



Kofax RPA

Desktop Automation Service Guide

Version: 11.5.0

Date: 2023-10-02

KOFAX

© 2017–2023 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

| | |
|---|-----------|
| Preface..... | 4 |
| Related Documentation..... | 4 |
| Training..... | 5 |
| Getting help with Kofax products..... | 6 |
| Chapter 1: Desktop Automation configuration..... | 7 |
| Prerequisites and installation..... | 7 |
| Automate the Start menu and UWP applications..... | 8 |
| Configure the service..... | 9 |
| Configure the host..... | 9 |
| Configure Screen Lock on Startup..... | 10 |
| Configure logging..... | 11 |
| Configure proxy servers..... | 11 |
| Check Java Access Bridge..... | 12 |
| Change default OCR language..... | 13 |
| Add integrations..... | 14 |
| Activate a virtual input driver..... | 14 |
| Enable integration with SAP..... | 14 |
| Chapter 2: Desktop Automation management..... | 15 |
| Start service or view status..... | 15 |
| Use Lock Screen..... | 15 |
| View and modify configuration options..... | 15 |
| Manage Desktop Automation Service..... | 21 |

Preface

This guide describes how to configure and manage the Desktop Automation Service.

Related Documentation

The documentation set for Kofax RPA is available here:¹

<https://docshield.kofax.com/Portal/Products/RPA/11.5.0-nlfihq5gwr/RPA.htm>

The documentation set includes the following resources listed in alphabetical order:

Kofax RPA Administrator's Guide

Describes administrative and management tasks in Kofax RPA.

Kofax RPA Best Practices Guide

Offers recommended methods and techniques to help you optimize performance and ensure success while using Robot Lifecycle Management in your Kofax RPA environment.

Kofax RPA Desktop Automation Service Guide

Describes how to configure and manage the Desktop Automation Service required to use Desktop Automation on a remote computer.

Kofax RPA Developer's Guide

Contains programmer user guides for the Java and the .NET APIs used to execute robots on RoboServer. Also, includes information on the Management Console REST services provided with the product.

Kofax RPA Getting Started with Robot Building Guide

Provides a tutorial that walks you through the process of using Kofax RPA to build a robot.

¹ You must be connected to the Internet to access the full documentation set online. For access without an Internet connection, see the *Installation Guide*.

Kofax RPA Getting Started with Document Transformation Guide

Provides a tutorial that explains how to use Document Transformation functionality in a Kofax RPA environment, including OCR, extraction, field formatting, and validation.

Kofax RPA Help


Describes how to use Kofax RPA. The Help is also available in PDF format and known as *Kofax RPA User's Guide*.

Kofax RPA Installation Guide

Contains instructions on installing Kofax RPA and its components in a development environment.

Kofax RPA Java API documentation

Provides access to the Kofax RPA Java API packages and classes for developers to use with Kofax RPA.

 The Kofax RPA APIs include extensive references to RoboSuite, the original product name. The RoboSuite name is preserved in the APIs to ensure backward compatibility. In the context of the API documentation, the term RoboSuite has the same meaning as Kofax RPA.

Kofax RPA Release Notes

Contains late-breaking details and other information that is not available in your other Kofax RPA documentation.

Kofax RPA Technical Specifications

Contains information on supported operating systems and other system requirements.

Kofax RPA Upgrade Guide

Contains instructions on upgrading Kofax RPA and its components to a newer version.

Kofax RPA User's Guide

Contains instructions for using Kofax RPA and its components. Includes the *Kofax RPA Help* topics, plus more in depth coverage not available in the *Help*.

Training


Kofax offers both classroom and computer-based training to help you make the most of your Kofax RPA solution. Visit the Kofax Education Portal at <https://learn.kofax.com/> for details about the available training options and schedules.

Also, you can visit the Kofax Intelligent Automation SmartHub at <https://smarthub.kofax.com/> to explore additional solutions, robots, connectors, and more.

Getting help with Kofax products

The [Kofax Knowledge Portal](#) repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Portal to obtain answers to your product questions.

To access the Kofax Knowledge Portal, go to <https://knowledge.kofax.com>.

 The Kofax Knowledge Portal is optimized for use with Google Chrome, Mozilla Firefox, or Microsoft Edge.

