

WEBFILTER UND KINDER-/ JUGENDSCHUTZSOFTWARE - WINDOWS-TABLETS AUS DER GERÄTEINITIATIVE ABSICHERN - EMPFEHLUNG FÜR ELTERN/ ERZIEHUNGSBERECHTIGTE

Vorarlberger Standardschulinstallation
Verfasser: Dietmar Köb

© 2022 IT-Regionalbetreuer Vorarlberg
6900 Bregenz, Römerstraße 14
Alle Rechte vorbehalten

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 als benutzerdefiniertes Skript, das neben dem „Hauptskript“ auch noch ein weiteres, das so genanntes "Erkennungsskript" („Detection-Script“) zugeordnet bekommt.

Inhalt des ersten Skripts (=Erkennungsskript):

```
# DK 17.02.2026 V5 (Update für IPv6 Stabilität)
# für SuS-Geräte aus der Geräteinitiative (Windows)
# DNS-Serveradressen von cleanbrowsing (Family Filter) über Intune prüfen
# Skript prüft IPv4 UND IPv6 auf den aktiven Adaptern
#=====

$activeAdapter = Get-NetIPInterface | Where-Object { $_.ConnectionState -eq
"Connected" -and $_.InterfaceAlias -notmatch "Loopback|vEthernet|Pseudo" } |
Sort-Object InterfaceMetric | Select-Object -First 1

if ($null -eq $activeAdapter) {
    Write-Host "Kein aktiver Netzwerkadapter mit Internetverbindung gefunden."
    exit 0
}

$DNSv4 = (Get-DnsClientServerAddress -InterfaceIndex
$activeAdapter.InterfaceIndex -AddressFamily IPv4).ServerAddresses
$DNSv6 = (Get-DnsClientServerAddress -InterfaceIndex
$activeAdapter.InterfaceIndex -AddressFamily IPv6).ServerAddresses

$TargetIPv4Primary = "185.228.168.168"
$TargetIPv4Secondary = "185.228.169.168"
$TargetIPv6Primary = "2a0d:2a00:1::"
$TargetIPv6Secondary = "2a0d:2a00:2::"

$v4Passt = $false
if ($DNSv4 -contains $TargetIPv4Primary -or $DNSv4 -contains
$TargetIPv4Secondary) {
    $v4Passt = $true
}

$v6Passt = $true
```

```

if ($null -ne $DNSv6 -and $DNSv6.Count -gt 0) {
    if ($DNSv6 -contains $TargetIPv6Primary -or $DNSv6 -contains
$TargetIPv6Secondary) {
        $v6Passt = $true
    } else {
        $v6Passt = $false
    }
}

Try {
    if ($v4Passt -and $v6Passt) {
        Write-Host "Compliance erfüllt: CleanBrowsing DNS ist korrekt
konfiguriert."
        exit 0
    }
    else {
        Write-Host "Compliance nicht erfüllt."
        Write-Host "Adapter: $($activeAdapter.InterfaceAlias)"
        Write-Host "IPv4 vorhanden: $($DNSv4 -join ', ' ) (Status: $v4Passt)"
        Write-Host "IPv6 vorhanden: $($DNSv6 -join ', ' ) (Status: $v6Passt)"
        exit 1
    }
}
Catch {
    Write-Warning $_
    exit 1
}

```

Codezeilen in Textdatei kopieren und z. B. mit Dateinamen
DNS4Cleanbrowsing_Erkennung_v5.ps1 abspeichern.

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 (=Bereinigungsskript):

```

# # DK 17.02.2026 V5 (Update für IPv6 Stabilität)
# für SuS-Geräte aus der Geräteinitiative (Windows)
# DNS-Serveradressen von cleanbrowsing über Intune fix vorgeben
# Skript fragt zuerst ab, welche Netzwerkadapter momentan aktiv sind und ändert
deren DNS-Einträge (IP-V4 und IP-V6)
# Skript gemeinsam mit dem dazu passenden Erkennungsskript verwenden: MS Intune
Admin Center -> Geräte -> Skripts und Wartungen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausführen aktivieren -> Zeitplan auswählen
(stündlich) -> der Schülergerätegruppe (zB C_SUS) zuordnen
#=====

