

F5 BIG-IP APM

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.

F5 BIG-IP APM

[F5 APM](#) [APM](#) [F5](#) [F5 BIG-IP](#) [VPN](#)

1. 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).

2. Register your F5 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 F5 VPN server.

Example:

```
client <VPN Server IP> {  
  secret = testing123  
  shortname = F5  
}
```

3. Configuring new RADIUS AAA Server to APM

Configuring OTP authentication to APM means simply adding OpenOTP RADIUS AAA configuration to one of your Access Policies. To use an existing Access Profile then on APM management UI you only need to add a RADIUS through: Access Policy → AAA Servers → RADIUS and create a new RADIUS server which you can then attach to your existing access profile(s). To create an all-new Access Profile and RADIUS connector: 1. Login to your F5 web-based administration UI. 2. From the left-hand menu, select Wizards → Device Wizards. 3. Select Portal Access Setup Wizard.



4. To Basic Properties that opens up, set: * Policy Name - A descriptive name for your new access policy, i.e. OpenOTP_Policy

(white spaces are not allowed). * Caption - Use default value set for Policy Name.

- > Click Next to continue. 5. For Authentication Options select New and as Authentication select RADIUS.

Wizards >> Device Wizards >> Portal Access Setup

Select Authentication

Please select the type of authentication you would like to configure for your access policy. When end users access the virtual server they will be shown a logon page to enter credentials. These credentials are checked against a preconfigured external authentication server.

If you would like to test a basic access policy without authentication, you are not authenticating users at all, or you will configure authentication later, you can select No Authentication. To add authentication later, create a new AAA server, then edit your access policy and add an authentication action.

Authentication Options	<input checked="" type="radio"/> Create New <input type="radio"/> Use Existing
Select Authentication	<ul style="list-style-type: none"><input checked="" type="radio"/> RADIUS<input type="radio"/> LDAP<input type="radio"/> Active Directory<input type="radio"/> SecurID<input type="radio"/> HTTP<input type="radio"/> OCSP Responder<input type="radio"/> CRLDP<input type="radio"/> TACACS+<input type="radio"/> No Authentication

6. On Configure AAA Server page, set: * Server Addresses - IP address or hostname of your OpenOTP VM • Authentication Service Port - leave as default (1812). * Secret - enter testing123 (pre-configured to OpenOTP). * Click Next to continue.

Wizards >> Device Wizards >> Portal Access Setup

Portal Access

Specify the internal web application start URI. This defines the first page that will be shown to the end user after they log in through the local traffic virtual server (e.g. <http://myintranet.siterequest.com> or <http://myintranet/start.html>).

You can create your own application from scratch by selecting Custom, or you can use an existing application template from the Select Application list.

Select Application	Custom
Portal Access Start URI	<input type="text" value="https://my.intranet/sampleapp/"/>
SSO Configuration	<input type="checkbox"/> Configure SSO

7. On Portal Access and Virtual Server page set: * Virtual Server IP Address - Enter IP address of your external interface VLAN that your users would connect for access. * Click Next to continue.

Wizards » Device Wizards » Portal Access Setup

Virtual Server (HTTPS connection)

Specify an IP address to create a local traffic virtual server that is correctly configured for web applications. Your end users connect to a DNS name representing this destination address to start a web applications connection.

Check the option **Create Redirect Virtual Server (HTTP to HTTPS)** to create a local traffic virtual server that automatically redirects users who connect using **http://** instead of **https://** with their web browser.

For information on installing a valid SSL server certificate and using this destination address behind a firewall, please see the **Configuration Guide for BIG-IP® Access Policy Manager**.

Virtual Server IP Address	<input type="text" value="10.128.10.240"/>
Redirect Server	<input checked="" type="checkbox"/> Create Redirect Virtual Server (HTTP to HTTPS)


8. Review your configuration and click Next to let the wizard create your new access profile and AAA Server configuration. 9. Once the wizard completes, you will be able to test your access at the IP you set for your Virtual Server.

Note

Don't forget to authorize the communication on 1812 UDP port (default RADIUS port for the authentication) from your F5 APM system to your WebADM instance at the firewall level.

4. Test your APM login

1. Go to your Virtual Server IP with a web browser (one set in Wizard, i.e. <https://10.128.10.240/>).
2. Secure Login Page opens. 3. Enter your domain login name and password:




**Secure Logon
for F5 Networks**

Username

Password

4. Page will refresh to prompt you to enter your OTP. 5. Press enter the OTP you have at hand (Yubikey, Google Authenticator, Hard Token, ...).



Enter your TOKEN one-time password

6. Your intranet web resource should now open!

5. Video Tutorial



[Play Video on Youtube](#)

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