Configuración tipos autenticación en Prevengos

1. Introducción

Este documento tiene el propósito de mostrar, y guiar al usuario final, la configuración del modo de autenticación deseado de los diferentes usuarios en Prevengos (ya sean usuarios web o de Prevengos).

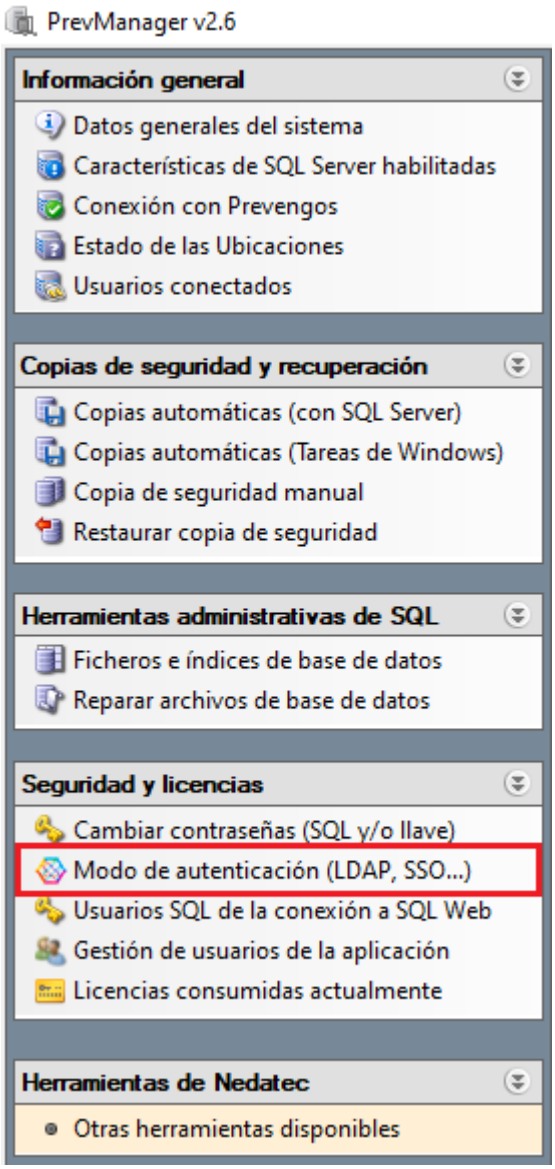
2. Breve descripción del uso de usuarios en Prevengos

Prevengos necesita siempre disponer de un usuario al cual se le asignan permisos, así como otras acciones u objetos a los que se tiene acceso dentro del aplicativo (ya sean usuarios web o de Prevengos).

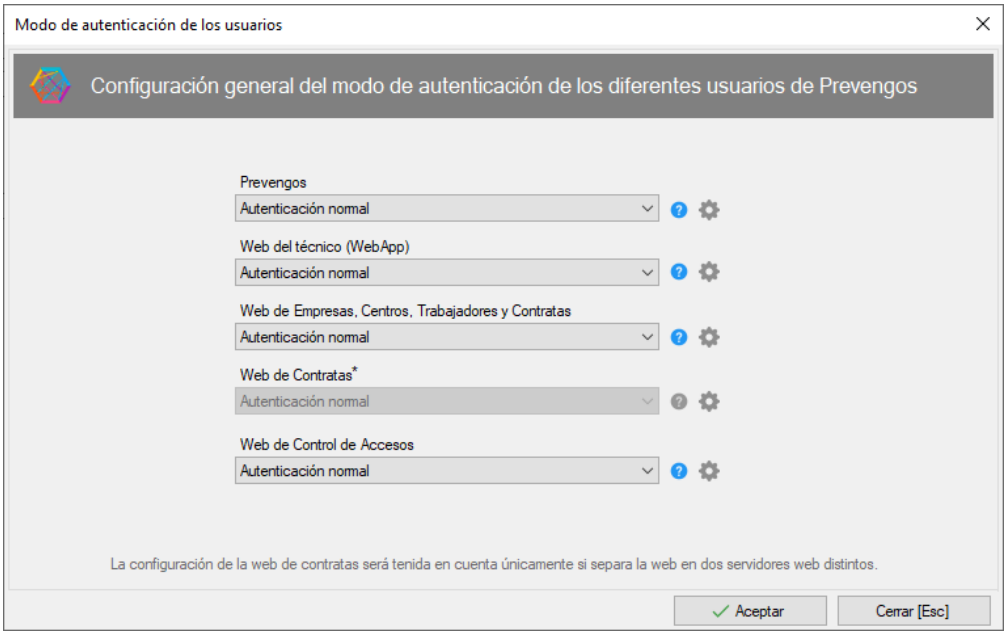
Toda esta configuración se almacena y registra dentro de la base de datos de Prevengos.

3. Modos de autenticación disponibles

Teniendo en cuenta lo descrito en el apartado anterior, puede autenticar a los diferentes usuarios de Prevengos (ya sea en la web o dentro del aplicativo) de 6 formas distintas y para ello deberá abrir el Panel de Control de Prevengos y seleccionar la opción *Modo de autenticación (LDAP, SSO...)*, bloque *Seguridad y licencias*, en el menú lateral izquierdo.



Al seleccionar esta opción, entrará directamente en la herramienta de gestión y configuración autenticación de los usuarios.



Selecionado el modo de autenticación, tendrá que usar el icono  para acceder a la configuración del mismo.

Aunque no se haya indicado el modo de atenticación, es posible su configuración para cambiar de un modo a otro de forma rápida.

3.1. Autenticación normal (contra SQL Server)

Cuando se utiliza este modo de autenticación, el aplicativo solicitará al usuario sus credenciales y se consultarán contra el servidor de datos. Por lo tanto, las contraseñas se almacenarán encriptadas en la base de datos de Prevengos (ya sean usuarios web o usuarios de Prevengos).

