OX Protect

v1.0.0

Product Guide

1 OX Protect

1.1 Introduction

This document provides an overview of the new product OX Protect. The document has been designed to help Open-Xchange customers and partners understand the logic behind this new product.

1.2 The Idea behind OX Protect

OX Protect provides a network-based protection service that offers family-friendly internet combining parental control tools and protection against malware and phishing.

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

It can be deployed by Internet Service Providers and offered towards their subscribers.

Protect comes with a web interface and easy to use Android and iOS apps for end-users that allow to change settings, be informed about the security-related events, and check the status of all devices in the home network, including IoT devices.

1.3 Features

OX Protect provides an end-user centric security solution including:

- Per-device, per profile filtering and settings
- Modular deployment with APIs for integration with third-party apps and ISP OSS systems for provisioning
- Notification Module for real-time notifications
- iOS and Android Apps as well as a web portal for end-user control

1.3.1 Key features for the end-users

OX Protect offers the following key elements:

- Safe and secure internet
- Family friendly internet access
- Control access to specific websites and apps
- Easy management of time windows
- Network based security for all your devices
- Protection against malware, phishing, botnets, etc
- Protects all devices in the home network, including the IoT devices: phones, tablets, laptops, smart tv's, camera's etc.
- Easy-to-use Android and iOS apps and a web portal
- Setup security and parental control Profiles per device and/or per family member
- Alerts and real-time notifications to inform users important events

1.3.2 Key features for Internet Service Providers

- Provide a secure internet experience for the entire family
- Engage with your subscribers
- Allow your users to control access to specific websites or limit the use of specific apps
- Offer Malware filtering and online security features
- Be in control of the content categories
- No additional end-user hardware required

1.4 Content filtering and time windows management

OX Protect for Families offers content filtering and parental control with unique Multi-Level Control for Safe Browsing per user and supports many categories, time-windows, and white- and black lists.

1.4.1 Features

- Selective filtering based on categorization of hundreds of millions of sites.
    - Parental control, selective parental control
    - Modest hardware requirements
    - Scales to tens of millions of customers
- Subscriber settings
    - Comes with subscriber Apps and self-management module
    - API to integrate with existing customer portals like self-care portal
- Selective filtering options
    - Select categories to be filtered (i.e. malware, 'child friendly', 'brand safe', advertising)
    - Per subscriber preset filter sets ('light, medium, strict')
    - Different filtering profiles for different devices in the household (to treat a kid’s laptop different from a parent’s tablet)
    - Per subscriber blacklist and whitelist
- Support existing, local, and/or other categorization lists
    - based on categorization of hundreds of millions of sites
    - including support for all the major categorization providers)
- Advanced time-window settings for filters

  - Time-window for filtering ('no filtering at specific times')
  - Allows for ‘homework time’ (e.g. block Facebook but allow Wikipedia and other educational websites during the afternoon)
  - ‘Bed time’ -settings (‘no social media after 21:00’)

1.5 Protection and Security

Often malware infections pass through DNS. DNS is the way to make malware hosting independent of IP addresses. This, of course, exactly parallels the role of DNS in the everyday world of the ordinary internet service provider. Attackers abuse the flexibility of DNS to evade discovery and law enforcement.

The PowerDNS filtering engine makes use of threat intelligence (bundled with the OX Protect solution) to block access to:

- Known bad domain names,
- Domain names that resolve to known bad IP addresses (i.e. IP blocking),
- Domain names that depend on known bad name servers.
- Domains that correspond to known malware Command and Control (C2) servers.

The primary goal of this solution is to prevent end-user devices becoming infected. The secondary goal is to detect infected devices, and in conjunction with third-party solutions, remediate infections.

1.6 Controlling content filtering and security

OX Protect can provide iOS and Android apps as well as a Web-gui to control security and parental control settings. These include:

- User Centric control apps
  - For iOS and Android
  - Centralized End-User Notifications and Control

- Configuration management
  - Control Filtering settings for household and for per-person or device profiles to allow settings for individual devices
- Push Notifications
  - Controllable Push Notifications of suspicious events

OX Protect can alternatively also be integrated with existing customer apps through the OX Protect Middleware REST APIs.

