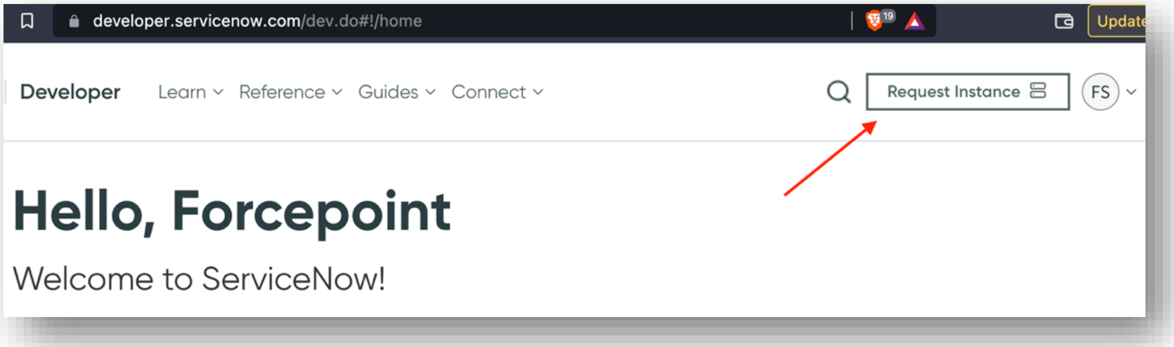
Forcepoint ONE and ServiceNow Integration Guide

Forcepoint

Forcepoint ONE Integrated with ServiceNow

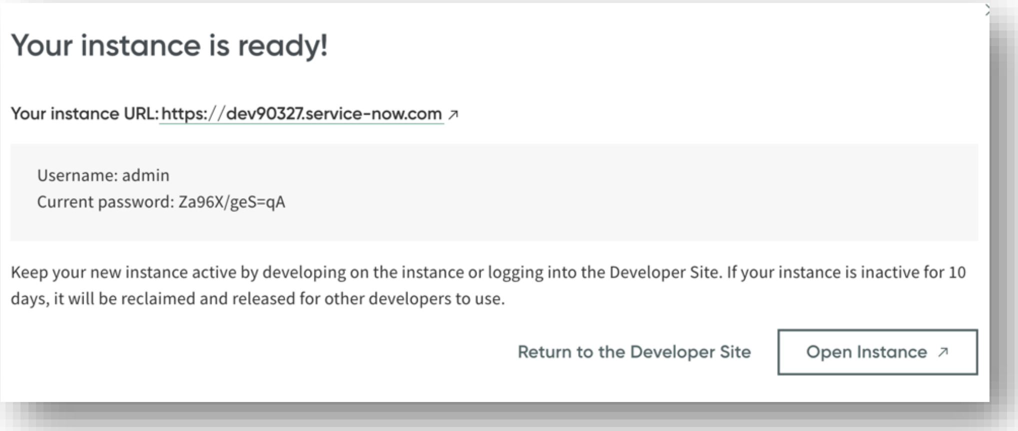
1. Go to **Manage** and click on **Instance.**
2. Then click on **Request Instance.**



Hello, Forcepoint

Welcome to ServiceNow!

3. Log in to the newly created instance using the credentials provided by ServiceNow.



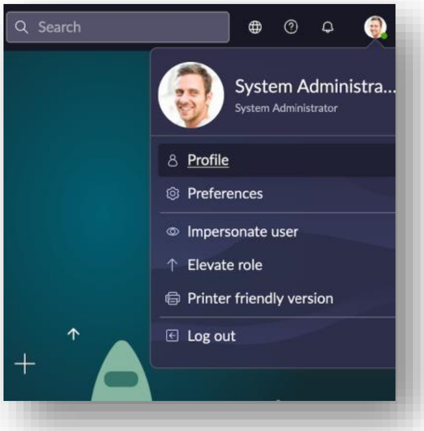
Your instance is ready!

Your instance URL: https://dev90327.service-now.com

Username: admin
Current password: Za96X/geS=qA

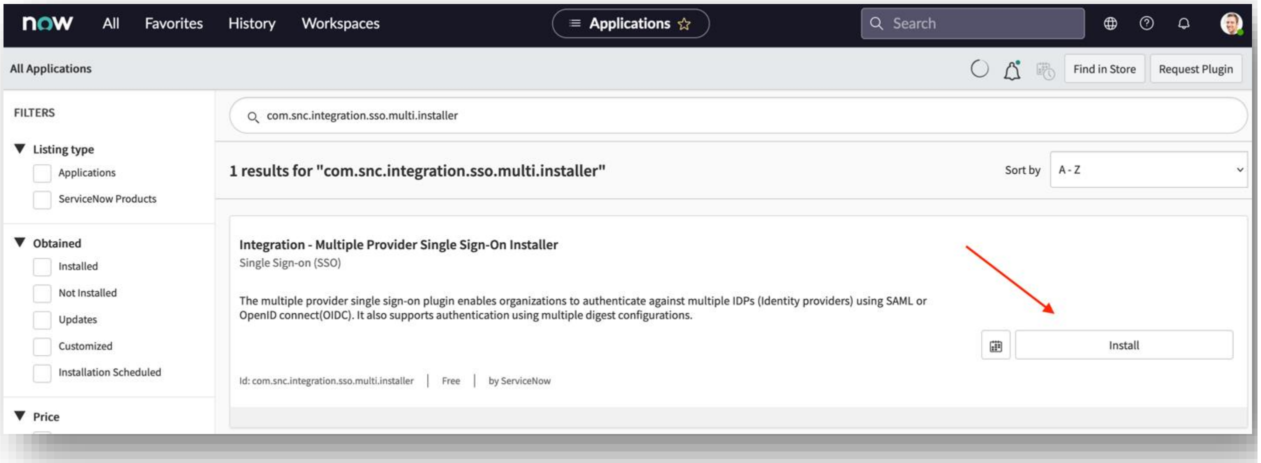
Keep your new instance active by developing on the instance or logging into the Developer Site. If your instance is inactive for 10 days, it will be reclaimed and released for other developers to use.

4. Once logged into ServiceNow, go to your Administrator profile.



5. Change your email address in your profile to the email address of your user in Forcepoint ONE (ServiceNow default is admin@example.com).

6. To use Single Sign-On (SSO) with the ServiceNow Service Portal, you must enable the integration via **All** > **Multiple Provider Single Sign-on Installer** plugin > search for “com.snc.integration.sso.multi.installer.”



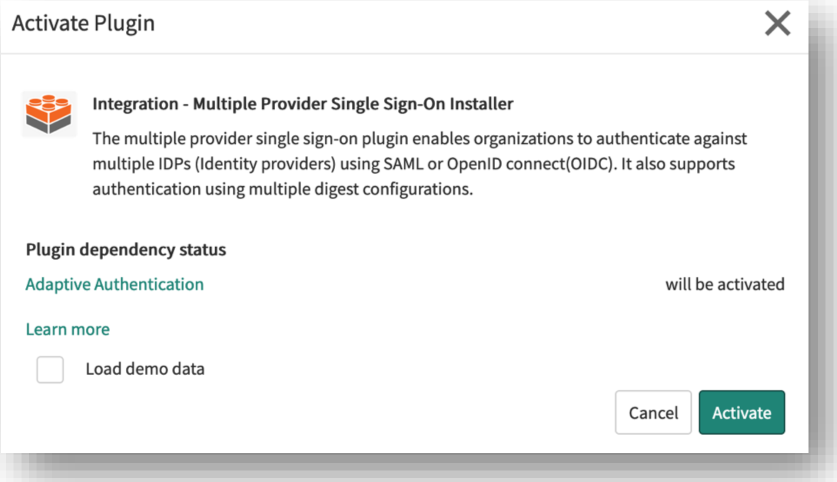
com.snc.integration.sso.multi.installer

1 results for "com.snc.integration.sso.multi.installer"

Integration - Multiple Provider Single Sign-On Installer
Single Sign-on (SSO)

The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (Identity providers) using SAML or OpenID connect(OIDC). It also supports authentication using multiple digest configurations.

