



Kofax Unified Client for Fujifilm Getting Started Guide

Version: 1.0.0

Date: 2024-03-14

KOFAX

Legal Notice

© 2024 Tungsten Automation. All rights reserved.

Tungsten and Tungsten Automation are trademarks of Tungsten Automation Corporation, 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 Tungsten Automation.

Table of Contents

Legal Notice.....	2
Chapter 1: Kofax Unified Client for Fujifilm.....	4
Chapter 2: Before you begin.....	6
Prerequisites.....	6
DRS and Unified Client communication ports.....	7
Supported card readers.....	8
Chapter 3: Configure DRS.....	9
Use DRS to deploy and configure the unified client.....	9
Chapter 4: Additional information.....	13
Product documentation.....	13
Troubleshooting the Unified Client for Fujifilm.....	13
Card reader issues.....	13
Host name limitation.....	14
Installation issues.....	14
Login issues.....	14
Error messages.....	15

Chapter 1

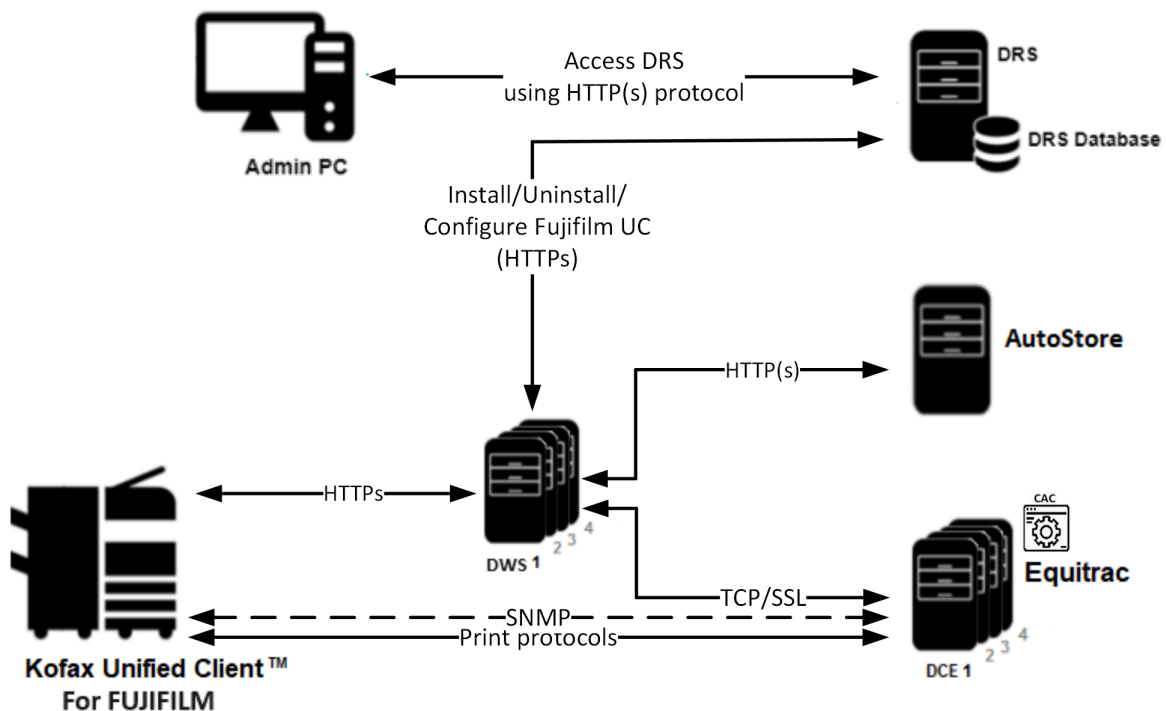
Kofax Unified Client for Fujifilm

The Kofax Unified Client for Fujifilm provides a unified client for capture and print management functionality on supported Fujifilm and Fuji Xerox devices. The capture (with process and route) functionality within the client is provided by Kofax AutoStore, while the print management capability is provided by Kofax Equitrac or Kofax Output Manager.

