

Saturn Studio – Credencial Slack



¿Qué es Slack?

Slack es una plataforma de comunicación empresarial basada en canales que centraliza conversaciones, archivos y herramientas en un solo lugar. Permite a los equipos colaborar en tiempo real, integrar servicios externos y automatizar flujos de trabajo mediante aplicaciones personalizadas, facilitando la gestión de proyectos y la comunicación interna de forma organizada.

Cómo obtener el Client ID y el Client Secret

Para integrar Slack con **Saturn Studio**, es necesario registrar una aplicación en el portal de desarrolladores de Slack para obtener las credenciales de acceso.

1. Acceso desde el módulo

- Dentro del módulo de Saturn Studio, haz clic en el enlace **“here”** ubicado debajo de los campos de credenciales.
- Esto te redirigirá automáticamente al sitio oficial de **Slack API**.

2. Creación de la Aplicación

- Una vez en el sitio y tras haber iniciado sesión, selecciona la opción para crear una nueva aplicación.
- En la ventana emergente **“Create an app”**, elige la opción **“From scratch”** para configurar manualmente la información básica y los permisos.
- Asigna un nombre a tu aplicación y selecciona el **Workspace (canal principal)** donde se instalará la integración.

Create an app ×

Choose how you'd like to configure your app's scopes and settings.

From a manifest

Use a manifest file to add your app's basic info, scopes, settings & features to your app. >

From scratch

Use our configuration UI to manually add basic info, scopes, settings, & features to your app. >

Need help? Check our [documentation](#), or [see an example](#)

3. Localización de Credenciales

Basic Information

App Credentials

These credentials allow your app to access the Slack API. They are secret. Please don't share your app credentials with anyone, include them in public code repositories, or store them in insecure ways.

- Tras crear la app, el sistema te dirigirá a la sección **“Basic Information”**.
- Desliza hacia abajo hasta encontrar el apartado **“App Credentials”**, donde verás que estas llaves permiten a tu app acceder a la API de Slack.
- Aquí encontrarás el **Client ID** y el **Client Secret**.
- Para visualizar el **Client Secret**, haz clic en el botón **“Show”**.
- Copia ambos valores y pégalos en los campos correspondientes dentro del módulo de Saturn Studio.

Client Secret

.....

Show

Regenerate

You'll need to send this secret along with your client ID when making your [oauth.v2.access](#) request.

Signing Secret

.....

Show

Regenerate

Slack signs the requests we send you using this secret. Confirm that each request comes from Slack by verifying its unique signature.

Resumen de Credenciales para Saturn Studio

Dato Requerido	Ubicación en Slack API	Notas de Seguridad
Client ID	Basic Information > App Credentials	Identificador público de la aplicación.
Client Secret	Basic Information > App Credentials	Es una clave secreta; no debe compartirse públicamente.

Importante: Las credenciales de la aplicación son secretas. No las incluyas en repositorios de código públicos ni las almacenes de forma insegura para evitar accesos no autorizados a tu Workspace de Slack.

[Saturn Studio – Credencial Supabase](#)



¿Qué es Supabase?

Supabase es una plataforma de desarrollo backend de código abierto que sirve como alternativa a Firebase. Proporciona una base de datos **PostgreSQL** completa, herramientas de autenticación, almacenamiento de archivos, funciones en el borde (Edge Functions) y, lo más importante, genera automáticamente **APIs REST y GraphQL** para que puedas interactuar con tus datos de forma inmediata.

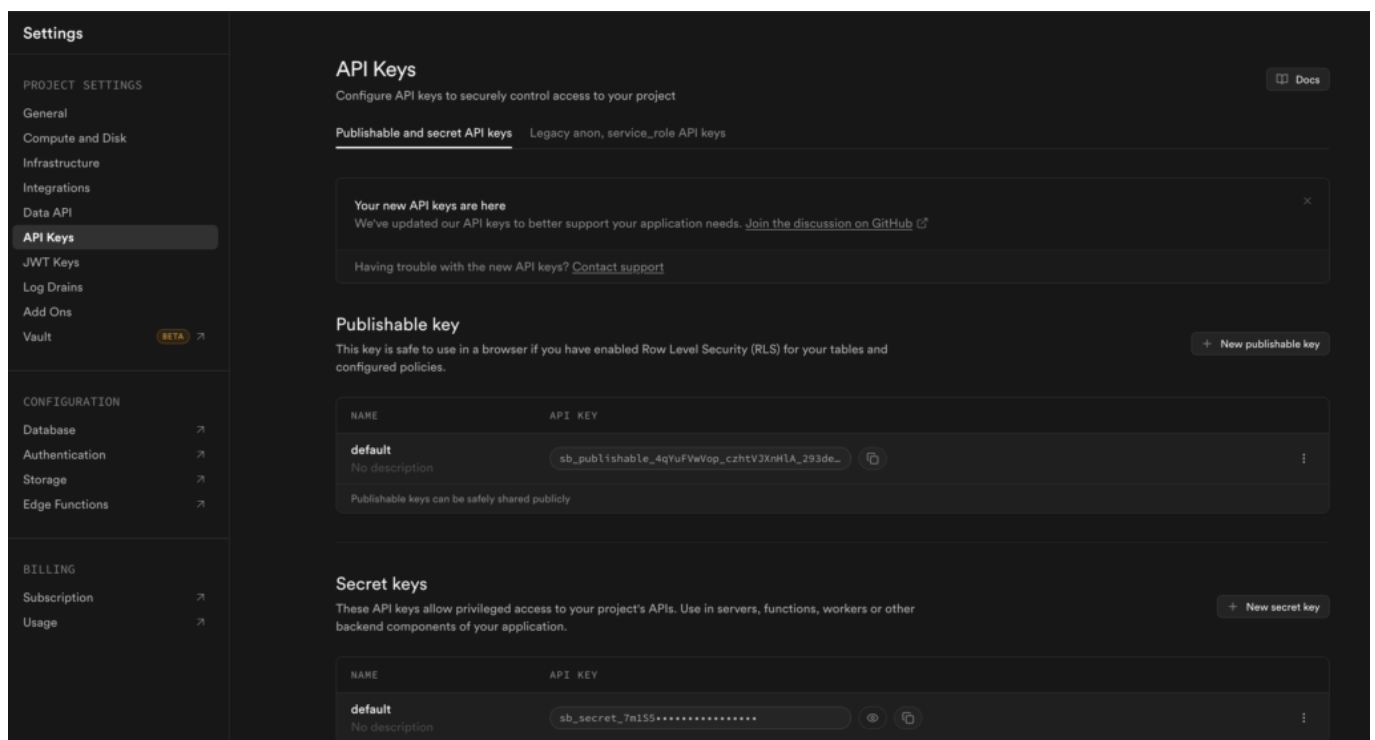
Cómo obtener la API Key y la URL en Supabase

Para vincular el módulo de **Saturn Studio** con tu base de datos, debes seguir estos pasos para extraer las credenciales desde el panel de control de Supabase.