Id: com.snc.integration.sso.multi.installer | Free | by ServiceNow



Integration - Multiple Provider Single Sign-On Installer

The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (Identity providers) using SAML or OpenID connect(OIDC). It also supports authentication using multiple digest configurations.

Plugin dependency status

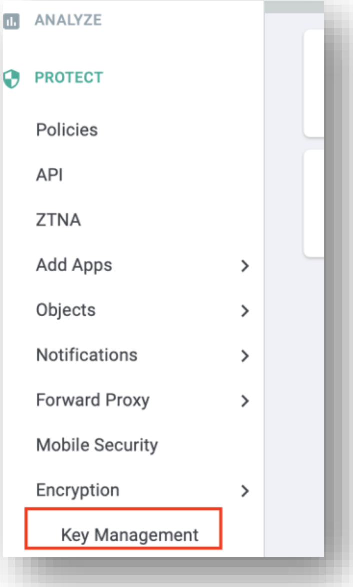
Adaptive Authentication — will be activated

Learn more

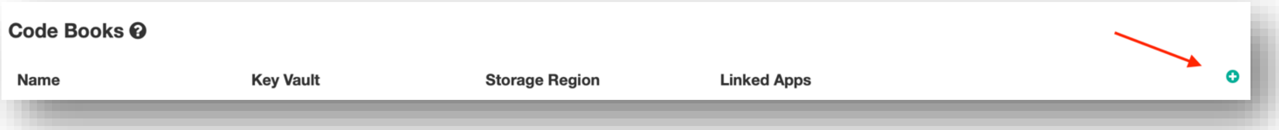
□ Load demo data

Settings in Forcepoint ONE

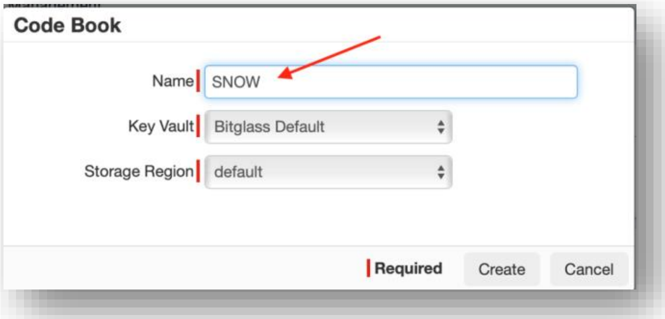
1. Log in to your Forcepoint ONE tenant with Administrator privileges. Navigate to **Protect** > **Key Management.**



2. Create a new code book by selectiong the green icon and give it a unique name.


Code Books

Name	Key Vault	Storage Region	Linked Apps

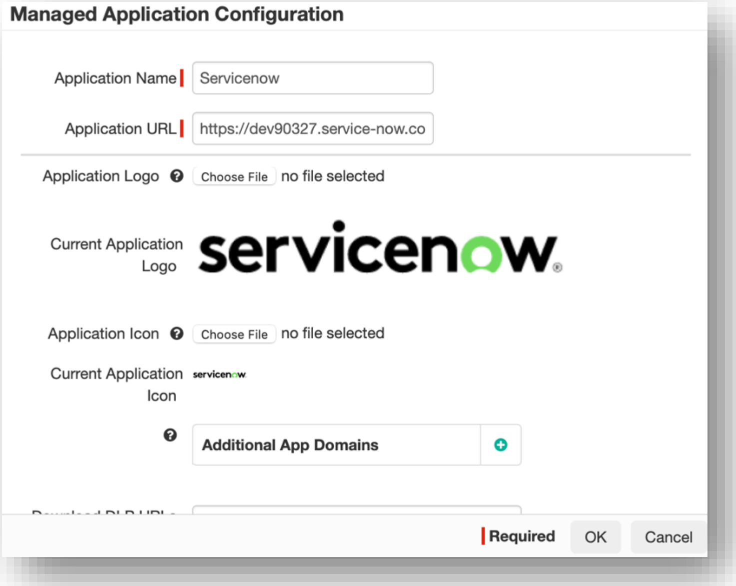

Code Book

Name: SNOW
Key Vault: Bitglass Default
Storage Region: default

3. Navigate to **Protect** > **Add Apps** > **Managed Apps**

   Select **Any Managed Application** and enter the information for the ServiceNow instance. (Note: the URL must end without any trailing characters.)

4. Press **OK** at the bottom and then **SAVE** at the top right.



Managed Application Configuration

Application Name: Servicenow

Application URL: https://dev90327.service-now.co

Application Logo: Choose File no file selected

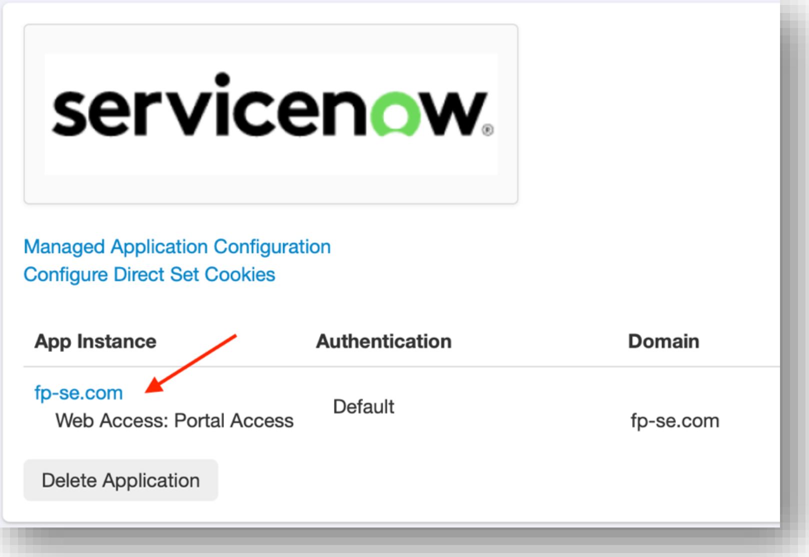
Current Application Logo

Application Icon: Choose File no file selected

Current Application Icon

Additional App Domains

5. Click on your App Instance name.



Managed Application Configuration
Configure Direct Set Cookies

App Instance	Authentication	Domain
fp-se.com Web Access: Portal Access	Default	fp-se.com

6. Here you must

   a) Add your Instance ID (Instance ID may not be available upon first configuration. Proceed without it if not shown.)

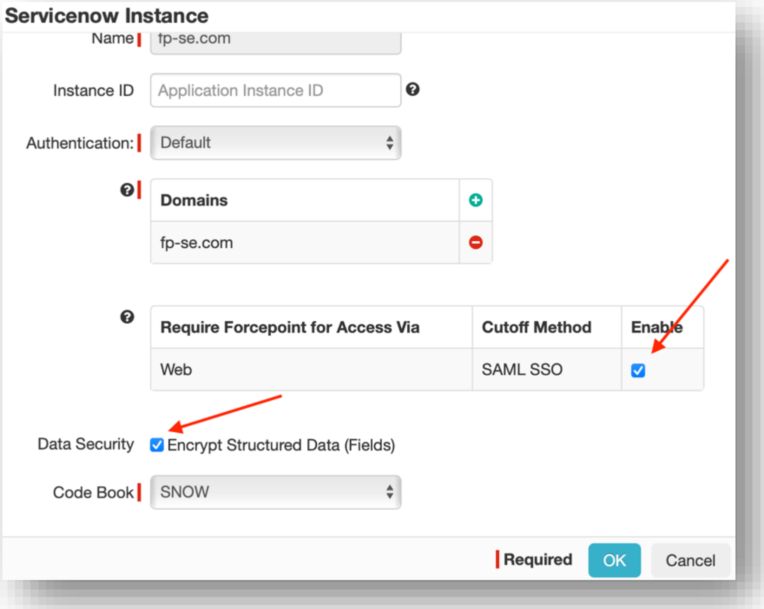
   b) Adjust the domains if needed

   c) Check the **SAML SSO** box

   d) Check the **Encrypt Structured Data** (fields) box

   e) Press **OK**

f) Then **SAVE** at the top right.



