

## Thingworx SSO Configuration with Okta as IDP

### Requirement:

Service Provider	Thingworx 9.3.12
Central Auth Server	Ping Federate 11.1
Identity Provider	Okta
Resource Provider	Windchill 12.1

### Checklist for the overall configuration

1. Refer [Software Matrix](#)
2. Refer [Release advisor](#)
3. Refer [Prerequisites](#)
4. Create Keystore for Thingworx (should contain pingfed\_signing\_certificate and Thingworx SSL certificate)
5. Create Database for Thingworx
6. Install Java
7. Install Thingworx Platform [Refer](#)
8. Configure License
9. Create Keystore for thingworx Navigate
10. Create Truststore for Thingworx Navigate
11. Install thingworx Navigate
12. Configure custom app for Thingworx in Okta
13. [Install Pingfederate](#)
14. Configure Pingfederate License
15. Configure SSL certificate
16. Import chain of certificates separately in Trust CAs (end cert, intermediate and root)
17. Update BaseURL and SP Entity ID (this can be anything, just a unique id to refer in okta configuration) [Refer](#)
18. Download Automation script from PTC software download page
19. Update the user.properties file as per the requirement
20. Place navigate SSL cert, ping federate Root CA cert alone, okta certificate in input folder of automation script
21. Install Git bash for windows
22. Run the automation script
23. The automation script creates four files
24. Place the server certificate in Java keystore
25. Place the signing certificate in thingworx keystore and okta application configuration
26. Point out idp\_metadata file while configuring thingworx navigate
27. Refer sp\_metadata.xml file and configure okta
28. Update securityContext.xconf file and web.xml file and do windchill configurations for sso
29. Run xconfmanager and restart apache and windchill
30. [Configure Thingworx navigate](#)

31. Add a user in to administrator group
32. Add other users to appropriate license group
33. [Validate services](#) in ptc-windchill-integration-connector and ptc-windchill-Odata-connector
34. Launch thingworx navigate from admin user account and configure the task collections as per your requirement
35. Troubleshoot for issues
36. Enable/Disable SSO by updating "EnableSSO" property in to true/false in platform-settings.json file and restart services

## Configure custom app for Thingworx in Okta

### Create SAML 2.0 custom application

**Single sign-on URL:** <https://<pingfederate host name>:9031/sp/ACS.saml2>

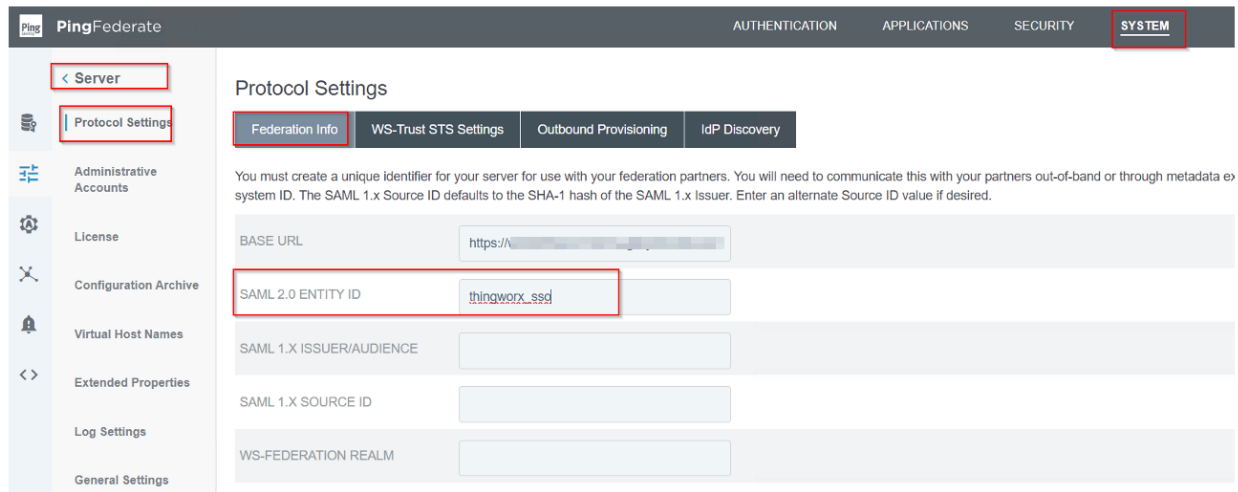
(This value is identified from pingfed\_sp\_metadata.xml file)

```

1 <md:EntityDescriptor ID="KmfwgXsQWpqggMdkKtqSIRZWBaf" cacheDuration="PT1440M" entityID="thingworx_sso" xmlns:md="urn:oasis:names:to:SAML:2.0:metadata">
2 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
3 <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><ds:KeyInfo><ds:X509Certificate><ds:X509Data></ds:X509Data></ds:KeyInfo></ds:Signature><md:KeyDescriptor><md:AssertionConsumerService index="0" Location="
4 https://<pingfederate host name>:9031/sp/ACS.saml2" Binding="urn:oasis:names:to:SAML:2.0:bindings:HTTP-POST" isDefault="true" />
5 <md:AttributeConsumingService index="0"><md:ServiceName xml:lang="en">AttributeContract</md:ServiceName><md:RequestedAttribute Name="uid" />
6 <md:RequestedAttribute Name="email" /><md:RequestedAttribute Name="group" /></md:AttributeConsumingService></md:SPSSODescriptor><md:ContactPerson
7 contactTypes="administrative" /></md:EntityDescriptor>

