auralis

secure mobile device management

Manual

auralis 2.5

Note – auralis in Univention App Center

auralis ist now available in Univention App Center.

Some of the configurations listed here are not available in the Univention version, since they are covered by the server system (IP, updates, etc).

The port 443 for external communication is pre-configured in the Univention version with the Port 7443. Keep this in mind when configuring the firewall!

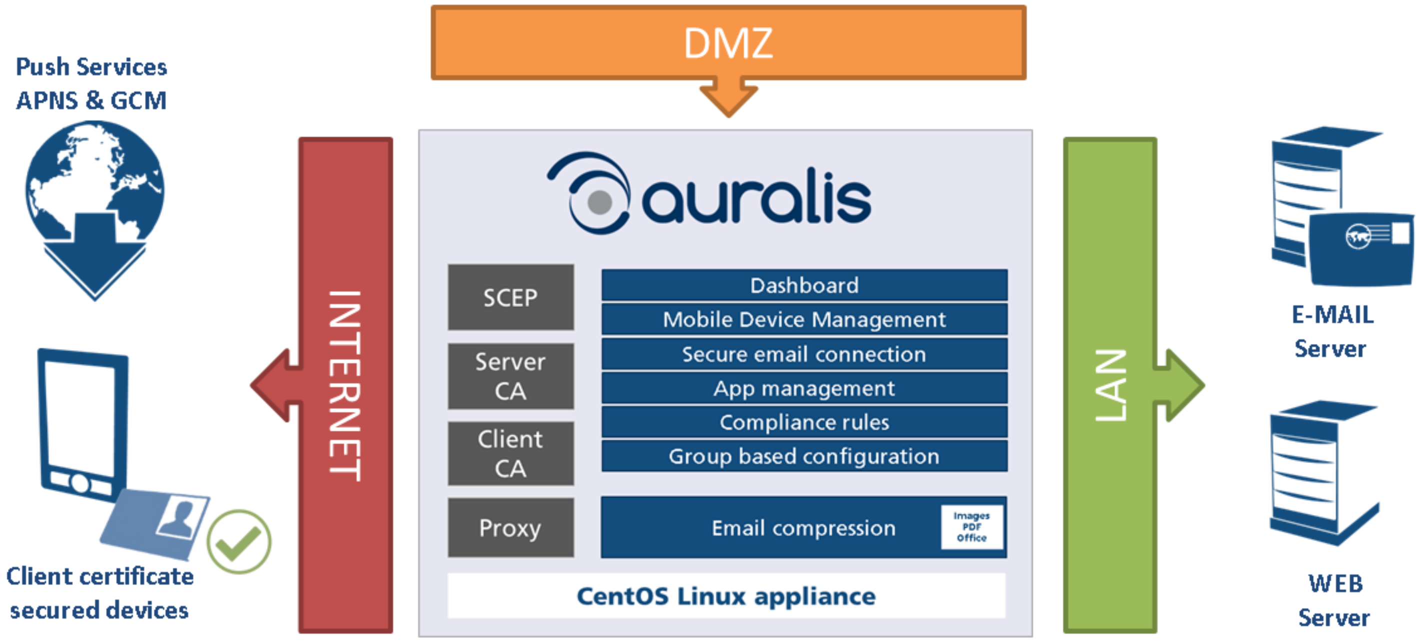
1.9.2015

1 auralis – secure mobile device management

auralis is a secure mobile device management solution. Through the use of client certificates for each Smartphone, it is perfect to protect your IT infrastructure such as Microsoft Exchange (or any other AcitveSync based solution as Zarafa or Kerio) and Web servers against man in-the middle attacks. auralis is a firewall for your email infrastructure.

1.1 Structure & functions

auralis is delivered as ISO installation media and is optimally designed for use on a virtual or physical machine in your DMZ. The basis of auralis is a hardened Linux CentOS operating system which will maintained with each auralis update from us. Through the implementation of SCEP, a server and client CA, as well as a reverse proxy, auralis is an efficiently ready to run mobile device management solution. You don't need to integrate these services by yourself.



1.2 System requirements

Virtual or physical machine:

CPU: Minimum 1 CPU with one core.

For the use of TrafficControl data compression for more than 50 users, we recommend using two CPUs or at least a dual core CPU.

RAM: Minimum 4 GB RAM

For the use of TrafficControl data compression for more than 50 users, we recommend at least 8GB of RAM.

HDD: 1 Partition with 20 GB disk space

The main use of the disk space is for logfiles. The logs are rotated and compressed on a daily base and deleted after six months. For really large numbers of devices, more disk space may be needed.

NIC: One network card

Auralis is designed for use in a DMZ which only requires one network card. auralis does not operate dual homed.

DNS: public DNS name: e.g. auralis.example.com

2 Installation

Note

To avoid problems during installation, we highly recommend to configure the DNS entry and the firewall rules prior to installation.

2.1 Firewall Rules

The following access rules are necessary for auralis:

Source	Destination	Ports
any	[auralis]	80/TCP; 443/TCP; 8443/TCP
[auralis]	[DNS-Server (LAN)]	53/UDP
[auralis]	[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 some rare cases, Exchange does not support SSL for ActiveSync. In these cases you need to use port 80/TCP instead.

Hinweis

For access to the Apple Appstore, Windows Store, Google Playstore, Google GCM Service and the auralis update server, access is required to the following web sites. If you don't want to configure websites directly and avoid ANY port 443 rule, alternatively configure a proxy server in the system configuration/network tab.

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/

2.2 DNS – Fully Qualified Domain Name

Please define a DNS name, pointing to the IP address of your auralis installation. Example: auralis.example.com

2.3 Installation environment

You can install auralis alternatively as a virtual or physical machine.

2.3.1 Virtual machine

Create a new virtual machine and select CentOS6 64bit or Linux Kernel 2.6 with 64Bit for the operating system. For system requirements see above. Select the auralis ISO image for system boot and start the virtual machine.

2.3.2 Physical maschine

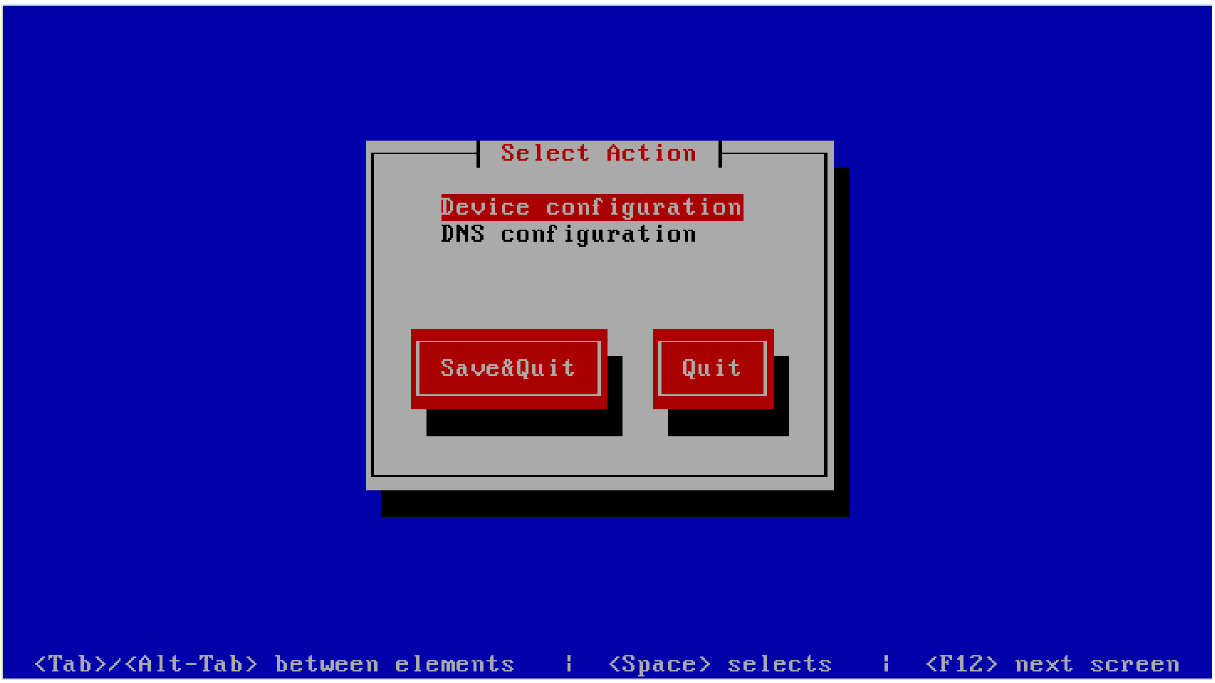
Burn the auralis ISO image to a CD and insert it into your server. Start the server from the CD.

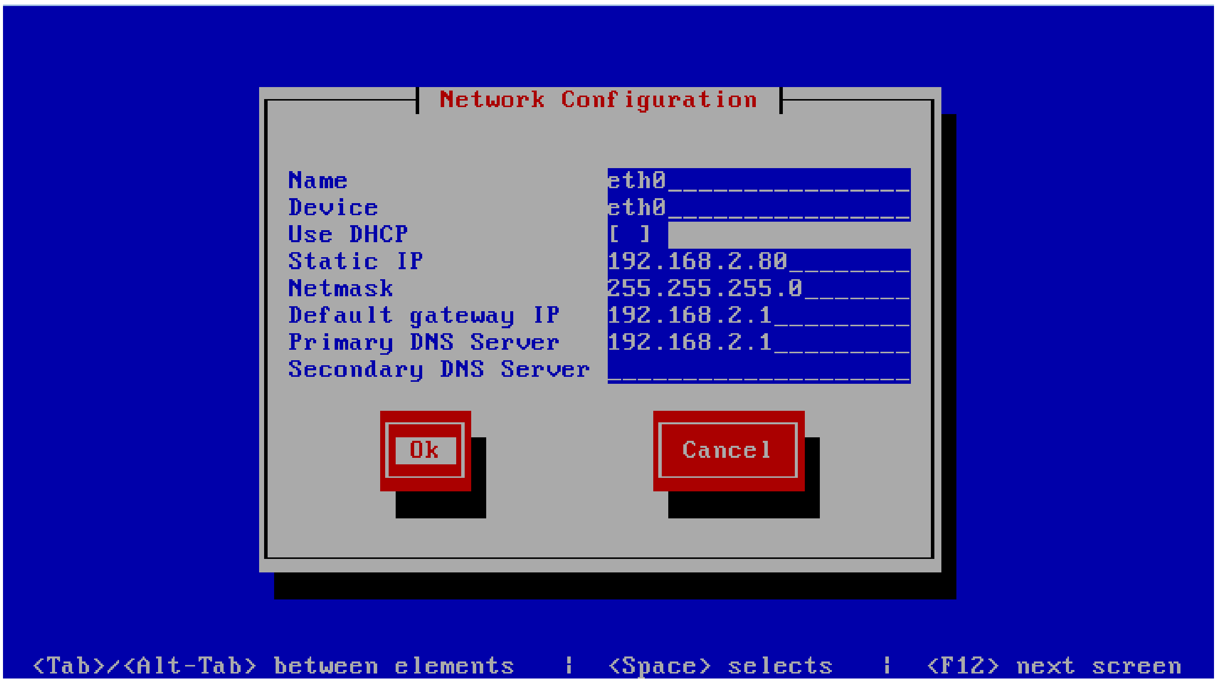
2.4 Initial setup

Please select „auralis installation” in the boot menu. Once the initial setup is completed, auralis will be started for initial configuration.

Choose „Device configuration“ with the cursor keys and press “Enter”.

Network

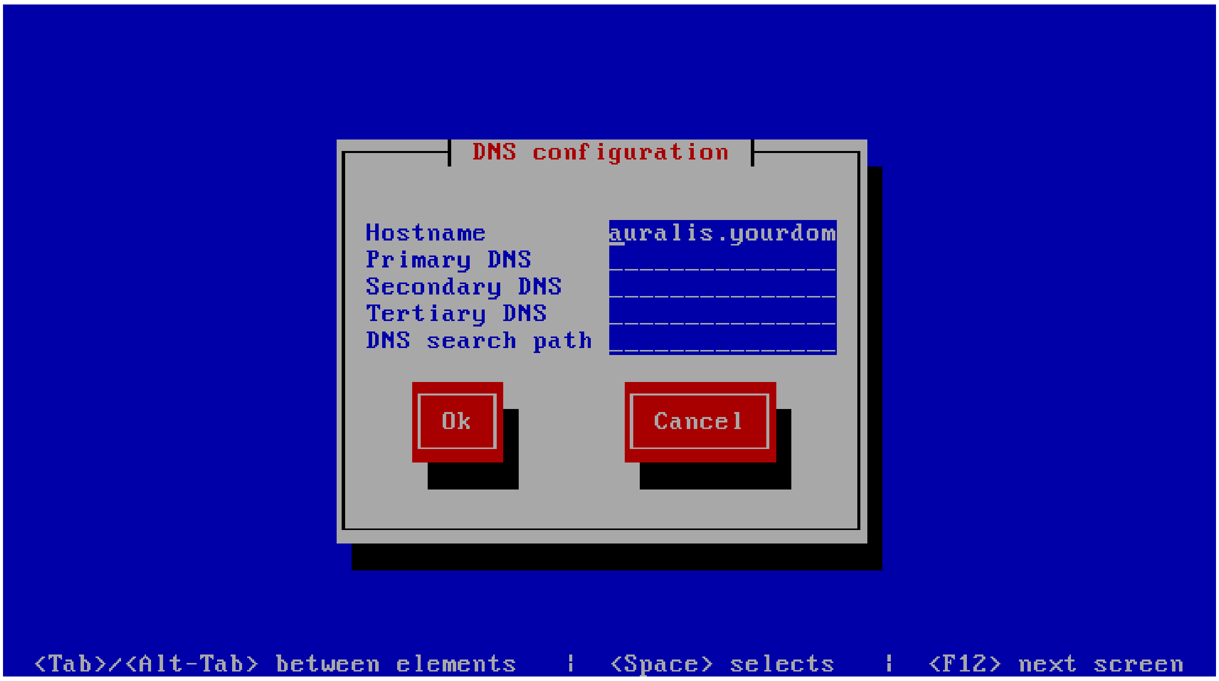

Select Action
Device configuration
DNS configuration
Save&Quit
Quit
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen


Network Configuration
Ok
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

```
Name                  eth0_________________
Device                eth0_________________
Use DHCP              [ ]
Static IP             192.168.2.80________
Netmask               255.255.255.0_______
Default gateway IP    192.168.2.1_________
Primary DNS Server    192.168.2.1_________
Secondary DNS Server  ____________________
```

Please configure the network interface eth0 according to your local network configuration.

DNS – Fully Qualified Domain Name

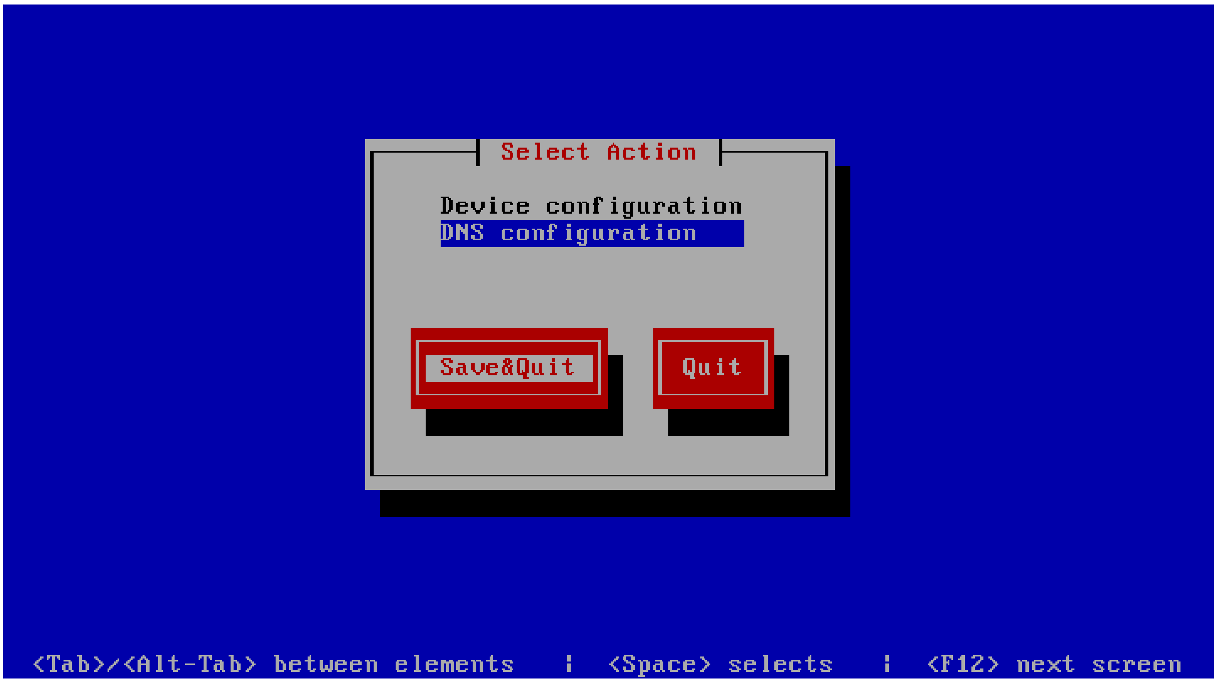


```
DNS configuration

Hostname          auralis.yourdom
Primary DNS       _______________
Secondary DNS     _______________
Tertiary DNS      _______________
DNS search path   _______________
```

Ok
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Set the hostname of your auralis system (Fully Qualified Domain Name, FQDN) and specify the IP addresses of your DNS servers. Select "OK" with the cursor keys and press "Enter".



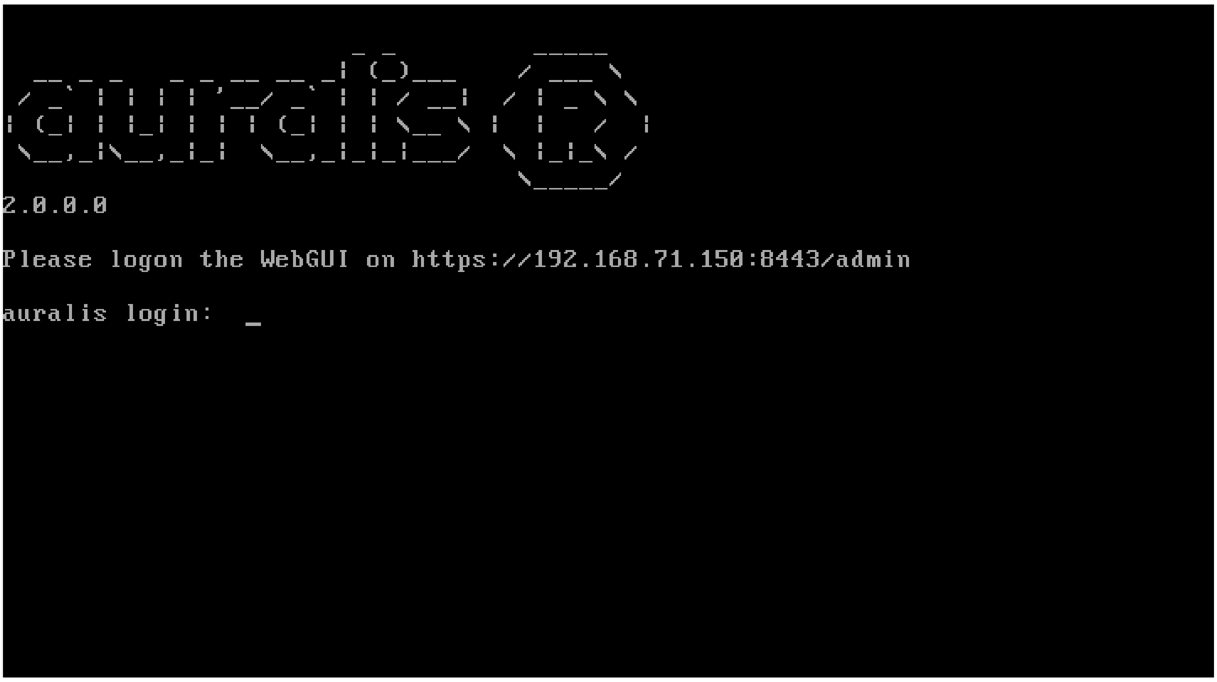
```
Select Action

Device configuration
DNS configuration
```

Save&Quit
Quit
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Select „Save & Quit“ and press "Enter".

auralis is installed



```
                        _ _          ______
  __ _ _   _ _ __ __ _| (_)___     / ____ \
 / _` | | | | '__/ _` | | / __|   / |  _ \ \
| (_| | |_| | | | (_| | | \__ \  |  | |_) | |
 \__,_|\__,_|_|  \__,_|_|_|___/  |  |  _ <  |
                                  \ |_| \_\ /
                                   \______/
2.0.0.0

Please logon the WebGUI on https://192.168.71.150:8443/admin

auralis login: _
```

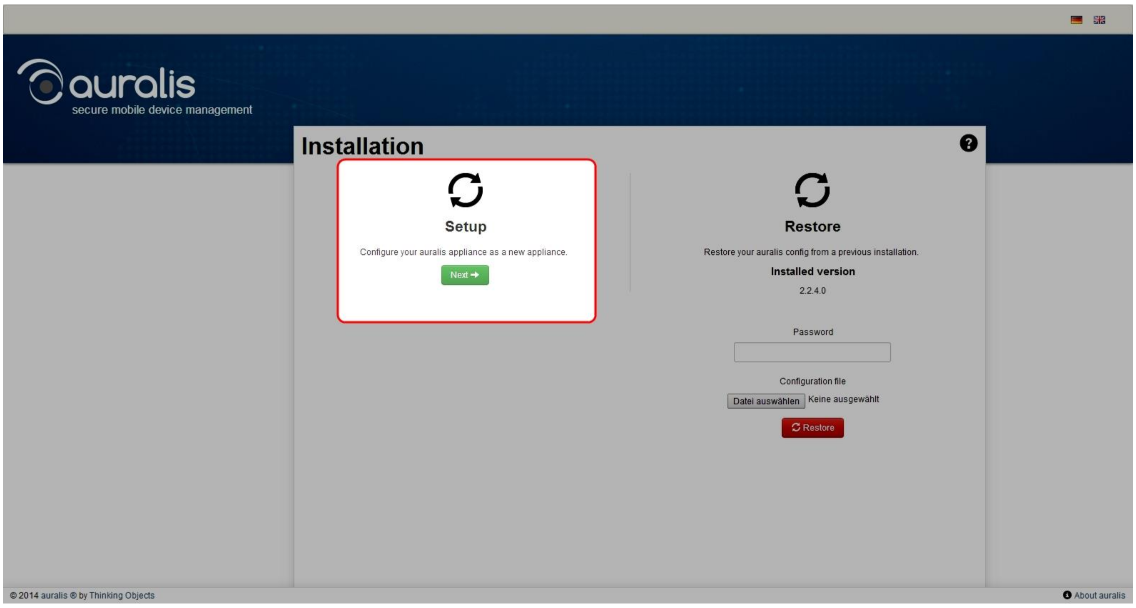
After startup, the URL to access the auralis configuration is displayed. Point your browser to the shown URL, e.g. https://*<IP-address>*:8443/admin.

Note

The console login is not needed, auralis is a software appliance, that can be managed completely with the web interface.

2.5 Initial configuration

In your browser, you will see the page shown below. Click on „Next“ to continue the auralis installation. You can also restore a backup from a previous installation at this point. Please note that the auralis version of the backup needs to match the installed version exactly.


auralis
secure mobile device management
Next
Datei auswählen
Restore
© 2014 auralis ® by Thinking Objects
About auralis

Installation

Setup

Configure your auralis appliance as a new appliance.

Restore

Restore your auralis config from a previous installation.

Installed version

2.2.4.0

Password

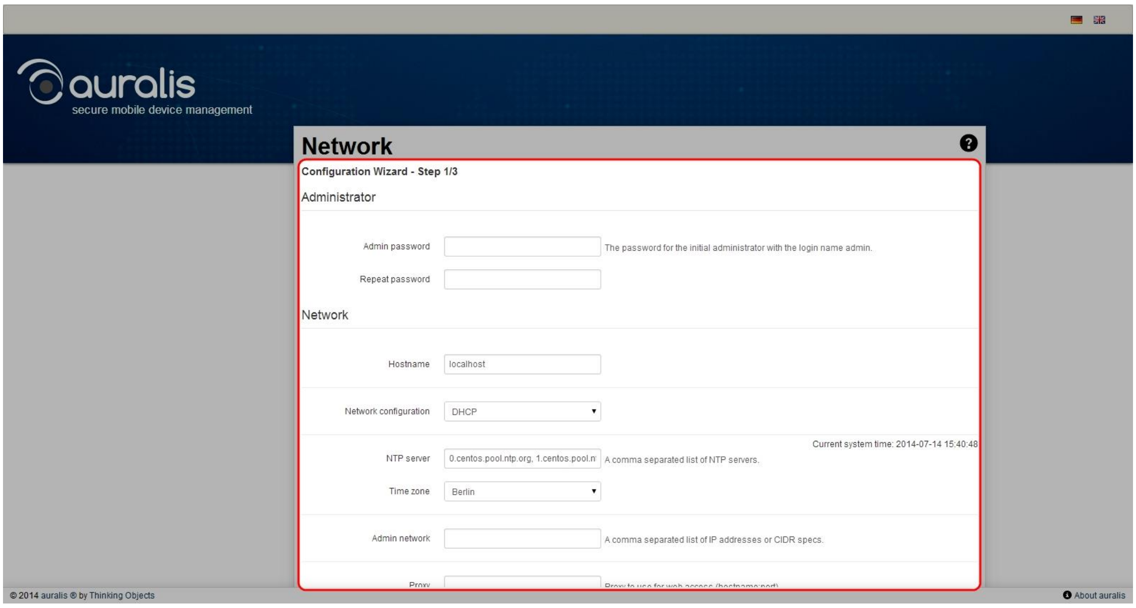
Configuration file

Keine ausgewählt

2.5.1 Configuration wizard – step 1 / 3

Please enter a password for the administrator, check the network settings and correct them if necessary. Then click “Save”.

You will now be asked to login with the user admin and the password set for the first time.


auralis
secure mobile device management
© 2014 auralis ® by Thinking Objects
About auralis

Network

Configuration Wizard - Step 1/3

Administrator

Admin password — The password for the initial administrator with the login name admin.

Repeat password

Network

Hostname: localhost

Network configuration: DHCP

Current system time: 2014-07-14 15:40:48

NTP server: 0.centos.pool.ntp.org, 1.centos.pool.n — A comma separated list of NTP servers.

Time zone: Berlin

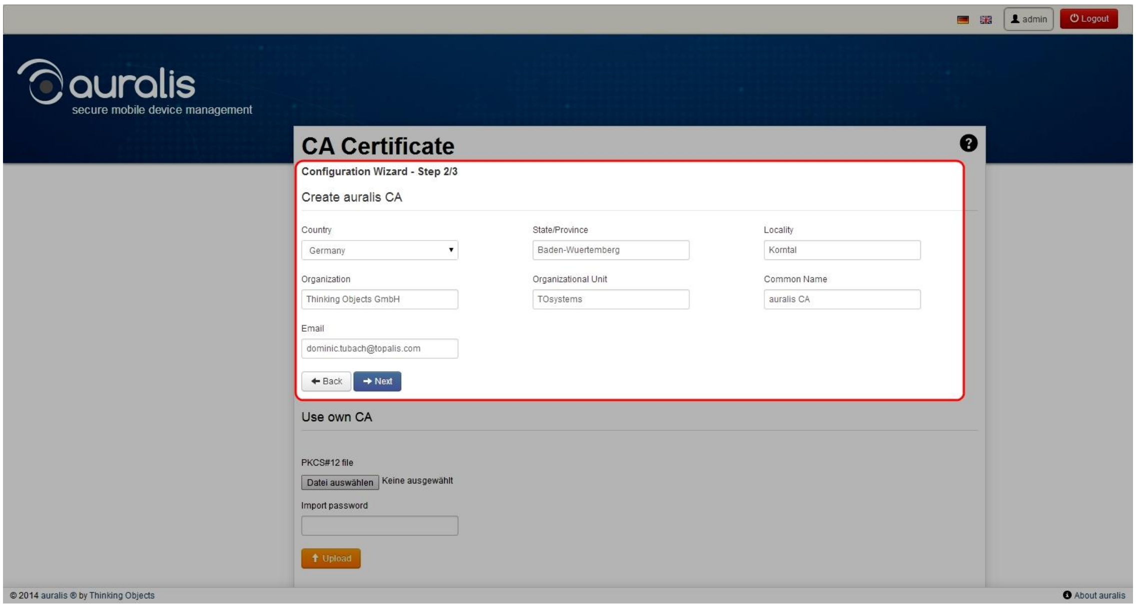
Admin network — A comma separated list of IP addresses or CIDR specs.

Proxy — Proxy to use for web access (hostname:port)

2.5.2 Configuration wizard – step 2 / 3

At this point the internal certificate authority will be created. All server and device certificates generated later will depend on this root CA. Every smartphone connected to auralis will get an individual device certificate signed by this CA.

Please enter all necessary data.


admin
Logout
auralis
secure mobile device management

CA Certificate

Configuration Wizard - Step 2/3

Create auralis CA

Country: Germany

State/Province: Baden-Wuertemberg

Locality: Korntal

Organization: Thinking Objects GmbH

Organizational Unit: TOsystems

Common Name: auralis CA

Email: dominic.tubach@topalis.com

Use own CA

PKCS#12 file

Datei auswählen Keine ausgewählt

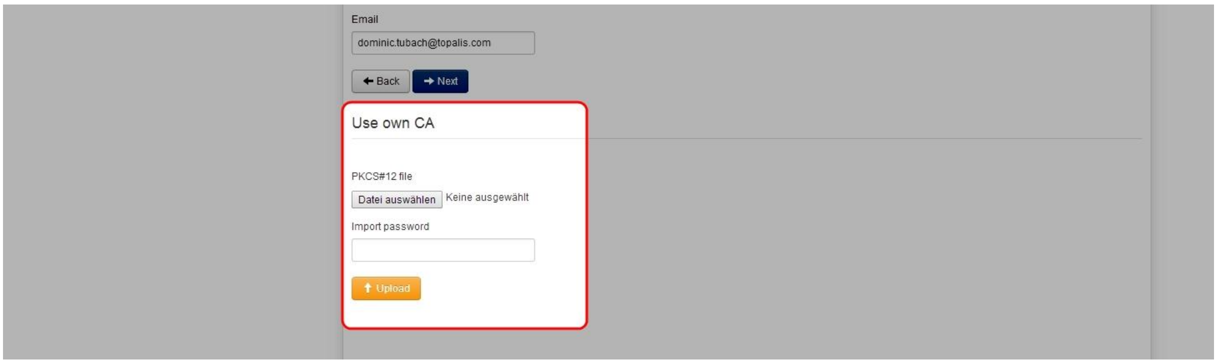
Import password

Upload
© 2014 auralis ® by Thinking Objects
About auralis

Caution

Don’t change the field „Common name“.

You can at this point also upload an existing CA. To do so select ”Upload FIle”, select the respective CA file, enter the import password and click “Upload”.



