Webfilter und Kinder-/Jugendschutzsoftware

Windows-Tablets aus der Geräteinitiative absichern
Empfehlung für Eltern / Erziehungsberechtigte

Version 23.01

Vorarlberger Bildungsservice
Verfasser: Dietmar Köb
Besuchen Sie uns im Internet
http://www.vobs.at/rb

Inhalt

1. Grundsätzliches

Von Elternseite wurde mehrfach der Wunsch geäußert, die Geräte der SuS dahingehend abzusichern, dass vor allem Webseiteninhalte blockiert werden die nicht für Kinder / Jugendliche geeignet sind.

Dazu gibt es mehrere Ansätze / Möglichkeiten - zwei Varianten werden hier vorgestellt. Grundsätzlich sollte es auch funktionieren, die beiden unten vorgestellten Varianten zu kombinieren (DNS-Serveradressen von Cleanbrowsing über Intune vorgeben und zusätzlich als Elternteil die App „Qustodio" einsetzen).

Grundsätzliche Bemerkungen:

- Die SuS haben laut unserem Konzept von ihrem Gerät den Administrator-Zugang, weil die Geräte ja im Privatbesitz der Schüler*innen bzw. der Eltern / Erziehungsberechtigten sind. Dieser Zugang eröffnet prinzipiell und verbunden mit entsprechendem Knowhow immer die Möglichkeit, vorgegebene Einstellungen und Beschränkungen wieder zu löschen oder zu umgehen. Soll dies verhindert werden, dann müssen die Eltern ein neues lokales Administratorpasswort vergeben, das den Schüler*innen nicht bekannt ist.

- Die hier vorgestellte Kindersicherungs-App „Qustodio" (=Variante 2) bietet den Eltern neben diversen Webfiltern erweiterte Überwachungsmöglichkeiten (Stichwort: „BigBrother") . Deshalb ist eine offene Kommunikation bzw. gemeinsame Umsetzung mit den Kindern / Jugendlichen und die genaue Information, was über besagte App alles abgerufen werden kann, ein Gebot der Stunde und zu empfehlen.
  Weiters ist zu begrüßen, dass die App „Qustodio" auch im kostenlosen Modus (Gratismodus) die wichtigsten Schutzfunktionen wie Webfilter und Zeitbeschränkungen für ein Gerät ermöglicht.

2. Variante 1 – „nur" Webfilter über Intune vorgeben

Es gibt diverse „Dienstleister", die über die so genannte DNS-Filterung dafür sorgen, dass unerwünschte und für Kinder nicht geeignete Webseiten gar nicht über die Geräte aufgerufen werden können.
Bei der DNS-Filterung wird das „Domain Name System" (DNS) genutzt, um schädliche Websites zu blockieren und böswillige oder unangemessene Inhalte herauszufiltern.

In der Praxis haben wir folgende zwei Services bei uns an den Schulen schon längere Zeit im Einsatz:

- Open-DNS
- Cleanbrowsing

Open-DNS eignet sich besonders für den Einsatz im Schulnetzwerk (Konfiguration über die Firewall und den DNS-Server der Schule) – siehe eigene Doku dazu (für IT-Betreuer*innen):
IT-Support-Bereich des Vobs -> Suche – Suchbegriff „DNS-Filter" (Anmeldung erforderlich)

Für unsere Zwecke (Filterung soll auch zu Hause und über alle Internetzugänge greifen) ist „Cleanbrowsing" besser geeignet. Es werden dabei „nur" die zwei DNS-Serveradressen auf den Tablets abgeändert und über Intune (= Microsoft Endpoint Manager) den Schülergeräten vorgegeben.
Die beiden DNS-Serveradressen von Cleanbrowsing, die den „Family Filter" bereitstellen, lauten:

```
185.228.168.168
185.228.169.168
```

Diese Einstellungen geben wir als Schule über Intune über ein Powershell-Script vor. Leider hat sich in der praktischen Umsetzung ein neues Problem gezeigt (danke an die Tester): Wechselt ein angemeldeter Benutzer ohne Admin-Rechte die WLan-Verbindung, so „greift" das Skript nicht, weil dieser Benutzer nicht die Rechte hat, die per DHCP zugewiesenen DNS-Einträge zu ändern. Über Intune zugewiesene normale Powershellskripte (wenn sie einmal funktioniert haben) werden kein weiteres Mal ausgeführt. Somit greift unser Skript nicht mehr.

Wir implementieren dieses Skript deshalb nicht als „normales“ Powershellskript, sondern als „Proactives Remediations-Sript“ („Proaktive Korrekturen“). Dafür ist neben dem „Hauptskript“ ein weiteres, das so genanntes „Detection-Script“ erforderlich.

Inhalt des ersten Skripts (=Erkennungsskript):

```
# DK 17.02.2023 V3
# für SuS-Geräte aus der Geräteinitiative (Windows)
# DNS-Serveradressen von cleanbrowsing über Intune fix vorgeben
# Skript fragt zuerst ab, welches der momentan aktive Netzwerkadapter ist und dann dessen DNS-Einträge
# Skript gemeinsam mit dem dazu passenden Wiederherstellungsskript verwenden: MS Endpoint Manager -> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausführen aktivieren -> Zeitplan auswählen -> der Schülergerätegruppe zuordnen
#================================================================

[int]$activeAdapter = Get-NetAdapter | % { Process { If ( $_.Status -eq "up" ) { $_.ifIndex } }};
$DNSactiveAdapter=Get-DnsClientServerAddress -interfaceIndex $activeAdapter -AddressFamily IPv4 | Out-String
$DNSpasst = $DNSactiveAdapter -match {185.228.168.168, 185.228.169.168}

Try {
    if ( $DNSpasst ) {
        Write-Host $True
        exit 0
    }
    else {
        Write-Host $False
        exit 1
    }
}
Catch {
    Write-Warning $_
    exit 1
}
```

Codezeilen in Textdatei kopieren und z. B. mit Dateinamen
`DNS4Cleanbrowsing_Erkennung_v3.ps1`
abspeichern (oder die Datei hier herunterladen).

Das Skript fragt ab, ab beim momentan aktiven LAN-Adapter die DNS Einträge von Cleanbrowsing vorhanden sind: Wenn ja, wird nichts weiter gemacht, wenn nein, wird das untenstehende Wiederherstellungsskript ausgeführt.

