Aplicaciones y Accesos

Manual del Dashboard Ironchip · Volumen 2

Entorno: testing.app.ironchip.com
Generado el 30 de abril de 2026

Contenido

CAPÍTULO 1

Listado de aplicaciones

Menú lateral · Applications.

Vista general

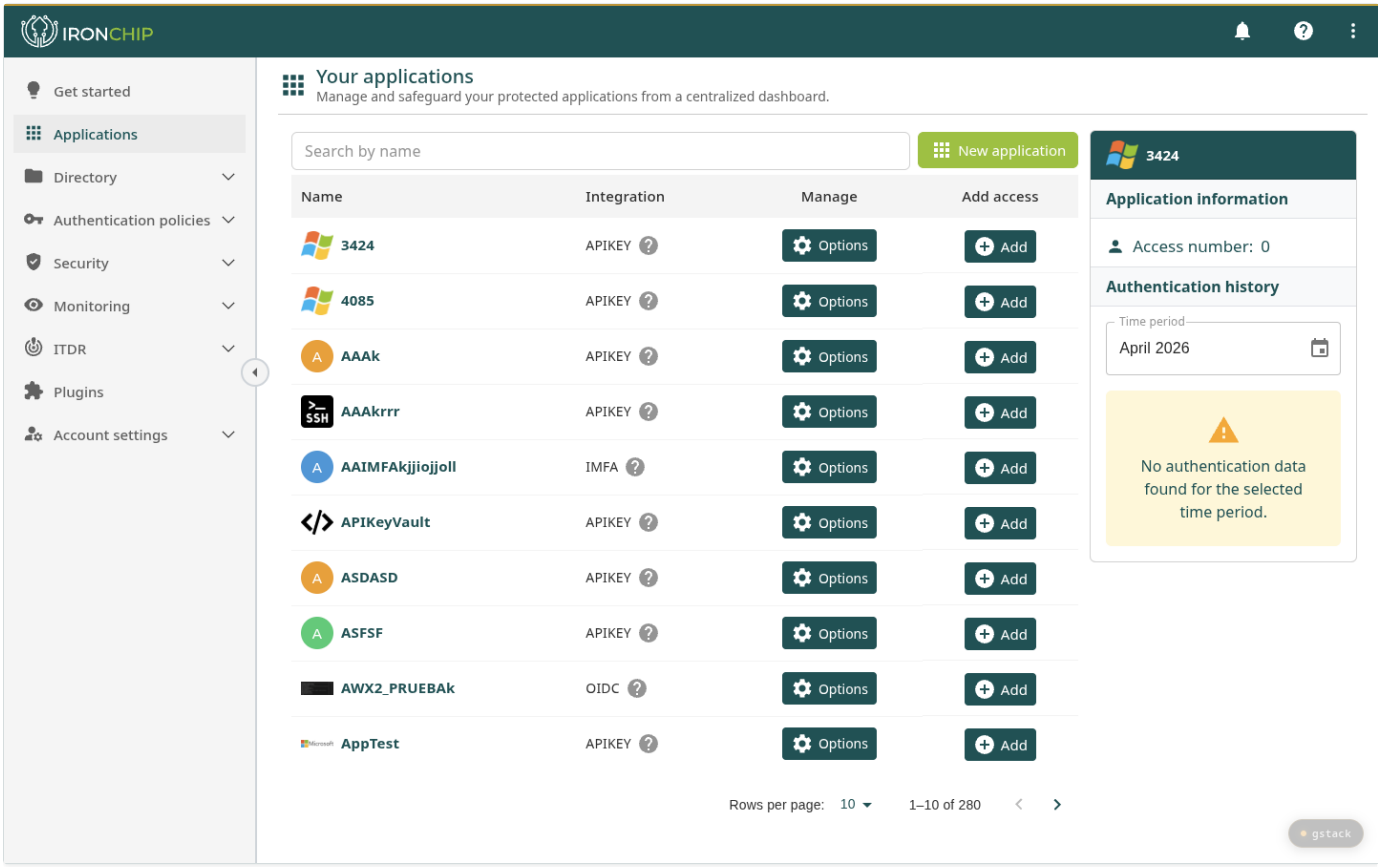


Tabla con todas las aplicaciones protegidas y panel lateral de información.

La pantalla **Your applications** es el centro de control de tus integraciones. Cada fila representa una aplicación protegida por Ironchip.

Columnas

- **Name:** nombre de la aplicación con icono identificativo (Microsoft, Linux, SAML, OIDC, SSH, etc.).
- **Integration:** tipo de integración: `APIKEY` , `OIDC` , `SAML` , `IMFA` , `RADIUS` ...
- **Manage** / **Options:** menú con View / Edit / Delete.
- **Add access:** atajo para asignar un nuevo acceso sin entrar al detalle.

Panel lateral

Al seleccionar una aplicación de la lista, el panel derecho muestra **Application information** con el número total de accesos y un gráfico de **Authentication history** filtrable por mes.

Acciones globales

- **Search by name:** filtro por nombre de aplicación.
- **New application:** abre el asistente de creación (capítulo 2).

CAPÍTULO 2

Crear una aplicación: catálogo de tipos

Asistente de 3 pasos: Select service type → Configure service → Overview.

Paso 1 — Selección de tipo

Pulsa **New application** para abrir el catálogo. Las integraciones se agrupan en cuatro categorías:

1. Operating system security

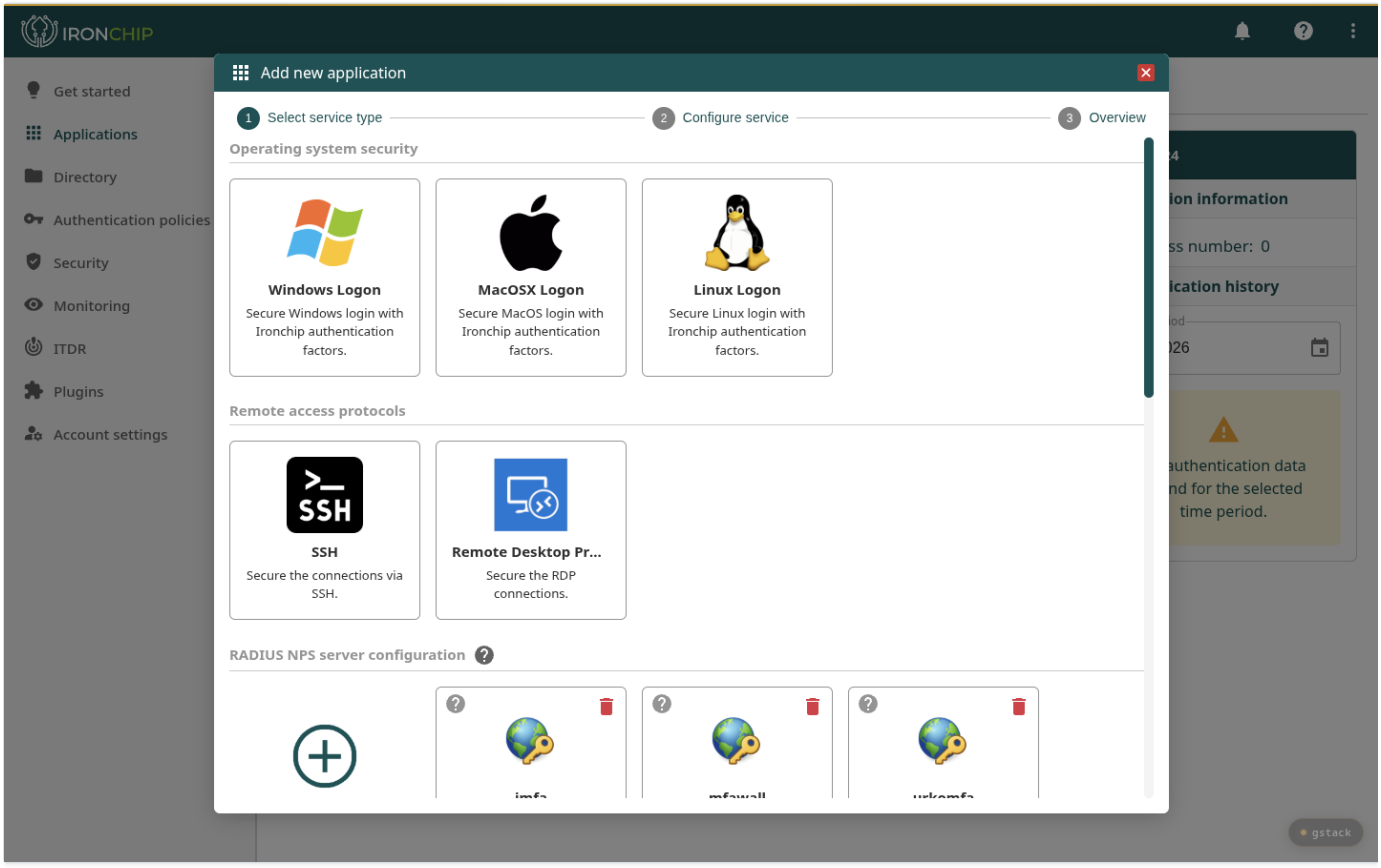
- **Windows Logon:** login seguro de Windows con factores Ironchip.
- **MacOSX Logon:** equivalente para macOS.
- **Linux Logon:** equivalente para Linux (PAM).

2. Remote access protocols

- **SSH:** protección de conexiones SSH.
- **Remote Desktop Protocol (RDP):** protección de RDP.

3. RADIUS NPS server configuration

Lista de servidores RADIUS NPS configurados en la empresa, con un botón **+ New NPS server** y un botón **Assign policy** por servidor.