Email: dominic.tubach@topalis.com

Use own CA

PKCS#12 file

Datei auswählen Keine ausgewählt

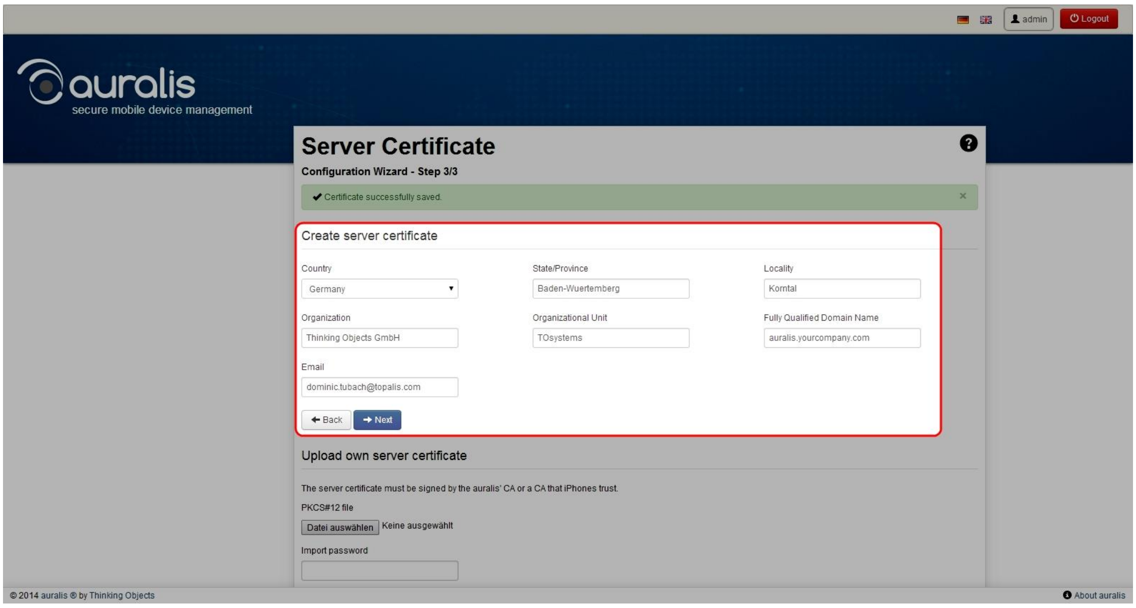
Import password

Then click „Continue“.

2.5.3 Configuration wizard – step 3 / 3

Please enter the necessary data for the generation of the server certificate. The server certificate will be used to encrypt the connection between the server and the devices.

Please make sure, that the name in the field „Fully Qualified Domain Name“ matches the DNS name of your auralis system e.g. *auralis.example.com.*



Server Certificate

Configuration Wizard - Step 3/3

✔ Certificate successfully saved.

Create server certificate

Country	State/Province	Locality
Germany ▾	Baden-Wuertemberg	Korntal
Organization	Organizational Unit	Fully Qualified Domain Name
Thinking Objects GmbH	TOsystems	auralis.yourcompany.com
Email		
dominic.tubach@topalis.com		

Upload own server certificate

The server certificate must be signed by the auralis' CA or a CA that iPhones trust.

PKCS#12 file

Datei auswählen Keine ausgewählt

Import password

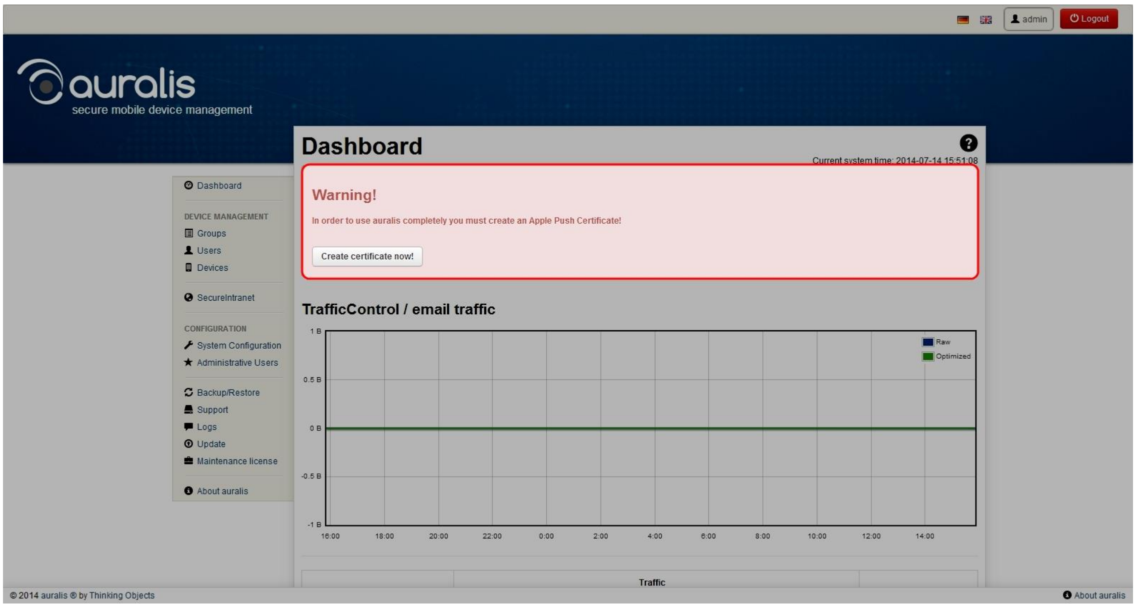
You can also use your own certificate here. Choose „Eigenes Zertifikat hochladen“ select your certificate file, enter the import password and click “Upload”.

Click “Continue” to finish the installation.

2.6 Create an Apple push certificate

After installation, auralis will notify you that no Apple push certificate has been created yet. The Apple push service is responsible for notifying devices of actions to be executed, so that e.g. the wipe of a device is performed as soon as possible. Only the request for the device to contact auralis, no user data will be sent to Apple.

Please click on “Create certificate now”.



Dashboard

Current system time: 2014-07-14 15:51:08

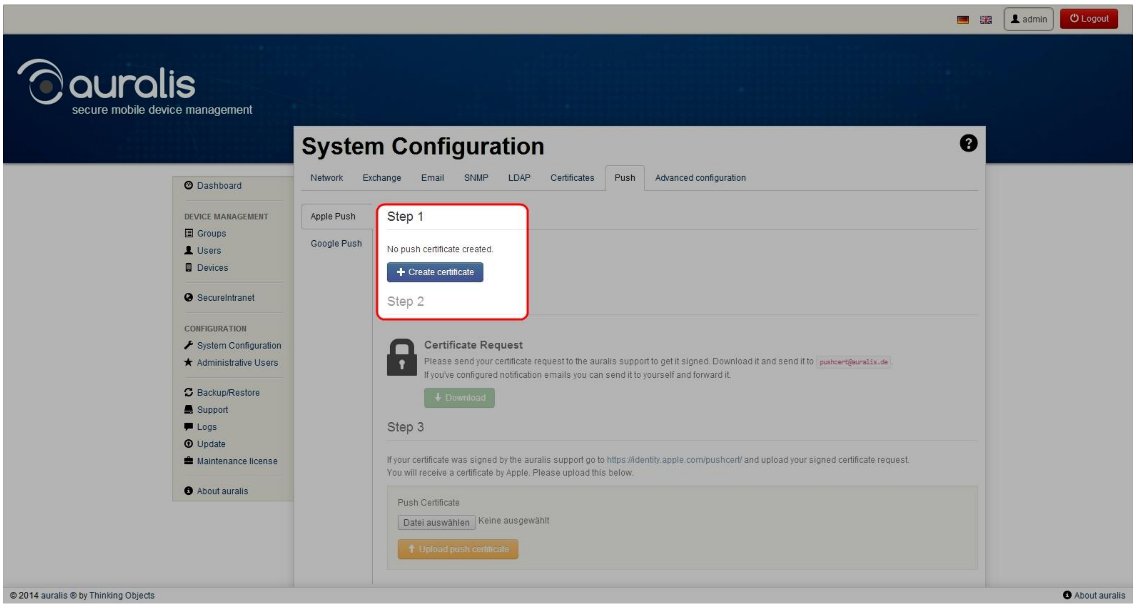
Warning!

In order to use auralis completely you must create an Apple Push Certificate!

Create certificate now!

TrafficControl / email traffic

To create an Apple push certificate, goto „System configuration“ and select the tab „Push“. Click on “Create certificate” in the section “Step 1 “.



System Configuration

Step 1

No push certificate created.

Create certificate

Step 2

Certificate Request

Please send your certificate request to the auralis support to get it signed. Download it and send it to pushcert@auralis.de.
If you've configured notification emails you can send it to yourself and forward it.

Download

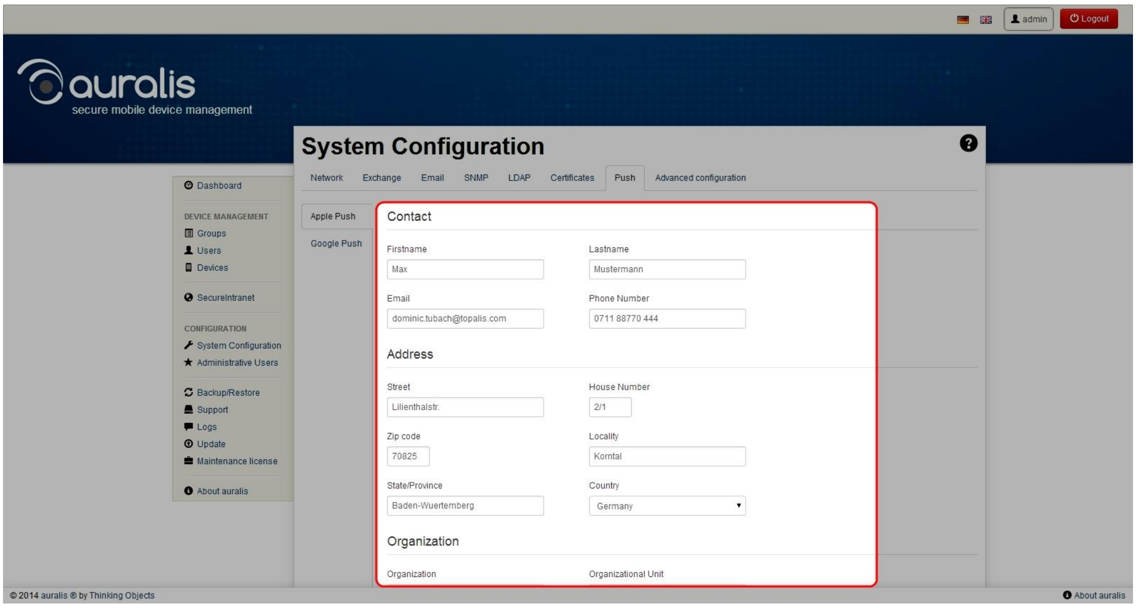
Step 3

If your certificate was signed by the auralis support go to https://identity.apple.com/pushcert/ and upload your signed certificate request.
You will receive a certificate by Apple. Please upload this below.

Push Certificate: Datei auswählen Keine ausgewählt

Upload push certificate

Enter your data in the fields „Contact“, „Address“ and „Organization“ and click on “Create certificate”.



System Configuration

Contact

Firstname: Max

Lastname: Mustermann

Email: dominic.tubach@topalis.com

Phone Number: 0711 88770 444

Address

Street: Lilienthalstr.

House Number: 2/1

Zip code: 70825

Locality: Korntal

State/Province: Baden-Wuertemberg

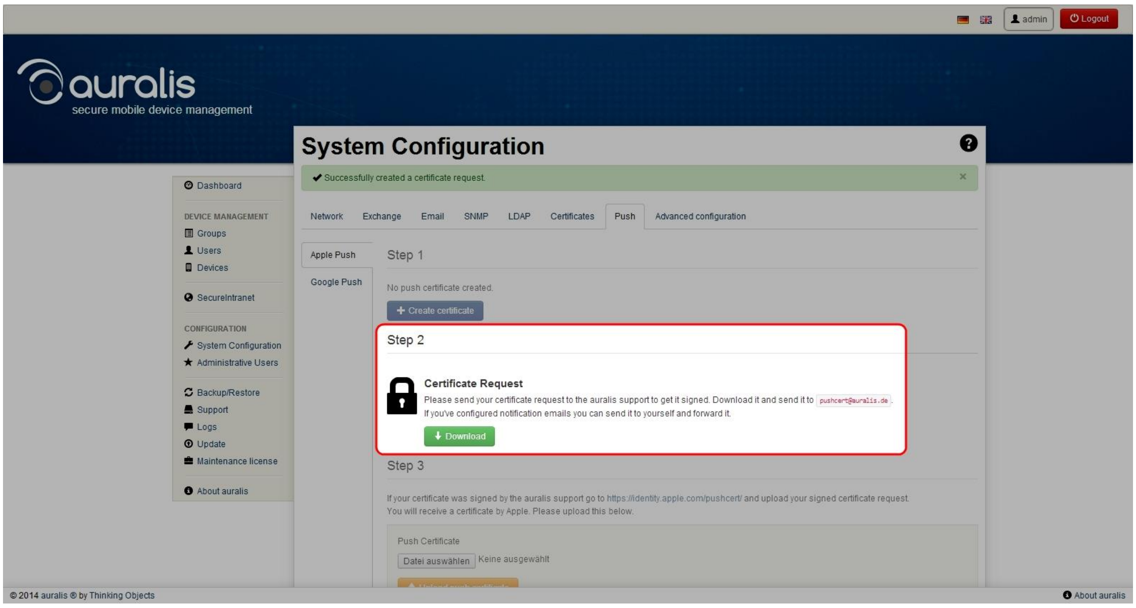
Country: Germany

Organization

Organization

Organizational Unit

In “Step 2” you can now download the certificate request. Please send this request to the auralis support (pushcert@auralis.de). We will sign your request as soon as possible and send you the signed request in response. This procedure is necessary, as Apple will only provide push certificates for requests signed by the MDM manufacturer.



System Configuration

✓ Successfully created a certificate request.

Step 1

No push certificate created.

Step 2

Certificate Request

Please send your certificate request to the auralis support to get it signed. Download it and send it to pushcert@auralis.de.
If you've configured notification emails you can send it to yourself and forward it.

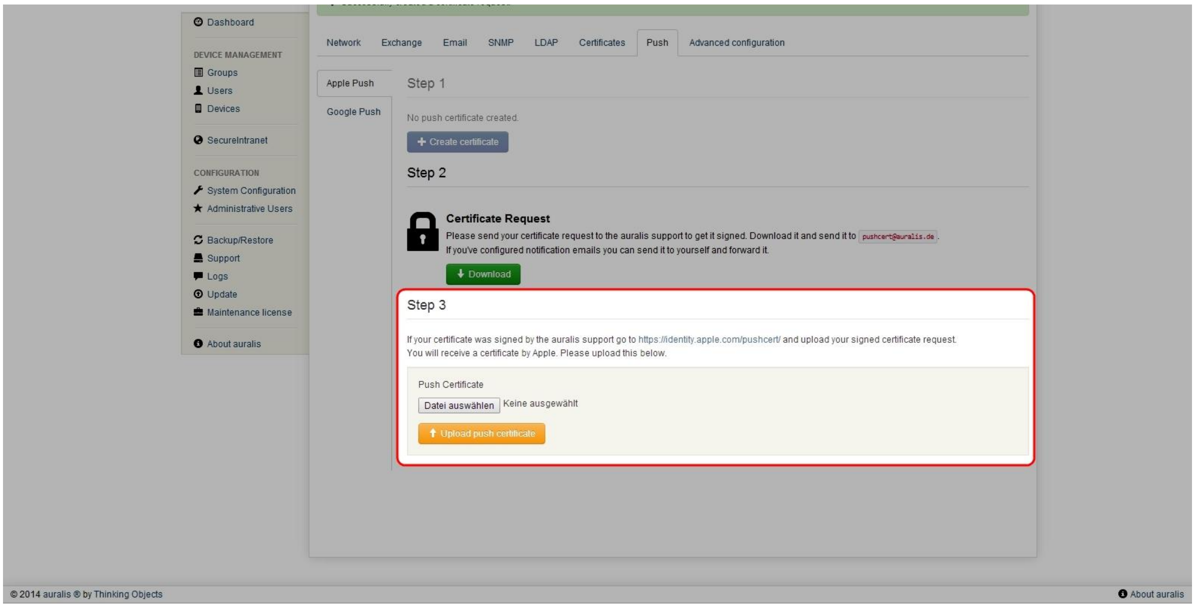
Step 3

If your certificate was signed by the auralis support go to https://identity.apple.com/pushcert/ and upload your signed certificate request.
You will receive a certificate by Apple. Please upload this below.

Push Certificate

Keine ausgewählt

As soon as your certificate was signed by the auralis support, goto https://identity.apple.com/pushcert/ and upload the signed certificate request. You will then be provided with your new push certificate by Apple.



Step 1

No push certificate created.

Step 2

Certificate Request

Please send your certificate request to the auralis support to get it signed. Download it and send it to pushcert@auralis.de.
If you've configured notification emails you can send it to yourself and forward it.

Step 3

If your certificate was signed by the auralis support go to https://identity.apple.com/pushcert/ and upload your signed certificate request.
You will receive a certificate by Apple. Please upload this below.

Push Certificate: Keine ausgewählt

© 2014 auralis ® by Thinking Objects

Select the push certificate from Apple in „Step 3“ and upload it to auralis.

Note

auralis is now activated with a 30 day trial license. You can create up to five users and use all features during that period.

The next chapter shows how to install a purchased license file.

In chapter 6.7 you can find additional information regarding the push services of Apple und Google, and the installation of the Google push service „GCM“.

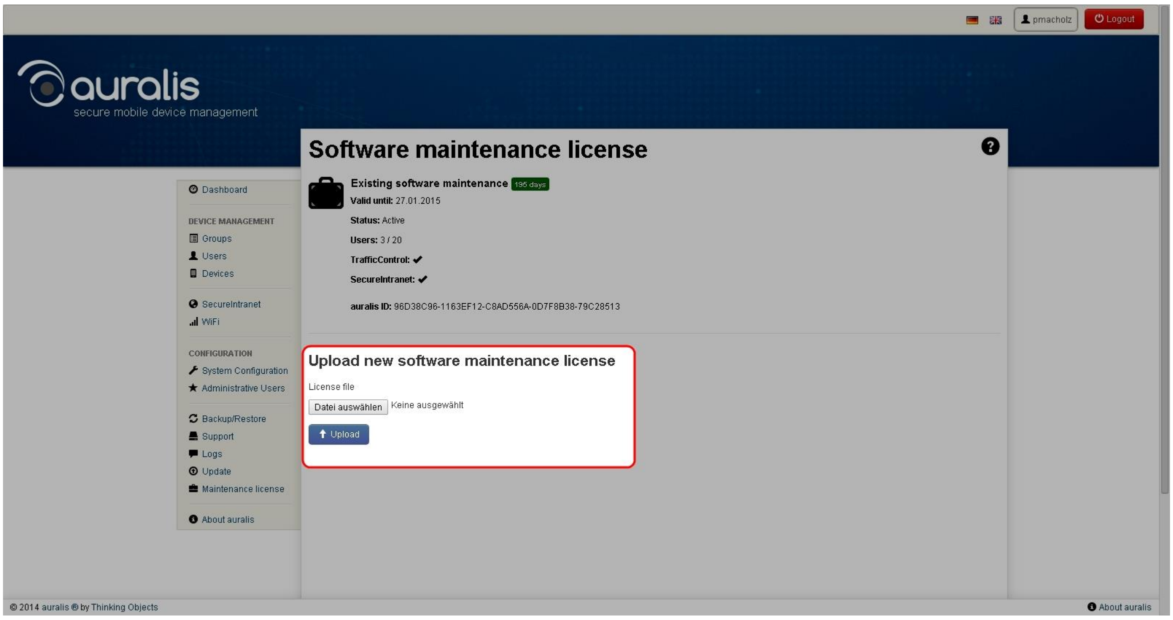
2.7 Install License

To activate an auralis license, you need an Apple push certificate.

Goto menu item „Maintenance license“ and click on “Browse”, select the license file and then click “Upload”

The license is now installed. The details of the license are shown are shown.

In the same way you can install a renewal license file.



Software maintenance license

Existing software maintenance 195 days

Valid until: 27.01.2015

Status: Active

Users: 3 / 20

TrafficControl: ✓

SecureIntranet: ✓

auralis ID: 96D38C96-1163EF12-C8AD556A-0D7F8B38-79C28513

Upload new software maintenance license

License file

Datei auswählen Keine ausgewählt

3 Administrator interface

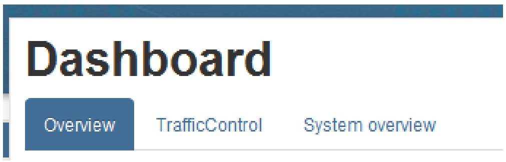
3.1 Dashboard

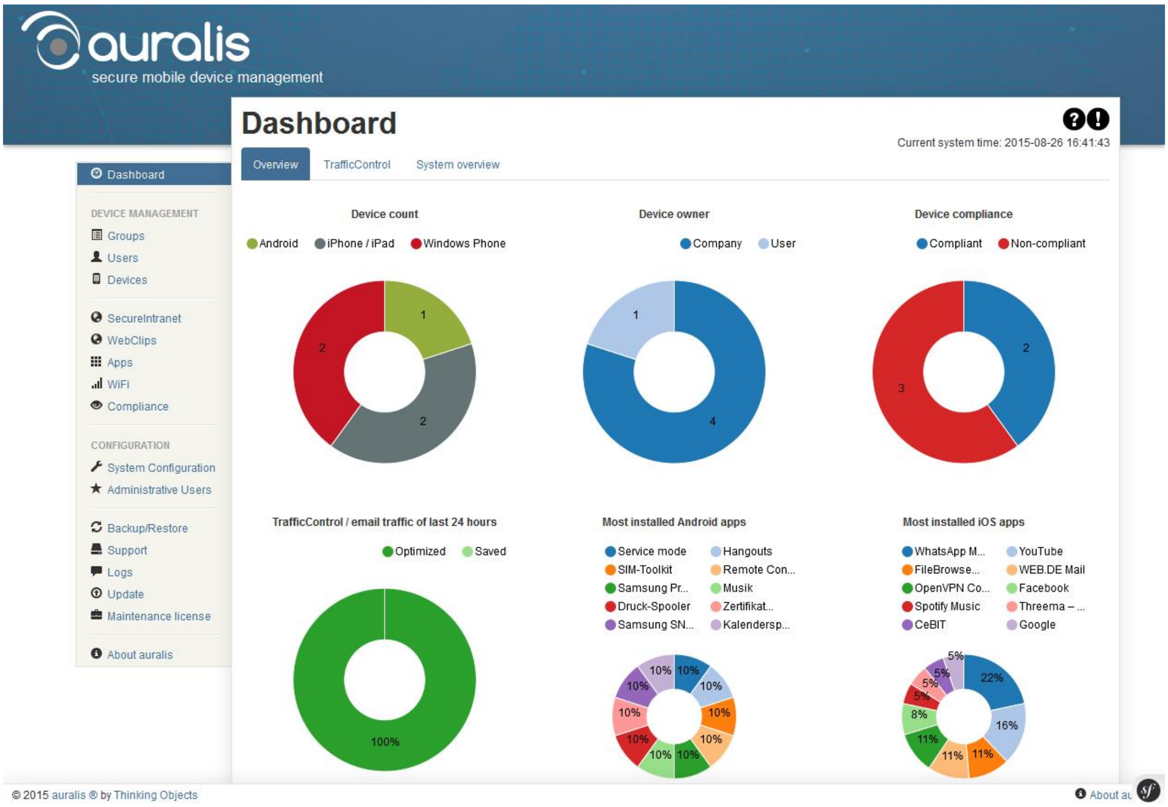
The dashboard is divided into thee tabs.

1) Overview
   An overview of all of your integrated smartphones. For example, number of devices according to OS, device owners (BYOD), top 10 apps installed, toptalkers (devices with the most e-mail data volume) and last active devices.

2) TrafficControl
   In this overview you see all information from our e-mail compression feature. Theoretical transmission values, actual and saved Traffic broken down by file type.

3) System overview
   See all system relevant information such as CPU, RAM, HDD and LAN utilization. Also you will be shown the status of Apple and Google push service and the accessibility of auralis update server.





3.2 Groups

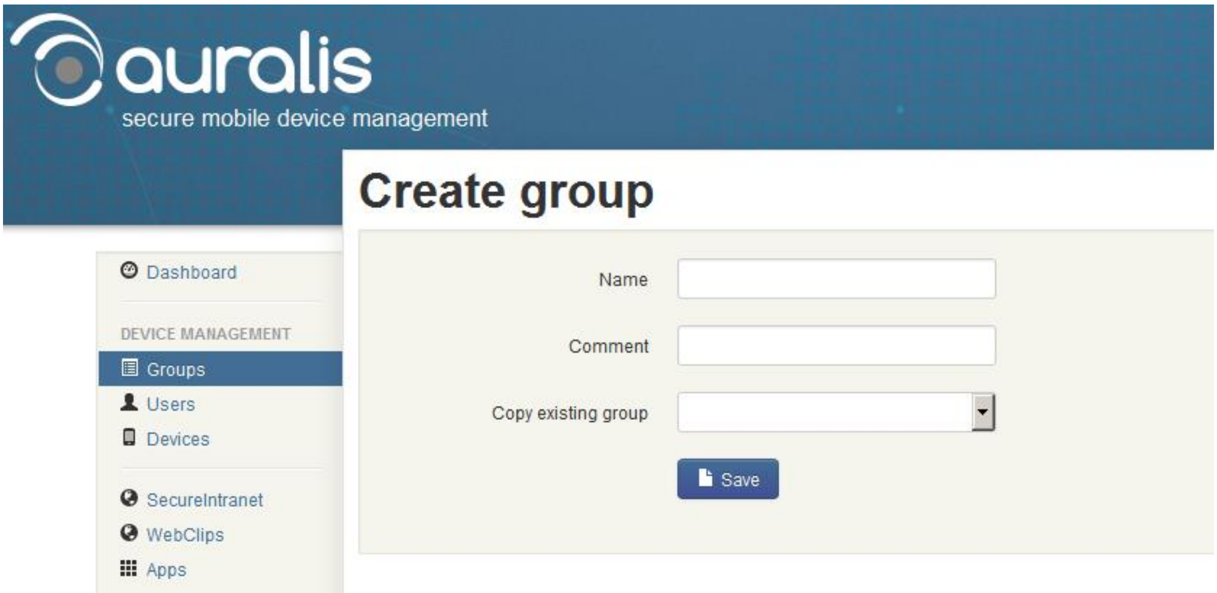
The menue itm “Groups” provides easy management of settings and policies for users and devices by assigning them to groups. By clicking on the item you get a list of all configured groups. You can edit and delete groups or create new groups.

Create Group

To add a new group, click the "Create group" button. In the field "Name", type the name of the new group. The "Comment" field is optional. Then, click "Save" button to add the group.

To minimize the configuration effort for several groups, you can at this point also copy an existing group and adjust the necessary changes.

For all devices in this group, the e-mail settings are automatically associated. Would you like to create a group without e-mail settings, you can create a group using the context menu without e-mail configuration. For each device in a group without e-mail profile a separate license is required.



Create group

Name

Comment

Copy existing group

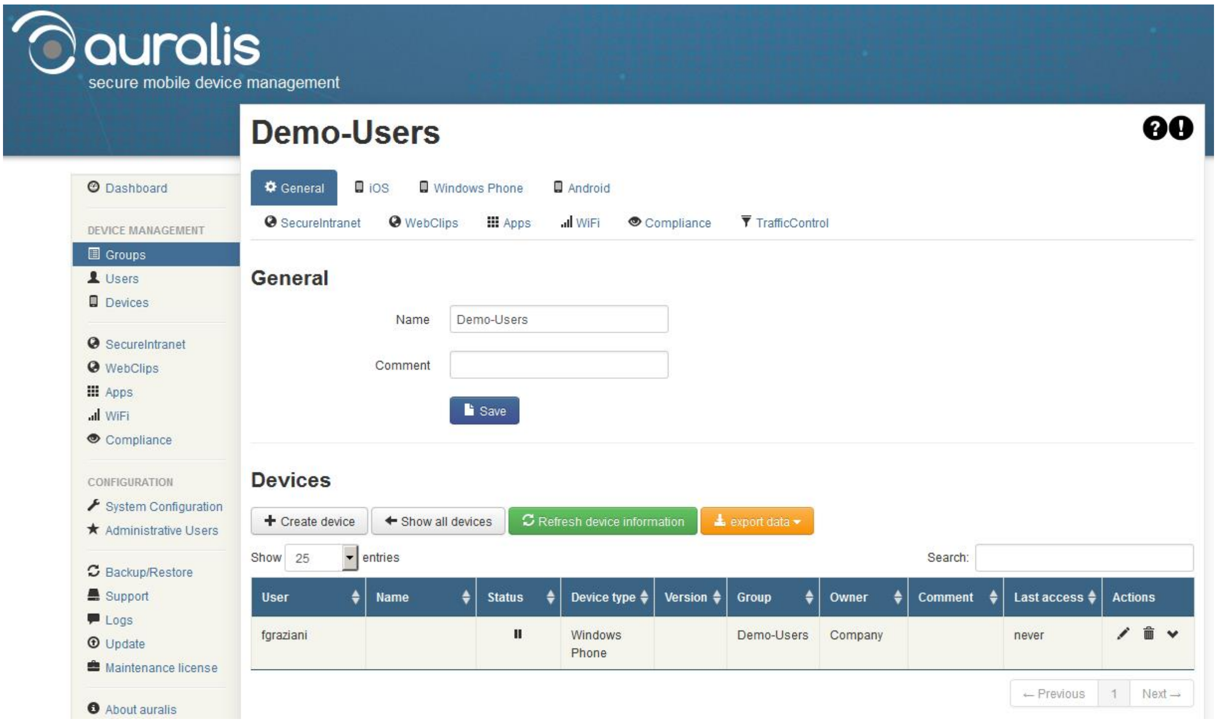
After creating a new group, you are taking to the settings of the group. You can always go to the settings page of a group by clicking on edit in the column actions.

3.2.1 Group settings

The configuration setting of a group contains various tabs. These apply to all devices assigned to the group.

3.2.2 General

You can change the group name, add or edit a comment for the group and add devices to the group. All devices assigned to the group will be shown in a list view.



Demo-Users

General

Name: Demo-Users

Comment:

Devices

Show 25 entries

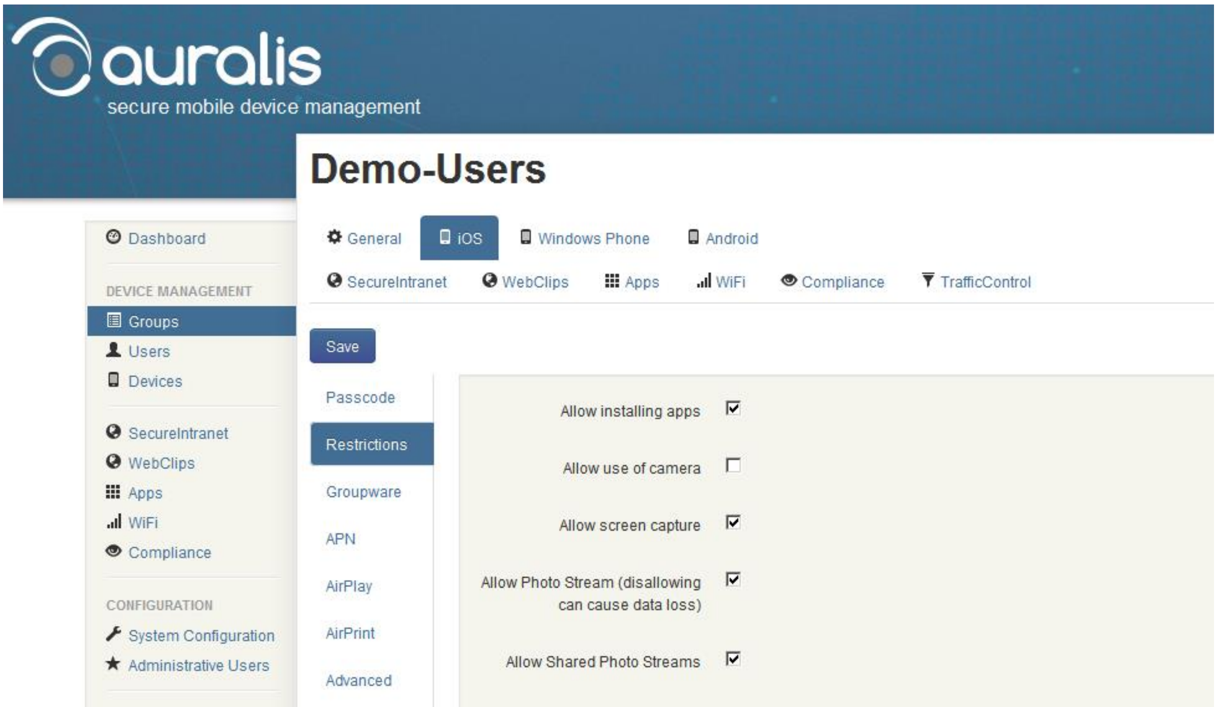
Search:

User	Name	Status	Device type	Version	Group	Owner	Comment	Last access	Actions
fgraziani		⏸	Windows Phone		Demo-Users	Company		never	

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

On the tabs "iOS", "Android", and "Windows Phone" you can change the settings for devices with the corresponding operating system. These include among others settings for device security and system restrictions.

