

SSO eliminates the need of creating a new login credential with a username and password.

If you already have an account, you can still retrieve it to log in from one system to another.

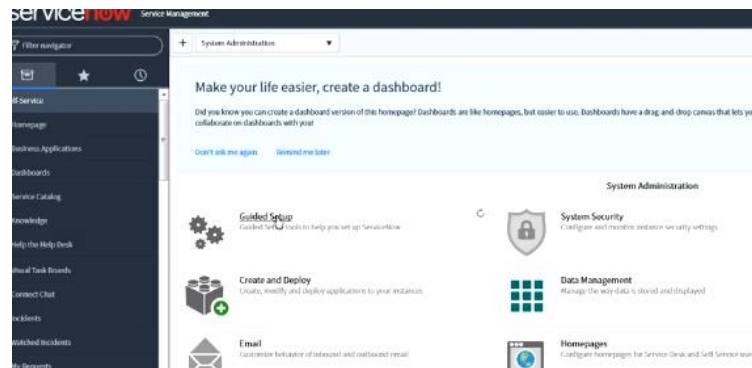
Let's say in an organization we create a new ServiceNow instance... and then we must migrate all the Users. Since they are in an Active Directory, we don't need to create them again from scratch. We can simply integrate them from one instance to another.

The benefit of SSO is if we have a large amount of Users, they are stored in an Active Directory. We can migrate them from one instance to another. We don't need to remember passwords... ServiceNow can remember the usernames and their respective passwords.

This is what the SSO page looks like:



...if we were to integrate a current user from one instance to another, we input his login credentials...



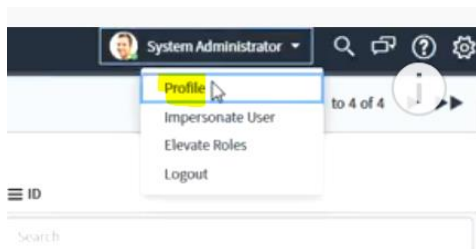
...and now he has successfully logged in to the newer ServiceNow instance.

We migrate the user from the Active Directory to the SSO.

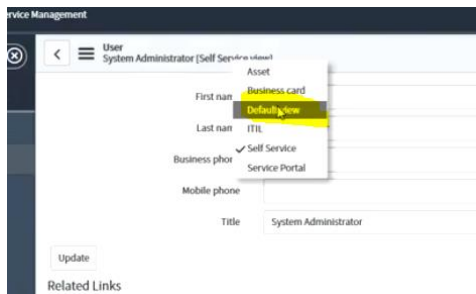
It is because of ServiceNow's capability to read the Active Directory that we don't need to create new user login credentials.

Step One: Obtain and save the local username and password:

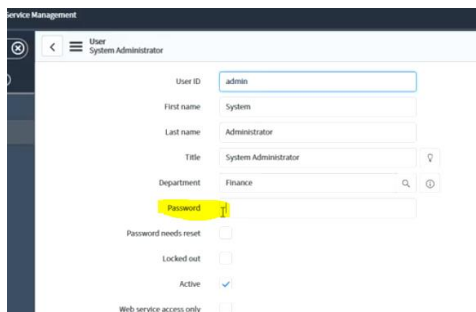
Go to Profile...



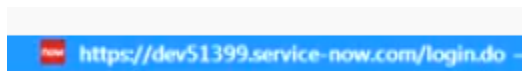
...then Default View...



...then input for Password...