1. Obtención de la API Key

La API Key permite a Saturn Studio realizar operaciones en tu nombre.

- **Acceso:** Haz clic en el enlace que aparece en el módulo de Saturn Studio para ir al sitio oficial de Supabase.
- **Proyecto:** Inicia sesión y selecciona el proyecto que deseas integrar (o crea uno nuevo).
- **Configuración:** Dirígete al menú lateral izquierdo y selecciona el icono de engranaje (**Project Settings**).
- **API Keys:** Dentro de los ajustes, busca la sección **API**. Allí verás el apartado **API Keys**.
- **Copia:** Puedes usar la clave anon (pública) o generar una nueva según las necesidades de tu flujo de trabajo.

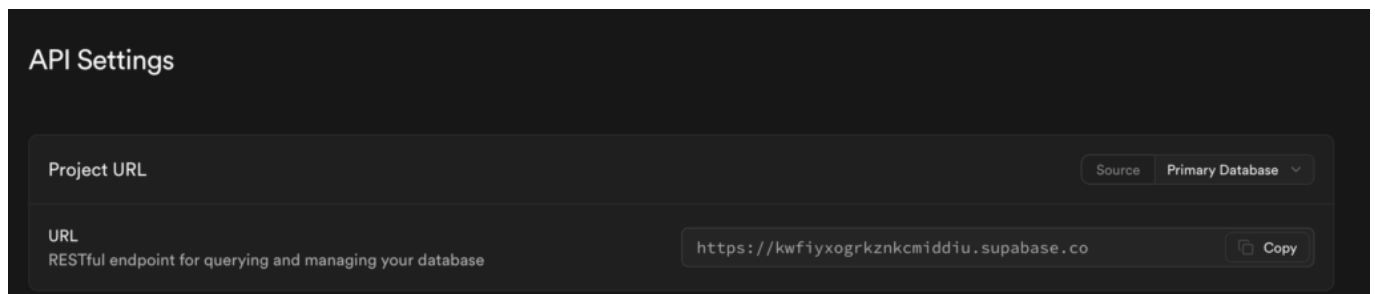


2. Obtención de la URL del Proyecto

La URL es la dirección única donde “vive” la API de tu proyecto.

- **Navegación:** Dentro de la misma pantalla de **Project Settings**, localiza en el submenú lateral la opción **Data API**.
- **Localización:** En la parte superior verás el campo **Project URL**.
- **Copia:** Copia la dirección que termina en .supabase.co para pegarla en la

configuración de Saturn Studio.



Resumen de Credenciales para Saturn Studio

Dato Requerido Ruta en el Panel de Supabase **Ejemplo de Formato**

Project URL Settings > Data API > URL `https://xyz.supabase.co`

API Key Settings > API > API Keys `sb_publishable_...`

[Saturn Studio – Credencial OpenRouter](#)



¿Qué es OpenRouter?

OpenRouter es una plataforma que ofrece una interfaz unificada para acceder a modelos de lenguaje (LLMs) de múltiples proveedores desde una sola API. Permite utilizar más de 300 modelos distintos, comparar precios, optimizar costos y mejorar la disponibilidad sin necesidad de gestionar múltiples integraciones.

Saturn Studio utiliza OpenRouter para conectarse a estos modelos de inteligencia artificial mediante una única credencial.

Cómo obtener la API Key de OpenRouter

The Unified Interface For LLMs

Better [prices](#), better [uptime](#), no subscriptions.

Get API Key

Explore Models 

25T

Monthly Tokens

5M+

Global Users

60+

Active Providers

300+

Models

Para configurar la credencial de OpenRouter en Saturn Studio es necesario generar una API Key desde la plataforma oficial de OpenRouter.

El proceso es el siguiente:

1. Desde la configuración de la credencial en Saturn Studio, hacer clic en el enlace directo incluido en el campo **OpenRouter API Key**.
2. El enlace redirige al sitio oficial de OpenRouter.
3. Iniciar sesión o crear una cuenta en OpenRouter.
4. Una vez dentro de la plataforma, acceder a la sección de API Keys.
5. Crear una nueva API Key.
6. Asignar un nombre identificador a la API Key.
7. Configurar los límites de uso o tokens según sea necesario.
8. Guardar la configuración.
9. OpenRouter generará automáticamente la API Key.
10. Copiar la API Key generada y pegarla en el campo **OpenRouter API Key** dentro de Saturn Studio.

API Keys

Create API Key



No API keys yet

Create your first API key to start using OpenRouter



Name ⓘ

Saturn Studio Key

Credit limit (optional) ⓘ

Leave blank for unlimited

Reset limit every... ⓘ

N/A



Expiration ⓘ

No expiration



Create



Your new key:

sk-or-v1-96b4f20084073b4425bf9e8692073dd79t



Please copy it now and write it down somewhere safe. **You will not be able to see it again.**

You can use it with OpenAI-compatible apps, or
[your own code](#)

Luego de ingresar la clave, se puede utilizar el botón **Check** para validar la conexión antes de guardar la credencial.

[Saturn Studio – Credencial Google Meet](#)



Google Meet

Este documento explica cómo integrar y autenticar el módulo **Google Meet** dentro de **Saturn Studio**, permitiendo acceder, crear y administrar reuniones de forma segura.

La integración puede realizarse mediante dos métodos **OAuth 2.0 con Google**

Cloud.