The range of settings differs depending on the mobile operating system and manufacturer.



Allow installing apps ☑

Allow use of camera □

Allow screen capture ☑

Allow Photo Stream (disallowing can cause data loss) ☑

Allow Shared Photo Streams ☑

3.2.4 WiFi

Enable or disable the wireless networks in the WiFi tab. All devices in the group will automatically connect to WIFI networks in range.

How to create WiFi networks are described in Chapter 5 - Global configurations.

3.2.5 SecureIntranet

SecureIntranet enables access to your internal web applications for your mobile devices. Instead of using a battery draining VPN connection, the access is provided safely by using the certificate based authorization of auralis. Please note, that some web applications might not support this mode of access.

In the tab „SecureIntranet“ you can enable access to specific URLs for the group. The corresponding links to the applications will be added automatically to the home screen on iOS and Android devices.

How to create SecureIntranet links is described in Chapter 5 - Global configurations.

3.2.6 Webclips

Web shortcuts to websites on home screen are called webclips. At this point you can specify which web clips automatically created for this group.

How to create Webclips is described in Chapter 5 - Global configurations.

3.2.7 Compliance

Specify which compliance rule for this group applies. There can only be set up one compliance rule per group.

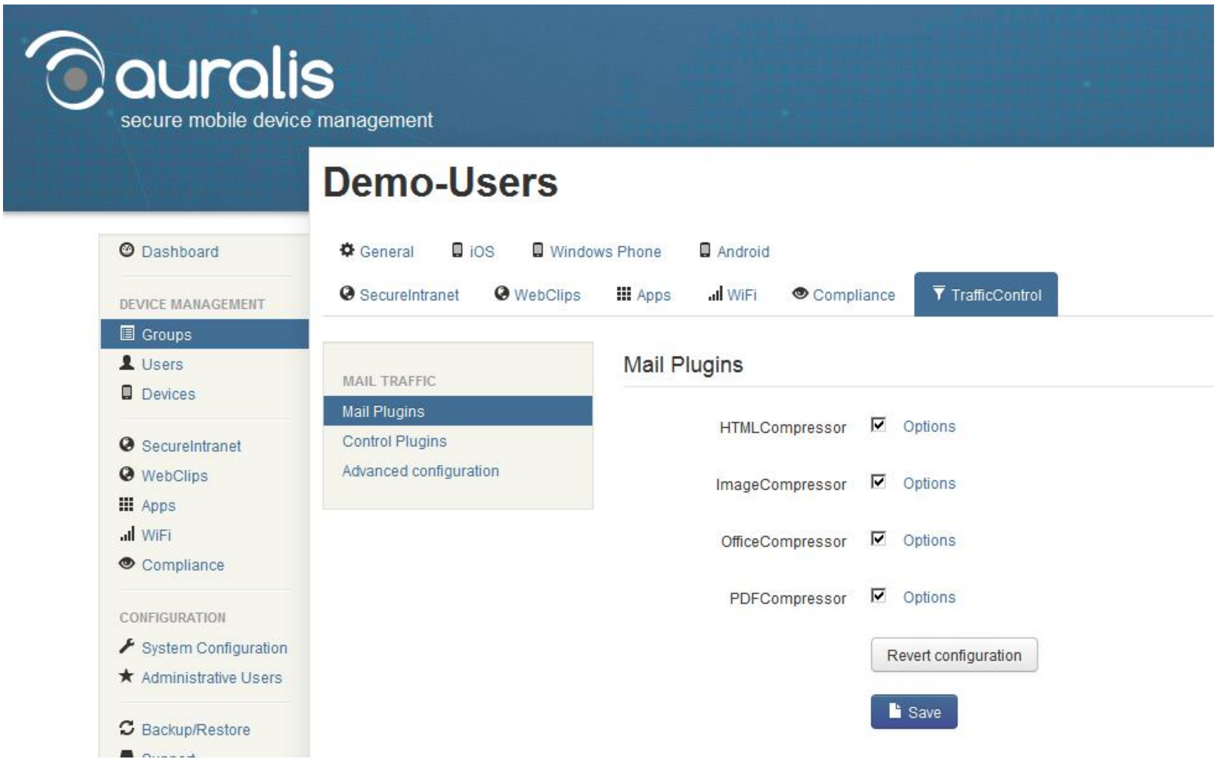
How to create compliance rules is described in Chapter 5 - Global configurations.

3.2.8 TrafficControl

TrafficControl compresses file attachments in emails and thus lowers communication costs and speeds up the transfer of email to the device. TrafficControl can compress images , Microsoft Office documents (starting with version 2007) and PDF files by up to 90 percent.

Mail Plugins

You can specify, which types of attachments are processed by TrafficControl. Clicking on “Options” lets you tweak the details of the compression for each compression plugin. In most cases it is best to leave these settings at their defaults.



Demo-Users

Mail Plugins

HTMLCompressor ☑ Options

ImageCompressor ☑ Options

OfficeCompressor ☑ Options

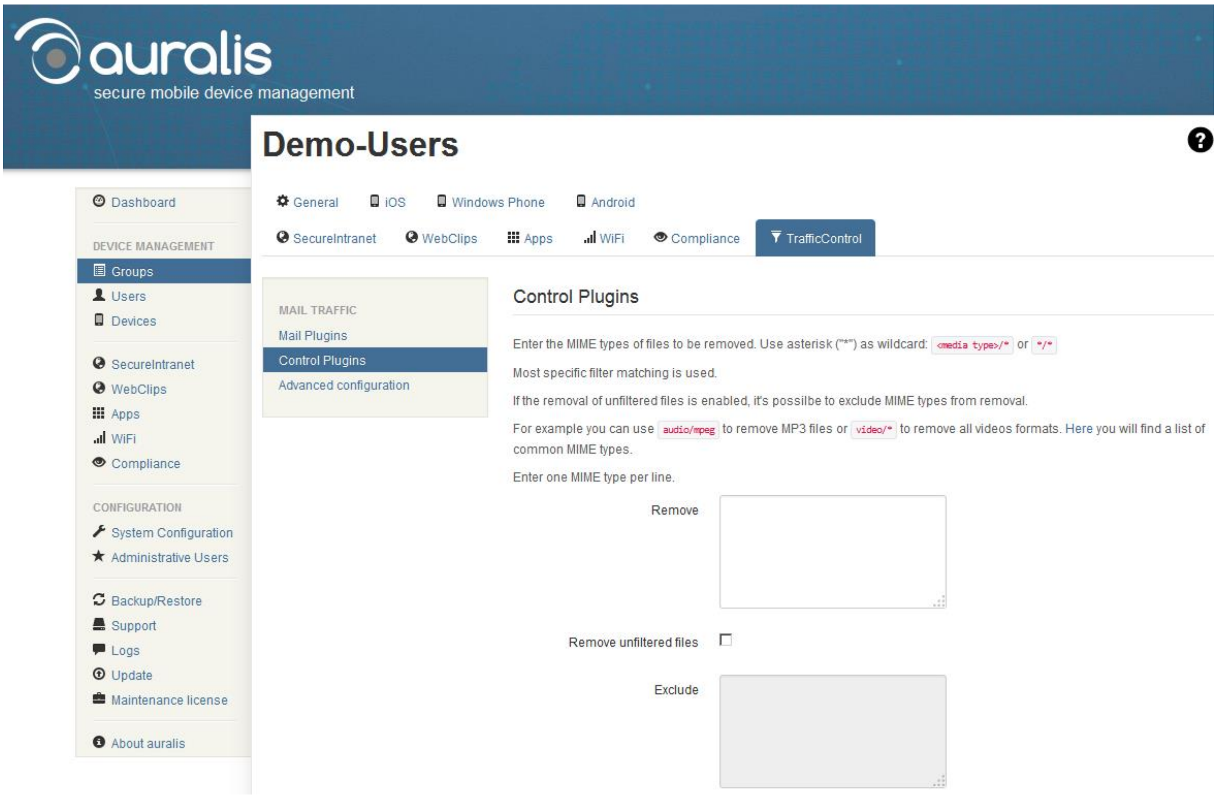
PDFCompressor ☑ Options

Note

The compression is only applied to the synchronized copy of the email on the mobile device. The original email residing on the server is not changed.

Control Plugins

Auralis offers you to filter certain attachment types and have them removed from the copy of the email transferred to the mobile device. The type of the attachment is specified using MIME types („<main type>/<sub type>“). In the field “Remove” you specify the mime types to remove, all others are not touched by the plugin. You can uses “*” as a wildcard e.g. “video/*”. To exempt certain sub types from the removal process, you can check “Remove unfiltered files” and specify the exception in “Exclude”.



Control Plugins

Enter the MIME types of files to be removed. Use asterisk ("*") as wildcard: `<media type>/*` or `*/*`

Most specific filter matching is used.

If the removal of unfiltered files is enabled, it's possilbe to exclude MIME types from removal.

For example you can use `audio/mpeg` to remove MP3 files or `video/*` to remove all videos formats. Here you will find a list of common MIME types.

Enter one MIME type per line.

Remove

Remove unfiltered files □

Exclude

Advanced configuration

This setting affects the behavior of the plugins in case of a compression problem.

- Ignore: auralis ignores the erroneous file and continues with the next operation.
- Remove: The file is deleted from the message sent to the device.
- Pass-through: The ActiveSync message is delivered to the device unchanged.

3.2.9 Apps

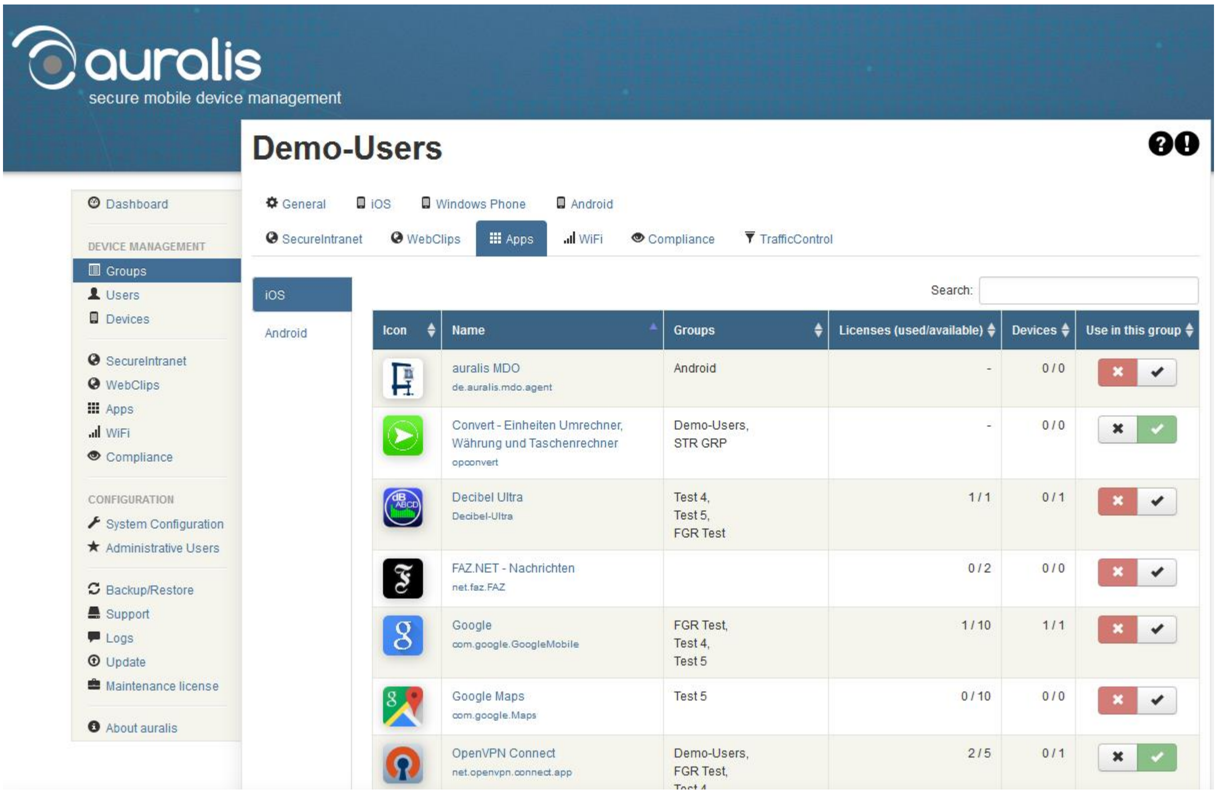
In Apps tab, you can activate the iOS or Android apps which will installed as managed app on all devices in the respective group. Users are prompted to install these apps.

iOS devices differs between normal managed and purchased apps by Apple VPP. In both cases, the user requires a separate/own Apple ID.

Normal free Apps installed immediately. For paid apps, the user has to enter his Apple ID to buy the app.

When Apps purchased through the Apple VPP program, the Apps will be associated to the private Apple ID of the user and the user can install it free of charge.

How to Configure Apps for centralized management is described in Capital 5 - Global configurations.



Demo-Users

Icon	Name	Groups	Licenses (used/available)	Devices	Use in this group
	auralis MDO de.auralis.mdo.agent	Android	-	0 / 0	✖ ✔
	Convert - Einheiten Umrechner, Währung und Taschenrechner opconvert	Demo-Users, STR GRP	-	0 / 0	✖ ✔
	Decibel Ultra Decibel-Ultra	Test 4, Test 5, FGR Test	1 / 1	0 / 1	✖ ✔
	FAZ.NET - Nachrichten net.faz.FAZ		0 / 2	0 / 0	✖ ✔
	Google com.google.GoogleMobile	FGR Test, Test 4, Test 5	1 / 10	1 / 1	✖ ✔
	Google Maps com.google.Maps	Test 5	0 / 10	0 / 0	✖ ✔
	OpenVPN Connect net.openvpn.connect.app	Demo-Users, FGR Test, Test 4	2 / 5	0 / 1	✖ ✔

3.3 Users

The menu item “Users” lists all configured users and gives details for each user. New users can be created and existing user can be modified. You can also import users from an existing LDAP repository.

3.3.1 Create user

To create a new user, click “Create user”. Enter all necessary information into the form.

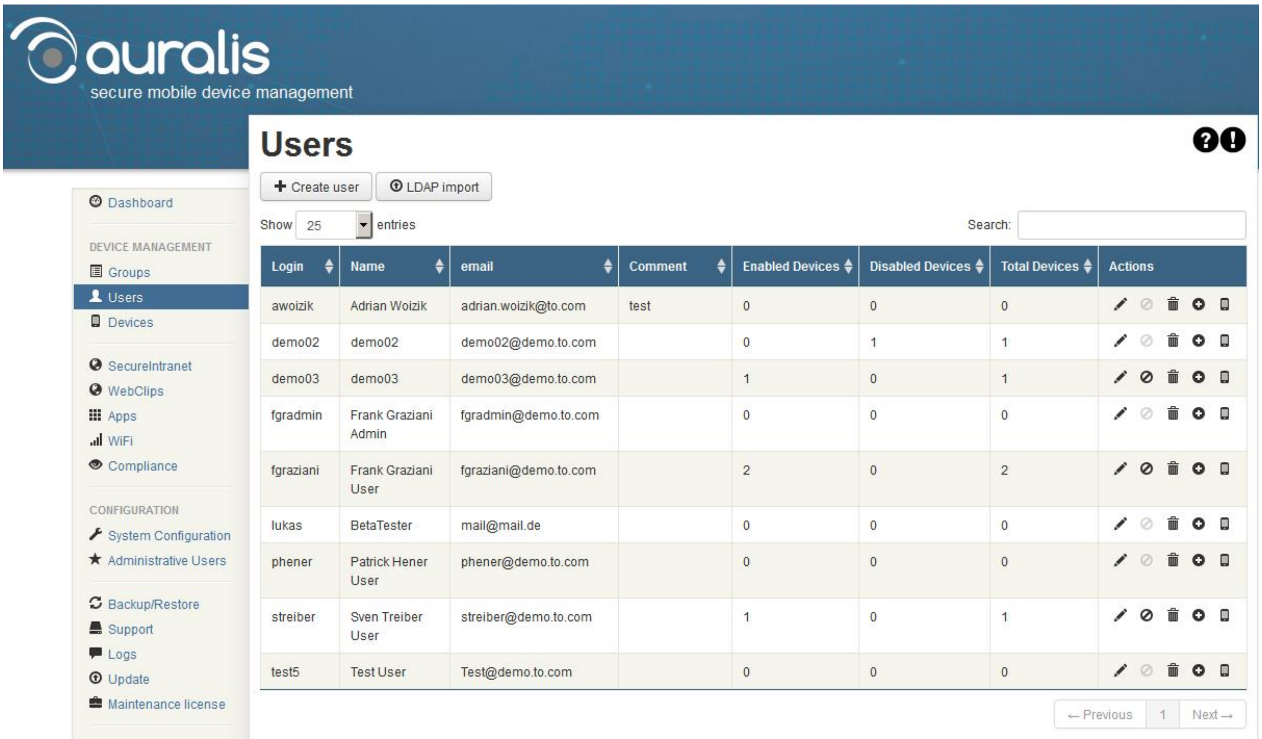
Login: The login name of the user. The user later uses this name to login to auralis to start the provisioning of the device.

Name: The full name of the user.

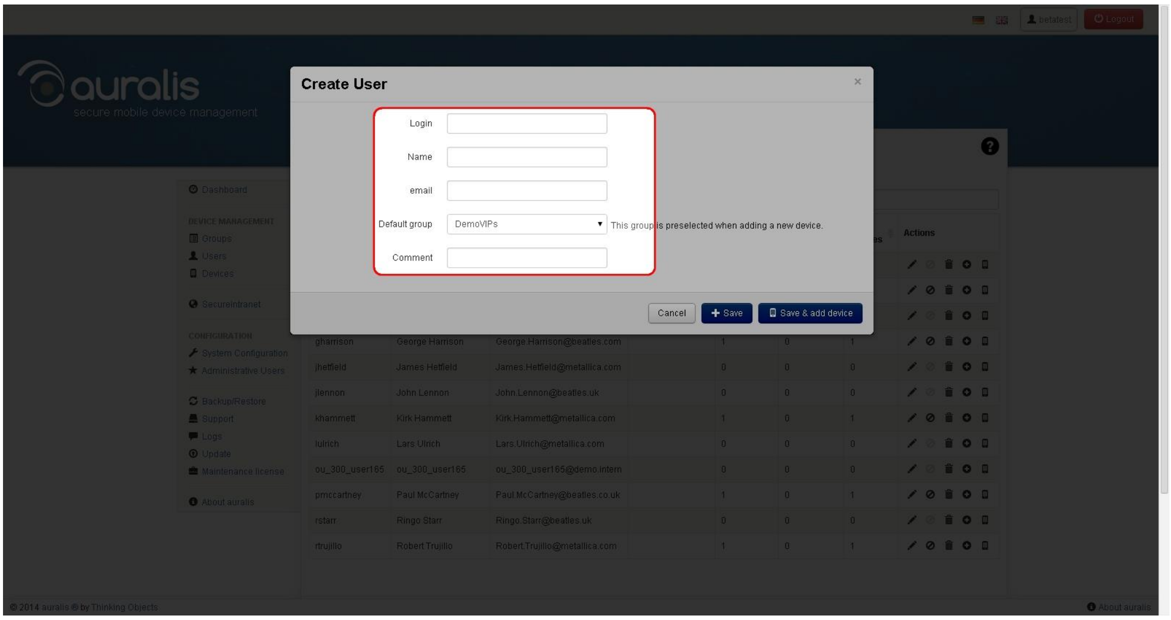
eMail: The email address of the user.

Default group: The group used as default, when creating a new device. Beyond that use the default group has no additional meaning.

Comment: Additional information regarding the user at you disposal.



Login	Name	email	Comment	Enabled Devices	Disabled Devices	Total Devices	Actions
awoizik	Adrian Woizik	adrian.woizik@to.com	test	0	0	0	✎ ⊘ 🗑 ⊕ ▯
demo02	demo02	demo02@demo.to.com		0	1	1	✎ ⊘ 🗑 ⊕ ▯
demo03	demo03	demo03@demo.to.com		1	0	1	✎ ⊘ 🗑 ⊕ ▯
fgradmin	Frank Graziani Admin	fgradmin@demo.to.com		0	0	0	✎ ⊘ 🗑 ⊕ ▯
fgraziani	Frank Graziani User	fgraziani@demo.to.com		2	0	2	✎ ⊘ 🗑 ⊕ ▯
lukas	BetaTester	mail@mail.de		0	0	0	✎ ⊘ 🗑 ⊕ ▯
phener	Patrick Hener User	phener@demo.to.com		0	0	0	✎ ⊘ 🗑 ⊕ ▯
streiber	Sven Treiber User	streiber@demo.to.com		1	0	1	✎ ⊘ 🗑 ⊕ ▯
test5	Test User	Test@demo.to.com		0	0	0	✎ ⊘ 🗑 ⊕ ▯



Create User

Login	
Name	
email	
Default group	DemoVIPs ▾ This group is preselected when adding a new device.
Comment	

Cancel | + Save | Save & add device

gharrison	George Harrison	George.Harrison@beatles.com	1	0	1
jhetfield	James Hetfield	James.Hetfield@metallica.com	0	0	0
jlennon	John Lennon	John.Lennon@beatles.uk	0	0	0
khammett	Kirk Hammett	Kirk.Hammett@metallica.com	1	0	1
lulrich	Lars Ulrich	Lars.Ulrich@metallica.com	0	0	0
ou_300_user165	ou_300_user165	ou_300_user165@demo.intern	0	0	0
pmccartney	Paul McCartney	Paul.McCartney@beatles.co.uk	1	0	1
rstarr	Ringo Starr	Ringo.Starr@beatles.uk	0	0	0
rtrujillo	Robert Trujillo	Robert.Trujillo@metallica.com	1	0	1

After filling out the form click “Save” to create the user.

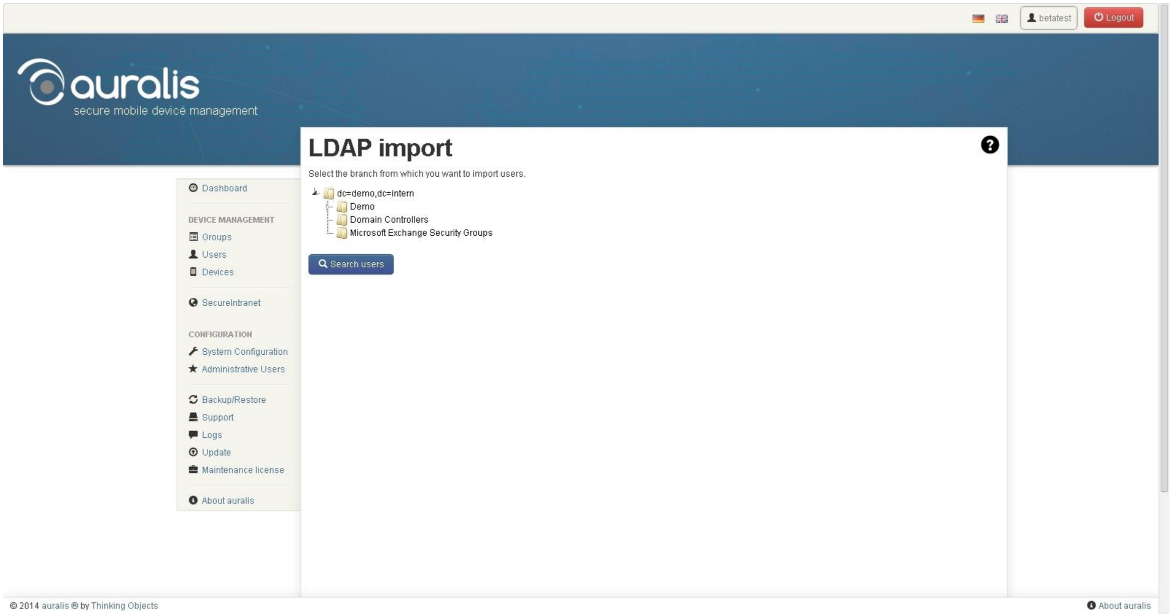
If you want to add a device for the user immediately in addition, click “Save & add device”. You can always add devices to a user later.

By clicking on “Cancel”, all information is discarded and now user is created.

LDAP Import

To be able to use the LDAP import, you need to configure a LDAP server first (see Chapter 5 – Global configurations).

To import users from your LDAP server, click “LDAP import”, select the OU to import users from and click “Search users”.



LDAP import

Select the branch from which you want to import users.

- dc=demo,dc=intern
  - Demo
  - Domain Controllers
  - Microsoft Exchange Security Groups

The users found will be displayed in a chart. Check the users you want to import and select a group for the users. To create a device for each user and send an email to the user upon import check “Create devices”.

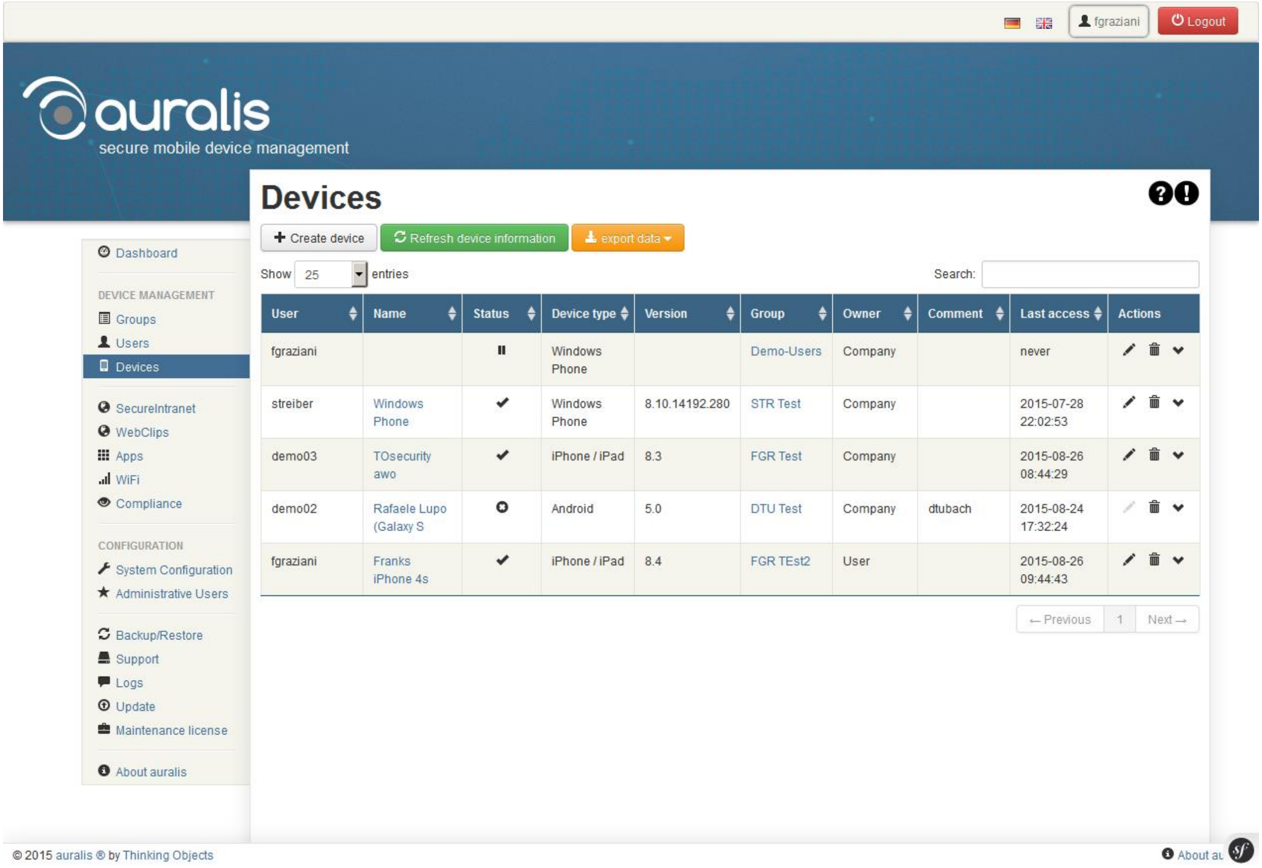
You can edit the values for import by clicking on the values in the chart and editing them. The LDAP will not be changed.

Once your data is ready, click “import selected users” to start the import.

3.4 Devices

All configured devices are displayed in the menu item “Devices”.

See chapter 3.5 how to crate new devices.



User	Name	Status	Device type	Version	Group	Owner	Comment	Last access	Actions
fgraziani		⏸	Windows Phone		Demo-Users	Company		never	✎ 🗑 ▾
streiber	Windows Phone	✓	Windows Phone	8.10.14192.280	STR Test	Company		2015-07-28 22:02:53	✎ 🗑 ▾
demo03	TOsecurity awo	✓	iPhone / iPad	8.3	FGR Test	Company		2015-08-26 08:44:29	✎ 🗑 ▾
demo02	Rafaele Lupo (Galaxy S	○	Android	5.0	DTU Test	Company	dtubach	2015-08-24 17:32:24	✎ 🗑 ▾
fgraziani	Franks iPhone 4s	✓	iPhone / iPad	8.4	FGR TEst2	User		2015-08-26 09:44:43	✎ 🗑 ▾

You can create new devices, export device information and data in CSV or XLSX format and modify device configurations. All configured devices are shown the table “Devices”. The table also displays some basic information about each device.

User: The username of the owner of the device. Multiple devices can be assigned to the same user.

Name: The name of the device. The name is read from the device. By clicking on the device name, you get the information overview for the device.

Status: The status icon of the device which can be provisioned (check icon), to be provisioned (pause icon) or disabled (disabled icon).

Device type: The type of the device „iPhone/iPad“, „Android“, „Windows Phone“ or „Other“.

Version: Version information about the installed OS of the device.

Group: The group assigned to the device. You can get the group settings by clicking on the group name.

Last access: The last time the device was connected to auralis.

Owner: Company owned or BYOD Device.

Comment: The optional comment.

Actions: By clicking on the down arrow you get access to all actions available for the device. The Actions “Edit” and “Delete” can be accessed directly by clicking on the corresponding icon.

Edit: Edit the device settings.

Delete: A popup asks you to confirm the deletion of the device. After confirmation, a wipe command will be sent to the device removing all changes made by auralis. Afterwards the state of the device will resemble the state before provisioning it to auralis. All other settings on the device are kept. The “delete” icon will be shown in red, until auralis receives the wipe confirmation from the device.

To finally remove the device from the list, click the red “delete” icon.

Note

By wiping the device all certificates associated with the device will be revoked by auralis. To reenable the devices, it needs tob e provisioned again.

Additional actions:

Info: Shows the detailed device information. This item is only available after the device has been successfully provisioned as the information is read from the device. The information can be requested by clicking on ###“refresh”###. ###”Disable Device???###

Remote wipe: Send a wipe command to the device. All changes made to the device by auralis will be removed and the device certificates will be revoked afterwards.

Factory reset: The device will be reset to factory settings. ###?###

Caution

A factory reset will irrevocably delete all data on the device.

Clear passcode: The passcode will be disabled. The device can be unlocked without a passcode afterwards.

Lock: Locks the device. An optional warning message and phone number will be displayed to the user. The PIN of the device remains. Thus, the finder of this device can contact the telephone number. This feature is only available for iOS and Android devices.

Download device certificate: Donwloads the device certificate for devices of type “other”. The certificate will be encrypted with the rollout password.

