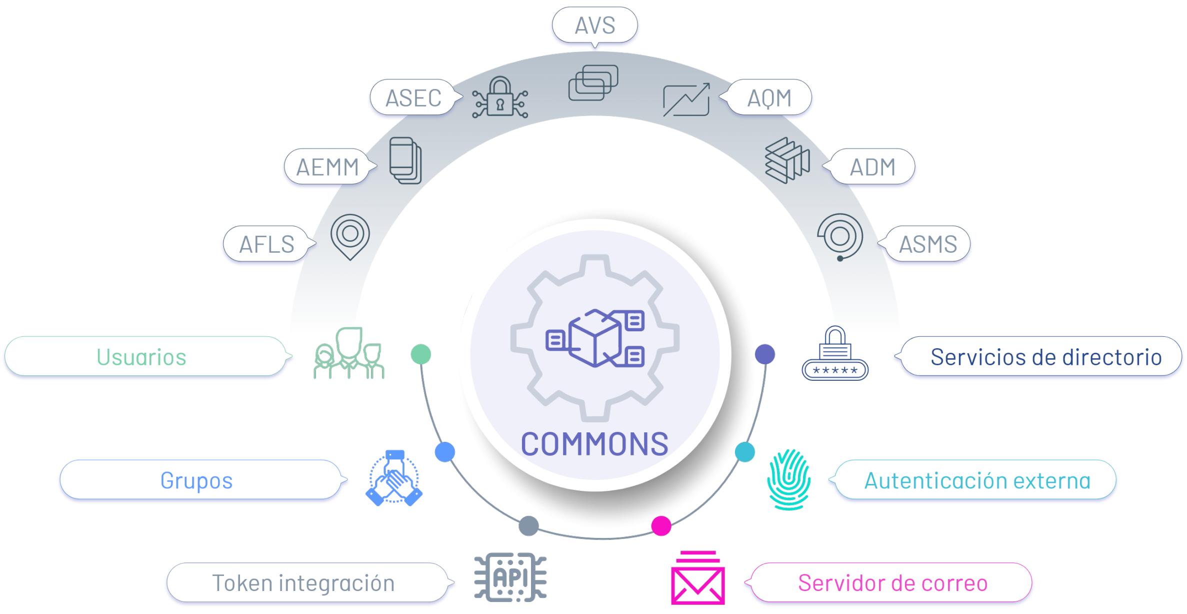
Configuración de Commons

In the configuration processes of the different Aranda applications, there are transversal concepts and functionalities that allow for the streamlining and sharing of related data for each project.

Aranda COMMONS is a library that shares components or transversal modules for the general configuration processes of Aranda products such as ASEC, AVS, AFLS, ADM, AQM.



2. Modules

The following common configuration modules integrate natively with our solutions:

Common Modules	Implemented in:

Common Modules

Implemented in:

Who is this Handbook for?

This manual is designed for users of Aranda products who share different Aranda COMMON transveral configuration modules.

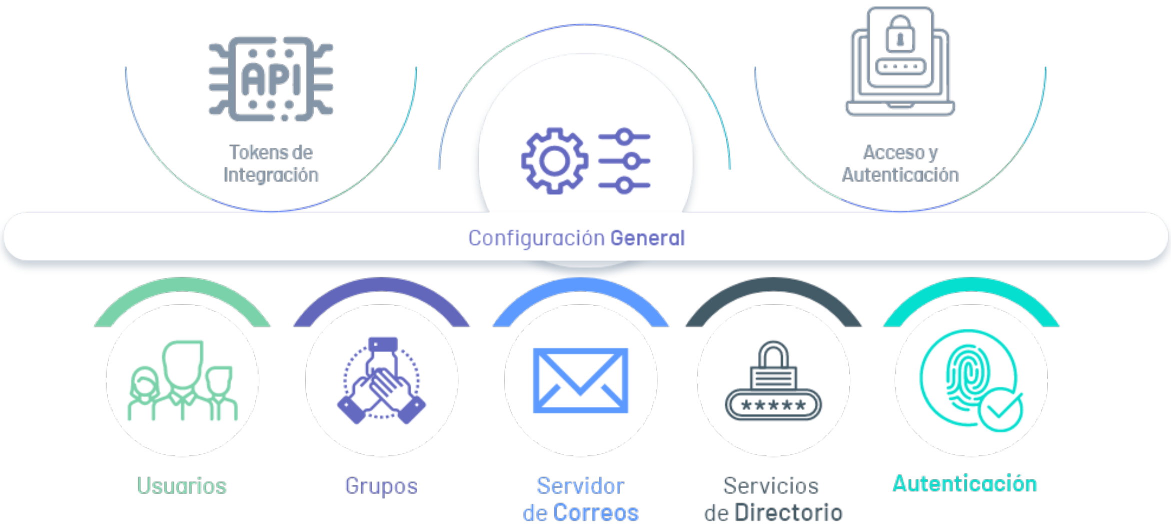
What is Our Documentation?

- ADM Integration Manual (You are HERE)

Configuration Modules

Common Modules

The general administrator from the Web console will be able to perform the following traversal configuration tasks:



1. Users

In this module you will be able to configure the users in charge of the different management processes of Aranda products. These configurations can only be made by a user with an administrator role. Additionally, you can associate groups and roles.

For more information, see the User Management ↪.

2. User groups

In this module, you will be able to configure and manage user groups to perform role assignment in a more efficient way.

For more information, see the Group Management ↪.

3. Mail Server

In this module you will be able to configure a mail provider for the operation of Aranda products; Notifications will be sent to users from this server. The email is configured to be able to perform password recovery for users who have been created manually (It does not apply to those who are imported).

For more information, see the Mail Server Management ↪.

4. Directory Services

In this module, you can set the directory services that can be used in an Aranda application, such as the lightweight directory access protocol LDAP, which allows you to configure the connection to other business directories or the directory service Azure Active Directory

For more information, see the [Management Directory ↪ Services](#).

5. Authentication Providers

In this module, you can set the external authentication providers, which follow the SAML (Security Assertion Markup Language) standard to perform user authentication in the application. and subsequent and notification on the status of the validation.

For more information, see the [Authentication Provider ↪ Management](#).

6. Integration Tokens

In this module, you will be able to perform the API connection configuration and add details for the creation of the Token. This token allows the APIs of the product that requires it to be consumed, from external applications, without the need for authentication credentials.

For more information, see the [Integration ↪ Token Management](#).

Environment Commons

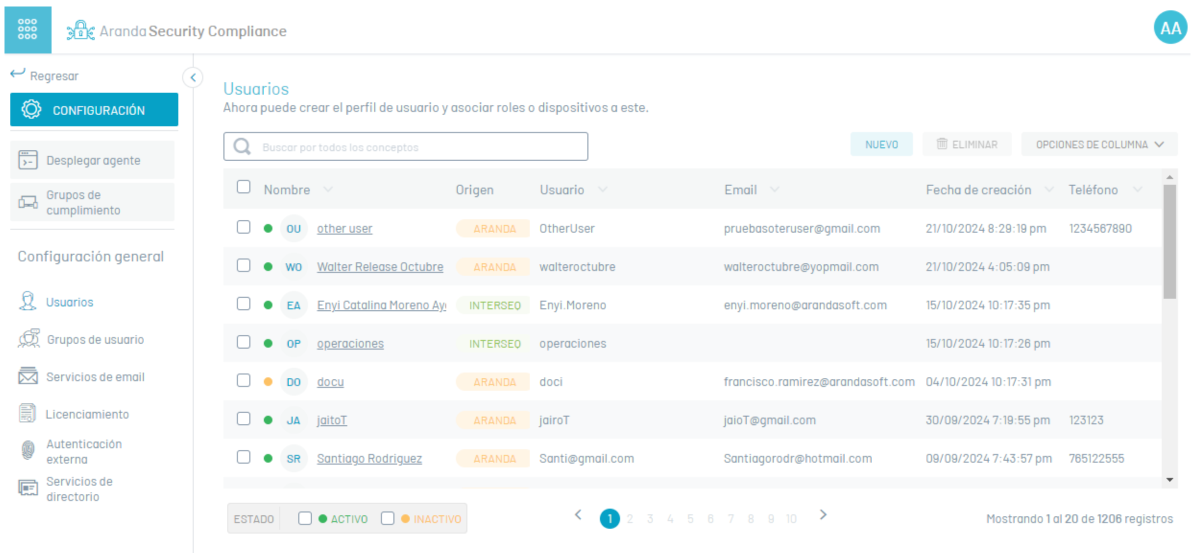
The management and configuration of the configuration processes for different Aranda applications are carried out from a web environment with shared options and actions.

Visualize Environment

1. After logging in, log in to the product's web console with the role set (admin, specialist, users).

2. In the main menu of the Aranda product, in the **Configuration**, select the respective module (Users, Mail Server, External Authentication, Directory Services, Integration Tokens) and doing so enables the information view with the related data.

> ⚐ **Example:** In the following image you can see the configuration section of the Aranda Security product, with the common modules used.



Usuarios

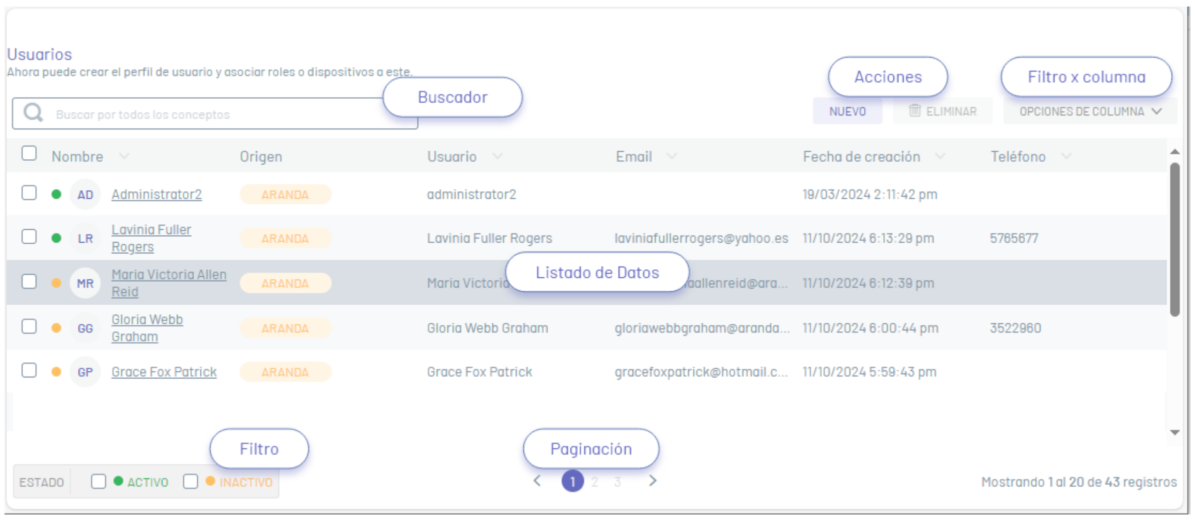
Ahora puede crear el perfil de usuario y asociar roles o dispositivos a este.

□	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
□ ●	OU other user	ARANDA	OtherUser	pruebasoteruser@gmail.com	21/10/2024 8:29:19 pm	1234567890
□ ●	WO Walter Release Octubre	ARANDA	walteroctubre	walteroctubre@yopmail.com	21/10/2024 4:05:09 pm	
□ ●	EA Enyi Catalina Moreno Ay	INTERSEQ	Enyi.Moreno	enyi.moreno@arandasoft.com	15/10/2024 10:17:35 pm	
□ ●	OP operaciones	INTERSEQ	operaciones		15/10/2024 10:17:26 pm	
□ ●	DO docu	ARANDA	doci	francisco.ramirez@arandasoft.com	04/10/2024 10:17:31 pm	
□ ●	JA jaitoT	ARANDA	jairoT	jaioT@gmail.com	30/09/2024 7:19:55 pm	123123
□ ●	SR Santiago Rodriguez	ARANDA	Santi@gmail.com	Santiagorodr@hotmail.com	09/09/2024 7:43:57 pm	765122555

Mostrando 1 al 20 de 1206 registros

Environment Commons/ Modules

3. In the information view of the selected common module (Users, Mail Server, Directory Services, External Authentication) you can find transversal actions that complement the management tasks such as:



Usuarios

Ahora puede crear el perfil de usuario y asociar roles o dispositivos a este.

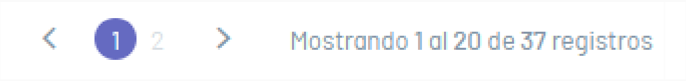
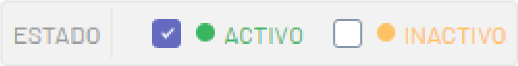
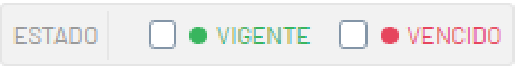
Buscar por todos los conceptos

	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
AD	Administrator2	ARANDA	administrator2		19/03/2024 2:11:42 pm	
LR	Lavinia Fuller Rogers	ARANDA	Lavinia Fuller Rogers	laviniafullerrogers@yahoo.es	11/10/2024 6:13:29 pm	5765677
MR	Maria Victoria Allen Reid	ARANDA	Maria Victoria	aallenreid@ara...	11/10/2024 6:12:39 pm	
GG	Gloria Webb Graham	ARANDA	Gloria Webb Graham	gloriawebbgraham@aranda...	11/10/2024 6:00:44 pm	3522960
GP	Grace Fox Patrick	ARANDA	Grace Fox Patrick	gracefoxpatrick@hotmail.c...	11/10/2024 5:59:43 pm	

Mostrando 1 al 20 de 43 registros

Below are the available options and the commons modules where they are used:

Option	Description	Common Modules
Search	It allows you to search for the list of users according to the search criteria. You can search by the name of the defined fields of each associated concept. Buscar por todos los conceptos	👥 ☝ ✉ 🔒 API
Data Listing	This section groups the information from the found records by selected module or item. The information presented is grouped into columns with the data entered. By selecting the record from the available list, you will be able to view and edit the associated data, or delete the record.	👥 ☝ ✉ 🔒 API
New	This button defines the action to create a record for each Aranda product management concept. Activating this action enables a window to fill in the related information. NUEVO	👥 ☝ ✉ 🔒

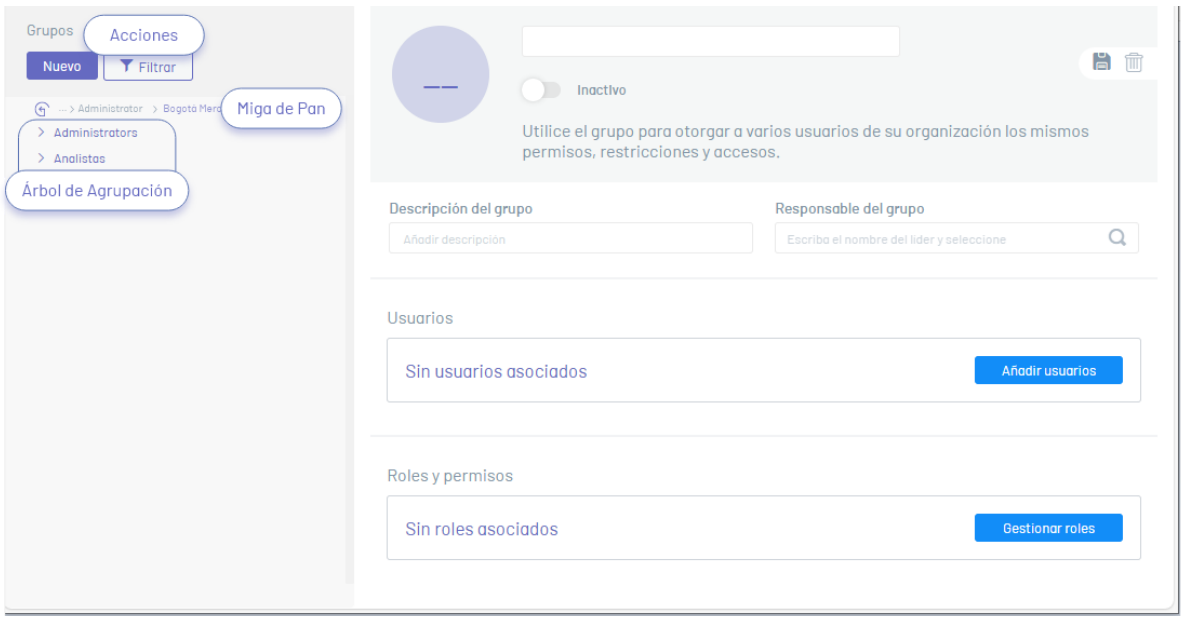
Option	Description	Common Modules
Eliminate	This button defines the action for deleting a record that has already been created in the management processes. 	👥 🫆 ✉ 🔒 API
Filter by column	Allows you to show or hide options from the list. The column options of the users module are: Name, origin, user, email, date of creation and phone.	👥
Pagination	It allows you to navigate between the pages of the list of user records found.  Mostrando 1 al 20 de 37 registros	👥 🫆 ✉ 🔒 API
Filter by Status	Allows you to filter by the active or inactive status of users or authentication providers.  ESTADO ☑ ● ACTIVO □ ● INACTIVO In the Integration Tokens module, you allow you to filter by the current or expired status of API connection tokens created.  ESTADO □ ● VIGENTE □ ● VENCIDO	👥 🫆 🔒 API
Safety	This button 	🔒

Option	Description	Common Modules
	defines the action to perform the reCAPTCHA settings to use it at the time of user authentication.	

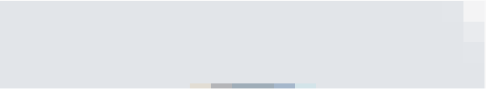
Commons Environment/ Groups Module

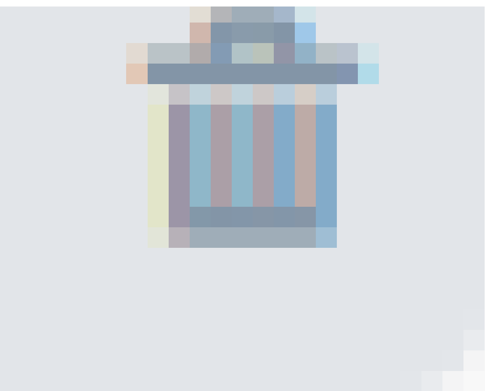
4. In the information view of the selected common module (Groups) you can find actions that complement the management tasks.

5. In the tree-like structure for user groups, you can identify the following components:



Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

Option	Description	Common Modules
New	This button Nuevo Defines the action for creating a User Groups record. Activating this action enables a window to fill in the related information.	
Filter	This button Filtrar Defines the action to perform an advanced search through the entire group tree. Activating this action enables a window to fill in the related information	
Grouping tree	This section displays the defined groups and subgroups.	
	This button 	

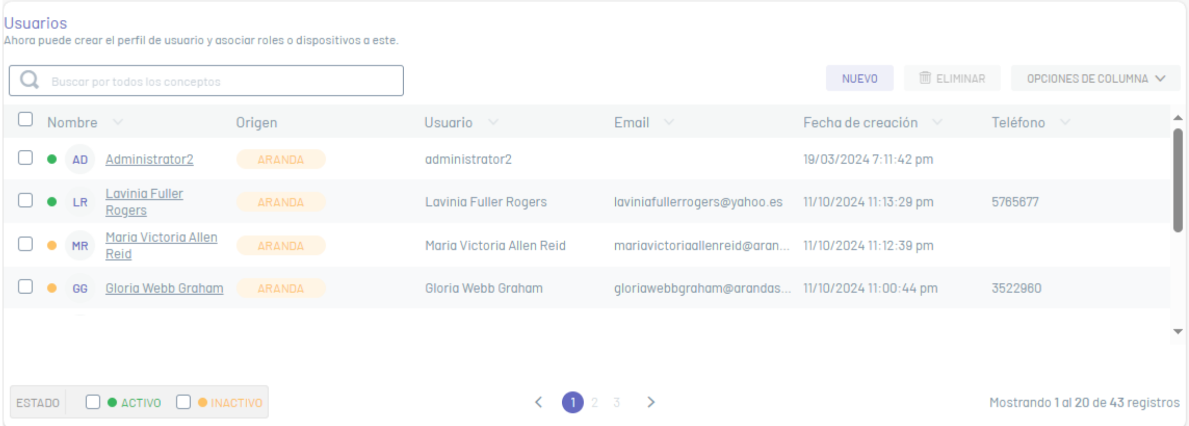
Option	Description	Common Modules
Eliminate	 Defines the action to delete an already created group record	
Breadcrumbs	This icon Displays the current location in the group tree.	
Add Users	This button Defines the action for associating users with an established group.	
Manage Roles	This button Gestionar roles Defines the action for associating roles with an established group.	

Users Module

User Management

View Users

1. In the Users information view, you can view the list of registered or imported users, grouped by data such as:



Usuarios

Ahora puede crear el perfil de usuario y asociar roles o dispositivos a este.

Buscar por todos los conceptos

NUEVO | ELIMINAR | OPCIONES DE COLUMNA

	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
□ ● AD	Administrator2	ARANDA	administrator2		19/03/2024 7:11:42 pm	
□ ● LR	Lavinia Fuller Rogers	ARANDA	Lavinia Fuller Rogers	laviniafullerrogers@yahoo.es	11/10/2024 11:13:29 pm	5765677
□ ● MR	Maria Victoria Allen Reid	ARANDA	Maria Victoria Allen Reid	mariavictoriaallenreid@aran...	11/10/2024 11:12:39 pm	
□ ● GG	Gloria Webb Graham	ARANDA	Gloria Webb Graham	gloriawebbgraham@arandas...	11/10/2024 11:00:44 pm	3522960

ESTADO □ ● ACTIVO □ ● INACTIVO

Mostrando 1 al 20 de 43 registros

Field	Field Type	Description
Name	Text	Name with which the user identifies himself.
Origin	Text	Indicates the origin by which the user was created
User	Text	Name used by the user to access the application.
Email	Text	User’s email to receive information.
Date of creation	Selector	Indicates whether the user is active or inactive.
Telephone	Text	User’s phone number.

⚐ **Note:** The Column **Origin** indicates the name of the directory service that imported the user; if the source name is **Aranda** They are users that were not imported but were created directly from this interface.

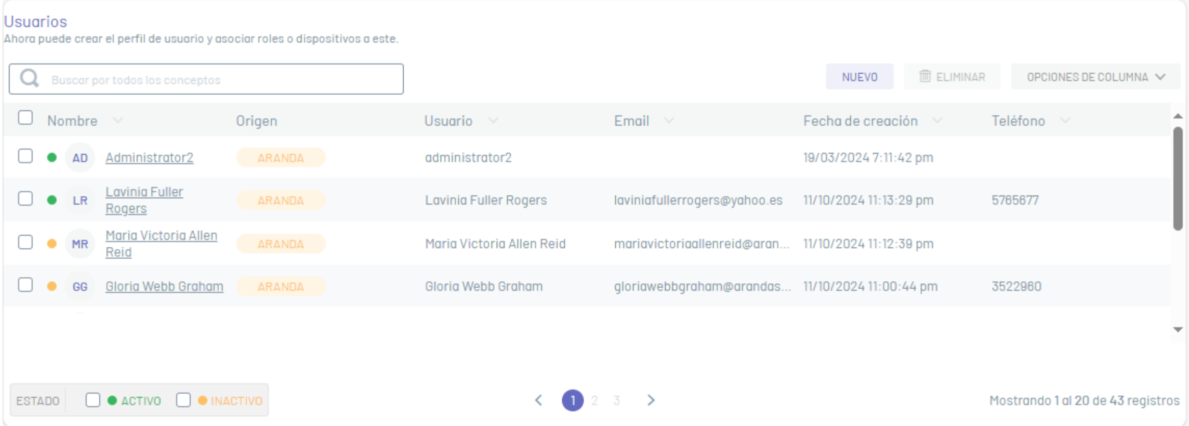
2. In the user information view, you will have information management and organization actions enabled.[Information View in Commons Environment]

▯ Related Links:

- Create Users
- Edit Users
- Delete Users

Create users

1. To create a new user, in the user information view, click the **New**.



Usuarios
Ahora puede crear el perfil de usuario y asociar roles o dispositivos a este.

Buscar por todos los conceptos | NUEVO | ELIMINAR | OPCIONES DE COLUMNA

□	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
□	● AD Administrator2	ARANDA	administrator2		19/03/2024 7:11:42 pm	
□	● LR Lavinia Fuller Rogers	ARANDA	Lavinia Fuller Rogers	laviniafullerrogers@yahoo.es	11/10/2024 11:13:29 pm	5765677
□	● MR Maria Victoria Allen Reid	ARANDA	Maria Victoria Allen Reid	mariavictoriaallenreid@aran...	11/10/2024 11:12:39 pm	
□	● GG Gloria Webb Graham	ARANDA	Gloria Webb Graham	gloriawebbgraham@arandas...	11/10/2024 11:00:44 pm	3522960

ESTADO □ ● ACTIVO □ ● INACTIVO

< 1 2 3 >

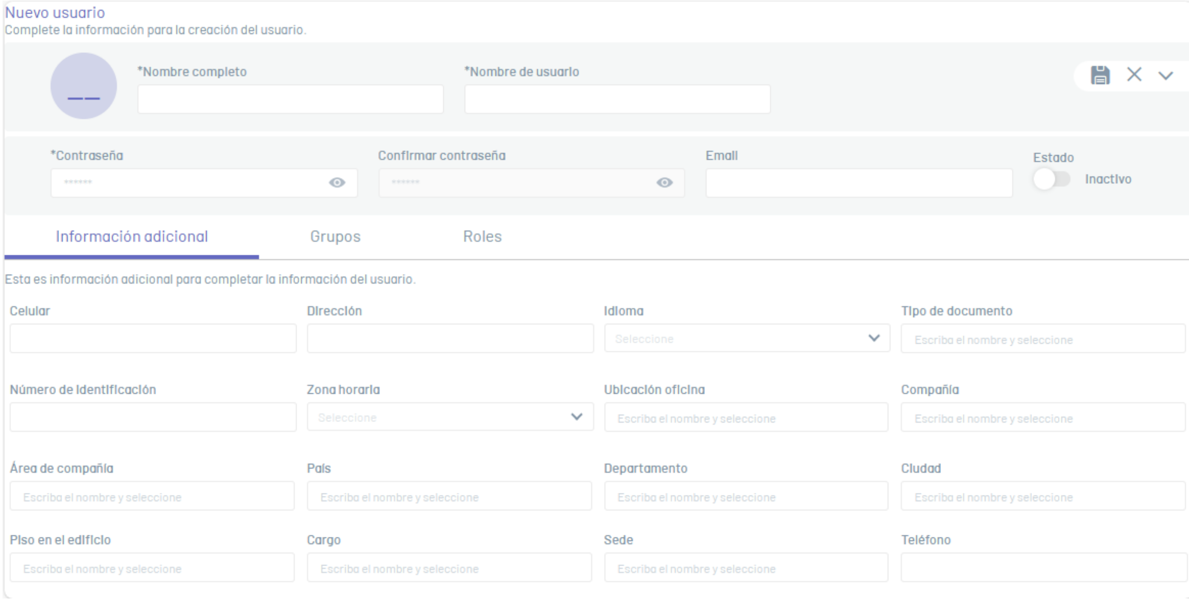
Mostrando 1 al 20 de 43 registros

⚐ **Nota:** No podrá crear un usuario con el mismo **nombre de usuario** a menos que pertenezca a otro proveedor de autenticación.

Basic Facts

2. In the window that is enabled you will be able to fill in the basic user data, additional information, association of groups and roles.

3. In the user’s basic data, you can enter fields such as name, password, email, and status. Each of the user’s fields must take into account the Specifications for Common Fields



Nuevo usuario

Complete la información para la creación del usuario.

Esta es información adicional para completar la información del usuario.

Celular
Dirección
Idioma
Seleccione
Tipo de documento
Escriba el nombre y seleccione
Número de identificación
Zona horaria
Seleccione
Ubicación oficina
Escriba el nombre y seleccione
Compañía
Escriba el nombre y seleccione
Área de compañía
Escriba el nombre y seleccione
País
Escriba el nombre y seleccione
Departamento
Escriba el nombre y seleccione
Ciudad
Escriba el nombre y seleccione
Piso en el edificio
Escriba el nombre y seleccione
Cargo
Escriba el nombre y seleccione
Sede
Escriba el nombre y seleccione
Teléfono

Additional Information

4. On the **Additional information** Enter the following fields: Cell phone number, address, language, phone, among others. Each of the user's fields must take into account the [Specifications for Fields](#)

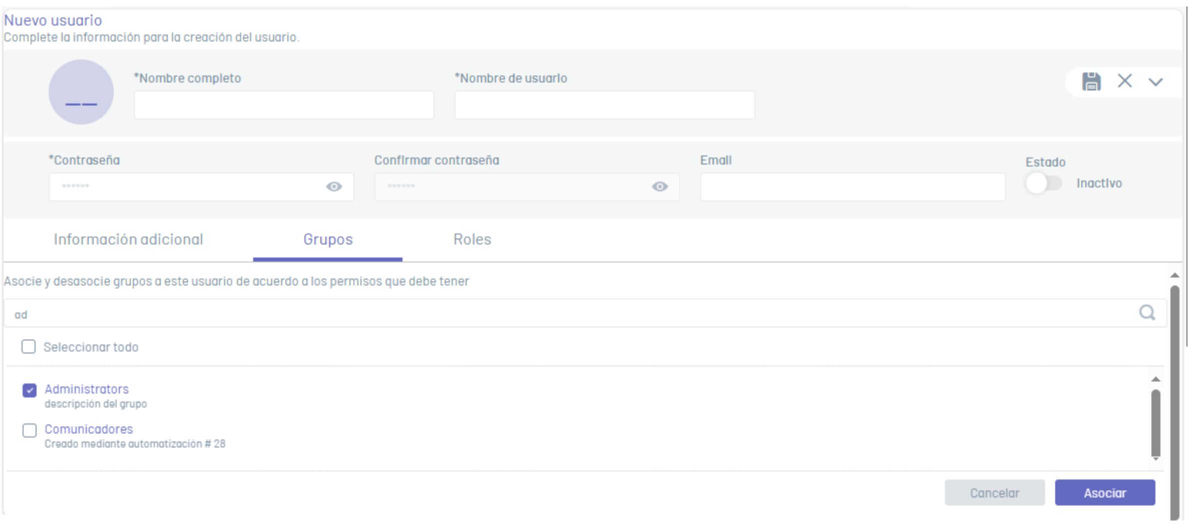
⚐ **Note:** Additional User Information is optional and is not required for user creation.

Association and disassociation of Groups

5. On the **Groups**, in the search field for associating groups, you can relate the user, the required User Group(s).

6. Select one or all of the required groups and click the**Associate**.

⚐ **Note:** In the search field for associating groups, groups that are not imported and are active will appear.



Nuevo usuario

Complete la información para la creación del usuario.

Asocie y desasocie grupos a este usuario de acuerdo a los permisos que debe tener

ad

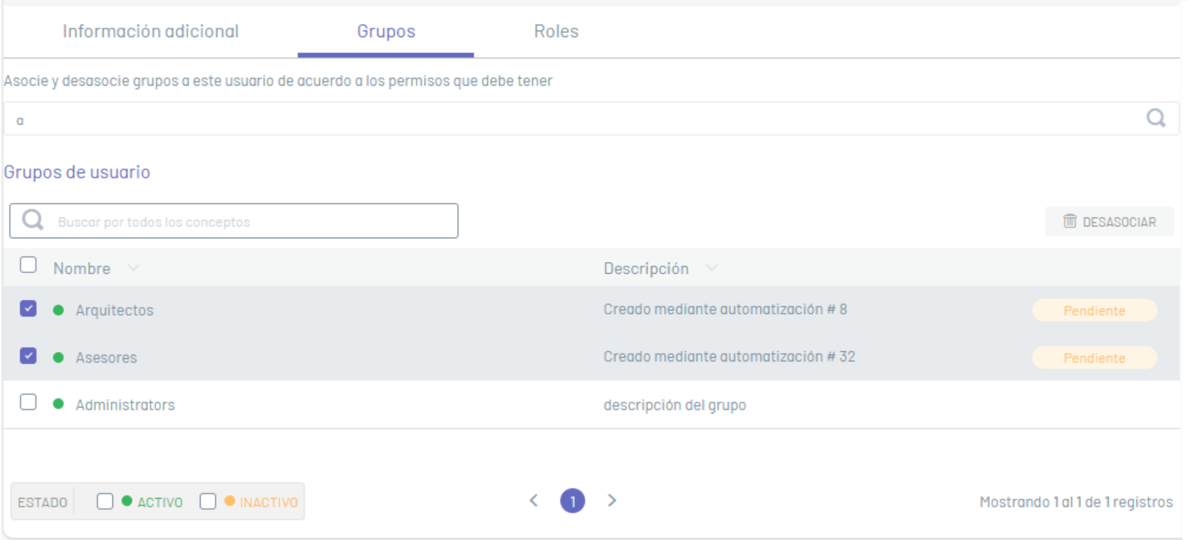
□ Seleccionar todo

☑ Administrators
descripción del grupo

□ Comunicadores
Creado mediante automatización # 28

7. The associated groups can be displayed in the list of user groups. 8. To search for groups that belong to the user, you can use the search bar for already associated groups. Groups in state **earring** They do not allow filtering, or searching by text.

9. To disassociate a group, select a record from the list of user groups and click the**Disassociate**.



Asocie y desasocie grupos a este usuario de acuerdo a los permisos que debe tener

a

Grupos de usuario

□	Nombre	Descripción	
☑	● Arquitectos	Creado mediante automatización # 8	Pendiente
☑	● Asesores	Creado mediante automatización # 32	Pendiente
□	● Administrators	descripción del grupo	

ESTADO □ ● ACTIVO □ ● INACTIVO

Mostrando 1 al 1 de 1 registros

⚐ Note:

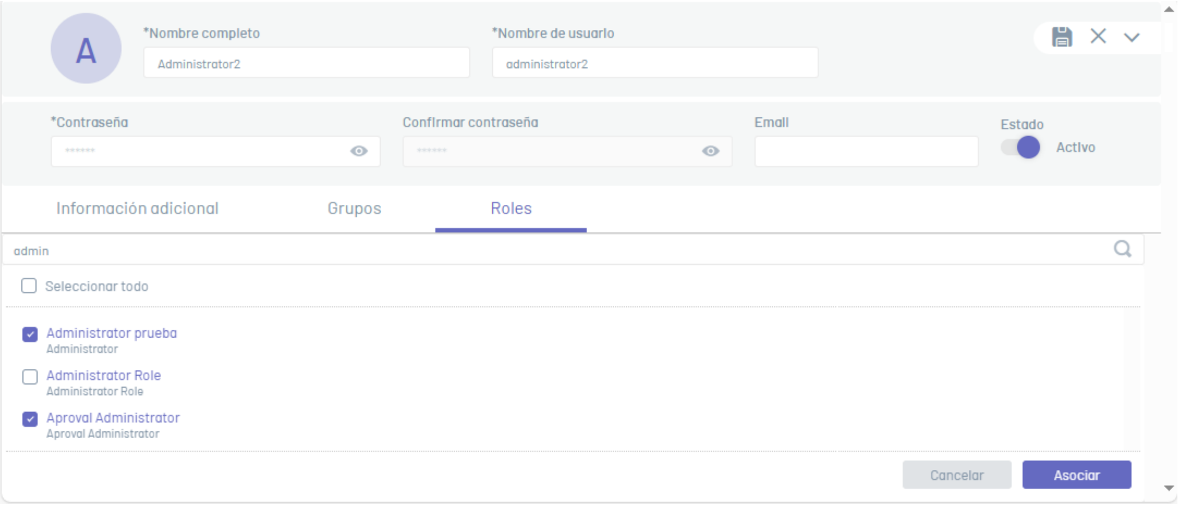
- All roles in the group will be inherited to users who belong to this group.
- If the changes have not been saved, a column will appear with the messageEarring which means that the changes have not been saved and do not yet belong to the user.

Association and disassociation of Roles

10. On the Roles, in the search field to associate roles, you can relate the roles to the selected user, according to the permissions you set.

11. Select one or all of the roles you want to relate and click the **Associate**.

⚐ **Note:** Only active roles will appear in the search field for associating roles.



*Nombre completo: Administrator2

*Nombre de usuario: administrator2

*Contraseña: ******

Confirmar contraseña: ******

Email:

Estado: Activo

admin

☐ Seleccionar todo

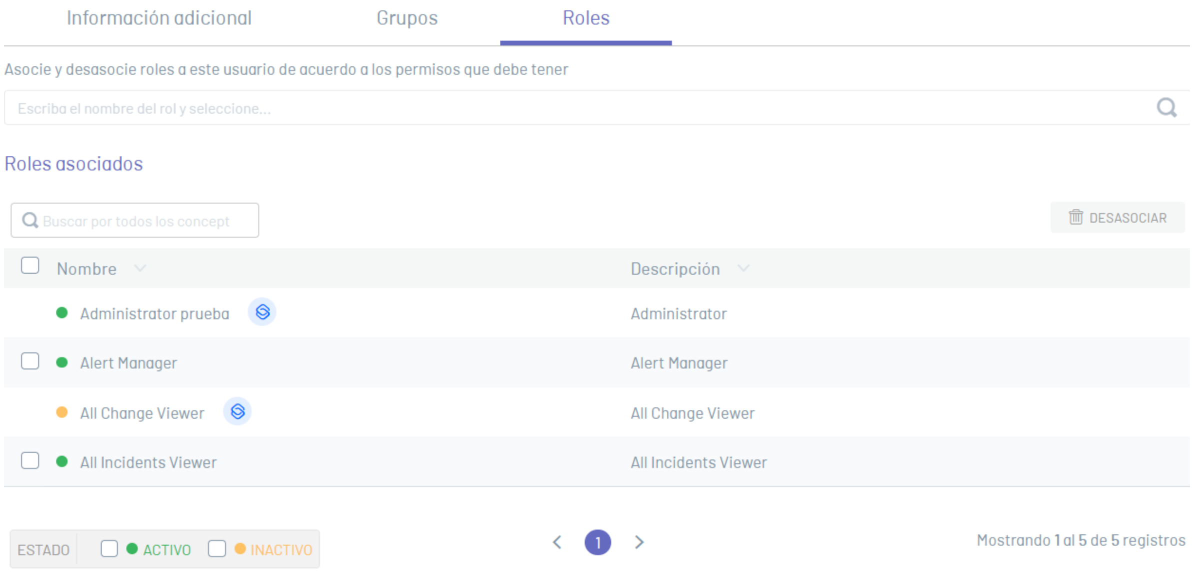
☑ Administrator prueba
Administrator

☐ Administrator Role
Administrator Role

☑ Aproval Administrator
Aproval Administrator

12. The associated roles can be displayed in the list of user roles. 13. To search for roles that belong to the user, you can use the search bar for roles already associated with the user. Roles in status **earring** They do not allow filtering, or searching by text.

14. To detach a role, select a record from the list of user roles and click the **Disassociate**.



Asocie y desasocie roles a este usuario de acuerdo a los permisos que debe tener

Escriba el nombre del rol y seleccione...

Roles asociados

Buscar por todos los concept

☐ Nombre	Descripción
● Administrator prueba	Administrator
☐ ● Alert Manager	Alert Manager
● All Change Viewer	All Change Viewer
☐ ● All Incidents Viewer	All Incidents Viewer

ESTADO ☐ ● ACTIVO ☐ ● INACTIVO

Mostrando 1 al 5 de 5 registros

⚐ Note:

- If the role is in a state **Earring** It is because the user's information has not been saved and therefore has not been associated with the user.

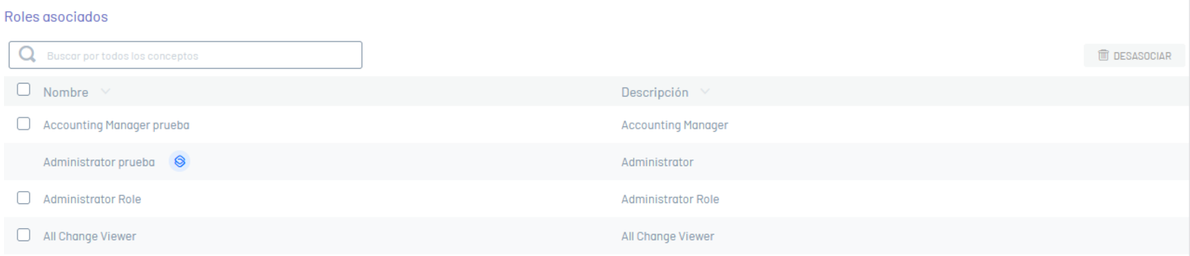
15. When you finish setting up the new user, click the **Save**

to confirm the changes made.

> ⚐ **Note:** : All users created by this means are of type **Aranda**, this value is displayed in the **Origin** in the list of users.

16. If the user belongs to a group, the group will inherit the roles from the group. Each role is identified by the

and it can only be disassociated by removing the user from the group.



Roles asociados

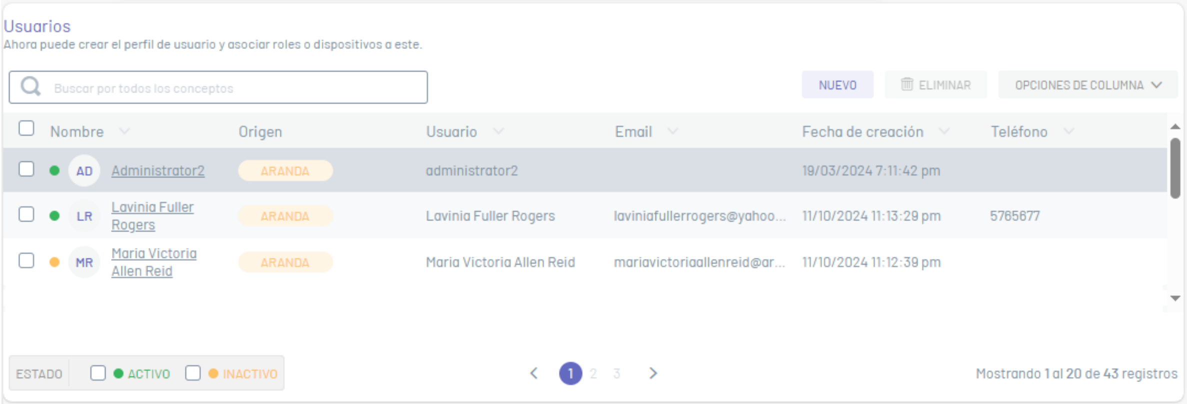
Buscar por todos los conceptos

DESASOCIAR

□ Nombre	Descripción
□ Accounting Manager prueba	Accounting Manager
Administrator prueba	Administrator
□ Administrator Role	Administrator Role
□ All Change Viewer	All Change Viewer

Edit users

1. To modify a user, in the user information view, select a record from the list of existing users.



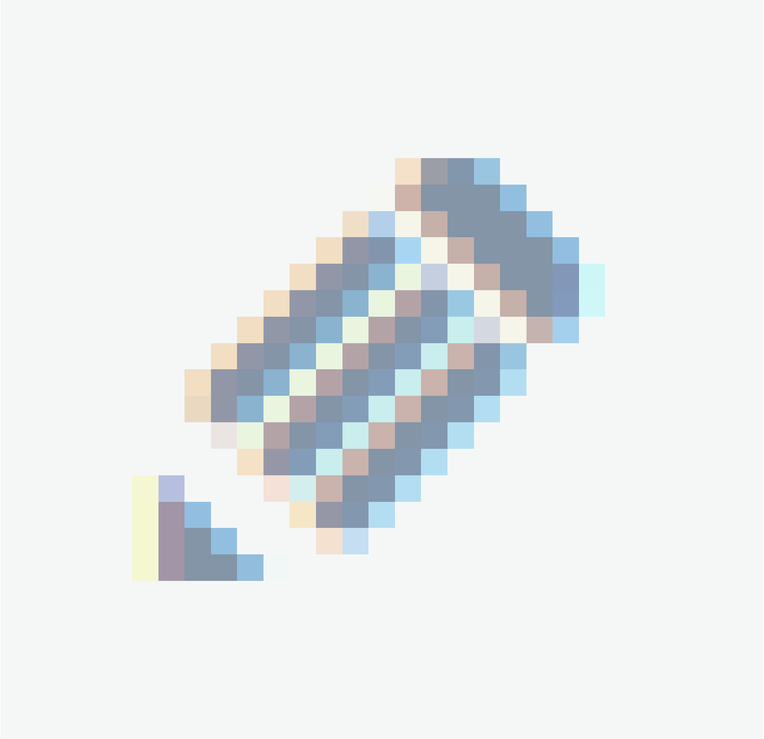
Usuarios

Ahora puede crear el perfil de usuario y asociar roles o dispositivos a este.

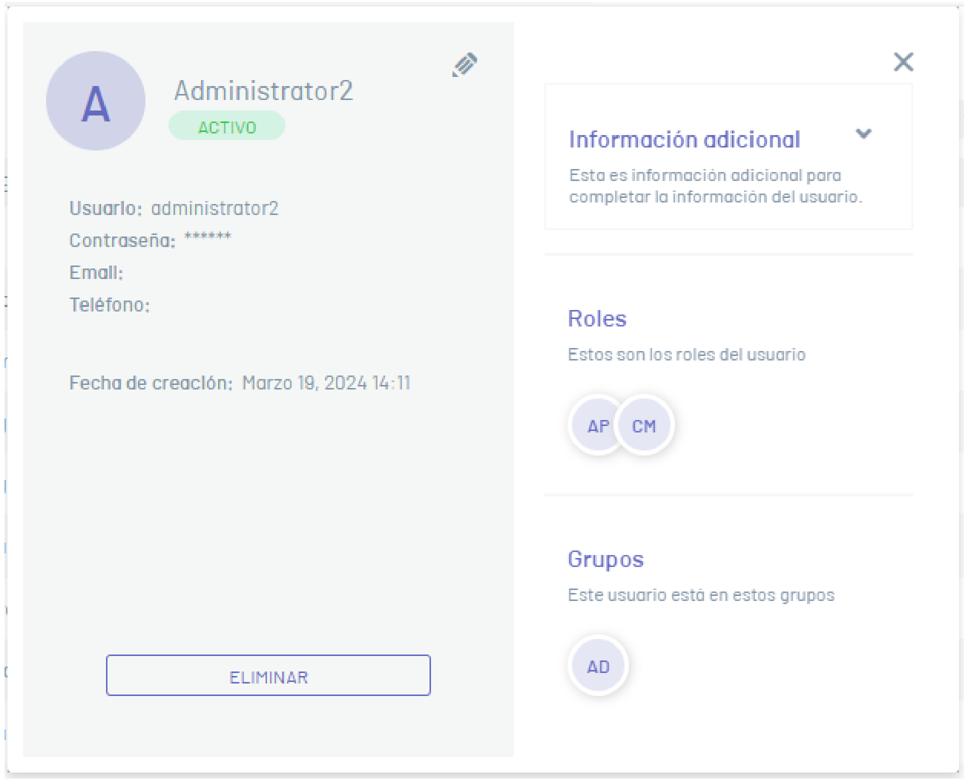
□	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
□ ●	AD Administrator2	ARANDA	administrator2		19/03/2024 7:11:42 pm	
□ ●	LR Lavinia Fuller Rogers	ARANDA	Lavinia Fuller Rogers	laviniafullerrogers@yahoo...	11/10/2024 11:13:29 pm	5765677
□ ●	MR Maria Victoria Allen Reid	ARANDA	Maria Victoria Allen Reid	mariavictoriaallenreid@ar...	11/10/2024 11:12:39 pm	

Mostrando 1 al 20 de 43 registros

2. In the user's detail view, click the **Edit**



and modify the required information.



Administrator2

ACTIVO

Usuario: administrator2

Contraseña: ******

Email:

Teléfono:

Fecha de creación: Marzo 19, 2024 14:11

Información adicional

Esta es información adicional para completar la información del usuario.

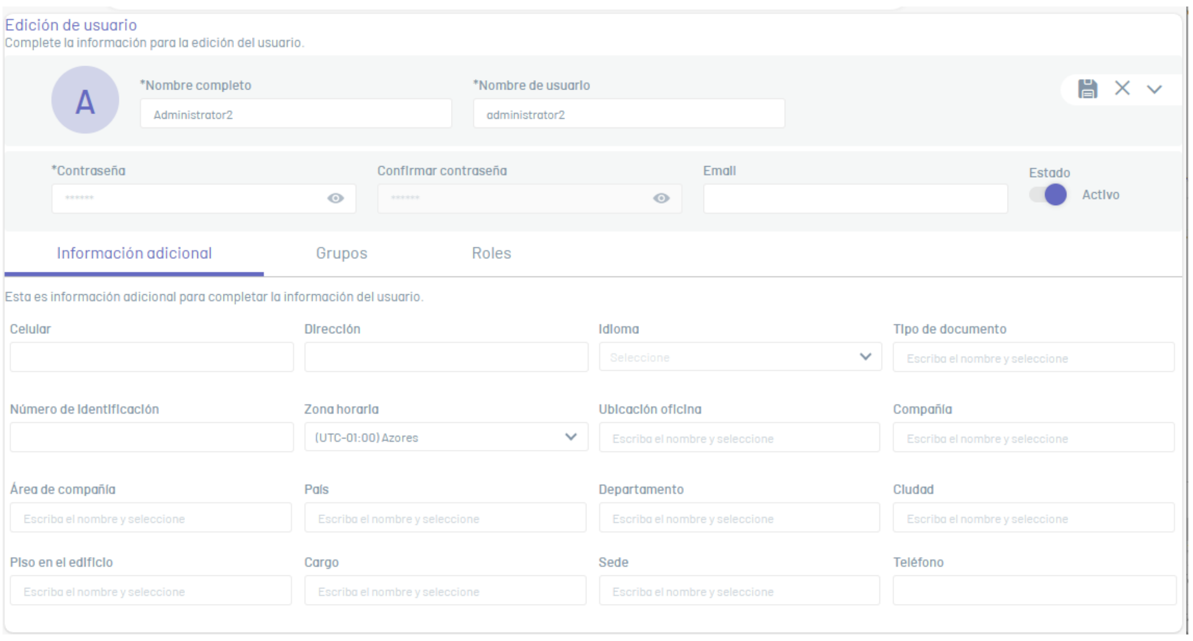
Roles

Estos son los roles del usuario

Grupos

Este usuario está en estos grupos

2. In the window **User Edition** you will be able to update the user's basic and additional information; as well as the groups and roles associated with the user.



Edición de usuario

Complete la información para la edición del usuario.

*Nombre completo: Administrator2

*Nombre de usuario: administrator2

*Contraseña: ******

Confirmar contraseña: ******

Email

Estado: Activo

Esta es información adicional para completar la información del usuario.

Celular

Dirección

Idioma: Seleccione

Tipo de documento: Escriba el nombre y seleccione

Número de identificación

Zona horaria: (UTC-01:00) Azores

Ubicación oficina: Escriba el nombre y seleccione

Compañía: Escriba el nombre y seleccione

Área de compañía: Escriba el nombre y seleccione

País: Escriba el nombre y seleccione

Departamento: Escriba el nombre y seleccione

Ciudad: Escriba el nombre y seleccione

Piso en el edificio: Escriba el nombre y seleccione

Cargo: Escriba el nombre y seleccione

Sede: Escriba el nombre y seleccione

Teléfono

⚐ **Note:** Only users of the Aranda provider may be modified. Imported users only allow associating and unassociating roles, modifying the state, language, and time zone fields.

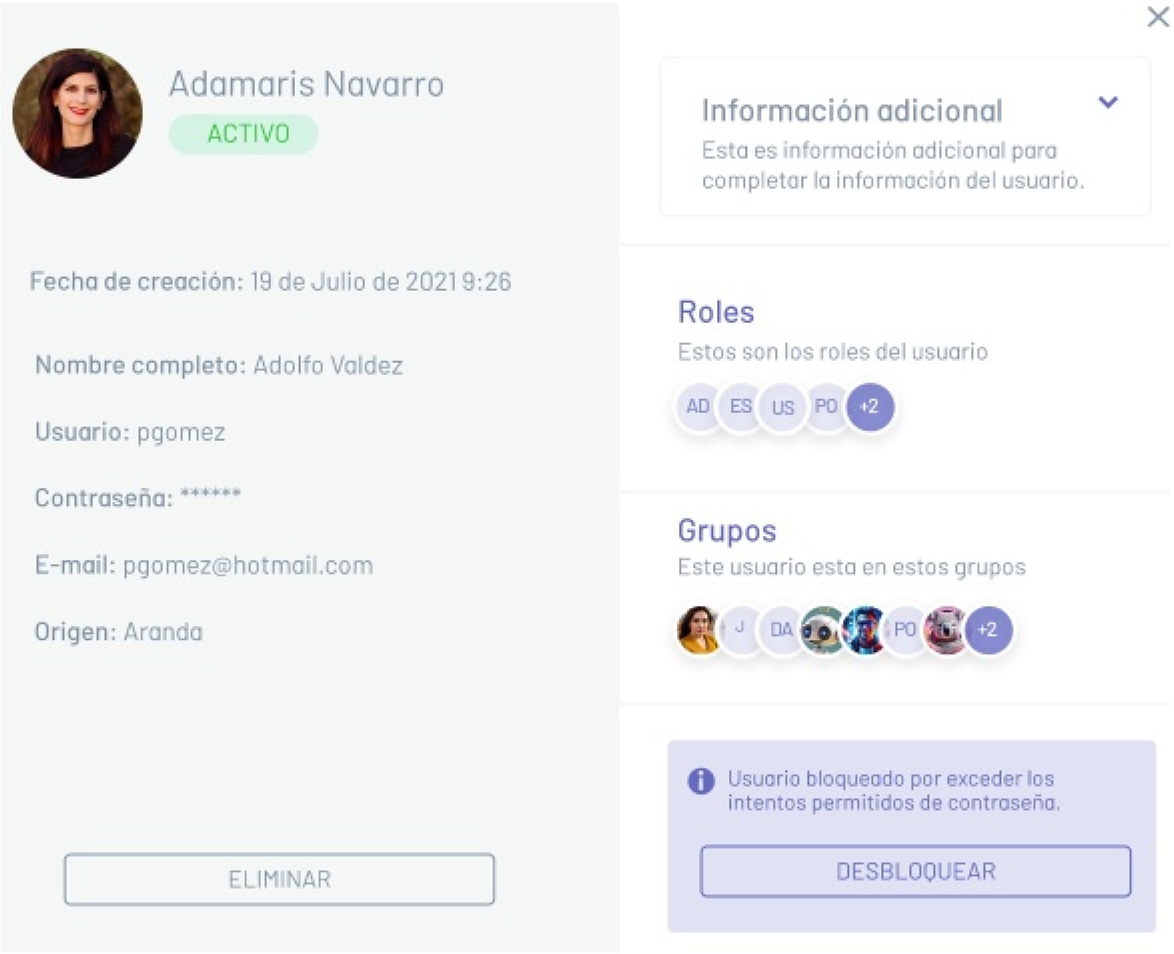
3. When you finish editing the user, click on the **Save**

💾

to confirm the changes made.

Unlock User

⚐ **Note:** When a user is blocked for exceeding the allowed password attempts, in the user's detail view, a warning message is activated and the **UNBLOCK**. By performing this action, the blocked user will be able to log in again.



Adamaris Navarro

ACTIVO

Fecha de creación: 19 de Julio de 2021 9:26

Nombre completo: Adolfo Valdez

Usuario: pgomez

Contraseña: ******

E-mail: pgomez@hotmail.com

Origen: Aranda

ELIMINAR

Información adicional

Esta es información adicional para completar la información del usuario.

Roles

Estos son los roles del usuario

Grupos

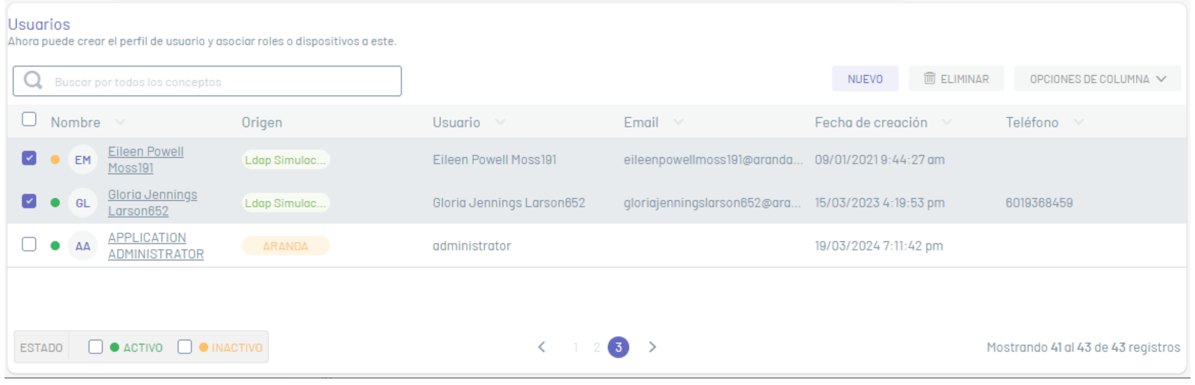
Este usuario esta en estos grupos

Usuario bloqueado por exceder los intentos permitidos de contraseña.

DESBLOQUEAR

Delete users

1. In the user information view, select one or more records from the list of existing users and click the **Eliminate** to clear the associated information.



Usuarios

Ahora puede crear el perfil de usuario y asociar roles o dispositivos a este.

Buscar por todos los conceptos

□	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
☑	● EM Eileen Powell Moss191	Ldap Simulac...	Eileen Powell Moss191	eileenpowellmoss191@aranda...	09/01/2021 9:44:27 am	
☑	● GL Gloria Jennings Larson652	Ldap Simulac...	Gloria Jennings Larson652	gloriajenningslarson652@ara...	15/03/2023 4:19:53 pm	6019368459
□	● AA APPLICATION ADMINISTRATOR	ARANDA	administrator		19/03/2024 7:11:42 pm	

ESTADO □ ● ACTIVO □ ● INACTIVO

Mostrando 41 al 43 de 43 registros

2. You will be able to display a confirmation message to validate the deletion action.

⚐ Note:

- A deleted user cannot be restored.
- If the user has associated records in the database, the deletion will fail.
- Users with the Administrator role and are logged in will not be allowed to be deleted.
- If you delete users **Imported**, in the next synchronization of the **Directory Service**, it is possible to believe again.

Specification Fields

Users/Basic Data

Field	Field Type	Description
Full name	Text	Name with which the user identifies himself.
Username	Text	Name used by the user to access the application.
Password	Text	Password used by the user to access the application, depends on the configuration made in the Password Policy from the Aranda authentication provider.
Confirm Password	Text	Password confirmation
Email	Text	User's email to receive information.
State	Selector	Indicates whether the user is active or inactive.

⚐ **Note:** The password must comply with policies established by the site administrator, and can be active or inactive according to the configuration made in the **Directory Service**. If the policy is not active, compliance with it is not required when creating or modifying a password; Only active policies will be required.

Users/Additional Information

Field	Field Type	Description
Cellular	Text	User’s cell phone number.
Address	Text	User’s home address.
Language	Selector	User preference language.
Document Type	Catalogue	Type of official identification that the user has.
Identification number	Text	Official user identification number.
Time zone	List	Time zone of the user’s preference.
Office Location	Catalogue	Name of the building where you work.
Company	Catalogue	Company where you work.
Company Area	Catalogue	Area within the company where you work.
Country	Catalogue	The user’s country of residence.
Department	Catalogue	Department or state of the country where you reside.
City	Catalogue	City of residence of the user.
Flat in the building	Catalogue	Flat in the building where he works.
Charge	Catalogue	Position within the company.
Headquarters	Catalogue	Name of the office where you work.
Telephone	Text	User’s phone number.

> ⚐ **Note:** The type fields **Catalogue** These are lists created by the site administrator. To view the logs, enter a letter to search for the desired value, or with the cursor key, down arrow you can display the existing options.
> If there are no catalogs for a field, no information will be displayed in the list, **and this field cannot be filled in**

Groups Module

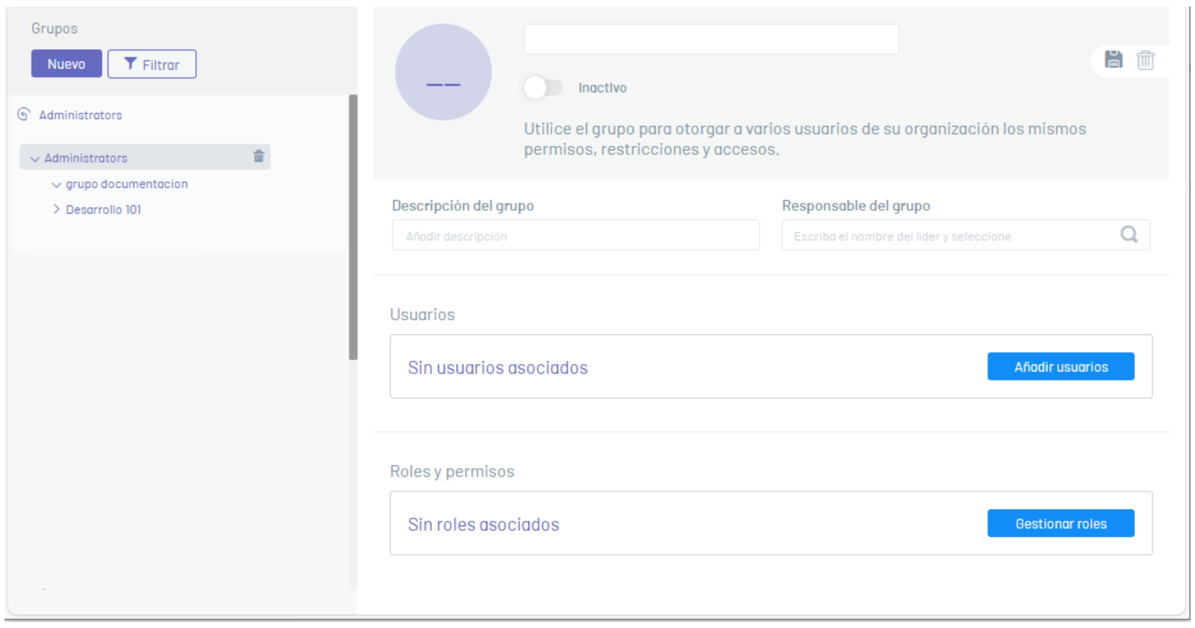
Group Management

View User Groups

1. In the User Groups information view, you can display a tree-like structure with the registered or imported user groups and subgroups.

2. By selecting the name of a group, you can display the information of the related subgroups. In the information view, you can view the group information in three sections:

- **Basic Info**: Basic group information such as name, status, description of the group and the group leader is presented; You will also be able to edit related information.
- **Users**: In this section you can manage users to the user group.
- **Roles and permissions:** In this section, you can manage the roles in the user group.



Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

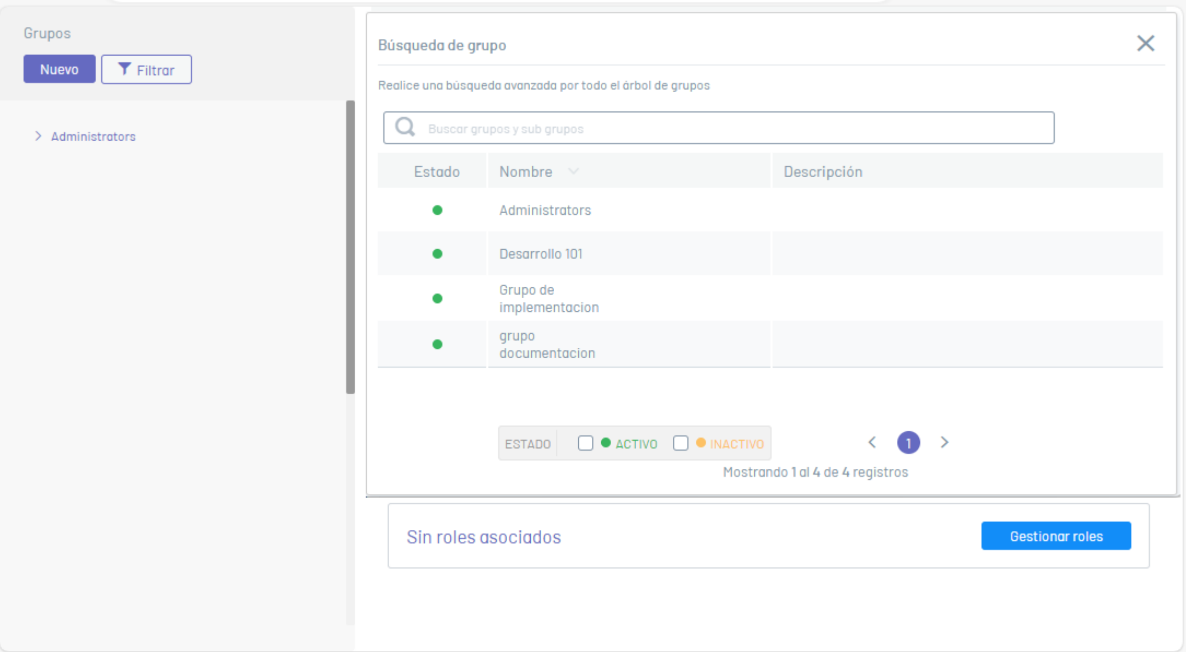
⚐ **Note:** Even if a group is disabled, it will be displayed in the tree.

2. In the group information view, you will have information management and organization actions enabled.[Information View in Commons Environment]()

Group filtering

1. In the user group information view, select the **Filter**.

2. The window is enabled **Group Search** where you can make the required consultation; In the Search field, enter a keyword.

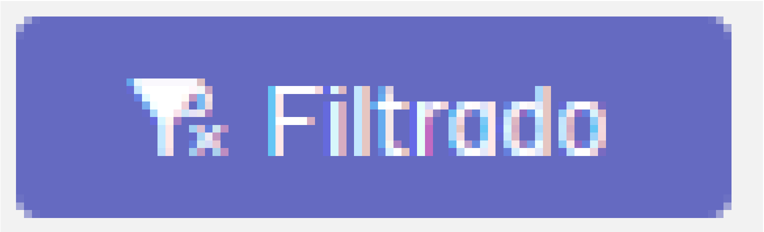


Realice una búsqueda avanzada por todo el árbol de grupos

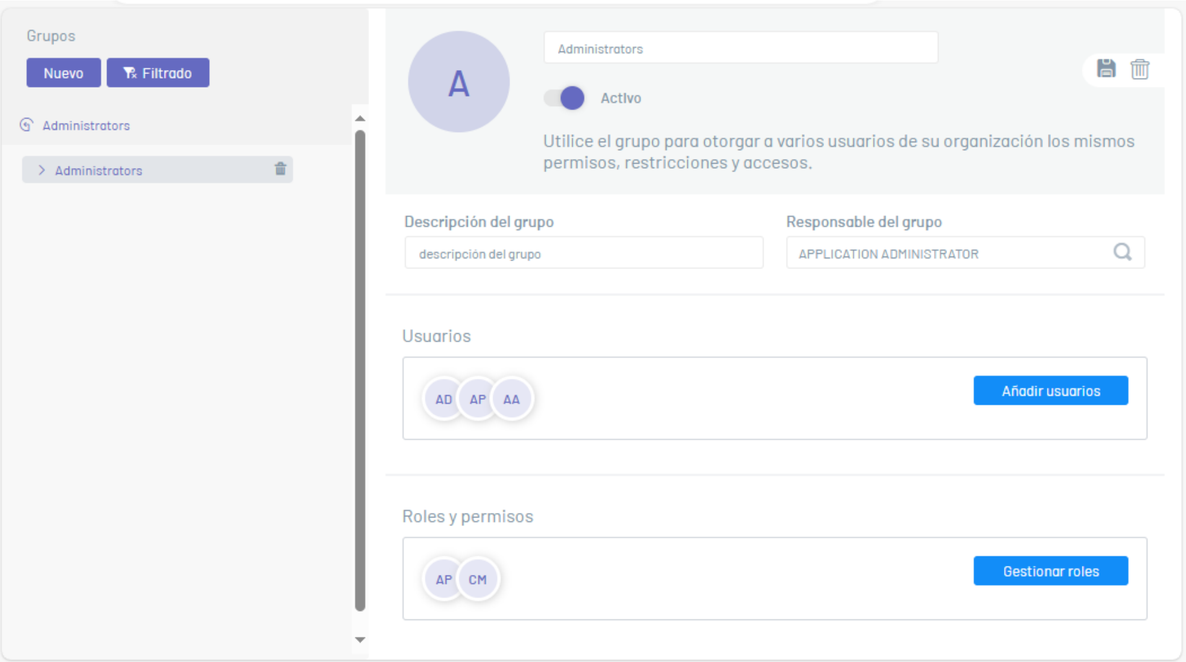
Estado	Nombre	Descripción
●	Administrators	
●	Desarrollo 101	
●	Grupo de implementacion	
●	grupo documentacion	

Mostrando 1 al 4 de 4 registros

3. Select a record from the groups found in the search. Doing so enables the group details window. 4. In the User Group Information view, you can clean up the filtered information by clicking the



.



