auralis

secure mobile device management

Administration Manual

auralis 3.7

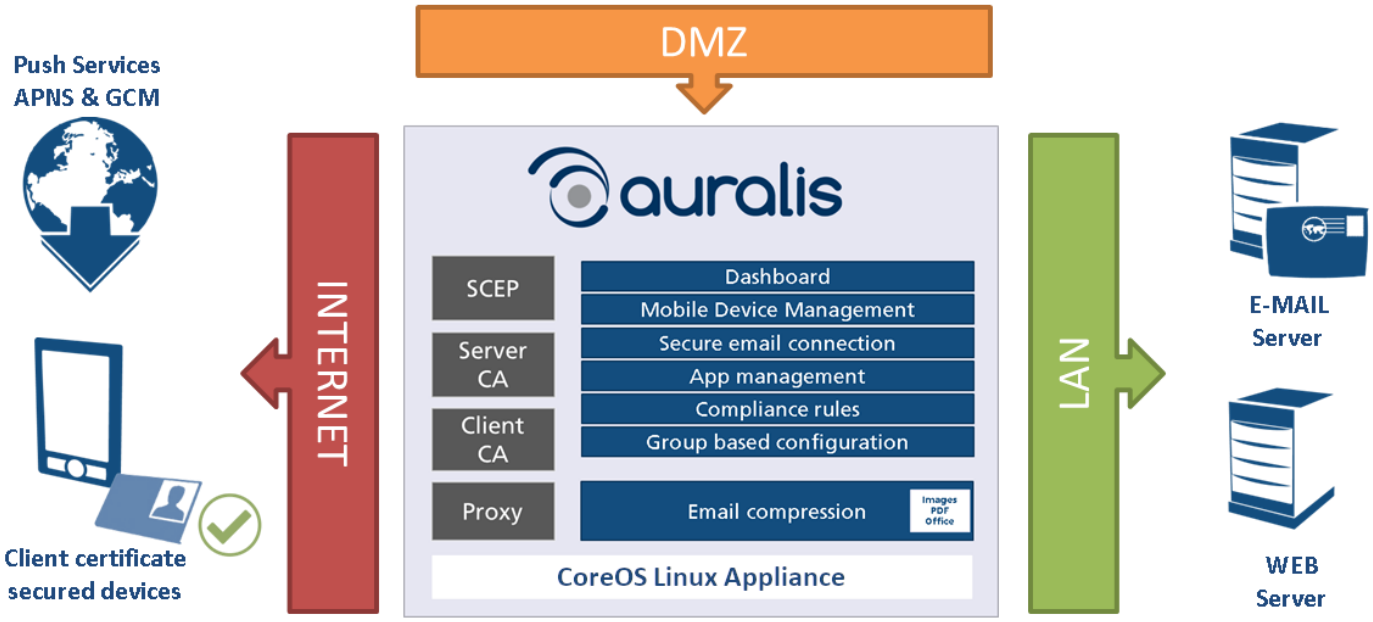
2022-02-17

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 ActiveSync based solution like Zarafa or Kerio) and Web servers against man in-the middle attacks. auralis is a firewall for your email infrastructure.

1.1 Structure and 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 CoreOS Linux 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 2 Cores

The required computing power depends on the number of user and the email traffic.

RAM: Minimum 4 GB RAM

For the use of TrafficControl data compression for more than 50 users, we recommend at least 8GB of RAM. There should be at least 1 GB RAM for every additional tenant.

HDD: 30 GB Disk space

Since log files are written during operation we recommend at least 30 GB disk space. Log files will be removed after 30 days.

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 which is reachable from the internet, e.g. auralis.example.com

Note

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

2 Preparation and installation

2.1 Firewall rules

The following access rules are necessary for auralis:

Source	Destination	Ports
any	[auralis]	Device port/TCP (Default: 443); Mixed port/TCP (Default: 8443)
[auralis]	[ActiveSync server]	443/TCP*
[auralis]	[SMTP server]	25/TCP (depending on configuration)
[auralis]	[LDAP server]	389/TCP or 636/TCP (depending on configuration)
[SNMP monitoring]	[auralis]	161/UDP

* or 80/TCP if you don't use TLS for ActiveSync

Note

For access to services used by auralis access is required to the web addresses below. If you cannot configure URLs in your firewall directly and want to avoid an ANY port 443 rule, you can configure an HTTP proxy in the system configuration.

URLs required to access

- https://nebraska.auralis.de/
- https://registry.auralis.de/
- https://repo.auralis.de/
- https://quay.io/
- https://*.quay.io/
- https://quay-registry.s3.amazonaws.com/
- https://*.cloudfront.net/
- https://acme-v02.api.letsencrypt.org/
- https://api.push.apple.com/
- https://itunes.apple.com/
- https://vpp.itunes.apple.com/
- https://*.mzstatic.com/
- https://mdmenrollment.apple.com/
- https://fcm.googleapis.com/fcm/send
- https://play.google.com/store/
- https://*.ggpht.com/
- https://*.googleusercontent.com/

2.2 DNS – fully qualified domain name

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

2.3 Installation environment

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

Virtual machine

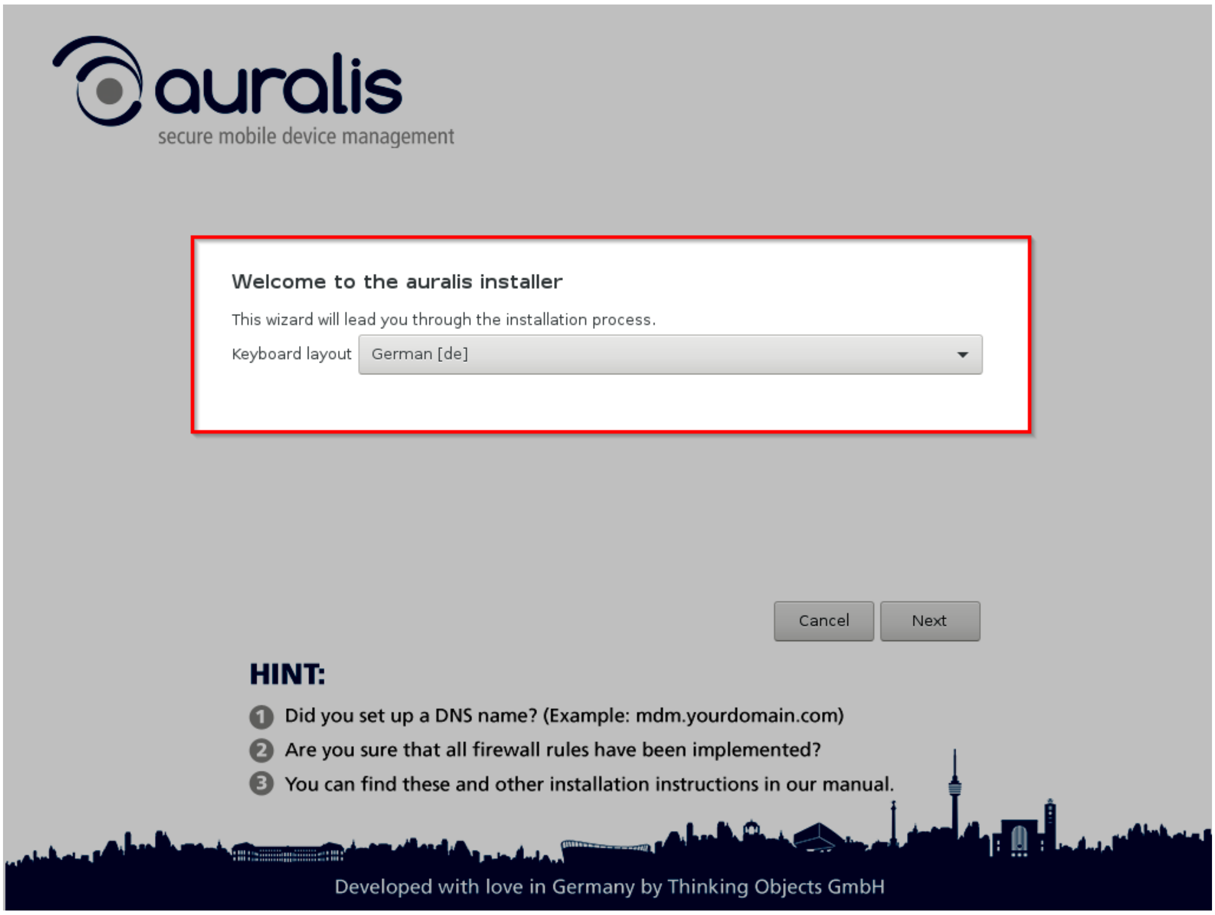
Create a new virtual machine and select CoreOS or Linux with 64 bit for the operating system. For system requirements see above. Select the auralis ISO image for system boot and start the virtual machine.

Physical machine

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

2.4 Installation

Start your machine from the auralis installer ISO and choose "auralis Installation" in the boot menu. Now the auralis installer will be loaded. In the first step you need to choose your keyboard layout.



Welcome to the auralis installer

This wizard will lead you through the installation process.

Keyboard layout: German [de]

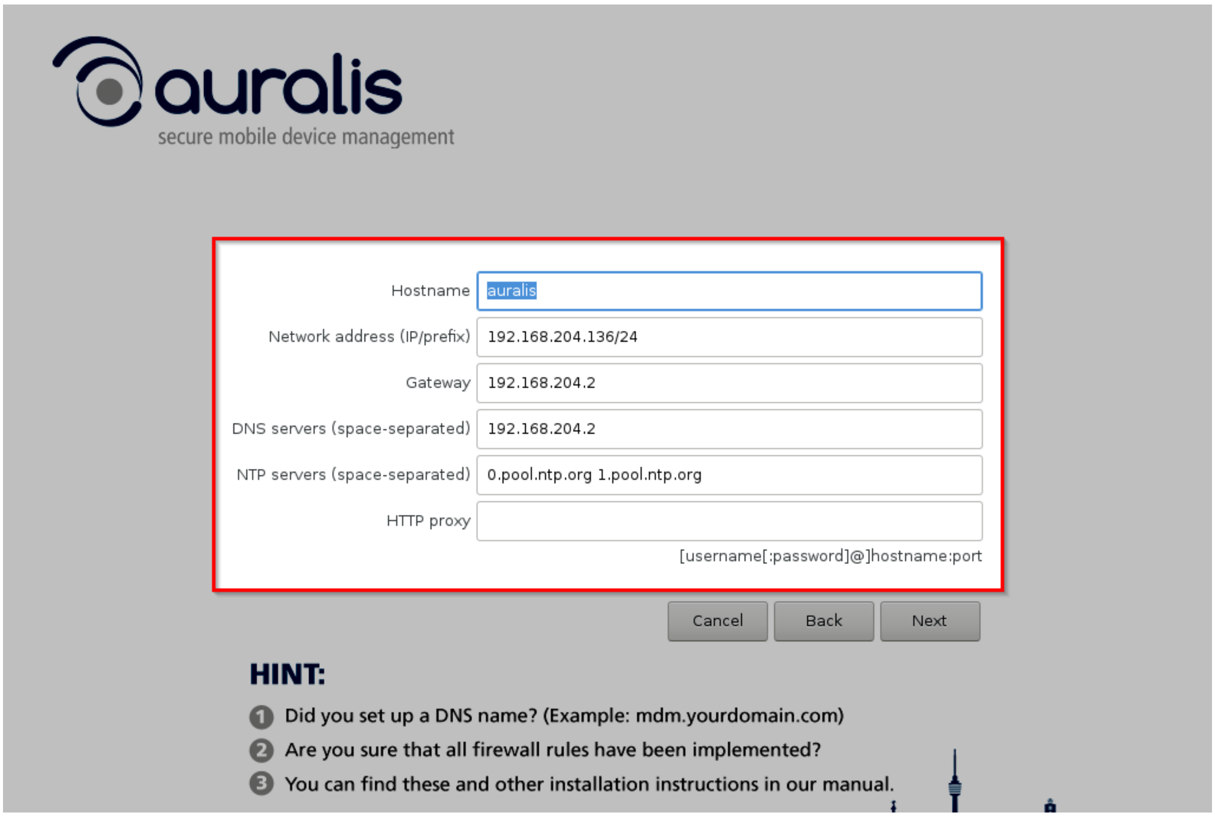
auralis
secure mobile device management
Cancel
Next

HINT:

1. Did you set up a DNS name? (Example: mdm.yourdomain.com)
2. Are you sure that all firewall rules have been implemented?
3. You can find these and other installation instructions in our manual.

Developed with love in Germany by Thinking Objects GmbH

Please enter your network configuration in the next step. The installer tries to pre-fill the fields with appropriate values. The chosen hostname is only internal and doesn't need to be a public DNS name.



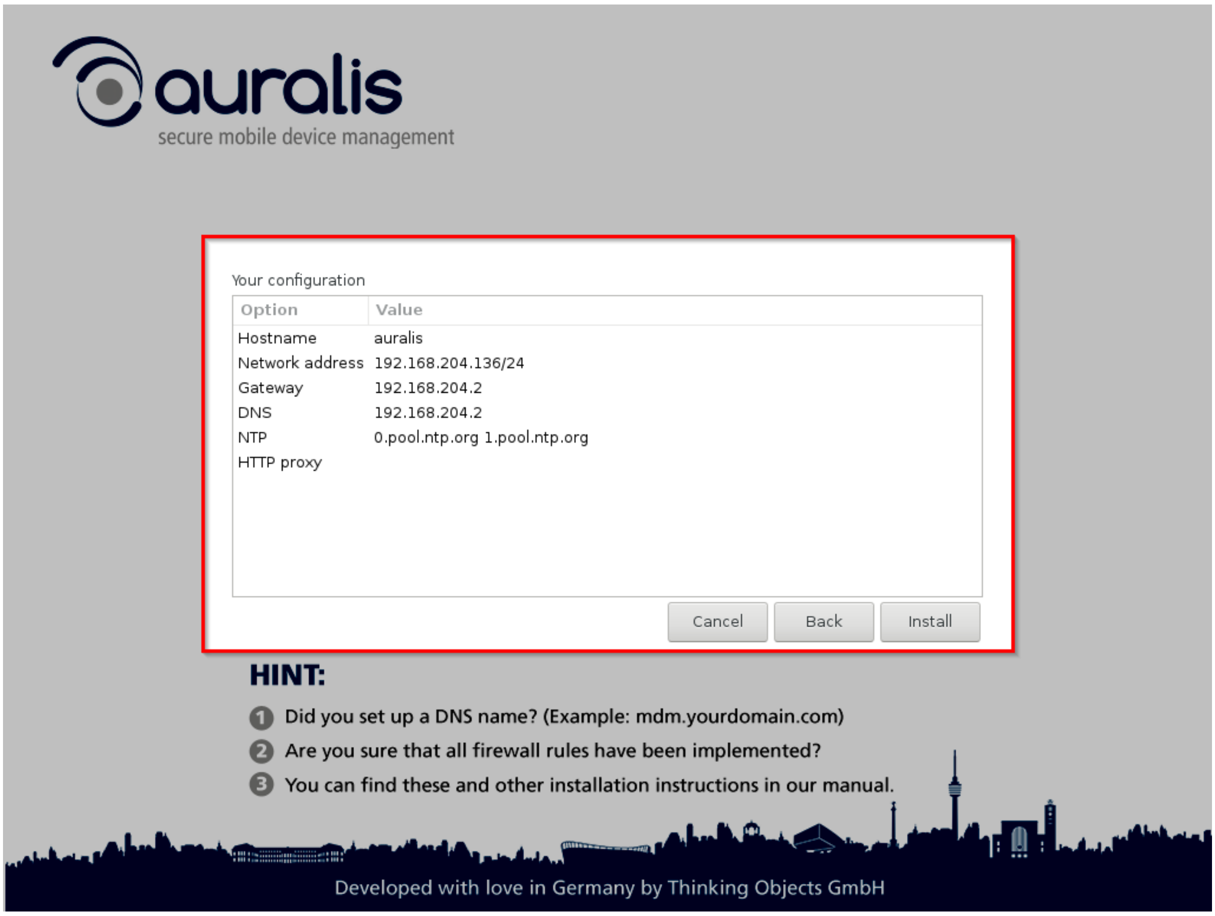
Hostname	auralis
Network address (IP/prefix)	192.168.204.136/24
Gateway	192.168.204.2
DNS servers (space-separated)	192.168.204.2
NTP servers (space-separated)	0.pool.ntp.org 1.pool.ntp.org
HTTP proxy	

[username[:password]@]hostname:port

HINT:

1. Did you set up a DNS name? (Example: mdm.yourdomain.com)
2. Are you sure that all firewall rules have been implemented?
3. You can find these and other installation instructions in our manual.