The Kofax Knowledge Portal provides:

- Powerful search capabilities to help you quickly locate the information you need.
Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.
To locate articles, go to the Knowledge Portal home page and select the applicable Solution Family for your product, or click the View All Products button.

From the Knowledge Portal home page, you can:

- Access the Kofax Community (for all customers).
On the Resources menu, click the **Community** link.
- Access the Kofax Customer Portal (for eligible customers).
Go to the [Support Portal Information](#) page and click **Log in to the Customer Portal**.
- Access the Kofax Partner Portal (for eligible partners).
Go to the [Support Portal Information](#) page and click **Log in to the Partner Portal**.
- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.
Go to the [Support Details](#) page and select the appropriate article.

Chapter 1

Desktop Automation configuration

This chapter describes how to configure the Desktop Automation Service. Typically, these tasks are performed by an administrator.

- [Prerequisites and installation](#)
- [Configure the service](#)
- [Configure the host](#)
- [Configure Screen Lock on Startup](#)
- [Configure logging](#)
- [Configure proxy servers](#)
- [Check Java Access Bridge](#)
- [Change default OCR language](#)
- [Add integrations](#)

User tasks for mapping devices, preparing devices, and setting preferences are described in the *Kofax RPA Help*.

Prerequisites and installation

All Desktop Automation Service requirements and prerequisites are in the "Dependencies and Prerequisites" chapter of the *Kofax RPA Installation Guide*.

Installation instructions are provided in "Install Desktop Automation Service" of the *Kofax RPA Installation Guide*.

There is no hard-coded limit to the number of elements that the Desktop Automation Service can read in the automated application tree. The depth is limited by the stack thread size, and the total number of nodes is limited by available memory.

Use the Max Depth and Max Siblings settings in the Tree Modes setting to prevent any device issue errors and to limit the number of elements loaded.



- The Desktop Automation Service relies on Windows UI Automation API. Do not run any UI Automation API clients on the same computer simultaneously with the Desktop Automation Agent.
- The Desktop Automation Service cannot automate, remove the focus from, or generate input, such as keyboard input or a mouse click, for an application that has the High integrity level as defined by Windows. The Desktop Automation Service runs as a process with the Medium integrity level and cannot generate input for applications with a higher level. Examples of applications running at the High integrity level are the Task Manager, System Properties, and applications ran as administrator. Also, the Desktop Automation Service cannot generate a tree for applications with a higher integrity level.

Workarounds: Run the Desktop Automation Service as administrator to increase the integrity level to High. Or, install the Desktop Automation Service with the virtual input driver and set the environment variable `KOFAX_RPA_VIRTUAL_INPUT` to `Y`. For more information on the environment variable, see "Install the virtual input driver" in the *Kofax RPA Installation Guide*.

Automate the Start menu and UWP applications

If you are using Windows 10 or newer, automate the Windows Start menu and UWP applications.

Starting with Windows 10, Microsoft implemented the Universal Windows Platform (UWP), formerly the Metro-style application platform. When looping (enumerating) open applications on a Windows 10 or newer desktop, by default some interface elements are skipped to improve performance.

In the Kofax RPA 10.3.0.1 and newer versions, the UWP and Metro-style applications are not automated by default. As a result, the Start menu is not selectable and does not appear as a tab in the Recorder View when running on a remote device with Kofax RPA.



Metro-style applications for Windows version 8.1 need modifications to migrate to UWP.

A robot is slower when the Desktop Automation Service is running on Windows 10 and newer versions (and corresponding server versions). Additionally, it is possible that the robot using Desktop Automation on Windows 10 and newer versions (and corresponding server versions) might not identify some interface elements such as a window or a popup, which would be recognized on earlier Windows versions.

To automate the Windows Start menu tab and UWP applications, set the following environment variable:

```
KAPOWHUB_APPLIST_VERSION=2
```

Be advised that this setting may lead to performance degradation.

Configure the service

If your computers meet all the requirements for Desktop Automation Service described in [Prerequisites and installation](#), install and configure the Desktop Automation Agent.

1. To automate Java applications:
 - a. Install Java JRE or JDK on remote devices.
 - b. Enable or verify that the Java Access Bridge is enabled on your devices. See [Check Java Access Bridge](#).
2. Download and run the Kofax RPA Desktop Automation installer on your device.
3. From the Start menu, start the Desktop Automation Service.