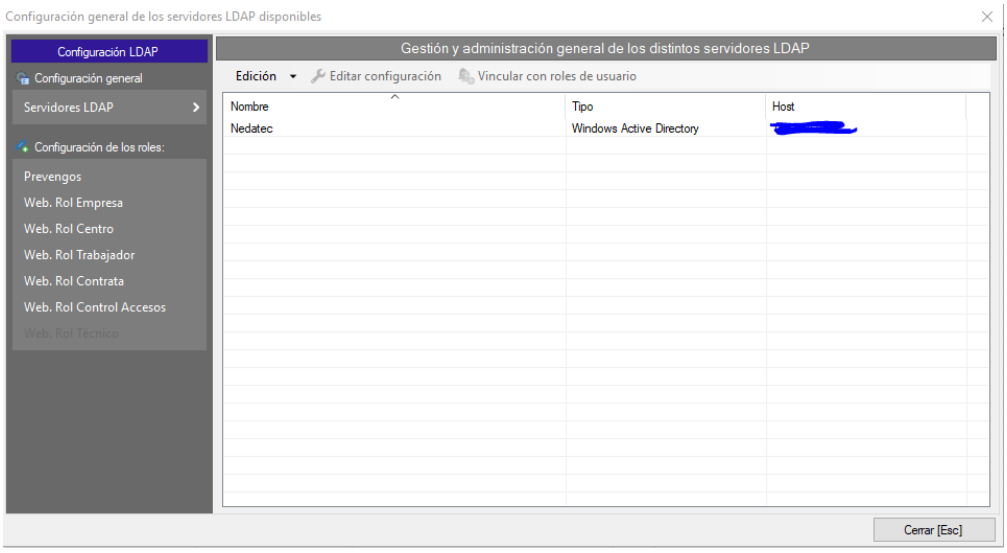
Si no se configura nada, este es el modo de autenticación por defecto.

3.2. Autenticación contra LDAP (solicitando usuario y contraseña)

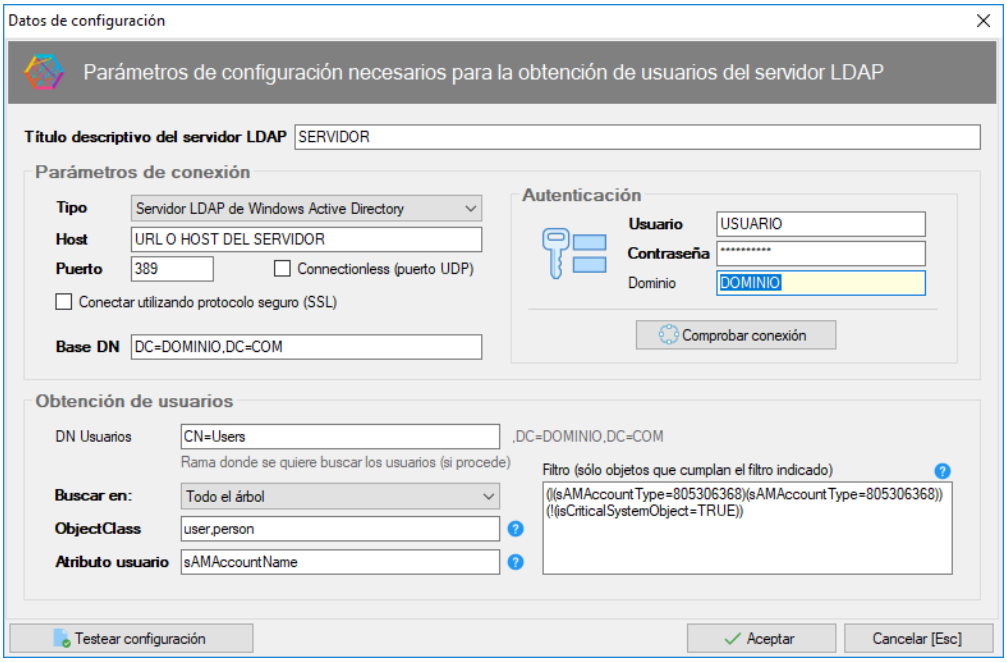
Cuando se utiliza este modo de autenticación, el aplicativo solicitará al usuario sus credenciales y se validarán contra el servidor LDAP que seleccione. Esto conlleva que las contraseñas de usuario no residen dentro de la base de datos de Prevengos. Además, dicho el usuario del directorio LDAP deberá estar debidamente vinculado con un usuario en Prevengos (ya sean usuarios web, o del aplicativo).

3.2.1. Cómo configurar servidores LDAP

Tras pulsar en el icono  , accede al siguiente formulario:



En el apartado de “Servidores LDAP” deberá añadir tantos servidores LDAP como servidores de usuario disponga. La pantalla de creación de un servidor LDAP es la siguiente:



Se considerarán todos los usuarios que estén en el directorio LDAP a partir del DN de usuarios indicado.

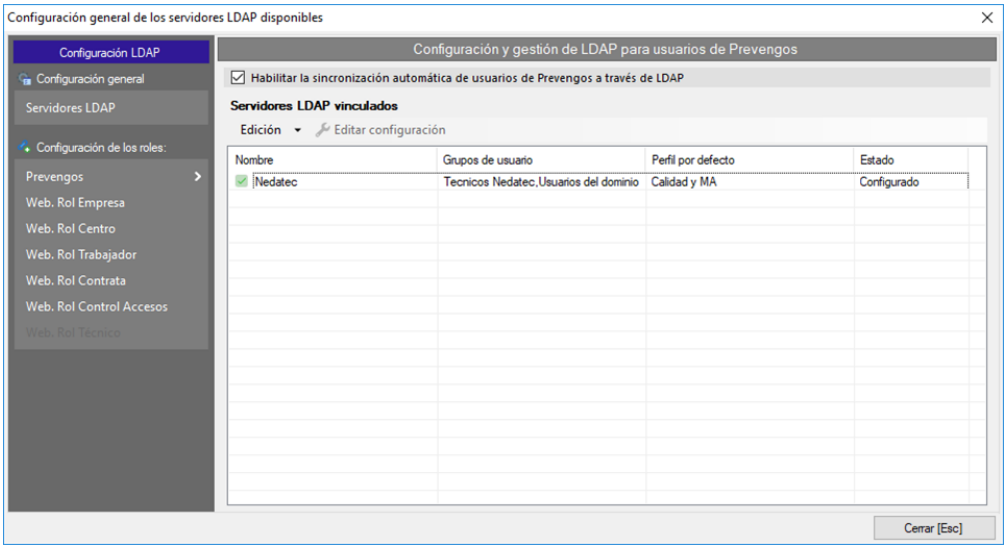
Una vez haya configurado los parámetros de conexión y los datos generales para la obtención de usuarios, debe vincular dicho servidor con los diferentes roles de usuario de Prevengos disponibles.

