

Welcome to

dreamOle[®]



Cognizant



FORMTITAN



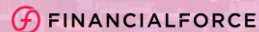
MAKEMECLOUD
consulting



blue-
infinity

Linked by isobar

Dentsu Aegis Network



BLACKBIRD



Demystifying Single Sign On and oAuth with Salesforce Identity

Eugenio Roldan
Technical Architect at Cosentino

¿Que es el SSO y por que usarlo?



- SSO: acceso a multiples servicios mediante un solo Proveedor de identificacion
- Mejora la experiencia de usuario – una solo password para todo
- Facilita la gestion – centraliza el control de credenciales
- Mejora la seguridad – desactiva/ activa el acceso co una accion unica

Piezas del SSO

SAML

Security Assertion Markup Language – Lenguaje estandar para Autenticacion y autorizacion

Identity Provider

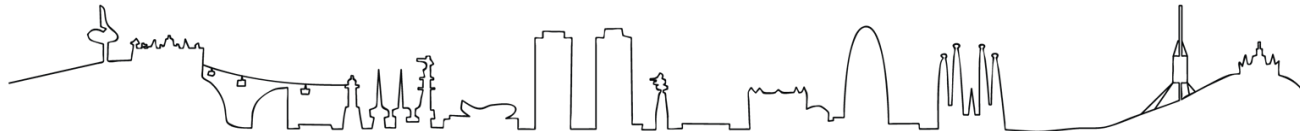
Aquella entidad que proporciona y valida la informacion del usuario

