Kofax Kapow

Device Automation Service User's Guide

Version: 10.2.0.1

Date: 2017-09-29

Table of Contents

Chapter 1

Device Automation Service Configuration

Device Automation Prerequisites

This topic provides a list of components that must be installed and configured on the Automation Device before you can use Kapow.

Java Access Bridge
To automate Java programs or Java applets on remote devices with Kapow, install Java 32-bit on your device (JRE or JDK) and enable the Java Access Bridge in the Java Runtime Environment used by the application. We recommend using the latest available Java version.

For JRE 7 or Later

To enable Java Access Bridge for Java version 7 or later, navigate to the `bin` directory in the Java installation directory and run the following command.

```
jabswitch -enable
```

For JRE6
Follow this procedure to install Java Access Bridge 2.0.2 on a Windows 32-bit system. For older applications that require Java version 1.6, copy the following files to the specified destination directories, where %WINDOWSHOME% is the directory where Microsoft Windows is installed (for example, C:\WINDOWS), and %JAVAHOME% is the directory where your JDK or JRE is installed. The following are examples of directory names for Java SE 6 Update 24.

- `JDK: C:\Program Files\Java\jdk1.6.0_24\jre`
- `JRE: C:\Program Files\Java\jre6`

The following table lists Java Access Bridge Windows Libraries and Related Files for Windows 32-bit

Java Access Bridge File	Destination Directory
`WindowsAccessBridge.dll`	`%WINDOWSHOME%\SYSTEM32`
`JavaAccessBridge.dll`	`%JAVAHOME%\bin`
`JAWTAccessBridge.dll`	`%JAVAHOME%\bin`
`accessibility.properties`	`%JAVAHOME%\lib`
`access-bridge.jar`	`%JAVAHOME%\lib\ext`
`jaccess.jar`	`%JAVAHOME%\lib\ext`

For more information, search the Downloads page on the Oracle web site (http://www.oracle.com/technetwork/java/javase/downloads/) to locate and download jab-2-0-2. For installation instructions, see installing-jab-32-bit on the http://docs.oracle.com website.

Perform the following to test that you have installed Java Access Bridge properly.

1. Run the SwingSet2 application and then run the JavaMonkey.exe application.
2. Select **File** > **Refresh Tree** in the Java Monkey application and the SwingSet2 application should appear.

Alternatively, you can use the JavaFerret.exe application.

Device Automation on Windows

If you get the error: "Module automationnative not found", install the following update.

https://support.microsoft.com/en-us/kb/2999226

On some systems Windows Update is not available, but there is a workaround to install updates.

1. Create a `c:\temp\976571` folder.
2. Use the following command to extract the contents of the MSU file:

   ```
   Expand -F:* c:\kb976571\Windows6.1-KB976571-v2-x64.msu c:\temp\976571
   ```

   This command extracts multiple files, from the `Windows6.1-KB976571-v2-x64.cab` file.
3. Run the following command:

   ```
   DISM.exe /Online /Add-Package /PackagePath:c:\temp\976571\Windows6.1-KB976571-v2-x64.cab
   ```

For more information, see *How to use DISM to install a hotfix from within Windows* on the Microsoft Technet website https://blogs.technet.microsoft.com.

Prerequisites for Internet Explorer

To automate Internet Explorer using the Device Automation feature, check the following requirements.

- For IE 11 only, check that a `FEATURE_BFCACHE` subkey with a `DWORD` value named `iexplore.exe` is present in the registry on the target computer. This subkey enables the driver to maintain a connection to the instance of Internet Explorer it creates. For 32-bit Windows, examine the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BFCACHE` key in the registry editor. For 64-bit Windows, examine the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BFCACHE` key. If the `FEATURE_BFCACHE` subkey is not present, create it and create a `DWORD` value named `iexplore.exe` with the value "0" in the key.
- For IE 10 and higher, disable the Enhanced Protected Mode in the Security settings on the Advanced tab of the Internet Options window.
- In Internet Explorer 7 and higher on Windows Vista and Windows 7, set the same value (either On or Off) in the Protected Mode settings for each zone. To open the Protected Mode settings in Internet Explorer, select **Tools** > **Internet options** and click the **Security** tab. For each zone, select the **Enable Protected Mode** option and select the same security level.
- Set the browser zoom level to 100% to align the native mouse events with the correct coordinates.

