

Bring your own device per App

How to für paedML® Windows

OctoGate
EINFACH. SICHER. GESCHÜTZT.

Version 1.5

Versionshistorie

Datum	Person / Abt.	Version	Kommentar
30.11.2018	Vertrieb	1.0	Initial
04.12.2018	Vertrieb	1.1	Korrektur OctoGate Konfig
21.01.2019	Vertrieb	1.2	Ergänzung Linkliste
29.01.2019	Vertrieb	1.3	Korrektur Linkliste
28.02.2019	Vertrieb	1.4	De-Installation von Zertifikaten
04.03.2019	Vertrieb	1.5	Fehlerbehebung Android

OctoGate IT Security Systems GmbH, Friedrich-List-Str. 42
33100 Paderborn

Tel.: +49 5251 18040 0
Fax: +49 5251 18040 39
Email: info@octogate.de
Internet: www.octogate.de

Inhalt

1	Einleitung.....	4
2	Systemvoraussetzungen.....	5
3	Einstellungen auf der OctoGate.....	6
4	Installation der App.....	7
5	Installation von Stammzertifikaten.....	8
6	Konfigurationseinstellungen Apple.....	9
7	Problembehebung unter Android.....	11
8	Steuerung über die Schulkonsole.....	12
9	App-Einstellungen über OctoGate Central.....	13
10	Linkliste für paedML® Windows MySite.....	16
	Anlage 1: De-Installation von Stammzertifikaten.....	17
	Anlage 2: De-Installation der Android-App.....	23

1 Einleitung

Die aktuellen Pläne des „Digitalpakts Schule“ der Kultusminister sehen unter anderem den Einsatz privater mobiler Endgeräte an Schulen vor. Das Modell „Bring your own device“ (BYOD) umfasst im Wesentlichen Laptops, Notebooks, Smartphones oder Tablets von Lehrern und / oder Schülern.

Bisher wurde der Zugang zum WLAN Gästernetz meistens über Voucher Codes gewährt und führte häufig zu Problemen mit Stammzertifikaten, welche auf den Endgeräten installiert werden mussten, um https-Seiten öffnen zu können. Darüber hinaus war eine Internetsteuerung der mobilen Geräte über die Konsole der paedML® Windows nicht möglich, weshalb private Tablets & Co. im Unterricht nur bedingt eingesetzt wurden.

Mittels der OctoGate App ist sowohl der vereinfachte Zugang zum Gästernetz als auch die Integration von privaten mobilen Geräten in die Schulkonsole der paedML® Windows möglich.

Für das Surfen im Internet auf dem BYOD Gerät gelten nun dieselben Filterregeln, die für die Klasse in der Schulkonsole festgelegt wurden. Ein Schüler kann auf seinem privaten Gerät also nur solche Seiten betrachten, die er auf einem Computer im Schulnetz auch sehen könnte, da der gleiche Filtermechanismus wirkt.

Durch die Installation der App und der damit verbundenen erzwungenen Zertifikatsinstallation kann die Schule ein WLAN für BYOD Geräte anbieten, welches hohe Anforderungen an den Jugendschutz erfüllt. Es werden nicht nur URLs oder DNS-Adressen überprüft, sondern es werden die angeforderten Inhalte nach den von Ihnen konfigurierten Filterkategorien durchsucht und gefiltert.

2 Systemvoraussetzungen

- Sie benötigen neben der Android oder iOS App die OctoGate Version ab 3.0.42 inklusive gültiger OctoGuest Lizenz.
- Damit die Contentfilterung bzw. Internetsteuerung analog zur paedML® Windows auch für BYOD entsprechend greift, erstellen Sie bitte ein Support-Ticket, damit die erforderliche Einstellung und die kostenlose Freischaltung des Moduls BYOD auf der Firewall vorgenommen wird.
- Folgende Versionsstände sind für die Endgeräte erforderlich: iOS ab Version 11.7 bzw. Android ab Version 4.0.
- Für die Pflege der in der App angezeigten Linkliste benötigen Sie zusätzlich einen gültigen Central Zugang. Sollten Sie noch keine Zugangsdaten haben, ist Ihnen der Vertrieb gern behilflich.

Wir empfehlen Ihnen, die Benutzeroberfläche Central über den Webbrowser Google Chrome aufzurufen.

Wichtiger Hinweis: bitte beachten Sie, dass wenn die App deinstalliert wird, die Verbindung zum WLAN zunächst weiterbestehen bleibt, sofern zuvor nicht der „Abmelden“-Button (OctGate 3.0.43) genutzt wurde. Die verbleibende Dauer der Verbindung richtet sich dann nach dem Zeitfenster der Gültigkeit, welches auf der OctoGate hinterlegt wurde (vgl. Seite 6).

Zudem sind Benutzerdaten und Stammzertifikat manuell zu entfernen. Eine musterhafte Darstellung der erforderlichen Schritte finden Sie am Ende des Dokumentes (Anlage 1).

3 Einstellungen auf der OctoGate

Aktivieren Sie unter „OctoGuest“ – „Einstellungen“ zunächst den Haken „Transparenter Proxy“ sowie das „Erlaube Domänen-Login“:

OctoGate
EINFACH. SICHER. GESCHÜTZT.

Hilfe Downloads Speichern Abmelden

FL42 > support > OctoGate Guest > Einstellungen

- Übersicht
 - Status
- Administration
- WAN
- Webfilter
- Firewall
- Netzwerk
- VPN / Remote
- OctoGate Guest
 - Einstellungen**
 - Zugangscodes
- Reports

Einstellungen

Transparenter Proxy ☒

Interface: VLAN_AP2410

Erlaube Domänen-Login ☒

AD-Login Gültigkeit (Tage:Stunden:Minuten): 0 : 01 : 00

Portfreischaltungen

+ Neuer Eintrag Bearbeiten Löschen Verwerfen Beschreibung

Beschreibung	Port	Protokoll	Quelle	Ziel	Action
Guest		ALL	0.0.0.0	0.0.0.0	ACCEPT

Wählen Sie die Zeitdauer für den WLAN Zugang unter „AD-Login Gültigkeit“:

OctoGate
EINFACH. SICHER. GESCHÜTZT.

Hilfe Downloads Speichern Abmelden

FL42 > support > OctoGate Guest > Einstellungen

- Übersicht
 - Status
- Administration
- WAN
- Webfilter
- Firewall
- Netzwerk
- VPN / Remote
- OctoGate Guest
 - Einstellungen**
 - Zugangscodes
- Reports
- Wireless

