datomo MDM Sicherheitsrichtlinie

Willkommen zu einem neuen „How To“ der datomo MDM Lösung.
Beachten Sie bitte Folgendes:
Vor dem Einbinden des mobilen Gerätes in die datomo MDM Lösung sollte Ihr Gerät auf die Werkseinstellungen zurückgesetzt werden um auszuschließen, dass Drittkomponenten den Einbindungsprozess behindern. Stellen Sie sicher, dass eine Datensicherung gemacht wurde. Darüber hinaus darf Ihr Gerät keinerlei Komponenten anderer MDM Software enthalten.
datomo MDM unterstützt eine Vielzahl gängiger Geräte und Plattformen. Allerdings kann es gerade bei einigen “ Android-Exoten“ und WP8 Geräten speziell aus dem unteren Preissegment vorkommen, dass sich solche Geräte nicht immer sauber einbinden lassen, weil zum Beispiel Entwicklersignaturen fehlen oder die Firmware nicht den Herstellerstandards entsprechen.
Auch gerootete oder gejailbreakte Geräte lassen sich nicht immer reibungslos verwalten.

Für die Konfiguration der Sicherheitsrichtlinie gehen Sie wie folgt vor. :

1. **Sicherheitsrichtlinie konfigurieren**

Melden Sie sich hierfür über Ihren Browser mit den Login Daten an der datomo Seite an. Sie sehen die Administrator-Oberfläche. Diese Seite besteht aus 2 Hauptregisterkarten: datomo MDM und Verwaltung. Navigieren Sie unter datomo MDM auf Einstellungen, öffnen die Registerkarte Richtlinien und dann den TAB Sicherheitsrichtlinie.

Hier sehen Sie, dass es bereits eine Default Security Policy gibt. Diese Sicherheitsrichtlinie ist das Herzstück für die Behandlung von Einstellungen (Restriktionen für Anwendungen, Hardware, Mobilfunk usw.). Jedes Gerät in der datomo MDM Lösung erhält explizit eine Sicherheitsrichtlinie. Das bedeutet, dass Sie entweder nur mit einer Sicherheitsrichtlinie arbeiten oder auch mehrere Sicherheitsrichtlinien erstellen können. Um eine Sicherheitsrichtlinie zu konfigurieren klicken Sie entweder auf den Namen der Richtlinie oder rechts auf das Symbol Bearbeiten (s. Abb. 1).

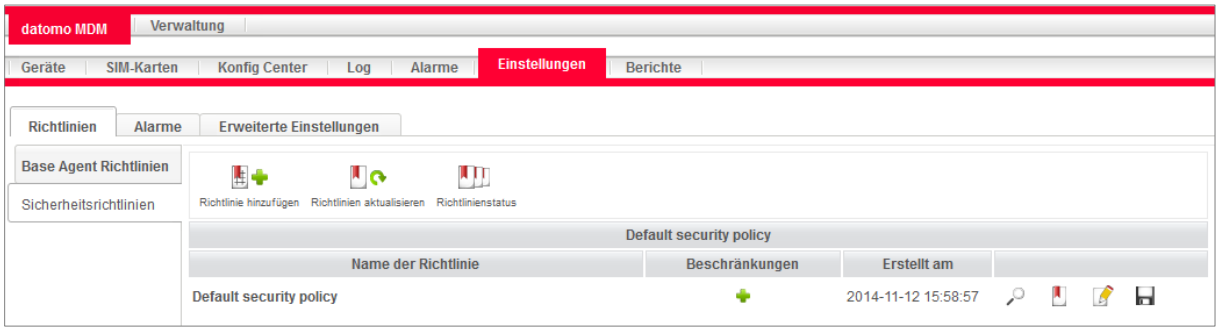

Abb. 1 Sicherheitsrichtlinie

Es erscheint das Menü Sicherheitsrichtlinie bearbeiten.

Als erstes wird Ihnen der Vorlagenname angezeigt, den Sie jederzeit ändern können. Dazu wird Ihnen das Feld Priorisierung angezeigt (später hierzu mehr). Wichtig ist folgende Option (s. Abb. 2):

Richtlinie automatisch auf dem Gerät aktualisieren:
Bestimmt, ob die Geräte Änderungen an der Richtlinie automatisch aktualisieren oder ob die Sicherheitsrichtlinie durch den Administrator via Push aktualisiert werden muss.

- Keine Aktivierung (Standard), sonst Haken setzen.

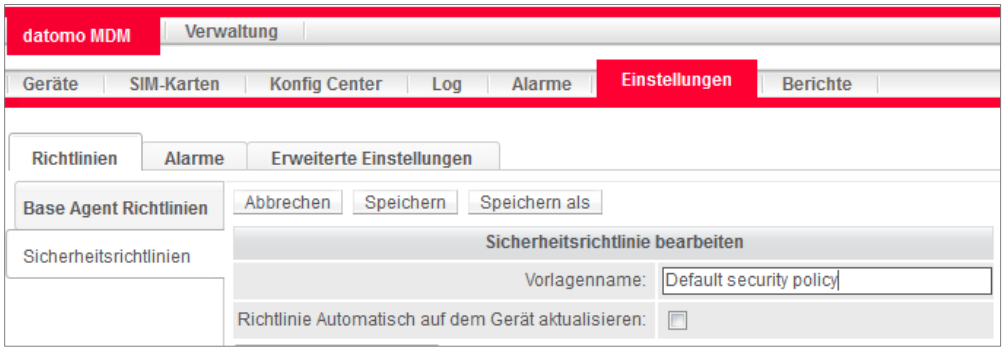

Abb. 2 Sicherheitsrichtlinie - Bearbeiten

Die Sicherheitsrichtlinie besteht aus 2 einzelnen TABs (Haupteinstellungen und Anwendungseinstellungen) (s. Abb. 3). Sobald Sie eine zweite Sicherheitsrichtlinie erstellen, wird Ihnen zusätzlich der TAB Gruppen angezeigt (s. Abb. 4).

Sie können alle Tabs in einem Ablauf konfigurieren und am Ende einmal speichern oder jederzeit mit einem Klick auf Speichern Ihre Einstellungen sichern.

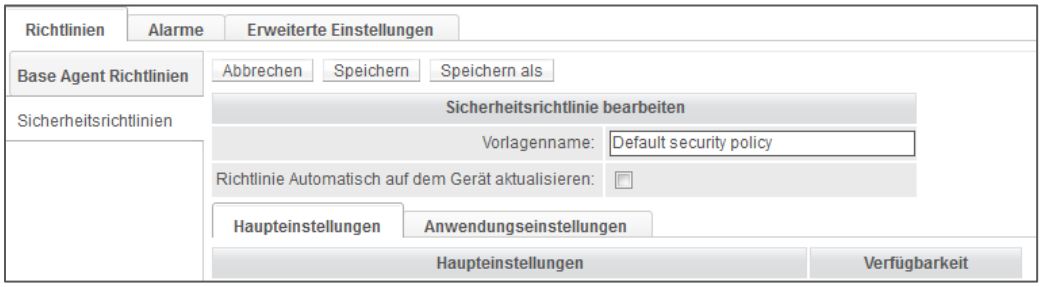

Abb. 3 Sicherheitsrichtlinie – TABs

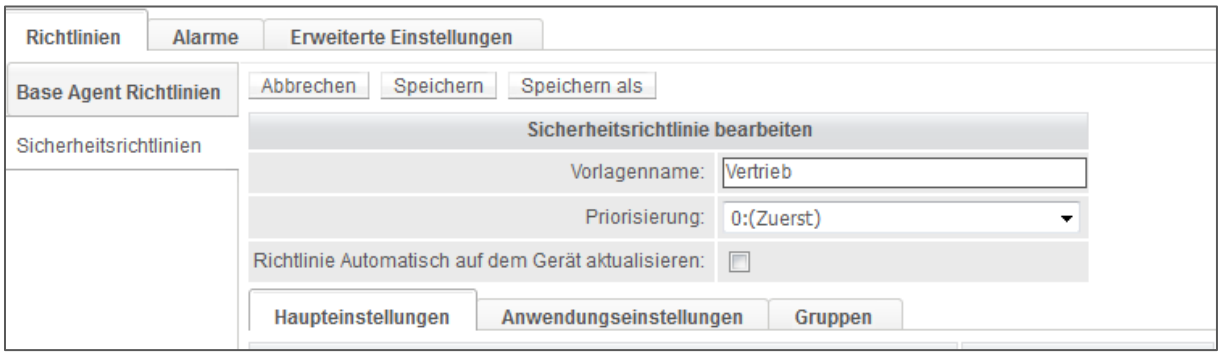

Abb. 4 Sicherheitsrichtlinie – TABs

TAB 1: Haupteinstellung:

Der TAB Haupteinstellung ist in 5 Bereiche aufgeteilt (Wipe, Netzwerk, Lokalisierung, Hardware, Verschlüsselung). Sie sehen unter Haupteinstellung die Funktionen, die Sie aktivieren/deaktivieren können und unter Verfügbarkeit die Plattform, die diese Funktion unterstützen (s. Abb. 5).

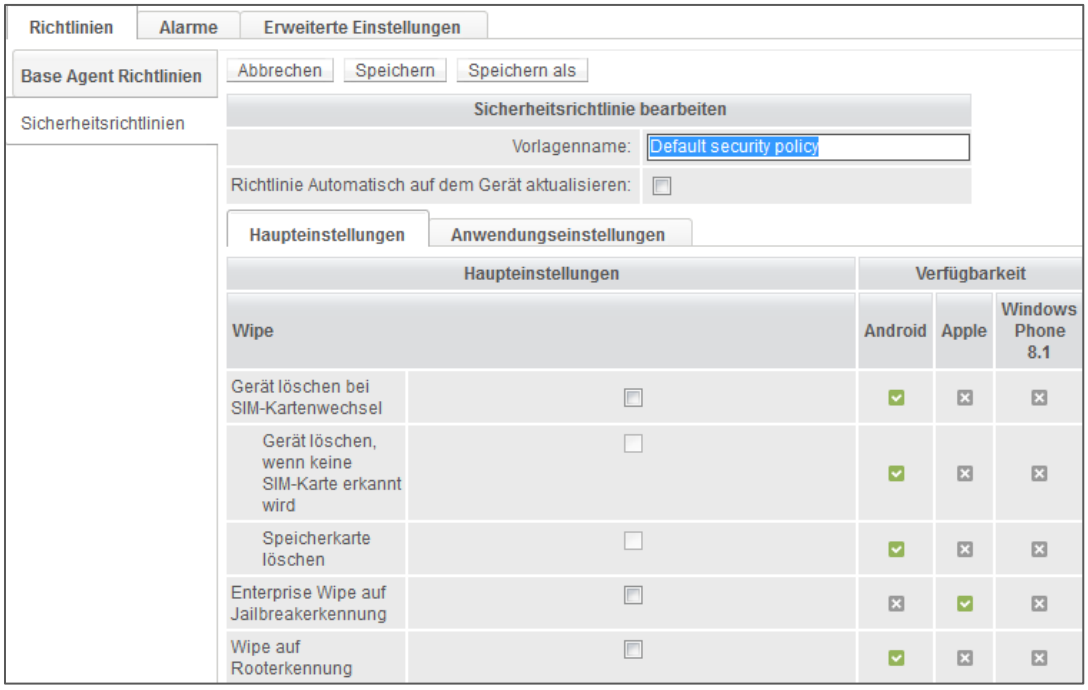

Abb. 5 Sicherheitsrichtlinie Funktion/Verfügbarkeit

Das Sternchen bei einem grünen Haken bedeutet, dass Sie hier weitere Plattformdetails erfahren, wenn Sie den Mauszeiger auf diesen grünen Haken bewegen (S. Abb. 6)

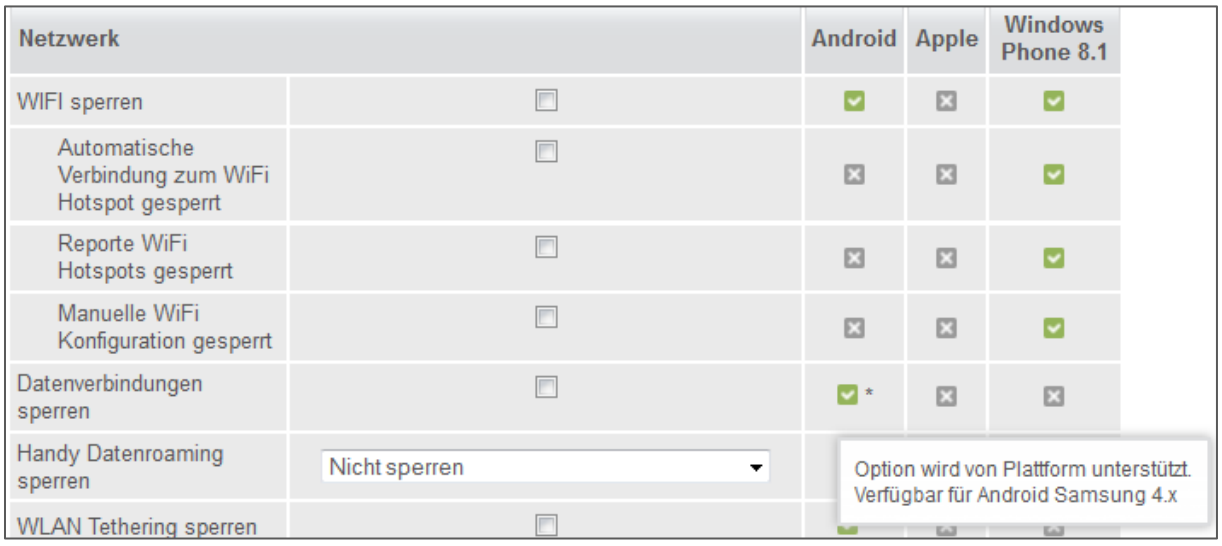

Abb. 6 Sicherheitsrichtlinie Plattformdetails

WIPE (s. Abb. 7):

Gerät löschen bei SIM-Kartenwechsel

Bestimmt, ob ein Gerät automatisch gewiped wird wenn SIM-Karten Wechsel registriert wird.

- Keine Aktvierung (Standard), sonst Haken setzen

Gerät löschen, wenn keine SIM-Karte erkannt wird

Bestimmt, ob ein Gerät automatisch gewiped wird, wenn keine SIM-Karte erkannt wird. (Achtung: wird der Flugmodus aktiviert erkennt der Agent auf dem Gerät keine SIM Karte mehr und das Gerät würde gewiped werden.)

- Keine Aktvierung (Standard), sonst Haken setzen

Speicherkarte löschen

Bestimmt, ob bei einem Wipe aus den beiden vorherigen Funktionen auch die Speicherkarte mitgelöscht wird.

- Keine Aktvierung (Standard), sonst Haken setzen

Enterprise Wipe auf Jailbreakerkennung

Bestimmt, ob ein gejailbreaktes Gerät automatisch mit einem Enterprise Wipe versehen wird.

- Keine Aktvierung (Standard), sonst Haken setzen

Wipe auf Rooterkennung

Bestimmt, ob ein gerootetes Gerät automatisch gewiped wird.

