BioStar Air

GUÍA DEL ADMINISTRADOR DE

Versión 2.13.0

Español

ES 102.00.BSA

suprema

SECURITY & BIOMETRICS

CONTENIDO

¿Qué es BioStar Air? 4

Plataforma de control de acceso 100% en la nube 4

Flexibilidad de credenciales sin igual 4

No se requiere infraestructura local 4

Gestión multisede sencilla 4

Escalabilidad preparada para el futuro con arquitectura edge 5

Optimizado para empresas centradas en la nube 5

Funciones de BioStar Air 5

Dispositivos Compatibles 6

Marco de seguridad 7

Administrador del sitio 10

Primeros Pasos 10

Selector de sitios 21

Primeros pasos con la aplicación BioStar Air 23

Administrar sitios 25

Configurar ajustes del sitio 215

Configurar SSO Y SCIM 236

Configuración adicional del sitio 267

Socios e Instaladores 295

Usa el Portal de Socios 295

Administrar sitios federados 297

Invitar administradores de socios. 299

Invitar a un administrador del sitio. 304

Administrar técnicos de socios 309

Instalar el hardware 323

Credencial de usuario 344

Uso de credenciales móviles 344

Configurar funciones avanzadas 346

Ajustar la sensibilidad Bluetooth 351

Desarrollador 353

Inicio rápido 353

Autenticación de la API 355

Uso de la API de gestión de usuarios 358

Solución de Problemas 363

Solución de problemas al agregar usuarios en masa 363

Solucionar problemas con la tarjeta móvil 366

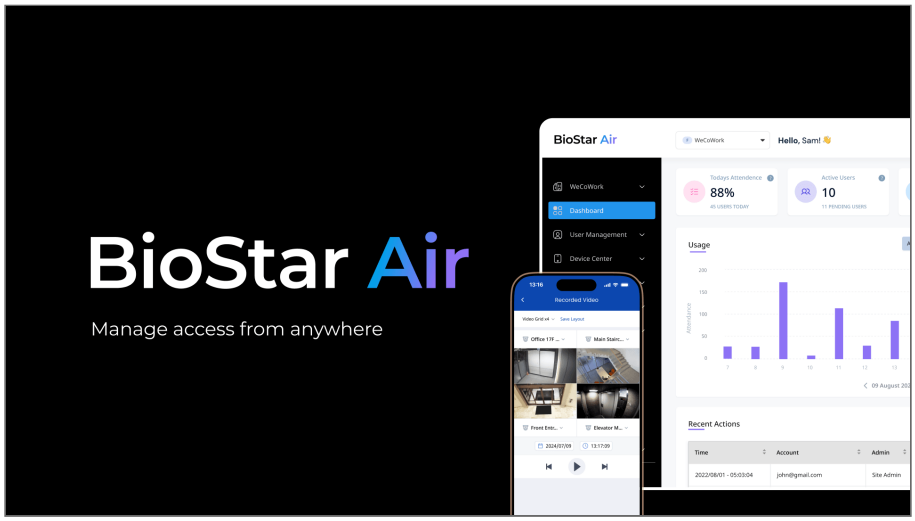
¿Por qué se me solicita activar los servicios de ubicación? 368

Solución de problemas de reproducción de video 369

¿Qué es BioStar Air?

Plataforma de control de acceso 100% en la nube

BioStar Air es una solución nativa en la nube desarrollada por Suprema, líder mundial en seguridad biométrica. Diseñada para eliminar la necesidad de infraestructura local, BioStar Air ofrece un control de acceso seguro, flexible y escalable que se puede gestionar desde cualquier lugar. Con **lectores inteligentes** que se conectan directamente a la nube, las organizaciones pueden controlar fácilmente el acceso en múltiples sitios usando únicamente un teléfono o un navegador.



Flexibilidad de credenciales sin igual

BioStar Air ofrece la gama más amplia de opciones de autenticación, lo que permite a las organizaciones gestionar el acceso a sus instalaciones de forma segura y práctica.

- **Autenticación facial**
- **Credenciales móviles personalizadas para iOS y Android** (gratuitas)
- **Múltiples formatos RFID**
- **QR dinámico y LinkPass sin aplicación**

No se requiere infraestructura local

BioStar Air elimina la necesidad de servidores en las instalaciones, máquinas virtuales, VPN o controladores de puertas. No se requiere mantenimiento de TI. Instale un **lector inteligente** y conéctelo a la nube para comenzar a gestionar el acceso de inmediato. Los lectores funcionan en múltiples sitios sin importar la red o la ubicación física.

Gestión multisede sencilla

Ya sea para administrar el acceso en **oficinas**, **almacenes**, **tiendas** o **sitios remotos**, BioStar Air ofrece una solución completa para controlar el acceso a todas las ubicaciones desde un único sistema.

Escalabilidad preparada para el futuro con arquitectura edge

La **arquitectura edge** de BioStar Air integra el control de acceso directamente en el lector inteligente, eliminando la necesidad de controladores de puertas independientes. Esto permite a las organizaciones **escalar con facilidad**: comprar solo lo que necesitan hoy y expandirse fácilmente sin actualizaciones complejas.

Optimizado para empresas centradas en la nube

BioStar Air está diseñado para **integradores de sistemas** y **clientes** que buscan una solución de control de acceso totalmente nativa en la nube con biometría líder en la industria. Ofrece un enfoque moderno, flexible y altamente seguro para la gestión de accesos en empresas centradas en la nube.

Funciones de BioStar Air

Función	Descripción
Solución completa de control de acceso	Soportado
Alta seguridad	ISO 27001 / 27701, TLS 1.2, AES-256
Biometría: reconocimiento facial y huella dactilar	Ofrece soporte nativo para los lectores de Suprema e incluye una base de datos biométrica integrada.
Tarjetas RFID	MIFARE Classic, DESFire, FeliCa, EM4100, formatos Wiegand personalizados, iCLASS, Seos. Admite hasta ocho tarjetas por usuario.
Credenciales móviles	Gratuitas e ilimitadas. Incluyen credenciales seguras BLE/NFC (iOS, Android), LinkPass sin aplicación y autenticación mediante QR.
Despliegue	Nativo en la nube
Interfaz	Navegador, aplicación iOS, aplicación Android
Modelo de precios	Por suscripción
Integración	APIs, webhooks y SDKs extensos
Arquitectura Edge	Los lectores incluyen un controlador integrado y se conectan directamente a la nube vía Ethernet. No se requieren nodos en la nube adicionales ni paneles de control de acceso.
inicio de sesión	Accesible desde cualquier lugar.
Ubicación del servidor	Corea (global) y Alemania (Europa)

Función	Descripción
Control de tiempo y asistencia	Los botones de control de tiempo y asistencia del lector se registran como eventos y pueden integrarse en los informes de horas trabajadas.
Video	VMS integrado con soporte para ONVIF y Uniview. No se requiere NVR; el lector actúa como puerta de enlace.
Alarmas	Permite notificar a los administradores sobre intrusiones en zonas de alarma.
Partición de datos	Estándar
Objetivo	Franquicias, multisitio, multi-tenant, ubicaciones remotas y más

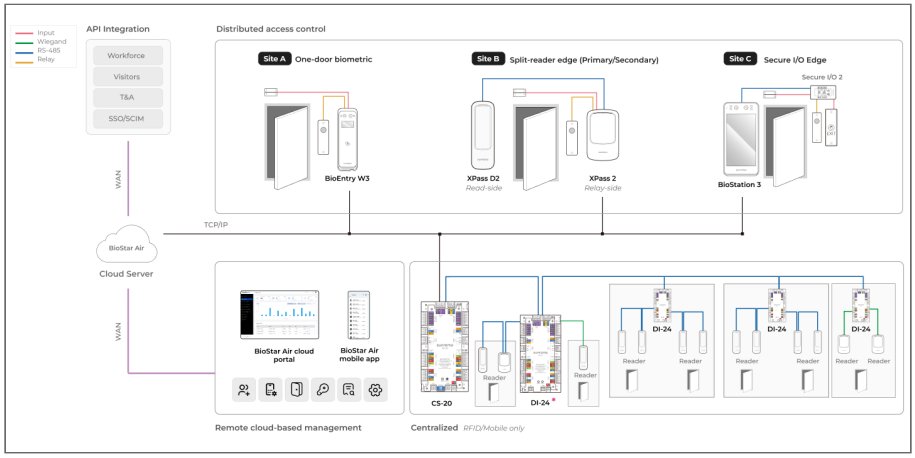
Dispositivos Compatibles

BioStar Air admite una gestión flexible de dispositivos tanto en arquitecturas de control de acceso distribuidas como centralizadas. Permite registrar, configurar, supervisar, actualizar y operar dispositivos desde la nube, de modo que cada sitio pueda usar la configuración más adecuada para sus puertas, su cableado y sus requisitos de seguridad.

Los sitios pueden usar dispositivos edge que se conectan directamente a la nube, o paneles de control que gestionan lectores aguas abajo mediante RS-485 o Wiegand. Ambas arquitecturas pueden coexistir en el mismo sitio y admiten nuevas instalaciones, implementaciones biométricas, modernizaciones y configuraciones centralizadas basadas en paneles.

Dispositivos compatibles

BioStar Air es compatible con una amplia variedad de dispositivos de control de acceso y se integra a la perfección con los dispositivos de Suprema para ofrecer control de acceso en la nube.



Lectores

- **XPass 2** (MDPB, GDPB, GKDPB)
- **X-Station 2** (DPB)
- **BioEntry W3**
- **BioStation 3**

- **XPass D2**

Paneles

- **CoreStation 20** (CS-20)

Dispositivos Patch

- **Airfob Patch** (AP-H)
- **Airfob Tag** (AP-B)

Otros dispositivos compatibles

- **Output Module** (OM-120)
- **Secure I/O 2** (SIO2)
- **Interfaz de puerta** (DI-24, próximamente)

Marco de seguridad

BioStar Air es la solución segura y basada en la nube de Suprema para control de acceso móvil. Los equipos de ingeniería de hardware, software y firmware de Suprema trabajan según el principio de «seguridad por diseño». Cada capa de la arquitectura del sistema y cada punto de contacto en la comunicación están diseñados para preservar la privacidad y la integridad de los datos.

Medidas clave:

- Protección de datos y cifrado del portal de gestión y de la base de datos de BioStar Air
- Cifrado y protección de los datos en tránsito entre la API de BioStar Air y los clientes
- Cifrado de los datos de la tarjeta móvil almacenados en el smartphone
- Protección de la comunicación entre el smartphone y el lector (Suprema Pass)
- Prevención de la falsificación de credenciales móviles (Suprema Pass)

Certificación ISO 27001

Suprema obtuvo la certificación ISO 27001, cumpliendo con estándares internacionales para la gestión de la protección de datos, los controles de seguridad y la privacidad. La conformidad con ISO 27001, obtenida en agosto de 2019, también se alinea con regulaciones similares como el Reglamento General de Protección de Datos (GDPR) y la Ley de Privacidad del Consumidor de California (CCPA).

Tecnología probada para la seguridad de extremo a extremo

Acceso seguro al portal y protección de datos

El portal de gestión de BioStar Air se ejecuta en una instancia cifrada de base de datos Amazon RDS de AWS que utiliza cifrado AES-256 o superior. Además, todos los datos personales están cifrados.

Comunicación cifrada con la API de BioStar Air

Todas las comunicaciones con la API REST de BioStar Air están cifradas con TLS 1.2 a través de HTTPS y requieren un token de acceso (con expiración predeterminada de 1 hora). AWS API Gateway limita las solicitudes a la API para prevenir ataques de fuerza bruta.

Identificadores de tarjetas móviles cifrados y con hash

Los identificadores de tarjetas móviles están cifrados con AES-256 para evitar su exposición en servidores de terceros. Los datos de las tarjetas están firmados digitalmente para verificar su autenticidad.

Almacenamiento seguro de tarjetas móviles en el dispositivo

Las credenciales móviles Suprema Pass y los datos relacionados están cifrados con AES-256. Las claves de cifrado se almacenan en el entorno de ejecución confiable (TEE) del dispositivo, como Secure Enclave (Apple) o TrustZone (ARM).

Comunicación segura entre el dispositivo móvil y el lector

Para bloquear ataques de repetición sobre Bluetooth Low Energy (BLE), BioStar Air utiliza una clave de cifrado de un solo uso para cada conexión y termina la conexión inmediatamente después de la transmisión, previniendo ataques man-in-the-middle (MITM).

Prevención de la falsificación de credenciales móviles

Cada credencial móvil Suprema Pass está protegida por una firma digital basada en PKI, única para cada sitio de BioStar Air. Un proceso de verificación propietario detecta cualquier intento de modificación o falsificación.

Gestión de vulnerabilidades

El equipo de seguridad de la información de Suprema lidera la gestión de vulnerabilidades con el apoyo de expertos externos en seguridad.

- Escaneos automatizados y continuos en busca de amenazas
- Auditoría anual de recertificación ISO 27001 con revisión integral del sistema
- Pruebas de penetración y evaluación de riesgos antes de lanzamientos importantes
- Comprobaciones de la higiene de contraseñas, la resistencia frente a la ingeniería social y el cumplimiento de procedimientos
- Documentación e informes exhaustivos de todas las vulnerabilidades y de las acciones de remediación

Enfoque de evaluación de riesgos

Los activos se clasifican según su confidencialidad, integridad y disponibilidad. Se identifican las amenazas, se evalúan las vulnerabilidades y se valoran los riesgos en función de su probabilidad e impacto. Las acciones de mitigación se priorizan según la gravedad del riesgo.

Autenticación multifactor (MFA)

La autenticación multifactor (MFA) se está implementando por fases.

- Autenticación de dos factores por correo electrónico para cuentas de administrador

- Autenticación de dos factores basada en código para la aplicación BioStar Air
- Bloqueo automático de cuentas de administrador inactivas tras 90 días
- Expiración configurable de contraseñas (30, 60 o 90 días)

Políticas clave de seguridad

- Cifrado de datos en tránsito: TLS 1.2
- Cifrado de datos en reposo: AES-256
- Protección contra DoS: limitación de solicitudes mediante AWS API Gateway
- Disponibilidad del servicio: 99.9% de tiempo de actividad (según el SLA)
- Seguridad de la API: autenticación basada en tokens, solo HTTPS y validación estricta de endpoints
- Acceso al portal: basado en la nube para la gestión global; se está desarrollando una opción de nube privada

Administrador del sitio

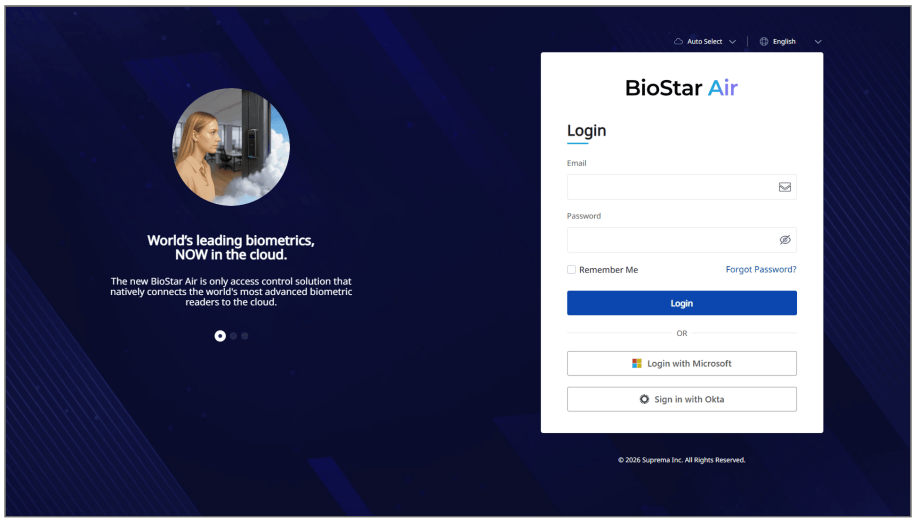
El administrador del sitio es responsable del funcionamiento general de un sitio de BioStar Air. Guía a los administradores en todas las tareas de gestión necesarias, incluyendo la inscripción de usuarios y la gestión de credenciales; la configuración de dispositivos, puertas y ascensores; la definición de permisos de acceso y horarios; la supervisión de eventos; y la configuración de los ajustes y servicios del sistema.

Primeros Pasos

El Portal de BioStar Air ofrece una interfaz unificada en la web y en las aplicaciones móviles, proporcionando una experiencia de usuario coherente. Desde el Portal de BioStar Air, los administradores pueden gestionar el control de acceso, supervisar el uso del sitio y administrar usuarios y dispositivos sin complicaciones.

Accede al portal

Abre un navegador web y ve a https://admin.biostarair.com para acceder al Portal de BioStar Air. Cuando aparezca la página de inicio de sesión, selecciona **Global Server** o **EU Server** según tu ubicación.

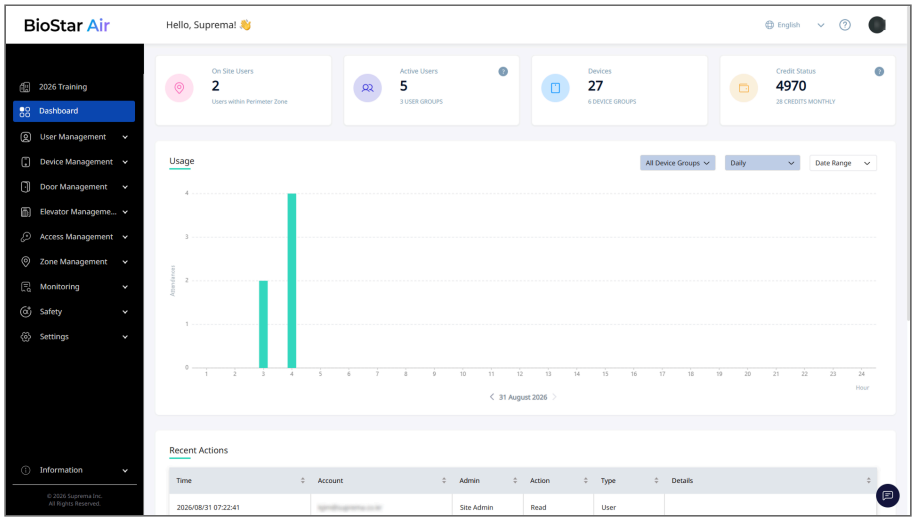


Información

No puedes crear una cuenta registrándote. El instalador del sistema o un administrador existente debe invitarte al sitio. Para más información sobre la gestión de cuentas de administrador e invitaciones, consulta Administrar cuentas y roles de administradores.

Explora el panel

Después de iniciar sesión, aparece **Panel de Control** y muestra información clave del sitio.



- **Usuarios en el sitio**: Ver usuarios en el sitio en tiempo real. El sistema calcula el estado de presencia según los registros de autenticación de los dispositivos de entrada y salida configurados en **Perímetro**. Para más información, consulta lo siguiente.
  - Administrar Zonas
  - Comprobar Presencia
- **Usuarios activos**: Muestra el número total de usuarios registrados y activos. Haz clic en la tarjeta para abrir **Gestión de usuarios**.
- **Dispositivos**: Muestra el número de dispositivos registrados. Haz clic en la tarjeta para abrir **Gestión de dispositivos**.
- **Estado de crédito**: Muestra los créditos restantes de la cuenta. Haz clic en la tarjeta para abrir **Ajustes** → **Centro de crédito**.
- **Uso**: Ordena el uso por grupo de dispositivos, frecuencia (diaria, semanal, mensual) o rango de fechas personalizado.
- **Acciones recientes**: Muestra un registro de actividad con las acciones de los administradores, como inicios de sesión, actualizaciones de dispositivos y creación de usuarios.

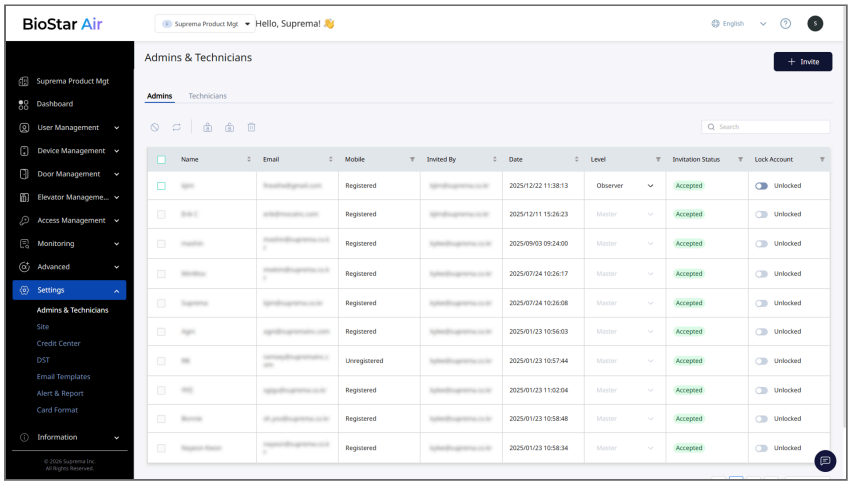
Guía de configuración del sitio

Sigue estas instrucciones para configurar un nuevo sitio.

1 Agregar administradores

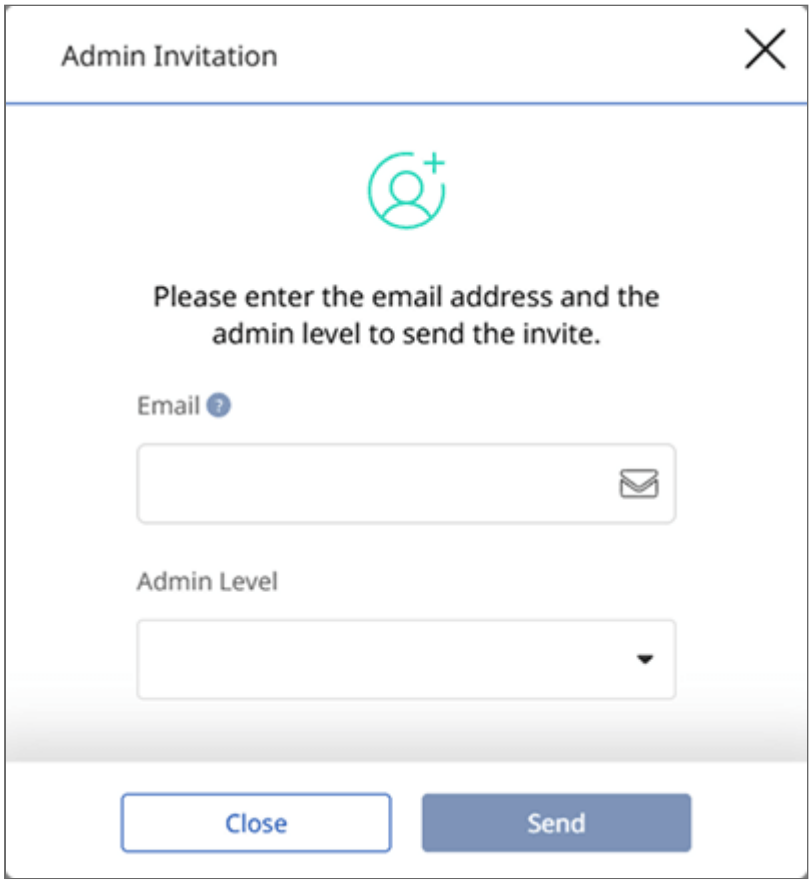
Invita a administradores.

1. Haga clic en **Ajustes** → **Administradores y técnicos** en la barra lateral izquierda.



2. Haga clic en **Invitar** en la esquina superior derecha de la pantalla.

3. Cuando aparezca la ventana **Invitación de administrador**, ingresa la dirección de correo electrónico del administrador y asigna un rol.

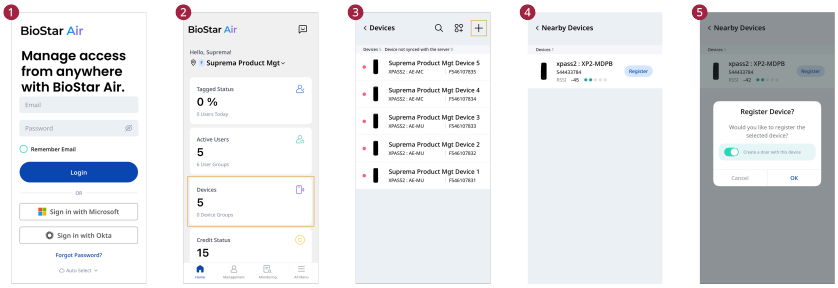


4. Haz clic en **Enviar**.

> **Información**
>
> Los administradores del sitio pueden gestionarlo, y los usuarios autenticados solo pueden acceder a él a través de la app **Suprema Pass**.

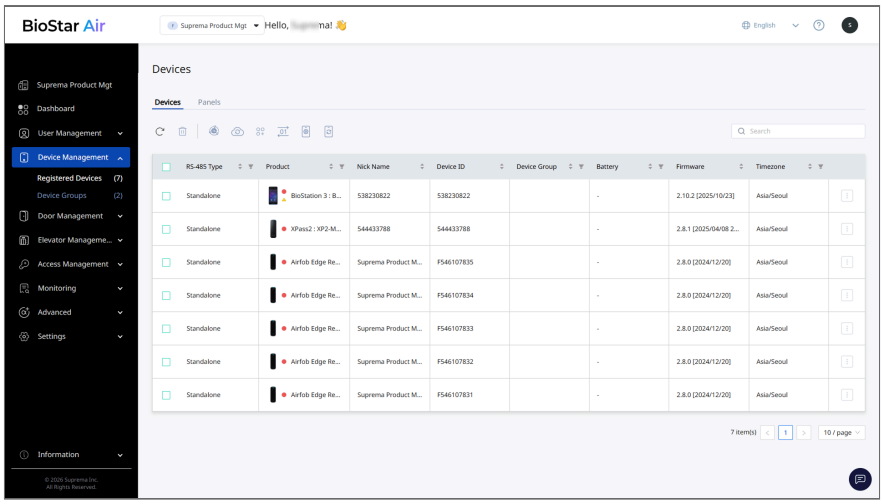
2 Registrar dispositivos

Utilice la aplicación móvil BioStar Air para registrar dispositivos. Registre los dispositivos mediante Bluetooth Low Energy (BLE) y adminístrelos desde el portal BioStar Air.



1. Abra la aplicación BioStar Air en su dispositivo móvil e inicie sesión.
2. Toque la tarjeta **Dispositivos**.
3. Toque + en la esquina superior derecha de la pantalla.
4. En la pantalla de búsqueda de dispositivos, toque **Registrar** en el dispositivo que desea registrar.
5. Cuando aparezca la ventana de registro del dispositivo, toque **OK**.

Vuelve a la lista de dispositivos y confirma que se agregó el dispositivo. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.

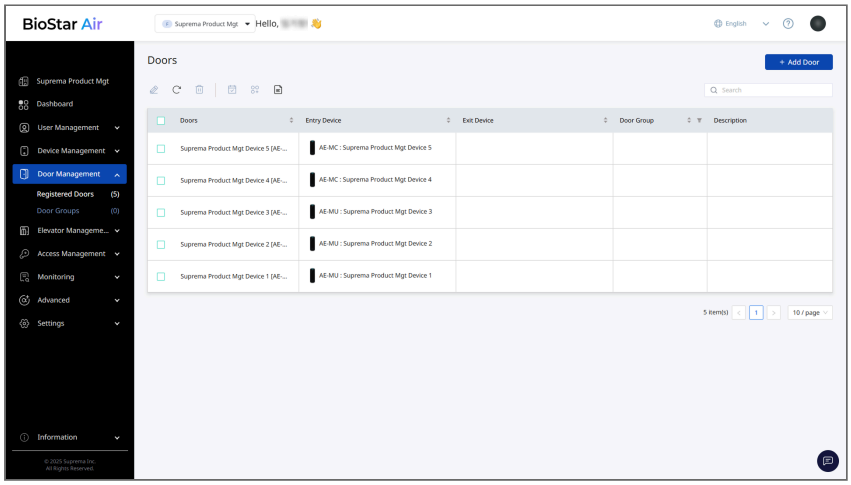


- Si el dispositivo no está registrado, pide a otro administrador que lo registre en el sitio con la app móvil de BioStar Air.
- En **Dispositivos registrados**, elimina dispositivos, actualiza el firmware y gestiona grupos de dispositivos.

3 Crear y administrar puertas

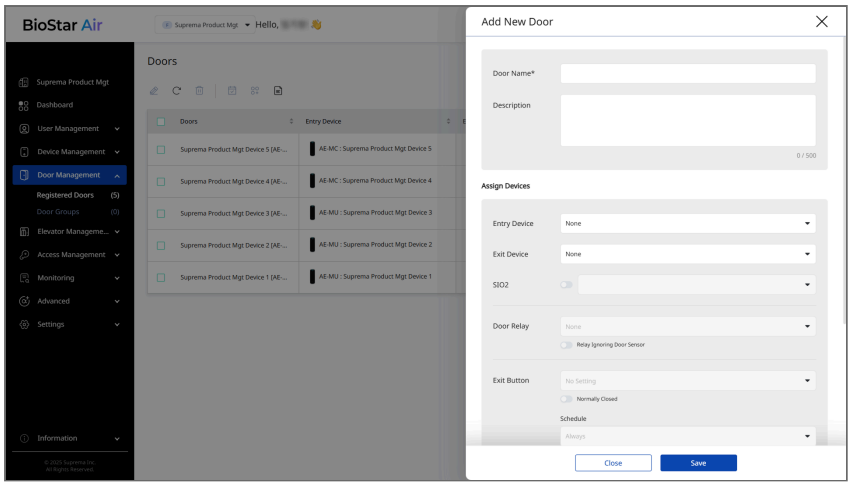
Agregar puertas y asignar dispositivos.

1. Haga clic en **Gestión de Puerta** → **Registrados Puerta** en la barra lateral izquierda.



2. Si no aparece ninguna puerta en la lista, haz clic en **Agregar Puerta** en la esquina superior derecha.

3. Cuando aparezca el panel **Agregar nuevo puerta**, ingresa un nombre y una descripción.



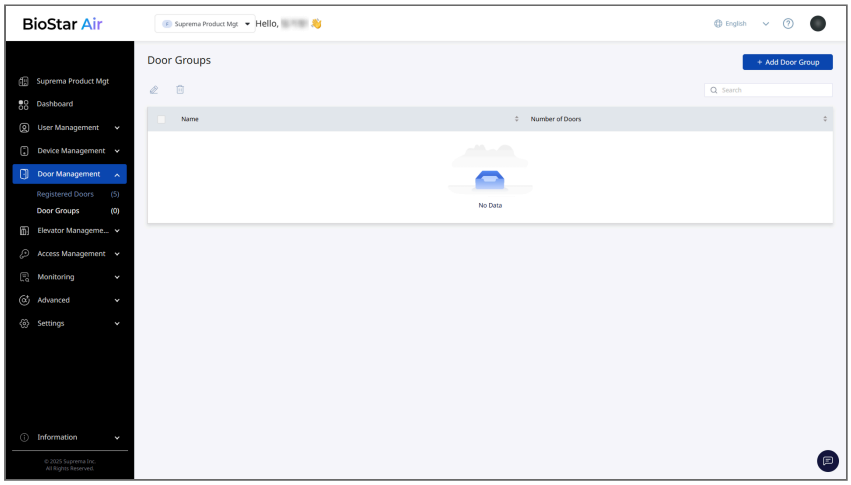
4. Asigna los dispositivos registrados a **Dispositivo de entrada** y a **Dispositivo de salida**.

En **Gestión de Puerta** puedes editar o eliminar puertas, configurar sus horarios y administrarlas por grupo.

4 Categorizar puertas en grupos

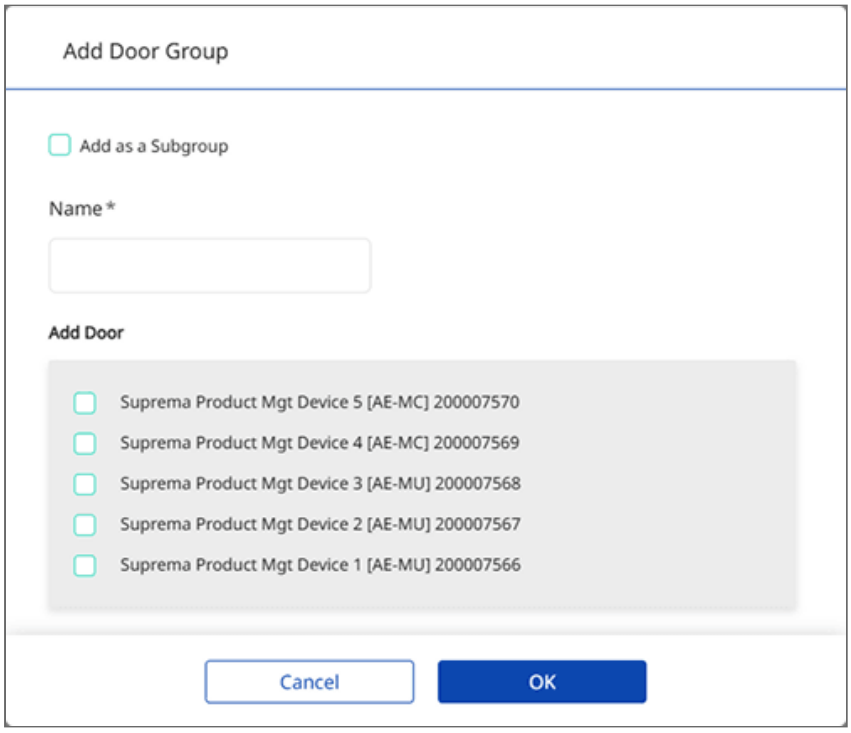
Categorizar puertas en grupos.

1. Haga clic en **Gestión de Puerta** → **Grupo de Puerta** en la barra lateral izquierda.



2. Haga clic en **Nombre del Grupo de Puerta** en la parte superior derecha de la pantalla.

3. Cuando aparezca la ventana **Nombre del Grupo de Puerta**, ingresa un nombre de grupo como **Indoor**, **Outdoor** o **Trap Doors** y selecciona las puertas deseadas.



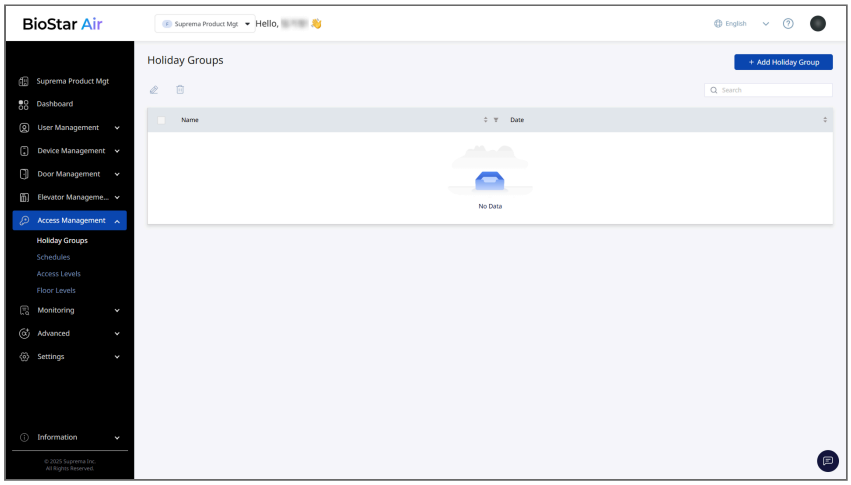
4. Después de seleccionar todas las puertas, haz clic en **OK**.

5 Configurar derechos de acceso

Sigue estos pasos para administrar los derechos de acceso.

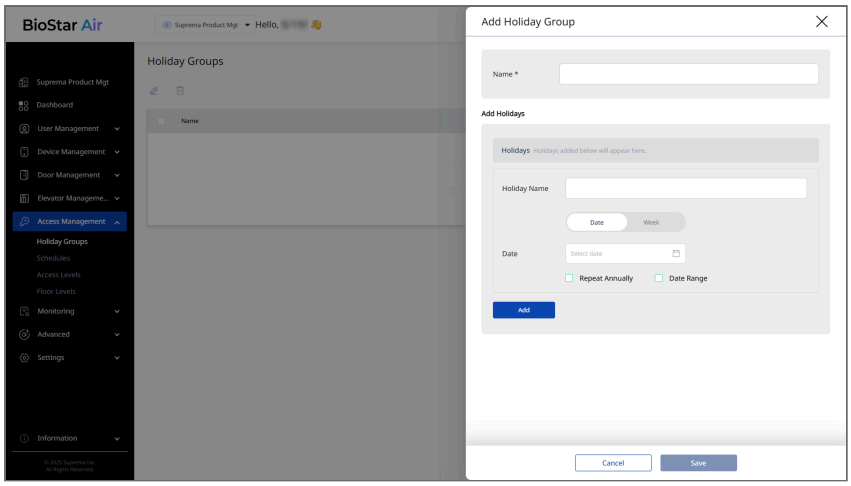
6 Configurar grupos de días festivos

1. En la barra lateral izquierda, haz clic en **Gestión de Acceso** → **Grupos de festivos**.



2. Haz clic en **Agregar grupo de festivos** en la esquina superior derecha de la pantalla.

3. Cuando aparezca el panel **Agregar grupo de festivos**, ingresa un nombre (por ejemplo, "Korea Holidays").

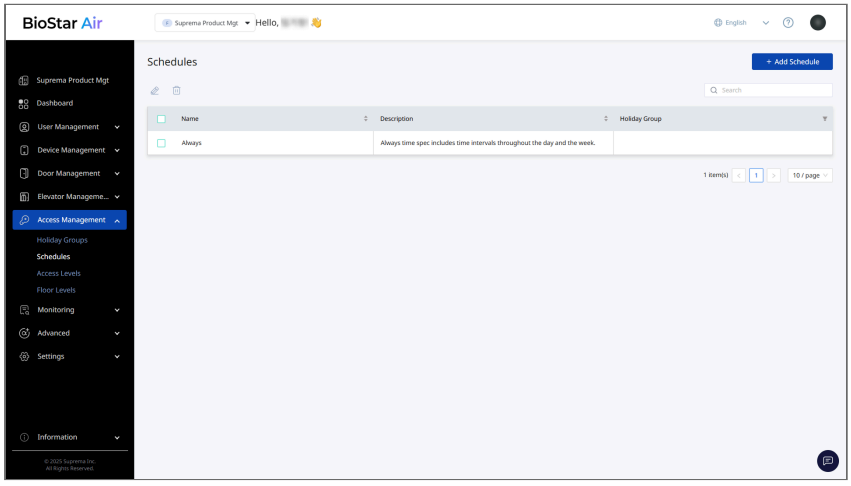


4. En la sección **Añadir días Festivos**, especifica los días festivos en los que se debe restringir el acceso y haz clic en **Agregar**.

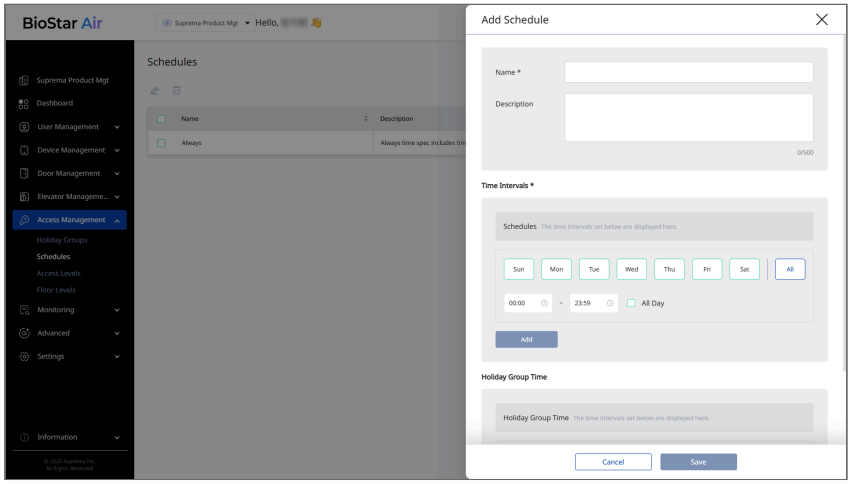
5. Después de agregar todos los días festivos, haz clic en **Guardar**.

7 Crear horarios

1. Haz clic en **Gestión de Acceso** → **Horarios** en la barra lateral izquierda.



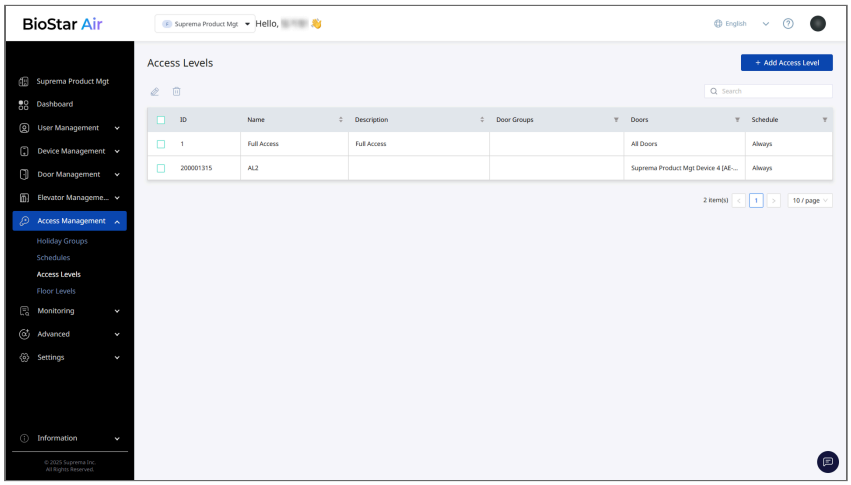
2. Haz clic en **Agregar Horarios** en la esquina superior derecha de la pantalla.
3. Cuando aparezca el panel **Agregar Horarios**, ingresa un nombre.



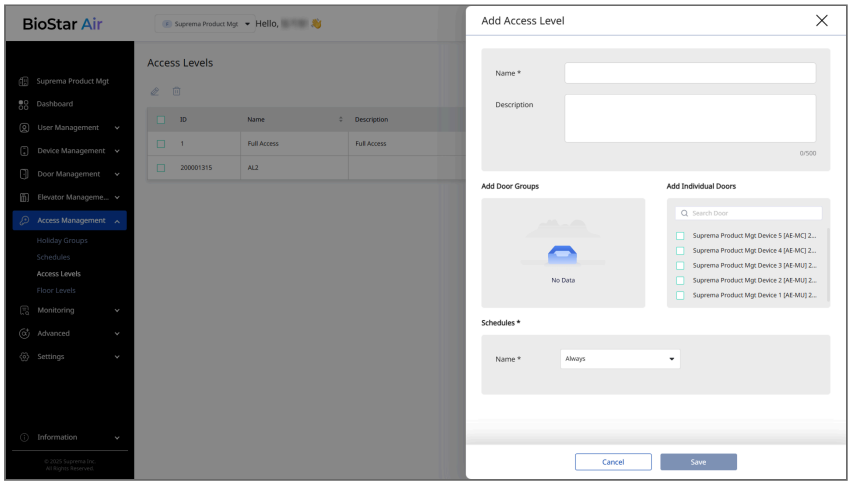
4. Selecciona los días a activar y vincula un grupo de días festivos.
5. Una vez completado el horario, haz clic en **Guardar**.

8 Definir niveles de acceso

1. Haga clic en **Gestión de Acceso** → **Niveles de acceso** en la barra lateral izquierda.



2. Haga clic en **Agregar Nivel de Acceso** en la esquina superior derecha de la pantalla.
3. Cuando aparezca el panel **Nivel de acceso**, ingresa un nombre y asigna grupos de puertas, puertas individuales y horarios.

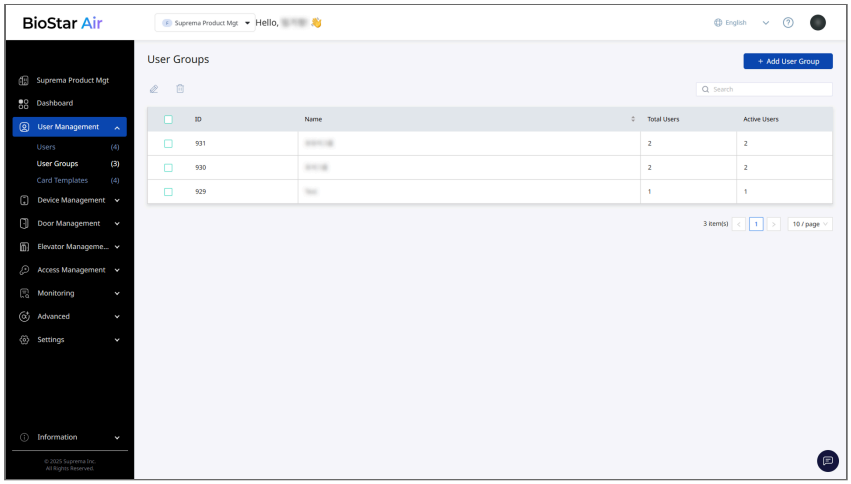


4. Una vez configurado el nivel de acceso, haz clic en **Guardar**.

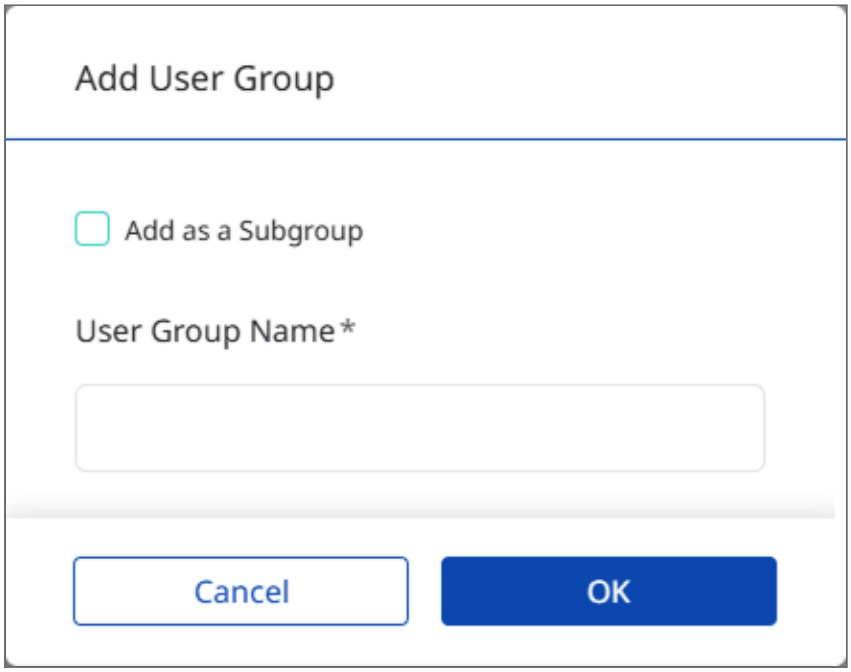
9 Crear grupos de usuarios y agregar usuarios

Cree un grupo de usuarios y agregue usuarios al nuevo grupo.

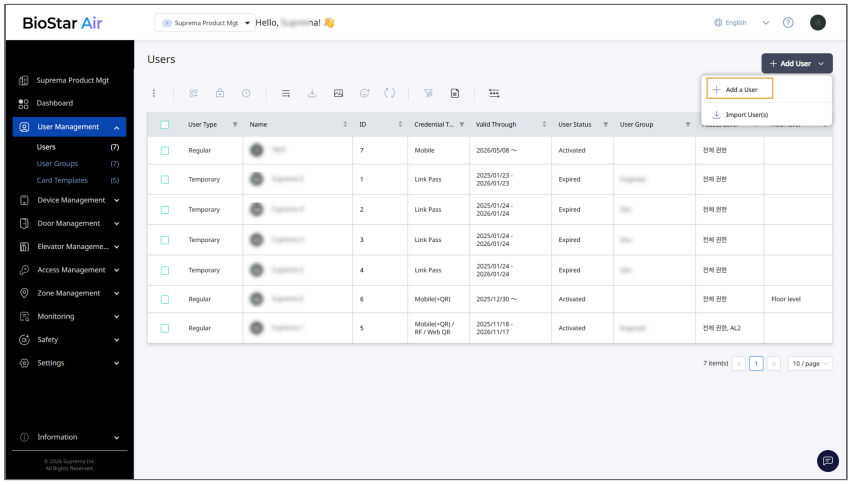
1. Haz clic en **Gestión de usuarios** → **Grupos de Usuarios** en la barra lateral izquierda.



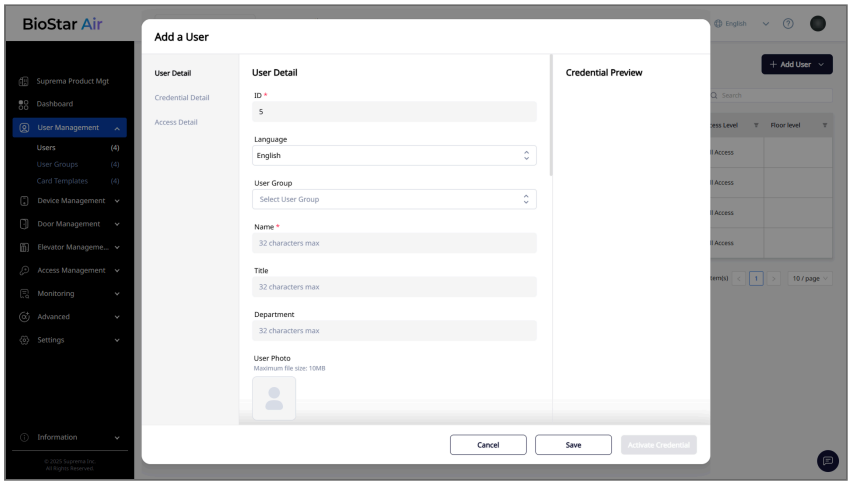
2. Haz clic en **Agregar grupos de usuarios** en la parte superior derecha de la pantalla.
3. Cuando aparezca la ventana **Agregar grupo de usuarios**, ingresa el nombre del grupo de usuarios.



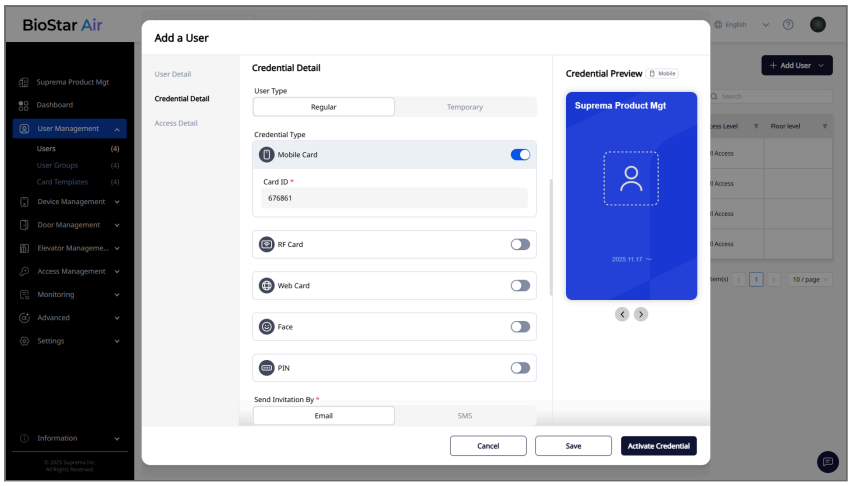
4. Haga clic en **OK** para guardar el grupo de usuarios.
5. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
6. Haga clic en **Añadir nuevo usuario** → **Agregar un usuario** en la esquina superior derecha de la pantalla.



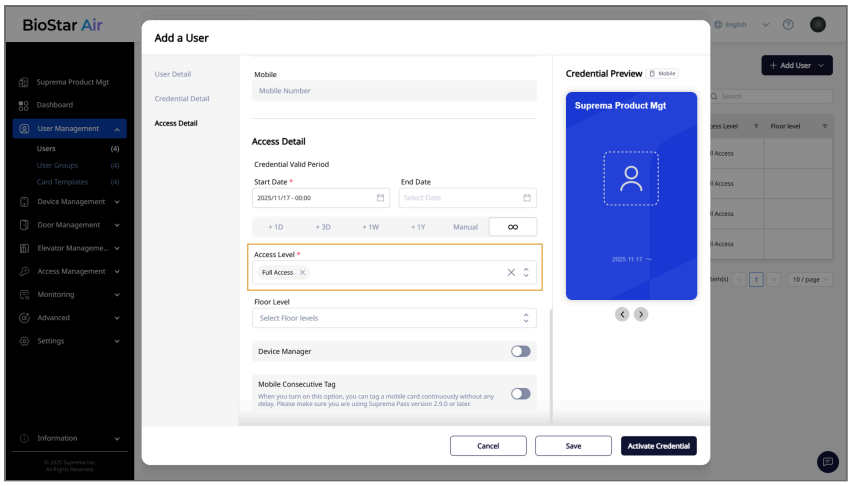
7. Cuando aparezca la ventana **Agregar un usuario**, introduzca el ID del usuario, el nombre, etc. en la sección **Detalles del usuario**.



8. En la sección **Detalles de la Credencial**, habilite uno o más tipos de credenciales.



9. En la sección **Detalles de acceso**, seleccione un nivel de acceso.



10. Para finalizar la configuración del acceso del usuario, haga clic en **Activar Credencial** en la esquina inferior derecha.

> **Información**
>
> En el menú **Gestión de usuarios** → **Grupos de Usuarios** puede administrar usuarios de forma masiva: reemitir, suspender o eliminar usuarios; exportar datos y cargar imágenes de perfil en lote.

Consejo

Lista de verificación

Para resumir, siga estos pasos.

1. Agregar administradores.
2. Registrar dispositivos.
3. Crear puertas y asignar dispositivos.
4. Categorizar puertas en grupos.
5. Configurar derechos de acceso (días festivos, horarios, niveles de acceso).
6. Crear grupos de usuarios y agregar usuarios.

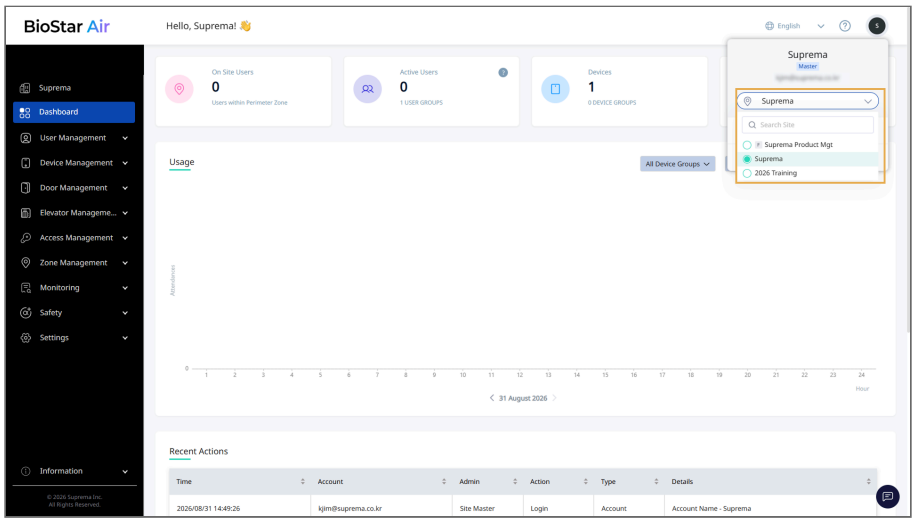
Seguir estos pasos permite configurar el sitio de BioStar Air sin problemas. Consulte los tutoriales en video individuales de la guía del usuario para obtener más detalles.

Selector de sitios

La función **Selector de sitios** simplifica los procesos y reduce la necesidad de iniciar sesión varias veces al permitir administrar múltiples sitios con una sola dirección de correo electrónico.

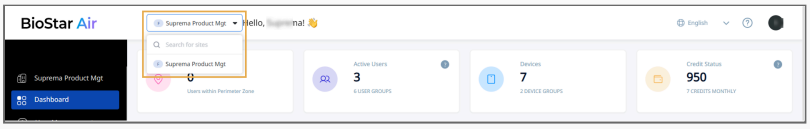
¿Qué es el Selector de sitios?

La función **Selector de sitios** permite iniciar sesión en el portal de BioStar Air con una sola dirección de correo electrónico, incluso cuando se administran múltiples sitios. No es necesario iniciar sesión con direcciones de correo distintas para cada sitio. Inicie sesión una vez con una sola dirección de correo y luego use el menú **Selector de sitios** para cambiar fácilmente entre los sitios que administra.



Información

- Aunque se use una dirección de correo unificada, los permisos y la configuración de cada sitio siguen siendo independientes. Los roles de administrador y los derechos de acceso se gestionan por separado para cada sitio.
- Si la función **Selector de sitios** no aparece o se muestra un sitio incorrecto, verifique que la solicitud de migración esté completa; si no lo está, comuníquese con el equipo de soporte para recibir ayuda.
- La función **Selector de sitios** agiliza el proceso de inicio de sesión y consolida varios sitios en una sola cuenta, ahorrando tiempo y esfuerzo al gestionar múltiples sitios en BioStar Air.
- Los sitios marcados con un icono F son Sitios federados en la lista de selección de sitios. Los Sitios federados se muestran en la esquina superior izquierda de la pantalla. Para obtener más información sobre Sitios federados, consulte Administrar sitios federados.



