Passwortrichtlinie

Zur Steigerung der Datensicherheit steht Administratoren die Möglichkeit zur Verfügung, für Nutzer Passwort-Richtlinien zu aktivieren.

Funktionsweise

Es gibt drei Passwortrichtlinien, die standardmäßig allen Einheiten zur Verfügung stehen:

- Mindestlänge 6, alle Zeichen erlaubt
- Mindestlänge 8, Klein- und Großbuchstaben, Zahl
- Mindestlänge 10, Klein- und Großbuchstaben, Zahl, Sonderzeichen

Sie werden über Berechtigungsgruppen, bzw. Nutzer-Einstellungen zugewiesen/vererbt.

Individuelle Passwortrichtlinien

Innerhalb der PRO-Version steht zusätzlich das Anlegen eigener Passwort-Richtlinien zur Verfügung, die dann den Einheiten als Vorgabe zur Verfügung gestellt/eingeschränkt werden kann.

Richtlinien

Standardmäßig (und damit neu für alle Nutzer) muss ein Passwort erfüllen (Richtlinie 1):

- Nicht einfach zu erraten (zum Beispiel "123456")
- Mindestlänge 6 Zeichen
- Nicht der E-Mail Adresse entsprechen
- Passwort-Entropie (s.u.)

Passwort-Entropie

Zugegeben, wir sind nicht alle ausgebildete/studierte Informatiker. Daher nachfolgend ein paar Links die einfach und kurz erklären was diese Passwort-Entropie eigentlich ist.

> **Was macht ein sicheres Passwort aus?**
>
> Die Sicherheit eines Kennworts lässt sich am einfachsten über die Entropie definieren. Die Wikipedia erklärt es ziemlich gut: Ein Kennwort mit einer Entropie von 42 Bits benötigt 2 hoch 42 Versuche, um alle Möglichkeiten durchzuspielen. Die Entropie hängt neben der Länge mit den verwendeten Zeichen zusammen. Eine gute Richtlinie ist: Mindestens acht Zeichen lang, große und kleine Buchstaben, ein paar Sonderzeichen. Das amerikanische NIST (National Institute of Standards and Technology) schlägt zudem vor, dass künftig nicht mehr nur das englische Alphabet, sondern alle druckbaren ASCII-Zeichen in Kennwörtern erlaubt sind. Eine gute Alternative ist ein Passwort-Manager.

Quellen und Links:

- https://www.security-insider.de/was-ist-ein-sicheres-passwort-a-572229/
- https://www.computerweekly.com/de/definition/Passwort-Entropie
- https://en.wikipedia.org/wiki/Password_strength#Entropy_as_a_measure_of_password_strength (Englisch)

Mindestens (((aufgerundet) Mindestlänge / 2) + 1) verschiedene Zeichen.

Beispiel: Mindestlänge 6
((6 / 2) + 1) = 4
Beispiel Mindestlänge 7
((7 / 2) + 1) = (4 + 1) = 5

Maximal aber nur 6 verschiedene Zeichen, also bei 14 Zeichen Mindestlänge müssen nicht 8 verschiedene Zeichen benutzt werden, sondern nur 6

Eigene Richtlinien

Eigene Richtlinien (PRO Version), können nicht schwacher sein, als Richtlinie 1. Es stehen folgende Parameter zur Verfügung:

- Passwortlänge (mind. 6)
- Großbuchstaben erforderlich
- Kleinbuchstaben erforderlich
- Zahlen erforderlich
- Sonderzeichen erforderlich
- autom. Ablauf (in Monaten)
- Wiederverwendung von Passwörtern beschränken (auf die letzten X Passwörter)

Ablauf eines Passworts

In den Standardregeln, die der FREE + ALARM Version zur Verfügung stehen, läuft das Passwort niemals ab.

