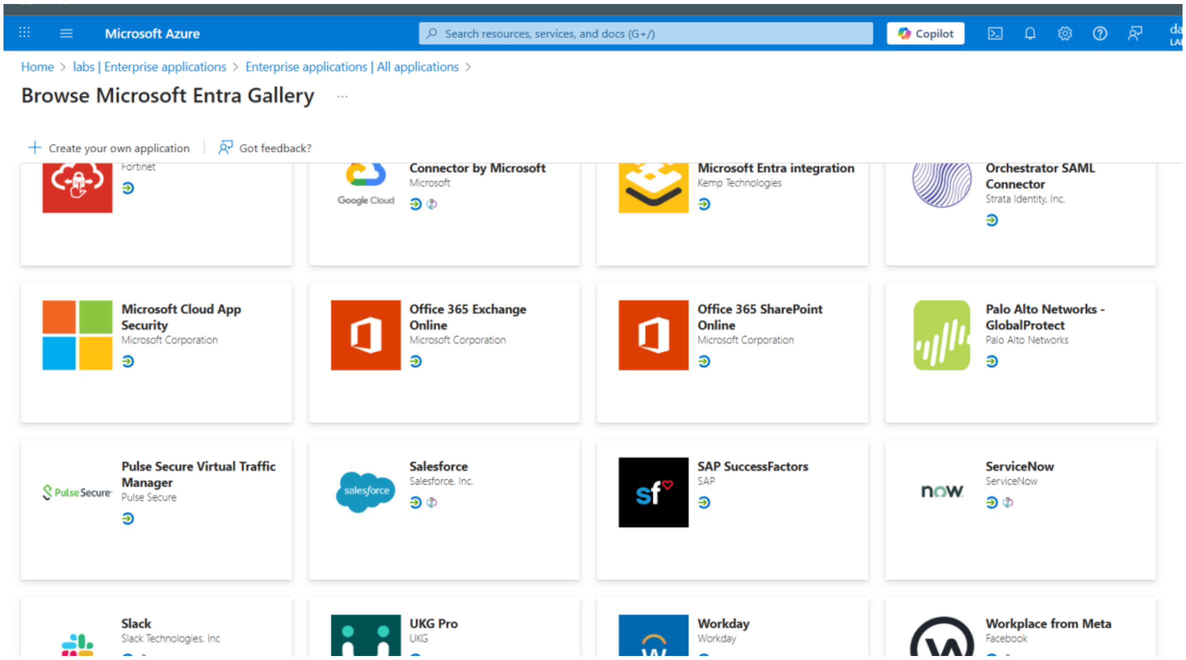
Azure Lab Enable SAML SSO with Sales Force

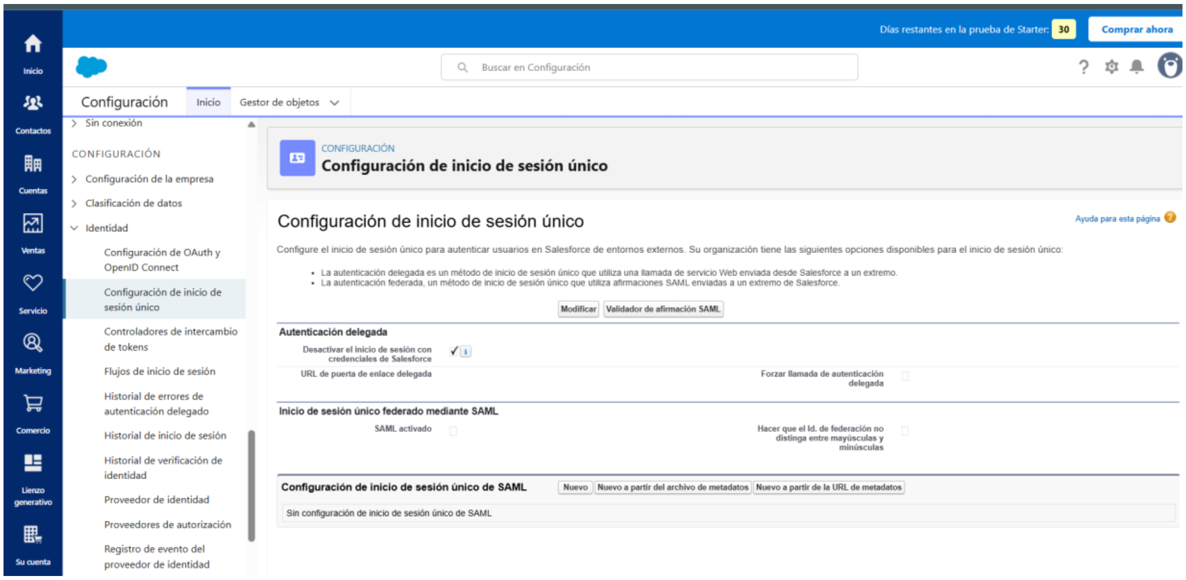
Requirements Azure tenant previously configured and Sales force account.

