ITDR, Directorio y Cuenta

Manual del Dashboard Ironchip · Volumen 4

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

Contenido

CAPÍTULO 1

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".

CAPÍTULO 2

ITDR · Realtime feed

Stream de eventos en tiempo real.

La pestaña

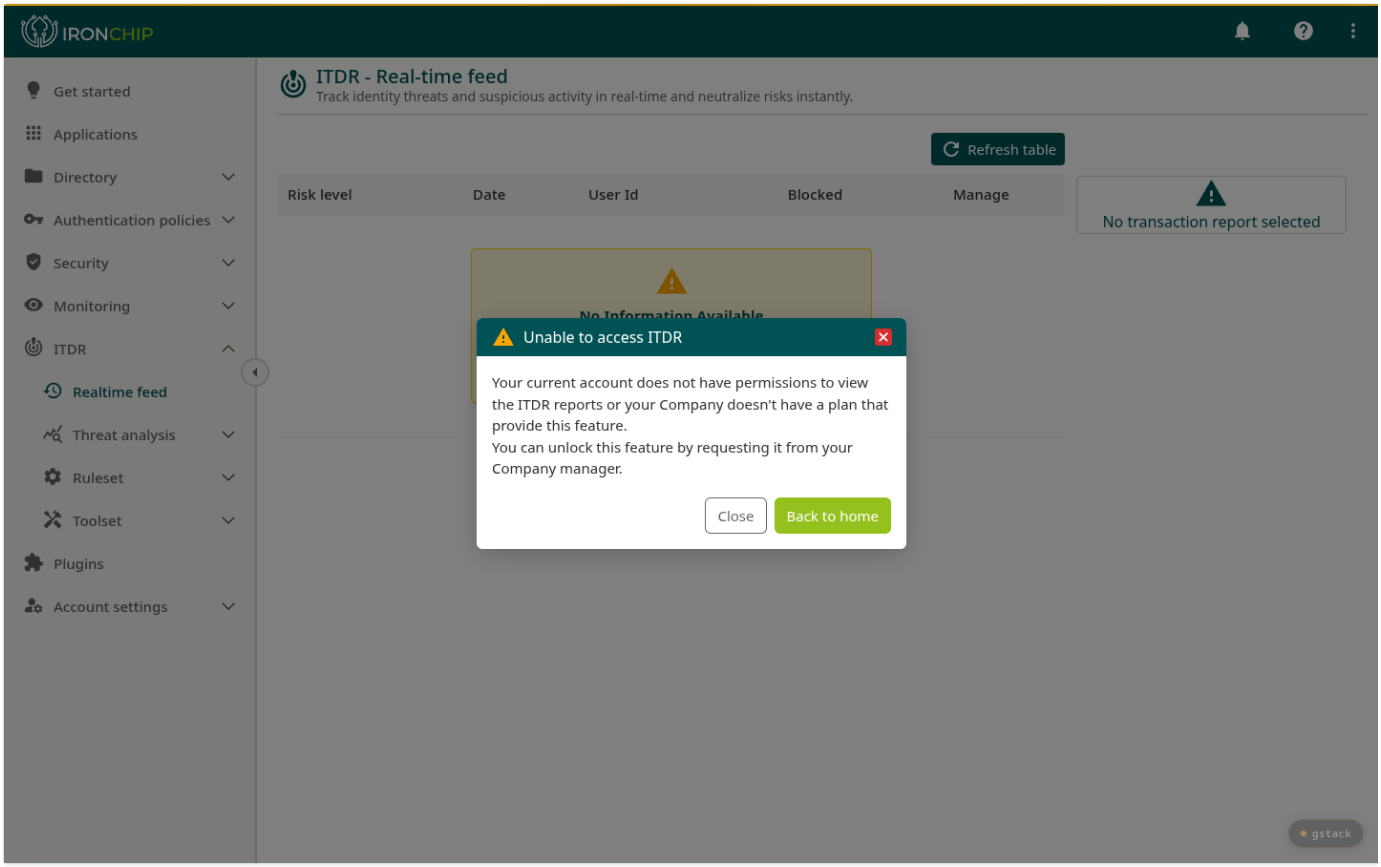


Tabla con Risk level, Date, User Id, Blocked y Manage; panel de detalle a la derecha.

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.

CAPÍTULO 3

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.

