How can I configure my SIP2 device to work with WMS?

Last updated: Thu, 16 Jun 2022 18:37:58 GMT

Applies to

- WorldShare Circulation

Answer

There are several steps to set up a SIP2 device to work with WMS. These are listed below.

If you need help configuring the device, see your user manual or ask your vendor. Unfortunately, OCLC cannot help with how to configure different devices.

OCLC SIP2 configuration only supports IP authentication with SIP2 devices.

Step 1: Give the device a unique external IP address, or set a username and password for the device.

Ideally, each device will have its own, unique external IP address.

WMS's SIP2 will work with Network Address Translation (NAT), where multiple devices will use the same external address, but you must give each device a username and password. This helps WMS identify which device the transactions are coming from.

Step 2: Decide if you will use an encrypted SIP2 connection or an unencrypted one

By default, SIP2 sends its messages as plain text over the internet, meaning they can be easily intercepted and read.

OCLC recommends encrypting your SIP2 connection, so all the information exchanged is secure.

- **For encrypted connections**: you will need to install SLL tunneling software on your device. A suitable candidate is **stunnel**. Work with your IT department or vendor to install it. Note that our SIP2 servers do not require an SSL certificate to be added - they use IP Address recognition to authenticate the SIP connection. A program like stunnel is only used to secure the communication between the device and our servers.

- **For unencrypted connections**: OCLC will ask you to sign a waiver in case any of your patron's personal information is intercepted. Please contact **OCLC Support** to discuss this option.
Step 3: Add the hostname and port for OCLC's SIP2 server to your device

Please contact OCLC Support to confirm which hostname you should use - it will depend on which data center your WMS instance has been set up in.

OCLC recommends that you use the hostname rather than the IP address, in case the IP address changes. But the IP address will work if your system does not support hostnames.

Whether you use the **unencrypted port** number or the **encrypted port** number depends on whether you set up SSL tunneling in Step 2 above.

<table>
<thead>
<tr>
<th>DATA CENTER</th>
<th>HOSTNAME</th>
<th>IP ADDRESS</th>
<th>UNENCRYPTED PORT</th>
<th>ENCRYPTED PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dublin (United States)</td>
<td>sip2.sd00.worldcat.org</td>
<td>132.174.0.71</td>
<td>2090</td>
<td>2093</td>
</tr>
<tr>
<td>Amsterdam (Europe)</td>
<td>sip2.sd02.worldcat.org</td>
<td>193.240.184.103</td>
<td>2090</td>
<td>2093</td>
</tr>
<tr>
<td>Sydney Australia</td>
<td>sip2.sd03.worldcat.org</td>
<td>113.29.23.195</td>
<td>2090</td>
<td>2093</td>
</tr>
<tr>
<td>Toronto Canada</td>
<td>sip2.sd04.worldcat.org</td>
<td>38.117.94.67</td>
<td>2090</td>
<td>2093</td>
</tr>
</tbody>
</table>

Step 4: In Service Configuration, configure your SIP2 Connection

The SIP2 Connection settings determine how SIP2 devices will interact with WMS, including which messages are accepted, what sort of information WMS will send, and how items are to be sorted by automatic sorting machines.

These settings are configured at the branch level - all SIP2 devices at that branch will use the same settings.

Follow the instructions on the **SIP2 Configuration** page.

Step 5: In Service Configuration, configure the SIP2 IP address

The SIP2 IP Address settings tell WMS which IP address to accept communication from. You can also set the device’s username and password here.

Note that this username and password is only for SIP2. It is completely separate from WMS accounts.

Follow the instructions on the **SIP2 IP Address** page.
Step 6: (Optional) In Service Configuration, configure the SIP2 Custom Messages

The SIP2 Custom Messages page lets you customise the messages that are displayed to the device's user when certain events happen. It also lets you provide those messages in multiple languages.

This step is optional. If you do not change the SIP2 Custom Messages, the default messages will be used.

Follow the instructions on the SIP2 Custom Messages page.

Step 7: Test your device

Once the device is configured, test it. Try placing a check-in or check out.

If the test doesn't work, contact OCLC Support. To help us troubleshoot the problem, include as much of this information as possible:

1. What is the institution name, OCLC symbol, and branch? (remember, SIP2 is configured by branches)
2. What is the exact make, model, and IP address of the SIP2 device?
3. What is the error message or problem? Can we get a screenshot from the device?
4. What were the exact actions that caused the problem?
5. What date and time did the problem happen? This helps us check our log files.
6. Is there a log file from the SIP2 device? Please send it to us.

Additional information

SIP2 Configuration
SIP2 IP Address
SIP2 Custom Messages

Page ID
32358