# Installation Guide

v 1.0

OS: **Ubuntu 22.04**

apt update

apt install krb5-config krb5-user libpam0g-dev ruby ruby-dev libpam-krb5 libpam-script libauthen-simple-pam-perl libredis-perl libwww-perl libjson-perl libjson-parse-perl libdigest-sha-perl libdigest-hmac-perl build-essential freeradius-python3 nginx freeradius-redis python3-yaml python3-redis python3-pyotp supervisor redis redis-sentinel postfix

gem install rpam2 rotp redis mail sinatra rack-throttle rackup

git clone <https://github.com/hophuongnam/otpserver>

**All files mentioned are relatively on otpserver folder. Copy to the path provided.**

### Active Directory

krb5.conf.example => /etc/krb5.conf (edit if necessary)

To test authentication:

* **kinit** to get tickets.
* **klist** to list tickets.
* **kdestroy** to delete tickets.

### nginx

nginx.otp => /etc/nginx/sites-enabled/otp (edit if necessary)

nginx.conf => /etc/nginx/nginx.conf (edit if necessary)

Pay attention to things like certificates, hostnames ...

### PAM (pluggable authentication modules)

pam.d.otp => /etc/pam.d/otp

pam\_script\_acct => /usr/share/libpam-script/pam\_script\_acct (chmod +x)

test.pam.rb => ~/test.pam.rb (edit if necessary)

Use test.pam.rb to test for authentication:

ruby test.pam.rb

### Postfix

postfix.main.cf => /etc/postfix/main.conf (edit if necessary)

### Redis Configuration

Recommended instances: 3

On SLAVE, edit /etc/redis/redis.conf:

- Comment out "bind 127.0.0.1 ::1"

- Paste at the end:

protected-mode no

requirepass secret\_here

masterauth secret\_here

replicaof ip\_of\_master 6379

On MASTER, edit /etc/redis/redis.conf

- Comment out "bind 127.0.0.1 ::1"

- Paste at the end:

protected-mode no

requirepass secret\_here

masterauth secret\_here

requirepass and masterauth secret must be identical on all 3 instances.

### Sentinel Configuration

Configuration is the same in all instances.

/etc/redis/sentinel.conf

Comment these lines:

bind 127.0.0.1 ::1

sentinel monitor mymaster 127.0.0.1 6379 2

Add to the TOP of configuration file:

sentinel monitor mymaster ip\_of\_master 6379 2

sentinel auth-pass mymaster secret\_here

requirepass secret\_here

### supervisord

supervisord.otp.conf => /etc/supervisor/conf.d/otp.conf

### Server

config.otp.yaml => /etc/freeradius/3.0/config.otp.yaml (edit if necessary)

Create **otp** folder:

mkdir /etc/freeradius/3.0/otp

jquery-qrcode.min.js => /etc/freeradius/3.0/otp/jquery-qrcode.min.js

sha.js => /etc/freeradius/3.0/otp/sha.js

otp.html => /etc/freeradius/3.0/otp/otp.html (edit if necessary)

otp.rb => /etc/freeradius/3.0/otp/otp.rb (chmod +x) (edit if necessary)

otp.py => /etc/freeradius/3.0/mods-config/python3/otp.py (chmod +x) (edit if necessary)

dictionary => /etc/freeradius/3.0/dictionary

ldap => /etc/freeradius/3.0/sites-enabled/ldap

otp => /etc/freeradius/3.0/sites-enabled/otp

ldapotp => /etc/freeradius/3.0/sites-enabled/ldapotp

python3 => /etc/freeradius/3.0/mods-enabled/python3

# Operation Guide

To debug, stop freeradius service and run “freeradius -X” to observe the emitted logs.

The core web server is run by **supervisor** service, proxied through **nginx.**

Add clients to /etc/freeradius/3.0/clients.conf

Example for a client is shown belows:

client wifi {   
 ipaddr = 10.255.1.0/24   
 secret = LBCYh47ndBxA3Ts2   
 virtual\_server = otp   
}

Where virtual\_server must be one of the following:

* otp: the desired outcome: username and password, followed by OTP.
* ldap: only username and password are required.
* ldapotp: OTP is appended to password, user sent username and password+otp

|  |  |  |
| --- | --- | --- |
| Redis Schema | | |
| **Key** | **Value** | **Desc** |
| username | OTP Key | The main key |
| username\_token | Token | The token that was sent to user's email. This is set to expired in 5 min |
| username\_email | Email address | Set to the user's email address. Server will send provision token to this address if set. |
| username\_noop | 1 | Value is arbitrary. This will override the server's settings and will authenticate user by LDAP only |
| username\_attributes | RADIUS Attributes | String. Additional attributes that will be sent to the RADIUS's client in Accept-Access message. |