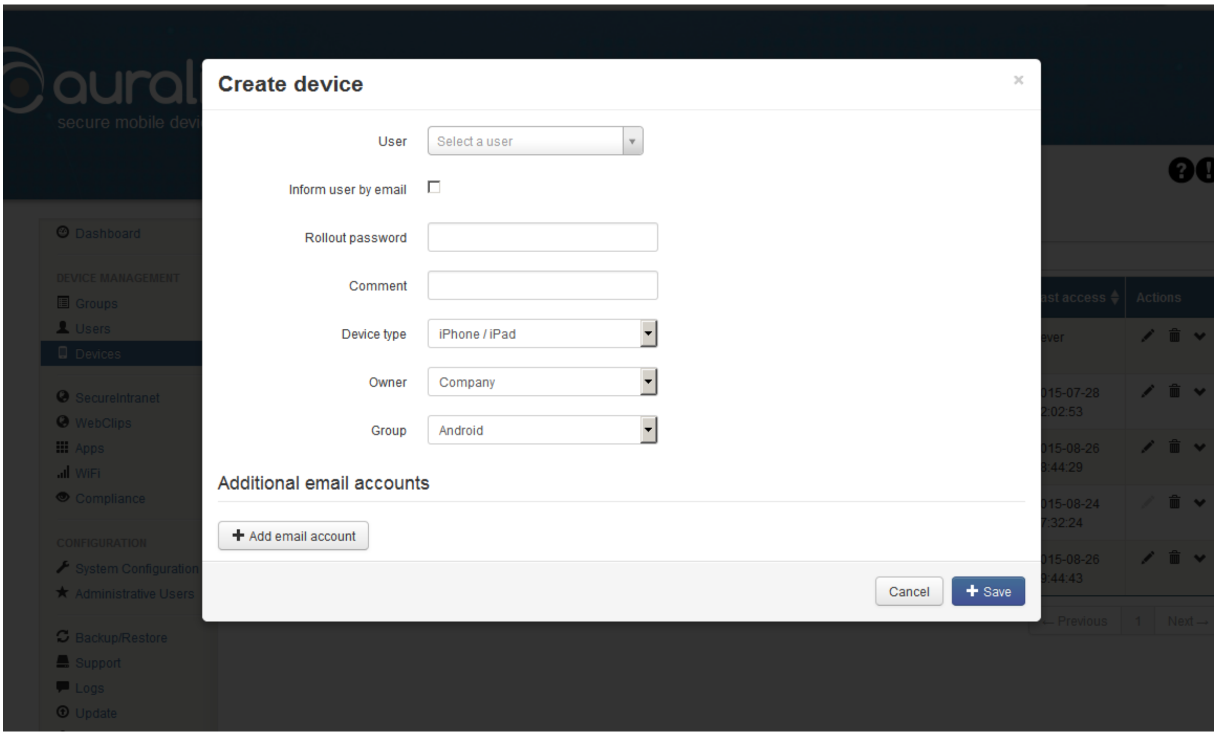
Resend push message: Sends a push message to the device asking it to retrieve available actions from auralis manually. As soon as an action is available for a device, auralis will automatically send a push message to the device. If the device doesn’t respond, auralis will resend the push message at regular intervals.

Delete: See Actions: Delete above.

Edit: See Actions: Edit above.

3.5 Create device

Use "create device".



Create device

User Select a user

Inform user by email □

Rollout password

Comment

Device type iPhone / iPad

Owner Company

Group Android

Additional email accounts

+ Add email account

Cancel | + Save

User: Select user for this device.

Inform user by email: User will get email instructions.

Rollout-password: Choose rollout one time password.

Comment: Comment for the device.

Device type: Choose between „iPhone/iPad“, „Android“, „Windows Phone“ and „Others“.

Owner: Company owned or user (BYOD).

Group: Select the profile group for this device.

Additional email accounts: Is there a need to assign multiple email accounts you can do that here.

4 Device - Provisioning

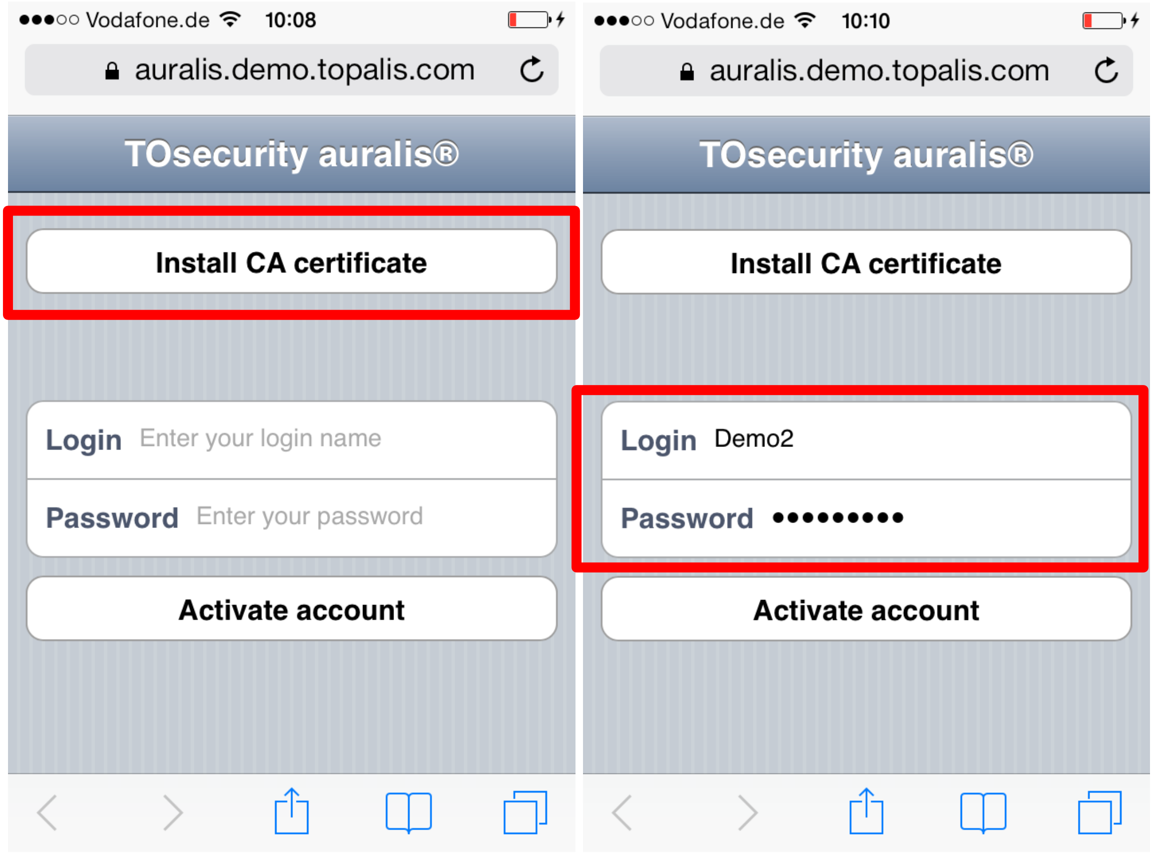
This chapter details the provisioning of different mobile devices. The subchapters give detailed explanations for Apple iPhone, Android devices und devices with the Windows Phone operating system.

4.1 iPhone/iPad/iPod

Please make sure, that any Apple device you want to provision has at least iOS version 5 or newer installed. Once the administrator has added the device in auralis, the user gets an email (if configured) containing a link to the user provisioning instructions.

Open the URL https://*<auralis-host>*:8443 on your iOS device.

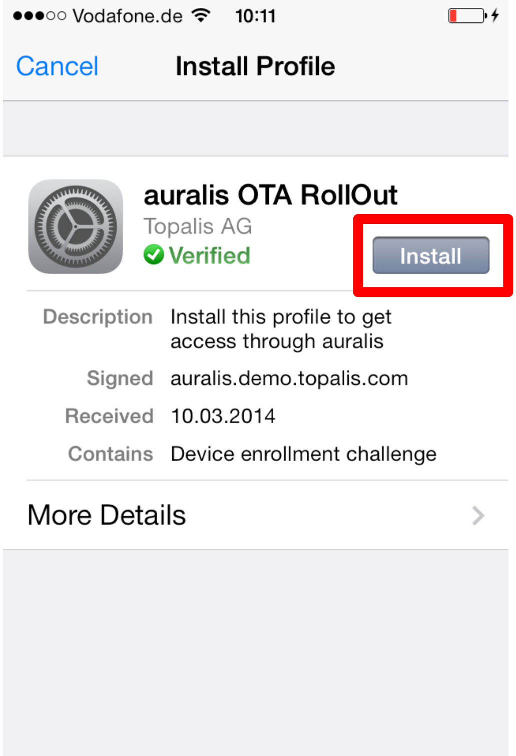
Choose "Install CA certificate", the CA will be installed. After coming back to the site, enter your credentials (your username and one time password for provisioning) and press "Enable access" to start the provisioning process.



Login Demo2

Password •••••••••

You will be asked to install a profile. Press “install” to proceed and confirm the next query by pressing “install”.



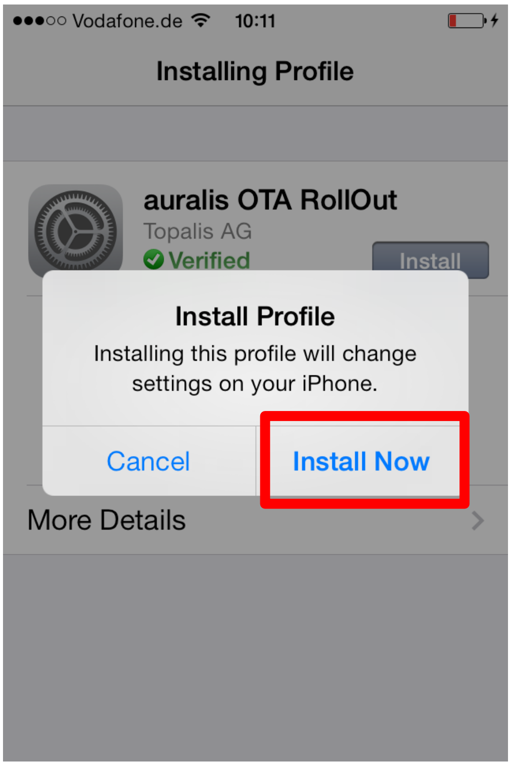
●●●○○ Vodafone.de 10:11

Cancel Install Profile

auralis OTA RollOut
Topalis AG
✓ Verified
Install

Description	Install this profile to get access through auralis
Signed	auralis.demo.topalis.com
Received	10.03.2014
Contains	Device enrollment challenge

More Details



●●●○○ Vodafone.de 10:11

Installing Profile

auralis OTA RollOut
Topalis AG
✓ Verified
Install

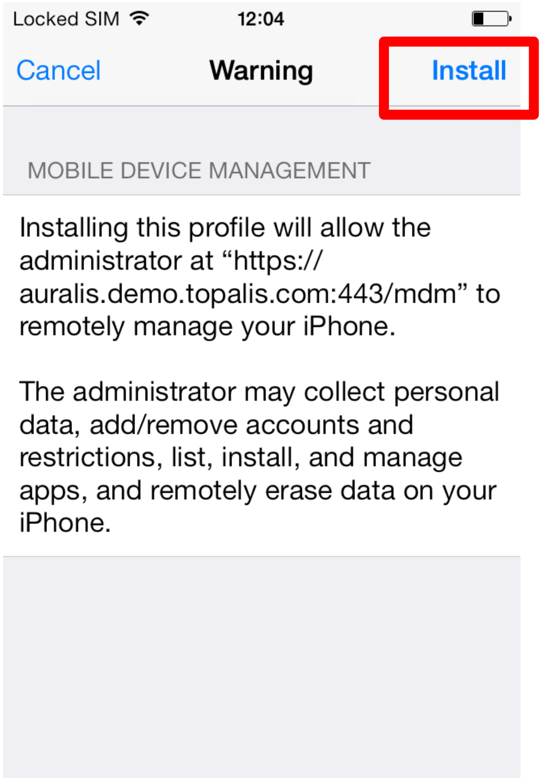
Install Profile

Installing this profile will change settings on your iPhone.

Cancel Install Now

More Details

Please acknowledge the warning „Mobile Device Management“ by pressing “install”. The following notification can be closed by pressing “done”



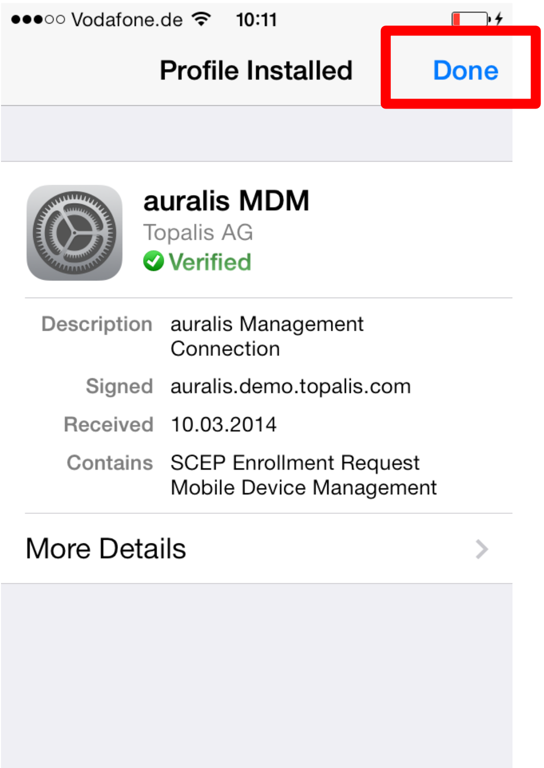
Locked SIM 12:04

Cancel Warning Install

MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at “https://auralis.demo.topalis.com:443/mdm” to remotely manage your iPhone.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPhone.



●●●○○ Vodafone.de 10:11

Profile Installed Done

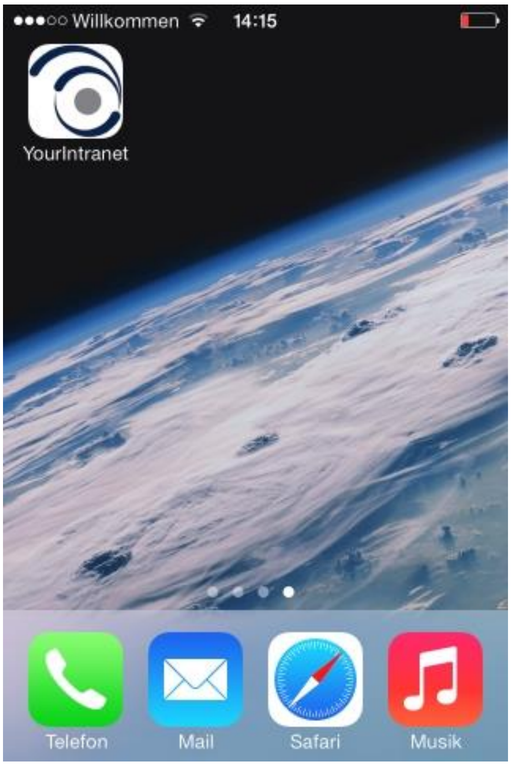
auralis MDM
Topalis AG
✓ Verified

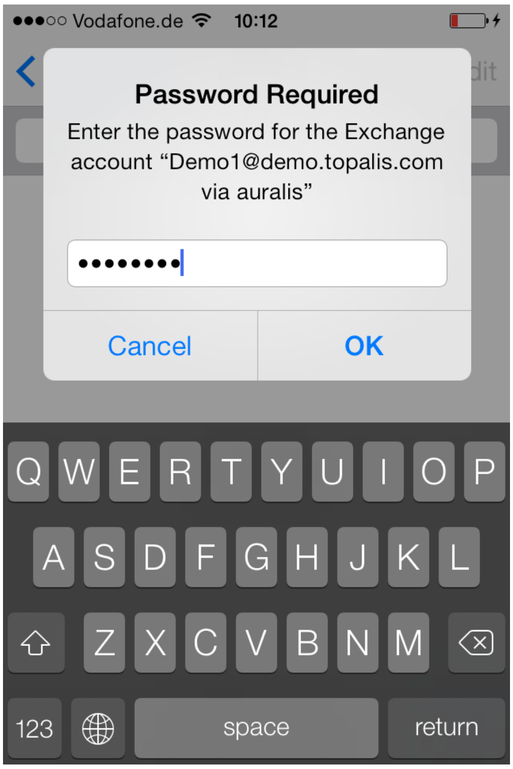
Description	auralis Management Connection
Signed	auralis.demo.topalis.com
Received	10.03.2014
Contains	SCEP Enrollment Request Mobile Device Management

More Details

If SecureIntranet applications are configured for your device, auralis will install the configured links on your home screen.

Please start the email application now. Enter the password for your email account in the password dialogue that also shows the email address of your account and press ok. Your emails are now synched with your device.





Password Required

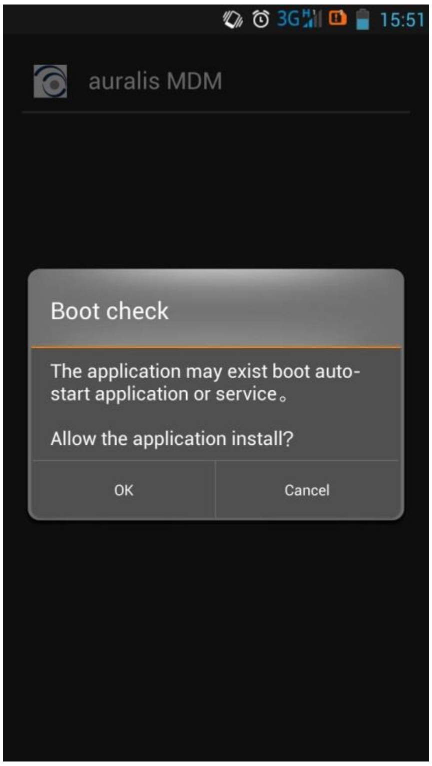
Enter the password for the Exchange account “Demo1@demo.topalis.com via auralis”

Note

Depending on the quality and speed of your internet connection, the provisioning of a device can take several minutes.

4.2 Android

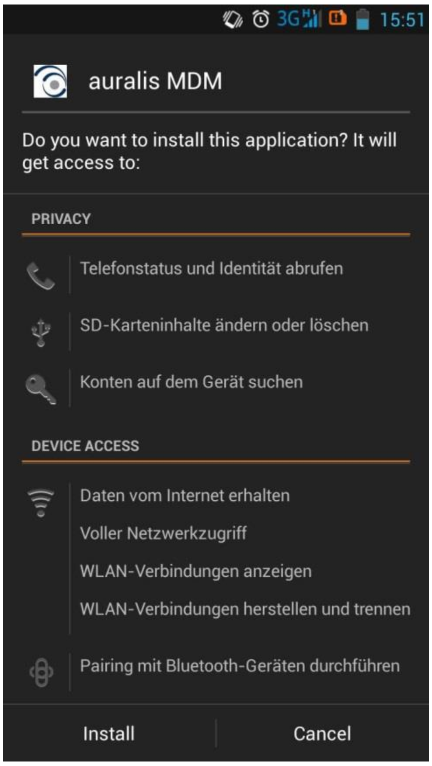
Please make sure, that any Android device you want to provision has at least Android version 4.2.1 or newer installed. Search for “auralis” in the Play Store and install the auralis MDM app.



Boot check

The application may exist boot auto-start application or service。

Allow the application install?



auralis MDM

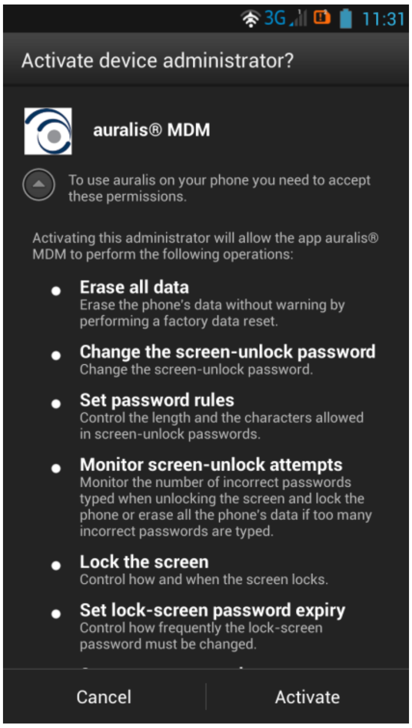
Do you want to install this application? It will get access to:

PRIVACY

- Telefonstatus und Identität abrufen
- SD-Karteninhalte ändern oder löschen
- Konten auf dem Gerät suchen

DEVICE ACCESS

- Daten vom Internet erhalten
- Voller Netzwerkzugriff
- WLAN-Verbindungen anzeigen
- WLAN-Verbindungen herstellen und trennen
- Pairing mit Bluetooth-Geräten durchführen



Activate device administrator?

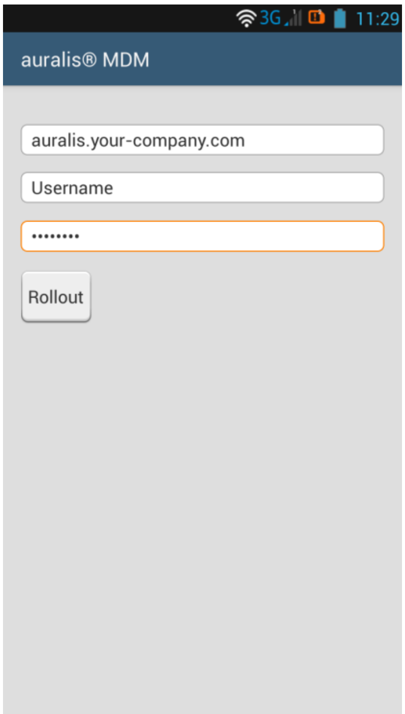
auralis® MDM

To use auralis on your phone you need to accept these permissions.

Activating this administrator will allow the app auralis® MDM to perform the following operations:

- **Erase all data**
  Erase the phone’s data without warning by performing a factory data reset.
- **Change the screen-unlock password**
  Change the screen-unlock password.
- **Set password rules**
  Control the length and the characters allowed in screen-unlock passwords.
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords typed when unlocking the screen and lock the phone or erase all the phone’s data if too many incorrect passwords are typed.
- **Lock the screen**
  Control how and when the screen locks.
- **Set lock-screen password expiry**
  Control how frequently the lock-screen password must be changed.

Depending on your Android version, the security query shown to the left may be raised. Auralis needs the authorization to be able to manage the device. Please confirm the query if necessary by pressing “ok”, “activate” or “install”.



3G 11:29

auralis® MDM

auralis.your-company.com

Username

••••••••

Rollout

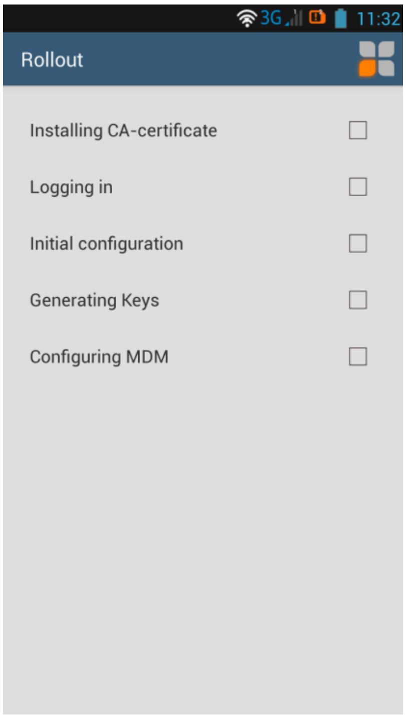
Now open the app „auralis MDM“ on your device and enter your provisioning credentials. For information on adding a device to auralis please see chapter 3.4 “Devices”.

Enter the address of your auralis system (e.g. aurails.mycompany.com) into „auralis Hostname“.

Enter the name of the user, to whom the device is assigned into „username“ and the one time rollout password into „Password“.

Please make sure, that the device is connected to the internet an press “Rollout” to start the process.

During the rollout, you need to confirm three requests to install a certificate. The requests are for the auralis CA (Certificate Authority), the server certificate used by auralis to authenticate with the device and a temporary certificate generated by the app and used during the process.



3G 11:32

Rollout

Installing CA-certificate □

Logging in □

Initial configuration □

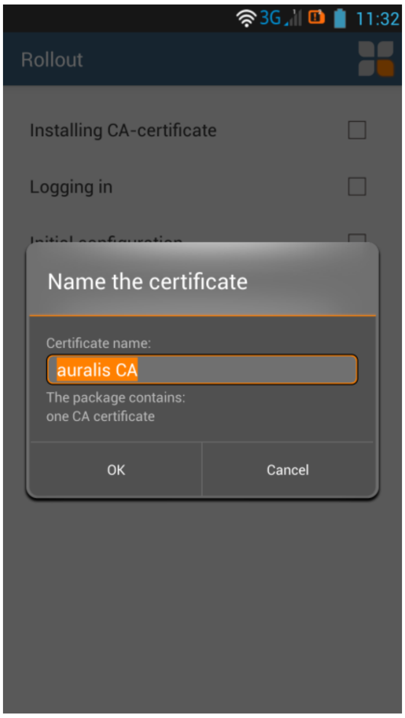
Generating Keys □

Configuring MDM □

Note

Depending on the quality and speed of your internet connection, the provisioning of an Android device can take several minutes. The app will show the progress during the process.

The following information will be asked:



3G 11:32

Rollout

Installing CA-certificate □

Logging in □

Name the certificate

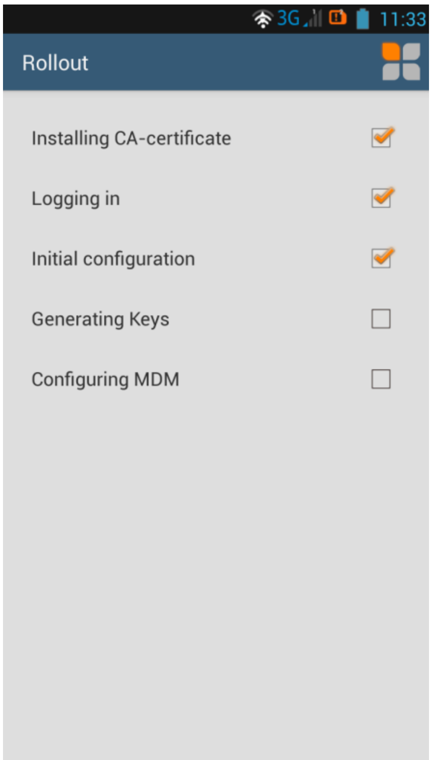
Certificate name:

auralis CA

The package contains:
one CA certificate

OK Cancel

- „Certificate name“ (auralis CA): This is the name used for the auralis CA. If you don't require a different name, you can just accept the default „auralis CA“ and press „OK“.
- „Certificate name“ (auralis Profile Service): This is the name used for the user key and certificate. You can choose your own name if you like. Confirm by pressing „OK“.
- „Certificate name“ (auralis MDM Authentication): Please enter the shown password and press “Ok”. Change the certificate name if you like and press “Ok.”



3G 11:33

Rollout

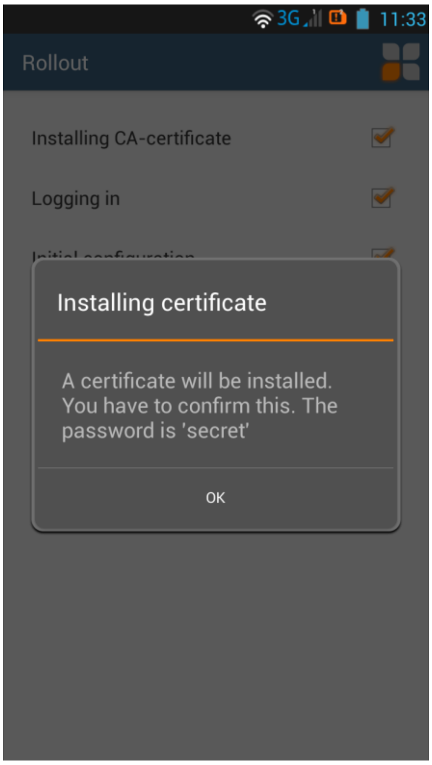
Installing CA-certificate ☑

Logging in ☑

Initial configuration ☑

Generating Keys □

Configuring MDM □



3G 11:33

Rollout

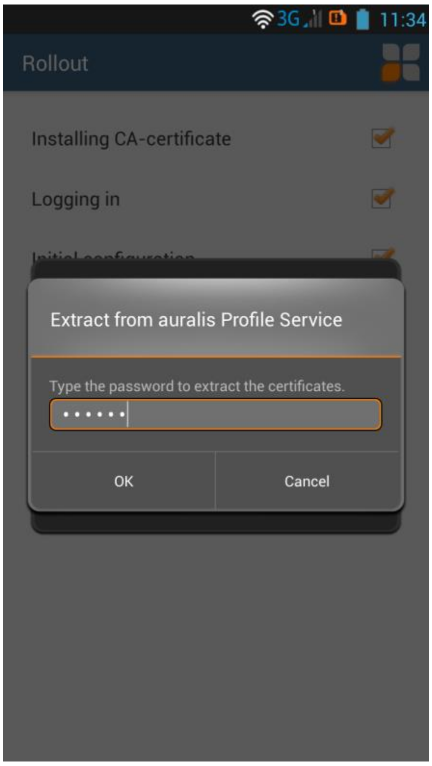
Installing CA-certificate ☑

Logging in ☑

Installing certificate

A certificate will be installed. You have to confirm this. The password is 'secret'

OK



Rollout

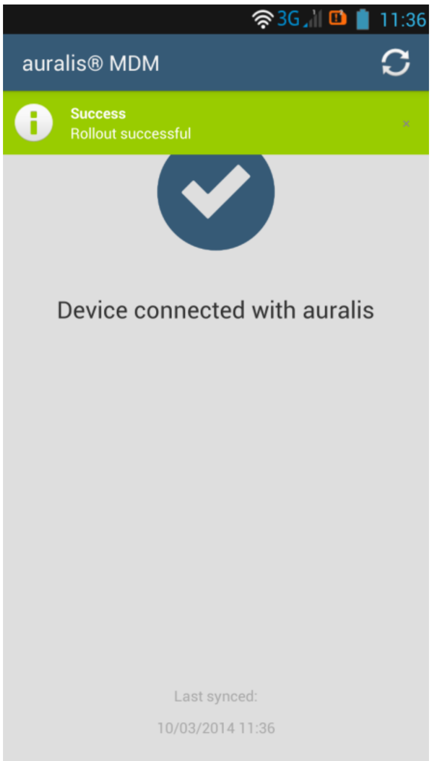
Installing CA-certificate ☑

Logging in ☑

Extract from auralis Profile Service

Type the password to extract the certificates.

••••••



auralis® MDM

Success
Rollout successful

Device connected with auralis

Last synced:
10/03/2014 11:36

Your Android device is now configured successfully. The app show the message ###“Device is connected to auralis”.###

Use the following steps to configure your email account in the Android mail app.

Note

Depending on the Android version of your device a request to configure an new email account will be shown. If this is note the case, please use the instructions in the following paragraph.

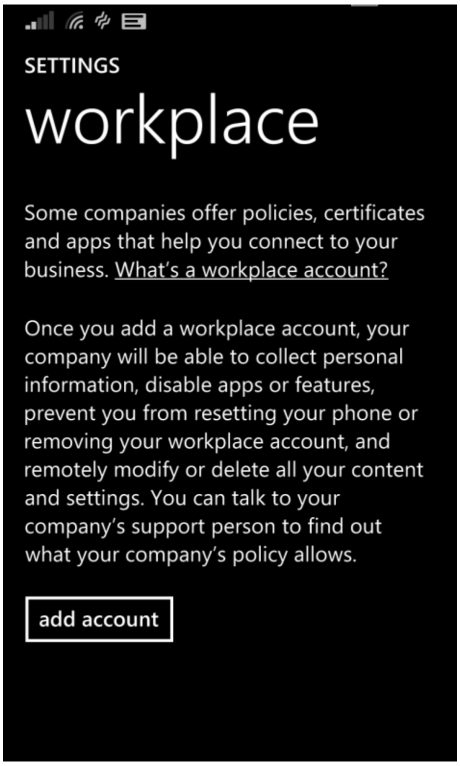
Open the email app of your choice on your device and create a new email account. Use your user credentials and the address for your mail server configured in the auralis system settings.

