email Address
- User Principal Name Defaults to **userprincipalname** and cannot be changed.
- User Name
- Primary PIN or Access Card Number
- Department

2. Click **Save**.

Configuring the Field Mapping for OnPremiseExtensionAttributes

Introduction

The Workplace Cloud Azure AD Advanced mode allows Workplace Cloud to read Azure AD User Profile values which are contained in the OnPremiseExtensionAttributes compound object.



Note: You can configure your Azure Users in your tenant to have the OnPremiseExtensionAttributes value using the Microsoft Graph API. For more information, refer to [Add custom data to resources using extensions - Microsoft Graph | Microsoft Learn](#).

To configure the Field Mapping for OnPremiseExtensionAttributes:

1. Select **Account > Settings > Azure AD Connection**.
2. Click on the required Azure AD Connection to edit.
3. Select the **Field Mapping** tab.
4. Enter the Field Mapping value, so that it uses one of the sub-components of the OnPremiseExtensionAttribute. For example, providing **Primary PIN or Access Card Number** with COMPOUND_ATTRIBUTE / SUB_ELEMENT.

Example: OnPremiseExtensionAttributes / extensionAttribute5.

5. Click **Save**.

SETTINGS: HELLOID CONNECTION

Use the HelloID page to login to your HelloID tenant and to register a new application that Xerox® Workplace Cloud will use when authenticating users.

Adding an HelloID Connection

To add an **HelloID** connection, do the following:

1. Login to your **HelloID** tenant to register a new application that Xerox® Workplace Cloud will use when authenticating users.
2. Select **Applications** from the Dashboard.
3. Open the Application Catalog and find **Xerox Workplace Cloud** and select **+Add**.
4. Save the Application using the Default Configuration.



Note: All configuration settings required by **HelloID** are pre-set. Review the configuration and click **Save** to finish configuration.

5. Retrieve the Client ID and Secret from the **Configuration** sub menu.
6. Log in to the Xerox® Workplace Cloud Web Portal using your credentials.
7. Select **Account > Settings > HelloID Connection**.
8. Enter the retrieved Client ID and Secret on **HelloID Connection**.
9. Set up the **Hello ID Discovery Document**, refer to [HelloID Discovery Document](#) section.
10. Click **Save**.

HelloID Connection is added successfully.

HelloID Discovery Document

Xerox Workplace Cloud will fetch the discovery document through the provided URL, this allows the solution to communicate with HelloID for authentication requests.

The HelloID Discovery Document webpage URL is the actual webpage URL present on the HelloID Admin portal, to obtain and set up the HelloID Discovery Document URL, refer to [Setting up the HelloID Discovery Document URL](#).

Setting up the HelloID Discovery Document URL

To Set up the HelloID Discovery Document URL do the following steps:

1. Login to your **HelloID** tenant.
2. Select the **Edit** option for **Xerox Workplace Cloud** from your application list.
3. Click **Configuraition** tab and click on **View Discovery Document**.
View Discovery Document webpage is opened.
4. Copy the webpage URL.
5. Log in to the Xerox® Workplace Cloud Web Portal using your credentials.
6. Select **Account > Settings > HelloID Connection**.
7. Under the URL field of Hello Discovery Document, paste the copied URL of View Discovery Document.

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 desktop client and the Web portal optionally. If the user is logged into their workstation, the solution attempts to log the user into Xerox® Workplace Cloud using that same identity. Configure your IdP to trust the Xerox® Workplace Cloud application and provide information for the Xerox® Workplace Cloud solution to communicate with the IdP. This capability is supported for workstations that runs Microsoft Windows.

SAML login is only supported by:

- XWC Desktop Windows Client.
- XWC Web Portal.



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

Fallback Authentication: When a User connects to Cloud and if SAML is enabled and the connection fails, then Xerox® Workplace Cloud will use the current Xerox® Workplace Cloud authentication setting.

IdP and Xerox® Workplace Cloud Configuration

To use SAML, the administrator is required to supply information to the IdP about Xerox® Workplace Cloud, so that it can trust communication coming from the Xerox® Workplace Cloud solution. Similarly, the administrator needs to configure Xerox® Workplace Cloud with information about the IdP so that it knows how to connect to the provider.

If the domain name is not returned as part of the new User SAML claim, you can configure an optional domain value that will be pre-pended to the user name value. See below for more information.

Email Check for SAML Onboarding:

If a user on-boards using the Web Portal or Cloud Client using SAML, the Xerox® Workplace Cloud solution will obtain the email of the User from the SAML claim. The Workplace Cloud solution will check the current email domain mapping for the cloud company and compare it with the User's email domain.

- If they match, then the user will be on-boarded to the respective company.
- If they do not match, the login attempt will be rejected and the user account will not be created. The following error message will be displayed:

User's email domain is not mapped to the company.

To have an email domain mapped to a cloud company, please submit a Xerox support ticket.

The required information includes the following:

- Service provider information to be entered in the IdP
 - Workplace Cloud identifier: `urn:xerox:services:xwctest`
 - SAML assertion endpoints: For the Web portal <https://xwc.services.xerox.com/login/acs>, and for the desktop client <https://com.xerox.services.xwc/login/acs>.
 - Binding: HTTP-POST
 - Field mappings: Ensure that you map the associated fields in your identity provider to the provided Xerox® Workplace Cloud attribute values. The following table shows the importance required in contrast to optional values and the recommended mapping of attributes in ADFS or LDAP to Workplace Cloud:

IDENTITY PROVIDER ATTRIBUTE	WORKPLACE CLOUD	IMPORTANCE
Source: LDAP Attribute Attribute: Email Address Source: Azure Attribute: user.mail	email	Required
Source: ADFS Claim Claim: Windows account name Source: Azure Attribute: user.sAMAccountName	username	Required (for LDAP authentication) Optional (for other methods)
Source: Azure Attribute: user.userprincipalname	user.userprincipalname	Required (for Azure if different than email) Optional (for other methods)

IDENTITY PROVIDER ATTRIBUTE	WORKPLACE CLOUD	IMPORTANCE
Source: LDAP Attribute Attribute: Department Source: Azure Attribute: user.department	department	Optional
Source: Customer Unique Attribute: Customer Unique	pin	Optional



Note: The username attribute value in Workplace Cloud must conform to the format of domain \username. The ADFS claim value of Windows account name returns a value of the format domain \username. It is recommended that you use the ADFS claim value for Windows account name instead of using the LDAP field of SAM-Account-Name.

- **Domain Name:** For new users on-boarding via SAML, if the optional domain name value is configured and the returned username claim from SAML returns only the Username, then the solution will pre-pend the configured domain and a backward slash (\) to the username value before storing it in the Xerox Workplace Cloud user record. This is an optional field and by default, the domain value will be blank.
- Identity provider information to be entered in Workplace Cloud.
 - 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 Cloud 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 Cloud 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

Portal and Client Configuration

To use SAML in the desktop client and Web portal, to bypass the normal email prompt screen, the customer is required to supply an email domain hint as part of the initial connection information to Xerox® Workplace Cloud. The method varies for the Web portal and client. Ensure that the provided domain is preconfigured in Xerox® Workplace Cloud for your company. To map your domain, send a request to your Xerox representative.

Access to the Web Portal

For Web browser authentication, the user is required to provide the domain hint in the URL. The format of the browser URL is `https://xwc.services.xerox.com/<domain>`.

Access to the Desktop Client

For the desktop client, the administrator is required to configure the email domain using the JSON configuration file on the workstation of the user. When a login request is required, the desktop client application reads the configuration file. The file name is `PdlParserSettings.json`, and is located at `%PROGRAMDATA%\Xerox\XMPC`. The contents of the file is as follows:

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

Intranet Zone Configuration

For SAML to work, the Web portal and the desktop client login methods 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*.

SAML Connectivity Requirements

For more information on SAML connectivity requirements, refer to the *Xerox® Workplace Cloud Security Guide*. You can find the guide at <https://security.business.xerox.com>, then select **Software Solutions > Xerox Workplace Cloud**.

General Steps to Configure to SAML with Azure AD

1. Submit a request to your Xerox Support Analyst to map your domain(s) to your Company.
2. Enable Xerox Workplace Cloud SAML.
3. Creation of Azure Entra ID Enterprise App.
4. Testing SAML using the Xerox Workplace Cloud portal.
5. Configuration of Xerox Workplace Cloud Client.

The client domains need to be mapped to the Xerox Workplace Cloud tenant.

Step 1: Tenant Domain Mapping Process

1. Submit a request with the following information to your Xerox Support Analyst to map your domain(s) to your Company.
2. Provide your Company Name.
3. Provide your Company Code.
4. Provide the domains you want to be mapped.

Step 2: Enablement of Xerox Workplace Cloud SAML

In the Xerox Workplace Cloud portal, select **Account > Settings > SAML Connection**.

1. Check the **Enable SAML Support** check box.
Once enabled, the settings will be used to create the Azure Entra ID app.
2. Click **Save**.

Step 3: Creation of Azure Entra ID Enterprise App

1. Log into the Azure Portal.
2. Go to Microsoft Entra ID.
3. Click on **Enterprise Applications**.
4. Click on **New Application**.
5. Click on **Create your own application**.
6. Give the application a name.
7. Select **Integrate any other application you don't find in the gallery (Non-gallery)** radio option which is a default setting.
8. Click on the **Create Button**.
9. Under option 1, click **Assign users and groups**.
10. Click on **Add user/group**.
11. Add the Users or Groups to be assigned to this app.
12. Once Users have been assigned, click on **Overview** in the left Pane.
13. Under option 2, click **Get Started**.
14. Click on **SAML**.
15. Click on **Edit** in Basic SAML Configuration section.
16. Add the identifier from the Xerox Workplace Cloud portal to the Add identifier space.
17. Add the SAML Assertion Endpoint(s) URL from the Xerox Workplace Cloud portal to the Add reply URL space.
18. Click **Save**.
19. Close the Basic SAML Configuration section.
20. Click **Edit** in Attributes & Claims section.
21. Double click the claim name that has a default value of user.email.
22. Update the **Name** and **Namespace** fields.
23. Change the **Name** as email.
24. Delete the **Namespace** URL and leave it as blank.
25. Click **Save**.
26. In SAML Certificates section copy the App Federation Metadata Url to the clip board.
27. Paste the App Federation Metadata Url in the **Metadata URL** field in Xerox Workplace Cloud portal.
28. Enter the optional **Domain Name** field in Xerox Workplace Cloud portal.

29. Click Save.

30. Click on **Refresh** icon.

Step 4: Testing SAML using the Xerox Workplace Cloud Portal

- To skip the email prompt when logging into the Xerox Workplace Cloud web portal, you can supply it as part of the browser URL: **https://xwc.services.xerox.com/<email-domain>**.
- The **email domain** should be the same email domain used by the User in their registered email account: **username@<email-domain>**.

Example: **https://xwc.services.xerox.com/customer.com**.

Step 5: Xerox Workplace Cloud Client Configuration

- To skip the email prompt when logging into the Xerox Workplace Cloud client, a JSON configuration file needs to be installed on the User workstation. This can be done manually or by using a customer deployment tool.
- The file name is **PdlParserSettings.json** and needs to be stored in **%PROGRAMDATA%\Xerox\XMPC**.
- The contents of the file should be:

```
{
  "CompanyLookup": {
    "Domain": "abc.com"
  }
}
```



Note: Replace abc.com with the domain of the customer.



Note: By default, PROGRAMDATA is typically a hidden directory

- Allows hidden items in the windows explorer view.
- You should select **Show File Name Extensions** in explorer.exe to ensure the file extension is json.
- Once the json file is in place, log out of the Xerox Workplace Cloud desktop client.
- Log in again to the desktop client, and you will no longer need to type the password.

SETTINGS: NETWORK APPLIANCES

Setting Up the Network Appliances for Auto Release

Xerox® Workplace Cloud supports different appliances. For instructions on how to set them up, see the following:

- [RF Ideas Ethernet 241](#)
- [Elatec TCPConv](#)
- [Elatec TCPConv2/3](#)

RF Ideas Ethernet 241

Configuring the RF Ideas Ethernet 241 Network Appliance

1. Plug in the network cable, the RF Ideas Ethernet 241 card reader, and the USB power. The green power LED should light up, and the card reader LED should be solid red.
2. Download the latest tools from <https://www.rfideas.com/files/downloads/software/DiscoveryTool.zip>.
3. Install the Ethernet241DiscoveryTool and run it.



Note: the Ethernet 241 and PC running the discovery tool must be on the same Ethernet subnet.

4. Click the **Find local 241 devices** button. It should discover the local 241 device on the local subnet.
5. Highlight the device, and click the **Visit web configuration page** link.
6. On the IP tab, verify Client is **On**, and Addressing Mode is **DHCP**.
7. On the Ports tab, select **Disabled** for the **SSL** option.
8. Select the following on the Server tab:
 - a. **Data Server IP**: enter all zeros.
 - b. **Data Server URL**: enter in the Agent IP Address or Hostname. For example, [http:// ONPREM9020.sdi.na.xde3.xerox.org](http://ONPREM9020.sdi.na.xde3.xerox.org).
 - c. **Data Server Port**: enter **2001**
 - d. **Data Server Str: \$1**. This sends the card data.
 - e. Click the **Update** button.
9. On the Status tab, verify the **USB 0**: card reader is detected.
10. On the System page, verify the Firmware Current Version is v1.10 or higher.
11. Click the **Reboot** button. The power and network LEDs will go off and then on, and the card reader resets.
12. Swipe the card over the card reader, verify the card reader LED blinks, and the Status page **USB 0**: updates to show the **Last Card (DEC)**: card information.

Configuring Xerox® Workplace Cloud to Use the RF Ideas Ethernet 241 Network Appliance

1. In **Account > Settings > Network Appliances**, under the Models tab, verify that the following settings are set:
 - a. RF Ideas 241 is **Enabled**
 - b. **Use SSL** is **Disabled** (unchecked)
 - c. **Listener Port Number** is set to **2001**.
 - d. If necessary, select the RF Ideas Ethernet 241 and modify the settings.
2. Select the **Appliances** tab. Add a new Network Appliance using **Actions > New**. Enter the IP Address from the 241DiscoveryTool, and select the **RF Ideas Ethernet 241** model.
3. Associate it with an enabled printer, by clicking **Select Printer**, selecting the desired printer from the list, and clicking **Save**.
4. Click **Save** again.

5. Select the **Printers** tab, find the printer associated in the previous step and select it to open the **Details** page for the printer.
6. Select the **Features** tab. Under **Auto Release All Jobs**, select the **Using Network Appliance** option and **Change**.
7. Find the network appliance that was added earlier, select it, and then click **Save**.
8. Click **Save** again to store the Auto Release All Jobs setting.
9. If you wish to enable SSL, follow the steps:
 - a. Select **Account > Settings > Network Appliances**.
 - b. On the Models tab, select the **RF Ideas Ethernet 241** model.
 - c. Select the **Use SSL** checkbox and click **Save**.
 - d. Using a web browser, connect to the configuration page of the Ethernet 241.
 - e. On the Ethernet 241 web configuration page, click the **Ports** tab, switch **SSL** from Disabled to **Enabled**, and make sure the **SSL Port** is set to **2001**.
 - f. On the Ethernet 241 web configuration page, click the **Server** tab, the **Data Server Url** entry should be changed from **http** to **https**.
 - g. Click **Update**.
 - h. Click the **System** tab and click **Reboot**.



Note: If you have trouble getting SSL to work after performing these steps, you may need to log into the PC running the Agent, and restart the **Xerox Workplace Cloud**.

Elatec TCPConv

Configuring the Elatec TCPConv Network Appliance

1. Plug in a network cable into either RJ45 jack of the TCPConv, and plug the card reader into the USB port.
2. Plug in the power to the TCPConv. The TCPConv green LED with the white dash symbol should light up. Most card readers have a LED that lights up when the reader is connected.
3. Download the latest tools:
 - a. Go to <https://www.elatec-rfid.com/en/download-center/>.
 - b. Look for the TCPConv row and select the link to download the tools.
 - c. Unzip the file to a local directory.
4. Run the configuration tool **TCCConfig.exe**, or whichever is the latest name of the tool. It should discover the TCPConv on the local subnet.



Note: The PC must be on the same subnet as the TCPConv.

5. Verify the firmware version is at least V1.08 or higher.
6. Select the **TCPConv** then click **Configuration**.



Note: The default login credentials are **admin / blank**.

7. On the **Network** tab, check Use **DHCP**. You can optionally set the Device Name if desired.

8. On the **USB** tab:
 - a. Check **TCP Client**.
 - b. Enter the **Remote IP Address** of the Agent.
 - c. The **Remote Port** of the server should be **7778**.
 - d. Select **Connect if data is available**.
 - e. Select **Connect on any character**.
 - f. Select **Disconnect on char: 13**.
 - g. Select **Send disconnect char**.
 - h. Set **Disconnect timeout** to be **5** seconds.
9. Click **OK**. The configuration tool Protocol text box UI should indicate **Writing new configuration: OK**.
10. Click **Restart**. The configuration tool UI should indicate **Device is restarting**.
11. On the TCPConv, the link/speed LEDs should go off and then on in approximately 10 seconds.
12. Scan a card at the reader, verify the card reader LED and the TCPConv green LEDs blink.

Configuring Xerox® Workplace Cloud to Use the Elatec TCPConv Network Appliance

Assumption: Print is already discovered and enabled for Xerox® Workplace Cloud.

1. Under **Account > Settings > Network Appliances**, select the **Elatec TCPConv** Model.
2. Select the checkbox to **Enabled** and set the **Listener Port Number** to **7778**. Click **Save**.
3. Select the **Appliances** tab, and then using the Actions drop-down select **New**.
4. Enter the following under **Details**:
 - a. Set the **Display Name** to ElatecTCPConv.
 - b. Enter the **IP Address** of the TCPConv (for example, 13.121.187.124).
 - c. Make sure the **Model** is set to **Elatec TCPConv**.
 - d. Click the **Select Printer** link.
5. Find the desired printer in the list, select it and **Save**.
6. The Associated Device is now updated. Select **Save**.
7. Select the **Printers** tab, find the printer associated in the previous step and select it to open the printer Details page.
8. Select the **Features** tab. Under **Auto Release All Jobs**, select the **Using Network Appliance** option and select **Save**.

Elatec TCPConv2/3



Note: If you use TCPConv3, use the **Elatec TCPConv2/3** setting.

Configuring the Elatec TCPConv2/3 Network Appliance



Note: It is assumed that most users use the TCPConv2/3 device in NAT mode for a single IP address shared by the network appliance and the printer. If required, you can use the device in non-NAT mode, which makes it behave similar to the TCPConv device, which functions in non-NAT mode. The following procedures are for users who use the device in NAT mode.

1. Power off the TCPConv2/3 device.
2. Power on the printer.
3. Connect the printer cable, host cable, and the magnetic stripe or proximity USB card reader.
4. Connect the TCPConv2/3 device to the power supply.


The green power LED lights, then at the display, a `Busy` message appears. After approximately 30 seconds, the messages `Power` and `Ready` appear. Most card readers have an LED that usually goes green when the connection is good.

5. Download the latest tools:
 - a. Go to <https://www.elatec-rfid.com/en/download-center/>.
 - b. Download the associated .zip file and extract the files.
6. Run the configuration tool.
7. Select **Search for TCPConv2/3 Devices on LAN**. Ensure that the utility discovers the TCPConv2/3 device on the local subnet.



Note: If the TCPConv2/3 device is not discovered, to discover it, there is a technique that uses the static IP address on the printer port of the TCPConv2/3. For more information, refer to the TCPConv2/3 manual.

8. Select **TCPConv2/3** device, then click **Open the Homepage of the TCPConv2/3**. You are prompted to supply login credentials. For example, username: `admin`, and password: `admin`.
9. Select the **Status** tab, and verify the following:
 - The firmware version is at least `STD1.2.0.10` or higher.
 - The USB card reader shows `HID Keyboard Reader Connected`.
10. Power on the printer, then verify that the link and speed LEDs on the TCPConv2/3 device are on.
11. Verify that the Print status displays as **OK** in the TCPConv2/3 Web Portal.
12. Select the **Setup** link at the top of the page.
13. On the Setup page, select the following:
 - a. In the Network Settings area, select the check box for **Use DHCP**.
 - b. At the top of the page, click **USB**.
14. In TCP/IP Configuration, select the radio button for **TCPConv 2/3 as Client**.
15. In TCP/IP Client Configurations, select the following:
 - a. Click **Send Plan Text Data**.
 - b. For Remote Hostname or IP, supply the Fully Qualified Domain Name (FQDN) or IP address of the computer that runs the Agent.
 - c. Set Remote Port to **7777**.

- d. Deselect the radio button for **Connect automatically and stay connected**.
 - e. Select the radio button for **Connect on any character**.
 - f. Deselect the radio button for **Connect on character**, then select the radio button for **Send connect character**.
 - g. Select the radio button for **Disconnect on character**, set it to **13**, then select the radio button for **Send disconnect character**.
 - h. Set Disconnect timeout to 5 seconds.
16. After you complete the setup, at the bottom of the page, click **Apply**.
 17. Select the **Home** option at the top of the page, then select **Reboot**.
Wait for the appliance to complete the restart process.
 18. Ensure that the printer is configured for DHCP, then power off or on the printer.
-  Note: If you use a Jetdirect card J7961G V.38.05, ensure that it is set to **BOOTP**.
19. In the configuration tool, verify the TCPConv2/3 Web Portal connection, for example, <http://13.121.187.114:81>.
 20. In the configuration tool, verify the printer Web Portal connection, for example, <http://13.121.187.114:80>.

Configuring Xerox® Workplace Cloud to Use the Elatec TCPConv2/3 Network Appliance

1. In the Xerox® Workplace Cloud Web portal, select the **Agents** tab.
2. From the list of agents, to edit the required agent, click the pencil icon.
3. Select the **Discovery Settings** tab, then do the following:
 - a. Select the discovery setting that you want to change, then click **Edit**.
 - b. To discover the printer at the same address as the TCPConv2/3 device, modify your agent. To modify your agent, enter an IP address, for example, 13.121.187.114.
 - c. Click **Save**.
4. Return to the Agents page. To discover agents, click the printer icon next to the Agent name.
5. After you complete the discovery, select the **Printers** tab, then select the printer from the list.
6. Select the **Features** tab, then select the check box for **Enable Printer**.
7. In the Auto Release All Jobs area, select the radio button for **Using Network Appliance**, then click **Save**.

8. To select an associated device, do one of the following:
 - Select **Associated Device > Select Printer**, then select the radio button next to the required printer.
 - Select the **Account** tab, then do the following:
 - Select **Settings > Network Appliances**, then select the **Elatec TCPConv2/3** model.
 - In the Details area, do the following:
 - Set the **Listener Port Number** to **7777**.
 - Select the check box for **Enabled**.
 - Select the check box for **NAT Enabled**.
 - Click **Save**.
 - Select the **Appliances** tab, then from the Actions menu, click **New**.
 - In the Details area, enter the following information:
 - Display Name: Type a display name.
 - IP Address: Type the IP address of the TCPConv2/3, for example, 13.121.187.114.
 - Model: Ensure that the model is set to **Elatec TCPConv2/3**.
 - Associated Device: Select the **Select Printer** link.
 - Select the radio button next to the required printer.
 - Click **Save**. The Associated Device field is updated.
 - Select **Save**.

SETTINGS: PERFORMANCE

Content Delivery Network

When enabled, this setting configures the system to use the Azure Front Door Content Delivery Network (CDN) to improve print performance at job release time. Print ready data is sent to an Azure Front Door server where it can then be pulled to a printer.

Workplace Cloud uses the Azure Front Door network to optimize delivery of dynamic content such as print ready files that are unique to the requestor and not cacheable. The advantage of having a CDN deliver this dynamic content is performance and scaling. The CDN will establish and maintain secure connections closer to the requestor, and with the CDN being on the same network as the Azure storage account, routing is accelerated back to the storage account to retrieve dynamic content. The path between the Workplace Cloud Azure blob storage and the CDN edge server is essentially a super highway to quickly get the data from one of the Azure sites used by Workplace Cloud (US or UK) to the CDN endpoint. The data is then pulled down to the printer from the CDN edge server, which is physically close to the printer, minimizing the network path that the data needs to travel. The print job data is never stored or cached in the CDN endpoint. The data just streams through the CDN endpoint to the local printer. Caching of data at the CDN endpoint is explicitly disabled.

The Azure Front Door provides substantial performance improvements for document delivery at print release. Large files, greater than 10 MB, see the most improvement when travelling through the CDN network. However even smaller documents (less than 10 MB) see a decrease in the time it takes to deliver the document from the cloud down to a printer. Figures 1 and 2 show the average improvement of 20-100%, for both small and large

documents passing through the CDN network. Therefore, it is most optimal for all accounts to maintain the enablement of the Content Delivery Network performance setting.

Enabling CDN

Administrators can configure the Xerox® Workplace Cloud client to use features that improve print performance. The **Enable CDN** option configures the system to use the Azure Front Door Content Delivery Network to improve print performance at print job release time. Enabling this feature creates an improvement of 50–70% in job release processing time for jobs that are over 10 MBytes.

To configure print performance settings, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select **Account > Settings > Performance**.
3. To enable the CDN, select the **Enable CDN** check box.



Note: By default, the **Enable CDN** setting is disabled for all new accounts.

Printer Internet Connection

When you enable the Printer Internet Connection performance setting, to improve print performance when you release jobs, it uses all Xerox printer internet connection.

This setting manipulates how the Workplace Cloud Agent releases print jobs to PrintFromUrl also known as Pull Printing capable Xerox Printers. When you enable, the Workplace Cloud Agent is not download the converted print ready file from cloud and send it to the device and also known as Push Printing; instead, it uses the Xerox device capability PrintFromUrl by sending a Job Ticket with a document download URL. The download URL can be an Azure Front Door Content Delivery Network URL or Cloud Web Service URL. This configuration option improves the Workplace Cloud Agent performance by decreasing the number of print ready files required to be processed through the agent.

Unless printers cannot connect to the internet due to networking constraints at a customer location, to improve print performance and agent load capacity, ensure that the customers maintain the enablement of the Printer Internet Connection setting.

Enabling Printer Internet Connection

The Printer Internet Connection option allows all Xerox® printers to connect to the Internet to improve print performance when you release jobs.



Note:

- This setting is enabled by default for all accounts that upgrade to Xerox® Workplace Cloud version 5.2
- If printers in your company are not able to connect to the Internet, to improve system performance, disable this setting.

To enable Printer Internet Connection, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select **Account > Settings > Performance**.
3. To enable Printer Internet Connection, select the check box for **Printer can connect to the internet**.

SETTINGS: PRINT DEFAULTS

Document Release Order

The Document Release Order feature controls the order in which jobs are printed. You can set the document release order for an account. The feature has two options:

- **Maximize Performance:** This option processes print jobs with the intent to print them as quickly as possible. The jobs do not print in the order received or listed. For existing and new accounts, the default option is **Maximize Performance**.
- **Enforce job order:** This option processes the print jobs in the order in which they are received. The use of this option can result in degraded print performance.

The default document release order for new users is the setting specified for the account that the users are assigned to initially.

Setting the Document Release Order for an Account

To set the default document release order for new users of an account, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Settings > Print Defaults**.
3. In the Document Release Order area, to set as a default option for a new user, select one of the following:
 - **Maximize Performance**
 - **Enforce job order**
 For more information on these options, refer to [Document Release Order](#).
4. To confirm the changes, click **Save**, or to cancel the changes, click **Cancel**.

SETTINGS: XSM EXPORT

Xerox Service Managers (XSM) Connection for Xerox Workplace Solutions Analytics (XWSA)

The XSM Export feature enables non-XSM-connected Workplace Cloud accounts to support for the Xerox Workplace Solutions Analytics solution.

The XSM Export feature exists in XSM-connected cloud accounts. You can modify and reuse the user interface. For more information, refer to [Requirements for XSM Export](#).

Requirements for XSM Export

The XSM Export feature requires the following actions:

- The administrator specifies an XSM account ID.
- To match the XSM configuration for identifying printers in data import files, the administrator selects MD5 or SHA1.
- Add the Identification Algorithm settings.
- Enable the XSM Export feature.

- Enable the XSM Login functionality that was created originally for Cloud Fleet Management.



Note: The XSM Export feature allows users to switch between XSM-connected accounts and non-XSM-connected accounts.

Finding an XSM Account ID

To find the XSM (Xerox Service Managers) account ID, perform the following steps:

1. Log in using your credentials for the XSM.
2. From the left panel, select **Administration > Account Settings**.
3. To view your account ID, click **Details**.

Configuring the XSM Connection for XWSA



Note: When you have access to the Xerox Service Managers (XSM) Connection and XSM functions, the following setup is available in the Cloud portal.

To enable the XSM Export function for non-XSM-connected cloud accounts and to enable support for the Xerox Workplace Solutions Analytics function, perform the following steps:


1. Log in as an administrator.
2. Click **Account > Settings > XSM Export**.
The Xerox Services Manager Export Settings window appears.
3. By default, Enable Jobs Export is disabled. To enable a job export, select the check box for **Enable Jobs Export**.
The Details and Schedule tabs appear. In the Details tab, in the System Identity section, the system name appears automatically as Xerox Workplace Cloud - Company Name.
4. In the Details tab, perform the following steps:
 - a. In the Account ID field, enter your account information.
The default Identification Algorithm is MD5.
 - b. In the Scheduled section, the default schedule is Weekly. To change the schedule, select an option:
 - **Disabled**
 - **Everyday**
 - **Weekly**
 - c. To save your schedule selection, click **Save**.
5. Click **Run Now**.
6. The job history shows the job that was last run, when the job started and ended, who ran the job, and the next scheduled run. In the History section, for the status of the job export, click **Refresh**.

The Last Run area shows the job status as one of the following:


- Processing
- Success
- Failed

SETTINGS: SINGLE SIGN-ON

Single Sign-On


 Note: For enabling Single Sign-On feature for Cloud Direct Devices, refer to [Enable Single Sign-On for Cloud Direct Devices](#).

The Single Sign-On feature is for applications that are installed and run on Xerox® devices, for example, Dropbox or Google Drive. There are specific apps that are designed to support the Single Sign-On feature. When Single Sign-On is enabled, third-party applications can store and retrieve user access data using the Xerox® Workplace Cloud solution.

 Note: For more information about the Single Sign-On feature, access the Single Sign-On page, then click the Information (i) button.

To activate the Single Sign-On (SSO) license, create a Workplace Cloud account in trial mode, then activate the Single Sign-On license. You can apply the Printer Essential Bundle (PEB) license to the Single Sign-On license. Note that the Single Sign-On license cannot be applied to the existing PEB license. After the Single Sign-On license is activated, the following tabs are available:

- Printers
- Sites
- Agents
- Users
- Account

 Note: When only an SSO license is activated, many Workplace Cloud features are hidden. The Cloud with only SSO activated does not support cards, phones, printing, the EIP App, or the Accounting feature.

Activating a Single Sign-On License


Xerox® Workplace Cloud Single Sign-On is supported with a new Single Sign-On Pack. You can authenticate using an email and password only. Single Sign-On (SSO) is supported with the Printer Essentials Bundle (PEB) license.

 Note: All SSO packs expire after 1 year.

1. Log in as an administrator to Xerox® Workplace Cloud.
2. Click **Account > Licensing**.
The Licensing page appears.
3. In the New License field, type the Activation Key and the Serial Number, then click **Activate**.

 Note: You can apply the SSO license for Cloud to a trial account only.

4. After the SSO license is applied, the New License section changes to allow multiple and simultaneous PEB or SSO license activation. In the License Information field, enter the required information. To add PEB or SSO licenses to the Validated Licenses field, click the license names.

 Note: You can select multiple licenses for simultaneous activation.

5. Click **Activate**.



Note: Error messages appear when SSO is applied to a system with a Job Pack or Device Pack license.

Enabling Single Sign-On

1. Log in as an administrator to Xerox® Workplace Cloud.
2. Select **Account > Settings > Single Sign-On**.
3. Select the check box for **Enable Single Sign-On**.
4. Click **Save**.

All Registered Apps appear with the status Activated.

Enable Single Sign-On for Cloud Direct Devices

1. Enable Single Sign-On for your Workplace Cloud Company:
 - a. Select **Account > Settings > Single Sign-On**.
 - b. Select the check box for **Enable Single Sign-On**.
 - c. Click **Save**.All Registered Apps appear with the status Activated.
2. Create a root certificate for your Workplace Cloud Company, refer to [Creating and Activating a Company Root Certificate](#).
3. Ensure printer is enabled for Cloud Direct, refer to [Manual Enablement of Cloud Direct feature of the Printers on the Workplace Cloud Portal](#).
4. Enable Authentication if it is not enabled, refer to [Set Authentication Mode](#).
5. Do repair if already enabled for authentication, refer to [Repair](#).



Note: After enabling authentication on the printer, the solution will install a unique client certificate on the printer to allow authentication using Single Sign-On.

Single Sign-On Settings for User Profile

You can manage your Single Sign-On authentication data for the applications that are installed on your printers.

1. Log in to Xerox® Workplace Cloud Web Portal as an administrator.
2. To access the User Profile feature, click the user name email ID.
The User Options page appears.
3. On the User Options webpage, click **Single Sign-On**.
4. To change the Single Sign-On Settings options, from the list, select your application, then select **Action > Reset**.
The stored authentication data are deleted for the selected apps. The Single Sign-On Agreement status appears as Not Accepted.

SETTINGS: MICROSOFT UNIVERSAL PRINT

The Microsoft Universal Print feature allows Xerox® Workplace Cloud to create a single pull print queue in the Microsoft Azure Universal Print service for the customer tenant. After you register a pull print queue, you can authorize and deploy it to all your users of the organization, like with any other Microsoft Universal Print Printer.



Note: To add an Azure Universal Printer, Windows 10 version 1903 or later is required.

