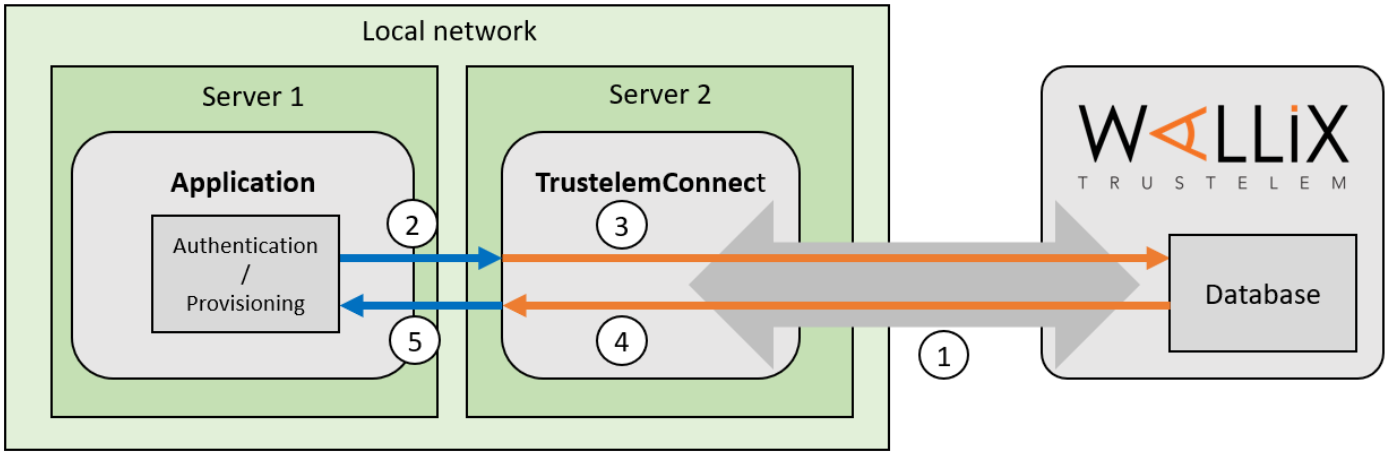
LDAP-Radius

The goal is to use Trustelem database to provision/authenticate users on an application using LDAP or Radius.
To do so, a connector, **TrustelemConnect**, is installed on a server able to contact the application.



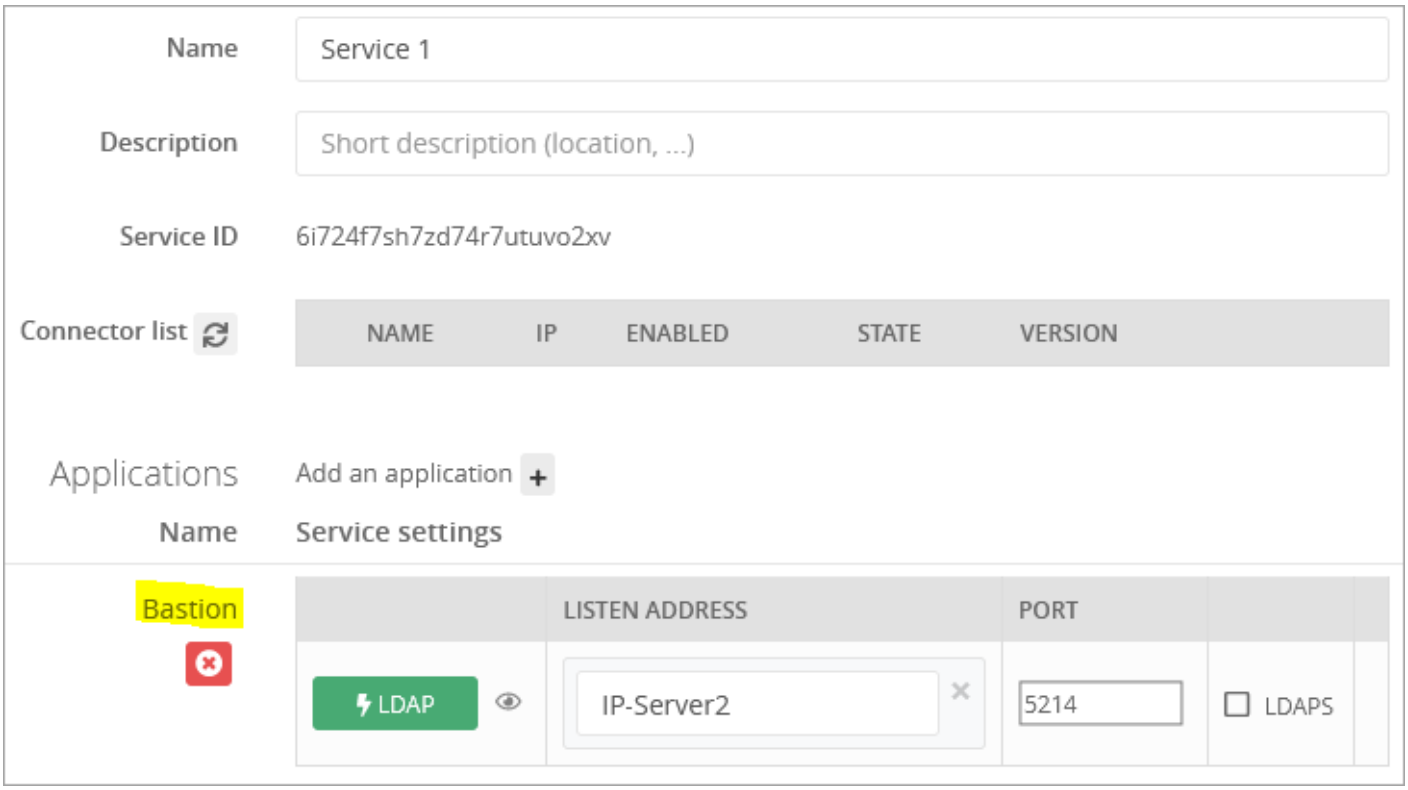
1/ During the setup, **TrustelemConnect** opens a **websocket** to **Trustelem services** using **port 443**.
Note: with the websocket, information is encrypted by TLS protocol and with an additional symmetric encryption.