Note

The email app needs to support client certificate based authentication.

4.3 Windows Phone 8

Open „Settings“ → ###„Enterprise-Apps“###. Press ###„New account“###, enter your rollout credentials and press “connect”. A dialogue requesting additional data will be shown.

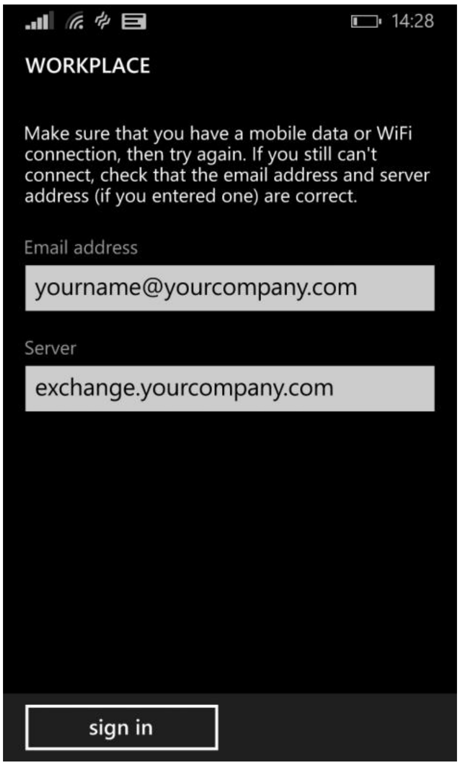


SETTINGS

workplace

Some companies offer policies, certificates and apps that help you connect to your business. What’s a workplace account?

Once you add a workplace account, your company will be able to collect personal information, disable apps or features, prevent you from resetting your phone or removing your workplace account, and remotely modify or delete all your content and settings. You can talk to your company’s support person to find out what your company’s policy allows.



WORKPLACE

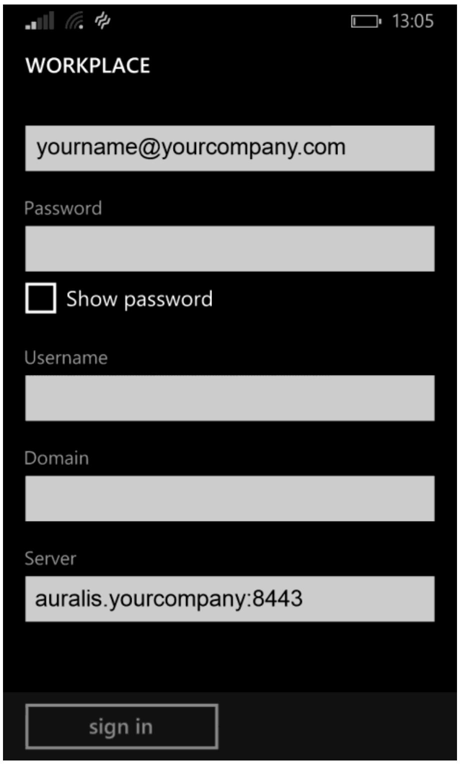
Make sure that you have a mobile data or WiFi connection, then try again. If you still can't connect, check that the email address and server address (if you entered one) are correct.

Email address: yourname@yourcompany.com

Server: exchange.yourcompany.com

Enter the address and port of your auralis server (e.g. auralis.mycompany.com:8443) into „Server“ (see „System configuration“ → „Advanced configuration“) and press ###”connect”###. The default port for auralis is 8443.

When the warning ###”Certificate problem” is raised, please press ###”continue”###. The certificate created by auralis will not be trusted by Windows Phone because it is not signed by any recognized official certificate authority. This does not pose a security risk! On the contrary, as auralis uses its own certificate authority, you are protected better.



yourname@yourcompany.com

Password

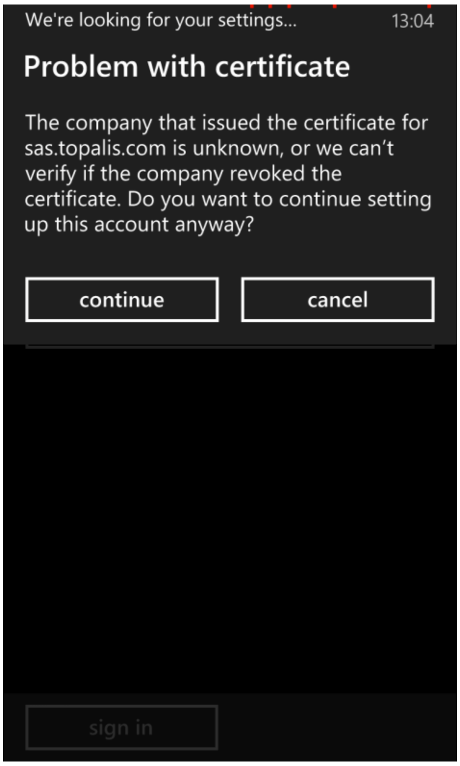
□ Show password

Username

Domain

Server

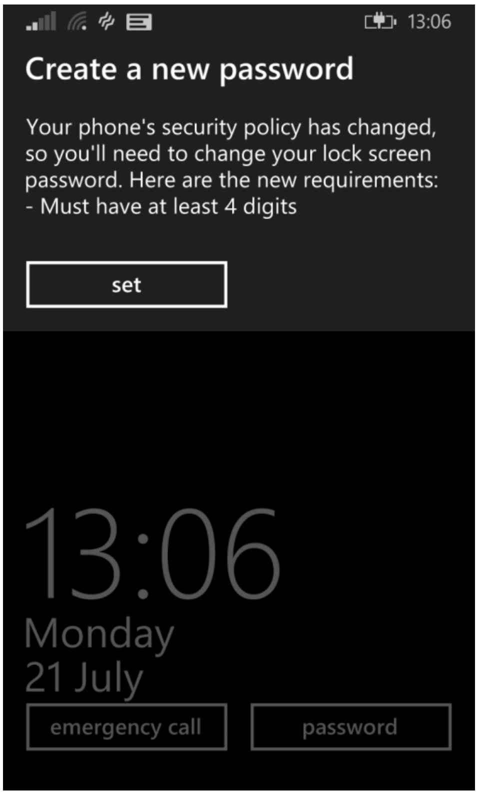
auralis.yourcompany:8443



Problem with certificate

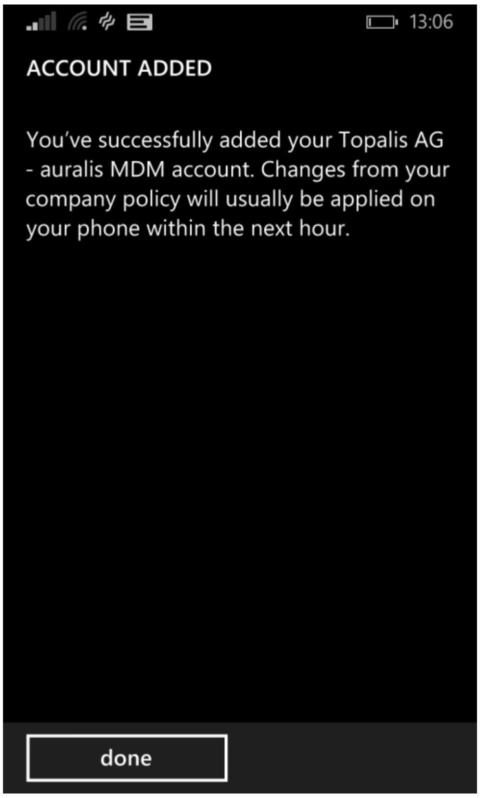
The company that issued the certificate for sas.topalis.com is unknown, or we can't verify if the company revoked the certificate. Do you want to continue setting up this account anyway?

Depending on the security policy the device lock password maybe needed to change. The new password policy will be shown in the message. Press ###”change”### and enter a new password according to the policy. Confirm the password in ###„confirm password“ and press ###”finished”###.



Create a new password

Your phone's security policy has changed, so you'll need to change your lock screen password. Here are the new requirements:
- Must have at least 4 digits

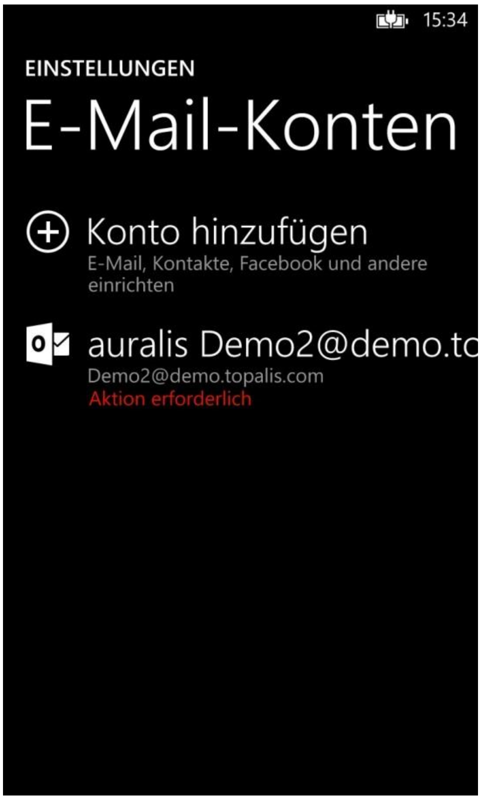


ACCOUNT ADDED

You’ve successfully added your Topalis AG - auralis MDM account. Changes from your company policy will usually be applied on your phone within the next hour.

Acknowledge the message ###„Account added”### by pressing ###„finished“###.

Goto the newly created email account. Please press the button to synchronize your account. Enter the password for your email account and press ###”ok”###. Your Windows Phone is now successfully configured.



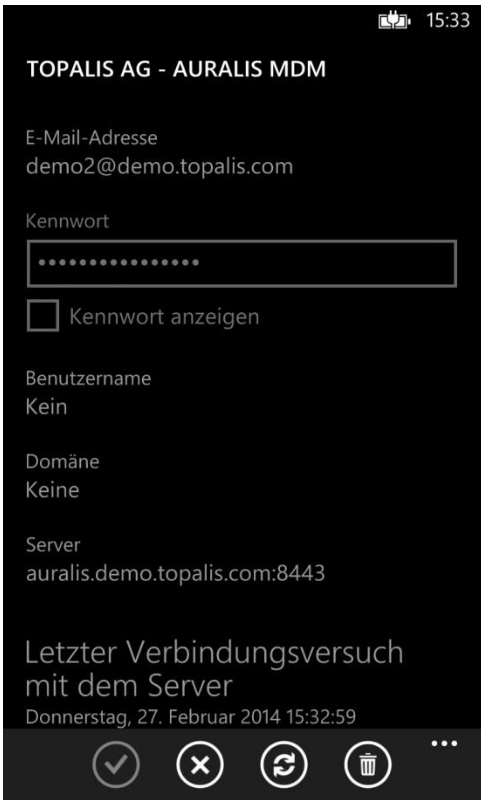
15:34

EINSTELLUNGEN

E-Mail-Konten

⊕ Konto hinzufügen
E-Mail, Kontakte, Facebook und andere einrichten

auralis Demo2@demo.to
Demo2@demo.topalis.com
Aktion erforderlich



15:33

TOPALIS AG - AURALIS MDM

E-Mail-Adresse
demo2@demo.topalis.com

Kennwort
••••••••••••••••

□ Kennwort anzeigen

Benutzername
Kein

Domäne
Keine

Server
auralis.demo.topalis.com:8443

Letzter Verbindungsversuch mit dem Server
Donnerstag, 27. Februar 2014 15:32:59

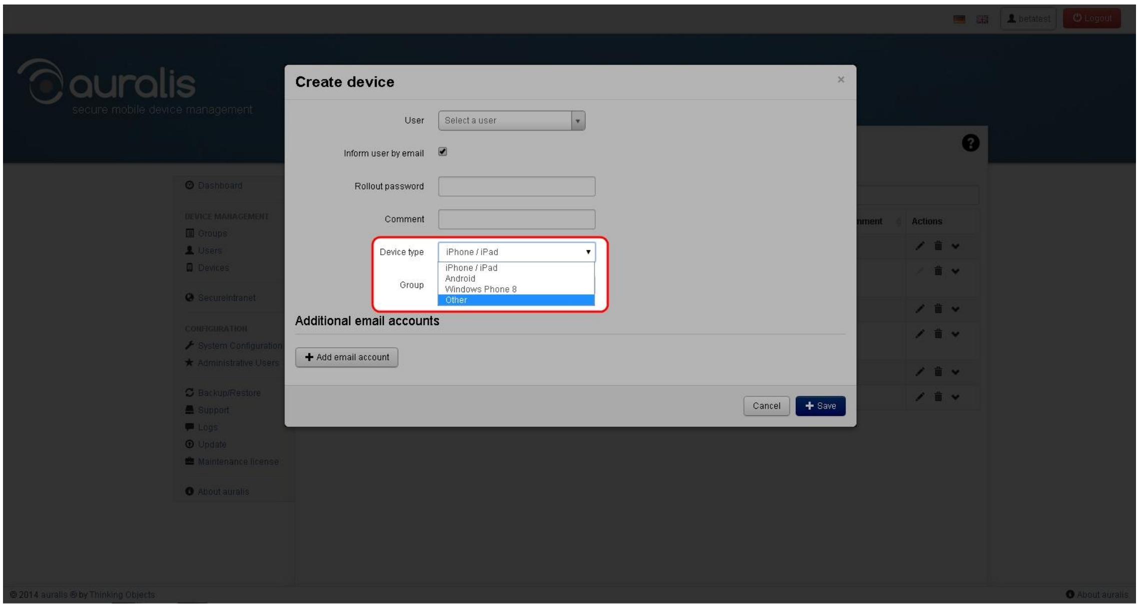
Caution

To reprovision a Windows Phone the second time after a wipe, the device needs tob e reset to factory default. Doing so will delete all user settings and user data on the device.

4.4 Other

To use a device not officially suppoted by auralis, use the following instructions.

Create a new device and select “Other” as the type of your device.



Create device

User: Select a user

Inform user by email: ☑

Rollout password:

Comment:

Device type: iPhone / iPad

Group:

Additional email accounts

The device needs to support the use of client certificates (sometimes also called device certificates). To be able to connect to your email account, the email application also needs to support authenticating with a client certificate. To use SecureIntranet, the browser also needs to support client certificate authentication.

Connect with your device using your rollout credentials.

Note

This step differs from device to device. Wether Auralis will work (properly) with your device cannot be guaranteed. Regarding this topic the manual is not exhaustive.

If the devices was provisioned successfully, you download the device certificate by going to devices and choosing “Download device certificate” from the devices Actions. Depending on the device, the certificate will have been requested and stored already during the provision process. In any other case the device certificate needs to be downloaded and installed manually on the device.

Now you can configure your email account on the device select the device certificate to authenticate.

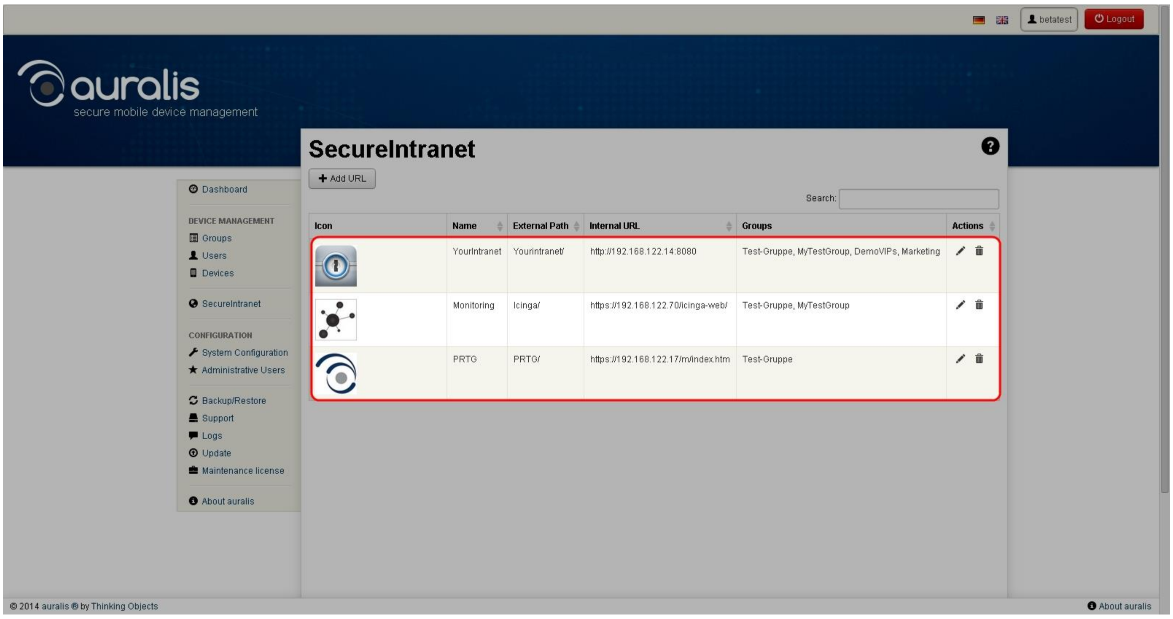
To use SecureIntranet please use a browser supporting client certificates for authentication on your device.

5 Global configurations

Global configurations are SecureIntranet, Webclips, App Management, WiFi and Compliance.

5.1 SecureIntranet

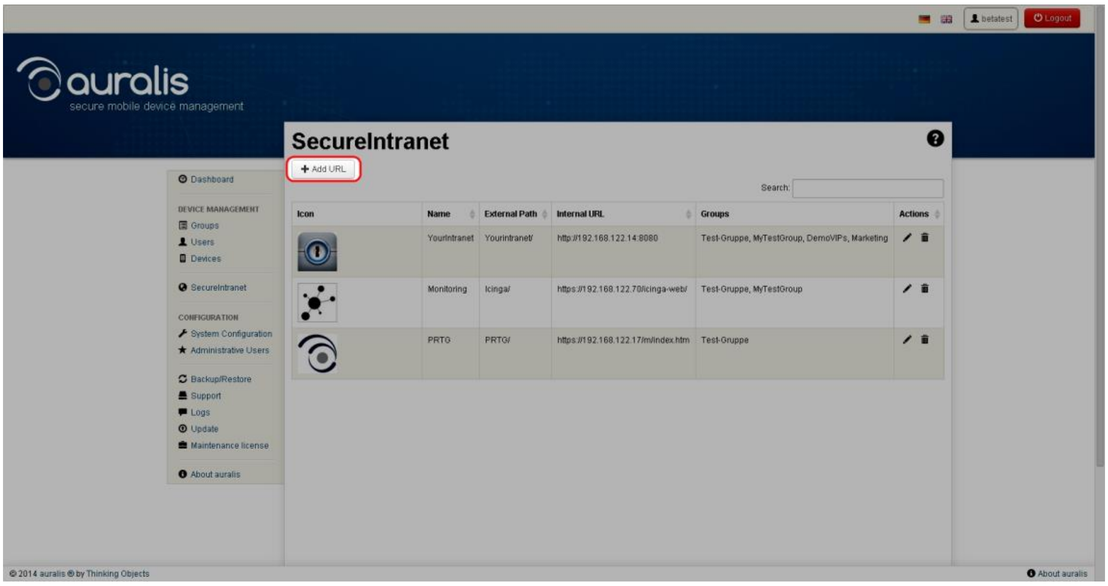
Auralis® SecureIntranet enables secure and easy access to your web enabled intranet applications e.g. Microsoft Sharepoint, CRM-Tools or a ticket request system. You don't need a separate VPN connection, as auralis already provides a SSL secured connection to your corporate network.



Icon	Name	External Path	Internal URL	Groups	Actions
	YourIntranet	Yourintranet/	http://192.168.122.14:8080	Test-Gruppe, MyTestGroup, DemoVIPs, Marketing	
	Monitoring	Icinga/	https://192.168.122.70/icinga-web/	Test-Gruppe, MyTestGroup	
	PRTG	PRTG/	https://192.168.122.17/m/index.htm	Test-Gruppe	

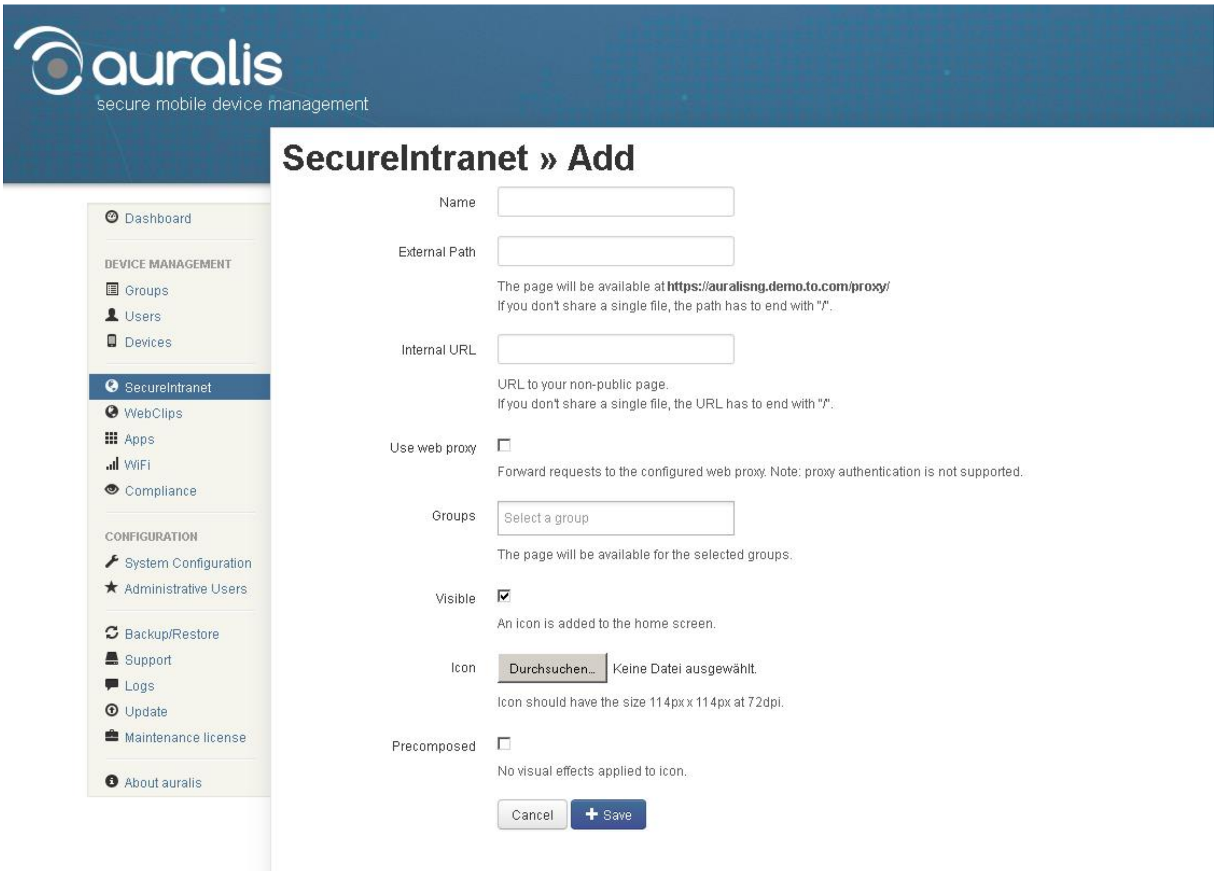
Add URL

To enable access to an intranet URL for provisioned devices, click "Add URL" in the menu "SecureIntranet".



Icon	Name	External Path	Internal URL	Groups	Actions
	YourIntranet	Yourintranet/	http://192.168.122.14:8080	Test-Gruppe, MyTestGroup, DemoVIPs, Marketing	
	Monitoring	Icinga/	https://192.168.122.70/icinga-web/	Test-Gruppe, MyTestGroup	
	PRTG	PRTG/	https://192.168.122.17/m/index.htm	Test-Gruppe	

A form for creating a new entry opens. Enter all required data in the appropriate fields.



SecureIntranet » Add

Name

External Path
The page will be available at **https://auralisng.demo.to.com/proxy/**
If you dont share a single file, the path has to end with "/".

Internal URL
URL to your non-public page.
If you dont share a single file, the URL has to end with "/".

Use web proxy □
Forward requests to the configured web proxy. Note: proxy authentication is not supported.

Groups Select a group
The page will be available for the selected groups.

Visible ☑
An icon is added to the home screen.

Icon Durchsuchen... Keine Datei ausgewählt.
Icon should have the size 114px x 114px at 72dpi.

Precomposed □
No visual effects applied to icon.

Cancel + Save

Name: The name for the new SecureIntranet application.

External Path: The path at which the application will be made available. If you don't share a single data file, the path needs to end with "/".

Internal URL: The URL of the application in your intranet. If you don't share a single data file, the path needs to end with "/".

Proxy: Forward requests to the configured web proxy. Note: proxy authentication is not supported.

Groups: The list of groups for which the application will be made available.

Visible: Check to add an icon to the home screen on the mobile devices.

Icon: Optional individual icon. For optimal display the icon size should be 114px x 114px at 720dpi.

Precomposed: Check to disable device specific visual effects.

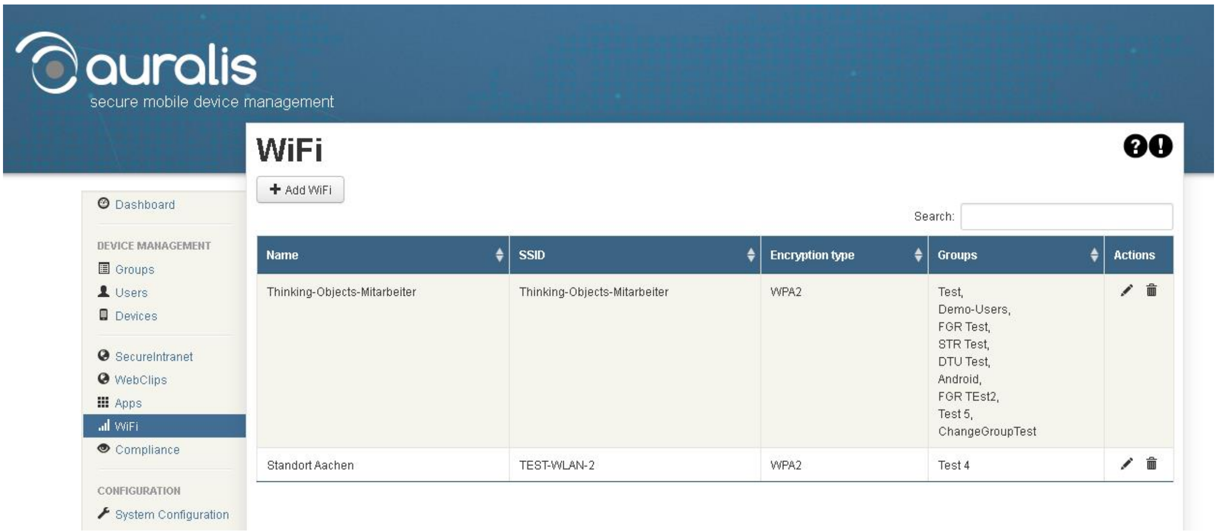
Notes

To use SecureIntranet with an Android device, you need to use a browser supporting certificate based authentication.

At the moment it is unfortunately not possible to access applications published with SecureIntranet on a Windows Phone.

5.2 WiFi

In the central WiFi configuration, you can all networks that you want to store on the smartphone Configure. So you need not hand over user Wi-Fi passwords more. Once a device is within range of a WLAN's known, this automatically connects.



auralis
secure mobile device management

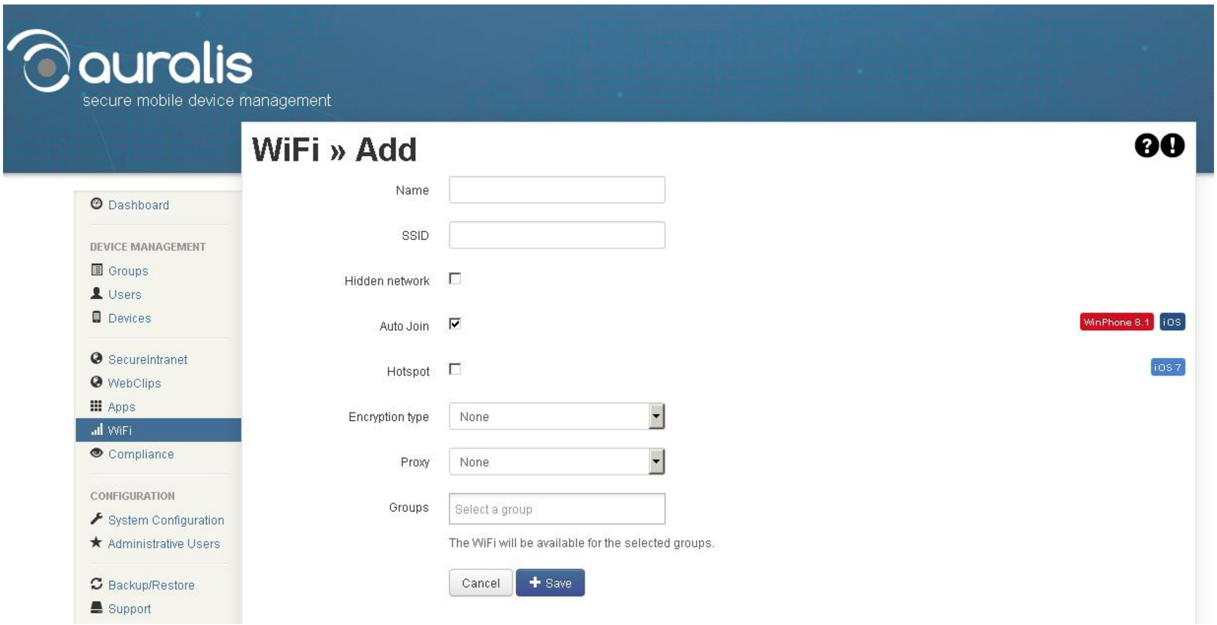
WiFi

Search:

Name	SSID	Encryption type	Groups	Actions
Thinking-Objects-Mitarbeiter	Thinking-Objects-Mitarbeiter	WPA2	Test, Demo-Users, FGR Test, STR Test, DTU Test, Android, FGR TEst2, Test 5, ChangeGroupTest	
Standort Aachen	TEST-WLAN-2	WPA2	Test 4	

To add a new configuration, use the button "CAdd WiFi"

Configuration: In the configuration screen you will find a self-explanatory overview of standard WiFi configurations.



auralis
secure mobile device management

WiFi » Add

Name

SSID

Hidden network □

Auto Join ☑ WinPhone 8.1 iOS

Hotspot □ iOS 7

Encryption type None

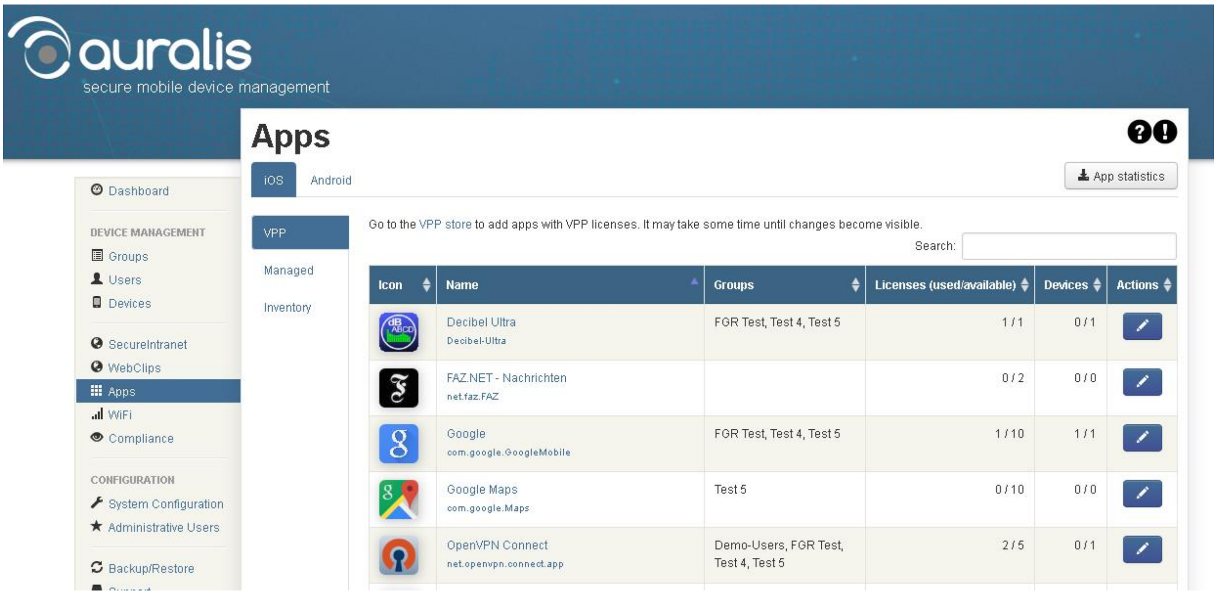
Proxy None

Groups Select a group

The WiFi will be available for the selected groups.