```

```

# Variablen definieren (CleanBrowsing Family Filter)
$dnsV4 = @("185.228.168.168", "185.228.169.168")
$dnsV6 = @("2a0d:2a00:1::", "2a0d:2a00:2::")
$allDns = $dnsV4 + $dnsV6

#=====
=====
[Console]::OutputEncoding = [System.Text.Encoding]::GetEncoding(1252)

Clear-DnsClientCache
Write-Host "DNS-Auflösungscache wurde geleert." -ForegroundColor Cyan

$activeAdapters = Get-NetAdapter | Where-Object { $_.Status -eq "up" }

if ($activeAdapters) {
    foreach ($adapter in $activeAdapters) {
        Write-Host "Bearbeite Adapter: $($adapter.Name) (Index: $
($adapter.ifIndex))" -ForegroundColor Green

        try {
            Set-DnsClientServerAddress -InterfaceIndex $adapter.ifIndex -
ServerAddresses $allDns -ErrorAction Stop
            Write-Host " -> DNS-Einträge für CleanBrowsing wurden gesetzt." -
ForegroundColor Gray
        }
        catch {
            Write-Warning " -> Fehler bei Adapter $($adapter.Name): $
($_.Exception.Message)"
        }
    }
}
else {
    Write-Host "Keine aktiven Netzwerkverbindungen gefunden." -ForegroundColor
Yellow
}

Clear-DnsClientCache
Write-Host "Vorgang abgeschlossen." -ForegroundColor Cyan

exit 0

```

Codezeilen in Textdatei kopieren und z. B. mit Dateinamen
DNS4Cleanbrowsing_Wiederherstellung_v5.ps1 abspeichern.

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: Geräte -> Skripts und Wartungen -> "Erstellen"

Microsoft Intune Admin Center

Home > Geräte

Geräte | Skripts und Wartungen

Suche

- Windows 365
- Registrierung
- Geräte verwalten
 - Konfiguration
 - Kompatibilität
 - Bedingter Zugriff
 - Skripts und Wartungen**
 - Analyse von Gruppenrichtlinien
 - eSIM-Mobilfunkprofile (Vorschau)

Wartungen Plattformskripts

Erstellen Sie Skriptpakete auf Geräten und führen Sie sie aus, um die wichtigste Organisation proaktiv zu finden und zu beheben. Verwenden Sie diese Tal bereitgestellten Skriptpakete anzuzeigen und die Erkennungs- und Wiede überwachen. Die Ergebnisse werden als Anzahl der betroffenen Geräte an

+ Erstellen Aktualisieren Exportieren Spalten

Suchen Filter hinzufügen

Skriptpaketname	Autor	Status

Benutzerdefiniertes Skript erstellen

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

Erstellen Sie ein neues benutzerdefiniertes Skriptpaket aus von Ihnen geschriebenen Skripts für Erkennung und Wartung.

Name * DNS-fixieren4cleanbrowsing ✓

Beschreibung

Stellt die beiden DNS-Einträge um auf den Family-Filter von cleanbrowsing.org:
185.228.168.168
185.228.169.168
Das Skript kontrolliert ca. jede Stunde, ob die Einträge oben stimmen
(=Erkennungsskript) und wenn nicht, wird das Wiederherstellungsskript ausgeführt,
das diese Einträge macht.

Herausgeber Admin Borg Egg

Version 1

Zurück Weiter

Erkennungsskript zuordnen:

Benutzerdefiniertes Skript erstellen ...

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

Datei auswählen

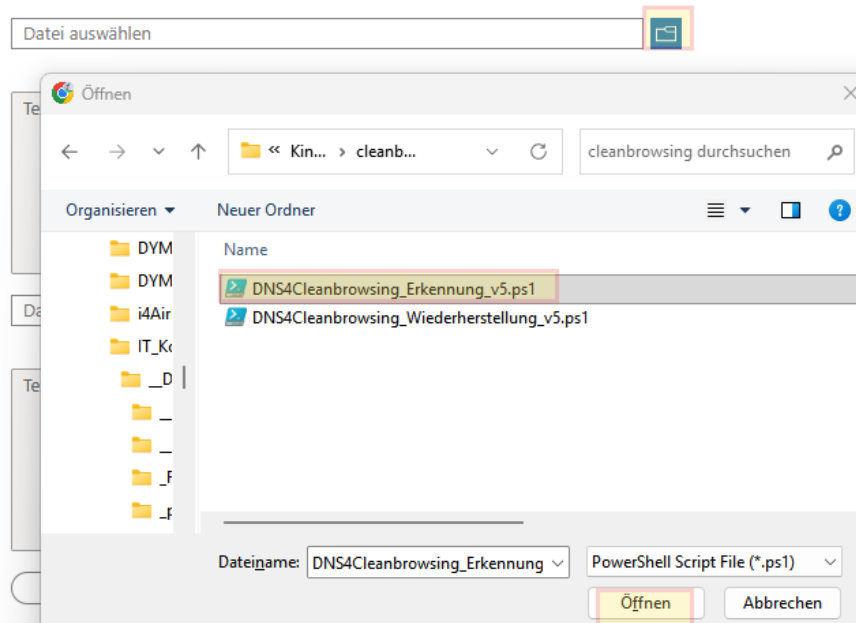


Erkennungsskript

Datei mit Bereinigungsskript

Wiederherstellungsskript

Dieses Skript mit den
Anmeldeinformationen des ...



Bereinigungsskript zuordnen:

Benutzerdefiniertes Skript erstellen ...