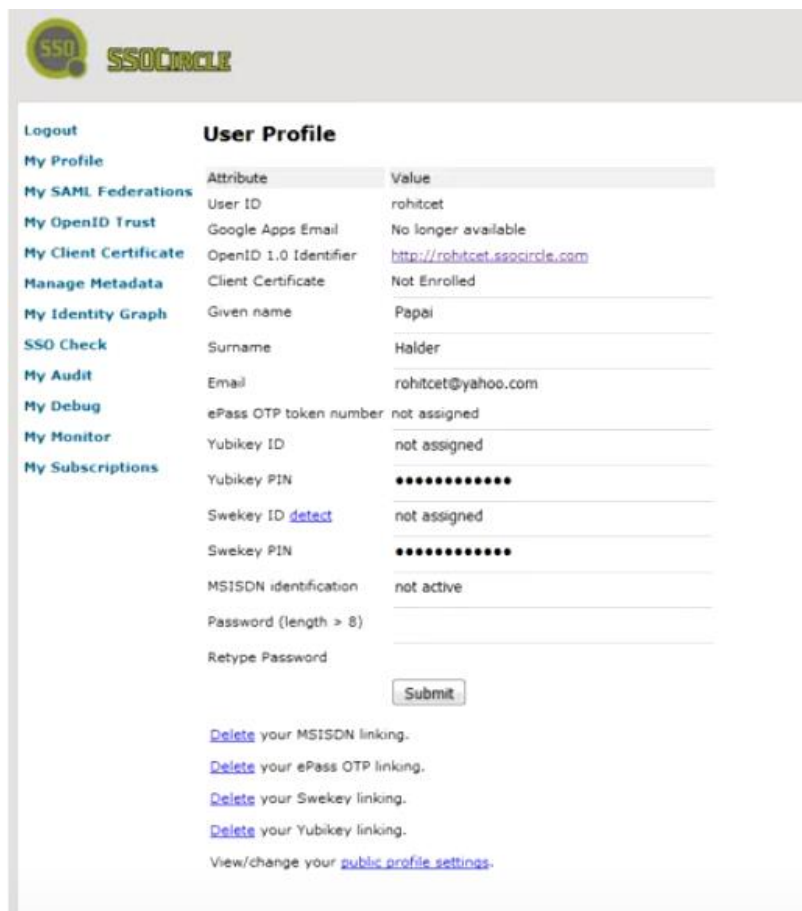


...if you encounter issues, you may also obtain username and password via the XML file in the link:



Step Two: Configure the IdP:

For example, SSOCircle:



The screenshot shows the SSOCircle User Profile page. On the left is a sidebar with navigation links: Logout, My Profile, My SAML Federations, My OpenID Trust, My Client Certificate, Manage Metadata, My Identity Graph, SSO Check, My Audit, My Debug, My Monitor, and My Subscriptions. The main content area is titled 'User Profile' and contains a table with two columns: 'Attribute' and 'Value'. The table lists various attributes and their current values, including User ID, Google Apps Email, OpenID 1.0 Identifier, Client Certificate, Given name, Surname, Email, ePass OTP token number, Yubikey ID, Yubikey PIN, Swekey ID, Swekey PIN, MSISDN identification, Password, and Retype Password. At the bottom of the table is a 'Submit' button. Below the table, there are several links for deleting or managing specific linkings: 'Delete your MSISDN linking.', 'Delete your ePass OTP linking.', 'Delete your Swekey linking.', 'Delete your Yubikey linking.', and 'View/change your public profile settings.'

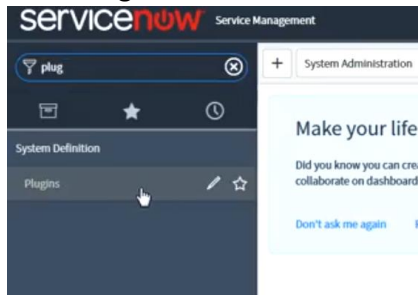
| Attribute | Value |
|----------------------------------|---|
| User ID | rohitcet |
| Google Apps Email | No longer available |
| OpenID 1.0 Identifier | http://rohitcet.ssocircle.com |
| Client Certificate | Not Enrolled |
| Given name | Papoi |
| Surname | Halder |
| Email | rohitcet@yahoo.com |
| ePass OTP token number | not assigned |
| Yubikey ID | not assigned |
| Yubikey PIN | ***** |
| Swekey ID detect | not assigned |
| Swekey PIN | ***** |
| MSISDN identification | not active |
| Password (length > 8) | |
| Retype Password | |

[Delete](#) your MSISDN linking.
[Delete](#) your ePass OTP linking.
[Delete](#) your Swekey linking.
[Delete](#) your Yubikey linking.
View/change your [public profile settings](#).

