auralis
secure mobile device management

Handbuch

auralis 2.6

Hinweis – auralis im Univention App Center

auralis ist ab sofort auch im Univention App Center verfügbar.

Einige der hier aufgeführten Konfigurationen sind in in der Univention Version nicht verfügbar, da sie durch das Serversystem abgedeckt werden (IP, Updates, etc).

Der Port 443 für die externe Kommunikation ist in der Univention Version mit dem Port 7443 vorkonfiguriert. Achten Sie bei der Konfiguration der Firewall Regel darauf!

31.5.2016

1 auralis – secure mobile device management 3
1.1 Aufbau und Funktionen von auralis 3
1.2 Systemvoraussetzungen 4
2 Installation 5
2.1 Firewall Regeln 5
2.2 DNS – Fully Qualified Domain Name 6
2.3 Installationsumgebung 6
2.3.1 Virtuelle Maschine 6
2.3.2 Physikalische Maschine 6
2.4 Erster Start von auralis 7
2.5 Initiale Konfiguration 10
2.5.1 Konfigurationsassistent – Schritt 1 / 3 10
2.5.2 Konfigurationsassistent – Schritt 2 / 3 11
2.5.3 Konfigurationsassistent – Schritt 3 / 3 12
2.6 Apple Push Zertifikat erstellen 13
2.7 Lizenz einspielen 16
3 Administrationsoberfläche 17
3.1 Dashboard 17
3.2 Gruppen 18
3.2.1 Gruppenkonfigurationen 19
3.2.2 Allgemein 19
3.2.3 „iOS“, „Android“ und „Windows Phone“ 20
3.2.4 WiFi 20
3.2.5 SecureIntranet 20
3.2.6 Webclips 21
3.2.7 Compliance 21
3.2.8 TrafficControl 21
3.2.9 Apps 23
3.2.10 VPN 23
3.3 Benutzer 24
3.3.1 Benutzer anlegen 24
3.4 Geräte 27
3.5 Geräte hinzufügen 30
4 Geräte – Rollout 31
5 Globale Konfigurationen 31

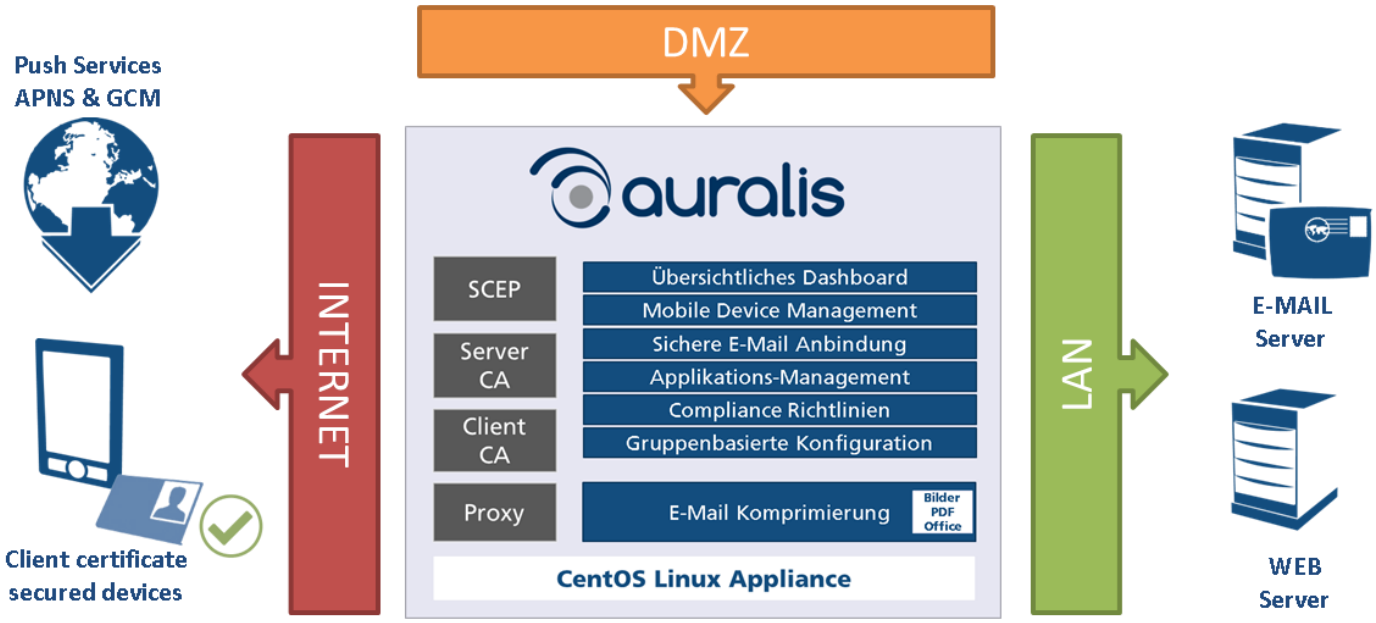
5.1 SecureIntranet 31
5.2 WiFi 34
5.3 VPN 35
5.4 APP Verwaltung 36
5.4.1 *iOS* 36
5.4.2 *Android* 36
5.5 Compliance 37
5.6 Reporting 40
6 Systemkonfiguration 41
6.1 Netzwerk 41
6.2 Groupware 43
6.3 eMail 44
6.4 SNMP 45
6.5 LDAP 46
6.6 Zertifikate 47
6.7 Push Dienste 50
6.7.1 Apple Push Dienst 51
6.7.2 Google Push Dienst 52
6.8 Apps 53
6.9 Erweiterte Konfiguration 53
7 Administratoren 55
8 Backup / Restore 57
9 Wartung 58
10 Logs 61
11 Update 62
12 Lizenz 64
13 Support 65
14 Über uns 65

1 auralis – secure mobile device management

auralis ist eine sichere Mobile Device Management Lösung. Durch den Einsatz von Client Zertifikaten für jedes Smartphone, ist sie perfekt geeignet um Ihre IT Infrastruktur wie Exchange (oder jede andere AcitveSync basierte Lösung wie Zarafa oder Kerio) und Webserver vor Man-In-The-Middle Attacken zu schützen. auralis ist so gesehen eine Firewall für Ihre E-Mail Infrastruktur.

1.1 Aufbau und Funktionen von auralis

auralis wird als ISO Installationsmedium ausgeliefert und ist optimal für den Einsatz auf einer virtuellen oder physikalischen Maschine in Ihrer DMZ vorgesehen. Die Basis von auralis ist ein gehärtetes Linux CentOS Betriebssystem welches mit jedem auralis Update von uns mitgewartet wird. Durch die Implementierung von SCEP, einer Server und Client CA, sowie eines Reverse Proxy, ist auralis komplett für den sofortigen Einsatz um Mobile Device Management effizient betreiben zu können. Sie müssen diese Dienste nachträglich nicht selbst in Ihre Infrastruktur integrieren.



1.2 Systemvoraussetzungen

Virtuelle oder Physikalische Maschine:

CPU: Minimum 1 CPU mit einem Kern.

Für den effizienten Einsatz unserer E-Mail Komprimierung empfehlen wir ab 50 Benutzern mindestens zwei CPUS oder zwei Kerne.

RAM: Minimum 4 GB RAM

Für den effizienten Einsatz unserer E-Mail Komprimierung empfehlen wir ab 50 Benutzern mindestens 8GB RAM

HDD: 1 Partition mit 20 GB Festplattenspeicher

Da während des Betriebes Logfiles geschrieben werden. Empfehlen wir mindestens 20GB Festplattenspeicher. Logfiles werden im Rotationsverfahren einerseits komprimiert, aber auch nach 6 Monaten gelöscht.

NIC: Eine Netzwerkkarte

Da auralis für die DMZ konzipiert ist, arbeitet auralis mit nur einer Netzwerkkarte und wird nicht Dual-Homed betrieben.

DNS: Öffentlicher DNS Name Ihrer Umgebung: auralis.example.com

2 Installation

Hinweis

Damit es während der Installation nicht zu Fehlermeldungen kommt, empfehlen wir vor der Installation die Erstellung der Firewall-Regeln sowie die Konfiguration des öffentlichen DNS Eintrages. Bei der Univention Version von auralis ist für die erste Regel der Port 7443 anstatt 443 vorkonfiguriert.

2.1 Firewall Regeln

Konfigurieren Sie Ihre Firewall auf folgenden Ports:

Source	Destination	Ports
any	[auralis]	80/TCP; 443/TCP; 8443/TCP
[auralis]	[DNS-Server (LAN)]	53/UDP
[auralis]	[any oder konfigurierter NTP-Server (LAN)]	123/UDP
[auralis]	17.0.0.0/8 (Apple Push Service)	2195; 2196; 5223; 443/TCP
[auralis]	[Exchange-Server (LAN)]	443/TCP*
[auralis]	[SMTP-Server (LAN)]	25/TCP
[auralis]	[Active Directory (LAN)]	389/TCP oder 636/TCP
[SNMP Monitoring]	[auralis]	161/UDP

*in seltenen Fällen unterstützt Exchange kein SSL für ActiveSync. Nutzen Sie dann stattdessen Port 80/TCP.

Hinweis

Für den Zugriff auf den Apple Store, Windows Store, den Google Playstore, den Google GCM Service und den auralis Update Server wird der Zugriff auf folgende Internetseiten benötigt. Wenn Sie in Ihrer Firewall keine Internetseiten direkt eingeben und eine Any Port 443 Regel vermeiden wollen, können Sie alternativ in der Systemkonfiguration im Reiter Netzwerk einen Proxy hinterlegen. Richten Sie stattdessen für diesen eine Firewall Regel ein.

https://android.googleapis.com/gcm/send/ & https://play.google.com/store/
https://repo.auralis.de & https://itunes.apple.com/ & https://www.windowsphone.com/ &
http://www.windowsphone.com/ & https://www.microsoft.com/ & http://*.mzstatic.com/ &
https://*.ggpht.com/ & https://*.googleusercontent.com/

2.2 DNS – Fully Qualified Domain Name

Definieren und richten Sie einen DNS-Namen ein, über den die IP-Adresse Ihrer auralis-Installation vom Internet erreichbar ist. Beispiel: auralis.example.com

2.3 Installationsumgebung

Sie können auralis alternativ als virtuelle oder physikalische Maschine installieren.

2.3.1 Virtuelle Maschine

Erstellen Sie eine virtuelle Maschine. Wählen Sie als Betriebssystem CentOS6 64bit. Oder Linux Kernel 2.6 mit 64Bit. Empfohlene Leistungsdaten Siehe Systemvoraussetzungen. Binden Sie das ISO Image als Bootmedium ein und starten die virtuelle Maschine.

2.3.2 Physikalische Maschine

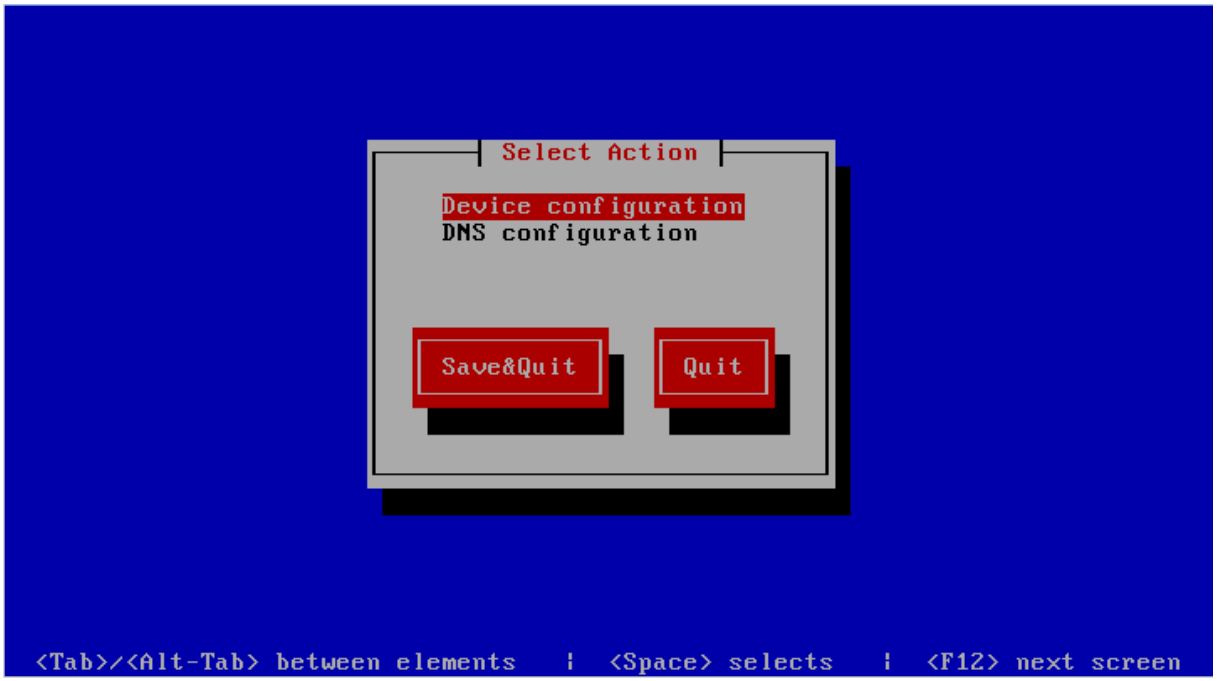
Brennen Sie das auralis ISO Image auf eine CD und legen Sie diese in Ihren Server ein. Achten sie auf die Boot Reihenfolge, damit der Server von der CD starten kann.

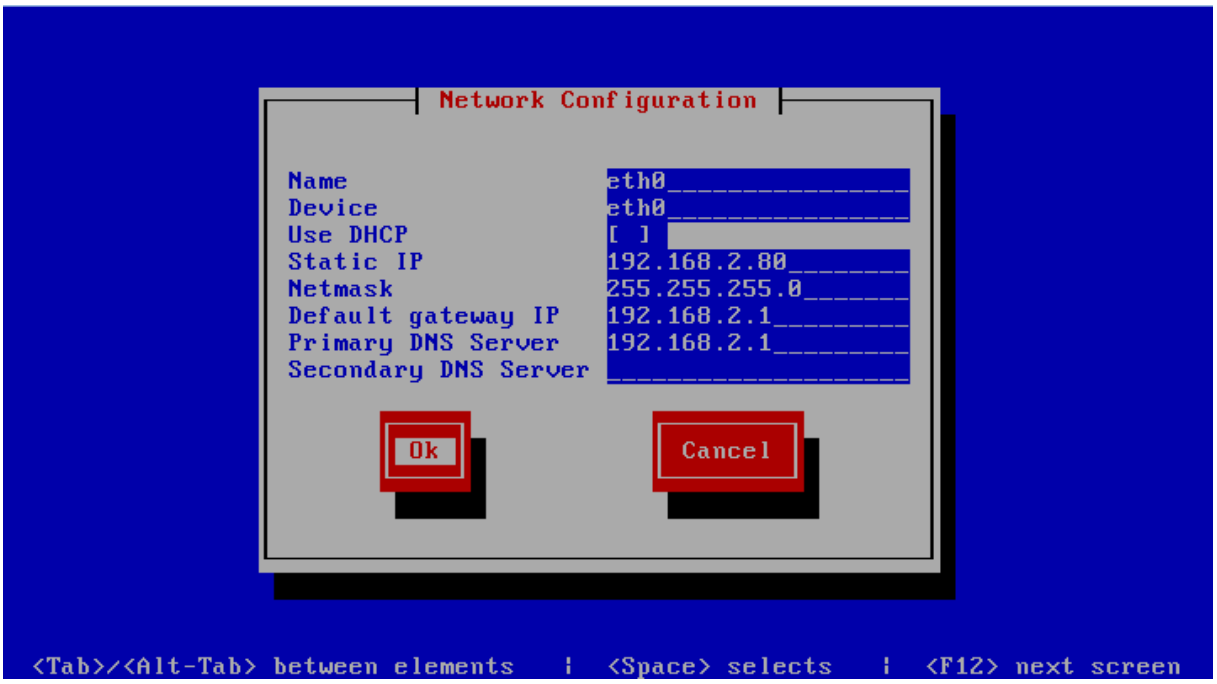
2.4 Erster Start von auralis

Wählen Sie im Bootmenü „auralis Installation“ aus. Nachdem das initial Setup abgeschlossen ist, wird auralis für die erste Konfiguration gestartet.

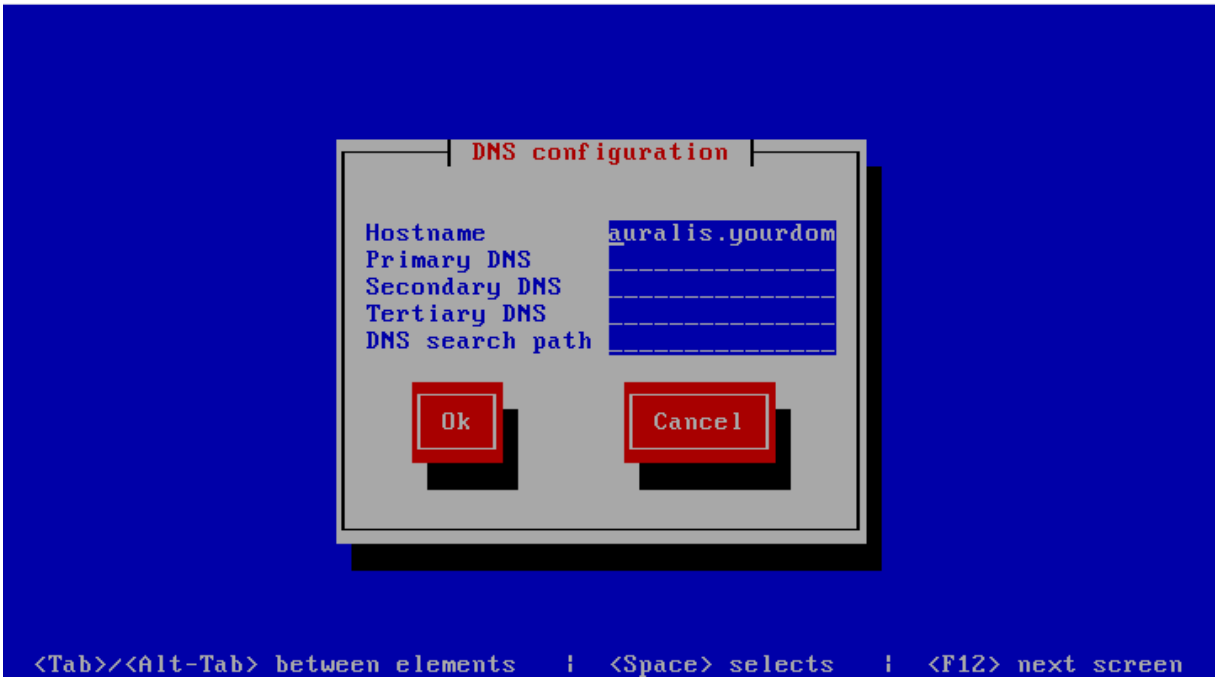
Wählen Sie das Feld „Device configuration“ mit den Pfeiltasten und der Eingabetaste aus.

Netzwerk

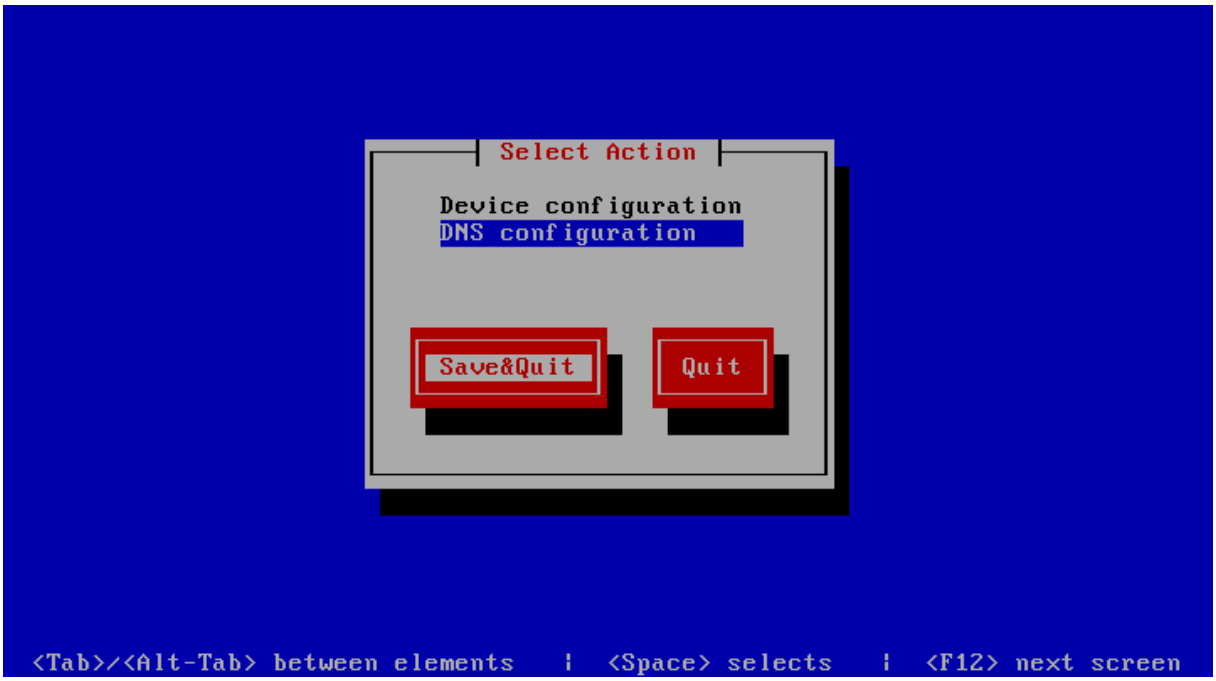




Konfigurieren Sie das Netzwerk-Interface eth0 passend zu Ihrer Infrastruktur.



Konfigurieren Sie den öffentlichen DNS-Hostname Ihres auralis-Systems (Fully Qualified Domain Name, FQDN) und die Einstellungen zu den DNS-Servern. Navigieren Sie jetzt mit den Pfeiltasten auf „Ok“ und drücken Sie die Eingabetaste.



Wählen Sie jetzt „Save & Quit“ und drücken Sie erneut die Eingabetaste.

auralis ist bereit

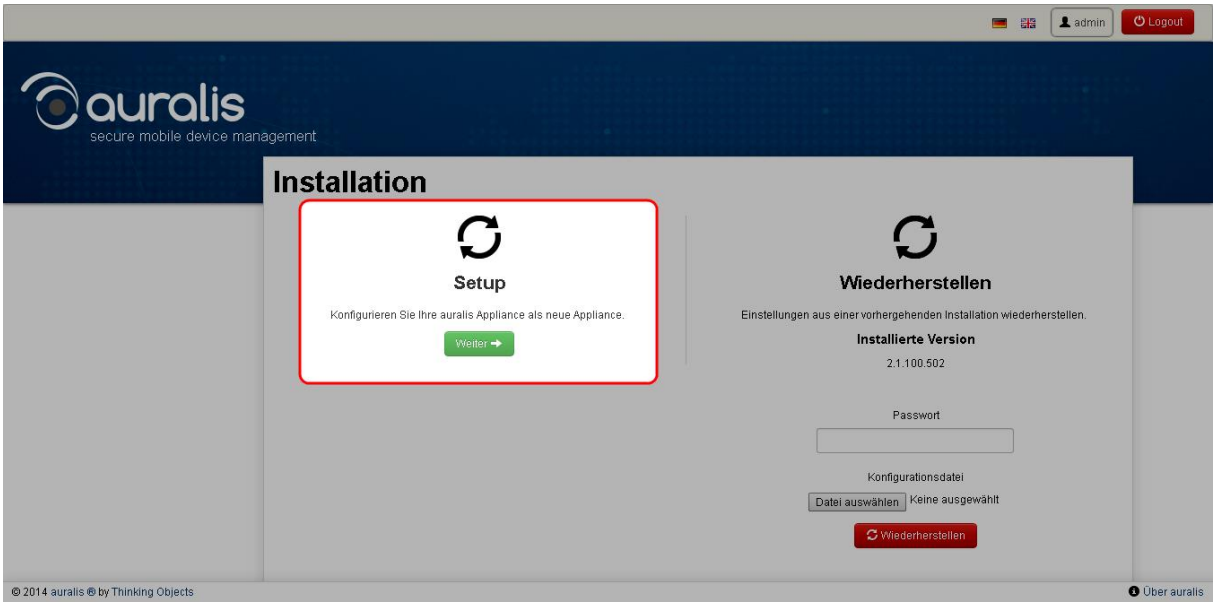


Öffnen Sie in Ihrem Webbrowser jetzt die von Ihrem System angezeigte Adresse. https://*<IP-Adresse>*:8443/admin

> ***Hinweis***
>
> Der an dieser Stelle angezeigte Login per Konsole ist nicht nötig. auralis ist eine Software Appliance, die komplett per Webinterface administriert werden kann.

2.5 Initiale Konfiguration

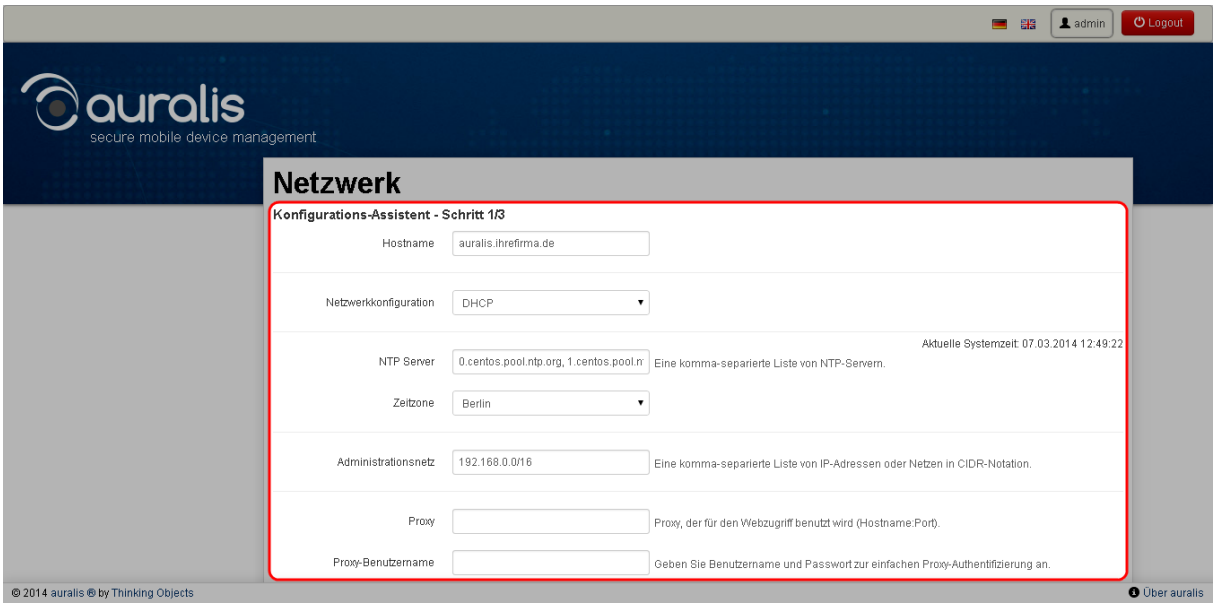
In Ihrem Webbrowser erscheint nun die abgebildete Seite. Klicken Sie unter „Setup“ auf die grüne Schaltfläche „Weiter“, um die Installation von auralis fortzusetzen. Alternativ können Sie an dieser Stellen ein Backup einspiele. Beachten Sie, dass die Versionsnummer des Backups und der Zielinstallation exakt übereinstimmen müssen.