2 Deployment of OX Protect

2.1 System Requirements

OX Protect integrates with the Network of the Internet service Provider at the DNS level. It uses the PowerDNS platform for the DNS-integration. (Note that the existing DNS infrastructure can remain in place if that is preferred).

For installation of the OX Protect middleware and the Notification Center, specific system requirements must be met. These are documented at http://oxpedia.org/wiki/index.php?title=Protect:OX_Protect

3 Using the OX Protect App and Web Interface

3.1 The general design

Protect comes with an Android and an iOS app and also includes a web portal. The App acts as the ‘central control’ interface, from which the user can control the settings of OX Protect, define profiles, receive real-time notifications, and more.

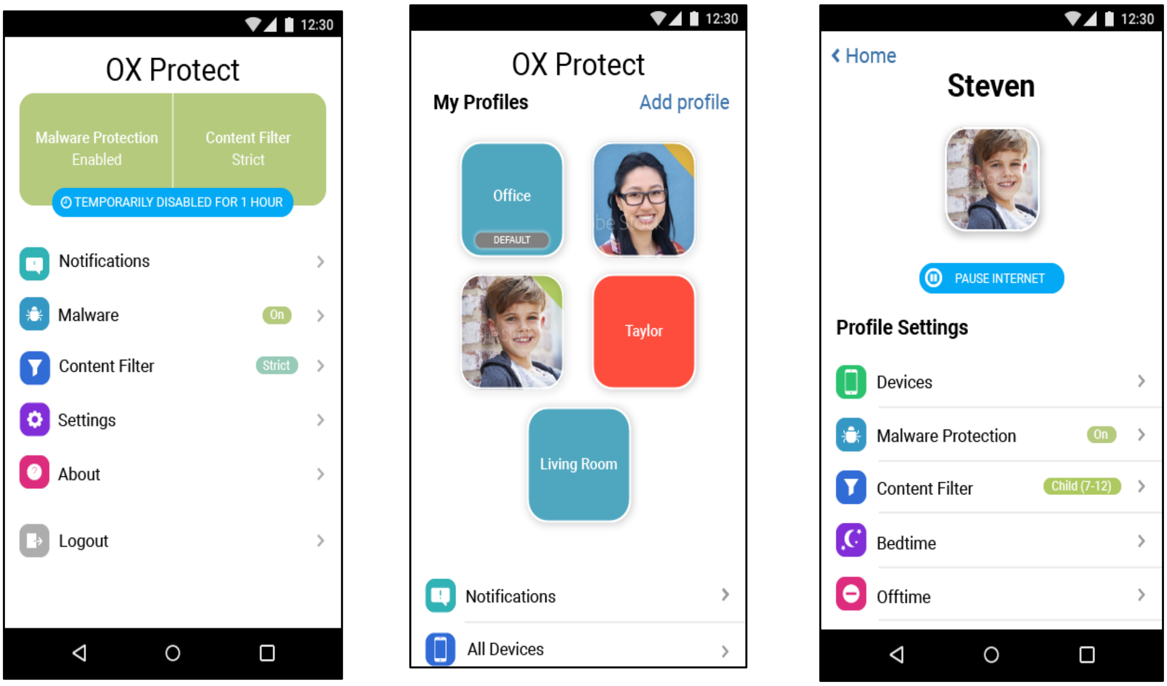


Figure 1, Screenshots of the Protect app for Android showing a) the overview 'home' screen, b) the various defined profiles, and c) the detailed settings of a profile.

