Políticas y Seguridad

Manual del Dashboard Ironchip · Volumen 3

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

Contenido

CAPÍTULO 1

Políticas como factores de autenticación

Por qué existen las "Authentication policies".

El modelo de Ironchip

Ironchip no se queda en "usuario y contraseña". El acceso a una aplicación se concede cuando el usuario satisface una **cadena de factores** que tú defines. Cada factor es una *política de autenticación* — un conjunto de reglas que valida algo del contexto del usuario:

- ¿Está usando un dispositivo conocido?
- ¿Está conectándose desde una ubicación segura?
- ¿Su contraseña cumple con la política?

Las políticas se definen una vez en el menú lateral **Authentication policies** y luego se asignan a los accesos (vol. 2 cap. 8).

El menú tiene tres tipos:

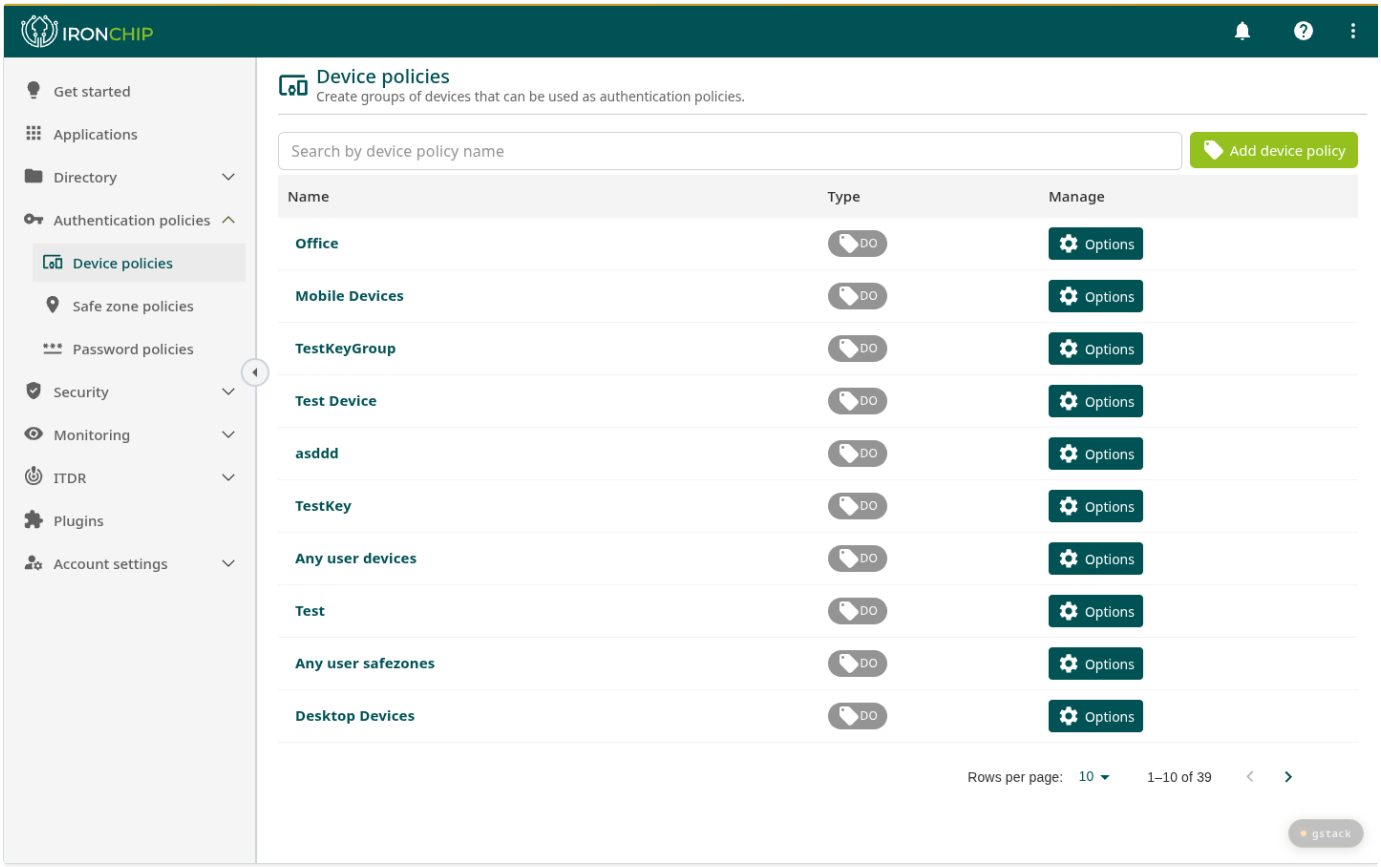
1. **Device policies** — qué dispositivos son válidos.
2. **Safe zone policies** — desde qué ubicaciones se permite acceder.
3. **Password policies** — qué reglas debe cumplir la contraseña (origen LDAP, Azure...).

CAPÍTULO 2

Device policies

Authentication policies · Device policies.

Listado de políticas de dispositivo



Cada política agrupa los dispositivos válidos para un perfil.

Una política de dispositivo es esencialmente un grupo de dispositivos que *califican* como factor válido. Ejemplos típicos en este entorno: **Office**, **Mobile Devices**, **Desktop Devices**, **Any user devices**.

Cabecera

- **Search by device policy name:** filtro.
- **Add device policy:** botón verde para crear una política nueva.

Columnas

- **Name:** nombre de la política.
- **Type:** tag `DO` (Device).
- **Manage** / **Options:** ver, editar miembros, eliminar.