```

**Audience URI (SP Entity ID) Thingworx\_sso** (this value is taken from pingfederate configuration)



**Default Relaystate :** <http://<Thingworx host name>:8443/Thingworx/Runtime/index.html?mashup=LandingPageAccessAppMashup>

Attribute statements (optional)

Name	email	Name format	Basic	Value	user.email
------	-------	-------------	-------	-------	------------

"email" is the attribute name that will be passed by the IDP to the CAS server. This attribute should be added in user.properties file and mentioned while configuring thingworx navigate. We can add any attribute as per our requirement

## Okta custom app configuration page:

**A** SAML Settings

**General**

Single sign-on URL ?   
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ?

Default RelayState ?   
If no value is set, a blank RelayState is sent

**Attribute Statements (optional)** [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="uid"/>	<input type="text" value="Basic"/>	<input type="text" value="user.email"/>
<input type="text" value="email"/>	<input type="text" value="Basic"/>	<input type="text" value="user.email"/>

## Thingworx navigate configuration page

ThingWorx Navigate Configuration

**Basic Settings for Identity Provider and Service Provider**

PTC

IDP metadata file (\*.xml file)

You can obtain the IDP metadata file from your CAS

SAML Assertion UserName AttributeName

Enter your ThingWorx Service Provider connection information here

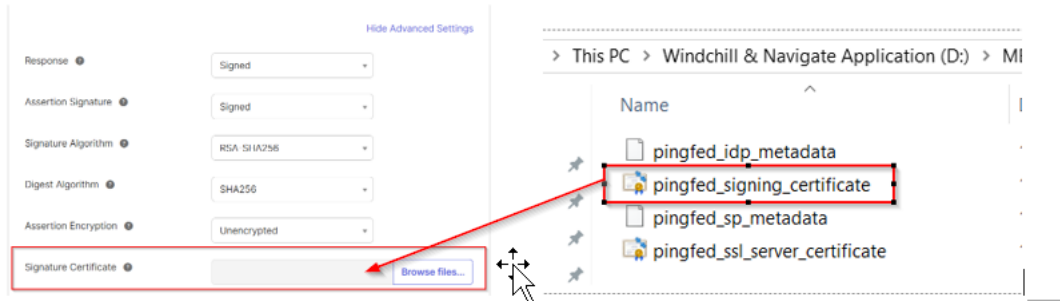
Metadata Entity ID

This is the unique ID that you provided when configuring the Service Provider connection in your CAS.