3.2.2. Configuración LDAP para un rol de usuario

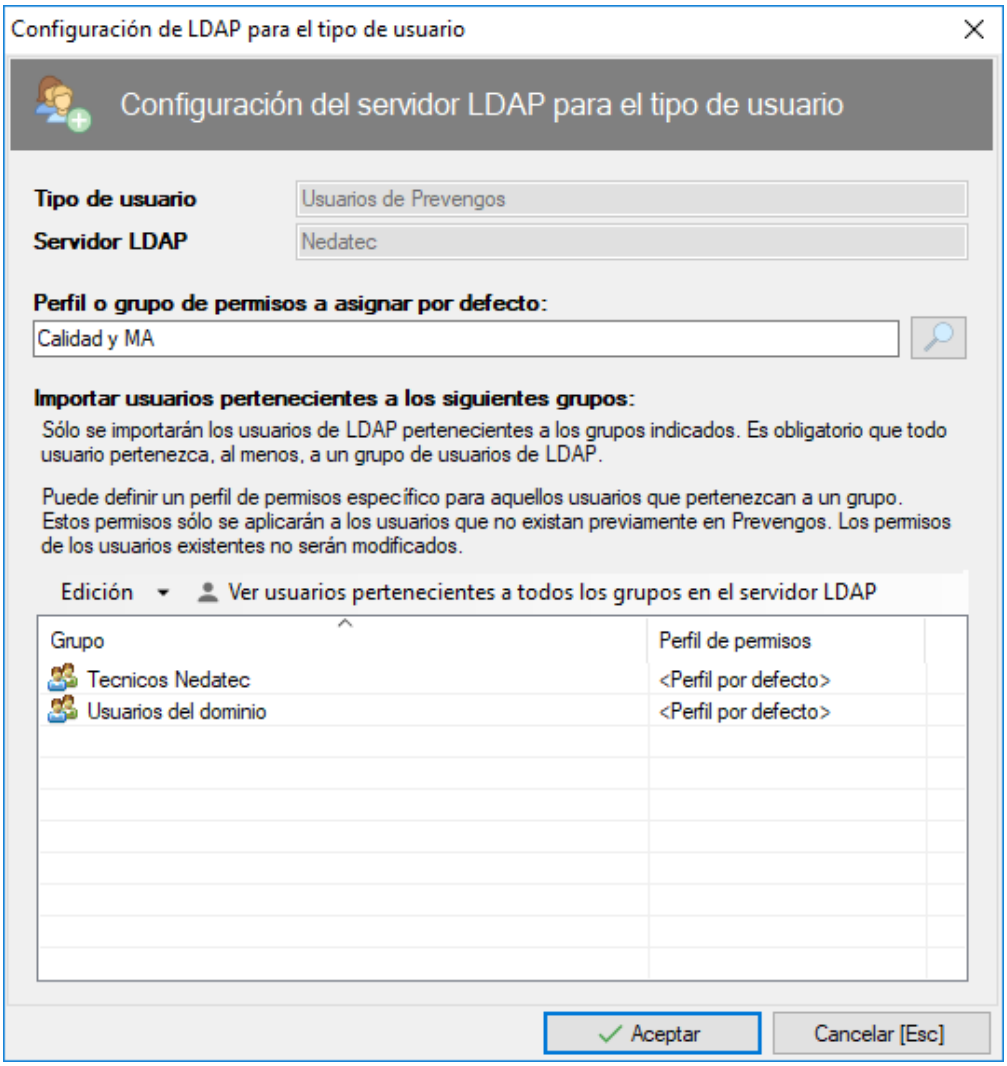
Debido a que podemos tener varios “tipos” de usuario dentro del directorio LDAP, se hace necesario vincular y configurar cada servidor LDAP con cada tipo o rol de usuario en Prevengos. Esta configuración consiste básicamente en indicar qué permisos se van a establecer por defecto en el caso de tener que crear nuevos usuarios así como qué grupos de usuarios de LDAP serán tenidos en cuenta.

Habilitar la sincronización automática de usuarios de Prevengos a través de LDAP

Si habilita esta opción, cada vez que se logue un usuario en el aplicativo, se leerá el listado de usuarios de LDAP pertenecientes a los grupos configurados (según el rol) e intentará asociar cada usuario automáticamente por su Login. En el caso de crear usuarios en Prevengos, éstos se crearán sin contraseña. Deberá asignarla manualmente bien, en el Panel de Control de Prevengos si son usuarios de Prevengos o dentro de la administración web en caso de ser usuarios Web.



Pantalla general



Datos de configuración

3.2.3. Gestión de usuarios

En este apartado visualizará los usuarios de LDAP disponibles según la configuración establecida. Puede visualizar los usuarios según LDAP o según Prevengos. Sea cual sea la vista que utilice, deberá vincular cada usuario de LDAP con el usuario en Prevengos.

Las herramientas de las que dispone en esta sección son:

- **Leer usuarios de LDAP**
  Lee usuarios de LDAP disponibles para el tipo de usuario indicado. No genera Login de usuario ni “casa” cada usuario de LDAP con el usuario en Prevengos. Únicamente actualiza el listado de usuarios disponibles en los servidores LDAP.

- **Vincular/desvincular usuario de LDAP**
  Esta herramienta elimina la vinculación entre el usuario de LDAP y el usuario en Prevengos.

