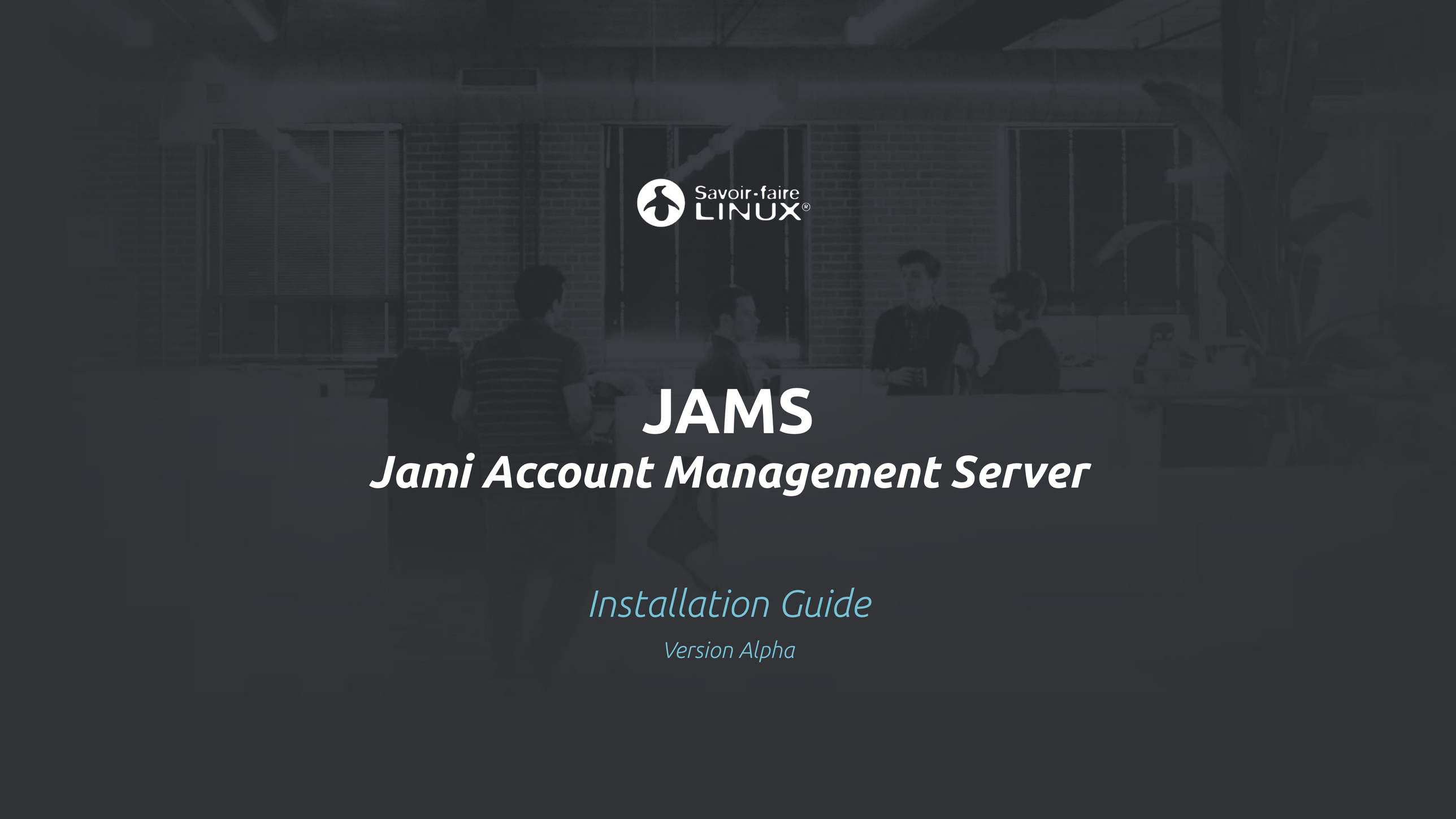


Savoir-faire LINUX®

JAMS

Jami Account Management Server

Installation Guide

Version Alpha

JAMS : Jami Account Management Server

- **Prerequisites**

  - A server available to deploy and run JAMS.

  - A JDK 11+ runtime. It can be downloaded from:
    - https://www.azul.com/downloads/zulu-community/?&version=java-11-lts&os=windows&os-details=Windows&architecture=x86-64-bit&package=jdk
    - or https://www.oracle.com/technetwork/java/javase/downloads/jdk12-downloads-5295953.html

  - If you plan on making the service accessible OUTSIDE your internal network and you want to use HTTPS, you must supply to have a valid domain and a SSL certificate for the domain.

    If you plan on running JAMS behind IIS/Apache/Nginx or any other web-server which already provides an SSL interface, you do not need to supply JAMS with a domain SSL certificate.

  - Some of the features require the existence of a service account in R/O mode on your Active Directory server.

JAMS : Jami Account Management Server

- **Step 1 : JAMS deployment**
  - Launch JAMS
    - Download the latest version of JAMS from https://jami.net/services
    - Open and extract the ZIP file.
    - Open a Terminal.
    - Go in the extracted JAMS folder.
    - Launch JAMS with the command : *java -jar account-management-server-alpha.jar*
    - The installation wizard will automatically open in your web browser.

