Best Practices AuthPoint
Token Verwaltung - Was tun wenn es nicht klappt?

Thomas Fleischmann
Senior Sales Engineer Central Europe

Agenda

- Was ist ein Token?
  - OTP - Was ist das?
  - Hardware, Software und was noch?
- Welche Verfahren setzt WatchGuard AuthPoint ein?
  - RFCs
- Token Verwaltung mit der WatchGuard Cloud
  - Logging
- Token Verwaltung auf dem Device
- Ausblick in die Zukunft – Woran wir gerade arbeiten

Was ist ein Token?

- Ein Security-Token (einfach: Token) ist eine *Hardwarekomponente* zur Identifizierung und Authentifizierung von Benutzern. Gelegentlich werden damit auch *Softwaretoken* bezeichnet. Sie sind meist Bestandteil eines Systems der Zugriffskontrolle mit Zwei-Faktor-Authentisierung.

- Gegebenenfalls sind gegen Missbrauch weitere Merkmale zur *Authentifizierung* heranzuziehen, möglich sind u. a. die Kenntnis eines *Passworts* bzw. einer *PIN* oder *biometrische Merkmale* des Benutzers.
- Security-Token können personalisiert sein, sie sind dann eindeutig einem bestimmten Benutzer zugeordnet.

Quelle: Wikipedia https://de.wikipedia.org/wiki/Security-Token

OTP - Was ist das?

- Die oft gebrauchte Abkürzung *OTP* steht für englisch **one-time password**, was der direkten Übersetzung von „Einmalkennwort“ entspricht.

- Ein Einmalkennwort oder Einmalpasswort ist ein Kennwort zur *Authentifizierung* oder auch *Autorisierung*.
- Jedes Einmalkennwort ist nur für eine einmalige Verwendung gültig und kann kein zweites Mal benutzt werden. Entsprechend erfordert jede Authentifizierung oder Autorisierung ein neues Einmalkennwort.

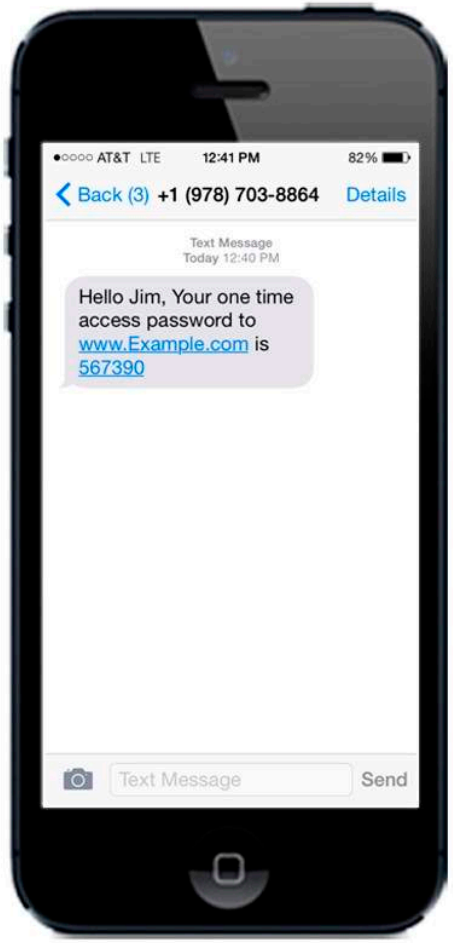
- Quelle: Wikipedia https://de.wikipedia.org/wiki/Einmalkennwort#Zeitgesteuert

Hardware, Software und was noch?

- Die gebräuchlichste Version eines Tokens ist der Hardware Token. Der Hardware Token stellt den OTP dar, kann aber keine andere Verfahren umsetzen.

- Software Token generieren über eine Applikation (App) auf einen Device den OTP. Je nach Device Typ kann man mit weiteren Sicherheitsverfahren die App oder den Token absichern.
- Dazu gehören biometrische Verfahren (wie z.B. Fingerprint, Iris Scan, …) oder durch das Setzen eines PINs.
- Ist das Device mit dem Internet verbunden, kann über das Empfangen einer PUSH Benachrichtigung die Authentifizierung des Users bestätigt werden.

Hardware, Software und was noch?



- SMS wird auch noch verwendet. Eine Textnachricht wird an das Device des Benutzers gesendet.