2.5.1 Konfigurationsassistent – Schritt 1 / 3

Bitte geben Sie ein Kennwort für den Administrator ein, überprüfen Sie die Netzwerk-Einstellungen und korrigieren Sie sie gegebenenfalls. Klicken Sie dann auf „Speichern“.

Sie werden nun aufgefordert sich mit dem Benutzer „admin“ und Ihrem soeben hinterlegen Kennwort das erste mal anzumelden.

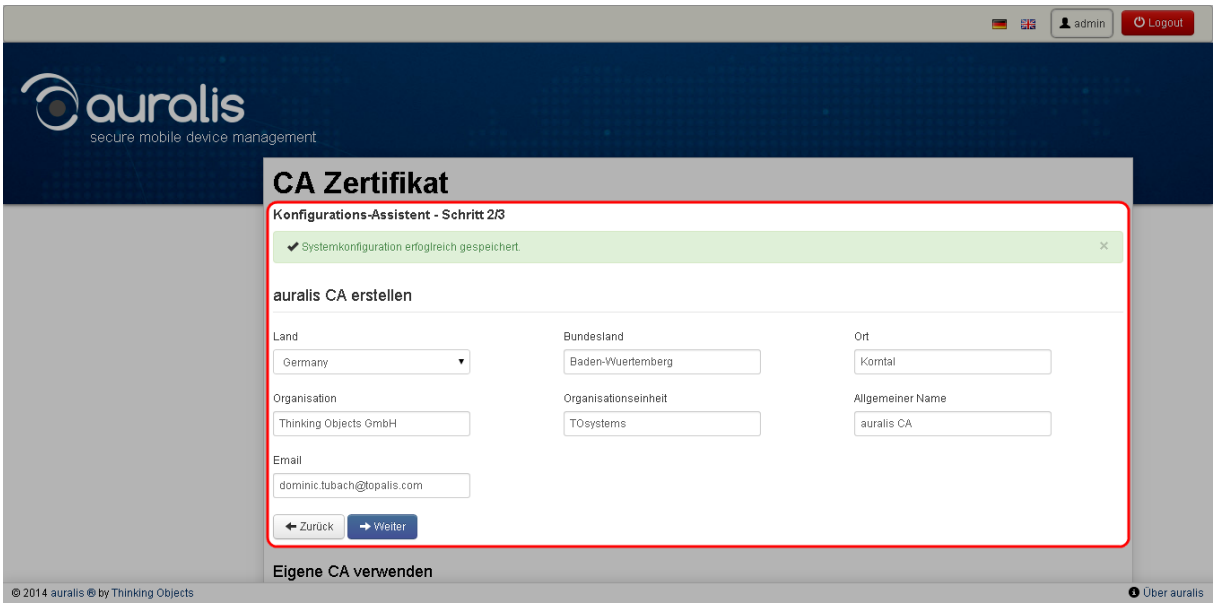


2.5.2 Konfigurationsassistent – Schritt 2 / 3

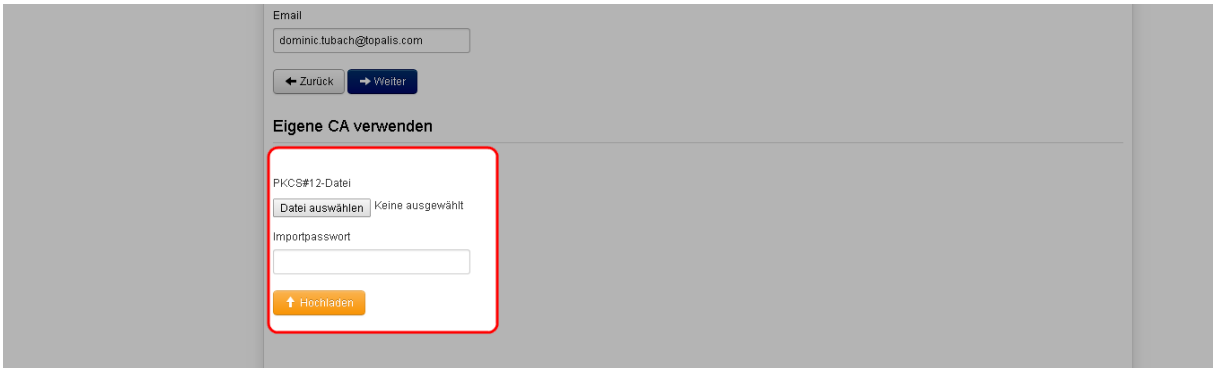
Zu diesem Zeitpunkt wird die Certificate Authoroty erstellt. Also die „root CA“, die später alle weiteren Server und Client Zertifikate nach sich zieht. Jedes Smartphone, welches an auralis angebunden wird, erhält beim Rollout ein eigenes persönliches Client-Zertifikat.

Geben Sie hier alle erforderlichen Daten ein.

> ***Vorsicht***
>
> Ändern Sie das Feld „Allgemeiner Name“ nicht.



Alternativ können Sie eine bereits vorhandene CA hochladen. Wählen Sie dafür unter „Eigene CA hochladen“ die entsprechende Datei aus, geben Sie das Importpasswort ein und klicken Sie dann auf „Hochladen“.

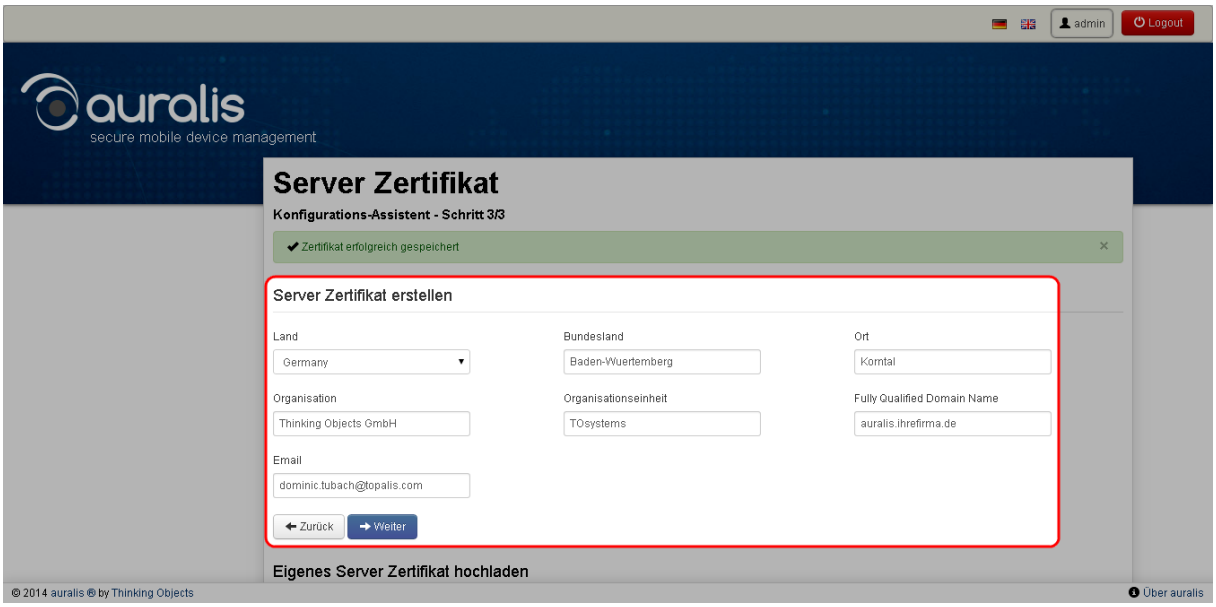


Klicken Sie dann auf „Weiter“.

2.5.3 Konfigurationsassistent – Schritt 3 / 3

Geben Sie in „Schritt 3/3“ die erforderlichen Daten zum Erstellen eines Server-Zertifikats ein. Dieses Zertifikat wird zur verschlüsselten Verbindung zu Ihrem auralis-System verwendet.

Achten Sie darauf, dass der Name im Feld „Fully Qualified Domain Name“ der für auralis festgelegte entspricht. Beispiel: auralis.example.com



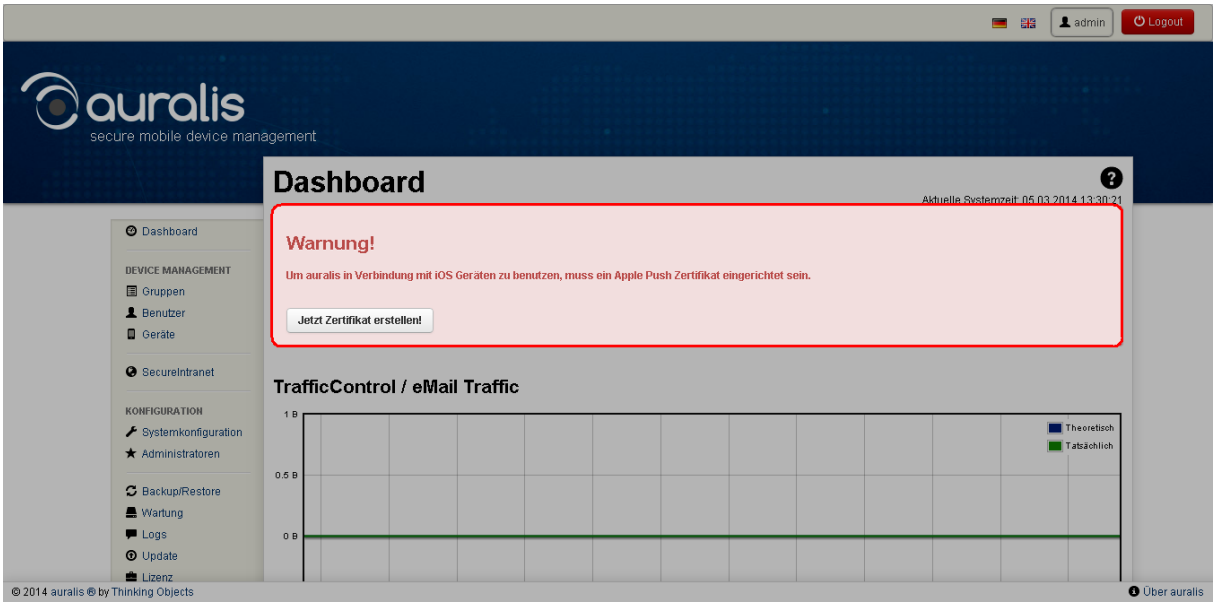
Auch hier können Sie alternativ Ihr eigenes Zertifikat verwenden. Wählen Sie hierfür unter „Eigenes Zertifikat hochladen“ die entsprechende Datei aus, geben Sie das zugehörige Passwort ein und klicken Sie auf „Hochladen“.

Klicken Sie jetzt auf „Weiter“, um die Installation abzuschließen.

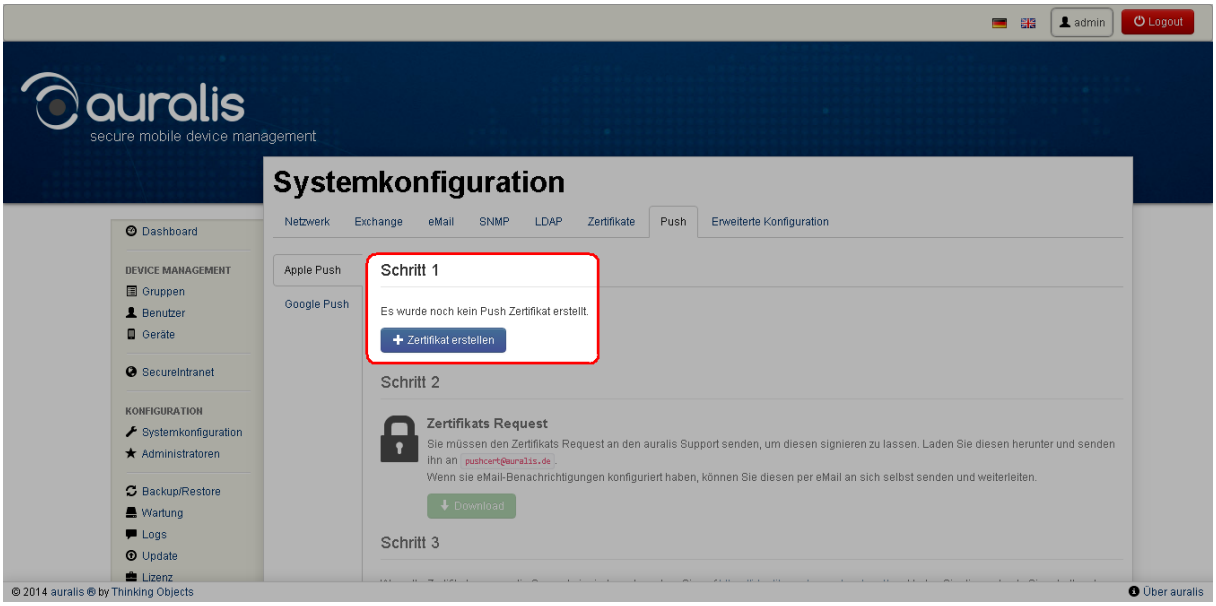
2.6 Apple Push Zertifikat erstellen

Nach der Installation wird Sie auralis darauf hinweisen, dass noch kein Apple Push Zertifikat eingerichtet wurde. Das Apple Push verfahren ist ein Dienst von Apple, der dafür sorgt das Konfigurationsänderungen oder die Löschung eines Gerätes so schnell wie möglich ausgeführt werden. Es werden keine Daten an Apple gesendet. Lediglich der Hinweis für das Gerät, sich sofort bei seinem Mobile Device Management zu melden.

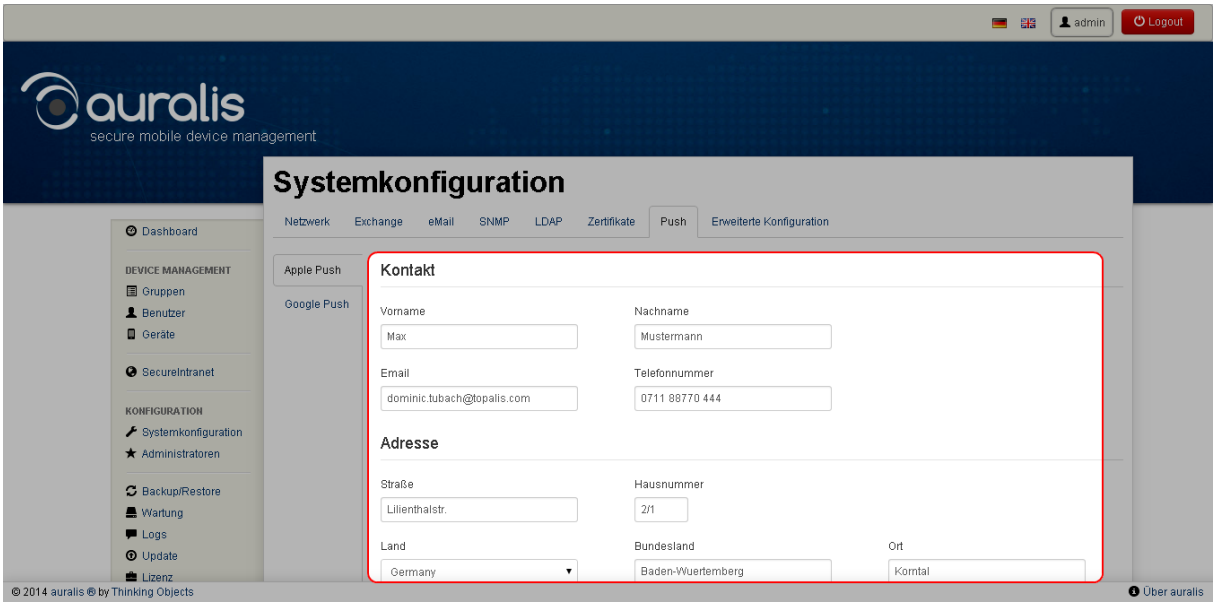
Klicken Sie auf *„Jetzt Zertifikat erstellen“.*



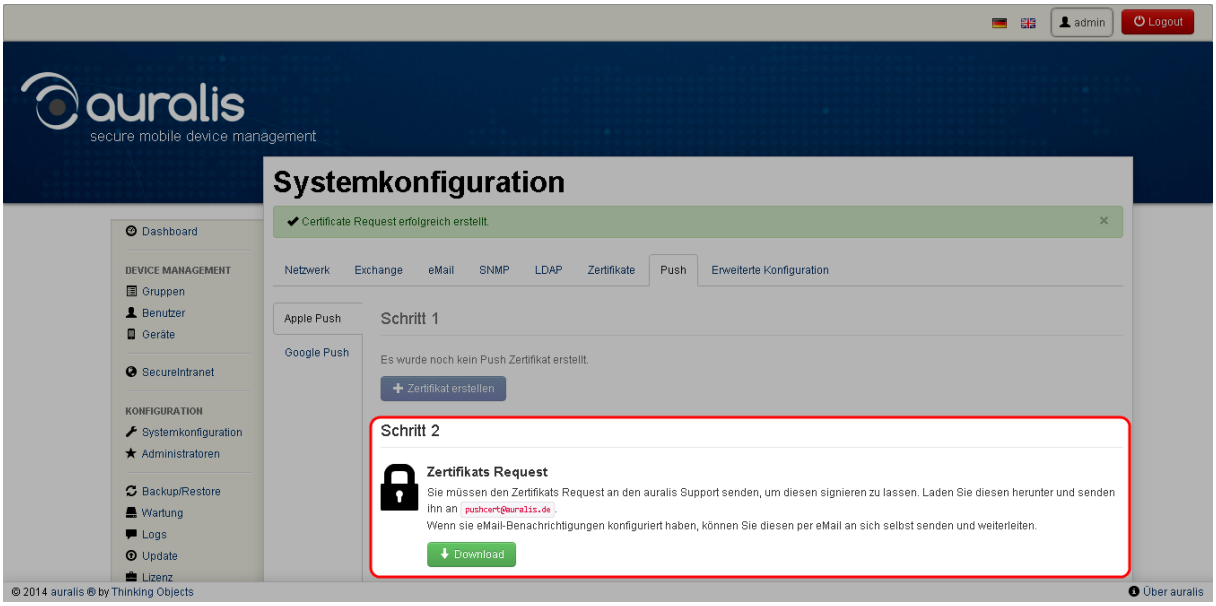
Um ein Apple Push Zertifikat anzulegen, klicken Sie im Menü auf der linken Seite auf „Systemkonfiguration“ und dann auf den Reiter „Push“. Klicken Sie dort unter „Schritt 1“ auf die Schaltfläche „Zertifikat erstellen“.



Geben Sie in die Felder unter „Kontakt“, „Adresse“ und „Organisation“ die erforderlichen Daten ein und klicken Sie dann auf „Zertifikat erstellen“.



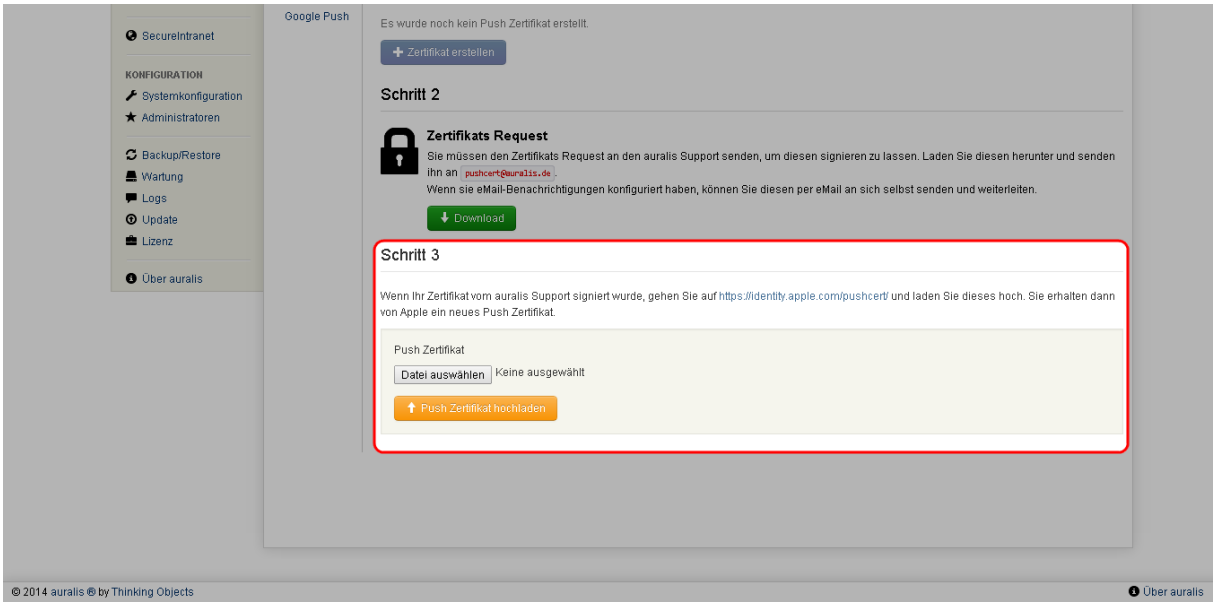
Sie können jetzt in „Schritt 2“ den Zertifikats Request herunterladen. Senden Sie diesen an den auralis Support (pushcert@auralis.de). Wir signieren diese Zertifikatsanfrage so schnell wie möglich. Dieses verfahren ist notwendig, da Apple jedes Zertifikat für ein Mobile Device Management vom Hersteller signiert haben möchte.



Sobald Ihr Zertifikat vom auralis Support signiert wurde, besuchen Sie https://identity.apple.com/pushcert/ und laden die signierte Zertifikatsanforderung hoch. Sie erhalten dann von Apple ein neues, eigenes Push Zertifikat.

Vorsicht

Merken Sie Sich den Account den Sie für die Zertifikatsgenerierung verwendet haben. Die Zertifikate sind nur ein Jahr gültig und müssen danach in diesem Account verlängert werden. Haben Sie diesen vergessen und es muss mit einem neuen Account ein Zertifikat generiert werden, verlieren alle bisher ausgerollten iOS Geräte Ihre MDM Verbindung.



Wählen Sie in „Schritt 3“ das Push Zertifikat von Apple aus und laden Sie es in auralis hoch.

Hinweis

auralis ist jetzt mit einer Demo Lizenz für 30 Tage aktiviert. Sie können in diesem Zeitraum bis zu fünf Benutzer anlegen und alle Funktionen von auralis testen.

Wie Sie eine erworbene Lizenz einspielen, können Sie im folgenden Kapitel nachlesen.

Weiterführende Informationen zu den Push Diensten von Apple und Google, sowie die Einrichtung des Google Push Dienstes „GCM“ erhalten Sie im Kapitel 6.7.

2.7 Lizenz einspielen

Um auralis mit einer Lizenz zu aktivieren, benötigen Sie ein Apple Push Zertifikat.

Navigieren Sie ins Menü „Wartungslizenz“ und wählen Sie dort unter „Neue Lizenz hochladen“ die passende Lizenzdatei aus. Klicken Sie anschließend auf „Hochladen“.

auralis ist jetzt lizenziert. Alle relevanten Daten zu Ihrer Lizenz werden Ihnen jetzt unter „Lizenz“ angezeigt.

Diesen Vorgang können Sie auch nutzen, um eine bestehende Lizenz zu verlängern.



3 Administrationsoberfläche

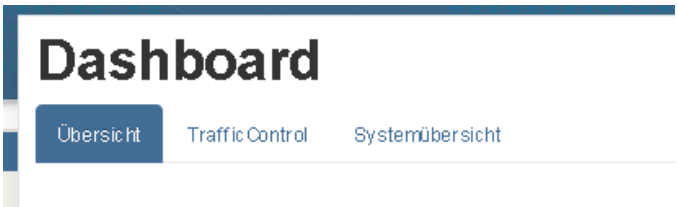
3.1 Dashboard

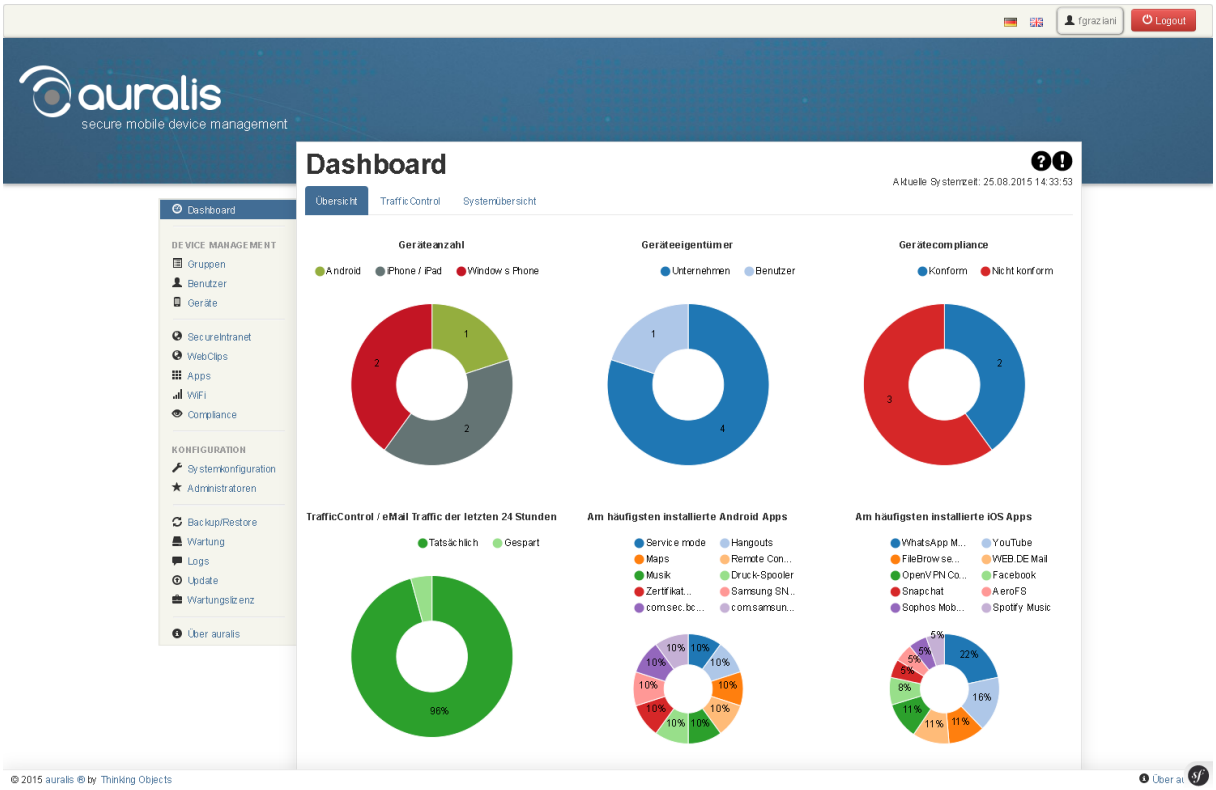
Das Dashboard ist aufgeteilt in drei Reiter.