- ✓ Grundeinstellungen
2 Einstellungen
3 Bereichstags
4 Zuweisungen
5 Überprüfen und 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 *

DNS4Cleanbrowsing_Erkennung_v5.ps1

Erkennungsskript

```
# DK 17.02.2026 V5 (Update für IPv6 Stabilität)
# für SuS-Geräte aus der Geräteinitiative (Windows)
# DNS-Serveradressen von cleanbrowsing (Family Filter) über Intune prüfen
# Skript prüft IPv4 UND IPv6 auf den aktiven Adaptern
#=====
=====
```

Datei mit Bereinigungsskript

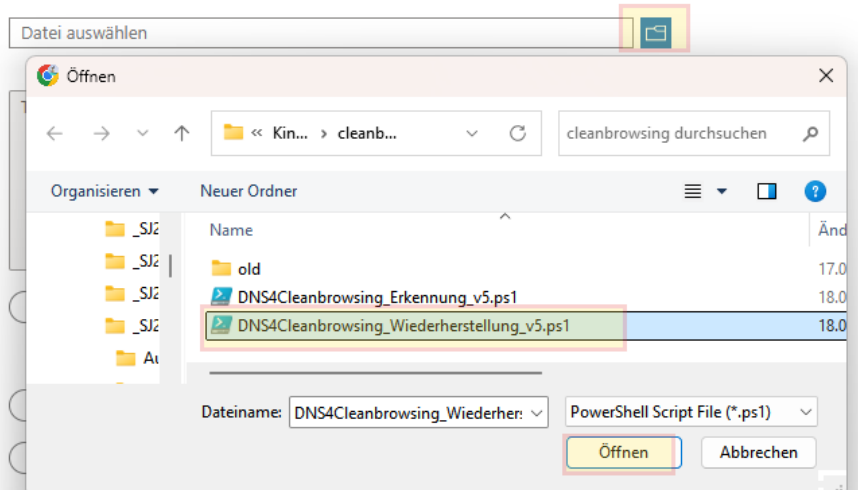
Datei auswählen

Wiederherstellungsskript

Dieses Skript mit den
Anmeldeinformationen des
angemeldeten Benutzers ausführen

Skriptsignaturprüfung erzwingen

Skript in 64-Bit-PowerShell ausführen



Bearbeiten: DNS-fixieren4cleanbrowsing ...

1 Einstellungen **2** Überprüfen und speichern

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

Datei mit Erkennungsskript 

Erkennungsskript

```
# DK 17.02.2026 V5 (Update für IPv6 Stabilität)
# für SuS-Geräte aus der Geräteinitiative (Windows)
# DNS-Serveradressen von cleanbrowsing (Family Filter) über Intune prüfen
# Skript prüft IPv4 UND IPv6 auf den aktiven Adaptern
#=====
=====
```

Datei mit Bereinigungsskript 

Wiederherstellungsskript

```
# # DK 17.02.2026 V5 (Update für IPv6 Stabilität)
# für SuS-Geräte aus der Geräteinitiative (Windows)
# DNS-Serveradressen von cleanbrowsing über Intune fix vorgeben
# Skript fragt zuerst ab, welche Netzwerkadapter momentan aktiv sind und
  ändert deren DNS-Einträge (IP-V4 und IP-V6)
# Skript gemeinsam mit dem dazu passenden Erkennungsskript verwenden: MS
  Intune Admin Center -> Geräte -> Skripts und Wartungen -> Skriptpaket
```

Dieses Skript mit den ☐ Ja ☒ Nein

Anmeldeinformationen des
angemeldeten Benutzers ausführen

Skriptsignaturprüfung erzwingen ☐ Ja ☒ Nein

Skript in 64-Bit-PowerShell ausführen ☒ Ja ☐ Nein

--> keine Bereichstags

Der Gerätegruppe zuweisen:

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 Gruppen

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

Zurück

Weiter

Zeitplan

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

Häufigkeit

Stündlich

Wiederholung alle

1

Stund

Anwenden

Zurücksetzen

--> 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

Aktualisieren Spalten Exportieren

Übersicht

Verwalten

Eigenschaften

Überwachen

Gerätestatus

Nach Gerätenamen suchen

Wiederherstellungsstatus: 0 ausgewählt

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

Dietmar Köb



Email

dietmar.koeb@borg.at

Passwort

.....

☒ Ich stimme den [Nutzungsbedingungen](#) und der [Datenschutzrichtlinie](#) zu.