After the service starts, view its status by looking at the icon in the notification area. See [Start service or view status](#).
4. Edit the Desktop Automation Service parameters using one of the following methods.
 - To configure the options in the user interface:
 - Click **Configure**.

This action opens the Desktop Automation Service window. For parameter descriptions and valid entries, see [View and modify configuration options](#).
 - After configuring the options, click **Save and Restart**.
 - To manually configure the options, edit and save the `server.conf` file on your automation desktop.

The file is located in the `\[User]\AppData\Local\Kofax RPA\[version]` folder.
5. Check that the device is registered in the Management Console under the **Admin > Devices** section.

When the Desktop Automation Service connects to the Management Console, the Management Console tests the connection to the Desktop Automation Service. If it is successful, the status Available appears.
6. To connect to devices over an RDP connection when session management through Remote Desktop Sessions is preferred to normal login sessions, complete the steps in "Use RDP Connection" in the *Kofax RPA Help*.

Configure the host

In Kofax RPA, computers controlled by the Desktop Automation Service require an active Windows login session. The Desktop Automation Service provides a feature to automatically create a session and lock its screen.

In some cases, it is necessary to have a robot log in to a remote host to start an automation device or to lock the screen on the automation device. These actions are performed using an RDP connection to the automation device.

With the Desktop Automation Service running on a remote computer, you can lock the screen when using the Remote Device Action step in robots.

To log into an automation device or lock its screen, your device must meet the following RDP log in and Lock Screen requirements.

- The Remote Desktop connection server component must be enabled and configured for the Lock Screen feature.
- The user running the Desktop Automation Service must be allowed to connect through Remote Desktop (as a member of the Admin group or the Remote Desktop group) and use a password.
- The account configured for this feature must be permitted to remotely access the system using the Remote Desktop feature. See [Configure the service](#).
- The group policy "*Always prompt for password upon connection*" must be off.

To check the policy setting, use **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security**.

- Port 3389 must be accessible.
- The automation device cannot be a domain controller.
- NTLM authentication must be permitted.
- If Windows is configured to show an extra screen when the user logs in, the Lock Screen tries to detect this extra screen and dismiss it by pressing OK. If the screen is not dismissed, the action may fail. When an extra screen is detected, the Lock Screen feature dismisses it three seconds after the connection with the system is established. If automatic detection fails or three seconds is not long enough:
 1. Add a `KAPOW_LEGALNOTICE_SECONDS` system variable in the environment variables file on your automated device.
 2. Set the number of seconds in the "Variable value" field to wait before dismissing the window after the connection.
 3. Restart the Desktop Automation Service after adding the variable and saving the environment variables file.

Configure Screen Lock on Startup

If you need to restart your computer frequently and cannot use the automatic login feature of Windows, configure the Configure Screen Lock on Startup. This option enables the Desktop Automation Service to automatically create a session and lock the screen after the computer is restarted.

1. Right-click the Desktop Automation Service icon in the notification area and select **Configure**. The Desktop Automation Service window appears.
2. Click the **System** tab.
3. Click the **Configure Screen Lock on Startup** button.

The system requests elevation. You might receive a UAC elevation prompt. The elevation might require entering the credentials for another account that has administrative privileges.
4. Provide the credentials of the user account used to log in and create a session after a computer restart.

The user field in the credentials dialog is pre-filled with the currently logged in user. It is not necessarily the user account that is used for the elevation.

i When you change the user's account password, update it directly in the Task Scheduler or click the **Configure Screen Lock on Startup** again.

A Task Scheduler is created. This task executes the **Lock Screen** a minute after the computer is restarted. The task is created under the folder `Kofax/RPA`.

To delete the lock on restart, go to the folder `Kofax/RPA` in the Task Scheduler and delete the task "Lock screen after boot."

Configure logging

Kofax RPA collects usage information on specific Desktop Automation Service events, which may be useful to improve the service performance.

- If the Desktop Automation Service is connected to a Management Console, the events are stored in the RoboServer Log Database of the Management Console. To view the events, on the **Log view** page, select **DAS messages**.

i If the connection parameters for the Management Console are specified in the Desktop Automation Service configuration window, the events are always logged to the Management Console, even if the Single User mode is selected, that is, the connection to the automation desktop is established directly, without the Management Console.