- **Activar/desactivar la sincronización de los usuarios LDAP selecionados**
  Esta herramienta sirve para no tener en cuenta el usuario seleccionado. Es decir, si marca un usuario como que NO se va a sincronizar, será omitido en todos los procesos. Esta herramienta sirve únicamente para no tener en cuenta ciertos usuarios que pueden cumplir con todos los filtros pero no queremos que sean

tenidos en cuenta para la aplicación. Por defecto, todos los usuarios se tienen en cuenta.

- **Asociar automáticamente todos los usuarios de LDAP con los usuarios web/Prevengos**
  Esta herramienta sirve para asociar automáticamente cada usuario LDAP con el usuario en Prevengos (ya sea un usuario web o un usuario de Prevengos según los usuarios que se estén gestionando). La casación de estos usuarios se realizará por Login. Buscará en la base de datos si existe un usuario con el mismo Login y en caso de existir lo vinculará. En caso contrario, lo creará si así se indica.

3.3. Autenticación con Windows

Sólo disponible para usuarios de PREVENGOS (no es válido para usuarios WEB)

Cuando se utiliza este modo de autenticación, el aplicativo no solicitará al usuario sus credenciales. Se cogerá el usuario de Windows y se contrastará contra todos los servidores LDAP configurados (como se ha indicado en el *apartado 3.2.*). En caso de ser un usuario existente y de alta en el directorio LDAP la autenticación será satisfactoria. Además, dicho el usuario del directorio LDAP deberá estar debidamente vinculado con un usuario en Prevengos.

Debido a las limitaciones de navegadores, esta implementación no está disponible para el portal web.

3.4. SSO (OAuth2 - SAML 2.0)

Los protocolos SAML 2.0 y OAuth2 para Azure y Google permiten realizar el inicio de sesión único en las aplicaciones de Prevengos (Prevengos Central, PrevengosWeb, WebApp y PrevengosControlAccesos). Los usuarios web en Prevengos se crearán automáticamente la primera vez que intente acceder dicho usuario al portal.

Información general

SAML son las siglas de Security Assertion Markup Language. Está diseñado para autenticar a un usuario, por lo que proporciona datos de identidad del usuario a un servicio mientras que OAuth está diseñado como un protocolo de autorización que permite a un usuario compartir el acceso a recursos específicos con un proveedor de servicios.

SAML se suele utilizar para el SSO en aplicaciones gubernamentales y empresariales (gestión de identidades), donde el procesamiento de XML por parte del sistema backend es habitual. SAML se utiliza principalmente en escenarios SSO basados en web.

OAuth son las siglas de Open Authorization. Es un estándar abierto que permite a los usuarios conceder permiso a aplicaciones de terceros para acceder a sus datos y/o realizar acciones en su nombre sin compartir sus credenciales. Se utiliza ampliamente en aplicaciones de consumo y empresariales, tanto en roles de autorización como de autenticación.

Desde un punto de vista técnico, SAML define un formato de token, su cifrado es complejo y el tamaño de los mensajes intercambiados es significativo mientras que OAuth2 no utiliza ningún tipo de cifrado (se basa en HTTPS) y no define un formato de token.

OAuth2 puede utilizarse en dispositivos móviles, dispositivos inteligentes, aplicaciones web, aplicaciones de una sola página, etc. SAML, en cambio, no se diseñó teniendo en cuenta la variedad de aplicaciones existentes y es por ello que se suele utilizar sólo en aplicaciones web.

Implementación en Prevengos

- OAuth2

La implementación de OAuth requiere la creación de las aplicaciones de Prevengos (Prevengos, PrevengosWeb, WebApp…) en el portal correspondiente (Azure o Google). También será necesario crear grupos (grupos de seguridad) para incluir a los usuarios que tiene acceso a dichas aplicaciones, por ejemplo, podríamos crear el grupo “PrevengosWeb – Trabajador” donde incluiríamos a todos los trabajadores que tienen acceso a la aplicación “PrevengosWeb”

Una vez configuradas las aplicaciones se deberá indicar en el aplicativo Prevengos el modo de autenticación, ya sea SSO Azure o SSO Google e indicar los datos de las aplicaciones creadas en el portal.

Las aplicaciones de Prevengos se conectarán via API a Azure o a Google para obtener la información del usuario conectado para lo cual, en algunos casos, se deberá dar permisos de acceso a algunas APIs.

- SAML 2.0

La implementación de SAML requiere la creación de las aplicaciones de Prevengos (Prevengos, PrevengosWeb, WebApp…) en el portal correspondiente (Azure, Google, …). Prevengos facilitará los datos de la url ACS y el ID de la entidad.

Al igual que en el caso de OAuth se deberán crear grupos donde incluir a los usuarios que tengan acceso a dichas aplicaciones. Pero, a diferencia de la implementación mediante OAuth será SALM quien comunique la información del usuario conectado a las aplicaciones mediante la creación de “atributos y reclamaciones” del propio protocolo siendo necesario definir los atributos Nombre, Apellidos, Email, Teléfono, DNI y Grupos asociados al usuario.

Una vez configurado SAML en el portal se deberá configurar en Prevengos el tipo de autenticación SAML e indicar los datos de la aplicación creada en el portal (url de login, url de logout, etc)

Importancia de las Aplicaciones y Grupos (perfiles de usuario) **en Prevengos**

Por cada aplicación de Prevengos se crearán aplicaciones en Azure y Google para autorizar el acceso por SSO

Prevengos		Azure
Prevengos Central	→	Prevengos
Prevengos Web	→	Prevengos Web
Prevengos Contratas*	→	Prevengos Contratas
Prevengos Control de Accesos	→	Prevengos Control de Accesos
Prevengos WebApp	→	Prevengos WebApp

Los datos de cada una de las aplicaciones de Azure y Google formarán parte de la configuración del SSO para configurar Prevengos.

Cualquier usuario con acceso a la aplicación de Azure y Google podrá acceder a la aplicación asociada en Prevengos a la cual se le podrá asignar un PERFIL POR DEFECTO de forma que todos los usuarios asignados

puedan acceder con dicho perfil.