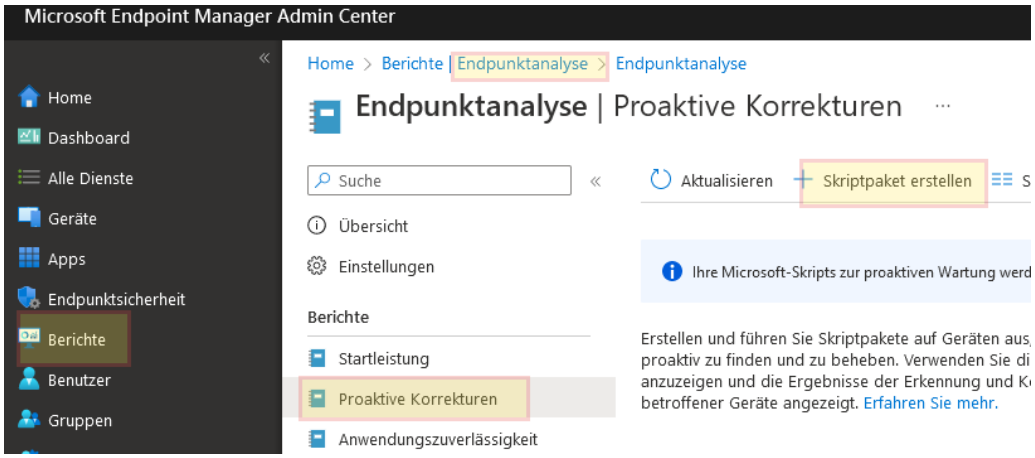
Inhalt des Haupt-Skripts (=Wiederherstellungsskript):

```
# DK 17.02.2023 V3
# für SuS-Geräte aus der Geräteinitiative (Windows)
# DNS-Serveradressen von cleanbrowsing über Intune fix vorgeben
# Skript fragt zuerst ab, welches der momentan aktive Netzwerkadapter ist und ändert dann dessen DNS-Einträge
# Skript gemeinsam mit dem dazu passenden Erkennungsskript verwenden: MS Endpoint Manager -> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausführen aktivieren -> Zeitplan auswählen -> der Schülergerätegruppe zuordnen
#=============================================

# Variablen definieren
#DNS-Nameserver-IP-Adressen (sind immer die gleichen IPs)
#OpenDNS
#$dns1 = "208.67.222.222"
#$dns2 = "208.67.220.220"

#cleanbrowsing.org Family-Filter
$dns1 = "185.228.168.168"
$dns2 = "185.228.169.168"

#================================================================================================
# Skript fragt den aktiven Netzwerkadapter ab und ändert dann bei diesem Adapter die DNS-Einträge
ipconfig -flushdns

#DNS-Serveradressen dem aktiven Netzwerkadapter zuordnen
[int]$activeAdapter = Get-NetAdapter | % { Process { If ( $_.Status -eq "up" ) { $_.ifIndex } }};
Set-DNSClientServerAddress -interfaceIndex $activeAdapter -ServerAddresses ($dns1,$dns2);

ipconfig -flushdns
exit 0
```

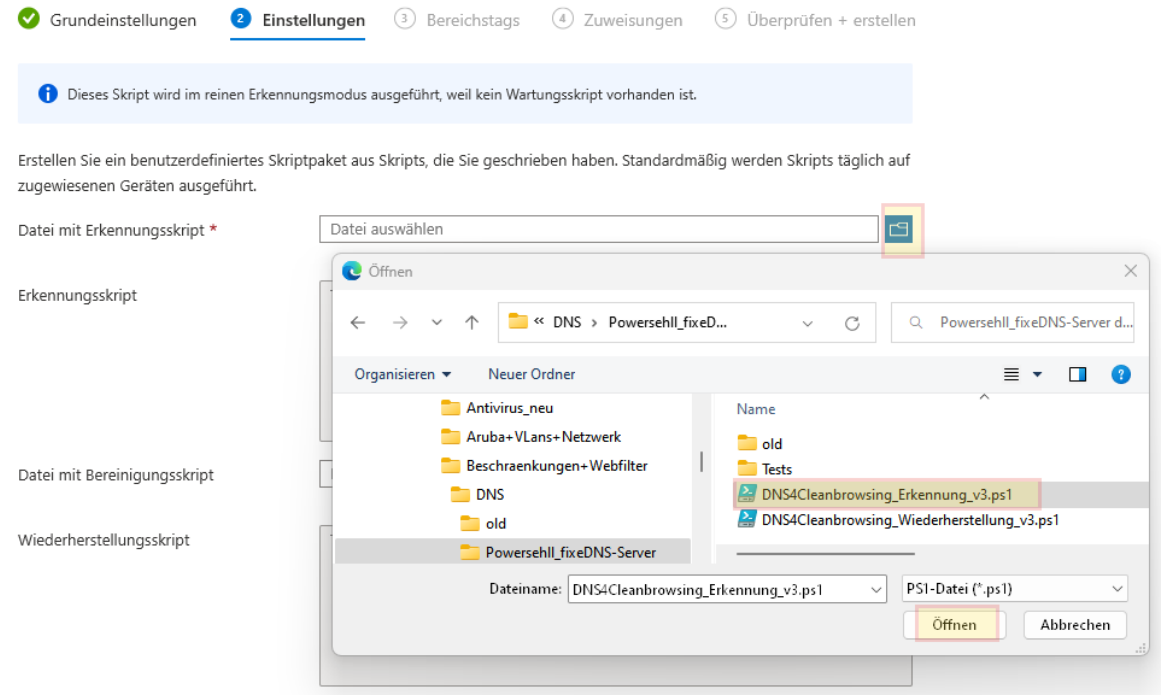
Codezeilen in Textdatei kopieren und z. B. mit Dateinamen
`DNS4Cleanbrowsing_Wiederherstellung_v3.ps1`
abspeichern (oder die Datei hier herunterladen).

Das Skript fragt über den Adapter-Index ab, welcher LAN-Adapter momentan aktiv ist und ändert anschließend die DNS Einträge nur von diesem aktiven LAN-Adapter.

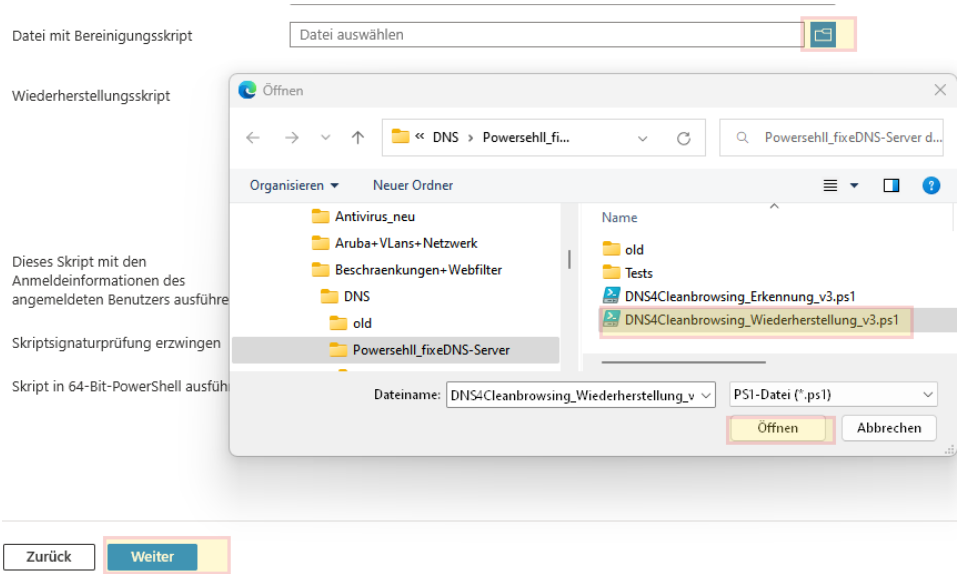
In Intune: Berichte -> Endpunktanalyse -> Proaktive Korrekturen:

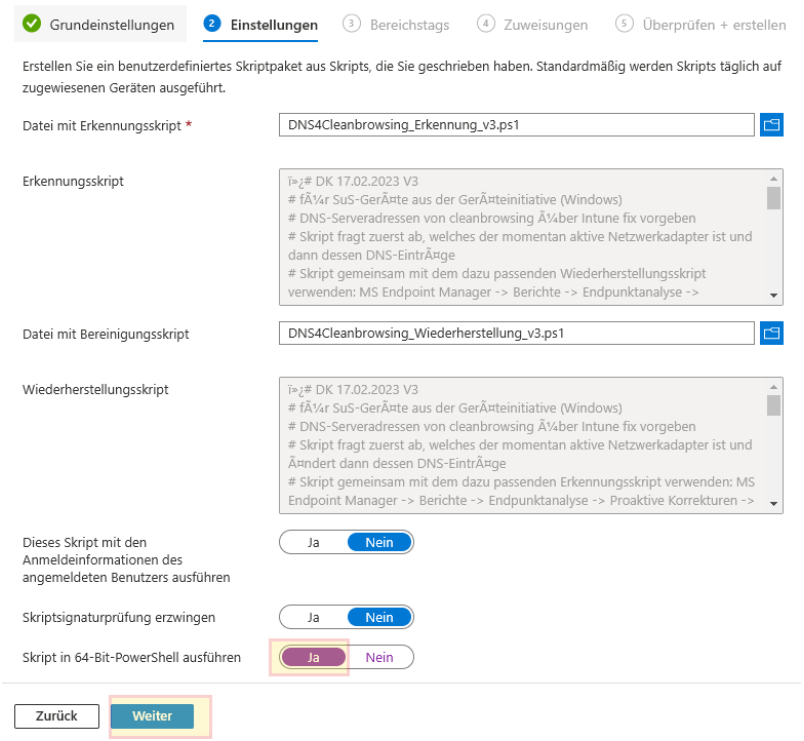


Erkennungsskript zuordnen:



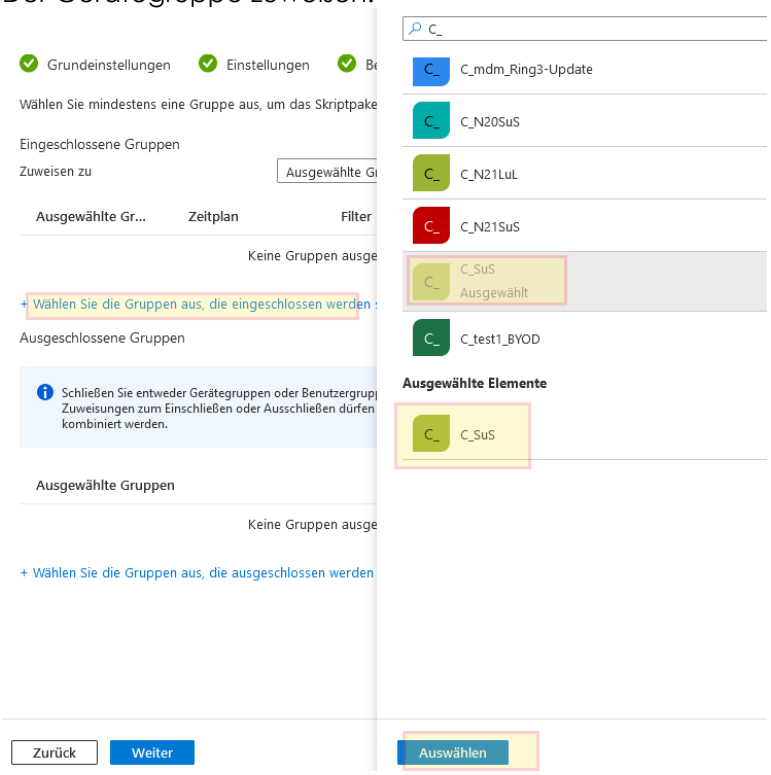
Wiederherstellungsskript zuordnen:



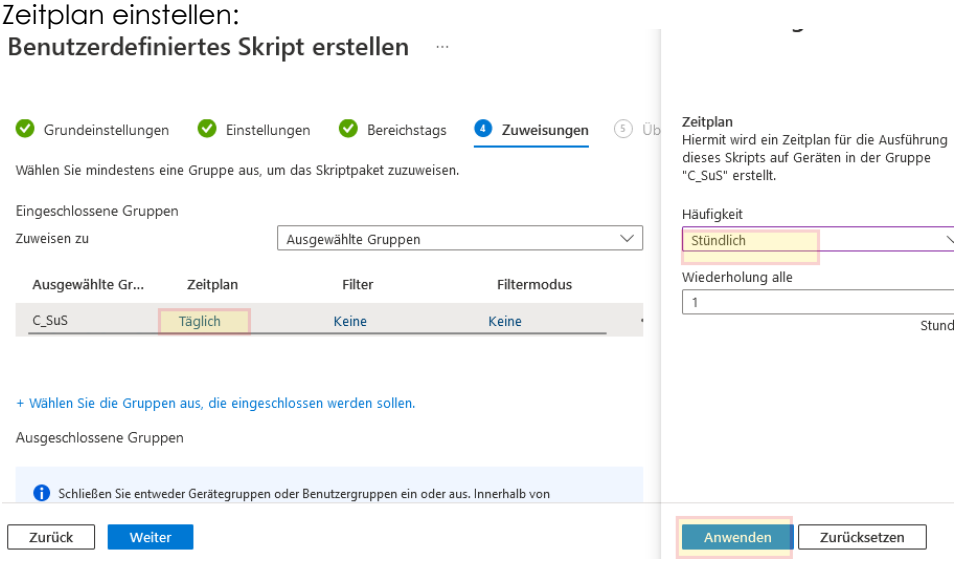


➔ keine Bereichstags

Der Gerätegruppe zuweisen:



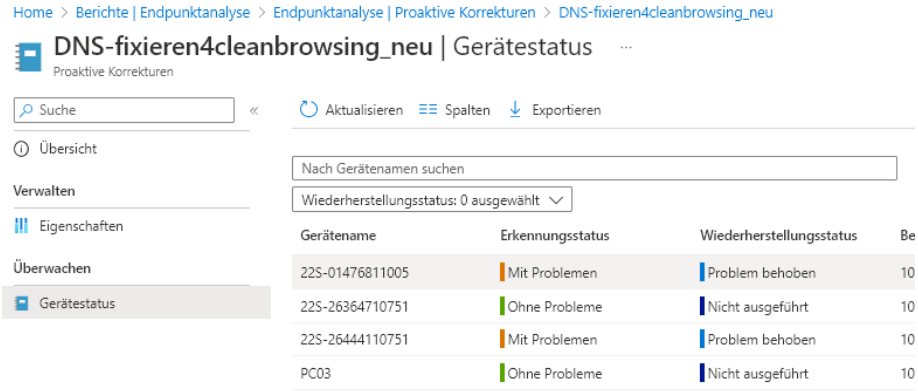
Zeitplan einstellen:



➔ Erstellen

Damit wird ca. jede Stunde (hängt auch davon ab, wann sich ein Gerät wieder bei Intune „meldet“ = „Letzter Check-In“) kontrolliert, ob die beiden DNS Einträge 185.228.168.168 und 185.228.169.168 da sind (=Erkennungsskript). Wenn ja, passiert nichts, wenn nein, wird das Wiederherstellungsskript ausgeführt, welches besagte Einträge macht.

In Intune schaut das dann z. B. so aus:



„Mit Problemen“ heißt in diesem Fall „DNS-Einträge nicht da“ -> Wiederherstellungsskript wird ausgeführt -> „Problem behoben“ 😊
„Ohne Probleme“ (= DNS Einträge passen) -> Wiederherstellungsskript wird gar nicht ausgeführt.

Information zu diesem Filter:
Der Family-Filter blockiert den Zugriff auf alle nicht jugendfreien, pornografischen und expliziten Seiten. Er blockiert auch Proxy- und VPN-Domains, die zur Umgehung der Filter verwendet werden. Seiten mit gemischten Inhalten (wie Reddit) werden ebenfalls blockiert. Google, Bing und Youtube sind auf den abgesicherten Modus eingestellt. Schädliche und Phishing-Domains werden blockiert.

Hinweis: Mit dem Administrator-Zugang kann diese Einstellung am Gerät recht einfach „rückgängig“ gemacht werden. Um dies zu verhindern, muss (z.B. von den Eltern) ein neues Administrator-Passwort vergeben werden, das der/dem Schüler*in nicht bekannt ist.

3. Variante 2 – Programm „Qustodio“

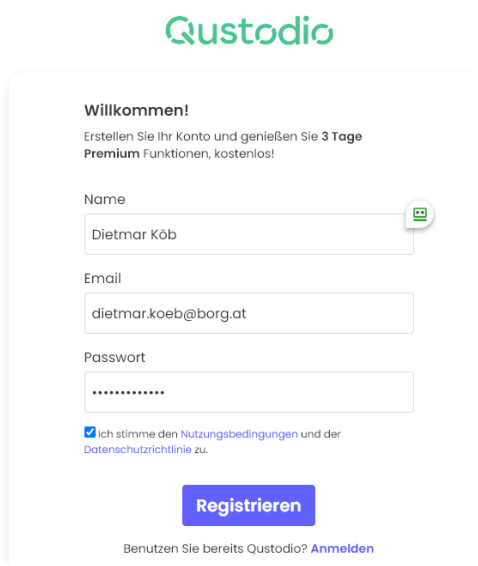
Mehr Möglichkeiten und Einstellungen bietet ein Kinder-/Jugendschutzprogramm a la „Qustodio“.

In Unterschied zu Variante 1 wird bei dieser Option das Programm nicht fix von der Schule über Intune vorgegeben. **Die Eltern erstellen bei Qustodio einen Account und installieren das Programm (gemeinsam mit den SuS) auf dem Schülergerät.** Es bietet sich an, diese Minianleitung den Eltern zur Verfügung zu stellen und damit die Entscheidung über eine „Beschränkung bzw. Überwachung“ den einzelnen Erziehungsberechtigten zu überlassen.

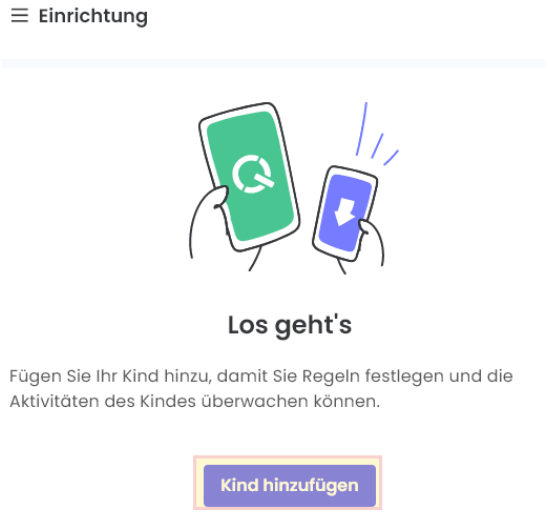
3.1. Qustodio – Konto anlegen

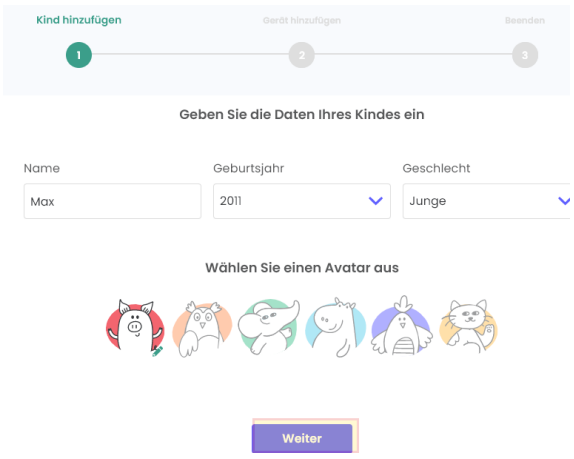
Als Elternteil / Erziehungsberechtigte(r) Registrierung auf qustodio.com (das kann von jedem x-beliebigen Gerät aus gemacht werden):
https://www.qustodio.com/de/

- ➔ „Einloggen“ -> Familien
- ➔ „Registrieren“ mit Name, Emailadresse und Passwort
- ➔



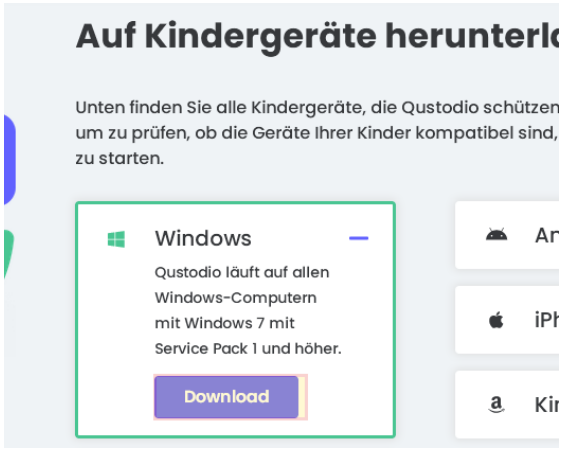
-> man erhält eine E-Mail: Emailadresse bestätigen …