In der PRO Version kann über eine eigene Passwort-Richtlinie (Standortvorgaben / Sicherheit) das Ablaufen eines Passworts aktiviert werden. 1 Woche vor Ablauf eines Passwortes erhält der Nutzer einer Direktnachricht mit der Aufforderung sein Passwort zu ändern. Sobald das Passwort abgelaufen ist, erscheint in der App eine erste Aufforderung das Passwort zu ändern, was überspringbar ist. Beim zweiten Öffnen der App wird forciert das Passwort zu ändern.

Letzte X Passwörter sperren

In einer eigenen Passwortrichtlinie kann eingestellt werden, dass die letzten X Passwörter nicht verwendet werden dürfen. Das ist optional und nicht in den Standard-Richtlinien aktiviert.
Zum Entsperren kann der Nutzer die "Passwort-vergessen"-Funktion der WebApp verwenden. Er erhält anschließend eine Mail, mittels derer sich ein neues Passwort setzen lässt. Alternativ kann der Verwalter der Einheit den Benutzer über die Benutzer-Einstellungen im Tab "Extras" entsperren, indem er den Haken bei "Benutzer sperren" entfernt und anschließend speichert.

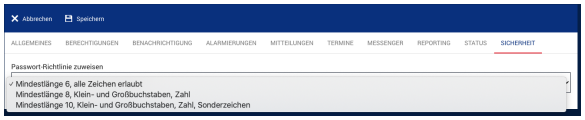
> **Hinweis**
>
> Bestehende Accounts werden dadurch nicht ungültig! Die Richtlinien greifen erst bei dem Setzen eines neuen Passworts.

Verwalten und Zuweisen von Passwortrichtlinien

> **Hinweis**
>
> Die Standard-Passwort-Richtlinien können in der ALARM und FREE Version nicht weiter angepasst werden. Eine individuelle Konfiguration der Passwort-Richtlinien kann nur in der PRO Version vorgenommen werden.

Passwort-Richtlinie in der ALARM / FREE Version

Innerhalb der Berechtigungen /Berechtigungsgruppen können Nutzer mit Verwaltungsrechten eine entsprechende Passwort-Richtlinie für ihre Einheit auswählen. Hier stehen drei verschiedene Richtlinien zur Verfügung, die sich in ihrer Stärke unterscheiden.

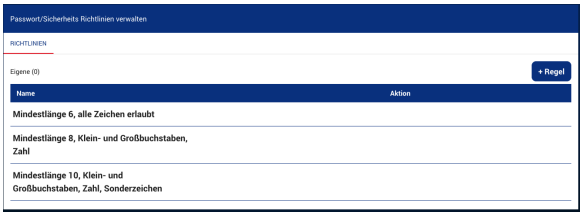


Passwort-Richtlinien in der PRO-Version

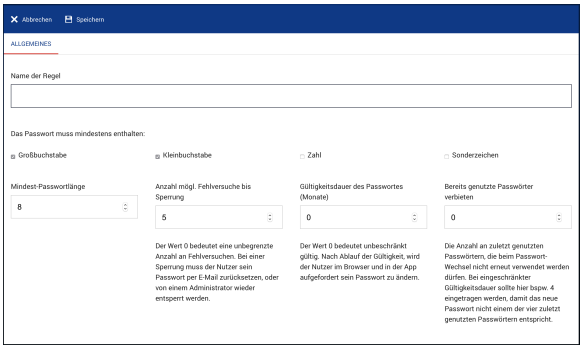
Gehen Sie zum Konfigurieren der Passwort-Richtlinien in die Zentrale Verwaltung. Unter *Zentrale Einstellungen - Standortvorgaben - Sicherheit* finden Sie die entsprechenden Konfigurationen

Innerhalb der Konfiguration finden Sie bereits die drei vorgegebenen Regeln.

Mithilfe des **+ Regel** Buttons können Sie neue Regeln anlegen.



Hier können, basierend auf vorgegebenen Parametern, verschiedene Sicherheitsstufen und zusätzliche Regeln definiert werden.



Verwandte Artikel

- Dashboards
- Lichter anschalten mittels Android Ereignis (IFTTT)
- Monitor-App – Installationshinweise
- Monitor-App – Download
- iOS - Download im App Store