Myths and facts about EZproxy, federated identity, and browser changes

Don Hamparian
Senior Product Manager, OCLC Platforms
Web browsers cannot block IP addresses

• Apple Private Relay available with Apple Safari on MacOS or IOS option to shield user IP addresses (like TOR) so servers can't see the browser user's IP address (since 2021 July)

• Setting in the OS settings for your account

• Some EZproxy remediation required (coming up)

https://support.apple.com/en-us/HT212614

Apple Private Relay

iCloud Private Relay keeps your internet activity private

Private Relay hides your IP address and browsing activity in Safari and protects your unencrypted internet traffic so that no one—including Apple—can see both who you are and what sites you're visiting.

Private Relay

Without access to your IP address, some websites may require extra steps to sign in or access content. Learn more...

IP Address Location Settings

Maintain general location

Use country and time zone

You can keep using your general IP address location so that websites can provide local content in Safari, or you can choose to use a broader IP address location in your country and time zone.
What is happening to web browsers?

- **Chrome & Firefox** introduced new Federated Credential Management API (FedCM) to provide privacy benefits during authentication.
- Currently “experimental code” in both browsers
- Google publicly announced they will move to FedCM in Chrome by November 2023
- Targeting consumer web experience, for example, login to Google accounts
- No EZproxy remediation required
What is FedCM?

- FedCM (Federated Credential Management) is a **new API** and a privacy-preserving approach where the user registers the identity service they trust for a particular site with the browser; the browser prevents exchange of information until the user consents.


FedCM Goals

FedCM is a multi-step journey to make identity on the web better, and in its first step we are focused on reducing the impact of third-party cookie phase-out on federated identity.

Third party cookies

- Third party cookies have a different domain than the URL in the browser bar
- Used sometimes for “tracking”
- Used when there are iframes that set cookies
- EZproxy will continue to work in this evolving environment

Concepts in development for more privacy preserving ways to allow cookies across domains:

OCLC is involved in this effort via InCommon and other identity federations

https://wiki.refeds.org/display/GROUPS/Browser+Changes+and+Federation
Impacts to EZproxy IP proxying

• No impact

• Browser obfuscation of an IP address is not an issue for EZproxy-to-publisher functionality

• Third-party publishers will see the EZproxy IP address, regardless of browser IP address
Why EZproxy IP proxying is not impacted
Libraries who decide against on-campus proxying may be impacted

- ‘ExcludeIP’ is a directive that can be configured into EZproxy at set-up

- Libraries use this directive to skip proxying on campus, and instead use its institution's campus IP range

- Because the user's IP is blocked by the browser, EZproxy is not able to apply the logic of the ‘ExcludeIP’ rule. Instead, users will be prompted by EZproxy to login before it will proxy the website
Other directives and a condition that may be impacted

<table>
<thead>
<tr>
<th>Audit</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoLoginIP</td>
<td>LogFormat %a</td>
</tr>
<tr>
<td>AutoLoginIPBanner</td>
<td>LogSPU %h</td>
</tr>
<tr>
<td>IfIP</td>
<td>Option ExcludeIPMenu</td>
</tr>
<tr>
<td>IntrusionAPI</td>
<td>Security Rules for 7.1 and higher</td>
</tr>
<tr>
<td></td>
<td>• EnforceOCLCIPLimit</td>
</tr>
<tr>
<td></td>
<td>• OCLCIPLimit10day</td>
</tr>
<tr>
<td></td>
<td>• OCLCIPLimit10</td>
</tr>
</tbody>
</table>
The future of EZproxy

- OCLC will support IP proxying via EZproxy for the foreseeable future
- EZproxy remains the leading access method to connect users to e-resources
- EZproxy keeps librarians in control of their data
- OCLC continues to explore modern integration with third-party publisher websites
Don't be like this guy...

OCLC is aware of future access methods that may need to be supported
In summary

**Myth:** EZproxy is broken because of these changes

**Fact!** EZproxy has little impact by these changes

**Myth:** EZproxy is the only solution impacted by these changes

**Fact!** When "log in" is changed by FedCM, every industry requiring a single sign-on will be impacted
Questions?
Because what is known must be shared.®

Thank you!

Don Hamparian
Senior Product Manager, OCLC Platforms
Hamparid@oclc.org