Categorías superiores: SO, protocolos remotos y servidores RADIUS NPS.

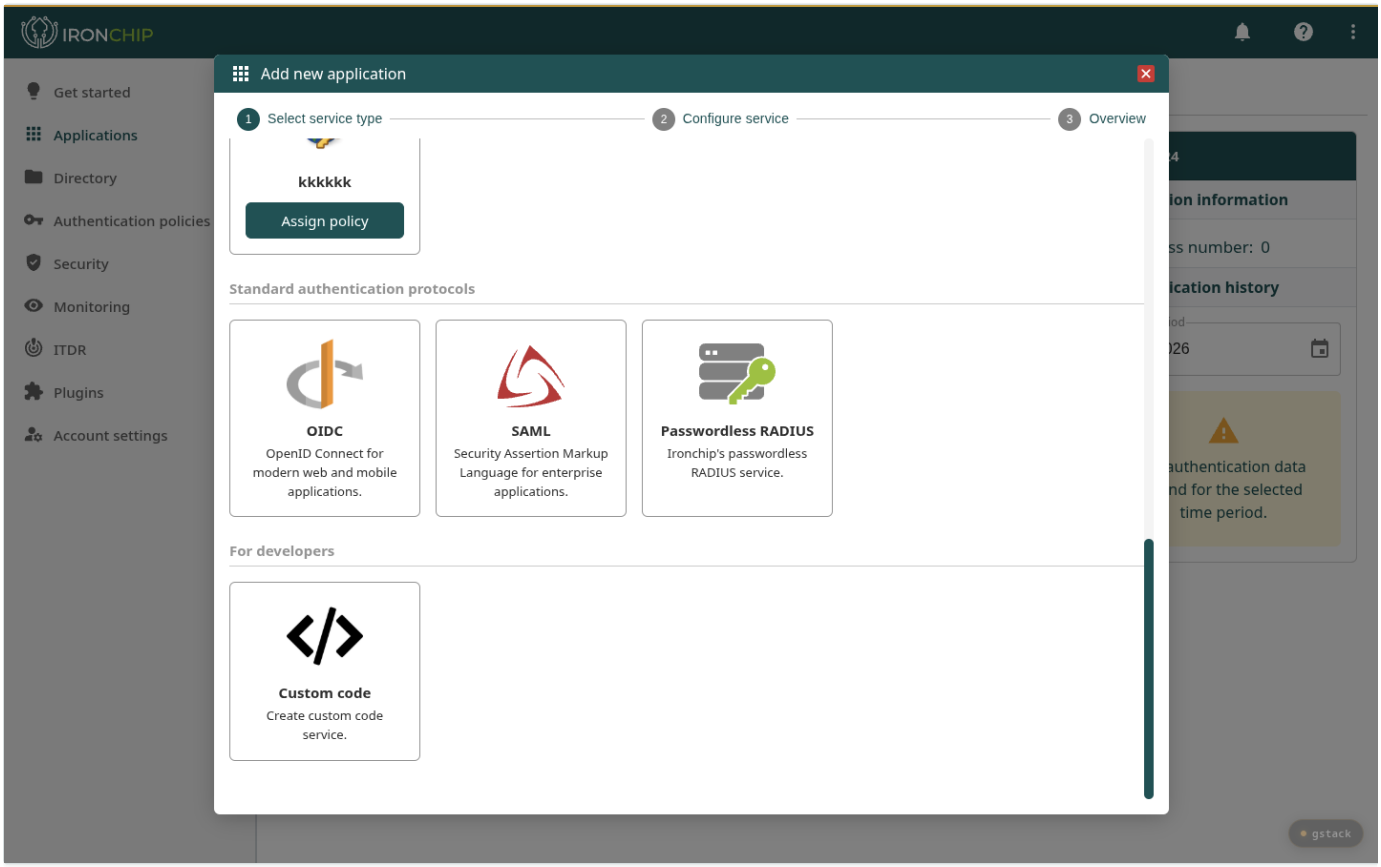
4. Standard authentication protocols

Y al final del catálogo, los protocolos estándar:

- **OIDC:** OpenID Connect 1.0 sobre OAuth 2.0 — para apps web y móviles modernas.
- **SAML:** Security Assertion Markup Language — para SSO empresarial.
- **Passwordless RADIUS:** servicio passwordless de Ironchip.

5. For developers

- **Custom code:** servicio configurable mediante código personalizado.



Protocolos estándar (OIDC, SAML, Passwordless RADIUS) y custom code.

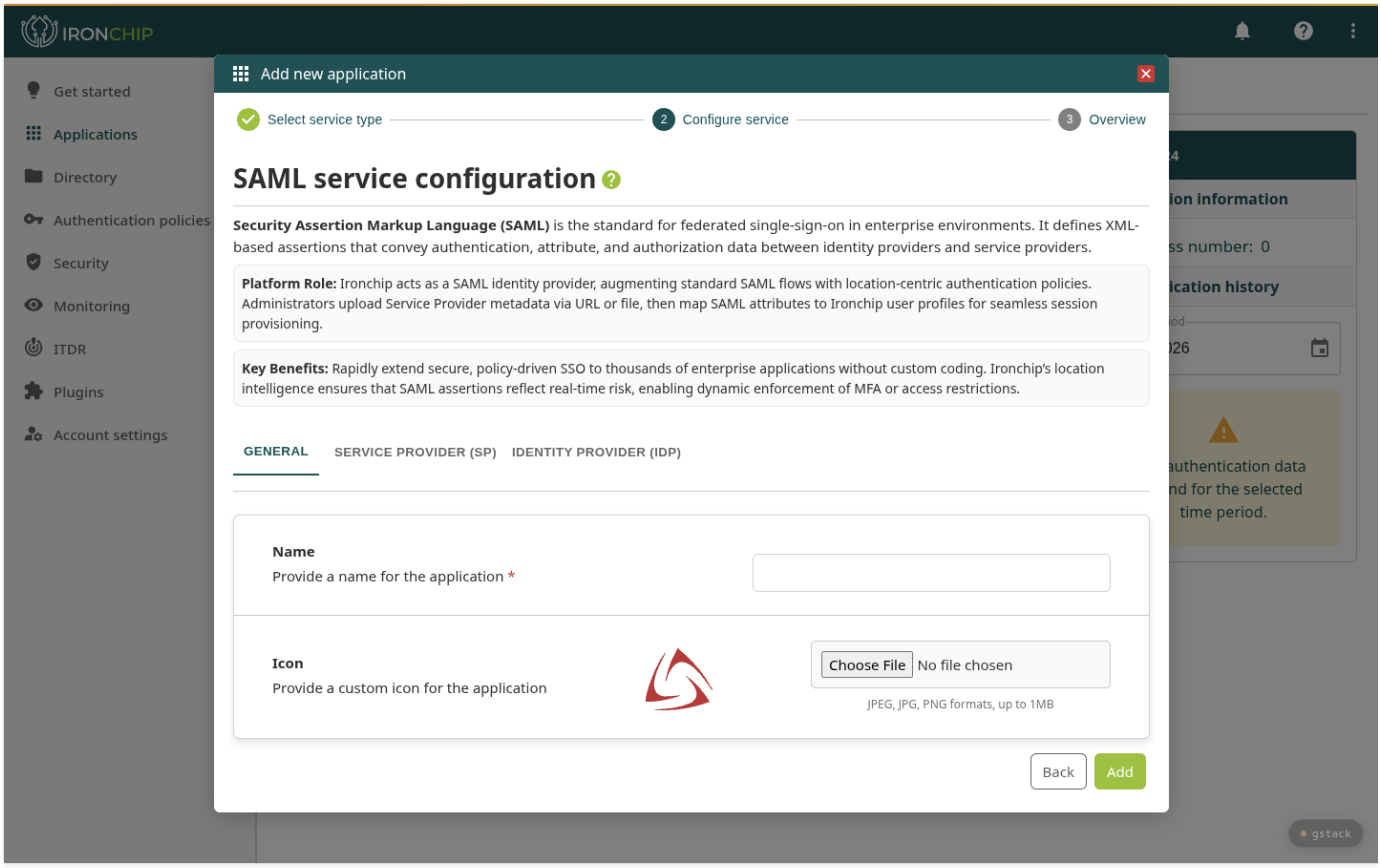
CAPÍTULO 3

Crear una aplicación SAML

Para integraciones SSO empresariales.

Paso 2 — Configuración SAML

Al seleccionar SAML en el catálogo, el asistente avanza al paso 2 con un encabezado explicativo del protocolo y tres pestañas de configuración.

