Contents

Operating System Requirements ........................................................................................................... 3
Recommended Actions ............................................................................................................................ 3
Release Notes ......................................................................................................................................... 4

Configuration Updates ............................................................................................................................ 4
  HTTPHeader Directive Enhanced ........................................................................................................... 4
  AnonymousURL Directive Enhanced ...................................................................................................... 4
  Support for Wildcards in the Subject Alternate Name of SSL Certificates ........................................ 4
  New Audit Event: Session.IPChange .................................................................................................... 5
  New Shibboleth Webpage for Customization ......................................................................................... 6
  EZproxy Administration Page – Server Status Updates ......................................................................... 6

Authentication Updates .......................................................................................................................... 6
  LDAP: Obscure Passwords Can Be Used on the Test LDAP Page ......................................................... 6
  Ticket: SHA256 and SHA512 Hashes Are Now Supported .................................................................... 7

Security Updates ..................................................................................................................................... 7
  EZproxy Now Uses OpenSSL 1.0.2.d .................................................................................................... 7
  New Directive: ConnectWindow ........................................................................................................... 7
  EZproxy Will No Longer Generate Private Certificates with 512 Bit Keys ....................................... 8

WSKey Updates ....................................................................................................................................... 8
  New Handling of WSKey Licenses with More Accurate Warnings ..................................................... 8

Bug Fixes ................................................................................................................................................. 9
  IPv4 addresses misidentified as private are now matched to their correct locations ............................ 9
  The ExcludeIP directive recognizes IPv6 addresses ........................................................................... 9
  Option LogSPUEdit correctly logs SPUEdit redirect URLs ................................................................... 9
  Requests with bodyless responses are logged .................................................................................... 9
  Directives controlling IP address access will only generate warnings when extra-large ranges are entered ........................................................................................................................................ 9

EZproxy Release Notes

Release Date: September 2015
Daylight Savings Time (DST) time zone offsets are correctly detected and recorded

SSLCipherSuite directive allows end-user modification of communication with the OCLC WSKey server

EZproxy Guardian will restart EZproxy upon recoverable failure

A MimeFilter directive with invalid arguments will not cause EZproxy to shut down

Known Issues

Important Links
Operating System Requirements

EZproxy is supported under three different operating systems:

- Linux
- Solaris (x86)
- Windows

The supported versions of these operating systems along with their minimum hardware requirements can be found at EZproxy: Hardware and Operating System Requirements.

Recommended Actions

For this release, we recommend that you review the following checklists and complete the relevant tasks. These checklists identify updates that we have determined as significant for most institutions. We encourage you to review all of the items in the release notes to determine whether there are other items that might require additional action or follow up by your institution.

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ If you are upgrading from an EZproxy version earlier than V6.0, you will need to request a WSKey. To request a WSKey, you will need to have a current, annual subscription. EZproxy moved to the annual subscription model in July 2013, so if you purchased your EZproxy subscription prior to that time, you will need to update. To purchase an annual subscription, you can request a quote, and you will be provided with a quote and information about how to subscribe. If you are uncertain if your subscription is current, please email <a href="mailto:orders@oclc.org">orders@oclc.org</a>. If you have already upgraded to V6.x, your existing WSKey will work with this upgrade.</td>
</tr>
<tr>
<td>❑ Review the EZproxy Security FAQ, especially if you are upgrading from a version older than V5.7.44. EZproxy V6.1 has many security updates that may make previous configurations in your config.txt file unnecessary, and you can remove certain directives after installing V6.1.</td>
</tr>
</tbody>
</table>
Release Notes

Configuration Updates

HTTPHeader Directive Enhanced

1. New syntax supported by the HTTPHeader directive allows arbitrary processing of both the headers sent from the user to the content provider and from the content provider back to the user. These directives only apply when proxying content and not when the user is interacting with internal EZproxy services such as the login page or administration pages.

2. In the HTTP request header, the Access-Control-Request-Header and Access-Control-Request-Method headers are now forwarded to the content provider and the Origin header’s value is rewritten from normal to rewritten form.

3. If the HTTP response headers include the Access-Control-Allow-Origin header, the value is unrewritten back to its normal form.

For more information, see HTTPHeader.