- Keine Aktvierung (Standard), sonst Haken setzen

Abb. 7 Sicherheitsrichtlinie – Wipe

Netzwerk (s. Abb. 8):

Wi-Fi sperren

Bestimmt, ob WLAN auf den Geräten deaktiviert wird.

- Keine Aktvierung (Standard), sonst Haken setzen

Automatische Verbindung zum Wi-Fi Hotspot gesperrt

Bestimmt, ob Verbindungen zu Wi-Fi Hotspots automatisch geöffnet werden.

- Keine Aktvierung (Standard), sonst Haken setzen

Reporte Wi-Fi Hotspots gesperrt

Bestimmt, ob verfügbare Wi-Fi Hotspots auf dem Gerät angezeigt werden.

- Keine Aktvierung (Standard), sonst Haken setzen

Manuelle Wi-Fi Konfiguration gesperrt

Bestimmt, ob die manuelle Konfiguration von WLAN Verbindungen gesperrt ist.

- Keine Aktvierung (Standard), sonst Haken setzen

Datenverbindungen sperren

Bestimmt, ob mobile Datenverbindungen verfügbar sind.

- Keine Aktvierung (Standard), sonst Haken setzen

Handy Datenroaming sperren

Bestimmt, ob Datenroaming gesperrt ist

- Nicht sperren (Standard)
- Deaktivieren und Aktivierung verhindern

WLAN Tethering sperren

Bestimmt, ob WLAN Tethering möglich ist.

- Keine Aktvierung (Standard), sonst Haken setzen

USB Tethering sperren

Bestimmt, ob USB Tethering möglich ist.

- Keine Aktvierung (Standard), sonst Haken setzen

Gemeinsame Nutzung des Internets gesperrt

Bestimmt, ob eine Internetverbindung geteilt werden kann

- Keine Aktvierung (Standard), sonst Haken setzen

VPN über Mobilfunk gesperrt

Bestimmt, ob VPN Verbindungen über das mobile Datennetz aufgebaut werden können.

- Keine Aktvierung (Standard), sonst Haken setzen

Gerätenutzungsreport an Microsoft gesperrt

Bestimmt, ob das Gerät Nutzungsdaten an Microsoft meldet

- Keine Aktvierung (Standard), sonst Haken setzen

Roaming VPN über Mobilfunk gesperrt

Bestimmt, ob VPN Verbindungen über das mobile Datennetz im Roaming Modus aufgebaut werden können.

- Keine Aktvierung (Standard), sonst Haken setzen

Netzwerk		Android	Apple	Windows Phone 8.1
WIFI sperren	☐	☑	☒	☑
Automatische Verbindung zum WiFi Hotspot gesperrt	☐	☒	☒	☑
Reporte WiFi Hotspots gesperrt	☐	☒	☒	☑
Manuelle WiFi Konfiguration gesperrt	☐	☒	☒	☑
Datenverbindungen sperren	☐	☑ *	☒	☒
Handy Datenroaming sperren	Deaktivieren und Aktivierung verhindern	☑	☒	☑
WLAN Tethering sperren	☐	☑ *	☒	☒
USB Tehtering sperren	☐	☑ *	☒	☒
Gemeinsame Nutzung des Internets gesperrt	☐	☒	☒	☑
VPN über Mobilfunk gesperrt	☐	☒	☒	☑
Gerätenutzungsreport an Microsoft gesperrt	☐	☒	☒	☑
Roaming VPN über Mobilfunk gesperrt	☐	☒	☒	☑

Abb. 8 Sicherheitsrichtline - Netzwerk

Lokalisierung (s. Abb. 9):

GPS Steuerung

Bestimmt, wie die GPS Funktionen auf dem Gerät verwendet werden.

- Nicht sperren (Standard)
- GPS aktivieren
- GPS aktivieren und Deaktivierung verbieten
- GPS deaktivieren
- GPS deaktivieren und Aktivierung verhindern

Lokalisierung gesperrt

Bestimmt, ob Lokalisierung auf dem Gerät verboten ist.

- Keine Aktvierung (Standard), sonst Haken setzen

Lokalisierung		Android	Apple	Windows Phone 8.1
GPS Steuerung	Nicht sperren	☑ *	☒	☒
Lokalisierung gesperrt	☐	☒	☒	☑

Abb. 9 Sicherheitsrichtline - Lokalisierung

Hardware (s. Abb. 10):

Bluetooth gesperrt

Bestimmt, ob Bluetooth auf dem Gerät verfügbar ist.

- Keine Aktvierung (Standard), sonst Haken setzen

Anwendung zur Sprachaufzeichnung gesperrt

Bestimmt, ob Sprachassistenten genutzt werden können.

- Keine Aktvierung (Standard), sonst Haken setzen

Kamera sperren

Bestimmt, ob die Kamera auf dem Gerät genutzt werden darf

- Keine Aktvierung (Standard), sonst Haken setzen

Deaktivierungssperre des Geräteadministrators

Bestimmt, ob der Geräteadministrator auf Gerät deaktiviert werden kann.

- Keine Aktvierung (Standard), sonst Haken setzen

USB Debugging sperren

Bestimmt, ob auf dem Gerät USB-Debugging aktiviert werden darf.

- Keine Aktvierung (Standard), sonst Haken setzen

USB Mediaplayer sperren

Bestimmt, ob das Gerät per USB als Audioquelle genutzt werden darf.

- Keine Aktvierung (Standard), sonst Haken setzen

OTA Update sperren

Bestimmt, ob das Gerät OTA (Over The Air) Updates (Firmware) laden und installieren darf.

- Keine Aktvierung (Standard), sonst Haken setzen

Zurücksetzen auf Werkseinstellungen

Bestimmt, ob das Gerät über die Einstellung und Klammergriff auf Werkseinstellung zurückgesetzt werden darf.

- Keine Aktvierung (Standard), sonst Haken setzen

Sperre Entwicklungsmodus

Bestimmt, ob auf dem Gerät Entwicklerfunktionen aktiviert werden dürfen.

- Keine Aktvierung (Standard), sonst Haken setzen

Sperre des Task Managers

Bestimmt, ob der Taskmanager auf dem Gerät verfügbar ist.

- Keine Aktvierung (Standard), sonst Haken setzen

Unbekannte Quellen gesperrt

Bestimmt, ob die unbekannten Quellen auf dem Gerät aktiviert werden dürfen.

- Keine Aktvierung (Standard), sonst Haken setzen

NFC gesperrt

Bestimmt, ob NFC auf dem Gerät verfügbar ist.

- Keine Aktvierung (Standard), sonst Haken setzen

Sperre der Speicherkarte

Bestimmt, ob Speicherkarten verfügbar sind.

- Keine Aktvierung (Standard), sonst Haken setzen

Copy & paste lock

Bestimmt, ob auf dem Gerät Kopieren/Einfügen verfügbar ist.

- Keine Aktvierung (Standard), sonst Haken setzen

Bildschirm Fotos gesperrt

Bestimmt, ob auf dem Gerät Screenshots erlaubt sind.

- Keine Aktvierung (Standard), sonst Haken setzen

USB Dateimanager gesperrt

Bestimmt, ob der Dateimanager über USB verfügbar ist.

Keine Aktvierung (Standard), sonst Haken setzen

Hardware		Android	Apple	Windows Phone 8.1
Bluetooth gesperrt	☐	☑	☒	☑
Anwendung zur Sprachaufzeichnung gesperrt	☐	☑ *	☒	☑
Kamera sperren	☐	☑ *	☒	☑
Deaktivierungssperre des Geräteadministrators	☐	☑ *	☒	☒
USB Debugging sperren	☐	☑ *	☒	☑
USB Mediaplayer sperren	☐	☑ *	☒	☒
OTA Update sperren	☐	☑ *	☒	☒
Zurücksetzen auf Werkseinstellungen	☐	☑ *	☒	☑
Sperre Entwicklungsmodus	☐	☑ *	☒	☒
Sperre des Task Managers	☐	☑ *	☒	☒
Unbekannte Quellen gesperrt	☐	☑ *	☒	☒
NFC gesperrt	☐	☒	☒	☑
Sperre der Speicherkarte	☐	☑ *	☒	☑
Copy & paste lock	☐	☒	☒	☑
Bildschirm Fotos gesperrt	☐	☒	☒	☑
USB Dateimanager gesperrt	☐	☒	☒	☑

Abb. 109 Sicherheitsrichtline – Hardware

Verschlüsselung (s. Abb. 11):

Verschlüsselung interner Speicher

Bestimmt, ob die interne Speicherverschlüsselung erzwungen wird.

- Keine Aktvierung (Standard), sonst Haken setzen

Verschlüsselung		Android	Apple	Windows Phone 8.1
Verschlüsselung interner Speicher	☐	☑ *	☑	☑
Abbrechen Speichern				

Abb. 11 Sicherheitsrichtlinie - Verschlüsselung

TAB 2: Anwendungseinstellung

Der TAB Anwendungseinstellungen ist in 5 Bereiche aufgeteilt (Installation, Anwendungen, Kennwortschutz von Anwendungen, Individuelle Benachrichtigungen und Android). Sie sehen unter Haupteinstellung die Funktionen, die Sie aktivieren/deaktivieren können und unter Verfügbarkeit die Plattform, die diese Funktionen unterstützen. Das Sternchen bei einem grünen Haken bedeutet, dass Sie hier weitere Plattformdetails erfahren, wenn Sie den Mauszeiger auf diesen grünen Haken bewegen (S. Abb. 12).

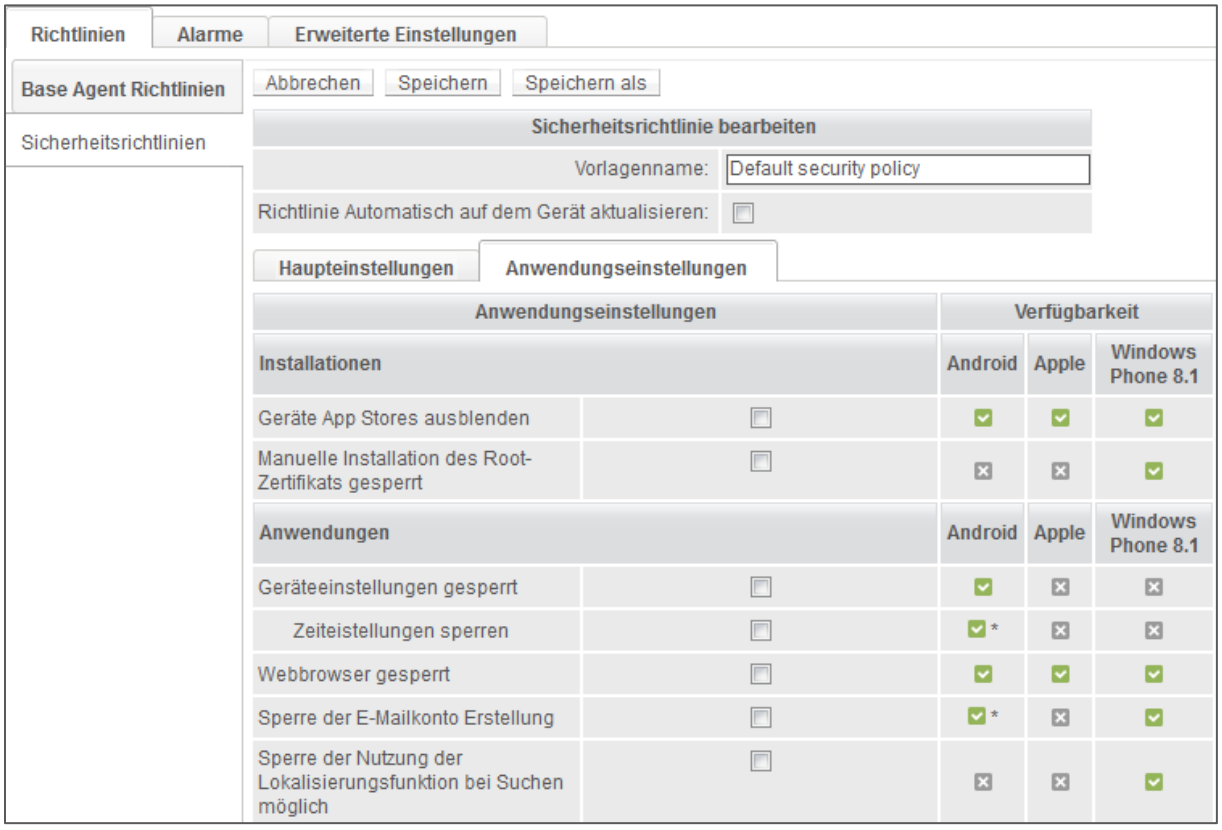

Abb. 12 Sicherheitsrichtline – Anwendungseinstellungen

Installationen (s. Abb. 13):

Geräte App-Stores ausblenden

Bestimmt, ob die nativen App-Stores auf den Geräten verfügbar sind.

- Keine Aktvierung (Standard), sonst Haken setzen

Manuelle Installation des Root- Zertifikats gesperrt

Bestimmt, ob manuell Zertifikate in den Root Speicher installiert werden dürfen.

- Keine Aktvierung (Standard), sonst Haken setzen

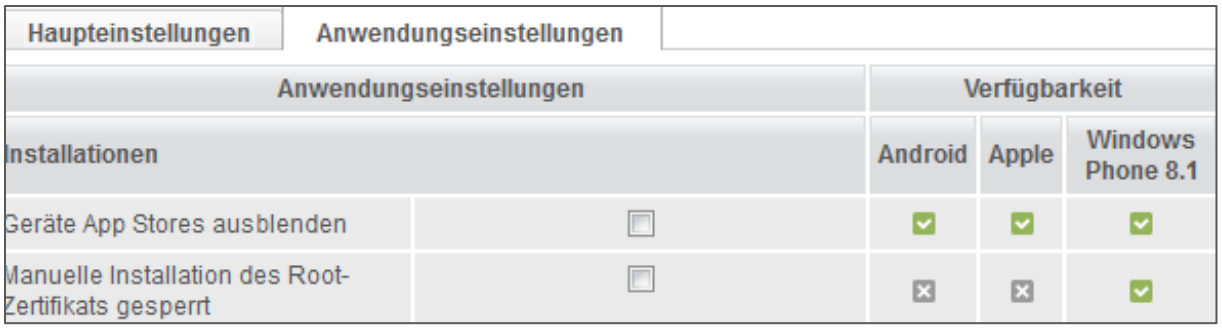

Abb. 13 Anwendungseinstellung – Installation

Anwendungen (s. Abb. 15):

Geräteeinstellungen gesperrt

Bestimmt, ob die Einstellungen auf dem Gerät verfügbar sind.

- Keine Aktvierung (Standard), sonst Haken setzen

Zeiteistellungen sperren

Bestimmt, ob auch die Zeiteinstellung auf dem Gerät gesperrt sind. (Nur verfügbar, wenn die Einstellungen gesperrt sind)

- Keine Aktvierung (Standard), sonst Haken setzen

Webbrowser gesperrt

Bestimmt, ob die nativen Webbrowser auf dem Gerät verfügbar sind.