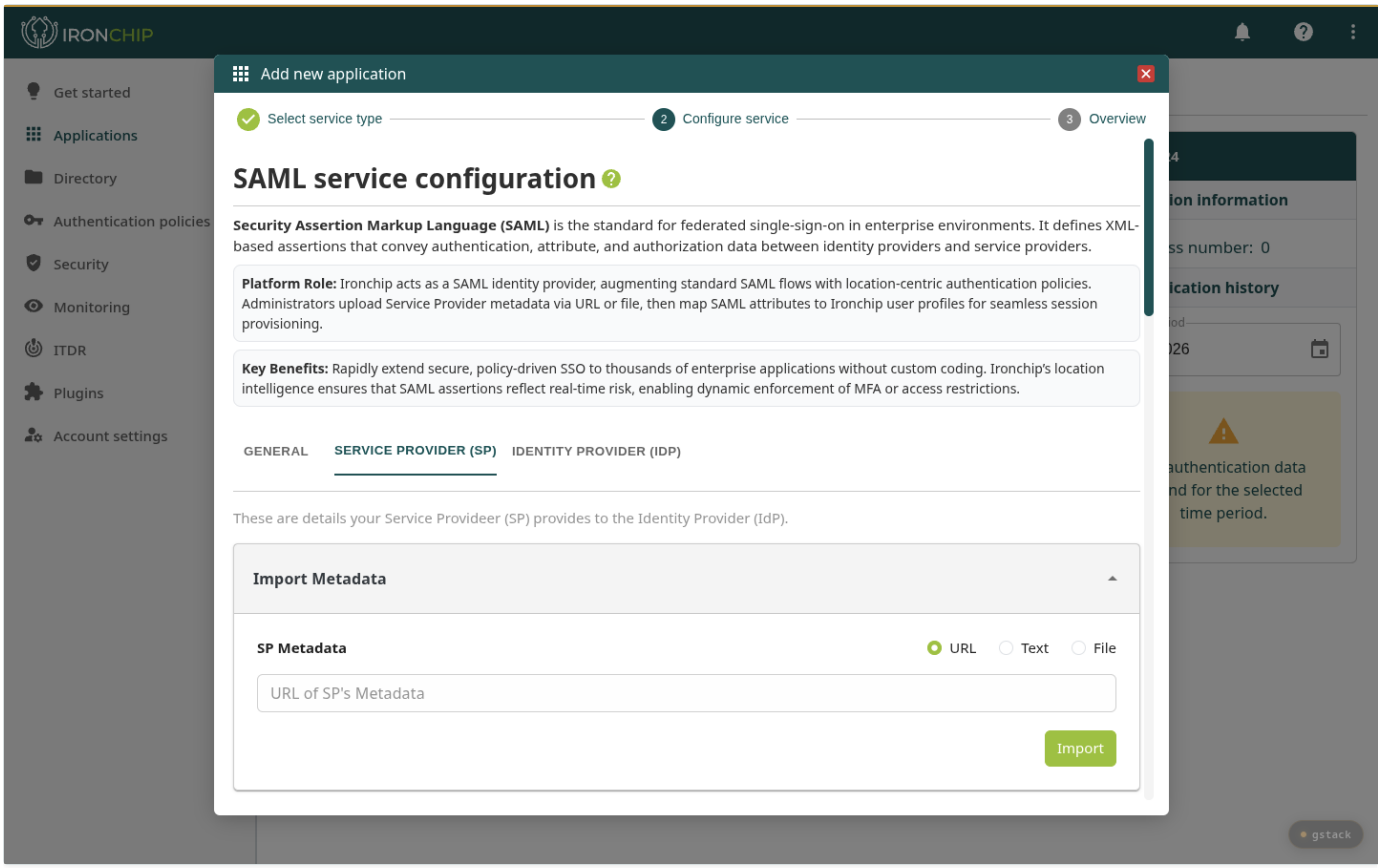


*Pestaña **GENERAL**: nombre y logo de la aplicación.*

Pestaña GENERAL

1. **Name *:** nombre interno (no afecta al SAML EntityID, sólo a la visualización en el dashboard).
2. **Icon:** imagen JPEG, JPG o PNG (hasta 1 MB) que aparecerá en el listado y en el cliente.

Pestaña SERVICE PROVIDER (SP)



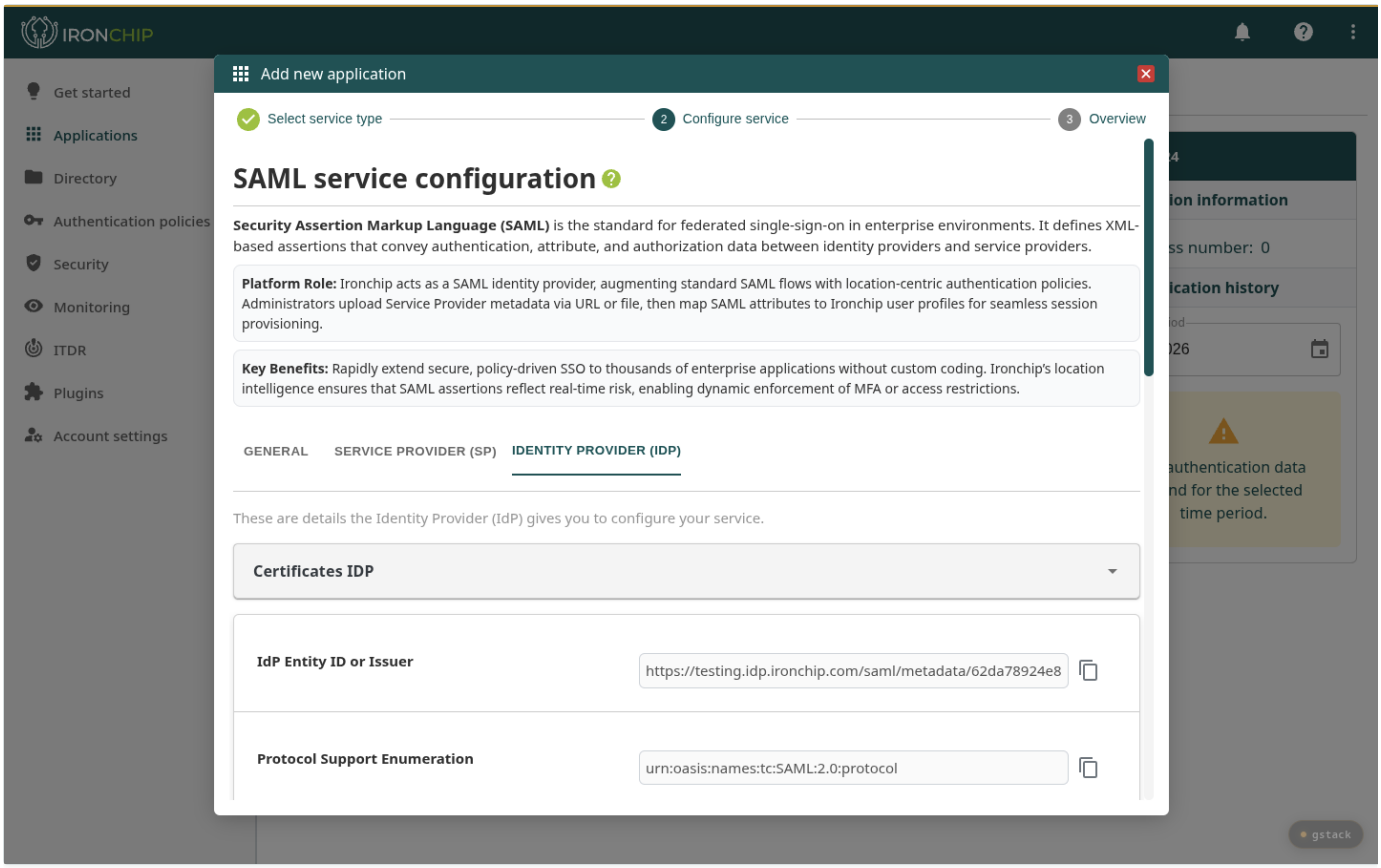
Importación del metadata del SP por URL, texto o fichero.

Aquí se cargan los datos del Service Provider (la aplicación que va a confiar en Ironchip como IdP). Hay tres modos de importar el metadata:

- **URL:** indica una URL pública desde la que descargar el metadata XML del SP.
- **Text:** pega el XML directamente.
- **File:** sube el fichero `metadata.xml` exportado del SP.

Tras importar, pulsa **Import** para que Ironchip parsee EntityID, ACS URL, NameID format y certificados.

Pestaña IDENTITY PROVIDER (IDP)



Datos que el SP necesita para confiar en Ironchip como IdP.

Esta pestaña contiene los valores generados por Ironchip que el SP debe configurar:

- **Certificates IDP:** certificado de firma del IdP.
- **IdP Entity ID or Issuer:** URL única tipo `https://testing.idp.ironchip.com/saml/metadata/<id>`.
- **Protocol Support Enumeration:** `urn:oasis:names:tc:SAML:2.0:protocol`.
- Y a continuación: SSO URLs, formatos de NameID y atributos exportados.

Cada campo tiene un botón "copiar al portapapeles" para facilitar el cableado con el SP.

Pulsa **Add** para finalizar y crear la aplicación. Saltarás al paso 3 (*Overview*) con un resumen.

> **Buena práctica:** en producción, importa siempre el metadata del SP por URL en lugar de pegarlo. Así, cuando el SP rote certificados, Ironchip se sincroniza solo (si tu SP soporta auto-rotation).