- Diese Verfahren ist nicht mehr sicher, da SMS Textnachrichten umgeleitet werden können.(Schwachstelle im so genannten SS7-Netzwerk)

Welche Verfahren setzt WatchGuard AuthPoint ein?

- WatchGuard AuthPoint setzt als Verfahren das sog. TOTP ein, d.h. Timebased One-Time-Password.

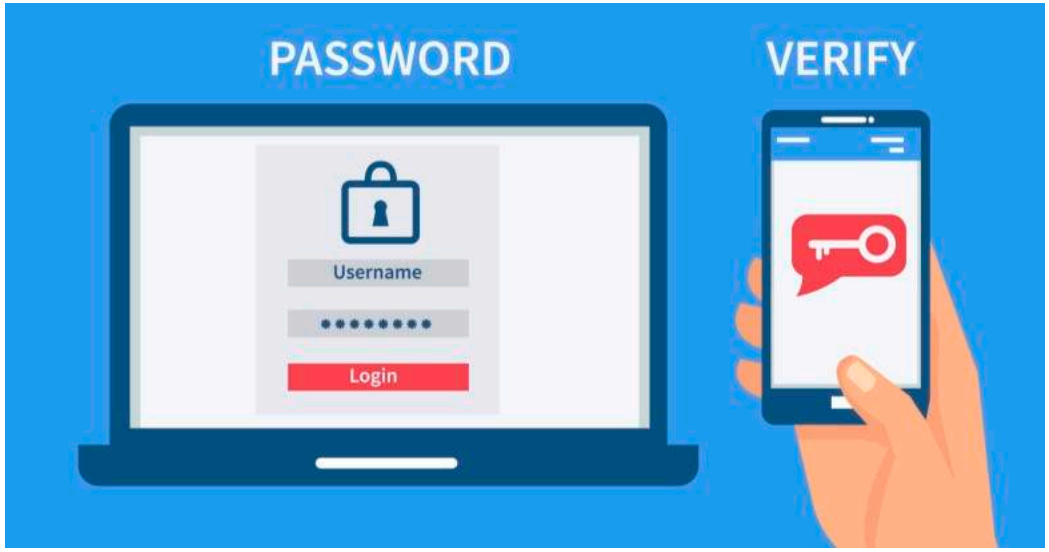
- Der generierte OTP ist für eine definiertes Zeitfenster verwendbar. In der Regel 30 bis 60 Sekunden.

- Ein anderes Verfahren ist das HOTP (ereignisgesteuerter OTP). Hier wird ein Token generiert, welches für ein Ereignis gilt. Der Token hat kein Zeitfaktor.
- Dieses Verfahren ist nicht so sicher, wie OTP. Es wird **nicht** von WatchGuard verwendet!

Welche Verfahren setzt WatchGuard AuthPoint ein?

- WatchGuard verwendet folgende RFC:
  - Algorithm — OATH time-based OTP (RFC 6238)

- Wir unterstützen folgende Format und Interval des Tokens:
  - Response Format — Six-digit time-based OTP that includes only numbers with a 30 or 60 second time interval

