

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

Setup > Identity > Identity Provider

The screenshot shows the Salesforce Identity Provider Setup page. The left sidebar contains a search bar with 'identity' and a list of navigation items: Identity, Auth. Providers, Identity Connect, Identity Provider (selected), Identity Provider Event Log, Identity Verification, Identity Verification History, Login Flows, Login History, OAuth Custom Scopes, and Single Sign-On Settings. The main content area is titled 'Identity Provider' and includes a 'Help for this Page' link. Below the title is a description: 'Enable Salesforce.com as an identity provider so you can use single sign-on with other web sites, and define the appropriate service providers whose applications support single sign-on. You can switch to different service providers without having to log in again. [Learn more...](#)'. The 'Identity Provider Setup' section has buttons for 'Edit', 'Disable', 'Download Certificate', and 'Download Metadata'. It contains three expandable sections: 'Details' (Issuer: https://devorg7com-dev-ed.my.salesforce.com), 'Currently chosen certificate details' (Label: SelfSignedCert_25Nov2020_114913, Unique Name: SelfSignedCert_25Nov2020_114913, Created Date: 25/11/2020, 10:49 pm, Expiration Date: 25/11/2021, 11:00 am, Key Size: 2048), and 'SAML Metadata Discovery Endpoints' (Salesforce Identity: https://devorg7com-dev-ed.my.salesforce.com/.well-known/samlidp.xml, Guardian2 Community Identity: https://davedevorg7-developer-edition.ap24.force.com/guardian2community/.well-known/samlidp.xml). The 'Service Providers' section has a link 'Service Providers are now created via Connected Apps. Click here.' and a table with columns 'Name' and 'Created Date', currently showing 'No Service Providers'.

Setup > Identity > Identity Provider

devorg7com-dev-ed.lightning.force.com/lightning/setup/idpPage/home

Apps | salesforce | sf | PA | 9d | AU | drive | login.salesforce | weather

Search Setup

Setup | Home | Object Manager

identity

Identity

- Auth. Providers
- Identity Connect
- Identity Provider**
- Identity Provider Event Log
- Identity Verification
- Identity Verification History
- Login Flows
- Login History
- OAuth Custom Scopes
- Single Sign-On Settings

Didn't find what you're looking for?
Try using Global Search.

Identity Provider

Help for this Page

Enable Salesforce.com as an identity provider so you can use single sign-on with other web sites, and define the appropriate service providers whose applications support single sign-on. You can switch to different service providers without having to log in again. [Learn more...](#)

Quick Tips

- [Certificates and Keys](#)
- [About Single Sign-On](#)
- [My Domain](#)

Identity Provider Setup

Edit Disable Download Certificate Download Metadata

Details

Issuer	https://devorg7com-dev-ed.my.salesforce.com
--------	---

Currently chosen certificate details

Label	SelfSignedCert_25Nov2020_114913	Unique Name	SelfSignedCert_25Nov2020_114913
Created Date	25/11/2020, 10:49 pm	Expiration Date	25/11/2021, 11:00 am
Key Size	2048		

SAML Metadata Discovery Endpoints

Salesforce Identity	https://devorg7com-dev-ed.my.salesforce.com/.well-known/samlidp.xml
Guardian2 Community Identity	https://davedevorg7-developer-edition.ap24.force.com/guardian2community/.well-known/samlidp.xml

Service Providers

Service Providers are now created via Connected Apps. [Click here.](#)

Name	Created Date
No Service Providers	

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

devorg7com-dev-ed.lightning.force.com/lightning/setup/ConnectedApplication/page?address=%2Fapp%2Fmgmt%2Fforceconnectedapps%2FforceAppDet...

Apps | salesforce | sf | PA | 9d | AU | drive | login.salesforce | weather

Search Setup

Setup | Home | Object Manager

app manager

Apps

App Manager

Didn't find what you're looking for?
Try using Global Search.