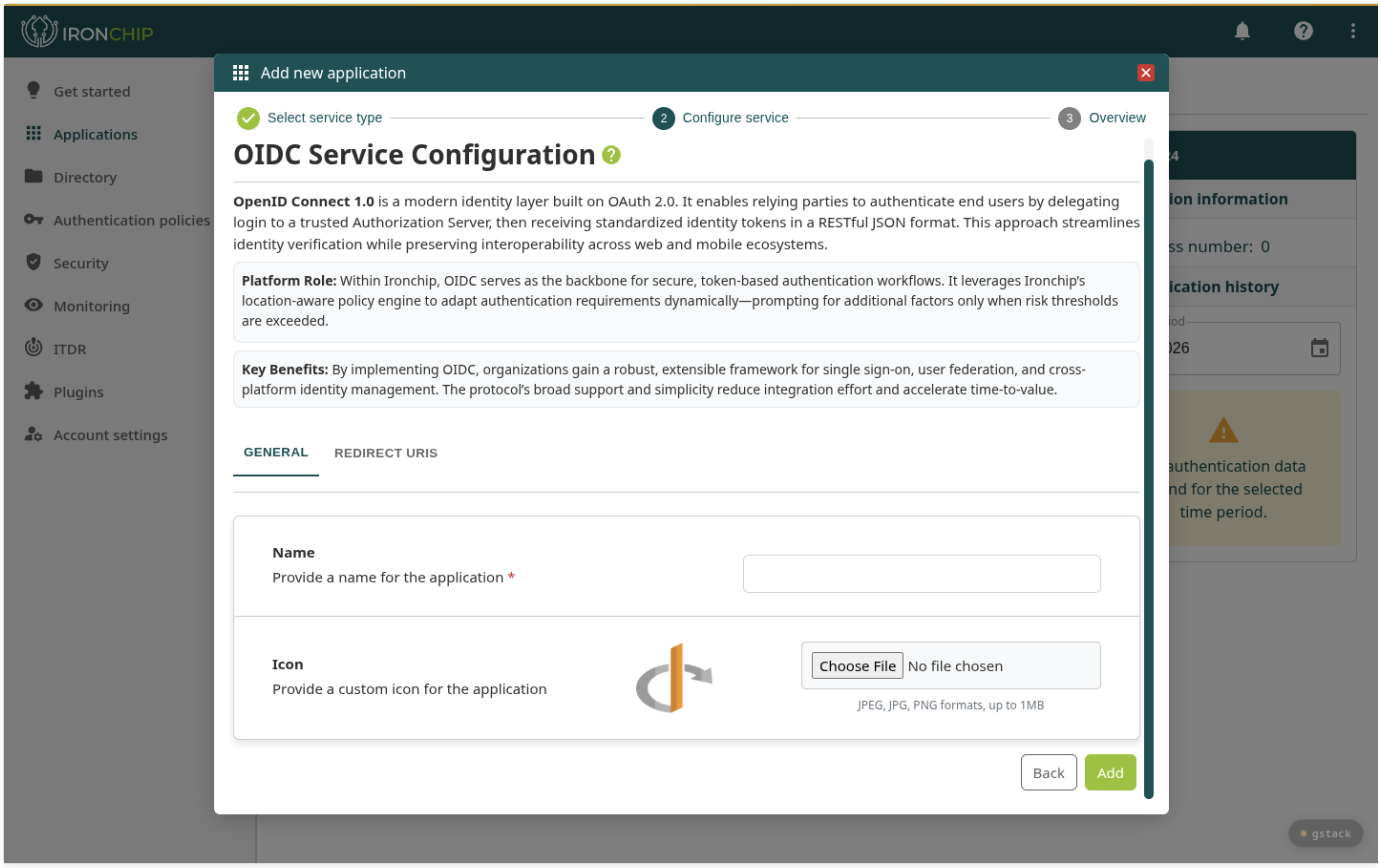
CAPÍTULO 4

Crear una aplicación OIDC

Para apps web modernas y aplicaciones móviles.

Paso 2 — Configuración OIDC

Al elegir **OIDC** el asistente muestra dos pestañas: **GENERAL** y **REDIRECT URIS**.

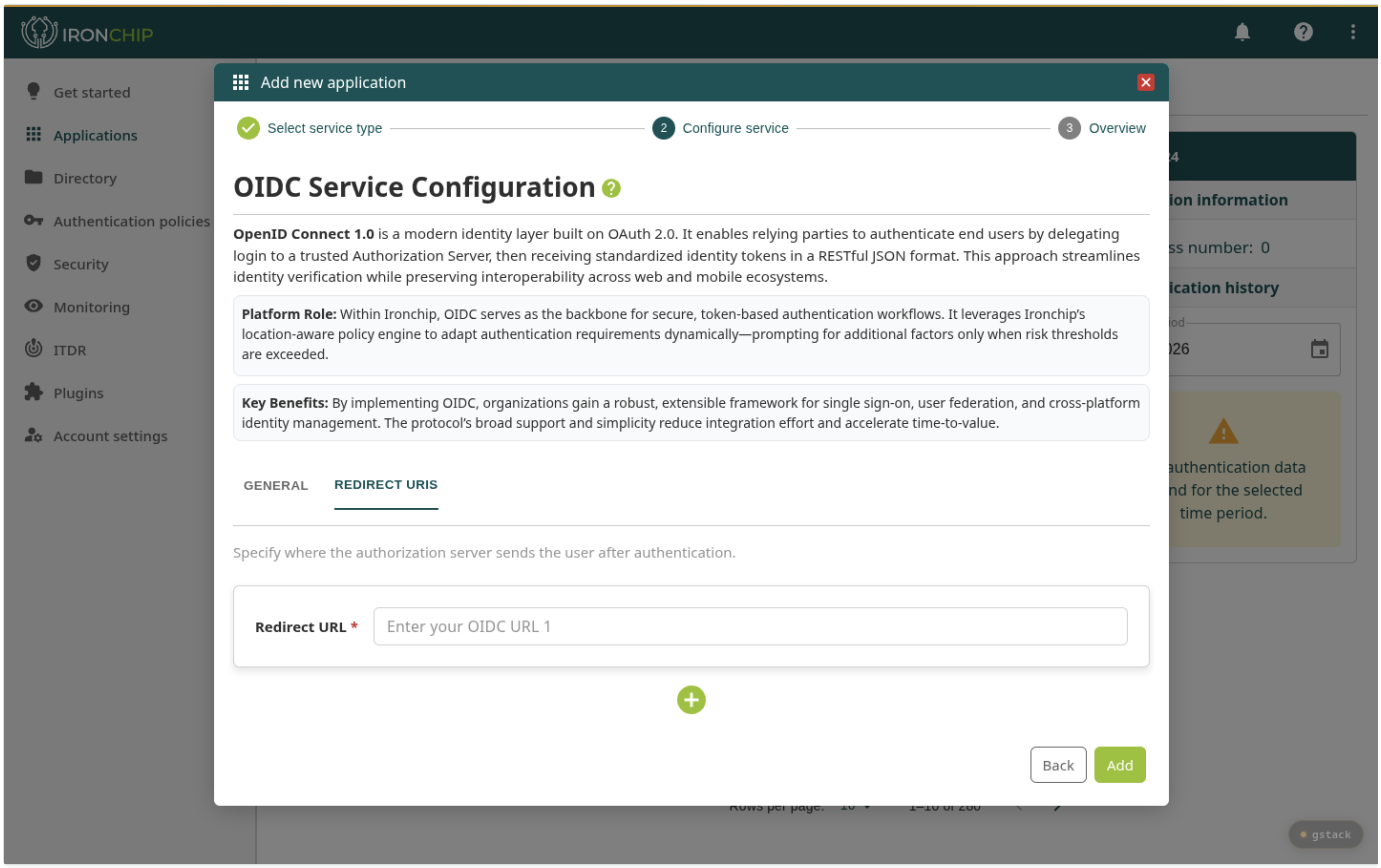


Datos básicos: nombre y logo.

Pestaña GENERAL

Idéntica al resto: **Name** * y **Icon**.

Pestaña REDIRECT URIS



Lista editable de URLs de redirección autorizadas.

1. **Redirect URL *:** URL a la que el authorization server redirige al usuario tras autenticar (en una app web típica, algo como `https://miapp.com/oidc/callback`).
2. Pulsa el **+** verde para añadir más URLs (apps suelen necesitar varias: producción, staging, mobile deep-link...).

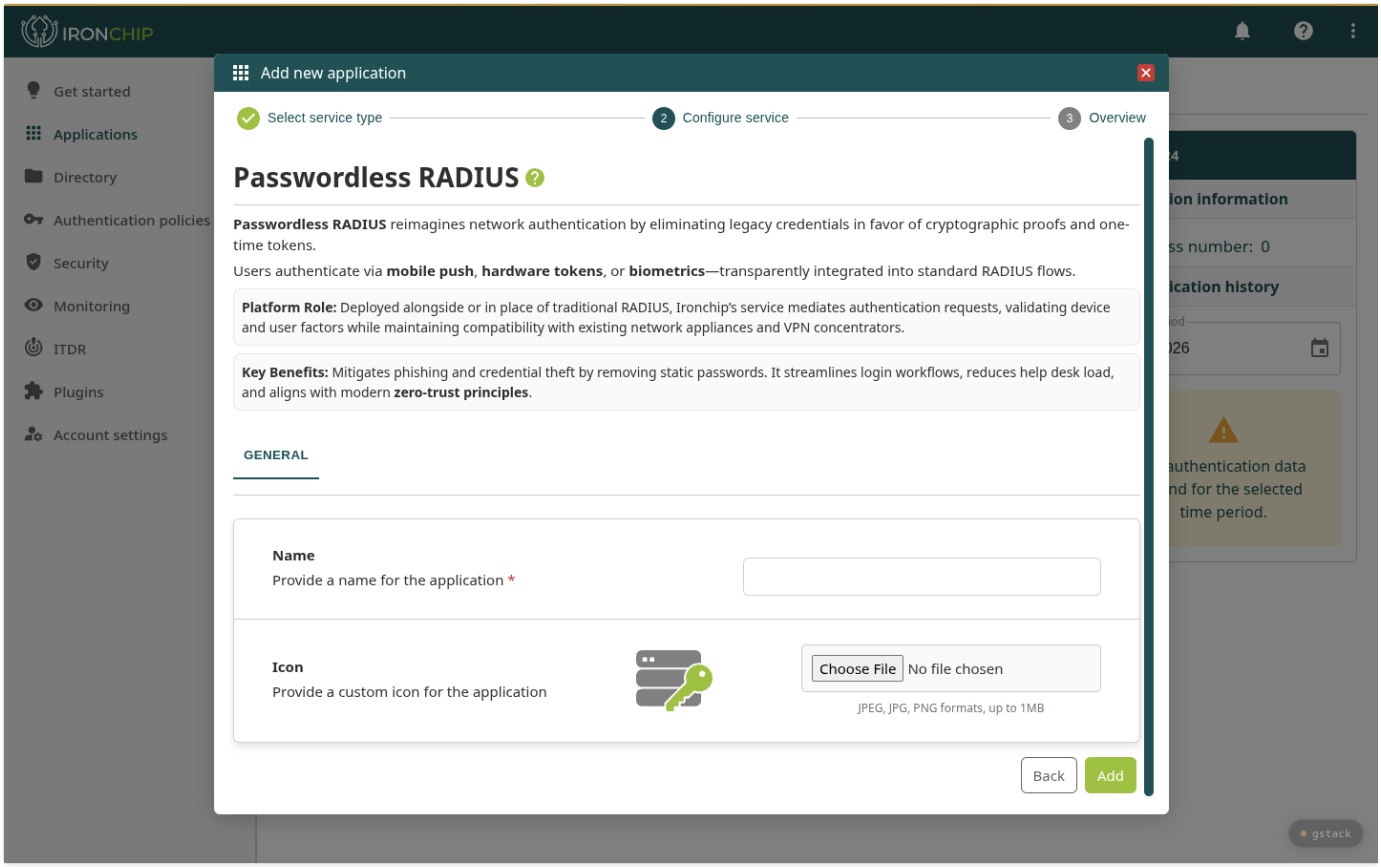
Confirma con **Add**. Tras crear la app, en el detalle podrás recuperar el `client_id` y `client_secret` generados por Ironchip.