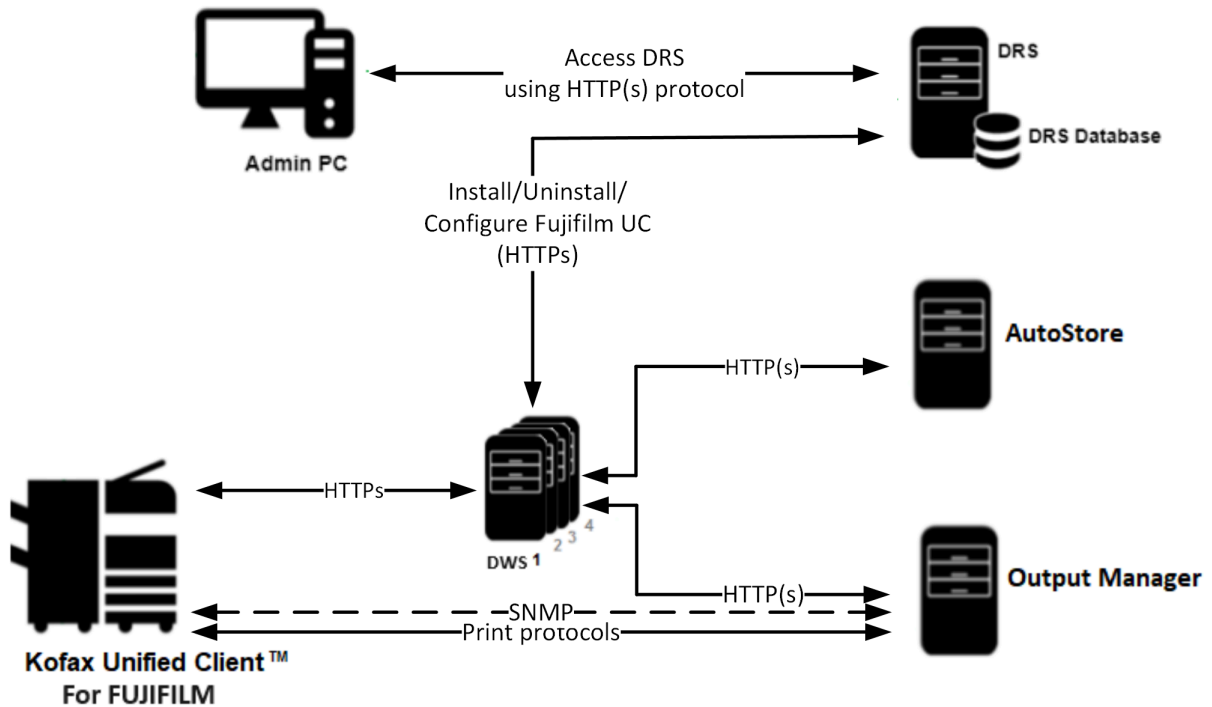
The unified client uses the Device Registration Service (DRS) to configure and deploy the embedded client to single or multiple devices, using one of the following server configurations:

- Server using both AutoStore and Equitrac components.
- Server using both AutoStore and Output Manager components.
- Server using the Equitrac component only.
- Server using the Output Manager component only.
- Server using the AutoStore component only.

This figure illustrates a typical architecture for a system that includes the Unified Client for Fujifilm with Equitrac and AutoStore:



This figure illustrates a typical architecture for a system that includes the Unified Client for Fujifilm with Output Manager and AutoStore:



The Unified Client provides device authentication to securely access the device. It provides a single application for Kofax print and capture workflows.

When deployed to the device with Equitrac or Output Manager, the Unified Client controls access to the device and acts as the gateway for Kofax functionality. Users must authenticate to gain access to Kofax-controlled device functions. In this case, the client allows users to select functions, such as Print-to-Me and scanning, from a common Kofax Launcher screen (where users can start the available workflows), provides card reader support, searchable billing codes at device login, and job accounting. It supports Equitrac authentication through user name, password, and card swipe with an optional PIN.

When deployed to the device with AutoStore only, the client does not control access to the device and provides capture workflows from a Kofax Launcher screen.

The Unified Client supports DWS and DCE failover. You can specify up to three additional DWS servers and DCE servers to ensure that the device continues to function for users if your primary DWS or DCE is offline.

The Unified Client for Fujifilm uses HTTPS and TLS 1.3 (if available) or TLS 1.2 to secure the communication and connections between the device and the Kofax servers. To use TLS 1.3, the DRS server and DWS server must both be installed on a Windows systems that supports TLS 1.3.

Chapter 2

Before you begin

Prerequisites

Before you begin, ensure that 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](#)

Check	Description
<input type="checkbox"/>	Verify that your device is supported. For the latest list of supported Fujifilm and Fuji Xerox models, consult your local representative or refer to the Kofax Supported Devices web page.
<input type="checkbox"/>	Verify that your device supports API 7.
<input type="checkbox"/>	Verify that your device supports Embedded Web Browser (EWB) 5.
<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 if you are deploying AutoStore. This is necessary for the successful installation of 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 confirm 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 Server Manager > Local Server > IE Enhanced Security Configuration .
<input type="checkbox"/>	Verify that you have Administrative access to the device.
<input type="checkbox"/>	If the Unified Client for Fujifilm is configured as the authentication mode, verify that a third-party custom authentication application does not exist on the device.

