

OX Protect
v2.0

Feature Overview

1. OX Protect v2.0	3
1.1. Intention of this Document	3
1.2. Key Benefits of OX Protect v2.0	3
2. Security Reports	5
2.1. Security Dashboard	5
3. Notifications and Event Filtering	6
3.1. Simpler View of Notifications.....	6
3.2. Notifications by Device	7
3.3. Actions on Notifications	7
4. Time Windows	9
4.1. Homework Time.....	9
4.2. App Indicators for Active Schedules	9
4.3. Per-User Time Zones	10
5. Additional Enhancements	11

1. OX Protect v2.0

1.1. Intention of this Document

This document provides an overview of the new frontend and backend improvements and other changes included in this major release of OX Protect v2.0.

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. Key Benefits of OX Protect v2.0

Open-Xchange is pleased to announce the release of OX Protect v2.0. OX Protect provides a network-based protection service that offers family-friendly internet with parental control tools and protection against malware and phishing.

OX Protect protects the subscriber's connected devices in the (home) network in one go, including smartphones, laptops and computers, as well as 'Internet of Things' devices.

OX Protect comes with a web interface and easy to use Android and iOS apps that allow changes to settings and end-users to be informed about security-related events, as well as check the status of all devices on the subscriber's network.

Major enhancements in OX Protect v2.0 include:

- Security dashboard — OX Protect 2.0 comes with a security dashboard that allows users to view reports that show the security status of their network and the connected devices. It informs about blocked attempts to access filtered content, potentially malware-infected devices, and more. Security reports can be viewed over a time period ranging from one to thirty days.
- Enhanced notifications and event aggregation — a simpler way of displaying, consolidating, and acting on notifications about events such as attempts to visit blacklisted pages, blocked phishing attacks, and more.

- Homework Time — Homework Time provides a feature whereby a more restrictive set of filtering rules can be applied during certain times, for example, to support children doing their homework and removing distractions such as messaging apps or video streaming. This can be done on a per-profile basis, so different family members can have different homework times and settings.

2. Security Reports

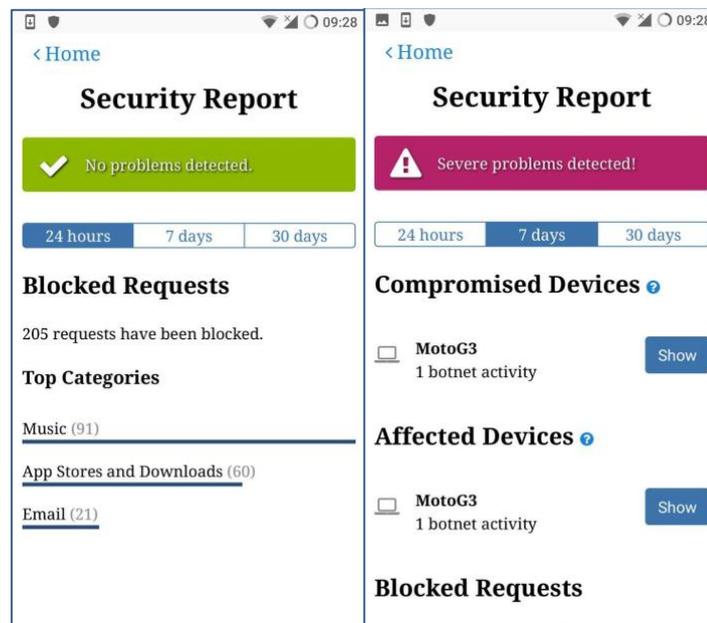
2.1. Security Dashboard

OX Protect 2.0 includes an improved end-user security dashboard that allows users to view reports that show the security status of their home and the devices within it.

If threats are detected, a status banner provides immediate insight. If this banner is shown, users can directly click “check now” to proceed to the security dashboard immediately, or they can navigate there using the regular menu. The security dashboard provides an overview of malicious activity of devices on the network. It shows affected devices that encountered “blocked” events triggered by malware, phishing or other malicious activities or parental control filters, and also compromised devices which show botnet activity and are potentially infected with a botnet or malicious software.

The security dashboard also provides an overview of the alerts that occurred in the past 24 hours, 7 days, or 30 days, allowing users to track malicious activity and act upon that.

With the new version of OX Protect, periodic per-subscriber reports can be made available to provide a regular security overview to users. These reports aggregate and summarize all relevant threat events. Similar to the security dashboard, reports can be generated at the device level to allow users to determine which specific devices might be compromised so further actions can be taken.