Crear un nuevo sitio

Al crear un nuevo sitio a través del Partner Portal, utilice una dirección de correo electrónico que ya esté registrada como cuenta de administrador en otro sitio. El sistema vincula automáticamente el nuevo sitio al correo existente, lo que permite administrar múltiples sitios con una sola cuenta.

- Cree un nuevo sitio mediante el Partner Portal.
- Cuando se solicite el correo electrónico del administrador, introduzca la dirección que ya está vinculada a otro sitio.
- El nuevo sitio se vincula automáticamente a la cuenta existente.

Información

Para obtener información detallada sobre cómo registrarse y usar el Partner Portal, consulte Usa el Portal de Socios.

Usar una misma dirección de correo en varios sitios

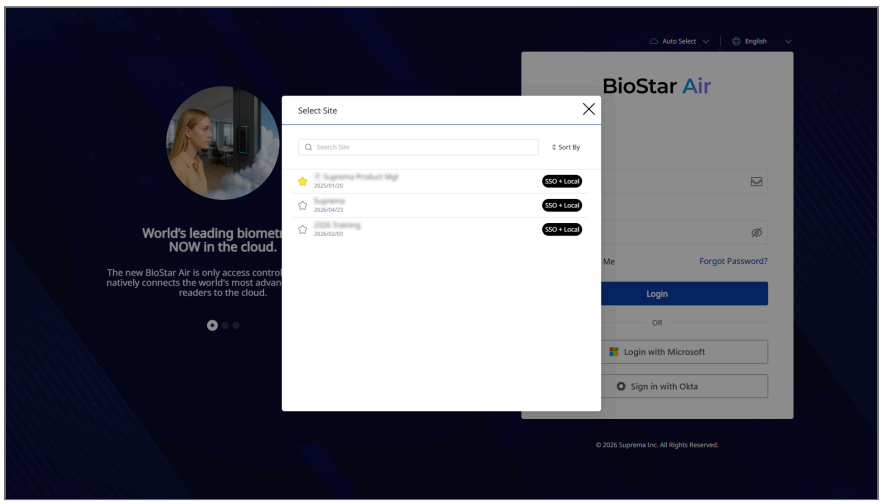
Si ya administra varios sitios pero cada uno utiliza credenciales de inicio de sesión distintas, solicite una migración manual a **Suprema**. Este proceso consolida las direcciones de correo electrónico y permite administrar todos los sitios con un único inicio de sesión.

- Comuníquese con el equipo de soporte y solicite una migración manual de los sitios.
- Si se usan direcciones alias como bob+site1@example.com y bob+site2@example.com, proporcione la dirección de correo raíz (bob@example.com).
- Si se usan direcciones de correo completamente distintas para cada sitio, proporcione la lista completa de direcciones de correo electrónico.
- Una vez completada la migración, acceda a todos los sitios con una sola dirección de correo mediante la función **Selector de sitios**.

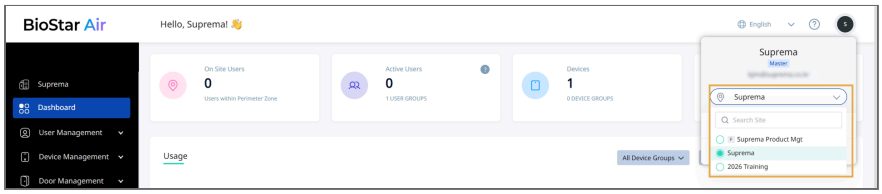
Cómo usar el Selector de sitios

Si su dirección de correo está asociada a varios sitios, iniciar sesión y cambiar entre ellos es sencillo.

1. Ingrese su dirección de correo electrónico y su contraseña.
2. Si administra varios sitios, use la ventana **Seleccionar Sitio** para encontrar rápidamente el sitio que desea. Al seleccionar un sitio, accederá al panel de control.



3. Después de iniciar sesión, haga clic en el icono de su perfil en la esquina superior derecha de la pantalla.
4. Cuando aparezca el menú emergente, haga clic en la opción **Selector de sitio** situada debajo de su dirección de correo electrónico.



Puede ver una lista de todos los sitios asociados a su dirección de correo electrónico.

Primeros pasos con la aplicación BioStar Air

La aplicación BioStar Air ofrece las mismas funciones que el portal web. Los usuarios pueden gestionar el control de acceso, supervisar los registros de eventos, controlar dispositivos y realizar tareas administrativas directamente desde un dispositivo móvil.

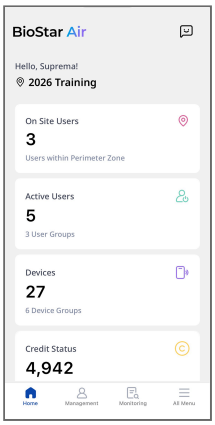
Descarga la aplicación móvil

Descarga la aplicación BioStar Air en tu dispositivo móvil e inicia sesión.

- Descarga e instala la aplicación BioStar Air en tu dispositivo móvil.
  - iOS
  - Android
- Inicia sesión con el mismo ID y contraseña que usas para el portal web de BioStar Air.

Información

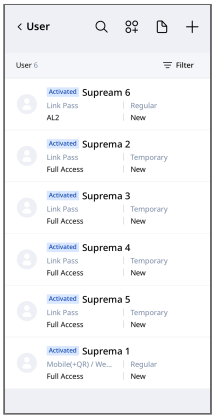
- Verifica que hayas iniciado sesión con las mismas credenciales que en la versión web.
- Mantente cerca del dispositivo para actualizarlo en modo BLE.
- Algunas funciones, como el monitoreo de video en tiempo real, requieren una cámara conectada.



Panel de control

Después de iniciar sesión en la aplicación móvil, **Panel de Control** en la pantalla de inicio muestra la siguiente información.

- Accesos diarios de usuarios
- Total de usuarios registrados activos
- Dispositivos conectados
- Estado de crédito



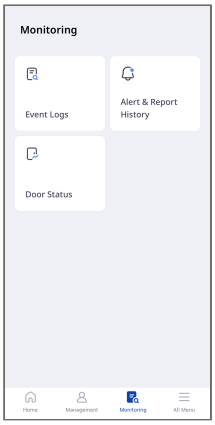
Gestión de usuarios

Toca la tarjeta **Usuarios activos** en la pantalla de inicio, o toca en secuencia **Administrar** → **Usuarios**.

- Selecciona un usuario y revisa los detalles.
- Modifica el estado del usuario (reemitir, suspender, eliminar o activar).
- Toca el botón + e ingresa los datos requeridos para agregar un nuevo usuario.

Información

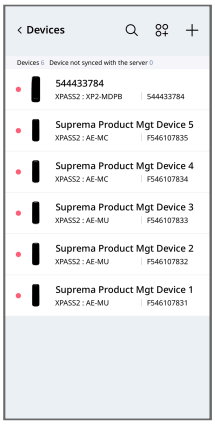
- Para aprender a agregar usuarios desde la aplicación móvil, consulta Agregar usuarios.
- Para aprender a agregar usuarios a través del portal de BioStar Air, consulta Agregar usuarios.
- Para obtener más información sobre la gestión de usuarios, consulta Administrar Usuarios.



Supervisión

Monitoreo proporciona la siguiente información.

- **Registros de eventos**: Supervisar y analizar los registros de eventos y de auditoría. Para más información, consulte Usar registros de eventos y Usar registros de auditoría.
- **Historial de Alertas e Informes**: Ver alertas anteriores y el historial de informes generados a través del portal web y la aplicación móvil. Para más información, consulte Consultar historial de alertas e informes.
- **Estado de puerta**: Supervisar el estado en tiempo real de las puertas conectadas al sitio. Para más información, consulte Supervisar el estado de la puerta.
  - Consultar el estado de la puerta y controlarla de forma remota.
  - Toque una puerta una vez para editarla, o manténgala pulsada para seleccionar varias puertas y realizar acciones en lote.
  - Configurar una puerta en **Modo de desbloqueo** o **Modo de bloqueo** anula la configuración del relé o los horarios.
  - Elimine las puertas no utilizadas según sea necesario.
- Video en tiempo real (si hay una cámara conectada)



Dispositivos

Toque la tarjeta **Dispositivos** en la pantalla de inicio, o toque **Administrar** → **Dispositivos** en ese orden.

- Ver todos los dispositivos registrados.
- Seleccione un dispositivo para editarlo, actualizar su firmware o reiniciarlo.
- Si el dispositivo no está conectado a la red, utilice el modo **BLE** cerca del dispositivo para actualizar su firmware.
- Toque el botón + para agregar un nuevo dispositivo.

> **Información**
>
> Para obtener más información sobre la gestión de dispositivos, consulte lo siguiente.
>
> - Aplicación BioStar Air: Registrar y Eliminar Dispositivos Edge
> - Portal BioStar Air: Dispositivos

Administrar sitios

En BioStar Air, un **sitio** es la unidad central del sistema de control de acceso y representa una ubicación física a la que pueden acceder los usuarios. Cada sitio puede contar con ajustes, usuarios, dispositivos y permisos de acceso propios. Los administradores pueden crear y administrar varios sitios para gestionar el control de acceso de forma eficiente en distintas

ubicaciones.

Consulte los siguientes documentos para saber cómo administrar los sitios de manera eficaz en el portal de BioStar Air.

Usuarios

Esta sección explica cómo crear cuentas de usuario en BioStar Air, configurar distintas credenciales (tarjeta móvil, tarjeta RF, tarjeta web, autenticación facial y PIN) y establecer permisos de acceso y periodos de vigencia. Aborda todos los aspectos de la gestión de usuarios, desde el manejo de usuarios individuales hasta la realización de operaciones masivas, la administración de grupos de usuarios y el uso de filtros.

> **Consejo**
> Vea el siguiente video para comprender mejor las funciones de gestión de usuarios.

Agregar usuarios

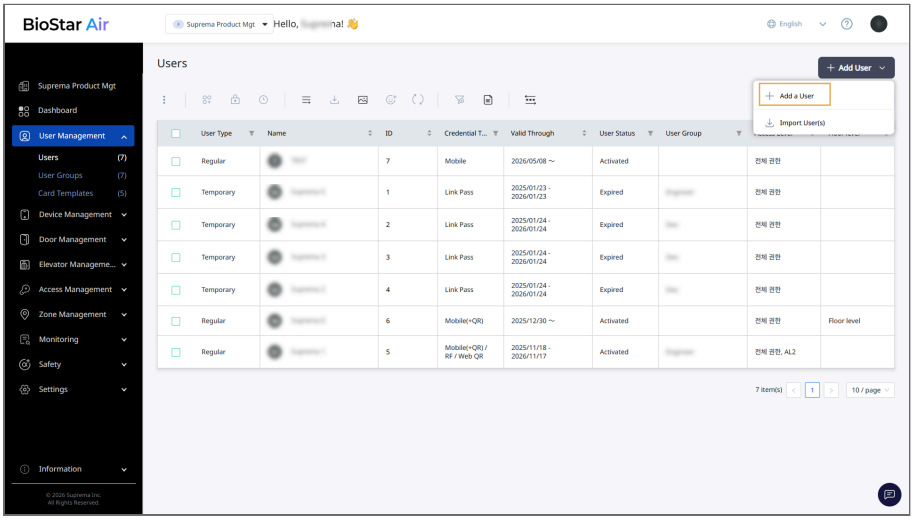
Este documento ofrece instrucciones paso a paso para agregar y administrar usuarios individuales en BioStar Air. Cubre todo el proceso: seleccionar el tipo de usuario (regular o temporal), emitir las credenciales correspondientes y establecer los niveles de acceso y los períodos de validez. También muestra cómo editar o eliminar la información del usuario agregado.

> **Consejo**
> Vea el siguiente video para seguir una guía paso a paso sobre el proceso completo de agregar un nuevo usuario.

Agregar usuarios

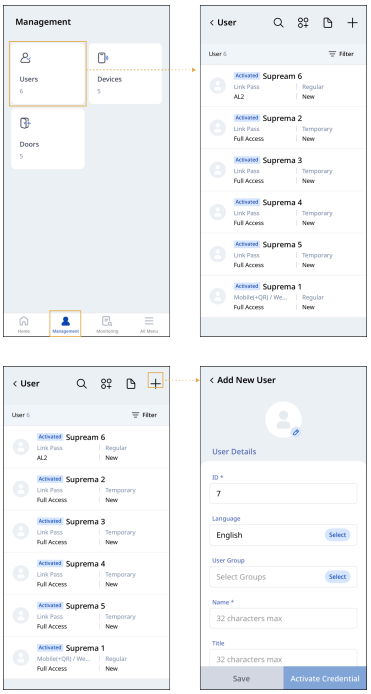
Web

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Aparece una lista de usuarios.
3. Haga clic en **Añadir nuevo usuario** → **Agregar un usuario** en la esquina superior derecha de la pantalla.



Cuando aparezca la ventana **Agregar un usuario**, ingrese y configure la información requerida en cada sección. Rellene los campos obligatorios de todas las secciones y haga clic en **Activar Credencial** en la esquina inferior derecha.

Mobile



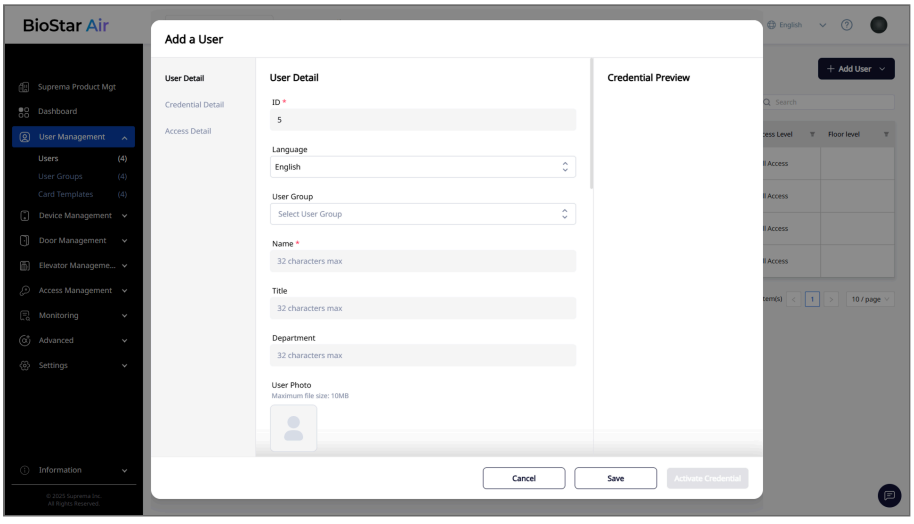
1. Inicie sesión con la aplicación móvil.
2. Toque **Administrar** en la parte inferior de la pantalla.
3. Toque la tarjeta **Usuarios**.
4. Toque + en la parte superior de la lista de usuarios.

Cuando aparezca la pantalla **Agregar un usuario**, ingrese y configure la información requerida en cada sección. Rellene los campos obligatorios de todas las secciones y haga clic en **Activar Credencial** en la esquina inferior derecha.

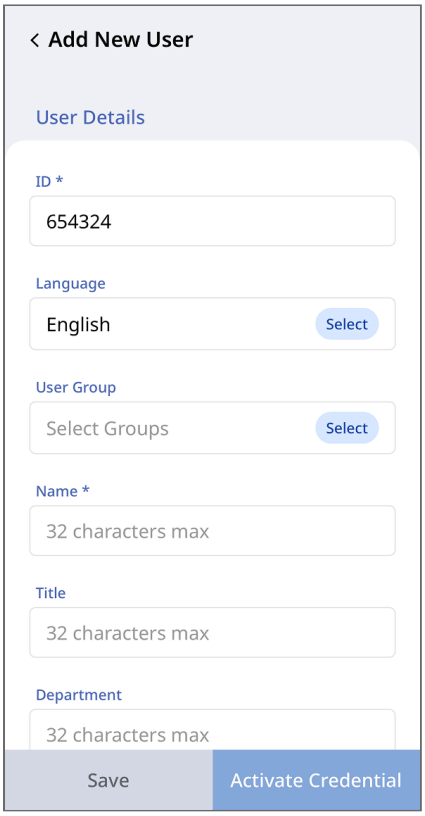
Ingrese la información del usuario

Ingrese la información básica del nuevo usuario en la sección **Detalles del usuario**.

Web



Mobile



- **ID**: Ingrese un ID específico manualmente o permita que el sistema lo genere de forma secuencial.
- **Idioma**: Seleccione el idioma predeterminado del usuario.
- **Grupo de usuario**: Seleccione el grupo al que pertenece el usuario.
- **Nombre**: Ingrese el nombre completo del usuario.
- **Puesto**: Ingrese el cargo del usuario.
- **Departamento**: Ingrese el nombre del departamento del usuario.
- **Foto de usuario**: Cargue la imagen de perfil del usuario. Para más información, consulte Subir imagen de perfil.

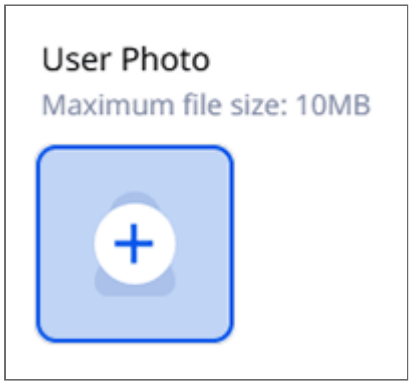
Información

- * indica un campo obligatorio.
- Ingrese el correo electrónico y el número de teléfono del usuario en **Enviar invitación por** en la sección **Detalles de la Credencial**.

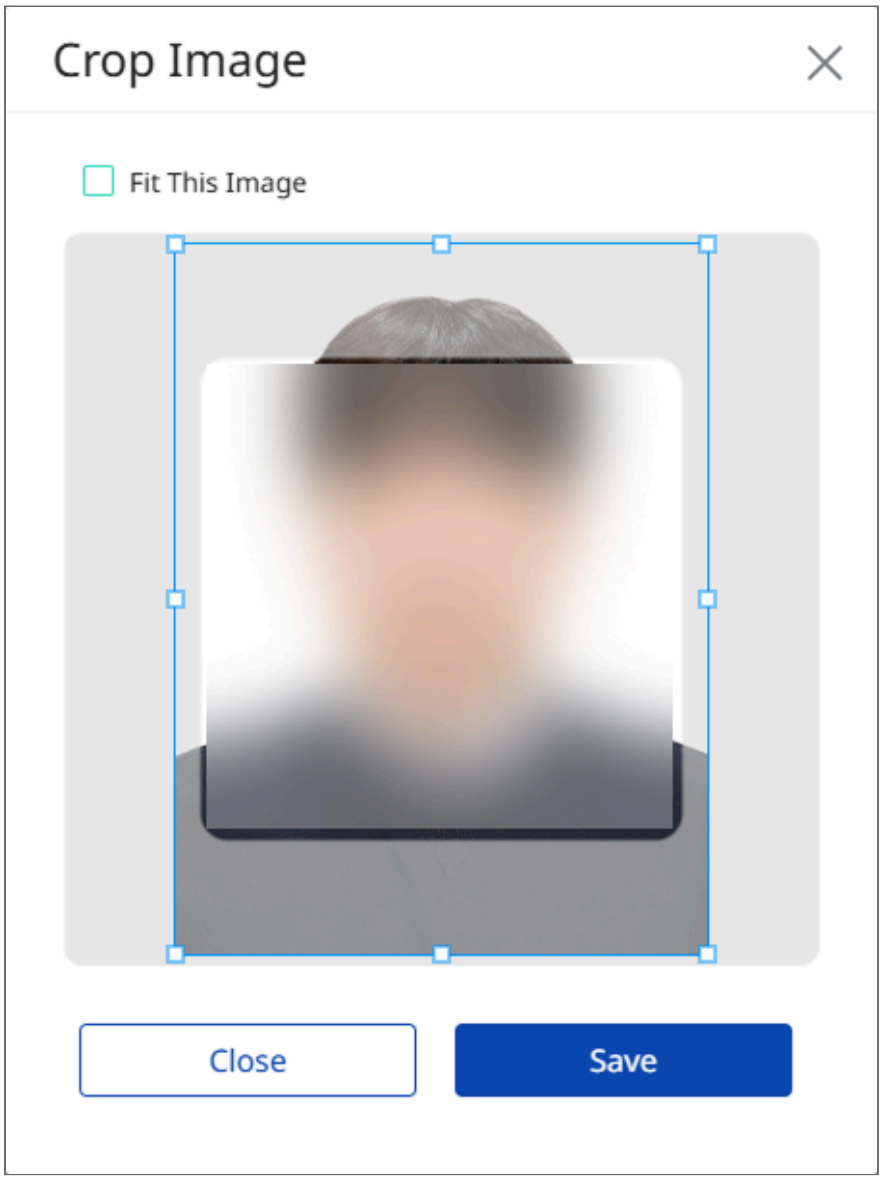
Subir imagen de perfil

Web

1. Pase el cursor sobre el área de la imagen de perfil y haga clic en el icono +.

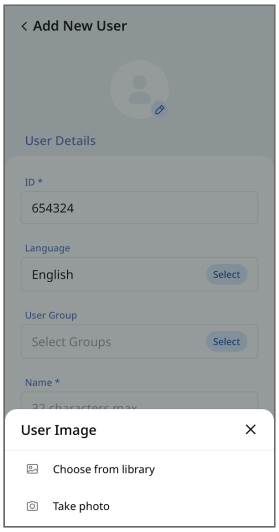


2. Seleccione el archivo de imagen guardado localmente.
3. Cuando aparezca la ventana **Delimitar imagen**, ajuste la foto al tamaño deseado. Haga clic en **Ajuste esta imagen** para redimensionarla automáticamente.



4. Haga clic en **Guardar** para guardar la imagen cargada como imagen de perfil.

Mobile



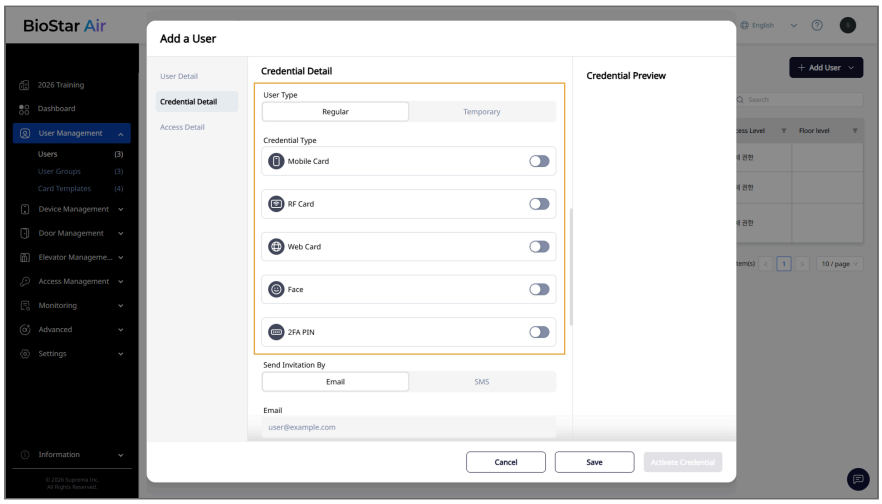
1. Toque la imagen de perfil del usuario.
2. Elija cómo agregar una imagen desde el menú que aparece en la parte inferior.
   - **Seleccionar de la biblioteca**: Seleccione un archivo de imagen guardado en su dispositivo móvil para subirlo.
   - **Tomar foto**: Utilice la cámara de su dispositivo móvil para tomar una foto y subirla.
3. Redimensione la imagen cargada a un tamaño adecuado y guárdela.

Seleccionar el tipo de usuario

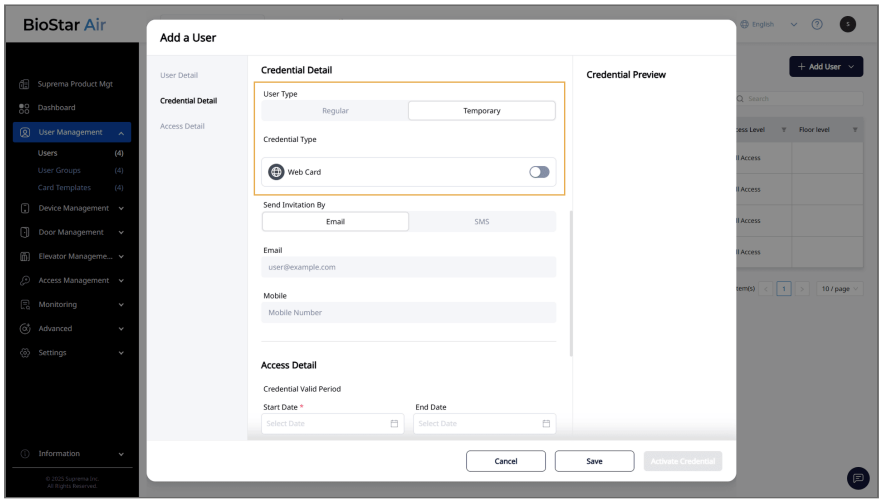
Web

Seleccione si el usuario que está agregando en la sección **Detalles de la Credencial** es un usuario regular o un visitante. Los tipos de credenciales que se pueden emitir varían según el tipo de usuario.

- **Regular**: Un usuario que es miembro regular de una organización o instalación y que requiere acceso a largo plazo. Se pueden emitir todos los tipos de credenciales.

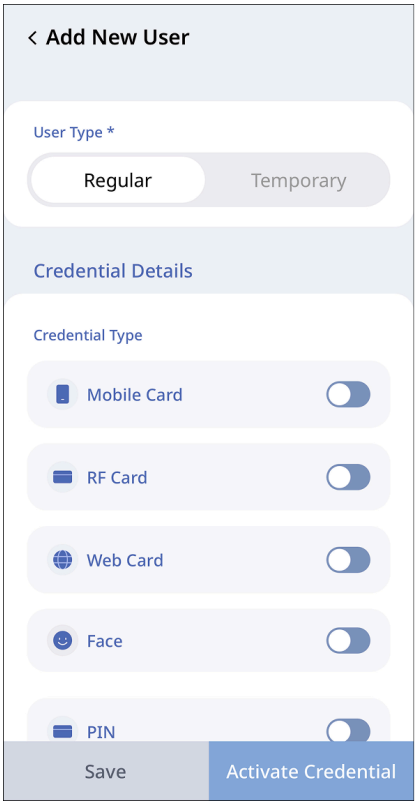


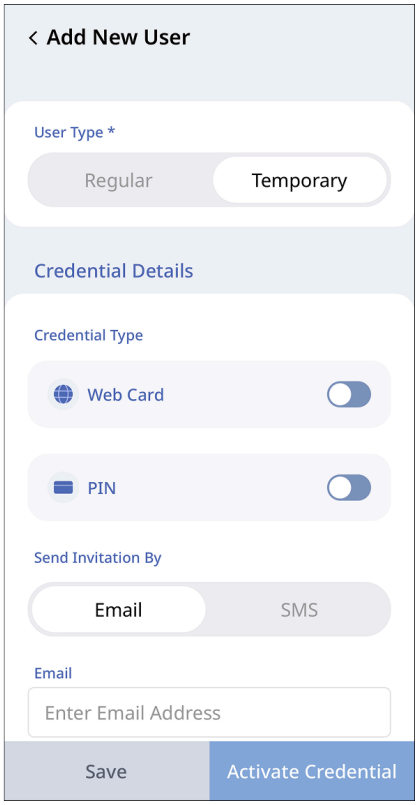
- **Invitada**: Un visitante o miembro no regular que necesita acceso limitado y de corta duración. Esto puede incluir huéspedes, visitantes externos, contratistas temporales, mensajeros de entrega, etc. Solo se pueden emitir las credenciales **Tarjeta Web**, incluyendo el código QR y LinkPass.



Mobile

Seleccione si el usuario que está agregando en **Detalles de la Credencial** es un usuario regular o un visitante. Los tipos de credenciales que se pueden emitir varían según el tipo de usuario.





- **Regular**: Un usuario que es miembro regular de una organización o instalación y que requiere acceso a largo plazo. Se pueden emitir todos los tipos de credenciales.
- **Invitada**: Un visitante o miembro no regular que necesita acceso limitado y de corta duración. Esto puede incluir huéspedes, visitantes externos, contratistas temporales, mensajeros de entrega, etc. Solo se pueden emitir las credenciales **Tarjeta Web**, incluyendo el código QR y LinkPass.

Información

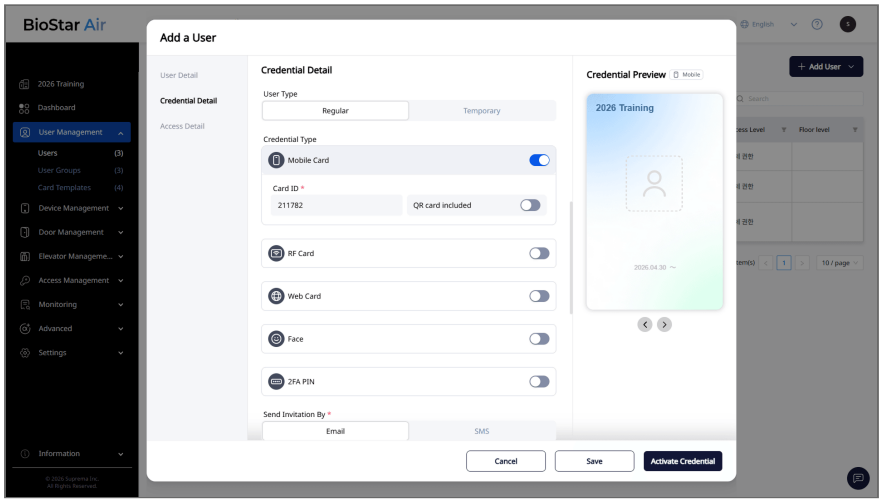
- A los usuarios **Regular** se les asigna automáticamente el nivel de acceso completo, mientras que los usuarios **Invitada** deben seleccionar manualmente un nivel de acceso.
- La opción **Tipo de Usuario** es compatible con BioStar Air versión 2.6 o superior.

Emitir credenciales

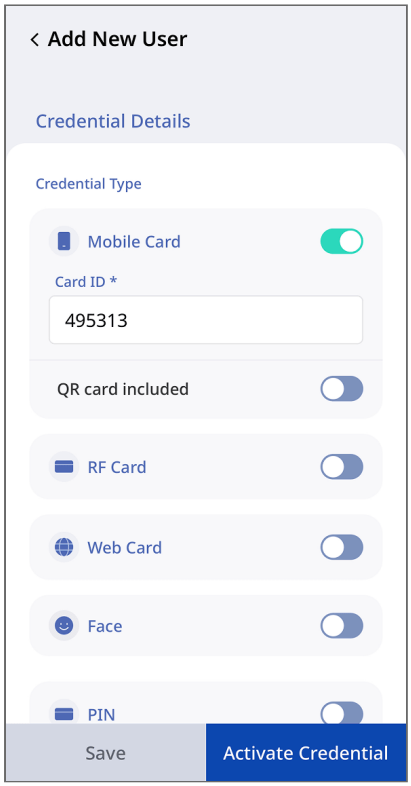
Introduzca la información del usuario y, a continuación, configure las credenciales que se usarán para la autenticación de acceso en la sección **Detalles de la Credencial**. Cada credencial tiene un interruptor para activarla o desactivarla.

- **Tarjeta Móvil**: Utilice la aplicación móvil Suprema Pass como método de autenticación de acceso. El administrador puede editar el ID de la tarjeta.

Web

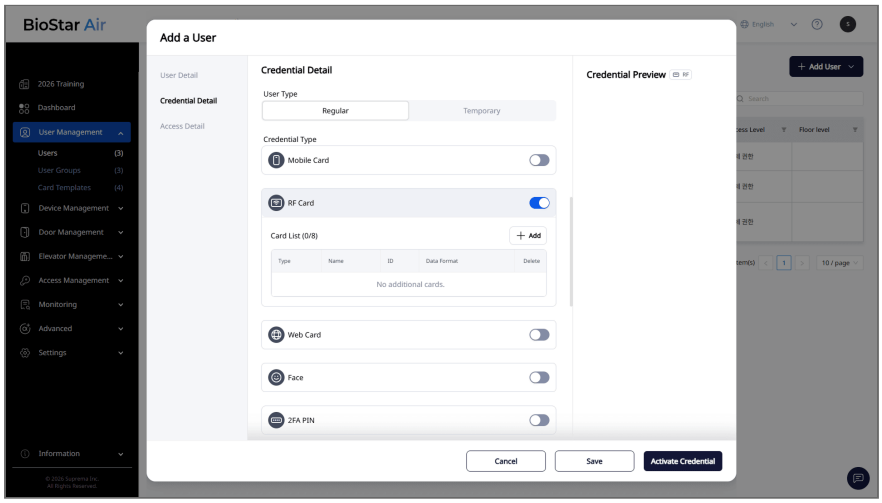


Mobile

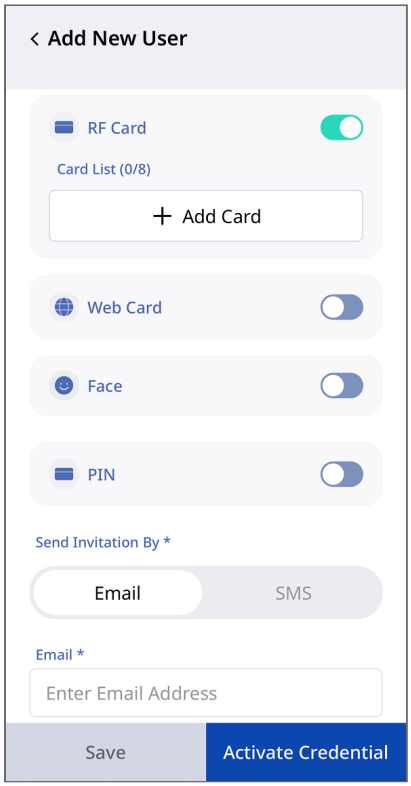


- **Tarjeta RF**: Agregue hasta ocho tarjetas RFID por usuario para la autenticación de acceso. Haga clic en **Agregar**.

Web

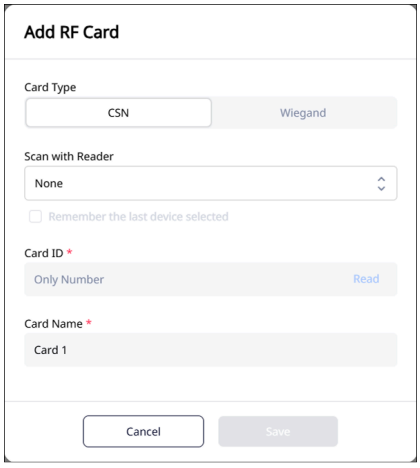


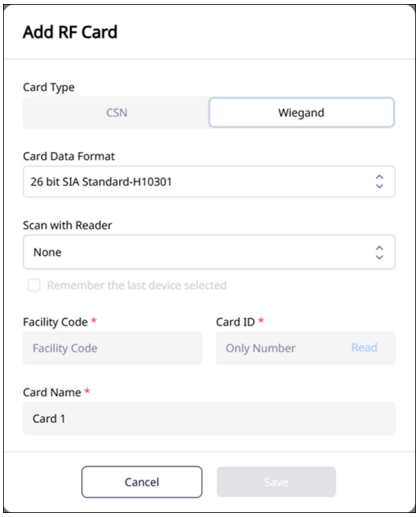
Mobile



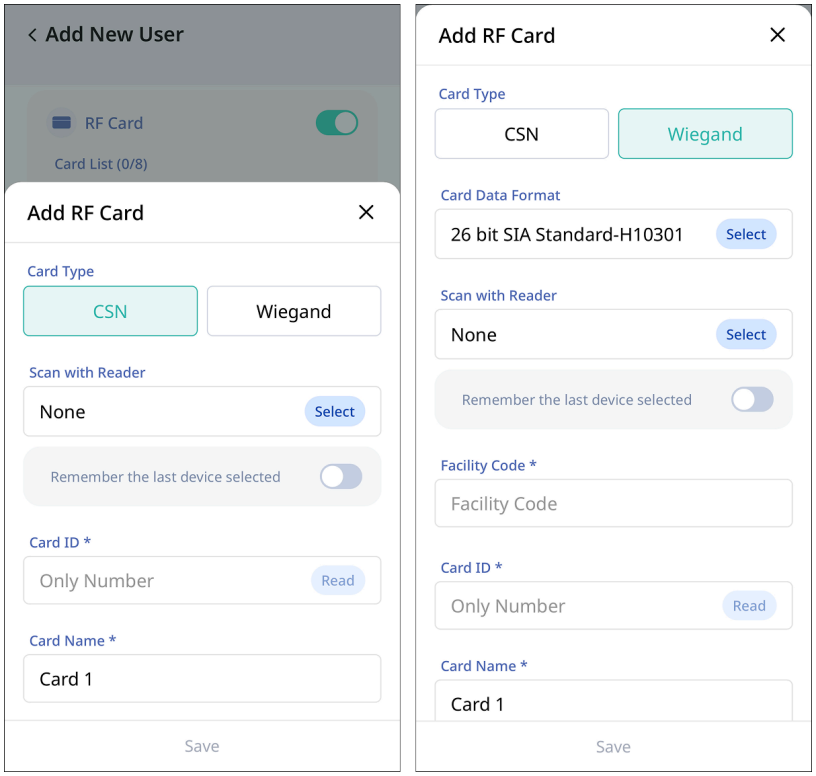
Configure el tipo de tarjeta (CSN o Wiegand), el ID de la tarjeta y el nombre de la tarjeta. Seleccione un lector en **Escanear con el lector.**. Opcionalmente, escanee una tarjeta RFID física con el lector conectado.

Web



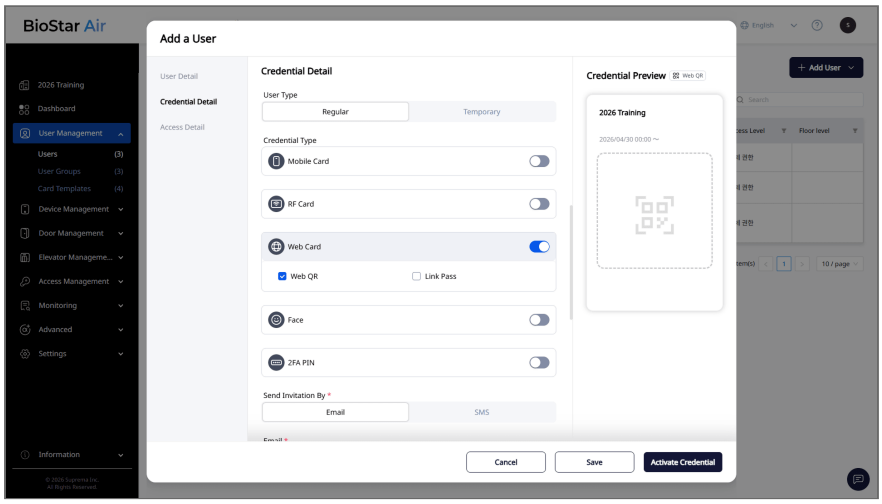


Mobile

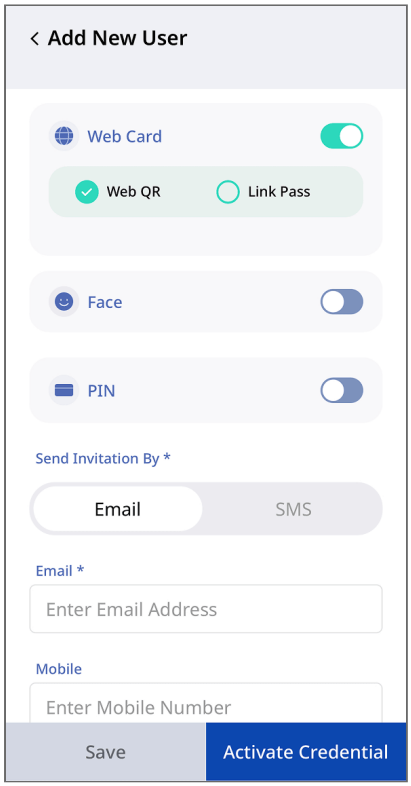


- **Tarjeta Web**: Utilice **Web QR** o **Pase de enlace** como métodos de autenticación de acceso.

Web



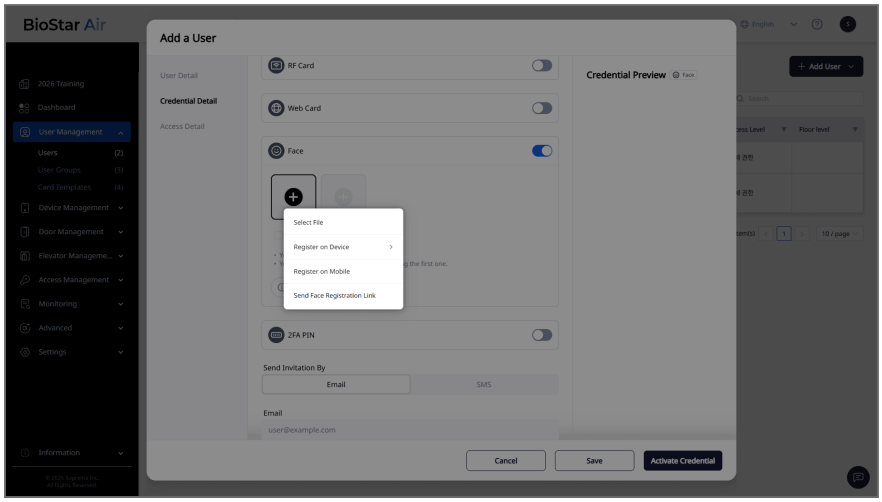
Mobile



> **Web QR** aparece solo después de habilitar **Lector QR** en **Ajustes** → **Sitio** → **Adicionales**.

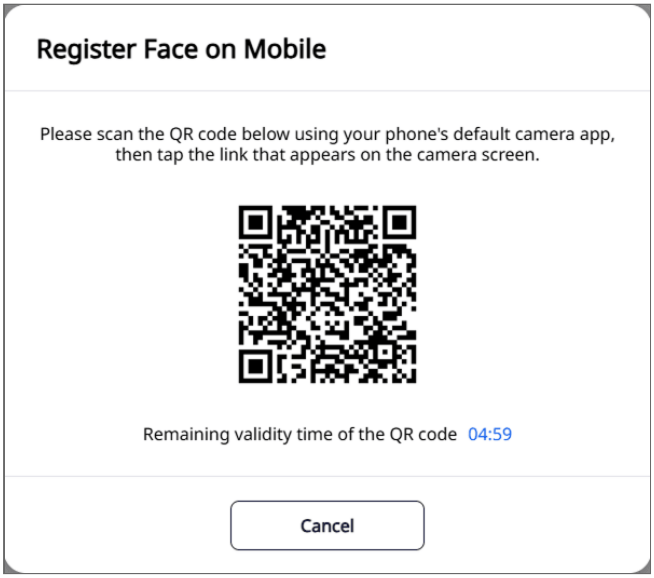
- **Rostro**: Agregue hasta dos imágenes de perfil para la Autenticación facial. Puede subir una imagen existente o inscribirla mediante un lector conectado. Alternativamente, envíe al usuario un enlace por correo electrónico o SMS para que inscriba su rostro directamente con la cámara de su dispositivo móvil.

Web



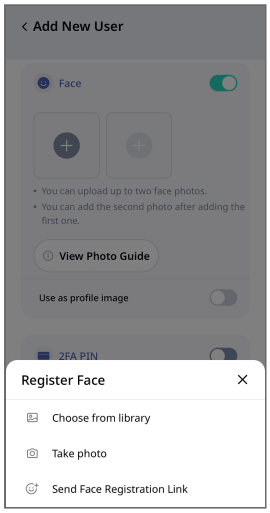
  - **Seleccionar Archivo**: Seleccione un archivo de imagen guardado localmente para subirlo.
  - **Registrar en el Dispositivo**: Utilice el lector conectado para registrar una imagen facial.

– **Registrarse en el Móvil**: Escanee un código QR con la cámara del dispositivo móvil para abrir un enlace y registrar una imagen facial.



– **Enviar Enlace de Registro Facial**: Envíe al usuario un enlace por correo electrónico o SMS para que inscriba su rostro directamente con la cámara de su dispositivo móvil.

Mobile



Toque + para agregar una foto de rostro. Elija cómo agregarla desde el menú que aparece en la parte inferior.

– **Seleccionar de la biblioteca**: Seleccione un archivo de imagen guardado en su dispositivo móvil para subirlo.

– **Tomar foto**: Utilice la cámara de su dispositivo móvil para tomar una foto y subirla.

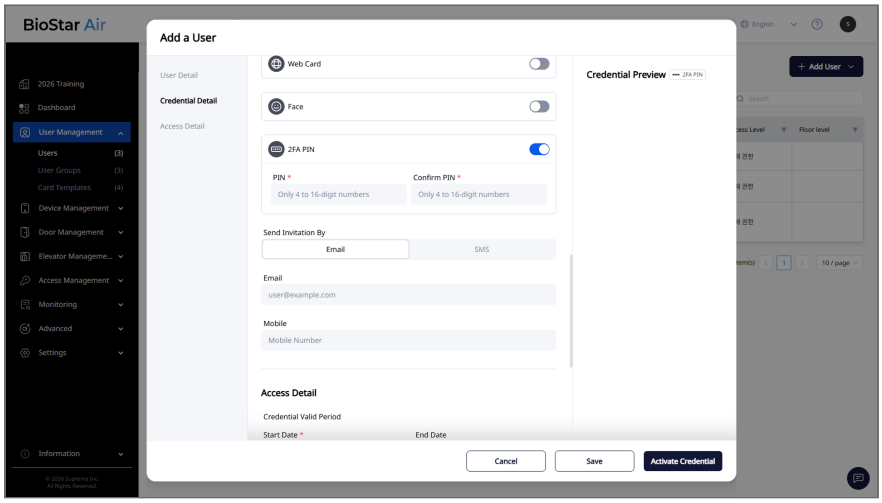
– **Enviar Enlace de Registro Facial**: Enviar al usuario por correo electrónico un enlace de inscripción facial para que pueda inscribir su rostro directamente con la cámara de su dispositivo móvil.

– **Usar como imagen de perfil**: Puede usar la imagen actualmente configurada como foto de perfil para su credencial facial.

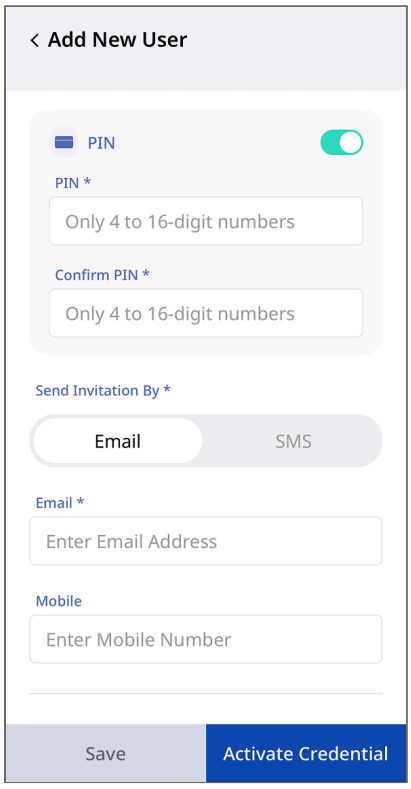
> Para obtener más información sobre cómo registrar una foto de rostro, consulte **Ver Guía de Fotos**.

• **2FA PIN**: Establezca un PIN de 4 a 16 dígitos para usar como parte de la autenticación de dos factores (2FA).

Web



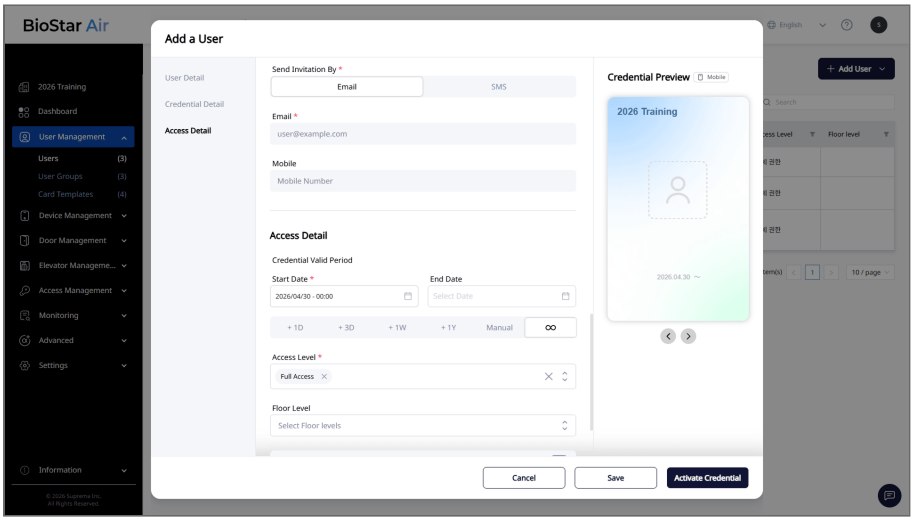
Mobile



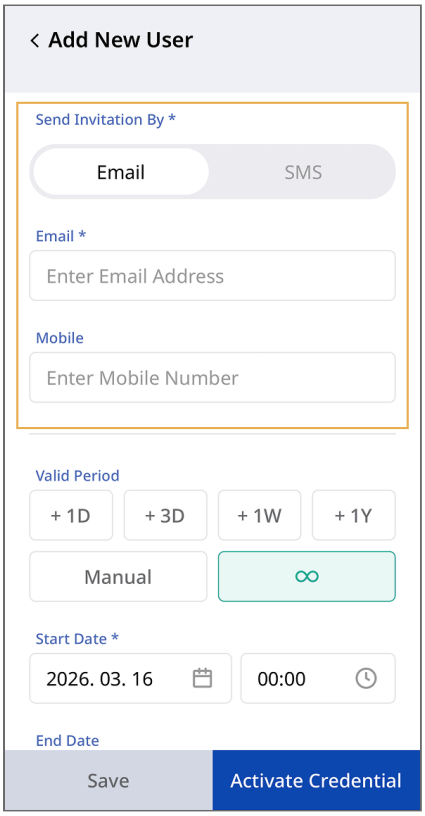
Enviar enlace de invitación

Envíe por correo electrónico el enlace de descarga de la aplicación Suprema Pass a los usuarios que utilizan **Tarjeta Móvil** o **Tarjeta Web**. Ingrese la dirección de correo electrónico (obligatoria) y el número de teléfono (opcional).

Web



Mobile

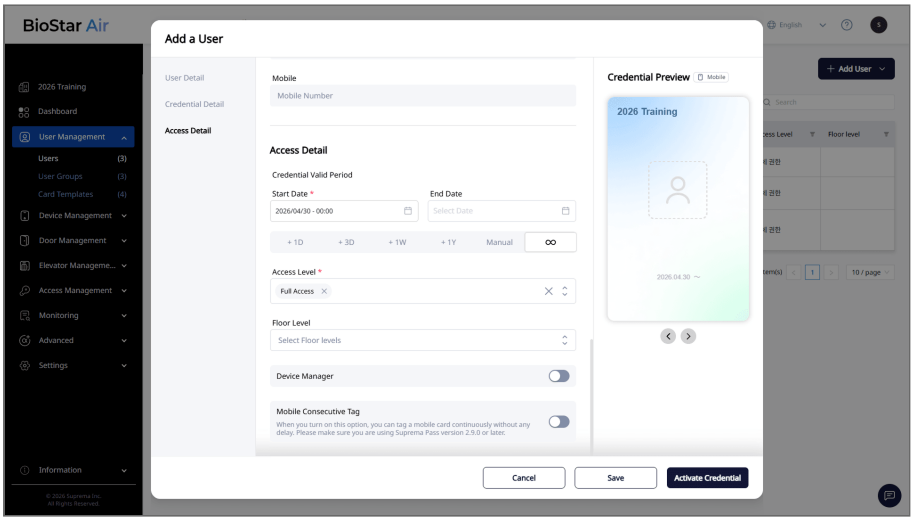


> **Información**
>
> Solicite la recarga de crédito SMS en **Ajustes** → **Centro de crédito** para usar la opción **Correo electrónico**.

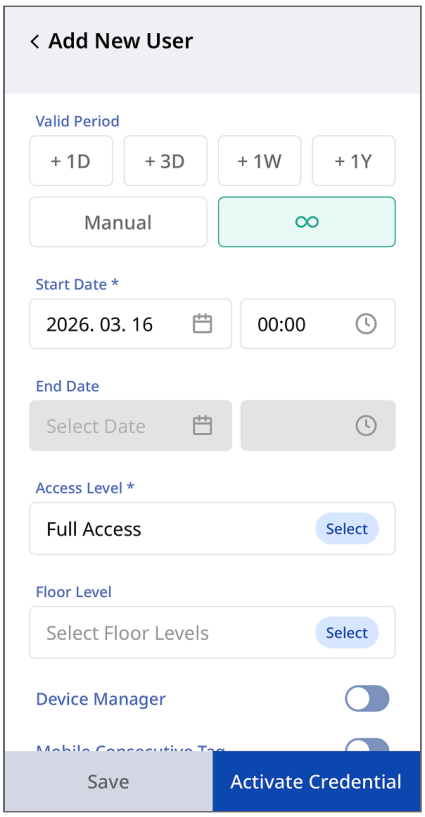
Establecer niveles de acceso y vigencia

Después de seleccionar las credenciales, configure el período de vigencia de las credenciales, los niveles de acceso y los niveles de planta en la sección **Detalles de acceso**.

Web



Mobile



- **Período de validez de la credencial**: Establezca el período de vigencia de las credenciales emitidas al usuario. Haga clic en ∞ para dejar la fecha de expiración sin límite.
- **Nivel de acceso**: Seleccione los niveles de acceso para el usuario. Otorgue acceso total o elija un nivel de acceso predefinido.
- **Nivel del suelo**: Seleccione los niveles de planta a los que el usuario puede acceder.
- **Gerenciador de Dispositivos**: Permita que un usuario administre los permisos de acceso en un lector específico.
- **Etiqueta móvil consecutiva**: Permite lecturas consecutivas de tarjetas móviles sin tiempo de espera. Esta función está disponible en la aplicación Suprema Pass versión 2.9.0 o superior.

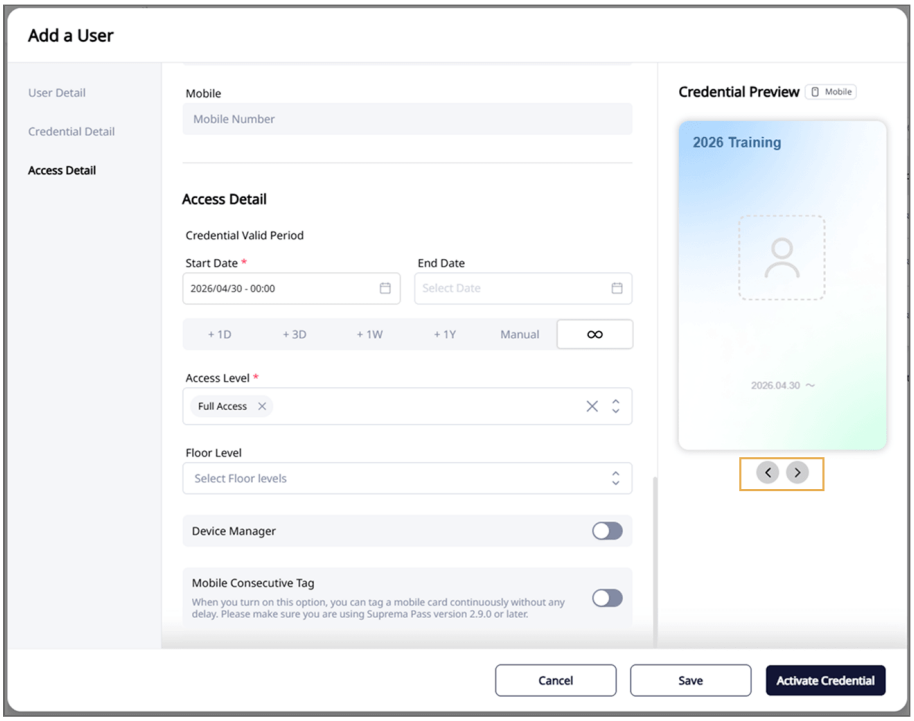
Información

- Para obtener más información sobre la configuración de niveles de planta, consulte Gestionar Niveles de Piso.
- La opción **Gerenciador de Dispositivos** está disponible solo para usuarios de BioStation 3 y X-Station 2. Los usuarios designados como administradores de dispositivo pueden acceder al menú de administrador en los dispositivos BioStation 3 y X-Station 2.

