WorldCat Navigator: EZproxy Configuration Guide

OCLC™

The world's libraries.
Connected.

Contents

WorldCat Navigator

EZproxy Configuration Guide

I. Introduction

This document describes authentication and session management operations within WorldCat Navigator. Included are instructions for configuring your downloaded EZproxy to allow session management via OCLC's userObject API, plus detailed instructions on how to configure EZproxy to allow proxied authentication between a library's remote user authentication systems (III, LDAP, and Shibboleth) and the Master EZproxy server.

About the process…

If you already have EZproxy installed and running on your system, you should begin with **Section 4, Configuring EZproxy to Allow userObject**.

If you do not yet have EZproxy installed in your system, you will follow a 4-step process:

1) Obtain an EZproxy license as described in **Section 2** below.
2) Once you have obtained your license, download and install EZproxy, following instructions at: http://www.oclc.org/us/en/support/documentation/ezproxy/setup.htm.
3) When EZproxy installation is complete, follow the instructions at: http://www.oclc.org/us/en/support/documentation/ezproxy/usr/ to enable basic authentication for your existing authentication method.
4) When initial authentication is enabled, follow the instructions in **Section 4, Configuring EZproxy to Allow userObject** and **Section 5** (for your authentication method).

Things you should know…

About Firewalls

Please allow traffic through your firewall:

- **To** these URLs on port **443**
  - masternavezp.idm.oclc.org
  - proxy.vdxhost.com
- **From** the above URLs for the port on which your EZproxy server listens

About SSL

In order to ensure the integrity of the small amount of patron data sent from your institution's EZproxy server to Navigator, Navigator requires Secure Socket Layer (SSL) encryption of this data between your institution and Navigator. In order to activate SSL, an SSL certificate is required. See **Section 6** of this document for more information.

About IP Address Changes

You should notify OCLC Support (support@oclc.org) if at any time you change the IP address or domain name of your EZproxy server. If you fail to notify OCLC of this change, Navigator will cease to work for your system.

Warning: If you have identified your interface via an IP address (rather than a DNS name), you must also update **`Interface <xxx.xxx.xxx>`** in `config.txt.`

About Home Library Locations

To ensure proper handling of ILL requests, the patron's home library should be specified when requesting is done by more than one library within an institution. Please contact your OCLC Implementation Manager for more information.

About E-Mail Addresses

The e-mail addresses used to send notifications to users may be stored in two separate places, depending upon how they are submitted to Navigator.

- Authentication Process: When submitted as part of the authentication process (patron loads, EZproxy authentication), the e-mail address becomes part of the user record in the OCLC Navigator database.
- Patron Request: When submitted as part of the Navigator Request form, the e-mail address becomes part of the request.

If an e-mail address is available in both the database and the request, the address from the request is used. If your institution does not implement user notification, there is no need to store the e-mail address in the user record (Navigator database).

2. Obtaining an EZproxy license

Navigator Request Engine users who do not already own a license may obtain a no-cost license by e-mailing exproxy@oclc.org to receive an order form (.pdf format). When you complete the form:

1. Leave the PRICE QUOTE and QUOTED BY areas empty.
2. Enter **WorldCat Navigator Participant — No Charge** in the COMMENTS area at the bottom of the form.

Print the completed form and return it via:

Mail: OCLC
6565 Kilgour Place
Dublin, OH 43017-3395

Fax: 1-888-339-3921

You will receive a welcome letter containing your license key.

The licensing agreement is included in the form. This agreement indicates the valid uses of EZproxy, including under what circumstances multiple copies of EZproxy can be used and also the valid use of EZproxy on multiple servers.

3. The EZproxy userObject

The EZproxy userObject is a data structure used to pass patron information among the various components of the Navigator system. Your local EZproxy must be configured to map data from your institution's authentication system into the userObject.

The EZproxy userObject consists of 42 attributes. Of these, the ten shown below provide primary data for Navigator operation. The full list of userObject attributes is given in Appendix B, EZproxy UserObject.

Attribute Name	Description	Required?
uid	patron barcode or unique ID	Always
forename	Patron first or given name	No (but recommended)
surname	Patron last or family name	No (barcode will be used if not provided)

emailAddress	Patron e-mail address	No (but recommended)
category	Patron type	No (but recommended)
location	Home library location	Yes, when applicable
joinDate	Join or registration date	No
expiryDate	Expiration date	No (requesting is not allowed after this date if a date is supplied)
bannedInRemoteCirculation	User privileges revoked	No (but recommended)

4. Configuring EZproxy to allow userObject

Once you have installed (or upgraded to) EZproxy 5.1c or later, you must manually edit the config.txt file to allow userObject support.