Service Provider

Servicio al que vamos a proporcionar acceso

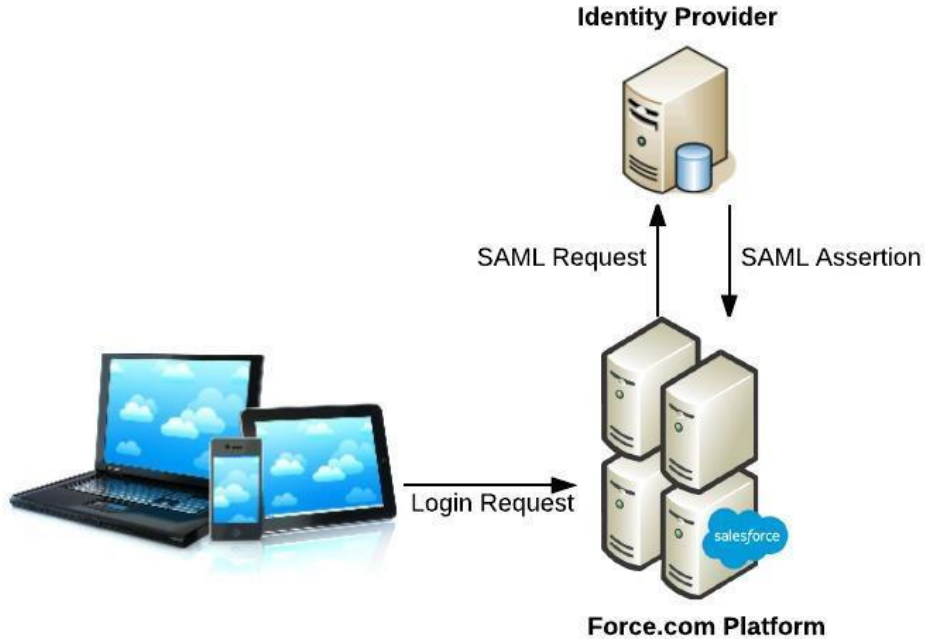
User Agent

Usualmente un Navegador Web que hara de intermediario en las peticiones

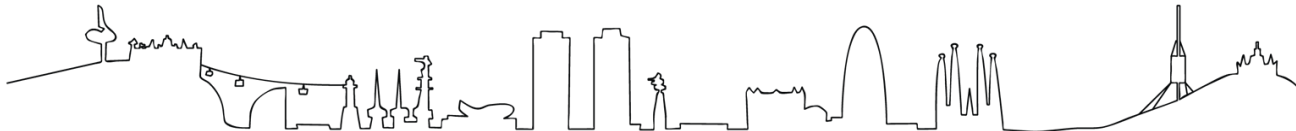
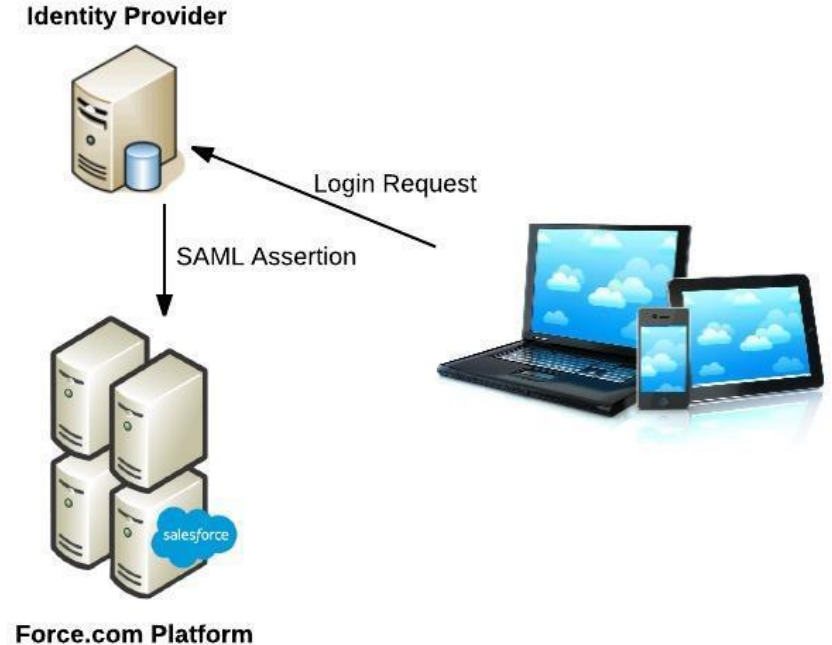


SP Initiated SSO vs IdP initiated SSO

Service Provider Initiated Login



Identity Provider Initiated Login



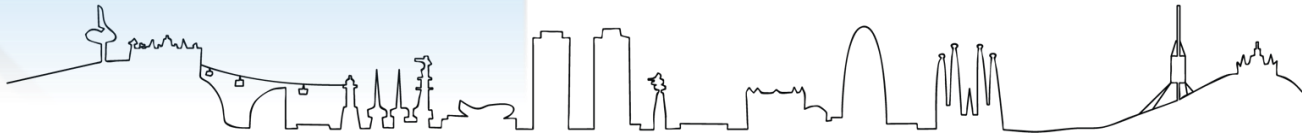
My Domain

Personaliza tu pagina de login y la url de tu ORG

Permite realizar un Service Provider SSO

Permite usar tu Salesforce Org como un Identity Provider

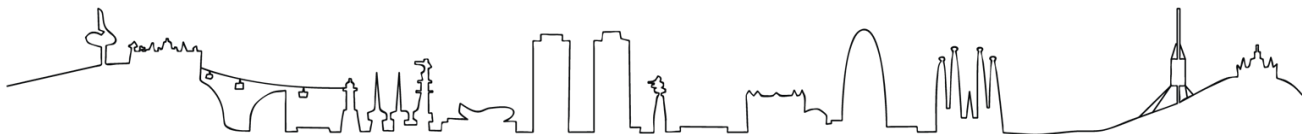
Previene el deep linking de posibles migraciones de nodos



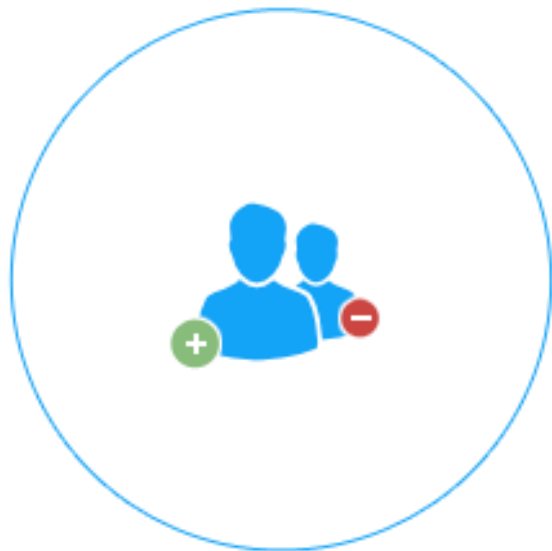
Parametro Relay State

The screenshot shows a browser window with the following elements:

- Address bar: `https://.../one.app#/s/Object/ContentDocument/home` (indicated by a red arrow)
- Navigation bar: "Take a Tour of Salesforce" and "Choose Your Tour"
- Search bar: "Search Salesforce"
- Navigation tabs: "Salesforce Chatter", "Chatter", "Files" (selected)
- Section header: "FILES Owned by Me" (0 items - Sorted by Last Modified Date)
- Table with columns: "Owned by Me", "TITLE", "OWNER", "LAST MO".
- Message: "There's nothing in Owned by Me yet. When records are added to this list view, you'll see them here."