Administrators

Activo

Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

Descripción del grupo: descripción del grupo

Responsable del grupo: APPLICATION ADMINISTRATOR

Related Links:

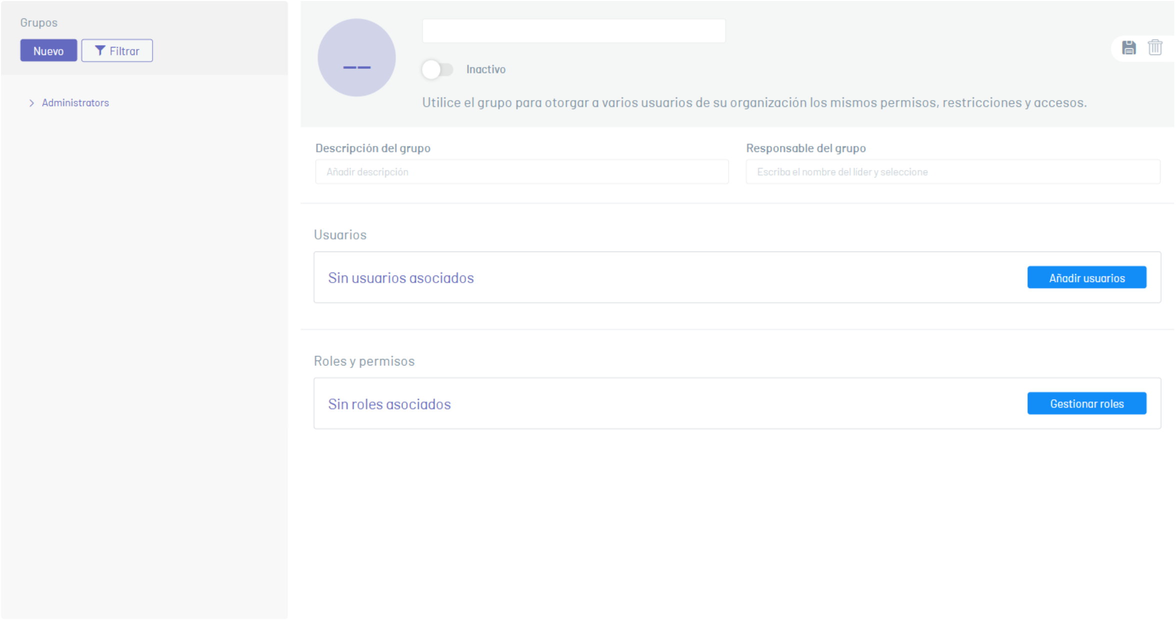
- [Create Groups]
- [Edit Groups]
- [Delete Groups]

Create groups

Basic Facts

1. For the creation of a group without any higher hierarchy, it must be located at the root of the tree; In the information view, you can view the form to fill in the required information (basic information, associate users and roles).

2. If the group to be created must belong to another group, click on the required parent group and click on theNew and fill in the required information. Each of the fields in the group must take into account the Specifications for Common Fields.



Inactivo

Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

Sin usuarios asociados

Sin roles asociados

⚐ Note:

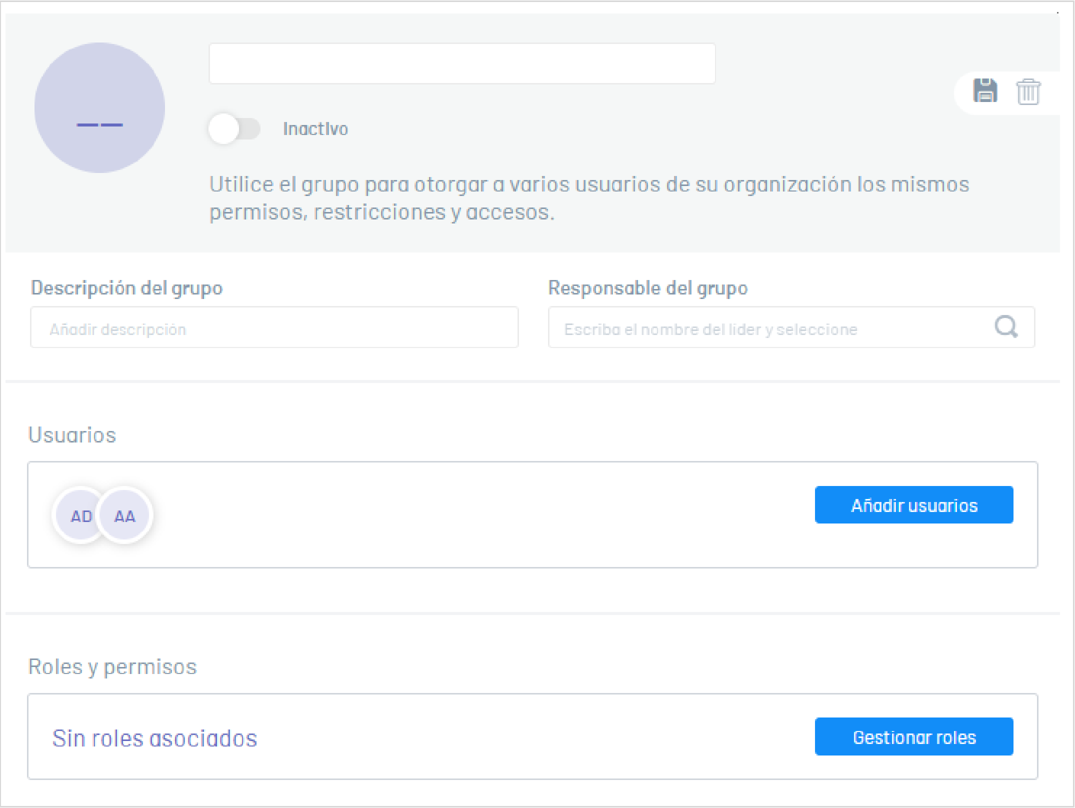
- Imported groups cannot be created as it is information collected from the service directory.
- You can create as many subgroups as you need. Subgroups (child groups) do not inherit users or roles from the parent group (parent group).
- Two groups cannot have the same name if they are at the same hierarchy level.

3. When you finish setting up the new group, click the Save

to confirm the changes made. 4. Once the user group has been created, the message confirming the creation of the group will be displayed and its location will be displayed in the tree

Associate and disassociate users with the group

6. To add users, in the information view of a user group, in the Users section, select the **Add users**.



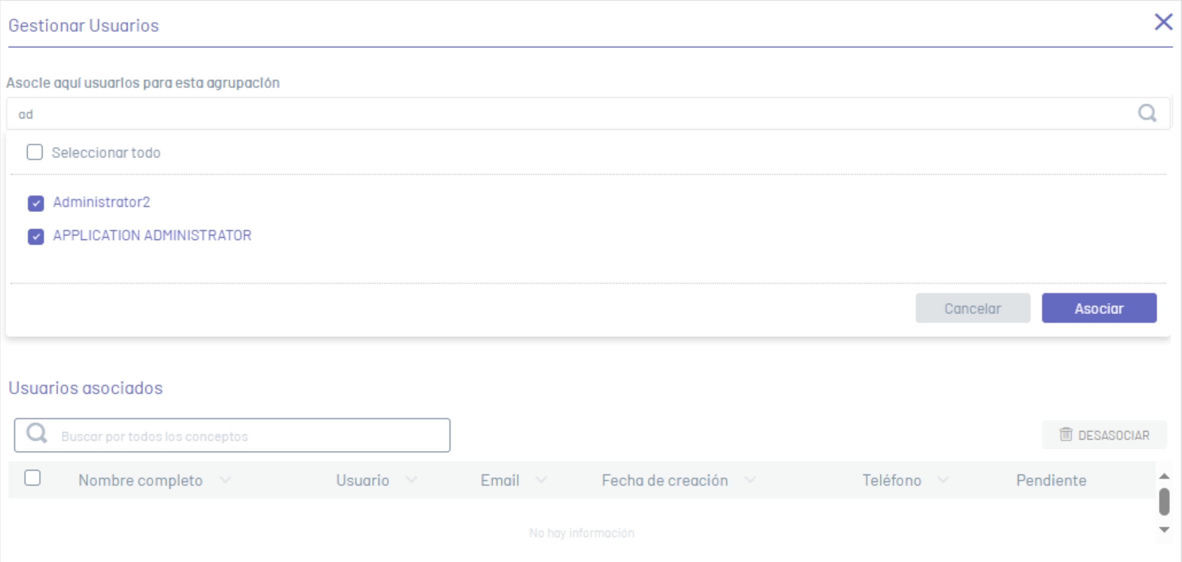
Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

Descripción del grupo: Añadir descripción

Responsable del grupo: Escriba el nombre del líder y seleccione

Sin roles asociados

7. The window is enabled **Manage Users**, where you can view and add the required users for the defined group. In the search field to associate users, enter the name of the required user and from the list of results select the user to add. 8. When finished, click on the **Associate**.



Gestionar Usuarios

Asocie aquí usuarios para esta agrupación: ad

□ Seleccionar todo

☑ Administrator2

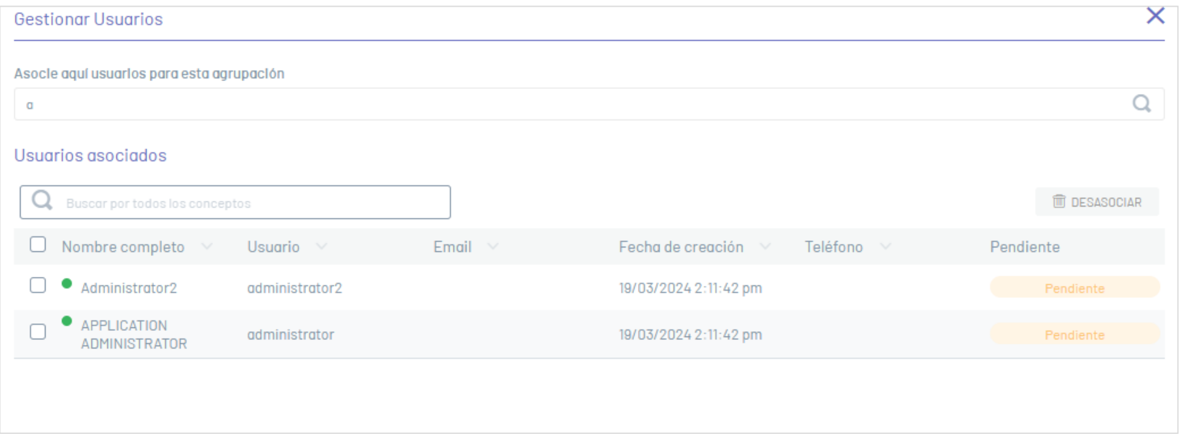
☑ APPLICATION ADMINISTRATOR

□	Nombre completo	Usuario	Email	Fecha de creación	Teléfono	Pendiente

No hay información

⚐ Notes:

- In the search field for associating users, the users who are active will appear. The added users will be left with the roles of the group.
- Once associated, users are left in a state **Earring** until the group is saved



Asocie aquí usuarios para esta agrupación

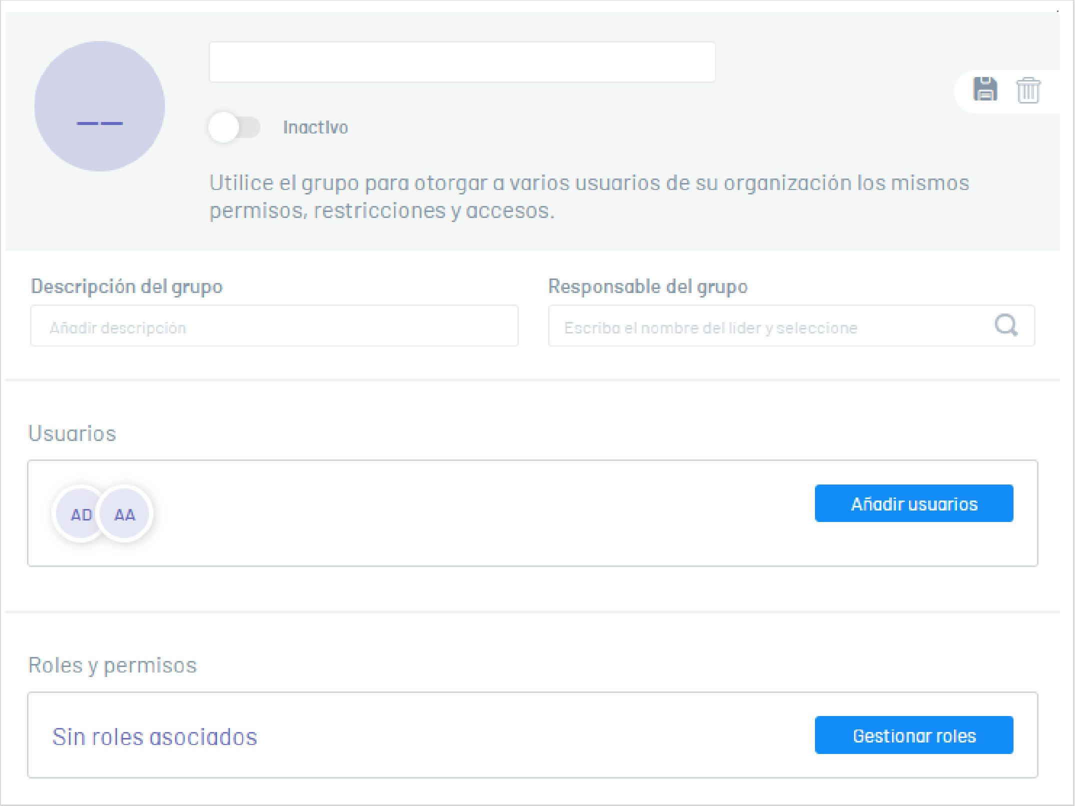
a

□	Nombre completo	Usuario	Email	Fecha de creación	Teléfono	Pendiente
□	● Administrator2	administrator2		19/03/2024 2:11:42 pm		Pendiente
□	● APPLICATION ADMINISTRATOR	administrator		19/03/2024 2:11:42 pm		Pendiente

9. To remove a user from a group, in the **Manage Users** Select one or more records from the list of users and click the **Disassociate**. Confirm that you want to disassociate users by clicking the**Accept**.

Associating and Disassociating Roles

10. To add roles, in the information view of a user group, in the Roles and Permissions section, select the**Manage** Roles.



Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

Descripción del grupo: Añadir descripción

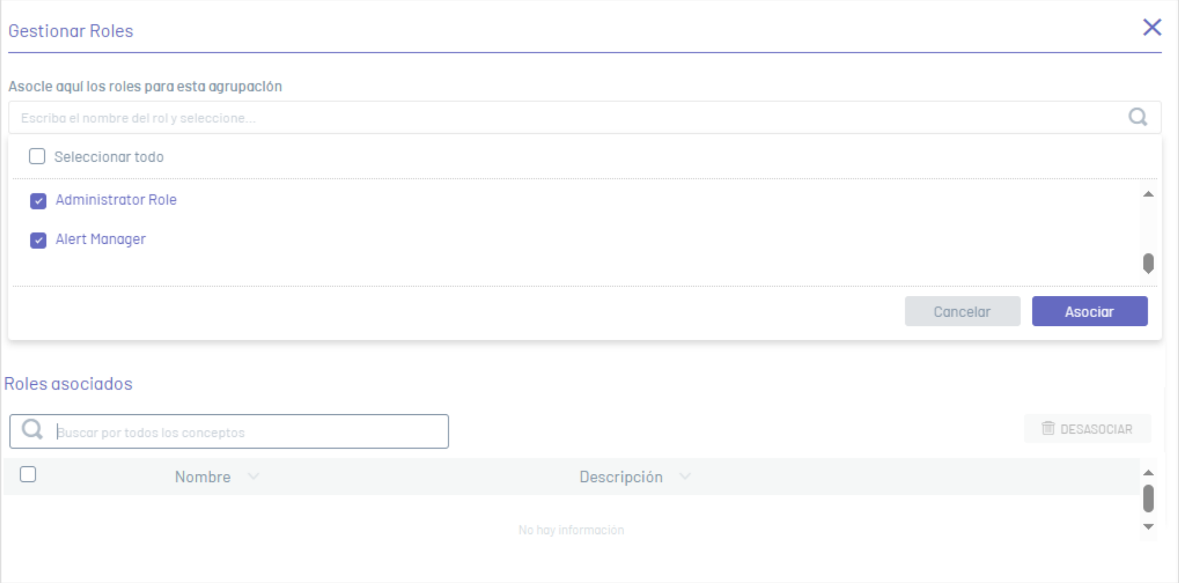
Responsable del grupo: Escriba el nombre del líder y seleccione

Sin roles asociados

11. The window is enabled**Manage Roles**, where you can view and add the required roles for the defined group. In the search field to associate roles, enter the name of the required role and from the list of results select the role to add.

> ⚐ **Note:** In the search field for associating roles, only active roles will appear.

12. When finished, click **Associate**.



Asocie aquí los roles para esta agrupación

Escriba el nombre del rol y seleccione...

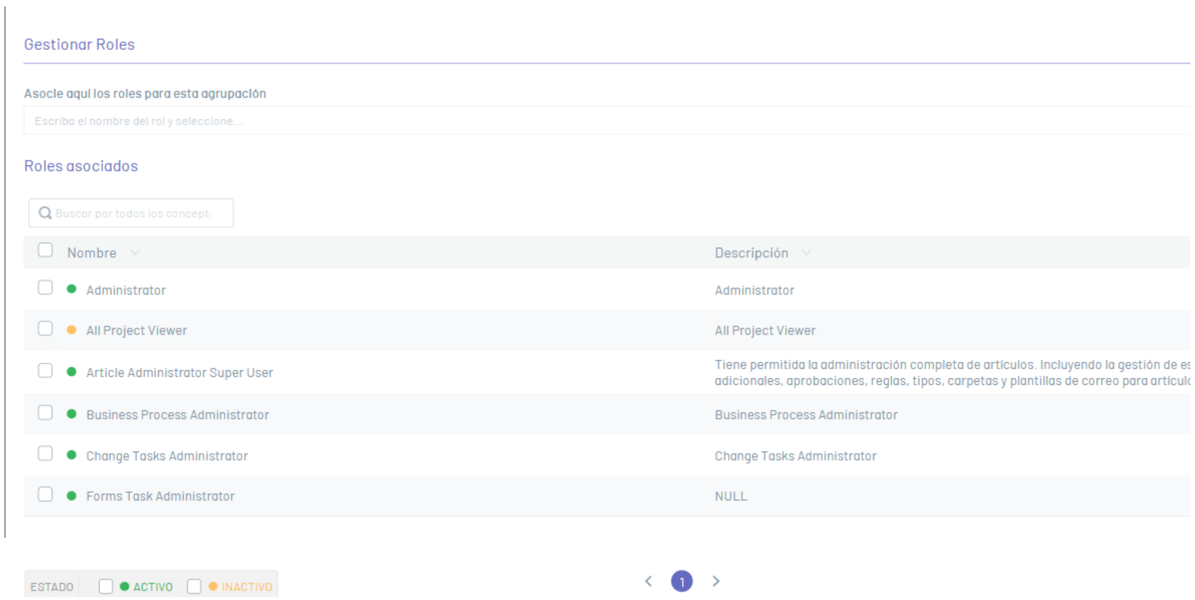
□ Seleccionar todo

☑ Administrator Role

☑ Alert Manager

□	Nombre	Descripción
	No hay información	

> ⚐ **Note:** The status of the role is pending until the changes are saved.



Gestionar Roles

Asocie aquí los roles para esta agrupación

Escribe el nombre del rol y seleccione...

Roles asociados

Buscar por todos los concept

□ Nombre	Descripción
□ ● Administrator	Administrator
□ ● All Project Viewer	All Project Viewer
□ ● Article Administrator Super User	Tiene permitida la administración completa de articulos. Incluyendo la gestión de es adicionales, aprobaciones, reglas, tipos, carpetas y plantillas de correo para articul
□ ● Business Process Administrator	Business Process Administrator
□ ● Change Tasks Administrator	Change Tasks Administrator
□ ● Forms Task Administrator	NULL

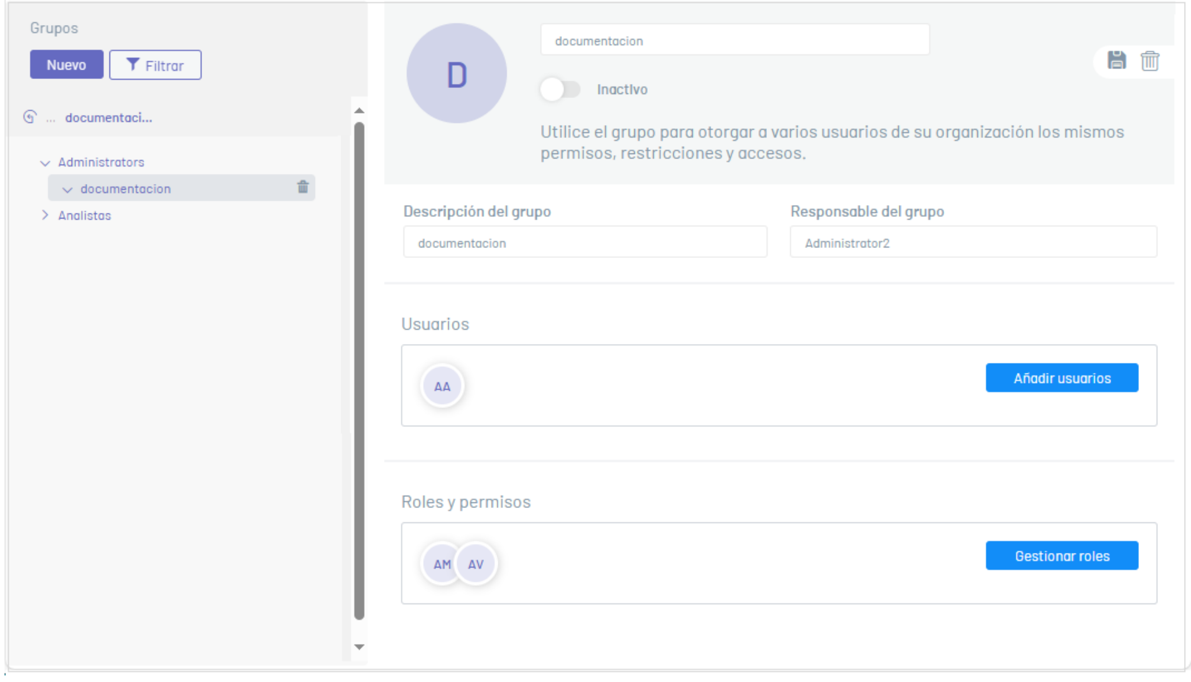
ESTADO □ ● ACTIVO □ ● INACTIVO

13. To detach roles from a group, in the **Manage Roles** Select one or more records from the list of roles and click the **Disassociate**. Confirm that you want to disassociate users by clicking the**Accept**. 14. When you finish setting up the new group, click the **Save**

to confirm the changes made.

Edit from groups

1. To modify a group or subgroup, in the user group information view, select a record from the grouping tree; You will be able to view the group details and modify the required information.



documentacion

Inactivo

Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

Descripción del grupo: documentacion

Responsable del grupo: Administrator2

Usuarios

Roles y permisos

⚐ **Note:** If the group is imported from an Active Directory, you can only modify the roles and status of a group. Users will not be able to edit

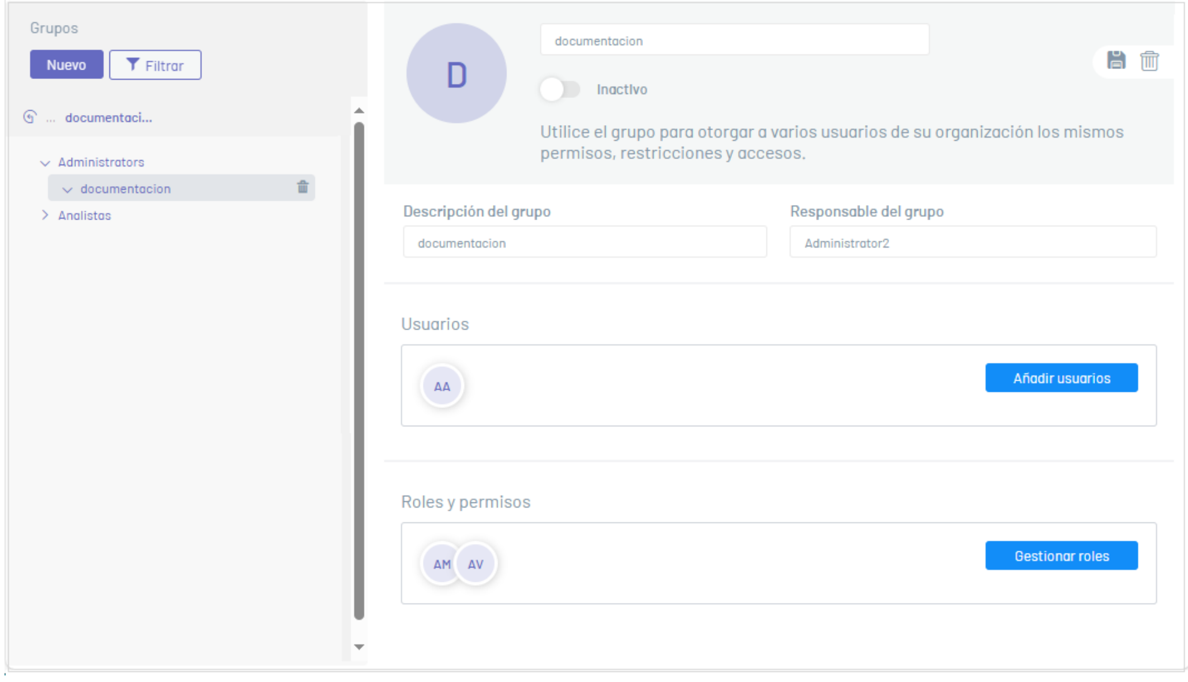
2. When you finish editing the group, click the Save

to confirm the changes made.

Remove from Groups

1. In the user group information view, select a record from the grouping tree and click the Eliminate

to clear the associated information.



documentacion

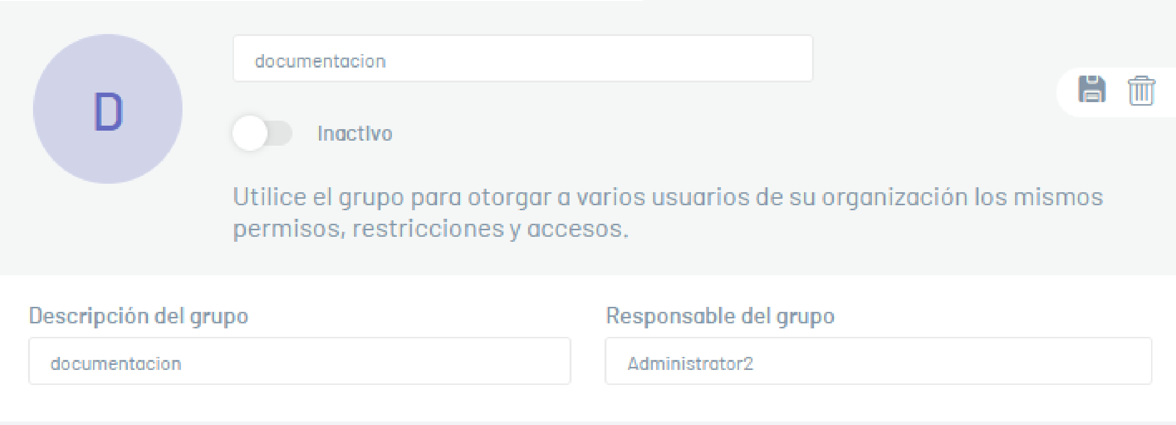
Inactivo

Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

Descripción del grupo: documentacion

Responsable del grupo: Administrator2

2. Alternatively, in the detail view of the selected group, click the Eliminate to clear the associated information.



D

documentacion

Inactivo

Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

Descripción del grupo: documentacion

Responsable del grupo: Administrator2

3. You will be able to display a confirmation message to validate the deletion action.

⚐ Note:

- When you delete a group, if it is a parent group, the subgroups that belong to it will be deleted.
- Users and roles are not deleted if the group is deleted.
- If you want to delete only one subgroup, you must select the subgroup to be deleted.
- Imported groups can be deleted. However, there is a chance that the group will be imported back from the service directory.

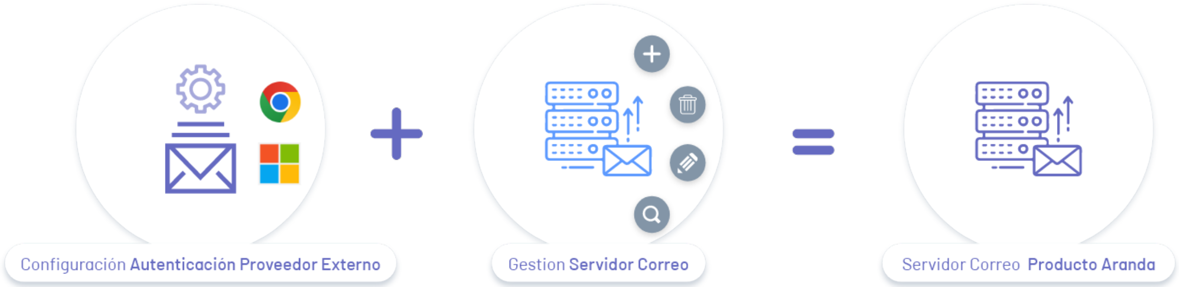
Specification Fields

Groups/Basic Data

Field	Field Type	Description
Name	Text	Name with which the group is identified.
Description	Text	Additional group information.
Group Manager	Text	Query a defined user, who will become the group leader.
Active/Inactive	Text	Activate or deactivate a group.
Add Users	N/A	This button Defines the action for associating users with an established group.
Manage Role*	N/A	This button Gestionar roles Defines the action to authorize one or more permissions according to the added role.

Mail Server Module

Mail Server Preliminary Configuration


Configuración Autenticación Proveedor Externo
Gestion Servidor Correo
Servidor Correo Producto Aranda

1. Configuration of Third-Party Server Providers

Configure third-party providers (Microsoft Azure, Google) for mail server authentication processes.

For more information, see the Oauth/Microsoft ↪ Modern Authentication.

For more information, see the Oauth/Google ↪ Modern Authentication.

2. Mail Server Module Management

In the Mail Server module, you can create, update, and delete email server configurations for notifications that will be sent to users from the web console.

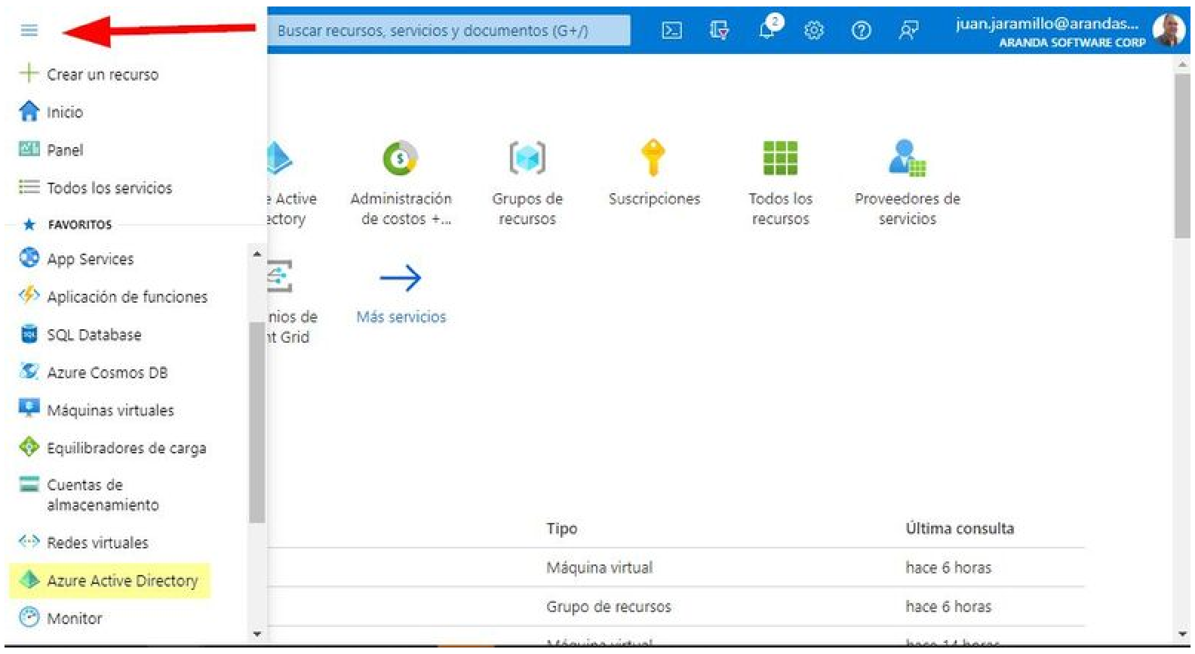
For more information, see the Mail Server Management ↪.

OAuth 2.0/Microsoft Authentication

Creating an Application in Azure

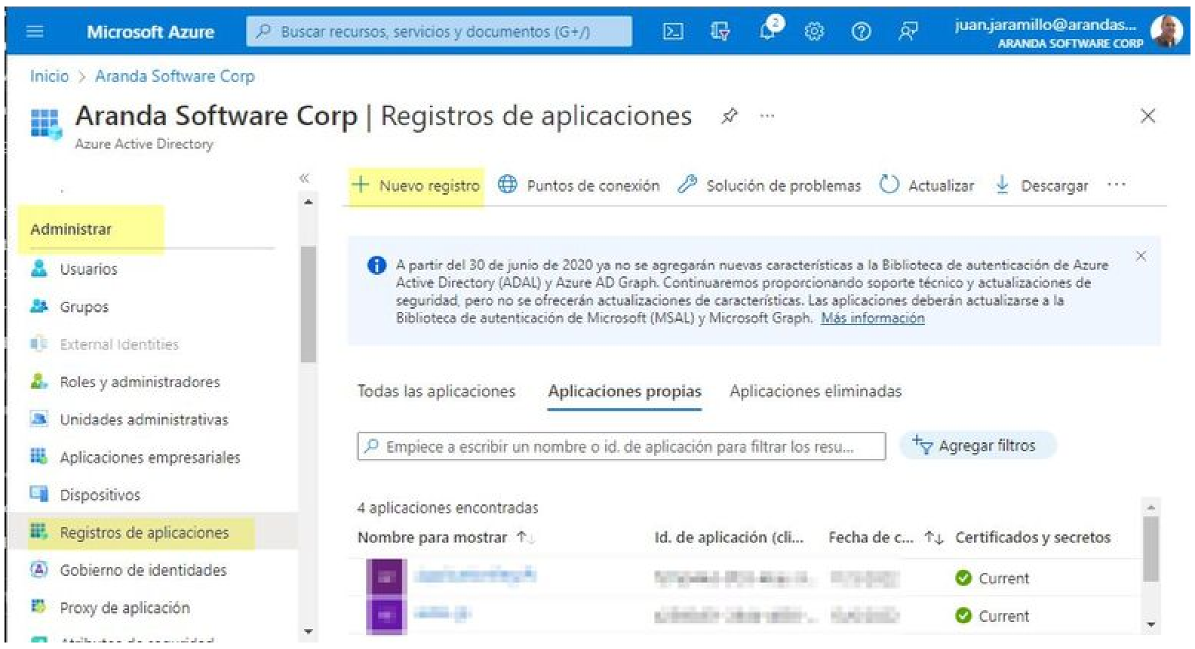
▶ Requisitos Autenticación Azure: ❯

1. Access the Azure portal View Microsoft Azure , search and select **Azure Active Directory**.



Tipo	Última consulta
Máquina virtual	hace 6 horas
Grupo de recursos	hace 6 horas

2. . In the **Administer** Search and select **Application logs**, click **New Registration**.

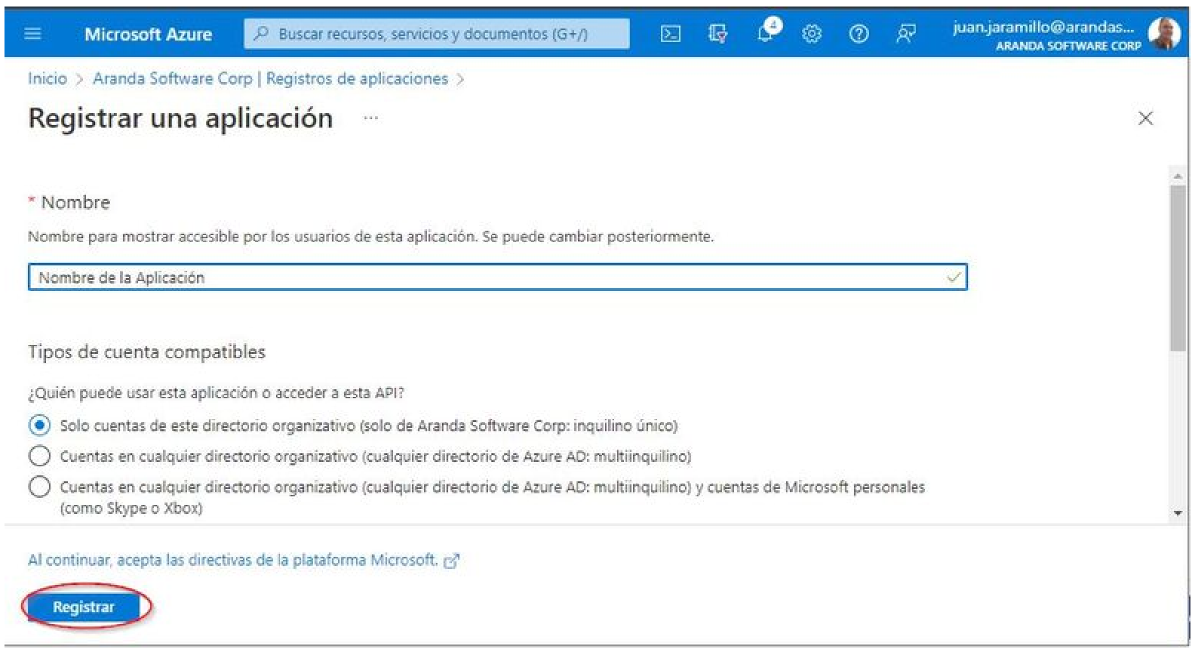


A partir del 30 de junio de 2020 ya no se agregarán nuevas características a la Biblioteca de autenticación de Azure Active Directory (ADAL) y Azure AD Graph. Continuaremos proporcionando soporte técnico y actualizaciones de seguridad, pero no se ofrecerán actualizaciones de características. Las aplicaciones deberán actualizarse a la Biblioteca de autenticación de Microsoft (MSAL) y Microsoft Graph. Más información

4 aplicaciones encontradas

Nombre para mostrar	Id. de aplicación (cli...	Fecha de c...	Certificados y secretos
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	Current

3. The name field is filled in and the desired option is selected under (Supported Account Types), clickRegister.


Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
juan.jaramillo@arandas...
ARANDA SOFTWARE CORP
Inicio > Aranda Software Corp | Registros de aplicaciones >
Registrar una aplicación
Registrar

* Nombre

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

Nombre de la Aplicación

Tipos de cuenta compatibles

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

● Solo cuentas de este directorio organizativo (solo de Aranda Software Corp: inquilino único)

○ Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino)

○ Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino) y cuentas de Microsoft personales (como Skype o Xbox)

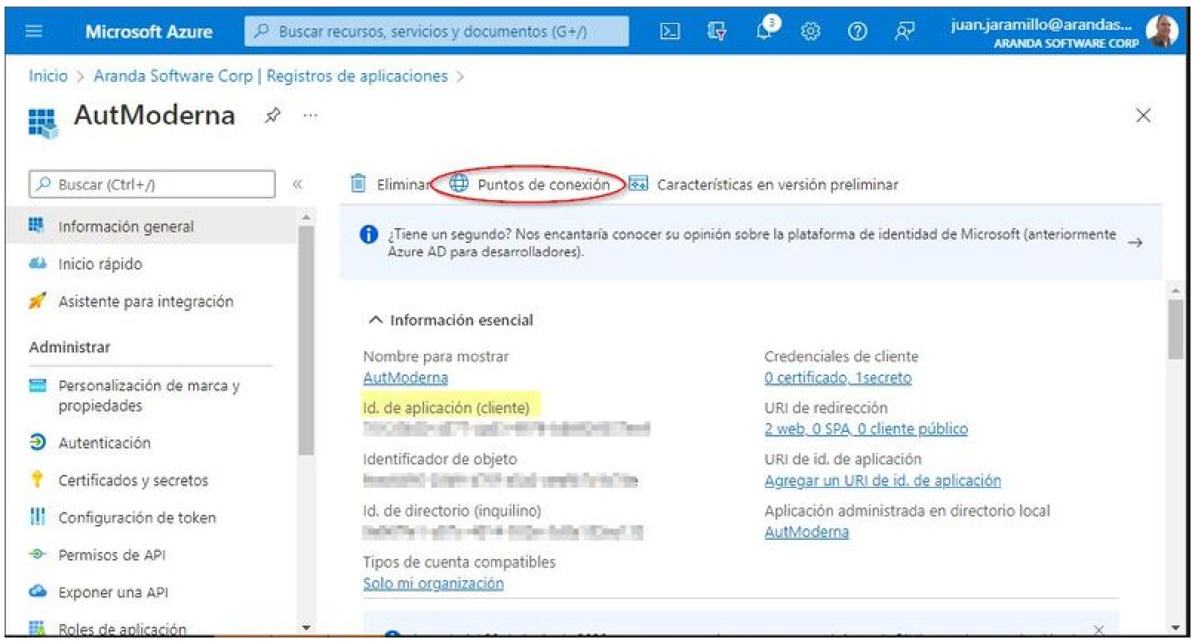
Al continuar, acepta las directivas de la plataforma Microsoft.

4.Once your app is registered, save the following data that is required for configuration in Aranda apps.

- Application ID (Client) -> Client ID.

Click on the option (Endpoints).

- OAuth 2.0 authorization endpoint (v2) -> authorization URL.
- OAuth 2.0 (v2) token endpoint - > token URL.



¿Tiene un segundo? Nos encantaría conocer su opinión sobre la plataforma de identidad de Microsoft (anteriormente Azure AD para desarrolladores).

Información esencial

Nombre para mostrar: AutModerna

Id. de aplicación (cliente): [redacted]

Identificador de objeto: [redacted]

Id. de directorio (inquilino): [redacted]

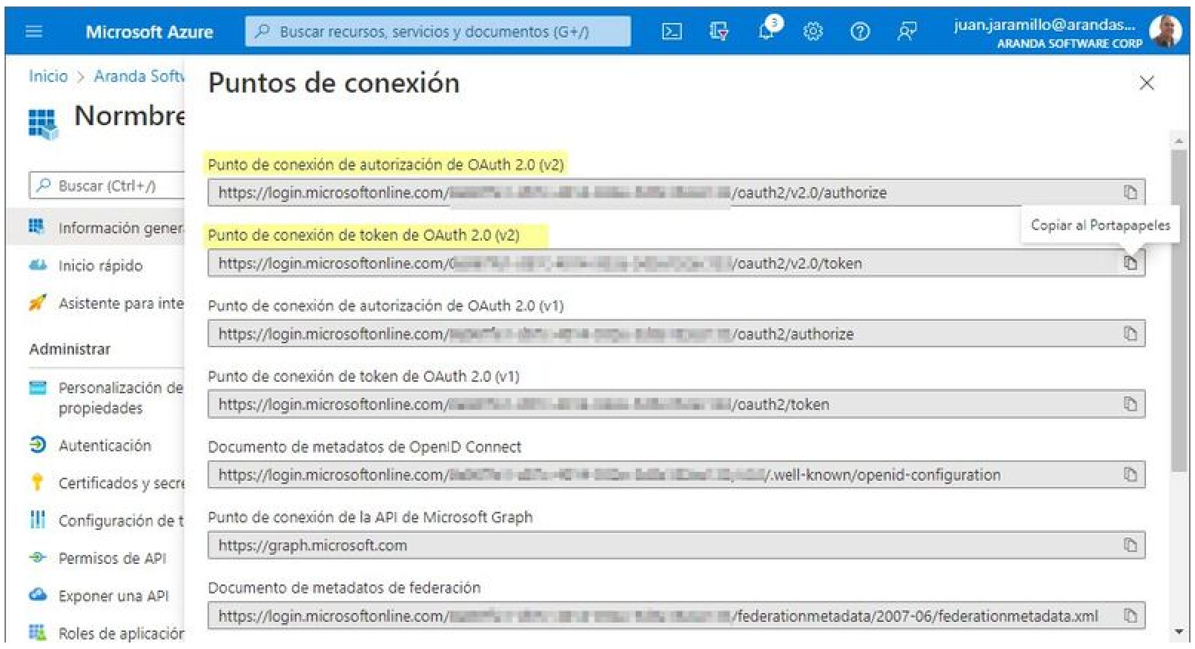
Tipos de cuenta compatibles: Solo mi organización

Credenciales de cliente: 0 certificado, 1 secreto

URI de redirección: 2 web, 0 SPA, 0 cliente público

URI de id. de aplicación: Agregar un URI de id. de aplicación

Aplicación administrada en directorio local: AutModerna



Punto de conexión de autorización de OAuth 2.0 (v2)
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

Punto de conexión de token de OAuth 2.0 (v2)
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/token

Punto de conexión de autorización de OAuth 2.0 (v1)
https://login.microsoftonline.com/[redacted]/oauth2/authorize

Punto de conexión de token de OAuth 2.0 (v1)
https://login.microsoftonline.com/[redacted]/oauth2/token

Documento de metadatos de OpenID Connect
https://login.microsoftonline.com/[redacted]/.well-known/openid-configuration

Punto de conexión de la API de Microsoft Graph
https://graph.microsoft.com

Documento de metadatos de federación
https://login.microsoftonline.com/[redacted]/federationmetadata/2007-06/federationmetadata.xml

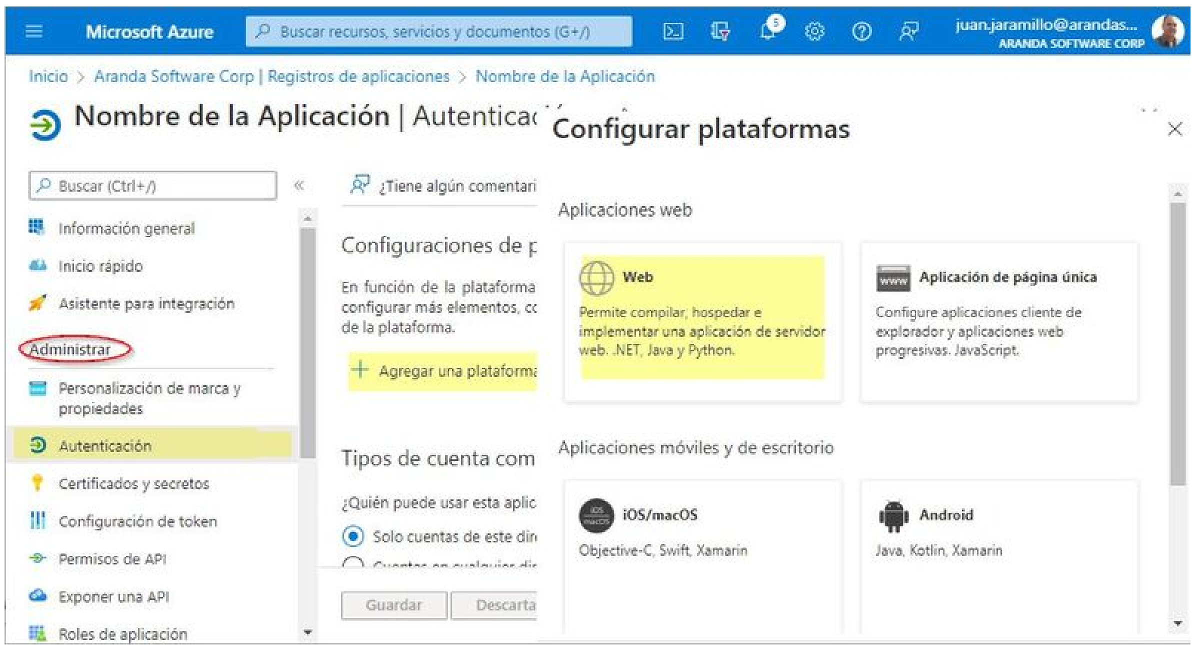
Configure your application in the Azure portal

When you have the application created and have the data saved, you proceed to configure the application as follows:

How to set up authentication

1. You enter the Azure portal > Azure Active Directory > Menu > Application Logs > select the created application from the list that appears in the view.

2. In the **Administer** Search and select > **Authentication** then in **Add a platform**, select the **Web**.



En función de la plataforma configurar más elementos, cc de la plataforma.

¿Quién puede usar esta aplic

○ Solo cuentas de este dir

Permite compilar, hospedar e implementar una aplicación de servidor web. .NET, Java y Python.

Configure aplicaciones cliente de explorador y aplicaciones web progresivas. JavaScript.

3. For the product **Aranda Service Management ASMS** fill out the **Redirect URIs** as follows:

- **Output Server:** https://[domain]/[SiteAdministration]/Main/Pages/OauthToken.aspx
- **Input Server (Case Creator):** (http://localhost) and perform the [Manual token generation process](Postman).

- Replace the [**domain**] as appropriate, and then select **Configure**.

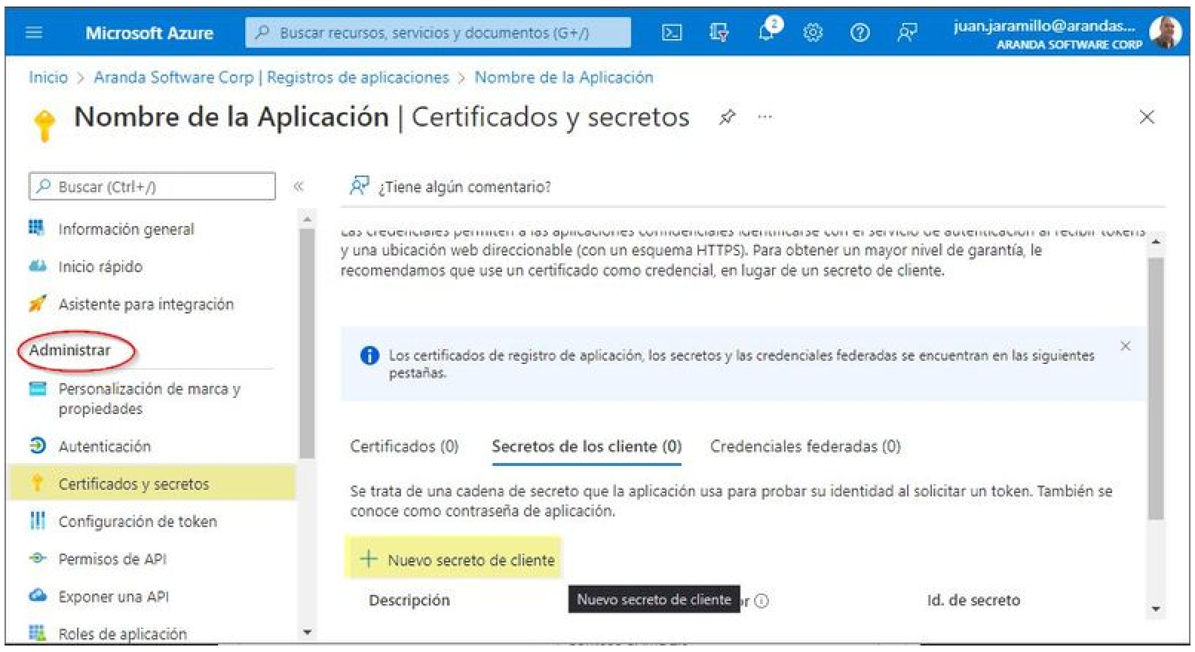
- Replace [**SiteAdministration**] with the name of the directory or application of the administration site.

- **Note:** This name is case-sensitive and must be written as configured.
  4. Para los demás productos Aranda, la **Url de redirección** es: https://[dominio]/api/oauth2

Creation of the Secret

1. To create the secret, enter the Azure portal > Azure Active Directory > Menu > Application Logs > select the created application from the list that appears in the view.

2. In the **Administer** Search and select **Certificates and secrets** > Then click **New client secret**.

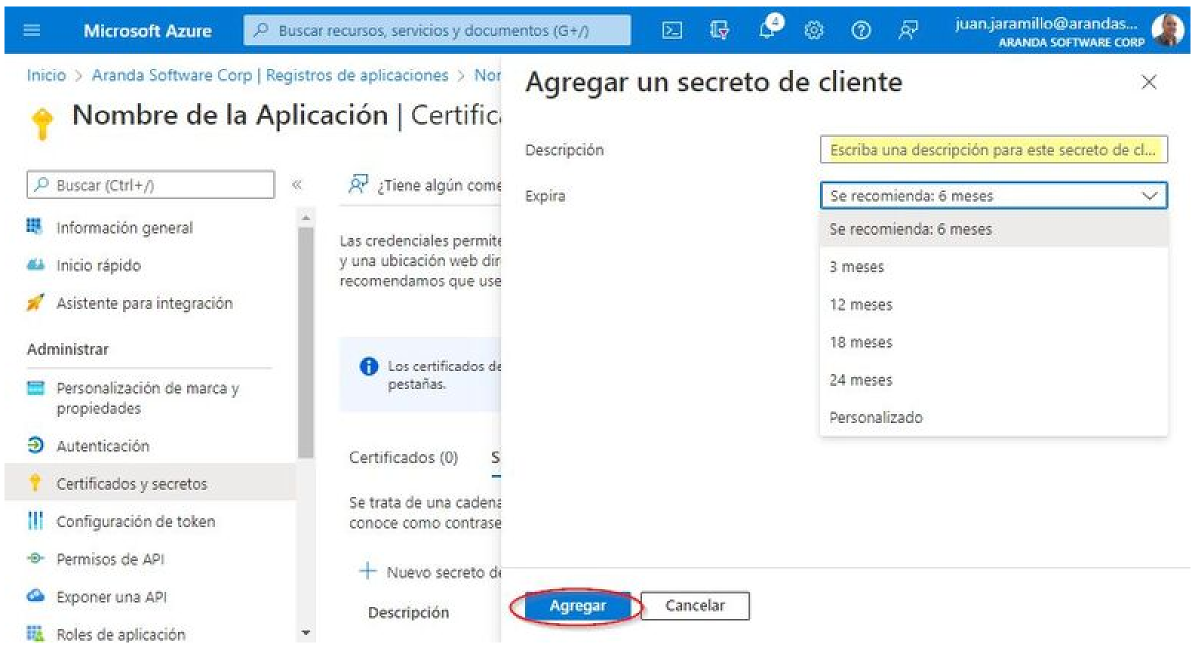

Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
juan.jaramillo@arandas...
ARANDA SOFTWARE CORP
Inicio > Aranda Software Corp | Registros de aplicaciones > Nombre de la Aplicación
Nombre de la Aplicación | Certificados y secretos
Buscar (Ctrl+/)
¿Tiene algún comentario?
Información general
Inicio rápido
Asistente para integración
Administrar
Personalización de marca y propiedades
Autenticación
Certificados y secretos
Configuración de token
Permisos de API
Exponer una API
Roles de aplicación
Certificados (0)
Secretos de los cliente (0)
Credenciales federadas (0)
Nuevo secreto de cliente
Descripción
Id. de secreto

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.

Los certificados de registro de aplicación, los secretos y las credenciales federadas se encuentran en las siguientes pestañas.

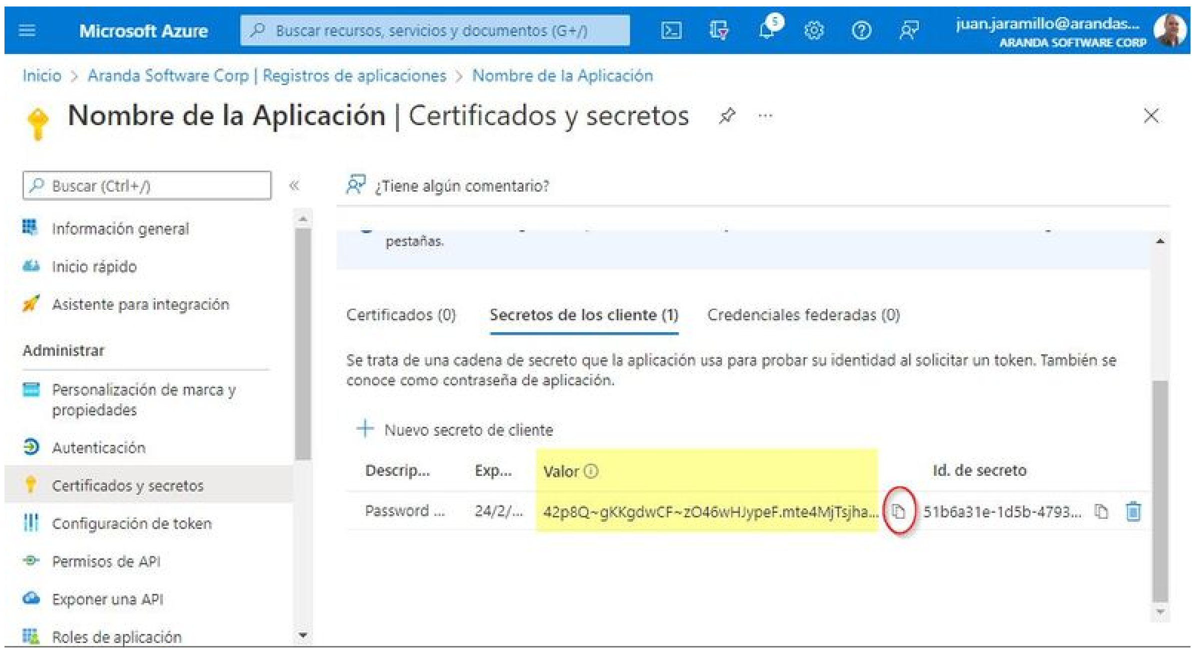
Se trata de una cadena de secreto que la aplicación usa para probar su identidad al solicitar un token. También se conoce como contraseña de aplicación.

3. At the Hearing **Add a client secret** fill in the field **Description**, configure the **Expires** which corresponds to the duration of the secrecy. Then select **Add** (It is important to always keep this duration in mind since, when it expires, if it is not updated, authentication will fail.)



4. The value of the secret is only visible when it is created, so it must be saved for later use and retained for the configurations required in Aranda products.

- Client Secret Value -> Client Secret.


Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
juan.jaramillo@arandas...
ARANDA SOFTWARE CORP
Inicio > Aranda Software Corp | Registros de aplicaciones > Nombre de la Aplicación
Nombre de la Aplicación | Certificados y secretos
Buscar (Ctrl+/)
¿Tiene algún comentario?
Información general
Inicio rápido
Asistente para integración
Administrar
Personalización de marca y propiedades
Autenticación
Certificados y secretos
Configuración de token
Permisos de API
Exponer una API
Roles de aplicación
pestañas.
Certificados (0)
Secretos de los cliente (1)
Credenciales federadas (0)
Nuevo secreto de cliente

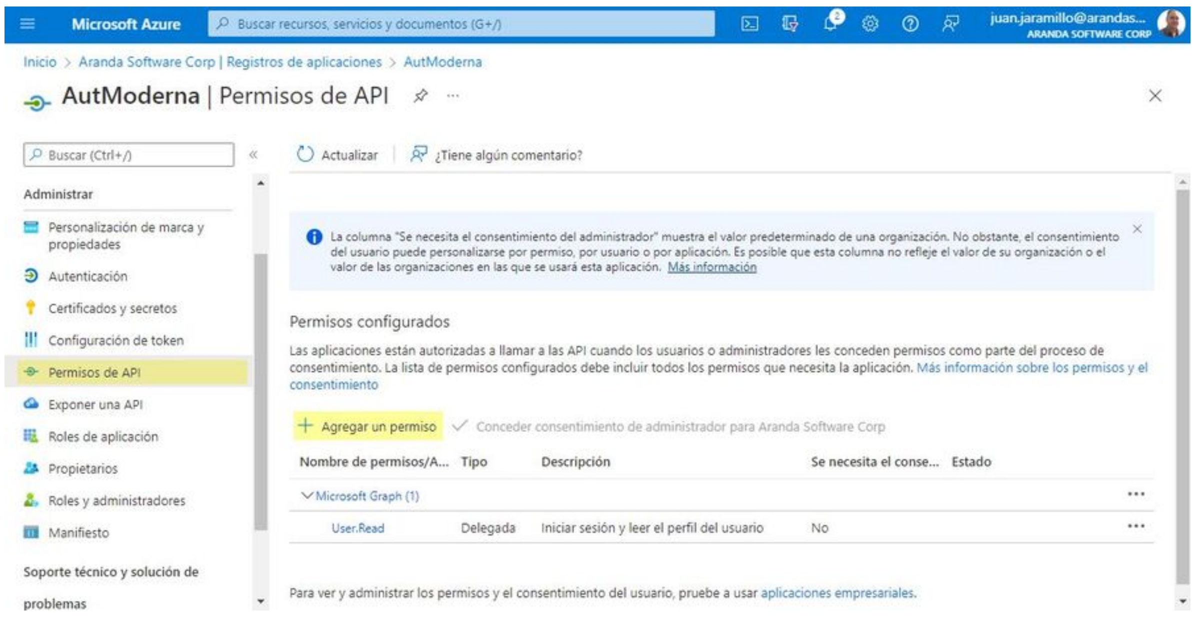
Se trata de una cadena de secreto que la aplicación usa para probar su identidad al solicitar un token. También se conoce como contraseña de aplicación.

Descrip...	Exp...	Valor	Id. de secreto
Password ...	24/2/...	42p8Q~gKKgdwCF~zO46wHJypeF.mte4MjTsjha...	51b6a31e-1d5b-4793...

Configure API permissions

1. To configure API permissions, go to the Azure portal > Menu > Azure Active Directory > Application Logs > select the created application from the list that appears in the view.

2. In the **Administer** Search and select **API permissions** >Then click **Add a Permission**.



Inicio > Aranda Software Corp | Registros de aplicaciones > AutModerna

AutModerna | Permisos de API

Actualizar | ¿Tiene algún comentario?

Administrar: Personalización de marca y propiedades; Autenticación; Certificados y secretos; Configuración de token; Permisos de API; Exponer una API; Roles de aplicación; Propietarios; Roles y administradores; Manifiesto

Soporte técnico y solución de problemas

La columna "Se necesita el consentimiento del administrador" muestra el valor predeterminado de una organización. No obstante, el consentimiento del usuario puede personalizarse por permiso, por usuario o por aplicación. Es posible que esta columna no refleje el valor de su organización o el valor de las organizaciones en las que se usará esta aplicación. Más información

Permisos configurados

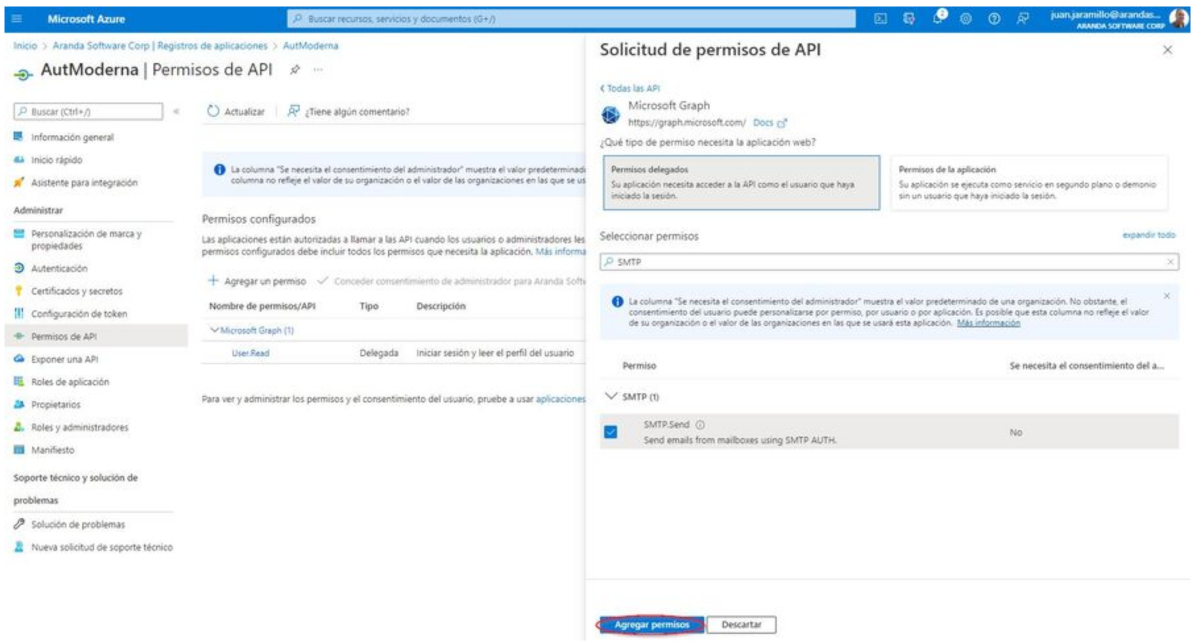
Las aplicaciones están autorizadas a llamar a las API cuando los usuarios o administradores les conceden permisos como parte del proceso de consentimiento. La lista de permisos configurados debe incluir todos los permisos que necesita la aplicación. Más información sobre los permisos y el consentimiento

+ Agregar un permiso | ✓ Conceder consentimiento de administrador para Aranda Software Corp

Nombre de permisos/A...	Tipo	Descripción	Se necesita el conse...	Estado
Microsoft Graph (1)				
User.Read	Delegada	Iniciar sesión y leer el perfil del usuario	No	

Para ver y administrar los permisos y el consentimiento del usuario, pruebe a usar aplicaciones empresariales.

3. At the Hearing **Request API permissions** select **Microsoft Graph** > later **Delegated permissions**, Select the permissions according to your requirements: **SMTP. Send** (Sending mails), **IMAP** and **POP** (Reading emails). Click **Add permission**.



Solicitud de permisos de API

Todas las API

Microsoft Graph
https://graph.microsoft.com/ Docs

¿Qué tipo de permiso necesita la aplicación web?

Permisos delegados: Su aplicación necesita acceder a la API como el usuario que haya iniciado la sesión.

Permisos de la aplicación: Su aplicación se ejecuta como servicio en segundo plano o demonio sin un usuario que haya iniciado la sesión.

Seleccionar permisos — expandir todo

SMTP

La columna "Se necesita el consentimiento del administrador" muestra el valor predeterminado de una organización. No obstante, el consentimiento del usuario puede personalizarse por permiso, por usuario o por aplicación. Es posible que esta columna no refleje el valor de su organización o el valor de las organizaciones en las que se usará esta aplicación. Más información

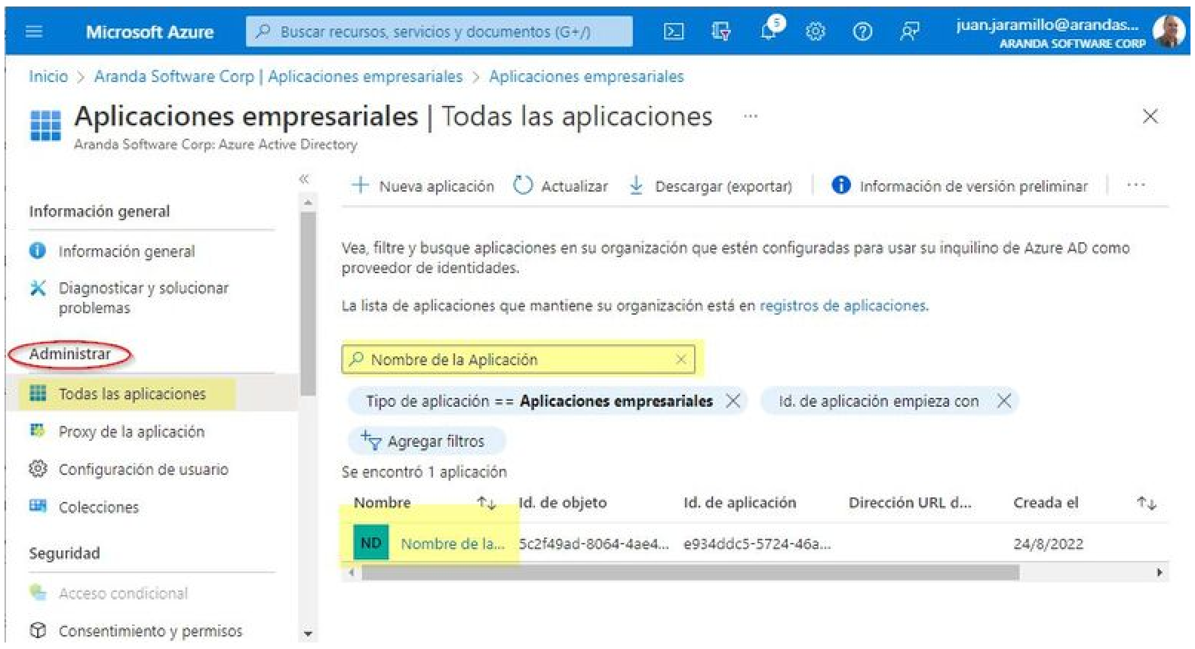
Permiso	Se necesita el consentimiento del a...
SMTP (1)	
☑ SMTP.Send Send emails from mailboxes using SMTP AUTH.	No

Agregar permisos | Descartar

User and group settings

In this configuration, the email account(s) that will be able to access the application are associated.

1. You enter the Azure portal> Menu> Azure Active Directory> Business Applications> select the created application from the list that appears in the view.



Inicio > Aranda Software Corp | Aplicaciones empresariales > Aplicaciones empresariales

Aplicaciones empresariales | Todas las aplicaciones
Aranda Software Corp: Azure Active Directory

+ Nueva aplicación | Actualizar | Descargar (exportar) | Información de versión preliminar

Información general: Información general; Diagnosticar y solucionar problemas

Administrar: Todas las aplicaciones; Proxy de la aplicación; Configuración de usuario; Colecciones

Seguridad: Acceso condicional; Consentimiento y permisos

Vea, filtre y busque aplicaciones en su organización que estén configuradas para usar su inquilino de Azure AD como proveedor de identidades.

La lista de aplicaciones que mantiene su organización está en registros de aplicaciones.