Note In some cases, out-of-browser Silverlight applications can interfere with Device Automation. The cause of the problem is the Internet Explorer subdriver. To disable the IE subdriver, clear the **Extended Internet Explorer Support** option on the **Windows** tab of the Device Automation Service configuration window.

SAP Prerequisites
To automate SAP application using the Device Automation feature, enable scripting on both the server and the client sides.

- On the client, go to **SAP GUI Options** and enable scripting. Also, turn off notifications, because they interrupt the automation process.
- To enable scripting on the SAP server, perform the following steps. Note that you must have administrative privileges to change the `sapgui/user_scripting` parameter.
  1. Logon to your SAP server.
  2. Run transaction RZ11. Specify the parameter name `sapgui/user_scripting` and click **Display**. If `Parameter name is unknown` appears in the status bar, this indicates that you are missing the current support package. Check your installed packages.
  3. Change the value to `TRUE`.
  4. Click **Save**.

Note that some elements, such as scroll bars, can only be available if you run the SAP client on a machine with a Windows Classic desktop theme.

Configure the Device Automation Service

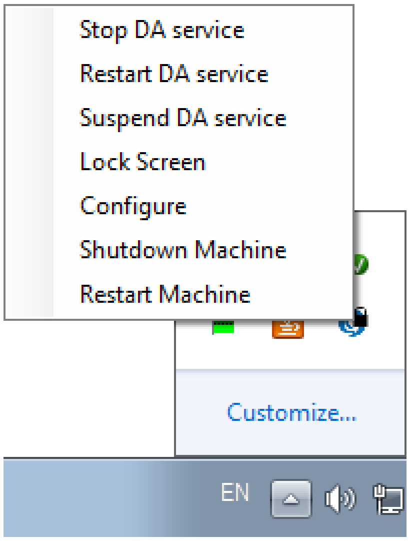
Once your computers meet all the necessary requirements for device automation, you can install and configure the Device Automation Service.

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 Device Automation installer on your device.
3. Start theDevice 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
◎	Device Automation Service is starting and trying to connect to the configured Management Console.
◎	Device Automation Service is running and either connected to a Management Console or running in single user mode depending on configuration.
◎	Device Automation Service is running and in use by RoboServer or Design Studio.
◎	Device Automation Service is not running.

Icon	Status
⚠	Device Automation Service is not running due to an error.

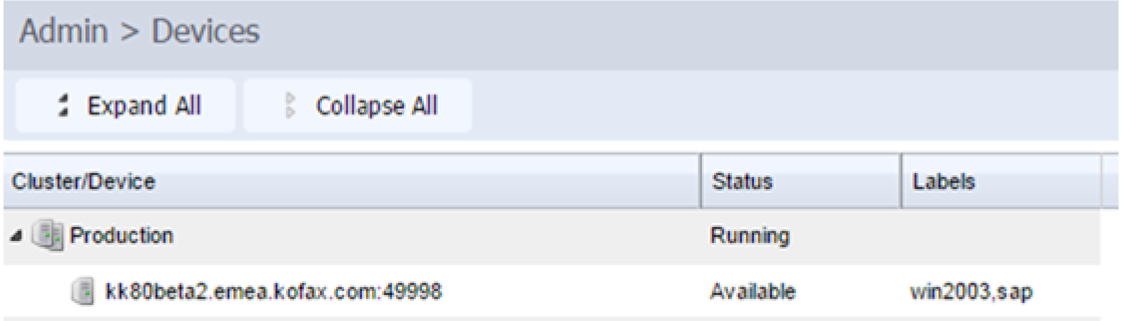
4. To edit the Device Automation Service parameters, right-click the Device Automation Service icon in the notification area and select **Configure**. This opens the Device Automation Service window. After changing the options, click **Save and Restart**.