3.2 Home Screen

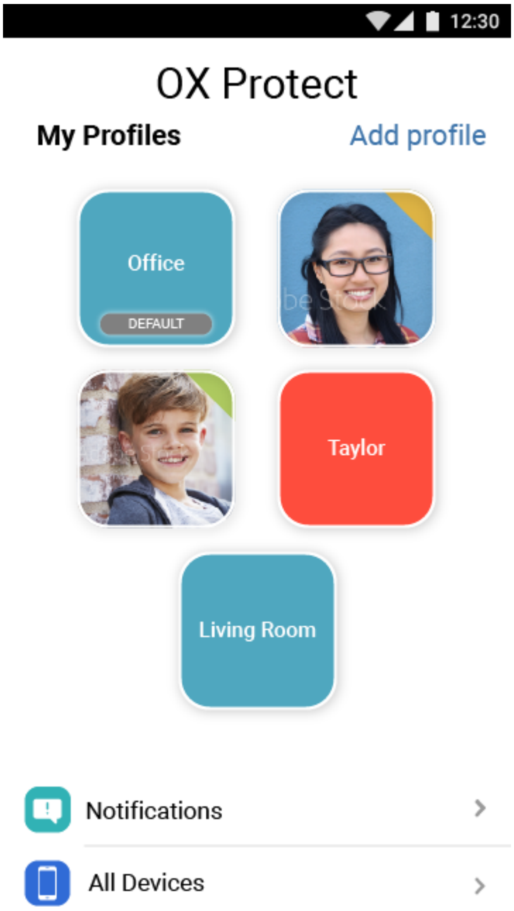
After logging in the app will show the User's profiles (at least one default profile) and the most recent notifications. The credentials are automatically stored, and the user will be logged in automatically next time accessing the app.

By selecting any of the profiles, the specific profile settings for that profile are shown and can be edited, see paragraph 3.3)

The home screen displays the following information and functions:

- 'Notifications' to view the recent Notifications
- 'All Devices', for a list of all devices, and selecting and assigning them to profiles
- Overview of existing profiles and the option to create a new profile

- Settings for generic settings of OX Protect and the Notifications.
- ‘About’
- ‘Logout’



OX Protect

My Profiles

Figure 2, The Home screen shows the defined profiles and allows for selecting and changing options.

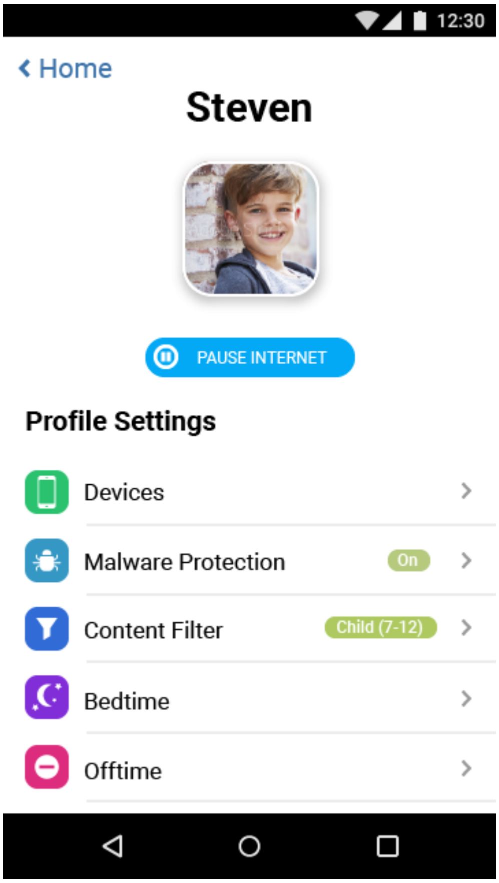
The option to add a new profile will start the ‘profile wizard’ and will guide the user though the setup process.

Once the app is authenticated and active, the device will receive native push notifications when there are new events that trigger a notification.