AnonymousURL Directive Enhanced

This directive now has a corresponding OPTIONS qualifier to indicate that the rest of the directive should match OPTIONS method requests from the browser but not others such as GET and POST. This allows an AnonymousURL directive to be more focused on just OPTIONS requests, which are required to enable some Cross-Origin Resource Sharing (CORS) requests but which are placed by browsers without including EZproxy’s cookie, thus preventing normal user authentication.

For more information, see AnonymousURL.

Support for Wildcards in the Subject Alternate Name of SSL Certificates

EZproxy can now detect wildcards in both the Common Name and Subject Alternate Name (SAN) fields of an SSL certificate. This change allows EZproxy administrators to have EZproxy generate a SAN that matches the server’s name exactly, contains the wildcard in front of the server’s name, or contains both when Creating a New SSL Certificate from the EZproxy administration page.

<table>
<thead>
<tr>
<th>Certificate name:</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>exproxy.yourlib.org (browser warnings proxying https web sites; less expensive)</td>
<td></td>
</tr>
<tr>
<td>*exproxy.yourlib.org (fewest to no browser warnings proxying https web sites; more expensive)</td>
<td></td>
</tr>
<tr>
<td>Subject Alternate Name:</td>
<td></td>
</tr>
<tr>
<td>exproxy.yourlib.org</td>
<td></td>
</tr>
<tr>
<td>*exproxy.yourlib.org</td>
<td></td>
</tr>
<tr>
<td>Expiration (for self-signed only)</td>
<td>1 year</td>
</tr>
<tr>
<td>Create:</td>
<td>Self-Signed Certificate or Certificate Signing Request</td>
</tr>
</tbody>
</table>
If server names are selected for entry in the SAN field, these will be displayed on the /admin Manage SSL Certificate page for that certificate or certificate signing request (CSR).

For more detail, see SSL Configuration.

New Directive: Option ForceWildcardCertificate

The new Option ForceWildcardCertificate directive is a rarely used directive that can be added to the config.txt file if you have a wildcard SSL certificate installed, but you experience either of the following:

- browser warnings when accessing secure (https) EZproxy administration pages
- secure URLs are not being rewritten with hyphens when you access them

For more information, see Option ForceWildcardCertificate.

New Audit Event: Session.IPChange

EZproxy administrators can now customize their audit logs to record any changes to a user’s IP address after an EZproxy session has been established. This new event must be manually added with the Audit directive for inclusion in the audit logs.

NOTE: Depending on your users’ network configuration, EZproxy may record many of these events in the audit logs because some institutions and network configurations will routinely change IP addresses in a session.

For more information, see Audit.
New Shibboleth Webpage for Customization

When a Shibboleth service provider sends a SAML Response document that EZproxy cannot interpret properly, it displays a warning to the end user:

Inter-institutional access failure. Please contact your system administrator for assistance.

This default warning can now be overridden by creating a new file with the name:

shibfailure.htm

and saving it to the docs directory. This file can contain a customized messaging with more detail for the end user.

Note: This file is not created by ezproxy –m. You will need to create and save your own new file.

For more details about this file, see Default Web Pages.

EZproxy Administration Page – Server Status Updates

On the EZproxy Server Status administration page (/status), if Include extended info is selected, EZproxy will display all of the HTTPHeader and MimeFilter directives to simplify remote debugging of proxying behavior. In addition, the numeric database index links from the Hosts table to the corresponding Databases table have been revised to work correctly in more browsers.

Authentication Updates

LDAP: Obscure Passwords Can Be Used on the Test LDAP Page

The Test LDAP admin page (/ldap) will now accept an obscure password in the Bind Password field. This allows EZproxy administrators to copy and paste an obscured password from the user.txt file into the Test LDAP screen when troubleshooting LDAP authentication issues and creating authorization rules based on LDAP attributes.

For more detail about how to use the Test LDAP (/ldap) page, see LDAP Authentication with Active Directory.
Ticket: SHA256 and SHA512 Hashes Are Now Supported

Ticket authentication uses cryptographic hashes for signatures. Originally, only MD5 and SHA1 were supported and implemented with the MD5 and SHA1 directives. Now users can add the directives SHA256 and SHA512 to a ticket authentication block to have EZproxy generate tickets with stronger hashes.