1) Übersicht
   Hier finden Sie einige Grafiken die Ihnen einen kurzen Überblick über all Ihre integrierten Smartphones liefern. Z.B. Geräteanzahl nach OS, Geräteeigentümer (BYOD), Top 10 installierte Apps, Toptalkers (Geräte mit dem meisten E-Mail Datenvolumen) und zuletzt aktive Geräte.

2) TrafficControl
   In dieser Übersicht sehen sie alle Informationen zu unserem E-Mail Komprimierungsfeature. Theoretische Übertragungswerte, tatsächliche und den eingesparten Traffic heruntergebrochen bis zum Dateityp.

3) Systemübersicht
   Hier finden Sie alle Systemrelevanten Informationen wie CPU, RAM, HDD Belegung und die LAN Auslastung. Ebenfalls wird Ihnen hier der Status des Apple und des Google Push Dienstes sowie die Erreichbarkeit des auralis Update Servers angezeigt.





3.2 Gruppen

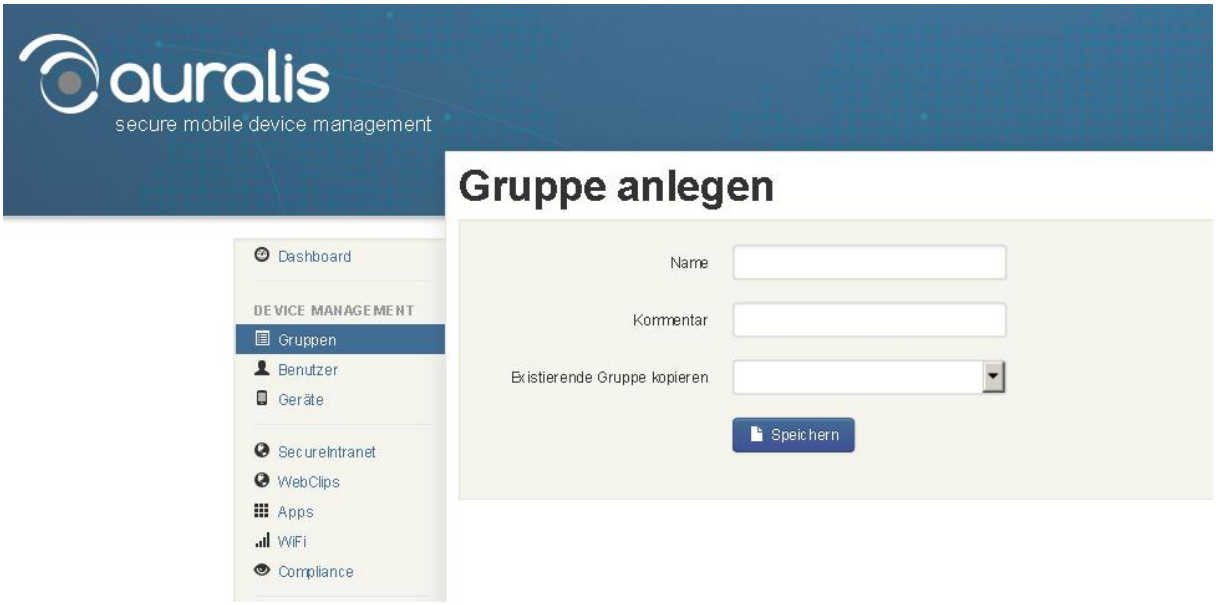
Im Menüpunkt „Gruppen“ finden Sie alle in auralis angelegten Gruppen. Gruppen bieten Ihnen eine bequeme Administration und Verwaltung von Zugriffsrechten der Geräte und Benutzer.

Gruppe hinzufügen

Um eine neue Gruppe hinzuzufügen, klicken Sie auf die Schaltfläche „Gruppe anlegen“. Geben Sie in das Feld „Name“ den Namen der neuen Gruppe ein. Das Feld „Kommentar“ ist optional. Klicken Sie dann auf die Schaltfläche „Speichern“, um die Gruppe anzulegen.

Um den Konfigurationsaufwand für mehrere Gruppen zu minimieren, können Sie an dieser Stelle auch eine vorhandene Gruppe kopieren und die notwendigen Änderungen im Anschluss anpassen.

Für alle Geräte in dieser Gruppe werden automatisch zum zugehörigen Benutzer die E-Mail Einstellungen vorgenommen. Möchten Sie eine Gruppe erstellen auf deren Geräte keine E-Mail Konfiguration vorhanden sein soll, so können Sie über das Kontextmenü eine Gruppe ohne E-Mail Konfiguration erstellen. Für jedes Gerät in einer Gruppe ohne E-Mail Profil wird eine eigene Lizenz benötigt.



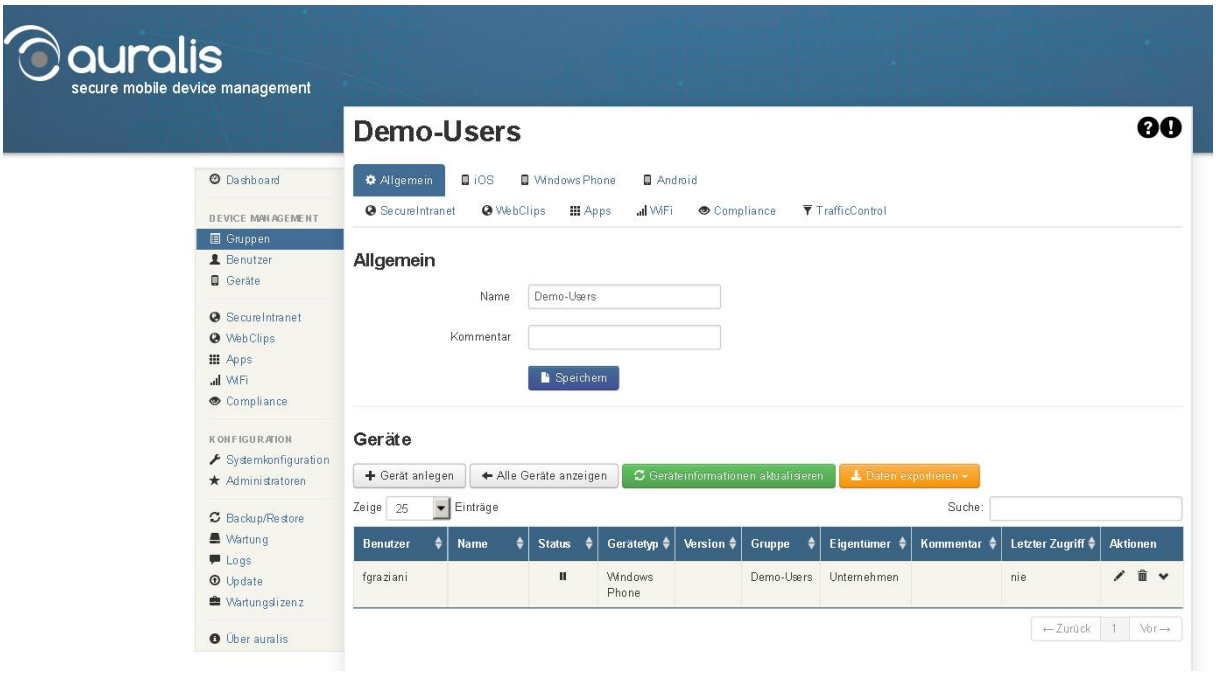
Nach dem Anlegen gelangen Sie zur Konfiguration der angelegten Gruppe. Um diese zu einem späteren Zeitpunkt zu erreichen, können Sie die Schaltfläche „Bearbeiten“ in der Spalte „Aktionen“ verwenden.

3.2.1 Gruppenkonfigurationen

In der Konfiguration der jeweiligen Gruppe finden Sie mehrere Reiter, unter denen Sie verschiedene Einstellungen zur Gruppe vornehmen können. Diese gelten für alle zur Gruppe gehörenden Geräte.

3.2.2 Allgemein

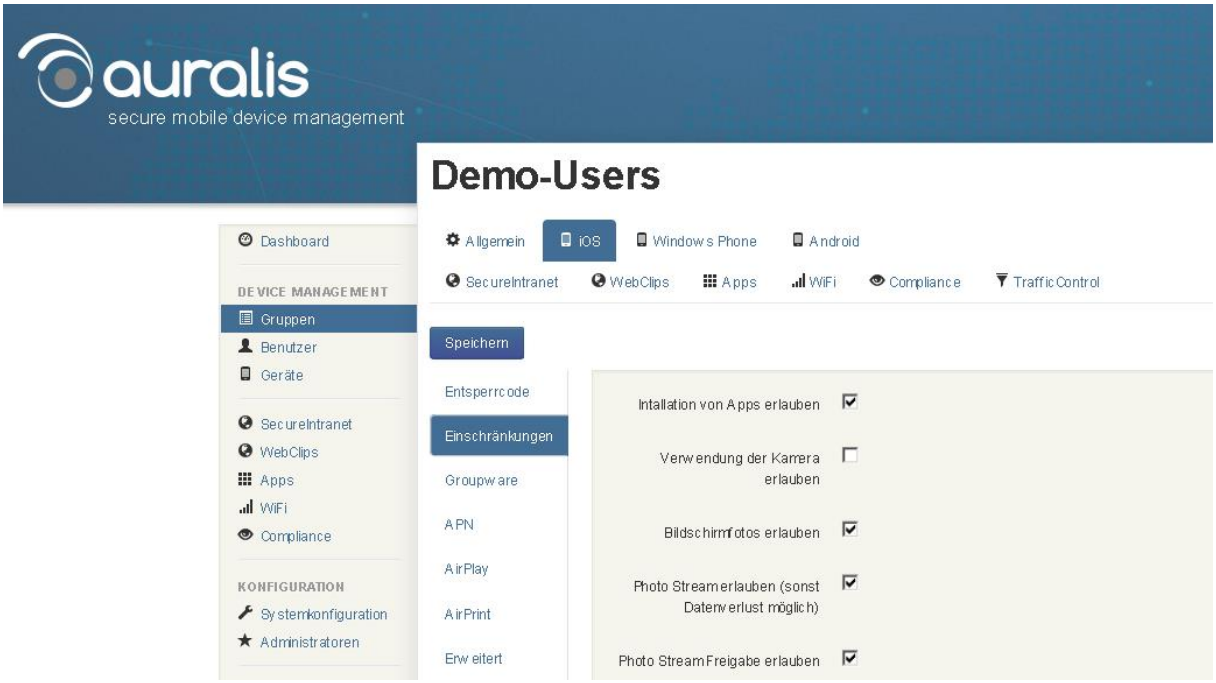
Hier können Sie den Gruppenname ändern, bei Bedarf einen Kommentar einfügen und Geräte zur Gruppe hinzufügen. Zur Gruppe gehörende Geräte werden in einer tabellarischen Übersicht dargestellt.



3.2.3 „iOS“, „Android“ und „Windows Phone“

In den Reitern „iOS“, „Android“ und „Windows Phone“ können Sie Einstellungen zu Geräten mit dem jeweiligen Betriebssystem tätigen. Darunter fallen z.B. Einstellungen zur Gerätesicherheit & Systemeinschränkungen.

Je nach mobilem Betriebssystem und Hersteller unterscheidet sich die Einstellungsvielfalt.



3.2.4 WiFi

Im Reiter WiFi aktivieren oder deaktivieren Sie die WLAN Netze die in dieser Gruppe automatisch verbunden werden sollen.

Wie Sie WiFi Netze anlegen erfahren Sie im Kapitel 5 – Globale Konfigurationen.

3.2.5 SecureIntranet

Mit SecureIntranet bietet Ihnen auralis Zugriff auf interne Web-Dienste von iOS- und Android-Geräten. Anstatt auf eine akkulastige VPN-Verbindung zu vertrauen, setzt SecureIntranet auf zertifikatsbasierte Authentifizierung der Geräte. auralis bietet Ihnen mit SecureIntranet eine gesicherte Anbindung der Geräte an das Intranet Ihrer Firma. Bitte beachten Sie, dass nicht alle Web-Anwendungen diese Art des Zugriffs unterstützen.

Im Reiter „SecureIntranet“ können Sie einzelne URLs für die Gruppe freischalten. Die Verknüpfungen zum Link eines jeweiligen SecureIntranets werden auf iOS- und Android-Geräten automatisch auf dem Startbildschirm abgelegt oder wieder von dort entfernt.

Wie Sie SecureIntranet Links erstellen erfahren Sie im Kapital 5 – Globale Konfigurationen.

3.2.6 Webclips

Als Webclips bezeichnet man Shortcuts auf Internetseiten. Diese werden direkt auf dem Endgerät als Icon hinterlegt. An dieser Stelle können Sie angeben welche Webclips für diese Gruppe automatisch erstellt werden sollen.

Wie Sie Webclips ertellen, erfahren Sie im Kapitel 5- Globale Konfiguration.

3.2.7 Compliance

Legen Sie fest welche Compliance Regel für diese Gruppe gilt. Es kann immer nur eine Compliance Regel pro Gruppe festgelegt werden.

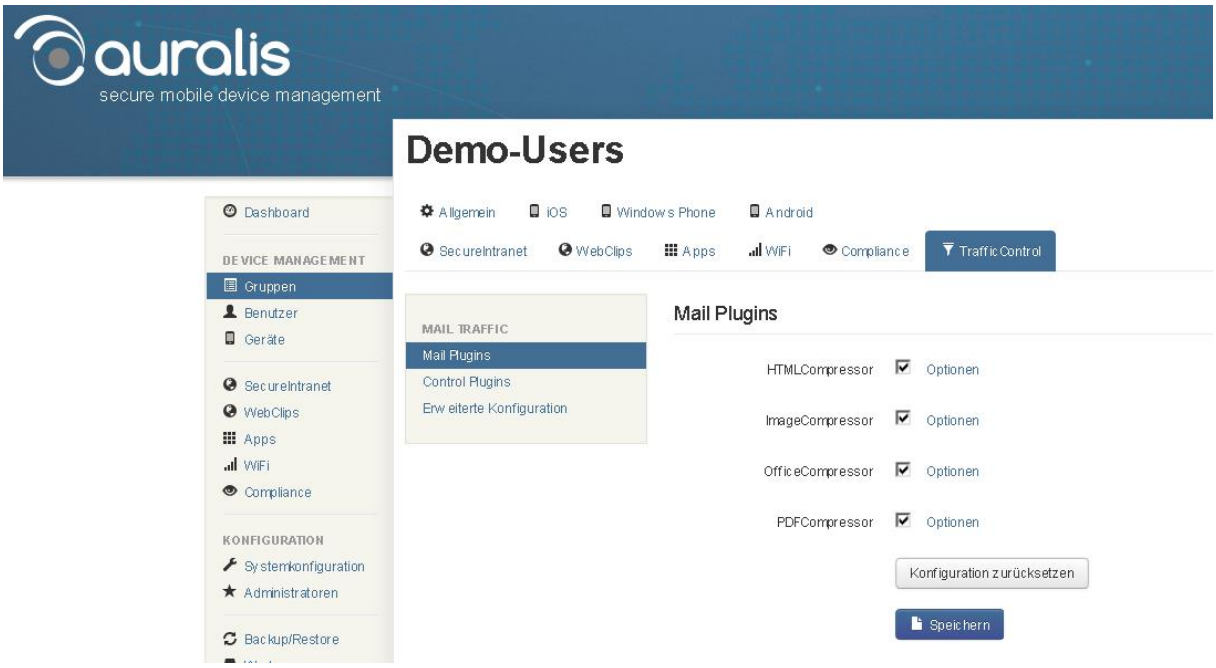
Wie sie Compliance Regeln erstelen, erfahren Sie im Kapitel 5 – Globale Konfiguration

3.2.8 TrafficControl

TrafficControl komprimiert Dateianhänge in E-Mails und sorgt damit für einen geringeren Verbrauch von mobilem Datenvolumen. Sowohl Bilder und Microsoft Office Dokumente (ab Version 2007), als auch PDF-Dateien kann TrafficControl um bis zu 90 Prozent komprimieren.

Mail Plugins

Legen Sie fest, welche Dateien von TrafficControl verlustbehaftet komprimiert werden sollen. In den Optionen von „HTML Compressor“, „ImageCompressor“, „OfficeCompressor“ und PDFCompressor“ finden Sie zusätzliche Feineinstellungen, mit denen Sie die Kompression optimieren können.

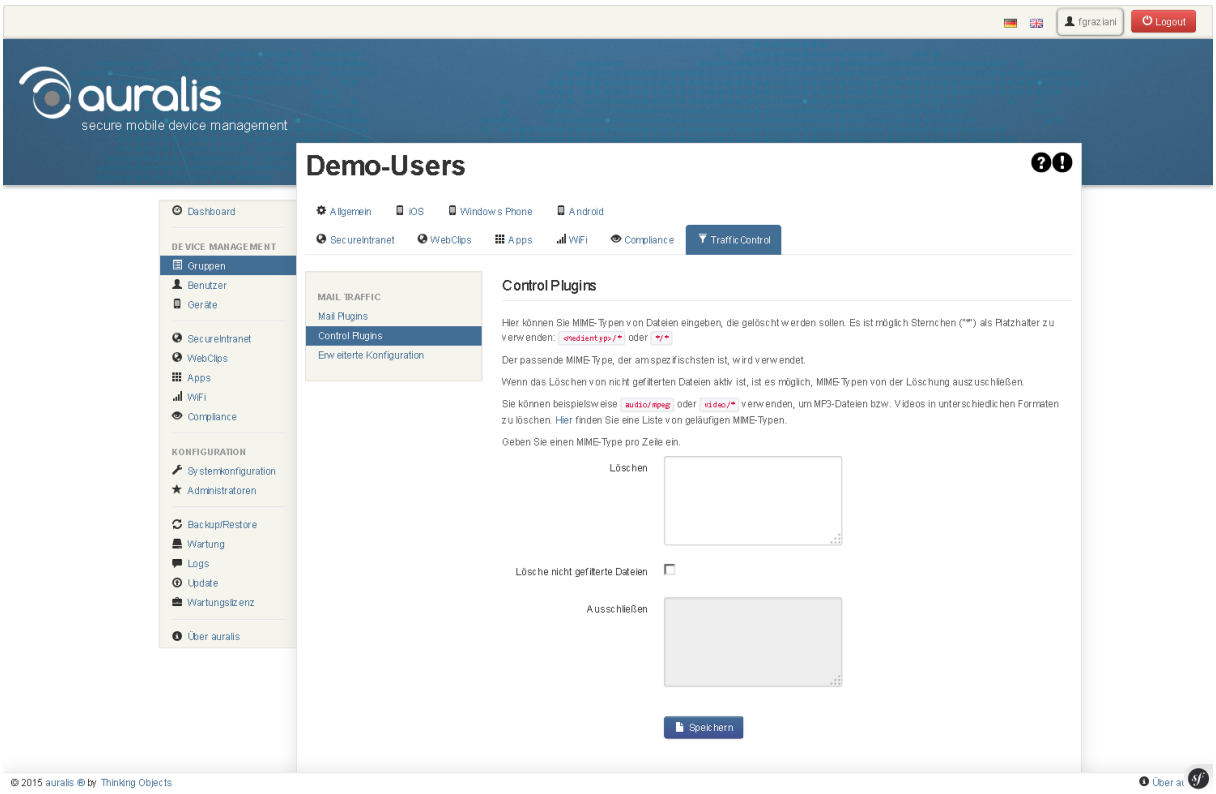


Hinweis

Die Kompression der Dateien geschieht nur beim Versand auf mobile Geräte. Die Originaldatei bleibt im Posteingang des E-Mail-Kontos weiterhin erhalten!

Control Plugins

Legen Sie in den Einstellungen des Control Plugins fest, ob bestimmte Dateitypen von TrafficControl gelöscht und nicht an die mobilen Geräte gesendet werden sollen. Verwenden Sie hierfür sogenannte MIME-Types („<Main-Type>/<Sub-Type>“). Sie können bestimmte Dateitypen löschen lassen und damit alle anderen erlauben. Sie können optional definieren, welche Sub-Typen innerhalb des MIME-Types von der Löschung ausgeschlossen werden sollen. Setzen Sie dafür den Haken im Feld „Lösche nicht gefilterte Dateien“ und definieren Sie dort den Sub-Type.



Erweiterte Konfiguration

Stellen Sie ein wie sich TrafficControl bei einem Fehler bei der Kompression verhalten soll.

- Ignorieren: auralis ignoriert die Datei, bei der der Fehler aufgetreten ist und fährt mit der nächsten Operation fort.
- Löschen: Die Datei, bei der der Fehler aufgetreten ist, wird gelöscht.
- Durchleiten: Die E-Mail wird unverändert an das Gerät ausgeliefert

3.2.9 Apps

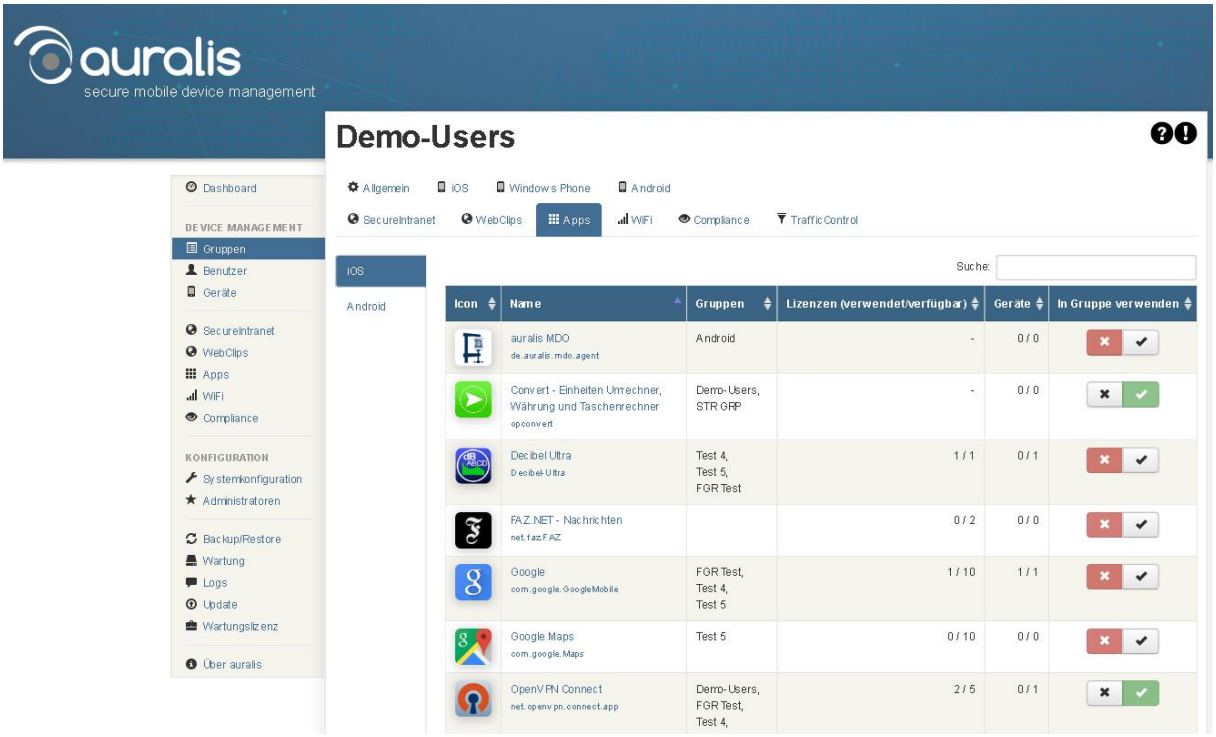
Im Reiter Apps können Sie die über auralis verwalteten iOS oder Android Apps in der jeweiligen Gruppe aktivieren. Benutzer werden nach Aktivierung aufgefordert diese Apps zu installieren.

Bei iOS Geräten wird zusätzlichen zwischen normalen verwalteten und vom Unternehmen gekauften VPP Lizenzen unterschieden. In beiden Fällen benötigt der Endanwender eine eigene Apple ID.

Normal verwaltete Apps die Kostenlos sind, werden sofort installiert. Bei kostenpflichtigen Apps wird der Benutzer aufgefordert eine/seine Apple ID anzugeben um die App zu kaufen.

Beim Apple VPP Programm werden die vom Unternehmen gekauften Apps mit der Apple ID des Benutzers assoziiert und der Benutzer kann diese kostenfrei installieren.

Wie Sie Apps für die zentrale Verwaltung konfigurieren erfahren Sie im Kapital 5 – Globale Konfigurationen.



3.2.10 VPN

Im Reiter VPN aktivieren oder deaktivieren Sie die VPN Netze.

Wie Sie VPN Netze anlegen erfahren Sie im Kapitel 5 – Globale Konfigurationen.

3.3 Benutzer

Im Menüpunkt „Benutzer“ listet auralis alle bisher angelegten Benutzer auf und zeigt detaillierte Informationen zu jedem Benutzer an. Zudem haben Sie in der Spalte „Aktionen“ Zugriff auf Einstellungen zu jedem Benutzer.

3.3.1 Benutzer anlegen

Klicken Sie auf die Schaltfläche „Benutzer anlegen“, um einen Benutzer in auralis hinzuzufügen.

Geben Sie in die Eingabemaske die erforderlichen Informationen zu dem neuen Benutzer ein.

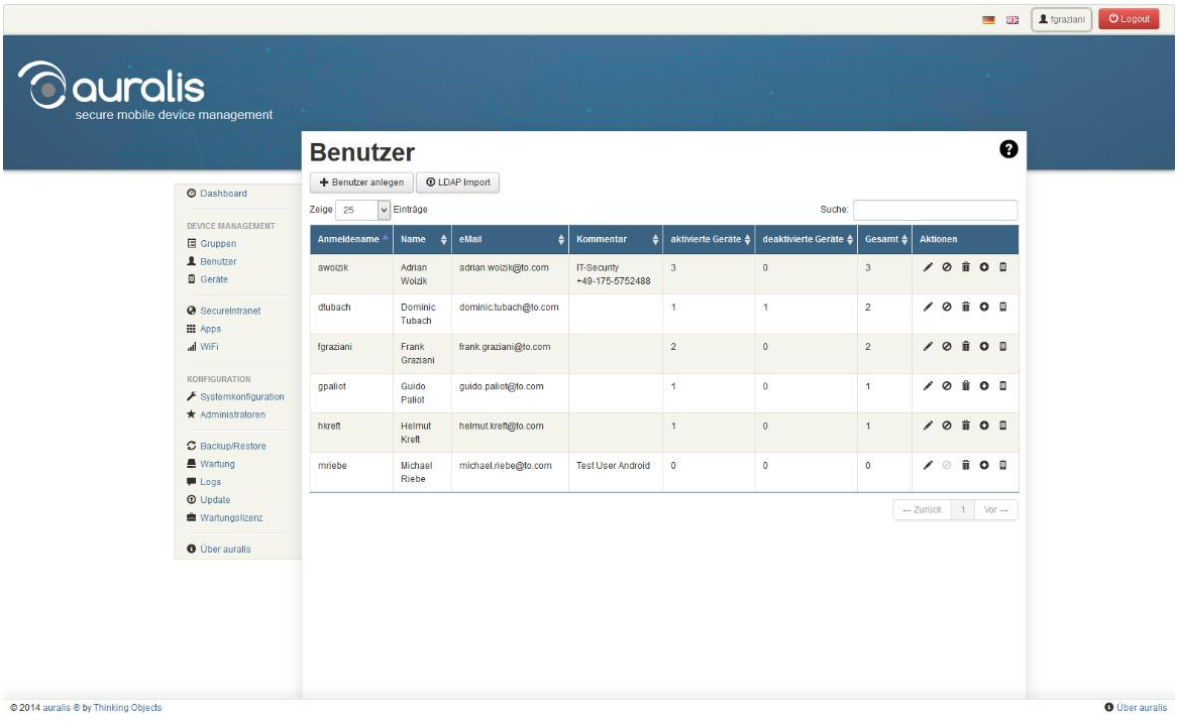
Anmeldename: Geben Sie hier den Benutzernamen ein. Mit diesem Namen meldet sich der Benutzer später in auralis an, um den Rollout seines Geräts anzustoßen.

