Windows domain authentication

Overview

Institutions that are using Windows Active Directory should also review LDAP Authentication for information on how to authenticate using LDAP. LDAP support is available in all versions of EZproxy.

The Windows Domain authentication described here is only available in EZproxy for Windows. In addition, to authenticate against a given domain, the computer running EZproxy must either be a member of that domain or be a member of a domain that has a trust relationship with the given domain.

To enable domain authentication, the account used to run EZproxy must possess the "Act as part of the operating system" right. If you run EZproxy as a service under the "local system" account, it will automatically have this right. If you run EZproxy interactively for testing or as a service under a different account, you must grant this right to this account by following these steps.

1. Launch Start -> Programs -> Administrative Tools (Common) -> User Manager
2. From "Policies", select "User Rights..."
3. Click "Show Advanced User Rights"
4. Select "Act as part of the operating system" from the "Right" popup
5. Click "Add"
6. Click "Show Users"
7. Select the account to be used to run EZproxy from the list of "Names:" then click "Add"
8. Click "OK" to exit "Add Users and Groups"
9. Click "OK" to exit "User Rights Policy"
10. From "User", select "Exit"
11. If you are currently logged in to the account you have just updated, you must logout and log back in to make this change take effect.

Once this is in place, simply edit user.txt and add a line like this:

::domain= your-domain

replacing your-domain with the domain name for authentication.

Errors recorded to

When using Domain authentication, EZproxy records errors for any failed attempt. These error message looks like this:
LogonUser for rdoe returned 1326

The numbers that appear at the end of these lines are the Windows error. These are the most common error codes:

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1326</td>
<td>Invalid username or password</td>
</tr>
<tr>
<td>1330</td>
<td>Expired password</td>
</tr>
<tr>
<td>1793</td>
<td>Account is expired</td>
</tr>
<tr>
<td>1909</td>
<td>Password must be changed before first login</td>
</tr>
</tbody>
</table>

A complete list of all possible error codes is available at:


If you encounter an error code and are unclear what it means, please contact support@oclc.org for help.

**Expired passwords**

If you use password expiration within your domain, you can configure EZproxy to support password changing for expired password.

For versions of EZproxy dated prior to 2005-01-22, the following steps only work for people who are required to change their password at first login, but does not help for people whose passwords have expired. Versions of EZproxy dated 2005-01-22 and later handle both pre-expired accounts and ongoing password expirations.

To enable EZproxy to allow users to change their expired passwords, use these steps:

1. Open a "Command Prompt" window by going to Start | Run..., typing cmd in the Open: box, then click OK.
   
   c: md \ezproxy cd \ezproxy

2. Change your current directory to the directory where EZproxy is installed with command like:
   
   c:
   cd \ezproxy

3. Create the files for handling password expiration by typing the command:
   
   ezproxy -mw

These steps create the file wexpired.htm in the docs subdirectory. The presence of wexpired.htm tells EZproxy to handle expired passwords. You can edit this file to customize it to your needs, but care must be taken to leave the pieces that refer to ^0, ^1, ^2, and ^3 in the same form to insure EZproxy can insert information into this form when it is presented to users who have expired passwords.