2/ The application asks about users to **TrustelemConnect** on a specific port (*for example 5214*) using **LDAP or Radius**.

3/ **TrustelemConnect** uses the **websocket** to send to **Trustelem services**:

- the request
- the IP (TrustelemConnect listen address) and port used by the application to contact **TrustelemConnect** (*in our example IP-Server2 and port 5214*)

4/ On Trustelem, the port is associated to a specific application. Trustelem returns to **TrustelemConnect** the users who have an access-rule for this app, using the **websocket**.



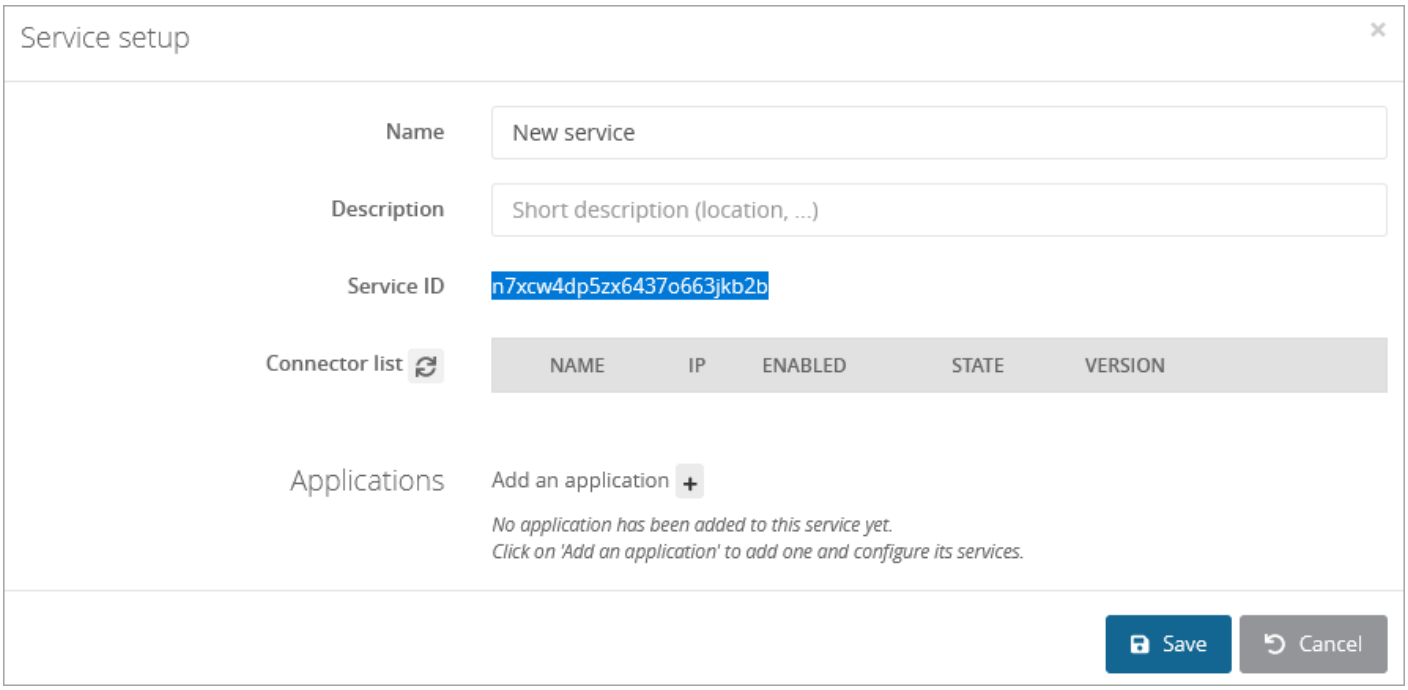
With the example, *IP-Server2* is allowed for *port 5214* so Trustelem returns the information about users who have an access-rule for the application *Bastion*.

