aPersona ASM End-User Self-Service v1.1.0 Installation & Configuration Guide

Published Oct 21, 2019

Release Version 1.1.0

aPersona End-User Self-Service v1.1.0 Installation & Configuration Guide

Release Version: 1.1.0

aPersona, Inc.
3737 Glenwood Ave
Suite 100
Raleigh, NC 27612
United States of America

Disclaimers
This document is furnished "AS IS." aPersona, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. aPersona, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of aPersona, Inc. and its licensors, and are furnished under a license from aPersona, Inc.

aPersona, Inc. and the aPersona logo, are trademarks of aPersona, Inc., and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Trademarks
aPersona™

Contents

Welcome & Support

Welcome to the aPersona End-User Self-Service Installation & Configuration Guide. If after reviewing this guide, you have questions or would like to setup an online session for assistance, please call us. Generally the integration of aPersona takes a few hours to a couple of days depending on your specific setup.

Audience: Knowledgeable PHP web developer & Linux Administrators.

Assistance & Support:
http://support.apersona.com

Document Change Log

Installation Environment

All environments below were utilized in the development of the services. Other Operating Systems that support PHP can also be used, but have not been tested.

Application Operating System

- RHEL/CentOS 7.x (yum updated)
- selinux = permissive or disabled

Web Server

- httpd
- # yum install httpd
- # yum install mod_ssl openssl -y
- TLS v1.2 certificates properly configured and functioning for your desired setup (Public or Private)
- https://yourdomain.com properly routing and functioning.

Application Language - PHP

- PHP v 5.4.16
- # yum install php -y
- # yum install php-ldap -y

Back-end User Directory: LDAP

- Microsoft Active Directory running on Windows Server 2016

Operating Environment Configurations

Application Operating System

- selinux = permissive or disabled
- yum updated

Web Server (httpd)

- If you are not familiar with setting up HTTPS on httpd, then we provide some limited help here.

- First ensure your web server is working on Port 80: http://yourdomain.com
- Ensure SSL Port 443 is also open for the next set of steps.
- You will need at least 3 certificates.
    1. Your issues domain certificate. E.g. yourdomain.crt
    2. Your private key in pem format. E.g. yourdomain_pri_key.pem
    3. Your Server Certificate Chain/Bundle that includes your intermediate certificate. E.g. yourdomain_bundle.crt
- Copy the three files to the locations below:
- Edit the file: /etc/httpd/conf.d/ssl.conf

```
SSLCertificateFile /etc/pki/tls/certs/yourdomain.crt
SSLCertificateKeyFile /etc/pki/tls/private/yourdomain_pri_key.pem
SSLCertificateChainFile /etc/pki/tls/certs/yourdomain_bundle.crt
```

- Restart httpd: # systemctl restart httpd
- Ensure you can access page: https://yourdomain.com before you continue.

Back-end User Directory: AD/LDAP

- Export a BASE64/x.509 Public Certificate from AD/LDAP. DO NOT INCLUDE THE PRIVATE KEY.
- For Windows, here are the steps:
    1. Run >> mmc
    2. File >> Add Remove Snap-in
    3. Select Certificates from the Available snap-ins window, click Add > , Then Select “Computer account” >> Click Next >> Local Computer >> Finish >> OK
    4. Expand Console Root > Certificates (Local Computer) > Personal > Certificates
    5. Right click your domain certificate that is found that is you Server Authentication Purpose Cert. >> All Tasks >> Export **[Note, if your server does not have a valid certificate, then stop and contact your Windows Admin for certificate help.]**
    6. On the Certificate Export Wizard click Next >> No, do not export the private key >> Next >> Base-64 encoded x.509 (.CER) >> Next >> Click Browse and Enter a file name: ex. yourdomain.com.base64.x.509.pub.cer and save the certificate in a folder of your choice. >> Click Save.
- Ensure port 636 is open on the server firewall, and that port 636 is also open on any network routes to the server.
- LOCK DOWN THE SERVER PORT 636 to its own local IPv4 IP and to only the outside IP’s that will be executing queries against AD/LDAP!

Application Language: PHP

- Create a temporary 1 line PHP Info file on your webserver at: /var/www/html/phpinfo.php

```
<? php phpinfo(); ?>
```

Save the file.

- Run the program: https://yourdomain.com/phpinfo.php and ensure you get a php report back.
- Edit your php.ini file and update the following:
    1. session.cookie_secure = 1
    2. session.cookie_httponly = 1
    3. session.cookie_lifetime = 1200 *(Maxium session lifetime of 20 minutes. Set your setup as needed.)*

Save the file.