Nombre de la Aplicación

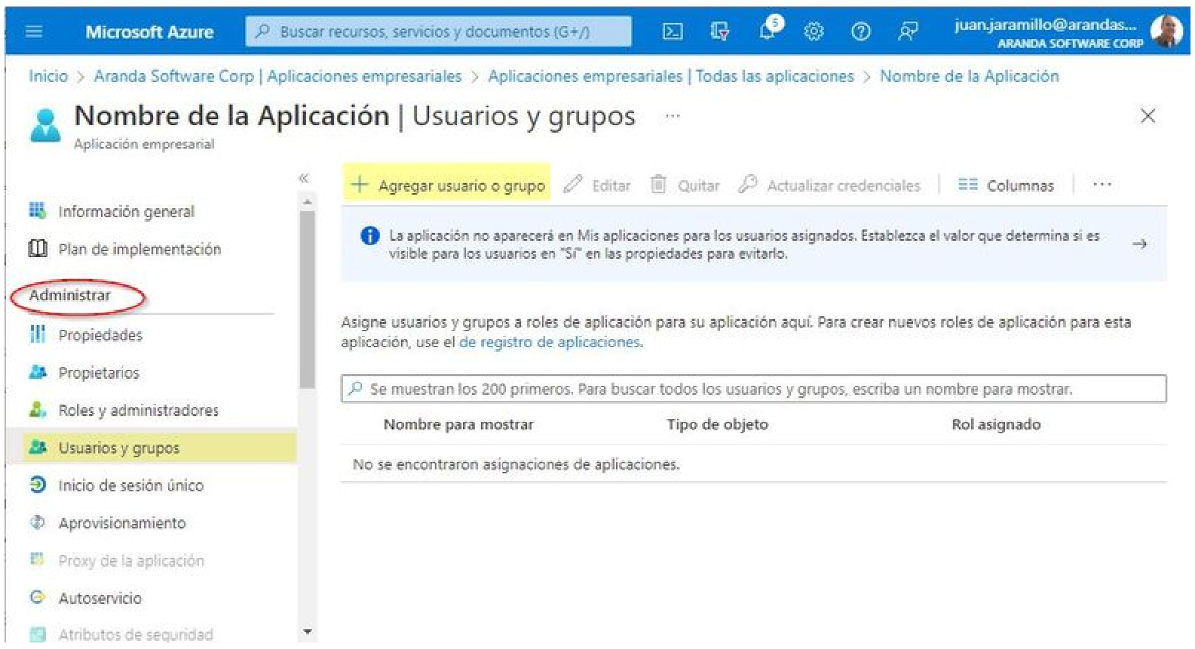
Tipo de aplicación == **Aplicaciones empresariales** | Id. de aplicación empieza con

Agregar filtros

Se encontró 1 aplicación

Nombre	Id. de objeto	Id. de aplicación	Dirección URL d...	Creada el
ND Nombre de la...	5c2f49ad-8064-4ae4...	e934ddc5-5724-46a...		24/8/2022

2. In the **Administer** Search and select **Users and groups**> and then **Add User or Group**.



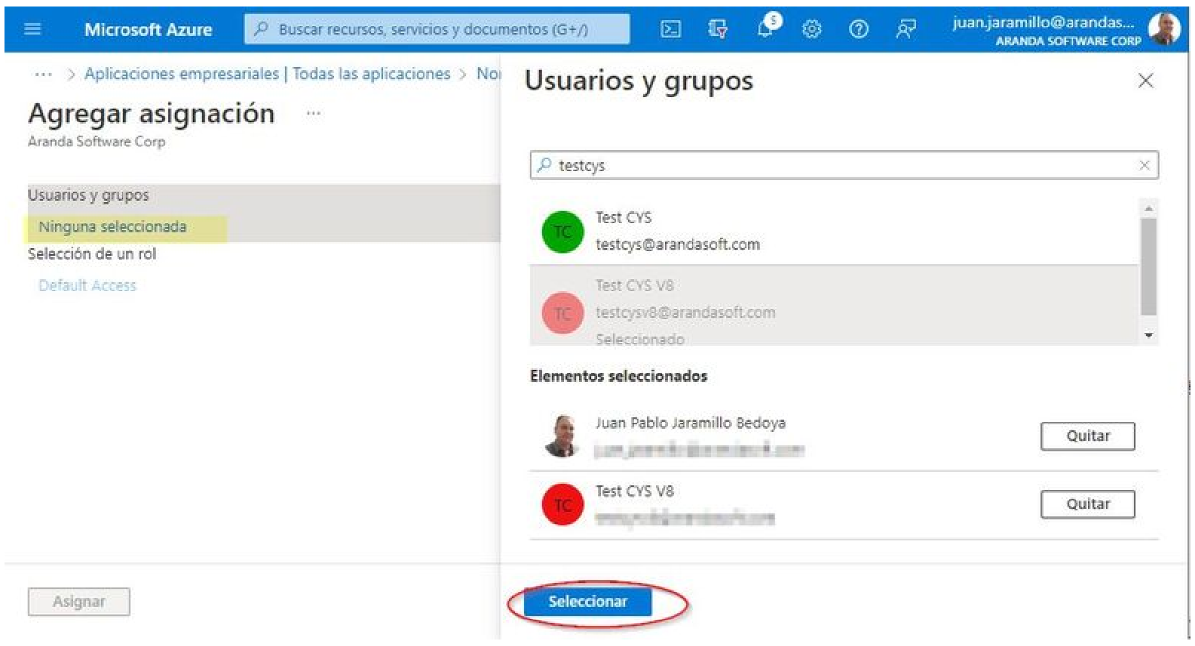
La aplicación no aparecerá en Mis aplicaciones para los usuarios asignados. Establezca el valor que determina si es visible para los usuarios en "Sí" en las propiedades para evitarlo.

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

Se muestran los 200 primeros. Para buscar todos los usuarios y grupos, escriba un nombre para mostrar.

No se encontraron asignaciones de aplicaciones.

3. In the Add Mapping view, select **None selected>** Then look for the email account(s) you want to add, when you have all the emails selected click on **Select**.



testcys

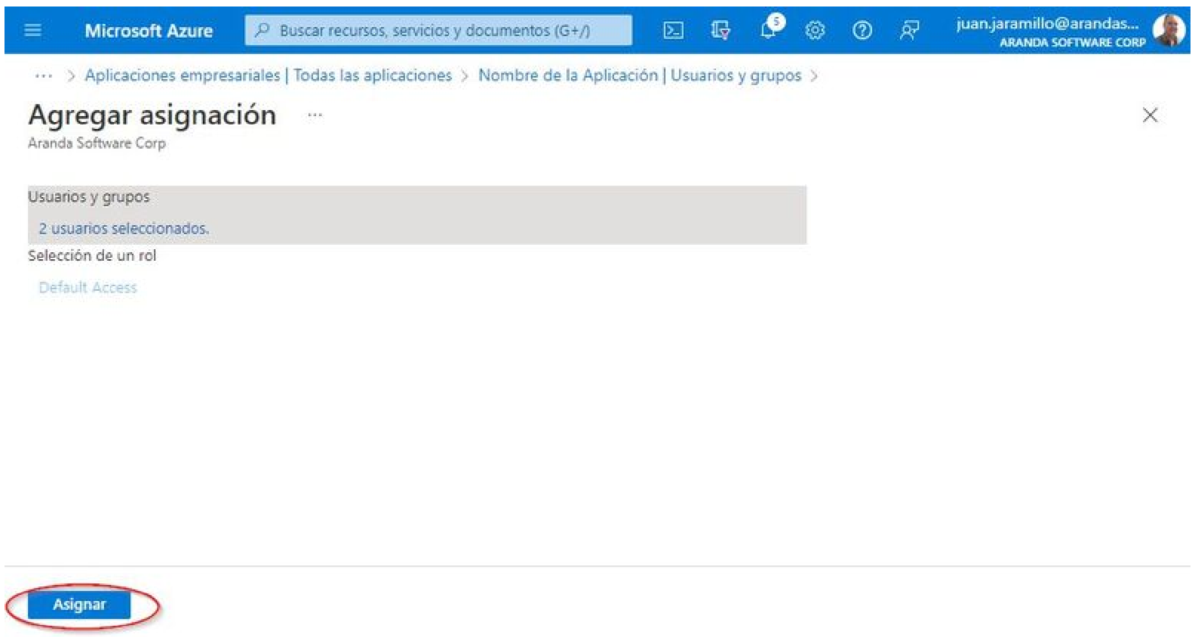
Test CYS
testcys@arandasoft.com

Test CYS V8
testcysv8@arandasoft.com
Seleccionado

Juan Pablo Jaramillo Bedoya
[redacted]

Test CYS V8
[redacted]

4. Finally select **Assign**.


Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
juan.jaramillo@arandas...
ARANDA SOFTWARE CORP
... > Aplicaciones empresariales | Todas las aplicaciones > Nombre de la Aplicación | Usuarios y grupos >
Agregar asignación
Aranda Software Corp
Usuarios y grupos
Selección de un rol
Default Access
Asignar

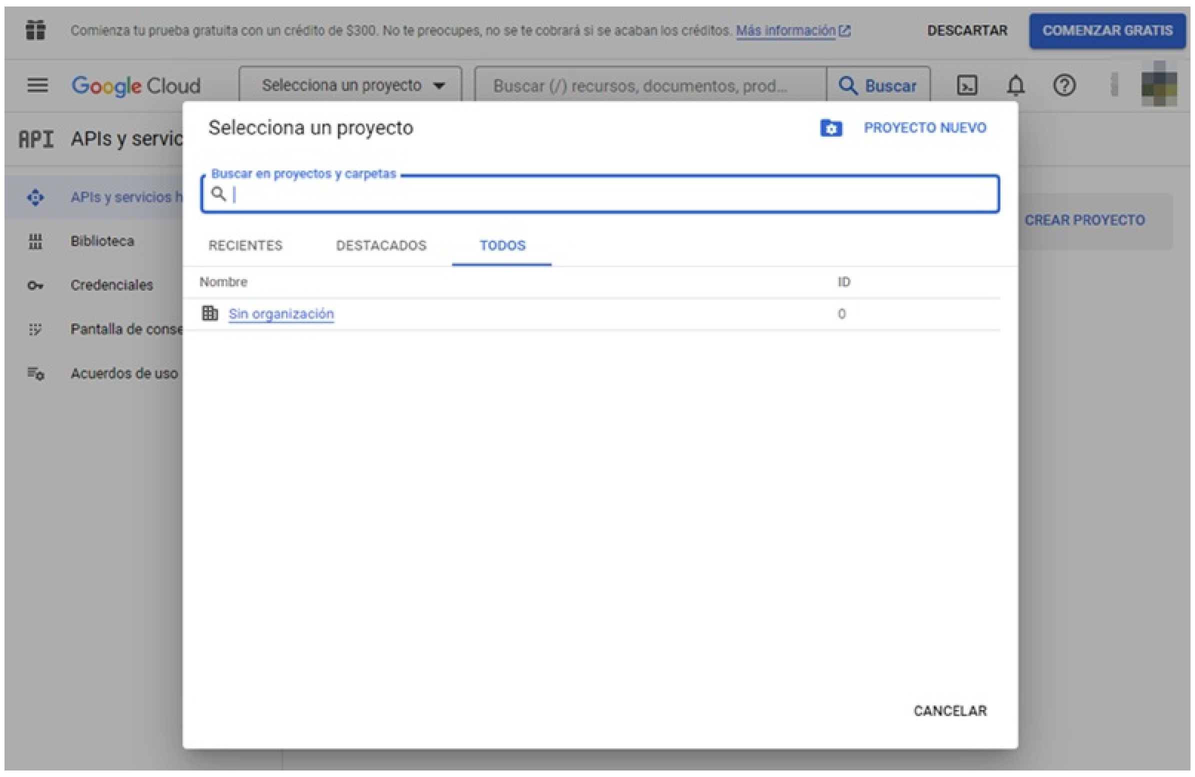
2 usuarios seleccionados.

OAuth 2.0/Google Authentication

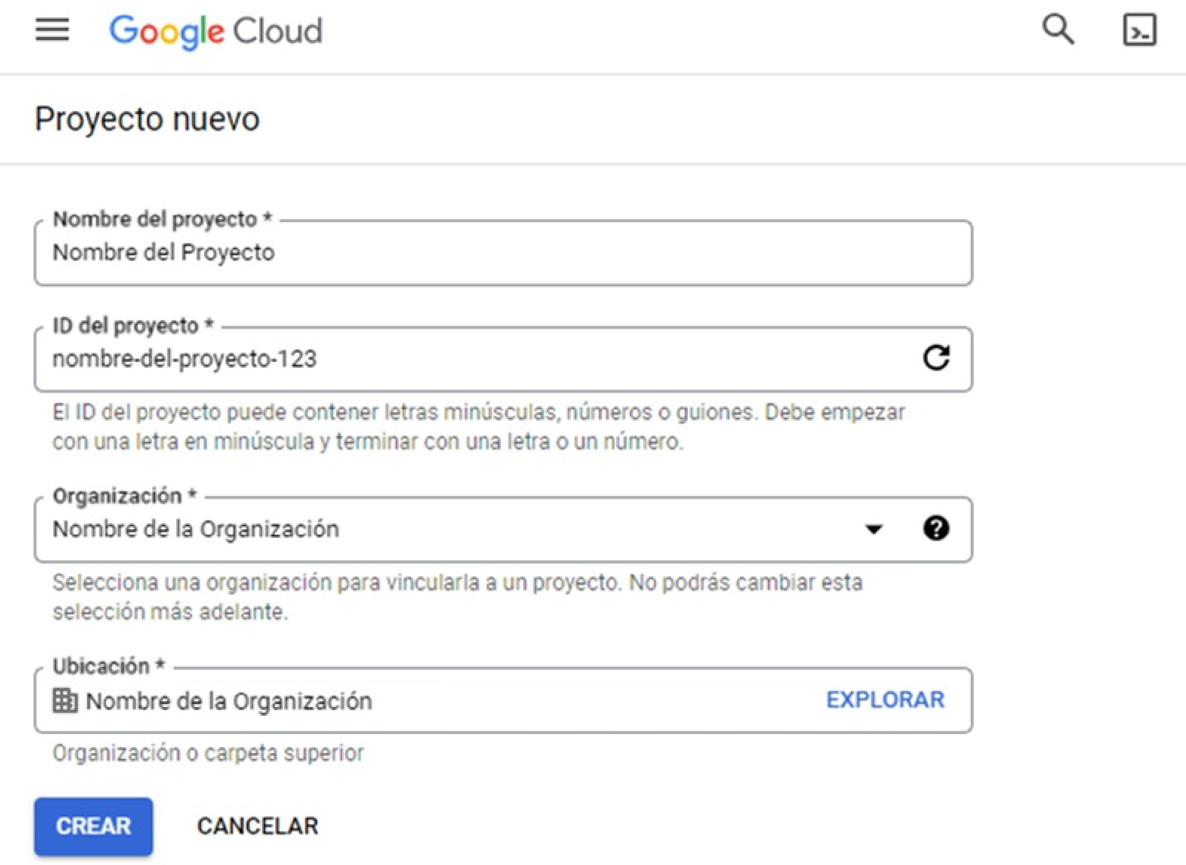
Creating a project on Google

⚐ **Note:** If you already have a project set up on Google, you can skip this step.

1. Access to the [Google Cloud Console](#) with the Google Account designated for this process, select the drop-down menu **Select a project** in the top navigation menu. Then, click the **NEW PROJECT**.



2. In the window **New project** Enter the four requested fields following the recommendations and click the**CREATE**.



Proyecto nuevo

Nombre del proyecto *
Nombre del Proyecto

ID del proyecto *
nombre-del-proyecto-123

El ID del proyecto puede contener letras minúsculas, números o guiones. Debe empezar con una letra en minúscula y terminar con una letra o un número.

Organización *
Nombre de la Organización

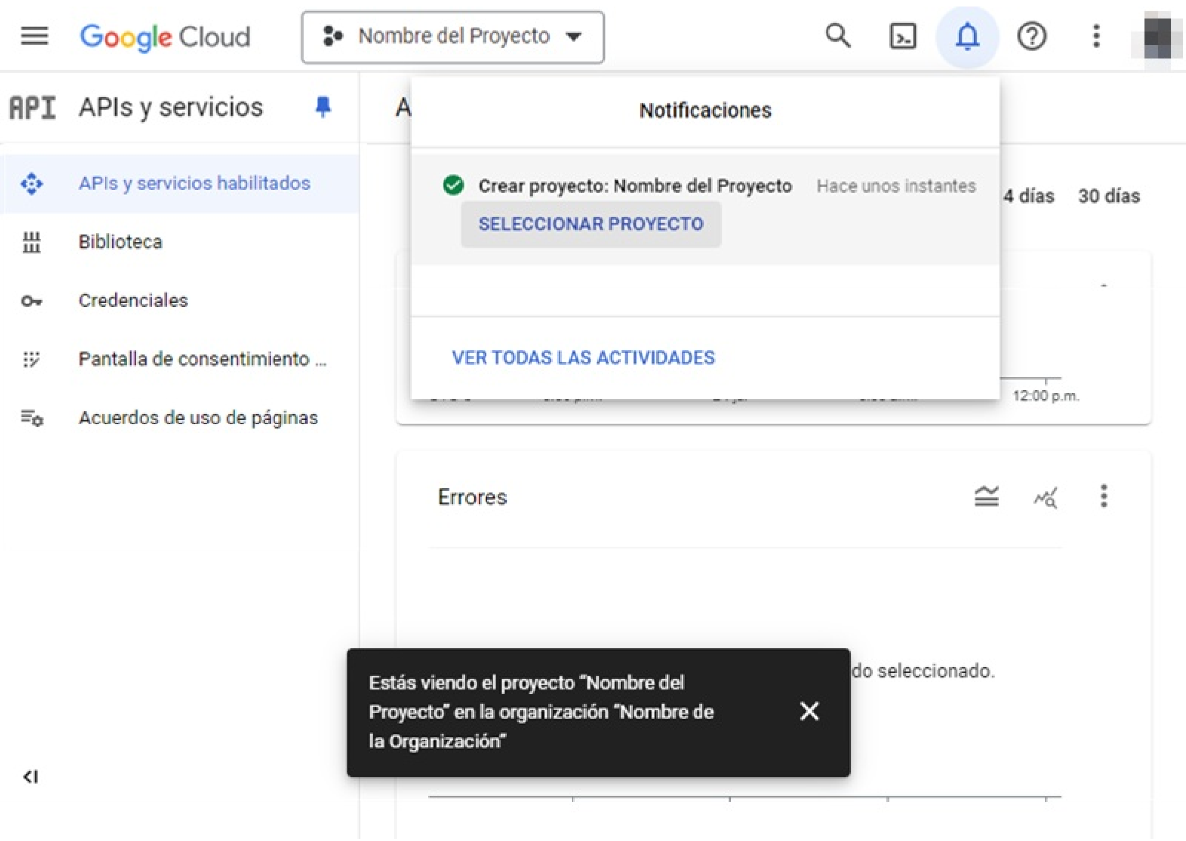
Selecciona una organización para vincularla a un proyecto. No podrás cambiar esta selección más adelante.

Ubicación *
Nombre de la Organización

Organización o carpeta superior

⚐ **Note:** If in the field **Organization** only the option is listed *No organization* is that the user with whom the project is being created does not have the required permissions.

3. The window is enabled **Notifications**. Click the **SELECT PROJECT** For the project created:



Crear proyecto: Nombre del Proyecto   Hace unos instantes

...do seleccionado.

Estás viendo el proyecto "Nombre del Proyecto" en la organización "Nombre de la Organización"

4. In the drop-down menu **Select a project** You will be able to display the name of the created project.

Create and configure your app on Google

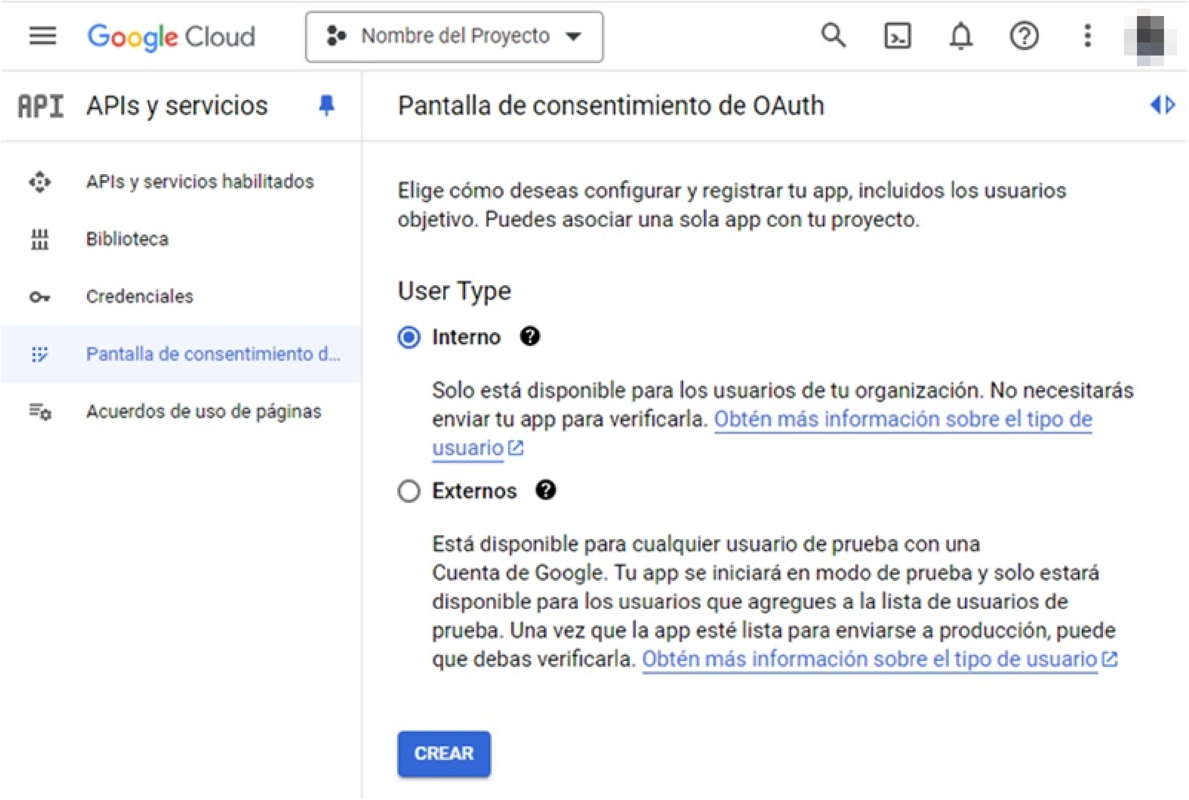
▶ Requisitos Autenticación GOOGLE: ❯

When the project is created and selected, proceed with the creation of an OAuth application as follows:

How to create an app on Google

1. In the Google Cloud Console section **APIs and services** Select the option **OAuth Consent Screen** and the type of user

- Select **Internal** if you're using a GSuite admin tenant and you're creating the app exclusively for your organization.
- Select **External** if you're trying a separate Gmail account.



Google Cloud
Nombre del Proyecto
API APIs y servicios
APIs y servicios habilitados
Biblioteca
Credenciales
Pantalla de consentimiento d...
Acuerdos de uso de páginas

Pantalla de consentimiento de OAuth

Elige cómo deseas configurar y registrar tu app, incluidos los usuarios objetivo. Puedes asociar una sola app con tu proyecto.

User Type

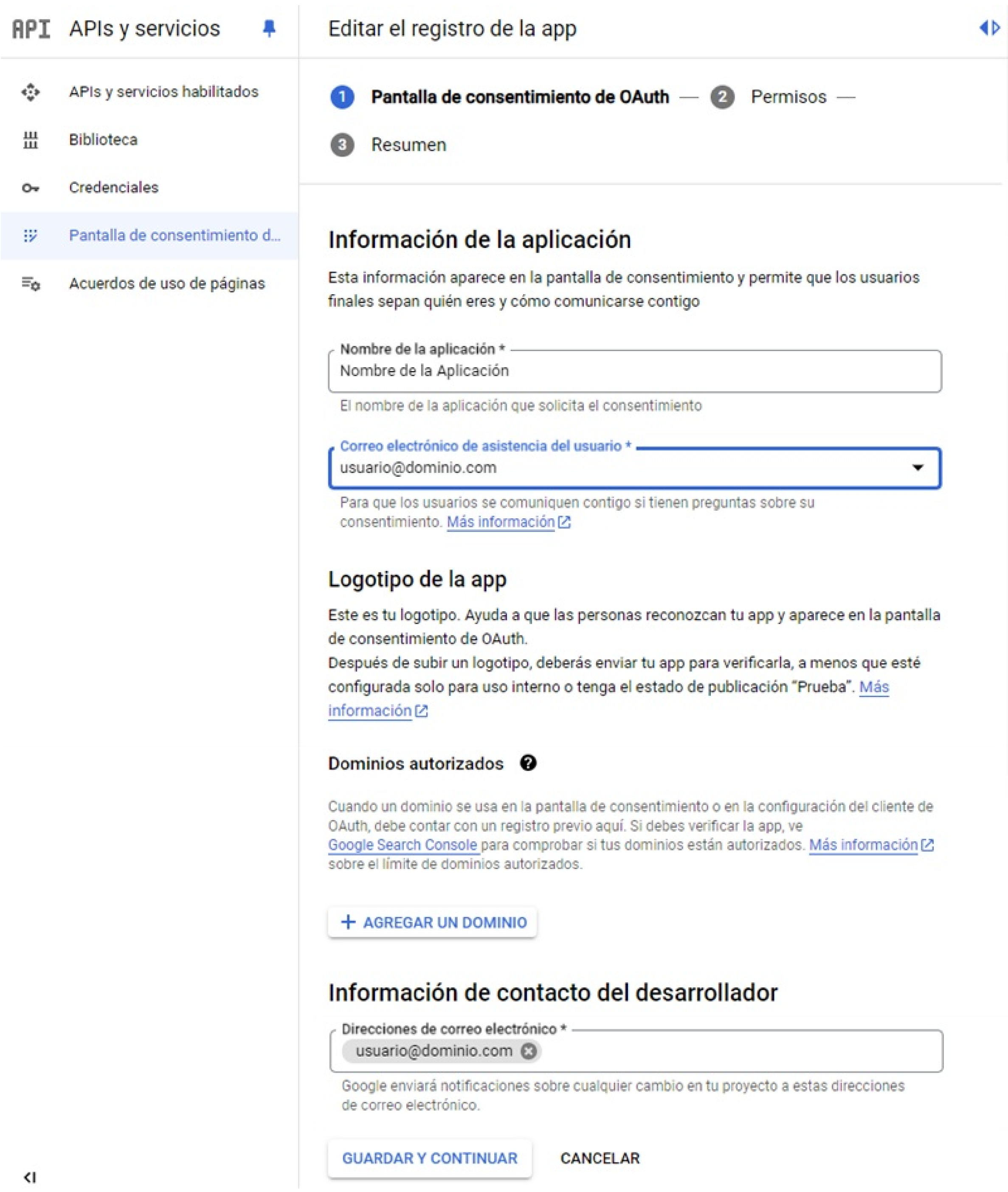
● Interno

Solo está disponible para los usuarios de tu organización. No necesitarás enviar tu app para verificarla. Obtén más información sobre el tipo de usuario

○ Externos

Está disponible para cualquier usuario de prueba con una Cuenta de Google. Tu app se iniciará en modo de prueba y solo estará disponible para los usuarios que agregues a la lista de usuarios de prueba. Una vez que la app esté lista para enviarse a producción, puede que debas verificarla. Obtén más información sobre el tipo de usuario

2. Click the **CREATE**. 3. In the window **OAuth Consent Screen** Enter the fields *App Name*, *User Support Email* in the **Application Information** and *Email addresses* in the **Developer Contact Information** according to the recommendations of each field (the other fields are optional). Then, click the **SAVE & CONTINUE**.



API APIs y servicios

APIs y servicios habilitados

Biblioteca

Credenciales

Pantalla de consentimiento d...

Acuerdos de uso de páginas

Editar el registro de la app

1 Pantalla de consentimiento de OAuth — 2 Permisos — 3 Resumen

Información de la aplicación

Esta información aparece en la pantalla de consentimiento y permite que los usuarios finales sepan quién eres y cómo comunicarse contigo

Nombre de la aplicación *: Nombre de la Aplicación

El nombre de la aplicación que solicita el consentimiento

Correo electrónico de asistencia del usuario *: usuario@dominio.com

Para que los usuarios se comuniquen contigo si tienen preguntas sobre su consentimiento. Más información

Logotipo de la app

Este es tu logotipo. Ayuda a que las personas reconozcan tu app y aparece en la pantalla de consentimiento de OAuth.
Después de subir un logotipo, deberás enviar tu app para verificarla, a menos que esté configurada solo para uso interno o tenga el estado de publicación "Prueba". Más información

Dominios autorizados

Cuando un dominio se usa en la pantalla de consentimiento o en la configuración del cliente de OAuth, debe contar con un registro previo aquí. Si debes verificar la app, ve Google Search Console para comprobar si tus dominios están autorizados. Más información sobre el límite de dominios autorizados.

+ AGREGAR UN DOMINIO

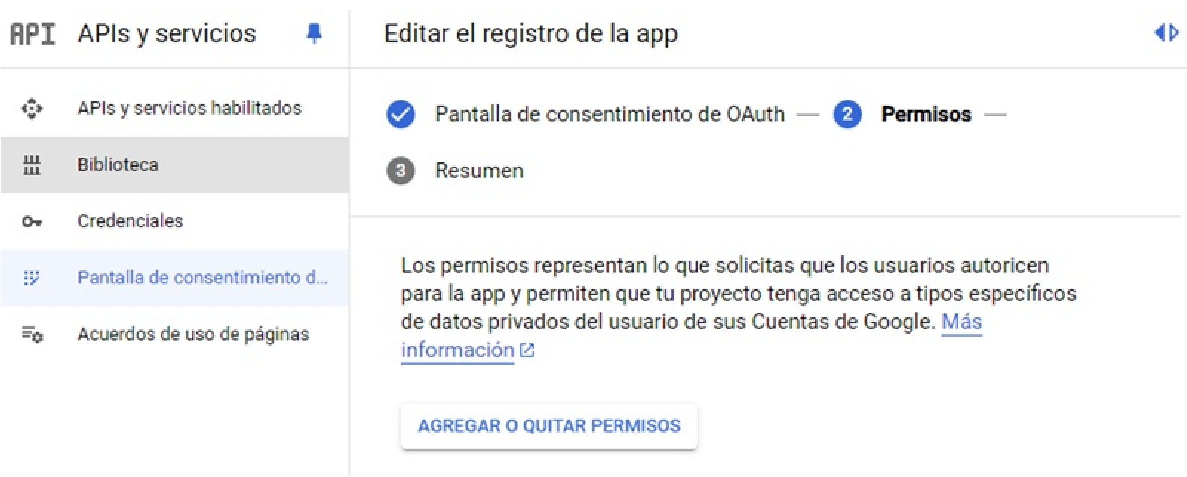
Información de contacto del desarrollador

Direcciones de correo electrónico *: usuario@dominio.com

Google enviará notificaciones sobre cualquier cambio en tu proyecto a estas direcciones de correo electrónico.

GUARDAR Y CONTINUAR CANCELAR

4. In the window Permissions Click the ADD OR REMOVE PERMISSIONS.



API APIs y servicios

APIs y servicios habilitados

Biblioteca

Credenciales

Pantalla de consentimiento d...

Acuerdos de uso de páginas

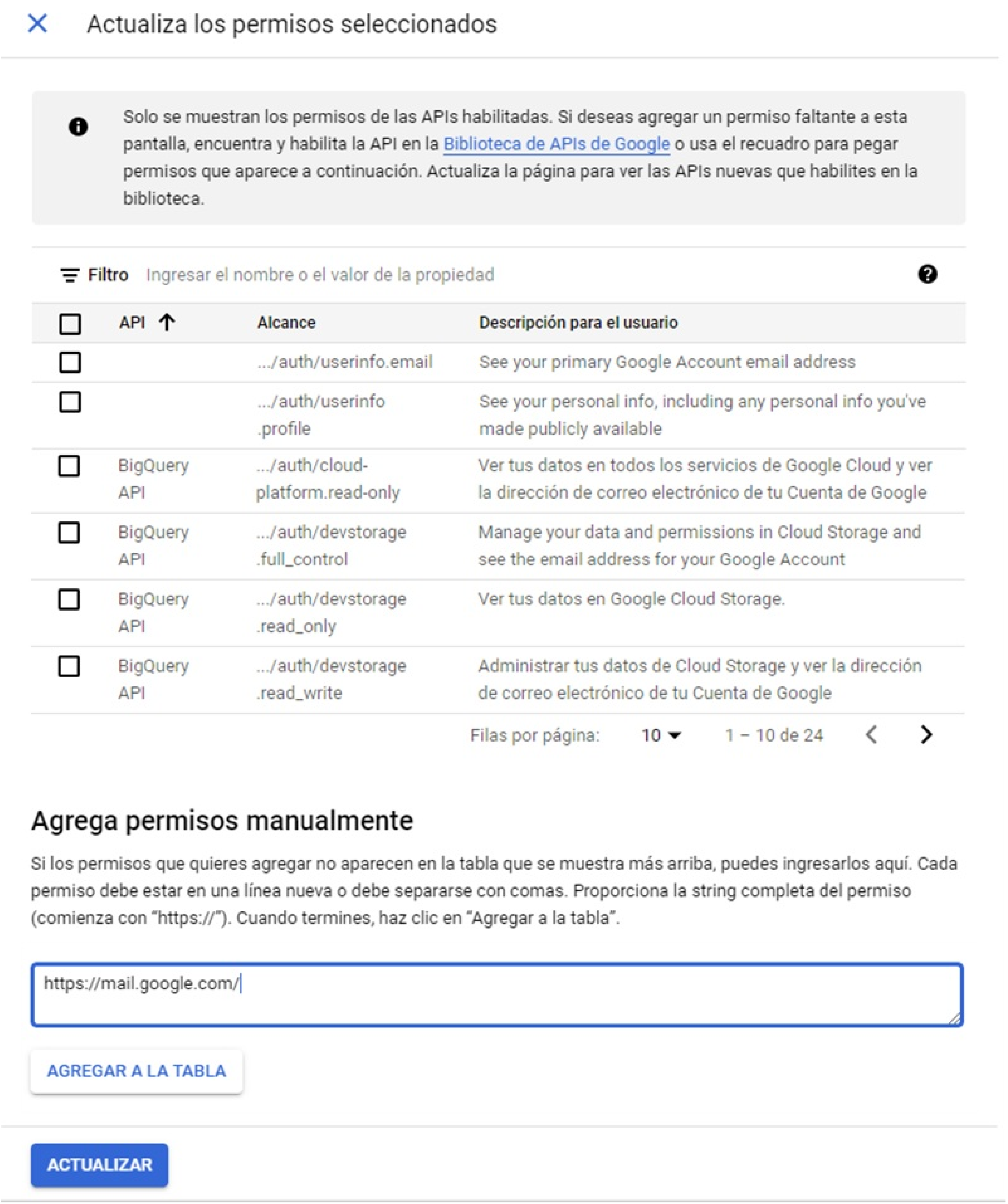
Editar el registro de la app

✓ Pantalla de consentimiento de OAuth — 2 Permisos — 3 Resumen

Los permisos representan lo que solicitas que los usuarios autoricen para la app y permiten que tu proyecto tenga acceso a tipos específicos de datos privados del usuario de sus Cuentas de Google. Más información

AGREGAR O QUITAR PERMISOS

5. In the window Update selected permissions in the Add permissions manually Enter the value https://mail.google.com/ and click the ADD TO TABLE. Then in UPDATE.



✕ Actualiza los permisos seleccionados

Solo se muestran los permisos de las APIs habilitadas. Si deseas agregar un permiso faltante a esta pantalla, encuentra y habilita la API en la Biblioteca de APIs de Google o usa el recuadro para pegar permisos que aparece a continuación. Actualiza la página para ver las APIs nuevas que habilites en la biblioteca.

Filtro Ingresar el nombre o el valor de la propiedad

□	API ↑	Alcance	Descripción para el usuario
□		.../auth/userinfo.email	See your primary Google Account email address
□		.../auth/userinfo .profile	See your personal info, including any personal info you've made publicly available
□	BigQuery API	.../auth/cloud-platform.read-only	Ver tus datos en todos los servicios de Google Cloud y ver la dirección de correo electrónico de tu Cuenta de Google
□	BigQuery API	.../auth/devstorage .full_control	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
□	BigQuery API	.../auth/devstorage .read_only	Ver tus datos en Google Cloud Storage.
□	BigQuery API	.../auth/devstorage .read_write	Administrar tus datos de Cloud Storage y ver la dirección de correo electrónico de tu Cuenta de Google

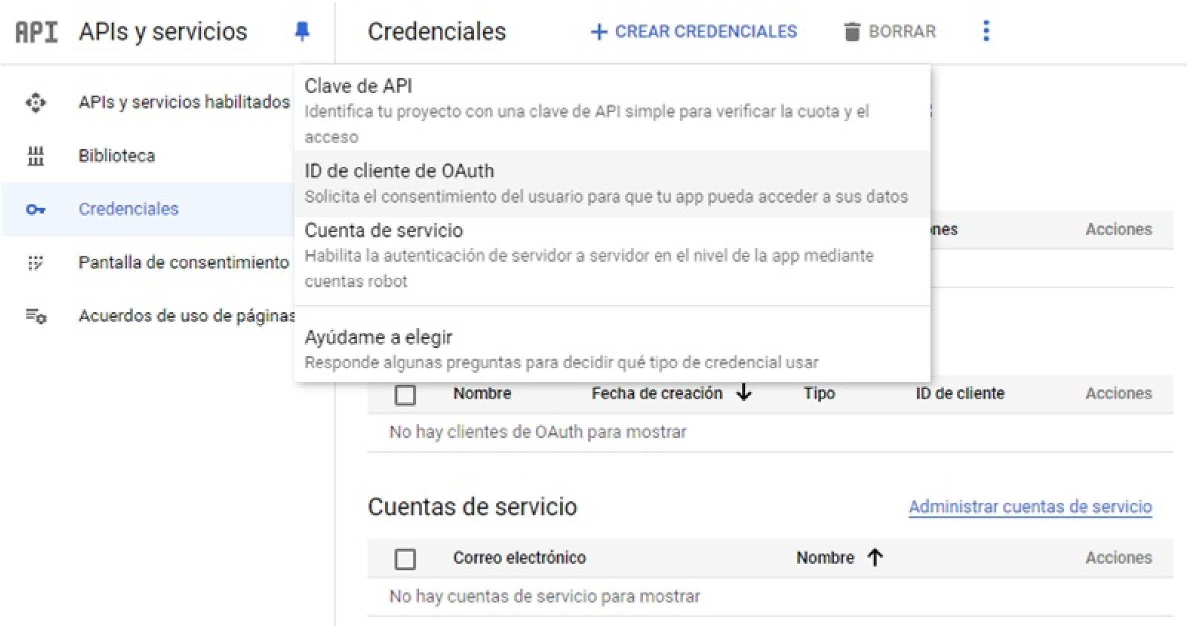
Filas por página: 10 ▾ 1 – 10 de 24 ‹ ›

Agrega permisos manualmente

Si los permisos que quieres agregar no aparecen en la tabla que se muestra más arriba, puedes ingresarlos aquí. Cada permiso debe estar en una línea nueva o debe separarse con comas. Proporciona la string completa del permiso (comienza con "https://"). Cuando termines, haz clic en "Agregar a la tabla".

https://mail.google.com/

6. In the window **Permissions** Verify that the permission has been added in the **Your restricted permissions** and click the **SAVE & CONTINUE** to advance to the window **Summary** where you can view the data from the new application. 7. Select the option **Credentials**, click the **CREATE CREDENTIALS** and select the **OAuth Client ID**.



API APIs y servicios
Credenciales
+ CREAR CREDENCIALES
BORRAR
APIs y servicios habilitados
Biblioteca
Credenciales
Pantalla de consentimiento
Acuerdos de uso de páginas

Clave de API
Identifica tu proyecto con una clave de API simple para verificar la cuota y el acceso

ID de cliente de OAuth
Solicita el consentimiento del usuario para que tu app pueda acceder a sus datos

Cuenta de servicio
Habilita la autenticación de servidor a servidor en el nivel de la app mediante cuentas robot

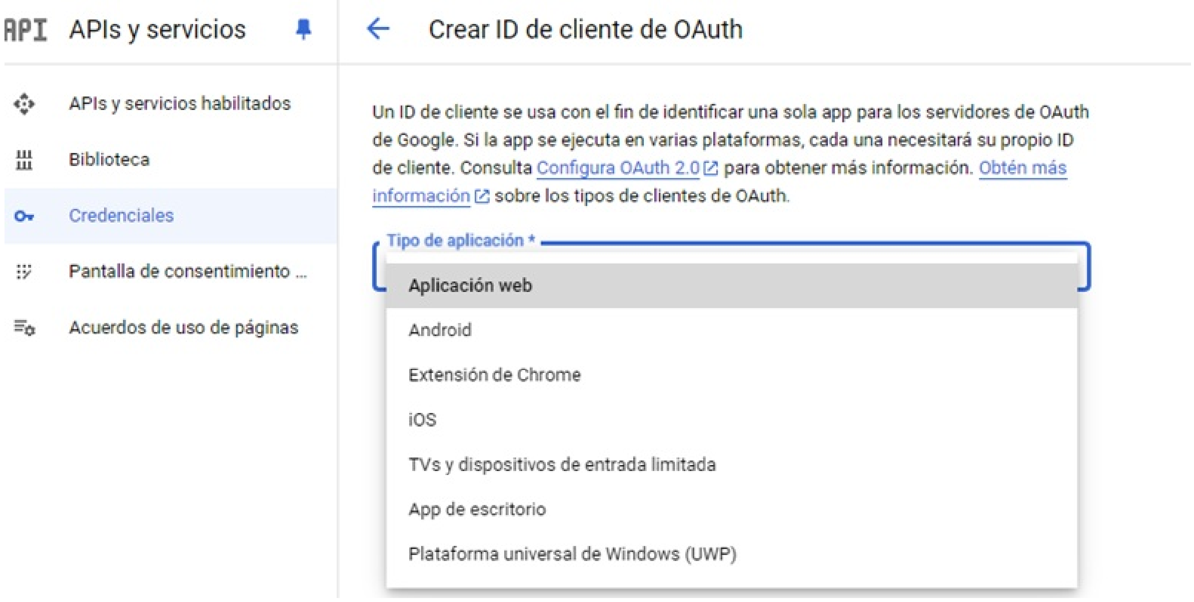
Ayúdame a elegir
Responde algunas preguntas para decidir qué tipo de credencial usar

□	Nombre	Fecha de creación ↓	Tipo	ID de cliente	Acciones
	No hay clientes de OAuth para mostrar				

Cuentas de servicio — Administrar cuentas de servicio

□	Correo electrónico	Nombre ↑	Acciones
	No hay cuentas de servicio para mostrar		

8. In the window **Create OAuth Client ID** In the field *Application Type*, select the **Web application**.


API APIs y servicios
APIs y servicios habilitados
Biblioteca
Credenciales
Pantalla de consentimiento ...
Acuerdos de uso de páginas

Crear ID de cliente de OAuth

Un ID de cliente se usa con el fin de identificar una sola app para los servidores de OAuth de Google. Si la app se ejecuta en varias plataformas, cada una necesitará su propio ID de cliente. Consulta Configura OAuth 2.0 para obtener más información. Obtén más información sobre los tipos de clientes de OAuth.

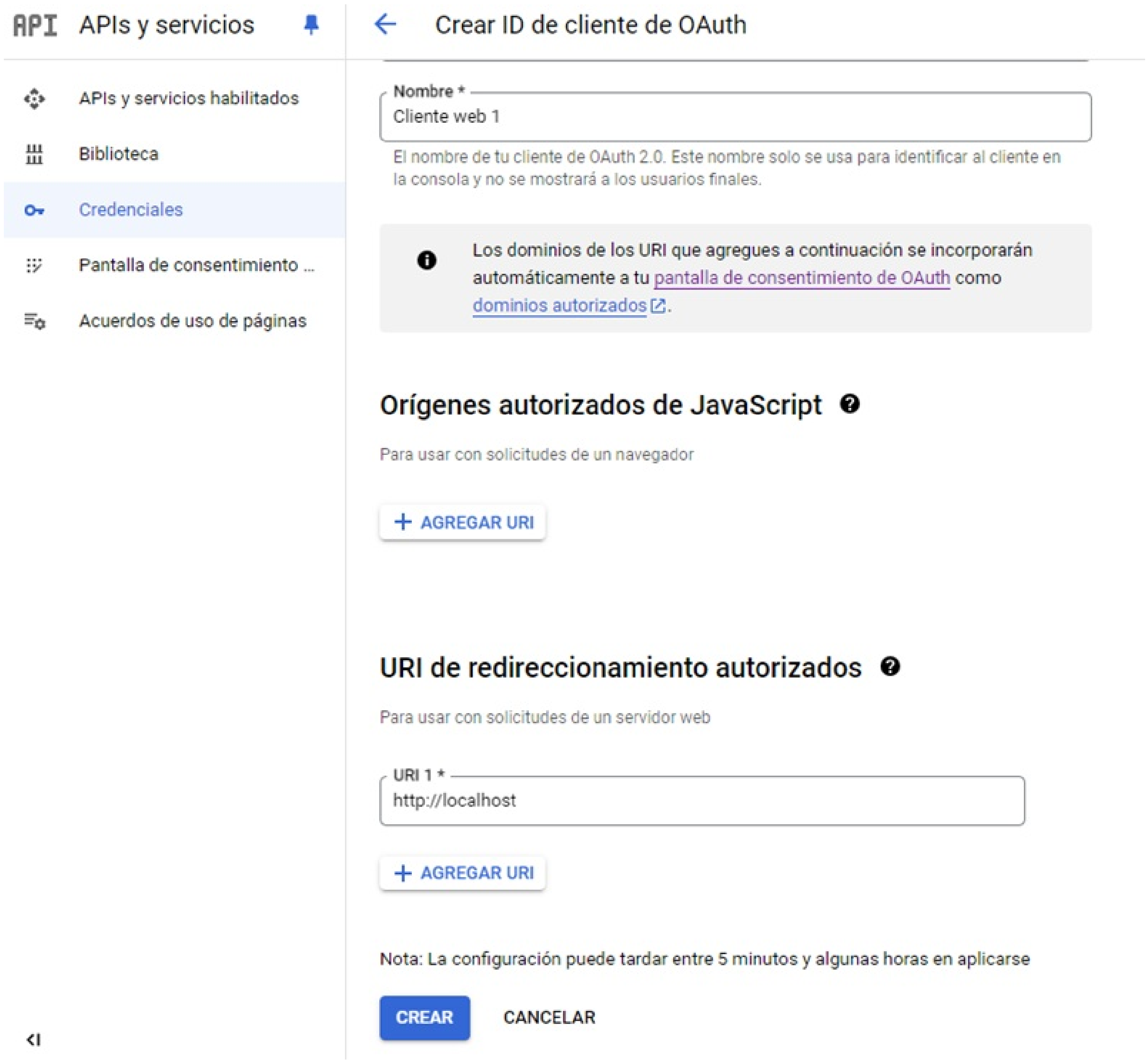
Tipo de aplicación *

- Aplicación web
- Android
- Extensión de Chrome
- iOS
- TVs y dispositivos de entrada limitada
- App de escritorio
- Plataforma universal de Windows (UWP)

9. In the window **Create OAuth Client ID** in the **Authorized redirect URIs**, enter the appropriate URI for each product:

- **Aranda Service Management (ASMS)** as follows:
- **Output Server:** https://[domain]/ASMSAdministrator/Main/Pages/OauthToken.aspx
- **Input Server (Case Creator):** (http://localhost)
- For all other Aranda products, the authorized redirect URI is: https://[domain]/api/oauth2

Finally, click the **CREATE**.


API APIs y servicios
APIs y servicios habilitados
Biblioteca
Credenciales
Pantalla de consentimiento ...
Acuerdos de uso de páginas
AGREGAR URI
AGREGAR URI
CREAR
CANCELAR

Crear ID de cliente de OAuth

Nombre *
Cliente web 1

El nombre de tu cliente de OAuth 2.0. Este nombre solo se usa para identificar al cliente en la consola y no se mostrará a los usuarios finales.

Los dominios de los URI que agregues a continuación se incorporarán automáticamente a tu pantalla de consentimiento de OAuth como dominios autorizados.

Orígenes autorizados de JavaScript

Para usar con solicitudes de un navegador

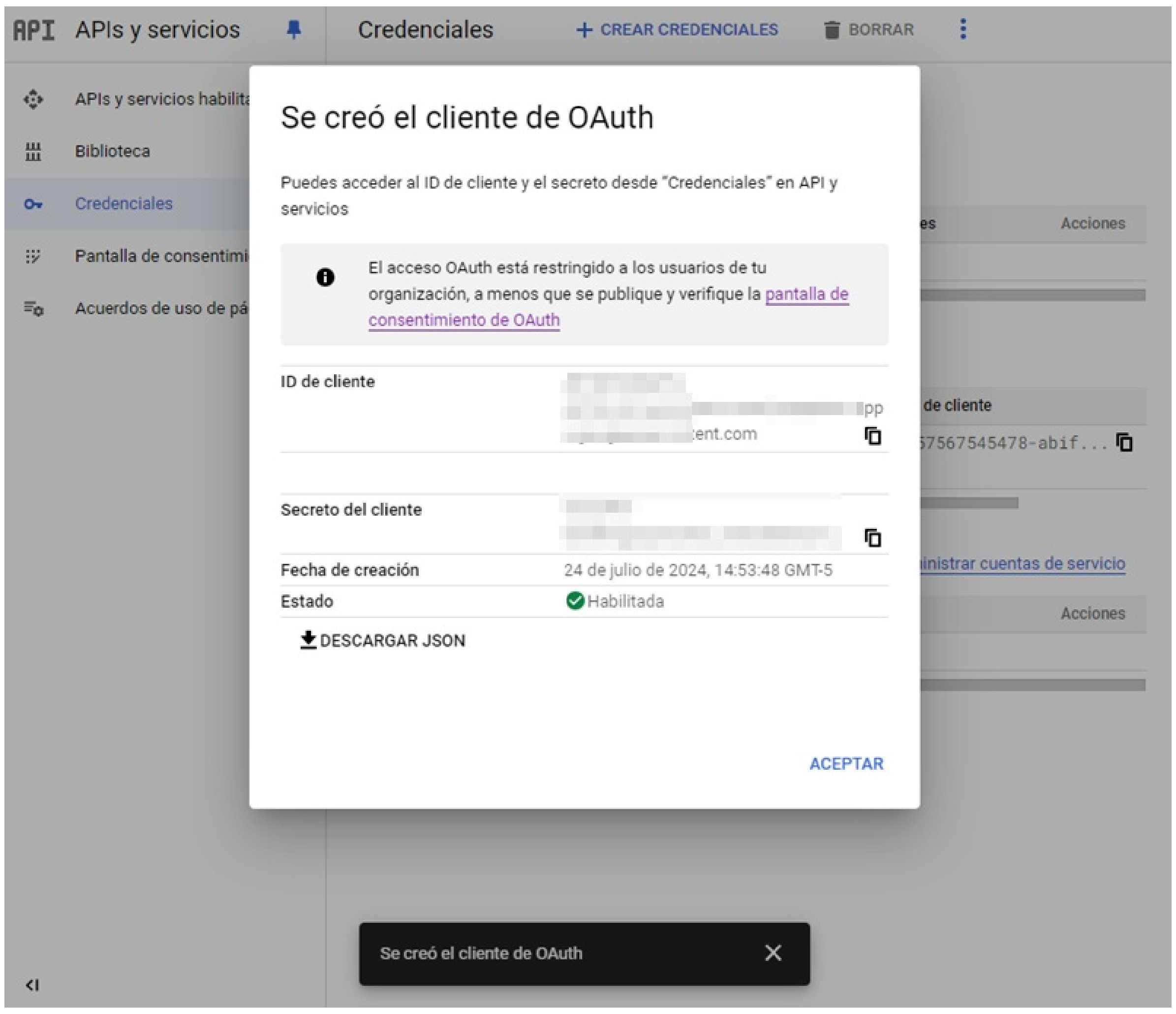
URI de redireccionamiento autorizados

Para usar con solicitudes de un servidor web

URI 1 *
http://localhost

Nota: La configuración puede tardar entre 5 minutos y algunas horas en aplicarse

10. In the window **The OAuth client was created** save the following data that is required for configuration in Aranda applications and in the generation of the Access Token and Refresh Token.



Se creó el cliente de OAuth

Puedes acceder al ID de cliente y el secreto desde "Credenciales" en API y servicios

El acceso OAuth está restringido a los usuarios de tu organización, a menos que se publique y verifique la pantalla de consentimiento de OAuth

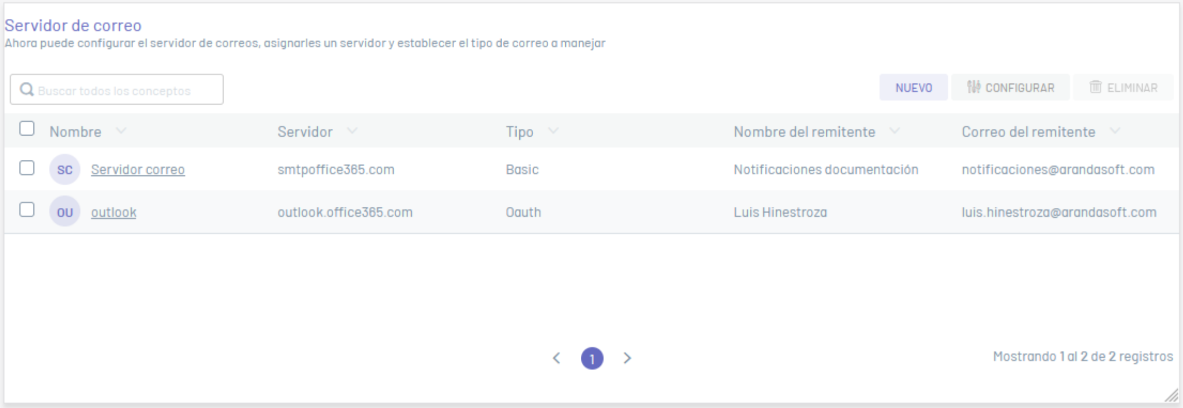
ID de cliente	[redacted]
Secreto del cliente	[redacted]
Fecha de creación	24 de julio de 2024, 14:53:48 GMT-5
Estado	✓ Habilitada

- Client ID -> Client ID.
- Client Secret Value -> Client Secret.
- -> token url https://oauth2.googleapis.com/token.
- Authorization url -> https://accounts.google.com/o/oauth2/v2/auth?access_type=offline&prompt=consent

Mail Server Management

View Mail Server

1. In the Mail Server information view, you can view the list of servers grouped by basic mail server data and the type of authentication.



Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

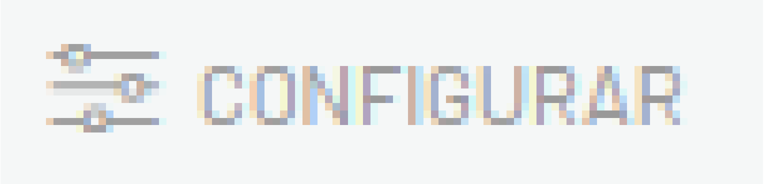
□	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
□	SC Servidor correo	smtpoffice365.com	Basic	Notificaciones documentación	notificaciones@arandasoft.com
□	OU outlook	outlook.office365.com	Oauth	Luis Hinestroza	luis.hinestroza@arandasoft.com

Mostrando 1 al 2 de 2 registros

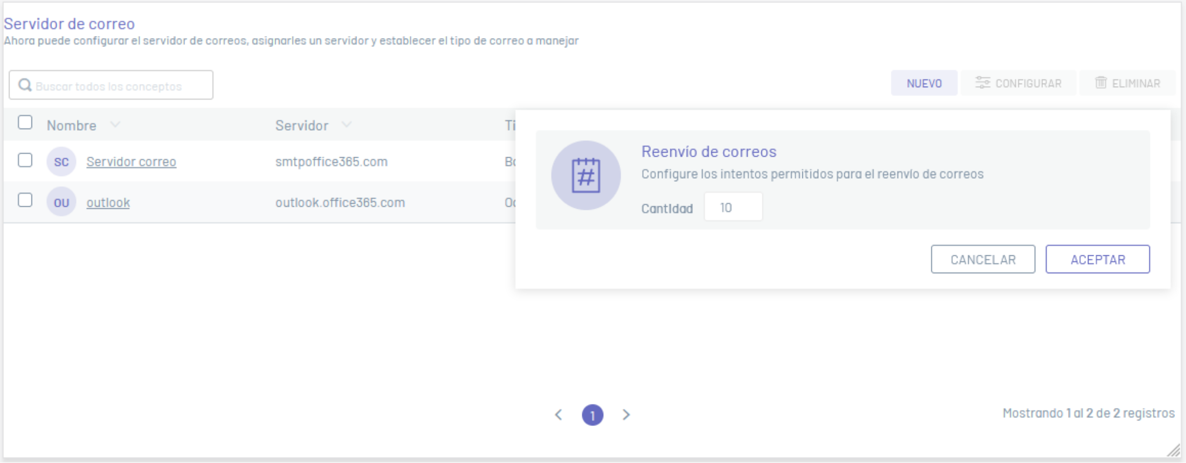
2. En la vista de información de servidor de correo, tendrá habilitadas acciones de gestión y organización de la información.Vista de Información en Entorno Commons

Set up mail forwarding

To perform mail forwarding settings, in the Server Information view, select the



and you can configure the attempts allowed for mail forwarding.



Servidor de correo
Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

Buscar todos los conceptos

Nombre	Servidor	Ti
SC Servidor correo	smtpoffice365.com	Bı
OU outlook	outlook.office365.com	Oı

Reenvío de correos
Configure los intentos permitidos para el reenvío de correos
Cantidad 10

Mostrando 1 al 2 de 2 registros

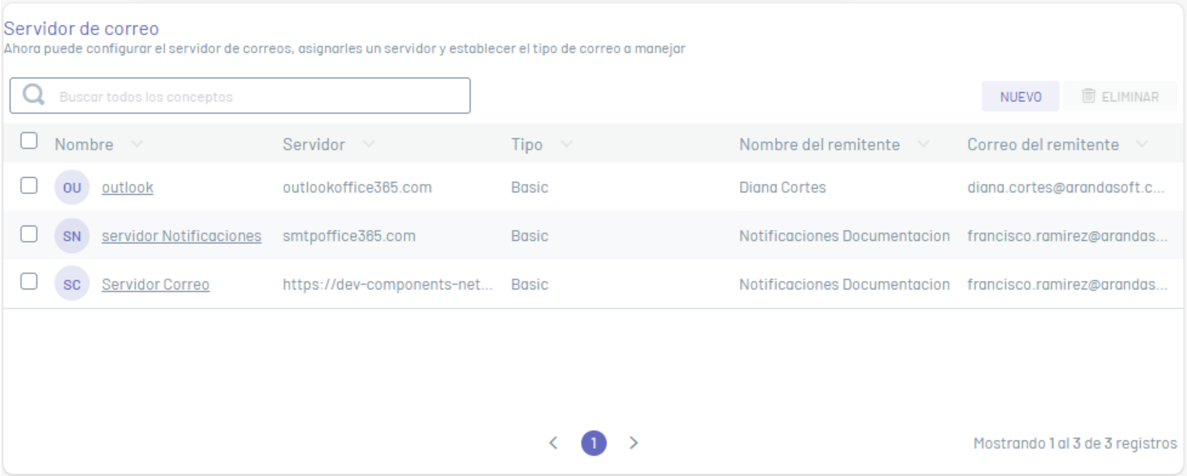
⚠ **Important**: Only a maximum of 100 attempts are allowed for mail forwarding. If this condition is not met, the default configuration of the Common will be taken.

🔗Related Links:

- Create Mail Server
- Edit Mail Server
- Delete Mail Server

Create Mail Server

1. In the mail server information view, select the **New**



Servidor de correo
Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

Buscar todos los conceptos

Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
OU outlook	outlookoffice365.com	Basic	Diana Cortes	diana.cortes@arandasoft.c...
SN servidor Notificaciones	smtpoffice365.com	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...
SC Servidor Correo	https://dev-components-net...	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...

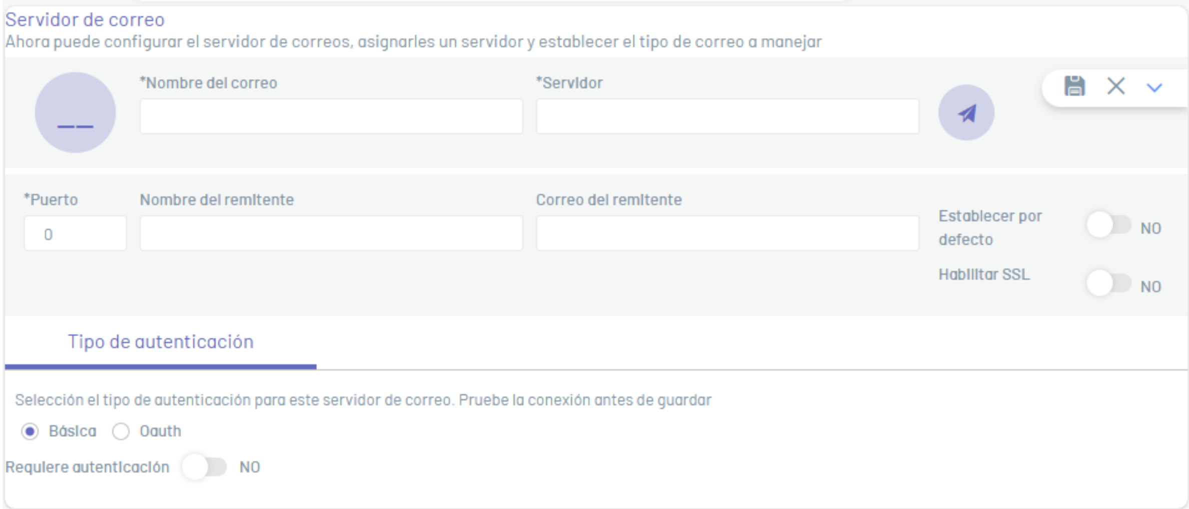
Mostrando 1 al 3 de 3 registros

Basic Facts

2. In the window that is enabled you will be able to fill in the basic data of the mail server and the type of authentication

3. In the basic server data you will be able to enter fields such as name, server, port, name and sender's mail.

Each of the directory services fields must take into account the Specifications for Common Fields



Servidor de correo
Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

*Nombre del correo
*Servidor
*Puerto 0
Nombre del remitente
Correo del remitente
Establecer por defecto NO
Habilitar SSL NO

Tipo de autenticación

Selección el tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

● Básica ○ Oauth

Requiere autenticación NO

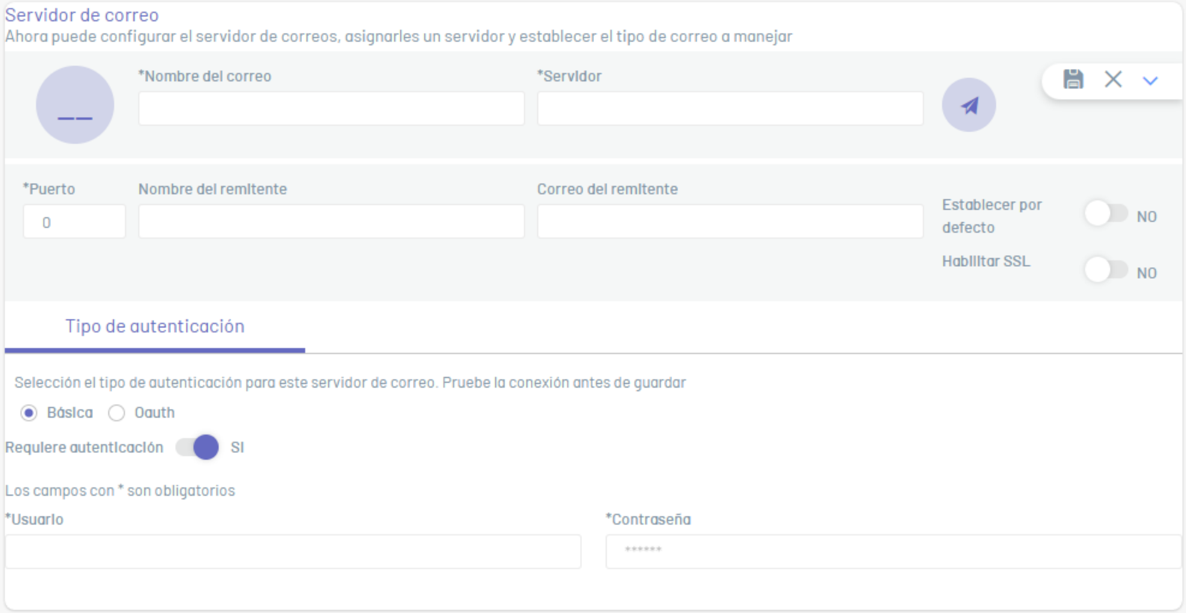
4. On the **Authentication Type**, you can select the available options by type of provider:

- Basic Authentication

- Oauth Authentication

Basic Authentication

5. For Basic Authentication, enable the **Requires Authentication** and enter the mail server login and password required.



Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

*Nombre del correo

*Servidor

*Puerto: 0

Nombre del remitente

Correo del remitente

Establecer por defecto: NO

Habilitar SSL: NO

Tipo de autenticación

Selección el tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

● Básica ○ Oauth

Requiere autenticación: SI

Los campos con * son obligatorios

*Usuario

*Contraseña: ******

Oauth Authentication (Open Authorization)

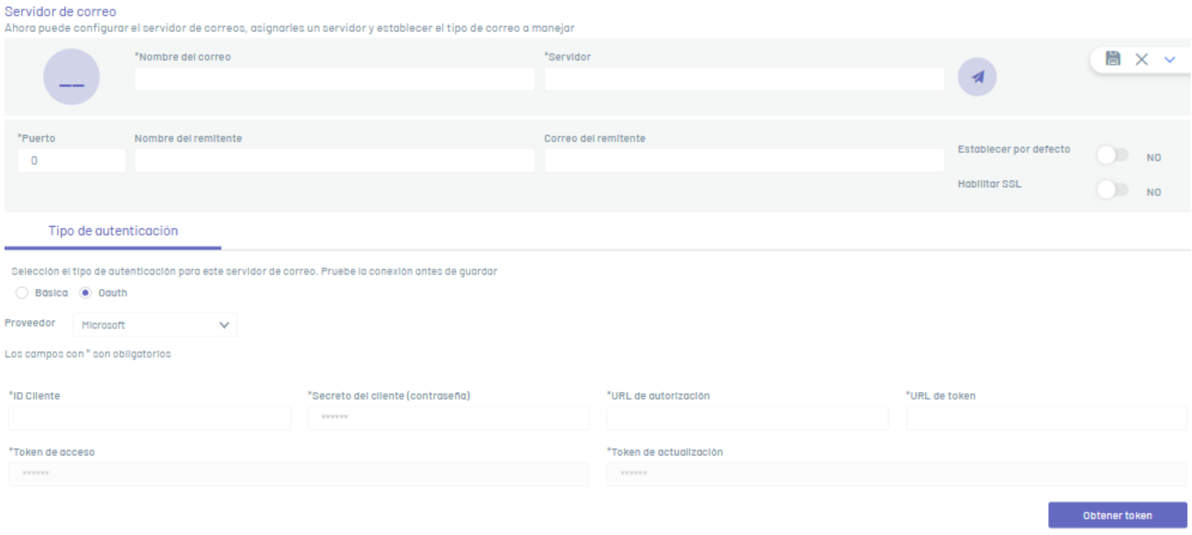
6. For OAuth authentication, define an authentication provider (Microsoft, Google, Manual Configuration).

> ⚐ **Note:** Yes **Microsoft** is the Authentication provider, pre-configure the relevant information to the Oauth mail provider in the Azure portal, generating the required parameters for the mail server authentication fields:

- Client ID, authorization url, and token url
- Client Secret

> ⚐ **Note:** Yes **Google** If you are the Authentication provider, you can pre-configure the relevant information to the Oauth mail provider in the Google portal, generating the required parameters for the mail server authentication fields:

- Client ID, Authorization URL, Token URL, and Client Secret



Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

*Nombre del correo

*Servidor

*Puerto: 0

Nombre del remitente

Correo del remitente

Establecer por defecto: NO

Habilitar SSL: NO

Tipo de autenticación

Selección el tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

○ Básica ● Oauth

Proveedor: Microsoft

Los campos con * son obligatorios

*ID Cliente

*Secreto del cliente (contraseña): ******

*URL de autorización

*URL de token

*Token de acceso: ******

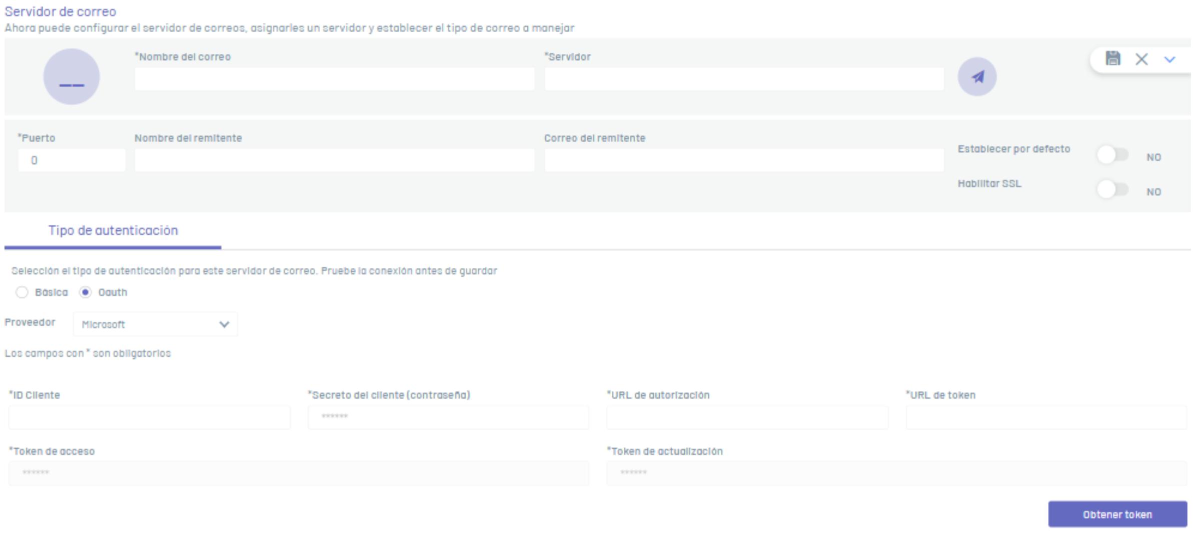
*Token de actualización: ******

7. For each supplier you can define the required fields such as customer ID, customer secret, authorization url, among others. Each of the mail server fields for the Oauth authentication type must be taken into account Specifications for Common Fields.

8. If the connection is with a provider **Microsoft or Google** You can obtain the access token and the update token by clicking **Get Token** and then authenticate to the provider.