3.3 Profile Settings-screen

The Profile Settings screen displays the following profile settings:

- ‘Devices’, to see all devices assigned to this specific profile
- ‘Malware Protection’ shows if malware protection is active, and allows to switch it on or off
- ‘Content Filtering’ shows the currently active filter and allows to change the settings of the current filter. See paragraph 3.4
- ‘Bedtime’ allows to implement timers for pausing the internet for this profile at specific times.
- ‘Offtimes’, allows to 1 the chosen profiles or devices from the internet completely



Steven

Profile Settings

Devices

Malware Protection On

Content Filter Child (7-12)

Bedtime

Offtime

Figure 3, When selecting a profile, the specific settings for that profile (i.e. family member) can be changed, Malware filtering can be switched on and off, and the content filer settings can be adjusted.

3.4 Content Filtering-screen

The Content-filter is used to define filter-settings for each of the profiles.

The screen displays a number of age-based pre-define filter levels and allows the user to select one of them for the profile under consideration. Below that, it displays the blocked and allowed categories for the selected pre-defined filter.

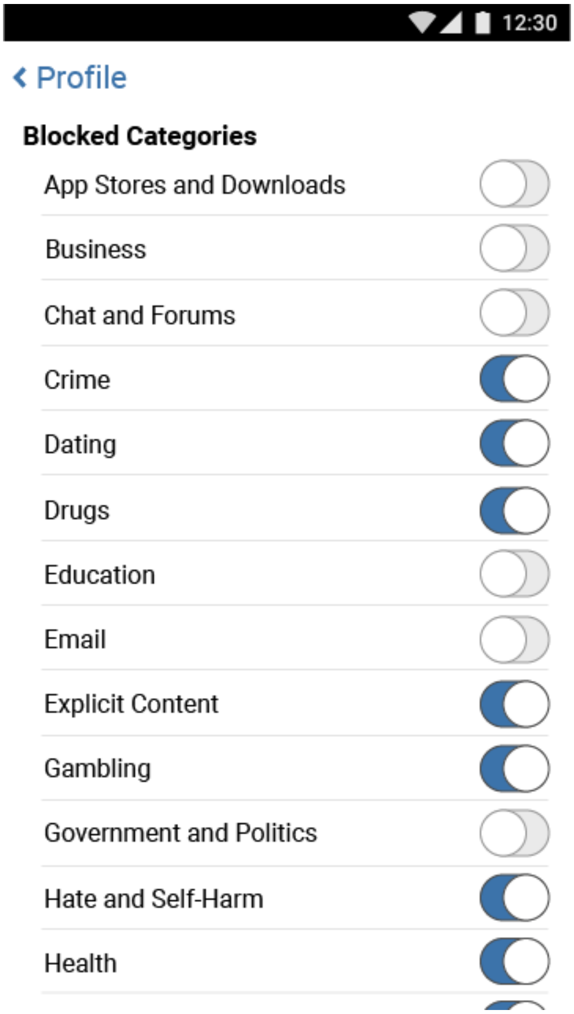
Selecting ‘custom’ in the pre-defined profile list allows to manually fine-tune the categories blocked, **Fehler! Verweisquelle konnte nicht gefunden werden.**.

Below the ‘filter level settings’, it allows settings of the following features:

- Whitelisted platforms, to specifically block or allow ‘internet platforms’ on top of the default filter-profiles

- Black and whitelist, to add domains on a per profile level to either black or whitelists (precedes other filters)

- Safe search, to switch on the Bing, Google and YouTube safe searching features.



12:30

‹ Profile

Blocked Categories

App Stores and Downloads	○
Business	○
Chat and Forums	○
Crime	●
Dating	●
Drugs	●
Education	○
Email	○
Explicit Content	●
Gambling	●
Government and Politics	○
Hate and Self-Harm	●
Health	●

Figure 4, The ' blocked Categories' section allows fine-tuning of the Categories that should or should not be blocked.

3.5 Configurability

The various defaults, settings, and pre-set profiles in the OX Protect interface are configurable by the ISP. This allows for local adjustments regarding age-range of profiles, specific categories that need to be blocked based on the customer base, and more.