Manage Connected Apps

Connected App Name: Retail2 Community

[Back to List: Custom Apps](#)

[Edit](#) [Delete](#) [Manage](#)

Version: 1.0

API Name: Retail2_Community

Created Date: 26/11/2020, 12:03 pm

By: David Ohan

Contact Email: dohan@salesforce.com

Contact Phone:

Last Modified Date: 26/11/2020, 12:03 pm

By: David Ohan

Description:

Info URL:

Web App Settings

Start URL	Entity Id	https://davedevorg8-developer-edition.ap24.force.com/retail2community
ACS URL	Enable Single Logout	Disabled
Subject Type	Name ID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Issuer	IdP Certificate	Default IdP Certificate
	Signing Algorithm for SAML Messages	SHA1

Custom Connected App Handler

Apex Plugin Class

Run As

Trusted IP Range for OAuth Web Server Flow

[New](#)

No records to display

Custom Attributes

[New](#)

No records to display

Assign the Connected App to the Customer Community Profiles

Setup > Apps > Connected Apps > Manage Connected Apps

The screenshot shows the Salesforce Setup interface for a 'Retail2 Community' Connected App. The left sidebar contains navigation links for Setup, Home, Object Manager, and various app management options. The main content area displays the 'Connected App Detail' for 'Retail2 Community'. Key sections include:

- System Info:** Installed By (David Dore), Last Modified By (David Dore), Installed Date (26/11/2020, 12:03 pm), Last Modified Date (26/11/2020, 12:22 pm).
- Basic Information:** Info URL, Start URL, Mobile Start URL.
- SAML Service Provider Settings:** Entry ID (https://devorg7com-dev-ed.my.salesforce.com/ap24/force.com/retail2community), Subject Type (Federation ID), Key Certificate (SelfSignedCert_@b6a000...11893), Name ID Format (urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified), Signing Algorithm for SAML Messages (SHA1), Verify Request Signature (SHA1), Enable Single Logout (Disabled).
- SAML Login Information:** View and download SAML endpoint metadata for your organization, communities, or custom domains. Your Organization (Download Metadata).
- For Communities:** Custom Connected App Handler (App: Proprietary Class, Role: Admin), User Provisioning Settings (Enable User Provisioning).
- Trusted IP Range for OAuth Web Server Flow:** No application-defined IP ranges.
- Profiles:** Manage Profiles, Profile Description.
- Permission Sets:** Manage Permission Sets.
- Custom Attributes:** No Custom Attributes.

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

The screenshot shows the 'SAML Login Information' page in Salesforce Setup. It provides a view and download SAML endpoint metadata for your organization, communities, or custom domains. The page is divided into two main sections:

- Your Organization:**
 - IdP-Initiated Login URL: <https://devorg7com-dev-ed.my.salesforce.com/idp/login?app=0sp5q000000PAsX>
 - SP-Initiated POST Endpoint: <https://devorg7com-dev-ed.my.salesforce.com/idp/endpoint/HttpPost>
 - SP-Initiated Redirect Endpoint: <https://devorg7com-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect>
 - Metadata Discovery Endpoint: https://devorg7com-dev-ed.my.salesforce.com/.well-known/samlidp/Retail2_Community.xml
 - Single Logout Endpoint: <https://devorg7com-dev-ed.my.salesforce.com/services/auth/idp/saml2/logout>
- For Communities:**
 - Community Name: **Guardian2 Community** (Download Metadata)
 - IdP-Initiated Login URL: <https://davedevorg7-developer-edition.ap24.force.com/guardian2community/idp/login?app=0sp5q000000PAsX>
 - SP-Initiated POST Endpoint: <https://davedevorg7-developer-edition.ap24.force.com/guardian2community/idp/endpoint/HttpPost>
 - SP-Initiated Redirect Endpoint: <https://davedevorg7-developer-edition.ap24.force.com/guardian2community/idp/endpoint/HttpRedirect>
 - Metadata Discovery Endpoint: https://davedevorg7-developer-edition.ap24.force.com/guardian2community/.well-known/samlidp/Retail2_Community.xml
 - Single Logout Endpoint: <https://davedevorg7-developer-edition.ap24.force.com/guardian2community/services/auth/idp/saml2/logout>

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

Setup > Security > Remote Site Settings

devorg8com-dev-ed.lightning.force.com/lightning/setup/SecurityRemoteProxy/page?address=%2F0rp5g000000XZDQ%3FappLayout%3Dsetup%26tour%3D%2...