> ⚐ **Note:** In case the supplier is **Google** and you have previously obtained the access token and the refresh token, first Revoke the Permit from your profile to allow the refresh token to be sent again. **Google** It only

sends the token the first time the request is made.



Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

*Nombre del correo

*Servidor

*Puerto: 0

Nombre del remitente

Correo del remitente

Establecer por defecto: NO

Habilitar SSL: NO

Tipo de autenticación

Selección el tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

○ Básica ● Oauth

Proveedor: Microsoft

Los campos con * son obligatorios

*ID Cliente

*Secreto del cliente (contraseña): ******

*URL de autorización

*URL de token

*Token de acceso: ******

*Token de actualización: ******

9. Si la conexión es con un proveedor Oauth diferente a **Microsoft ó Google** podrá establecer la **Configuración Manual** y pegar los valores de token de accesso y el token de actualización directamente. 10. If you wish, you can perform a test of sending mail by clicking on the

⚐ **Note:** The test email will be sent to the email that has been filled out in the field*Sender's mail*

11. When you finish configuring the mail server, click the**Save**

to confirm the changes made.

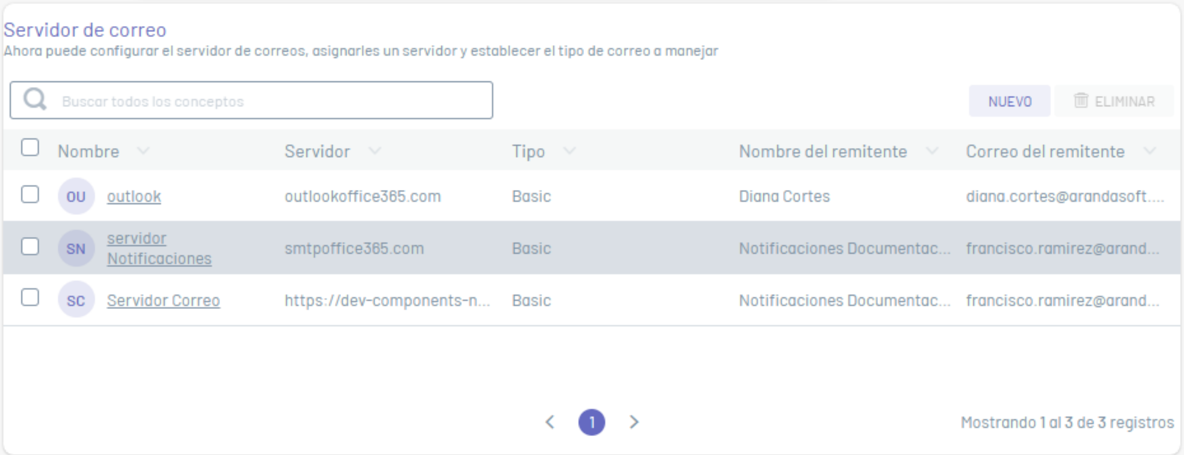
⚐ **Note:** :

- Only vendors that have the full fields, including the Access Token and Refresh Token fields, can be saved

- If you have created more than one mail server configuration, only one of them can be marked as a configuration By default.

Edit Mail Server

1. To edit a mail server, in the Server Information view, select a record from the existing mail list.

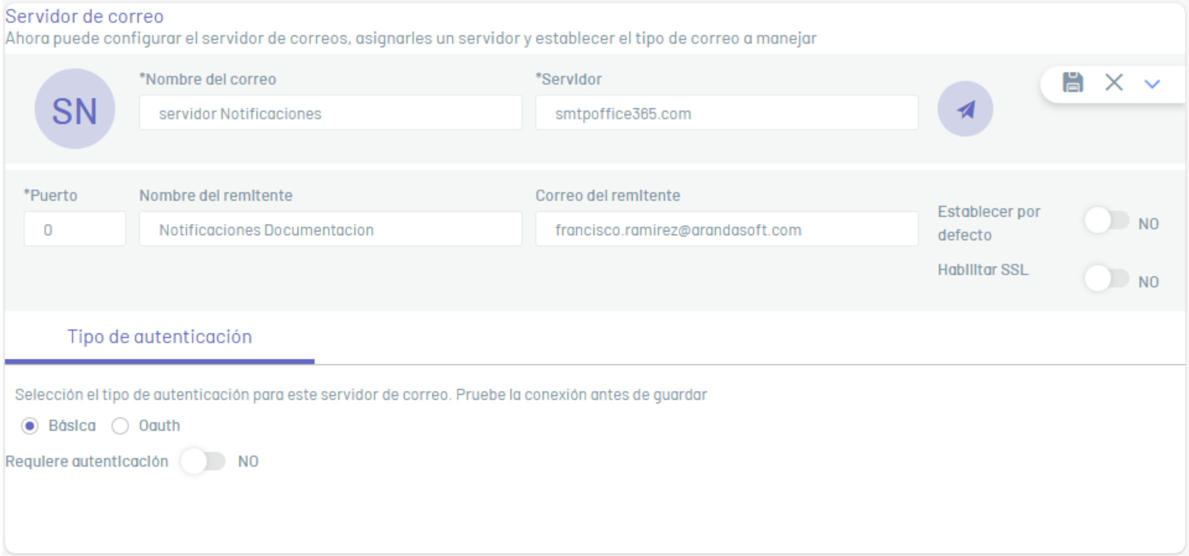


Servidor de correo
Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
□	OU outlook	outlookoffice365.com	Basic	Diana Cortes	diana.cortes@arandasoft....
□	SN servidor Notificaciones	smtpoffice365.com	Basic	Notificaciones Documentac...	francisco.ramirez@arand...
□	SC Servidor Correo	https://dev-components-n...	Basic	Notificaciones Documentac...	francisco.ramirez@arand...

Mostrando 1 al 3 de 3 registros

2. The Mail Server window is enabled, where you can modify the basic data of the mail server or authentication type.



Servidor de correo
Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

SN
*Nombre del correo: servidor Notificaciones
*Servidor: smtpoffice365.com
*Puerto: 0
Nombre del remitente: Notificaciones Documentacion
Correo del remitente: francisco.ramirez@arandasoft.com
Establecer por defecto: NO
Habilitar SSL: NO

Tipo de autenticación

Selección el tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar
● Básica ○ Oauth
Requiere autenticación: NO

⚐ **Note:** If you need to update a vendor's access token and refresh token **Oauth** guy **Google** or **Microsoft** Enter the field **Client Secret** again to perform the update.

3. When you finish editing the mail server, click the **Save**

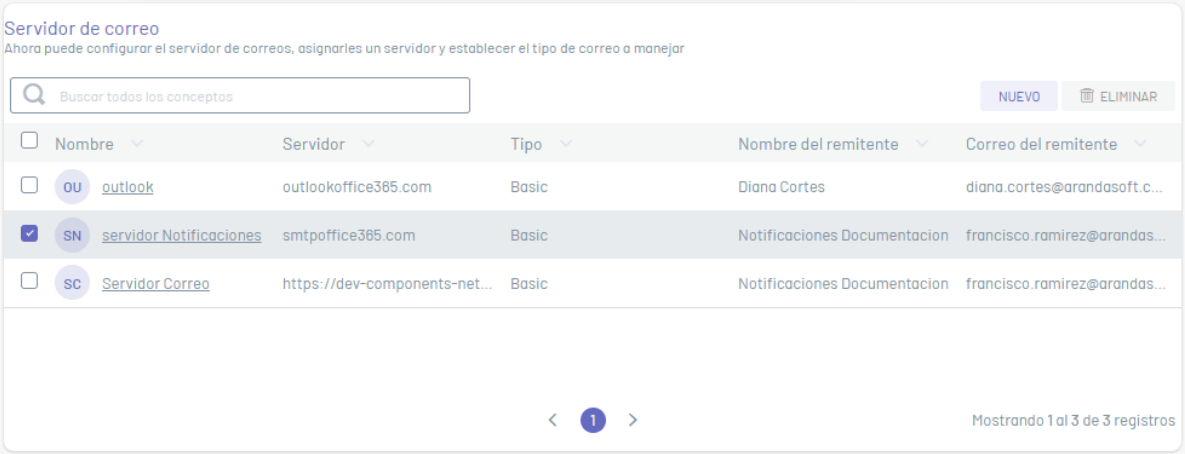
to confirm the changes made.

Delete Mail Server

1. In the Mail Server Information view, select a record from the list of mail services that you want to delete, and click

the

.



Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

□	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
□	OU outlook	outlookoffice365.com	Basic	Diana Cortes	diana.cortes@arandasoft.c...
☑	SN servidor Notificaciones	smtpoffice365.com	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...
□	SC Servidor Correo	https://dev-components-net...	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...

2. You will be able to display a confirmation message to validate the deletion action.

Specification Fields

Mail Server/Basic Data

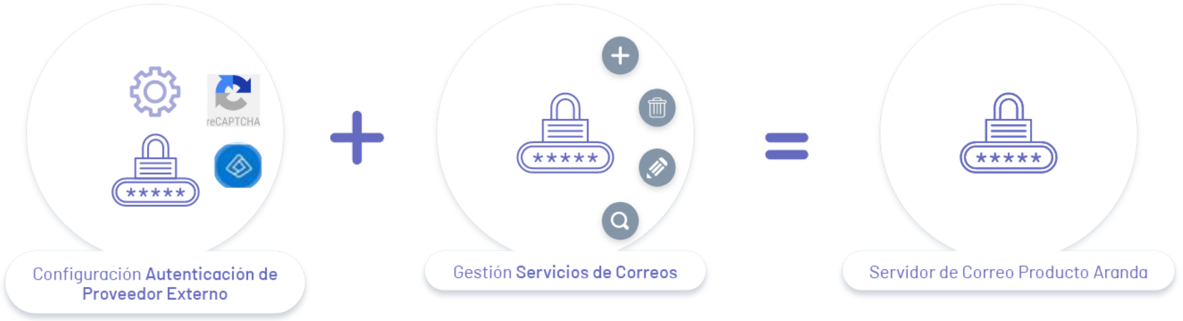
Field	Description
Name	The name of the server that allows mail to be transported.
Server	DNS name of the mail server. - If the provider is Microsoft for business, the server is: *outlook.office365.com* - If the provider is Google, the server is: *smtp.gmail.com* - If you are a different provider, please refer to the provider's documentation
Send Test Email	This button Defines the action to send a test mail to the configured mail server.
Port	TCP Service Operation Port
Sender name	Name of the sender of the notification of the emails
Sender's mail	Sender's email address
Set by Default	Indicates whether you want that provider to be the only one authorized to send mail in AES
Enable SSL	Indicates whether your connection uses secure protocol

Mail Server/Oauth Authentication Types

Field	Description	Supplier
Client ID	Client ID given by your Oauth provider.	Microsoft/Google/Manual Settings
Secret Key	Password	Microsoft/Google/Manual Settings
Authorization URL	URL address to be able to carry out the authorization.	Microsoft/Google/Manual Settings
Url Token	URL for authorization token generation.	Microsoft/Google/Manual Settings
Access Token	This will be generated during the credential generation process.	Microsoft/Google/Manual Settings
Refresh Token	This will be generated during the credential generation process	Microsoft/Google/Manual Settings

Directory Service Module

Pre-Configuration Directory Services


reCAPTCHA
Configuración Autenticación de Proveedor Externo
Gestión Servicios de Correos
Servidor de Correo Producto Aranda

1. Configuring Authentication Providers

Configure providers (LDAP, Microsoft Entra ID) for Active Directory user synchronization processes.

For more information, see the Microsoft Entra ID ↪ Sync.

2. reCAPTCHA Configuration (Optional)

Configure a security level in the authentication processes, defining the Google reCAPTCHA configuration to be used at the time of user login.

For more information, see the reCAPTCHA ↪ Security Configuration.

3. Management Module Directory Services

In the Directory Server module, you can create, update, and delete email server configurations for notifications that will be sent to users from the web console.

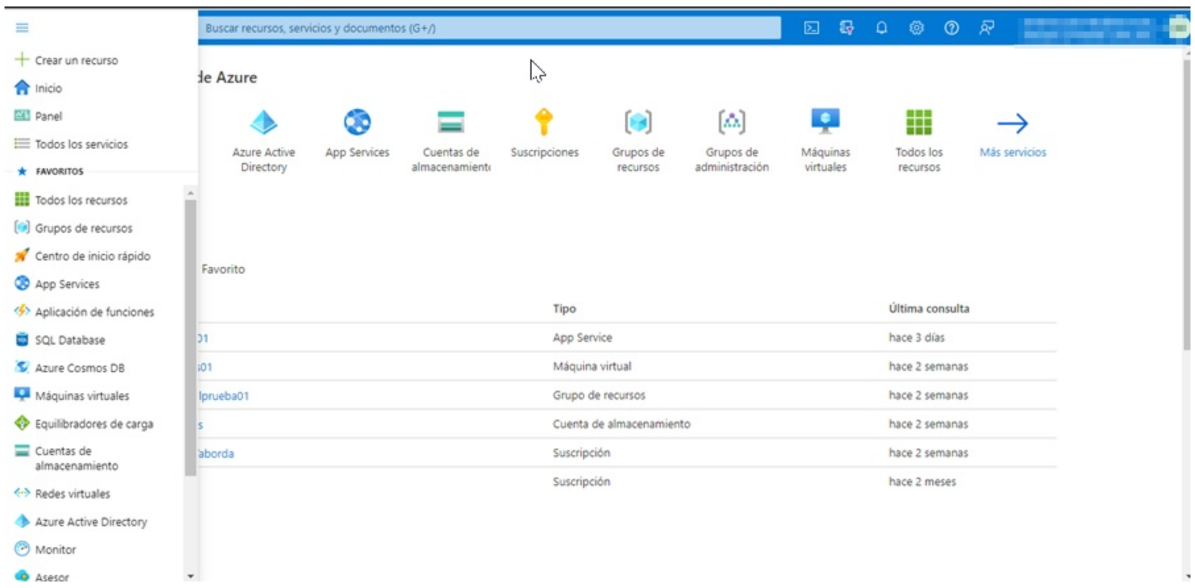
For more information, see the Management of Directory Service ↪.

Ldap/Microsoft Entra ID Synchronization

Build your app in Azure

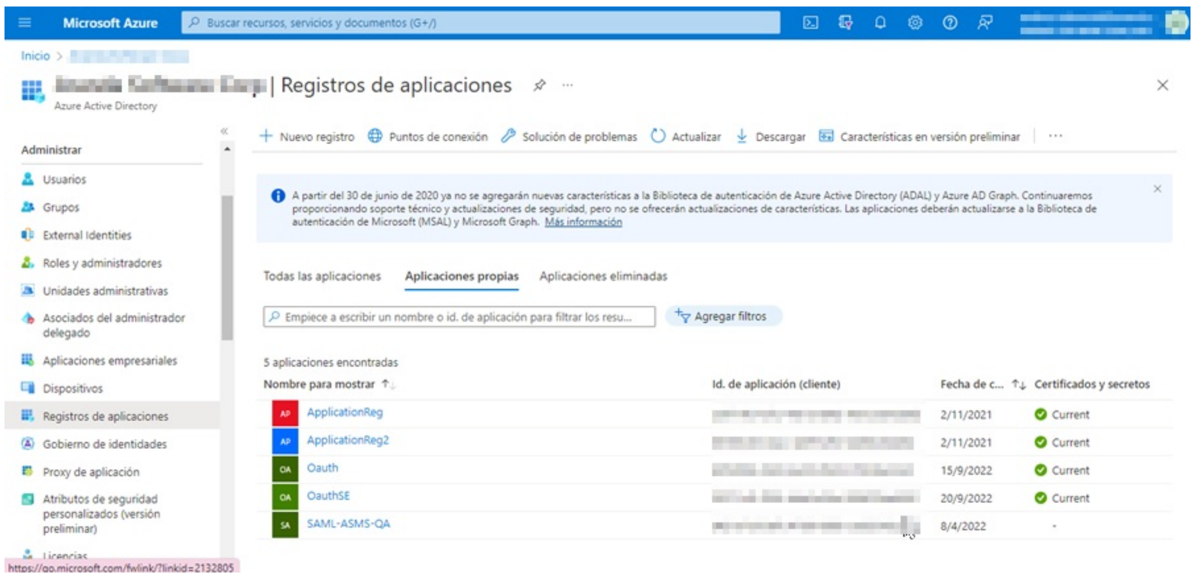
▶ Requisitos Autenticación Azure: ❯

1. Access the Azure portal [View Microsoft Azure](https://portal.azure.com) , search and select **Microsoft Enter ID**.



	Tipo	Última consulta
01	App Service	hace 3 días
:01	Máquina virtual	hace 2 semanas
lprueba01	Grupo de recursos	hace 2 semanas
s	Cuenta de almacenamiento	hace 2 semanas
aborda	Suscripción	hace 2 semanas
	Suscripción	hace 2 meses

2. . In the **Administer** Search and select **Application logs**, click **New Registration**.

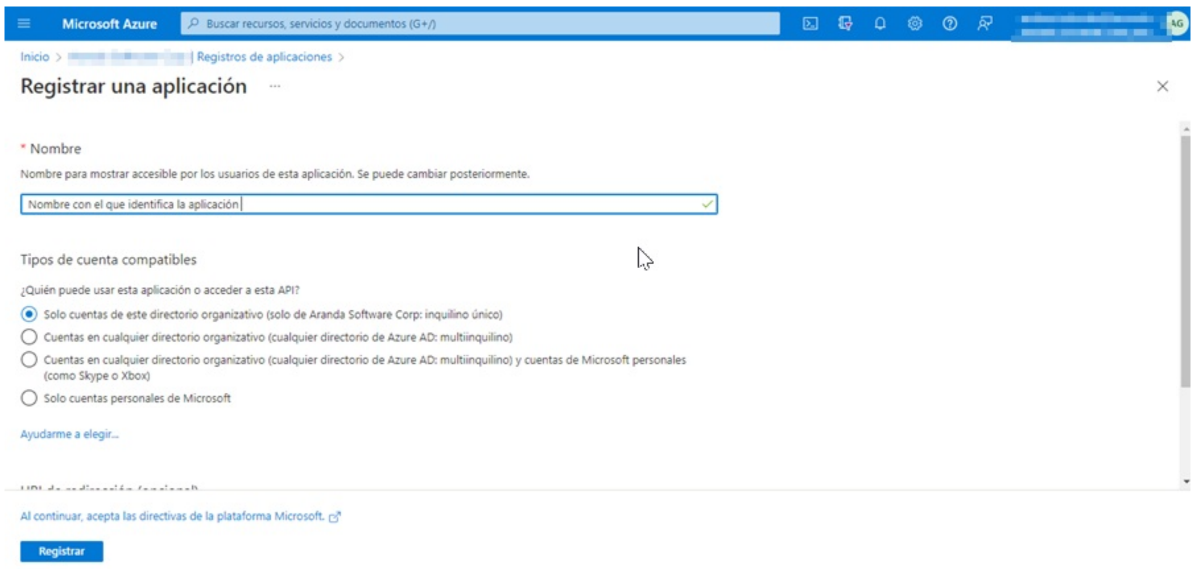

Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
Inicio >
| Registros de aplicaciones
Azure Active Directory
Nuevo registro
Puntos de conexión
Solución de problemas
Actualizar
Descargar
Características en versión preliminar
Administrar
Usuarios
Grupos
External Identities
Roles y administradores
Unidades administrativas
Asociados del administrador delegado
Aplicaciones empresariales
Dispositivos
Registros de aplicaciones
Gobierno de identidades
Proxy de aplicación
Atributos de seguridad personalizados (versión preliminar)
Licencias
https://go.microsoft.com/fwlink/?linkid=2132805
Todas las aplicaciones
Aplicaciones propias
Aplicaciones eliminadas
Empiece a escribir un nombre o id. de aplicación para filtrar los resu...
Agregar filtros

A partir del 30 de junio de 2020 ya no se agregarán nuevas características a la Biblioteca de autenticación de Azure Active Directory (ADAL) y Azure AD Graph. Continuaremos proporcionando soporte técnico y actualizaciones de seguridad, pero no se ofrecerán actualizaciones de características. Las aplicaciones deberán actualizarse a la Biblioteca de autenticación de Microsoft (MSAL) y Microsoft Graph. Más información

5 aplicaciones encontradas

Nombre para mostrar	Id. de aplicación (cliente)	Fecha de c...	Certificados y secretos
AP ApplicationReg	[redacted]	2/11/2021	✓ Current
AP ApplicationReg2	[redacted]	2/11/2021	✓ Current
OA Oauth	[redacted]	15/9/2022	✓ Current
OA OauthSE	[redacted]	20/9/2022	✓ Current
SA SAML-ASMS-QA	[redacted]	8/4/2022	-

3. The name field is filled in and the desired option is selected under (Supported account types), click**Register**.


Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
Inicio > | Registros de aplicaciones >

Registrar una aplicación

* Nombre

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

Nombre con el que identifica la aplicación

Tipos de cuenta compatibles

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

● Solo cuentas de este directorio organizativo (solo de Aranda Software Corp: inquilino único)

○ Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino)

○ Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino) y cuentas de Microsoft personales (como Skype o Xbox)

○ Solo cuentas personales de Microsoft

Ayudarme a elegir...

Al continuar, acepta las directivas de la plataforma Microsoft.

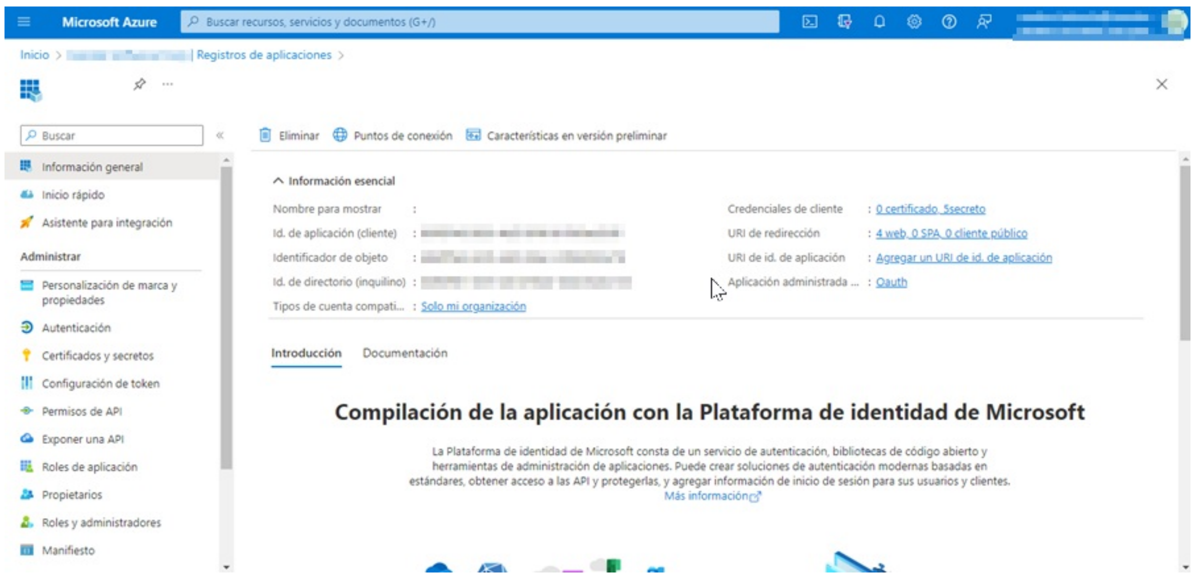
Registrar

4.When the application is registered, save the following data that is required for configuration in LDAP synchronization with Microsoft Entra ID.

- Directory ID (tenant) = URL

⚐ **Note:** The URL should be configured as follows: (https://login.microsoftonline.com/ + Tenant/Directory ID)

- Application ID (client) = Client id



Información esencial

Nombre para mostrar :
Id. de aplicación (cliente) : [redacted]
Identificador de objeto : [redacted]
Id. de directorio (inquilino) : [redacted]
Tipos de cuenta compati... : Solo mi organización
Credenciales de cliente : 0 certificado, 5secreto
URI de redirección : 4 web, 0 SPA, 0 cliente público
URI de id. de aplicación : Agregar un URI de id. de aplicación
Aplicación administrada ... : Oauth

Compilación de la aplicación con la Plataforma de identidad de Microsoft

La Plataforma de identidad de Microsoft consta de un servicio de autenticación, bibliotecas de código abierto y herramientas de administración de aplicaciones. Puede crear soluciones de autenticación modernas basadas en estándares, obtener acceso a las API y protegerlas, y agregar información de inicio de sesión para sus usuarios y clientes.

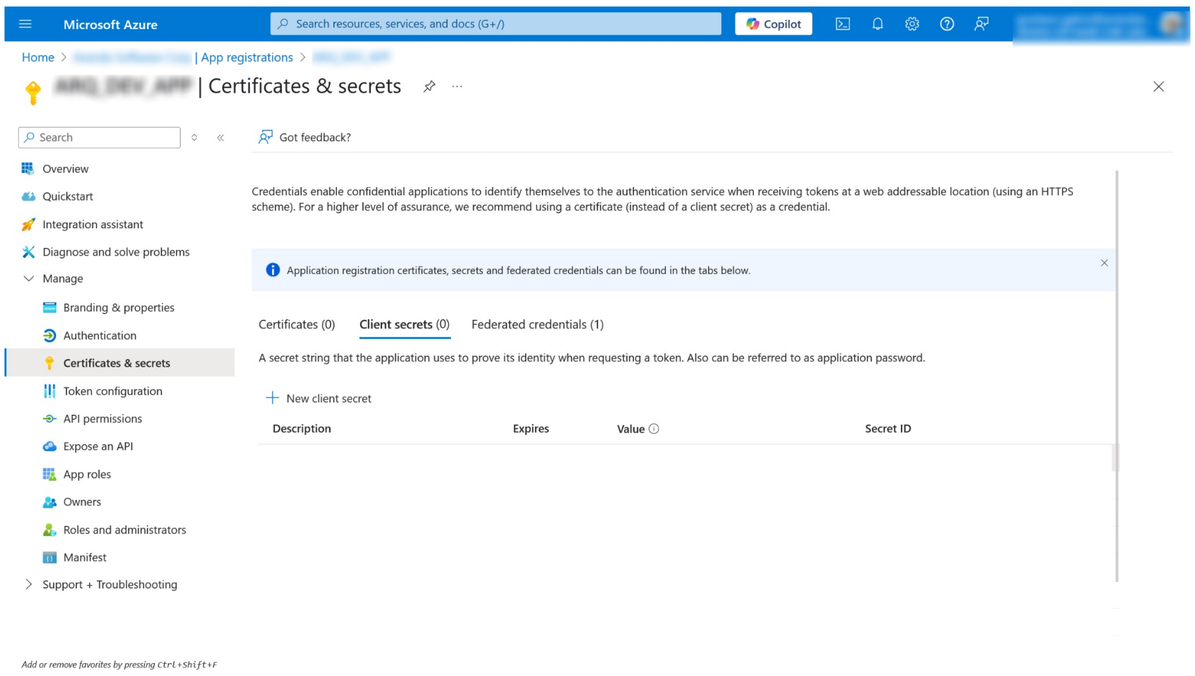
Configure Azure App

Once you have the app created and the data saved, you can configure the app as follows:

Creation of the Secret

1. To create the secret, log in to the Azure portal > Microsoft> Menu Enter ID > Application Registrations > select the created application from the available list.

2. In the **Administer** Select the option **Certificates and secrets** > and in the information view, click the **New client secret**.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

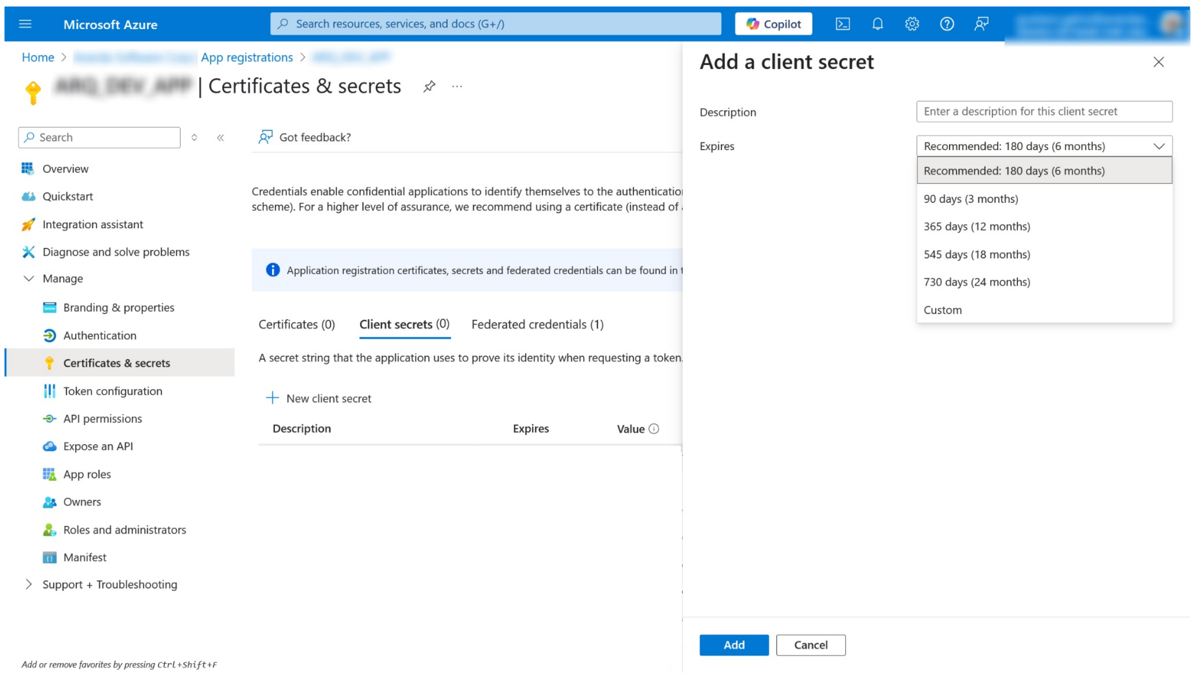
Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Add or remove favorites by pressing Ctrl+Shift+F

3. In the window **Add a client secret** fill in the field **Description**, define the duration of the secret in the field **Expires** and click the **Add**.

> ⚐ **Note:** It is recommended not to forget the configured duration time. In case of expiration, if it is not updated, authentication will fail



Credentials enable confidential applications to identify themselves to the authenticatio scheme). For a higher level of assurance, we recommend using a certificate (instead of a

Application registration certificates, secrets and federated credentials can be found in t

A secret string that the application uses to prove its identity when requesting a token.

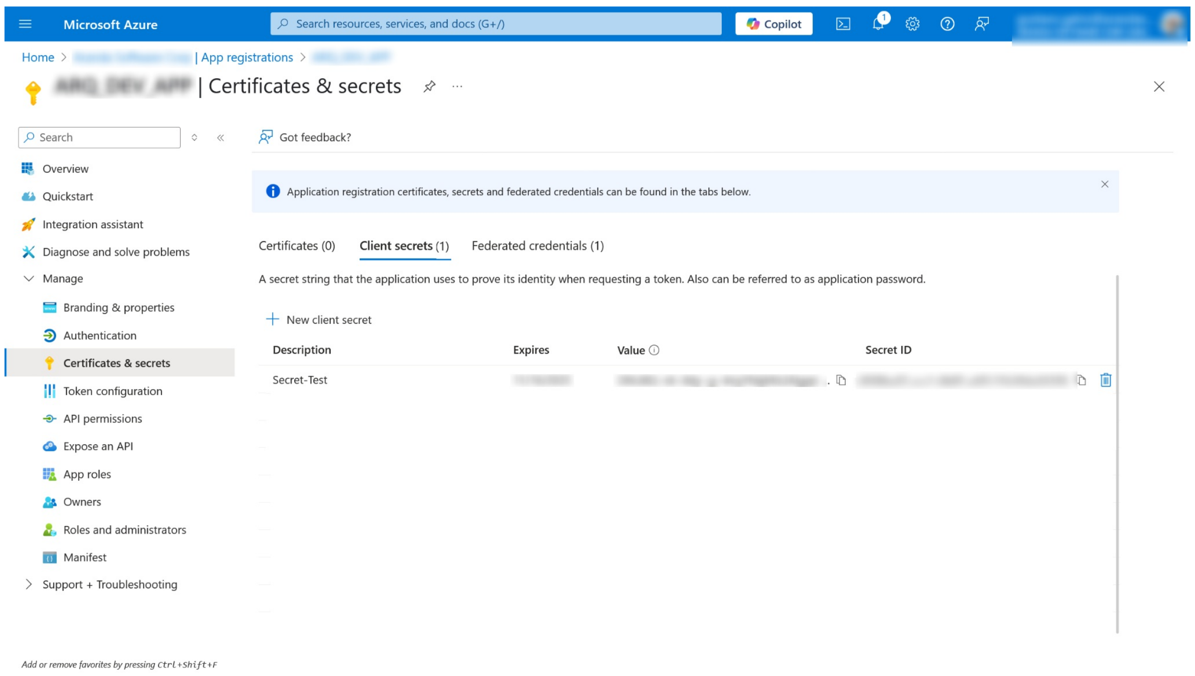
Description: Enter a description for this client secret

Expires: Recommended: 180 days (6 months)

- Recommended: 180 days (6 months)
- 90 days (3 months)
- 365 days (12 months)
- 545 days (18 months)
- 730 days (24 months)
- Custom

4. The value of secrecy is only visible when it is created; should be saved for later use or referenced during configurations required on Aranda products.

- Secret Customer Value = Secret Client.



Application registration certificates, secrets and federated credentials can be found in the tabs below.

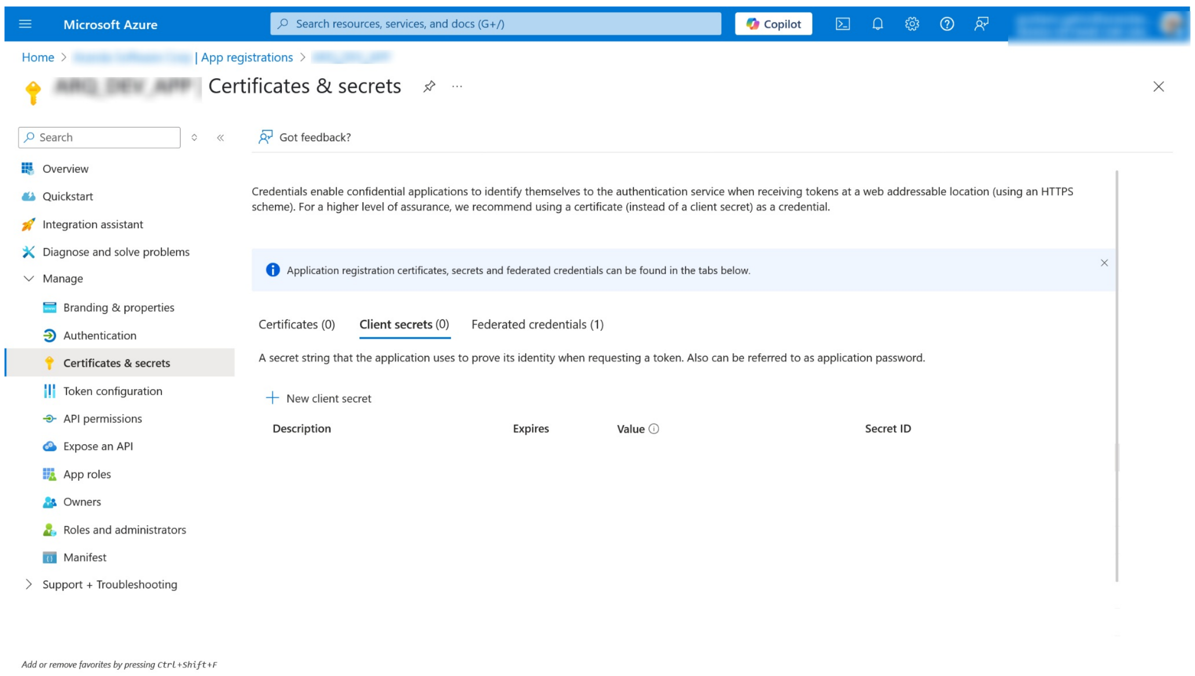
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Secret-Test	[redacted]	[redacted]	[redacted]

Configure API permissions

1. To configure API permissions, enter the Azure portal > Microsoft'> Menu Enter ID > Application Registrations > select the created application from the available list.

2. In the **Administer** from the main menu, select the **API permissions** > and in the information view, in the Configured Permissions section, click **Add a Permission**.



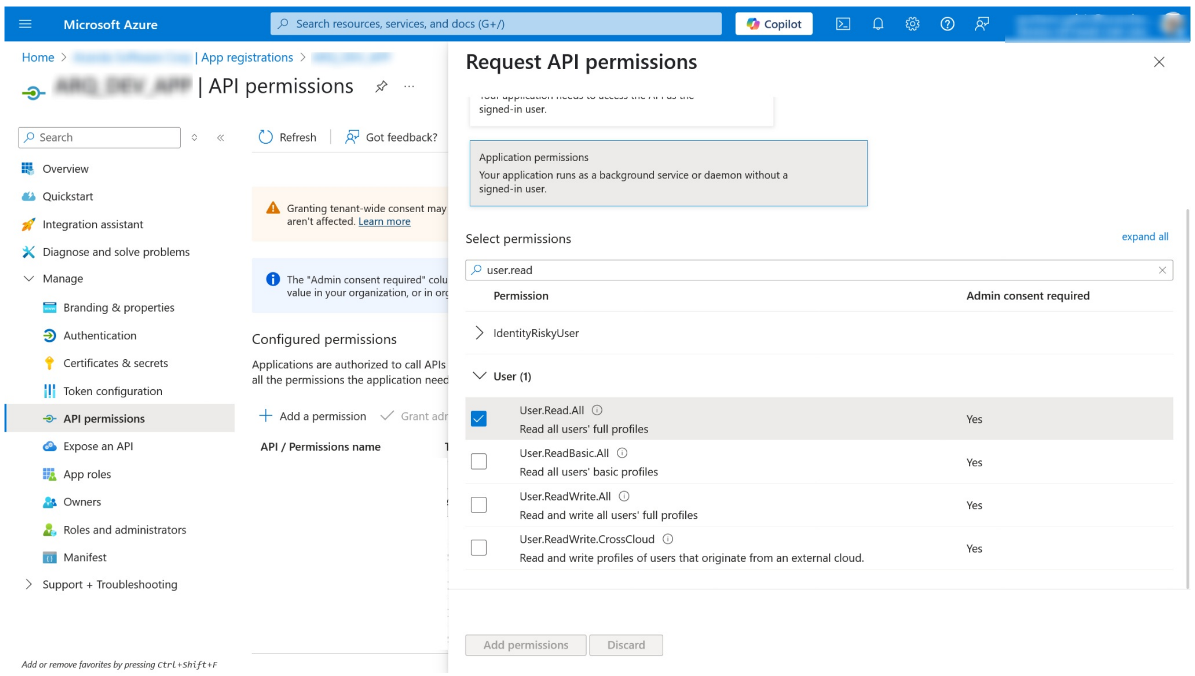
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

3. In the window **Request API permissions**, select the **Microsoft Graph** > and then **Application Permissions**, enable permissions according to your requirements: **User.Read.All** (Allows you to read information from all users in the directory) and **Group.Read.All** (Allows you to read information from all groups in the directory.) Finally click **Add permission**.

> ⚐ **Note:** Your organization may require the administrator to approve these permissions before they are enabled.



Granting tenant-wide consent may aren't affected. Learn more

The "Admin consent required" colu value in your organization, or in org

Configured permissions

Applications are authorized to call APIs all the permissions the application need

Request API permissions

signed-in user.

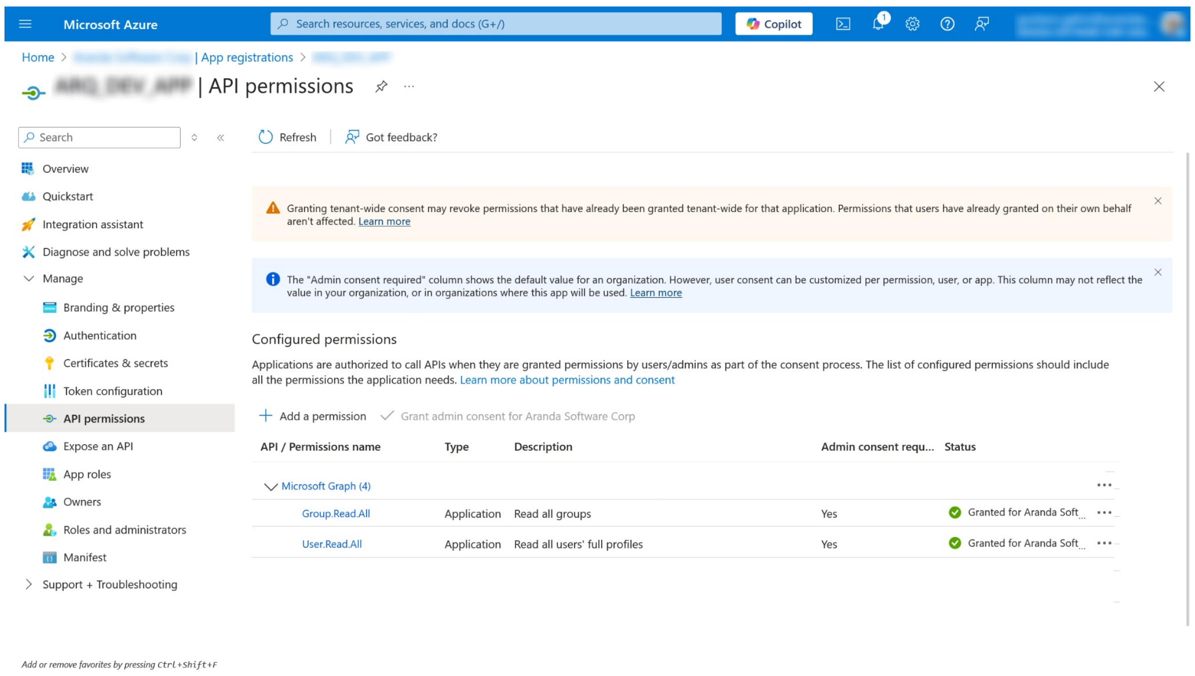
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions — expand all

user.read

	Permission	Admin consent required
	IdentityRiskyUser	
	User (1)	
☑	User.Read.All Read all users' full profiles	Yes
☐	User.ReadBasic.All Read all users' basic profiles	Yes
☐	User.ReadWrite.All Read and write all users' full profiles	Yes
☐	User.ReadWrite.CrossCloud Read and write profiles of users that originate from an external cloud.	Yes

Once this process is done, and permissions are enabled, you can finish syncing with Azure AD:



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > [redacted] | App registrations > [redacted]
[redacted] | API permissions
Search
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Add or remove favorites by pressing Ctrl+Shift+F
Refresh
Got feedback?
Add a permission
Grant admin consent for Aranda Software Corp

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. Learn more

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

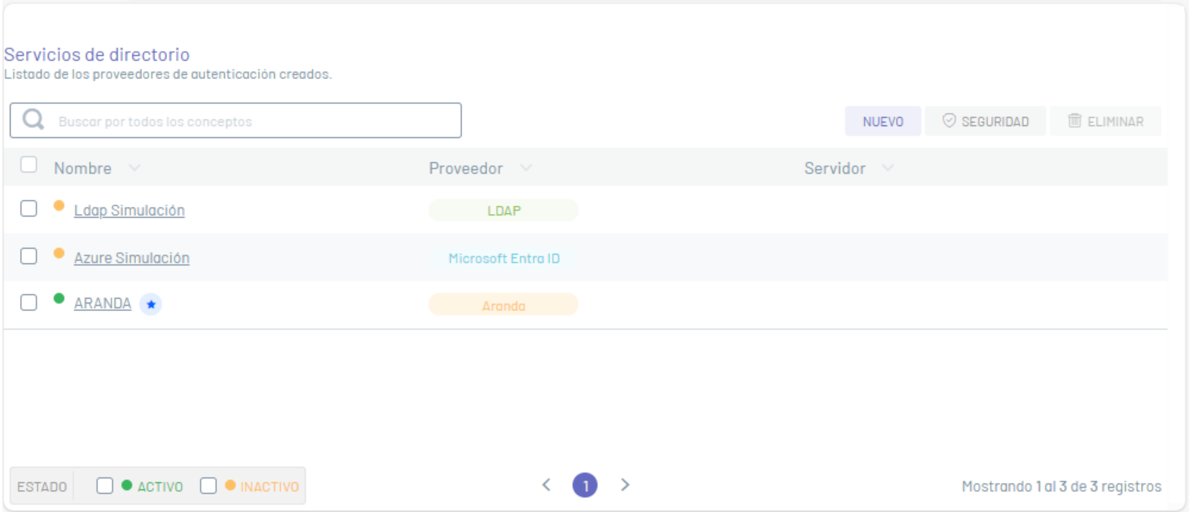
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Aranda Soft...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Aranda Soft...

Directory Management

Management of directory services

View Directory Service

1. In the Directory Service information view, you can view the list of authentication providers, grouped by data such as:



Servicios de directorio
Listado de los proveedores de autenticación creados.

Buscar por todos los conceptos
NUEVO
SEGURIDAD
ELIMINAR

Nombre	Proveedor	Servidor
● Ldap Simulación	LDAP	
● Azure Simulación	Microsoft Entra ID	
● ARANDA ★	Aranda	

ESTADO □ ● ACTIVO □ ● INACTIVO
1

Mostrando 1 al 3 de 3 registros

Field	Field Type	Description
Name	Text	The name by which the directory service is identified.
Supplier	Text	Type of directory service.
Server	Text	Name and/or IP where the domain is located.

⚐ **Note:** The Column **Supplier** indicates the type of directory service provider; which can be**Aranda**, **LDAP** and **Microsoft Enter ID**

⚐ **Note:** Through the in-house vendor type options[Aranda](), you can configure the name, password policies, and more for this type of provider.

2. In the directory services information view, you will have information management and organization actions enabled.[Information View in Commons Environment]()

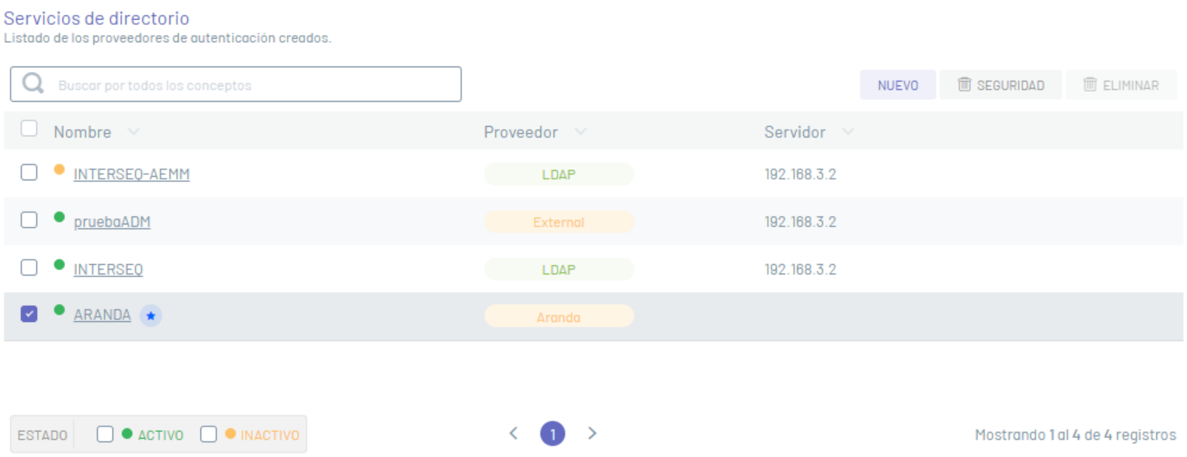
 Related Links:

- [Create Directory Service]()
- [Edit Directory Service]()
- [Delete Directory Service]()

Aranda type supplier

The type supplier **Aranda** is the default provider of the system, the settings that are configured for this provider affect users who are of this type of provider.

1. To configure provider options, in the directory services information view, select the type provider record**Aranda** .



Servicios de directorio
Listado de los proveedores de autenticación creados.

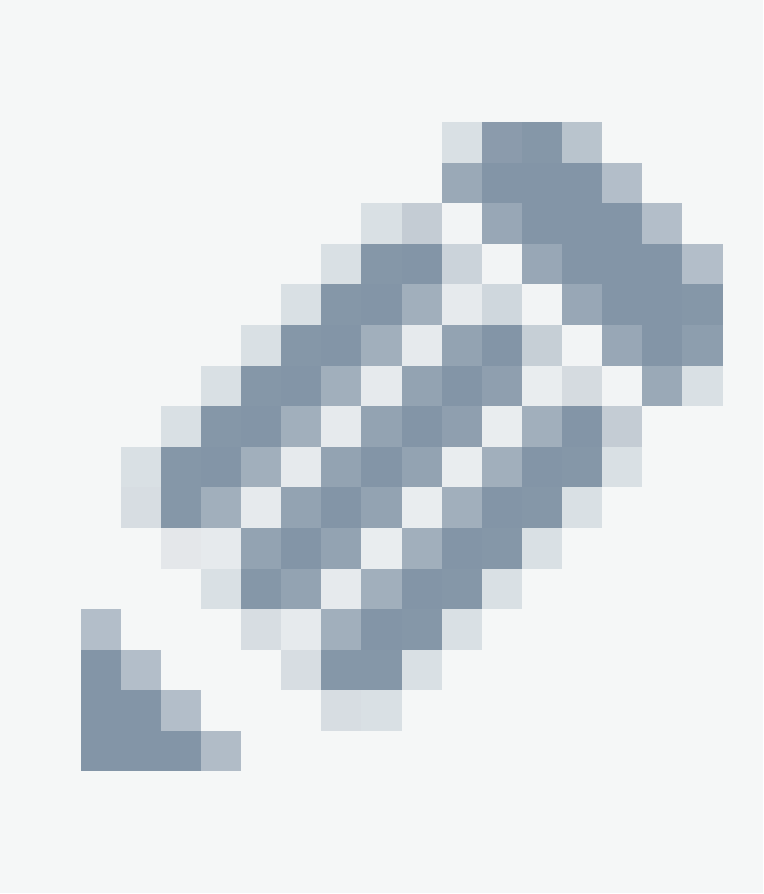
Buscar por todos los conceptos
NUEVO
SEGURIDAD
ELIMINAR

Nombre	Proveedor	Servidor
□ ● INTERSEQ-AEMM	LDAP	192.168.3.2
□ ● pruebaADM	External	192.168.3.2
□ ● INTERSEQ	LDAP	192.168.3.2
☑ ● ARANDA ★	Aranda	

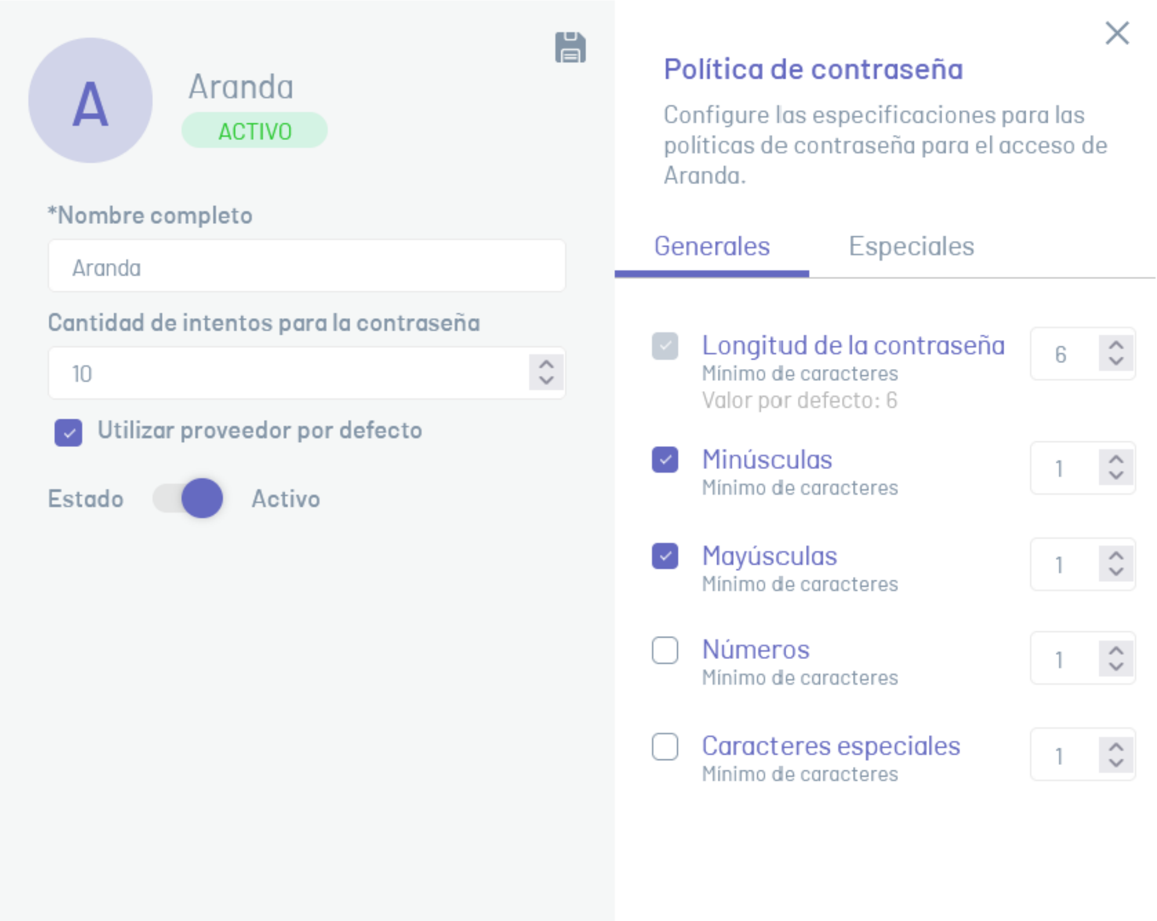
ESTADO □ ● ACTIVO □ ● INACTIVO
1

Mostrando 1 al 4 de 4 registros

2. In the Aranda Provider Detail view, click the **Edit**



to modify the required information according to the business rules or needs of the client, enabling the controls in each type of policy and setting the values for each option.



A

Aranda

ACTIVO

*Nombre completo

Aranda

Cantidad de intentos para la contraseña

10

☑ Utilizar proveedor por defecto

Estado ● Activo

Política de contraseña

Configure las especificaciones para las politicas de contraseña para el acceso de Aranda.

☑ Longitud de la contraseña
Mínimo de caracteres
Valor por defecto: 6
6

☑ Minúsculas
Mínimo de caracteres
1

☑ Mayúsculas
Mínimo de caracteres
1

☐ Números
Mínimo de caracteres
1

☐ Caracteres especiales
Mínimo de caracteres
1

3. A continuación se presentan las opciones disponibles en el proveedor tipo Aranda:

Field	Field Type	Description
Name Change	Text	Allows you to change the name to a custom one.
Number of attempts	Text	In this option you can configure the maximum number of attempts to enter the password, before blocking the user.
Use Default Provider	Selector	If selected, it will be the user’s initial choice at the time of authenticating to the Login.
Password Policies	Multiple	You will be able to configure the specifications for the Password Policies

⚐ Note:

- If you change the name of the type provider Aranda, make sure the name is the same on all the products you have installed (ADM, AFLS, ASMS, etc.), to ensure that the integrations work correctly.
- Example: If you have ASMS and ADM installed, and you need to change the name of the type provider Aranda to *internal*, validate that the name is equal to *internal*.

Configure Password Policies

3. On the General In the Password Policies section, you can modify the number of characters in parameters such as password length, lowercase, uppercase, numbers, and special characters.

4. On the Special In the Password Policies section, you can configure the password's special allowed and disallowed characters.

⚐ Note: The password field defined during the configuration process of Aranda Users, must comply with all [Password requirements]

5. Click Save

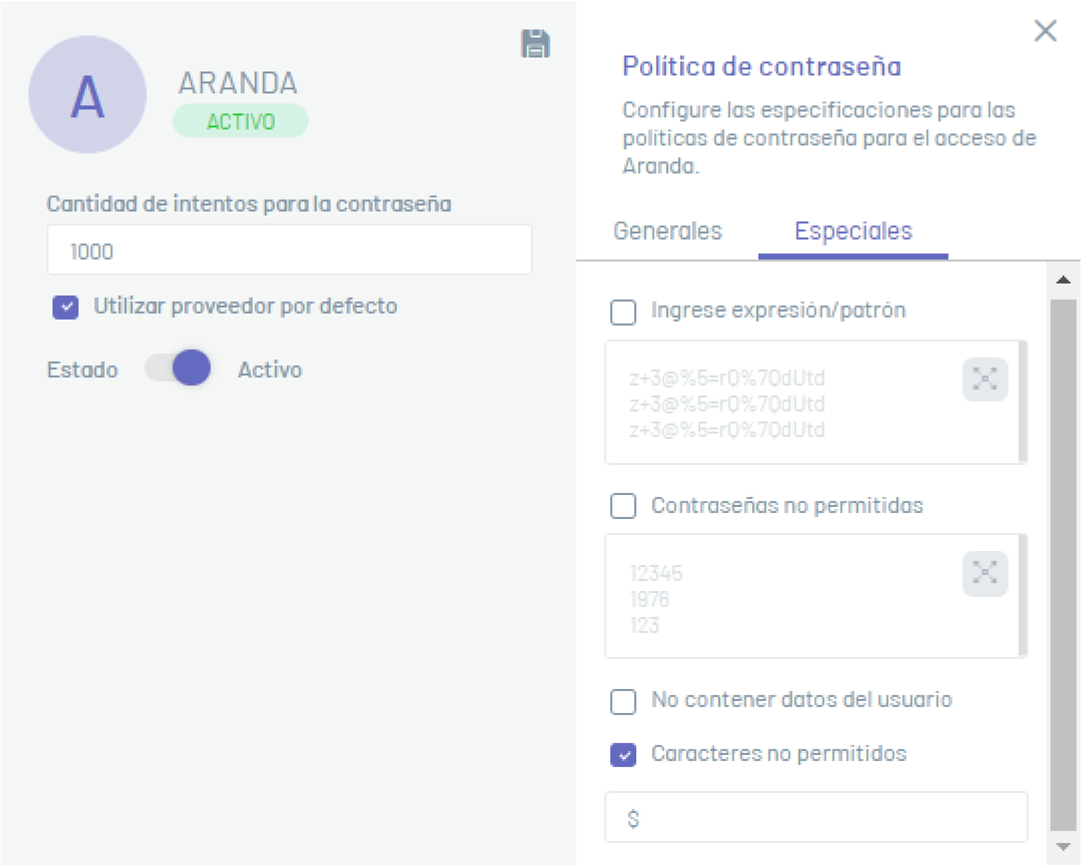
💾

to store the new specifications of special and/or general password policies.

⚐ Note:

- Password policies apply only to users created in the local directory (Aranda).
- When you modify password policies, they will be enforced for the creation of new users or when changing the password of existing users in the local directory.

Password Policies



A ARANDA ACTIVO

Cantidad de intentos para la contraseña
1000

☑ Utilizar proveedor por defecto

Estado ● Activo

Politica de contraseña ✕

Configure las especificaciones para las politicas de contraseña para el acceso de Aranda.

Generales | Especiales

□ Ingrese expresión/patrón

z+3@%5=r0%70dUtd
z+3@%5=r0%70dUtd
z+3@%5=r0%70dUtd

□ Contraseñas no permitidas

12345
1976
123

□ No contener datos del usuario

☑ Caracteres no permitidos

$

General Policies

These types of policies are mandatory and users must comply with them in order to create their password.

Field	Field Type	Description
Password length	Numerical	The password must be the length set by the administrator.
B	Numerical	Requires that the password be one or more lowercase characters.
B	Numerical	Requires that the password be one or more uppercase characters.
Numbers	Numerical	Requires the password to have one or more numeric characters.
Special characters	Numerical	Requires the password to have one or more special characters.

Políticas Especiales

Estas políticas son restrictivas; si la contraseña del usuario coincide con una de las políticas especiales **NO** se podrá usar esa contraseña

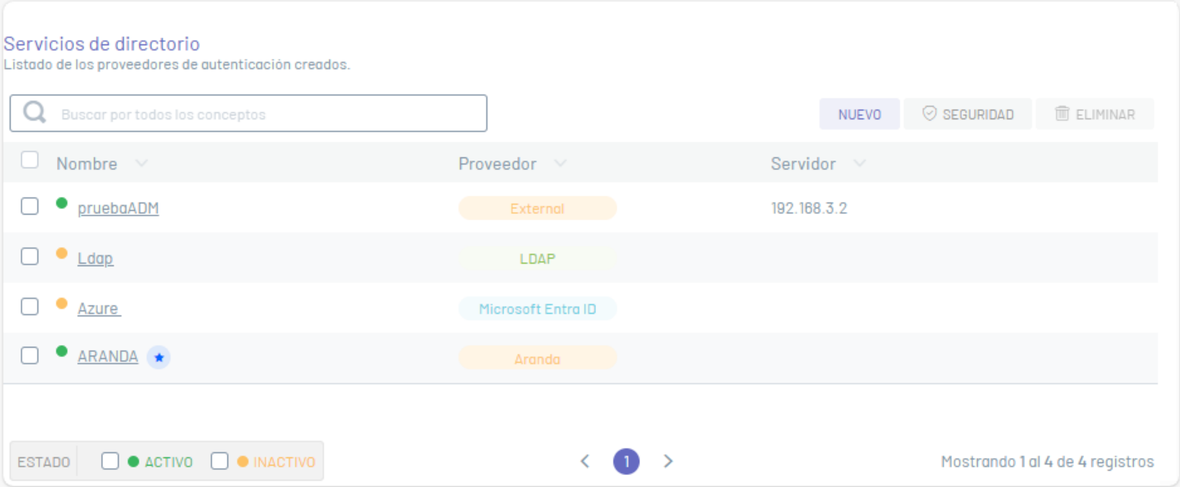
Field	Field Type	Description
Expression/Pattern	Text	It allows you to determine regular expressions to avoid the use of patterns in passwords; To define multiple expressions, they must be separated by a line break
Password Not Allowed	Text	List of passwords that cannot be used. To set multiple disallowed passwords, they must be separated with a line break.
Password with user data	Selector	It does not allow the username to be used within the password.
Passwords with disallowed characters	Text	The use of the indicated characters is not permitted. To define multiple characters, type one followed by the other without spaces. Example: *#%* It will not allow the use of any of the #, or % in the password

Related Links:

- Management of Directory Service

Create Directory Services

1. In the directory server information view, select the **New**.



Servicios de directorio

Listado de los proveedores de autenticación creados.

Buscar por todos los conceptos
NUEVO
SEGURIDAD
ELIMINAR

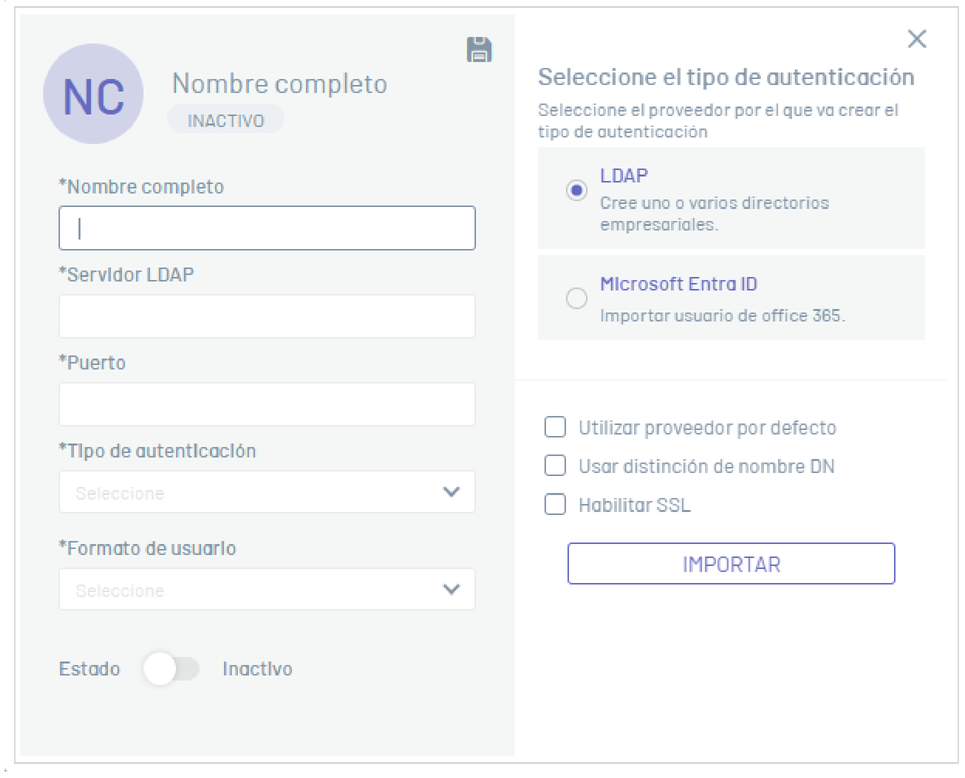
	Nombre	Proveedor	Servidor
□	● pruebaADM	External	192.168.3.2
□	● Ldap	LDAP	
□	● Azure	Microsoft Entra ID	
□	● ARANDA ★	Aranda	

ESTADO □ ● ACTIVO □ ● INACTIVO
1
Mostrando 1 al 4 de 4 registros

Basic Facts

2. In the window that is enabled you will be able to fill in the basic information required to establish the connection with your directory server such as name, server, port, authentication type, providers, among others.

Each of the directory services fields must take into account the Specifications for Common Fields



*Nombre completo

*Servidor LDAP

*Puerto

*Tipo de autenticación: Seleccione

*Formato de usuario: Seleccione

Estado: Inactivo

Seleccione el tipo de autenticación

Seleccione el proveedor por el que va crear el tipo de autenticación

● LDAP
Cree uno o varios directorios empresariales.

○ Microsoft Entra ID
Importar usuario de office 365.

□ Utilizar proveedor por defecto

□ Usar distinción de nombre DN

□ Habilitar SSL

Authentication Type

4. In the **Authentication Type**, you can set the type of provider for authentication:

- LDAP: It is a standard application protocol for queries, which can store, manage, protect and authenticate user information.
- Microsoft EntraID: Microsoft's cloud-based identity management service, from which Office 365 users can be imported

LDAP Provider

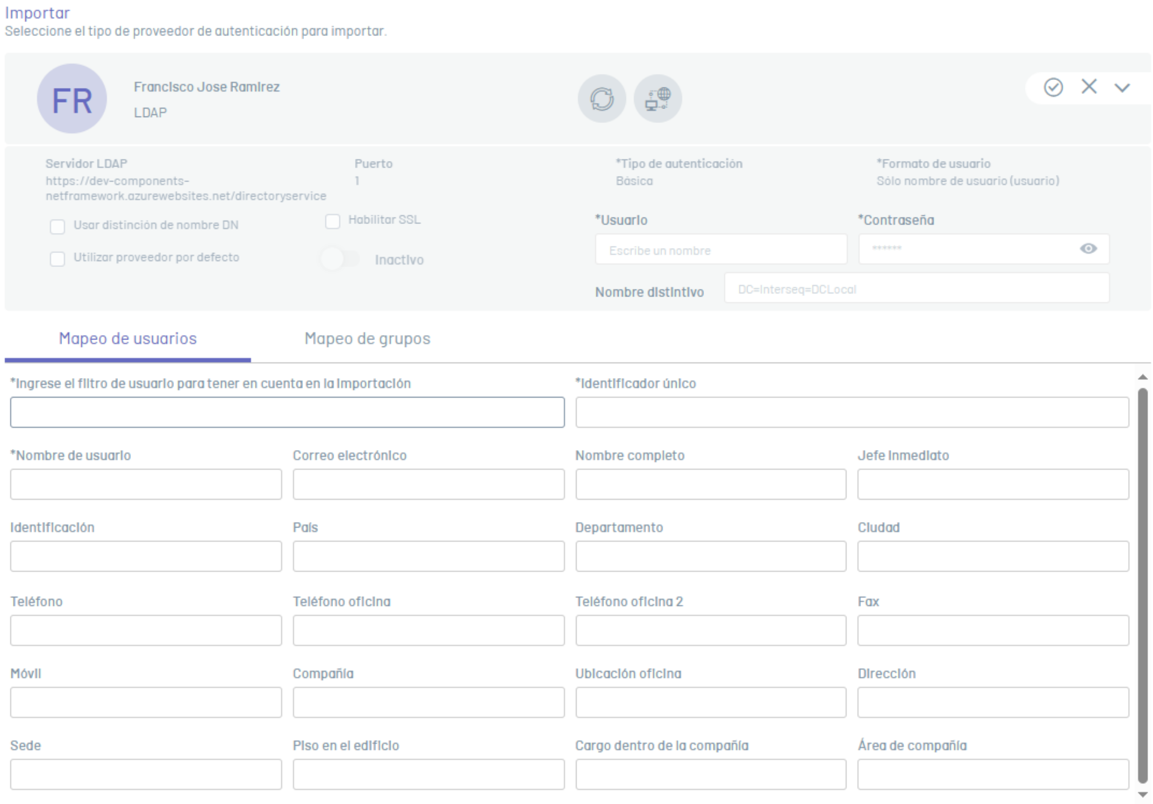
5. In the Vendor Detail view, click the **IMPORT**; window is enabled **Import** where you will be able to enter the necessary data for synchronization. In the LDAP Business Directory Basic Information, enter the username and password data.

> ⚐ Note:

- For active directories configured with OpenLDAP, fill in the Distinguished Name field.
- Check out some filters example for LDAP

In the Mappings tabs, you can specify the corresponding naming attributes for each field, and filters must comply with LDAP syntax to synchronize the information.

On the **User Mapping** the mandatory fields to be registered are: User filter to take into account in the import, unique identifier and username.



Importar
Seleccione el tipo de proveedor de autenticación para importar.

