

Test system Build Diary

2022 R1 (V12 patch 29) install SAML2 service provider and 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
2022 R1 – install SAML2 service and configure X3 for SAML2 build diary	4
Objective	4
Documentation to use for planning and execution of this task	5
Install SimpleSAMLphp as a Windows service	6
Configure Sage X3 to use SAML2 authentication	18
Edit Sage X3 nodelocal.js for SAML2.....	20
Logout behavior from X3 / SAML.....	23
Additional Sage X3/SAML2 configuration to provide best practice/security	24
Troubleshooting.....	29
Conclusion.....	30

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 2022 R1, but the steps would be similar for other Sage X3 versions.

2022 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 a test server running Sage X3 2022 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.

Starting architecture and notes

Windows Server 2019 servers (Server name X3ERP12SQLVM)

Software already loaded:

Windows Server 2019

OpenJDK 1.8.0_282

Edge, Firefox and Chrome browsers

7-Zip 19.00

SQL Server 2019

All components of Sage X3 2022 R1

Windows users setup (Local users)

“x3admin” for installation and management

“X3run” for service runtime

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

<http://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

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 VS16.

Extract the “Apache24” directory from httpd-2.4.26-Dev-Win64-VC15.zip to your installation drive. I am installing everything onto D:\

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

*Be sure you installed latest 14.31.31103.0 Visual C++ Redistributable Visual Studio 2015-2022 :
vc_redist_x64 or vc_redist_x86 see Redistributable*

In my case this is already installed so do not need to take any action

Edit D:\Apache24\conf\httpd.conf

As I already have Apache running for X3 on this server, I need to be careful about which port I select. Port 8888 is free on my server.

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

Also make the following changes

```
Listen 8888
ServerName X3ERPv12SQLVM
```

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 already have an existing Apache service so need to use a different 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.

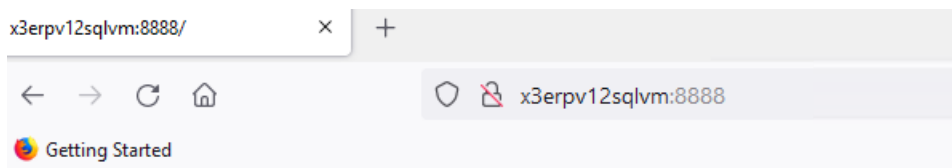
C:\Windows\system32>D:\Apache24\bin\httpd.exe -k install -n "Apache SAML2"
Installing the 'Apache SAML2' service
The 'Apache SAML2' service is successfully installed.
Testing httpd.conf....
Errors reported here must be corrected before the service can be started.

C:\Windows\system32>
```

Then start the service

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

Test you can access Apache on port 8888



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 7.4 Win64 version, currently PHP 7.4.28 "VC15 x64 Thread Safe (2022-Feb-24 17:53:21)". Make sure you download the "Thread Safe" version
NOTE: I did try PHP 8.1.4 but had lots of errors when trying to launch SimpleSAMLphp

Extract "php-7.4.28-Win32-vc15-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:

```
extension_dir = "ext"  
error_log = php_errors.log
```

```
;extension=bz2  
extension=curl  
;extension=ffi  
;extension=ftp  
;extension=fileinfo  
;extension=gd  
;extension=gettext  
;extension=gmp  
;extension=intl  
;extension=imap  
extension=ldap  
extension=mbstring  
;extension=exif ; Must be after mbstring as it depends on it  
;extension=mysqli  
;extension=oci8_12c ; Use with Oracle Database 12c Instant Client  
;extension=oci8_19 ; Use with Oracle Database 19 Instant Client  
;extension=odbc  
extension=openssl  
;extension=pdo_firebird  
extension=pdo_mysql  
;extension=pdo_oci  
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

```

Setup httpd.conf to add the following section:

```

#
#  Added for PHP integration
#
LoadModule php7_module "D:/php/php7apache2_4.dll"
AddHandler application/x-httpd-php .php
# configure the path to php.ini
PHPIniDir "D:/php"
#
#  End of PHP integration
#

```

```

496
497 # Fancy directory listings
498 #Include conf/extra/httpd-autoindex.conf
499
500 # Language settings
501 #Include conf/extra/httpd-languages.conf
502
503 # User home directories
504 #Include conf/extra/httpd-userdir.conf
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/XHTML1
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 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 php7_module "D:/php/php7apache2_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 #

```

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 1.19.5 from

<https://github.com/simplesamlphp/simplesamlphp/releases/download/v1.19.5/simplesamlphp-1.19.5.tar.gz>)

Extract “simplesamlphp-1.19.5.tar.gz” to “simplesamlphp-1.19.5.tar”

Extract “simplesamlphp-1.19.5.tar” to D:, ignoring the four “*Cannot create symbolic link*” messages

In my case I end up with my installation in directory “D:\simplesamlphp-1.19.5” which I then rename to “D:\simplesaml”

Edit the Apache 2.4 httpd.conf file

- Modify the DocumentRoot parameter and create the directory
“D:/simplesaml/www/X3ERPv12SQLVM”

