



PFSENSE

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs Security.

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

1. Overview

This document explains how to enable OpenOTP authentication with Radius Bridge and pfSense. For this recipe, you will need to have WebADM, OpenOTP installed and configured. Please, refer to [WebADM Installation Guide](#) and [WebADM Administration Guide](#) to do it.

2. WebADM/OpenOTP/Radius Bridge

For this recipe, you will need to have WebADM/OpenOTP installed and configured. Please, refer to [WebADM Installation Guide](#) and [WebADM Manual](#) to do it. You have also to install our [Radius Bridge product](#) on your WebADM server(s).

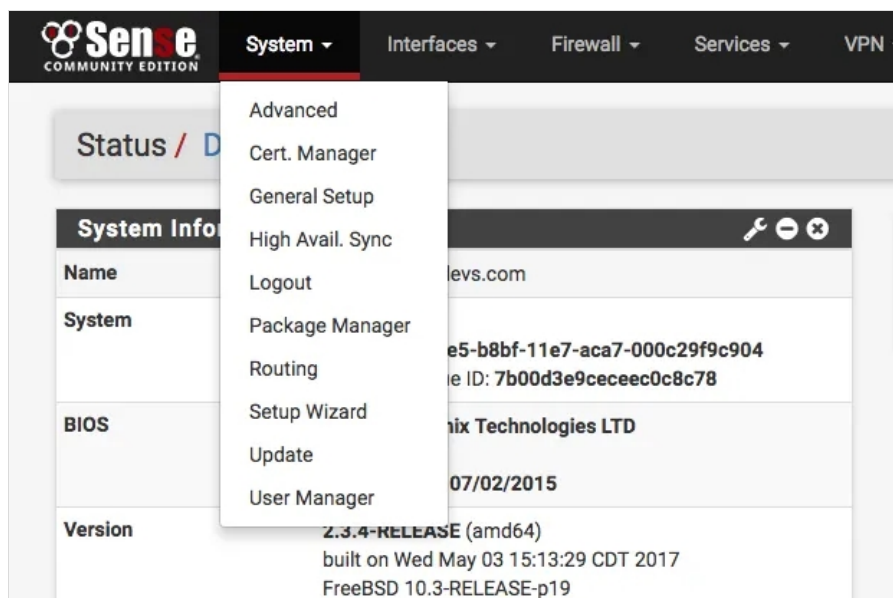
3. Register your pfSense in RadiusBridge

On your OpenOTP RadiusBridge server, edit the `/opt/radiusd/conf/clients.conf` and add a RADIUS client (with IP address and RADIUS secret) for your pfSense VPN server:

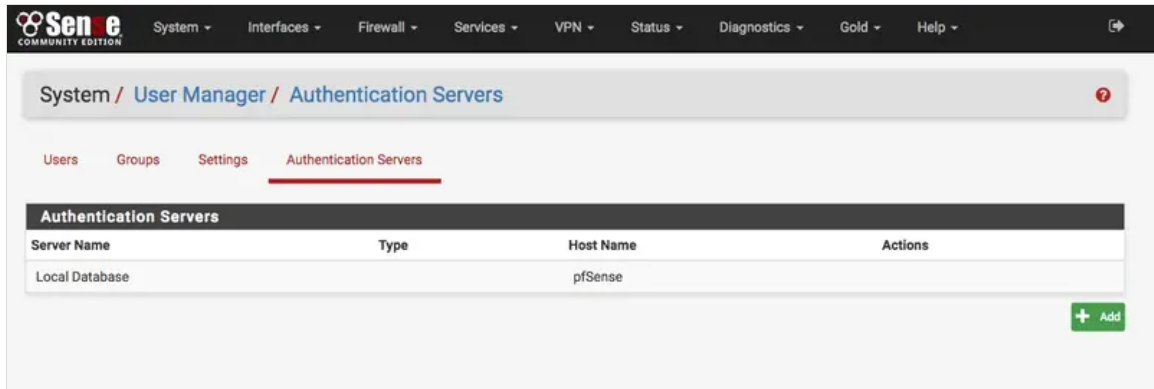
```
client <pfSense Server IP> {  
  secret = testing123  
  shortname = pfSense  
}
```

4. Configuring New Radius Server on pfSense

Here, we will configure a new RADIUS Server through the pfSense GUI. Go on the `System` tab and click on `User Manager`.