On the next screen you may check your configuration. A click on “Install” will start the installation, click “Back” if you want to revise a value.



Your configuration

Option	Value
Hostname	auralis
Network address	192.168.204.136/24
Gateway	192.168.204.2
DNS	192.168.204.2
NTP	0.pool.ntp.org 1.pool.ntp.org
HTTP proxy	

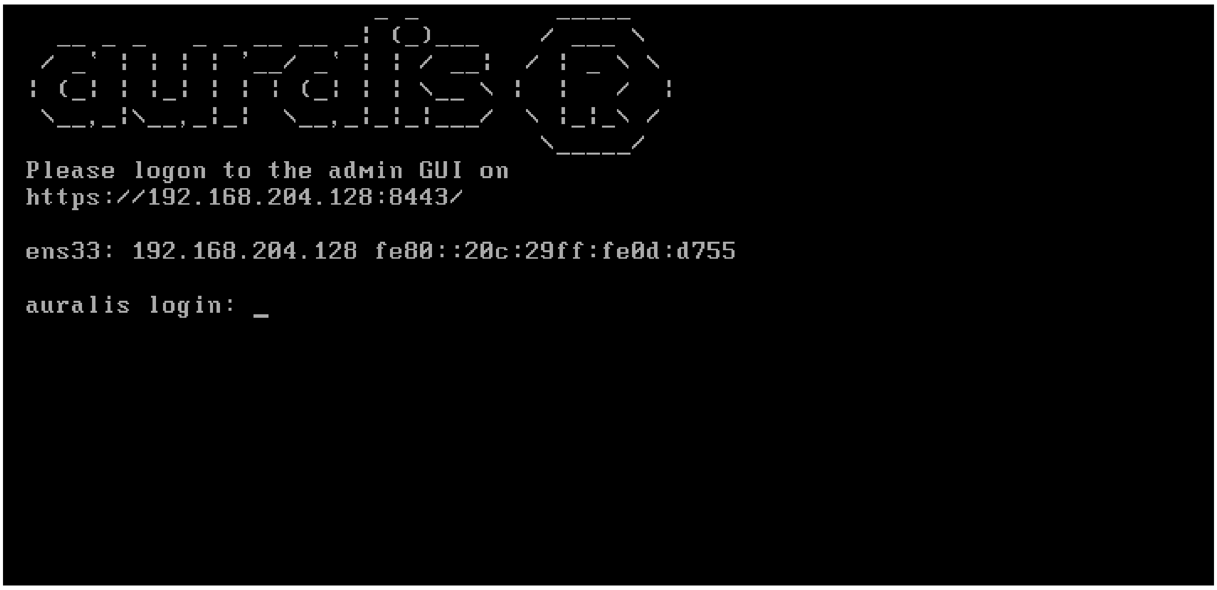
HINT:

1. Did you set up a DNS name? (Example: mdm.yourdomain.com)
2. Are you sure that all firewall rules have been implemented?
3. You can find these and other installation instructions in our manual.

Developed with love in Germany by Thinking Objects GmbH

Now the base system will be downloaded and installed. If this step is finished a click on “OK” will restart the system and boot into the base system. After boot up the auralis container images will be downloaded and the required containers created.

auralis is ready



```
Please logon to the admin GUI on
https://192.168.204.128:8443/

ens33: 192.168.204.128 fe80::20c:29ff:fe0d:d755

auralis login: _
```

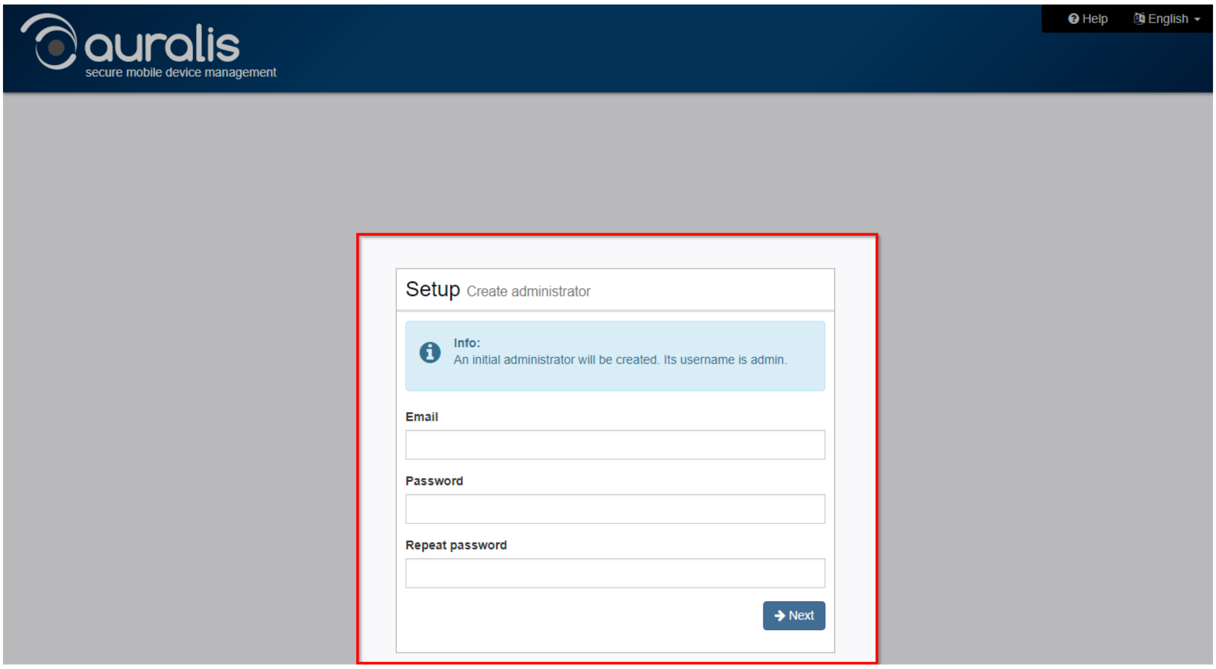
The URL to access the auralis Control web interface is displayed when the containers are created. Point your browser to the shown URL, https://*<IP-address>*:8443/. Please note the web interface might not be available immediately, but should be within a minute.

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. Enter an email address and a password for the initial administrator.



Setup Create administrator

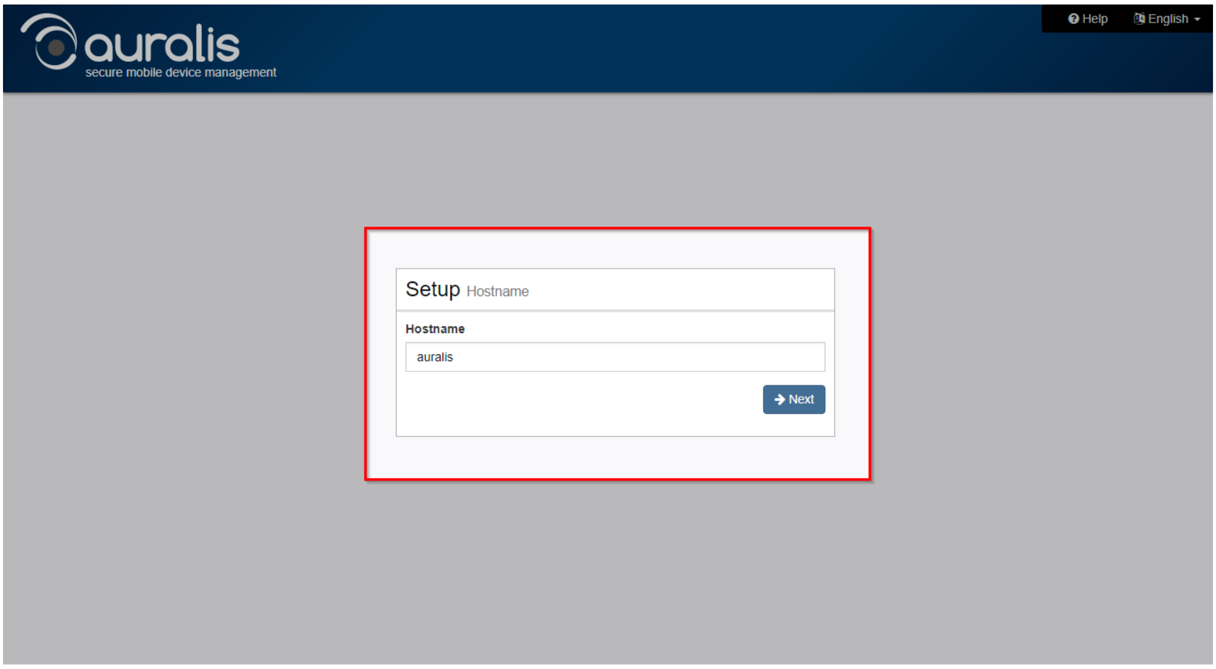
Info:
An initial administrator will be created. Its username is admin.

Email

Password

Repeat password

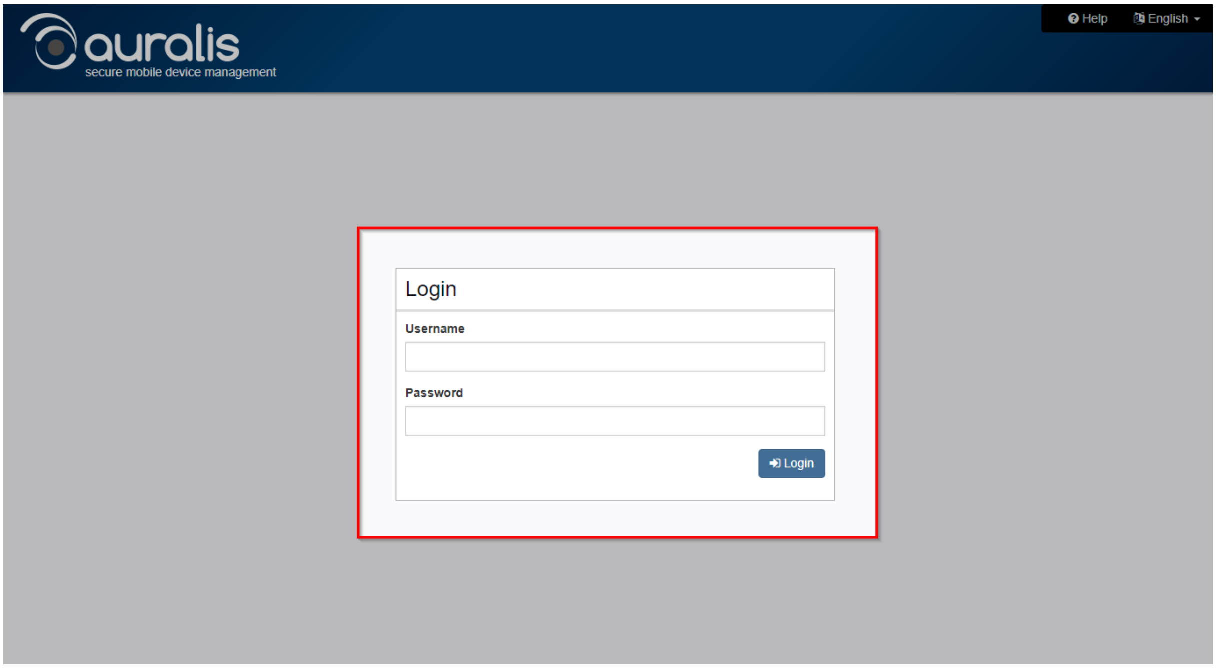
To complete the initial configuration you need to enter the hostname which is used to reach auralis Control. A public domain name is not required. Do not use the DNS name which you have planned to use for device access.



Setup Hostname

Hostname: auralis

After reloading the Page, log in with the username “admin” and the previously chosen password.



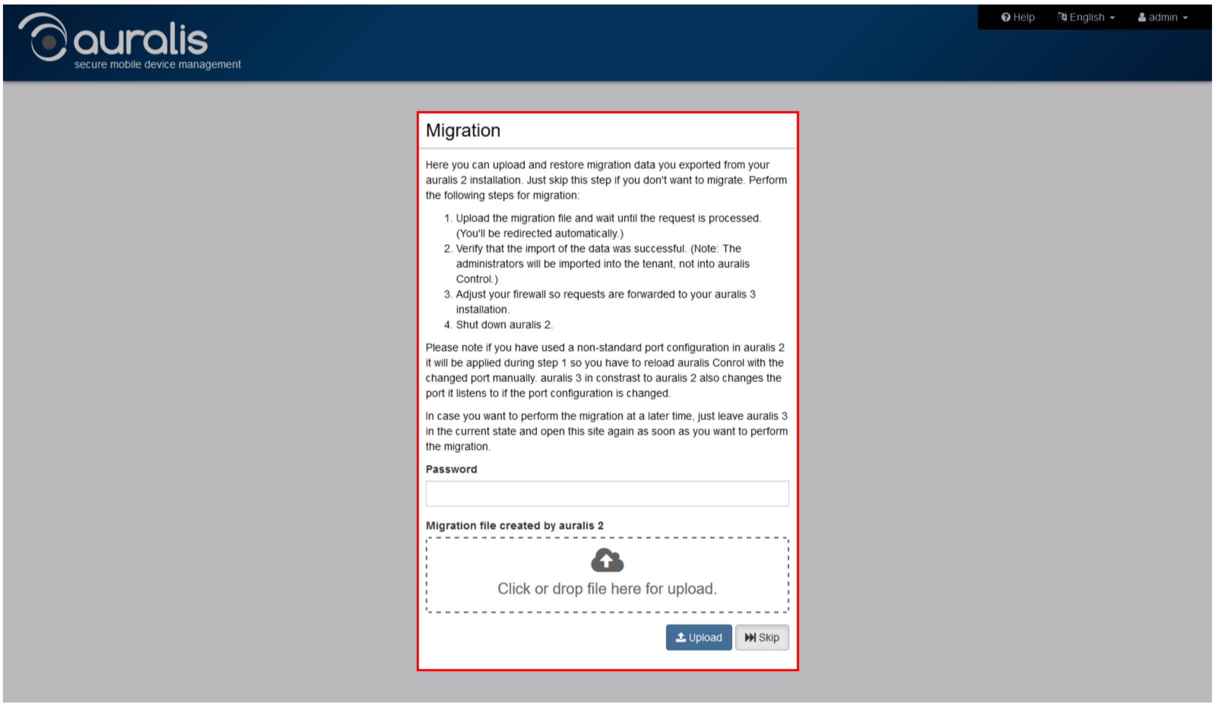
Login

Username

Password

Login

You now have the option to complete a migration from auralis 2. Just add the migration file created by auralis 2 and upload it.



Migration

Here you can upload and restore migration data you exported from your auralis 2 installation. Just skip this step if you don't want to migrate. Perform the following steps for migration:

1. Upload the migration file and wait until the request is processed. (You'll be redirected automatically.)
2. Verify that the import of the data was successful. (Note: The administrators will be imported into the tenant, not into auralis Control.)
3. Adjust your firewall so requests are forwarded to your auralis 3 installation.
4. Shut down auralis 2.

Please note if you have used a non-standard port configuration in auralis 2 it will be applied during step 1 so you have to reload auralis Conrol with the changed port manually. auralis 3 in constrast to auralis 2 also changes the port it listens to if the port configuration is changed.

In case you want to perform the migration at a later time, just leave auralis 3 in the current state and open this site again as soon as you want to perform the migration.

Password

Migration file created by auralis 2

Click or drop file here for upload.

Upload Skip

After the completion of the migration, or skipping this step, is auralis successfully installed.

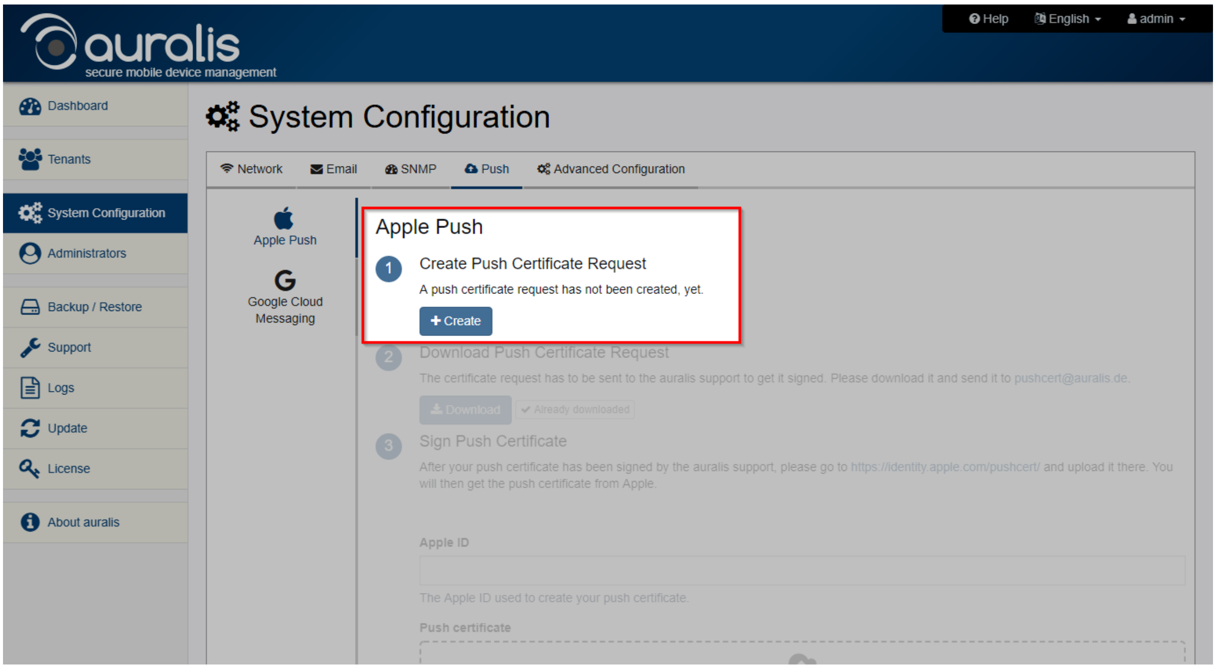
Note

In case you want to perform the migration at a later time, just leave auralis 3 in the current state and open the migration site again under https://*<IP-Adresse>*:8443/migration as soon as you want to perform the migration.

2.6 Create an Apple push certificate

After installation, you should configure an Apple push certificate. 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.

Go to System Configuration > Push > Apple Push. Click on the button “Create” to create a certificate request.



Apple Push

1 Create Push Certificate Request

A push certificate request has not been created, yet.

+ Create

2 Download Push Certificate Request

The certificate request has to be sent to the auralis support to get it signed. Please download it and send it to pushcert@auralis.de.

Download ✓ Already downloaded

3 Sign Push Certificate

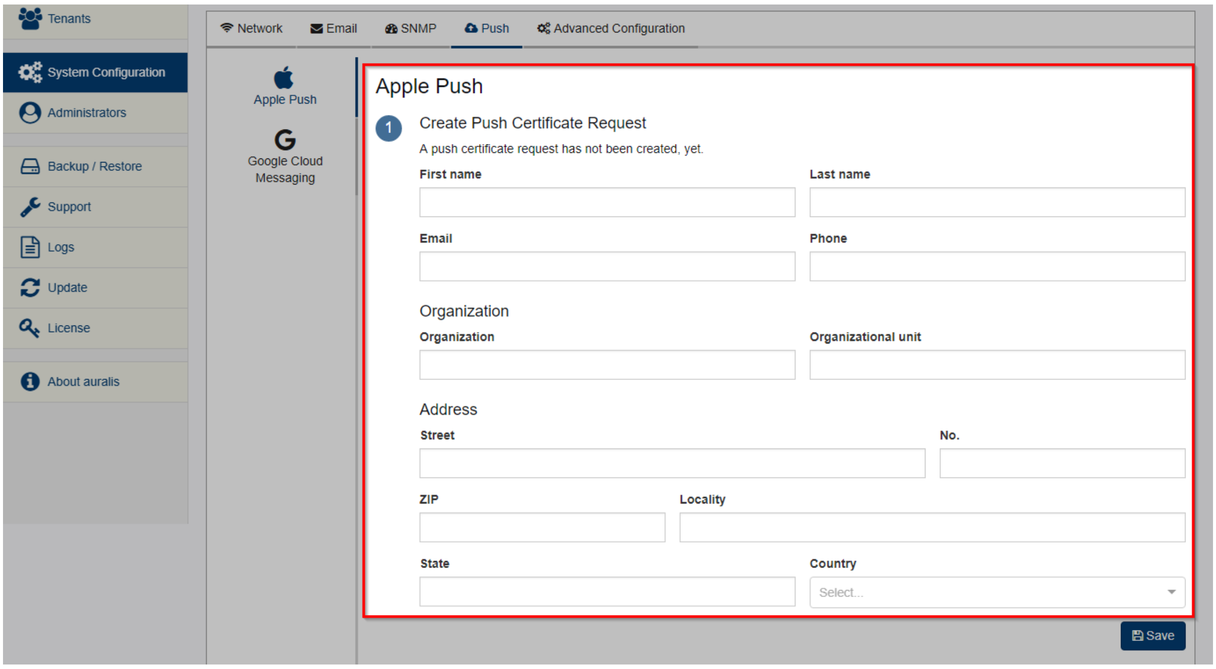
After your push certificate has been signed by the auralis support, please go to https://identity.apple.com/pushcert/ and upload it there. You will then get the push certificate from Apple.

Apple ID

The Apple ID used to create your push certificate.

Push certificate

Enter the required data in the form and click on “Save”.



Apple Push

1 Create Push Certificate Request

A push certificate request has not been created, yet.

First name | Last name

Email | Phone

Organization

Organization | Organizational unit

Address

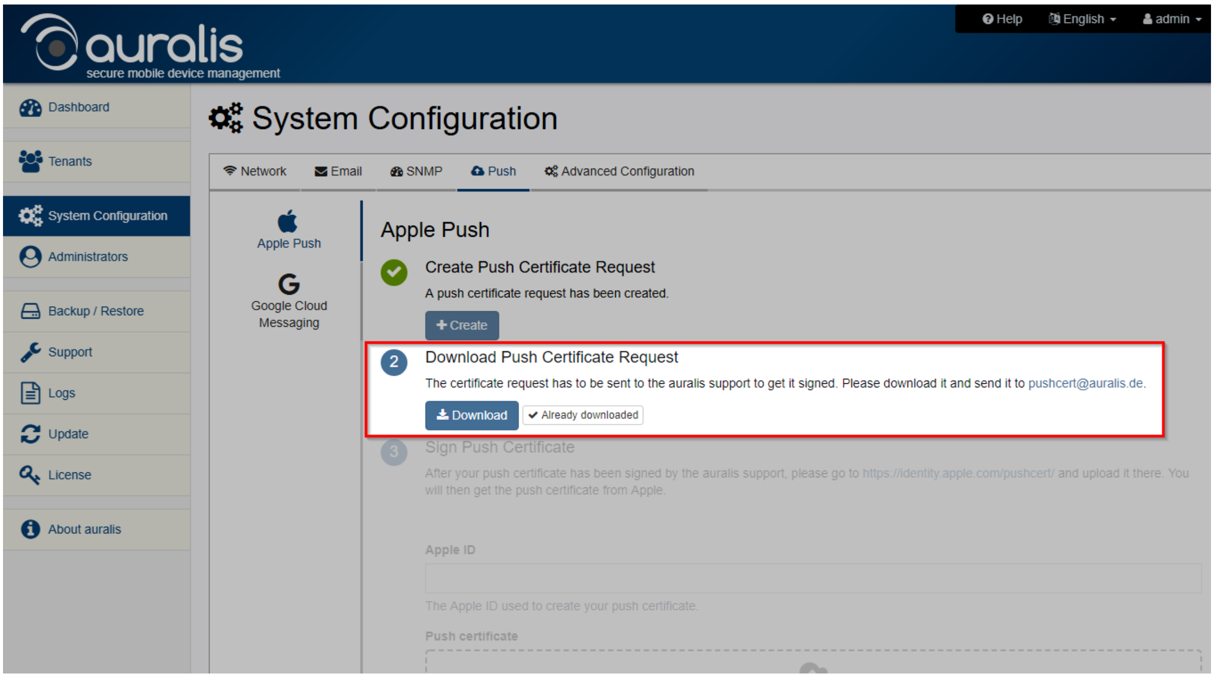
Street | No.

ZIP | Locality

State | Country: Select...

Save

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

Apple Push

Create Push Certificate Request

A push certificate request has been created.

2 Download Push Certificate Request

The certificate request has to be sent to the auralis support to get it signed. Please download it and send it to pushcert@auralis.de.

3 Sign Push Certificate

After your push certificate has been signed by the auralis support, please go to https://identity.apple.com/pushcert/ and upload it there. You will then get the push certificate from Apple.

Apple ID

The Apple ID used to create your push certificate.

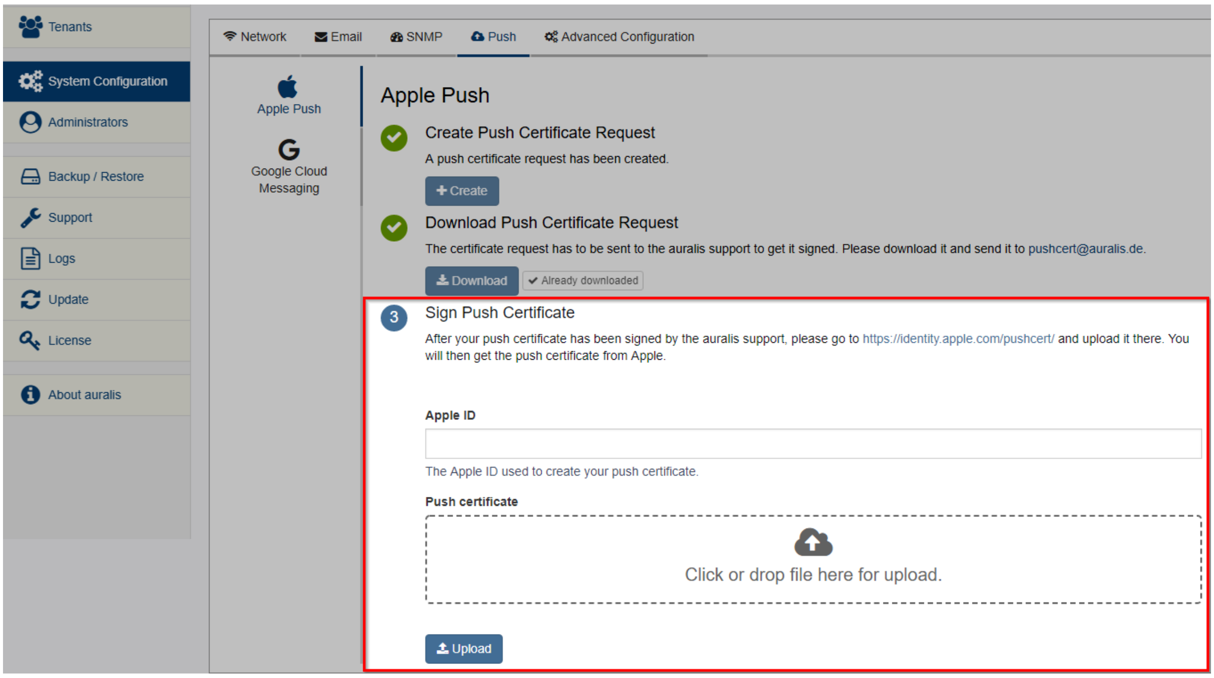
Push certificate

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

Caution

The certificate is only valid for one year and has to be renewed with the same Apple ID. If a new certificate is generated with another Apple ID, all rolled out iOS devices will lose their MDM connection.

Select the push certificate from Apple in step 3 and upload it to auralis.



Apple Push

Create Push Certificate Request

A push certificate request has been created.

Download Push Certificate Request

The certificate request has to be sent to the auralis support to get it signed. Please download it and send it to pushcert@auralis.de.

3 Sign Push Certificate

After your push certificate has been signed by the auralis support, please go to https://identity.apple.com/pushcert/ and upload it there. You will then get the push certificate from Apple.

Apple ID

The Apple ID used to create your push certificate.

Push certificate

Click or drop file here for upload.

2.7 License

auralis is equipped with a demo license. It allows you to create an unlimited number of tenants and assign up to five licenses to them. You can test all features before you purchase a license. A purchased license can be installed easily while auralis is running. The required steps are explained in chapter 12.

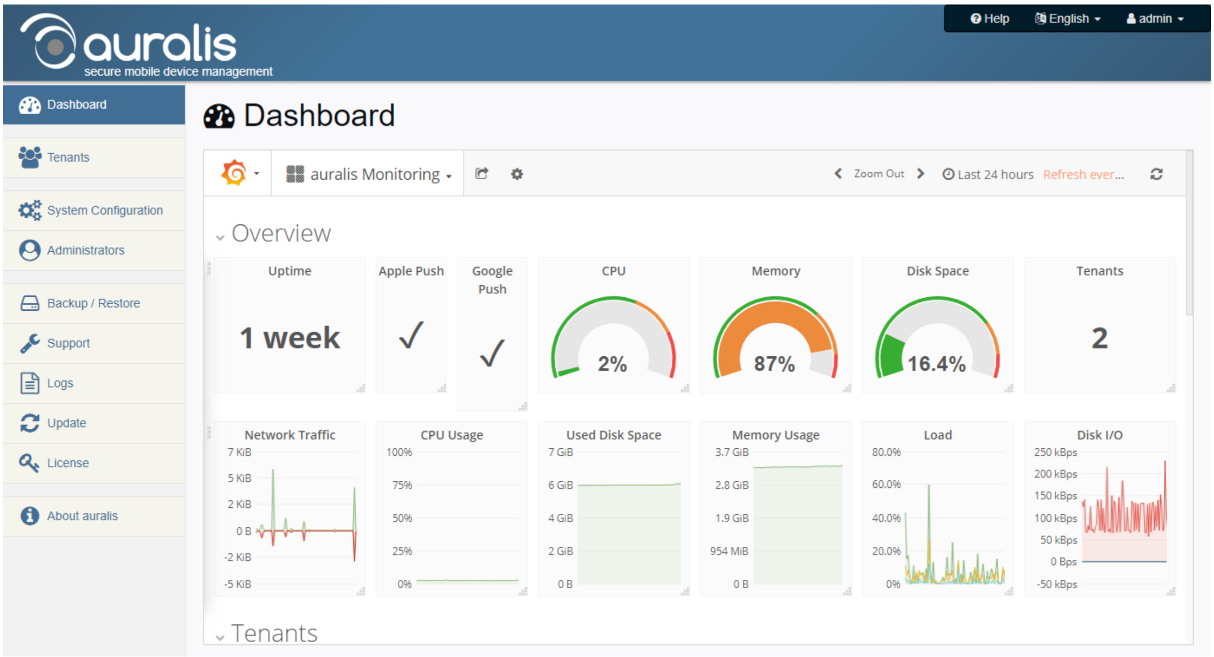
Details about our license model and prices are available at https://auralis.de/en/. If you are interested in purchasing a license, please contact us at info@auralis.de.

3 Dashboard

The dashboard is divided into three categories.

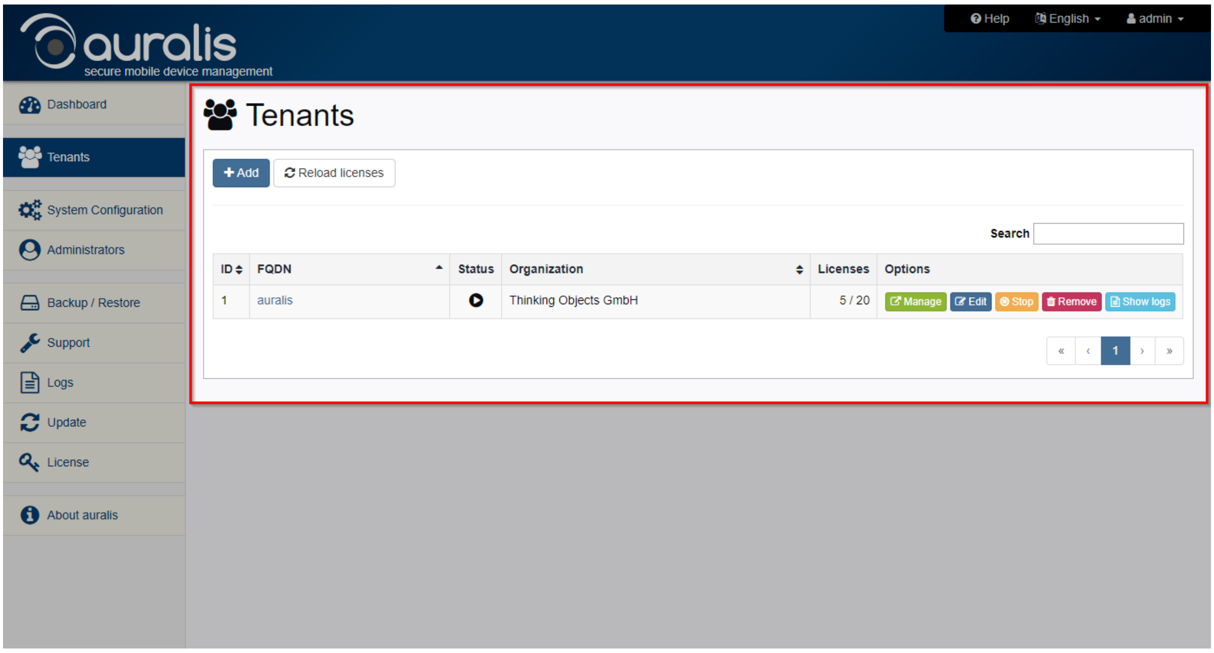
1) Overview
   Here you can find all system specific information such as CPU, memory, disk usage or network usage. Likewise the number of tenants is shown. You can see whether the push services of Apple and Google are configured and available.
2) Tenants
   In this category you get information about all tenants.

3) Container
   Here you can see the resource usage of the different auralis containers.



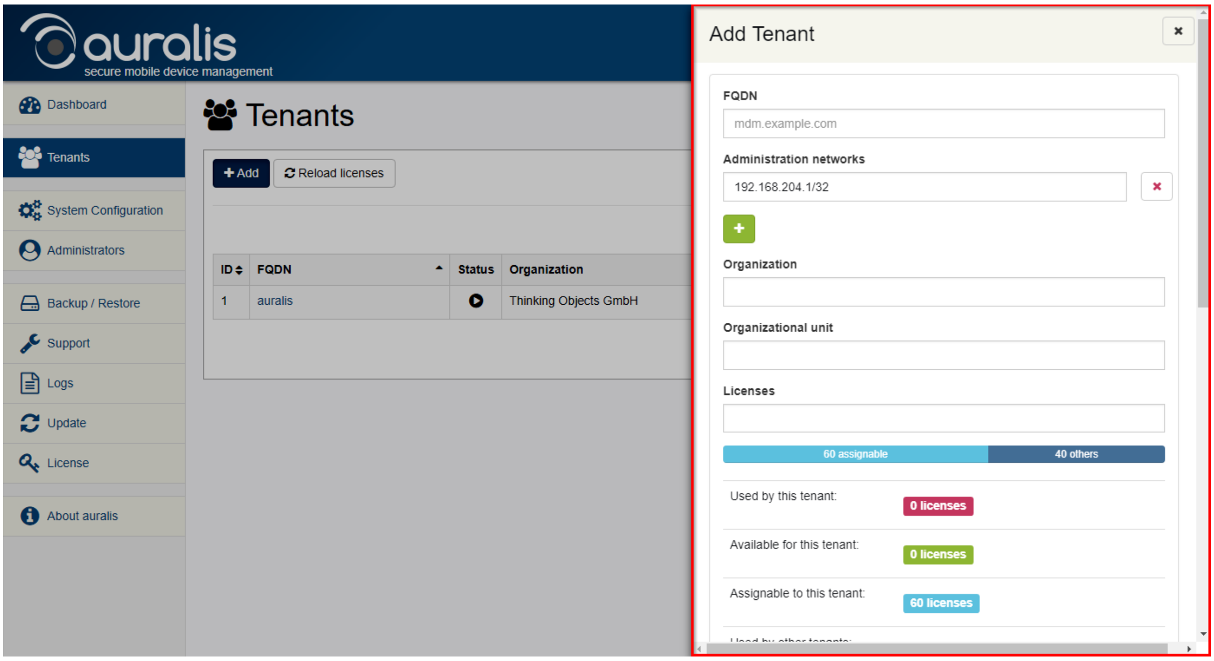
4 Tenants

Under this menu item you may add and manage tenants. In the overview you can find the most important information of the different tenants: the unique ID, the Fully Qualified Domain Name (FQDN), the status, the related organization as well as the used and assigned licenses.



ID	FQDN	Status	Organization	Licenses	Options
1	auralis	▶	Thinking Objects GmbH	5 / 20	Manage Edit Stop Remove Show logs

To create a new tenant, click on "Add" which will open the necessary form. It allows you to assign available licenses and enter basic information about the tenant. Fill in the form and click on "Save" to add the tenant. The given values are used for the creation of the initial certificates.



ID	FQDN	Status	Organization
1	auralis	▶	Thinking Objects GmbH

FQDN
mdm.example.com

Administration networks
192.168.204.1/32

Organization

Organizational unit

Licenses

Used by this tenant:	0 licenses
Available for this tenant:	0 licenses
Assignable to this tenant:	60 licenses

FQDN: Enter a Fully Qualified Domain Name that will be used to connect to the tenant. The smartphones will use it for communication so it needs to be public. The tenant's administration interface will be available at https://<FQDN>:8443/admin. (In case you have modified the port configuration change the port accordingly.)

Administration networks: This allows to define the networks from which the tenant can be managed. If the tenant shall be manageable from every sender IP address (not recommended) enter “0.0.0.0/0”.

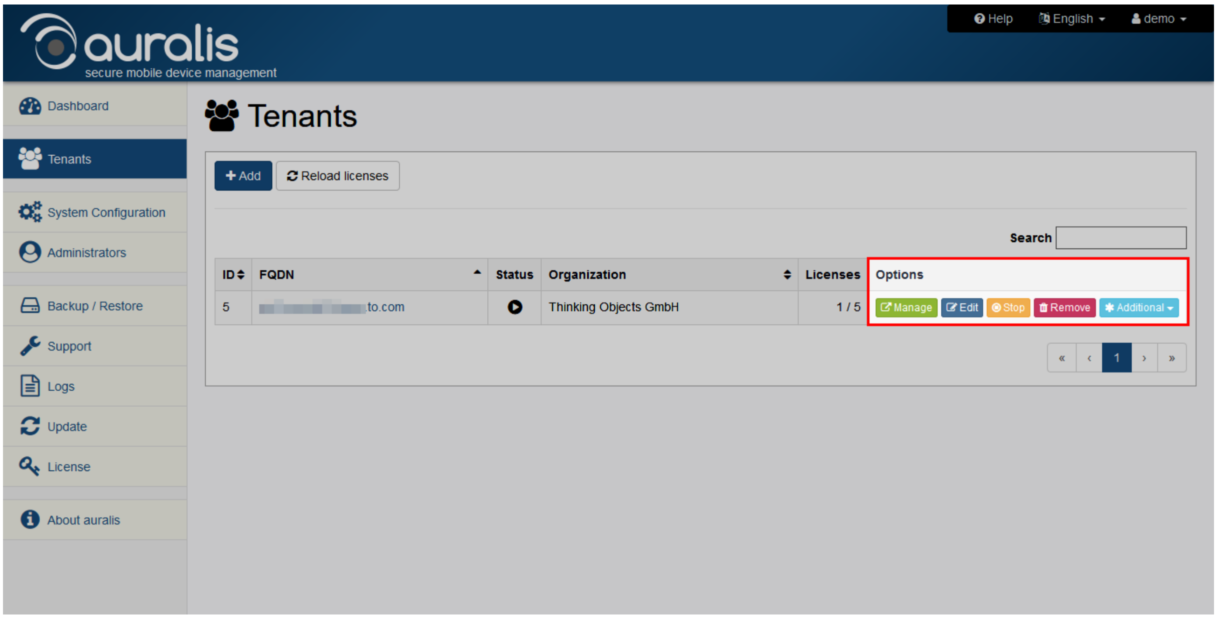
Organization: Enter the tenant’s organization.

Organizational unit: Enter the tenant’s organizational unit. It allows to distinguish tenants of the same organization.

Licenses: Here you can assign licenses to the tenant. The number of licenses specifies how many users may be created in the tenant.

Password of tenant administrator "admin": Enter the password for the initial administrator and repeat it in the field below.

Contact: Enter the contact details of the tenant’s contact person.



ID	FQDN	Status	Organization	Licenses	Options
5	[redacted]to.com	▶	Thinking Objects GmbH	1 / 5	Manage Edit Stop Remove Additional

Manage: A click on this button will open the tenant’s administration interface. You will be logged in automatically with your current account and do not need to enter a password. The handbook of the tenant administration you can get there with a click on the “?” icon.

Edit: Here you can modify the tenant.

Stop/Start: This allows to stop and start a tenant’s container.

Delete: To delete a tenant, click on this button.

Additional: Offers additional actions for the tenant.

- *Show logs:* Opens the logs of the tenant.
- *Create device report:* Creates a report with the devices that have been created in a definable time period.

- *Show license history:* Displays the history of license assignments.

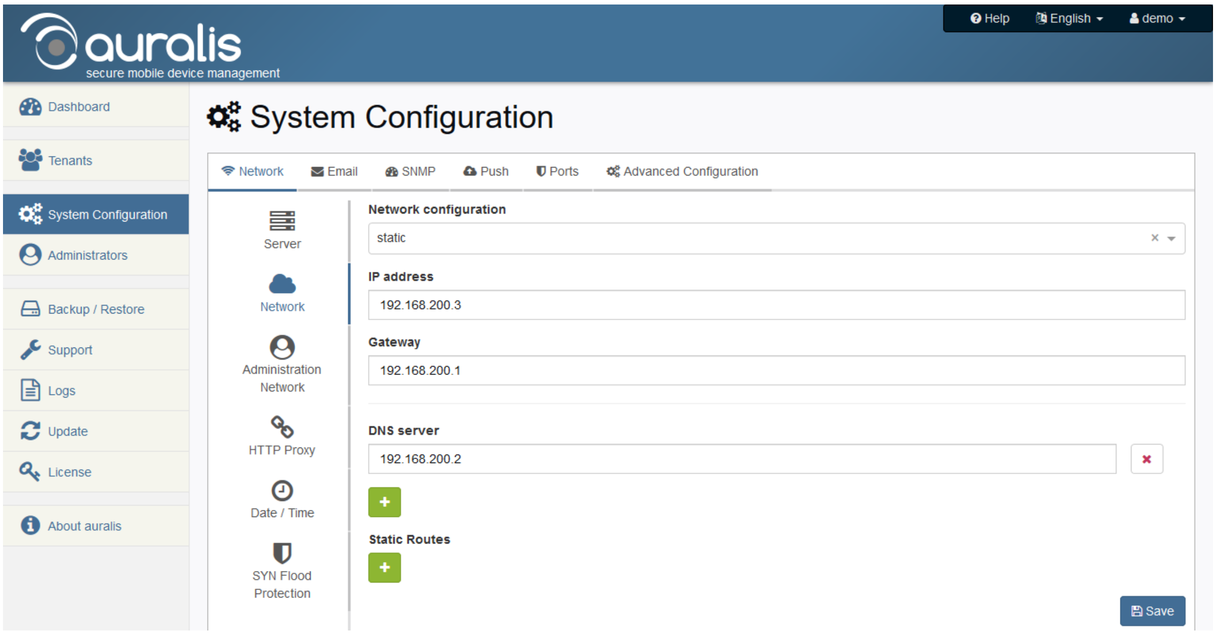
> **Note**
>
> For every administrator in auralis Control an account in each tenant will be created. You can login into every tenant with an "@" before your username (e.g. @username) and your usual password. This account is not visible in the tenant in the list of administrators.

5 System configuration

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

5.1 Network

On the "Network" tab you can find all relevant settings regarding the network connection of auralis.



System Configuration

Network configuration: static

IP address: 192.168.200.3

Gateway: 192.168.200.1

DNS server: 192.168.200.2

Static Routes

Server:

Hostname: Enter the hostname which is used to reach auralis Control. A public domain name is not necessary.

The second form allows you to upload a custom server certificate for auralis Control. The certificate needs to be in a PCKS #12 file including the entire certificate chain.

Network:

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.

DNS server: The IP address of the DNS server to use. Click on the plus sign to add further DNS servers.

Static routes: It is possible to define static routes. Therefore enter the target and the gateway.

Administration Network: The networks from which the auralis Control web interface may be accessed. Enter the networks in CIDR notation.

Note

If you cannot access your auralis system due to the network configuration, you can always modify the configuration by selecting “CoreOS Configure” in the boot loader menu upon system startup. Hereby the administration network will be reset.

HTTP Proxy: Configure an HTTP proxy for web access.

Proxy host: The IP address or hostname of the proxy.

Proxy port: The port of the proxy.

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

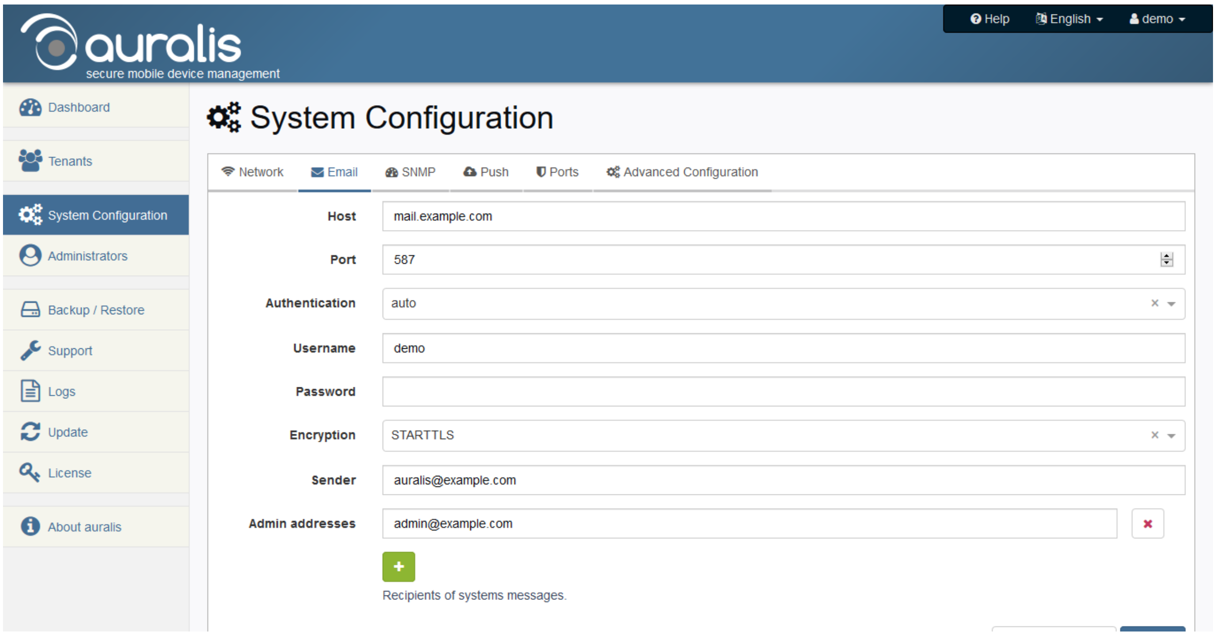
Proxy password: The password used to authenticate to the proxy if necessary.

Date / Time: Configure NTP servers for time synchronization.

SYN Flood Protection: If a SYN flood protection is wanted, you can enable it here.

5.2 Email

In the “Email” tab you can perform the configuration necessary for auralis to send system notifications via email.



Host: mail.example.com
Port: 587
Authentication: auto
Username: demo
Password:
Encryption: STARTTLS
Sender: auralis@example.com
Admin addresses: admin@example.com
Recipients of systems messages.

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

Port: The port of the SMTP server.

Authentication: The method used for authentication.

Username: The username for authentication.

Password: The password for authentication.

Encryption: The method used for encryption.

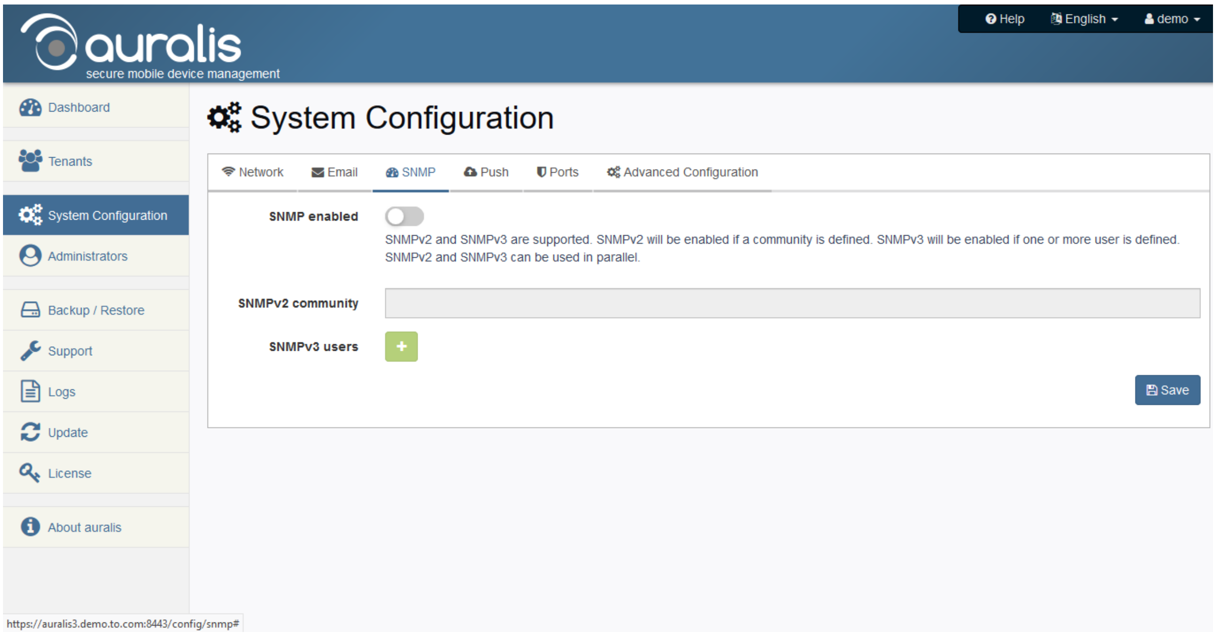
Sender: The sender address used for system notifications.

Admin addresses: The receiver addresses for system notifications.

Send test email: With this button you can test if sending emails works.

5.3 SNMP

auralis can deliver status information of the system via SNMP. If you want to use SNMP you may enable it here. For SNMPv2 a community has to be specified; for SNMPv3 at least one user has to be defined.



SNMP enabled

SNMPv2 and SNMPv3 are supported. SNMPv2 will be enabled if a community is defined. SNMPv3 will be enabled if one or more user is defined. SNMPv2 and SNMPv3 can be used in parallel.

SNMPv2 community

SNMPv3 users

https://auralis3.demo.to.com:8443/config/snmp#

5.4 Push

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 a new MDM command was created 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 are used only to request a 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.

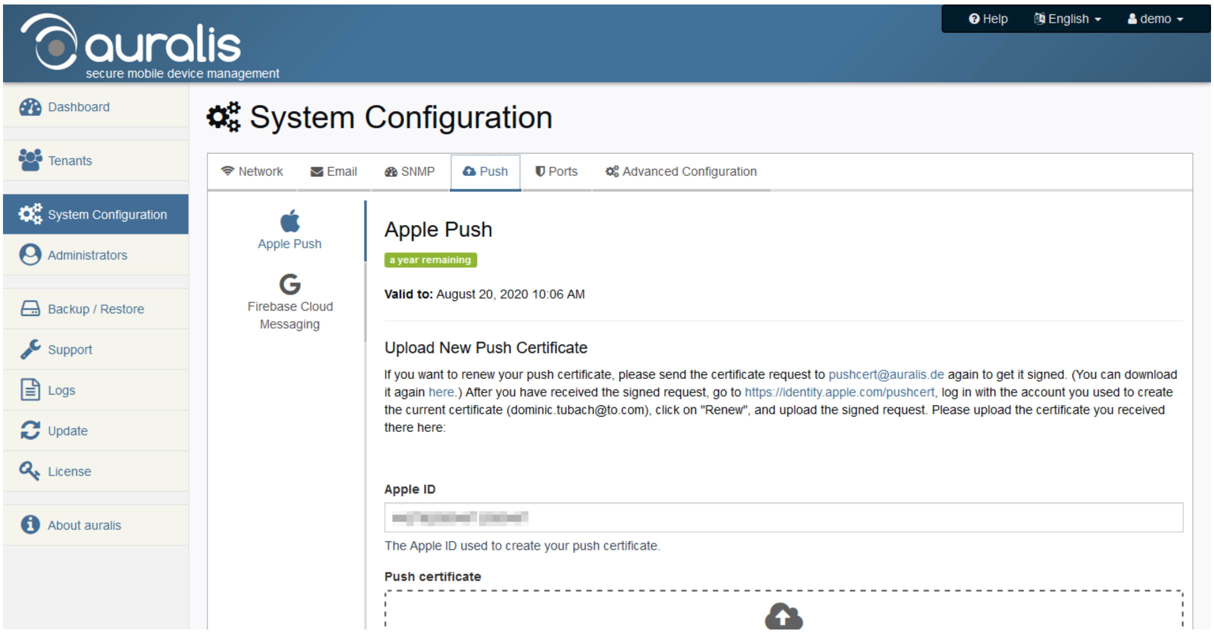
If an Android or iOS device receives no push messages, e.g. due to a failure of the push service, it will not retrieve any MDM commands from auralis. In the auralis app for Android, the retrieval of available commands can be triggered manually in this case. To do so, open the auralis app and press the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

5.4.1 Apple Push

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" to upload the file to auralis. The push certificate is then installed and used for all iOS devices.



System Configuration

Apple Push

a year remaining

Valid to: August 20, 2020 10:06 AM

Upload New Push Certificate

If you want to renew your push certificate, please send the certificate request to pushcert@auralis.de again to get it signed. (You can download it again here.) After you have received the signed request, go to https://identity.apple.com/pushcert, log in with the account you used to create the current certificate (dominic.tubach@to.com), click on "Renew", and upload the signed request. Please upload the certificate you received there here:

Apple ID

[redacted]

The Apple ID used to create your push certificate.

Push certificate

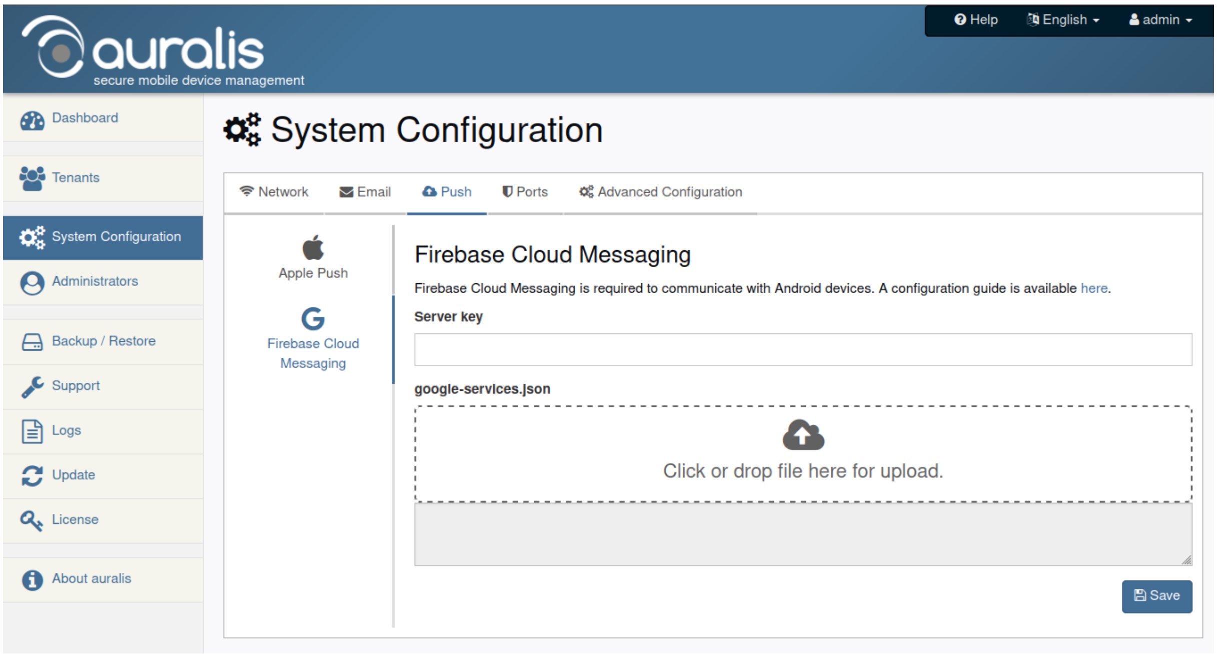
Caution

The certificate is only valid for one year and has to be renewed with the same Apple ID. If a new certificate is generated with another Apple ID, all rolled out iOS devices will lose their MDM connection.

5.4.2 Firebase Cloud Messaging

To access Firebase Cloud Messaging, the push service from Google, a server key and a *google-services.json* is needed. You can request this from Google as described here: https://auralis.de/en/fcm.

Enter the server key and load your *google-servies.json*. Then click “Save” to update the configuration.



Firebase Cloud Messaging

Firebase Cloud Messaging is required to communicate with Android devices. A configuration guide is available here.

Server key

google-services.json

Click or drop file here for upload.

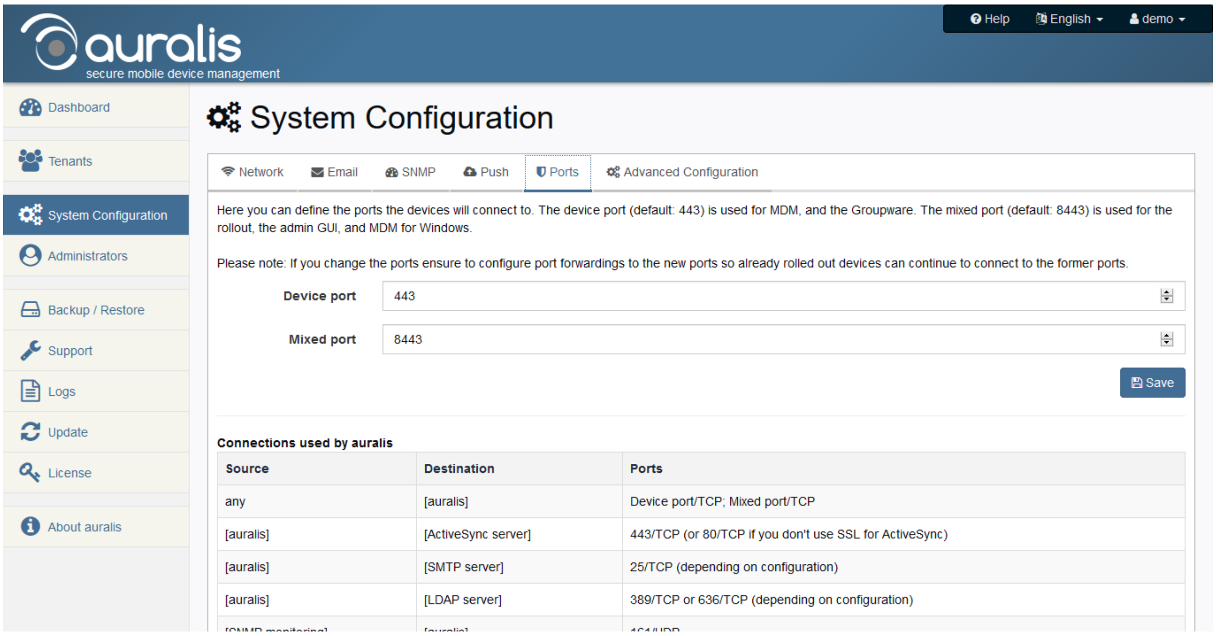
Save

Caution

If you change the server key later, communication between already rolled out Android devices and the MDM is no longer possible.

5.5 Ports

In the ports configuation you can define the ports which are used by auralis. The “Device port” (default: 443) is used for Mobile Device Management (MDM), and the groupware connection. The “Mixed port” (default: 8443) is used for the rollout, the administration GUI and the Simple Certificate Enrollment Protocol (SCEP). Additionally, you can see the firewall rules required for auralis.



System Configuration

Here you can define the ports the devices will connect to. The device port (default: 443) is used for MDM, and the Groupware. The mixed port (default: 8443) is used for the rollout, the admin GUI, and MDM for Windows.

Please note: If you change the ports ensure to configure port forwardings to the new ports so already rolled out devices can continue to connect to the former ports.

Device port: 443

Mixed port: 8443

Connections used by auralis

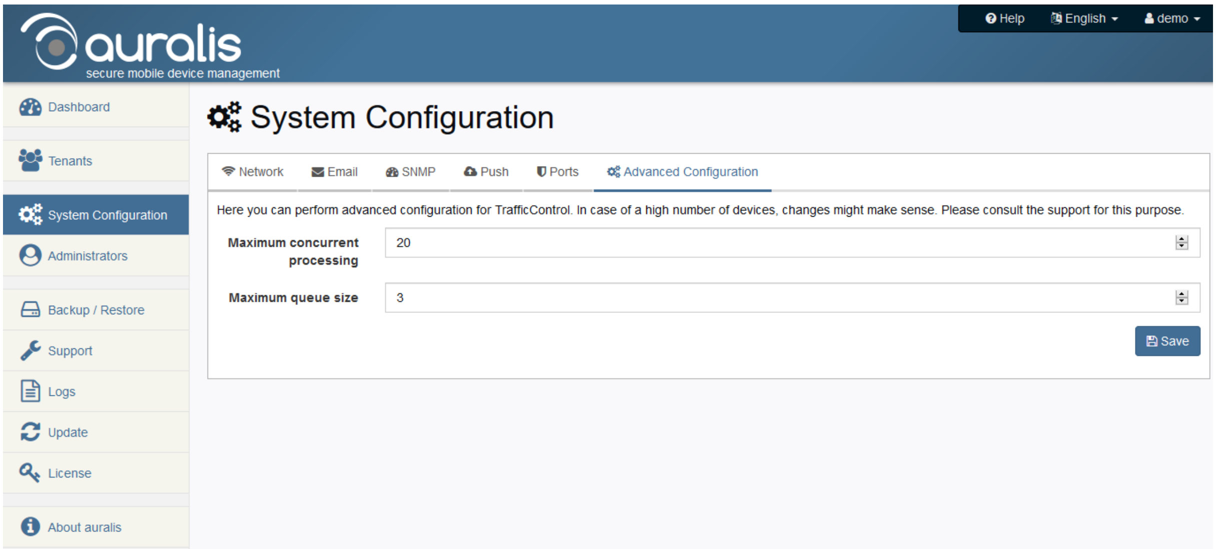
Source	Destination	Ports
any	[auralis]	Device port/TCP; Mixed port/TCP
[auralis]	[ActiveSync server]	443/TCP (or 80/TCP if you don't use SSL for ActiveSync)
[auralis]	[SMTP server]	25/TCP (depending on configuration)
[auralis]	[LDAP server]	389/TCP or 636/TCP (depending on configuration)
[SNMP monitoring]	[auralis]	161/UDP

Note

If you change the ports make sure via port forwarding that devices already rolled out can still reach the previous ports.

5.6 Advanced Configuration

In the advanced configuration you can change the maximum concurrent processing and maximum queue size of TrafficControl. Please consult the support (support@to.com) for this purpose.



System Configuration

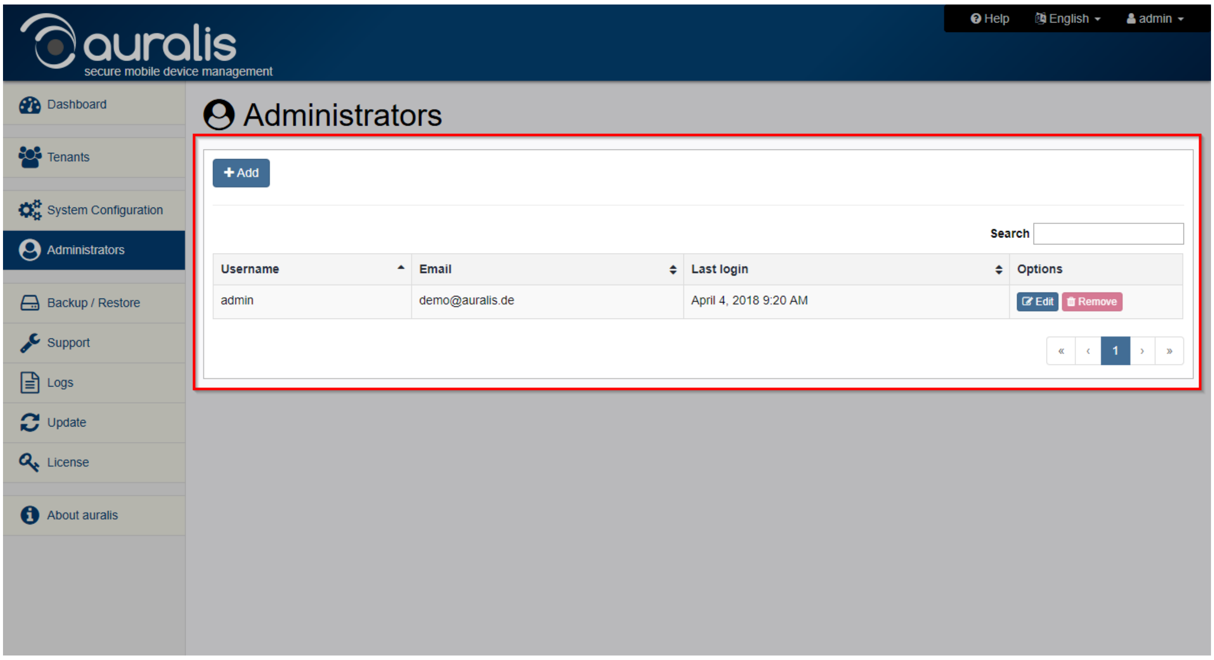
Here you can perform advanced configuration for TrafficControl. In case of a high number of devices, changes might make sense. Please consult the support for this purpose.

Maximum concurrent processing: 20

Maximum queue size: 3

6 Administrators

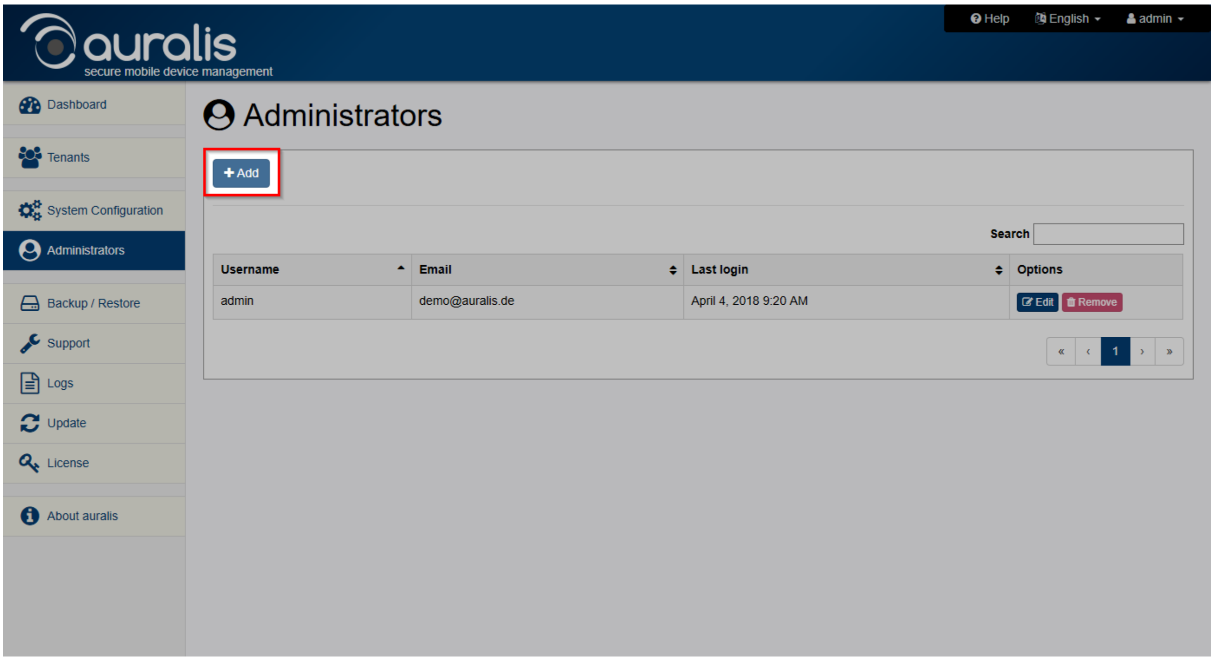
To manage users with administrative privileges click on “Administrators”. A list of administrators is shown. You can create new users and edit or delete existing ones.



Username	Email	Last login	Options
admin	demo@auralis.de	April 4, 2018 9:20 AM	Edit Remove

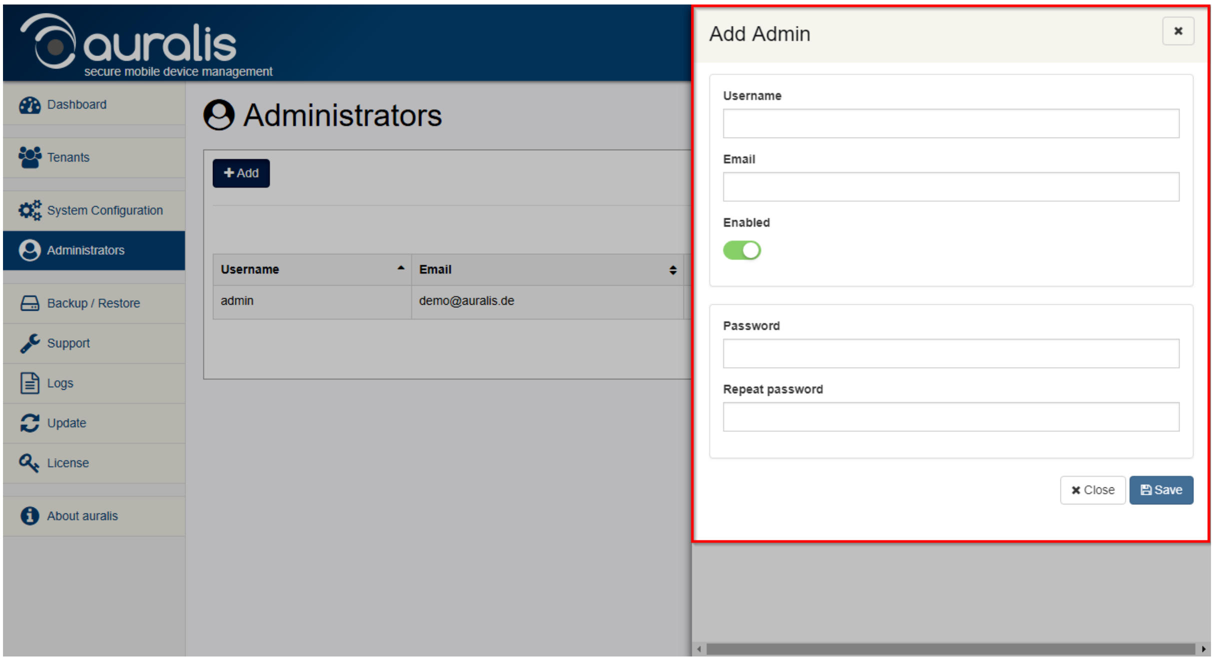
New Administrator

To create a new administrator, click on “Add”.



Username	Email	Last login	Options
admin	demo@auralis.de	April 4, 2018 9:20 AM	Edit Remove

Enter the required data and click “Save”.



Username: The name with which the user can logon to auralis as an administrator.

Email: The email address of the administrator.

Enabled: Allows to enable or disable an administrator account. If an account is deactivated it still exists, but a login isn't possible, anymore.

Password: The password for the administrator.

Repeat password: Repeat the password entered before.

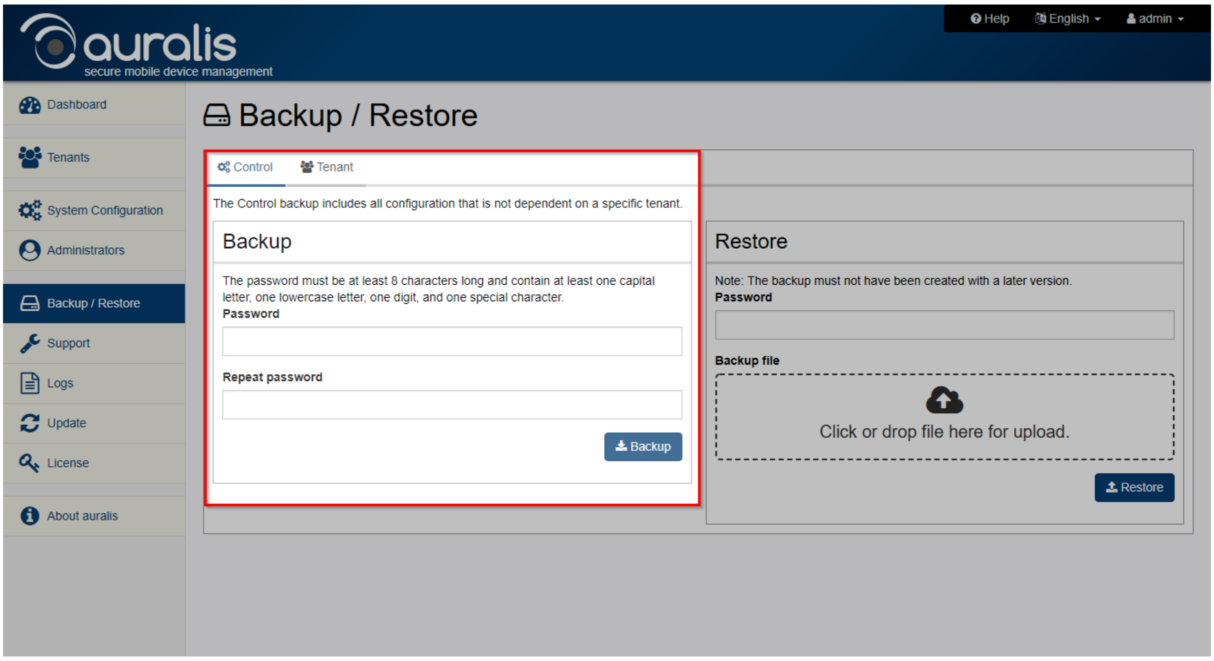
Click on "Save" to add the administrator. With a click on "Close" you can close the dialog.

7 Device rollout

Ensure that you have at least one tenant and created a device to roll out. Then follow the steps under https://auralis.de/en/rollout to connect the device to the corporate network.

8 Backup / Restore

8.1 Control



The Control backup includes all configuration that is not dependent on a specific tenant.

Backup

The password must be at least 8 characters long and contain at least one capital letter, one lowercase letter, one digit, and one special character.

Password

Repeat password

Restore

Note: The backup must not have been created with a later version.

Password

Backup file

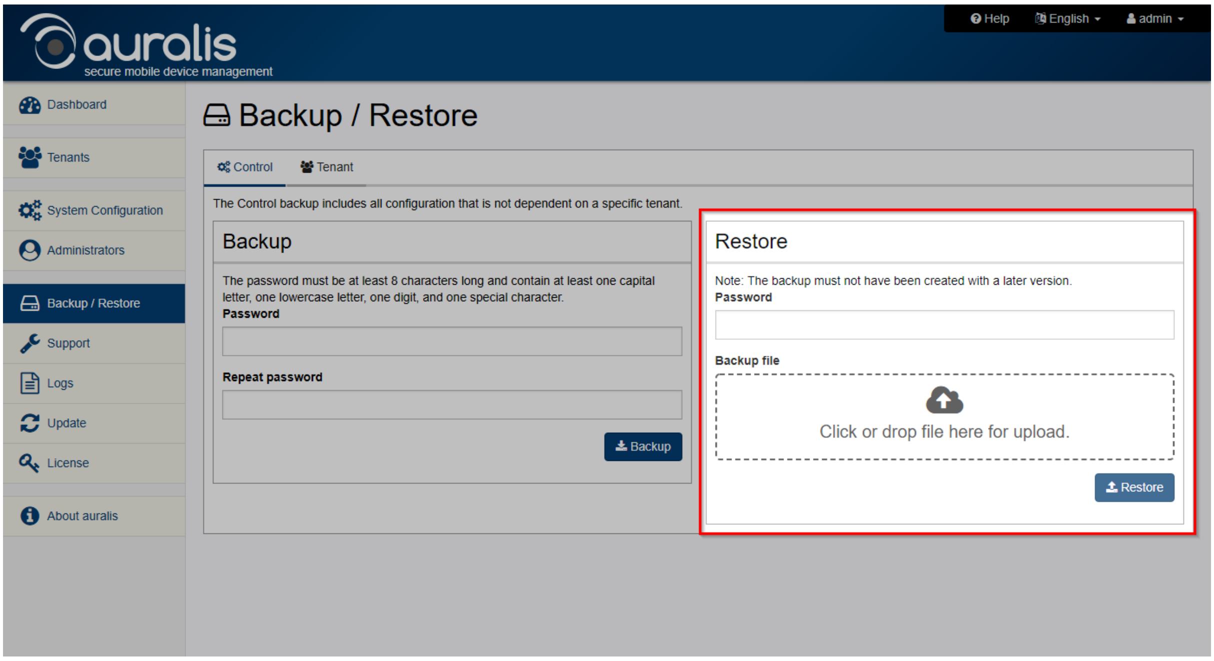
Click or drop file here for upload.

A backup of auralis Control allows you to create a manual backup of your configuration. This backup contains all tenant independent settings that you can configure in auralis Control (apart from the network interface configuration). To create a backup you need to enter a sufficient complex password. The password requirements are described above the password field. Click on “Backup” to start the backup process. The backup will be offered as download.

Restore

> ***Note***
>
> The backup must not have been created with a later version of auralis.

To restore a previously created backup, chose the backup file and enter the appropriate password that you have used to create the backup. A click on “Restore” will start the restoration process.



Backup / Restore

The Control backup includes all configuration that is not dependent on a specific tenant.

The password must be at least 8 characters long and contain at least one capital letter, one lowercase letter, one digit, and one special character.

Password

Repeat password

Note: The backup must not have been created with a later version.

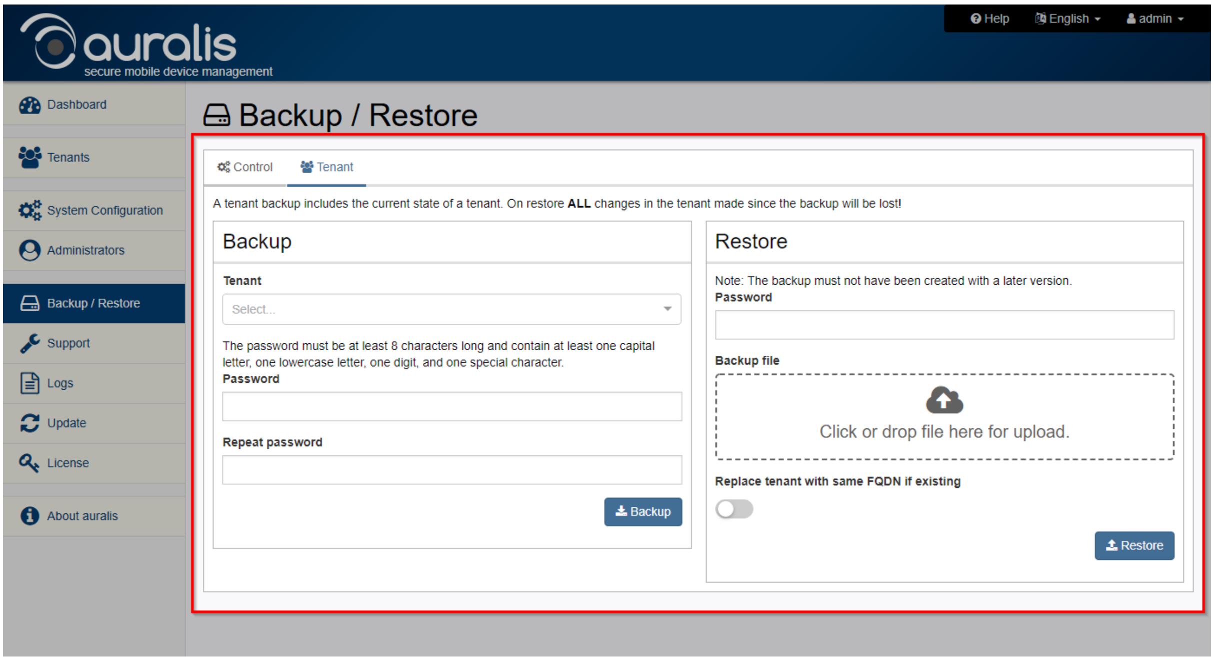
Password

Backup file

8.2 Tenant

The backup of a tenant is basically similar to the backup of auralis Control.

Chose the tenant of which you want to create a backup. Enter a backup password and then click on “Backup”. The backup of the chosen tenant will be offered as download.



Backup / Restore

A tenant backup includes the current state of a tenant. On restore **ALL** changes in the tenant made since the backup will be lost!

Tenant

The password must be at least 8 characters long and contain at least one capital letter, one lowercase letter, one digit, and one special character.

Password

Repeat password

Note: The backup must not have been created with a later version.

Password

Backup file

Replace tenant with same FQDN if existing

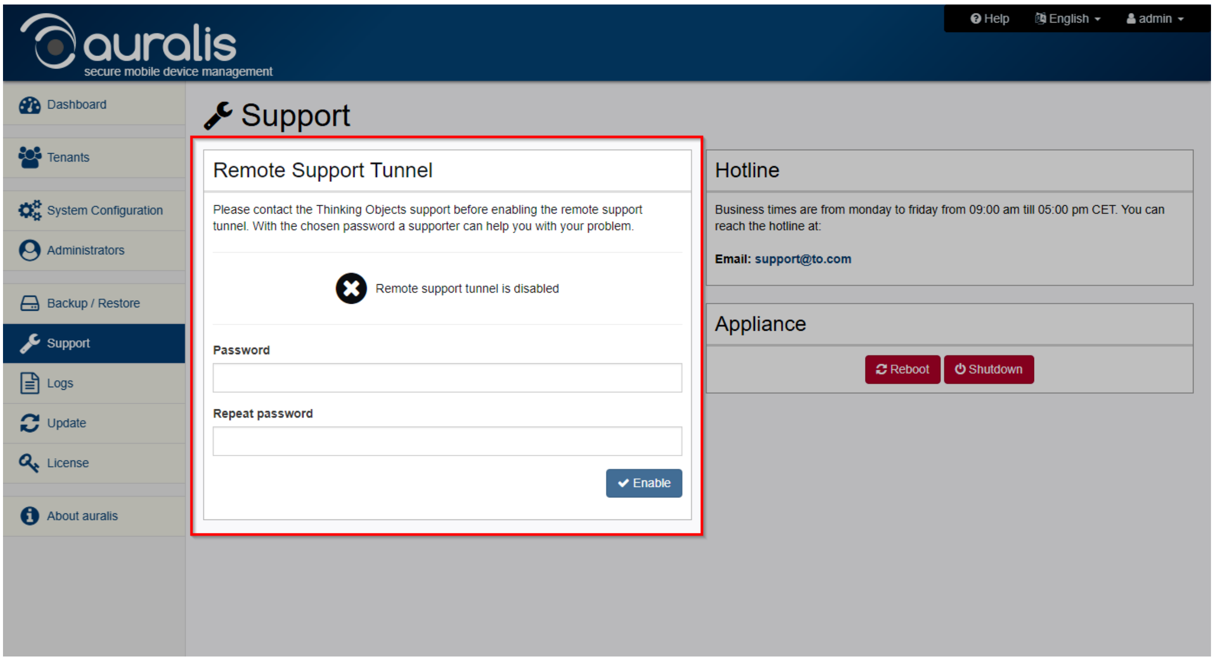
Caution

All changes made in a tenant will be lost on restore. (The option to replace an existing tenant with the same Fully Qualified Domain Name needs to be enabled.)

9 Support

Remote Support Tunnel

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



Remote Support Tunnel

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

Remote support tunnel is disabled

Password

Repeat password

Hotline

Business times are from monday to friday from 09:00 am till 05:00 pm CET. You can reach the hotline at:

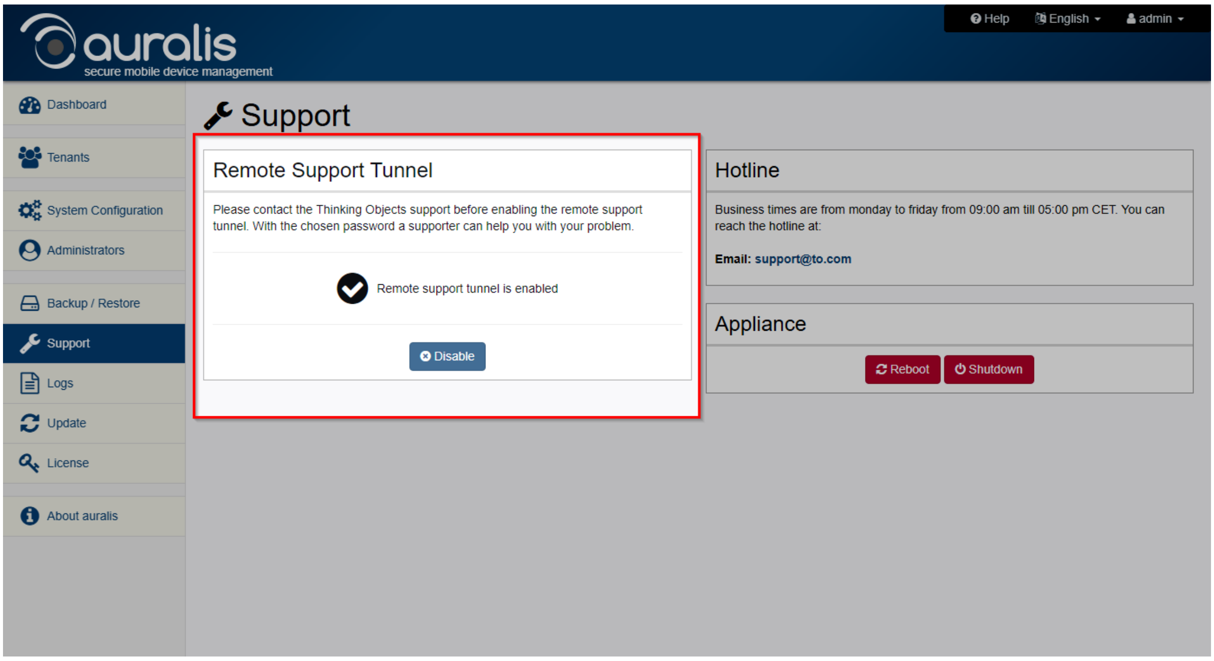
Email: support@to.com

Appliance

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. If you changed the port configuration the hotline needs to now this as well.

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

You can disable the remote support tunnel at any time by clicking on “Disable”.



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

Remote support tunnel is enabled

Business times are from monday to friday from 09:00 am till 05:00 pm CET. You can reach the hotline at:

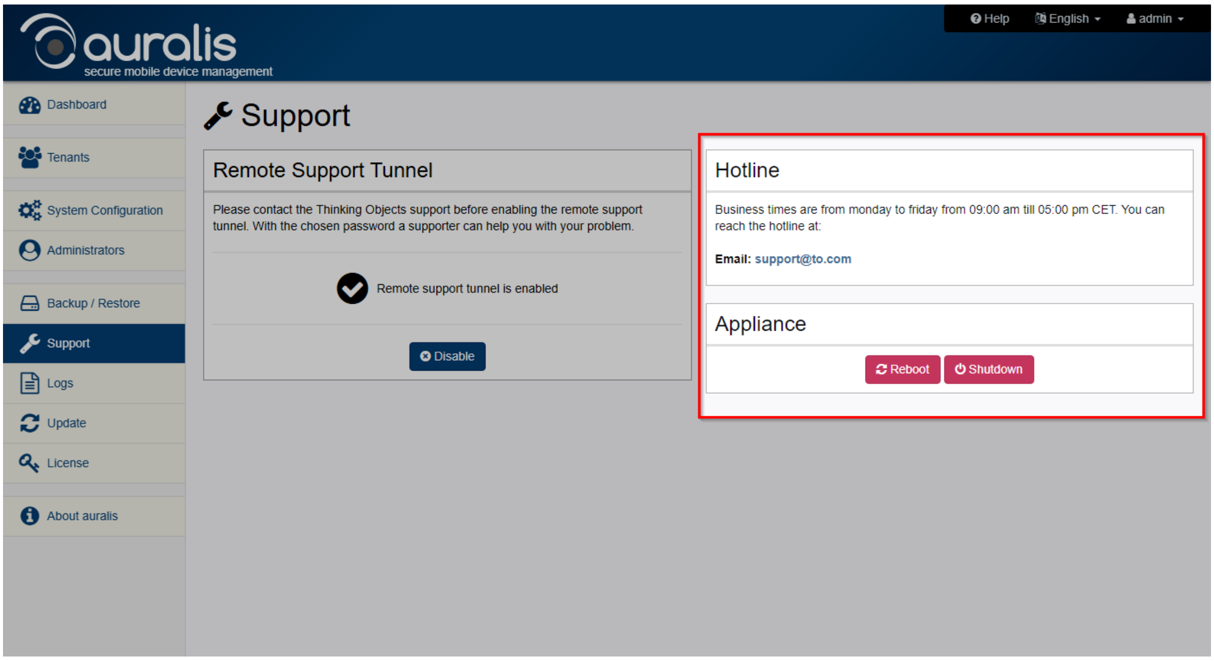
Email: support@to.com

Hotline

This shows the service hours of the Thinking Objects hotline. You can contact the hotline via email at support@to.com.

