Kofax Unified Client for Konica Minolta

Getting Started Guide

Version: 1.1.0

Date: 2023-03-23

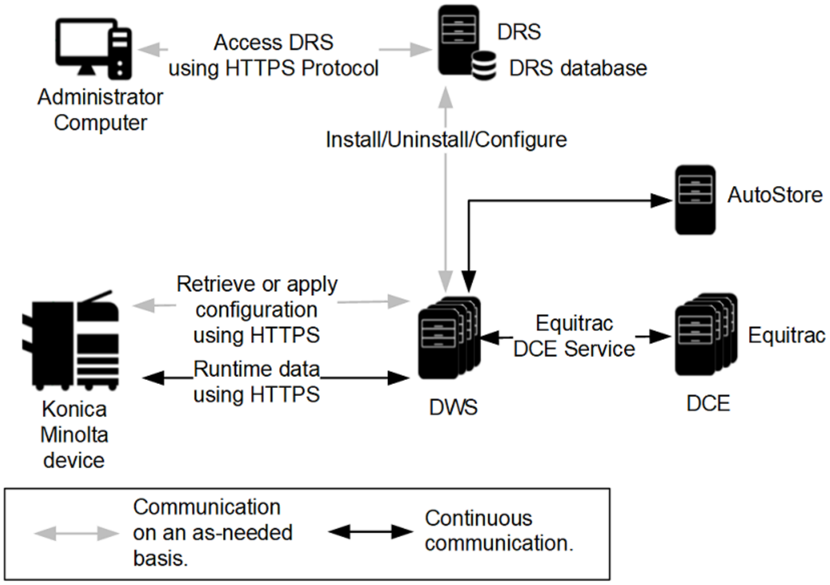
Table of Contents

Chapter 1

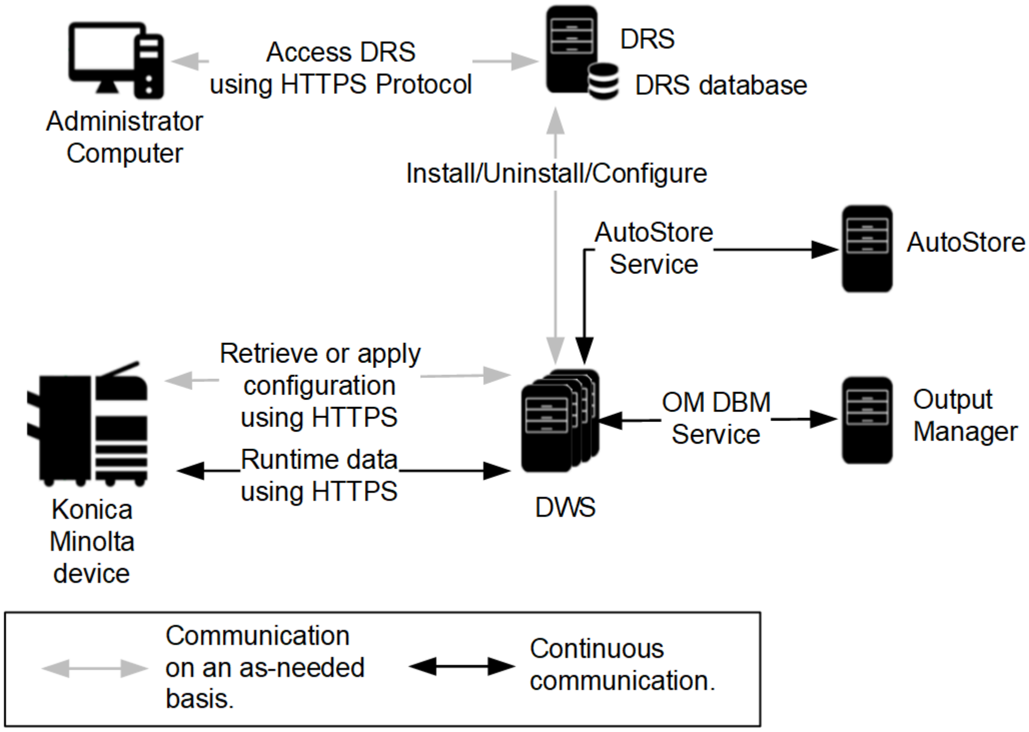
Kofax Unified Client for Konica Minolta

The Unified Client for Konica Minolta adds print and capture capabilities to Konica Minolta devices through AutoStore, Equitrac, and Output Manager while still using device-specific features.