5.3 App Management

The app management offers the possibility to install apps for iOS & Android smartphone, directly from the respective App-Store.



Go to the VPP store to add apps with VPP licenses. It may take some time until changes become visible.

Icon	Name	Groups	Licenses (used/available)	Devices	Actions
	Decibel Ultra Decibel-Ultra	FGR Test, Test 4, Test 5	1 / 1	0 / 1	
	FAZ.NET - Nachrichten net.faz.FAZ		0 / 2	0 / 0	
	Google com.google.GoogleMobile	FGR Test, Test 4, Test 5	1 / 10	1 / 1	
	Google Maps com.google.Maps	Test 5	0 / 10	0 / 0	
	OpenVPN Connect net.openvpn.connect.app	Demo-Users, FGR Test, Test 4, Test 5	2 / 5	0 / 1	

5.3.1 *iOS*

VPP: If you have an Apple VPP Enterprise account and the token is stored in the system configuration, automatically your purchased apps appear at this point. The licenses column shows how many licenses have been acquired and available. In actions column you can edit the settings. Assign groups or see the device list, on which this app is installed.

Managed: Search apps from the Apple App-Store and specify which group this app to be distributed automatically. Alternatively, you can also upload your own apps and distribute them to your smartphones.

Inventory: Here you can see all the apps that are installed on all devices. You can also take apps in automatic management and see which devices have already installed this app.

5.3.2 *Android*

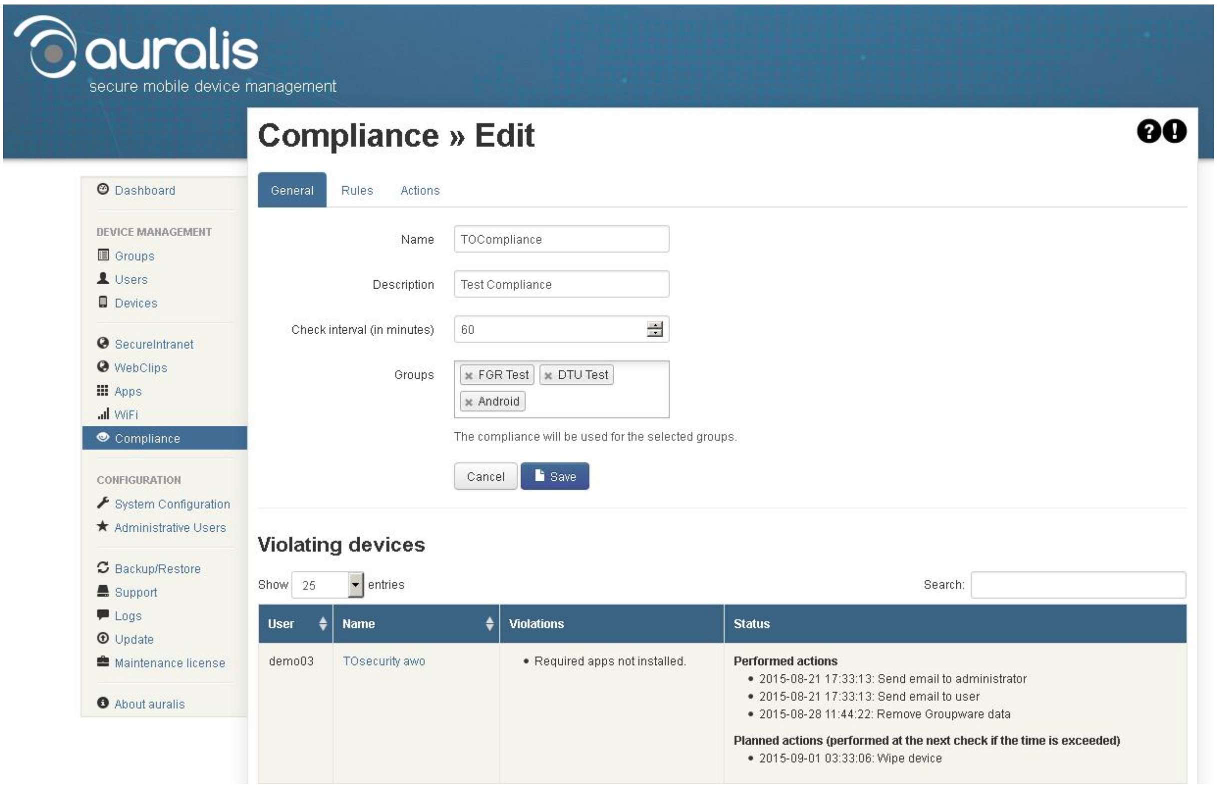
Managed: Search apps from the Google Play Store and specify which group this app to be distributed automatically. Alternatively, you can also upload your own apps and distribute them to your smartphones.

Inventory: Here you can see all the apps that are installed on all devices. You can also take apps in automatic management and see which devices have already installed this app.

System Apps: Here you see all the factory installed Android system apps.

5.4 Compliance

With compliance settings you can define specific rules as your devices must be configured. The devices are polled regularly. If there are violations of these rules, you can carry out certain actions.



Compliance » Edit

Name: TOCompliance

Description: Test Compliance

Check interval (in minutes): 60

Groups: FGR Test, DTU Test, Android

The compliance will be used for the selected groups.

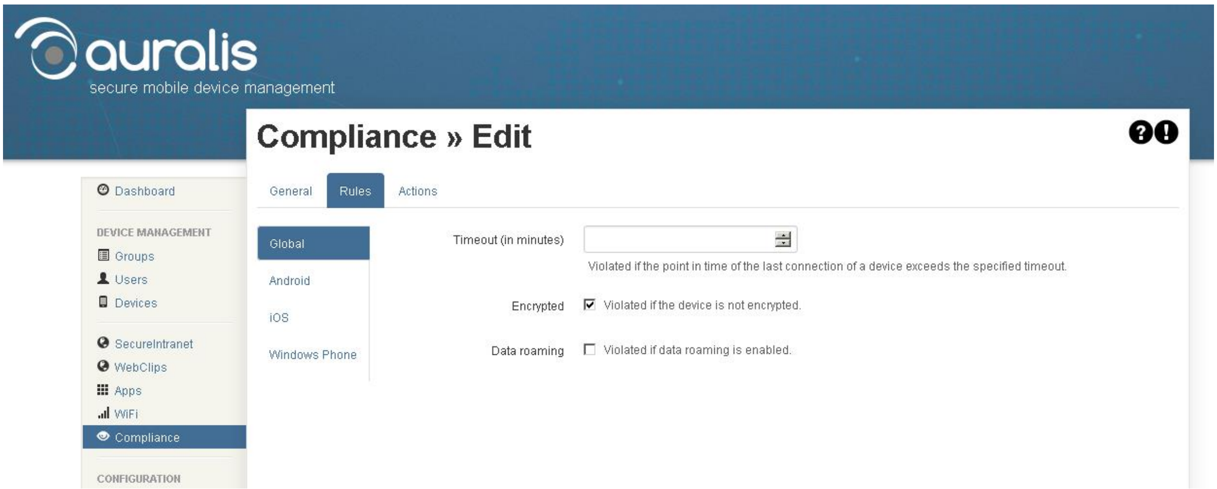
Violating devices

Show 25 entries   Search:

User	Name	Violations	Status
demo03	TOsecurity awo	• Required apps not installed.	**Performed actions** • 2015-08-21 17:33:13: Send email to administrator • 2015-08-21 17:33:13: Send email to user • 2015-08-28 11:44:22: Remove Groupware data **Planned actions (performed at the next check if the time is exceeded)** • 2015-09-01 03:33:06: Wipe device

General: Here you can define the name, description, the test interval and the associated device groups. In an overview you see the devices which violates against the compliance rule. In status column you see the performed and planned actions.

Rules: Define the global, iOS, Android and Windows Phone specific rules.



Compliance » Edit

Timeout (in minutes):

Violated if the point in time of the last connection of a device exceeds the specified timeout.

Encrypted ☑ Violated if the device is not encrypted.

Data roaming □ Violated if data roaming is enabled.

Global:

Timeout: Violated if the point in time of the last connection of a device exceeds the specified timeout.
Encrypted: Violated if the device is not encrypted.
Data Roaming: Violated if data roaming is enabled.

Android:

Minimal OS version: Violated if the installed operating system version is lower.

Maximal OS version: Violated if the installed operating system version is higher.

Non play store apps: Violated if installation of non play store apps is allowed.

Required apps: Violated if a required app is not installed.

Forbidden apps: Violated if a forbidden app is installed.

iOS:

Minimal OS version: Violated if the installed operating system version is lower.

Maximal OS version: Violated if the installed operating system version is higher.

Required apps: Violated if a required app is not installed.

Forbidden apps: Violated if a forbidden app is installed.

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: With the app policy you can deny (blacklist), or allow (whitelist) choosen applications. Applications can be chosen by their GUID or their publisher. In contrast to the other rules the policy is enforced by the device and not verified by auralis.

The usual way to find GUID or a publisher, is on the Windows Phone App Store. The GUIDs are part of the URL to the application. For example, contains the URL

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

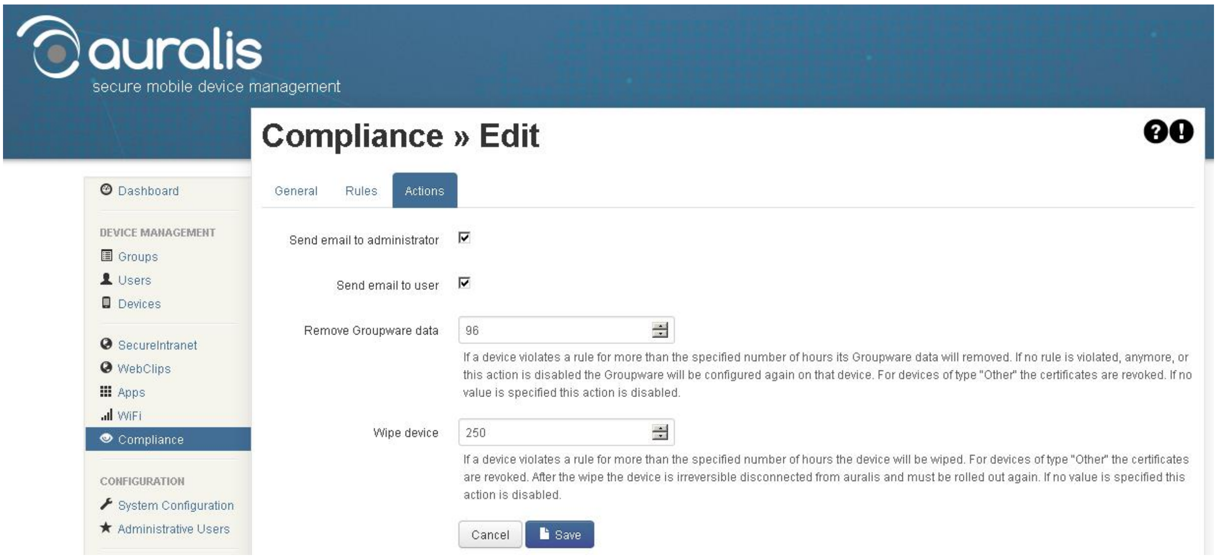
Actions: Bei Regelverstößen können Sie zwischen bestimmten Aktionen auswählen.

Send email to administrator: The administrator receives an email with the violation and the planned actions, if selected.

Send email to user: The user receives an email with the violation and the planned actions, if selected.

Remove Groupware data: The email account will be deleted from the device until the device is brought back to compliance guidelines.

Wipe device: The device is completely deleted from the Mobile Device Management after the defined period of time and must be re-enrolled!



Compliance » Edit

Send email to administrator ☑

Send email to user ☑

Remove Groupware data: 96

If a device violates a rule for more than the specified number of hours its Groupware data will removed. If no rule is violated, anymore, or this action is disabled the Groupware will be configured again on that device. For devices of type "Other" the certificates are revoked. If no value is specified this action is disabled.

Wipe device: 250

If a device violates a rule for more than the specified number of hours the device will be wiped. For devices of type "Other" the certificates are revoked. After the wipe the device is irreversible disconnected from auralis and must be rolled out again. If no value is specified this action is disabled.

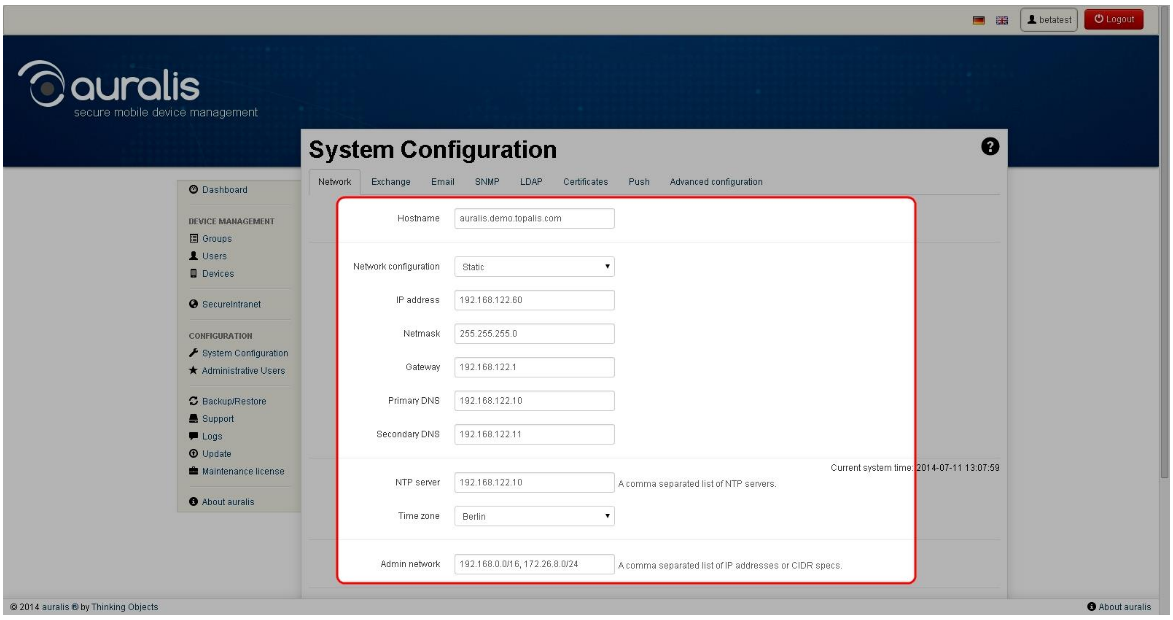
Cancel | Save

6 System Configuration

The system configuration contains all important settings for the configuration of the basic system necessary to integrate auralis into your IT infrastructure.

6.1 Network

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



System Configuration

Hostname: auralis.demo.topalis.com

Network configuration: Static

IP address: 192.168.122.60

Netmask: 255.255.255.0

Gateway: 192.168.122.1

Primary DNS: 192.168.122.10

Secondary DNS: 192.168.122.11

Current system time: 2014-07-11 13:07:59

NTP server: 192.168.122.10 A comma separated list of NTP servers.

Time zone: Berlin

Admin network: 192.168.0.0/16, 172.26.8.0/24 A comma separated list of IP addresses or CIDR specs.

Hostname: The full qualified domain name for auralis.

Note

The hostname needs to have a corresponding DNS A record pointing to the systems IP address.

Network configuration: Static or DHCP. If you choose static, you need to provide additional data for the network interface.

IP address: The ip address assigned to auralis.

Netmask: The netmask used for the interface.

Gateway: The IP address for the network gateway router.

Primary DNS: The IP address of the primary DNS server.

Secondary DNS: The IP address of a secondary DNS server, which is used if the primary server does not respond.

NTP-Server: A comma separated list of network time protocol (NTP) servers used to keep the system time. The current system time at the moment of access to the page is displayed to the right.

Time zonee: The time zone your auralis system is in.

Admin network: A comma separated list of networks in CIDR notation to allow access to the auralis web interface from.

Note

If you cannot access your Auralis system due tot he network configuration, you can alway reset the admin network by selecting „CentOS Configure“ in the boot loader menu upon system startup.

Proxy: If auralis needs to ues a proxy to access the World Wide Web, you need to enter the hostname or IP address and port here.

Proxy username: The username for authenticating to the proxy if necessary.

Proxy password: The password used to authenticate to the proxy if necessary.

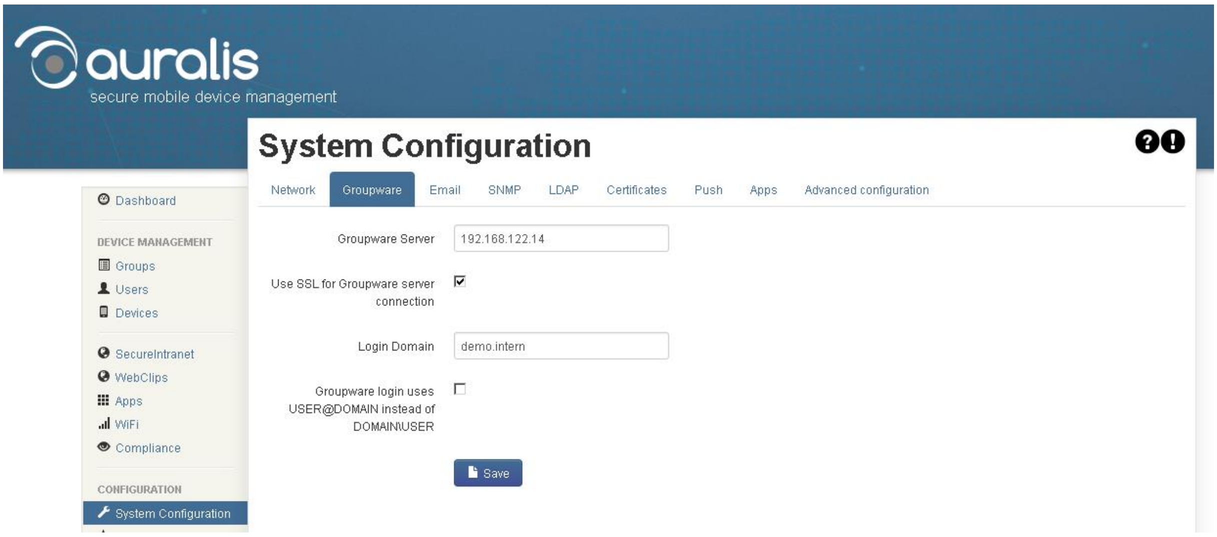
Note

The proxy only needs to be entered if Auralis cannot access web servers directly. The access is needed for the Google Cloud Messaging-Service (see chapter „Push“) and to a get system updates.

To activate the configuration click “Save”.

6.2 Groupware

In this Tab you configure access to your ActiveSync server.



System Configuration

Groupware Server: 192.168.122.14

Use SSL for Groupware server connection: ☑

Login Domain: demo.intern

Groupware login uses USER@DOMAIN instead of DOMAIN\USER: □

Groupware Server: The hostname or IP address of your ActiveSync server.

Use SSL for Groupware server connection: Enable SSL for the connection to protect against wiretapping.

Login Domain: The domain used to logon to the server.

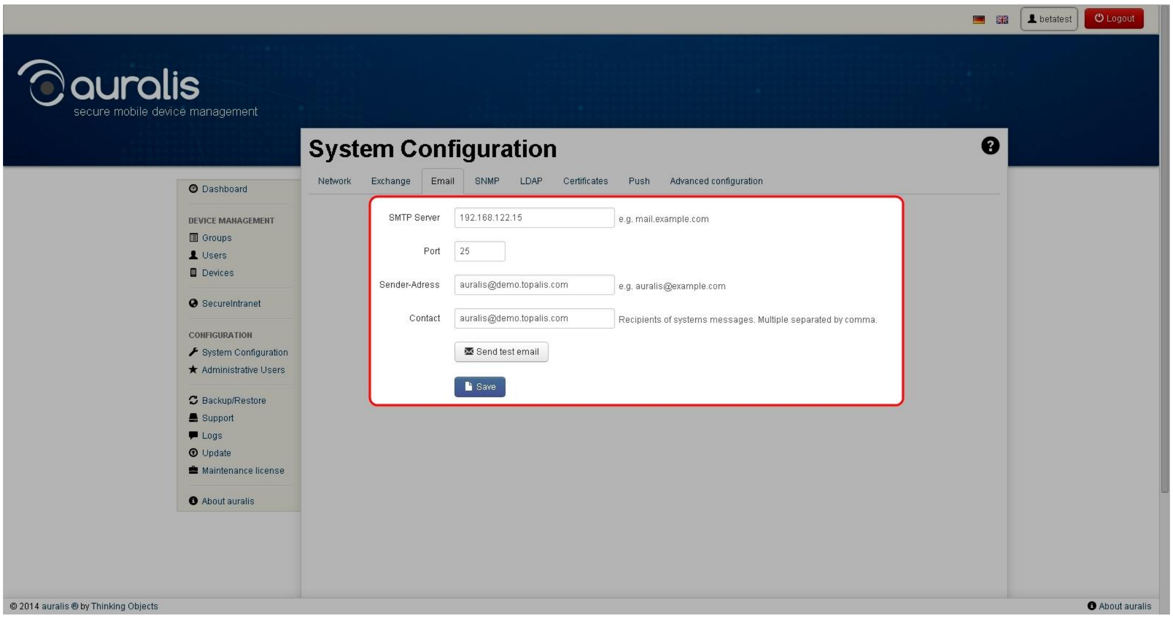
Groupware-Login uses USER@DOMAIN instead of DOMAIN\USER: Choose how auralis sends the username and domain to the server.

To activate the configuration click “Save”.

6.3 Email

All emails sent by auralis are sent to the server and email addresses configured here.

Enter all the necessary information required for sending emails.



System Configuration

SMTP Server: 192.168.122.15 e.g. mail.example.com

Port: 25

Sender-Adress: auralis@demo.topalis.com e.g. auralis@example.com

Contact: auralis@demo.topalis.com Recipients of systems messages. Multiple separated by comma.

SMTP Server: The hostname or IP address of the mail server or relay.

Port: The port of the SMTP server.

Sender-Address: The from address used when sending email. This address is used for all sent emails.

Contact: A comma separated list of email recipients for system email messages.

To test the settings, you can initiate a test email to the list of contacts by clicking on “Send test email”.

To activate the configuration click “Save”.

6.4 SNMP

If enabled detailed system information can be retrieved with SNMP. Beside of standard SNMP data, auralis also provides specific information located beneath OID „1.3.6.1.4.1.4952.3.1.100“ containing the following data (see “TO-auralis-MIB.txt” link on the page):

- Number of recently active devices (access within the last 5 minutes)
- Number of registered devices
- Total email traffic
- Email traffic saved by compression
- License expiration date
- Number of permitted users
- Number of available users

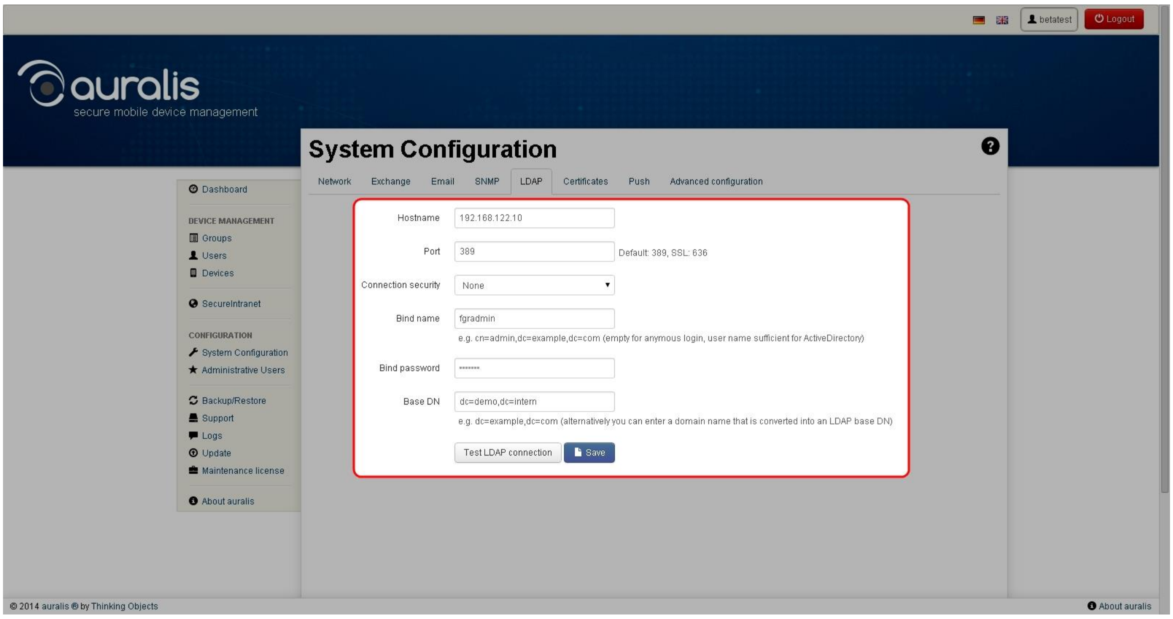
In addition, specific information for each device is provided beneath subentry “1”. Each entry starts with an ascending device id. The following entries are provided for each device:

- Ascending device id
- Last IP address used
- Time of last access
- Device id sent by device
- Comment
- Deactivated yes/no
- Connected (last access within 5 minutes)
- Email traffic

To enable SNMP check the box, enter the SNMP community for read and click “Save”.

6.5 LDAP

In the LDAP settings, you can configure the connection to an LDAP server.



System Configuration

Hostname: 192.168.122.10

Port: 389 Default: 389, SSL: 636

Connection security: None

Bind name: fgradmin

e.g. cn=admin,dc=example,dc=com (empty for anymous login, user name sufficient for ActiveDirectory)

Bind password: ••••••••

Base DN: dc=demo,dc=intern

e.g. dc=example,dc=com (alternatively you can enter a domain name that is converted into an LDAP base DN)

Test LDAP connection | Save

An LDAP server is required, if you want to use the feature for the automatic creation of users.

The following configuration data is required:

Hostname: The hostname or IP address of the LDAP server.

Port: The port of the LDAP server. The default is to use port 389 (SSL: 636).

Connection security: None, SSL or TLS.

Bind name: The name used to logon to the LDAP server.

Bind password: The password used to authenticate to the LDAP server.

Base DN: The distinguished name (DN) used as the base for searches. You can also simply enter a domain name which will be converted to the corresponding DN.

To test the connection prior to saving it, click on “Test LDAP connection”. If the connection was successful, you will get a message “Successfully connected to LDAP directory”, if not you will get an error message giving details about the problem.

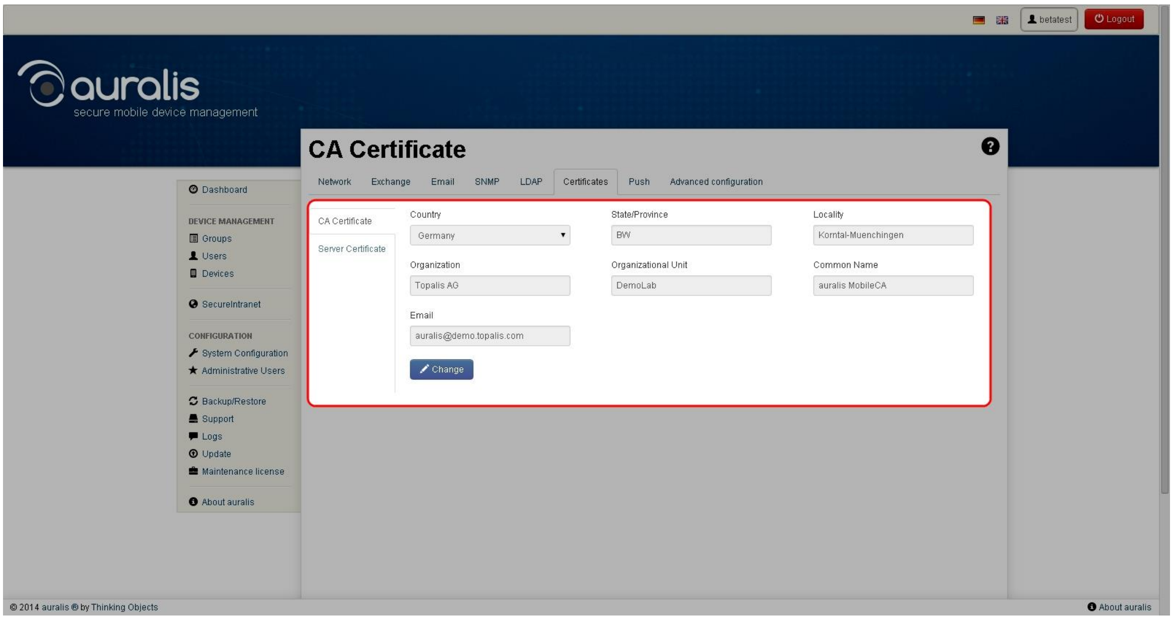
To save and activate the connection, click “Save”.

6.6 Certificates

CA Certificate

The certificate authority (CA) certificate is used to sign the server certificate and the client side certificates. In addition it gets installed on every device, to verify any certificates sent by auralis.

To protect against changes, the details of the CA certificate are set read-only. To edit the data, click the "Change" button.



CA Certificate

Country: Germany

State/Province: BW

Locality: Korntal-Muenchingen

Organization: Topalis AG

Organizational Unit: DemoLab

Common Name: auralis MobileCA

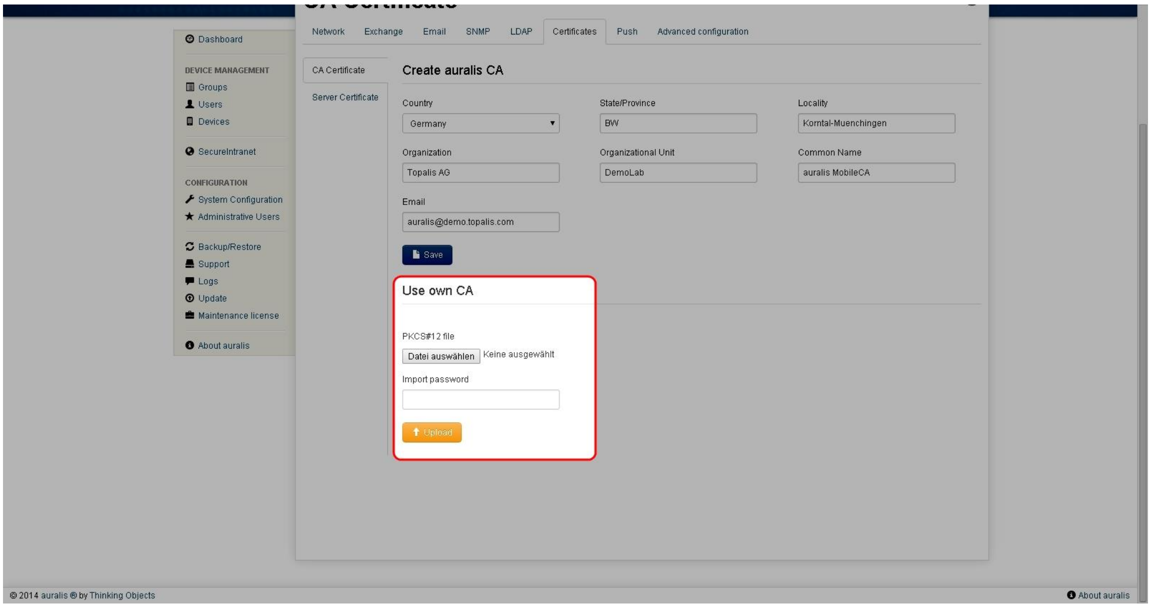
Email: auralis@demo.topalis.com

When you click “Save”, a new CA certificate will be generated.