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 remote support tunnel. With the chosen password a supporter can help you with your problem.

Remote support tunnel is enabled

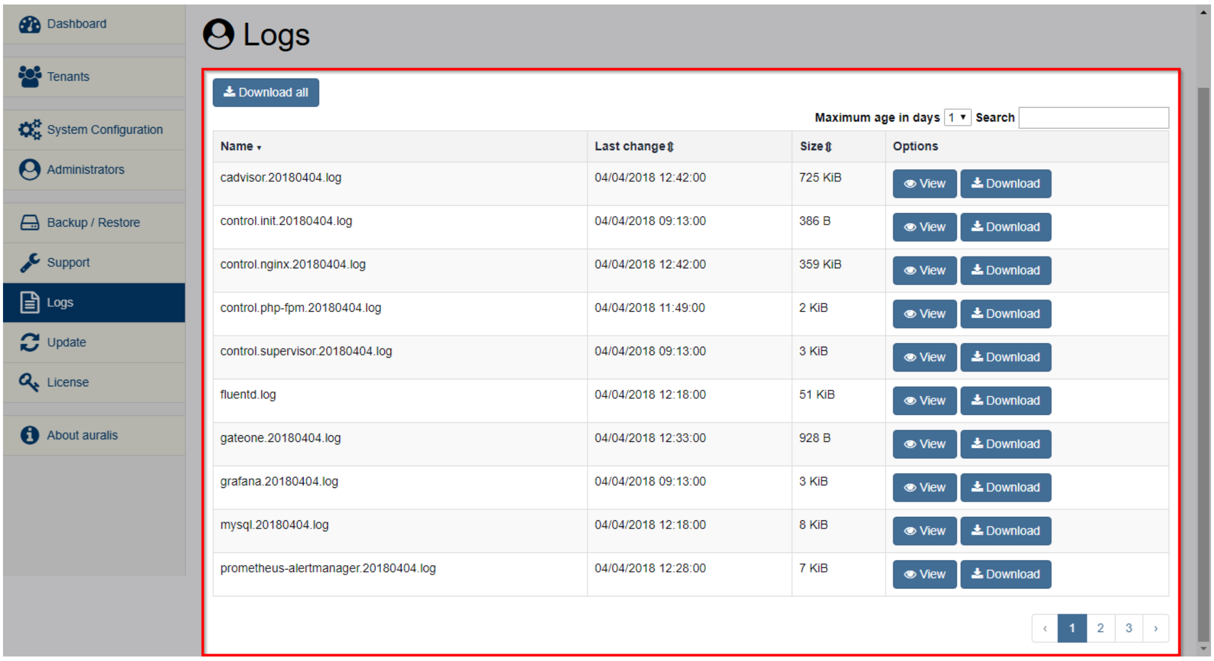
Business times are from monday to friday from 09:00 am till 05:00 pm CET. You can reach the hotline at:

Email: support@to.com

10 Logs

To view a log file, click on “View”. The requested log file will be loaded in a new browser tab. You can download a log file by clicking the “Download” button. The button “Download all” allows you to download all log files collected in an archive.

By changing the value of “Maximum age in days” you can display older log files. The field “Search” allows you to look for log files with a specific name.



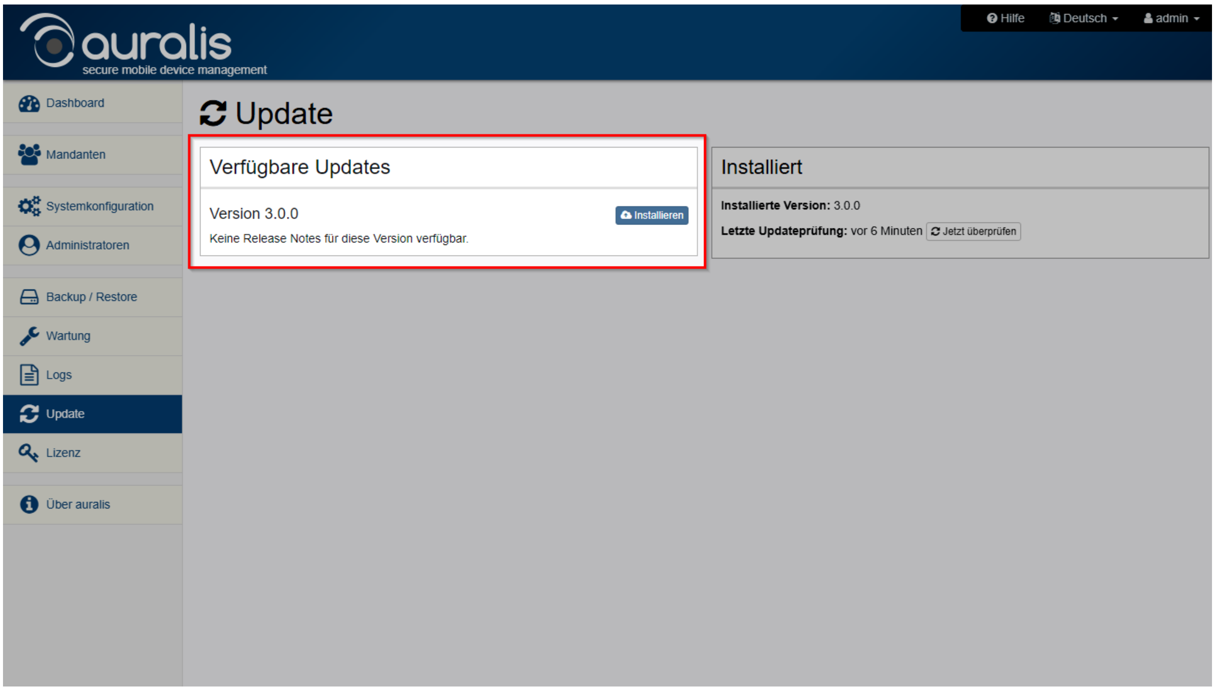
Maximum age in days 1 Search

Name	Last change	Size	Options
cadvisor.20180404.log	04/04/2018 12:42:00	725 KiB	View Download
control.init.20180404.log	04/04/2018 09:13:00	386 B	View Download
control.nginx.20180404.log	04/04/2018 12:42:00	359 KiB	View Download
control.php-fpm.20180404.log	04/04/2018 11:49:00	2 KiB	View Download
control.supervisor.20180404.log	04/04/2018 09:13:00	3 KiB	View Download
fluentd.log	04/04/2018 12:18:00	51 KiB	View Download
gateone.20180404.log	04/04/2018 12:33:00	928 B	View Download
grafana.20180404.log	04/04/2018 09:13:00	3 KiB	View Download
mysql.20180404.log	04/04/2018 12:18:00	8 KiB	View Download
prometheus-alertmanager.20180404.log	04/04/2018 12:28:00	7 KiB	View Download

11 Update

At this point auralis displays information about the current version of auralis and available updates. The button “Check now” on the right side allows you to look for new updates.

If a new version of auralis is available, it is displayed on the left side. You can view the changelog and install the update by clicking on “Install”. Before you install an update you should create a snapshot of your VM or make backups of auralis Control and all tenants.



Update

Verfügbare Updates

Version 3.0.0

Keine Release Notes für diese Version verfügbar.

Installiert

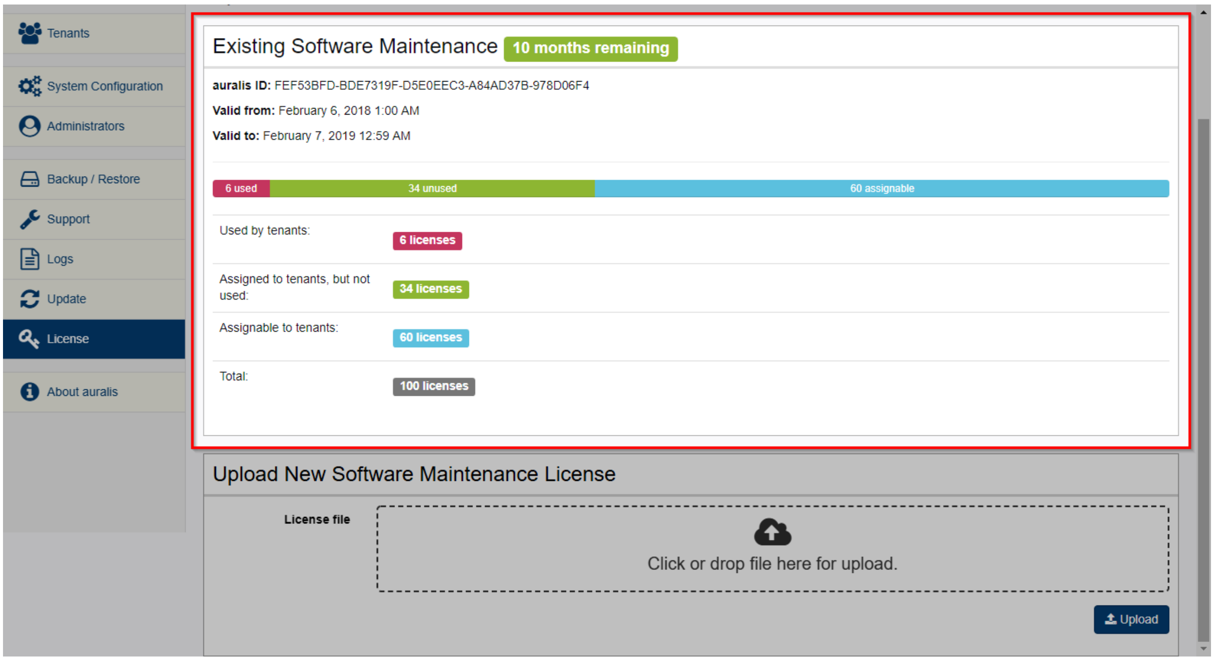
Installierte Version: 3.0.0

Letzte Updateprüfung: vor 6 Minuten

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

12 License management

The view under the menu item “License” shows the details of your installed license.



Existing Software Maintenance 10 months remaining

auralis ID: FEF53BFD-BDE7319F-D5E0EEC3-A84AD37B-978D06F4

Valid from: February 6, 2018 1:00 AM

Valid to: February 7, 2019 12:59 AM

6 used | 34 unused | 60 assignable

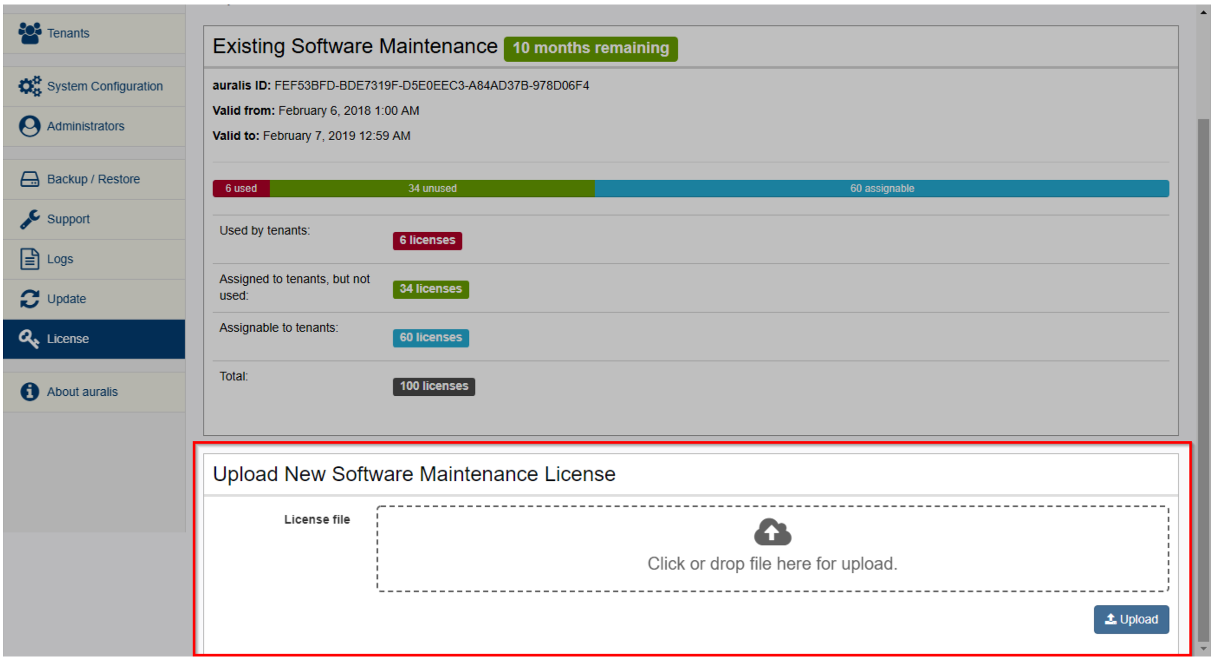
Used by tenants:	6 licenses
Assigned to tenants, but not used:	34 licenses
Assignable to tenants:	60 licenses
Total:	100 licenses

Upload New Software Maintenance License

License file: Click or drop file here for upload.

Upload New Software Maintenance License

To renew your license, or to install a license for the first time, click on the upload field and choose the license file you have received from Thinking Objects. Click on “Upload” to activate the new license.



Existing Software Maintenance 10 months remaining

auralis ID: FEF53BFD-BDE7319F-D5E0EEC3-A84AD37B-978D06F4

Valid from: February 6, 2018 1:00 AM

Valid to: February 7, 2019 12:59 AM

6 used | 34 unused | 60 assignable

Used by tenants: 6 licenses

Assigned to tenants, but not used: 34 licenses

Assignable to tenants: 60 licenses

Total: 100 licenses

Upload New Software Maintenance License

License file: Click or drop file here for upload.

13 Further questions

If you have any further questions or need assistance with the integration, please do not hesitate to contact our support.

It’s 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

Manager:

Markus Klingspor, Michael Föck, Adrian Woizik

Commercial register: Amtsgericht Stuttgart, HRB 19769

VAT REG NO / TAX ID.: DE193103278