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


Administrator Computer
Access DRS using HTTPS Protocol
DRS
DRS database
Install/Uninstall/Configure
AutoStore
Retrieve or apply configuration using HTTPS
Runtime data using HTTPS
Equitrac DCE Service
Equitrac
Konica Minolta device
DWS
DCE
Communication on an as-needed basis.
Continuous communication.

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


Access DRS
using HTTPS Protocol
DRS
DRS database
Administrator
Computer
Install/Uninstall/Configure
AutoStore
Service
AutoStore
Retrieve or apply
configuration
using HTTPS
Runtime data
using HTTPS
OM DBM
Service
Output
Manager
DWS
Konica
Minolta
device
Communication
on an as-needed
basis.
Continuous
communication.

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

Follow these steps to prepare:

Check	Description
□	Verify that your device is supported. For the latest list of supported Konica Minolta models, consult your local Konica Minolta representative or see the MFD & Productivity Supported Devices Information page.
□	Verify that the server machine is a member of a domain.
□	Verify that you have Administrative access rights to Windows on the server.
□	Check that all important Windows updates are installed.
□	Verify that **Microsoft Windows Updates** is turned on while you are deploying AutoStore, which is required to install Microsoft Windows Identity Foundation (TFS).
□	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).
□	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**).
□	Verify that you have Administrative access to the device.
□	Verify that you have supported card readers. See Supported devices and card readers.

Check	Description
□	Verify that you have configured components, devices, and card readers to work with . See the Prepare for deployment of Unified Client for Konica Minolta section of the *ControlSuite 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 Konica Minolta.

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	
Unified Client for Konica Minolta	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 3310: Default Web Server port when SSL is enabled. 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: DWS certificate for Unified Client for Konica Minolta		

Supported devices and card readers

The Unified Client for Konica Minolta supports the following devices and card readers.

Supported devices

The Technical Specifications document has the full list of supported devices. Please note the following:

- The Unified Client for Konica Minolta supports Konica Minolta, Develop, and Olivetti devices that supports the iOption/OpenAPI framework with the Chromium browser and supports medium and large operation panel screen sizes.
- The following Konica Minolta bizhub MFP and SFP devices are supported:
  - IT5 devices with function level 4.2 or higher
  - IT6 devices with function level 2.0 or higher
- Production Print devices are *not* supported, including iOption-capable devices.

Kofax card readers

The following devices require the wedge loadable driver, which is available from Konica Minolta, to be installed on the device.

- Kofax Micro Card Reader
- Kofax Equitrac ID Card Reader

ⓘ Wedge mode card readers require the keyboard wedge loadable driver to be installed on the device. This driver is available from Konica Minolta and only in the Americas region.

Third-party card readers

The Unified Client for Konica Minolta has also been tested with the following third-party card readers.

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

Proprietary mode card readers

- HID Omnikey 5427 G2 (AU-205H)
- HID Omnikey 5427 CK (AU-205H)
- HID Magtek 21040140 (AU-204H)
- Ysoft KM USB Reader 3 MFX

Keyboard emulation (wedge) mode card readers

ⓘ Wedge mode card readers require the keyboard wedge loadable driver to be installed on the device. This driver is available from Konica Minolta and only in the Americas region.

- Elatec TWN3
- Elatec TWN4
- RFIDeas pcProx RDR-7L81AKU
- RFIDeas pcProx RDR-80081AKU

- RFIDeas pcProx RDR-80581AKU
- Ysoft 3 MF+ Card Reader
- Unitech MS146 Barcode Reader

Chapter 3

Configure DRS

DRS setup and device registration

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

- Make sure you have administrative credentials for the device.
- The Unified Client for Konica Minolta, 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 Konica Minolta. Unregister any embedded client that is configured as an authentication agent before registering the Unified Client for Konica Minolta.

  The ControlSuite server can support multiple Kofax embedded solutions for Konica Minolta. So, it can support certain Konica Minolta devices running the Unified Client for Konica Minolta and other Konica Minolta devices running with other Kofax embedded clients, such as Kofax Combined Client for Konica Minolta.
- If you want to use custom images on the welcome screen, they must be in .bmp, .jpeg, .jpg, and .png format and meet these dimensions:
  - Application logo: 288 x 72 pixels.
  - Welcome screen: 174 x 174 pixels.

Do the following:

1. On the server, install DRS and make sure that the Device Registration System service is running.
2. Open the DRS Web Client.
3. 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 **Konica Minolta Unified Client**.

      Additional fields appear.
   e. Enter the addresses of the primary and backup DWS servers.
   f. In the **Server Configuration** field, enter the server configuration to be used for the application.

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

   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.

