



saico

Conocimiento
hecho software.

Configuración Entrald - Gente, Autogestión y Portal Azure

Instructivo de configuración

Creación

21-05-2025

Versión

1.0.0

Plantilla

SS-IC-01-ES

Código

SAICO-IC-01-ES

Autor

Maurizio Quaroni



Índice

1	Introducción	3
2	Propósito	3
3	Audiencia.....	3
4	Términos y Acrónimos	3
5	Pasos para la Configuración de Entrald en Gente-Autogestión y Portal Azure	4
5.1	Configuración en Portal Azure.....	4
5.1.1	Ingresar al portal azure	4
5.1.2	Obtener datos (Tenant Id).....	4
5.1.3	Registro de aplicación.	5
5.1.4	Permisos de Api.	6
5.1.5	Autenticación.....	6
5.1.6	Información y propiedades de la aplicación.....	7
5.1.7	Asignación requerida.....	8
5.1.8	Certificados y secretos	9
5.2	Configuración en Gente.....	11
5.2.1	Configuración Autogestión.....	11
5.2.2	Pestaña Acceso y Contraseñas.....	11
5.2.3	Configuración JSON con datos Azure	11
5.2.4	Configuración UPN.....	13
5.3	Configuración para Autogestión:.....	14
5.3.1	Configuración saicoageentraid.ini	14
5.3.2	Copiar archivo generado.	14
5.3.3	Ajuste en web.config	15
6	Verificación	15
6.1	Login única empresa	15
6.2	Escenario Multi-Empresa	16
6.2.1	Pantalla de selección de empresa.....	17



1 Introducción

El objetivo de este documento es brindar apoyo para la correcta configuración Gente y Autogestión para el correcto funcionamiento de Entrald en el sistema.

2 Propósito

Establecer las pautas necesarias para garantizar que todo lo que corresponda con Entrald se configure de manera uniforme y adecuada.

3 Audiencia

Este documento está dirigido a los equipos de las distintas áreas de SAICO que requieran comprender la configuración necesaria para el correcto funcionamiento de lo que abraza Entrald. También para aquellos clientes que necesiten configurar y/o visualizar la configuración de Entrald para su correcto funcionamiento en el sistema.

4 Términos y Acrónimos

Término	Definición o descripción
Entrald	Solución de administración de identidades y acceso de Microsoft que ayuda a las organizaciones a proteger y administrar identidades en entornos locales y en la nube.
Portal Azure	Portal donde se harán las configuraciones para generar el vínculo entre el login de Microsoft por entra id, con autogestión.



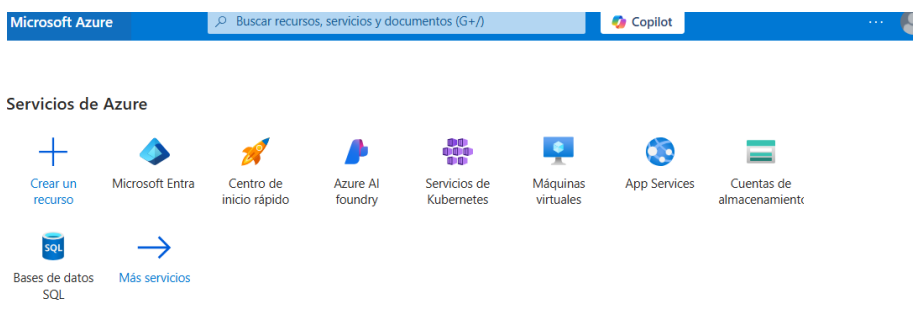
5 Pasos para la Configuración de EntraId en Gente-Autogestión y Portal Azure

5.1 Configuración en Portal Azure.

5.1.1 Ingresar al portal azure

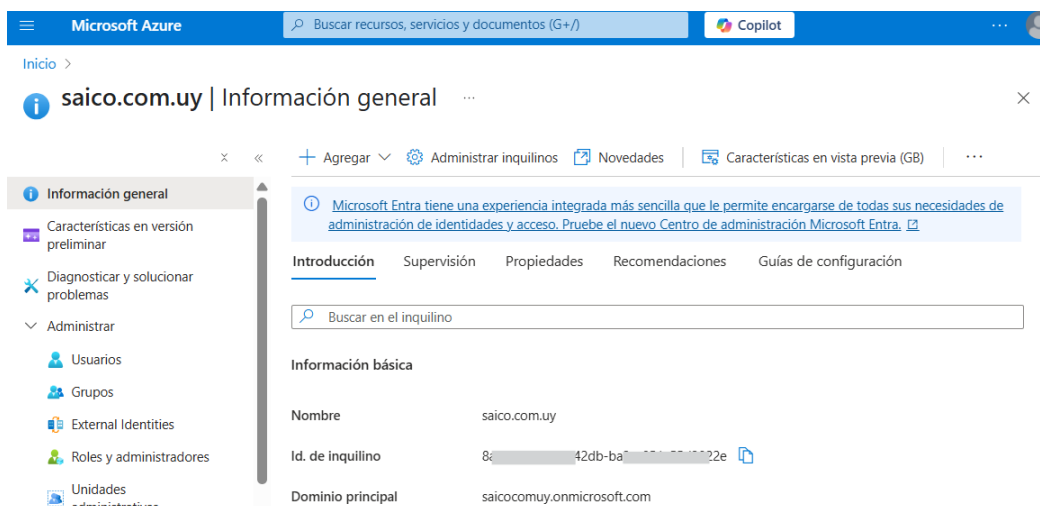
Dirigirse a: <https://azure.microsoft.com/es-es/get-started/azure-portal/>

