



Kofax Unified Client for Xerox Getting Started Guide

Version: 1.1.0

Date: 2023-03-23

KOFAX

© 2023 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Table of Contents

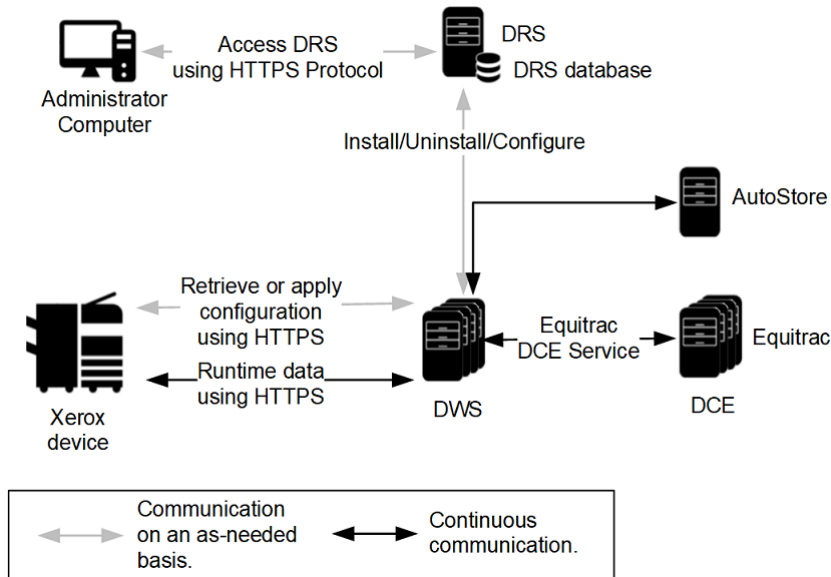
Chapter 1: About Kofax Unified Client for Xerox.....	4
Chapter 2: Before you begin.....	6
Prerequisites.....	6
DRS and Unified Client communication ports.....	7
Supported card readers.....	7
Chapter 3: Configure DRS.....	9
DRS setup and device registration.....	9
Chapter 4: Additional information.....	12
Product documentation.....	12
Troubleshooting the Unified Client for Xerox.....	12
Device registration issues.....	12
Connection error issues.....	13
Scan issues.....	13
Print issues.....	13
Job tracking issues.....	13
Customization issues.....	13
Error messages.....	13