Gestion de usuarios



Provisioning

Proceso de creacion de usuarios y actualizaciones.

JIT (Just in Tie Provisioning) : creacion / actualizacion automatica de usuarios basado en la informacion del SAML Assertion

De-Provisioning

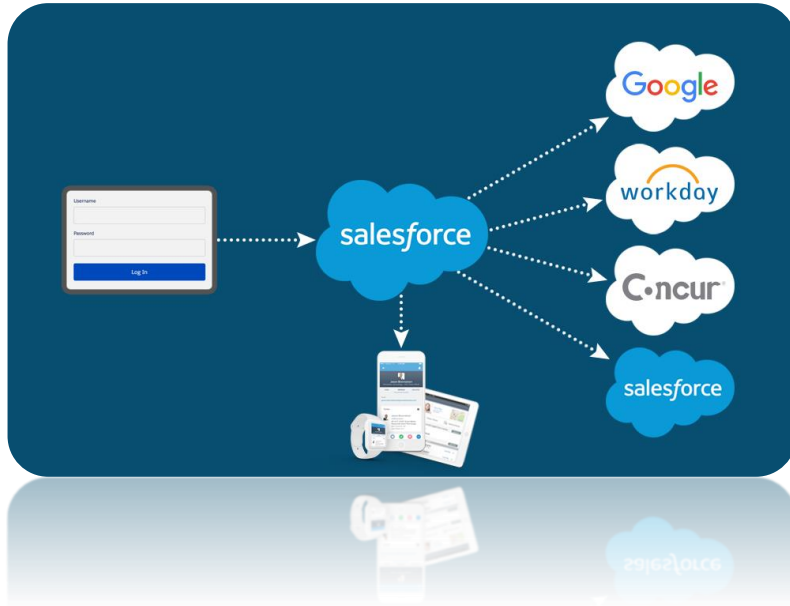
Desactivado de usuarios y bajas

No soportado en JIT

Requiere integracion a medida via WS o SF Identity Connect



Salesforce Identity