- Keine Aktvierung (Standard), sonst Haken setzen

Sperre der E-Mail Kontoerstellung

Bestimmt, ob auf dem Gerät manuell Mailkonten hinzugefügt werden können.

- Keine Aktvierung (Standard), sonst Haken setzen

Sperre der Nutzung der Lokalisierungsfunktion bei Suchen möglich

Bestimmt, ob die lokale Geräte Suche auf Standortdaten des Gerätes zurückgreifen darf.

- Keine Aktvierung (Standard), sonst Haken setzen

Speichern als Funktionalität in Microsoft Office Sperre

Bestimmt, ob Dateien in Office Programmen unter einem anderen Namen gespeichert werden dürfen.

- Keine Aktvierung (Standard), sonst Haken setzen

Funktionalität, Daten zu teilen, ist in Outlook gesperrt

Bestimmt, ob Daten aus Outlook in weiteren Programmen genutzt (geteilt) werden dürfen.

- Keine Aktvierung (Standard), sonst Haken setzen

Windows Phone application policy

- Legen Sie fest ob für Windows Phone Geräte die Anwendungsliste als Whiteliste oder Blacklist konfiguriert wird.

Anwendungen		Android	Apple	Windows Phone 8.1
Geräteeinstellungen gesperrt	☐	☑	☒	☒
Zeiteistellungen sperren	☐	☑*	☒	☒
Webbrowser gesperrt	☐	☑	☑	☑
Sperre der E-Mailkonto Erstellung	☐	☑*	☒	☑
Sperre der Nutzung der Lokalisierungsfunktion bei Suchen möglich	☐	☒	☒	☑
Speichern als Funktionalität in Microsoft Office Sperre	☐	☒	☒	☑
Funktionalität Daten zu teilen ist in Outlook gesperrt	☐	☒	☒	☑
Windows Phone application policy	Block applications on the list	☒	☒	☑

Abb. 14 Sicherheitsrichtline – Anwendungen

Kennwortschutz von Anwendung (s. Abb. 15):

Kennwort erforderlich, um auf Anwendungen zuzugreifen

Bestimmt, ob beim Zugriff auf Anwendungen ein weiteres Kennwort angegeben werden muss.

- Fragt nicht nach Passwort (Standard)
- Nach Sperrcode fragen (Gerätekennwort)
- Nach Passwort fragen (Administrator Kennwort s. Base Agent Richtlinie)

Anmeldezeit für Passwort überschritten

Bestimmt, nach welchem Zeitraum der Inaktivität der Anwendung das Kennwort erneut angefordert wird.

- 5 Minuten (Standard)
- 1 Minute
- 10 Minuten
- 15 Minuten

Kennwortschutz von Anwendung		Android	Apple	Windows Phone 8.1
Kennwort erforderlich, um auf Anwendungen zuzugreifen	Fragt nicht nach Passwort	☑	☒	☒
Anmeldezeit für Passwort überschritten	5 Minuten	☑	☒	☒

Abb. 15 Sicherheitsrichtline - Kennwortschutz von Anwendung

Individuelle Benachrichtigungen (s. Abb. 16):

Benachrichtigung, wenn die Installation gesperrt ist.
Bestimmt die Mitteilung, die auf dem Gerät angezeigt wird, wenn die Installation von Anwendungen auf dem Gerät gesperrt ist.
- Installation der Anwendung ist nicht erlaubt (Standard)

Nachricht die angezeigt wird, wenn eine Anwendung durch ein Kennwort gesperrt wurde
Bestimmt die Mitteilung, die auf dem Gerät angezeigt wird, wenn der Zugriff auf eine Anwendung ein Kennwort erfordert.
- Bitte geben Sie das Kennwort ein, um diese Anwendung zu benutzen (Standard)

Benachrichtigung, wenn Applikation auf der Blacklist steht
Bestimmt die Mitteilung, die auf dem Gerät angezeigt wird wenn die Verwendung einer Anwendung verboten ist.
- Anwendung ist nicht erlaubt (Standard)

Individuelle Benachrichtigungen		Android	Apple	Windows Phone 8.1
Benachrichtigung, wenn die Installation gesperrt ist.	Installation der Anwendung ist nicht erlaubt	☑	☒	☒
Nachricht die angezeigt wird, wenn eine Anwendung durch ein Kennwort gesperrt wurde	Bitte geben Sie das Kennwort ein, um diese Anwe	☑	☒	☒
Benachrichtigung, wenn Applikation auf der Blacklist steht	Anwendung ist nicht erlaubt	☑	☒	☒

Abb. 16 Sicherheitsrichtlinie – Individuelle Benachrichtigungen

Android (s. Abb. 17):

In diesem Bereich können Sie Anwendungen auswählen und bestimmen, wie diese auf dem Gerät behandelt werden. Klicken Sie als erstes auf Anwendung hinzufügen (s. Abb. 16)

Abb. 17 Sicherheitsrichtlinie – Android

Sie sehen ein kleines Fenster in dem Sie aufgefordert werden, eine Anwendung auszuwählen. Beginnen Sie, in das freie Feld einen Namen einzugeben z.B. Google. Unterhalb Ihrer Eingabe erscheint ein Dropdown Menü mit passenden Einträgen (s. Abb. 18). Die angezeigten Anwendungen kommen von den Gerätemonitordaten Ihrer Geräte. Wählen Sie z.B. die Anwendung „com.google.android.apps.books“ aus und klicken auf Hinzufügen(s. Abb. 19).

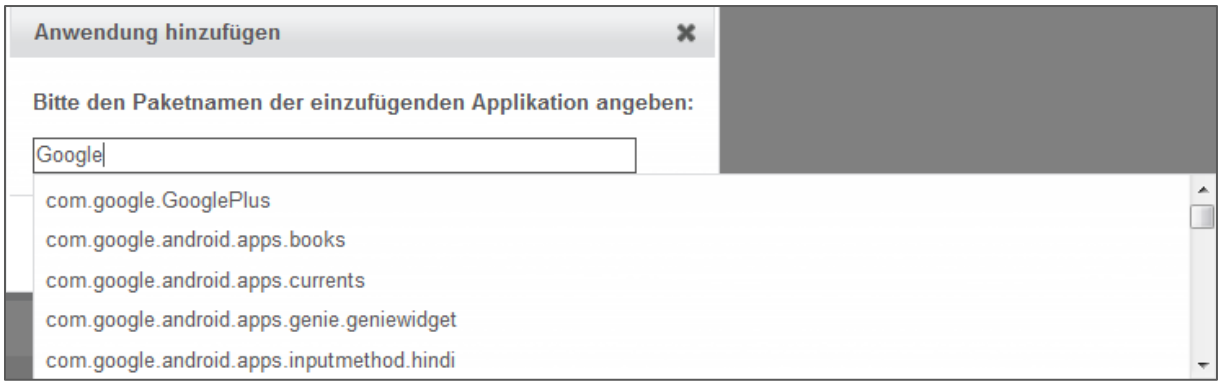

Abb. 18 Android – Anwendung suchen

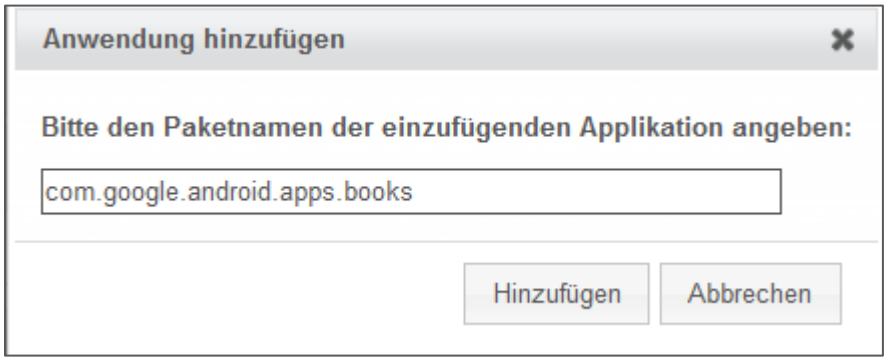

Abb. 19 Android – Anwendung hinzufügen

Sie sehen jetzt, dass die Anwendung in der Liste angezeigt wird. Sie können jetzt 3 unterschiedliche Kriterien festlegen, wie diese Anwendung auf dem Gerät behandelt wird.