Part I.

Go in our azure tenant as global admin and find Entra ID → enterprise app → select Sales force


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > labs | Enterprise applications > Enterprise applications | All applications >
Browse Microsoft Entra Gallery
Create your own application
Got feedback?
Fortinet
Connector by Microsoft
Microsoft
Google Cloud
Microsoft Entra integration
Kemp Technologies
Orchestrator SAML Connector
Strata Identity, Inc.
Microsoft Cloud App Security
Microsoft Corporation
Office 365 Exchange Online
Microsoft Corporation
Office 365 SharePoint Online
Microsoft Corporation
Palo Alto Networks - GlobalProtect
Palo Alto Networks
Pulse Secure Virtual Traffic Manager
Pulse Secure
Salesforce
Salesforce, Inc.
SAP SuccessFactors
SAP
ServiceNow
ServiceNow
Slack
Slack Technologies, Inc
UKG Pro
UKG
Workday
Workday
Workplace from Meta
Facebook

Then let's configure SAML. For this we need an Entity ID to get it go our Sales Force admin portal, configuration, SS-ON settings to set up a Entity ID


Días restantes en la prueba de Starter: 30
Comprar ahora
Buscar en Configuración
Inicio
Contactos
Cuentas
Ventas
Servicio
Marketing
Comercio
Lienzo generativo
Su cuenta
Configuración
Inicio
Gestor de objetos
Sin conexión
CONFIGURACIÓN
Configuración de la empresa
Clasificación de datos
Identidad
Configuración de OAuth y OpenID Connect
Configuración de inicio de sesión único
Controladores de intercambio de tokens
Flujos de inicio de sesión
Historial de errores de autenticación delegado
Historial de inicio de sesión
Historial de verificación de identidad
Proveedor de identidad
Proveedores de autorización
Registro de evento del proveedor de identidad
CONFIGURACIÓN
Configuración de inicio de sesión único
Ayuda para esta página
Modificar
Validador de afirmación SAML
Nuevo
Nuevo a partir del archivo de metadatos
Nuevo a partir de la URL de metadatos

Configuración de inicio de sesión único

Configure el inicio de sesión único para autenticar usuarios en Salesforce de entornos externos. Su organización tiene las siguientes opciones disponibles para el inicio de sesión único:

- La autenticación delegada es un método de inicio de sesión único que utiliza una llamada de servicio Web enviada desde Salesforce a un extremo.
- La autenticación federada, un método de inicio de sesión único que utiliza afirmaciones SAML enviadas a un extremo de Salesforce.

Autenticación delegada

Desactivar el inicio de sesión con credenciales de Salesforce ✓

URL de puerta de enlace delegada

Forzar llamada de autenticación delegada □

Inicio de sesión único federado mediante SAML

SAML activado □

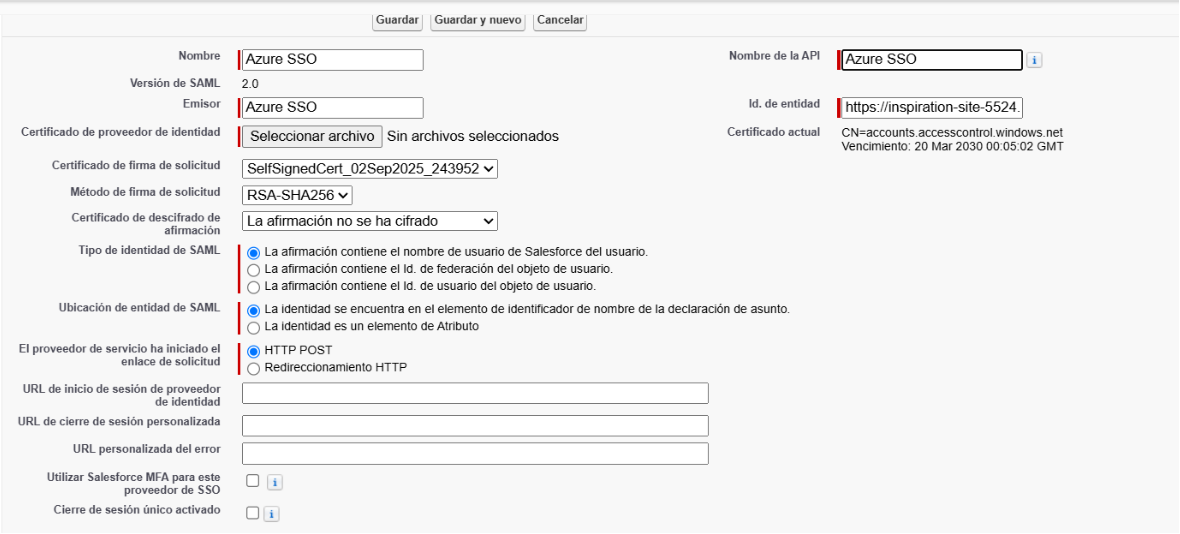
Hacer que el Id. de federación no distinga entre mayúsculas y minúsculas □