Before you begin

You must contact your OCLC Implementation Manager at WorldCatLocalIM@oclc.org to obtain your pre-assigned value for MYWSKEY (used in: `LocalWSKey MYWSKEY`).

Configure server for userObject

Step	Action
1	Open the *config.txt* file with a text editor.
2	Provide the DNS resolvable name of your local EZproxy server. Change: `Name ezproxy.hostname.edu` To: `Name <yourFullyQualifiedDomainName>`
3	Provide the DNS resolvable name or IP address of the local EZproxy server. Change: `Interface ezproxy.hostname.edu` To: `Interface <yourFullyQualifiedDomainName>` **OR** `Interface <yourIPaddress>` **OR** `Interface ANY` [binds to all IP addresses of your local EZproxy server]
4	To provide the SSL login port to be used in production:

	Change: **LoginPortSSL 443** To: **LoginPortSSL <yourPortNumber>**
5	To provide your pre-assigned WSKey: Change: **LocalWSKey MYWSKEY** To: **LocalWSKey <from your Implementation Manager>**
6	**Optional (for Linux and Solaris only; Windows environments skip this step).** To assign a RunAs user value (Linux and Solaris only): Change: **##RunAs nobody:nobody** To: **RunAs nobody:nobody**
7	**Optional.** To replace the admin console login port: Change: **LoginPort 2048** To: **LoginPort <yourPortNumber>**
8	Save and close *config.txt*, then re-start EZproxy
9	Edit the *user.txt* file of your EZproxy server according to the instructions in **Section 5** of this document. For example usr.txt files for various authentication systems, see: http://wcn.oclc.org/index.php/EZProxy_Configuration_for_use_with_Navigator

5a. Configuring EZproxy for Innovative Interfaces, Inc.

Note: This requires the III Patron API Module.

Mandatory.
In your EZproxy *user.txt* file you **must** set the following:

- Directive: **Set session:uid = login:user**
  Result: Sets userObject Unique ID to user ID/barcode

- Directive*: **Set session:location = auth:p53**
  Result: Sets userObject Home Library Location to user’s home library
  * when applicable, otherwise Recommended

- Directive: **Set session:groupNumber = NNNNN**
  Result: Sets userObject groupNumber to your consortium’s Group Number

- Directive: **Set session:instNumber = NNNNN**
  Result: Sets userObject institutionNumber to your library’s WorldCat Registry ID

Recommended.
In your EZproxy *user.txt* file you **should** set the following:

- Directive: **Set ParseName(auth:pn, “S,F,M,X”, “session”)**

S = surname
F = first name
M = middle name
X = prefix

Note: Name entry is based on local practice so SFMX should be arranged with commas to match your local convention.
Result: Allows EZproxy to derive userObject name values

- Directive: **`Set session:category = auth:p47`**
  Result: Sets userObject Patron Category to local patron type

- Directive: **`Set session:emailAddress = auth:pz`**
  Result: Sets userObject emailAddress to user's e-mail address

Optional.
In your EZproxy *user.txt* file you **may** set the following:

- Directive: **`Set session:dateFormat = "MM-DD-YY"`**
  Result: Sets userObject date format

- Directive: **`Set session:joinDate = auth:p83`**
  Result: Sets userObject Registration date to the user's registration date

- Directive: **`Set session:expirydate = auth:p43`**
  Result: Sets userObject Expiration date to your library's assigned expiration date (if any).
  Note: If a date is provided, requesting is blocked after this date.

Local blocking.
Your library may want to block based on local conditions derived from III authentication. Implementing this type of blocking requires two steps:

1. Block all circulation
2. Unblock circulation based on the selected condition(s)

Example:

1. Block circulation:

```
Set session:bannedInRemoteCirculation = "Y"
```

2. Unblock circulation only if there are no message blocks (p56):

```
If auth:p56 eq "-"
 {Set session:bannedInRemoteCirculation = "N"}
```

Or

Unblock if there are no message blocks (p56) and if the patron type is valid:

```
    If auth:p56 eq "-" && auth:p47 =~ "/^(2|3|4|5|6|15|16|…)$/"
     {Set session:bannedInRemoteCirculation = "N"}
```