5/ **TrustelemConnect** replies to the application using **LDAP or Radius**.

Setup TrustelemConnect

In your Trustelem administration page:

- Go to the **Services** tab.
  `https://admin-mydomain.trustelem.com/app#/services`
  Note: if you don't have access to this feature, please contact WALLIX Trustelem support.
- Click on the button **+ Create a service** and copy the **service ID**.

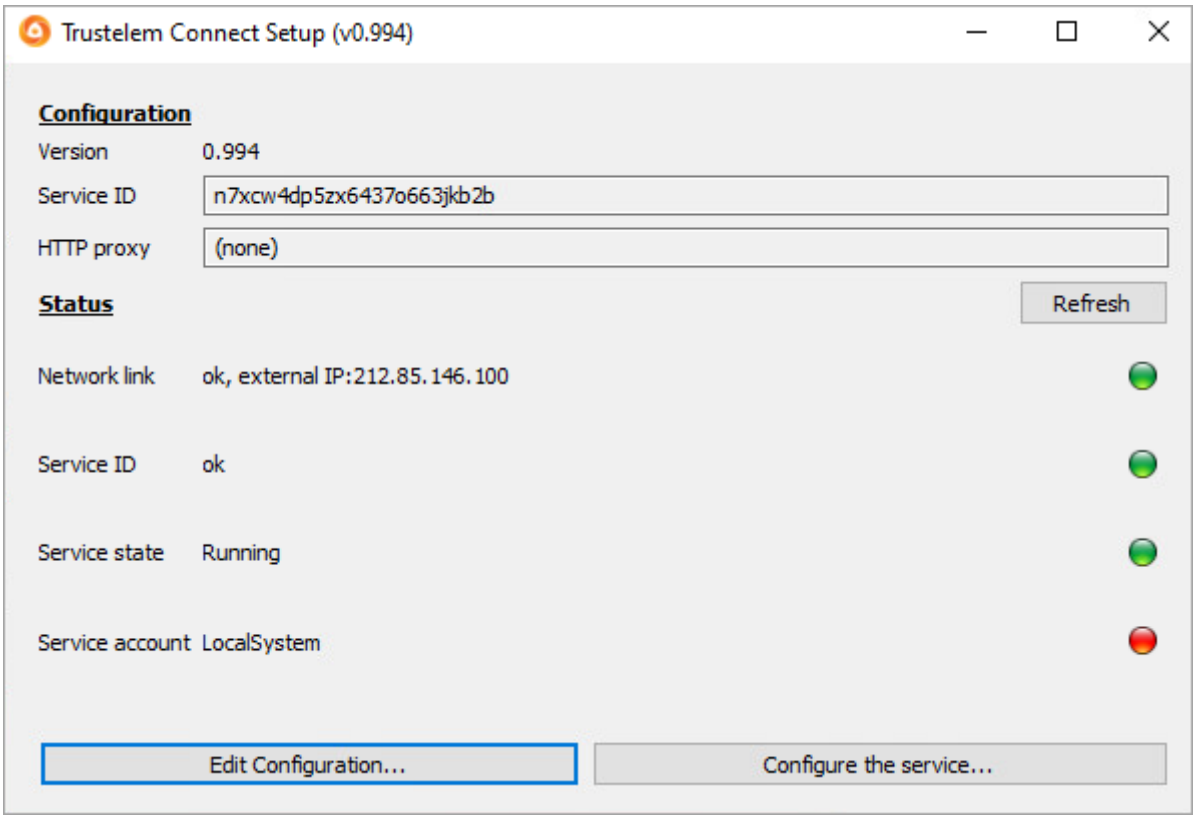


On your server:

- Download the latest version of **Trustelem Connect**, available at this URL:
  https://dl.trustelem.com/connect/
- Start the setup, and paste your **service ID** in the setup (window or file).
- If you want to use LDAPs, on the Trustelem folder, add a config.ini file and provide the following information :

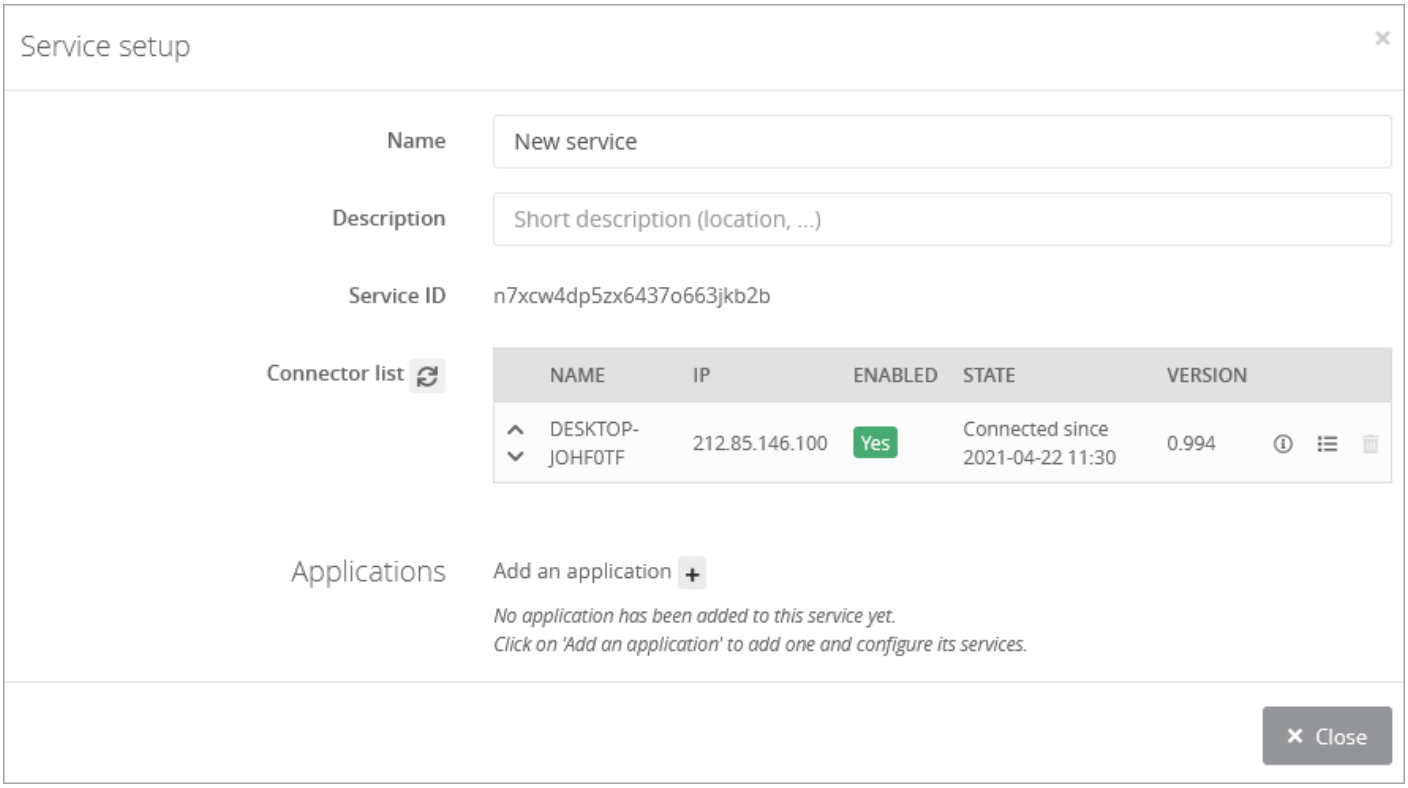
```
tls_cert = "C:\Program Files (x86)\Trustelem\connector.crt"
tls_cert_key = "C:\Program Files (x86)\Trustelem\connector.key"
```

- Start the service.