Caution

Any changes to the CA certifcate lead to all devices loosing the trust relationship with the server. After a change to the CA certificate, alle devices need to be reprovisioned.

If you are using an existing CA, you can also upload your own CA certificate.



Create auralis CA

Country: Germany

State/Province: BW

Locality: Korntal-Muenchingen

Organization: Topalis AG

Organizational Unit: DemoLab

Common Name: auralis MobileCA

Email: auralis@demo.topalis.com

Use own CA

PKCS#12 file: Keine ausgewählt

Import password

© 2014 auralis ® by Thinking Objects

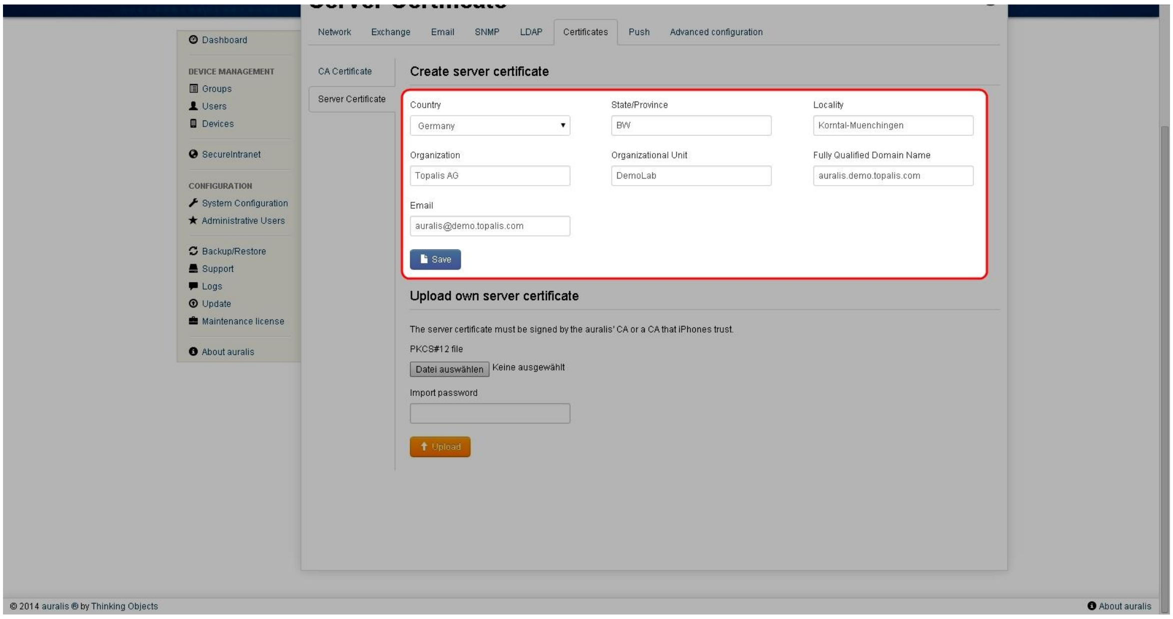
Browse for the file and choose the appropriate CA certificate, enter the password for the certificate and click “Upload”, to install the certificate. The certificate needs to be in PKCS#12 formats.

Caution

Any changes to the CA certifcate lead to all devices loosing the trust relationship with the server. After a change to the CA certificate, alle devices need to be reprovisioned.

Server certificate

The server certificate is used by auralis, to authenticate to the connected devices. This certificate is signed by the CA and can therefore be changed without having to reconfigure all devices. To edit the entries in the certificate, click the "Change" button. You can now change the information in the server's certificate. Then click on "Save" to generate a new certificate with the entered data.



Create server certificate

Country: Germany
State/Province: BW
Locality: Korntal-Muenchingen
Organization: Topalis AG
Organizational Unit: DemoLab
Fully Qualified Domain Name: auralis.demo.topalis.com
Email: auralis@demo.topalis.com

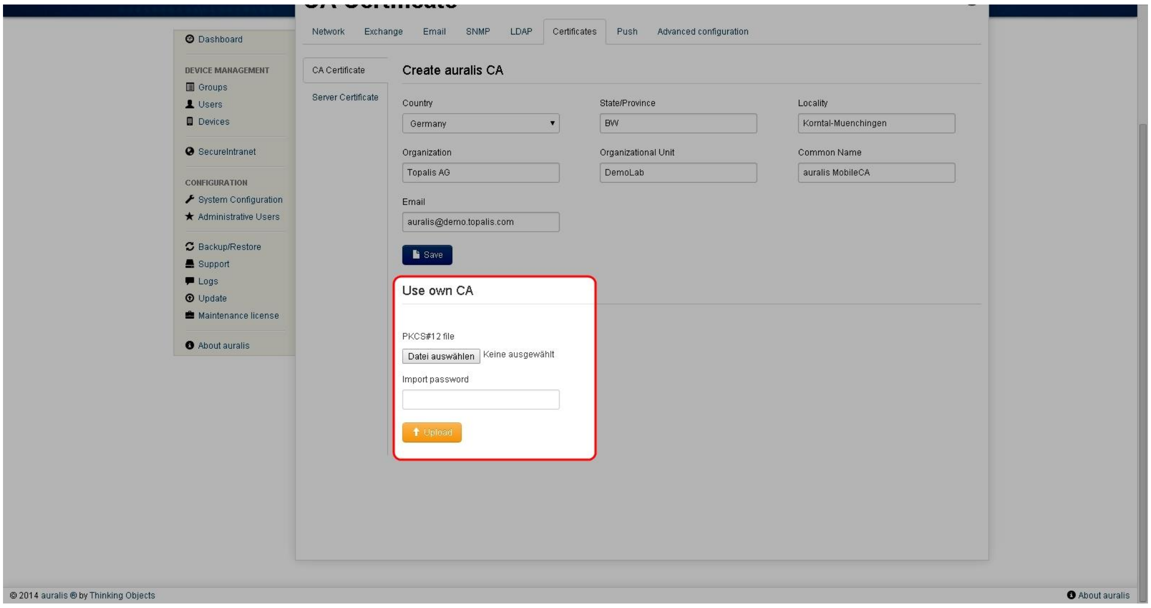
Upload own server certificate

The server certificate must be signed by the auralis' CA or a CA that iPhones trust.

PKCS#12 file: Keine ausgewählt

Import password

To upload your own certificate, select the certificate you want to upload, enter the password for the certificate, and click "Upload". Make sure that all mobile devices trust the uploaded certificate.



Create auralis CA

Country: Germany
State/Province: BW
Locality: Korntal-Muenchingen
Organization: Topalis AG
Organizational Unit: DemoLab
Common Name: auralis MobileCA
Email: auralis@demo.topalis.com

Use own CA

PKCS#12 file: Keine ausgewählt

Import password

6.7 Push services

In the menu “Push” you can configure the use of push services from Apple (Apple push notification service [APNS]) and Google (Google cloud Messaging [GCM]).

A push message is sent to the push services, if you created a new MDM command for a device. This message contains the push token of the particular device. The push service identifies the corresponding device and transmits the message to it. The device then connects to auralis to retrieve the available commands. The push messages sent by auralis only are used to request device to connect to auralis and contain no user data.

Android and iOS devices maintain a permanent connection to their push service to receive push messages with minimum delay. A similar system does not exist for Windows phone at the moment - devices with this system poll commands from auralis at regular intervals. Therefore a delay is to be expected before an MDM command reaches the device. The poll can be initiated manually by going to "settings → company apps" and select the Exchange account and pressing the button to synchronize the account.

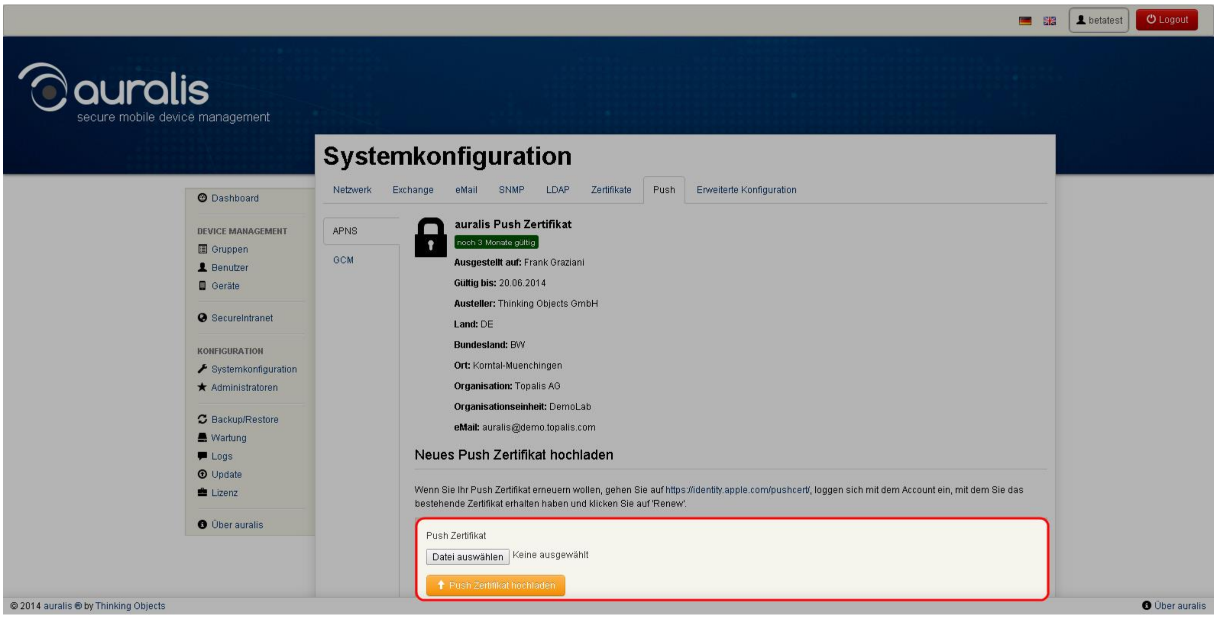
If an an Android or iOS device receives no push messages, e.g. due to a failure of the push service, it will not retrieve any MDM commands from auralis. In the auralis app for Android, the retrieval of available commands can be triggered manually in this case. To do so, open the auralis app and press the button in the upper right corner to synchronize the device with auralis.

6.7.1 Apple push service

If you already imported an Apple push certificate into auralis, all information about the certificate is displayed by clicking on the menu "Apple Push". On top auralis shows, how long the certificate is valid.

To send messages with the Apple push notification service, you will need a push certificate signed by Apple. To obtain a new certificate from Apple or to renew your existing certificate, please visit this page https://identity.apple.com/pushcert/ and follow the instructions there.

To upload a new certificate, select the corresponding file and then click “Upload push certificate” to upload the file to auralis. The push certificate is then installed and used for all iOS devices.



auralis Push Zertifikat

noch 3 Monate gültig

Ausgestellt auf: Frank Graziani

Gültig bis: 20.06.2014

Austeller: Thinking Objects GmbH

Land: DE

Bundesland: BW

Ort: Korntal-Muenchingen

Organisation: Topalis AG

Organisationseinheit: DemoLab

eMail: auralis@demo.topalis.com

Neues Push Zertifikat hochladen

Wenn Sie Ihr Push Zertifikat erneuern wollen, gehen Sie auf https://identity.apple.com/pushcert/, loggen sich mit dem Account ein, mit dem Sie das bestehende Zertifikat erhalten haben und klicken Sie auf 'Renew'.

Push Zertifikat

Datei auswählen Keine ausgewählt

Push Zertifikat hochladen

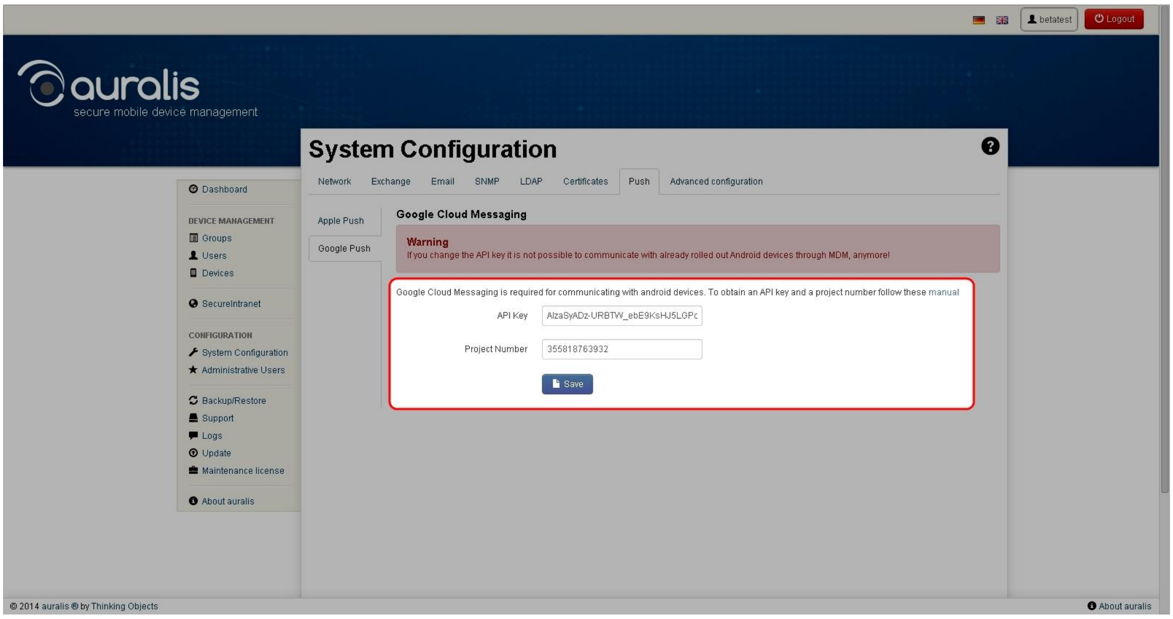
© 2014 auralis ® by Thinking Objects

Über auralis

6.7.2 Google push service

To access Google cloud messaging, the push service from Google, an API key and a project number is needed. You can request this on Google, as described in the web interface.

Enter the API key and the project number in the appropriate input fields and click “Save” to update the configuration.



System Configuration

Google Cloud Messaging

Warning
If you change the API key it is not possible to communicate with already rolled out Android devices through MDM, anymore!

Google Cloud Messaging is required for communicating with android devices. To obtain an API key and a project number follow these manual

API Key: AIzaSyADz-URBTW_ebE9KsHJ5LGPc

Project Number: 355818763932

© 2014 auralis ® by Thinking Objects

Caution

If you change the API key, communication to already configured Android devices with MDM is no longer possible.

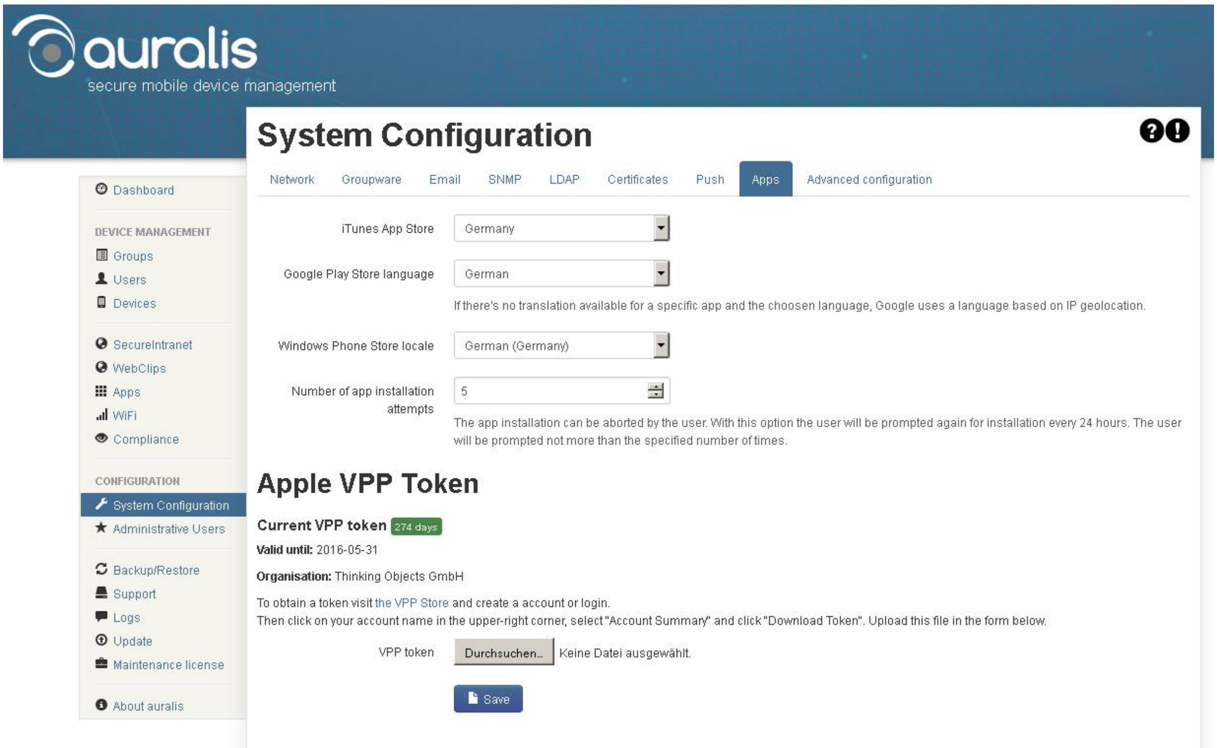
6.8 Apps

Here you can you can choose the regional app sores und upload your Apple VPP token.

To register for the Apple VPP program please visit the following website and follow the instructions.

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

After successful registration, you can download the token in "Account Summary" and import in auralis. About Apple VPP purchased apps now appear automatically in the global app configuration.



System Configuration

iTunes App Store: Germany

Google Play Store language: German

If there's no translation available for a specific app and the choosen language, Google uses a language based on IP geolocation.

Windows Phone Store locale: German (Germany)

Number of app installation attempts: 5

The app installation can be aborted by the user. With this option the user will be prompted again for installation every 24 hours. The user will be prompted not more than the specified number of times.

Apple VPP Token

Current VPP token 274 days

Valid until: 2016-05-31

Organisation: Thinking Objects GmbH

To obtain a token visit the VPP Store and create a account or login.
Then click on your account name in the upper-right corner, select "Account Summary" and click "Download Token". Upload this file in the form below.

VPP token: Durchsuchen... Keine Datei ausgewählt.

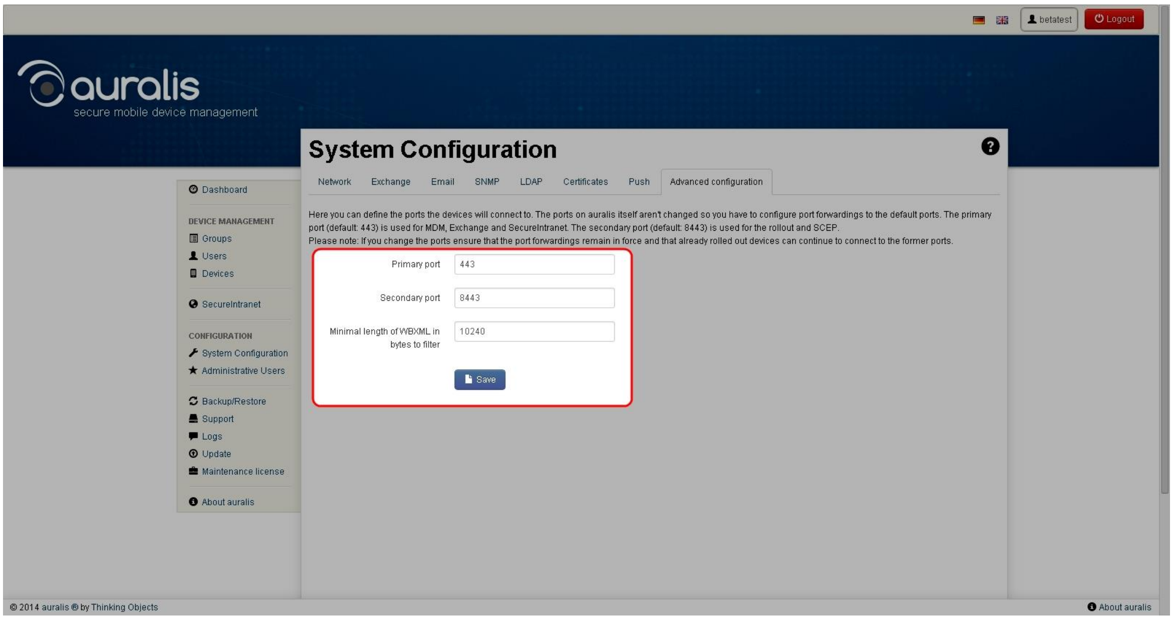
Save

6.9 Advanced configuration

In the advanced configuration, you can define the ports to which the devices connect. The ports used by auralis itself are not changed, so you have to use port forwarding of the configured ports to the default ports. The primary port (default: 443) is used for the mobile device management (MDM), Exchange, and SecureIntranet. The secondary port (default: 8443) is used for the rollout and the simple certificate enrollment Protocol (SCEP).

Note

Make sure to keep the existing port forwarding too in case of changes to ensure connectivity for already provisioned devices.



System Configuration

Here you can define the ports the devices will connect to. The ports on auralis itself aren't changed so you have to configure port forwardings to the default ports. The primary port (default: 443) is used for MDM, Exchange and SecureIntranet. The secondary port (default: 8443) is used for the rollout and SCEP.
Please note: If you change the ports ensure that the port forwardings remain in force and that already rolled out devices can continue to connect to the former ports.

Primary port: 443

Secondary port: 8443

Minimal length of WBXML in bytes to filter: 10240

The field "Minimum length of WBXML in bytes to filter", specifies which size of ActiveSync messages are processed by auralis. The default is 10240 bytes. Smaller ActiveSync messages are routed through unchanged.

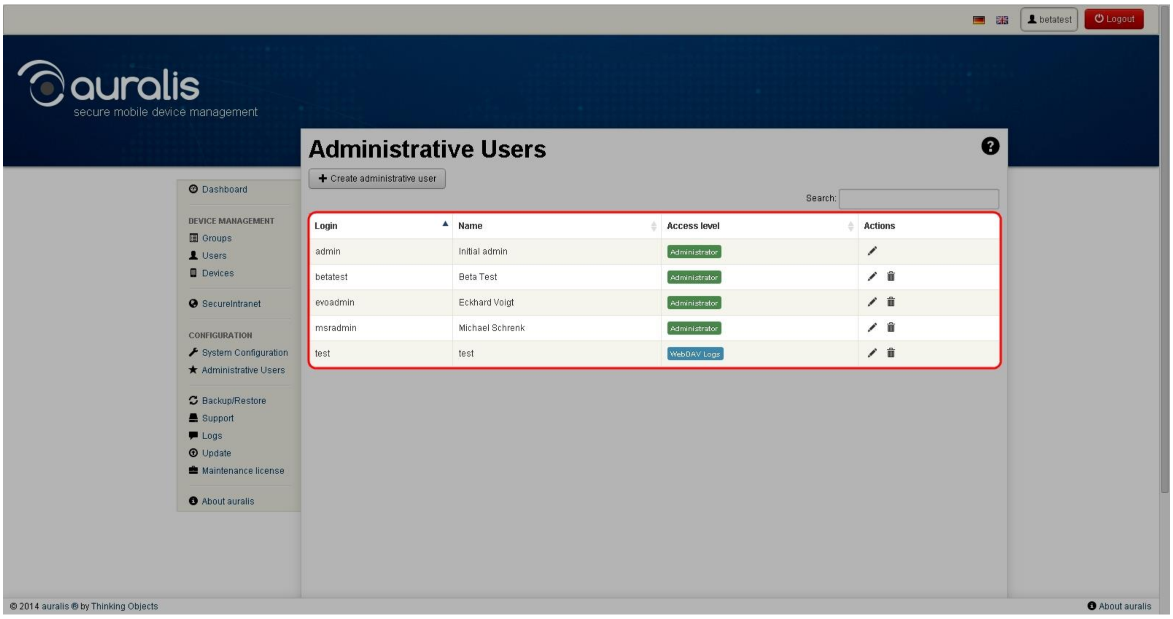
Note

If a lot of non-compressible data is send through Auralis, you can raise the minimum length above the size of the regarding documents to enhance processing performance.

Click “Save” to apply any changes or leave the page to discard them.

7 Administrative Users

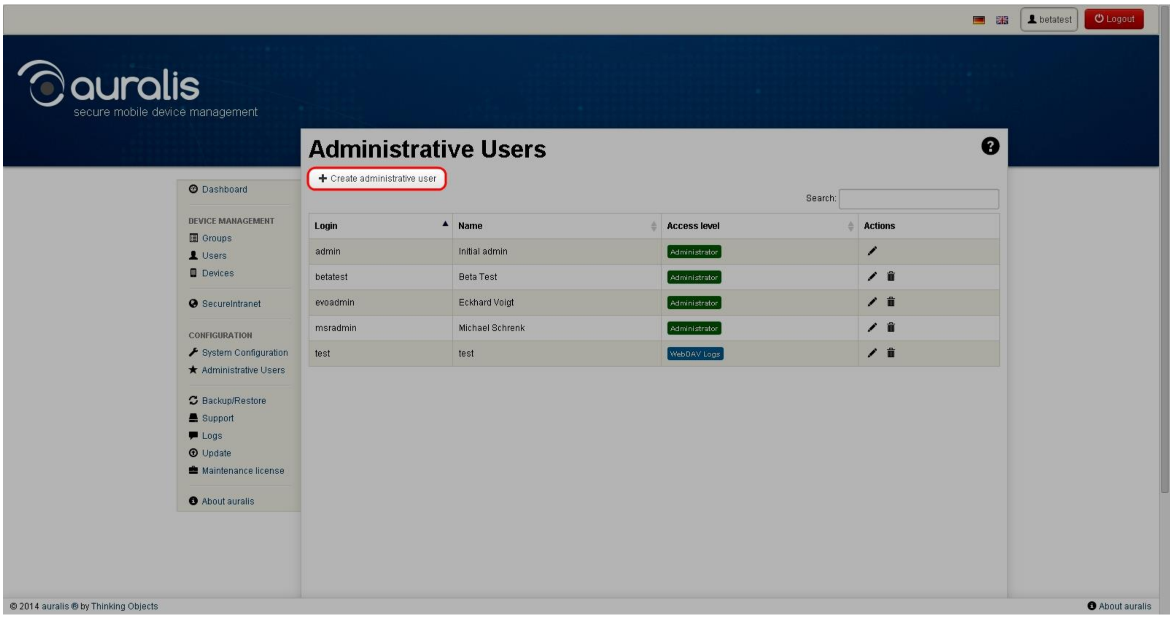
To manage users with administrative privileges click on “Administrative Users”. A list of admin users is shown. You can create new users and edit or delete existing users by clicking on the pen or garbage can icon.



Login	Name	Access level	Actions
admin	Initial admin	Administrator	✎
betatest	Beta Test	Administrator	✎ 🗑
evoadmin	Eckhard Voigt	Administrator	✎ 🗑
msradmin	Michael Schrenk	Administrator	✎ 🗑
test	test	WebDAV Logs	✎ 🗑

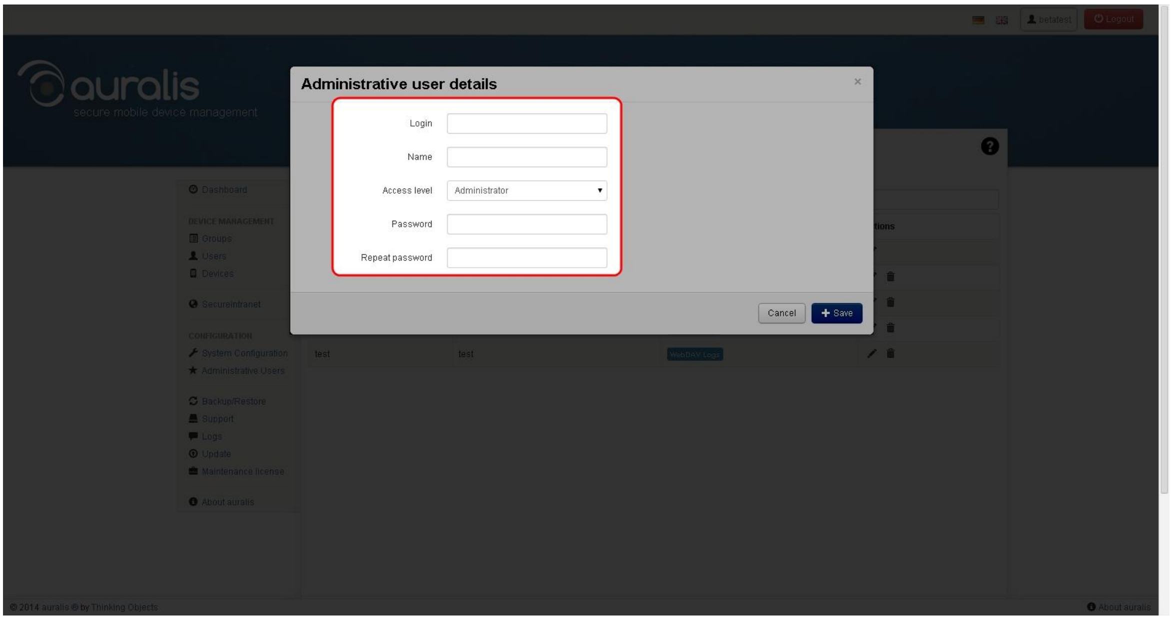
Create administrative user

To create a new admin user, click on “Create administrative user”.



Login	Name	Access level	Actions
admin	Initial admin	Administrator	✎
betatest	Beta Test	Administrator	✎ 🗑
evoadmin	Eckhard Voigt	Administrator	✎ 🗑
msradmin	Michael Schrenk	Administrator	✎ 🗑
test	test	WebDAV Logs	✎ 🗑

Enter the required data and click “Save”.



Administrative user details

Login

Name

Access level: Administrator

Password

Repeat password

Login: The name with which the user can logon to auralis as an admin.

Name: The complete name of the user for identification.

Access Level: Specify the access rights for the user.

Administrator: The user has full access to all settings.

Supporter: The user has limited access to the settings.

WebDAV Logs: The user is only allowed to access the system logs using WebDAV.

Password: The password for the user.

Repeat password: Confirmation of the password to detect typing errors.

Click "Save" to create the administrator or on "Cancel" to discard the entered data.

The account "admin" with the name "Initial Admin" is the default account and cannot be deleted to ensure there is always at least one admin account.

8 Backup / Restore

Backup of the configuration

Configuration Backup allows you to make a backup copy of the system settings. The backup requires a strong password for protection. The password requirements are listed on the page. The password needs to be repeated to avoid typing errors. Click on “Backup” to start the backup. The backup file will be automatically downloaded.

Restore

Note

Backup files can only be restored tot he same version of Auralis.

To restore a previous backup, click on “Select file” and select the backup file. Enter the password you used to create the backup file in the “Password” field and click “Restore”. The backup will now be restored.