   We recommend changing the **Trust self-signed Certificate** setting for the server to **False** to use certificates from a trusted certificate authority. If you need to use self-signed certificates, leave the option set to **True**.

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

h. If you use Equitrac or Output Manager, additional fields appear for authentication. For **Authentication**, select **True** to use the Unified Client for Konica Minolta as the authentication application on the device or **False** to use another authentication application.

   Note the following:

   - If you set **Authentication** to **True**, you can have Unified Client for Konica Minolta overwrite the existing authentication agent by setting **Overwrite Existing Authentication Agent (if any)** set to **True**.
   - If you set **Authentication** to **False**, you must have a third-party authentication agent available to authenticate the user.
   - 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.

i. Click the **Save** button (💾) at the top of the **Add Application** screen.

4. If you are uploading files to use for customizing the welcome screen, make sure they meet the requirements and do the following:

   a. Select the **Files** tab.

   b. In the **Device Type** field, select **Konica Minolta Unified Client**.

   c. Click **Upload**.

   d. Follow the instructions on the screen to select the files and upload them to the server.

   The files appear in the list.

5. Add 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 Konica Minolta device that identifies it on the network.

d. In the **Address** field (required), enter the IP address or the hostname of the device.

> ℹ 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 (required), select the application you have created from the list.

Based on the application you select, fields that apply to that application appear.

g. To change the name of the application as it appears on the device, set **Customize Application Name** to **True** and enter the name in the **Application Name** field. To use the default application name, set **Customize Application Name** to **False**.

Note the following:

- A maximum of 32 characters can appear on the device front panel. Keep the application name to that length.
- After installation, if you need to change the application name or return to default values, the app must be installed again.

h. In the **Logon Screen** field, select **Welcome (default)** or **Logon**. If you select **Welcome (default)**, you have options to customize the welcome screen. If you select **Logon**, only the logon prompt appears.

i. If you had set **Logon Screen** to **Welcome (default)**, you can customize the Welcome screen by doing the following:

- To customize the Welcome screen, set **Customize Welcome Screen Text** to **True** and enter the text you want to appear in the **Welcome Screen Text** field (up to 255 characters).
- If you want to change the logo and image that appears on the Welcome screen, set **Customize Assets** to **True**. In the **Application Logo** and **Welcome Screen Image** fields (both required), select the file name of the image you want to use. Images that meet the requirements and have been uploaded to the server appear in this list. You can also select **Default** to use the default logo or image, or **None** to not use an image.

> ℹ If the files do not appear in the **Application Logo** and **Welcome Screen Image** field, make sure you have uploaded them as shown in step 4 and that they meet the requirements listed in this section.

j. If you have selected an application that includes authentication, use the **Card Reader Type** field to select the card reader attached to the device. Note the following for these card readers:

- For OmniKey, additional options are available to use the reader in CCID and wedge modes.
- YSoft readers are only supported in CCID mode, and they only deliver data in hex or converted to decimal. Wedge mode is not available.

    - If you select **Custom**, enter the PID and VID. The card reader will be supported in keyboard wedge mode only.
    - All other card readers are in wedge mode.

   k. Click the **Save** (💾) button at the top of the **Add Device** pane.

      Assets you have specified in DRS are pushed to DWS for deployment.

6. Install the Unified Client for Konica Minolta client application onto the device. From the drop-down list at the top of the **Details** pane, select **Install and Configure** option and click the **Run Action** button ▶.

   Follow deployment status feedback under **Action History**. The action may take a few moments to complete. If you had customized the Welcome screen by uploading files on the **Files** tab, set **Customize Assets**, and selected those uploaded files in the **Application Logo** and **Welcome Screen Image** fields, those files are synced with the devices.

   Once finished, a **Successfully completed** message appears in the **Action History** pane at the bottom of the screen.

Chapter 4

Additional information

Product documentation

The full product documentation set for the Kofax Unified Client for Konica Minolta 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 Konica Minolta

This chapter provides information for troubleshooting problems with the Unified Client for Konica Minolta.

Error codes

If the Unified Client for Konica Minolta returns an error code, refer to this table for an explanation and resolution.

Error Code	Explanation and Resolution
2236	The certificate security credentials cannot be verified. Configure the device to accept the Web server certificate from DWS.

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 an error state, registration or unregistration will fail.
- Make sure no users are logged on to the client before using the the Install and Configure or Update Configuration action.