Microsoft Universal Print allows the users in your Azure AD domain to add the universal printer that is connected to Xerox® Workplace Cloud and submit jobs for later release. To submit jobs, Microsoft Universal Print uses the Xerox® Workplace Cloud release clients, such as the @PrintByXerox App, Workplace Mobile applications, and network appliances.

Microsoft Universal Print Guidelines

- To set the printer defaults, in the Azure portal for the Xerox® Workplace Cloud registered printer, go to **Printer properties > Printer Defaults**.
- The Microsoft Account used to register the Universal Printer should have the following roles and rights:
 - Cloud Company Account Administrator
 - Must have an appropriate license that allows Universal Printing in Azure:
 - Microsoft 365 Enterprise F3, E3, E5, A3, A5
 - Windows 10 Enterprise E3, E5, A3, A5
 - Microsoft 365 Business Premium
 - Universal Print (standalone)
 - Should have one of the following roles in Azure:
 - Printer Administrator
 - Global Administrator
- The Microsoft Universal Print service converts jobs to PDF format, then uploads the jobs to Xerox® Workplace Cloud.
- To ensure that jobs are assigned to users, before you deploy Microsoft Universal Print, it is recommended that you map your email domain. To map your email domain, send a request to your Xerox representative.
- Jobs are sent to the local Microsoft Universal Print driver on the client computer and are processed as follows:
 - Xerox® Workplace Cloud Web portal pulls the job from the Azure AD portal.
 - The email address attached to the job is verified against the current user list in the Xerox® Workplace Cloud Web portal.
 - If the user exists, the job is assigned to them.
 - If the user does not exist:

- If the authentication types are OKTA and Azure AD, Xerox® Workplace Cloud compares the email domain to the users mapped to the account. If the domain is found, an account is created for the user and the job is assigned to the user.
 - If a job is not assigned to the user, the job is cancelled. The cancelled job is visible in the job section of the universal printer that you created in the Azure AD Portal.
- After Xerox® Workplace Cloud pulls the job from Universal Print, the Xerox® Workplace Cloud account follows the job retention period policy. For more information, refer to [Data Retention Policy](#).

Setting the Azure AD Web Application Values

To set the values in the Azure AD Web Application tab, do the following:

1. In the Azure Portal, go to your Azure Active Directory Tenant.
2. From the Overview page, copy the Directory (tenant ID) value.
3. Go to the Xerox® Workplace Cloud Web portal, then do the following:
 - a. Select **Account > Settings > Microsoft Universal Print**.
 - b. In the Provide the following values from the Azure Tenant and the App just registered area, paste the copied value in the Tenant ID (from Azure AD tenant overview) field.
4. Register a new application, do the following:
 - a. Go to the Azure portal, then from the navigation pane, select **App registrations > New registration**.
The Register an application window appears.
 - b. Enter a name for the application.
 - c. Select **Accounts in this organization directory only (<domain name> Single Tenant only)**.
 - d. Click **Register**.
5. From the new application that you created in the Azure Portal, click **Overview**, then copy the Application (client) ID value.
6. Go to the Xerox® Workplace Cloud Web portal.
7. In the Provide the following values from the Azure Tenant and the App just registered area, paste the copied value in the Application ID (from the app just registered) field.
8. Grant the new application that you created, the following permissions:
 - a. Go to the Azure portal, then from the navigation pane, click **API Permissions**.
 - b. Click **Add a Permission > Universal Print**.
A dialog box appears.
 - c. Select **Delegated Permissions > Printers**.
 - d. Enable the following Delegated permissions, select the check box for **Printers.Create Create (register) new printers**.
 - e. In the upper right corner of the Request API Permissions box, select **Application Permission**.

- f. Enable the following Application permissions check boxes:
 - **Printers.Read** Read printers
 - **PrinterProperties.ReadWrite** Read and write the properties and attributes of printers
 - **Print.Job.Read** Read the metadata and payload of users' print jobs
 - **Print.Job.Read WriteBasic** Read and write the metadata of users' print jobs
 - g. To save the permissions, select **Add Permissions**.
 - h. In the Configured permissions area, click **Grant admin consent for**.
A confirmation message appears.
 - i. To confirm the changes, click **Yes**.
9. To create and copy the client secret value, do the following:
 - a. Go to the Azure portal, then from the navigation pane of the registered app, click **Certificates & Secrets**.
The Client Secrets page appears. The status of the client secret changes.
 - b. Click **+ New Client Secret**.
The Add a Client Secret page appears. Do the following:
 - In the Description field, enter a description.
 - In the Expires area, select one of the radio buttons.
 - Click **Add**.
 In the Client Secrets grid, the client secret value appears in the Value column.
 - c. Copy the Client Secret value.
 10. Go to the Xerox® Workplace Cloud Web portal.
 11. In the Provide the following values from the Azure Tenant and the App just registered area, paste the copied value in the Client Secret (from step 3 above) field.
 12. To set up authentication, do the following:
 - a. From the Xerox® Workplace Cloud Web portal, in the Register a new application in the Azure AD Tenant area, from the Redirect URI field, copy the value.
 - b. Go to the Azure portal, then from the navigation pane of the registered application, click **Authentication**.
The Platform configurations page appears.
 - c. Click **Add a platform**.
The Configure Platforms dialog appears.
 - d. Click **Web**.
The Redirect URIs field appears in the window.
 - e. Go to the Azure portal, then paste the copied value in Redirect URIs field.
 - f. Click **Configure**.
 13. To complete the Universal Print Setup section, do the following:

- a. Go to the Xerox® Workplace Cloud Web portal.
 - b. Select **Account > Settings > Microsoft Universal Print**, on the Universal Print Setup section, do the following:
 - In the Name field, enter the name of your Universal Print printer that appears in the Azure portal.
 - To define the storage Location of your pull print documents from Microsoft Universal Print, select the Document Location from the drop down:
 - West Europe (Default)
 - UK South
 - South Central US
14. Click **Register**.
 15. Log in to the Azure AD portal.

The Azure AD portal redirects you to the Xerox® Workplace Cloud Web portal. A dialog box appears with a confirmation message that states that the printer is registered.
 16. After you complete the registration, complete the setup of the new universal printer in the Azure portal.

To deploy a Universal Printer to your users, follow the Microsoft Azure AD instructions. For more information on deploying Universal Printers, refer to <https://docs.microsoft.com/en-us/universal-print/fundamentals/universal-print-getting-started>.

Troubleshooting

When you do not enter correct settings, after you register Azure AD authentication, the printer does not enter the Ready state.

To resolve the issue, do the following:

1. Go to the Xerox® Workplace Cloud Web portal.
2. Click **Account > Settings > Microsoft Universal Print**.
3. From the Microsoft Universal Print page, click **Unregister**.
4. For the Universal Print App that you created, verify the Azure AD settings.
5. Go to the Azure portal, then from the navigation pane, click **API Permissions**.
6. Ensure that the API Permissions are set correctly.
7. Ensure that the URLs are set correctly.
8. Copy the App settings to the Microsoft Universal Print page on the Xerox® Workplace Cloud Web portal again.
9. If you do not have the Client Secret, create a new one in the Azure AD portal, then copy it to the Xerox® Workplace Cloud Web portal again.
10. Ensure that the settings are correct, then click **Register**.

Unregistering a Microsoft Universal Print Printer

Guidelines to Unregister a Microsoft Universal Print Printer:

- If you need to unregister your Microsoft Universal Printer, you need to unregister the Microsoft Universal Print printer in the Xerox® Workplace Cloud Web portal.
- When you have a registered universal printer, all the values in the fields in the Microsoft Universal Print page are in read-only mode. To unregister the Microsoft Universal Print printer, you are required to remove the values from these fields.
- After you unregister the Universal printer in Xerox® Workplace Cloud, you have to unregister the universal printer manually in the Azure Portal.
- Users who have installed the Microsoft Universal Print printer have to manually remove it from their computer.
- If you do not follow these steps to unregister a universal printer, you cannot register a printer with the same name again.

To unregister a Microsoft Universal Print printer, do the following:

1. In the Xerox® Workplace Cloud Web portal, select **Account > Settings > Microsoft Universal Print**.
2. Click **Unregister**.

The fields in the Azure AD Web Application and Universal Print Setup sections become editable.

3. Remove the values from these fields.
4. Unregister the printer in the Azure AD Portal.
5. Remove the universal printer from your computer.

Account: Policies

This chapter contains the configuration information for the following topics:

- Policies: Print Controls
- Policies: Data Retention Policy
- Policies: Encryption
- Policies: Public Printing
- Policies: Agent Upgrades
- Policies: Access Controls
- Policies: Printer Authentication
- Policies: Security
- Policies: Rules
- Policies: Printer Selection
- Policies: Offline Mode
- Policies: Content Security
- Policies: Client Application

POLICIES: PRINT CONTROLS

Controlling Which Printer Features are Available to Users

1. From the Workplace Cloud Web Portal, select **Account > Policies > Print Controls**.
2. Select the radio buttons for features you want to make available:

Print Control Policy	Feature
Details	<ul style="list-style-type: none"> • Both Single and Double-Sided Printing are Allowed • Only Double-Sided Printing is Allowed
Color Options	<ul style="list-style-type: none"> • Both Color and Black-and-White Printing are Allowed • Only Black-and-White is Allowed
Paper Substitution	<ul style="list-style-type: none"> • Paper Substitution Enabled • Paper Substitution Disabled

3. Select **Save**.

Users only see the printer features you make available.

Enabling or Disabling the Paper Substitution

When Paper Substitution is enabled and paper tray information is available for the selected printer, the system scales the entire job to the closest available paper size needed by the first page of the job. With Paper Substitution disabled, jobs may be held at the printer if the correct paper size is unavailable. Most paper sizes are supported; for example Letter will be resized to A4, A3 will be resized to Ledger, etc.

1. From the Web Portal, select **Account > Policies > Print Controls**.
2. Make a Paper Substitution selection and select **Save**:
 - Paper Substitution Enabled
 - Paper Substitution Disabled



Note:

- Whether or not paper substitution is enabled, users may select a specific media size for their job to be printed on.
- When all paper trays are empty, the paper size settings for paper trays may not be detected and auto-scaling may not be applied.
- Paper substitution is not available when printing through print queues because paper tray information cannot be determined.

Media Size Conversion

The DCE (Document Conversion Engine) server is a server which is used to convert documents such as TIFF, jpeg, .txt, .docx, PDF, and .ppt file formats to PS or PCL.

The DCE supports scaling of the incoming document size to accommodate these well-known paper size substitutions as follows:

- A4: Letter (8.5 x 11 in.)
- A3: Tabloid (11 x 17 in.)

For example, A Letter (8.5 x 11 in.) document is printed on a Xerox® VersaLink printer that is loaded with A4 (210 x 297 mm), and the printer does not have the Paper Substitution enabled. The DCE converts the incoming document to PDF format and scales it to the A4 (210 x 297 mm) paper size loaded in the printer.

The normal scaling of the DCE by +/- 1.6 inches applies to PDF output files. For example, based on the paper loaded in the printer, a .ppt file of 7.5x10 in. scales to an output PDF file of 8.5x11 in.

POLICIES: DATA RETENTION POLICY

Data Retention Policy

Retention Policy determines how long your print job remains within the Xerox Workplace Cloud system.



Note: Documents submitted and not printed will be deleted after 3 days. Documents printed and retained will be deleted based on the retention settings defined.

Setting Data Retention Policy

Guidelines:

- An unprinted job is held for maximum of 3 days.
- If a job is printed, then the retention setting will be used to retain a job in Workplace Cloud (Immediate, 1 day or 3 days).
- The maximum amount of time a job resides in Workplace Cloud is 3 days, if a job is submitted on day 1 and released on day 3 with a retention value of 3 days, then the job will be deleted 3 days from the initial submission.

You can set a job-retention period for your print jobs, which removes the job after printing, to display a warning message for user interaction, or to retain the job for 1–3 days after printing, select any of the following check box and click **Save**.

- **Immediate:** Documents will be deleted immediately after printing.
- **1 Day:** Documents will be deleted after 1 day.
- **3 Days:** Documents will be deleted after 3 days.

Lockdown Client Settings

It is the responsibility of the company IT department to ensure that the lockdown settings are in place and installed on Workplace Cloud Client computers. To enable this feature, the company IT department is required to deploy a lockdown settings file with the Workplace Cloud Client application, using Microsoft System Center Configuration Manager. To maintain security, it is recommended that the IT department ensures the following:

- That users cannot modify or remove the lockdown settings file.
- To avoid inadvertent overwriting of the file, that users are prevented from installing the Xerox Workplace Cloud Client on their computers.

It is recommended that the requirements for enabling the feature are discussed with the individuals involved in the implementation and configuration of Workplace Cloud as required.

When the lockdown setting is deployed to the Workplace Cloud Client, the following applies:

- To allow you to sign in, the Desktop Client verifies whether a lockdown settings file exists.
- If the current company is the same as the Company Indicator in the lockdown setting, you can log in to the desktop client.
- If you are an unknown user, to log in, you are required to provide the Company Indicator that matches the lockdown setting.
- When the Desktop Client renews your authorization token, the Desktop Client verifies your Company Indicator against the lockdown setting. If the settings do not match, the system logs you out.

POLICIES: ENCRYPTION

The Encryption feature has three sections, which are as follows:

- **Summary**
- **Account**
- **Desktop**

Summary

The Workplace Cloud solution supports several options for document encryption. The Summary tab indicates which encryption method is used for the different print workflows and for documents at rest in the cloud. All documents are symmetrically encrypted using a unique key. The key is encrypted using one of the following mechanisms:



Note: For desktop printing, only jobs sent to the cloud are encrypted.

- **Xerox Encryption:** A common public certificate and private key are used to encrypt and decrypt documents at rest. Documents are decrypted for conversion and when released and downloaded to a printer or agent. Decryption happens in the cloud.
- **Account Encryption:** A Bring Your Own Key (BYOK) option which allows the customer to create and upload their own certificate and private key pair. This option is used for documents at rest. Documents are decrypted for conversion and when released and downloaded to a printer or agent. Decryption happens in the cloud.
- **Desktop Enhanced Encryption:** For more information, refer to [Desktop](#).

Managing Certificates in Xerox® Workplace Cloud

Both the Account Encryption and Desktop Enhanced Encryption options require the customer to upload their own certificate. When you install a certificate, the initial status is `new`. Multiple certificates can exist in the `new` state at one time. Certificates that are in a `new` state are not distributed to Xerox® Workplace Cloud Clients.

After the administrator activates the certificate that is in the `new` state, the status moves from `new` to `active`. Any certificate that has an `active` status becomes `inactive`. After a certificate becomes `inactive`, the public key and the thumbprint are no longer distributed to Xerox® Workplace Cloud Clients.

Enabling Encryption in Xerox® Workplace Cloud

To use your certificate keys, perform the following steps:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Accounts > Policies > Encryption**.
3. Do one of the following:
 - For account encryption, select the **Account** tab.
 - For desktop encryption, select the **Desktop** tab.

4. In the Certificate Manager area, click the **Actions** menu. Select one of the following options:
If you are a new user, before you select **Activate** or **Deactivate**, ensure that you have selected the certificate. If no certificate is selected, the error message `This action can only be done on one item at a time. Please select exactly one item and try again.` appears.
 - **Activate:** This option activates the currently selected certificate. If there was a previous active certificate, that certificate is deactivated. When you select this option, a warning appears. To continue, click **OK**. If you try to activate multiple certificates, an error appears.
 - **Deactivate:** This option deactivates the currently selected and active certificate. When you select this option, a warning appears. To continue, click **OK**
 - **Upload:** Choose this option to upload a certificate file to the Certificate management grid. To upload the certificate, click **Upload**, a Xerox Workplace Cloud window appears. In the Upload Certificate area, click **Choose file**, then browse to the location of the file on your computer. Click **Open**. At the confirmation message, to upload the file, click **OK**, or to cancel the upload, click **Cancel**. After you upload the certificate, the status is new, until the administrator activates the certificate manually.

Account

The Account tab allows you to configure Account Enhanced Encryption. This feature provides customers with an extra layer of document security for all files submitted to Xerox® Workplace Cloud. The Account Enhanced Encryption feature allows customers to upload a PKCS#12 file (pfx) file that contains a public certificate and private key. The public certificate is used to encrypt all documents at rest in Xerox® Workplace Cloud. Decryption of jobs using the private key is performed for document conversion and download. The Account tab allows you to upload, activate, or deactivate your certificate.

If there is an active account certificate available for the Xerox® Workplace Cloud company account, the certificate is used for the following:

- Mobile jobs: Encryption of the symmetric key used for original and converted documents.
- Desktop jobs: The desktop client downloads the certificate and uses the certificate for encrypting print jobs that are uploaded to the cloud.
- Agent received jobs: Includes iOS Native jobs and Agent Incoming jobs that are sent to LPR queues and Windows network shared queues.

The Xerox® Workplace Cloud solution includes a mapping from the encrypted document to the corresponding certificate that was used for each job. Xerox® Workplace Cloud supports the decryption of any job that is encrypted using an uploaded account certificate, regardless of whether the account certificate is active or inactive.

Desktop

The Desktop tab allows you to configure End-to-End Enhanced Encryption. This feature provides customers an extra layer of document security for custom-driver-submitted jobs to Xerox® Workplace Cloud. The feature allows customers to upload a public key certificate that the desktop client application downloads and uses to encrypt the document content before it is uploaded to Xerox Workplace Cloud.

After you activate a certificate, Xerox® Workplace Cloud distributes it to the Xerox® Workplace Cloud Clients.

Desktop Print Job Encryption

Customers who require additional security can install their own pair of public and private certificates that contain keys used for encryption and decryption. The public certificate is uploaded to Xerox® Workplace Cloud using the

Web Portal and is downloaded by the client. The public certificate is used to encrypt any job sent to Xerox® Workplace Cloud. The customer installs a private certificate in the Windows Certificate Store of each Xerox® Workplace Cloud Agent. When a job is released to a printer, the job is routed to an Agent. The Agent performs the decryption, then transfers the job to the printer. When files are not on the internal network of the customer, they always remain in an encrypted format.

If you have a Xerox® AltaLink® C80xx or B80xx product that is running release 103.xxx.020.23120 (R20-08) or later, the printer supports the ability to decrypt these print jobs without routing the job to the Agent. Printer decryption can improve the print performance and it can help reduce the number of agents that are required for a given customer.

If you use the customer-installed certificates or keys, all print jobs are routed through the Agent or to an appropriately configured Xerox® AltaLink® device. This process can increase the network traffic and processing load of the Agent significantly. If a customer wants to continue to use this feature, it is possible to increase the number of agents being used. If the customer has set Local Print Optimization to Local without Cloud Backup or Local with Cloud Backup, the impact on the Agent is minimal. If Local Print Optimization is disabled, all jobs are routed through the Agent. To plan the number of Agents for the customer, use the guideline that an Agent can process approximately 45 jobs per minute.

Desktop Client Encryption



Note: The Encryption feature is supported for custom driver jobs.

The Encryption feature uses a combination of symmetric encryption of a print job and asymmetric encryption of the key before they are uploaded to Xerox® Workplace Cloud. When client and agent encryption is enabled, all custom driver jobs are encrypted and Xerox® Workplace Cloud print rules are not applied.

Agent Decryption

The certificate that has the private key is installed on the Windows Certificate Store of the system on which the Xerox® Workplace Cloud Agent runs. The Agent administrator can view the installed certificates at the Agent user interface. To get the active thumbprints for the account, the agent contacts Xerox® Workplace Cloud.

Printer Decryption

If the printer has to decrypt the job, ensure that the private key certificate is installed on Xerox® AltaLink® printers. Ensure that the root CA certificate that is used to sign the private key certificate is installed on the printer. The printer validates the chain of trust between the private certificate and the root CA certificate. If the chain of trust cannot be validated, the printer deletes the encrypted print job.

To enable the printer decryption option, refer to [Set File Decryption Mode](#).

Setting up Desktop Enhanced Encryption

This is a summary of the sequential steps for setting up desktop enhanced encryption:

1. Create public and private certificates.
2. At the Web portal, in the Desktop area, upload your public certificate.
3. To decrypt jobs from the agent and print the jobs, do the following:
 - a. Update the certificate.
 - b. Install the private certificate in the Windows Certificate Store of each Xerox® Workplace Cloud Agent.
 - c. Verify that the certificate is correct in the agent.

4. To decrypt print jobs on the printer, do the following:
 - a. Upload the private key certificate to the Xerox® AltaLink® Printer.
 - b. Enable the printer decryption option. For more information, refer to [Set File Decryption Mode](#).

POLICIES: PUBLIC PRINTING

Managing User Access to the Printers of Other Companies

1. From the Workplace Cloud Web Portal, select **Account > Policies > Public Printing**.
2. Select a Public Printing policy and select **Save**:
 - Allow users to access only your company printers
 - Allow users to access printers enabled by other companies

Allowing Users to Print to Public Print Providers

Administrators can allow users to see and print to Xerox® Workplace Cloud printers that have been made available by other companies. It also allows users to view and print to other Public Print providers in the mobile app, as they become available.

Printing to public print providers outside of Xerox® Workplace Cloud is only available from the Xerox® Workplace Mobile App. It is not available from the Web Portal.



Note: When printing to public printers outside of Xerox® Workplace Cloud, users will receive a code from the public print provider that they will use to retrieve their printed output.

1. From the Workplace Cloud Web Portal, select **Account > Policies > Public Printing**.
2. Select a Public Printing policy and select **Save**:
 - Allow users to access only your company printers
 - Allow users to access printers enabled by other companies

POLICIES: AGENT UPGRADES

Setting Up the Agent Upgrade Policy

By default, agents are set to upgrade automatically when a new version of the agent software is available, but you can upgrade them manually if you prefer. If an agent is not capable of auto-upgrade, or if you have opted not to have your agents upgraded automatically, you will receive an email with a download link when new software is available.

Within your account, only one agent will be upgraded at a time. This minimizes disruption of services in your account.



Note: If an agent fails to upgrade in a timely manner after entering an auto-upgrade process, you will receive an email indicating that an agent is not responding and should be reviewed.

1. From the Workplace Cloud Web Portal, select **Account > Policies > Agent Upgrades**.

2. Select **Automatically upgrade my agent(s)** or **Do not automatically upgrade my agent(s)**.
3. Select **Save**.



Note: Only agents added or upgraded in Xerox® Workplace Cloud version 1.5 or later (agent version 2.2 and newer) are eligible for automatic upgrade. Each agent installed prior to version 1.5 must be manually upgraded once. From that point forward, agents will upgrade automatically unless you have set the Agent Upgrade Policy to not allow auto-upgrade of your agents.



Note: The Xerox® Workplace Cloud Agent icon is normally available in the system tray of the agent PC or server. If the icon is not present, manually start the agent user interface from the PC's Start menu.

POLICIES: ACCESS CONTROLS

Controlling Access to the Private Printers of Your Company

From the Workplace Cloud Web portal, select **Account > Policies > Access Controls**. Users who sign in with your company code have access to private printers automatically.

1. To enable other users to access your company private printers, add new users to the Allowed Users list under **Access Controls > Allowed Users**.
2. Using the **Allowed Users** list, you can control printer access.
 - **Standard Security (Easy Administration):** Users can self register with company code, or you can add the user or domain to the Allowed Users list.
 - If required, select the check box for **Allow users not associated with this Company Account to access the Printer Client Application. This toggle can be used to provide a Guest Access print workflow..**
 - **Advanced Security (Manual Administration):** Ensure that you add every user or domain to the Allowed Users list.
 - If required, select the check box for **Allow users not associated with this Company Account to access the Printer Client Application. This toggle can be used to provide a Guest Access print workflow..**
3. To restrict access to private printers, add the email addresses or email domains to the Blocked Users list. Select **Access Controls > Blocked Users**.



Note:

- The Search field allows you to search for specific email addresses in the Allowed Users list or Blocked Users list.
- Settings in the Private Printers section do not affect anonymous direct email printing. To prevent an unregistered user from printing, add the individual email address or the email domain to the Blocked Users list.

Controlling Access to the Public Printers of Your Company

1. From the Workplace Cloud Web Portal, select **Account > Policies > Access Controls**.
2. To restrict access to all printers, add email addresses or email domains to the Blocked Users list:

- a. Select the **Blocked Users** tab.
- b. Under **Public and Private Printers**, select **Add** from the Actions menu.
- c. Enter the email address in the **Value** field and select the **Save** button.

Ensuring a User Can No Longer Access Your Company Printers

When a user is removed from your company account, the user can still access the account when he or she logs in again and enters the company code. To ensure that a user can no longer access the account, do the following:

1. From the Workplace Cloud Web Portal, select **Account > Policies > Access Controls > Blocked Users**.
2. Select **Add** from the **Actions** menu.
3. Enter the email address of the user and select **Save** to add it to the Blocked Users list.

Alternatively, you can go to **Account > Policies > Access Controls**, select **Apply To All Users** and set up the Allowed Users list. Only email addresses or domains listed there will have access to your company's printers.

POLICIES: PRINTER AUTHENTICATION

Auto Registration

The Auto Registration mechanism specifies whether the user can register their card themselves through onboarding, 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. Credentials can be email and password, LDAP user name and password, Azure AD user name and password, or OKTA user name and password. If the credentials are valid, the card number is added to the database and the user is recognized the next time they swipe their card.

Enabling Auto Registration

By default, Auto Registration is disabled.



Note: **Badge Registration email validity period** and **Custom email Onboarding Message** setting is only available when using OKTA, HelloID and Azure AD as a authentication method.

To enable the Auto Registration feature, do the following:

1. Log in as an administrator to Xerox® Workplace Cloud.
2. Select **Account > Policies > Printer Authentication > Auto Registration**.
3. Select the check box for **Enabled**.
4. On the Badge Registration email validity period, define the maximum amount of time allowed for the user to respond to the badge registration email.
If a user does not respond to the Badge Registration email on time, they can re-swipe the card and try again.
5. Select the check box of **Enable** under Custom email Onboarding Message, for more information refer to [Custom Email Onboarding Message](#).

Custom Email Onboarding Message

When you enable the Auto Registration feature, the Custom Email Onboarding Message section appears. You can customize email messages that are sent during badge registration using OKTA, Hello ID and Azure-authentication.

Customizing an Email Onboarding Message

To customize an email onboarding message, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select **Account > Policies > Printer Authentication > Auto Registration**.
3. Select the check box of **Enabled**.
4. Under Custom Email Onboarding Message, select the check box of **Enable**.



Note: If you enable the check box and you do not make any changes to the message, the default message is sent.

5. From the Select Language menu, select the required language.
The default language is English.
6. In the text box, you can edit the email message.
For the text box, there are two options as follows:
 - **Reset to default:** This option allows you to reset the message.
 - **Insert Badge Registration Link:** This option allows you to insert the badge registration link.
7. Click **Insert Badge Registration Link**.

In the text box, the link is populated within the square brackets.
8. To save the settings, click **Save**.

Authentication Auto Enablement for Workplace Cloud Direct Printers

When the printers are configured for Workplace Cloud authentication, the Authentication Auto Enablement for Workplace Cloud Direct Printers setting enables authentication automatically. Xerox® Workplace Cloud authentication is supported on specific printer models.

This feature is only available on Xerox® AltaLink® and VersaLink® devices with the appropriate firmware level. For detailed information on Cloud Direct Printer enablement, refer to [Workplace Cloud Direct \(Manage Printer without an Agent\)](#).

Enabling Authentication Auto Enablement for Workplace Cloud Direct Printers

By default, Authentication Auto Enablement for Workplace Cloud Direct Printers is disabled.

To enable the Authentication Auto Enablement for Workplace Cloud Direct Printers feature, do the following:

1. Log in to Xerox® Workplace Cloud as an administrator.
2. Select **Account > Policies > Printer Authentication > Authentication Auto Enablement for Workplace Cloud Direct Printers**.
3. Select the check box for **Enabled**.

4. To save the settings, click **Save**.

A notification displays confirming that the settings have been successfully updated.

Disabling Authentication Auto Enablement for Workplace Cloud Direct Printers

To disable the Authentication Auto Enablement for Workplace Cloud Direct Printers feature, do the following:

1. Log in to Xerox® Workplace Cloud as an administrator.
2. Select **Account > Policies > Printer Authentication > Authentication Auto Enablement for Workplace Cloud Direct Printers**.
3. Select the check box for **Disabled**.
4. To save the settings, click **Save**.

A notification displays confirming that the settings have been successfully updated.

Cancel Jobs Timeout

An enhanced security mode is available, which enables you to set a time limit for how long released jobs of the user continue to process after the user logs out of the printer. This feature is available for follow-you jobs released using the @PrintByXerox App to a Xerox® VersaLink® or Xerox® AltaLink® printer. Additionally, to take advantage of this option, ensure that the Local Print Optimization setting is disabled.

Enabling the Cancel Jobs Time-Out Settings

To configure the settings, do the following:

1. Log in as Administrator.
2. Touch **Account > Policies > Printer Authentication > Cancel Jobs Time-out**.
3. Click **Enabled**.
4. Enter the number for the timeout in seconds.



Note:

- The time range for Cancel Jobs Time-out is 30–3600 seconds.
- The Cancel Jobs Time-out feature can be powered on or powered off with an optional timer.

For example, if the time is set for 1 minute when a user logs off, after 1 minute, the device cancels all the jobs that belong to that user.

Job Cancelling for Xerox® VersaLink® Devices

The Cancel option works with Xerox® VersaLink® devices with a software version later than 1.50.8, for example, version 1.55.0 or 1.57.3. Devices are configured to display the Cancel option in the @PrintByXerox EIP App.

1. Open a Web browser. Access the Embedded Web Server page for your Xerox® VersaLink® device.
2. Go to **Permission > Guest Access**, then click **Edit**.
3. Select a device user role.
4. Click **Everything except Setup**.

5. Click **OK**.



Note: If the device has software version 1.50.8, the Cancel function works without additional device configuration.

Job Cancelling for Xerox® AltaLink® Devices

1. Open a Web browser. Access the Embedded Web Server page for your Xerox® AltaLink® device.
2. To enable job management, select **Properties > Apps > Printing > Web Services**.
3. Select **Properties > Login/Permissions/Accounting > User Permissions/User Permission Roles**, then click **Edit**.
4. Click a non-logged in user name, then click **Edit**.
5. Click **Apps and Tools**.
6. Click **Presets**, then select **Custom**.
7. Click **Jobs permission**, then select **Allowed**.

PIN Authentication

PIN Authentication provides the ability for a user to authenticate using Alternate Login and entering their PIN.

- The PIN can be a registered physical card number, an LDAP imported PIN code, an administrator entered or imported PIN, or Auto-Generated PIN.
- When **Auto-Generated PINs** is selected, only auto-generated pins can be used to log in from printer alternate login. The auto generated pin login takes the place of managed pin login. If auto-generated PIN is enabled, managed pin login cannot be used. (This does not impact card/badge login using a card reader nor does it impact manual credential entry for the configured authentication type. For example: LDAP).
- The Auto-Generated PIN can only be viewed by the end user.
- The other pins can be viewed by the end user and the Administrator.



Note:

- PIN Authentication workflow is disabled by default.
- Alternate login using PIN is supported by the following authentication methods: Cloud Authentication, LDAP Authentication, Azure AD, OKTA Authentication, and HelloID.

Auto Generated Pins Overview:

- To generate a pin for an existing user, from the **User** tab the Administrator can select one or more users, then select the **Actions** menu and click **Generate New PIN**.
- If a user visits their Profile page and they do not have an Auto Generated Pin, a Pin will be automatically generated.
- When you generate a pin for a user, a link to the User Profile page is emailed to the user. The Auto Generated PIN can only be viewed on the User Profile page by the end User.

Enable PIN Authentication

1. Log in as an administrator to Xerox® Workplace Cloud.

2. Select **Account > Policies > Printer Authentication**.
3. To enable PIN Authentication, select the radio button for **Enabled**.

Once enabled the following two options appears.

- **Card Number/Administrator Managed Pins** (Default): When selected the User can login with their card pin.
- **Auto-Generated Pins**: When selected, all newly onboarded users will get a new PIN generated. Users can see their auto-generated PIN in their User Profile.

4. Click **Save**.

Guidelines for PIN Auto Generation:

- The ability to use auto-generated pins applies only to the Printer Essentials Bundle license. The functionality will be hidden for other license types.
- The auto-generated pin will not be stored in the Cloud Print Agent user security cache.
- The auto-generated pin cannot be exported or imported.
- An XWC Administrator cannot see the auto-generated pin associated with the user.
- About the Pin value:
 - The pins are numeric only.
 - The default length is 6 digits.
 - The minimum length of a pin is 4 numeric characters and the maximum is 8.
- If the system runs out of digits when creating pins the solution will automatically increase the length of the auto-generated Pin.
- All auto-generated PINs will be prepended with an @ character and the user must enter the @ prepended to their Pin to authenticate..
- A pin is never reused in a company.

Disable PIN Authentication

1. Log in as an administrator to Xerox® Workplace Cloud.
2. Select **Account > Policies > Printer Authentication**.
3. To disable PIN Authentication, select the radio button for **Disabled**.



Note: **Disabled** option is a default setting.

4. Click **Save**.

Allow Multiple Primary PINs or Access Cards

The Allow Multiple Primary PINs or Access Cards feature enables users to register multiple cards. Users can authenticate and release jobs using any of the registered cards.

Enabling Allow Multiple Primary PINs or Access Cards

To authenticate and release jobs, enable the Allow Multiple Primary PINs or Access Cards feature. The feature identifies an account that is tagged against multiple cards.

To enable the Allow Multiple Primary PINs or Access Cards feature, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Select **Account > Policies > Printer Authentication**.
3. In the Allow Multiple Primary PINs or Access Cards area, select the radio button for **Enabled**.
By default, the setting is disabled.
4. To save the setting, click **Save**.



Warning: If the Allow Multiple Primary PINs or Access Cards feature is enabled and you later disable it, all the PINs or access card numbers are deleted.

After you enable the Allow Multiple Primary PINs or Access Cards feature, in the **Users > Edit User** page, the Registered Cards / PINs area appears. For more information, refer to [User: Details](#).

