
ORACLE®

Agenda

1. Short introduction into SSO based authentication
2. Configuring supported SSO types
3. Common issues when misconfiguring SSO
4. Troubleshooting Tips
5. Demo
6. Q&A

Short introduction into SSO based authentication

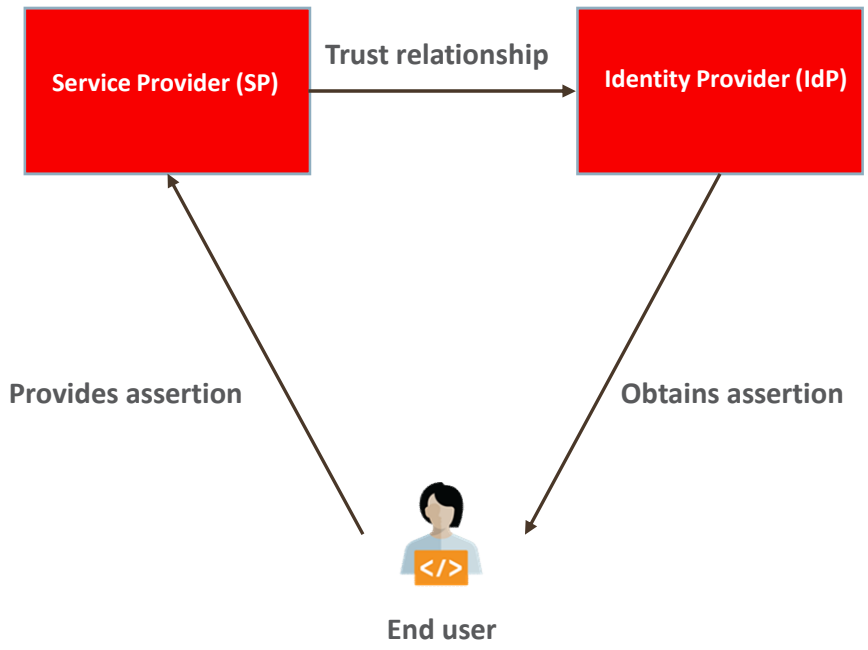
Short introduction into SSO based authentication

- Identity Provider(IdP)

  - User credentials repository / creates and manages authentication services.

- Service Provider(SP)

  - Federation partner that provides services to users



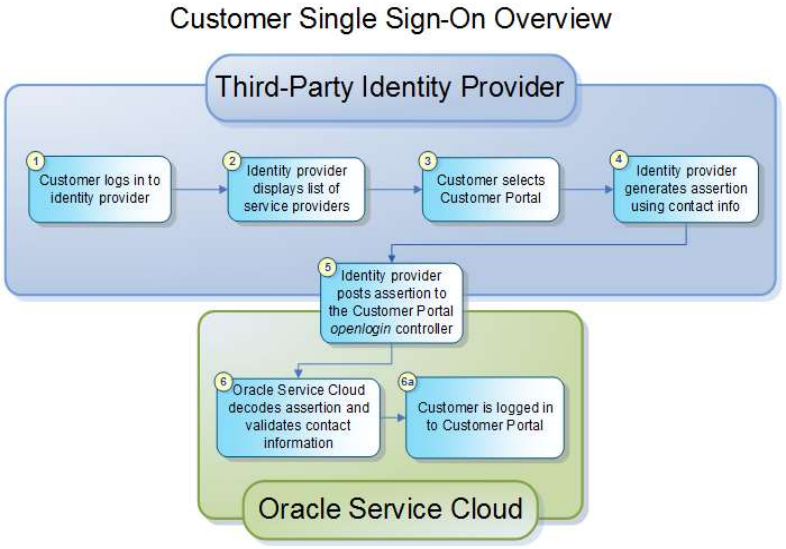
Configuring supported SSO types

Customer Portal SSO

- Supports only Identity Provider(IdP) initiated SSO
- Assertion Consumer Service (ACS) URL
  https://[site]/ci/openlogin/saml/<loginParameter>

