

Kofax Kapow

Desktop Automation Service User's Guide

Version: 10.3.2

Date: 2018-11-07



© 2018 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: Desktop Automation Service Configuration.....	4
Desktop Automation Prerequisites.....	4
Configure the Desktop Automation Service.....	4
Configure Proxy Servers in Desktop Automation.....	10
Change Default OCR Language.....	10
Manage Remote Desktop.....	11
Manage the Desktop Automation Service.....	11
Use Lock Screen.....	11

Chapter 1

Desktop Automation Service Configuration






Desktop Automation Prerequisites

All Desktop Automation requirements and prerequisites are listed in the "System Requirements chapter" of the Kofax Kapow *Installation Guide*.

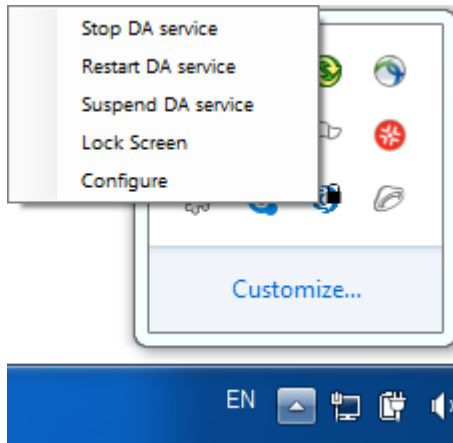
Configure the Desktop Automation Service

Once your computers meet all the necessary requirements for Desktop Automation, you can install and configure the Desktop Automation Service.

1. If you need to automate Java applications, install Java 32-bit (JRE or JDK) on remote devices and check that the Java Access Bridge is enabled on your devices.
2. Download and run the Kapow Desktop Automation installer on your device.
3. Start the Desktop Automation Service from the Start menu. Once the service starts, you can see its status by looking at the icon in the notification area.

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

4. To edit the Desktop Automation Service parameters, right-click the Desktop Automation Service icon in the notification area and select **Configure**. This opens the Desktop Automation Service window. After changing the options, click **Save and Restart**.



To manually edit the options, open the `server.conf` file on your automation device. The file is located in `Users > UserName > AppData > Local > Kapow 10.3.2` directory where `UserName` is the name of the user the service is running under.

See the table with Desktop Automation Service options below.

5. Check that the device is registered in the Management Console under **Admin > Devices** tab.

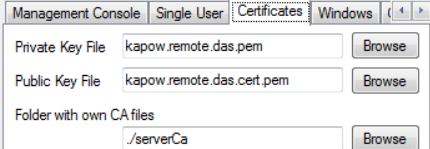
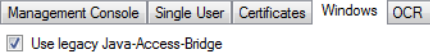
Admin > Devices		
<input type="button" value="Expand All"/> <input type="button" value="Collapse All"/>		
Cluster/Device	Status	Labels
Production <ul style="list-style-type: none"> kk80beta2.emea.kofax.com:49998 	Running Available	win2003,sap

The following is a Desktop Automation Service configuration window.

The following table lists the available Desktop Automation Agent options.

Configuration Window Option	server.conf Option	Value and Description
Single User Clear (default) Select for direct connection to the Automation Device from Design Studio or when using the RDP connection.	"singleUser"	false (default) true Set to false to automatically register the Desktop Automation Agent with the specified Management Console. For direct connection to the Automation Device, set to true and specify a token.*

Configuration Window Option	server.conf Option	Value and Description
Host name	"hostName"	Name or IP address of the computer running the Desktop Automation Agent. 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.
Command port	"commandPort"	49998 (default) Reassign this port for the Automation Device if necessary.
Stream port	"streamPort"	49999 (default) This port is used to send data between Design Studio and the Desktop Automation Agent. If streamPort is set to "0", the Desktop Automation Agent selects a random port number. You might need to assign the streamPort if there is a firewall between Design Studio and the Automation Device.
CA file	"caFile"	empty (default) You can communicate with the Management Console using SSL. If the default certificate in <code>node.js</code> is not used, you can specify a path to another certificate file using this parameter.
Timeout	"commandTimeout"	This option specifies the timeout for command execution in seconds. 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. If a command cannot be completed in a specified time, the service sends a notification and execution of the robot stops. Note that in case of a Location Found guard, this setting applies to invoking the guard in the workflow, but waiting for the guard to be satisfied is not bound to this timeout and can wait forever. 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. The command timeout for automating terminals or browsing websites in Desktop Automation Workflow is set either on the Desktop Automation tab of the Design Studio Settings window for executing the workflow in Design Studio, or in the Desktop Automation section on the Security tab of the RoboServer Settings window for roboServer execution.