Registrieren

Benutzen Sie bereits Qustodio? [Anmelden](#)

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



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

Max

2011



Junge



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



Ar



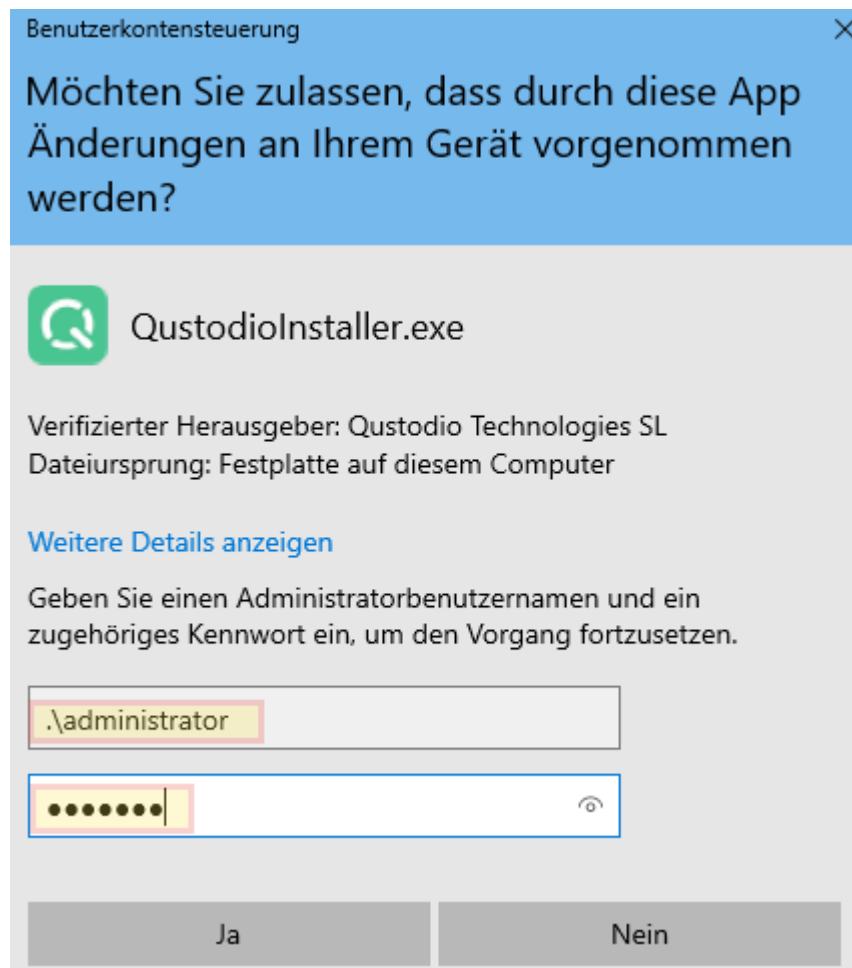
iP



Kir

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 ...

Willkommen bei Qustodio!

Installieren Sie Qustodio und schützen Sie dieses Gerät.

Indem Sie fortfahren, erklären Sie, dass Sie unsere [Allgemeinen Geschäftsbedingungen](#) gelesen haben und akzeptieren.

Abbrechen

Akzeptieren und Installieren

Qustodio

Instal

Web-Browser erkannt



Jede offene Web-Browser geschlossen, bevor die Software installiert werden kann. Klicken Sie auf OK, um das automatische Schließen aller Web-Browser jetzt.

OK

Willkommen

Dieser Assistent hilft Ihnen bei der Installation von Qustodio auf diesem Gerät.

☐ Ich bin neu bei Qustodio

☒ Ich habe bereits ein Eltern-Konto

Nächste

Willkommen zurück!

Geben Sie Ihre Anmeldedaten ein, um sich anzumelden.

E-Mail Adresse

dietmar.koeb@borg.at

Kennwort

.....

[Haben Sie Ihr Passwort vergessen?](#)

Vorherig

Nächste

--> 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

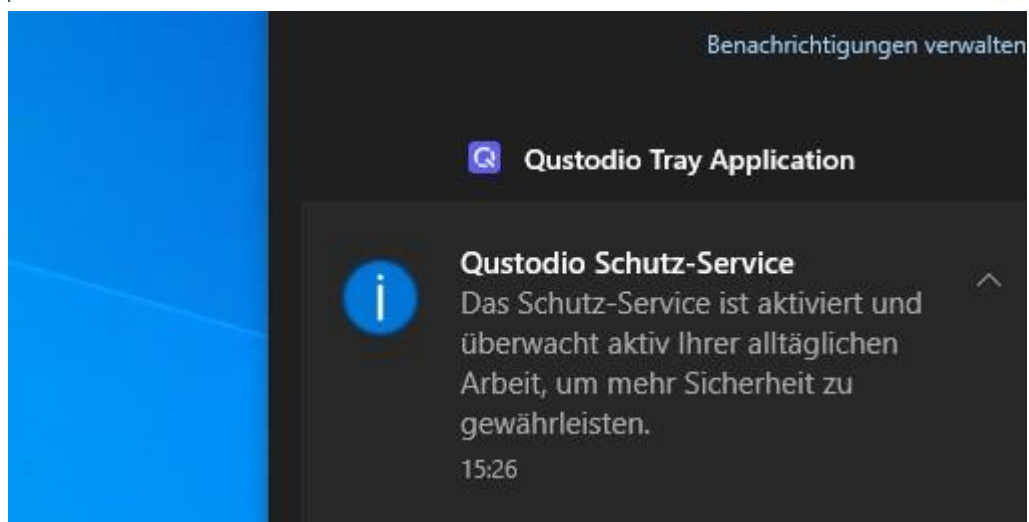




Fertig!