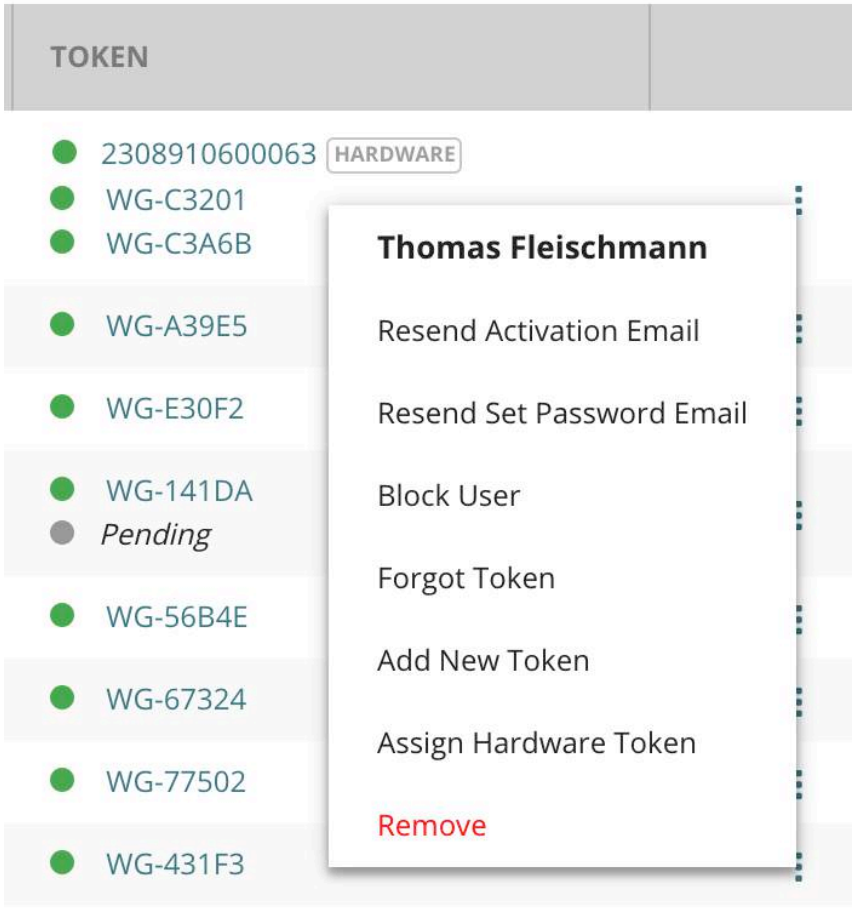


Token Verwaltung mit der WatchGuard Cloud

- Die WatchGuard Cloud ist die Verwaltungsoberfläche für WatchGuard AuthPoint.
- Alle Einstellungen werden in dieser Oberfläche vorgenommen.

- Für die Verwaltung der Token ist der Menü-Punkt „Users“ maßgeblich. Hier wird einen User ein Token zugeordnet und dieser wird verwaltet.

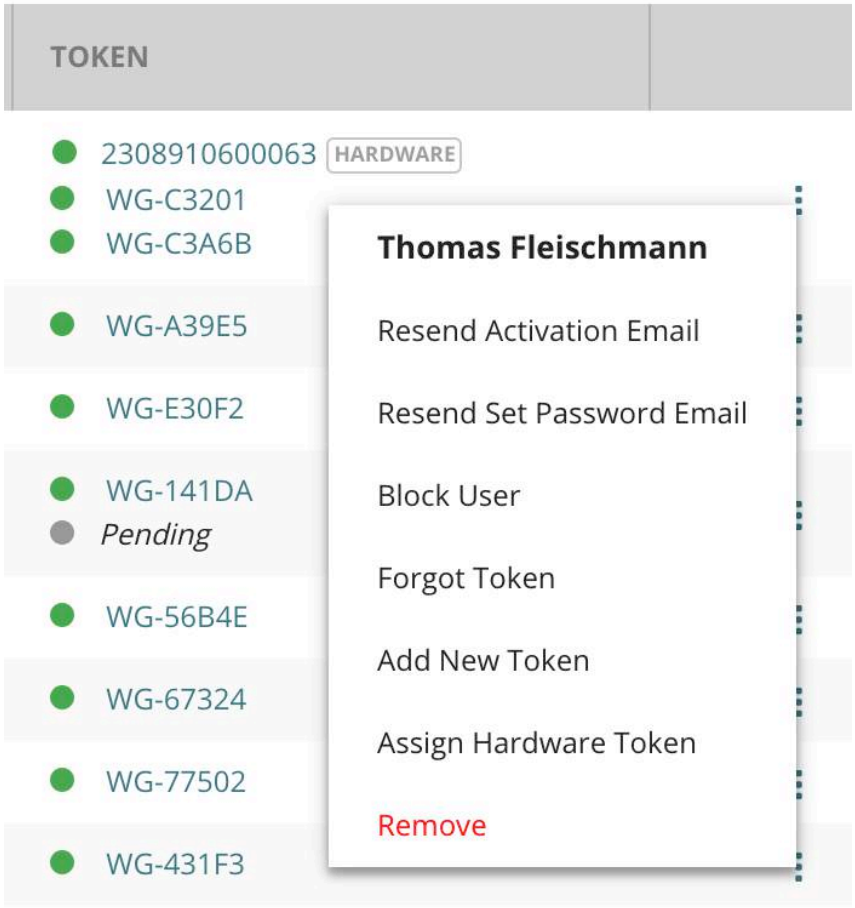
Token Verwaltung mit der WatchGuard Cloud



- Wenn man auf die drei Punkte im Menü klickt, bekommt man ein Menü dargestellt, welche einige Funktionen zur Verwaltung der Token darstellt.