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

DRS and Unified Client communication ports

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

Component	Device display menu protocol	Device file transport protocol	Default communication port	Port configurab	Required device components
DRS server	HTTP, HTTPS	HTTP, HTTPS	Web server: 8753 REST-based web service: 8755 Client Server: 9000 Web client: 9000	Yes	
Unified Client for Fujifilm	HTTP, HTTPS	HTTP, HTTPS	AutoStore application port (http/https): - AutoStore server: 3310 (DWS to AutoStore) Output Manager application port - http: 8068 - https: 8069 DWS (https) - 8444 (Device to DWS)	Yes	
			Equitrac application port (http/https): - 2939 (DWS to Equitrac) Device port for HTTPS communications: - 58501 (DWS to device) Default print port from: - 9100 (Equitrac to device) SNMP traffic - 161, 162 (Output Manager to device)	No	

Supported card readers

The Unified Client for Fujifilm supports the following card readers:

Kofax card readers

- Kofax Micro ST Reader
- Kofax Micro Card Reader
- Kofax Equitrac ID Card Reader

The Unified Client for Fujifilm has also been tested with the following card readers:

Third-party card readers

- Fujifilm ICCR-B card reader
- Baltech Micro2
- Baltech Micro
- Baltech ID Card Readers USB Gen 2 Business Connect compatible
- Elatec TWN3
- Elatec TWN4
- RFIDEas pcProx RDR-7L81AKU
- RFIDEas pcProx RDR-80581AKU
- HID Omnikey 5427



- An update from Unified Client for Fujifilm is required to support a new card reader.
- When a third-party card reader is used, a third-party card reader license is required. Since January 2023, third-party card readers are provided free of charge for ControlSuite. Please ensure that licenses are available for the amount of card readers being used within the ControlSuite deployment.

Chapter 3

Configure DRS

Use DRS to deploy and configure the unified client

DRS is installed as a ControlSuite component. Administrative access to the server is required. The following steps are performed on the server where the installation takes place.

1. Open DRS. In a web browser, enter `http(s)://<DRSServerIP>:9000/` where `<DRSServerIP>` is the IP address of the server where DRS is installed.
2. Create an application in DRS:
 - a. Select the **Applications** tab.
 - b. Click the New (+) button at the top left of the **Applications** pane.
 - c. In the **Name** field (required), enter an application name.
 - d. Select **Fujifilm Unified Client** as the **Application Type**.
 - e. In the **DWS Server Address** field (required), enter the primary DWS host name. It is recommended that you use the fully qualified domain name of the server instead of the IP address.
 - f. If you have additional DWS servers for failover purposes, enter their host names in the **DWS Server #2 Address**, **DWS Server #3 Address**, and **DWS Server #4 Address** fields.
 - g. In the **DWS Server(s) Port** field, enter the port number. The default is 8444.
 - h. For **Trust Self-signed Certificate for DWS Server**, select **False** to use certificates from a trusted certificate authority or **True** to use self-signed certificates.
 - i. In the **Server Configuration** list, select one of the following options: **AutoStore and Equitrac**, **AutoStore and Output Manager**, **Equitrac**, **Output Manager** or **AutoStore**.

i If your Fujifilm device is a Single-Function Printer (SFP), if you select a configuration with AutoStore, the AutoStore workflows are not shown in the Unified Client Launcher as scanning is not supported.

Based on the server selection, only some of the following application fields are visible.


- j. If you select **AutoStore** as part of the configuration, complete the following information:
 - Enter the host name or IP address for the **AutoStore Server Address**.
 - Enter the **AutoStore Server TLS Port** number that the AutoStore server uses to communicate with the Unified Client for Fujifilm. By default, the port number is 3310.
 - For **AutoStore Server Use TLS**, select **False** if you do not want to use TLS.