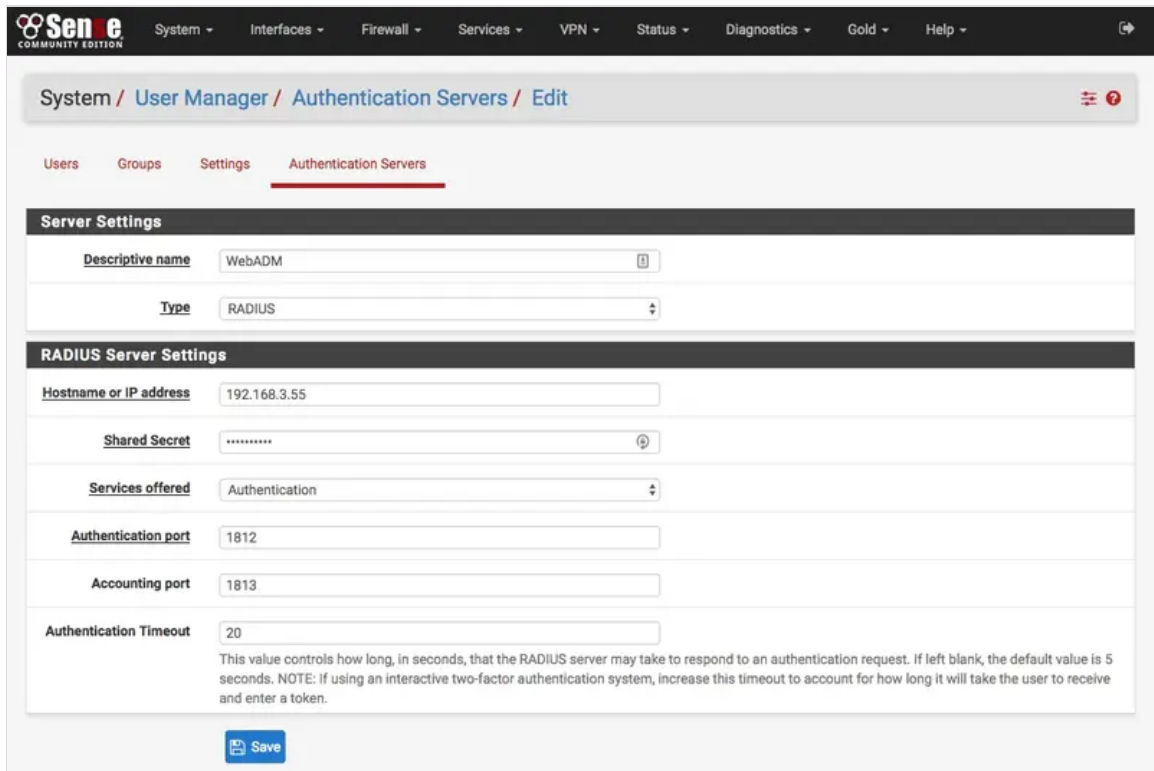


In the `Authentication Server` tab, click on `Add` :



Configure your WebADM server as a RADIUS server. Shared secret is previously defined in

```
/opt/radiusd/conf/clients.conf.
```



Note

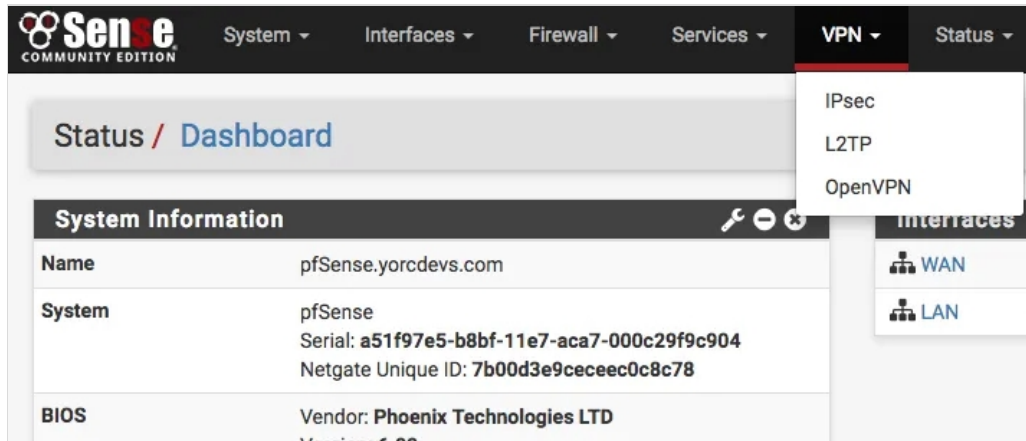
Set the Authentication Timeout to 20.

