Audit

Last updated: Mon, 13 Jan 2025 15:19:32 GMT

Learn how to use Audit logs view information about user and security related issues in EZproxy.

Why is Audit important?

Audit logs allow EZproxy administrators to gain insight into a range of user and security related issues. The data collected in these logs is highly customizable and, when used with other security directives in your config.txt, can provide you with a picture of what limits should be set to strike a balance between security and providing your users with the access to the resources they need.

This information can be used to determine if users are regularly having difficulty accessing your EZproxy resources. If your audit logs reflect numerous failed attempts and denied access to EZproxy, consider providing more specific instructions via documentation or tutorials to teach your users how to access resources remotely.

Description

Audit is a position-independent config.txt directive that commands EZproxy to record the occurrence of specified auditing events. The logs created by this directive are placed in a directory named 'audit' within the EZproxy installation directory. Individual files are created daily and named by year, month, and day (e.g. 20250113). Audit events can be viewed from the **/audit** EZproxy administration page.

Some libraries prefer to limit the timeframe over which such information is retained. Adding the AuditPurge directive allows you to specify the number of audit files that should be retained, allowing the automatic deletion of older audit files.

Fields to customize events to be audited

Audit should be followed by one or more of the events to be audited. Multiple events can be entered, but should be separated by spaces. The description tells what action caused this event to be logged in the audit file.

EVENT	DESCRIPTION
BlockCountryChange	A user's access was blocked because the country of the IP address from which the session began changed after access to EZproxy was established. This event only occurs if Option BlockCountryChange and Location directives appear in config.txt.
Info.usr*	Audit event defined by the EZproxy administrator. Info.usr will appear in the Event column, and the user defined text will appear in the Other column when the

EVENT	DESCRIPTION
	defined event occurs.
IntrusionAPI.BadIP*	Intrusion API indicates the address is associated with a known pirate/hacker
IntrusionAPI.Error*	An error occurred consulting the intrusion API (more information recorded in Other field); includes scenario in which SSL connection fails validation
IntrusionAPI.None	Intrusion API responded that address is not in database (this event is not enabled by AuditMost and must be added explicitly such as Audit Most IntrusionAPI.None)
IntrusionAPI.AllowIP*	Intrusion API responded that the address is allowed in their system (this event is not recorded if the address falls within a AllowIP range)
Login.Denied*	User denied access based on a Deny directive in user.txt. This event may be suppressed from the audit logs by using `Deny -NoAudit filename.`
Login.Success*	Successful attempt to log in to EZproxy.
Login.Success.Groups	Groups to which the user is assigned are logged as part of the Login.Success event.
Login.Failure*	Failed attempt to log in to EZproxy.
Login.Intruder.IP*	Intrusion attempts based on the IntruderIPAttempts directive.
Login.Intruder.User*	Intrusion attempts based on the IntruderUserAttempts directive.
Security.Exempt*	When enabled exemptions for triggered security events will be logged to audit logs.
Most	Most is a special value that indicates that all of the events in this table marked with an asterisk (*) should be audited.
Session.IPChange	A user established an EZproxy session from one IP address, and during that session the IP address changed. Depending on your users' network configuration, many of these messages could be

EVENT	DESCRIPTION
	recorded messages in messages.txt. Some institutions and network configurations will routinely change IP addresses in your session.
Session.ReconnectBlocked*	An unauthenticated user attempted to connect to an existing session using the /connect request after the connect window had closed. See ConnectWindow for additional information.
System*	General system activities that do not fall under other audit event categories (e.g. system startup).
Unauthorized*	Unauthorized attempts to access administrative features of EZproxy (e.g. /admin).
UsageLimit*	Events resulting from the UsageLimit directive.

* Most commonly audited events.

Syntax

The most common format for the Audit directive is:

```
Audit Most
```

This directive statement will provide you with a record of the most commonly audited events, marked with an asterisk in the table Fields to customize events to be audited.