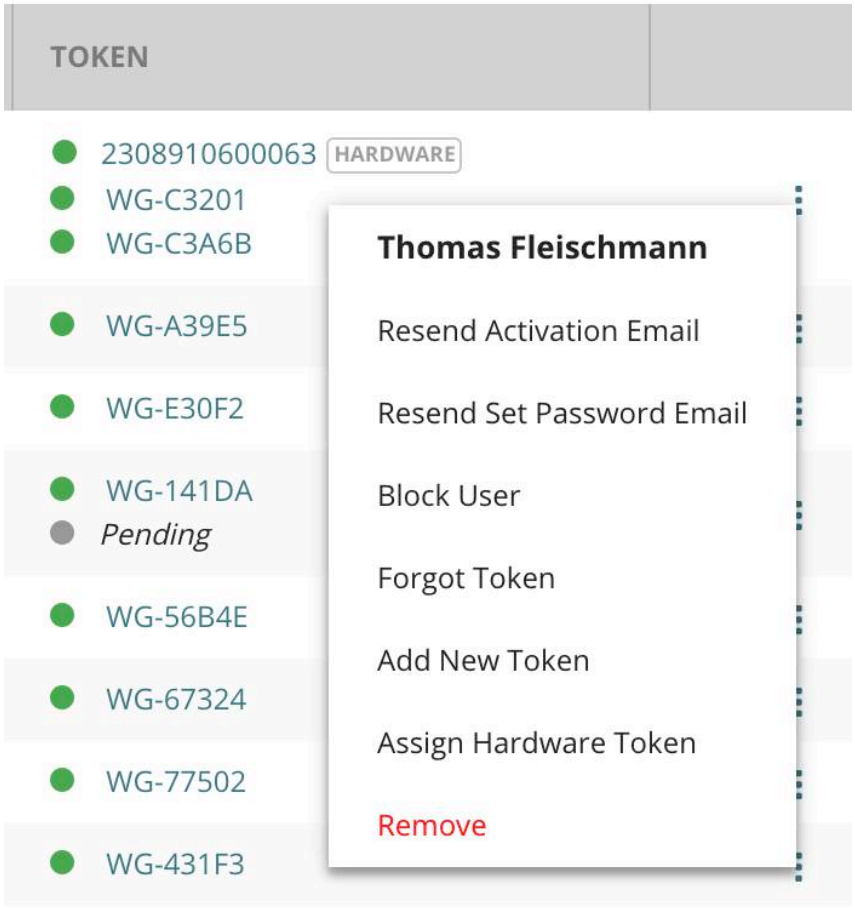
- Ein User kann bis zu fünf (5) Token zugewiesen bekommen. Dies deckt seine Lizenz ab.

Token Verwaltung mit der WatchGuard Cloud



- Add New Token
  - Ein neuer Token wird generiert. Der Benutzer erhält auf seiner hinterlegten Email Adresse eine Email mit dem Link zur Aktivierung.
- Assign Hardware Token
  - Ein eingepflegter Hardware Token kann den User zugeordnet werden.
  - Ein Hardware Token wird als „Hardware“ angezeigt.