Configuración OAuth 2.0 con Google Cloud

Este método brinda mayor control sobre los permisos y seguridad, ideal para entornos de trabajo colaborativos o producción.

Crear / elegir proyecto y habilitar APIs

- Ingresa a [Google Cloud Console](#).
- Inicia sesión con tu cuenta de Google.
- Crea un nuevo proyecto o selecciona uno existente desde la barra superior.

Notificaciones



Crear proyecto: My First Project

hace 4 minutos

[Seleccionar proyecto](#)

[Ver todas las actividades](#)

- Desde la barra de búsqueda, busca y habilita las siguientes API:
 - **Google Meet API** (requerida para crear, obtener y modificar reuniones de meet)
 - **Google Calendar API** (requerida para consultar, editar, compartir y borrar todos los calendarios a los que puedes acceder a través del Calendario de Google)
- Verifica que la API quede con estado **Habilitado**.
Si no lo está, la autenticación podría completarse, pero las llamadas devolverán errores del tipo `access_not_configured`.



Google Meet REST API

[Google](#)

Habilitar

[Probar esta API](#)



Google Calendar API

[Google Enterprise API](#)

Manage calendars and events in Google Calendar.

Habilitar

[Probar esta API](#)

Configurar la Pantalla de consentimiento OAuth

- En el menú lateral, entra a:
APIs y servicios → Pantalla de consentimiento OAuth → Configurar pantalla de consentimiento.

Credenciales [+ Crear credenciales](#) [Borrar](#) [Restablecer credenciales borradas](#)

Crea credenciales para acceder a tus API habilitadas. [Más información](#)

Recuerda configurar la pantalla de consentimiento de OAuth con información sobre tu app. [Configurar pantalla de consentimiento](#)

Claves de API

☐	Nombre	Fecha de creación ↓	Restricciones	Acciones
No hay claves de API para mostrar				

IDs de clientes de OAuth 2.0

☐	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			

- Completa los campos solicitados:
 - **Nombre de la aplicación**
 - **Correo de soporte**
 - *(Opcional)* Logo, dominio, enlaces de privacidad y términos.

- Elige el tipo de usuario según tu caso:

Tipo de usuario	Descripción	Recomendación
Interno	Solo usuarios de tu organización (requiere dominio Google Workspace).	Úsalo si tu equipo pertenece al mismo dominio.
Externo	Permite acceso a cualquier cuenta de Google (modo de prueba).	Ideal para uso personal o con cuentas @gmail.com.

❏ **Nota:** en modo Externo (prueba) deberás agregar manualmente a los usuarios de prueba, incluido tu propio correo. Solo esos usuarios podrán autorizar la app mientras esté en prueba.

Guarda los cambios al finalizar.

✓ Información de la app

|

✓ Público

|

✓ Información de contacto

|

4 Finalizar

✓ Acepto la [política sobre los datos del usuario de los servicios de las APIs de Google](#). [↗](#)

Continuar

Crear

Cancelar

Agregar scopes (permisos) a la app

1. Desde la misma sección de **Pantalla de consentimiento OAuth**, ve a **Acceso a los datos** → **Agregar o quitar permisos**.

2. Añade los siguientes scopes recomendados:

Scope

`https://www.googleapis.com/auth/userinfo.email`

`openid`

`https://www.googleapis.com/auth/meetings.space.readonly`

`https://www.googleapis.com/auth/meetings.space.created`

`https://www.googleapis.com/auth/calendar`

Descripción

Accede al correo del usuario autenticado.

Requerido para la autenticación mediante OAuth 2.0.

Permite leer sobre cualquier espacio de reunión al que el usuario tenga acceso.

Permite crear, leer y modificar sobre los espacios de reuniones creados.

Permite Consultar, editar, compartir y borrar los calendarios a los que se pueden acceder a través del calendario de Google.

Actualiza y guarda los cambios.

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	Ver la dirección de correo electrónico principal de tu Cuenta de Google
☐	../auth/userinfo.profile	Permite ver su información personal, incluidos los datos personales que haya hecho públicos
☐	openid	Asociarlo con su información personal en Google
☐	Analytics Hub API ../auth/bigquery	View and manage your data in Google BigQuery and see the email address for your Google Account
☐	Analytics Hub API ../auth/cloud-platform	Ver, editar, configurar y borrar tus datos de Google Cloud y ver la dirección de correo electrónico de tu Cuenta de Google.
☐	BigQuery API ../auth/bigquery.readonly	Consultar tus datos en Google BigQuery.
☐	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".

Crear el Client ID y Client Secret

- Ve a **APIs y servicios** → **Credenciales** → **Crear credencial** → **ID de cliente de OAuth**.
- Completa los datos de la siguiente manera:

- **Tipo de aplicación:** Aplicación web
- **Nombre:** *Saturn Studio*
- **URIs de redirección:** <https://studio.rocketbot.com/>
- **URIs de redirección QA:** <https://qa-saturn.myrb.io/>

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

Nombre *

Saturn Studio

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

[+ Agregar URI](#)

URLs de redireccionamiento autorizados

Para usar con solicitudes de un servidor web

URI 1 *

<https://studio.rocketbot.com>

[+ Agregar URI](#)

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

[Crear](#)

[Cancelar](#)

- Al guardar, Google generará:
 - **Client ID**
 - **Client Secret**Cópioslos y resérvalos.

Se creó el cliente de OAuth

Se puede acceder al ID de cliente desde la pestaña Clientes en Google Auth Platform.



El acceso OAuth está restringido a los [usuarios de prueba](#) que aparecen en la [pantalla de consentimiento de OAuth](#)

ID de cliente



ap



A partir de junio de 2025, ya no podrás ver ni descargar el secreto del cliente una vez que cierres este diálogo. Asegúrate de haber copiado o descargado la información que aparece a continuación y de haberla almacenado de forma segura.

Secreto del cliente



Fecha de creación

18 de julio de 2025, 11:58:56 GMT-3

Estado

✓ Habilitada

⬇ Descargar JSON

Aceptar

Cargar credenciales en Saturn Studio

1. Regresa al módulo **Google Meet** en Saturn Studio y selecciona para crear una nueva credencial.
2. Pega el **Client ID** y **Client Secret** obtenidos en los campos correspondientes.