Dieses Gerät ist jetzt durch Qustodio geschützt.

Beenden

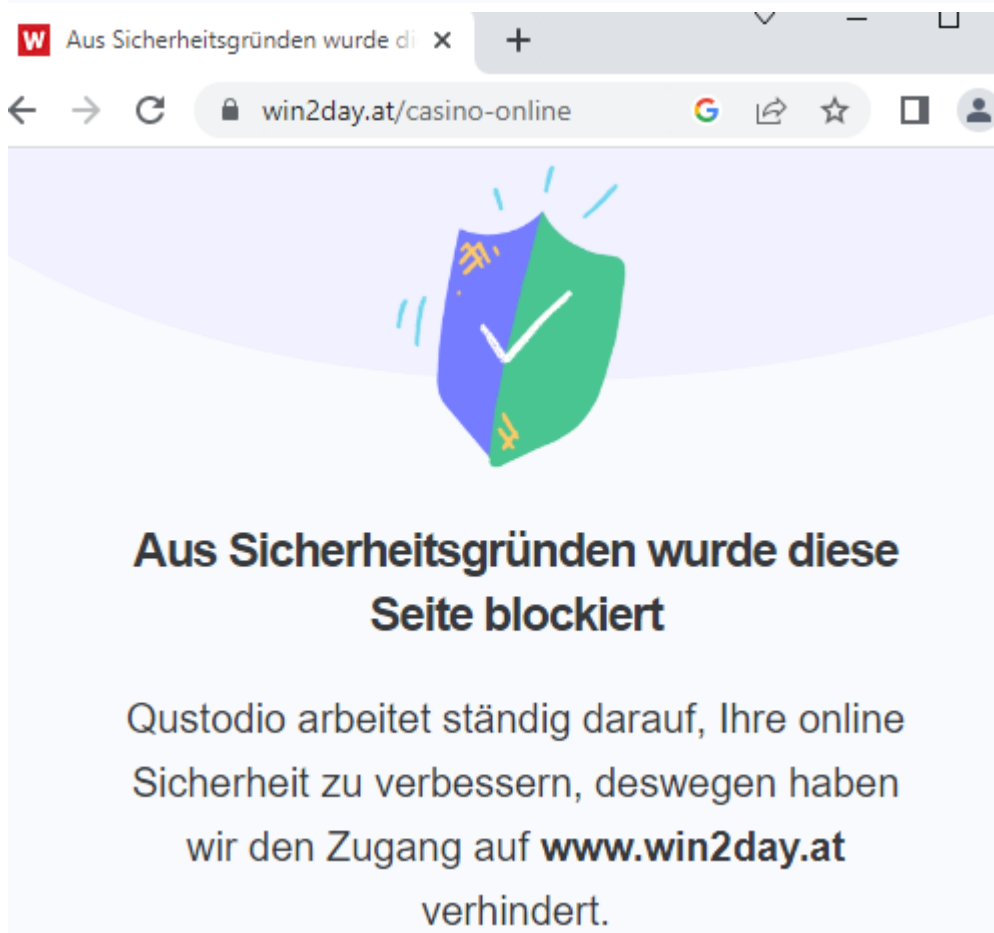
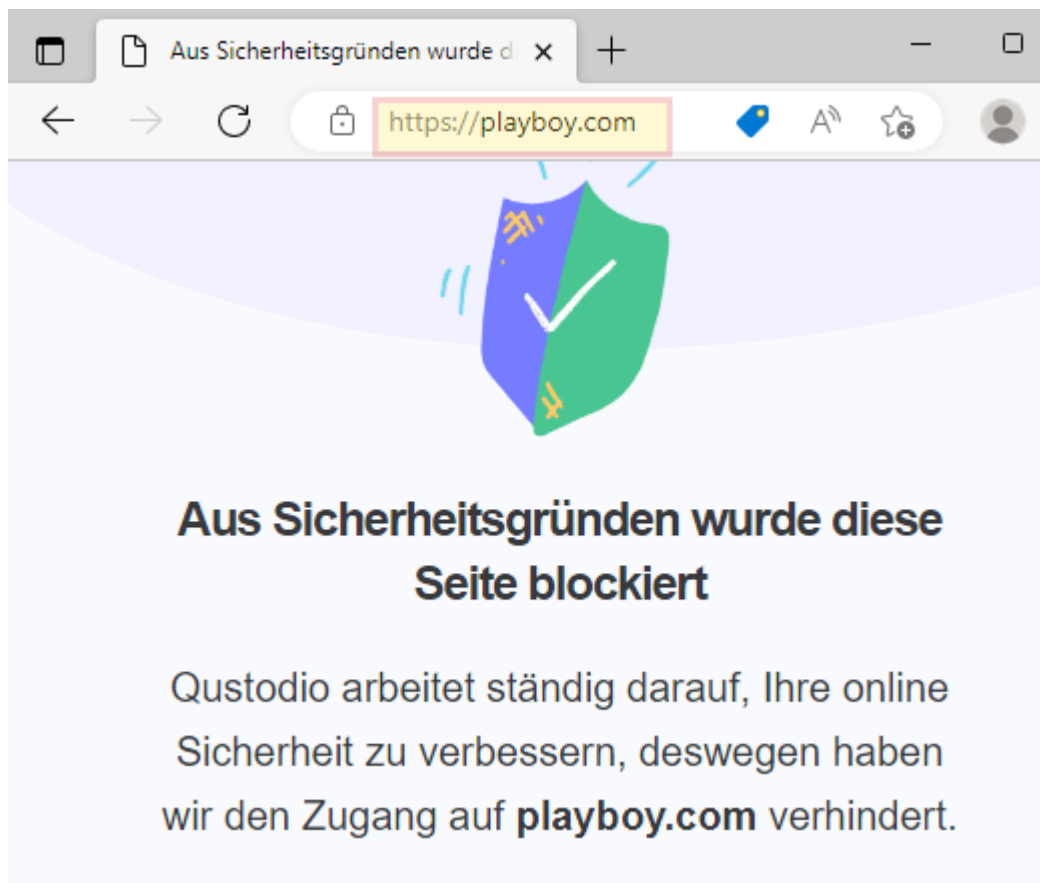


