PLIVO SMS GATEWAY & WEBADM

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.

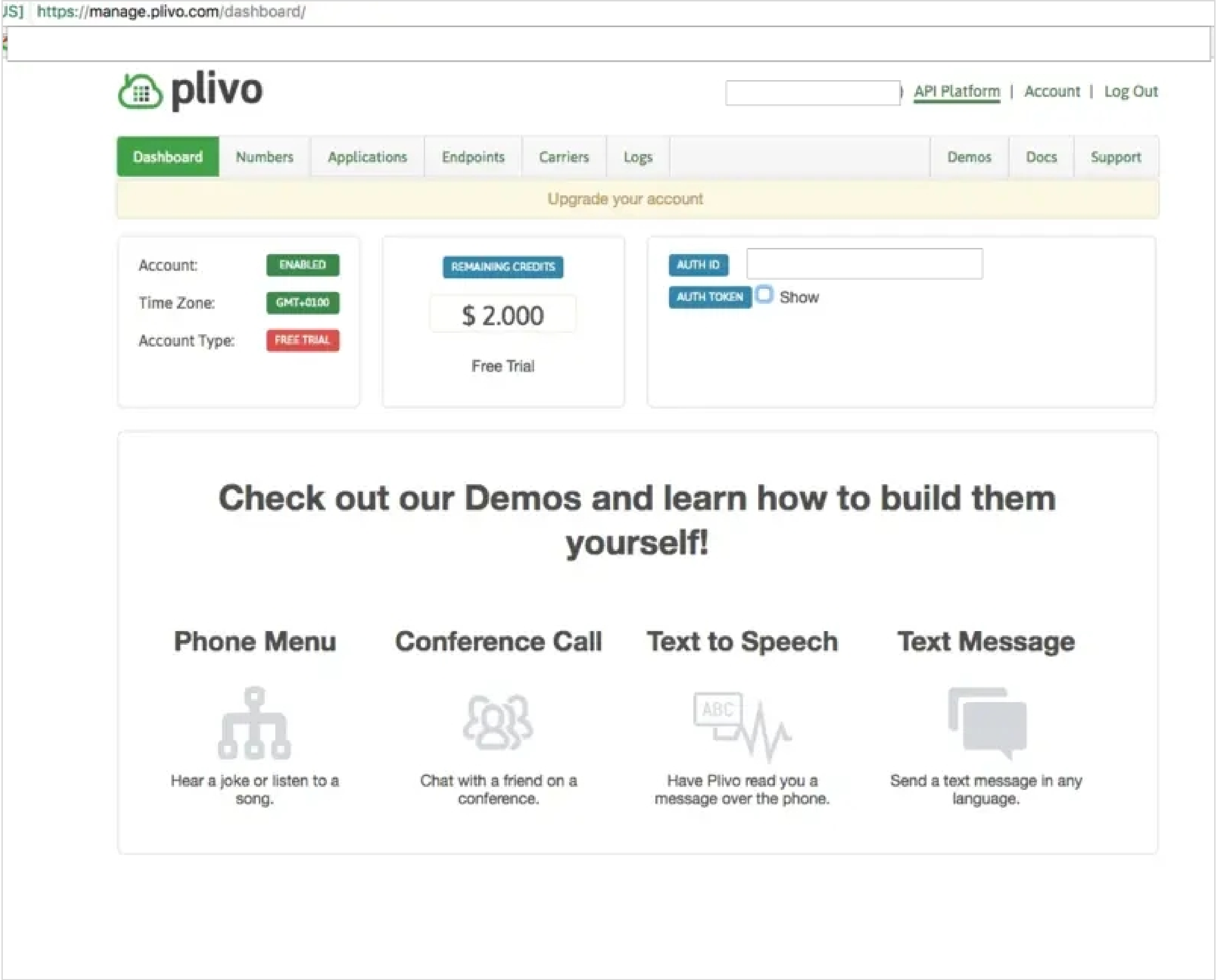
Limited Warranty - Copyright (c) 2010-2024 RCDevs Security SA. All Rights Reserved.