Elegimos el servicio Microsoft Entra



5.1.2 Obtener datos (Tenant Id)

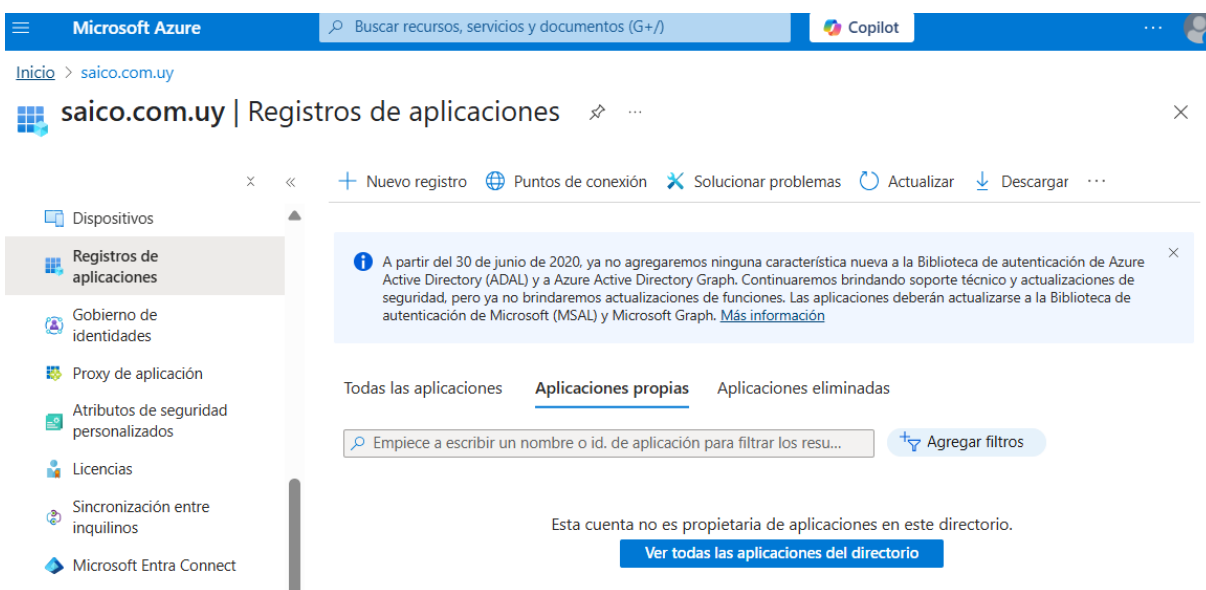
Nos llevará a la pantalla principal, donde podremos obtener el dato del TenantId (o inquilino).





5.1.3 Registro de aplicación.

Como siguiente paso debemos crear la aplicación (si no se tiene una creada). Para ello hay que dirigirse dentro del menú principal, a la opción Registro de aplicaciones y presionar sobre + Nuevo Registro.



Configuramos el tipo de cuenta compatible y confirmamos

Inicio > saico.com.uy | Registros de aplicaciones >

Registrar una aplicación

Nombre para mostrar accesible por los usuarios de esta aplicación. Se puede cambiar posteriormente.

Tipos de cuenta compatibles

¿Quién puede usar esta aplicación o acceder a esta API?

- Solo cuentas de este directorio organizativo (solo de saico.com.uy; inquilino único)
- Cuentas en cualquier directorio organizativo (cualquier inquilino de id. de Microsoft Entra - multiinquilino)
- Cuentas en cualquier directorio organizacional (cualquier inquilino del id. de Microsoft Entra - multiinquilino) y cuentas personales de Microsoft (por ejemplo, Skype, Xbox)
- Solo cuentas personales de Microsoft

[Ayudarme a elegir...](#)

URI de redirección (opcional)

Devolveremos la respuesta de autenticación a esta dirección URI después de autenticar correctamente al usuario. Este dato es opcional y se puede cambiar más tarde, pero se necesita un valor para la mayoría de los escenarios de autenticación.

Seleccionar una plataforma

Registre una aplicación en la que esté trabajando aquí. Integre aplicaciones de la galería y otras aplicaciones de fuera de la organización agregándolas desde [Aplicaciones empresariales](#).

Al continuar, acepta las directivas de la plataforma Microsoft. [?](#)

[Registrar](#)



5.1.4 Permisos de Api.

El siguiente paso sería, una vez creada la aplicación, ingresar en ella y seleccionar la opción de menú Permisos de Api.

Los permisos se asignan a partir del botón + Agregar un permiso → Microsoft Graph → Permisos Delegados y ahí marcamos las casillas de email, openid y profile.

Nombre de permiso...	Tipo	Descripción	Se necesita el conse...	Estado
Microsoft Graph (4)				
email	Delegada	Ver la dirección de correo...	No	Concedido para saico.c...
openid	Delegada	Iniciar la sesión de usuarios	No	Concedido para saico.c...
profile	Delegada	Ver el perfil básico de los ...	No	Concedido para saico.c...
User.Read	Delegada	Iniciar sesión y leer el per...	No	Concedido para saico.c...