Nach Abschluss der Installation erscheint das Gerät im Qustodio-Onlineaccount:



... und der Schutz ist aktiviert.

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

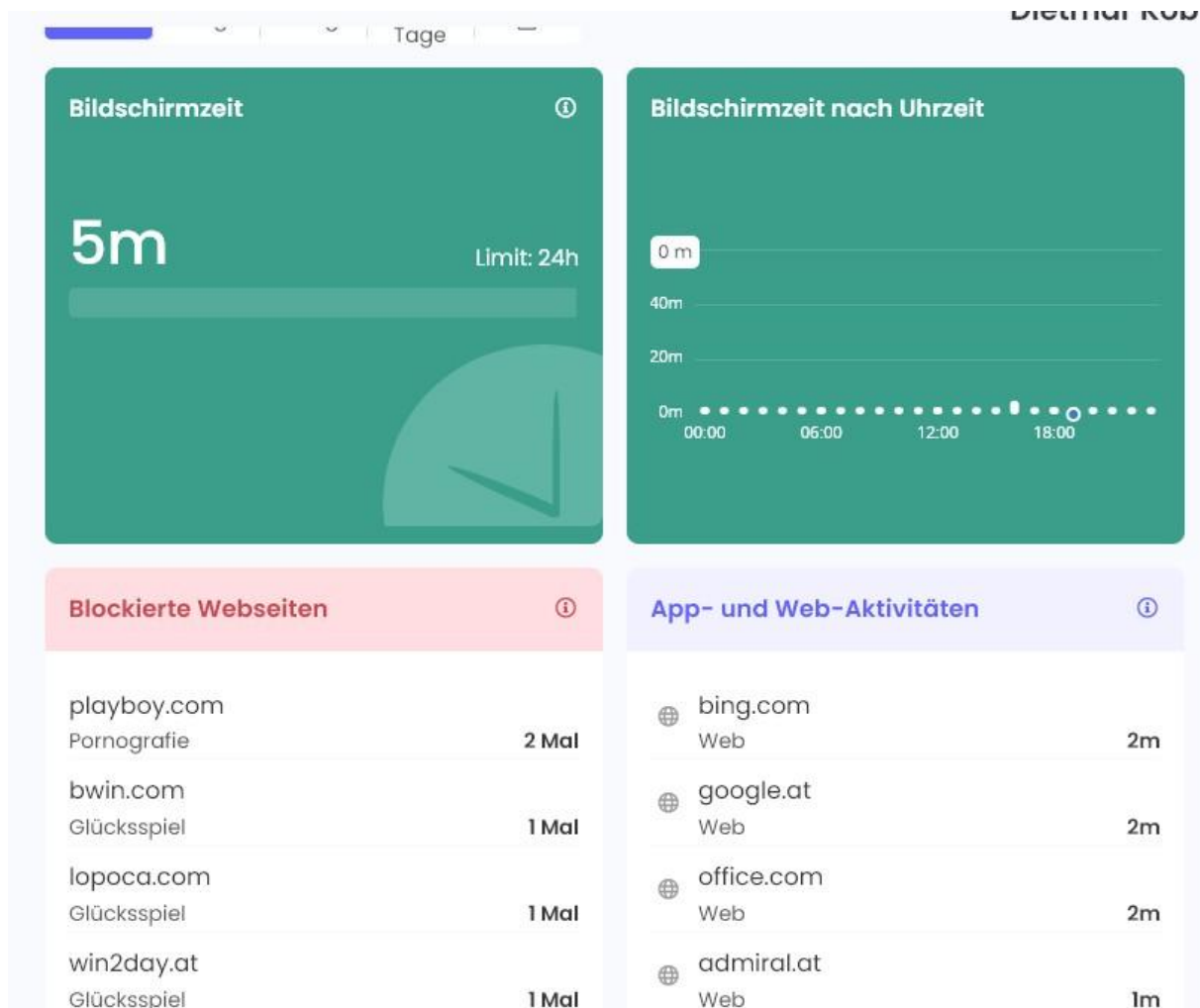


4. Einstellungen und Infos zu „Qustodio“



Max

Mit dem Klick auf **Aktiv** 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	...

