



## Autenticación de Ironchip en **Google Workspace**

[www.ironchip.com](http://www.ironchip.com)



# Autenticación de Ironchip en **Google Workspace**

Introducción.....	3
Crear la aplicación SAML en IRONCHIP.....	3
Configurar GOOGLE WORKSPACE.....	5
Obtener URL del metadato para IRONCHIP.....	6
Activación de SSO en GOOGLE WORKSPACE.....	7
Video Guía.....	7

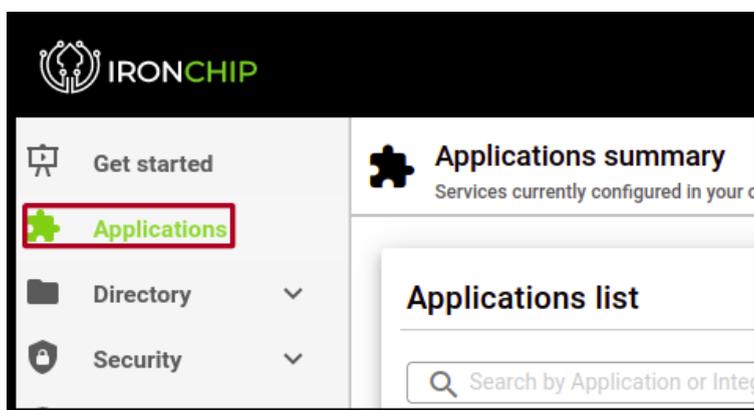


## Introducción

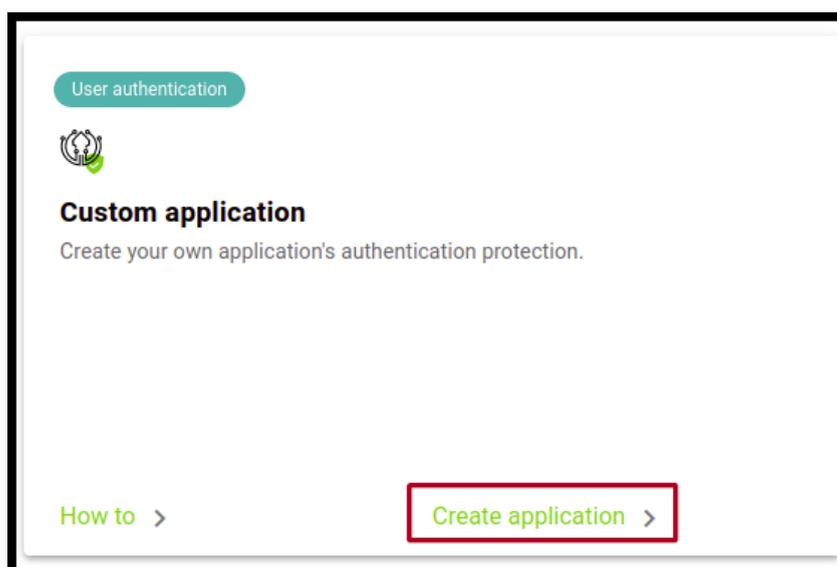
Este documento muestra cómo integrar el autenticador IRONCHIP mediante SAML en GOOGLE WORKSPACE para validar usuarios existentes en IRONCHIP. Para poder realizar esta integración será necesario tener un usuario registrado en GOOGLE WORKSPACE y ser usuario de la plataforma IRONCHIP, ambos con permisos de administración en sus diferentes ambientes.

## Crear la aplicación SAML en IRONCHIP

En el panel de IRONCHIP acceda al apartado aplicaciones.



Pulse en nueva aplicación y elija la opción aplicación personalizada.





## Autenticación de Ironchip en Google Workspace

En esta pestaña, póngale un nombre identificativo, seleccione aplicación tipo SAML y en caso de quererlo añadir una imagen como logo de la aplicación. No cierre esta pestaña.

**Add a new application** ✕

Application settings

Application name (alias)  
Google Workspace

OIDC - OAUTH 2.0

API KEY

**SAML**

Antes de entrar al panel de administrador de google, descarga el archivo de metadato de Ironchip.

**SAML service configuration**

SAML integration allows you to connect SAML services through the location based authentication identity provider. This integration requires your service provider metadata file that is going to be downloaded from the URL you specify below.