- If you are using Unified Client for Konica Minolta with the Combined Client for Konica Minolta, register the Unified Client for Konica Minolta first. If you attempt to register Unified Client for Konica Minolta when the Combined Client for Konica Minolta is already registered, credential fields will not appear when you start Unified Client for Konica Minolta. If you already have the Combined Client for Konica Minolta installed, remove it and then register it again after you install Unified Client for Konica Minolta.
- Do not select **False** for **Overwrite Existing Authentication Agent** unless you are sure an authentication agent does not exist on the device. If one is there already, the installation of the Unified Client for Konica Minolta authentication program will fail.
- If you get the error, "Error received from device for operation AppReqExtLogin...Message: fail DeviceLock," it indicates 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.

Connection error issues

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 Konica Minolta and then log back on. You need to log out manually when there is a failover, even after the secondary DWS goes online.

Configuring dual-stack IPv6 environments

In a dual-stack environment, use IPv6 addressing or fully qualified domain names with IPv6 DNS entries. Mixing IPv4 device addressing and IPv6 server and endpoint configurations is not recommended.

Server issues

If a server appears to have gone offline, it may be caused by a certificate error or an expired certificate. Check for the following errors in the Neuf log:

- An "Unexpected server certificate" error indicates that the server certificate has been changed. If the change is not expected, research the cause of the change. If this change is expected, re-pin the certificate as follows:
  1. Run DWS Web Admin.
  2. Click the **Security** tab.
  3. Scroll to the **Security Certificates** section on the bottom.
  4. In the row with the changed server certificate, click the **Re-pin** link.
- A "Cannot build trust manager without server certificate" error indicates that the device was configured in DRS to use TTL, but the server is not presenting a certificate. In AutoStore, make sure **Use SSL** is selected.

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 Konica Minolta 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.

Failover issues

When configuring DWS servers for failover, make sure you use the same address format (host name or IP address) for the connected devices. Differences in address format can result in the following errors:

- Under Failover Summary Info, the DWS status is shown as N/A.

  If this happens, on the DWS failover server, stop the DWS service, reinstall the device, and then restart the DWS service.
- DRS displays the following warning message after installing, "Failed to configure the following DWS server."

  If this happens, make sure the DWS failover server is running the DWS service. In DRS, update the configuration for the devices.

Print release issues

If you are unable to release a document in A4 or US Letter, make sure A4/A3<->LTR/LGR Auto Switch is set to On.

Search issues

If you get a "Error during prompt processing" error when performing a search from a List or Lookup List field, the ODBC data source needs to be properly configured. Check the configuration of the ODBC data source used for the lookup.

Error messages

Registration error messages

Code	Message	Comments
502	Unable to proceed. Please restart device.	The device may be in an error state or the device does not support OpenAPI. If the device is started and this error still occurs, contact Kofax Support.

Code	Message	Comments
503	Invalid password. Please retry login.	Verify that you enter the correct device admin password in the device Details pane in Device Registration Service.
504	Unable to connect to device. Please restart device.	
505	Maximum registered applications exceeded. Please remove unused applications and retry.	
506	Device is locked. Please retry later.	Verify that the device is not in authentication mode or application mode.
507	Logo icon file does not exist. Contact Kofax Support.	Contact KofaxSupport.
508	Device solution key file not found. Contact Kofax Support.	Contact KofaxSupport.
509	Invalid Output Manager server address. Enter correct server address and retry.	The Output Manager server address is blank. Enter the Output Manager server on the Applications tab in Device Registration Service.
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.
512	Invalid password. Enter the valid password and retry.	Reenter your credentials using a valid password.
518	Invalid AutoStore server address. Enter the valid address and retry.	The AutoStore server address is blank. Enter the AutoStore server on the Applications tab of Device Registration Service.
519	Invalid Web application port number. Enter the valid port number and retry.	The Web Application Port setting is blank or contains a negative number. Enter a valid port number for Web Application Port on the Application tab of Device Registration Service.
522	Administrator is logged in. Log out from device or the device website and try again.	When the administrator is logged into the device or the device website, Device Registration Service cannot unregister client application or authentication.

Unregistration error messages

Unregistration requires that the device is on and functioning normally. Ping the device or access PageScape to verify that the device is communicating with the network.

Code	Message	Comments
502	Unable to proceed. Please restart device.	The device may be in a faulted state or the device does not support OpenAPI. If the device is started and this still occurs, contact Kofax Support.

Code	Message	Comments
503	Invalid password. Please retry login.	Verify that you enter the correct device administrator password.
504	Unable to connect to device. Please restart device.	
506	Device is locked. Please retry later.	Verify that the device is not in authentication mode or application mode.
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 unregistering the client again.
513	Unregistration failed because no Unified Client has been registered.	There is no registered Unified Client application.