- If the Desktop Automation Service cannot connect to a Management Console (because Management Console is not configured), it writes the events to the Desktop Automation Service Usage.csv log file, which resides in:

```
{path}\AppData\Local\Kofax RPA\<version number>\Logs\
```

Configure the file location in the `log4net.xml` file.

The information for each event includes:

- Time that the event occurred in UTC.
- Type of event: start, stop, connect, disconnect, suspend, or lock screen.
- Identification of Desktop Automation Service, consisting of an ID in the form `host:port`, the user account running the service, and the labels defined for the service.
- Name of the robot and the execution ID (only for connect and disconnect).
- Severity indication (always "Info").
- Message (always empty).

Configure proxy servers

All robots can use the Kofax RPA global proxy settings when automated with the Desktop Automation Service. The Desktop Automation Service uses the same proxy settings as Design Studio and Management Console.

The local proxy settings of the built-in browser in the Desktop Automation Service have a higher priority than the Kofax RPA global proxy settings configured in Design Studio > Design Studio Settings. Make sure that the robot uses the Kofax RPA global proxy settings, unless the task requires it to use local proxy settings. For more information, see *Kofax RPA Help*.

Also, the `cef.cfg` file should not be used to configure proxy settings, but if it is used, it has a higher priority than all of the local and global proxy settings.

Configure proxy server settings in one of two ways.

1. For all robots running on the Desktop Automation Service, in the **Design Studio Settings** dialog box, on the **Proxy Servers** tab, complete the following proxy server details.
 - Host
 - Port number
 - Username
 - Password
 - Excluded hosts
2. For all deployed robots, on the Management Console **Admin > RoboServers > Cluster settings > Proxy servers** tab, select **New proxy** and complete the following proxy server details.
 - Host
 - Port
 - User name
 - Password
 - Exclusions

Check Java Access Bridge

Java Access Bridge is an essential component to automate your Java applications. Depending on the Java version, some required files may be missing from system folders, resulting in Java Access Bridge being disabled on the computer where the Desktop Automation Service is installed.

To check your Java Access Bridge installation, perform the following steps.

1. Right-click the Desktop Automation icon in the notification area and select **Configure**.
2. Click the **System** tab and click **Check Java Access Bridge files**.
The Java Access Bridge dialog box opens, showing installed Java versions and Java Access Bridge installation status for each version.
3. Verify that the **JAB Installed** column, **Java Access Bridge is installed into Windows system folders**, and **Java Access Bridge is enabled** all display **Yes**.
When these display Yes, the Java Access Bridge is properly installed and enabled on the computer.
4. If your implementation of Java is not listed under **Java Home Directories**, click **Add Folder** and specify a home folder with installed Java files.

5. If any of the files are missing, such as **JAB Installed** column shows **No**, click **Show Missing Files**.

The Java Access Bridge Missing Files dialog box shows files that must be copied to specified folders. Copy the missing files to the destination folders.

6. If **Java Access Bridge is enabled** shows **No**, click **Enable Access Bridge**.

Change default OCR language


When a robot performs text recognition in the Extract Text From Image Step using the Desktop Automation Service, the service uses the language selected on the OCR tab of the Desktop Automation Service window.

Kofax RPA uses OmniPage and Tesseract (default) OCR engines to capture text from images.

- For OmniPage, Kofax RPA installs all supported languages.
- For Tesseract, Kofax RPA installs only the English language.

To change the default language for OCR, perform the following steps.

1. Right-click the Desktop Automation icon in the notification area and select **Configure**.
2. Click the **OCR** tab.
 - To use the OmniPage engine, select **Use Kofax OmniPage OCR (only for packages version 11.1 or later)**.
 - To use a single language other than the default, replace `eng` (default) with the other language, such as `jpn`, in the **Enabled OCR languages** field.
The language code must be in ISO 639-3 or ISO 639-1 format.
 - To use more than one language, add another language using the plus sign such as `eng+jpn` in the **Enabled OCR languages** field.

 Using more than one language simultaneously for screen recognition slows down robot execution and deteriorates recognition results.

3. Click **Save and Restart**.

To use Tesseract for text recognition in a language other than English.