Plivo SMS Gateway & WebADM

SMS

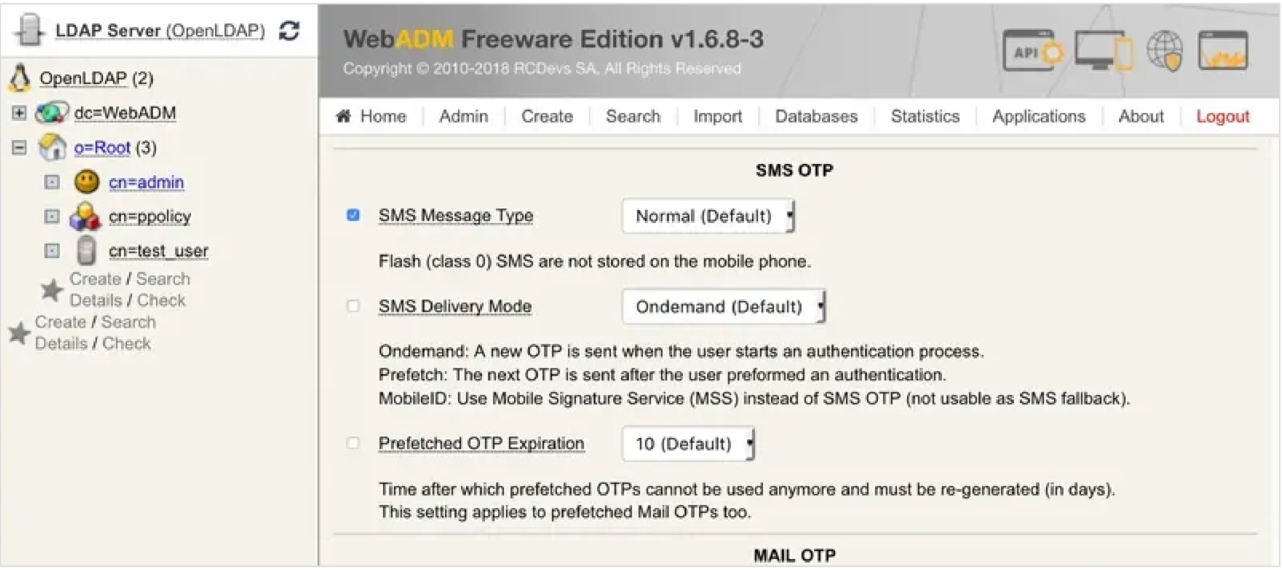
1. Set up an Account on Plivo

- Sign up for an account.
- Add the credit to the account (however, you should get some initial free credit when signing up).
- From the Dashboard go to API Platform and copy the AuthID and the AuthToken.


https://manage.plivo.com/dashboard/
plivo
API Platform | Account | Log Out
Dashboard
Numbers
Applications
Endpoints
Carriers
Logs
Demos
Docs
Support
Upgrade your account
Account: ENABLED
Time Zone: GMT+0100
Account Type: FREE TRIAL
REMAINING CREDITS
$ 2.000
Free Trial
AUTH ID
AUTH TOKEN
□ Show
Check out our Demos and learn how to build them yourself!
Phone Menu
Hear a joke or listen to a song.
Conference Call
Chat with a friend on a conference.
Text to Speech
ABC
Have Plivo read you a message over the phone.
Text Message
Send a text message in any language.

2. Configure WebADM:

- Login to WebADM.
- Go to `Applications` –> `MFA Authentication Server`.
  - Configure the section `SMS OTP`.
- `SMS Message Type` ==> `Normal` (We advise testing using Normal first).



SMS OTP

☑ SMS Message Type: Normal (Default)

Flash (class 0) SMS are not stored on the mobile phone.

