



Webfilter und Kinder-/Jugendschutzsoftware

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

Version 23.01

Inhalt

1.	Grundsätzliches	3
2.	Variante 1 – „nur“ Webfilter über Intune vorgeben	3
3.	Variante 2 – Programm „Qustodio“	10
3.1.	Qustodio – Konto anlegen	10
3.2.	Qustodio – Clientprogramm auf dem Schülergerät installieren	11
4.	Einstellungen und Infos zu „Qustodio“	14

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-Skript 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-Skript“ 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, ob 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.

Erkennungsskript zuordnen:

- 1 Grundeinstellungen 2 **Einstellungen** 3 Bereichstags 4 Zuweisungen 5 Überprüfen + erstellen

i Dieses Skript wird im reinen Erkennungsmodus ausgeführt, weil kein Wartungsskript vorhanden ist.

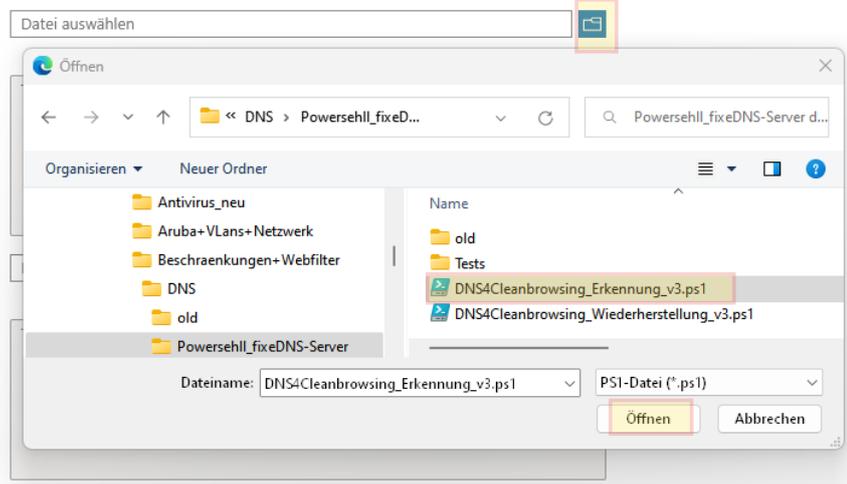
Erstellen Sie ein benutzerdefiniertes Skriptpaket aus Skripts, die Sie geschrieben haben. Standardmäßig werden Skripts täglich auf zugewiesenen Geräten ausgeführt.

Datei mit Erkennungsskript *

Erkennungsskript

Datei mit Bereinigungsskript

Wiederherstellungsskript



Wiederherstellungsskript zuordnen:

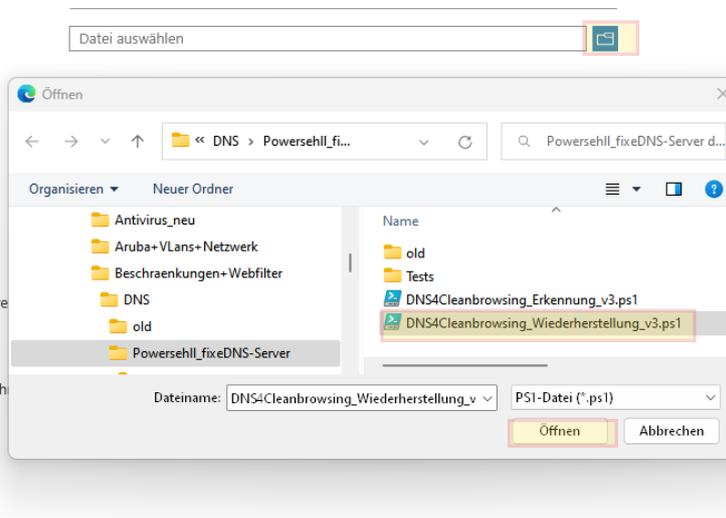
Datei mit Bereinigungsskript

Wiederherstellungsskript

Dieses Skript mit den Anmeldeinformationen des angemeldeten Benutzers ausführen

Skriptsignaturprüfung erzwingen

Skript in 64-Bit-PowerShell ausführen



Zurück

Weiter

Erstellen Sie ein benutzerdefiniertes Skriptpaket aus Skripten, die Sie geschrieben haben. Standardmäßig werden Skripte täglich auf zugewiesenen Geräten ausgeführt.