Apps salesforce sf PA 9d AU drive login.salesforce weather

Search Setup

Setup Home Object Manager

remote

Custom Code

Remote Access

Security

Remote Site Settings

Didn't find what you're looking for? Try using Global Search.

Remote Site Settings

Remote Site Details

Help for this Page

Remote Site Detail Edit Delete Clone

Remote Site Name	Guardian2Community	Modified By	David Ohan, 30/11/2020, 4:37 pm
Remote Site URL	https://devorg7com-dev-ed.lightning.force.com		
Disable Protocol Security	<input type="checkbox"/>		
Description			
Active	<input checked="" type="checkbox"/>		
Created By	David Ohan, 26/11/2020, 8:53 am		

Edit Delete Clone

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.

devorg8com-dev-ed.lightning.force.com/lightning/setup/SingleSignOn/page?address=%2F0LE5g000000sYij

Apps salesforce sf PA 9d AU drive login.salesforce weather

Search Setup

Setup Home Object Manager

single

Identity

Single Sign-On Settings

Didn't find what you're looking for? Try using Global Search.

Single Sign-On Settings

SAML Single Sign-On Settings

Back to Single Sign-On Settings

Help for this Page

Edit Delete Clone Download Metadata SAML Assertion Validator

Name	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=Salesforce.com, OU=00D5g000000iNB, CN=SelfSignedCert_25Nov2020_114913		
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.ap24.force.com/guardian2community/ldp/endpoint/HttpRedirect		
Custom Logout URL			
Custom Error URL			
Single Logout Enabled	<input type="checkbox"/>		

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/logout
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/retaillogin/discovery/login
Logout URL	https://davedevorg8-developer-edition.ap24.force.com/retaillogin/discovery/services/auth/sp/saml2/logout

Community Name: Retail2 Community

Login URL	https://davedevorg8-developer-edition.ap24.force.com/retail2community/login
Logout URL	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

←

→

↺

davedevorg8-developer-edition.ap24.force.com/retail2community/communitySetup/cwApp.app#/c/page/loginAndRegistration

☆

⚙

👤

⋮

Apps📁 salesforce📁 sf📁 PA📁 9d📁 AU📁 drive📁 login.salesforce📁 weather

⚙Administration

Retail2 Community

Settings

Preferences

Members

Contributors

Login & Registration

Emails

Pages

Rich Publisher Apps

?

👤David Ohan

Login & Registration

Brand, configure, and customize your community's login experience, which includes pages used to log in users, verify identities, reset passwords, register members, and for login flows. Tip: To view your login pages as you work, open the URL for your community using your browser's private browsing mode.

Branding Options

Customize your community's login experience to reflect your brand. You can use dynamic branding URLs to change how login and related pages appear at runtime. [Learn about Dynamic Branding URLs](#)

Logo Type

File


📘

Logo File

Choose file

No file chosen

JPG, GIF or PNG, 100 KB max.



125 px max

250 px max

Background Type

Color

📘

Background

🎨

#FFE1B9

📘

Login Button

🎨

#1797C0

📘

Right Frame URL

📘

Footer Text

Welcome to the Retail Community!

📘

Login Page Setup

Choose a login page type to create a branded login experience. Depending on the login page type, your users can log in with their username, email, phone number, or other user identifier. [Learn more](#)

Login Page Type

Default Page

📘

☒ Allow internal users to log in directly to the community [📘](#)

Select login options to display on the login page. To add more login options, visit [Single Sign-On Settings](#) or [Auth. Providers in Setup](#). [📘](#)

☒ Salesforce username and password

☒ Guardian Community

☐ devorg7 IdP

Logout Page URL

Full URL

📘

Allow System Administrator user to login to the Community

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

Lightning Experience | Salesforce

Administration | Login & Registr

Single Sign-On Settings | Sale

+

← → ↻

davedevorg7-developer-edition.ap24.force.com/guardian2community/communitySetup/cwApp.app#/c/page/loginAndRegistration

Apps

salesforce

sf

PA

9d

AU

drive

login.salesforce

weather

Administration

Guardian2 Community

Settings

Preferences

Members

Contributors

Login & Registration

Emails

Pages

Rich Publisher Apps

Login & Registration

Brand, configure, and customize your community's login experience, which includes pages used to log in users, verify identities, reset passwords, register members, and for login flows. Tip: To view your login pages as you work, open the URL for your community using your browser's private browsing mode.