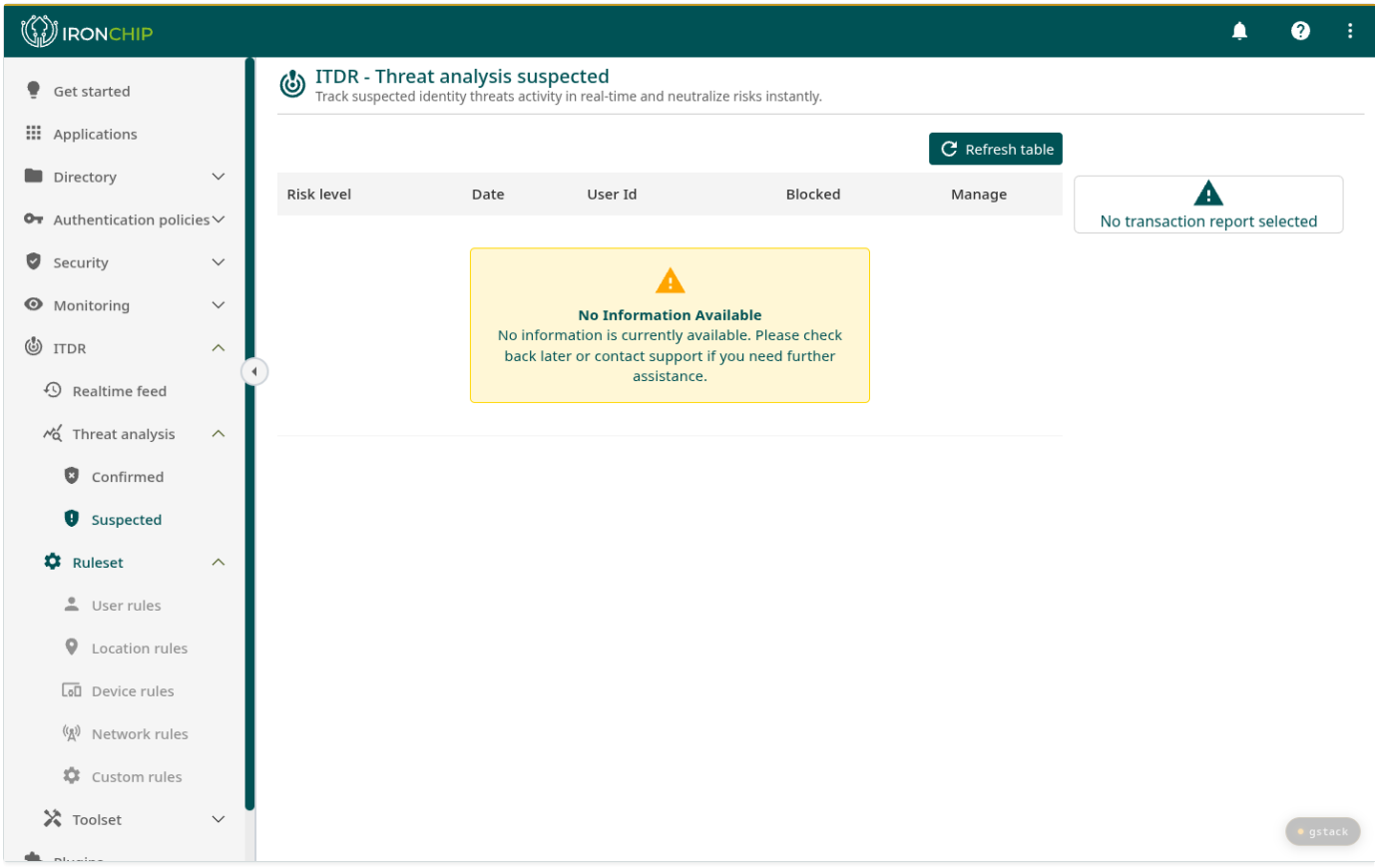
Cada listado se navega de la misma forma: filtrar, abrir el detalle, decidir si se escala a respuesta (bloqueo, aviso al usuario, escalado a SOC).

CAPÍTULO 4

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.).

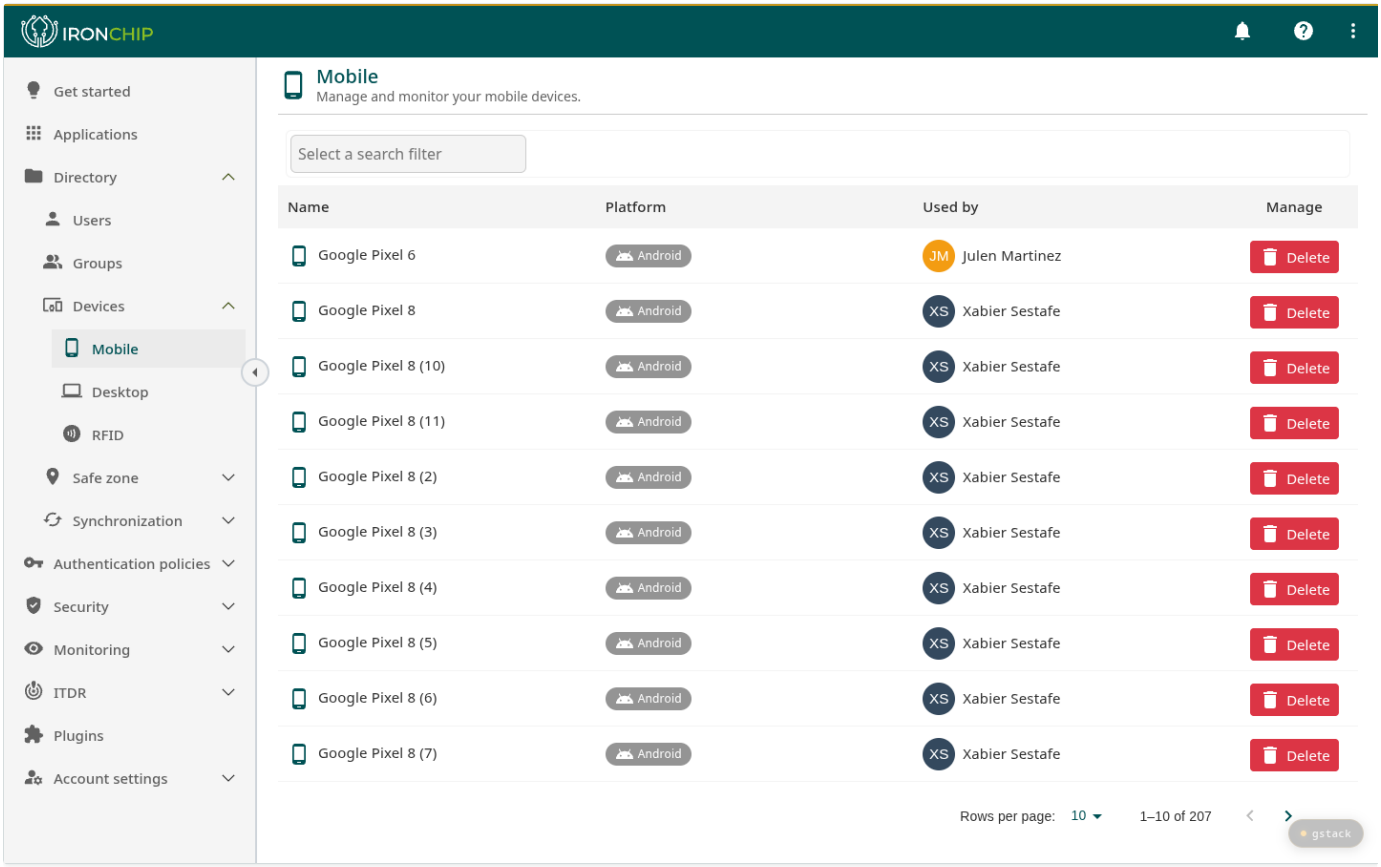
En cuentas sin licencia ITDR, ambos submenús muestran una pantalla de "Contact sales to activate this feature".

