

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.

Copyright (c) 2010-2017 RCDevs SA. All rights reserved. http://www.rcdevs.com

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

Limited Warranty

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. WebADM/OpenOTP/Radius Bridge

For this recipe, you will need to have WebADM/OpenOTP installed and configured. Please, refer to <u>WebADM Installation Guide</u> and <u>WebADM Manual</u> to do it. You have also to install our Radius Bridge product on your WebADM server(s). Another documentation on that setup is provided by Cisco at this link

2. Register your ASA SSL 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 ASA SSL VPN server.

Ex:

```
client ASA-SSL {
    ipaddr = <VPN Server IP>
    secret = testing123
}
```

3. Configuring new RADIUS AAA Server to Cisco

Configuring OTP authentication to ASA means adding a RADIUS AAA Server configuration to a new or an existing Connection Policy. To do add both new RADIUS AAA Server and Connection Policy:

- 1. Log in to your Cisco ASA Device Manager administration UI.
- 2. From the top menu, select Configuration and then from left menu Remote Access SSL VPN.
- 3. Under AAA/Local Users select AAA Server Groups.
- 4. In AAA Server Groups page that opens select Add.
- 5. Set (see example picture below):
- > Name OpenOTP_Servers
- > Protocol select RADIUS
- > Leave rest as defaults and commit add.

When Configuration Montoring Server Group Periode List Image: Configuration > Device Hanagement In 10.64.100.153 In 10.64.100.100.100 In 10.64.100.100.100.100.100.100.100.100.100.1	File View Tools Wizards Windo	ow Help					
Device List Image: Configuration > Device Hanagement • Add Delete Connect • Add Delete Connect • Io.64.100.94 • Io.64.100.94 • Io.64.100.133 • Io.134.127.254 • Io.64.100.133 • Io.134.127.254 • Io.64.100.74 • Io.64.100.94 • Io.64.100 • Io.64.100	🚳 Home 🦓 Configuration 🔯 Monitoring 🔚 Save 🔇 Refresh 🚫 Back 🚫 Forward 🧳 Help						
Find: Go Server Group Protocol III.064.100.153 III.014.127.254 IIII.014.127.254 Protocol III.014.127.254 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Device List □ ₽ × ♣ Add □ Delete Ø Connect	Configuration > Device Management > AAA Server Groups	C Add AAA Server Group				
OK Cancel Help	Find: Go ID.64.72.1 ID.64.100.94 ID.64.100.153 ID.134.126.254 ID.134.126.254 ID.134.127.254 Device Management ID ID.64.00.153 ID.134.127.254 ID.134.127.254 ID ID Period Management Access ID ID ID ID ID Management Access ID ID ID IDAP Attribute Map ID AAA Access ID DYNamic Access Policies ID ID ID<	Server Group Protocol LOCAL LOCAL Find: Servers in the Selected Group Server Name or IP Address Interface	AAA Server Group: OpenOTP_Servers Protocol: RADIUS Accounting Mode: Simultaneous Simultaneous Single Reactivation Mode: Depletion Timed Timed Dead Time: 10 ID minutes Max Failed Attempts: 3 Enable interim accounting update Enable Active Directory Agent mode VPN3K Compatibility Option OK Cancel				

- 6. In Servers in the Selected Group section select Add.
- 7. In Add AAA Server view set (see example picture below):
- > Interface interface through which Cisco communicates with OpenOTP. This should be management or intranet.
- > Server Name or IP Address OpenOTP IP address or hostname.
- > Timeout i.e. 10 seconds.
- > Server Secret Key value testing123 (preconfigured to OpenOTP).
- > Leave other values as default and commit add.

File View Tools Wizards Windo	w Help						
I Home 💑 Configuration 🔯 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🢡 Help							
Device List 리 무 ×	Configuration > Remote Access VPN	> Clientless SSL VPN Access > Connection Pr	<u>ofiles</u>				
Device List Image: Connect Find: Go Image: Connect Go Find: Go Image: Connect Image: Connect Image: Connect Image: Connect Image: Connect Connect Image: Connect Image: Connect Image: Connect Connect Image: Connect Image: Connect	Configuration > Remote Access VPN Access Interfaces Enable interfaces for clientless SSL VPN Interface outside dmz inside partner-dmz Image Setting Allow user to select connection profile Allow user to enter internal password Shutdown portal login page. Connection Profiles Connection profile (tunnel group) specition Name DefaultRAGroup DefaultWEEVPNGroup	Solution of the login page. Allow decess Allow Access Image: Imag	ice Certificate Port Setting • You can configure the map				
Host Scan Image							

8. Cisco ASA - OpenOTP RADIUS connectivity is now configured. The remaining step is to activate the new RADIUS Server on or more of Cisco ASA Connection Profiles, whereas here we create a test profile.

9. Select Clienteles SSL VPN Access -> Connection Profiles

10. Click Add in Connection Profiles section.

11. In Add Clientless SSL VPN Connection Profile set (see example picture below):

- > Name OpenOTP_Test_Profile
- > AAA Server Group select the previously created server group OpenOTP_Servers.
- > In Clienteles SSL VPN menu entry on left:
- > In Connection Aliases section select Add.
- > Enter Alias OpenOTP (user will display a drop-down menu on login with OpenOTP as one entry).
- > Click OK



12. In Login Page Settings section check Allow users to select connection profile.

13. Cisco ASA is now configured and you can proceed to test your login.

🛕 Note

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

4. Simple push-based authentication with ASA

This chapter is only relevant if you want to use simple push to Accept/Reject as the 2nd-factor authentication. For more information on simple push please see how to configure push login with OpenOTP

Cisco ASA radius authentication timeouts are typically too short for the user to be able to authenticate with a simple push. To use push authentication, you must edit the */opt/radiusd/conf/radiusd.conf* and enable "fix_timeout = yes" option.

If you have configured multiple Radius Bridge servers in high-availability mode into your ASA AAA Server Group, you also need to ensure that the Cisco ASA config-aaa-server-host timeout setting is longer than your Push Timeout.

📬 Add AAA Server		×			
Server Group:	RAD_SVR_GRP				
Interface Name:	inside 💌				
Server Name or IP Address:	192.168.1.2				
Timeout:	45	seconds			
RADIUS Parameters					
Server Authentication Port: 1645					
Server Accounting Port:	1646				
Retry Interval:	10 seconds				
Server Secret Key:					
Common Password:					
ACL Netmask Convert:	Standard				
ACE NOTINGS CONVERT					
ОК	Cancel Help				
OK	Cancel Help				

This manual was prepared with great care. However, RCDevs 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 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 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 S.A. The latter especially applies for data processing systems. RCDevs 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 S.A. @ 2019 RCDevs S.A, All Rights Reserved