3. Guarda la credencial y realiza la conexión.

☐ **Listo:** tu credencial avanzada quedará configurada correctamente para el uso completo del módulo Google Meet.

☐ **Notas importantes**

- **Usuarios externos (modo de prueba):** agrega los correos de los usuarios en la lista de “Usuarios de prueba”. De lo contrario, no podrán autorizar la app.
- **Interno:** solo disponible con cuentas de dominio empresarial (Google Workspace).
- **Scopes y APIs:** los *scopes* otorgan permisos, pero las *APIs* *habilitadas* son las que permiten ejecutar las acciones.
- **URIs de redirección:** deben coincidir exactamente con la configuración de Google Cloud.
- **Verificación:** si deseas publicar la app (modo producción) y usas *scopes sensibles*, Google podría solicitar verificación del dominio, logo y políticas de privacidad.

Saturn Studio – Credencial Odoo



Las credenciales de **Odoo** permiten a Saturn Studio autenticarse contra una instancia de Odoo y ejecutar comandos del módulo (listar, obtener o crear registros en modelos).

Estas credenciales son obligatorias para utilizar cualquier acción del módulo Odoo.

Descripción

La credencial de Odoo utiliza autenticación mediante **usuario y contraseña**, asociada a una **base de datos específica** de una instancia de Odoo accesible por URL.

Campos requeridos

Odoo URL

Dirección base de la instancia de Odoo a la que se desea conectar.

Debe ser accesible desde Saturn Studio y corresponder al servidor donde se encuentra alojado Odoo.

Database

Nombre de la base de datos de Odoo contra la cual se realizará la autenticación.

Debe coincidir exactamente con el nombre configurado en la instancia de Odoo.

Username

Usuario de Odoo que se utilizará para la conexión.

El usuario debe existir en la base de datos indicada y contar con permisos sobre los modelos que se utilizarán desde el módulo.

Password

Contraseña correspondiente al usuario de Odoo especificado.

Se utiliza para validar la autenticación contra la instancia.

Validación de credenciales

El botón **Check** permite verificar que:

- La URL de Odoo sea accesible
- La base de datos exista
- El usuario y la contraseña sean válidos

Si la validación es exitosa, la credencial puede guardarse y utilizarse en los comandos del módulo.

Consideraciones

- El usuario configurado debe tener permisos adecuados sobre los modelos de Odoo que se vayan a consultar o modificar.
- La base de datos debe estar activa y accesible desde la instancia indicada.

Saturn Studio – Credencial Notion



Las credenciales de **Notion** permiten a Saturn Studio autenticarse contra la API de Notion para ejecutar los comandos del módulo, como crear bases de datos, crear páginas, obtener información o listar contenido.

Estas credenciales son obligatorias para utilizar cualquier comando del módulo Notion.

Descripción

La credencial de Notion utiliza un **Integration Token**, generado desde Notion, que autoriza a Saturn Studio a acceder a los espacios, páginas y bases de datos que hayan sido compartidos con la integración.

Campos requeridos

Notion Integrational Token

Token de autenticación generado desde Notion para una integración.

Este token identifica a la integración y define el nivel de acceso a los recursos de Notion que hayan sido compartidos explícitamente con ella.

Obtención del Integrational Token en Notion

Para obtener el token necesario:

1. Acceder a la sección de integraciones de Notion.
2. Crear una nueva integración.
3. Copiar el **Internal Integration Token** generado por Notion.
4. Utilizar ese token en el campo correspondiente de la credencial.



General

Perfil

Configuración

Estadísticas

Códigos promocionales

Aprender

Anuncios

Plantillas

Servicios

Integraciones

Integraciones

Crea, revisa y edita información y credenciales de desarrollo.

Las integraciones utilizan la API para acceder a las páginas, las bases de datos y los usuarios de Notion. [Obtén más información aquí.](#)

Ver todas ▾



Nueva integración



General

Perfil

Configuración

Estadísticas

Códigos promocionales

Aprender

Anuncios

Plantillas

Servicios

Integraciones

Nueva integración

Nombre de la integración *

Espacio de trabajo asociado *

Selecciona un espacio de trabajo en el que instalar la integración. Los propietarios del espacio de trabajo también podrán gestionar la integración y después podrás mejorarla para utilizar OAuth.

Tipo *

Puedes cambiar el tipo de integración en cualquier momento. Ten en cuenta que el cambio a integración pública puede requerir campos adicionales.