5b. Configuring EZproxy for LDAP

Mandatory.
In your EZproxy *user.txt* file you **must** set the following:

- Directive: `Set session:uid = login:user`
  Result: Sets userObject Unique ID to user ID/barcode

- Directive: `Set session:groupNumber = NNNNN`
  Result: Sets userObject groupNumber to your consortium's Group Number

- Directive: `Set session:instNumber = NNNNN`
  Result: Sets userObject institutionNumber to your library's WorldCat Registry ID

Recommended.
In your EZproxy *user.txt* file you **should** set the following:

- Directive: `Set session:forename = auth:givenName`
  Result: Sets userObject forename to patron first/given name

- Directive: `Set session:surname = auth:sn`
  Result: Sets userObject surname to patron surname/last name

- Directive: `Set session:middleName = auth:initials`
  Result: Sets userObject middleName to patron middle initial(s)

- Directive: `Set session:emailAddress = auth:email`
  Result: Sets userObject emailAddress to user's e-mail address

Local blocking.
Your library may want to block based on local conditions derived from LDAP authentication. Implementing this type of blocking requires two steps:

1. Block all circulation
2. Unblock circulation based on the selected condition(s)

Example:

1. Block circulation:

```
     Set session:bannedInRemoteCirculation = "Y"
```

2. Unblock circulation if the user has at least one educational affiliation [Count] and that affiliation is not *alum*.

```
     If Count (auth:eduPersonAffiliation) >=1 &&
     ! All (auth:eduPersonAffiliation, "alum")
          {Set session:bannedInRemoteCirculation = "N"}
```

5c. Configuring EZproxy for Shibboleth

Mandatory.
In your EZproxy *shibuser.txt* file you **must** set the following:

- Directive: `Set session:uid = auth:urn:mace:dir:attribute-def:uid`
  Result: Sets userObject Unique ID to user ID/barcode

Recommended.
In your EZproxy *shibuser.txt* file you **should** set the following:

- Directive:
  `Set session:forename = auth:urn:mace:dir:attribute-def:givenName`
  Result: Sets userObject forename to patron first/given name

- Directive:
  `Set session:surname = auth:urn:mace:dir:attribute-def:sn`
  Result: Sets userObject surname to patron surname/last name

Local blocking.
Your library may want to block based on local conditions derived from Shibboleth authentication. Implementing this type of blocking requires two steps:

1. Block all circulation.
2. Unblock circulation based on the selected condition(s).

Example:

1. Block circulation:

```
     Set session:bannedInRemoteCirculation = "Y"
```

2. Unblock circulation if the user has at least one educational affiliation [Count] and that arffiliation is not *alum*.

```
If Count (auth:urn:mace:dir:attribute-def:eduPersonAffiliation) >=1 &&
! All (auth:urn:mace:dir:attribute-def:eduPersonAffiliation, "alum")
      {Set session:bannedInRemoteCirculation = "N"}
```

5d. Configuring EZproxy for Multiple Sources

It might be necessary to use more than one source to construct a viable userObject. You can configure the *user.txt* file to account for this scenario. It is possible to do field swapping as necessary in order to ensure that the userObject has session:uid set to how the user is known to both the local ILS and to Navigator. These values **must** match.

This combination mainly works with III, LDAP and SIP, as those are the most robust sources of data.

Example:
This example also requires creating a secondary file called *iii.txt* which will be called to perform specific Innovative Interfaces API information harvesting.

```
::LDAP
BindUser CN=ezproxy,CN=users,DC=yourlib,DC=org
BindPassword verysecret
URL ldap://ldapserv.yourlib.org/CN=users,DC=yourlib,DC=org?
    sAMWAccountName?sub?(objectClass=person)

IfUnauthenticated; Stop

If auth:barcode ne ""
  {
   Set saveuser = login:user          #Preserve provided login username
   Set login:user = auth:barcode      #Switch to barcode from LDAP
   If UserFile ("iii.txt")            #Call to external file iii.txt
    {
     #Logic to perform if III authentication successful
    }
   Set login:user = saveuser          #Switch back to provided username
  }

/LDAP
```

Create a file called iii.txt and enter this code:

```
::III
Password None
III iii.yourlib.org
IfUnauthenticated; Stop

Set session:uid = login:user
Set ParseName(auth:pn, "S,FM,X","session")
/III
```

6. Configuring an SSL certificate

Obtaining an SSL certificate is a three-step process:

1. Generate a Certificate Request in your library's EZproxy.
2. Submit the Certificate Request to the Certificate Authority of your choice.
3. Import the received SSL Certificate into your EZproxy.