Domain Qualification

When Company Authentication Type is set to **LDAP**, the Domain Qualification feature is available. By default, the Domain Qualification feature is enabled. When the feature is enabled, credential information is sent to the printer, and the system prepends the user domain to the network user name. For example: DOMAIN\USERNAME. To enable LDAP authentication, refer to [LDAP Authentication](#).

If the Domain Qualification feature is disabled, the domain name is removed.

Disabling Domain Qualification

To disable Domain Qualification, do the following:

1. Click **Account > Policies > Printer Authentication**.
2. Deselect the check box for **Enabled**.
3. To save the configuration, click **Save**.

4-Digit Code Unlock with Workplace Mobile App

The 4-Digit Code Unlock with Workplace Mobile App features enables the users to unlock a printer by entering the 4-digit code displayed on the blocking screen of the printer in the Workplace Mobile App. This is a supplemental login workflow provided for cases where users do not have their physical card with them.

Enable or Disable a 4-Digit Code Unlock with Workplace Mobile App

To enable authentication on Xerox® devices using Xerox® Workplace Cloud, set a blocking screen message. To unlock Xerox® devices, users can input a code in a mobile app.

To configure the settings, perform the following steps:

1. Log in as an administrator.
2. Select **Account > Policies > Printer Authentication > 4-Digit Code Unlock with Workplace Mobile App**.
3. By default, the setting is Disabled. To enable the unlock settings, select **Enabled**.
4. To disable the unlock settings, select **Disabled**.

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

A notification displays confirming that settings have been successfully updated.

QR Code Unlock with Workplace Mobile App

Guidelines for Unlocking the Printer Using QR Code:

There are several ways to unlock the printer by scanning a QR Code.

- The Welcome Page contains two QR Codes, one to install the Workplace Cloud App, the other QR Code is used to unlock the printer while using the Workplace Cloud App.
- The Generate Label QR Code can be used in multiple ways depending on a setting.
 - Normal function with **Allow Mobile Unlock Using Native Camera** turned off, the QR Code can be used to unlock the printer from the Workplace Cloud App.
 - With **Allow Mobile Unlock Using Native Camera** turned on, the QR Code can be used in two ways.
 - If the Xerox® Workplace App is not installed in the mobile device, it redirects you to install the App.
 - If the Xerox® Workplace App is installed, then it opens the Workplace App and if you are logged in, it unlocks the printer.
- If you are currently using mobile unlock and wish to enable the **Allow Mobile Unlock Using Native Camera** feature, you need to repair your printers after doing so. If you are using the Xerox Workplace Cloud printer labels, you should regenerate the labels and attach them to the printers.

Display QR Code

Displays a QR Code on the authentication blocking screen of the printer. Users may scan the QR Code using the Workplace Mobile App to unlock the printer.

1. Log in as an **Administrator**.
2. Select **Account > Policies > Printer Authentication > QR Code Unlock with Workplace Mobile App > Display QR Code**.
3. By default, the setting is Disabled. To enable the unlock settings, select **Enable**.

A mobile with the Workplace App installed will support the unlock feature.

4. To save the settings, click **Save**.

A notification displays confirming that the settings have been successfully updated.

Allow Mobile Unlock Using Native Camera


For mobile devices with Workplace App installed, allow the native camera application to unlock the printer when scanning the QR Code on the blocking screen or on a label affixed to the printer.


1. Log in as an **Administrator**.
2. Select **Account > Policies > Printer Authentication > QR Code Unlock with Workplace Mobile App > Allow Mobile Unlock Using Native Camera**.
3. By default, the setting is Disabled. To enable the unlock settings, select **Enable**.

A mobile with the Workplace App installed will support the unlock feature using the native camera.

4. To save the settings, click **Save**.

A notification displays confirming that the settings have been successfully updated.

 **Important:** Changes to this setting will not be applied to existing printers. After saving your change repair all existing printers to which you would like this setting to be applied. If using QR Code labels please reprint the same and attach it to the respective devices.

 **Note:** VersaLink® does not support QR Code blocking screen. To use QR Code unlock use the **Generate Labels** feature and attach the printer label to the printer. For more information refer to [Generate Labels](#).

Machine Access

Convenience Authentication Service Pathway Options allows Xerox® Workplace Cloud administrators to block a device user interface, or to allow locked services to be managed at the device. The following options are available:


- **Manage Machine Access at the Device:** This option prevents Xerox® Workplace Cloud from modifying device access settings, and locking screen settings are not pushed to the device. With this option enabled, if a user attempts to access the @PrintByXerox EIP app, they are required to log in to the app using the configured Workplace Cloud authentication method.
- **Manage Machine Access Using Print Management:** This option permits management of device access settings by Xerox® Workplace Cloud. When Manage Machine Access Using Print Management is enabled, the following options are available:
 - **Service Pathway Enabled:** Xerox® Workplace Cloud pushes blocking settings to the target device, and blocking screen displays at the device local user interface, and access to the device is prevented.
 - **Service Pathway Disabled:** Xerox® Workplace Cloud pushes blocking settings to the target device, but no blocking screen displays at the device local user interface, and access to the device is permitted.

Configuring Service Pathway Options for Convenience Authentication

To configure service pathway options:

1. Click **Account > Policies > Printer Authentication**, then select **Machine Access**.
2. For managing machine access, select from the following options:
 - **Manage Machine Access at the Device**
 - **Manage Machine Access using Print Management**
3. If you select **Manage Machine Access using Print Management**, to enable the Service Pathway option, select **Service Pathway Enabled**.
4. To save the settings, click **Save**.

A notification displays confirming that the settings have been updated.

 **Note:** Updates that are made to Service Pathway Options settings are automatically applied to newly added printers but are not applied to existing printers. To apply updates to existing printers, perform the Repair function on the printer.

Printer Control Panel: Administrator Login

The Administrator Login feature provides a user access to printer administrator functions when the printer is locked down and managed by Workplace Cloud. When the administrator enables this feature, users can use the Alternate Login option to log in to the printer control panel and access the printer administrator functions.

To use this feature, on the first Alternate Login screen the user is required to enter the user name as `admin`, then enter the password that was provided at the time of enablement of the feature.



Note:

- You must use an authentication method for your cloud company that supports Alternate Login.
- Alternate login is supported by the following authentication methods: Cloud Authentication, LDAP Authentication, Azure AD and OKTA Authentication.

Enabling the Administrator Login Feature from Xerox® Workplace Cloud

To enable the Administrator Login feature and to access the administrator function of a printer, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Policies > Printer Authentication**.
3. In the Printer Control Panel: Administrator Login section, select the check box for **Enable**.
4. In the Password text field, type the administrator password.



Note: The password do not need to match the current printer administrator password. When this feature is enabled the password you enter is used to login to the printer as a printer administrator.

5. Enter the password you want to login to the printer as an administrator when this feature is enabled.
6. To confirm your changes, click **Save**, or to cancel the changes, click **Cancel**.

Using the Administrator Login Feature

To access the administrator functions at the printer, do the following:

1. Select the Alternate Login icon.
2. In the Enter PIN or Email field, type `admin`, then select **Enter**.
If you do not enter `admin`, the printer assumes you are logging on as a non-administrative or a regular Cloud user.
3. In the Password field, enter the password that was used when the feature was enabled, then select **Enter**.

Administering Your Printer at the Local User Interface

If you are using the Cardless or Card based Authentication feature and you wish to perform administration functions via the Local User Interface, you may need to temporarily change the printer's Authentication mechanism using CentreWare Internet Services on the printer from Convenience Authentication / Xerox Secure Access to Local mode. This allows an administrator to log into the Local User Interface and perform administration tasks. Once complete, the authentication mechanism can be changed back to Convenience Authentication / Xerox Secure Access.

Card Setup

If proximity card readers are used, 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

Security



Note: The Company Root Certificate is only use for Single Sign-On feature and printers configured for Cloud Direct.

This section allows the you to create and manage the Company Root Certificate for Workplace Cloud Company, this certificate will be used for Single Sign-On authentication when a Cloud Direct printer connects to the Workplace Cloud solution. This Certificate is used to validate the identify of the printer when making Single Sign-On requests.

For more information on Cloud Direct, refer to [Workplace Cloud Direct \(Manage Printer without an Agent\)](#).

For enabling Single Sign-On on Cloud Direct printer, refer to [Enable Single Sign-On for Cloud Direct Devices](#)

A unique client certificate will be created and installed on the printer when enabling the printer authentication feature and only active Company Root Certificate is supported.



Important: After creating or activating a different root certificate, you must perform a repair action or disable and enable authentication on your printers.

Company Root Certificate Management

Creating and Activating a Company Root Certificate

To create and Activate Root Certificate:

1. Click **Account > Policies > Security**.
2. Under Company Root Certificate Management, click on **Actions > Create**.

The new Root Certificate is created.



Note: The first Company Root Certificate is activated automatically.

3. To change the Company Root Certificate, refer to [Changing the Company Root Certificate](#).

Changing the Company Root Certificate

To Change the Company Root Certificate:

1. Add a new Root Certificate, under Company Root Certificate Management, click on **Actions > Create**.

A new Company Root Certificate is created.

2. Select the required Root Certificate and click on **Actions > Activate**.

The Selected Root Certificate is activated for Single Sign-On authentication.



Note: Activating the selected root certificate deactivates the currently active root certificate. You must perform a repair action or disable and enable authentication on your printers to synchronize the root certificate for Single Sign-On authentication.

Delete the Company Root Certificate

To delete the Root Certificate:



Note: You cannot delete the Active Root Certificate, if necessary change the Root Certificate and perform the deletion action.

1. Click **Account > Policies > Security**.

Select the required Root Certificate.

2. Click **Actions > Delete**.

The Selected Root Certificate is deleted. You must perform a repair action or disable and enable authentication on your printers to synchronize the new root certificate for Single Sign-On authentication.

POLICIES: RULES

Rules can be created to define print controls, print quotas and print limits. You can apply rules to All Users or User Groups. This section contains the information on using the following Rules:

- **Print Controls**
- **Print Quotas**
- **Print Limits**



Note: Refer to **Implementing Rules** section for instructions on how to test the rules before applying them to your users.

Print Controls

Print Controls Overview

The Print Control rule controls printer access for Users and User Groups, Printer and Printer Groups by defining the Print Release Time and Printing Attributes.

Print Controls Rule Guidelines

- Rules apply only when you release a job to a printer.
- 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. The warning email depends on if you have the Email Notifications turned on.
 - If using @PrintByXerox, the app shows a warning
 - If using the Workplace Mobile App, the portal shows a job status of Modified
 - If mobile phone notifications are on, the cloud sends you a message.
- When you are assigned to multiple rules, the rule that enables the most permissions takes precedence over rules that are more restrictive.
- When using desktop print path with custom drivers, or direct print the Print Controls Rules are not applicable at least for color access and plex. You must use the driver XML tool if you want to enforce certain values for example: you can only print in B&W. For more information on the XML tool, refer to [Xerox® Driver Configuration](#).
- Below is a list of print paths with details on the forcing part of the print controls.
 - Follow-You print with Xerox® Generic Driver (GPD): Print Controls do apply.
 - Follow-You print with custom driver: Print Controls don't apply, use XML tool.
 - Direct print with Xerox® Generic Driver (GPD): Print Controls don apply, use XML tool.
 - Direct print with custom driver: Print Controls don apply, use XML tool.

Print Control Rule Actions

To create, delete, enable, or disable a rule:

1. Select **Account > Policies > Rules > Print Controls**.
A list of rules appears.
2. To change the status of a rule, select a rule from the list. Select **Actions > Delete**, **Actions > Enabled**, or **Actions > Disabled**.
A confirmation message appears.
3. Click **OK**.

Creating a New Print Control Rule

To create a rule:

1. Select **Account > Policies > Rules > Print Controls**.
The Rules tab appears.
2. Select **Actions > New**.
The Create New Rule tab guides you through the rule creation process.
3. Type the Rule Name and a brief Rule Description, 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. To select a User Group, click **Actions > Add**.
The Add User Groups page appears.
3. From the available User Groups list, select user groups to add to the rule.
4. Click **Save**.
The selected User Groups appear on the User Association page.
5. 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 printer groups to the new rule:
 - a. Click **Printer Groups**.
 - b. To select a Printer Group, click **Actions > Add**.
The Manage Printer Access page appears.
 - c. From the available Printer Groups list, select printer groups to add to the rule.
 - d. Click **Save**.
The selected Printer Groups appear on the Devices page.
 - e. 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 Content Rule Summary, select the **Enabled** check box.
2. To edit the new rule, click **Back**.
3. To save the rule, click **Finish**.

Modifying Print Control Rules

You can modify existing print control rules to adjust settings as required.

To modify an existing print control rule:

1. Select **Account > Policies > Rules > Print Controls**.
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**.

Viewing the Print Control Rules Assigned to a User

To view the assigned rules for an existing user:

1. Select the **Users** tab.
A list of current users appears on the Users subtab.
2. To view the 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

The Print Quotas feature provides administrators with the ability to control and restrict the total number of pages that a user can print. Print Quota rules define how many pages a user can print in a Daily, Weekly and Monthly period.



Note:

- When more than one print quota rule is enabled, the more restrictive rule will be 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 will always be enforced first.
- Print Quota Rules are designed to allow a print job to be completed even if the job 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.

Setting Print Quota Parameters

Users have the option to configure the Print Quota period and pages per job estimation when print jobs cannot be parsed to determine the number of pages in the job.


1. Click **Account > Policies > Rules**.
2. To set the print quota period, select one of the following options:
 - **Daily** – Select this option to replenish the allocated print quota every 24 hours at 00:00 server time.
 - **Weekly** – Select this option to replenish the allocated print quota every 7 days on Monday at 00:00 local time. The duration is Monday to Saturday.
 - **Monthly** – Select this option to replenish the allocated print quota on the first day of each calendar month at 00:00 local time.
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

To create or modify a print quota rule:

1. Click **Account > Policies > Rules**, then select the **Print Quotas** tab.
2. To create a new rule, click **Actions**, then select **Add**.
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, select the required group from the Available User Groups list, then to save the changes and exit the Add User Groups dialog, click **Save..**
 - b. To remove a User Group from the Associated User Groups, select the required User Group, then click **Actions > Delete**. To confirm your selection, click **OK**.
 - c. To create a new User Group, click **Users > User Groups**, then select **Actions > New**. Follow the on screen instructions
 - 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 left blank. You must insert a value between 1 and 999.
- The default setting for the print quota period is Monthly. 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

Users have the ability to enable or disable print quota rules for all users or specific users.

To enable or disable a print quota rule:

1. Click **Account > 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 the selected rule, click **Actions**, then select **Enable**.

An Enable Rule dialog displays. To enable the rule, click **OK**, or to exit the Enable Rule dialog box and cancel any changes, click **Cancel**. Any changes are saved automatically.

4. To disable the selected rule, click **Actions**, then select **Disable**.

A Disable Rule dialog displays. To disable the rule, click **OK**, or to exit the Disable Rule dialog box and cancel any changes, click **Cancel**. Any changes are saved automatically.

Deleting a Print Quota Rule

To delete an existing print quota rule:

1. Click **Account > 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 Remove Rule dialog box appears.

4. To confirm your selection, click **OK**, or to exit the dialog box without saving your changes, click **Cancel**.


The settings are saved automatically.

Modifying Print Quota Rules

You can modify existing print quota rules to adjust settings as required.

To modify an existing print quota rule:

1. Click **Account > Policies > Rules**, then select the **Print Quotas** tab.
2. To open the details page for the rule you want to modify, click the name of the rule.

3. Adjust the settings as required:
 - To enable or disable the rule, click the **Details** tab, then select the required option.
 - To update the rule name and rule description, click the **Details** tab, then enter the new information as required.
 - To change the user association for the rule, click the **Users** tab, then select one of the following options:
 - **All Users**: This option applies the print quota rule to all users.
 - **Select User Group(s)**: This option applies the print quota rule to selected user groups that are created in the Users > User Groups menu.
 - To update the print quota pages value, click the **Quota** tab, then update the value as required.
-  Note: The value must be a number between 1 and 999.
4. To save the settings, click **Save** or to cancel any changes and exit the print quota rules page, click **Cancel**.

Setting Override Print Quota Rules for Individual Users

To set a print quota for an individual user:

1. Click **Users**, then select the required user from the list.
2. Click **Details**.
3. To override general print quota rules and display configuration options for the individual user, select the **Override Print Quota Rules** check box.
4. To set print quota rules, choose one of the following options:
 - **Unlimited**: This option allows the user to print unlimited page and overrules the general print quota page limit.
 - **Limited**: This option allows you to set the page limit for the user and overrules the general print quota page limit.
5. To set the print quota for the user, enter the required value
6. To set the print quota period, refer to [Setting Print Quota Parameters](#).
7. To save the settings, click **Save**.

A notification displays confirming that the changes have been saved.

Analyzing Print Quotas - Actions Menu

You can view an overview of an individual user print quota, as well as any enforced rules that affect the user.

To show user Print Quota information:

1. Click **Users**, then select a user from the list.
2. Select **Actions > Analyze Print Quota**.

Print quota information for the user displays.
3. To exit the Analyze Print Quota dialog box, click **Close**.

Print Limits

Print Limits Overview

The Print Limits feature provides administrators the ability to restrict the number of pages that all users or user groups can print in a single job.

Print Limits Guidelines

- You can apply Print Limits to All Users or Selected User Groups.
- You can set the Color Page Limit and Total Page Limit for a print job.
- A user will not be able to print a job if they are not associated with any of the rules defined based on their group membership.
- Whenever a user attempts to print a job with one or more rules defined, the largest Color and Total Page count will be used against all rules.
- 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 2 copies of a 9–page job, the job gets blocked from printing.
- When a user exceeds their Print Limits for Desktop jobs, Workplace Cloud 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.

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 @PrintByXerox application that exceeds their print limit, the job fails and a message appears on the EIP app and on the printer console in addition to the email notification.
- For auto-release jobs the user will get an email notification.
- 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 Cloud Administration Job History page.

Modifying the Notification Settings Message

The notification message appears in available languages.

1. To modify the notification message, click **Account > 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, type in the required notification message with the following options that are to be inserted in the Message field:
 - **Reset to default:** This option modifies the notification message and resets the message to the default message.
 - **Insert Document Name:** This option inserts your print jobs Document Name in your customized notification message.
 - **Insert Rule:** This option inserts the Print Limit Rule which is blocking your print job in your customized notification message.
 - **Insert Page Count:** This option inserts the permitted Page Count for your print job in your customized notification message.
4. Click **Reset to default** option to reset to the default notification message.
5. To save the changes, click **Save**.

A notification displays confirming that the settings have been saved successfully.

Creating a Print Limits Rule

To create a print limit rule:

1. To create a rule for Print Limits, click **Account > Policies > Rules**, then select the **Print Limits** tab.
2. To create a new rule, Click **Actions**, then select **add**.
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. 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, Click on **Actions**, then select **add**:
 - a. A pop-up window appears. To add a User Group to the Associated User Groups, select the required group from the Available User Groups list, then to save the changes and exit the Add User Groups dialog, click **Save..**
 - b. To remove a User Group from the Associated User Groups, select the required User Group, then click **Actions > Delete**. To confirm your selection, click **OK**.
 - c. To create a new User Group, refer to [Creating User Groups](#).
 - d. To add the Associated User Groups to the new rule, click the check box of the required User Groups.
7. To confirm the settings, click **Next**.
8. To Set Page Count Limits for the new rule, in the Color section, select one of the following:
 - Select the **Unlimited** radio button to allow users to print unlimited color pages per job.
 - Select the **Page Limit** radio button and enter the maximum number of color pages that can be printed per job.
9. To Set Page Count Limits for the new rule, in the Total section, select one of the following:
 - Select the **Unlimited** radio button to allow users to print unlimited pages per job.
 - Select the **Page Limit** radio button and enter the maximum number of pages that can be printed per job.

10. 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.

Editing an Existing Rule

To edit an existing rule:

1. Select **Account > Policies > Rules > Print Limits**.
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** and **Limits**.

Enabling or Disabling a Print Limits Rule

Users have the ability to enable or disable print limit rules for all users or specific users.

To enable or disable a print quota rule:

1. To enable or disable a printing limit rule, click **Account > 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 the selected rule, click **Actions**, then select **Enable**.
A dialog box appears.
4. Click **OK** to save the settings or click **Cancel** to change the selection.
5. To disable the selected rule, click **Actions**, then select **Disable**.
A dialog box appears.
6. Click **OK** to save the settings or click **Cancel** to change the selection.

Deleting a Print Limits Rule

1. To delete a rule from the Rules list, click **Account > 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. Click **OK** to save the settings or click **Cancel** to change the selection.

Viewing the User Print Limits Summary

To access information about Print Limits rules that apply to a user account.

To view user print limits:

1. Log in to the Xerox Workplace Cloud application.

2. In the upper-right corner of the screen, click your user name.
3. Under **User Profile, Details** section, click on **User Information**.

Your print limit summary appears.

Viewing the Users Print Limits through Admin

Admin can access information about Print Limits rules that apply to an user account.

To view user print limits:

1. Log in to the Xerox Workplace Cloud application.
2. Click **Users** tab.
3. On the Users email list, click on the required User email.
4. Click **Rules > Print Limits** tab.

The User print limits summary appears.

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 continue to print while you validate the 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, that contains the Rule options 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.

POLICIES: PRINTER SELECTION

Direct Printer Selection

Direct Printer Selection enables the following print submission paths:

- User access to the Print > Web tab from the Xerox Workplace Cloud web portal.
- User access to direct printers in the Xerox Workplace App.
- User job submission to a printer direct print email address.



Note: When Direct Printer Selection is disabled, these print submission paths are not available to the user.

Enabling and Disabling Direct Printer Selection

To enable or disable Direct Printer Selection:

1. Click **Account > Policies > Printer Selection**.
2. To enable Direct Printer Selection, ensure that the **Allow Direct Print** check box is selected.
3. To disable Direct Printer Selection, ensure that the **Allow Direct Print** check box is not selected.
4. To save any changes, click **Save**.

A notification appears confirming that the settings have been updated.

QR Code Printer Selection

To reduce the amount of print jobs that are sent to the printer and never picked up, administrators can require users to sign in to the printer using the QR Code on the Welcome Sheet by the printer or using the QR Code on the @PrintByXerox app.

Enabling the QR Code Login at the Printer

When you enable this feature, all printing requires to scan the QR Code of the Welcome Sheet or the Xerox App Gallery: QR Code App using the Print Portal Mobile application. When the user scans the QR code all the users jobs are automatically released.

To enable the QR code login at the printer, do the following:

1. Select **Account > Policies > Printer Selection**.
2. Select the check box for **Require QR Code Printer Selection**.
3. Click **Save**.
4. For more information to log in at the printer, refer to [Logging into the @PrintByXerox App using a QR Code](#).

POLICIES: OFFLINE MODE

This section is used to configure the behavior of the system when the Xerox services are not available or cannot be reached using the Internet.

Enable DNS Offline Mode Checking

When you enable the Enable DNS Offline Mode Checking feature, the Xerox® Workplace Cloud Client checks for cloud connectivity periodically and switches between online and offline modes automatically. To use the Enable DNS Offline Mode Checking feature, configure DNS server appropriately. For more information, refer to [Configuring the DNS server for Offline Mode](#).

Configuring the DNS server for Offline Mode

To use the Enable DNS Offline Mode Checking feature, the customer IT department has to set up the DNS server, to add a DNS Flag used by Xerox® Workplace Cloud. For more information, refer to [Configuring the Microsoft® Windows® DNS Server](#).

1. Identify the DNS Zone that serves the Xerox® Workplace Cloud Agent. In **DNS Manager > Forward Lookup Zones**, create a new primary zone called `print.internal.xcp`.
2. Create a DNS TXT record in the DNS Server `OfflineMode.print.internal.xcp.xx.xx.xxx.xxx` (`XWC.OfflineMode.Enabled= True`).
The value of the TXT record is: `XWC.OfflineMode.Enabled=TRUE`.

3. To save the settings, click **OK**.

Offline Printing Using Rules

When the system is in offline mode, the following printing behavior are enforced by the Desktop Client:

- **Do not allow printing in offline mode when rules are enabled:** If this option is enabled, when any rules are enabled, the system does not allow printing from the client when the server cannot be reached. If rules are disabled then the system allows printing in offline mode. For more information on rules, refer to [Print Control Rule Actions](#).
- **Allow printing in offline mode, but rules will not be applied:** If this option is enabled, the system allows printing regardless of the state of the rules.

Enforcing Printing Behavior by the Desktop Client

To enforce printing behavior by the desktop client, do the following:

1. Log in to Xerox® Workplace® Cloud as an administrator.
2. Click **Account > Policies**, then select **OfflineMode**.

The Offline Mode page appears.

3. In the Offline Printing Using Rules area, select any of the following printing behavior:
 - **Do not allow printing in offline mode when rules are enabled**
 - **Allow printing in offline mode, but rules will not be applied**

POLICIES: CONTENT SECURITY



Note: The Content Security option supports the Home Worker Print Tracker workflow.

The Content Security feature identifies when business documents that are labeled to restrict their distribution and use are released to the printer.

An administrator can configure content security. You can define search strings to use in the identification process and configure the list of email addresses that receive alerts. Alerts are sent to these email addresses when a document that contains any of these search strings is released to a printer. Additionally, content security results are reflected in the company printer jobs history, and the data is reflected in the Job Reporting Dashboard. For more information on company printer jobs history, refer to [Viewing the Job Status of the History and Print Tracker](#).

For more information on job reporting, refer to [Dashboard](#).



Note: The Content Security feature applies to files that are processed as PS or PCL Custom Driver jobs that are submitted through the Windows Client.

Content Security Workflow Guidelines

Search strings are keywords used to search documents that are submitted for printing. The Content Security Workflow guidelines are as follows:

- Content Security applies to documents submitted using the Windows Client only.
- Content Security ensures that the Home Worker Print Tracker jobs are processed.

- Content Security parses the file for search strings in the text, but not in the images.
- Content Security checks for all search strings. After the Content Security feature has found a particular search string, it moves to the next search string. The matched search strings are stored with the job history.
- When you print a document, you can set an email alert to send an email to preselected recipients automatically. The email informs the recipients that the document matched a Content Profile. The document prints on the named device at the device location.
- Content Security targets the jobs that contain commonly used Microsoft Office or Microsoft Windows fonts.

Enabling Content Security



Note: By default, **Enable Content Security** is disabled for existing and new accounts.

To enable Content Security, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Policies**, then select **Content Security**.
3. Select the check box for **Enable Content Security**.

The Search Strings and Email Alert sections appear.

4. In the Search Strings section, in the New Value field, specify any search strings.
5. Add the search strings using the arrows.
By default, there is no search string. Ensure that each search string in the list is unique. If you attempt to add an existing search string, the duplicate search string is not added to the list. If no search strings are specified and you attempt to save the settings, an error message appears that states *Content Security cannot be enabled without at least one search string specified*. If any of the specified search strings exist in the file content, all PS or PCL Custom Driver jobs are parsed at submission time and are flagged, if any of the specified search strings exist in the file content.
 - a. In the New Value field, enter a search string.
 - b. To add the New Value field content to the Search Strings list, click the right arrow.



Note: If you attempt to add a duplicate search string to the list, when you click the arrow, the value is not added.

6. Remove the existing search strings.
 - a. From the Search Strings list, to remove a string from the list, select the search string.
 - b. To remove the value, click the left arrow.
7. In the Email Alert section, configure the required email addresses.
 - a. In the New Value field, enter an email address.
 - b. To add the New Value field content to the To Email Addresses list, click the right arrow.
When you click the arrow to add a duplicate email address to the list, the value is not added. To ensure that email addresses are in the correct format, they are validated. The correct format for email addresses is `name@company.domain`, for example: `tester@test.com`.
8. Remove existing email addresses:
 - a. From the To Email Addresses list, select the email address.

- b. To remove the value, click the left arrow.
9. To save the settings, click **Save**.
You cannot enable Content Security unless at least one search string and one email address are specified.

After you enable the Content Security feature:

- All PS or PCL Custom Driver jobs are parsed for search strings at submission time.
- When jobs released to a printer are identified as containing one or more of the configured search strings, email notifications are sent.
- Content security information is shown in the job history, home worker print tracker job history, and reporting data.

Disabling Content Security

To disable Content Security, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Account > Policies**, then select **Content Security**.
3. Clear the check box for **Enable Content Security**.
4. To save the setting, click **Save**.

After you disable the Content Security feature:

- You do not need to specify any search strings.
- All PS or PCL Custom Driver jobs are not parsed for search strings at submission time.
- You do not need to specify any email addresses.
- Content security information is not shown in the job history, home worker print tracker job history, and reporting data.

POLICIES: CLIENT APPLICATION

Client Application authentication supports Mobile Application, Chrome extension, Mac, and Windows Clients.

Enabling the @PrintByXerox Login

Administrators can set it up so that users can use the Workplace Mobile App to scan the QR Code shown in the client application of the printer. Once the users successfully scan the QR Code, they are logged into the @PrintByXerox app with their current jobs selected and ready to print.

1. Log in to <https://xwc.services.xerox.com> as an administrator.
2. Select **Account > Company Profile**.

3. Under Client Application Authentication (@PrintByXerox Login), select the **@PrintByXerox Login Enabled** check box.



Note: When you initially set up a company, you can select **Use as alias** in the Details area of the Web UI and use a unique email address instead of **print@printbyxerox**. When Use as alias is selected, the **Enable Express Code for [email address]** check box becomes available. When this check box code is selected, the user will get an email upon successful submission of documents to the cloud, and that email will contain a 6 digit number. The user may then walk up to any printer in their company, and type in the 6 digit number on the @PrintByXerox app. The @PrintByXerox app will log them in and display the documents they submitted. If the express code is not enabled, the user would have to log into @PrintByXerox app with their email address and password in order to print their documents.

4. Refer to [Logging into the @PrintByXerox App using a QR Code](#) for instructions.

Account: Accounting

This chapter contains the configuration information for:

- [Accounting: Accounting Options](#)
- [Accounting: Accounting Prompts](#)
- [Accounting: Administrative Defaults](#)
- [Accounting: Job Reporting](#)

ACCOUNTING: ACCOUNTING OPTIONS

Xerox® Workplace Cloud supports printing to Accounting-enabled printers for companies to track printer usage by users.

One of the following modes can be enabled to track printer usage:

- Xerox® Network Accounting
- Xerox® Standard Accounting



Note: These accounting modes are only available on select Xerox® devices.

Xerox® Network Accounting

Xerox® Network Accounting automatically tracks printer usage for each user. Network Accounting is run over a network and the accounting functions are performed remotely via third party software.

Xerox® Standard Accounting

Xerox® Standard Accounting automatically tracks printer usage for each user. Limits can be applied to users to restrict their usage. Standard Accounting is configured via Internet Services and requires no additional software.

Setting Up a Default Accounting Mode for the Printers of Your Company

When each printer is first discovered, it is automatically configured with the default accounting mode. Selecting a Xerox® accounting mode is recommended only when most printers in the environment have Xerox® accounting enabled. Settings for existing printers can be changed on the **Printers** tab.



Note: This setting does not affect print queues.

1. From the Web Portal, select the **Account** tab.
2. Select **Accounting**.
3. Select **Accounting Options**.
4. Select an accounting mode under **Set the default printer Accounting mode for your Company's Printers**.
5. Select **Save**.

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. They 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.

1. From the Xerox® Workplace Cloud Web Portal, select the **Account** tab.
2. Select **Accounting**.
3. Select the check box for **Allow User Accounting Data to be Saved** as the Accounting data retention policy.
4. Select **Save**.

Adding the Accounting Data in the Job History Report

1. From the Web Portal, select the **Account** tab.
2. Select **Accounting**.
3. Select the check box for **Show User Accounting Data in Job History Report** as the Accounting retention data policy.
4. Select **Save**.

Allowing Direct Email Printing When Accounting is Enabled

Direct email printing is sending an email directly to a Xerox® Workplace Cloud-enabled printer's email 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 app or Web Portal and have entered their accounting information.

When printing from the Web Portal, users must enter their accounting information on the **Print** tab, save it, and print. If the user does not print, the accounting information that they entered is not saved. If users previously printed to that printer or print queue, and have entered their accounting information, Xerox® Workplace Cloud will apply the saved information on subsequent email submissions.



Note: Xerox® Workplace Cloud does not store user passwords.

1. From the Web Portal, select the **Account** tab.
2. Select **Accounting**.
3. Select **Allow User Accounting Data to be Saved**.
4. Select **Save**.

Sending User Domain Information to Server-Based 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. From the Web Portal, select the **Account** tab.
2. Select **Accounting > Accounting Options**.

3. Select the check box for **User domain will be sent to the accounting system** under **Server-based Accounting**.

This check box is not available unless an agent reports available LDAP domains.

When this check box is selected, users will be prompted for the domain and username (i.e., domain\username) when entering accounting information for submitting jobs to print queues.

4. Select **Save**.



Note: Xerox® Workplace Cloud does not store user passwords.

ACCOUNTING: ACCOUNTING PROMPTS

This section is used to enable User Accounting prompts. Once Accounting prompts are enabled, users are required to enter a valid accounting code at the time of authentication at the printer. The accounting code(s) they enter will be saved with the job accounting data for user level job tracking.

Accounting Prompts Guidelines:

- The label name for accounting prompting is what the end user will see on the printer. If you change the label name of the User ID and/or Account ID fields, new accounting fields are not created. The user entered values will still map to the underlying User ID and Account ID Accounting fields. When you generate an accounting Report, the heading in the report still reflects the underlying values of Accounting User ID and Account ID.
- When the user enters accounting codes into the User ID and Account ID Accounting fields, the codes they enter are compared to the data in the Xerox Workplace Cloud Valid Values fields. If they enter a code that does not match an entry, they will be prompted to re-enter the value.
- When the user enters accounting codes into the User ID and Account ID Accounting fields, the data is copied into the Users current login session on the printer, such that any printing, copying, scanning, and faxing task they perform will include the entered accounting data from the session. This information will be included in the Reporting data of the solution when using the Usage Tracking feature.
- When using this feature, it is recommended to enable **Usage Tracking** so that Xerox Workplace Cloud can retrieve the Network Accounting Data from the printer and include it in the Reporting feature of the solution.
- The User ID and Account ID codes that the User enters are not saved for the individual User.

