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

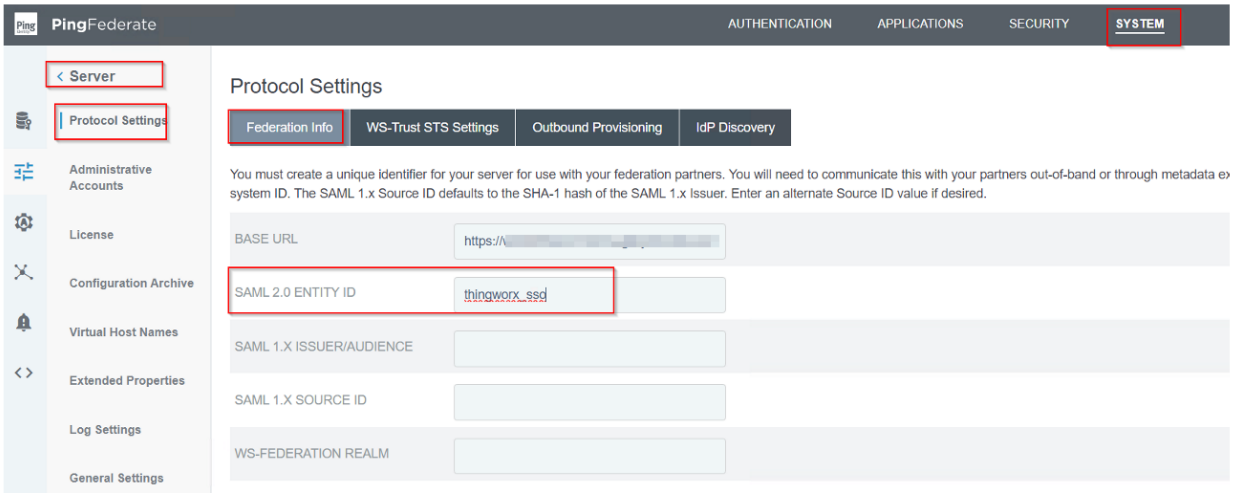
31. Add a user in to administrator group
32. Add other users to appropriate license group
33. Validate services in ptc-windchill-integration-connector and ptc-windchill-Odata-connector
34. Launch thingworx navigate from admin user account and configure the task collections as per your requirement
35. 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)

Audience URI (SP Entitiy ID) Thingworx_sso (this value is taken from pingfederate configuration)