Logotipo



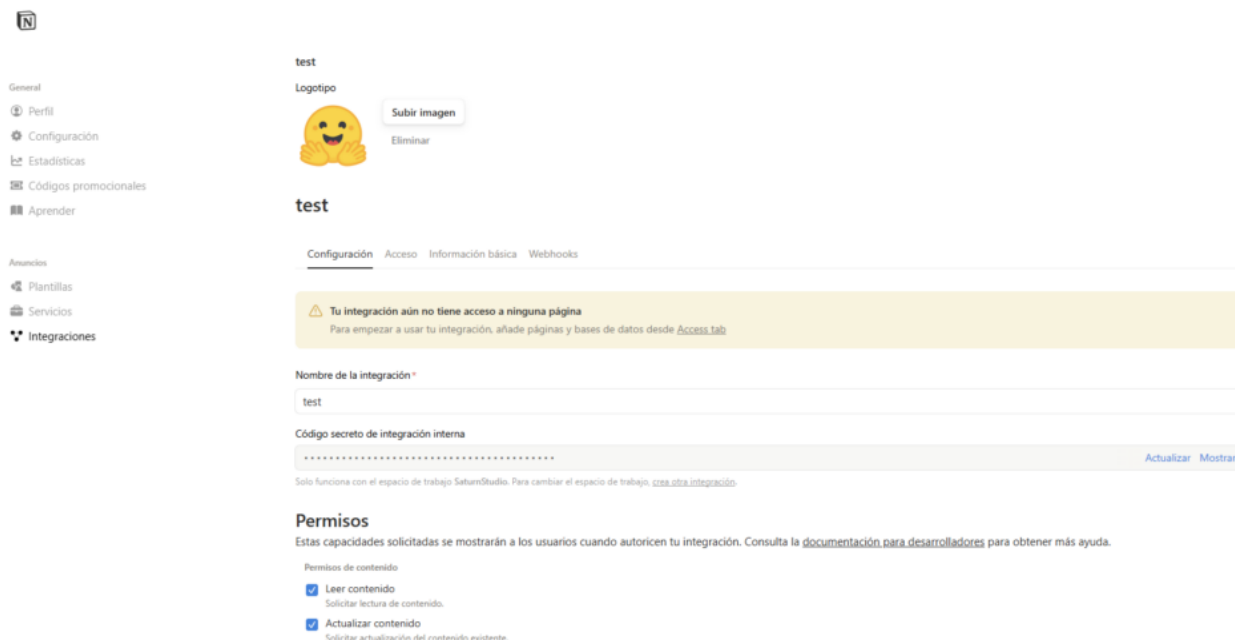
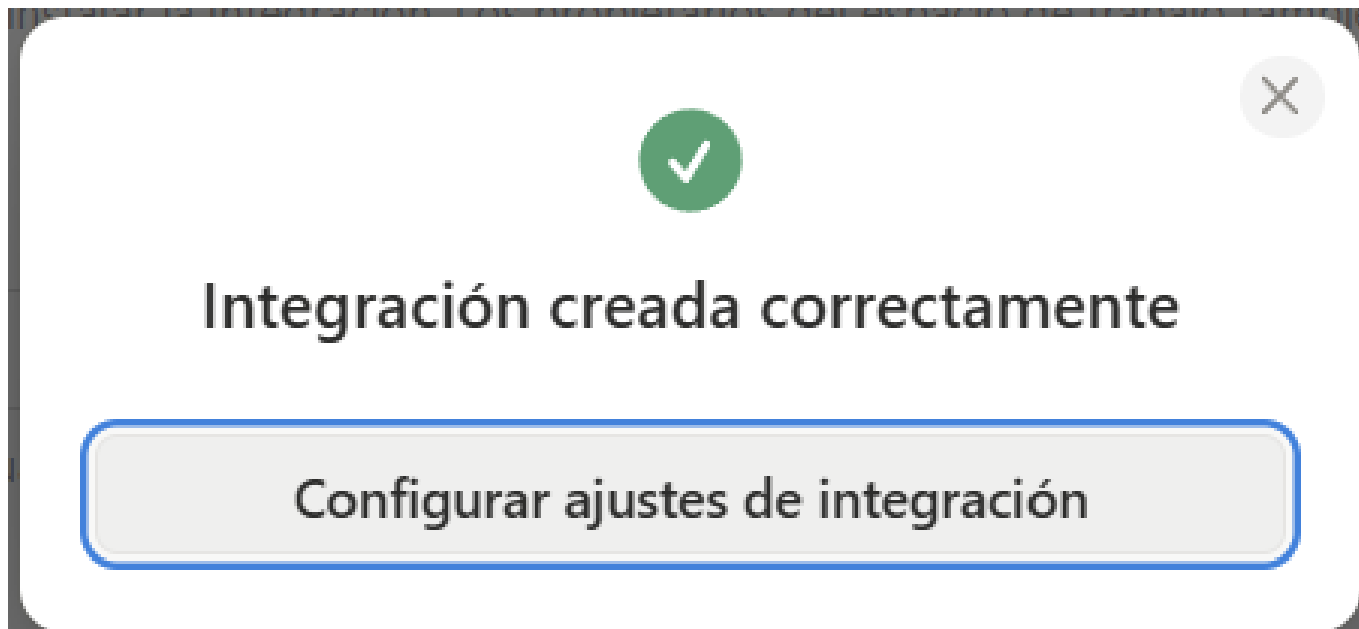
Subir

512 x 512

Al enviar, aceptas los [Términos de Notion para Desarrolladores](#).

Cancelar

Guardar



La integración debe permanecer activa para que la credencial funcione correctamente.

Permisos y acceso a contenido

- El Integration Token **no otorga acceso automático** a páginas ni bases de datos.
- Cada página o base de datos que se desee utilizar debe **agregarse manualmente a la integración** desde Notion.
- Para otorgar acceso, se debe ingresar a la página o base de datos en Notion y, desde el menú de opciones (•••), seleccionar **Add connections** y elegir la integración creada.
- Solo los recursos que hayan sido conectados explícitamente podrán ser utilizados por los comandos del módulo Notion.

Validación de credenciales

El botón **Check** permite verificar que el token:

- Sea válido
- No esté revocado
- Corresponda a una integración activa

Si la validación es exitosa, la credencial puede guardarse y utilizarse en los comandos del módulo Notion.

Consideraciones

- Se recomienda utilizar una integración dedicada para automatizaciones.
- Si el token es revocado o regenerado en Notion, la credencial deberá actualizarse.
- El acceso efectivo depende de los permisos otorgados a la integración dentro de Notion.

Saturn Studio – Credencial MongoDB



MongoDB es una base de datos NoSQL orientada a documentos, diseñada para almacenar y gestionar grandes volúmenes de datos de forma flexible y escalable. Utiliza documentos en formato JSON/BSON y permite operaciones rápidas de lectura y escritura.

Credencial de MongoDB

La credencial de MongoDB permite configurar la conexión a un servidor MongoDB para que los comandos del módulo puedan acceder a bases de datos y colecciones, realizar consultas, inserciones, actualizaciones y eliminaciones de documentos.

Esta credencial define el servidor al que se conectará el módulo y puede reutilizarse en distintos comandos que utilicen la misma conexión.

Configuración de la credencial

Para crear una nueva credencial de MongoDB, complete los siguientes campos:

Nombre de la credencial

Campo utilizado para identificar la credencial dentro de la plataforma.

Este nombre es solo de referencia interna y sirve para distinguir esta conexión de otras configuraciones de MongoDB.

Ejemplo de uso

MongoDB Producción

MongoDB Local

MongoDB Testing

Cadena de conexión

Ingresa la dirección IP o el nombre del servidor al que desea conectarse.

Este campo define la **cadena de conexión del servidor MongoDB** al que se conectará el módulo.