Click on **Save** when the configuration is done.

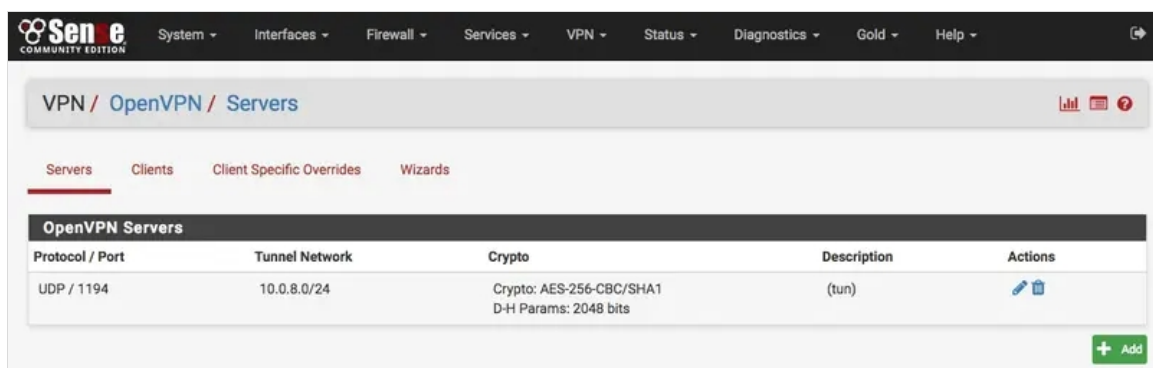
5. Configuring OpenOTP Authentication for OpenVPN Server on pfSense

⚠ Note

In this how-to, we will not explain how to configure the OpenVPN server. Please refer to OpenVPN or pfSense documentation for this part.



Now on your OpenVPN configuration, click on **Servers** tab and edit your OpenVPN server.



For the Server mode setting, select **Remote Access (User Auth)** and for the backend authentication option, choose your RADIUS Server previously created, in my case 'WebADM'.

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards

General Information

Disabled Disable this server
Set this option to disable this server without removing it from the list.

Server mode Remote Access (User Auth)

Backend for authentication WebADM
Local Database

Protocol UDP

Device mode tun

Interface WAN

Local port 1194

Description

A description may be entered here for administrative reference (not parsed).

It's done for the authentication part.

5.1 Configuring OpenOTP Authentication for IPsec

Same procedure as above, you have to select WebADM in the Extended Authentication (Xauth) if you use L2TP and IPsec:

Extended Authentication (Xauth)

User Authentication WebADM
Local Database

Source

Group Authentication none

Source

6. Configuring WebADM/OpenOTP Client Policy

Note

OpenVPN doesn't manage the RADIUS challenge authentication. So, we will create a client policy to be able to log in on the OpenVPN server with OpenOTP and the concatenated mode (LDAP password+OTP in the same password field.)

Login on the WebADM GUI, click on **Admin** tab and click on **Client Policies** button.

The screenshot shows the WebADM Freeware Edition v1.6.8-2 administration interface. The top navigation bar includes Home, Admin, Create, Search, Import, Databases, Statistics, Applications, About, and Logout. The main content area is titled "WebADM Server Administration" and displays the following information:

- WebADM v1.6.8-2 (64bit) running on server rcvm7.local (192.168.3.155) in standalone mode.
- Server Version Details: Apache/2.4.37 PHP/7.1.23 OpenSSL/1.0.2p-fips
- Internal Server Time: 2018-11-23 17:51:21 Europe/Berlin (NTP check Ok)
- Hardware Modules: No HSM Connected
- WebADM Features: WebApps (Enabled), WebSrvs (Enabled), Manager (Enabled)
- Active LDAP Server: LDAP Server (127.0.0.1) Active SQL Server: SQL Server (127.0.0.1)
- Active Session Server: Session Server (:::1) Active PKI Server: PKI Server (127.0.0.1)

Below the status information, there are several configuration cards:

- Local Domains (1)**: Associate domain names with LDAP user search bases.
- Trust Domains (0)**: Bridge remote domain names located on distant servers.
- Client Policies (0)**: Define custom policy settings for consumer applications.
- LDAP Mount Points (0)**: Connect secondary LDAP servers to the tree view.
- LDAP Option Sets (1)**: Define LDAP tree constraints for your "other" administrators.
- Administrator Roles (1)**: Create admin role templates for your "other" administrators.