Before you begin.

1. You must have obtained a valid EZproxy license key and successfully installed EZproxy on your server.

2. You must have the following information available to complete the *Create New SSL Certificate* form:

   a) Server name: ____

   b) Key size**:** ______________________ (select from drop-down)

   c) Country: ______________________ (two-letter country code)

   d) *****State or Province**:** _____________ (do not abbreviate; ;use *Ohio*, not *OH*)

   e) *****City or Locality: ____________________________________

   f) Organization: ____

   g) *****Organization Unit: ___________________________________

   h) Administrator email: __________________________________

   i) Expiration : __________________________ (self-signed only; select from drop-down)

   ***** = optional field

3) You must choose a Certificate Authority from which to purchase a certificate, and locate the appropriate area of the Authority's Web site. You must also have a payment method that the Authority will accept.

Procedure

For the procedure to configure an SSL certificate for EZproxy, see: http://www.oclc.org/support/documentation/exproxy/cfg/ssl/ .

7. Testing your EZproxy configuration

You can test your EZproxy by configuring your EZproxy server to return the results of an authentication attempt in a userObjectResponse.

Step	Action
1	Open the config.txt file with a text editor.
2	Add the following: `Option UserObjectTestMode`
3	Save and close the file.
4	Re-start EZproxy.
5	After re-start, send a URL in this form to your server: **`https://<yourFullyQualifiedDomainName>/userObject?service=getToken`**
6	Enter your User Name and Password. **Result:** A userObjectResponse similar to the one shown below is displayed, populated with your data.

Example: Fully populated userObjectResponse:

```
<userObjectResponse>
  <serviceStatus>OK</serviceStatus>
  <userDocument>
    <lastAuthenticated>2009-01-23T17:16:13Z</lastAuthenticated>
    <groupNumber>NNNNN</groupNumber>
    <instNumber>NNNNN</instNumber>
    <uid>999999</uid>
    <location>plxc</location>
    <category>11</category>
    <forename>jane</forename>
    <surname>smith</surname>
    <emailAddress>jane.smith@oclc.org</emailAddress>
    <dateformat>MM-DD-YY</dateFormat>
    <joinDate>01-21-09</joinDate>
    <expiryDate>03-03-09</expiryDate>
    <bannedInRemoteCirculation>N</bannedInRemoteCirculation>
  <userDocument>
</userObjectResponse>
```

Appendix A: Custom EZproxy `config.txt`

```
############################################
#################

# The DNS resolvable name of the local EZproxy server
Name ezproxy.hostname.edu

# Either the DNS resolvable name or an IP address of the local
EZproxy server
#    or the value "ANY" which will bind to all IP addresses of
the host server
Interface ezproxy.hostname.edu

# Initial login port to be able to access the /admin console
LoginPort 2048

# Force high encryption
Option DisableSSL40bit

# SSL Port which should be used in production
LoginPortSSL 443

# ForceHTTPSLogin to enable it once SSL certificates are in place
Option ForceHTTPSLogin

# start as root then drop privileges   uncomment for Unix
# systems
##RunAs nobody:nobody

# Required to allow the use of userObjects
Option UserObject

# Uncomment UserObjectTestMode to be able to view the
#     raw userObject during testing by sending this URL to the
#     EZproxy server
#     https://ezproxy.hostname.edu/userObject?service=getToken
#Option UserObjectTestMode

# Insert the pre-assigned WSKey below - must be 80 characters in
length
LocalWSKey MYWSKEY

# Allow the Master EZproxy server
Option RedirectSafe oclc.org

#############################################################
```

Appendix B: EZproxy userObject

The EZproxy userObject contains these 42 attributes:

session:groupNumber	session:note1
session:groupSymbol	session:note2
session:instNumber	session:note3
session:instSymbol	session:note4
session:uid	session:note5
session:location	session:note6
session:category	session:note7
session:title	session:note8
session:forename	session:note9
session:middleName	session:note10
session:surname	session:addressee
session:nameSuffix	session:bulding
session:emailAddress	session:street
session:dateFormat	session:district
session:joinDate	session:city
session:expirydate	session:region
session:userGroups	session:country
session:bannedInRemoteCirculation	session:poBox
session:canRequestIfBanned	session:postcode
session:clientPresignedCopyright	session:phoneNumber
session:attributes	session:faxNumber