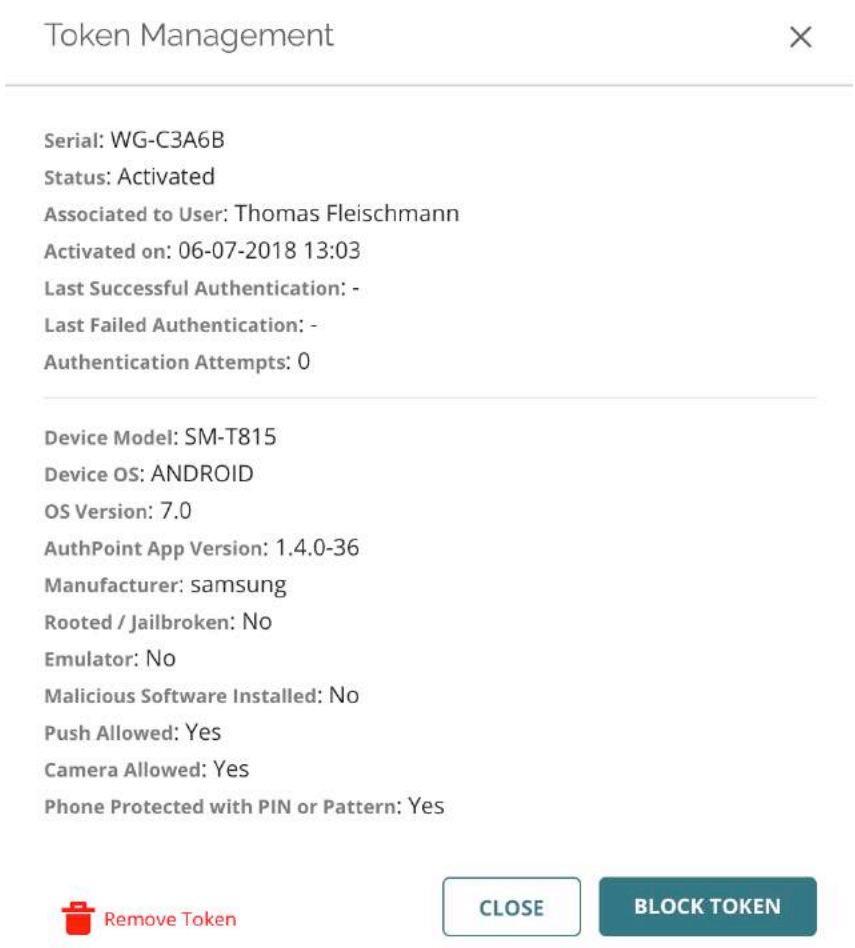
Token Verwaltung mit der WatchGuard Cloud



- Forgot Token
  - Wenn der Benutzer kein Token bei sich hat, kann er mit Hilfe des Administrators des WatchGuard AuthPoint Kontos einen temporären Zugangsschlüssel erhalten.
  - Der User kann sich dann für die festgelegt Zeit ohne Token am System anmelden.
  - Die Funktion kann auch mit Radius verwendet werden, wenn die Applikation dies unterstützt.

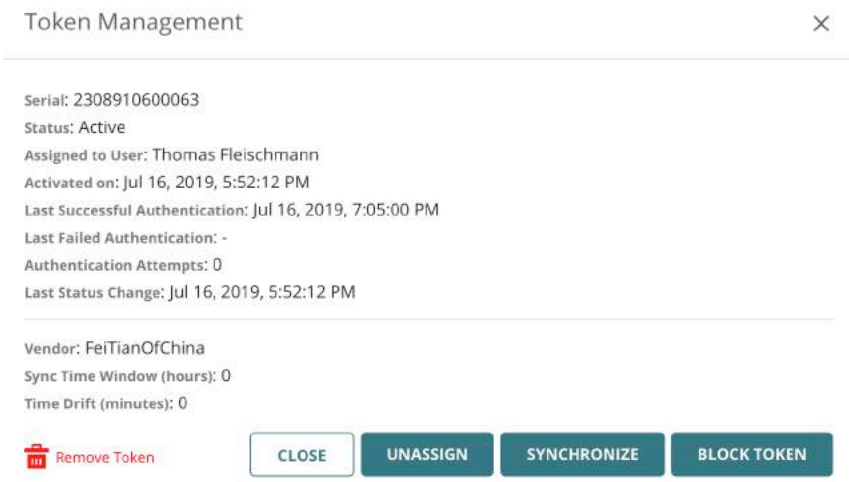
Token Verwaltung mit der WatchGuard Cloud

- Durch Anklicken des Tokens sieht man den Status des Tokens.
- Des Weiteren hat man hier die Möglichkeit, den Token zu blocken oder den Token komplett zu verwerfen.
- Diese Darstellung zeigt einen Software Token von WatchGuard AuthPoint.