In your administration page

- Refresh your **Services** page.
- Turn on the service by clicking on **No**.



You now have a functional connector.

Note: if you want to install the connector on a Linux machine, follow these steps

- Download the tgz version, and install the connector as a service with the setup.sh script.
- To complete the configuration, please complete /opt/wallix/trustelem-connect/config.ini file containing the synchronization id.
- A sample minimal config.ini would be:

```
service_id = 2jy34wpcohrhdytr6hutym6qfi2l7nnw
state_dir = run/
```

- The run folder must have read write rights for the trustelem user.
- You can add your own X509 certificate for ldaps and starttls. Accepted format is PEM.

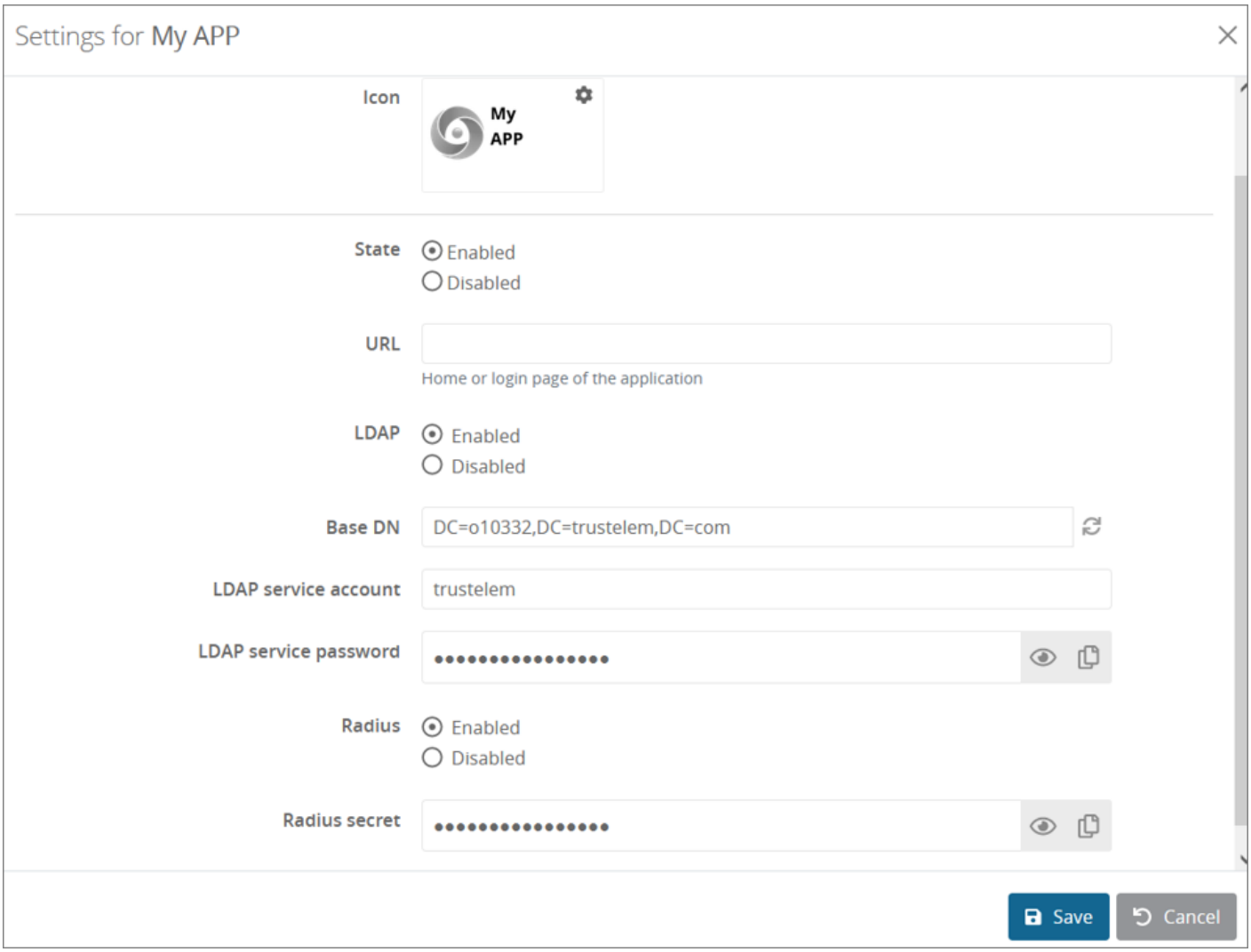
```
tls_cert = run/connector.crt
tls_cert_key = run/connector.key
```