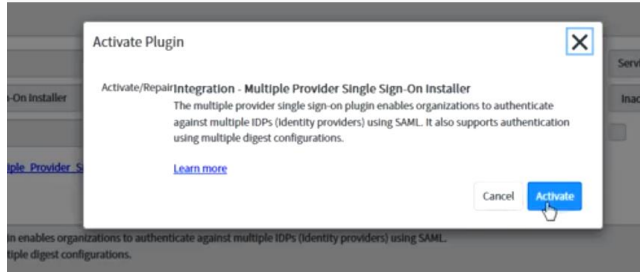
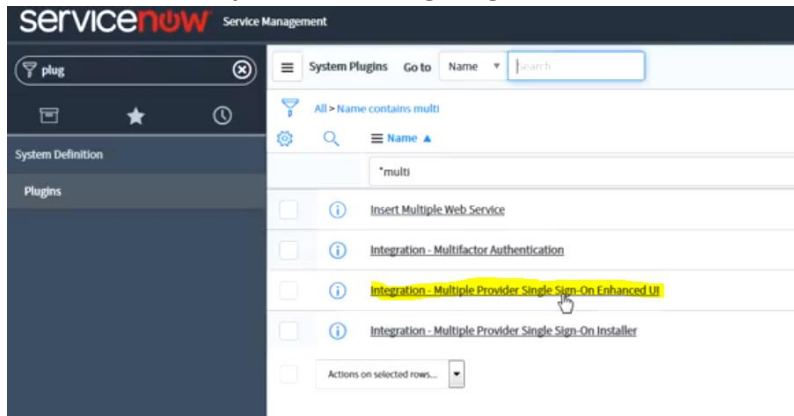
...for organizational purposes, every organization has an SSO.

Step Three: Activate the SSO Plugin:

Go to **Plugins...**

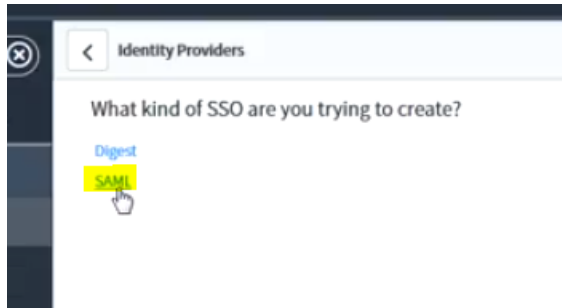
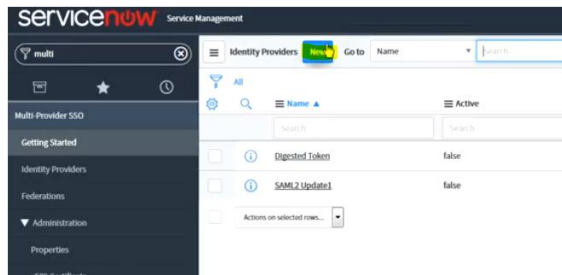
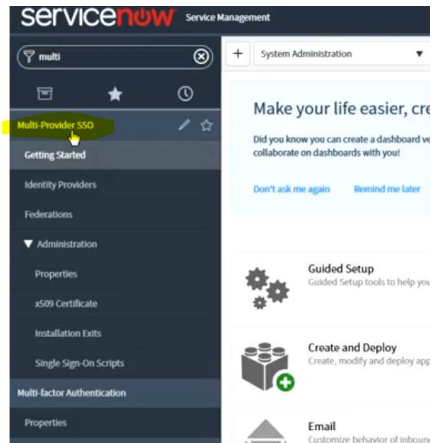


...then select **Multiple Provider Single Sign-On** and activate it...

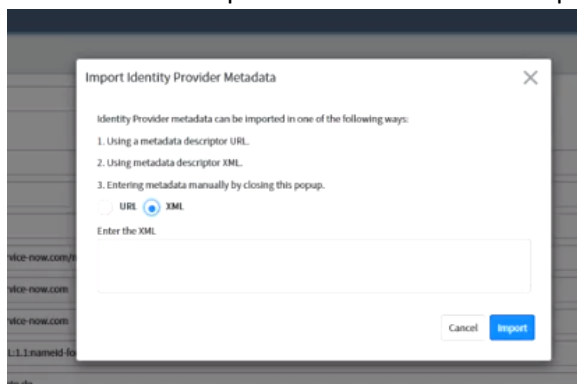


Step Four: Create a New SSO:

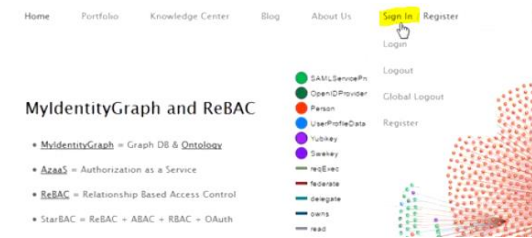
We can now see the new Module for Multi-Provider SSO...