Servicenow Instance

Name: fp-se.com

Instance ID: Application Instance ID

Authentication: Default

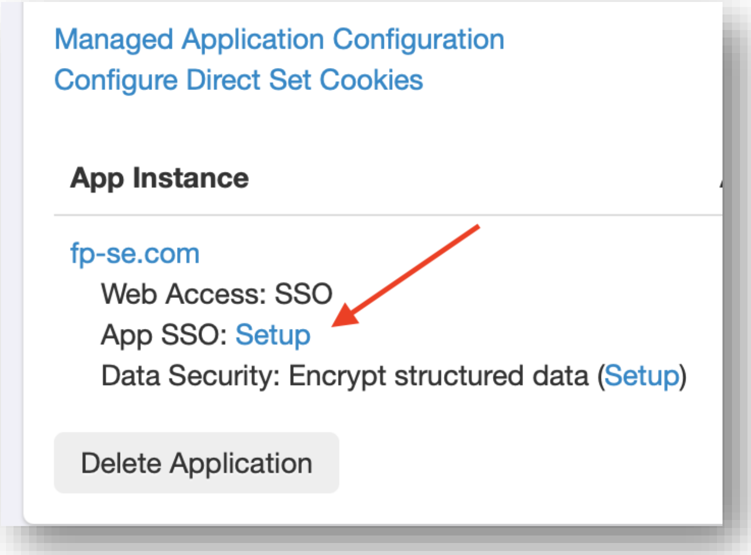
Domains
fp-se.com

Require Forcepoint for Access Via	Cutoff Method	Enable
Web	SAML SSO	☑

Data Security: ☑ Encrypt Structured Data (Fields)

Code Book: SNOW

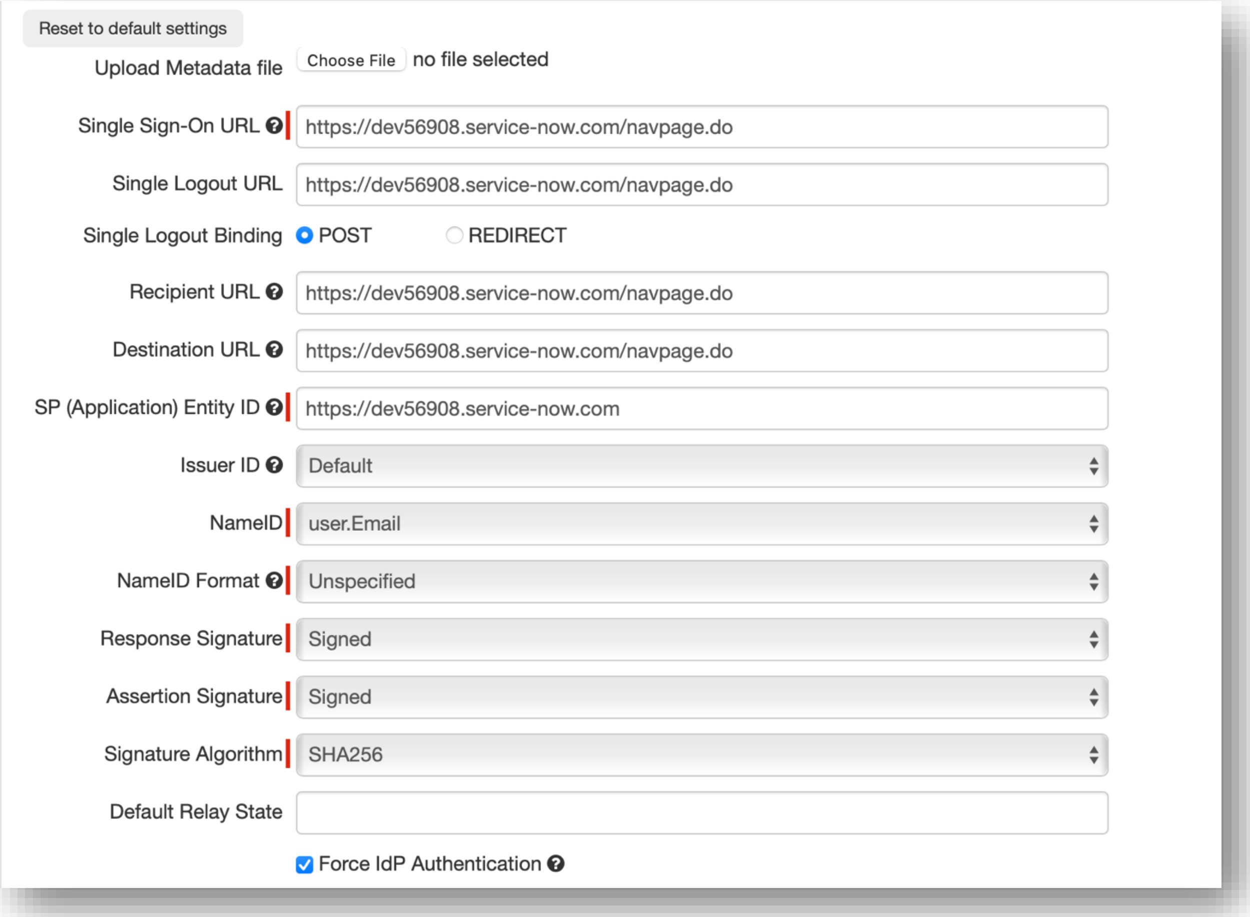
7. Navigate to **App SSO Setup**, change **Single Logout Binding** to **POST** and check the box for **Force IdP Authentication.**



Managed Application Configuration
Configure Direct Set Cookies

App Instance

fp-se.com
Web Access: SSO
App SSO: Setup
Data Security: Encrypt structured data (Setup)



Reset to default settings

Upload Metadata file: Choose File no file selected

Single Sign-On URL: https://dev56908.service-now.com/navpage.do

Single Logout URL: https://dev56908.service-now.com/navpage.do

Single Logout Binding: ● POST ○ REDIRECT

Recipient URL: https://dev56908.service-now.com/navpage.do

Destination URL: https://dev56908.service-now.com/navpage.do

SP (Application) Entity ID: https://dev56908.service-now.com

Issuer ID: Default

NameID: user.Email

NameID Format: Unspecified

Response Signature: Signed

Assertion Signature: Signed

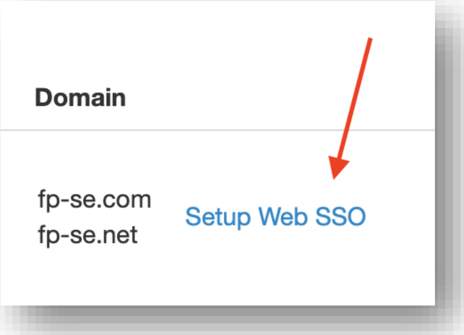
Signature Algorithm: SHA256

Default Relay State:

☑ Force IdP Authentication

8. Save.

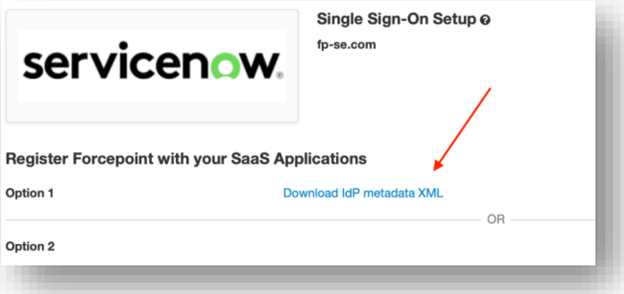
9. Go to **Setup Web SSO** and download the IdP metadata XML.