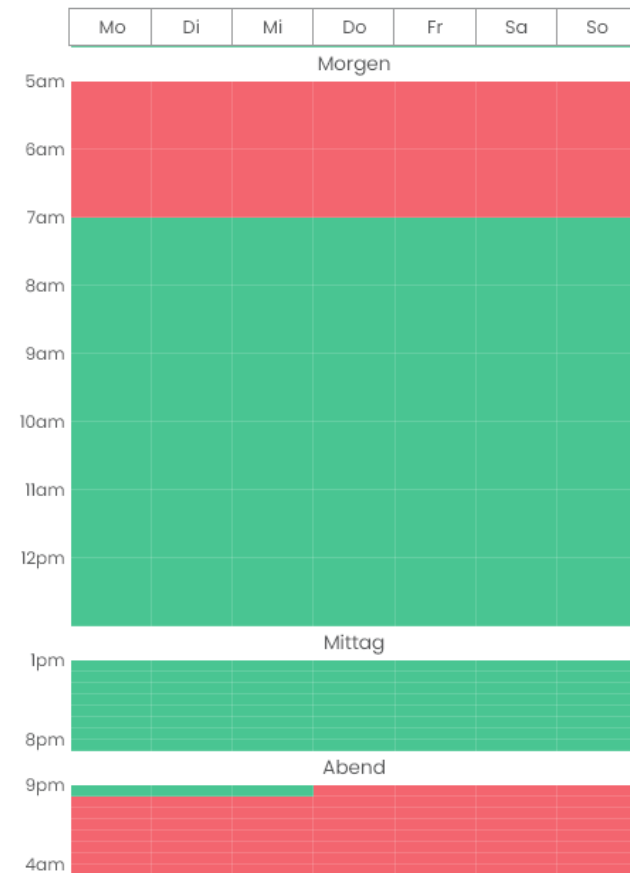
Der Webfilter kann „eingestellt“ werden ..

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

Zeitbeschränkungen anwenden



Planen Sie Zeitbeschränkungen, indem Sie diese rot markieren.