1. Download and copy necessary language packs as follows.
 - a. [Download the .traineddata file](#) for the required language from GitHub.
Example: `fra.traineddata` is for the French language.
If the files are not available in the link above, search for version 3.04 from the [main repository page](#).
Tesseract version 3.05.00 is compatible with Kofax RPA 11.5.0. However, RPA uses Tesseract 3.04.00 training files.
 - b. Copy the downloaded file to `Kofax RPA\<version>\lib\tessdata` in the **ProgramData** folder.
Example: `C:\ProgramData\Kofax RPA\11.5.0.0_110\lib\tessdata`.

2. Train Tesseract to recognize your character set using either TTF fonts or UI screen shots. See the *Train Tesseract* topic in *Kofax RPA Help*.


Add integrations

Use the following information to integrate other components with the Desktop Automation Service.

Activate a virtual input driver

A virtual input driver is a Windows device driver capable of simulating a hardware keyboard.

- For operating systems supported by the driver, refer to the *Kofax RPA Technical Specifications*.
- For information on installing the driver, refer to the *Kofax RPA Installation Guide*.

 Virtual input drivers do not function when the desktop of an automated computer is locked, such as by an RDP step or the Lock Screen function.

To enable a virtual input driver, set the environment variable `KAPOW_KEYBOARD_INPUT_METHOD` to `VIRTUAL_KEYBOARD` on the automated device.

To disable a virtual input driver, remove or comment out the environment variable.

Enable integration with SAP

To work with the SAP application in Robots, perform the following steps.

1. From the product installation files, download and save the `RegSAPSurrogate.reg` file on the computer running the Desktop Automation Service.
The file is in the `{path}\DesktopAutomationService\bin` folder.
2. Run it and accept any warnings.
3. Restart the Desktop Automation Service Agent.

Chapter 2

Desktop Automation management






This chapter describes Desktop Automation Service management tasks.

- [Start service or view status](#)
- [Use Lock Screen](#)
- [View and modify configuration options](#)
- [Manage Desktop Automation Service](#)

Start service or view status

Start the Desktop Automation Service from the Start menu.

After the service starts, view its status by looking at the icon in the notification area.

| Icon | Status |
|---|---|
|  | Service is starting and trying to connect to the configured Management Console. |
|  | Service is running and either connected to a Management Console or running in single-user mode, depending on configuration. |
|  | Service is running and in use by RoboServer or Design Studio. |
|  | Service is not running. |
|  | Service is not running due to an error. |

Use Lock Screen

To use this option, the Desktop Automation Service must be installed and configured. See [Configure the service](#) and [Configure the host](#). See also [Configure Screen Lock on Startup](#).

1. Before locking your device screen, make sure the service is running and is in the connected state.
2. From the Desktop Automation Service menu or icon, select **Lock Screen**.

View and modify configuration options

Use the Desktop Automation Service window to configure Desktop Automation Agent and Management Console options.

The following table describes options and values.

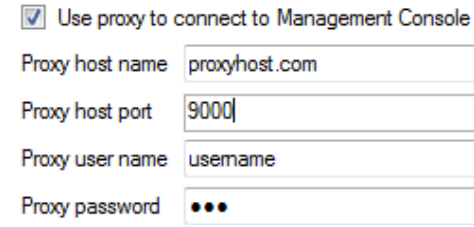
| Configuration window option | server.conf option | Value and description |
|-----------------------------|--------------------|---|
| Single User | singleUser | <p>Empty (default).</p> <p>Select for direct connection to the automation device from Design Studio or when using an RDP connection.</p> <p>Leave empty to automatically register the Desktop Automation Agent with the specified Management Console.</p> <p>The direct connection to the automation device is recommended only for creating and debugging a robot in Design Studio as well as for using with an RDP connection. See "Use RDP Connection" in <i>Kofax RPA Help</i>.</p> |
| Host name | hostName | <p>Name or local IP address of the computer running the Desktop Automation Agent.</p> <p>If a computer has multiple names or IP addresses, specify the one that RoboServers and Design Studio contact this Desktop Automation Agent with. That is, the host name or IP address must be reachable from RoboServers and Design Studio.</p> |
| Command port | commandPort | <p>49998 (default).</p> <p>If the Desktop Automation Service is started without being manually configured, it uses the default configuration and listens on the default 49998 port.</p> <p>Reassign this port to the automation device if necessary.</p> |
| Stream port | streamPort | <p>49999 (default).</p> <p>This port sends data between Design Studio and the Desktop Automation Agent.</p> <p>If set to "0," the Desktop Automation Agent selects a random port number.</p> <p>You might need to assign the stream port if there is a firewall between Design Studio and the automation device.</p> |