FR Francisco Jose Ramirez
LDAP

Servidor LDAP
https://dev-components-netframework.azurewebsites.net/directoryservice

Puerto
1

*Tipo de autenticación
Básica

*Formato de usuario
Sólo nombre de usuario (usuario)

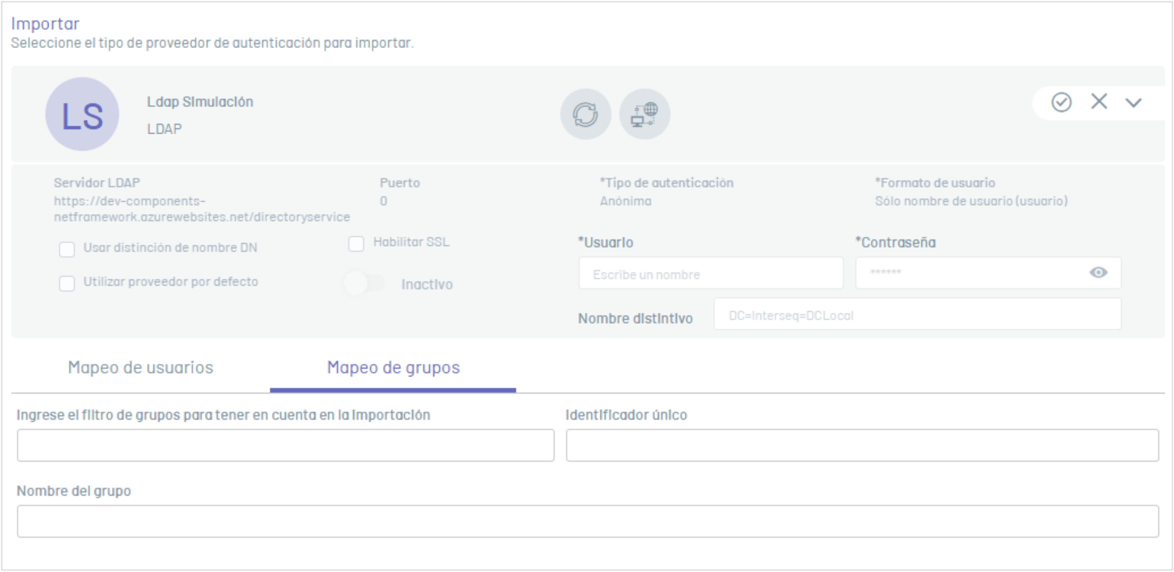
□ Usar distinción de nombre DN
□ Habilitar SSL
□ Utilizar proveedor por defecto
Inactivo

*Usuario: Escribe un nombre
*Contraseña: ******
Nombre distintivo: DC=Interseq=DCLocal

Mapeo de usuarios | Mapeo de grupos

*Ingrese el filtro de usuario para tener en cuenta en la importación
*Identificador único
*Nombre de usuario
Correo electrónico
Nombre completo
Jefe inmediato
Identificación
País
Departamento
Ciudad
Teléfono
Teléfono oficina
Teléfono oficina 2
Fax
Móvil
Compañía
Ubicación oficina
Dirección
Sede
Piso en el edificio
Cargo dentro de la compañía
Área de compañía

On the **Group Mapping** (user groups) if you enter any value in the field "Enter the group filter to take into account in the import", the fields "Unique identifier" and "group name" become mandatory.



Importar
Seleccione el tipo de proveedor de autenticación para importar.

LS Ldap Simulación
LDAP

Servidor LDAP
https://dev-components-netframework.azurewebsites.net/directoryservice

Puerto
0

*Tipo de autenticación
Anónima

*Formato de usuario
Sólo nombre de usuario (usuario)

□ Usar distinción de nombre DN
□ Habilitar SSL
□ Utilizar proveedor por defecto
Inactivo

*Usuario: Escribe un nombre
*Contraseña: ******
Nombre distintivo: DC=Interseq=DCLocal

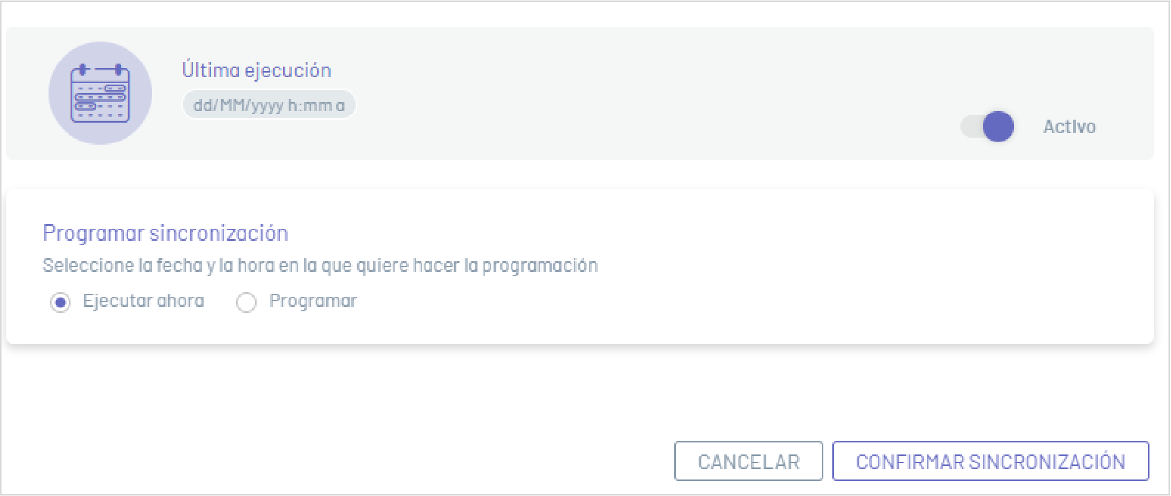
Mapeo de usuarios | Mapeo de grupos

Ingrese el filtro de grupos para tener en cuenta en la importación
Identificador único
Nombre del grupo

6. When registering the fields, click on the **Test Connection**

. If the connection was successful, you will be able to view the message: **The information is complete, you can now finish the import** and the continuation of the process is authorized.
7. When you finish recording the information, click the **Synchronize**

and in the window that is enabled, activate synchronization.



Última ejecución

dd/MM/yyyy h:mm a

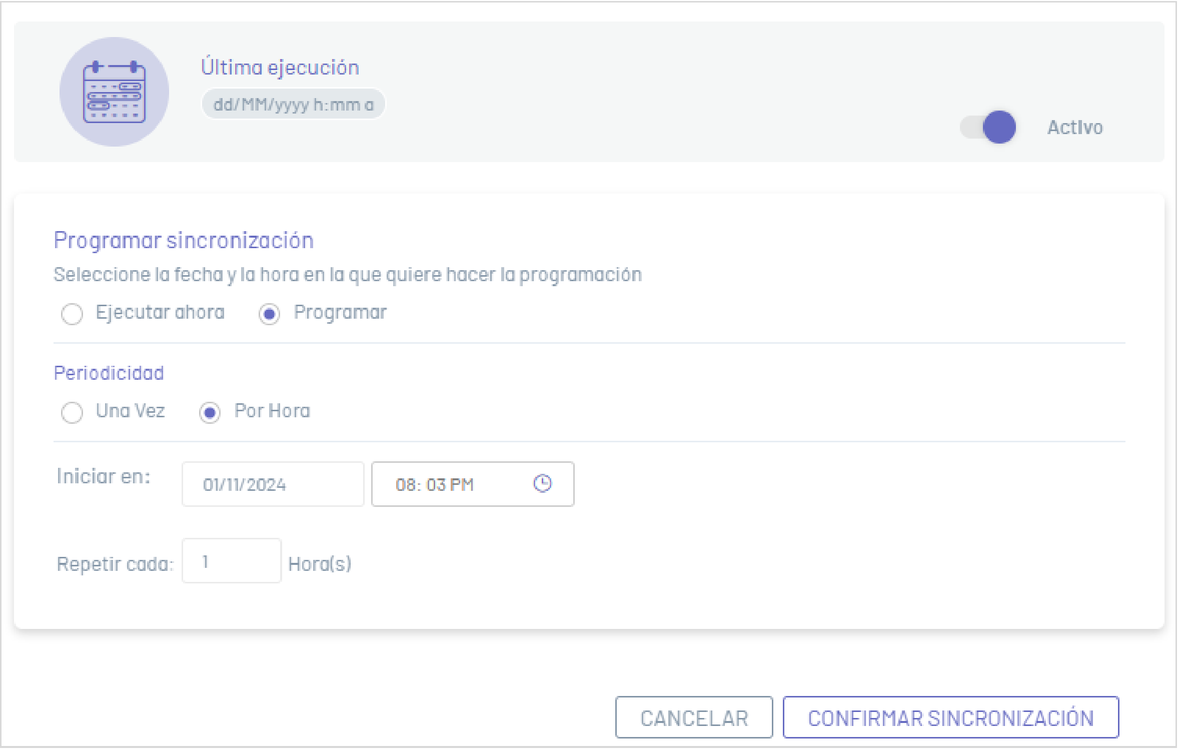
Activo

Programar sincronización

Seleccione la fecha y la hora en la que quiere hacer la programación

● Ejecutar ahora ○ Programar

8. Synchronization can be manual (immediately) or it can be automatically scheduled once or every few hours to update new users. After selecting the sync type and performing the settings, click the CONFIRM SYNCHRONIZATION.



Última ejecución

dd/MM/yyyy h:mm a

Activo

Programar sincronización

Seleccione la fecha y la hora en la que quiere hacer la programación

○ Ejecutar ahora ● Programar

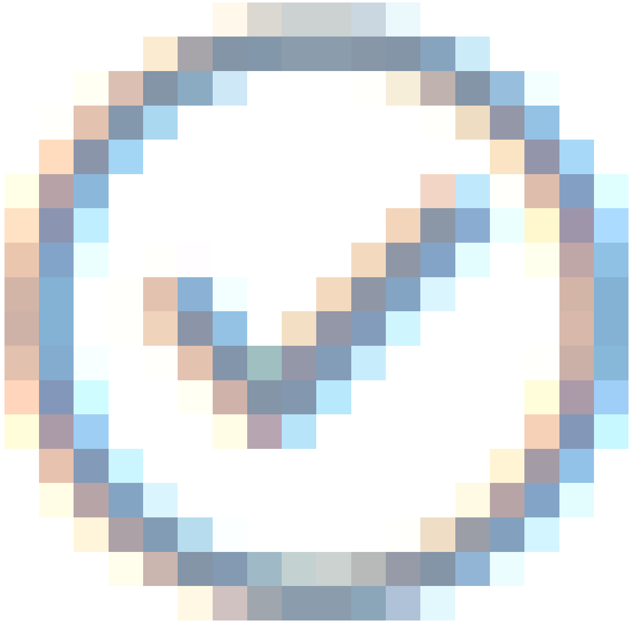
Periodicidad

○ Una Vez ● Por Hora

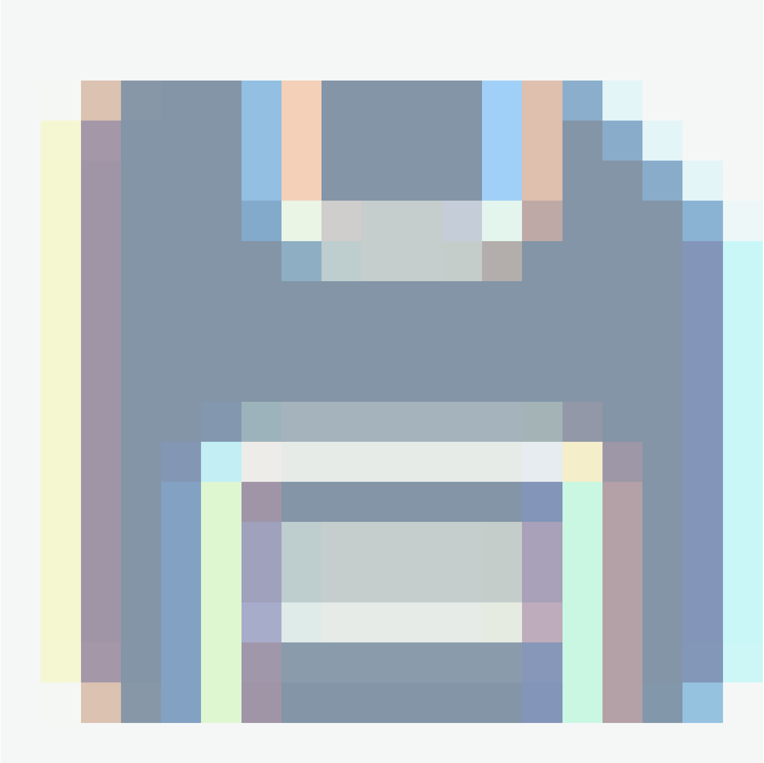
Iniciar en: 01/11/2024 08: 03 PM

Repetir cada: 1 Hora(s)

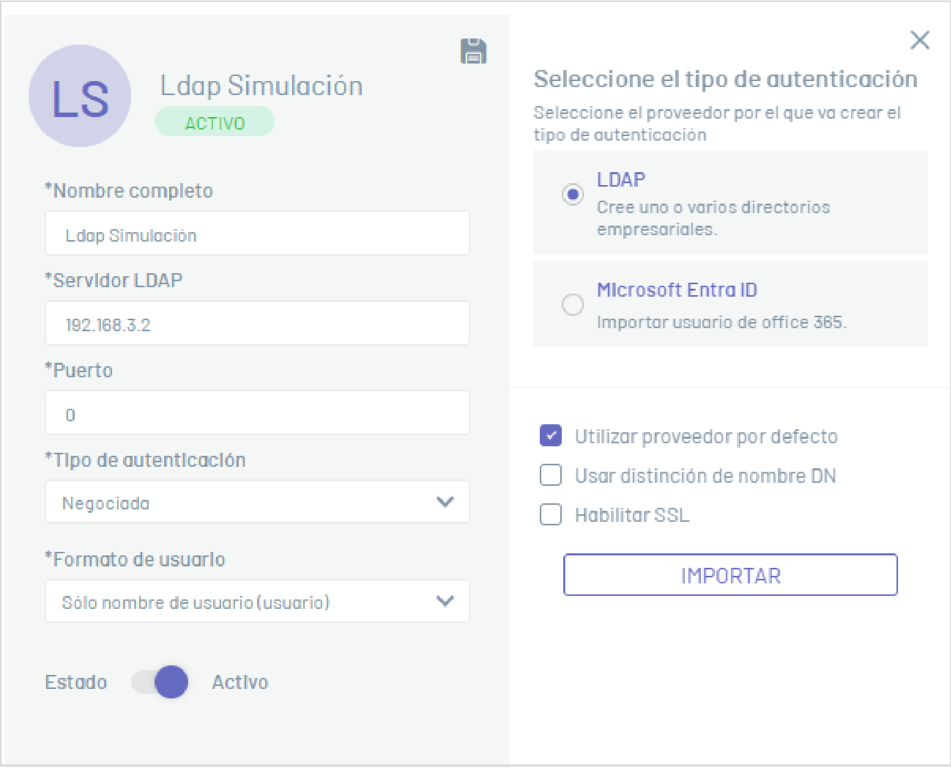
9. When you finish configuring the LDAP directory, in the Import window, click the confirmation button



and in the LDAP Basic Configuration window, click Save



.



LS Ldap Simulación
ACTIVO

*Nombre completo
Ldap Simulación

*Servidor LDAP
192.168.3.2

*Puerto
0

*Tipo de autenticación
Negociada

*Formato de usuario
Sólo nombre de usuario (usuario)

Estado Activo

Seleccione el tipo de autenticación

Seleccione el proveedor por el que va crear el tipo de autenticación

● LDAP
Cree uno o varios directorios empresariales.

○ Microsoft Entra ID
Importar usuario de office 365.

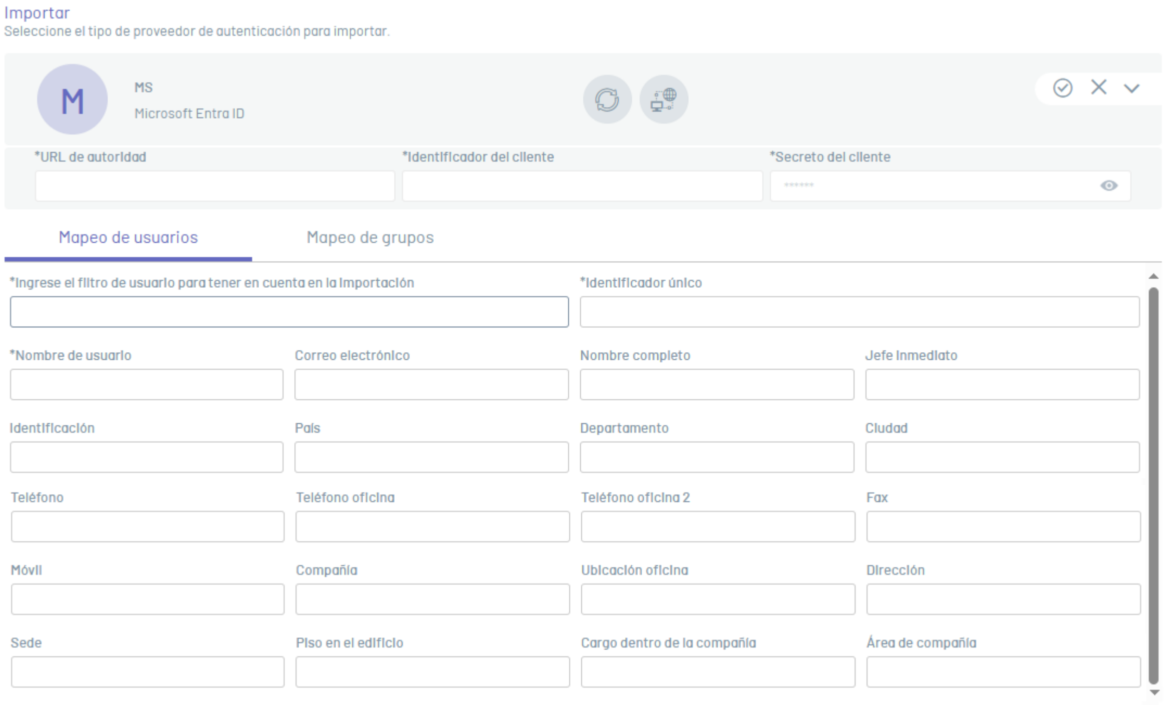
☑ Utilizar proveedor por defecto
☐ Usar distinción de nombre DN
☐ Habilitar SSL

10. Once the synchronization is complete, the administrator will be able to assign the respective roles to the synchronized users.

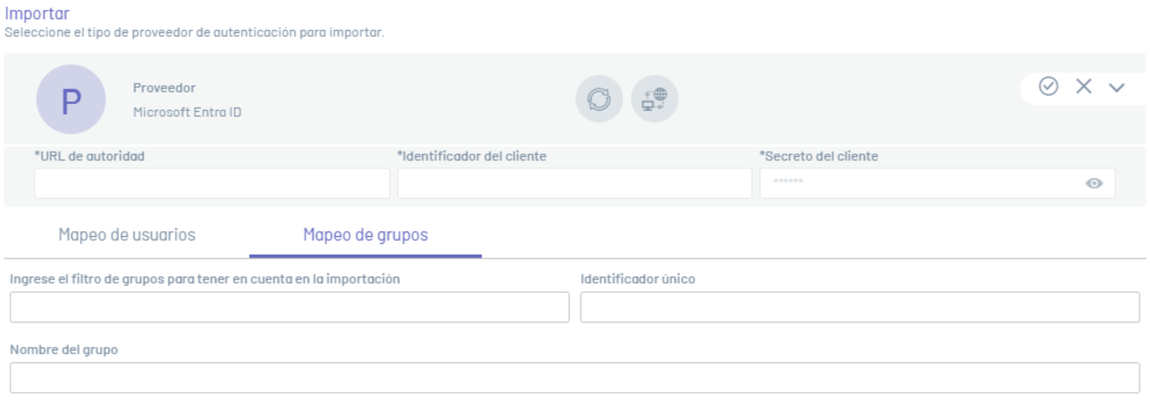
Microsoft EntraID Provider

1. In the provider detail view, enter the full name of the directory you want to sync and click the**IMPORT**; window is enabled **Import** where you will be able to enter the necessary data for synchronization. In the basic directory information, enter the authority URL, client ID, and client secret supplied by Microsoft EntraID.

On the **User Mapping** the mandatory fields to be registered are:User filter for import, unique identifier and Username.


Importar
Seleccione el tipo de proveedor de autenticación para importar.

On the **Group Mapping** (user groups) if you enter any value in the field "Enter the group filter to take into account in the import", the fields "Unique identifier" and "group name" become mandatory.


Importar
Seleccione el tipo de proveedor de autenticación para importar.

For information about user filters and attributes for field mapping, you can consult Microsoft's documentation at the following links: User and group filter
User fields
Group Fields

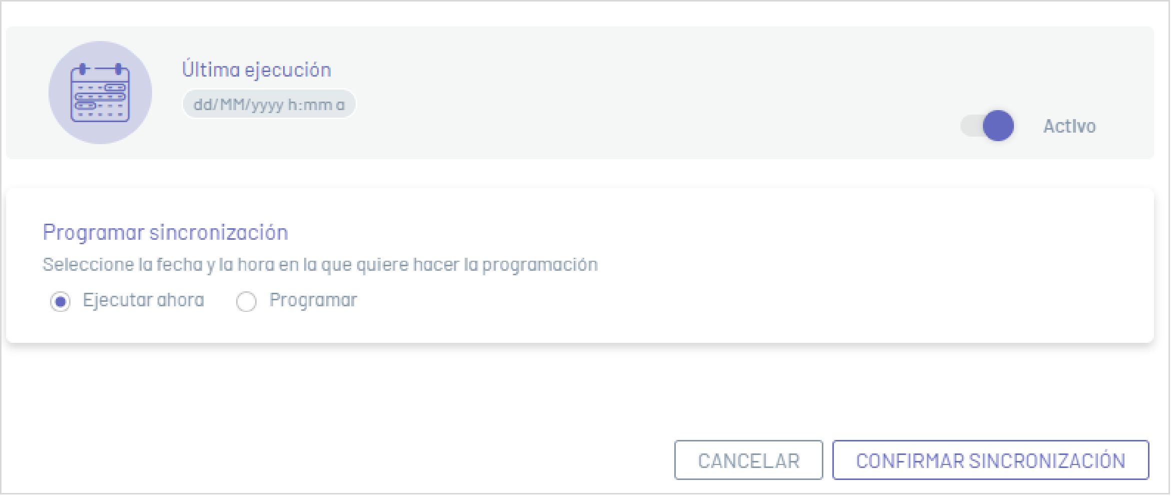
⚐ Note:

- Check out some filters and Field Mapping Microsoft EntraID example
- Learn how to create your app Microsoft Enter ID

6. When registering the fields, click on the **Test Connection**

. If the connection was successful, you will be able to view the message: The information is complete, you can now finish the import and the continuation of the process is authorized. 7. When you finish recording the information, click the Synchronize

and in the window that is enabled, activate synchronization.



Última ejecución

dd/MM/yyyy h:mm a

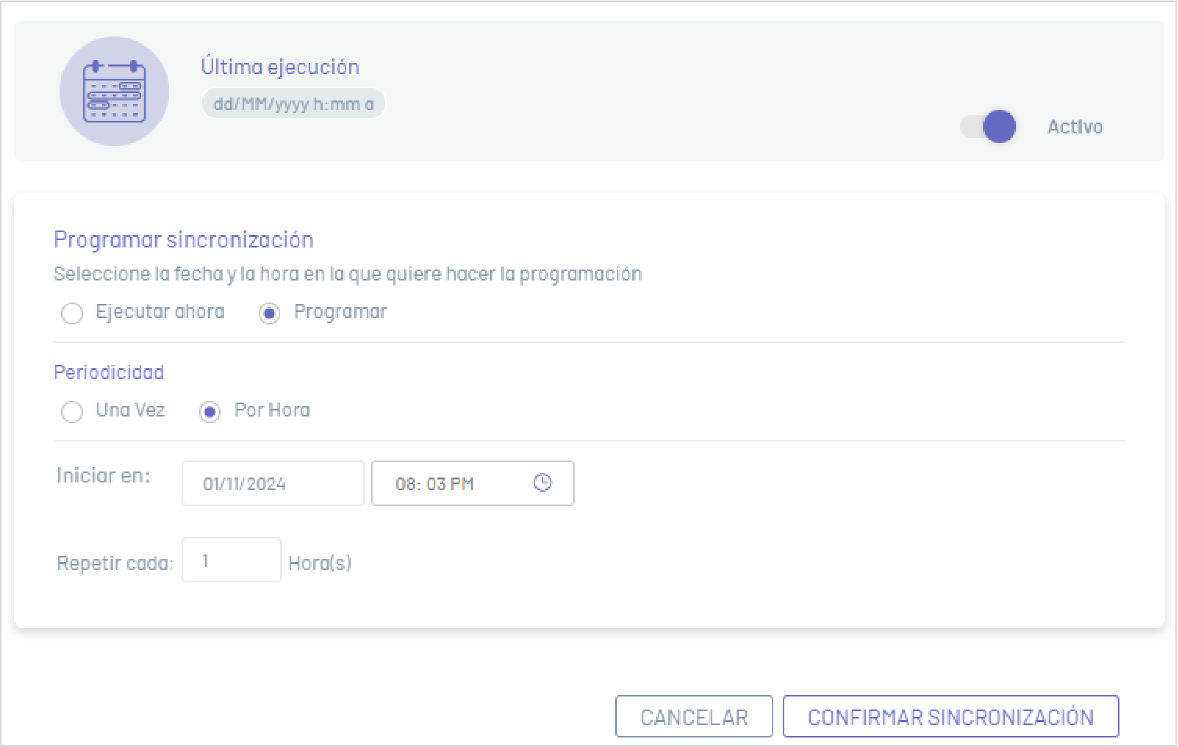
Activo

Programar sincronización

Seleccione la fecha y la hora en la que quiere hacer la programación

● Ejecutar ahora ○ Programar

8. Synchronization can be manual (immediately) or can be scheduled automatically once or every few hours. After selecting the sync type and performing the settings, click the CO-SIGN SYNCHRONIZATION.



Última ejecución

dd/MM/yyyy h:mm a

Activo

Programar sincronización

Seleccione la fecha y la hora en la que quiere hacer la programación

○ Ejecutar ahora ● Programar

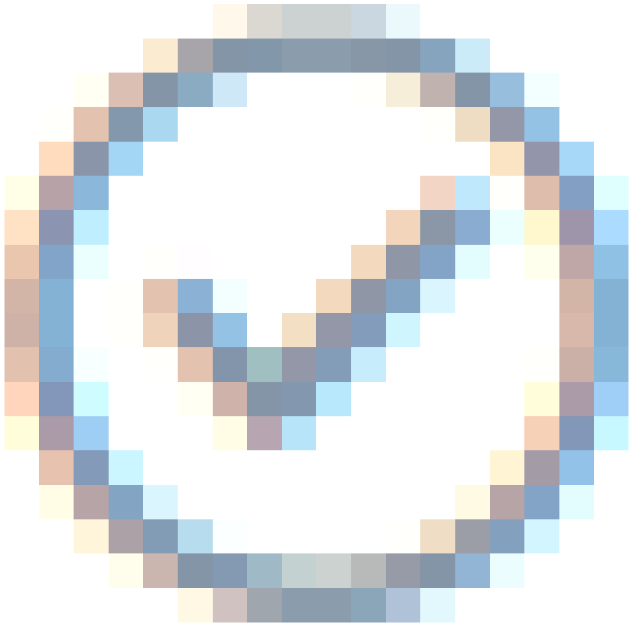
Periodicidad

○ Una Vez ● Por Hora

Iniciar en: 01/11/2024 08: 03 PM

Repetir cada: 1 Hora(s)

9. When you finish configuring the Microsofrt Enter ID directory in the Import window, click the confirmation button



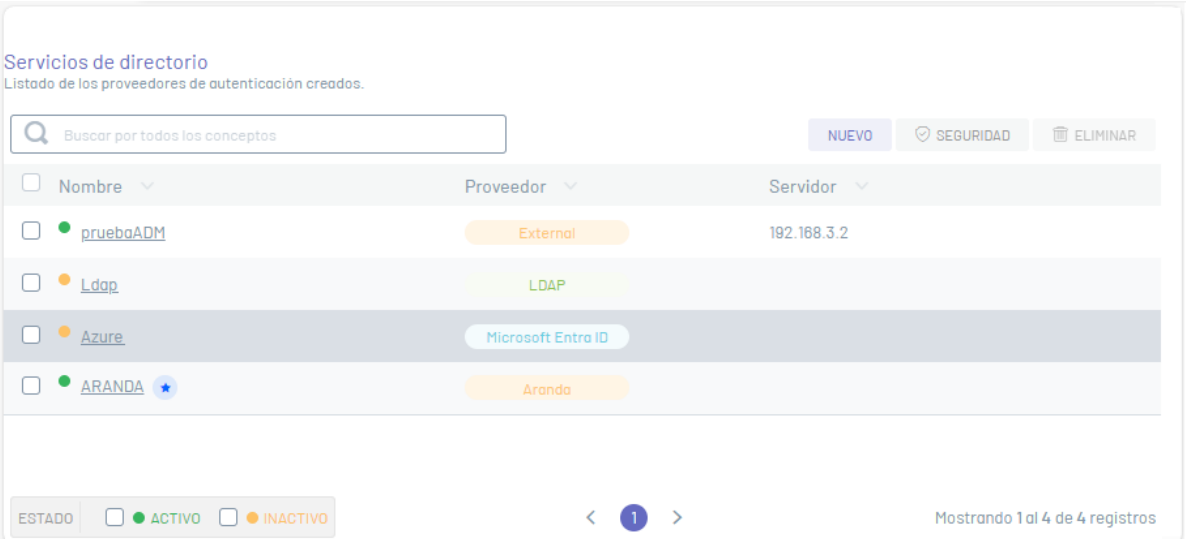
and in the basic vendor configuration window, click **Save**

.

⚠ **Important**: The Microsoft Entra ID provider only allows synchronization of users and groups of users, it does not apply to be used as an authentication provider, so it always remains in an Inactive state. To access the Aranda product website using the users of this type of directory, the external authenticity (SAML) must be configured.

Edit Directory Services

1. To edit a directory or authentication provider, in the Directory Services information view, select a record from the list of existing providers.



Servicios de directorio

Listado de los proveedores de autenticación creados.

Buscar por todos los conceptos

NUEVO · SEGURIDAD · ELIMINAR

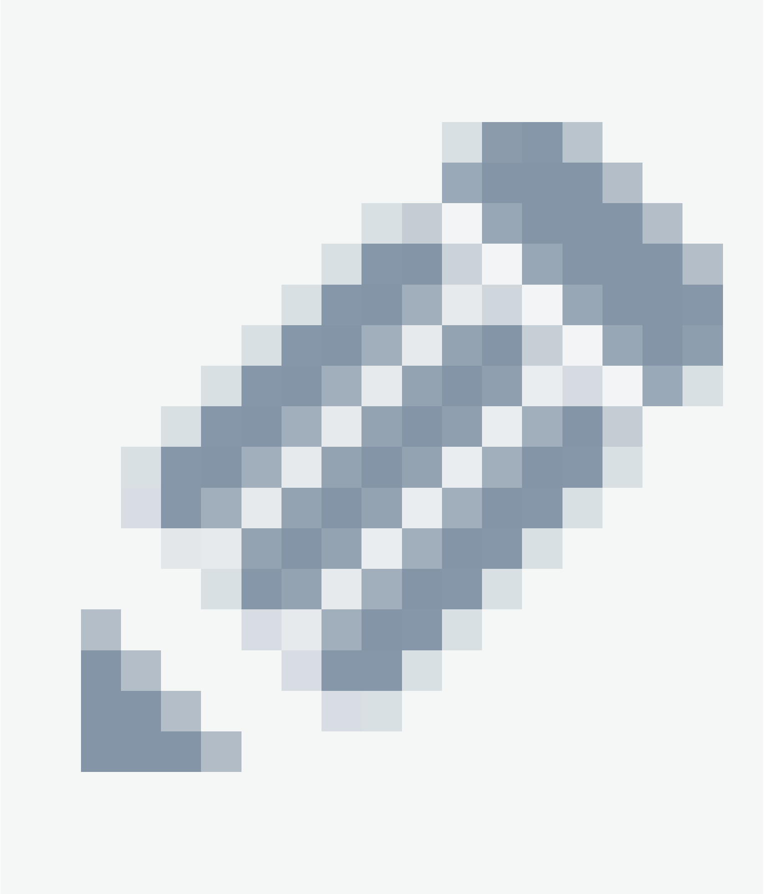
□	Nombre	Proveedor	Servidor
□	● pruebaADM	External	192.168.3.2
□	● Ldap	LDAP	
□	● Azure	Microsoft Entra ID	
□	● ARANDA ★	Aranda	

ESTADO □ ● ACTIVO □ ● INACTIVO

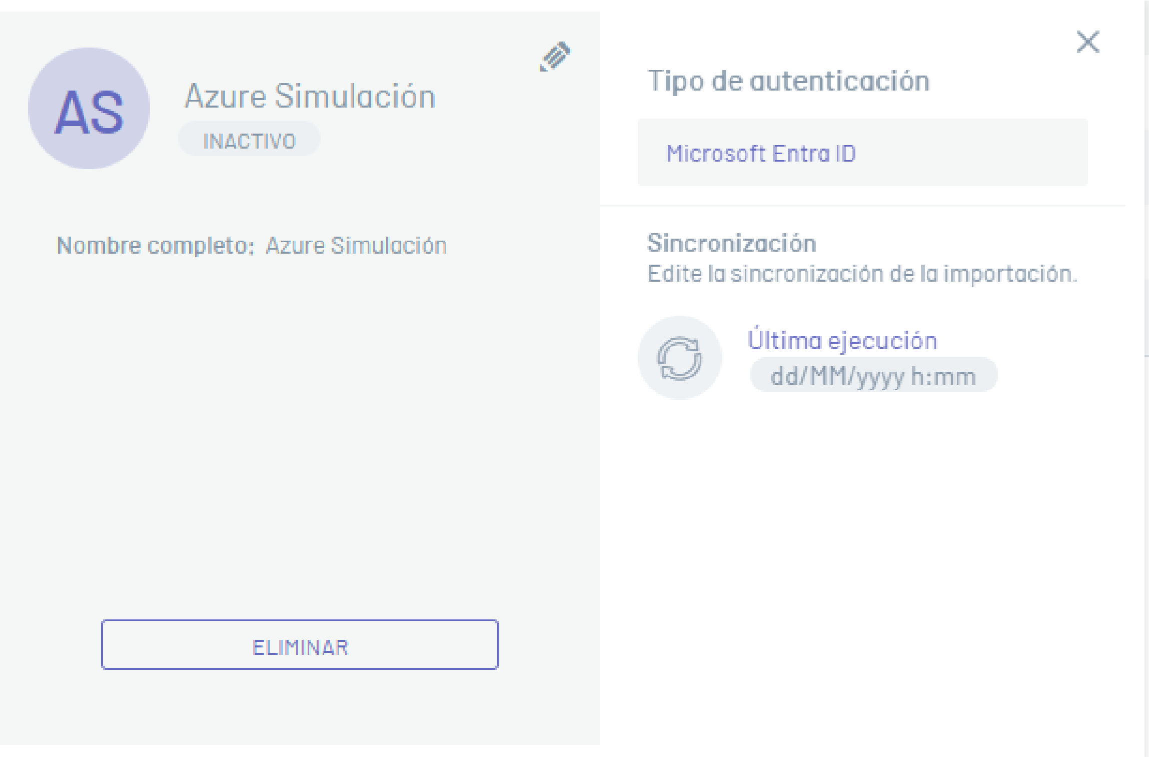
‹ 1 ›

Mostrando 1 al 4 de 4 registros

2. In the detail view click the edit icon



to modify the required information.



AS

Azure Simulación

INACTIVO

Nombre completo: Azure Simulación

ELIMINAR

Tipo de autenticación

Microsoft Entra ID

Sincronización

Edite la sincronización de la importación.

Última ejecución

dd/MM/yyyy h:mm

3. In the Directory Edit window, you can update the basic information and the imported information from the vendor.
4. When you finish editing the user, click on the **Save**

💾

to confirm the changes made.

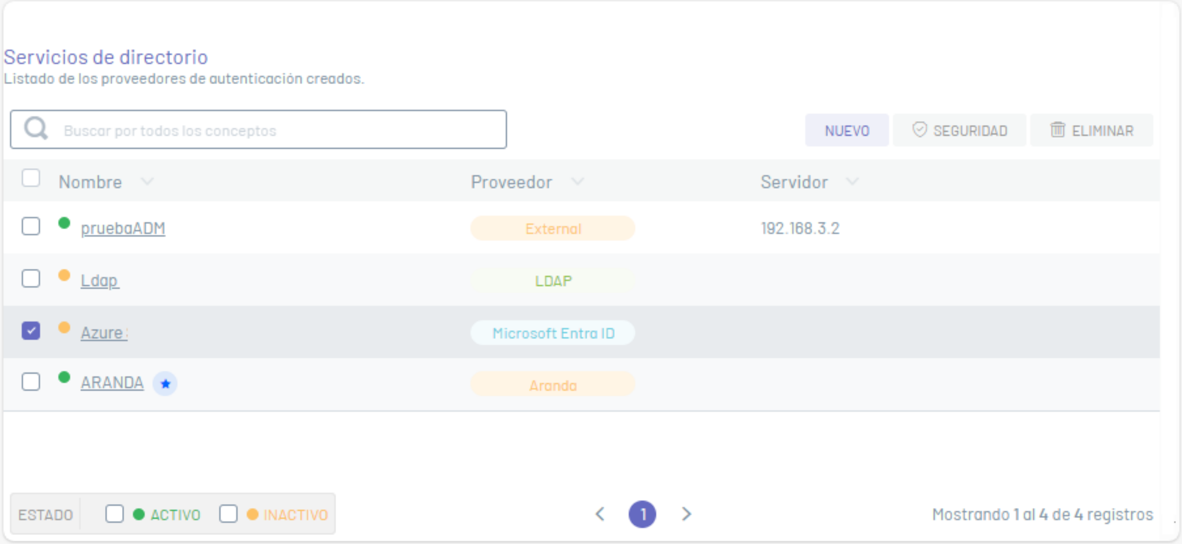
Delete Directory Services

Deleting directory services records can be done in two ways:

1. In the Directory Services Information view, select a record from the list of directory services or authentication providers that you want to delete, and click the

🗑 ELIMINAR

.



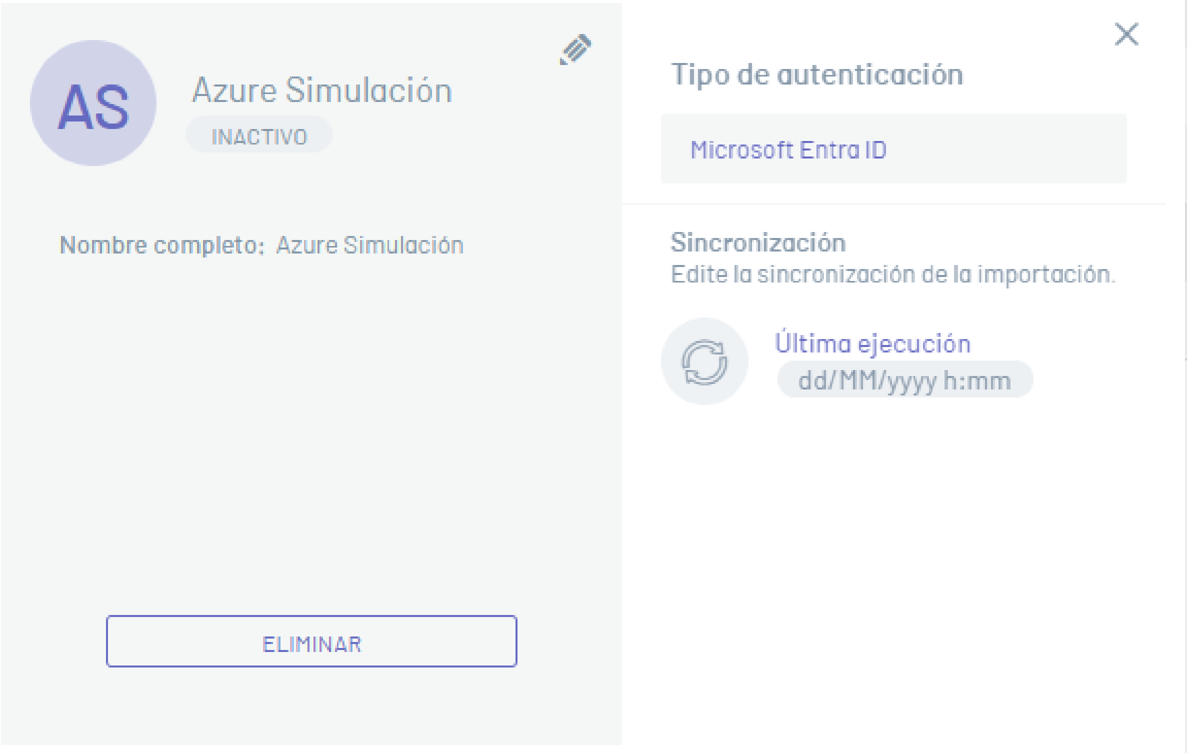
Servicios de directorio
Listado de los proveedores de autenticación creados.

Buscar por todos los conceptos

☐	Nombre	Proveedor	Servidor
☐	● pruebaADM	External	192.168.3.2
☐	● Ldap	LDAP	
☑	● Azure	Microsoft Entra ID	
☐	● ARANDA ★	Aranda	

Mostrando 1 al 4 de 4 registros

2. In the detail view of a selected directory service or provider that you want to delete, click theELIMINATE



Azure Simulación

Nombre completo: Azure Simulación

Tipo de autenticación: Microsoft Entra ID

Sincronización

Edite la sincronización de la importación.

Última ejecución: dd/MM/yyyy h:mm

3. In both cases, you can display a confirmation message to validate the deletion action.

Specification Fields

Basic Facts

Field	Description
Full name	Name you want to assign to your directory.
LDAP Server	DNS or directory server IP.
Port	TCP port to establish communication with the directory server.
Authentication Type	Authentication mode through which connections are allowed.
User Format	You can choose from 3 user formats: UserNameOnly, FullyQualifiedDomainName, and UserPrincipalName.
State	For the creation of the directory, you must select the active state.
Authentication provider	You can choose between two LDAP or Azure AD providers.
Use Default Provider	This option is activated so that the authentication type that appears by default is the one created (LDAP or Azure AD) when entering the AVS site.
Use DS Name Distinction	This option is enabled when the directory server is OpenLDAP and you must submit the distinguished name for logon (Username is not used).
Enable SSL	Indicate if you apply a security protocol.

LDAP/Sample Filters

Filter	Example
Filter to synchronize all users.	(&(objectCategory=person))
Filter to synchronize all groups.	(objectClass=organizationalUnit)
Filter for synchronizing users from the accounting group.	(name=Accounting)

Microsoft EntraID/Sample Filters

Filter	Example
Filter to synchronize all users.	*
Filter to synchronize all users.	*
Filter for synchronizing users from the accounting group.	displayName eq ‘Accounting’

Microsoft EntraID/Example Minimal Field Mapping

Field	EntraId nomenclature
Unique user identifier	*Id*
Username	*UserPrincipalName*

⚐ **Note:** : When the directory is synchronized from a **LDAP on premise** It is used:

- Unique User Identifier : OnPremisesImmutableId
- Username : OnPremisesSamAccountName

⚐ **Note:** : If you want to use the user’s mail as your username, you must:

- Assign **Username : Mail**
- And change the claim in case you have external providers configured in Azure Active Directory

Microsoft EntraID/Example Field Mapping

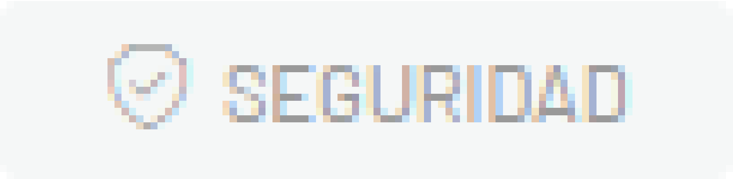
Field	Entrald nomenclature
Company	*CompanyName*
Unique user identifier	*Id*
Username	*UserPrincipalName*
Email	*Mail*
Immediate boss	*Manager*
Country	*Country*
City	*City*
Phone	*BusinessPhones*
FAX	*FaxNumber*
Cell or Mobile	*MobilePhone*
Location in the company	*Building*
Headquarters	*OfficeLocation*
Position within the company	*JobTitle*
Company Area	*Department*
Unique Group Identifier	*Id*
Group Name	*Name*

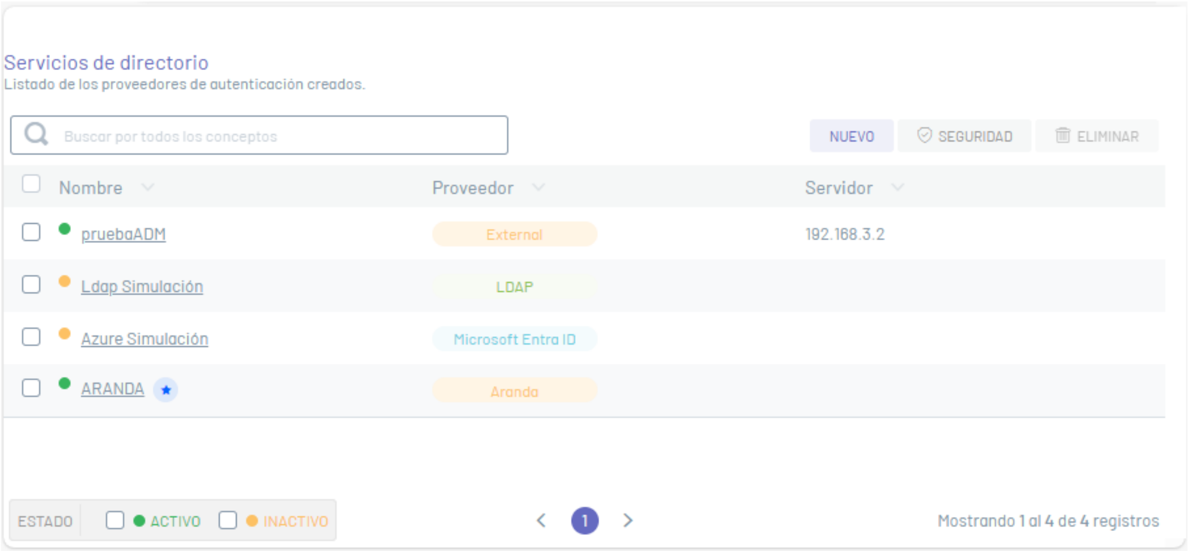
reCAPTCHA Security Configuration

⚠ Important:

- The reCAPTCHA configuration is a component **Optional** that you can implement in directory service provider management, if you require this authentication condition.
- The reCAPTCHA configuration does not apply if the authentication is performed with external providers.

1. To configure reCAPTCHA, in the directory server information view, select the





Servicios de directorio

Listado de los proveedores de autenticación creados.

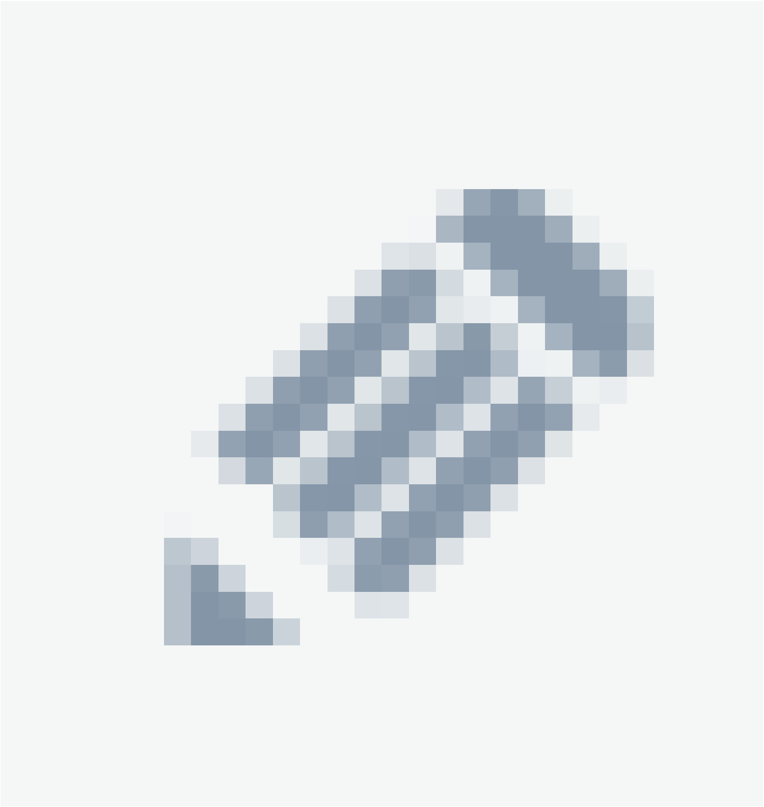
Buscar por todos los conceptos
NUEVO
SEGURIDAD
ELIMINAR

□	Nombre	Proveedor	Servidor
□	● pruebaADM	External	192.168.3.2
□	● Ldap Simulación	LDAP	
□	● Azure Simulación	Microsoft Entra ID	
□	● ARANDA ★	Aranda	

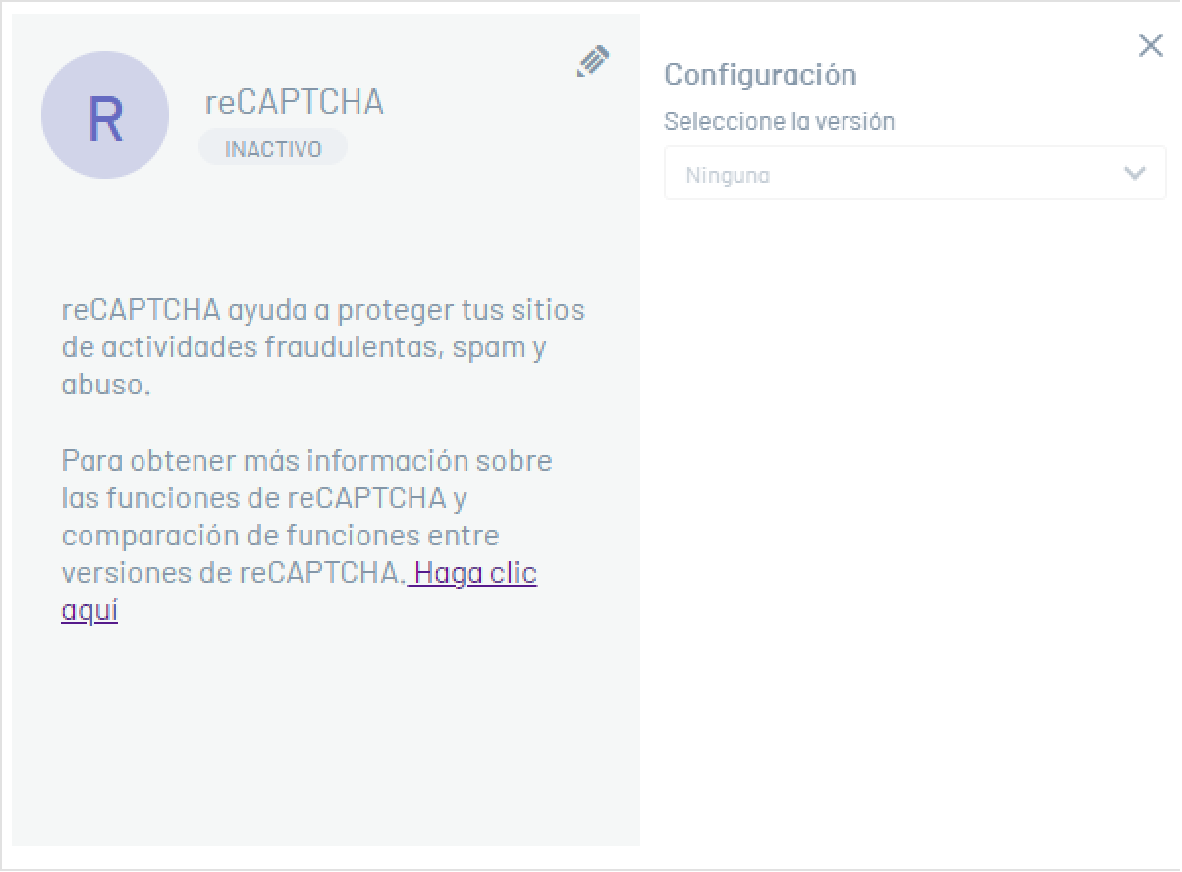
ESTADO □ ● ACTIVO □ ● INACTIVO
‹ 1 ›

Mostrando 1 al 4 de 4 registros

2. The reCAPTCHA window is enabled where you can configure this component. Click the Edit



.



reCAPTCHA

INACTIVO

reCAPTCHA ayuda a proteger tus sitios de actividades fraudulentas, spam y abuso.

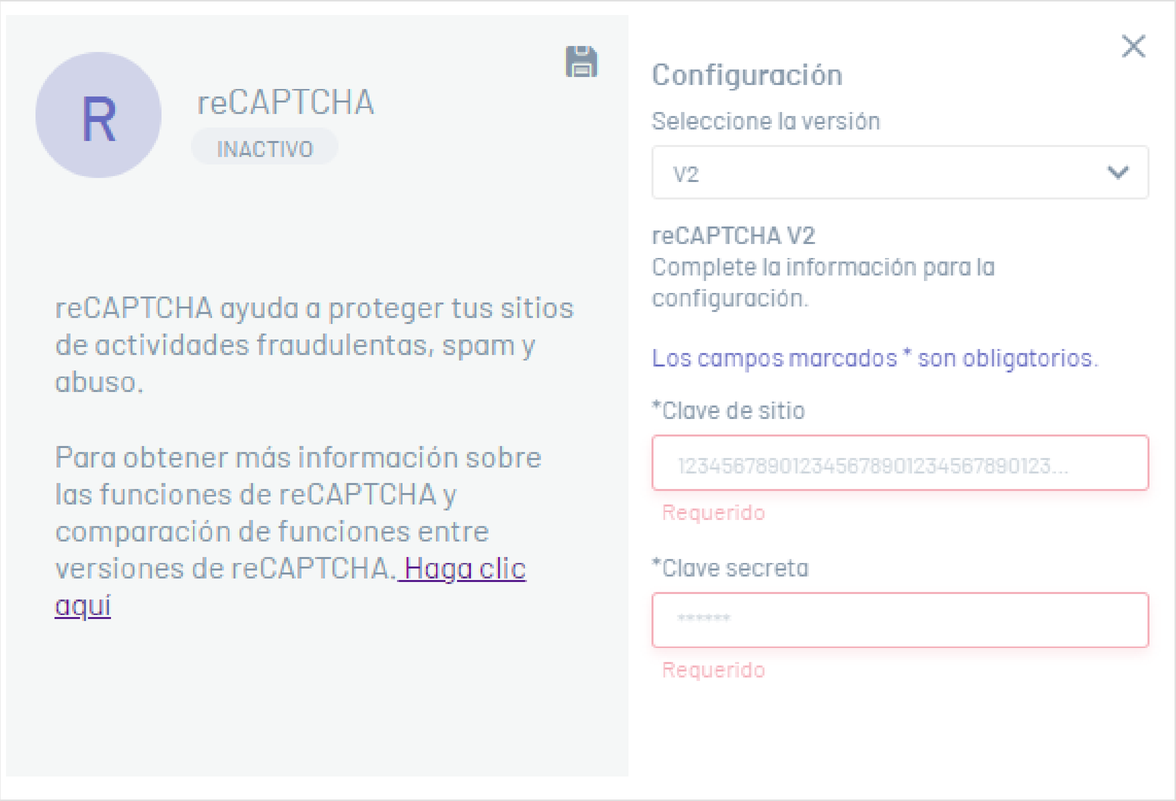
Para obtener más información sobre las funciones de reCAPTCHA y comparación de funciones entre versiones de reCAPTCHA. Haga clic aquí

Configuración

Seleccione la versión

Ninguna

2. Select the required version, according to the type of Key set up on Google and complete the requested information:



R

reCAPTCHA

INACTIVO

reCAPTCHA ayuda a proteger tus sitios de actividades fraudulentas, spam y abuso.

Para obtener más información sobre las funciones de reCAPTCHA y comparación de funciones entre versiones de reCAPTCHA. Haga clic aquí

Configuración

Seleccione la versión

V2

reCAPTCHA V2
Complete la información para la configuración.

Los campos marcados * son obligatorios.

*Clave de sitio

12345678901234567890123456789012З...

Requerido

*Clave secreta

******

Requerido

Field	Field Type	Description
Version	Selector	Version configured in Google.
Site Key	Text	Public key obtained from the configuration made in Google.
Secret Key	Text	Secret key obtained from the configuration made in Google.
Punctuation	Text	If you choose V3 version, set the Score for user rating

⚐ Note:

1. When changing the version of reCAPTCHA, enter the requested fields again or cancel the operation.
2. If the reCAPTCHA configuration is not set correctly, access to the console will be prevented due to lack of validation. To resolve the conflict, make the adjustment in the database.

Configuration for reCAPTCHA V2 and V3

Preconditions

Create reCAPTCHA keys for websites

- Sign up for Google.
- Prepare your environment for reCAPTCHA Enterprise.
- Make sure you have the Identity and Access Management role: reCAPTCHA Enterprise Administrator (roles/recaptchaenterprise.admin)
- Define the key type that best fits your use case.

Configure tokens for google recaptcha

Information Needed for Setup

⚐ Note: A previously created google account and environment are required for reCAPTCHA Enterprise: To create Google Cloud console and Google Cloud project: Go to Google Cloud

Enable the reCAPTCHA Enterprise API

1. In the Google Cloud console, go to the Google Cloud API page. **reCAPTCHA Enterprise**
2. Verify that the project name appears in the project selector at the top of the page. If you do not see the project name, click the project selector and select the required project.
3. Click Enable.

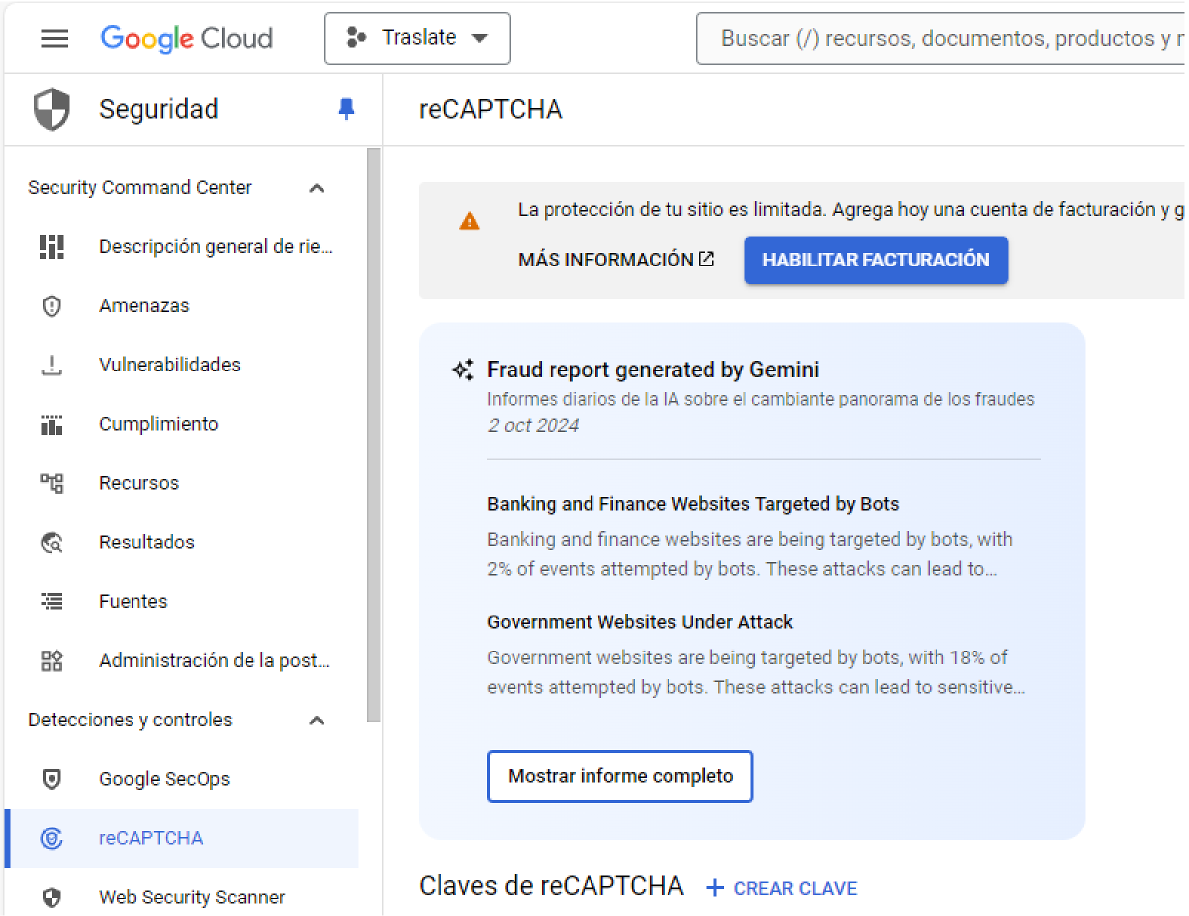
> ⚐ **Note:** Redirection is performed on the page, where the creation of credentials will be allowed.

Creating reCAPTCHA Keys

1. In the Google Cloud console, go to the reCAPTCHA Enterprise page.
2. Verify that the project name appears in the resource selector at the top of the page.

> ⚐ **Note:** If you do not see the project name, click on the resource selector and select the required project.

3. Click **Create key.**



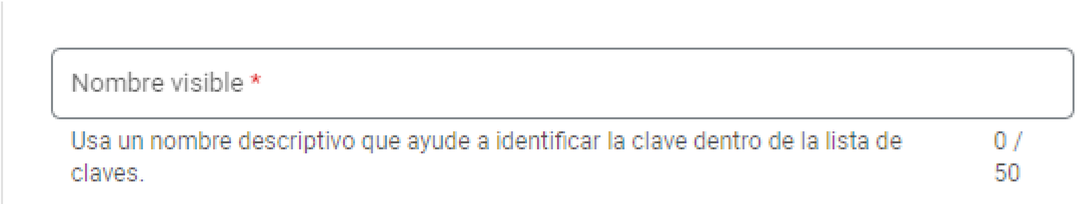
La protección de tu sitio es limitada. Agrega hoy una cuenta de facturación y g

Fraud report generated by Gemini
Informes diarios de la IA sobre el cambiante panorama de los fraudes
2 oct 2024

Banking and Finance Websites Targeted by Bots
Banking and finance websites are being targeted by bots, with 2% of events attempted by bots. These attacks can lead to...

Government Websites Under Attack
Government websites are being targeted by bots, with 18% of events attempted by bots. These attacks can lead to sensitive...

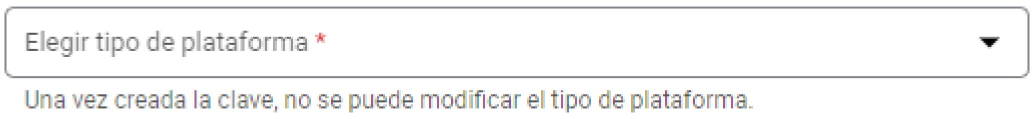
4. En el campo **Nombre visible**, ingrese el nombre visible para la clave.



Nombre visible *

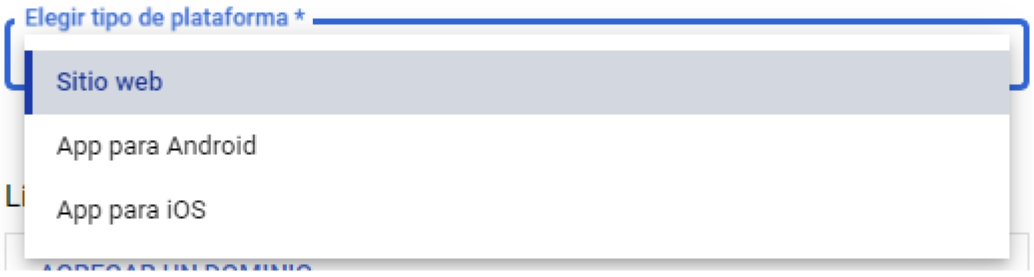
Usa un nombre descriptivo que ayude a identificar la clave dentro de la lista de claves. 0 / 50

5. En el menú **Elegir tipo de plataforma**, seleccione **Sitio web**.



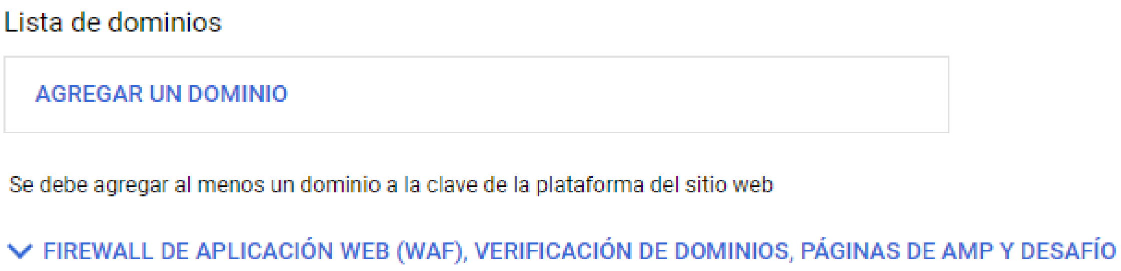
Elegir tipo de plataforma *

Una vez creada la clave, no se puede modificar el tipo de plataforma.



⚐ **Note:** The **List of domains**.

6. Enter the domain name of the website:


Lista de dominios
AGREGAR UN DOMINIO

Se debe agregar al menos un dominio a la clave de la plataforma del sitio web

FIREWALL DE APLICACIÓN WEB (WAF), VERIFICACIÓN DE DOMINIOS, PÁGINAS DE AMP Y DESAFÍO

- En la sección **Lista de dominios**, haga clic en **Agregar un dominio, ingrese el nombre del dominio.**
- En el campo **Dominio**, ingrese el nombre del dominio.
- Opcional: Para agregar un dominio adicional, haga clic en **Agregar un dominio** e ingrese el nombre de otro dominio en el campo **Dominio**. Se podrán agregar hasta 250 dominios.
  La clave de reCAPTCHA, para sitios web, es única para los dominios y subdominios definidos. Se podrá definir más de un dominio si se entrega el sitio web desde varios dominios. Si define un dominio (por ejemplo, examplepetstore.com), no es requerido definir los subdominios (por ejemplo, subdomain.examplepetstore.com).
  Según el tipo de clave de reCAPTCHA que requiere crear para el sitio web, podrá realizar cualquiera de las acciones correspondientes:

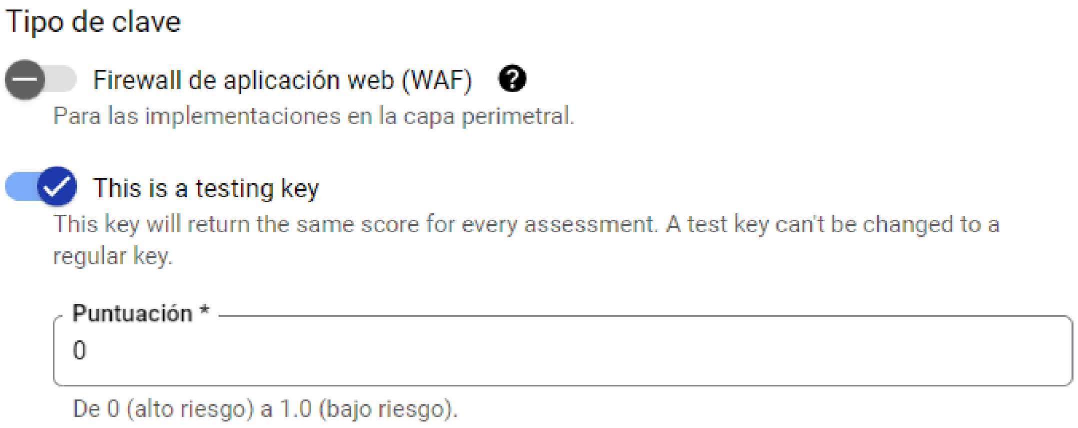
  ⚐ **Note:** Creating a key based on scores is the default option in the Google Cloud console."

- **reCAPTCHA based on scores:**

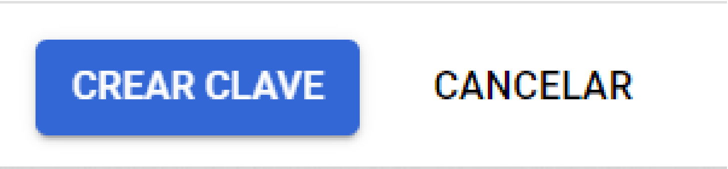
- To protect the reCAPTCHA key for domain and subdomains, validate that the Disable domain verification option is disabled.
  If you require the score-based key to work with Accelerated Mobile Pages (AMP), toggle the **Disabling domain verification is a security risk because there are no restrictions on the site, so anyone can access and use the reCAPTCHA key.

```
<center><img src="/common/en/assets/images/configurar_recaptcha/img8.png" ></center>
```

  - Si requiere que la clave basada en puntuaciones funcione con Accelerated Mobile Pages (AMP), active el botón **Permitir que esta clave funcione con páginas de AMP**.
  - En entornos que no son de producción, si requiere especificar una puntuación que muestre la clave al crear evaluaciones para ella, haz lo siguiente:
    - Haga clic en el botón de activación **Esta es una clave de prueba.**.
    - En el cuadro **Score**, especifique una puntuación entre 0 y 1.0.


Tipo de clave
Firewall de aplicación web (WAF)
Para las implementaciones en la capa perimetral.
This is a testing key
This key will return the same score for every assessment. A test key can't be changed to a regular key.
Puntuación *
0
De 0 (alto riesgo) a 1.0 (bajo riesgo).

  - Haga clic en **Crear clave**.



⚐ Note: The new key will appear on the**reCAPTCHA keys**.

⚐ Note: Using checkbox keys is not recommended, as they increase user friction and do not improve accuracy.

