Admin users (/admin)

Last updated: Fri, 25 Feb 2022 16:58:07 GMT

Administrative users can access the EZproxy Administration page. Learn how to create users and assign groups. The ability to access the /admin URL is limited to administrative users.

You can create an administrative user by editing user.txt and adding a line like:

```
rdoe:verysecret:admin
```

The :admin at the end of the line indicates that rdoe is an administrative user.

If your institution does not include a place to enter a password on your login form, then omit the password and use an unusual username, such as:

```
rdoeverysecret::admin
```

Once you have added the appropriate line to user.txt, you can go to the /admin URL of your server, log in, and you should see a page of administrative options.

**Special note for CAS, CGI and Shibboleth authentication**

If you are using an authentication method that redirects users to a different place for authentication, including CAS, CGI, and Shibboleth, logging in as an administrative user requires that you use a URL like this:

```
http://ezproxy.yourlib.org:2048/login?user=rdoe&pass=verysecret
```

where you specify your administrative username and password as part of the /login URL. If you have to log in in this manner, limit the characters in your username and password to letters, digits, hyphens (-), underscores (_), and periods (.)

Security Note: Use this method to log in to your admin account with caution as this entire URL, containing your username and password, will be stored in your EZproxy log file whenever you log in.

After you log in, you can then access:

```
http://ezproxy.yourlib.org:2048/admin
```

**Administrative user groups**

This feature is available in EZproxy 6.2.2 and later. Previously, the EZproxy Administration features were an (almost) all or nothing proposition in which users either had total administrative privilege or none. The only exception was the ability to give users access to the Token cross-reference feature.
The majority of options on the Administration page can now be granted to users individually by assigning them to special groups. When setting up this type of access, the historical Admin command is no longer used, but instead users are placed into special groups that correspond to the URL over the Admin feature. For example, the Audit page is available from /audit, so the group that grants access to this is Admin.Audit.

The groups available are:

- Admin.Audit
- Admin.DecryptVar
- Admin.Groups
- Admin.Intrusion
- Admin.LDAP
- Admin.Messages
- Admin.Restart
- Admin.Security
- Admin.Shibboleth
- Admin.SSLUpdate
- Admin.SSLView
- Admin.StatusUpdate
- Admin.StatusView
- Admin.Token
- Admin.Usage
- Admin.UsageLimits
- Admin.User
- Admin.Variables

The /admin page automatically adjusts based on group membership to display the options that correspond to these group memberships.

The SSL and Status pages have the ability to change key aspects of EZproxy’s behavior, so these features have been divided into Update and View groups. Users in the Update group have the full functionality available in previous versions, whereas users in the View group are only able to view information on these pages.

Users who are full administrators through the classic Admin command or who have the Admin.Groups privilege can see a list of all of these groups at the /groups URL.

Admin users are assigned to these groups via user.txt. They cannot be used within config.txt.

**Do not** assign individuals to groups as follows:

```
someuser:somepass:group=Admin.StatusView
```

The above entry is equivalent to:
::group=Admin.StatusView
someuser:somepass

which tells EZproxy that all users from that point forward should be assigned into the Admin.StatusView group.

Instead, add users to groups following this example:

::group=+Admin.StatusView
someuser:somepass
otheruser:otherpass
::group=-Admin.StatusView

This would assign both someuser and otheruser into the StatusView group in addition to any other groups already set up, while ensuring that users who follow will not be in this special group.

Within an authentication method such as LDAP, sample usage would be:

::LDAP BindUser CN=ezproxy,CN=users,DC=yourlib,DC=org
BindPassword verysecret
ldap://ldapserv.yourlib.org/CN=users,DC=yourlib,DC=org?
sAMAccountName?sub?(objectClass=person)
IfUnauthenticated; Stop
IfUser jdoe; Group +Admin.StatusView
/LDAP

in which specific users are identified and have the special group enabled.

When initially deploying groups, OCLC recommends using:

Audit Most Login.Success.Groups

This tells EZproxy’s Audit feature to include the groups to which a user is assigned in the Other column, making it easy to determine if users are being assigned to the expected groups.