

# Cognos Shibboleth Installation and Configuration



- [About](#)
- [Install and Configure Shibboleth](#)
  - [sp-key.pem and sp-cert.pem](#)
- [Configure Cognos](#)
- [Configure Apache](#)
- [Revert Back to LDAP Authentication](#)

## About

This document details the process to install and configure Shibboleth with Cognos. This process will need to be followed on each gateway server for Shibboleth / Apache, and a re-configuration on the Content Managers for ldap.

## Install and Configure Shibboleth

Install Shibboleth on the front end gateway servers (add the shibboleth 7 subscription to the GW servers in satellite.uoregon.edu before installing)

```
# yum install shibboleth
# yum install openssl.x86_64
```

Grab the metadata from Shibboleth:

```
# cd /etc/shibboleth
# wget https://shibboleth.uoregon.edu/idp-metadata.xml
```

### sp-key.pem and sp-cert.pem

We will need to generate new keys by running the keygen utility. Allow the keygen utility to overwrite the default existing keys. Since we are in a load-balanced scenario, the hostname is the CNAME used by the load balancer to reach the cognos proxy servers. The key/cert files are created on a single server, then copied over to all the other load-balanced servers.

```
cd /etc/shibboleth

./keygen.sh -u shibd -g shibd -e -f https://cognostest.uoregon.edu/shibboleth
```

Modify the shibboleth2.xml and attribute-map.xml files with the following:

```
# vim /etc/shibboleth/shibboleth2.xml

<!-- The ApplicationDefaults element is where most of Shibboleth's SAML bits are defined. -->
  <ApplicationDefaults entityID="https://cognostest.uoregon.edu/shibboleth"
    REMOTE_USER="uid"
    cipherSuites="DEFAULT:!EXP:!LOW:!aNULL:!eNULL:!DES:!IDEA:!SEED:!RC4:!3DES:!kRSA:!SSLv2:!SSLv3:!TLSv1:!
    TLSv1.1">

<!-- UO MOD kitday 1.30.2020 increase timeout -->
    <Sessions lifetime="32400" timeout="32400" relayState="ss:mem"
      checkAddress="false" handlerSSL="false" cookieProps="http">
<!-- UO MOD end -->

<SSO entityID="https://shibboleth.uoregon.edu/idp/shibboleth">
  SAML2
</SSO>

<MetadataProvider type="XML" path="/etc/shibboleth/idp-metadata.xml"/>

<CredentialResolver type="File" use="signing"
  key="sp-key.pem" certificate="sp-cert.pem"/>
```

```
# vim /etc/shibboleth/attribute-map.xml

<!-- UO MOD kitday 1.30.2020 -->
<!-- duckid -->
<Attribute name="urn:oid:0.9.2342.19200300.100.1.1" id="uid" />
<!-- mail -->
<Attribute name="urn:oid:0.9.2342.19200300.100.1.3" id="mail" />
<!-- displayName -->
<Attribute name="urn:oid:2.16.840.1.113730.3.1.241" id="displayName" />
<!-- lastname -->
<Attribute name="urn:oid:2.5.4.4" id="sn"/>
<!-- firstname -->
<Attribute name="urn:oid:2.5.4.42" id="givenName"/>
<!-- uoaffiliation -->
<Attribute name="urn:oid:1.3.6.1.4.1.14395.1.1.1.1.26" id="uopersonaffiliation"/>
<!-- uoaffiliation -->
<Attribute name="urn:oid:1.3.6.1.4.1.14395.1.1.1.1.26" id="uoPersonAffiliation" />
<!-- uoDirectoryname -->
<Attribute name="urn:oid:1.3.6.1.4.1.14395.1.1.1.1.21" id="uoDirectoryName" />
<!-- uoIsMemberOf -->
<Attribute name="urn:oid:1.3.6.1.4.1.14395.1.1.5.1.1" id="uoIsMemberOf"/>
<!-- UO MOD END -->
```

Save your configurations and start Shibboleth and restart Apache:

```
# service shibd start
# systemctl enable shibd
# service httpd restart
```



I copied the entire /etc/shibboleth directory from one gateway server to the other so they are identical.

Submit a ticket to the IDM team to register your Metadata with the following URL:

<https://cognostest.uoregon.edu/Shibboleth.sso/Metadata>

## Configure Cognos

In Cognos Configuration, we'll need to update the following values for ldap to accept the REMOTE\_USER header and map the uid to userID for Cognos (This only is done on the Content Managers via an [X11 session](#) under the Explorer menu Security--> LDAP-PROD):

```
User Lookup: (&(uid=${userID}))(|(isMemberOf=cn=u_o_cognos,ou=Groups,dc=uoregon,dc=edu)
(uoIsMemberOf=u_o_cc_cognos)))
```

Use External Identity: True

External Identity Mapping: (uid=\${environment("REMOTE\_USER")})

Advanced Properties, Click the Edit icon and add the following:

Name: singleSignonOption

Value: IdentityMapping

Name: trustedCredentialType

Value: IdentityMappingForTc

The screenshot shows the IBM Cognos Configuration interface. The left pane displays the Explorer tree with the following structure:

- Local Configuration
  - Environment
    - Configuration Group
      - Logging
        - File
        - Oracle Audit Logging
        - Oracle Audit Logging
      - IBM Cognos services
        - IBM Cognos
        - Portal Services
      - Security
        - Authentication
          - Cognos
          - LDAP-PROD
        - Cryptography
          - Cognos
        - Replication
          - IBM Cognos Application Firewall
      - Data Access
        - Content Manager
          - Oracle Content Store
          - cos
        - Notification
          - IBM Cognos Planning
          - Contr...

The right pane shows the LDAP-PROD - Namespaces - Resource Properties configuration table:

| Name                         | Value                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------|
| Type                         | LDAP - General default values                                                                             |
| Namespace ID                 | ldap-prod                                                                                                 |
| Host and port                | ldap.uoregon.edu:636                                                                                      |
| Base Distinguished Name      | dc=uoregon,dc=edu                                                                                         |
| User lookup                  | (&(uid=\${userID}))( (isMemberOf=cn=u_o_cognos,ou=Groups,dc=uoregon,dc=edu)(uoIsMemberOf=u_o_cc_cognos))) |
| Use external identity?       | True                                                                                                      |
| External identity mapping    | (uid=\${environment("REMOTE_USER")})                                                                      |
| Bind user DN and passw...    | *****                                                                                                     |
| Size limit                   | -1                                                                                                        |
| Time out in seconds          | -1                                                                                                        |
| Use bind credentials for ... | True                                                                                                      |
| Allow empty password?        | False                                                                                                     |
| Unique identifier            | dn                                                                                                        |
| Data encoding                | UTF-8                                                                                                     |
| SSL certificate database     | /home/cognos/certs/db/cert8.db                                                                            |
| Selectable for authentica... | True                                                                                                      |
| Advanced properties          | singleSignonOption...                                                                                     |
| Multitenancy                 |                                                                                                           |
| Tenant ID Mapping            |                                                                                                           |
| Tenant Bounding Set Ma...    |                                                                                                           |
| Folder mappings (Adv...      |                                                                                                           |
| Object class                 | organizationalunit                                                                                        |
| Description                  | description                                                                                               |
| Name                         | ou                                                                                                        |
| Group mappings (Adv...       |                                                                                                           |
| Object class                 | groupofuniquenames                                                                                        |
| Description                  | description                                                                                               |
| Member                       | uniquemember                                                                                              |
| Name                         | cn                                                                                                        |
| Account mappings (A...       |                                                                                                           |
| Account object class         | uomember                                                                                                  |
| Business phone               | telephonenumber                                                                                           |
| Content locale               | preferredlanguage                                                                                         |

Specifies a set of advanced properties.

The user needs to provide the name and the value for each advanced property.

Save the configuration and restart the CM

## Configure Apache

Next, modify the apache cognos.conf files on the GW servers to the following (this will be managed in git):

```
# vim /etc/httpd/conf.d/cognos.conf

# Licensed Materials - Property of IBM
# IBM Cognos Products: gate
# (C) Copyright IBM Corp. 2017, 2018
# US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule
Contract with IBM Corp.
#
# this is a sample cognos.conf for Apache 2.4. To use it, rename or
# copy it to "cognos.conf"
#

LoadModule headers_module modules/mod_headers.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule expires_module modules/mod_expires.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule deflate_module modules/mod_deflate.so
LoadModule filter_module modules/mod_filter.so
LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
LoadModule slotmem_plain_module modules/mod_slotmem_plain.so
LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so

#Load Cognos SSO module
LoadModule cognos_module "/opt/apps/cognos/cgi-bin/mod2_4_cognos.so"

<IfModule mod_expires.c>
    <FilesMatch "\.(jpe?g|png|gif|js|css|json|html|woff2?|template)$">
        ExpiresActive On
        ExpiresDefault "access plus 1 day"
    </FilesMatch>
</IfModule>

<IfModule mod2_4_cognos.c>
    CGIBinDir "/opt/apps/cognos/cgi-bin"
</IfModule>

<Directory /opt/apps/cognos>
    <IfModule mod_deflate>
        AddOutputFilterByType DEFLATE text/html application/json text/css application/javascript
    </IfModule>
    Options Indexes MultiViews
    AllowOverride None
    Require all granted
</Directory>

#Set up a cluster for load-balancing
<Proxy balancer://mycluster>
    #BalancerMember http://is-cognostestds1.uoregon.edu:9300 route=1
    #BalancerMember http://is-cognostestds2.uoregon.edu:9300 route=1
    BalancerMember http://cognosdispatch-test.uoregon.edu:9300 route=1
</Proxy>

# UI to monitor/configure load balancer
<Location /ibmcognos/balancer-manager>
    SetHandler balancer-manager
</Location>

Alias /ibmcognos /opt/apps/cognos/webcontent

RewriteEngine On
# Send default URL to service
RewriteRule ^/$ /ibmcognos/ [R,L]
RewriteRule ^/ibmcognos/bi/$ balancer://mycluster/bi/ [P]

#UO MOD kitday add rule for Jupyter Server
RewriteRule ^/ibmcognos/bi/v1/jupyter/(user/[^]*)/(api/kernels/[^]+/channels)(.*) ws://is-cognostestcm2.
```

```

uoregon.edu:8000/bi/v1/jupyter/$1/$2$3 [P,L]

#UO MOD kitday send REST API to dispatcher pool
RewriteRule ^/ibmcognos/bi/v1/disp/rds/(.+) http://cognosdispatch-test.uoregon.edu:9300/bi/v1/disp/rds/$1 [P]
ProxyPassReverse ^/ibmcognos/bi/v1/disp/rds/(.+) http://cognosdispatch-test.uoregon.edu:9300/bi/v1/disp/rds/

# Send login requests and legacy UI's through cognos module for SSO
RewriteRule ^/ibmcognos/bi/v1/(login|disp)(/.*)? /ibmcognos/sso/bi/v1/$1$2 [PT,L]
# OR (enable one or the other)
# Send login requests and legacy UI's through the cognos cgi for SSO
# RewriteRule ^/ibmcognos/bi/v1/(login|disp)(/.*)? /ibmcognos/cgi-bin/cognos.cgi/bi/v1/$1$2 [PT]

# Rewrite Event Studio static references
RewriteCond %{HTTP_REFERER} v1/disp [NC,OR]
RewriteCond %{HTTP_REFERER} (ags|cr1|prompting|ccl|common|skins|ps)/(.*)\.css [NC]
RewriteRule ^/ibmcognos/bi/(ags|cr1|prompting|ccl|common|skins|ps)/(.*) /ibmcognos/$1/$2 [PT,L]

# Rewrite Saved-Output and Viewer static references
RewriteRule ^/ibmcognos/bi/rv/(.*)$ /ibmcognos/rv/$1 [PT,L]

# Define cognos location
<Location /ibmcognos>
    RequestHeader set X-BI-PATH /ibmcognos/bi/v1
    AuthType shibboleth
    ShibRequestSetting requiresession 1
    Require shib-attr uoIsMemberOf ~ ^uo_cc_cognos$
</Location>

#Allow API Rest endpoints without Shibboleth
<Location /ibmcognos/bi/v1/disp/rds>
    AuthType Shibboleth
    ShibRequestSetting requireSession false
    Require shibboleth
    Require all granted
</Location>

# Route CA REST service requests through proxy with load balancing
<Location /ibmcognos/bi/v1>
    ProxyPass balancer://mycluster/bi/v1
</Location>

# UO MOD enable sticky session
<Location /ibmcognos/bi/v1>
    Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e; path=/ibmcognos/bi/v1"
    env=BALANCER_ROUTE_CHANGED
    ProxyPass balancer://mycluster/bi/v1 stickysession=ROUTEID
</Location>

ProxyPass /Shibboleth.sso !
ProxyPassReverse /Shibboleth.sso !
ProxyRequests Off
ProxyPreserveHost On

<Proxy *>
    Require all granted
</Proxy>

# Route login and legacy UI requests through mod_cognos
<Location /ibmcognos/sso>
    SetHandler cognos-handler
    AuthType shibboleth
    ShibRequestSetting requiresession 1
    Require shib-attr uoIsMemberOf ~ ^uo_cc_cognos$
</Location>

<Directory "/opt/apps/cognosfiles/images">
    Options Indexes FollowSymLinks MultiViews IncludesNoExec
    AddOutputFilter Includes html
    AllowOverride None
    Require all granted
    DAV On

```

```

</Directory>

Alias /ibmcognos/bi/v1/ext/Custom_Media/images "/opt/apps/cognos/temp/extensions/Custom_Media/images"
<Directory "/opt/apps/cognos/temp/extensions/Custom_Media/images">
    Options Indexes FollowSymLinks MultiViews IncludesNoExec
    AddOutputFilter Includes html
    AllowOverride None
    Require all granted
    DAV On
</Directory>

Alias /ibmcognos/samples/images "/opt/apps/cognos/webcontent/bi/samples/images"
<Directory "/opt/apps/cognos/webcontent/bi/samples/images">
    Options Indexes FollowSymLinks MultiViews IncludesNoExec
    AddOutputFilter Includes html
    AllowOverride None
    Require all granted
    DAV On
</Directory>

Alias /samples "/samples"

<Directory "/samples/images">
    Options Indexes FollowSymLinks MultiViews IncludesNoExec
    AllowOverride None
    Require all granted
</Directory>

<Location /samples>
    DAV On
</Location>

```

Since the backend gateway servers are running on port 80 and ssl offloading is handled at the F5, in order to Shibboleth to use https bindings we need to add the following lines to httpd.conf:

```

# vim /etc/httpd/conf/httpd.conf

<VirtualHost *:80>
    ServerName https://cognostest.uoregon.edu
    Include conf.d/cognos.conf
</VirtualHost>

```

We'll also need to configure the LD\_LIBRARY\_PATH for apache for the Cognos web module to load correctly:

```

# vim /etc/sysconfig/httpd

#OPTIONS=
LD_LIBRARY_PATH=/opt/apps/cognos/cgi-bin

```

Now restart apache and test

## Revert Back to LDAP Authentication

If Shibboleth authentication stops working and we need to revert back to ldap authentication, do the following on **each** gateway server (is-cognosprod-gw1, is-cognosprod-gw2):

```

# cd /etc/httpd/conf.d
# cp cognos.conf.preshib cognos.conf
# service httpd restart

```