If you would like to record the events included with the Most field as well as other audit events, such as the BlockCountryChange event, you would enter the following:

```
Audit Most BlockCountryChange
```

Examples

The following table presents scenarios where information recorded in the audit log can be useful, the config.txt directive statement that would record that information, and a discussion of why this statement would provide you with that information.

WHAT YOU WANT TO KNOW	CONFIG.TXT DIRECTIVE	WHY THIS WORKS

Login Data
 	
You want to know if your users have difficulty logging in to EZproxy to determine if you need to provide better information about how to access your resources remotely. You are confident that your EZproxy is secure, and you only need data about user logins.
	`Audit Login.Denied`
	`Login.Success`
	`Login.Success.Groups`
	`Login.Failure`
		Adding this directive statement containing only information about login events and related user groups allows you to create a focused dataset of information about only your users' login attempts. You can parse the data to identify how many logins were successful, how many failed, and how many were denied. Including the Login.Success.Groups event will provide details about whether individuals from certain groups were able to login successfully more often than users from other groups, and allow you to target training about how to log in to those user groups who have the most difficulty with remote access.

UsageLimit Data
 	
A resource provider recently requested that you add a usage limit to their databases beginning after your renewal in 2 months. If you would like your users to have a higher limit, you will have to pay more for that resource. You wonder if this limit will impact your users' ability to get the information they need, and have the funds to pay more if necessary, but you do not want to spend the extra money if users do not regularly exceed this limit.
	`Audit UsageLimit`
	`UsageLimit -MB=100`
	`Selective`
	`Title Some Database`
	`URL`
	`http://www.somedb.com/`
	`Domain somedb.com`
	`UsageLimit -end Selective`
		Adding this directive along with the UsageLimit on the specific resource in question will cause any events related to this UsageLimit to be recorded in the audit logs. Because this usage limit is not enforced, your users will be able to download as much data from these databases as they wish; however, any time they exceed the 100MB limit in a 24 hour period, a message with the overage will be recorded in the audit log. You can review these logs, determine how often the limit is exceeded, and decide if it is worth paying the extra money to allow your users to download additional data.

Security Data
 	
You have recently added some new security and limit directives (IntruderIPAttempts, IntruderUserAttempts, and UsageLimit) to your config.txt, and
	`Audit Most`
	`AuditPurge 180`
	`IntruderIPAttempts -interval=5 -expires=15 20`
	`IntruderUserAttempts -interval=5 -expires=15 10`
		Adding the Audit Most directive statement along with this baseline security and limit configuration will provide you with audit log data for the most common audit events as denoted by the asterisks in the table under the Overview tab. This

WHAT YOU WANT TO KNOW	CONFIG.TXT DIRECTIVE	WHY THIS WORKS
you are wondering if the starting values are appropriate for your server and your users or if you need to make adjustments to allow for larger amounts of data to be downloaded, lengthen the amount of time a user has to wait before a suspension ends, or lengthen the amount of time over which to consider transfer limits. Note: For more detailed information about how to combine the different security features of EZproxy in your config.txt and the configuration given in the example, see Securing Your EZproxy Server.	`UsageLimit -enforce -interval=15 -expires=120 -MB=100 Global`	combination of security and limit directives and audit statement will record the following details in your audit log: • any instance in excess of 20 in which an individual attempts to log in from the same IP address with invalid credentials during a 5 minute interval • any instance in excess of 10 in which an individual attempts to log in with a valid username and wrong password during a 5 minute interval • any time a single user attempts to download more than 100MB of data within 15 minutes If the audit log shows that any of these events is logged numerous times and all the users, IP addresses, and downloads are legitimate, it could show that your users need higher limits set due to their resource needs. However, it would also be worth investigating whether these limits were reached and exceeded due to a security breach.

Related directives

The following directives interact with or control functions related to this directive:

AuditPurge, IntruderIPAttempts, IntruderUserAttempts, IntrusionAPI, Location, UsageLimit