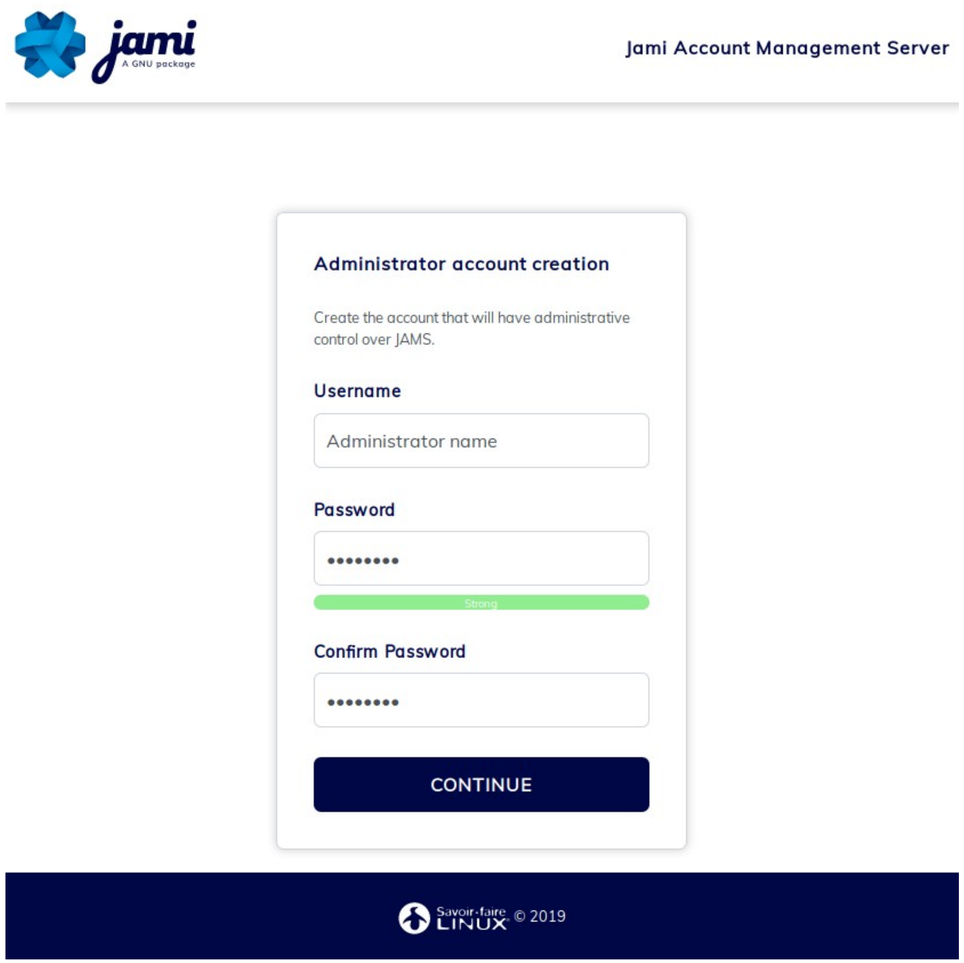
JAMS configuration

- **Step 2 :** administrator account creation

  - This account will have administrative control over JAMS.

  - **Username :** username of the account used to manage Jami users and their associated devices.

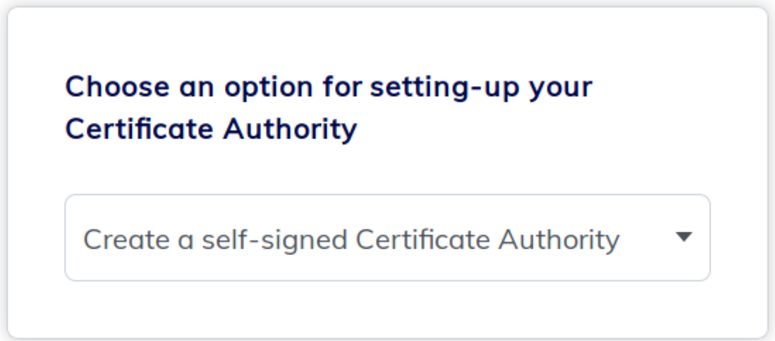
  - **Password :** administrator password required to connect to JAMS.