Domain

fp-se.com
fp-se.net

Setup Web SSO



Single Sign-On Setup

fp-se.com

Register Forcepoint with your SaaS Applications

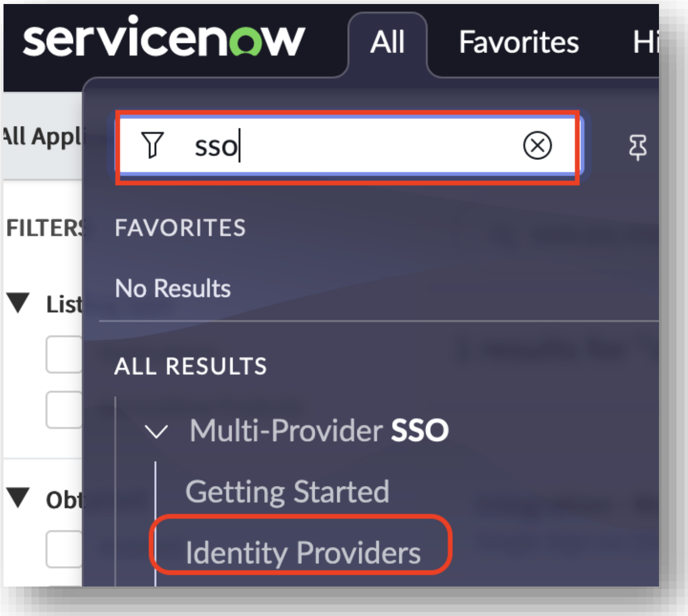
Option 1 Download IdP metadata XML

OR

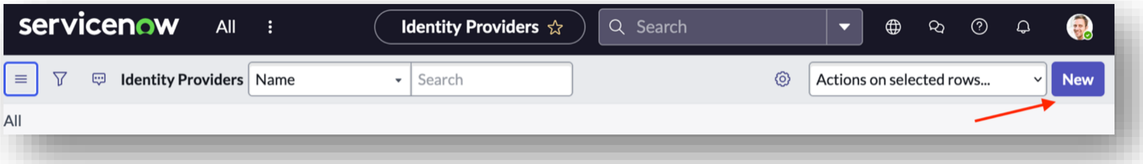
Option 2

Settings in ServiceNow

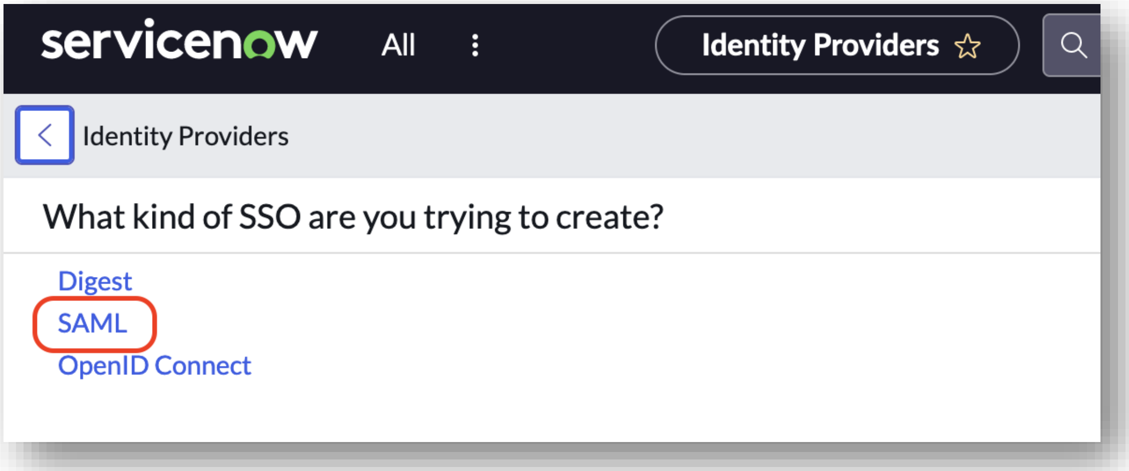
1. Search for **SSO** > **Identity Providers.**



2. Click on **New.**

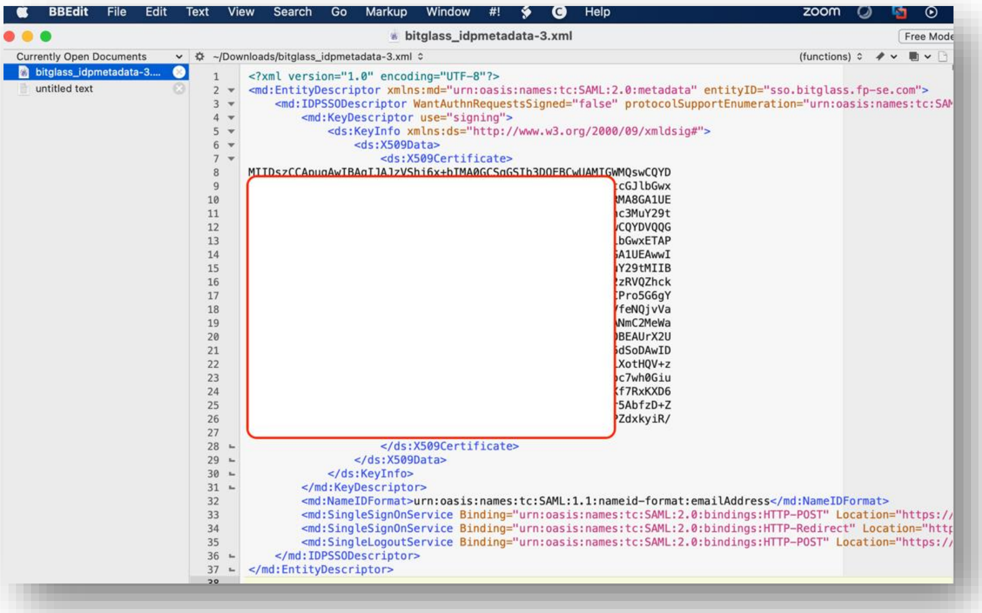


3. Choose **SAML.**

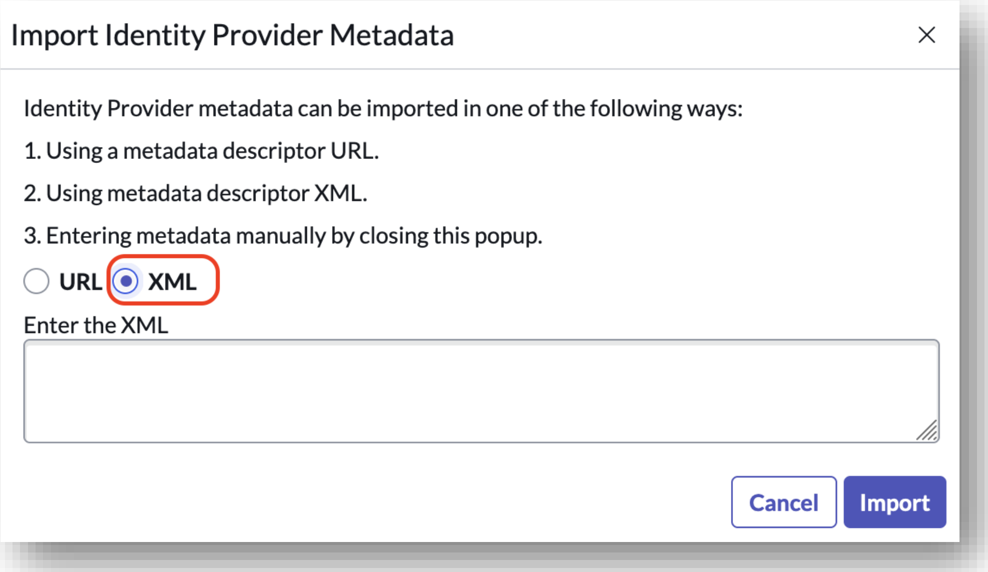


4. Choose **XML.**

5. Open the Forcepoint ONE IdP metadata.xml with an editor (BBEdit used below) and copy and paste the information into the field and press **Import.**



```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="sso.bitglass.fp-se.com">
    <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAM
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
[redacted]
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
    </md:IDPSSODescriptor>
</md:EntityDescriptor>
```