Click now on **Add Client**.

The screenshot shows the "Registered Client Policies" page in the WebADM Freeware Edition v1.6.8-2 administration interface. The page displays the following information:

- Registered Client Policies
- No Client Policy configured
- Buttons: Add Client, Ok

Name your client policy as you prefer, click on **Proceed** button and on **Create Object** button.

The screenshot shows the "Create Configuration Object of Type Client" page in the WebADM Freeware Edition v1.6.8-2 administration interface. The page displays the following information:

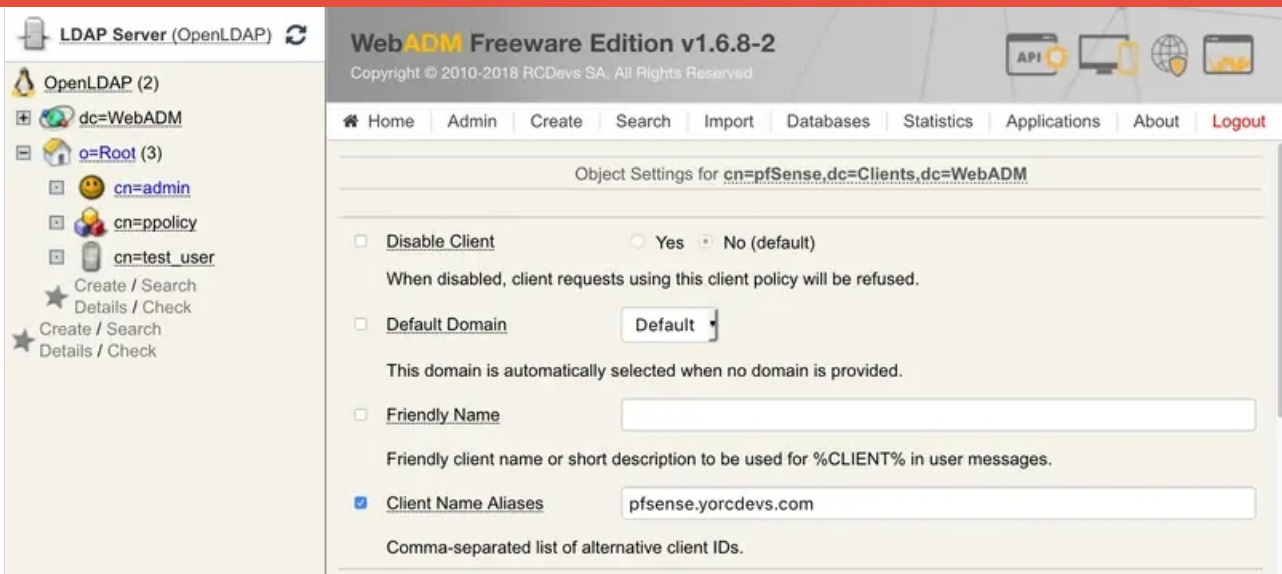
- Create Configuration Object of Type Client
- Mandatory attributes**
 - Container: dc=Clients,dc=WebADM (with a Select button)
 - Common Name: pfSense
 - WebADM Object Type: WebADM Client Policy (Client)
- Optional attributes**
 - WebADM Settings: You can edit this attribute once object is created.
 - Description / Note: (empty text field)
- Proceed button

Now you are on the client policy configuration page. Edit the setting **Client Name Aliases** with the name of your pfSense

server. In my case: pfsense.yorcdevs.com

⚠ Note

This setting is very important, it will do the matching between the pfsense server and the client policy.



The screenshot shows the WebADM Freeware Edition v1.6.8-2 interface. On the left, the LDAP Server (OpenLDAP) tree is visible, showing the hierarchy: dc=WebADM > o=Root (3) > cn=admin, cn=ppolicy, and cn=test_user. The main content area displays the 'Object Settings for cn=pfSense,dc=Clients,dc=WebADM'. The settings include:

- Disable Client** (Yes/No (default))
- Default Domain** (Default)
- Friendly Name** (empty field)
- Client Name Aliases** (pfsense.yorcdevs.com)

After that, you can scroll down and check the box **Forced Application Policies** and click on **Edit** button:



The screenshot shows the 'Forced Application Policies' section in the WebADM interface. The **Application Settings (Default)** checkbox is checked. Below it is an empty text area for entering application settings, with an **Edit** button to its right. The text below the text area reads: 'List of application settings which override any default, user or group level setting. The format is the same as for the web services' request settings (see API documentation). The request settings (if present) will still override the application settings. Enter one setting per line in the form OpenOTP.LoginMode=OTP.'