- For **Trust Self-signed Certificate for AutoStore Server**, select **False** to use certificates from a trusted certificate authority or **True** to use self-signed certificates.
 - k. If you select **Equitrac** as part of the configuration, complete the following information:
 - In the **DCE Server Address** field (required), enter the IP address or host name used by the Equitrac Server.
 - If you have additional DCE servers for failover purposes, enter their IP addresses in the **DCE Server #2 Address**, **DCE Server #3 Address**, and **DCE Server #4 Address** fields.
 - For **Trust Self-signed Certificate for DCE Server**, select **False** to use certificates from a trusted certificate authority or **True** to use self-signed certificates.
 - To use **DCE certificate pinning** to pin a specific DCE that belongs to your configuration for the duration of that configuration, select **True**.
 - l. If you select **Output Manager** as part of the configuration, complete the following information:
 - In the **Print Manager Address** field, enter the IP address or host name used by the Output Manager server.
 - Enter the **Print Manager TLS Port** number. By default, the port number is 8069.
 - For **Print Manager Use TLS**, select **True** or **False**.
 - For **Trust Self-signed Certificate for Print Manager**, select **False** to use certificates from a trusted certificate authority or **True** to use self-signed certificates.
 - m. For **Bypass button**, select **True** to allow a user to skip authentication to use the device native functions without logging in or **False** to remove this option. This option is not available for an AutoStore only configuration.
 - n. For **Authentication**, select **True** if the Unified Client for Fujifilm is an authentication provider on the device or **False** if authentication is completed by a third-party provider, such as CAC. This option is not available for an AutoStore only configuration.
 - o. If you want to remove any active print jobs that are in the print queue when a user logs out of the Unified Client for Fujifilm, select **True** for **Purge Print Buffer On Logout**. This option is only available when the **Server Configuration** contains Equitrac or Output Manager.
 - p. Click **Save** (📁).
3. Add a device in DRS:
- a. Click the **Devices** tab.
 - b. Click the **New** (+) button at the top left of the **Devices** pane. The **Add Device** function loads into the right pane.
 - c. In the **Name** field (required), enter a name for the Fujifilm device or device group that identifies it on the network.
 - d. In the **Address** field (required), enter the address of the device. While IP addresses can be used, it is preferable to use the fully-qualified domain name.
 - e. Enter the **Username** and **Password** for the device. Typically, the username is admin.
 - f. In the **Application** list (required), select the application you created in the previous step. The remaining device fields appear.


- g. For **Trust Self-signed Certificate for device**, select **False** to use certificates from a trusted certificate authority or **True** to use self-signed certificates.
- h. To collect client debugging logging files for troubleshooting purposes, set the **Enable Debug Log** to **True**.
- i. If you set **Authentication** to **True** when you created your application, select the **Authentication Screen** for users:
 - **Welcome (default)**: The logon prompt appears on a welcome screen that you can customize.
 - **Logon**: Only the logon prompt appears.
 - **Device Home**: The home screen for the device appears.

This option is not available for an AutoStore only configuration.

- j. To change the Welcome Screen Logo, Welcome Screen Image, or Welcome Screen Text, set **Customized Assets** to **True**.
 - When the Welcome Screen Logo list or Welcome Screen Image list is displayed, select the image file. If you want to use custom images, they must be in .jpg or .png format, no larger than 1MB or the following dimensions:
 - Welcome Screen Logo: 288 x 72 pixels
 - Welcome Screen Image: 174 x 174 pixels
 - If you want to change the Welcome Screen Text, set the **Customize Welcome Screen Text** to **True**. In the **Welcome Screen Text** field, enter the new text for the Welcome screen. The text cannot exceed 60 characters.
 - k. For **Customize Workflow Buttons**, select **True** if you want to display the device native apps on the Launcher screen. The **Workflow Applications** field appears. Choose the available workflow applications for your device.
 - l. Click **Save** (📁) at the top of the **Add Device** pane.
4. From the list at the top of the **Details** pane, select **Install and Configure**.

 The primary DWS must be online and available when installing the application.

5. Click **Run Action** (▶). This 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 want to change any settings in the application (such as the primary DWS server or server details for Equitrac, Output Manager, or AutoStore), you must use the **Uninstall and Delete** action to remove the application profile from the device, update the application settings, then choose the **Update Configuration** action again.
- If you made any updates to the customized workflow buttons or assets for the Unified Client for Fujifilm, run **Update Configuration** to push the changes to the device.

If you add a Device Group in DRS, you can set up multiple devices at the same time with a common configuration. You can also override individual settings per device if you want to group your devices but still have certain settings different. When you run an action at

the group level, it will run that command on each of the devices in the group, for a bulk installation. For more information, see [Working with Device Groups](#).

Chapter 4

Additional information

Product documentation

The full product documentation set for the Unified Client for Fujifilm 1.0.0 is available online at the [Kofax ControlSuite 1.5.0 site](#). This documentation set consists of the following documentation to assist you with installing, configuring, and using the product.

