EZproxy v7.1 release notes

Last updated: Thu, 21 Jan 2021 15:26:15 GMT

Release Date: January 2021

Overview

This release is one of the biggest releases of EZproxy to date. It introduces powerful new features that improve your library’s security posture, offer significant time savings, and provide more continuous access to your e-resource subscriptions.

Supporting materials

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

New features and enhancements

This release includes the following features:

- Robust security rules engine that significantly improves your library’s security posture and automates staff workflows
- Ability to view and manage security rule information in the EZproxy Administration site
- Optional pseudonymous user identifier that saves you time and streamlines e-resource access
- Ability to use the pseudonymous user identifier to quickly find compromised single sign-on credentials in the EZproxy Administration site

See more details about these features below.

Robust security rules engine augments existing detection triggers, improving security posture and automating workflows

EZproxy now uses sophisticated security rules engine to automatically detect and disable compromised single sign-on
credentials in real-time. It uses a consistent syntax and is designed to:

• Automate some administrative workflows for your staff
• Provide more continuous access to your e-resource subscriptions
• Avert data breaches that put systems and patrons at risk
• Transform network and account security at your library

Previously, you may have been notified of compromised single sign-on credentials after the fact by IT or a content provider, potentially interrupting access. To find them, you had to manually search log files. This manual work is no longer necessary, and you can partner better with IT to proactively mitigate data breaches that interrupt access and compromise patron privacy.

New detection triggers provide a more secure operating environment

While some detection triggers already exist in EZproxy, the following new detection triggers will be added by this feature:

• Multiple IP Addresses
• Multiple Geographies
• PDFs Downloaded
• PDF Byte Limit
• Bytes Transferred
• Login Failures per User

Read more information for the new detection triggers here.

Enforce rules to either log or block end user accounts when triggered

The new security rules engine has two enforcement modes:

• “Logged” enforcement mode only logs an end user account when a rule is triggered; blocking the account needs to be done manually in this mode.
• “Blocked” enforcement mode blocks an end user account when a rule is triggered; this mode is a more proactive approach because it blocks potential compromised accounts in real-time.

End user accounts that have been blocked can be unblocked at any time or exempted from rules if needed.

The security rules engine will be sent out with a combination of both “logged” and “blocked” enforcement modes. Read more information for the default enforcement modes here.

Augment rules to support your library’s unique security needs and goals

Security rules can be tuned to meet your library’s workflows. Read more information on tuning your rules here.

Security rule information can be viewed and managed in the EZproxy Administration site

We have added new pages and capabilities to the EZproxy Administration site so your library can take full advantage of
the new security rules engine. You can now access a “View security rules” page and corresponding subpages in the “Current Activity” section to:

- Easily view information about your security rules
- Add, delete, and update security rule exemptions
- Better understand how and why rules are tripped

These updates to the EZproxy Administration site help you effectively manage the new security rules engine to enhance network security, partner better with IT, and provide a more seamless end user experience.

**View a summary of rules and tripped events on the “Security Rules” page**

The new “Security Rules” page provides a summary of your library’s security rules. You also have the ability to view more detailed information about tripped events for each rule in the “Tripped” column.

Note: You can only change security rules in the Config file. See the documentation for more information.

**View and manage rule exemptions on the “Security Exemptions” page**

The new Security Exemptions page provides a summary of your library’s security rule exemptions. You can update or delete an existing exemption by clicking on the user ID in the User column and add a new exemption by clicking Add Exemption.

User ID and expiration date are required fields to add a new exemption, and you can optionally add a comment to record the exemption reason.

**Better understand tripped rule events on the “Tripped Security Rules” page**

The new Tripped Security Rules page provides a comprehensive view of tripped security rule events. Here, you can see information like who tripped a rule, when, and how many times. Click an event number in the Observed column to see more detailed security evidence.

You can also filter tripped events by rule enforcement mode and other categories. Read more information about the security rules administrative pages here.

**Optional pseudonymous user identifier improves feedback loops with content providers, saving time and streamlining access**

You can now enable a pseudonymous user identifier feature in EZproxy to resolve security issues faster and streamline access. If enabled, a pseudonymous user identifier is sent with every EZproxy request via an HTTP header to content providers that have signed a data protection agreement with OCLC. It has been developed to preserve patron privacy.

Read more here.

This optional feature saves you time and streamlines access by:

- Enabling content providers to better determine the unauthorized user in the event of a data breach and avoid turning off licensed database access for all library users.
- Providing you and content providers with a unique piece of privacy-preserving information that can be exchanged to
find compromised single sign-on credentials faster.

Previously, content providers may have turned off database access to protect licensed e-content when they suspected a data breach, interrupting access for all library users. Then, you had to manually search log files to find the compromised credentials. If this feature is enabled, content providers can better determine an unauthorized user, avoid turning off database access for all library users, and share a unique identifier to help you find the compromised credentials faster.

The pseudonymous user identifier feature requires configuration to enable

To enable this feature you will need to set the Identifier Secret.

For hosted sites, your library will first have to agree to new OCLC Terms and Conditions prior to OCLC setting the Identifier Secret. OCLC will contact hosted sites for details on the process.

For self-hosted sites, your library will have to agree to new OCLC Terms and Conditions presented on the OCLC web site as you download EZproxy V7.1 prior to you setting the Identifier Secret.

Pseudonymous user identifier can be used to find compromised single sign-on credentials faster in the EZproxy Administration site

We have added new pages and capabilities to the EZproxy Administration site so your library can take full advantage of the pseudonymous user identifier feature. You can now access a “View identifiers” page to enter an identifier in the search box and find compromised single sign-on credentials.

If you have the pseudonymous user identifier feature enabled, this update helps you more quickly find compromised credentials and contact library users so they can reset their passwords or follow other security protocols.

Other Enhancements

1. Reject.htm now supports special variables
2. OpenSSL has release 1.1.1i with security updates rated high

Bug fixes

1. V7.0 memory leak issue resolved on Windows
2. When the Option ForceHttpsAdmin is specified, redirect to ssl/https when /admin is accessed

Known Issues

1. Potential rules 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.” In this case, since groups are tripped at the username level, false trips of rules may occur.
2. Rules with longer watch periods will consume more disk space to store evidence.

Increasing the watch period from 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 shipped in EZproxy 7.1 contain monitoring periods longer than 60 minutes. If you find you are having disk space constraints, consider commenting out those rules.