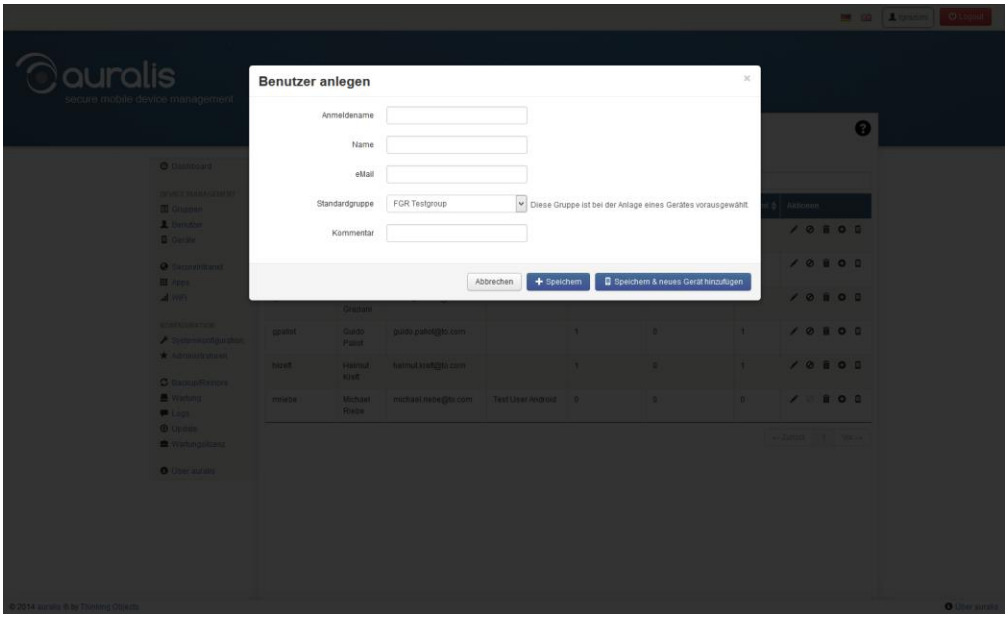
Name: Geben Sie hier den vollständigen Namen des Benutzers ein.

eMail: Geben Sie hier die E-Mail-Adresse des Benutzers ein.

Standardgruppe: Diese Gruppe ist beim Anlegen eines Geräts für diesen Benutzer die vorausgewählte Gruppe. Sie hat darüber hinaus keine zusätzliche Bedeutung.

Kommentar: Hier können Sie einen optionalen Kommentar zum neuen Benutzer eingeben.





Klicken Sie jetzt auf „Speichern“, um den Benutzer anzulegen.

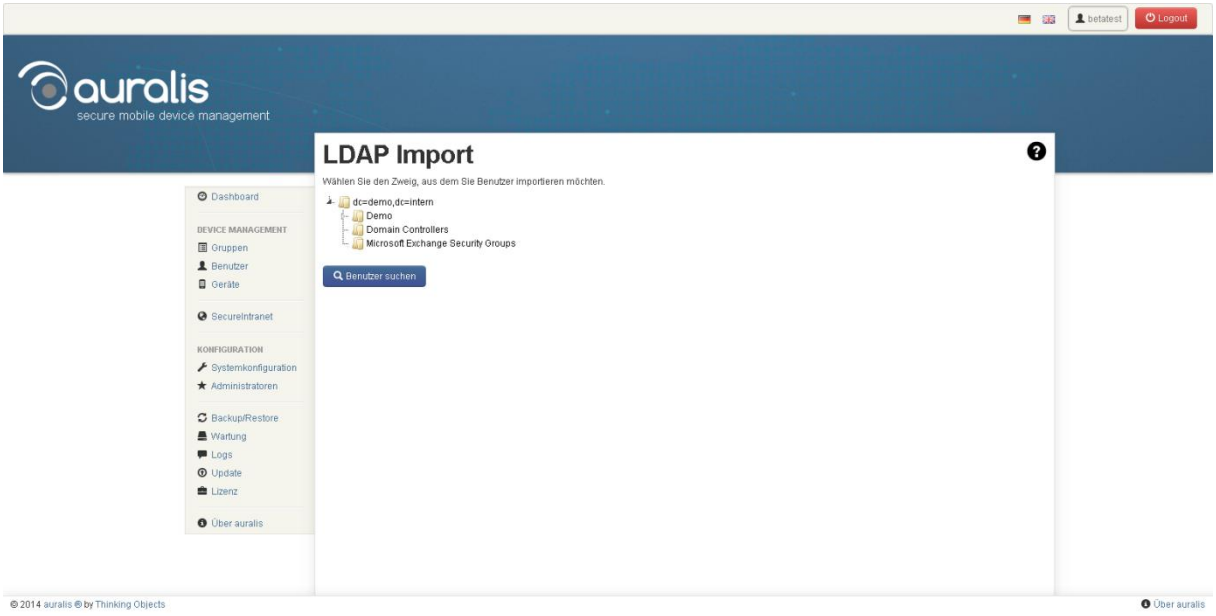
Möchten Sie für den neuen Benutzer auch gleich ein Gerät anlegen, klicken Sie auf „Speichern & neues Gerät hinzufügen“. Wie Sie ein Gerät nachträglich hinzufügen, können Sie im Kapitel „Gerät hinzufügen“ nachlesen.

Mit der Schaltfläche „Abbruch“ wird die Eingabe verworfen und der Benutzer nicht angelegt.

LDAP-Import

Wie Sie den LDAP-Import konfigurieren, können Sie im Kapitel 6.5 nachlesen.

Um Benutzer über LDAP zu importieren, klicken Sie auf die Schaltfläche „LDAP Import“ und markieren Sie die OU, aus dem Sie Benutzer importieren möchten. Klicken Sie dann auf „Benutzer suchen“.



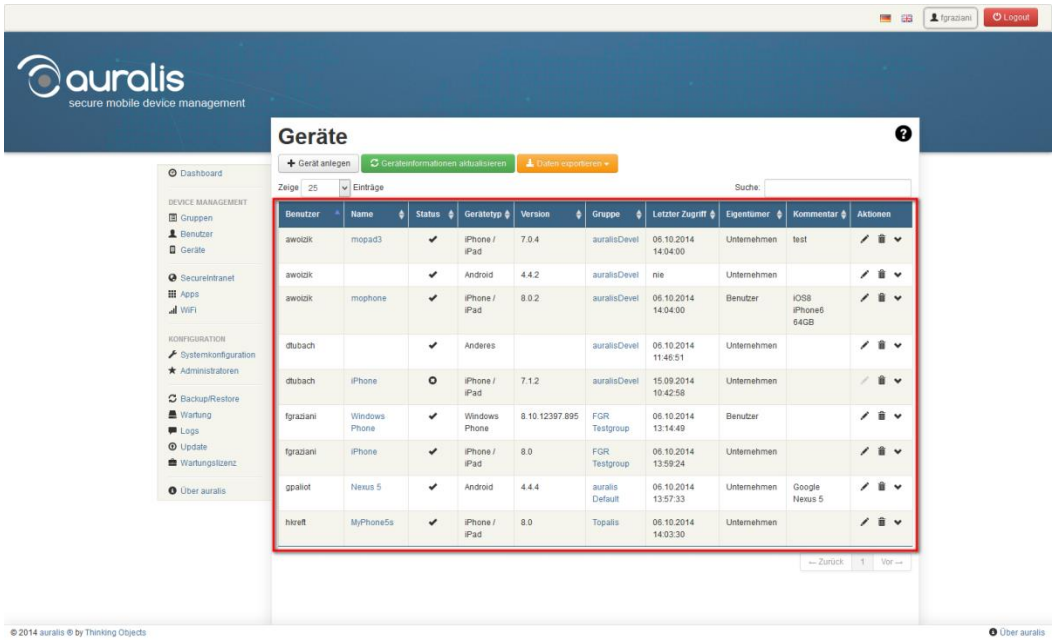
Die im gewählten Zweig gefundenen Benutzer werden in einer Tabelle dargestellt. Markieren Sie die Benutzer, die Sie in auralis importieren möchten und weisen Sie den Benutzern dann eine Gruppe zu. Optional können Sie für die Benutzer jeweils ein neues Gerät anlegen und sie per Mail darüber informieren lassen.

Mit einem Klick auf eine Zelle der Tabelle kann der darin enthaltene Wert für den Import angepasst werden. Eine Änderung im LDAP-Verzeichnis findet nicht statt.

3.4 Geräte

Im Menüpunkt „Geräte“ werden alle Geräte angezeigt, die eingerichtet wurden.

Unter 3.5 erfahren Sie, wie Geräte hinzugefügt werden.



Hier können Sie neue Geräte anlegen, die Geräteinformationen und Geräte daten exportieren (CSV, XLSX). In der Tabelle „Geräte“ sind alle Geräte aufgelistet. Sie enthält Basisinformationen zu den einzelnen Geräten.

Benutzer: Hier wird der Benutzer angezeigt, zu dem das Gerät gehört. Für einen Benutzer können mehrere Geräte in auralis angelegt sein.

Name: Hier wird der Name des Geräts angezeigt. Der Name wird vom Gerät abgefragt. Mit einem Klick auf den Namen gelangen Sie direkt in die Informations-Übersicht des Geräts.

Status: Hier wird der aktuelle Status des Geräts angezeigt. auralis unterscheidet hier zwischen ausgerollten Geräten, auszurollenden Geräten und zu löschenden Geräten.

Gerätetyp: Anzeige des Gerätetyps. Unterscheidung zwischen „iPhone/iPad“, „Android“, „Windows Phone“ und „Andere“.

Version: Die Versionsnummer des installierten mobilen Betriebssystems

Gruppe: Hier wird die Gruppe angezeigt, die dem Gerät zugewiesen wurde. Mit einem Klick auf den Gruppenname gelangen Sie in die Gruppeneinstellungen.

Letzter Zugriff: Der angezeigte Zeitpunkt gibt an, wann sich das Gerät das letzte Mal eine Verbindung zu auralis hatte.

Eigentümer: Die Anzeige des Eigentümers zeigt Ihnen an ob es sich um ein Firmen- oder Privatgerät handelt.

Kommentar: Dieses Feld ist beim Anlegen eines Geräts optional und wird an dieser Stelle in der Übersicht angezeigt.

Aktionen: Hier haben Sie Zugriff auf alle gerätespezifischen Einstellungen und Optionen.

Bearbeiten: bringt Sie direkt in die Geräteeigenschaften.

Löschen: entfernt das Gerät aus der Liste der ausgerollten Geräte. Eine Anzeige zur Bestätigung des Löschbefehls schützt vor versehentlichem Löschen eines Geräts. Nach dem Bestätigen der Abfrage wird ein Enterprise-Wipe-Befehl an das Gerät gesendet, der alle durch auralis vorgenommenen Einstellungen rückgängig macht. Das Gerät ist danach im Zustand wie vor dem Rollout, alle anderen Einstellungen auf dem Gerät bleiben bestehen. Solange auralis auf die Wipe-Bestätigung des Geräts wartet, wird das „Löschen"-Symbol rot angezeigt.

Sollten Sie ein Gerät nicht über auralis sondern direkt am Gerät auf Werkseinstellung zurücksetzen, müssen Sie das Gerät vor einem erneuten Rollout endgültig aus der Liste entfernen, klicken Sie auf das rote „Löschen"-Symbol.

Hinweis

Durch das endgültige Löschen werden alle mit dem Gerät verbundenen Zertifikate von auralis widerrufen. Es kann dadurch nicht mehr mit auralis synchronisiert werden und muss neu ausgerollt werden.

Weitere Aktionen:

Informationen: Mit dieser Schaltfläche gelangen Sie zu den Geräteinformationen. Dort hält auralis detaillierte, gerätespezifische Informationen bereit. Diese Informationen sind erst nach erfolgreichem Rollout verfügbar, da sie vom Gerät zu diesem Zeitpunkt übertragen werden. Die können auch durch einen Klick auf „Aktualisieren" angefordert werden.

Wipe: Über diese Funktion senden Sie einen Wipe-Befehl an das ausgewählte Gerät. Dadurch werden alle durch auralis getätigten Veränderungen am System rückgängig gemacht und anschließend alle Gerätezertifikate widerrufen.

Auf Werkseinstellungen zurücksetzen: Mit dieser Funktion wird das Gerät auf den Auslieferungszustand zurückgesetzt.

Vorsicht

Mit der Funktion „Auf Werkseinstellungen zurücksetzen" werden sämtliche Daten auf dem Gerät gelöscht. Dieser Schritt kann nicht rückgängig gemacht werden.

PIN zurücksetzen: Der aktuelle PIN wird gelöscht. Der Sperrbildschirm des Geräts kann dann ohne PIN entsperrt werden.

Sperren: Der Benutzer des Geräts bekommt eine optionale Meldung und Telefonnummer auf dem Sperrbildschirm seines Geräts angezeigt. Der PIN des Geräts bleibt bestehen. Somit kann ein Finder dieses Gerätes sich bei der angegebenen Telefonnummer melden. Diese Funktion ist nur für iOS- und Android-Geräte verfügbar. Mit dieser Funktion kann ein

Gerätezertifikat herunterladen: Das Gerätezertifikat können Sie hier für Geräte des Typs „Andere" herunterladen, um es manuell auf dem Gerät zu installieren. Das Zertifikat wird mit dem Rollout-Passwort verschlüsselt.

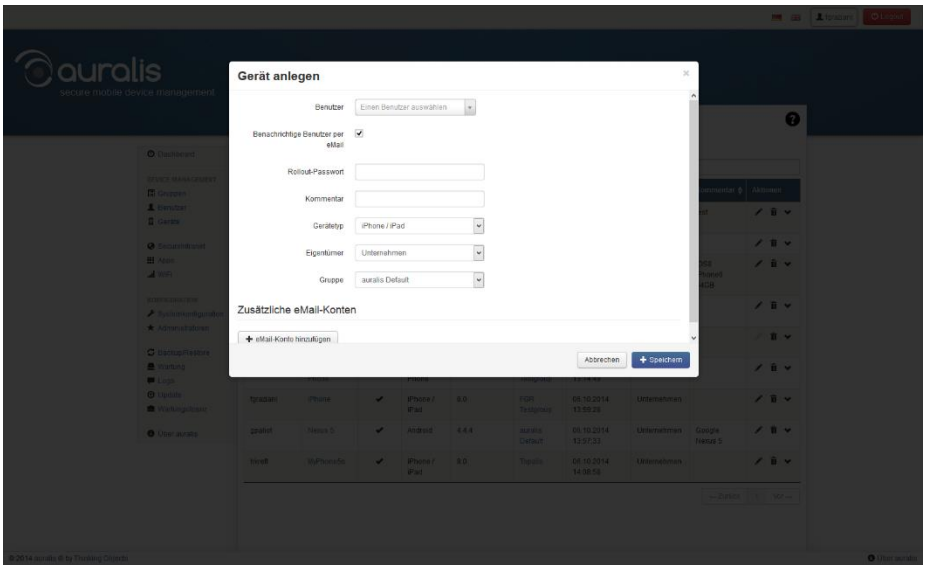
Push Message erneut senden: Mit dieser Option können Sie bei iOS-Geräten manuell eine erneute Push Message versenden. Eine Push-Message wird automatisch gesendet, sobald ein Befehl von auralis für das Gerät verfügbar ist. Gibt es keine Rückmeldung vom Gerät, wird in regelmäßigen Abständen erneut eine Push-Message gesendet.

Löschen: Diese Option hat die gleiche Funktion wie die Schaltfläche „Löschen" in der Spalte „Aktionen".

Bearbeiten: Diese Option hat die gleiche Funktion wie die Schaltfläche „Bearbeiten" in der Spalte „Aktionen".

3.5 Geräte hinzufügen

Ein Geräte können Sie alternativ über das Aktionsmenü in der Benutzerübersicht oder über den Menüpunkt „Gerät anlegen“ auf der Geräteübersichtsseite erstellen.



Benutzer: Hier wird der Benutzer ausgewählt für den das Gerät konfiguriert werden soll.

E-Mail Benachrichtigung: Hier können Sie entscheiden ob der Benutzer eine E-Mail mit weiteren Hinweisen (Anleitung) zum Rollout erhalten soll.

Rollout-Passwort: Vergeben Sie das Rollout Kennwort für die erstmalige Integration. Dieses Kennwort ist nur einmal gültig!

Kommentar: Geben Sie einen Kommentar für dieses Gerät ein.

Gerätetyp: Wählen Sie zwischen „iPhone/iPad“, „Android“, „Windows Phone“ und „Andere“.

Eigentümer: Wählen Sie den Eigentümer des Gerätes.

Gruppe: Wählen Sie die Gruppe in die dieses Geräte integriert werden soll.

Zusätzliche eMail Konten: Besteht der Bedarf einem Benutzer mehrere eMail Account zuzuweisen können Sie das hier tun.

4 Geräte – Rollout

Bitte befolgen Sie die Schritte in der Anleitung unter https://auralis.de/rollout, um Ihr Endgerät mit dem Unternehmensnetzwerk zu verbinden.

5 Globale Konfigurationen

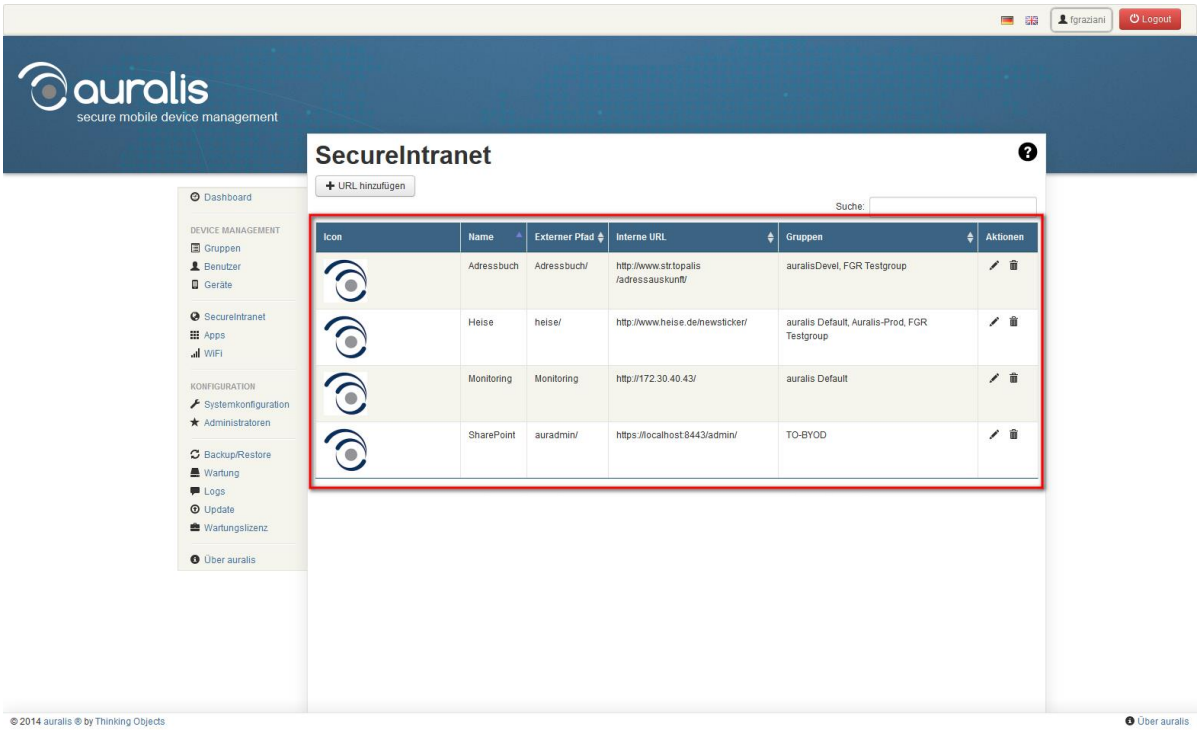
Globale Konfigurationen sind SecureIntranet Links, Webclips, App Verwaltung, WLAN, VPN Zugänge und Compliance.

5.1 SecureIntranet

Hinweis

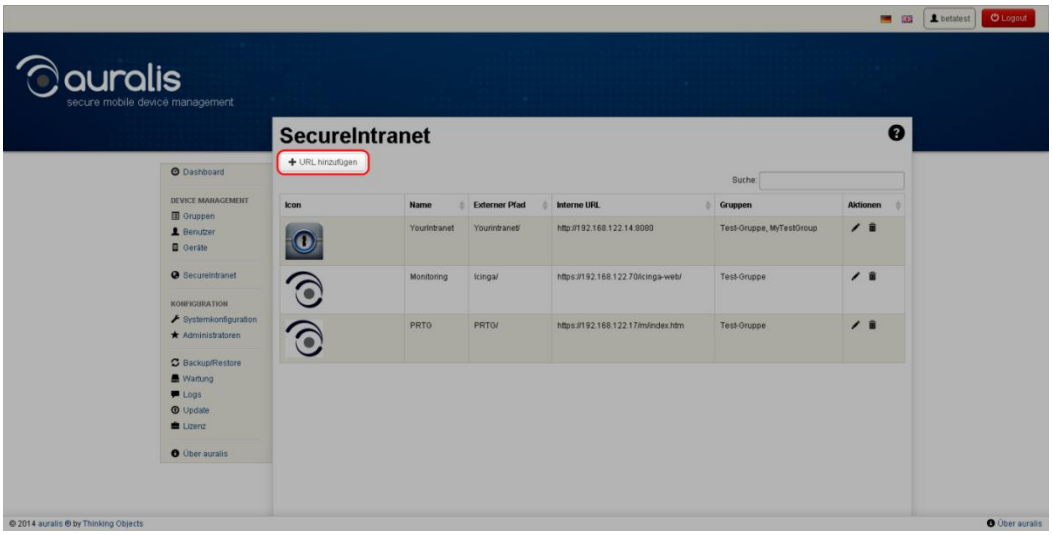
Das Feature SecureIntranet ist mit auralis 2.6 abgekündigt und wird nicht mehr weiterentwickelt. Es bleibt aber als solches mit dem jetzigen Funktionsumfang erhalten. Bitte haben Sie dafür Verständnis, dass wir keinen Support mehr anbieten können. Bitte beachten Sie, dass SecureIntranet nur mit sehr einfachen Seiten funktioniert.

Mit auralis® SecureIntranet greifen Sie einfach auf Ihr Intranet zu. Dazu benötigen Sie keine gesondert einzurichtende VPN-Verbindung, denn Sie sind bereits durch auralis sicher über SSL verschlüsselt mit Ihrem Firmennetzwerk verbunden. Beachten Sie das SecureIntranet nicht mit jeder Intranet Anwendung kompatibel sein kann.



URL hinzufügen

Um eine URL des Intranets für ausgerollte Geräte freizugeben, klicken Sie im Menü „SecureIntranet“ auf die Schaltfläche „URL hinzufügen“.



Eine Eingabemaske zum Erstellen eines neuen Eintrags öffnet sich. Tragen Sie hier alle erforderlichen Daten in die entsprechenden Felder ein.



Name: Geben Sie hier einen Namen für das neue SecureIntranet ein.

Externer Pfad: Unter dem angegebenen Pfad wird das SecureIntranet vom Endgerät erreichbar sein. Wenn Sie keine einzelne Datei freigeben, muss der Pfad mit „/" enden.

Interne URL: Geben Sie hier den internen Pfad zu der Seite des Intranets an, die Sie freigeben möchten. Wenn Sie keine einzelne Datei freigeben, muss die URL mit „/" enden.

Proxy: Leitet Anfragen an den Global konfigurierten Web Proxy weiter. Hinweis: Proxy-Authentifizierung wird nicht unterstützt.

Gruppen: Geben Sie an, für welche Gruppen das SecureIntranet verfügbar gemacht werden soll.

Sichtbar: Setzen Sie den Haken, wenn zu diesem SecureIntranet ein Icon auf dem Homescreen der entsprechenden Geräte angelegt werden soll.

Icon: Optional können Sie ein eigenes Icon für dieses SecureIntranet festlegen. Für eine optimale Darstellung sollte das Icon die Größe 114px x 114px bei 720dpi haben.

Fertiggestelltes Symbol: Aktivieren Sie die Option, um gerätespezifische visuelle Effekte nicht darzustellen.

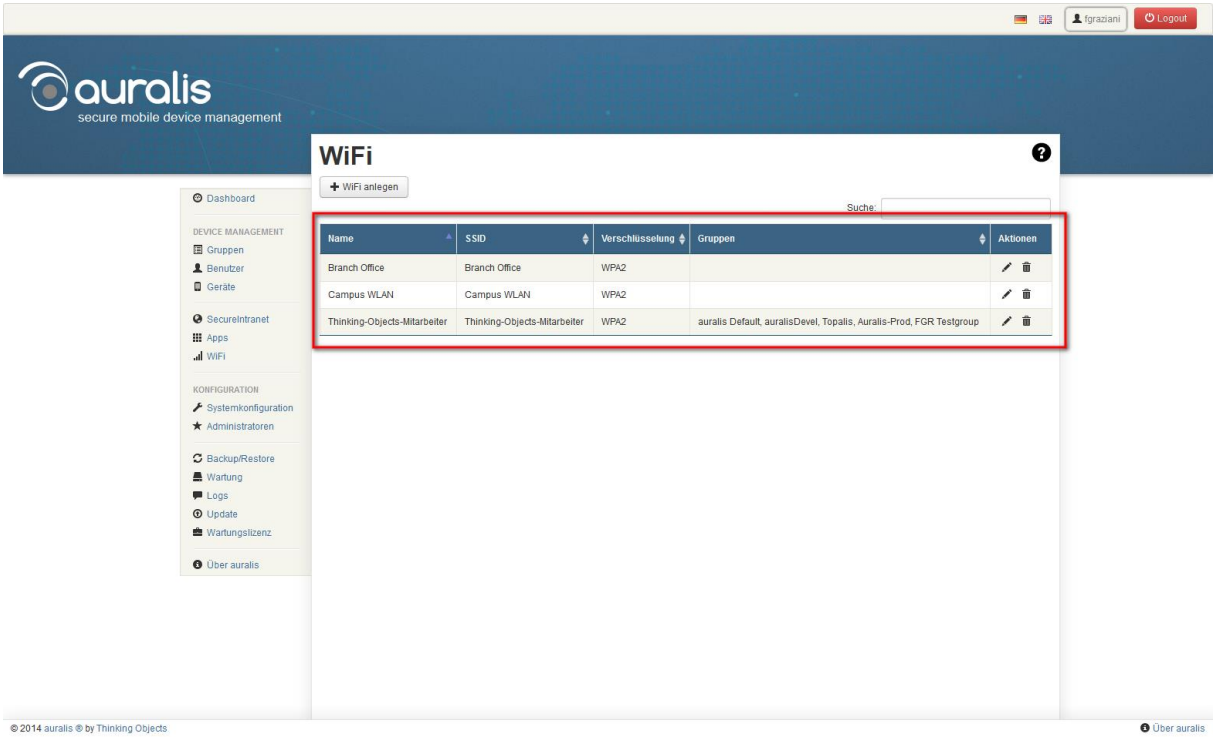
Hinweis

Um SecureIntranet auf einem Android-Gerät nutzen zu können, benutzen Sie bitte einen Browser, der zertifikatsbasierte Authentifizierung unterstützt.