```
DocumentRoot "D:/simplesaml/www/X3ERPv12SQLVM"
```

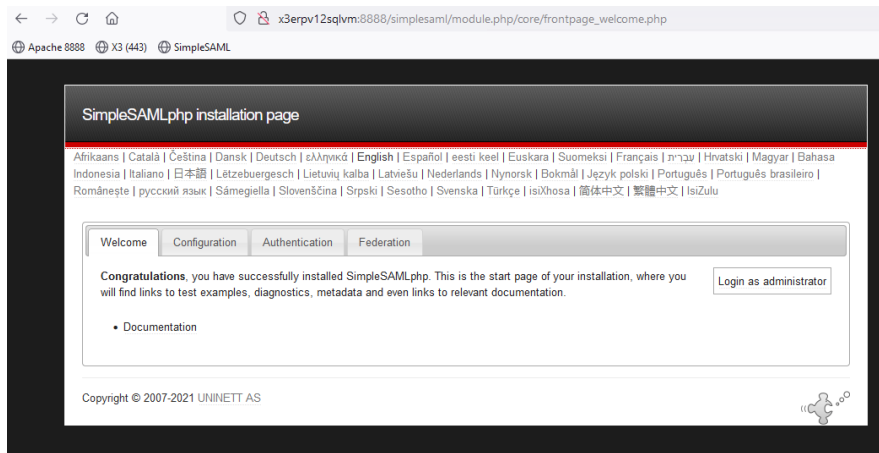
Add the following section at the end

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

Edit D:\simplesaml-1.19.5\config\config.php file for the lines below:

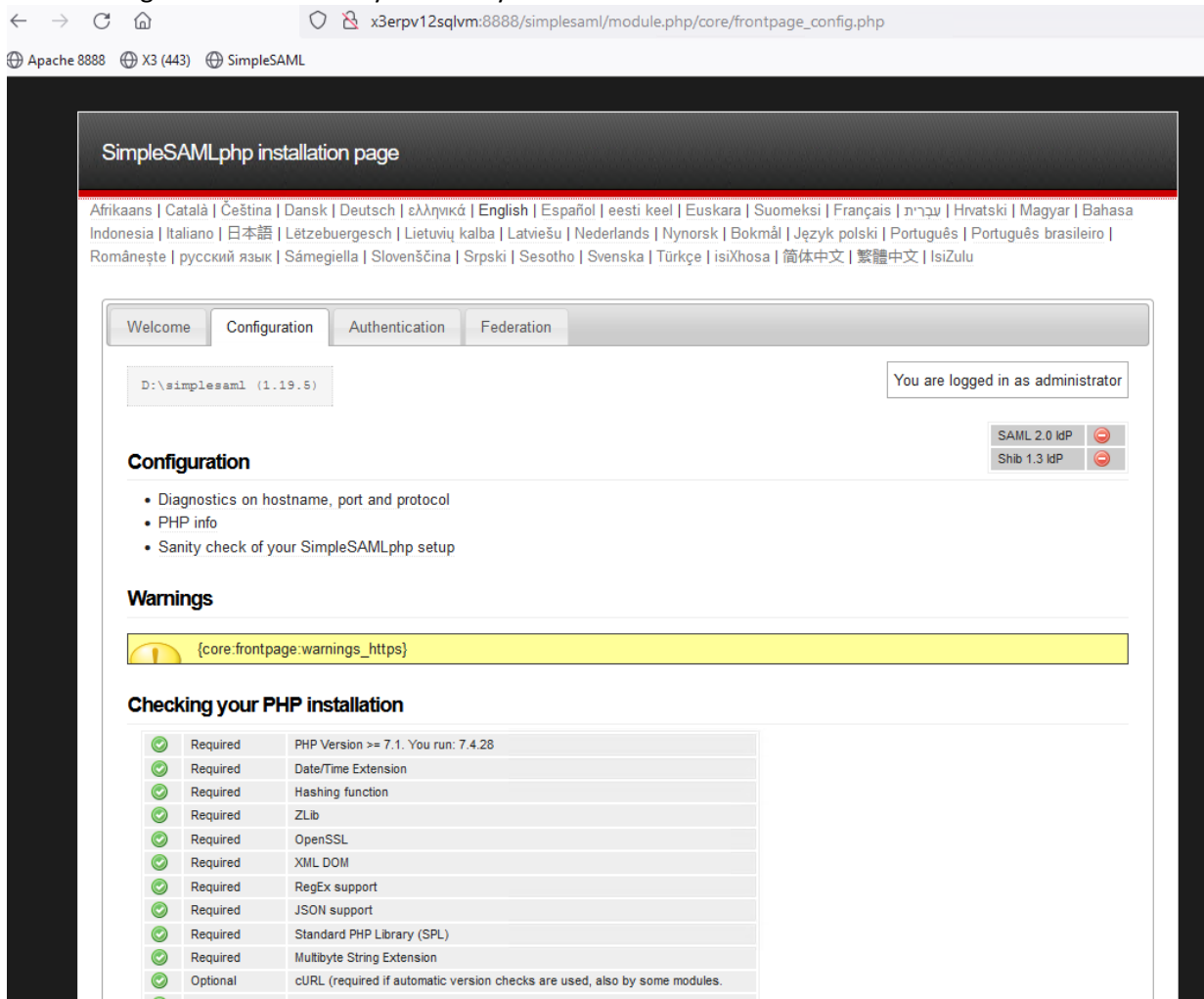
```
'technicalcontact_email' => 'admin@example.com',
'timezone' => 'Europe/London',
'secretsalt' => 'gobbledygook123',
'auth.adminpassword' => 'Password1',
'trusted.url.domains' => ['http://x3erpv12sqlvm:8888'],
'debug' => array(
    'saml' => true,
'logging.level' => SimpleSAML\Logger::DEBUG,
'logging.handler' => 'file',
'session.cookie.secure' => false,
```

Restart Apache SAML service, then test URL <http://X3ERPv12SQLVM:8888/simplesaml/>



Login as administrator (password defined as “Password1”)

Click “Configuration” tab and try the Sanity check



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

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

'enable.saml20-idp' => 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".

Edit "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
```

```

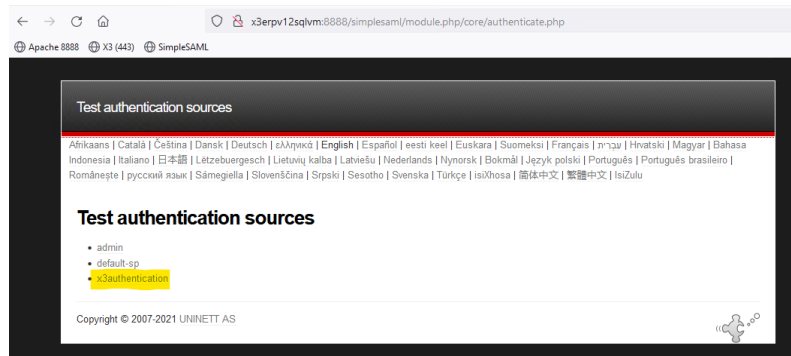
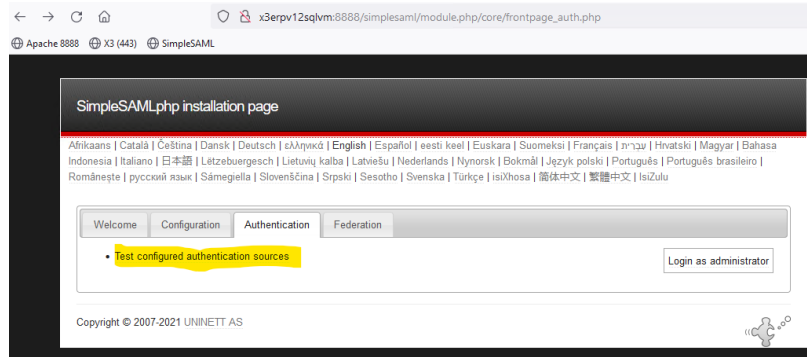
301
302 // A list of available LDAP servers.
303 //
304 // The index is an identifier for the organization/group. When
305 // 'username_organization_method' is set to something other than 'none',
306 // the organization-part of the username is matched against the index.
307 //
308 // The value of each element is an array in the same format as an LDAP
309 // authentication source.
310 'employees' => [
311     // A short name/description for this group. Will be shown in a dropdown list
312     // when the user logs on.
313     //
314     // This option can be a string or an array with language => text mappings.
315     'description' => 'Employees',
316
317     // The rest of the options are the same as those available for
318     // the LDAP authentication source.
319     'hostname' => 'ldap.employees.example.org',
320     'dnpattern' => 'uid=%username%,ou=employees,dc=example,dc=org',
321 ],
322
323 'students' => [
324     'description' => 'Students',
325
326     'hostname' => 'ldap.students.example.org',
327     'dnpattern' => 'uid=%username%,ou=students,dc=example,dc=org',
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

```

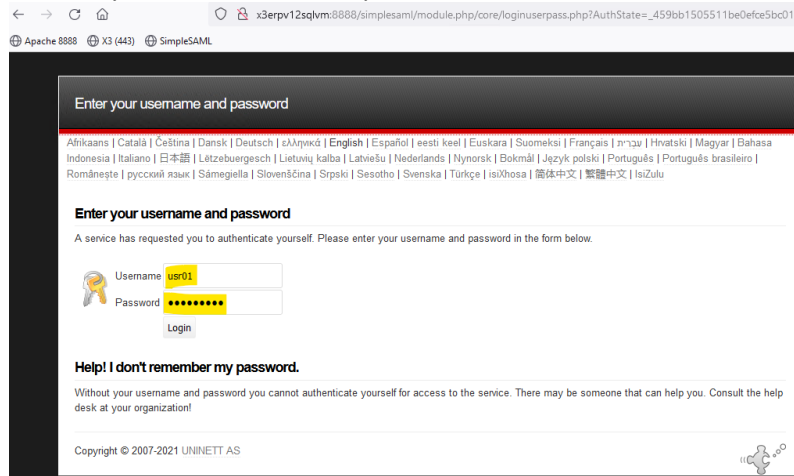
Update file “D:\simplesaml\metadata\saml20-idp-hosted.php” to update the authentication source

```

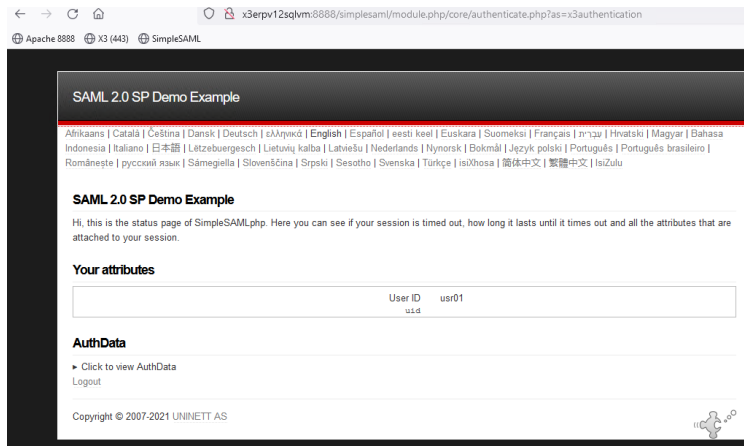
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
```



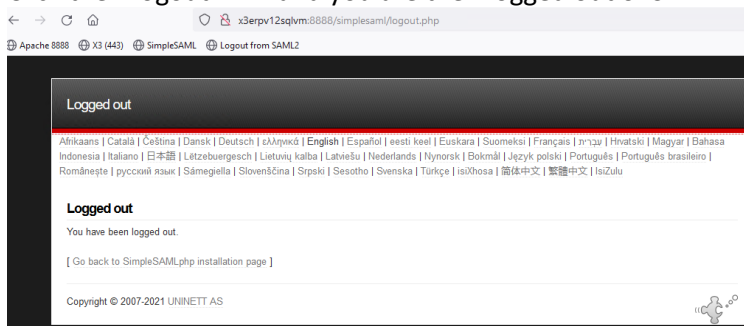
Enter any of the users and all passwords are “Password1” then click “Login”



We then see a screen which echoes the returned attributes.



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

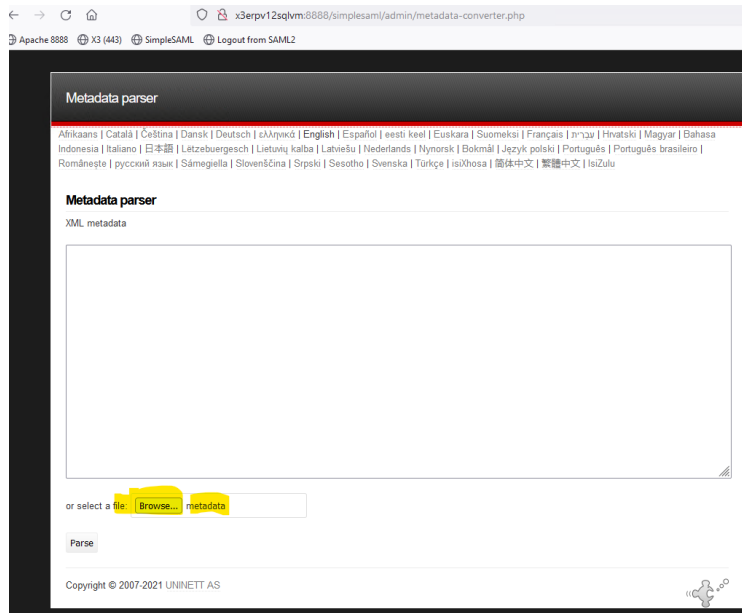


I need to create a self-signed certificate as defined in "saml20-idp-hosted.php" file. To do so, I need "openssl" available on any PC or server, but in this case will just install on to the server I am working on.

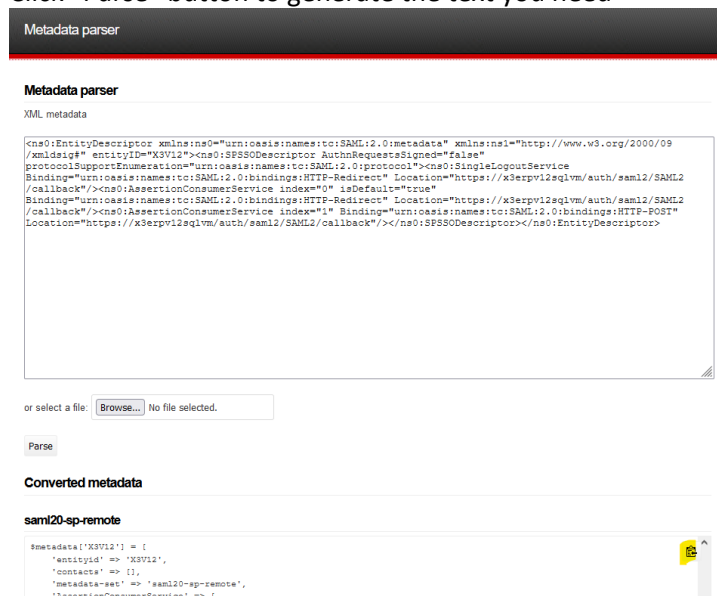
After installing openssl into “c:\openssl” directory, I then launch a CMD windows, navigate to directory “D:\simplesaml\cert” and run the following command to generate the private key and corresponding self-signed certificate:

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


[illegible]



Click “Parse” button to generate the text you need



Click the “Copy to clipboard” button to pick up the text in the “saml20-sp-remote” box and add this text to the “saml20-sp-remote” file located in “D:\simplesaml\metadata”

```

26  */
27  */
28  metadata['google.com'] = [
29    'AssertionConsumerService' => 'https://www.google.com/a/s.feide.no/acs',
30    'NameIDFormat' => 'urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress',
31    'simpleSaml.nameidattribute' => 'uid',
32    'simpleSaml.attributes' => false,
33  ];
34  */
35  */
36  */
37  metadata['https://legacy.example.edu'] = [
38    'AssertionConsumerService' => 'https://legacy.example.edu/saml/acs',
39    'Currently, SimpleSamlPhp defaults to the SHA-256 hashing algorithm.',
40    ' * Uncomment the following option to use SHA-1 for signatures directed
41    ' * at this specific service provider if it does not support SHA-256 yet.
42    ' *
43    ' * WARNING: SHA-1 is disallowed starting January the 1st, 2014.
44    ' * Please refer to the following document for more information:
45    ' * https://csrc.nist.gov/publications/nistpubs/800-131a/sp800-131a.pdf
46    ' * //signature.algorithm' => 'http://www.w3.org/2000/09/xmldsig#rsa-sha1',
47  ];
48  */
49  */
50  metadata['XSPV12'] = [
51    'entityid' => 'XSPV12',
52    'contacts' => [],
53    'metadata-set' => 'saml20-sp-remote',
54    'AssertionConsumerService' => [
55      [
56        'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
57        'Location' => 'https://x3srv12agvlvm/auth/saml2/SAMF2/callback',
58        'index' => 0,
59        'isDefault' => true,
60      ],
61    ],
62    [
63      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
64      'Location' => 'https://x3srv12agvlvm/auth/saml2/SAMF2/callback',
65      'index' => 1,
66    ],
67    'SingleLogoutService' => [
68      [
69        'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
70        'Location' => 'https://x3srv12agvlvm/auth/saml2/SAMF2/callback',
71      ],
72    ],
73    'validate.authrequest' => false,
74  ];
75  */
76  */
77  */

```

Restart Apache SAML for the change to take effect

Edit Sage X3 nodelocal.js for SAML2

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

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

```

9
10 exports.config = {
11   port: 8124,
12   streamlineFromCI: true,
13   x3key: true,
14   collaboration: {
15     driver: "mongodb",
16     dataset: "syracuse",
17     hostname: "x3srv12agvlvm",
18     port: 27017,
19     logpath: "D:\\Sage\\SafeX3\\SyrsaSrv\\syracuse\\logs",
20     certdir: "D:\\Sage\\SafeX3\\SyrsaSrv\\syracuse\\certs",
21     cacheDir: "D:\\Sage\\SafeX3\\SyrsaSrv\\syracuse\\cache"
22   },
23   mongodb: {
24     options: {
25       w: 1,
26       ssl: true,
27       sslCA: require('fs').readFileSync("D:\\Sage\\SafeX3\\SyrsaSrv\\syracuse\\certs\\mongodb\\ca.cacrt"),
28       sslValidate: true,
29       sslKey: require('fs').readFileSync("D:\\Sage\\SafeX3\\SyrsaSrv\\syracuse\\certs\\mongodb\\client.pem"),
30       sslCert: require('fs').readFileSync("D:\\Sage\\SafeX3\\SyrsaSrv\\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: "x3srv12agvlvm",
40     port: 9200,
41   },
42   x3fusion: {
43     records: {
44       "dumpPath": "D:\\Sage\\SafeX3\\SyrsaSrv\\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 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”

Admin > Administration > Administration > Users

[Login](#)
[Information](#)
[Administration](#)
[Explorer](#)
[Custom locales](#)

Login

Login *
☒ Active

Authentication:

☐ Standard

☐ DB

☐ LDAP

☒ SAML2.0

SAML2 Id Provider *

SAML2 id provider

New signature code:

LDAP instance for synchronization:

LDAP directory

Information

Title: ☒ Mr ☐ Mrs

 First name:
 Last name *:
 Email:
 CTI ID:
 Photo:

Administration

Groups


Super administrators

Endpoints login

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

[←](#)
[→](#)
[↺](#)
[🏠](#)
[🔒](#)
[https://x3erpv12sqlvm/auth/login/page](#)


X3 (443) SimpleSAML Logout from SAML2



Sage X3

☐ Remember me on this computer

External Accounts




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


Enter your username and password

Afrikaans | Català | Čeština | Dansk | Deutsch | ελληνικά | English | Español | eesti keel | Euskara | Suomi | Français | עברית | Hrvatski | Magyar | Bahasa Indonesia | Italiano | 日本語 | Letzebuergesch | Lietuvių kalba | Latviešu | Nederlands | Nynorsk | Bokmål | Język polski | Português | Português brasileiro | Românește | русский язык | Sámeigiella | Slovenščina | Srpski | Sesotho | Svenska | Türkçe | isiXhosa | 简体中文 | 繁體中文 | IsiZulu

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

Login

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 all is working OK, you will be redirected to the X3 homepage

Warehouse manager

KEY INFORMATION BUSINESS PROCESS

ORD. LINES TO DELIVER CALENDAR

1401 Records Page size: 10 = 1 2 3 4 5 6 ... 141 ☰ ⚙️

Planned deliv date	Expression	Line	Product	Description 1	Ordered Qty	Line Status
☺	SOCA00110002	1	D0002	Standard keyboard	250	Live
☺	SOCA00110001	1	D0002	Standard keyboard	200	Live
☺	SOCA00110001	1	D0002	Standard keyboard	200	Live
☺	SOCA00110001	1	D0002	Standard keyboard	300	Live
☺	SOCA00110001	1	D0002	Standard keyboard	400	Live
☺	SOCA00110001	2	D0002	Confless standard keyboard	300	Live
☺	SOCA00110001	2	D0002	Confless standard keyboard	200	Live
☺	SOCA00110001	2	D0002	Confless standard keyboard	200	Live
☺	SOCA00110001	2	D0002	Confless standard keyboard	200	Live

ORDERS LINES TO RECEIVE CALENDAR

1132 Records Page size: 10 = 1 2 3 4 5 6 ... 114 ☰ ⚙️

Planned receipt date	Expression	Line	Product	Description 1	Ordered qty
☺	01/01/2020	PQ0801100001	1 000	A53001 Server	3
☺	01/01/2020	PQ0801100001	2 000	BMS062 Dell Xps 17 inch Laptop	12
☺	10/01/2020	PQ0801100001	1 000	BMS013 20" radius rim - Road	100
☺	10/01/2020	PQ0801100001	2 000	BMS032 Children's bicycle crank-Road	50
☺	10/01/2020	PQ0801100001	3 000	BMS038 25" yne - Mountain	24
☺	10/01/2020	PQ0801100001	4 000	BMS056 Adult comfort saddle	36
☺	16/01/2020	PQ080210013	1 000	SAB021 Pisco Beams	1 000
☺	16/01/2020	PQ080210013	1 000	SAB029 50kg Lumbo BD, 12 PK Carton	400
☺	16/01/2020	PQ080210013	2 000	SAB020 70kg Lumbo BD, 8 PK Carton	400
☺	16/01/2020	PQ080210013	2 000	SAB030 Beams	750

STOCK CONTROLLER INDICATORS

Warehouse manager Indicators

- Stock lines with status Product
- Shortage orders planned delivery date
- NO in shortageWO start date

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 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, firstly by implementing HTTPS for the SAML2 server but also perhaps needing to implement certificate signing for the requests and/or responses. The following steps describe how to setup this additional security.

Setup Apache to enable SSL

Edit the D:\Apache24\conf\httpd.conf and uncomment the following lines

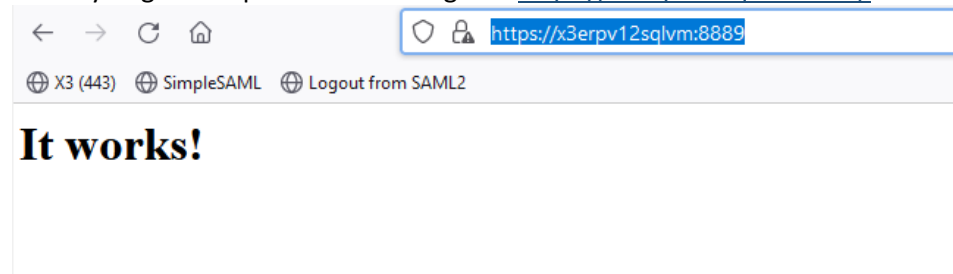
```
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule ssl_module modules/mod_ssl.so
Include conf/extra/httpd-ssl.conf
```

Edit D:\Apache24\conf\extra\httpd-ssl.conf and change the port being used to an appropriate, unused port. I will use port 8889 for my HTTPS traffic as the default port 443 is already in use. I am also going to be **very** lazy and re-use the same SSL certificate I already generated for use with SimpleSAML

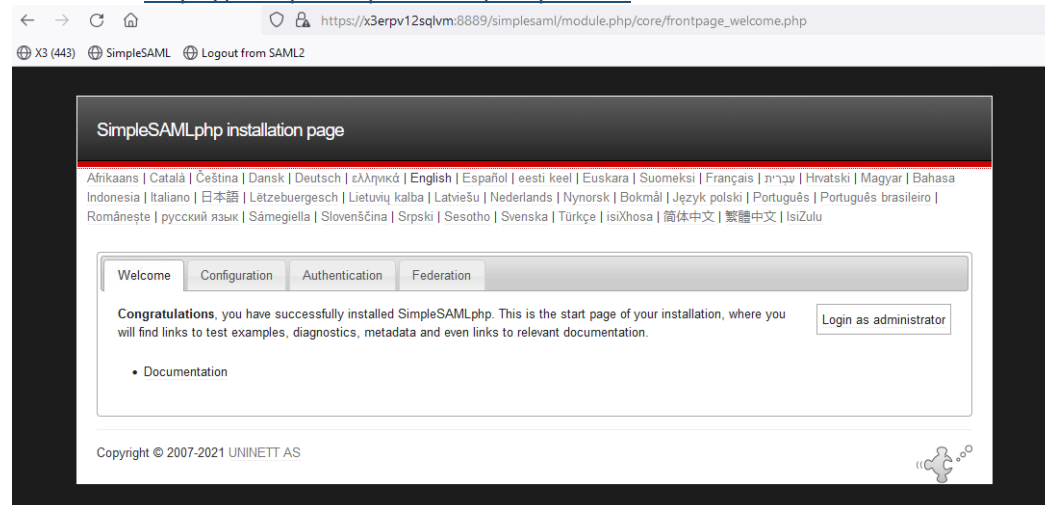
```
Listen 8889
<VirtualHost _default_:8889>
ServerName X3ERPv12SQLVM
SSLCertificateFile "D:/simplesaml/cert/server.crt"
SSLCertificateKeyFile "D:/simplesaml/cert/server.pem"
```

Re-start Apache service

Check you get a response when using URL <https://x3erpv12sqlvm:8889/>



Also check <https://x3erpv12sqlvm:8889/simplesaml> still works OK



Change config.php

```
'trusted.url.domains' => ['https://X3ERPv12SQLVM:8889'],
'session.cookie.secure' => true,
```

Login to X3

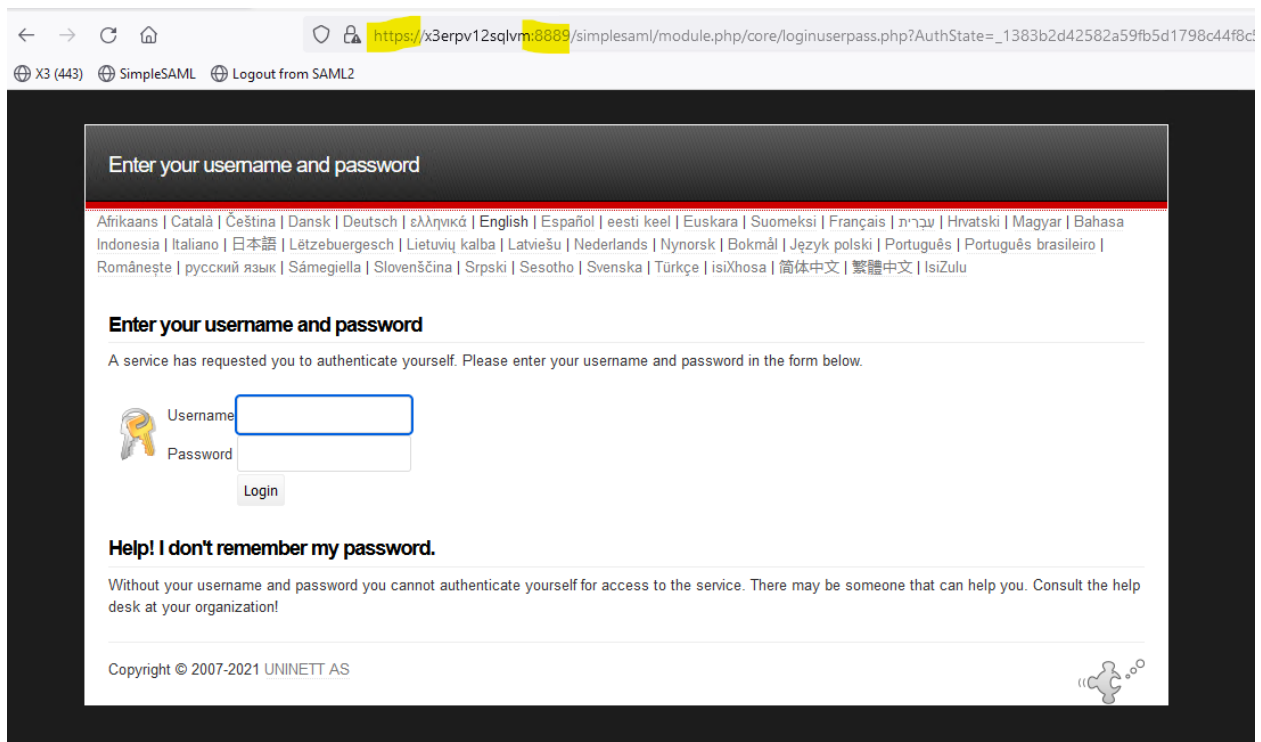
Navigate to Administration, Administration, Authentication, SAML2 id provider

Edit your SAML2 provider record

Change the “Authorize URL” and “Logout response URL” to replace http with https and replace the references to port 8888 to 8889

Save the changes, regenerate the metadata and update “saml20-sp-remote.php” file

Restart Apache SAML and Syracuse services, then re-test to confirm results



← → ↺ 🏠 https://x3erpv12sqlvm:8889/simplesaml/module.php/core/loginuserpass.php?AuthState=_1383b2d42582a59fb5d1798c44f8c


🌐 X3 (443) 🌐 SimpleSAML 🌐 Logout from SAML2


Enter your username and password

Afrikaans | Català | Čeština | Dansk | Deutsch | ελληνικά | English | Español | eesti keel | Euskara | Suomeksi | Français | עברית | Hrvatski | Magyar | Bahasa Indonesia | Italiano | 日本語 | Lëtzebuergesch | Lietuvių kalba | Latviešu | Nederlands | Nynorsk | Bokmål | Język polski | Português | Português brasileiro | Românește | русский язык | Sámegiella | Slovenščina | Srpski | Sesotho | Svenska | Türkçe | isiXhosa | 简体中文 | 繁體中文 | IsiZulu

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

Login

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!

Copyright © 2007-2021 UNINETT AS 

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:\simplesaml\cert"

The screenshot shows the 'Certificate' configuration page for 'saml_server_cert'. It includes tabs for 'Information', 'Private key', and 'Context'. The 'Information' tab is active, displaying details about the certificate, its validity period, and the private key information.

Information	Private key	Context
Name saml_server_cert Description Certificate used by the SAML2 server Internal X Certificate Valid from: 4/11/2022 1:39 PM, Valid until: 4/10/2032 1:39 PM	Private key exists X Private key Distinctive name: C=GB, ST=Berkshire, L=Winkers Triangle, O=Sage, CN=X3ERP125QLVM Issuer distinctive name: C=GB, ST=Berkshire, L=Winkers Triangle, O=Sage, CN=X3ERP125QLVM	CA Certificates Server Syracuse hosts

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

Set the "ID provider certificate" as "saml_server_cert"

The screenshot shows the 'SAML2' configuration page. It includes tabs for 'Information', 'Connection properties', and 'Users'. The 'Information' tab is active, displaying the 'Name' (SAML2) and 'Display Name' (Login using SAML2). The 'Connection properties' tab is also visible, showing various URLs and settings. The 'ID Provider certificate' is set to 'saml_server_cert'.

Restart Syracuse and Apache SAML, then retest login to X3 still works OK

This is a duplicate of the previous screenshot, showing the 'SAML2' configuration page with the 'ID Provider certificate' set to 'saml_server_cert'.

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.

As I am only on a test system, I'll generate my own certificate using the "mzMongoDB_Certs.cmd" script which is part of the "mzCertificates" package, which can be downloaded from the Sage UK Support GitHub site. (Contact me directly if you need access to these scripts)

Navigate to Administration, Administration, Certificates, Certificates of Certification Authorities and load the new CA certificate.

All > Administration > Administration > Certificates

Certificate of Certification Authority

Information Distinctive names

Name	Description	Internal	CA Certificate	Valid from	Valid until
x3_signing_ca	SAML2 signing CA	✗		4/20/2022 3:04 PM	4/17/2032 3:04 PM

Distinctive names

Distinctive name	Issuer distinctive name
C=GB, ST=Berkshire, L=Winnersh, O=Sage UK Ltd, OU=UK, CN=TestRootCA	C=GB, ST=Berkshire, L=Winnersh, O=Sage UK Ltd, OU=UK, CN=TestRootCA

Navigate to Administration, Administration, Certificates, Certificates
Load the new server certificate and private key. Specify the Root CA certificate

All > Administration > Administration > Certificates

Certificate x3_signing_cert

Information Private key Context

Name	Description	Internal	Certificate	Valid from	Valid until
x3_signing_cert	X3 SAML2 Signing Certificate	✗		4/20/2022 3:12 PM	4/17/2032 3:12 PM

Private key

Private key exists	Private key	Distinctive name	Issuer distinctive name
✓		C=GB, ST=Berkshire, L=Winnersh, O=Sage UK Ltd, OU=UK, CN=X3ERPVI25QLVM	C=GB, ST=Berkshire, L=Winnersh, O=Sage UK Ltd, OU=UK, CN=TestRootCA

Context

CA Certificates

x3_signing_ca ⚙

Server

Navigate to Administration, Administration, Authentication, SAML2 id provider

Select the appropriate "Certificate" from the list of values and save the change

Information Connection properties Users

Name

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

Authorize URL https://x3erpv12sqlvm:8889/simplesaml/saml2/idp/SSOService.php URL for SAML2 Id Provider authorization request	Logout response URL https://x3erpv12sqlvm:8889/simplesaml/saml2/idp/SingleLogoutService.php URL for response to single logout request	Callback path /auth/saml2/SAML2/callback	Metadata path /auth/saml2/SAML2/metadata
Issuer X3V12 Value of the issuer within the authorization request	Response attribute uid Name or OID of the SAML2 assertion which will be used to determine the user	Force authentication ✖	Protocol binding HTTP-POST Protocol that the ID Provider uses to send the assertion
Certificate x3_signing_cert Certificate used for signing the SAML2 request	ID Provider certificate saml_server_cert Certificate used by ID provider for signing the SAML2 response		

<https://x3erpv12sqlvm:8889/simplesaml/admin/metadata-converter.php>

©2021 The Sage Group plc or its licensors. All rights reserved. Sage, Sage logos, and Sage product and service names mentioned herein are the trademarks of Sage Global Services Limited or its licensors. All other trademarks are the property of their respective owners.

Troubleshooting

Syracuse logging can be updated to allow “login.saml2” messages to be written out

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

There may also be useful messages in the Apache log files located in D:\Apache24\logs, or the “simplesamlphp.log” in D:\simplesaml\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 2022 R1, but the steps would be similar for other Sage X3 versions.