También se podrán definir GRUPOS a los que asociar los perfiles de acceso de forma que los usuarios asociados a esos grupos podrán acceder a las aplicaciones de prevengos con los permisos especificados en dichos perfiles

Se podrán definir tantos grupos en Azure y Google como se desee y desde la configuración de Prevengos se asignará un PERFIL DE ACCESO a cada uno de esos GRUPOS.

Como caso particular tenemos el caso de la Web de Empresa/Centro/Trabajador ya que podremos configurar, por defecto, que todos los usuarios que accedan a la aplicación tengan perfil trabajador y, además, asignando grupos, podríamos hacer que alguno de esos trabajadores tenga rol de empresa o centro.

Por ejemplo, podremos crear los grupos “PrevengosWeb – Empresa” y “PrevengosWeb – Trabajador” asociando “PrevengosWeb – Empresa” a un perfil de rol Empresa mientras el grupo “PrevengosWeb – Trabajador” lo asociamos a un perfil de rol trabajador en Prevengos, de este modo un usuario que esté en ambos grupos podrá acceder a la aplicación “PrevengosWeb” tanto como empresa como trabajador y tendrá los permisos asociados al perfil indicado.

Sí sólo lo incluimos en el grupo “PrevengosWeb – Trabajador” sólo podrá acceder a la web con el rol trabajador.

Si tenemos varios tipos de trabajadores y a cada uno queremos asignarle permisos de acceso diferentes podríamos crear grupos para dichos trabajadores, por ejemplo, “PrevengosWeb – Formación Trabajadores” y “PrevengosWeb – Reconocimientos Trabajadores” en ambos casos asociaríamos estos grupos con un perfil de rol trabajador, pero serían perfiles diferentes, cada uno con permisos específicos para el acceso a las distintas áreas de la web.

Los perfiles de acceso dependerán de la aplicación, por lo que para vincular un grupo con un perfil se tendrá que definir a que aplicación pertenece el perfil de forma que se mostrarán perfiles de Prevengos Central o bien perfiles Web de distintos roles.

Aplicación	Grupo	Perfil
Prevengos Central		Técnicos
Prevengos Web		(ninguno)
	Prevengos Empresa	Perfil completo
	Prevengos Centro	Centro. Planificacion
	Prevengos Trabajador	Trabajador Acceso Completo
Prevengos WebApp		Técnicos WebApp

En Azure y Google los grupos NO están vinculados a aplicaciones, pero, por ejemplo, se podría hacer que los usuarios, Usuario1, Usuario2, Usuario3 y Usuario4 tengan acceso a la aplicación Prevengos y sólo Usuario2 y Usuario3 accedieran a la aplicación Prevengos WebApp especificando en ambos usuarios un TIPO DE PERFIL DIFERENTE.

Además, podría configurar que los usuarios Trabajador1, Trabajador2, Trabajador3, Trabajador4 accedieran a la aplicación Prevengos Web con PERFIL TRABAJADOR y sólo Trabajador2 accediera también como PERFIL EMPRESA al incluirlo en el grupo de Prevengos Empresa de Azure o Google.

Si quisiera que Trabajador2 no pudiera entrar como trabajador, pero si como empresa tendría que dar acceso a los cuatro trabajadores, pero sin establecer perfil por defecto ya que lo tendría que obtener del grupo al que pertenecen, de esta forma incluiría en el grupo “Prevengos Trabajador” a Trabajador1, Trabajador3 y Trabajador4 y en el grupo “Prevengos Empresa” a Trabajador2

Una vez identificado el usuario del SSO conectado tendremos también sus perfiles de Prevengos asociados (bien por tener perfil por defecto para la aplicación o bien por pertenecer a un grupo)

En el caso de Prevengos Central sólo pueden acceder técnicos por lo que buscaremos en la tabla de usuarios los usuarios cuyo login sea el identificador de Azure o Google(ya sea DNI o email).

> *Si existe se permitirá el acceso con dicho usuario.*
>
> *En caso de no existir se creará el usuario según el perfil definido por la aplicación o el grupo al que pertenezca.*

Este proceso será similar en el resto de aplicaciones Web, pero se filtrará por el rol indicado por el perfil del usuario.

> *Si un usuario de Azure o Google accede a PrevengosWeb y tiene tres perfiles asociados se creará un grupo con tres usuarios (uno por cada rol). El login del grupo será el identificador de Azure o Google (DNI o email).*