Auf einem Windows Phone ist es derzeit leider nicht möglich auf SecureIntranet veröffentlichte Seiten zuzugreifen.

5.2 WiFi

In der zentralen WiFi Konfiguration können Sie alle Netze die Sie auf den Smartphones hinterlegen möchten Konfigurieren. Damit brauchen Sie keinem Benutzer mehr WLAN Kennwörter auszu händigen. Sobald ein Gerät in Reichweite eines bekannten WLAN's ist, verbindet sich dieses automatisch.



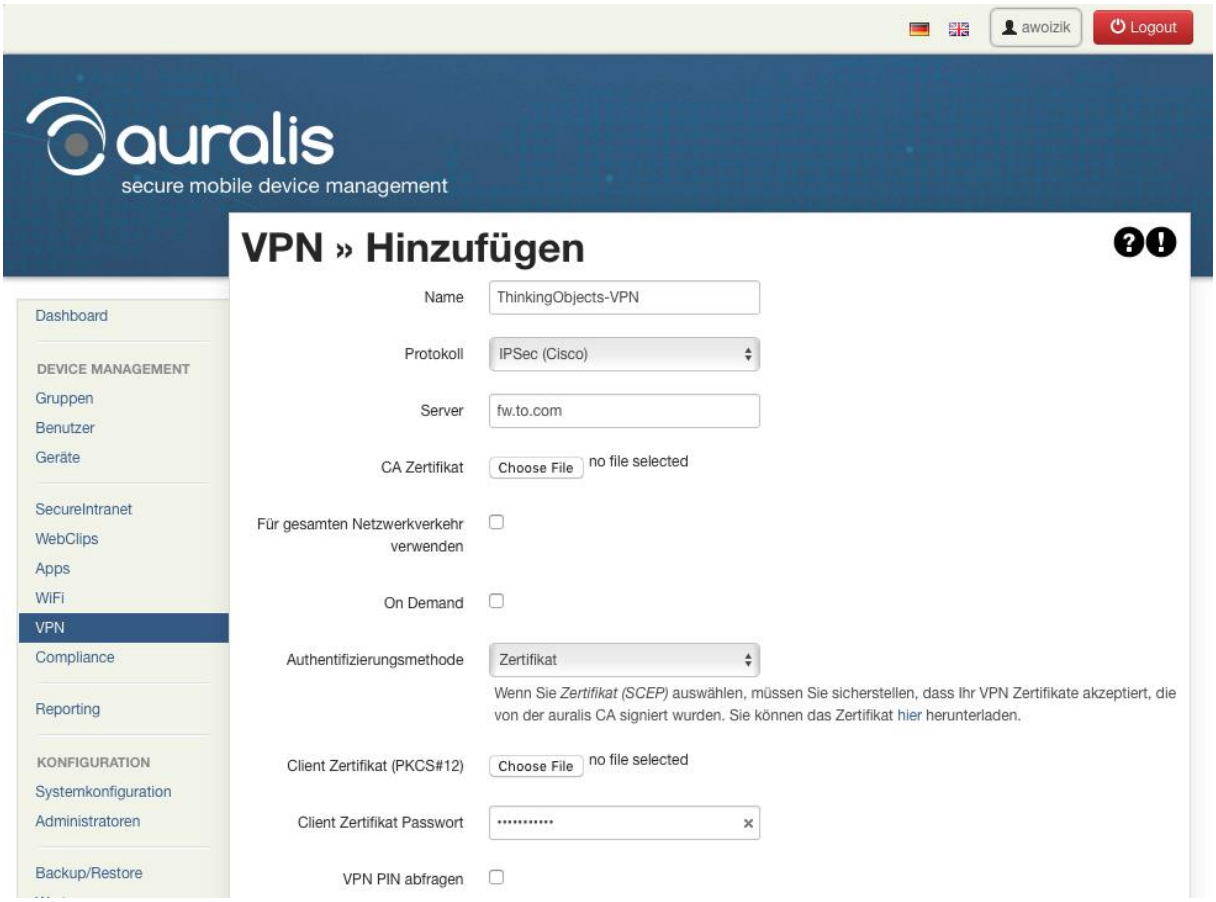
Um eine neue Konfiguration hinzuzufügen benutzen Sie die Schaltfläche „WiFi anlegen"

Konfiguration: In der Konfigurationsmaske finden Sie eine selbsterklärende Übersicht einer Standard WLAN Konfiguration.

5.3 VPN

In der zentralen VPN Konfiguration können Sie alle Netze die Sie auf den Smartphones hinterlegen möchten Konfigurieren. Diese können Sie später auch als „Per App VPN“ innerhalb der App Konfiguration hinterlegen.

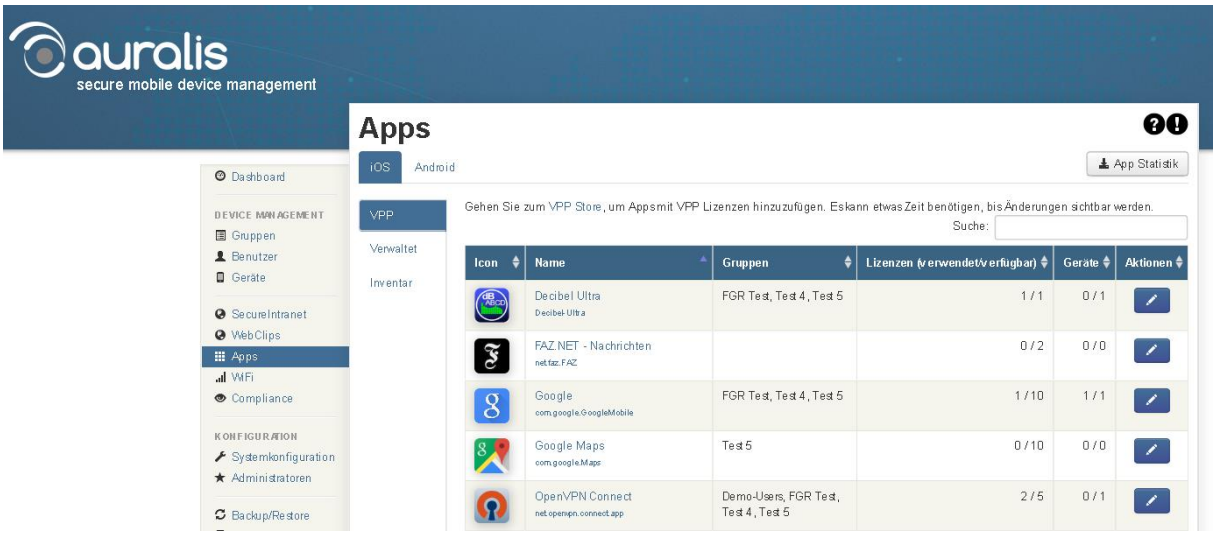
Um eine neue Konfiguration hinzuzufügen benutzen Sie die Schaltfläche „VPN anlegen“



Konfiguration: In der Konfigurationsmaske finden Sie eine selbsterklärende Übersicht einer Standard VPN Konfiguration.

5.4 APP Verwaltung

Die App Verwaltung bietet Ihnen die Möglichkeit, Apps für iOS & Android Smartphones, direkt aus dem jeweiligen Appstore automatisch zu installieren.



5.4.1 *iOS*

VPP: Wenn Sie einen Apple VPP Enterprise Account haben und dieser in der Systemkonfiguration hinterlegt ist, erscheinen an dieser Stelle automatisch Ihre gekauften Apps. In der Spalte Lizenzen sehen Sie wie viele Lizenzen erworben worden und verfügbar sind. Über die Aktion bearbeiten können Sie bereits Gruppen zuweisen oder die Geräteliste einsehen auf welchen diese App installiert ist.

Verwaltet: Suchen Sie Apps aus dem Apple Store und legen fest in welcher Gruppe diese App automatisch verteilt werden soll. Alternativ können Sie auch eigene entwickelte Apps hochladen und über auralis auf Ihre Smartphones installieren lassen.

Inventar: Hier sehen Sie alle Apps die auf allen Geräten installiert sind. Über das Aktionsmenü können Sie auch hier Apps in die automatische Verwaltung nehmen und einsehen welche Geräte bereits diese App installiert haben.

App Konfiguration: Unterstützt eine App die Konfiguration über eine Datei, können Sie diese hier hochladen und der App zuweisen.

5.4.2 *Android*

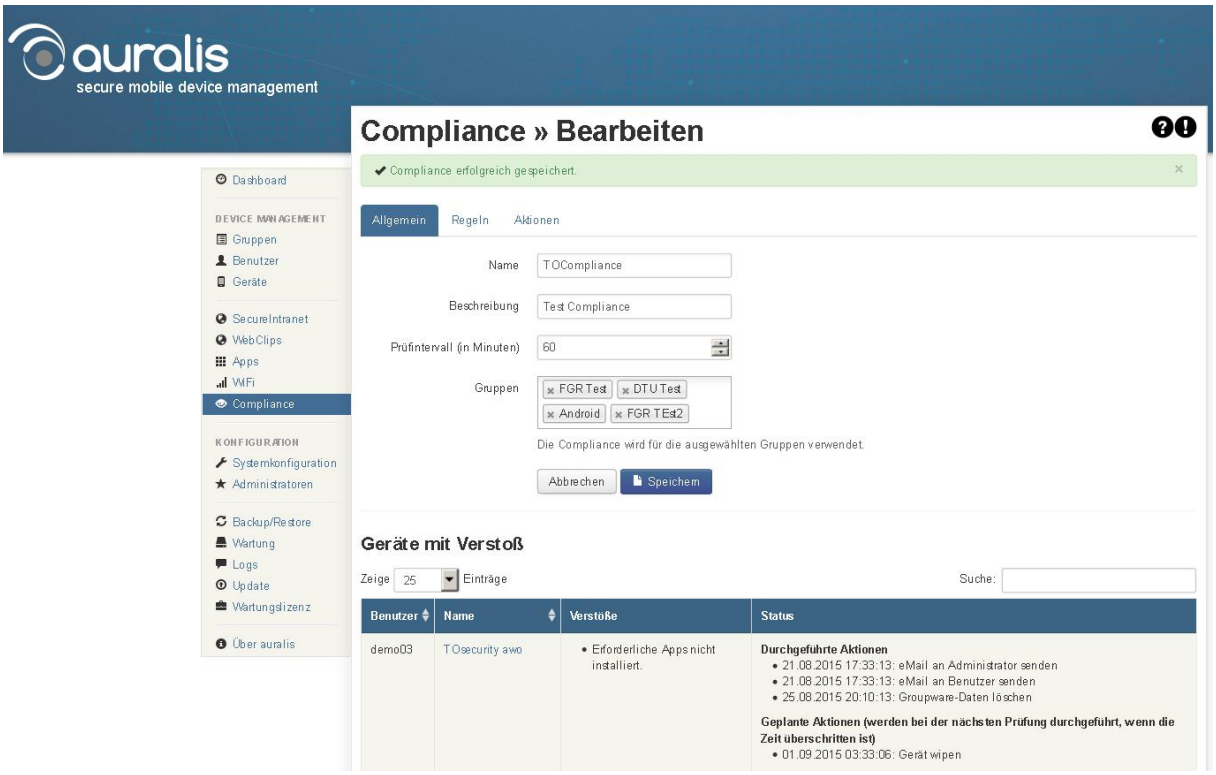
Verwaltet: Suchen Sie Apps aus dem Google Playstore und legen fest in welcher Gruppe diese App automatisch verteilt werden soll. Alternativ können Sie auch eigene entwickelte Apps hochladen und über auralis auf Ihre Smartphones installieren lassen.

Inventar: Hier sehen Sie alle Apps die auf allen Geräten installiert sind. Über das Aktionsmenü können Sie auch hier Apps in die automatische Verwaltung nehmen und einsehen welche Geräte bereits diese App installiert haben.

System Apps: Hier sehen Sie alle Werkseitig installieren Android System Apps.

5.5 Compliance

Mit den Compliance Einstellungen können Sie bestimmte Regeln definieren wie Ihre Geräte konfiguriert sein müssen. Die Endgeräte werden regelmäßig abgefragt. Bei Verstößen gegen diese Regeln können Sie bestimmte Aktionen durchführen.



Allgemein: Hier definieren Sie Name, Beschreibung, das Prüfintervall und die zugeordneten Gerätegruppen. In einer Übersicht sehen Sie die Geräte mit Compliance-Verstößen und den durchgeführten und geplanten Aktionen.

Regeln: An dieser Stelle können Sie globale, iOS, Android und Windows Phone spezifische Regeln definieren.



Global:

Timeout: Verletzt, wenn ein Gerät länger als definiert abwesend ist.
Verschlüsselt: Verletzt, wenn das Gerät nicht verschlüsselt ist.
Data Roaming: Verletzt, wenn im Gerät Daten-Roaming erlaubt ist.

Android:

Minimale OS Version: Verletzt, wenn die Version des installierten Betriebssystems kleiner ist.

Maximale OS Version: Verletzt, wenn die Version des installierten Betriebssystems größer ist.

Apps nicht aus Playstore: Verletzt, wenn die Installation von Apps, die nicht aus dem Play Store kommen, erlaubt ist.

Erforderliche Apps: Verletzt, wenn eine erforderliche App nicht installiert ist.

Verbotene Apps: Verletzt, wenn eine verbotene App installiert ist.

iOS:

Minimale OS Version: Verletzt, wenn die Version des installierten Betriebssystems kleiner ist.

Maximale OS Version: Verletzt, wenn die Version des installierten Betriebssystems größer ist.

Erforderliche Apps: Verletzt, wenn eine erforderliche App nicht installiert ist.

Verbotene Apps: Verletzt, wenn eine verbotene App installiert ist.

Windows Phone:

Minimale OS Version: Verletzt, wenn die Version des installierten Betriebssystems kleiner ist.

Maximale OS Version: Verletzt, wenn die Version des installierten Betriebssystems größer ist.

App Policy: Die App Policy ermöglicht es, ausgewählte Anwendungen zu verbieten (Blacklist) bzw. zu erlauben (Whitelist). Anwendungen können über die Suche, ihre GUID oder ihren Herausgeber ausgewählt werden.

Der übliche Weg, eine Anwedungs GUID oder einen Herausgeber zu finden, ist über den Windows Phone App Store. Die Anwednungs GUIDs sind Teil der URL zur Anwendung. Zum Beispiel enthält die URL

*http://www.windowsphone.com/de-de/store/app/flashlight/**3a81b414-7e97-4697-8c27-9ee0802846f8*** die Anwendungs GUID *3a81b414-7e97-4697-8c27-9ee0802846f8*.

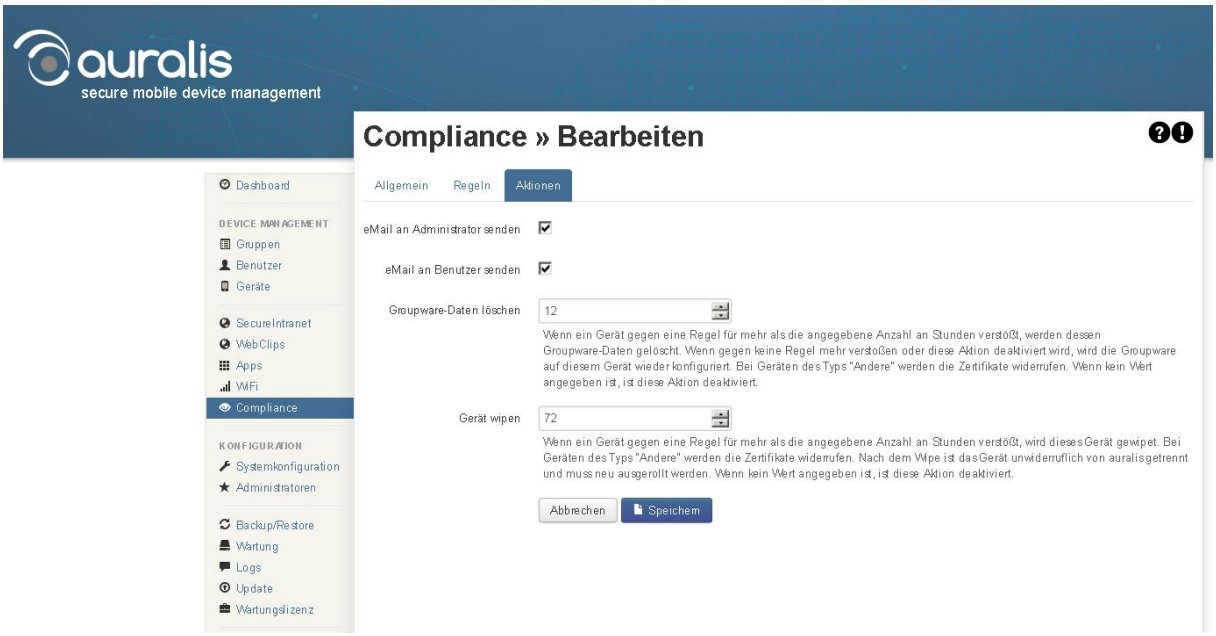
Aktionen: Bei Regelverstößen können Sie zwischen bestimmten Aktionen auswählen.

eMail an Administrator senden: Der Administrator bekommt eine eMail mit dem Verstoß und den geplanten Aktionen, wenn ausgewählt.

eMail an Benutzer senden: Der Benutzer bekommt eine eMail mit dem Verstoß und den geplanten Aktionen, wenn ausgewählt.

Groupware-Daten löschen: Das E-Mail Profil wird vom Endgerät nach einem definierten Zeitraum gelöscht bis das Gerät wieder den Compliance Richtlinien entspricht.

Gerät wipen: Das Gerät wird komplett aus dem Mobile Device Management nach dem definierte Zeitraum gelöscht und muss neu ausgerollt werden!



5.6 Reporting

Hier finden Sie ein Auswahl an Reporting Möglichkeiten per PDF oder Excel. Ebenso können Sie diese per Scheduler planen. Mehrer Empfänger sind durch ein Komma zu trennen.

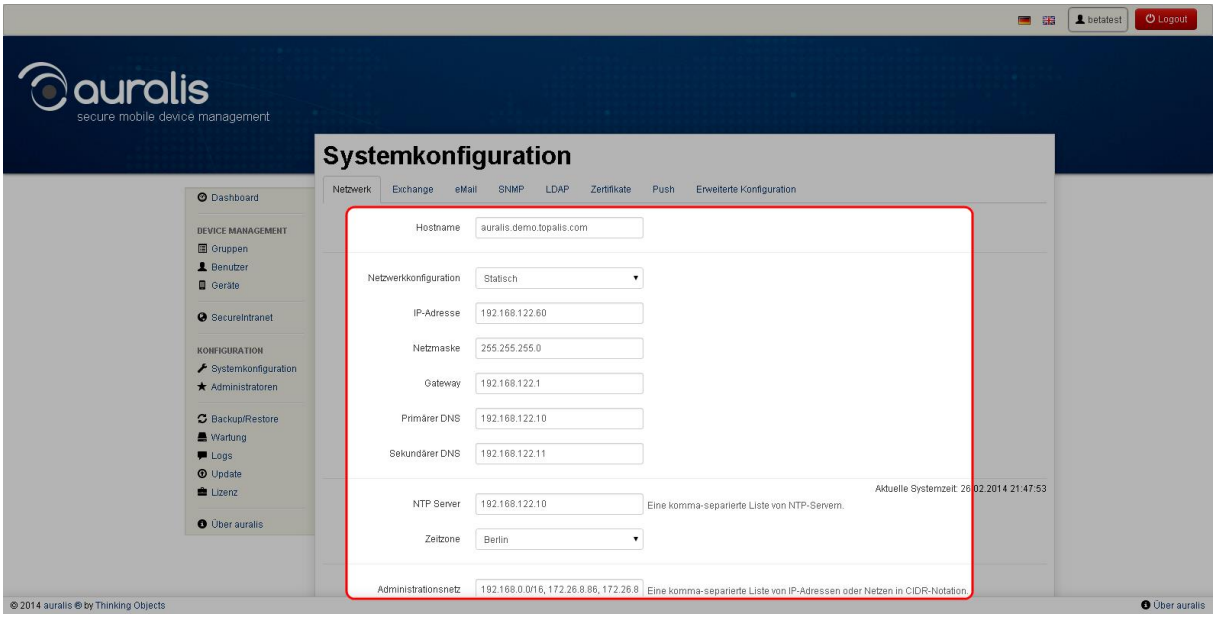


6 Systemkonfiguration

In der Systemkonfiguration können Sie grundlegende Einstellungen vornehmen und auralis passend zu Ihrer IT-Infrastruktur konfigurieren.

6.1 Netzwerk

Im Reiter „Netzwerk“ finden Sie alle relevanten Einstellungen zur Verbindung von auralis.



Hostname: Geben Sie hier den Hostname ein, unter dem Ihr auralis-System erreichbar ist. Dieser besteht entweder aus einer Sub-Domain oder einer eigenständigen Domain.

> ***Hinweis***
>
> Bei einer Domain muss es sich um einen A-Record im DNS (Domain Name System) handeln.

Netzwerkkonfiguration: Wählen Sie hier zwischen den Optionen „Statisch“ und „DHCP“. Wird dem System, auf dem auralis läuft, automatisch eine IP durch einen DHCP-Server in Ihrem Netzwerk zugewiesen, wählen Sie „DHCP“. Wählen Sie andernfalls „Statisch“ und geben Sie die erforderlichen Daten in die vorgesehenen Felder ein.

IP-Adresse: Geben Sie hier die IP-Adresse ein, die für das auralis-System vorgesehen ist.

Netzmaske: Geben Sie hier die Netzmaske des Netzwerks ein, in dem das auralis-System arbeiten wird.

Gateway: Gebens Sie hier die IP-Adresse des Gateway-Servers ein.

Primärerer DNS: Geben Sie hier die IP-Adresse des gewünschten DNS-Servers (Domain Name System) ein.

Sekundärer DNS: Geben Sie hier die IP-Adresse eines alternativen DNS-Servers ein. Auf diesen DNS-Server greift auralis zu, wenn der primäre DNS-Server nicht erreichbar ist.

NTP-Server: Geben Sie hier mindestens eine IP-Adresse oder einen DNS-Namen eines NTP-Servers ein. Von den angegebenen NTP-Servern bezieht auralis die aktuelle Systemzeit, welche Sie zur Kontrolle auf der rechten Seite angezeigt bekommen. Die angezeigte Uhrzeit entspricht dem Zeitpunkt des Seitenaufrufs. Sie können mehrere NTP-Server angeben, indem Sie die verschiedenen IPs durch Kommata trennen.

Zeitzone: Geben Sie hier die Zeitzone an, in der der auralis-Server sich befindet.

Administrationsnetz: Geben Sie an, aus welchen Netzen auf die auralis-Weboberfläche zugegriffen werden darf. Verwenden Sie hier die CIDR-Notation. Sie können mehrere Netze angeben, indem Sie sie durch Kommata trennen.

> ***Hinweis***
>
> Sollte Ihr auralis-System aufgrund der Netzwerkkonfiguration nicht mehr erreichbar sein, können Sie diese anpassen, indem Sie das System über den Eintrag „CentOS Configure“ im Menü des Boot-Loaders starten. Das Administrationsnetz wird dabei zurückgesetzt.

Proxy: Greift das auralis-System über einen Proxy auf das Web zu, muss die IP-Adresse oder der DNS-Name des Proxy-Servers hier eingegeben werden. Trennen Sie IP-Adresse bzw. DNS-Name und Port des Proxy-Servers durch einen Doppelpunkt.

Proxy-Benutzername: Geben Sie hier den Benutzername zur einfachen Proxy-Authentifizierung ein, wenn diese erforderlich ist.

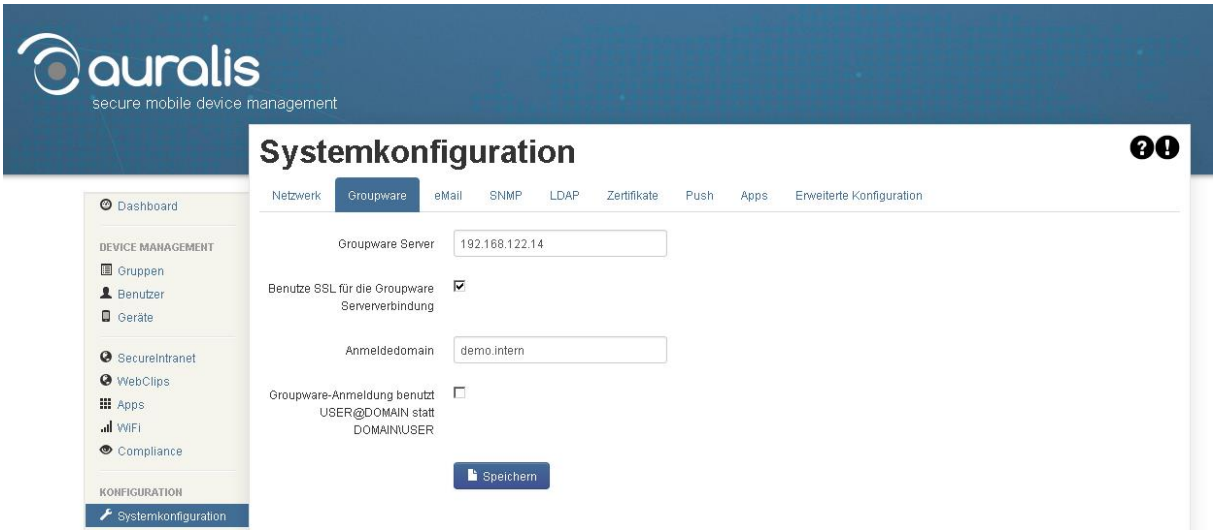
Proxy-Passwort: Geben Sie hier das zum Benutzername zugehörige Passwort zur einfachen Proxy-Authentifizierung ein.