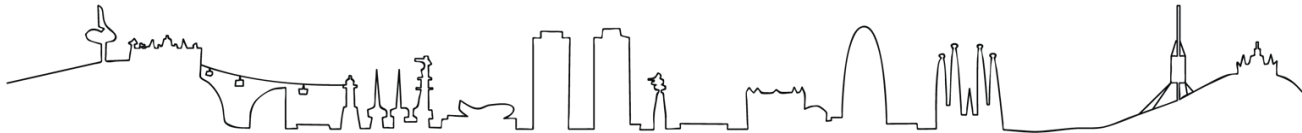


Utiliza Salesforce como Identity Provider para tus empleados y clientes

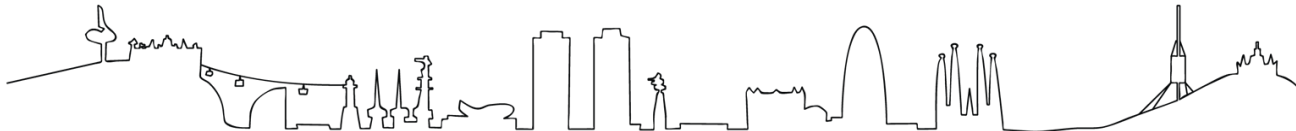
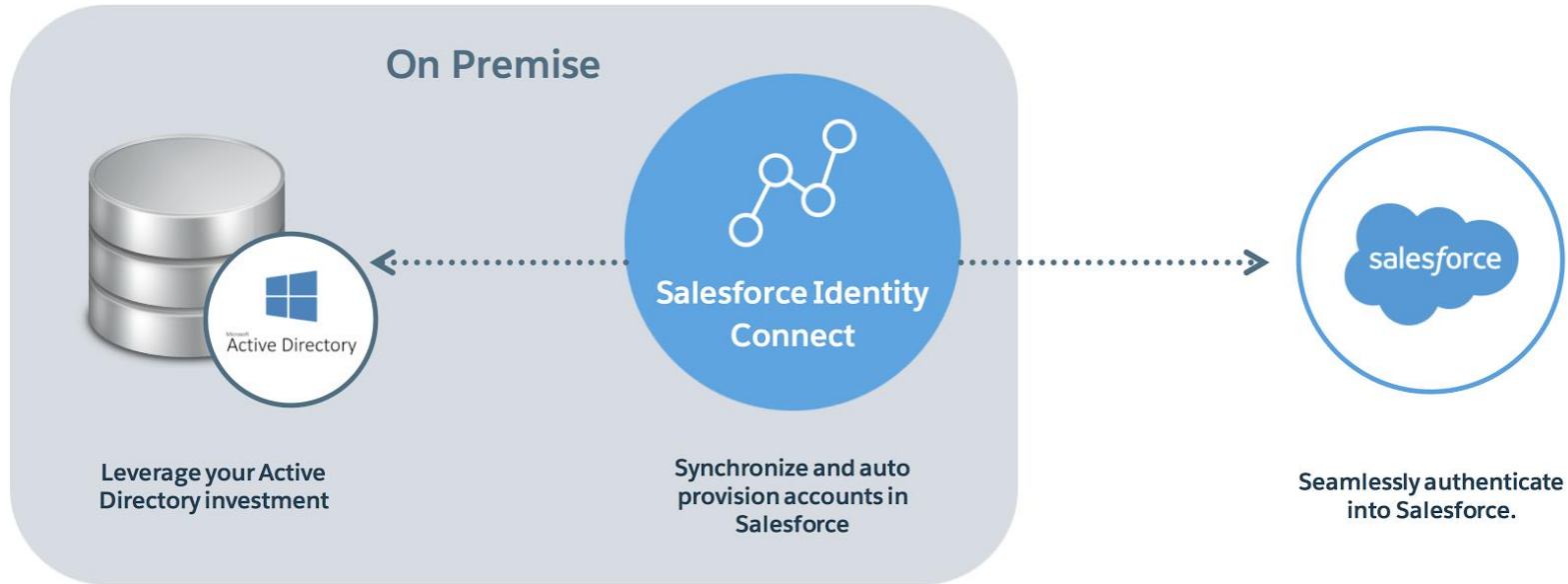
Soporta SSO y Social Sign-On

Capacidad para Two -factor authentication

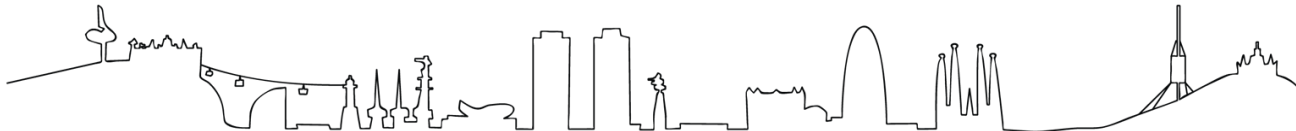
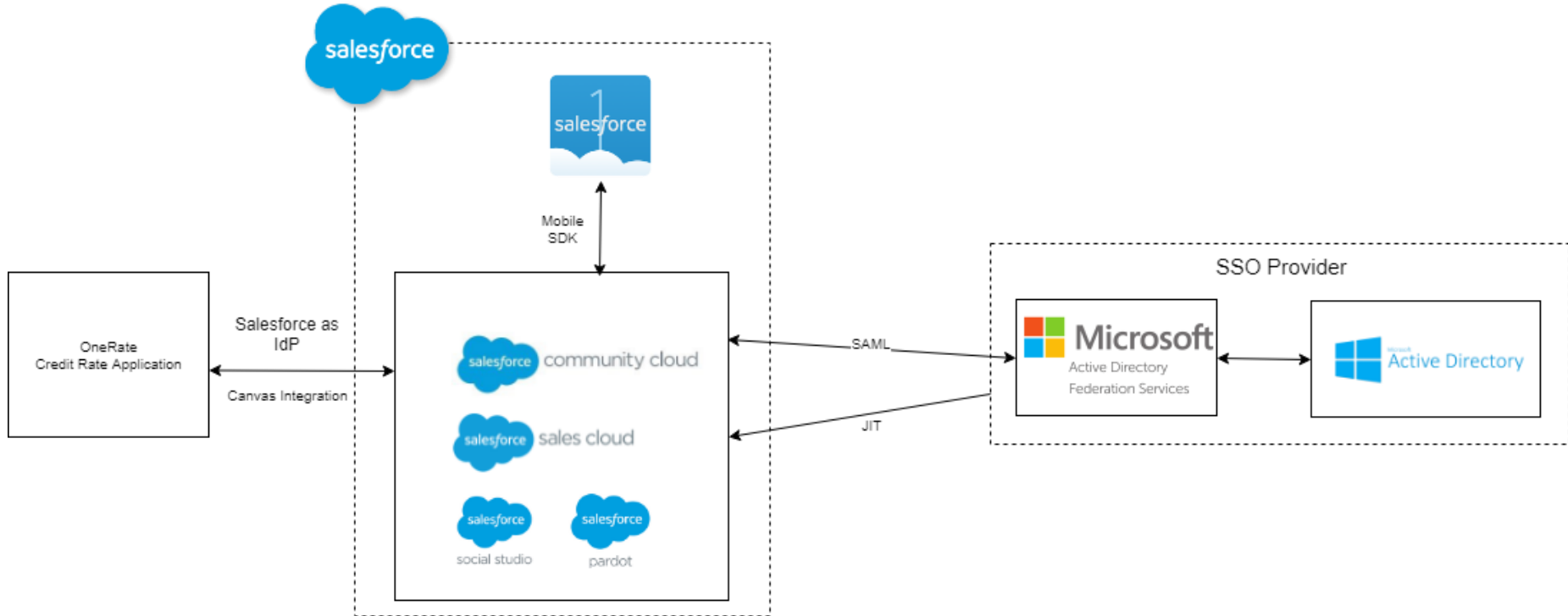
Licencias integradas para empleados y External Identity Licenses para clientes