Import Identity Provider Metadata

Identity Provider metadata can be imported in one of the following ways:

1. Using a metadata descriptor URL.

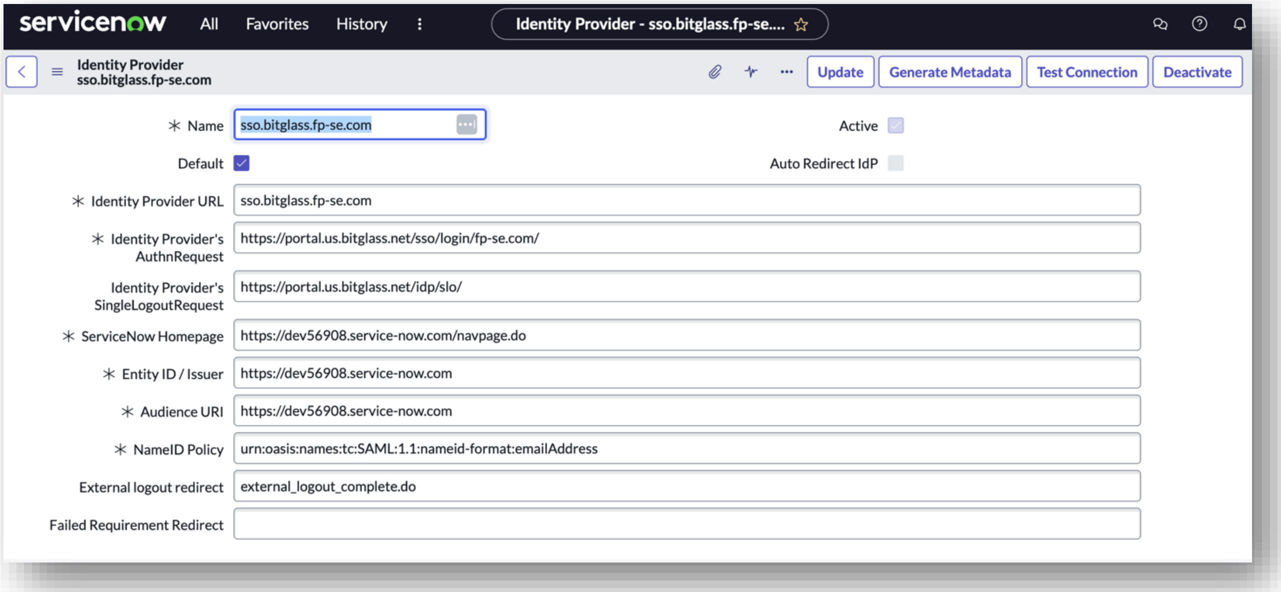
2. Using metadata descriptor XML.

3. Entering metadata manually by closing this popup.

○ URL ● XML

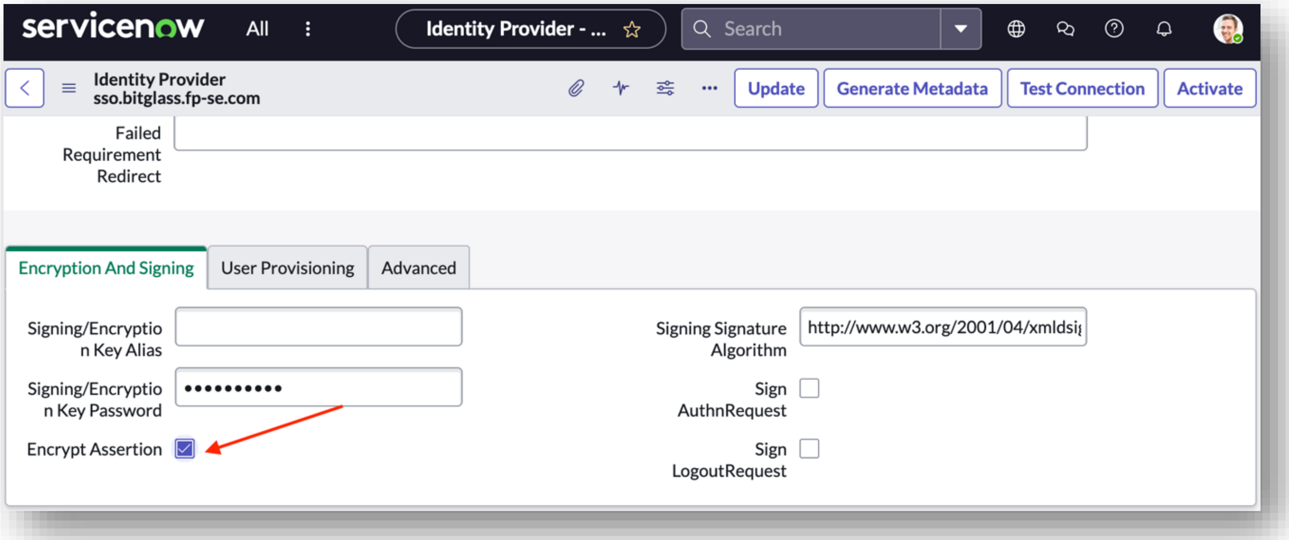
Enter the XML

6. Adjust the settings as shown below.



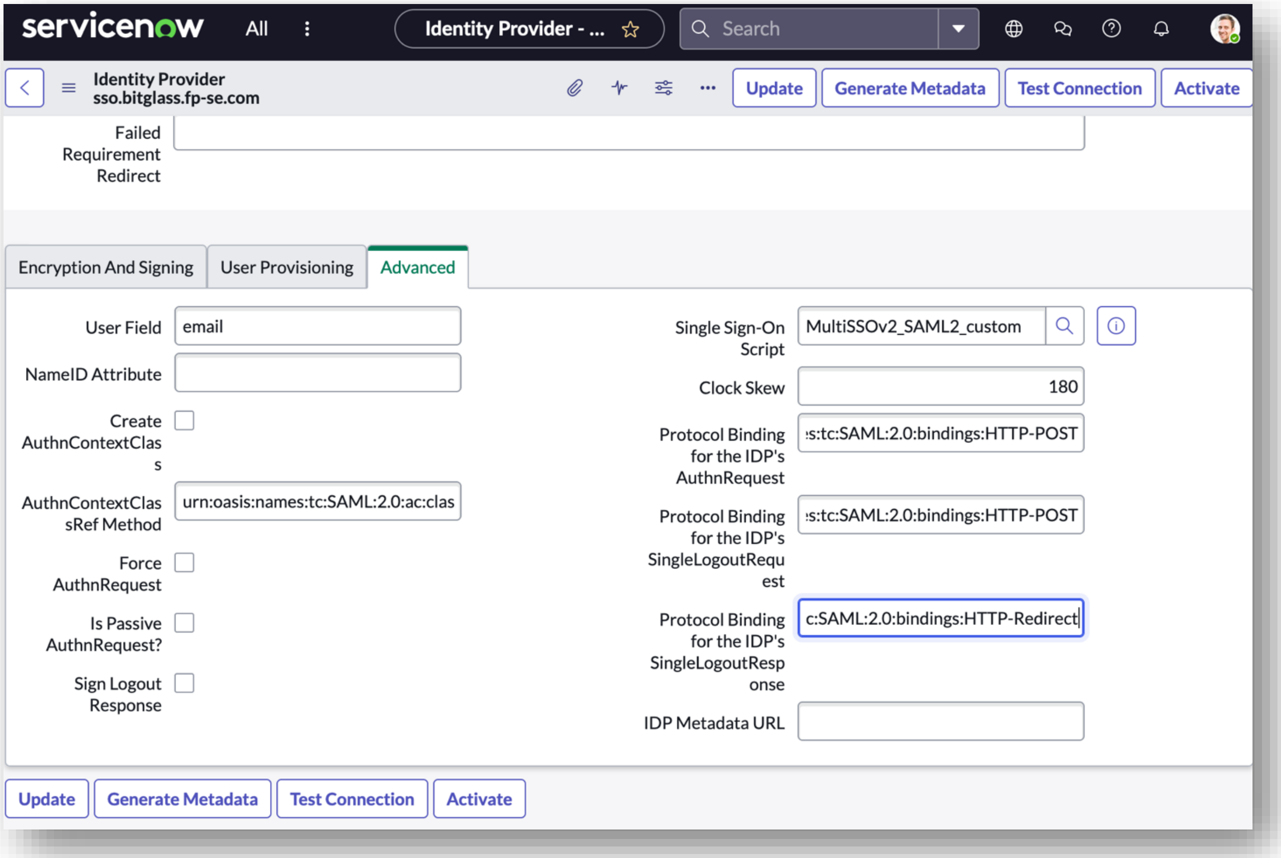
Identity Provider
sso.bitglass.fp-se.com

∗ Name	sso.bitglass.fp-se.com
Active	☑
Default	☑
Auto Redirect IdP	□
∗ Identity Provider URL	sso.bitglass.fp-se.com
∗ Identity Provider's AuthnRequest	https://portal.us.bitglass.net/sso/login/fp-se.com/
Identity Provider's SingleLogoutRequest	https://portal.us.bitglass.net/idp/slo/
∗ ServiceNow Homepage	https://dev56908.service-now.com/navpage.do
∗ Entity ID / Issuer	https://dev56908.service-now.com
∗ Audience URI	https://dev56908.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	



Identity Provider
sso.bitglass.fp-se.com

Failed Requirement Redirect	
Signing/Encryption Key Alias	
Signing/Encryption Key Password	••••••••••
Encrypt Assertion	☑
Signing Signature Algorithm	http://www.w3.org/2001/04/xmldsi
Sign AuthnRequest	□
Sign LogoutRequest	□



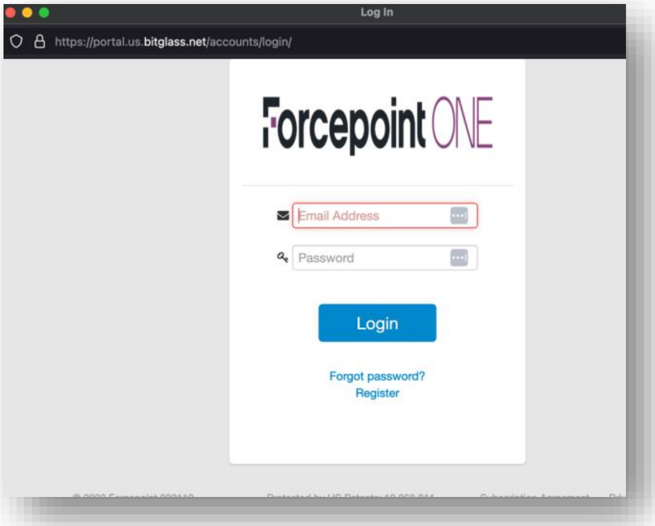
Failed Requirement Redirect

User Field	email
NameID Attribute	
Create AuthnContextClass	□
AuthnContextClassRef Method	urn:oasis:names:tc:SAML:2.0:ac:clas
Force AuthnRequest	□
Is Passive AuthnRequest?	□
Sign Logout Response	□
Single Sign-On Script	MultiSSOv2_SAML2_custom
Clock Skew	180
Protocol Binding for the IDP's AuthnRequest	:s:tc:SAML:2.0:bindings:HTTP-POST
Protocol Binding for the IDP's SingleLogoutRequest	:s:tc:SAML:2.0:bindings:HTTP-POST
Protocol Binding for the IDP's SingleLogoutResponse	c:SAML:2.0:bindings:HTTP-Redirect
IDP Metadata URL	

7. Test the connection (it can’t be activated unless tested successfully).

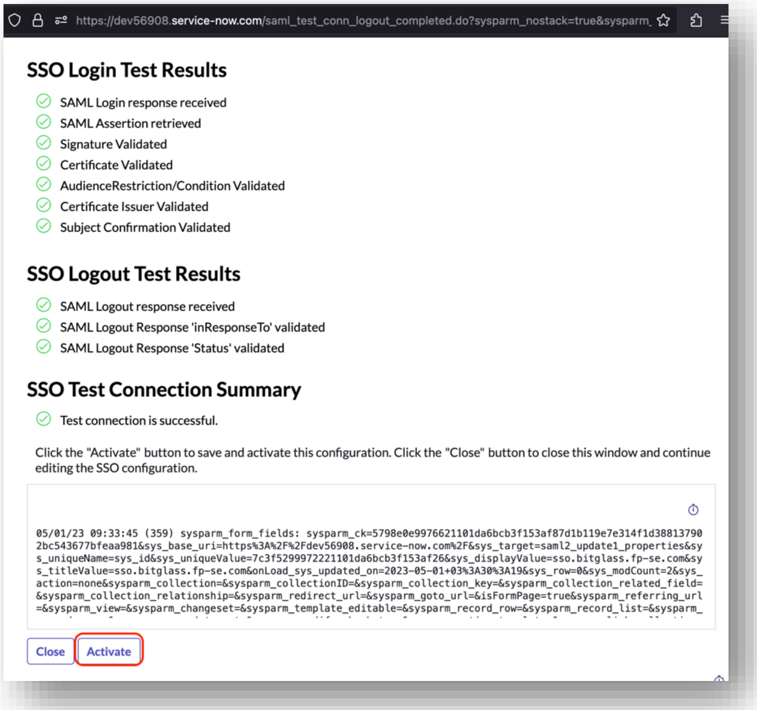
Note: The test connection must be done with Direct App Access in Forcepoint ONE Policies and using the Admin that is of the federated domain and exists in Forcepoint ONE and ServiceNow.

8. Traffic will be redirected to the Forcepoint portal. Use your credentials to log in.



A successful test should look like this.