Chapter 1

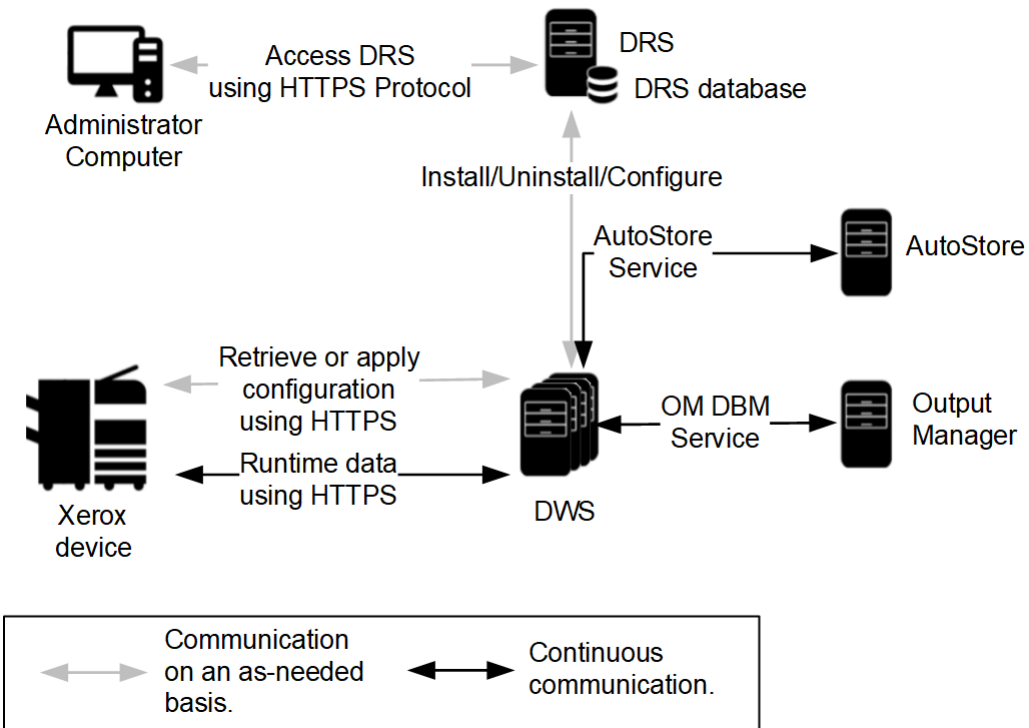
About Kofax Unified Client for Xerox

The Unified Client for Xerox adds print and capture capabilities to Xerox devices through AutoStore, Equitrac, and Output Manager while still using device-specific features. See the [Unified Client for Xerox Release Notes](#) for information about new features.

The Unified Client for Xerox connects with the rest of ControlSuite in an Equitrac configuration as shown in this diagram.



When used in an Output Manager configuration, the Unified Client for Xerox connects with the rest of ControlSuite as shown.



Chapter 2

Before you begin

Prerequisites

Before you begin, make sure the following requirements are met.

Use the following links to view the technical specifications and minimum requirements for each of the ControlSuite components. Specific requirements depend on the number of servers in a deployment, operating systems, expected production volume, and other applications in the environment.

- [AutoStore](#)
- [Equitrac](#)
- [Output Manager](#)
- [DRS](#)
- [DWS](#)

For steps to prepare

Check	Description
<input type="checkbox"/>	Verify that your device is supported. For the latest list of supported Xerox models, consult your local Xerox representative or see the MFD & Productivity Supported Devices Information page.
<input type="checkbox"/>	Verify that the server machine is a member of a domain.
<input type="checkbox"/>	Verify that you have Administrative access rights to Windows on the server.
<input type="checkbox"/>	Check that all important Windows updates are installed.
<input type="checkbox"/>	Verify that Microsoft Windows Updates is turned on while you are deploying AutoStore, which is required to install Microsoft Windows Identity Foundation (TFS).
<input type="checkbox"/>	Ensure that Windows Identity Foundation 3.5 is installed on the server (launch Server Manager > Local Server and verify that Windows Identity Foundation 3.5 is listed under Roles and Features).
<input type="checkbox"/>	Verify that IE Enhanced Security Configuration is turned off for Administrators in IE Enhanced Security Configuration (to access this, go to Server Manager > Local Server).
<input type="checkbox"/>	Verify that you have Administrative access to the device.
<input type="checkbox"/>	Verify that you have supported card readers. See Supported card readers .

Check	Description
<input type="checkbox"/>	Verify that you have configured components, devices, and card readers to work with Unified Client for Xerox. See the Prepare for deployment of Unified Client for Xerox section of the <i>ControlSuite Help</i> .

DRS and Unified Client communication ports

The following table provides general information on ports and protocols for the DRS server and the Kofax Unified Client for Xerox.

Component	Device display menu protocol	Device file transport protocol	Default communication port	Port configurable	Required device components
DRS server	HTTP, HTTPS	HTTP, HTTPS	8753: Web server 8755: REST-based web service 9000: Client server 9000: Web client	Yes	
Kofax Unified Client for Xerox	HTTP, HTTPS	HTTP, HTTPS	80: HTTP port for connections to the device 443: Secure port for HTTP, TLS, and SSL communications 2939: Equitrac application port 8068: Default port for AutoStore and Print Manager if TLS is not used. 8069: Default port for AutoStore and Print Manager if TLS is used. 8443: Root CA certificate for other used by other ControlSuite clients 8444: Root CA certificate for Kofax Unified Client for Xerox		

Supported card readers

The Kofax Unified Client for Xerox supports the following card readers.

Kofax card readers


- Kofax Micro Card Reader

- Kofax Equitrac ID Card Reader

The Kofax Unified Client for Xerox has also been tested with the following card readers.

Third-party card readers

- Elatec TWN3
- Elatec TWN4
- RFIDEas pcProx RDR-7L81AKU
- RFIDEas pcProx RDR-80581AKU
- Custom

 When a third-party card reader is used, a third-party card reader license is required.

Chapter 3

Configure DRS

DRS setup and device registration

Set up DRS and create an application for the Unified Client for Xerox. Before you begin, note the following:

- Make sure you have administrative credentials for the device.
- Make sure the device is not in an error state (such as from a paper jam or out of paper) before registering or unregistering the client on it. If the device is in an error state, registration or unregistration will fail.
- The Unified Client for Xerox, when configured as the authentication agent, cannot coexist with another embedded client on the device that is also handling authentication. This includes the Kofax Combined Client for Xerox, Kofax Equitrac ECSP Client for Xerox, and Kofax EIP Client for Xerox. Unregister any embedded client that is configured as an authentication agent before registering the Unified Client for Xerox.

The ControlSuite server can support multiple Kofax embedded solutions for Xerox. So, it can support certain Xerox devices running the Unified Client for Xerox and other Xerox devices running with other Kofax embedded clients, such as Kofax Combined Client for Xerox, Kofax Equitrac ECSP Client for Xerox, and Kofax EIP Client for Xerox.

- If you are using IPv6, Xerox requires a working DNS and does not work with static IPv6 addresses with Authentication set to On. Xerox Convenience Authentication does not support IPv6 using static IPv6 addresses. Therefore, to use any supported Xerox device with the Unified Client for Xerox in control of the authentication, use either IPv4 addresses or host names for the address of DWS. Host names can resolve to an IPv6 address.


Then, do the following:

1. Install DRS and make sure that the Device Registration System service is running.
2. Create the application in DRS.
 - a. Select the **Applications** tab.
 - b. Click the green Add (+) button at the top of the left **Applications** pane. The **Add Application** function loads into the right pane.
 - c. In the **Name** field (required), enter a name for the application. You can use any name.
 - d. In the **Application Type** field (required), select **Xerox Unified Client**. Additional fields appear.
 - e. Enter the addresses of the DWS servers.

- f. In the **Server Configuration** field, enter the server configuration to be used for the application.

Note the following:

- The selections you make should reflect your server configuration as defined in ControlSuite.
- If you use Equitrac or Output Manager, additional fields appear for authentication. For **Authentication**, select **True** to use the Unified Client for Xerox as the authentication application on the device or **False** to use another authentication application.

 If authentication is managed by CAC, **Authentication** must be set to **False**. The CAC user name must match the **User principal name** field for the user's Windows user account in Output Manager. Otherwise, single-sign-on will fail.


- g. In the fields that appear, enter the host name or address, port, and other configuration settings for the servers.

The selections you make should reflect your server configuration as defined in ControlSuite.


For each server, select whether or not you are using TLS. For the port number, select the following depending on what servers you use:


- If you are using AutoStore, enter the port number in the **AutoStore Server TLS Port** if TLS is used or **AutoStore Server Port** if TLS is not used.
- If you are using Equitrac, enter the DCE server names.
- If you are using Output Manager, enter the port number in the **Print Manager TLS Port** if TLS is used or **Print Manager Port** if TLS is not used.

The default port number is 8069 if TLS is used or 8068 if TLS is not used.

- h. Click the **Save** button () at the top of the **Add Application** screen.


3. Register the device in DRS.

- a. Select the **Devices** tab.
- b. Click the green Add () button at the top of the left Devices pane. The **Add Device** function loads into the right pane.
- c. In the **Name** field (required), enter a name for the Xerox device that identifies it on the network.
- d. In the **Address** field (required), enter the IP address or the hostname of the device.


 For the IP address, you can enter IPv4 or IPv6 addresses depending on the configuration of your system. If you enter an IPv6 address, brackets ([]) are automatically added to it if missing when you exit from the field.



- e. Enter the **Username** and **Password** for the device.
- f. In the **Application** field, select the application you have created from the list. Based on the application you select, fields that apply to that application appear.
- g. In the **Device Port** field, use the default port of 443 or change it to the appropriate port number.


- h. For the **Decentralized** field, select **True** (the default setting) to use decentralized workflows or false to access Kofax workflows through the Unified Client for Xerox.
- i. Complete the fields for the SNMP server, which are required. Note the following:
 - SNMP must be configured for version 3.
 - The **SNMP Encryption Algorithm** and **SNMP Digest Algorithm** fields must match the settings for the device.
- j. If desired, you can customize the application name and authentication screen:
 - To change the name of the applications as they appears on the device, set **Customize Application Name** to **True** and enter the names in the application name fields. To use the default application name, set **Customize Application Name** to **False**.

 If **Verify Server Certificate** is enabled, the **Customize Application Name** option is not supported. When you install the Unified Client, the name is not changed.

- To customize the authentication screen, set **Customize Authentication Screen** to **True** and enter the text that you want to appear in the **Authentication Title** and **Authentication Message** fields. To use the default text, set **Customize Authentication Screen** to **False**.

 If you need to change the application name or return to default values, the app must be registered again.

- k. Click the **Save**  button at the top of the **Add Device** pane.
4. Register Unified Client for Xerox client application on the device.
- a. From the drop-down list at the top of the **Details** pane, select **Install and Configure**.
 - b. Click the **Run Action** button . You can follow deployment status feedback under **Action History**. The register action may take a few moments to complete. Once finished, a **Successfully completed** message appears in the **Action History** pane at the bottom of the screen.

 If you are using a VersaLink device and Authentication is on, the device is restarted at the end of installation and uninstallation.

Chapter 4

Additional information

Product documentation

The full product documentation set for the Kofax Unified Client for Xerox is available online at the [Kofax ControlSuite 1.4.0 site](#). This documentation set consists of the following documentation to assist you with installing, configuring, and using the product.

- [ControlSuite Help](#), which also contains online help for ControlSuite, DRS, and other components and clients.
- [Release Notes](#)
- [Technical Specifications](#)

Troubleshooting the Unified Client for Xerox

This section provides information for troubleshooting problems with the Unified Client for Xerox.

Device registration issues

If a device fails to register or unregister in DRS, check the following:

- Make sure the device is not in an error state (such as from a paper jam or out of paper) before registering or unregistering the client on it. If the device is in an error state, registration or unregistration will fail.
- If the Combined Client for Xerox has been registered on the device, unregister it before registering Unified Client for Xerox with the Combined Client for Xerox. The Combined Client for Xerox and Unified Client for Xerox cannot be on the same device because only one can be used as the authentication agent.
- If an application fails to register or unregister in DRS because of device errors, it can leave the application half configured on the device. Correct the errors on the device and then delete the application manually with RegClient tool, which is available through Xerox support. You can then try registering the application again.
- If an "Unable to configure" error appears for remote scan or remote print, make sure the SNMP password is the same for DRS and the device. Also be sure to enable all EIP web services on the device, which includes WS-Scan and WS-Print, before registration.

Connection error issues

If you are unable to launch the Unified Client for Xerox app, check the server configuration and connection as follows:

- If you are using a third-party authentication provider with Authentication set to Off, make sure the Xerox device is configured on the Output Manager server. Otherwise, the Unified Client for Xerox app will not connect when you attempt to log on.
- If the primary DWS server goes offline, a connection error occurs that might not go away when the secondary DWS server goes online. When this happens, log off from the Unified Client for Xerox and then log back on. You need to log out manually when there is a failover, even after the secondary DWS goes online.

Scan issues

If a scan job fails to complete, it may be caused by a server failover as follows:

- Scanned documents sent by Unified Client for Xerox are not automatically sent to the replacement database.
- Any in-flight scan or print jobs or inputted metadata when a failover occurs may not be preserved.
- Scan jobs in progress on the secondary server may be lost when the primary server comes back online.

If this occurs, resend the scan job.

Print issues

If you attempt to print documents with the Unified Client for Xerox, make sure there is paper in the tray. If you print when the paper tray is empty, no error message appears, and the job does not print. You can confirm the condition by checking the native jobs application.

Job tracking issues

If jobs are not tracked, make sure the date and time are synchronized between the devices and DWS. Jobs may not be tracked if the time is not set correctly.

Customization issues

If **Verify Server Certificate** is enabled, the **Customize Application Name** option is not supported. When you install the Unified Client, the name is not changed.

Error messages

Code	Message	Comments
400	Failed to register device with DWS	Device errors. Contact Support for assistance.

Code	Message	Comments
401	Invalid credentials	The credentials you provided to the device are incorrect. Provide correct credentials and try logging on again.
402	Failed to deregister device from DWS	Device errors. Contact Support for assistance.
403	Failed to update configuration	Device errors. Click the + button to view details. See Detail messages for errors for a list of results.
508	DWS server not reachable	The DWS server is offline, or the wrong address was entered for the DWS server used by the application.
509	DWS authentication failed	An unsecured fault or binding mismatch exists between DRS and the DWS service. This can occur if the service is configured for security, and the client is not using security.
510	DWS installation failed	Device errors. Click the + button to view details. See Detail messages for errors for a list of results.
511	DWS certificate invalid	An internal error occurred when DRS called to the DWS service. This can occur in the following situations: <ul style="list-style-type: none"> • An error occurred during the initial security context. The message depends on whether Simple and Protected GSS-API Negotiation (SPNEGO) or TLSNego negotiation protocol is used. • A security session is being established on top of an initial security context. • A key renewal takes place for an existing security session. • Security negotiation errors occur as part of the SPNEGO/SSLNego or SecureConversation protocol. Make sure security protocols are properly configured.
512	DWS is currently having another installation in progress	An installation has already started. Wait until it completes before starting a new one.
513	DWS failed to configure device	Device errors. Click the + button to view details. See Detail messages for errors for a list of results.
514	DWS failed to reboot device	Device errors prevent the job from completing. Correct the errors and try restarting again.
515	DWS failed to establish SSL/TLS connection to device	Occurs because the device is rebooting, off, or is otherwise disconnected from the network. This error also appears if the IP address for the device is invalid. Correct the errors and try again.
516	Unsupported device	Appears when you attempt to use AutoStore with an SFP device. AutoStore requires a device with a scanner.

Detail messages for errors

Some errors provide additional details. Click + to view these messages.

Installation Result	Message	Description
DONE_ALREADY_INSTALLING	Currently another installation is in progress.	An installation has already started. Wait until it completes before starting a new one.
DONE_INVALID_CREDENTIALS	Invalid administrator credentials	The credentials you provided to the device are incorrect. Provide correct credentials and try logging on again.
	Invalid SNMP configuration	
DONE_CONFIGURATION_FAILURE	Unable to remove applications on device	Device errors. Contact Support for assistance.
	Unable to register application on device	
	Configuring convenience authentication failed	
	Configuring JBA failed	
	Unable to set default application	
	Unable to reset default application	
	Unable to get device capabilities	
	Unable to configure job limits	
	Unable to configure remote scan	Make sure the SNMP password is the same for DRS and the device. Also be sure to enable all EIP web services on the device, which includes WS-Scan and WS-Print, before registration.
Unable to configure remote print	Occurs because the device is rebooting, off, or is otherwise disconnected from the network. This error also appears if the IP address for the device is invalid. Correct the errors and try again.	
UNSUPPORTED_PRINT_ONLY_DEVICE	Device does not have a scanner	Appears when you attempt to use AutoStore with an SFP device. AutoStore requires a device with a scanner.