To manually edit the options, open the `server.conf` file on your Automation Device. The file is located in **Users** > **UserName** > **AppData** > **Local** > **Kapow10.2.0.1** directory where UserName is the name of the user the service is running under.

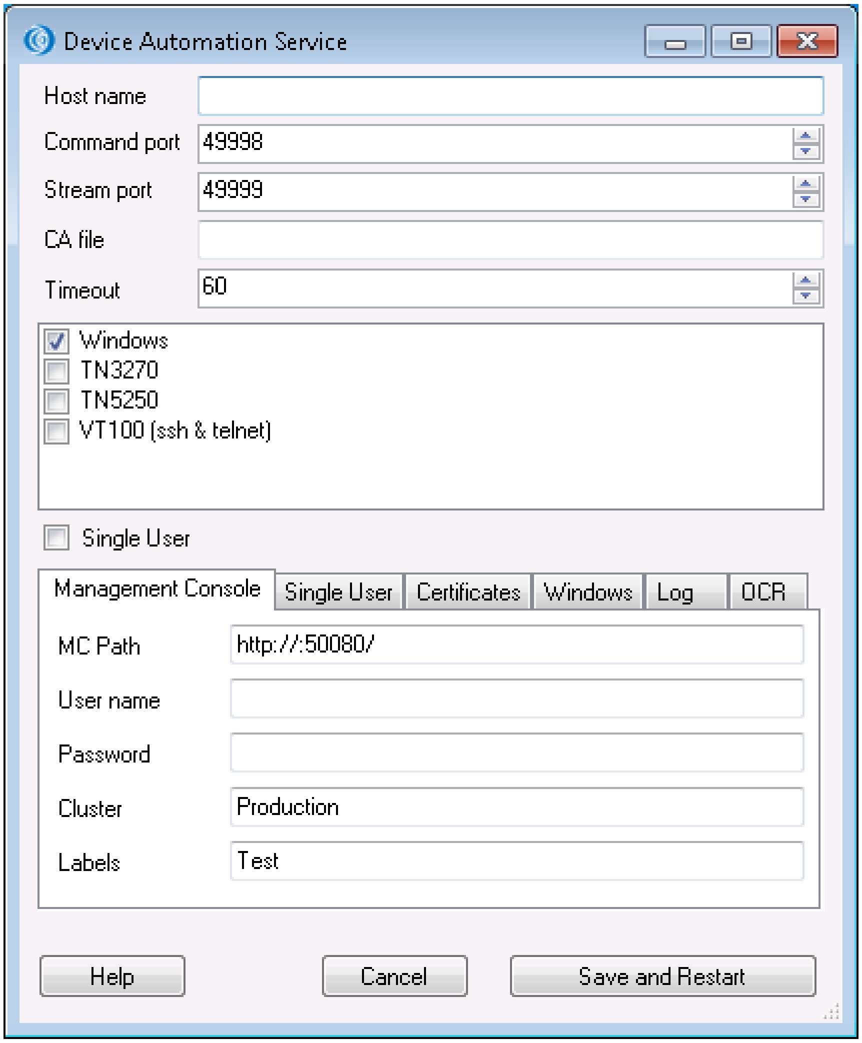
See the table with Device Automation Service options below.

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



Cluster/Device	Status	Labels
Production	Running	
kk80beta2.emea.kofax.com:49998	Available	win2003,sap

The following is a Device Automation Service configuration window.