Datei mit Erkennungsskript *

Erkennungsskript

```

        ># DK 17.02.2023 V3
        # fÄ¼r SuS-GerÄ¼te aus der GerÄ¼teinitiative (Windows)
        # DNS-Serveradressen von cleanbrowsing Ä¼ber Intune fix vorgeben
        # Skript fragt zuerst ab, welches der momentan aktive Netzwerkadapter ist und
        # dann dessen DNS-EintrÄ¼ge
        # Skript gemeinsam mit dem dazu passenden Wiederherstellungsskript
        verwenden: MS Endpoint Manager -> Berichte -> Endpunktanalyse ->
        
```

Datei mit Bereinigungsskript

Wiederherstellungsskript

```

        ># DK 17.02.2023 V3
        # fÄ¼r SuS-GerÄ¼te aus der GerÄ¼teinitiative (Windows)
        # DNS-Serveradressen von cleanbrowsing Ä¼ber Intune fix vorgeben
        # Skript fragt zuerst ab, welches der momentan aktive Netzwerkadapter ist und
        # Ä¼ndert dann dessen DNS-EintrÄ¼ge
        # Skript gemeinsam mit dem dazu passenden Erkennungsskript verwenden: MS
        Endpoint Manager -> Berichte -> Endpunktanalyse -> Proaktive Korrekturen ->
        
```

Dieses Skript mit den Anmeldeinformationen des angemeldeten Benutzers ausföhren Ja Nein

Skriptsignaturprüfung erzwingen Ja Nein

Skript in 64-Bit-PowerShell ausföhren Ja Nein

➔ keine Bereichstags

Der Gerätegruppe zuweisen:

1 Grundeinstellungen
 2 **Einstellungen**
3 **Bereichstags**
4 **Zuweisungen**
5 Überprüfen + erstellen

Wählen Sie mindestens eine Gruppe aus, um das Skriptpaket zuzuweisen.

Eingeschlossene Gruppen

Zuweisen zu

Ausgewählte Gr...	Zeitplan	Filter
Keine Gruppen ausgewählt		
+ Wählen Sie die Gruppen aus, die eingeschlossen werden sollen:		
		<ul style="list-style-type: none"> <input type="checkbox"/> C_mdm_Ring3-Update <input type="checkbox"/> C_N20SuS <input type="checkbox"/> C_N21LuL <input type="checkbox"/> C_N21SuS <input checked="" type="checkbox"/> C_SuS <small>Ausgewählt</small> <input type="checkbox"/> C_test1_BYOD
Ausgewählte Elemente		
		<ul style="list-style-type: none"> <input checked="" type="checkbox"/> C_SuS
Ausgeschlossene Gruppen		
Keine Gruppen ausgeschlossen		
+ Wählen Sie die Gruppen aus, die ausgeschlossen werden sollen:		

Zeitplan einstellen:

Benutzerdefiniertes Skript erstellen

✓ Grundeinstellungen ✓ Einstellungen ✓ Bereichstags **4 Zuweisungen** 5 Überprüfen

Wählen Sie mindestens eine Gruppe aus, um das Skriptpaket zuzuweisen.

Eingeschlossene Gruppen
Zuweisen zu

Ausgewählte Gr...	Zeitplan	Filter	Filtermodus
C_SuS	Täglich	Keine	Keine

+ Wählen Sie die Gruppen aus, die eingeschlossen werden sollen.

Ausgeschlossene Gruppen

i Schließen Sie entweder Gerätegruppen oder Benutzergruppen ein oder aus. Innerhalb von

Zeitplan
Hiermit wird ein Zeitplan für die Ausführung dieses Skripts auf Geräten in der Gruppe "C_SuS" erstellt.

Häufigkeit

Wiederholung alle
 Stund

➔ 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:

[Home](#) > [Berichte](#) | [Endpunktanalyse](#) > [Endpunktanalyse](#) | [Proaktive Korrekturen](#) > [DNS-fixieren4cleanbrowsing_neu](#)

DNS-fixieren4cleanbrowsing_neu | Gerätestatus

Proaktive Korrekturen

Suche <<

Übersicht

Verwalten

Eigenschaften

Überwachen

Gerätestatus

Gerätename	Erkennungsstatus	Wiederherstellungsstatus	Be
22S-01476811005	Mit Problemen	Problem behoben	10
22S-26364710751	Ohne Probleme	Nicht ausgeführt	10
22S-26444110751	Mit Problemen	Problem behoben	10
PC03	Ohne Probleme	Nicht ausgeführt	10

„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](https://www.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
- ➔



Willkommen!
Erstellen Sie Ihr Konto und genießen Sie 3 Tage Premium Funktionen, kostenlos!