Einstellungen

Transparenter Proxy ☐

Interface: VLAN_AP2410

Erlaube Domänen-Login ☐

AD-Login Gültigkeit (Tage:Stunden:Minuten): 0 : 01 : 00

Portfreischaltungen

+ Neuer Eintrag Bearbeiten Löschen Verwerfen Beschreibung

Beschreibung	Port	Protokoll	Quelle	Ziel	Action
Guest		ALL	0.0.0.0	0.0.0.0	ACCEPT

Übersicht Export

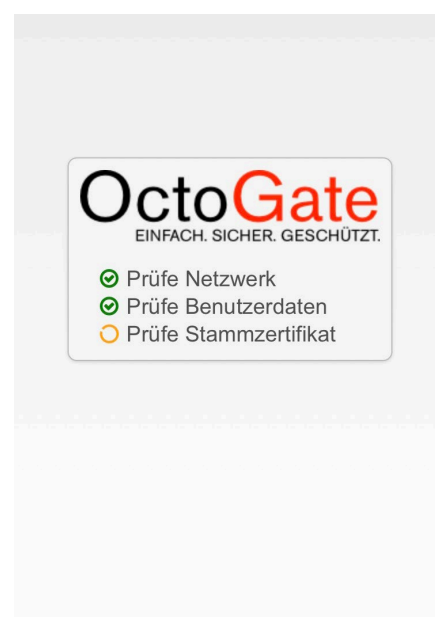
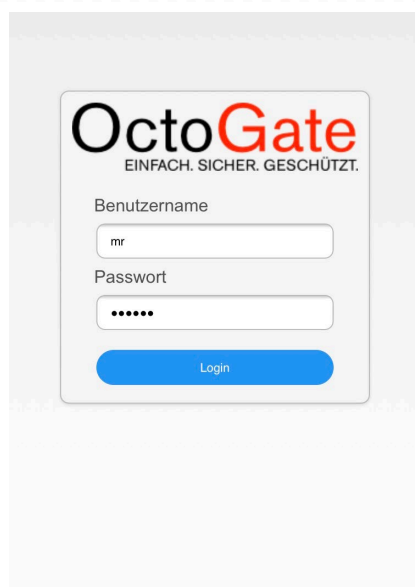
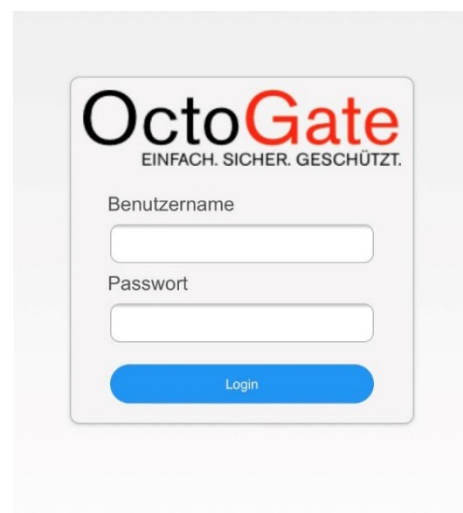
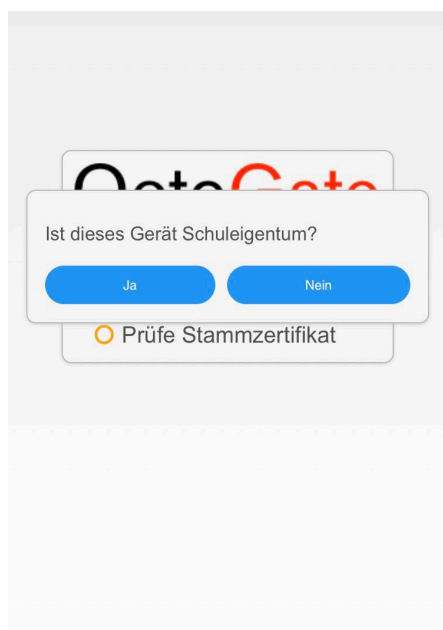
Beachten Sie bitte, dass die Nutzer Mitglieder der Active-Directory-Sicherheitsgruppe „octo_id_voucher“ sein müssen.

4 Installation der App

Installieren Sie die OctoGate App aus den Google Play Store oder aus dem Apple Store auf das jeweilige Gerät. Wählen Sie auf dem mobilen Endgerät das Gäste-Netz aus, mit dem sich verbunden werden soll.

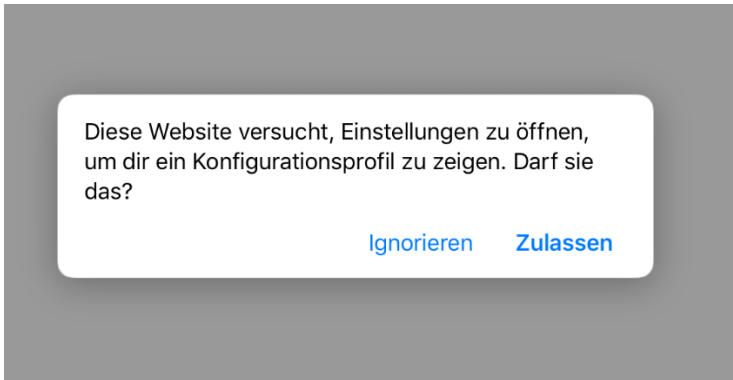
Beim ersten Start der App erfolgt die Abfrage, ob sich das Gerät im Schuleigentum befindet. Wählen Sie den Button „Nein“, wenn die Log-In Daten **dauerhaft** auf dem Gerät gespeichert werden dürfen.

Im nächsten Schritt loggen Sie sich mit Ihrem bekannten Benutzernamen und Passwort (Domänen Log-In) in der App ein.

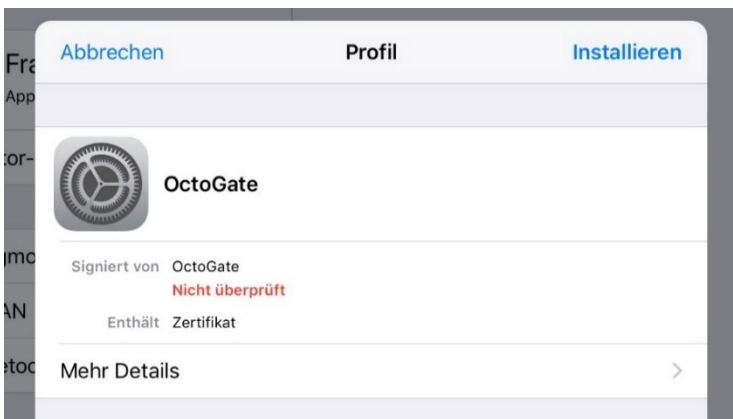


5 Installation von Stammzertifikaten

Während die Installation von Stammzertifikaten bei Android automatisiert im Hintergrund verläuft, muss bei Apple Geräten die Installation des Stammzertifikats beim ersten Aufruf von https-Seiten bestätigt werden, dies geschieht mit „Zulassen“:



Klicken Sie oben rechts auf „Installieren“:

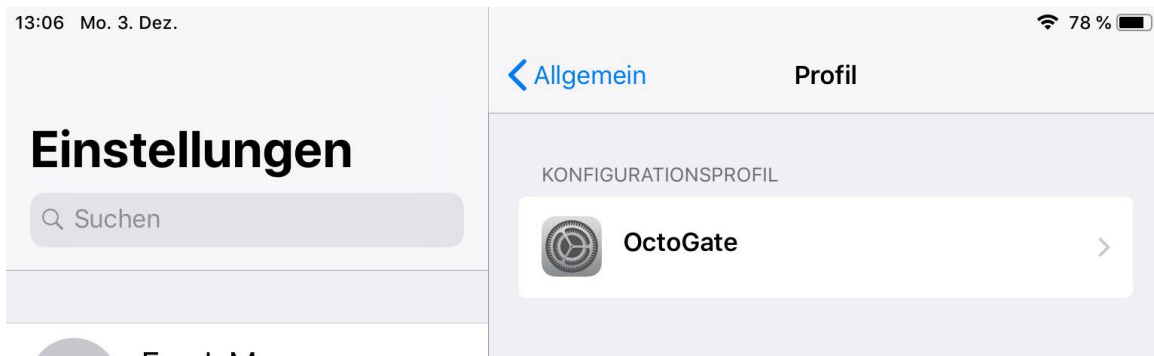


Vor dem Installieren erhalten Sie den Hinweis, dass wir unser Zertifikat zur Liste der vertrauenswürdigen Zertifikate zufügen. Lesen Sie diesen Abschnitt genau durch und klicken dann auf „Installieren“:

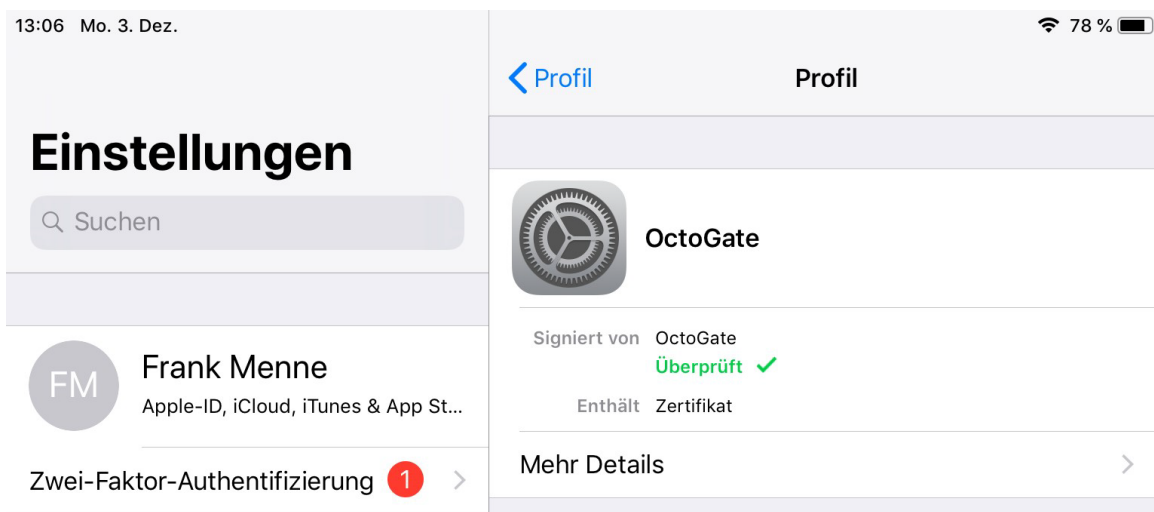


6 Konfigurationseinstellungen Apple

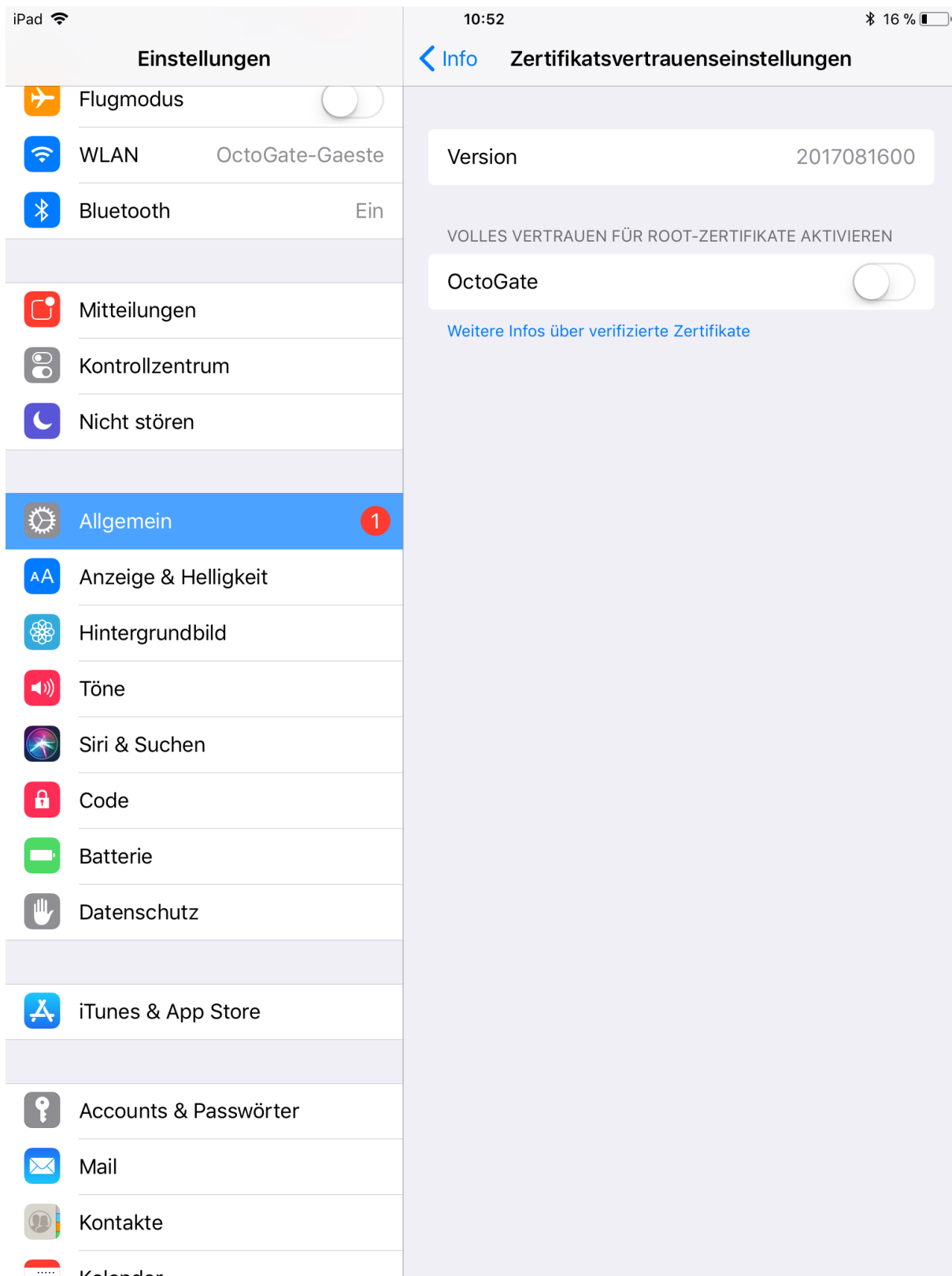
Unter „Allgemeine Einstellungen“ wählen Sie den Menüpunkt „Profil“ und danach das „Konfigurationsprofil“ OctoGate :



Die erfolgreiche Aktivierung des Zertifikates wird wie folgt dargestellt:

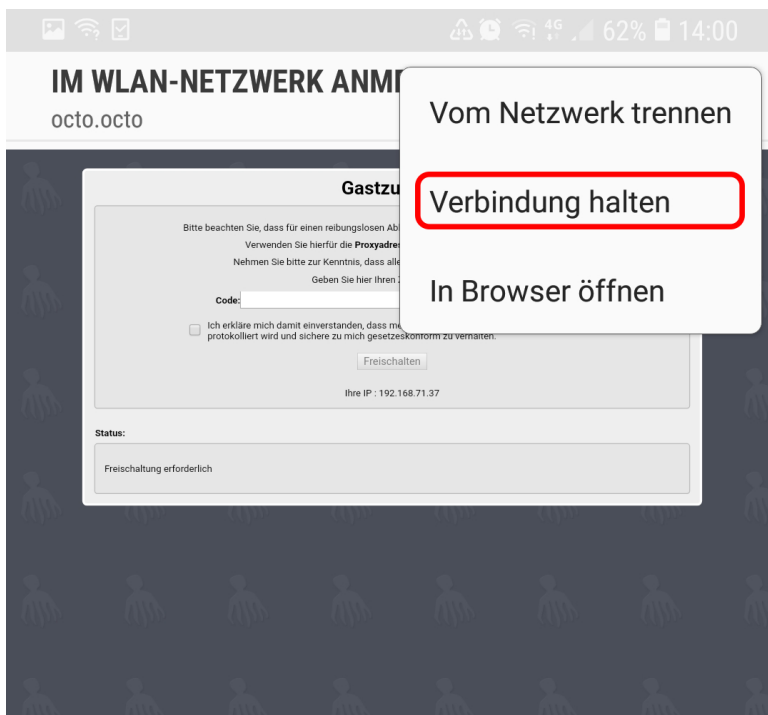
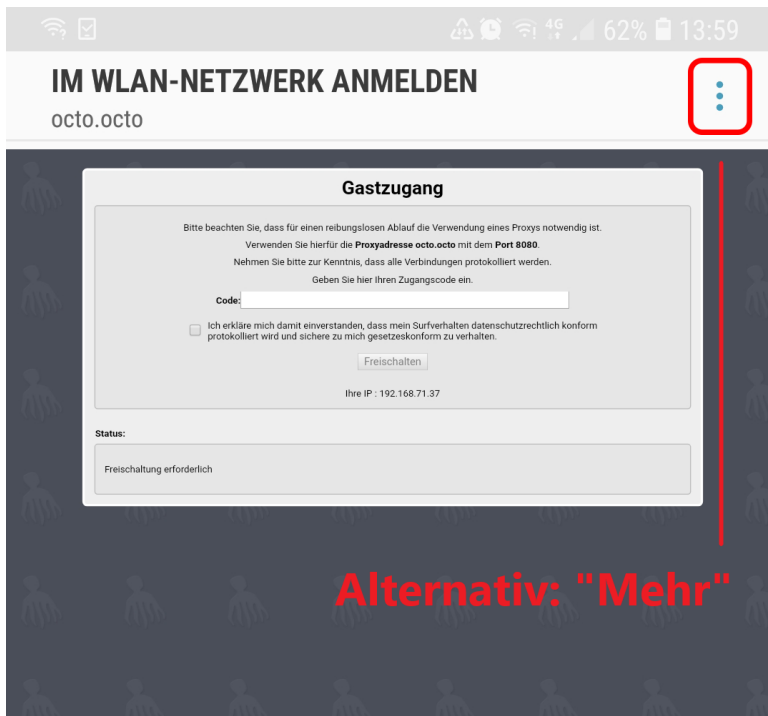