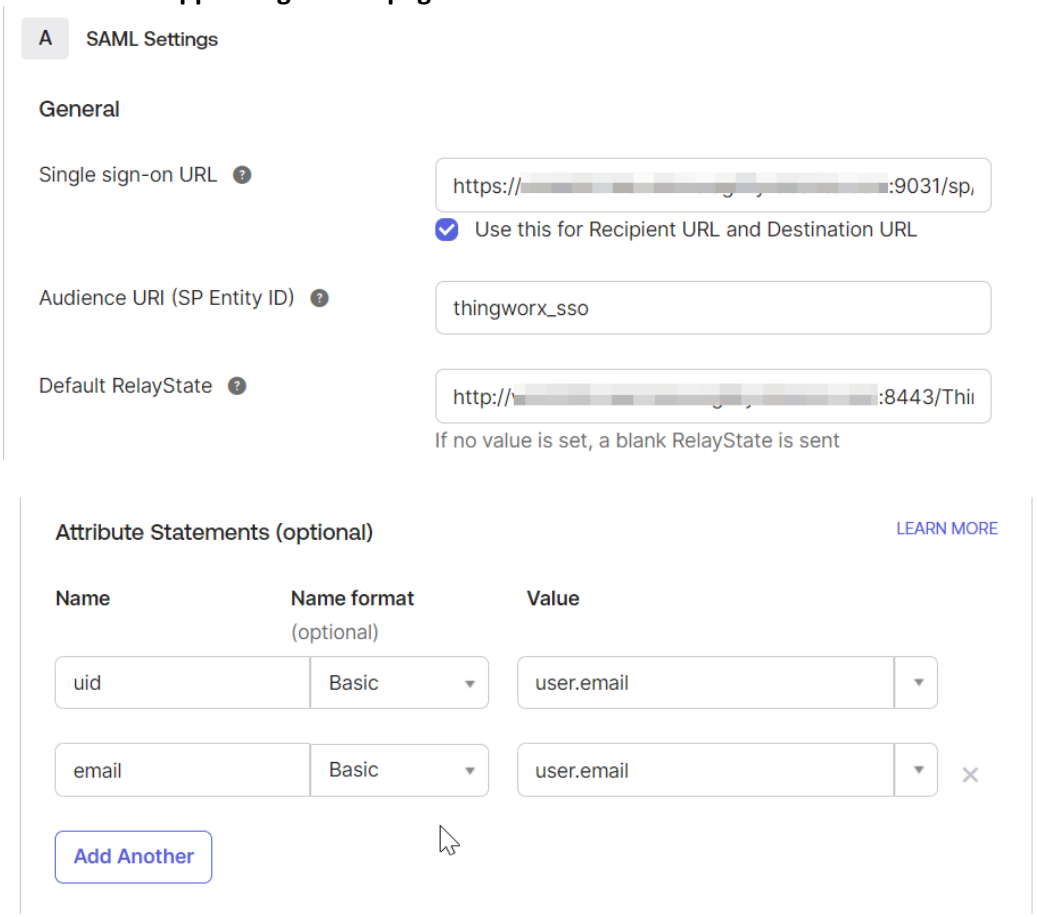
Default Relaystate : http://<Thingworx host name>:8443/Thingworx/Runtime/index.html?mashup=LandingPageAccessAppMashup

Attribute statements (optional)

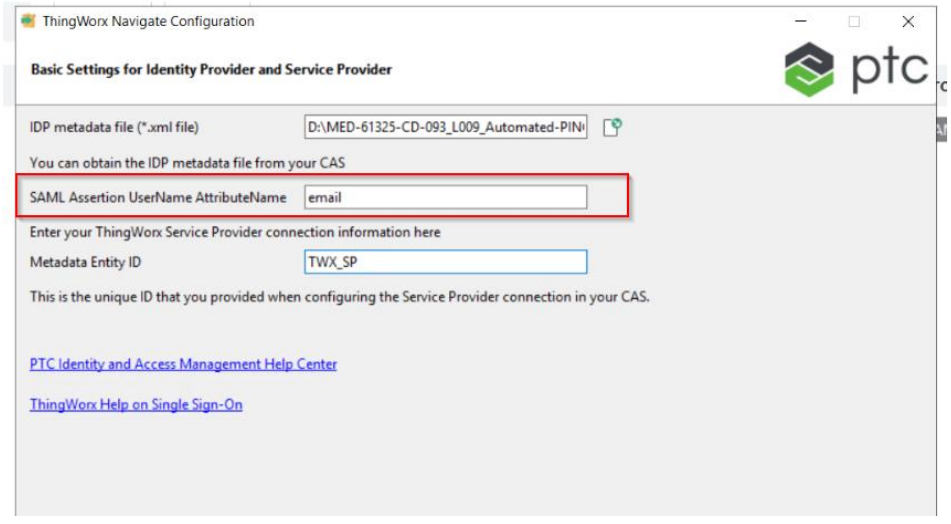
Name	email	Name format	Basic	Value	user.email