Configuración de inicio de sesión único de SAML

Sin configuración de inicio de sesión único de SAML

Let’s create a new SAML with the following values

Salesforce Field	**Value**
Name	Azure AD SSO
API Name	Azure_AD_SSO
Version	2.0
Entity ID / Issuer	https://inspiration-site-5524.my.salesforce.com
Identity Provider Certificate	Upload .cer file downloaded from Azure AD
Signature Method	RSA-SHA256
Name ID Format	Username (Email)
Identity Location	Subject
SP-initiated	HTTP POST

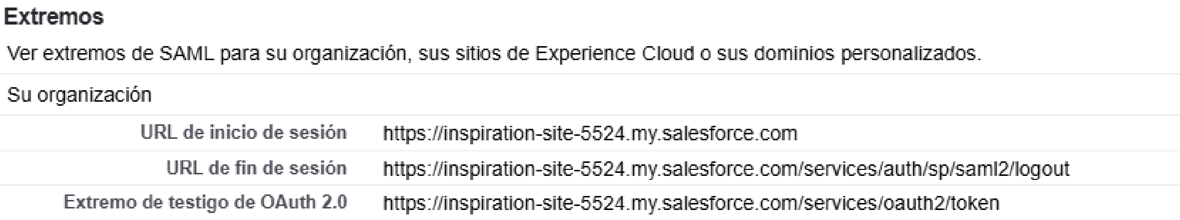


Nombre	Azure SSO	Nombre de la API	Azure SSO
Versión de SAML	2.0		
Emisor	Azure SSO	Id. de entidad	https://inspiration-site-5524.
Certificado de proveedor de identidad	Seleccionar archivo Sin archivos seleccionados	Certificado actual	CN=accounts.accesscontrol.windows.net Vencimiento: 20 Mar 2030 00:05:02 GMT
Certificado de firma de solicitud	SelfSignedCert_02Sep2025_243952		
Método de firma de solicitud	RSA-SHA256		
Certificado de descifrado de afirmación	La afirmación no se ha cifrado		
Tipo de identidad de SAML	● La afirmación contiene el nombre de usuario de Salesforce del usuario. ○ La afirmación contiene el Id. de federación del objeto de usuario. ○ La afirmación contiene el Id. de usuario del objeto de usuario.		
Ubicación de entidad de SAML	● La identidad se encuentra en el elemento de identificador de nombre de la declaración de asunto. ○ La identidad es un elemento de Atributo		
El proveedor de servicio ha iniciado el enlace de solicitud	● HTTP POST ○ Redireccionamiento HTTP		
URL de inicio de sesión de proveedor de identidad			
URL de cierre de sesión personalizada			
URL personalizada del error			
Utilizar Salesforce MFA para este proveedor de SSO	□		
Cierre de sesión único activado	□		

Then go to Azure Enterprise ID Connect Sales Force enable SAML and used the following values to set up SSO

Azure Field	**Value**
Identifier (Entity ID)	https://inspiration-site-5524.my.salesforce.com
Reply URL (ACS URL)	https://inspiration-site-5524.my.salesforce.com/services/auth/sp/saml2/acs
Sign-on URL	https://inspiration-site-5524.my.salesforce.com
Logout URL	https://inspiration-site-5524.my.salesforce.com/services/auth/sp/saml2/logout
NameID	user.userprincipalname

(These values were obtained from Sales Force endpoint section)