In the **Applications** box on the top left, click on **OpenOTP** and now, you are able to reconfigure completely the OpenOTP application for pfSense. But here, only one setting interest us who is the **Challenge Mode Supported**. You have to set the setting to **No** because OpenVPN doesn't manage the RADIUS Challenge. Of course, my default configuration of OpenOTP is set for **LDAPOTP** login mode.

The screenshot shows the 'Authentication Policy' configuration page in the WebADM Freeware Edition v1.6.8-2 Administration Console. The left sidebar shows the OpenLDAP (2) tree with users like cn=admin, cn=ppolicy, and cn=test_user. The main content area is titled 'Application Settings' and 'Authentication Policy'. It includes a list of applications on the left with 'OpenOTP' selected. The configuration options for OpenOTP are:

- Login Mode:** LDAPOTP (Default). Description: The login mode (required login factors) should be adjusted via Client Policies.
 - LDAPOTP: Require both LDAP and OTP passwords.
 - LDAPU2F: Require both LDAP and FIDO response.
 - LDAPMFA: Require LDAP and either OTP or FIDO.
 - LDAP: Require LDAP password only.
 - OTP: Require OTP password only.
- OTP Type:** TOKEN (Default). Description:
 - TOKEN: OATH HOTP/TOTP/OCRA, YubiKey or MobileOTP Token.
 - SMS: SMS one-time password (On-demand or Prefetched).
 - MAIL: Email one-time password (On-demand or Prefetched).
 - LIST: Pre-generated OATH OTP password list (to be printed).
 - PROXY: Forward requests to another RADIUS server (for migrations).
- OTP Fallback:** TOKEN. Description: Fallback OTP Type to be used as secondary authentication method. LASTOTP let users use the last validated OTP which expires after a delay. Use DISABLED to disabled fallback if there is a configuration by default.
- OTP Password Length:** 6 (Default). Note: This setting is ignored for OCRA Tokens as OTP length is part of the OCRA Suite. Warning: Changing this setting after having registered OATH Tokens will invalidate these Tokens.
- OTP PIN Prefix:** Yes (selected) / No (default). Description: When enabled a static prefix has to be prepended to any OTP password in the form [PIN][OTP]. The OTP Prefix must be registered first and must be at least 4 alpha-numeric characters.
- Challenge Mode Supported:** No (selected) / Yes (default). Description: You can disable challenged OTP/FIDO if your client applications does not support it. OpenOTP assumes concatenated OTP passwords when disabled with simpleLogin requests. Note: Challenge is required for Simple-Push, FIDO, OATH-OCRA and on-demand SMS/Mail OTP.

You can now click on **Apply**, twice, to save the configuration.

The screenshot shows the 'Registered Client Policies' page in the WebADM Freeware Edition v1.6.8-2 Administration Console. The left sidebar is the same as in the previous screenshot. The main content area shows a list of registered client policies. One policy is visible:

- pfSense** (cn=pfSense,dc=Clients,dc=WebADM)
 - Status: **Enabled** [CONFIGURE] [RENAME] [REMOVE]
 - Aliases: pfsense.yorcdevs.com
 - Application Settings: OpenOTP.ChallengeMode=No

At the bottom of the page, there are two buttons: 'Add Client' and 'Ok'.

Now you can test the authentication.

7. Authentication Test

Note

Before testing, you should have an Activated User in WebADM/OpenOTP and a Token enrolled on your user account. We will not explain here how to do it, so please refer to the following documentation if required: [User Activation and Token enrollment](#)

You can test an authentication through your VPN client or through the Authentication Diagnostic tool available on the pfSense GUI.

I will test through the diagnostic tool, so I select my WebADM server as Authentication server.