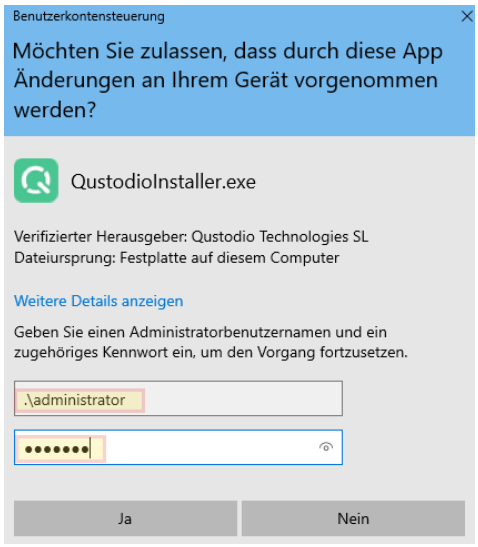
3.2. Qustodio – Clientprogramm auf dem Schülergerät installieren

Spätestens jetzt wechseln wir auf das Schülergerät und laden das „Qustodio-Clientprogramm“ herunter: www.qustodio.com/downloads

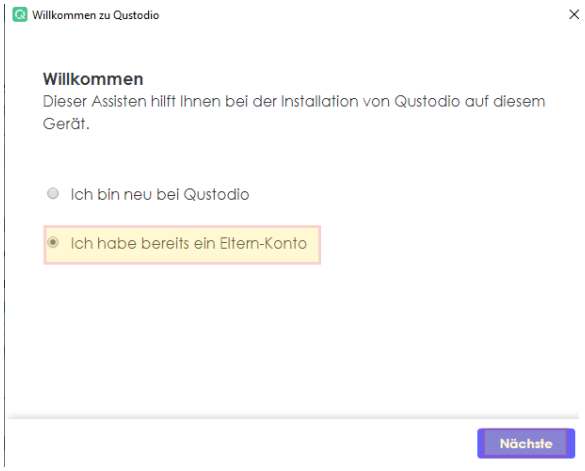


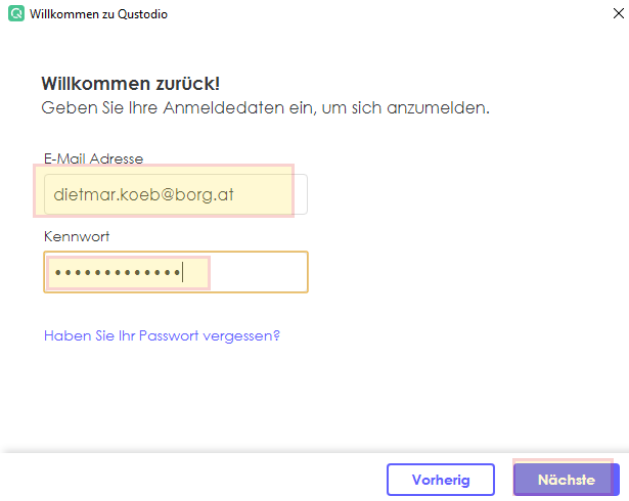
direkter Downloadlink: https://family.qustodio.com/download/windows

Das heruntergeladene Programm („QustodioInstaller.exe“) wird gestartet und das Programm mit den Standardeinstellungen installiert. Sollte der angemeldete Benutzer keine Administratorrechte haben, dann meldet sich die „Benutzerkontensteuerung“ und es müssen die Administrator-Anmeldedaten eingegeben werden:



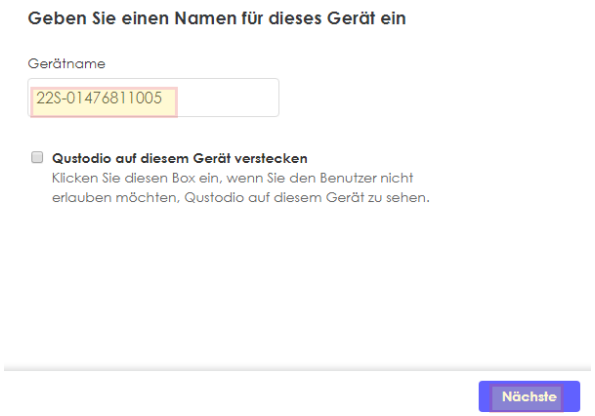
Achtung beim Benutzer: .\ voran stellen …