1. **Blacklist** (s. Abb. 20):
   Blockiert den Zugriff auf diese Anwendung. Je nach Android Plattform wird die Anwendung ausgeblendet auf dem Gerät oder es erscheint die individuelle Benachrichtigung. Wenn Sie diese Option setzten, sind die anderen beiden Möglichkeiten ausgegraut.
   - Keine Aktvierung (Standard), sonst Haken setzen

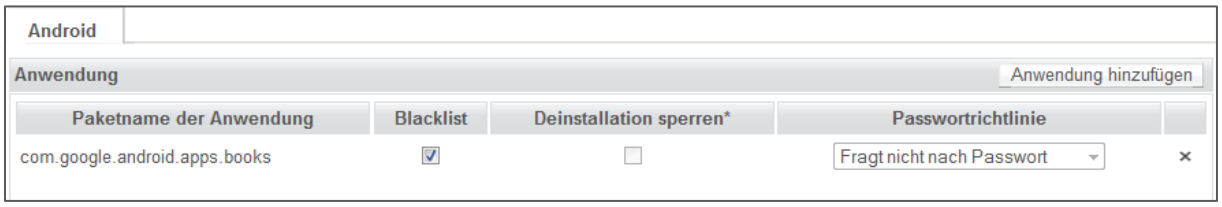

Abb. 20 Android – Blacklist

2. **Deinstallation sperren** (s. Abb. 21):
   Verhindert die Deinstallation der Anwendung durch den Benutzer (nur Samsung Android). Wenn Sie diese Option setzten, sind die anderen beiden Möglichkeiten ausgegraut.
   - Keine Aktvierung (Standard), sonst Haken setzen

Abb. 21 Android – Deinstallation sperren

3. **Passwortrichtlinie** (s. Abb. 22):

Bestimmt, ob der Zugriff auf diese Anwendung freizugänglich oder mit einem Kennwort geschützt ist. Diese Einstellungen können mit der Funktion „Deinstallation sperren“ kombiniert werden.

- Fragt nicht nach Passwort (Standard)
- Nach Sperrcode fragen
- Nach Admin Password fragen

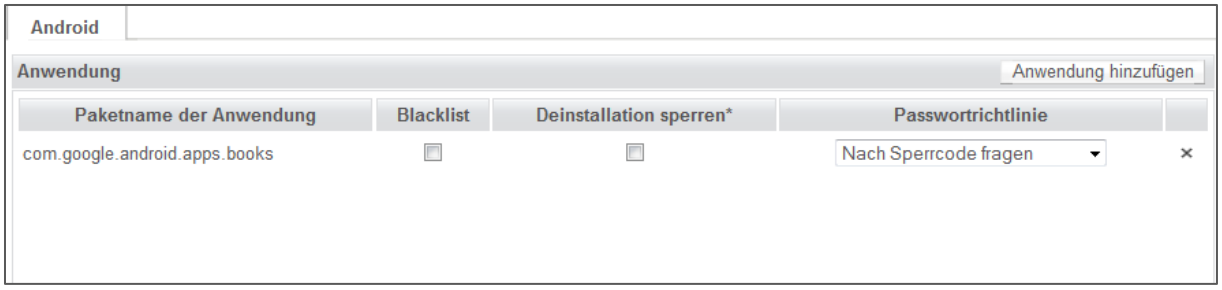

Abb. 22 Android - Passwortrichtlinie

4. **Anwendung Beenden Sperren / Daten löschen sperren** (s. Abb. 23)
   Bestimmt, ob eine Anwendung beendet oder deren Cache Daten gelöscht werden dürfen.

Abb. 23 Android – Beenden / Daten löschen

5. **Windows Phone Anwendungen** (s. Abb. 24)
   In diesem Bereich können Sie Anwendungen auswählen und bestimmen, wie diese auf dem Gerät behandelt werden. Klicken Sie als erstes auf Anwendung hinzufügen.

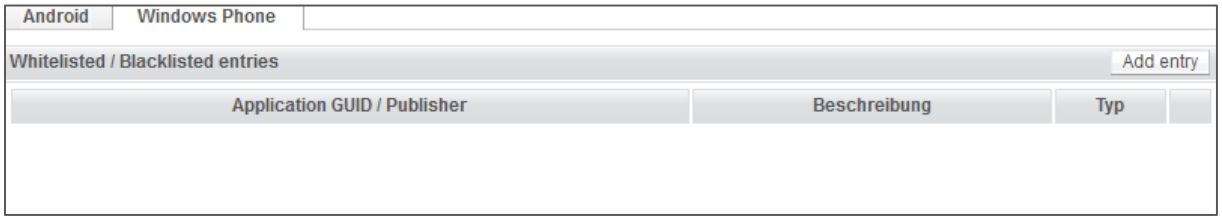

Abb. 24 Windows Phone

Sie sehen ein kleines Fenster in dem Sie aufgefordert werden, eine Anwendung auszuwählen. Hinterlegen Sie hier entweder die Entwickler ID oder die GUID (s. Abb. 25). Wie Sie diese Daten ermitteln, wird in einem separaten Add-On Beschrieben. Nach dem Sie auf Hinzufügen geklickt haben, wählen Sie auch ob es sich um eine GUID oder einen Entwickler handelt (s. Abb. 26).

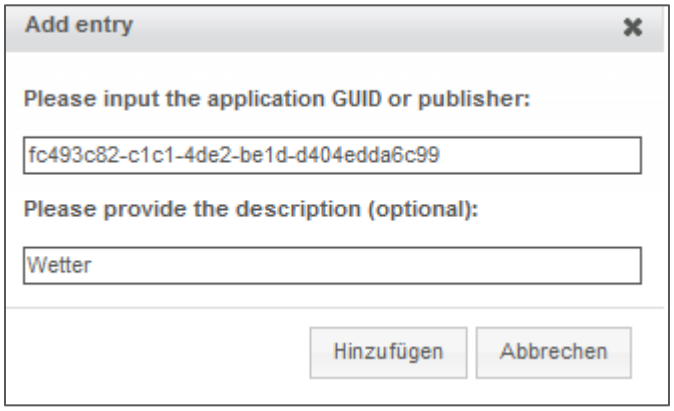

Abb. 25 Entwickler / GUID angeben

Abb. 26 Auswahl Entwickler / Anwendung

TAB 3 Gruppen (s. Abb. 27):

Nutzergruppe hinzufügen:
Hier können Sie alle Gruppen auswählen, die Sie unter Verwaltung – Gruppen im System angelegt haben. Dieser TAB wird nur bei einer neuen oder kopierten Base Agent Richtlinie angezeigt

Speichern Sie nun Ihre Einstellungen.

