OX Abuse Shield

Release Notes for Release 2.8.0

2022-12-19

Copyright notice

©2022 by OX Software GmbH. All rights reserved. Open-Xchange and the Open-Xchange logo are trademarks or registered trademarks of OX Software GmbH. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

1 General Information

Open-Xchange is pleased to announce the release of OX Abuse Shield v2.8.0.

OX Abuse Shield provides abuse-prevention for Web Applications (including Webmail), POP, and IMAP. It is integrated with both OX App Suite and OX Dovecot Pro to prevent login and authentica-tionabuse as well as protecting against brute-force attacks.

The goal of OX Abuse Shield is to detect brute forcing of passwords across many servers, services and instances, as well as enforce policy for authentication and authorization. In order to support the real world, brute force detection policy can be tailored to deal with " bulk, but legitimate" users of your service, as well as botnet-wide slow-scans of passwords.

The new OX Abuse Shield v2.8.0 provides the following main improvements and new features:

- Support ELK 7.x Stack
- Support Date Expansion in WebHook URLs
- Enable IP and Login substitution in blocklist return messages
- Add config option to disable password for /metrics endpoint
- Support redis usernames and passwords for redis authentication
- Support hostnames for redis configuration in addition to IP addresses

The new OX Abuse Shield v2.8.0 provides the following fixes:

- Fix an issue where IPv6 ComboAddress returned zero port number (which caused v6 HTTP listen addresses to not work)
- Return the IP address of the client in JSON of ACL denied response

The new wforce-policy v2.8.0 provides the following main improvements and new features:

- Add redis authentication support to wforce policy
- Docker image for wforce policy, based on wforce docker image

Download and Installation

For further details about OX Abuse Shield installation, mandatory and optional packages, policies, please refer to the documentation provided:https://oxpedia.org/wiki/index.php?title=AppSuite:OX_Abuse_Shield

General Information – Please Note

- Open-Xchange encourages administrators to regularly update to the latest available release. To ensure a stable and up to date environment please note the different versions supported. An overview of the latest supported Major, Minor and Public Patch Releases can be found in the OXpedia at: https://oxpedia.org/wiki/index.php?title=OXAbuseShield:Version_Support_Commitment

Support ELK 7.x Stack

Support Elasticsearch, Logstash and Kibana 7.x stack:

- Continuous Integration now tests against ELK 7.x
- Logstash Templates now work with 7.x
- Kibana Dashboards are now in ndjson format

Support Date Expansion in WebHook URLs

WebHook URLs can be specified with fields representing years, months and days that are expanded at runtime, for example: `config_key["url"] = "https://example.com/foo/index-%{YYYY}-${MM}-{%dd}"`
See the wforce_webhook man page for more details.

Enable IP and Login Substitution in blocklist return messages

For example:
```
setBlackistIPRetMsg("Go away your IP {ip} is blacklisted")
setBlackistLoginRetMsg("Go away your login {login} is blacklisted")
```
See the wforce.conf man page for more details.

Add config option to disable password for /metrics endpoint

Adding the following to wforce.conf or trackalert.conf: `setMetricsNoPassword()` will disable the password for the metrics endpoint.
See wforce.conf and trackalert.conf manpages for more details.

Support redis usernames and passwords for redis authentication

Redis authentication is supported with the following configuration in wforce.conf:
`blacklistRedisUsername()`
`blacklistRedisPassword()`
`whitelistRedisUsername()`
`whitelistRedisPassword()`
The username is optional, depending on whether a username is set in redis.
See wforce.conf manpage for more details.

Support hostnames for redis configuration in addition to IP addresses

The blacklistPersistDB() and whitelistPersistDB() configuration commands now accept hostnames as well as IP addresses.

Add redis authentication support to wforce policy

Redis databases setups that require authentication are now supported, including both username and password and password-only use-cases.

2 Shipped Version

wforce v2.8.0
wforce-policy v2.8.0
replfwd v2.8.0

Find more information about product versions and releases at http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning_and_Numbering and http://documentation.open-xchange.com/.