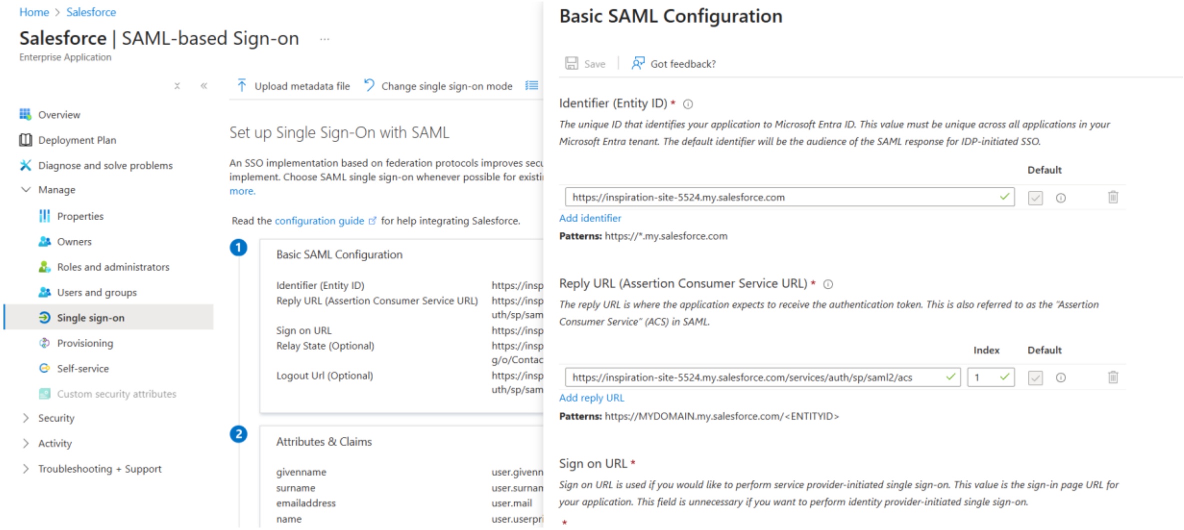
Extremos

Ver extremos de SAML para su organización, sus sitios de Experience Cloud o sus dominios personalizados.

Su organización

URL de inicio de sesión	https://inspiration-site-5524.my.salesforce.com
URL de fin de sesión	https://inspiration-site-5524.my.salesforce.com/services/auth/sp/saml2/logout
Extremo de testigo de OAuth 2.0	https://inspiration-site-5524.my.salesforce.com/services/oauth2/token

In Basic SAML configuration section in azure with used these values to set up it .



Salesforce | SAML-based Sign-on
Enterprise Application

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves secu
implement. Choose SAML single sign-on whenever possible for existi
more.

Read the configuration guide for help integrating Salesforce.

1 Basic SAML Configuration

Identifier (Entity ID)	https://insp
Reply URL (Assertion Consumer Service URL)	https://insp uth/sp/sam
Sign on URL	https://insp
Relay State (Optional)	https://insp g/o/Contac
Logout Url (Optional)	https://insp uth/sp/sam

2 Attributes & Claims

givenname	user.givenn
surname	user.surnan
emailaddress	user.mail
name	user.userpri

Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://inspiration-site-5524.my.salesforce.com ✓	☑

Patterns: https://*.my.salesforce.com

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://inspiration-site-5524.my.salesforce.com/services/auth/sp/saml2/acs ✓	1 ✓	☑

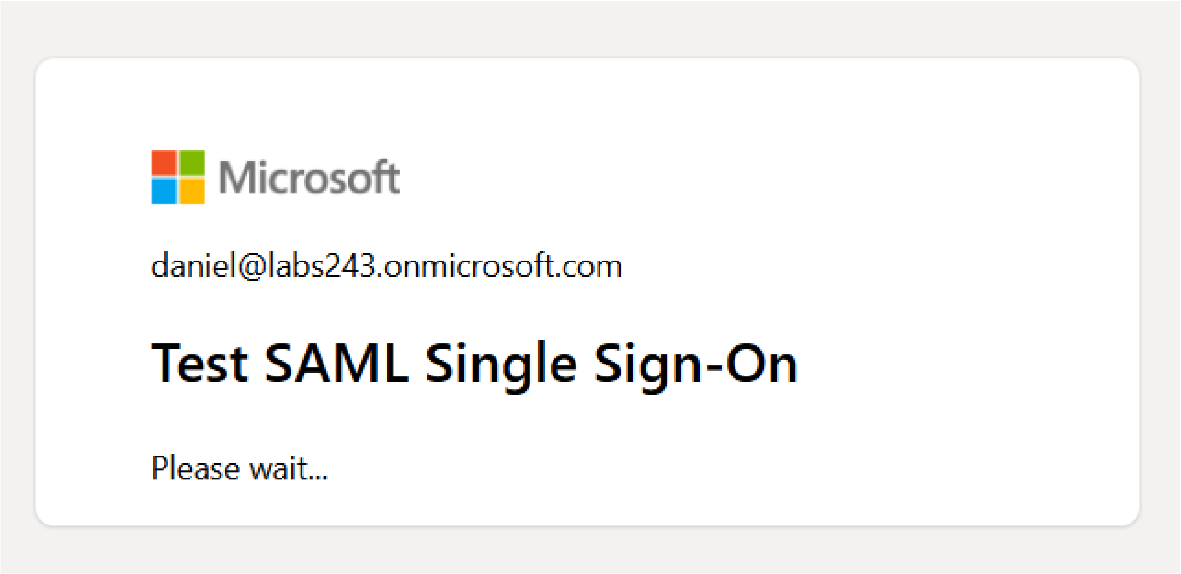
Patterns: https://MYDOMAIN.my.salesforce.com/<ENTITYID>

