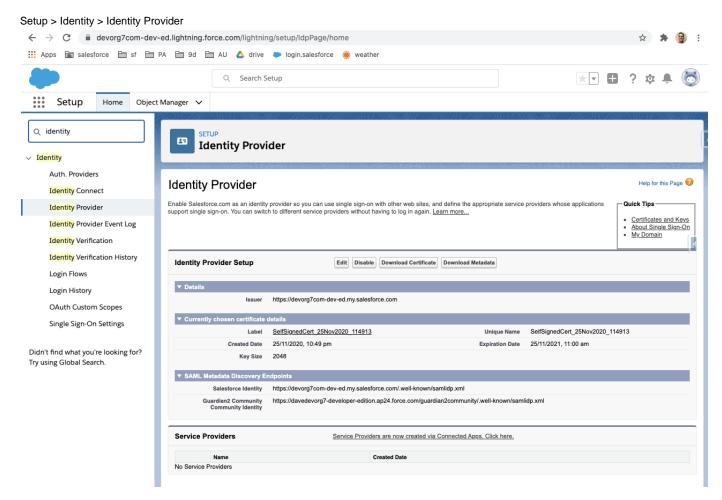
# Communities SSO Setup

- · Configure the Identity Provider in the Identity Provider org
- Download the Identity Provider Certificate
- Configure the Connected App in the Identity Provider org
- Assign the Connected App to the Customer Community Profiles
- Download the Connected App Metadata
- · Add the Identity Provider domain as a Remote Site in the Service Provider org
- Add the SSO button to the SP Community
- Allow System Administrator user to login to the Community
- Set User Federation Id
- Test an IdP-Initiated SSO
- Test an SP-Initiated SSO

## Configure the Identity Provider in the Identity Provider org

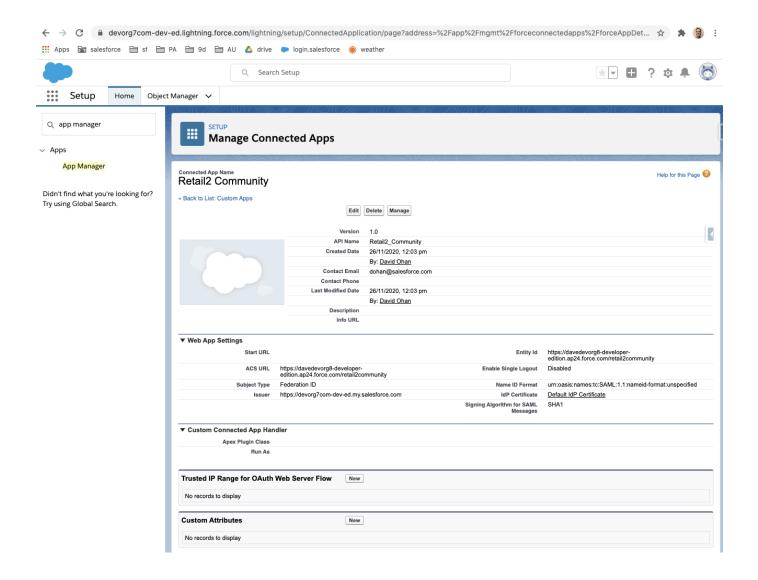


### Download the Identity Provider Certificate

Click Download Certificate and save the certificate file. This will be used in the Single Sign-On Settings in the Service Provider org.

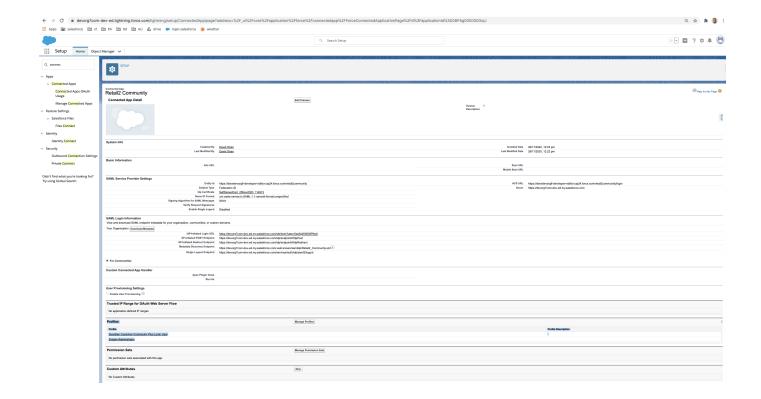
# Configure the Connected App in the Identity Provider org