Branding Options

Customize your community's login experience to reflect your brand. You can use dynamic branding URLs to change how login and related pages appear at runtime. [Learn about Dynamic Branding URLs](#)


Logo Type

File *i*

Logo File

Choose file No file chosen

JPG, GIF or PNG, 100 KB max.



125 px max

250 px max

Background Type

Color *i*

Background

#B1BAC1 *i*

Login Button

#1797C0 *i*

Right Frame URL

i

Footer Text

Welcome to the Guardian Community! *i*

Login Page Setup

Choose a login page type to create a branded login experience. Depending on the login page type, your users can log in with their username, email, phone number, or other user identifier. [Learn more](#)

Login Page Type

Default Page *i*

☒ Allow internal users to log in directly to the community *i*

Select login options to display on the login page. To add more login options, visit [Single Sign-On Settings](#) or [Auth. Providers in Setup](#). *i*

☒ Salesforce username and password

☐ Retail *i*

Logout Page URL

Full URL

i

Password Pages

Change how passwords are handled by selecting custom pages, if they are available.

Forgot Password

Experience Builder Page

Forgot Password *i*

Reset Password

Default Page

Registration Page Configuration

☐ Allow external users to self-register

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.

The screenshot shows the Salesforce Setup interface for a Connected App. The left sidebar contains navigation links: Apps, Connected Apps, Feature Settings, Salesforce Files, Identity, and Security. The main content area is titled 'SETUP' and displays the following sections:

- System Info:** Installed By (David Ohan), Last Modified By (David Ohan), Installed Date (26/11/2020, 12:03 pm), Last Modified Date (26/11/2020, 12:22 pm).
- Basic Information:** Info URL, Start URL, Mobile Start URL.
- SAML Service Provider Settings:**
 - Entity Id: https://davedevorg8-developer-edition.ap24.force.com/retail2community
 - Subject Type: Federation ID
 - IdP Certificate: SelfSignedCert_25Nov2020_114913
 - Name ID Format: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
 - Signing Algorithm for SAML Messages: SHA1
 - Verify Request Signatures: Enabled
 - Enable Single Logout: Disabled
- SAML Login Information:**
 - View and download SAML endpoint metadata for your organization, communities, or custom domains.
 - Your Organization: Download Metadata
 - IdP-Initiated Login URL: https://devorg7com-dev-ed.my.salesforce.com/idp/login?app=0sp5g000000PAsX
 - SP-Initiated POST Endpoint: https://devorg7com-dev-ed.my.salesforce.com/idp/endpoint/HttpPost
 - SP-Initiated Redirect Endpoint: https://devorg7com-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
 - Metadata Discovery Endpoint: https://devorg7com-dev-ed.my.salesforce.com/.well-known/saml2/Retail2_Community.xml
 - Single Logout Endpoint: https://devorg7com-dev-ed.my.salesforce.com/services/auth/idp/saml2/logout
 - For Communities: Download Metadata
 - IdP-Initiated Login URL: https://davedevorg7-developer-edition.ap24.force.com/guardian2community/idp/login?app=0sp5g000000PAsX
 - SP-Initiated POST Endpoint: https://davedevorg7-developer-edition.ap24.force.com/guardian2community/idp/endpoint/HttpPost
 - SP-Initiated Redirect Endpoint: https://davedevorg7-developer-edition.ap24.force.com/guardian2community/idp/endpoint/HttpRedirect
 - Metadata Discovery Endpoint: https://davedevorg7-developer-edition.ap24.force.com/guardian2community/.well-known/saml2/Retail2_Community.xml
 - Single Logout Endpoint: https://davedevorg7-developer-edition.ap24.force.com/guardian2community/services/auth/idp/saml2/logout
- Custom Connected App Handler:** Apex Plugin Class, Run As.
- User Provisioning Settings:** Enable User Provisioning (checked).
- Trusted IP Range for OAuth Web Server Flow:**

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.



To access this page, you have to log in to Retail2 Community.

Username

Password

Log In

☐ Remember me

[Forgot Your Password?](#)

Or log in using:

[Guardian Community](#)