Seleccionar plantilla de tarjeta

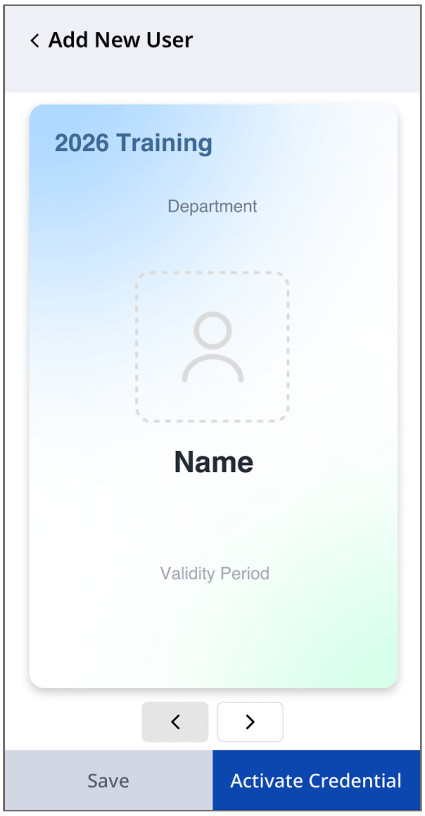
Web

Haga clic en ‹ o › debajo de Plantilla de tarjeta en el panel derecho para cambiar el diseño.



Mobile

Seleccione la pestaña ‹ o › en **Vista previa de credenciales** para cambiar el diseño de la plantilla de tarjeta.



Información

Para obtener más información sobre cómo crear nuevas plantillas de tarjeta, consulte Administrar plantillas de tarjeta.

Guardar o activar al usuario

Después de configurar todos los ajustes del usuario, elija una de las siguientes opciones.

- Haga clic en **Guardar** para guardar al usuario para su activación posterior.
- Haga clic en **Activar Credencial** para emitir y activar las credenciales de inmediato.

Siguiente paso

Una vez que haya aprendido a agregar usuarios uno por uno, aprenda a registrar varios usuarios a la vez.

Administrar Usuarios
La lista de usuarios es una herramienta esencial para los administradores encargados del control de acceso en una organización. Permite realizar todas las tareas de gestión de usuarios, incluida la administración organizacional mediante la agrupación de usuarios, la respuesta inmediata a empleados nuevos o que se marchan con activación/suspensión en tiempo real, la gestión integrada de distintos tipos de credenciales, el refuerzo de la seguridad mediante el control de su vigencia y la preparación de informes y auditorías mediante el filtrado y la generación de reportes.

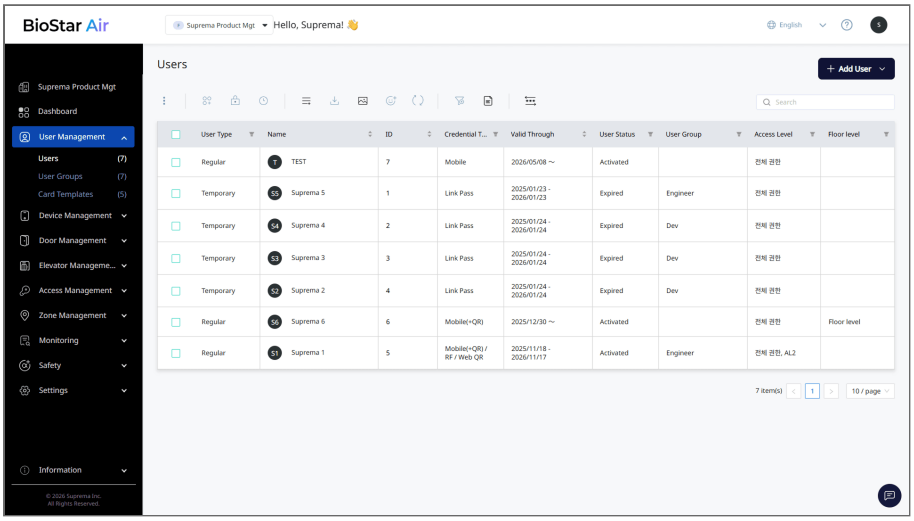
Ver la lista de usuarios

La lista de usuarios muestra de un vistazo todos los usuarios registrados en BioStar Air. Vea los detalles de cada usuario y

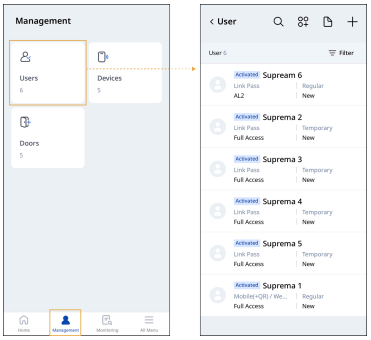
utilice las funciones de filtro y ordenamiento para encontrar rápidamente usuarios específicos. Edite, elimine y asigne grupos a los usuarios directamente desde la lista.

Web

Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.



Mobile



Use la función de gestión de usuarios en la app de BioStar Air.

1. Abre **BioStar Air** en tu dispositivo móvil.
2. Toque **Administrar** en la barra de navegación inferior.
3. Toque **Usuarios**.

Aparece una lista de usuarios. Agregue nuevos usuarios o edite los detalles de los usuarios existentes.

Información del usuario

La tabla de la lista de usuarios muestra la siguiente información.

- **Tipo de Usuario**: Indica si el usuario es regular o temporal. Para obtener más información sobre usuarios regulares y temporales, consulte Tipos de tarjetas y credenciales de usuario.
- **Nombre**: El nombre del usuario.
- **ID**: El identificador único del usuario.
- **Tipo de Credencial**: Muestra las credenciales emitidas al usuario. Para obtener más información sobre los tipos de credenciales, consulte Tipos de tarjetas y credenciales de usuario.
- **Válido hasta el**: El período de vigencia de las credenciales emitidas al usuario.
- **Estatus de usuario**: Indica si el usuario está activo o inactivo.
- **Grupo de usuario**: El grupo al que pertenece el usuario. Para obtener más información sobre grupos de usuarios, consulte Administrar Grupos de Usuarios.
- **Nivel de acceso**: El nivel de acceso asignado al usuario. Para obtener más información sobre niveles de acceso,

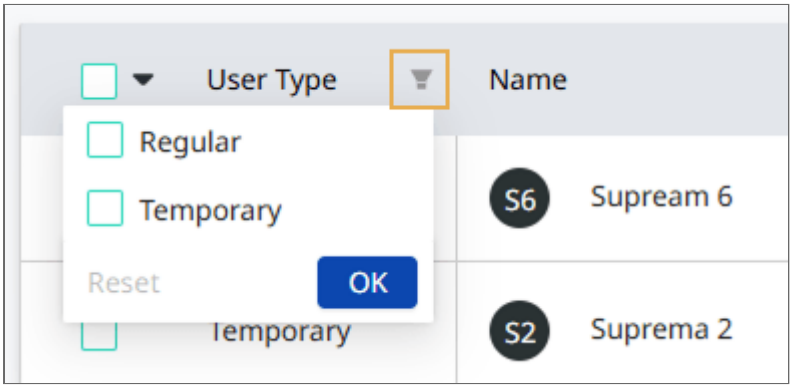
consulte Administrar Niveles de Acceso.

- **Nivel del suelo**: Los permisos del usuario para los pisos a los que puede acceder. Para obtener más información sobre niveles de piso, consulte Gestionar Niveles de Piso.

Filtrar

Web

Use la función de filtrado en la parte superior de la lista de usuarios. Haga clic en en el encabezado para establecer las condiciones deseadas.

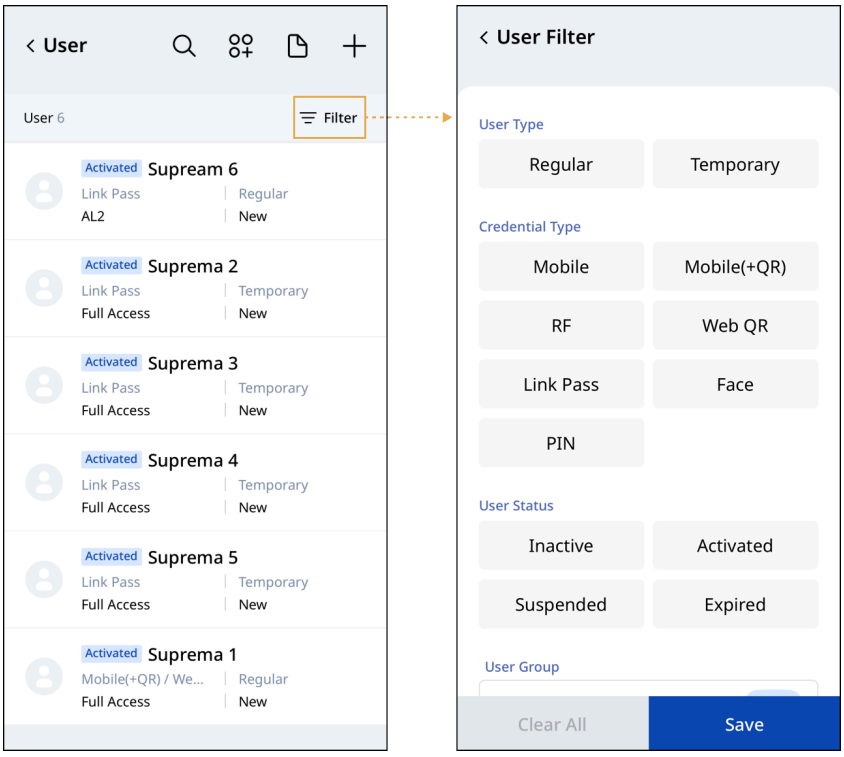


Información

Haga clic en en la parte superior de la lista de usuarios para restablecer las condiciones de filtro aplicadas.

Mobile

En la app móvil, puede filtrar y ver a los usuarios en la lista según los criterios deseados. Toque **Filtros** en la esquina superior derecha de la lista de usuarios. Puede filtrar usuarios por los siguientes criterios.

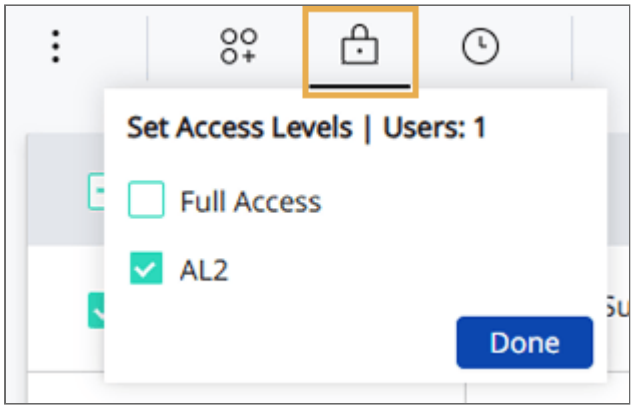


- **Tipo de Usuario**: Filtra por tipo de usuario (regular o temporal).
- **Tipo de Credencial**: Filtra por tipo de credencial.
- **Estatus de usuario**: Filtra por estado de activación.
- **Grupo de usuario**: Filtra por grupo de usuarios.

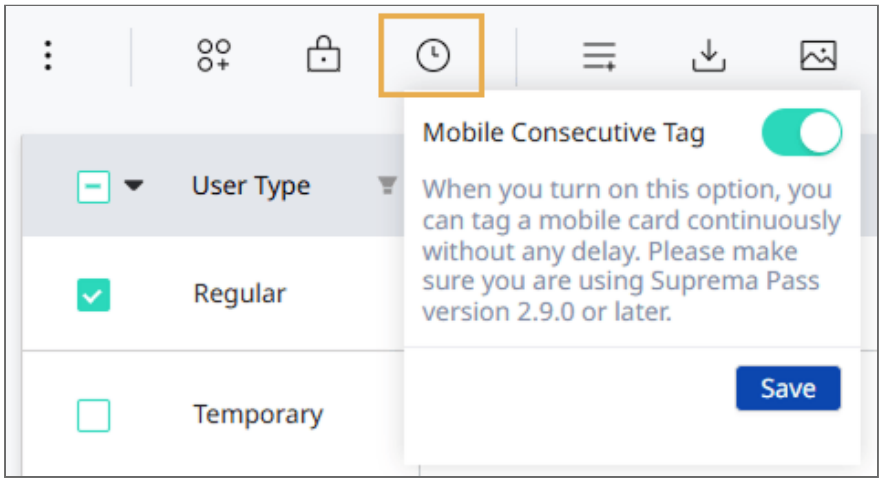
Funciones adicionales

Las funciones disponibles en la parte superior de la lista de usuarios son las siguientes.

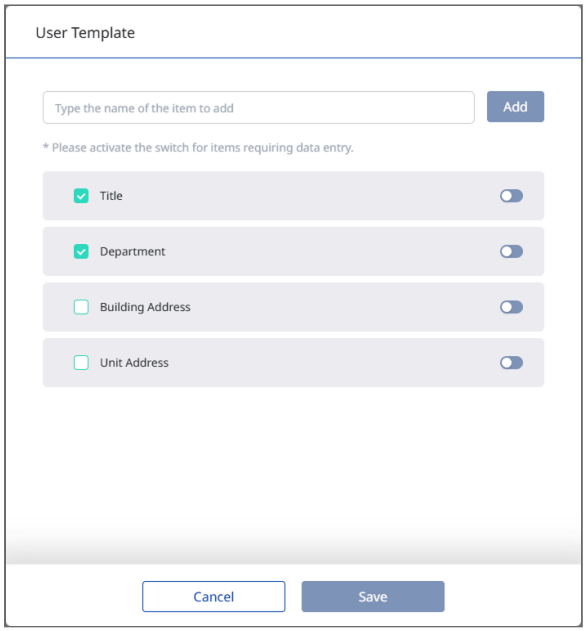
- : Asignar, quitar o mover a los usuarios seleccionados a un grupo. Para más información, consulte Administrar grupos de usuarios.
- : Cambiar el nivel de acceso de los usuarios seleccionados. Para más información sobre los niveles de acceso, consulte Administrar Niveles de Acceso.



- : Permite que los usuarios seleccionados marquen tarjetas móviles de forma consecutiva sin tiempo de espera. La app Suprema Pass admite esto a partir de la versión 2.9.0.



- : Aplica una plantilla de usuario a los usuarios seleccionados. Añade cualquier otra información necesaria además de la información predeterminada del usuario.



- : Exporta la información de los usuarios seleccionados a un archivo PDF o CSV.
- : Sube imágenes de usuarios en lote. El nombre de cada archivo de imagen que se suba debe coincidir con el ID del usuario.

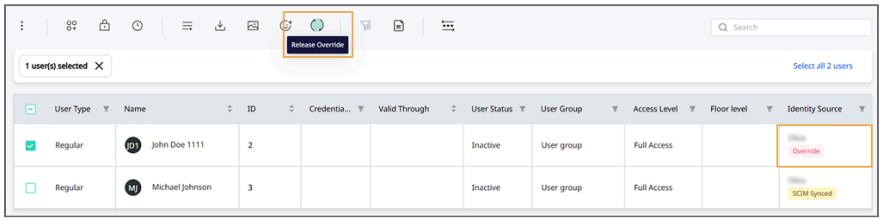
  Por ejemplo, el archivo 601.jpg corresponde al usuario con ID 601.

  > **Requisitos de formato de archivo**
  > – Formatos compatibles: *.jpg*, *.jpeg*, *.png*
  > – Límite de tamaño de archivo: **1 MB** por imagen

- : Envía un enlace de registro facial a los usuarios seleccionados por correo electrónico o mensaje de texto. Cuando un usuario haga clic en el enlace y registre su rostro en la página web, se le otorgará acceso mediante autenticación facial.

  > El enlace no puede enviarse a usuarios que no tengan una dirección de correo electrónico o número de teléfono registrado.

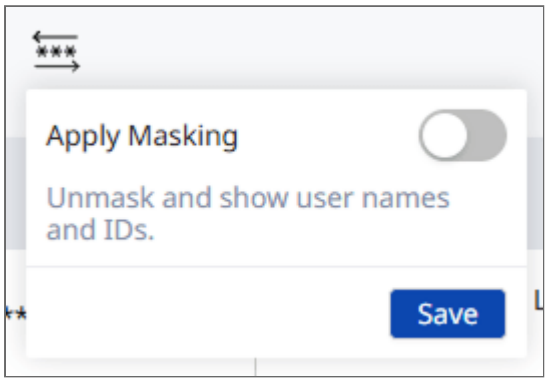
- : Si cambia manualmente la información local de usuarios sincronizados con SCIM, el estado cambia a **Anulación**. Cancele los cambios locales para volver al estado administrado por SCIM. Para más información, consulte Configurar SSO Y SCIM.



- : Restablece todos los filtros aplicados a la lista de usuarios. Esta opción está disponible solo cuando se han aplicado filtros. Para obtener más información sobre cómo aplicar filtros, consulte Filtrar.
- : Configura los informes de usuarios. Una vez generado, el informe se envía al correo electrónico del administrador.

Para más información sobre la configuración de informes, consulte Crear un informe de usuario.

- : Enmascara (***) información como el nombre y el ID en la lista de usuarios para proteger la privacidad. Esta función es útil en entornos que requieren privacidad. Active el interruptor para habilitarla y haga clic en **Guardar**.

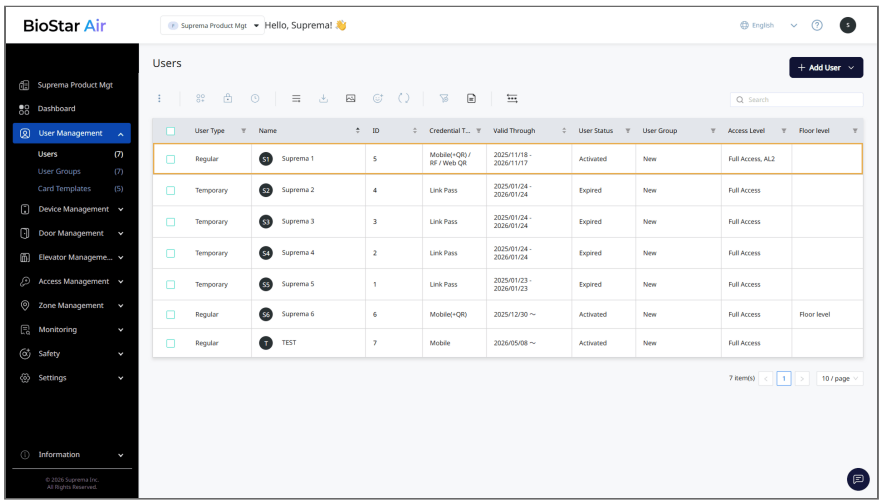


Editar información del usuario

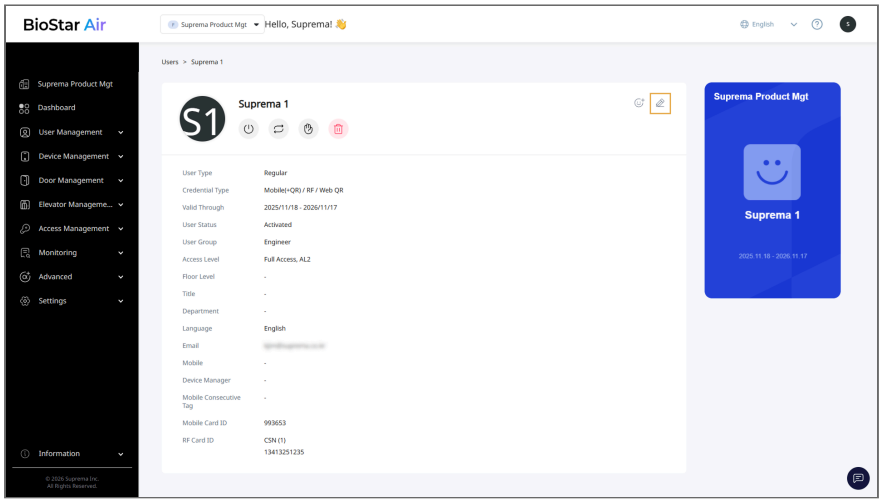
Web

Siga estos pasos para editar los datos de un usuario o cambiar sus credenciales.

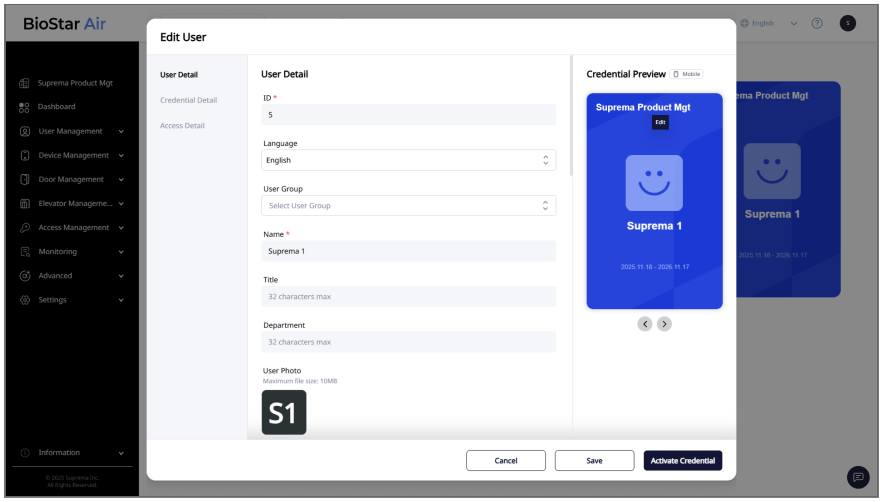
1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en el usuario que desea editar en la lista.



3. Haga clic en en la esquina superior derecha de los detalles del usuario.

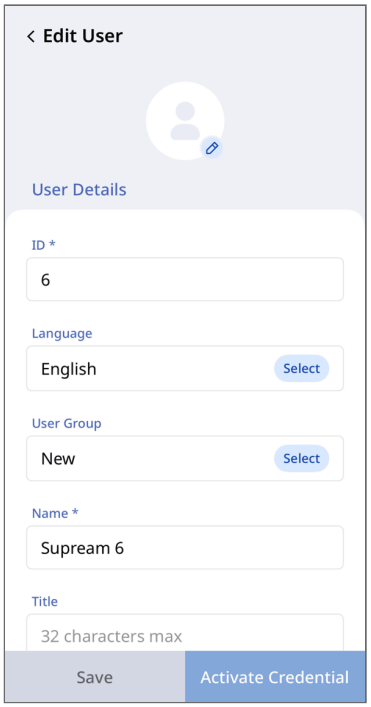


4. Edite los datos requeridos cuando aparezca la ventana **Editar usuario**.



5. Después de editar, haga clic en **Guardar** en la esquina inferior derecha.

Mobile



Para editar la información detallada de un usuario en la aplicación móvil, siga estos pasos.

1. Toque el usuario que desea editar en la lista de usuarios.
2. Toque ✎ en la esquina superior derecha.
3. Edite la información necesaria en la pantalla **Editar usuario**.
4. Para guardar los cambios, toque **Guardar**.

   Utilice **Activar Credencial** para emitir credenciales.

> **Información**
>
> Para obtener más información sobre los usuarios, consulte Agregar usuarios.

Administrar grupos de usuarios

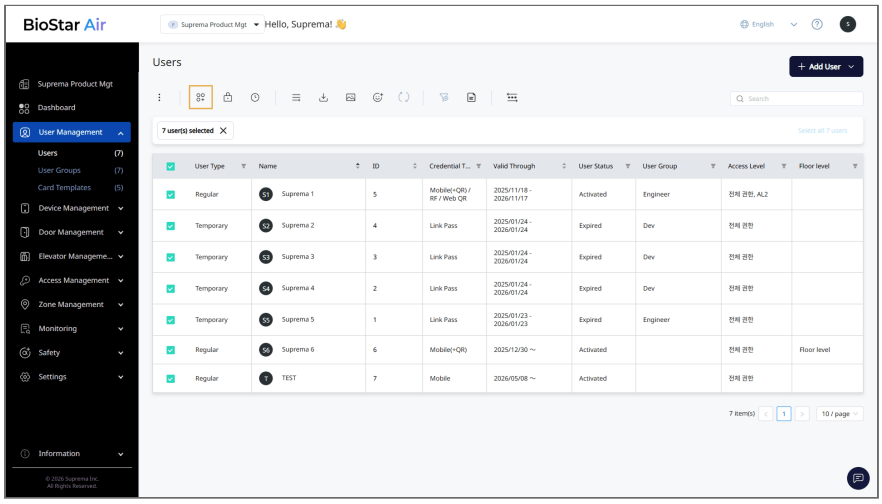
Esta guía explica cómo asignar, mover o excluir usuarios de un grupo de usuarios. Para obtener más información sobre la creación y administración de grupos de usuarios, consulte Administrar Grupos de Usuarios.

Web

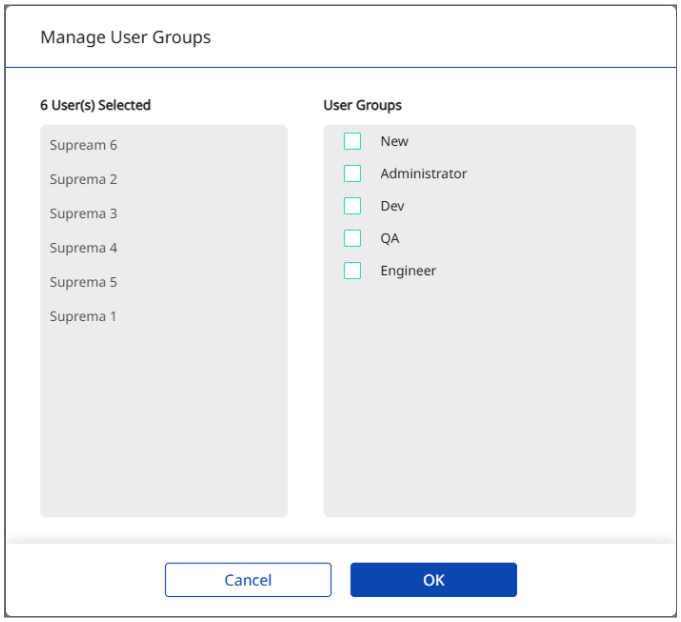
Asignar usuarios a un grupo

Después de crear un grupo de usuarios, puede agregar usuarios al grupo desde la lista de usuarios.

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en la casilla junto a los usuarios que desea asignar al grupo en la lista de usuarios.
3. Haga clic en en la parte superior izquierda de la lista de usuarios.

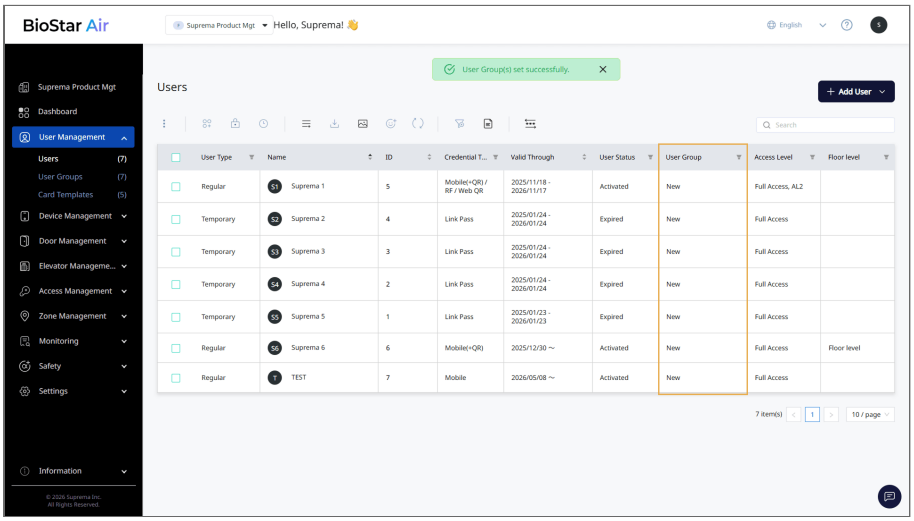


4. Cuando aparezca la ventana **Administrar grupos de usuarios**, seleccione el grupo principal o el subgrupo al que asignar los usuarios.



5. Complete la selección y, para guardar la configuración del grupo, haga clic en **OK**.

Confirme que los usuarios están asignados al nuevo grupo en la columna **Grupo de usuario** de la lista de usuarios.



Regrese a **Grupos de Usuarios** para confirmar que la columna **Usuarios totales** del grupo se actualizó.

Eliminar o mover un grupo

Puede excluir usuarios de un grupo de usuarios o moverlos a otro grupo.

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en la casilla junto a los usuarios que desea quitar de un grupo o mover entre grupos en la lista de usuarios.

> Al mover usuarios, primero seleccione usuarios del mismo grupo y luego continúe.

3. Haga clic en en la parte superior izquierda de la lista de usuarios.
4. Cuando aparezca la ventana **Administrar grupos de usuarios**, realice una de las siguientes acciones:
   - Para desasignar el grupo, desmarque la casilla del grupo seleccionado.

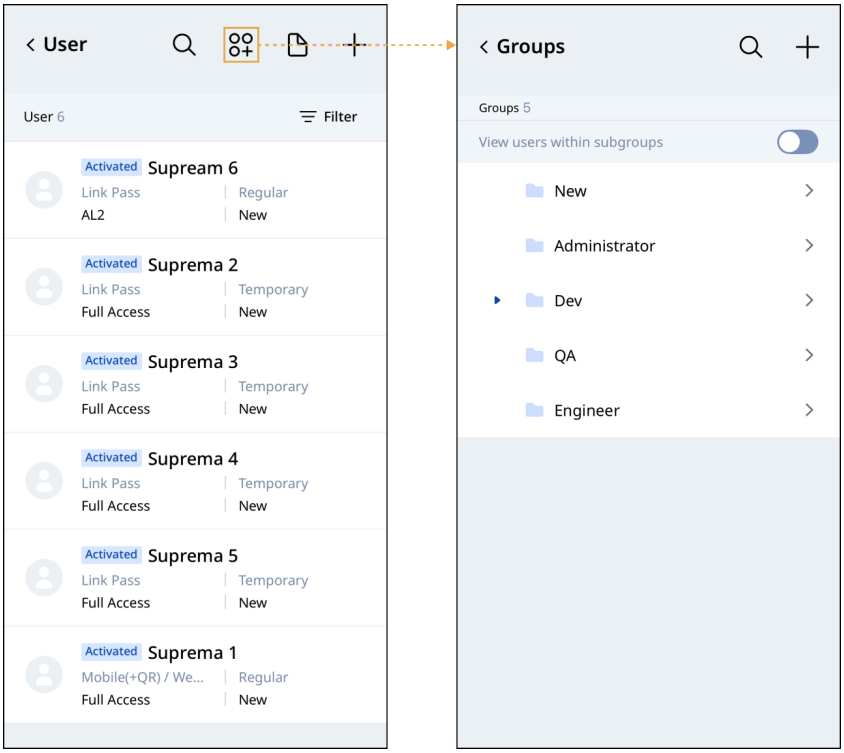
- Para mover el grupo, seleccione la casilla del grupo actual y luego elija el grupo de destino.

5. Haga clic en **OK** para guardar la configuración del grupo.

Confirme los cambios del grupo en la columna **Grupo de usuario** de la lista de usuarios.

Mobile

Puedes administrar los grupos de usuarios en la aplicación móvil. Toca en la parte superior de la lista de usuarios. Aparecerá la lista de grupos de usuarios.



- Para ver los usuarios de un grupo, toca > a la derecha del grupo deseado.
- Para agregar un nuevo grupo, toca + en la esquina superior derecha.
- Para editar el nombre de un grupo, mantén presionado el grupo deseado y toca en la parte inferior.
- Para eliminar un grupo, mantén presionado el grupo deseado y toca en la parte inferior. Selecciona uno o más grupos para eliminarlos.

> **Información**
>
> Para obtener más información sobre la gestión de grupos de usuarios, consulta Administrar Grupos de Usuarios.

Administrar el estado del usuario

Activa o suspende los permisos de acceso de un usuario. También vuelve a emitir las credenciales.

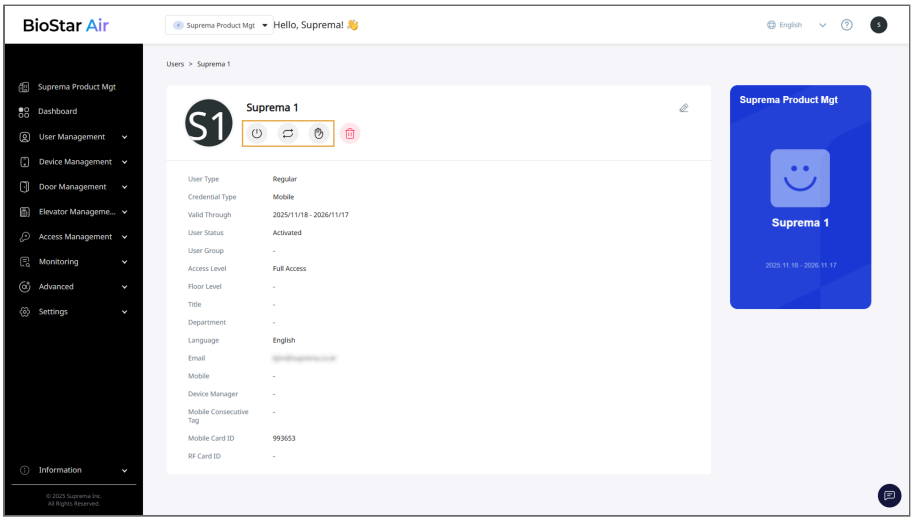
Información

Cuando un administrador reemite las credenciales de un usuario en BioStar Air, las credenciales móviles previamente emitidas y los códigos QR y LinkPasses son revocados y reemplazados. El usuario recibirá un correo electrónico o SMS, dependiendo de la configuración del sitio, que contenga un enlace a las credenciales actualizadas. El usuario debe seguir el enlace para descargar la nueva credencial móvil en la aplicación Suprema Pass o acceder al nuevo código QR o LinkPass. Los intentos de acceso usando credenciales móviles revocadas, códigos QR o LinkPasses fallarán.

Usuario individual

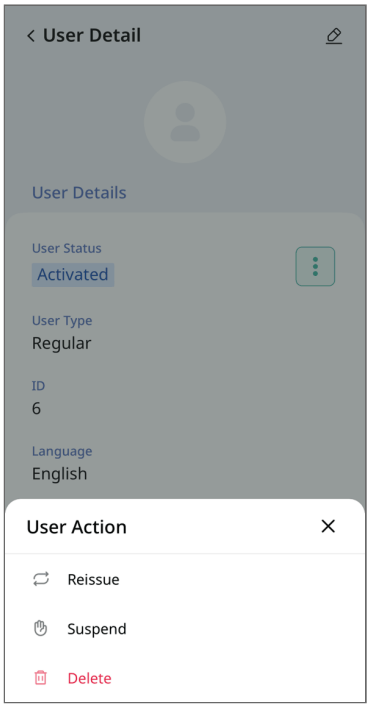
Web

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en el usuario de la lista para cambiar su estado.
3. Seleccione la acción deseada en la parte superior de los detalles del usuario.



- : Activa los permisos de acceso del usuario. Usa esta función para la activación inicial de nuevos usuarios o para reactivar a usuarios suspendidos.
- : Vuelve a emitir las credenciales. Usa esta función cuando las credenciales del usuario hayan expirado o no estén disponibles.
- : Bloquea el acceso del usuario. Usa esta función cuando el usuario esté activo.

Mobile



En la aplicación móvil, toca un usuario en la lista. En la pantalla **Detalles del usuario**, toca ⋮. Aparece el menú **Acciones de usuario**.

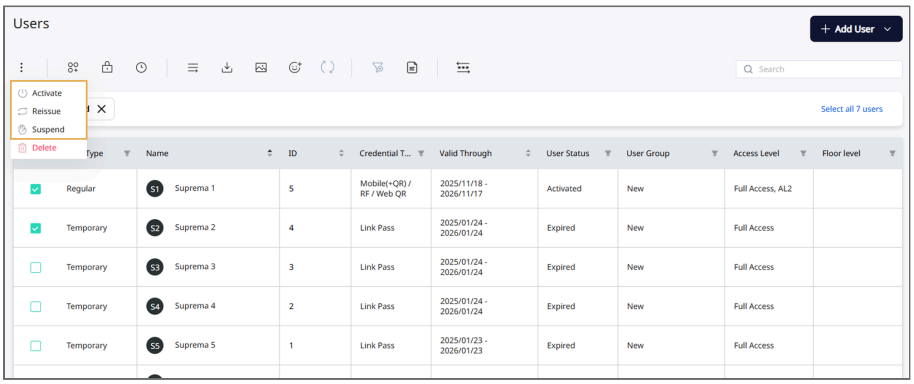
- **Activar** / **Reactivar**: Activa los permisos de acceso del usuario. Usa esta función para la activación inicial de usuarios nuevos o para reactivar a usuarios suspendidos.
- **Reedición**: Vuelve a emitir las credenciales del usuario.
- **Suspender**: Desactiva temporalmente al usuario. Los usuarios suspendidos no pueden acceder.
- **Borrar**: Elimina al usuario del sistema.

> **Información**
>
> La opción **Reactivar** aparece solo para usuarios suspendidos.

Acciones masivas

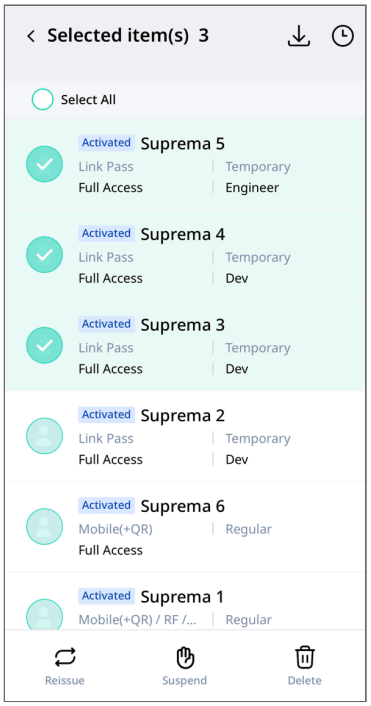
Web

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en la casilla de cada usuario en la lista para cambiar su estado. Puede seleccionar más de un usuario.
3. Toca ⋮ en la esquina superior izquierda de la pantalla y selecciona la acción deseada del menú emergente.



- **Activar** / **Reactivar**: Activa los permisos de acceso del usuario. Usa esta función para la activación inicial de usuarios nuevos o para reactivar a usuarios suspendidos.
- **Reedición**: Vuelve a emitir las credenciales. Usa esta función cuando las credenciales del usuario hayan expirado o no estén disponibles.
- **Suspender**: Bloquea el acceso del usuario. Usa esta función cuando el usuario esté activo.

Mobile



En la aplicación móvil, mantenga presionado a un usuario en la lista para cambiar su estado. Seleccione los usuarios adicionales cuyo estado desee cambiar. Toque la acción deseada en el menú **Acciones de usuario** en la parte inferior de la pantalla.

- **Activar** / **Reactivar**: Activa los permisos de acceso del usuario. Usa esta función para la activación inicial de usuarios nuevos o para reactivar a usuarios suspendidos.
- **Reedición**: Vuelve a emitir las credenciales del usuario.
- **Suspender**: Desactiva temporalmente al usuario. Los usuarios suspendidos no pueden acceder.
- **Borrar**: Elimina al usuario del sistema.

> **Información**
> La opción **Reactivar** aparece solo para usuarios suspendidos.

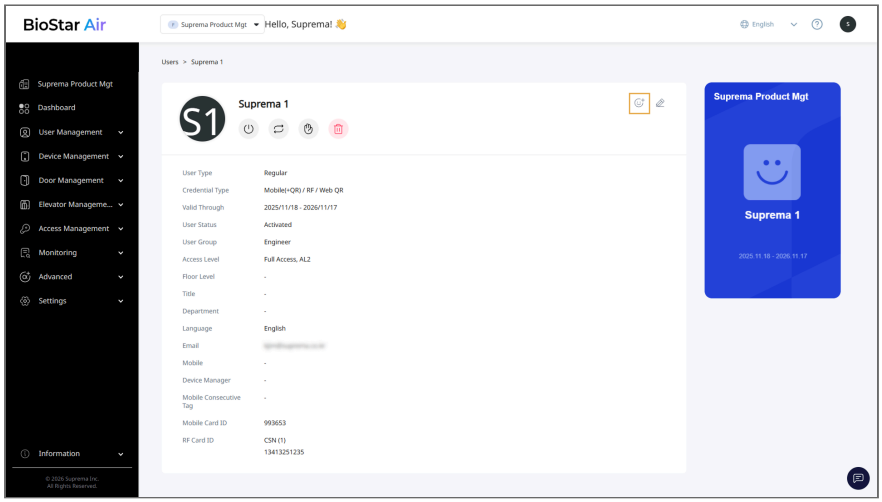
Enviar enlace de inscripción facial

Envía un enlace de inscripción facial a los usuarios existentes por correo electrónico o mensaje de texto para guiarlos a inscribir su rostro. Cuando un usuario hace clic en el enlace e inscribe su rostro en la página web, obtiene acceso mediante Autenticación facial.

> **Información**
> El enlace no puede enviarse a usuarios que no tengan una dirección de correo electrónico o número de teléfono registrado.

Usuario individual

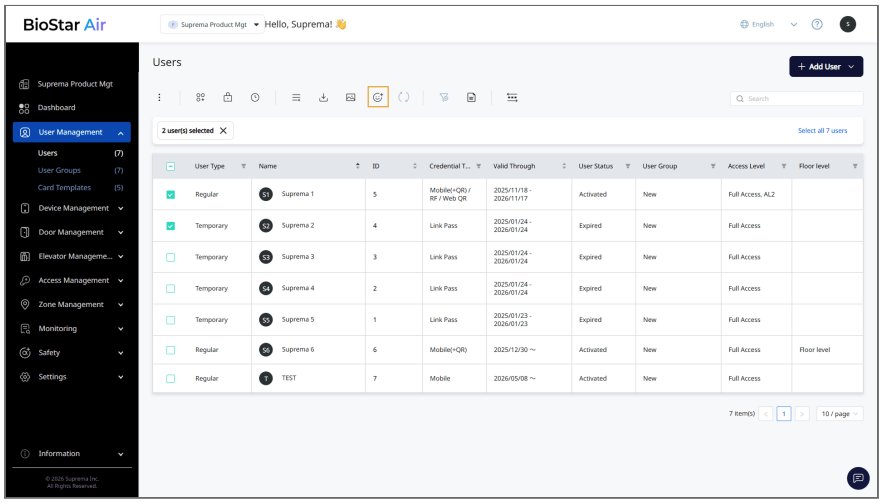
1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en el usuario de la lista para enviar el enlace de inscripción facial.
3. Haga clic en el botón en la esquina superior derecha de los detalles del usuario.



4. Cuando aparezca un mensaje emergente, haga clic en el botón **Sí**.

Acciones masivas

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Seleccione las casillas de los usuarios en la lista para enviar el enlace de inscripción facial. Puede seleccionar más de un usuario.
3. Haga clic en el botón en la parte superior izquierda de la pantalla.



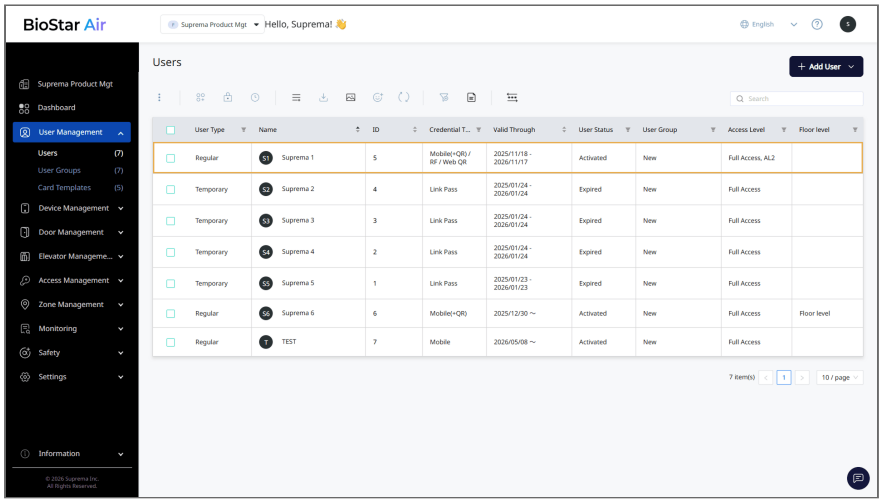
4. Cuando aparezca un mensaje emergente, haga clic en el botón **Sí**.

Eliminar usuarios

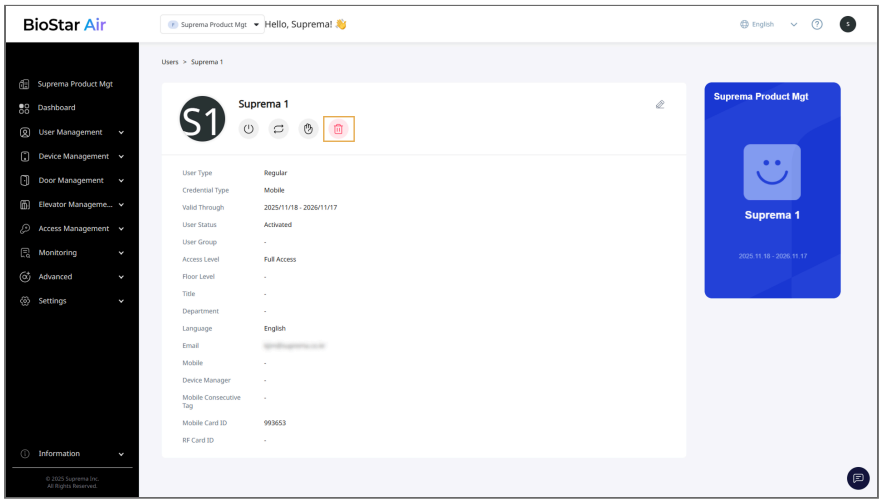
> **Precaución**
> Los usuarios eliminados no se pueden recuperar. Asegúrese de verificar antes de eliminarlos.

Usuario individual

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en el usuario que desea eliminar en la lista.



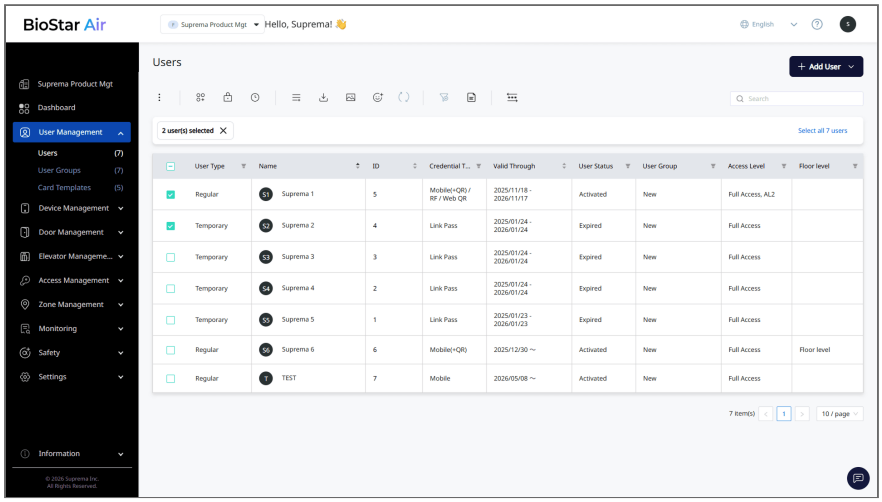
3. Haga clic en en los detalles del usuario.



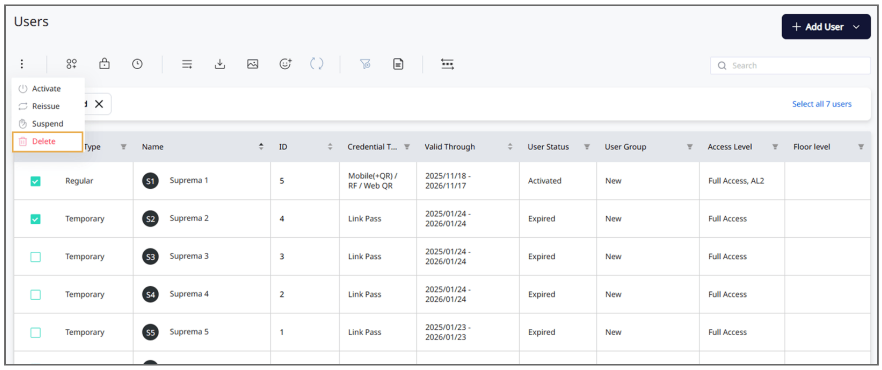
4. Cuando aparezca un mensaje de advertencia, haga clic en **Sí**.

Eliminar varios usuarios

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Marque la casilla de cada usuario que desea eliminar en la lista. Puede seleccionar más de un usuario.



3. Haga clic en ⋮ → **Borrar** en la esquina superior izquierda de la pantalla.

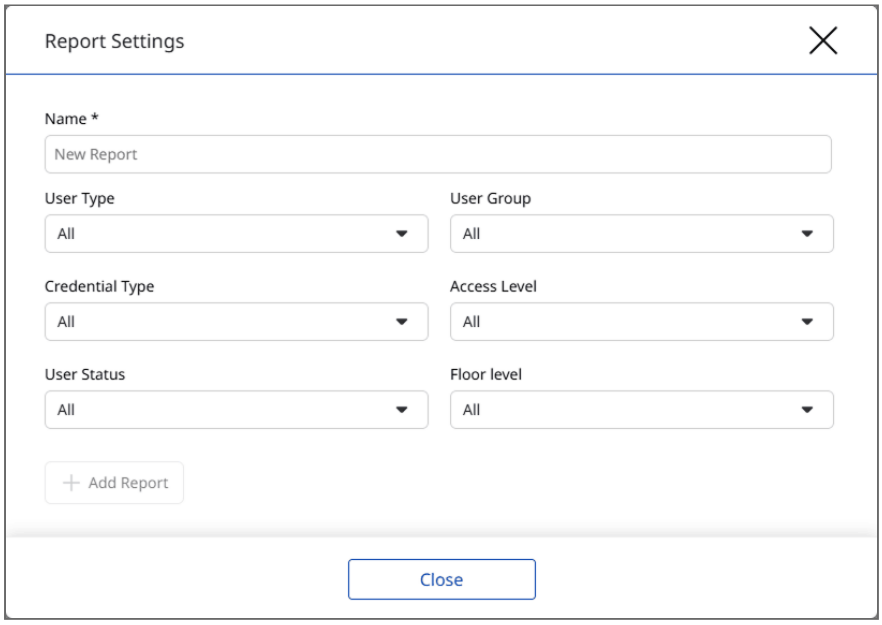


4. Cuando aparezca un mensaje de advertencia, haga clic en **Sí**.

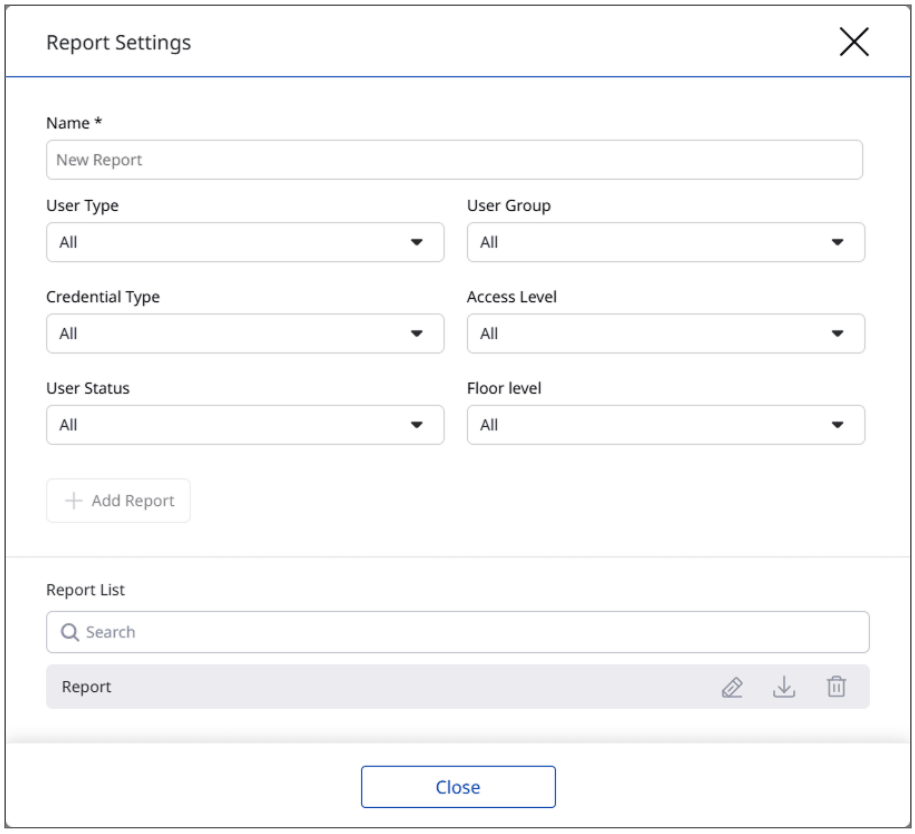
Crear un informe de usuario

Cree un informe de usuario y envíelo al correo electrónico del administrador.

1. Haga clic en en la parte superior de la lista de usuarios.
2. Cuando aparezca la ventana **Configuración de informes**, ingrese un nombre para el informe.



3. Seleccione los elementos que desea incluir en el informe en cada opción de filtro.
4. Haga clic en **Agregar informe** para guardar el informe.
5. Se crea un **Lista de informes** y se envía un enlace de descarga al correo electrónico del administrador.

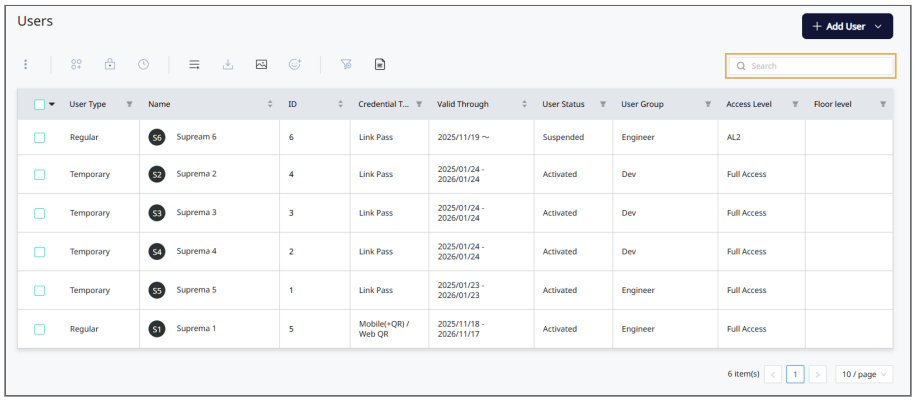


Información

En **Lista de informes**, busque, edite, descargue o elimine los informes generados.

Buscar usuarios

Utilice el campo de búsqueda en la esquina superior derecha de la lista de usuarios para encontrar rápidamente usuarios específicos. Busque por nombre de usuario, ID o número de teléfono.



Agregar usuarios masivamente

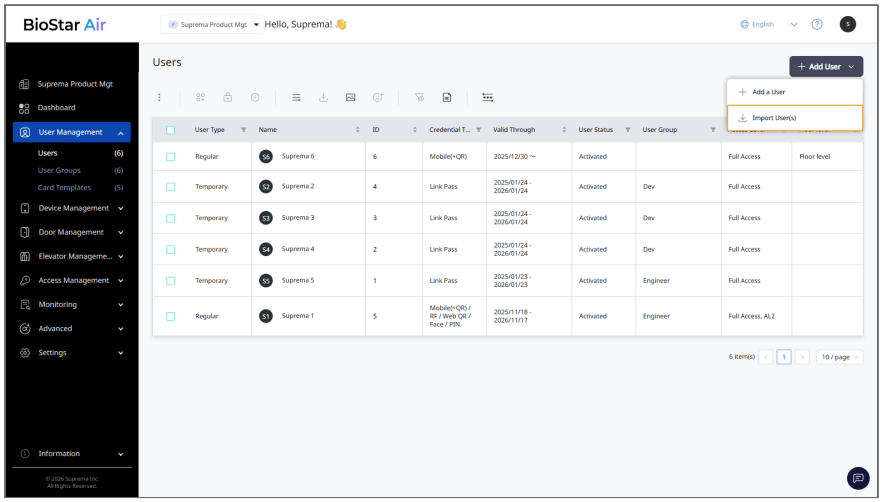
Si necesita agregar varios usuarios a la vez, utilice la función de importación masiva de usuarios de BioStar Air. Suba un archivo CSV para registrar decenas o cientos de empleados en solo minutos. También puede subir masivamente imágenes de perfil al introducir la información de los usuarios. Este documento ofrece instrucciones paso a paso para descargar la plantilla CSV, preparar el archivo, subirlo, gestionar las imágenes de perfil y verificar la información de los usuarios tras la importación.