Metadata URL

 Download Ironchip's **SAML IDP metadata** to enable your Service Provider to properly communicate:

**Download metadata file**



## Configurar GOOGLE WORKSPACE

Ahora entre a el panel de administrador de Google, vaya a Seguridad > Autenticación > SSO con IdP externo y agregue un perfil de SAML.



Abra el metadato descargado anteriormente y rellena los campos con los siguientes datos :

- Para el ID de entidad del IDP utilice la propiedad “EntityID” en el tag XML “EntityDescriptor”.
- Para la URL de la página de acceso utilice la propiedad “Location” en el tag XML “SingleSignOnService”.
- Para la URL de la página de salida, busque de nuevo la propiedad “Location” en el tag XML “SingleLogoutService”.
- Para la subida del certificado que te requiere, genere un nuevo fichero con extensión “.crt” y guarde en ese archivo el resultado de pegar dentro del primer campo de esta herramienta el contenido del tag XML “X509Certificate” del metadato, ambos certificados son idénticos: [https://www.samltool.com/format\\_x509cert.php](https://www.samltool.com/format_x509cert.php)

Esta herramienta añadirá las cabeceras necesarias para que GOOGLE WORKSPACE detecte el certificado como válido. Una vez guardado el archivo, súbalo.

El resto de campos pueden quedar por defecto, guarde los cambios.



## Autenticación de Ironchip en Google Workspace

### Detalles del IDP

ID de entidad del IDP

<https://testing.idp.ironchip.com/saml/metadata/64914fecb0df0495aef>

URL de la página de acceso

<https://testing.idp.ironchip.com/saml/sso/64914fecb0df0495ae626d88>

Debe ser una URL válida (por ejemplo, <https://dominio.com>). Esta es la URL que visitan los usuarios para acceder.

URL de la página de salida

<https://testing.idp.ironchip.com/saml/slo/64914fecb0df0495ae626d88>

Debe ser una URL válida (por ejemplo, <https://dominio.com>). Esta es la URL a la que se envía a los usuarios después de que salen de sus cuentas.

Cambiar URL de contraseña

Debe ser una URL válida (por ejemplo, <https://dominio.com>). Esta es la URL a la que se redirige a los usuarios cuando intentan cambiar la contraseña de sus Cuentas de Google.

### Certificado de verificación

Sube dos certificados como máximo. Debe ser un certificado X.509 con el formato PEM o DER y debe contener una clave pública.

[SUBIR CERTIFICADO](#)

## Obtener URL del metadato para IRONCHIP

Para obtener el URL del metadato que nos pide la plataforma IRONCHIP modifica el siguiente código con los datos correspondientes:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
validUntil="2022-09-16T10:40:54Z" cacheDuration="PT604800S" entityID="google.com">
<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://www.google.com/a/acs" index="1"/>
</md:SPSSODescriptor>
</md:EntityDescriptor>
```



## Autenticación de Ironchip en Google Workspace

- Sustituya el contenido de **entityID** por el ID de entidad que se encuentra en el apartado detalles del SP.
- Sustituya el contenido de **Location** por el url de ACS que se encuentra en el apartado detalles del SP.

Detalles del SP	El IDP necesitará estos detalles para configurar el SSO con Google como SP. Consulta la documentación del IDP para obtener más información.
ID de entidad	<input type="text" value="https://accounts.google.com/samlr/metadata?rpId=02djd0n41exj18g"/> 
URL de ACS	<input type="text" value="https://accounts.google.com/samlr/acs?rpId=02djd0n41exj18g"/> 

Cuando haya generado este archivo, súbalo a una dirección pública de Internet y provea esta URL en formato raw añadiéndola al campo Metadata URL en el diálogo de Add new service en la plataforma IRONCHIP.

## Activación de SSO en GOOGLE WORKSPACE

Para activar el login mediante la integración SAML recién creada, navegue de nuevo a Seguridad > Autenticación > SSO con proveedor externo de identidad es su interfaz de Google Admin.

Pulse en “Gestionar asignaciones de perfil de SSO”. En la parte izquierda puede configurar los grupos o individuos que se autenticarán utilizando el segundo factor de autenticación de IRONCHIP.

Recuerde configurar estos usuarios en el servicio SAML que ha creado en IRONCHIP.

### Video Guía