5.1.5 Autenticación

Aquí configuraremos la uri de redirección. Luego de autenticar o cerrar sesión, Microsoft debe tener en esta sección las url válidas a las que puede redirigir.

Web Inicio rápido Docs Docs

URI de redirección

Las URI que aceptaremos como destino cuando devolvamos las respuestas de autenticación (tokens) después de autenticar o cerrar la sesión de los usuarios con éxito. La URI de redirección que se envía en la solicitud al servidor de inicio de sesión debe coincidir con una de las que se muestran aquí. También se conocen como URL de respuesta. [Más información sobre los URI de redireccionamiento y sus restricciones](#)

`http://localhost/GenteAGgxe3MQuaroni.Net/puenteauthpkcee.aspx` 🗑️



La otra configuración a tener en cuenta es la de flujos de concesión y tipos de cuenta compatibles.

Luego de cargada esa información se puede confirmar la autenticación.

Flujos de concesión implícita e híbridos

Solicite un token directamente desde el punto de conexión de autorización. Si la aplicación tiene una arquitectura de página única (SPA) y no usa el flujo de código de autorización, o si invoca una API web mediante JavaScript, seleccione los tokens de acceso y los tokens de id. Para aplicaciones web de ASP.NET Core y otras aplicaciones web que usen la autenticación híbrida, seleccione solo los tokens de id. [Obtenga más información sobre los tokens.](#)

Seleccione los tokens que quiera que emita el punto de conexión de autorización:

- Tokens de acceso (usados para flujos implícitos)
- Tokens de id. (usados para flujos híbridos e implícitos)

Tipos de cuenta compatibles

¿Quién puede usar esta aplicación o acceder a esta API?

- Solo cuentas de este directorio organizativo (solo de saico.com.uy: inquilino único)
- Cuentas en cualquier directorio organizativo (cualquier inquilino de id. de Microsoft Entra - multiinquilino)

5.1.6 Información y propiedades de la aplicación

En Aplicaciones empresariales → nombre de la aplicación, donde dice Id. de aplicación obtendremos el otro valor necesario para la configuración del archivo creado desde Gente.

[Inicio](#) > [Aplicaciones empresariales](#) | [Todas las aplicaciones](#) >

saicoagpruebaentraid | Información general ...
Aplicación empresarial

Propiedades

Nombre ⓘ
saicoagpruebaentraid

Id. de aplicación ⓘ
fc63 191-6c...

Id. de objeto ⓘ

Getting Started



5.1.7 Asignación requerida

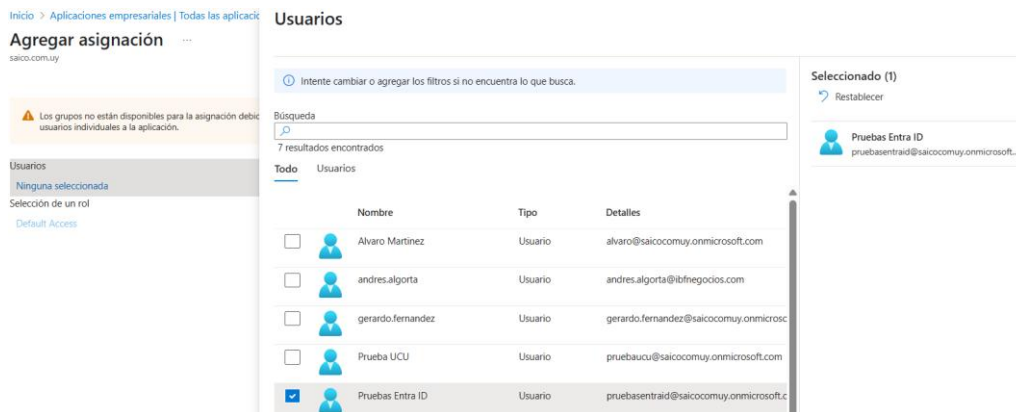
Ahora debemos dirigirnos a la opción de menú Propiedades para configurar (opcional), si para acceder a dicha aplicación se requiere estar asignado. También sirve para el escenario que por algún motivo un usuario (o grupo) no deba tener más acceso a la aplicación, quitándolo de la lista de asignados, al intentar acceder nuevamente a la aplicación ya no se le permitirá el acceso.

The screenshot shows the 'Propiedades' configuration page for the application 'saicoagpruebaentraid'. The left sidebar contains a navigation menu with options like 'Información general', 'Plan de implementación', 'Diagnosticar y solucionar problemas', and 'Administrar'. The 'Administrar' section is expanded to show 'Propiedades' selected. The main content area contains several configuration fields: '¿Habilitado para que los usuarios inicien sesión?' (Yes/No), 'Nombre' (saicoagpruebaentraid), 'Dirección URL de la página principal', 'Logotipo' (a green square with 'S'), 'Id. de aplicación' (fc635031-7511-4a8f-a191-6cbb181e0492), 'Id. de objeto' (c0045c37-8152-4121-8cc0-72ced1b30928), '¿Asignación requerida?' (Yes/No), and '¿Es visible para los usuarios?' (Yes/No).