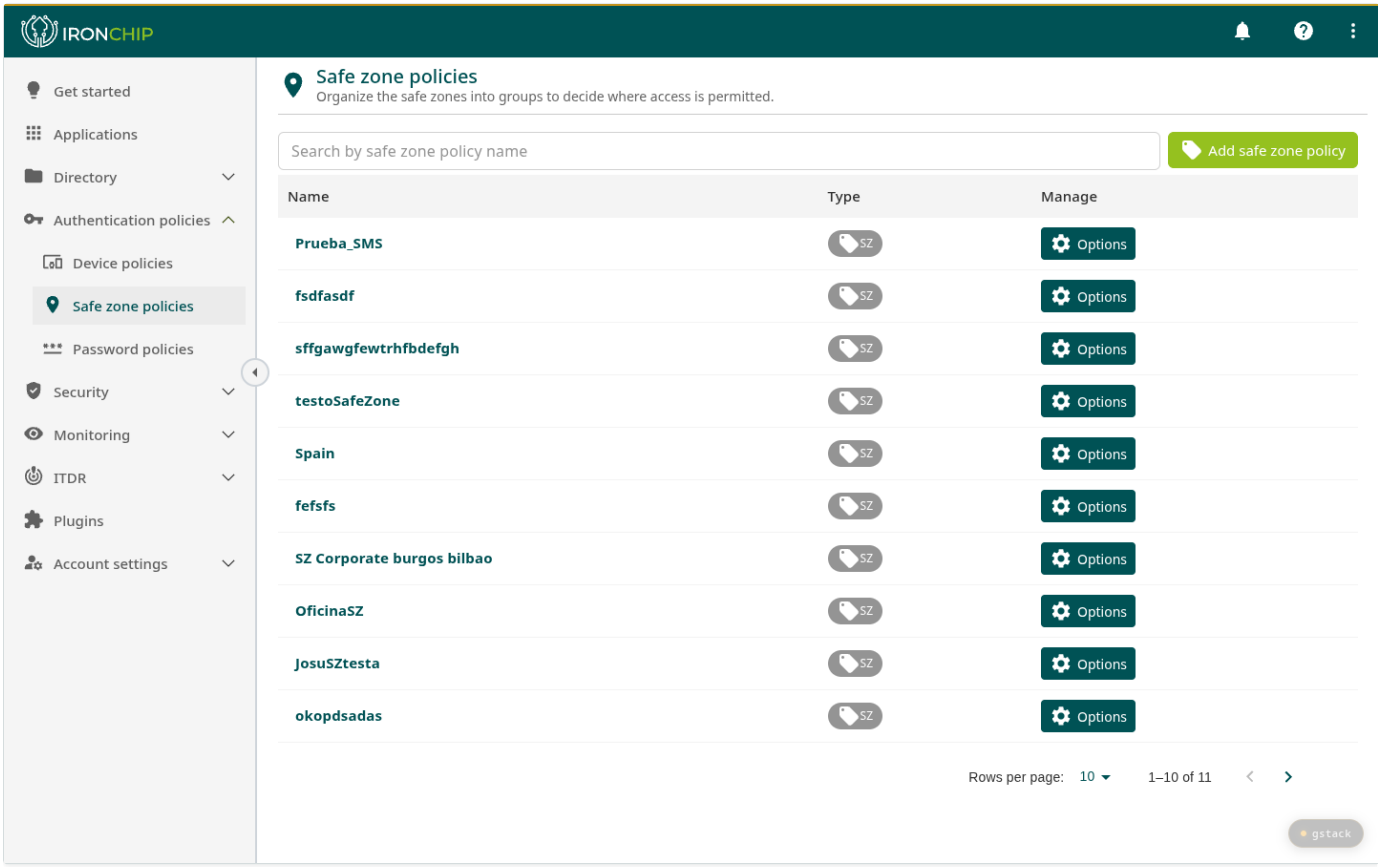
> **Ejemplo de uso:** creas una política "Corporate laptops" que solamente incluye los portátiles inventariados de la empresa. La asignas como factor a un acceso a Microsoft 365. Resultado: aunque el usuario tenga credenciales válidas, sólo puede entrar desde un portátil corporativo.

CAPÍTULO 3

Safe zone policies

Authentication policies · Safe zone policies.

Listado



Políticas que agrupan zonas seguras (geofences).

Las **safe zones** son geocercas (zonas geográficas que tú defines en *Directory · Safe zone*). Una **política de safe zone** agrupa varias safe zones para usarlas como un único factor.

Columnas

- **Name:** nombre de la política.
- **Type:** tag `SZ`.
- **Manage:** ver/editar miembros, eliminar.

Cabecera: **Search by safe zone policy name** y **Add safe zone policy**.