Abb.27 Gruppen

2. Sicherheitsrichtlinie organisieren/ steuern

Nachdem Sie die Sicherheitsrichtline gespeichert haben sehen Sie wieder die Übersicht der Sicherheitsrichtlinie. Hier haben Sie den Namen der Richtlinie das Beschränkungsfeld 4 Symbole (s. Abb. 28):

Symbole:
Zeigt eine Vorschau der Richtlinie an

Zeigt den Status der Richtlinie an

Öffnet die Richtlinie zur Bearbeitung

Speichern als Funktion, um eine Kopie der Richtlinie zu erstellen

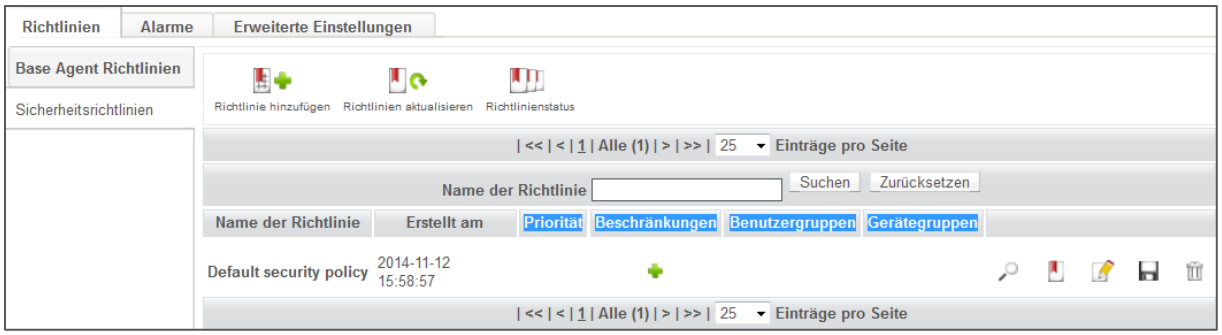

Abb. 28 Sicherheitsrichtline

Eine weitere Richtlinie erstellen Sie entweder als neue Richtlinie, indem Sie auf Richtlinie hinzufügen klicken oder das Disketten Symbol zum Kopieren einer vorhanden Richtlinie anklicken (s. Abb. 29).

Abb. 29 Speichern als

Sie werden aufgefordert, einen Namen der Richtlinie zu vergeben. Die Priorisierung dieser Richtlinie sollte auf Zuerst stehen (s. Abb. 30). Klicken Sie nun auf Speichern.

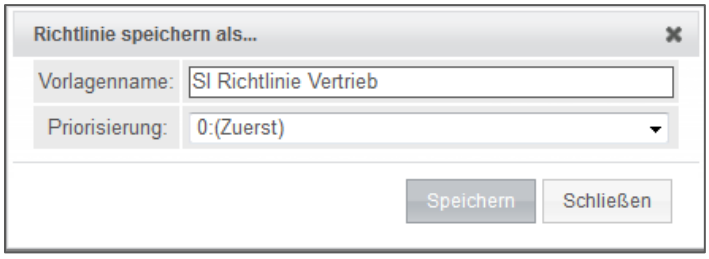

Abb. 30 Namen festlegen

Anschließend sehen Sie wieder die Richtlinien Übersicht und einige weitere Felder. Klicken Sie auf Bearbeiten der SI Richtlinie Vertrieb (s. Abb. 31).

Priorität:

Bestimmt die Reihenfolge der Sicherheitsrichtlinie. Das System arbeitet immer von oben nach unten. Somit ist die „unterste“ Richtlinie immer die letzte Richtlinie.

Beschränkungen:

Hier können Sie definieren, dass in bestimmten Zeitfenstern oder anhand von Lokalisierungsdaten andere Parameter der Sicherheitsrichtlinie gelten.

Benutzergruppen:

Bestimmt, welche Benutzergruppe(n) diese Sicherheitsrichtlinie zugewiesen bekommen.

Symbole:

Zeigt eine Vorschau der Richtlinie an

Zeigt den Status der Richtlinie an

Öffnet die Richtlinie zur Bearbeitung

Speichern als Funktion, um eine Kopie der Richtlinie zu erstellen

Löscht die Richtlinie

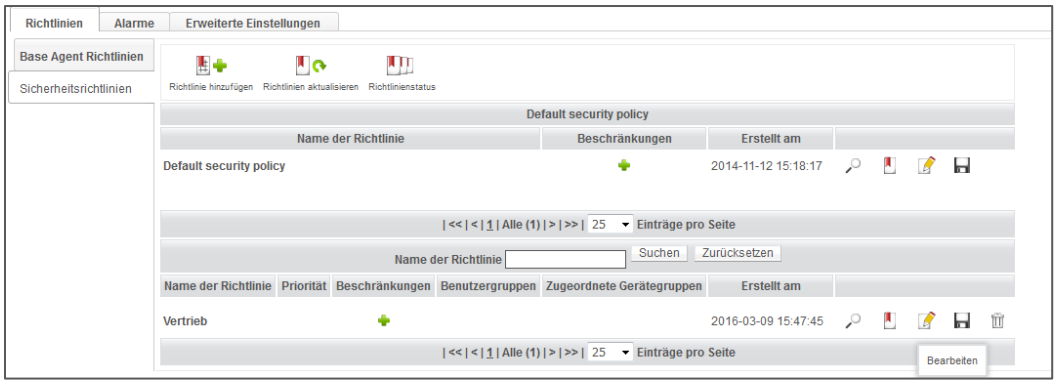

Abb. 31 Bearbeiten

Führen Sie die Änderungen in der Richtlinie durch, die Sie für den Vertrieb durchsetzen wollen und weisen unter dem TAB Gruppen die entsprechende Benutzergruppe zu. Speichern Sie anschließend die Richtlinie (s. Abb. 32).

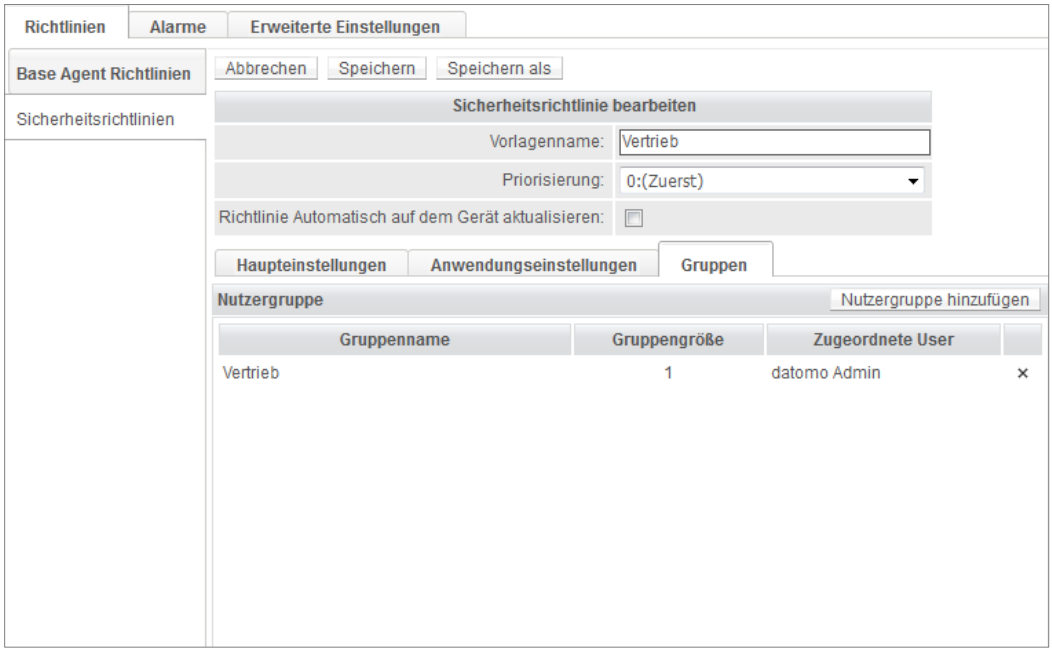

Abb. 32 Gruppe zuweisen

In der Übersicht sehen Sie jetzt die Struktur der Richtlinien. Die Vertrieb Security Richtlinie ist die erste mit der Zuweisung einer bestimmten Gruppe (Vertrieb). Alle anderen Geräte erhalten die Default security policy (s. Abb. 33).