Salesforce Identity Connect



Cosentino SSO Architecture



¿Que es el oAuth y por que usarlo?

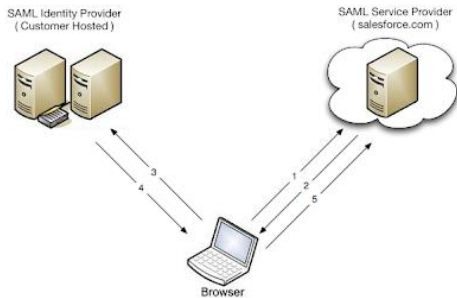


- Permite la autorizacion entre aplicaciones para el acceso a la informacion del usuario
- oAuth se utiliza para Autorizacion, NO para autenticacion
- Delimita el nivel de acceso y los temporaliza.
- Multiples flujos segun las necesidades



oAuth vs SAML SSO

SAML Flow

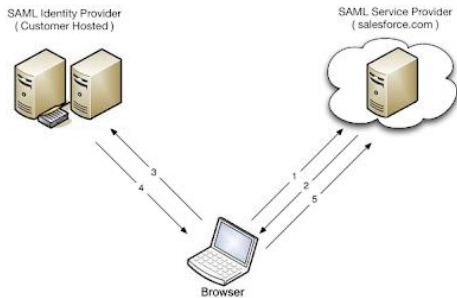


1. Usuario solicita acceso a un recurso en SF
2. Sf determina si debe ser autenticado y redirige al idP
3. Usuario se autentica en el idP
4. idP envia el SAML assertion de Vuelta a Salesforce incluyendo el RelayState
5. SF acepta la identidad, loga al usuario y redirige al URL del RelayState



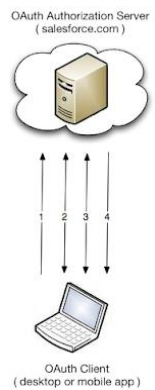
oAuth vs SAML SSO

SAML Flow

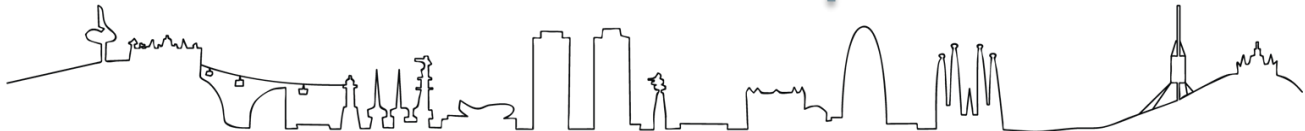


1. Usuario solicita acceso a un recurso en SF
2. Sf determina si debe ser autentificado y redirige al idP
3. Usuario se autentica en el idP
4. idP envia el SAML assertion de Vuelta a Salesforce incluyendo el RelayState
5. SF acepta la identidad, loga al usuario y redirige al URL del RelayState

oAuth Flow

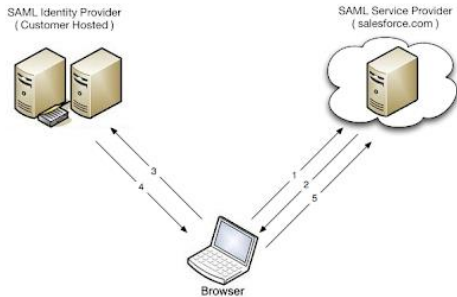


1. El cliente oAuth realiza una peticion de autorizacion
2. El servidor oAuth autentica al usuario
3. El usuario autoriza a la aplicacion y verifica los permisos
4. La aplicacion es autorizada mediante un oAuth token