9. Click **Activate.**



https://dev56908.service-now.com/saml_test_conn_logout_completed.do?sysparm_nostack=true&sysparm_

SSO Login Test Results

- ✓ SAML Login response received
- ✓ SAML Assertion retrieved
- ✓ Signature Validated
- ✓ Certificate Validated
- ✓ AudienceRestriction/Condition Validated
- ✓ Certificate Issuer Validated
- ✓ Subject Confirmation Validated

SSO Logout Test Results

- ✓ SAML Logout response received
- ✓ SAML Logout Response 'inResponseTo' validated
- ✓ SAML Logout Response 'Status' validated

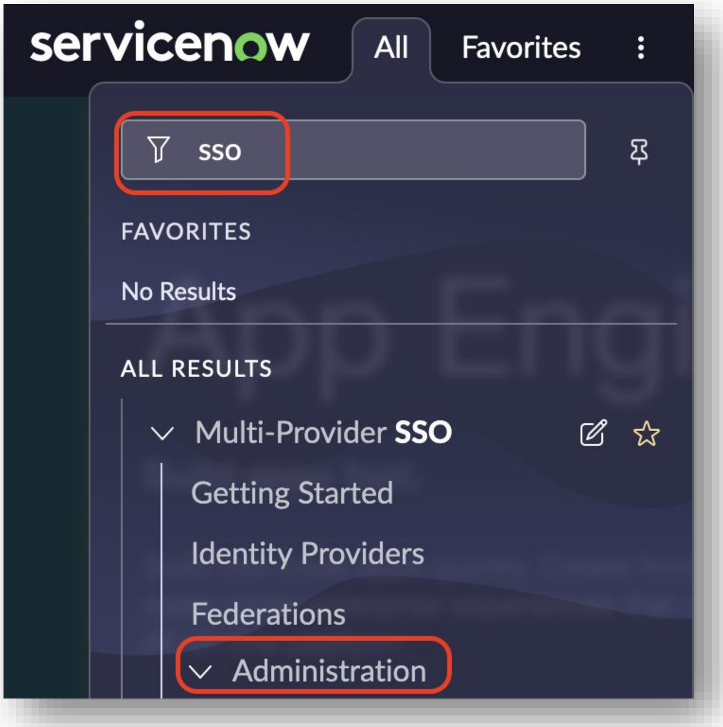
SSO Test Connection Summary

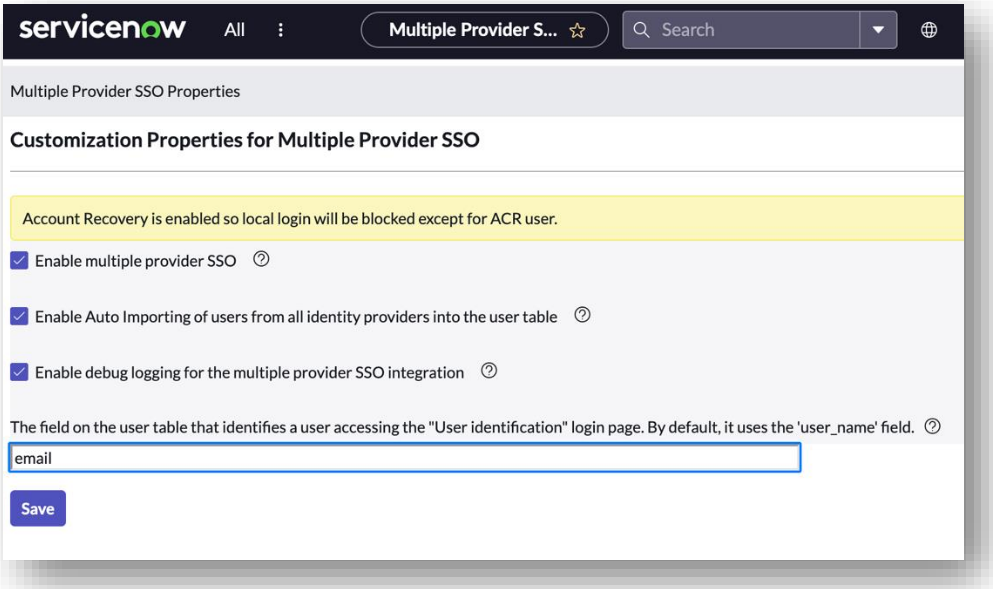
- ✓ Test connection is successful.

Click the "Activate" button to save and activate this configuration. Click the "Close" button to close this window and continue editing the SSO configuration.

```
05/01/23 09:33:45 (359) sysparm_form_fields: sysparm_ck=5798e0e9976621101da6bcb3f153af87d1b119e7e314f1d38813790
2bc543677bfeaa981&sys_base_uri=https%3A%2F%2Fdev56908.service-now.com%2F&sys_target=saml2_update1_properties&sy
s_uniqueName=sys_id&sys_uniqueValue=7c3f5299972221101da6bcb3f153af26&sys_displayValue=sso.bitglass.fp-se.com&sy
s_titleValue=sso.bitglass.fp-se.com&onLoad_sys_updated_on=2023-05-01+03%3A30%3A19&sys_row=0&sys_modCount=2&sys_
action=none&sysparm_collection=&sysparm_collectionID=&sysparm_collection_key=&sysparm_collection_related_field=
&sysparm_collection_relationship=&sysparm_redirect_url=&sysparm_goto_url=&isFormPage=true&sysparm_referring_url
=&sysparm_view=&sysparm_changeset=&sysparm_template_editable=&sysparm_record_row=&sysparm_record_list=&sysparm_
```

10. Now go to **Multi Provider SSO** > **Administration** > **Properties** and check all three boxes with **Yes**, then change the field for **User Identification** to **Email.**





Multiple Provider SSO Properties

Customization Properties for Multiple Provider SSO

Account Recovery is enabled so local login will be blocked except for ACR user.

☑ Enable multiple provider SSO

☑ Enable Auto Importing of users from all identity providers into the user table

☑ Enable debug logging for the multiple provider SSO integration

The field on the user table that identifies a user accessing the "User identification" login page. By default, it uses the 'user_name' field.

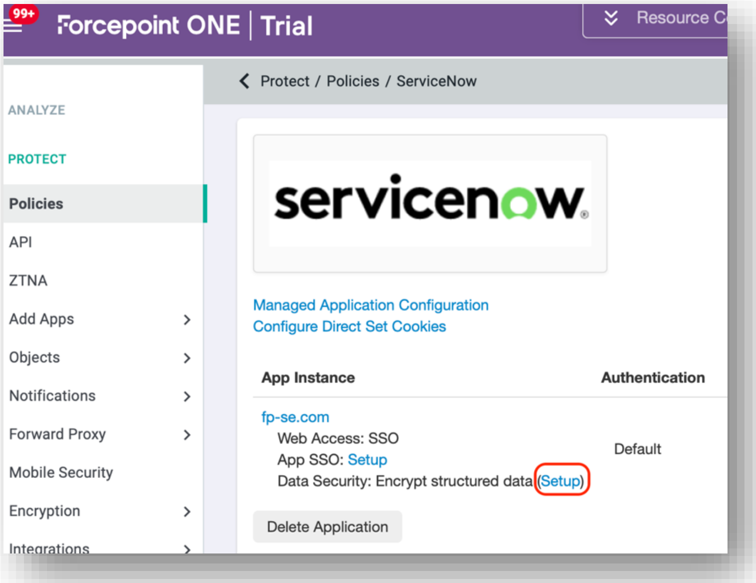
email

Save

11. Save your settings.
12. Test logins via Portal and via direct link (dev####.service-now.com).
13. This marks the end of the configuration process for SSO integration of Forcepoint ONE and ServiceNow.