Setup > Apps > App Manager > New Connected App



Assign the Connected App to the Customer Community Profiles

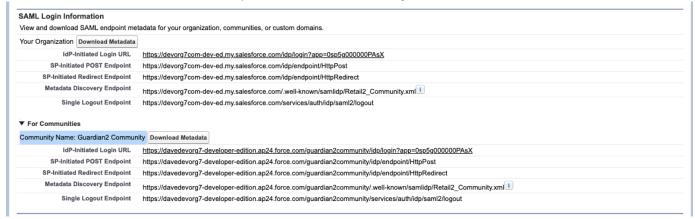
Setup > Apps > Connected Apps > Manage Connected Apps



# Download the Connected App Metadata

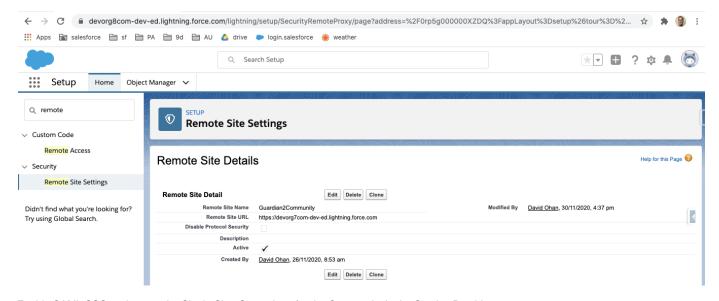
Setup > Apps > Connected Apps > Manage Connected Apps > SAML Login Information > For Communities

Note: Download the Metadata from the Community that is the IdP, not from Your Organisation



Add the Identity Provider domain as a Remote Site in the Service Provider org

Setup > Security > Remote Site Settings



Enable SAML SSO and create the Single Sign On settings for the Community in the Service Provider org:

Setup > Identity > Single Sign-On Settings > New from Metadata File. Upload the Metadata XML file that was downloaded from the Connected App in the Identity Provider org.

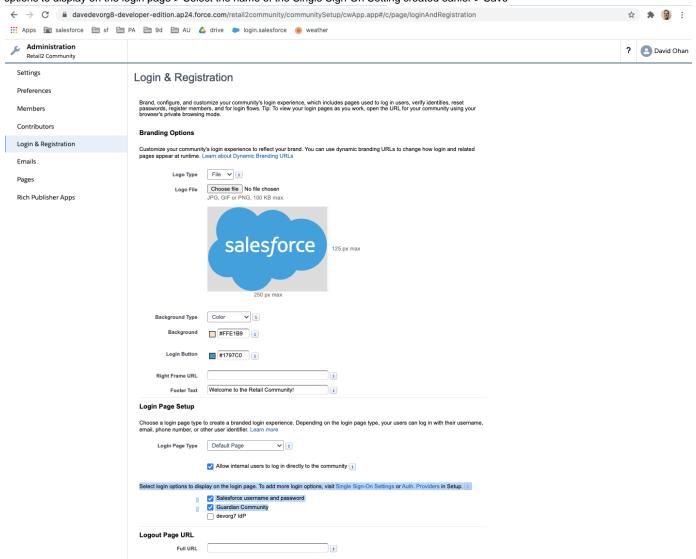
In the Identity Provider Certificate field, upload the certificate that was downloaded from the Identity Provider. ☆ 🗯 📵 : ## Apps alesforce sf PA 9d AU A drive | login.salesforce | weather \* P 🖪 ? 🌣 🗕 🐻 Q Search Setup Setup Home Object Manager 🗸 Q single Single Sign-On Settings √ Identity Single Sign-On Settings SAML Single Sign-On Settings Help for this Page Back to Single Sign-On Settings Didn't find what you're looking for? Try using Global Search. Edit Delete Clone Download Metadata SAML Assertion Validator 4 Guardian Community API Name devorg7\_Guardian\_Community SAML Version 2.0 Issuer https://devorg7com-dev-ed.my.salesforce.com Entity ID https://davedevorg8-developer-edition.ap24.force.com/retail2community Identity Provider Certificate  $C=USA, ST=CA, L=San\ Francisco,\ O=Sales force.com,\ OU=00D5g0000001tNB,\ CN=SelfSignedCert\_25Nov2020\_114913\ Expiration:\ 25\ Nov\ 2021\ 00:00:00\ GMT$ Request Signing Certificate SelfSignedCert\_25Nov2020\_211938 Request Signature Method RSA-SHA256 Assertion Decryption Certificate Assertion not encrypted SAML Identity Type Federation ID SAML Identity Location Subject Service Provider Initiated Request Binding HTTP Redirect Identity Provider Login URL https://davedevorg7-developer-edition.ap 24. force.com/guardian 2 community/idp/endpoint/HttpRedirect.pdf. and the properties of theCustom Logout URL Custom Error URL Single Logout Enabled Just-in-time User Provisioning User Provisioning Enabled Endpoints View SAML endpoints for your organization, communities, or custom domains Your Organization Login URL https://devorg8com-dev-ed.my.salesforce.com Logout URL https://devorg8com-dev-ed.my.salesforce.com/services/auth/sp/saml2/logou OAuth 2.0 Token Endpoint https://devorg8com-dev-ed.my.salesforce.com/services/oauth2/token **▼** For Communities Community Name: Retail LoginDiscovery Login URL https://davedevorg8-developer-edition.ap24.force.com/retaillogindiscovery/login Logout URL https://davedevorg8-developer-edition.ap24.force.com/retaillogindiscovery/service Community Name: Retail2 Community Login URL https://davedevorg8-developer-edition.ap24.force.com/retail2community/login https://davedevorg8-developer-edition.ap24.force.com/retail2community/services/auth/sp/saml2/logout Edit Delete Clone Download Metadata SAML Assertion Validator