Device Automation Service

Host name	
Command port	49998
Stream port	49999
CA file	
Timeout	60

☑ Windows
☐ TN3270
☐ TN5250
☐ VT100 (ssh & telnet)

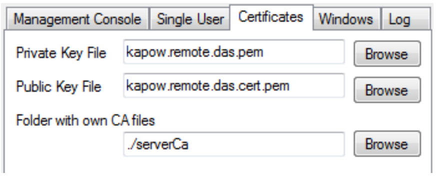
☐ Single User

MC Path	http://:50080/
User name	
Password	
Cluster	Production
Labels	Test

The following table lists the available Automation Device 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 Automation Device Agent with the specified Management Console. For direct connection to the Automation Device, set to `true` and specify a token.*

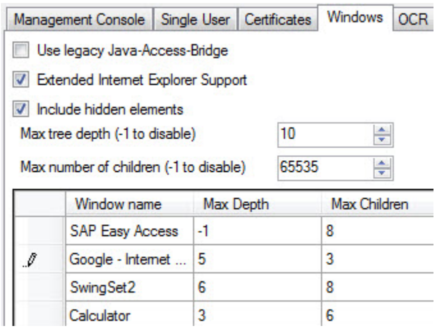
Configuration Window Option	server.conf Option	Value and Description
Host name	"hostName"	Name or IP address of the computer running the Automation Device Agent. If a computer has multiple names or IP addresses, specify the one that RoboServers and Design Studio contact this Automation Device Agent with. 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 Automation Device Agent. If streamPort is set to "0", the Automation Device 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 `node.js` 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. If a command cannot be completed in a specified time, the service sends a notification and execution of the robot stops.
Token on **Single User** tab	"token"	empty (default) If the "singleUser" option is set to `false`, leave this option empty. If you use the direct connection to the Automation Device (`"singleUser": true`), 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 terminal from the Automation Device, select the corresponding driver.

<table>
<tr><th>Configuration Window Option</th><th>server.conf Option</th><th>Value and Description</th></tr>
<tr><td><b>Certificates</b> tab


Private Key File kapow.remote.das.pem
Public Key File kapow.remote.das.cert.pem
Folder with own CA files ./serverCa</td><td>"tlsServerConfig"</td><td>Kapow provides TLS communication between Automation Device and RoboServer or Design Studio. The communication uses certificates for encrypting the communication. The following is a <code>cerver.conf</code> file code extract. For more information see Use TLS Communication in Kapow help.<pre>
   "tlsServerConfig": {
     "key": "kapow.remote.das.pem",
     "cert":
  "kapow.remote.das.cert.pem",
     "ca": "./serverCa"
   },
</pre></td></tr>
</table>

<table>
<tr><th>Configuration Window Option</th><th>server.conf Option</th><th>Value and Description</th></tr>
<tr>
<td>

Windows tab



□ Use legacy Java-Access-Bridge
☑ Extended Internet Explorer Support
☑ Include hidden elements
Max tree depth (-1 to disable) 10
Max number of children (-1 to disable) 65535

<table>
<tr><th>Window name</th><th>Max Depth</th><th>Max Children</th></tr>
<tr><td>SAP Easy Access</td><td>-1</td><td>8</td></tr>
<tr><td>Google - Internet ...</td><td>5</td><td>3</td></tr>
<tr><td>SwingSet2</td><td>6</td><td>8</td></tr>
<tr><td>Calculator</td><td>3</td><td>6</td></tr>
</table>

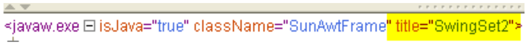
</td>
<td>"automationnative"</td>
<td>

"useLegacy": In some situations the Java Access Bridge does not work and it can help to switch to legacy mode. Default is false.

"maxTreeDepth": The maximum number of nested elements shown in the Automation Device View in Design Studio.

- -1: no restrictions.
- 65535: the maximum number of elements.

defaultMaxTreeDepth and DefaultMaxChildrenCount set the default tree depth and a maximum number of children elements each node shows for all application windows in the view. You can set restrictions on a particular application window in the table below the **Max number of children** option or by specifying maxDepth and maxChildren properties in the "window": [] property. For the window name use the title attribute.



<javaw.exe ⊟ isJava="true" className="SunAwtFrame" title="SwingSet2">

"ieSupport": Support for working with Internet Explorer on the Automation Device. See Prerequisites for Internet Explorer for more information.