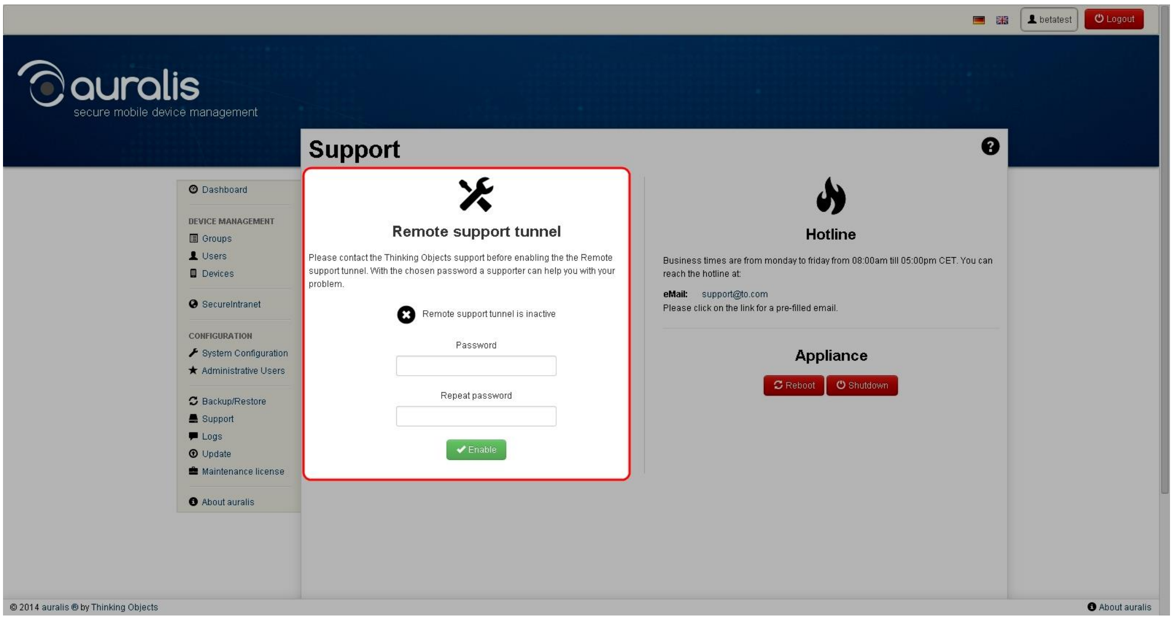
Caution

All changes made since the backup are lost upon restore.

9 Support

Remote support tunnel

Using the remote support tunnel, you can allow access to your system for the Thinking Objects hotline. When activated, encrypted password protected access is allowed from the IP address of the Thinking Objects hotline. With this connection enabled the hotline can analyze the system and solve problems. When the tunnel is deactivated, no access to your system is possible.



Support

Remote support tunnel

Please contact the Thinking Objects support before enabling the the Remote support tunnel. With the chosen password a supporter can help you with your problem.

☒ Remote support tunnel is inactive

Password

Repeat password

✓ Enable

Hotline

Business times are from monday to friday from 08:00am till 05:00pm CET. You can reach the hotline at:

eMail: support@to.com
Please click on the link for a pre-filled email.

Appliance

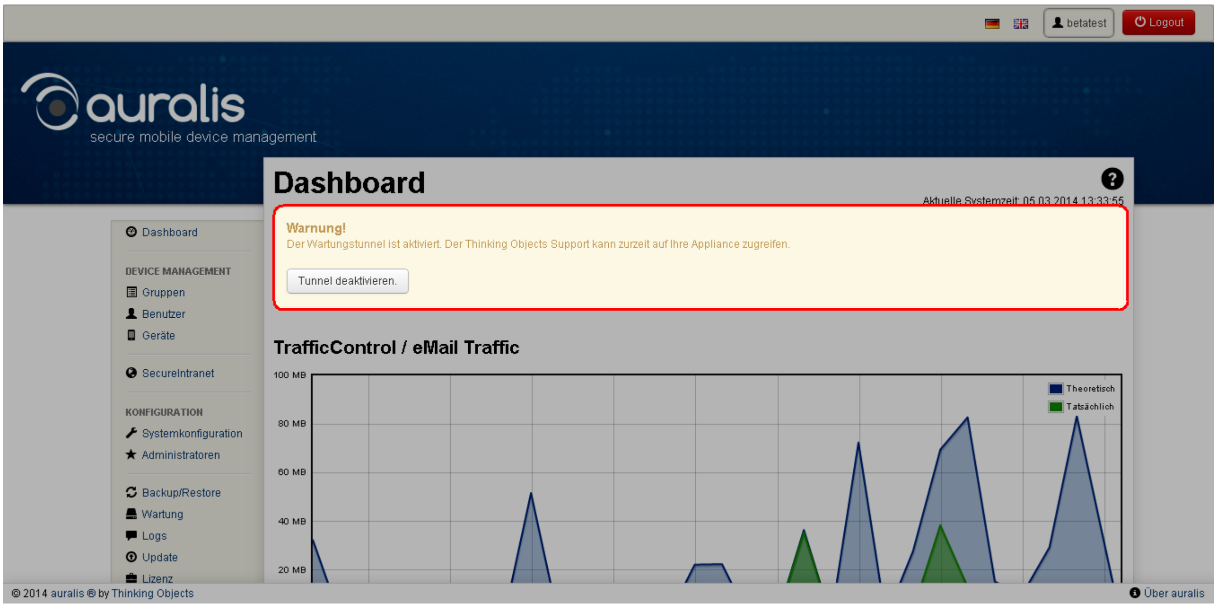
Reboot Shutdown

Please contact the Thinking Objects hotline prior to activating the remote support tunnel. Please choose a strong password and share this with the Thinking Objects hotline upon request to allow access. Click enable to activate.

Note

The hotline can only access your system after you shared the password with them. Access is only possible from the Thinking Objects network.

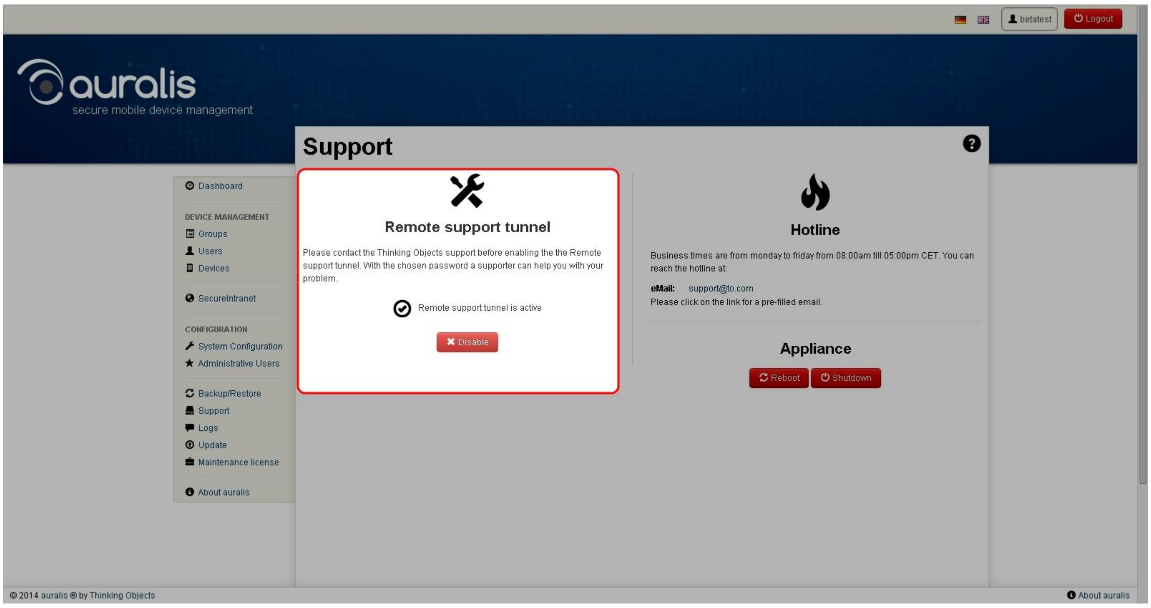
When the remote support tunnel is enabled, auralis will display a warning on the dashboard.



Warnung!
Der Wartungstunnel ist aktiviert. Der Thinking Objects Support kann zurzeit auf Ihre Appliance zugreifen.

Tunnel deaktivieren.

You can disable the remote support tunnel at any time by clicking on the “deactivate tunnel” button shown there, which will take you to the Support menu. Click “Disable” in the Support menu to stop deactivate the remote maintenance tunnel.



Please contact the Thinking Objects support before enabling the the Remote support tunnel. With the chosen password a supporter can help you with your problem.

Remote support tunnel is active

Disable

Business times are from monday to friday from 08:00am till 05:00pm CET. You can reach the hotline at:

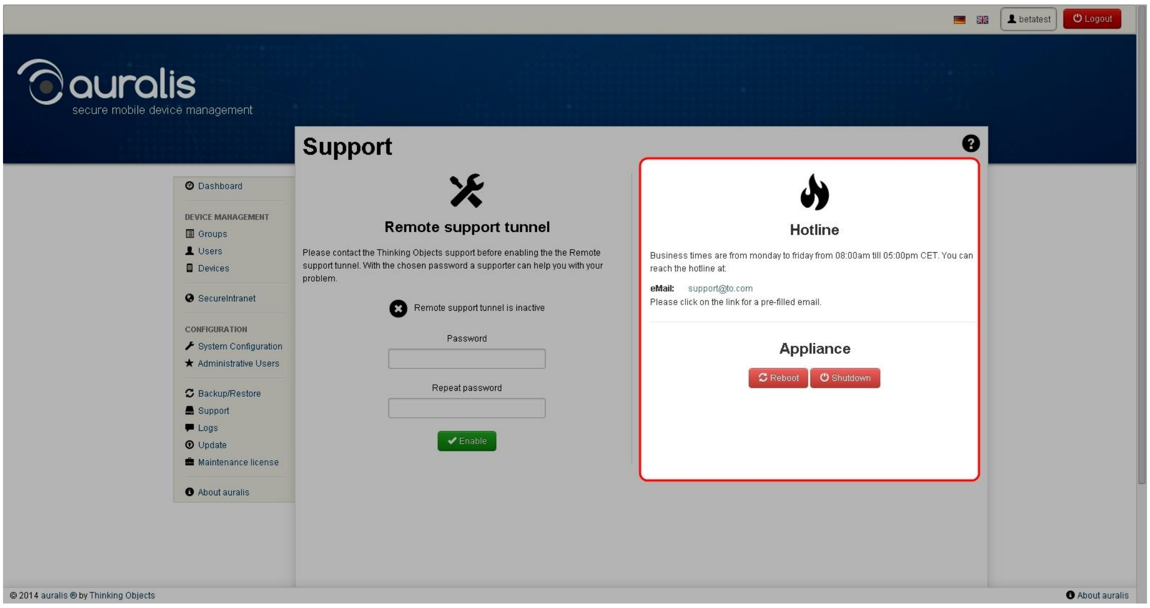
eMail: support@to.com
Please click on the link for a pre-filled email.

Hotline

This shows the service hours of the Thinking Objects Hotline. You can also send an email. When you clik on the email ink, your email client will open a new email to the Hotline, already containing basic information about your system.

Appliance

Here you can reboot or shutdown the appliance. Shutdown will stop all services and then halt the system. Reboot will stop all services and then reboot the system.



Please contact the Thinking Objects support before enabling the the Remote support tunnel. With the chosen password a supporter can help you with your problem.

Remote support tunnel is inactive

Business times are from monday to friday from 08:00am till 05:00pm CET. You can reach the hotline at:

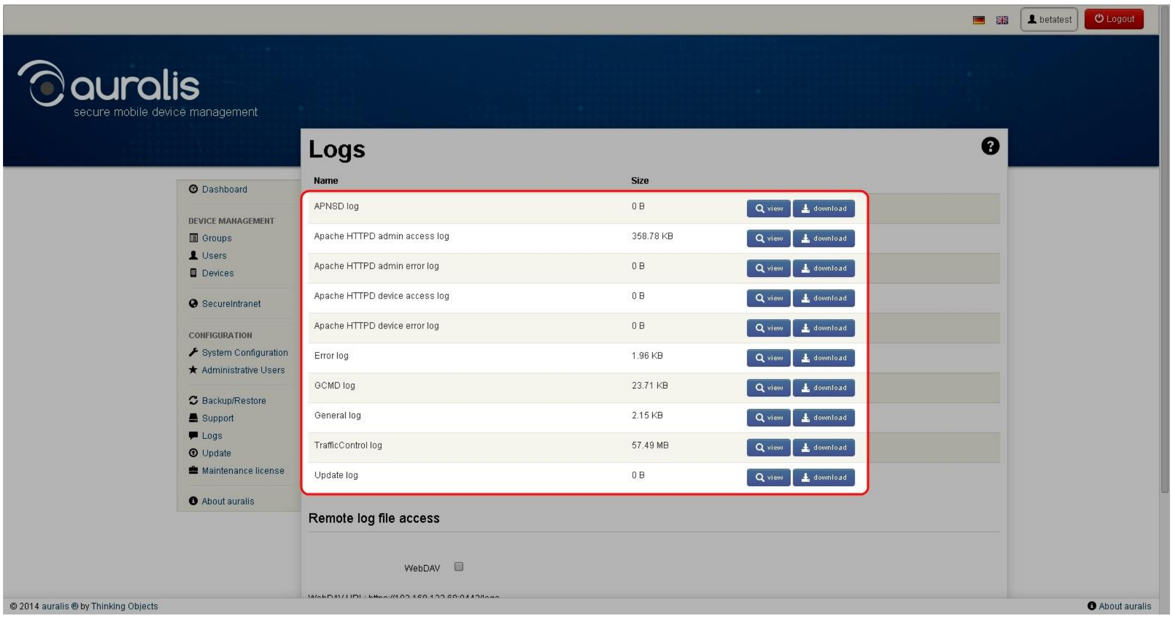
eMail: support@to.com

Please click on the link for a pre-filled email.

10 Logs

To view a log file, click on view. You can then view the log file in a new browser tab. To update the view in real time, activate refresh automatically in the upper right corner. You can also filter the log for specific events. For this purpose enter a filter term in the Filter field. The matched rows are displayed with the matching strings highlighted.

You can download the displayed data by clicking on download.



Logs

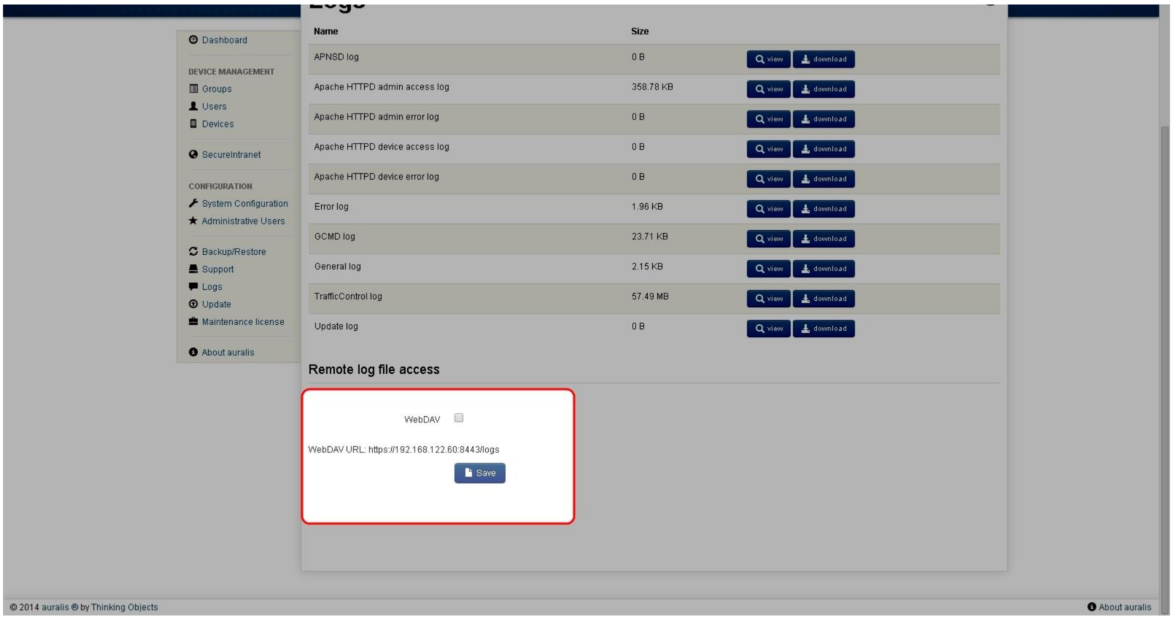
Name	Size		
APNSD log	0 B	view	download
Apache HTTPD admin access log	358.78 KB	view	download
Apache HTTPD admin error log	0 B	view	download
Apache HTTPD device access log	0 B	view	download
Apache HTTPD device error log	0 B	view	download
Error log	1.96 KB	view	download
GCMD log	23.71 KB	view	download
General log	2.15 KB	view	download
TrafficControl log	57.49 MB	view	download
Update log	0 B	view	download

Remote log file access

WebDAV ☐

Access to log files via WebDAV

It is possible to enable direct access to the log files via WebDAV by checking the option WebDAV. Use the displayed WebDAV URL to access the logfiles. Click “Save” to apply the setting.



Name	Size		
APNSD log	0 B	view	download
Apache HTTPD admin access log	358.78 KB	view	download
Apache HTTPD admin error log	0 B	view	download
Apache HTTPD device access log	0 B	view	download
Apache HTTPD device error log	0 B	view	download
Error log	1.96 KB	view	download
GCMD log	23.71 KB	view	download
General log	2.15 KB	view	download
TrafficControl log	57.49 MB	view	download
Update log	0 B	view	download

Remote log file access

WebDAV ☐

WebDAV URL: https://192.168.122.60:8443/logs

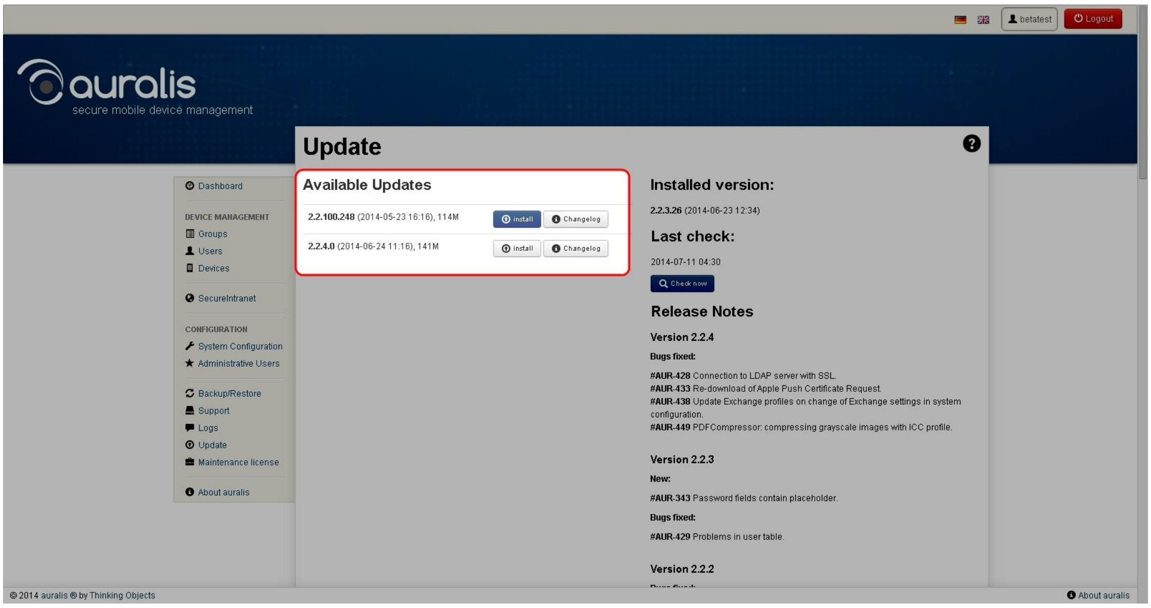
Save

11 Update

Available updates

The update settings display Information about the current version of auralis and available updates.

If a new version of auralis is available, it is displayed on the left side. You can install the update, or view the ChangeLog.



Update

Available Updates

2.2.100.248 (2014-05-23 16:16), 114M install Changelog

2.2.4.0 (2014-06-24 11:16), 141M install Changelog

Installed version:

2.2.3.26 (2014-06-23 12:34)

Last check:

2014-07-11 04:30

Check now

Release Notes

Version 2.2.4

Bugs fixed:

#AUR-428 Connection to LDAP server with SSL.
#AUR-433 Re-download of Apple Push Certificate Request.
#AUR-438 Update Exchange profiles on change of Exchange settings in system configuration.
#AUR-449 PDFCompressor: compressing grayscale images with ICC profile.

Version 2.2.3

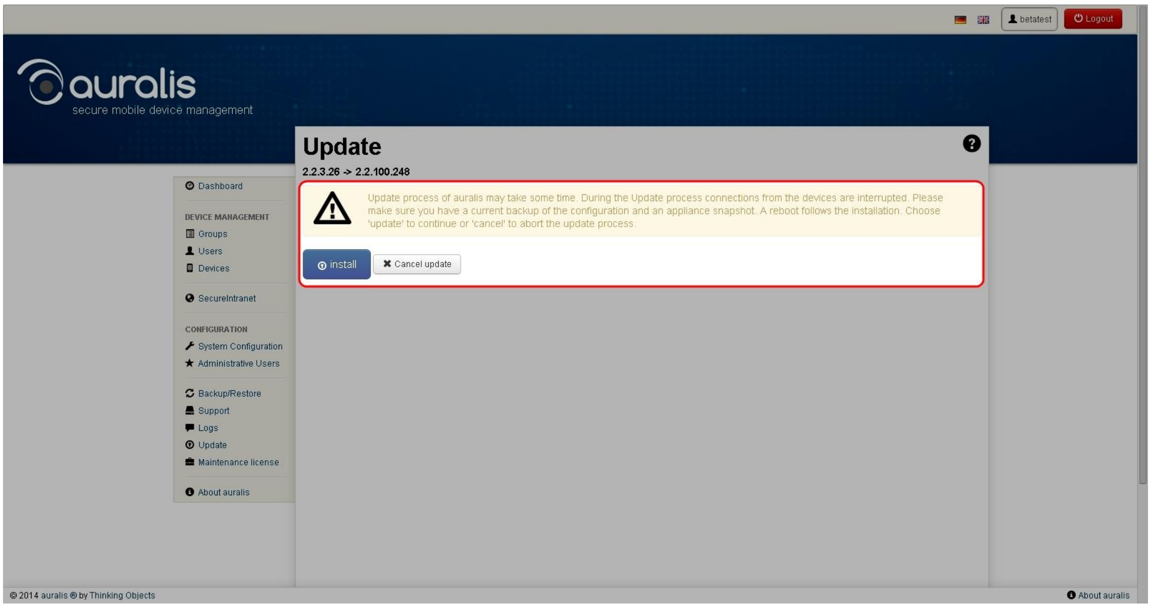
New:

#AUR-343 Password fields contain placeholder.

Bugs fixed:

#AUR-429 Problems in user table.

Version 2.2.2



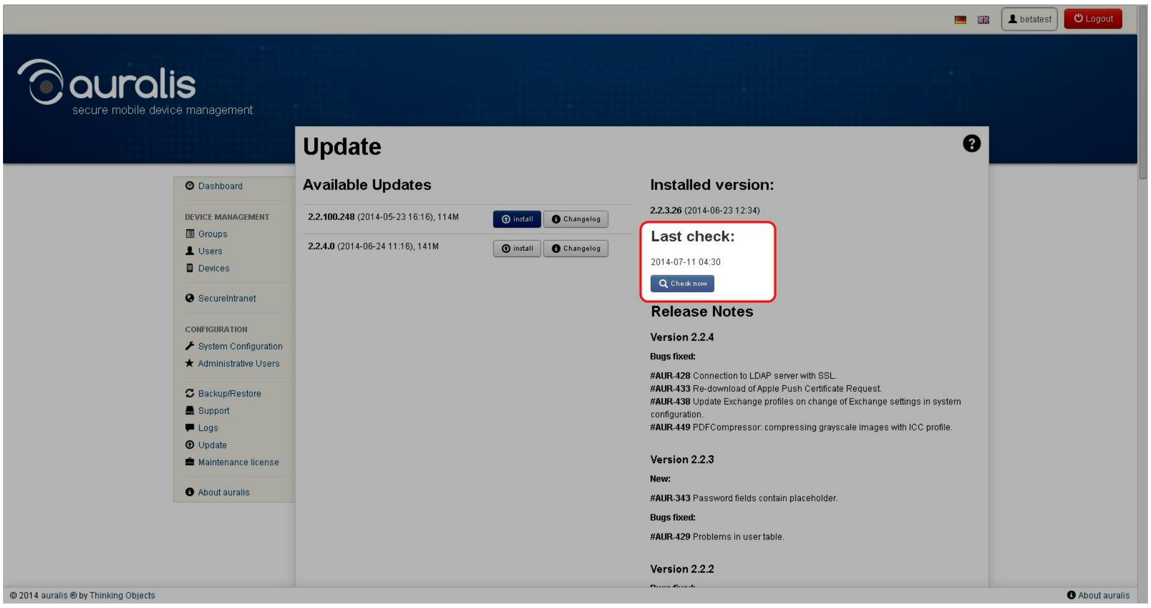
Update

2.2.3.26 -> 2.2.100.248

Update process of auralis may take some time. During the Update process connections from the devices are interrupted. Please make sure you have a current backup of the configuration and an appliance snapshot. A reboot follows the installation. Choose 'update' to continue or 'cancel' to abort the update process.

install ✖ Cancel update

The currently installed version of auralis is displayed on the right side. Below information about the last automatic check for updates is shown. To check for updates manually, click on the button Check now.



Update

Available Updates

2.2.100.248 (2014-05-23 16:16), 114M

2.2.4.0 (2014-06-24 11:16), 141M

Installed version:

2.2.3.26 (2014-06-23 12:34)

Last check:

2014-07-11 04:30

Release Notes

Version 2.2.4

Bugs fixed:

#AUR-428 Connection to LDAP server with SSL.
#AUR-433 Re-download of Apple Push Certificate Request.
#AUR-438 Update Exchange profiles on change of Exchange settings in system configuration.
#AUR-449 PDFCompressor: compressing grayscale images with ICC profile.

Version 2.2.3

New:

#AUR-343 Password fields contain placeholder.

Bugs fixed:

#AUR-429 Problems in user table.

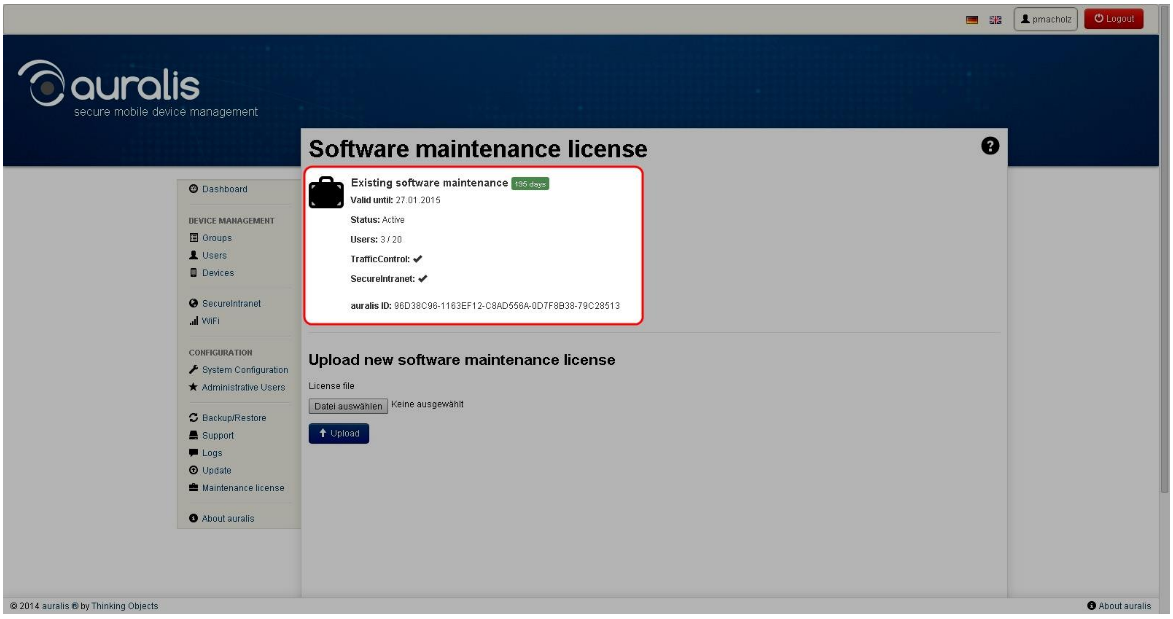
Version 2.2.2

The most recent changes and new features in the respective versions are displayed in the release notes.

The admin addresses specified in the email settings will receive an email whenever a new version is available. The check for updates takes place daily.

12 License

This dialogue shows the details of your installed license.



Software maintenance license

Existing software maintenance 195 days
Valid until: 27.01.2015
Status: Active
Users: 3 / 20
TrafficControl: ✓
SecureIntranet: ✓

auralis ID: 96D38C96-1163EF12-C8AD556A-0D7F8B38-79C28513

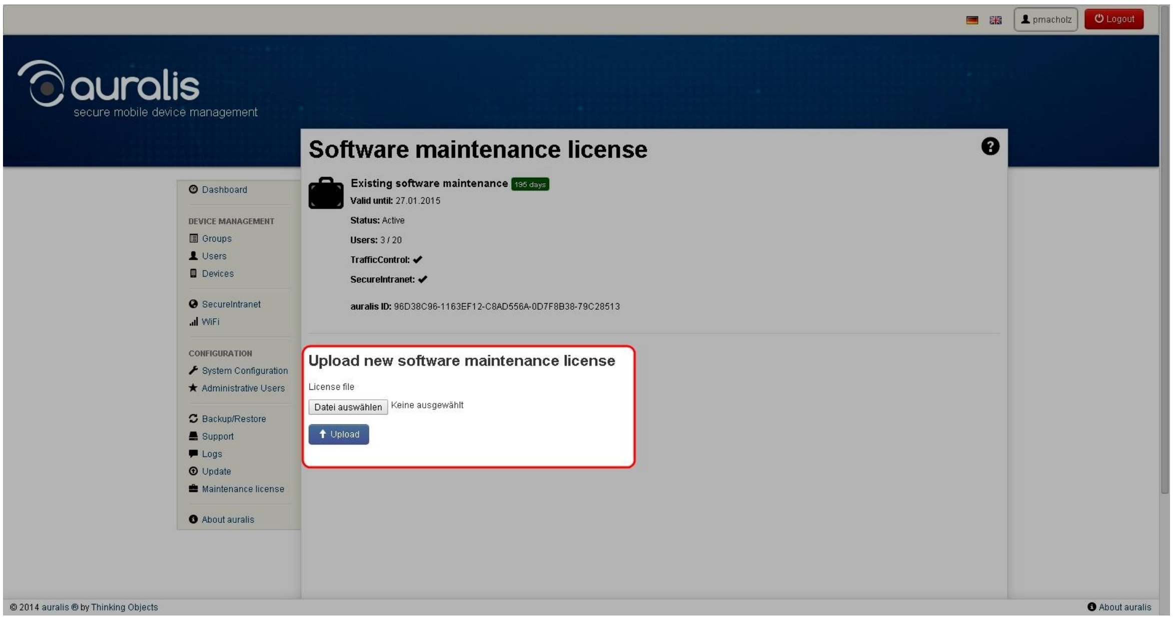
Upload new software maintenance license

License file
Datei auswählen Keine ausgewählt
Upload

© 2014 auralis ® by Thinking Objects
About auralis

Upload a new license file

To renew your license, upload the license file that you have received from Thinking Objects. Click on Upload to activate the new license.



Software maintenance license

Existing software maintenance 195 days
Valid until: 27.01.2015
Status: Active
Users: 3 / 20
TrafficControl: ✓
SecureIntranet: ✓

auralis ID: 96D38C96-1163EF12-C8AD556A-0D7F8B38-79C28513

Upload new software maintenance license

License file
Datei auswählen Keine ausgewählt
Upload

© 2014 auralis ® by Thinking Objects
About auralis

13 Support

If you have further questions or need assistance with the integration, please contact our support.

Available from Monday to Friday from 09:00 AM to 05:00 PM CET at support@to.com.

14 About us

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)