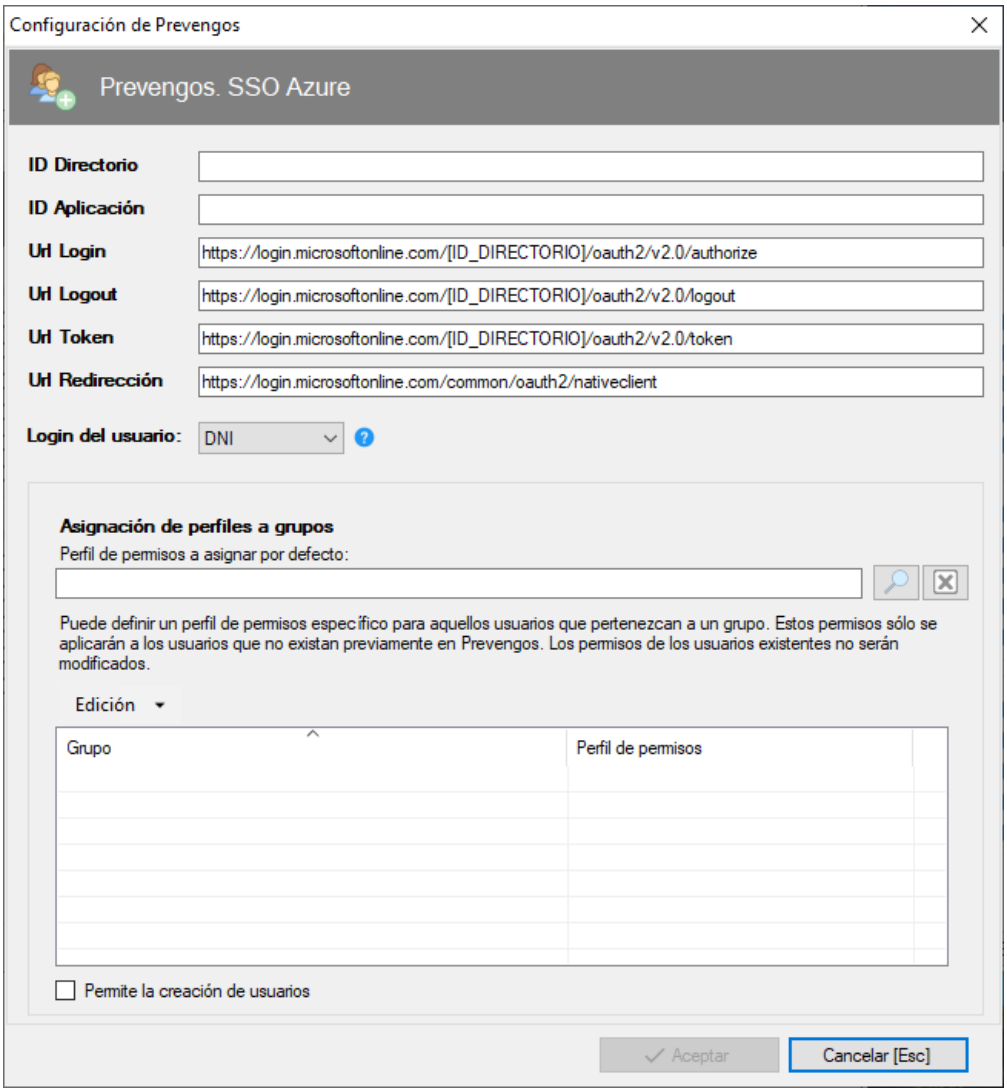
Si un mismo usuario del SSO está en dos grupos asociados a perfiles del mismo rol se utilizará el perfil más permisivo ya que solo pueden tener un usuario de un tipo en cada grupo.

Desde Prevengos se podrán modificar los permisos asociados a los usuarios independientemente de lo que tengan asignado en el SSO e incluso se podrá crear un grupo asociado al usuario para, por ejemplo, permitirle el acceso a otras empresas o centros.

3.4.1. SSO Azure

Para permitir el SSO con protocolo OAuth2 mediante Azure (Microsoft) se deberán crear “aplicaciones” dentro del directorio activo de la empresa (Microsoft Entra ID) en el *portal de Azure*, con sus usuarios y grupos.

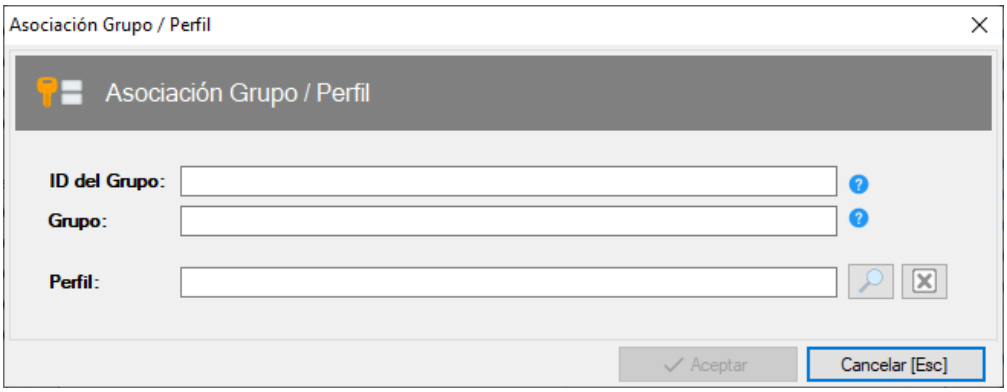
Tras pulsar en el icono , accede al siguiente formulario para configurar los datos de dicha aplicación:



Aquí tendrá que indicar la **ID Directorio** e **ID Aplicación**, generados al crear la aplicación, así como el como el campo **Login del usuario** entre DNI o Email.

En los campos **Url Login**, **Url Logout** y **Url Token** ha de susituir la etiqueta *[ID_DIRECTORIO]* con el valor correspondiente al campo **ID Directorio**.

Para la asignación de perfiles a los grupos de la aplicación use el menú *Edición* > *Añadir grupo*:



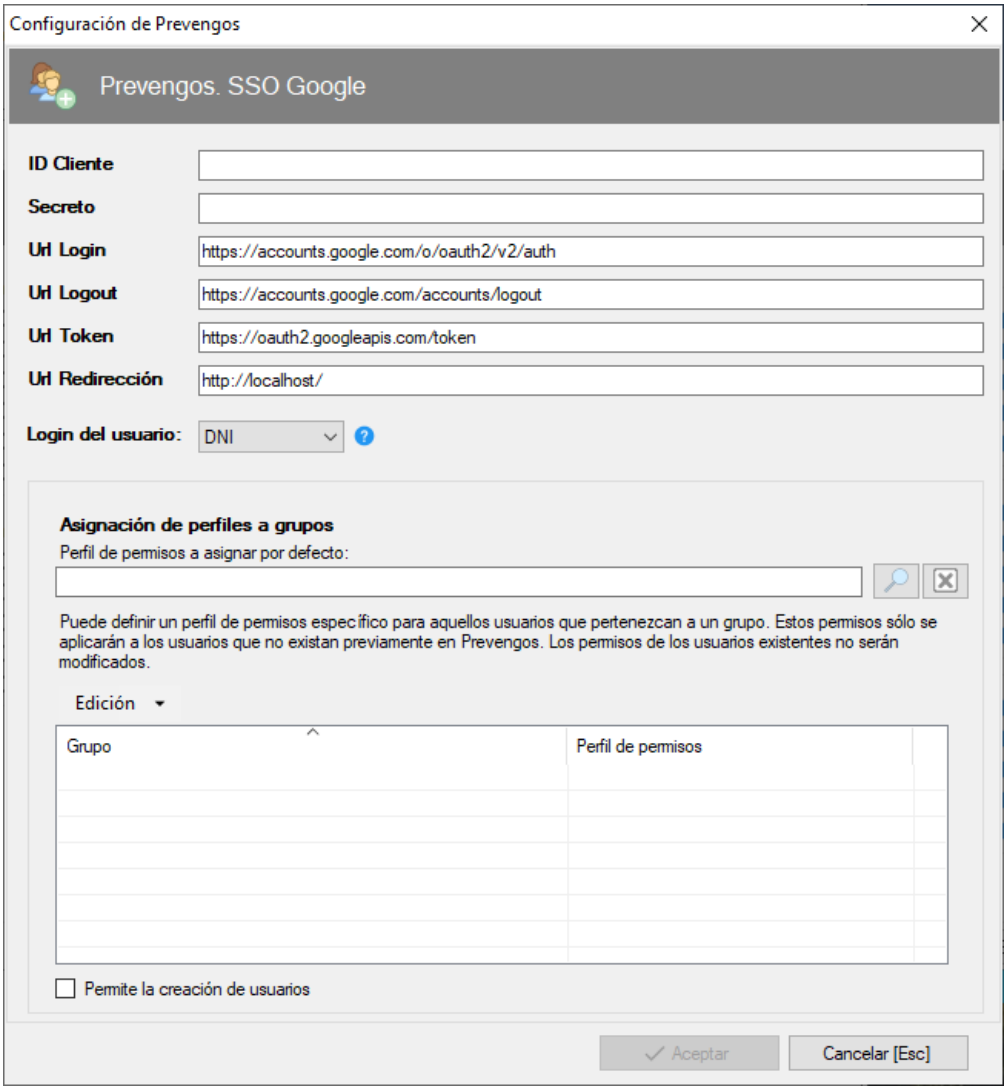
Aquí debe indicar la ID del grupo, nombre del mismo y seleccionar el perfil de Prevengos a asignar.

Este modo de autenticación también es válido para los usuarios web.

3.4.2. SSO Google

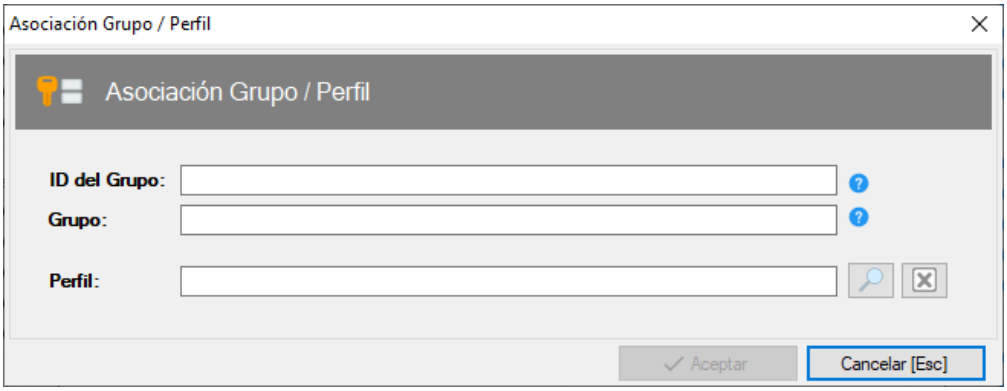
Para permitir el SSO con protocolo OAuth2 mediante Google se deberán crear “aplicaciones” en la *consola de administración de Google*, con sus usuarios y grupos.

Tras pulsar en el icono , accede al siguiente formulario para configurar los datos de dicha aplicación:



Aquí tendrá que indicar la **ID Cliente** y **Secreto de cliente**, generados al crear la aplicación, así como el como el campo **Login del usuario** entre DNI o Email.

Para la asignación de perfiles a los grupos de la aplicación use el menú *Edición* > *Añadir grupo*:



Aquí debe indicar la ID del grupo, nombre del mismo y seleccionar el perfil de Prevengos a asignar.

Este modo de autenticación también es válido para los usuarios web.

3.4.3. SAML (Security Assertion Markup Language)

Para permitir el SAML deben crear las aplicaciones SAML en el *portal de Azure* o en la *consola de administración de Google*, con sus usuarios y grupos.

Para todas las aplicaciones creadas hay que indicar el siguiente mapeo de atributos: ***Nombre, Apellidos, DNI, Email, TelefonoMovil y Grupos.***

Ejemplos de mapeo de atributos en Azure y Google:

AZURE:

- Nombre = user.givenname
- Apellidos = user.surname
- DNI = user.employeeid
- Email = user.mail
- TelefonoMovil = user.mobilephone
- Grupos = user.groups (notificación de grupo)

***Importante*:**

Azure devuelve el ID del grupo por lo que la vinculación con el perfil se hace por ID.

Se debe definir que grupos de los usuarios se envía via SAML en función de la seguridad aplicada en Azure, por lo general habrá que indicar “Todos los grupos” o bien “Grupos de seguridad” o “Grupos asignados a la aplicación”. Si no se envía ningún grupo no se podrá acceder a la aplicación de Prevengos.

El “espacio de nombres” debe dejarse en blanco

Los campos notificados vía SAML “Nombre”, “Apellidos”, “DNI”, “Email”, “TelefonoMovil”, “Grupos” deben escribise “tal cual” . Notese que “TelefonoMovil” no tiene acento.