> **Consejo**
>
> Consulte el siguiente video para obtener una guía paso a paso sobre cómo agregar varios usuarios de forma masiva.

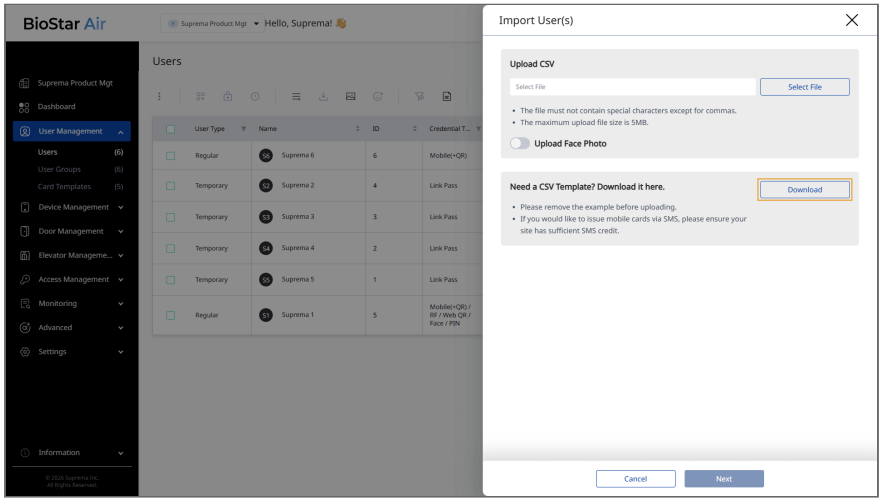
Descargar la plantilla CSV

Siga estos pasos para descargar la plantilla CSV.

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en **Añadir nuevo usuario** → **Importar usuarios** en la esquina superior derecha de la pantalla.



3. Cuando aparezca el panel **Importar usuarios**, haga clic en **Descargar**.



4. Guarde el archivo de plantilla CSV (*biostar-import-user-csv-example.csv*) localmente.

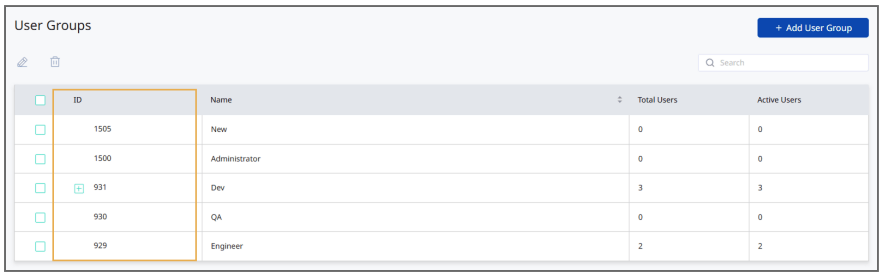
Preparar el archivo CSV

Descargue la plantilla CSV e ingrese los datos requeridos para cada usuario.

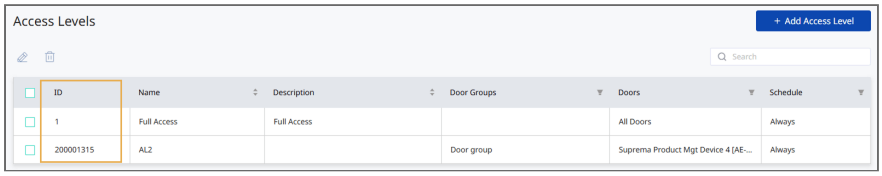
Campos clave

Los campos clave a ingresar son los siguientes.

- **ID do Grupo de usuários**: Verifique el ID del grupo en **Gestión de usuarios** → **Grupos de Usuarios**.



- **ID de Nivel de acceso**: Verifique el ID del nivel de acceso en **Gestión de Acceso** → **Niveles de acceso**. **Acceso completo** siempre está establecido en **1**. Use comas (`,`) como separadores para especificar varios niveles de acceso.



- **Correo electrónico**: Ingréselo si planea enviar invitaciones por correo electrónico.
- **Móvil**: Ingréselo si planea enviar invitaciones por SMS.

> **Precaución**
>
> **Correo electrónico** y **Móvil** no deben duplicarse. Subir un archivo CSV con valores duplicados puede provocar errores.

Compatibilidad con formatos Wiegand personalizados

Puede configurar libremente cualquier formato Wiegand, incluidos códigos de instalación, segmentos, bits de paridad y más.

- Se admiten los formatos HID Corporate 1000, iCLASS SE y Seos.
- **Plantilla CSV**
  - Cada formato definido (personalizado o predeterminado) aparece como una columna separada en el archivo CSV.

    > ***26 bit SIA Standard-H10301*, *HID 37 bit-H10302*, *HID 37 bit-H10304*, *HID Corporate 1000*, *HID Corporate 1000 48bit***

  - Separe varias entradas en un solo campo con una barra (`/`).
  - Use comillas simples (`'`) alrededor del nombre de la tarjeta. Evite usar comillas dobles (`"`); pueden provocar errores.

    > ✓ *'Nombre de la tarjeta'* | ✕ *"Nombre de la tarjeta"*

> **Ejemplo**
> - Con un código de instalación: *1234567-100-'Main Office Card'* (`CardID` - `FacilityCode` - `'CardName'`)
> - Con varios segmentos: *12-3456-78-'Lab Entry Card'*

Soporte para múltiples tarjetas

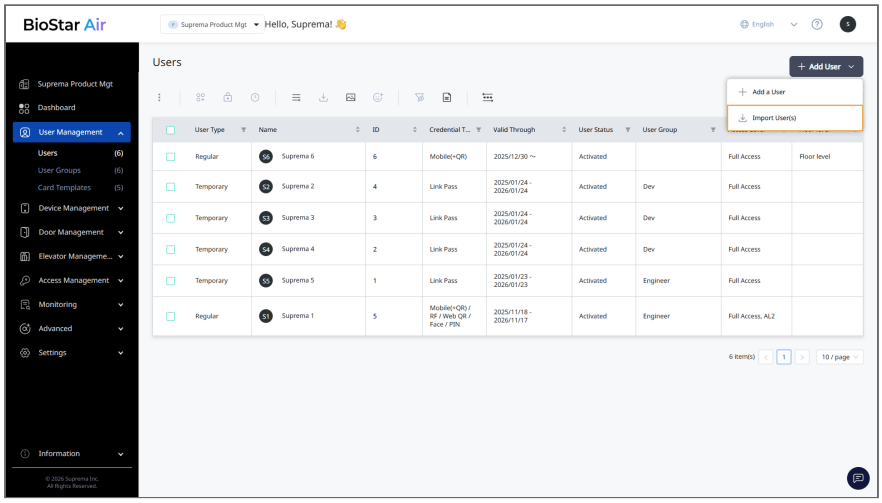
- Asigne hasta ocho formatos de tarjeta CSN o Wiegand por usuario.
- **Plantilla CSV**
  - Para una sola tarjeta, ingrese el número CSN.
  - Separe los números de tarjeta CSN con una barra (`/`) al registrar múltiples tarjetas.

> **Formato de nombre de tarjeta:** `CSN` - `'Card Name'`
>
> Ejemplo: *1234567-'Main Entry' / 7654321-'Back Door'*

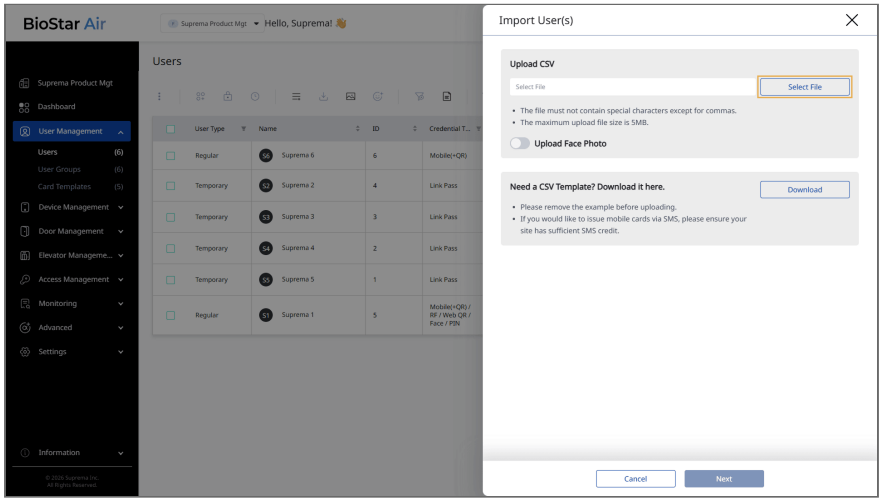
Subir el archivo CSV

Una vez preparado el archivo CSV, cárguelo.

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en **Añadir nuevo usuario** → **Importar usuarios** en la esquina superior derecha de la pantalla.



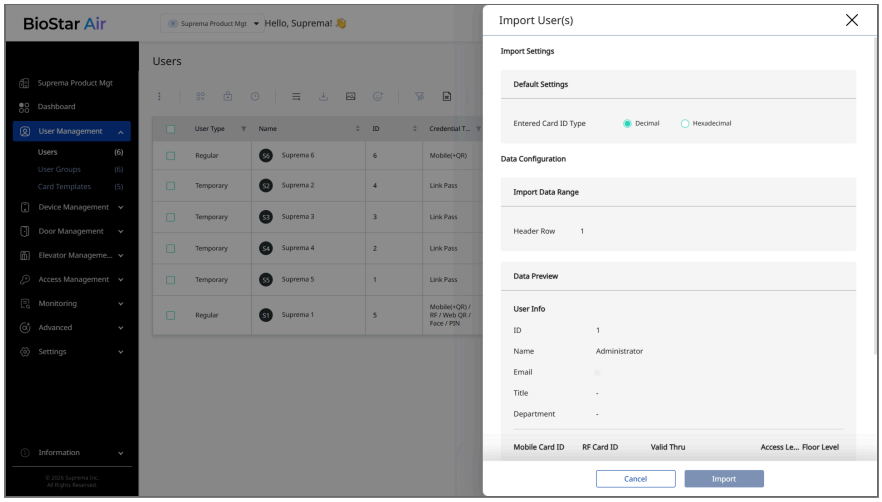
3. Cuando aparezca el panel **Importar usuarios**, haga clic en **Seleccionar Archivo**.



4. Seleccione el archivo CSV que preparó.

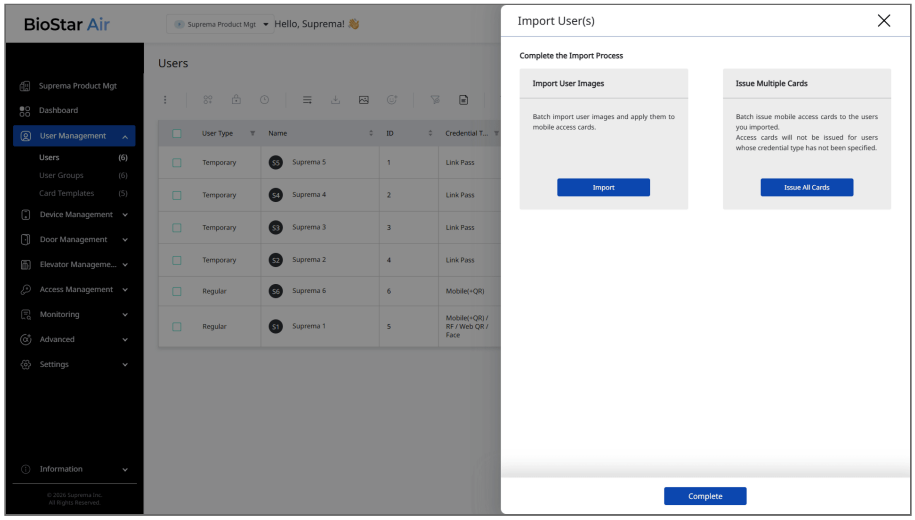
> Si las imágenes de perfil de los usuarios están listas, active la opción **Subir Foto de Rostro**. Para más información, consulte Subir imágenes de perfil de usuario.

5. Haga clic en **Siguiente** en la esquina inferior derecha de la pantalla.
6. En la sección **Vista previa de datos**, revise la precisión de los datos en la primera columna.



7. Si no hay problemas, haga clic en **Importar** en la esquina inferior derecha.

Después de que finalice la carga, podrá importar imágenes de usuarios o emitir tarjetas móviles en lote en la siguiente pantalla. Seleccione la acción deseada.



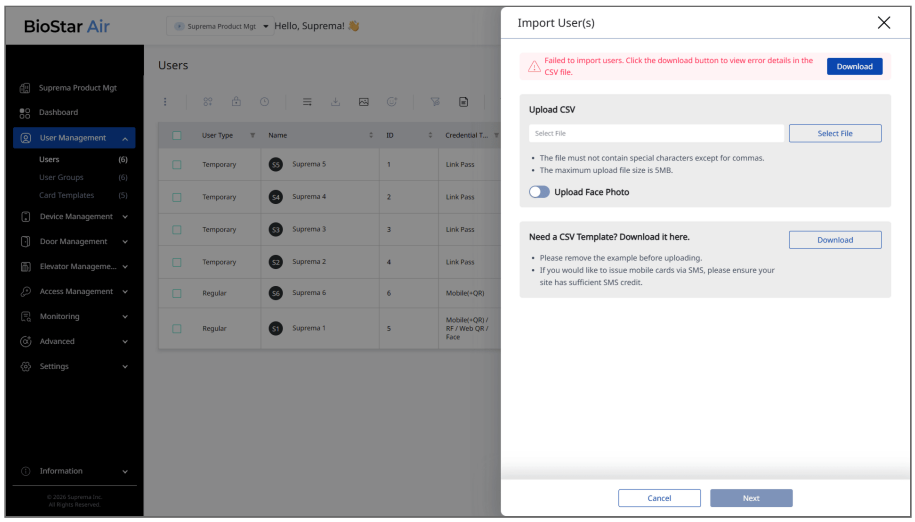
Información

- No use caracteres especiales distintos de las comas (,) en el nombre del archivo CSV.
- El tamaño máximo del archivo CSV es **5MB**.
- Alternativamente, arrastre y suelte el archivo CSV en el campo **Subir CSV** del panel **Importar usuarios**.

Validación del archivo CSV

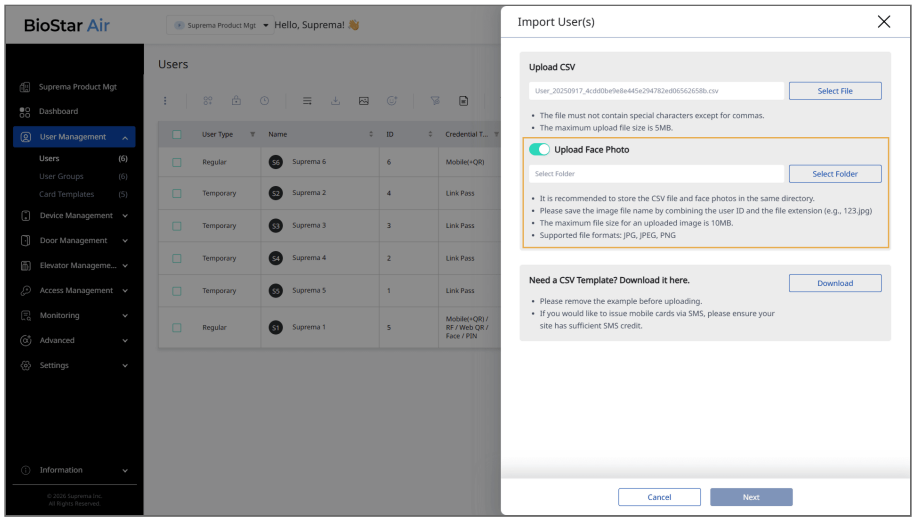
El proceso de carga de CSV ahora proporciona **retroalimentación de errores a nivel de fila**, lo que facilita la solución de

problemas. Si se producen errores durante la carga, se ofrece un informe detallado para su revisión. Haga clic en **Descargar** para descargar el informe.



Subir imágenes de perfil de usuario

Las imágenes de perfil se pueden subir automáticamente con el archivo CSV o cargarlas manualmente de forma masiva más adelante.



1. Prepare los archivos de imagen de perfil que coincidan con la columna **Clave de usuario** del archivo CSV.

   Por ejemplo, el archivo *601.jpg* corresponde al usuario con ID **601**.

2. Después de cargar el archivo CSV en el panel **Importar usuarios**, habilite la opción **Subir Foto de Rostro**.

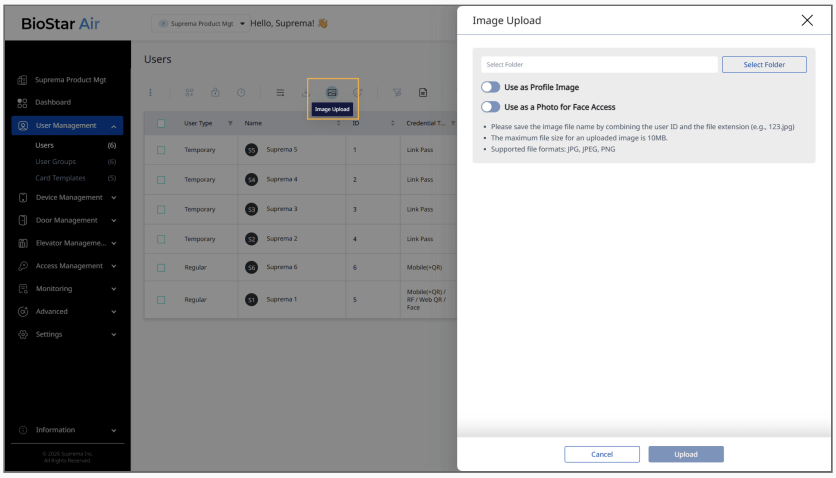
3. Haga clic en **Seleccionar Carpeta**, luego seleccione la carpeta que contiene las imágenes de perfil.

Requisitos de formato de archivo

- Formatos compatibles: *.jpg*, *.jpeg*, *.png*
- Límite de tamaño de archivo: **1 MB** por imagen

Consejo

Si las imágenes de perfil no estaban listas cuando se cargó el archivo CSV, utilice **Subir imagen**() en la lista de usuarios para agregarlas más tarde.



Finalizar la carga masiva

Una vez que se han cargado todos los datos de usuario y las imágenes, el sistema procesa las entradas y los nuevos usuarios aparecen en la lista con las credenciales asignadas.

Solución de Problemas

Si tiene problemas al cargar el CSV, consulte Solución de problemas al agregar usuarios en masa para obtener ayuda con la solución de problemas comunes. El documento también incluye fórmulas de Excel que le ayudan a validar los datos y a eliminar duplicados.

Administrar Grupos de Usuarios

Utiliza los grupos de usuarios para clasificar y gestionar usuarios por departamento, rol, ubicación y más. Los grupos de usuarios de BioStar Air no son jerárquicos, por lo que un usuario puede pertenecer a varios grupos al mismo tiempo; esto te permite combinar libremente grupos de departamento, rol y ubicación. Los grupos te permiten administrar los niveles de acceso de forma centralizada y manejar de manera eficiente el filtrado de registros de eventos, la generación de informes y la asignación de dispositivos a zonas de reunión.

Consejo

Consulta el siguiente video para ver la guía sobre cómo gestionar grupos de usuarios.

Antes de comenzar

Composición del grupo de usuarios

Los grupos de usuarios no están organizados de forma jerárquica.

- Los usuarios en un subgrupo **no** aparecen automáticamente en el grupo principal.
- El recuento total de usuarios del grupo principal no incluye a los miembros del subgrupo a menos que se los agregue manualmente.
- Al seleccionar un subgrupo, se muestran únicamente los usuarios asignados a ese subgrupo.

Configurar múltiples grupos de usuarios

Los usuarios en BioStar Air pueden pertenecer a **múltiples grupos de usuarios**.

En BioStar 2, los grupos de usuarios normalmente estaban vinculados a un único departamento. BioStar Air los separa, lo que permite un uso más dinámico.

- Filtra la lista de usuarios por grupo para administrar rápidamente los niveles de acceso.

  > *p. ej., departamento de Recursos Humanos*

- Crea grupos específicos que abarquen varios departamentos.

  > *p. ej., vestuario masculino*

- Los grupos de usuarios se utilizan para el **filtrado de registros de eventos** y la **generación de informes**.

- Asigna grupos de usuarios a dispositivos o a grupos de dispositivos de la **zona de reunión** para aplicar protocolos de seguridad específicos.

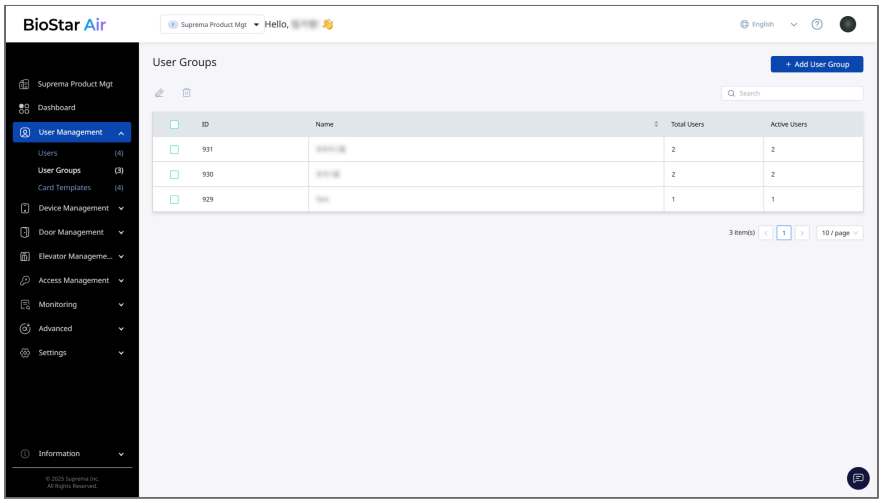
Esta flexibilidad facilita la gestión de roles de usuario superpuestos y de escenarios de acceso.

Crear grupo

Crear grupo de usuarios

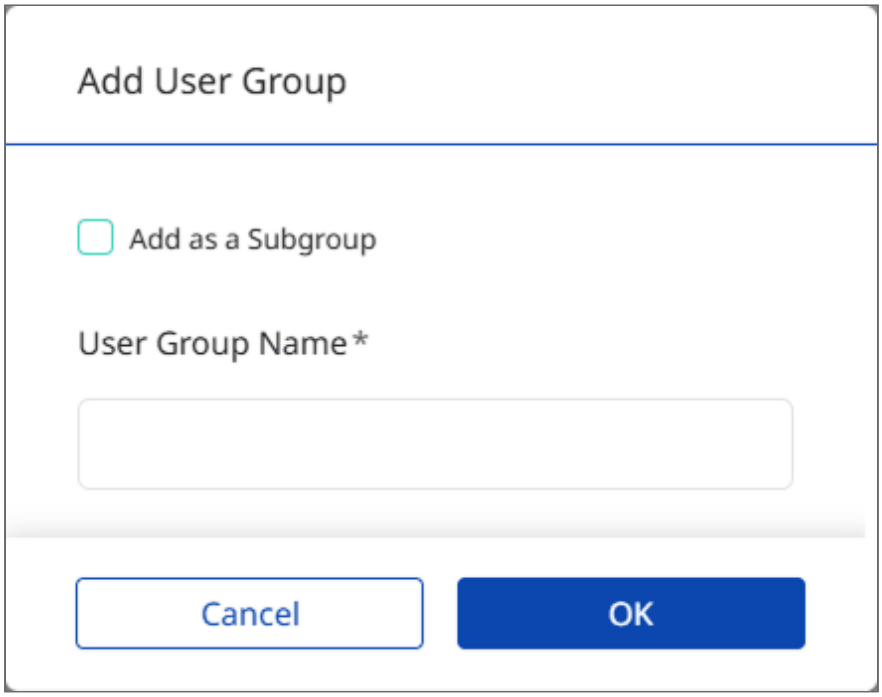
Crear un nuevo grupo de usuarios.

1. Haz clic en **Gestión de usuarios** → **Grupos de Usuarios** en la barra lateral izquierda.



2. Haz clic en **Agregar grupos de usuarios** en la parte superior derecha de la pantalla.

3. Cuando aparezca la ventana **Agregar grupo de usuarios**, ingresa el nombre del grupo de usuarios.



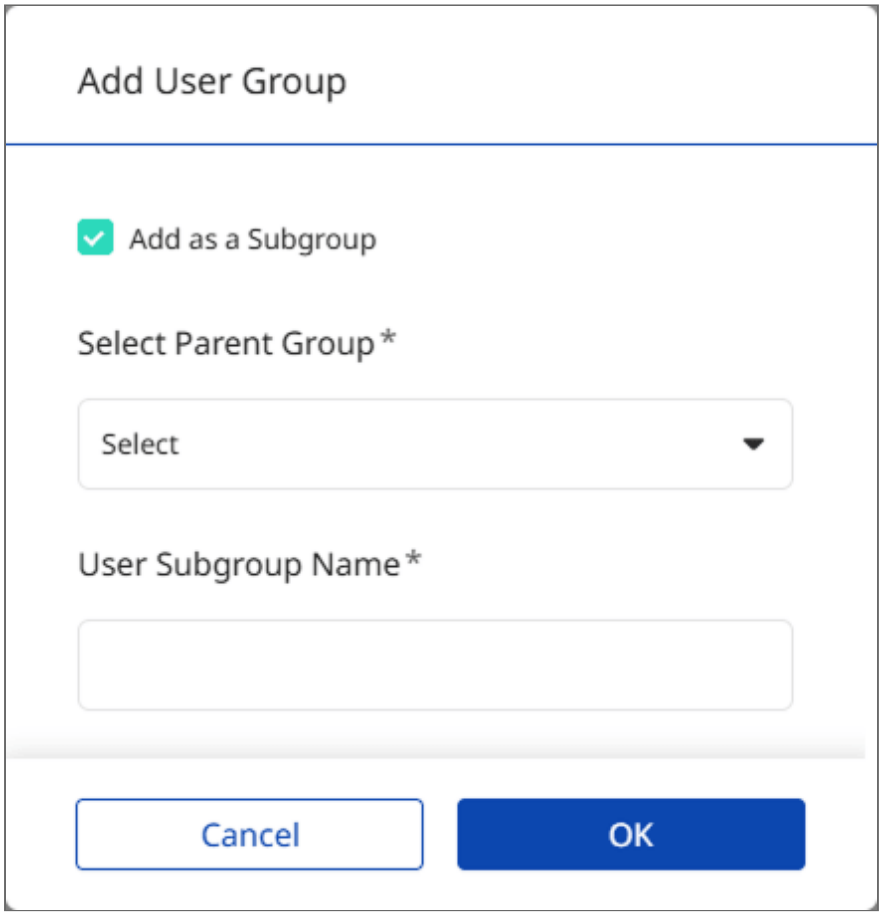
4. Haga clic en **OK** para crear el grupo.

> **Información**
>
> - Eliminar un grupo no elimina a los usuarios que contiene. Solo se les quita la pertenencia al grupo.
> - Para obtener más información sobre cómo asignar usuarios a grupos, consulte Administrar Usuarios.

Crear subgrupo

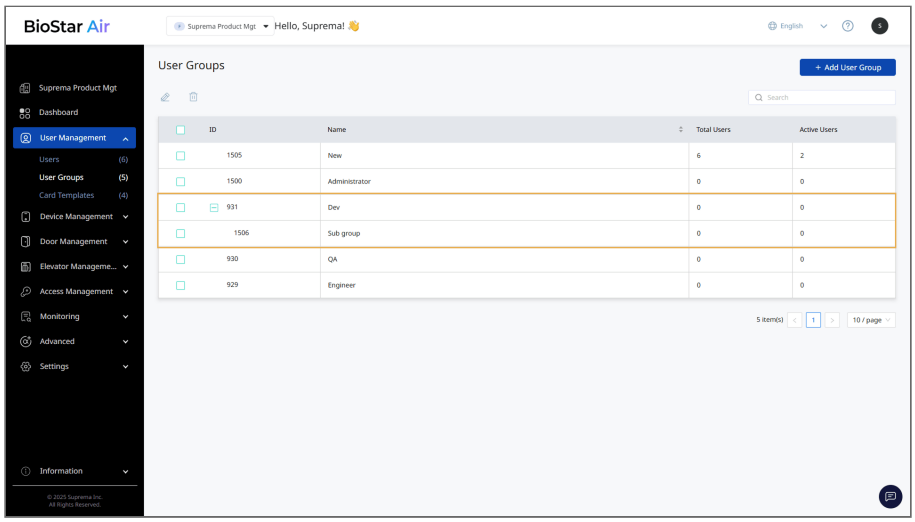
Puede usar subgrupos para clasificar aún más los grupos de usuarios. Sin embargo, los subgrupos **no son jerárquicos**. Esto significa que los usuarios de un subgrupo no se incluyen automáticamente en el grupo principal.

1. Haz clic en **Gestión de usuarios** → **Grupos de Usuarios** en la barra lateral izquierda.
2. Haz clic en **Agregar grupos de usuarios** en la parte superior derecha de la pantalla.
3. Cuando aparezca la ventana **Agregar grupo de usuarios**, haz clic en la opción **Agregar como un subgrupo**.



4. En **Seleccionar grupo principal**, seleccione el grupo principal.
5. Ingrese el nombre del grupo en **Nombre del subgrupo de usuarios**.
6. Haz clic en **OK** para crear el subgrupo.

El subgrupo recién creado aparece con sangría debajo del grupo principal en la lista de grupos de usuarios.

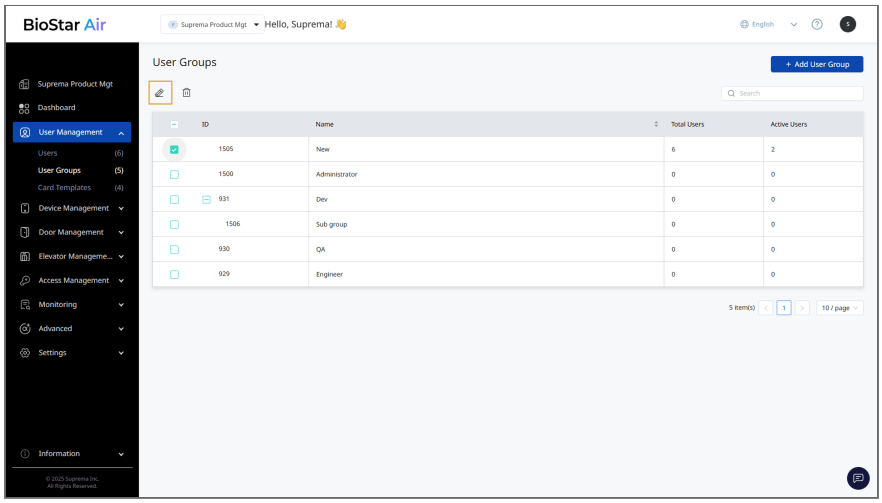


Editar nombre del grupo

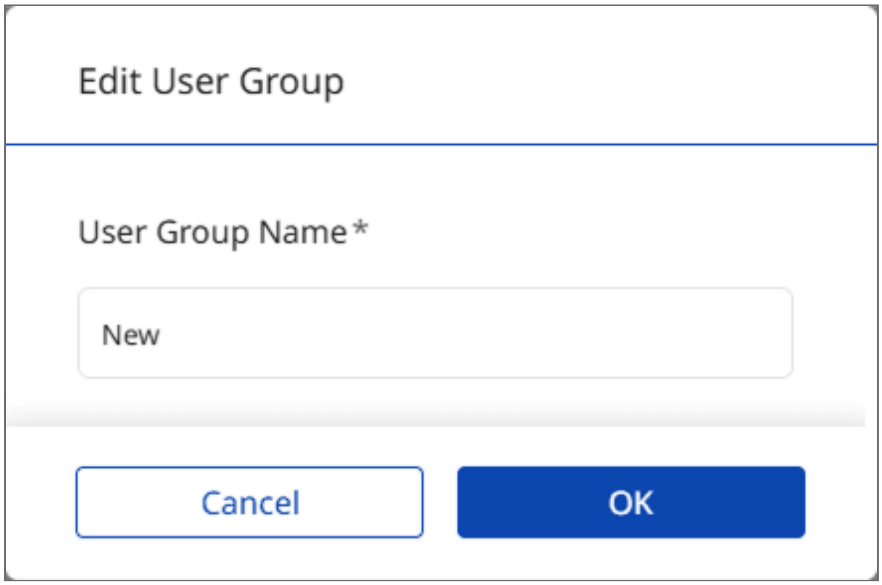
Modifica el nombre de un grupo de usuarios existente.

1. Haz clic en **Gestión de usuarios** → **Grupos de Usuarios** en la barra lateral izquierda.
2. Marca la casilla del grupo de usuarios que deseas editar en la lista.

3. Haz clic en en la parte superior izquierda de la lista de grupos de usuarios.



4. Cuando aparezca la ventana **Editar grupo de usuarios**, edita el nombre del grupo.



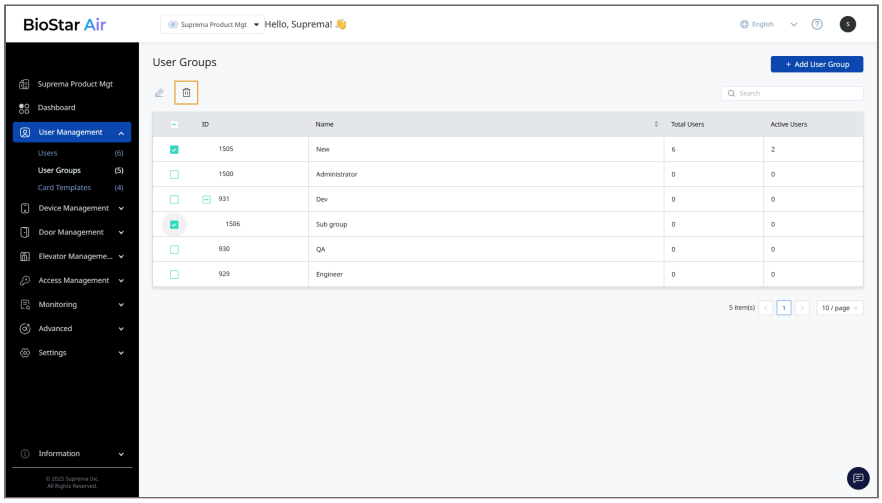
5. Haz clic en **OK** para guardar los cambios.

> **Información**
> El nombre del grupo solo se puede editar cuando se selecciona un único grupo.

Eliminar grupo

Elimina los grupos de usuarios que ya no sean necesarios.

1. Haz clic en **Gestión de usuarios** → **Grupos de Usuarios** en la barra lateral izquierda.
2. Marca la casilla del grupo de usuarios que deseas eliminar en la lista.
3. Haz clic en en la parte superior izquierda de la lista de grupos de usuarios.



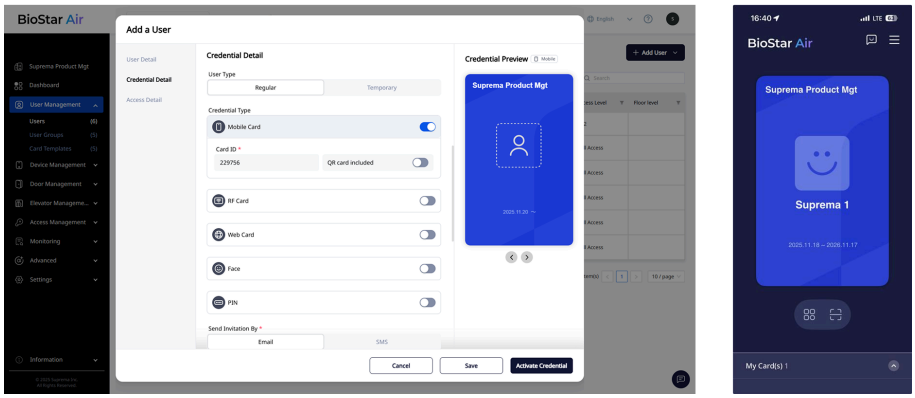
4. Cuando aparezca un mensaje de advertencia, haz clic en **Sí**.

Administrar plantillas de tarjeta

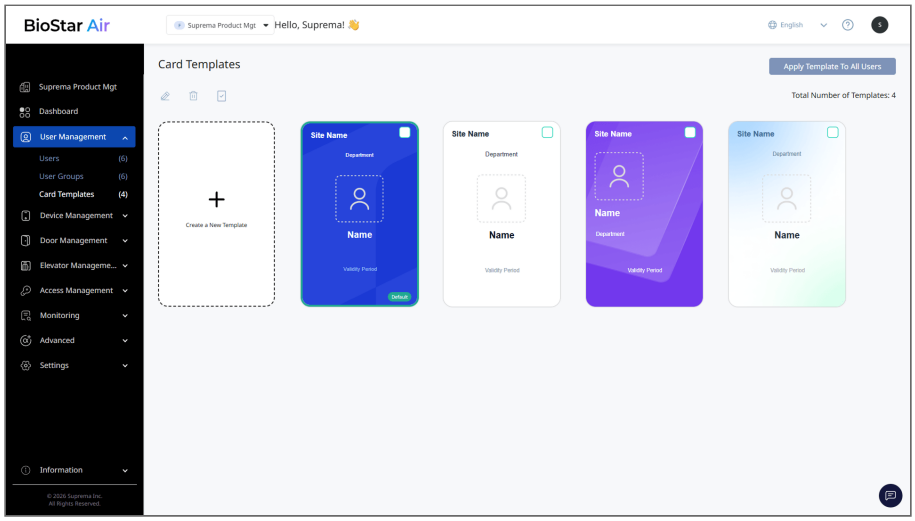
Con las plantillas de tarjeta en BioStar Air, los administradores pueden diseñar y personalizar las tarjetas móviles de los usuarios. Las plantillas refuerzan la identidad de marca al incluir colores corporativos, logotipos e información personalizada. Se aplican a las tarjetas móviles utilizadas en la aplicación Suprema Pass.

BioStar Air

Mobile device



Cada sitio de BioStar Air incluye plantillas predeterminadas. Haga clic en **Gestión de usuarios** → **Plantillas de tarjetas** en la barra lateral izquierda.



Vea las plantillas predeterminadas. Los administradores aplican las plantillas de tarjeta móvil de una de las siguientes tres maneras.

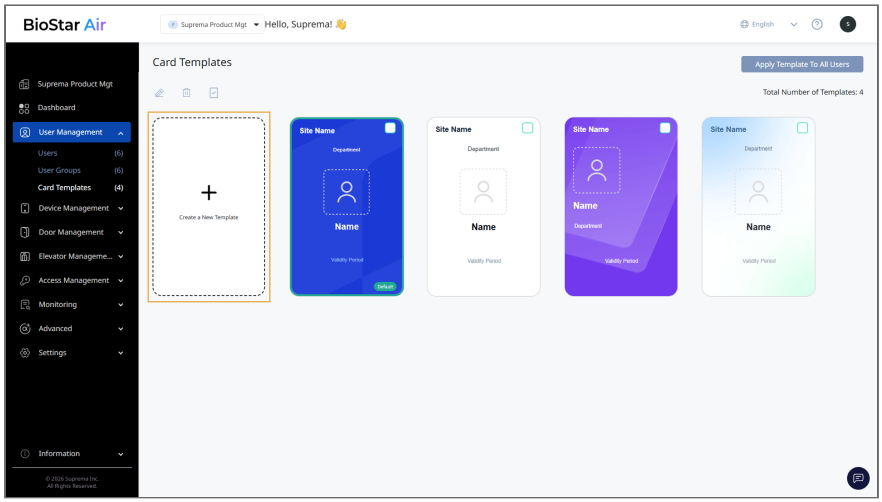
- Aplicar la plantilla de tarjeta predeterminada a la tarjeta móvil de un usuario
- Modificar los parámetros de una plantilla existente para aplicar una tarjeta móvil personalizada
- Crear una nueva plantilla personalizada y aplicarla en lugar de la plantilla existente

> **Consejo**
> Vea el siguiente video para aprender cómo administrar las plantillas de tarjeta.

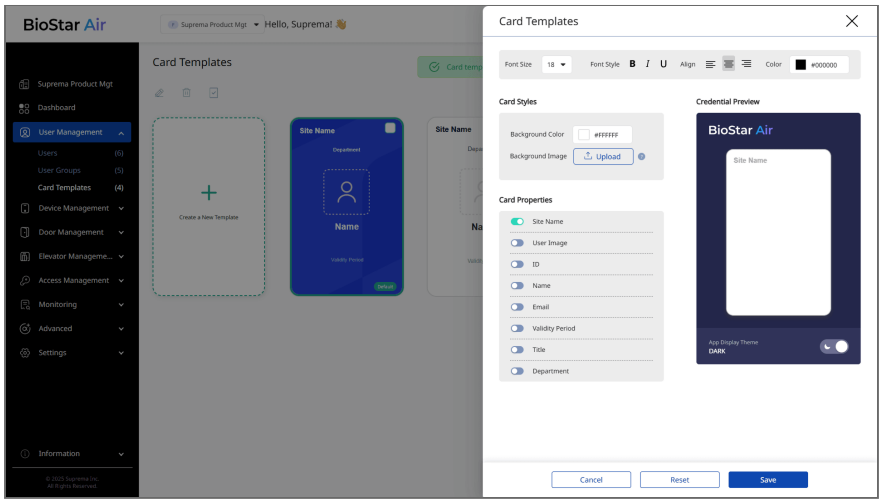
Crear una nueva plantilla de tarjeta

Crear una nueva plantilla de tarjeta.

1. Haga clic en **Gestión de usuarios** → **Plantillas de tarjetas** en la barra lateral izquierda.
2. Haga clic en **Crear una nueva plantilla**.



3. Cuando aparezca el panel **Plantillas de tarjetas**, establezca el diseño y la disposición de la tarjeta.

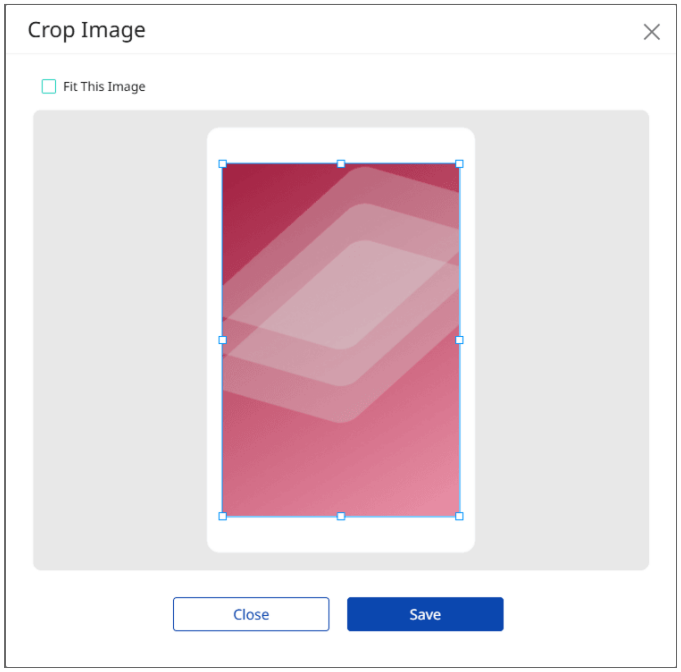


4. Después de aplicar la configuración deseada, haga clic en **Guardar** para guardar la plantilla de tarjeta móvil.

Estilos de tarjeta

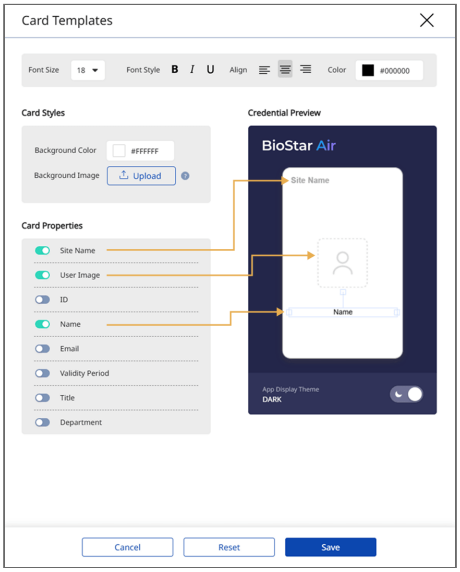
En la sección **Estilos de tarjeta** puede establecer el color de fondo o la imagen de fondo de la tarjeta.

- **Color de fondo**: Establezca el color de fondo de la tarjeta móvil.
- **Imagen de fondo**: Cargue una imagen de fondo para la tarjeta móvil. Haga clic en **Subir** y luego seleccione un archivo de imagen de fondo almacenado localmente. Cuando aparezca la ventana **Delimitar imagen**, haga clic en la opción **Ajuste esta imagen** o ajuste el tamaño manualmente. Tras completar los ajustes de la imagen, haga clic en **Guardar**.

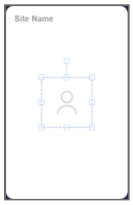


Propiedades de la tarjeta

En la sección **Propiedades de la tarjeta** puede seleccionar qué atributos incluir en la tarjeta móvil. Haga clic en el interruptor para mostrar los atributos seleccionados en la vista previa **Vista previa de credenciales** a la derecha.



- Después de colocar un atributo, haga clic en él en la vista previa **Vista previa de credenciales** para mostrar las manijas que permiten redimensionarlo, reposicionarlo y rotarlo.



- Personalice la fuente de cada atributo. Haga clic en un atributo colocado y luego utilice las opciones de fuente en la parte superior. Ajuste el tamaño, el estilo, la alineación y el color de la fuente.



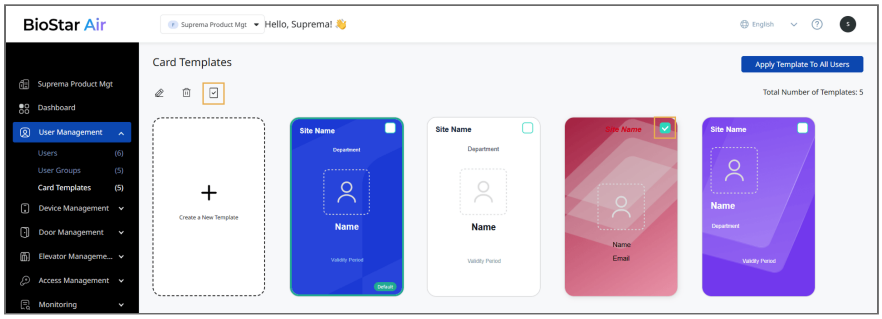
- Seleccione el modo oscuro o el modo claro en **Visualización de Aplicaciones**.
- Haga clic en **Reiniciar** para inicializar el diseño configurado.

- Después de completar todas las configuraciones, haga clic en **Guardar** para guardar la plantilla de tarjeta móvil.

Establecer la plantilla de tarjeta predeterminada

Establezca una plantilla de tarjeta móvil recién agregada como predeterminada.

1. Haga clic en **Gestión de usuarios** → **Plantillas de tarjetas** en la barra lateral izquierda.
2. Haga clic en la casilla de verificación en la esquina superior derecha de la plantilla deseada.
3. Haga clic en ☑ en la parte superior izquierda de la lista de plantillas.



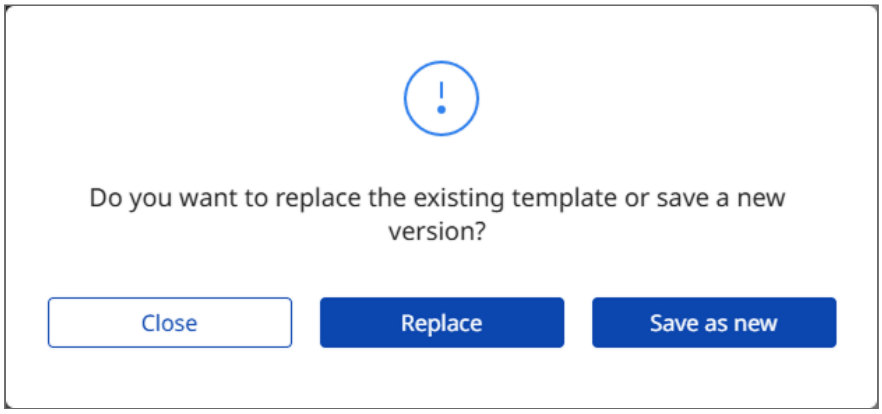
4. Cuando aparezca la ventana de mensaje, haga clic en **Sí**.

La plantilla de tarjeta móvil predeterminada se aplica automáticamente cuando se agrega un nuevo usuario.

> **Información**
> Solo se puede establecer una plantilla como predeterminada.

Editar plantillas de tarjeta

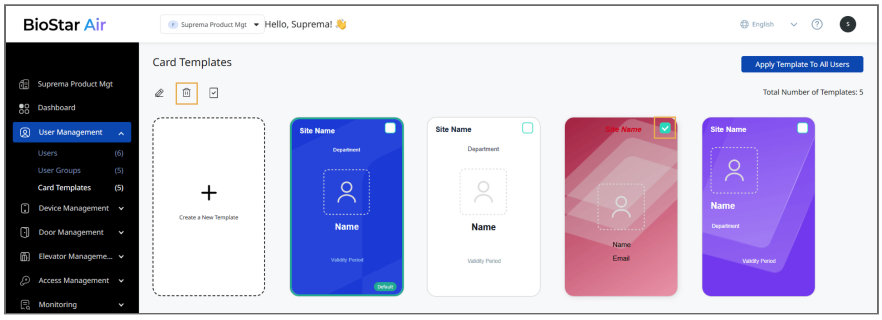
1. Haga clic en **Gestión de usuarios** → **Plantillas de tarjetas** en la barra lateral izquierda.
2. Haga clic en la plantilla que desea editar en la lista de plantillas. O bien seleccione la casilla de verificación en la esquina superior derecha de la plantilla y haga clic en ✎.
3. Cuando aparezca el panel **Plantillas de tarjetas**, modifique el diseño y la distribución de la tarjeta.
4. Haz clic en **Guardar** para guardar los cambios.
5. Cuando aparezca la ventana de mensaje, haga clic en **Reemplazar** o en **Guardar como nuevo**.



- **Reemplazar**: Guarde los cambios en la plantilla existente.
- **Guardar como nuevo**: Guarde los cambios como una nueva plantilla.

Eliminar plantillas de tarjeta

1. Haga clic en **Gestión de usuarios** → **Plantillas de tarjetas** en la barra lateral izquierda.
2. En la lista de plantillas, haga clic en la casilla de verificación en la esquina superior derecha de cada plantilla que desee eliminar. Puede seleccionar una o más plantillas.
3. Haga clic en en la parte superior izquierda de la lista de plantillas.

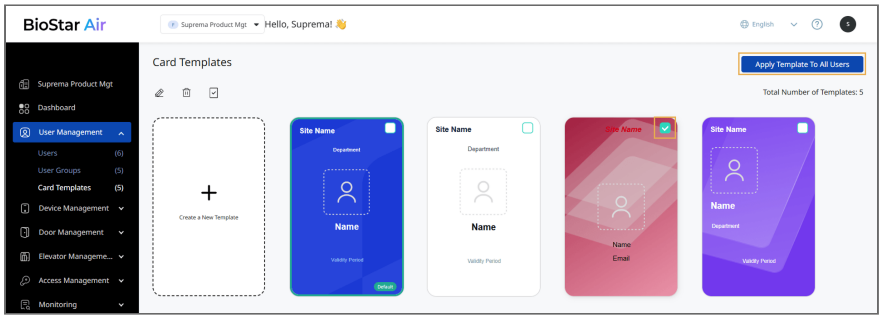


4. Cuando aparezca la ventana de mensaje, haga clic en **Sí**.

> **Información**
> No se pueden eliminar las plantillas predeterminadas.

Aplicar plantillas a todos los usuarios

1. Haga clic en **Gestión de usuarios** → **Plantillas de tarjetas** en la barra lateral izquierda.
2. En la lista de plantillas, haga clic en la casilla de verificación en la esquina superior derecha de la plantilla que desea aplicar.
3. Haga clic en **Aplicar plantilla a todos los usuarios** en la parte superior derecha de la pantalla.



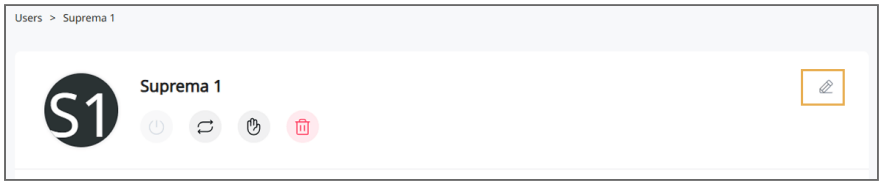
4. Cuando aparezca la ventana de mensaje, haga clic en **Sí**.

> **Información**
>
> - Al aplicar la plantilla de tarjeta seleccionada a todos los usuarios, se reemplaza cualquier plantilla establecida anteriormente.
> - Solo se puede aplicar una plantilla de tarjeta a todos los usuarios.

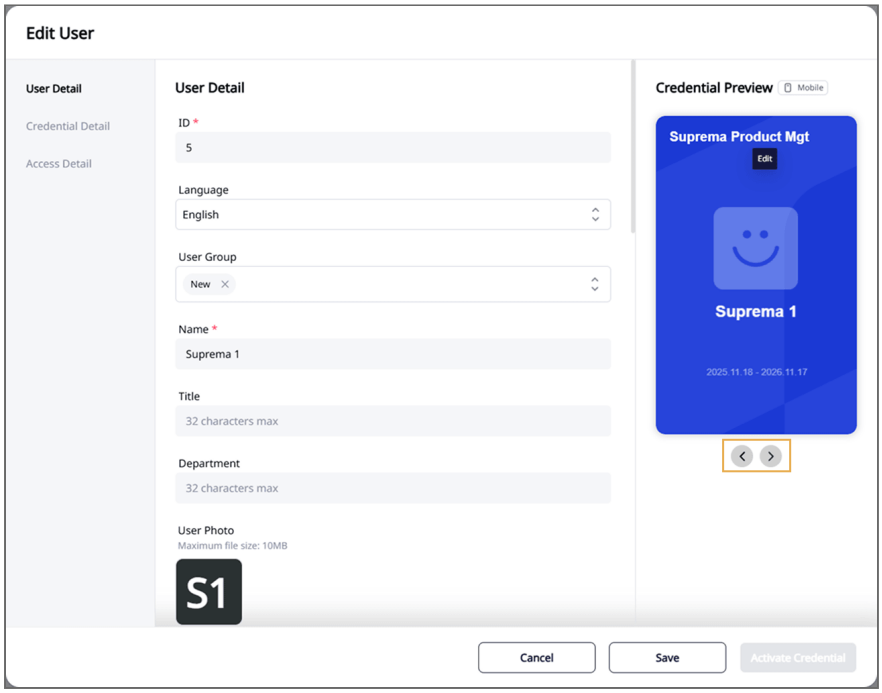
Cambiar la plantilla de tarjeta de un usuario

Siga estos pasos para cambiar la plantilla de tarjeta de un usuario en particular.

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en el usuario en la lista para aplicar una plantilla de tarjeta.
3. Haz clic en en la esquina superior derecha de la sección de detalles del usuario.



4. Cuando aparezca la ventana **Editar usuario**, haz clic en o bajo 'Plantilla de tarjeta' en el panel derecho para seleccionar la plantilla deseada.



5. Haz clic en **Guardar** para aplicar los cambios.

Tipos de tarjetas y credenciales de usuario

A partir de la versión 2.6 de BioStar Air se introdujeron dos tipos de usuario para mejorar la gestión.

- **Regular**: Un usuario que es miembro regular de una organización o instalación y que requiere acceso a largo plazo. Se pueden emitir todos los tipos de credenciales.
- **Invitada**: Un visitante o miembro no regular que necesita acceso limitado y de corta duración. Esto puede incluir huéspedes, visitantes externos, contratistas temporales, mensajeros de entrega, etc. Solo se pueden emitir las credenciales **Tarjeta Web**, incluyendo el código QR y LinkPass.

> **Información**
>
> Para obtener más información sobre la emisión de credenciales al agregar o editar usuarios, consulte Agregar usuarios.

> **Consejo**
>
> Vea el video a continuación para obtener un tutorial sobre los tipos de usuario y de tarjeta.

Tipos de tarjetas para usuarios regulares

Las credenciales que puede emitir a los usuarios regulares son las siguientes.

> **Información**
>
> Para obtener más información sobre cómo usar credenciales móviles con la aplicación Suprema Pass, consulte Uso de credenciales móviles.

Tarjeta Móvil

- Se asigna automáticamente un **ID de tarjeta** único, aunque también puede establecerse manualmente.
- Al usar un **Airfob Tag** o **Airfob Patch**, integre el sistema de control de acceso existente utilizando el número de la tarjeta móvil como número de serie de la tarjeta.
- Para compatibilidad con un sistema anterior, el ID de la tarjeta móvil puede coincidir con el número de tarjeta RF del sitio anterior.