Configuration Window Option	server.conf Option	Value and Description
Token on Single User tab	"token"	empty (default) If the "singleUser" option is set to <i>false</i> , leave this option empty. If you use the direct connection to the Automation Device ("singleUser": <i>true</i>), specify a token. It can be any token you define.
List of drivers to load at startup, such as Windows, TN3270, TN5250, VT100, and others Windows (default)	"drivers"	["automationnative"] (default) You can select drivers to load at startup. Windows is the default driver for automating native Windows and Java applications. Leave this parameter as is. To access a terminal from the Automation Device, select the corresponding driver.
Certificates tab 	"tlsServerConfig"	Kapow provides TLS communication between the Automation Device and the RoboServer or Design Studio. The communication uses certificates for encrypting the communication. The following is a <i>server.conf</i> file code extract. For more information, see "Use TLS Communication" in the Kapow help. <pre> "tlsServerConfig": { "key": "kapow.remote.das.pem", "cert": "kapow.remote.das.cert.pem", "ca": "./serverCa" }, </pre>
Windows tab 	"automationnative"	"useLegacy" : In some situations, the Java Access Bridge does not work and it can help to switch to legacy mode. Default is <i>false</i> .
OCR	"ocrConfig"	"defaultLanguage" : "eng" Specifies a language to perform an OCR operation. By default, Kapow installs the English language. See Change Default OCR Language below for language installation instructions.
System tab Use this tab to open and examine the log file for any errors, or to view the version and location of the service file.		
Management Console Options		
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.

Configuration Window Option	server.conf Option	Value and Description
	"path"	empty (default) The part of the path to the standalone Management Console after the port number. For example, if your Management Console is deployed on Tomcat at <code>http://computer.domain.com:8080/ManagementConsole/</code> , specify <code>"/ManagementConsole/"</code> in this parameter. Leave this parameter empty for the embedded Management Console installation.
User name	"user"	empty (default) User name to authenticate on the specified Management Console.
Password	"password"	empty (default) Password to authenticate on the specified Management Console.
Cluster	"cluster"	Production (default) Cluster name on the specified Management Console.
Labels	"labels"	"label1,label2" (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"	Select this option for the Desktop Automation Service to use as a proxy when connecting to Management Console. All necessary parameters are specified in the following fields. <input checked="" type="checkbox"/> Use proxy to connect to Management Console Proxy host name <input type="text" value="proxyhost.com"/> Proxy host port <input type="text" value="9000"/> Proxy user name <input type="text" value="username"/> Proxy password <input type="password" value="●●●"/> Under Linux, you can set up proxy parameters in the <code>managementConsole</code> section of the <code>server.conf</code> file. <pre>"useProxy": true, "proxyHostName": "proxyhost.com", "proxyPort": 9000, "proxyUserName": "username", "proxyPassword": "pwd"</pre>

* 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 Kapow help.

Configure Proxy Servers in Desktop Automation

All Desktop Automation Service robots can use the Kapow global proxy settings. The Desktop Automation Service uses the same proxy settings as Design Studio and Management Console. There are two ways to configure proxy server settings.

Important Remember that the local proxy settings of the built-in browser in Desktop Automation Service have a higher priority than the Kapow global proxy settings. Make sure the robot uses the Kapow global proxy settings, unless the task requires it to use local proxy settings. For more information on Desktop Automation, see the Kofax Kapow online Help.

