

Test system Build Diary

2023 R1 (V12 patch 33) Install test SAML2 service provider then configure X3 to authenticate using SAML2

Disclaimer

This document is provided "as is" and is for your guidance and educational purposes only. It does not replace the Online documentation, nor is any warranty expressed nor implied for the steps described herein.

Document Information

Author: Mike Shaw, Sage UK X3 Support Team

Contents

Introduction	3
2023 R1 – install SAML2 service and configure X3 for SAML2 build diary	4
Objective	4
Documentation to use for planning and execution of this task	6
Install SimpleSAMLphp as a Windows service	7
Create SSL certificate	7
Update firewall rules for “mzAuth”	16
Configure Sage X3 to use SAML2 authentication	17
Edit Sage X3 nodelocal.js for SAML2 (MZWEB1, MZWEB2, MZWEB3).....	19
Logout behavior from X3 / SAML.....	22
Additional Sage X3/SAML2 configuration to provide best practice/security	23
Troubleshooting.....	25
Conclusion.....	26

Introduction

What is a "Build Diary"

A Build Diary simply describes the steps taken by Sage Support to perform a task or tasks on our internal test systems. Build diaries could be created for major multi-node installations, but may also just be describing the steps taken when installing a small hotfix, or anything in-between.

Why is this being shared

It may be useful for you to see the steps we have taken to create or implement some feature or installation, as this may highlight "gotcha's", issues encountered or just give you some guidance if you are planning something similar yourself.

You could potentially use these documents as the base for your own "Workplan document" (Described in "Overview of patching X3 and supporting technologies" <https://www.sagecity.com/gb/sage-x3-uk/b/sage-x3-uk-support-insights/posts/sage-x3-technical-support-tips-and-tricks---march-2021-index>) when you are planning your own activities

Target Audience

This document is aimed at Sage X3 Certified Technical consultants. Sage prescribe that X3 system installation, maintenance, migrations, etc. should be performed by suitably qualified Sage X3 consultants. The prerequisite consideration would be for them to have the latest "Sage X3 Certified Technical Consultant" certification. You can read more about the Sage X3 qualifications and requirements in Sage University (<https://sageu.csod.com/catalog/CustomPage.aspx?id=20000242#tc>)

Additional things to note

- This document does NOT purport to illustrate "best practice" for the task being described
- The steps described will not necessarily be for a "perfect" task, as there may have been issues that needed to be overcome, worked around, or ignored
- The Sage internal test system has network and hardware configuration specific to Sage
- The Sage internal test system does not necessarily include a Windows Domain and has Sage sandbox specific Windows security setup, so operating system permissions are generally not discussed
- If you intend to use these notes as a guide for your own activities, use with caution and perform your own testing to ensure the described steps are suitable and identify any additional considerations that apply to your own situation
- Ensure you only install and use software you are licensed for

What does this Build Diary describe?

This build diary describes setting up a server as a **TEST** SAML2 service provider, which you can then use to configure Sage X3 to authenticate against. I am using X3 version 2023 R1, but the steps would be similar for other Sage X3 versions.

2023 R1 – install SAML2 service and configure X3 for SAML2 build diary

Objective

I want to implement and test SAML2 authentication with Sage X3. I already have my “Big Build” test servers running Sage X3 2023 R1 but do not want to use an external SAML2 provider as it costs money.

I have found an open source SAML2 provider <https://simplesamlphp.org/> that can be implemented on a test server as an on-premise service, which I will use for this activity. NOTE: use third party software at your own risk. Sage have no affiliation with the SAML2 software provider and do not provide support for this software.

Starting architecture and notes

My “Big Build” instance is installed on six Windows Server 2022 servers (Server names mzAD, mzDB, mzPRINT, mzWEB1, mzWEB2, mzWEB3)

Software already loaded:

- Windows Server 2022
- OpenJDK 1.8.0_282
- Edge, Firefox and Chrome browsers
- 7-Zip 19.00
- Sage X3 2023 R1 (Patch 33)

Windows users setup (Local users)

- “x3admin” for installation and management
- “X3run” for service runtime

mzWEB1

- Syracuse (12.18.4.2-0)
- MongoDB (4.4.12.9)
- X3 Runtime (95.2.97)
- AdxAdmin (95.2.97)
- Powershell 7.3.1

mzWEB2

- Syracuse (12.18.4.2-0)
- MongoDB (4.4.12.9)
- X3 Runtime (95.2.97)
- AdxAdmin (95.2.97)
- Powershell 7.3.1

mzWEB3

- Syracuse (12.18.4.2-0)
- MongoDB (4.4.12.9)
- X3 Runtime (95.2.97)

- AdxAdmin (95.2.97)
- Powershell 7.3.1

mzPRINT

- Elastic Search (7.16.3)
- Print Server (2.28.0.10)
- AdxAdmin (95.2.97)

mzAD

- MS AD
- Apache Load Balancer (Apache 2.4)
- X3 Console (2.57.0.11)

mzDB

- SQL Server Database (2019)
- SSMS (18.12.1)

[Firewall setup](#)

The “Big Build” servers are in the same MS AD domain. Firewall rules between these servers allow all traffic. Only external traffic needs to be added to the firewall rules, which should only be port 443 into the MZAD server (see notes later in this document).

My SAML2 installation will be on a separate server (Servername: mzAuth) which will be setup outside the “Big Build” network segment, so will need to ensure appropriate firewall rules are configured.

[Summary of steps to take](#)

Install SimpleSAMLphp as a Windows service (NOTE: If you already have a SAML2 provider available, you can skip this and go straight to the X3 configuration)

- Install and configure Apache service
- Install and configure PHP
- Install and configure SimpleSAMLphp
- Check you can authenticate user against SimpleSAMLphp itself

Configure Sage X3 to use SAML2 authentication

Additional Sage X3/SAML2 configuration to provide best practice/security

Documentation to use for planning and execution of this task

Sage Online documentation

Overall V12 documentation

<https://online-help.sageerpx3.com/erp/12/public/index.html>

SAML2

https://online-help.sageerpx3.com/erp/12/public/administration-reference_saml2.html

Sage Knowledgebase articles or Blogs

How to setup SAML2 with ADFS

<https://support.na.sage.com/selfservice/viewdocument.do?externalId=82916>

How to setup SAML2 authentication with Microsoft Azure

<https://support.na.sage.com/selfservice/viewdocument.do?externalId=91984>

How do I configure Okta to work with SAML2 in X3

<https://support.na.sage.com/selfservice/viewdocument.do?externalId=93491>

External sites

SimpleSAMLphp Installation and Configuration

<https://simplesamlphp.org/docs/latest/simplesamlphp-install.html>

Install SimpleSAMLphp as a Windows service

Use the online help “SimpleSAMLphp Installation and Configuration” at <https://simplesamlphp.org/docs/latest/simplesamlphp-install.html>