☐ SMS Delivery Mode: Ondemand (Default)

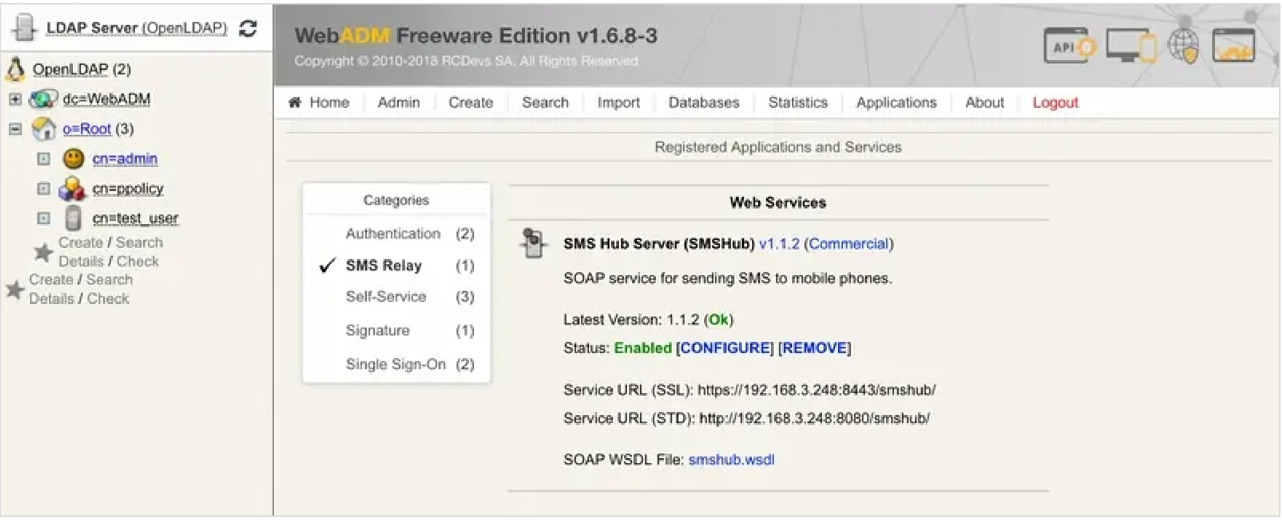
Ondemand: A new OTP is sent when the user starts an authentication process.
Prefetch: The next OTP is sent after the user preformed an authentication.
MobileID: Use Mobile Signature Service (MSS) instead of SMS OTP (not usable as SMS fallback).

☐ Prefetched OTP Expiration: 10 (Default)

Time after which prefetched OTPs cannot be used anymore and must be re-generated (in days).
This setting applies to prefetched Mail OTPs too.

MAIL OTP

- Apply changes.
- Go to `Applications` —> `SMS Relay`.
  - Register the SMS Hub Server application (if you haven't already).
  - Click on `CONFIGURE`.



Web Services

SMS Hub Server (SMSHub) v1.1.2 (Commercial)

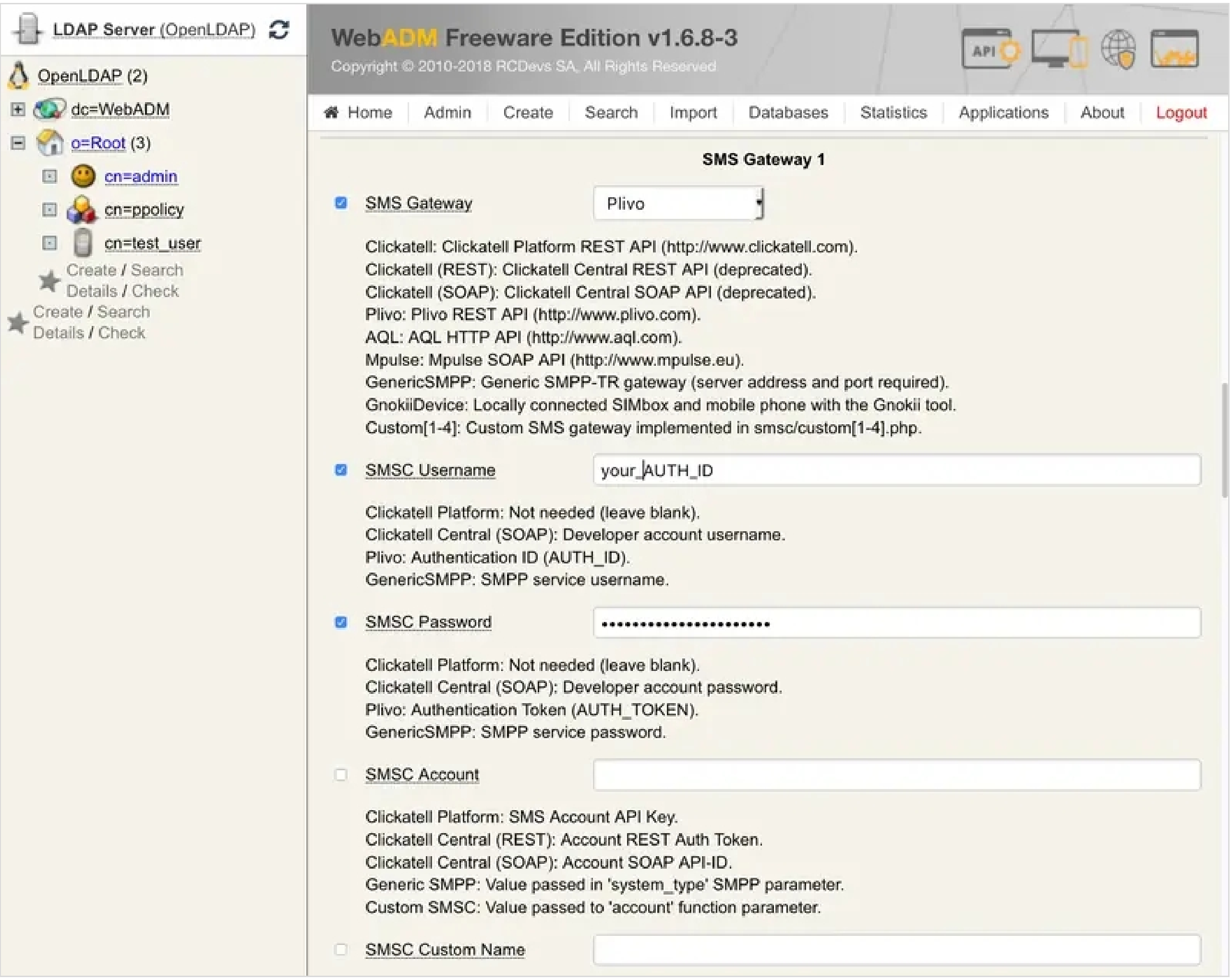
SOAP service for sending SMS to mobile phones.

Latest Version: 1.1.2 (Ok)
Status: Enabled [CONFIGURE] [REMOVE]

Service URL (SSL): https://192.168.3.248:8443/smshub/
Service URL (STD): http://192.168.3.248:8080/smshub/

SOAP WSDL File: smshub.wsdl

- Set up the `SMS Gateway 1` section with the details from Plivo - instructions are embedded in the page.



SMS Gateway 1

☑ SMS Gateway: Plivo

Clickatell: Clickatell Platform REST API (http://www.clickatell.com).
Clickatell (REST): Clickatell Central REST API (deprecated).
Clickatell (SOAP): Clickatell Central SOAP API (deprecated).
Plivo: Plivo REST API (http://www.plivo.com).
AQL: AQL HTTP API (http://www.aql.com).
Mpulse: Mpulse SOAP API (http://www.mpulse.eu).
GenericSMPP: Generic SMPP-TR gateway (server address and port required).
GnokiiDevice: Locally connected SIMbox and mobile phone with the Gnokii tool.
Custom[1-4]: Custom SMS gateway implemented in smsc/custom[1-4].php.

☑ SMSC Username: your_AUTH_ID

Clickatell Platform: Not needed (leave blank).
Clickatell Central (SOAP): Developer account username.
Plivo: Authentication ID (AUTH_ID).
GenericSMPP: SMPP service username.

☑ SMSC Password: ••••••••••••••••••••••

Clickatell Platform: Not needed (leave blank).
Clickatell Central (SOAP): Developer account password.
Plivo: Authentication Token (AUTH_TOKEN).
GenericSMPP: SMPP service password.

□ SMSC Account

Clickatell Platform: SMS Account API Key.
Clickatell Central (REST): Account REST Auth Token.
Clickatell Central (SOAP): Account SOAP API-ID.
Generic SMPP: Value passed in 'system_type' SMPP parameter.
Custom SMSC: Value passed to 'account' function parameter.

□ SMSC Custom Name

- Apply changes.

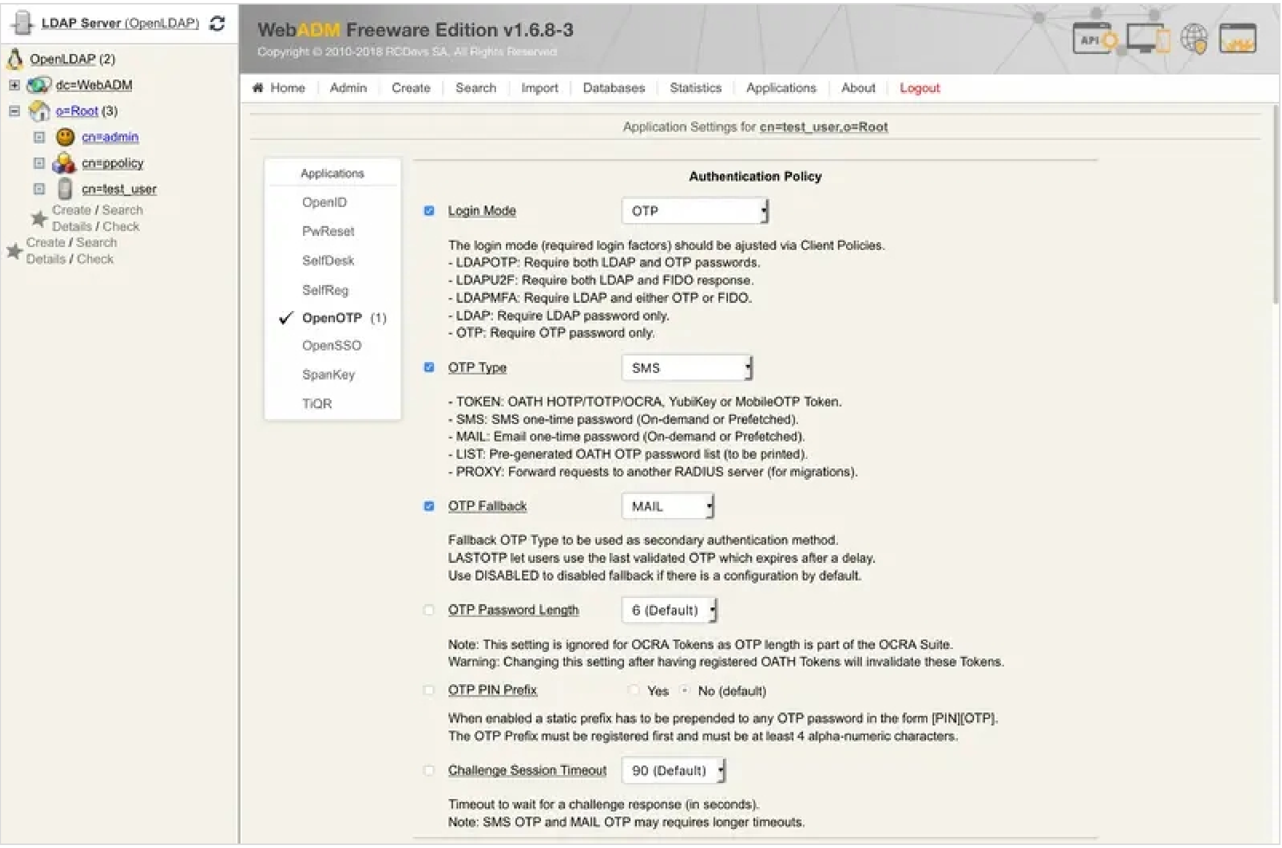
3. Activate SMS Login on Group of Users:

- Select the AD/LDAP group.
- If the group is not activated (to openotp), choose `Activate` now.
- In the `Object Details` box, choose to `CONFIGURE` on WebADM Settings.
- Choose OpenOTP Settings and set.

```
OTP Type ==> SMS
```

4. Configure User (if needed)

- The user needs a mobile number, which can be added (if not already existing) as an attribute.
- The user needs an OpenOTP authentication setup which uses SMS - (in WebADM settings for the user, under `OpenOTP` configuration).



Application Settings for cn=test_user,o=Root

Authentication Policy

☑ Login Mode: OTP

The login mode (required login factors) should be ajusted 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: SMS

- 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: MAIL

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 ● No (default)

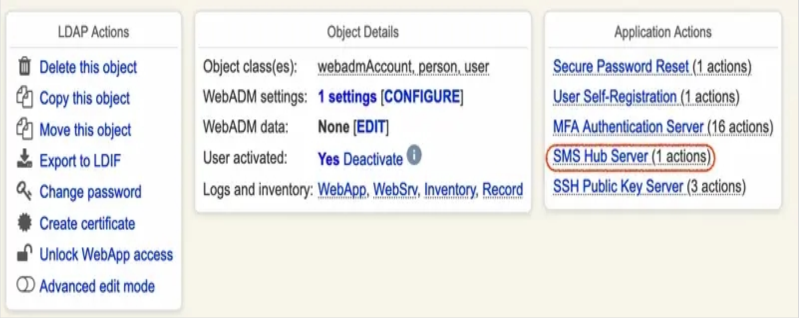
When enabled a static prefix has to be prepended to any OTP password in the form [PIN][OTP].
The OTP Prefix must be registered first and must be at least 4 alpha-numeric characters.

□ Challenge Session Timeout: 90 (Default)

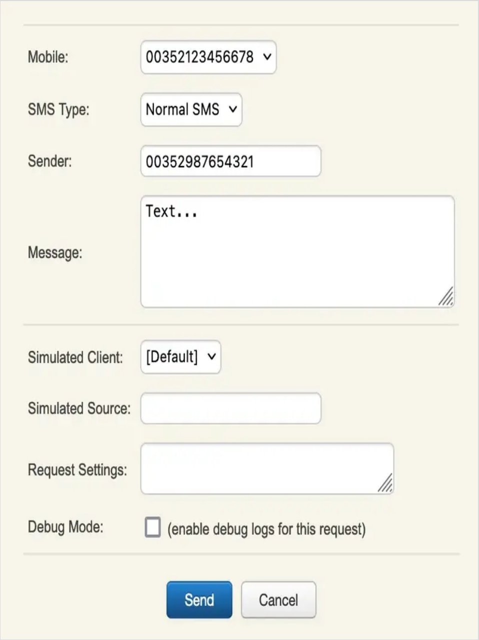
Timeout to wait for a challenge response (in seconds).
Note: SMS OTP and MAIL OTP may requires longer timeouts.

5. Test

- Test the configuration using a valid user with a mobile number and using the MFA Authentication service link in the user's page :



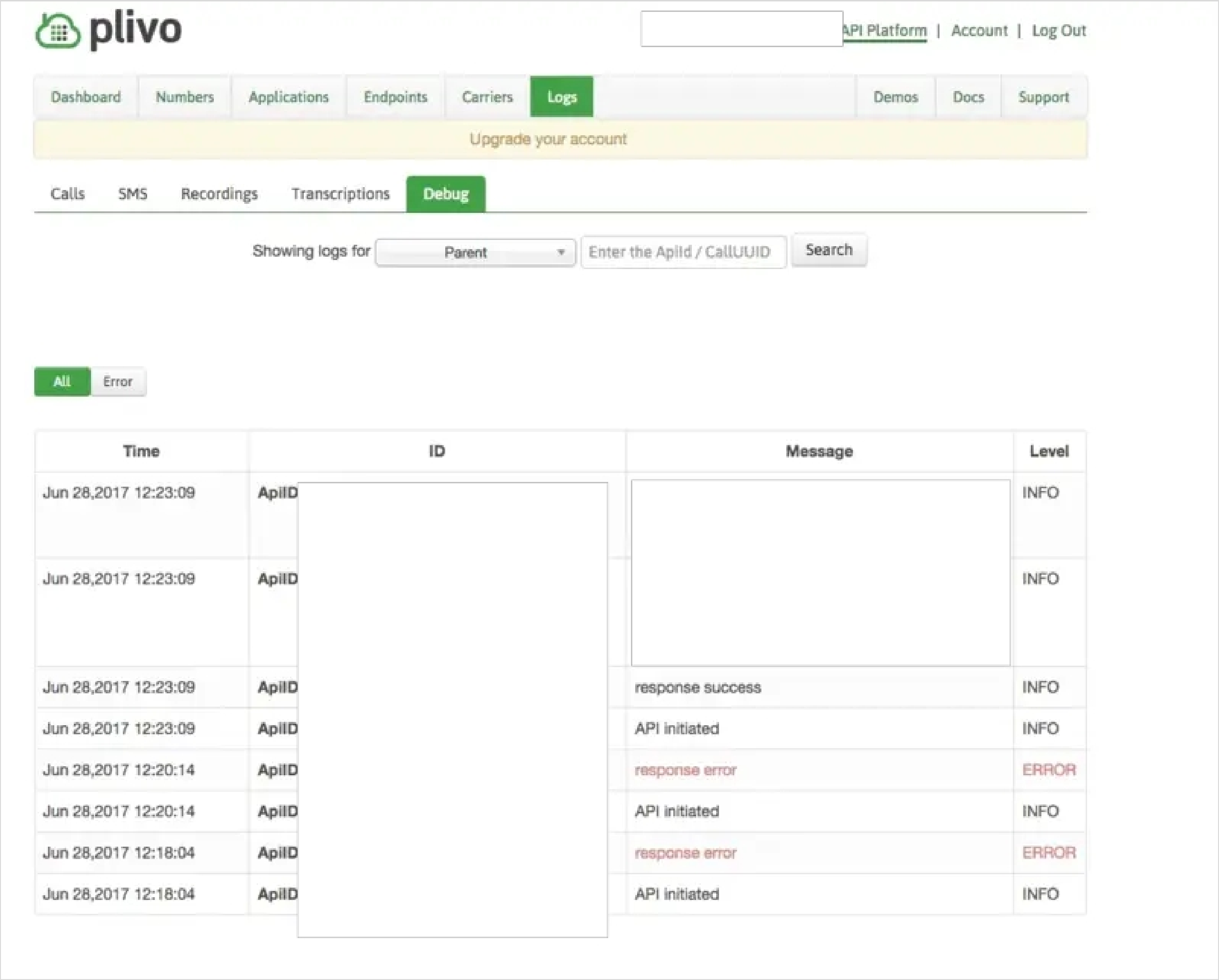
Object class(es): webadmAccount, person, user
WebADM settings: 1 settings [CONFIGURE]
WebADM data: None [EDIT]
User activated: Yes Deactivate
Logs and inventory: WebApp, WebSrv, Inventory, Record



Mobile:	00352123456678
SMS Type:	Normal SMS
Sender:	00352987654321
Message:	Text...
Simulated Client:	[Default]
Simulated Source:	
Request Settings:	
Debug Mode:	□ (enable debug logs for this request)

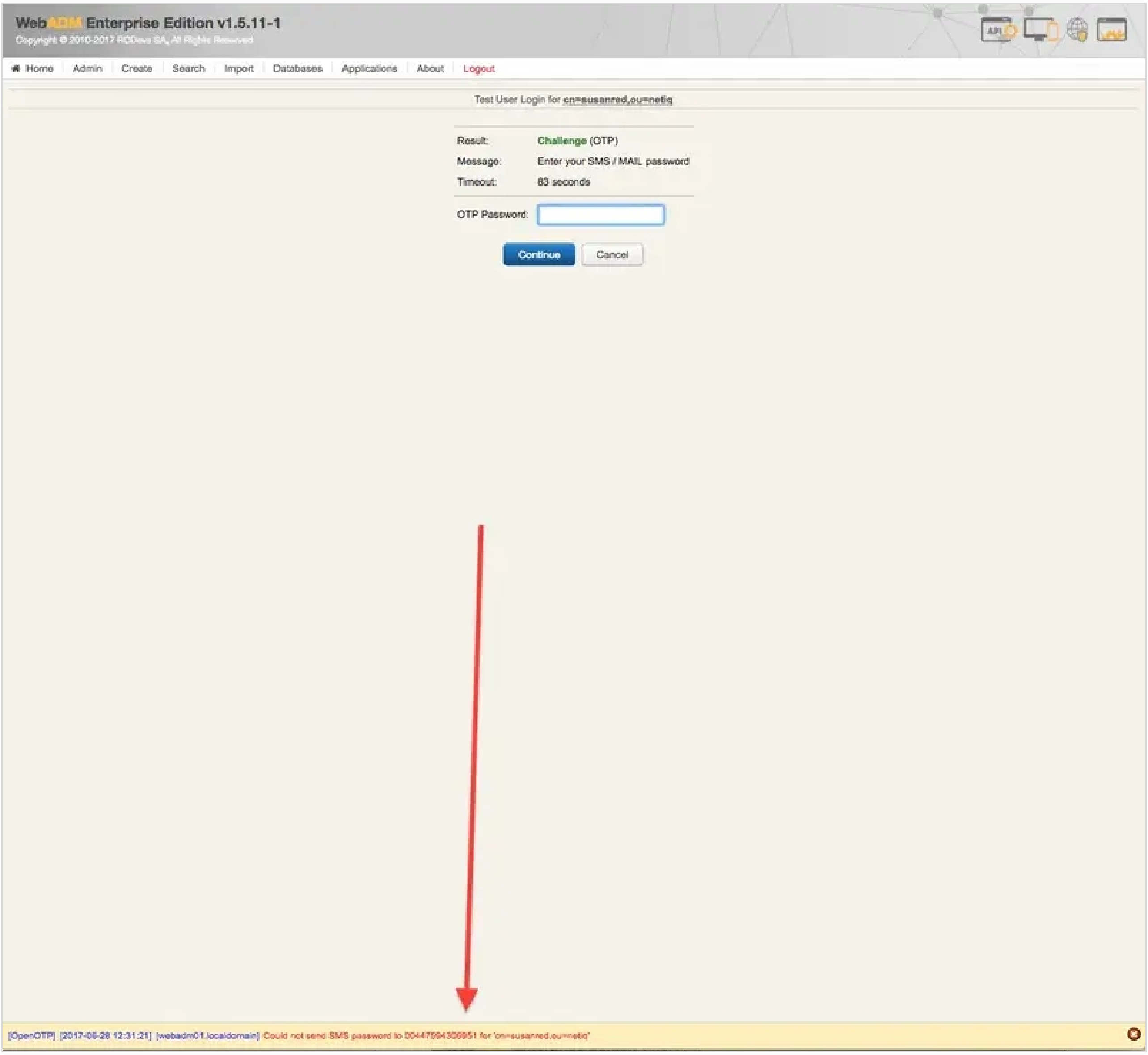
6. Troubleshooting

- **BEWARE** of the “Sandbox” numbers, check Plivo documentation website.
- In case of problems with Plivo, head to the Logs -> Debug section in your dashboard to check what’s happening (and/or check the WebADM Logs).



Time	ID	Message	Level
Jun 28,2017 12:23:09	ApiID		INFO
Jun 28,2017 12:23:09	ApiID		INFO
Jun 28,2017 12:23:09	ApiID	response success	INFO
Jun 28,2017 12:23:09	ApiID	API initiated	INFO
Jun 28,2017 12:20:14	ApiID	response error	ERROR
Jun 28,2017 12:20:14	ApiID	API initiated	INFO
Jun 28,2017 12:18:04	ApiID	response error	ERROR
Jun 28,2017 12:18:04	ApiID	API initiated	INFO

- If WebADM fails to send the SMS, you will be notified at the bottom of the page (typical WebADM notification pattern).


WebADM Enterprise Edition v1.5.11-1
Copyright © 2010-2017 RCDevs SA, All Rights Reserved
Home
Admin
Create
Search
Import
Databases
Applications
About
Logout
Continue
Cancel

Test User Login for cn=susanred,ou=netiq

Result: Challenge (OTP)

Message: Enter your SMS / MAIL password

Timeout: 83 seconds

OTP Password:

[OpenOTP] [2017-06-28 12:31:21] [webadm01.localdomain] Could not send SMS password to 00447594306951 for 'cn=susanred,ou=netiq'

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