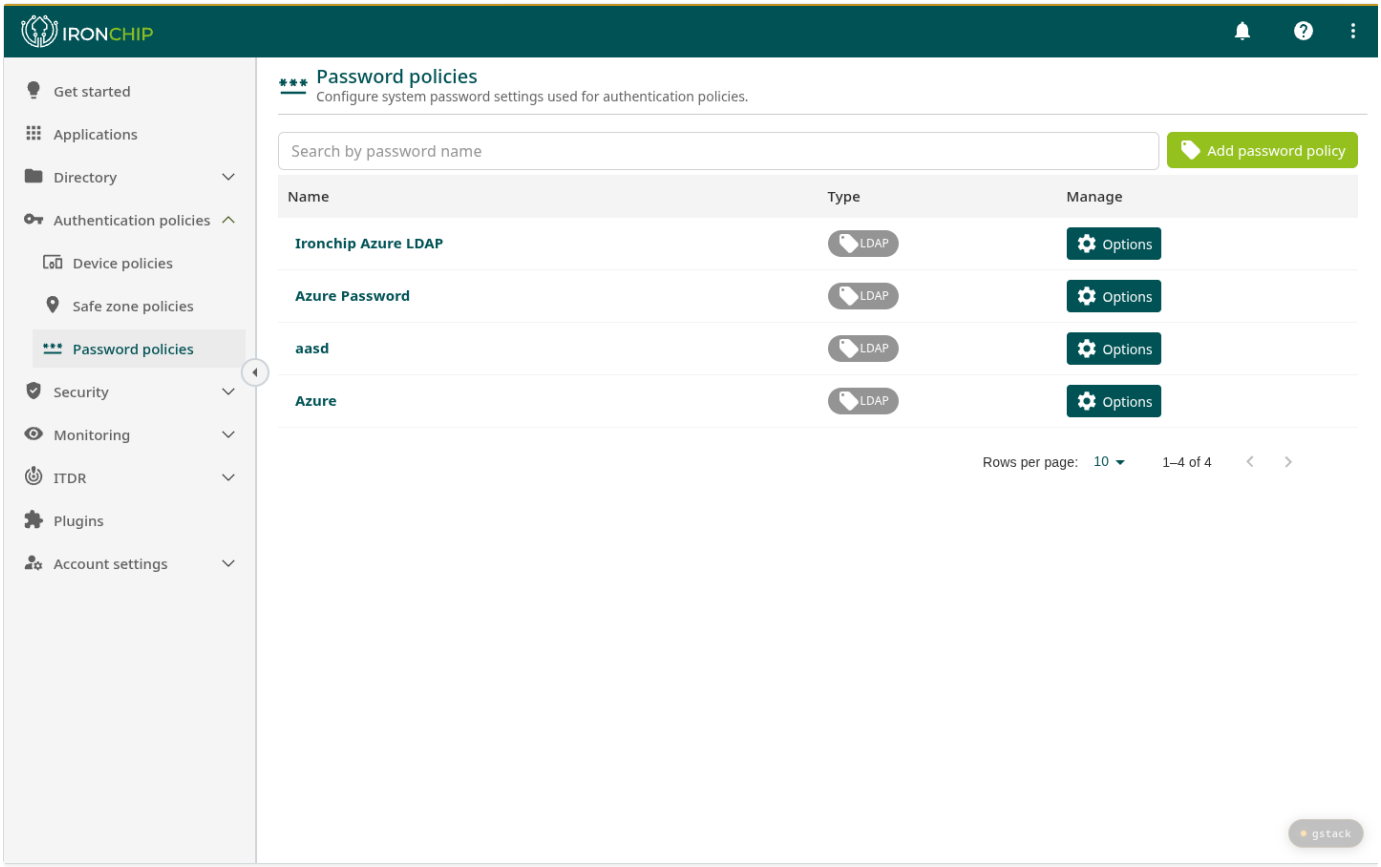
> **Ejemplo:** política "Spain offices" que agrupa las safe zones *Madrid HQ*, *Bilbao office* y *Barcelona office*. Asigna como factor a un acceso de RRHH para que sólo se pueda entrar desde una oficina española física.

CAPÍTULO 4

Password policies

Authentication policies · Password policies.

Listado



Configuración de orígenes de contraseña (LDAP, Azure...).

Aunque Ironchip es passwordless por filosofía, hay flujos legacy en los que se necesita validar la contraseña del usuario contra un origen externo (Azure AD, LDAP corporativo, etc.). Las **password policies** definen ese origen.

Columnas

- **Name:** nombre de la política.
- **Type:** origen — `LDAP` en este entorno.
- **Manage:** editar configuración, eliminar.

Cabecera: **Search by password name** y **Add password policy**.

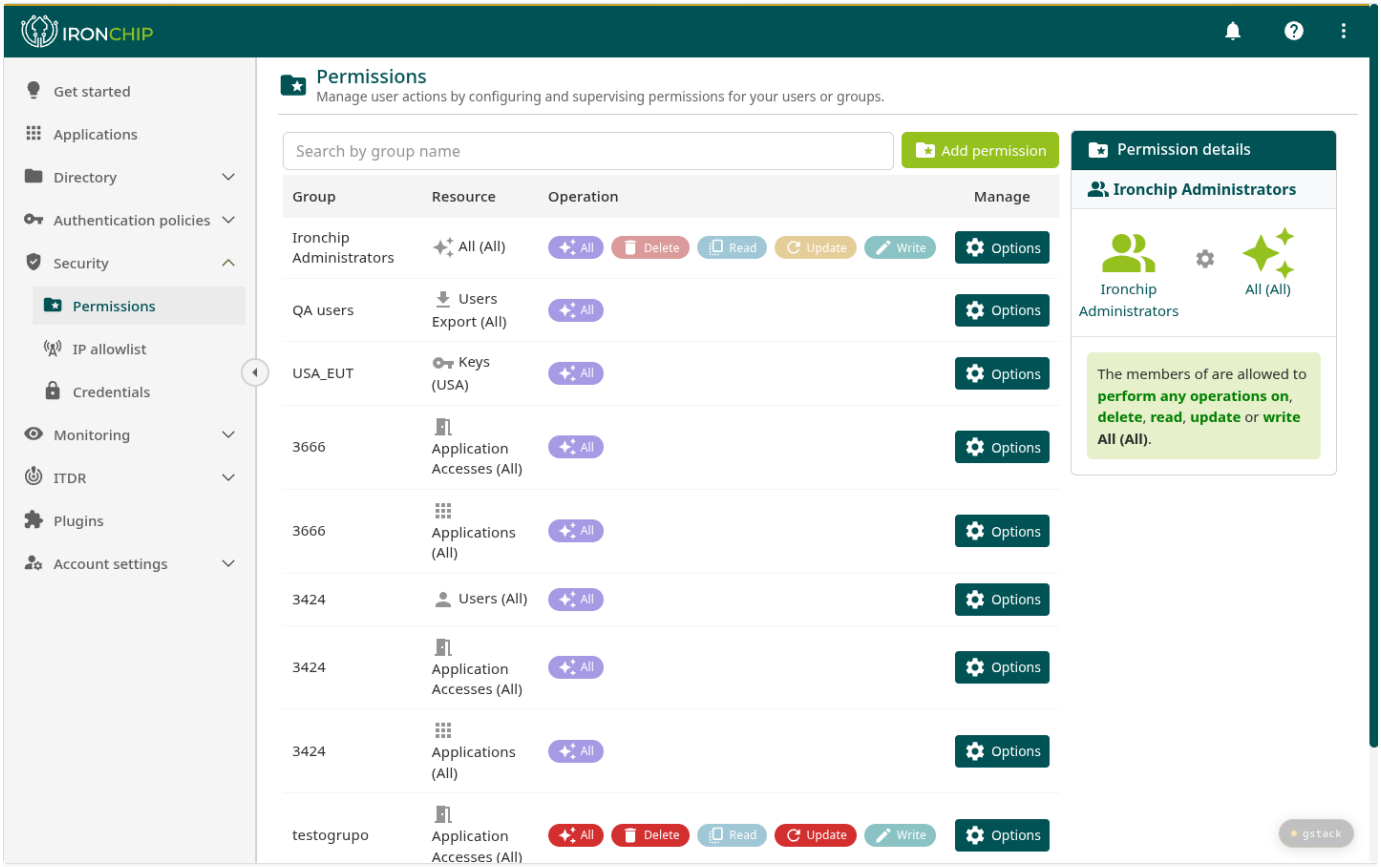
CAPÍTULO 5

Permisos de administradores

Security · Permissions.

Concepto

Esta sección controla **quién puede hacer qué dentro del propio dashboard**. No regula el acceso a aplicaciones externas (eso se hace en *Applications · Add access*); regula los privilegios de los administradores sobre la propia plataforma.



Cada fila es un permiso: grupo + recurso + operaciones autorizadas.

Anatomía de un permiso

- **Group:** grupo de administradores que recibe el permiso (p. ej. *Ironchip Administrators*, *QA users*).
- **Resource:** recurso afectado (Users, Keys, Application Accesses, Applications, Users Export...). Cada recurso puede limitarse a una región/aplicación o ser *(All)*.
- **Operation:** operaciones permitidas — combinación de `All`, `Delete`, `Read`, `Update`, `Write`.
- **Manage:** editar o eliminar el permiso.

Panel de detalle

Al pulsar sobre una fila, el panel derecho **Permission details** resume el permiso en lenguaje natural: *"The members of <grupo> are allowed to perform any operations on, delete, read, update or write <recurso>."*

Acciones

- **Search by group name:** filtro.
- **Add permission:** crear un permiso nuevo combinando grupo + recurso + operaciones.

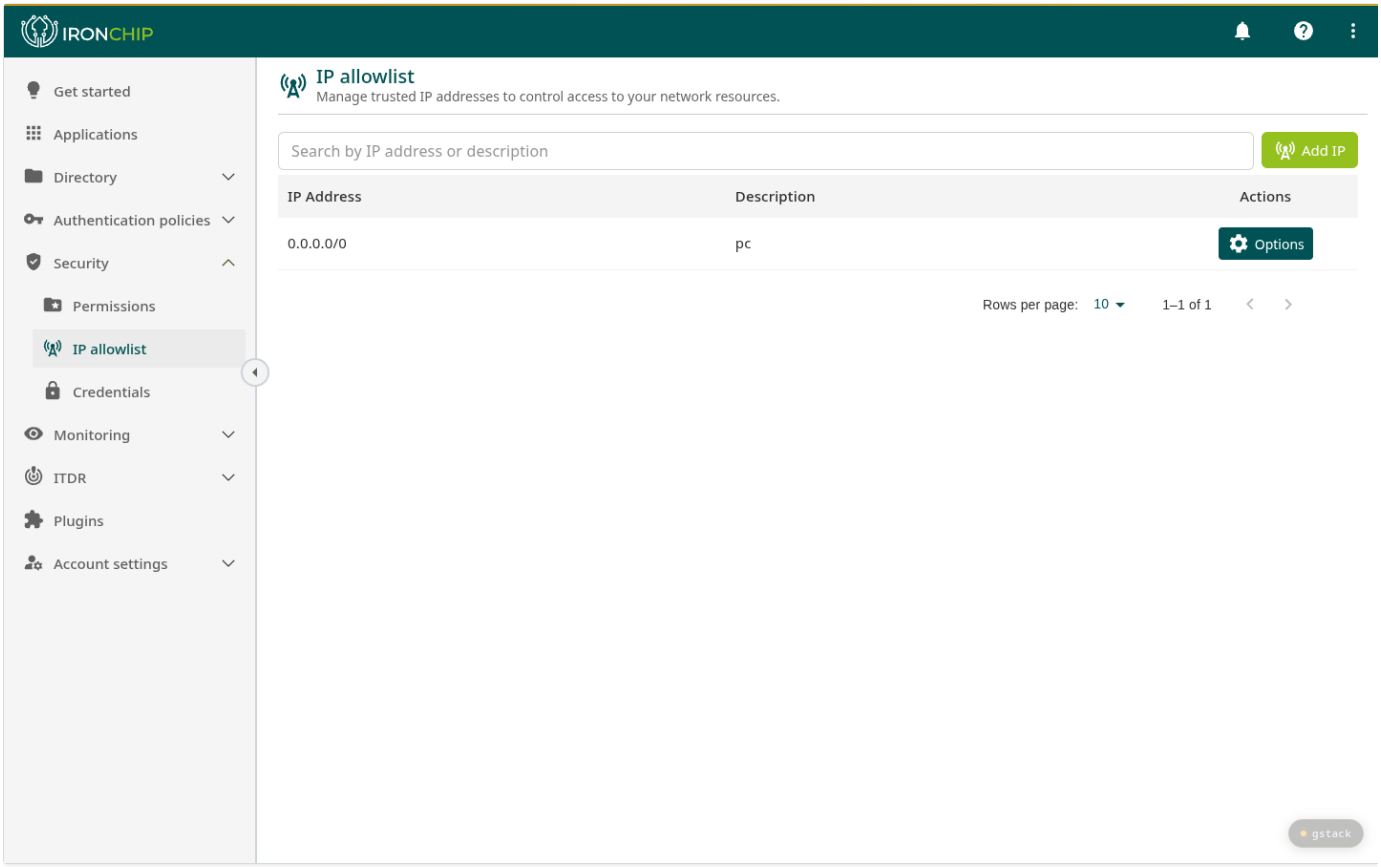
> **Cuidado con "All / All":** conceder operaciones *All* sobre el recurso *All* equivale a un super-admin. Reserva esto para un grupo muy reducido (idealmente sólo *Ironchip Administrators*).

CAPÍTULO 6

Lista blanca de IPs

Security · IP allowlist.

Listado



Direcciones o rangos CIDR de confianza para acceder a recursos de red.

Define IPs o rangos CIDR autorizados para controlar el acceso a recursos de red de la empresa.

Columnas

- **IP Address:** IP individual o CIDR (p. ej. `0.0.0.0/0` para "cualquiera").
- **Description:** texto libre para documentar a qué corresponde la entrada.
- **Actions** / **Options:** editar o eliminar.

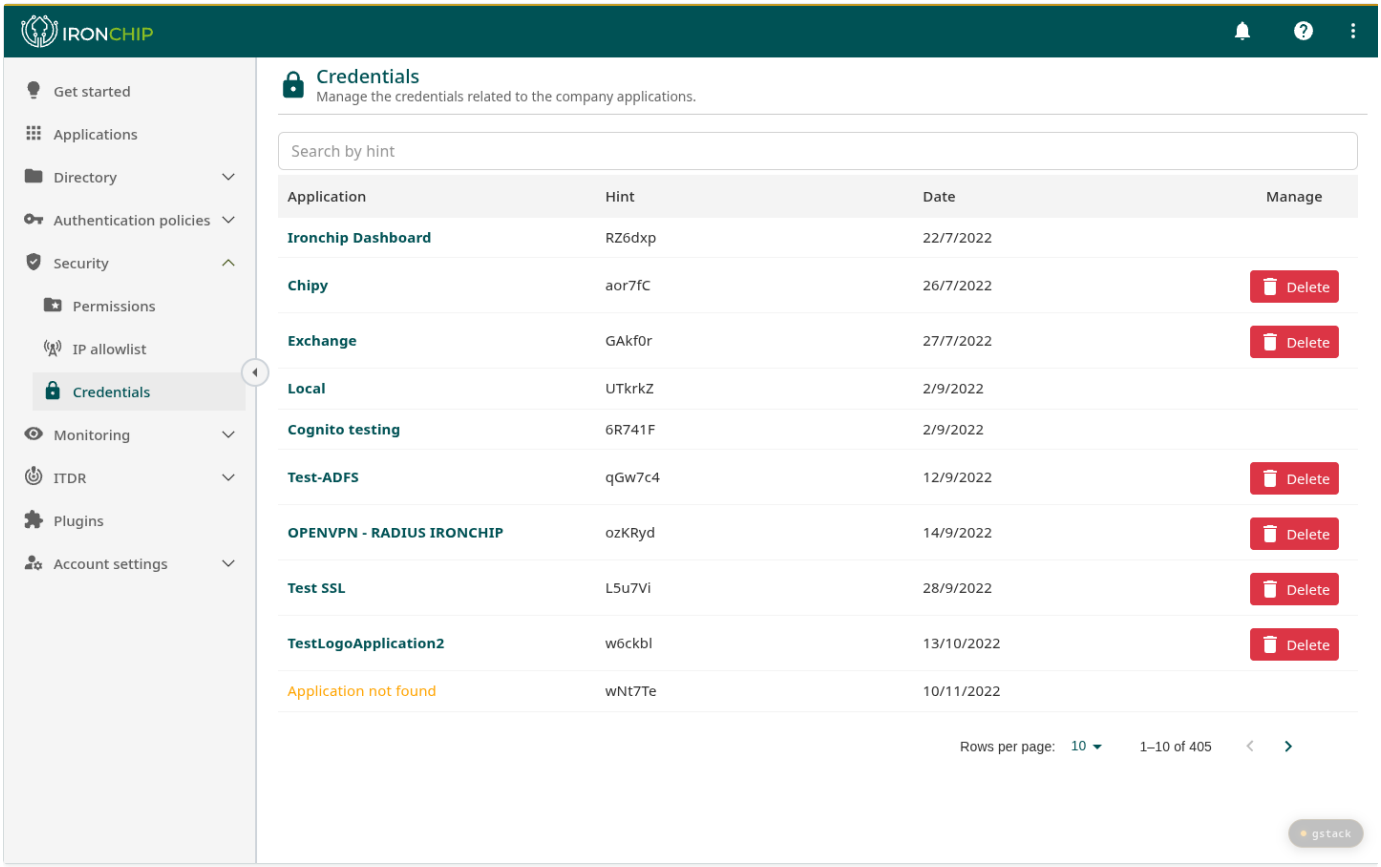
Cabecera: **Search by IP address or description** y **Add IP**.

CAPÍTULO 7

Credenciales de aplicaciones

Security · Credentials.

Listado



Histórico de credenciales (API keys) emitidas por Ironchip.

Ironchip emite credenciales (API keys) para que servicios externos hablen con la plataforma. Esta tabla las gestiona.

Columnas

- **Application:** aplicación a la que pertenece la credencial.
- **Hint:** primeros caracteres de la credencial (lo único que se mantiene visible — la credencial completa sólo se muestra en el momento de la creación).
- **Date:** fecha de emisión.
- **Manage:** botón **Delete** (rojo) para revocarla.

Cabecera: **Search by hint** permite buscar por las primeras letras del secreto.

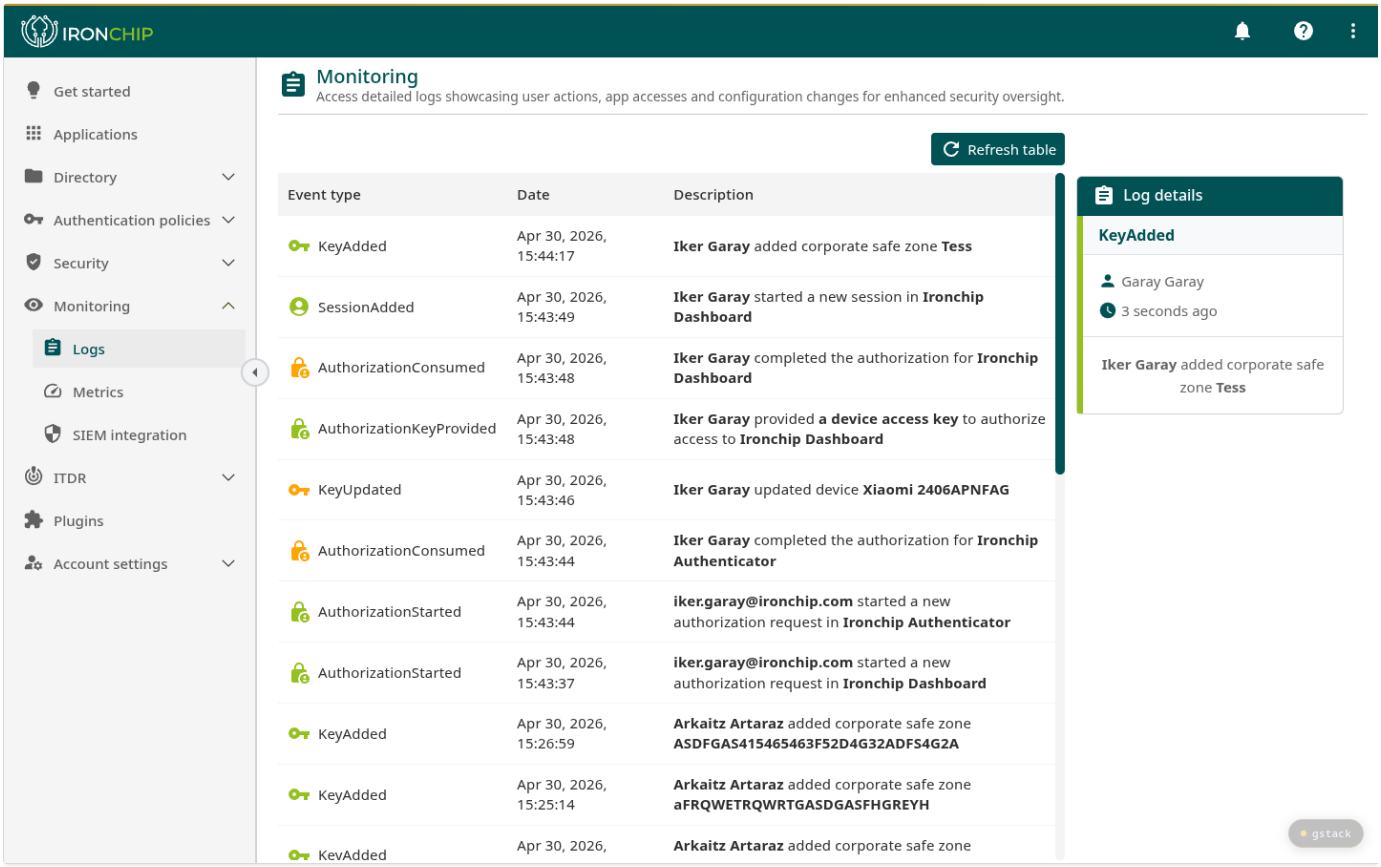
> **Rotación:** si una credencial se filtra, bórrala desde aquí y emite una nueva en el detalle de la aplicación correspondiente. La credencial borrada deja de funcionar de inmediato.

CAPÍTULO 8

Monitoring · Logs

Monitoring · Logs (timeline de actividad).

Vista en timeline



Eventos en tiempo real con panel de detalle a la derecha.

Stream cronológico de todos los eventos de la cuenta: altas, bajas, autenticaciones, cambios de configuración. Útil para auditoría y forense.

Columnas

- **Event type:** tipo (KeyAdded, SessionAdded, AuthorizationConsumed, AuthorizationProvided, AuthorizationStarted, etc.).
- **Date:** fecha y hora.
- **Description:** resumen en lenguaje natural ("<User> added corporate safe zone <X>", "started a new session in Ironchip Dashboard"...).

Panel de detalle

Al pulsar sobre un evento, el panel **Log details** a la derecha muestra todos los metadatos del evento (User ID, timestamps, payload).

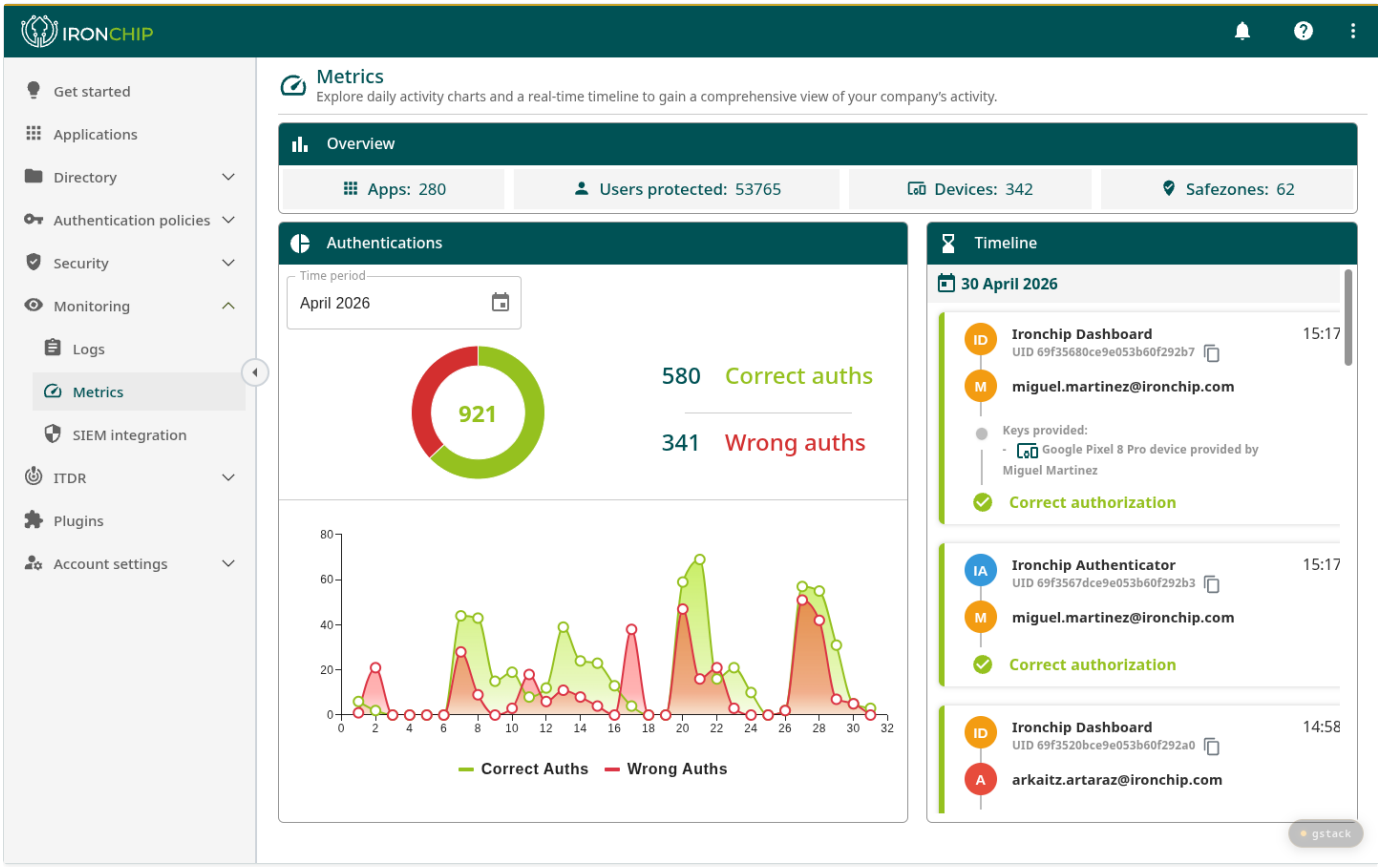
Pulsa **Refresh table** en la cabecera para recargar.

CAPÍTULO 9

Monitoring · Metrics

KPIs y serie temporal de autenticaciones.

Dashboard de métricas



Overview, gráfico circular y serie temporal diaria.

Bloque Overview

- **Apps:** número total de aplicaciones protegidas.
- **Users protected:** usuarios totales en la plataforma.
- **Devices:** dispositivos enrolados.
- **Safezones:** safe zones definidas.

Bloque Authentications

- **Time period:** selector de mes.
- Gráfico circular con número total y desglose entre **Correct auths** (verde) y **Wrong auths** (rojo).
- Serie temporal por día con líneas verde/rojo para autorizaciones correctas/incorrectas.

Bloque Timeline

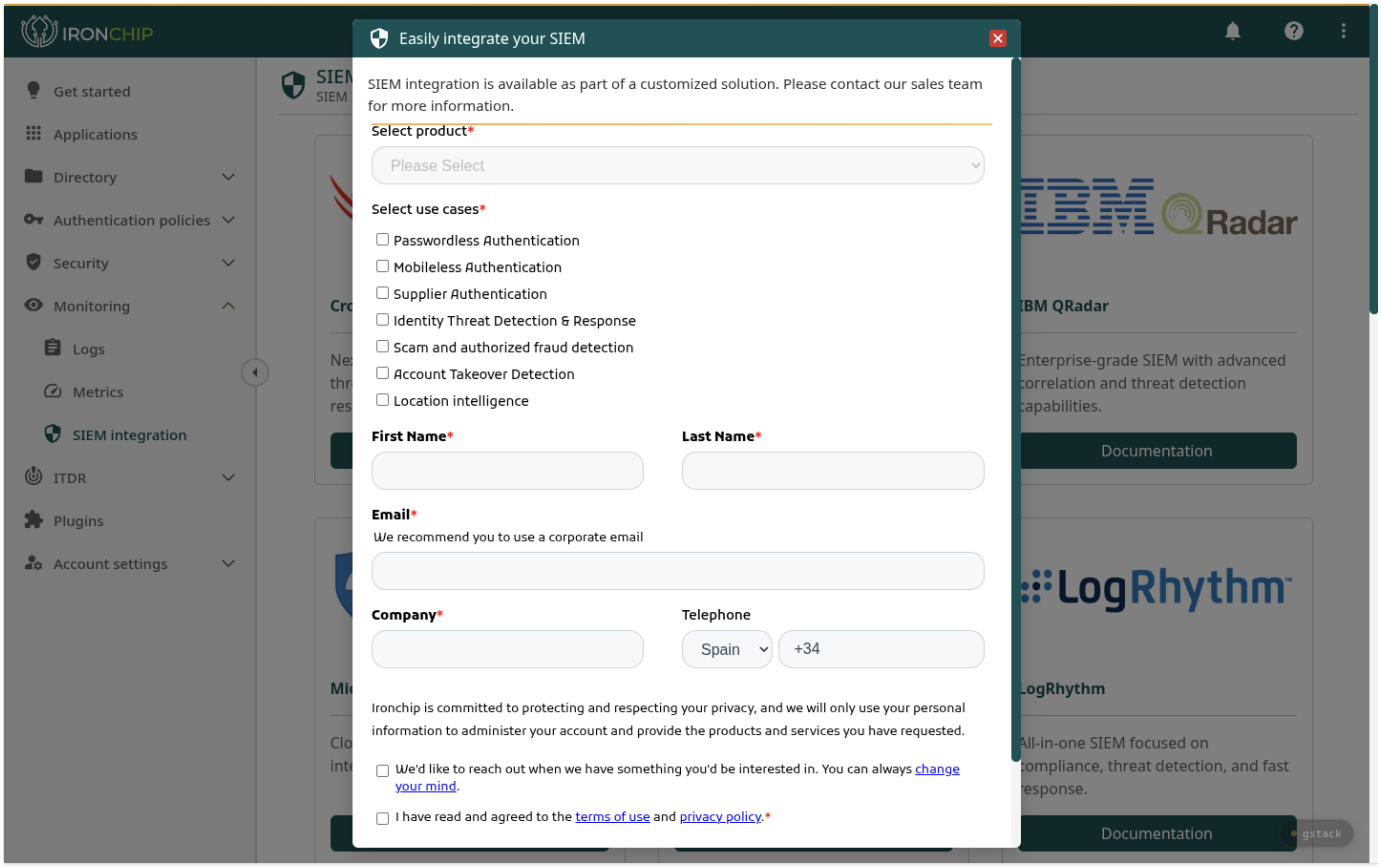
Panel lateral derecho con eventos del día seleccionado: usuario, dispositivo y resultado.

CAPÍTULO 10

Monitoring · SIEM integration

Conexión con sistemas SIEM externos.

Activación bajo solicitud



Formulario de contacto para activar la integración SIEM.

La integración con SIEM (IBM QRadar, LogRhythm, Splunk...) se ofrece como solución personalizada. Al entrar a la pestaña, aparece un formulario de contacto para que el equipo de ventas active la funcionalidad.

Datos a rellenar

1. **Select product:** producto SIEM destino.
2. **Select use cases:** casos de uso (Passwordless, Mobileless, Supplier auth, ITDR, fraud detection, Account Takeover, Location intelligence).
3. Datos de contacto: First Name, Last Name, Email, Company, Telephone.
4. Aceptar términos y privacidad.

Tras enviarlo, el equipo comercial contacta para configurar el pipeline de logs hacia el SIEM elegido.

> **Mientras tanto:** los logs siempre se pueden exportar manualmente desde *Monitoring · Logs*, o consumirse vía API REST (con credenciales gestionadas en Security · Credentials).