> ***Hinweis***
>
> Die folgenden Felder müssen nur ausgefüllt werden, wenn der Zugriff auf das Web über einen Proxy erfolgt. Der Web-Zugriff wird benötigt, um den Google Cloud Messaging-Service (s. Kapitel „Push“) zu erreichen und Updates zu laden.

Klicken Sie auf die Schaltfläche „Speichern“, um die eingegebenen Daten zu übernehmen und anzuwenden.

6.2 Groupware

In diesem Einstellungs-Reiter konfigurieren Sie den Zugang zum Groupware-Server.



Groupware-Server: Geben Sie hier die IP-Adresse des E-Mail-Servers ein, auf den auralis zugreifen soll.

Benutze SSL für die Serververbindung: Setzen Sie den Haken bei dieser Option, wenn auralis nur über eine SSL-Verbindung (Secure Sockets Layer) mit dem Groupware-Server kommunizieren soll. Diese Option verbessert die Abhörsicherheit der Kommunikation zwischen auralis und dem Groupware-Server.

Anmeldedomain: Geben Sie die Anmeldedomain des Groupware-Servers ein.

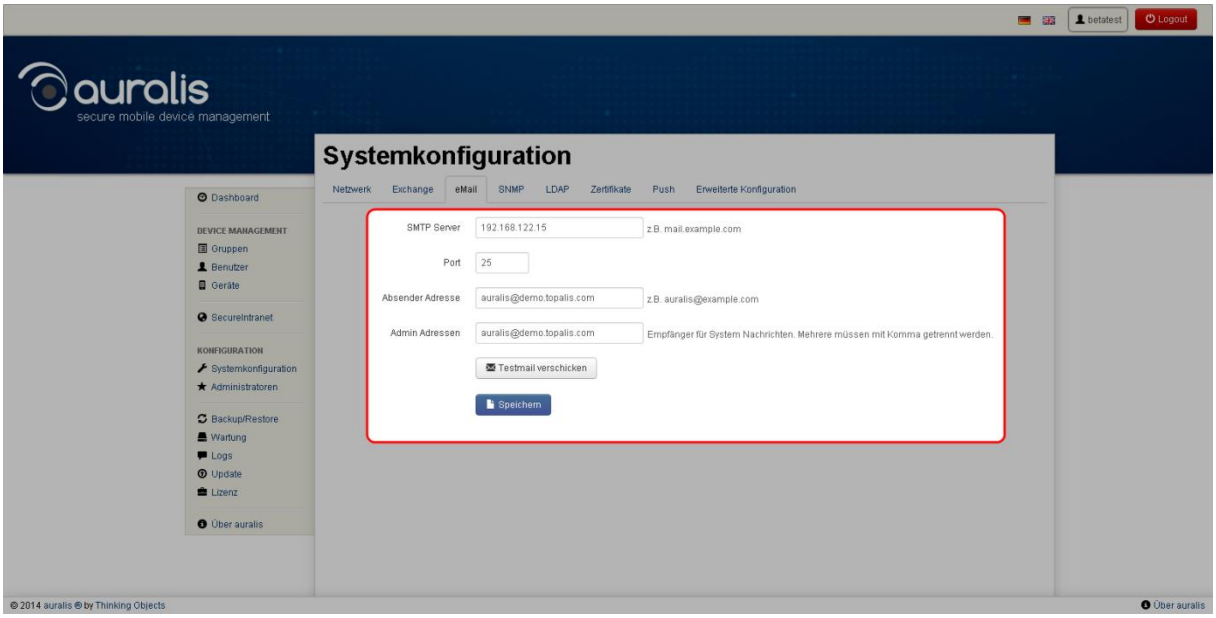
Exchange-Anmeldung: Geben Sie an, ob bei der Anmeldung am Groupware-Server die Schreibweise „User@Domain“ oder „Domain\User“ genutzt werden soll.

Klicken Sie auf die Schaltfläche „Speichern“, um die eingegebenen Daten in auralis zu übernehmen.

6.3 eMail

Im Reiter „eMail“ wird der Versand von eMails aus auralis eingestellt. Über den angegebenen Server werden alle eMails gesendet.

Geben Sie hier alle nötigen Informationen ein, die zum Versenden von eMails notwendig sind.



SMTP-Server: Geben Sie hier die IP-Adresse oder die Domain des zu verwendenden Mail-Servers ein.

Port: Geben Sie hier den Port zum SMTP-Server ein, über den die Verbindung aufgebaut werden soll.

Absenderadresse: Geben Sie hier an, mit welcher Adresse auralis eMails versenden soll. Diese Adresse wird für alle eMails verwendet, die von auralis gesendet werden.

Admin Adresse: Geben Sie hier an, wohin eMails mit System-Nachrichten versendet werden sollen. Sie können mehrere Adressen angeben, indem Sie diese per Komma trennen.

Über die Schaltfläche *„Testmail verschicken“* veranlassen Sie den Versand einer Testmail an die angegebenen Administrator-Adressen zur Überprüfung der Konfiguration.

Klicken Sie auf die Schaltfläche „Speichern“, um die eingegebenen Daten in auralis zu übernehmen.

6.4 SNMP

auralis kann per SNMP Status-Informationen des Systems liefern. Neben allgemeinen Daten werden auch auralis-spezifische Daten bereitgestellt. Diese befinden sich unterhalb der OID „1.3.6.1.4.1.4952.3.1.100“ und beinhalten folgende Werte (s. MIB-Datei auf der Konfigurationsseite):

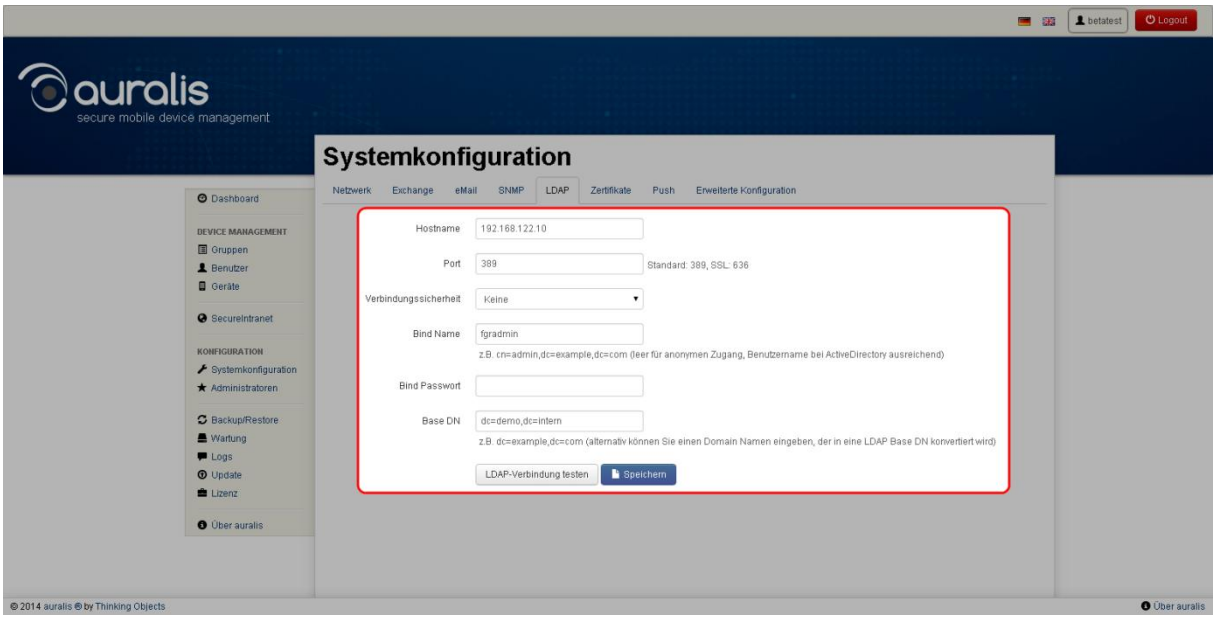
- Anzahl der kürzlich aktiven Geräte (das heißt: ein Zugriff innerhalb der letzten 5 Minuten)
- Anzahl der registrierten Geräte
- Der gesamte eMail Traffic
- Der eingesparte eMail Traffic
- Das Lizenzablaufdatum
- Die Anzahl der erlaubten Benutzer
- Die Anzahl der verfügbaren Benutzer

Darüber hinaus finden Sie im Unterzweig „1“ spezifische Informationen zu jedem Gerät. Jeder Eintrag beginnt mit einer aufsteigenden Geräte ID. Folgende Daten werden für jedes Gerät bereitgestellt:

- Aufsteigende Geräte ID
- Letzte IP-Adresse
- Zeitpunkt des letzten Zugriffs
- Vom Gerät gelieferte ID
- Kommentar
- Deaktiviert ja/nein
- Verbunden (das heißt: ein Zugriff innerhalb der letzten 5 Minuten)
- eMail Traffic

6.5 LDAP

In den LDAP-Einstellungen können Sie die Verbindung zu einem LDAP-Server konfigurieren und verwalten.



Die Verbindung zu einem LDAP-Server ist erforderlich, wenn Sie die Funktion zum automatischen Anlegen von Benutzern verwenden möchten.

Hostname: Geben Sie hier die IP-Adresse oder den Hostname des zu verwendenden LDAP-Servers ein

Port: Geben Sie hier den Port ein, über den auralis die Verbindung zum LDAP-Server aufbauen soll. Standardmäßig wird für LDAP Port 389 (SSL: 636) verwendet.

Verbindungssicherheit: Geben Sie an, ob die Verbindung zwischen dem LDAP-Server und auralis verschlüsselt werden soll. Wählen Sie gegebenenfalls zwischen „SSL“ und „TLS“.

Bind Name: Der Bind Name gibt den Namen an, mit dem sich auralis am LDAP-Server anmelden soll.

Bind Password: Das Bind Password gibt das Passwort an, das zur Authentifizierung am LDAP-Server verwendet wird.

Base DN: Geben Sie in diesem Feld den Base Domain Name ein. Alternativ können Sie einen Domain Namen eingeben, der in eine LDAP Base DN konvertiert wird.

Klicken Sie auf die Schaltfläche *„LDAP-Verbindung testen“,* um die Konfiguration testen zu lassen. Sollte in der Konfiguration ein Fehler vorliegen, wird auralis einen Fehler-Code zurückliefern. Ist der Verbindungstest erfolgreich, meldet auralis „Verbindung zum LDAP-Verzeichnis erfolgreich“.

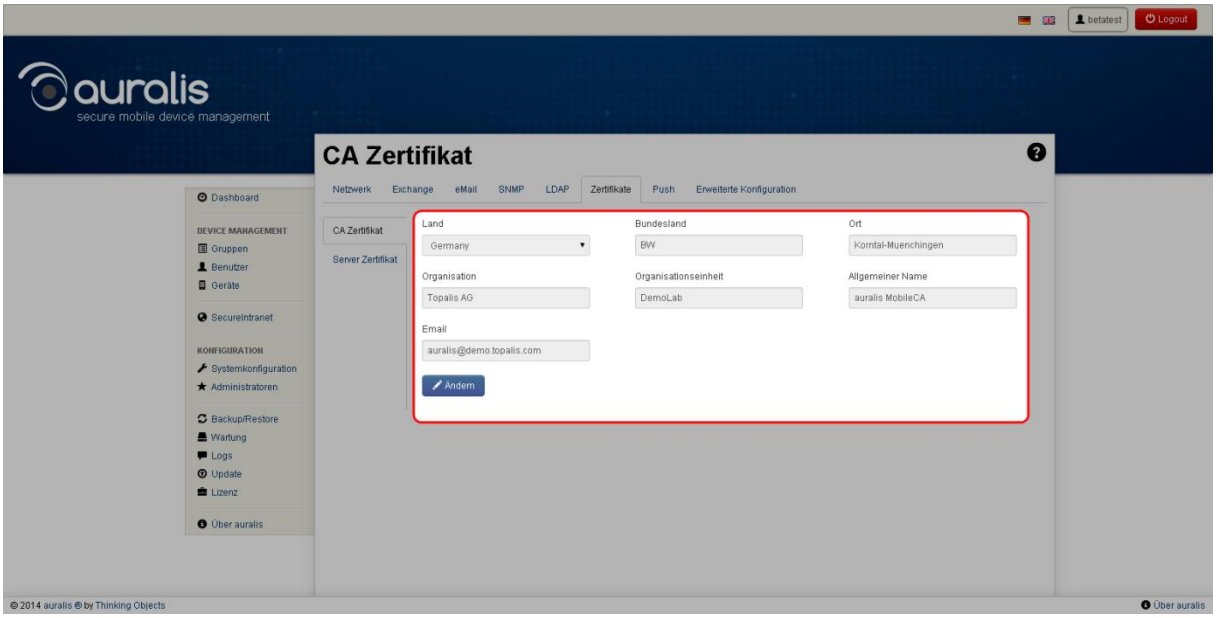
Klicken Sie auf die Schaltfläche „Speichern“, um die eingegebenen Daten in auralis zu übernehmen.

6.6 Zertifikate

CA Zertifikat

Die Certificate Authority (CA) des Servers wird zur Signierung des Serverzertifikats und der Client-Zertifikate eingesetzt. Zudem wird sie auf jedem Gerät installiert, um die von auralis gesendeten Zertifikate zu verifizieren.

Zum Schutz vor Änderungen sind die Angaben des CA Zertifikats schreibgeschützt. Um die Einträge im Zertifikat zu editieren, klicken Sie auf die Schaltfläche „Ändern“.

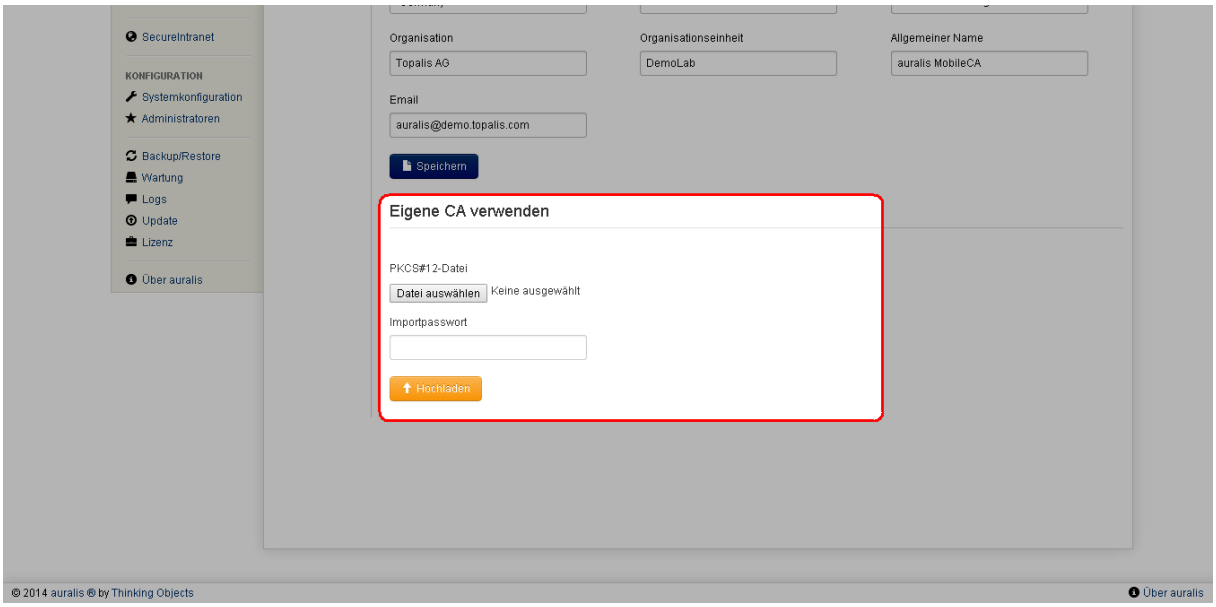


Wenn Sie das darauffolgende Formular speichern, wird ein neues CA-Zertifikat erzeugt.

Vorsicht

Wenn Sie an der CA Änderungen vornehmen, vertraut kein verbundenes Gerät mehr dem auralis-Server. In diesem Fall müssen die Geräte neu ausgerollt werden.

Alternativ können Sie ein eigenes Zertifikat hochladen.



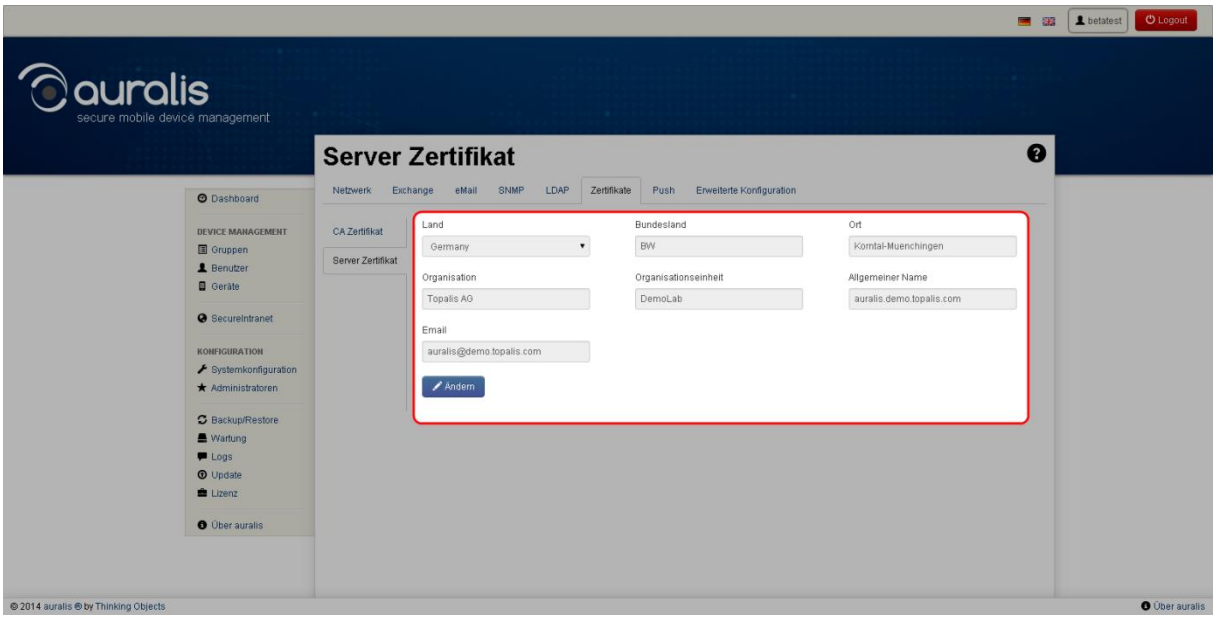
Wählen Sie hierfür im Feld „PKCS#12-Datei“ ein CA Zertifikat aus, das Sie in auralis importieren möchten. Geben Sie dann in das Feld „Importpasswort“ das Passwort für Ihr CA Zertifikat ein und klicken Sie dann auf die gelbe Schaltfläche „Hochladen“.

Vorsicht

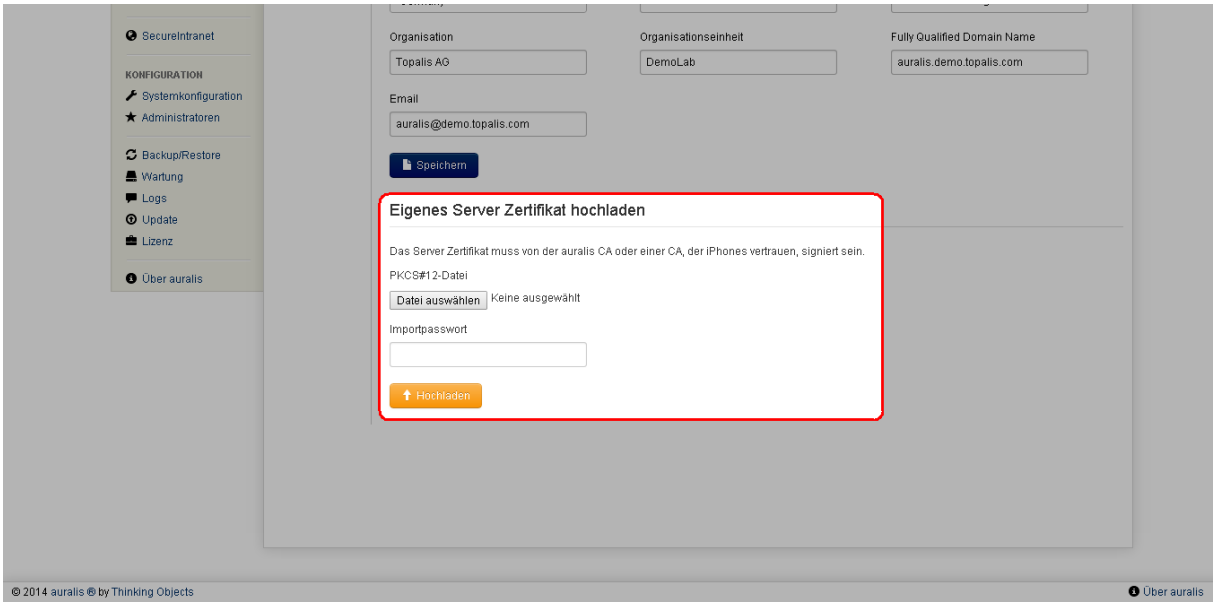
Wenn Sie an der CA Änderungen vornehmen, vertraut kein verbundenes Gerät mehr dem auralis-Server. In diesem Fall müssen die Geräte neu ausgerollt werden.

Server Zertifikat

Das Server Zertifikat wird von auralis dazu verwendet, sich gegenüber den verbundenen Geräten zu authentifizieren. Dieses Zertifikat wird von der CA unterschrieben und kann deshalb verändert werden, ohne alle Geräte neu ausrollen zu müssen. Um die Einträge im Zertifikat zu editieren, klicken Sie auf die Schaltfläche „Ändern“. Sie können die Angaben im Server-Zertifikat jetzt verändern. Klicken Sie danach auf „Speichern“, um ein neues Zertifikat mit den eingegebenen Daten zu erzeugen.



Alternativ können Sie ein eigenes Server-Zertifikat hochladen. Klicken Sie dazu auf den Button „Auswählen…“ und wählen Sie das Zertifikat aus, das Sie in auralis importieren möchten. Geben Sie zusätzlich das Passwort ein, mit dem das Zertifikat geschützt ist und klicken Sie dann auf „Hochladen“. Stellen Sie sicher, dass die Endgeräte dem hochgeladenen Zertifikat vertrauen.



6.7 Push Dienste

Im Menü „Push“ können die Zugänge zu den Push-Services von Apple (Apple Push Notification Service [APNS]) und Google (Google Cloud Messaging [GCM]) konfiguriert werden.

An die Push-Services wird eine Push-Message gesendet, wenn ein neues MDM-Kommando erstellt wurde. Diese Push-Message enthält das Push-Token des jeweiligen Geräts. Mit diesem identifiziert der Push-Service das Gerät und sendet die Nachricht an dieses weiter. Daraufhin meldet sich das Gerät beim auralis-System, um die verfügbaren Kommandos abzurufen. Die von auralis gesendeten Push-Messages dienen lediglich zur Aufforderung an ein Gerät, das auralis-System zu kontaktieren und enthalten keinerlei Nutzdaten.

Android- und iOS-Geräte haben eine permanente Verbindung zu ihrem Push-Service, um mit möglichst geringer Verzögerung Push-Messages zu empfangen. Ein vergleichbares System existiert für Windows Phone derzeit nicht – Geräte mit diesem System fragen in regelmäßigen Abständen bei auralis nach neuen Kommandos, so dass diese das Gerät nur mit Verzögerung erreichen. Ein manueller Abruf der verfügbaren Kommandos ist möglich. Navigieren Sie hierfür zu „Einstellungen → Unternehmens-Apps“ und wählen Sie das entsprechende Exchange-Konto aus. Drücken Sie dann den Button zum Synchronisieren des Kontos.

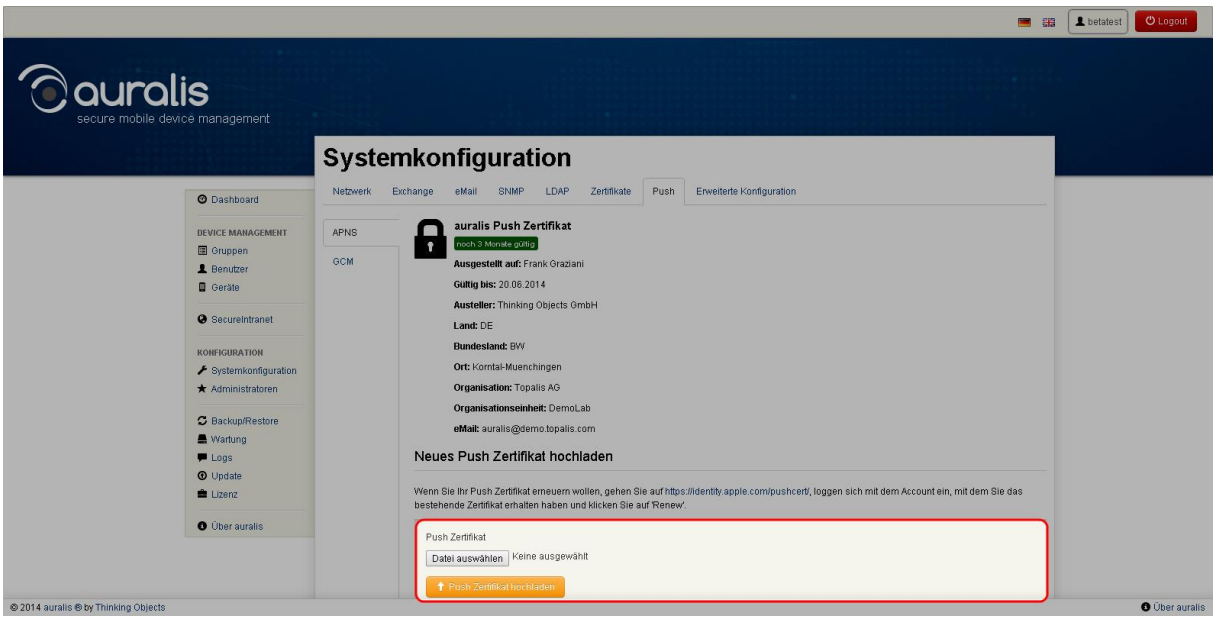
Erhält ein Android- oder iOS-Gerät keine Push-Messages, zum Beispiel wegen Ausfall des Push-Services, wird es keine MDM-Kommandos von Ihrem auralis-System abrufen. In der auralis App für Android kann in solch einem Fall manuell der Abruf verfügbarer Kommandos angestoßen werden. Öffnen Sie hierfür die auralis App und drücken Sie den Button in der rechten oberen Ecke , um das Gerät mit auralis zu synchronisieren.

6.7.1 Apple Push Dienst

Sollten Sie bereits ein Apple Push Zertifikat in auralis importiert haben, werden Ihnen mit einem Klick auf das Menü „Apple Push“ alle Informationen über das Zertifikat angezeigt. Oberhalb der Informationen zeigt Ihnen auralis zudem, wie lange das Zertifikat noch gültig ist.