- **reCAPTCHA with checkboxes:**
- Expand the section **Web Application Firewall (WAF), Domain Verification, AMP Pages, and Challenge**.

```
  <center><img src="/common/en/assets/images/configurar_recaptcha/img7.png" ></center> -  To protect the
reCAPTCHA key for domain and subdomains, confirm that the Disable domain verification option is disabled. Disabling
domain verification is a security risk because there are no restrictions on the site, so anyone can access and use the
reCAPTCHA key.

  <center><img src="/common/en/assets/images/configurar_recaptcha/img8.png" ></center> -  Enable the Activation
Button **Use the checkbox challenge**.

  <center><img src="/common/en/assets/images/configurar_recaptcha/img12.png" ></center> -  Select the option
**Challenge Security** adequate. -  For a non-production environment, if you need to specify a score that displays the key
when you generate assessments for it, keep the following in mind:


- Click on the activation button **This is a test key.**.
- In the painting **Score**, specifies a score between 0 and 1.0.
- Select the option **Challenge Type** adequate.

 - On some occasions, the challenge appears as **automatic**.
 - **No CAPTCHA** it does not show a challenge.
 - One **Unsolved challenge** shows the images, but the challenge is not approved.


   <center><img src="/common/en/assets/images/configurar_recaptcha/img13.png" ></center>
```

- Click **Create key**.

```
<center><img src="/common/en/assets/images/configurar_recaptcha/img10.png" ></center>
```

⚐ Note: The new key will appear on the**reCAPTCHA keys**.

⚐ Note:

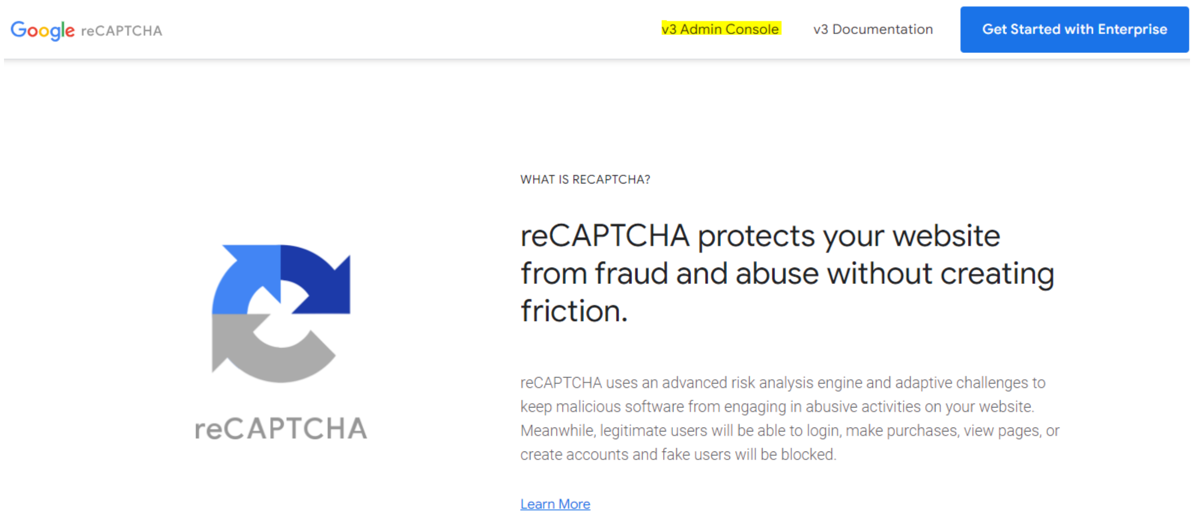
- The challenge safety option controls the likelihood of prompting a user for a secondary challenge to select images based on an identified category (for example, select the images with a motorcycle or ladders).
- To ensure better fraud protection, select (more bot safe)**.
- If you select the**Difficulty of the simplest challenge**, users are less likely to be prompted for the visual challenge.

⚐ Note: Note: After you create the reCAPTCHA keys, you can edit or delete them. You will not be able to recover deleted keys.

Configure reCAPTCHA V2

reCAPTCHA Version 2

1. Once registered in google, enter the administration by reCAPTCHA



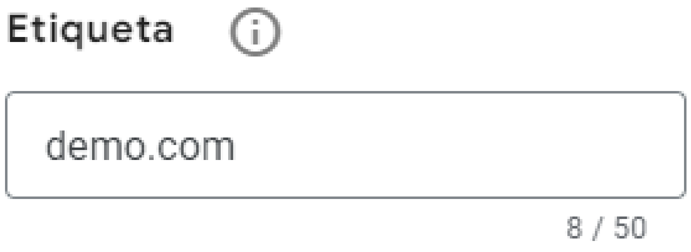
WHAT IS RECAPTCHA?

reCAPTCHA protects your website from fraud and abuse without creating friction.

reCAPTCHA uses an advanced risk analysis engine and adaptive challenges to keep malicious software from engaging in abusive activities on your website. Meanwhile, legitimate users will be able to login, make purchases, view pages, or create accounts and fake users will be blocked.

Learn More

2. Add the field value **Label**

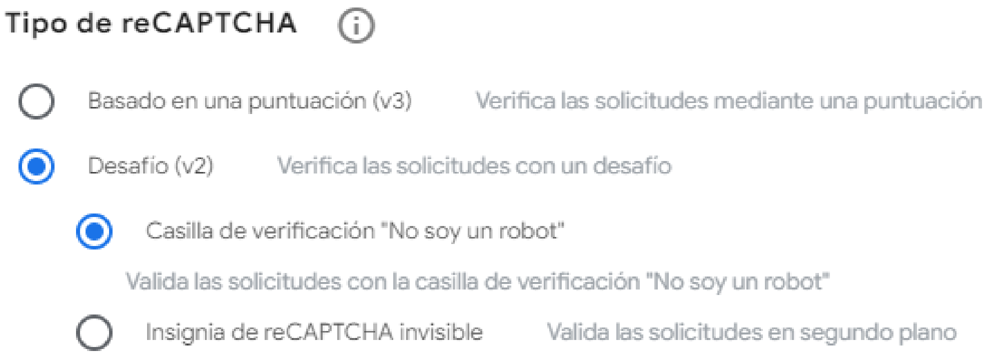

Etiqueta

demo.com

8 / 50

3. On the screen that is enabled select **Challenge (v2)** and depending on the desired configuration:

- Check the option **"I'm not a robot" checkbox"**
- Check the option **"Invisible reCAPTCHA badge"**


Tipo de reCAPTCHA

○ Basado en una puntuación (v3) Verifica las solicitudes mediante una puntuación

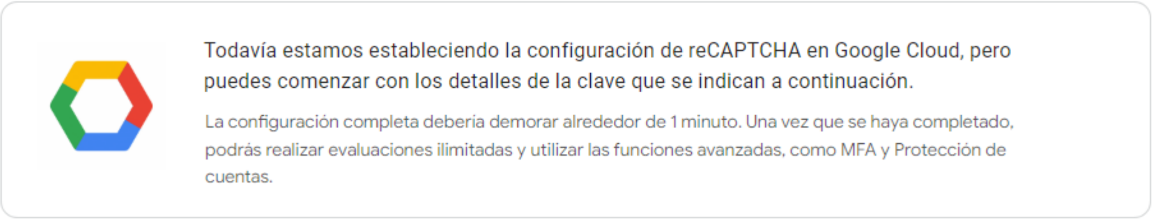
● Desafío (v2) Verifica las solicitudes con un desafío

● Casilla de verificación "No soy un robot"

Valida las solicitudes con la casilla de verificación "No soy un robot"

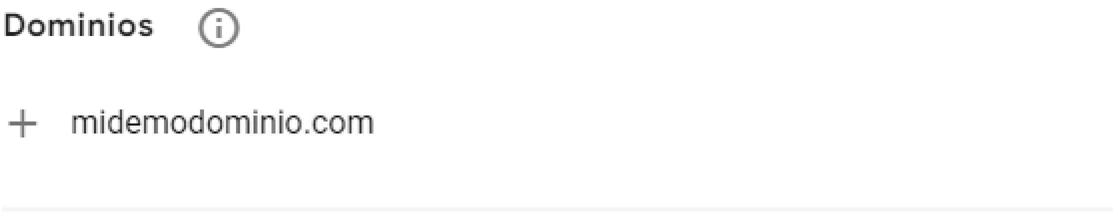
○ Insignia de reCAPTCHA invisible Valida las solicitudes en segundo plano

⚐ **Note:** You will be able to view a site configuration notification; Wait for options to be enabled to continue:


Todavía estamos estableciendo la configuración de reCAPTCHA en Google Cloud, pero puedes comenzar con los detalles de la clave que se indican a continuación.

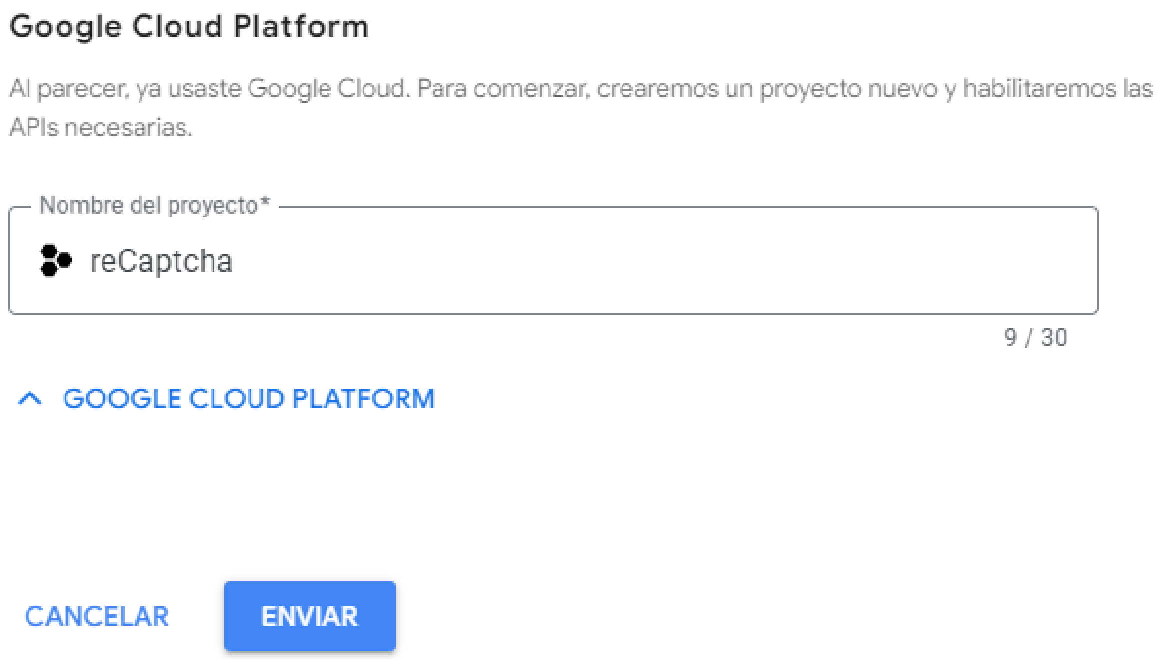
La configuración completa debería demorar alrededor de 1 minuto. Una vez que se haya completado, podrás realizar evaluaciones ilimitadas y utilizar las funciones avanzadas, como MFA y Protección de cuentas.

4. Add the value of the field **Domains**.


Dominios

+ midemodominio.com

5. Select the project name and click **Send**.



Google Cloud Platform

Al parecer, ya usaste Google Cloud. Para comenzar, crearemos un proyecto nuevo y habilitaremos las APIs necesarias.

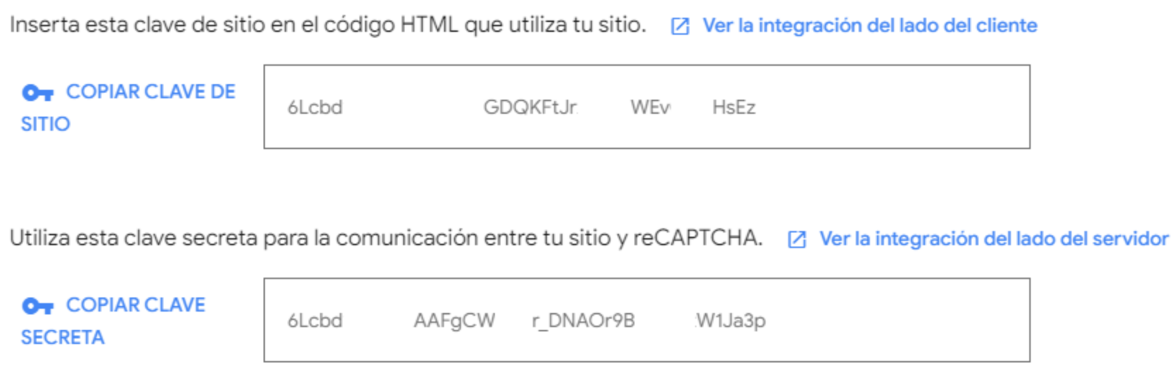
Nombre del proyecto*: reCaptcha

9 / 30

⚐ **Note:** The page will automatically display the site keys, for later configuration in the DirectoryServices component

6. Copy the information displayed in the fields:

- Site key.
- Secret key.



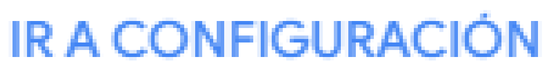
Inserta esta clave de sitio en el código HTML que utiliza tu sitio. Ver la integración del lado del cliente

COPIAR CLAVE DE SITIO: 6Lcbd GDQKFtJr WEv HsEz

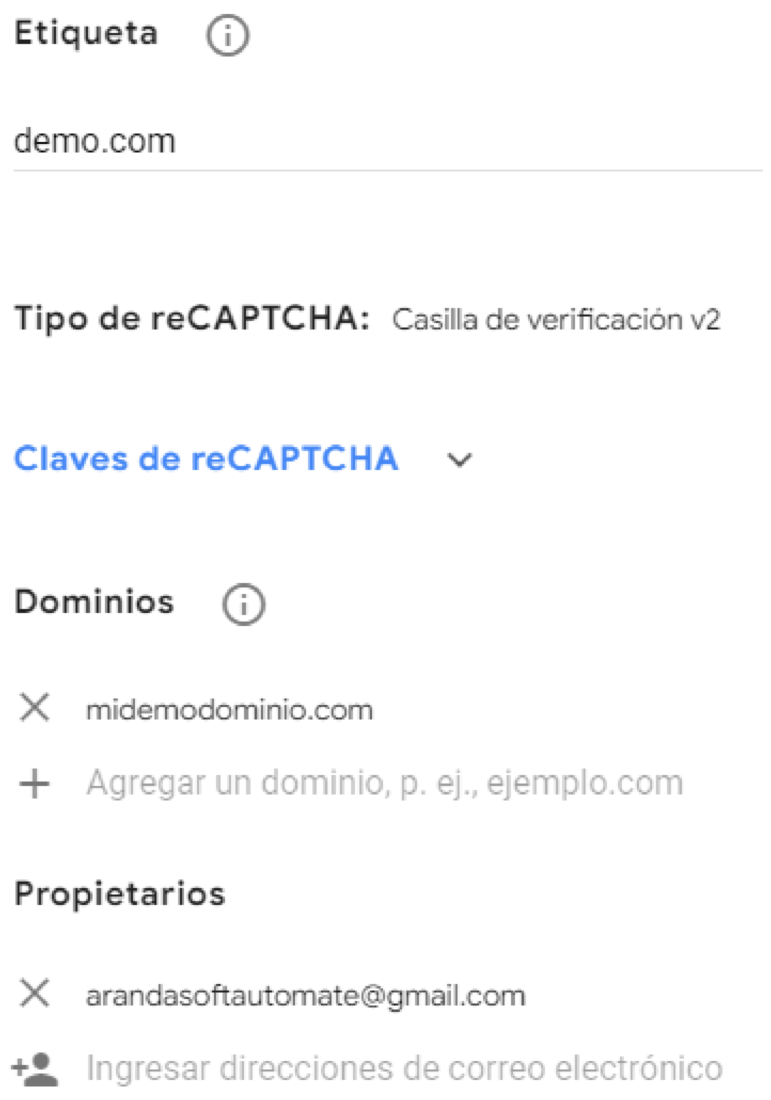
Utiliza esta clave secreta para la comunicación entre tu sitio y reCAPTCHA. Ver la integración del lado del servidor

COPIAR CLAVE SECRETA: 6Lcbd AAFgCW r_DNAOr9B W1Ja3p

7. After saving or configuring the keys, click on the "GO TO SETTINGS" button



⚐ **Note:** Verify on the page that it is enabled that the information presented corresponds to the values previously filled out.



Etiqueta

demo.com

Tipo de reCAPTCHA: Casilla de verificación v2

Claves de reCAPTCHA

Dominios

× midemodominio.com

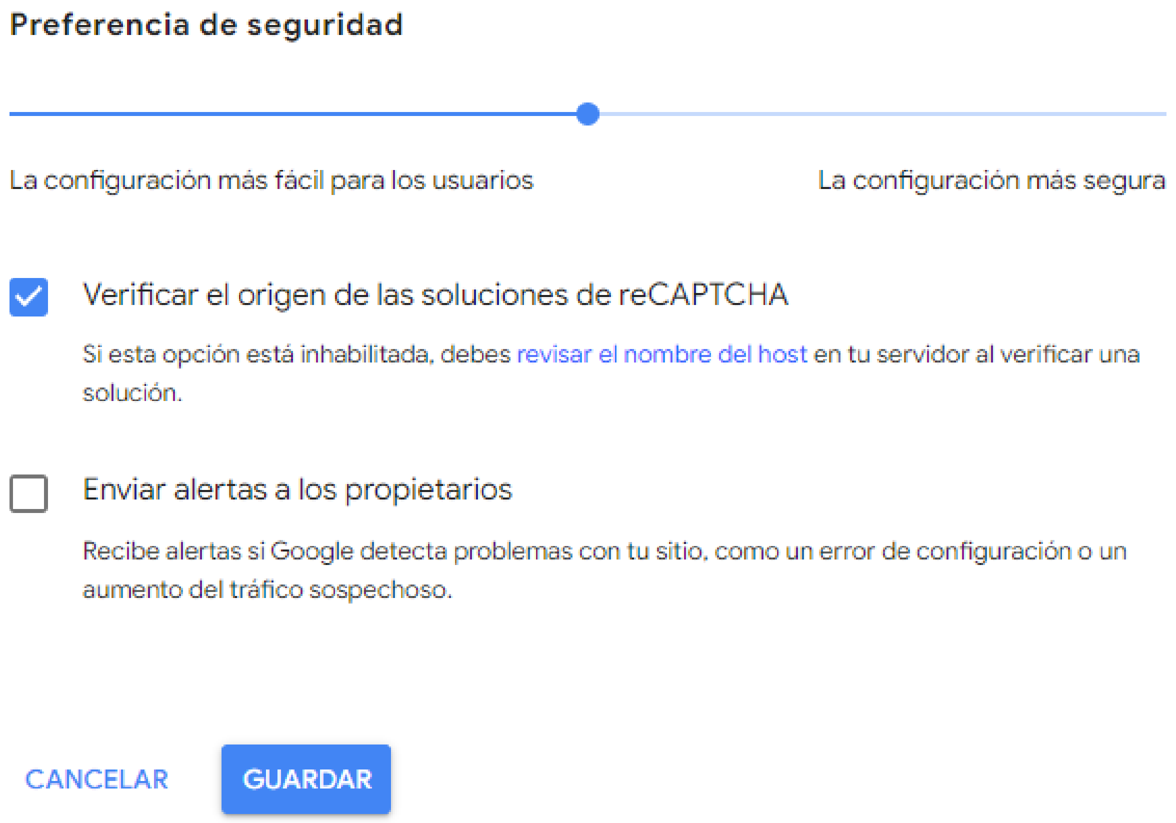
+ Agregar un dominio, p. ej., ejemplo.com

Propietarios

× arandasoftautomate@gmail.com

Ingresar direcciones de correo electrónico

8. Validate and configure the Security Preference as required and click the Save



Preferencia de seguridad

La configuración más fácil para los usuarios

La configuración más segura

☑ Verificar el origen de las soluciones de reCAPTCHA

Si esta opción está inhabilitada, debes revisar el nombre del host en tu servidor al verificar una solución.

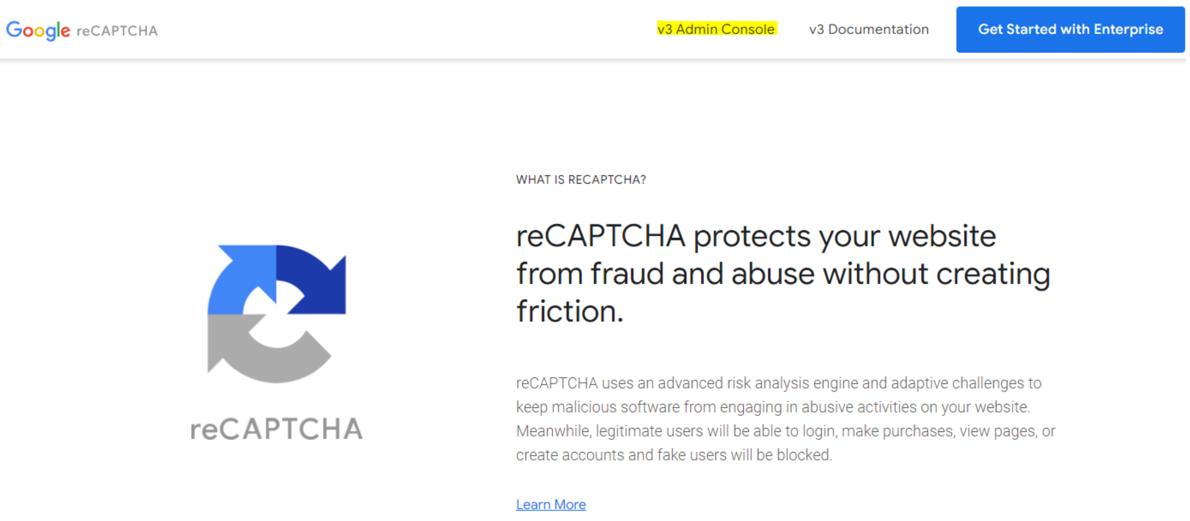
□ Enviar alertas a los propietarios

Recibe alertas si Google detecta problemas con tu sitio, como un error de configuración o un aumento del tráfico sospechoso.

Configure reCAPTCHA V3

reCAPTCHA Version 3

1. Once registered in google, enter the [administration]() by reCAPTCHA



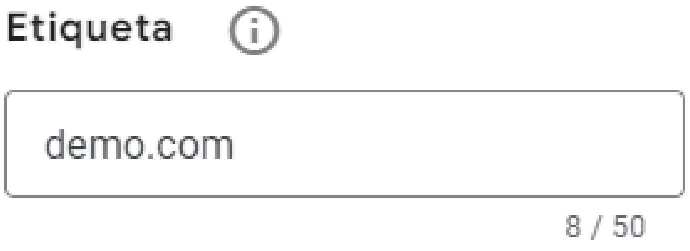
WHAT IS RECAPTCHA?

reCAPTCHA protects your website from fraud and abuse without creating friction.

reCAPTCHA uses an advanced risk analysis engine and adaptive challenges to keep malicious software from engaging in abusive activities on your website. Meanwhile, legitimate users will be able to login, make purchases, view pages, or create accounts and fake users will be blocked.

Learn More

2. Add the field value **Label**

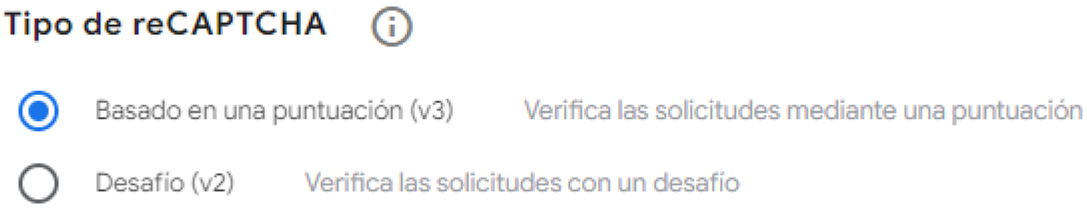


Etiqueta

demo.com

8 / 50

3. On the screen that is enabled select **Based on a score (v3)** and depending on the desired configuration:

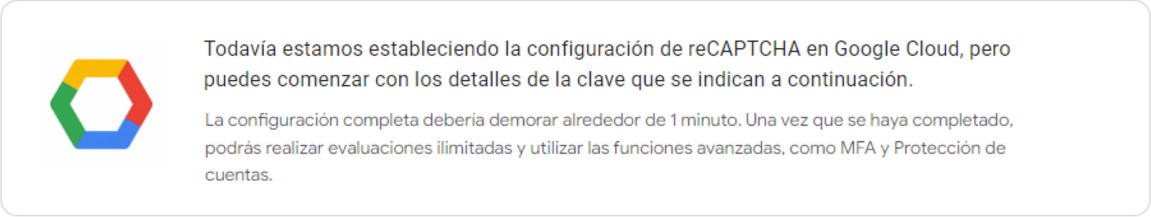


Tipo de reCAPTCHA

● Basado en una puntuación (v3) Verifica las solicitudes mediante una puntuación

○ Desafío (v2) Verifica las solicitudes con un desafío

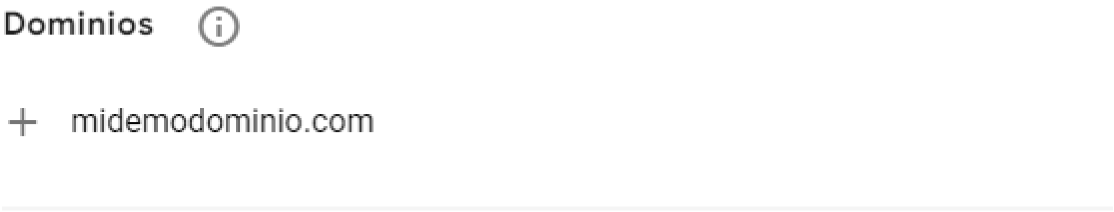
⚐ **Note:** When viewing the site configuration notification, wait for the options to continue to be enabled:



Todavía estamos estableciendo la configuración de reCAPTCHA en Google Cloud, pero puedes comenzar con los detalles de la clave que se indican a continuación.

La configuración completa debería demorar alrededor de 1 minuto. Una vez que se haya completado, podrás realizar evaluaciones ilimitadas y utilizar las funciones avanzadas, como MFA y Protección de cuentas.

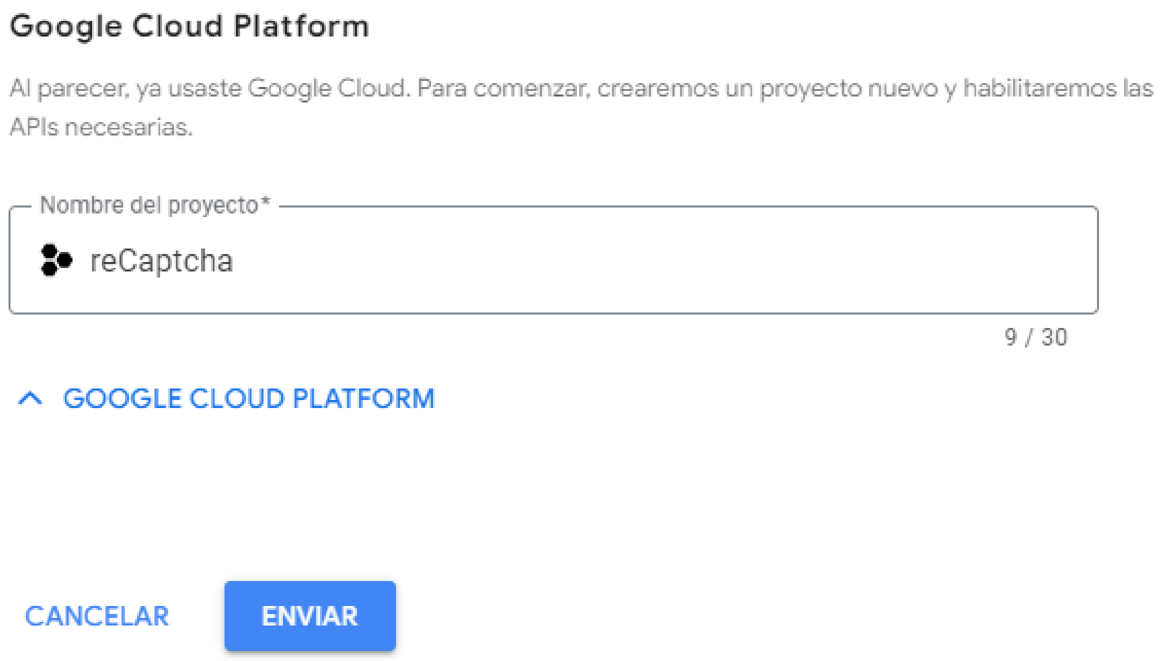
4. Add the value of the field **Domains**.



Dominios

+ midemodominio.com

5. Select the project name and click **Send**.



Google Cloud Platform

Al parecer, ya usaste Google Cloud. Para comenzar, crearemos un proyecto nuevo y habilitaremos las APIs necesarias.

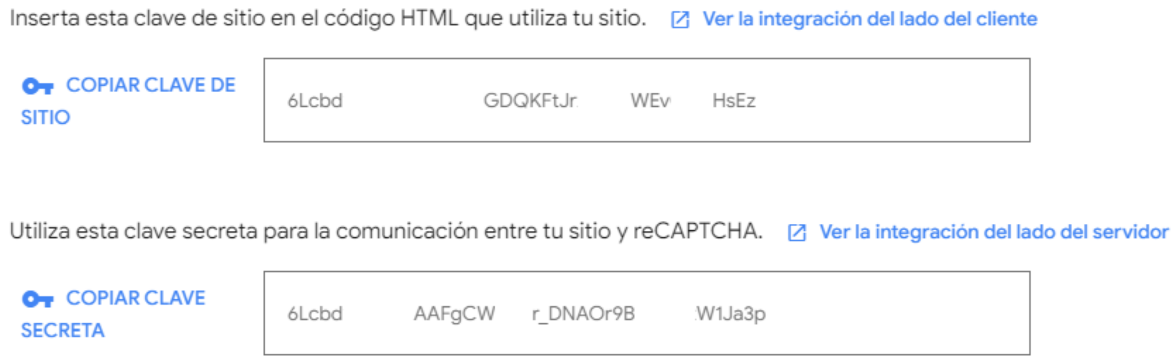
Nombre del proyecto*: reCaptcha

9 / 30

⚐ Note: The page will automatically display the site keys, for later configuration in the DirectoryServices component

6. Copy the information displayed in the fields:

- Site key.
- Secret key.



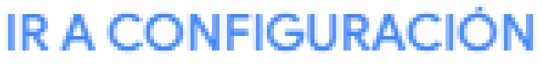
Inserta esta clave de sitio en el código HTML que utiliza tu sitio. Ver la integración del lado del cliente

COPIAR CLAVE DE SITIO: 6Lcbd GDQKFtJr WEv HsEz

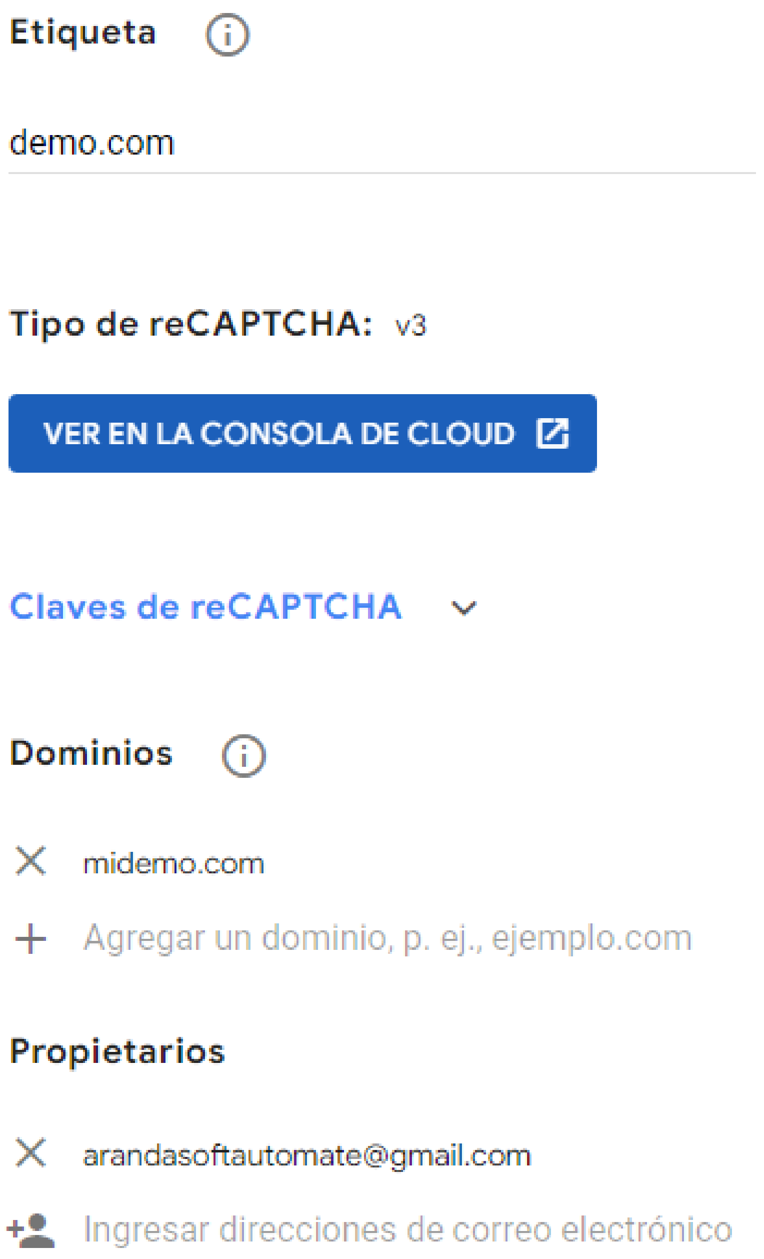
Utiliza esta clave secreta para la comunicación entre tu sitio y reCAPTCHA. Ver la integración del lado del servidor

COPIAR CLAVE SECRETA: 6Lcbd AAFgCW r_DNAOr9B W1Ja3p

7. After saving or configuring the keys, click on the "GO TO SETTINGS" button



⚐ Note: Verify on the page that it is enabled that the information presented corresponds to the values previously filled out.



Etiqueta

demo.com

Tipo de reCAPTCHA: v3

Dominios

midemo.com

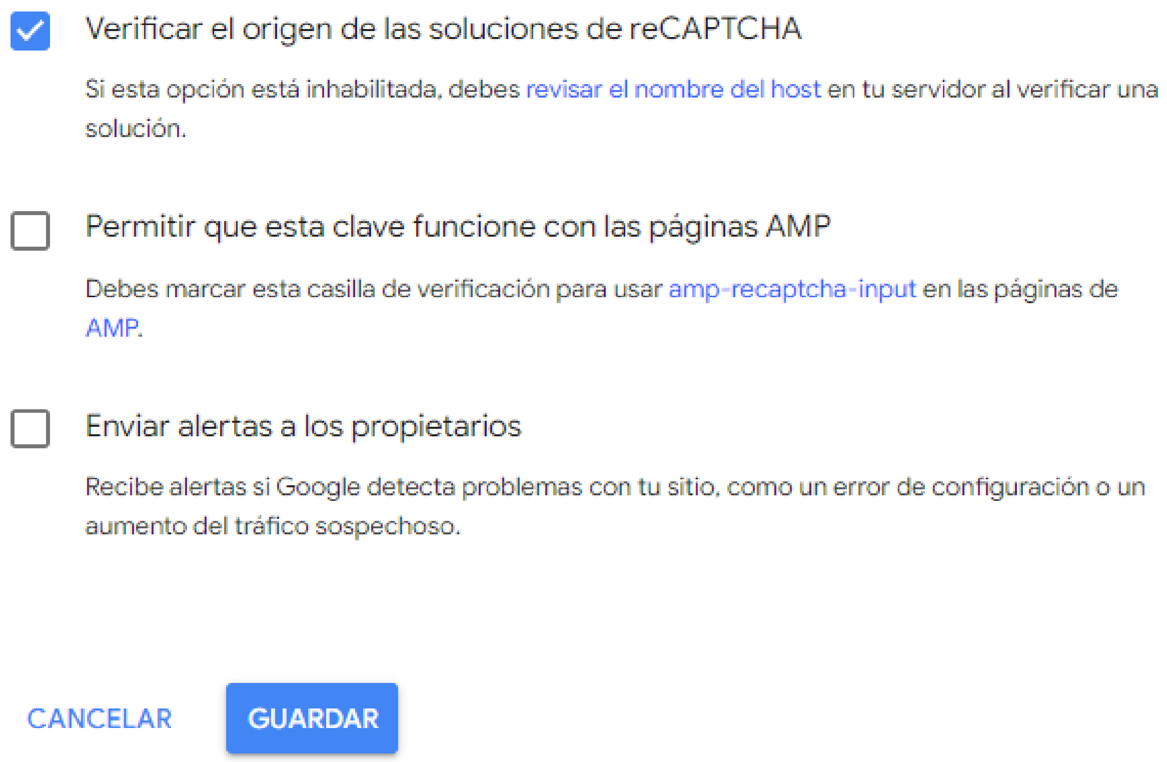
Agregar un dominio, p. ej., ejemplo.com

Propietarios

arandasoftautomate@gmail.com

Ingresar direcciones de correo electrónico

8. Validate and configure the **Security Preference** as required and click the **Save**



☑ Verificar el origen de las soluciones de reCAPTCHA

Si esta opción está inhabilitada, debes revisar el nombre del host en tu servidor al verificar una solución.

□ Permitir que esta clave funcione con las páginas AMP

Debes marcar esta casilla de verificación para usar amp-recaptcha-input en las páginas de AMP.

□ Enviar alertas a los propietarios

Recibe alertas si Google detecta problemas con tu sitio, como un error de configuración o un aumento del tráfico sospechoso.

External Authentication Module

Preview Vendor Data

1. Get ADFS Provider Data

Configure the corresponding application in ADFS (Active Directory Federation Service).

Microsoft's AD FS (Active Directory Federation Services) configuration is used to enable federated authentication and Single Sign-On (SSO), allowing users to access multiple applications and services (both on-premises and in the cloud)

using a single identity.
For more information, see [ADFS ↪ Configuration].

2. Get Azure Devops provider data

Configure the corresponding application in Azure Active Directory.

Configuring SAML (Security Assertion Markup Language) in Azure DevOps allows you to integrate federated authentication with an external Identity Provider (IdP), such as Azure Active Directory (Azure AD), Okta, ADFS, or other SAML 2.0-compliant providers. This allows users to sign in to Azure DevOps using their corporate credentials, enabling Single Sign-On (SSO) and more secure access control.
For more information, see [Azure Active Directory ↪].

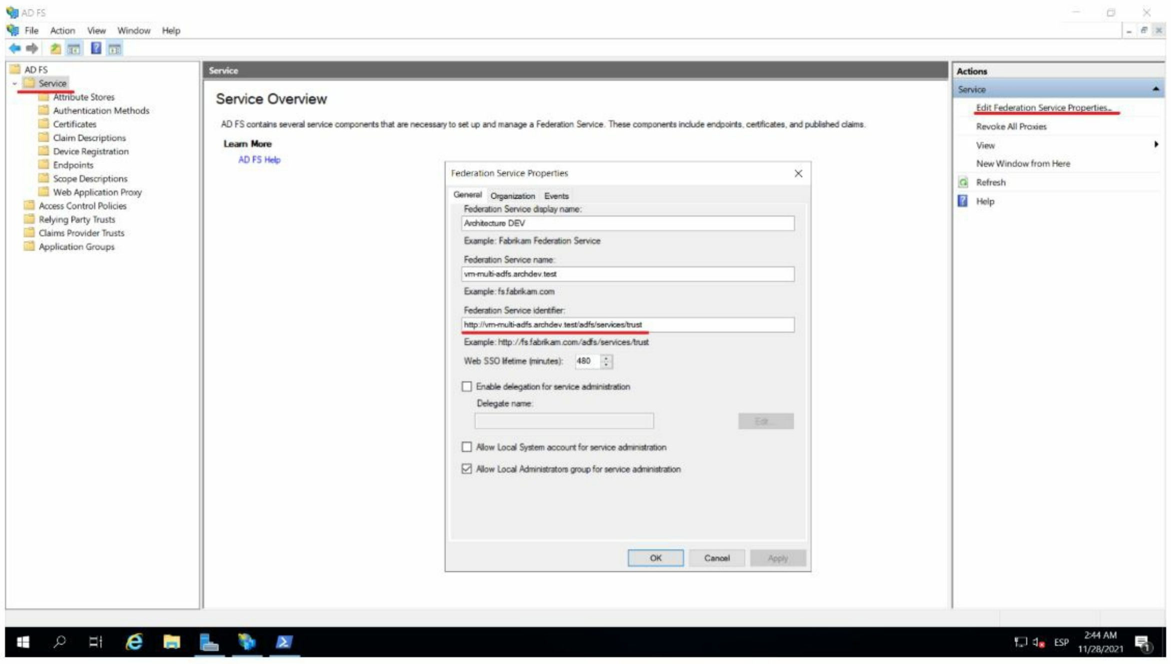
Preview Vendor Data

ADFS Configuration

Get supplier data

1. The identity identifier can be obtained directly from the ADFS server by opening the console **AD FS Management**, in the main menu by selecting the **Service** and in the Actions menu by selecting the **Edit Federation Service Properties** located on the right.

> ⚐ **Note:** Identity identifier: In a default installation, its value corresponds to https://**/adfs/services/trust.



Service Overview

AD FS contains several service components that are necessary to set up and manage a Federation Service. These components include endpoints, certificates, and published claims.

Learn More
AD FS Help

Federation Service Properties

General | Organization | Events

Federation Service display name: Architecture DEV
Example: Fabrikam Federation Service

Federation Service name: vm-multi-adfs.archdev.test
Example: fs.fabrikam.com

Federation Service identifier: http://vm-multi-adfs.archdev.test/adfs/services/trust
Example: http://fs.fabrikam.com/adfs/services/trust

Web SSO lifetime (minutes): 480

☐ Enable delegation for service administration
Delegate name:
Edit...

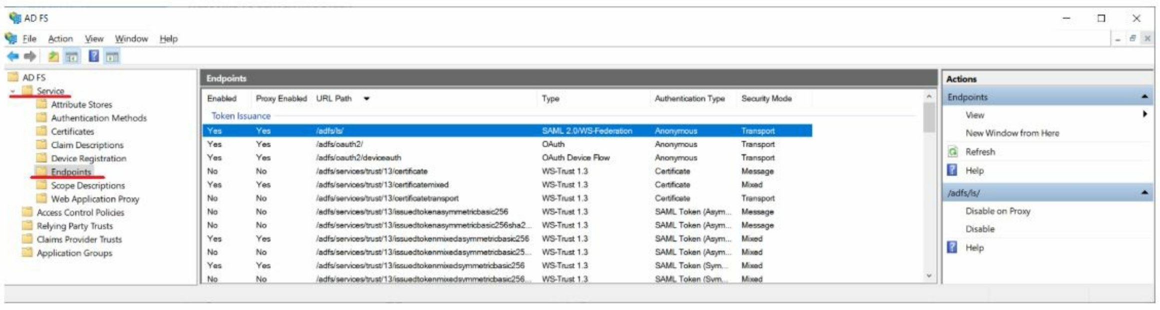
☐ Allow Local System account for service administration

☑ Allow Local Administrators group for service administration

OK | Cancel | Apply

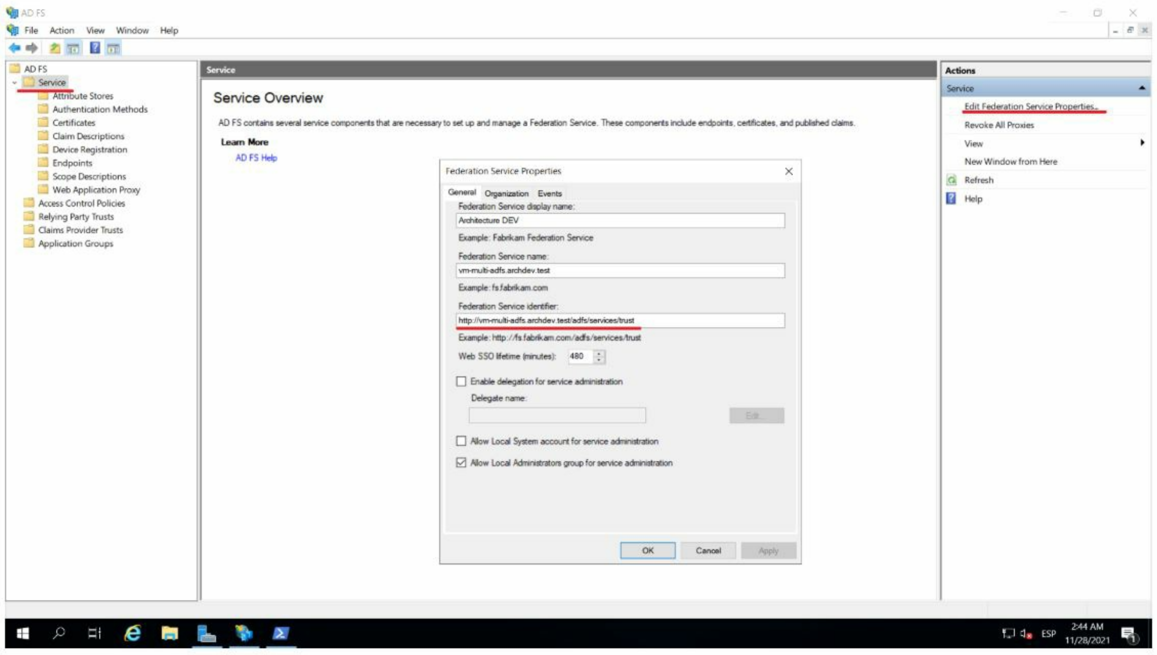
2. The login URL can be obtained directly from the ADFS server by opening the console **AD FS Management**, in the main menu by selecting the **Service** and **Endpoints**.

> ⚐ **Note:** Login URL: In a default installation, its value corresponds to https://**/adfs/ls/.



Endpoints

Enabled	Proxy Enabled	URL Path	Type	Authentication Type	Security Mode
Token Issuance					
Yes	Yes	/adfs/ls/	SAML 2.0/WS-Federation	Anonymous	Transport
Yes	Yes	/adfs/oauth2/	OAuth	Anonymous	Transport
Yes	Yes	/adfs/oauth2/deviceauth	OAuth Device Flow	Anonymous	Transport
No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	Certificate	Message
Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	Certificate	Mixed
No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3	Certificate	Transport
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256	WS-Trust 1.3	SAML Token (Asym...	Message
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256sha2...	WS-Trust 1.3	SAML Token (Asym...	Message
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic256	WS-Trust 1.3	SAML Token (Asym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic25...	WS-Trust 1.3	SAML Token (Asym...	Mixed
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256...	WS-Trust 1.3	SAML Token (Sym...	Mixed



Service Overview

AD FS contains several service components that are necessary to set up and manage a Federation Service. These components include endpoints, certificates, and published claims.

Learn More

AD FS Help

Federation Service Properties

Federation Service display name: Architecture DEV

Example: Fabrikam Federation Service

Federation Service name: vm-multi-adfs.archdev.test

Example: fs.fabrikam.com

Federation Service identifier: http://vm-multi-adfs.archdev.test/adfs/services/trust

Example: http://fs.fabrikam.com/adfs/services/trust

Web SSO lifetime (minutes): 480

☐ Enable delegation for service administration

Delegate name:

☐ Allow Local System account for service administration

☑ Allow Local Administrators group for service administration

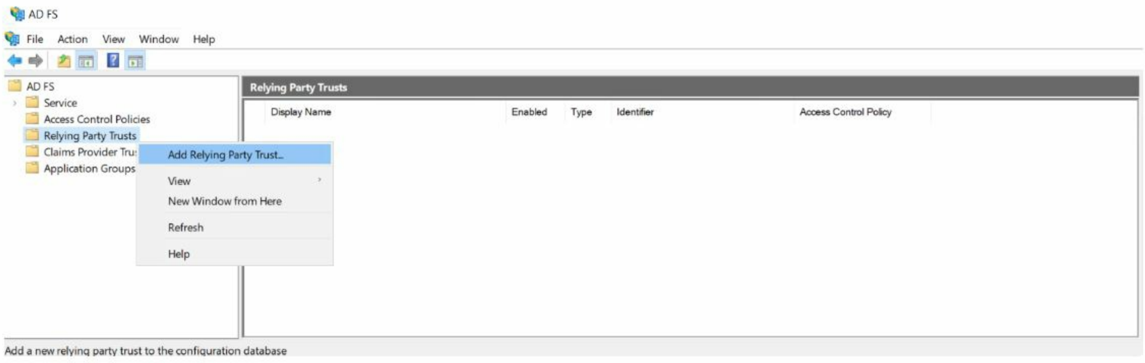
⚐ **Note:** Logout URL: In a default installation its value corresponds to https://**/adfs/ls/?wa=wsignout1.0

You can do the same to get the login URL and add the value ?wa=wsignout1.0 to it

This data must be entered when creating an external authentication provider in the admin console. See External Authentication configuration.

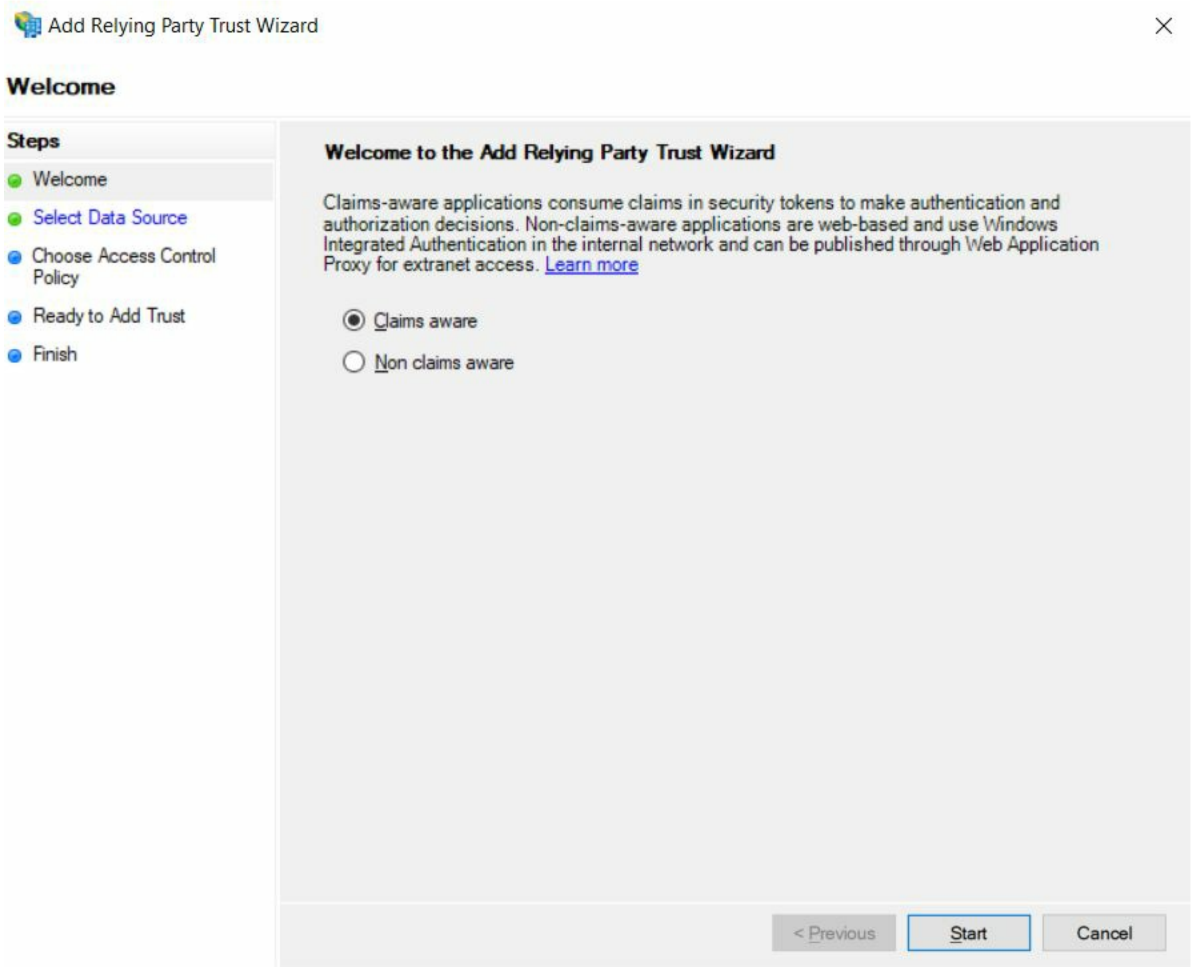
Configuring the trust relationship

1. Start the console **AD FS Management** from the server where the ADFS is installed, right-click on the**Relying Party Trusts**Select **Add Relying Party Trust...**



Add a new relying party trust to the configuration database

2. Select **Claims aware** and click **Start**.



Welcome

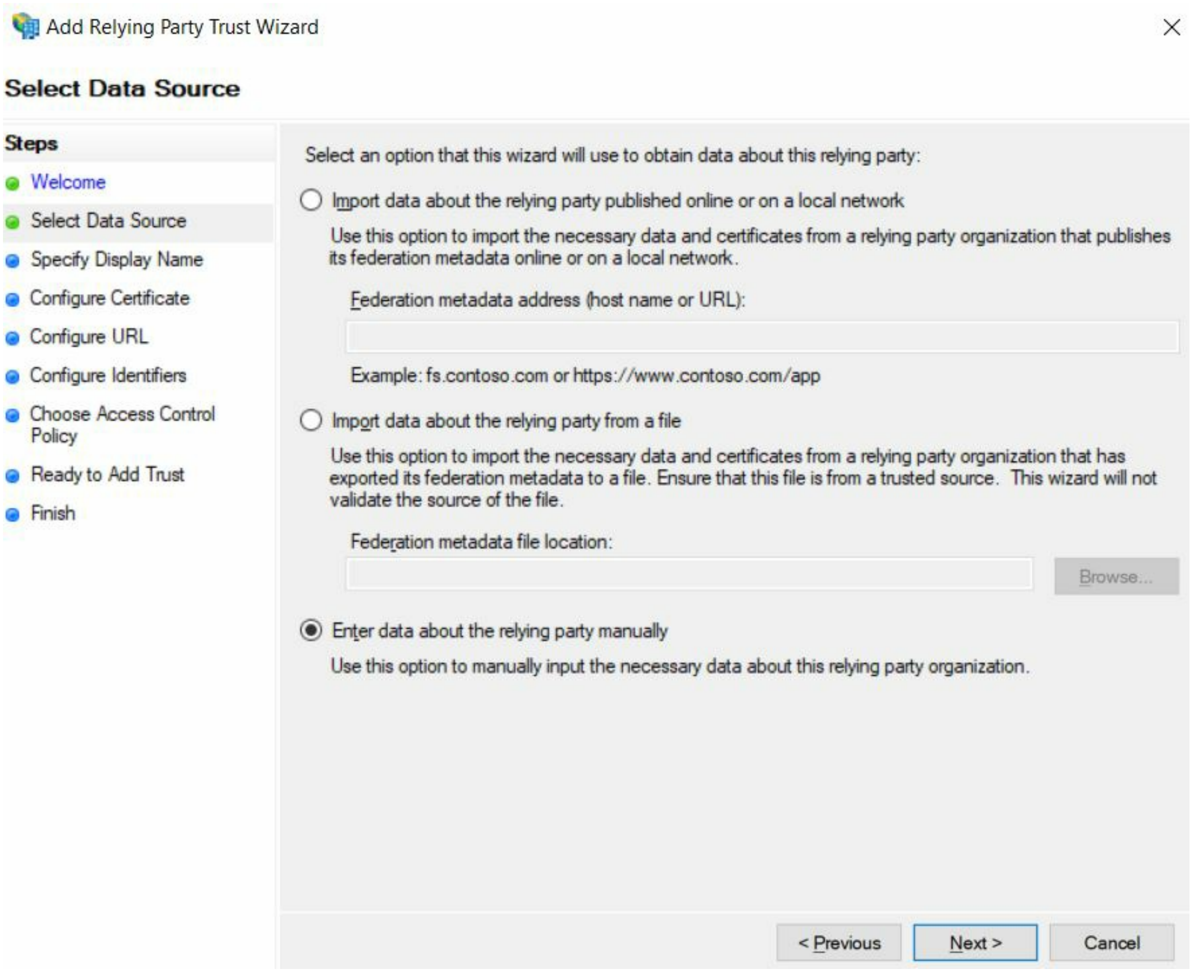
Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

3. Select **Enter data about relying party manually**, then in **Next**.



Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

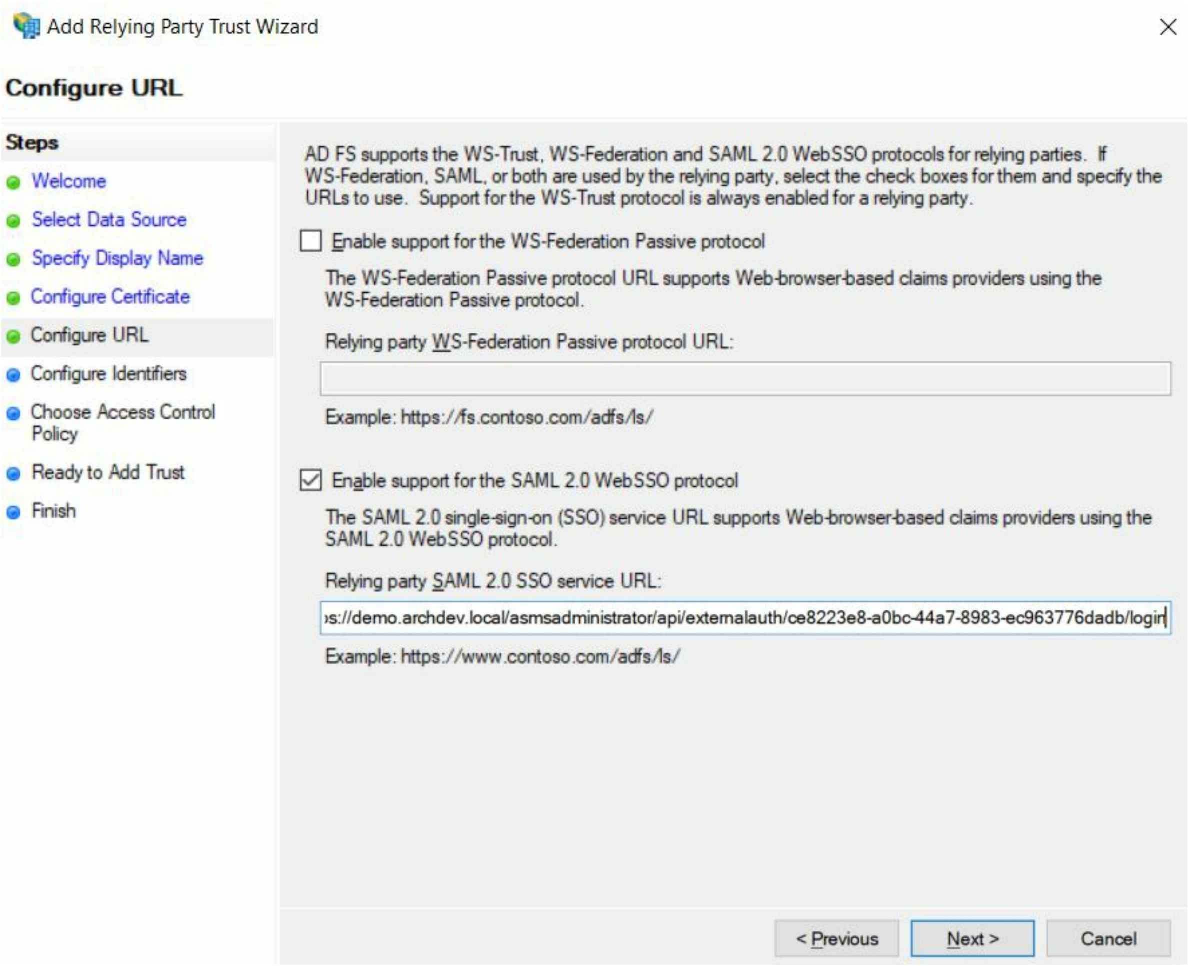
Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

4. Enter a descriptive name and record the additional information. Click**Next**. 5. You can click **Next** In El Paso **Configure certificate** to leave the defaults.

6. Select **Enable support for the SAML 2.0 WebSSO protocol** and enter the console sign-in URL, click **Next**



Add Relying Party Trust Wizard

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

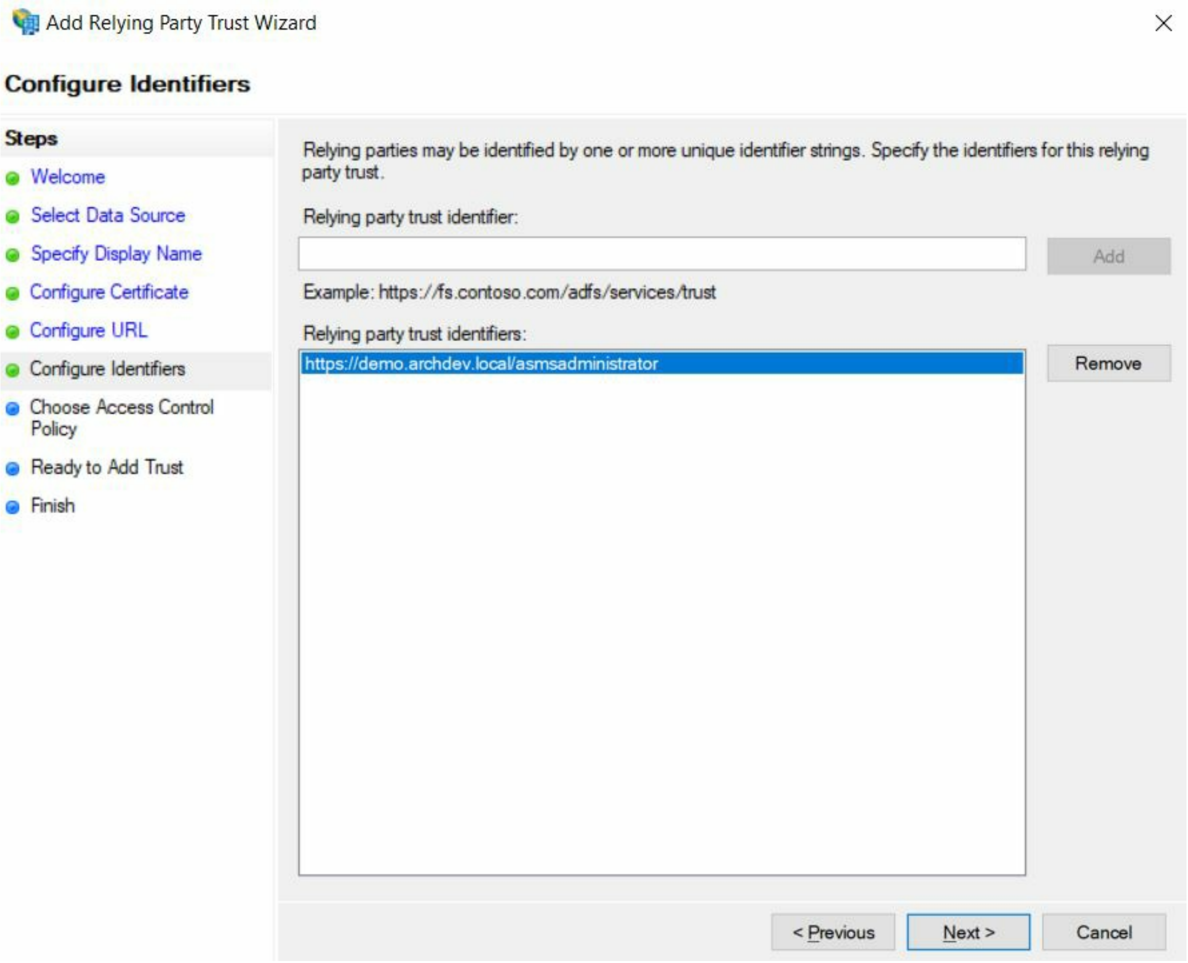
The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

›s://demo.archdev.local/asmsadministrator/api/externalauth/ce8223e8-a0bc-44a7-8983-ec963776dadb/login

Example: https://www.contoso.com/adfs/ls/

7. Enter the console URL, click **Add** and later in **Next**.



Add Relying Party Trust Wizard

Configure Identifiers

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

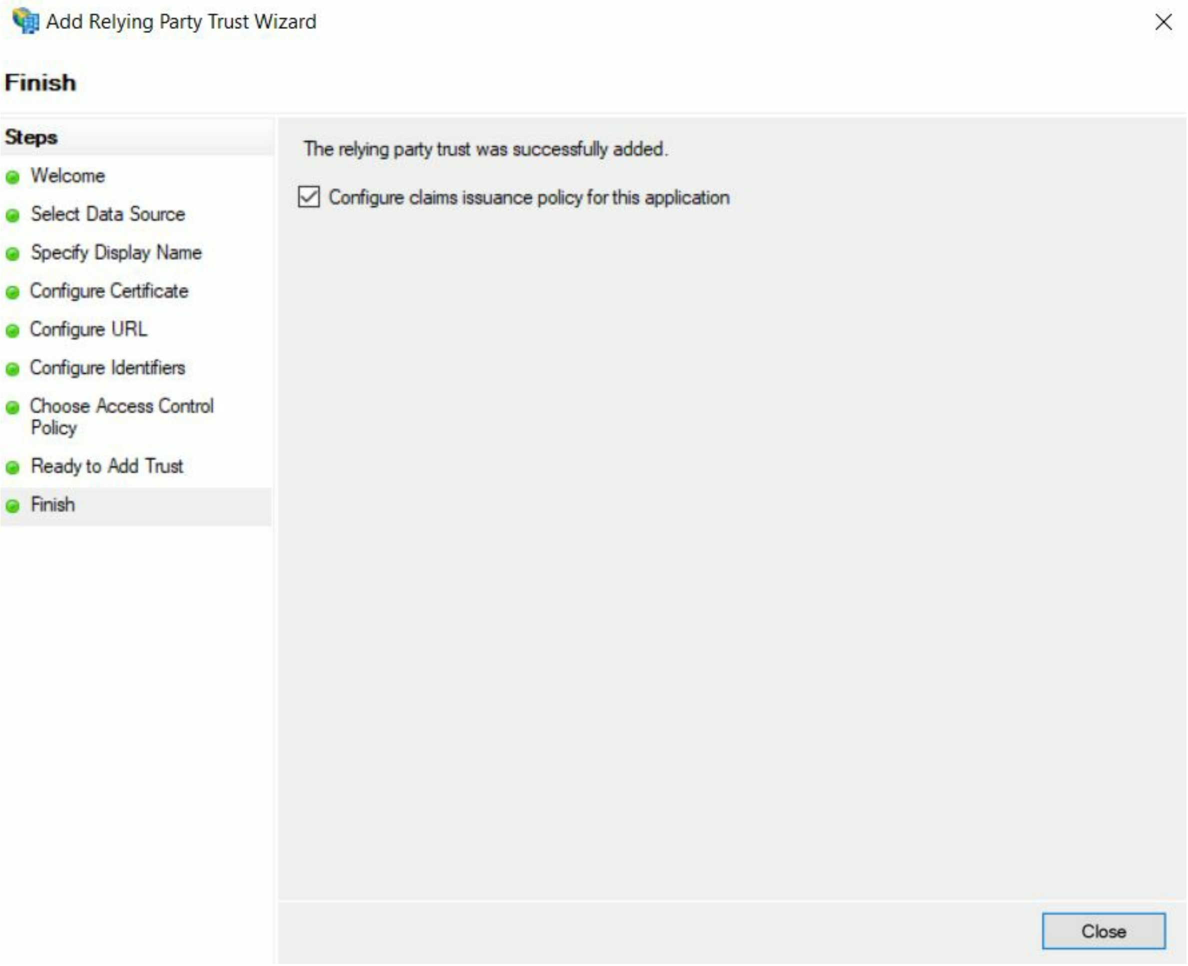
Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:
https://demo.archdev.local/asmsadministrator

8. Select the type of access policy to be applied, based on your security requirements, click **Next**. 9. You can view the summary of the click settings on **Next**.

10. Verify that the option is selected **configure claims issuance policy for this application** to configure the policies for the issuance of claims to be used for the integration; Click **Close** to complete the wizard.



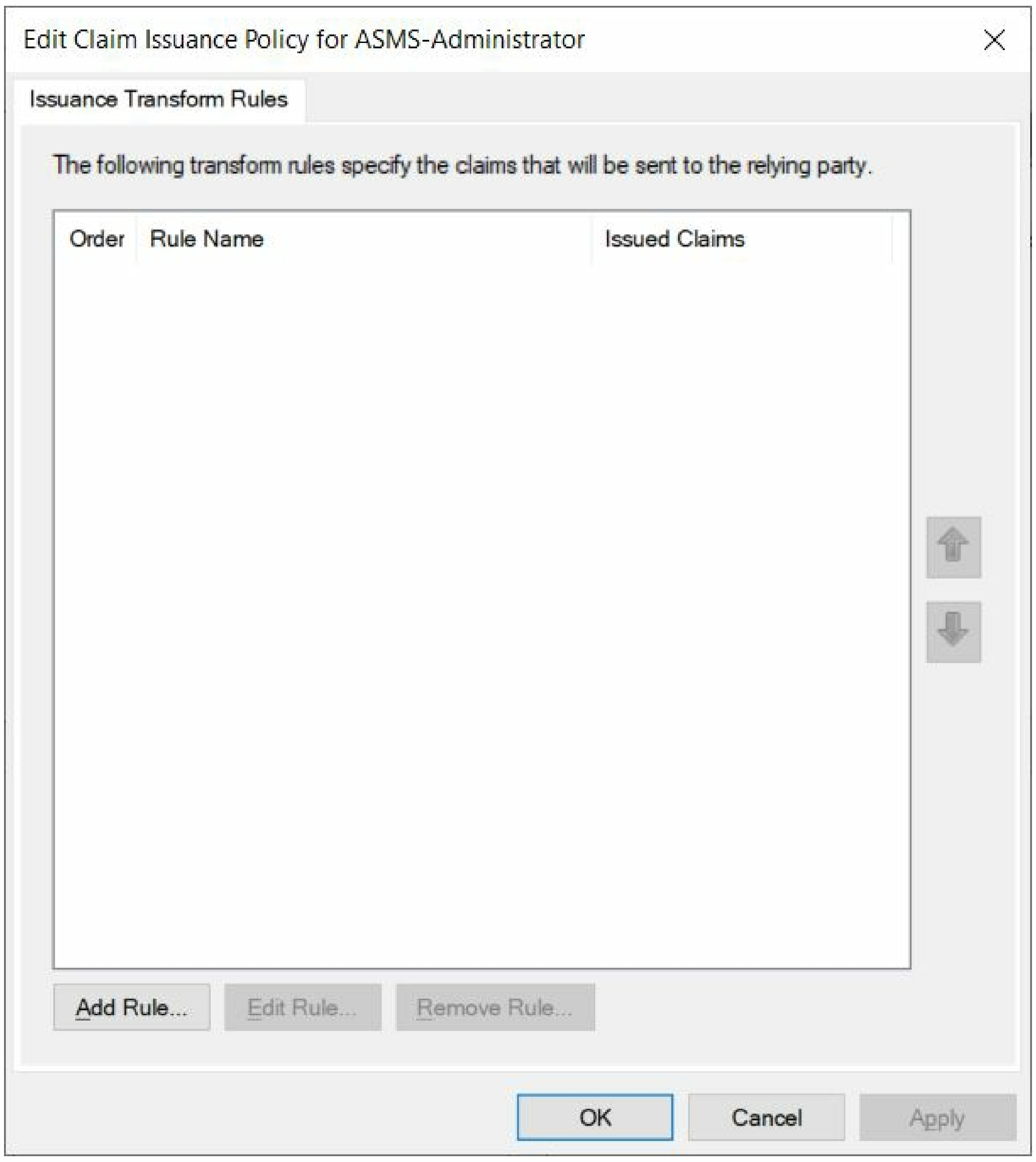
Add Relying Party Trust Wizard

Finish

The relying party trust was successfully added.

☑ Configure claims issuance policy for this application

11. You will then find a new window to configure the policies, click **Add Rule**.

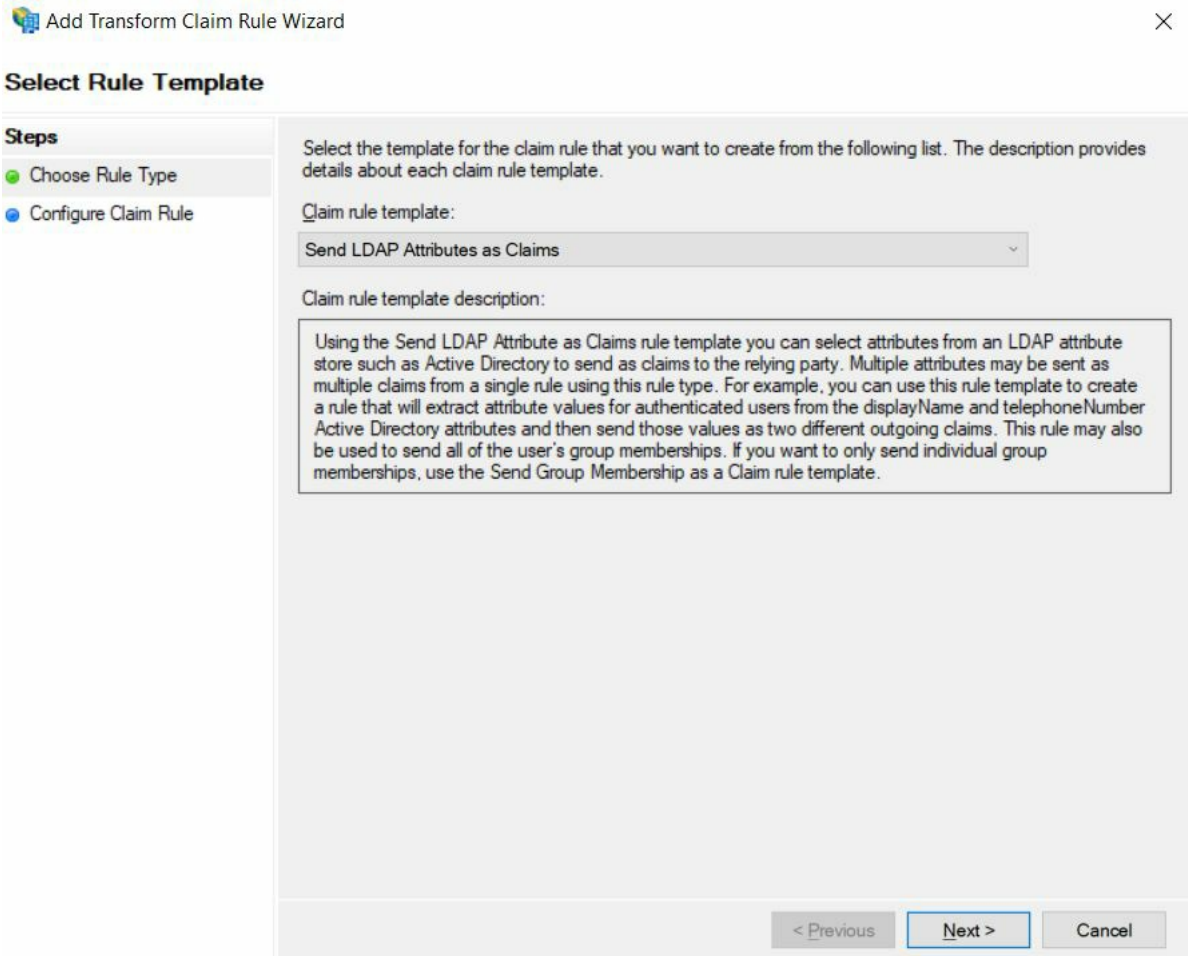


Edit Claim Issuance Policy for ASMS-Administrator

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

12. Select the template Send LDAP attributes as Claims, click Next.



Add Transform Claim Rule Wizard

Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

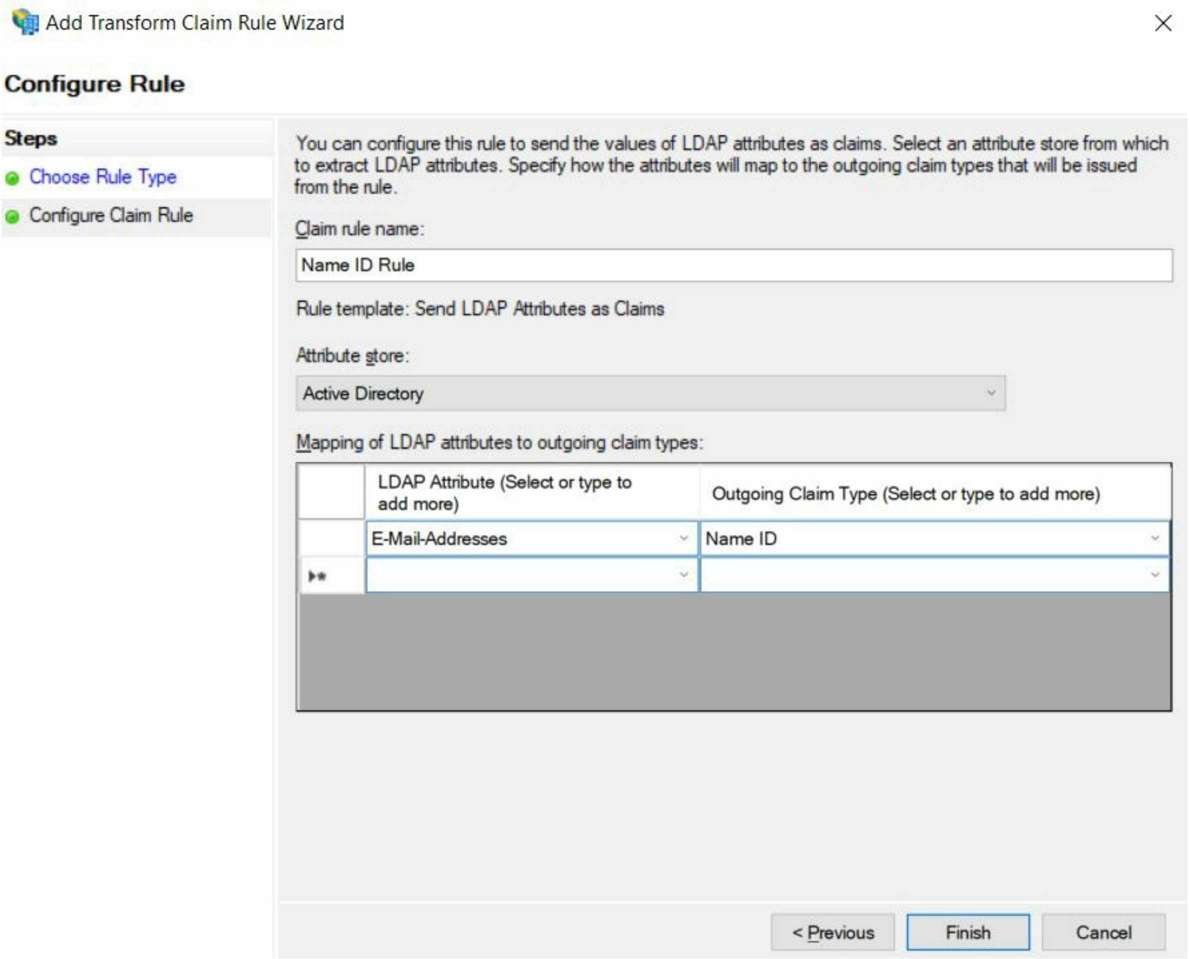
Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

13. Enter a name to the rule, select Active Directory in the Attribute store, on the left side of the table, select E-Mail-Addresses and on the right side select Name ID; Finish the rule creation by clicking the Finish.

> ⚐ Note: On the left side of the table you can change E-Mail-Addresses, for the field that is mapped as UserName on importing users in LDAP



Add Transform Claim Rule Wizard

Configure Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Name ID Rule

Rule template: Send LDAP Attributes as Claims

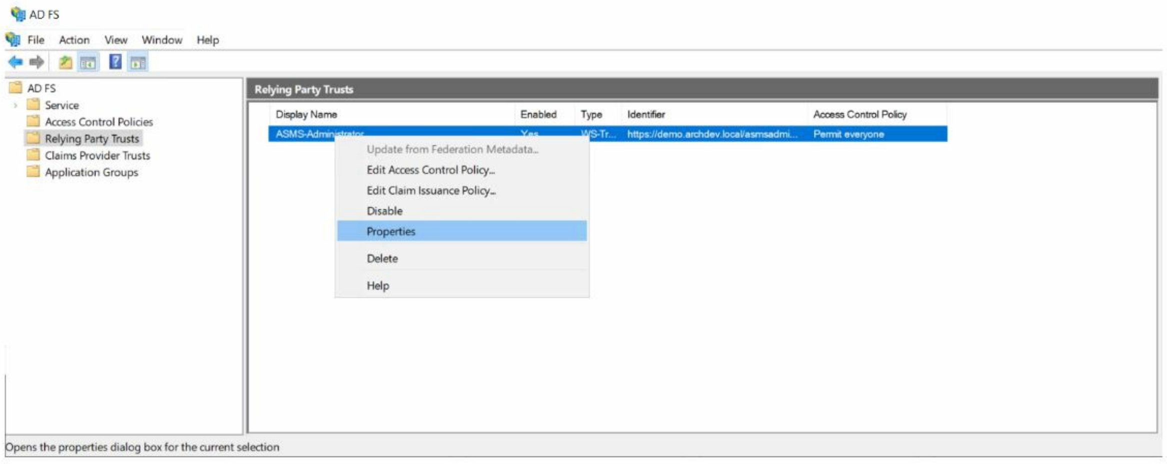
Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	E-Mail-Addresses	Name ID
▸*		

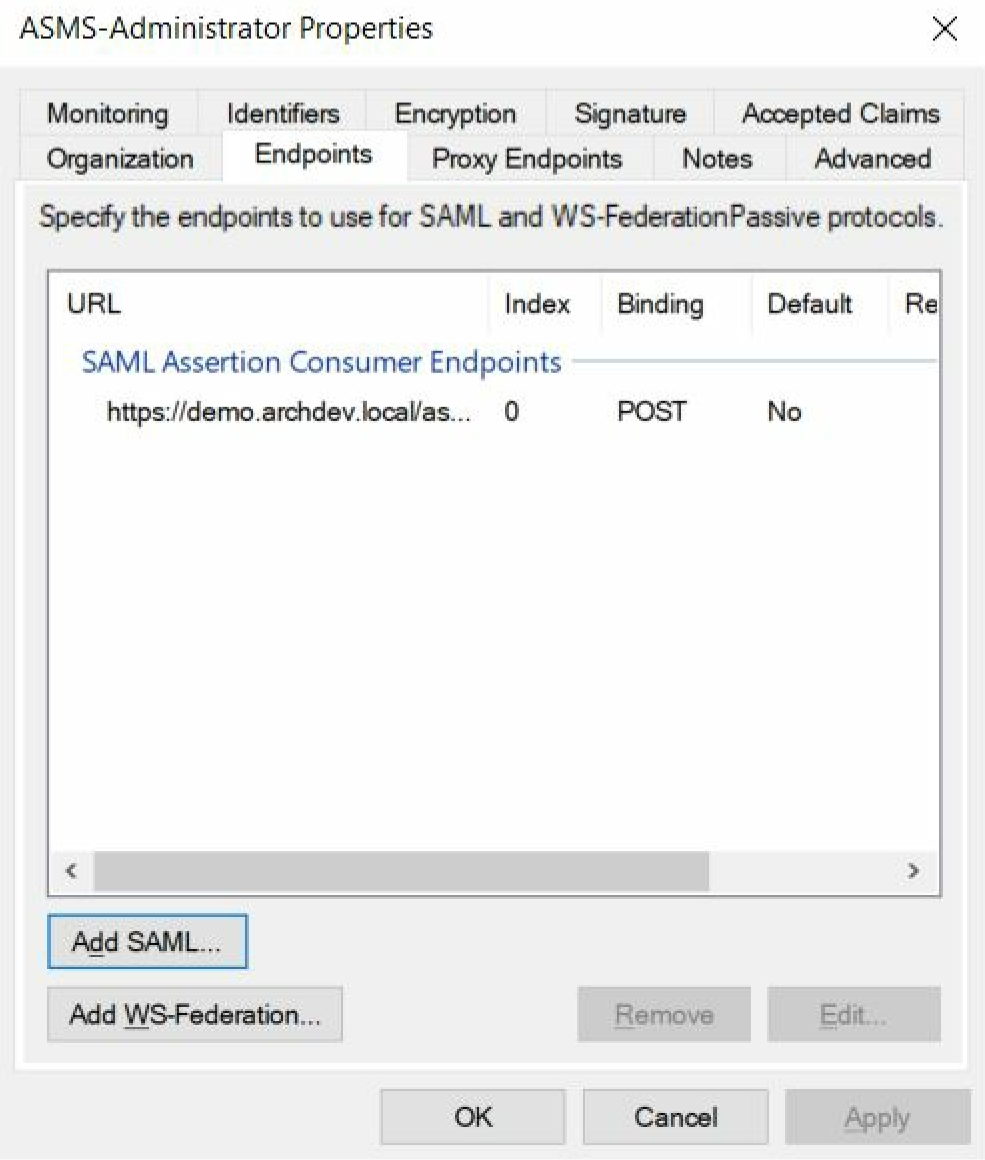
14. To complete the Policy Editing Wizard, click the **OK**. 15. To add the console logoff address, edit the provider created in the ADFS, do **right-click on the provider's name** in the **properties**. You can also do this by choosing the name of the provider and left-clicking on it.



Display Name	Enabled	Type	Identifier	Access Control Policy
ASMS-Administrator	Yes	WS-Tr...	https://demo.archdev.local/asmsadmi...	Permit everyone

Opens the properties dialog box for the current selection

16. Select the tab option **Endpoints** and click the **Add SAML....*

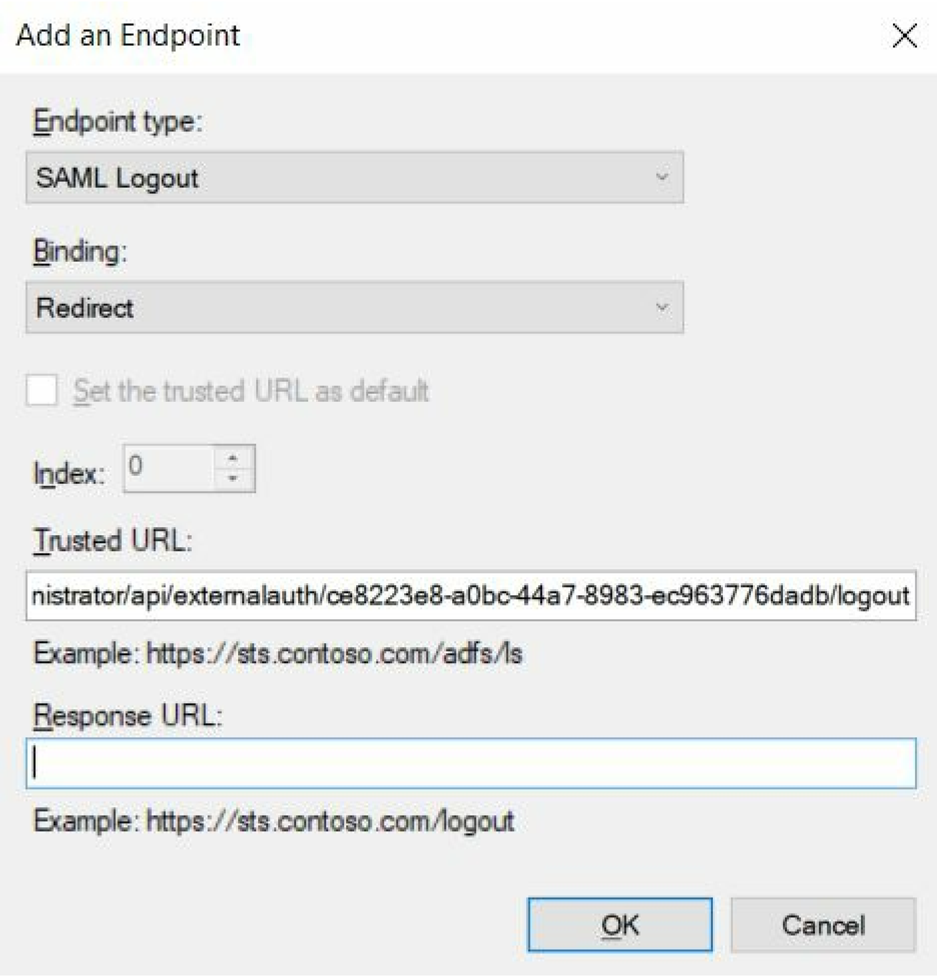


ASMS-Administrator Properties

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://demo.archdev.local/as...	0	POST	No	

17. Select SAML Logout in the Endpoint Type later Redirect in the Binding and finally enter the URL of the corresponding console logout.



Endpoint type: SAML Logout

Binding: Redirect

□ Set the trusted URL as default

Index: 0

Trusted URL: nistrator/api/externalauth/ce8223e8-a0bc-44a7-8983-ec963776dadb/logout

Example: https://sts.contoso.com/adfs/ls

Response URL:

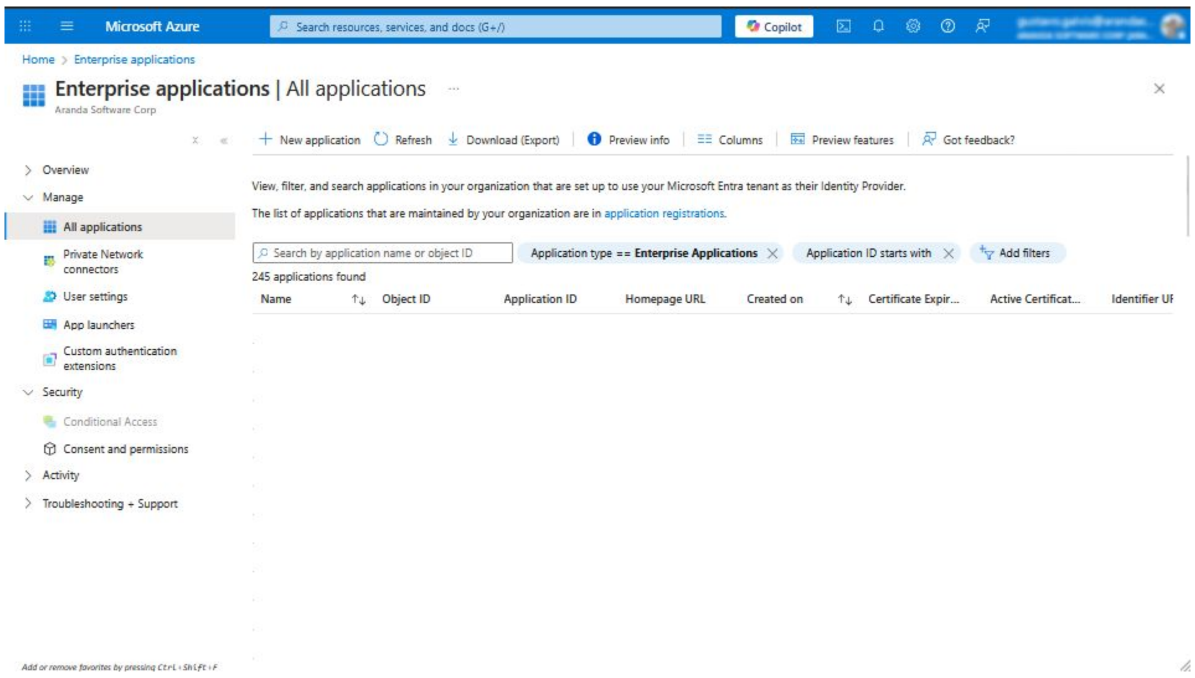
Example: https://sts.contoso.com/logout

18. Click the OK button and close the properties window, click theOK.

Azure Active Directory configuration

Get supplier data

1. First, create an enterprise application through the Azure portal.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Enterprise applications
Enterprise applications | All applications
Aranda Software Corp
New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?
Overview
Manage
All applications
Private Network connectors
User settings
App launchers
Custom authentication extensions
Security
Conditional Access
Consent and permissions
Activity
Troubleshooting + Support
Add or remove favorites by pressing Ctrl+Shift+F

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

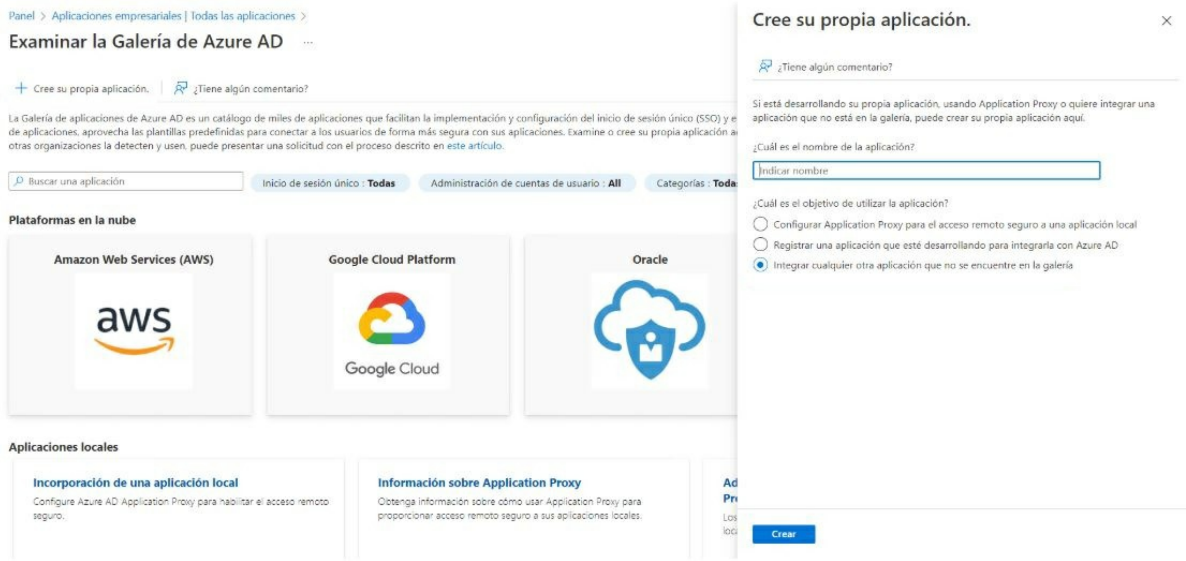
The list of applications that are maintained by your organization are in application registrations.

Search by application name or object ID | Application type == Enterprise Applications | Application ID starts with | Add filters

245 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expir...	Active Certificat...	Identifier UF

2. Select the option Create your own app and in the window that you enable, enter a name for the app and verify that the option is enabled Integrate any other application that is not in the gallery; then click theCreate. Wait a moment while the app is created.


Panel > Aplicaciones empresariales | Todas las aplicaciones >
+ Cree su propia aplicación.
¿Tiene algún comentario?
Buscar una aplicación
Inicio de sesión único : Todas
Administración de cuentas de usuario : All
Categorías : Toda
Amazon Web Services (AWS)
aws
Google Cloud Platform
Google Cloud
Oracle
Crear

Examinar la Galería de Azure AD

La Galería de aplicaciones de Azure AD es un catálogo de miles de aplicaciones que facilitan la implementación y configuración del inicio de sesión único (SSO) y e de aplicaciones, aprovecha las plantillas predefinidas para conectar a los usuarios de forma más segura con sus aplicaciones. Examine o cree su propia aplicación a otras organizaciones la detecten y usen, puede presentar una solicitud con el proceso descrito en este artículo.

Plataformas en la nube

Aplicaciones locales

Incorporación de una aplicación local
Configure Azure AD Application Proxy para habilitar el acceso remoto seguro.

Información sobre Application Proxy
Obtenga información sobre cómo usar Application Proxy para proporcionar acceso remoto seguro a sus aplicaciones locales.

Cree su propia aplicación.

Si está desarrollando su propia aplicación, usando Application Proxy o quiere integrar una aplicación que no está en la galeria, puede crear su propia aplicación aquí.

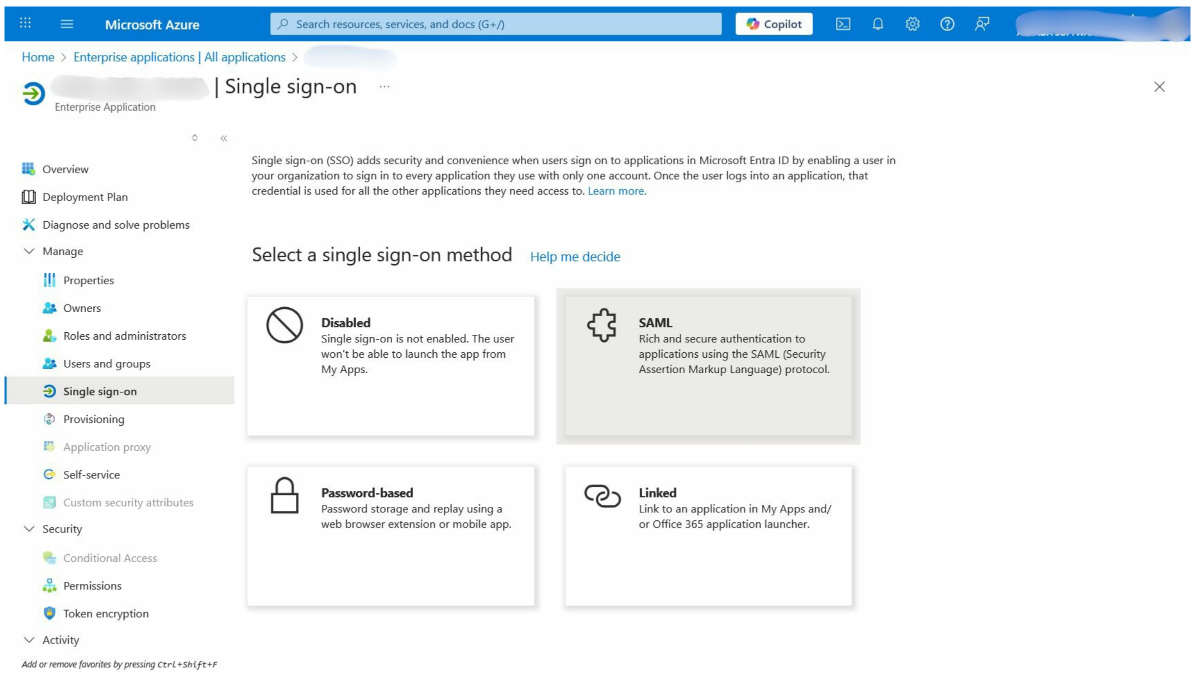
¿Cuál es el nombre de la aplicación?

Indicar nombre

¿Cuál es el objetivo de utilizar la aplicación?

○ Configurar Application Proxy para el acceso remoto seguro a una aplicación local
○ Registrar una aplicación que esté desarrollando para integrarla con Azure AD
● Integrar cualquier otra aplicación que no se encuentre en la galería

3. After creating the app, select the **Single sign-on**, then select **SAML** as a single sign-on method.



[redacted] | Single sign-on

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method Help me decide

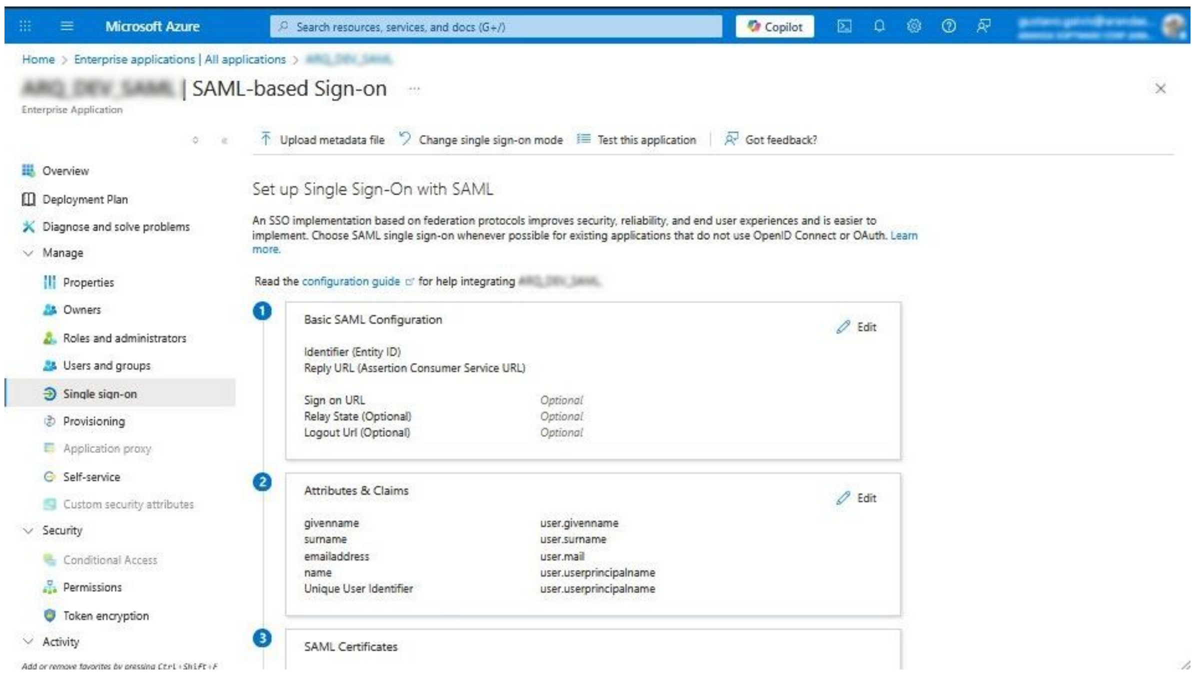
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/ or Office 365 application launcher.

4. On the page **Configuring Single Sign-On with SAML**icon, click the **Pencil** SAML Basic Settings to edit the settings.



[redacted] | SAML-based Sign-on

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating [redacted]

1 Basic SAML Configuration

Identifier (Entity ID)	
Reply URL (Assertion Consumer Service URL)	
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

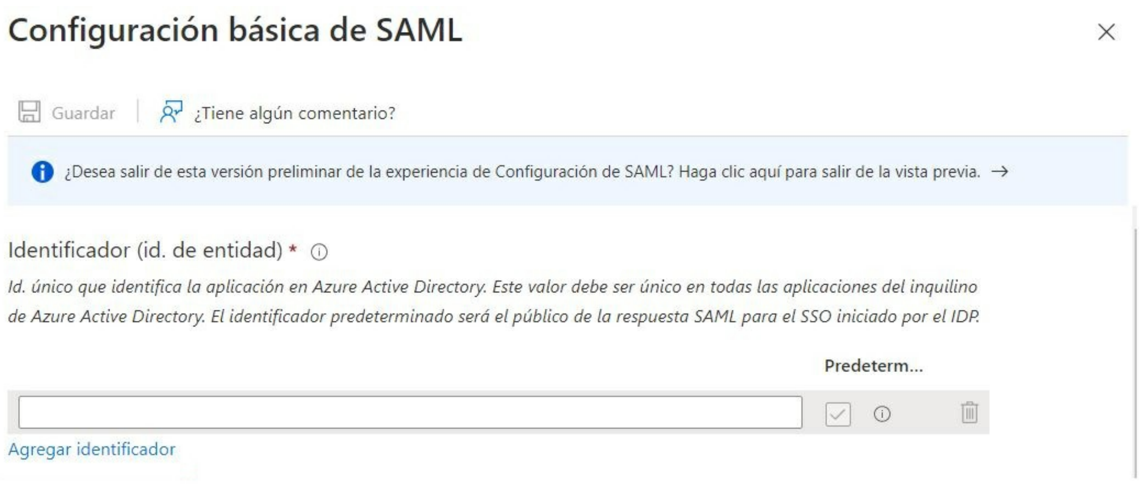
2 Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

5. In the **Basic SAML Configuration**, follow these steps:

- Add an identifier and type the **Console URL**.



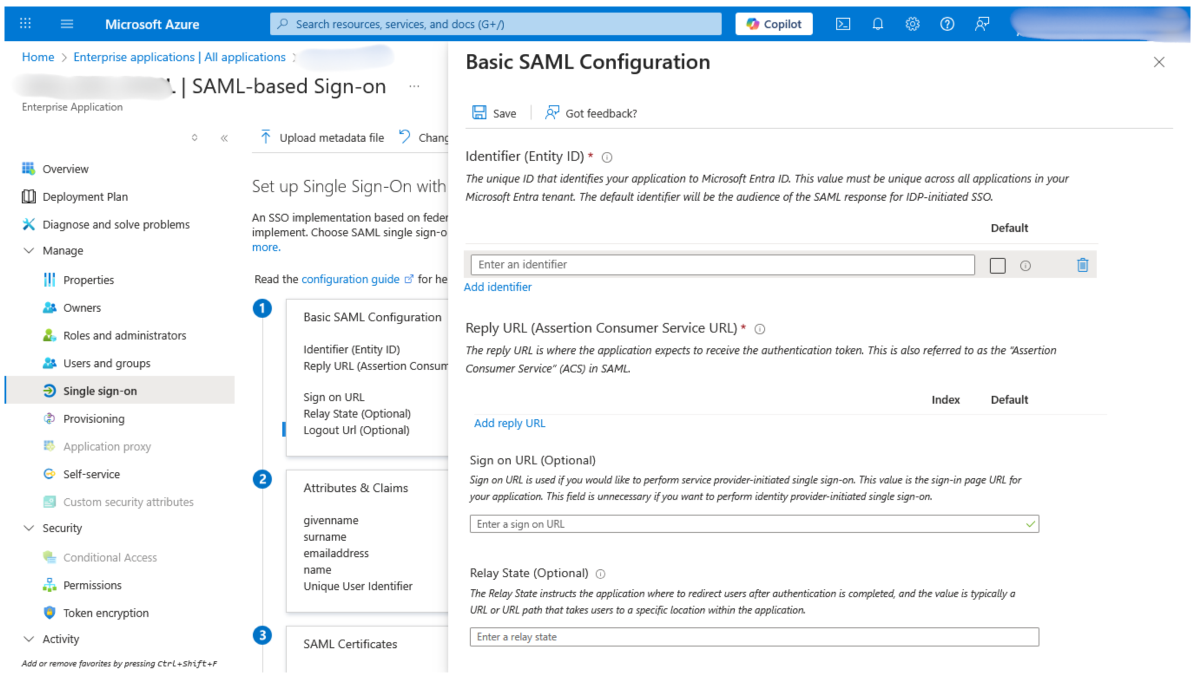
Configuración básica de SAML

¿Desea salir de esta versión preliminar de la experiencia de Configuración de SAML? Haga clic aquí para salir de la vista previa. →

Identificador (id. de entidad) *

Id. único que identifica la aplicación en Azure Active Directory. Este valor debe ser único en todas las aplicaciones del inquilino de Azure Active Directory. El identificador predeterminado será el público de la respuesta SAML para el SSO iniciado por el IDP.

- Subsequently, add a **Reply URL** and type in the text box the **Login URL** of the console.



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

Enter an identifier

Add identifier

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

Add reply URL

Sign on URL (Optional)

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.

Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

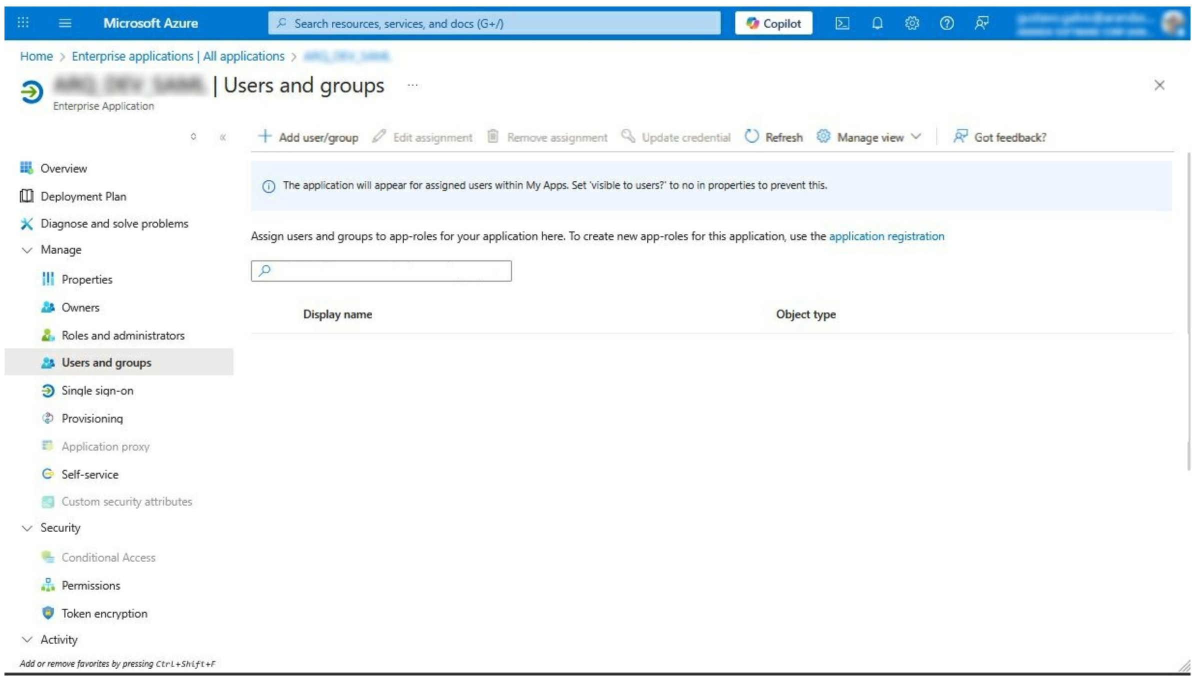
- Finish the setup by selecting the **Save**.

> ⚐ **Note:** You can now copy the following values, for later use in this section

- **Login URL**: Corresponds to the field **Login URL** in the external authentication settings of the Admin console.
- **Azure AD ID**: Corresponds to the field **Identity Identifier** in the external authentication settings of the Admin console.
- **Logout URL**: Use the following address: https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0

User permissions that can access the application

Remember to grant permissions to users who can access through the **Users and groups**.



The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

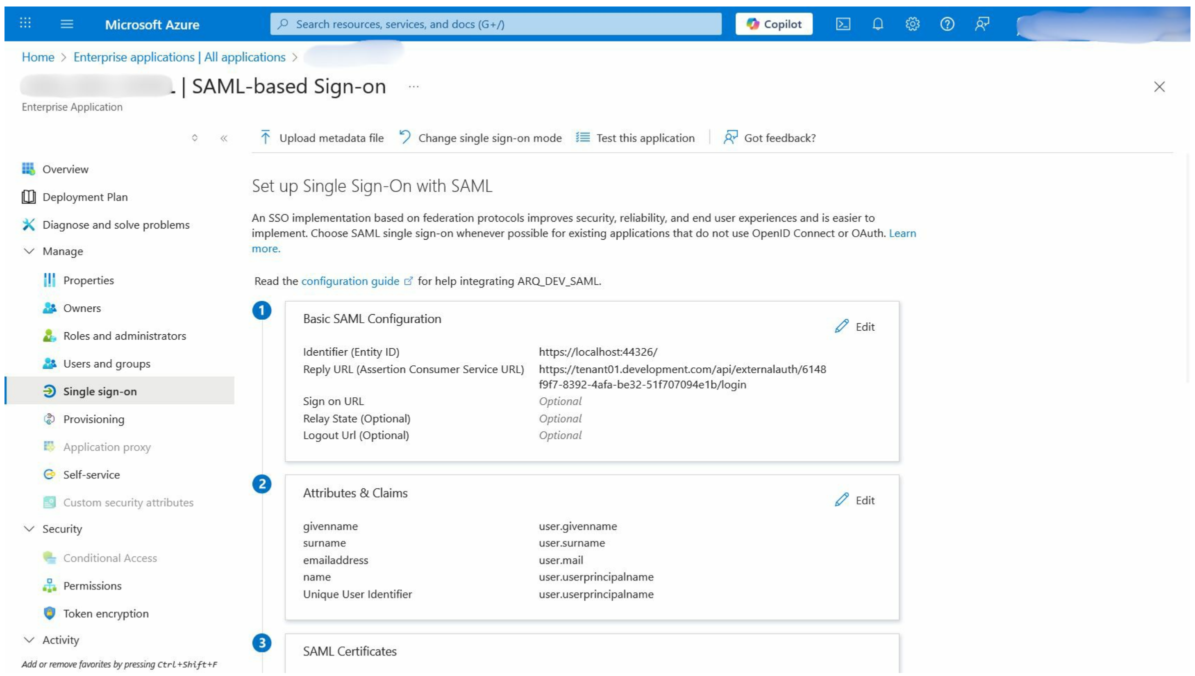
Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration

Display name	Object type

Claims Validation

At the time of login, the **claim Unique User Identifier (Name ID)** with the field that is mapped as **UserName** on importing users in Microsoft EntraId. To do this, you can change the claim if necessary as follows:

1. Enter the option **Attributes & Claims**



[redacted] | SAML-based Sign-on

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating ARQ_DEV_SAML.

1 Basic SAML Configuration

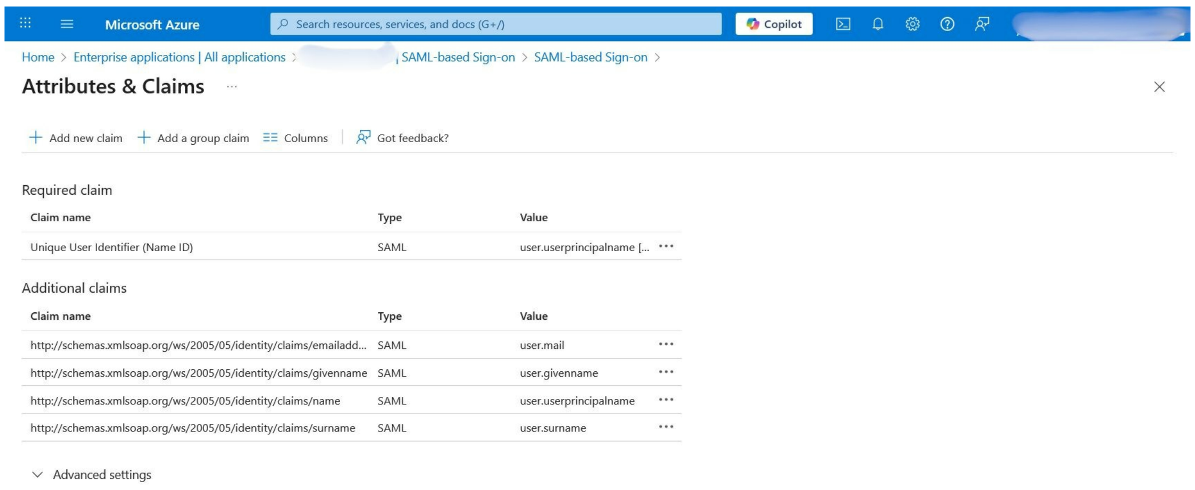
Identifier (Entity ID) https://localhost:44326/
Reply URL (Assertion Consumer Service URL) https://tenant01.development.com/api/externalauth/6148f9f7-8392-4afa-be32-51f707094e1b/login
Sign on URL *Optional*
Relay State (Optional) *Optional*
Logout Url (Optional) *Optional*

2 Attributes & Claims

givenname user.givenname
surname user.surname
emailaddress user.mail
name user.userprincipalname
Unique User Identifier user.userprincipalname

3 SAML Certificates

2. Click on **Unique User Identifier (Name ID)**


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Enterprise applications | All applications > | SAML-based Sign-on > SAML-based Sign-on >
Add new claim
Add a group claim
Columns
Got feedback?
Advanced settings

Attributes & Claims

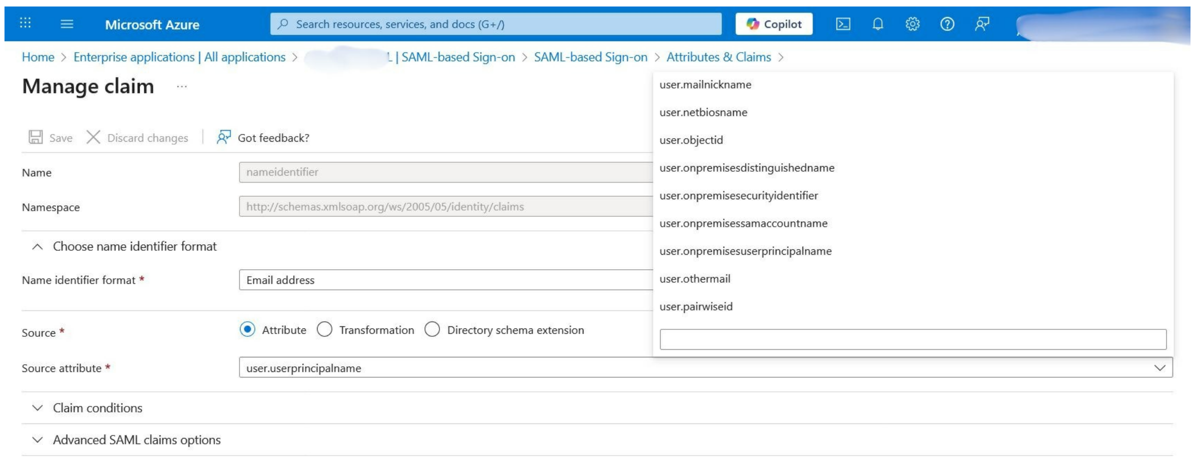
Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

3. And in the countryside **Source attribute** change it to the claim that is mapped as **UserName**


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Enterprise applications | All applications > | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >
Save
Discard changes
Got feedback?
Choose name identifier format
Claim conditions
Advanced SAML claims options
user.mailnickname
user.netbiosname
user.objectid
user.onpremisesdistinguishedname
user.onpremisesecurityidentifier
user.onpremisessamaccountname
user.onpremisesuserprincipalname
user.othermail
user.pairwiseid

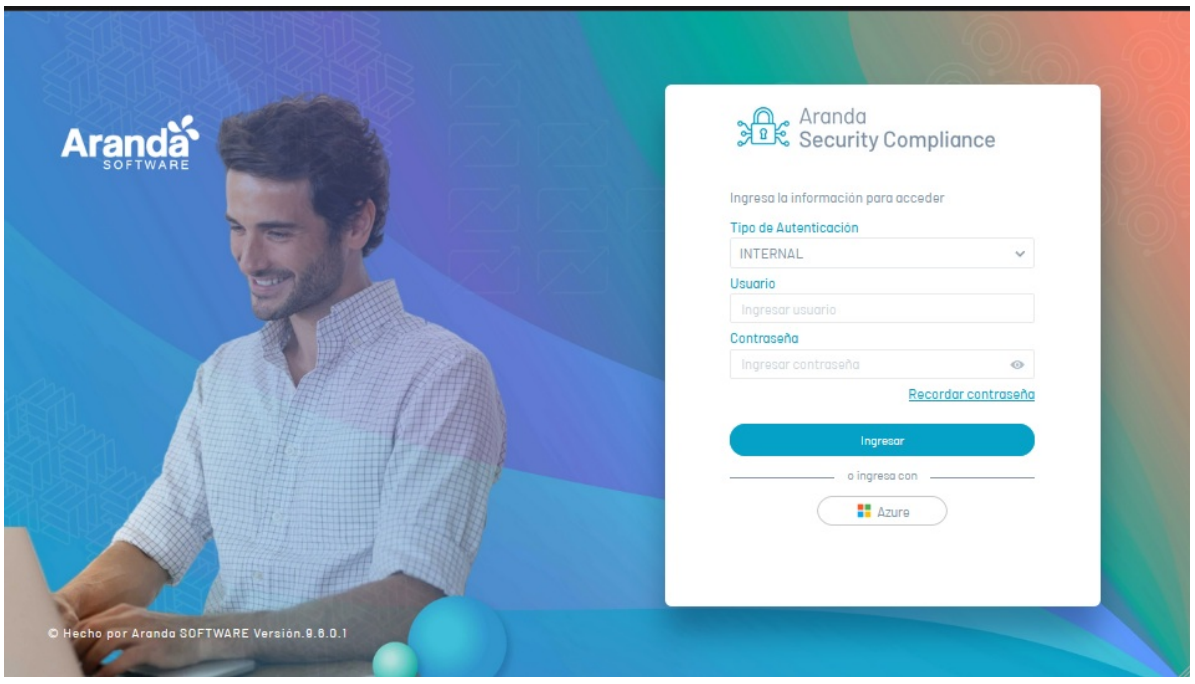
Manage claim

Name: nameidentifier
Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims
Name identifier format *: Email address
Source *: ● Attribute ○ Transformation ○ Directory schema extension
Source attribute *: user.userprincipalname

Login validation

> ⚐ **Note:** The user who logs in must be previously configured so that they can enter the corresponding console.

1. In the login window of the console that has been configured, you will find a button with the name of the configured provider at the bottom of the window.

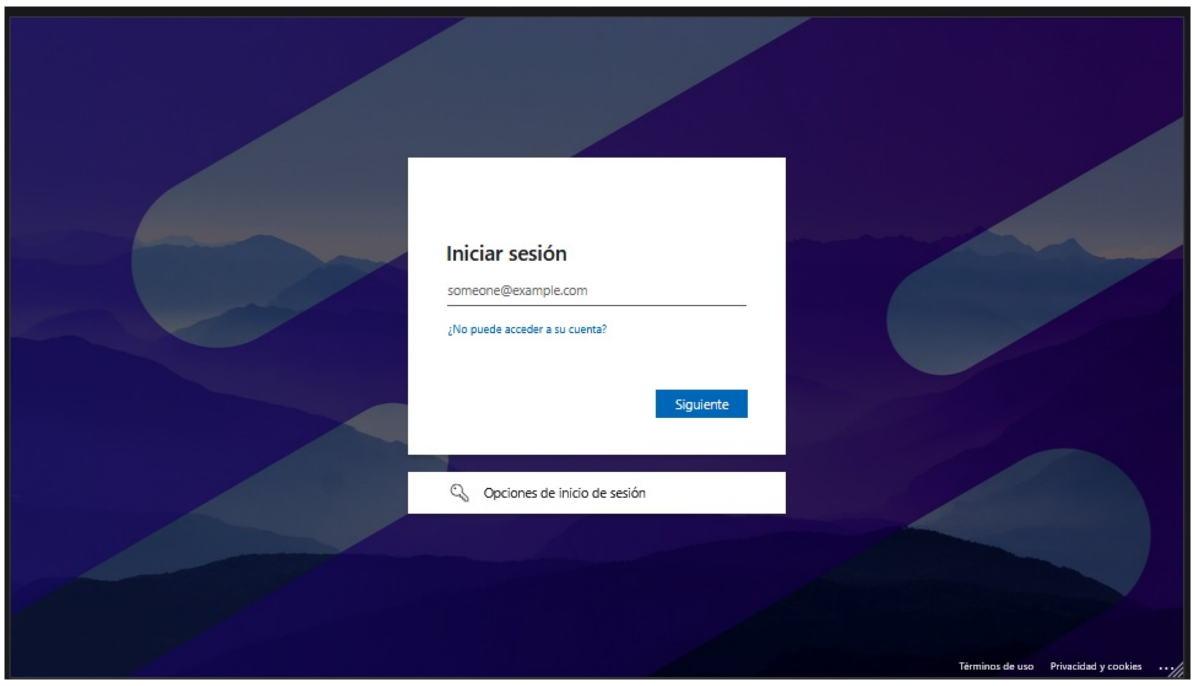

Aranda SOFTWARE
Aranda Security Compliance
Ingresa la información para acceder
Recordar contraseña
Ingresar
o ingresa con
Azure
© Hecho por Aranda SOFTWARE Versión.9.6.0.1

Tipo de Autenticación: INTERNAL

Usuario: Ingresar usuario

Contraseña: Ingresar contraseña

2. Clicking on the button redirects you to the authentication provider, where you can enter the corresponding login data.



3. Al finalizar el proceso de autenticación, se redireccionará automáticamente a la consola y podrá ver reflejado el usuario autenticado.

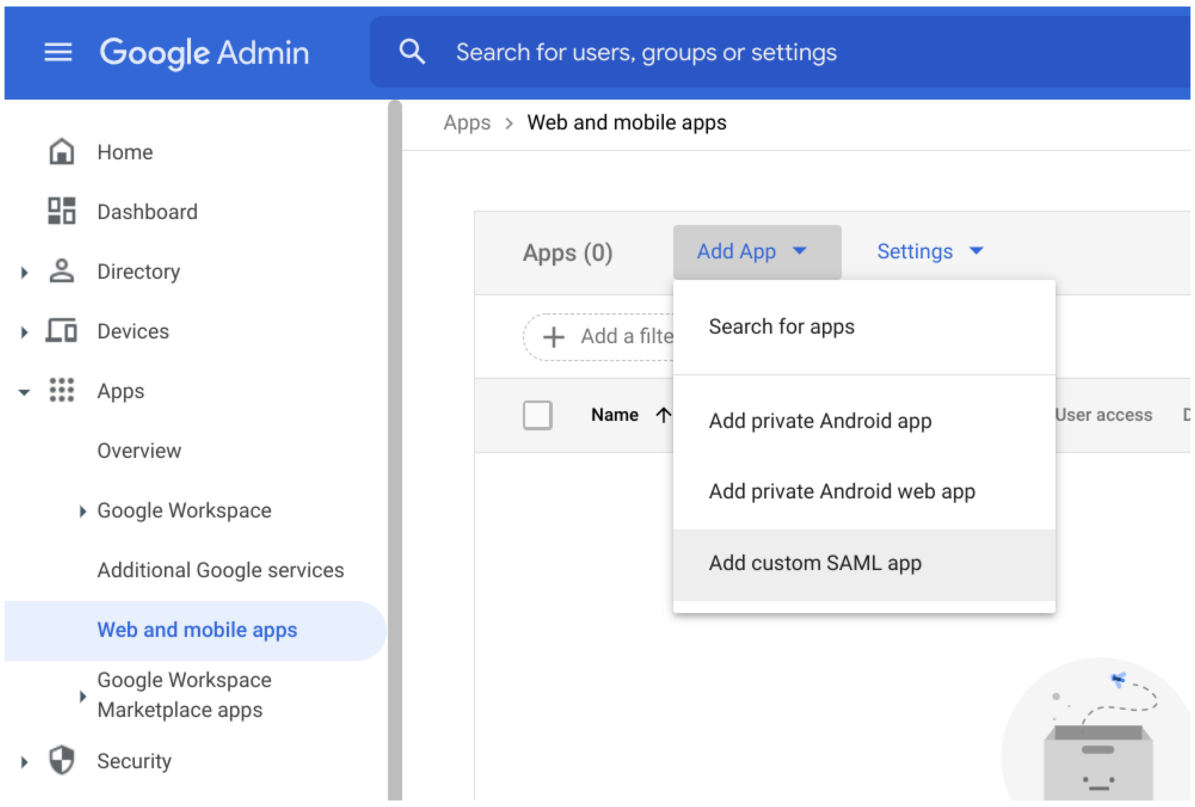
Google Settings

Set up Google Workspace

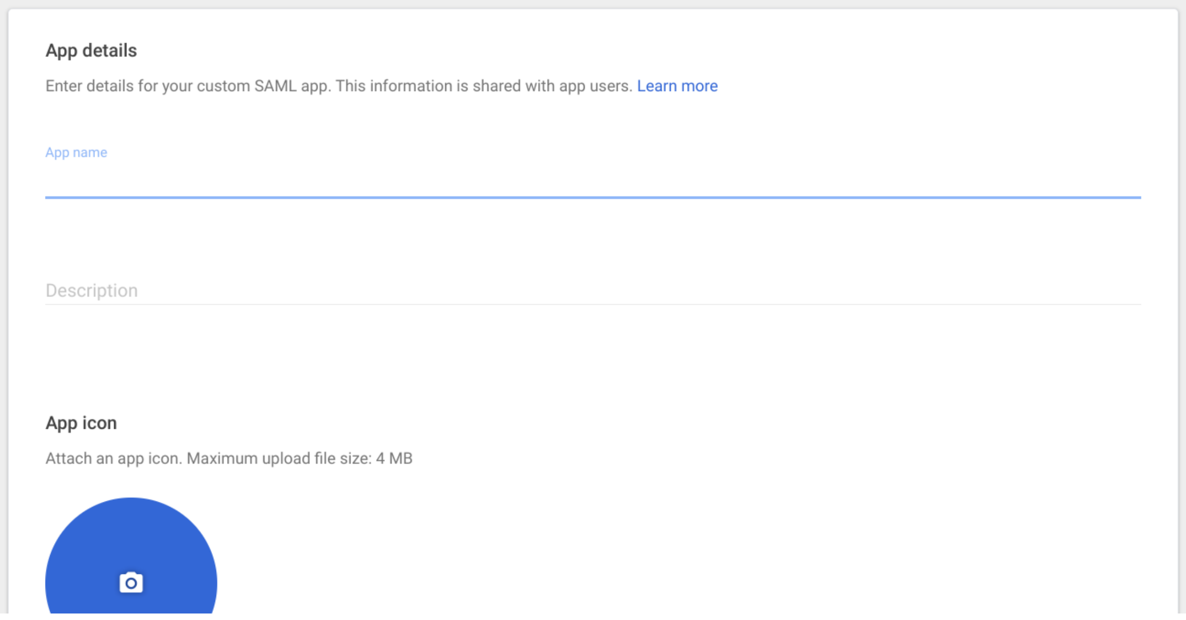
1. Log in to the Google Admin console

2. From the main menu select the *Apps* and *Web and mobile apps*

In the information view, click *Add App* and select the *Add custom SAML application.*



3. To set up app details, enter a name for the app and add a logo (optional). Then click *Continue*. Configure application details



App details

Enter details for your custom SAML app. This information is shared with app users. Learn more

App name

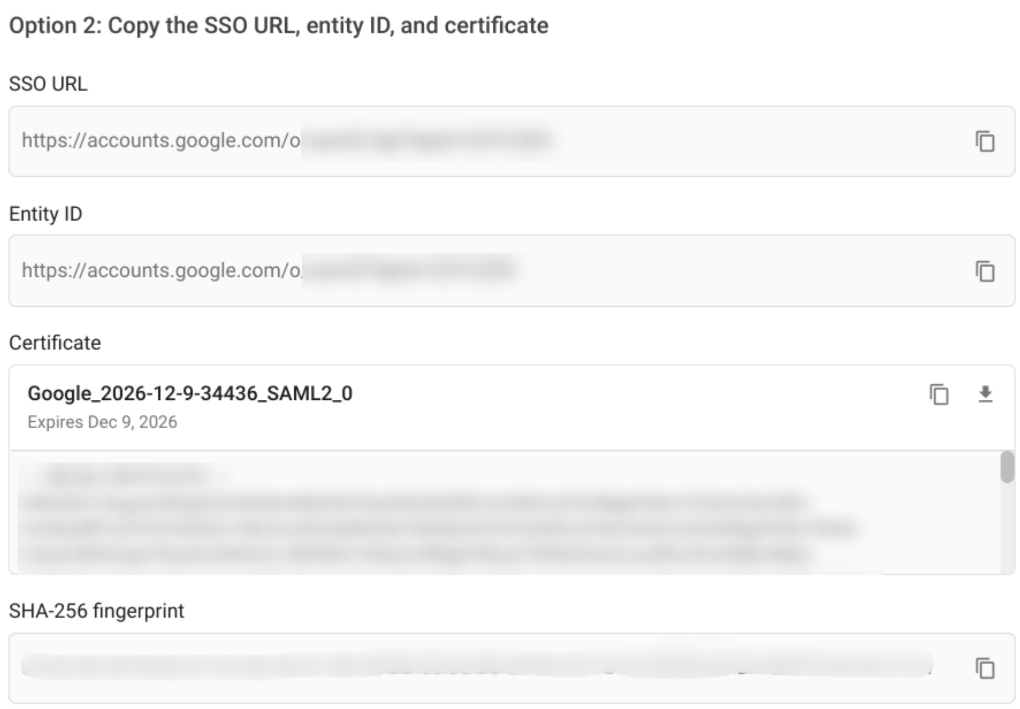
Description

App icon

Attach an app icon. Maximum upload file size: 4 MB

4. Identity provider data To define the identity provider data, copy the following values, for later use in this section

- URL de SSO: Corresponds to the field **Login URL** (right side of the form) in the external authentication settings of the Admin console.
- Entity ID: Corresponds to the field **Identity Identifier** in the external authentication settings of the Admin console.
- Google doesn't support single sign-on (SLO)



Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL

https://accounts.google.com/o[redacted]

Entity ID

https://accounts.google.com/o[redacted]

Certificate

Google_2026-12-9-34436_SAML2_0
Expires Dec 9, 2026

[redacted]

SHA-256 fingerprint

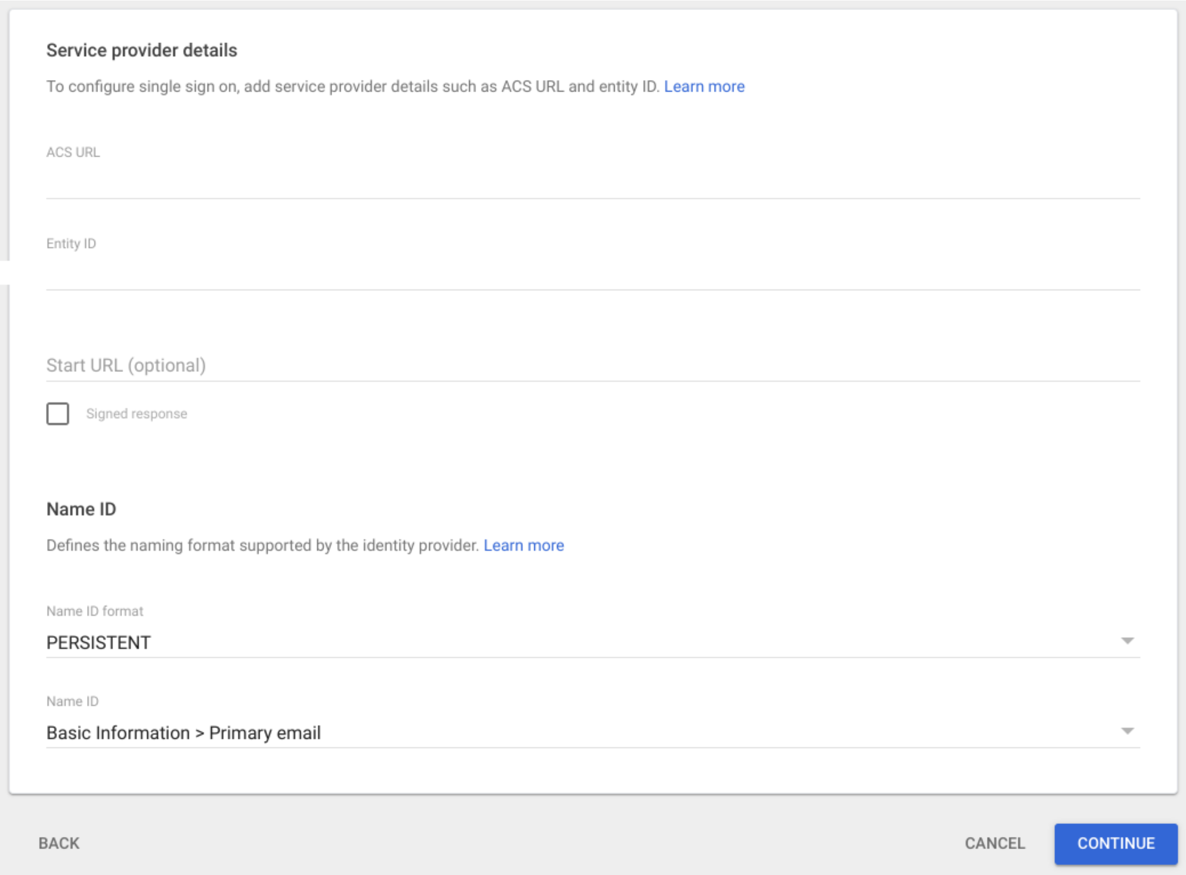
[redacted]

5. To configure service provider data, enter the values generated in this section

- URL de ACS: Enter the value of **Login Url** (left side of the form) in the external authentication settings of the

Admin console.

- **Entity ID:** Enter the value of **Console URL** in the external authentication settings of the Admin console.



Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. Learn more

ACS URL

Entity ID

Start URL (optional)

☐ Signed response

Name ID

Defines the naming format supported by the identity provider. Learn more

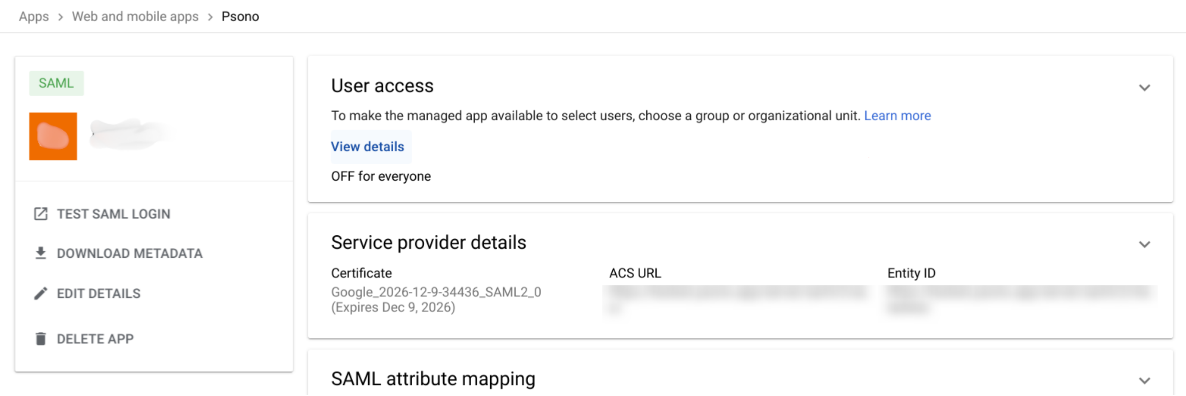
Name ID format: PERSISTENT

Name ID: Basic Information > Primary email

6. Set up User Access To configure *User Access* Select the users (or groups) who will be able to sign in with the app. Click on the

⌄

alongside *User Access* Configure the required attributes as shown below.



User access

To make the managed app available to select users, choose a group or organizational unit. Learn more

View details

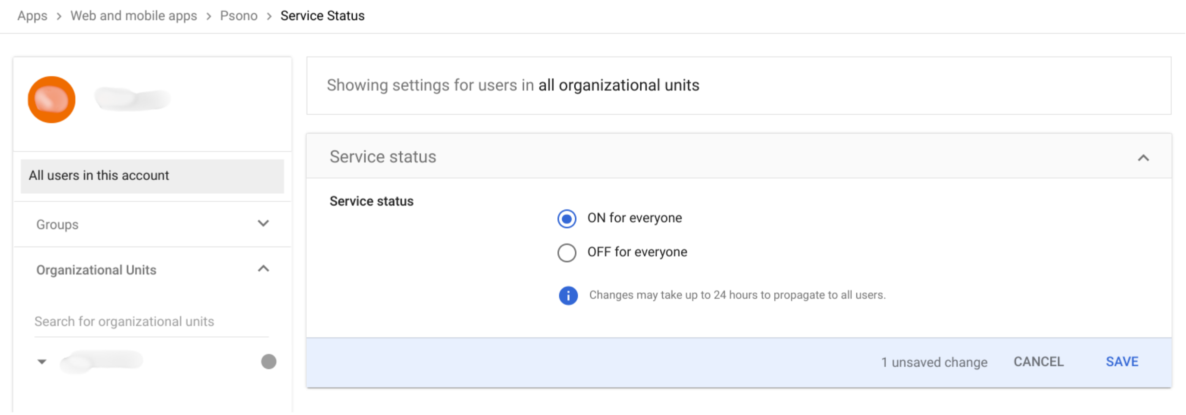
OFF for everyone

Service provider details

Certificate	ACS URL	Entity ID
Google_2026-12-9-34436_SAML2_0 (Expires Dec 9, 2026)	[redacted]	[redacted]

SAML attribute mapping

As an example, select the *All*, but you can restrict access to certain groups if you need to.



Apps › Web and mobile apps › Psono › Service Status

All users in this account

Groups

Organizational Units

Search for organizational units

Showing settings for users in **all organizational units**

Service status

Service status

● ON for everyone

○ OFF for everyone

Changes may take up to 24 hours to propagate to all users.

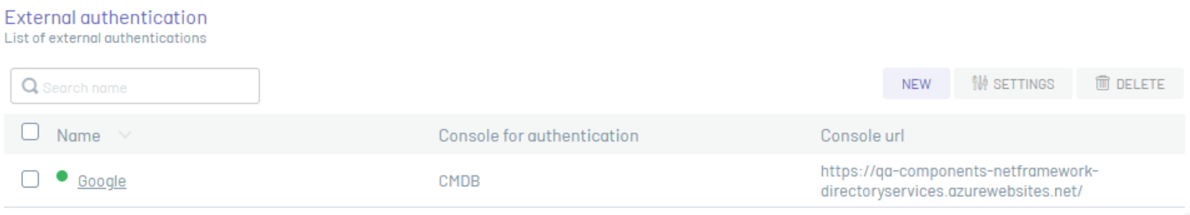
1 unsaved change CANCEL SAVE

- Finish the setup by selecting the **Save**.

Third-Party Vendor Management

View Third-Party Vendors

1. In the information view of external suppliers you can view the list of registered suppliers, grouped by data such as:



External authentication

List of external authentications

Search name

NEW SETTINGS DELETE

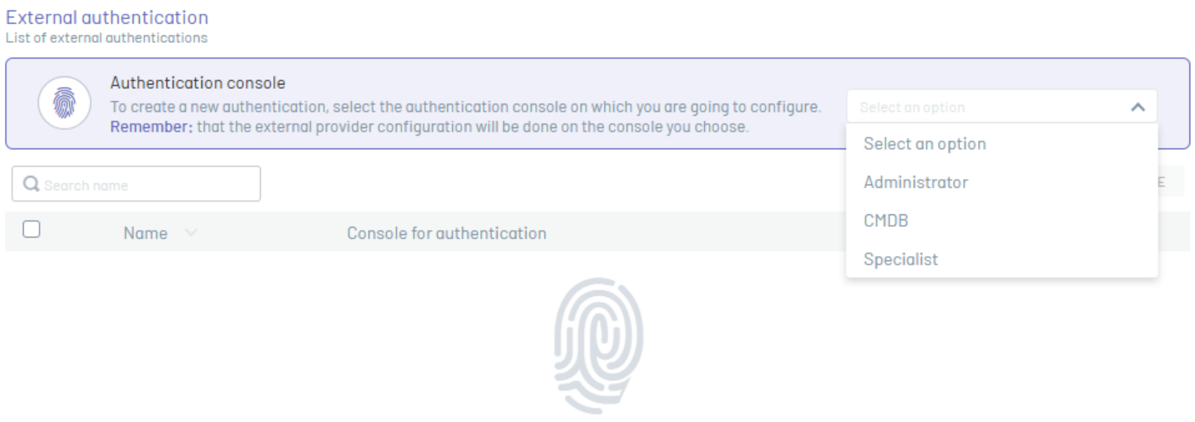
□	Name	Console for authentication	Console url
□	● Google	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/

Field	Field Type	Description
Name	Text	Name with which the supplier is identified.
Console for authentication	Text	Indicates the type of console you want to integrate.
Console URL	Text	This is the public URL of the console, this value must be provided to the authentication provider as an identifier (Entity ID).

2. In the information view of external suppliers, you will have information management and organization actions enabled. [Information View in Commons Environment]()

> ⚠ **Important**: Settings for products that have authentication consoles will be able to display a box labeled **Authentication console** with default options called Administrator, Specialist, and CMDB.

3. In the third-party vendor information view for products that have authentication consoles, you can view it as follows:



External authentication

List of external authentications

Authentication console

To create a new authentication, select the authentication console on which you are going to configure.

Remember: that the external provider configuration will be done on the console you choose.

Select an option

Select an option

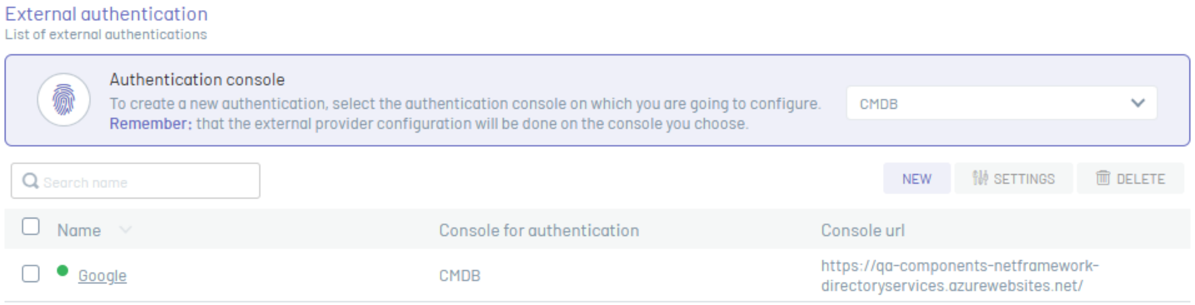
Administrator

CMDB

Specialist

Search name

□	Name	Console for authentication



External authentication

List of external authentications

Authentication console

To create a new authentication, select the authentication console on which you are going to configure.

Remember: that the external provider configuration will be done on the console you choose.

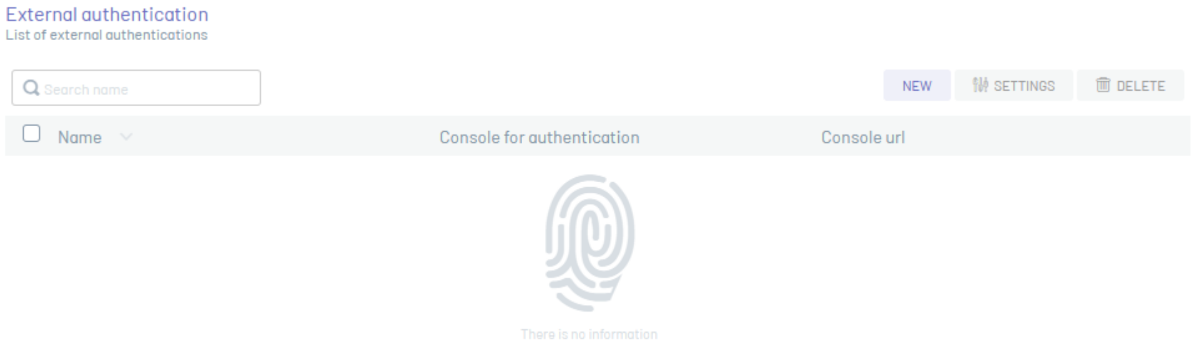
□ Name	Console for authentication	Console url
□ ● Google	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/

Related Links:

- [Create third-party provider]
- [Edit third-party provider]
- [Remove third-party provider]
- [Third-Party Provider Configuration]

Create Third-Party Vendor

1. To create a new third-party vendor, in the vendor information view, click the **New**.



External authentication

List of external authentications

□ Name	Console for authentication	Console url

There is no information

> ⚐ **Note:** There is no restriction on creating external providers with duplicate information, as many as necessary can be created.

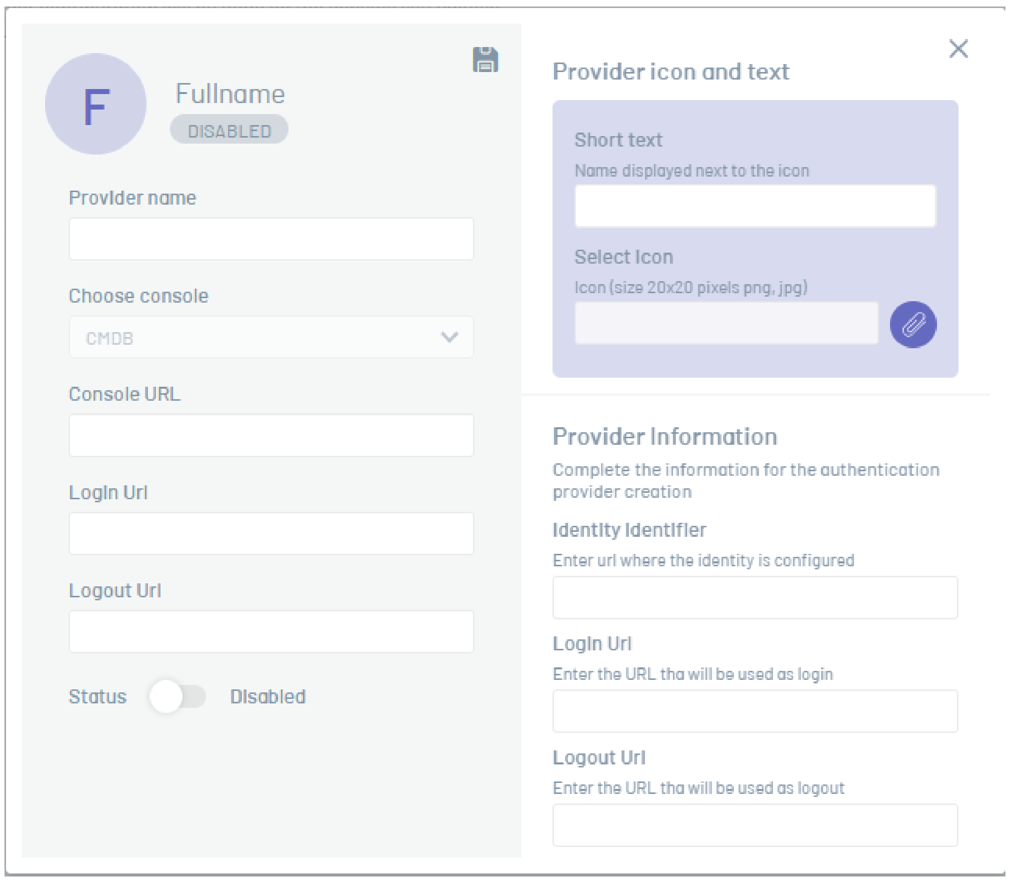
> ⚠ **Important**: Products that have authentication consoles such as ASMS, the **New** will be disabled until you select an authentication console in the box **Authentication console**.

Basic Facts

2. In the window that is enabled, you will be able to fill in the basic data of the external provider such as provider name, console URL, login URL, logout URL, status, icon and text of the provider, among others.
Each of the third-party vendor fields must take into account the Specifications for Fields

> ⚐ Notes:

- The fields **Login URL** and **URL log out** have auto-complete functionality and are based on the information provided in the field **Console URL**.



F Fullname
DISABLED

Provider name

Choose console
CMDB

Console URL

Login Url

Logout Url

Status Disabled

Provider icon and text

Short text
Name displayed next to the icon

Select Icon
Icon (size 20x20 pixels png, jpg)

Provider Information
Complete the information for the authentication provider creation

Identity Identifier
Enter url where the identity is configured

Login Url
Enter the URL tha will be used as login

Logout Url
Enter the URL tha will be used as logout

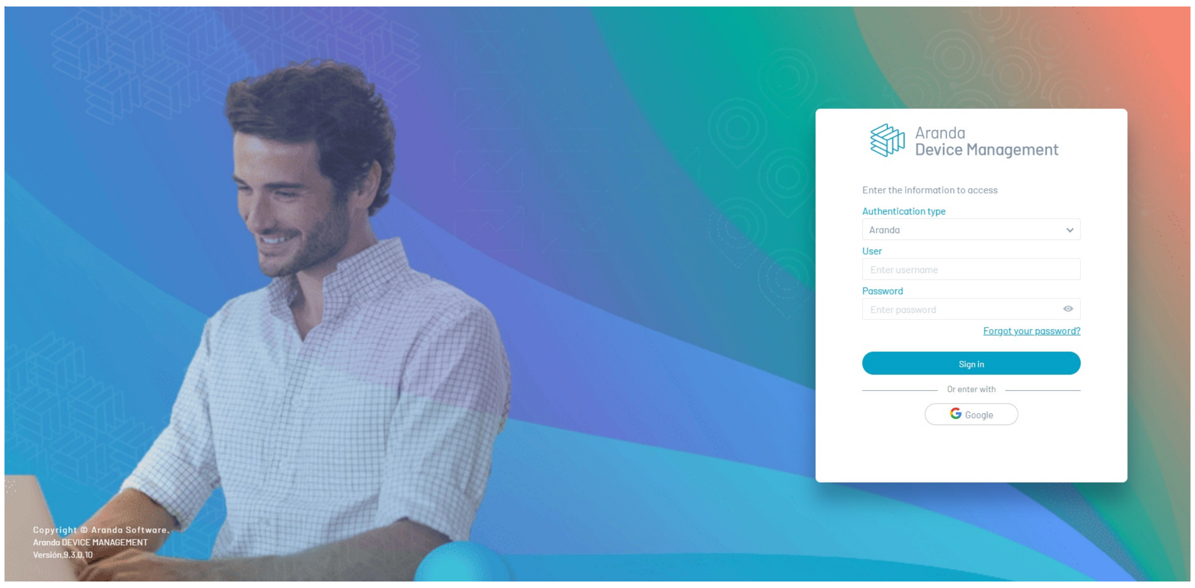
⚐ Notes:

- In products that have authentication consoles such as ASMS, the value of the **Authentication Console** corresponds to the Console defined at the beginning of the vendor creation.

3. When you finish setting up provider authentication, click the **Save**.

⚐ Notes:

- If the configuration is successful, in the external vendor view you can view the records of the last vendors created.
- On the home screen and access to the required application, you will be able to display the icon with the name given to the external provider.



Aranda
Device Management

Enter the information to access

Authentication type
Aranda

User
Enter username

Password
Enter password

Forgot your password?

Sign in

Or enter with

Google

Copyright © Aranda Software.
Aranda DEVICE MANAGEMENT
Versión.9.3.0.10

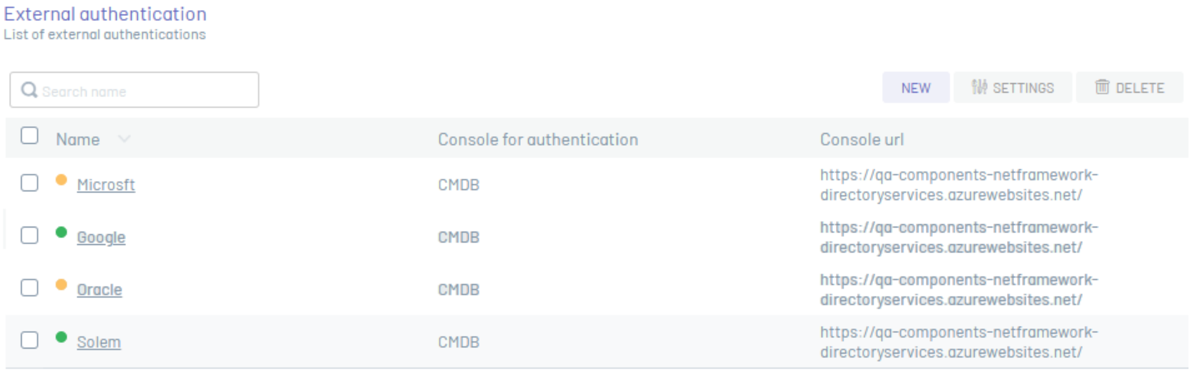
⚐ Notes:

- The email with which the authentication is carried out from the external provider is used as the user's identification and must be registered in the respective application.
- In order for the website to authenticate the user, the user must be imported or created before performing the external authentication configuration.
- To authenticate local users, the username must match the email.

Edit Third-Party Vendor

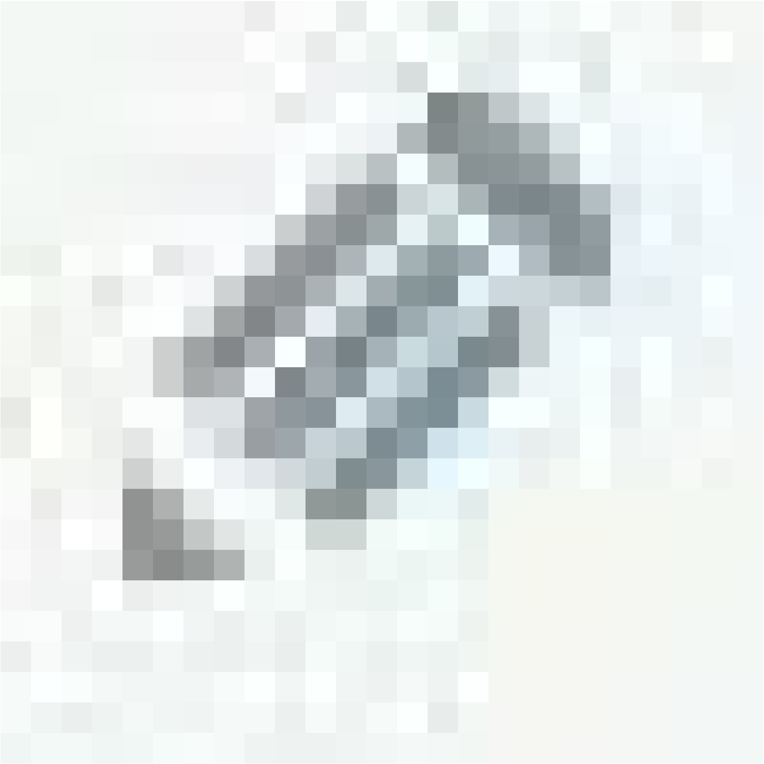
⚠ **Important**: For products that have authentication consoles and their third-party provider settings are not correct, you won't be able to change the authentication console in the edit window, so you must delete the third-party provider and create a new third-party provider with the correct information.

1. In the third-party vendor information view, select a record from the existing vendor list.

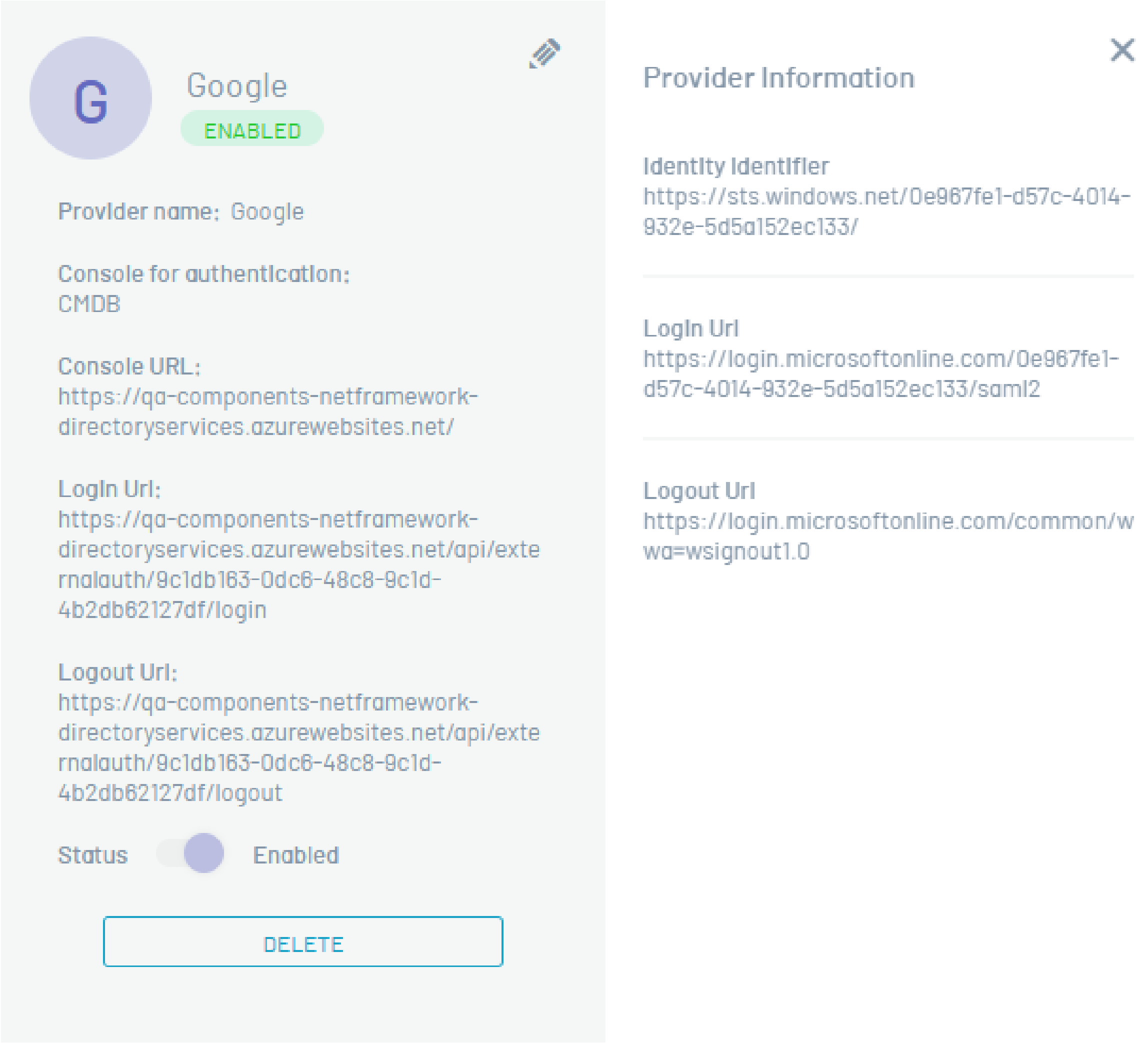


□ Name	Console for authentication	Console url
□ ● Microsft	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/
□ ● Google	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/
□ ● Oracle	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/
□ ● Solem	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/

2. In the vendor detail view, click the **Edit**



and modify the required information.



Provider name: Google

Console for authentication: CMDB

Console URL: https://qa-components-netframework-directoryservices.azurewebsites.net/

Login Url: https://qa-components-netframework-directoryservices.azurewebsites.net/api/externalauth/9c1db163-0dc6-48c8-9c1d-4b2db62127df/login

Logout Url: https://qa-components-netframework-directoryservices.azurewebsites.net/api/externalauth/9c1db163-0dc6-48c8-9c1d-4b2db62127df/logout

Status Enabled

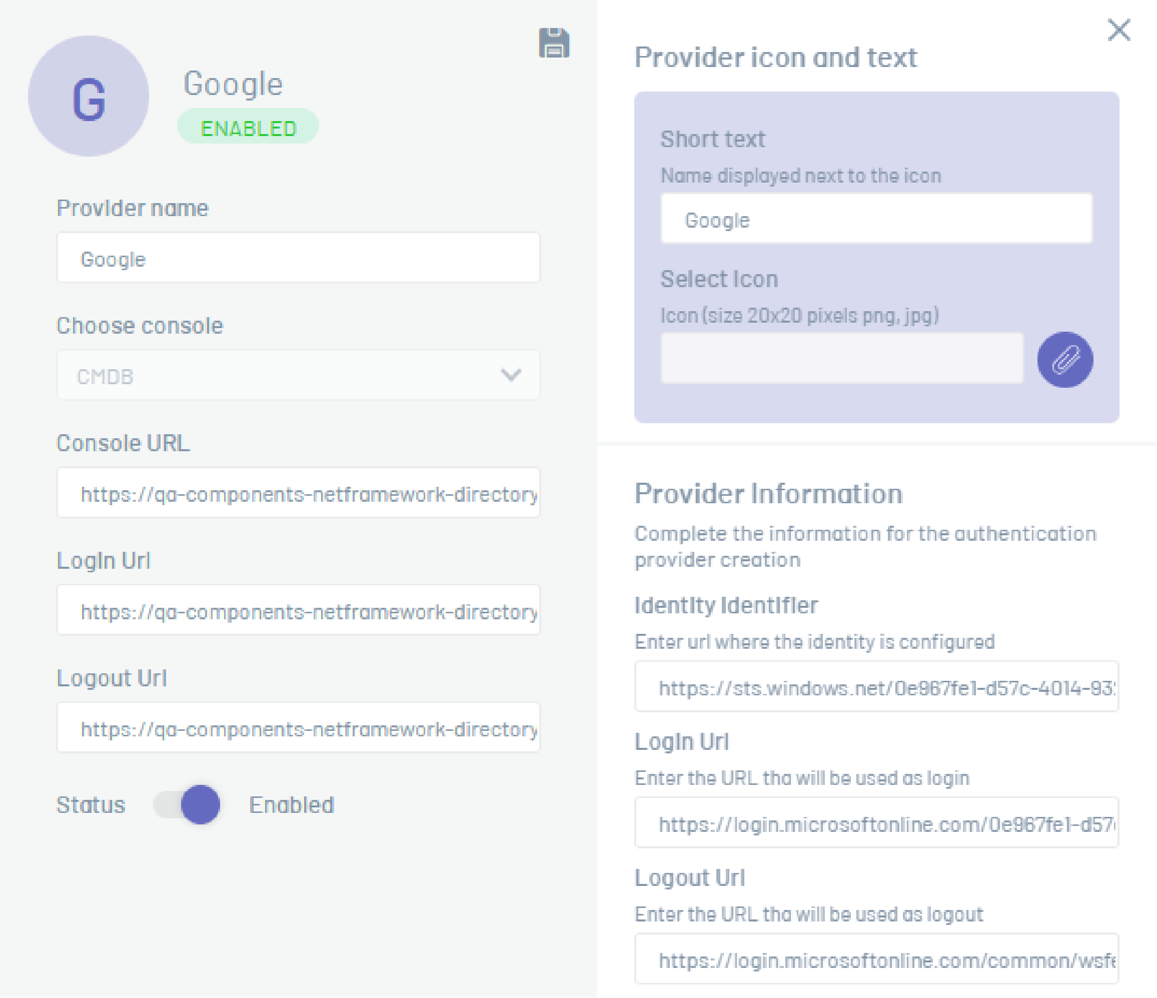
Provider Information

Identity Identifier
https://sts.windows.net/0e967fe1-d57c-4014-932e-5d5a152ec133/

Login Url
https://login.microsoftonline.com/0e967fe1-d57c-4014-932e-5d5a152ec133/saml2

Logout Url
https://login.microsoftonline.com/common/wa=wsignout1.0

3. In the window **Third-Party Vendor Editing** You will be able to update the basic information of the supplier.



G

Google

ENABLED

Provider name

Google

Choose console

CMDB

Console URL

https://qa-components-netframework-directory

Login Url

https://qa-components-netframework-directory

Logout Url

https://qa-components-netframework-directory

Status Enabled

Provider icon and text

Short text

Name displayed next to the icon

Google

Select Icon

Icon (size 20x20 pixels png, jpg)

Provider Information

Complete the information for the authentication provider creation

Identity Identifier

Enter url where the identity is configured

https://sts.windows.net/0e967fe1-d57c-4014-93

Login Url

Enter the URL tha will be used as login

https://login.microsoftonline.com/0e967fe1-d57

Logout Url

Enter the URL tha will be used as logout

https://login.microsoftonline.com/common/wsfe

⚐ Notes:

- The value of the field **Authentication Console** corresponds to the Console defined at the beginning of the vendor creation. This field is not editable.
- The value of the field **Select icon** It will not be visible in edit mode. If no changes are made to this field, the image saved when you created the vendor is retained.

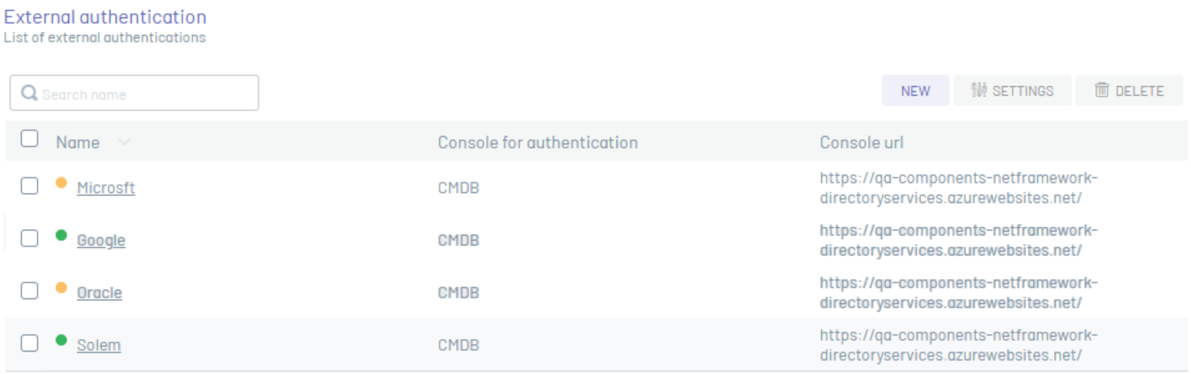
4. When you finish editing the third-party provider, click the **Save**

to confirm the changes made.

Remove Third-Party Provider

Deleting third-party vendor records can be done in two ways:

1. To delete a third-party provider, in the provider information view, in the 'Authentication console' box, select an available option from the list of consoles.

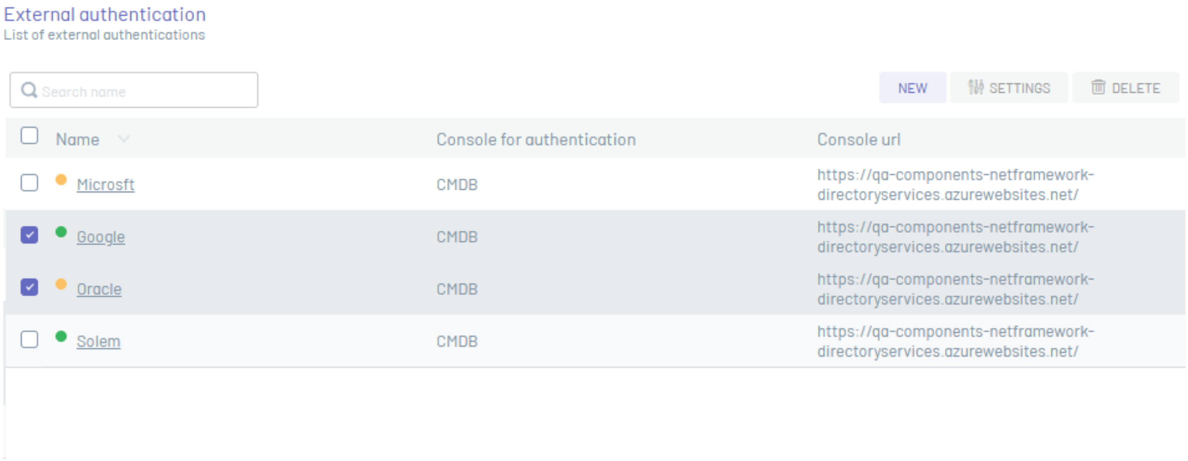


External authentication
List of external authentications

□	Name	Console for authentication	Console url
□	● Microsft	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/
□	● Google	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/
□	● Oracle	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/
□	● Solem	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/

2. In the Third-Party Vendor Information view, select one or more records from the Vendor List that you want to delete, and click the

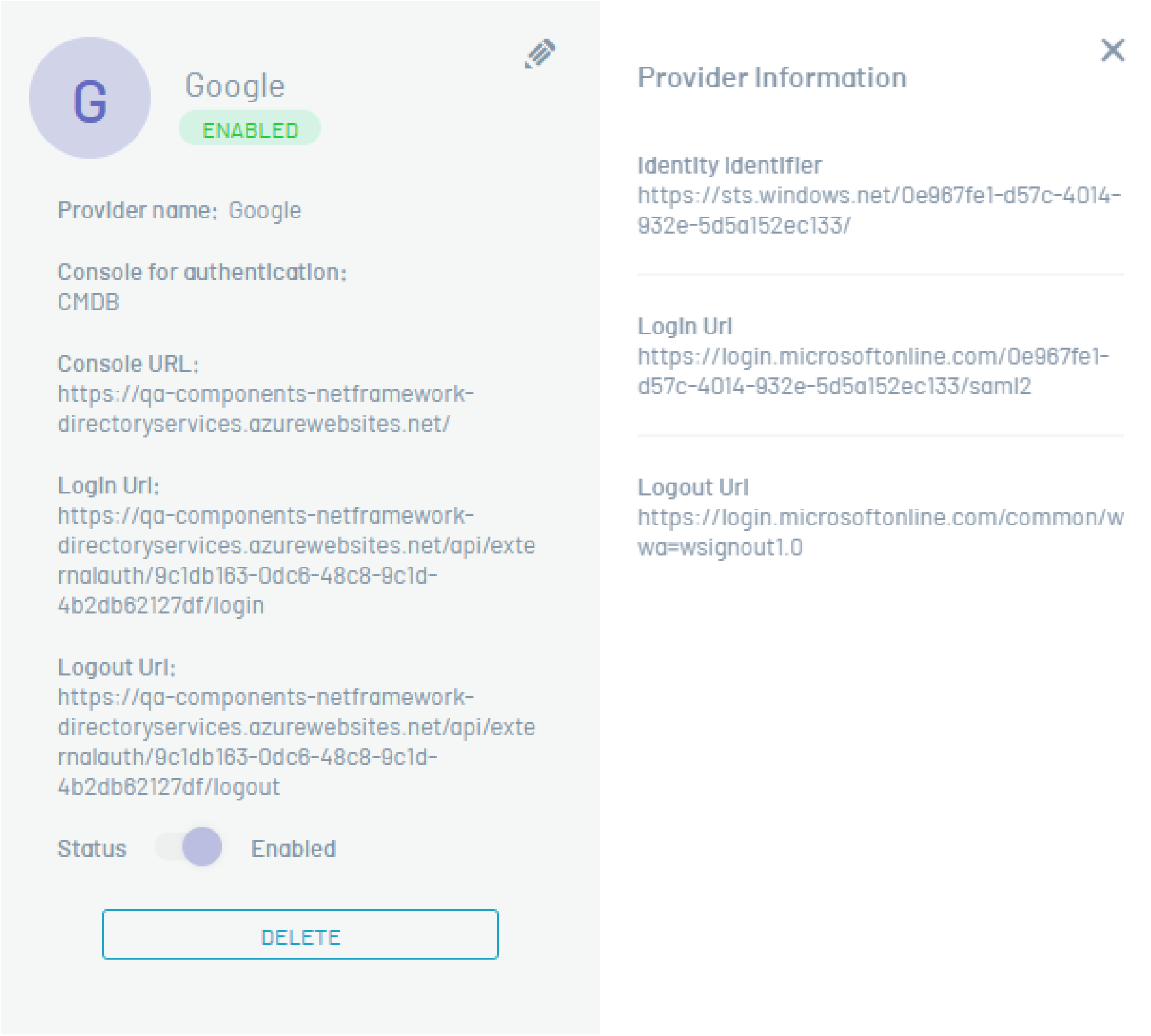
.



External authentication
List of external authentications

□	Name	Console for authentication	Console url
□	● Microsft	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/
☑	● Google	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/
☑	● Oracle	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/
□	● Solem	CMDB	https://qa-components-netframework-directoryservices.azurewebsites.net/

3. In the detail view of a selected vendor that you want to delete, click theELIMINATE



Google
ENABLED

Provider name: Google

Console for authentication:
CMDB

Console URL:
https://qa-components-netframework-directoryservices.azurewebsites.net/

Login Url:
https://qa-components-netframework-directoryservices.azurewebsites.net/api/externalauth/9c1db163-0dc6-48c8-9c1d-4b2db62127df/login

Logout Url:
https://qa-components-netframework-directoryservices.azurewebsites.net/api/externalauth/9c1db163-0dc6-48c8-9c1d-4b2db62127df/logout

Status Enabled

Provider Information

Identity Identifier
https://sts.windows.net/0e967fe1-d57c-4014-932e-5d5a152ec133/

Login Url
https://login.microsoftonline.com/0e967fe1-d57c-4014-932e-5d5a152ec133/saml2

Logout Url
https://login.microsoftonline.com/common/wwa=wsignout1.0

3. In both cases, you can display a confirmation message to validate the deletion action.

⚐ Note:

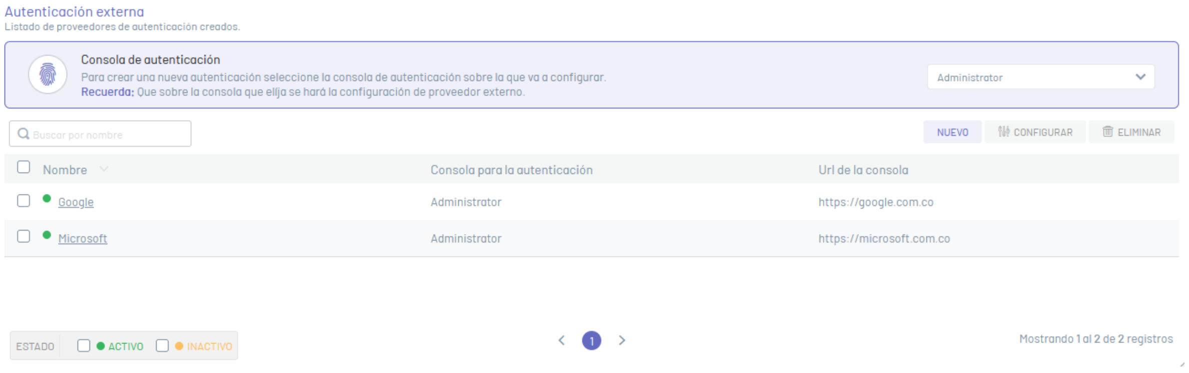
- A deleted provider cannot be restored.

- The provider has no restriction on its disposal.

Configure Third-Party Provider

> ⚠ **Important**: The **Configuration** For third-party providers, it will only be enabled if an authentication console is selected.

1. To perform the configuration, in the Third-Party Vendor Information view, select the



Autenticación externa

Listado de proveedores de autenticación creados.

Consola de autenticación

Para crear una nueva autenticación seleccione la consola de autenticación sobre la que va a configurar.

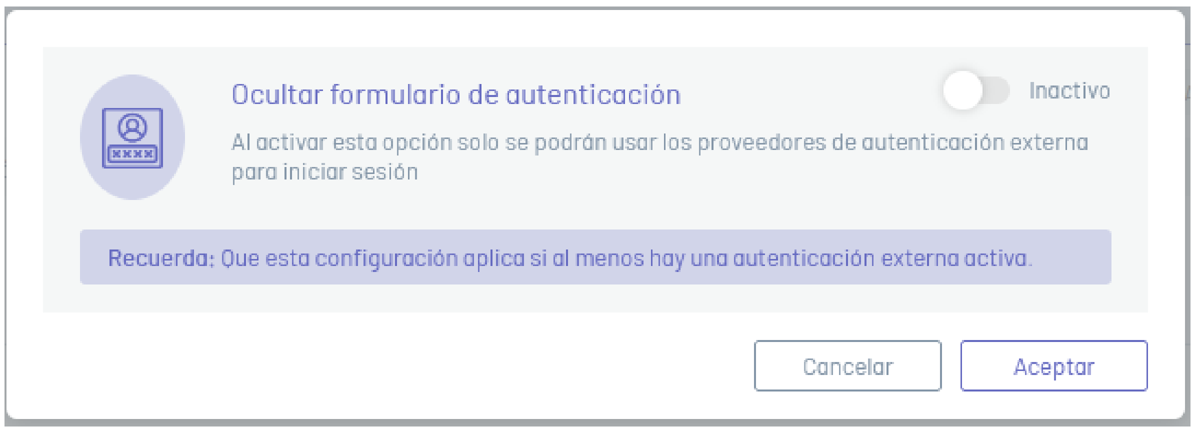
Recuerda: Que sobre la consola que elija se hará la configuración de proveedor externo.

☐ Nombre	Consola para la autenticación	Url de la consola
☐ ● Google	Administrator	https://google.com.co
☐ ● Microsoft	Administrator	https://microsoft.com.co

ESTADO ☐ ● ACTIVO ☐ ● INACTIVO

Mostrando 1 al 2 de 2 registros

2. In the window that is enabled, you can activate or not the authentication options (username and password). When finished, click on the **Accept**

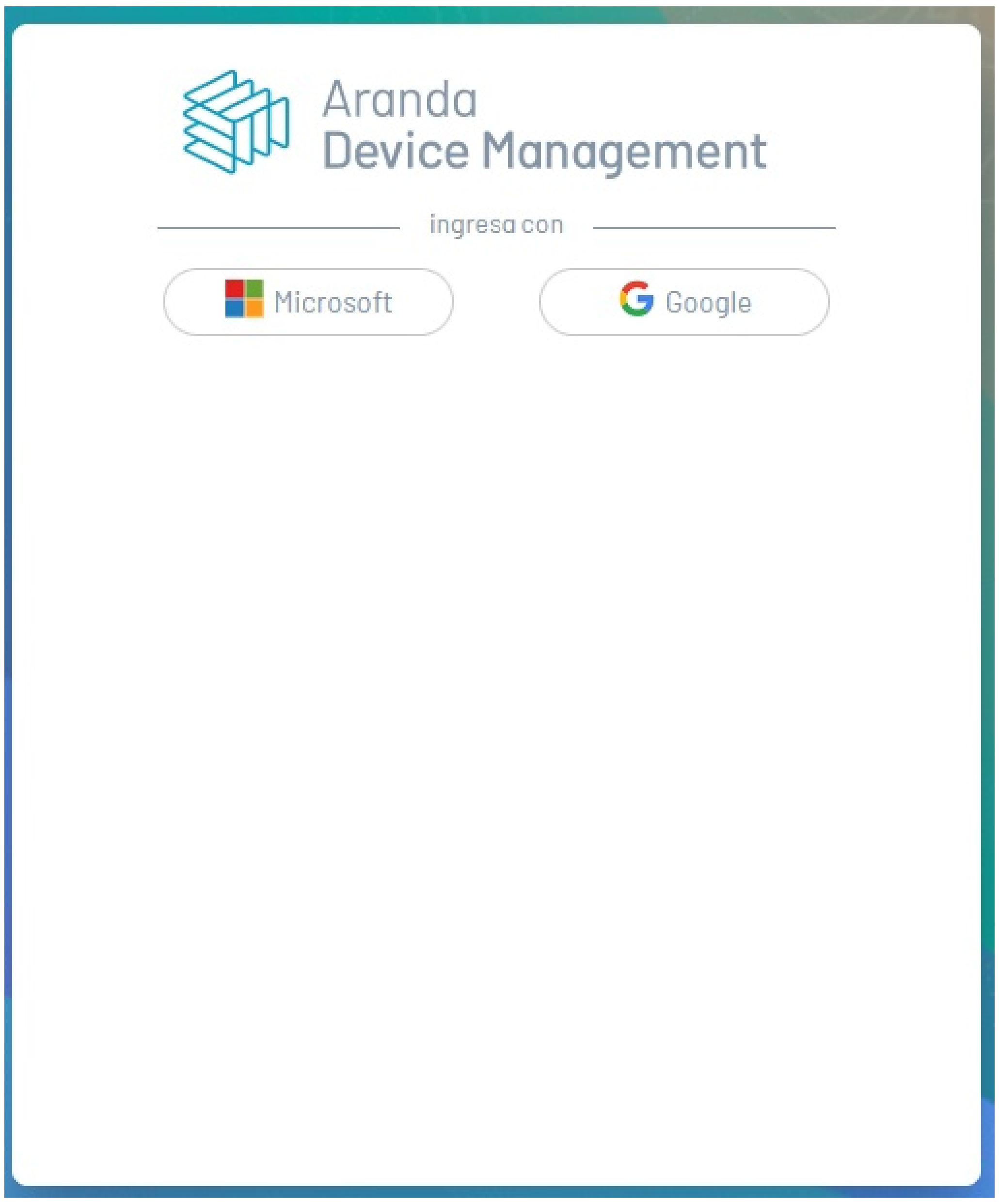


Ocultar formulario de autenticación

Al activar esta opción solo se podrán usar los proveedores de autenticación externa para iniciar sesión

Recuerda: Que esta configuración aplica si al menos hay una autenticación externa activa.

3. If you enabled the option to **Hide Authentication Form**, in the authentication process you will only be allowed to enter as an external provider.



⚐ **Note:** To hide the authentication form (username, password), there must be at least one active third-party provider.

Specification Fields

Third-Party Providers

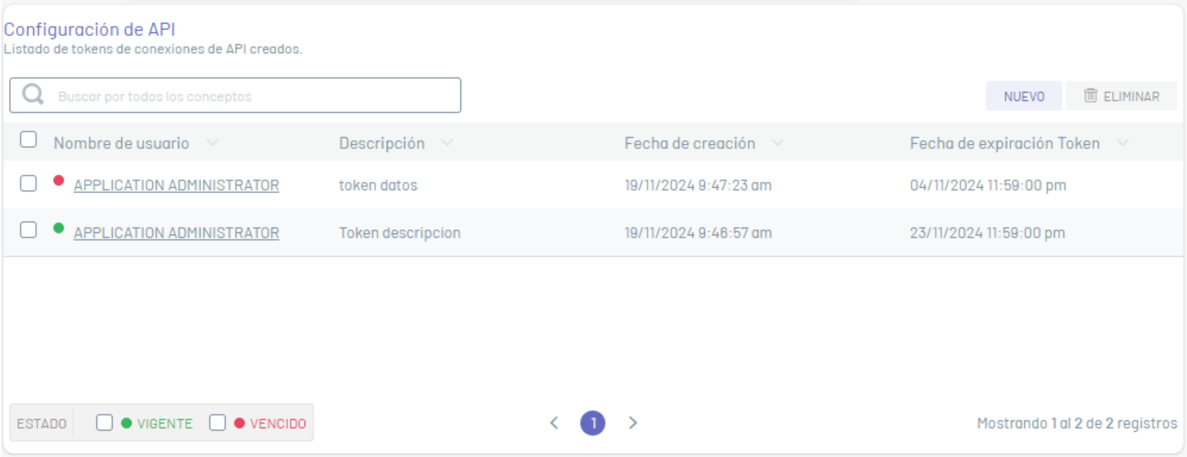
Field	Description
Vendor Name	Name to be given to the provider; This name is the name that will appear on the authentication screen of the corresponding console.
Console for configuring authentication	Type of console to be integrated.
Console URL	Public console URL. This value must be provided to your authentication provider as an Identifier (entity ID).
Login URL	Autocomplete value that is supplied from field information**Console URL** where the final structure ends in /login.
URL log out	Autocomplete value that is supplied from field information**Console URL** where the final structure ends in /logout.
State	Enables third-party vendor integration using the selector in the "**Active**".
Select icon	This is the figure that is displayed in the login option of the third-party provider enabled to authenticate
Short text	Friendly name of the provider enabled and configured for authentication
Identity Identifier	Identity ID of the authentication provider.
Login URL / Log Out URL	Data that must be provided to your authentication provider to perform the configuration of the trust relationship between the two parties login and logout

Integration Token Module

Token Management

View Tokens

1. In the Token information view, you can view the list of tokens created, grouped by data such as:



Configuración de API

Listado de tokens de conexiones de API creados.

Buscar por todos los conceptos

NUEVO   ELIMINAR

□	Nombre de usuario	Descripción	Fecha de creación	Fecha de expiración Token
□	● APPLICATION ADMINISTRATOR	token datos	19/11/2024 9:47:23 am	04/11/2024 11:59:00 pm
□	● APPLICATION ADMINISTRATOR	Token descripcion	19/11/2024 9:46:57 am	23/11/2024 11:59:00 pm

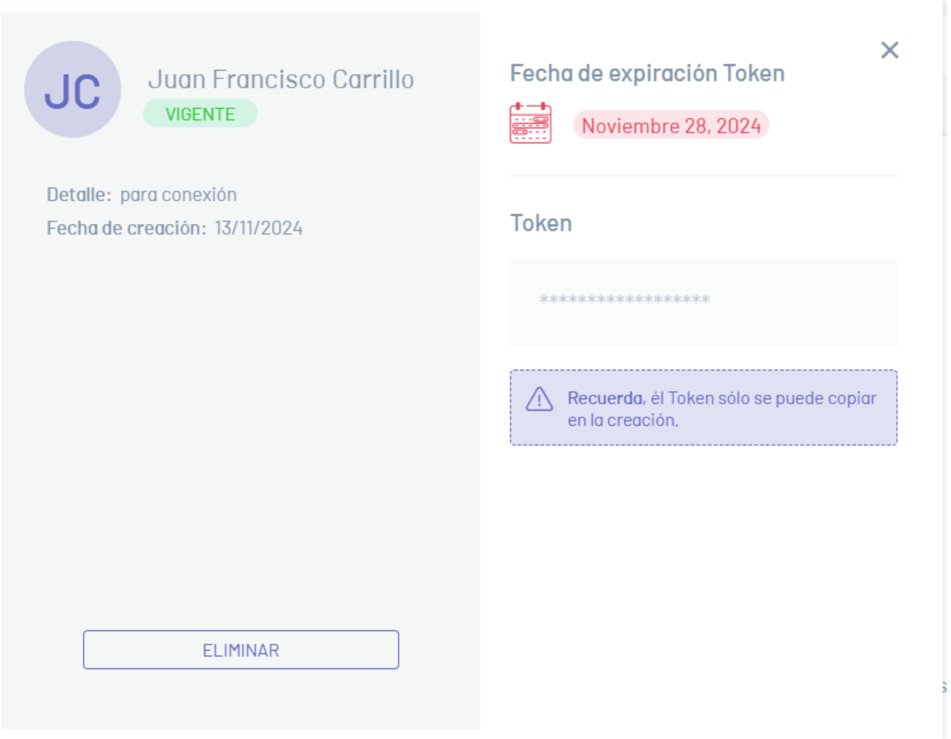
ESTADO □ ● VIGENTE □ ● VENCIDO

‹ 1 ›

Mostrando 1 al 2 de 2 registros

Field	Field Type	Description
Username	Text	Name of the user associated with the token.
Description	Text	Description of the token.
Date of creation	Text	Date of creation.
Token Expiration Date	Text	Date the token expires.

2. In the token information view, you will have information management and organization actions enabled.[Information View in Commons Environment](#) 3. To display an integration token, in the token information view, select a record from the list of existing tokens. In the token detail view you will be able to view the information with which the token was created, this information cannot be edited.



JC Juan Francisco Carrillo
VIGENTE

Detalle: para conexión
Fecha de creación: 13/11/2024

Fecha de expiración Token
Noviembre 28, 2024

Token
****

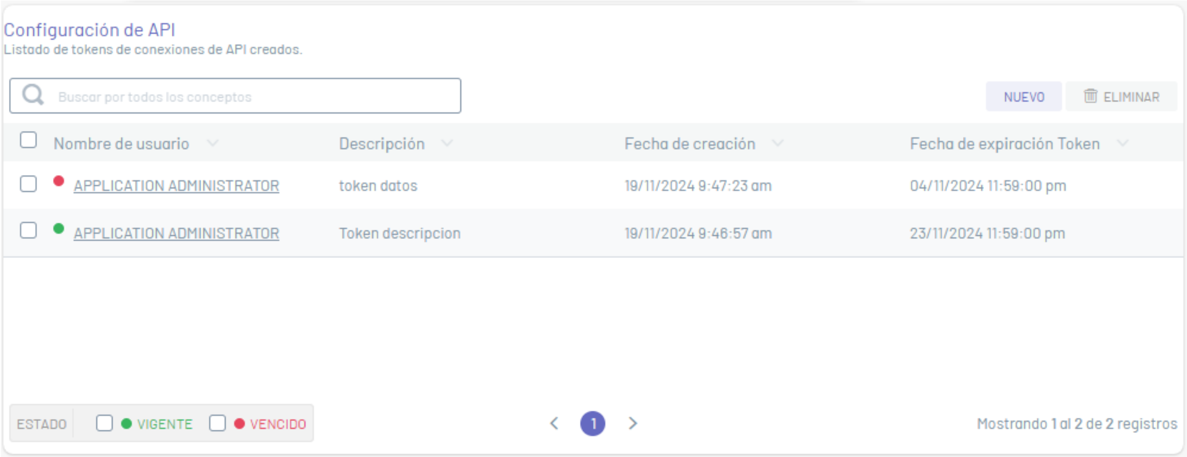
Recuerda, él Token sólo se puede copiar en la creación.

❓Related Links:

- [Create Token Integration](#)
- [Remove Token Integration](#)

Create tokens

1. To create a new integration token, in the token information view, click the **New**.



Configuración de API
Listado de tokens de conexiones de API creados.

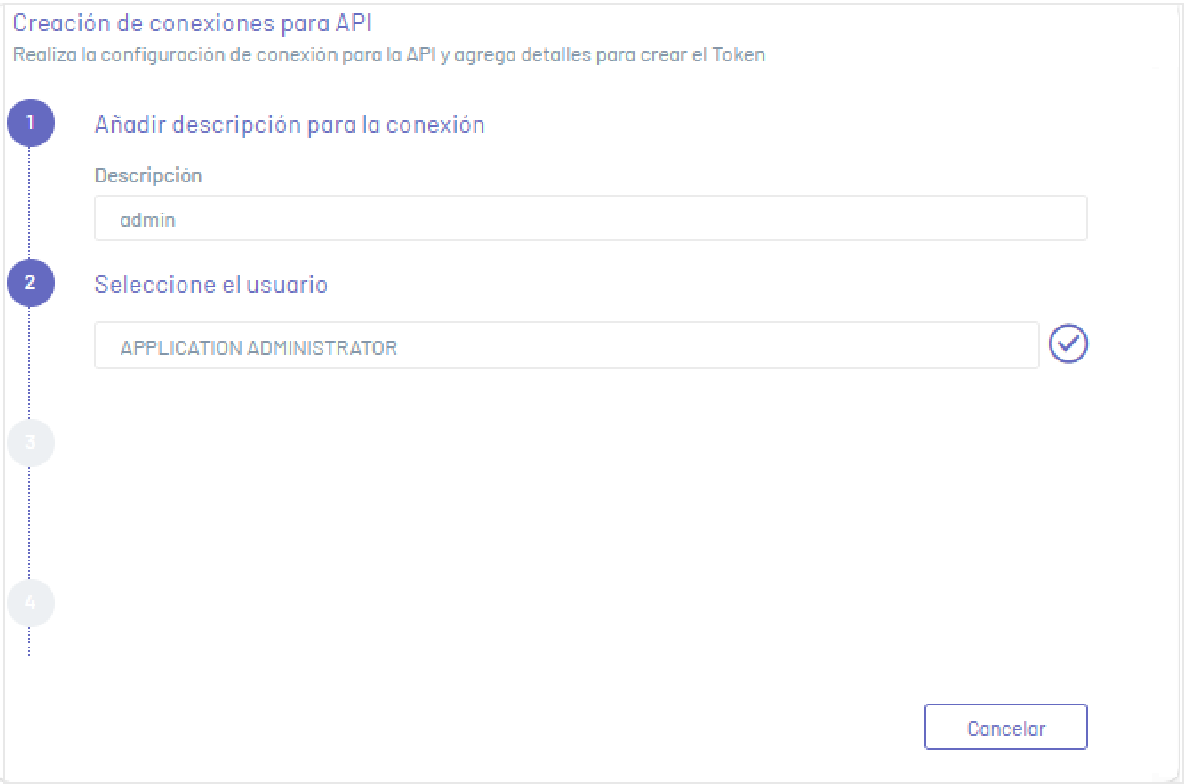
	Nombre de usuario	Descripción	Fecha de creación	Fecha de expiración Token
□	● APPLICATION ADMINISTRATOR	token datos	19/11/2024 9:47:23 am	04/11/2024 11:59:00 pm
□	● APPLICATION ADMINISTRATOR	Token descripcion	19/11/2024 9:46:57 am	23/11/2024 11:59:00 pm

ESTADO □ ● VIGENTE □ ● VENCIDO

Mostrando 1 al 2 de 2 registros

Basic Facts

2. In the window that is enabled you will be able to fill in the token data: Description, user and expiration date. Each of the token fields must take into account the [Specifications for Common Fields](#)



Creación de conexiones para API

Realiza la configuración de conexión para la API y agrega detalles para crear el Token

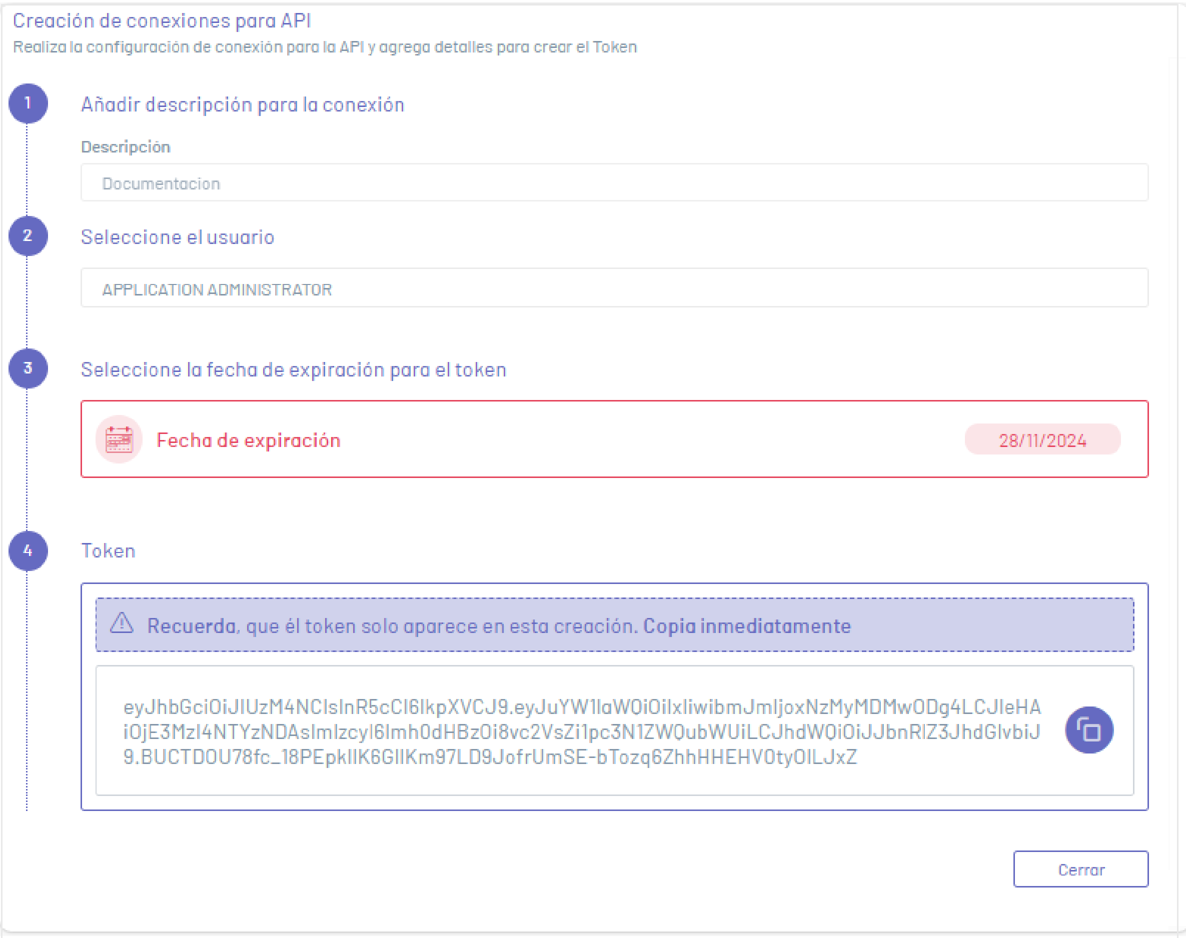
1 Añadir descripción para la conexión

Descripción: admin

2 Seleccione el usuario

APPLICATION ADMINISTRATOR ✓

3. When completing the configuration of each field, click on the ✓ to commit the generated changes.



Creación de conexiones para API

Realiza la configuración de conexión para la API y agrega detalles para crear el Token

1 Añadir descripción para la conexión

Descripción: Documentacion

2 Seleccione el usuario

APPLICATION ADMINISTRATOR

3 Seleccione la fecha de expiración para el token

Fecha de expiración 28/11/2024

4 Token

⚠ Recuerda, que él token solo aparece en esta creación. Copia inmediatamente

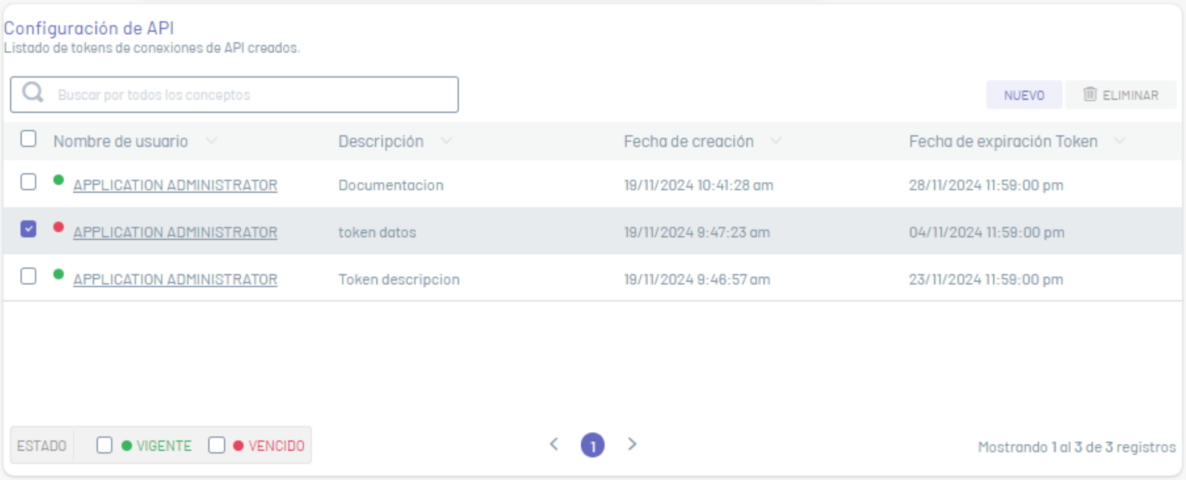
```
eyJhbGciOiJIUzM4NCIsInR5cCI6IkpXVCJ9.eyJuYW1laWQiOiIxIiwibmJmIjoxNzMyMDMwODg4LCJleHA
iOjE3MzI4NTYzNDAsImlzcyI6Imh0dHBzOi8vc2VsZi1pc3N1ZWQubWUiLCJhdWQiOiJJbnRlZ3JhdGlvbiJ
9.BUCTDOU78fc_18PEpkIlK6GIlKm97LD9JofrUmSE-bTozq6ZhhHHEHV0tyOILJxZ
```

⚐ Note: :

- Integration tokens cannot be edited, so the data recorded must be correct, or else you must create another token.
- The generated token must be copied and saved at the time of creation, given thatthat will not be shown again.

Deleting Tokens

1. In the token information view, select one or more records from the existing token list and click the to clear the associated information.



Configuración de API
Listado de tokens de conexiones de API creados.

□	Nombre de usuario	Descripción	Fecha de creación	Fecha de expiración Token
□	● APPLICATION ADMINISTRATOR	Documentacion	19/11/2024 10:41:28 am	28/11/2024 11:59:00 pm
☑	● APPLICATION ADMINISTRATOR	token datos	19/11/2024 9:47:23 am	04/11/2024 11:59:00 pm
□	● APPLICATION ADMINISTRATOR	Token descripcion	19/11/2024 9:46:57 am	23/11/2024 11:59:00 pm

ESTADO □ ● VIGENTE □ ● VENCIDO

Mostrando 1 al 3 de 3 registros

2. You will be able to display a confirmation message to validate the deletion action.

Specification Fields

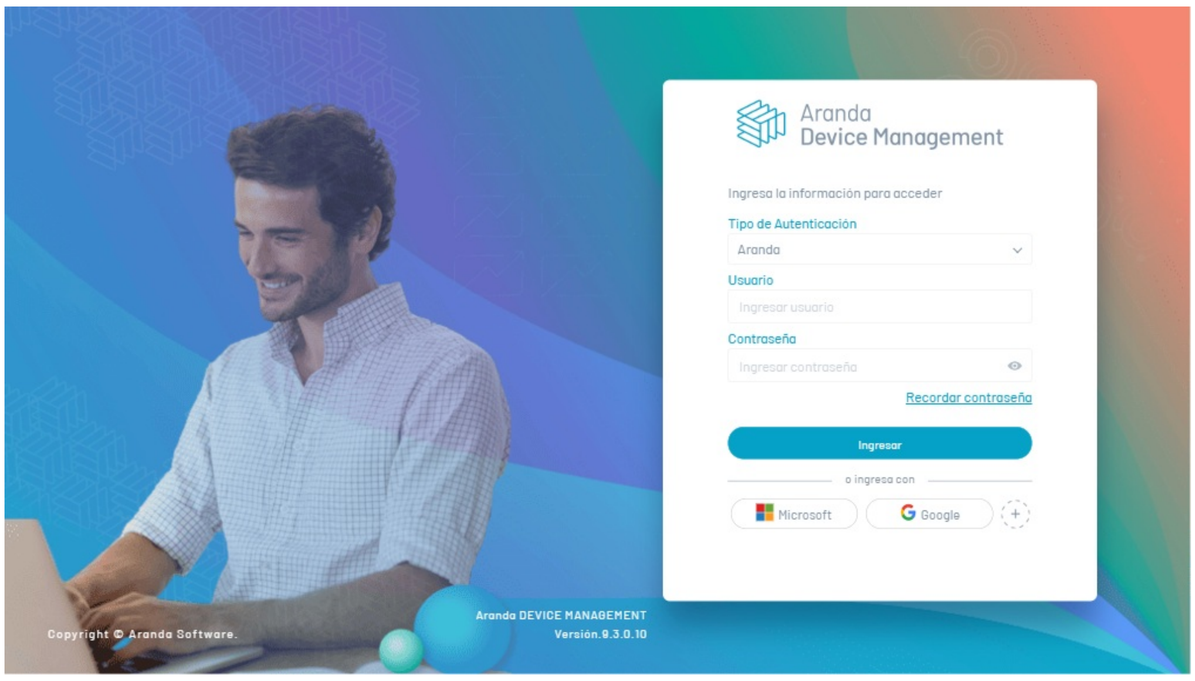
Integration/Data Tokens

Field	Description
Description	Information to describe the token to be created.
User	User to whom the token is to be generated
Token expiration date	Date the token will expire

Login Module

Login

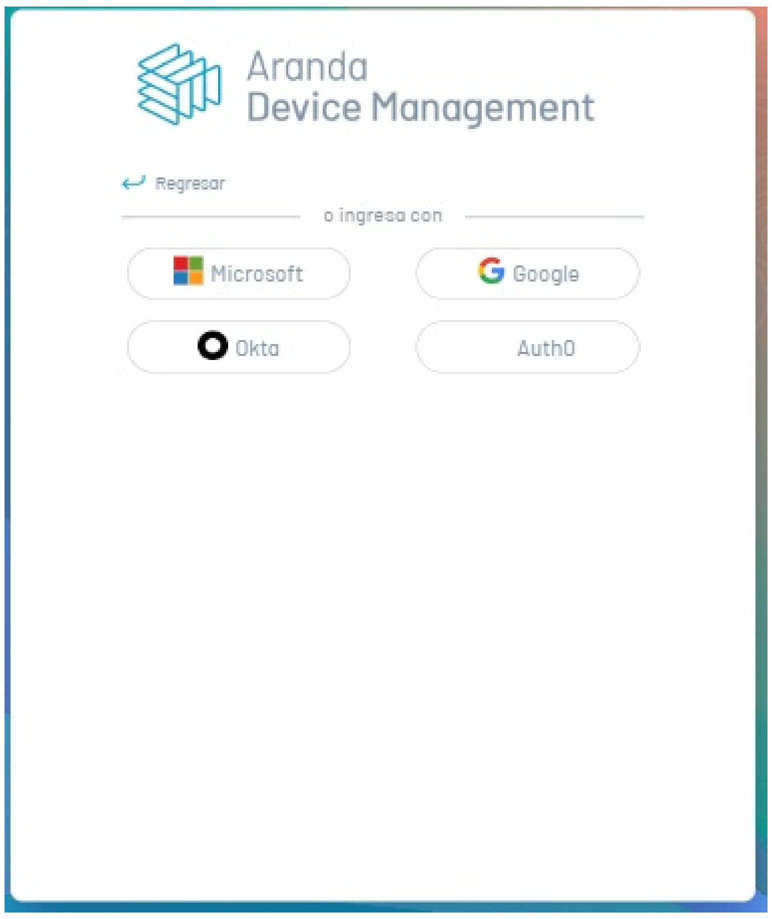
1. To log in to the application, enter the assigned username and password, taking into account the Authentication field specifications.



⚐ Note:

- The name of the product varies according to the application you are using.
- At the bottom you will find the name of the product and the number of**version**
- In case you forget your password, select the **Authentication Type** and click on the Remember password

2. If you have external authentication providers configured, they can be displayed in the authentication option. If you have multiple providers configured, the ⊕ which will allow you to view all available external authentication providers.



Related Links:

- [Remember password]

Remember password

1. If you forget a provider's password, request a new one, select the authentication type and click **Remember password**

2. In the window that is enabled, enter **email or username**.

> ⚐ **Note:** This option applies to recover the password of the users of the directory service,**Not applicable** To recover your password from authentication providers **external**.

> 3. When you enter a valid email or username, you will receive a message with the link to reset the password. ⚐ **Note:**

- Depending on the product you are using, you may be able to recover the password with username, user email, or both.
- The recovery email will depend on the product you are using.
- The link in the email will be valid for 24 hours, if the password is not reset within this time, carry out the application process again.

4. By clicking on the link sent, you will enter the screen *Reset Password*, where you can set the new password that complies with the established policies.

> ⚐ **Note:** The password must comply with policies established by the site administrator, and can be active or inactive according to the configuration made in the [Directory Service]. If the policy is not active, compliance with it is not required when creating or modifying a password; Only active policies will be required.

Specification Fields

Login/login

Field	Field Type	Description
User	Text	System user name.
Password	Text	User password.