Debe contener la información necesaria para establecer la conexión con el servidor MongoDB correspondiente.

Parámetros de la credencial

Parámetro

Cadena de conexión

Descripción

Cadena de conexión del servidor MongoDB al que desea conectarse. Puede ser una dirección IP, un nombre de dominio o una cadena de conexión completa según la configuración del servidor.

Identificador

cadena_de_conexión

Ejemplo

localhost

127.0.0.1

mongo.mi-servidor.com

Notas importantes

- La cadena de conexión debe apuntar a un servidor MongoDB accesible desde el entorno donde se ejecuta el bot.
- Si el servidor se encuentra en la nube o en otra red, asegúrese de que los puertos y reglas de acceso estén correctamente configurados.
- Una misma credencial puede reutilizarse en múltiples comandos siempre que apunten al mismo servidor MongoDB.
- Si necesita conectarse a distintos servidores, deberá crear una credencial diferente para cada uno.

Uso de la credencial

Una vez creada y guardada, esta credencial podrá seleccionarse desde los comandos del módulo MongoDB, como por ejemplo:

- Obtener documentos
- Insertar documentos
- Actualizar documentos
- Eliminar documentos

[Saturn Studio – Credencial Reddit](#)



¿Qué es este módulo?

Las credenciales de Reddit permiten autenticar los módulos que interactúan con la API de Reddit para **publicar, leer y gestionar contenido programáticamente** mediante OAuth2 y credenciales de aplicación. Para obtener estas credenciales es necesario registrar una aplicación en el portal de desarrolladores de Reddit y copiar los valores de *App ID* y *App Secret*.

Método de autenticación

OAuth2

Descripción

La autenticación con Reddit se realiza mediante **OAuth2**, donde la aplicación registrada proporciona un *App ID* (Client ID) y *App Secret* que Saturn Studio utiliza para autorizar solicitudes a la API de Reddit.

Este método permite:

- Acceder programáticamente a funciones de Reddit (crear posts, comentarios, etc.)
- Publicar y gestionar contenido en nombre de un usuario autorizado
- Integrar acciones de Reddit en flujos automatizados

Campos de la credencial

Credential name

Nombre identificador de la credencial dentro de Saturn Studio.

Ejemplo:

Reddit Publicaciones

Reddit Automatización

App ID (Client ID)

Identificador único generado por Reddit para la aplicación registrada.

Cómo obtenerlo

1. Acceder a Reddit y loguearse con la cuenta que se va a usar para la integración.
2. Ir a la página de aplicaciones de desarrollador en Reddit:
<https://www.reddit.com/prefs/apps>.
3. Hacer clic en **Create App**.
4. Completar los campos del formulario (nombre de la app, tipo de aplicación, redirect URI).
5. Después de crear la aplicación, el **Client ID** aparecerá bajo el nombre de la app en la lista de aplicaciones creadas.

Notas importantes

- El App ID también puede llamarse *Client ID*.
- Se usa para autenticar las solicitudes de la aplicación ante Reddit.
- De ejemplo la app tendrá la siguiente información:
 - Saturn Studio
 - Web App
 - URL: <https://studio.rocketbot.com/>

App Secret

Clave secreta proporcionada por Reddit para la aplicación.

Cómo obtenerlo

1. En la misma pantalla donde se creó la aplicación en [reddit.com/prefs/apps](https://www.reddit.com/prefs/apps), aparecerá un valor etiquetado como **secret**.

2. Ese valor es el **App Secret** y no debe compartirse públicamente.

Requisitos previos

- Cuenta activa en **Reddit**
- Acceso a *reddit.com/prefs/apps*
- Aplicación creada para la integración
- App ID y App Secret generados

Configuración en Saturn Studio

Al crear la credencial en Saturn Studio para Reddit, se deben completar los siguientes campos:

- **Credential name** – Nombre descriptivo
- **App ID (Client ID)** – Copiado desde la app de Reddit
- **App Secret** – Copiado desde la app de Reddit

Saturn Studio puede incluir un botón de **Check** (verificación) para validar que los datos ingresados sean correctos antes de guardar la credencial.

En este caso es el botón de “Sign in with Reddit”.

Saturn Studio – Credencial Pinecone



¿Qué es este módulo?

Las credenciales de Pinecone permiten autenticar los módulos que interactúan con la API de Pinecone para la gestión de índices y vectores, utilizando **API Keys administradas por proyecto** desde la consola oficial de Pinecone.

Esta documentación se basa en el funcionamiento real de Pinecone y en su documentación oficial de gestión de API Keys.

Método de autenticación

API Key por proyecto

Descripción

La autenticación se realiza mediante una **API Key asociada a un proyecto de Pinecone**. Cada API Key puede configurarse con permisos específicos que determinan qué operaciones están permitidas sobre los recursos del proyecto.

Este método permite:

- Control granular de acceso mediante permisos
- Separación de entornos (producción, testing, desarrollo)
- Uso seguro en entornos productivos
- Integración directa con Saturn Studio

Campos de la credencial

Credential name

Nombre identificador de la credencial dentro de Saturn Studio.

Este valor es solo descriptivo y permite identificar fácilmente la credencial en el futuro.

Ejemplos:

Pinecone Producción Pinecone Testing

API Key

Clave utilizada para autenticar las solicitudes realizadas por Saturn Studio contra la API de Pinecone.

Cómo obtenerla

1. Acceder a la consola oficial de Pinecone.
2. Seleccionar el proyecto donde se utilizará la integración.
3. Ingresar a la sección **API Keys** del proyecto.

4. Crear una nueva API Key.
5. Asignar un nombre descriptivo.
6. Seleccionar los permisos necesarios según las operaciones que realizará Saturn Studio.
7. Confirmar la creación de la API Key.

Importante: Por motivos de seguridad, Pinecone muestra el valor completo de la API Key solo una vez. Si se pierde, debe generarse una nueva.

Verificación de la API Key en Saturn Studio

Al ingresar la API Key en Saturn Studio, el campo incluye un botón **Check**.

Este botón permite:

- Validar que la API Key sea correcta
- Verificar que los permisos asignados sean suficientes
- Confirmar la conectividad con Pinecone antes de guardar la credencial

Si la verificación es exitosa, la credencial queda lista para ser utilizada por los comandos del módulo.