Basic steps are to:

- Install and configure Apache service
- Install and configure PHP
- Install and configure SimpleSAMLphp
- Check you can authenticate user against SimpleSAMLphp itself

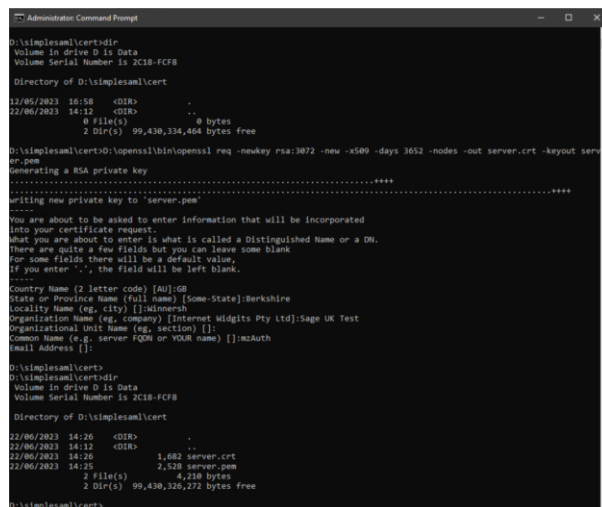
IMPORTANT NOTE: The configuration described in this document is not setup securely, as it should only ever be used for test instances. Even for test instances you may want to tighten up on the security settings once you have got it working OK.

Create SSL certificate

I need to create a self-signed certificate to use in Apache SSL configuration and is also defined in "saml20-idp-hosted.php" file. To do so, I need "openssl" available on any PC or server, but in this case will just install on to the server I am working on.

After installing openssl into “D:\openssl” directory, I then launch a CMD windows, navigate to directory “D:\cert” and run the following command to generate the private key and corresponding self-signed certificate:

```
D:\openssl\bin\openssl req -newkey rsa:3072 -new -x509 -days 3652 -nodes -out server.crt -keyout server.pem
```



```

Administration: Command Prompt
D:\simplesaml\cert>dir
Volume in drive D is Data
Volume Serial Number is 2C18-FCF8

Directory of D:\simplesaml\cert

12/05/2023 16:58 <DIR>          .
22/06/2023 14:12 <DIR>          ..
                0 file(s)          0 bytes
                2 DIR(s)    99,430,334,464 bytes free

D:\simplesaml\cert>D:\openssl\bin\openssl req -newkey rsa:3072 -new -x509 -days 3652 -nodes -out server.crt -keyout server.pem
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'server.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GB
State or Province Name (full name) [Some-State]:Berkshire
Locality Name (eg, city) []:Mimmsesh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Sage UK Test
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:mzAuth
Email address []:

D:\simplesaml\cert>
D:\simplesaml\cert>dir
Volume in drive D is Data
Volume Serial Number is 2C18-FCF8

Directory of D:\simplesaml\cert

22/06/2023 14:26 <DIR>          .
22/06/2023 14:12 <DIR>          ..
22/06/2023 14:26                1,682 server.crt
22/06/2023 14:26                2,528 server.pem
                2 file(s)          4,210 bytes
                2 DIR(s)    99,430,326,272 bytes free

D:\simplesaml\cert>

```

Install and configure Apache 2.4

Download Apache from your preferred location. I will go to <https://www.apachelounge.com/download/> and download the latest Win64 version, currently VS17.

Extract the “Apache24” directory from httpd-2.4.26-Dev-Win64-VC15.zip to your installation drive. I am installing everything onto the server D: so it will be located in “D:\Apache24”

As per the note at <https://www.apachelounge.com/download/>

*Be sure you installed latest 14.36.32532 Visual C++ Redistributable Visual Studio 2015-2022 :
vc_redist_x64 or vc_redist_x86 see Redistributable*

Edit D:\Apache24\conf\httpd.conf

Be careful about which port to use. Port 80 and 443 are free on my server, so will use these for now. NOTE: the latest versions of SAML2 insist on HTTPS protocol and didn’t work for me when I originally tried HTTP

As I am installing on D: I need to change all references to C: to now point to D:

```
Define SRVROOT "D:/Apache24"
```

Also make the following changes

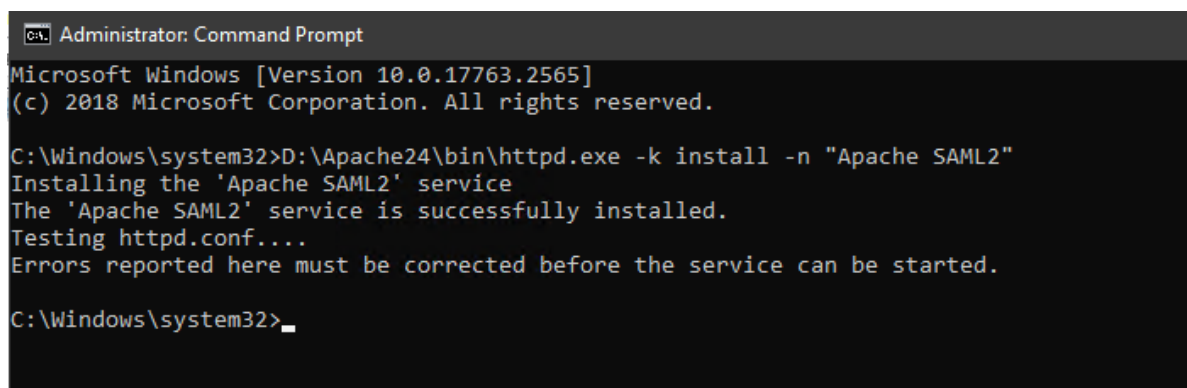
```
Listen 80
ServerName mzAuth
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule ssl_module modules/mod_ssl.so
Include conf/extra/httpd-ssl.conf
```

Edit D:\Apache24\conf\extra\httpd-ssl.conf and change the port being used to an appropriate, unused port. I will use port 443 for my HTTPS traffic. I will be lazy and use the same SSL certificate I will generate for both Apache and SimpleSAML

```
Listen 443
<VirtualHost _default_:443>
ServerName mzAuth
ErrorLog "${SRVROOT}/logs/SSLerror.log"
TransferLog "${SRVROOT}/logs/SSLaccess.log"
SSLCertificateFile "D:/cert/server.crt"
SSLCertificateKeyFile "D:/cert/server.pem"
```

Install as a service. Launch Command prompt window (CMD) using “Run as administrator” then run the following command. I am adding the “-n” flag as I want to use a specific service name:

```
D:\Apache24\bin\httpd.exe -k install -n "Apache SAML2"
```



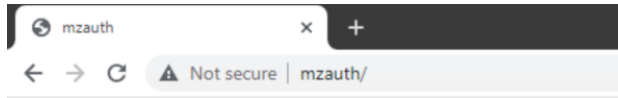
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2565]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>D:\Apache24\bin\httpd.exe -k install -n "Apache SAML2"
Installing the 'Apache SAML2' service
The 'Apache SAML2' service is successfully installed.
Testing httpd.conf...
Errors reported here must be corrected before the service can be started.

C:\Windows\system32>
```


Then start the service

Test you can access Apache on port 80 and 443



It works!

Install and configure PHP

Download PHP from your preferred location. I will go to <https://www.php.net/> which redirects us to <https://windows.php.net/download/> to download the latest Win64 version, currently PHP 8.2.7. **Make sure you download the "Thread Safe" version.** VS16 x64 Thread Safe (2023-Jun-07 11:01:22)

Extract "php-8.2.7-Win32-vs16-x64.zip" into "PHP" directory on your installation drive. I am installing everything onto D: so will extract to "D:\PHP"

Add "D:\PHP" to the system path

Control Panel, System, Advanced System Settings, Environment Variables

Follow the installation steps from the PHP online help at

<https://www.php.net/manual/en/install.windows.php>

Copy D:\PHP\php.ini-development to D:\PHP\php.ini

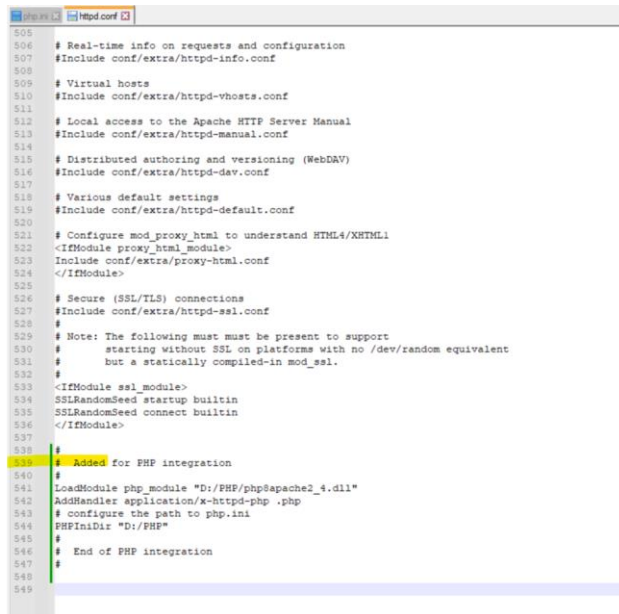
Modify the php.ini file as below:

```
error_log = "D:\PHP\log\php_errors.log"
extension_dir = "D:\PHP\ext"
extension=ldap
extension=curl
extension=mbstring
extension=openssl
extension=pdo_mysql
extension=pdo_odbc
extension=pdo_pgsql
extension=pdo_sqlite
```

```
913 ;extension=bz2
914 extension=curl
915 ;extension=ffi
916 ;extension=ftp
917 ;extension=fileinfo
918 ;extension=gd2
919 ;extension=gettext
920 ;extension=gmp
921 ;extension=intl
922 ;extension=imap
923 extension=ldap
924 extension=mbstring
925 ;extension=exif ; Must be after mbstring as it depends on it
926 ;extension=mysqli
927 ;extension=oci8_12c ; Use with Oracle Database 12c Instant Client
928 ;extension=odbc
929 extension=openssl
930 ;extension=pdo_firebird
931 extension=pdo_mysql
932 ;extension=pdo_oci
933 extension=pdo_odbc
934 extension=pdo_pgsql
935 extension=pdo_sqlite
936 ;extension=pgsql
937 ;extension=shmop
938
```

Setup httpd.conf to add the following section:

```
#
# Added for PHP integration
#
LoadModule php_module "D:/PHP/php8apache2_4.dll"
AddHandler application/x-httpd-php .php
# configure the path to php.ini
PHPIniDir "D:/PHP"
#
# End of PHP integration
#
```



```
505
506 # Real-time info on requests and configuration
507 #Include conf/extra/httpd-info.conf
508
509 # Virtual hosts
510 #Include conf/extra/httpd-vhosts.conf
511
512 # Local access to the Apache HTTP Server Manual
513 #Include conf/extra/httpd-manual.conf
514
515 # Distributed authoring and versioning (WebDAV)
516 #Include conf/extra/httpd-dav.conf
517
518 # Various default settings
519 #Include conf/extra/httpd-default.conf
520
521 # Configure mod_proxy_html to understand HTML4/XML
522 <IfModule proxy_html_module>
523 Include conf/extra/proxy-html.conf
524 </IfModule>
525
526 # Secure (SSL/TLS) connections
527 #Include conf/extra/httpd-ssl.conf
528 #
529 # Note: The following must be present to support
530 # starting without SSL on platforms with no /dev/random equivalent
531 # but a statically compiled-in mod_ssl.
532 #
533 <IfModule ssl_module>
534 SSLRandomSeed startup builtin
535 SSLRandomSeed connect builtin
536 </IfModule>
537
538
539 # Added for PHP integration
540 #
541 LoadModule php_module "D:/PHP/php8apache2_4.dll"
542 AddHandler application/x-httpd-php .php
543 # configure the path to php.ini
544 PHPIniDir "D:/PHP"
545 #
546 # End of PHP integration
547 #
548
549
```

Restart the Apache SAML service to make sure there are no errors.

Install and configure SimpleSAMLphp

Download the latest version of SimpleSAMLphp from <https://simplesamlphp.org/download/> (Currently 2.0.4 from

<https://github.com/simplesamlphp/simplesamlphp/releases/download/v2.0.4/simplesamlphp-2.0.4.tar.gz>)

Extract “simplesamlphp-2.0.4.tar.gz” to “simplesamlphp-2.0.4.tar”

Extract “simplesamlphp-2.0.4.tar” to D: ignoring the four “Cannot create symbolic link” messages.

In my case I end up with my installation in directory “D:\simplesamlphp-2.0.4” which I then rename to “D:\simplesaml”

Create the directory “D:/simplesaml/www/mzAuth”

Edit the Apache 2.4 httpd.conf file

- a. Modify the DocumentRoot parameter

```
DocumentRoot "D:/simplesaml/www/mzAuth"
```

Add the following section at the end

```
# Added for SimpleSAMLphp
SetEnv SIMPLESAMPLPHP_CONFIG_DIR /simplesaml/config
Alias /simplesaml /simplesaml/public
<Directory /simplesaml/public>
<IfModule mod_authz_core.c>
    Require all granted
</IfModule>
DirectoryIndex index.php
</Directory>
# End of SimpleSAMLphp configuration
```

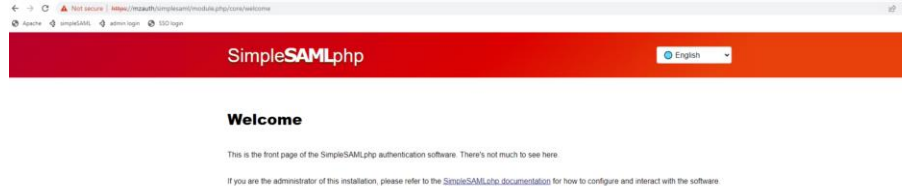
Create directories “D:\simplesaml\tmp” and “D:\simplesaml\log”

Copy D:\simplesaml\config\config.php.dist to D:\simplesaml\config\config.php

Edit D:\simplesaml\config\config.php file for the lines below:

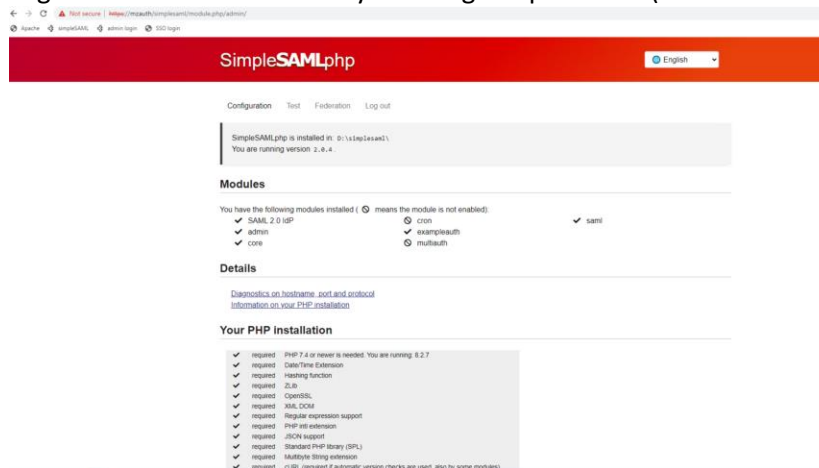
```
'certdir' => 'd:/cert',
'loggingdir' => 'log/',
'tempdir' => 'tmp/',
'technicalcontact_email' => 'admin@example.lan',
'timezone' => 'Europe/London',
'secretsalt' => 'gobbledygook123',
'auth.adminpassword' => 'Password1',
'trusted.url.domains' => ['https://mzAuth'],
'debug' => [
    'saml' => true,
'logging.level' => SimpleSAML\Logger::DEBUG,
'logging.handler' => 'file',
'session.cookie.secure' => true,
'language.cookie.secure' => true,
'production' => false,
```

Restart Apache SAML service, then test URL <https://mzAuth/simplesaml/>



Use the URL <https://mzAuth/simplesaml/admin>

Login as administrator user by entering the password (defined in the configuration as “Password1”)



Setup simplest Service Provider and Identity Provider

Setup Service Provider as described in "SimpleSAMLphp Service Provider QuickStart"

<https://simplesamlphp.org/docs/latest/simplesamlphp-sp.html>

Setup Identity Provider as described in "SimpleSAMLphp Identity Provider QuickStart"

<https://simplesamlphp.org/docs/latest/simplesamlphp-idp.html>

Edit config.php

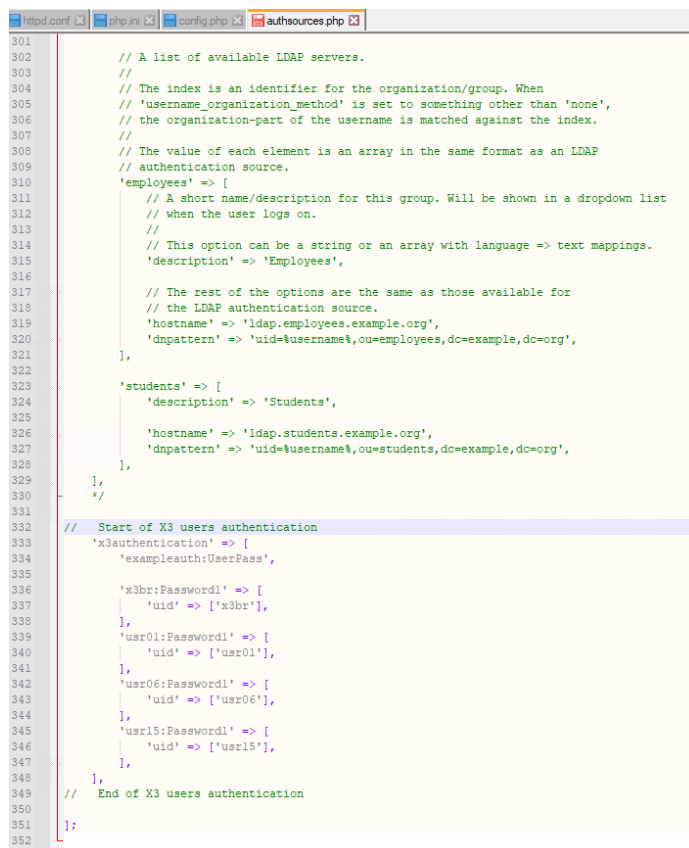
```
'enable.saml20-idp' => true,

'module.enable' => [
    'exampleauth' => true,
    'core' => true,
    'admin' => true,
    'saml' => true
],
```

You can configure SimpleSAMLphp to use a variety of different sources for the user data (user name, password and attributes needed to link to the X3 user data) For example you could use an LDAP server if you already have one available. For the purposes of this exercise, I will use the simplest possible option which is to store the user data in the file “authsources.php”.

Copy “D:\simplesaml\config\authsources.phpdist” to “D:\simplesaml\config\authsources.php”
 Edit “D:\simplesaml\config\authsources.php” add the following to the end of the file. This is suitable for SEED folder users:

```
// Start of X3 users authentication
'x3authentication' => [
    'exampleauth:UserPass',
    'x3br:Password1' => [
        'uid' => ['x3br'],
    ],
    'usr01:Password1' => [
        'uid' => ['usr01'],
    ],
    'usr06:Password1' => [
        'uid' => ['usr06'],
    ],
    'usr15:Password1' => [
        'uid' => ['usr15'],
    ],
],
// End of X3 users authentication
```



```
301 // A list of available LDAP servers.
302 //
303 // The index is an identifier for the organization/group. When
304 // 'username_organization_method' is set to something other than 'none',
305 // the organization-part of the username is matched against the index.
306 //
307 // The value of each element is an array in the same format as an LDAP
308 // authentication source.
309 'employees' => [
310     // A short name/description for this group. Will be shown in a dropdown list
311     // when the user logs on.
312     //
313     // This option can be a string or an array with language => text mappings.
314     'description' => 'Employees',
315     //
316     // The rest of the options are the same as those available for
317     // the LDAP authentication source.
318     'hostname' => 'ldap.employees.example.org',
319     'dnpattern' => 'uid=%username%,ou=employees,dc=example,dc=org',
320 ],
321
322 'students' => [
323     'description' => 'Students',
324     //
325     'hostname' => 'ldap.students.example.org',
326     'dnpattern' => 'uid=%username%,ou=students,dc=example,dc=org',
327 ],
328 ],
329 //
330 //
331
332 // Start of X3 users authentication
333 'x3authentication' => [
334     'exampleauth:UserPass',
335     //
336     'x3br:Password1' => [
337         'uid' => ['x3br'],
338     ],
339     'usr01:Password1' => [
340         'uid' => ['usr01'],
341     ],
342     'usr06:Password1' => [
343         'uid' => ['usr06'],
344     ],
345     'usr15:Password1' => [
346         'uid' => ['usr15'],
347     ],
348 ],
349 // End of X3 users authentication
350 ];
351
352
```

Copy “D:\simplesaml\metadata\saml20-idp-hosted.php.dist” to “D:\simplesaml\metadata\saml20-idp-hosted.php”
 Update file “D:\simplesaml\metadata\saml20-idp-hosted.php” to update the authentication source. I am overwriting the default example in the file for quickness.

```

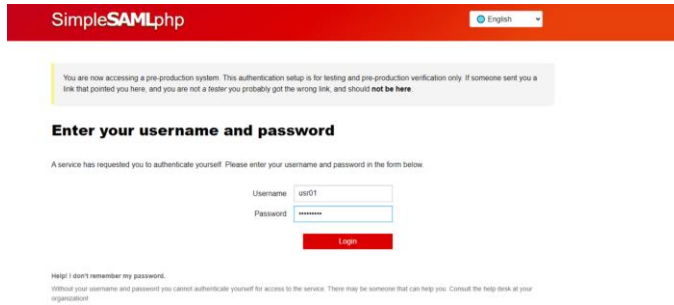
1  <?php
2
3  /**
4   * SAML 2.0 IdP configuration for SimpleSAMLphp.
5   *
6   * See: https://simplesamlphp.org/docs/stable/simplesamlphp-reference-idp-hosted
7   */
8
9  // $metadata['urn:x-simplesamlphp:example-idp'] = [
10 $metadata['https://mzauth/simplesaml'] = [
11     /*
12     * The hostname of the server (VHOST) that will use this SAML entity.
13     *
14     * Can be '__DEFAULT__', to use this entry by default.
15     */
16     'host' => '__DEFAULT__',
17
18     // X.509 key and certificate. Relative to the cert directory.
19     'privatekey' => 'server.pem',
20     'certificate' => 'server.crt',
21
22     /*
23     * Authentication source to use. Must be one that is configured in
24     * 'config/authsources.php'.
25     */
26     'auth' => 'x3authentication',
27
28     /* Uncomment the following to use the uri NameFormat on attributes. */
29     /*
30     'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri',
31     'authproc' => [
32         // Convert LDAP names to oids.
33         100 => ['class' => 'core:AttributeMap', 'name2oid'],
34     ],
35     */
36
37     /*
38     * Uncomment the following to specify the registration information in the
39     * exported metadata. Refer to:
40     * http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html
41     * for more information.
42     */
43     /*
44     'RegistrationInfo' => [
45         'authority' => 'urn:mace:example.org',
46         'instant' => '2008-01-17T11:28:03Z',
47         'policies' => [
48             'en' => 'http://example.org/policy',
49             'es' => 'http://example.org/politica',

```

Restart Apache SAML and test you can login using the above user/passwords when accessing “x3authentication” source



Enter any of the users and all passwords are “Password1” then click “Login”



SimpleSAMLphp English

You are now accessing a pre-production system. This authentication setup is for testing and pre-production verification only. If someone sent you a link that pointed you here, and you are not a tester you probably got the wrong link, and should **not be here**.

Enter your username and password

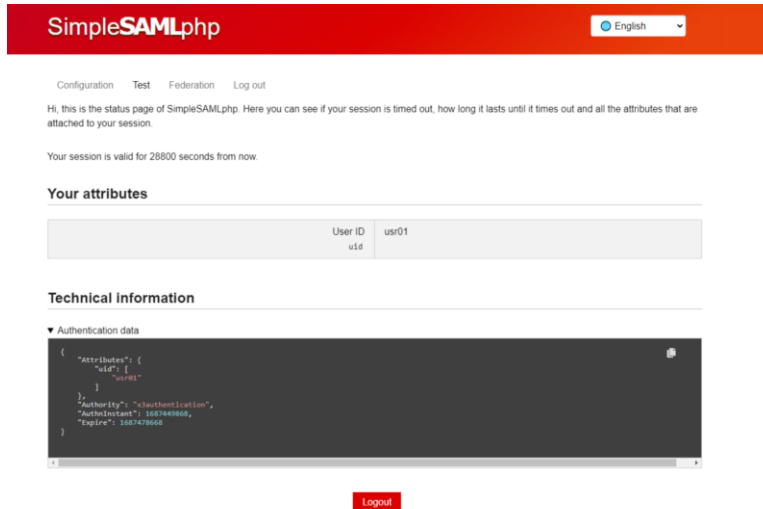
A service has requested you to authenticate yourself. Please enter your username and password in the form below.

Username:

Password:

Help! I don't remember my password.
Without your username and password you cannot authenticate yourself for access to the service. There may be someone that can help you. Consult the help desk at your organization.

We then see a screen which echoes the returned attributes.



SimpleSAMLphp English

[Configuration](#) [Test](#) [Federation](#) [Log out](#)

Hi, this is the status page of SimpleSAMLphp. Here you can see if your session is timed out, how long it lasts until it times out and all the attributes that are attached to your session.

Your session is valid for 28800 seconds from now.

Your attributes

User ID	usr01
uid	

Technical information

▼ Authentication data