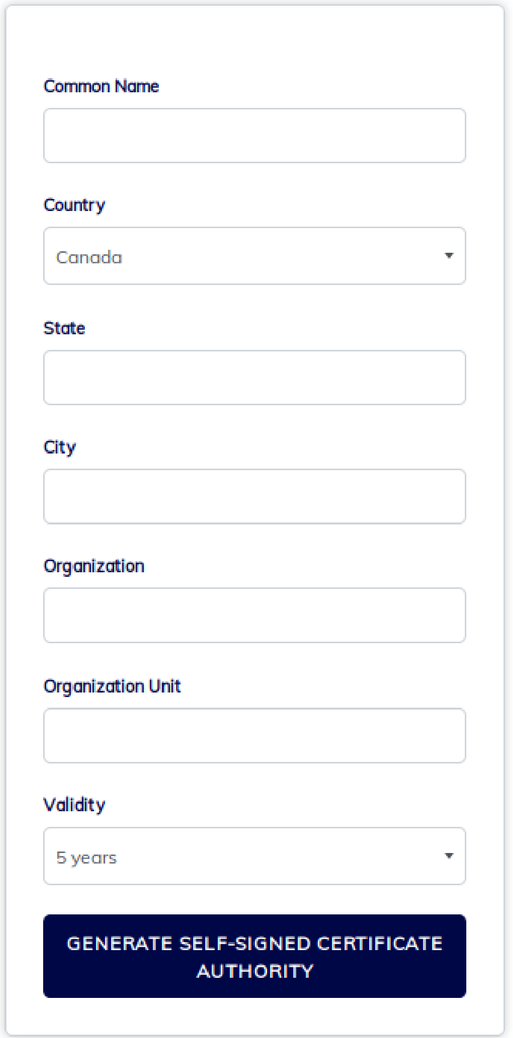


iOS

JAMS configuration

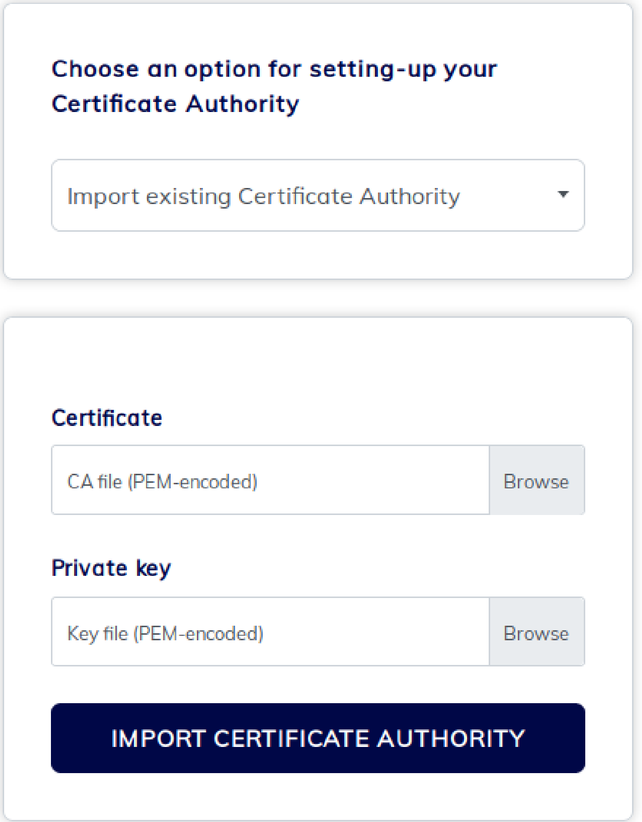
- **Step 3 :** certificate authority (CA) set-up
  - This CA is used to sign all Jami account generated on this JAMS instance. You can either generate a new one or import an existing one.
  - Option 1 : generate self-signed CA
    - To create a self-signed certificate, administrator is requested to provide a name for the certificate and additional information about the organization.
    - The certificate has to be renewed once the validity period is expired.





JAMS configuration

- **Step 3 :** certificate authority (CA) set-up
  - Option 2 : import an existing CA
    - If an organization has an existing certificate (provided by an external provider or issued by the organization itself), the files containing the certificate and the private key can be uploaded here.

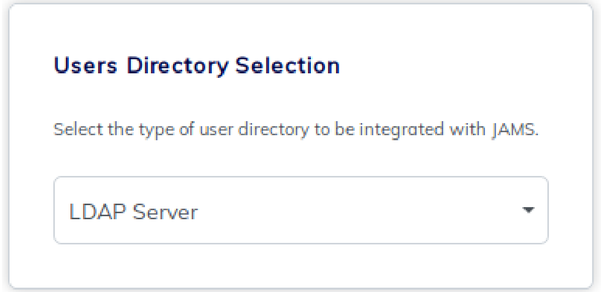


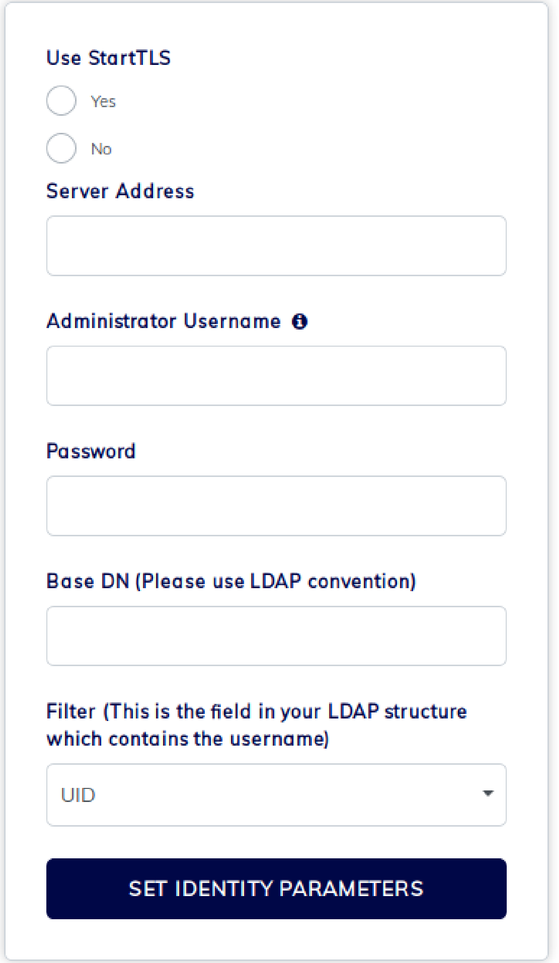
JAMS configuration

- **Step 4 :** users directory selection

  This step allows you to setup the integration of JAMS with your LDAP user registry.

  - **Use StartTLS:** if selected, StartTLS strengthens the authentication and attempts to upgrade an insecure connection to a secure one. It is recommended to activate it.
  - **Server Address:** the domain or IP address and the port of your LDAP server. (ex.: https://example.com:8080)
  - **Administrator Username:** the administrator username of your service account. (ex.: cn=name, ou=unit, dc=domain)
  - **Password:** password linked to the administrator username.
  - **Base DN:** location from where users are searched in the LDAP tree. (ex.: ou=users, dc=organization, dc=com)
  - **Filter:** field which contains the username in the LDAP structure.





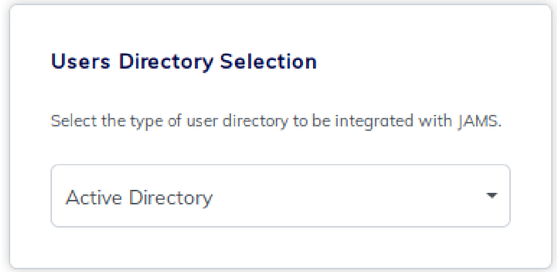
iOS

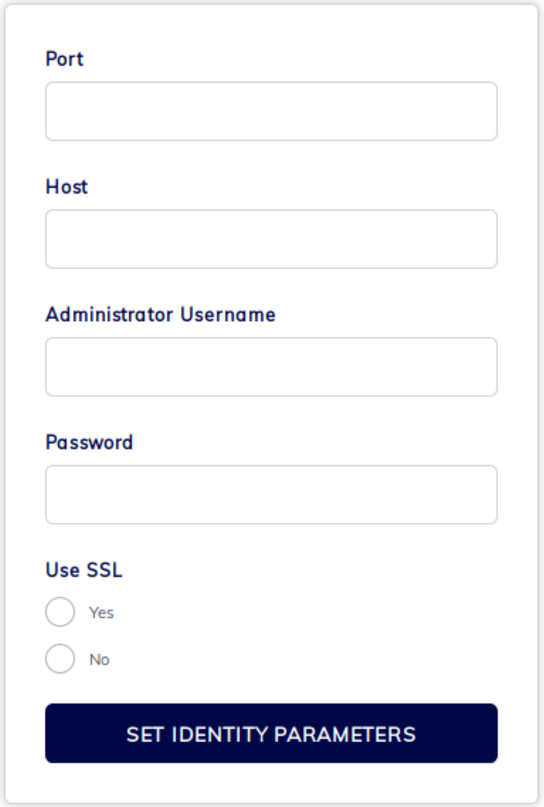
JAMS configuration

- **Step 4 :** users directory selection

This step allows you to setup the integration of JAMS with your Active Directory (AD) user registry. Select Active Directory as User Identity Source.