Um Push-Messages über den Apple Push Notification Service zu senden, benötigen Sie ein von Apple signiertes Push Zertifikat. Um ein neues Zertifikat von Apple zu erhalten oder Ihr bestehendes Zertifikat zu erneuern besuchen Sie bitte diese Seite https://identity.apple.com/pushcert/ und folgen Sie den dort beschriebenen Schritten.

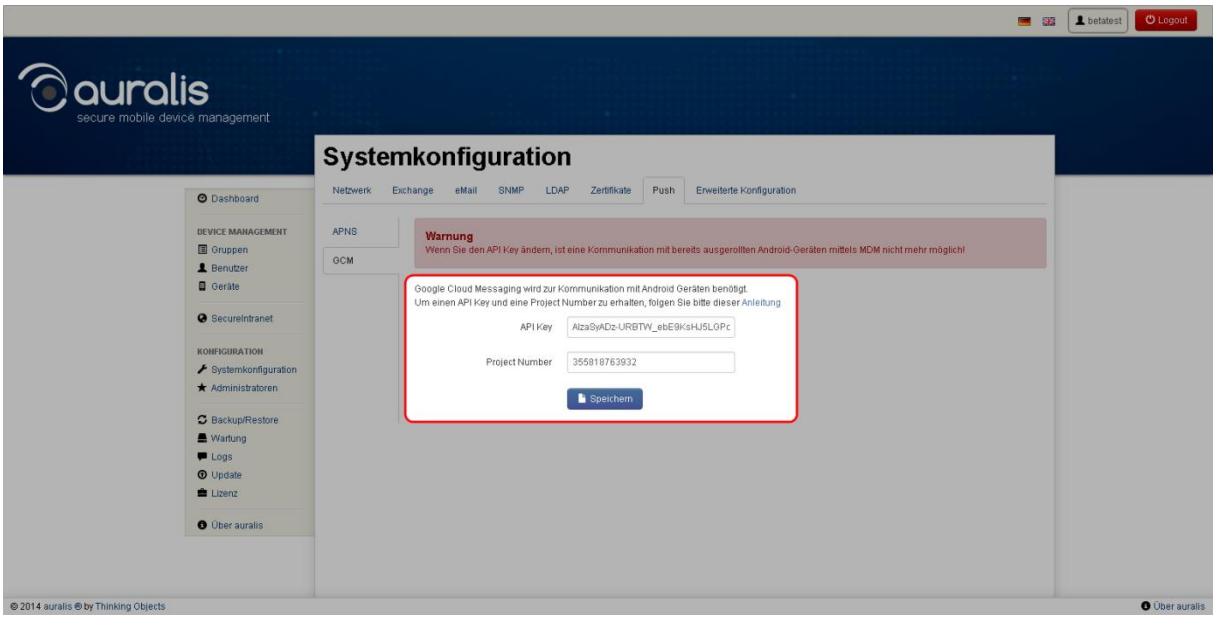
Das Push-Zertifikat von Apple können Sie dann unter „Neues Push Zertifikat“ hochladen. Wählen Sie dazu die Datei auf Ihrem Computer aus und klicken Sie dann auf die gelbe Schaltfläche „Push Zertifikat hochladen“. Das Push-Zertifikat ist dann in auralis eingebunden und wird für alle iOS-Geräte verwendet.



6.7.2 Google Push Dienst

Für den Zugriff auf Google Cloud Messaging, den Push-Service von Google, benötigen Sie einen API Key und eine „Project Number“. Diese können Sie bei Google anfordern, wie hier beschrieben https://auralis.de/gcm .

Geben Sie dann den erhaltenen API Key und die „Project Number“ in die zwei vorhergesehenen Felder ein. Klicken Sie anschließend auf die Schaltfläche „Speichern“, um die eingegebenen Daten in auralis zu übernehmen.



Vorsicht

Wenn Sie den API Key nachträglich ändern, ist eine Kommunikation mit bereits ausgerollten Android-Geräten mittels MDM nicht mehr möglich.

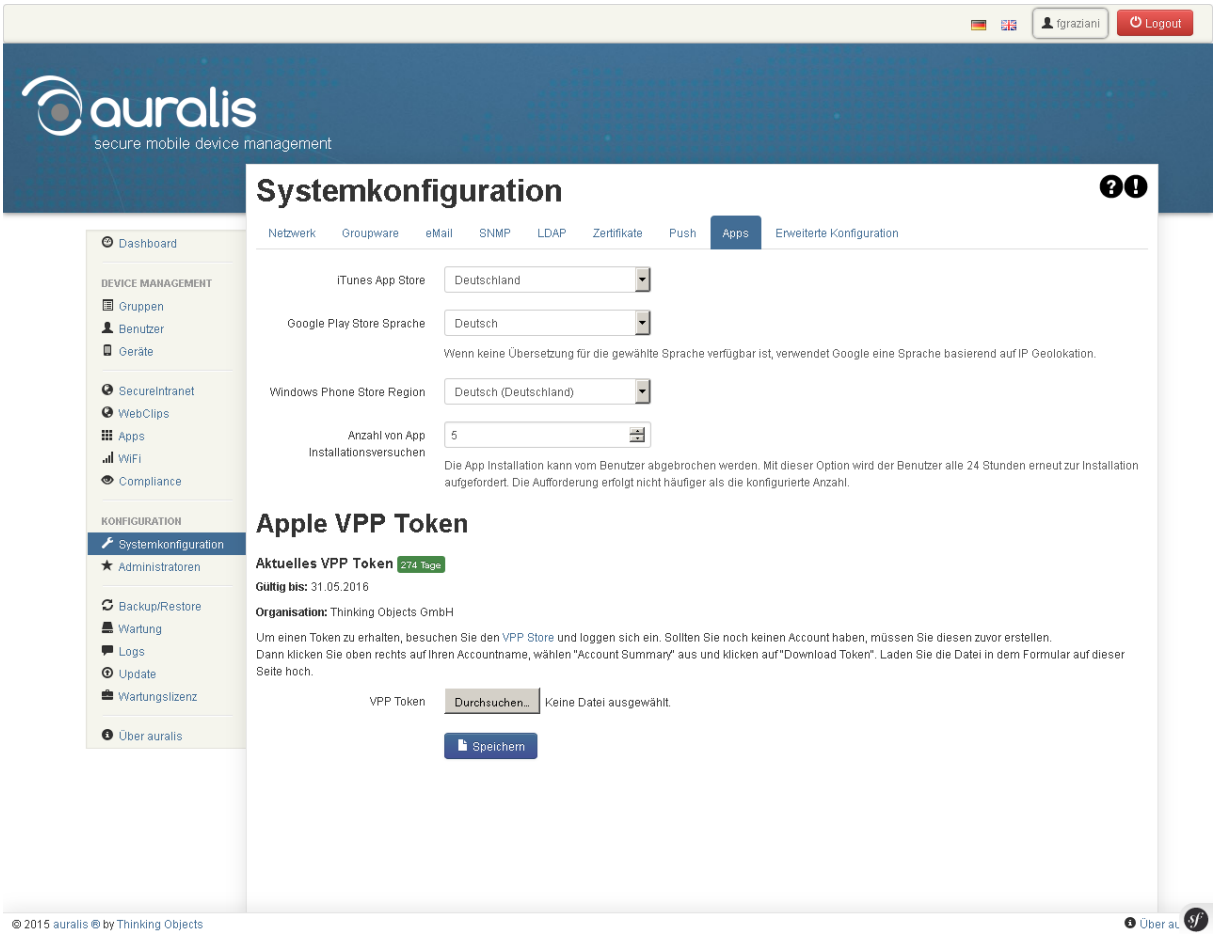
6.8 Apps

In den App Einstellungen können Sie die App Store Regionen und das Apple VPP Token hinterlegen.

Um Sich für das Apple VPP Programm zu registrieren besuchen Sie folgende Webseite und befolgen die Anweisungen.

http://www.apple.com/de/business/programs/

Nach erfolgreicher Registrierung können Sie im „Account Summary“ das Token herunterladen und in auralis importieren. Über Apple VPP gekaufte Apps erscheinen nun automatisch in der globalen App Konfiguration.

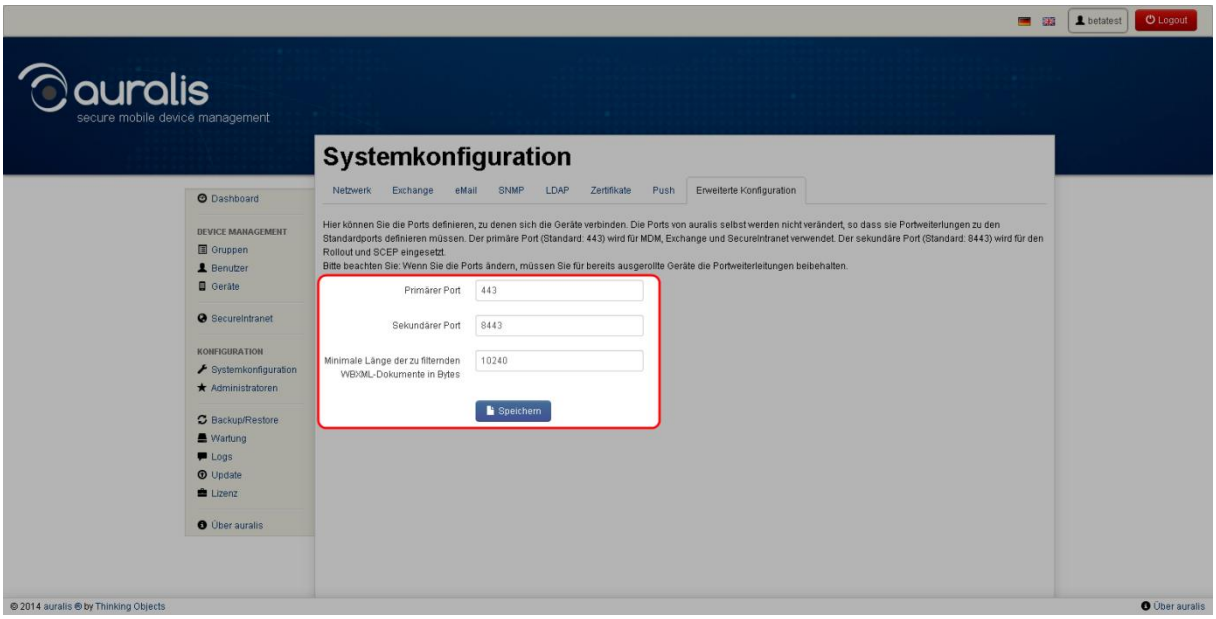


6.9 Erweiterte Konfiguration

In der erweiterten Konfiguration können Sie die Ports definieren, zu denen sich die Geräte verbinden. Die Ports von auralis selbst werden nicht verändert, sodass sie Portweiterlungen zu den Standardports definieren müssen. Der primäre Port (Standard: 443) wird für das Mobile Device Management (MDM), Exchange und SecureIntranet verwendet. Der sekundäre Port (Standard: 8443) wird für den Rollout und das Simple Certificate Enrollment Protocol (SCEP) eingesetzt.

Hinweis

Stellen Sie nach einer Änderung sicher, dass die Weiterleitungen bestehen bleiben und ausgerollte Geräte die bisherigen Ports weiterhin erreichen können.



Im Feld „Minimale Länge der zu filternden WBXML-Dokumente in Bytes“ können Sie angeben, ab welcher Größe von ActiveSync-Nachrichten von auralis bearbeitet werden sollen. Dieser Wert ist standardmäßig auf 10240 Bytes eingestellt. Kleinere E-Mail-Nachrichten werden von auralis unverändert durchgeleitet.

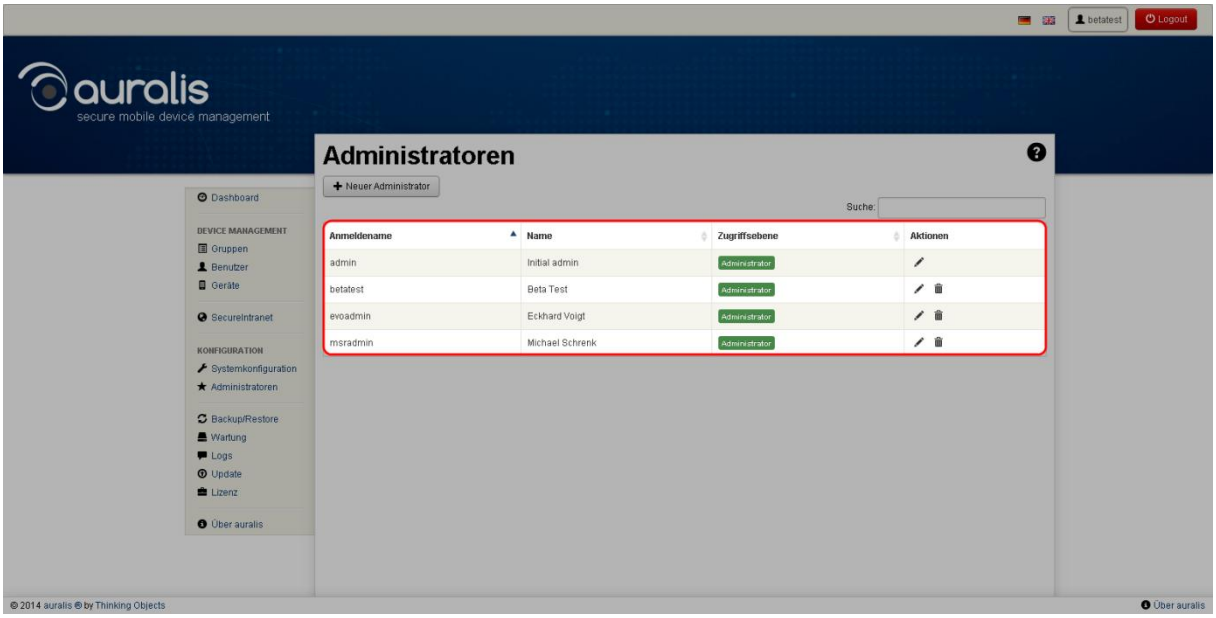
Hinweis

Sollten über auralis viele nicht komprimierbare Dateien geschickt werden, kann es einen Performance-Vorteil mit sich bringen, wenn Sie die minimale Länge der zu filternden WBXML-Dokumente über die Dateigröße der Dateien erhöhen.

Klicken Sie nach einer Änderung auf die Schaltfläche „Speichern“, um die angegebenen Daten in auralis zu übernehmen.

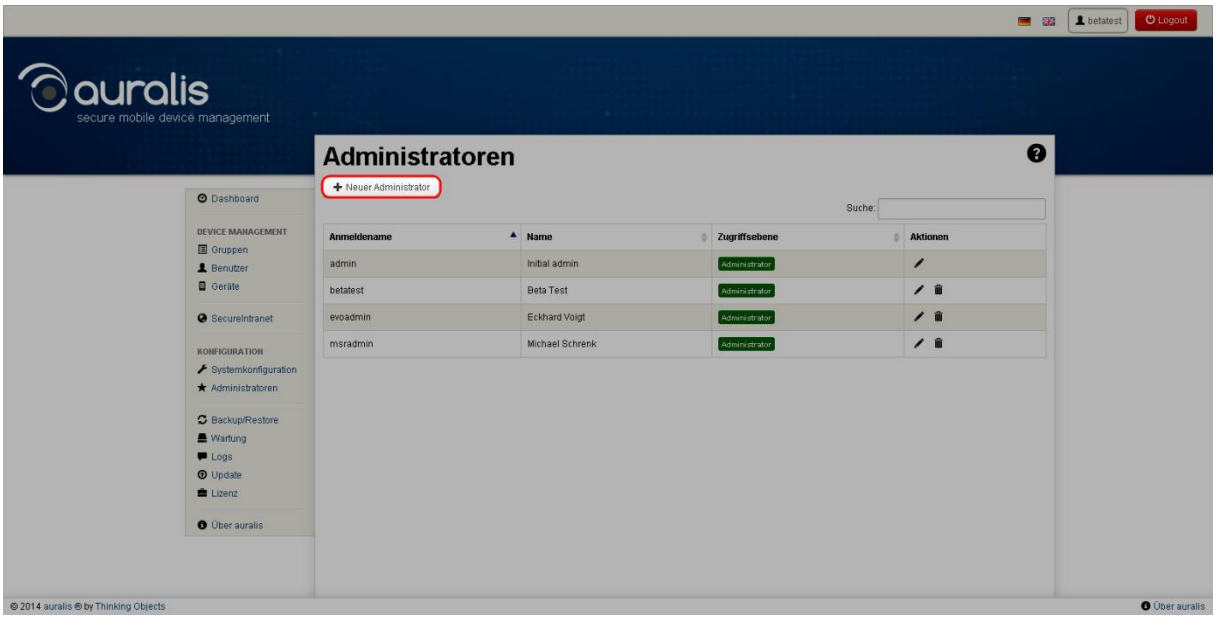
7 Administratoren

Im Menü „Administratoren“ werden die auralis-Administratoren verwaltet. Mit einem Klick auf den Menüeintrag „Administratoren“ gelangen Sie zu einer Übersicht über alle angelegten Administrator-Zugänge. Sie können in der Spalte „Aktionen“ einzelne Administratoren bearbeiten oder löschen.

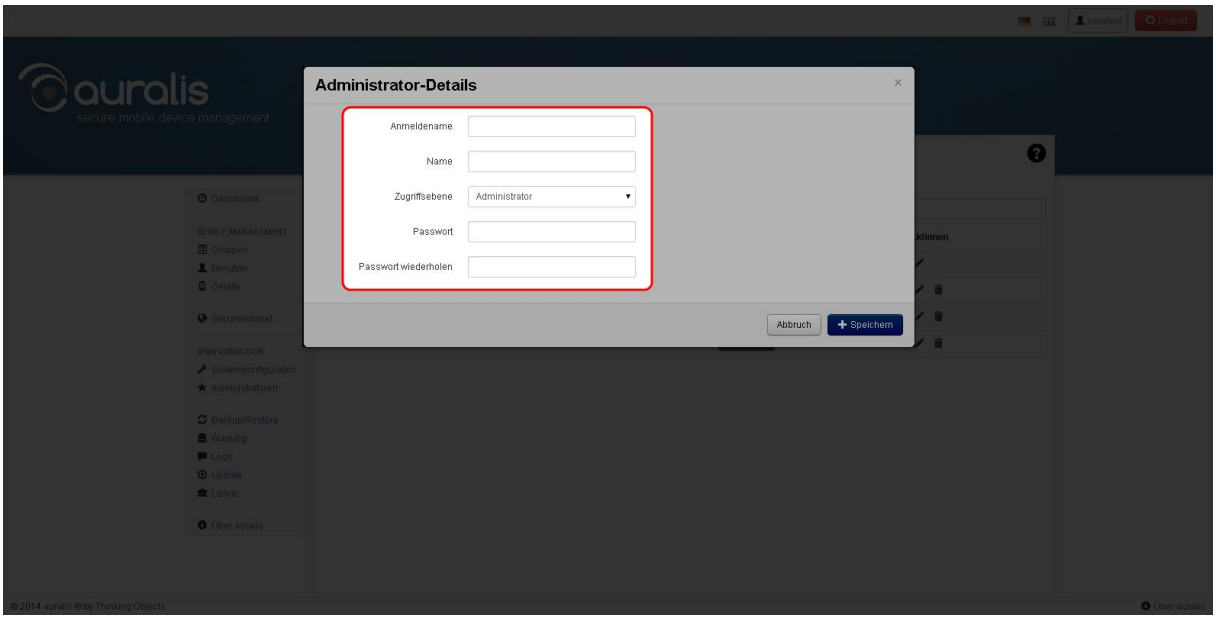


Neuer Administrator

Um einen neuen Administrator anzulegen, klicken Sie auf die Schaltfläche „Administrator anlegen“.



Geben Sie in die erscheinende Eingabemaske die erforderlichen Daten ein.



Anmeldename: Geben Sie hier den Namen ein, mit dem sic der Administrator auf der auralis Weboberfläche anmelden soll.

Name: Geben Sie hier den vollständigen Namen des Administrators ein.

Zugriffsebene: Geben Sie an, welche Rechte der Administrator erhalten soll. Sie können zwischen „Administrator“ und „WebDAV Logs“ unterscheiden.

> *Administrator:* Der Benutzer erhält vollen Zugriff auf alle Einstellungen.
>
> *Support:* Der Benutzer erhält einen eingeschränkten Zugriff. Am besten geeignet für den 1st oder 2nd level Support
>
> *WebDAV Logs:* Der Benutzer erhält nur Zugriff auf die Log-Dateien des Systems mittels WebDAV.

Passwort: Geben Sie hier ein Passwort für den Administrator ein.

Passwort wiederholen: Bestätigen Sie das eingegebene Passwort.

Klicken Sie auf „Speichern“, um den Administrator anzulegen oder auf „Abbruch“, um die eingegebenen Daten zu verwerfen.

Der Administrator „admin“ mit dem Namen „Initial Admin“ ist standartmäßig vorhanden und kann nicht gelöscht werden. Dieser Administrator-Account stellt sicher, dass mindestens immer ein Administrator im System vorhanden ist.

8 Backup / Restore

Sicherung der Konfiguration

Mit „Sicherung der Konfiguration“ haben Sie die Möglichkeit ein manuelles Backup des auralis-Systems zu erstellen. Sie erreichen die Funktion über das Hauptmenü. Zum Erstellen eines Backups müssen Sie ein ausreichend starkes Passwort angeben. Die Anforderungen an die Komplexität des Passworts werden Ihnen in der Beschreibung oberhalb des Passwortfelds angezeigt. Geben Sie zur Kontrolle das Passwort in das Feld „Passwort wiederholen“ ein, um Tippfehler im Passwort zu vermeiden. Klicken Sie dann auf die grüne Schaltfläche „Backup“, um die Sicherung von auralis zu starten. auralis wird Ihnen das fertige Backup als ZIP-Datei zum Download bereitstellen.

Wiederherstellen

Hinweis

Das Backup muss mit der gleichen Minor Version von auralis erstellt worden sein.

Um ein früheres Backup wiederherzustellen, wählen Sie im Feld „Konfigurationsdatei“ die Sicherungsdatei aus und geben Sie im Feld „Passwort“ das dazugehörige Passwort ein, das Sie beim Erstellen der Sicherung angegeben haben.

Vorsicht

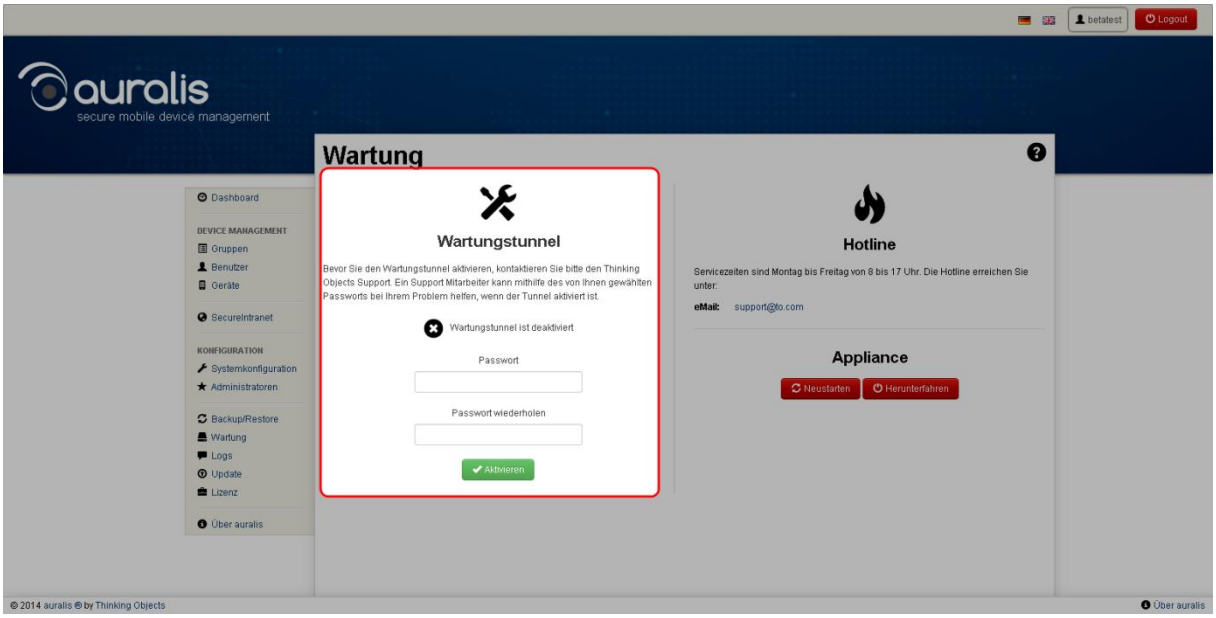
Alle Änderungen, die Sie seit dem Backup vorgenommen haben, gehen bei einer Wiederherstellung verloren.

Klicken Sie jetzt auf die rote Schaltfläche „Wiederherstellen“. Das ausgewählte Backup wird jetzt in auralis eingespielt.

9 Wartung

Wartungstunnel

Mit dem Wartungstunnel können Sie einem Support-Mitarbeiter von Thinking Objects den Zugang auf Ihr auralis-System gewähren. Bei der Aktivierung werden auf Port 443, also verschlüsselt, die IP Adressen unserer Hotline freigeben. Während dieser Zeit können wir Ihr System analysieren und evtl. Fehler beheben. Sobald Sie den Wartungstunnel deaktivieren ist auch kein Zugriff mehr vom Support möglich.

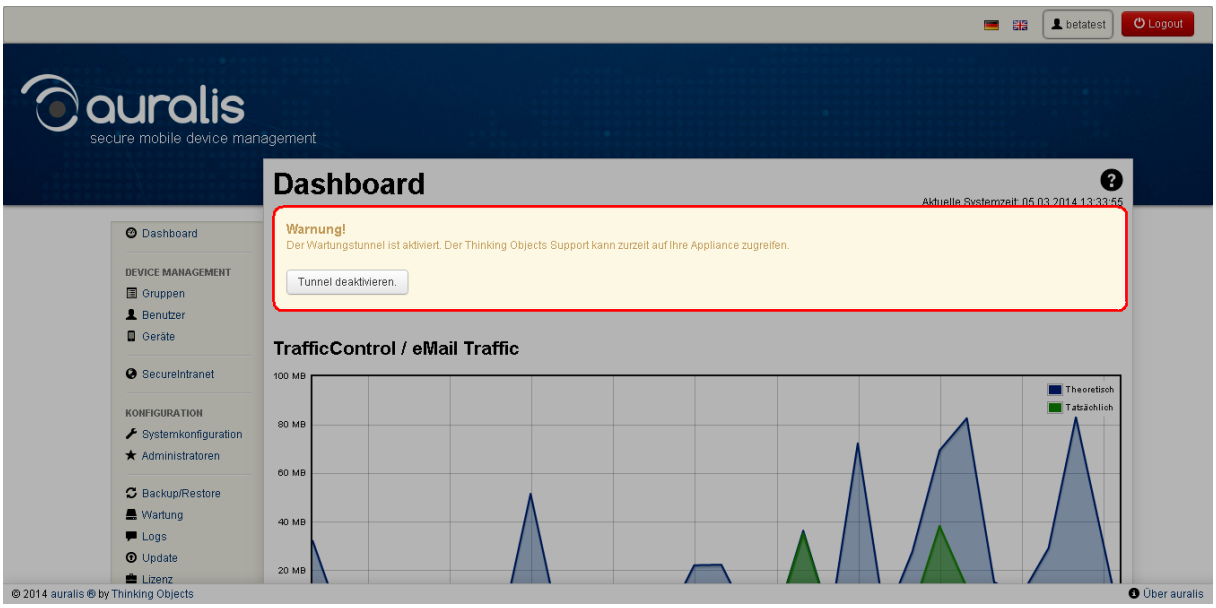


Setzen Sie sich vor dem Aktivieren des Wartungstunnels mit einem Mitarbeiter von Thinking Objects in Verbindung. Aktivieren Sie dann den Wartungstunnel mit einem ausreichend starken Passwort und teilen Sie dem Support-Mitarbeiter auf Anfrage das Passwort für den Wartungstunnel mit.

