Learn how to use NCIP authentication tasks and terms to configure FirstSearch for your library.

## Tasks

### Identify and test the local system host and port

An administrator has the ability to identify one local system per FirstSearch authorization for use in authenticating patron access to the circulation system.

Complete the following steps to perform this task.

<table>
<thead>
<tr>
<th>ACTION</th>
<th>RESULT OR NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Local System Host and Port field, enter a local system host and port string that identifies the local system you want to define for authenticating patron access. OCLC uses only https protocol to talk to your local system host, so your local system must support https. <strong>Example:</strong> <a href="https://sp03e15.prod.oclc.org:4103">https://sp03e15.prod.oclc.org:4103</a></td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Save Changes</strong>. The system displays, &quot;NCIP screen changes saved,&quot; under the screen title.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Test</strong>. If the test is successful, the system displays a FirstSearch login screen that shows local prompts for NCIP access. If the test is not successful, the system displays an error message similar to the following: NCIP messaging problem. Please contact your library's system</td>
</tr>
</tbody>
</table>

https://help.oclc.org/Discovery_and_Reference/FirstSearch/Authentication/NCIP_access/NCIP_authentication_tasks

Printed: Fri, 12 Jun 2020 01:46:11 GMT
Control requirements for authenticating access to FirstSearch

An administrator has the ability to control whether or not a patron logging in to FirstSearch must be log on with both a known IP address and approved NCIP access.

**Note:** If IP address recognition is not already set up for your authorization, you'll receive an error message when you try to save changes.

Complete the following steps to perform this task.

<table>
<thead>
<tr>
<th>ACTION</th>
<th>RESULT OR NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want to require a patron logging in to FirstSearch to have to log in from a known IP address and have approved NCIP access, check the On box.</td>
<td>The default state of the On box is <em>not checked</em>.</td>
</tr>
<tr>
<td>If you do not want to require a patron logging in to FirstSearch to have to log in from a known IP address and have approved NCIP access, do not check the On box.</td>
<td>The system displays, &quot;NCIP screen changes saved,&quot; under the screen title.</td>
</tr>
</tbody>
</table>

Add an addendum to the error message displayed for unsuccessful logins

An administrator has the ability to add a custom-text addendum to the system-generated error message reporting an unsuccessful NCIP login attempt.

Complete the following steps to perform this task.
<table>
<thead>
<tr>
<th>ACTION</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Error Message Addendum text entry box, type custom text to be appended to the system error message reporting an unsuccessful NCIP login attempt. Include specific contact information such as the name and phone number of the person to contact.</td>
</tr>
<tr>
<td>Example: Call I. Fixitall at 555-1234.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Save Changes</strong>.</td>
</tr>
</tbody>
</table>

**Construct URLs**

IP address recognition can be used to trigger NCIP authentication. If you have existing IP address recognition URLs, you can reconfigure them with NCIP to allow access using IP address recognition and/or NCIP authentication.

**NCIP authentication only**

The following sample URLs allow access to the FirstSearch service using only NCIP authentication:

- https://host:port/FSNCIP?ncipautho=xxx
- https://host:port/FSNCIP?autho=xxx

**Note:** The FSNCIP parameter signifies only NCIP will be used. An authorization is required in the URL. These samples assume authorization XXX is configured with NCIP details in the administrative module.

**IP and/or NCIP, same authorizations**

These sample URLs allow access to the FirstSearch service using IP recognition and/or NCIP authentication:

- https://host:port/FSIP?autho=xxx
- https://host:port/FSIP
- https://host:port/FSIP?ncipautho=xxx
The nicipautho parameter is used when the IP authorization and the NCIP authorization are different (this allows you to create a single URL for access to the FirstSearch service that can be used for both IP and for remote users).

The autho= parameter denotes a secondary authorization for IP purposes. If an authorization is noted, it will be used to check whether NCIP authentication should be attempted. If no authorization is noted, the primary authorization associated with the IP address will be checked to see if NCIP authentication should be attempted.

In the administrative module, for a given authorization, you can indicate whether both IP and NCIP must be successful for access to the service. In this case, the above URLs can all be used as long as the IP authorization and the NCIP authorization are the same (regardless of whether they are noted in the URL).

**IP and/or NCIP, different authorizations**

The following sample URLs can be used when the authorization for IP and the authorization for NCIP are different:

https://host:port/FSIP?ipautho=xxx&nicipautho=yyy

https://host:port/FSIP?nicipautho=xxx

This allows a single URL for FirstSearch access that attempts NCIP authentication only in the event that IP address recognition fails. All IP parameters, such as screen name, database, and others will also work with NCIP.

**Terms**

**toAgencyId**

The term *Agency* refers to an institution, or to an agent operating on its behalf. Agencies are represented in NCIP messages by the parameters displayed in the *toAgencyId* and *fromAgencyId* fields.

The *toAgencyId* field is automatically assigned by OCLC to indicate the target institution (scheme) and its FirstSearch authorization (value).

Libraries should check with their local system vendor because they may need to enter the *toAgencyId* somewhere in their local system in order for NCIP messaging to be successful.

**fromAgencyId**

The term *Agency* refers to an institution, or to an agent operating on its behalf. Agencies are represented in NCIP messages by the parameters displayed in the *toAgencyId* and *fromAgencyId* fields.

The *fromAgencyId* field is automatically assigned by OCLC to indicate the specific context in which OCLC is sending the message.
Libraries should check with their local system vendor because they may need to enter the `fromAgencyId` somewhere in their local system in order for NCIP messaging to be successful.