...now we need to provide the Metadata...it is preferable to provide it via XML:



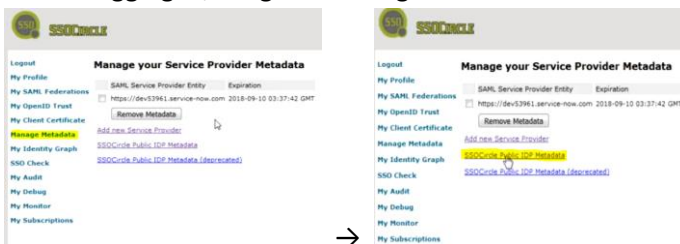
...so we need to go to SSO Circle webpage and sign in:



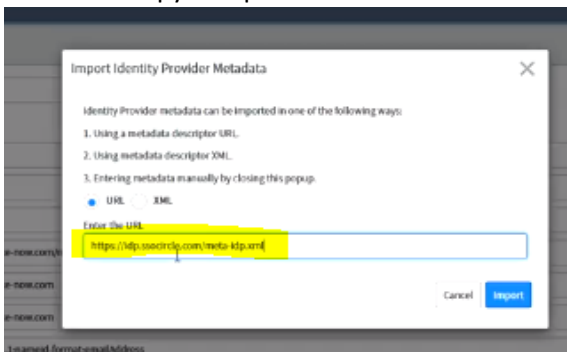
If this is for a newcomer, we can create a **New User**:



...after logging in, we go to Manage Metadata...



...we then copy and paste the URL to the Metadata...



...and the blank fields are automatically populated:

Identity Provider
https://dp.sso.oracle.com

Name: https://dp.sso.oracle.com Active: ☐

Default: ☐ Auto Redirect IDP: ☐

Identity Provider URL: https://dp.sso.oracle.com

Identity Provider's AuthnRequest: https://dp.sso.oracle.com/443/urn:oasis:names:tc:SAML:2:protocol:AuthnRequest

Identity Provider's SingleLogoutRequest: https://dp.sso.oracle.com/443/urn:oasis:names:tc:SAML:2:protocol:LogoutRequest

ServiceNow Homepage: https://dev1309.service-now.com/change.do

Entity ID / Issuer: https://dev1309.service-now.com

Audience URI: https://dev1309.service-now.com

NameID Policy: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

External Logout Redirect: external_logout_complete.do

Failed Requirement Redirect:

Encryption and Signing: ☐ Start Provisioning: ☐ Advanced: ☐

Signing/Encryption Key Alias:

Signing/Encryption Key Password: *****

Signing Signature Algorithm: http://www.w3.org/2001/04/xmldsig-core#rsa-sha256

Sign AuthnRequest: ☐


Sign LogoutRequest: ☐

Encrypt Assertion: ☐

Update: Generate Metadata: Test Connection: Activate

...then, right-click and Save.

Step Five: Add the instance:



The screenshot shows the 'SAML Service Provider Metadata Import' page in the Cisco ISE GUI. On the left is a navigation menu with options: 'Logout', 'My Profile', 'My SAML Federations', 'My OpenID Trust', 'My Client Certificate', 'Manage Metadata', 'My Identity Graph', 'SSO Check', 'My Audit', 'My Debug', 'My Monitor', and 'My Subscriptions'. The main content area has a title 'SAML Service Provider Metadata Import' and a 'User ID: robotcat' label. Below this is a 'Submit' button. A text input field contains the URL 'http://sp.cohesive.de', with a yellow box highlighting the domain 'sp.cohesive.de'. Below the input field is a checkbox labeled 'Attributes sent in assertion (optional)'. Under this checkbox are four sub-options: 'First Name', 'Last Name', 'Email Address', and 'UserID', each with an unchecked checkbox. At the bottom, there is a section titled 'Insert the SAML Metadata information of your SP' with a note that if the SP does not provide a standard SAML Metadata document, it can be built using a link.