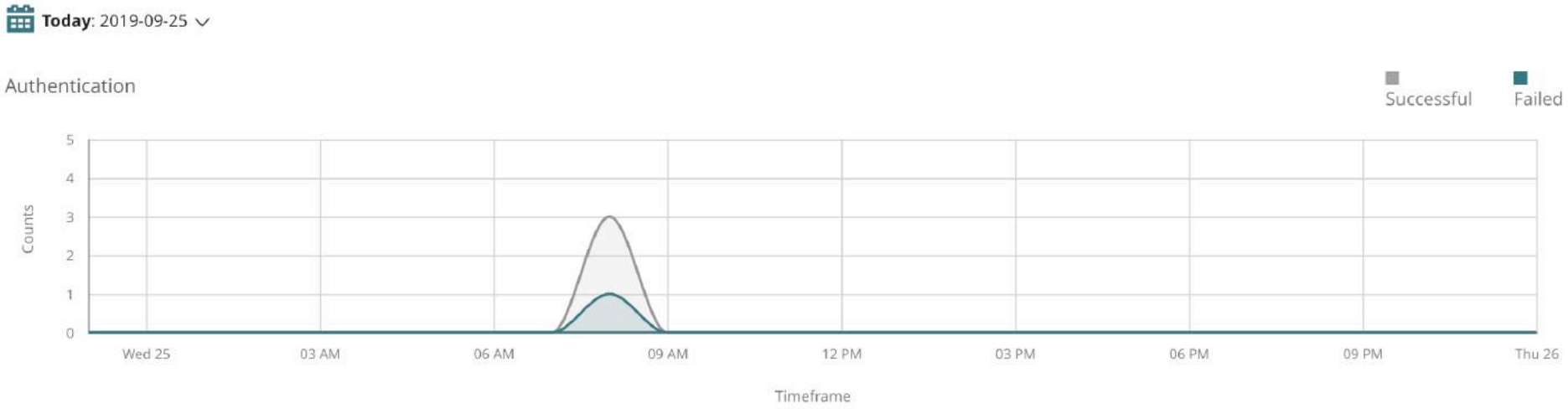
Token Verwaltung mit der WatchGuard Cloud

- Ein Hardware Token zeigt andere Optionen zusätzlich an.
- Unassign – Der Hardwaretoken wird den Benutzer entzogen und kann einen anderen User zugeordnet werden.
- Synchronize – Bei Einrichten des Tokens muss eine Synchronisation zwischen Cloud und Hardware eingerichtet werden.



Logging in der WatchGuard Cloud

Token Verwaltung mit der WatchGuard Cloud



User Activity

11

Inactive

2

Active

Authentication

1

Failed Authentications

3

Successful Authentications

Resource Activity

3

WGDCE

1

Dimension

Denied Push Notifications

1

Denied

This happens when a user denies a push notification.

Token Verwaltung mit der WatchGuard Cloud

- Im Report „Authentication“ sieht man, gefiltert nach der der Zeit, erfolgreiche oder fehlgeschlagene Anmeldeversuche aufgelistet nach Benutzer.

- Im Bereich Benutzer kann man die Informationen zu den einzelnen Ereignissen sich anzeigen lassen.

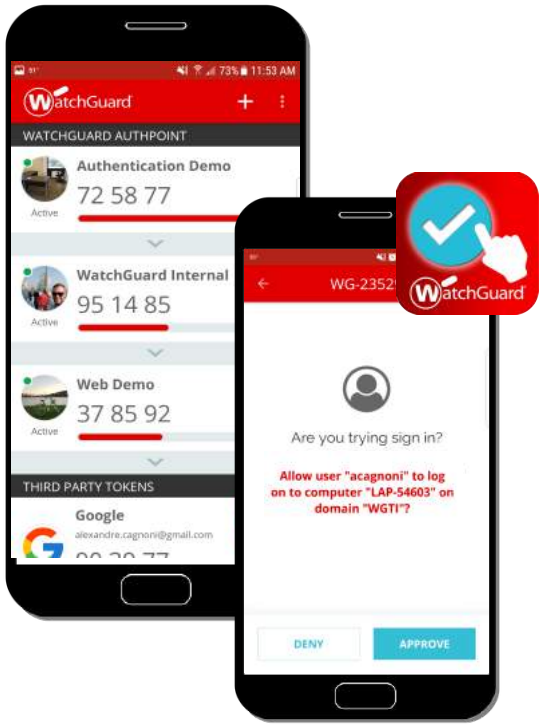
Token Verwaltung mit der WatchGuard Cloud

- Im Report “Denied Push Notification“ erhält man Informationen, ob eine Push Anmeldung fehlgeschlagen ist.
- In der Zukunft wird man weitere Informationen sehen können, besonders Angaben zum zeitlichen Verlauf der Push Nachricht.