[PTC Identity and Access Management Help Center](#)

[ThingWorx Help on Single Sign-On](#)

## Import pingfed signing certificate (created by pingfed automation script) in okta

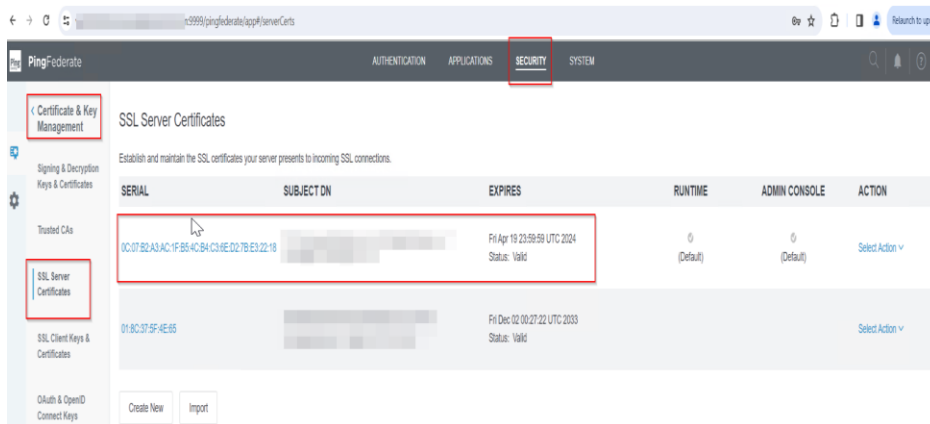


## User.properties file (In pingfed automation script)

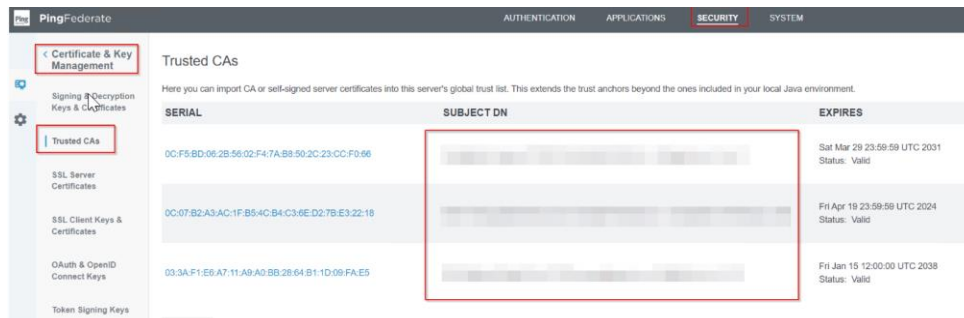
```
##IDP CONNECTIONS - GENERIC SAML
create_idp_saml2_connection_entityId='http://www.okta.com/
create_idp_saml2_connection_baseUrl='https://
create_idp_saml2_connection_input_sign_verif_cert='okta.crt'
create_idp_saml2_connection_assertion_consumer_service_url='/app/
create_idp_saml2_attr_uid='uid'
create_idp_saml2_attr_group='group'
create_idp_saml2_attr_email='email'
```

## Configure SSL certificate in pingfederate

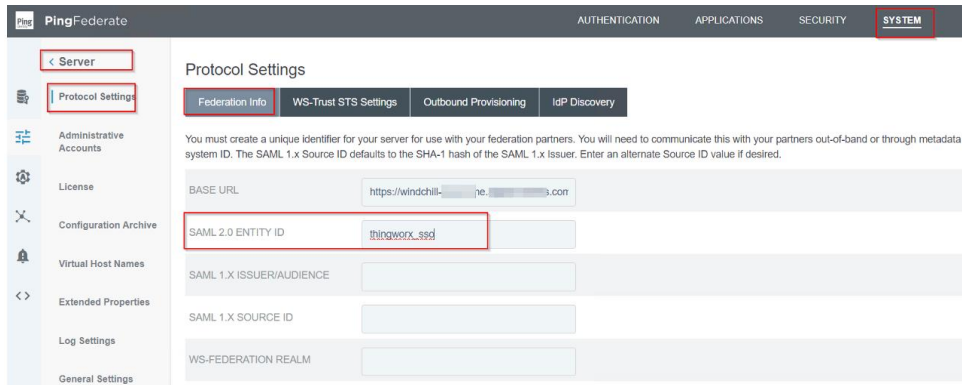
SSL certificate should be in PKCS12 format



## Add the chain of certificates in Trust CAs

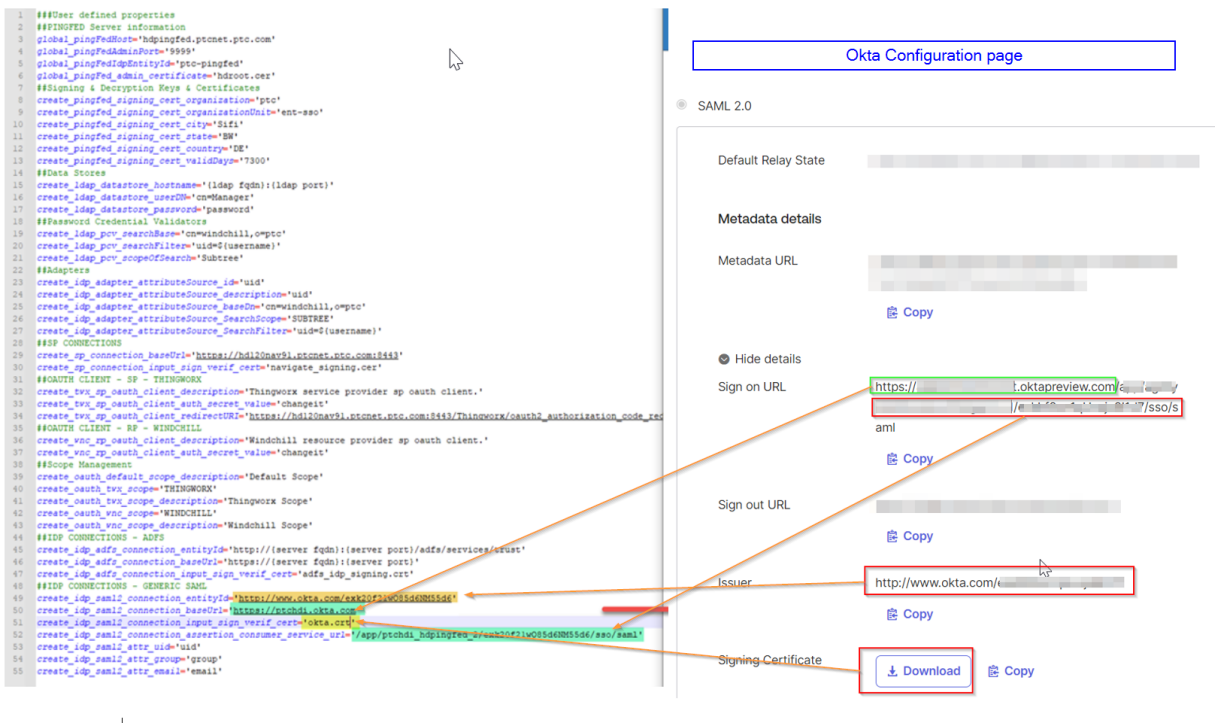


Update BaseURL and SP Entity ID (this can be anything, just a unique id to refer in okta configuration)

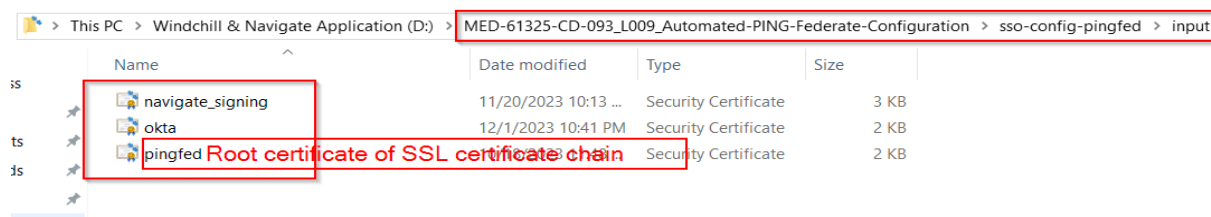


Update the user.properties file as per the requirement

Refer this PTC Case: <https://www.ptc.com/en/support/article/CS335189>



Place certificates in the input folder of automation script



## Run the automation script

Successful script run looks like this

```

MINGW64/d/MED-61325-CD-093_L009_Automated-PING-Federate-Configuration/sso-config-pingfed
kavitha.gunasekaran@windchill11-dev MINGW64 /d/MED-61325-CD-093_L009_Automated-PING-Federate-Configuration
$ cd sso-config-pingfed/
kavitha.gunasekaran@windchill11-dev MINGW64 /d/MED-61325-CD-093_L009_Automated-PING-Federate-Configuration/sso-config-pingfed
$ ./config.sh -d
1. PingFederate as IDP - LDAP
2. External IDP - ADFS
3. External IDP - Generic SAML 2.0
Enter the Option:
1
Option Selected:
External IDP - Generic SAML 2.0
Enter PingFederate admin user password:
SUCCESSFULLY CREATED PINGFED SIGNING CERTIFICATE: tvpnpmg9G2e4v5j2ftumff81
SUCCESSFULLY DOWNLOADED PINGFED SIGNING CERTIFICATE: 'output/pingfed_signing_certificate.crt'
SUCCESSFULLY CREATED AUTH POLICY CONTRACT: qs15HMVbtioefnIR
SUCCESSFULLY DOWNLOADED PINGFED SSL SERVER CERTIFICATE: 'output/pingfed_ssl_server_certificate.crt'
SUCCESSFULLY CREATED SP Connection: a9fm32pG9Mv1lu2nBHoPonpJMgt
SUCCESSFULLY EXPORTED PINGFED METADATA: 'output/pingfed_idp_metadata.xml'
SUCCESSFULLY CREATED ACCESS TOKEN MANAGER: default
SUCCESSFULLY CREATED ACCESS TOKEN MAPPING: default|default
SUCCESSFULLY CREATED TWX SP CLIENT: twx-sp-client
SUCCESSFULLY CREATED WNC RP CLIENT: wnc-rp-client
SUCCESSFULLY CREATED TWX AND WNC SCOPES: THINGWORX WINDCHILL
SUCCESSFULLY CREATED GENERIC SAML2.0 IDP Connection: XslV6GQ,twz3X-1mDn0iKAuid7a
SUCCESSFULLY EXPORTED PINGFED IDP METADATA: 'output/pingfed_sp_metadata.xml'
Successfully configured PingFederate and generated artifacts for the SSO setup in output folder.
kavitha.gunasekaran@windchill11-dev MINGW64 /d/MED-61325-CD-093_L009_Automated-PING-Federate-Configuration/sso-config-pingfed
$

```

### The automation script creates four files in output folder

> This PC > Windchill & Navigate Application (D:) > MED-61325-CD-093\_L009\_Automated-PING-Federate-Configuration > sso-config-pingfed > output

Name	Date modified	Type	Size
pingfed_idp_metadata	12/7/2023 2:27 AM	XML Document	3 KB
pingfed_signing_certificate	12/7/2023 2:26 AM	Security Certificate	2 KB
pingfed_sp_metadata	12/7/2023 2:27 AM	XML Document	6 KB
pingfed_ssl_server_certificate	12/7/2023 2:26 AM	Security Certificate	3 KB

## Update securityContext.xconf file and web.xml file

### SecurityContext.xconf

```

<Property default="/oauth/**" name="com.ptc.eauth.identity.oauth2.rs"/>
<Property default="https://windchill-dev. .com:9031/as/introspect.oauth2"
name="org.springframework.security.oauth2.provider.token.RemoteTokenServices.checkTokenEndpointUrl"/>
<!--# Client ID required to authorize access to token validation/introspection endpoint.-->
<Property default="wnc-rp-client" name="org.springframework.security.oauth2.provider.token.RemoteTokenServices.clientId"/>
OAuth client name mentioned in user.properties file for pingfederate configuration
<!--# Client secret required to authorize access to token validation/introspection endpoint.-->
<Property default="changeit" name="org.springframework.security.oauth2.provider.token.RemoteTokenServices.clientSecret"/>
windchill scope pwd mentioned in user.properties file
#SCOPE can be WINDCHILL- allow user to access Windchill services-->
<Property default="WINDCHILL" name="com.ptc.eauth.identity.oauth2.rs.InMemoryResourceScopeService.resourceScopes./**"/>
windchill scope name mentioned user.properties file

```

### Web.xml file

#### Refer:

[https://support.ptc.com/help/windchill/wc110\\_hc/whc\\_en/#page/Windchill\\_Help\\_Center%2FWCAdvDeAuth\\_ConfigAltAuth\\_RegisterScope.html%23](https://support.ptc.com/help/windchill/wc110_hc/whc_en/#page/Windchill_Help_Center%2FWCAdvDeAuth_ConfigAltAuth_RegisterScope.html%23)