SAML Service Provider Metadata Import

User ID: robotcat

Enter the URL of the Service Provider ex: sp.cohesive.de


☐ Attributes sent in assertion (optional)

☐ First Name
☐ Last Name
☐ Email Address
☐ UserID

Insert the SAML Metadata information of your SP
 If your SP does not provide a XML formatted SAML Metadata document, you can build it [here](#)

...as well as the url of the Metadata...

here.' The bottom of the page is redacted with a yellow box."/>

 Shibboleth

SAML Service Provider Metadata Import

Logout

My Profile

My SAML Endpoints

My SAML Trust

My Client Certificate

Manage Metadata

My Identity Graph

SSO Check

My Audit

My Debug

My Monitor

My Subscriptions

User ID: rohnket

Enter the PQDN of the ServiceProvider ex: sp.colos.de

dn:51269.service-bus.com

Attributes sent in assertion (optional)

☐ FirstName
☐ LastName
☐ EmailAddress
☐ UserID

Insert the SAML Metadata information of your SP
 If your SP does not provide a XML formatted SAML Metadata document, you can do it [here](#).

...how? Go to the instance and click **Generate Metadata**, which will open in a new tab...

[illegible]

→

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://dev53399.service-now.com/">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAuthnRequestsSig="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dev53399.service-now.com/urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dev53399.service-now.com/urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dev53399.service-now.com/urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dev53399.service-now.com/urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
  </SPSSODescriptor>
</EntityDescriptor>
```

...copy and paste it into the field:

Py Client Certificate
Manage Metadata
Py Identity Graph
SSO Check
Py Audit
Py Unlog
Py Monitor
Py Subscriptions

Enter the FQDN of the ServiceProvider ex: sp.abc.co.uk
dev31399.service-now.com

Attributes sent in assertion (optional)

☐ FirstName
☐ LastName
☐ EmailAddress
☐ UserID

Insert the SAML Metadata information of your SP
Below SP does not provide a SSO Requester SAML Metadata document, you can build a [dummy](#)