Tarjeta RF

- Agregue hasta ocho tarjetas RFID por usuario.
- Configure **Tipo de tarjeta** (CSN o Wiegand), **ID de tarjeta**, y **Nombre de la tarjeta** para simplificar la gestión cuando se asignan varias tarjetas.
- Seleccione un lector en **Escanear con el lector.** para escanear una tarjeta RFID existente con un dispositivo Suprema conectado.
- Si una tarjeta RF existente tiene un **CSN** (número de serie de la tarjeta), ingrese el CSN manualmente.

Web QR

- Los usuarios regulares pueden usar el **código QR** de una tarjeta móvil.
- Acceda al código QR tocando el botón en la interfaz de la tarjeta móvil.

Pase de enlace

- Envíe un enlace web a la dirección de correo electrónico o al número de teléfono del usuario.
- El usuario abre el enlace recibido en un navegador web y hace clic en **Abierto** para obtener acceso.

> **Información**
> Para obtener más información sobre las credenciales LinkPass, consulte Credenciales LinkPass.

Credencial facial

- Agregue hasta dos imágenes de perfil facial por usuario.
- Regístrate mediante un lector conectado o cargando una imagen.
- Envía al usuario un enlace por correo electrónico y, a continuación, captura una foto con la cámara del dispositivo móvil para registrarlo.

PIN 2FA

Establece un PIN de 4 a 16 dígitos para usar como parte de la autenticación de dos factores (2FA).

Tipos de tarjetas para usuarios temporales

Los usuarios temporales no reciben tarjetas móviles ni tarjetas RFID. En su lugar, emite **credenciales web** que no requieren la descarga de una aplicación. Las opciones disponibles son las siguientes:

Web QR

- Envía por correo electrónico o por mensaje de texto.
- Accesible a través de un navegador web.
- Usa un **código QR dinámico**, que se actualiza cada cinco minutos, para mejorar la seguridad.

Pase de enlace

Envía al usuario un enlace web por correo electrónico o por mensaje de texto. El usuario obtiene acceso al hacer clic en **Abierto** en un navegador web.

> **Información**
> Para obtener más información sobre las credenciales LinkPass, consulte Credenciales LinkPass.

Administrar niveles de acceso

Configura los **niveles de acceso** para controlar dónde se pueden usar las credenciales, independientemente de si el usuario es regular o temporal.

> **Precaución**
> Si el usuario es temporal, asigna con cuidado niveles de acceso restrictivos y evita emitir credenciales con acceso ilimitado.

Credenciales LinkPass

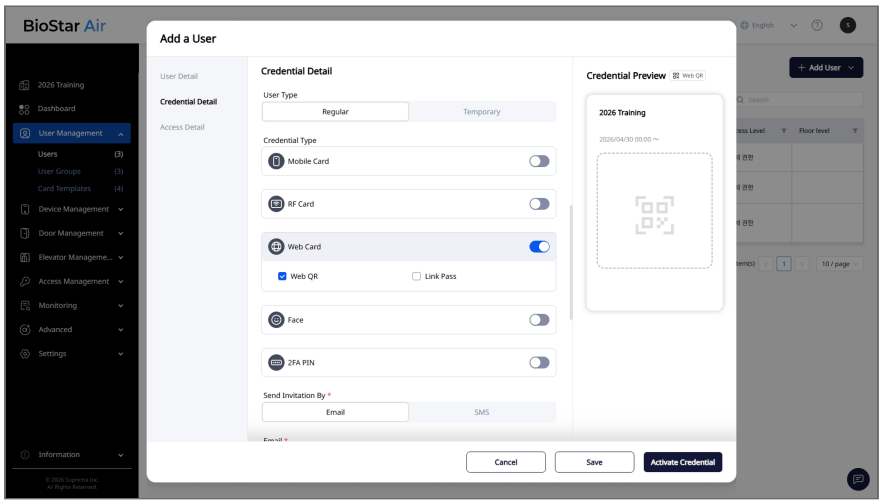
LinkPass es una credencial móvil que se puede usar en BioStar Air sin una app. Los administradores pueden otorgar acceso a usuarios sin que instalen una app ni utilicen BLE o NFC. Como LinkPass funciona a través de la nube de BioStar Air y se activa mediante un enlace web seguro, es ideal para la entrada de clientes, entregas o accesos de baja seguridad, como portones de estacionamiento y vestíbulos.

- **Alcance de la credencial**: Una credencial LinkPass otorga acceso a las mismas puertas que las otras credenciales asignadas al usuario. No se recomienda emitir una credencial LinkPass a usuarios que no tienen acceso a áreas de alta seguridad.
- **No se requiere app**: LinkPass funciona a través de un navegador web, por lo que no necesita una app móvil, Bluetooth ni comunicación NFC.
- **Acceso en la nube**: Los comandos de LinkPass se envían a través de la nube de BioStar Air y pueden activarse desde cualquier lugar con conexión a Internet. No comparte ni rastrea la ubicación.
- **Conectividad del lector**: El lector de la puerta debe estar en línea y conectado a BioStar Air para que LinkPass funcione correctamente.
- **Casos de uso recomendados**: LinkPass es adecuado para visitantes temporales, entregas y áreas de baja seguridad como vestíbulos o portones de estacionamiento.

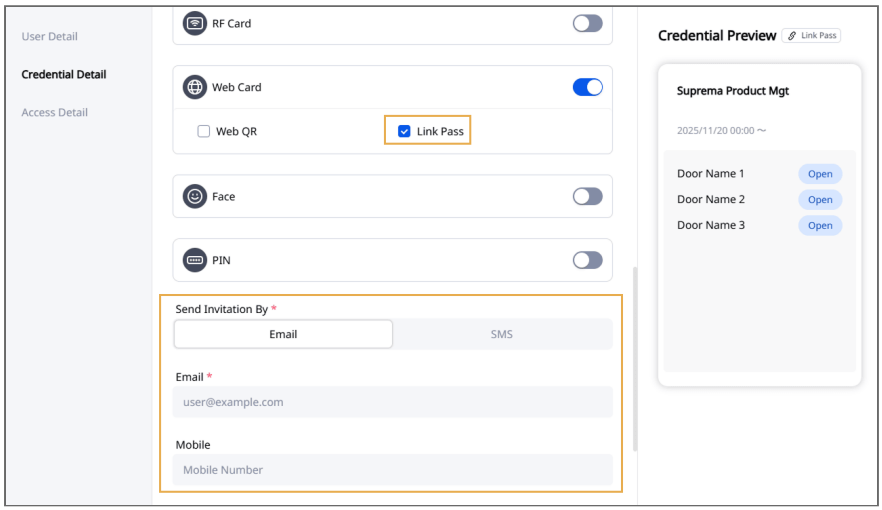
Activar credenciales LinkPass

1. Inicie sesión en el sitio web de BioStar Air.
2. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.

3. Navegue a la pantalla **Editar usuario** o **Añadir nuevo usuario** usando uno de los siguientes métodos.
   - Seleccione un usuario existente en la lista y luego haga clic en ✎ en la esquina superior derecha.
   - Haga clic en **Añadir nuevo usuario** → **Añadir nuevo usuario** en la esquina superior derecha de la pantalla.
4. Vaya a la sección **Detalles de la Credencial**.
5. Active la opción **Tarjeta Web**.



6. Haga clic en la casilla **Pase de enlace**.
7. Ingrese en **Enviar invitación por** una **dirección de correo electrónico** o un **número de teléfono** únicos donde el usuario pueda recibir el enlace de la credencial.



8. Seleccione el **Nivel de acceso** correspondiente y configure el **Válido hasta el** del usuario.
9. Haga clic en **Activar Credencial** para emitir la credencial.
10. Envíele al usuario una invitación con la URL única de LinkPass por correo electrónico o SMS.

Usar LinkPass

1. En un dispositivo móvil, abra la URL de LinkPass desde el correo electrónico o el SMS.
2. La página web muestra todas las puertas asignadas al usuario, y cada puerta tiene **Abierto**.
3. Haga clic en **Abierto** para abrir la puerta enviando un comando de desbloqueo en la nube al lector.

Información
LinkPass no requiere comunicación por Bluetooth ni NFC.

Dispositivos

Los ajustes flexibles de gestión de dispositivos de BioStar Air permiten configurar cada sitio exactamente según sus requisitos. En este documento, la gestión de dispositivos se refiere al ciclo de vida completo de un dispositivo, que incluye la inscripción, los ajustes, la gestión de firmware, la supervisión y la operación continua.

BioStar Air admite dos arquitecturas de dispositivos diferentes. Ambas pueden utilizarse en el mismo sitio, lo que permite a las organizaciones elegir el mejor enfoque para cada puerta o área.

Arquitectura distribuida

En una arquitectura distribuida, cada dispositivo edge contiene su propio controlador y se conecta directamente a la nube mediante Ethernet. Los dispositivos siguen operando de forma independiente durante interrupciones de red y se sincronizan automáticamente cuando se restablece la conectividad.

Los dispositivos edge también pueden actuar como controladores para lectores secundarios conectados vía RS-485.

Esta arquitectura se utiliza comúnmente para:

- Nuevas instalaciones
- Dispositivos biométricos
- Despliegues en los que es importante minimizar la infraestructura.

Arquitectura centralizada

En una arquitectura centralizada, los lectores se conectan a un panel de control mediante RS-485 o Wiegand. El panel de control se conecta a la nube vía Ethernet y actúa como controlador para los dispositivos aguas abajo.

El panel de control gestiona la redundancia y las decisiones de acceso para los lectores conectados durante interrupciones de red.

Esta arquitectura se utiliza comúnmente para:

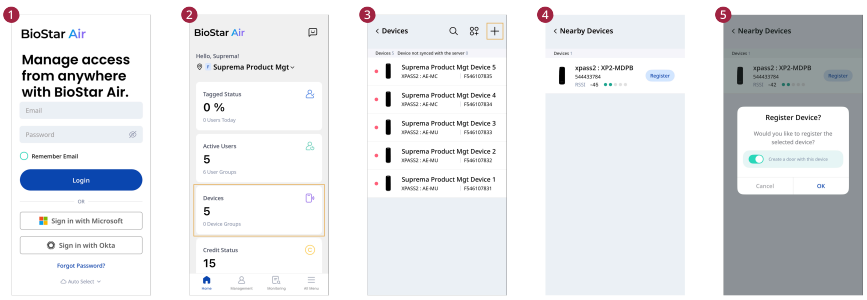
- Proyectos de modernización con cableado de bajo voltaje existente
- Sitios que reemplazan sistemas heredados de control de acceso
- Despliegues con salas de seguridad o paneles centralizados

Registrar y Eliminar Dispositivos Edge
Utilice la aplicación móvil BioStar Air para agregar dispositivos: registre nuevos dispositivos, elimine los existentes y actualice el firmware mediante una conexión inalámbrica.

Registrar dispositivo

Utilice la aplicación móvil BioStar Air para registrar dispositivos. Registre los dispositivos mediante Bluetooth Low Energy

(BLE) y adminístrelos desde el portal BioStar Air.



1. Abra la aplicación BioStar Air en su dispositivo móvil e inicie sesión.
2. Toque la tarjeta **Dispositivos**.
3. Toque + en la esquina superior derecha de la pantalla.
4. En la pantalla de búsqueda de dispositivos, toque **Registrar** en el dispositivo que desea registrar.
5. Cuando aparezca la ventana de registro del dispositivo, toque **OK**.

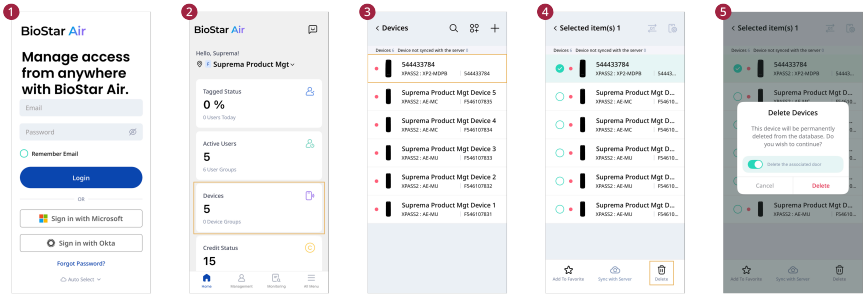
Vuelva a la lista de dispositivos y verifique que el dispositivo se haya agregado.

> **Consejo**
>
> Para obtener el mejor rendimiento, confiabilidad y acceso a las funciones más recientes, asegúrese de buscar actualizaciones de firmware tan pronto como se registren los dispositivos. Es posible que haya firmware nuevo disponible entre el momento en que el dispositivo se empaquetó y se instaló. Para obtener más información sobre las actualizaciones de firmware, consulte Actualizar Firmware.

> **Información**
>
> - No se pueden registrar dispositivos en el portal web. Registre el dispositivo mediante la aplicación móvil BioStar Air.
> - Al registrar un dispositivo, manténgalo cerca del dispositivo móvil y asegúrese de que el Bluetooth esté activado.
> - Para evitar que el dispositivo registrado se configure como una puerta, desactive la opción **Create a door with this device** en la ventana de registro del dispositivo.

Eliminar dispositivos

Si un dispositivo aparece desconectado en la lista de dispositivos del portal BioStar Air, elimínelo mediante la aplicación móvil.



1. Abra la aplicación BioStar Air en su dispositivo móvil.
2. Toque la tarjeta **Dispositivos**.
3. Mantenga presionado el dispositivo que desea eliminar. Seleccione los demás dispositivos que desee eliminar.
4. Toque el botón en la esquina inferior derecha.
5. En la ventana emergente, elija si desea eliminar la puerta vinculada.
6. Toque **Eliminar**.

> **Información**
> Los dispositivos distintos de X-Station 2 se pueden eliminar desde el portal BioStar Air, aunque el dispositivo debe estar en línea. Se recomienda eliminarlo mediante la aplicación móvil BioStar Air.

Administrar Dispositivos Edge Registrados

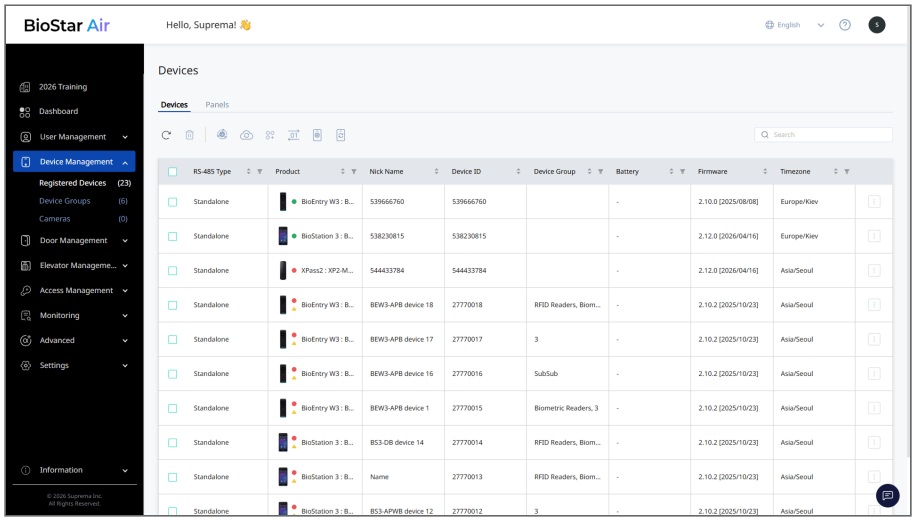
Vea de un vistazo el estado de conexión de los dispositivos, cambie la configuración biométrica y de tarjetas o actualice el firmware. Administre algunos dispositivos de forma individual y otros de forma masiva para operar su sistema de seguridad de manera eficiente.

> **Información**
> - Los dispositivos solo se pueden registrar en la **aplicación móvil BioStar Air** para iOS o Android. No es posible registrar dispositivos desde el portal web. Para obtener instrucciones detalladas sobre cómo registrar dispositivos mediante la aplicación móvil, consulte Registrar y Eliminar Dispositivos Edge.
> - Se requiere acceso a Internet para usar ciertas funciones, como el **acceso remoto**, la **autenticación biométrica**, el **acceso mediante código QR** y las **actualizaciones de firmware**.

> **Consejo**
> Consulte el siguiente video para ver la guía de registro y gestión de dispositivos.

Ver la lista de dispositivos

La lista de dispositivos le permite ver de un vistazo todos los dispositivos registrados en BioStar Air. Obtenga información clave de cada dispositivo, como estado de conexión, nombre de modelo y versión de firmware. Haga clic en un dispositivo para ver los detalles y modificar la configuración.



Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.

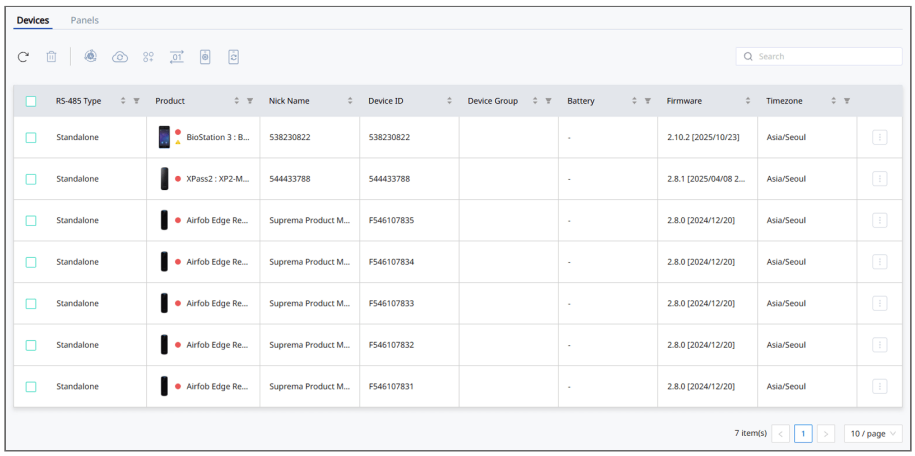
Estado de conexión del dispositivo

Compruebe el estado de conexión de cada dispositivo mediante los iconos de estado en la lista de dispositivos.

- 🟢 **Verde**: El dispositivo está en línea, puede controlarse de forma remota y puede aceptar y actualizar la autenticación por QR.
- 🔴 **Rojo**: El dispositivo está desconectado.
- 🟠 **Naranja**: Se está actualizando el firmware.
- ○ **No conectado**: El dispositivo no tiene conexión a la red. (p. ej., Airfob Patch)
- ⚠️ **Advertencia**: Se requiere sincronización entre el servidor y el dispositivo. Consulte Resincronizar dispositivos sin conexión para ver las instrucciones de resincronización.

Información del dispositivo

Cada columna de la lista de dispositivos contiene la siguiente información.



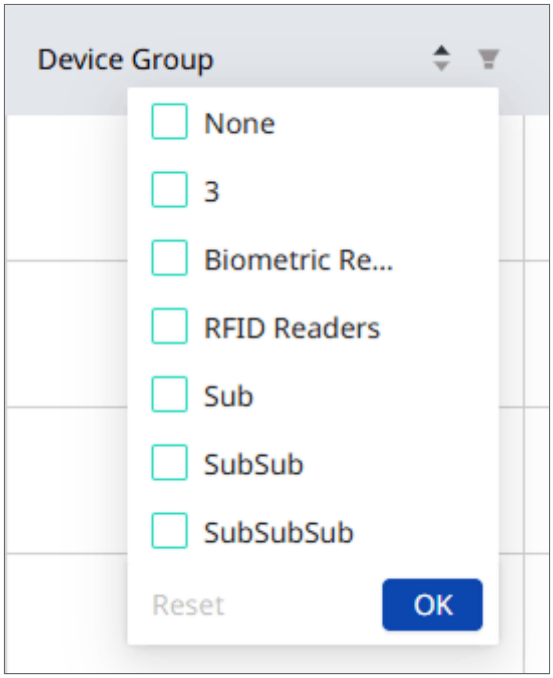
- **RS-485 Tipos**: Disponible en dispositivos que admiten comunicación RS-485. Verifique si el dispositivo es primario o secundario. Los dispositivos que no estén configurados como primario o secundario aparecen como **Independente**.
- **Producto**: El nombre y el modelo del dispositivo obtenidos de la base de datos de Suprema.
- **Apodo**: Un campo editable por el usuario para facilitar su identificación. Edítelo en la ventana **Editar dispositivo** que

aparece al hacer clic en el dispositivo en la lista.

- **Identificación del dispositivo**: El identificador único asignado al dispositivo.
- **Grupo de dispositivos**: El grupo al que pertenece el dispositivo.
- **Batería**: Disponible solo en dispositivos con batería. Compatible únicamente con dispositivos Airfob Tag.
- **Firmware**: La versión de firmware instalada actualmente.
- **Zona horaria**: La zona horaria configurada en el dispositivo.

Filtrar

Puedes usar la función de filtro en el encabezado superior de la lista de dispositivos. Haz clic en en el encabezado para establecer las condiciones deseadas.

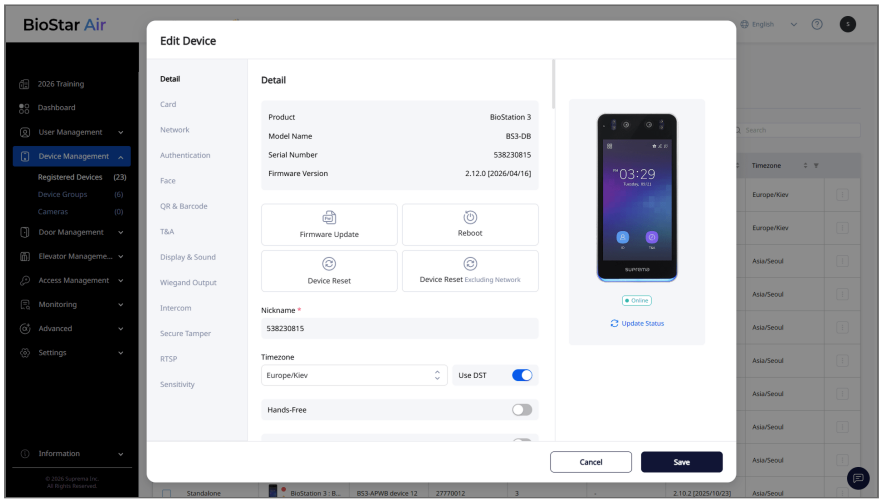


Información

Para restablecer los filtros aplicados, haga clic en y seleccione **Restablecer**.

Editar la información y los ajustes individuales del dispositivo

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haz clic en el dispositivo que deseas editar en la lista.
3. Aparece la ventana **Editar dispositivo**.



La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

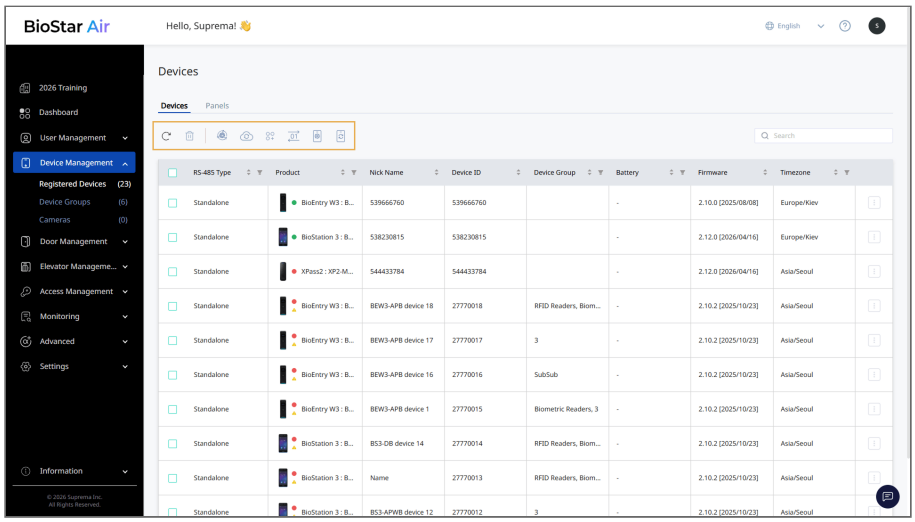
4. Edita los detalles o la configuración del dispositivo.

5. Haz clic en **Guardar** en la parte inferior para guardar los cambios.

Para obtener más información sobre cómo editar campos y configurar las opciones de cada sección, consulta Opciones de Configuración de Dispositivos y Paneles.

Acciones masivas para dispositivos

Usa los controles en la parte superior de la lista de dispositivos para administrar varios dispositivos a la vez.



- : Actualizar la lista de dispositivos.
- : Elimina los dispositivos registrados en el sitio.

> **Alerta**
>
> Solo los dispositivos en línea pueden eliminarse de forma permanente. Si el dispositivo está fuera de línea, elimínalo primero en la aplicación móvil BioStar Air antes de agregarlo a otro sitio. Para obtener más información sobre cómo eliminar dispositivos mediante la aplicación móvil, consulta Registrar y Eliminar Dispositivos Edge.

- : Actualiza el firmware de los dispositivos seleccionados. Para obtener más información sobre las actualizaciones de firmware, consulta Actualizar Firmware.

- : Sincroniza las plantillas biométricas de los dispositivos seleccionados con el servidor.
- : Asigna los dispositivos seleccionados a un grupo. Para más información sobre la gestión de grupos de dispositivos, consulta Gestión de grupos de dispositivos.
- : Cambia el orden de bytes de la tarjeta RF del dispositivo seleccionado en la lista a **MSB** o **LSB**.
  - **MSB**: Procesa los datos de la tarjeta en orden de unidades de byte grandes a pequeñas, almacenando secuencialmente el número de serie de la tarjeta (CSN) de izquierda a derecha.
  - **LSB**: Procesa los datos de la tarjeta en orden de unidades de byte pequeñas a grandes, almacenando el número de serie de la tarjeta (CSN).
- : Importa los ajustes del dispositivo configurados originalmente en modo autónomo.
- : Actualiza el estado de los dispositivos seleccionados en la lista de dispositivos.

Resincronizar dispositivos sin conexión

Si un dispositivo ha estado sin conexión durante mucho tiempo, su información puede dejar de coincidir con la del servidor, y puede ser necesario resincronizarlo manualmente.

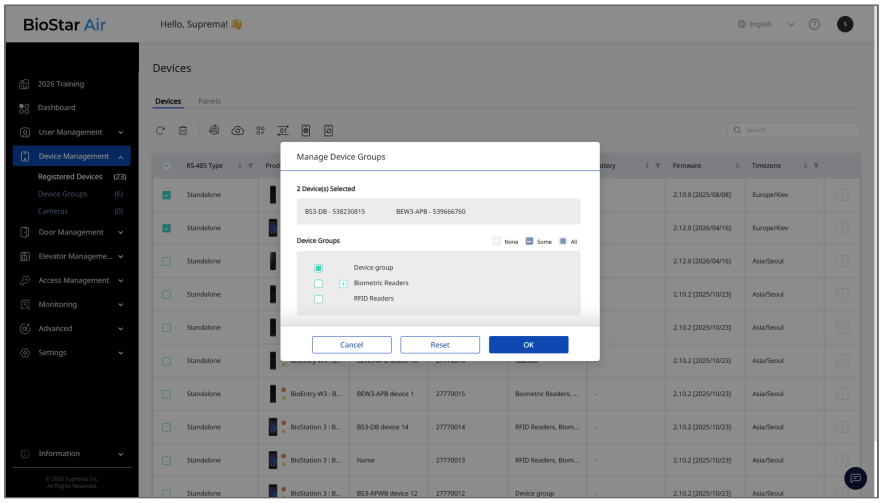
1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Busque dispositivos con el icono en la columna **Producto** de la lista de dispositivos.
3. Seleccione la casilla del dispositivo.
4. En la barra de herramientas, en la parte superior de la lista, haga clic en el botón .

> **Información**
> Los dispositivos que han estado sin conexión por menos de 7 días se sincronizan automáticamente cuando vuelven a conectarse, así que no se requiere ninguna acción adicional.

Gestión de grupos de dispositivos

En la lista de dispositivos, selecciona dispositivos individuales para añadirlos a un grupo o retirarlos de uno existente.

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. En la lista de dispositivos, haga clic en la casilla del dispositivo para agregarlo o quitarlo de un grupo.
3. Haga clic en en la parte superior de la lista de dispositivos.
4. Cuando aparezca la ventana **Administrar grupos de dispositivos**, agrega o elimina los dispositivos seleccionados del grupo.



Las casillas de verificación de **Grupos de dispositivos** tienen los siguientes significados:

- **Ninguna**: Elimina los dispositivos seleccionados del grupo.
- **Alguno**: Algunos de los dispositivos seleccionados ya pertenecen al grupo.
- **Todos**: Agrega los dispositivos seleccionados al grupo.

5. Haz clic en **OK** para guardar los cambios.

> **Información**
>
> - Al seleccionar otro grupo en la ventana **Administrar grupos de dispositivos**, los dispositivos seleccionados se mueven a ese grupo.
> - Un dispositivo puede pertenecer a varios grupos. Ese mismo dispositivo puede asignarse a varios grupos.
> - Haz clic en **Restablecer** para restablecer los cambios.

Registrar y Eliminar Paneles

BioStar Air versión 2.12 permite expandir el sistema de control de acceso mediante el panel CoreStation 20 (CS-20). Usar el cableado RS-485 existente para conectar dispositivos adicionales localmente reduce los costos de infraestructura y admite configuraciones de puertas complejas.

Este documento proporciona instrucciones paso a paso para inscribir el panel CS-20 y configurar dispositivos RS-485, OSDP y Wiegand como dispositivos secundarios.

> En BioStar Air, los dispositivos se clasifican como primarios, que actúan como controladores, y secundarios, que se conectan a los controladores. Algunos sistemas usan los términos Master/Slave para este concepto, pero la documentación de BioStar Air no emplea esos términos.

Registrar panel

El CoreStation 20 (CS-20) permite expandir el sistema de control de acceso conectando dispositivos que usan comunicación RS-485. Siga estos pasos para registrar el CS-20.

Antes de comenzar

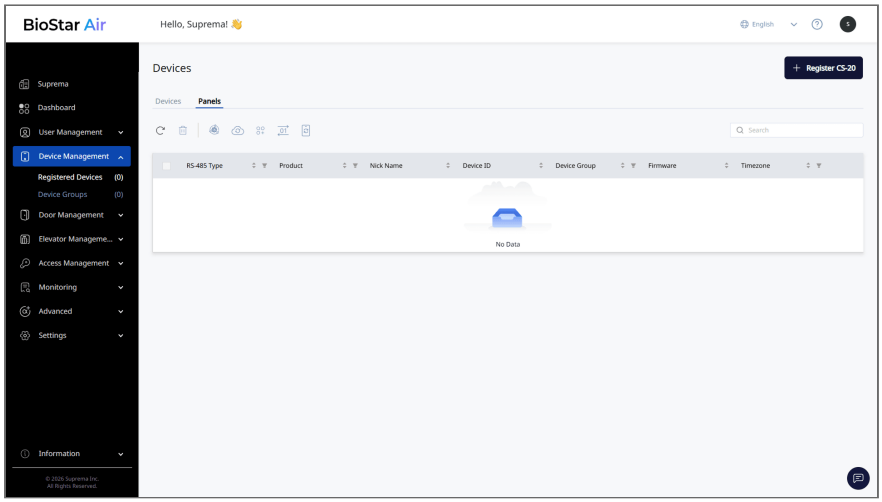
- Asegúrese de que el CS-20 esté encendido y sea accesible físicamente para presionar el botón **INIT**.

- El CS-20 debe estar conectado a Internet. Si la conexión de red es inestable, pueden producirse problemas durante el registro.
- Se requiere un número de serie de 9 dígitos. El número de serie se encuentra en la etiqueta en la parte posterior de la unidad.

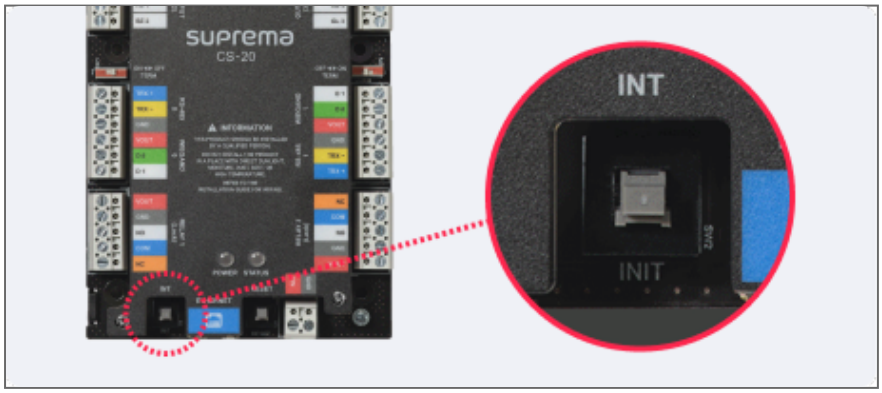
> **Información**
> Para más información sobre el CoreStation 20, consulte la Guía de instalación del CoreStation 20.

Registrar CS-20

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haga clic en la pestaña **Paneles**.

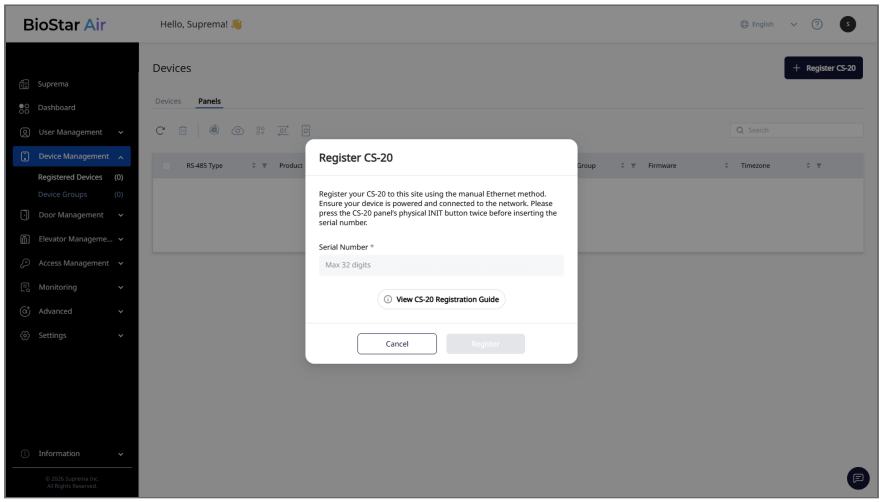


3. Haga clic en **Registrar CS-20** en la esquina superior derecha de la pantalla.
4. Cuando aparezca la ventana **Registrar CS-20**, presione el botón **INIT** del panel CS-20 dos veces.



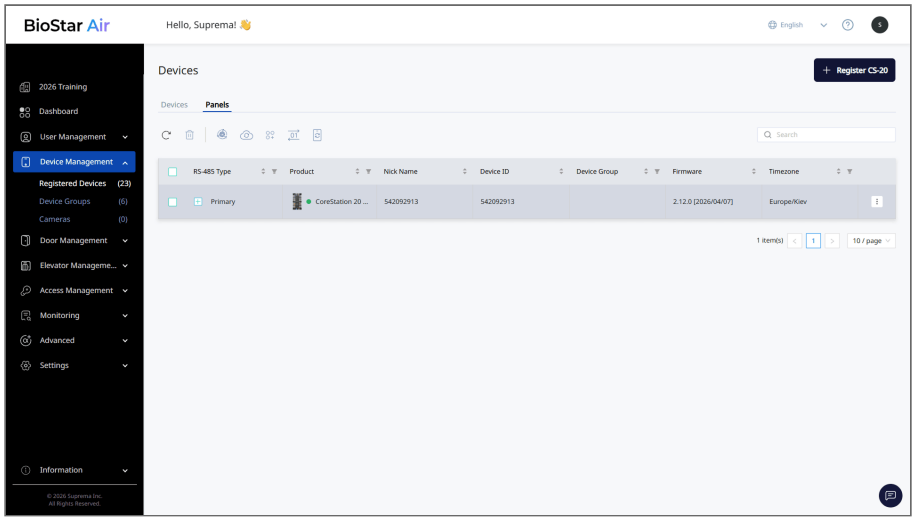
> **Precaución**
> Después de presionar el botón **INIT**, dispone de una ventana de 5 minutos para completar el registro del CS-20.

5. Ingrese el número de serie.



6. Después de ingresar el número de serie completo, haga clic en **Registrar**.

Una vez completado el registro, el sistema establece automáticamente una conexión segura y muestra el nuevo CS-20 en la lista de paneles. Si el registro es exitoso, aparece un punto verde junto al nombre del dispositivo.



> **Consejo**
>
> Para obtener el mejor rendimiento, confiabilidad y acceso a las funciones más recientes, asegúrese de buscar actualizaciones de firmware tan pronto como se registren los dispositivos. Es posible que haya firmware nuevo disponible entre el momento en que el dispositivo se empaquetó y se instaló. Para obtener más información sobre las actualizaciones de firmware, consulte Actualizar Firmware.

> **Información**
>
> Para más información sobre el proceso de registro del CS-20, consulte **Ver Guía de Registro CS-20**.

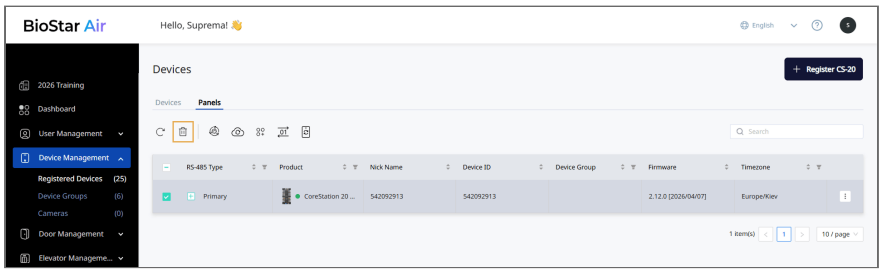
Eliminar panel

Sigue estos pasos para eliminar un panel inscrito en BioStar Air. Los paneles eliminados no se pueden recuperar. Antes de eliminar un panel, confirma que los dispositivos periféricos conectados a él ya no son necesarios.

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haga clic en la pestaña **Paneles**.

3. En la lista, marque la casilla del panel que eliminará.

4. Haz clic en en la parte superior izquierda de la pantalla.



5. Cuando aparezca la ventana emergente, haga clic en **Confirmar**.

> **Precaución**
>
> Si necesita reutilizar los dispositivos periféricos conectados, elimine esos dispositivos antes de eliminar el panel, ya que la clave SCB puede estar vinculada.

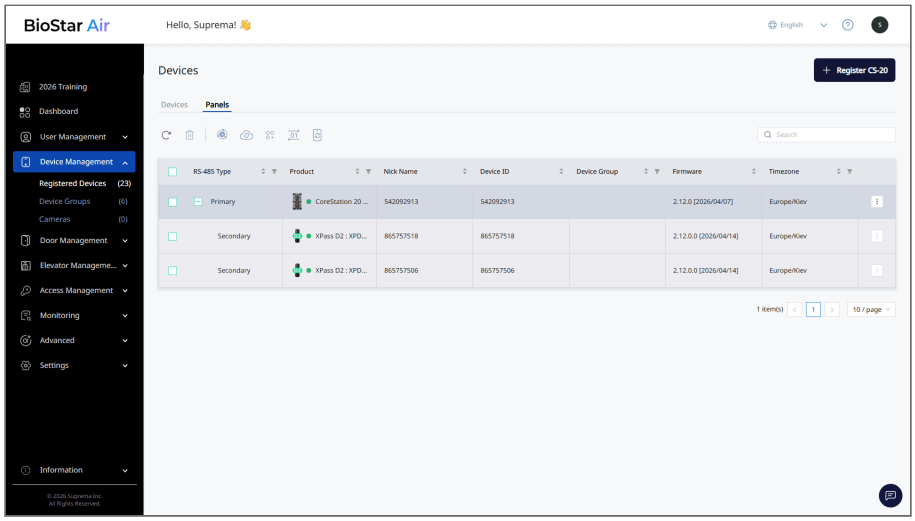
Administrar Paneles Registrados

Administra todos los paneles registrados en BioStar Air desde un único lugar. Supervisa el estado de cada panel, edita la información según sea necesario, organiza los paneles en grupos y actualiza el firmware. Este documento cubre todas las funciones necesarias, desde ver la lista de paneles hasta administrar grupos.

> **Información**
>
> En BioStar Air, los dispositivos se clasifican como primarios, que actúan como controladores, y secundarios, que se conectan a los controladores. Algunos sistemas usan los términos Master/Slave para este concepto, pero la documentación de BioStar Air no emplea esos términos.

Ver la lista de paneles

Administra los paneles registrados desde la pestaña **Paneles**. La lista de paneles proporciona información clave de un vistazo, incluyendo el tipo y el estado de cada panel o dispositivo secundario, el nombre, la ID, el grupo, el firmware y la zona horaria.



Estado de paneles y dispositivos

Comprueba el estado de conexión de cada panel o dispositivo secundario mediante los iconos de estado en la lista de paneles.

- 🟢 **Verde**: El panel o dispositivo secundario está en línea, puede controlarse de forma remota y puede actualizarse.
- 🔴 **Rojo**: El panel o dispositivo secundario está fuera de línea.
- 🟠 **Naranja**: Se está actualizando el firmware.
- ⚠️ **Advertencia**: Se requiere sincronización entre el servidor y el panel o dispositivo auxiliar. Consulte Resincronizar paneles sin conexión y dispositivos secundarios para ver las instrucciones de resincronización.

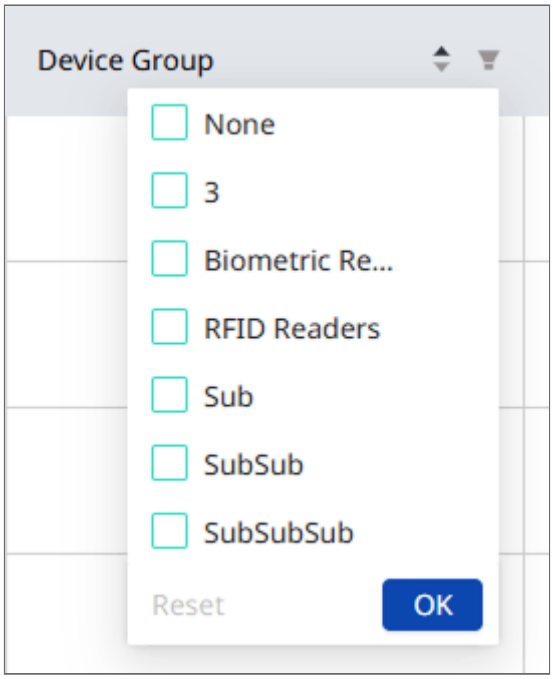
Información de paneles y dispositivos

Cada columna de la lista de paneles incluye la siguiente información.

- **RS-485 Tipos**: Indica los paneles o dispositivos secundarios que admiten la comunicación RS-485. Indica si el dispositivo es primario o secundario.
- **Producto**: El nombre, el modelo y el estado del panel o dispositivo secundario obtenidos de la base de datos de Suprema.
- **Apodo**: Campo editable por el usuario para facilitar la identificación. Edite la información en la ventana que aparece al hacer clic en un panel o subdispositivo en la lista.
- **Identificación del dispositivo**: El identificador único asignado al panel o subdispositivo.
- **Grupo de dispositivos**: El grupo al que pertenece el panel.
- **Firmware**: La versión de firmware instalada actualmente.
- **Zona horaria**: La zona horaria configurada en el panel o subdispositivo.

Filtrar

Use el filtro en el encabezado de la lista de paneles. Haga clic en en el encabezado para establecer las condiciones deseadas.

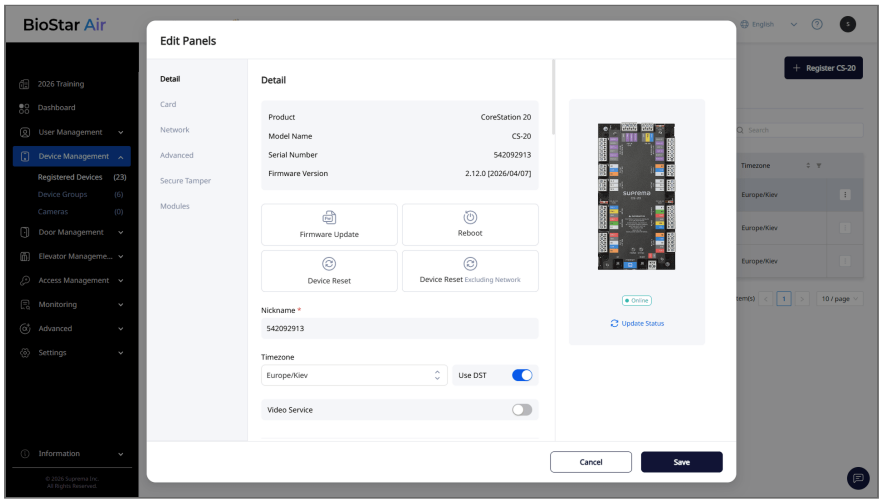


Información

Para restablecer los filtros aplicados, haga clic en y seleccione **Restablecer**.

Editar información del panel

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haga clic en la pestaña **Paneles**.
3. Haga clic en el panel cuya información desea editar en la lista para abrir la ventana **Editar Paneles**.

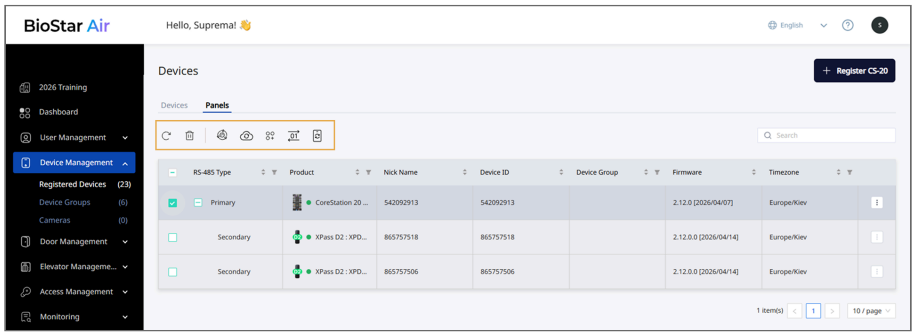


4. Edite los detalles o ajustes del panel.
5. Haz clic en **Guardar** en la parte inferior para guardar los cambios.

> **Información**
>
> Para obtener más información sobre cómo editar campos y configurar las opciones de cada sección, consulta Opciones de Configuración de Dispositivos y Paneles.

Funciones de administración de paneles

Selecciona un panel en la lista para usar las funciones de administración en la parte superior.



- : Actualizar la lista.
- : Eliminar paneles o subdispositivos registrados.
- : Actualizar el firmware de los paneles o subdispositivos seleccionados en la lista. Para más información sobre las actualizaciones de firmware, consulte Actualizar Firmware.

  > – Los subdispositivos conectados a un CS-20 se pueden actualizar uno a la vez.
  > – Para más información sobre la actualización de dispositivos XPass D2, consulte Actualizar Firmware.

- : Sincronizar las plantillas biométricas de los paneles seleccionados con el servidor.
- : Asignar los paneles seleccionados a un grupo. Para más información sobre la gestión de grupos, consulte Gestionar grupos de paneles.
- : Cambiar el orden de bytes de la tarjeta RF del panel seleccionado en la lista a **MSB** o **LSB**.
  - **MSB**: Procesa los datos de la tarjeta en orden de unidades de byte grandes a pequeñas, almacenando secuencialmente el número de serie de la tarjeta (CSN) de izquierda a derecha.
  - **LSB**: Procesa los datos de la tarjeta en orden de unidades de byte pequeñas a grandes, almacenando el número de serie de la tarjeta (CSN).
- : Importar los ajustes configurados originalmente en modo autónomo.
- : Actualizar el estado de los paneles seleccionados.

> **Información**
>
> Los subdispositivos conectados a un CS-20 solo admiten las funciones de actualización (), eliminación () y actualización de firmware ().

Resincronizar paneles sin conexión y dispositivos secundarios

Si un panel o dispositivo auxiliar ha estado sin conexión durante mucho tiempo, su información puede desincronizarse con el servidor y requerir una resincronización manual.

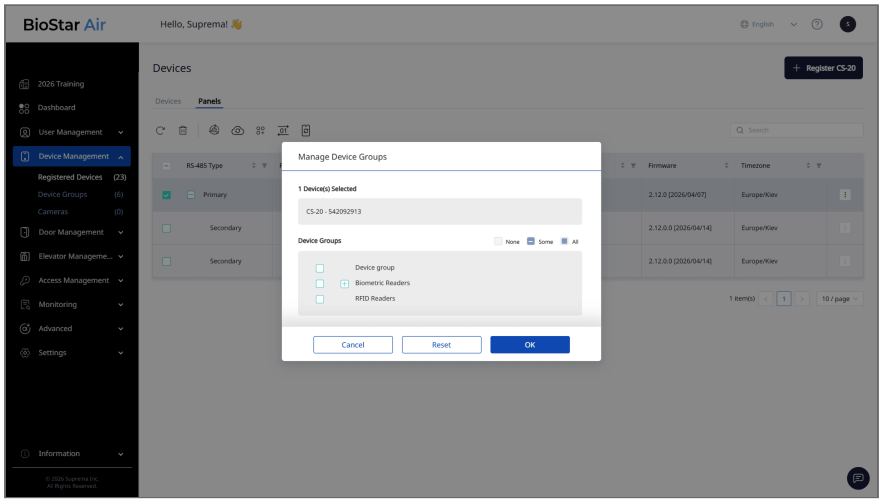
1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haga clic en la pestaña **Paneles**.
3. En la lista, revise el panel o dispositivo auxiliar con el icono ⚠ en la columna **Producto**.
4. Seleccione la casilla del panel o dispositivo auxiliar.
5. En la barra de herramientas, en la parte superior de la lista, haga clic en el botón .

> **Información**
> Los paneles o dispositivos auxiliares que han estado sin conexión durante menos de 7 días se sincronizan automáticamente cuando se reconectan, así que no se requiere ninguna acción.

Gestionar grupos de paneles

Seleccione paneles individuales en la lista para agregarlos o eliminarlos de un grupo.

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haga clic en la pestaña **Paneles**.
3. En la lista de paneles, marque la casilla del panel que desea agregar o quitar de un grupo.
4. Haga clic en en la parte superior de la lista de paneles.
5. Cuando aparezca la ventana **Administrar grupos de dispositivos**, agregue los paneles seleccionados a un grupo o elimínelos de él.



Las casillas de verificación de **Grupos de dispositivos** tienen los siguientes significados:

- **Ninguna**: Elimina los paneles seleccionados del grupo.
- **Alguno**: Algunos de los paneles seleccionados están en el grupo.
- **Todos**: Agrega los paneles seleccionados al grupo.

6. Haz clic en **OK** para guardar los cambios.

> **Información**
>
> - Seleccionar otro grupo en la ventana **Administrar grupos de dispositivos** mueve los paneles seleccionados a ese grupo.
> - Un panel puede pertenecer a varios grupos. Un mismo panel puede asignarse a varios grupos.
> - Los dispositivos secundarios en la lista de paneles solo admiten actualizaciones de firmware.
> - Haz clic en **Restablecer** para restablecer los cambios.

Agregar y Administrar Dispositivos en el Panel

BioStar Air conecta varios tipos de dispositivos secundarios al panel primario CS-20. El soporte para RS-485, OSDP y Wiegand permite integrarlos fácilmente con los sistemas de seguridad existentes. Este artículo explica cómo configurar, administrar y eliminar dispositivos secundarios.

Configurar dispositivos secundarios

Después de registrar el CS-20, configure los dispositivos secundarios usando uno de los siguientes métodos:

Dispositivos secundarios	Descripción
Dispositivos Suprema RS-485	Conecte XPass D2 y OM-120 mediante el cableado RS-485 existente y protocolos de comunicación estándar.
Dispositivo OSDP	Utiliza un protocolo de comunicación con mayor seguridad.
Dispositivo Wiegand	Dispositivos compatibles con Wiegand existentes, como lectores de tarjetas.

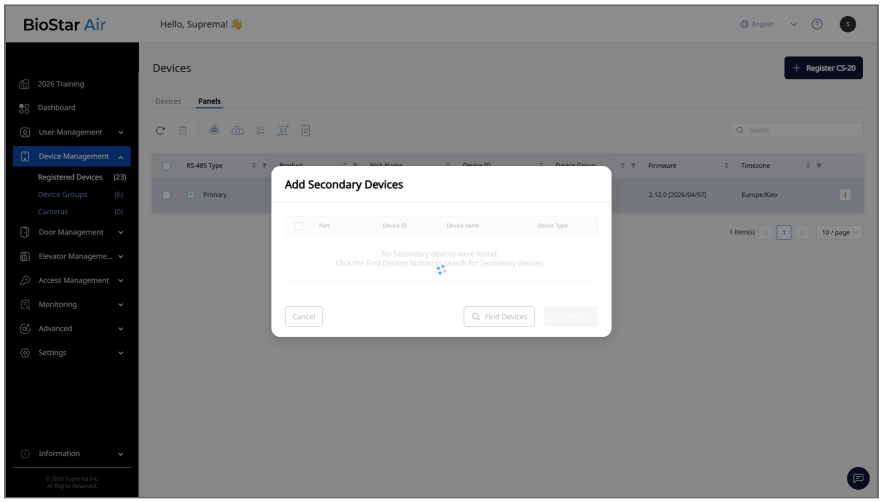
Configurar dispositivos secundarios

Conecte los dispositivos que admiten comunicación RS-485 al CS-20 para configurarlos como dispositivos secundarios. Los dispositivos secundarios aparecen anidados bajo el CS-20 en la lista de paneles.

1. En la lista de paneles, haga clic en ⋮ en el extremo derecho del panel CS-20 registrado.



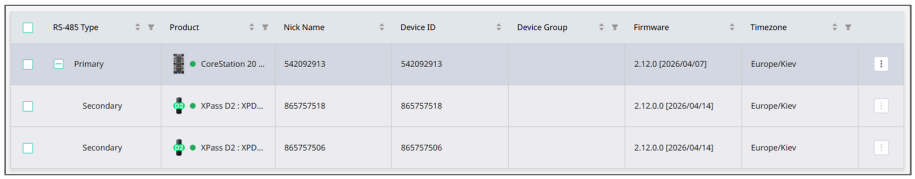
2. Haga clic en **Agregar Dispositivos Secundarios** para abrir la ventana **Agregar Dispositivos Secundarios**.



> Si no se encuentran dispositivos secundarios, haga clic en **Buscar Dispositivos** para volver a escanear los dispositivos conectados al CS-20.

3. Cuando los dispositivos secundarios conectados aparezcan en la lista, marque la casilla junto a cada dispositivo para seleccionar los que desea agregar.
4. Una vez completadas las selecciones, haga clic en **Agregar**.

Los dispositivos secundarios conectados aparecen anidados bajo el CS-20. Vea todos los dispositivos conectados al CS-20 de un vistazo en la lista de paneles.



> **Consejo**
>
> Para obtener el mejor rendimiento, confiabilidad y acceso a las funciones más recientes, asegúrese de buscar actualizaciones de firmware tan pronto como se registren los dispositivos. Es posible que haya firmware nuevo disponible entre el momento en que el dispositivo se empaquetó y se instaló. Para obtener más información sobre las actualizaciones de firmware, consulte Actualizar Firmware.

> **Información**
>
> - Para obtener más información sobre la edición y administración de dispositivos secundarios, consulte Administrar Dispositivos Edge Registrados.
> - Para obtener más información sobre los campos y ajustes de dispositivos secundarios, consulte Opciones de Configuración de Dispositivos y Paneles.
> - Para más información sobre la actualización de dispositivos XPass D2, consulte Actualizar Firmware.

Configurar dispositivos OSDP

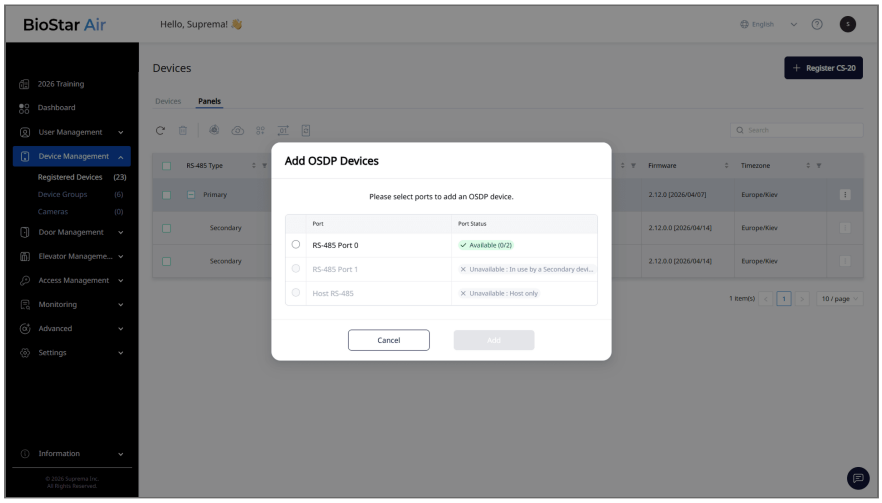
OSDP (Open Supervised Device Protocol) es un protocolo de comunicación mejorado para seguridad. En entornos que requieren alta seguridad, conecte dispositivos compatibles con OSDP al CS-20.

1. En la lista de paneles, haga clic en ⋮ en el extremo derecho del panel CS-20 registrado.



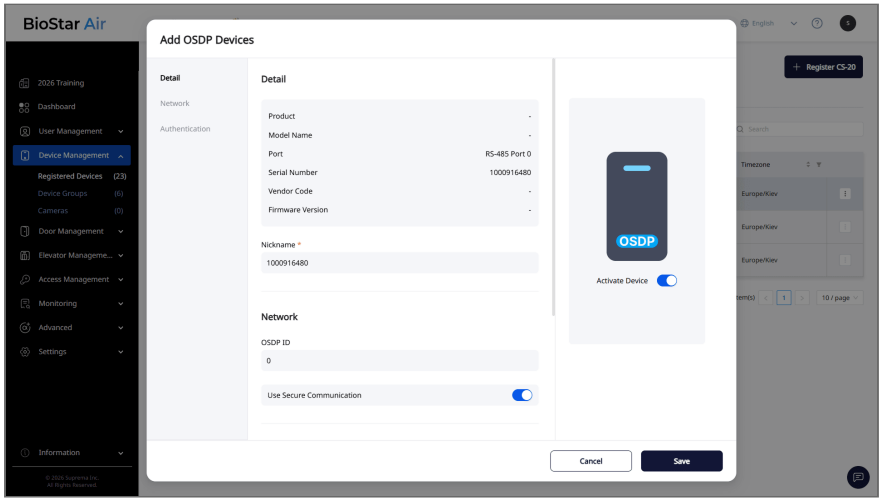
2. Haga clic en **Agregar Dispositivos OSDP** en el menú emergente.

3. Cuando aparezca la ventana **Agregar Dispositivos OSDP**, seleccione el puerto al que desea agregar el dispositivo.



4. Después de seleccionar un puerto, haga clic en **Agregar**.

5. Tras completar los ajustes requeridos en la ventana **Agregar Dispositivos OSDP**, haga clic en **Guardar**.



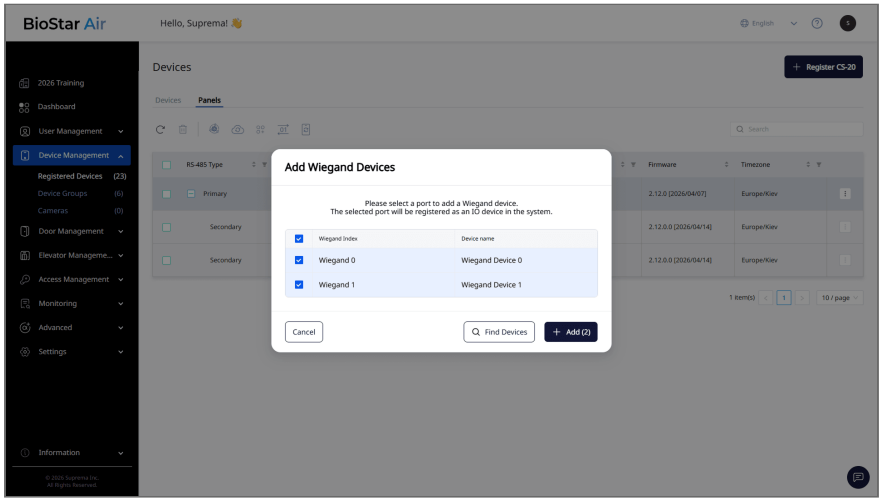
Configurar dispositivos Wiegand

Wiegand es un protocolo de comunicación ampliamente utilizado en sistemas de control de acceso. Conecte un dispositivo Wiegand al CS-20 para configurarlo como un dispositivo secundario Wiegand.

1. En la lista de paneles, haga clic en ⋮ en el extremo derecho del panel CS-20 registrado.



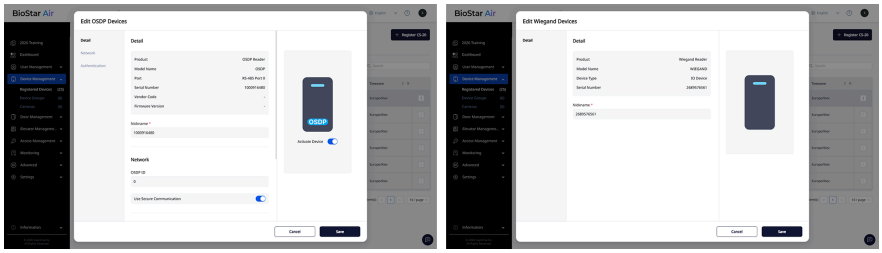
2. En el menú emergente, haga clic en **Agregar Dispositivos Wiegand**.
3. Cuando aparezca la ventana **Agregar Dispositivos Wiegand**, seleccione un puerto para añadir un dispositivo.



4. Después de seleccionar un puerto, haga clic en **Agregar**.

Editar información de dispositivos OSDP/Wiegand

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haga clic en la pestaña **Paneles**.
3. Haga clic en el icono + del dispositivo primario en la lista para expandir la lista de dispositivos secundarios conectados.
4. Haga clic en el dispositivo secundario OSDP o Wiegand para editar su información.
5. Cuando aparezca la ventana Editar información del dispositivo, edite los detalles o ajustes.



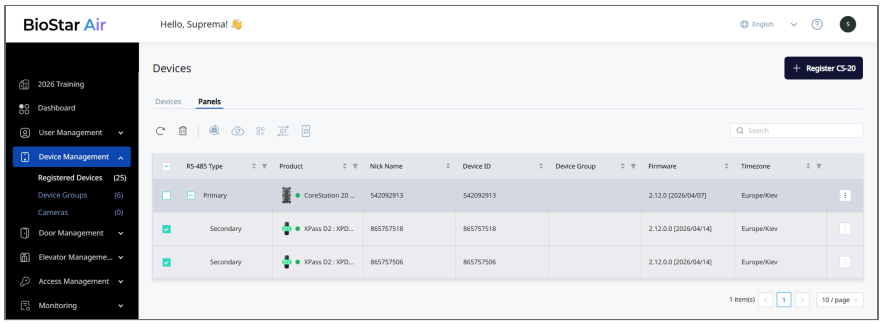
- Dispositivo OSDP: Establezca el nombre del dispositivo, los ajustes de red, los ajustes de autenticación (RF Card, RF Card + PIN) y el tiempo de espera de autenticación.
- Dispositivo Wiegand: Edite el nombre del dispositivo.

6. Haz clic en **Guardar** en la parte inferior para guardar los cambios.

Eliminar dispositivos secundarios

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haga clic en la pestaña **Paneles**.
3. Haga clic en el icono + del dispositivo primario en la lista para expandir la lista de dispositivos secundarios conectados.
4. Marque la casilla del dispositivo secundario que desea eliminar.

5. Haga clic en el botón en la parte superior de la lista.



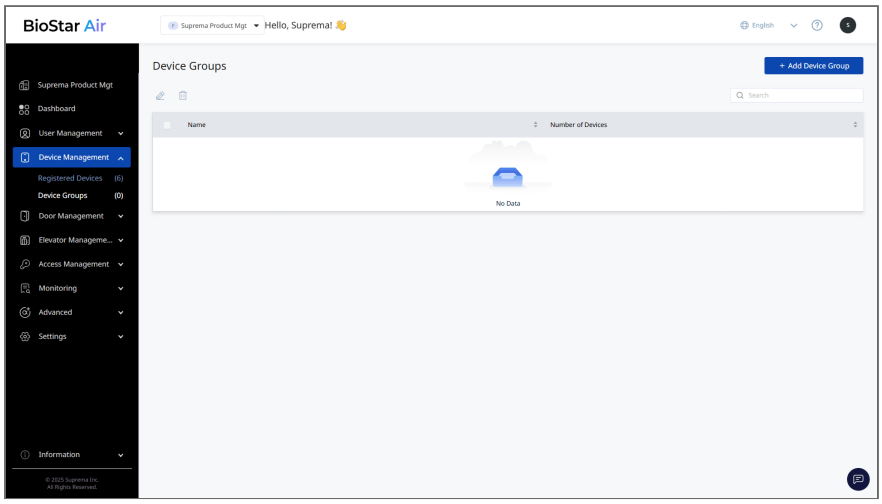
6. Cuando aparezca la ventana emergente, haga clic en **Confirmar**.

Gestionar Grupos de Dispositivos y Paneles

BioStar Air permite gestionar eficientemente múltiples dispositivos y paneles mediante grupos. Los grupos de dispositivos permiten aplicar el mismo ajuste a varios dispositivos a la vez o supervisar fácilmente el estado de los dispositivos de un grupo determinado.

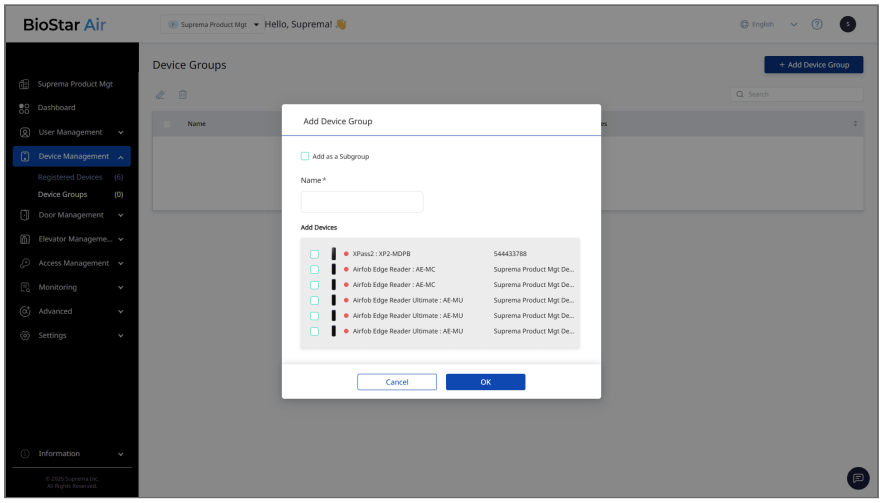
Agregar un grupo de dispositivos

1. Haga clic en **Gestión de dispositivos** → **Grupos de dispositivos** en la barra lateral izquierda.



2. Haga clic en **Agregar grupos de dispositivos** en la parte superior derecha de la pantalla.

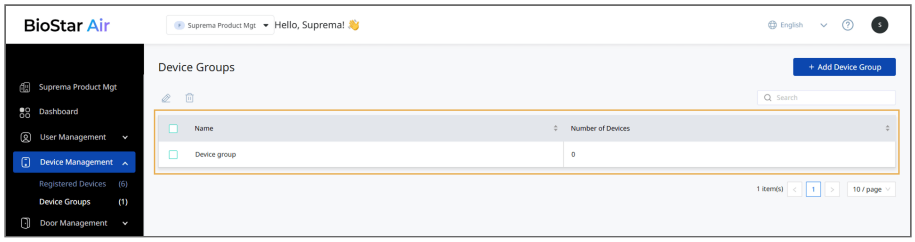
3. Cuando aparezca la ventana **Agregar grupo de dispositivos**, ingrese el nombre del grupo.



> Haga clic en **Agregar como un subgrupo** y luego seleccione el grupo principal para agregar el grupo de dispositivos como subgrupo.

4. En **Agregar dispositivos**, seleccione los dispositivos que desea incluir en el grupo.
5. Después de seleccionar todos los dispositivos, haga clic en **OK**.

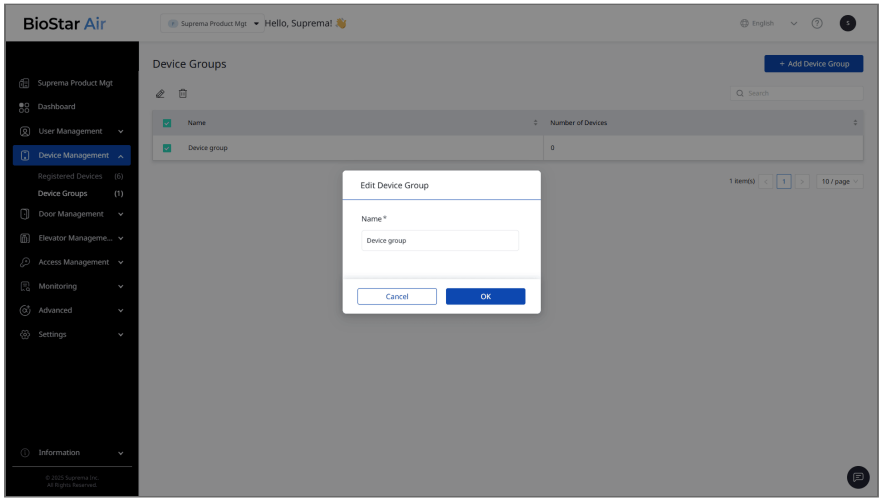
La lista de grupos de dispositivos muestra el grupo recién agregado y la cantidad de dispositivos que contiene. Haga clic en un grupo de dispositivos para ver los dispositivos que forman parte de ese grupo.



> **Información**
>
> Para obtener más información sobre cómo agregar dispositivos a un grupo o eliminarlos de un grupo existente, consulte Administrar Dispositivos Edge Registrados.

Cambiar el nombre de un grupo de dispositivos

1. Haga clic en **Gestión de dispositivos** → **Grupos de dispositivos** en la barra lateral izquierda.
2. Seleccione la casilla del grupo de dispositivos que desea renombrar.
3. Haga clic en en la parte superior de la lista de grupos de dispositivos.
4. Cuando aparezca la ventana **Editar grupo de dispositivos**, ingrese el nuevo nombre del grupo.



5. Haga clic en **OK** para guardar el nuevo nombre del grupo.

Eliminar un grupo de dispositivos

1. Haga clic en **Gestión de dispositivos** → **Grupos de dispositivos** en la barra lateral izquierda.

2. Seleccione la casilla del grupo de dispositivos que desea eliminar.
3. Haga clic en 🗑 en la parte superior de la lista de grupos de dispositivos.
4. Cuando aparezca un mensaje de advertencia, haga clic en **Sí**.

El grupo de dispositivos seleccionado se elimina de la lista. Sus subgrupos también se eliminan. Eliminar un grupo no elimina los dispositivos.

Usar Edge Readers como Dispositivos Primarios

Configure XPass 2 como dispositivo primario para conectar XPass D2 como dispositivo secundario. Gestione toda la lógica de control de acceso en XPass 2. Configure una puerta con dispositivos de entrada y salida sin requerir dos conexiones de red.

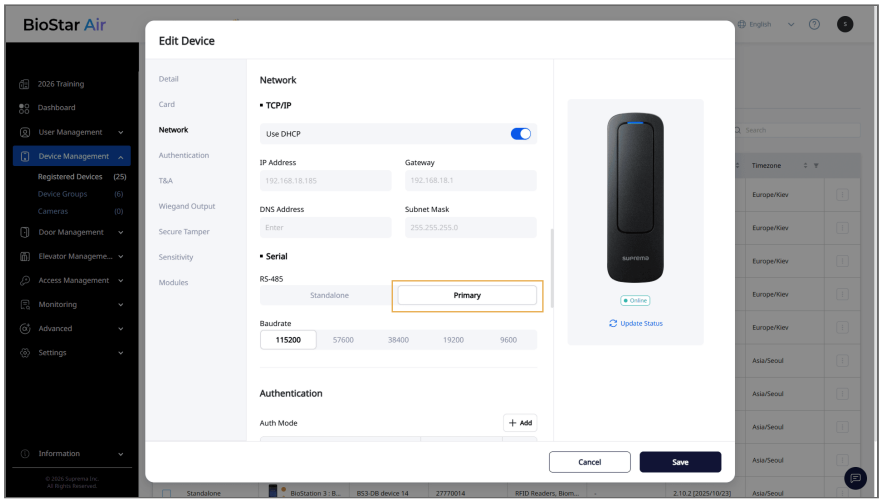
Este documento ofrece instrucciones paso a paso para configurar XPass 2 como dispositivo primario y conectar XPass D2 como dispositivo secundario. También explica las características compatibles y las limitaciones de la configuración primario-secundario.

Antes de comenzar

Actualice el firmware a la versión 2.12 o posterior antes de configurar XPass 2 como dispositivo primario. Para obtener más información sobre las actualizaciones de firmware, consulte Actualizar Firmware.

Configurar XPass 2 como dispositivo primario

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. En la lista de dispositivos, haz clic en XPass 2.
3. Cuando aparezca la ventana **Editar dispositivo**, ve a la sección **Red**.
4. Cambia el ajuste **RS-485** a **Primario**.

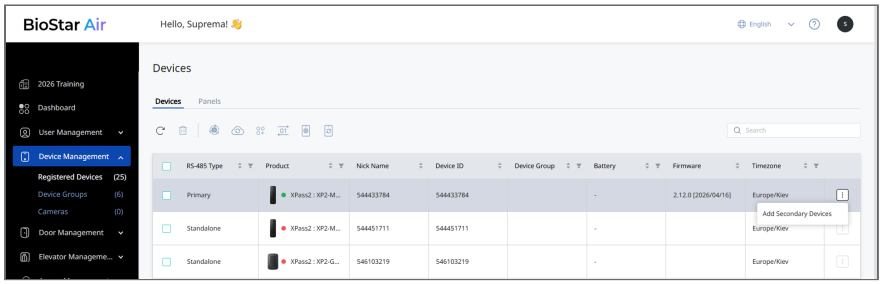


5. Haz clic en **Guardar** en la parte inferior para guardar los cambios.

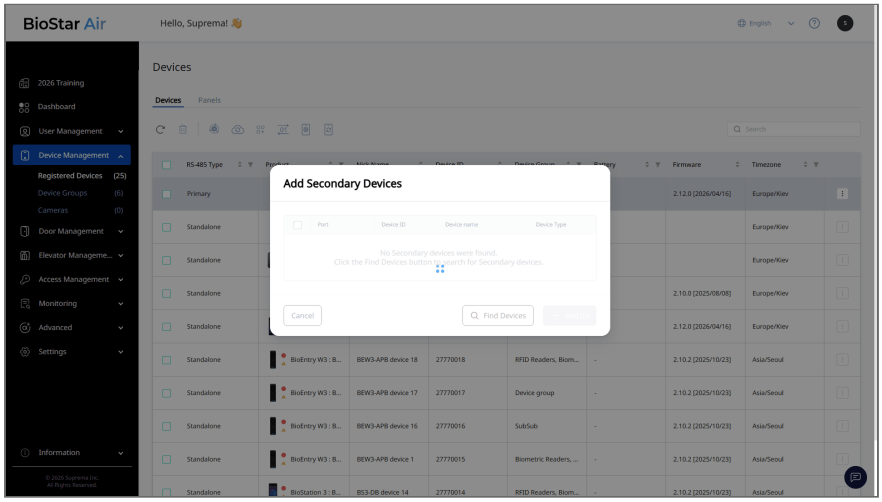
Agregar un dispositivo secundario

Agregue un dispositivo secundario como XPass D2 o Secure I/O 2 (SIO2).

1. En la lista de dispositivos, haga clic en ⋮ en el extremo derecho del XPass 2 configurado como dispositivo primario.



2. Haga clic en **Agregar Dispositivos Secundarios** para abrir la ventana **Agregar Dispositivos Secundarios**.



> Si no se encuentran dispositivos secundarios, haga clic en **Buscar Dispositivos** para buscar nuevamente dispositivos conectados a XPass 2.

3. Cuando los dispositivos secundarios conectados aparezcan en la lista, marque la casilla junto a cada dispositivo que agregará.

4. Una vez completadas las selecciones, haga clic en **Agregar**.

Los dispositivos secundarios conectados aparecen de forma jerárquica debajo de XPass 2. Vea todos los dispositivos conectados a XPass 2 de un vistazo en la lista del panel.

> **Información**
>
> - Para obtener más información sobre XPass D2, consulte la guía de instalación de XPass D2.
> - Un XPass 2 configurado como dispositivo primario puede tener hasta 31 dispositivos secundarios asignados.
> - Para más información sobre Secure I/O 2 (SIO2), consulte la guía de instalación de Secure I/O 2.

Opciones de Configuración de Dispositivos y Paneles

Este documento es una referencia para los ajustes de dispositivos y paneles en BioStar Air. Los administradores pueden ver información básica del hardware y ejecutar acciones como actualizar el firmware, reiniciar o restablecer. Pueden configurar ajustes de operación como red, autenticación, formato de tarjeta, registro de tiempo y asistencia, Wiegand, sensibilidad y módulos conectados. Los ajustes disponibles varían según el modelo de dispositivo y el tipo de panel.

▼ AirFob Edge

Detalle

La sección **Detalle** proporciona información básica — como el nombre del dispositivo, el modelo, el número de serie y la versión de firmware — e incluye un menú de acciones para controlar funciones y ajustes predeterminados.

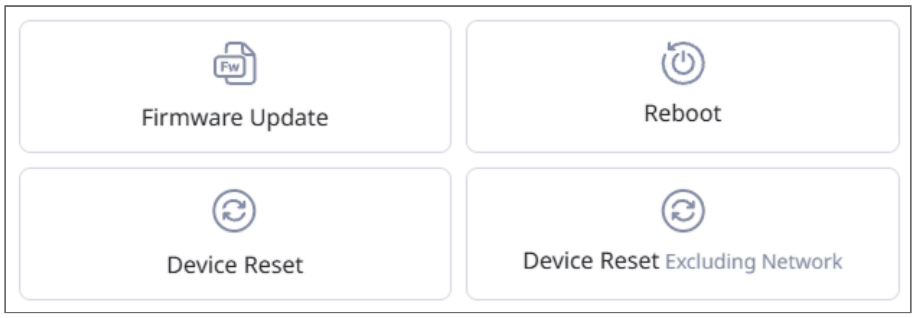
Información básica

Vea la información básica del dispositivo. Esta información no se puede editar.

- **Producto**: El nombre del producto.
- **Nombre del modelo**: El nombre del modelo del dispositivo.
- **Número de serie**: El número de serie del dispositivo.
- **Versión de Firmware**: La versión de firmware instalada en el dispositivo.

Acciones

La función **Acción** te permite controlar las funciones del dispositivo.



- **Actualización de firmware**: Actualice el firmware del dispositivo a la versión más reciente.
- **Reiniciar**: Reinicie el dispositivo de forma remota cuando ocurra un problema o anomalía.
- **Dispositivo Reiniciado**: Inicialice todos los ajustes almacenados en el dispositivo. Esta acción elimina todos los ajustes y datos del dispositivo.
- **Dispositivo Reiniciado Excluida la red**: Inicialice todos los ajustes excepto la configuración de red. Esta acción elimina todos los ajustes y datos, pero conserva la configuración de red.

Ajustes iniciales

Modifique los ajustes predeterminados del dispositivo.

- **Apodo**: El alias que aparece en la lista de dispositivos y en los registros. Puede editar este campo directamente.
- **Zona horaria**: Establezca la zona horaria del dispositivo para mantener los registros consistentes cuando los relojes del sitio y del dispositivo difieran. Active la opción **Usar DST** para aplicar el horario de verano (DST).
- **Manos Libres**: Amplíe el alcance BLE.
- **Lector QR**: Confirme que un lector QR RS-485 esté conectado al dispositivo.

> – Cuando un lector QR esté conectado al dispositivo, no se puede usar otro dispositivo RS-485.
> – Si utiliza un SIO2, no podrá usar un lector QR en el dispositivo conectado a esa puerta.

- **Tarjeta NFC/RF**: Active o desactive la autenticación por tarjeta. Se admiten los formatos de tarjeta DESFire y Felica.
- **Configuración del pitido**: Configure el pitido de confirmación para la autenticación de acceso.

Tarjetas propietarias

Para tarjetas Wiegand, seleccione **iClass (SE / SEOS)** y **HID Prox**. Haga clic en el interruptor para activar la función y luego seleccione el formato de tarjeta deseado en **Tarjetas propietarias**.

> **Información**
>
> - La compatibilidad puede variar según el dispositivo.
> - Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Red

Modifique la configuración de red del dispositivo.

- **Configuración de la red**: Configure el dispositivo para obtener una dirección IP automáticamente.

  Para configurar la red manualmente, desactive **Configuración de la red** y complete los siguientes campos.
  - **Usar DHCP**
  - **Dirección IP**
  - **Entrada**
  - **Dirección DNS**

T&A(Tiempo y asistencia, T&A)

Cuando esta función esté habilitada, **Evento T&A** se registra en el **Registro de eventos** y se utiliza en **Informe de tiempo y asistencia**.

- **Usar T&A**: Haga clic en el interruptor para activar o desactivar la gestión de asistencia.
- **Modo T&A**: Seleccione el modo de asistencia deseado.
  - **Por horario**: Los eventos de asistencia cambian automáticamente según el horario establecido. Puede seleccionar un horario para aplicarlo a los eventos de asistencia.
  - **Fijado**: Solo se puede usar el evento de asistencia seleccionado.
  - **Móvil**: Al presentar una credencial móvil, la app Suprema Pass permite al usuario seleccionar el evento de asistencia.

> **Información**
>
> Para más información sobre la configuración de tiempo y asistencia, consulte Tiempo y asistencia (T&A).

Salida Wiegand

Esta función se integra con sistemas externos (por ejemplo, paneles de alarma). Activa la opción **Usar salida Wiegand** para usar esta función.

- **Modo de salida**: Configura el modo de salida de la señal Wiegand.
  - **Regular**: Escanea tarjetas usando el formato Wiegand configurado.
    - **Usar código de fallo**: Puede establecer códigos de error y elegir el valor a enviar cuando falle la autenticación de la tarjeta Wiegand.
  - **Omitir**: Envía el CSN independientemente de la autenticación Wiegand. Activa esta opción si lo usas como un dispositivo sin función de control de puertas.
- **Información de salida**: Selecciona la información que se enviará durante la autenticación.
- **Ancho de pulso**: Establece el ancho de pulso para la señal Wiegand.
- **Intervalo de pulso**: Establece el intervalo de pulso para la señal Wiegand.
- **Etiqueta móvil consecutiva**: Etiqueta tarjetas móviles consecutivamente sin tiempo de espera.
- **Límite de etiquetas consecutivas**: Define el número máximo de etiquetas consecutivas para tarjetas móviles.

> **Información**
> La función **Etiqueta móvil consecutiva** es compatible con la app Suprema Pass 2.9.0 o posterior.

Sensibilidad

Ajuste el valor RSSI para definir qué tan cerca debe estar el dispositivo móvil para desbloquear la puerta.



- Los valores más bajos ayudan a evitar activaciones no deseadas.
- Los valores más altos mejoran la detección en entornos con mucha interferencia.

> **Información**
> Para restablecer la configuración, haga clic en **Restablecer**.

Módulos

Opción para detectar un módulo OM-120 conectado al dispositivo. Haga clic en **Agregar** para detectar el módulo.

▼ XPass 2

Detalle

La sección **Detalle** proporciona información básica — como el nombre del dispositivo, el modelo, el número de serie y la versión de firmware — e incluye un menú de acciones para controlar funciones y ajustes predeterminados.

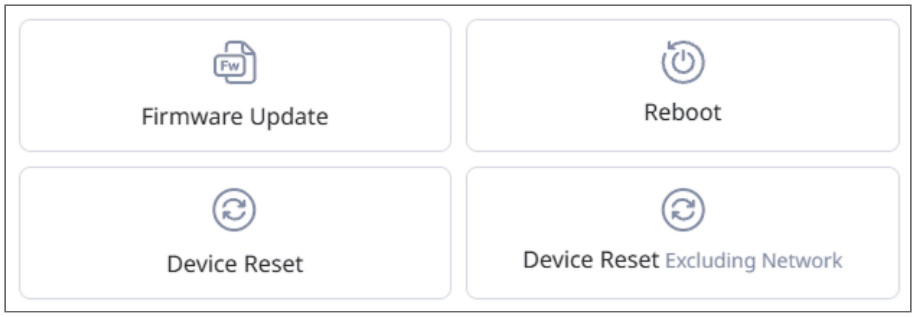
Información básica

Vea la información básica del dispositivo. Esta información no se puede editar.

- **Producto**: El nombre del producto.
- **Nombre del modelo**: El nombre del modelo del dispositivo.
- **Número de serie**: El número de serie del dispositivo.
- **Versión de Firmware**: La versión de firmware instalada en el dispositivo.

Acciones

La función **Acción** te permite controlar las funciones del dispositivo.



- **Actualización de firmware**: Actualice el firmware del dispositivo a la versión más reciente.
- **Reiniciar**: Reinicie el dispositivo de forma remota cuando ocurra un problema o anomalía.
- **Dispositivo Reiniciado**: Inicialice todos los ajustes almacenados en el dispositivo. Esta acción elimina todos los ajustes y datos del dispositivo.
- **Dispositivo Reiniciado Excluida la red**: Inicialice todos los ajustes excepto la configuración de red. Esta acción elimina todos los ajustes y datos, pero conserva la configuración de red.

Ajustes iniciales

Modifique los ajustes predeterminados del dispositivo.

- **Apodo**: El alias que aparece en la lista de dispositivos y en los registros. Puede editar este campo directamente.
- **Zona horaria**: Establezca la zona horaria del dispositivo para mantener los registros consistentes cuando los relojes del sitio y del dispositivo difieran. Active la opción **Usar DST** para aplicar el horario de verano (DST).
- **Número de tarjeta RFID como PIN**: Ingrese el número de la tarjeta RF mediante el teclado para poder usarla.

> Esta función es compatible únicamente con el modelo **XP2-GKDPB**, que tiene un teclado.

- **Manos Libres**: Amplíe el alcance BLE.
- **Lector QR**: Confirme que un lector QR RS-485 esté conectado al dispositivo.

  > – Cuando un lector QR esté conectado al dispositivo, no se puede usar otro dispositivo RS-485.
  > – Si utiliza un SIO2, no podrá usar un lector QR en el dispositivo conectado a esa puerta.

- **Configuración del pitido**: Configure el pitido de confirmación para la autenticación de acceso.
- **Servicio de Video**: Conecte cámaras IP al dispositivo para ver video en vivo y grabado. Para más información sobre los ajustes de conexión de cámaras IP, consulte Soporte y configuración de cámaras IP.

Tarjeta

En la sección **Tarjeta** puede modificar los ajustes de autenticación por tarjeta.

Tarjeta NFC/RF

- **Tarjeta NFC/RF**: Haga clic en el interruptor para activar o desactivar la autenticación de acceso por tarjeta. Seleccione los tipos de tarjeta compatibles.
  – **EM4100 (125 KHz)**
  – **Mifare Classic/Mifare DESFire/FeliCa**
- **Orden de bytes**
  – **MSB**: Procesa los datos de la tarjeta en orden de unidades de byte grandes a pequeñas, almacenando secuencialmente el número de serie de la tarjeta (CSN) de izquierda a derecha.
  – **LSB**: Procesa los datos de la tarjeta en orden de unidades de byte pequeñas a grandes, almacenando el número de serie de la tarjeta (CSN).
- **Método de lectura de datos**: Seleccione CSN (predeterminado) o el formato Wiegand.

  > Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Tarjetas propietarias

Para tarjetas Wiegand, seleccione **iClass (SE / SEOS)** y **HID Prox**. Haga clic en el interruptor para activar la función y luego seleccione el formato de tarjeta deseado en **Tarjetas propietarias**.

> **Información**
>
> - La compatibilidad puede variar según el dispositivo.
> - Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Red

Modifique la configuración de red del dispositivo.

- **Configuración de la red**: Configure el dispositivo para obtener una dirección IP automáticamente.

  Para configurar la red manualmente, desactive **Configuración de la red** y complete los siguientes campos.
  - **Usar DHCP**
  - **Dirección IP**
  - **Entrada**
  - **Dirección DNS**
- **RS-485**: Configure el dispositivo en modo maestro para agregar los dispositivos XPass D2 como dispositivos auxiliares.
- **Tasa de baudios**: Configure la tasa de baudios de la comunicación serial entre el dispositivo y los dispositivos auxiliares.

Autenticación

- **Modo de autenticación**: Agregue métodos de autenticación. Haga clic en **Agregar** para agregar un método de autenticación.
  - **XP2-MDPB / XP2-GDPB**: Solo se pueden seleccionar tarjetas RF como método de autenticación.
  - **XP2-GKDPB**: Puede usar una combinación de tarjeta RF y PIN como método de autenticación.
- **Tiempo de espera de autenticación**: La autenticación fallará si la credencial no se valida dentro del tiempo establecido.

> Esta función solo es compatible con el modelo **XP2-GKDPB**.

> **Información**
> Puede configurar distintos métodos de autenticación para el horario seleccionado. Por ejemplo, puede permitir únicamente la autenticación con tarjeta durante el horario laboral y permitir autenticación con tarjeta y PIN fuera del horario laboral.

T&A(Tiempo y asistencia, T&A)

Cuando esta función esté habilitada, **Evento T&A** se registra en el **Registro de eventos** y se utiliza en **Informe de tiempo y asistencia**.

- **Usar T&A**: Haga clic en el interruptor para activar o desactivar la gestión de asistencia.
- **Modo T&A**: Seleccione el modo de asistencia deseado.
  - **Por horario**: Los eventos de asistencia cambian automáticamente según el horario establecido. Puede seleccionar un horario para aplicarlo a los eventos de asistencia.
  - **Fijado**: Solo se puede usar el evento de asistencia seleccionado.
  - **Móvil**: Al presentar una credencial móvil, la app Suprema Pass permite al usuario seleccionar el evento de asistencia.

> **Información**
> Para más información sobre la configuración de tiempo y asistencia, consulte Tiempo y asistencia (T&A).

Salida Wiegand

Esta función se integra con sistemas externos (por ejemplo, paneles de alarma). Activa la opción **Usar salida Wiegand** para usar esta función.

- **Modo de salida**: Configura el modo de salida de la señal Wiegand.
  - **Regular**: Escanea tarjetas usando el formato Wiegand configurado.
    - **Usar código de fallo**: Puede establecer códigos de error y elegir el valor a enviar cuando falle la autenticación de la tarjeta Wiegand.
  - **Omitir**: Envía el CSN independientemente de la autenticación Wiegand. Activa esta opción si lo usas como un dispositivo sin función de control de puertas.
- **Información de salida**: Selecciona la información que se enviará durante la autenticación.
- **Ancho de pulso**: Establece el ancho de pulso para la señal Wiegand.
- **Intervalo de pulso**: Establece el intervalo de pulso para la señal Wiegand.
- **Etiqueta móvil consecutiva**: Etiqueta tarjetas móviles consecutivamente sin tiempo de espera.
- **Límite de etiquetas consecutivas**: Define el número máximo de etiquetas consecutivas para tarjetas móviles.

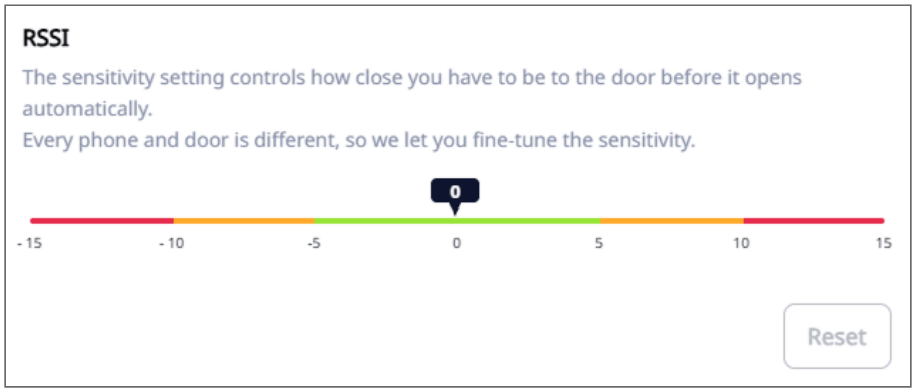
> **Información**
> La función **Etiqueta móvil consecutiva** es compatible con la app Suprema Pass 2.9.0 o posterior.

Protección contra manipulaciones seguras

Si ocurre un evento de manipulación, configure el dispositivo para eliminar **toda la información de usuario**, **todos los registros** y **las claves de seguridad** almacenadas en el dispositivo.

Sensibilidad

Ajuste el valor RSSI para definir qué tan cerca debe estar el dispositivo móvil para desbloquear la puerta.



- Los valores más bajos ayudan a evitar activaciones no deseadas.
- Los valores más altos mejoran la detección en entornos con mucha interferencia.

> **Información**
> Para restablecer la configuración, haga clic en **Restablecer**.

Módulos

Opción para detectar un módulo OM-120 conectado al dispositivo. Haga clic en **Agregar** para detectar el módulo.

▼ XPass D2

Detalle

La sección **Detalle** proporciona información básica — como el nombre del dispositivo, el modelo, el número de serie y la versión de firmware — e incluye un menú de acciones para controlar funciones y ajustes predeterminados.

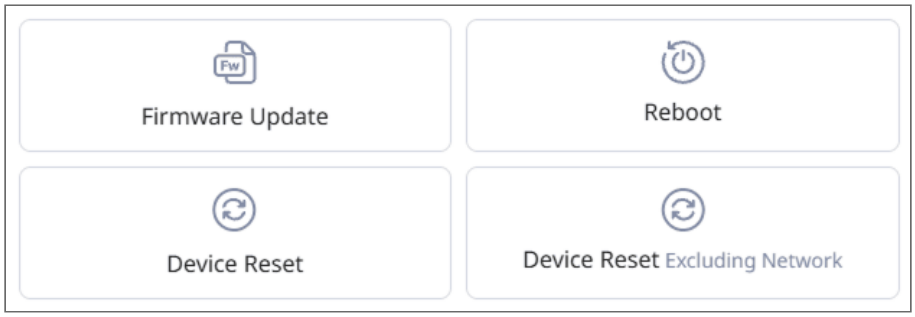
Información básica

Vea la información básica del dispositivo. Esta información no se puede editar.

- **Producto**: El nombre del producto.
- **Nombre del modelo**: El nombre del modelo del dispositivo.
- **Número de serie**: El número de serie del dispositivo.
- **Versión de Firmware**: La versión de firmware instalada en el dispositivo.

Acciones

La función **Acción** te permite controlar las funciones del dispositivo.



- **Actualización de firmware**: Actualice el firmware del dispositivo a la versión más reciente.
- **Reiniciar**: Reinicie el dispositivo de forma remota cuando ocurra un problema o anomalía.
- **Dispositivo Reiniciado**: Inicialice todos los ajustes almacenados en el dispositivo. Esta acción elimina todos los ajustes y datos del dispositivo.
- **Dispositivo Reiniciado Excluida la red**: Inicialice todos los ajustes excepto la configuración de red. Esta acción elimina todos los ajustes y datos, pero conserva la configuración de red.

Ajustes iniciales

Modifique los ajustes predeterminados del dispositivo.

- **Apodo**: El alias que aparece en la lista de dispositivos y en los registros. Puede editar este campo directamente.
- **Manos Libres**: Amplíe el alcance BLE.
- **Configuración del pitido**: Configure el pitido de confirmación para la autenticación de acceso.

Tarjeta

En la sección **Tarjeta** puede modificar los ajustes de autenticación por tarjeta.

Tarjeta NFC/RF

- **Tarjeta NFC/RF**: Haga clic en el interruptor para activar o desactivar la autenticación de acceso por tarjeta. Seleccione los tipos de tarjeta compatibles.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **Orden de bytes**
  - **MSB**: Procesa los datos de la tarjeta en orden de unidades de byte grandes a pequeñas, almacenando secuencialmente el número de serie de la tarjeta (CSN) de izquierda a derecha.
  - **LSB**: Procesa los datos de la tarjeta en orden de unidades de byte pequeñas a grandes, almacenando el número de serie de la tarjeta (CSN).
- **Método de lectura de datos**: Seleccione CSN (predeterminado) o el formato Wiegand.

> Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Tarjetas propietarias

Para tarjetas Wiegand, seleccione **iClass (SE / SEOS)** y **HID Prox**. Haga clic en el interruptor para activar la función y luego seleccione el formato de tarjeta deseado en **Tarjetas propietarias**.

Información

- La compatibilidad puede variar según el dispositivo.
- Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Autenticación

- **Modo de autenticación**: Agregue métodos de autenticación. Haga clic en **Agregar** para agregar un método de autenticación. Solo se pueden seleccionar tarjetas RF como método de autenticación.

Información

Puede configurar distintos métodos de autenticación para el horario seleccionado. Por ejemplo, puede permitir únicamente la autenticación con tarjeta durante el horario laboral y permitir autenticación con tarjeta y PIN fuera del horario laboral.

T&A(Tiempo y asistencia, T&A)

Cuando esta función esté habilitada, **Evento T&A** se registra en el **Registro de eventos** y se utiliza en **Informe de tiempo y asistencia**.

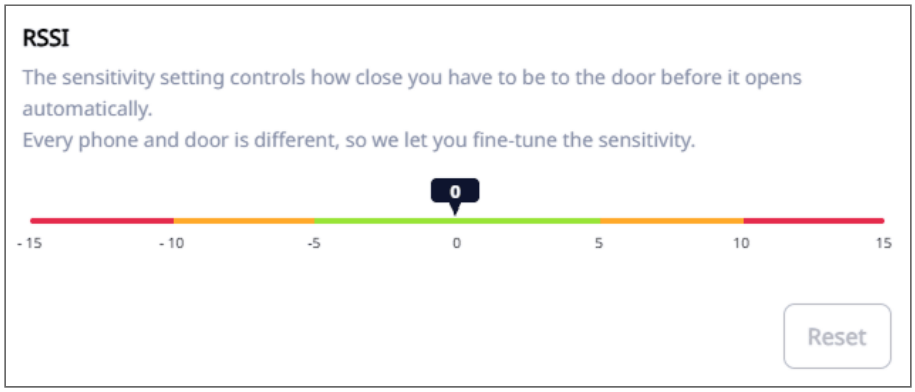
- **Usar T&A**: Haga clic en el interruptor para activar o desactivar la gestión de asistencia.
- **Modo T&A**: Seleccione el modo de asistencia deseado.
  - **Por horario**: Los eventos de asistencia cambian automáticamente según el horario establecido. Puede seleccionar un horario para aplicarlo a los eventos de asistencia.
  - **Fijado**: Solo se puede usar el evento de asistencia seleccionado.

Información

Para más información sobre la configuración de tiempo y asistencia, consulte Tiempo y asistencia (T&A).

Sensibilidad

Ajuste el valor RSSI para definir qué tan cerca debe estar el dispositivo móvil para desbloquear la puerta.



- Los valores más bajos ayudan a evitar activaciones no deseadas.
- Los valores más altos mejoran la detección en entornos con mucha interferencia.

> **Información**
> Para restablecer la configuración, haga clic en **Restablecer**.

▼ X-Station 2

Detalle

La sección **Detalle** proporciona información básica — como el nombre del dispositivo, el modelo, el número de serie y la versión de firmware — e incluye un menú de acciones para controlar funciones y ajustes predeterminados.

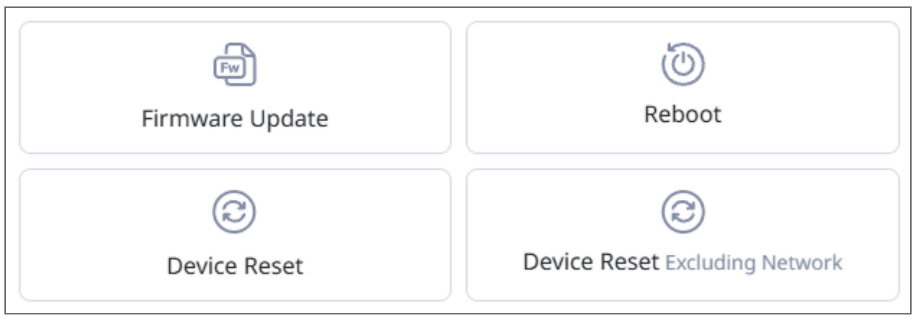
Información básica

Vea la información básica del dispositivo. Esta información no se puede editar.

- **Producto**: El nombre del producto.
- **Nombre del modelo**: El nombre del modelo del dispositivo.
- **Número de serie**: El número de serie del dispositivo.
- **Versión de Firmware**: La versión de firmware instalada en el dispositivo.

Acciones

La función **Acción** te permite controlar las funciones del dispositivo.



- **Actualización de firmware**: Actualice el firmware del dispositivo a la versión más reciente.
- **Reiniciar**: Reinicie el dispositivo de forma remota cuando ocurra un problema o anomalía.
- **Dispositivo Reiniciado**: Inicialice todos los ajustes almacenados en el dispositivo. Esta acción elimina todos los ajustes y datos del dispositivo.

- **Dispositivo Reiniciado Excluida la red**: Inicialice todos los ajustes excepto la configuración de red. Esta acción elimina todos los ajustes y datos, pero conserva la configuración de red.

Ajustes iniciales

Modifique los ajustes predeterminados del dispositivo.

- **Apodo**: El alias que aparece en la lista de dispositivos y en los registros. Puede editar este campo directamente.
- **Zona horaria**: Establezca la zona horaria del dispositivo para mantener los registros consistentes cuando los relojes del sitio y del dispositivo difieran. Active la opción **Usar DST** para aplicar el horario de verano (DST).
- **Manos Libres**: Amplíe el alcance BLE.
- **Lector QR**: Confirme que un lector QR RS-485 esté conectado al dispositivo.

  - Cuando un lector QR esté conectado al dispositivo, no se puede usar otro dispositivo RS-485.
  - Si utiliza un SIO2, no podrá usar un lector QR en el dispositivo conectado a esa puerta.

- **Tarjeta NFC/RF**: Active o desactive la autenticación por tarjeta. Se admiten los formatos de tarjeta DESFire y Felica.

Tarjetas propietarias

Para tarjetas Wiegand, seleccione **iClass (SE / SEOS)** y **HID Prox**. Haga clic en el interruptor para activar la función y luego seleccione el formato de tarjeta deseado en **Tarjetas propietarias**.

Información

- La compatibilidad puede variar según el dispositivo.
- Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Red

Modifique la configuración de red del dispositivo.

- **Configuración de la red**: Configure el dispositivo para obtener una dirección IP automáticamente.

  Para configurar la red manualmente, desactive **Configuración de la red** y complete los siguientes campos.
  - **Usar DHCP**
  - **Dirección IP**
  - **Entrada**
  - **Dirección DNS**

T&A(Tiempo y asistencia, T&A)

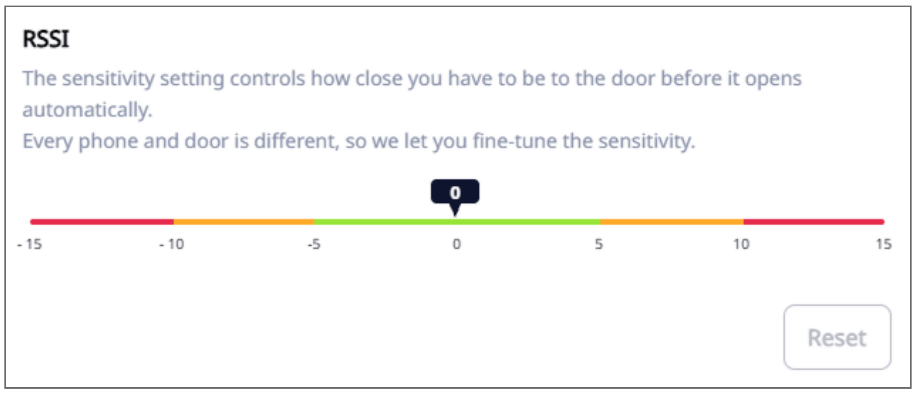
Cuando esta función esté habilitada, **Evento T&A** se registra en el **Registro de eventos** y se utiliza en **Informe de tiempo y asistencia**.

- **Usar T&A**: Haga clic en el interruptor para activar o desactivar la gestión de asistencia.
- **Modo T&A**: Seleccione el modo de asistencia deseado.
  - **Por horario**: Los eventos de asistencia cambian automáticamente según el horario establecido. Puede seleccionar un horario para aplicarlo a los eventos de asistencia.
  - **Fijado**: Solo se puede usar el evento de asistencia seleccionado.
  - **Móvil**: Al presentar una credencial móvil, la app Suprema Pass permite al usuario seleccionar el evento de asistencia.

> **Información**
> Para más información sobre la configuración de tiempo y asistencia, consulte Tiempo y asistencia (T&A).

Sensibilidad

Ajuste el valor RSSI para definir qué tan cerca debe estar el dispositivo móvil para desbloquear la puerta.



- Los valores más bajos ayudan a evitar activaciones no deseadas.
- Los valores más altos mejoran la detección en entornos con mucha interferencia.

> **Información**
> Para restablecer la configuración, haga clic en **Restablecer**.

Módulos

Opción para detectar un módulo OM-120 conectado al dispositivo. Haga clic en **Agregar** para detectar el módulo.

▼ BioEntry W3

Detalle

La sección **Detalle** proporciona información básica — como el nombre del dispositivo, el modelo, el número de serie y la versión de firmware — e incluye un menú de acciones para controlar funciones y ajustes predeterminados.

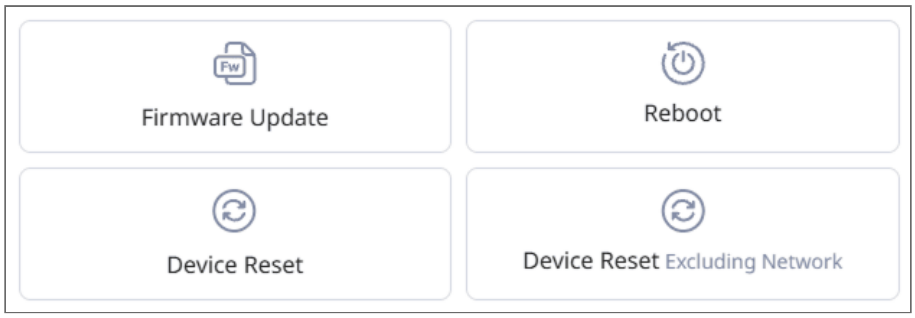
Información básica

Vea la información básica del dispositivo. Esta información no se puede editar.

- **Producto**: El nombre del producto.
- **Nombre del modelo**: El nombre del modelo del dispositivo.
- **Número de serie**: El número de serie del dispositivo.
- **Versión de Firmware**: La versión de firmware instalada en el dispositivo.

Acciones

La función **Acción** te permite controlar las funciones del dispositivo.



- **Actualización de firmware**: Actualice el firmware del dispositivo a la versión más reciente.
- **Reiniciar**: Reinicie el dispositivo de forma remota cuando ocurra un problema o anomalía.
- **Dispositivo Reiniciado**: Inicialice todos los ajustes almacenados en el dispositivo. Esta acción elimina todos los ajustes y datos del dispositivo.
- **Dispositivo Reiniciado Excluida la red**: Inicialice todos los ajustes excepto la configuración de red. Esta acción elimina todos los ajustes y datos, pero conserva la configuración de red.

Ajustes iniciales

Modifique los ajustes predeterminados del dispositivo.

- **Apodo**: El alias que aparece en la lista de dispositivos y en los registros. Puede editar este campo directamente.
- **Zona horaria**: Establezca la zona horaria del dispositivo para mantener los registros consistentes cuando los relojes del sitio y del dispositivo difieran. Active la opción **Usar DST** para aplicar el horario de verano (DST).
- **Manos Libres**: Amplíe el alcance BLE.

Tarjeta

En la sección **Tarjeta** puede modificar los ajustes de autenticación por tarjeta.

Tarjeta NFC/RF

- **Tarjeta NFC/RF**: Haga clic en el interruptor para activar o desactivar la autenticación de acceso por tarjeta. Seleccione

los tipos de tarjeta compatibles.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **Orden de bytes**
  - **MSB**: Procesa los datos de la tarjeta en orden de unidades de byte grandes a pequeñas, almacenando secuencialmente el número de serie de la tarjeta (CSN) de izquierda a derecha.
  - **LSB**: Procesa los datos de la tarjeta en orden de unidades de byte pequeñas a grandes, almacenando el número de serie de la tarjeta (CSN).
- **Método de lectura de datos**: Seleccione CSN (predeterminado) o el formato Wiegand.

> Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Tarjetas propietarias

Para tarjetas Wiegand, seleccione **iClass (SE / SEOS)** y **HID Prox**. Haga clic en el interruptor para activar la función y luego seleccione el formato de tarjeta deseado en **Tarjetas propietarias**.

> **Información**
>
> - La compatibilidad puede variar según el dispositivo.
> - Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Red

Modifique la configuración de red del dispositivo.

- **Configuración de la red**: Configure el dispositivo para obtener una dirección IP automáticamente.

  Para configurar la red manualmente, desactive **Configuración de la red** y complete los siguientes campos.
  - **Usar DHCP**
  - **Dirección IP**
  - **Entrada**
  - **Dirección DNS**

Autenticación

- **Modo de autenticación**: Agregue métodos de autenticación. Haga clic en **Agregar** para agregar un método de autenticación. Puede usar una combinación de tarjeta RF y reconocimiento facial como método de autenticación.

Información

Puede configurar distintos métodos de autenticación para el horario seleccionado. Por ejemplo, puede permitir únicamente la autenticación con tarjeta durante el horario laboral y permitir autenticación con tarjeta y PIN fuera del horario laboral.

Rostro

Seguridad

- **Detección de falsificaciones**: Evite la autenticación de usuarios con rostros falsificados, como fotografías.
- **Comprobación de duplicados**: Verifique registros duplicados al inscribir rostros.

Detección

- **Sensibilidad del Sensor de Movimiento**: Establezca la sensibilidad para detectar movimiento alrededor del dispositivo.
- **Ángulo Máximo de la Postura de la Cabeza**: Establezca el ángulo máximo de rotación permitido para el rostro.
- **Búsqueda amplia**: Amplíe el área en la vista de la cámara donde se reconocen los rostros.
- **Distancia de Detección (cm)**: Establezca la distancia mínima y máxima de reconocimiento.
- **Tiempo de registro (seg)**: Si no se registra un rostro dentro del tiempo establecido durante el registro, el proceso se cancelará.

Detección de mascarilla

Active la opción **Detección de mascarilla** para configurar la detección de mascarillas.

- **Nivel de Detección de Mascarilla**: Seleccione la sensibilidad de la detección de mascarilla.
- **Si falla la detección de mascarilla**
  - **Denegar acceso**: A los usuarios que no lleven mascarilla se les deniega la autenticación y se registra un evento de incumplimiento del uso de mascarilla.
  - **Permitir acceso después de iniciar sesión**: Los usuarios que no lleven mascarilla aún pueden autenticarse, pero se registra un evento de incumplimiento del uso de mascarilla.
- **Comprobación de mascarilla**
  - **Después del acceso**: Después de la autenticación, verifique el uso de mascarilla o mida la temperatura.
  - **Antes del acceso**: Verifique el uso de mascarilla o mida la temperatura antes de la autenticación. En este caso, los usuarios que no lleven mascarilla o cuya temperatura supere el umbral no podrán autenticarse.
  - **Sin acceso**: Utilice el dispositivo solo para comprobar el uso de mascarilla o medir la temperatura. Los usuarios que lleven mascarilla o cuya temperatura esté por debajo del umbral pueden acceder sin autenticarse.
- **Autenticar QR o código de barras con la cámara del dispositivo**: Defina si se permite la autenticación QR/código de barras mediante la cámara del dispositivo.
- **Autenticar el número de tarjeta con QR**: Configure la autenticación para aceptar un código QR que contenga los mismos datos que la tarjeta CSN o la tarjeta Wiegand emitida al usuario. Esta función está disponible cuando la opción **Autenticar QR o código de barras con la cámara del dispositivo** está habilitada.

> **Información**
> Al usar credenciales no faciales, el momento de "antes" y "después" suele ser importante.

T&A(Tiempo y asistencia, T&A)

Cuando esta función esté habilitada, **Evento T&A** se registra en el **Registro de eventos** y se utiliza en **Informe de tiempo y asistencia**.

- **Usar T&A**: Haga clic en el interruptor para activar o desactivar la gestión de asistencia.
- **Modo T&A**: Seleccione el modo de asistencia deseado.
  - **Por horario**: Los eventos de asistencia cambian automáticamente según el horario establecido. Puede seleccionar un horario para aplicarlo a los eventos de asistencia.
  - **Fijado**: Solo se puede usar el evento de asistencia seleccionado.

> **Información**
> Para más información sobre la configuración de tiempo y asistencia, consulte Tiempo y asistencia (T&A).

Salida Wiegand

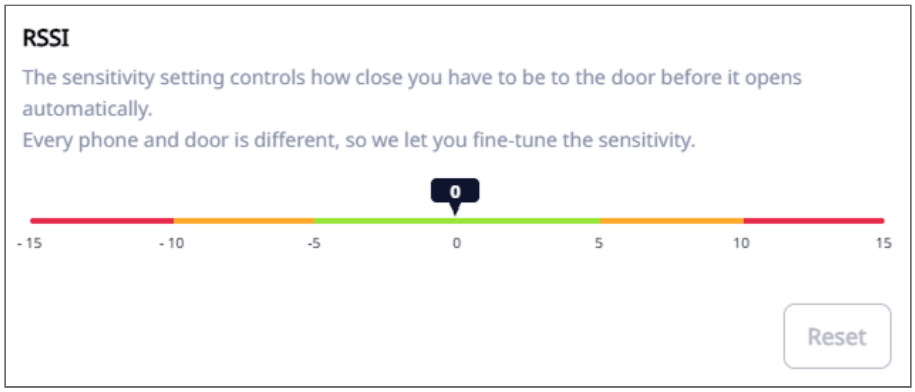
Esta función se integra con sistemas externos (por ejemplo, paneles de alarma). Activa la opción **Usar salida Wiegand** para usar esta función.

- **Modo de salida**: Configura el modo de salida de la señal Wiegand.
  - **Regular**: Escanea tarjetas usando el formato Wiegand configurado.
    - **Usar código de fallo**: Puede establecer códigos de error y elegir el valor a enviar cuando falle la autenticación de la tarjeta Wiegand.
  - **Omitir**: Envía el CSN independientemente de la autenticación Wiegand. Activa esta opción si lo usas como un dispositivo sin función de control de puertas.
- **Información de salida**: Selecciona la información que se enviará durante la autenticación.
- **Ancho de pulso**: Establece el ancho de pulso para la señal Wiegand.
- **Intervalo de pulso**: Establece el intervalo de pulso para la señal Wiegand.
- **Etiqueta móvil consecutiva**: Etiqueta tarjetas móviles consecutivamente sin tiempo de espera.
- **Límite de etiquetas consecutivas**: Define el número máximo de etiquetas consecutivas para tarjetas móviles.

> **Información**
> La función **Etiqueta móvil consecutiva** es compatible con la app Suprema Pass 2.9.0 o posterior.

Sensibilidad

Ajuste el valor RSSI para definir qué tan cerca debe estar el dispositivo móvil para desbloquear la puerta.



- Los valores más bajos ayudan a evitar activaciones no deseadas.
- Los valores más altos mejoran la detección en entornos con mucha interferencia.

> **Información**
> Para restablecer la configuración, haga clic en **Restablecer**.

▼ BioStation 3

Detalle

La sección **Detalle** proporciona información básica — como el nombre del dispositivo, el modelo, el número de serie y la versión de firmware — e incluye un menú de acciones para controlar funciones y ajustes predeterminados.

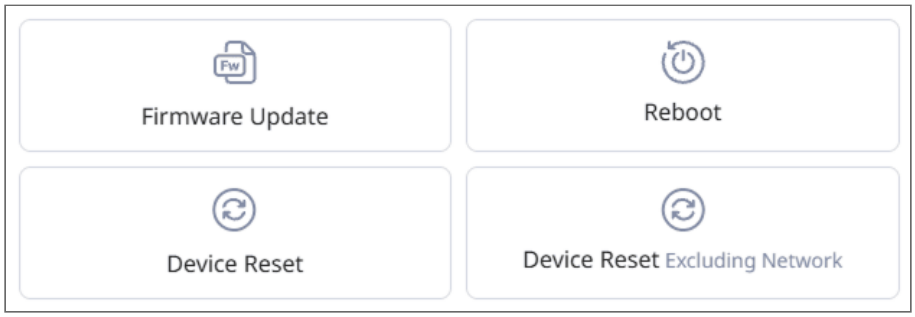
Información básica

Vea la información básica del dispositivo. Esta información no se puede editar.

- **Producto**: El nombre del producto.
- **Nombre del modelo**: El nombre del modelo del dispositivo.
- **Número de serie**: El número de serie del dispositivo.
- **Versión de Firmware**: La versión de firmware instalada en el dispositivo.

Acciones

La función **Acción** te permite controlar las funciones del dispositivo.



- **Actualización de firmware**: Actualice el firmware del dispositivo a la versión más reciente.

- **Reiniciar**: Reinicie el dispositivo de forma remota cuando ocurra un problema o anomalía.
- **Dispositivo Reiniciado**: Inicialice todos los ajustes almacenados en el dispositivo. Esta acción elimina todos los ajustes y datos del dispositivo.
- **Dispositivo Reiniciado Excluida la red**: Inicialice todos los ajustes excepto la configuración de red. Esta acción elimina todos los ajustes y datos, pero conserva la configuración de red.

Ajustes iniciales

Modifique los ajustes predeterminados del dispositivo.

- **Apodo**: El alias que aparece en la lista de dispositivos y en los registros. Puede editar este campo directamente.
- **Zona horaria**: Establezca la zona horaria del dispositivo para mantener los registros consistentes cuando los relojes del sitio y del dispositivo difieran. Active la opción **Usar DST** para aplicar el horario de verano (DST).
- **Manos Libres**: Amplíe el alcance BLE.
- **Servicio de Video**: Conecte cámaras IP al dispositivo para ver video en vivo y grabado. Para más información sobre los ajustes de conexión de cámaras IP, consulte Soporte y configuración de cámaras IP.

Tarjeta

En la sección **Tarjeta** puede modificar los ajustes de autenticación por tarjeta.

Tarjeta NFC/RF

- **Tarjeta NFC/RF**: Haga clic en el interruptor para activar o desactivar la autenticación de acceso por tarjeta. Seleccione los tipos de tarjeta compatibles.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **Orden de bytes**
  - **MSB**: Procesa los datos de la tarjeta en orden de unidades de byte grandes a pequeñas, almacenando secuencialmente el número de serie de la tarjeta (CSN) de izquierda a derecha.
  - **LSB**: Procesa los datos de la tarjeta en orden de unidades de byte pequeñas a grandes, almacenando el número de serie de la tarjeta (CSN).
- **Método de lectura de datos**: Seleccione CSN (predeterminado) o el formato Wiegand.

> Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Tarjetas propietarias

Para tarjetas Wiegand, seleccione **iClass (SE / SEOS)** y **HID Prox**. Haga clic en el interruptor para activar la función y luego seleccione el formato de tarjeta deseado en **Tarjetas propietarias**.

Información

- La compatibilidad puede variar según el dispositivo.
- Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Red

Modifique la configuración de red del dispositivo.

- **Configuración de la red**: Configure el dispositivo para obtener una dirección IP automáticamente.

  Para configurar la red manualmente, desactive **Configuración de la red** y complete los siguientes campos.
  - **Usar DHCP**
  - **Dirección IP**
  - **Entrada**
  - **Dirección DNS**

Autenticación

- **Modo de autenticación**: Agregue métodos de autenticación. Haga clic en **Agregar** para agregar un método de autenticación. Puede elegir una combinación de tarjeta RF, reconocimiento facial, identificación y PIN para la autenticación.
- **Mostrar nombre de usuario** / **Mostrar ID de usuario**: Elija si mostrar el nombre de usuario o el ID en la pantalla de autenticación. Seleccione **Oculto** para ocultarlos.
- **Tiempo de espera de autenticación**: La autenticación fallará si la credencial no se valida dentro del tiempo establecido.

Información

Puede configurar distintos métodos de autenticación para el horario seleccionado. Por ejemplo, puede permitir únicamente la autenticación con tarjeta durante el horario laboral y permitir autenticación con tarjeta y PIN fuera del horario laboral.

Rostro

Seguridad

- **Detección de falsificaciones**: Evite la autenticación de usuarios con rostros falsificados, como fotografías.
- **Comprobación de duplicados**: Verifique registros duplicados al inscribir rostros.

Detección

- **Sensibilidad del Sensor de Movimiento**: Establezca la sensibilidad para detectar movimiento alrededor del dispositivo.
- **Ángulo Máximo de la Postura de la Cabeza**: Establezca el ángulo máximo de rotación permitido para el rostro.
- **Búsqueda amplia**: Amplíe el área en la vista de la cámara donde se reconocen los rostros.
- **Distancia de Detección (cm)**: Establezca la distancia mínima y máxima de reconocimiento.
- **Tiempo de registro (seg)**: Si no se registra un rostro dentro del tiempo establecido durante el registro, el proceso se cancelará.

Detección de mascarilla

Active la opción **Detección de mascarilla** para configurar la detección de mascarillas.

- **Nivel de Detección de Mascarilla**: Seleccione la sensibilidad de la detección de mascarilla.
- **Si falla la detección de mascarilla**
  - **Denegar acceso**: A los usuarios que no lleven mascarilla se les deniega la autenticación y se registra un evento de incumplimiento del uso de mascarilla.
  - **Permitir acceso después de iniciar sesión**: Los usuarios que no lleven mascarilla aún pueden autenticarse, pero se registra un evento de incumplimiento del uso de mascarilla.
- **Comprobación de mascarilla**
  - **Después del acceso**: Después de la autenticación, verifique el uso de mascarilla o mida la temperatura.
  - **Antes del acceso**: Verifique el uso de mascarilla o mida la temperatura antes de la autenticación. En este caso, los usuarios que no lleven mascarilla o cuya temperatura supere el umbral no podrán autenticarse.
  - **Sin acceso**: Utilice el dispositivo solo para comprobar el uso de mascarilla o medir la temperatura. Los usuarios que lleven mascarilla o cuya temperatura esté por debajo del umbral pueden acceder sin autenticarse.
- **Autenticar QR o código de barras con la cámara del dispositivo**: Defina si se permite la autenticación QR/código de barras mediante la cámara del dispositivo.
- **Autenticar el número de tarjeta con QR**: Configure la autenticación para aceptar un código QR que contenga los mismos datos que la tarjeta CSN o la tarjeta Wiegand emitida al usuario. Esta función está disponible cuando la opción **Autenticar QR o código de barras con la cámara del dispositivo** está habilitada.

> **Información**
> Al usar credenciales no faciales, el momento de "antes" y "después" suele ser importante.

T&A(Tiempo y asistencia, T&A)

Cuando esta función esté habilitada, **Evento T&A** se registra en el **Registro de eventos** y se utiliza en **Informe de tiempo y asistencia**.

- **Usar T&A**: Haga clic en el interruptor para activar o desactivar la gestión de asistencia.
- **Modo T&A**: Seleccione el modo de asistencia deseado.

- **Selección manual**: Cuando la tecla de asistencia aparece en la pantalla, el usuario selecciona el evento de asistencia al autenticarse.

  > **Se requiere T&A**: Habilite esta opción para exigir que los usuarios registren un evento de asistencia al autenticarse.

- **Por horario**: Los eventos de asistencia cambian automáticamente según el horario establecido. Puede seleccionar un horario para aplicarlo a los eventos de asistencia.
- **Última opción**: El usuario continúa usando el último evento de asistencia seleccionado.
- **Fijado**: Solo se puede usar el evento de asistencia seleccionado.

> **Información**
> Para más información sobre la configuración de tiempo y asistencia, consulte Tiempo y asistencia (T&A).

Pantalla y sonido

Pantalla

- **Usar protector de pantalla**: Reduzca el brillo del LCD cuando el dispositivo no esté en uso para disminuir el consumo de energía innecesario.
- **Retroiluminación siempre activa**: Mantenga la retroiluminación siempre encendida o atenúela después de inactividad.
- **Tiempo de espera de la retroiluminación**: Configure el tiempo antes de que la retroiluminación se apague automáticamente.
- **Idioma**: Configure el idioma que se mostrará en la pantalla del dispositivo.
- **Pantalla de inicio**: Configure los elementos que se muestran en el fondo de la pantalla de inicio del dispositivo.
  - **Normal**: Muestra la imagen predeterminada en la pantalla de inicio.
  - **Logotipo**: Muestra una imagen registrada por el usuario en la pantalla de inicio.
  - **Aviso**: Muestra el contenido ingresado por el administrador en la pantalla de inicio.

  > Tras hacer clic en **Actualizar** y guardar, la imagen o el aviso deja de aparecer en la pantalla de edición, pero permanece en el dispositivo.

Sonido

- **Usar instrucciones de voz**: Usa la guía por voz en lugar de los tonos de notificación.
- **Volumen del dispositivo**: Ajusta el volumen de los sonidos generados por el dispositivo.
- **Volumen del altavoz del intercomunicador** / **Volumen del micrófono del intercomunicador**: Ajusta el volumen de salida o de entrada al usar la función de intercom IP.

Salida Wiegand

Esta función se integra con sistemas externos (por ejemplo, paneles de alarma). Activa la opción **Usar salida Wiegand** para usar esta función.

- **Modo de salida**: Configura el modo de salida de la señal Wiegand.
  - **Regular**: Escanea tarjetas usando el formato Wiegand configurado.
    - **Usar código de fallo**: Puede establecer códigos de error y elegir el valor a enviar cuando falle la autenticación de la tarjeta Wiegand.
  - **Omitir**: Envía el CSN independientemente de la autenticación Wiegand. Activa esta opción si lo usas como un dispositivo sin función de control de puertas.
- **Información de salida**: Selecciona la información que se enviará durante la autenticación.
- **Ancho de pulso**: Establece el ancho de pulso para la señal Wiegand.
- **Intervalo de pulso**: Establece el intervalo de pulso para la señal Wiegand.
- **Etiqueta móvil consecutiva**: Etiqueta tarjetas móviles consecutivamente sin tiempo de espera.
- **Límite de etiquetas consecutivas**: Define el número máximo de etiquetas consecutivas para tarjetas móviles.

> **Información**
> La función **Etiqueta móvil consecutiva** es compatible con la app Suprema Pass 2.9.0 o posterior.

Intercomunicador

- **Usar intercomunicador**: Activa o desactiva la función de intercom IP.
- **Transporte del servidor SIP**: Elige el método de transporte SIP al configurar el servidor SIP del intercomunicador.
- **Dirección del servidor SIP**: Introduce la dirección del servidor SIP.
- **Puerto del servidor SIP**: Introduce el puerto del servidor SIP.
- **Duración del registro**: Introduce la duración del registro. El dispositivo intentará registrarse en el servidor SIP cada vez que expire ese periodo.
- **Nombre de usuario SIP**: Introduce el nombre de usuario de la cuenta SIP.
- **Clave**: Introduce la contraseña de la cuenta SIP.
- **ID de autorización**: Introduce el ID de autorización de la cuenta SIP.
- **Servidor proxy de salida**: Utiliza un servidor proxy saliente separado para los servicios SIP si es necesario.
- **Número de extensión**: Agrega o edita números de extensión.
- **Resolución de vídeo**: Seleccione la resolución de video al usar el intercomunicador.
- **Botón de apertura de puerta**: Seleccione el botón que desbloquea la puerta durante una llamada.

Protección contra manipulaciones seguras

Si ocurre un evento de manipulación, configure el dispositivo para eliminar **toda la información de usuario**, **todos los registros** y **las claves de seguridad** almacenadas en el dispositivo.

RTSP

Configure los detalles del **Protocolo de transmisión en tiempo real** (RTSP). La cámara del dispositivo puede transmitir video en vivo.

- **Usar RTSP**: Active o desactive la transmisión RTSP.
- **Dirección**: Dirección del servidor RTSP.
- **Puerto**: Ingrese el puerto del servidor RTSP.
- **ID** / **Clave**: Ingrese el ID y la contraseña del servidor RTSP.
- **Resolución de video RTSP**: Seleccione la resolución de video al usar RTSP.

> **Información**
> La función de transmisión RTSP solo es compatible con BioStation 3.

Sensibilidad

Ajuste el valor RSSI para definir qué tan cerca debe estar el dispositivo móvil para desbloquear la puerta.



- Los valores más bajos ayudan a evitar activaciones no deseadas.
- Los valores más altos mejoran la detección en entornos con mucha interferencia.

> **Información**
> Para restablecer la configuración, haga clic en **Restablecer**.

▼ CoreStation 20

Detalle

La sección **Detalle** proporciona información básica — como el nombre del dispositivo, el modelo, el número de serie y la versión de firmware — e incluye un menú de acciones para controlar funciones y ajustes predeterminados.

Información básica

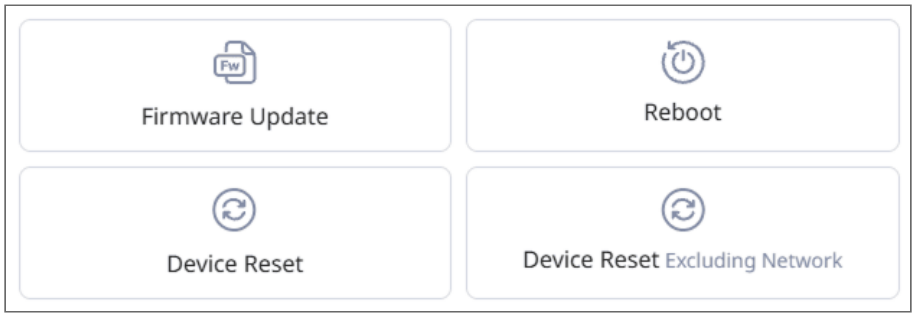
Vea la información básica del dispositivo. Esta información no se puede editar.

- **Producto**: El nombre del producto.

- **Nombre del modelo**: El nombre del modelo del dispositivo.
- **Número de serie**: El número de serie del dispositivo.
- **Versión de Firmware**: La versión de firmware instalada en el dispositivo.

Acciones

La función **Acción** te permite controlar las funciones del dispositivo.



- **Actualización de firmware**: Actualice el firmware del dispositivo a la versión más reciente.
- **Reiniciar**: Reinicie el dispositivo de forma remota cuando ocurra un problema o anomalía.
- **Dispositivo Reiniciado**: Inicialice todos los ajustes almacenados en el dispositivo. Esta acción elimina todos los ajustes y datos del dispositivo.
- **Dispositivo Reiniciado Excluida la red**: Inicialice todos los ajustes excepto la configuración de red. Esta acción elimina todos los ajustes y datos, pero conserva la configuración de red.

Ajustes iniciales

Modifique los ajustes predeterminados del dispositivo.

- **Apodo**: El alias que aparece en la lista de dispositivos y en los registros. Puede editar este campo directamente.
- **Zona horaria**: Establezca la zona horaria del dispositivo para mantener los registros consistentes cuando los relojes del sitio y del dispositivo difieran. Active la opción **Usar DST** para aplicar el horario de verano (DST).
- **Servicio de Video**: Conecte cámaras IP al panel para ver video en vivo y grabado. Para más información sobre los ajustes de conexión de cámaras IP, consulte Soporte y configuración de cámaras IP.

Tarjeta

En la sección **Tarjeta** puede modificar los ajustes de autenticación por tarjeta.

Tarjeta NFC/RF

- **Tarjeta NFC/RF**: Haga clic en el interruptor para activar o desactivar la autenticación de acceso por tarjeta. Seleccione los tipos de tarjeta compatibles.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **Orden de bytes**
  - **MSB**: Procesa los datos de la tarjeta en orden de unidades de byte grandes a pequeñas, almacenando secuencialmente el número de serie de la tarjeta (CSN) de izquierda a derecha.
  - **LSB**: Procesa los datos de la tarjeta en orden de unidades de byte pequeñas a grandes, almacenando el número de serie de la tarjeta (CSN).

- **Método de lectura de datos**: Seleccione CSN (predeterminado) o el formato Wiegand.

> Wiegand admite 5 formatos predeterminados. Agregue más formatos en **Ajustes** → **Formato de tarjeta**. Para más información sobre la configuración de formatos de tarjeta personalizados, consulte Formato de tarjeta Wiegand personalizado.

Red

Modifique la configuración de red del dispositivo.

- **Configuración de la red**: Configure el dispositivo para obtener una dirección IP automáticamente.

  Para configurar la red manualmente, desactive **Configuración de la red** y complete los siguientes campos.
  - **Usar DHCP**
  - **Dirección IP**
  - **Entrada**
  - **Dirección DNS**
- **Clave SCB**: Ingrese la clave de seguridad del Serial Communication Block (SCB). Ingrese hasta 32 caracteres. Protege la comunicación serial.
- **Confirmar Clave SCB**: Vuelva a ingresar el mismo valor para evitar errores de clave de seguridad.
- **Tasa de baudios**: Configure la tasa de baudios de la comunicación serial entre el panel y los dispositivos secundarios.
  - **Host**: Tasa de baudios de comunicación del panel
  - **0** / **1**: Tasa de baudios para cada puerto conectado a un dispositivo auxiliar

> **Información**
>
> - Establezca la clave SCB antes de agregar dispositivos OSDP. Si ya se añadieron dispositivos OSDP, la clave SCB no se puede cambiar.
> - Si el fabricante de un dispositivo OSDP de terceros utiliza una clave SCB específica, configure el CS-20 para usar la misma clave que el dispositivo OSDP.
> - Si las claves SCB del CS-20 y del dispositivo OSDP no coinciden, no es posible conectar con el dispositivo mediante **Secure Session**.
> - **Tasa de baudios**: Configure una tasa de baudios diferente de forma independiente; el valor predeterminado es `115200`.

Avanzado

Estado de Entrada del Dispositivo

Si un sensor de manipulación, un sensor de fallo de energía o un detector de incendios está conectado al puerto AUX IN, habilítelo o deshabilítelo.

- **Tamper**

- **Fallo de CA**
- **Incendio**

> **Información**
> Para usar una cerradura Fail Safe, conecte un relé **N/C**; para usar una cerradura Fail Secure, conecte un relé **N/O**. Para más información sobre las conexiones de relé, consulte la guía de instalación del CoreStation 20.

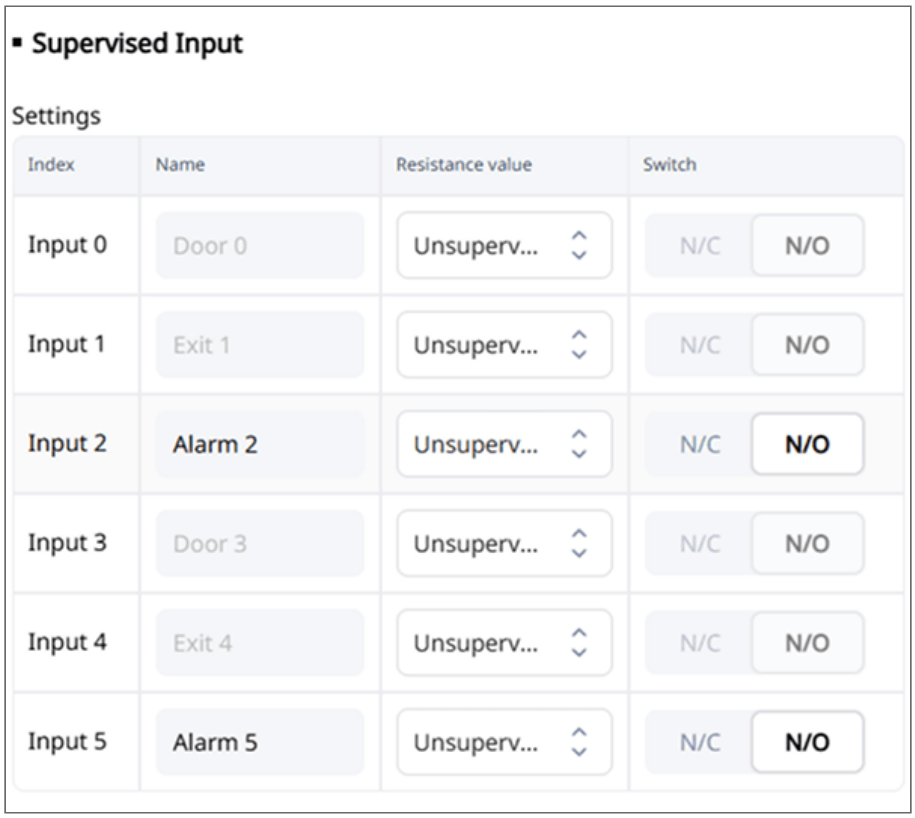
Entrada Wiegand

Configure los ajustes detallados de entrada Wiegand.

- **Usar Entrada Wiegand**: Habilite o deshabilite la función de entrada Wiegand.
- **Formato de Entrada**: Seleccione el formato de entrada Wiegand.
- **Ancho de pulso**: Establece el ancho de pulso para la señal Wiegand.
- **Intervalo de pulso**: Establece el intervalo de pulso para la señal Wiegand.

Entrada Supervisada

Configure el puerto Supervised Input para que funcione como puerto de entrada y ajuste el valor de la resistencia usado para Supervised Input. Los valores disponibles son 1 kΩ, 2.2 kΩ, 4.7 kΩ o 10 kΩ.



Protección contra manipulaciones seguras

Si ocurre un evento de manipulación, configure el panel para eliminar **toda la información de usuario, todos los registros** y **las claves de seguridad** almacenadas en el panel.

Módulos

Opción para detectar un módulo OM-120 conectado al panel. Haga clic en **Agregar** para detectar el módulo.

Configurar Airfob Patch y Tag

Registra el Airfob Patch en la aplicación BioStar Air

Antes de comenzar

- Instale la app BioStar Air en su dispositivo móvil. Instale la app móvil mediante el siguiente enlace.
  - iOS
  - Android
- Inicie sesión con el mismo ID y contraseña que usa para el portal de administración de BioStar Air.
- Asegúrese de que BLE esté habilitado en su dispositivo móvil.
- Fije el Airfob Patch al lector de forma permanente o temporal. Para obtener más información, consulte Instalar Airfob Patch.

> **Información**
> Para obtener más información sobre el uso de la app móvil BioStar Air, consulte Primeros pasos con la aplicación BioStar Air.

Registrar Airfob Patch

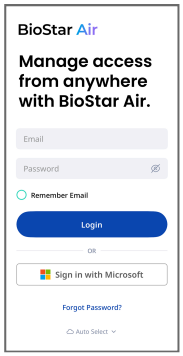
1. Abra la aplicación BioStar Air en su dispositivo móvil e inicie sesión.
2. En la pantalla principal de BioStar Air, toque **Administrar** en la parte inferior.
3. Acerca su dispositivo móvil a menos de 10 cm del Airfob Patch y luego toque el botón + en la esquina superior derecha de la pantalla.
4. En la pantalla de búsqueda de dispositivos, toque **Registrar** en el Airfob Patch para enrolarlo.
5. Cuando aparezca la ventana de registro del dispositivo, toque **OK**.

Vuelva a la lista de dispositivos y confirme el Airfob Patch agregado.

Pasos de configuración

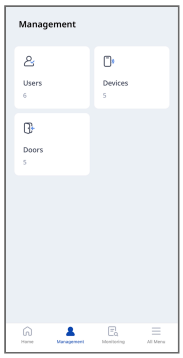
Instala el Airfob Patch o Tag y regístralo en la aplicación BioStar Air. Sigue estos pasos para configurar el dispositivo.

1 Abre la aplicación



1. Abre **BioStar Air** en tu dispositivo móvil.
2. Inicia sesión en el sitio donde está registrado el Airfob Patch o Tag.

2 Ve a la configuración del dispositivo



1. En la pantalla principal de **BioStar Air**, toca **Administrar** en la parte inferior.
2. Para ver los dispositivos registrados, toca **Dispositivos**.
3. Selecciona el Airfob Patch o Tag de la lista de dispositivos.

3 Activa el modo BLE

- Acerca el dispositivo móvil a la unidad.
- Activa **Modo BLE** en la aplicación.

4 Configura el método de salida del ID de tarjeta

- Desplázate hasta **Método de salida del ID de tarjeta** y toca **Editar**.
- Toca **Seleccionar** junto a **ID de tarjeta de usuario**.

5 Selecciona el método de salida

- **Ninguno**: Seleccione esta opción cuando no desee enviar un ID de tarjeta. Útil para el control de tiempo y asistencia, ya que prolonga la vida útil de la batería.
- **Dispositivo fijo**: Envía el ID de tarjeta fijo preprogramado. Útil para cerraduras o intercomunicadores que requieren programar cada tarjeta RFID de forma individual. Solo este ID fijo aparece en los registros del dispositivo.
- **ID de tarjeta de usuario**: Envía un ID de tarjeta único para cada usuario que coincide con el número de tarjeta

RFID registrado en el sistema de control de acceso. Esto permite una integración sin necesidad de emitir nuevas tarjetas físicas.

- **Entrada directa**: Especifique manualmente el ID de la tarjeta que se enviará. Útil para configuraciones personalizadas en las que un mismo ID debe utilizarse en varias unidades.

6 Guardar la configuración

- Mantenga el dispositivo móvil cerca de la unidad, toque **Guardar** y confirme las selecciones.
- Se muestra el mensaje 'Actualización completada'.

Lectores y credenciales biométricos
BioStar Air ahora es compatible con lectores y credenciales biométricos para mejorar el control de acceso. Registra y configura dispositivos biométricos compatibles, como BioStation 3 (BS3) y BioEntry W3 (W3), para autenticar a los usuarios mediante reconocimiento facial. La función admite la autenticación de uno o dos factores, lo que aumenta la flexibilidad y la seguridad.

- **Registrar lectores**: Usa la app móvil de BioStar Air para registrar lectores biométricos.
- **Configuración del dispositivo**: Ve al BioStar Air Portal → **Gestión de dispositivos** → **Dispositivos registrados** para configurar la autenticación facial del dispositivo.
- **Configuración de la credencial facial**: Ve al BioStar Air Portal → **Gestión de usuarios** → **Usuarios** para agregar o editar usuarios. Activa la credencial facial en la sección **Detalles de la Credencial**.

Antes de comenzar

- Debe instalarse un firmware compatible con BioStar Air para que el lector biométrico funcione correctamente.
- Se pueden usar hasta dos plantillas faciales por usuario.
- Para una configuración avanzada, consulta la guía del usuario de BioEntry W3 o BioStation 3.
- Registra al menos dos credenciales para usar la autenticación de dos factores. Por ejemplo, registra tanto la credencial de tarjeta RF como la credencial facial.

Paso a paso

1 Registrar dispositivo biométrico

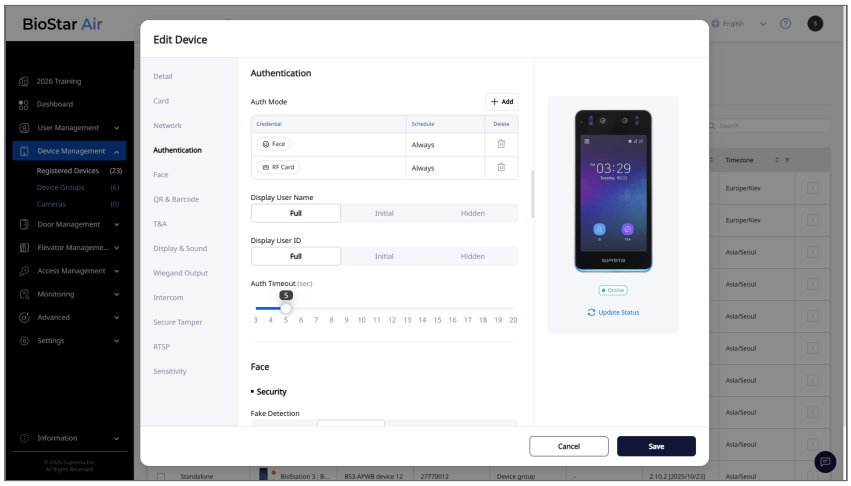
Verifica que el firmware compatible con BioStar Air esté instalado en el BioEntry W3 o BioStation 3. Los modelos cuyos nombres terminan con `-AIR` ya incluyen el firmware predeterminado suministrado por Suprema.

Abre la app BioStar Air en el dispositivo móvil e inicia sesión con el ID y la contraseña de administrador. Registra el dispositivo de la misma manera que cualquier otro lector.

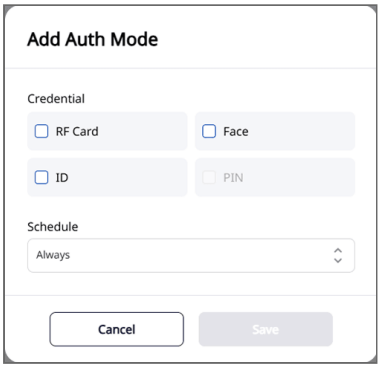
> **Información**
> Para obtener más información sobre el registro de dispositivos, consulta Registrar y Eliminar Dispositivos Edge.

2 Configurar el lector

1. Inicia sesión en el BioStar Air Portal con una cuenta de administrador.
2. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
3. Haz clic en el lector biométrico en la lista de dispositivos.
4. Cuando aparezca la ventana **Editar dispositivo**, ve a la sección **Autenticación**.



5. Configura **Modo de autenticación**.
   - **Autenticación de un factor**: Autentica mediante tarjeta RF o reconocimiento facial.
   - **Autenticación de dos factores**: Elimina el factor de tarjeta RF o el de autenticación facial y, a continuación, vuelve a inscribir ambos para activar la autenticación de dos factores. Haz clic en **Agregar** y combina los métodos de autenticación que prefieras.



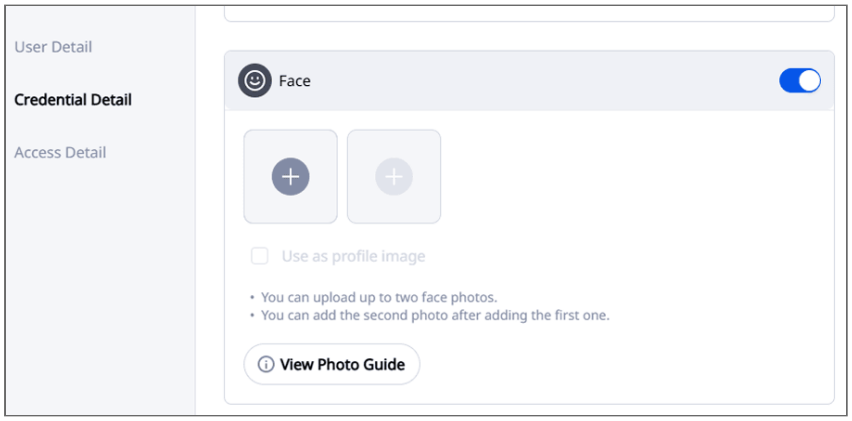
6. Configura **Tiempo de espera de autenticación**. Si la credencial no se autentica dentro del tiempo especificado, la autenticación fallará.
7. Configure las siguientes opciones en la sección **Rostro**.
   - **Detección de falsificaciones**
   - **Sensibilidad del Sensor de Movimiento**
   - **Ángulo Máximo de la Postura de la Cabeza**
   - **Distancia de Detección**
8. Configure opciones adicionales.

- **Comprobación de duplicados**
- **Tiempo de registro**
- **Detección de mascarilla**

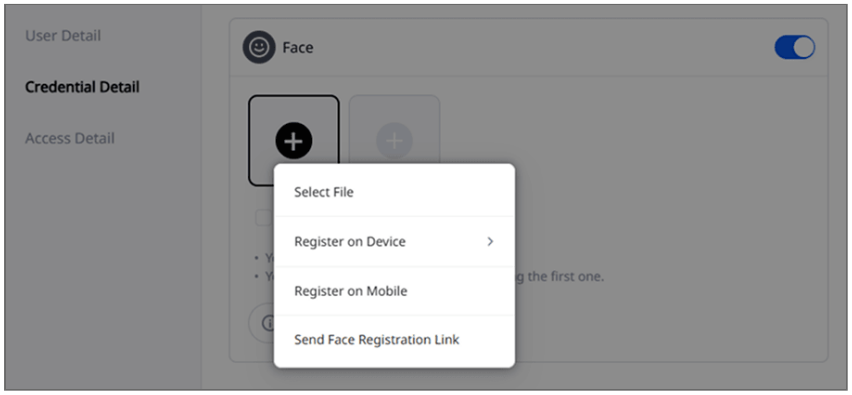
> **Información**
> Para obtener más información sobre los ajustes en la sección **Autenticación**, consulte Opciones de Configuración de Dispositivos y Paneles.

3 Registrar rostros de usuario

1. Haga clic en **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Abra la ventana para agregar un usuario nuevo o editar uno existente.
   - **Agregar un nuevo usuario**: Haga clic en **Añadir nuevo usuario** en la esquina superior derecha de la lista de usuarios.
   - **Editar un usuario existente**: Seleccione el usuario en la lista y luego haga clic en ✎.
3. En la ventana de información del usuario, vaya a la sección **Detalles de la Credencial** y active la credencial **Rostro**.



4. Haga clic en + y agregue la plantilla facial.



- **Seleccionar Archivo**: Seleccione un archivo de imagen almacenado localmente
- **Registrar en el Dispositivo**: Utilice el lector biométrico conectado (BioEntry W3 o BioStation 3)
- **Registrarse en el Móvil**: Escanee el código QR enviado al dispositivo móvil del usuario y registre el rostro

desde dicho dispositivo

- **Enviar Enlace de Registro Facial**: Enviar un enlace de inscripción facial al correo electrónico o por SMS al teléfono del usuario para que inscriba su rostro directamente con la cámara de su dispositivo móvil.

> Solo se pueden subir dos fotos de rostro por usuario. Por lo general, una es suficiente.

5. Haga clic en **Guardar** para completar el registro facial.

> **Información**
> Para obtener más información sobre cómo subir fotos de perfil de usuarios de forma masiva, consulte Agregar usuarios masivamente.

Actualizar Firmware

Actualice el firmware de BioStar Air para mejorar el rendimiento del dispositivo, reforzar la seguridad y aprovechar las nuevas funciones. Este proceso sencillo se puede realizar desde el portal web de BioStar Air o desde la aplicación móvil.

Antes de comenzar

- Los dispositivos deben estar **en línea** para actualizar el firmware. Compruebe el estado del dispositivo en la columna **Producto** de la lista de dispositivos. Un punto verde (🟢) junto a la imagen del dispositivo indica que el dispositivo está en línea.
- Durante la actualización del firmware, el dispositivo queda **temporalmente sin conexión**, pero debería volver a conectarse en **3–5 minutos**.
- Recomendamos realizar las actualizaciones de firmware fuera del horario laboral, ya que los dispositivos quedan temporalmente desconectados.
- Configure las notificaciones para recibir alertas cuando haya nuevo firmware disponible. Para más información sobre la configuración de alertas, consulte Configurar alertas y informes.

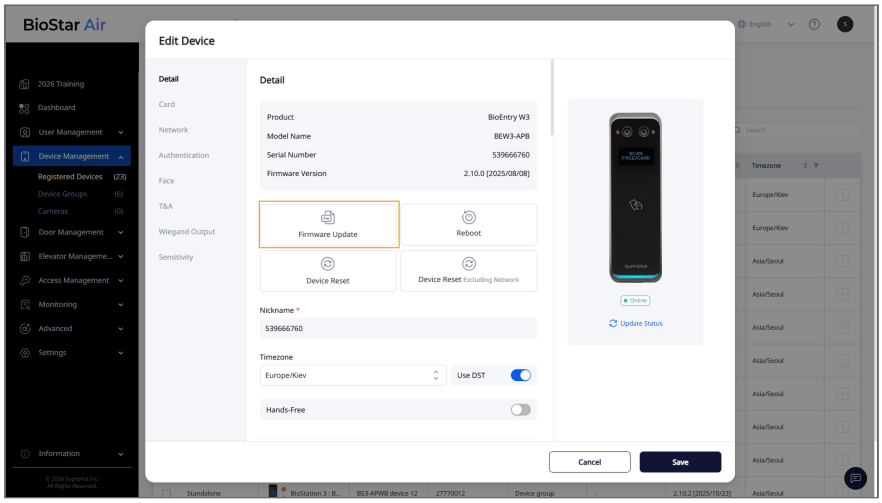
> **Información**
> Para más información sobre la gestión de dispositivos, consulte Administrar Dispositivos Edge Registrados.

Actualizar el firmware de un dispositivo individual

Web

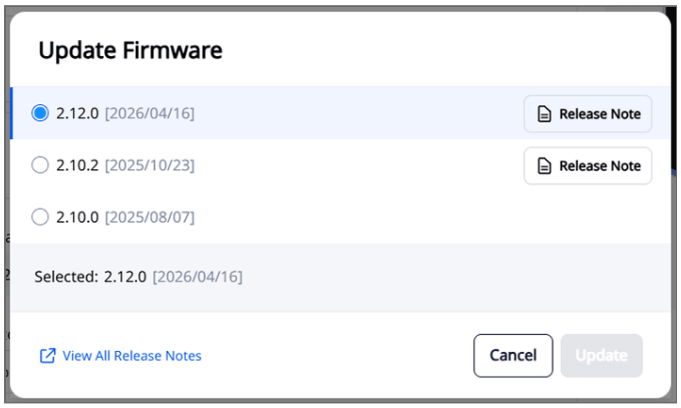
Inicie sesión en el portal BioStar Air y siga estos pasos para actualizar el firmware.

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haga clic en el dispositivo que desea actualizar en la lista de dispositivos.
3. Cuando aparezca la ventana **Editar dispositivo**, vaya a la sección **Detalle**.
4. Haga clic en **Actualización de firmware**.



La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

5. Cuando aparezca la ventana **Actualizar firmware**, seleccione la versión más reciente del firmware y haga clic en **Actualizar**.



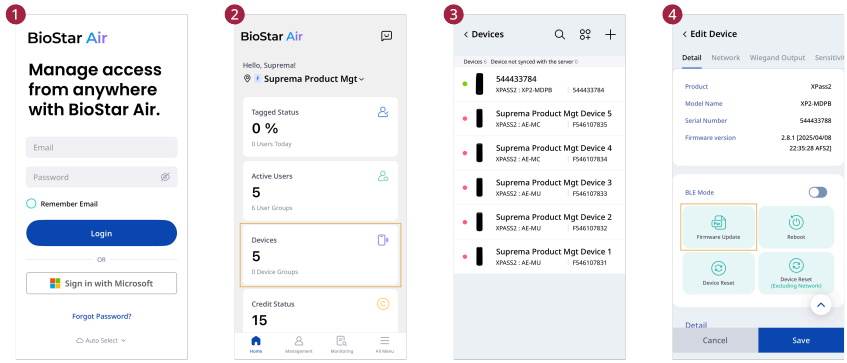
Espere a que el dispositivo se reinicie automáticamente y vuelva a estar en línea. Un punto verde (🟢) junto a la imagen del dispositivo indica que está en línea.

Información

- Haga clic en **Nota de versión** para ver las notas de la versión de ese firmware.
- Haga clic en **Ver todas las notas de versión** para ver las notas de la versión de firmware de todos los dispositivos.

Mobile

Esta guía explica cómo actualizar el firmware mediante la aplicación móvil.

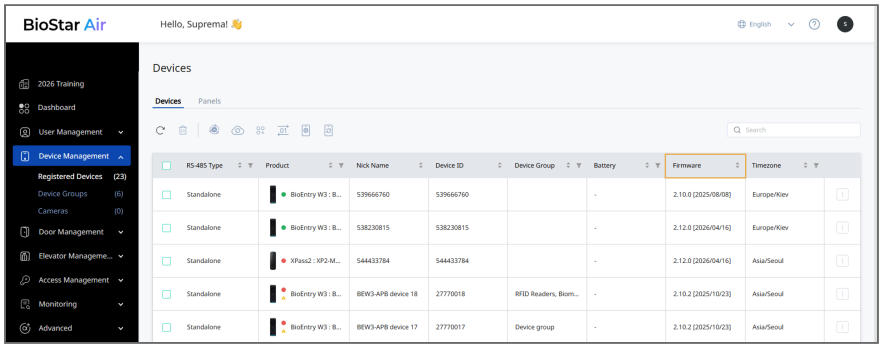


1. Abra la aplicación BioStar Air en su dispositivo móvil e inicie sesión.
2. Toque la tarjeta **Dispositivos**.
3. Toque el dispositivo en la lista cuyo firmware desea actualizar.
4. Toque **Actualización de firmware**.
5. Seleccione la versión de firmware más reciente y toque **OK**.
6. Cuando aparezca la ventana de mensajes, revise la información y toque **Confirmar**.

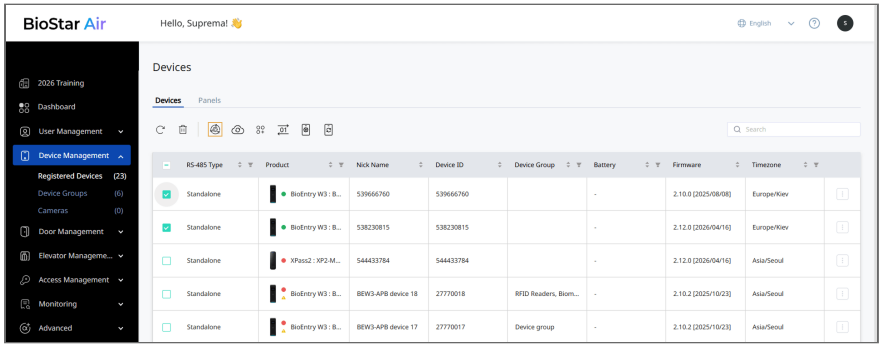
> **Información**
>
> - La actualización del firmware puede tardar entre 5 y 10 minutos, durante los cuales el dispositivo no estará disponible.
> - No apague el dispositivo.
> - El dispositivo se reinicia automáticamente después de completar la actualización de firmware.

Actualizar el firmware de varios dispositivos a la vez

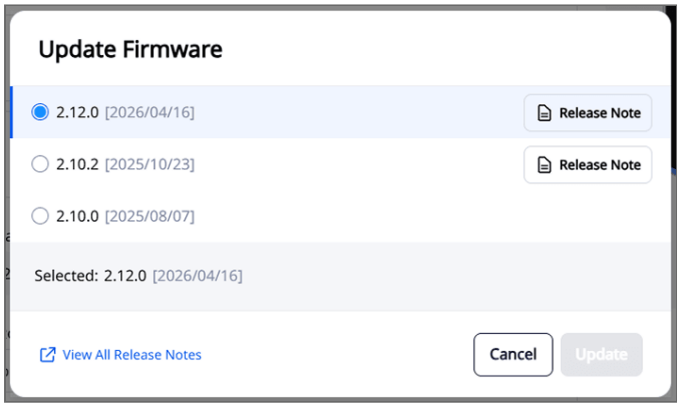
1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Compruebe la versión actual de cada dispositivo en la columna **Firmware** de la lista de dispositivos.
3. Haga clic en la flecha a la derecha de la columna **Firmware** para ordenar los dispositivos por versión de firmware.



4. Seleccione la casilla a la izquierda de cada dispositivo que desea actualizar. Debe seleccionar dispositivos del mismo tipo.
5. Haga clic en el botón en la parte superior de la lista de dispositivos.



6. Cuando aparezca la ventana **Actualizar firmware**, seleccione la versión más reciente del firmware y haga clic en **Actualizar**.



Espere a que los dispositivos seleccionados se reinicien automáticamente y vuelvan a estar en línea. Un punto verde (🟢) junto a la imagen del dispositivo indica que está en línea.

Información

- La actualización del firmware puede tardar entre 5 y 10 minutos, durante los cuales el dispositivo no estará disponible.
- No apague el dispositivo.
- El dispositivo se reinicia automáticamente después de completar la actualización de firmware.
- Haga clic en **Nota de versión** para ver las notas de la versión de ese firmware.
- Haga clic en **Ver todas las notas de versión** para ver las notas de la versión de firmware de todos los dispositivos.

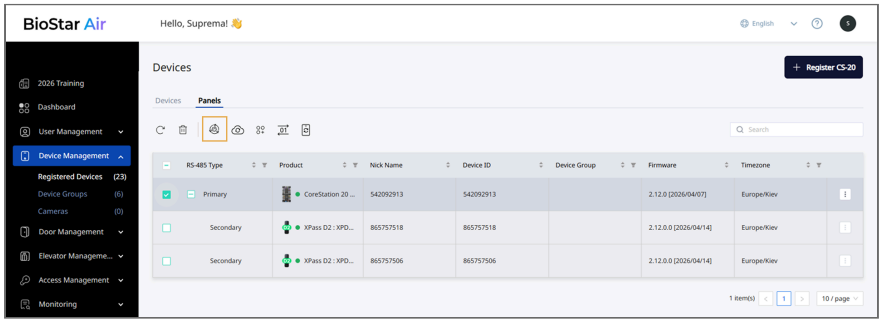
Actualización de firmware de XPass D2

XPass D2 usa dos componentes de firmware.

- **MICOM**: Incluye actualizaciones para la operación del dispositivo, la comunicación RS-485, el procesamiento de autenticación, la estabilidad y correcciones generales de errores.
- **BLE**: Incluye actualizaciones relacionadas con la comunicación Bluetooth.

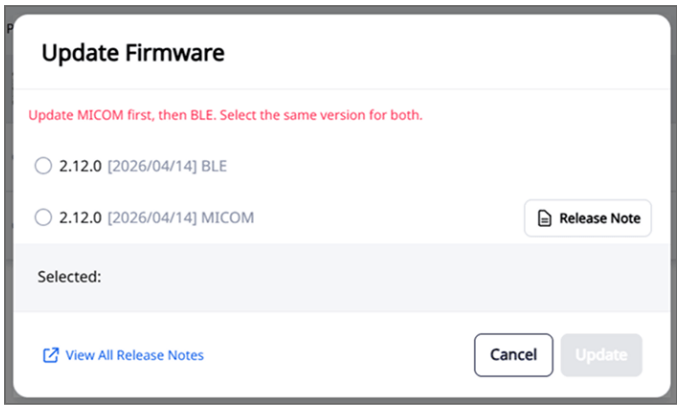
El firmware de XPass D2 debe actualizarse en el orden **MICOM** → **BLE**.

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haga clic en la pestaña **Paneles**.
3. Haga clic en la casilla de XPass D2. Seleccione solo 1 dispositivo.



4. Haga clic en ⚙ en la parte superior de la lista.

5. Cuando aparezca la ventana **Actualizar firmware**, seleccione la versión de firmware **MICOM**.



6. Haga clic en **Actualizar**.
7. Espere a que el dispositivo se reinicie automáticamente y vuelva a estar en línea. Un punto verde (🟢) junto a la imagen del dispositivo indica que está en línea.
8. Repita el proceso de actualización de firmware para seleccionar y actualizar la versión **BLE**.

> **Precaución**
>
> - La versión de firmware que aparece en pantalla no permite verificar individualmente el estado de instalación de los componentes **MICOM** y **BLE**. Continúe la actualización de firmware hasta que finalice la actualización BLE.
> - El dispositivo vuelve a estar en línea después de la actualización **MICOM** y nuevamente después de la actualización **BLE**. No confíe únicamente en el indicador verde en línea (🟢) para confirmar que la actualización completa haya finalizado. Confirme que ambos pasos hayan finalizado.
> - Solo un dispositivo secundario conectado vía CS-20 puede actualizar su firmware a la vez.

Puertas

La gestión de puertas en BioStar Air es fundamental para mantener un control de acceso y seguridad eficientes. Registra puertas, configura los dispositivos de entrada y salida, y administra el control de acceso a gran escala mediante grupos y horarios. Las políticas automatizadas de bloqueo y desbloqueo, así como el control de acceso basado en autenticación, aumentan aún más la seguridad.

Administrar puertas registradas

Asigne dispositivos de acceso a las puertas registradas, configure relés y niveles de acceso, y establezca los horarios de acceso. Controle el acceso para seguridad, evacuación por incendio y control de tiempo y asistencia (T&A).

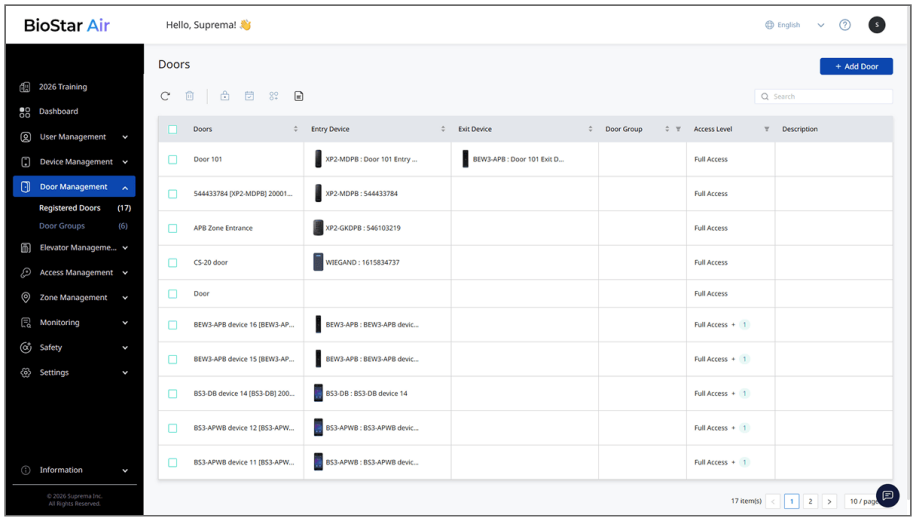
> **Consejo**
>
> Vea el siguiente video para aprender a registrar y administrar puertas.

Explorar la lista de puertas

La lista de puertas muestra todas las puertas registradas en BioStar Air de un vistazo. Consulte la información clave de cada

puerta, como su nombre, los dispositivos asignados, el grupo y los niveles de acceso. Haga clic en una puerta de la lista para ver los detalles y modificar los ajustes.

Haga clic en **Gestión de Puerta** → **Registrados Puerta** en la barra lateral izquierda para ver las puertas registradas.



Información de la puerta

La lista de puertas muestra la siguiente información.

- **Puerta**: El nombre de la puerta. Normalmente se asigna automáticamente durante el registro del dispositivo, pero los administradores pueden cambiarlo.
- **Dispositivo de entrada**: Dispositivo que autentica a los usuarios al ingresar por la puerta.
- **Dispositivo de salida**: Dispositivo que autentica a los usuarios al salir por la puerta.
- **Grupo de Puerta**: Nombre del grupo asignado a la puerta.
- **Nivel de acceso**: El nivel de acceso que el sistema asigna a la puerta. Para obtener más información sobre la asignación de niveles de acceso, consulte Establecer niveles de acceso por lotes.
- **Descripción**: Descripción de la puerta.
- **Cámara**: Muestra la información de la cámara asociada a la puerta. La columna **Cámara** aparece solo después de habilitar la función **Gestión de Vídeos** en **Ajustes** → **Sitio** → **Adicionales**.

Funciones adicionales

Cuando se selecciona una o más puertas en la lista, los administradores pueden gestionarlas mediante las siguientes herramientas.

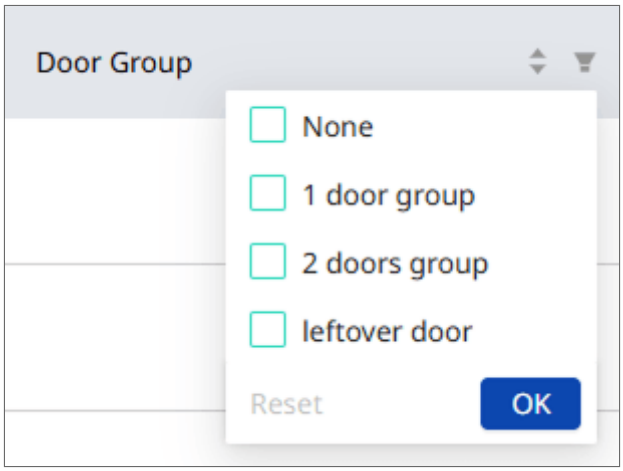
- : Actualizar la lista de puertas.
- : Eliminar las puertas seleccionadas de la lista.
- : Establecer niveles de acceso para las puertas seleccionadas. Para más información, consulte Establecer niveles de acceso por lotes.
- : Establecer un horario para los estados de apertura y bloqueo de la puerta. Para obtener más información sobre cómo gestionar los horarios de las puertas, consulte Administrar horarios de las puertas.
- : Agrupar las puertas seleccionadas. Para obtener más información sobre cómo gestionar los grupos de puertas,

consulte Administrar Grupo de Puertas.

- : Generar informes de las puertas. Para obtener más información sobre cómo generar informes de puertas, consulte Generar informes de puertas.

Filtrar

Filtre la lista de puertas por grupo. Haga clic en la columna **Grupo de Puerta** y en su botón y seleccione el grupo deseado. Haga clic en **OK** para mostrar solo las puertas del grupo seleccionado.



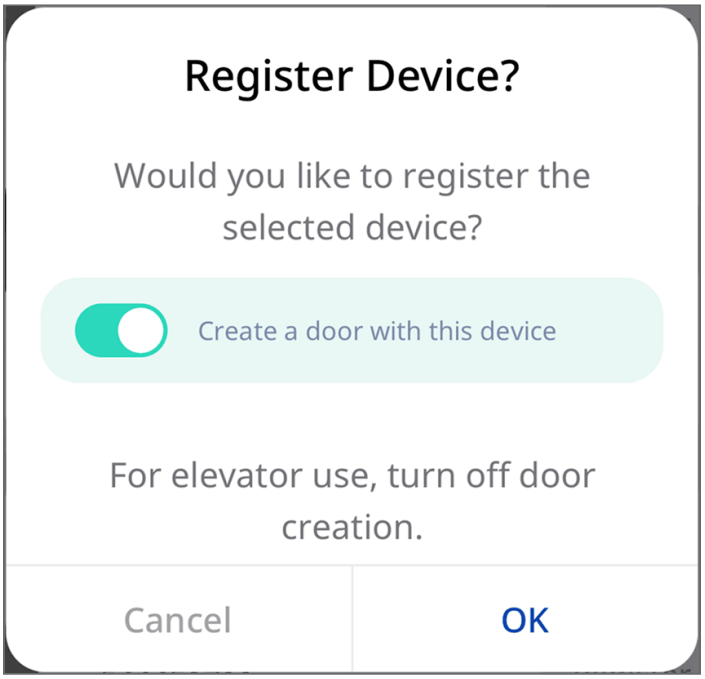
Información

Para restablecer los filtros aplicados, haga clic en y seleccione **Restablecer**.