Example:
::Ticket
SHA256 sesame-sha256
/Ticket

::Ticket
SHA512 sesame-sha512
/Ticket

For more information, see Ticket Authentication.

Security Updates

EZproxy Now Uses OpenSSL 1.0.2.d

1. EZproxy 6.1 was built with OpenSSL 1.0.2d, so it now supports TLS 1.0, 1.1, and 1.2.
2. To address the Logjam Attack, the minimum Diffie-Hellman group used is now 2048 bits.
3. EZproxy also supports the following advanced SSL options:
   • SSLHonorCipherOrder directive supported. This directive can be assigned the values On or Off. The default for this directive is on, which indicates EZproxy should choose the cipher to use when accepting incoming secure connections. If this directive is set to Off, the client will choose the cipher to use.
   • Diffie-Hellman parameters can now be included within a key file in the SSL subdirectory. Such values can be generated with OpenSSL using the openssl dhparam command. For more information see dhparam in the OpenSSL documentation.
   • Elliptical Curve Parameters can now be included within a key file in the SSL subdirectory. Such values can be generated with the openssl ecparam command. For more information, see ecparam in the OpenSSL documentation.
   • EZproxy supports a new SSLOpenSSLConfCmd directive that allows OpenSSL-specific commands to be used to control advanced settings of OpenSSL. See Supported Configuration File Commands in the OpenSSL documentation for a list of supported commands.

For more information see EZproxy & OpenSSL.

New Directive: ConnectWindow

The amount of time in which the /connect endpoint can be used to initiate access to an existing EZproxy session has been reduced. By default, this endpoint will only remain open for 60 seconds after a user has logged in to EZproxy.
The new directive ConnectWindow can be used to customize the number of seconds this window is open. For example, if you would like the window to be open only 5 seconds to further minimize the chance of illicit access, the following could be entered in config.txt:

```
ConnectWindow 5
```

In addition, the new audit event Session.ReconnectBlocked can be used to record any attempts made to use /connect outside the connect window. This event is included in Audit Most, and Session.ReconnectBlocked will be recorded in the Other column on the Audit Events /admin screen along with the number of seconds that have elapsed between the original, valid use of /connect and the recording of the invalid attempt.

For more information see ConnectWindow and Audit.

**EZproxy Will No Longer Generate Private Certificates with 512 Bit Keys**

512 bit private keys are regarded as insecure and are now rejected by IE 10. EZproxy no longer offers the option to generate private 512 bit keys.

**WSKey Updates**

**New Handling of WSKey Licenses with More Accurate Warnings**

Beginning with EZproxy 6.0 and the introduction of WSKeys, licenses were validated for 90 days after the WSKey was first installed, leading to misleading expiration messages. EZproxy license handling has been revised to handle license revalidation with the EZproxy WSKey and display expiration warnings differently. As long as your WSKey license can be validated by the WSKey server, the startup message should read:

```
EZproxy license key is valid
```

If EZproxy is not able to validate your license with the WSKey server, additional warning messages regarding the WSKey’s expiration will be recorded at startup and hourly in the messages.txt log.

**Other resolved issues:**

1. When EZproxy starts up, if the license has expired or is highly incorrect due to clock issues, EZproxy will automatically try to revalidate the license with the OCLC WSKey server. If revalidation succeeds, EZproxy starts up immediately. If revalidation fails, EZproxy records the error to messages.txt and shuts down.
2. If an EZproxy license is successfully applied using the command line –k option while EZproxy is running, the running copy is notified to start using the license instead of requiring EZproxy to be stopped and restarted to pick up the license.
3. The /about EZproxy admin page can be used to view the date by which the current license must be revalidated with OCLC before expiring. This is NOT the WSKey expiration date, just the date by which your key must be revalidated with the OCLC WSKey server.

For more details about how EZproxy validates WSKey licenses, see WSKey Validation and Messages.
Bug Fixes

IPv4 addresses misidentified as private are now matched to their correct locations

After IPv6 updates, IPv4 addresses ending in *.*.*.10, *.*.*.172, and *.*.*.192 were wrongly labeled private addresses and assigned a Location 98 in audit logs that contained a location field. This problem was corrected in EZproxy V6.1, and now only IP addresses beginning with 10.*.*.* and the ranges 172.16.0.0-172.31.255.255 and 192.168.0.0-192.168.255.255 are identified as private, while the others are assigned their correct location.

