



OPENVPN

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 OpenVPN.

The advantage of integrating RadiusBridge with OpenVPN is :

- > Secure access with [MFA](#) .
- > Authentication of Ldap users via OpenVPN client.

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 OpenVPN 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 OpenVPN :

```
client <OpenVPN Server IP> {  
    ipaddr = <OpenVPN Server IP>  
    secret = Testing123  
}
```

4. Configuring New Radius Server on OpenVPN

Here, we will configure a new RADIUS Server through the OpenVPN GUI.

OPENVPN Access Server v2.10.3

STATUS
CONFIGURATION
USER MANAGEMENT
AUTHENTICATION 1
Settings
RADIUS 2
LDAP
TOOLS
DOCUMENTATION
SUPPORT

Logout

POWERED BY OPENVPN
© 2009-2022 OpenVPN Inc.
All Rights Reserved

RADIUS Authentication

To use an existing RADIUS system for user authentication with Access Server, you must first configure and enable it. RADIUS authentication can then be used as the default authentication system, or only for specific groups or users.

RADIUS Settings

Enable RADIUS Authentication 3
 Enable RADIUS Accounting reports No
 Account names are case-sensitive No

RADIUS Server

Specify the RADIUS server connection details below.

4	5	6	Authentication Port	Accounting Port
RADIUS_IP_ADDR	*****	1812	1812	1813
			1812	1813
			1812	1813
			1812	1813
			1812	1813

RADIUS Authentication Method 7

The connection to the RADIUS Server is authenticated via one of these methods.

PAP Yes

CHAP No

MS-CHAP v2 No

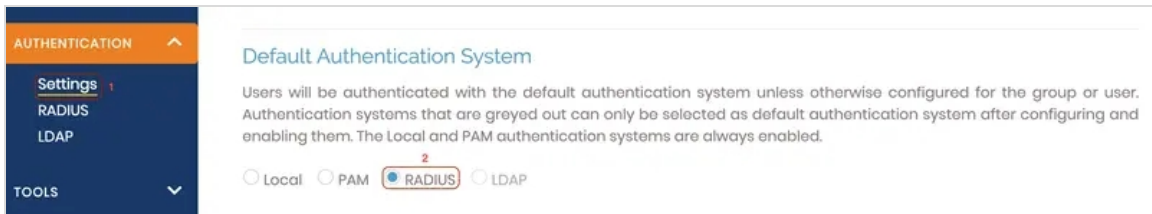
Save Settings

- > Go on the **AUTHENTICATION** tab.
- > Click on **RADIUS**.
- > Set the toggle to **Yes** to enable **RADIUS authentication**.
- > Specify the hostname or IP address for your **RADIUS server**.
- > Specify the **shared secret**. You must configure the **RADIUS server** with the same shared secret.

> Define the port where the **RADIUS** protocol sends UDP packets. The default port is 1812. **Accounting Port** : Define the port where the RADIUS protocol listens for accounting requests. The default port is 1813, and the accounting port is only required when you enable RADIUS accounting.

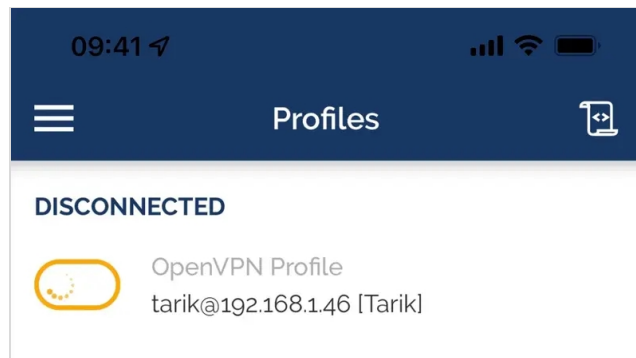
> Define the **RADIUS** Authentication Method.

In the same menu, click on **Settings** and choose **RADIUS** :

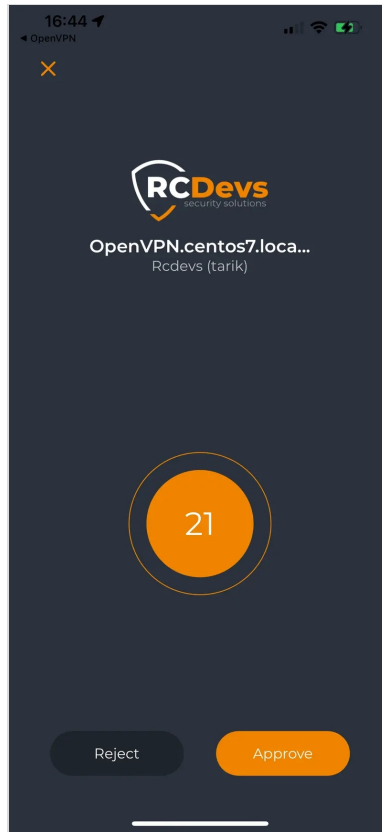


Don't forget to **Save Settings** after each modification.

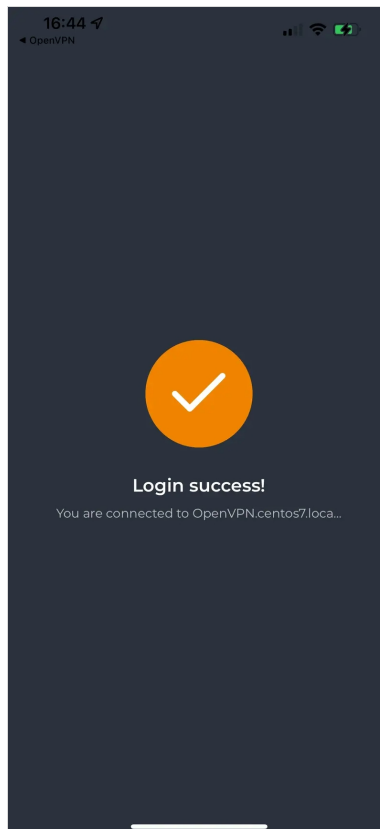
Test of Authentication :

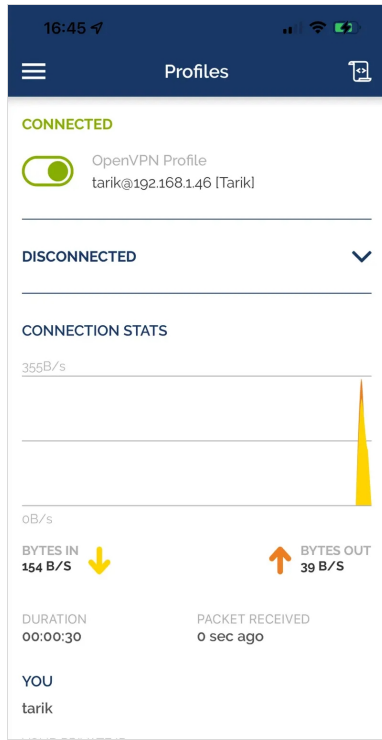


Receiving push notification :



Login success :





WebADM logs : Below the OpenVPN session logs after the success login with OpenOTP :

```
[2022-06-22 15:59:17] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] New openotpSimpleLogin SOAP request
[2022-06-22 15:59:17] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] > Username: tarik
[2022-06-22 15:59:17] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] > Password: xxxxxxxxxxxxxx
[2022-06-22 15:59:17] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] > Client ID:
OpenVPN.centos7.localdomain
[2022-06-22 15:59:17] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] > Options: RADIUS,NOVOICE,-U2F
[2022-06-22 15:59:17] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Registered openotpSimpleLogin request
[2022-06-22 15:59:17] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Resolved LDAP user: cn=tarik,o=Root
[2022-06-22 15:59:17] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Using SQL server 'SQL Server'
[2022-06-22 15:59:18] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Started transaction lock for user
[2022-06-22 15:59:18] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Found 48 user settings:
LoginMode=LDAPOTP,OTPTType=TOKEN,PushLogin=Yes,ChallengeMode=Yes,ChallengeTimeout=90,Challenge
1:HOTP-SHA1-6:QN06-
T1M,DeviceType=FIDO2,U2FPINMode=Discouraged,SMSType=Normal,SMSMode=Ondemand,MailMode=Onc
[2022-06-22 15:59:18] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Found 5 user data:
TokenType,TokenKey,TokenState,TokenID,TokenSerial
[2022-06-22 15:59:18] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Found 1 registered OTP token (TOTP)
[2022-06-22 15:59:18] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Requested login factors: LDAP & OTP
[2022-06-22 15:59:18] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] LDAP password Ok
[2022-06-22 15:59:18] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Session already started (overriding)
[2022-06-22 15:59:18] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Authentication challenge required
[2022-06-22 15:59:18] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Sent push notification for token #1
(session AVAR256yr0aZRrrB)
[2022-06-22 15:59:18] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Waiting 27 seconds for mobile response
[2022-06-22 15:59:21] [172.16.3.9:56174] [OpenOTP:6EZZ8LR2] Received mobile login response from
172.16.3.9
[2022-06-22 15:59:21] [172.16.3.9:56174] [OpenOTP:6EZZ8LR2] > Session: AVAR256yr0aZRrrB
[2022-06-22 15:59:21] [172.16.3.9:56174] [OpenOTP:6EZZ8LR2] > Password: 16 Bytes
[2022-06-22 15:59:21] [172.16.3.9:56174] [OpenOTP:6EZZ8LR2] Found authentication session started
2022-06-22 15:59:18
[2022-06-22 15:59:21] [172.16.3.9:56174] [OpenOTP:6EZZ8LR2] PUSH password Ok (token #1)
[2022-06-22 15:59:21] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Updated user data
[2022-06-22 15:59:21] [127.0.0.1:52988] [OpenOTP:6EZZ8LR2] Sent login success response
```

Radiusd logs using debug mode :


```
(11) Received Access-Request Id 109 from 192.168.1.46:57336 to 192.168.1.28:1812 length 98
(11) User-Name = "tarik"
(11) User-Password = "*****"
(11) NAS-Identifier = "OpenVPN.centos7.localdomain"
(11) Service-Type = Outbound-User
(11) NAS-Port = 6
(11) Framed-Protocol = PPP
(11) NAS-Port-Type = Virtual
(11) # Executing section authorize from file /opt/radiusd/lib/radiusd.ini
(11) authorize {
(11) eap: No EAP-Message, not doing EAP
(11) [eap] = noop
(11) pap: WARNING: No "known good" password found for the user. Not setting Auth-Type
(11) pap: WARNING: Authentication will fail unless a "known good" password is available
(11) [pap] = noop
(11) [openotp] = ok
(11) } # authorize = ok
(11) Found Auth-Type = OTP
(11) # Executing group from file /opt/radiusd/lib/radiusd.ini
(11) Auth-Type OTP {
rlm_openotp: Found client ID attribute with value "OpenVPN.centos7.localdomain"
rlm_openotp: Found client IP attribute with value "192.168.1.46"
rlm_openotp: Sending openotpSimpleLogin request
rlm_openotp: OpenOTP authentication succeeded
rlm_openotp: Reply message: Authentication success
rlm_openotp: Sending Access-Accept
(11) [openotp] = ok
(11) } # Auth-Type OTP = ok
(11) Login OK: [tarik] (from client 192.168.1.46 port 6)
(11) Sent Access-Accept Id 109 from 192.168.1.28:1812 to 192.168.1.46:57336 length 44
(11) Reply-Message := "Authentication success"
(11) Finished request
Waking up in 9.9 seconds.
(11) Cleaning up request packet ID 109 with timestamp +1582 due to cleanup_delay was reached
Ready to process requests
Connection to 192.168.3.168 closed by remote host.
Connection to 192.168.3.168 closed.
```

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