CAPÍTULO 5

Directory · Devices

Móvil, escritorio y RFID.

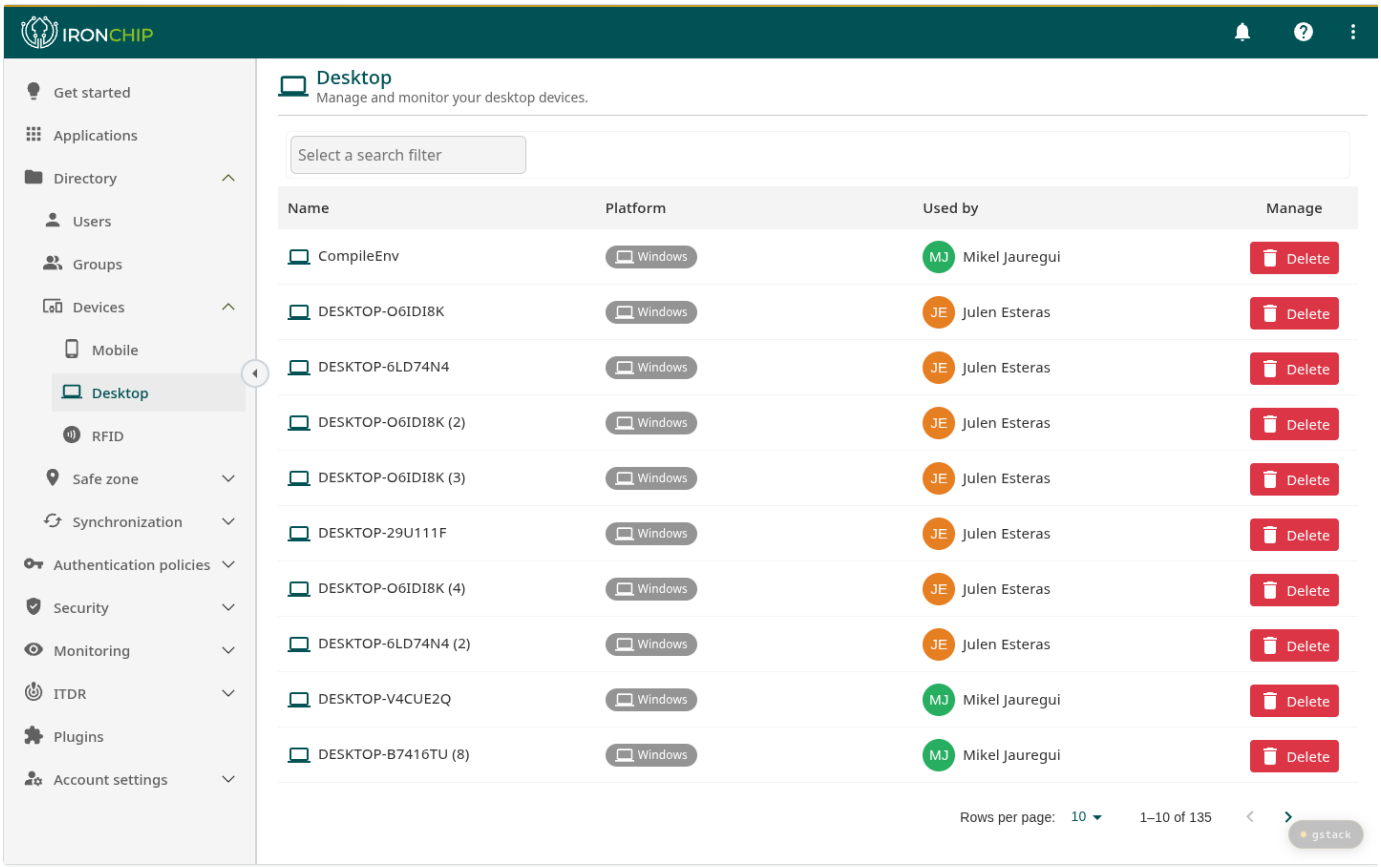
Mobile devices



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.

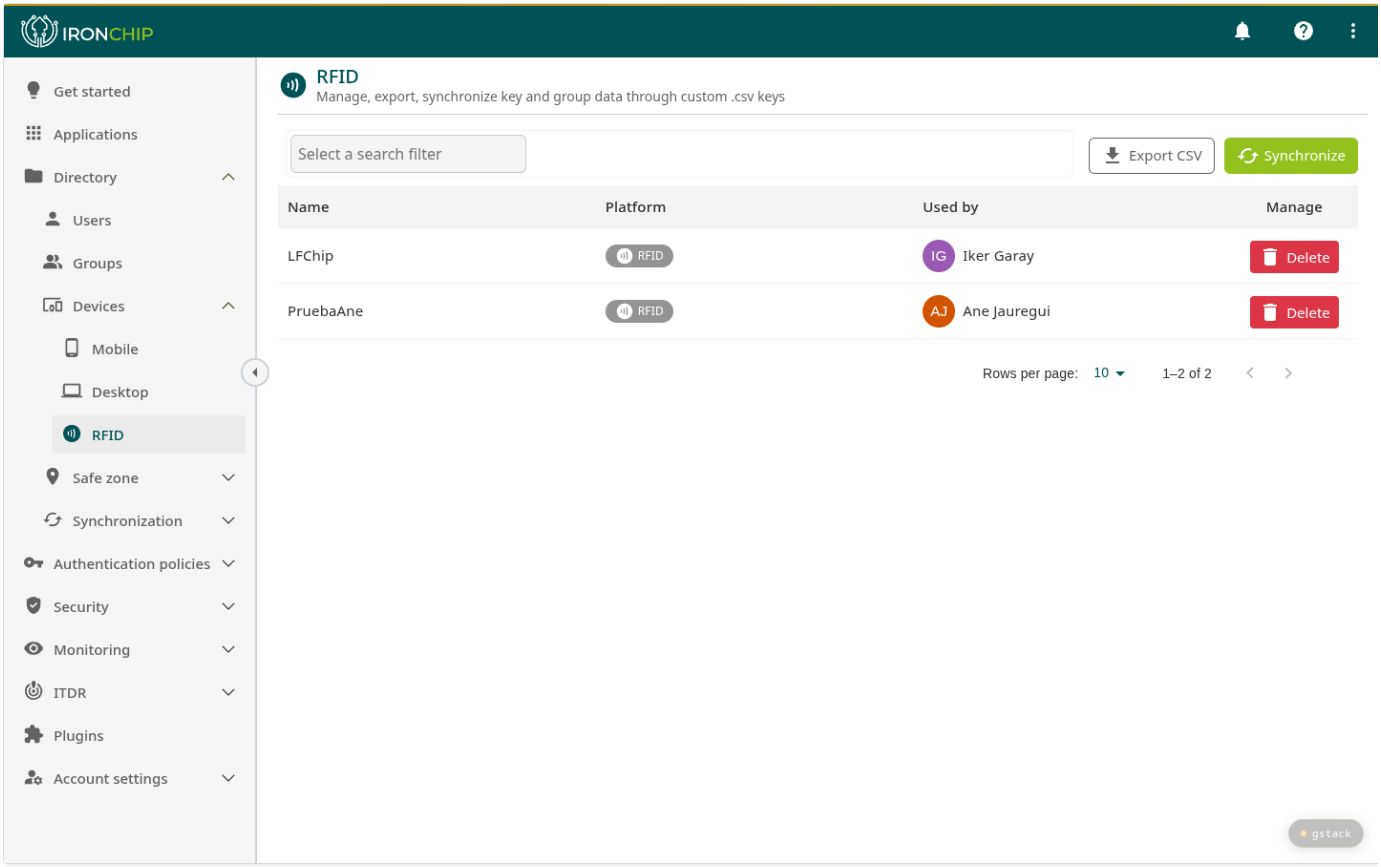
Desktop devices



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

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

RFID



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.

CAPÍTULO 6

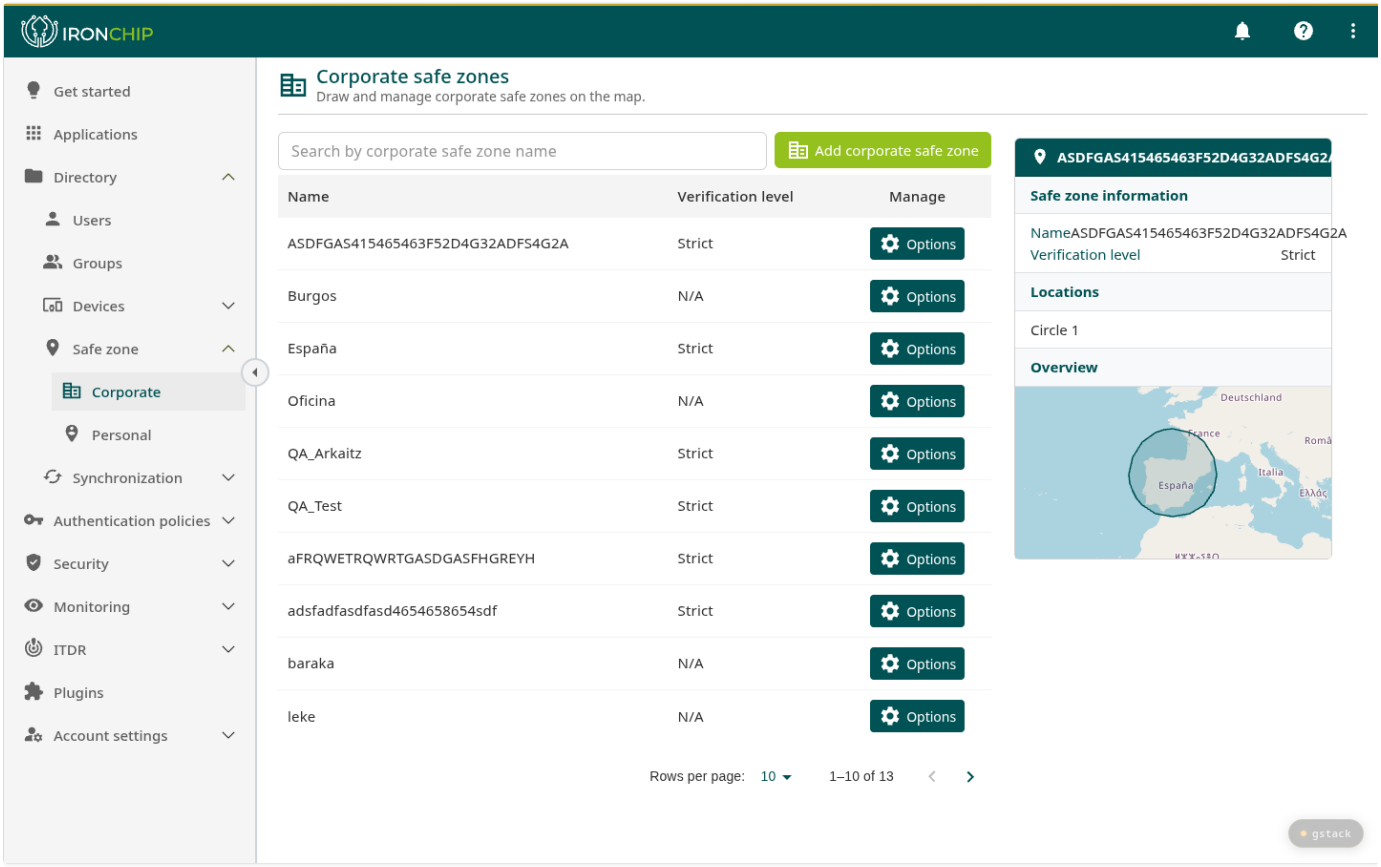
Directory · Safe zones

Corporate y Personal.

Diferencia entre las dos

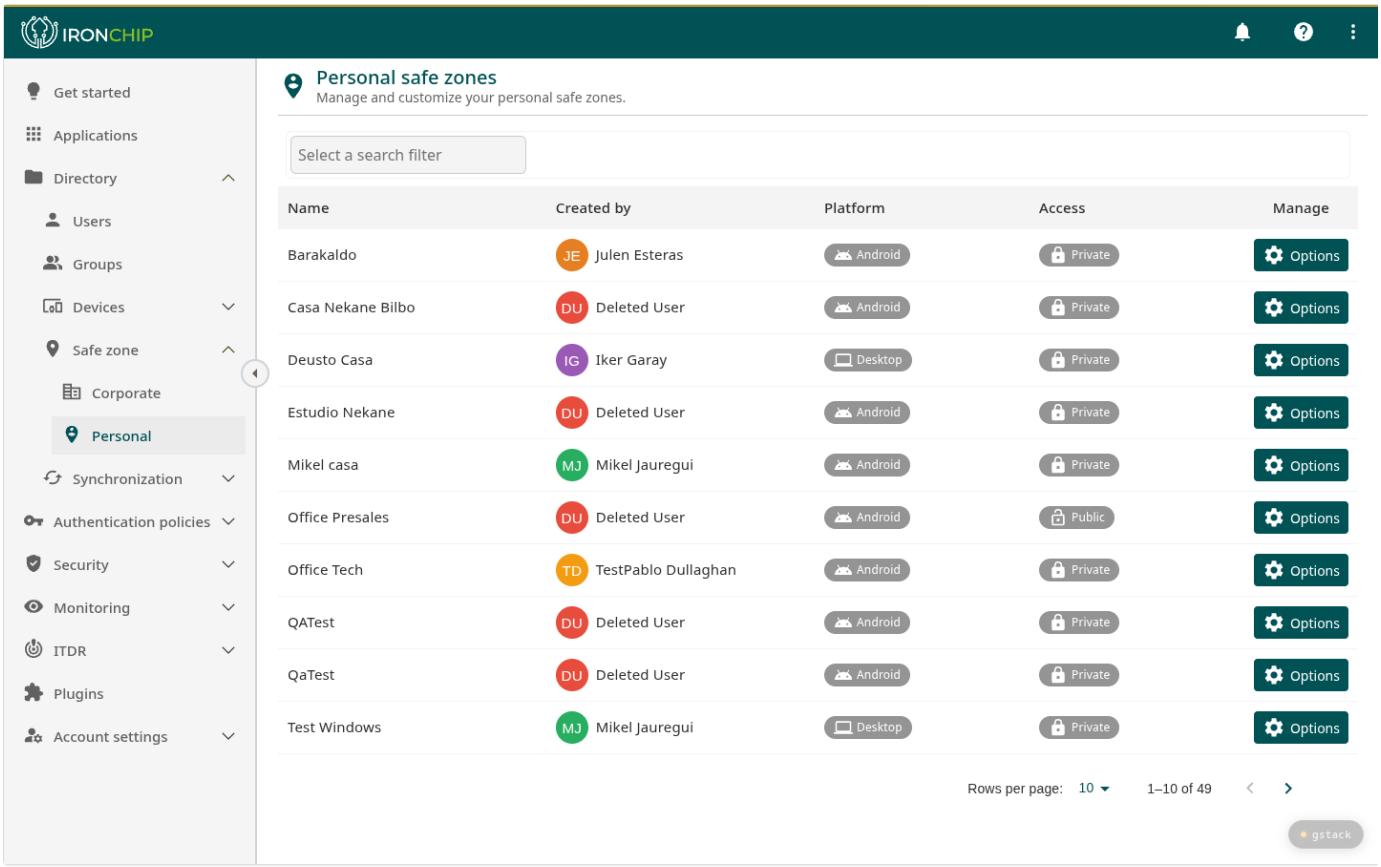
- **Corporate:** zonas definidas por la empresa (oficinas, data centers, sucursales). Centralmente gestionadas por administradores.
- **Personal:** zonas definidas por el propio usuario en su app móvil (su casa, casa de los padres, espacio coworking habitual). Útil para que los empleados puedan trabajar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

Corporate safe zones



Geocercas corporativas con mapa.

Personal safe zones



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.