```
{
  "Attributes": {
    "uid": [
      "usr01"
    ]
  },
  "Authority": "https://localhost",
  "AuthnContext": "urn:oasis:names:tc:SAML:1.1:profile:browser:authn",
  "Expire": 1687478668
}
```

Click the “Logout” link and you are then logged out of SAML2

Update firewall rules for “mzAuth”

Allow access to port 443

Configure Sage X3 to use SAML2 authentication

Login to Sage X3 using the external URL, i.e. the same as you will be using to login using SAML2

Navigate to Administration, Administration, Authentication, SAML2 id provider

Select “Create saml2”

Name: SAML2

Display Name: Login using SAML2

Authorize URL:

<https://mzauth/simplesaml/saml2/idp/SSOService.php>

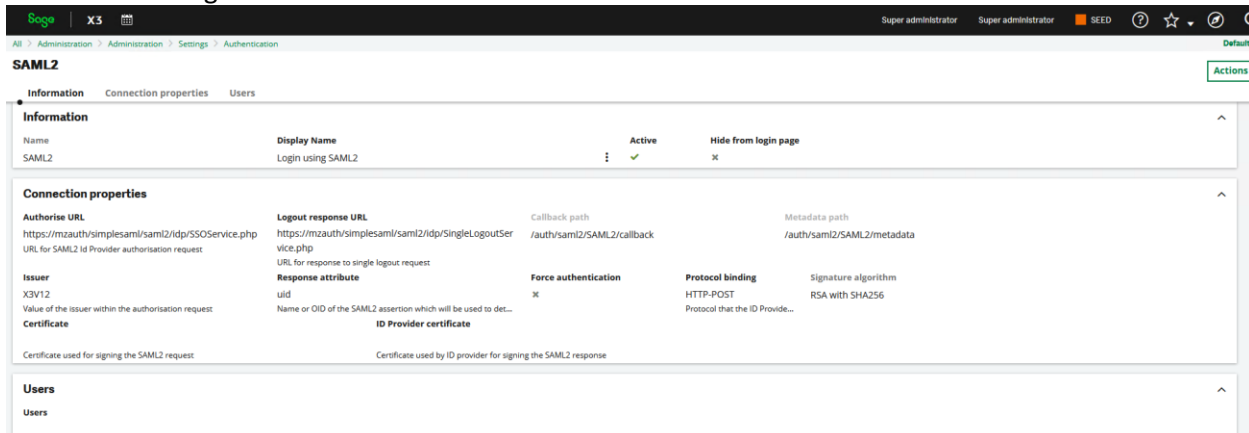
Logout response URL:

<https://mzauth/simplesaml/saml2/idp/SingleLogoutService.php>

Issuer: X3V12 (Any unique code)

Response attribute: uid (Default)

SAVE these changes



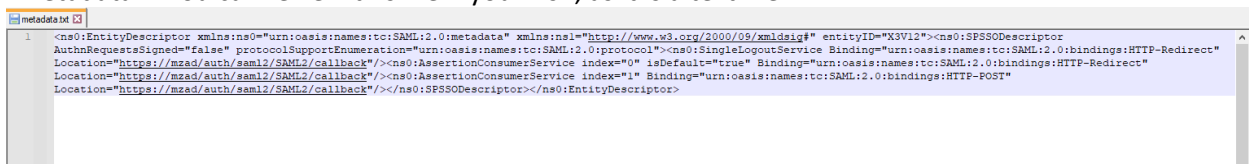
The screenshot shows the Sage X3 Administration interface for SAML2 configuration. The 'Information' tab is active, displaying the following details:

Name	Display Name	Active	Hide from login page
SAML2	Login using SAML2	✓	x

The 'Connection properties' tab is also visible, showing:

- Authorize URL:** <https://mzauth/simplesaml/saml2/idp/SSOService.php>
- Logout response URL:** <https://mzauth/simplesaml/saml2/idp/SingleLogoutService.php>
- Issuer:** X3V12
- Response attribute:** uid
- Force authentication:** x
- Protocol binding:** HTTP-POST
- Signature algorithm:** RSA with SHA256

Use the “Get metadata” button and save the generated file to disk. The filename defaults to “metadata” You can review this file if you wish, as it is a text file



```

1 <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
2 <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="X3V12">
3   <SPSSODescriptor AuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
4     <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
5       Location="https://mzad/auth/saml2/SAML2/callback"/>
6     <AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
7       Location="https://mzad/auth/saml2/SAML2/callback"/>
8     <AssertionConsumerService index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
9       Location="https://mzad/auth/saml2/SAML2/callback"/>
10   </SPSSODescriptor>
11 </EntityDescriptor>
  
```

Use the SimpleSAMLphp URL to convert the text to be added to “saml20-sp-remote” file.

<https://mzauth/simplesaml/module.php/admin/federation/metadata-converter>

Login using the “admin” password.

Use the “Browse” button to pick up the “metadata” file you saved

Click “Parse” button to generate the text you need

Metadata parser

XML metadata

```
<ns0:EntityDescriptor xmlns:ns0="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ns1="http://www.w3.org/2000/09/xmldsig#" entityID="X3V12"><ns0:SPSSODescriptor
AuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><ns0:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://mzad/auth/saml2/SAML2/callback"/><ns0:AssertionConsumerService index="0" isDefault="true"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://mzad/auth/saml2/SAML2/callback"/><ns0:AssertionConsumerService index="1"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://mzad/auth/saml2/SAML2/callback"/></ns0:SPSSODescriptor></ns0:EntityDescriptor>
```

Parse

Scroll down, then click the “Copy to clipboard” button to pick up the text in the “saml20-sp-remote” box

Parse

Converted metadata

```
saml20-sp-remote
$metadata['X3V12'] = [
    'entityid' => 'X3V12',
    'contacts' => [],
    'metadata-set' => 'saml20-sp-remote',
    'AssertionConsumerService' => [
        [
            'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
            'Location' => 'https://mzad/auth/saml2/SAML2/callback',
            'index' => 0,
            'isDefault' => true,
        ],
        [
            'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
            'Location' => 'https://mzad/auth/saml2/SAML2/callback',
            'index' => 1,
        ],
    ],
    'SingleLogoutService' => [
        [
            'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
            'Location' => 'https://mzad/auth/saml2/SAML2/callback',
        ],
    ],
    'validate.authnrequest' => false,
];
```

Copy “D:\simplesaml\metadata\saml20-sp-remote.php.dist” to “D:\simplesaml\metadata\saml20-sp-remote.php”

Add the generated text to the “D:\simplesaml\metadata\saml20-sp-remote.php” file. For ease of reading, I removed the examples included in the original file.

```

saml20-sp-remote.php
1 <?php
2
3 /**
4  * SAML 2.0 remote SP metadata for SimpleSAMLphp.
5  *
6  * See: https://simplesamlphp.org/docs/stable/simplesamlphp-reference-sp-remote
7  */
8
9 $metadata['X3V12'] = [
10     'entityid' => 'X3V12',
11     'contacts' => [],
12     'metadata-set' => 'saml20-sp-remote',
13     'AssertionConsumerService' => [
14         [
15             'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
16             'Location' => 'https://mzad/auth/saml2/SAML2/callback',
17             'index' => 0,
18             'isDefault' => true,
19         ],
20         [
21             'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
22             'Location' => 'https://mzad/auth/saml2/SAML2/callback',
23             'index' => 1,
24         ],
25     ],
26     'SingleLogoutService' => [
27         [
28             'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
29             'Location' => 'https://mzad/auth/saml2/SAML2/callback',
30         ],
31     ],
32     'validate.authnrequest' => false,
33 ];
34
35

```

Restart Apache SAML for the change to take effect

Edit Sage X3 nodelocal.js for SAML2 (MZWEB1, MZWEB2, MZWEB3)

Located in directory “D:\Sage\SafeX3\SyraSrv\syracuse\bin”

Modify the “auth” line to add “saml2”:

```

nodelocal.js
9
10 exports.config = {
11     port: 8134,
12     streamlineFromCI: true,
13     x3key: true,
14     collaboration: {
15         driver: "mongodb",
16         dataset: "syracuse",
17         hostname: "x3srv12ag1vm",
18         port: 2702,
19         logpath: "D:\\Sage\\SafeX3\\SyraSrv\\syracuse\\logs",
20         certdir: "D:\\Sage\\SafeX3\\SyraSrv\\syracuse\\certs",
21         cacheDir: "D:\\Sage\\SafeX3\\SyraSrv\\syracuse\\cache"
22     },
23     mongodb: {
24         options: {
25             w: 1,
26             ssl: true,
27             sslCA: require('fs').readFileSync("D:\\Sage\\SafeX3\\SyraSrv\\syracuse\\certs\\mongodb\\ca.cacert"),
28             sslValidate: true,
29             sslKey: require('fs').readFileSync("D:\\Sage\\SafeX3\\SyraSrv\\syracuse\\certs\\mongodb\\client.pem"),
30             sslCert: require('fs').readFileSync("D:\\Sage\\SafeX3\\SyraSrv\\syracuse\\certs\\mongodb\\client.pem")
31         }
32     },
33     session: {
34         timeout: 20, // minutes
35         checkInterval: 60, // seconds
36         auth: ["basic", "bearer", "saml2"],
37     },
38     searchEngine: {
39         hostname: "x3srv12ag1vm",
40         port: 9200,
41     },
42     x3fusion: {
43         records: {
44             "dumpPath": "D:\\Sage\\SafeX3\\SyraSrv\\syracuse\\cache\\_cvg_\\_USERNAME_"
45         }
46     },
47     etna: {

```

Re-start Syracuse service for the change to take effect

Setup X3 users for testing purposes

Create Syracuse users for x3br, usr01, usr06 and usr15.

Navigate to Administration, Administration, Users, Users

For each user, create “New”

Set Authentication to “SAML2.0” and select the “SAML2 id Provider”

The screenshot shows the Sage user administration interface. At the top, there are navigation tabs: Login, Information, Administration, Explorer, and Custom locales. The 'Login' tab is active. Below the tabs, there are three main sections: Login, Information, and Administration.

Login Section:

- Login:** A text input field containing 'x3br' and a checked 'Active' checkbox.
- Authentication:** Radio buttons for Standard, DB, LDAP, and SAML2.0 (selected).
- SAML2 Id Provider:** A dropdown menu with 'SAML2' selected and 'SAML2 id provider' listed below it.
- New signature code:** Two input fields labeled 'Password' and 'Confirm password'.
- LDAP instance for synchronization:** An input field with 'LDAP directory' listed below it.

Information Section:

- Title:** Radio buttons for Mr (selected) and Mrs.
- First name:** An empty text input field.
- Last name:** A text input field containing 'x3br'.
- Email:** An empty text input field.
- CTI ID:** An empty text input field.
- Photo:** A text input field with the placeholder text 'Drop file from explorer or Select it' and a 'Select file' button.

Administration Section:

- Groups:** A search bar containing 'Super administrators' and a search icon.
- Endpoints login:** A text input field.

Test the user by going to the X3 login page and selecting “Login using SAML2”

The screenshot shows the Sage X3 login page. At the top, there is the Sage logo. Below it, the text 'Sage X3' is displayed. The page contains a login form with the following elements:

- Login:** A text input field with a yellow border.
- Password:** A text input field.
- Remember me on this device:** A checkbox that is currently unchecked.
- Sign in:** A green button.
- External Accounts:** A section with a green button labeled 'Login using SAML2'.

Login using the users you configured, for example “x3br” with password “Password1”

You are now accessing a pre-production system. This authentication setup is for testing and pre-production verification only. If someone sent you a link that pointed you here, and you are not a tester you probably got the wrong link, and should **not be here**

Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below.

Username

Password

Help! I don't remember my password.

Without your username and password you cannot authenticate yourself for access to the service. There may be someone that can help you. Consult the help desk at your organization.

If you type in the correct username/password and all is working OK, you will be redirected to the X3 homepage.

The screenshot shows the Sage X3 A/R accounting manager interface. The main content area is divided into two sections: 'CUSTOMERS EXCEEDING CREDIT LEV' and 'LATE CUSTOMER OPEN ITEMS'. The left sidebar contains a navigation menu with roles like Workshop manager, Planning manager, Executive, Product design, System administrator, Buyer, Design/methods manager, Stock manager, Planning manager, Material buyer, and Warehouse manager.

Company	Customer	Company Name	Authorized Credit	Global Credit	Delivery Credit	Shipped n
AE1Q	AE001	Al Rostamani Communications	0	23 863.37	-0.01	
AE1Q	AE002	Al Zahra Computers	0	716 625.00	0	
AE1Q	AE003	Cosmos Computer Co LLC	0	70 996.38	0	
AO2Q	AO006	Distribuidora do Cavito	0	1 494 350.00	0	
AU1Q	AU003	JB Lee	0	1 110.00	0	
AU1Q	AU003	JB Lee	0	33 903.66	731.10	
BE2Q	BE001	BE Concept	0	2 323.40	0	
BH1Q	BH001	Global Computers And Electronics	0	4 541.26	0.02	
DE1Q	DE001	1 2 3 Rad GmbH	0	467 607.22	204.68	
DE1Q	DE002	Bike & Outdoor Company GmbH	0	129 983.95	-0.00	

Pay-by BP	Company Name	Due date	Balance	Accounting currency	Site	Journal number
AE001	Al Rostamani Communications	27/02/2022	131.88	AED	AE011	SIN1901AE0110
AE001	Al Rostamani Communications	02/03/2022	1 050.00	AED	AE011	SIN1901AE0110
AE001	Al Rostamani Communications	13/03/2022	204.23	AED	AE011	SIN1902AE0110
AE001	Al Rostamani Communications	19/07/2022	118.19	SAR	SA011	SA0111906INVB
AE002	Al Zahra Computers	28/01/2022	10 000.00	AED	AE011	SIN1901AE0110
AE002	Al Zahra Computers	29/01/2022	18 375.00	AED	AE011	SIN1901AE0110
AE002	Cosmos Computer Co LLC	29/01/2022	65.94	AED	AE011	SIN1901AE0110
AE002	Cosmos Computer Co LLC	31/01/2022	2 000.00	AED	AE011	SIN1901AE0110
AO001	Luanda BTT.	03/08/2022	-400.00	EUR	PT031	PT0311708-REC
AO001	Luanda BTT.	31/01/2023	10 715 375.00	ADA	AO012	ECL-AO0121306

Logout behavior from X3 / SAML

The “Log out” link from X3 takes you back to the X3 homepage but does not release the SAML session. This means you are not asked to login again, until you close the browser or explicitly logout from SAML.

You can change this behavior by enabling the “Force Authentication” flag on the Sage X3 SAML server setup. If this flag is checked then:

- a. When you logout from X3, you will need to provide the SAML credentials again if you go back into X3
- b. If you have an existing SAML session (from some other software) then this will be ignored, and you will need to login to SAML again when accessing X3. (This overwrites the existing SAML session)

NOTE: any time you change something on the SAML2 server setup, remember to re-export the metadata and update the “saml20-sp-remote.php” file on the SAML server itself.

Additional Sage X3/SAML2 configuration to provide best practice/security

What we have done so far may be all you need to do for your own internal testing. However, in practice most systems will need to be more secure. For example, you could implement certificate signing for the requests and/or responses. The following steps describe how to setup this additional security.

Enable certificate signing from SAML server (responses)

SAML is already configured to sign responses, but X3 is currently ignoring them. We can configure X3 to validate the signatures, which provides validation as to the authenticity of the SAML server

What I need to do in order to be able to recognize the signatory is to load the server certificate being used by the SAML2 server as a certificate to X3 using Administration, Administration, Certificates, Certificates. I only need to load the Server certificate (no private key is needed) This may seem a little confusing in this case, as my SAML2 server is on the same host as the X3 installation, but essentially I just need to load the "server.crt" file from directory "D:\cert"

The screenshot shows the Sage X3 Administration interface for the 'Certificate' configuration of 'saml2server'. The 'Information' tab is active, displaying a table with the following data:

Name	Description	Internal	Certificate	Valid from	Valid until
saml2server	SAML2 server	X		22/06/2023 14:26	21/06/2033 14:26

Below the table, the 'Private key' section shows 'Private key exists' as 'X'. The 'Context' section lists 'CA Certificates' and 'Server'.

Now navigate to Administration, Administration, Authentication, SAML2 id provider

Set the "ID provider certificate" as "saml_server_cert"

The screenshot shows the Sage X3 Administration interface for the 'SAML2' configuration. The 'Information' tab is active, displaying the following configuration:

- Name:** SAML2
- Display Name:** Login using SAML2
- Active:**
- Hide from login page:**

Connection properties:

- Authorise URL:** https://mzauth/simplesaml/saml2/rdp/SSOService.php
- Logout response URL:** https://mzauth/simplesaml/saml2/rdp/SingleLogoutService
- Callback path:** /auth/saml2/SAML2/callback
- Metadata path:** /auth/saml2/SAML2/metadata
- Issuer:** X3V12
- Response attribute:** uid
- Force authentication:**
- Protocol binding:** HTTP-POST, HTTP-Redirect
- Signature algorithm:** RSA with SHA256, RSA with SHA1

Certificate: The 'ID Provider certificate' is set to 'saml2server'.

Enable certificate signing to SAML server (requests)

The next step we can do if needed is setup request signing, which sets up validation of the X3 server from the SAML server perspective. For this, we need a server certificate for the X3 server itself.

Troubleshooting

Syracuse logging can be updated to allow “login.saml2” messages to be written out to the Syracuse “N”.log files.

All > Administration > Administration > Settings

Settings

General settings Authentication Proxy Mailer CTI Service License Log

⊖ Collapse all

Code	Description	Level
session	session	Info
login		
accessRights		Error
authentication		Error
saml2	SAML2 authentication	Debug
sitemap		Error
user		Error
memory	Memory usage information	Error

On the SAML server check the log files for interesting messages

- Apache log files located in D:\Apache24\logs (sslerror.log, SSLaccess.log and ssl_request.log)
- PHP log. D:\PHP\log\php_errors.log
- SimpleSAML log. D:\simplesaml\log\simplesamlphp.log

Issues you may encounter

Most issues will probably happen when clicking the “Login using SAML2” button and are likely to be configuration issues

Error: **Cannot convert object to primitive value**

This error is seen when DEBUG level logging is enabled for SAML2. Select “Info” level if you need to diagnose SAML2 until this issue is resolved.

Error: **Missing passphrase**

Error in the passphrase used for certificate being used for the x3 signing (x3_signing_cert) Re-edit this certificate and resave the passphrase

Error: **Missing cookie**

When using Edge or Chrome browsers, when accessing the SimpleSAMLphp login page you see an error “Missing cookie. You appear to have disabled cookies in your browser” Firefox browser works OK This is due to not setting “`session.cookie.secure' => true`” as described in the SSL configuration notes above.

Conclusion

This build diary has described the steps to setup a server as a **TEST** SAML2 service provider, which you can then use to configure Sage X3 to authenticate against. I am using X3 version 2023 R1, but the steps would be similar for other Sage X3 versions.