CAPÍTULO 5

Crear un servicio Passwordless RADIUS

Reemplazo passwordless de RADIUS legacy.

Paso 2 — Configuración Passwordless RADIUS



Servicio passwordless RADIUS de Ironchip.

El formulario es minimalista — sólo pide nombre y logo. Toda la lógica passwordless (push móvil, hardware token, biometría) se hereda de las políticas de autenticación que asignes posteriormente al servicio en su detalle.

> **RADIUS NPS vs Passwordless RADIUS:** el listado de "RADIUS NPS server configuration" del paso 1 son *servidores RADIUS NPS preexistentes* (Microsoft NPS) a los que se les asigna una política. *Passwordless RADIUS* en cambio es el servicio nativo de Ironchip que reemplaza por completo al NPS.

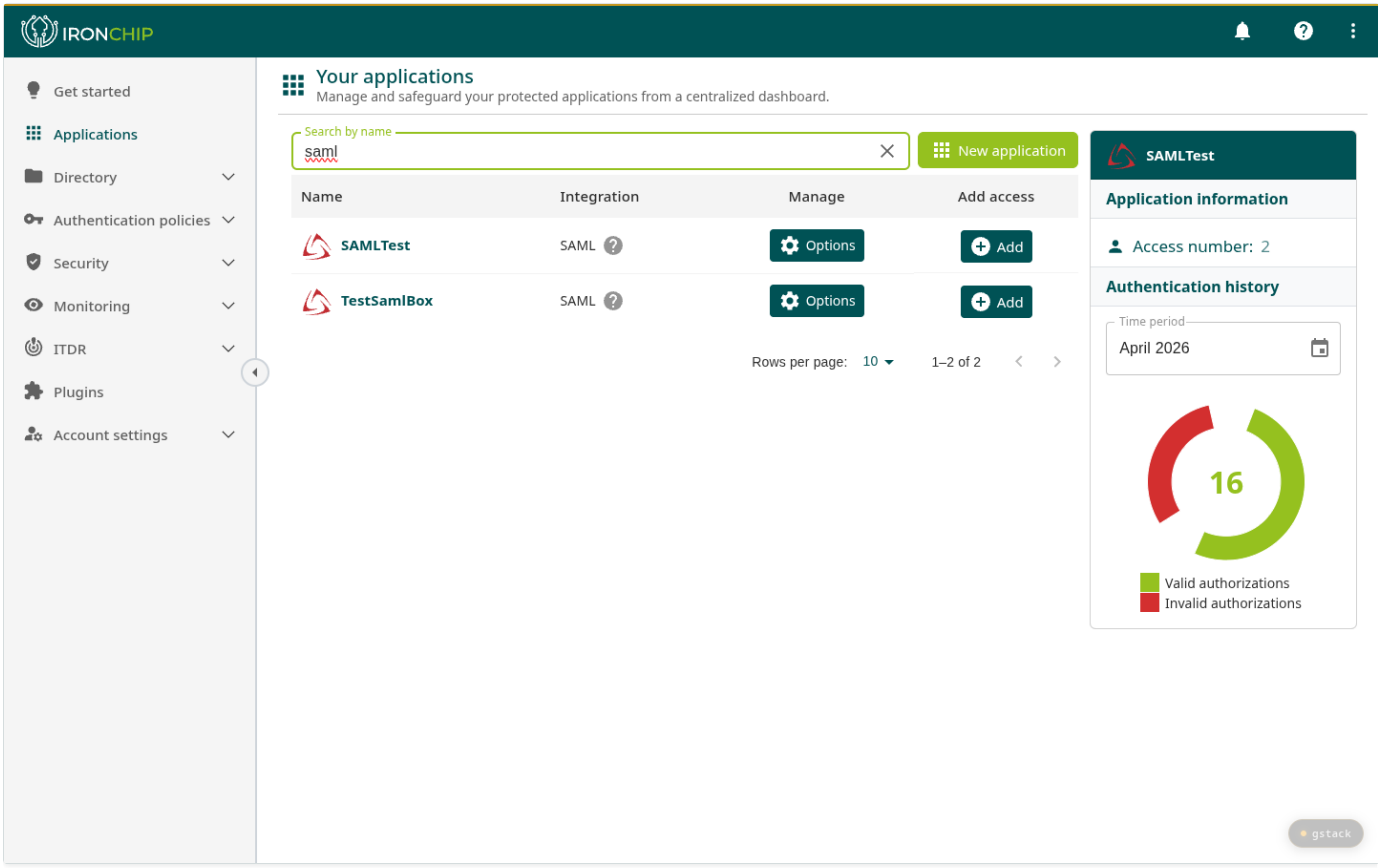
CAPÍTULO 6

Buscar y gestionar una aplicación existente

Filtros y menú "Options" del listado.

Buscar por nombre

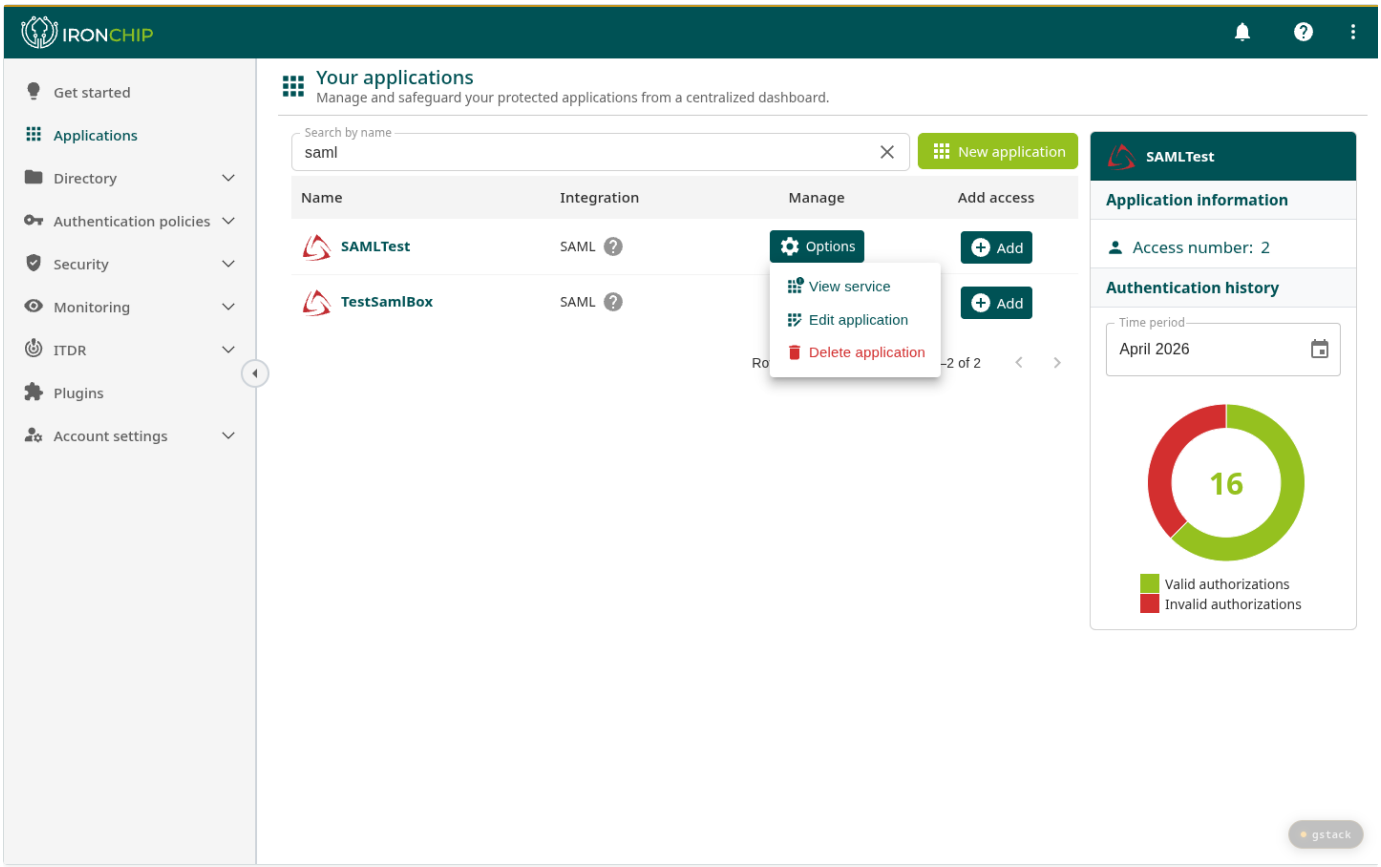
Escribe en **Search by name** para filtrar el listado en tiempo real:



Ejemplo: filtrar por "saml" muestra las dos aplicaciones SAML.