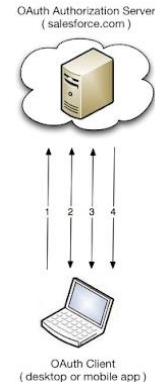
oAuth vs SAML SSO

SAML Flow



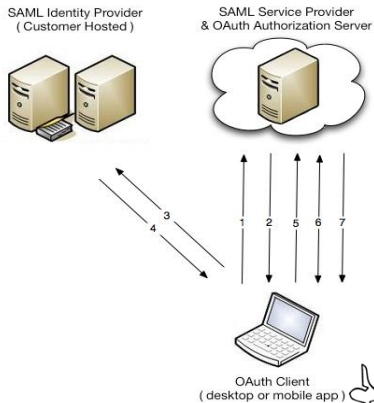
1. Usuario solicita acceso a un recurso en SF
2. Sf determina si debe ser autenticado y redirige al idP
3. Usuario se autentica en el idP
4. idP envia el SAML assertion de Vuelta a Salesforce incluyendo el RelayState
5. SF acepta la identidad, loga al usuario y redirige al URL del RelayState

oAuth Flow



1. El cliente oAuth realiza una peticion de autorizacion
2. El servidor oAuth autentica al usuario
3. El usuario autoriza a la aplicacion y verifica los permisos
4. La aplicacion es autorizada mediante un oAuth token

SAML + oAuth Flow



1. El cliente oAuth realiza una peticion de autorizacion
2. oAuth servidor determina si debe ser autenticado y redirige al idP
3. Usuario se autentica en el idP
4. idP envia el SAML assertion de Vuelta a Salesforce incluyendo el RelayState
5. SF acepta la identidad, loga al usuario y redirige al URL del RelayState que contiene el servidor de autorizacion
6. El usuario autoriza a la aplicacion y verifica los permisos
7. La aplicacion es autorizada mediante un oAuth token

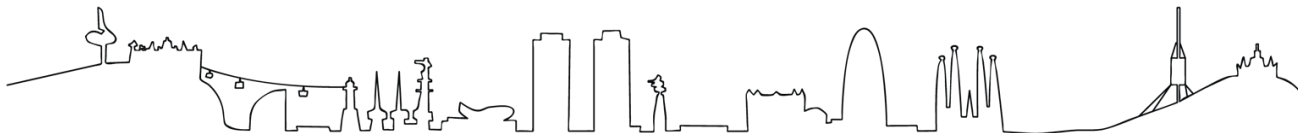
Workshop

Thanks to Enrrico Murru:
<https://blog.enree.co>

Pre-rrequisitos

- Haber atendido los ultimos 25 – 30 minutos :P
- Una developer org con My domain activado o cualquier Playground de trailhead
- Una cuenta en Heroku (Si no tienes una, Sign up en <https://signup.heroku.com>)
- Descargar este paquete de recursos:

<https://sforce.co/2HfiYNq>



Creacion Community

salesforce

Help & Training

LIGHTNING BOLT

Enter a Name

Not sure what to enter? Don't worry—you can always change it later.