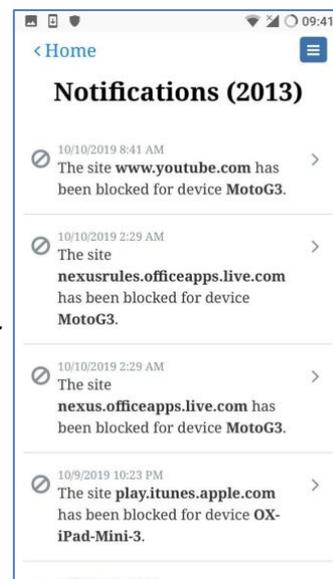
The security report provides insight into recent security-related events and indicates which devices were involved.

3. Notifications and Event Filtering

With OX Protect v2.0, Open-Xchange has improved the notifications and filtering of events, such as attempts to visit blacklisted webpages, blocked phishing attacks, and more. Notifications are now displayed in a simpler view, are allocated per device, and directly offer actions to users.

3.1. Simpler View of Notifications

While keeping a user's network secure and blocking harmful or unauthorized requests, several events are recognized. To avoid overwhelming users with many messages including the repeated messages for the same kind of event¹, the operator can now decide to enable advanced throttling of events. This lets OX Protect throttle repeated messages from the same origin and also limit the maximum number of notifications that a user can receive in a given day. An indicator displays a count of messages, allowing the user to keep track of the times a specific event occurred and providing the option to expand the consolidated view to see all entries.



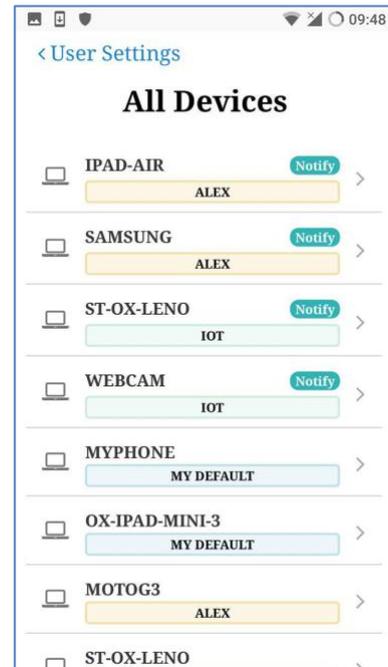
The notifications distinguish between malware, phishing and botnet activities, and users are provided with dedicated notifications for each type of malicious activity. Finally, OX Protect v2.0 supports storing all events in a versatile database for per user and/or per system wide reporting.

¹ For example, a single malware instance can generate many events in an hour. Throttling those to a single end-user notification keeps notifications useful and allows users to have an overview without being flooded by messages.

3.2. Notifications by Device

For a better overview of events and notifications per person, the OX Protect v2.0 notifications now display a user name for each device. This allows users to select and filter notifications by name and device, based on manually added device names or user-friendly names automatically set by the network.

Additionally, users can manage the devices for which they would like to receive notifications. A badge indicates devices for which notifications are enabled.



3.3. Actions on Notifications

OX Protect v2.0 provides actionable notifications. The following table gives an overview of the actions available to users for specific events.

Type of event	Available actions
Blocked site	<ul style="list-style-type: none"> • Add site to whitelist • Allow category (and switch to "custom")
Login failed	<ul style="list-style-type: none"> • Hide notification
New device recognized	<ul style="list-style-type: none"> • Edit device • Hide notification

Malware identified	<ul style="list-style-type: none"> • See report • Ignore site • Hide notification
Blocked site from blacklist	<ul style="list-style-type: none"> • Remove from Blacklist (of the related profile) • Ignore site • Hide notification
Blocked category	<ul style="list-style-type: none"> • Allow category (of the related profile) • Add to whitelist (of the related profile) • Ignore site • Hide notification

Actions available to users for different types of events

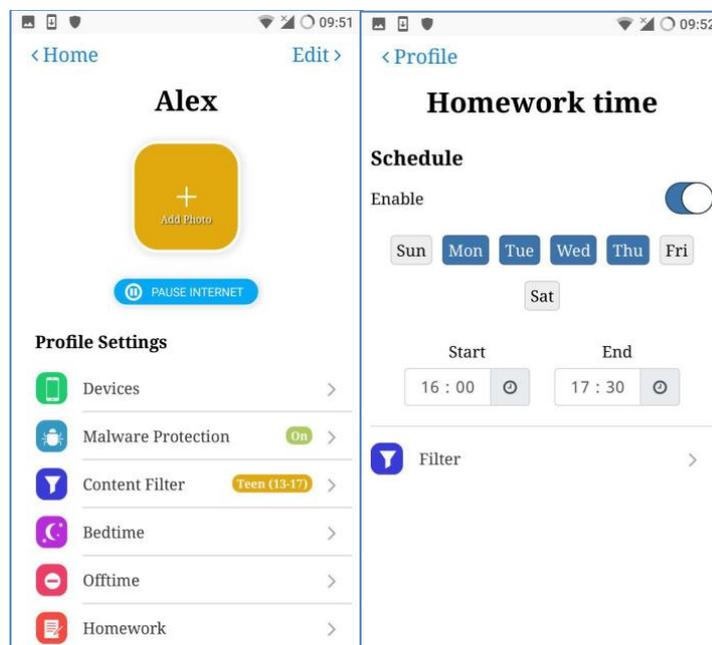
Users can also choose to ignore specific notifications. An “Ignore” button has been added to every notification, allowing a user to suppress future notifications of the respective event. Ignored pages can be edited on a dedicated ignore list page. Notifications will be listed, but a user will not receive any notifications via push, email, or text message (SMS) about events concerning ignored pages. In general, users can enable or disable notifications by email or text message (SMS) separately for malware, content, and device notifications. Finally, users are also able to delete specific or all notifications in the notifications list.

4. Time Windows

4.1. Homework Time

OX Protect’s scheduling concept helps users to restrict internet access at specific times. This lets users, for example, create schedules such as “bed time” or “dinner time” where internet access is not available to certain profiles.

OX Protect v2.0 now also supports advanced schedules called “homework time.” During the selected time(s), the regular content filtering can be made more restrictive without completely blocking access to the internet. For example, during homework time, children could still have access to sites such as Wikipedia and other educational websites, whereas social media, messaging, gaming and streaming services are blocked.



Users are able to select ‘homework time’ in their profile and then specify the days, time, and the filter that is applied during homework times

4.2. App Indicators for Active Schedules

To let users quickly check whether a schedule is active for specific profiles, OX Protect v2.0 provides dedicated indicators on the home screen. A badge indicates if any type of off-time is enabled for a user (paused, bed time, homework time, etc.).

4.3. Per-User Time Zones

Previously, OX Protect only supported a single time zone for all users. Now users can specify their local time zone (it will also be auto-detected when using the OX Protect app), and schedules will apply according to the selected time zone. This means that a single OX Protect installation can handle users across many different time zones.

5. Additional Enhancements

In addition to more user-friendly notifications and improved time windows, OX Protect v2.0 comes with the following additional enhancements.

Enhancement	Description
OX Feed	Efficient and uniform way of distributing the security feeds from Open-Xchange to customers, as well as more efficiently distributing feeds between nodes at a customer setup.
Push down to update	Users can update a current page by using push down.
Take a new photo for profile pictures	Users can use the device's camera to take a new picture when adding a profile picture (iOS).
Show version number	App shows current version number on the "About" page (iOS).
Warning about missing OX Protect categories	Admin is warned if a platform installation does not contain any OX Protect categories.
Prometheus metrics	Admin sees Middleware web service metrics via Prometheus, such as request response times, number of active and total sessions, and other system metrics.
Download personal data (GDPR)	To satisfy GDPR requirements, a user can download his or her "personal data" in JSON format. This includes the user's userID, mail address, phone number, profile(s) name, off-time schedule names, deviceId, Mac, and device name.
Inactivity timeout	To improve security measures, an admin user can configure an inactivity timeout of a session. An inactive session will be invalidated once the timeout has been reached.
Show error messages for middleware unavailability	If for any reason the OX Protect middleware is not available, the UI displays an appropriate status to users providing detailed error messages.

Information about the need to reestablish sessions	To avoid failing attempts to send changes to the (web-) middleware once a user session is not or no longer valid, users are informed and guided through a session reestablishment process.
Notification about JavaScript and Cookies	OX Protect requires JavaScript and Cookies to perform as desired. If a user's browser does not support JavaScript or the user has disabled JavaScript and Cookies, a notification is displayed asking the user to enable JavaScript and Cookies.