| Configuration window option | server.conf option | Value and description |
|-----------------------------|--------------------|--|
| <p>CA file</p> | <p>caFile</p> | <p>Empty (default). Specify the path to the file with the exported certificate. You can communicate with the Management Console using SSL. If the default certificate in <code>node.js</code> is not used, specify a path to another certificate file using this parameter. Note that you need to have a root certificate for this to work. To save a root certificate in a file from a Google Chrome browser:</p> <ol style="list-style-type: none"> 1. Click the lock icon next to the URL. 2. Select Connection is secure. 3. Select Certificate is valid. The Certificate Viewer dialog box appears. 4. Go to the Details tab and select the top entry in the Certificate Hierarchy. 5. Click Export. 6. Save the certificate as a Base64-encoded ASCII, single certificate file with the <code>.crt</code> extension. |

| Configuration window option | server.conf option | Value and description |
|---------------------------------|--------------------|--|
| Timeout | commandTimeout | <p>This option specifies the timeout for command execution in seconds.</p> <p>A command is an instruction sent to the automation device, such as <i>click mouse button</i>, <i>open application</i>, <i>add a location found guard</i>, and so forth.</p> <p>If a command cannot be completed in a specified time, the service sends a notification, and the execution of the robot stops.</p> <p>Note that in case of a Guarded Choice step, this setting applies to invoking the guard in the workflow, but waiting for the guard to be satisfied is not bound to this timeout setting and can wait forever.</p> <p>A similar situation occurs when using the Move Mouse and Extract steps. The commands must be invoked on the device with the timeout specified in this field, but the robot waits for up to 240 seconds for the commands to complete.</p> <p>Set the command timeout for automating terminal sessions or browsing websites in either of the following ways:</p> <ul style="list-style-type: none"> • On the Desktop Automation tab of the Design Studio Settings window for executing the workflow in Design Studio. • In the Automation Device section on the Security tab of the RoboServer Settings window for RoboServer execution. |
| Token on Single User tab | token | <p>Empty (default).</p> <p>Leave empty if Single User is empty.</p> <p>If you selected Single User for direct connection to the automation device from Design Studio or an RDP connection, specify a token. It can be any token you define.</p> |

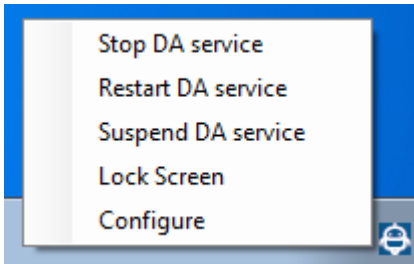
| Configuration window option | server.conf option | Value and description |
|---|-------------------------|---|
| <p>Certificates tab</p> <p>Remote hub</p> <p>Private Key File <input type="text" value="kofax.remote.das.pem"/></p> <p>Public Key File <input type="text" value="kofax.remote.das.cert.pem"/></p> <p>Folder with own CA files</p> <p><input type="text" value="/serverCa"/></p> <p>Local hub</p> <p>Private Key File <input type="text" value="kofax.local.das.pem"/></p> <p>Public Key File <input type="text" value="kofax.local.das.cert.pem"/></p> | <p>tlsServerConfig</p> | <p>Kofax RPA provides TLS communication between the automation device and the RoboServer or Design Studio.</p> <p>The communication uses certificates for encrypting the communication. The following is a <code>server.conf</code> file code extract.</p> <pre data-bbox="997 590 1463 768">"tlsServerConfig": { "key": "kofax.remote.das.pem", "cert": "kofax.remote.das.cert.pem", "ca": ". /serverCa" },</pre> <p>For more information, see "Use TLS Communication" in the <i>Kofax RPA Help</i>.</p> |
| <p>Windows tab</p> | <p>automationnative</p> | <ul style="list-style-type: none"> • Installed packages Lists Desktop Automation Service packages installed on this computer. New version packages are installed automatically if the Lock package option is not selected. The packages in ZIP files are installed to <code>C:\ProgramData\Kofax RPA</code> on the automated device. The appropriate package is selected automatically depending on the RoboServer version. • Lock package If you want to specify only one version package to be used, select Lock package and select one of the installed packages. A RoboServer with a different version cannot connect to this service. By default, the option is not selected. Select this option or change the setting to <code>true</code> in the <code>server.conf</code> file to run robots with triggers. • Map RFS share to drive letter The Windows drive that the Robot File System file share is available in. When the file share is mapped to a Windows drive, other Windows applications can access this file share. |