  - Ex:contact.login(default), contact.id, contact.email.address
- Redirect added to ACS URL - can point to any page (/app/*) or controller endpoint (/ci/* or /cc/*)

  - Ex: ci/openlogin/saml/subject/contact.id/redirect/app/ask
- Entity ID can be any value in the IdP
- Passed to the openlogin controller



Agent Console IdP initiated SSO configuration – Version 1

- ACS URL set at IdP side:

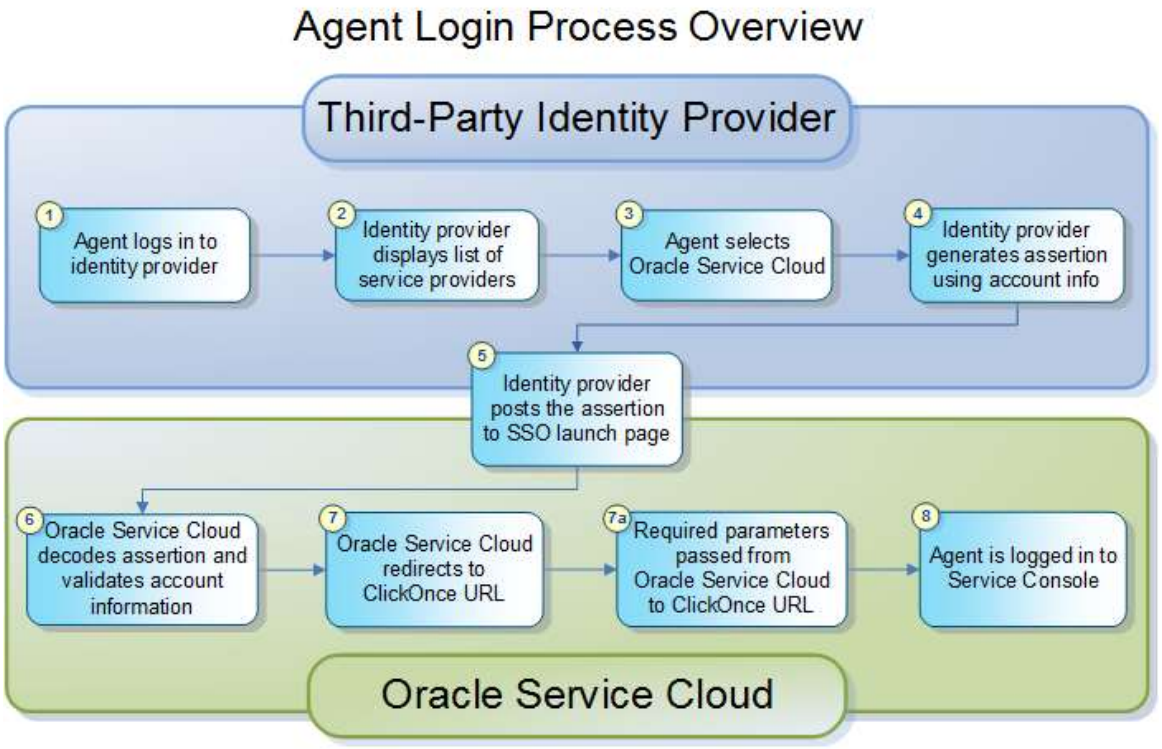
https://[site]/cgi-bin/[interface].cfg/php/admin/sso_launch.php?p_subject=<loginParameter>

- p_subject values:
  - **Account.Login**(default parameter/value is case sensitive)
  - **Account.Emails.Address**(value is case insensitive)
  - **Account.ID**
- SSO profile permissions enabled
- Entity ID can be any unique value in the IdP
- Must use Internet Explorer or Edge to launch console / .NET constraint

Agent Console IdP initiated SSO configuration – Version 2

- Must be used if implementing for AgentWeb(BUI)
- ACS URL https://[site]/cgi-bin/[interface].cfg/php/sso/saml2/sp/post/acs.php
  - Configuration performed from console via “Single Sign-On Configuration” component
  - Export SP metadata file and import into IdP
  - Import IdP’s metadata file into OSvC
- Only tick “Active” checkbox from “Single Sign-On Configuration” component
- SSO profile permissions enabled
- Can define NameID Format
- Supports Encryption
- Entity ID can be any unique value in the IdP
- Must use Internet Explorer or Edge to launch console / .NET constraint

Agent Console IdP SSO login process



Browser User Interface (BUI) IdP initiated SSO

- Initiated at IdP side

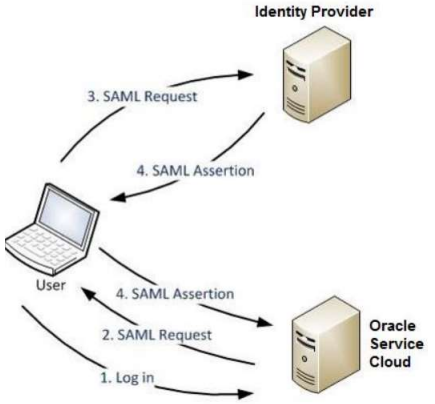
- ACS URL https://[site]/cgi-bin/[interface].cfg/php/sso/saml2/sp/post.acs.php
  - Configuration performed from console via “Single Sign-On Configuration” component
  - Export SP metadata file and import into IdP
  - Import IdP’s metadata file into OSvC
- Only tick “Active” checkbox from “Single Sign-On Configuration” component
- SSO Profile Permissions + AgentBUI/Account Authentication
- Relay state set to point to https://[site]/AgentWeb via HTTPS POST at IdP side

Agent Console and BUI service provider(SP) initiated SSO

- Initiated at SP(OSvC) side

- ACS URL https://[site]/cgi-bin/[interface].cfg/php/sso/saml2/sp/post.acs.php
  - Configuration performed from console via “Single Sign-On Configuration” component
  - Export SP metadata file and import into IdP
  - Import IdP’s metadata file into OSvC

- Tick “Active” and “Web SSO” checkbox from “Single Sign-On Configuration” component
- Relay state configuration not needed
- Entity ID from console must match value from IdP
- Supports single logout
- Can define NameID Format
- Supports Encryption



Mandatory requirements when implementing SSO

- Upload public signing certificates into File Manager
  - File Manager folders:
    - Additional Root Certificates
    - Intermediate certificates
- Place value/s in SAML_20_SIGN_CERTS setting
  - Fingerprint of the signing certificate
  - Character proof the fingerprint(colons/quotations)

Common issues when misconfiguring SSO

Common issues when misconfiguring SSO - 1

- SAML_20_SIGN_CERTS configuration setting value/s
  - Different fingerprint altogether
- Colons/quotation marks are not removed from the fingerprint

  e.g. : ("**43:51:43:A1:B5:FC:8B:B7:0A:3A:A9:B1:0F:66:73:A8**")
  - Hidden spaces at either the beginning or end of the fingerprint
- ANY-TRUSTED value used in a Production environment
  - Signing Certificate cannot be validated against uploaded certificates

Common issues when misconfiguring SSO - 2

- Entity ID does meet IdP requirements
  - Some IdPs do not support special characters(+,--,=)
- Incorrect Subject values or missing Subject
  - Subject value does not match authentication field from DB
  - Subject values are case sensitive
  - E-mail not set as the login field
  - Account or contact not created in the DB / Auto-Provisioning not enabled
  - Subject is not define and not passed in the response

Common issues when misconfiguring SSO - 3

- Public Signing certificate cannot be validated
  - Certificate is expired
  - Certificate requires intermediated/chain certificates
  - Incorrect certificate is uploaded
- HTTP POST/GET binding type is properly used
- Servers are not time-synchronized

Troubleshooting Tips

Troubleshooting Tips

- Check Certificate Validity
  - OpenSSL
  - https://www.sslshopper.com
  - Discern if certificate needs intermediate certificates
- SAML response decoders / resource capturing tools
  - Fiddler – can capture SAML Response
  - SAML tracers Firefox/Chrome – Read assertion/Response
  – https://www.samltool.com - Decode and read assertion
- Error logs
  - Console> Configuration> Site Configuration> Logs

Demo

Q&A


ORACLE®