Unter Umständen finden Sie das Zertifikat nicht wie oben angegeben, sondern unter „Allgemeine Einstellungen“ – „Info“ – „Zertifikatsvertrauenseinstellungen“. Aktivieren Sie dann mittels des Reglers das Vertrauen für das OctoGate Zertifikat (siehe Grafik auf nächster Seite).



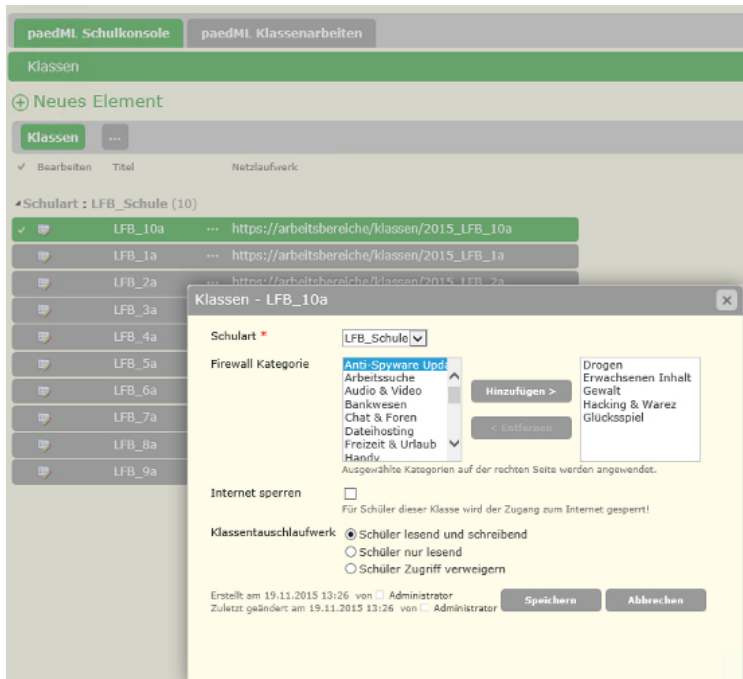
7 Problembehebung unter Android

Sollte einmal die App für Android nach der Eingabe von Benutzername und Kennwort hängen bleiben (zwischen Abb. 3 und 4 auf Seite 7), und sich die Seite des Captive Portal im Vordergrund öffnen, bitte die nachfolgenden Schritte durchführen:



8 Steuerung über die Schulkonsole

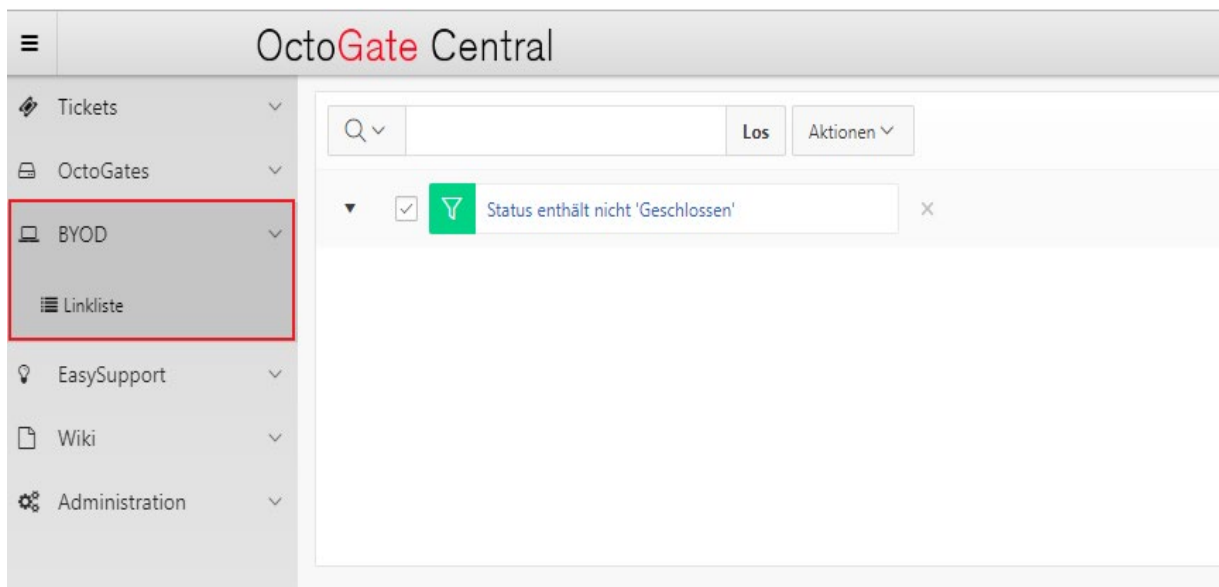
Nach der erfolgreichen Anmeldung im Gäste-WLAN ist das Gerät nun über die Schulkonsole steuerbar:



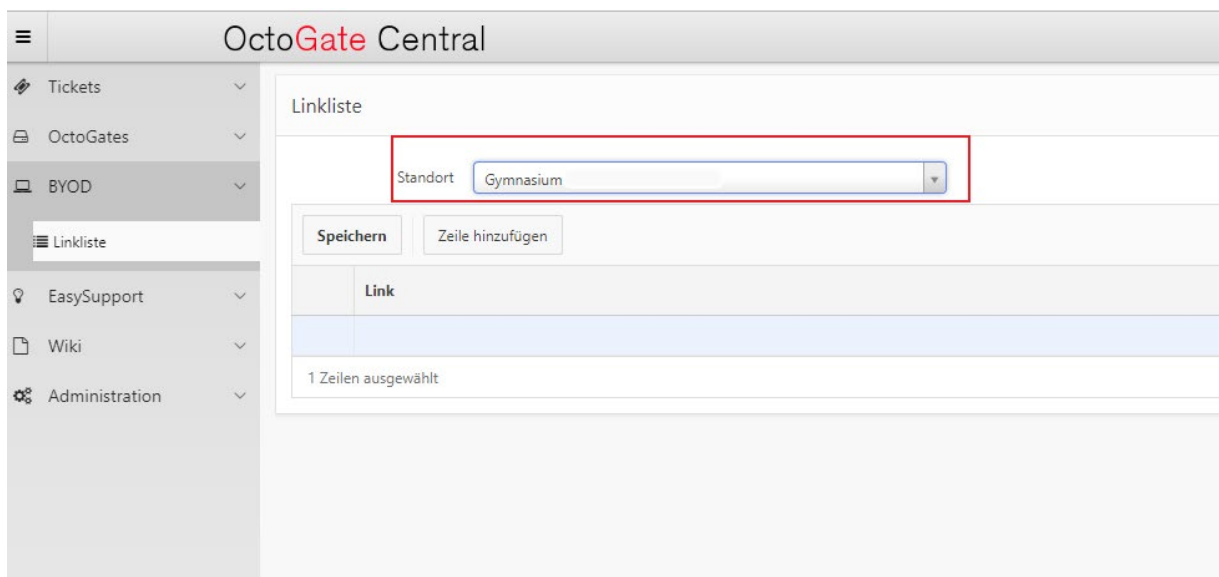
9 App-Einstellungen über OctoGate Central

Über die App können von Ihnen favorisierte Internetseiten aufgerufen werden (z. B. Wikipedia), dazu sind die jeweiligen Adressen in OctoGate Central zu hinterlegen.