- **Port:** the port of your AD.
- **Host:** the domain or IP address of your AD.
- **Administrator Username:** the administrator username of your service account. (ex: cn=name, ou=unit, dc=domain)
- **Password:** password linked to the administrator username.
- **Use SSL:** if selected, the use of SSL strengthens the authentication. It is recommended to activate it.





JAMS configuration

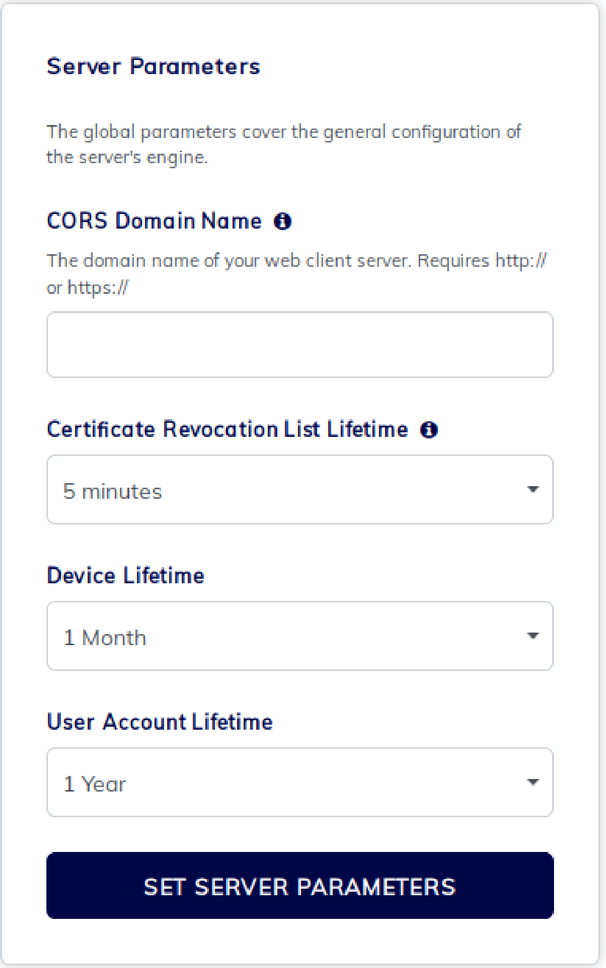
- **Step 5 :** server parameters

  - **CORS domain name:** set the domain of the web client server to connect to the JAMS admin dashboard and Jami accounts. It will also be used to define where the clients should download CRLs and submit OCSP queries. In case you are running a proxied instance (i.e. JAMS behind IIS), please make sure to set this field correctly, otherwise devices will not be able to download CRLs or validate certificates.

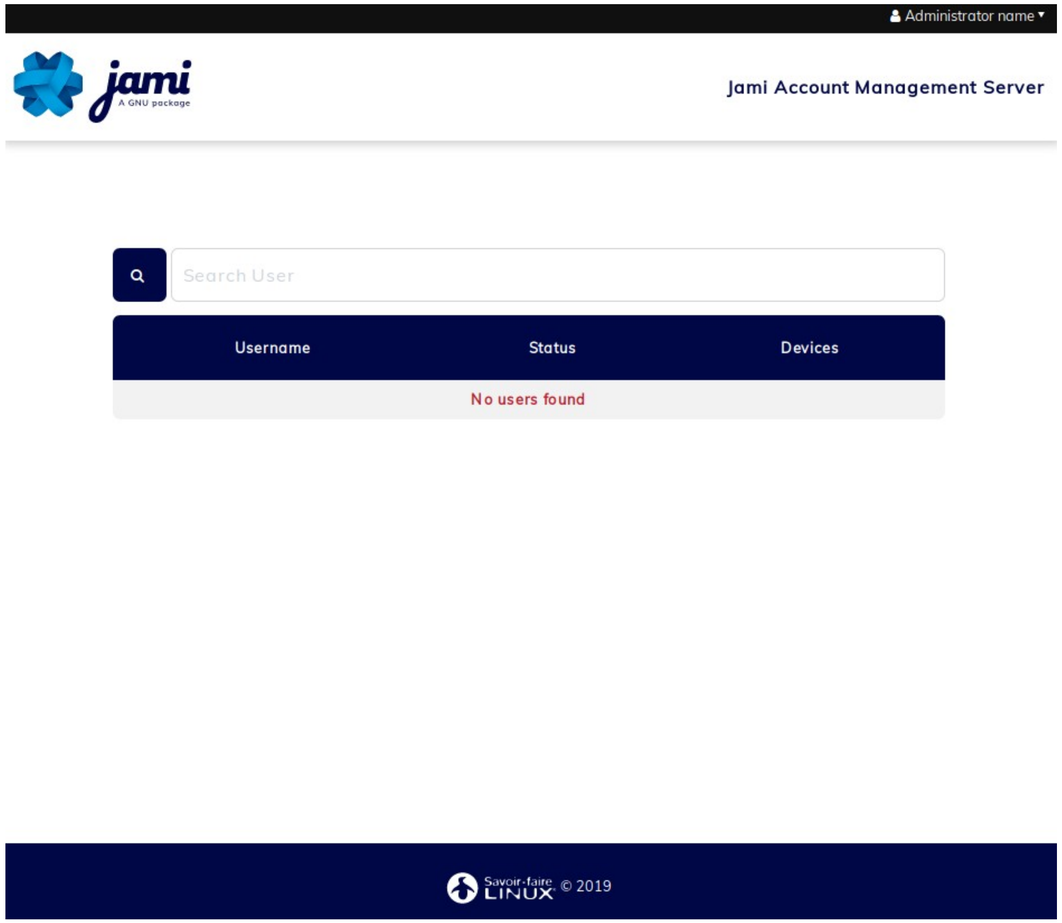
  - **Certificate Revocation List (CRL) Lifetime:** set the lifetime of the CRL which contains the list of the certificates that have been revoked before their scheduled expiration date.

  - **Device Lifetime:** set the lifetime of the user's device certificate.

  - **User Account Lifetime:** set the lifetime of the user account certificate.



JAMS configuration



- **Welcome to JAMS!**

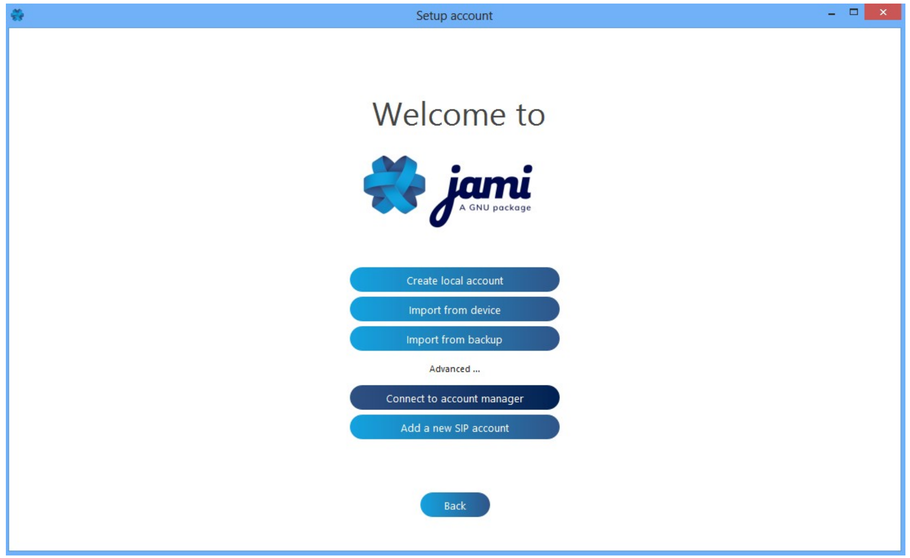
- Once the setup is completed, you will arrive on the JAMS administration page. By default, no users are displayed. Jami accounts will be created as users connect to Jami using their LDAP or AD credentials for the first time.

- You can now invite users to connect to Jami using their corporate credentials and the domain name.

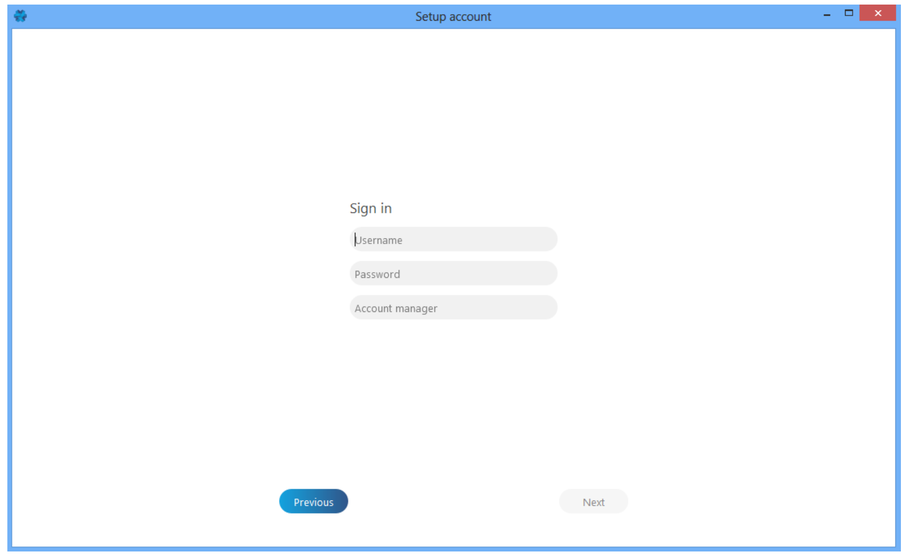
iOS

JAMI connection

- To connect to JAMI with their corporate credentials, users have to select the “Connect to account manager” option available in the advanced options.

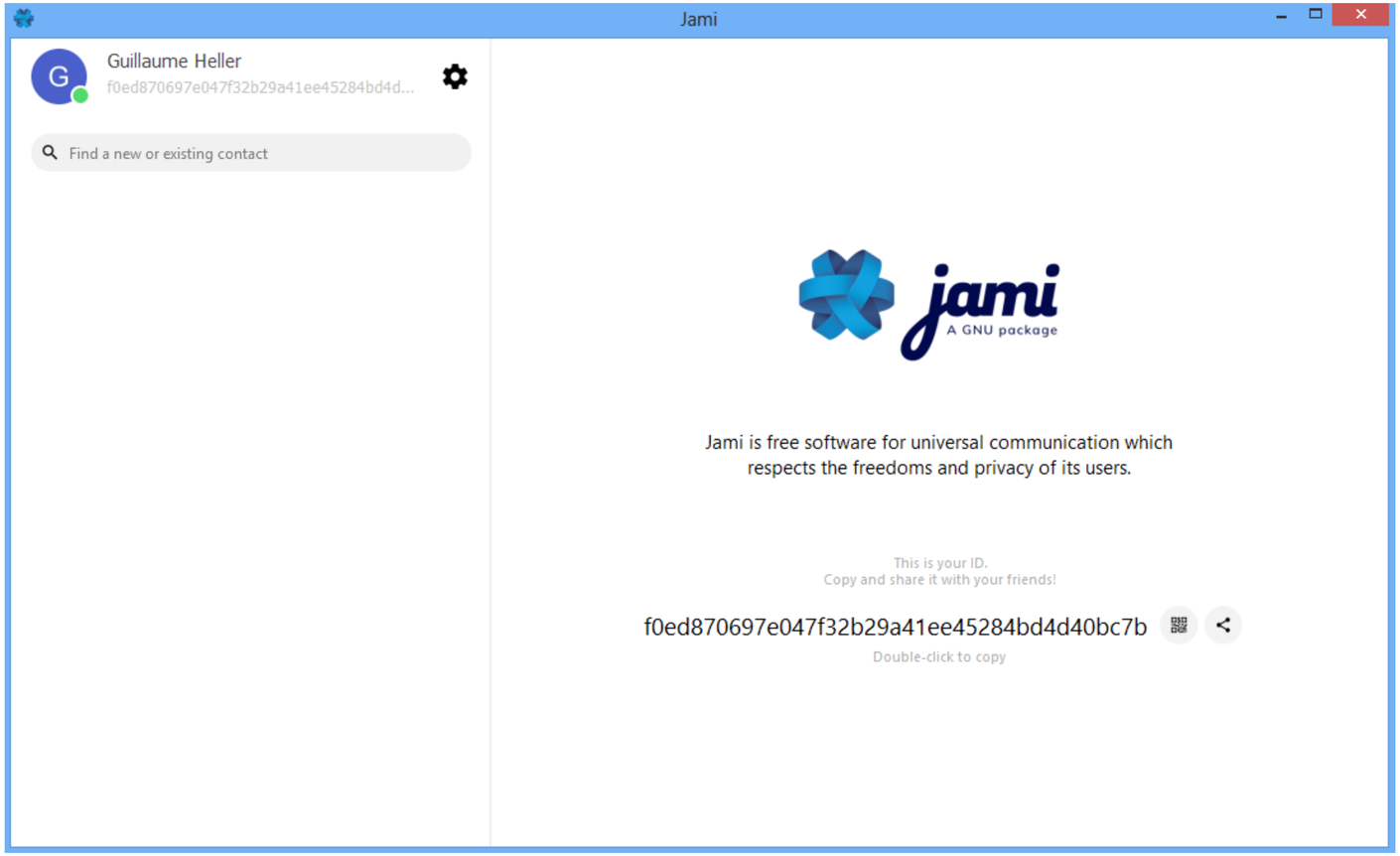


- **Login parameters**
  - **Username:** LDAP or AD (REALM\username) username of the user.
  - **Password:** LDAP or AD password .
  - **Account manager:** address or domain where JAMS is hosted.



iOS

JAMI connection



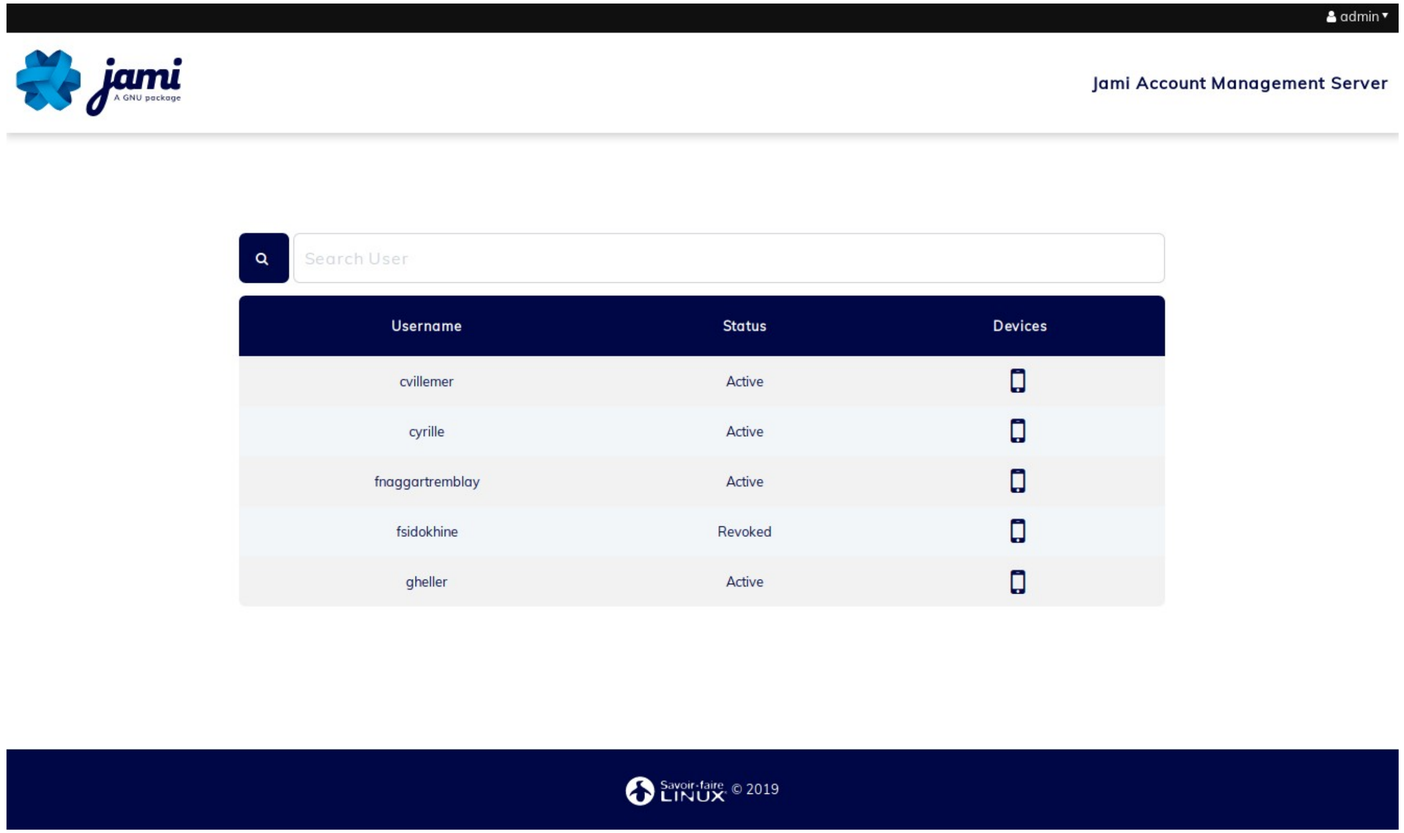
- **You can now start chatting!**

- Use the search bar on the top left to find users from your organization via their username.

iOS

JAMS administration

- JAMS dashboard – available features
  - **Administrator**
    - The administrator can view the list of users who have connected to Jami. For each user, the administrator can see:
      - **Username:** corporate username of the user.
      - **Status:** JAMI status. Active or Revoked.
      - **Devices:** view the list of all devices used by the user to connect to Jami.
  - **Users**
    - Users can also connect to JAMS to view and manage the list of all devices connected to their Jami account.



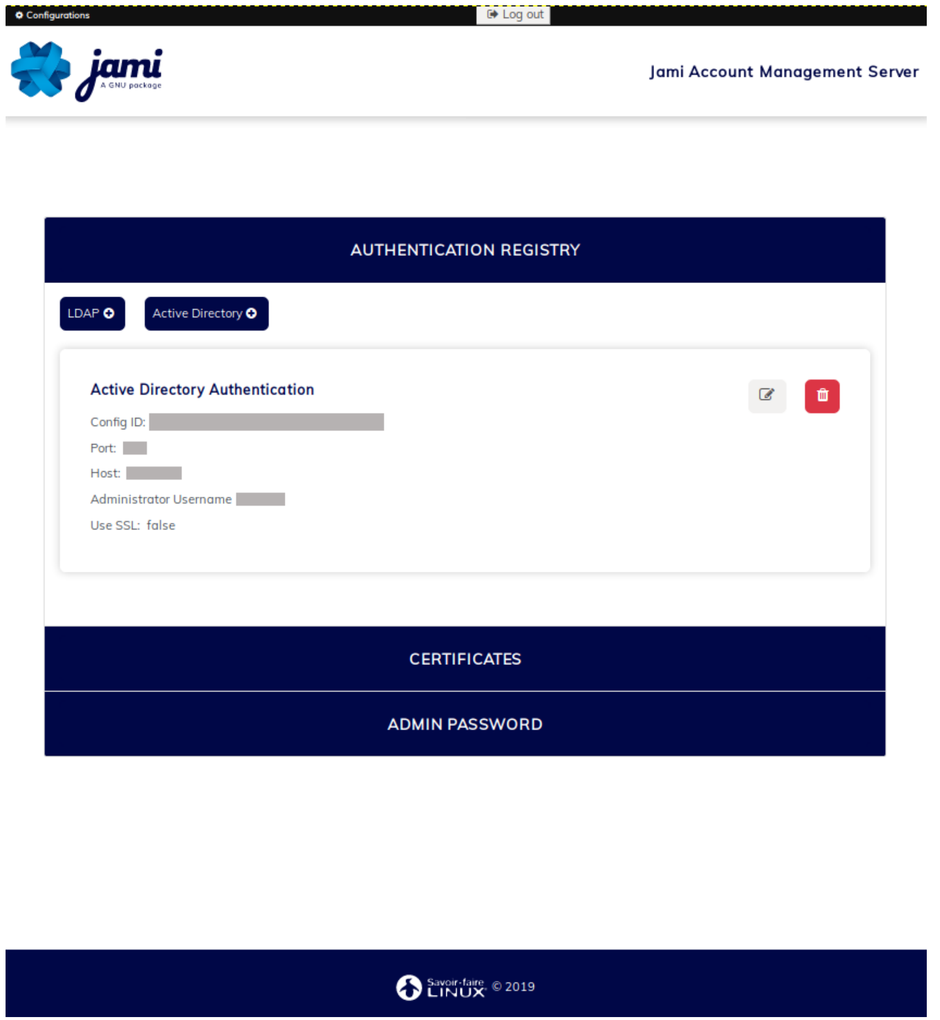
JAMS administration

- JAMS dashboard – available features

  - **Configuration management:** the administrator can view, modify or delete an existing AD/LDAP configuration.

  - Configurations can also be updated directly through the config.json file.

  - **Note**: the server has to be restarted to make the modifications effective .



