



Políticas y Seguridad

Manual del Dashboard Ironchip · Volumen 3

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

Contenido

1. Concepto: políticas como factores de autenticación
2. Políticas de dispositivo (Device policies)
3. Políticas de zona segura (Safe zone policies)
4. Políticas de contraseña (Password policies)
5. Permisos de administradores (Permissions)
6. Lista blanca de IPs (IP allowlist)
7. Credenciales de aplicaciones (Credentials)
8. Monitoring - Logs
9. Monitoring - Metrics
0. Monitoring - SIEM integration

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...).

Device policies

Authentication policies · Device policies.

Listado de políticas de dispositivo

Device policies
Create groups of devices that can be used as authentication policies.

Search by device policy name Add device policy

Name	Type	Manage
Office	DO	Options
Mobile Devices	DO	Options
TestKeyGroup	DO	Options
Test Device	DO	Options
asddd	DO	Options
TestKey	DO	Options
Any user devices	DO	Options
Test	DO	Options
Any user safezones	DO	Options
Desktop Devices	DO	Options

Rows per page: 10 1–10 of 39 gstack

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.

Safe zone policies

Authentication policies · Safe zone policies.

Listado

Safe zone policies
Organize the safe zones into groups to decide where access is permitted.

Search by safe zone policy name Add safe zone policy

Name	Type	Manage
Prueba_SMS		Options
fsdfasdf		Options
sffgawfewtrhfbdefgh		Options
testoSafeZone		Options
Spain		Options
fefsf		Options
SZ Corporate burgos bilbao		Options
OficinaSZ		Options
JosusZtesta		Options
okopdsadas		Options

Rows per page: 10 1–10 of 11 gstack

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 .
- **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.

Password policies

Authentication policies · Password policies.

Listado

***** Password policies**
Configure system password settings used for authentication policies.

Search by password name Add password policy

Name	Type	Manage
Ironchip Azure LDAP	LDAP	Options
Azure Password	LDAP	Options
aasd	LDAP	Options
Azure	LDAP	Options

Rows per page: 10 ▾ 1-4 of 4 < >

gstack

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**.

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.

The screenshot displays the 'Permissions' management page in the Ironchip dashboard. On the left is a navigation sidebar with categories like 'Get started', 'Applications', 'Directory', 'Authentication policies', 'Security', 'Permissions', 'IP allowlist', 'Credentials', 'Monitoring', 'ITDR', 'Plugins', and 'Account settings'. The main area is titled 'Permissions' and includes a search bar and an 'Add permission' button. Below is a table with columns for Group, Resource, Operation, and Manage. The table lists permissions for groups like 'Ironchip Administrators', 'QA users', 'USA_EUT', and 'testgrupo'. The 'Permission details' panel on the right provides a natural language summary for the 'Ironchip Administrators' group: 'The members of are allowed to perform any operations on, delete, read, update or write All (All)'.

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*).

Lista blanca de IPs

Security · IP allowlist.

Listado

The screenshot shows the IRONCHIP IP allowlist management interface. On the left is a navigation sidebar with options like 'Get started', 'Applications', 'Directory', 'Authentication policies', 'Security', 'Permissions', 'IP allowlist' (selected), 'Credentials', 'Monitoring', 'ITDR', 'Plugins', and 'Account settings'. The main content area is titled 'IP allowlist' with the subtitle 'Manage trusted IP addresses to control access to your network resources.' It features a search bar 'Search by IP address or description' and an 'Add IP' button. Below is a table with columns 'IP Address', 'Description', and 'Actions'. One entry is visible: IP Address '0.0.0.0/0' and Description 'pc'. An 'Options' button is next to this entry. At the bottom right of the table area, it says 'Rows per page: 10' and '1-1 of 1'. A 'gstack' logo is in the bottom right corner of the interface.

IP Address	Description	Actions
0.0.0.0/0	pc	Options

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**.

Credenciales de aplicaciones

Security · Credentials.

Listado

Credentials
Manage the credentials related to the company applications.

Search by hint

Application	Hint	Date	Manage
Ironchip Dashboard	RZ6dxp	22/7/2022	
Chipy	aor7fC	26/7/2022	Delete
Exchange	GAkf0r	27/7/2022	Delete
Local	UTkrkZ	2/9/2022	
Cognito testing	6R741F	2/9/2022	
Test-ADFS	qGw7c4	12/9/2022	Delete
OPENVPN - RADIUS IRONCHIP	ozkRyd	14/9/2022	Delete
Test SSL	L5u7Vi	28/9/2022	Delete
TestLogoApplication2	w6ckbl	13/10/2022	Delete
Application not found	wNt7Te	10/11/2022	

Rows per page: 10 1–10 of 405

gstack

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.

Monitoring · Logs

Monitoring · Logs (timeline de actividad).

Vista en timeline

Monitoring
Access detailed logs showcasing user actions, app accesses and configuration changes for enhanced security oversight.

Refresh table

Event type	Date	Description
KeyAdded	Apr 30, 2026, 15:44:17	Iker Garay added corporate safe zone Tess
SessionAdded	Apr 30, 2026, 15:43:49	Iker Garay started a new session in Ironchip Dashboard
AuthorizationConsumed	Apr 30, 2026, 15:43:48	Iker Garay completed the authorization for Ironchip Dashboard
AuthorizationKeyProvided	Apr 30, 2026, 15:43:48	Iker Garay provided a device access key to authorize access to Ironchip Dashboard
KeyUpdated	Apr 30, 2026, 15:43:46	Iker Garay updated device Xiaomi 2406APNFAG
AuthorizationConsumed	Apr 30, 2026, 15:43:44	Iker Garay completed the authorization for Ironchip Authenticator
AuthorizationStarted	Apr 30, 2026, 15:43:44	iker.garay@ironchip.com started a new authorization request in Ironchip Authenticator
AuthorizationStarted	Apr 30, 2026, 15:43:37	iker.garay@ironchip.com started a new authorization request in Ironchip Dashboard
KeyAdded	Apr 30, 2026, 15:26:59	Arkaitz Artaraz added corporate safe zone ASDFGAS415465463F52D4G32ADFS4G2A
KeyAdded	Apr 30, 2026, 15:25:14	Arkaitz Artaraz added corporate safe zone aFRQWETRQWRTGASDGASFHGREYH
KeyAdded	Apr 30, 2026,	Arkaitz Artaraz added corporate safe zone

Log details

KeyAdded

Garay Garay
3 seconds ago

Iker Garay added corporate safe zone Tess

gstack

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

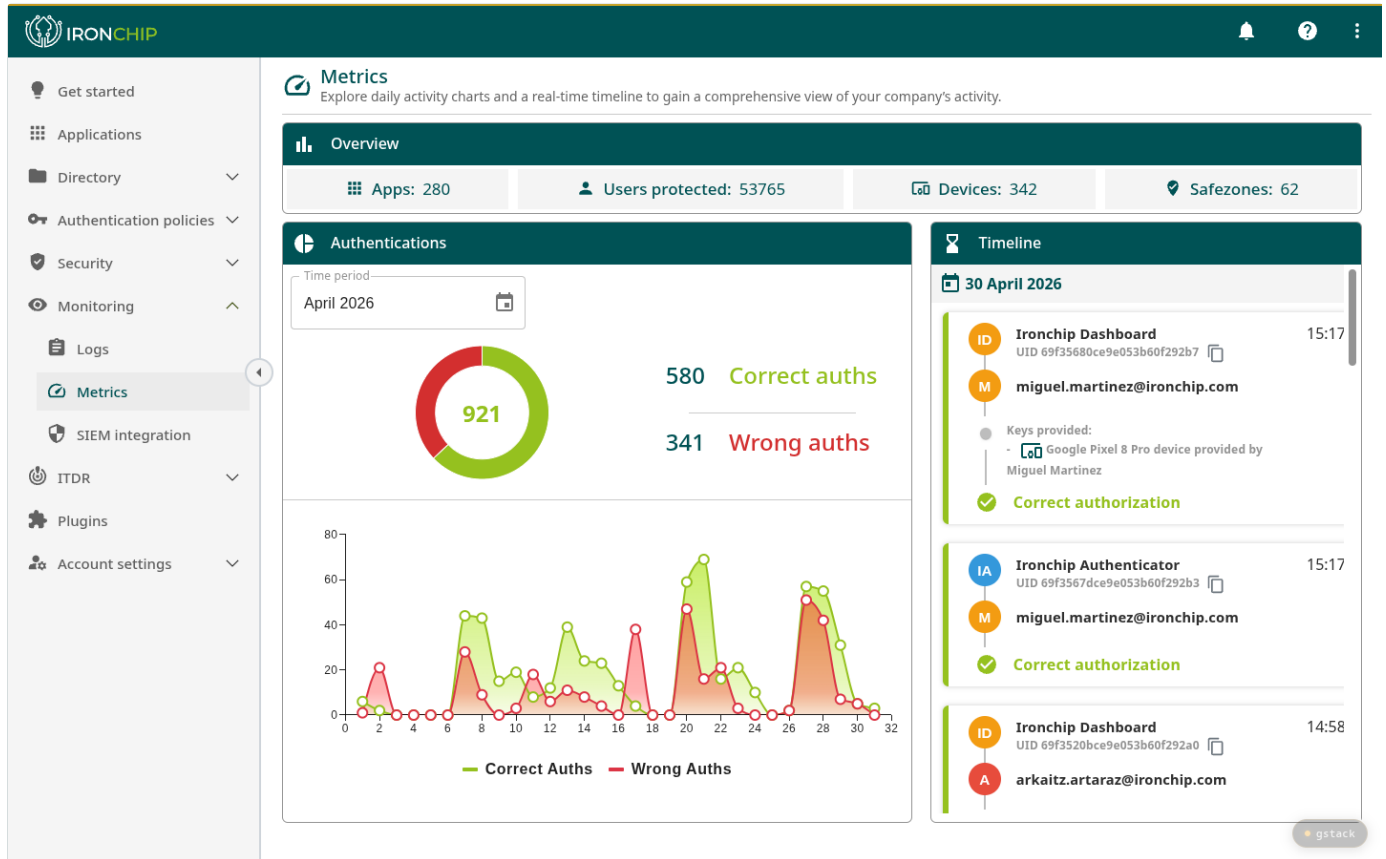
Al pulsar sobre un evento, el panel **Log details** a la derecha muestra todos los metadatos del evento (User ID, timestamps, payload).

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

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.

Monitoring · SIEM integration

Conexión con sistemas SIEM externos.

Activación bajo solicitud

Easily integrate your SIEM

SIEM integration is available as part of a customized solution. Please contact our sales team for more information.

Select product*

Please Select

Select use cases*

- Passwordless Authentication
- Mobileless Authentication
- Supplier Authentication
- Identity Threat Detection & Response
- Scam and authorized fraud detection
- Account Takeover Detection
- Location intelligence

First Name*

Last Name*

Email*
We recommend you to use a corporate email

Company*

Telephone
Spain +34

Ironchip is committed to protecting and respecting your privacy, and we will only use your personal information to administer your account and provide the products and services you have requested.

We'd like to reach out when we have something you'd be interested in. You can always [change your mind](#).

I have read and agreed to the [terms of use](#) and [privacy policy](#).*

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*).