Menú Usuarios y grupos, botón + Agregar usuario o grupo

The screenshot shows the 'Usuarios y grupos' configuration page for the application 'saicoagpruebaentraid'. The left sidebar is expanded to show 'Usuarios y grupos' selected. The main content area features a toolbar with '+ Agregar usuario o grupo', 'Editar asignación', 'Quitar asignación', and 'Actualización de credencial'. A blue information box states: 'La aplicación no aparecerá en Mis aplicaciones para los usuarios asignados. Establezca el valor que determina si es visible para los usuarios en "Sí" en las propiedades para evitarlo.' Below this, there is a text prompt: 'Asigne usuarios y grupos a roles de aplicación para su aplicación aquí. Para crear nuevos roles de aplicación para esta aplicación, utilice el registro de la aplicación'. A search bar contains the text 'Se muestran los primeros 200, busque en to...'. A table header is visible with columns 'Nombre para mostrar' and 'Tipo de objeto'. The table content shows 'No se encontraron asignaciones de aplicaciones.'

Seleccionar y asignar



Inicio > Aplicaciones empresariales | Todas las aplicaci...

Agregar asignación ...

saico.com.uy

⚠ Los grupos no están disponibles para la asignación de usuarios individuales a la aplicación.

Usuarios

Ninguna seleccionada

Selección de un rol

Default Access

Usuarios

Intente cambiar o agregar los filtros si no encuentra lo que busca.

Búsqueda

7 resultados encontrados

Todo Usuarios

	Nombre	Tipo	Detalles
<input type="checkbox"/>	Alvaro Martinez	Usuario	alvaro@saicocomuy.onmicrosoft.com
<input type="checkbox"/>	andres.algorta	Usuario	andres.algorta@bfnegocios.com
<input type="checkbox"/>	gerardo.fernandez	Usuario	gerardo.fernandez@saicocomuy.onmicrosc
<input type="checkbox"/>	Prueba UCU	Usuario	pruebaucu@saicocomuy.onmicrosoft.com
<input checked="" type="checkbox"/>	Pruebas Entra ID	Usuario	pruebasentraid@saicocomuy.onmicrosoft.c

Seleccionado (1)

Restablecer

Pruebas Entra ID
pruebasentraid@saicocomuy.onmicrosoft...



+ Agregar usuario o grupo ✎ Editar asignación 🗑 Quitar asignación 🔍 Actualización de credencial 🔄 Actualizar ⚙

ⓘ La aplicación no aparecerá en Mis aplicaciones para los usuarios asignados. Establezca el valor que determina si es visible para los usuarios en

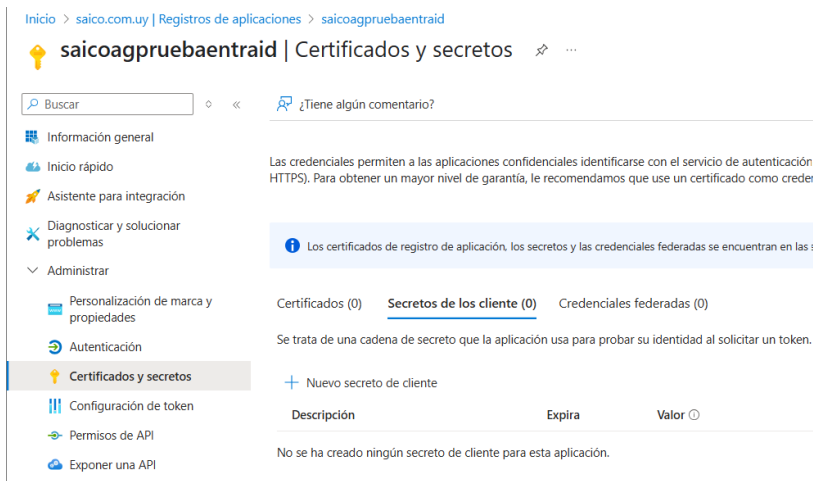
Asigne usuarios y grupos a roles de aplicación para su aplicación aquí. Para crear nuevos roles de aplicación para esta aplicación, utilice el

🔍 Se muestran los primeros 200, busque en to...

Nombre para mostrar	Tipo de objeto
<input type="checkbox"/> PE Pruebas Entra ID	User

5.1.8 Certificados y secretos

Por último, dentro de **Registro de aplicaciones → Certificados y secretos**, debemos crear una clave (secreto). Apenas se cree se tiene que guardar, ya que luego la aplicación la oculta y si se pierde se deberá generar una nueva. Este es el tercer y último ítem de los configurados en Gente para configurar el acceso a Entra Id.



Inicio > saico.com.uy | Registros de aplicaciones > saicoagpruebaentraid

saicoagpruebaentraid | Certificados y secretos ...

🔍 Buscar 🗨 ¿Tiene algún comentario?

📄 Información general

🚀 Inicio rápido

🔧 Asistente para integración

🔍 Diagnosticar y solucionar problemas

📂 Administrar

🏷 Personalización de marca y propiedades

🔄 Autenticación

🔑 Certificados y secretos

🔑 Configuración de token

🔑 Permisos de API

🔑 Exponer una API

Las credenciales permiten a las aplicaciones confidenciales identificarse con el servicio de autenticación HTTPS). Para obtener un mayor nivel de garantía, le recomendamos que use un certificado como credencial.