Ensure that the following match:

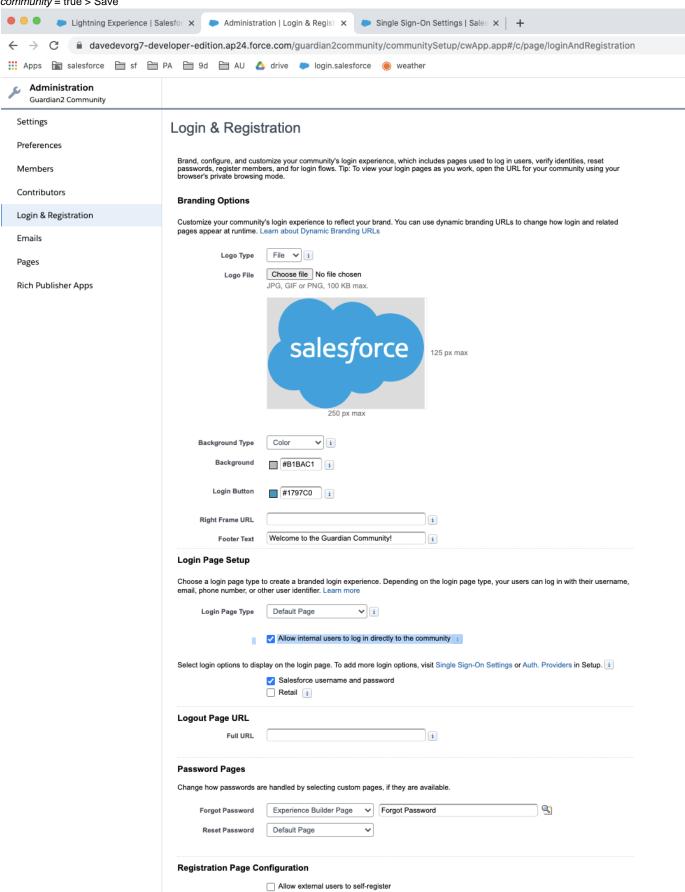
Identity Provider Connected App	Service Provider Single Sign-On Settings
Entity Id	Entity ID
ACS URL	Endpoints > For Communities > SP Community Name > Login URL
Issuer	Issuer
Subject Type = Federation ID	SAML Identity Type = Federation ID
Service Provider Initiated Request Binding = HTTP Redirect	
SAML Login Information > For Communities > SP Community Name > SP-Initiated Redirect Endpoint	Identity Provider Login URL

### Add the SSO button to the SP Community

In the Service Provider org, go to Community Experience Builder > Administration > Login & Registration > Login Page Setup > Select login options to display on the login page > Select the name of the Single Sign-On Setting created earlier > Save



In both orgs, go to the Community Experience Builder > Administration > Login & Registration > Set Allow internal users to log in directly to the community = true > Save