"includeHidden": Specifies whether to extract the entire widget tree of an application. Default is true. If the option is set to false, Kapow skips elements that are reported as off-screen, such as list boxes or tables with many elements. Deselect (or set to false) this option to reduce the time needed to extract the tree.

```
"automationnative": {
    "useLegacy": false,
    "maxTreeDepth": {
      "defaultMaxTreeDepth": 10,
      "DefaultMaxChildrenCount":
 65535,
      "window": [
        { "name": "SAP Easy Access",
          "maxDepth": -1,
          "maxChildren": 8 },
        { "name": "Google - Internet
 Explorer",
          "maxDepth": 5,
          "maxChildren": 3 },
        { "name": "SwingSet2",
          "maxDepth": 6,
          "maxChildren": 8 },
        { "name": "Calculator",
          "maxDepth": 3,
          "maxChildren": 6 }
      ]
    },
    "ieSupport": true
    "includeHidden": true }
```

</td>
</tr>
</table>

Configuration Window Option	server.conf Option	Value and Description
Log tab This tab helps you open the log file to examine for any errors and shows the version and location of the service file.		
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.
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.
	"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 http://computer.domain.com:8080/ManagementConsole/, specify `"/ManagementConsole/"` 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.
	"pingInterval"	5000 (default) Time interval for the Automation Device Agent to ping the Management Console.
Cluster	"cluster"	Production (default) Cluster name on the specified Management Console.
Labels	"labels"	"label1,label2" (default) Labels to distinguish the Automation Devices.

* 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 RDP connection. See Use RDP Connection in Kapow help.

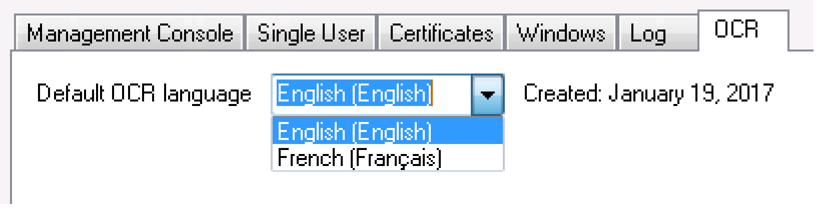
Change Default OCR Language

Kapow uses the Tesseract OCR engine to capture text from images. By default, Kapow installs English language for OCR. When your robot performs text recognition in the Extract Text From Image Step, the Device Automation Service uses the language selected on the **OCR** tab of the Device 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 downloaded trained data file to `DeviceAutomationService\lib\tessdata` in the Device Automation service installation directory. Example:

   ```
   C:\Program Files (x86)\Kapow DeviceAutomation 10.1.0 x32\DeviceAutomationService
   \lib\tessdata
   ```

3. Right-click the Device Automation icon in the notification area and select **Configure**.
4. Click the **OCR** tab and select a language in the **Default OCR language** list.

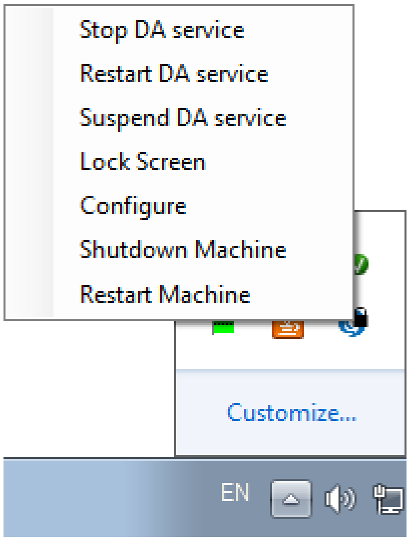
   Default OCR language English (English)

   Created: January 19, 2017

   Click **Save and Restart**.

Manage Remote Device

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



Manage the Device Automation Service

The following commands help you manage the Device 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 Device 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 Device 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 Device Automation Service icon and select **Lock Screen**.

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

- Remote Desktop connection must be enabled.
- The user under which the Device 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.

Manage the Automation Device

The following shortcut menu commands help you restart and shut down the computer running Device Automation Service.

- **Shutdown Machine**: Shuts down the computer.
- **Restart Machine**: Restarts the computer.