Live
Token Management
in der WatchGuard Cloud

Token Verwaltung auf dem Device

- Die wichtigsten Funktionen des WatchGuard Authenticator (AuthPoint App) sind:
  - Fingerabdruck Scanner Integration
  - Automatische Token-Bereitstellung
  - Drittanbieter-Tokens
  - PIN-Code Sicherheit / Schutz
  - QR Code-Leser
  - Device DNA



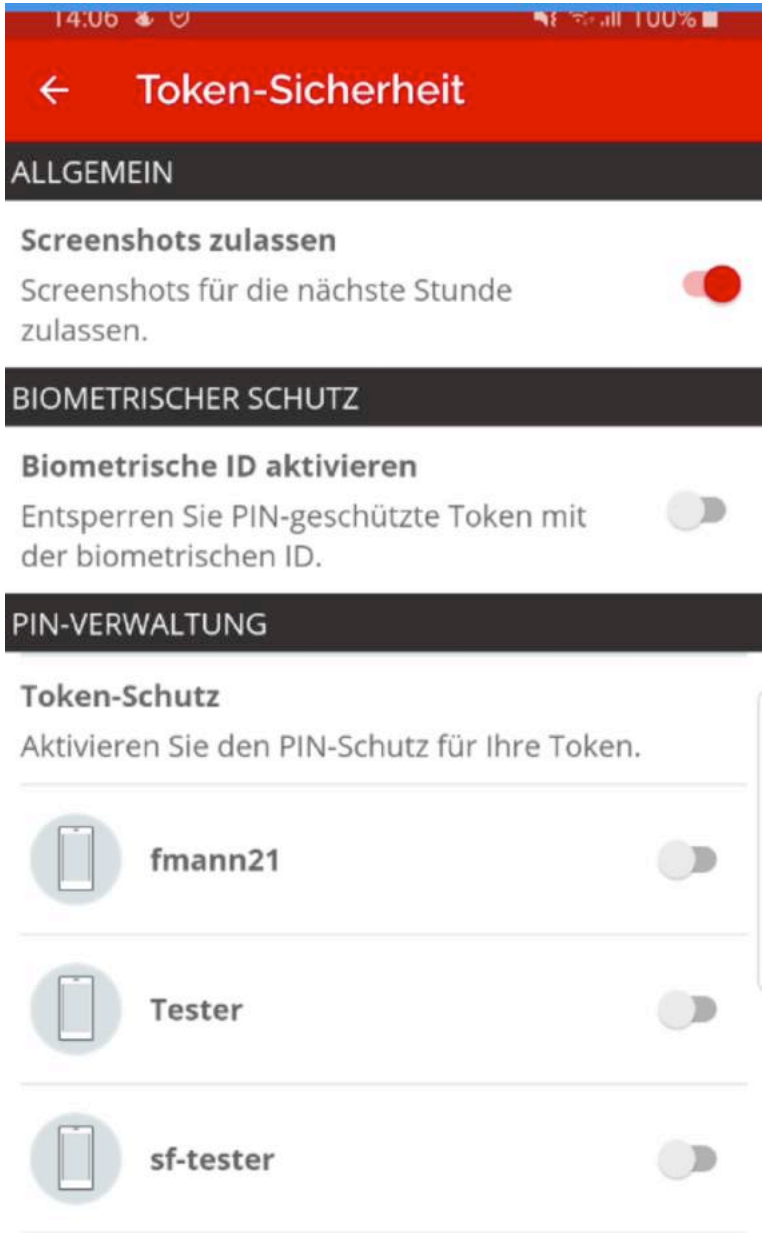
Token Verwaltung auf dem Device

- Folgende Authentifizierung Methoden unterstützt die AuthPoint App
  - Push Notification – Das Device erhält über einen sicheren Kanal (HTTPs) eine Information/Anfrage gesendet, um eine Authentifizierung abzuschließen. Der Benutzer muss nur Ja oder NEIN sagen.
  - One-Time Password (OTP) – Der Token wird in der App angezeigt und kann für die Authentifizierung verwendet werden.
  - QR Code – Die App nutzt die Kamera des Devices, um einen QR Code auf einer Seite (Web, Logon App, ..) einzuscannen. Daraus wird dann in der App der OTP berechnet. Dieses Verfahren ermöglicht es, ohne Verbindung ins Internet eine Anmeldung durchzuführen.