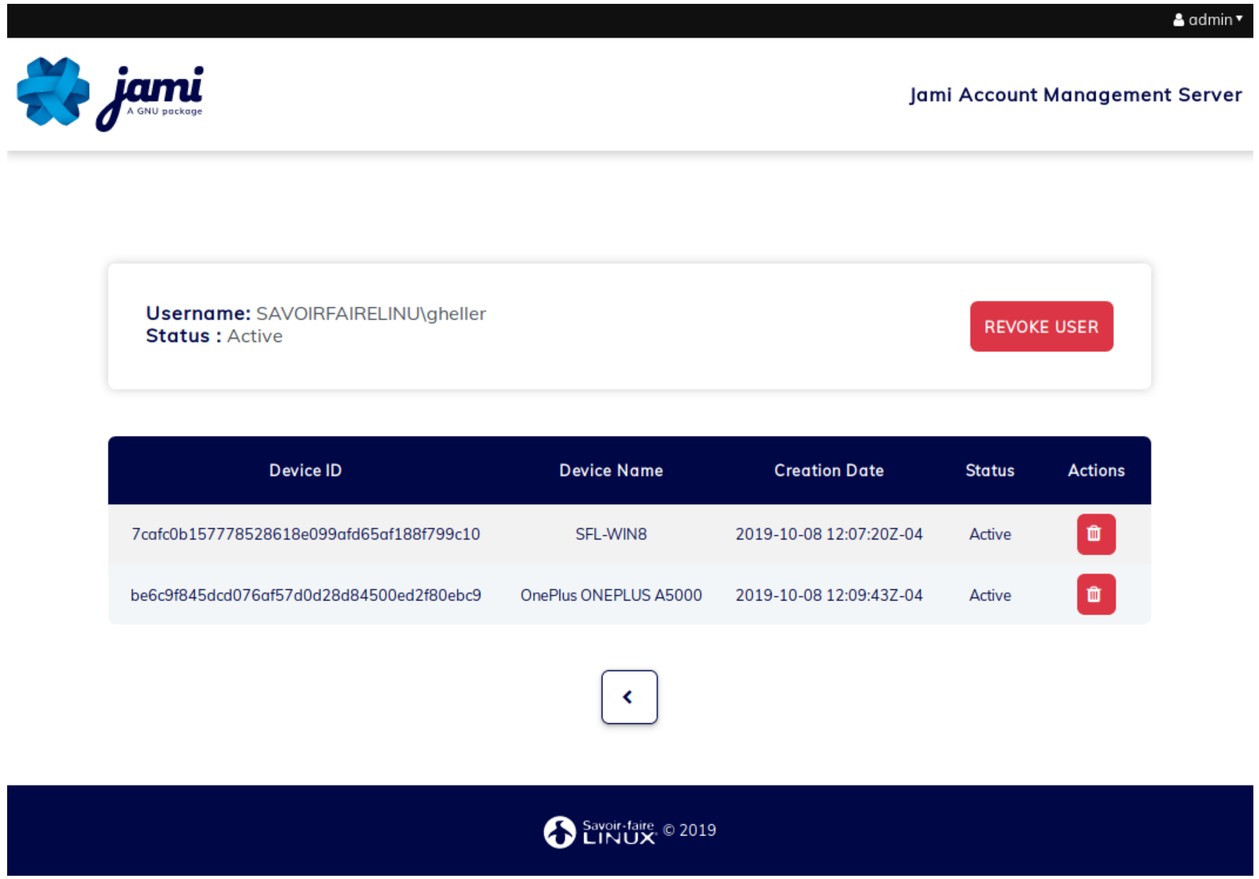
iOS

JAMS administration

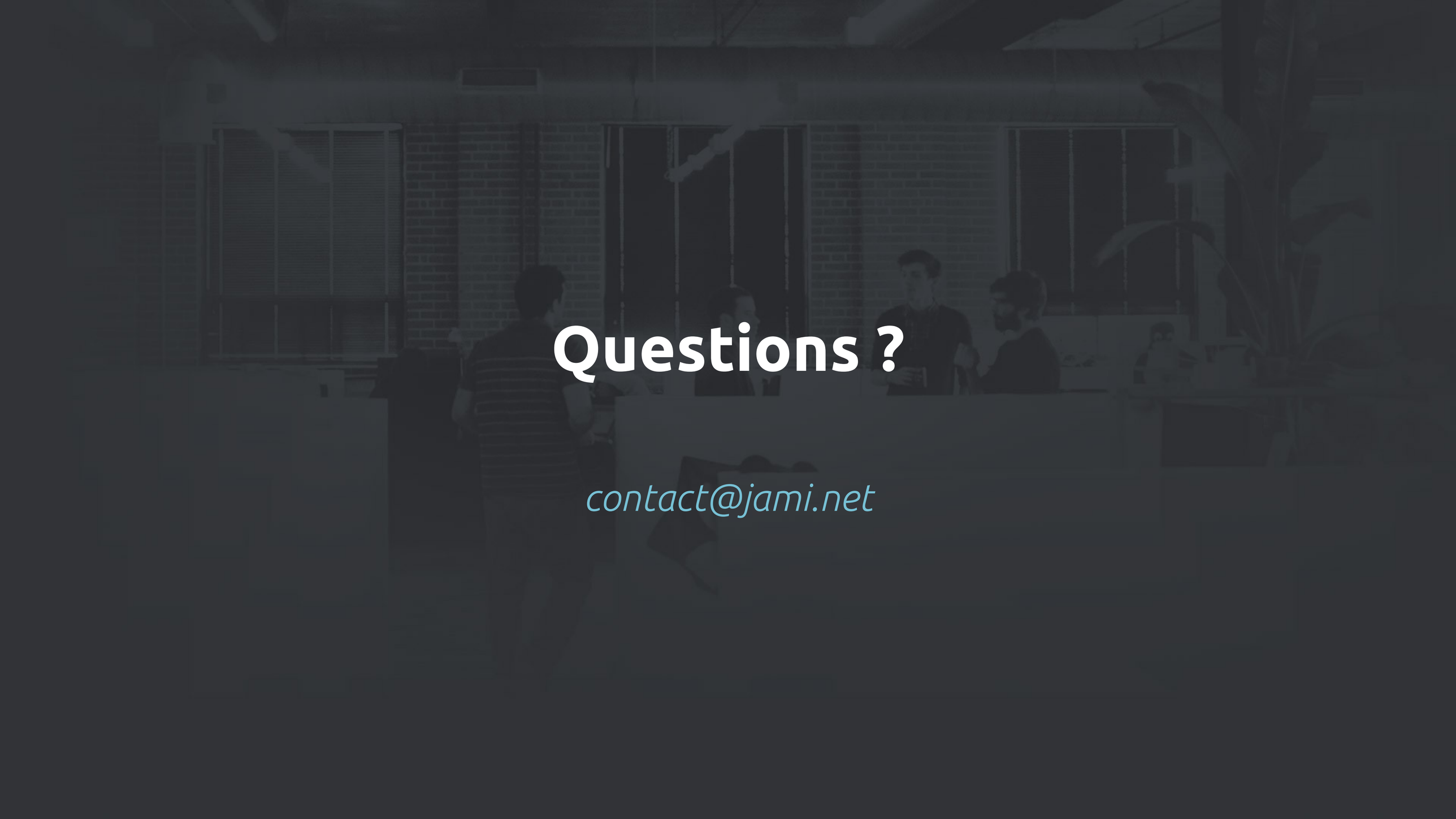
- JAMS dashboard – available soon

- **User management:** the following actions will be available when selecting an user:
  - **Revoke user:** use to completely revoke a user's certificate. Once a user is revoked, he/she can't use Jami to communicate.
  - **Revoke device:** use to revoke a device's certificate. It prevents a user from using Jami with a specific device.

- **Configuration management:** it will be possible for an administrator to view, modify or delete an existing AD/LDAP configuration. In the meantime, configurations can be updated through the config.json file.



iOS



Questions ?

contact@jami.net