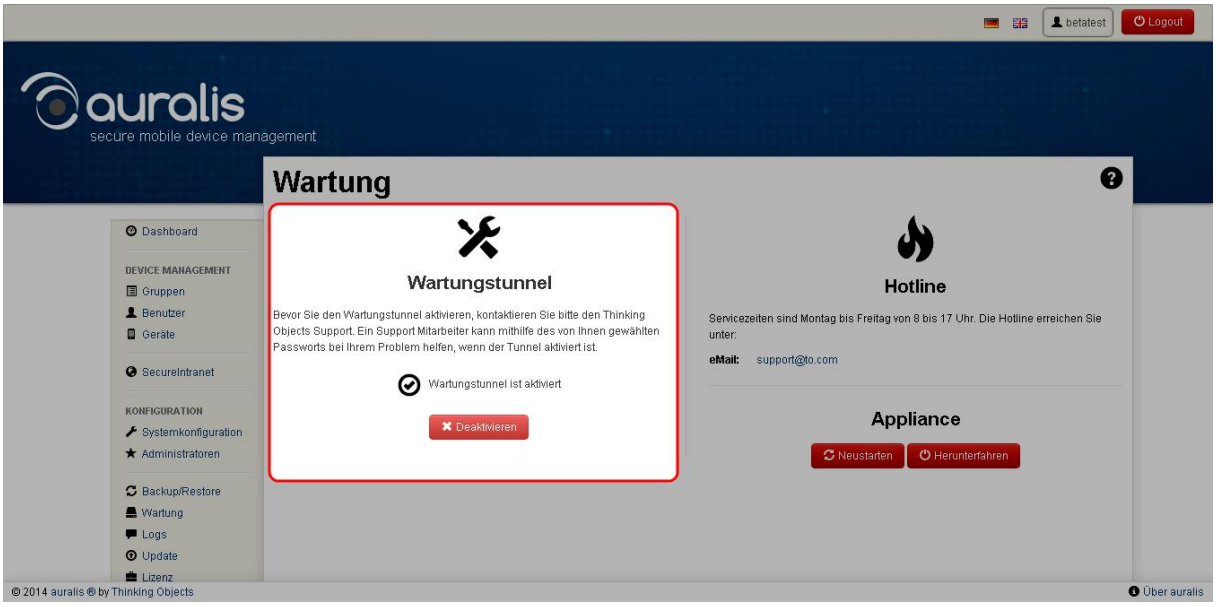
Hinweis

Der Mitarbeiter kann erst auf Ihre Appliance zugreifen, wenn er das Passwort kennt. Ein Zugriff ist ausschließlich aus dem Netz vom Thinking Objects Support möglich.

Solange der Wartungstunnel aktiviert ist, zeigt auralis auf dem Dashboard eine Warnung an.



Sie können den Wartungstunnel jederzeit über den dort angezeigten Button oder im Menü „Wartung“ deaktivieren.

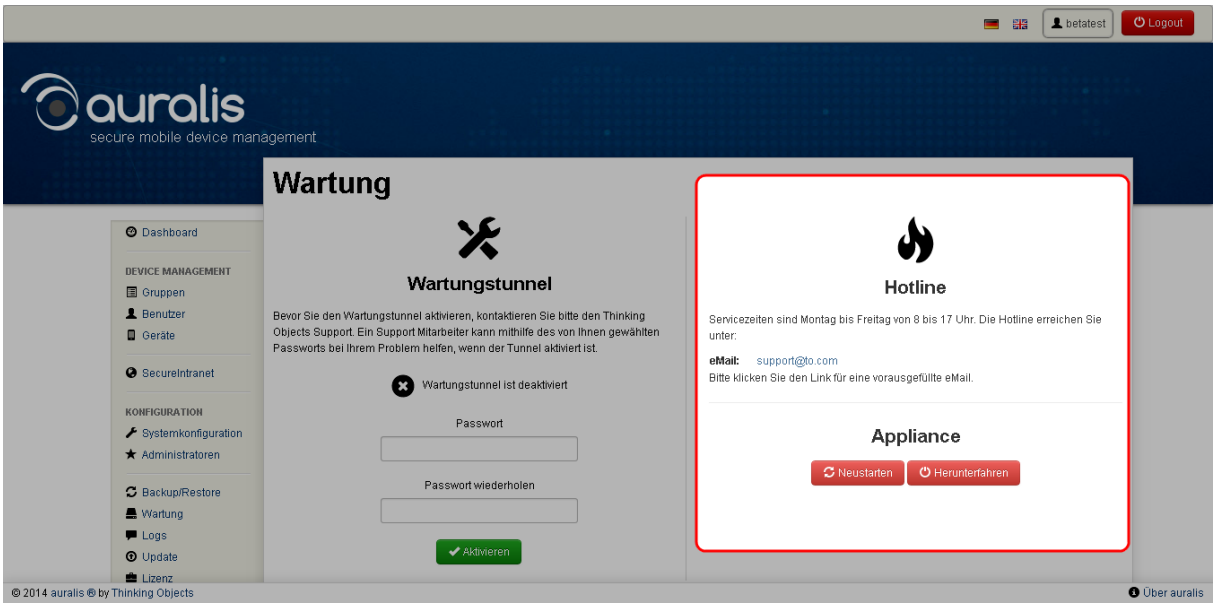


Hotline

Hier finden Sie die Service-Zeiten der Thinking Objects Hotline. Zudem erreichen Sie über die eMail-Adresse die Mitarbeiter von Thinking Objects. Wenn Sie auf die E-Mail-Adresse klicken, öffnet sich eine vorausgefüllte E-Mail.

Appliance

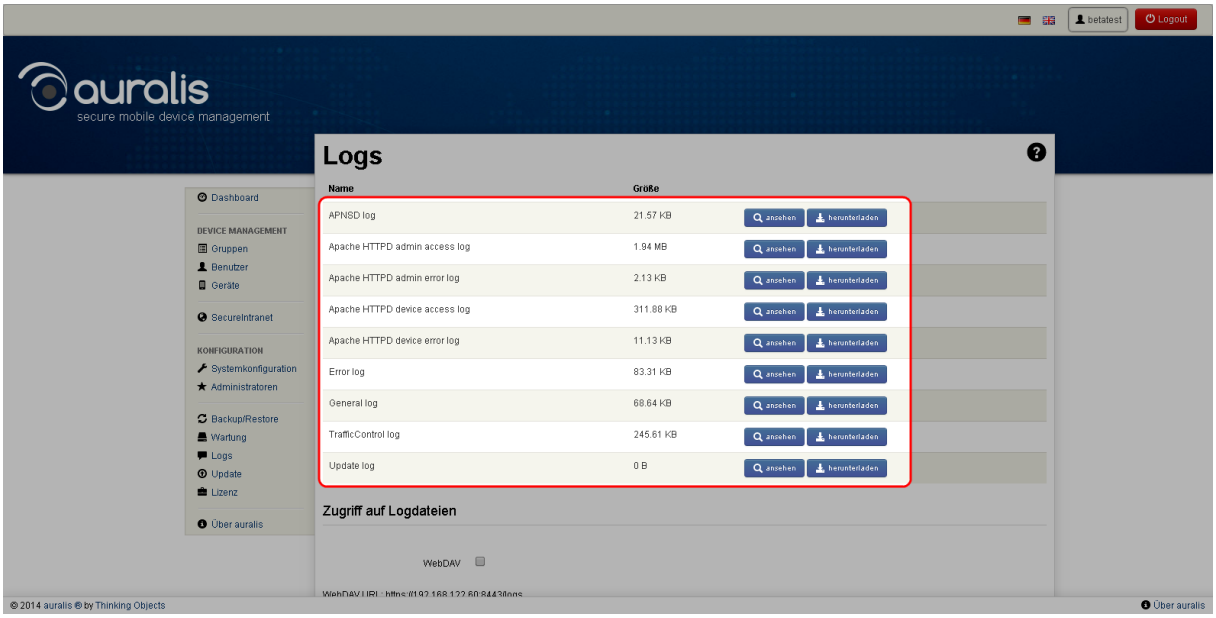
Mit den Optionen „Neustarten“ und „Herunterfahren“ können Sie an dieser Stelle Ihr gesamtes auralis-System neu booten oder ausschalten.



10 Logs

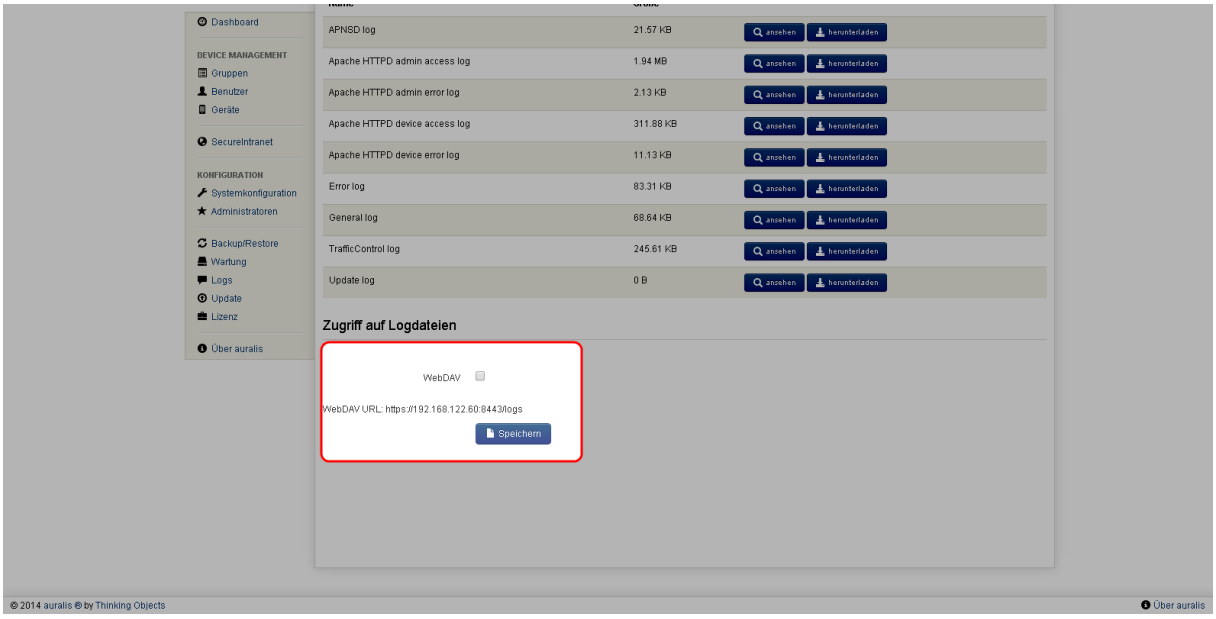
Um eine Logdatei anzusehen, klicken Sie auf „ansehen“. In einem neuen Browser-Tab können Sie den Log in Echtzeit mitverfolgen. Aktivieren Sie hierfür die Option „automatisch aktualisieren“ in der rechten oberen Ecke. Sie können die Logdatei zudem nach bestimmten Ereignissen filtern. Geben Sie hierfür einen Filter-Begriff in das Feld „Filter“ ein. Die gefundenen Zeilen werden angezeigt, die Treffer farblich hervorgehoben.

Klicken Sie auf „herunterladen“, um eine Logdatei mit dem aktuellen Stand abzuspeichern.



Zugriff auf Logdateien per WebDAV

Schalten Sie den Zugriff auf Logdateien frei, indem Sie die Option „WebDAV“ aktivieren. Administratoren können die Logdateien dann per WebDAV über den angezeigten Pfad erreichen. Klicken Sie anschließend auf „Speichern“, um die Einstellung anzuwenden.

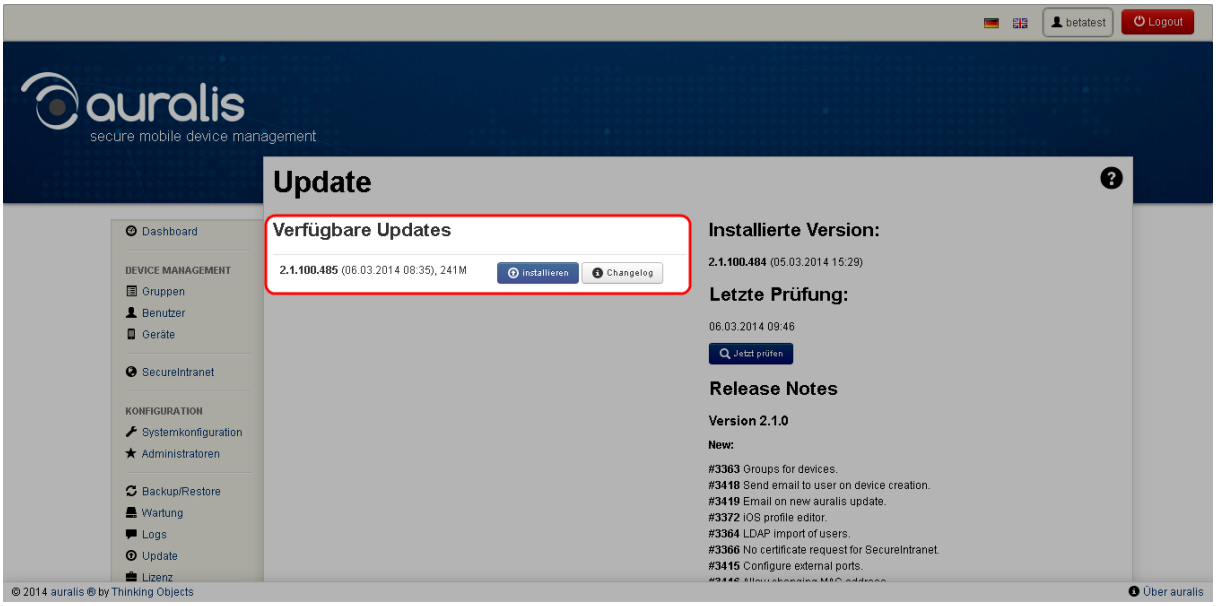


11 Update

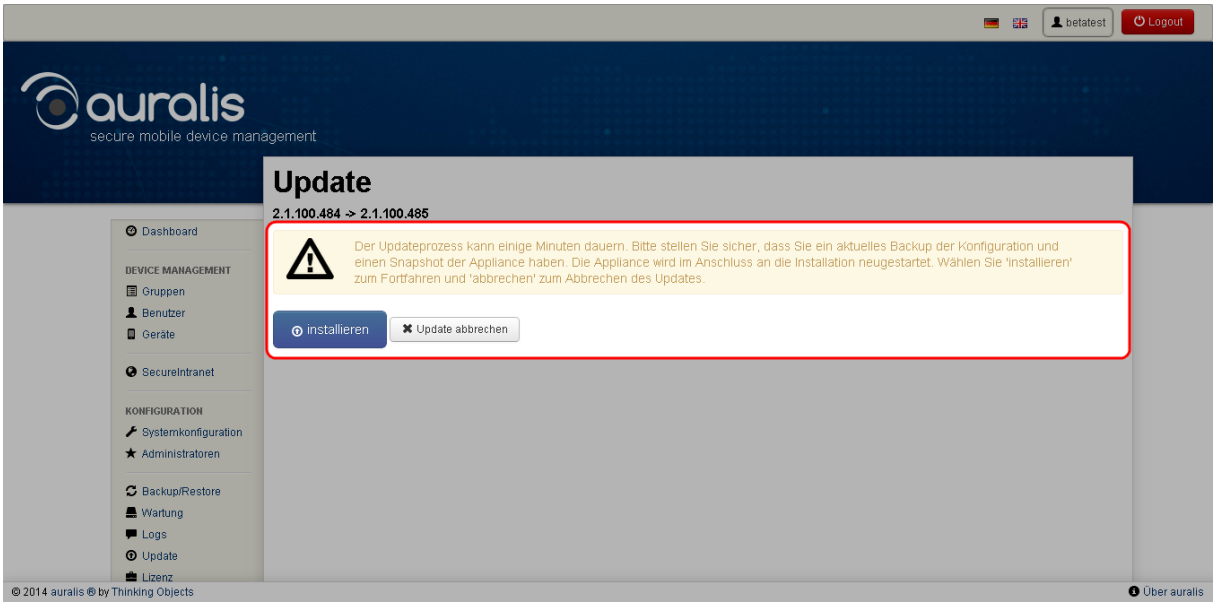
Verfügbare Updates

In den Einstellungen zu Updates werden Ihnen Informationen über die aktuelle auralis-Version und verfügbare Updates angezeigt.

Steht eine neue Version von auralis zur Installation bereit, wird Ihnen diese auf der linken Seite angezeigt. Sie können das Update installieren oder das Changelog ansehen.

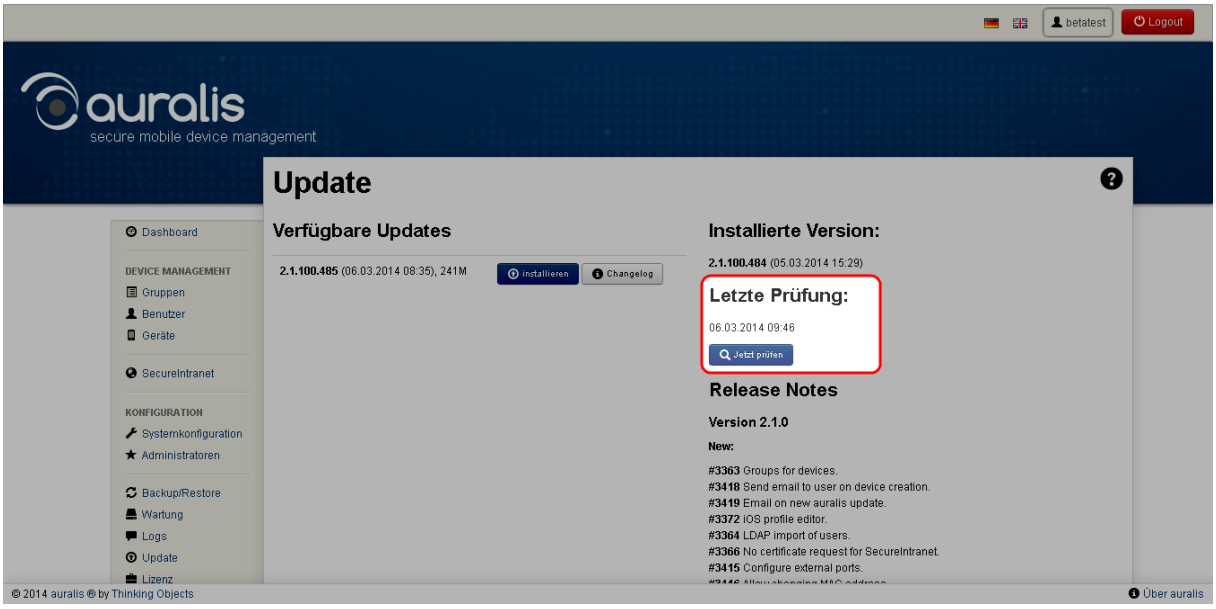


Wenn Sie das Update installieren möchten, klicken Sie auf die Schaltfläche „Installieren“. Beachten Sie bitte den daraufhin folgenden Sicherheitshinweis.



Klicken Sie dann auf „Installieren“, um das Update von auralis zu starten.

Die aktuell installierte Version von auralis wird Ihnen auf der rechten Seite angezeigt. Darunter informiert Sie auralis über die letzte automatische Suche nach Updates. Sie können die Suche manuell anstoßen, klicken Sie dafür auf die Schaltfläche „Jetzt prüfen“.

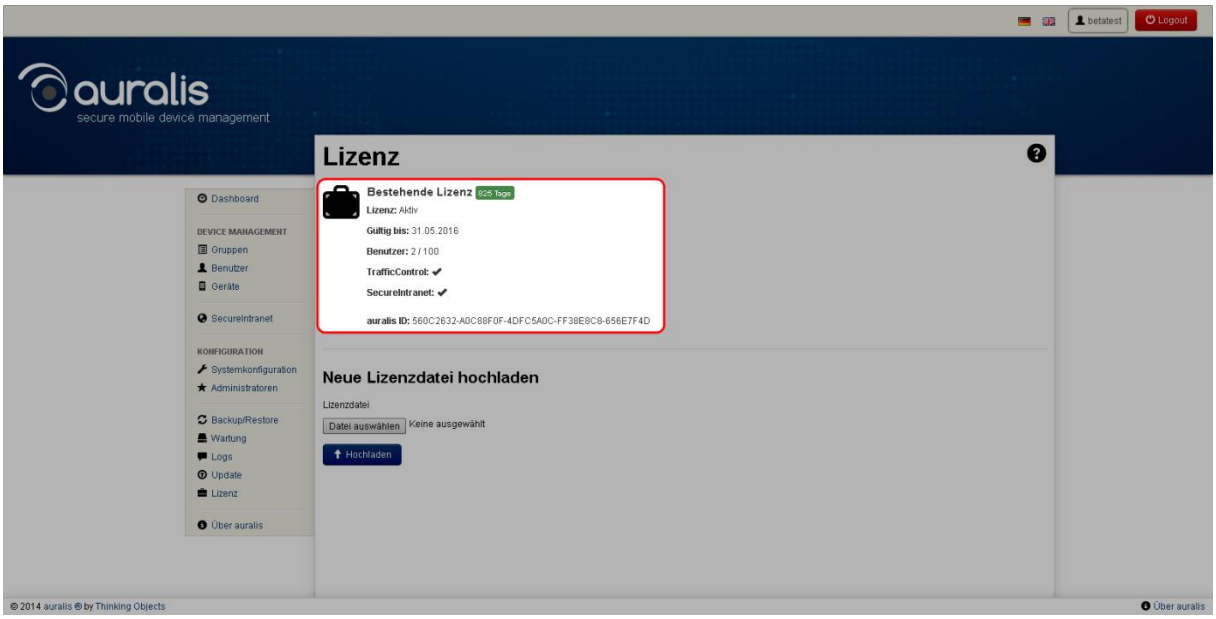


In den Release Notes werden die letzten Änderungen und neuen Features in den jeweiligen Versionen angezeigt.

Die in den eMail-Einstellungen festgelegten Admin-Adressen erhalten eine eMail, sobald eine neue Version verfügbar ist. Die Prüfung auf Updates findet täglich statt.

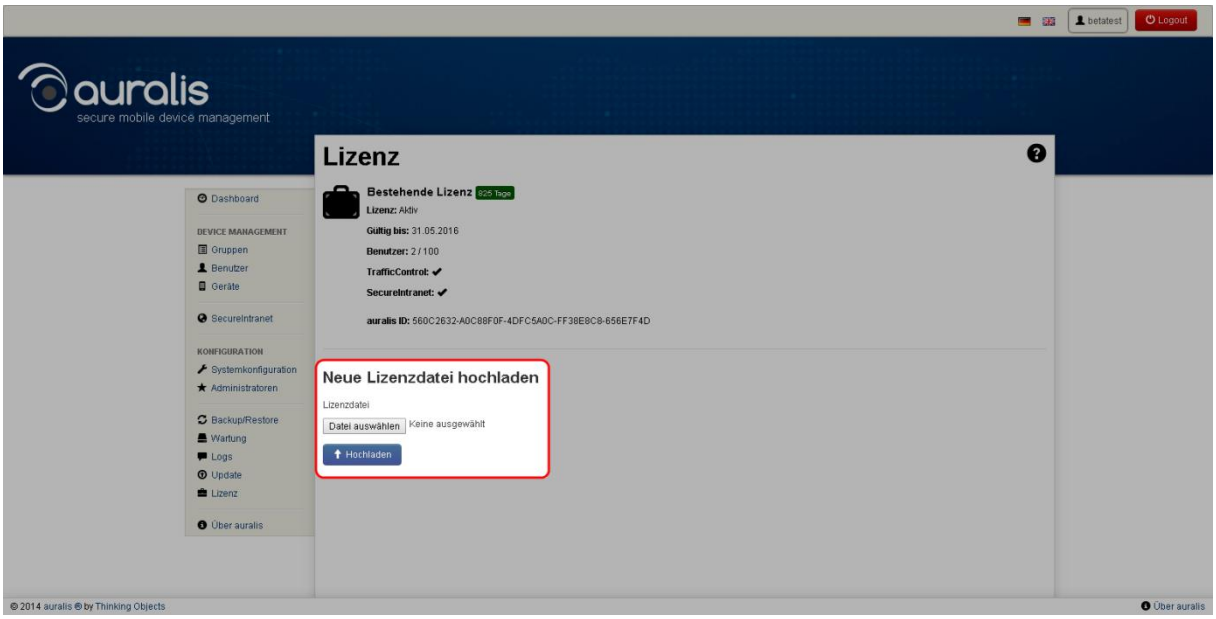
12 Lizenz

Behalten Sie hier den Überblick über Ihre auralis-Lizenz. Alle relevanten Daten zu Ihrer Lizenz werden hier angezeigt.



Neue Lizenzdatei hochladen

Möchten Sie Ihre Lizenz verlängern und eine neue Lizenzdatei hochladen, klicken Sie auf „Durchsuchen“ und wählen Sie die Lizenzdatei aus, die Sie von Thinking Objects erhalten haben. Klicken Sie dann auf „Hochladen“, um die neue Lizenz zu aktivieren.



13 Support

Sollten Sie weitere Fragen haben oder Hilfestellung bei der Integration benötigen, wenden Sie sich an unseren Support.

Dieser ist Montag bis Freitag von 09:00 – 17:00 Uhr per E-Mail unter support@to.com für Sie erreichbar.

14 Über uns

Thinking Objects GmbH

Lilienthalstraße 2/1

70825 Korntal-Münchingen

Tel. +49 711 88770400

Fax +49 711 88770449

E-Mail: info@auralis.de

Vertretungsberechtigte Geschäftsführer:

Markus Klingspor, Rudolf Zimmermann, Michael Föck

Registergericht: Amtsgericht Stuttgart

Registernummer: HRB 19769

Umsatzsteuer-IdNr.: DE193103278

Inhaltlich Verantwortlicher gemäß § 55 Absatz 2 MDStV: Markus Klingspor (Anschrift wie oben)