Enable Accounting Prompts

You can enable either one or both the prompts by configuring a valid set of accounting codes below. The accounting codes will be included in the user login session on the printer.



Note: Printer Authentication has to be enabled for this functionality to work.



Important: These settings are automatically applied to newly added printers, but not existing ones. After saving your changes, repair all existing printers to which you would like these settings to be applied.

The Enable Accounting Prompts section has the below options:

- **Enable User ID**
- **Enable Account ID**

Enable the User ID:

1. From the Web Portal, select the **Account** tab.
2. Select **Accounting**.
3. Select **Accounting Prompts**.
4. In the Enable Accounting Prompts section, select the check-box for **Enable User ID**.



Note: Once the prompting is enabled, ensure that the device is repaired.

5. Enter the User ID in the Label field.
The Label field sets the label to be displayed at the time of prompting during authentication.
6. Enter the valid values in the New Value field.
Use the right-arrow to move the values to the Saved Values field.
7. Optionally enable the option **Mask Accounting Code** to mask the accounting code that the user enters during the authentication sequence.

Enable the Account ID:

1. In the Enable Accounting Prompts section, select the check-box for **Enable Account ID**.
2. Enter the Account ID in the Label field.
The Account ID can be an alphanumeric text box which supports up to 64 characters with UTF8 Support.
3. Enter the valid values in the New Value field.
Use the right-arrow to move the values to the Saved Values field.
4. Optionally enable the option **Mask Accounting Code** to mask the accounting code that the user enters during the authentication sequence.

Session Accounting Codes

If accounting codes are available in the user session of the printer, the @PrintByXerox app retrieves the codes and uses them for the jobs released using the app. For desktop jobs released to a Xerox printer, if you submit the job using a Xerox print driver, then the solution attempts to add or update the accounting codes to the job. Mobile jobs use the accounting codes from the session regardless of this setting always.

Using Accounting Codes for Desktop Jobs

To enable the use of accounting codes from user session for desktop jobs, do the following:

1. From the Web Portal, select the **Account** tab.
2. Select **Accounting > Accounting Prompts**.
3. In the **Session Accounting Codes** area, select the check box for **Use accounting codes from user session for desktop jobs**.
4. To save the setting, click **Save**.

ACCOUNTING: ADMINISTRATIVE DEFAULTS

Allowing the Welcome Page Printing When Accounting is Enabled

When accounting is enabled on a printer or server-based accounting is used, accounting information is required with each job in order to print. To print Welcome Pages when accounting is enabled, default accounting information must be set. Default accounting information can be saved for each form of accounting on a company basis. To set the defaults:

1. From the Web Portal, select the **Account** tab.
2. Select **Accounting**.
3. Select **Administrative Defaults**.
4. For your accounting mode, select the required Set Defaults:
 - **Xerox Network Accounting**
 - **Xerox Standard Accounting**
 - **Server-based Accounting (User name only)**
5. Enter the default information and select **Save**.

ACCOUNTING: JOB REPORTING



Note: Before you use the Job Reporting feature, ensure that you enable **Usage Tracking (Network Accounting)** on the printers. When Usage Tracking (Network Accounting) is enabled on a printer, the report data includes the printer Job Based Accounting (JBA) data.

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 administrator Web Portal, **Account > Accounting > Job Reporting**.
- The Job Reporting feature can be enabled or disabled.
- If you want to view the Dashboard tab and export job reports data in the Reports menu, enable the Export Data setting.

Reporting

- When the process runs, the Job Reporting report is updated with the latest information from the Cloud database and Printers that have Usage Tracking enabled.
- Printers that have Workplace Cloud Usage Tracking enabled successfully is queried for their current Network Accounting Records. For more information, refer to [Set Usage Tracking Mode](#).
- If the Network Accounting Records are successfully downloaded, they are purged from the Printer.

When a Printer has Usage Tracking enabled:

For printers that support Xerox Network Accounting:

- Network accounting is automatically turned on at the Printer with accounting prompts turned off.
- In some cases on older printer models the Network Accounting setting will have to be manually enabled.
- Workplace Cloud collects 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 is augmented with data from Workplace Cloud, such as user name and email address. User data is prioritized from Workplace Cloud. Print data is prioritized from the printer.
- Workplace Cloud jobs that does not 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 Workplace Cloud Authentication or third-party Authentication enabled, the job owner field in the report is set to unknown in the report for Copy, Scan, and Fax Jobs. There can be a job owner value for print jobs that depend 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 contains job history information for job data from the Workplace Cloud. The report contains the Workplace Cloud print job history for that printer. In some cases, if Usage tracking is not enabled on a printer, the report may contain data for job-owner, job-name, Color Printed, 2-sided Printed, Color Pages Printed, and black and white Pages Printed only. To obtain Best results, use the Xerox driver and office job types.
- The Job Reporting report contains missing or inconsistent data if the Network Accounting data of the printer is also being downloaded and purged from a third-party accounting package on the same printer.

About the Job Reporting Report:

To ensure that the most recent job information is included, Select **Account > Accounting > Job Reporting**, then click **Run Now**.

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 contains 2016-11-22 18:15:18.000, since the printer has a time zone of -05:00:00

For more information on Job Reporting report fields, refer to [Reports](#).

Enabling Job Reporting

When you enable Job Reporting, the export of reporting data for dashboards and for the .csv export is enabled.

When you enable Job Reporting, it allows the solution to create Dashboards. You can view the reporting data using the Web portal. Administrators can export the reporting data to a .csv file.

When you disable Job Reporting, the analytics feature is available, but the .csv export and the dashboards are not supported.

After you enable Job Reporting, reporting data is collected for jobs that are completed.

To enable Job Reporting, do the following:

1. Select **Account > Accounting > Job Reporting**.
2. To enable Job Reporting, select the check box for **Enabled**.

The Schedule section appears. For more information on scheduling, refer to [Schedule](#).

3. To save the configuration, click **Save**.

Schedule

Configure the frequency in which the Workplace Cloud Agent retrieves accounting data from all enabled printers.

- Disabled
- Hourly: Specify the hours between 1-23, the default interval is 12 Hours.
- Every Day
- On: Specify which day to run, At approximate time and Time Zone.
- Run Now

Refreshing the Dashboard Reports

To ensure that the most recent job information appears in the Dashboard and Job Reporting sections, refresh the dashboards regularly. To refresh the dashboards, do the following:



Note: The data retrieved from a scheduled or **Run Now** command can take up to 2 hours to appear in the Dashboard and the .csv export file. A background task runs every 2 hours and processes the reporting data.

1. Select **Account > Accounting > Job Reporting**.
2. To collect the data periodically, set the Schedule and time. You can configure the schedule with the option for either everyday or selective days in a week. You can also set the approximate time and Time Zone.
3. Click **Run Now**.

A report appears with the History of the Last Run and with the schedule for the Next Run.

4. To save the configuration, click **Save**.

Disabling Job Reporting

To disable Job Reporting, do the following:

1. Select **Account > Accounting > Job Reporting**.
2. To disable Job Reporting, deselect the check box for **Enabled**.

The Export Data and Schedule sections are hidden.

3. To save the configuration, click **Save**.

Account: Licensing

LICENSE OPTIONS

Licenses may be offered in varying quantities and configurations. Contact your authorized Xerox representative.

Licensing Options

LICENCE OPTIONS	JOB OR DEVICE PACKS TOKEN LIFETIME	PRINTER ESSENTIALS PACK	AZURE AD AUTHENTICATION: ANY LICENSE PACK	OKTA AUTHENTICATION
Windows Client for Workplace Cloud	24 hours	7 days	Use Azure Refresh token until the Refresh token is no longer valid	Use OKTA refresh token until the refresh token is no longer valid
Workplace App of Apple Devices using iOS	24 hours with option to store credentials on the device	7 days	Use Azure Refresh token until the Refresh token is no longer valid	

ACTIVATING XEROX® WORKPLACE CLOUD LICENSES

To enable Workplace Cloud licenses for use in the Xerox® Workplace Cloud environment, account administrators can activate multiple licenses on the Xerox® Workplace Cloud Web Portal using activation keys. Users can view various details for previously activated licenses, including the license status, activation date, expiration date, serial number, and key.



Note: To enable a device or service, the appropriate activation key and license information is required. For further information about licensing options and obtaining licenses, contact your Xerox® representative.

Workplace Cloud allows you to assign a license to a Country and only printers of that Country can use that licenses. Country licensing mode can support multinational installations of Workplace Cloud that require licenses to be purchased in the same country as the machines were purchased.

License Modes for License Activation

Workplace Cloud allows you to activate the licenses in the following modes:

- Global [Default]
- Country

License mode allows you to select a mode in which the licenses should operate for the company, you can choose any one of the following license modes and these modes can be changed after license activation.

Global [Default]: This is the default license mode. Use this mode when your company is not required to track licenses by Country. When selected, the licenses are not linked to any specific Country and the Country selection is not mandatory field.

Country: When Country Mode is selected, the licenses should be linked to their respective country of use. Use this mode if your printers are enabled and assigned to the sites of multiple Countries. The Printers assigned to the sites

use the respective Country licenses for enabling the printers.



Note: Before activating the license on Country mode, ensure that you have added all the required sites of the Countries, to manage sites refer to [Sites](#) section. The printers should be assigned to the same site as the license Country, to change site of the printer refer to [Change Site](#).

Global [Default] mode Guidelines

- When the license mode is **Global [Default]**, no Country restrictions apply to the license usage, enabled devices use all available licenses regardless of the license country.
- Use this mode if your printers are located in one country, or if accounting/financial tracking of enabled printers are not material to your cloud company.
- When the devices linked to the Country license expires, workplace cloud maps the devices to the available global licenses.
- You can switch to **Global [Default]** mode any time during the license period.
- You can change the **Global [Default]** license to a **Country** licence anytime during the license period.

Country Mode Guidelines

- When the license is in Country mode, Country restrictions are applied to the license utilization, enabled devices utilizes only the Country licenses based on the devices assigned sites country.
- Use this mode if your printers are located in more than one country and accounting/financial tracking of enabled printers is required for your cloud company.
- You can change the Country of the license anytime during the license period, changing the sites of an enabled printer should be done within the same country as the license country to utilize that Country license.
- You can change a Country license to a Global [Default] licence.
- If you choose Global [Default] as the Country for a licence, then the country mode restrictions does not apply to that license. The license can be applied to any device irrespective of the Country location.
- The devices are tied to the same country when the licenses expire.
- Workplace Cloud runs a License allocation task which assigns and aligns all existing devices to the respective country license if available and frees up currently used Global licenses which can be used if there is a lack of country licenses, you can do this manually by clicking **Run Now** option.

Activating License on Global [Default] Mode

To activate a Workplace Cloud license in **Global [Default]** mode:

1. On the Web Portal, click **Account > Licensing**.
2. In the New License section, under License Information enter the **Activation Key**.
3. To validate the license, click the right arrow button.
4. To validate additional licenses, repeat steps 3 and 4.
5. In the Country selection, select **Global [Default]**.

6. To activate all added licenses, click **Activate Now**.

A notification appears confirming that the licenses are activated and you can see the activated licenses in **License History > Active** section. Refer to [License History](#) for more information.



Note: To save the licenses for later user, refer to [Save License for Later Use](#).

Activating License on Country Mode

To activate a Workplace Cloud license in **Country** mode:



Note: Ensure that the sites linked to your devices are configured for the same country as your activated licenses. Failing to do so may disable the devices linked to another country when their current license expires.

Country License Activation Setting

- Ensure that you have created the Sites that you want to assign printers and licenses.
 - Ensure that the Printers are assigned to the Sites.
 - Ensure that the Licenses are assigned to the countries that are used in the Sites.
1. On the Web Portal, create the necessary Sites, refer to [Sites](#).
 2. Assign the printers to the required Sites, refer to [Change Site](#).
 3. Click **Account > Licensing**.
 4. In the License Mode section, select **Country**.
 5. In the New License section, under License Information enter the Activation Key.
 6. To validate the license, click the right arrow button.
 7. In the **Country** section, select the required Country from the dropdown list.
 8. To validate additional licenses, repeat steps 3 to 5.
 9. To activate all added licenses, click **Activate Now**.

A notification appears confirming that the licenses are activated and you can see the activated licenses in **License History > Active** section. Refer to [License History](#) for more information.



Note: To save the licenses for later user, refer to [Save License for Later Use](#).

Save License for Later Use

Workplace Cloud allows you to save multiple licenses on your Workplace Cloud company account to enable them for future use. You can set the activation date, clear activation date, delete and change the country of the saved licenses.

Guidelines

- The saved license does not have an expiration date until activated.
- You can set the activation date for the saved license to activate automatically on the assigned date.
- You can clear activation date, set new activation date and delete the saved licenses anytime before it is activated.

- You can change the country of the saved licenses.

Store License

To store the Workplace Cloud license to your Cloud company account do the following steps:

1. On the Web Portal, click **Account > Licensing**.
2. In the New License section, under License Information, enter the `Activation Key`.
3. To validate the license, click the right arrow button.
4. To validate additional licenses, repeat steps 3 and 4.
5. In the Country selection, select **Global [Default]** or the required Country for the licenses.
6. Click **Save for Later** and click on **Accept** on the license agreement page.

The licenses are saved and added to the **Available** section of the **History** tab, to activate or modify the imported license, refer to **Available** section.

Changing the License Mode after Activation

You can change the license mode from **Global [Default]** to **Country** mode or **Country** mode to **Global [Default]** mode any time after license activation or during the license period.

To change the Licence Mode for the Cloud Company account:

1. On the Web Portal, click **Account > Licensing**.
2. In the License Mode section, select **Global [Default]** or **Country** mode.

When **Country** mode is selected the existing enabled devices are validated and aligned to the active licenses in the company account.

3. Click **Close**.

The selected License Mode is applied to the Cloud Company account.

PURCHASING MORE PRINT JOBS OR MORE DEVICE LICENSES

To purchase additional licenses, contact your authorized Xerox® representative.

1. To add a new license, refer to **Activating Xerox® Workplace Cloud Licenses**.

For more information on how to acquire and purchase a license online, go to www.office.xerox.com/software-solutions/xerox-workplace-cloud/enus.html.



Note: You will receive an email notification 30 days prior to the expiration of your license, and every 9 days thereafter.

CHANGING A LICENSE TYPE



Important: Only the Account Administrator can change the license type.

1. Select **Account > Licensing** from the Web Portal.

2. Enter the Activation Key and Serial Number for the new license.



Note:

- If you are changing from a Job type license to a Printers type license, all unused jobs will be lost.
- When Printers type licenses are expired, cancelled or changed to Job type licenses, printers that were most recently enabled will be the first to be removed.

LICENSE HISTORY

The License History section displays the list of licenses that are activated or applied to the current Xerox® Workplace Cloud company account. The licensing view has the following tabs:

- Active
- Available
- Expired

Active

This tab displays the list of currently active licenses for the Xerox® Workplace Cloud company account, with the newest at the top. By default, the view is Active. If there are no active licenses, the Web portal displays **No Active Licenses** in place of the list of active licenses.

Viewing the Active License Information

To view the Active Licence Information:

1. On the Web Portal, click **Account > Licensing**.
2. In the License History section under **Active** tab you can see the list of licenses and you can see the following details:
 - Item
 - Status of the license
 - Country of the license
 - Count section provides the total no of devices that can be enabled using the license



Note: Count section in Country mode shows number of license available in that Country.

- Used section provides the total no of devices enabled using the license



Note: Used section in Country mode shows number of printers in that country that are using the license.

- Activation date
- Expiration date
- Serial number
- Key

License Information available in Country Mode

This license information provides the details of the printers enabled on each Country license, you can click on the license and view the following information:

- Printer Friendly Name
- IP Address of the Printer
- Associated Site
- Printer associated Country

Changing the Country of the Active License



Note:

- When in **Global [Default]** or **Country** license mode you can change the country of the license anytime during the license period, before you change the country of a license ensure that the device associated to the sites are assigned to the new country which is being selected.

To change a Workplace Cloud license Country:

1. On the Web Portal, click **Account > Licensing**.
2. In the License History section, select the **Active** tab, select the required license, click **Actions > Change Country**.

A dialogue box appears with the confirmation message, click **Confirm**, a **Select Country** dialogue box appears.

3. If you need to change the **Country** license to a **Global [Default]** license, select the **Global [Default]** from the list and click **OK**.

The Country license is changed to a Global [Default] license.

4. If you need to change or assign a **Country** to a license, select the required **Country** from the list and click **OK**.

The selected license is assigned to a new Country.

Delete the Active License

To delete the **Active** license do the following:

1. On the Web Portal, click **Account > Licensing**.
2. In License History section, under **Active** tab, you can see the list of active licenses.
3. Select the required license.
4. Click **Actions > Delete**.

The selected license is deleted from the **Active** tab.

Available

This tab displays the list of licenses that are imported and saved for later use for the Xerox® Workplace Cloud company account. If there are no Available licenses, the Web portal displays **No Available Licenses** in place of the list of available licenses.

Viewing the Available License Information

To view the Available Licence Information:

1. On the Web Portal, click **Account > Licensing**.
2. In the License History , section under **Available** tab you can see the list of available licenses and you can see the following details:

- Item
- Count section provides the total no of devices that can be enabled using the license



Note: Count section in Country mode shows number of license available in that Country.

- Status
- Country of the license
- Activation date



Note: The activation date is the date in which the licence would be automatically activated for the imported licenses. It can be set using **Set Activation Date** option.

Activate Imported Licence

To activate the imported licence:

1. On the Web Portal, click **Account > Licensing**.
2. In License History section, select **Available** tab, you can see the list of available licenses.
3. Select the required licence from the list, click **Actions > Activate**.

The selected license is activated to your Workplace Cloud company account, and the licence is moved from **Available** to **Active** tab.

Set Activation Date

You can set the activation date for the available licences which can be automatically activated on defined date, to set the activation date:

1. On the Web Portal, click **Account > Licensing**.
2. In the License History section, select the **Available** tab, select the required license, click **Actions > Set Activation Date**.

A Set Activation Date dialogue box appears.

3. Select the required activation date for the license and click **OK**.

The licence activation date is set to the available licence and the status is set to Scheduled.

Clear Activation Date



Note: Clearing the activation date of available license prevents the licence from activating on the defined date.

To clear the available licence activation date:

1. On the Web Portal, click **Account > Licensing**.

2. In the License History section, select the **Available** tab, select the required license, click **Actions > Clear Activation Date..**

The activation date is cleared for the selected license and the status is set to Pending.

Changing the Country of Available License

To change a Workplace Cloud license Country of available licence:

1. On the Web Portal, click **Account > Licensing**.
2. In the License History section, select the **Available** tab, select the required license, click **Actions > Change Country**.

A dialogue box appears with the confirmation message, click **Confirm**, a **Select Country** dialogue box appears.

3. If you need to change the **Country** license to a **Global [Default]** license, select the **Global [Default]** from the list and click **OK**.

The Country license is changed to a Global [Default] license.

4. If you need to change or assign a **Country** to a license, select the required **Country** from the list and click **OK**.

The selected license is assigned to a new Country.

Delete the Available License

To delete the **Available** license do the following:

1. On the Web Portal, click **Account > Licensing**.
2. In License History section, under **Available** tab, you can see the list of available licenses.
3. Select the required license.
4. Click **Actions > Delete**.

The selected license is deleted from the **Available** tab.

Expired

This tab displays the list of expired licenses for the Xerox® Workplace Cloud company account, with the newest at the top. If there are no expired licenses, the Web portal displays **No Expired Licenses** in place of the list of expired licenses.

Viewing the Expired License Information

To view the expired licence information:

1. On the Web Portal, click **Account > Licensing**.

2. In the License History section, select **Expired** tab you can see the list of expired licenses and you can see the following details:

- Item
- Status of the license
- Country of the license
- Count section provides the total no of devices that can be enabled using the license



Note: Count section in Country mode shows number of license available in that Country.

- Used section provides the total no of devices enabled using the license



Note: Used section in Country mode shows number of printers in that country that are using the license.

- Activation date
- Expiration date
- Serial number
- Key

License Expiration

Activated Workplace Cloud licenses have an expiration date, and when they expire, printers will be disabled automatically.

License Expiration Notification

The license expiration notification email will be sent to you in the order listed below:

- 30 days before expiration
- 7 days before expiration
- On the day of expiration.

For an expiring **Global [Default]** license you need to purchase a new license.

For an expiring **Country** license, do the following action when the license expires:

1. Click **Account > Licensing**.
2. In the License Mode, under **Country** section, click on **Run Now** to re-validate the enabled devices and licenses.
3. The 'Run Now' button will validate all the devices and available licenses. If there is a combination of **Global [Default]** licenses and **Country** licenses, it will reassign the devices with the preference to a **Country** license and then to a **Global [Default]** license if available.



Note: This task can be manually run by clicking on the **Run Now** button or will run daily at 12 midnight.

If you don't have enough licenses to enable your devices purchase a new license.

Delete the Expired License

To delete the **Expired** license do the following:

1. On the Web Portal, click **Account > Licensing**.

2. In License History section, under **Expired** tab, you can see the list of expired licenses.
3. Select the required license.
4. Click **Actions > Delete**.

The selected license is deleted from the **Expired** tab.

Reports

This chapter contains:

- Dashboard..... 260
- Job Reporting..... 262
- User Audit 269
- User Activity 270

Dashboard

The Xerox® Workplace Cloud job reporting dashboard provides predefined summary information for customers who use the reporting capability of Workplace Cloud. The **Dashboard** of the **Reports** tab provides the following reports:

- **Print Summary**
- **Cost Savings**
- **Paper Summary**
- **Most Used Printers**
- **Least Used Printers**
- **Top Users**
- **Top Departments**

The Dashboard menus include the following options:

- **Dashboard Report:** This menu allows you to select different Dashboards.
- **Time Period:** This menu allows you to select the time period for the data reported. Options include **Monthly**, **Quarterly**, and **Yearly**.
- **Job Type:** This menu allows you to select the source of the job data.
 - **All Network Accounting Jobs:** This option shows the data only for the jobs collected through Network Accounting, on the Dashboard.
 - **All Marked Jobs:** This option shows the data from printers that have the Workplace Cloud Usage Tracking (Network Accounting) feature and the Home Worker Print Tracker feature enabled. Additionally, the report shows data from Workplace Cloud jobs. The job data includes data from any page marked by the printer.
 - **All Home Worker Print Tracker Jobs:** This option shows the data from Workplace Cloud when the Home Worker Print Tracker feature is enabled.
- **Modify Cost:** This option allows you to configure the cost parameters of a printed page for Dashboard reports.



Note: Before you can use the Dashboard, enable the **Job Reporting** feature of Workplace Cloud. The Job Reporting feature is available with the Printer Essentials Bundle license.

SUMMARY OF THE DASHBOARD REPORTS

- **Print 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 Cloud 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 computes an estimated cost savings on jobs not printed.

- This report applies to Workplace Cloud jobs. It does not include jobs submitted outside of this solution such as copies and emails.
- The 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 system includes an Estimated Jobs savings.
- **Paper Summary:** This Dashboard report provides details on the number of 1-sided and 2-sided jobs that were printed during the specified time. A graph appears that shows the ratios for the percentage of Simplex and Duplex jobs printed.
- **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. The report consolidates the top departments in terms of printed pages where the cloud groups all the jobs for particular department. To obtain results for this dashboard report, users are assigned to a Department. To assign users to a Department, select the **Users** tab, select a user, then add a value to the Department field.

MODIFYING ESTIMATED COST

Use the **Modify Cost** feature to configure the estimated cost of a printed page. You can set the following Cost parameters individually:

- **Currency Symbol:** The symbols of the country currency, such as Dollar, Euro, British Pounds, and Japanese Yen.
- **Sheet Cost:** Hardware and Paper Cost
- **Marking Cost:** Black and White, and Color images
- **Estimated Default Cost:** Estimated Jobs relates to a full print job, and not printed sheets.

Job Reporting

VIEWING JOB REPORTING DATA

To view job reporting data, do the following:

1. Click **Reports > Job Reporting**.
2. Select the **View** tab.
3. 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**

EXPORTING JOB REPORTING DATA



Note: Before you can use the export option, enable the **Job Reporting** feature of Workplace Cloud. The Job Reporting feature is available with the Printer Essentials Bundle license. For more information, refer to [Enabling Job Reporting](#).

To export job reporting data, do the following:

1. Click **Reports > Job Reporting**.
2. Click **Export**.
3. In the Initiate Export Request section, do the following:
 - a. From the Period menu, select one of the following predefined options:
 - **Today**
 - **Current Month**
 - **Last Month**
 - **Data Range**
 - b. Click **Initiate Export**.
4. In the History section, for the status of the job export, click the refresh icon.
5. After the status of the export is changed from **Processing** to **Completed**, click the .csv file.
The .csv file is downloaded to your computer.

SCHEDULE THE EMAIL DELIVERY OF JOB REPORTING DATA EXPORT



Note: This setting is disabled by default.

Schedule tab allows you to schedule the auto export and delivery of your Job Reporting data to your email addresses. Job reporting data can be mailed to you weekly or monthly using this setting.



Note: If the auto Job Reporting data export fails, you will receive the Failure notification email. Do the manual export of the data and wait for the next scheduled run.

To configure scheduled Job reporting export and email do the following:

1. Click **Reports > Job Reporting > Schedule** tab.

2. Select the check box of **Enable**.

The Schedule settings appears.

3. Select the email recurrence interval as **Weekly** or **Monthly**.



Note:

- If the job reporting export data email recurrence interval is selected as weekly, then the report would fetch the data from previous Sunday 00:00 hours to Saturday 24:00 hours. Similarly, if you choose monthly, then the report would fetch the data from first day of previous month to last day of that month.
- If you select **Weekly**, the report will be emailed every Sunday, if you select **Monthly**, the report will be emailed first day of every month.

4. Select the time and the time zone in which you wish to get the report generated and emailed.

5. On the Email Settings section, enter the required email addresses separated by comma.

6. Enter the Subject line and required message of the Job Reporting Export data email.

7. Click **Save**.

Your Changes have been saved message appears.

JOB REPORTING REPORT FIELD DESCRIPTIONS


Descriptions of the Job Reporting fields are in the following table:

NAME	DESCRIPTION	SOURCE OF INFORMATION: PRIMARY OR SECONDARY SOURCE
Company	Name of the company account	Cloud
job-owner-domain	Used for the association of job data with the network login name. If Job Based Accounting (JBA) is not enabled, use the value from the database. If JBA is enabled, use the supplied value.	Printer or Cloud
accounting-information-avp	Used for the association of validation field names with log data entries. If JBA is not enabled, use Null. If JBA is enabled, use double-quote-enclosed,	Printer

NAME	DESCRIPTION	SOURCE OF INFORMATION: PRIMARY OR SECONDARY SOURCE
	comma-separated UTF-8 name and value pairs.	
Billing Code	The value in JBA accounting-information-avp (XRX_ACCTID) takes precedence. If both JBA and DB are blank or not populated, the value is Null.	Printer or Cloud
device-name	Used to identify uniquely a printer from other printers.	Printer or Cloud
Printer IP	The Printer IP address that the job was submitted to.	Cloud
Serial Number	The serial number of the printer.	Cloud
Manufacturer	Manufacturer name of the printer.	Cloud
Model	Name of the printer model.	Cloud
Site	Name of the site that the printer is assigned to.	Cloud
Country	Name of the country where the printer is located.	Cloud
job-type	Specifies the type of job recorded. Each job has only one type. Supported Values: Delayed Print, Print, Report, Secure Print, Print Files	Printer or Cloud
job-type-detail	Provides job-type details designed to supplement the regular job-type attribute.	Printer
Job source	Identifies the source of the job. The value is <code>Workplace Cloud</code> . If the Home Worker Print Tracker feature is enabled, the value is <code>Home Worker Print Tracker</code> . For the jobs that are processed by the printer outside of the Workplace cloud solution, the value is <code>Other</code> .	Cloud
system-job-type	Identifies the system job type for the job log entry in which it appears.	Printer
job-identifier	The TCP/IP host name or string <code>job</code> concatenated with a unique printer number.	Printer
system-job-identifier	The string <code>job</code> concatenated with a unique printer number.	Printer
Report ID	Solution unique ID. Maps the job details to the internal data element to debug.	Cloud
job-name	The alphanumeric name of the job assigned by the user. If the name is not supplied by user, the name defaults to <code>Print</code> . The job identifier can be concatenated to any system-generated default job type. The job name can be the file name of the submitted job.	Printer or Cloud

NAME	DESCRIPTION	SOURCE OF INFORMATION: PRIMARY OR SECONDARY SOURCE
Server Received Time UTC	UTC time when a job was submitted to the system. Only applies to Print Management or Mobile Printing jobs.	Cloud
Transferred To Printer Time UTC	UTC time when a print job completely transferred to a printer. Only applies to Print Management or Mobile Printing jobs.	Cloud
printer-completion-time UTC	UTC time when a print job completes at the printer, such as printing, filing, emailing. Only applies to jobs tracked using JBA.	Printer
printer-completion-time	Time when a print job completes at the printer, such as printing, filing, emailing. Only applies to jobs tracked using JBA.	Printer
Completion Time UTC	UTC time when a print job completes at the printer, such as printing, filing, emailing. Only applies to jobs tracked using JBA.	Cloud
Job Status	Indicates the final status, success, or failure, of a job.	Cloud
JBA-completed-reasons	The final state of a job.	Printer
job-copies-completed	The number of sets of a job that were produced. For example, a 4-page document with 3 copies completed means that 3 sets of 4 pages each were produced.	Printer or Cloud
Color Printed	Indicates if a job had one or more color pages.	Cloud
finishing-staple	If JBA is enabled, indicates if the job used stapling. If JBA is disabled, this setting applies only to Print Management or Mobile Printing jobs, and indicates whether stapling was requested.	Printer or Cloud
finishing-punch	If JBA is enabled, indicates if the job used hole punching. If JBA is disabled, this setting always indicates No.	Printer or Cloud
finishing-fold	If JBA is enabled, indicates if the job was folded. If JBA is disabled, then this setting always indicates No.	Printer or Cloud
Duplex Printed	If JBA is enabled, indicates if the job resulted in one or more 2-sided pages. If JBA is disabled, this setting indicates if 2-sided was requested.	Printer
Color Pages Printed	The total number of color pages printed or total color images produced for a job. If JBA is disabled, this number indicates the total pages of a Print Management or Mobile Printing Job that were requested to print in color. It does not mean that all pages actually print using color.	Printer
Black And White	The total number of black and white pages printed or total black and white	Cloud

NAME	DESCRIPTION	SOURCE OF INFORMATION: PRIMARY OR SECONDARY SOURCE
Pages Printed	images produced for a job. If JBA is disabled, this number indicates the total pages of a Print Management or Mobile Printing Job that were requested to print in black and white.	
media-type	The type of paper used when you print a job. If JBA is disabled, this value is null. The supported values are printer-dependent and are not part of a fixed set.	Printer
media-color	The color of the paper used when you print a job. If JBA is disabled, this value is null. The supported values are printer-dependant and are not part of a fixed set.	Printer
media-size	Media size using well-known names, if available. If mapping the size to a name does not exist, the value of <code>Unknown</code> is returned.	Printer
media-size-in-mm	Media size in millimeters.	Printer
media-sheets-produced	The total number of sheets of media printed, such as paper, transparency, and so on. If JBA is not enabled, null is returned.	Printer
media-tiers	The number of media tiers for the given job. If tiered billing is not supported, or if JBA is not enabled, the value is null.	Printer
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, null is returned.	Printer
media-color-pages	The number of media sides to which color impressions are applied for the given media block. If JBA is disabled, null is returned.	Printer
number-of-images	Total count of impressions. The total includes banner pages and error pages, but only sheets that are printed, and not blank sheets.	Printer
media-other-pages	Sheet count for all new media types encountered after the first six media types. If JBA is disabled, null is used.	Printer
total-simplex-sheets	Total number of 1-sided sheets output by job content. The total includes banner pages and cover pages, and 1-sided imaged cover pages. Sheets that are printed on one side or that are blank on both sides are counted as 1-sided sheets.	Printer
total-duplex-sheets	Total number of 2-sided sheets output by job content including banner pages and cover pages. If a sheet is printed on both sides, it is counted as a duplex sheet.	Printer

NAME	DESCRIPTION	SOURCE OF INFORMATION: PRIMARY OR SECONDARY SOURCE
	 Note: Some 1-sided to 2-sided jobs contain both 2-sided and 1-sided output sheets.	
image-size	Image size using well known names, if available. If mapping of the size to a name does not exist, the value of Unknown is returned.	Printer
media-tier-1-count	The number of impressions at tier level 1. If tiered billing is disabled, or if JBA is disabled, the value is null.	Printer
media-tier-2-coXunt	The number of impressions at tier level 2. If tiered billing is disabled, or if JBA is disabled, the value is null.	Printer
media-tier-3-count	The number of impressions at tier level 3. If tiered billing is disabled, or if JBA is disabled, the value is null.	Printer
image-size-in-mm	Describes the size of the image that is scanned	Printer
image-other-size	The count of images scanned after the first three images	Printer
images-sheets-produced	The number of image sheets that were scanned	Printer
black-and-white-images	The number of black-and-white image sides that were scanned	Printer
color-images	The number of color image sides that were scanned	Printer
image-other-size	The count of image blocks scanned after the first three image blocks	Printer
total-network-destinations	The total number of scan destinations to which documents were scanned and filed, up to a maximum of six destinations.	Printer
total-scan-pages-delivered	The total number of pages scanned to all scan destinations	Printer
scan-other-pages	The total count of all impression sides sent to all new document paths after the first six documents.	Printer
total-number-of-images-filed	The total count of the number of images scanned and filed to files servers. Counts the 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. Only scanned images that are successfully filed are counted. If an image is filed to at least one file server, it is counted once. Image totals are computed as follows: number of network destinations times the number of images.	Printer

NAME	DESCRIPTION	SOURCE OF INFORMATION: PRIMARY OR SECONDARY SOURCE
number-of-phone-numbers	The total number of destination phone numbers used in the job	Printer
total-number-of-smtp-recipients	Contains the total number of all to, cc and bcc attributes in a scan to email job	Printer
fax-images-completed	The total number of fax images completed for a single job, which can be multiple fax calls	Printer
fax-success-calls	The total number of fax calls successfully completed for a single job	Printer
fax-failed-calls	The total number of failed fax calls for a single job	Printer
Department	The department is associated with a given user. The department is a database field in the user record. This field can be blank.	Cloud
Content Security Status	If content security is enabled for the account, this field contains: <code>Unknown</code> , <code>Match</code> , or <code>No Match</code> . If content security is not enabled, this column does not exist.	Cloud
Found Search Strings	If content security is enabled for the account and the value in the status column is <code>Match</code> , this field contains a semicolon-separated list of the content security search string values found in the document. If content security is enabled and the status column is <code>Unknown</code> or <code>No Match</code> , this column is blank. If content security is not enabled, this column does not exist.	Cloud

User Audit

1. Select **Reports > User Audit**.
2. Optionally, to refine your displayed data in the User Audit table, enter a search term.
3. Select **Export This Page** from the Actions menu.

