Stay Open.

Open-Xchange Abuse Shield

Major Release v2.4.0

Product Guide

1 OX Abuse Shield

1.1 Intention of this document

This document provides an overview of the improvements and other changes that come with this major release of OX Abuse Shield, v2.4.0.

The purpose of this document is to inform Open-Xchange customers and partners about the major changes that have been made in this release.

1.2 OX Abuse Shield in General

OX Abuse works with both OX Dovecot Pro and OX App Suite, or any third-party software via a REST API, as a component to protect against login/authentication abuse.

OX Abuse Shield runs on a cluster of servers and integrates with both OX App Suite and OX Dovecot Pro to detect abuse, brute force attacks and also to enforce common authentication/authorization policies across the platform.

1.3 Key Features

- Replicated/clustered architecture – Login reports are shared between all the servers in a cluster so there is a single view of abuse
    - Replication of cluster data between OX Abuse Shield clusters (replfwd daemon)
- Scriptable Policy Language – Using the Lua language, the functionality of the daemon can be extended to record and protect against a large variety of abusive behavior, as well as implement specific customer policies.
- DNS Lookup Feature – For looking up IPs or domains in blacklists
- GeoIP Lookup Feature – GeoIP lookups can be made and incorporated into policy decisions.

- Rate limiting and Tarpitting – Extremely flexible, these can be enabled and enforced based on IP address, login name, geoip location, time windows, etc.

- Flexible In-Memory Statistics Database – A versatile and extensible in-memory database is used to store statistics information about abuse over time periods from a few minutes to many hours.

- Integration with Customer Authentication/Authorization Systems – Customers can use the open HTTP REST API to benefit from the protection of the anti-abuse daemon in their own authentication/authorization systems.

- Admin Console – To retrieve statistics and query server state

- Persistent Replicated Blacklist – Configurable via a REST API or the Lua policy engine, supports auto-expiry of entries, replication between all cluster nodes, and optionally uses a Redis DB for persistence.

- Webhooks – Integrate Anti-Abuse Shield with other systems using webhooks to send events.

- Metrics - Generates Prometheus metrics to enable monitoring the OX Abuse Shield platform

1.4 The Goal of OX Abuse Shield

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.

Here is how it works:

- Report successful logins via JSON http-api

- Report unsuccessful logins via JSON http-api

- Query if a login should be allowed to proceed, should be delayed, or ignored via JSON http-api
- OX App Suite and OX Dovecot's Pro POP/IMAP server are pre-integrated with OX Abuse Shield. Other software can be integrated easily using the REST API

2 Key benefits of OX Abuse Shield v2.4

2.1 New Features

- New wf_dump_entries tool to dump stats DBs to file
  New tool to dump the contents of Stats DBs for debugging purposes
- Forwarding Type in Replication Messages
  Replication messages now have a forwarding flag, which is used to indicate when a message has been forwarded. This can be used to prevent forwarding loops.
- Support for Prometheus Metrics
  Both the wforce and trackalert daemons support native Prometheus metrics via the new /metrics REST API endpoint.
- New HTTP Response Headers
  All HTTP responses now include the following headers like Last-Modified, Date and Cache-Control
- Improved Logging for Lua Errors
  The Lua wrapper code has been updated to provide better traceback information, including line numbers, for Lua errors. This helps when writing Lua policy that triggers a Lua exception.
- Session-ID now logged for allow/report commands
- Custom Lua hook to handle RBL matches
- Replfwd is a daemon to forward replication messages and black/whitelist entries between wforce clusters