| Configuration window option | server.conf option | Value and description |
|--|------------------------------------|---|
| OCR | ocrConfig | Specifies one or more languages and an engine to perform an OCR operation on the automated desktop. Select from OmniPage or Tesseract (default) OCR engines. See Change default OCR language . |
| System tab | | Use this tab to: <ul style="list-style-type: none"> • Examine the log file for any errors. • View the version and location of the service file. • Check if Java Access Bridge is installed on the computer where the service is running. See Check Java Access Bridge. • Restart your computer frequently when you cannot use the automatic login feature of Windows. See Configure the host. |
| Management Console options | server.conf option | Value and description |
| MC Path Connection protocol, name or IP address, port number, and path of the Management Console the device must register with. The format is as follows: http://10.10.0.136:50080 | hostName | Name or IP address of the Management Console the device must register with. |
| | port | Connection port of the specified Management Console. |
| | schema | Connection protocol of the specified Management Console. |
| | path | Empty (default). Leave this parameter empty for an embedded Management Console installation. For a standalone installation, after the port number, specify the part of the path to the standalone Management Console. For example, if your Management Console is deployed on Tomcat at: http://computer.domain.com:8080/ManagementConsole/ then you would specify "/ManagementConsole/". |
| Authentication Specifies the method of authentication with the Management Console. | authType: ServiceAuthentication | Select Service Authentication to authenticate as DAS using a shared secret configured in the Management Console. See also "Service authentication" in <i>Kofax RPA Help</i> . |

| Configuration window option | server.conf option | Value and description |
|---|-------------------------------------|---|
| | authType: UsingManagementConsole | Select Using Management Console to interactively authenticate with the Management Console as a user. |
| Shared Secret | sharedSecret | Enter the shared secret configured in the Management Console. |
| Cluster | cluster | Production (default). Cluster name on the specified Management Console. |
| Labels | labels | Empty (default). Labels to distinguish the automation devices. |
| Ping interval (ms) | pingInterval | 5000 (default). Time interval for the Desktop Automation Service to ping the Management Console. |
| Use proxy to connect to Management Console | useProxy | <p>Select this option for the Desktop Automation Service to use as a proxy when connecting to Management Console.</p> <p>Specify all parameters in the fields.</p> <p>Example:</p>  <p>For Linux installations, you can set up proxy parameters in the managementConsole section of the server.conf file.</p> <pre>"useProxy": true, "proxyHostName": "proxyhost.com", "proxyPort": 9000, "proxyUserName": "username", "proxyPassword": "pwd"</pre> |

Manage Desktop Automation Service

Click the Desktop Automation Service shortcut menu to access the following options.



Use these options to manage the Desktop Automation Service running on a remote computer.

- **Stop DA service:** Stops the service, which makes the remote device unavailable. The computer running the Desktop Automation Service is removed from the list in the Management Console.
- **Restart DA service:** Stops and starts the service. A robot or Design Studio loses the connection to the device and must be reloaded to restore it.
- **Suspend DA service:** Suspends the device. If suspended, the service is displayed as suspended in the Management Console. To restore the service operation, a user or an administrator needs to manually start the Desktop Automation Service on the device.

The suspended state makes the DA service unavailable for robots to use, but the state information is sent to the Management Console through the ping mechanism and the devices are displayed in the **Admin > Devices** section. This command is useful if for some reason the service or the computer running it needs configuration changes.

- **Lock Screen:** Locks the screen on the remote device. The Desktop Automation Service must be installed and configured before you can use this option. See "Use Lock Screen" in the *Desktop Automation Service Guide*.
- **Configure:** Opens the Desktop Automation Service configuration dialog box. See the *Kofax RPA Desktop Automation Service Guide*.