The Save As window displays.



Note: To export all data in the table, select **Export All Pages** from the Actions menu.

4. Navigate to where you want to save the report, then click **Save**.



Note: The default filename for the report is XeroxCloudPrintUserAuditHistory.Workplace.Cloud.csv.

The **Actions** menu provides a list of tasks that you can perform:

- **Export This Page**
- **Export All Pages**

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

The **Users Per Page** indicator enables you to set the number of email addresses that are displayed per page.

The **Search** field enables you to quickly find specific email addresses in long lists.



Note: User Audit tracks Web portal Login, Client Login, Mobile App Login, Web Portal New User Registration and Alternate login with credentials.

User Activity

User Activity records and displays the activities performed by the user or administrator on the Workplace Cloud company account:

Data recorded in the User Activity are:

- Email
- Event type
- Result
- Date

User Activity tracks and update the status of print authentication, new card registrations, custom email onboarding message, scheduled job reporting export and license activation.

EXPORT USER ACTIVITY

To Export the User Activity:

1. Select **Reports > User Activity**.
2. Optionally, to refine your displayed data in the User Audit table, enter a search term.
3. Select **Export This Page** from the Actions menu.

The Save As window displays.



Note: To export all data in the table, select **Export All Pages** from the Actions menu.

4. Navigate to where you want to save the report, then click **Save**.



Note: The default filename for the report is XeroxCloudPrintUserActivity.Company NameHistory.Workplace.Cloud.csv.

The **Actions** menu provides a list of tasks that you can perform:

- **Export This Page**
- **Export All Pages**

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

The **Users Per Page** indicator enables you to set the number of email addresses that are displayed per page.

The **Search** field enables you to quickly find specific email addresses in long lists.

Troubleshooting

This chapter contains:

- Software Installation Issue (Unable to Install Program that is blocked by Windows)..... 272
- Account Issues 273
- Agent Issues 276
- Printer Issues..... 280
- Authentication Issues 291
- iOS Native Printing Issues..... 292

Software Installation Issue (Unable to Install Program that is blocked by Windows)

Issue: The file that you have downloaded from Workplace Cloud Web Portal can have the attribute defined as blocked. This can prevent the file from being installed and deployed.

The .zip file you have downloaded may have a setting that prevents it from being deployed and installed. It is recommended that you unblock the zip file because the EXE and DLL files inside the zip inherit the blocked setting.



Note: It is not necessary to extract the downloaded files and do the Unblock action on all the EXE and DLL files.

Make sure before you deploy the MSI file, the **Security: Unblock** property is checked.

Unblock the File

To check and Unblock the file:

1. Select the MSI file or the ZIP file that you downloaded.
2. **Right Click** on the file and select **Properties** from the menu.
3. From the **General** Tab, on the bottom in the Attributes section, make sure that the **Security: Unblock** setting is checked.
4. If the **Security: Unblock** is not checked, select the check box and click **OK**.

This issue can occur to the Cloud Agent, Windows Print Client and any other downloaded files.

Account Issues

USER CANNOT PRINT TO COMPANY PRIVATE PRINTERS

1. Go to **Account > Policies > Access Controls > Allowed Users** and check the selection for Allowed Users list for private printers.
 - When **Apply To Guested Users Only** is the selected access control setting for private printers, the user must either be logged in with your company code or be on the Allowed Users list for private printers.
 - When **Apply To All Users** is the selected access control setting for private printers, the user must be on the Allowed Users list. Users whose email address or domain is not on this list do not have access to private printers, even if they log in with the correct company code.
2. Go to **Account > Policies > Access Controls > Blocked Users** and check the Blocked Users list. A user whose email address or domain is on this list for private and public printers has no access to your company's printers.

If a user's email address or domain is on both the Allowed Users list and the Blocked Users list, the Blocked Users listing will override. For example, if a user email address is in the Allowed Users list, but their domain is in the Blocked Users list, the user will not be able to print to your company's printers.

USER CANNOT PRINT TO COMPANY PRINTERS

1. Go to **Account > Policies > Access Controls > Blocked Users** and check the Blocked Users list. Make sure that the user's email address or domain is not on the Blocked Users list. A user whose email address or domain is on this list for private and public printers has no access to your company's printers.
2. Go to **Account > Policies > Access Controls > Allowed Users** and check the selection for Allowed Users list for private printers.
 - When **Apply To Guested Users Only** is the selected access control setting for private printers, the user must either be logged in with your company code or be on the Allowed Users list for private printers.
 - When **Apply To All Users** is the selected access control setting for private printers, the user must be on the Allowed Users list. Users whose email address or domain is not on this list do not have access to private printers, even if they log in with the correct company code.

If a user's email address or domain is on both the Allowed Users list and the Blocked Users list, the Blocked Users listing will override. For example, if a user email address is in the Allowed Users list, but their domain is in the Blocked Users list, the user will not be able to print to your company's printers.

UNWANTED OR UNAUTHORIZED USERS PRINT TO COMPANY PRINTERS

A user that does not have a Xerox® Workplace Cloud account may still print to a public or private printer that has Anonymous Direct Email Printing enabled, even if the user's email address or domain are not on the Allowed Users list, as long as the following are true:

- The user's email address or domain are not on the Blocked Users list
- The user has the printer's email address

PROMPTED TO CREATE NEW ACCOUNT WHEN YOUR ACCOUNT ALREADY EXISTS

Make sure the email address was entered correctly.

The system automatically begins a new account creation process. When a prompt appears requesting you to enter a company code, click **Cancel** to return to the login screen and enter your correct email address.

COMMUNICATION ERROR WHEN USING A WIRELESS ADAPTER ON A VERSALINK PRODUCT

On a VersaLink product, you can add a wireless adapter. Both the wired Ethernet and the Wireless interface can run at the same time (this is different than Connect Key and AltaLink where only one interface can be enabled at a time). In addition to running concurrently, you can also select which interface is the Primary one from the LUI.

Web Service calls only work on the Primary interface.

WHY WOULD A COMPANY CODE NEED TO BE RESET?

When you create a company account, you distribute the Company Code to the users that you designate as authorized to use the account. When you remove users, change the company code to ensure that removed users cannot continue to access the account.

USER TYPE IS BLANK ON THE USERS PAGE

When users do not complete the end user account registration process, they show up in the list of users with the **Type** column blank on the **Users** page.

USER LIST IS NOT UPDATED WHEN AN ACCOUNT ADMINISTRATOR REMOVES A USER FROM A COMPANY ACCOUNT

User functionality is not updated while users remain logged in. Users will continue to have connectivity and the ability to print for 24 hours or until they log out (whichever occurs first).



Note: A login attempt after logging out will fail if the user has been removed from the Company Account.

USER ACCESS RIGHTS NOT UPDATED

When an administrator removes a user from a company account or changes permissions for that user, the changes will not take effect until the user logs out and logs back in again.

ACCOUNT SETTINGS ARE NOT BEING SAVED

Make sure you select **Save**, **Accept**, or **OK** before navigating away from a page after you have made changes. Changes will not take effect until the user logs out and logs back in again.

WINDOWS MESSAGES DISPLAY IN MIXED LANGUAGES

In some cases, if the installer, operating system, and browser language do not match, Windows messages may display in mixed languages. To alleviate this issue, install the Agent software in the same language as the PC operating system.

MESSAGES DISPLAY WITH QUESTION MARKS OR NONRECOGNIZABLE CHARACTERS

Do one of the following:

- Load the operating system language pack in the same language that was used to install the Xerox® Workplace Cloud software.
- Reinstall the Agent software in the same language as the PC operating system.

Agent Issues

AGENT COMMUNICATION ISSUES

1. Check that the agent is still communicating with the server by verifying that the last communication date on the **Agents** tab on the Web Portal is within the last 24 hours.
2. Check the proxy settings of the agent in the configuration tab and ensure that the proxy is configured properly to communicate with the internet from within your network location.
3. Check your PC services menu to be sure that the Xerox® Workplace Cloud Agent Services is started. The Agent must be running on your PC at all times for Xerox® Workplace Cloud to work.
4. If the agent is still not communicating with the server, restart the machine running the agent. Run a device search once the machine comes back on-line and verify that there is no communication error on the UI of the agent.
5. If the agent is still not communicating with the server after all these steps have been taken, please **reinstall the agent**:
 - a. At the Agent PC, uninstall the current agent software.
 - b. From the webpage **Agents** tab, select **Download the Xerox Workplace Cloud Agent Installer**.
 - c. Install and register the agent.
 - d. Retry a print submission to the device.

AGENT ICON NOT IN SYSTEM TRAY

If the icon is not present in the Agent PC system tray, manually start the agent user interface from the **Start** menu. The icon in the system tray is a shortcut to the user interface; it does not indicate whether or not the Agent service is running.

RECEIVED A PRINT AGENT NOT RESPONDING MESSAGE

Verify that the PC where each agent is installed is powered on and has internet access. Also, verify that the proxy settings within each print agent are correct.

A routine discovery is run every 7 hours to update information about the printers supported by an agent. The administrator receives a Print Agent not responding message if there is no communication with the agent for 5 days.

UNABLE TO INSTALL OR REGISTER AGENT SOFTWARE

If you receive an error message when registering the agent, it may be that your email address is not associated with the company the agent is set up for. You must be currently logged into that company account, or your last login to Xerox® Workplace Cloud must have been to that company.

UNABLE TO UPGRADE OR UNINSTALL THE AGENT

If you receive persistent errors when attempting to upgrade or uninstall the agent software, cancel the agent installation process and manually shut down the agent service. In the Services window in the Windows operating system, stop the Xerox® Workplace Cloud Agent Service (XeroxMobilityServiceAgent.exe). Begin the agent installation process again. Refer to [Setting Up a New Agent](#).

If you receive a Windows Installer Error, **Error opening installation log file. Verify that the specified location exists and is writable**, refer to the Microsoft Support knowledge base at, <http://support.microsoft.com/kb/2564571> for more information.

AGENT DOES NOT UPGRADE AUTOMATICALLY

If the agent software indicates it is eligible for auto-upgrade (auto-upgrade is enabled), but the yellow icon persists, you must manually upgrade the agent software.



Note: Agent software version 2.2 (and newer) supports auto-upgrade. Older agent software must be manually upgraded to the new version before it is capable of auto-upgrade.

PRINTER SEARCH STATUS SHOWS “UNABLE TO COMMUNICATE WITH AGENT”

In the **Agents** tab, an agent status displaying "Unable to Communicate" indicates that there was a communication issue when the Cloud attempted to contact the agent. Check the agent PC connectivity and ensure that the agent software is running:

1. Validate that the agent PC is connected to the Internet.
2. Manually restart the agent service. In the Services window in the Windows operating system, restart the Xerox® Print Workplace Cloud Agent Service (XeroxMobilityServiceAgent.exe).

Once restarted, the agent should regain communication.

RECEIVED A PRINT AGENT IS NOT INSTALLED FOR THIS PRINTER MESSAGE

There is a communications problem between the agent and the device.

1. Check the last communications date for the device. Correct the configuration to fix the communication of the existing agent, rather than installing a new replacement agent as it may have the same communications problem.
2. SNMP can stop working on a device. The symptoms are that either the device is not discovered initially, or that it is discovered, but at some point printing to the device fails and a message states that there is no agent for that device. Make sure the Xerox® Workplace Cloud Agent Service is running:
 - a. Reboot the device.
 - b. Log into the Agent PC.
 - c. Start the Xerox® Workplace Cloud Agent Service.
 - d. Reinitiate a discovery on the device.
3. The agent is not communicating with Xerox® Workplace Cloud. Check the proxy settings.

4. If you changed your SNMP Community Name to be something other than **public**, a setting must be added for that SNMP Community Name in **Agents > Edit > SNMP Settings**.
5. If you make changes to the hard drive on the PC that has the agent, you will need to register the agent again.

XEROX® WORKPLACE CLOUD AGENT SHOWS AS NOT CONNECTED ON AGENT PC

Do the following to reconnect the Xerox® Workplace Cloud Agent:

1. Verify the Agent PC is connected to the Internet.
2. Manually restart the Agent service.
3. In the Control Panel for the Windows operating system, navigate to **Administrative Tools** and select **Services**.
4. Select **Xerox Workplace Cloud** and restart the service.

Once the service is restarted, the Agent should reconnect and regain communication.

PRINT AGENT INSTALLATION FAILED

One of the following may be the issue:

- Connectivity issue (proxy setting or other)
- Unsupported operating system
- The PC does not meet minimum system requirements
- Try performing the installation in two steps: download and save the agent installer, and then run the installer from the PC

DISCOVERY ON A SUBNET RANGE TAKES TOO LONG

If scan settings are left blank, all the local subnets for the Agent PC will be scanned. It may be more efficient to split discovery ranges across multiple agents. This scan takes several minutes.

Do the following to manually identify a subnet range for scan settings when setting up an agent.

1. Select the **Agents** tab.
2. Select **New** for the **Actions** menu.
3. Enter a friendly name for the new Print Agent and click **Next**.
4. Select your site and click **Next**.
5. Select **Add Setting**.
6. Select the **IPv4 Range** search type.
7. Enter a start and end address and click **Save**.
8. Click **Next**, verify that the settings are correct, and click **Next** again.
9. Select **Download the Xerox Workplace Cloud Agent Installer**.
10. Select a language.
11. Follow the agent setup wizard.

PRINTER IS NOT DISCOVERED BY AGENT

- It could be a connectivity problem. The printer's IP address may have changed or it may no longer have network connectivity. Make sure you can ping the printer.
- Make sure your discovery criteria is correct. The printer's IP address or Domain Name System (DNS) name must be in the Discovery Settings range, and not in the Exclusions range. If you have changed the printer Simple Network Management Protocol (SNMP) Community Name, it must be listed in the agent SNMP Settings.
- The Agent must have a static IP Address in accounts that will be using Xerox® Workplace Cloud Cardless or Card based Authentication.

WHAT LAST DISCOVERED MEANS

This is the last time that an agent was able to communicate with that printer. This time should not exceed 7 hours for printers that are powered on continuously. If it has been longer than 7 hours, make sure the agent is powered on and connected and the printer is connected to the network. You can also select **Printer Search** to manually discover a printer.

PRINTERS ARE NOT DISCOVERED AFTER PRINTER SEARCH WAS INITIATED ON THE WEB PORTAL

If a printer search for a particular agent was initiated on the Web Portal and the printers do not appear under the **Enabled** tab as Discovered:

1. Check the agent to be sure it is powered on and connected to the internet.
2. Verify that the IP address of the printer is in the scan settings list of the agent that services the printer's print jobs. If the IP address is not in the scan settings list:
 - a. Add the IP address to the list.
 - b. Run a device search on the agent.
 - c. Verify that the last communication date is updated on the printer.
 - d. Check that the printer is listed under the **Enabled** tab of the Web Portal.
3. Attempt to print again.

UNABLE TO DELETE A SITE

You cannot delete the site that you set up when you created the account. You can rename a site and change the coordinates.

Printer Issues

PRINTING ISSUES

If you encounter printing issues, check the following:

Network

Check the network.

Job

1. Make sure the job did not already print. By default, jobs are deleted after printing.
2. The filename may contain unsupported characters.
3. If you received an Aborted status email for your job, this usually means that there is a problem in the print path. Check the print path.
4. The document may contain unsupported fonts or unsupported language. Refer to .

File Type

Make sure the document you printed is a supported file type: doc, docm, docx, xls, xlsx, xlsx, xlsx, png, ppt, pptx, pptm, pdf, txt, rtf, tif, tiff, jpg, gif, jpeg, zip, or eml. Adobe Portfolio files are not supported.



Note: Zip files are a supported file type, but they may contain file types that are not supported. Supported file types in a zip file will print even if the zip file also contains unsupported file types.

Agent

1. Check your PC services menu to be sure that the **Xerox Workplace Cloud Agent Services** is started. The Agent must be running on your PC at all times for Xerox® Workplace Cloud to work.



Note: On the agent, an icon with a printer and a triangle with an exclamation mark displays when a printer was discovered within the past five days, but was not discovered during the last discovery run. An icon with two printers displays when a printer is successfully discovered. An icon with a printer and check mark displays for a print queue.

2. The computer with the Agent installed on it can:
 - be turned off
 - not be working
 - no longer be communicating
 - a. Check the **Agents** tab on the Web Portal and identify if an agent is no longer communicating.
 - b. Restart the computer with the Xerox® Workplace Cloud Agent installed on it.
3. Install agents on additional computers if possible for redundancy.



Note: Every 5 days the system checks all the printers and agents to see when each printer last had communication with an agent. After 5 days with no communication, the printer is removed from the user view and remains in the administrator **Printers** tab until the Agent Administrator removes it manually.

Printer

1. Make sure you are using the correct email address for that printer.
2. The printer's IP address may have changed. Check with the owner of the printer.



Note: Administrators can use the Xerox® Workplace Cloud Agent to rediscover printers and find the target printer, or update discovery settings on the Xerox® Workplace Cloud Agent to include a target printer IP address.




3. The owner of the printer may be out of licenses. Check with the owner of the printer.
4. You can enable print submission notifications and print completion notifications to receive emails about job processing. The default is no notifications. Notification emails detail if the job was successful or if it failed along with failure details.
5. There may no longer be communication with the Agent because the printer is turned off. Turn on the target printer if it is off. Orphaned printers get removed from the user's printer list after 5 days of no communication.
6. If the printer is not on the enabled list:
 - a. Find the printer on the **All** printers list.
 - b. Select **Enable Printer** from the **Actions** menu.
 - c. Try to print again.



Note: A printer can only be enabled on one Xerox® Workplace Cloud account at a time.

7. If the last communication date on the printer is older than 24 hours:
 - a. Verify that the IP address of the printer has not changed by getting the IP from the printer and comparing it to what is on the **Printer** tab on the Web Portal. If the IPs do not match then update the agents with the new IP address, run a search for devices from the agent and attempt to print again.
 - b. Go to the **Agents** tab and make sure that the agents able to route jobs to the printer, have reported within the last 24 hours.
8. Check that the printer supports PDF, PCL5 or PCL6 and is configured correctly on the Web Portal under **Printers** and the last communication date is within the last 24 hours.
9. Make sure the printer is being discovered by the agent. For the following printers, make sure each is minimally at the recommended release:
 - WorkCentre 7525/7530/7535/7545/7556: Release 061.121.222.06507
 - ColorQube 9301, 9302, 9303: Release 061.180.222.08700
 - WorkCentre 7755/7765/7775: Release 061.090.222.09401

Paper Size

1. Check the printer to determine if the output is being held for resources. There is a paper substitution feature that resizes most page sizes, such as Letter for A4 or A3 for Ledger. The page size determined for the entire document is based on the size of page 1. The administrator can enable or disable this feature. If it is enabled, and the paper size needed to print the job is not loaded in the selected printer, the job will be scaled to fit the available paper.
 -  Note: When all paper trays are empty, the paper size settings for paper trays may not be detected and auto-scaling may not be applied.
 -  Note: Selecting **Original File Size** or selecting a specific paper size overrides scaling and paper substitution. If the printer does not have paper of the proper size loaded, the job will be held for resources.
2. Printers can have configuration settings for paper substitution. Even if the solution is not set to scale on paper mismatch, check the printer settings to ensure that the printer is either configured for that paper size or is set to perform paper size substitution.
 -  Note: Paper substitution is not available when printing through print queues because the paper tray information cannot be determined.


UNABLE TO ENABLE PRINTER

A printer can only be enabled by one Xerox® Workplace Cloud account at a time.

UNABLE TO ADD THE PRINTER CLIENT ON A XEROX® ALTALINK PRINTER

The Client Application Installation set up is present on the **Printers** tab on the Workplace Cloud Web Portal application:

- **Printers > Features > Client Application Installation.**
- **Printers** select the printer, **Action > Set Client Application Installation Mode.**

 Note: This setting will Install the client application on the printer.

If you have issues adding the Printer Client on AltaLink Printers do the following action:

- The solution to this issue may be caused by a printer setting, ensure the **EIP Remote Web Inspector** setting is disabled. This setting can be found on the AltaLink Printers on **Properties > General Setup > Extensible Service Setup > Diagnostics > EIP Remote Inspector.**

COMPANY PRINTERS DO NOT DISPLAY ON THE ACCOUNT

If you entered the wrong company code, you may now be connected to a different company.

If you see printers with your app that you do not recognize:

1. Log out of the mobile app and log in again using the correct company code.
2. Contact your administrator to make sure the printer is enabled in Xerox® Workplace Cloud.

DOCUMENTS DO NOT DISPLAY ON THE ACCOUNT

Check the following:

- Documents are available on a user account no matter which company code they are logged in with. The exception is when a user uploaded a document while logged into a Mobile Print Solution Account (onsite Mobile Print Server), it will not be available from within their Xerox® Workplace Cloud account.
- The document may already have been printed or have been in the system longer than 3 days. The default is that jobs are deleted after printing. To check the company Retention Policy setting, go to the **Account > Policies > Data Retention**.

WHEN USING OPEN IN FUNCTION IN APPLE IOS, WORKPLACE MOBILE APP DOES NOT DISPLAY AS AN OPTION

There may be a limit to the number of items shown in the item chooser, so all of the options may not be shown. On the iPad, make sure you use the hidden scroll bar to see all available items. Refer to Apple documentation for more information.

PRINTER SEARCH STATUS SHOWS “UNABLE TO COMMUNICATE WITH AGENT”

In the **Agents** tab, an agent status displaying "Unable to Communicate" indicates that there was a communication issue when Cloud attempted to contact the agent. Check the agent PC connectivity and ensure that the agent software is running:

1. Verify that the agent PC is connected to the Internet.
2. Reboot the agent PC and manually restart the agent service.

Once restarted, the agent should regain communication.

THE GPS COORDINATES OF THE PRINTER CHANGED

When you change a site to which a printer is assigned, the printer inherits the GPS coordinates of the new site.

JOB IS NOT DISPLAYED IN THE HISTORY

You may have more than one account. Select **Account > Company Profile** and view the company code to verify that you are looking in the correct account.



Note: Job history shows up to 7 days or up to 50 jobs, whichever occurs first.

When printing to public printers outside of Xerox® Workplace Cloud, the job will always display in the job history for 7 days.

JOB DID NOT PRINT AS EXPECTED

The printer may not support all features of the print job. Xerox® Workplace Cloud output will work with most non-Xerox devices that implement industry-standard PCL 5, PCL 6 or PostScript commands. If non-Xerox devices implement features in a proprietary manner or don't adhere to industry standards, the output may not print as expected.

The administrator should check which Page Description Language (PDL) Xerox® Workplace Cloud is using and make sure the printer supports that PDL.

It is recommended that you keep the selected defaults. If you experience image integrity or finishing issues, try different options to determine which give the best results.

Once a print job is transferred from the agent to the printer, Xerox® Workplace Cloud charges for that job. It is the user's responsibility to confirm that a print device is compatible with Xerox® Workplace Cloud. It is strongly recommended that you use a trial account or download the Xerox® Global Print Driver to test the compatibility of your devices.

JOB PRINTED 2-SIDED INSTEAD OF 1-SIDED

The administrator can set the **Print Control Policy** to print all Xerox® Workplace Cloud jobs 2-sided.

JOB PRINTED IN BLACK AND WHITE INSTEAD OF COLOR

The administrator can set the **Print Control Policy** to print all Xerox® Workplace Cloud jobs in black and white. If the user forwarded an email to a color printer and it printed in black and white, the company setting may be set to prohibit color printing or the printer may have a default set that overrides the user's preference.

UNABLE TO SELECT COLOR PRINTING

The administrator can set the **Print Control Policy** to print all Xerox® Workplace Cloud jobs in black and white. Users only see the color option if allowed by the administrator.

CHARGED FOR A BLANK EMAIL OR BLANK ATTACHMENT

Some email clients may convert email components (e.g., signatures) to attachments and may appear as a blank job. They will print and your company will be charged for the job.

PRINTER IS REQUESTING FOR PAPER TO BE LOADED WHEN IT CAN SUBSTITUTE

The paper substitution feature depends on information received from the printer. Some printers do not supply the required tray information for Xerox® Workplace Cloud to substitute a loaded paper size.

Paper substitution is not available when printing through print queues because the paper tray information cannot be determined.

The user may have selected Original File Size or a specific paper size for the print job.

MISSING IMAGES IN PRINTED OUTPUT

Linked images will not print if the linked content is password- or login-protected.

JOB DID NOT PRINT WITH CORRECT FONT

Documents containing custom or non-standard fonts may not print as expected, due to the font not being available to the Xerox® Workplace Cloud. For example, in order for Microsoft Office documents to print as expected, the font

used in the document needs to be a default Microsoft Office font and be supported by the target printer. To ensure your documents print as expected, replace the non-standard font with one that is supported by the application used for creating the document, and that is supported by the printer model you have selected.

UNABLE TO FIND PRINTED OUTPUT

Your default printer may have changed. The default printer is the last printer you printed to. Even if you set a printer to be your default at one time, the default will always be the printer you last printed to.

1. Go to <https://xwc.services.xerox.com> (Xerox® Workplace Cloud users only):
 - a. Select the **Jobs** tab.
 - b. Select the **History** tab and view where your print jobs were sent
2. If Secure Print is enabled on the printer, you must enter a passcode at the printer to release your job for printing:
 - a. If the job was submitted from the app or from the Web Portal, you created a passcode that must be entered at the printer to release the print job.
 - b. If Direct Email Printing was used, an email was generated by Xerox® Workplace Cloud that included a passcode that must be entered at the printer to release the print job.

DIRECT EMAIL PRINT JOB FAILS

If the printer has Xerox® Network Accounting or Xerox® Standard Accounting enabled, the administrator must allow accounting data to be stored in the system to enable the email printing feature. When printing from the Web Portal, users must enter their accounting information on the **Print** tab and save it before printing. If users do not print, the accounting information that they entered is not saved. If users previously printed to that printer or print queue, and have entered their accounting information, Xerox® Workplace Cloud applies the saved information on subsequent email submissions.

UNABLE TO FIND THE PRINTER WHEN ADDING THE PRINTER USING THE MOBILE APP

Do the following on the Web Portal:

1. Select the **Printers** tab, and make sure the **Last Discovered** communication date with the printer is within the last 24 hours.
2. Select the **Agents** tab, then:
 - a. Select the agent.
 - b. Select the **Discovery Settings** tab.
 - c. Verify that printer's IP Address is on the agent's **Settings** list.
 - d. Make sure the agent is online and available.
3. Check to see if this printer is served by a print queue rather than directly discovered by Xerox® Workplace Cloud. In the follow me print workflow, multiple printers are served by a print queue, and the individual QR codes do not apply. Print a Welcome Page for that print queue and instruct users to scan the Welcome Page QR code.

UNABLE TO SEE PRINTER OR PRINT QUEUE

Check that the user is logged into the correct company. When users access their Xerox® Workplace Cloud account and enter a company code, they see the printers and print queues that are associated with that company and those that other companies have made available.

UNABLE TO PRINT USING PRINT QUEUES

It is recommended that you print a welcome page to the print queue to make sure the information you entered is correct and the print queue is working properly.

If you are unable to print using print queues, do the following:

1. From the Web Portal, select a print queue on the **Print Queues** tab to place it in edit mode. Make sure the print queue has an agent assigned on the **Agents** tab and that the agent is on the network and available.
2. Make sure that the **LPD Server**, **LPR/LPD Port**, and **LPR Queue** names are correct on the **Details** tab.
3. If the print queue is being used with an accounting package, make sure you have **Server-based Accounting** selected on the **Accounting** tab.
4. Make sure your agent PC can communicate with the print queue.

JOB DID NOT PRINT WHEN ACCOUNTING IS ENABLED

Xerox® Workplace Cloud cannot determine if the user entered valid accounting information or has sufficient credits to print. It will send the job to the printer or print queue with the user-entered accounting information.

If user-entered accounting information is invalid or they have insufficient credits, the printer will delete the job. The job will be charged to the Xerox® Workplace Cloud company account.

DID NOT RECEIVE JOB SUBMISSION OR JOB COMPLETION NOTIFICATION

1. Verify that the job is not in your junk folder.
2. Make sure your mailbox is not full.
3. Make sure your email notification preferences are set correctly:
 - a. Go to the Web Portal, and click on your email address in the upper left corner.
 - b. Select **User Preferences**.
 - c. Verify that your **Email Notification Policy** preferences are selected.
4. Select the **Jobs** tab then the **History** tab and view the job status.

Devices running on Wi-Fi inside a secured-corporate environment will not receive push notifications if the firewall does not allow an outgoing connection to:

- iOS: port 5223
- Android: port 5228 (TCP+UDP)

UNABLE TO VIEW AND PRINT TO PRINTERS THAT ARE OUTSIDE THE COMPANY

It is at the discretion of your company to allow users to see and print to non-company printers.

To allow non-company printers, select **Account > Policies > Public Printing > Allow users to access printers enabled by other companies**.

When a user prints a document, the job will be charged to the company account that enabled the printer being used.

PRINTER MODEL NAME CONTAINS SPECIAL CHARACTERS

Printer model names are read directly from the printer. If the printer manufacturer has included special characters in the name, they will be displayed within Xerox® Workplace Cloud.

UNABLE TO FIND MY PUBLIC PRINTERS

Beginning with the release of Xerox® Workplace Cloud version 2.0, any printer that is not Secure Print capable will no longer be designated as a public printer. These printers will be changed to private printers. Printers that are Secure Print capable and have that feature enabled, will remain public printers.

MFP CLIENT APPLICATION (@PRINTBYXEROX) INSTALLATION ERROR

If you are unable to print using @PrintByXerox, you may get a “mismatch with device” error, or you may see an error on the Web Portal on the printer list or printer Details page.

1. Click the **Printers** tab.
2. Select the printer and click **Actions**.
3. Select **Repair**.

This will attempt to fix a Client Application installation error by rewriting the Client Application to the printer.



Note: The repair operation takes time, so feedback on its success or failure will not be immediate.

4. If this does not resolve the error:
 - a. Select **Printers > Administration > Printer Access Security** and check the Client Application configuration for the printer.
 - b. Validate that the printer’s administration credentials are correct on the **Administration** tab for the printer.
 - c. Make sure the printer has connectivity.
 - d. Make sure the agent has connectivity.
 - e. Using CentreWare Internet Services, select **Properties > General Setup > Extensible Services Setup > Browser Settings**. Check that **Enable the Extensible Services Browser** is selected and make sure the Registration API is enabled.
 - f. Using CentreWare Internet Services, ensure that the app has not been hidden.

The solution depends on your printer model.

CHECKING ALL AVAILABLE PRINTERS ARE DISCOVERED

1. Sort the list of printers by the last discovered date, to make sure they are being discovered.
2. Check the status of any printers that are more than one day old. The printer could be turned off. If necessary, turn on the printer.
3. Check the agent and the printer to see if the IP address changed.
4. Select **Printer Search** on the Print Agent to manually search for printers.

@PRINTBYXEROX ICON IS NOT VISIBLE OR DISPLAYS QUESTION MARKS (?) ON PRINTER

Check the following settings in Xerox® CentreWare® Internet Services:

1. Select **Properties > Services > Display > Show / Hide** to make sure the @PrintByXerox app is set to display.
2. Select **Properties > General Setup > Extensible Services Setup > Browser Settings** and check **Enable the Extensible Services Browser** to make sure that the browser is enabled.
3. Make sure that the DNS settings are correct.
4. Select **Properties > General Setup > Extensible Services Setup > Proxy** and make sure that the proxy settings are correct.

@PRINTBYXEROX ICON DOES NOTHING

Perform the following:

1. Using Centware Internet Services, make sure the proxy is set correctly. Select **Properties > General Setup > Extensible Services Setup > Proxy**.
2. Check to make sure the printer has network connectivity.

ERROR WHEN RESETTNG PASSWORD OR USER ID ON THE @PRINTBYXEROX APP USING AN AGENT

If you attempt to reset your password or User ID, and the reset link doesn't work or an error displays in your browser, perform the following:

1. Using Centware Internet Services, make sure the proxy is set correctly. Select **Properties > General Setup > Extensible Services Setup > Proxy**.
2. From the PC running the agent, check the Agent proxy settings on the **Configuration Settings** tab.

MESSAGE STATES "FOR ADMINISTRATION, YOUR HOME COMPANY SHOULD BE SET TO THE COMPANY TO WHICH THIS PRINTER IS REGISTERED. THIS PRINTER IS REGISTERED IN A DIFFERENT COMPANY."

If this is your printer, you may be connected to a different Xerox® Workplace Cloud company than this printer. Log out, then log back in with the same Company Code as this printer.

MESSAGE STATES “MAXIMUM NUMBER OF PRINTERS THAT YOU CAN ENABLE HAS BEEN REACHED. TO ENABLE THE PRINTER, DISABLE A DIFFERENT PRINTER OR PURCHASE ADDITIONAL PRINTER LICENSES.”

Maximum number of printers that you can enable has been reached. To enable the printer, disable a different printer or purchase additional printer licenses.

UNABLE TO UNLOCK MFP FROM THE WORKPLACE MOBILE APP USING CARDLESS OR CARD BASED AUTHENTICATION



Note: If you are using an Cloud Agent for authentication, ensure that the Proxy Bypass setting includes the Agent IP address.

If you are unable to unlock the printer or if the lock screen does not display at the MFP, make sure you are connected to the same company as the MFP and perform the following steps:

1. Click the **Printers** tab.
2. Select the printer and click **Actions**.
3. Select **Repair**.

This will attempt to fix a Client Application (@PrintByXerox) installation error by rewriting the Client Application to the printer.



Note: The repair operation takes time, so feedback on its success or failure will not be immediate. If this does not fix the problem, perform the following:

4. Make sure your account has an active Device License.
5. Make sure the printer has connectivity.
6. Make sure the agent discovering that printer has connectivity.
7. If the IP address of the Agent PC changes, do a repair on each printer using Cardless Authentication that is discovered by that agent.
8. Select **Printers > (PRINTER) > SNMP Settings**, then verify that the Administration settings and Fleet Management settings are correct.
9. Using CentreWare Internet Services, check the following:
 - Make sure SSL is enabled on the printer.
 - Make sure the Self-signed Certificate uses at least a 1024 bit key (512 bit key is not supported).

If Cardless Authentication is not working on the WorkCentre 6400, upgrade the printer software for 061.070.102.23501 or higher.

UNABLE TO UNLOCK A PRINTER USING ALTERNATE LOGIN

Perform the following:

1. Make sure the agent discovering that printer has connectivity.

2. Using CentreWare Internet Services:

- Check to make sure the Self-signed Certificate uses at least a 1024 bit key (512 bit key is not supported).
- Check to make sure SSL is enabled on the printer.
- Check to make sure Alternate Login is enabled for Convenience Authentication / Xerox Secure Access.

ADMINISTRATION BUTTON DOES NOT DISPLAY IN @PRINTBYXEROX APP

The reason is one of the following:

- The user does not have Xerox® Workplace Cloud administrator rights
- The user does not have printer administrator rights

@PRINTBYXEROX PRINT JOB DOES NOT PRINT

If you can release a job from the @PrintByXerox app but it does not print, check the job status of the printer. You may have missing resources, such as paper or supplies.

Authentication Issues

USER INTERFACE GIVES ME A MESSAGE THAT MFP IS NOT SET UP FOR CARD AUTHENTICATION

Verify that Card Authentication is set up.

CARD AUTHENTICATION IS NOT WORKING CORRECTLY

Ports 15042, 15043 and 443 need to be listening on firewall agent in order for Card Authentication to work correctly.

I AM NOT PROMPTED TO SWIPE MY ID BADGE

Verify that Card Authentication is set up.

I GET AN ERROR MESSAGE WHEN I SWIPE MY ID BADGE

Verify that the ID badge is registered and the Card Authentication setup is correct.

NOTHING HAPPENS WHEN I SWIPE MY ID BADGE

Verify that the card is registered and the Card Authentication setup is correct.

LOCAL USER DATABASE IS DELETED ON VERSALINK DEVICES

The local user database will be deleted on the Versalink devices whenever the Card Authentication / Convenience Authentication is changed on the Web Portal. The system administrator will need to input the local user database on a Versalink device each time the Card Authentication / Convenience Authentication is enabled or disabled.

OKTA AUTHENTICATION ON VERSALINK DEVICES

To ensure that the OKTA authentication is successful, configure the Xerox® VersaLink® devices:

1. Open a Web browser, then access the Web Portal for your Xerox® VersaLink® device. Log in.
2. Click **Apps > EIP Settings > Cross-Origin Resource Sharing (CORS)**.
3. Select **Allow only Trusted Domain**.
4. In the field that appears, type `*.xerox.com`, then select **Allow only Trusted Domain**.
5. Restart your Xerox® VersaLink® device.



Note: If the restart instruction is not shown in the Xerox VersaLink device Web Portal, the restart is unnecessary.

iOS Native Printing Issues

UNABLE TO SEE THE XEROX® WORKPLACE CLOUD WHEN USING IOS NATIVE PRINTING

1. When user and agent PC are on the same subnet:
 - a. Check that the iOS Native Printing and Automatic Discovery features are enabled on an agent. If the DNS Service Discovery (DNS-SD) has been configured, Automatic Discovery does not need to be enabled.
 - b. Check that the iOS device and the agent are on the same subnet.



Note: To enable iOS Native Printing across different subnets, refer to [Setting Up the DNS-SD for iOS Native Printing](#).

- c. Check the user's current wireless profile and ensure that the DHCP Search Domain matches the one configured when setting up the DNS Service Discovery.



Note: For more information on DNS Service Discovery setup, refer to [Setting Up the DNS-SD for iOS Native Printing](#).

2. When user and agent PC are on different subnets:
 - a. Check that the iOS Native Printing is enabled on an agent.
 - b. Check that the DNS Service Discover has been properly configured. Refer to [Setting Up the DNS-SD for iOS Native Printing](#).
 - c. Check the current wireless profile of the user's device and ensure that it is pointing to the DNS server where is Service Discovery configured.

USER AUTHORIZATION FAILS WHEN PRINTING THROUGH IOS NATIVE PRINT

1. Check that the user has created a Xerox® Workplace Cloud account, preferably through the Xerox® Workplace Mobile App. For additional assistance, refer the user to *Creating a Xerox® Workplace Cloud Account From a Mobile Device* in the *Xerox® Workplace Cloud User Guide*.
2. Check that the user is associated with the correct company. To do this, have the user log in to the Workplace Mobile App using your Company Code.
3. The user may not be using the correct log in credentials. These credentials are based on your company authentication type:

If Xerox® Workplace Cloud Authentication is enabled:

- iOS Native Print Username: Email Address
- iOS Native Print Password: Xerox® Workplace Cloud Password

If LDAP Authentication or Azure AD Authentication is enabled:

- iOS Native Print Username: Domain Username
- iOS Native Print Password: Domain Password



Note: Select **Account > Company Profile** on the Xerox® Workplace Cloud Web Portal to determine which Company Authentication Type that is being used.

USER DOES NOT RECEIVE PUSH NOTIFICATIONS WHEN PRINTING THROUGH IOS NATIVE PRINTING

Push notifications may not be allowed, depending on your network configuration.

Push notifications may be disabled in the Workplace Mobile App. To enable push notifications:

1. Open the user's Workplace Mobile App.
2. Go to the app's main screen.
You need to log out of the app if you are currently logged in.
3. Tap the gear icon.
4. Enable **Push Notifications**.

USER PRINT JOB NOT UPLOADING WHEN PRINTING THROUGH IOS NATIVE PRINTING

1. Check that user's iOS device is connected to the network.
2. Check that the agent is functioning correctly.
 - a. Open the agent on the Agent PC to display the Agent UI.
 - b. Select the **Configuration Settings** tab.
 - c. Check for error messages under **iOS Native Printing**.
3. Restart the agent.

DOCUMENT PRINTED IN A FORMAT THAT WAS NOT EXPECTED WHEN PRINTING THROUGH IOS NATIVE PRINTING

Xerox® Workplace Cloud cannot automatically adjust the formatting of PDF documents, when printed through iOS Native Printing. Try printing the document from the Workplace Mobile App:

1. Open the PDF document in the iOS device.
2. Choose the "Open in..." option from the **Actions** menu.
3. Select the **Workplace Mobile App**.
4. Print the document.

PRINTER APPEARS OFFLINE WHEN USING IOS NATIVE PRINTING

Check that the IPP Service Port 631 is open and allowing inbound requests.

New Features Overview

This appendix contains:

- New Features for Xerox Workplace Cloud Version 5.9.1..... 296
- New Features for Xerox Workplace Cloud Version 5.8.3..... 297
- New Features for Xerox Workplace Cloud Version 5.8.2..... 298
- New Features for Xerox Workplace Cloud Version 5.8.1..... 299
- New Features for Xerox® Workplace Cloud Version 5.8.0 300
- New Features for Xerox® Workplace Cloud Version 5.7.3..... 301
- New Features for Xerox Workplace Cloud Version 5.7 302
- New Features for Xerox® Workplace Cloud Version 5.6.1 303
- New Features for Xerox® Workplace Cloud Versions 5.5 and 5.6 304
- New Features for Xerox® Workplace Cloud Version 5.4 305
- New Features for Xerox® Workplace Cloud Version 5.3 307

New Features for Xerox Workplace Cloud Version 5.9.1

- The bottom of the Workplace Cloud Portal web page now provides Announcements link to Xerox Workplace Cloud Announcement Forum. The Forum is very important as it provides the Cloud Update information and Status.
 - The link name **Xerox Mobile** at the bottom left of the XWC portal web page has been changed to **Workplace Cloud**, while the actual link remains unchanged.
- A new selection option has been added in the **Company Profile > Details** tab called **Limit Express Codes for email job submission only**. This allows express codes to be sent only for email jobs and not for desktop job submissions.
- The Xerox Workplace Cloud now has the ability to notify administrators via email when user account is locked.
 - The user can reset their password to remove the lock. Alternatively, you can contact Xerox Support to unlock your account.
- Administrators can search for users by their **Cards/Managed PINs** numbers on the **Users** tab. It is applicable only for PEB and WEB License accounts. The search does not include Auto-Generated Pins.
- Xerox Workplace Cloud now includes a new feature called **Accounting Prompts**, which adds accounting prompt (s) at the time of authentication on the printer. The values entered when prompted are validated against stored values. This information will be included in the Reporting data of the solution when using the Usage Tracking feature.
- The feature known as **PIN Authentication** now allows users to alternate login to the printer using a new Auto-Generated Pin value. The auto generated Pin login takes the place of managed pin login. If auto generated PIN is enabled, managed pin login cannot be used.
- Updated the PS and PCL Cloud Global Print Drivers to version 5.1009.1.0, which includes support for Xerox AltaLink C82xx and B82xx and VersaLink B620/C620 printers.
- Ability to select a MAC PPD as a driver type for desktop printing Direct Print queues.

New Features for Xerox Workplace Cloud Version 5.8.3

- The limit of print release is increased from 10 to 20 jobs for all new Cloud Company accounts.
 - Existing companies that currently have a value of 10 will keep that same value.
 - Existing companies that had their default value changed to 20 will remain the same.
 - The older 8th generation UI WorkCentre devices do not support more than 10 jobs to be released at once. These devices will remain as 10.
- Added a new feature called as **User Management** to the **Agents** tab that allows User accounts to be deleted, updated, and added using a CSV file imported by the agent.
- Updated mobile unlock QR Code to now facilitate the installation of mobile application, IOS and Android, and unlock the printer.

New Features for Xerox Workplace Cloud Version 5.8.2

- Workplace Cloud allows you to choose Database and Document Storage Location during creation of Company Account, the selections are **European Union (EU)** or **United Kingdom (UK)**.
- When registering a Universal Print printer, the administrator can select the deployment location for job storage, the locations can be West Europe, UK South, and South Central US.
- In **Account > Settings > Desktop Printing**:
 - Renamed **Desktop Client** tab as **General**.
 - Moved **XML Driver Configuration** section from Desktop Client tab to a new tab, you can add multiple XML Driver Configuration file and associate user to them, also you can set priority to the XML Driver Configuration files.
 - Added **Queues** tab to create a **Pull Print Queues** and associate a Custom Driver, Composer File, or Mac PPD driver to it.
- Printers Deployment Groups have the ability to deploy Printers to **User Groups** and deploy **Pull Print Queues**.
- Ability to enable or disable the Direct Printing feature of the printers on the **Printers** tab using **Printers > Action** menu or edit printer settings.
- The Mac Client supports installing and printing to direct printers.
- Cloud Direct is supported by the VersaLink printer with the new plug in modules Xerox USB Card Reader (CR.3.0.xx) and XWC Connector Plugin installed. Refer to [Workplace Cloud Direct \(Manage Printer without an Agent\)](#) appendix.
- Xerox® Workplace Cloud have the Xerox PullPrint PS Driver 5.887.3.0 and PullPrint PCL6 Driver 5.887.3.0 drivers as pre-installed Custom Drivers, you can associate a Direct Printer or Pull Print Queues to these drivers.
- Added Printer Model and Finisher section to the Custom Driver **DriverMetaData.xml** configuration file, which allows you to set the Printer Model and add the Finishers to the Custom Driver. This is only supported with the Xerox Global Print driver as a Custom Driver.
- Auto Registration feature now allows you to define the **Badge Registration email validity period** which limits the maximum amount of time allowed for the user to respond to the Badge Registration email.
- Job Reporting tab allows you to schedule the auto export and email of the Job Reporting data and User activity tracks the Scheduled Job Reporting Export.
- Azure AD Advanced mode supports alternate login for users on the Xerox printers, users can login with PIN or email when Printer Authentication is On.
- Azure AD Simple and Advanced mode allows you to enable or disable the **Provide email domain hint for new users**, this setting is enabled by default. If set to disabled, then a new user will need to enter their email on the Azure AD login screen the first time they authenticate using Workplace Cloud with Azure AD.
- Akamai Content Delivery Network (CDN) support is changed to Azure Front Door Content Delivery Network (CDN).
- Added Workplace Cloud Load Balancer probe endpoint information to be Used by an Agent to provide failover system by detecting when a server is no longer operational and routing data to a different server.

New Features for Xerox Workplace Cloud Version 5.8.1

- Added a downloadable tool called **Xerox Workplace Solutions Print Queue Composer** that captures print drivers and settings and zips them into a file called a Composer file. The Composer zip file can be uploaded into Xerox Workplace Cloud and associated with a direct printer. Workplace Cloud Client has been updated to support direct printers that are associated with Print Queue Composer files.
- Added Deployment Groups under the Printers tab, which allows you to automatically deploy direct printers to client computers. Xerox® Workplace Cloud will act as a Print Queue Conductor and automatically deploy printers to client computers.
- Support to limit Copy Jobs with rules based on Print Quotas.
 - Enabling Copy Jobs option on **Set Usage Tracking Mode** for a printer will hold all the copy jobs and require pre-approval by Workplace Cloud in order for the job to be printed. If a job will cause the user to exceed their Quota, then the job will be rejected by the solution.
- Support for use of UPNs in addition to email addresses for Azure AD Simple and OKTA Authentication.
- Workplace Cloud supports the ability to read Azure AD User profile values which are contained in the OnPremiseExtensionAttributes compound object in Azure AD connections Field Mappings.
- Support for adding static IP address to your firewall allowed list to troubleshoot the Azure AD Simple Mode Alternate Login.
- Updated the PS and PCL Cloud Global Print Drivers to version 5.919.5.0 which includes support for VersaLink B625 / C625 printers.
- SAML claim response values have been updated to allow the return of the PIN (Card) as an optional attribute.
- Support for HelloID Authentication.
- Added Save License under **Account > Licensing** that allows you to save and store multiple licenses on your Workplace Cloud company account to enable them for future use. You can set the activation date, clear activation date, delete and change the country of the saved licenses.
- For any Country license, you can now change the Country back to a **Global [Default]** to make it work as a Global license.
- Support to select the Source of Authentication as **Xerox Workplace Cloud** or **Xerox Workplace Cloud Agent** when Allow Credential Access is enabled for Azure AD Simple authentication.
- Moved the **Custom Drivers** listings to a new tab in **Account > Settings > Desktop Printing**.
- Added a new tab **Available** under **Jobs** section to allow users to view and delete their uploaded jobs that are ready to be released from the printer.

New Features for Xerox® Workplace Cloud Version 5.8.0

- License activation by Country, Country mode allows you to assign a Country to a license and use it to enable printers based on the printer Site Country.
- Single Sign-On is now supported when using Cloud Direct on a Xerox® AltaLink B81XX and C81XX printers. Creation of a Company Root Certificate for the Single Sign-On communication is added to support this feature.
- Ability to manually add Domains to the Workplace Cloud Agent.
- Multiple email Address in the Contact email section of the Company Profile to facilitate the management of the workplace cloud account by multiple administrators.
- Use PIN as an Alternate Login entry with OKTA and Azure AD authentication.
- Date Range filter selection for Job Reporting.
- Delete Users using CSV import.
- Delete users using the new Remove action on the users tab.
- Support for Windows® 11 for Desktop Client.
- Support for Windows® 11 for Cloud Agent.
- Updated the Windows Desktop Client icons and color scheme.
- Updated the Workplace Cloud Web Portal color scheme.

New Features for Xerox® Workplace Cloud Version 5.7.3

- Added a new user role, Compliance Manager, which grants the users access to the Reporting tab.
- Ability to set the Print Limits to the user, this feature restricts the number of pages that all users or user groups can print in a single job.
- Cloud Direct – Agentless now supports the configuration of the blocking screen text, alternate login and locking of services if the Cloud Direct authentication is enabled. Also supports Mobile Unlock features which includes unlock code, QR code scanning and NFC on Xerox® AltaLink B81XX and C81XX devices.
- Supports printer Administrator Login when alternate login is enabled, users can use the alternate login option to log in to the printer control panel and access the printer Administrator functions.
- Supports manual device enablement of Workplace Cloud Direct Printer, this feature will allow the customer to link a Workplace Cloud Direct printer to their company and enable it without using an on premise agent.
- Allow Credential Access, this feature allows alternate login for Simple Azure AD authentication. When enabled, allows alternate login using PIN Authentication.
- The Data Retention period changed from 7 days to 3 days.
- The email print function does not support the open office document types odt, ods, odp, odg, and odf.
- Xerox® Workplace Cloud Agent is supported by Windows Server 2022.
- Additional instructions for setting up the drivers for EFI fiery controller for Macintosh and Windows Cloud Desktop Clients.

New Features for Xerox Workplace Cloud Version 5.7

- Advanced Azure AD integration that allows for the Single Tenant App for each domain and custom user field mappings.
- An enhanced agentless environment that is supported by Xerox® AltaLink® C81xx and B81xx Multifunction Printers at the latest software level. This new capability is referred to as Workplace Cloud Direct Remote Management.
- Support for primary and secondary authentication using LDAP and Azure AD Authentication.
- Single Sign-On with the Xerox® Workplace Cloud Web Portal and Windows client login in an Azure AD ADFS environment.
- Support for the Xerox® EC80XX Color Multifunction Printer.
- Improved license history, where expired licenses are displayed in the Inactive tab.
- Addition of a user field, called Alternate Access Card User.
- Support for identity provider SAML authentication.
- Improved encryption capabilities for print job and document storage encryption at the desktop and account level.

New Features for Xerox® Workplace Cloud Version 5.6.1

New Features for Xerox® Workplace Cloud Version 5.6.1

- Support for Universal Print in Microsoft Azure
- Setting to enable or disable the Job Reporting Data Export and the creation of Dashboards
- Addition of TCPConv3 to the network appliance menu
- Ability to set some print options when printing from the Chromebook App
- Content Security now supports Home Worker jobs
- By default, the CDN option is disabled for new Xerox® Workplace Cloud accounts
- Addition of the following fields to the reporting data .csv export file:
 - Site
 - Manufacturer
 - Model
 - Country
 - Serial number
 - Printer IP address
- Support hostname for the agent authentication server setting.
- Addition of a setting that controls whether Convenience Authentication session data is stored as username or domain\username.

New Features for Xerox® Workplace Cloud Versions 5.5 and 5.6

New Features for Xerox® Workplace Cloud Version 5.6

- Supports Xerox® AltaLink® B81XX and Xerox® AltaLink® C81XX series
- Agentless Authentication for Xerox® AltaLink® devices
- Supports multiple cards for the same user
- Delegate printing: Allows users who are designated as delegates to release print jobs for other users
- Basic Content Security for Xerox® Workplace Cloud Desktop Client only
- Ability to customize or add to the badge registration email for Azure AD Authentication or OKTA Authentication
- Home Worker Print Tracker: Allows users to print to local printers not enabled in Xerox® Workplace Cloud, and Xerox® Workplace Cloud tracks the print history of the user.
- Supports media resize for PDF conversion
- Addition of Department field to the Edit User details page
- Addition of a Notification Banner for Web Portal
- Support for the file Encryption/Decryption feature on the discovery platform printers
- Xerox® Workplace Cloud desktop client: Supports DNS Offline Mode Checking to switch between online and offline modes automatically.
- Cloud Agent: Support for Windows network shared print queue submission from Linux workstations

New Features for Xerox® Workplace Cloud Version 5.5

- Ability to enforce a job order when you release jobs from the @PBX app
- Allows administrator account for the local user interface access
- Allows for administrator access to the printer console even when blocked by the Xerox® Workplace Cloud authentication screen
- Allows companies to use the Xerox driver pre-configuration utility to set driver options and then upload this configuration to the Web Portal
- Allow companies to use their own public/private certificate pair that contains keys used for encryption and decryption on the Xerox® Workplace Cloud desktop client
- Ability to export the Discovery profile of an Agent to a .csv file and import the file to a different agent
- Supports user onboarding using the Alternate Login feature.
- Improved reporting data consistency when you use Usage Tracking feature (Network Accounting)
- Added the version number for the Windows and Mac Xerox® Workplace Cloud desktop clients or Agent that are downloaded
- When Content Delivery Network is enabled, the overall print performance is improved

New Features for Xerox® Workplace Cloud Version 5.4

Support DFE-Based Printers (EFI)

Xerox® Workplace Cloud software supports Xerox PrimeLink C9070 devices and PrimeLink B9100 devices with EFI capability. For more information, refer to [Xerox® Workplace Cloud for Xerox® Printers with an EFI Fiery Controller](#).

Update DCEs and Remove Support for PCL5

The Xerox® Workplace Cloud software updates Document Conversion Engines (DCEs) and does not support the PCL5 printer language. PCL5 for print jobs is disabled.

Job Management for Cancel Print

The Cancel Jobs Time-out is an optional timer configuration on the Xerox® Workplace Cloud Web portal during a session close. When the @PrintByXerox EIP App closes due to time out or when a user logs out, the jobs that are processing jobs are canceled. For more information, refer to [Cancel Jobs Timeout](#).

Support User Import by Administrator

Xerox® Workplace® Cloud software supports an updated user list using a .csv file. The User Import feature provides administrators with information about user import results using email communication. The account administrator can initiate a user import. For more information, refer to [User Import](#).

Printer name to the Job to Report Export File

When job reporting is enabled, you can initiate a .csv export. The .csv export file contains printer names and serial numbers.

Hide the open account for member users in a single company

When a new user creates an account with a new email address, if that open account is the home account of the user, the account is indicated in the My Companies file. When a user creates a company account after a new user account is created, and the open account is not the home account of the user, no open account is indicated in the My Companies file.

The 4-Digit Code Unlock with Workplace App

This feature provides the ability for users to unlock a printer when a 4-digit code is entered and appears on the blocking screen of the printer. There are two configurations: the default Disabled configuration and the Enabled configuration. When enabled, the device blocking screen does not display the 4-digit code to unlock the printer. For more information, refer to [Enable or Disable a 4 Digit Unlock Code](#).

Allow Account Level Token Time-Out Configuration

Xerox® Workplace Cloud software implements an account-level token time out configuration to provide users the ability to set access token lifetime settings. The token is set between 1–90 days. After the token expires, users are required to re-enter credentials.

You can select the Xerox Workplace Cloud Authentication Configuration or LDAP Authentication. Both options support the time out configuration. For more information about the Xerox Workplace Cloud Authentication Configuration, refer to [Configuring Xerox® Workplace Cloud Authentication](#). For more information about LDAP Authentication, refer to [LDAP Authentication](#).

Manual Agent Offline Mode

Xerox® Workplace Cloud implemented a manual agent offline mode to improve the usability of the solution. There are two configurable options for the agent offline mode from the Cloud Agent user interface: Automatic and Manual modes.

Xerox® Workplace Cloud Client for Mac 1.1

Xerox® Workplace Cloud Client for Mac supports Local Print Optimization options as the Cloud Client for Windows. Local Print Optimization option improves the performance of the Mac Client print jobs that are submitted to a custom generic printer for a later release. For more information, refer to [Xerox® Workplace Cloud for Mac](#).

Manage SNMP Settings for Multiple Devices

Xerox® Workplace Cloud implemented the ability for an account administrator to set SNMP settings at the same time for multiple devices. For more information, refer to [Manage SNMP settings](#).

Administration Settings for Multiple Devices

This feature updates the administrator user name and password values for all the selected printers in the Printers grid. To insert a user name and a password, you can select the Update Administrator Settings option..



Note: Update Administrator Settings and Set SNMP Settings do not push settings down to the device. Xerox® Workplace Cloud uses the settings to update the value to access and configure devices. Updates made through the two configurations are reflected in the Edit Printer Details Administration tab for all selected printers.

Edit IP Address of Agentless Printers

Xerox® Workplace Cloud allows administrators to edit the IP address of agentless printers. For more information, refer to [Editing the IP Address of Agentless Printers](#).

New Features for Xerox® Workplace Cloud Version 5.3

Xerox® Workplace Cloud Version 5.3.15

- Azure Connection error handling
- Requires a company code for new user onboarding
- Job management for EIP 9th generation that shows the printer job status
- Job management for EIP 9th generation that allows job cancelling
- Verify jobs of the previous user from the URL print path for an EIP print

Xerox® Workplace Cloud Client Version 5.3.201.0

- Parsing on and parsing off, and timeout file override for Workplace Cloud Client
- Improve IOT hub that has local-only client optimization reliability
- Clear messages when an IOT hub connection fails for print jobs
- Improved print job availability in the @PrintByXerox EIP App

Xerox® Workplace Cloud Agent Version 5.3.120

Quick single IP discovery

For more information, refer to the *Xerox® Workplace Cloud Administrator Guide* and the *Xerox® Workplace Cloud User Guide*.

Workplace Cloud Direct (Manage Printer without an Agent)

This appendix contains:

- Introduction..... 310
- Printers Supported and Firmware Requirements..... 311
- Methods to Enable the Cloud Direct Feature on a Printer..... 312
- Workplace Cloud Direct Authentication 320
- Troubleshooting the Workplace Cloud Direct Capability..... 323

Introduction

The Workplace Cloud Direct feature enables printers to connect to the Xerox® Workplace Cloud service and receive EIP-based Web service commands and requests without an agent. This allows the printer to support authentication and print submission without the need for an Agent. For more details on agentless features, refer to [Xerox® Workplace Cloud Configurations Comparison Chart](#).

An enhanced Workplace Cloud Direct environment introduced in Xerox® Workplace Cloud 5.7 is supported by specific Xerox printer models, such as Xerox® AltaLink® and VersaLink® Multifunction Printers. The new capability is referred as Remote Management. This new capability allows the printer to communicate with Xerox® Workplace Cloud using Microsoft IoT Hub technology, when you use Cloud Direct on specific Xerox Printer models.



Note: The Manage Printer without an Agent feature is renamed as Workplace Cloud Direct (Manage Printer without an Agent).

The Workplace Cloud Direct feature supports the following workflows:

- Printer Authentication including setting Authentication screen blocking text, Alternate Login and Locking of Services.



Note: For configuring Printer Authentication service pathway locking refer to [Machine Access](#).

- Mobile Unlock features which includes unlock code, QR code scanning and NFC.
- Usage Tracking (Network Accounting) including enabling usage tracking on the printer. Pulls the Network Accounting data from the printer.
- Installs the Cloud EIP Printer Client App.
- Single Sign On (SSO) of Gallery Apps is supported.
- Auto Release of all Jobs.

Printers Supported and Firmware Requirements



Note: Ensure that your device is updated with the appropriate firmware version to support the Cloud Direct feature.

Xerox® AltaLink® B80XX or C80XX: Version 103.xxx.010.14010 or later printers support only Workplace Cloud Direct Authentication.

Xerox® AltaLink® B81XX or C81XX: Version 114.xxx.042.25600 (launch release) printer supports Workplace Cloud Direct Authentication and Workplace Cloud Direct Remote Management.

Xerox® VersaLink® B620, C620, B625, C625, B415, and C415 running the latest software version that supports Workplace Cloud Direct Authentication and Workplace Cloud Direct Remote Management.

Xerox® VersaLink® B400–B405, C400–C405, C500–C600, C505–C605, C600–C610, B605–B615, C7000, C8000, C9000, B7025/30/35, C7020/25/30, B7125/30/35 and C7120/25/30 version printer supports Workplace Cloud Direct Authentication and Workplace Cloud Direct Remote Management running the latest firmware and with the new plug in modules (Xerox USB Card Reader (CR.3.0.xx) and XWC Connector Plugin).



Note: To set the above printers as Cloud Direct, refer to [Methods to Enable the Cloud Direct Feature on a Printer](#) and [Workplace Cloud Direct Authentication](#) sections.

Methods to Enable the Cloud Direct Feature on a Printer

You can enable the Workplace Cloud Direct setting on the Printer that is connected to the internet and supports Workplace Cloud Direct using any one of the following scenario considering the current Workplace Cloud Direct status of your printer.

Scenario 1: Auto enable Workplace Cloud Direct setting for new and not enabled printers

To auto enable Workplace Cloud Direct setting for the new and not enabled printers use **Auto Enable Workplace Cloud Direct** setting, this setting allows Workplace Cloud to auto enable the printer as Cloud Direct during printer discovery using an Agent. To use this method, refer to [Enable the Printers as Cloud Direct using the Auto Enablement of Remote Management Setting](#).

Scenario 2: Manual enablement of Workplace Cloud Direct setting for new and not enabled or already discovered and enabled Printers

To manually enable Workplace Cloud Direct setting for the new and not enabled or already discovered with an agent and enabled printers, refer to [Manual Enablement of Cloud Direct feature of the Printers on the Workplace Cloud Portal](#).

Scenario 3: Enable the Workplace Cloud Direct on a Printer using @PBX app (Without using an Agent) for new and not enabled printers

To enable Workplace Cloud Direct on a printer using @PBX app, refer to [Enabling Workplace Cloud Direct Printer using the @PrintByXerox Gallery App \(Without using Agent\)](#).

Scenario 4: Enable the Workplace Cloud Direct Authentication on a Printer for Xerox® AltaLink® B80XX or C80XX

To enable Workplace Cloud Direct Authentication on AltaLink B80XX or C80XX printers, refer to [Enable the Workplace Cloud Direct Authentication on Xerox AltaLink B80XX or C80XX Printers](#).

AUTO ENABLEMENT OF REMOTE MANAGEMENT



Note: Ensure the agent is updated to the latest version before using this setting.

The **Auto Enablement of Remote Management** setting is in the **Agents > Workplace Cloud Direct** tab, use this setting if you need to simultaneously enable Workplace Cloud Direct setting on several Cloud Direct supported printers during the printer discovery process using an Agent. The Workplace Cloud will determine if the printer supports remote management without an Agent. If this capability is supported by the printer and the printer is enabled in Workplace Cloud, the Agent will automatically configure the printer as a Workplace Cloud Direct device.

When the **Auto Enablement of Remote Management** is enabled and the printer supports remote management, the following settings are enabled automatically:

- The Workplace Cloud Direct (Manage Printer without an Agent) setting on the Workplace Cloud Web portal for the printers that are discovered.
- The Xerox Workplace Cloud connectivity setting on the printer.

Enable the Printers as Cloud Direct using the Auto Enablement of Remote Management Setting

To enable the Auto Enablement of Remote Management feature, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.

2. Click **Agents > Workplace Cloud Direct** tab.
3. In Auto Enablement of Remote Management section, select the radio button for **Enabled**.
4. To manage the SNMP setting, refer to [Manage SNMP settings](#) section.
5. Click **Save**.
6. Run the discovery search for printers. For more information, refer to [Updating Discovered Printers](#).
7. Enable the printers that are discovered. For more information, refer to [Enable or Disable Printer](#).
8. Run the discovery search again.



Note: After you discover and enable a printer, Workplace Cloud Direct (Manage without an Agent) is enabled automatically on the next discovery search. You can wait for next printer discovery search to run or initiate a manual discovery search.

9. To check the printers are enabled as Cloud Direct, refer to [Test Workplace Cloud Direct Connection of the Printers](#).
10. After you perform these steps, you can configure the printer for Workplace Cloud Direct authentication, refer to [Workplace Cloud Direct Authentication](#).



Note: When you change the printer management setting, the current configuration of the printer related to authentication, usage tracking, and the printer client application is not updated automatically. After you change this setting, perform a repair action on the printer.

Test Workplace Cloud Direct Connection of the Printers

To test the Cloud Direct Connection of the Printers:

1. Select **Printers > Enabled** tab.
2. On the Printer Grid section, ensure the **Globe** icon appears in blue with the green tick mark for the Cloud Direct Printers.
3. Hover over the **Globe** icon for Cloud Direct connectivity errors.
4. If there are errors in Cloud Direct connectivity, select the Printer Name to edit the Printer.
5. Select the **Agents** tab.
6. Under Print Management, make sure the **Workplace Cloud Direct (Manage Printer without an Agent)** is selected.
7. Click on **Test Connection** for the Cloud Direct connection status.
8. For troubleshooting the errors, refer to [Troubleshooting the Workplace Cloud Direct Capability](#).

Disable the Auto Enablement of Remote Management Setting



Note: This setting will not disable the Cloud Direct feature on the discovered printers which are already enabled as a Cloud Direct printer.

To disable the Auto Enablement of Remote Management setting, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal as an administrator.
2. Click **Agents > Workplace Cloud Direct** tab.

3. In Auto Enablement of Remote Management section, select the radio button for **Disabled** and click **Save**.
The Auto Enablement of Remote Management setting is disabled.

MANUAL ENABLEMENT OF CLOUD DIRECT FEATURE OF THE PRINTERS ON THE WORKPLACE CLOUD PORTAL



Note: This setting can be found in the **Printers > Actions** menu and on the **Edit Printer** setting.

Use this setting if the **Auto Enablement of Remote Management** is disabled on the **Agents > Workplace Cloud Direct** tab during the printer discovery. The Xerox® Workplace Cloud also supports the ability to unlink a device from your existing Agent that is used during printer discovery. After you unlink the device, you can configure the printer to be managed remotely, including authentication. To force the printer into Workplace Cloud Direct mode, perform the following steps:



Note: Skip step 2 and step 3 if your printers are already discovered through an agent and enabled in Workplace Cloud web portal.

1. Log in to the Xerox® Workplace Cloud Web Portal using your credentials.
2. Run the discovery search for printers on the agent. For more information, refer to [Updating Discovered Printers](#).
3. Enable the printers that are discovered. For more information, refer to [Enable or Disable Printer](#).
4. Select **Printers > Enabled** tab.
5. To enable the printer for Workplace Cloud Direct, do one of the following:



Note: Cloud Direct supported printers have the Globe icon on the printer grid.

- Enabling Workplace Cloud Direct from **Printers** tab:
 - Select the check box of required printers from the list, use search option if required.
 - Click **Actions > Workplace Cloud Direct (Manage Printer without an Agent)**.
The Printer is set for **Workplace Cloud Direct (Manage Printer without an Agent)**.
- Enabling Workplace Cloud Direct from **Edit Printer** option:
 - Select the Printer name to Edit Printer.
 - Select the **Agents** tab.
 - On Printer Management, select the radio button for **Workplace Cloud Direct (Manage Printer without an Agent)**.
 - Click Save.

The Printer is set for **Workplace Cloud Direct (Manage Printer without an Agent)**.

6. To test the Workplace Cloud Direct Connectivity, refer to [Test Workplace Cloud Direct Connection of the Printers](#).

7. After you perform these steps, you can configure the printer for Workplace Cloud Direct authentication, refer to [Workplace Cloud Direct Authentication](#).



Note: When you change the printer management setting, the current configuration of the printer related to authentication, usage tracking, and the printer client application is not updated automatically. After you change this setting, perform a repair action on the printer.

ENABLING WORKPLACE CLOUD DIRECT PRINTER USING THE @PRINTBYXEROX GALLERY APP (WITHOUT USING AGENT)



Note: These steps are applicable for any printer that supports the @PrintByXerox Gallery App, or Gallery Apps in general. If the printers supports Workplace Cloud Direct Remote Management, then you can install the @PrintByXerox app through the Web Portal.

Install the @PrintByXerox Printer App

To install the @PrintByXerox Printer App do the following:

1. Connect the Xerox® Multifunction Printer to the Internet and enable the printer.
2. Go to Xerox® App Gallery at appgallery.external.xerox.com/xerox_app_gallery, and log in with your User Name and Password. If you do not have an account, click the **Create Account** link.



Note: For detailed information on the use of Xerox® App Gallery, to add a device, and to install the @PrintByXerox printer app, go to www.support.xerox.com/support/xerox-app-gallery/ and download the *Xerox® App Gallery Channel Partner User Guide*. Also, for more information refer to *Xerox® @PrintByXerox Quick Start Guide*.

3. Log in to the Xerox® App Gallery website.
4. Click **Xerox App Gallery**.
5. The Xerox® App Gallery opens. From the gallery, locate and add **@PrintByXerox**.
6. Return to the Xerox® App Gallery and click the **Devices** tab.
7. Add the devices on which you want to install @PrintByXerox.
8. From the **Apps** tab, to install the app, select the down arrow. Accept the End-User License Agreement.
9. A dialog displays listing the devices you added. For each device you want to install the app on, select the free installation.

@PrintByXerox app is successfully installed on the required devices.

Register the Printer Using @PrintByXerox Printer App

1. Login to the printer as an Administrator.
2. Scroll down the app list and click on **@PrintByXerox** app.
Xerox® Workplace Cloud Login page is displayed.
3. Enter your Xerox® Workplace Cloud credentials to log in as the Multifunction Printer administrator to the @PrintByXerox app.
4. Click **Gear** icon and enable **Add Device to My Company** and **Enable Licensed Features** settings.

5. Click **OK**.

The Printer is successfully added to the Workplace Cloud Company Account.


Enable Workplace Cloud Direct Feature on the Printer

 Note: These steps are not applicable for the Xerox® AltaLink® B80xx or C80xx printers. If you have completed the registration of the Printer in Workplace Cloud using PBX app, you can continue with the task [Enable the Workplace Cloud Direct Authentication on Xerox AltaLink B80XX or C80XX Printers](#).

1. Login to the Printer Embedded Web Server using the administrator credentials.
2. Click **Properties > Connectivity > Setup**.
3. On **Remote Management > Xerox Workplace Cloud**, click **Edit**.
4. Under **Configuration**, click on **Connection**.
5. Enter the host as `wdm.services.xerox.com` with a port number of 443 and the Path as `/DM`.
6. Click **Save**.

The printer is enabled as Workplace Cloud Direct.

7. To test the Workplace Cloud connectivity of the printer, refer to [Test Workplace Cloud Direct Connection of the Printers](#).
8. After you perform these steps, you can configure the printer for Workplace Cloud Direct authentication, refer to [Workplace Cloud Direct Authentication](#).

 Note: When you change the printer management setting, the current configuration of the printer related to authentication, usage tracking, and the printer client application is not updated automatically. After you change this setting, perform a repair action on the printer.

ENABLE THE VERSALINK® PRINTERS AS CLOUD DIRECT

Prerequisites:

- On the Printer do the following actions:
 - Make sure the printers are updated to the latest Firmware version.
 - Activate the Plug-in modules, refer to [Activate the Plugin Modules](#).
- If you are using the SSO feature with the Gallery Apps and you want to enable Cloud Direct then on the Cloud Web portal, enable Single Sign-On and create a Company Root Certificate. Refer to [Enable Single Sign-On for Cloud Direct Devices](#).

Activate the VersaLink® Plugin Modules

To activate the Plugin Modules on the VersaLink® printers:



Note: Ensure that the printer is updated with the appropriate firmware version to support this feature. Plug-in Modules are supported on the specific series of Xerox® VersaLink® printers.

1. Login to the printer as an administrator.
2. Click on **System > Plug-in Settings** on the printer.
3. Select the **Xerox USB Card Reader (CR.3.0.XX)** Plugin and click on **Activate**.
4. Select the **XWC Connector Plugin** Plugin and click on **Activate**.
5. Click **Close**.

The Plugin Modules for the printer are activated.

6. Reboot the Printer.

Enabling the VersaLink® Printer as Cloud Direct using an Agent



Note: Ensure the agent is updated to the version 5.8.1xx or higher, the Agent auto-discovers the printers, enabling the printer as **Workplace Cloud Direct (Manage Printer without an Agent)**, the Agent configures the printer for remote management.

1. Login to Workplace Cloud Web portal and discover the printers with an Agent, refer to [Adding a Printer Using an Agent](#).
2. Enable the printers that are discovered, refer to [Enable or Disable Printer](#).
3. Select the **Printers > Enabled** tab, select the required printers from the list and click on **Actions > Workplace Cloud Direct (Manage Printer without an Agent)**.

Wait for the printer reboot to complete.

4. Enable Authentication, refer to [Enable Authentication for Cloud Direct Printers](#).

There will be two printer reboots, wait until they complete.

5. Do the repair action on the **Printers > Enabled** tab, select the required printers from the list and click on **Actions > Repair**.

There will be three printer reboots, wait until they complete.

Enabling the VersaLink® Printer as Cloud Direct without using an Agent

1. To add printers into Workplace Cloud Company account and configure as a Cloud Direct printer, refer to [Enabling Workplace Cloud Direct Printer using the @PrintByXerox Gallery App \(Without using Agent\)](#).
2. Login to Workplace Cloud Web portal, select the **Printers > Enabled** tab, select the required printers from the list and click on **Actions > Workplace Cloud Direct (Manage Printer without an Agent)**.

Wait for the printer reboot to complete.

3. Enable Authentication, refer to [Enable Authentication for Cloud Direct Printers](#).

There will be two printer reboots, wait until they complete.

4. Do the repair action on the **Printers > Enabled** tab, select the required printers from the list and click on **Actions > Repair**.

There will be three printer reboots, wait until they complete.

SWITCH CLOUD DIRECT PRINTER TO BE MANAGED BY AN AGENT

To switch the Cloud Direct Printer to be managed by an Agent, do the following steps:

1. Select **Printers > Enabled** tab.
2. Select the check box of required printers.
3. Click **Actions > Manage Printer using an Agent**.
4. Add printer to the Agent Discovery Profile [Adding a Printer Using an Agent](#).
5. Run the discovery search for printers on the agent. For more information, refer to [Updating Discovered Printers](#).
6. Repair the enabled printers, select the printers, click **Actions > Repair**.

The Cloud Direct printer is switched to be managed by an Agent.

Workplace Cloud Direct Authentication

Overview

The Workplace Cloud Direct Authentication feature allows printers to open a connection to the Xerox® Workplace Cloud service and receive EIP-based Web service commands and requests. EIP-based Web service commands and requests allow the printer to support authentication and print submission without an agent environment. For more information, refer to [Capabilities of Workplace Cloud Direct Authentication](#).

CAPABILITIES OF WORKPLACE CLOUD DIRECT AUTHENTICATION

The following workflows are supported in the Workplace Cloud Direct Authentication:

- Badge ID authentication: This workflow uses a personal identification card to authenticate users.
- Alternate Login Authentication: This workflow allows users to enter a PIN and email address for user authentication.
- Auto Release of jobs on authentication.
- Print submission is through all paths

ENABLE AUTHENTICATION FOR CLOUD DIRECT PRINTERS

To enable authentication for Cloud Direct printers do the following steps:



Note: Ensure the Printers are enabled for remote management before enabling the Cloud Direct authentication, refer to [Methods to Enable the Cloud Direct Feature on a Printer](#).

You can use any one of the following methods to enable the Workplace Cloud Authentication on the Printers:

1. Login to the Workplace Cloud Web Portal as an administrator.
2. Select **Printers > Enabled** tab.
3. To enable the Workplace Cloud Authentication on the Printers do any one of the following:
 - Enabling Workplace Cloud Authentication from **Printers > Action** menu:
 - Select the check box of required printers from the list, click **Actions > Set Authentication Mode**.
Set Authentication Mode dialogue box appears.
 - Select the radio button for **Enabled** and click on **Apply**.
The Workplace Cloud Direct Authentication is set for selected printers.
 - Enabling Workplace Cloud Authentication from **Edit Printer** option:
 - Select the Printer name to edit the printer settings.
 - Click on **Features** tab and select the radio button for **Enable** under Authentication.
 - Click **Save**.
The Workplace Cloud Direct Authentication is set for the printer.
4. After saving your changes, repair all the printers which are enabled to use Authentication.

CONFIGURING WORKPLACE CLOUD DIRECT AUTHENTICATION FOR XEROX ALTALINK B80XX OR C80XX PRINTERS

The steps to configure Workplace Cloud Direct Authentications are as follows:

1. Register or link your printer to your Xerox® Workplace Cloud company account.
2. To use Cloud Authentication, configure the printer.
3. Set the screen settings manually.
4. Enable the Workplace Cloud Direct authentication, refer to [Enable the Workplace Cloud Direct Authentication on Xerox AltaLink B80XX or C80XX Printers](#).

Enable the Workplace Cloud Direct Authentication on Xerox AltaLink B80XX or C80XX Printers

To enable Workplace Cloud Authentication on Xerox AltaLink B80XX or C80XX Printers, do the following:



Note: Skip step 2 and step 3 if your printers are already discovered through an agent and enabled in Workplace Cloud web portal.

1. Log in to the Xerox® Workplace Cloud Web Portal using your credentials.
2. Run the discovery search for printers on the agent. For more information, refer to [Updating Discovered Printers](#).




Note: You can also register the printer in Workplace Cloud using PBX app, refer to [Enabling Workplace Cloud Direct Printer using the @PrintByXerox Gallery App \(Without using Agent\)](#).

3. Enable the printers that are discovered using an agent or registered using the @PBX app. For more information, refer to [Enable or Disable Printer](#).
4. Enable Authentication at the Printers:
 - a. Connect to the printer using a Web browser.
 - b. Click **Properties > Login/Permissions/Accounting > Login Method**.
 - c. Select the **Control Panel Login** icon.
 - d. Change the Control Panel Login method to **Xerox Workplace Cloud**.
 - e. Change the Alternate Control Panel Login method to **User Name/Password – Validate on the Network**.
 - f. Save the setting.
 - g. To edit the link, select the **Convenience Authentication Setup** link.
 - h. To use host Name, configure the Server Communication and enter a value of `wdm.services.xerox.com` with a port number of 443.
 - i. For the Path value, enter `DM`.
 - j. Save the setting.
5. At the printer browser interface, the customer can set the desired blocking screen text. To set the blocking screen text, do the following:
 - a. Click **Properties**.
 - b. Select **Login/Permissions/Accounting > Login Method > Customize Blocking Screen (Edit)**.

6. At the printer browser interface, the customer can set the services that are locked. To enable the authentication for the printer using the Xerox Workplace Cloud Web Portal, do the following:
 - a. Click **Properties**.
 - b. Select **Login/Permissions/Accounting > Login Method > User Permission Roles (Edit) > Non-loggedIn (User) > Apps & Tools**.
7. Enable Workplace Cloud Direct setting for the printer on Workplace Cloud Portal:
 - Enabling Workplace Cloud Direct from **Printers** tab:
 - Select the check box of required printers from the list, use search option if required.
 - Click **Actions > Workplace Cloud Direct (Manage Printer without an Agent)**.
The Printer is set for **Workplace Cloud Direct (Manage Printer without an Agent)**.
 - Enabling Workplace Cloud Direct from **Edit Printer** option:
 - Select the Printer name to Edit Printer.
 - Select the **Agents** tab.
 - On Printer Management, select the radio button for **Workplace Cloud Direct (Manage Printer without an Agent)**.
 - Click Save.
The Printer is set for **Workplace Cloud Direct (Manage Printer without an Agent)**.
8. Enable Cloud Direct authentication, refer to [Enable Authentication for Cloud Direct Printers](#).

Troubleshooting the Workplace Cloud Direct Capability

When you select **Test Connection**, the possible results are as follows:

ERROR MESSAGE	CONDITION
Printer has not established a connection to the cloud.	<p>The printer has no active IoT Hub connection.</p> <p>Ensure the Printer settings for Xerox® Workplace Cloud is enabled.</p> <ul style="list-style-type: none"> Using the WebUI of the printer, go to Properties > Connectivity > Setup > Xerox Workplace Cloud. Select the Connection line. Enable the feature. Ensure that the Host value is <code>wdm.services.xerox.com</code> with a port of 443 and a Path of DM. Select Save. <p>If that does not resolve the error, The printer could not get to the IOT Hub Endpoint, possibly the endpoint its blocked due to the customers firewall.</p> <p> Note: Ensure that the time of the printer or device is within 5 minutes of the actual time else Microsoft will reject the IOT Hub connection.</p>
Failed sending request to printer.	<p>Xerox® Workplace Cloud attempted to send a request to the printer through the IoT Hub, but received the following error from Microsoft:</p> <p>Printer is successfully register with IOT hub, however it is not responding to Xerox® Workplace Cloud.</p> <p>Check printer internet connectivity, ensure that the Printer Proxy setting are correct.</p> <p>Validate the printer is turned on.</p>
Printer did not respond to request	<p>The IoT Hub request was made, but no follow-up response was received for the results of the request. It is possible that the SNMP settings are incorrect.</p>

To allow remote management to be enabled, the following Web services are enabled:

- EIP SNMP Configuration
- Print Submission
- Access Config
- Xerox Secure Access
- Extensible Service Registration

Usually, these printer services are enabled by default. If the services are not enabled, you can enable them manually in **Properties > Connectivity > HTTPS > Web Services**.

Xerox® Driver Configuration File

This appendix contains:

Xerox Print Driver Configuration Tool	326
---	-----

The Xerox® Workplace Cloud solution can distribute one Xerox® driver file to all end users only. If you want to use that method, to allow the color for some users and but prevent it for other, then ensure that two different Xerox® files are generated and at least one of them is managed or deployed to the color users outside the solution. Ensure that you use Microsoft System Center Configuration Manager or any IT deployment tool to push the file to the color users. The Xerox® Workplace Cloud client manages the file, used by the rest of the users.

Enforced Settings

Enforced settings allow an administrator to supply a default value that the user is not allowed to override the value, including within applications. Enforced Settings is the most restrictive level of enforcement.

Enforced Defaults

Enforced defaults allow an administrator to supply a default value that the user cannot override the value, within Printing Preferences in the Printers and Scanners dialog. The user can change features when they use an application.

Standard Defaults

Standard defaults are settings defined as recommended by the administrator for the feature. These defaults can override in the application and/or within Printing Preferences in the Printers and Scanners dialog. Changes cannot be made in Printer Properties/Printing Defaults. This is the least restrictive setting. The Standard Default setting is listed as default in the menu.

To check what value they have set the can look at the xml file. Here is what Enforced Setting looks like in the file:
<Setting Name="Monochrome" Behavior="EnforcedSetting" />.

Xerox Print Driver Configuration Tool

The latest tool is Xerox Print Driver Configuration Tool v3.7.55.0

The following features were added to this version of the Xerox Print Driver Configuration Tool:

- ICM Method can be configured
- Share Diagnostic data – An administrator can enable or disable analytics (telemetry)
- Based on the name of the queue, administrators can now configure an individual queue

DOWNLOADING THE XEROX PRINT DRIVER CONFIGURATION TOOL USER GUIDE

To download the user guide, do the following:

1. Go to www.xerox.com.
2. In the search field, type `xml configuration`.
3. To open the Customer Tip or User Guide, click **Xerox XML Configuration Editor for Print Drivers** link.

If `xml configuration` returns no result, in the search field, type `dynamic pre-configuration`, then do the following:

4. Click **Global Printer Driver – Xerox** link.
5. To open the Customer Tip or User Guide, in the Key Features list, click **Dynamic pre-configuration**.
If you get an old Tool version over 1 year old, in the web link of XGPD, replace the `wordenus` by `engb`. The link is <http://www.support.xerox.com/support/global-printer-driver/file-download/enus.html?contentId=116479>.
6. To download the latest Xerox Print Driver Configuration Tool, in the Prerequisites/Assumptions page, click :
<https://www.support.xerox.com/en-us/product/global-printer-driver/content/116479>.

PREPARING XEROX® DRIVER CONFIGURATION FILE

The latest Xerox® Workplace Cloud and Xerox® Workplace Cloud Client versions, in Desktop printing, allow to add an Xerox® Driver Configuration file to a Custom Driver.



Note: Ensure that there is no previous configuration by Xerox® Driver Configuration file that runs on the system.

To prepare the file, do the following:

1. Run the Xerox Print Driver Configuration Tool file.
The Xerox Print Driver Configuration Tool dialog box appears.
2. Click **+** next to Add New printer.
3. Select one of the following:
 - **Printer Model:** You can configure based on Pull Print Driver and XGPD name.
 - **Printer Queue:** You can configure an individual queue based on the name of the print queue installed in Windows Print Management. XGPD 5.703.x and higher. It allows different driver settings applied to print queues based on the same printer Model, installed on the same system.Set the required settings from the following:

a. Select **Printer Model**.

The key point is to use the right name according to the driver type.

The Reminder/Gold Rules dialog box appears. Set the required settings as follows:

- **Based on Pull Print Driver (and Specific Product Driver):** In the Advanced tab, ensure that the printer model name is based on the name that appears in the Driver field.
- **Based on GPD:** In the Administration tab, ensure that printer model name is based on the name that appears in the Configuration field.

b. Select **Printer Queue**. Set the required settings as follows:

You can have any driver but the name of the print queue is always set. You can have a print queue in black and white and another one in color, based on the same printer model.

4. Save the file with the file name: `CommonConfiguration.xml`. Do not change the name of the file name.
5. To add and enable a Xerox® Driver Configuration File, refer to [Xerox® Driver Configuration](#) section.
6. To upload a custom driver, refer to [Preparing the Driver for Upload](#).
7. If necessary, in the Desktop Printing area, download the latest version of the Windows Xerox® Workplace Cloud Client.
8. Select **Print > Desktop**, then click the created custom driver.
If you are performing the [Step 9](#) and [Step 10](#), do not run the installation now. If you are not performing the [Step 9](#) and [Step 10](#), you can proceed to [Step 11](#).

The `XeroxWorkplaceCloudClient.xwc.dp` is downloaded.

The [Step 9](#) and [Step 10](#) are not basically required but consolidates the XML file installation and reduce the 24 hours of waiting. This setting is based on XML Configuration experience outside Xerox® Workplace Cloud

9. Run Regedit, and type `\HKEY_LOCAL_MACHINE\SOFTWARE\Xerox\PrinterDriver\V5.0\Configuration`, then click **Enter**.
10. Right click the **Configuration**, then **Add > DWORD** with name `CacheExpirationInMinutes` and value 0 as setting.
11. Go back to folder where `XeroxWorkplaceCloudClient.xwcdp` is saved, and run it
Wait for the notification from Windows as it is completed. To check the printer is created, run Print Management. Open the created printer properties to see that Xerox Driver Configuration Tool has applied the right settings.

If the process is completed successfully, then you can view the following:

- In RegistryIn, RepositoryUNCPath file is added in `\HKEY_LOCAL_MACHINE\SOFTWARE\Xerox\PrinterDriver\V5.0\Configuration`.
- In `C:\ProgramData\Xerox\XMPC\DriverConfiguration`, the following files:
 - `CommonConfiguration.xml`
 - `DriverConfigHash.sha1`

Workplace Clients

This appendix contains:

Workplace Client Overview..... 330

Workplace Windows Client..... 332

Workplace Macintosh Client..... 333

Workplace Client Overview

INSTALLATION

Users need to either download and install the Xerox® Workplace Cloud client themselves, or the client need to be installed using your company programmatically. If you install the client by yourself, refer to the section [Print: Desktop](#). For administrator, refer to [Installation of the Workplace Cloud Windows Client](#).

SECURING THE XEROX® WORKPLACE CLOUD CLIENT TO AN ACCOUNT

To provide additional security, it is possible to limit the use of the Xerox® Workplace Cloud Client to a single company account.

When a Xerox® Workplace Cloud Client is secured, users can log in to the Xerox® Workplace Cloud Client only if their home account is the same company account that the Xerox® Workplace Cloud Client is secured to. If a user accesses a different company account in the Web Portal while they are logged in to the Client, when the authentication token refreshes, the Client logs the user out.



Note: Users can have access to multiple company accounts. The home account of a user is the company account that the user last logged into in the Web Portal.

To secure the Client, the company IT department is required to place a file that contains the necessary settings in the installation path for the Xerox® Workplace Cloud Client. For more information on securing a Xerox® Workplace Cloud Client to an account, contact a Xerox® representative.

HEALTH CHECK



Note: The following features are supported on the Windows version of the Workplace Client only.

To view the status of the Workplace Client, do the following:

1. Open the Windows system tray.
2. Right click the Xerox® Workplace Cloud Client.

The Menu appears.

3. Select the **Health Check** option

The Health Check dashboard shows the following information:

- **Client Version:** This is the current software version of the Workplace Cloud Client installed on your workstation.
- **Login Status:** This option indicates your current login status to Workplace Cloud.
- **Cloud Service:** This option indicates if the Xerox® Workplace Cloud service can be reached using your current network connection.
- **Print Optimization:** This is a feature that is managed by the Workplace Cloud administrator.
- **Quick Status Indicators:** This option indicates the status of print jobs.
- The time and date of the last status collection is displayed here.

- The data is not refreshed when you open this page. Data is collected periodically when start the application, when you add a new Workplace Cloud printer, and is refreshed once per day.

The printers that are installed on your workstation are shown along with the current status of each printer.

Workplace Windows Client

Windows Workplace Client supported languages are:

- Arabic
- Catalan
- Czech
- Danish
- German
- English
- UK English
- Spanish
- Finnish
- French
- Hungarian
- Italian
- Dutch
- Norwegian
- Polish
- Portuguese
- Romanian
- Russian
- Swedish
- Turkish
- Greek

Supported authentication types are:

- Xerox Workplace Cloud Authentication
- LDAP Authentication
- Azure AD Authentication
- OKTA Authentication.

Supported Windows OS:

- Windows 10
- Windows 11

Workplace Macintosh Client

XEROX® WORKPLACE CLOUD FOR MAC

Supported languages are:

- English
- German
- Spanish
- Italian
- French
- Dutch
- Portuguese.

Supported authentication types are:

- Xerox Workplace Cloud Authentication
- LDAP Authentication
- Azure AD Authentication
- OKTA Authentication.

Supported MAC OS version:

- Mac OS version 10.15: Catalina or greater.

Xerox® Workplace App for Chrome

This appendix contains:

Workplace App Settings for Google Chrome.....	336
Uploading the Xerox® Mobile Print Portal App Chrome Configuration File.....	337

This section describes the administration of the Xerox® Workplace App for Chrome. This information applies only when you use the Google Admin Console to manage users and settings.

Workplace App Settings for Google Chrome

SETTING	DESCRIPTION
DefaultServiceURL ; a 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, when students can use only designated student printers, and cannot add printers, select No.
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 release to the Xerox® EIP printer client for mobile printing.
Printers (List) Default: None	Displays a list of printers where you can select the default printer. For mobile app users, the 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, the feature 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, the feature eliminates the need to remember the user ID and passcode.
SingleSignOn (Yes/No) Default: No	If the Xerox® Workplace Cloud software supports this feature, this option requires the client to use Google Single Sign-on.

Uploading the Xerox® Mobile Print Portal 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 Mobile Print Portal 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?authuser=0#differences>.

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 Xerox Mobile Print Portal App, scroll the page.



Note: The configuration values for the Xerox Mobile Print Portal 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 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" },  
  ]  
}  
}
```


EFI Fiery® Controller

This appendix contains:

- Xerox® Workplace Cloud for Xerox® Printers with an EFI Fiery Controller 344
- Setting up the EFI fiery Custom Drivers for Mac Client 347
- Setting up the EFI Fiery Custom Drivers for Windows Desktop Client 349

Xerox® Workplace Cloud for Xerox® Printers with an EFI Fiery Controller

The EFI Fiery controller is an optional print controller that you configure for use with Xerox® PrimeLink® C9065/C9070 printers and Xerox® Color C60/C70 printers. The EFI Fiery controller uses the Raw protocol on port 9100. You can connect the EFI Fiery controller to the network, then connect the controller to the printer using one of the following configurations:

- Direct Configuration
- Network Hub Configuration

Direct Configuration

With this option, only the EFI Fiery controller is connected to the network. The printer is connected to the EFI Fiery controller, but the printer is isolated from the network. Sometimes referred to as the Single IP mode.

Network Hub Configuration

The printer and the EFI Fiery controller each have an IP address. The printer and controller connect to the network independently of each other. Sometimes referred to as the Dual IP mode.

Printing

For both configurations there are workflows for where you want the job to be sent to either to the Fiery Controller or directly to the Printer.

Driver setup when Printing to the Fiery

If you want to print to the Fiery controller directly, you will be using the Workplace Cloud Client for Windows and Macintosh. For both configurations, you will need to setup the drivers.

DIRECT CONFIGURATION SETUP

EFI Fiery Setup

Configure the EFI Fiery Controller as follows:

1. In a Web browser, type the IP address for the EFI Fiery controller.
2. Select the Configure tab. At the prompt, log in as an administrator.
3. Click **Network > Setup**.
4. For the Security level, select **Minimum**. This setting allows Set/Write requests and Get/Read requests.
5. Set the SNMP Community Names:
 - a. For Write Community Name, type `private`. EIP applications use private as the community string for Set requests. Ensure that this setting is identical for Xerox® Workplace Cloud, the Xerox printer, and the EFI Fiery controller.
 - b. For Read Community Name, type `public`. Ensure that this setting is identical for Xerox® Workplace Cloud, the Xerox printer, and the EFI Fiery controller.



Note: The community Set/Write and Get/Read names can be any string. Ensure that the string name is the same for Xerox® Workplace Cloud, the Xerox printer, and the EFI Fiery controller.

Adding the Printer

1. In a supported Web browser, log in to Xerox® Workplace Cloud.
2. Select the **Agents** tab. To view details, select an agent.
3. Select the **Discovery Settings** tab, then select **Add**.
4. Type the IP address of the EFI Fiery controller.



Note: Do not use the IP address of the printer.

5. Click **Save**, then exit the **Discovery Settings**.
6. Return to the **Agents** tab. In the search field, type **Agents**.
7. Click the **Printers** tab. Ensure that the printer appears in the list.

Xerox® Workplace Cloud and EFI Fiery Direct Configuration Printer Setup

1. In a supported Web browser, log in to Xerox® Workplace Cloud.
2. Select the **Printers** tab, then select the target printer.
3. If you want print Jobs to print directly to the Printer, in the Detail area about the printer, change the protocols to **Raw TCP Port**. For Port Number, type 9200.
4. If you want print Jobs to print to the Fiery Controller, in the Detail area about the printer, change the protocols to **Raw TCP Port**. For Port Number, type 9100, the default value.



Note: When you print the non-desktop jobs from the Printer EIP Client to the fiery, some of the printing options will not work because Cloud uses the Xerox Global Printer Driver to convert these jobs.

5. To save the change, click **Save**.
6. Select the **Feature** tab, then make changes to the options, as needed:
 - **Client Application Installation**
 - **Authentication**
 - **Auto Release All Jobs**
 - **Set Usage Tracking Model**, also known as Network Accounting

NETWORK HUB CONFIGURATION SETUP

EFI Fiery Setup

In the Network Hub Configuration setup, nothing has to be configured on the Fiery.

Adding the Printer

1. In a supported Web browser, log in to Xerox® Workplace Cloud.
2. Select the **Agents** tab. To view details, select an agent.
3. Select the **Discovery Settings** tab, then select **Add**.

4. Type the IP address of the EFI Fiery controller.



Note: Do not use the IP address of the printer.

5. Click **Save**, then exit the **Discovery Settings**.
6. Return to the **Agents** tab. In the search field, type Agents.
7. Click the **Printers** tab. Ensure that the printer appears in the list.

Xerox® Workplace Cloud and EFI Fiery Network Hub Configuration Setup

1. In a supported Web browser, log in to Xerox® Workplace Cloud.
2. Select the **Printers** tab, then select the target printer.
3. If you want print Jobs to print directly to the Printer, there are no settings required.
4. If you want print Jobs to print to the Fiery Controller, enable the setting Printing to Alternate IP Address, then enter the IP Address of the Fiery Controller in the IP address field.
5. To save the change, click **Save**.
6. Select the **Feature** tab, then make changes to the options, as needed:
 - **Client Application Installation**
 - **Authentication**
 - **Auto Release All Jobs**
 - **Set Usage Tracking Model**, also known as Network Accounting

Setting up the Drivers for the Macintosh Cloud Desktop Client

You can print Jobs to the Fiery Controller by using the EFI Fiery Driver. To set up the EFI fiery driver for Macintosh Cloud Desktop Client refer to [Setting up the EFI fiery Custom Drivers for Mac Client](#).



Note: You can also print Jobs directly to the printer, this should happen automatically because the Mac client uses the Xerox MAC Universal Print Driver by default.

Setting up the Drivers for the Windows Cloud Desktop Client

You can print Jobs to the Fiery Controller by using the EFI Fiery Driver. To set up the EFI fiery driver for the Windows Cloud Desktop Client refer to [Setting up the EFI Fiery Custom Drivers for Windows Desktop Client](#).



Note: You can also print Jobs directly to the printer, this should happen automatically with the help of Xerox Global Print Driver by default.

Setting up the EFI fiery Custom Drivers for Mac Client

ENABLING THE WORKPLACE CLOUD MAC CLIENT WITH THE FIERY CONTROLLER

Installing the Xerox Workplace Cloud Client MAC



Note: Jobs sent via the MAC client utilize the Fiery Driver, so Job programming is embedded in the Job.

1. Select **Print** tab then select **Desktop** tab.
2. In Install the Workplace Cloud Client, select **Mac**.
The Mac Client will download.
3. Install the Mac Client.
4. After you install the Mac Client, sign into the client.

Installing the Fiery Driver and Preparing the PPD for the Mac Client.

- Install the Fiery Driver version that matches the Fiery Controller you normally use.
- When installing the fiery driver, you can select install Driver only.

To prepare the PPD file, do the instructions to GZIP and copy the fiery ppd file:

1. When the drivers are installed, navigate to `/Library/Printers/PPDs/Content/Resources/`.
2. In the Resources folder, navigate to the language folder that you want the driver to use.
3. Copy the PPD file to a folder on your desktop.
4. To start a Mac Terminal window:
 - a. Click **Go > Utilities** from the menu bar.
 - b. In the Utilities folder, double-click **Terminal**.
5. From the Terminal window, go to the folder that you created on your Desktop. For example, type `cd /Users/<username>/Desktop/<Folder you created>`.
6. Create the GZIP PPD file. Run this GZIP command in the Terminal window. Example Command: **gzip -keep Xerox\ EX-i\ C60-C70\ Printer gzip**, keep <PPD File name use "\" to add spaces>
7. Now copy the GZIP PPD file you just created to this folder: `/Library/Printers/PPDs/Content/Resources/`.

Creating the Xerox®Workplace Client Desktop Follow Print Queue

1. On the Xerox®Workplace Cloud Web site, go to **Account > Settings > Desktop Printing**.
2. Select **Actions > New**, then unselect **Windows**.
3. Select **MAC**, then enter the driver name. This is the Administrative Printer Driver Name..
4. Enter PPD name, this name must match the same name of the PPD GZIP file you created without the “.gz” extension. Example of PPD Names : “Xerox EX-i C60-C70” Printer or “Xerox EX C60-C70 Printer”

5. Enter the printer name, this is the name of the generic upload printer end user will see.
6. Select **Enable**.
7. Select **Save**.

This will create a Mac Fiery Follow you print Queue.

Enabling the Printer to Release the Job to the Fiery Controller

1. From Xerox®Workplace Cloud, add and enable the printer that is connected to the Fiery Controller.
2. When the printer has been enabled, select the **Printer**.
3. Change the Protocol to “LPR/LPD”.
4. Go to the Printing to Alternate IP Address.
5. Enable the setting **Print to Alternate IP Address**.
6. Enter the IP address of the Fiery Controller.

Enabling the Printers on the Cloud MAC Client

1. From the MAC computer, ensure that you are logged into the MAC Cloud Client.
2. From the MAC Cloud Client, select **Sync Print Queues**.

The Fiery Desktop Follow Print Queue should automatically be created.

Setting up the EFI Fiery Custom Drivers for Windows Desktop Client

To create a Custom Driver using the Fiery Driver in Workplace Cloud, user needs:

- 32 and 64 Bit Fiery Driver
- Windows Print Management Tool, which is usually part of the OS
- 7-ZIP, zip program

PREPARING THE FIERY CUSTOM DRIVER

1. Install the Fiery Driver on a 32 and/or 64 bit OS. It is recommended to use windows 10 for 64 bit and Windows 7 for 32 bit.
2. After the Driver is installed, run the **Print Management** tool on your hard drive.
3. On the **Print Management** from the **Print Servers** drop down menu, click on **Drivers**.
4. Select the Fiery Driver which you have installed and scroll to the right on the tool, until you reach the **Inf Path** column.
5. Take the note of the Inf Path location.
This is the location from where you will copy the files to create the new Fiery Custom Driver.
6. Create a new folder on your hard drive and name it by the Fiery Driver file name which you have downloaded and installed.
7. Create a new folder inside the Fiery Driver folder which you have created and name it by X86 for 32bit.
8. Navigate to the Inf Path location and copy the files of the folder to X86 folder.
9. Do the steps from 2–8 for 64 bit OS.
10. Zip the X64 and X86 folders separately.
11. Preparing the DriverMetaData.xml:
 - a. Login to the Xerox Workplace Cloud application.
 - b. Go to **Account > Settings > Desktop Client**.
 - c. Under Custom Drivers menu, select **Actions > New**.
Upload Custom Driver Page appears.
 - d. Download the **DriverMetaData.xml** file under the **Select Driver** option.
 - e. Copy the **DriverMetaData.xml** file and paste it In the Fiery Driver folder which is created on your hard ware.
 - f. Open the **DriverMetaData.xml** in the Notepad and do the following action:
 - g. Rename the Manufacturer name as required at <Manufacturer>Manufacturer Name</Manufacturer>.
 - h. Rename the Model Name as required at <Model>Model Name</Model>.
 - i. Rename the Zip file Name as X86.zip at <ZipFile>ZipFile Name</ZipFile>.
 - j. Rename the InfFile Name at <InfFile>Inffile Name</InfFile> with the .inf file name present in your x86 zip folder.

- k. Rename the CatalogFile Name at <CatalogFile>CatalogFile Name</CatalogFile> with the .cat file name present in your x86 zip folder.
- l. Do the steps from i–k for X64.
- m. Save the **DriverMetaData.xml** file.



Note: DriverMetaData.xml file helps the user to upload the Fiery Custom Driver successfully on Xerox Workplace Cloud application. You can skip the attachment of DriverMetaData.xml file if there are no errors in uploading the drivers.

- 12. Select files X64, X86 and **DriverMetaData.xml**, and Zip them.
- 13. Rename the zipped folder with respect to your Fiery Driver folder name.

Fiery Custom Driver file is ready to upload in Custom Driver.



Note: To Upload and Enable the Fiery Custom Driver refer to **Custom Drivers** section.

Login Methods Using the Xerox® Workplace Mobile App

This appendix contains:

Logging in to a Printer Using a QR Code..... 352


Unlocking the Printer Using Native Camera 353

Logging in to a Printer Using Manual Code Entry 354

Logging into the @PrintByXerox App using a QR Code 355

Logging in to a Printer Using NFC 356

The log in methods available from the Xerox® Workplace Mobile App include:

 Note: Some of the methods allow you to login into the Printer or the @PrintByXerox App, see the details as follows.

- The ability to log in to the Printer using a QR Code.
- The ability to unlock the printer and facilitate the installation of mobile application, IOS, and Android using QR Code.
- The ability to log in to the Printer using a 4-digit Code.
- The ability to log in into the @PrintByXerox App using a QR Code.
- 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

You have to enable the QR Code Unlock with Workplace Mobile App feature, for more information, refer to [QR Code Unlock with Workplace Mobile App](#).

To log in to a multifunction printer using a QR Code:

1. Start the Xerox® Workplace Cloud Mobile App.
2. On a Xerox® AltaLink® printer, scan the QR Code on the printer Login Screen or the printed unlock QR code label.
3. On a VersaLink® printer, scan the QR Code on your printed Welcome to Xerox Workplace Cloud page or the QR Code Label.



Note: If you want to login using the Native Camera by scanning the QR code, refer to [Unlocking the Printer Using Native Camera](#).

Unlocking the Printer Using Native Camera



Note: This feature only works if the **Allow Mobile Unlock Using Native Camera** setting is enabled, refer to [Allow Mobile Unlock Using Native Camera](#)

1. Scan the QR code that is on the blocking screen or the QR Code label attached to the printer using the Native Camera application on your Android or IOS device.
2. If the Xerox® Workplace App is not installed in the mobile device, it redirects you to the Play Store or Apple Store respectively.

The page opens the Xerox® Workplace application install page in the Play Store or Apple Store.

3. If the Xerox® Workplace App is installed, then it opens the Workplace Application.
 - a. If the User is not signed in on the App, it will prompt for sign in. Once signed in, the solution will automatically proceed with the unlock call to unlock the device.
 - b. If the User is signed in, it performs an unlock call to unlock the device.

Logging in to a Printer Using Manual Code Entry

You have to enable the 4-Digit Code Unlock with Workplace Mobile App feature, for more details, refer to [4-Digit Code Unlock with Workplace Mobile App](#).

1. Log in to the Workplace Mobile App.
2. Select the Settings indicator, which appears on the screen as three bars.
3. Click **Settings**.
4. Click **Unlock Printer**.
5. Enter the code shown from the blocking screen of the printer into the Workplace Mobile App.

The printer details appear.

6. Click **Unlock**.

A message displays on the app that the printer is unlocked.

7. When the blocking screen is removed from the multifunction printer, access the printer.



Caution: When your printing is complete, to ensure that other users cannot access your documents, always log out.



Note: For more details, refer to the *Xerox® Workplace Mobile App Quick Start Guide*.

Logging into the @PrintByXerox App using a QR Code

If QR code scan has to be prompted, you have to enable the Client Application Authentication(@PrintByXerox Login) settings. For more information, contact your account administrator. Users have to supply their login credentials or they can use the Xerox® Workplace Mobile App to scan the QR Code shown in the client application of the printer.

The @PrintByXerox login option has to be enabled in order to be prompted to scan the QR Code.

1. Go to a Xerox® Workplace Cloud-enabled printer with the @PrintByXerox app.
2. Select the @PrintByXerox app on the printer. The app displays a QR code on the home screen.
3. Open the Xerox® Workplace Mobile App on your mobile device and select **@PrintByXerox Login**.



Note: Alternatively, you can set the @PrintByXerox Login scanning screen as the default screen on your app by selecting **My Preferences**.

4. Scan the QR code on the printer with your mobile device.
5. Select a job or jobs to print.

Logging in to a Printer Using NFC



Note: Devices that support Near Field Communication (NFC) are Android devices, and iOS version 13.0, iPhone 7, or newer devices.

Verify that you are using a NFC enabled mobile device and that NFC functionality is turned On. Also, make sure that the printer you are trying to unlock has NFC capabilities.

1. Locate the card reader device at the printer.
2. Take your mobile device and move it within 4 cm NFC enabled card reader on the printer.
3. You will hear a beep once your mobile device is recognized by the reader.
4. You will now be logged into the printer and will be able to access the @PrintByXerox application.



Note: If this is your first time using this mobile device to unlock a Xerox printer, you will have to register using your company username and password when prompted by the printer's user interface.

5. The printer user interface will prompt you to enter your email address and password.
6. After entering your email address and password, you will now be logged into the printer and should be able to access the @PrintByXerox application.



Note: The next time you use your mobile device with any Xerox printer at your company you will be immediately logged into the printer after swiping your mobile device within 2 inches of the NFC enabled card reader.

ENABLING NFC ON ALTALINK® DEVICES

1. Navigate to device IP webpage.
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**.

DELETING REGISTERED NFC CAPABLE MOBILE DEVICES FROM MY USER PROFILE

In order to delete a registered device from your user profile, you will have to log into the Xerox® Workplace Cloud Web Portal.

1. Log into the Xerox® Workplace Cloud Web Portal at <https://xwc.services.xerox.com>.
2. Under the company name in the top right corner of the home page, click on your username or email.
3. Click the **Set Card Information** button.
4. Click the **Delete User Devices** button.
5. Click **OK**.

Configuring Authentication

This appendix contains:

- Enabling Cardless Authentication and Card Authentication..... 360
- Using an ID Card to Unlock a Printer 362
- Deleting ID Card Information for My User Profile Using the Xerox® Workplace Cloud Web Portal..... 363

Enabling Cardless Authentication and Card Authentication



Note: If you are using an Cloud Agent for authentication, ensure that the Proxy Bypass setting includes the Agent IP address.



Cardless Authentication is the ability to control access to the UI functions and require users to log in to a Xerox Multifunction Printer without having to use a physical access key card.

Card Authentication is the ability to control access to the UI functions and require users to swipe an access key card at the Multifunction Printer to gain access.

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

The Account Administrator can lock a Multifunction Printer and require authentication. The Agent communicates with the device to lock the UI.

Requirements for this feature:

- Devices must support Cardless Authentication. For the latest list, refer to <http://www.office.xerox.com/software-solutions/xerox-workplace-cloud/enus.html>.
 - This feature is only available with Xerox® Workplace Cloud Device Pack licenses. For instructions, refer to [Activating Xerox® Workplace Cloud Licenses](#). Cardless Authentication is not available in accounts that have Job License.
 - Xerox® Workplace Cloud Agent software must be installed and must discover the Multifunction Printer.
 - The device must be enabled.
 - The Agent PC must have a static IP address in accounts that will be using Cardless Authentication.
1. Log in as an administrator to the web portal at <https://xwc.services.xerox.com>.
 2. Click the **Printers** tab and select a printer. You can use the **Search** box to find your printer by name or IP address.
 3. Select the **Actions** menu.
 4. Select **Set Cardless Authentication Mode**. Choices include:
 - **Do not modify** : Do not write this setting to the device. This tells the system not to use Xerox® Workplace Cloud Cardless Authentication. If there is existing Cardless Authentication set, such as Xerox Secure Access, it will continue to be in effect.
 - **Disabled**: Credentials are not required to access the console on the device. This tells the system to use Cardless Authentication to manage printer access and leave the printer unlocked.
-  Note: This will overwrite any existing Cardless Authentication setting currently on the printer.
- **Enabled**: Credentials are required to access the console on the device. This tells the system to use Cardless Authentication to manage printer access and lock the printer.
-  Note: This will overwrite any existing Cardless Authentication setting currently on the printer.

5. Select **Set Cardless Authentication Mode**.

The operation takes time, so feedback on its success or failure will not be immediate.

You can also set the Cardless Authentication mode on the **Printers > Features** tab.

Using an ID Card to Unlock a Printer

Swipe your ID badge next to the printer ID card reader device until you hear a beep indicating that the ID card was successfully read by the card reader.

1. Locate the card reader device at the printer.
2. Take your ID card move it within 4 cm of the printer's card reader.
3. You will hear a beep once your ID card is recognized by the reader.
4. You will now be logged into the printer and will be able to access the @PrintByXerox application.



Note: If this is your first time using your ID card to unlock a Xerox printer, you will have to register using your company username and password when prompted by the printer's user interface.

5. The printer's user interface will prompt you to enter your email address and password.



Note: The next time you use your ID card with any Xerox printer at your company, you will be immediately logged into the printer after you swipe your ID card within 4 cm of the card reader on the printer.

Deleting ID Card Information for My User Profile Using the Xerox® Workplace Cloud Web Portal

In order to delete an ID card from your user profile, you will have to log into the Xerox® Workplace Cloud Web Portal.

1. Log into the Xerox® Workplace Cloud Web Portal <https://xwc.services.xerox.com>.
2. Under the company name in the top right corner of the home page, click on your username or email.
3. Delete the ID card identification information from the Default Card text box.
4. Click **OK**.

Setting Up the DNS-SD for iOS Native Printing

This appendix contains:

Setting Up the DNS-SD for iOS Native Printing 366

Setting Up the DNS-SD for iOS Native Printing

INTRODUCTION TO DNS-SD FOR IOS NATIVE PRINTING

Purpose of this section

This section will help you advertise a service called “Upload to Xerox® Workplace Cloud” for all users in a large enterprise network.

When a Xerox® Workplace Cloud Agent is installed and enabled to use iOS Native Printing with automatic discovery turned on, any iOS 13.0 and higher mobile device connected to the same subnet will be able to discover the Xerox® Workplace Cloud Agent and upload documents to the cloud. For larger networks, it may not be suitable to install an agent per subnet. In order to advertise the Xerox® Workplace Cloud Agent on all WiFi subnets for mobile devices on the WiFi, the network administrator must configure the following DNS-SD solution.

What is DNS-SD

Domain Name System - Service Discovery (DNS-SD) is a solution that uses normal DNS queries to discover services on a network. For additional information go to: <http://dns-sd.org/>

To implement the DNS-SD solution, the network administrator must add several DNS records to the DNS server of the company and may be required to make additional changes on the DHCP server configuring WLAN clients. Refer to [Configuring a DHCP Server](#).

When do I need DNS-SD?

Set up the DNS-SD solution if you:

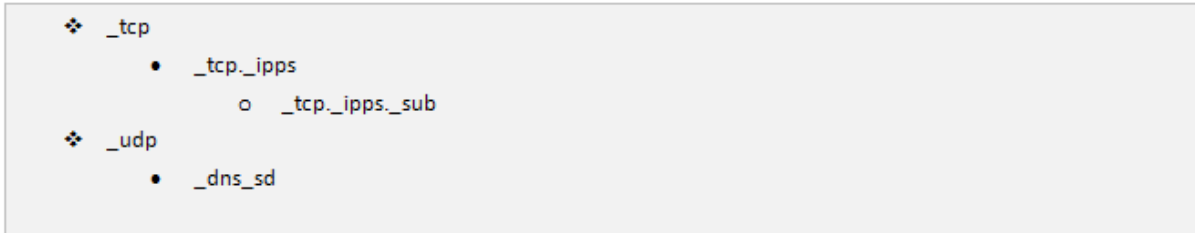
- have a WLAN subnet that is different from your LAN subnet
- want better control over what is displayed in your clients
- want to control the services advertised in your subnets

CONFIGURING THE MICROSOFT® WINDOWS® DNS SERVER

This procedure explains how to configure the Microsoft® Windows® DNS Server to achieve DNS-SD. The following example uses the domain name **internal.xcp** to illustrate changes.

DNS Zone

1. Identify the DNS Zone that will serve the Xerox® Workplace Cloud Agent. In **DNS Manager > Forward Lookup Zones**, create a new primary zone called: **print.internal.xcp**
2. Create the following domains:

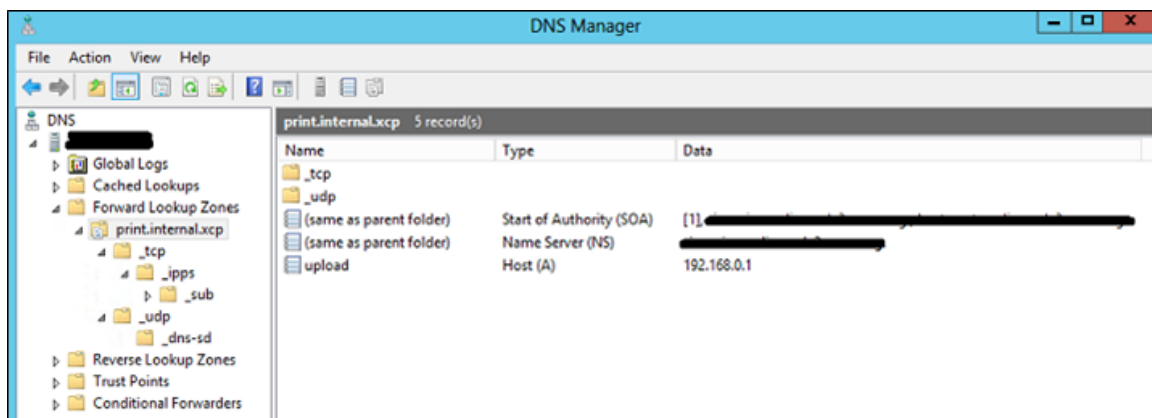


Record for the Xerox® Workplace Cloud Agent Machine

It is necessary to give a fully qualified DNS name to the machine that hosts the Xerox® Workplace Cloud Agent. If this machine is not associated already with a name:

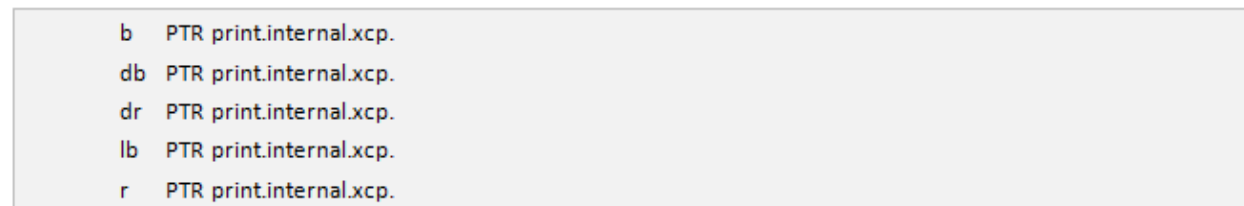
- Create one A entry in the print.internal.xcp zone with the IP address of the machine hosting the Xerox® Workplace Cloud Agent. In the example it is called `upload`.
- This machine will now be resolved if called `upload.print.internal.xcp`. Keep this information for future reference. You do not need this if your machine already has a fully qualified DNS name.

DNS SD Domain Structure



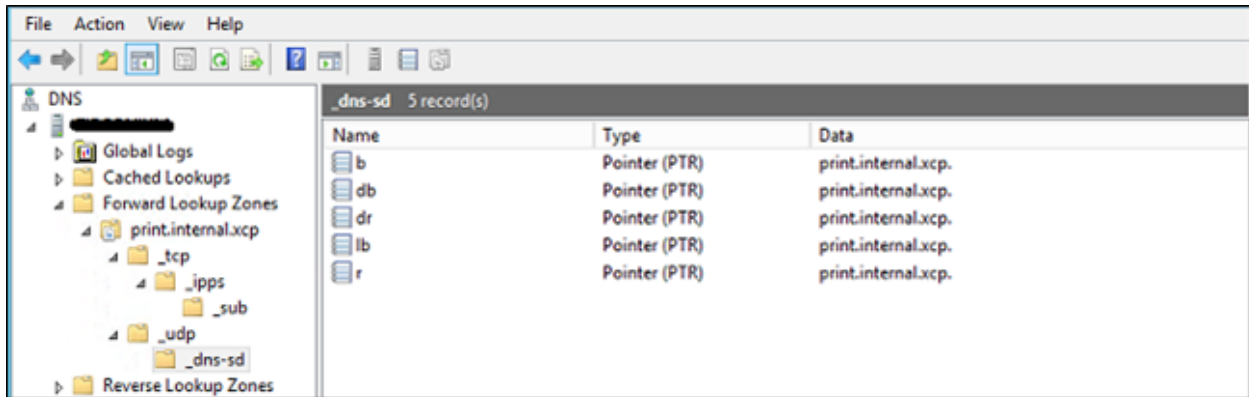
Records for DNS-SD

Add the following PTR records to the `_udp._dns-sd` domain:



The result can look like this:

DNS-SD Records



Records for the Xerox® Workplace Cloud Agent Service

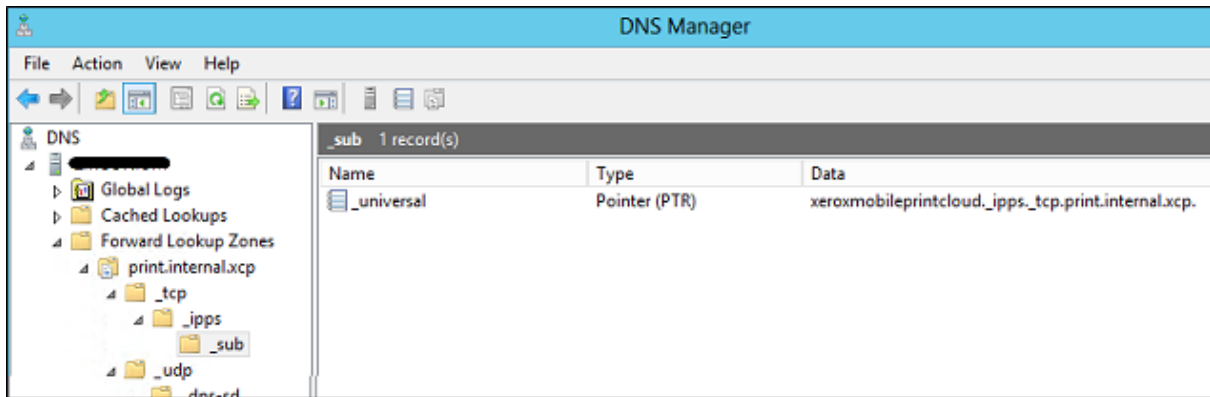
Choose a name with no spaces or non-ASCII characters for your upload service.

The following uses Xerox Workplace Cloud as an example.

1. In the `_tcp._ipps._sub` domain, add the following record:

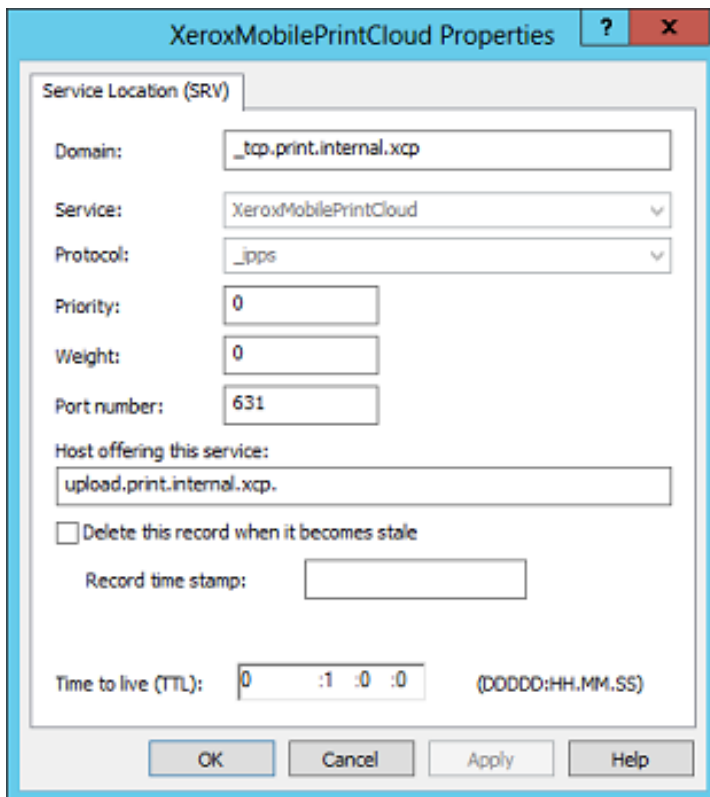
`_universal PTR xeroxmobileprintcloud._ipps.tcp.print.internal.xcp`

Universal Sub Type DNS Record



2. In the `_tcp` domain, add the following SRV record: `xeroxmobileprintcloud SRV 0 0 631 upload.print.internal.xcp.`, but replace `upload.print.internal.xcp` with the fully qualified domain name of your agent machine as set in the Record for the Xerox Workplace Cloud Agent Machine section above.


Creating the SRV Record



3. In the `_tcp._ipps` domain, add the records:

```
.PTR xeroxmobileprintcloud._ipps._tcp.print.internal.xcp.  
xeroxmobileprintcloudTXT
```

(Refer the following for text data)

 Note: Text for the text record must be in the following format.

```
txtvers=1  
qtotal=1  
priority=0  
ty=Xerox Mobile Print Cloud  
product=(Xerox Mobile Print Cloud)  
pdl=application/pdf,image/jpeg,image/urf,image/pwg-raster  
adminurl=https://xmpc.services.xerox.com  
TLS=1.2  
UUID=af3ad2b9-6920-491f-a924-89b22ac23874  
Duplex=T  
Color=T  
URF=V1.3,CP255,OB10,IS1,IFUO,DMI,FN3-4,PQ3-4-5,SRGB24,RS300-60  
kind=document, envelope, label, photo  
PaperMax=legal-A4  
rp=XeroxIPPPrintQueue1
```

CONFIGURING A BIND SERVER

This procedure explains how to configure a BIND Server to achieve DNS-SD.

DNS Zone

1. Locate your BIND server.
2. Add a new primary zone. This is usually configured in `/etc/bind/named.conf` or its dependencies, such as `/etc/bind/named.conf.default-zones`

```
zone "print.internal.xcp" IN {  
    type master;  
    file "/etc/bind/db.print.internal.xcp";  
};
```

Zone File Creation - DNS Records

1. Create the file for: `/etc/bind/db.print.internal.xcp`

```
$ORIGIN print.internal.xcp.
b._dns-sd._udp.print.internal.xcp.    IN PTR print.internal.xcp.
r._dns-sd._udp.print.internal.xcp.    IN PTR print.internal.xcp.
lb._dns-sd._udp.print.internal.xcp.    IN PTR print.internal.xcp.
db._dns-sd._udp.print.internal.xcp.    IN PTR print.internal.xcp.
dr._dns-sd._udp.print.internal.xcp.    IN PTR print.internal.xcp.
```

2. If your agent machine has a fully qualified DNS name, go to the next step. Otherwise add a fully qualified name and change the IP address to the IP address of your agent machine.

```
upload A 192.168.0.1
```

3. Choose a name for your printer. If you are using non-ASCII characters or spaces, prefix the Unicode with a back slash (\).
 - The TXT record should be on one line.
 - Add spaces between different values.
 - The SRV record highlight should match the fully qualified DNS name of your agent machine as defined above.



Note: The highlighted values can be changed.

```
_ipps._tcp PTR _ipps._tcp
_universal._sub._ipps._tcp PTR \226\152\129\032Xerox\032Mobile\032Print\032Cloud._ipps._tcp
\226\152\129\032Xerox\032Mobile\032Print\032Cloud._ipps._tcp SRV 0 0 631 upload.print.internal.xcp.
\226\152\129\032Xerox\032Mobile\032Print\032Cloud._ipps._tcp TXT "txtvers=1" "qtotal=1"
"pdI=application/pdf,image/jpeg,image/urf,image/pwg-raster" "TLS=1.2" "Duplex=T" "Color=T"
"URF=V1.3,CP255,OB10,IS1,IFU0,DM1,FN3-4,PQ3-4-5,SRGB24,RS300-60" "product=(Xerox Mobile Print Cloud
Printer)" "priority=0" "adminurl=https://xmpc.services.xerox.com" "rp=XeroxIPPPrintQueue1" "ty=Xerox
Mobile Print Cloud Printer" "note=Xerox Mobile Print Cloud Upload Agent/ Site Name"
```

CONFIGURING A DHCP SERVER

To find the new service, mobile devices must look for the service. When a mobile device joins a WLAN network, the device acquires network configuration information through a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server must be configured to send a search domain to its clients.

1. On a DHCP server configuration, the search domain is added as follows:

```
option domain-search "print.internal.xcp";
```

Mobile clients display the service in the search domain configuration. This is configured manually in the client.



2. To verify that the DHCP server is configured correctly with your mobile device, check that a new printer appears in the printer list on your mobile device.

FREQUENTLY ASKED QUESTIONS

1. What should I do if everything looks configured correctly, but the Xerox® Workplace Cloud Agent does not show up?
 - Check that the Xerox® Workplace Cloud Agent is up and running.
 - Make sure iOS Native Printing in the Agent is enabled.
 - The DNS cache on your mobile device may take some time to refresh, or require that you turn off and turn on the mobile device.
2. If I am using a Windows DNS server, can I change the icon?
 - The icon is represented as non-ASCII characters in the name and the interface does not provide a way to enter them.

User Profile

This appendix contains:

User Profile: User Profile 374

User Profile: User Preferences 376

User Profile: Single Sign-On 378

After you log in to the Web portal, in the upper right corner, select **User Profile**. The User Profile page appears, which shows the following information:

- **User Profile**
- **User Preferences**
- **Single Sign-On**

User Profile: User Profile

After you log in to the Web portal, in the upper right corner, select **User Name > User Profile**. The User Profile page appears, which shows the following information:

- User Information: You can view the following information in the User Information section:
 - Email Address
 - Username
 - Domain Name
 - User Principal Name
 - Alternate Access Card User
 - User Group
 - Default Card(s)
 - Generated PIN
 - User Device
- Print Quota: You can view the following information in the Print Quota section:
 - Last Modified Date and Time
 - Period
 - Enforced Quota
 - Remaining
- Print Limits: You can view the following information in the Print Limits section:
 - Total Page Limit
 - Color Page Limit
- My Companies: You can view your company codes associated with the account.

VIEWING AND DELETING YOUR REGISTERED CARDS

To view and delete your registered cards, do the following:

1. Log in to the Xerox® Workplace® Cloud Web portal using your user credentials.
2. In the upper-right corner of the screen, click your user name.
The User Options window appears.
3. Click **User Profile > User Information**.
Registered Cards: All your registered cards appear here.
To delete a card, click the delete icon.
4. To exit, click **Save**.

RESETTING YOUR GENERATED PIN

To reset your generated PIN, do the following:

1. Log in to the Xerox® Workplace® Cloud Web portal using your user credentials.
2. In the upper-right corner of the screen, click your user name.

The User Options window appears.

3. Click **User Profile > User Information**.

Generated PIN: When the user clicks the reset button, a new pin will be generated.

User Profile: User Preferences

After you log in to the Web portal, in the upper right corner, select **User Name > User Preferences**. The User Preferences page appears, where you can view and edit the following information:

- Email Notification Policy
- Retention Policy
- Print Preferences
- Document Release Order

CONFIGURING YOUR EMAIL NOTIFICATION POLICY

To manage the criteria for receiving emails from the Xerox® Workplace Cloud notification service, users can configure the notification policy for their account.



Note: For all new accounts created after the release of Xerox Workplace Cloud version 5.2, the notification policy is set to Failure Notifications Only by default.

To configure the notification policy for a user account:

1. Log in to the Xerox® Workplace Cloud Web Portal.
2. To access User Preferences, in the top-right corner of the home screen, click the email address of the logged-in user, then click **User Preferences**.
3. To set the email notification policy, for Print Job Submission and Print Job Completion, select an option:
 - **Receive All Notification:** This option instructs the Xerox® Workplace Cloud notification service to send an email notification for all successful and failed print jobs.
 - **Receive Failure Notifications Only:** This option instructs the Xerox® Workplace Cloud notification service to send an email notification for failed print jobs only.
 - **None:** This option instructs the Xerox® Workplace Cloud notification service not to send any email notifications.
4. To save the settings, click **Save**.

A notification appears that confirms that the settings are saved.

CONFIGURING YOUR RETENTION POLICY

You can set a job-retention period for your print jobs. You can set your jobs for removal from the document list after printing, to display a warning message for user interaction, or to retain the job for 1–3 days after printing, refer to [Data Retention Policy](#).

CONFIGURING YOUR PRINT PREFERENCES



Note: Depending on the capabilities of the printer, and the policies set by the administrator, Print Preferences are overridden at print time.

To set the print preferences to your document, select one of the following check boxes:

- Color
- 2 Sided Printing
- Staple

SETTING YOUR DOCUMENT RELEASE ORDER

To set the document release order for your user account, do the following:

1. Log in to the Xerox® Workplace Cloud Web Portal using your user credentials.
2. In the upper right corner of the screen, click your user name.

The User Options window appears.

3. Select **User Preferences**.
4. In the Document Release Order area, select one of the following options:

- **Maximize Performance**
- **Enforce job order**

For more information on these options, refer to [Document Release Order](#).

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

User Profile: Single Sign-On

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 **User Profile**.
The User Profile page appears.
3. Select **Single Sign-On**
The Single Sign-On Settings page appears..
4. From the Actions menu, click **Reset**.

Remove Workplace Cloud from your Environment

This appendix contains:

Remove Workplace Cloud from your Environment 380

Remove Workplace Cloud from your Environment

To remove Workplace Cloud from your environment, do the following steps:

1. Disable the Printer Authentication, refer to [Set Authentication Mode](#).
Disabling the Authentication will set the printer to local authentication mode.
2. Remove the @PrintByXerox app from the printers, refer to [Set Client Application Installation Mode](#).
3. Disable the Usage Tracking if currently enabled, refer to [Enable or Disable Set Usage Tracking Mode](#).
4. Disable all the printers from the Workplace Cloud, refer to [Enable or Disable Printer](#).
5. Remove all the printers from the Workplace Cloud, refer to [Removing Selected Printers from the Printer List](#).
6. Remove all the Agents from the **Agents** tab, refer to [Deleting an Agent](#).
7. Remove the Agent application from all the computers on which it is running.
8. Delete all the users from the Users tab, refer to [Remove User](#).