```
<?xml version='1.0' encoding='UTF-8'>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  title="sp.abc.co.uk">
  <IDPSSODescriptor AuthnRequestsSupported="false"
    WantAuthnRequestsTo="urn:oasis:names:tc:SAML:2.0:protocol">
    <SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://dev31399.service-now.com/logout.do" />
    <NameIDFormat
      uri="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://dev31399.service-now.com/logout.do" />
    <AssertionConsumerService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://dev31399.service-now.com/consumer.do" />
  </IDPSSODescriptor>
</EntityDescriptor>
```

**SSOCIRCLE**

[Logout](#)
[My Profile](#)
[My SAML Federations](#)
[My OpenID Trust](#)
[My Client Certificate](#)
[Manage Metadata](#)
[My Identity Graph](#)
[SSO Check](#)
[My Audit](#)
[My Debug](#)
[My Monitor](#)
[My Subscriptions](#)

Meta Data Import

Metadata was successfully imported

SP Expiration time: 2018-09-12 10:03:53 GMT

...then, click Submit. Metadata has now been successfully imported.

Now, if we wish, we may **Test the Connection:**

The screenshot shows the 'Identity Provider' configuration page in the Service Management console. The page is titled 'Identity Provider' with the URL 'https://idp.ssocircle.com'. It contains several sections for configuration:

- Name:** https://idp.ssocircle.com
- Default:** ☐
- Identity Provider URI:** https://idp.ssocircle.com
- Identity Provider's AuthRequest:** https://idp.ssocircle.com/43/sso/SSORedirect?metaId=public
- Identity Provider's SingleLogoutRequest:** https://idp.ssocircle.com/43/sso/SSOLogout?metaId=public
- Serviceflow Homepage:** https://dev51393.service-now.com/homepage.do
- Entity ID / Issuer:** https://dev51393.service-now.com
- Audience URI:** https://dev51393.service-now.com
- NameID Policy:** urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
- External Logout Redirect:** external_logout_complete.do
- Failed Requirement Redirect:**

Below these sections are tabs for 'EncryptionAnd Signing', 'User Provisioning', and 'Advanced'. The 'Advanced' tab is selected, showing fields for 'Signing/Encryption Key Alias', 'Signing/Encryption Key Password', and 'Encrypt Assertion'. At the bottom, there are buttons for 'Update', 'Generate Metadata', 'Test Connection' (highlighted in yellow), and 'Activate'.

...next, log in to the SSO...