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

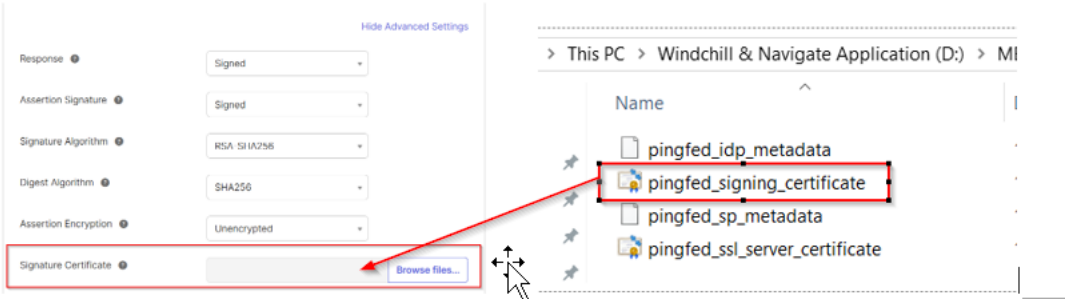
Okta custom app configuration page:



Thingworx navigate configuration page



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

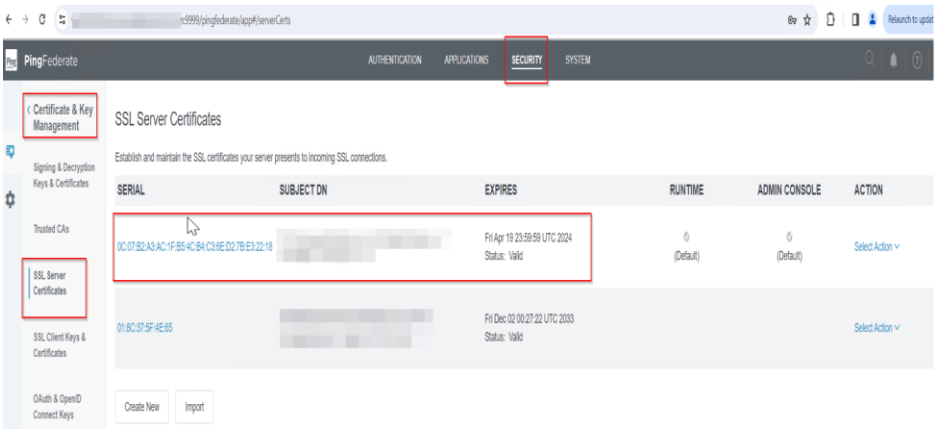


User.properties file (In pingfed automation script)

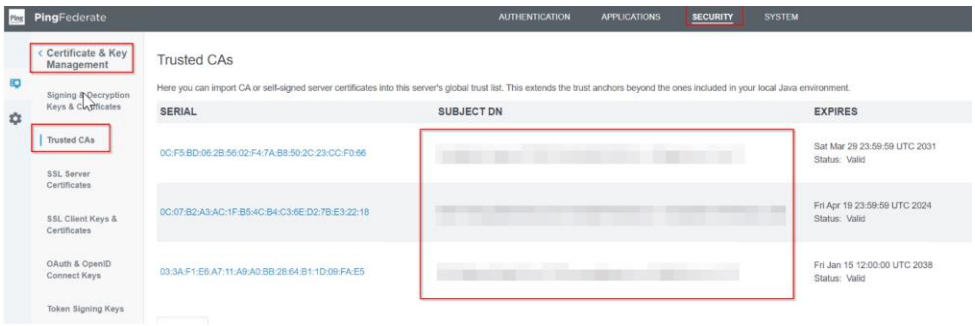
```
##IDP CONNECTIONS - GENERIC SAML
create_idp_saml2_connection_entityId='http://www.okta.com/
create_idp_saml2_connection_baseUrl='https://                .oktapreview.com'
create_idp_saml2_connection_input_sign_verif_cert='okta.crt'
create_idp_saml2_connection_assertion_consumer_service_url='/app/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

Configure SSL certificate in pingfederate

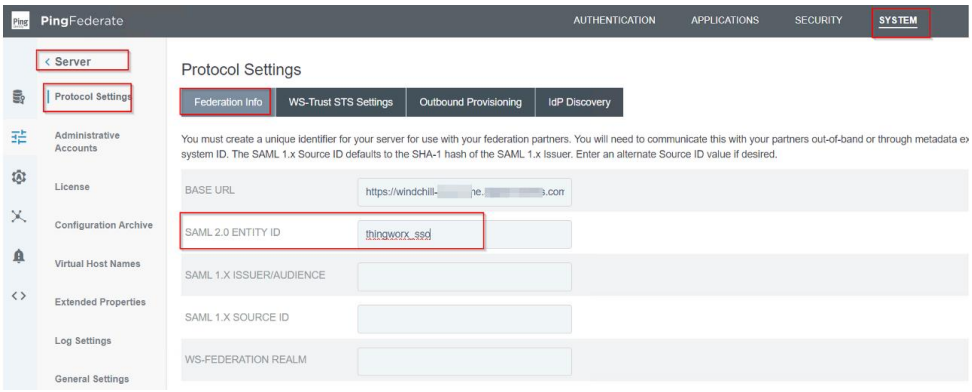
SSL certificate should be in PKCS12 format



Add the chain of certificates in Trust CAs

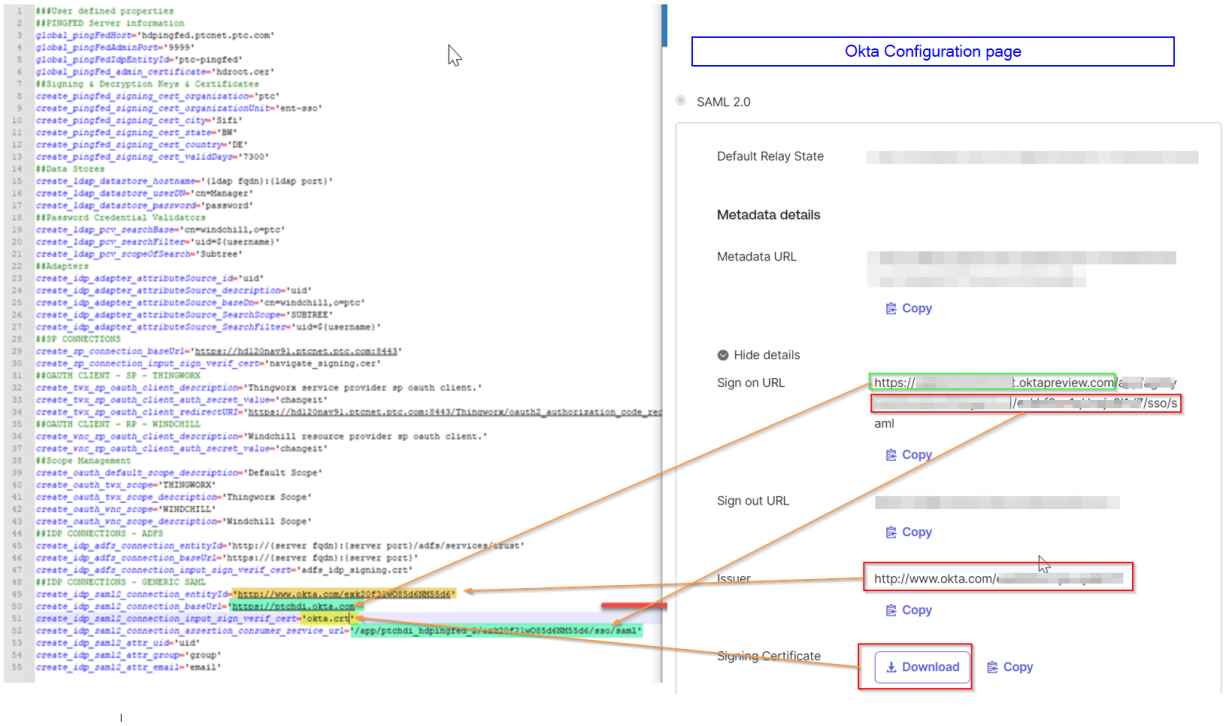


Update BaseURL and SP Entity ID (this can be anything, just a unique id to refer in okta configuration)

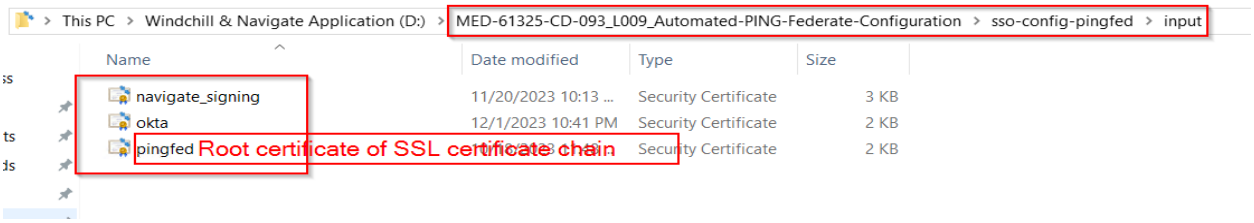


Update the user.properties file as per the requirement

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

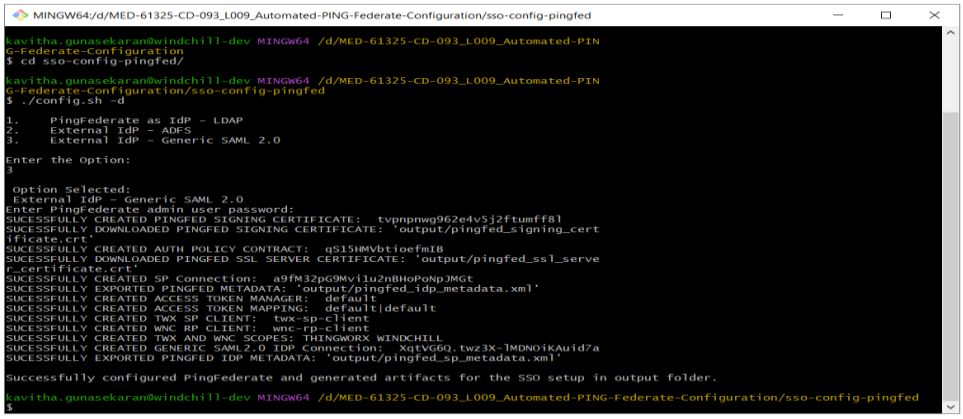


Place certificates in the input folder of automation script

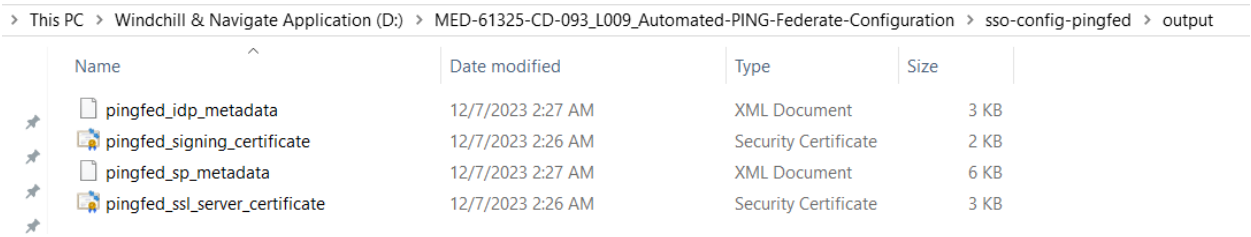


Run the automation script

Successful script run looks like this



The automation script creates four files in output folder



Update securityContext.xconf file and web.xml file

SecurityContext.xconf

Web.xml file

Refer:

https://support.ptc.com/help/windchill/wc110_hc/whc_en/#page/Windchill_Help_Center%2FWCAdvDepAuth_ConfigAltAuth_RegisterScope.html%23