Part II – Setting Up Data Sequestration

1. Go to **Apps > Policies** and click your **ServiceNow** icon > **Encrypt Structured Data Setup.**

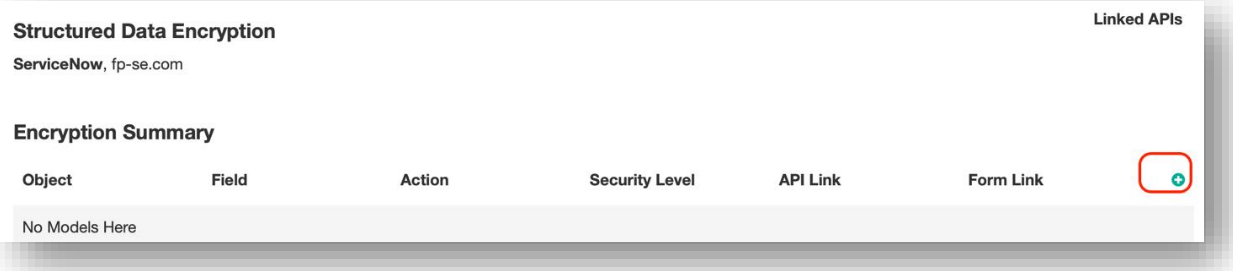


Protect / Policies / ServiceNow

Managed Application Configuration
Configure Direct Set Cookies

App Instance	Authentication
fp-se.com Web Access: SSO App SSO: Setup Data Security: Encrypt structured data (Setup)	Default

2. Start by adding a new Object.



Structured Data Encryption

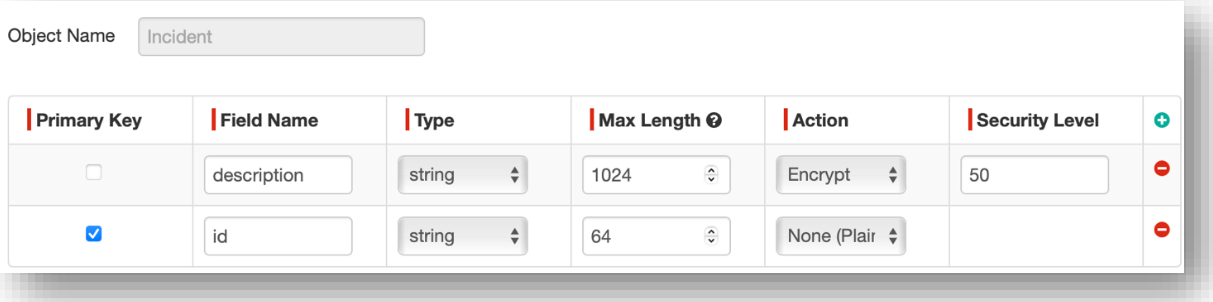
ServiceNow, fp-se.com

Linked APIs

Encryption Summary

Object	Field	Action	Security Level	API Link	Form Link
No Models Here					

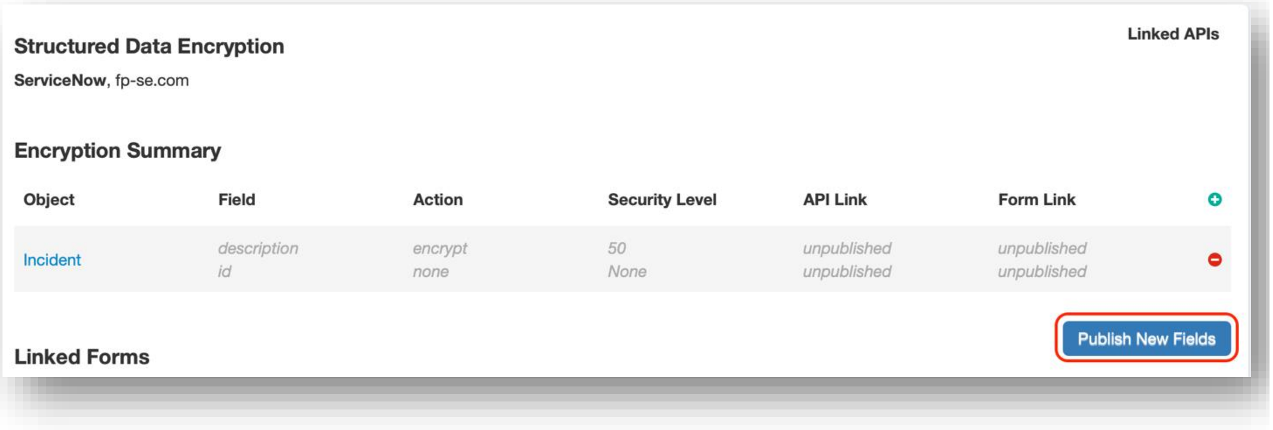
3. Provide an **Object Name** and add the **Field Name** required and set Type/Max Length/Action and Security Level accordingly. Create a field named “description/comments/id.” All will be strings, and the max length for description and comments is 1024 and 64 for ID. The action is **Encrypt** for description and comments and **None** for ID. Set the ID as the Primary Key for this case; we won’t use the Security Level and randomly chose to set its value to 50.



Object Name: Incident

Primary Key	Field Name	Type	Max Length	Action	Security Level
□	description	string	1024	Encrypt	50
☑	id	string	64	None (Plair	

4. Press **Save**.
5. After saving your Object, publish the new fields.



Structured Data Encryption

ServiceNow, fp-se.com

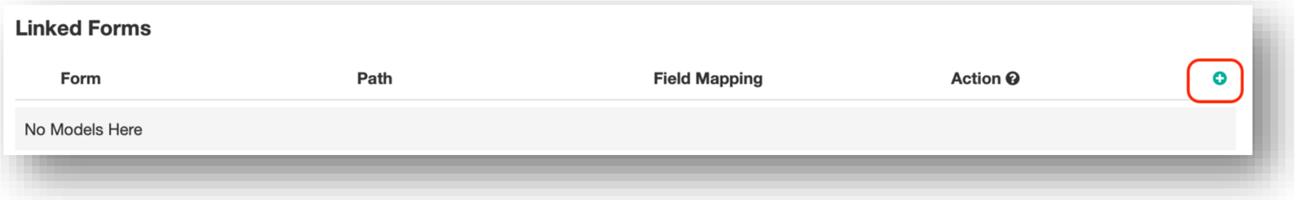
Linked APIs

Encryption Summary

Object	Field	Action	Security Level	API Link	Form Link	⊕
Incident	*description* *id*	*encrypt* *none*	*50* *None*	*unpublished* *unpublished*	*unpublished* *unpublished*	⊖

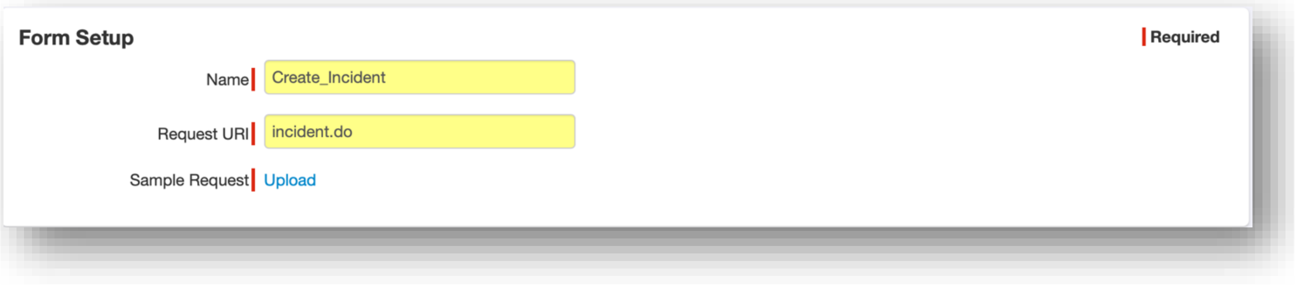
Linked Forms

6. Add Linked Forms to the encryption Object we just defined by pressing the **Plus** icon defining its Name (no spaces or special characters allowed) and Request URI.



Linked Forms

Form	Path	Field Mapping	Action ❓	⊕
No Models Here				



Form Setup

| Required

Name | Create_Incident

Request URI | incident.do

Sample Request | Upload

7. To find out the field name and URI for forms you want to protect, go to ServiceNow and fill in the corresponding form (in this case incident.do) with values that are easy to recognize. Open your browser debugger (Ctrl+Shift+E in FF, Ctrl-Shift-I in Chrome). Submit the filled-in form and search for the post of the corresponding form in the Network area.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP ONE and ServiceNow Integration Guide] 10Oct2023