- After that, you can start the service with: systemctl start trustelem-connect.service
- The service will run with the user trustelem

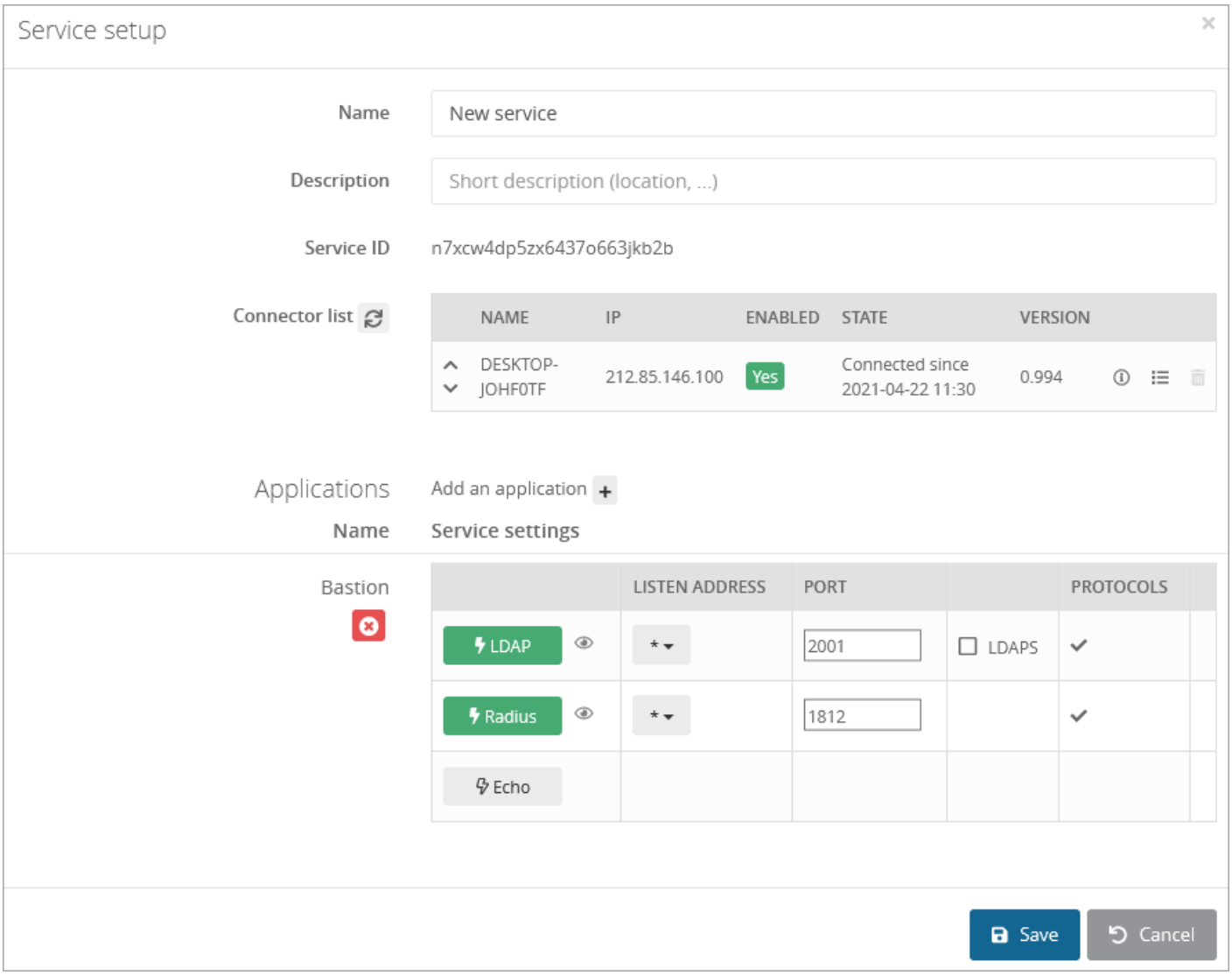
Setup Trustelem

In your Trustelem administration page:

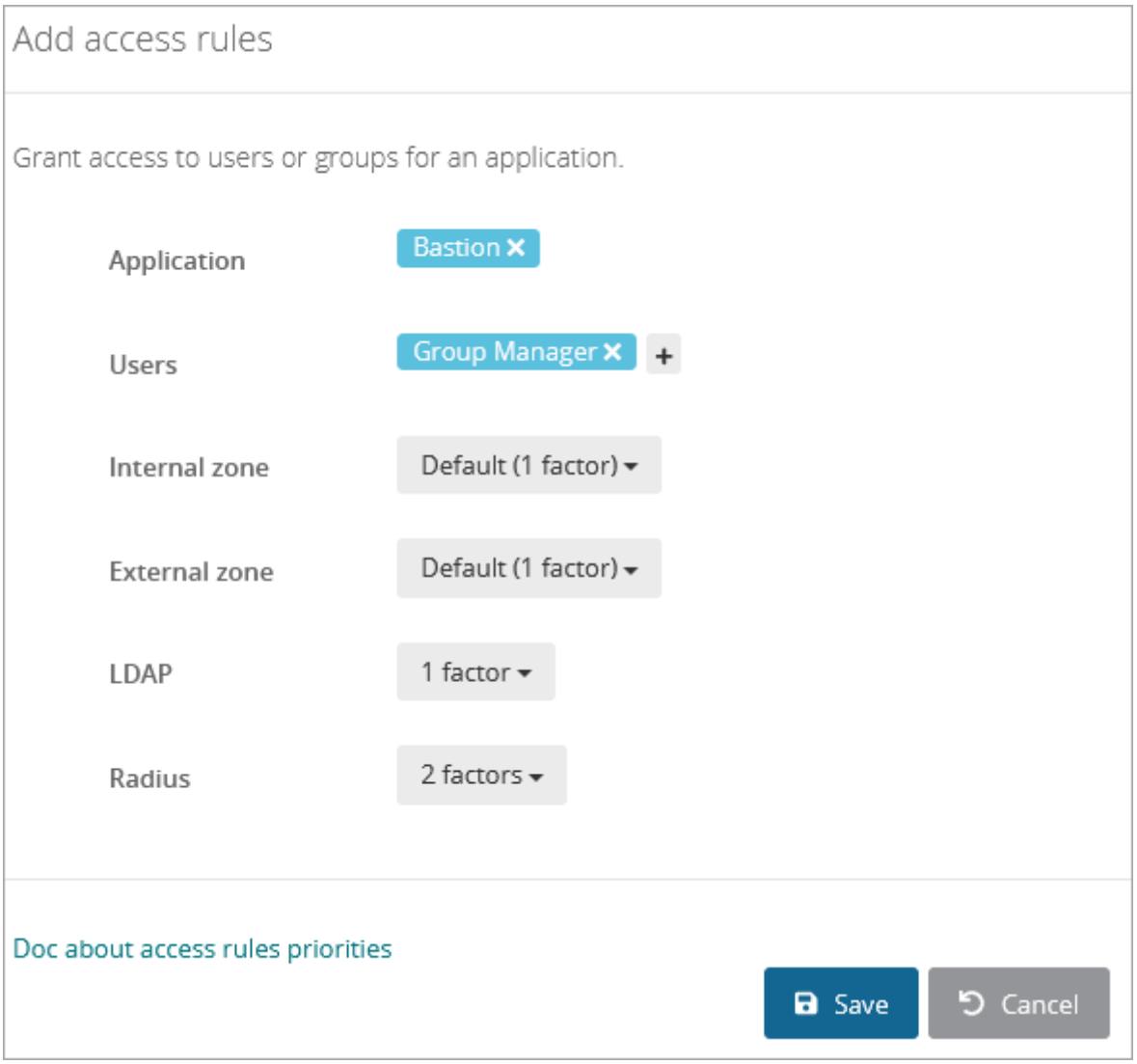
- Go to the **Apps** tab.
- Click on **+ Add an application**
- Choose either a pre-integrated application or a generic model depending on your need. *To use only LDAP / Radius the generic **Basic no SSO** model is enough*.
- Turn on LDAP and/or Radius.