Name

Email

Passwort

Ich stimme den Nutzungsbedingungen und der Datenschutzrichtlinie zu.

Registrieren

Benutzen Sie bereits Qustodio? [Anmelden](#)

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

☰ Einrichtung



Los geht's

Fügen Sie Ihr Kind hinzu, damit Sie Regeln festlegen und die Aktivitäten des Kindes überwachen können.

Kind hinzufügen

Kind hinzufügen Gerät hinzufügen Beenden

1 2 3

Geben Sie die Daten Ihres Kindes ein

Name Geburtsjahr Geschlecht

Wählen Sie einen Avatar aus



Weiter



Sehr gut! Fügen wir nun ein Gerät hinzu

Gehen Sie zum Gerät von Max und öffnen Sie den untenstehenden Link in einem Browserfenster.

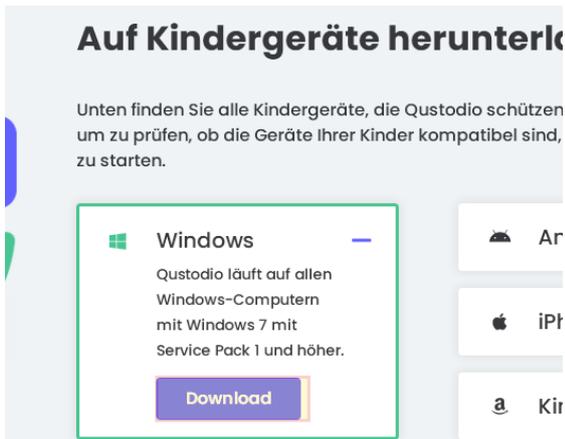
Laden Sie von dort Qustodio herunter und folgen Sie den Anweisungen auf dem Bildschirm.

www.qustodio.com/downloads 

Kommen Sie zurück, wenn die Installation beendet ist.

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



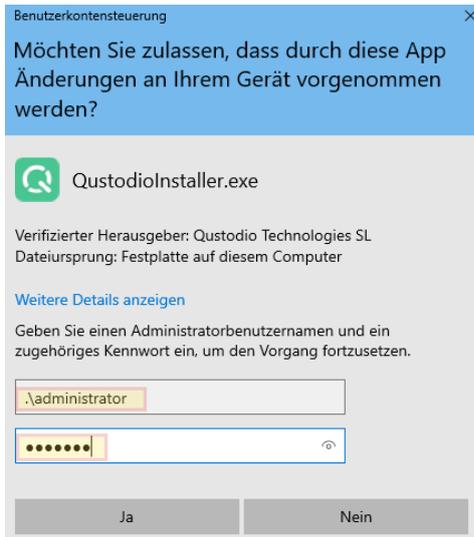
Auf Kindergeräte herunterl

Unten finden Sie alle Kindergeräte, die Qustodio schützen um zu prüfen, ob die Geräte Ihrer Kinder kompatibel sind, zu starten.

- Windows**
Qustodio läuft auf allen Windows-Computern mit Windows 7 mit Service Pack 1 und höher.
[Download](#)
- Android**
- iPad**
- Kinder**