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

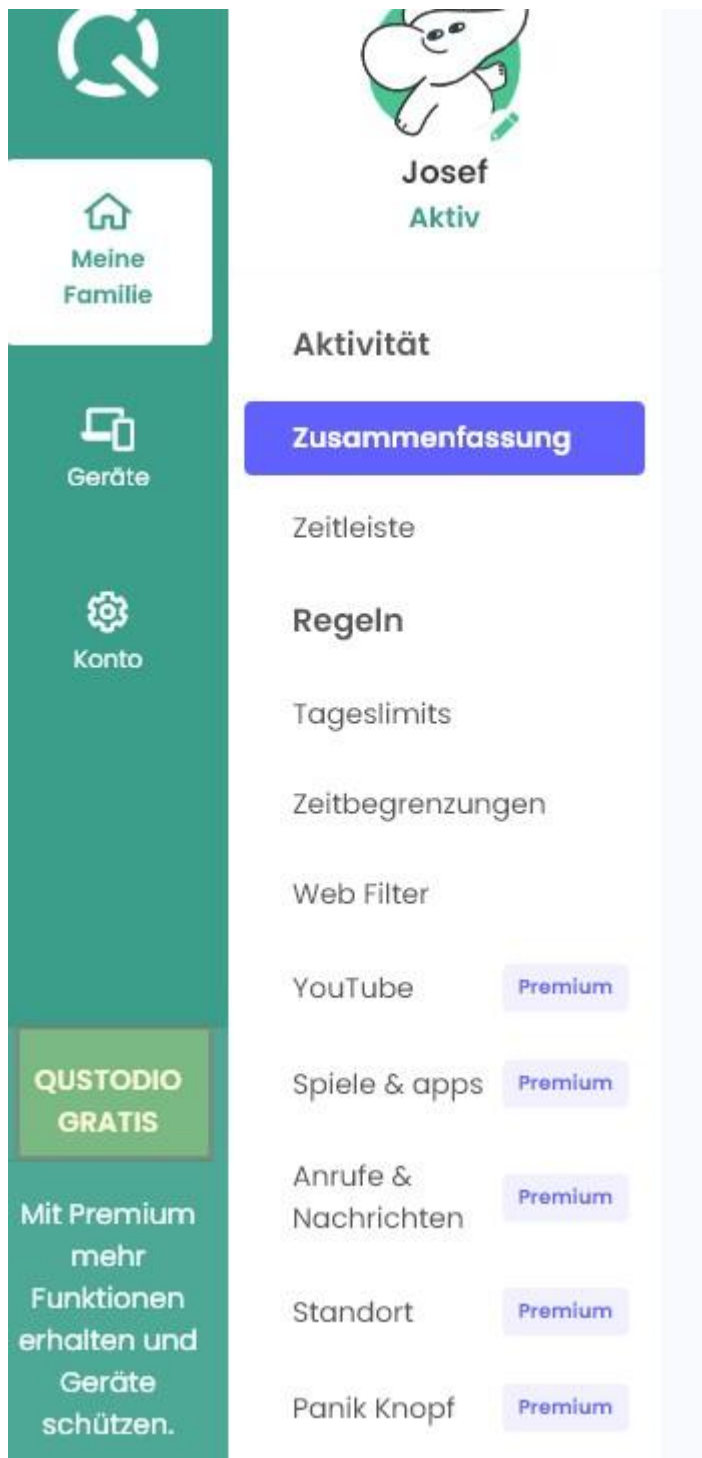
Benachrichtigen Sie mich

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

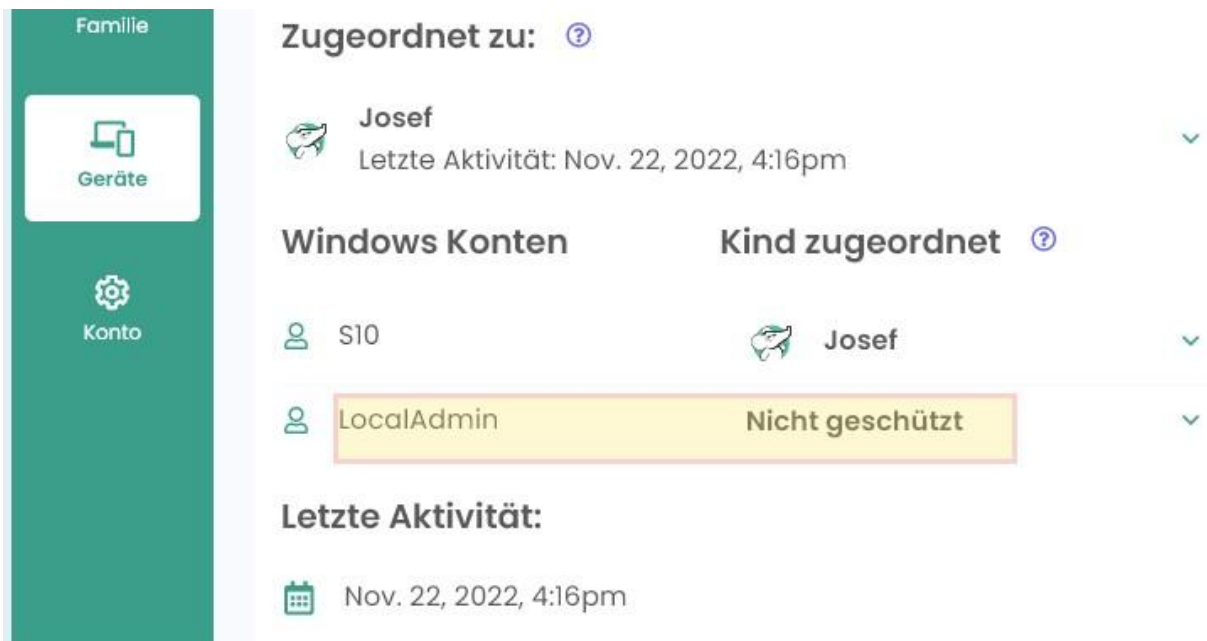
Einige der Funktionen sind der kostenpflichtigen Version von Qustodio vorbehalten. Nach der Registrierung stehen die Premiumfunktionen drei Tage lang kostenlos zur Verfügung. Nach drei Tagen wechselt das Programm in den „Gratismodus“.



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.

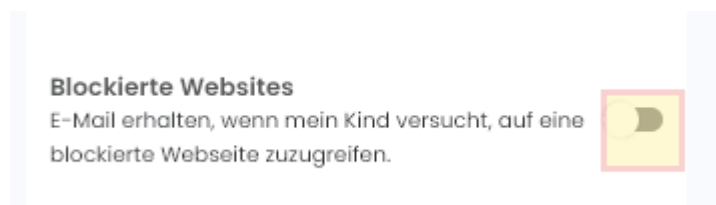
Über den Menüpunkt Geräte kann der Schutz für einzelne Benutzerkonten auf dem Schülergerät abgeschaltet werden:



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.

★Erstellt: 2025-11-14 09:26:21 UTC von Stephan Reiter

✎Zuletzt aktualisiert: 2026-02-18 15:47:19 UTC von dkoeb