The ExcludeIP directive recognizes IPv6 addresses

The ExcludeIP directive was not properly detecting IPv6 addresses to exclude. EZproxy V6.1 recognizes IPv6 addresses labeled for exclusion with the ExcludeIP directive.

Option LogSPUEdit correctly logs SPUEdit redirect URLs

When Option LogSPUEdit is active and a SPUEdit directive causes a redirect, EZProxy now correctly logs the target of the SPUEdit directive.

For more information, see SPUEdit and Option LogSPUEdit.

Requests with bodyless responses are logged

Previously, EZproxy would not create an entry in ezproxy.log if it accessed the proxied version of a page that contained no body in its response. This has been corrected. Entries for URLs that end in:

```
302 0
```

record requests with bodyless responses.

Directives controlling IP address access will only generate warnings when extra-large ranges are entered

EZproxy V6.0 caused warnings to be logged at startup when users included any of the following directives in config.txt:

```
AutoLoginIP
ExcludeIP
IncludeIP
RejectIP
```

The previous behavior was to only record warnings in messages.txt when these directives referred to more than 65,536 hosts or public IP addresses. This behavior has been reinstated in EZproxy V6.1, so
warnings will only be recorded in messages.txt when all IP addresses are included after one of these directives or the range exceeds 65,536.

For more detail about these warnings and the conditions that will trigger them, see EZproxy Alerts.

Daylight Savings Time (DST) time zone offsets are correctly detected and recorded

The tracking of the beginning and end of DST is controlled by the operating system. The Windows version of the C runtime library (MSVCRT) does not properly handle the generation of the time zone offset to include in ezproxy.log entries when adjusting for Daylight Savings Time. EZproxy V6.1 has been updated to detect and record the correct value when the operating system moves from standard time to DST. For example:

Noon in EST should be reported at “12:00:00 -0500” whereas EDT should be reported as “12:00:00 -0400.”

SSLCipherSuite directive allows end-user modification of communication with the OCLC WSKey server

EZproxy V6.1 allows EZproxy administrators to modify SSL connections to the OCLC WSKey server using the SSLCipherSuite directive. Previously these modifications could block communication with the OCLC WSKey server.

EZproxy Guardian will restart EZproxy upon recoverable failure

Previously, EZproxy would shut down if the Guardian start up process detected a failure in the Charge process. With EZproxy V6.1, if Guardian detects a failure in Charge, Guardian will stop the failing Charge process and start a new one.

A MimeFilter directive with invalid arguments will not cause EZproxy to shut down

Previously, EZproxy would shut down if the MimeFilter directive contained improperly constructed arguments. For example any of the following constructions:

MimeFilter
MimeFilter application/json * javascript
MimeFilter application/json .* invalidscript
MimeFilter application/json .* javascript

would cause EZproxy to shut down. With V6.1, after EZproxy encounters a MimeFilter directive with invalid arguments, it will continue to parse config.txt and run as best it can.
Note: EZproxy V6.0.8 introduced default rewriting of Mimetype “json”, making inclusion of the MimeFilter directive redundant and unnecessary. A properly constructed MimeFilter will not impact proxying, and with this update neither should an improperly constructed MimeFilter.

Known Issues

A list of known issues can be found at: https://www.oclc.org/support/services/ezproxy/known-issues.en.html

Important Links

Product web site
More product information can be found at: https://www.oclc.org/ezproxy.en.html

Support web sites
Support information for this product and related products can be found at:

- Documentation: http://www.oclc.org/support/services/ezproxy.en.html

© 2015 OCLC, Inc. All rights reserved. The following OCLC product, service and business names are trademarks or service marks of OCLC, Inc.: OCLC, WorldCat, WorldShare and “Because what is known must be shared.” In addition, the WorldCat and WorldShare symbols are service marks of OCLC. Third-party product service names are trademarks or service marks of their respective owners. OCLC grants permission to photocopy this publication as needed.