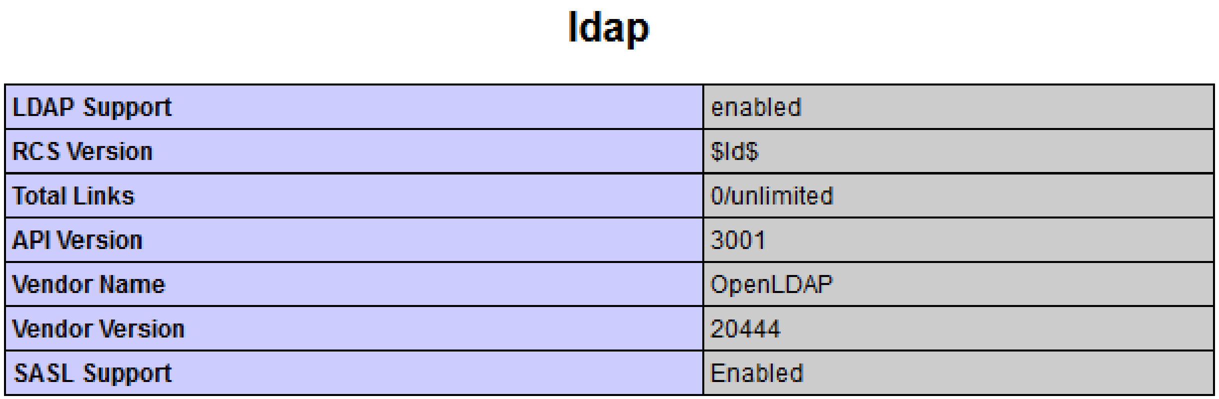
- Install your LDAP Public Certificate into PHP:
- Copy your cer file to: /etc/openldap/certs/yourdomain.com.base64.x.509.pub.cer
- Edit file: /etc/openldap/ldap.conf

  Add the following two lines:

```
TLS_REQCERT never
TLS_CACERT /etc/openldap/certs/yourdomain.com.base64.x.509.pub.cer
```

- Save the file.
- Restart httpd: # systemctl restart httpd
- Re-run https://yourdomain.com/phpinfo.php and verify the following in your PHP Info output. (Your specific Ldap section might be slightly different, but you should see the section.)

Additional .ini files parsed	/etc/php.d/ldap.ini
Protocols	ldap, ldaps



ldap

LDAP Support	enabled
RCS Version	Id
Total Links	0/unlimited
API Version	3001
Vendor Name	OpenLDAP
Vendor Version	20444
SASL Support	Enabled

aPersona End-User Application Installation and Configurations

Setup your .ini files

1. Decide where you want to store your .ini files and where you want to store your log file
2. Download the aPersona End-User Application and unzip the contents.
3. Edit the file: \asm_api\.application_setup.ini
   Edit each of the ini variables to point to the location of your planned configuration and log files. The default is /var/www/asm_self_svc

   ```
   apersona_asm_id_mgmt_branding_ini_file="/var/www/asm_self_svc/application_branding.ini"
   apersona_api_properties_ini_file="/var/www/asm_self_svc/apersona_api_properties.ini"
   ldap_connection_ini_file="/var/www/asm_self_svc/ldap_connection_properties.ini"
   ldap_properties_ini_file="/var/www/asm_self_svc/ldap_properties.ini"
   asm_id_mgmt_log_file="/var/www/asm_self_svc/asm-id-mgmt.log"
   apersona_copyright_version_ini_file="/var/www/asm_self_svc/copyright_version.ini"
   ```
4. Copy the aPersona ASM End-User Self-Service application to your web server. E.g. /var/www/html/asm_self_svc/
5. Copy the asm_self_svc configuration files to the location set in the .application_setup.ini file. e.g. /var/www/asm_self_svc/
6. Set ownership and rights to the configuration folder and files so apache can access them:
   From the linux console:

   ```
   # chown -R apache:apache /var/www/asm_self_svc
   # chmod 400 /var/www/asm_self_svc/*.ini
   ```

```
# chmod 644 /var/www/asm_self_svc/asm-id-mgmt.log
```

7. Edit each of the /var/www/asm_self_svc/ ini files as appropriate. Each file contains help and instructions for making modifications.

application_branding.ini	Mostly Text Branding. To brand the logo, replace ../branding/logo.png with your own. (201x40)
apersona_api_properties.ini	aPersona ASM URL and Security Policy Keys. The defaults will work against the aPersona ASM Test Cloud, so you can run some initial testing without installing your own aPersona ASM Service. You can request your own aPersona ASM Test instance here that will allow you to configure your security policies to your liking.
ldap_connection_properties.ini	LDAP Domain/Admin Credentials & LDAP URL
ldap_properties.ini	Lots of customization options here. Read the file and contact aPersona if you have any questions.

Optional: Setup a cron job to compress the log files once per day.

For Example: Move the log file to a tmp file (with overwrite), then zip it up 5 min later. Then move temp to old.
Edit /etc/contab

```
00 1 * * * root /usr/bin/mv -f /var/www/asm_self_svc/asm-id-mgmt.log /var/www/asm_self_svc/asm-id-mgmt.log.tmp
05 1 * * * root /usr/bin/zip /var/www/asm_self_svc/asm-id-mgmt_$(date +\%Y\%m\%d\%H).zip /var/www/asm_self_svc/asm-id-mgmt.log.tmp
10 1 * * * root /usr/bin/mv -f /var/www/asm_self_svc/asm-id-mgmt.log.tmp /var/www/asm_self_svc/asm-id-mgmt.log.prev
```

Save the file

```
# systemctl restart crond
```