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

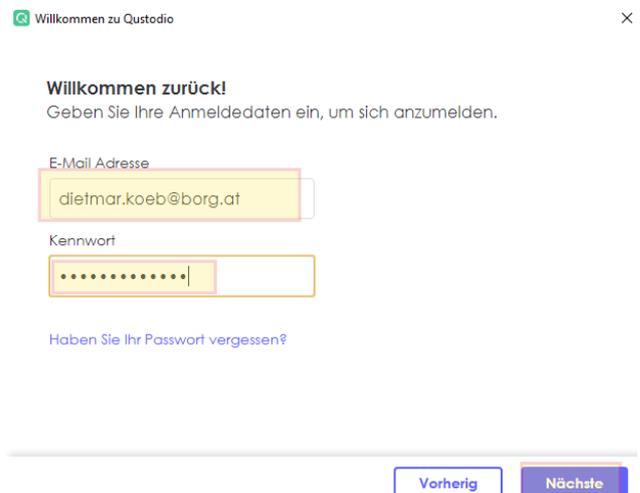
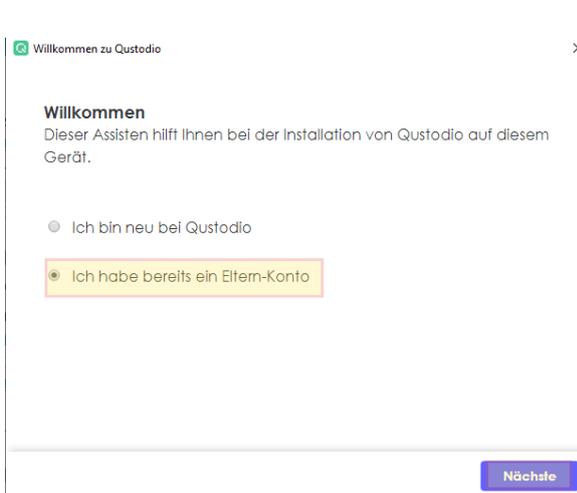
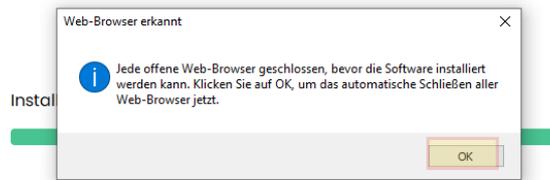
Das heruntergeladene Programm („QustodioInstaller.exe“) wird gestartet und das Programm mit den Standardeinstellungen installiert. Sollte der angemeldete Benutzer keine Administratorrechte haben, dann meldet sich die „Benutzerkontensteuerung“ und es müssen die Administrator-Anmeldedaten eingegeben werden:



Achtung beim Benutzer: .\ voran stellen ...



Qustodio



➔ Logindaten von der Registrierung ([Kap. 3.1](#)) eingeben

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

Geben Sie einen Namen für dieses Gerät ein

Gerätname

22S-01476811005

Qustodio auf diesem Gerät verstecken

Klicken Sie diesen Box ein, wenn Sie den Benutzer nicht erlauben möchten, Qustodio auf diesem Gerät zu sehen.

Nächste

Willkommen zu Qustodio

Wer benutzt dieses Gerät?



Max



Neuen Nutzer hinzufügen



Fertig!

Dieses Gerät ist jetzt durch Qustodio geschützt.

Beenden

Benachrichtigungen verwalten

Qustodio Tray Application



Qustodio Schutz-Service

Das Schutz-Service ist aktiviert und überwacht aktiv Ihrer alltäglichen Arbeit, um mehr Sicherheit zu gewährleisten.

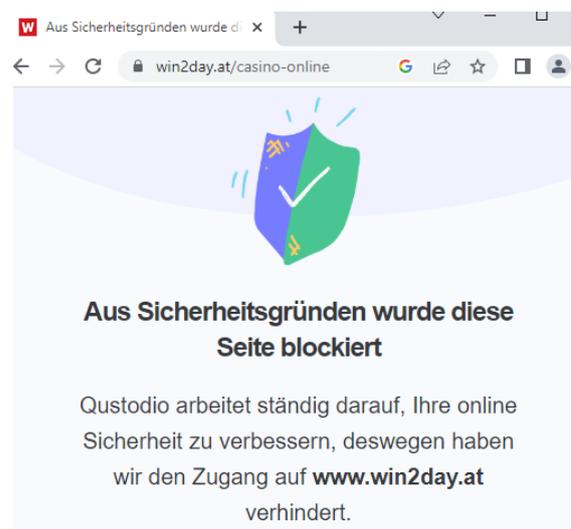
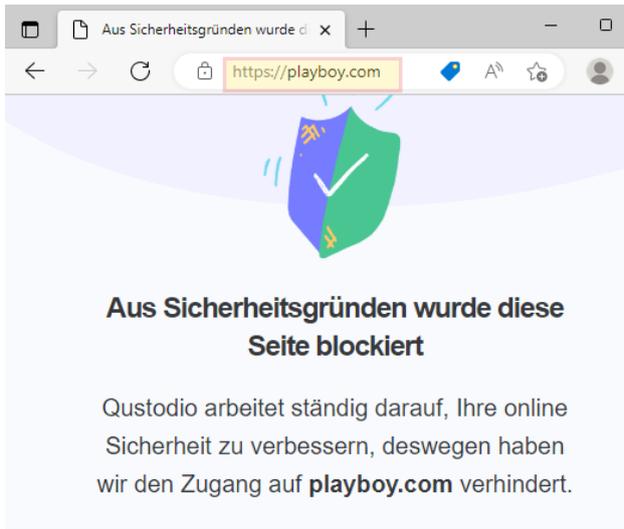
15:26

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

The screenshot shows the Qustodio online account interface. On the left is a green sidebar with icons for 'Meine Familie', 'Geräte', and 'Konto'. The main area is titled 'Meine Familie' and features a yellow banner for a 'Premium Test - 3 Tage verbleiben. Upgraden'. Below the banner, there is a user profile for 'Max' with a pig icon and the status 'Aktiv'. To the right of the profile is a blue circular button with a plus sign and the text 'Kind hinzufügen'.

... und der Schutz ist aktiviert.

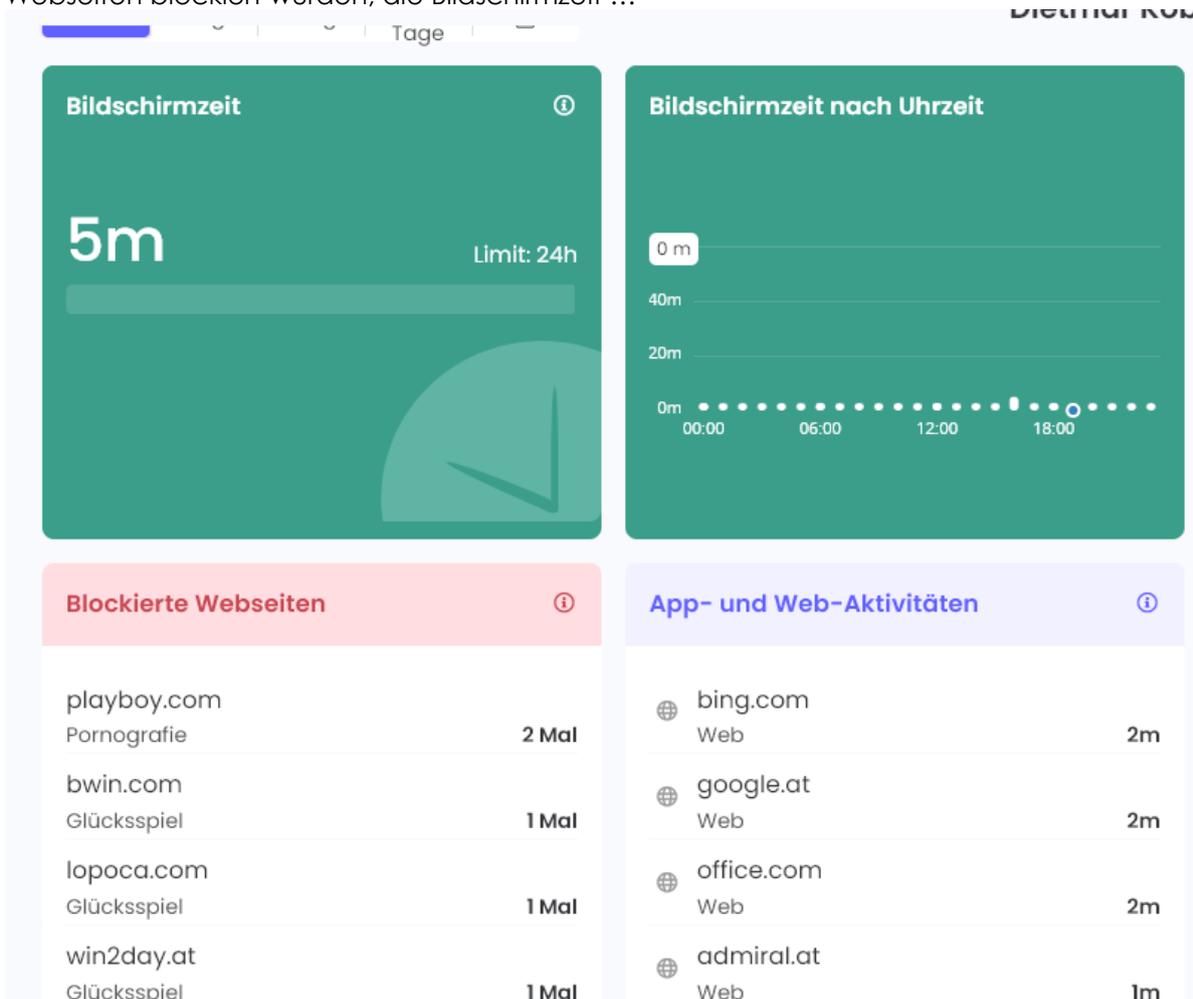
Auf dem Schülergerät werden entsprechende Webseiten (egal, mit welchem Browser sie geöffnet werden) geblockt:



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 ...



- Shopping ...
- Arbeit ...
- Webmail ...
- Forums ...
- Soziale Netzwerke ...
- Chat ...
- Teilen von Dateien ...
- Glücksspiel ...
- Proxies/Schlupflöcher ...
- Gewalt ...
- Waffen ...
- Obszönitäten ...
- nicht jugendfreie Inhalte ...
- Pornografie ...
- Alkohol ...
- Drogen ...
- Tabak ...

Der Webfilter kann „eingestellt“ werden ..

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

Zeitbeschränkungen anwenden

Planen Sie Zeitbeschränkungen, indem Sie diese rot markieren.

	Mo	Di	Mi	Do	Fr	Sa	So
Morgen							
5am							
6am							
7am							
8am							
9am							
10am							
11am							
12pm							
Mittag							
1pm							
8pm							
Abend							
9pm							
4am							

Einstellungen

Wenn die Zeit abgelaufen ist:

Internet sperren
Das Surfen im Internet und den Internetzugang sperren.

Gerät sperren
Apps auf Android blockieren und Apps auf iOS-Geräten ausblenden. Auf Desktop-Geräten von der Sitzung abmelden.

Benachrichtigungen

Benachrichtigen Sie mich
Sendet Ihnen Warnungen, sobald Ihr Kind das Limit erreicht hat.

Aktivität

Zusammenfassung

Zeitleiste

Regeln

Tageslimits

Zeitbegrenzungen

Web Filter

YouTube

Premium

Spiele & apps

Premium

Anrufe &
Nachrichten

Premium

Standort

Premium

Panik Knopf

Premium

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“.

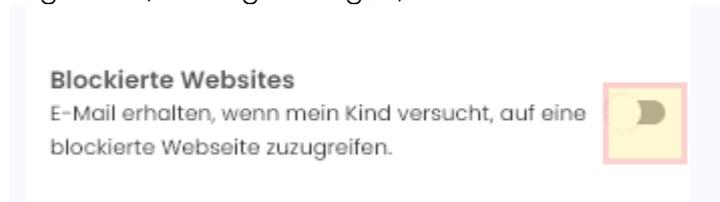
Aber auch im „Gratismodus“ stehen die Grundfunktionen (Webfilter, Tageslimits, Zeitbegrenzung) nach wie vor zur Verfügung und funktionieren.
 Weitere Einschränkung im „Gratismodus“: Es kann nur **ein** Gerät überwacht / geschützt werden.

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

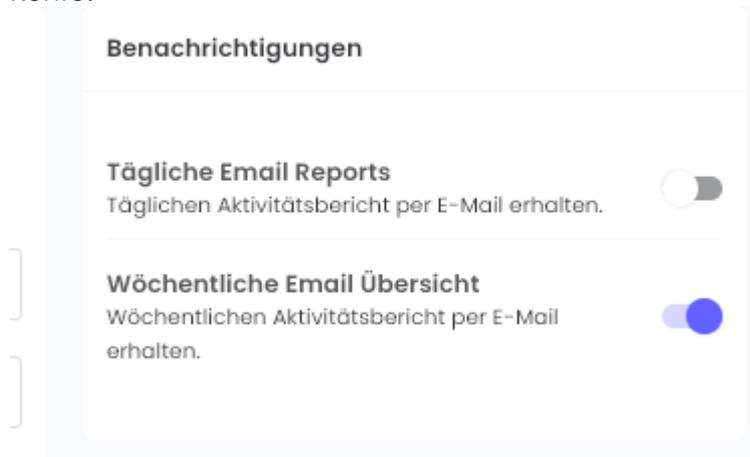
Emailbenachrichtigung:

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.