The screenshot shows the SSO login page. At the top, there is a warning message: 'Additional Authentication required' and 'Microsoft Office365 SAML Authentication Bypass. Are you sure your SP is not vulnerable? Click here to get more information.' Below the warning, there is a 'User Name / Password' section with input fields for 'User Name' (containing 'johndoe') and 'Password' (masked with asterisks). A yellow box highlights the 'Log In' button. Below the login fields, there are several login options: 'Certificate Log In', 'OTP Log In', 'Swires Log In', 'SwiresPIN Log In', 'Tollfree Log In', 'Voice & Pin Log In', and 'USSDL Log In'. At the bottom, there is a note: 'In order to use Strong Authentication with Certificate Based Log In, you need to enroll a certificate with the SSO Circle CA. Read more' and a link for 'Password forgotten?'.

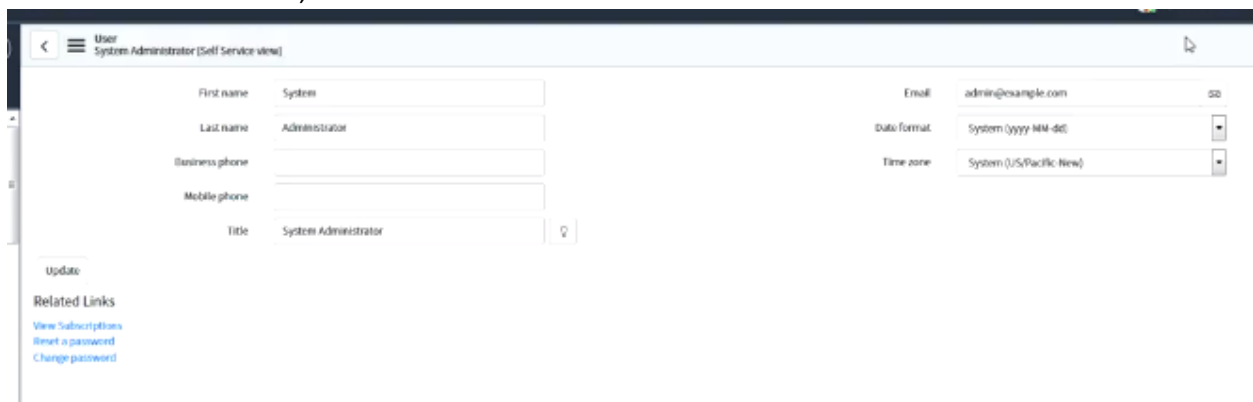
...and ensure the user profile info match between the SSO and the instance:



The screenshot shows the 'User Profile' page in an SSO interface. On the left is a navigation menu with links: Logout, My Profile, My SAML Federations, My OpenID Trust, My Client Certificate, Manage Metadata, My Identity Graph, SSO Check, My Audit, My Debug, My Monitor, and My Subscriptions. The main area is titled 'User Profile' and contains a table with 'Attribute' and 'Value' columns. The attributes listed are: User ID (rohitcet), Google Apps Email (No longer available), OpenID 1.0 Identifier (http://rohitcet.apsincle.com), Client Certificate (Not Enrolled), Given name (Pagal), Surname (Rohit), Email (rohitcet@yahoo.com), ePass OTP token number (not assigned), Yubikey ID (not assigned), Yubikey PIN (masked with asterisks), Skeykey ID (not assigned), Skeykey PIN (masked with asterisks), HGSID authentication (not active), Password (length 8), and Retype Password. A 'Submit' button is at the bottom of the form. Below the form are links to create or delete linkings for MSTRON, ePass, Skeykey, and Yubikey, and a link to view/change public profile settings.

| Attribute | Value |
|------------------------|---|
| User ID | rohitcet |
| Google Apps Email | No longer available |
| OpenID 1.0 Identifier | http://rohitcet.apsincle.com |
| Client Certificate | Not Enrolled |
| Given name | Pagal |
| Surname | Rohit |
| Email | rohitcet@yahoo.com |
| ePass OTP token number | not assigned |
| Yubikey ID | not assigned |
| Yubikey PIN | ***** |
| Skeykey ID | not assigned |
| Skeykey PIN | ***** |
| HGSID authentication | not active |
| Password (length = 8) | |
| Retype Password | |