Rufen Sie <https://central.octogate.de> auf und melden Sie sich mit Ihrer Email-Adresse an. Im linken Menü-Baum finden Sie die Linkliste unter „BYOD“:



Wählen Sie Ihren Standort aus:



Um eine neue Linkliste zu erstellen, klicken Sie bitte auf „Zeile hinzufügen“:

OctoGate Central

Linkliste

Standort: Gymnasium

Speichern Zeile hinzufügen

Link	Titel

1 Zeilen ausgewählt

In der Spalte „Link“ können Sie nun die gewünschten Adressen hinterlegen, klicken Sie dazu in die Zeile hinein und starten die Eingabe. Adressen, die mit https:// beginnen, werden später als „HTTPS“ „ja“ angezeigt.

Anschließend „Speichern“ Sie Ihre Eingabe ab:

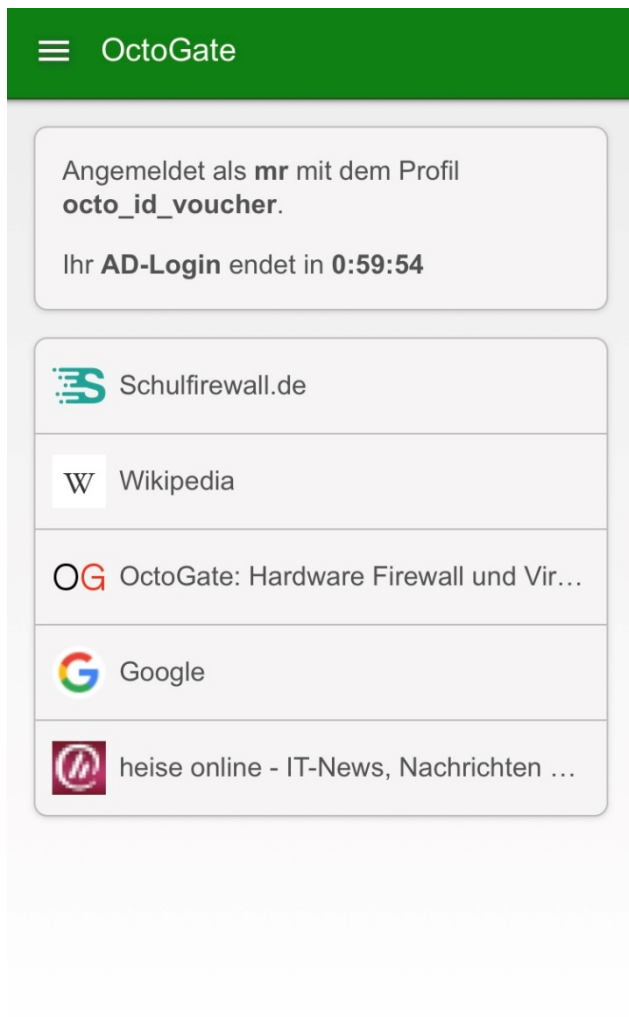
Linkliste

Standort: Gymnasium

Speichern Zeile hinzufügen

	Link	Titel	Icon	HTTPS
✗	www.octogate.de	OctoGate Startseite	OG	nein
✗	www.google.de	Google	G	nein
✗	www.wikipedia.de	Wikipedia	W	nein
✗	%%octogate%%.ozone.octogate.de:3002/lehrer/%%userlower%%	Sharepoint Lehrer		ja
✗	%%octogate%%.ozone.octogate.de:3002/schueler/%%userlower%%	Sharepoint Schüler		ja

Beispielhafte Darstellung einer Linkliste in der App:



10 Linkliste für paedML® Windows MySite

Um über die Linkliste auf MySite zugreifen zu können und nicht für jeden Nutzer einen Link generieren zu müssen, wird mit Platzhaltern (%%) gearbeitet:

%%userupper%%	bewirkt, dass der eingegebene Benutzername in Großbuchstaben umgewandelt wird (TestUser => TESTUSER)
%%userlower%%	bewirkt, dass der eingegebene Benutzername in Kleinbuchstaben umgewandelt wird (TestUser => testuser)
%%octogate%%	Name der OctoGate

Beispiel: OctoGate: abcdegh | Benutzername: KMuster
aus:
<https://%%octogate%%.ozone.octogate.de:3001/schueler/%%userlower%%>
wird:
<https://abcdegh.ozone.octogate.de:3001/schueler/kmuster>

Die MySite-Adressen der paedML® Windows, welche über die App angesteuert werden können:

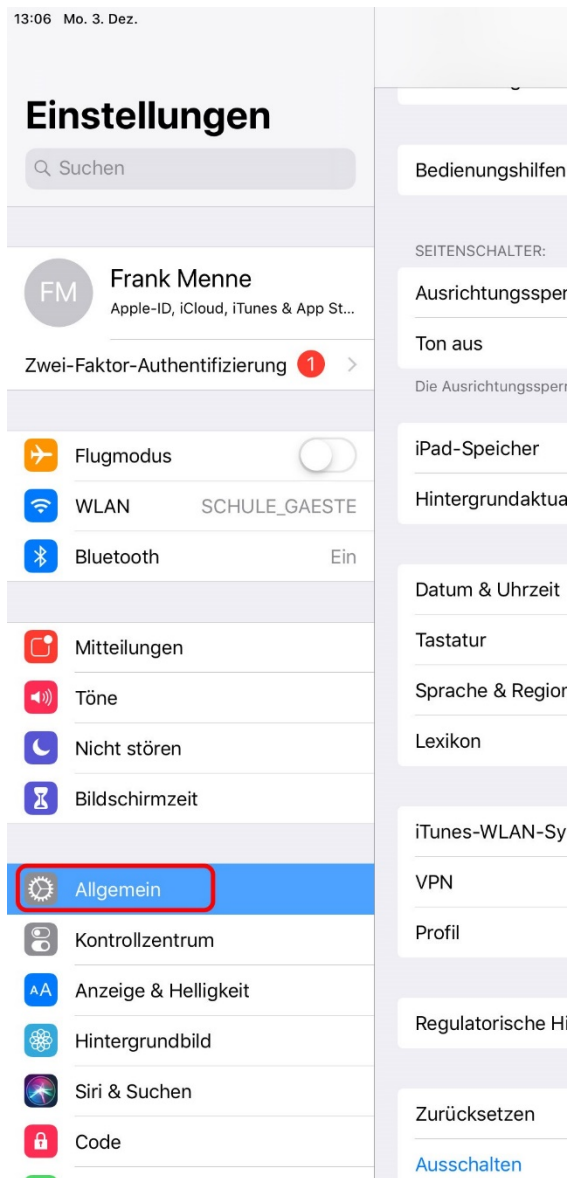
Für Lehrer:	https://%%octogate%%.ozone.octogate.de:3002/lehrer/%%userlower%%
Für Schüler:	https://%%octogate%%.ozone.octogate.de:3002/schueler/%%userlower%%

Anlage 1: De-Installation von Stammzertifikaten

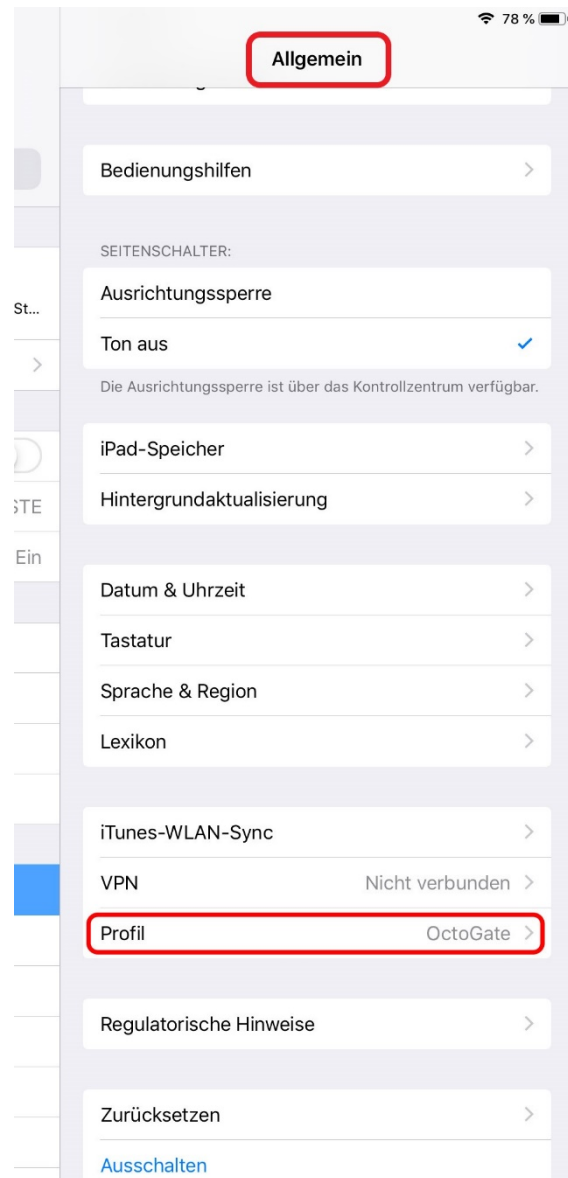
Nachfolgend finden Sie exemplarische Beispiele zur De-Installation von Stammzertifikaten

1. **iOS:** bitte führen Sie die folgenden Schritte durch:

„Einstellungen“ – „Allgemein“ – „Profil“

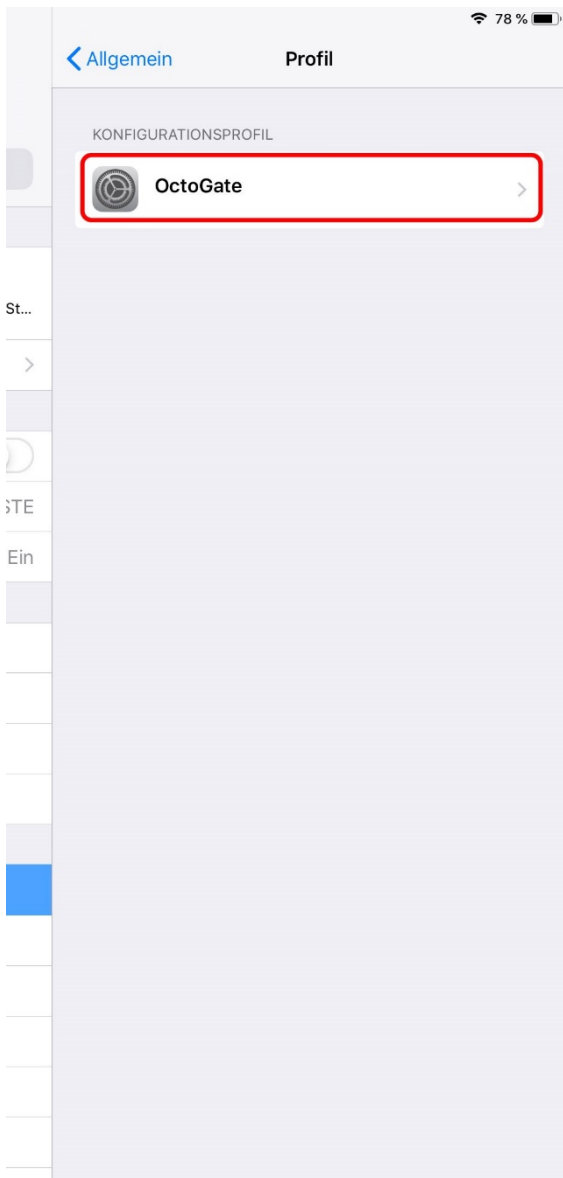


Schritt 1

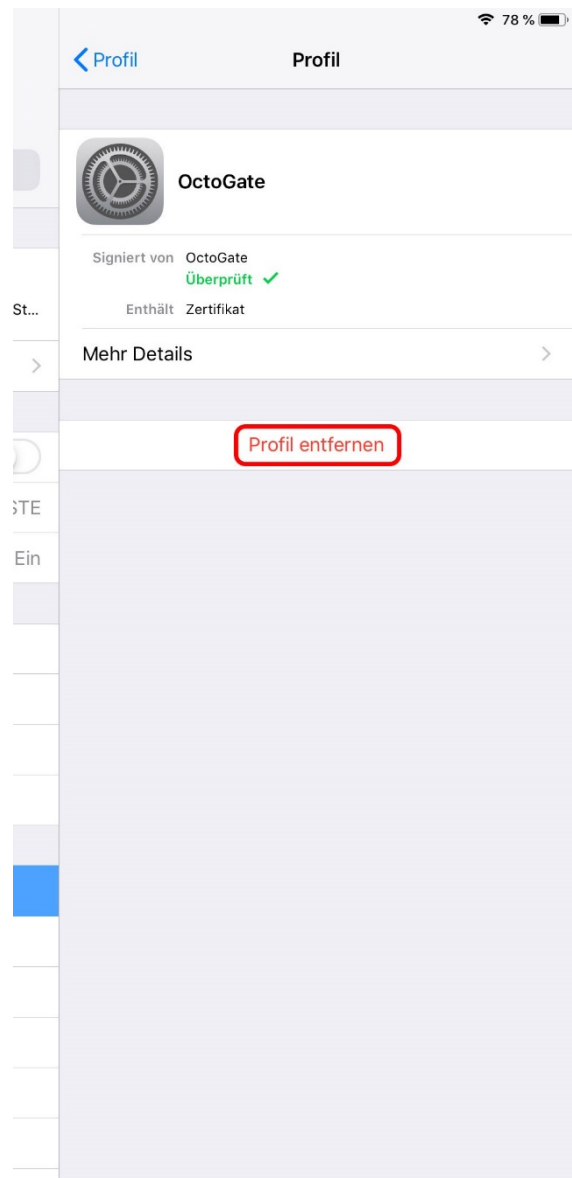


Schritt 2

Schritt 3

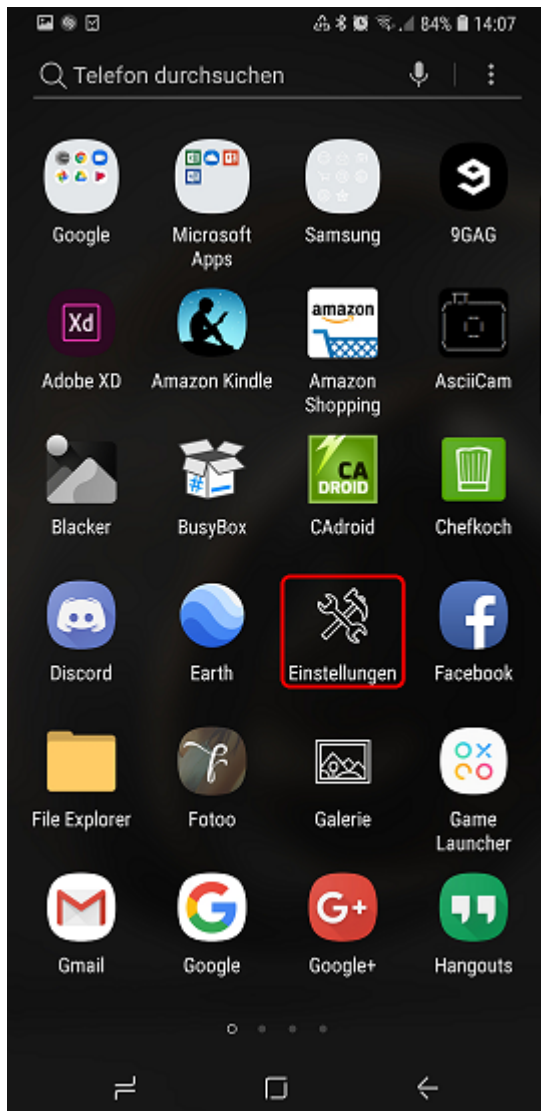


Schritt 4

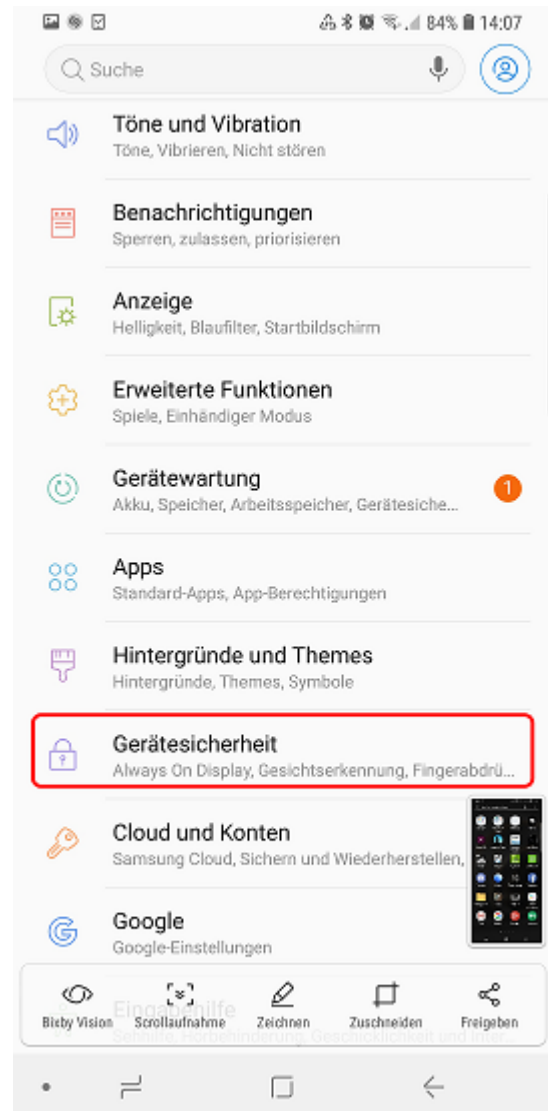


Die Benutzerdaten wurden bereits bei der De-Installation der App entfernt, weiteres manuelles Löschen ist nicht mehr erforderlich.

2. **Android:** bitte führen Sie die folgenden Schritte durch:

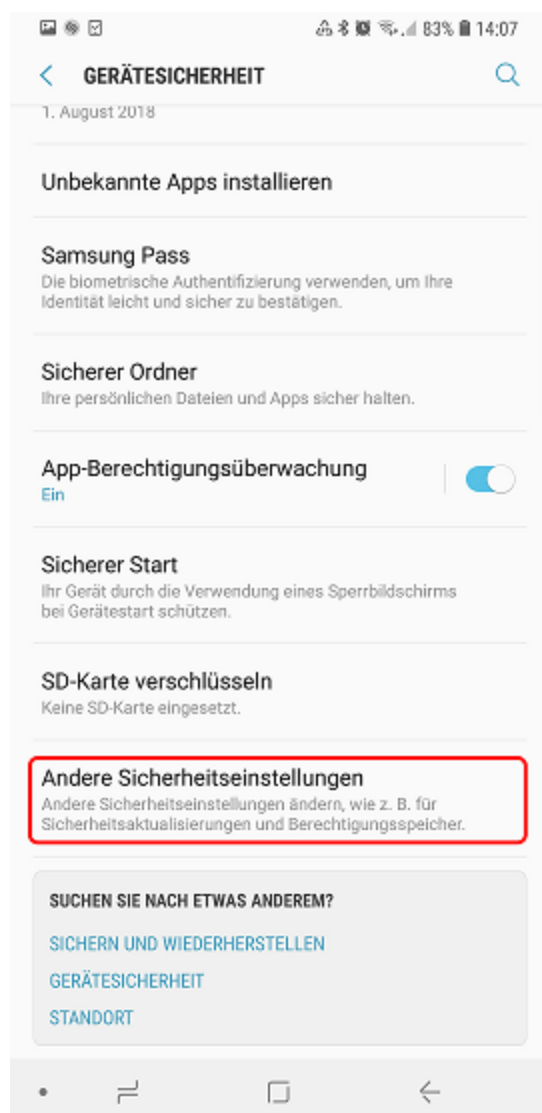


Schritt 1

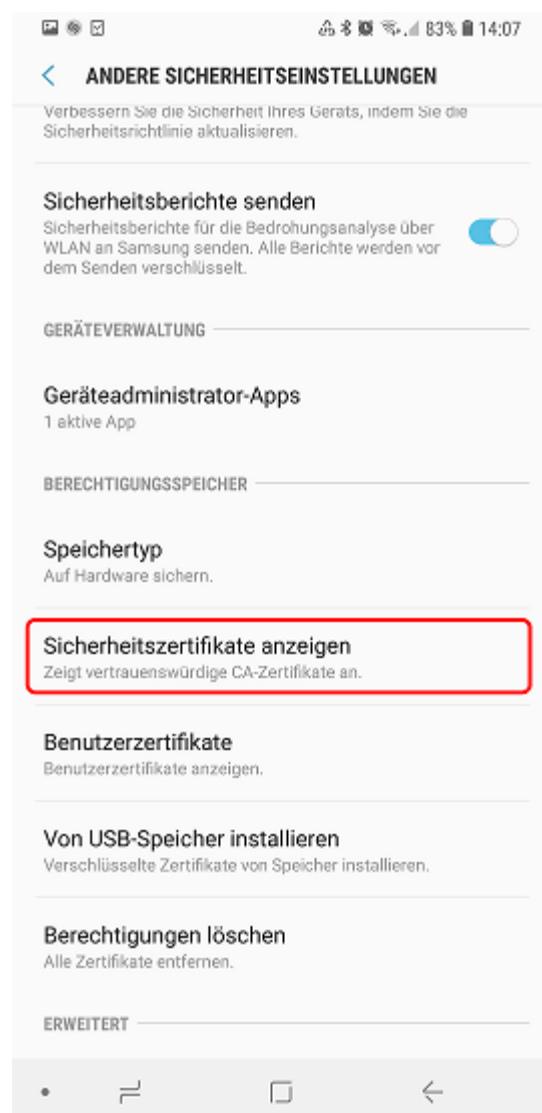


Schritt 2

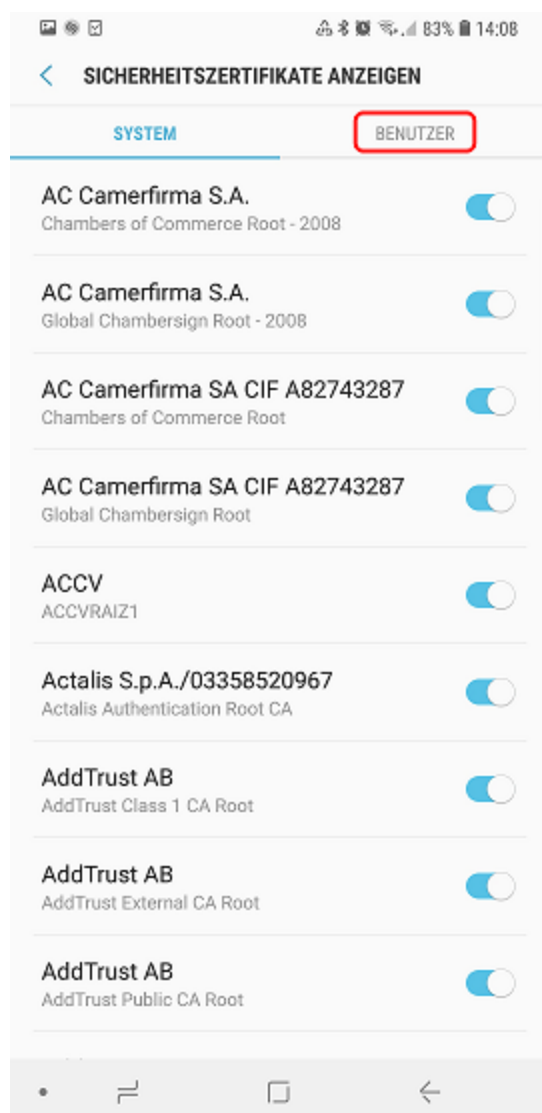
Schritt 3



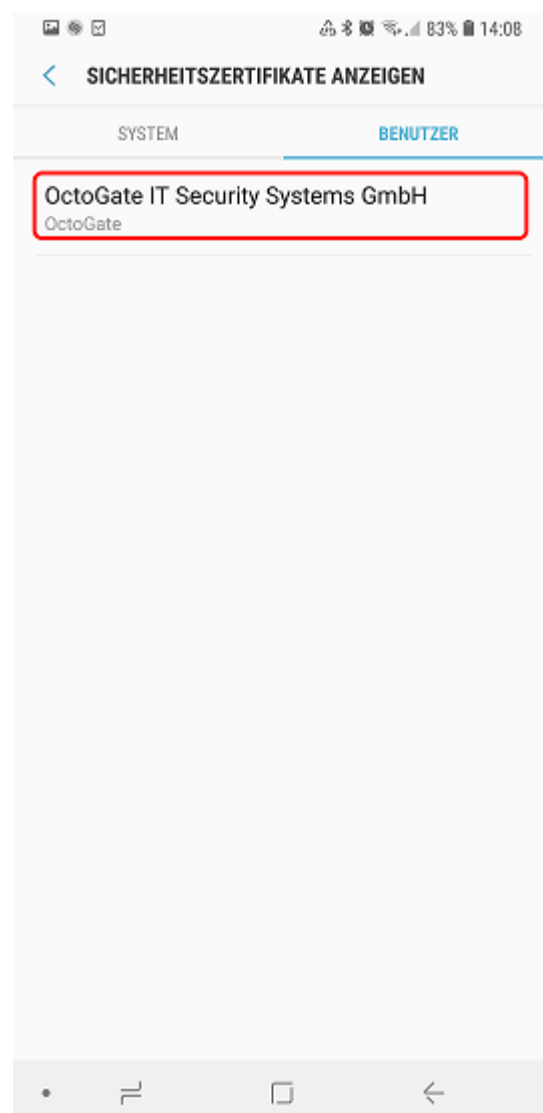
Schritt 4



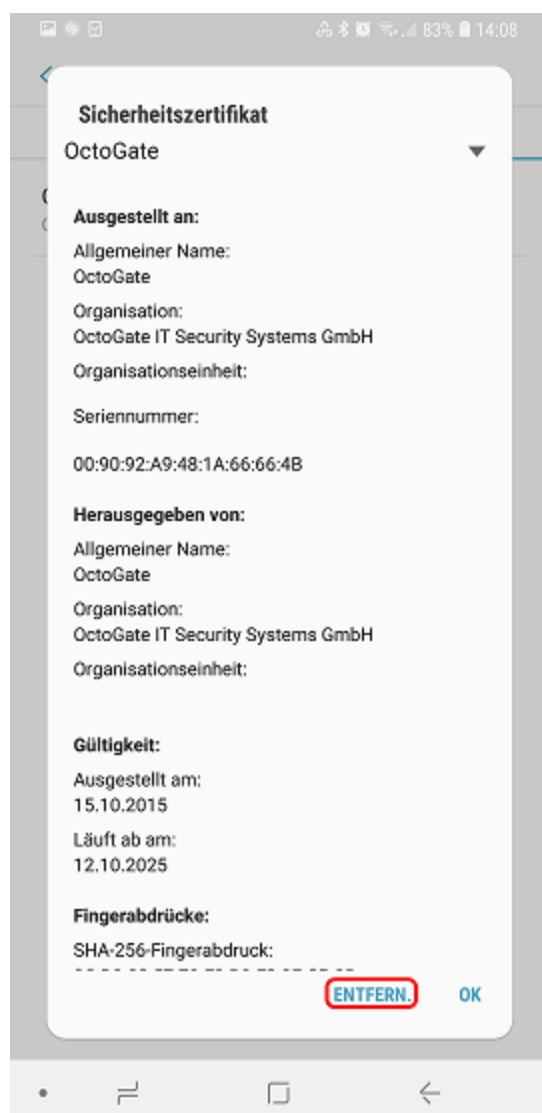
Schritt 5



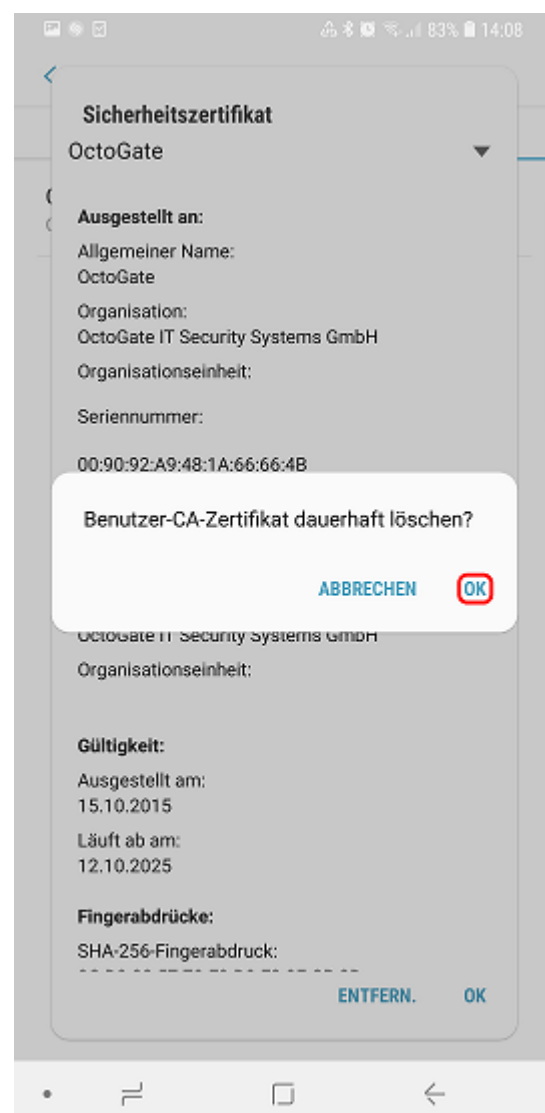
Schritt 6



Schritt 7



Schritt 8



Anlage 2: De-Installation der Android-App

Gehen Sie auf „Einstellungen“ – „Apps“ – „OctoGate BYOD“ und führen die nachfolgenden Schritte durch:

