



OPENID-SAML IDP WEB SERVICE

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.

OpenID-SAML IdP Web Service

[Web-Service](#) [SSO](#) [Federation](#)

OpenID/SAML Identity Provider

The installation of OpenID/SAML IdP is straightforward and only consists of running the self-installer and configure the application in WebADM.

You do not have to modify any files in the OpenID install directory! The web applications configurations are managed and stored in LDAP by WebADM. To configure OpenID/SAML, just enter WebADM as super administrator and got to the 'Applications' menu. Click OpenID/SAML to enter the web-based configuration.

OpenID/SAML application logs are accessible in the Databases menu in WebADM.

Note: To be able to use OpenID/SAML, any LDAP user must be a WebADM account. That means usable LDAP accounts are those containing the webadmAccount LDAP object class. You can enable the WebADM features on any LDAP user/group by extending it with the webadmAccount object class (from object extension list).

Inline WebApps:

You can embed a Web app on your website in an HTML iFrame or Object.

#Example

```
<object data="https://<webadm_addr>/webapps/openid?inline=1" />
```

1. SAML IdP Configuration

SAML IdP requires a certificate and a private key to be set in the configurations. You can generate an X.509 certificate and private key with OpenSSL:

```
openssl genrsa -out server.key 1024
openssl req -new -key server.key -out server.csr
openssl x509 -req -days 3650 -in server.csr -signkey server.key -out server.crt
```

You can copy/paste the server.crt and server.key contents in your configuration.

The SAML clients (Service Providers) need to know about the SAML IdP endpoints. Most clients will accept the auto-configuration with an XML-based metadata URL. The server metadata URL is:

<https://yourserver/webappd/openid/metadata/>. If you need to manually enter the IdP service URLs go to the HTML-based metadata URL with your Web browser:

<https://yourserver/webapps/openid/metadata/html/>. You will find client configurations like:

- > The SAML entityID of the IdP.
- > The SAML server certificate.
- > The SingleSignOnService URL.
- > The SingleLogoutService URL.

Important

Many SAML Service Providers will require your WebADM to be run with a trusted SSL certificate. You can replace the default WebADM SSL certificate with your own. Just replace the `/opt/webadm/pki/httpd.crt` and `/opt/webadm/pki/httpd.key`.

2. OpenID IdP Configuration

Version 1.2x includes the support for OpenID-Connect and OAuth2.

To use your identity provider in OpenID-Connect mode, the client configuration must pass the scope 'openid' in the IdP requests. The supported OpenID-Connect scopes are: basic, email, phone and profile.

To use your identity provider in OAuth2 mode, the client must pass the scope 'profile' in the IdP requests.

If your client application needs the user's email address, you can additionally request the openid email scope.

2.1 Sample OpenID Client Configurations

This chapter contains some sample configurations for some OpenID integrations, which can be used as a reference.

2.1.1 Grafana

First, create a new or update an existing Client Policy in WebADM > Admin > Client Policies. The policy name or friendly name must match the `client_id` defined in Grafana configuration (see below).

In the client policy, configure Application Settings > Edit > OpenID & SAML Provider > Client Secret. This secret must match the `client_secret` defined in Grafana.

Once these settings are applied, you can configure Grafana to use OpenOTP IdP for SSO login:

```
[auth.generic_oauth]
enabled = true
name = OpenOTP
allow_sign_up = true
client_id = grafana
client_secret = secret
scopes = openid profile email
auth_url = https://<openotp_server_address>/webapps/openid/index.php
token_url = https://<openotp_server_address>/webapps/openid/index.php
api_url = https://<openotp_server_address>/webapps/openid/index.php
tls_skip_verify_insecure = true
```

2.1.1 Apache Guacamole

First you need to install the OpenID extension to Apache Guacamole. See [Guacamole documentation](#) for instructions.

Please note that the authentication extensions in the GUACAMOLE_HOME/extensions directory are loaded in alphabetical order, so if you have another authentication extension which is alphabetically before the OpenID extension, then the OpenID extension will not be loaded. This is the case for example with guacamole-auth-jdbc-mysql extension. To bypass this issue you can rename the guacamole-auth-openid-1.0.0.jar to for example guacamole-auth-Openid-1.0.0.jar.

Once the extension is installed, you can configure the OpenID settings in GUACAMOLE_HOME/guacamole.properties

```
#OpenID authentication
openid-authorization-endpoint: https://<openotp_server_address>/openid/index.php
openid-jwks-endpoint: https://<openotp_server_address>/openid/certs.php
openid-issuer: https://<openotp_server_address>/webapps/openid/
openid-client-id: Guacamole
openid-redirect-uri: https://<guacamole_server_address>/guacamole/
```

Once the configuration is completed, you need to restart tomcat for it to take effect. If you want to login as an existing Guacamole Admin user (for example guacadmin) while OpenID is enabled, you need to create that user in WebADM as well.

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 SA, All Rights Reserved