...the first one is the SSO, and this bottom one is from the instance:

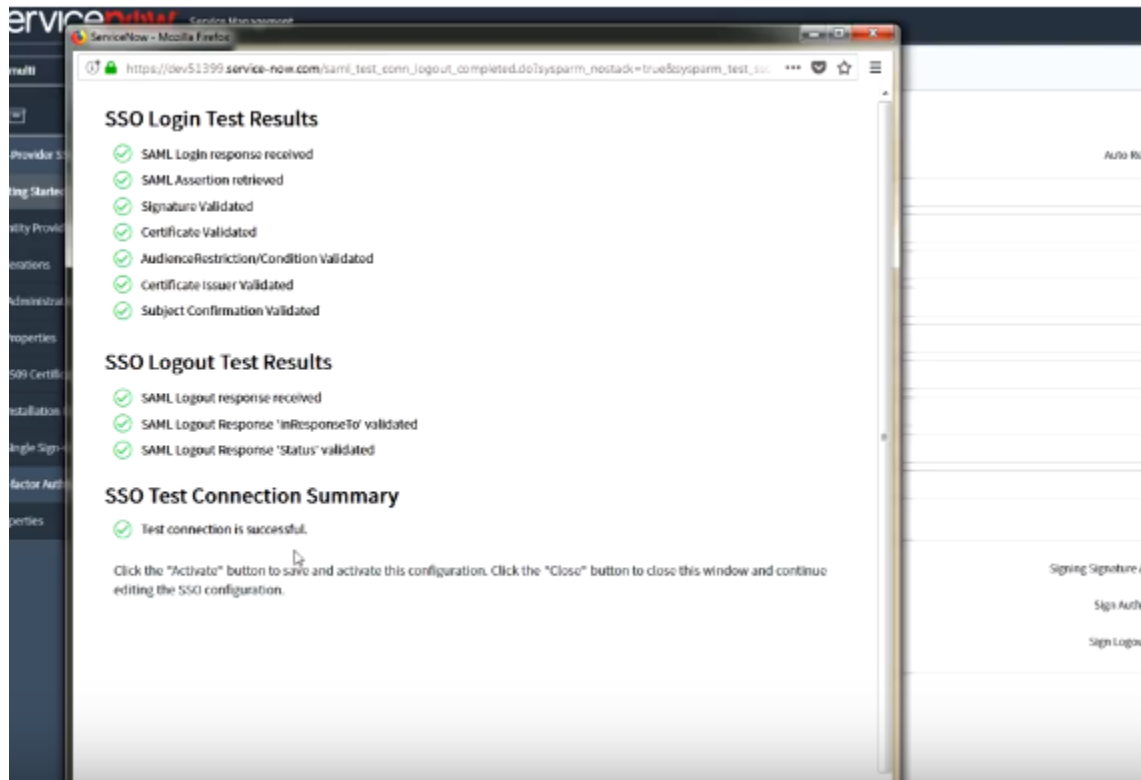


The screenshot shows the 'User Administrator (Self Service view)' page. It features a form for user details. On the left, there are fields for First name (System), Last name (Administrator), Business phone, Mobile phone, and Title (System Administrator). On the right, there are fields for Email (admin@example.com), Date format (System (yyyy-MM-dd)), and Time zone (System (US/Pacific-New)). An 'SSO' label is next to the email field. Below the form is an 'Update' button and a 'Related Links' section with links for View Subscriptions, Reset a password, and Change password.

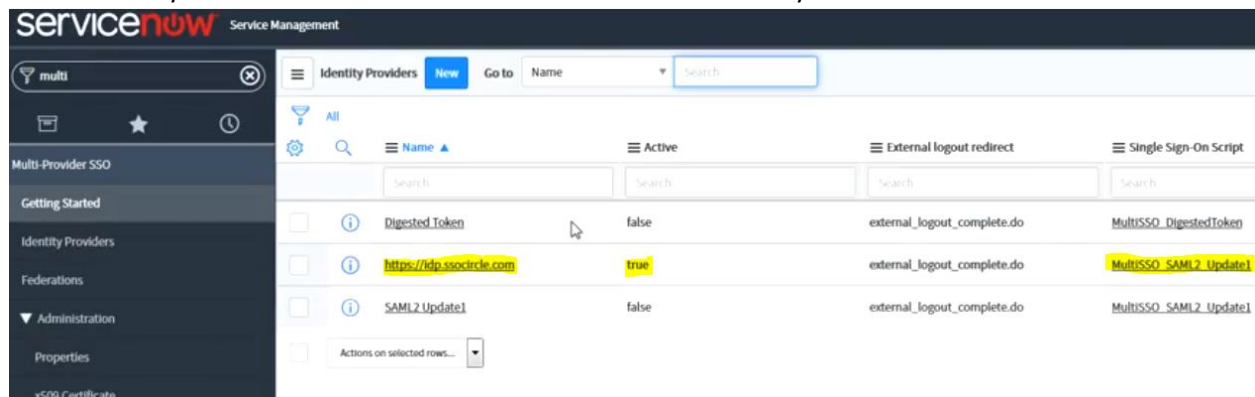
| | | | | |
|----------------|----------------------|-------------|-------------------------|-----|
| First name | System | Email | admin@example.com | SSO |
| Last name | Administrator | Date format | System (yyyy-MM-dd) | |
| Business phone | | Time zone | System (US/Pacific-New) | |
| Mobile phone | | | | |
| Title | System Administrator | | | |

...once you confirm they match, click **Test Connection** and log in to SSO again.

So now we see that the Connection was successful:



...now we may activate the Multi-Provider SSO... unless it is already active:



Step Six: Set as **Auto Redirect IdP**:

Identity Provider
https://idp.sso.circle.com

Identity Provider URL: https://idp.sso.circle.com

Identity Provider's AuthnRequest: https://idp.sso.circle.com:443/sso/SSORedirect/metaAlias/public/idp

Identity Provider's LogoutRequest: https://idp.sso.circle.com:443/sso/PSKPost/metaAlias/public/idp

ServiceNow Homepage: https://dev51399.service-now.com/homepage.do

Entity ID / Issuer: https://dev51399.service-now.com

Audience URI: https://dev51399.service-now.com

NameID Policy: urn:oasis:names:cs:SAML:1.1:nameid-format:emailAddress

External logout redirect: external_logout_complete.do

Failed Requirement Redirect:

Encryption And Signing | User Provisioning | Advanced

Signing/Encryption Key Alias:

Signing/Encryption Key Password: *****

Encrypt Assertion: ☐

Update | Generate Metadata | Test Connection | Deactivate

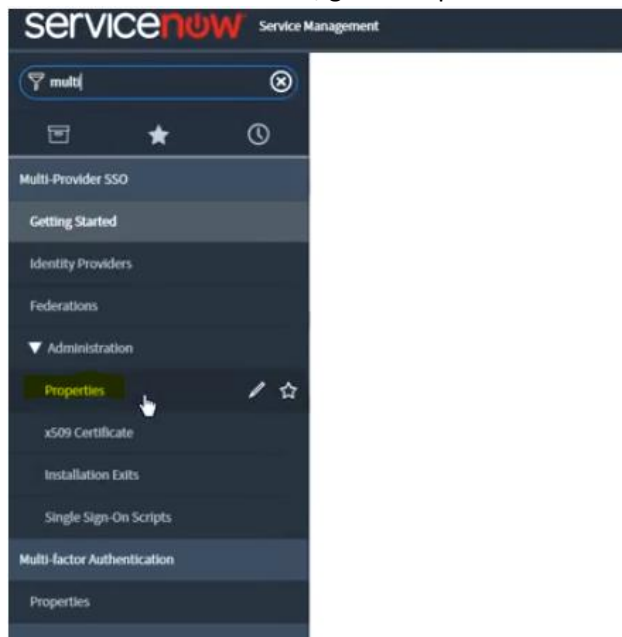
Related Links

[User Provisioning Transition Map](#)

[Set as Auto Redirect IdP](#)

X.509 Certificates | New | Edit... | Go to: X.509 certificate

Step Seven: Enable the SSO Property:
Under Multi-Provider SSO, go to Properties:



...and check **Yes** for Enable **multiple provider SSO**:

