



ITDR, Directorio y Cuenta

Manual del Dashboard Ironchip · Volumen 4

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

Contenido

1. ITDR · concepto general
2. ITDR · Realtime feed
3. ITDR · Threat analysis (Confirmed / Suspected)
4. ITDR · Ruleset y Toolset
5. Directory · Devices (Mobile, Desktop, RFID)
6. Directory · Safe zones (Corporate, Personal)
7. Directory · Synchronization (CSV, SCIM)
8. Plugins
9. Account settings · Billing
0. Account settings · Look & feel

ITDR — Identity Threat Detection & Response

Concepto general.

Para qué sirve

ITDR (Identity Threat Detection & Response) es el módulo de detección y respuesta ante amenazas de identidad de Ironchip. Su trabajo es:

1. Recolectar señales de actividad de identidad en tiempo real.
2. Detectar patrones sospechosos (login imposible, suplantación, anomalías).
3. Permitir al administrador investigar, confirmar y responder.

El módulo se divide en cuatro pestañas en el menú lateral:

- **Realtime feed:** stream de eventos en directo.
- **Threat analysis:** incidentes *Confirmed* y *Suspected*.
- **Ruleset:** reglas de detección por User, Location, Device, Network o Custom.
- **Toolset:** herramientas de respuesta.

Acceso bajo plan: ITDR es una funcionalidad de plan superior. En cuentas sin contrato ITDR se muestra un modal "Unable to access ITDR" al entrar y los submenús de Ruleset/Toolset llevan a una página de "Contact sales to activate this feature".

ITDR · Realtime feed

Stream de eventos en tiempo real.

La pestaña

The screenshot displays the 'ITDR - Real-time feed' interface. On the left is a sidebar with navigation items. The main area features a table with columns: Risk level, Date, User Id, Blocked, and Manage. A 'Refresh table' button is located above the table. A modal dialog box is centered on the screen, titled 'Unable to access ITDR', containing a warning icon and the following text: 'Your current account does not have permissions to view the ITDR reports or your Company doesn't have a plan that provide this feature. You can unlock this feature by requesting it from your Company manager.' The modal includes 'Close' and 'Back to home' buttons. In the top right of the table area, there is a message: 'No transaction report selected' with a warning icon. The bottom right corner of the interface shows a 'gstack' logo.

Tabla con Risk level, Date, User Id, Blocked y Manage; panel de detalle a la derecha.

Columnas

- **Risk level:** nivel de riesgo asignado por el motor de detección.
- **Date:** instante del evento.
- **User Id:** identidad afectada.
- **Blocked:** indicador de si se bloqueó automáticamente la actividad.
- **Manage:** abre el detalle del evento en el panel derecho.

El panel derecho **No transaction report selected** muestra el reporte completo del evento al seleccionarlo. Pulsa **Refresh table** en la cabecera para recargar.

ITDR · Threat analysis

Confirmed y Suspected.

Dos sub-pestañas

Threat analysis separa las amenazas según su grado de certeza:

- **Confirmed:** amenazas verificadas — el motor tiene alta confianza de que se trata de un incidente real.
- **Suspected:** amenazas potenciales — patrones que requieren revisión manual antes de actuar.

Cada listado se navega de la misma forma: filtrar, abrir el detalle, decidir si se escala a respuesta (bloqueo, aviso al usuario, escalado a SOC).

ITDR · Ruleset y Toolset

Configuración avanzada.

Submenús del Ruleset

Submenús de Ruleset y Toolset.

El Ruleset agrupa las reglas de detección en cinco categorías:

- **User rules:** reglas centradas en el comportamiento del usuario (login imposible, frecuencia, patrones de hora).
- **Location rules:** reglas geográficas (país de origen, salto entre ubicaciones, IPs sospechosas).
- **Device rules:** reglas sobre el dispositivo (jailbreak, root, modelo desconocido).
- **Network rules:** reglas sobre la red (Tor, VPN, ASN sospechosos).
- **Custom rules:** reglas a medida con expresiones lógicas (expr-lang) sobre el contexto del evento.

Toolset

El Toolset es el conjunto de acciones de respuesta disponibles cuando se detecta una amenaza (bloqueo, force-logout, notificación al usuario, integración SOAR, etc.).

En cuentas sin licencia ITDR, ambos submenús muestran una pantalla de "Contact sales to activate this feature".

Directory · Devices

Móvil, escritorio y RFID.

Mobile devices

Mobile
Manage and monitor your mobile devices.

Select a search filter

Name	Platform	Used by	Manage
Google Pixel 6	Android	JM Julen Martinez	Delete
Google Pixel 8	Android	XS Xabier Sestafe	Delete
Google Pixel 8 (10)	Android	XS Xabier Sestafe	Delete
Google Pixel 8 (11)	Android	XS Xabier Sestafe	Delete
Google Pixel 8 (2)	Android	XS Xabier Sestafe	Delete
Google Pixel 8 (3)	Android	XS Xabier Sestafe	Delete
Google Pixel 8 (4)	Android	XS Xabier Sestafe	Delete
Google Pixel 8 (5)	Android	XS Xabier Sestafe	Delete
Google Pixel 8 (6)	Android	XS Xabier Sestafe	Delete
Google Pixel 8 (7)	Android	XS Xabier Sestafe	Delete

Rows per page: 10 1-10 of 207 [gstack](#)

Listado de dispositivos móviles enrolados con Ironchip Authenticator.

Listado de dispositivos móviles enrolados en la plataforma. Cada fila incluye nombre del dispositivo, modelo, fabricante y usuario asociado.

Desktop devices

IRONCHIP

Desktop
Manage and monitor your desktop devices.

Select a search filter

Name	Platform	Used by	Manage
CompileEnv	Windows	MJ Mikel Jauregui	Delete
DESKTOP-O6IDI8K	Windows	JE Julen Esteras	Delete
DESKTOP-6LD74N4	Windows	JE Julen Esteras	Delete
DESKTOP-O6IDI8K (2)	Windows	JE Julen Esteras	Delete
DESKTOP-O6IDI8K (3)	Windows	JE Julen Esteras	Delete
DESKTOP-29U111F	Windows	JE Julen Esteras	Delete
DESKTOP-O6IDI8K (4)	Windows	JE Julen Esteras	Delete
DESKTOP-6LD74N4 (2)	Windows	JE Julen Esteras	Delete
DESKTOP-V4CUE2Q	Windows	MJ Mikel Jauregui	Delete
DESKTOP-B7416TU (8)	Windows	MJ Mikel Jauregui	Delete

Rows per page: 10 1-10 of 135 gstack

Equipos de escritorio enrolados (Windows / macOS / Linux).

Equipos de escritorio enrolados con plugin de Windows Logon, MacOSX Logon o Linux Logon.

RFID

IRONCHIP

RFID
Manage, export, synchronize key and group data through custom .csv keys

Select a search filter Export CSV Synchronize

Name	Platform	Used by	Manage
LFChip	RFID	IG Iker Garay	Delete
PruebaAne	RFID	AJ Ane Jauregui	Delete

Rows per page: 10 1-2 of 2 gstack

Tarjetas RFID/NFC asociadas.

Tarjetas RFID/NFC y dongles físicos asociados a los usuarios.

Operaciones comunes: desde estos listados puedes desenrolar un dispositivo (en caso de pérdida o baja del empleado), forzar una re-verificación o consultar el último uso.

Directory · Safe zones

Corporate y Personal.

Diferencia entre las dos

- **Corporate:** zonas definidas por la empresa (oficinas, data centers, sucursales). Centralmente gestionadas por administradores.
- **Personal:** zonas definidas por el propio usuario en su app móvil (su casa, casa de los padres, espacio coworking habitual). Útil para que los empleados puedan trabajar desde sitios "no corporativos" pero conocidos.

Corporate safe zones

Corporate safe zones
Draw and manage corporate safe zones on the map.

Search by corporate safe zone name Add corporate safe zone

Name	Verification level	Manage
ASDFGAS415465463F52D4G32ADFS4G2A	Strict	Options
Burgos	N/A	Options
España	Strict	Options
Oficina	N/A	Options
QA_Arkaitz	Strict	Options
QA_Test	Strict	Options
aFRQWETRQWRTGASDGASFHGREYH	Strict	Options
adsfadfasdfasd4654658654sdf	Strict	Options
baraka	N/A	Options
leke	N/A	Options

Rows per page: 10 | 1-10 of 13

ASDFGAS415465463F52D4G32ADFS4G2A

Safe zone information

Name: ASDFGAS415465463F52D4G32ADFS4G2A
Verification level: Strict

Locations

Circle 1

Overview

Geocercas corporativas con mapa.

Personal safe zones

IRONCHIP

Personal safe zones
Manage and customize your personal safe zones.

Select a search filter

Name	Created by	Platform	Access	Manage
Barakaldo	JE Julen Esteras	Android	Private	Options
Casa Nekane Bilbo	DU Deleted User	Android	Private	Options
Deusto Casa	IG Iker Garay	Desktop	Private	Options
Estudio Nekane	DU Deleted User	Android	Private	Options
Mikel casa	MJ Mikel Jauregui	Android	Private	Options
Office Presales	DU Deleted User	Android	Public	Options
Office Tech	TD TestPablo Dullaghan	Android	Private	Options
QATest	DU Deleted User	Android	Private	Options
QaTest	DU Deleted User	Android	Private	Options
Test Windows	MJ Mikel Jauregui	Desktop	Private	Options

Rows per page: 10 1-10 of 49

gstack

Geocercas personales del usuario.

Tras crear una safe zone (corporate o personal), agrúpalas en una **Safe zone policy** (vol. 3 cap. 3) para usarlas como factor de autenticación en accesos a aplicaciones.

Directory · Synchronization

CSV y SCIM.

Para qué sirve

Sincronización masiva de usuarios desde un sistema externo. Dos modos:

- **CSV:** import puntual desde fichero. Útil para migraciones one-shot.
- **SCIM:** sincronización continua estándar (System for Cross-domain Identity Management). Tu IdP (Okta, Azure AD, OneLogin...) propaga cambios al directorio de Ironchip.

CSV

Synchronization with CSV
Synchronize user and group data through custom .csv imports.

Find report Synchronize

Updated group	File name	Date	Status	Users	Manage
3424	synchronization_template (22)_...	March 17, 2026 at 12:00:40	✓	1/1	Options
3424	synchronization_template_Mar17...	March 17, 2026 at 11:29:46	✓	1/1	Options
AccessSubgroup	file_example_XLS_10_Mar1720261...	March 17, 2026 at 11:04:38	!	0/50	Options
AccessSubgroup	synchronization_template(56)_M...	March 17, 2026 at 11:04:22	✓	1/1	Options
AccessTest2	synchronization_template(55)_M...	March 13, 2026 at 12:37:43	✓	0/0	Options
3666	3424_Mar112026132109.txt	March 11, 2026 at 13:21:49	✓	0/0	Options

October gstack

Synchronization details

Synchronization information

Date: March 17, 2026 at 12:00:40
Group: 3424
File name: synchronization_template (...)

Synchronization result

Every user in the template (1/1) was successfully synchronized with the group 3424.

Subida de fichero CSV con usuarios.

Sube un CSV con los usuarios a importar. La pantalla muestra el formato esperado de columnas y las opciones de mapeo.

SCIM

IRONCHIP

Synchronization with SCIM
Synchronize user and group management with SCIM 2.0.

SCIM 2.0 Integration Setup

A SCIM API integration allows you to automatically provision, update and deprovision users and sync groups in real-time. This type of integration is based on the System for Cross-Domain Identity Management (SCIM) standard.

GET STARTED CREDENTIALS

Base URL:

https://api.ironchip.com/scim/v2

Integration Steps:

- **Set Up SCIM in Your Identity Provider.**
- Navigate to the "Provisioning" or "SCIM" section in your identity provider's dashboard.
- Input the **SCIM URL** and **Authentication Token** provided above.
- Save the configuration.

Supported Actions:

- **User Provisioning:** Automatically create, update, and delete users in the platform based on changes in your directory.
- **Group Management:** Assign and update groups based on your directory configuration.

Authentication Methods:

- Use Bearer Authentication with the token provided to securely connect your identity provider to the SCIM API.

gstack

Endpoint SCIM y token bearer para configurar tu IdP.

Aquí se obtienen el endpoint SCIM y el token bearer que tu IdP necesita para empujar usuarios y grupos hacia Ironchip.

Plugins

Catálogo de integraciones descargables.

Catálogo

The screenshot displays the Ironchip Plugins catalog. The sidebar on the left contains navigation links: Get started, Applications, Directory, Authentication policies, Security, Monitoring, ITDR, **Plugins**, and Account settings. The main content area is titled 'Plugins' and includes the subtitle 'Explore our diverse range of plugins, designed to effortlessly integrate our technology with your existing systems'. There are two main sections: 'Logon' and 'Authenticators'. Each section contains three cards for different operating systems: Microsoft (Windows), Linux, and macOS. Each card includes a description of the plugin and a 'Download' button.

Catálogo de plugins de Logon y Authenticators.

Catálogo de software descargable que extiende Ironchip a sistemas concretos:

Logon

- **Windows Logon** — MFA en login Windows.
- **Linux Logon** — MFA en PAM de Linux.
- **MacOS Logon** — MFA en login macOS.

Authenticators

Ciente Ironchip Authenticator para Windows, Linux y macOS — la app que recibe los push de autenticación.

Cada tarjeta tiene una descripción del plugin y un botón **Download** (algunos ofrecen ARM y x86 por separado). Tras descargar, sigue las instrucciones de instalación específicas de cada plataforma.

Account settings · Billing

Información de facturación y plan contratado.

Plan details

Datos del plan, facturación y consumo de recursos.

Current plan

- Plan actual contratado (p. ej. **Premium**) y fecha de expiración.
- Botón **Change plan** para cambiar de tier.

Billing details

- **Billing interval:** Yearly / Monthly.
- **Billing email:** correo al que se envían facturas.
- **Billing address.**
- **VAT/GST number.**
- **Update billing details:** editar la información anterior.

Next payment

Fecha y monto del próximo cargo, si lo hay.

Resource usage

- **Active users:** usuarios activos vs. máximo del plan.
- **Public zones:** zonas públicas usadas vs. límite.

Invoices

Panel lateral con facturas anteriores. Si no hay (caso de planes sin recibos emitidos), muestra el aviso "No invoices available at the moment".

Account settings · Look & feel

White-label del dashboard y de la app móvil.

Personalización visual

Configuración de logos y colores con preview en directo.

Permite personalizar la apariencia del dashboard y de la app móvil con la marca de la empresa. Hay dos pestañas:

- **WEB:** personalización del dashboard.
- **MOBILE:** personalización de la app Ironchip Authenticator.

Bloque Configuration

Assets:

- **Header logo:** logo de cabecera. Puede subirse por URL o por fichero.
- **Main logo:** logo principal. Idéntico mecanismo (URL o fichero).

Colors:

- **Primary color:** color de acento (botones primarios, enlaces).
- **Secondary color:** color secundario (cabeceras).
- **Background color:** color de fondo.

Pulsa **Save** para aplicar o **Reset** para volver a los valores por defecto.

Bloque Preview

Vista previa en directo de cómo quedará el login para los usuarios finales. Útil para validar contraste y legibilidad antes de aplicar.

Fin del manual: con esto quedan cubiertas todas las secciones del dashboard. Las secciones marcadas como "premium" (ITDR Ruleset/Toolset, SIEM integration) requieren contrato adicional con el equipo comercial de Ironchip.