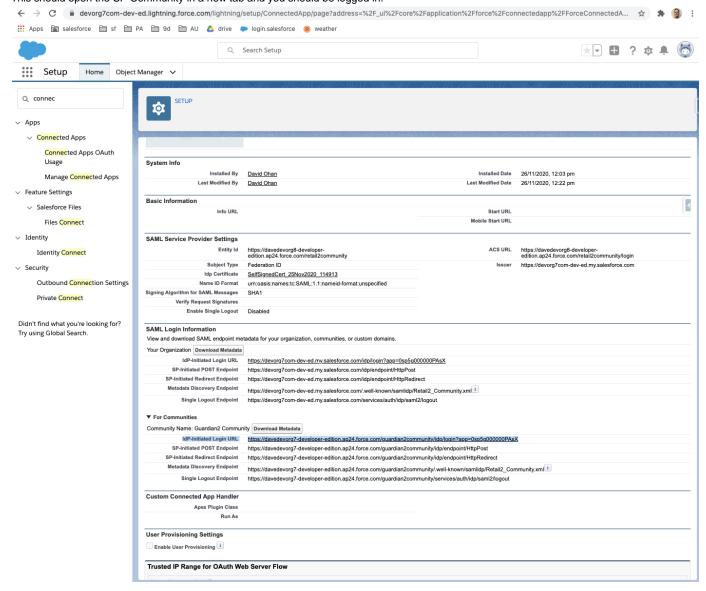


#### Set User Federation Id

For SSO to work between orgs/Communities, the User's Federation Id must match in both orgs.

### Test an IdP-Initiated SSO

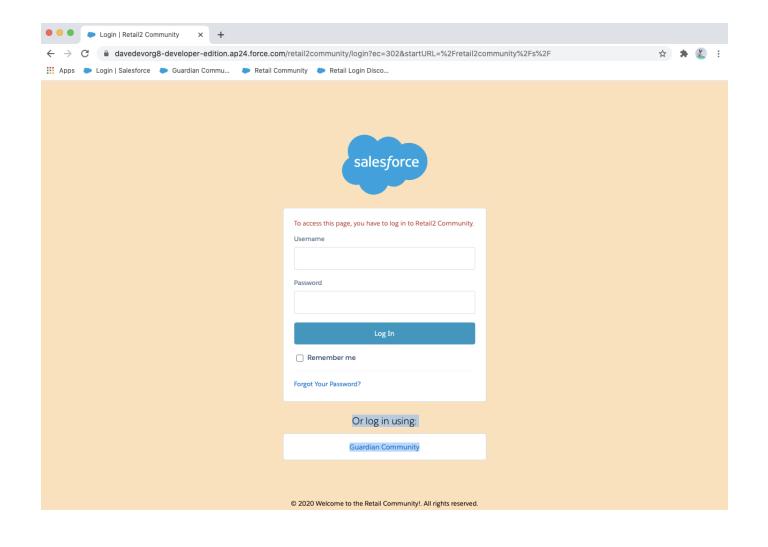
From the Connected App in the Identity Provider, go to SAML Login Information > For Communities > IdP-Initiated Login URL. Click the URL. This should open the SP Community in a new tab and you should be logged in.

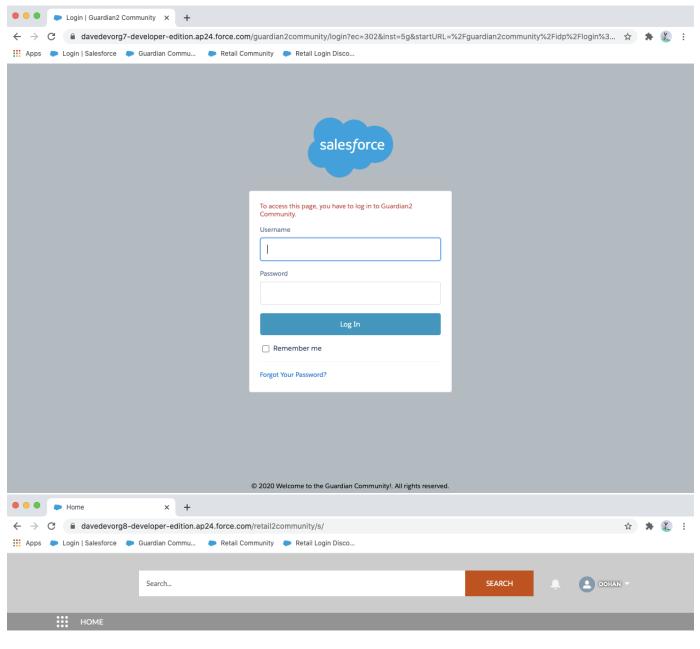


### Test an SP-Initiated SSO

Open the SP Community Login page > Click the button under Or log in using:

You will be redirected to the IdP Community. Login with your IdP Community user credentials. Once authenticated, you will be redirected back to the SP Community home page.





#### **WELCOME TO THE RETAIL COMMUNITY!**

A place where you can easily find solutions and ask questions

FEATURED DISCUSSIONS MY FEED ASKA QUESTION

Don't see what you're looking for?

ASK A QUESTION

CONTACT SUPPORT