- Go back to the previously configured service and click on **Add an application +**
- Click on LDAP and/or Radius, then enter the **listen address** and **port**
  Note: the listen address can be localhost, everything or a specific IP



- Go to the **Access Rules** tab
- Click **+ Create**
- Select your application, then enter the number of desired factors for LDAP and/or Radius authentications
  Note: internal and external zones are used for SAML, OpenID Connect or NoSSO access. They are not useful for only LDAP / Radius authentication.



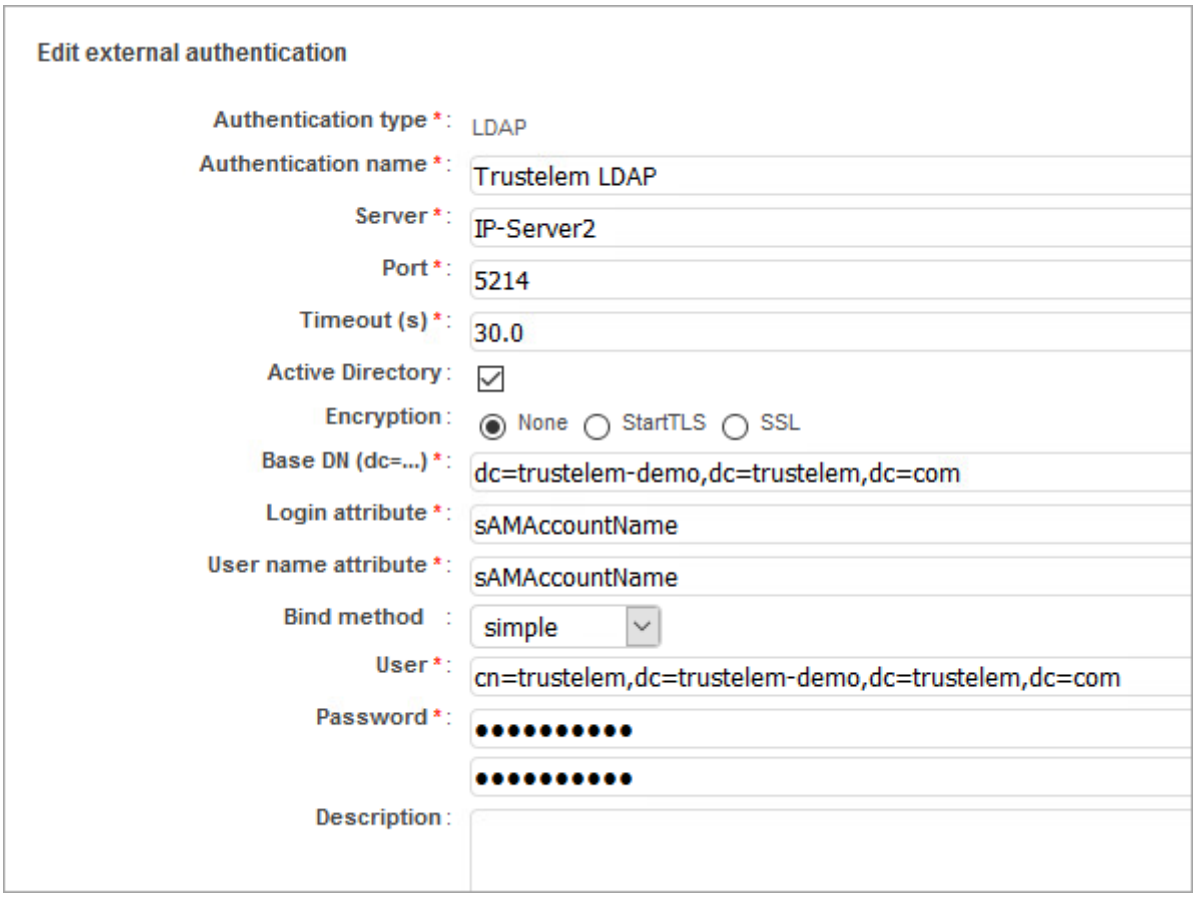
Trustelem is now ready to reply to applications sending requests to **TrustelemConnect** with the correct port and IP.

Setup the application

In your application, setup LDAP and/or Radius from the information provided by Trustelem:

- the port is defined in the Services tab
  `https://admin-mydomain.trustelem.com/app#/services`
- the domain / user / password are provided in the setup of the application
  `https://admin-mydomain.trustelem.com/app#/apps`

With the initial example:



Revision #3
Created 1 July 2022 08:22:01 by WALLIX Admin
Updated 27 October 2022 08:16:09 by WALLIX Admin