Environment

Identificador del entorno donde se encuentra desplegado el proyecto de Pinecone.

Este valor es obligatorio para que Saturn Studio pueda comunicarse correctamente con la API.

Cómo obtenerlo

1. Acceder a la consola de Pinecone.
2. Seleccionar el proyecto.
3. Visualizar la información general del proyecto.
4. Copiar el valor indicado como **Environment**.

Ejemplos:

us-east-1

us-west-2

gcp-starter

Index Name

Nombre del índice de Pinecone sobre el cual se ejecutarán las operaciones.

Debe coincidir exactamente con el nombre del índice creado en el proyecto.

Requisitos previos

- Cuenta activa en Pinecone
- Proyecto creado en Pinecone
- API Key activa
- Índice creado en el proyecto

Permisos de las API Keys (según Pinecone)

Las API Keys de Pinecone funcionan mediante **permisos explícitos** que determinan qué acciones pueden realizarse dentro del proyecto.

Los permisos se asignan al momento de crear la API Key y no pueden modificarse posteriormente. Para cambiar permisos, es necesario generar una nueva clave.

Permisos disponibles

Según la documentación oficial de Pinecone, los permisos se agrupan por tipo de operación:

- Indexes: crear, listar y eliminar índices
- Vectors: insertar, actualizar y eliminar vectores
- Query / Search: realizar búsquedas y consultas
- Project access: acceso general al proyecto

Permisos requeridos para Saturn Studio

Los permisos necesarios dependen de los comandos del módulo Pinecone que se utilicen.

Uso estándar del módulo

Para la mayoría de los flujos en Saturn Studio se recomienda que la API Key tenga al menos:

- Lectura de índices
- Escritura de vectores
- Consulta / búsqueda de vectores

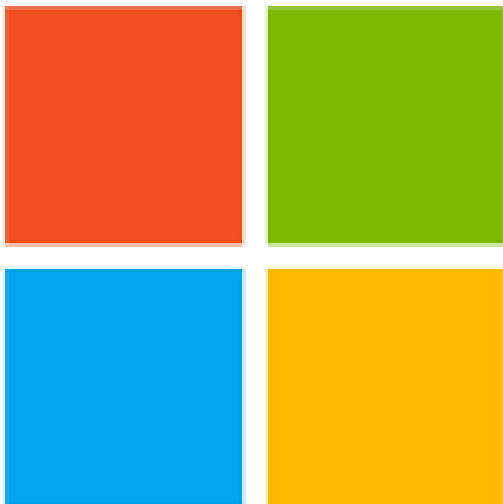
Comandos administrativos

Para comandos que administran recursos (por ejemplo, eliminar un índice), se requieren permisos adicionales:

- Eliminación de índices

Si la API Key no cuenta con los permisos necesarios, el comando fallará aunque la clave sea válida.

Saturn Studio – Credenciales Microsoft



Microsoft credentials

Las credenciales de Microsoft permiten autenticar los módulos que utilizan **Microsoft Graph API** mediante **OAuth 2.0**, usando una **aplicación registrada en Microsoft Entra ID (Azure)**.

Método de autenticación

Advanced Settings

Descripción

La autenticación se realiza mediante una **aplicación registrada en Microsoft Entra ID**, utilizando **Client ID**, **Client Secret** y **Tenant ID**.

Este método permite:

- Control total de permisos
- Uso en entornos productivos
- Reutilización de credenciales en múltiples módulos Microsoft
- Cumplimiento de políticas de seguridad corporativas

Campos de la credencial

Credential name

Nombre identificador de la credencial dentro de Rocketbot.

Ejemplo : Microsoft Excel , Microsoft OneDrive

Client ID

Identificador único de la aplicación registrada en Microsoft Entra ID.

Dónde obtenerlo

- Microsoft Azure Portal
- Microsoft Entra ID
- App registrations
- Seleccionar la aplicación
- Application (client) ID

Le damos la bienvenida a Azure

¿No tiene ninguna suscripción? Consulte las opciones siguientes.



Empiece con una prueba gratuita de Azure

Obtenga un crédito gratuito de 200 USD para los productos y servicios de Azure, más 12 meses de [servicios gratuitos populares](#).

[Inicio](#)

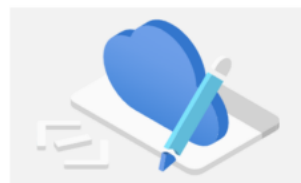


Administrar Microsoft Entra ID

Administre el acceso, establezca directivas inteligentes y mejore la seguridad con Microsoft Entra ID.

[Ver](#)

[Más información](#)



Microsoft Azure for Students

Obtenga software gratuito o crédito de Azure, o acceda a Azure Dev Tools for Teaching después de verificar su estado académico.

[Inicio](#)

Servicios de Azure



[Crear un recurso](#)



[Microsoft Ent...](#)



[Aplicaciones empresariales](#)



[App Services](#)



[Registro de actividad](#)



[Aplicaciones administradas](#)



[Microsoft Graph Data...](#)



[Grupos de aplicaciones](#)



[Suscripciones](#)



[Más servicios](#)

[+ Nuevo registro](#)
[Puntos de conexión](#)
[Solucionar problemas](#)
[Actualizar](#)
[Descargar](#)
[Características en versión preliminar](#)
[¿Tiene algún comentario?](#)

Información general
 Características en versión preliminar
 Diagnosticar y solucionar problemas
 Favoritos
Registros de aplicaciones
 Administrar
 Usuarios
 Grupos
 External Identities
 Roles y administradores
 Unidades administrativas
 Asociados del administrador delegado
 Aplicaciones

Agregue o quite favoritos presionando Ctrl+Shift+F

Inicio > Rocketbot | Registros de aplicaciones >

A partir del 30 de junio de 2020, ya no agregaremos ninguna característica nueva a la Biblioteca de autenticación de Azure Active Directory (ADAL) y a Azure Active Directory Graph. Continuaremos brindando soporte técnico y actualizaciones de seguridad, pero ya no brindaremos actualizaciones de funciones. Las aplicaciones deberán actualizarse a la Biblioteca de autenticación de Microsoft (MSAL) y Microsoft Graph. [Más información](#)