GOOGLE:

- Nombre = First name
- Apellidos = Last name
- DNI = Employee ID
- Email = Primary email
- TelefonoMovil = Phone number

- Grupos = Indicar los grupos que pueden ser enviados via SAML, por ejemplo “Prevengos Admin”, “Prevengos Tecnico”, etc

***Importante*:**

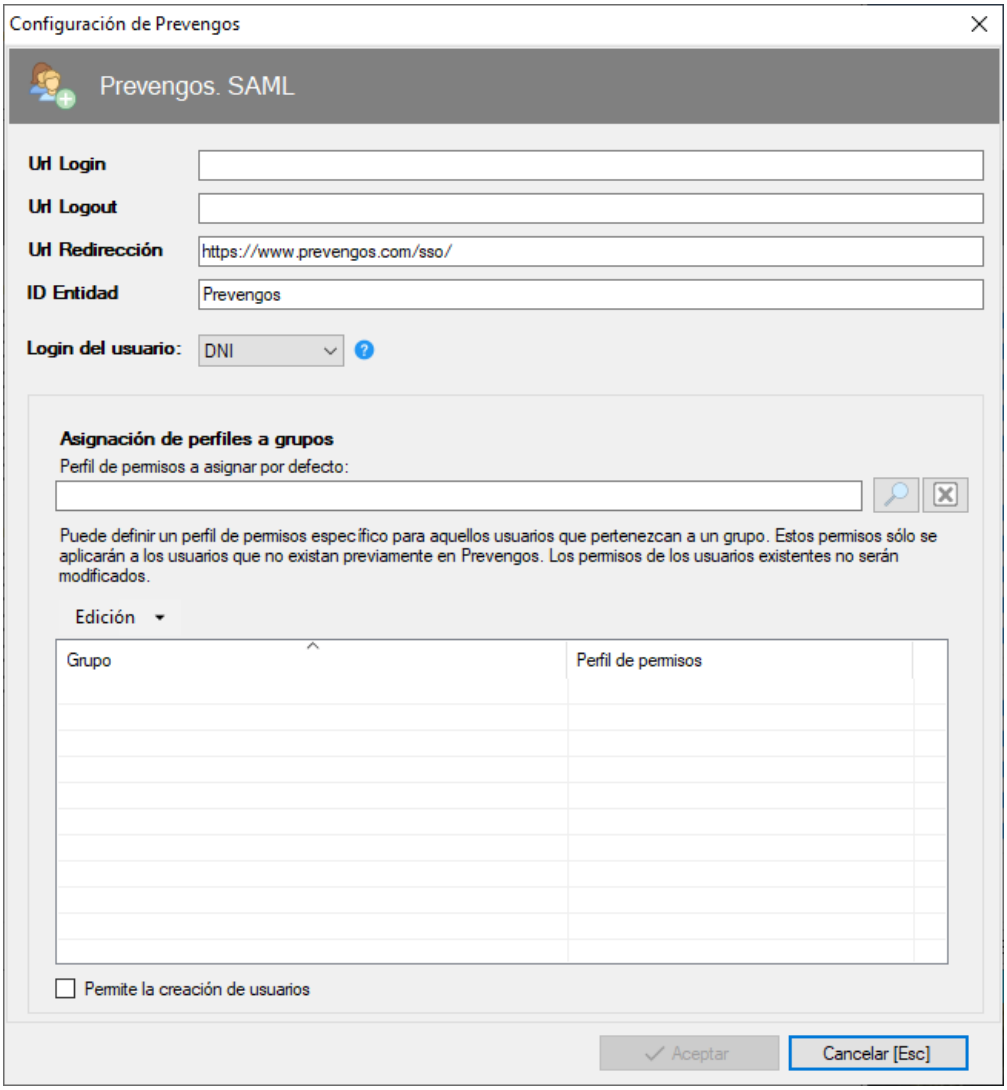
Google no permite indicar que campo se vincula al grupo por lo que siempre se envía via SAML el nombre del grupo por lo que el campo sIDGrupo será el propio nombre del grupo.
Los campos notificados vía SAML “Nombre”, “Apellidos”, “DNI”, “Email”, “TelefonoMovil”, “Grupos” deben escribise “tal cual”. Notese que “TelefonoMovil” no tiene acento.

Pertenencia a los grupos

Para cada aplicación se deben indicar los grupos que tienen acceso y en Prevengos vincular dichos grupos con los perfiles correspondientes. El atributo de la aplicación sea “Grupos”.

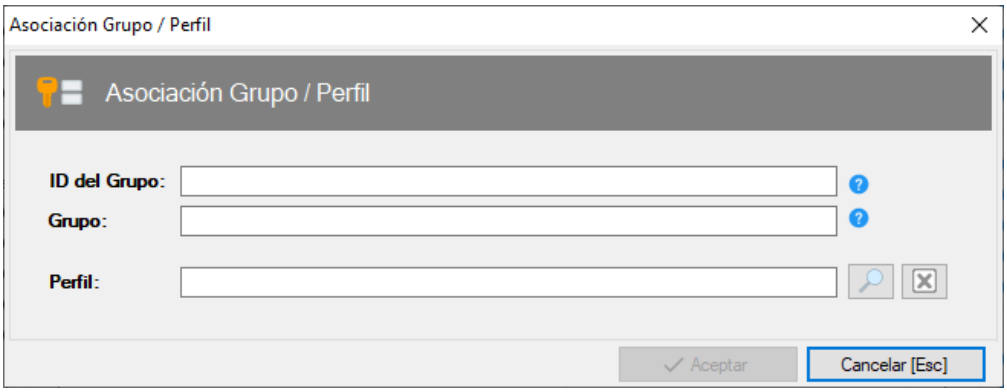
Por ejemplo para Prevengos se pueden definir los grupos “Prevengos Admin”, “Prevengos Tecnico”
Para Prevengos Web: “PrevengosWeb Empresa”, “PrevengosWeb Trabajador”, “PrevengosWeb Centro”…

Tras pulsar en el icono , accede al siguiente formulario para configurar los datos de dicha aplicación:



Aquí tendrá que indicar las URLs de la aplicación para inicio de sesión, **Url Login**, y cierre, **Url Logout**, así como el como el campo **Login del usuario** entre DNI o Email.

Para la asignación de perfiles a los grupos de la aplicación SAML, use el menú *Edición* > *Añadir grupo*:



Aquí debe indicar la ID del grupo, nombre del mismo y seleccionar el perfil de Prevengos a asignar.

Este modo de autenticación también es válido para los usuarios web.