ⓘ Los certificados de registro de aplicación, los secretos y las credenciales federadas se encuentran en las s

Certificados (0) Secretos de los cliente (0) Credenciales federadas (0)

Se trata de una cadena de secreto que la aplicación usa para probar su identidad al solicitar un token.

+ Nuevo secreto de cliente

Descripción	Expira	Valor
No se ha creado ningún secreto de cliente para esta aplicación.		



+Nuevo secreto de cliente:

Agregar un secreto de cliente

Descripción

Expira

El valor será el dato a guardar de forma segura y a configurar en “configuración de JSON para Entra Id”

saicoagpruebaentraid | Certificados y secretos

Buscar ¿Tiene algún comentario?

- Información general
- Inicio rápido
- Asistente para integración
- Diagnosticar y solucionar problemas
- Administrar
- Personalización de marca y propiedades
- Autenticación
- Certificados y secretos**

Las credenciales permiten a las aplicaciones confidenciales identificarse con el servicio de autenticación al recibir tokens y una ubicación web direccionable (con un esquema HTTPS). Para obtener un mayor nivel de garantía, le recomendamos que use un certificado como credencial, en lugar de un secreto de cliente.

Certificados (0) **Secretos de los cliente (1)** Credenciales federadas (0)

Se trata de una cadena de secreto que la aplicación usa para probar su identidad al solicitar un token. También se conoce como contraseña de aplicación.

+ Nuevo secreto de cliente

Descripción	Expira	Valor	Id. de secreto
clave prueba	17/11/2025	vKv8...j6F3...	4...c239...



5.2 Configuración en Gente

5.2.1 Configuración Autogestión

Dirigirse al menú: Herramientas → Configuración → Opción Autogestión.

5.2.2 Pestaña Acceso y Contraseñas.

Se debe marcar el check de “Habilitar Autenticación por Entra Id”. Y eso habilitará el ícono que nos va a permitir agregar información necesaria para la conexión.

Configuración de Autogestión

Acceso y Contraseñas Adelanto de sueldo Opciones habilitadas

Autenticación

- Habilitar Autenticación por Entra Id
- Habilitar Autenticación por LDAP

Acceso a Autogestión Cédula o LDAP ▾

Contraseñas

Las contraseñas caducan cada días (999=nunca)

- Requiere contraseña segura
- Habilitar Autenticación en 2 pasos

Ver plantilla para envío de contraseñas por correo electrónico

5.2.3 Configuración JSON con datos Azure

Hacer clic en el ícono de preferencias () y nos abrirá el siguiente popup:

Configuración de JSON para EntraID

Client ID: fc635031-1e049

Tenant Id: 8a1-ba3e-8

Client Secret: 321-9155-282

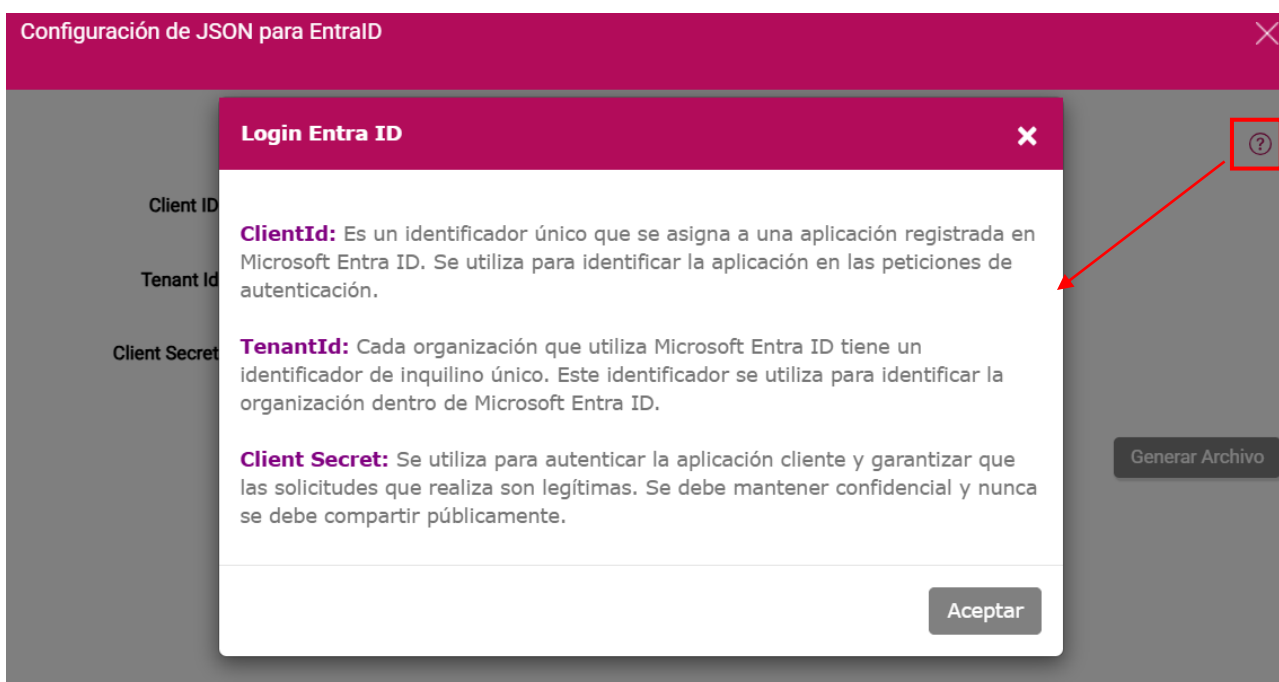
Generar Archivo

Debemos completar el Client Id, Teenant Id y Client Secret. Toda esa información la obtendremos del portal azure.



Al presionar sobre el icono '?' tendremos la definición de cada campo a completar.

Por último, luego de cargar los 3 valores, al clickear sobre **Generar Archivo** se nos generará un archivo con extensión json con la información encriptada para luego configurar en autogestión (desarrollado más adelante).



Archivo descargado ejemplo:

```
AzureAdSettings (6).json
1  {"ClientId": "zpKLTPlOfVY0gixOaEZGCMOnIQDxHRAZNEF31dAMzkU1xP8GSW7CGUhktOaeONmK",
   "TenantId": "Ck2Ibh37vG5P9s8kX+M/Q+9Gx666oDWAYGCzbFxAfHnFDHLirxFO06qEma66MhEO", "Instance": "kyVUbxPIKziBJPEpj2QXPqENALtHgK22UUazlZORFcSwMpiOjYDbT4Mae4q+rUB0", "ClientSecret": "Y6TACUEQpTaOr8gYIU7EK6p3/nNqEDt4Zef3m93gCxeA0D1s685EHK2jUrLoYBW5"}
```



5.2.4 Configuración UPN.

Como última configuración debemos agregar el upn (user principal name) en el funcionario. De esta forma se genera el vínculo a nivel de datos entre Gente/Autogestión y Entra Id.

Funcionario ✕

Número 1004 Kjhkjh Hgjhgjh, Jhfhfg Jgjhgj ⚙️

Datos personales Datos laborales/Asientos Banco/CJPPU Salud/Otros Créd. Social BROU **Autogestión**

Autogestión autorizada

Marcas

- Puede modificar las marcas de los funcionarios que supervisa
- Puede modificar los cronogramas de turno que supervisa

Accesos y Contraseñas

Usuario LDAP sasdasdasd 🔗

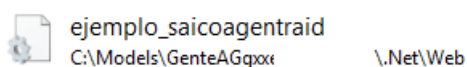
Usuario Principal Name pruebasentraid@saicomuy.onmicrosoft.com



5.3 Configuración para Autogestión:

5.3.1 Configuración saicoageentraid.ini

En dónde se encuentra instalada la aplicación de Autogestión, carpeta Web, podrán encontrar un archivo llamado ejemplo_saicoageentraid el cual se deberá copiar en la misma carpeta, pero sin el texto ejemplo_ (o simplemente renombrarlo) y ajustar la configuración.



De la siguiente manera podría quedar el archivo una vez configurado. Cada ítem explica cuales son sus opciones y como se comporta en cada caso. En este escenario, está habilitado el login con Entra Id, tiene una única empresa, se deja cargada la empresa en cuestión y por ultimo el nombre del archivo que se generó anteriormente desde Gente.

```
saicoageentraid.ini
1  habilitaEntraID=S
2  ; Opcion S: Habilita login por EntraId, Opcion N: DesHabilita login por EntraId
3  unicaEmpresaEntraID=S
4  ; En caso de tener una unica empresa marcar opcion S, si tiene mas de una empresa N
5  nombreEmpresaEntraID=genteDemoMQuaroni
6  ; Se toma en cuenta cuando unicaEmpresaEntraID = S. Toma nombreEmpresaEntraID como base
7  nombreArchivoAzure=AzureAdSettings
8  ; Nombre del archivo de configuracion de Azure para la conexion con EntraId
```

5.3.2 Copiar archivo generado.

Copiar el archivo generado en gente en el directorio Web dentro de la carpeta de instalación de Autogestión.

```
AzureAdSettings.json
1  {
2    "ClientId": "mp5TlAg59j9xZ04aacxArjwJXXJAY07z2PvSjIBZjp78dTrG7CTleDB40481NgCd",
3    "TenantId": "Ck2Ibh37vG5P9s8kX+M/Q+9Gx666oDWAYGCzbFxAfHNfDHLirxFO06qEma66MhEO",
4    "Instance": "kyVUbxPIKziBJPEpj2QXPqENALtHgK22UazlZORFcSwMpiOjYDbT4Mae4q+rUB0",
5    "ClientSecret": "mmphvDJgP1T4RkdP9g5tJ4SE9khx6IKDm6FRwzPOYtTkZB5uIsaKmI1KHVa+7zsM"
6  }
```

5.3.3 Ajuste en web.config

Se debe agregar la política de seguridad hacia <https://alcdn.msauth.net> porque Microsoft Entra Id utiliza ese dominio para cargar los scripts necesarios para el inicio de sesión. Si no se permite este dominio, el navegador bloquea esos scripts por política de seguridad, y el login no funciona correctamente.