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

Then we test it, to prove all are working well

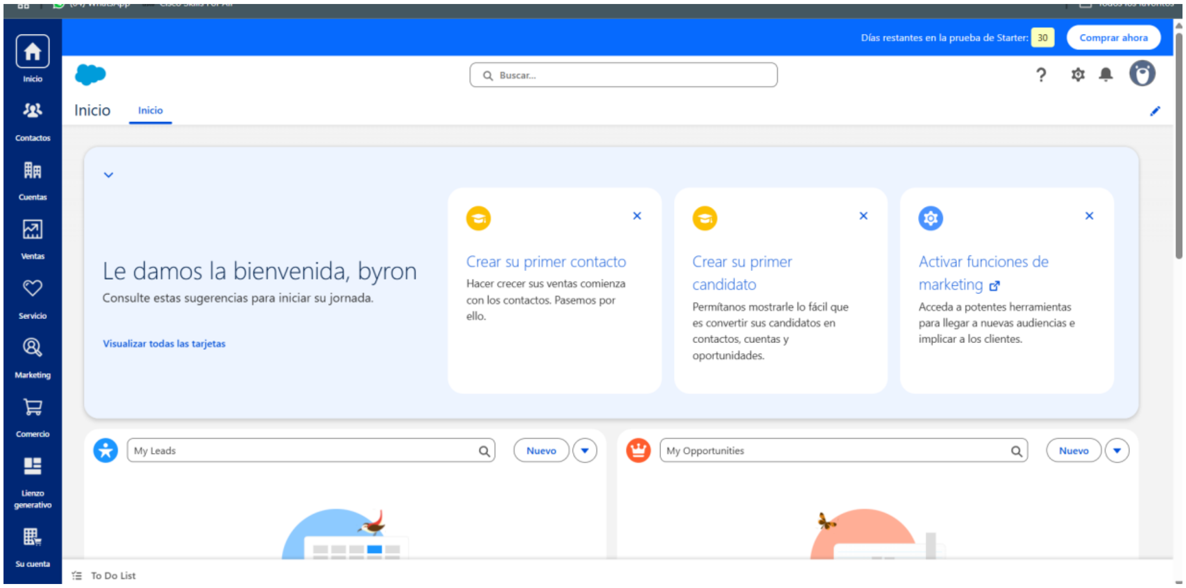


Microsoft

daniel@labs243.onmicrosoft.com

Test SAML Single Sign-On

Please wait...



Le damos la bienvenida, byron

Consulte estas sugerencias para iniciar su jornada.

Visualizar todas las tarjetas

Crear su primer contacto

Hacer crecer sus ventas comienza con los contactos. Pasemos por ello.

Crear su primer candidato

Permítanos mostrarle lo fácil que es convertir sus candidatos en contactos, cuentas y oportunidades.

Activar funciones de marketing

Acceda a potentes herramientas para llegar a nuevas audiencias e implicar a los clientes.

Conclusion.

In this lab, we successfully configured **SAML 2.0 Single Sign-On (SSO)** between **Salesforce** and **Azure Active Directory**. By setting up the correct **Entity ID**, **ACS URL**, and uploading the **IdP certificate**, we established a secure trust relationship between the Service Provider (Salesforce) and the Identity Provider (Azure AD).

After mapping users and testing SSO, we verified that authentication works seamlessly, allowing users to log in to Salesforce via Azure AD without needing to enter separate credentials. This setup enhances security, simplifies user access, and demonstrates the practical implementation of federated authentication using SAML.

Overall, this lab provides a comprehensive example of integrating cloud applications with a centralized identity provider, following best practices for enterprise SSO configurations.