[Todas las aplicaciones](#)
[Aplicaciones propias](#)
[Aplicaciones eliminadas](#)
[Aplicaciones de cuenta personal](#)

Empezar a escribir un nombre o id. de aplicación para filtrar los resu...
 [Agregar filtros](#)

2 aplicaciones encontradas

Nombre para mostrar	Id. de aplicación (cliente)	Fecha de c...	Certificados y secretos
Saturn Studio	feef6d15-84f9-4d08-92dd-f9ea209a8942	9/12/2024	Current
SaturnStudio	fa9e647d-1f8a-4634-bb00-0fb57acfee0e	9/12/2024	Expirado

Buscar
 [Eliminar](#)
[Puntos de conexión](#)
[Características en versión preliminar](#)

¿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 : Saturn Studio
 Id. de aplicación (cliente) : feef6d15-84f9-4d08-92dd-f9ea209a8942
 Identificador de objeto : 6bb4b206-52ca-4605-802f-e703c1ada11d
 Id. de directorio (inquilino) : 50b223f7-afa7-4eb0-ae3d-333447725fbb
 Tipos de cuenta compati... : Todos los usuarios de cuentas Microsoft

Credenciales de cliente : [0 certificado, 2secreto](#)
 URI de redirección : [4 web, 2 SPA, 0 cliente público](#)
 URI de id. de aplicación : [api://feef6d15-84f9-4d08-92dd-f9ea209a8942](#)
 Aplicación administrada ... : Saturn Studio

A partir del 30 de junio de 2020, ya no agregaremos ninguna característica nueva a la Biblioteca de autenticación de Azure Active Directory (ADAL) y a Azure Active Directory Graph. Continuaremos brindando soporte técnico y actualizaciones de seguridad, pero ya no brindaremos actualizaciones de funciones. Las aplicaciones deberán actualizarse a la Biblioteca de autenticación de Microsoft (MSAL) y Microsoft Graph. [Más información](#)

A partir del 9 de noviembre de 2020, los usuarios finales ya no podrán dar su consentimiento a aplicaciones multiinquilino que se hayan registrado recientemente sin editores comprobados. [Agregar id. de MPN para verificar el editor](#)

[Introducción](#)
[Documentación](#)

Compilación de la aplicación con la Plataforma de identidad de Microsoft

Formato

UUID (cadena alfanumérica con guiones)

Uso

Este valor puede reutilizarse en otros módulos de Microsoft.

Client Secret

Clave secreta generada para la aplicación registrada en Microsoft Entra ID. Permite que Rocketbot se autentique de forma segura contra Microsoft.

Dónde obtenerlo

- Microsoft Azure Portal
- Microsoft Entra ID
- App registrations
- Seleccionar la aplicación
- Certificates & secrets
- New client secret

Buscar x « ¿Tiene algún comentario?

Información general

Inicio rápido

Asistente para integración

Diagnosticar y solucionar problemas

Administrar

Personalización de marca y propiedades

Authentication (Preview)

Certificados y secretos

Configuración de token

Permisos de API

Exponer una API

Roles de aplicación

Propietarios

Roles y administradores

Manifiesto

Agregue o quite favoritos presionando Ctrl+Shift+F

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.

Certificados (0) **Secretos de los cliente (2)** Credenciales federadas (0)

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

+ Nuevo secreto de cliente

Descripción	Expira	Valor ①	Id. de secreto
test	25/4/2026	wPv*****	f97e7b94-9f8c-48db-844a-4ff49122b368
saturnSecret	10/9/2027	e6b*****	3ee24130-dea2-419d-8ed2-17297a5b85...

Notas importantes

- El valor del secreto se muestra solo una vez
- Si se pierde, debe generarse uno nuevo
- Se recomienda definir una expiración adecuada

Tenant ID

Identificador del tenant (directorio) de Microsoft Entra ID donde está registrada la aplicación.

Dónde obtenerlo

- Microsoft Azure Portal
- Microsoft Entra ID
- Overview
- Tenant ID (Directory ID)

Requisitos previos

- Cuenta Microsoft con acceso a Azure
- Aplicación registrada en Microsoft Entra ID
- Client Secret activo
- Permisos configurados en Microsoft Graph según el módulo

Permisos Microsoft Graph (referencia)

Los permisos necesarios dependen del módulo utilizado.
Ejemplos comunes:

- Files.Read
- Files.ReadWrite
- Sites.Read.All
- User.Read
- Mail.Read (Outlook)

Los permisos deben configurarse en **API permissions** de la aplicación.

Permisos de las credenciales por módulo

Las credenciales de Microsoft se configuran mediante **scopes (permisos)** definidos en Azure AD / Entra ID.

Cada módulo de Microsoft requiere **un conjunto específico de permisos**, por lo que **no siempre es posible reutilizar una misma credencial entre distintos módulos**.

Algunos scopes pueden coincidir entre módulos, pero **cada credencial debe configurarse según el módulo que se vaya a utilizar**.

Microsoft Excel

Scopes requeridos:

- User.Read
- Sites.Read.All
- Files.ReadWrite
- openid
- profile
- offline_access

Uso:

- Acceso a archivos Excel almacenados en OneDrive o SharePoint
- Lectura y escritura de archivos
- Modificación de contenido de hojas de cálculo

Microsoft Outlook

Scopes requeridos:

- User.Read
- Mail.ReadWrite
- Mail.Send
- Sites.Read.All
- Files.ReadWrite

- openid
- profile
- offline_access

Uso:

- Lectura y gestión de correos electrónicos
- Envío de correos
- Acceso a adjuntos y archivos relacionados

Comparación de scopes entre módulos

Scopes comunes:

- User.Read
- Sites.Read.All
- Files.ReadWrite
- openid
- profile
- offline_access

Scopes específicos:

- Outlook:
 - Mail.ReadWrite
 - Mail.Send

Esto implica que:

- Una credencial creada solo con permisos de Excel **no funcionará para Outlook**
- Una credencial creada con permisos de Outlook **sí puede incluir permisos de Excel**, siempre que se agreguen todos los scopes necesarios