CAPÍTULO 7

Directory · Synchronization

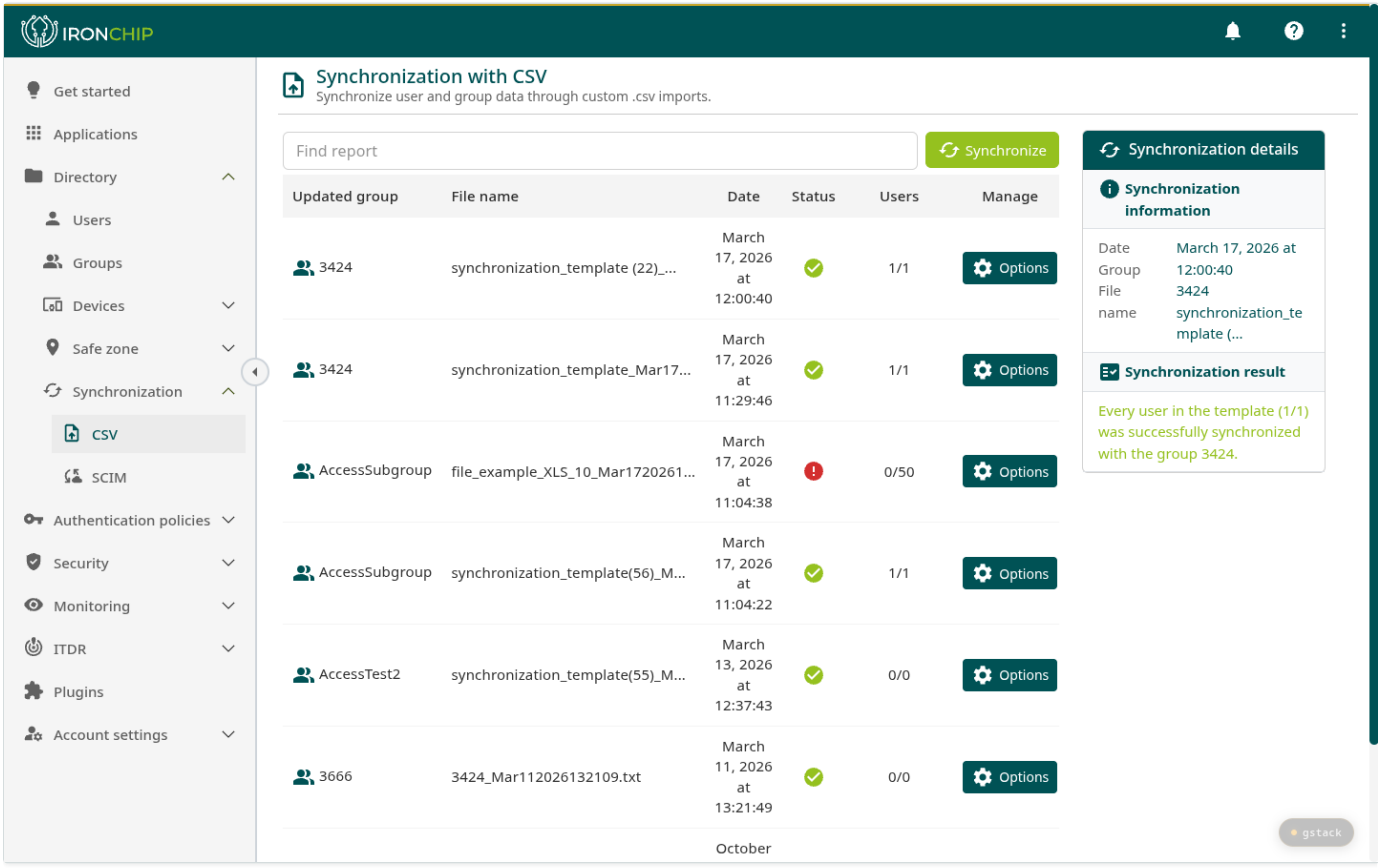
CSV y SCIM.

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.

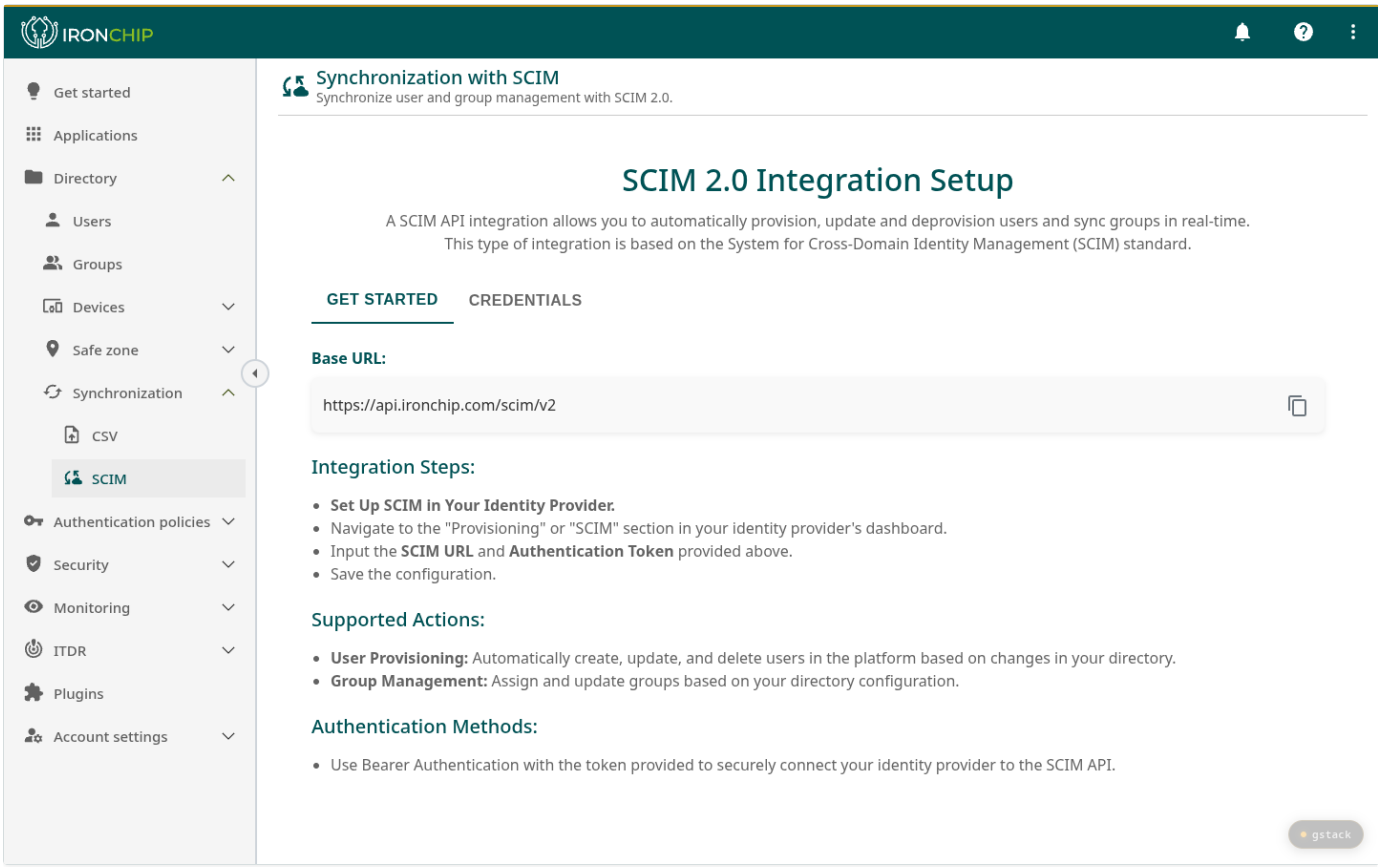
CSV



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



Endpoint SCIM y token bearer para configurar tu IdP.

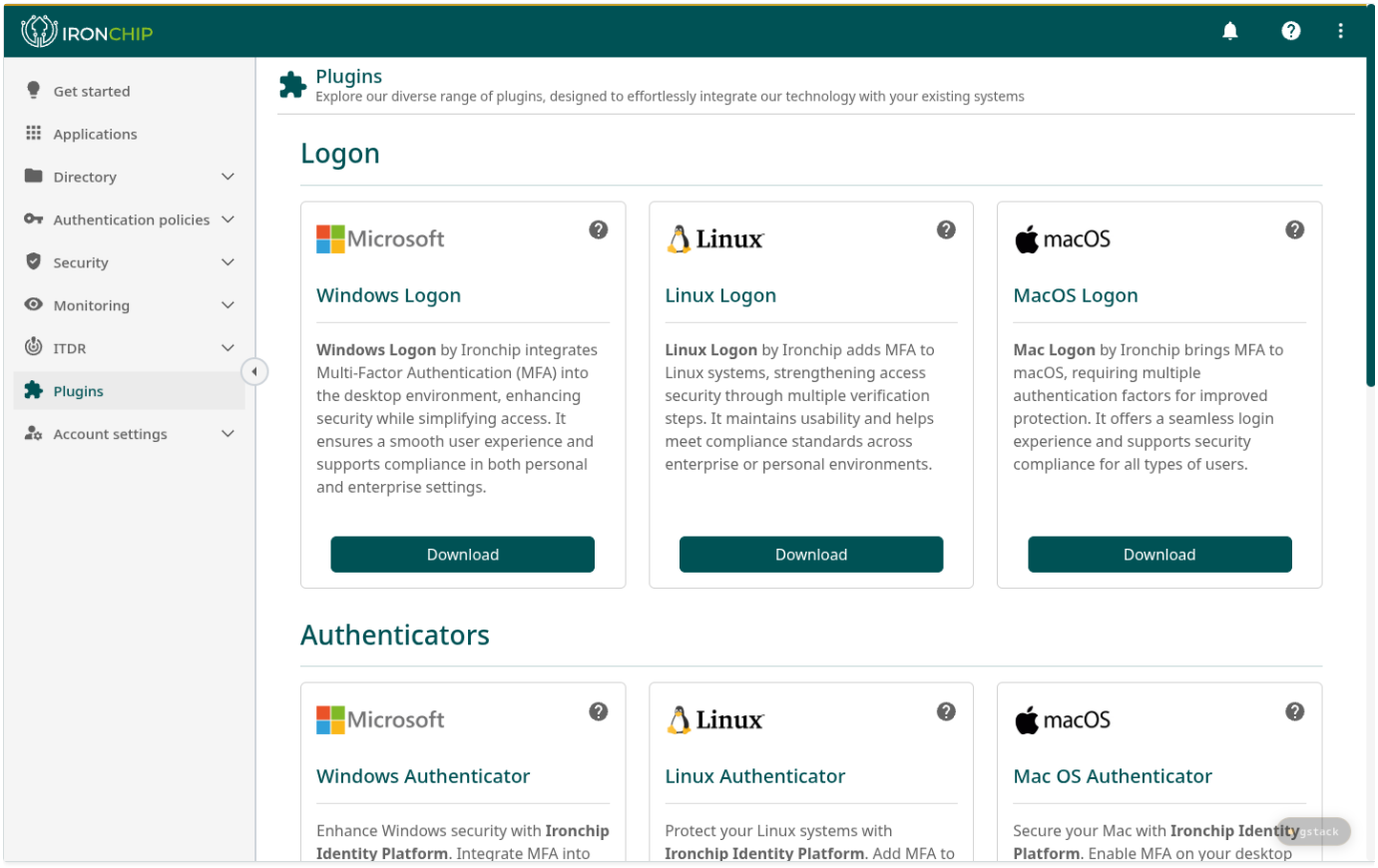
Aquí se obtienen el endpoint SCIM y el token bearer que tu IdP necesita para empujar usuarios y grupos hacia Ironchip.

CAPÍTULO 8

Plugins

Catálogo de integraciones descargables.

Catálogo



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

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

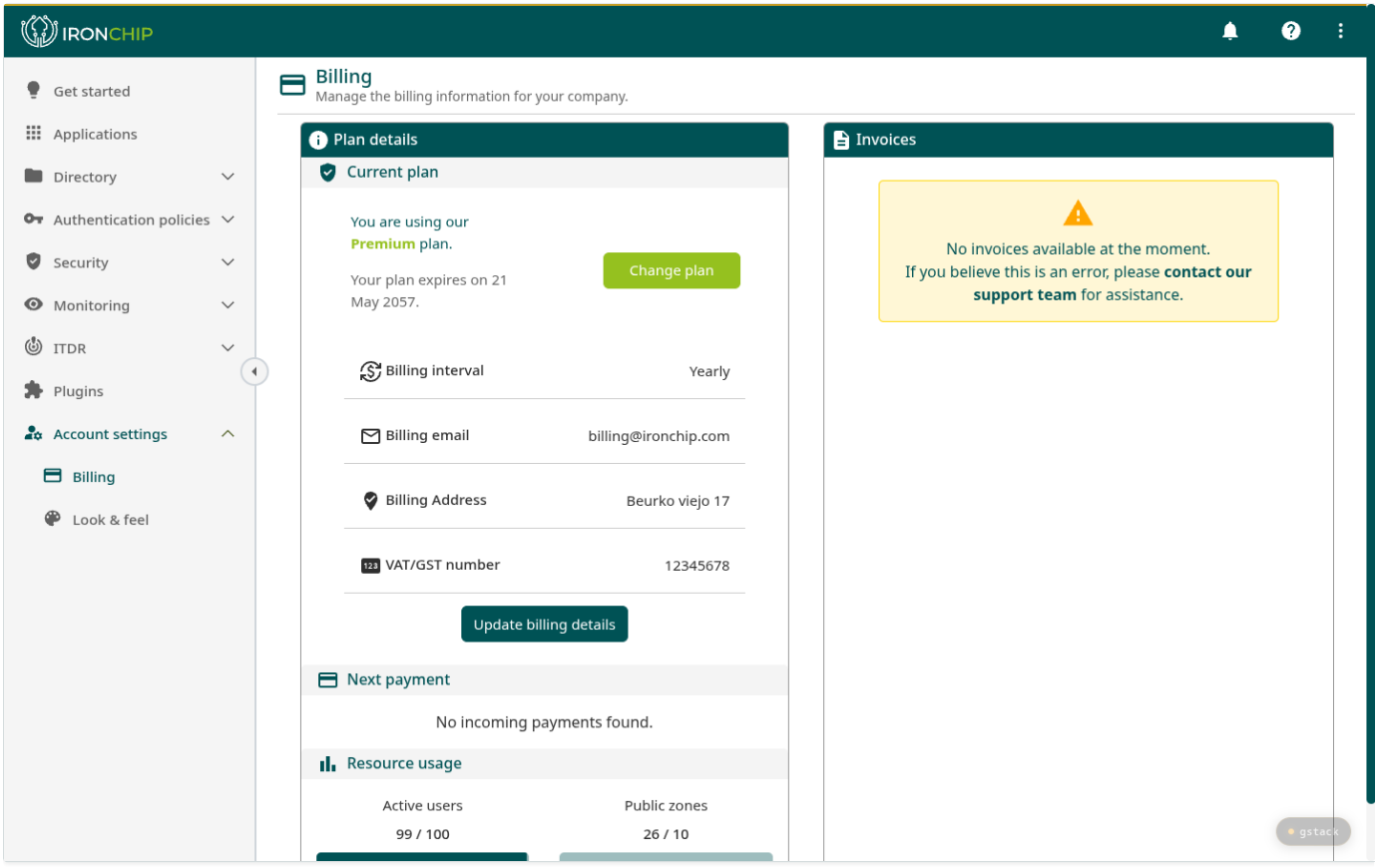
Cada tarjeta tiene una descripción del plugin y un botón **Download** (algunos ofrecen ARM y x86 por separado). Tras descargar, sigue las instrucciones de instalación específicas de cada plataforma.

CAPÍTULO 9

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

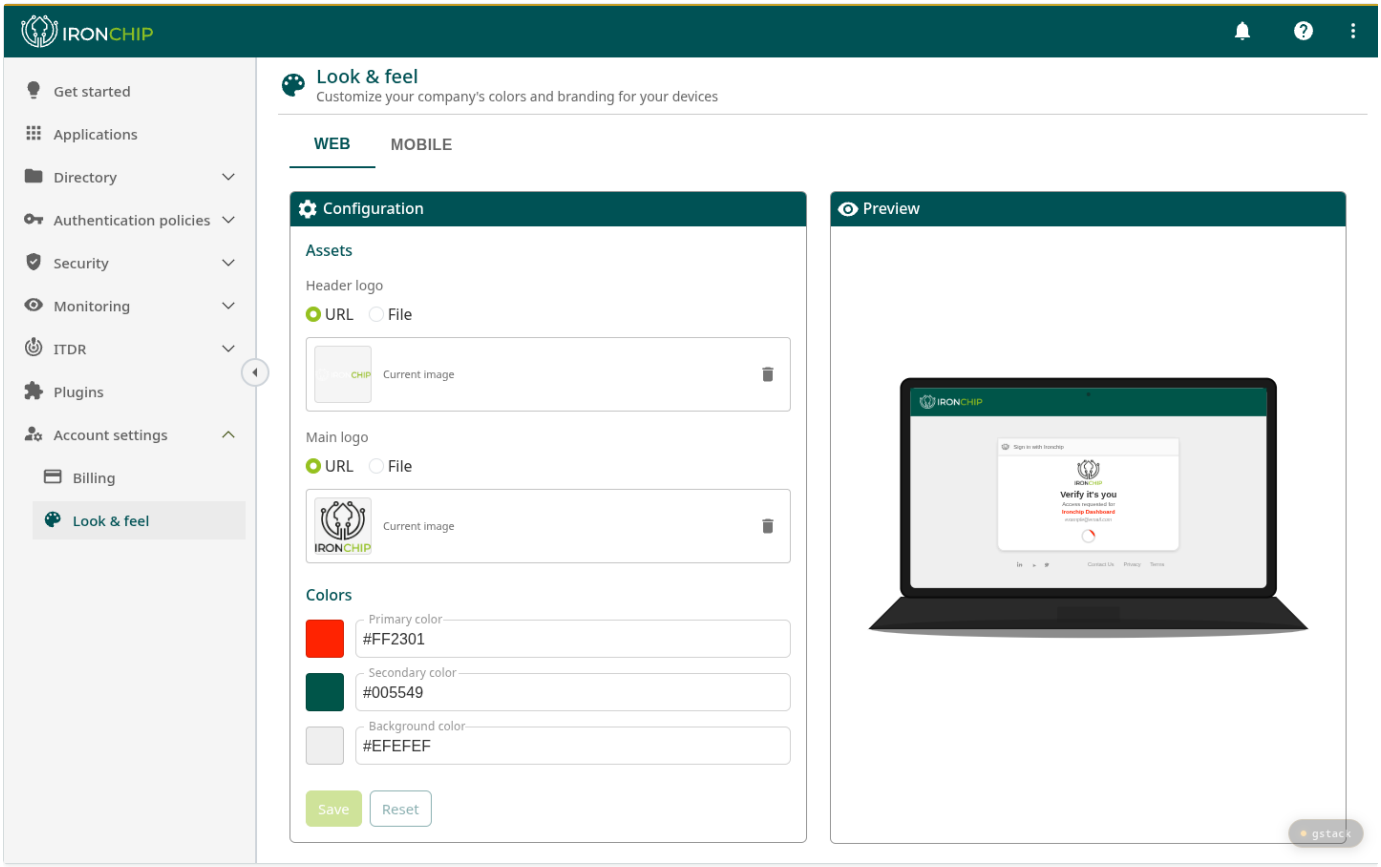
Panel lateral con facturas anteriores. Si no hay (caso de planes sin recibos emitidos), muestra el aviso "No invoices available at the moment".

CAPÍTULO 10

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.