Introduction

EZproxy version 7.2 expands the previously released security features capabilities to allow real-time notifications for alert events. This release includes the following features:

- Robust security rules events can now be configured to send real-time emails when alert events are triggered
- Two new security rules
- New interface for managing user sessions more easily
- Updated pseudonymous user identifier support for Optical Society’s new domain
- Optional pseudonymous user identifier now works with Taylor and Francis

Supporting materials

- Software download
- Upgrade guide
- Security rules documentation
- Pseudonymous identifier documentation
- Admin UI documentation: security rules, pseudonymous identifier

New features and enhancements

Robust security rules engine now provides real-time email alerts

EZproxy released new security rules in v7.1. This allowed many new capabilities to automate the security of the EZproxy server and created new events to monitor. With EZproxy v7.2, we are introducing real-time email alerts for the security rules events. This new capability allows EZproxy administrators to stay informed on security events without logging in to the EZproxy administration interface. The new email feature will:

- Generate and send an email notification when a rule trips, to the user(s) listed in the admin screen.
- If email server errors occur (email does not get sent or received), we will attempt to re-send the email once an hour for a 24-hour period.
• Successful attempts or errors sending emails will be logged in the messages.txt file.
  ◦ Errors will appear as "we attempted to send the following email to [email address] on date/time."
• An optional daily digest email will include the total collection of all emails generated for a user during a 24-hour period, summarizing all tripped rules.
  Note: If this option is selected individual emails will not be sent separately.

EZproxy’s security rules provide a robust tool for mitigating compromised credentials. The new real-time email feature makes it easier to monitor security rule alert events, further allowing organizations to proactively mitigate potential issues.

New security rules

Additional security rules have been introduced in v7.2 to allow better management of user sessions and user logins.

• OCLCLoginSuccessLimit examines the concurrent number of login_success events over a period and can log or block based on the configured thresholds.
  Example: OCLCLoginSuccessLimit if login_success over 4 per 1000 then log
• OCLCReLoginLimit examines the number of login_relogin events over a period and can log or block based on the configured thresholds.
  Example: OCLCReLoginLimit if login_relogin over 4 per 1000 then log

To add these new rules, edit or create a file called 000-default.txt in the security folder.

Manage user sessions

The status screen has been updated. The new interface provides a view that will allow you to end all sessions for a user in one location.

Users can log in multiple times which creates multiple sessions for the same user. Previously, to terminate all sessions for a single user, each session would have to be selected from the table and manually terminated one at a time. This process often requires scanning a large table for the repeated username.

Pseudonymous identifier

The pseudonymous identifier has been enhanced with the following changes:

• The pseudonymous identifier functionality was updated to allow support for the new Optical Society domain.
• The pseudonymous identifier now works with Taylor and Francis.

OpenSSL

OpenSSL v1.1.1o is included in the latest version of EZproxy. This latest version of OpenSSL provides various security improvements and bug fixes. For more details, please visit OpenSSL 1.1.1 Series Release Notes.
Accessibility improvements

Accessibility improvements to EZproxy’s administration pages include:

- Tables now utilize “th” for table headers to provide better compatibility with screen readers.
- User interface elements that can receive keyboard focus are now highlighted when focused on.
- The “lang” attribute has been added to EZproxy HTML documents. This will indicate the natural language of the pages EZproxy serves directly to screen readers.
- Labels have been added to inputs on html pages to allow better compliance with screen readers.
- Presentational elements like 'border', 'align', or 'bgcolor' are now included in CSS to allow a more accurate screen reader presentation.
- `<Bold>` tag has been replaced with `<strong>` to comply with current accessibility standards.

Log improvements

- SPU logs for redirectsafe will now include dbvar values.
- When audit.most is enabled in the config.txt exemptions for security rules will be displayed in the audit logs.
- The IntrusionAPI previously only logged HTTP status code events of 200 or 204 even when other status codes were presented. EZproxy now records all status events.

Bug fixes

SAML

EZproxy has been updated to adhere to the SAML specification more closely. Two changes have been made:

- EZproxy v7.2 now allows gzip compression on the SingleLogout request.
  - Previously SingleLogout would fail if the IDP enabled gzip compression. Logout would then fail until gzip compression was disabled by the IDP.
- Resolved an issue when EZproxy was configured for SAML authentication with Signed Requests enabled. Previously EZproxy was not creating the signature correctly. This update will resolve issues with SAML Login and Logout.

HTTPHeader (-server)

In v6.2, the HTTPheader directives functionality was extended with the addition of the server flag. The intent was to allow EZproxy to pass a header for pages that EZproxy serves (i.e., login.htm, loginbu.htm, menu.htm etc).

The implementation in V6.6.2 through V7.1 erroneously passed the header along with content EZproxy proxied as well. This has been corrected in this version. More detail can be found here.
ExcludedIP

ExcludedIP will now use a 302 redirect instead of a 301 redirect.

WhitelistIP is now AllowIP

The latest version of EZproxy now uses AllowIP instead of WhitelistIP. WhitelistIP will continue to work for compatibility. View the updated AllowIP documentation for more information.

Known issues

Potential for rules to trip if site uses Shibboleth authentication and usernames are not set in shibuser.txt

If the EZproxy session variables login:loguser and login:user are not set in shibuser.txt, then the default username for all users using SAML authentication becomes “shibboleth.” Because rules are tripped at the username level, false trips of rules may occur.

Rules with longer watch periods will consume more disk space

Watch periods of 60 minutes or longer will consume more disk space in the /security directory to store the required evidence in the security database. Please monitor the disk usage in the /security database.

Some of the default rules in EZproxy 7.1 contain monitoring periods longer than 60 minutes. If you have disk space constraints, consider commenting out those rules.

Important links

Support website(s)

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

- EZproxy
- Contact OCLC Support
- OCLC Community Center
- Browser compatibility chart