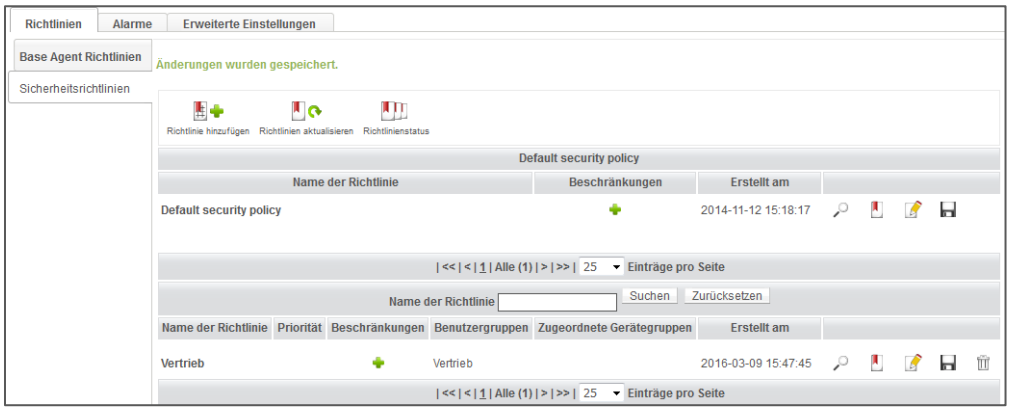

Abb. 33 Sicherheitsrichtlinie - Ansicht

3. Aktualisierung der Sicherheitsrichtlinie

Die Sicherheitsrichtlinie können Sie jederzeit durch einen Klick auf Richtlinien via Push an die Geräte verteilen (Push), oder Sie warten den Synchronisierungsintervall der Geräte ab, damit sich die Geräte automatisch aktualisieren (Pull). Wenn Sie auf Richtlinien aktualisieren klicken, sehen Sie das bekannte Operationsmenü. Sie können wie gewohnt Geräte hinzufügen und die Operation planen. Mit einem Klick auf Senden starten Sie die Operation (s. Abb. 34).

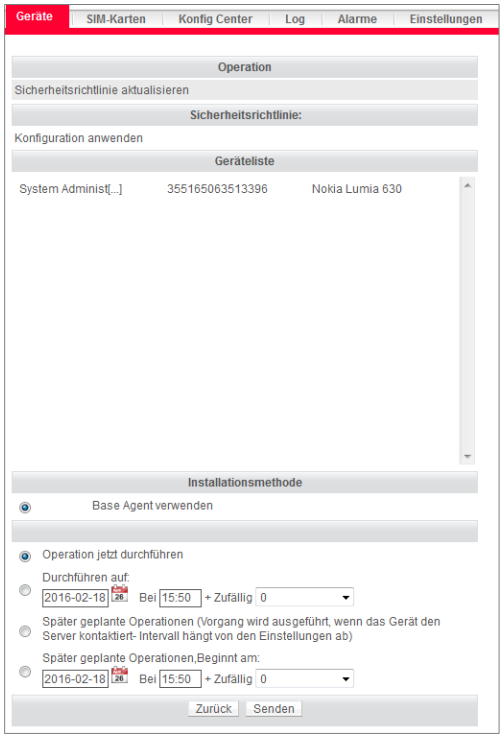

Abb. 34 Operation senden

4. Status Überwachung Sicherheitsrichtlinie

Mit einem Klick auf Richtlinienstatus (s. Abb. 35) wird Ihnen angezeigt, wie viele Geräte konform sind oder ob Sie als Administrator eingreifen müssen.

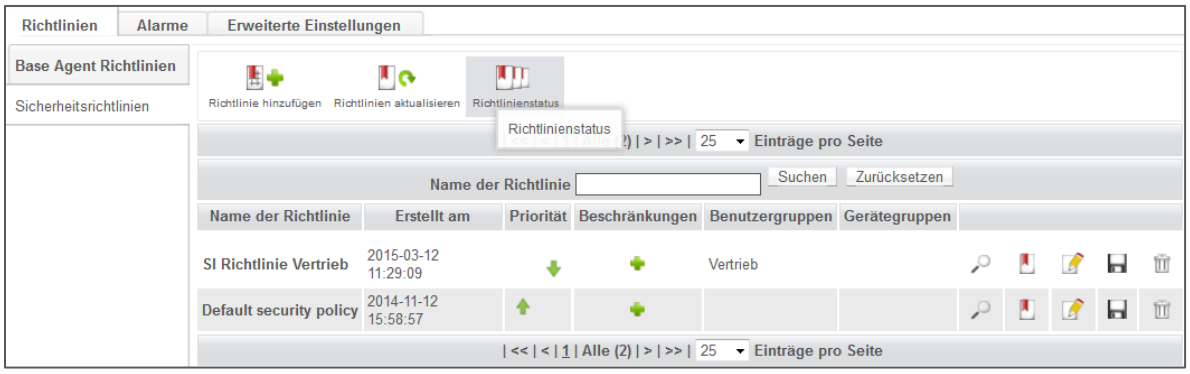

Abb.35 Richtlinienstatus

Mit einem Klick auf die Lupe werden Ihnen Geräteinformationen angezeigt. Mit einem Klick auf Richtlinien aktualisieren kommen Sie automatisch in das Operation Menü und die Geräte, die eine Aktualisierung erfordern, werden automatisch angezeigt.

Die einzelnen Status Meldungen sind (s. Abb. 36):

Geräte, die einer Richtlinie zugeordnet sind:
- Anzahl der verwalteten Geräte.

Konforme Geräte:
- Geräte, die mit der Sicherheitsrichtlinie übereinstimmen.

Geräte mit nicht-konformen Richtlinien:
- Geräte, die Änderungen der Base Agent Richtlinie noch nicht umgesetzt haben.

Geräte, auf denen die Richtlinie fehlgeschlagen ist:
- Geräte, die Probleme beim Aktualisieren der Base Agent Richtlinie haben.

Geräte, auf denen die Richtlinie noch nicht installiert ist:
- Geräte, die einen Sicherheitsrichtlinien Wechsel noch nicht durchgeführt haben.

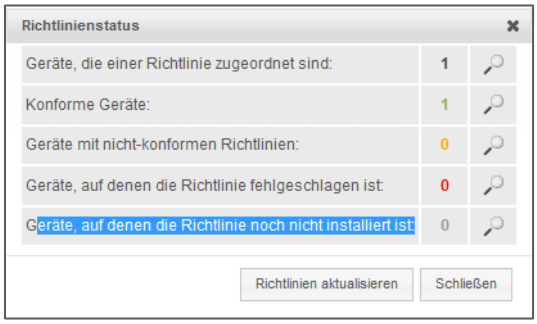

Abb.36 Richtlinienstatus

Sie haben nun erfolgreich gelernt, wie Sie eine Sicherheitsrichtlinie konfigurieren, kopieren, zuweisen, auf den Geräten aktualisieren und überwachen.

In weiteren „How To“ Anleitungen gehen wir auf weitere grundlegende Funktionen der Lösung ein, eine Übersicht über die Themen finden Sie unter **datomo – Versionen – Downloads.**