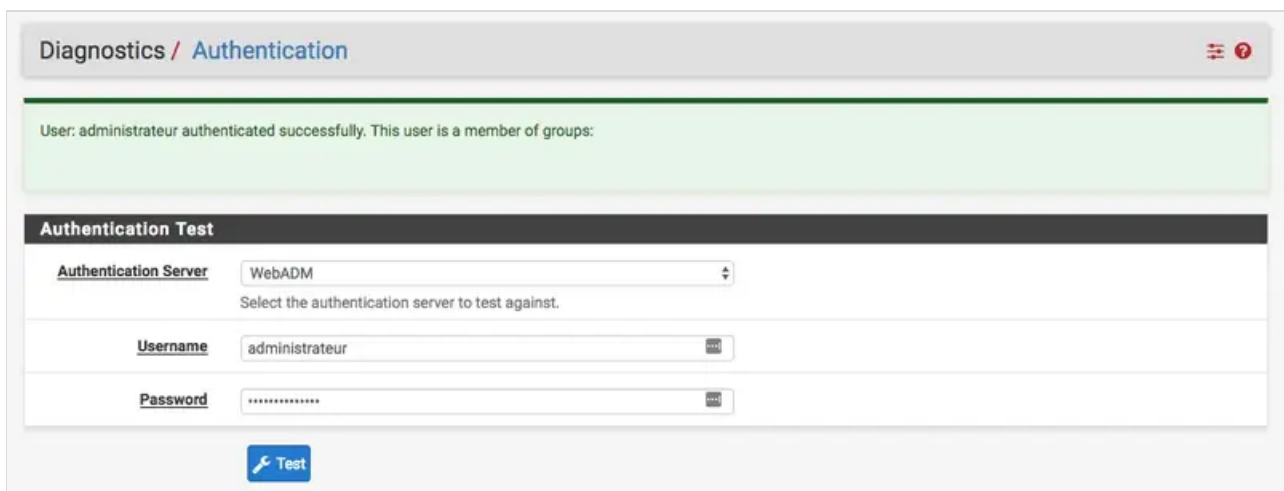


The screenshot shows a form titled "Authentication Test". It has three input fields: "Authentication Server" with a dropdown menu set to "WebADM", "Username" with the text "administrateur", and "Password" with masked characters "*****". Below the fields is a blue button with a wrench icon and the text "Test".

In the password field, I put my LDAP password and my OTP.

e.g : password123456

Where 'password' is my LDAP password and '123456' is my OTP.



The screenshot shows the "Diagnostics / Authentication" page. At the top, there is a green message box that says "User: administrateur authenticated successfully. This user is a member of groups:". Below this is the "Authentication Test" form, which is identical to the one in the previous screenshot, showing the "WebADM" server, "administrateur" username, and masked password. A blue "Test" button is at the bottom.

And I'm successfully logged.

8. WebADM Logs

We can show in the WebADM logs that the Client policy previously created is called, the challenge mode is disabled and the authentication is a success with an OTP.

[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] New openotpSimpleLogin SOAP request
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] > Username: administrateur
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] > Password: xxxxxxxxxxxxxxx
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] > Client ID: pfSense.yorcdevs.com
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] > Options: RADIUS,-U2F
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Enforcing client policy: pfSense (matched client ID)
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Registered openotpSimpleLogin request
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Resolved LDAP user:
CN=Administrateur,CN=Users,DC=yorcdevs,DC=com
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Resolved LDAP groups: propri\c3\xa9taires cr\c3\xa9ateurs de la strat\c3\xa9gie de groupe,admins du domaine,administrateurs de l\c3\xa9entreprise,administrateurs du sch\c3\xa9ma,administrateurs,utilisateurs du bureau \c3\xa0 distance,groupe de r\c3\xa9plication dont le mot de passe rodc est refus\c3\xa9
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Started transaction lock for user
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Found user language: EN
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Found 1 user mobiles: +33xxxxxxxxx
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Found 1 user emails: support@rcdevs.com
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Found 3 user certificates
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Found 37 user settings:
LoginMode=LDAPOTP,OTPTType=TOKEN,OTPLength=6,ChallengeMode=No,ChallengeTimeout=90,PushLogin:1:HOTP-SHA1-6:QN06-T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTime=300,ListChallengeMode=

[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Found 9 user data:
LoginCount,RejectCount,LastOTP,TokenType,TokenKey,TokenState,Device1Name,Device1Data,Device1State

[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Last OTP present (valid until 2017-10-25 14:54:30)
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Challenge mode disabled (assuming concatenated passwords)
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Found 1 registered OTP token (TOTP)
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Requested login factors: LDAP & OTP
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] LDAP password Ok
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] TOTP password Ok (token #1)
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Updated user data
[2017-10-25 14:52:20] [127.0.0.1] [OpenOTP:8VE13372] Sent success response

This manual was prepared with great care. However, RCDevs Security S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs Security S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs Security S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs Security S.A. The latter especially applies for data processing systems. RCDevs Security S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs Security. © 2024 RCDevs Security S.A., All Rights Reserved