Acciones de gestión

Cada fila tiene un botón **Options** con tres acciones:



View service · Edit application · Delete application.

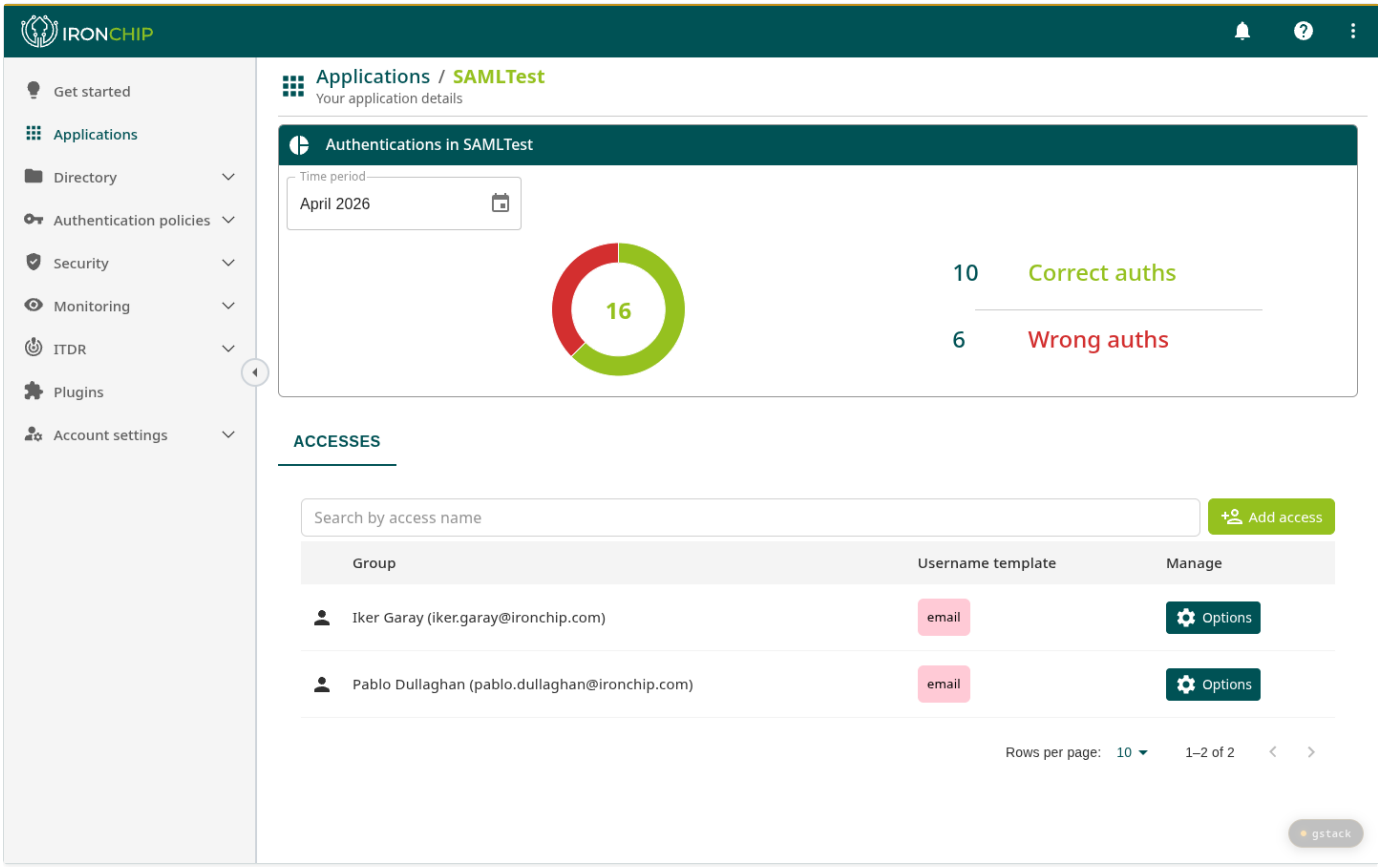
- **View service:** abre el detalle de la aplicación (capítulo 7).
- **Edit application:** permite cambiar el nombre y el logo. Para reconfigurar el SP/IdP/Redirect URIs hay que ir al detalle.
- **Delete application:** elimina la aplicación y todos sus accesos. Irreversible

CAPÍTULO 7

Detalle de una aplicación

Estadísticas de autenticación y gestión de accesos.

Cabecera



Aplicación SAMLTest — gráfico de autenticaciones y tabla de accesos.

El detalle de la aplicación muestra:

- **Authentications in <app>:** gráfico circular con autenticaciones **Correct** (verde) y **Wrong** (rojo) en el período seleccionado (selector *Time period*).
- **ACCESSES:** única pestaña visible, con la tabla de accesos asignados.

Tabla de accesos

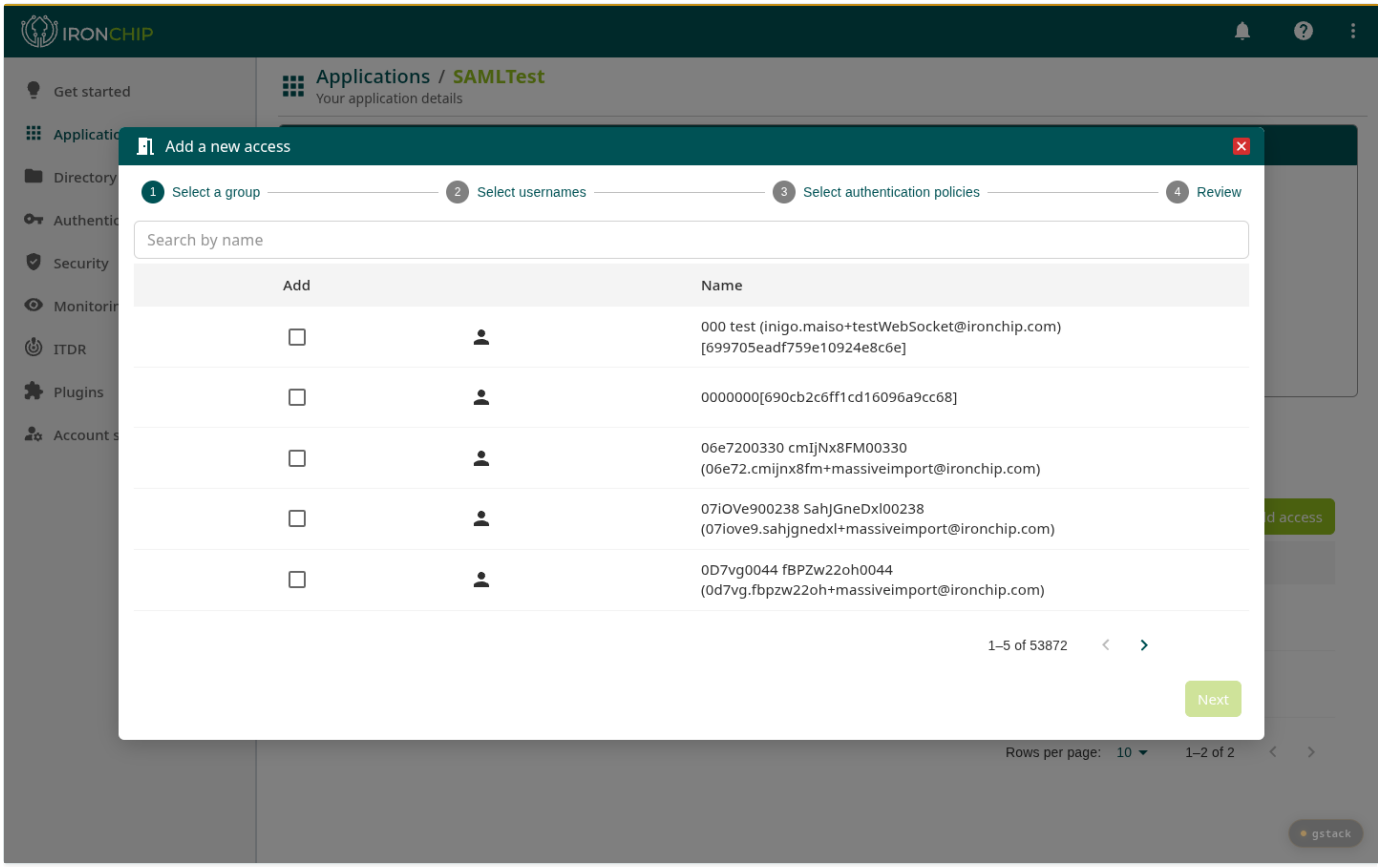
- **Group:** grupo o usuario al que se concedió el acceso.
- **Username template:** plantilla con la que se construye el username (p. ej. `email`).
- **Manage** / **Options:** menú con las acciones del acceso (capítulo 9).
- **Add access:** botón verde a la derecha — abre el asistente de creación de acceso.

CAPÍTULO 8

Crear un acceso

Asistente de 4 pasos para conceder permiso a un grupo de usuarios.

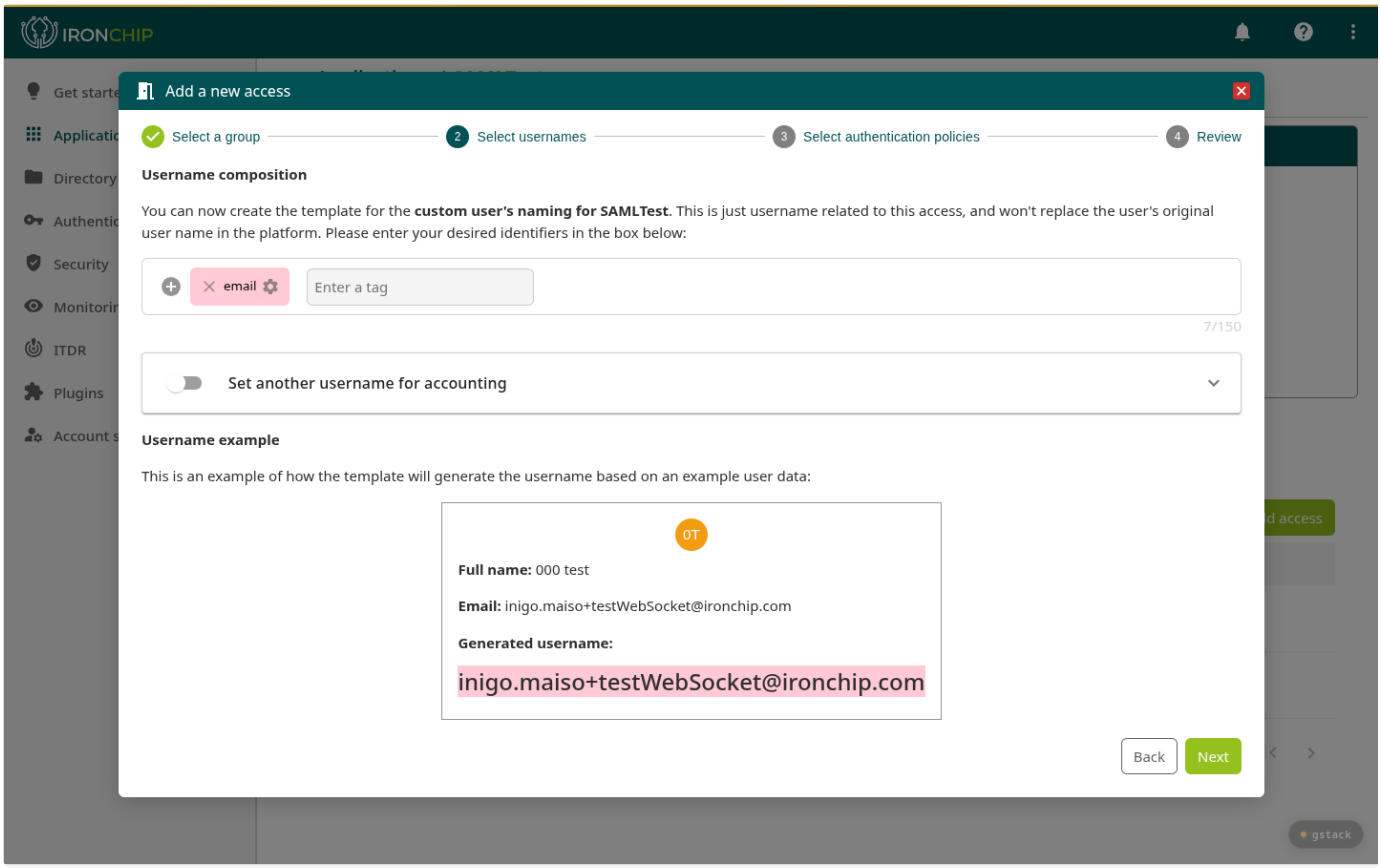
Paso 1 — Select a group



Selecciona uno o varios usuarios/grupos a los que dar acceso.

1. Busca con **Search by name**.
2. Marca el checkbox de cada usuario/grupo a incluir.
3. Pulsa **Next** para continuar.

Paso 2 — Select usernames (Username composition)

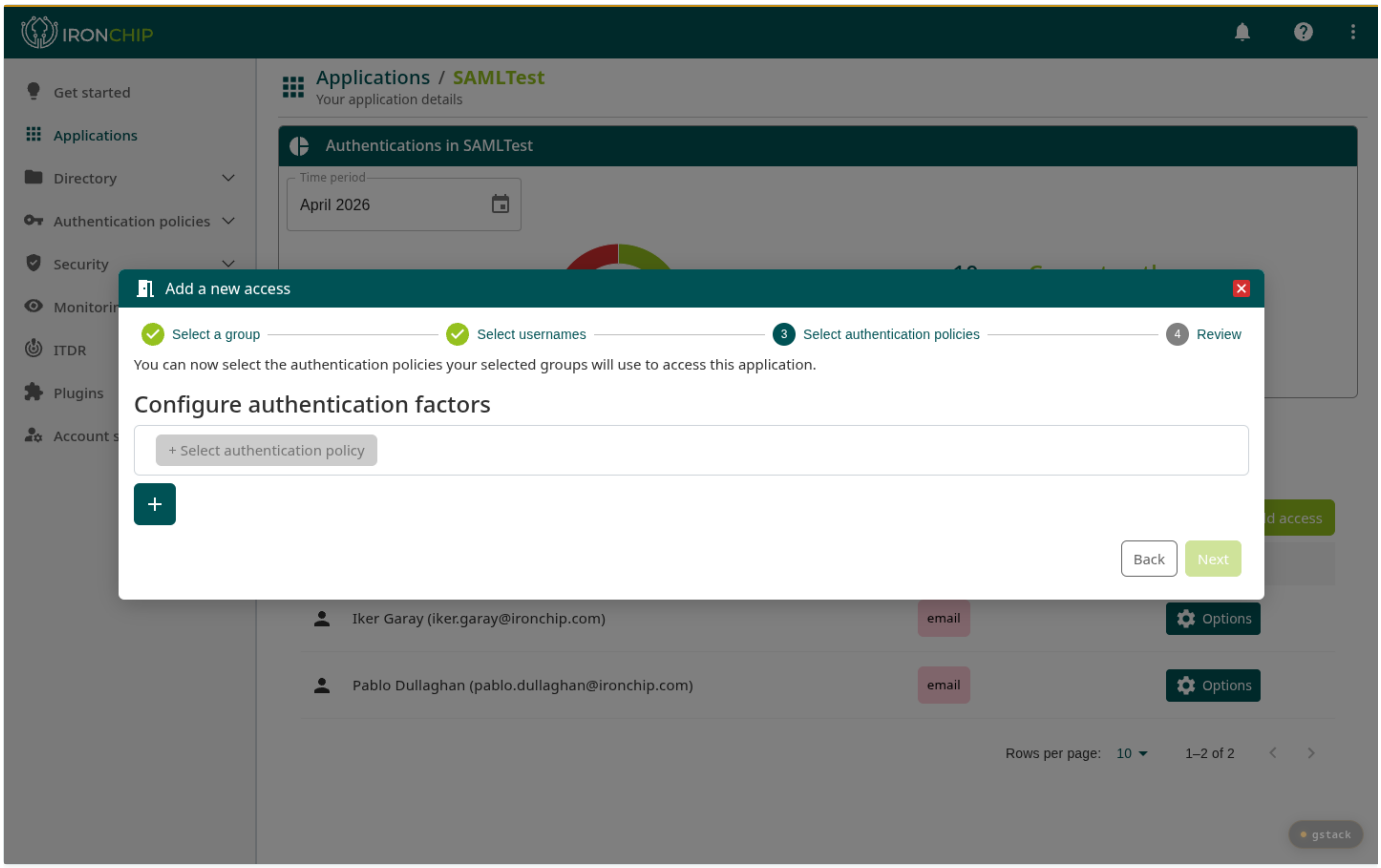


Define la plantilla con la que Ironchip generará el username de la aplicación.

Aquí se construye la plantilla del nombre de usuario que la aplicación verá. No reemplaza al nombre de usuario de la plataforma — solamente el que se le envía a la app.

1. Pulsa **+** para añadir tags (atributos del usuario).
2. Combina tags y texto literal en el campo "Enter a tag" (límite 150 caracteres).
3. Activa **Set another username for accounting** si necesitas un username distinto para auditoría/contabilidad.
4. El bloque **Username example** renderiza la plantilla con datos reales del primer usuario seleccionado para que veas el resultado antes de aplicar.

Paso 3 — Select authentication policies



Asigna las políticas que actuarán como factores de autenticación.

Este paso es donde se definen las **condiciones** que el usuario tendrá que cumplir para entrar:

1. Pulsa **+ Select authentication policy** para elegir una política existente (Device, Safe zone, Password, etc.).
2. Pulsa el **+** grande para añadir factores adicionales en cadena.
3. Cada política se evalúa en orden y el acceso se concede sólo si todas validan.

Las políticas se definen previamente en el menú lateral **Authentication policies** (volumen 3).

Paso 4 — Review

Resumen final con los grupos, plantillas de username y políticas seleccionadas. Confirma con **Submit** o vuelve atrás con **Back**.

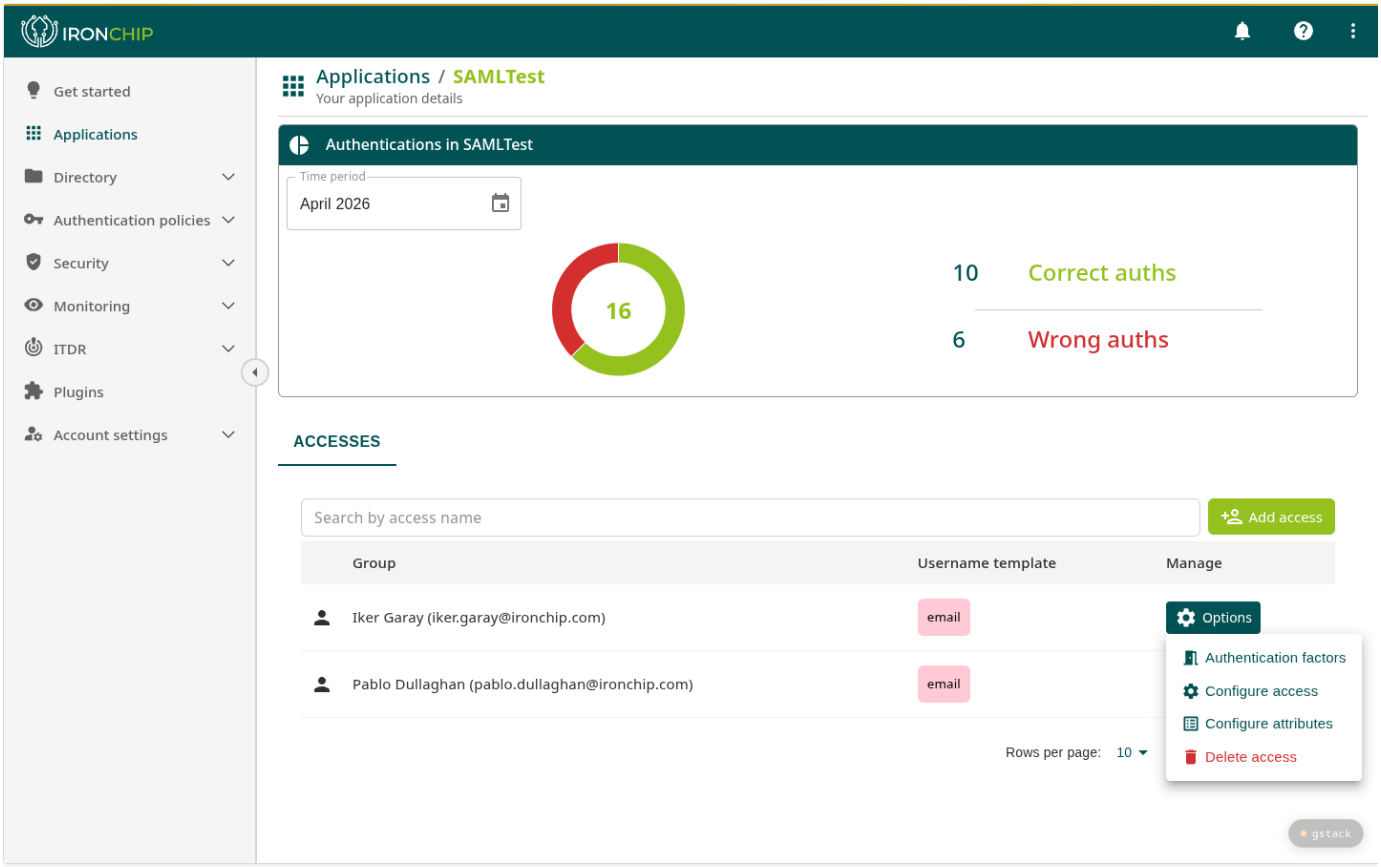
> **Borrar un acceso = quitar permiso:** eliminar un acceso desde la pestaña *Accesses* es la forma de revocar el permiso a un grupo o usuario sin tocar la aplicación ni los grupos.

CAPÍTULO 9

Gestionar un acceso existente

Menú "Options" de cada fila en la tabla de accesos.

Cuatro acciones



Authentication factors · Configure access · Configure attributes · Delete access.

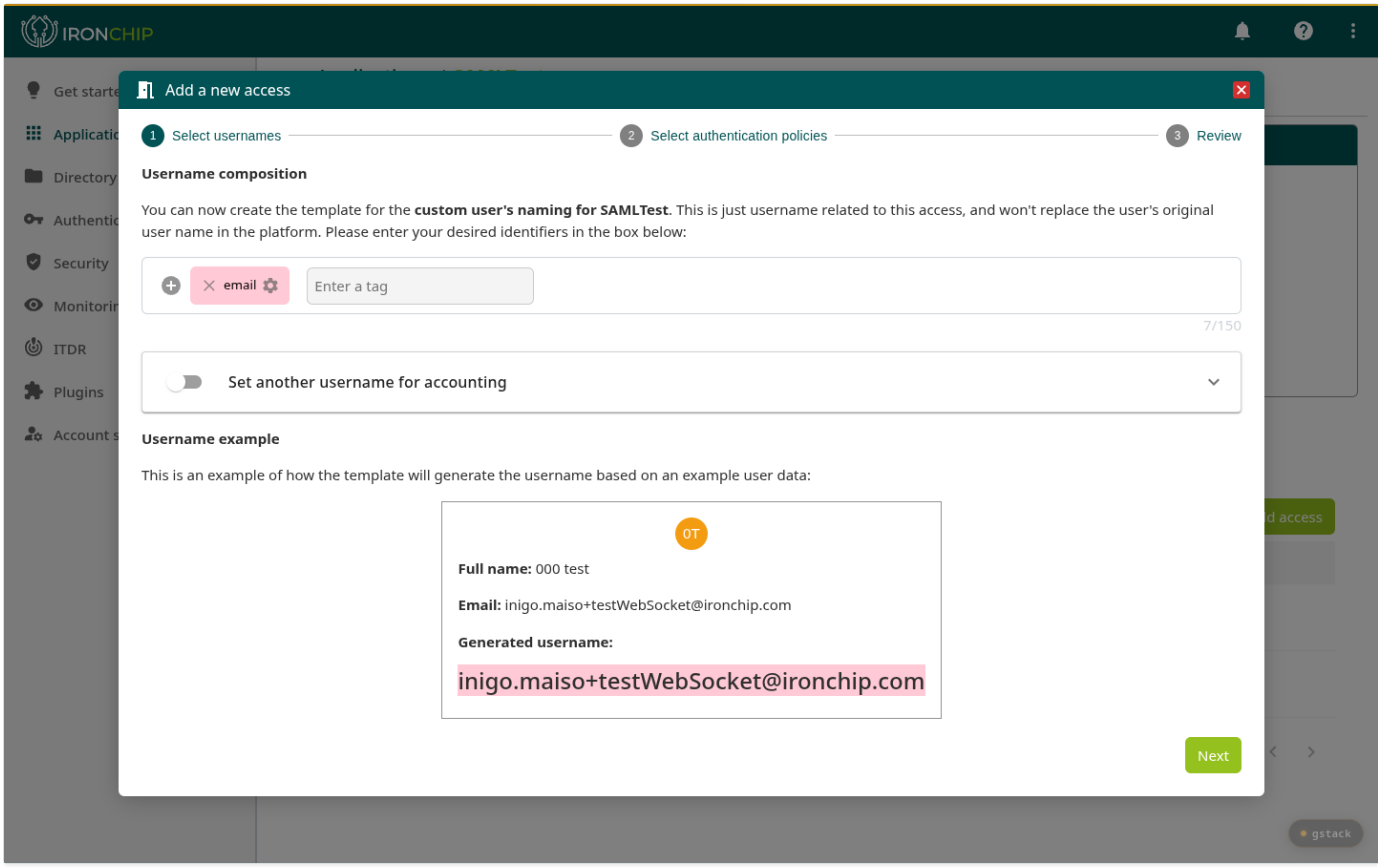
- **Authentication factors:** abre un modal en modo lectura con los factores actualmente requeridos para este acceso (igual que en la pestaña Accesses del usuario, vol. 1 cap. 7).
- **Configure access:** reabre el asistente desde el paso 1 (sin selección de grupo, ya está fijado) para reconfigurar username template y políticas (capítulo 10).
- **Configure attributes:** permite mapear atributos del usuario a atributos SAML/OIDC enviados a la aplicación.
- **Delete access:** revoca el acceso para ese grupo/usuario. Irreversible

CAPÍTULO 10

Reconfigurar un acceso (Configure access)

Cambiar el username template o las políticas sin recrear el acceso.

Asistente de 3 pasos



Mismo asistente que Add access pero sin el paso de selección de grupo.

Pulsando **Configure access** en el menú Options de un acceso entras en una versión simplificada del asistente:

1. **Select usernames:** editas la plantilla del username.
2. **Select authentication policies:** añades, quitas o reordenas factores.
3. **Review:** resumen y confirmación.

Es el flujo recomendado cuando, por ejemplo, quieres añadir un factor extra (p. ej. exigir Safe zone) a un acceso ya existente sin afectar al resto.

Resumen del flujo de accesos:

1. Crea grupos en *Directory · Groups*.
2. Crea aplicaciones en *Applications · New application*.
3. Crea políticas en *Authentication policies*.
4. En el detalle de cada aplicación, pulsa *Add access* para enlazar grupos + username template + políticas.
5. Itera con *Configure access* cuando cambien los requisitos.