



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.



Jami Account Management Server

Administrator account creation

Create the account that will have administrative control over JAMS.

Username

Password

Strong

Confirm Password

CONTINUE

Savoir-faire
LINUX © 2019



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.

Choose an option for setting-up your Certificate Authority

Create a self-signed Certificate Authority ▼

Common Name

Country
Canada ▼

State

City

Organization

Organization Unit

Validity
5 years ▼

GENERATE SELF-SIGNED CERTIFICATE AUTHORITY



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.

Choose an option for setting-up your Certificate Authority

Import existing Certificate Authority ▾

Certificate

CA file (PEM-encoded)

Browse

Private key

Key file (PEM-encoded)

Browse

IMPORT CERTIFICATE AUTHORITY



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.

Users Directory Selection

Select the type of user directory to be integrated with JAMS.

LDAP Server

Use StartTLS

Yes

No

Server Address

Administrator Username ⓘ

Password

Base DN (Please use LDAP convention)

Filter (This is the field in your LDAP structure which contains the username)

UID

SET IDENTITY PARAMETERS



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.

Users Directory Selection

Select the type of user directory to be integrated with JAMS.

Active Directory ▾

Port

Host

Administrator Username

Password

Use SSL

Yes

No

SET IDENTITY PARAMETERS



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.

Server Parameters

The global parameters cover the general configuration of the server's engine.

CORS Domain Name ⓘ

The domain name of your web client server. Requires http:// or https://

Certificate Revocation List Lifetime ⓘ

Device Lifetime


User Account Lifetime

SET SERVER PARAMETERS



JAMS configuration

Administrator name ▾

 **jami**
A GNU package

Jami Account Management Server

Search User

Username	Status	Devices
No users found		

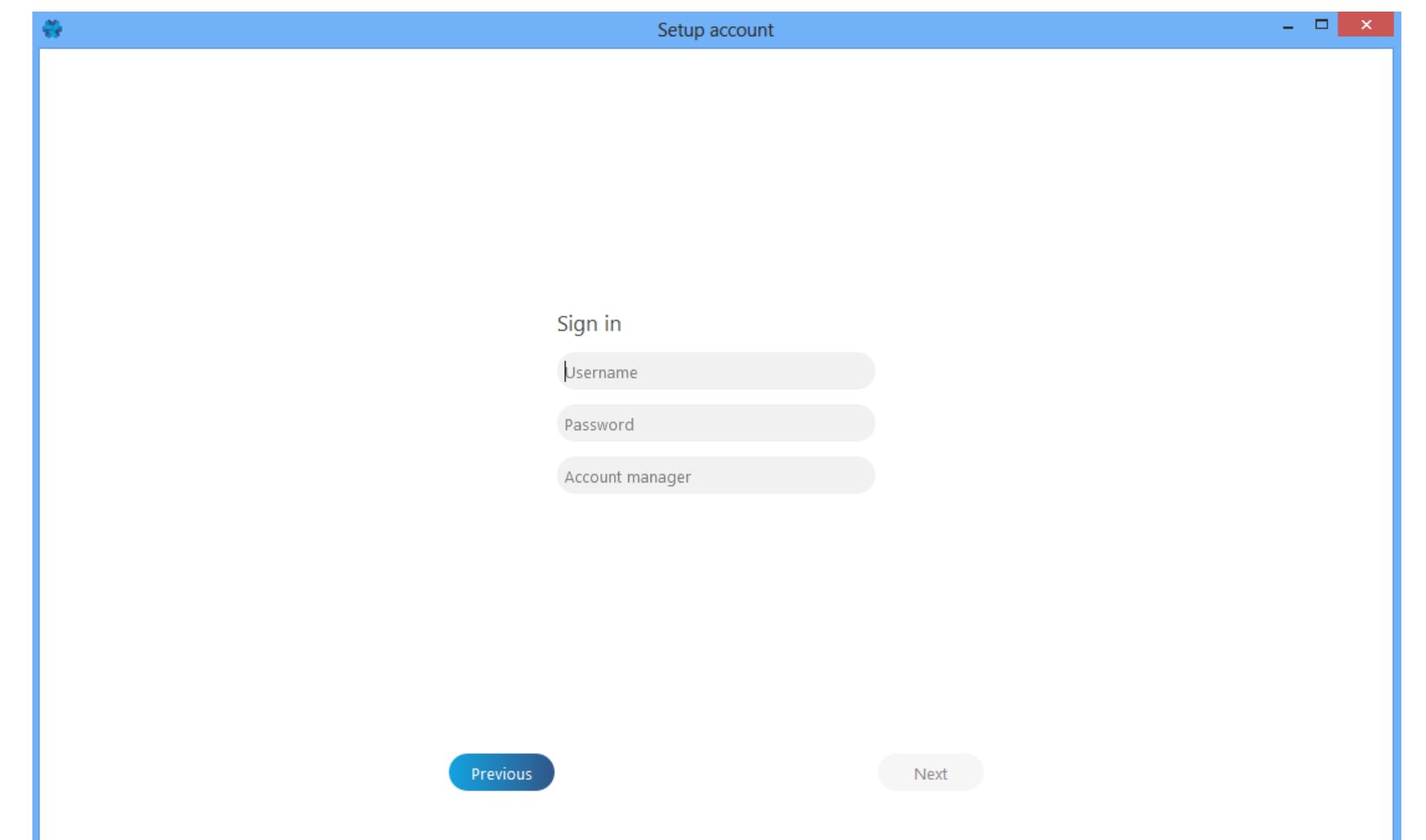
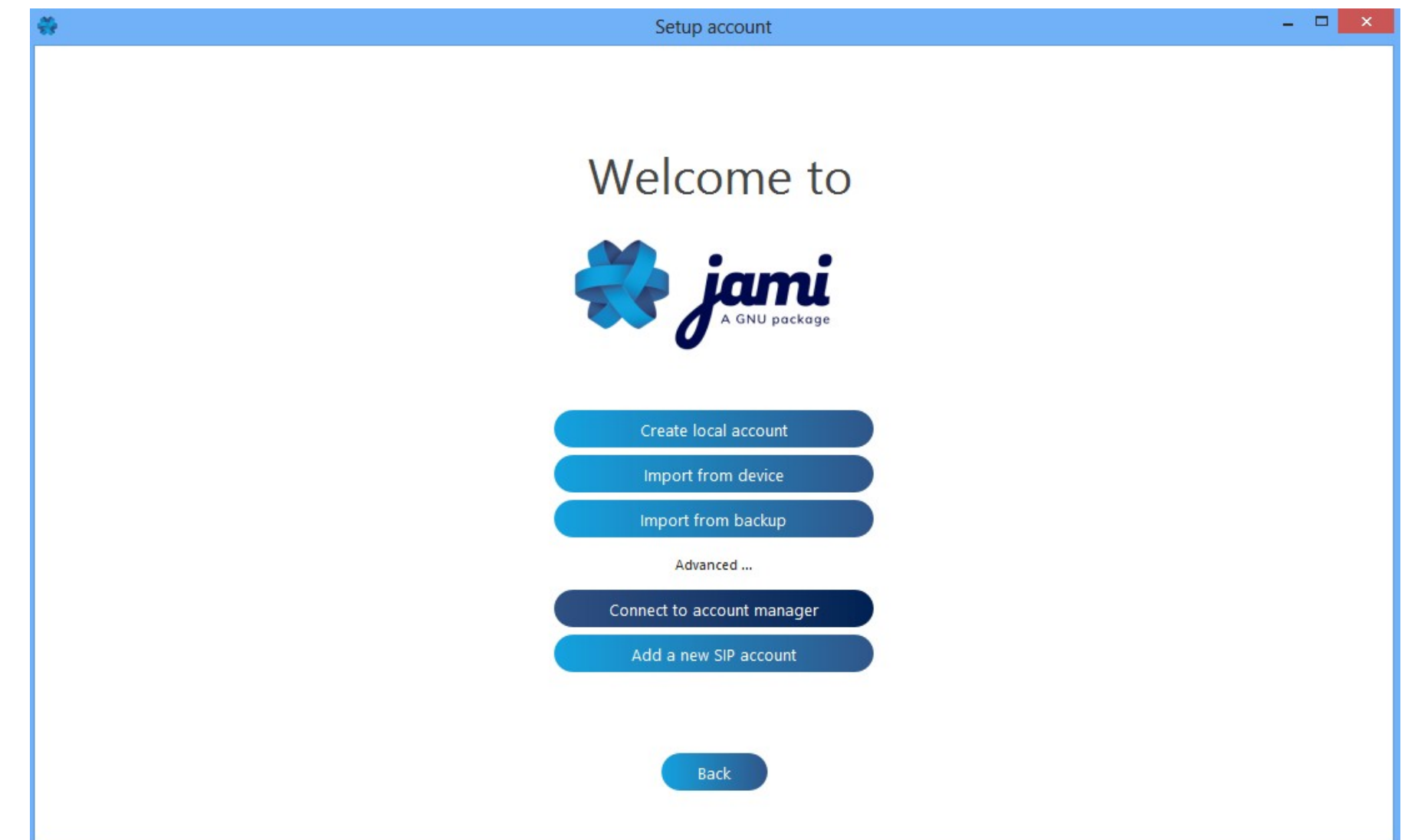
Savoir-faire LINUX © 2019

- ◆ **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.

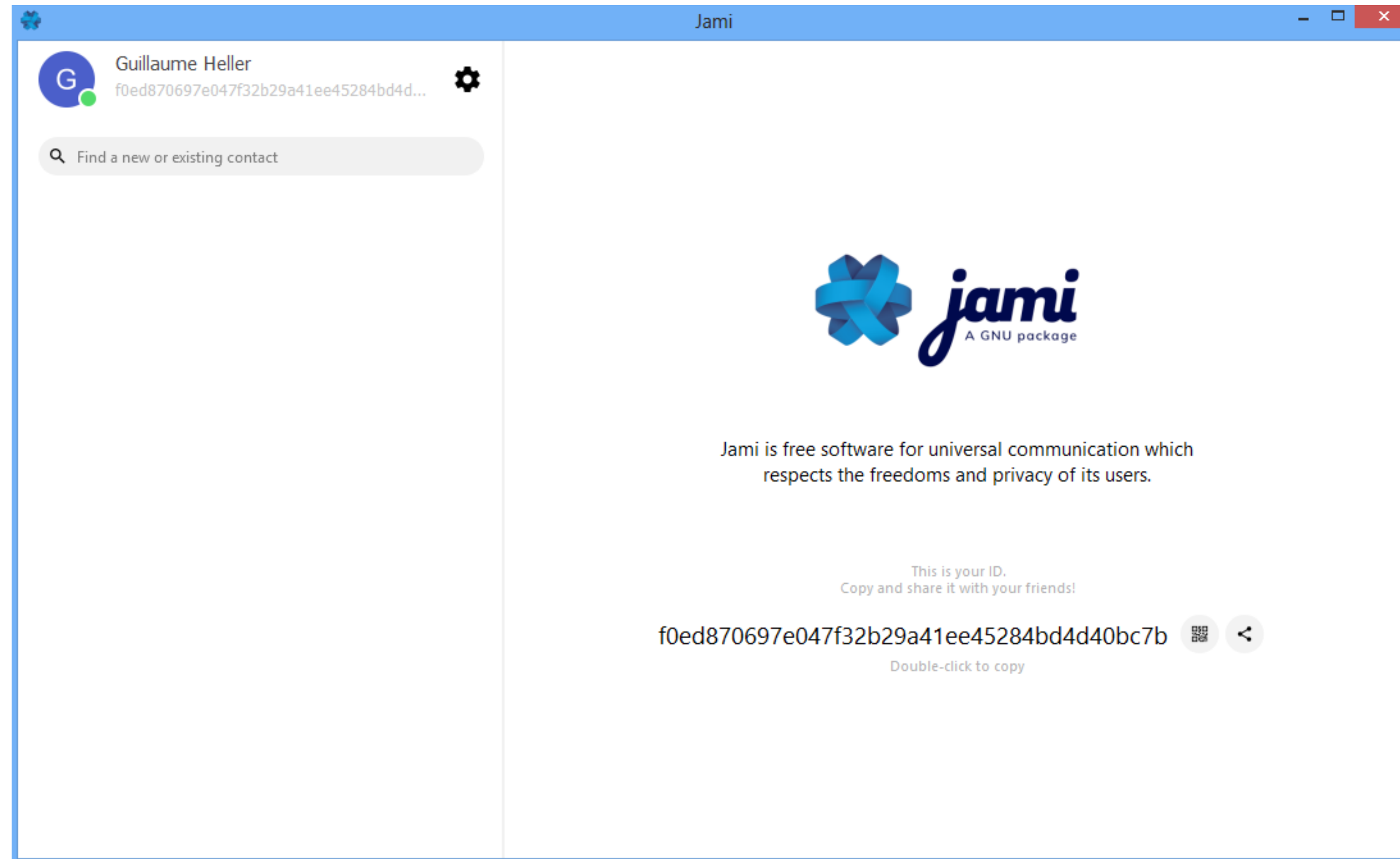


JAMI connection

- ♦ 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.



JAMI connection



- ◆ You can now start chatting!

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



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.

The screenshot shows the JAMS administration interface. At the top right, there is a user profile for 'admin'. The main header features the 'jami' logo (A GNU package) and the text 'Jami Account Management Server'. Below the header is a search bar labeled 'Search User'. A table displays a list of users with columns for Username, Status, and Devices. The table contains five rows of data.

Username	Status	Devices
cvillemer	Active	
cyrille	Active	
fnaggartremblay	Active	
fsidokhine	Revoked	
gheller	Active	

At the bottom of the page, there is a footer with the 'Savoir-faire LINUX' logo and the text '© 2019'.



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 .

The screenshot displays the JAMS administration interface. At the top, there is a navigation bar with 'Configurations' and 'Log out' options. The JAMS logo and 'A GNU package' are on the left, and 'Jami Account Management Server' is on the right. The main content area is titled 'AUTHENTICATION REGISTRY' and features two tabs: 'LDAP' and 'Active Directory'. The 'Active Directory' tab is selected, showing a configuration card for 'Active Directory Authentication'. This card includes fields for 'Config ID', 'Port', 'Host', and 'Administrator Username', along with a 'Use SSL: false' checkbox. Edit and delete icons are visible on the right side of the card. Below the configuration card are three sections: 'CERTIFICATES' and 'ADMIN PASSWORD', each with a dark blue header bar.



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.

admin

jami
A GNU package

Jami Account Management Server

Username: SAVOIRFAIRELINU\gheller
Status : Active

REVOKE USER

Device ID	Device Name	Creation Date	Status	Actions
7cafc0b157778528618e099afd65af188f799c10	SFL-WIN8	2019-10-08 12:07:20Z-04	Active	
be6c9f845dcd076af57d0d28d84500ed2f80ebc9	OnePlus ONEPLUS A5000	2019-10-08 12:09:43Z-04	Active	

<

Savoir-faire LINUX © 2019





Questions ?

contact@jami.net