Name

Identity

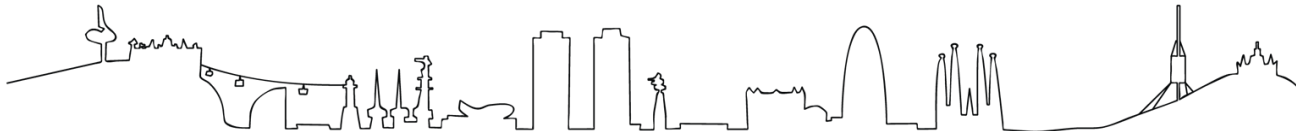
URL

playful-goat-21643-dev-developer-edition.eu... Identity

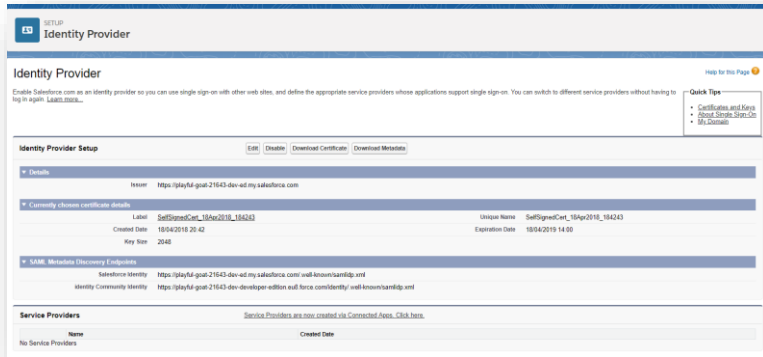
Create

1. Setup → All Communities → New Community.
Seleccionamos Salesforce tabs + Visualforce Template

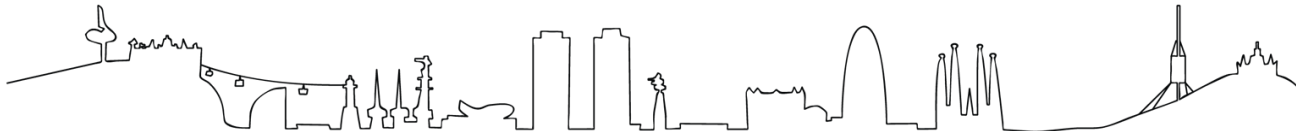
Si no esta habilitada, habilitamos dominio de community pegando el mismo que tengamos definido
2. Click en Administration → members y añadimos el perfil Customer Community (seleccionar Portal en el picklist)
3. Tabs: Añadimos Home y la ponemos primera
4. Login & registration : sube el logo que viene en el paquete de resources
5. Activamos la Community



Enable Identity Provider



1. Setup → Security Controls → Identity Provider y click en Enable Identity Provider.
2. Selecciona el certificado autofirmado por defecto
3. Copia el SAML Metada Discovery Endpoints de la comunidad que has creado y pegalo en el navegador en nueva Tab. Lo necesitaremos mas adelante.



Creacion de la Connected App

App Settings

Start URL

Enable SAML

Entity Id

ACS URL

Enable Single Logout

Subject Type

Name ID Format

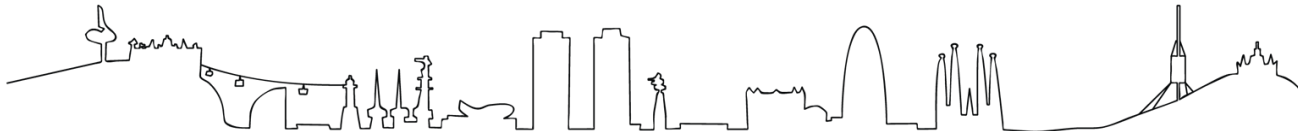
Issuer

IdP Certificate

Verify Request Signatures

Encrypt SAML Response

1. Setup → Create → Apps → New connected App
2. App Name: Dreamole SSO. API Name dejamos que lo rellene
3. Enable SAML true
4. Entity ID: dreamoleSSO
5. ACS URL: https://dreamole-ss0{ddMMyyyy}.herokuapp.com/login/callback
6. Subject Type: User ID
7. Name ID : urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
8. Issue: dejad el valor por defecto.



Creacion de la App Heroku

* SAML_ENTRYPOINT
Salesforce IdP SAML endpoint

* SAML_ISSUER
Local app issuer

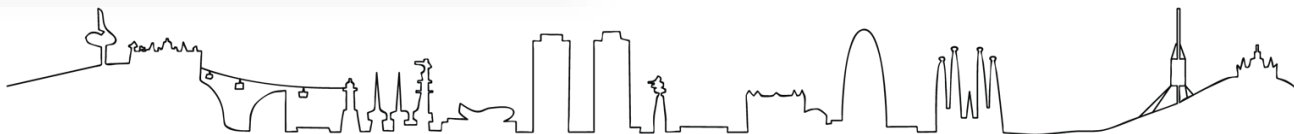
* SAML_CERT
Salesforce SAML certificate

* SAML_IDENTIFIER_FORMAT
SAML nameid format

* APP_NAME
Application name (on page's title and header)

* SF_HOME
Home Salesforce url

1. Abre el Shortcut Web que viene en la carpeta de recursos, denominado Deploy SSO App Heroku
2. App name: dreamole-sso{ddMMyyyy}
3. SAML_ENTRYPOINT: vamos a la tab con el XML que abrimos antes y copiamos el valor del tag *md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect*
4. SAML ISSUER: dreamoleSSO
5. SAML CERT: volvemos al XML, copiar toda la cadena de texto dentro del nodo *ds:X509Certificate*
6. SAML IDENTIFIER FORMAT: valor por defecto *urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified*
7. APP NAME: Dreamole SSO
8. SF_HOME: la URL base de la comunidad. La podeis encontrar en Setup → All communities. Copiamos y pegamos.