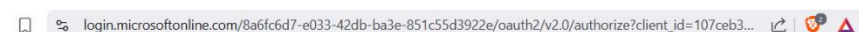
A continuación, adjunto un ejemplo de configuración del content security policy con la regla en negrita para entra id.

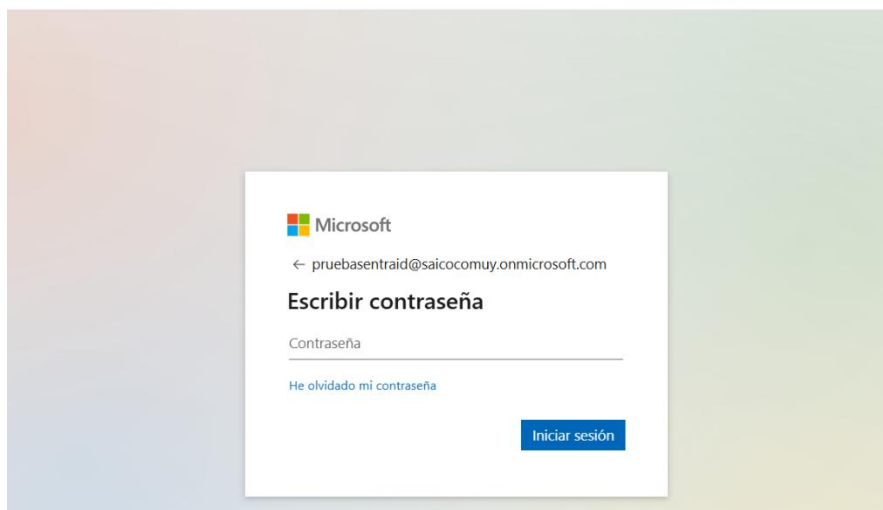
Ejemplo: `<add name="Content-Security-Policy" value="default-src 'self'; frame-ancestors 'self'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; font-src 'self' https://fonts.gstatic.com; form-action 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://alcdn.msauth.net; img-src 'self' data;"/>`

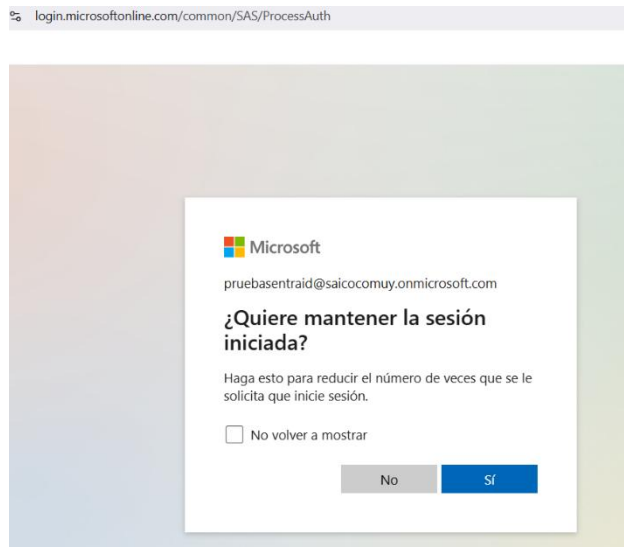
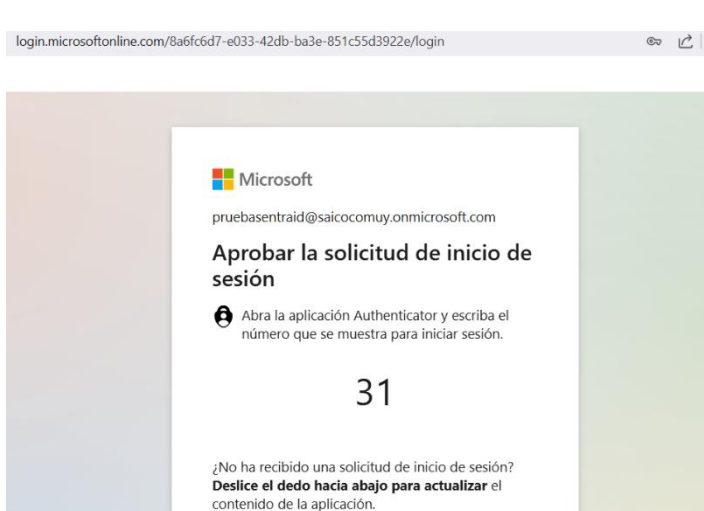
6 Verificación

1. Configurar un cliente con un email (upn) asignado a la aplicación.
2. Verificar que al dirigirse al link de login de Autogestión, automáticamente el sistema redirija al login de microsoft.
3. Ingresar las credenciales del usuario y confirmar que el acceso a la aplicación sea el correcto.