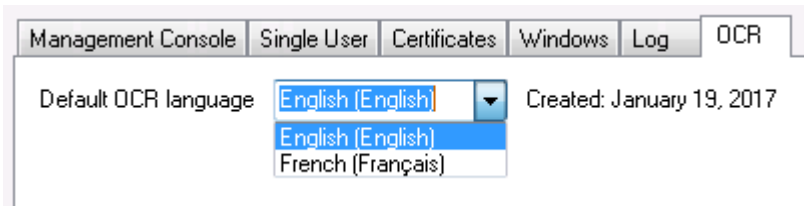
1. For all robots running in the Desktop Automation Service, in the Design Studio Settings dialog box, on the Proxy Servers tab, complete the following Proxy Server details.
 - Host
 - Port number
 - Username
 - Password
 - Excluded hosts
2. For all deployed robots, in Management Console > Cluster Settings> Proxy Servers tab, select Add Proxy Server and complete the following Proxy Server details.
 - Host name
 - Port number
 - User name
 - Password
 - Excluded host names

Change Default OCR Language

Kapow uses the Tesseract OCR engine to capture text from images. By default, Kapow installs the English language for OCR. When your robot performs text recognition in the Extract Text From Image Step, the Desktop Automation Service uses the language selected on the **OCR** tab of the Desktop Automation Service window. To change the default language for OCR, perform the following steps.

1. Download the `.traineddata` file for the required language from the <https://github.com/tesseract-ocr/tessdata>. For example, the file for the French language is `fra.traineddata`.
2. Copy the downloaded trained data file to `DesktopAutomationService\lib\tessdata` in the Desktop Automation service installation directory. Example:

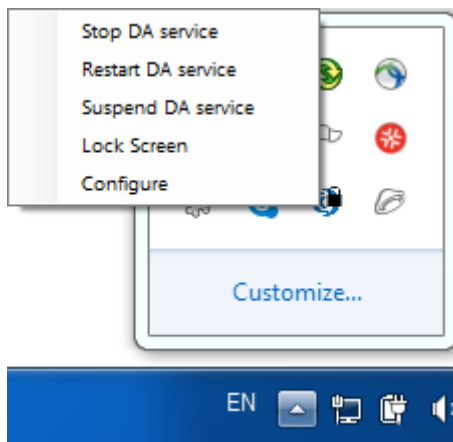
```
C:\Program Files (x86)\Kapow DesktopAutomation 10.1.0  
x32\DesktopAutomationService\lib\tessdata
```
3. Right-click the Desktop Automation icon in the notification area and select **Configure**.
4. Click the **OCR** tab and select a language in the **Default OCR language** list.



Click **Save and Restart**.

Manage Remote Desktop

You can perform the following actions using the Desktop Automation Service shortcut menu.



Manage the Desktop Automation Service

The following commands help you manage the Desktop Automation Service running on a remote computer.

- **Stop DA service:** Stops the service, which makes the remote device unavailable.
- **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.

Use Lock Screen

In some cases it is necessary to lock computer screens when working with automation devices. You can lock a screen by using the **Lock Screen** command on the Desktop Automation Service menu. Before locking your device screen, make sure the service is running and it is in the connected state. To lock a screen, right-click the Desktop Automation Service icon and select **Lock Screen**.

If Windows is configured to show an extra screen when the user logs in, Lock Screen tries to detect this extra screen and dismiss it by pressing OK. If this 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 do not suffice, add a `KAPOW_LEGALNOTICE_SECONDS` system variable in the environment variables on your automated device, and set the number of seconds in the *Variable value* field to wait before dismissing the window after the connection. Restart the Desktop Automation Service after adding the variable.

Lock Screen Usage Prerequisites

To use the Lock Screen feature with Desktop Automation, your device must meet the following requirements.

- Remote Desktop connection must be enabled.
- The user under which the Desktop Automation Service runs must be allowed to connect via Remote Desktop (as a member of the Admin group or the Remote Desktop group) and use a password.
- The effective group policy of **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security > "Always prompt for password upon connection"** must be off.
- Port 3389 must be open.
- The Automation Device cannot be a domain controller.