OX Abuse Shield

Release Notes for Release 2.6.0

2021-12-02

1 General Information

Open-Xchange is pleased to announce the release of OX Abuse Shield v2.6.0.

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 authenticationabuse 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 OX Abuse Shield v2.6.0 provides the following main improvements and new features

- REST API supports TLS/HTTPS natively
- Multiple REST API listeners can be configured
- Outbound HTTPS connection TLS behavior is configurable
- Build on Debian Bullseye
- Support for Debian Stretch has been removed

The OX Abuse Shield v2.6.0 provides the following bug fixes

- Fix issue where building of geoip2 functionality was dependent on legacy geoip library being installed

What’s New in General

Open-Xchange now provides more detailed overviews, data sheet and product guide, relating to new product major release. These can be found at https://www.open-xchange.com/resources/ox-product-updates/whats-new/

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

- With OX Abuse Shield v2.6.0, the mandatory wforce package has been moved to an own software repository at software.open-xchange.com. All related OX Abuse Shield packages are no longer available in the ’dovecot.fi’ repository. The new repository is available inside https://software.open-xchange.com/products/abuseshield/. Please add this repository when updating from OX Abuse Shield 2.4.1 to the new minor version. The new repository is available for all customers with a valid Open-Xchange license. Please read more: https://oxpedia.org/wiki/index.php?title=AppSuite:OX_Abuse_Shield#Mandatory_Packages. OX Abuse Shield customers that have difficulty accessing the new repository should either contact their Open-Xchange Account Manager or open a Support ticket.
- 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

REST API Supports TLS/HTTPS natively

The webserver() configuration command is now deprecated, and is replaced with addListener(), which enables both TLS and non-TLS listeners to be created, as well as enabling multiple listeners to be created on-currently. The new command setWebserverPassword() is used to set the password for the REST API (previously this was set as part of the webserver() command).

An example listener without TLS:

- `addListener("0.0.0.0:8084", false, "", "", {})`

An example listener with TLS:

- `addListener("1.2.3.4:1234", true, "/etc/wforce/cert.pem", "/etc/wforce/key.pem", {minimum_protocol="TLSv1.2"}) ``

For more details, see the man page for wforce.conf.

Outbound HTTPS connection TLS behavior is configurable

Various options for the configuration of outbound HTTPS connections are now supported, specifically:

- Mutual TLS Authentication - `setCurlClientCertAndKey()` is used to specify the location of a client certificate and key for mTLS.
- Using a different CA for checking server certificates - `setCurlCABundleFile()` is used to specify the location of a file containing certs to use for this purposes.
- Disable checking peer certificates - `disableCurlPeerVerification()` disables checking of peer certificates (not recommended except for debugging).
- Disable peer certificate hostname checking - `disableCurlHostVerification()` disables checking of the hostname in peer certificates (not recommended except for debugging).

Build on Debian Bullseye

Support for building on Debian Bullseye.

2 Shipped Product and Version

Open-Xchange Abuse Shield v2.6.0

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/.