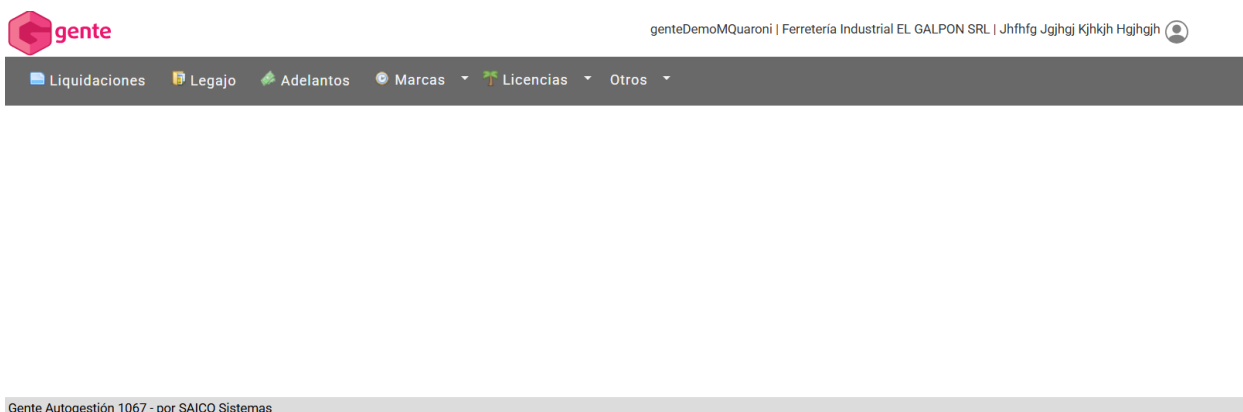
6.1 Login única empresa







Login exitoso

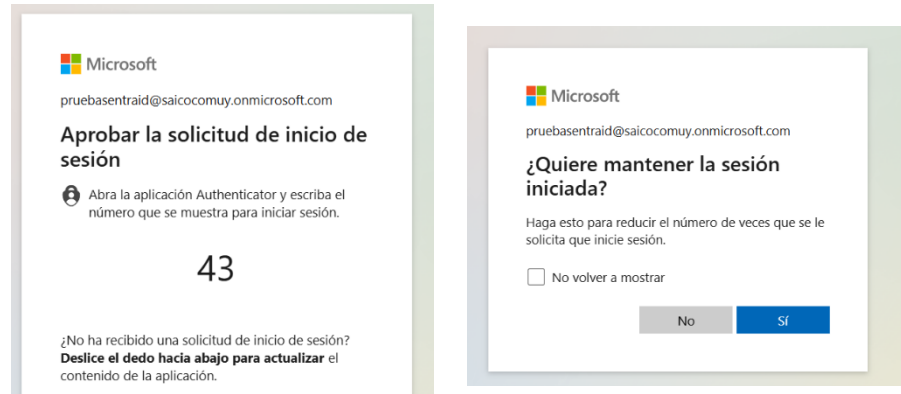


6.2 Escenario Multi-Empresa

Configuramos el .ini para que inhabilite el unicaEmpresa

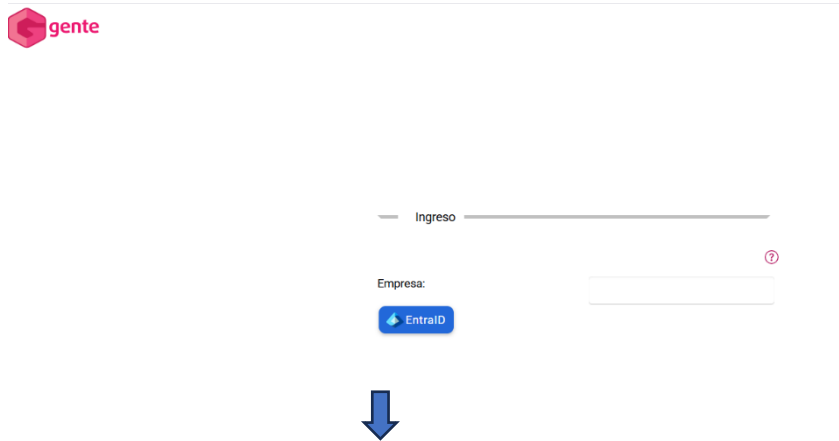
```
saicoentraid.ini
1  habilitaEntraID=S
2  ; Opcion S: Habilita login por EntraId, Opcion N: DesHabilita login por EntraId
3  unicaEmpresaEntraID=N
4  ; En caso de tener una unica empresa marcar opcion S, si tiene mas de una empresa N
5  nombreEmpresaEntraID=
6  ; Se toma en cuenta cuando unicaEmpresaEntraID = S. Toma nombreEmpresaEntraID como base
7  nombreArchivoAzure=AzureAdSettings
8  ; Nombre del archivo de configuracion de Azure para la conexion con EntraId
```

Mismo proceso de login indicando email, clave y segundo factor de autenticación.

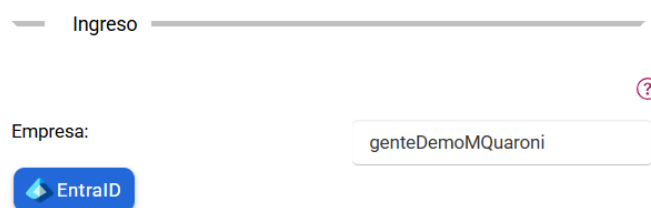


6.2.1 Pantalla de selección de empresa

El login de microsoft nos redirigirá a una pantalla intermedia con el login para ingresar la empresa del usuario.



Ingresamos la empresa y presionamos sobre el botón EntraID



Login exitoso







Historial de cambios al documento

Versión	Fecha	Autor	Detalle
1.0.0	21-05-2025	Maurizio Quaroni	Primera versión del documento