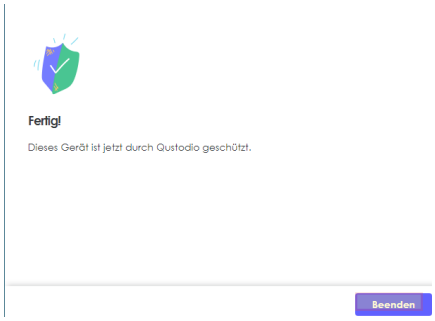


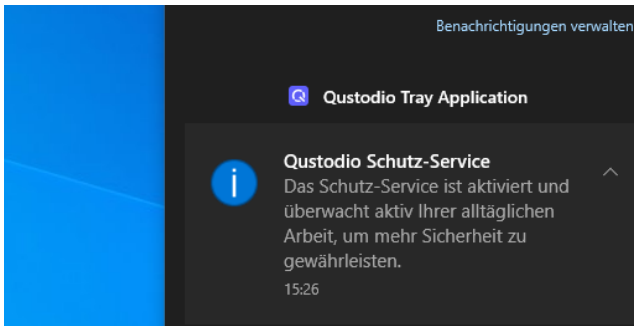


➔ Logindaten von der Registrierung (Kap. 3.1) eingeben

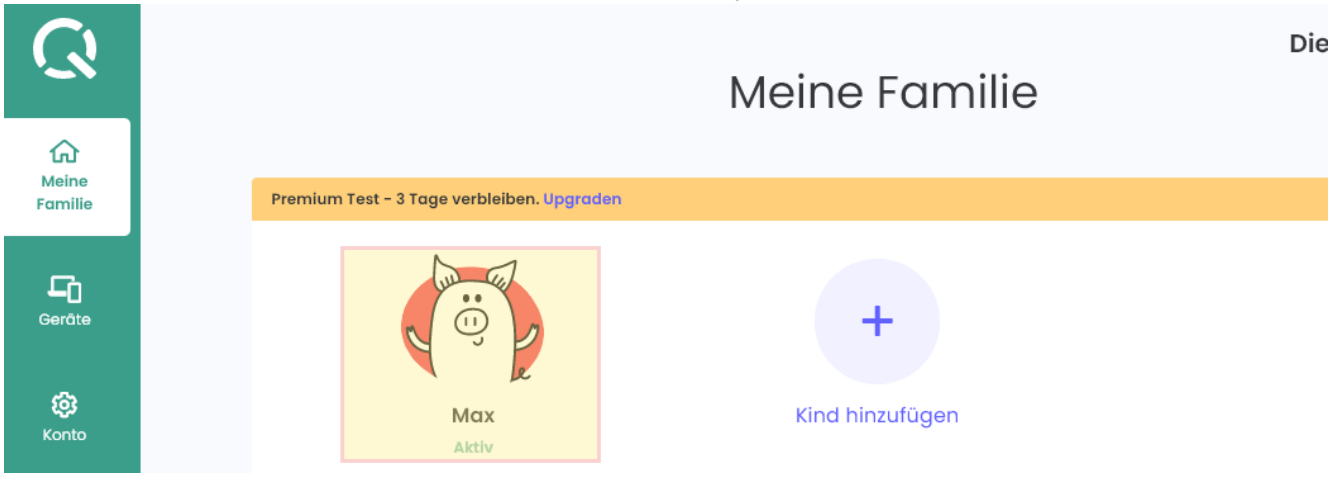
Es wird der Gerätename angezeigt (kann auch geändert werden):





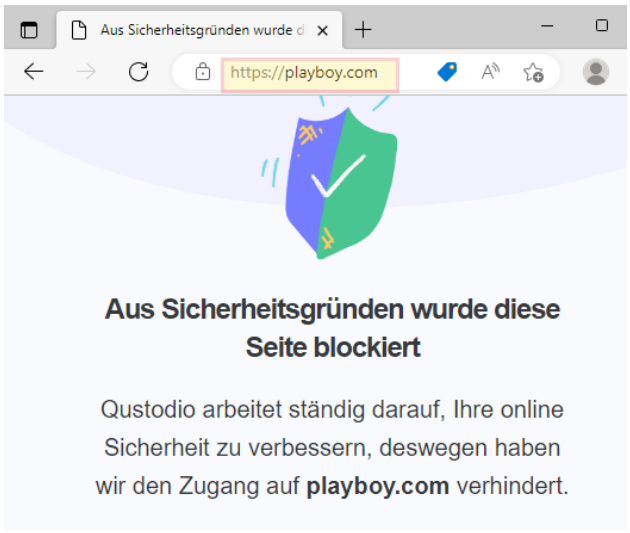


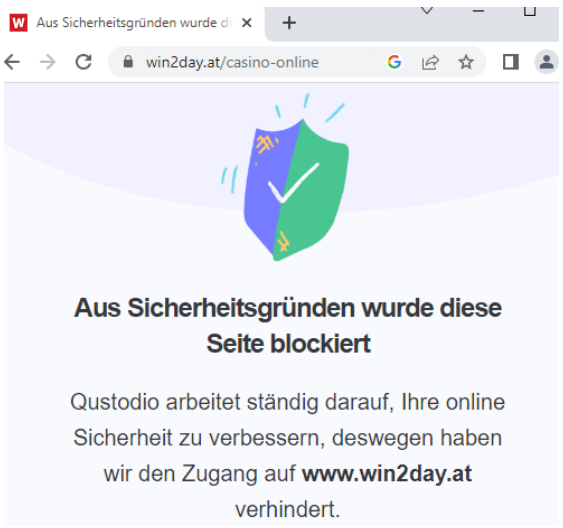
Nach Abschluss der Installation erscheint das Gerät im Qustodio-Onlineaccount:



… und der Schutz ist aktiviert.

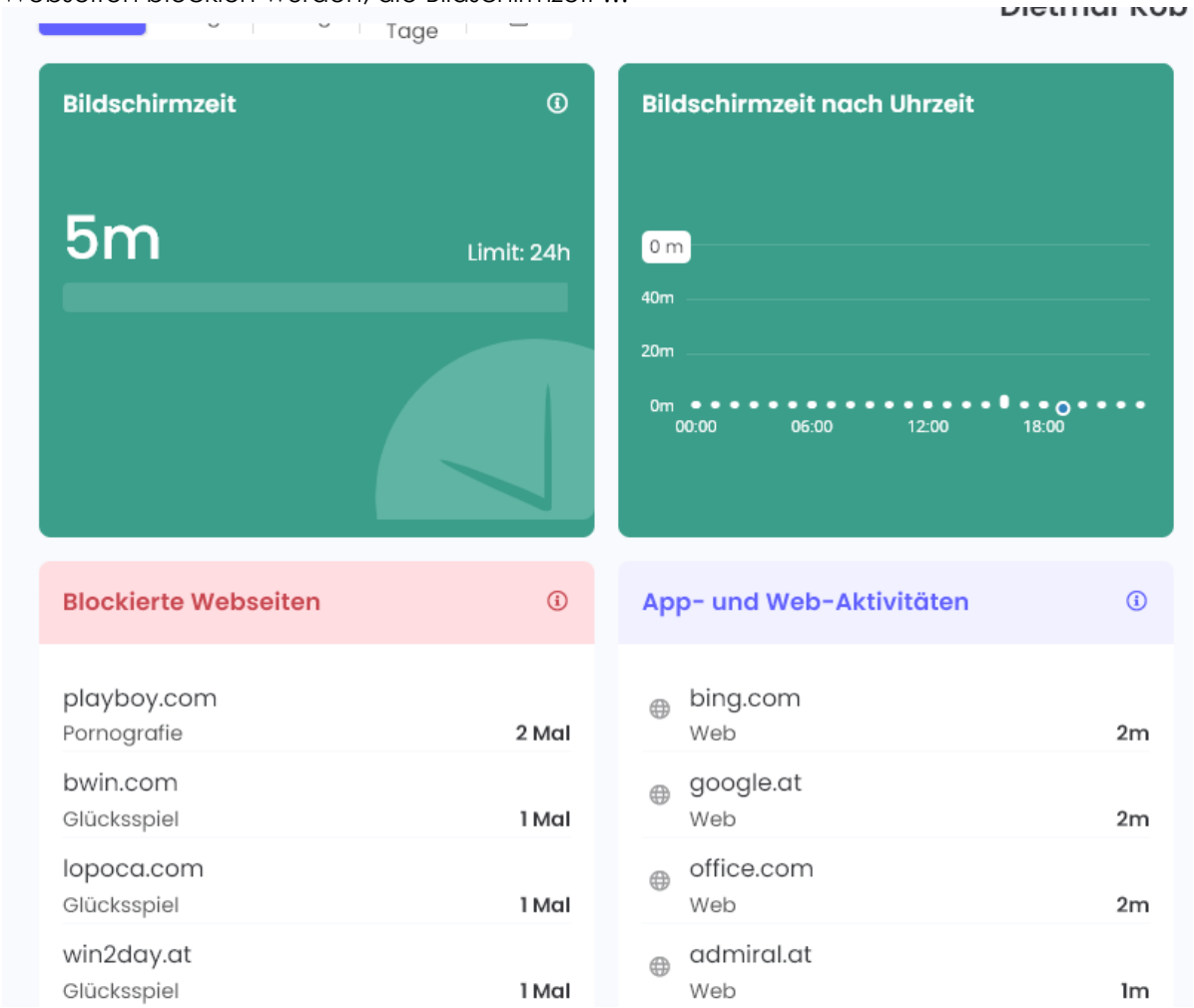
Auf dem Schülergerät werden entsprechende Webseiten (egal, mit welchem Browser sie geöffnet werden) geblockt:

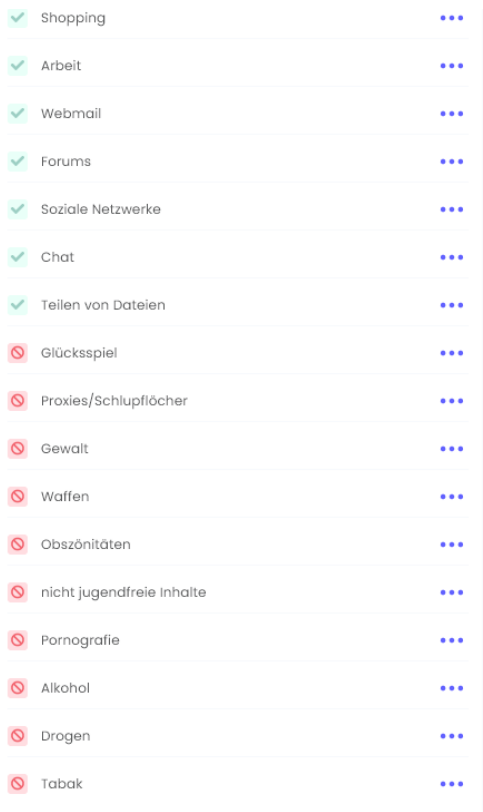




4. Einstellungen und Infos zu „Qustodio“

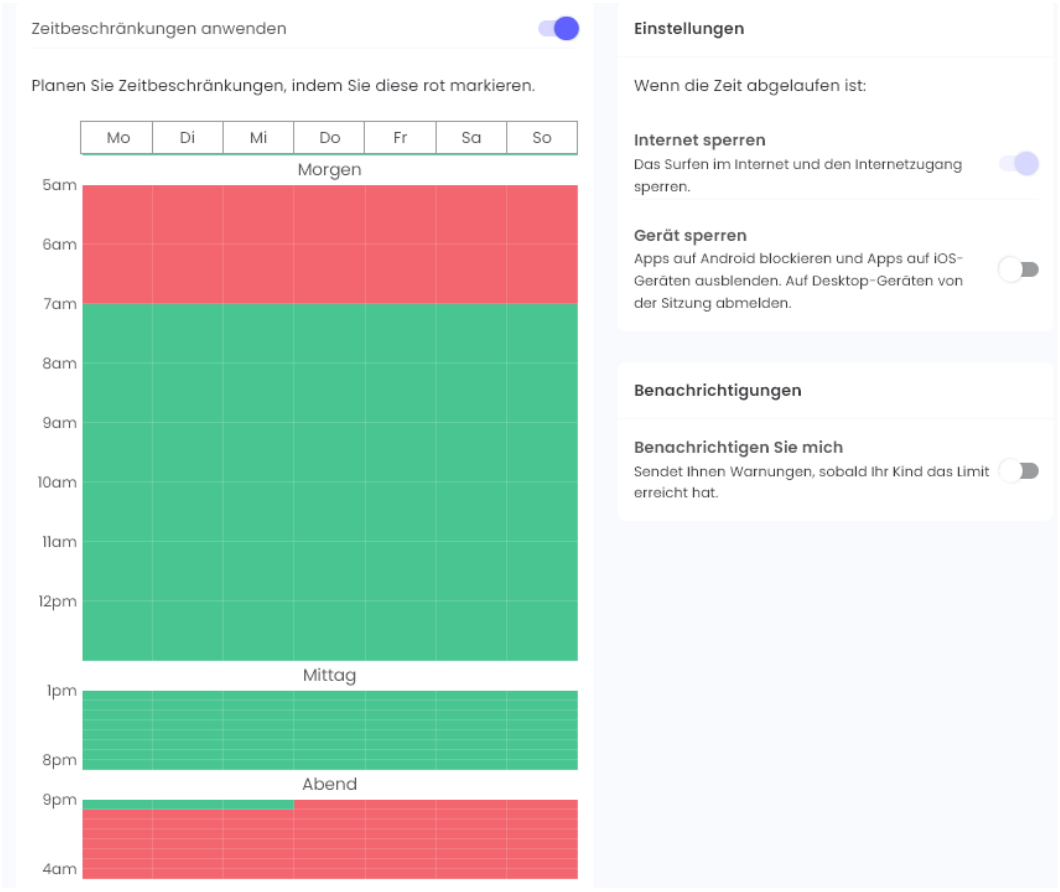
Mit dem Klick auf werden im Portal die Aktivitäten auf dem SuS-Gerät sehr detailliert angezeigt: Welche Seiten besucht wurden, welche Suchbegriffe eingegeben wurden, welche Webseiten blockiert wurden, die Bildschirmzeit …

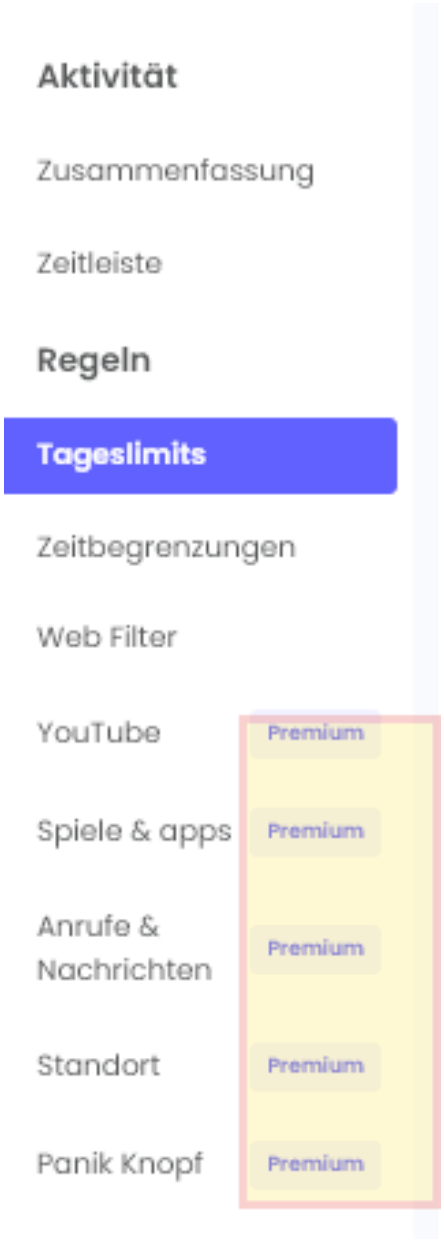




Der Webfilter kann „eingestellt“ werden ..