Sicherheitsfunktionen in der AuthPoint App

- Der Token selber kann durch einen PIN geschützt werden. Wenn man dies aktiviert, muss man den PIN angeben. Bei jeder Verwendung eines PIN geschützten Token wird der PIN wieder benötigt. Man kann den Token auswählen, für den ein Schutz aktiviert sein soll.
- Des Weiteren hat man die Möglichkeit, wenn das Device dies unterstützt, biometrische Verfahren zu nutzen.

Die AuthPoint App ist unter Android noch weiter geschützt, in dem man den Bildschirm der AuthPoint App nicht ohne Freigabe teilen kann (sharen).

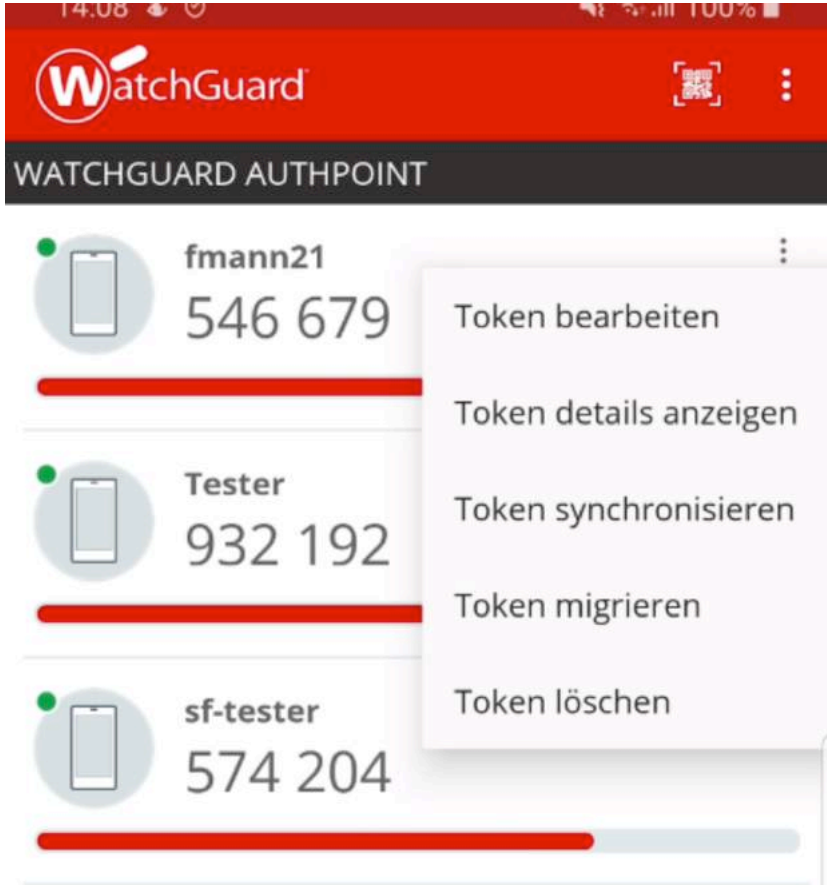


Der Token selber kann von Benutzer angepasst werden über ein Menü, welches beim Token angezeigt wird (Drei Punkte)

Folgend kann durchgeführt werden:

- Der Name des Tokens kann verändert werden.
- Ein Bild / Grafik kann den Token zugeordnet werden.
- Die Token Informationen werden angezeigt (z.B. isst er auch für PUSH registriert)
- Den Token mit dem Server synchronisieren.
- Den Token löschen

Die Migration des Tokens ermöglicht es, den Token auf ein anderes Device umzuziehen. Das System regelt dem Umzug selber ohne weiteren Aufwand des Administrators.




Live
Token Management
in der AuthPoint App

Ausblick in die Zukunft – Woran wir gerade arbeiten

- Für die Verwaltung der Token und AuthPoint App wird zurzeit an einigen Punkten gearbeitet.
- Zwei interessante Punkte sind
  - Verwaltung von Token Security Einstellungen auf der AuthPoint App durch den Administrator
  - Migration von 3rd Party Token