- [ControlSuite Clients Help](#), which contains help for the Unified Client for Fujifilm, DRS, and other components and clients
- [ControlSuite server help](#), which contains help for ControlSuite installation and configuration
- Release Notes
- [Technical Specifications](#)

Troubleshooting the Unified Client for Fujifilm

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

Card reader issues

- If you are experiencing any issues using the Fujifilm ICCR-B Card Reader to log in, verify that the IC Card Reader B USB Setup Plugin device setting is deactivated:
 1. For your Fujifilm device settings, go to **Web Device > System > Plug-in Settings**.
 2. If the **IC Card Reader B USB Setup Plugin** setting is **Activated**, change it to **Deactivated**.
 3. Plug in the card reader and try to use it again.
- If you are using the Fujifilm ICCR-B Card Reader, verify that the following configuration is complete:
 1. Open HID Omnikey 5x27 Reader Management page.
 2. Click the **Keyboard Wedge** tab.
 3. On the **General Config** tab, complete the following settings:
 - a. Select the **Keyboard Wedge Enabled** checkbox.
 - b. In the **Keyboard Wedge** list, choose **Output Type**.
 - c. Select the **Boot Interface** checkbox.

- d. In the **Card Out Event Keystrokes** field, leave **[ENTER]**. This is the default value.
- Sometimes, after tapping your card once, the Fujifilm ICCR Card Reader beeps several times and automatically logs in and logs out of the Unified Client for Fujifilm. Do the following:
 1. For your Fujifilm device settings, go to **Web Device > System > Plug-in Settings**.
 2. If the **IC Card Reader B USB Setup Plugin** setting is **Activated**, change it to **Deactivated**.
 3. In the **IC Card Selection and Settings** screen, enable the card types you want to use with the card reader.
 4. When tapping a card at the device, move the card away from the card reader once the beep is complete.

Host name limitation

Due to a Fujifilm device specification, the Unified Client for Fujifilm may not work properly if the server host name is more than 31 characters. To resolve the issue, do one of the following:

- Shorten the server host name.
- Change the DRS application to use the server IP address instead of the host name:
 1. Open DRS.
 2. Click the **Application** tab.
 3. Select **Fujifilm UC** application and click **Edit**.
 4. Change all of the server addresses from host name to IP address.
 5. Save the application.
 6. Reinstall the Unified Client for Fujifilm.

Installation issues

- If you experience an installation failure after running the **Install and Configure** action in DRS, verify that the following issues have not occurred:
 - You cannot get a device token from the Equitrac server because there is a duplicate device serial number. Delete the duplicate physical and embedded device entries in Equitrac and try again.
 - Some device models will refuse an installation command if there is paper on the input tray. Remove all paper and try again.
- The Unified Client for Fujifilm cannot be installed if the device already has an XCP plugin, Fujifilm Unified Client plugin, or another authentication plugin installed. Delete the plugin and try again.

Login issues

User IDs that are longer than 32 characters or contain the following types of characters cannot log in to the Unified Client for Fujifilm:

- special characters or unicode characters, or
- any of the following characters: " + ; < > ? [] () { | }

To resolve the issue, modify your user ID or use a different one.

Error messages

Registration error messages

Code	Message	Comments
400	Failed to register device with DWS.	Device errors. Contact Support for assistance.
401	Invalid credentials.	Verify that you entered the correct credentials and try logging on again.
402	Failed to deregister device from DWS.	Device errors. Contact Support for assistance.
403	Failed to configure DWS server.	Try again later.
503	Device is not reachable.	You receive this message when you run one of the following actions in DRS with an invalid IP address or host name: <ul style="list-style-type: none"> • Install and Configure • Uninstall • Update Configuration
505	DWS installation aborted due to licensing restrictions.	Contact Kofax Support.
506	Product has not been installed.	
507	DWS installation procedure has not completed yet, checking prerequisites.	Review the installation checklists and try again.
508	DWS server not reachable.	Try again later.
509	DWS authentication failed.	Contact Kofax Support.
510	DWS installation failed.	A device was in use or had a logged on user. Restart the device and make sure no user are logged on to the device, and there are no running scan jobs and registration processes. Then, try deploying the client again.
511	DWS certificate invalid.	Verify the certificate details or use another certificate.
512	Failed to sync asset to the following DWS servers: xxxx.	Reconfigure using the appropriate image. Supported image formats are .jpg, .png, and .bmp.
513	The customization has already been installed on DWS server: xxxx.	
514	Failed to apply customization on DWS server: xxxx.	Verify assets and workflows configuration for the device configuration.
515	Failed to remove customization on DWS server: xxxx.	Verify the device configuration and try again.

Code	Message	Comments
516	Failed to sync workflow to the following DWS server:xxxx.	Verify the workflows selected in the device configuration and try installing again.