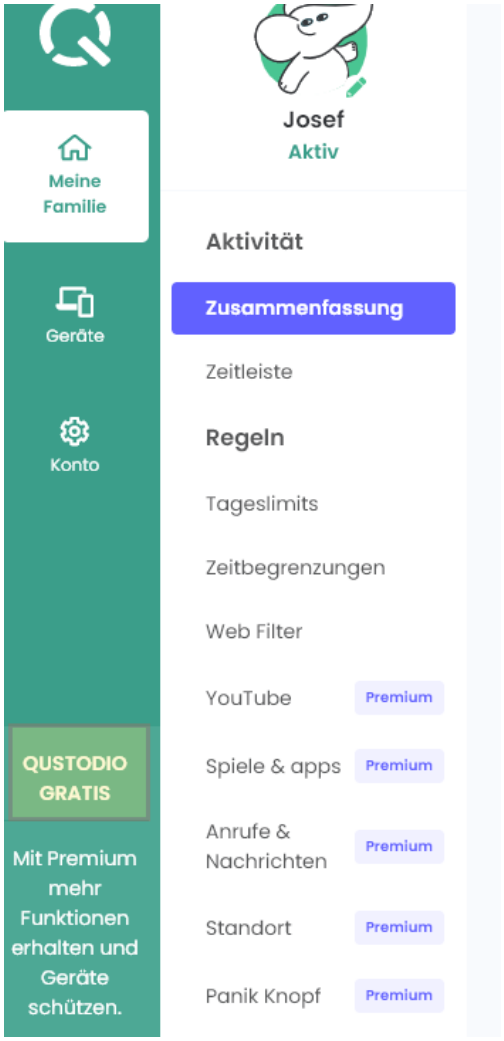
Weiters können Tageslimits (Bildschirmzeitkontingent / Tag) und Zeitbegrenzungen festgelegt werden:





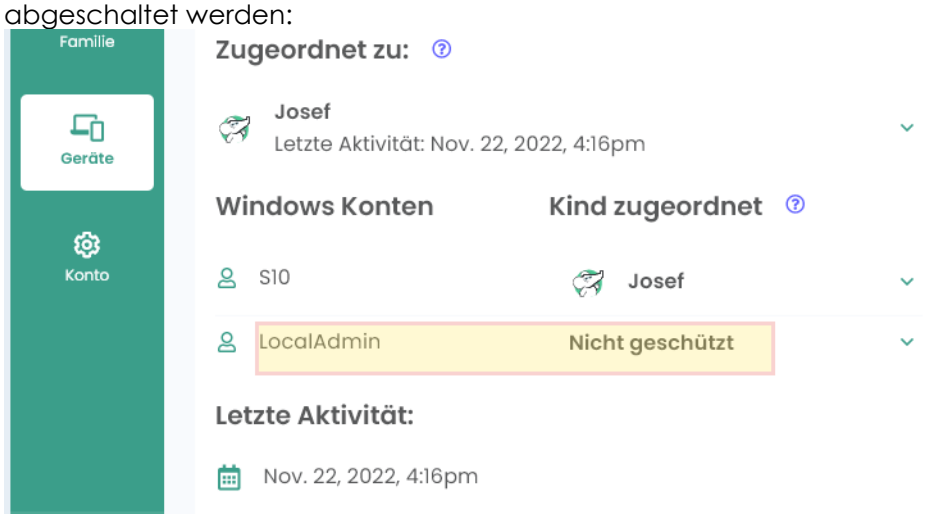
Einige der Funktionen sind der kostenpflichtigen Version von Qustodio vorbehalten.

Nach der Registrierung stehen die Premiumfunktionen drei Tage lang kostenlos zur Verfügung.
Nach drei Tagen wechselt das Programm in den „Gratismodus“.

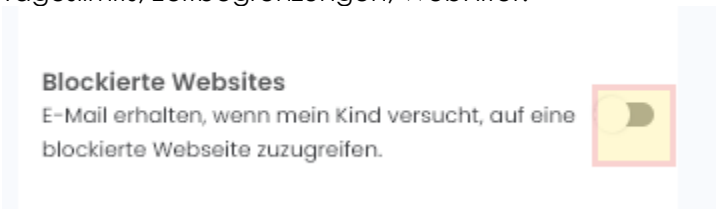


Aber auch im „Gratismodus“ stehen die Grundfunktionen (Webfilter, Tageslimits, Zeitbegrenzung) nach wie vor zur Verfügung und funktionieren.
Weitere Einschränkung im „Gratismodus“: Es kann nur **ein** Gerät überwacht / geschützt werden.

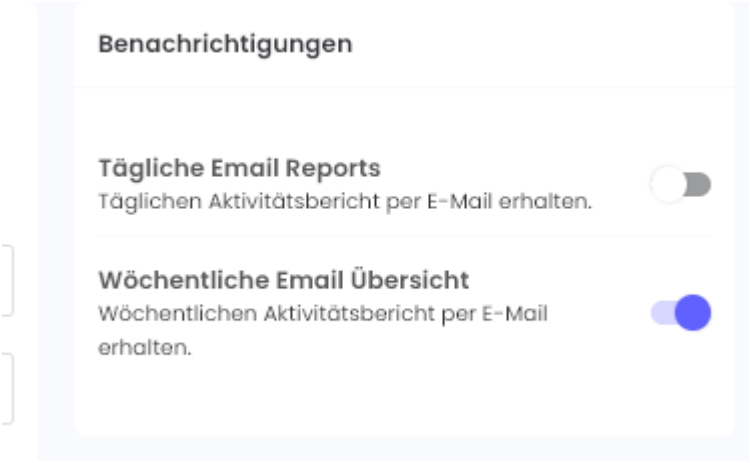
Über den Menüpunkt Geräte kann der Schutz für einzelne Benutzerkonten auf dem Schülergerät abgeschaltet werden:



Emailbenachrichtigung:
An diversen Stellen kann eine Emailbenachrichtigung ein- bzw. ausgeschaltet werden. Die Standardeinstellungen führen u. U. zu ordentlich Mailverkehr. Diese Einstellungen können geändert werden:
Tageslimits, Zeitbegrenzungen, WebFilter:



Konto:



Deinstallation des Programms:
Selbst wenn der Schüler / die Schülerin das Administratorpasswort kennt, ist es nicht ganz so einfach, das Programm „Qustodio“ vom Gerät zu deinstallieren, weil für die Deinstallation die Benutzerdaten des Onlineaccounts der Eltern (siehe Kap 3.1) benötigt werden.