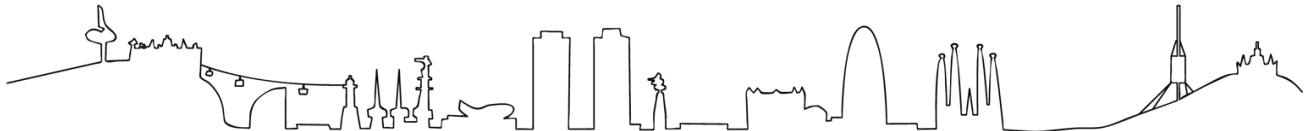
Creacion de usuario de prueba

User Edit [Save] [Cancel]

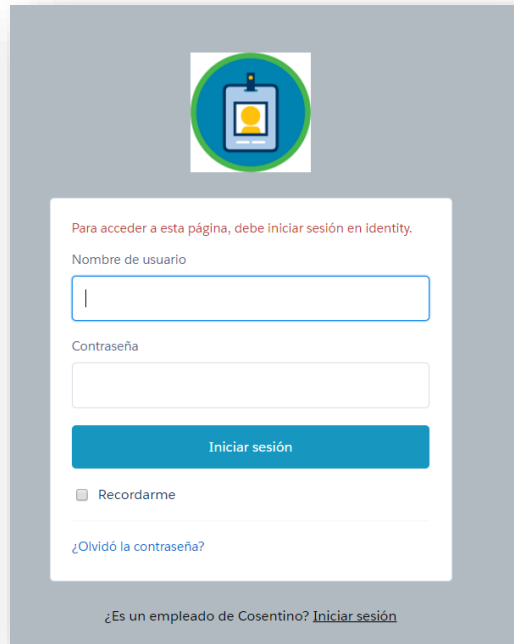
General Information

First Name: Eugenio
Last Name: Roldan Romasanta
Alias: eroldan
Email: eugenio_roidan@outlook.cor
Username: eugenio_roidan@outlook.cor
Nickname: eroldanro
Title: CEO
Company:
Department:
User License: Customer Community
Profile: Customer Community User
Active:
Data.com User Type: --None--
Data.com Monthly Addition Limit: 300
Mobile User:
Salesforce CRM Content User:
Receive Salesforce CRM Content Email Alerts:
Receive Salesforce CRM Content Alerts as Daily Digest:
Allow Forecasting:
Phone:
Extension:

1. Vamos a nuestro usuario y nos establecemos el rol de CEO
2. A continuacion, vamos a cualquier cuenta y creamos un contacto con nuestro nombre y correo electronico.
3. Manage External User → Enable Customer
4. User License : Customer Community
5. Profile: Customer Community User
6. Federation ID: copiamos email
7. Marcar Generate new password and notify user immediately y Save
8. Click en el Profile Customer Community user y otorgamos acceso a la Connected App *Dreamole SSO*
9. Buscamos en nuestro mail el correo de password y generamos la contraseña.



Probemos nuestro SSO!!



Para acceder a esta página, debe iniciar sesión en identity.

Nombre de usuario

Contraseña

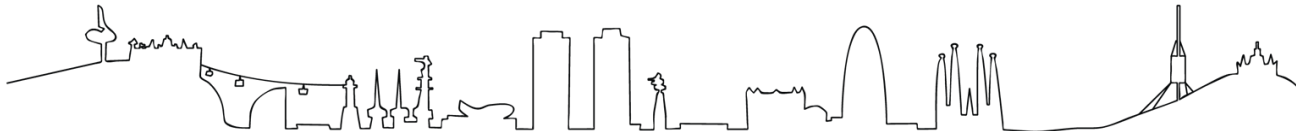
Iniciar sesión

Recordarme

[¿Olvidó la contraseña?](#)

[¿Es un empleado de Cosentino? Iniciar sesión](#)

1. Abrimos una ventana de incognito para no interferir sesiones
2. Solicitamos la url de nuestra app de Heroku:
`https://dreamole-ss0{ddMMyyyy}.herokuapp.com`
3. Pinchamos en Login
4. Introducimos nuestras credenciales
5. Veremos que ahora tenemos la opción de Profile y Logout. Abrimos profile para ver nuestro userId y username de Salesforce enviados por SAML
6. Pinchamos en Back to Salesforce y vemos como nos lleva a la community sin solicitarnos login.



IT'S MAGIC



Q & A



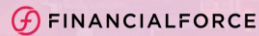
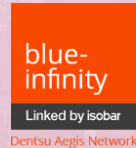
Cognizant



FORMTITAN



MAKEMECLLOUD
consulting



BLACKBIRD