PALO ALTO

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.

Palo Alto

How To Enable OpenOTP Authentication in Palo Alto SSL VPN

This document explains how to enable OpenOTP authentication in Palo Alto SSL VPN.

1. Register your Palo Alto VPN 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 Palo Alto VPN server.

Example:

```
client <VPN Server IP> {
 secret = testing123
 shortname = PaloAlto-VPN
 }
```

2. On Palo Alto Admin Interface, Set up a RADIUS Server Profile

Enter the Palo Alto administration interface.

Go to *Device* → *Server Profiles* → *RADIUS*.

Click the *Add* button, to add a new RADIUS server profile.

Configure the profile settings with:

- Name: OpenOTP RADIUS
- Timeout: 20
- Retries: 0

Under *Servers* click the *Add* button to add a RADIUS server.

Configure server settings with:

- Server: OpenOTP
- IP Address: Your RadiusBridge IP address.
- Secret: The secret you have defined in RB clients.conf file.
- Port: 1812

Save the RADIUS server profile.

3. Create an Authentication Profile

Go to Device->Authentication Profile.

Client the New button to add a new authentication profile.

Configure settings with:

- Profile Name: OpenOTP
- Authentication: RADIUS
- Server Profile: OpenOTP RADIUS

Save the authentication profile.

4. Configure your SSL VPN with OpenOTP

Go to *Network → SSL-VPN*.

Edit your VPN profile or create a new one.

Set the Authentication Profile to “OpenOTP”.

Save the SSL-VPN profile.

Click the *Commit* button at the top-right to apply new configurations.

Note

Don’t forget to authorize the communication on 1812 UDP port (default RADIUS port for the authentication) from your Palo-Alto system to your WebADM instance at the firewall level.