Agregar puertas

Agregar usando un dispositivo

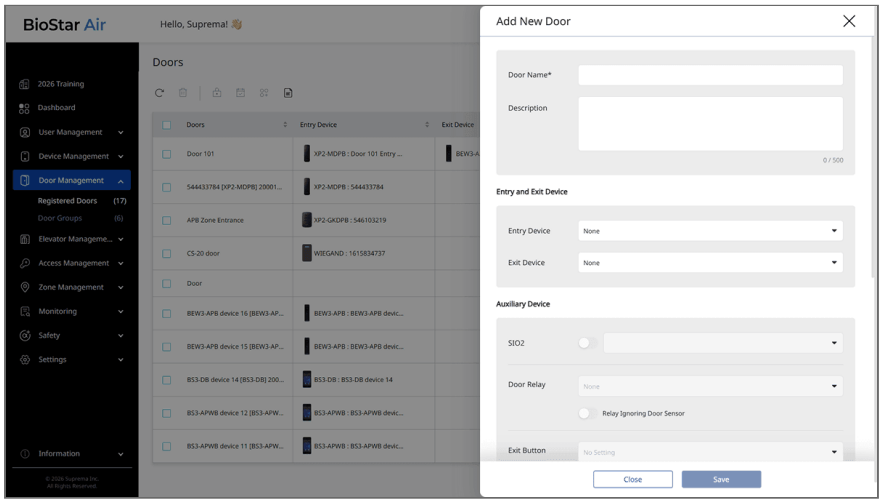
En el paso final del registro del dispositivo en la aplicación móvil, seleccione la opción **Create a door with this device** para crear una puerta. Para obtener más información sobre cómo registrar un dispositivo con la aplicación móvil, consulte Registrar y Eliminar Dispositivos Edge.



Agregar desde el portal web

Siga los pasos a continuación para agregar una nueva puerta en el portal BioStar Air.

1. Haga clic en **Gestión de Puerta** → **Registrados Puerta** en la barra lateral izquierda.
2. Haga clic en **Agregar nuevo puerta** en la parte superior derecha de la pantalla.
3. Cuando aparezca el panel **Agregar nuevo puerta**, ingrese **Nombre de Puerta**.



4. Seleccione **Dispositivo de entrada** y **Dispositivo de salida**.
5. Haga clic en **Guardar** para guardar y agregar la configuración de la puerta.

Reglas para asignar dispositivos a puertas

- Cada dispositivo solo puede asignarse a **una sola puerta**.
- Si un dispositivo ya está registrado pero no aparece en la lista de dispositivos disponibles, verifique si está asignado a otra puerta. Si lo está, quítelo de esa puerta e inténtelo de nuevo.
- **Un dispositivo no puede asignarse simultáneamente a una puerta y a un elevador**.

Puertas que usan dispositivos primario/secundario

- Un dispositivo primario controla la puerta (XPass 2 o CoreStation 20).
- Un XPass 2 configurado como primario puede asignarse a una sola puerta, sin importar cuántos dispositivos o módulos secundarios tenga asignados.
- Un XPass 2 configurado como primario puede tener hasta 31 dispositivos secundarios asignados. Puede agregar una nueva puerta cuyo relé controla un módulo Secure I/O 2 (SIO2) secundario.
- No se pueden crear puertas que usen una CoreStation 20 (CS-20) junto con un módulo Secure I/O 2 (SIO2).

Limitaciones de configuración de puertas

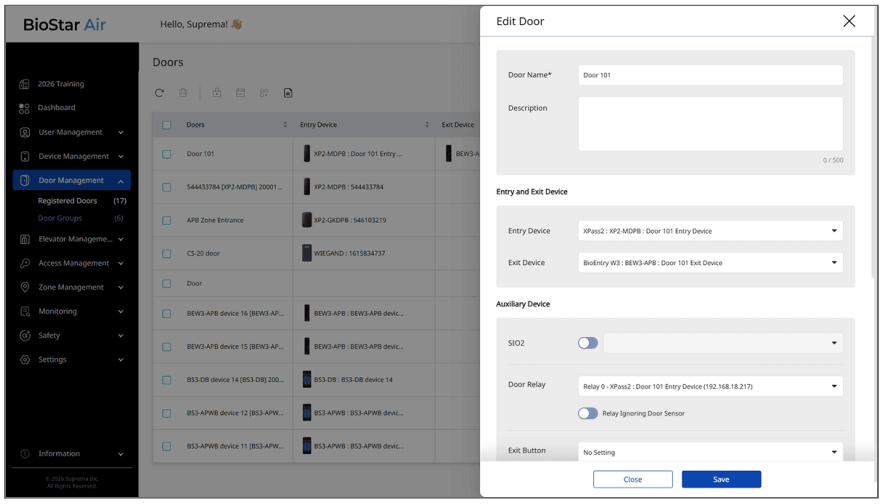
Las siguientes limitaciones aplican a la configuración de puertas.

- 1 XPass D2 + SIO2 (relé controlado por SIO2)
- 1 XPass 2 + XPass D2 (relé controlado por XPass 2)
- 2 XPass D2 (relé controlado por XPass 2)
- 1 o 2 dispositivos OSDP/Wiegand (relé controlado por CS-20)
- Solo se permite un SIO2 por puerta (relé para I/O): debe estar cableado al mismo XPass 2 que el XPass D2.

Editar puertas

Siga estos pasos para editar los detalles y la configuración de la puerta.

1. Haga clic en **Gestión de Puerta** → **Registrados Puerta** en la barra lateral izquierda.
2. Haga clic en la puerta que desea editar en la lista. O seleccione la casilla a la izquierda de la puerta y haga clic en en la barra lateral superior izquierda.
3. Cuando aparezca el panel **Editar puerta**, edite **Nombre de Puerta** y **Descripción**.

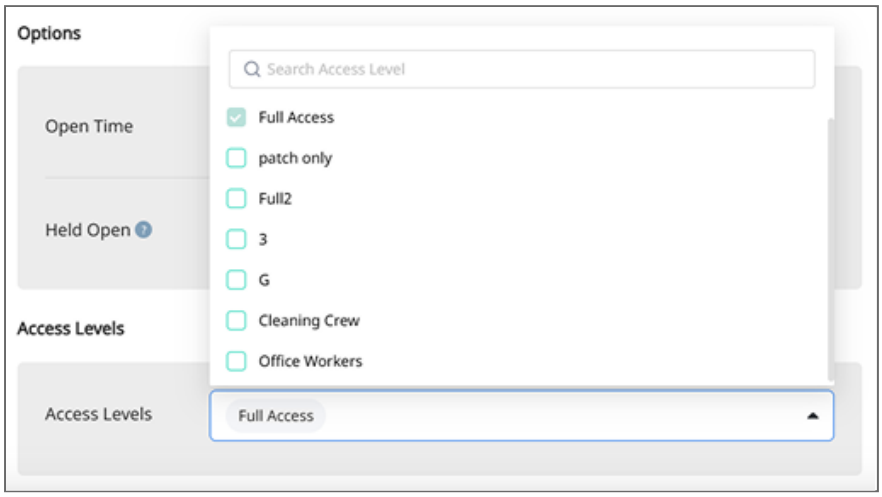


4. Seleccione el dispositivo para la autenticación de entrada de la puerta en la sección **Dispositivo de entrada y salida**.
   - **Dispositivo de entrada**: Seleccione el dispositivo que autentica a los usuarios al entrar por la puerta.
   - **Dispositivo de salida**: Seleccione el dispositivo que autentica a los usuarios al salir por la puerta.
5. Configure el dispositivo relé en la sección **Dispositivo auxiliar**.

- **Cámara**: Puede conectar una cámara CCTV para los registros de eventos.
- **Relé de puerta**: Seleccione el dispositivo relé que controla la cerradura de la puerta.
- **Ignorar relé de sensor de puerta**: Configure el relé para ignorar el sensor de la puerta.

> Para usar la cámara, habilite la función **Gestión de Vídeos** en **Ajustes** → **Sitio** → **Adicionales**.

6. Configure los ajustes adicionales.
   - Si está instalado, seleccione el puerto para configurarlo como **Botón de salida**.
   - Seleccione el puerto para configurarlo como **Sin ajustes**.
   - Establezca el tiempo que la puerta permanece abierta en **Hora de apertura**. (Predeterminado: 3 segundos)
7. En la sección **Nivel de acceso**, haga clic en las casillas de los niveles de acceso para asignarlos a la puerta o quitarlos de ella.



8. Haz clic en **Guardar** para aplicar los cambios.

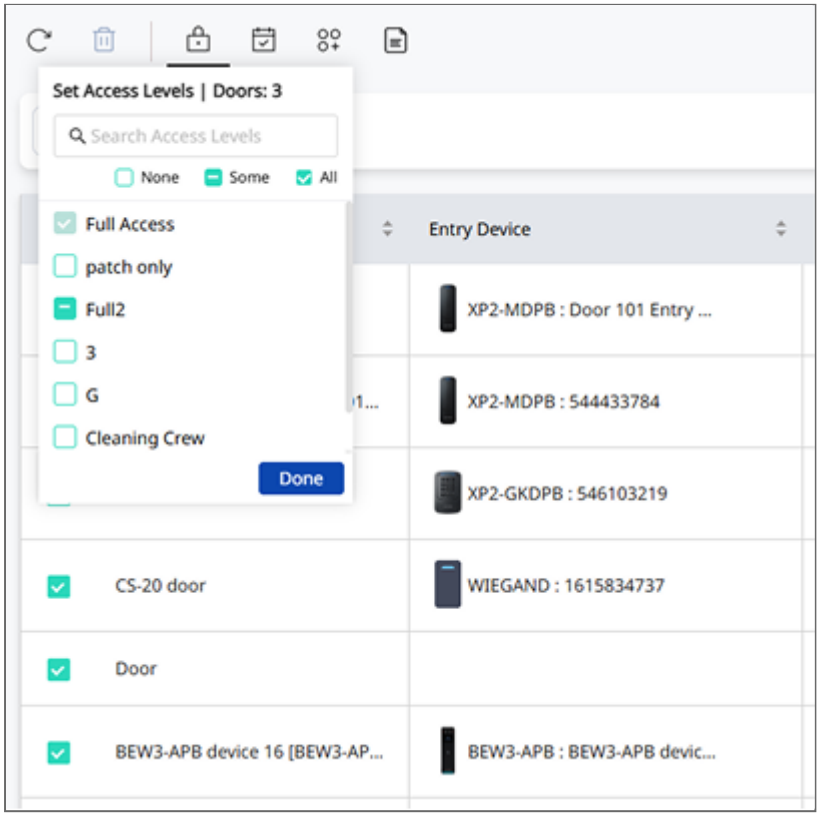
> **Información**
>
> - Por seguridad, el relé debe conectarse siempre al dispositivo en el lado seguro de la puerta. Use el relé del dispositivo de salida o un módulo SIO2.
> - Cuando está configurado para conexión directa a la nube, tanto el dispositivo de entrada como el de salida requieren cables de red separados.
> - Al usar una configuración primario-secundario, el dispositivo primario (generalmente el de salida) necesita una conexión de red y el dispositivo secundario se conecta al primario mediante RS-485.
> - Para obtener más información sobre cómo configurar el módulo SIO2 Secure, consulte Configurar el módulo seguro SIO2.

Establecer niveles de acceso por lotes

Asigne o anule la asignación de un nivel de acceso a varias puertas a la vez. Evite editar puertas una por una.

1. Haga clic en **Gestión de Puerta** → **Registrados Puerta** en la barra lateral izquierda.

2. Seleccione la casilla de al menos una puerta para establecer niveles de acceso.
3. Haga clic en en la parte superior de la lista de puertas.
4. Cuando aparezca el menú emergente **Establecer niveles de acceso**, seleccione las casillas de los niveles de acceso para aplicarlos a las puertas seleccionadas.



Busque el nivel de acceso en el campo de búsqueda, si es necesario.

- **Ninguno**: El sistema quita el nivel de acceso de las puertas seleccionadas.
- **Alguno**: Solo ciertas puertas seleccionadas tienen asignado el nivel de acceso.
- **Todos**: Todas las puertas seleccionadas tienen asignado el nivel de acceso.

5. Para finalizar, haga clic en **Listo**.

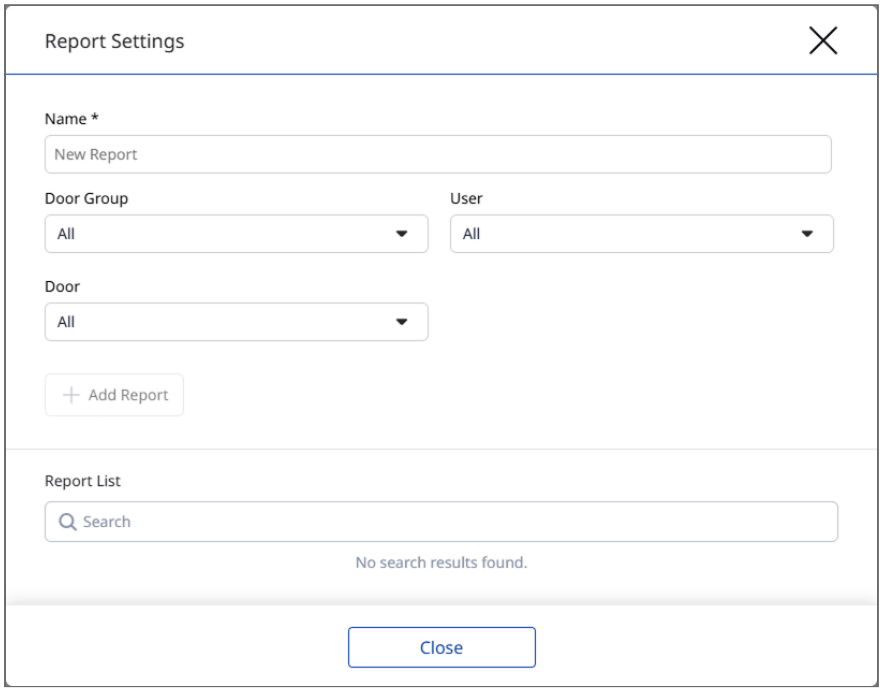
Información

- Si una o más puertas están sin conexión, el sistema aplica los cambios cuando se reconecten.
- El nivel de acceso **Acceso completo** lo administra automáticamente el sistema, por lo que no se puede cambiar.
- Los errores en ciertas puertas pueden impedir que el sistema aplique niveles de acceso. Un cuadro de diálogo muestra las puertas donde falló el cambio de nivel de acceso. Para volver a intentarlo, haga clic en **Reintentar las fallidas**.

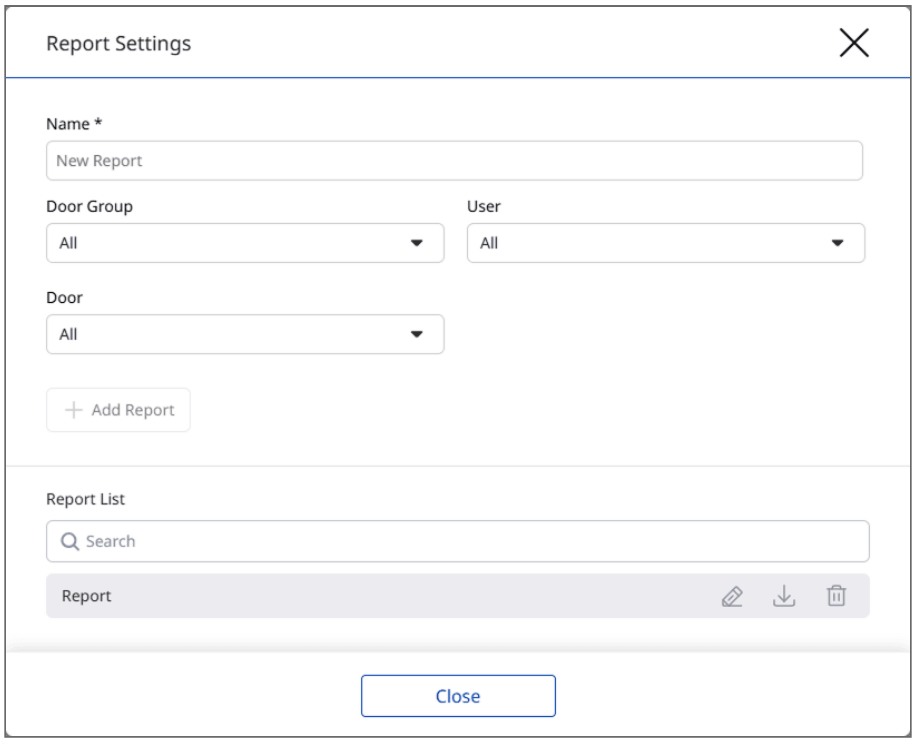
Generar informes de puertas

Genere informes de puertas y envíelos al correo electrónico del administrador. Un informe de puerta proporciona información sobre los usuarios que ingresaron por esa puerta.

1. Haga clic en **Gestión de Puerta** → **Registrados Puerta** en la barra lateral izquierda.
2. Haga clic en en la parte superior de la lista de puertas.
3. Cuando aparezca la ventana **Configuración de informes**, ingrese un nombre para el informe.



4. Seleccione los elementos que desea incluir en el informe.
5. Haga clic en **Agregar informe** para guardar el informe.
6. Se crea un **Lista de informes** y se envía un enlace de descarga al correo electrónico del administrador.



> **Información**
>
> En **Lista de informes**, busque, edite, descargue o elimine los informes generados.

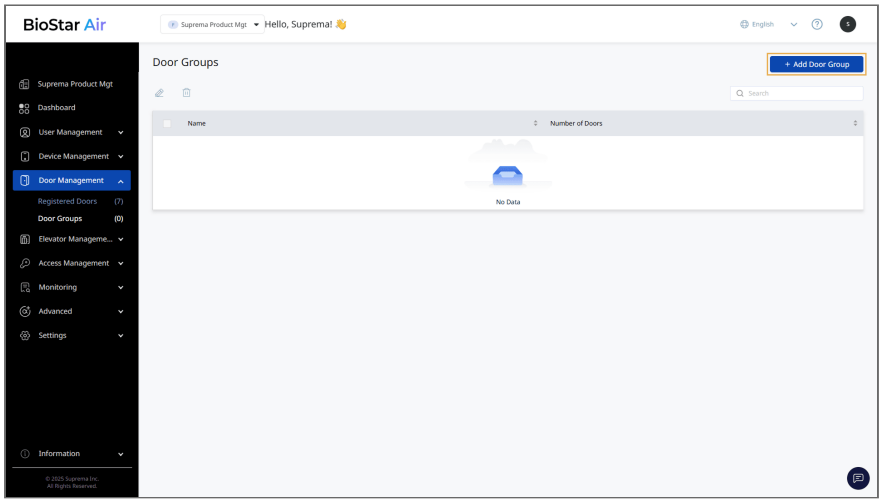
Administrar Grupo de Puertas

Al agrupar las puertas, puede gestionar las políticas de control de acceso con mayor eficiencia. Aplique políticas de seguridad coherentes a varias puertas asignando niveles de acceso y permisos a los grupos de forma simultánea.

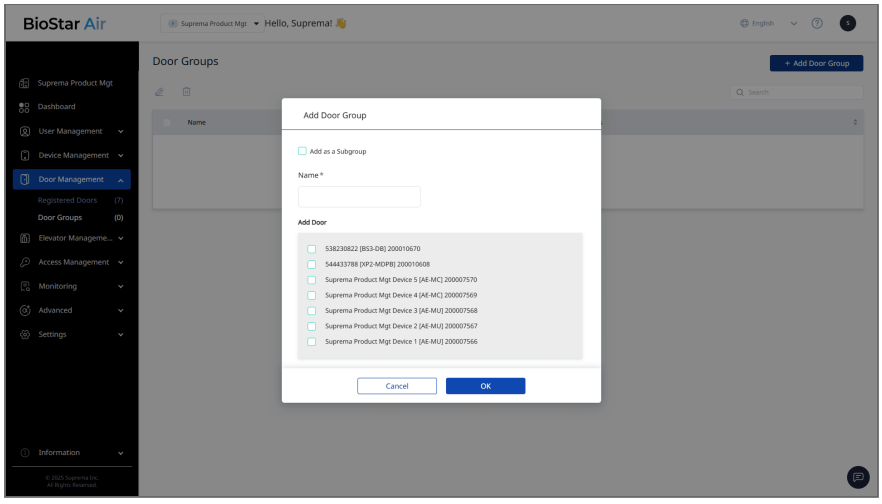
> **Información**
>
> - Para obtener más información sobre la gestión de puertas registradas, consulte Administrar puertas registradas.
> - Para obtener más información sobre los niveles de acceso, consulte Administrar Niveles de Acceso.

Agregar grupo de puertas

1. Haga clic en **Gestión de Puerta** → **Grupo de Puerta** en la barra lateral izquierda.
2. Haga clic en **Nombre del Grupo de Puerta** en la parte superior derecha de la pantalla.



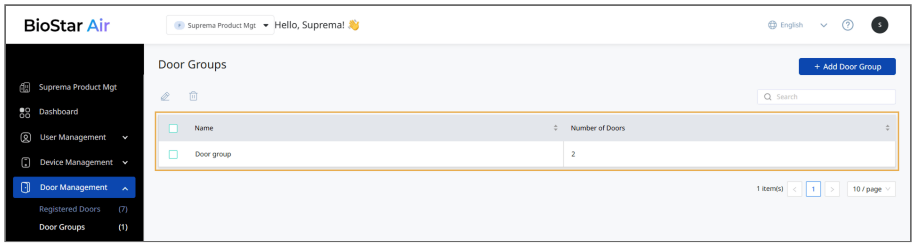
3. Cuando aparezca la ventana **Nombre del Grupo de Puerta**, ingrese el nombre del grupo de puertas.



> Haga clic en **Agregar como un subgrupo** y seleccione el grupo padre para agregar el grupo de dispositivos como subgrupo de un grupo específico.

4. En **Agregar Puerta**, seleccione las puertas que desea incluir en el grupo.
5. Haga clic en **OK** para guardar el grupo de puertas.

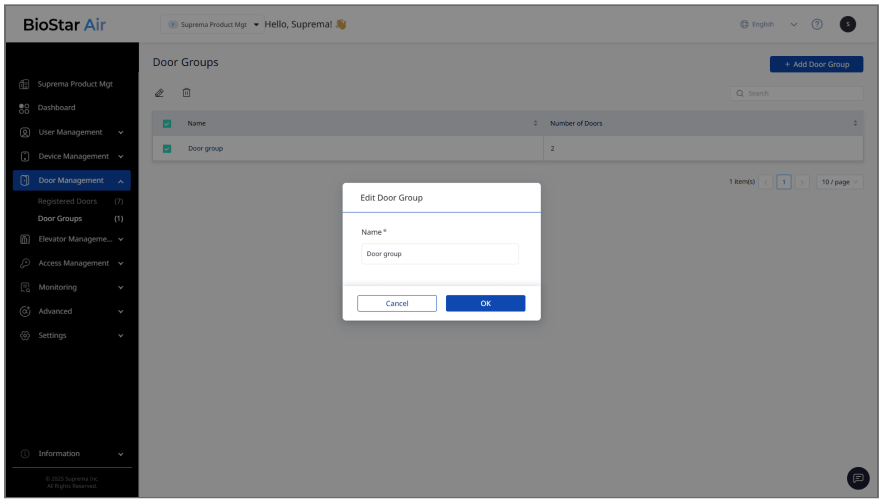
La lista de grupos de puertas muestra el grupo recién agregado y la cantidad de puertas que contiene. Haga clic en un grupo de puertas para ver las puertas que incluye.



> **Información**
>
> - Las puertas agregadas a un subgrupo no se incluyen automáticamente en el grupo padre.
> - Agregar un grupo padre vacío sin dispositivos ni puertas.

Renombrar grupo de puertas

1. Haga clic en **Gestión de Puerta** → **Grupo de Puerta** en la barra lateral izquierda.
2. Marque la casilla del grupo de puertas que desea renombrar en la lista.
3. Haga clic en ✎ en la parte superior de la lista de grupos de puertas.
4. Cuando aparezca la ventana **Agregar Grupo de Puerta**, ingrese el nuevo nombre del grupo.



5. Haga clic en **OK** para guardar el nuevo nombre del grupo.

Eliminar grupo de puertas

1. Haga clic en **Gestión de Puerta** → **Grupo de Puerta** en la barra lateral izquierda.

2. Marque la casilla del grupo de puertas que desea eliminar de la lista.
3. Haga clic en en la parte superior de la lista de grupos de puertas.
4. Cuando aparezca un mensaje de advertencia, haga clic en **Sí**.

El grupo de puertas seleccionado se eliminará de la lista. Sus subgrupos también se eliminarán. Las puertas de acceso no se eliminarán al borrar el grupo.

Administrar horarios de las puertas

Puede configurar horarios para que las puertas se bloqueen y se desbloqueen automáticamente según períodos de tiempo. Configure los horarios de bloqueo y desbloqueo y utilice opciones avanzadas como **abrir después de la primera autenticación** para mantener un acceso seguro y controlado.

> **Información**
>
> - Los horarios solo se aplican a puertas y dispositivos que estén conectados a Internet.
> - Los grupos de días festivos ignoran los horarios de desbloqueo a menos que se configuren por separado.
> - Mantenga al menos un administrador con acceso sin restricciones para emergencias.

Cuándo necesita horarios

Los horarios de las puertas son opcionales. La mayoría de los sitios funcionan correctamente con el control de acceso básico. Cuando un usuario autorizado presenta una credencial válida, la puerta se desbloquea automáticamente; no es necesaria ninguna configuración adicional de horarios.

Configure los horarios únicamente en las siguientes situaciones:

- Cuando necesite permitir acceso sin restricciones durante períodos específicos
- Cuando necesite bloquear el acceso a todos los usuarios durante períodos específicos
- Cuando necesite aplicar diferentes políticas de acceso en distintos horarios

Para evitar confusiones entre **Horario de desbloqueo** y **Horario de bloqueo** en BioStar Air, comprenda cómo funciona cada uno y cuándo utilizarlo.

Horario de desbloqueo vs Horario de bloqueo

Categoría	Horario de desbloqueo	Horario de bloqueo
Estado de la puerta durante el horario	Siempre desbloqueada	Siempre bloqueada
Autenticación requerida	No requerida; cualquiera puede acceder libremente	Las credenciales no pueden desbloquear la puerta
Desbloqueo manual	Posible	Solo el administrador del sitio puede desbloquearla
Operación del relé	Activado de forma continua	No se activa

> **Información**
>
> El término 'Administrador del sitio' se refiere a los administradores designados en el portal BioStar Air Admin o en la aplicación móvil.

Horario de desbloqueo

Durante el período programado, la puerta permanece desbloqueada y el relé permanece activado de forma continua. No se requiere autenticación; cualquiera puede entrar libremente durante este tiempo.

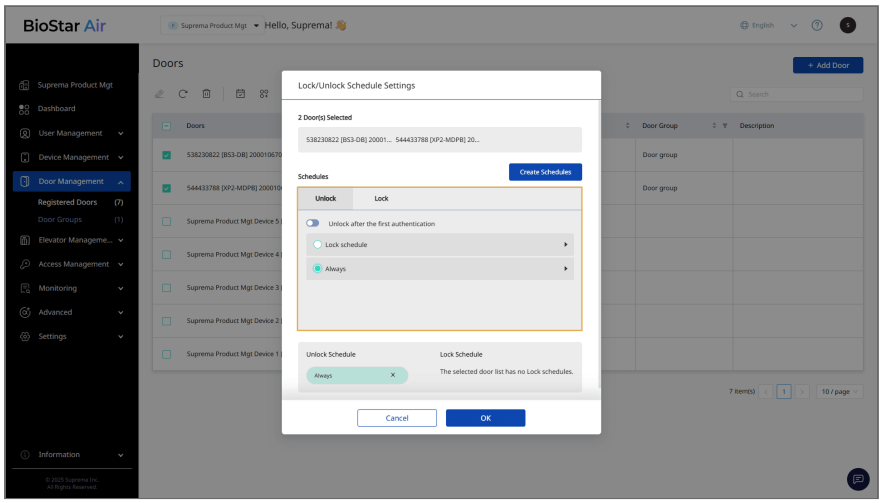
Casos de uso típicos

- Puertas principales en áreas públicas
- Áreas comunes en comunidades residenciales
- Puertas del vestíbulo de oficinas durante el horario laboral

Configurar horarios de desbloqueo

Configure un horario de desbloqueo como se indica a continuación.

1. Haga clic en **Gestión de Puerta** → **Registrados Puerta** en la barra lateral izquierda.
2. En la lista, marque la casilla de la puerta cuya programación de desbloqueo desea configurar.
3. Haga clic en en la parte superior de la lista de puertas.
4. Cuando aparezca la ventana **Configuración de programación de bloqueo/desbloqueo**, seleccione un horario predefinido o cree uno nuevo en la pestaña **Desbloquear**.



5. Haga clic en **OK** para aplicar el horario de desbloqueo.

Información

- Cuando **Desbloquear después de la primera autenticación** esté habilitado, la puerta permanecerá desbloqueada según el horario seleccionado después de que el primer usuario se autentique. Esta opción es útil en las siguientes situaciones.
  - Tiendas que solo abren después de la llegada del personal
  - Oficinas donde el primer empleado en llegar desbloquea el edificio para los demás
  - Instalaciones que requieren que el personal inicie el acceso antes de que los miembros puedan entrar
- Para obtener más información sobre cómo registrar horarios, consulte Registrar un nuevo horario.

Horario de bloqueo

Durante el período programado, la puerta permanece bloqueada y el relé no se activa. Incluso si se presenta una credencial válida, la puerta no puede desbloquearse mediante autenticación. Solo un administrador del sitio puede desbloquearla manualmente desde el portal BioStar Air Admin o la aplicación móvil.

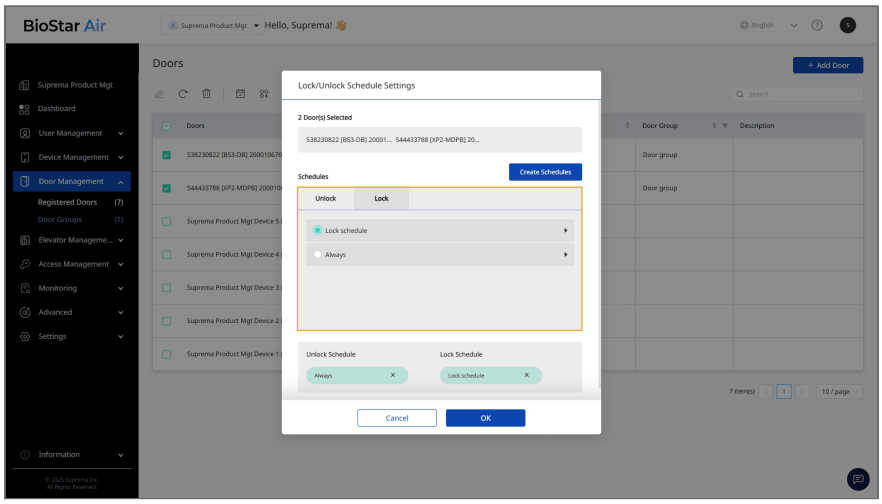
Casos de uso típicos

- Áreas que deben permanecer estrictamente cerradas después de ciertas horas
- Instalaciones como piscinas, gimnasios u otras áreas restringidas

Configurar horarios de bloqueo

Configure un horario de bloqueo como se indica a continuación.

1. Haga clic en **Gestión de Puerta** → **Registrados Puerta** en la barra lateral izquierda.
2. En la lista, marque la casilla de la puerta cuya programación de bloqueo desea configurar.
3. Haga clic en en la parte superior de la lista de puertas.
4. Cuando aparezca la ventana **Configuración de programación de bloqueo/desbloqueo**, seleccione un horario predefinido o cree uno nuevo en la pestaña **Bloquear**.



5. Haga clic en **OK** para aplicar el horario de bloqueo.

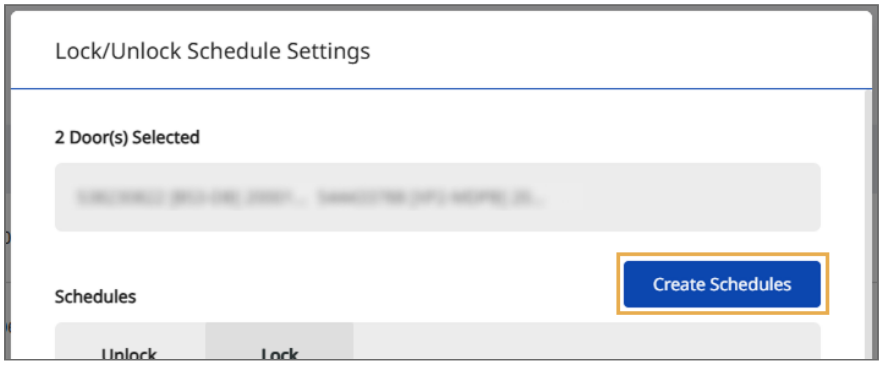
Información

- Debido a que un horario de bloqueo anula los derechos de acceso estándar, los usuarios no pueden dejar la puerta desbloqueada durante el período de bloqueo.
- Para obtener más información sobre cómo registrar nuevos horarios, consulte Registrar un nuevo horario.

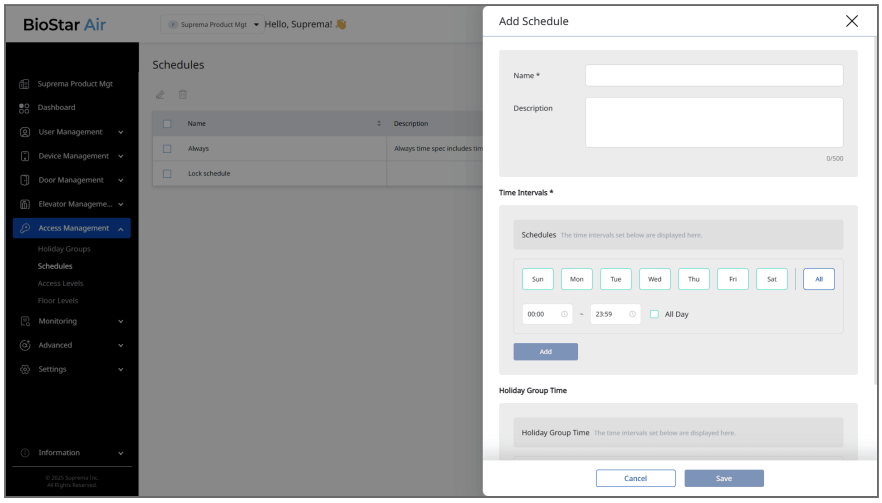
Registrar un nuevo horario

Siga los pasos a continuación para registrar un nuevo horario.

1. En la ventana **Configuración de programación de bloqueo/desbloqueo**, haga clic en **Crear Horarios**.



2. En la pantalla Agregar horario, ingrese **Nombre** y **Descripción** (opcional).



3. En la sección **Intervalos de tiempo ***, seleccione los días y los horarios en los que la puerta debe permanecer abierta sin autenticación y, a continuación, haga clic en **Agregar**.

4. Haga clic en **Guardar** para guardar el horario.

Después de registrar un nuevo horario, vuelva a **Gestión de Puerta** → **Registrados Puerta** y configure el horario de la puerta.

Ascensores

BioStar Air es compatible con el control de acceso de ascensores mediante el módulo OM-120 de Suprema. Gracias a este módulo, los administradores pueden integrar lectores compatibles con BioStar Air para controlar el acceso a los pisos. Una conexión en cadena de dispositivos OM-120 permite controlar hasta 144 pisos.

Consejo

Vea la siguiente guía en video sobre cómo gestionar ascensores.

Administrar Ascensores

Para configurar el control de acceso del ascensor, primero conecte el módulo OM-120 al dispositivo de control de acceso. Luego, asigne el nombre y el número de relé de cada piso y restrinja los horarios de acceso por piso para mejorar la seguridad.

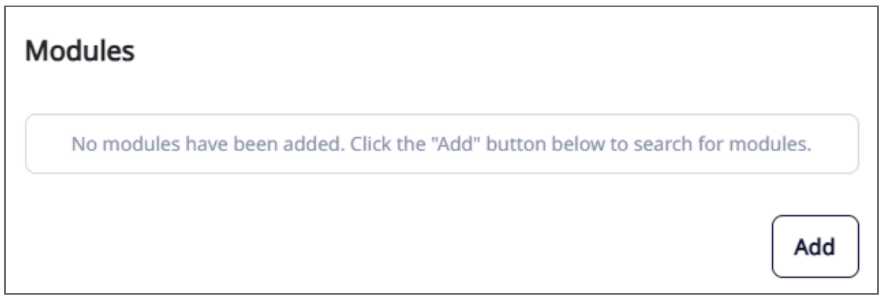
Requisitos

Cumpla los siguientes requisitos para activar la función de control de acceso del ascensor.

- Suprema OM-120 module: Cada módulo admite hasta 12 pisos. Conectar hasta 12 módulos OM-120 a un único dispositivo de control de acceso permite controlar hasta 144 pisos.
- Se requiere un dispositivo compatible con BioStar Air que pueda conectarse al OM-120.
- Se requiere un cableado adecuado al panel de control del ascensor. Para detalles sobre el cableado, contacte al fabricante del ascensor.
- Los horarios de acceso por piso tienen prioridad, y la configuración de días festivos puede anular las reglas normales de acceso.

Conectar dispositivos y módulos

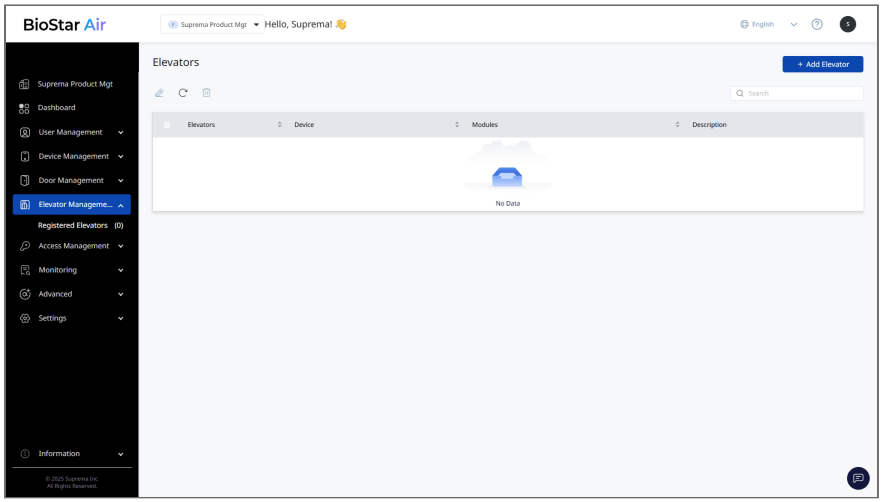
1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haga clic en el dispositivo de control de acceso que tenga un módulo OM-120 en la lista de dispositivos.
3. En la sección **Módulos**, haga clic en **Agregar**.



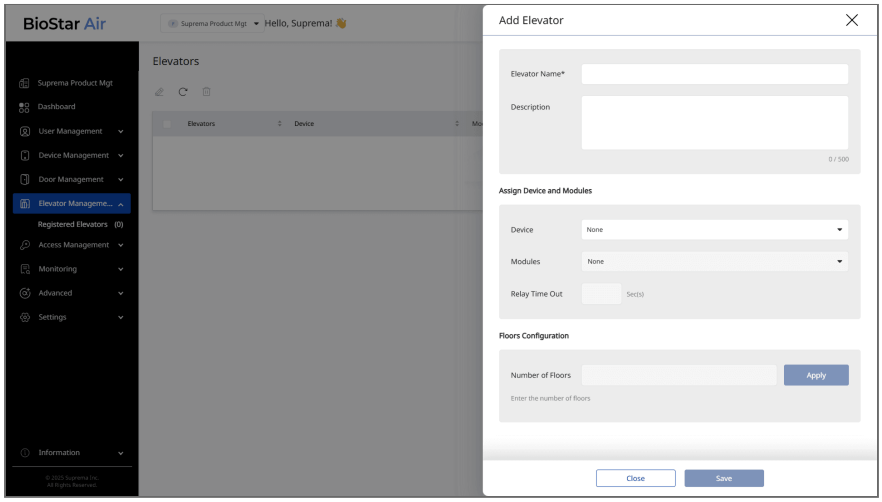
4. Seleccione el módulo OM-120 conectado al dispositivo y haga clic en **Guardar**.

Registrar ascensores

1. Haga clic en **Gestión de ascensores** → **Ascensores Registrados** en la barra lateral izquierda.
2. Haga clic en **Añadir ascensor** en la parte superior derecha de la pantalla.



3. Cuando aparezca el panel **Añadir ascensor**, ingrese **Nombre del ascensor** y **Descripción** (opcional).



4. En la sección **Asignar dispositivos y módulos**, seleccione el dispositivo y el módulo para la autenticación de acceso.

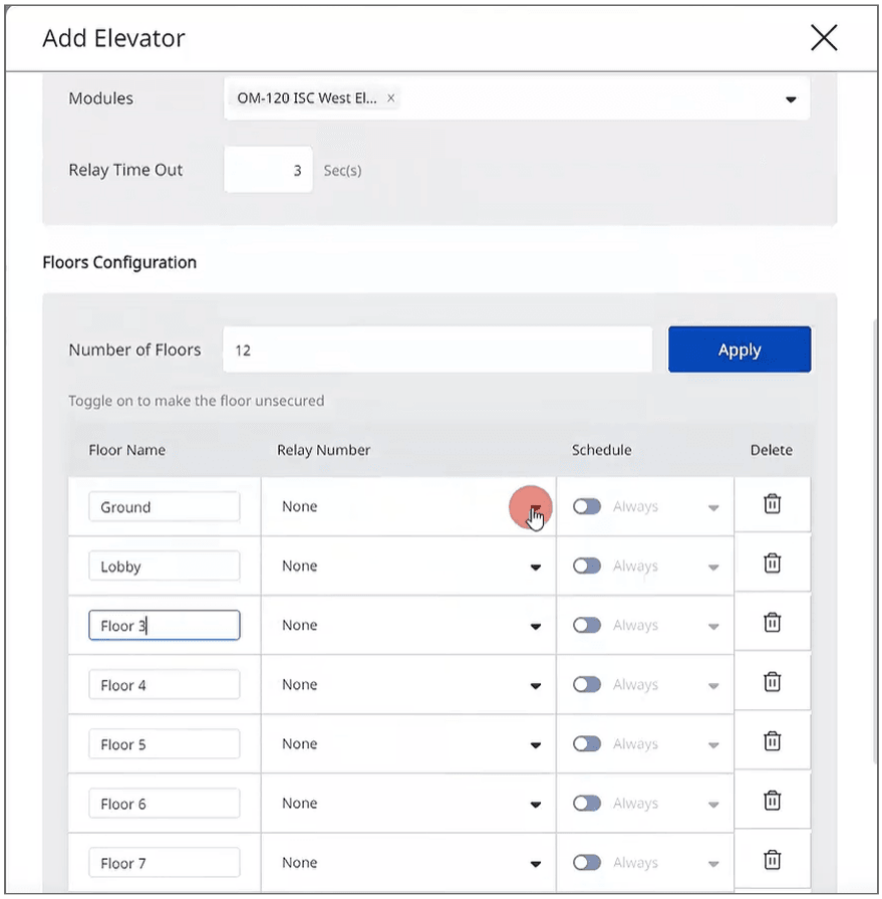
   - **Borrar**: Seleccione el dispositivo para la autenticación de acceso.

     > **Precaución**
     >
     > Si el dispositivo no aparece en la lista, verifique que esté asignado a una puerta. Un dispositivo no puede asignarse simultáneamente a una puerta y a un elevador.

   - **Módulos**: Seleccione el módulo OM-120 que controlará el relé del botón del ascensor.
   - **Tiempo de espera del relevo**: Establezca el tiempo durante el cual el botón del piso permanecerá activo después de completar la autenticación. Tras ese tiempo, el relé dejará de activar el botón del piso.

5. En la sección **Configuración de pisos**, ingrese el número de pisos a controlar y haga clic en **Aplicar**.

6. Configure el nombre, el número de relé y el horario de cada piso.



La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

- **Nombre del piso**: Ingrese el nombre del piso. Use nombres fácilmente identificables como 1F, vestíbulo o sala de conferencias.
- **Número de relé**: Seleccione la salida de relé que corresponde a cada botón de piso en el panel de control del ascensor.
- **Horario**: Establezca el horario de acceso para cada piso. Por ejemplo, puede restringir el acceso al piso de mantenimiento fuera del horario laboral.

7. Haga clic en **Guardar** para guardar y registrar la configuración del elevador.

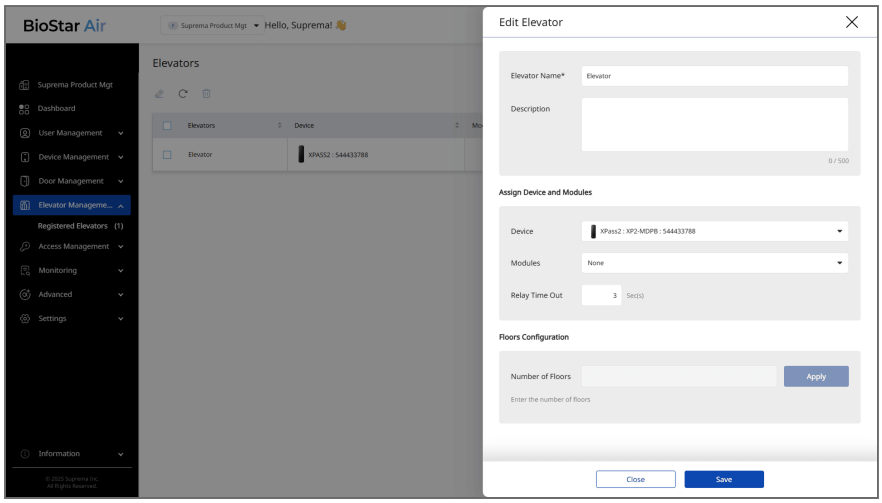
> **Información**
>
> - Cada módulo OM-120 admite hasta 12 pisos. Conecte varios módulos OM-120 en cadena para ampliar hasta 144 pisos.
> - En la sección **Configuración de pisos**, haga clic en para eliminar un piso.
> - Para obtener más información sobre cómo registrar horarios, consulte Administrar horarios.

Editar elevadores

Siga estos pasos para cambiar los detalles o la configuración de un elevador registrado.

1. Haga clic en **Gestión de ascensores** → **Ascensores Registrados** en la barra lateral izquierda.
2. En la lista, haga clic en el elevador que desea editar. Como alternativa, seleccione la casilla del elevador y haga clic en en la parte superior de la lista.

3. Cuando aparezca el panel **Editar ascensor**, cambie la información necesaria o modifique la configuración.



4. Haga clic en **Guardar** para guardar los cambios.

Eliminar elevadores

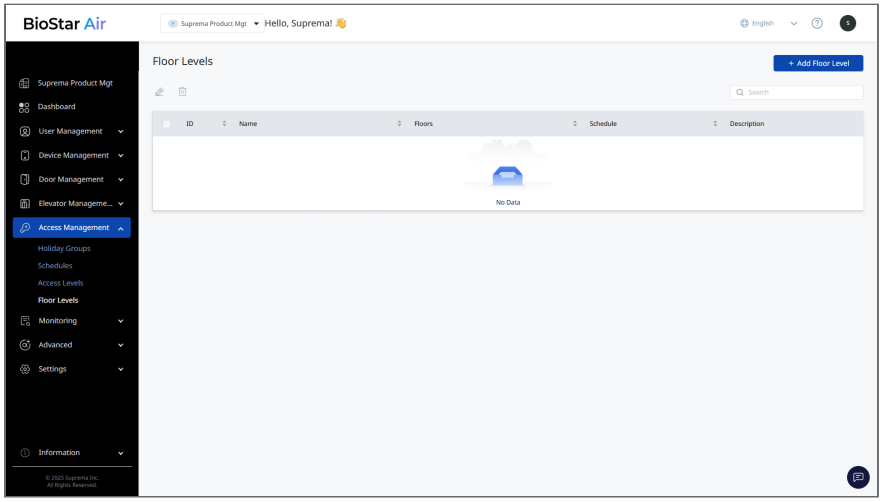
Siga estos pasos para eliminar un elevador registrado.

1. Haga clic en **Gestión de ascensores** → **Ascensores Registrados** en la barra lateral izquierda.
2. En la lista, seleccione la casilla del elevador que desea eliminar. Puede seleccionar uno o varios elevadores.
3. Haga clic en en la parte superior de la lista.
4. Cuando aparezca un mensaje de advertencia, haga clic en **Sí**.

Establecer permisos de acceso por piso

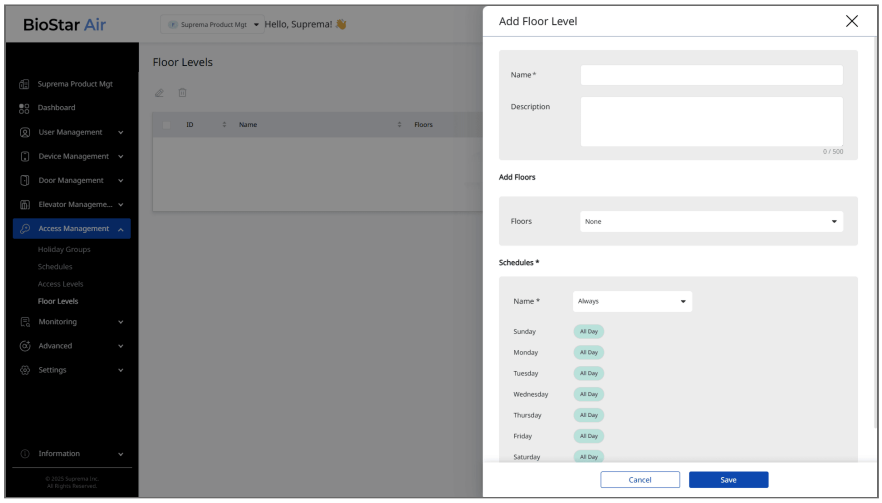
Registre un elevador y defina niveles de piso para restringir el acceso de usuarios y grupos a determinados pisos. Para cada nivel de piso, establezca horarios de acceso (p. ej., durante el horario laboral) y políticas de días festivos para gestionar la seguridad y la accesibilidad.

1. Haga clic en **Gestión de Acceso** → **Niveles de piso** en la barra lateral izquierda.
2. Haga clic en **Agregar nivel de piso** en la parte superior derecha de la pantalla.



3. Cuando aparezca el **Agregar nivel de piso** panel, ingrese **Nombre** y (opcional) **Descripción**.

> *Por ejemplo: equipo de seguridad, personal de limpieza*



4. En la sección **Agregar pisos**, seleccione los pisos a los que se aplicará el nivel de piso.
5. En la sección **Horarios**, establezca el horario de acceso.

   > *Por ejemplo, permitir que el personal de limpieza acceda únicamente fuera del horario laboral.*

6. Si es necesario, agregue **Grupos de festivos** para restringir el acceso en fechas específicas.
7. Haga clic en **Guardar** para agregar el nivel de piso.

> **Información**
>
> Para obtener más información sobre cómo agregar, editar o eliminar niveles de piso, consulte Gestionar Niveles de Piso.

Permisos de acceso

La gestión de los permisos de acceso es fundamental en un sistema de seguridad. Para controlar con precisión cuándo y dónde tienen acceso los usuarios, combina grupos de días festivos, horarios, niveles de acceso y niveles de piso.

> **Consejo**
>
> Consulta la siguiente guía en video sobre cómo gestionar los permisos de acceso.

Gestionar grupos de días festivos

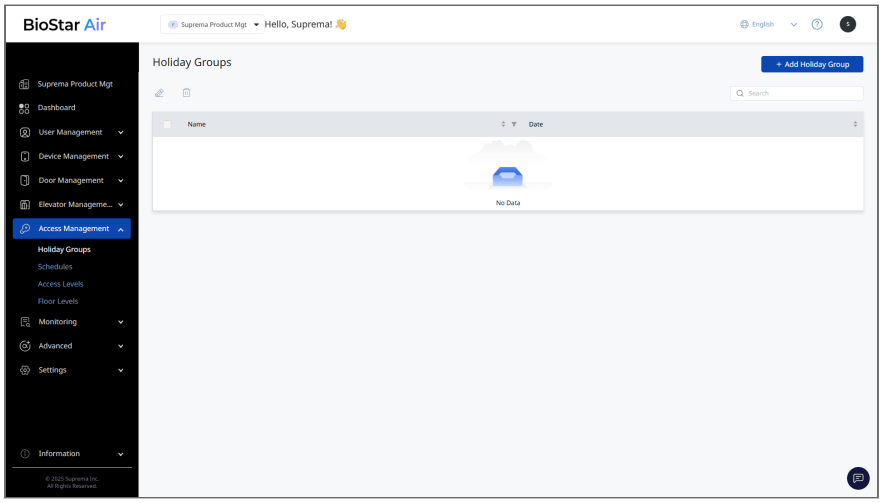
En BioStar Air, un grupo de días festivos sirve para ajustar las reglas de acceso en fechas o periodos específicos. Al configurar un grupo de días festivos, los administradores pueden restringir o modificar los permisos de acceso durante los días festivos o en fechas especiales. Este enfoque mantiene la seguridad a la vez que ofrece un control de acceso flexible.

> **Consejo**
>
> Vea el siguiente video para obtener una guía sobre la gestión del control de acceso.

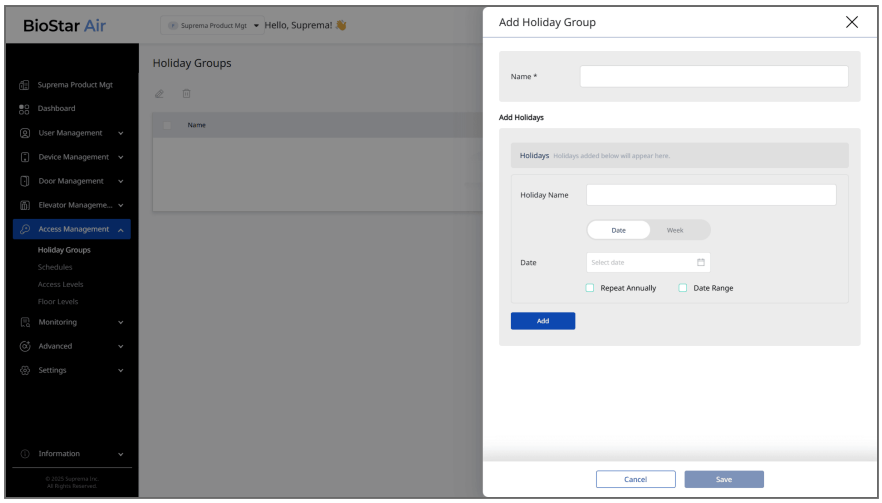
Agregar un grupo de días festivos

Un grupo de días festivos define los días festivos que se repiten anualmente y los que ocurren dentro de periodos específicos. Se utiliza para restringir o modificar los permisos de acceso durante esos periodos.

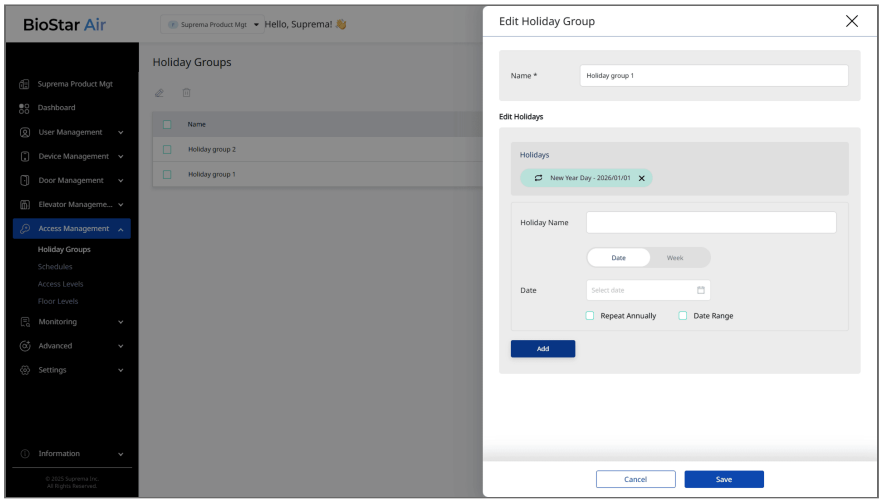
1. Haz clic en **Gestión de Acceso** → **Grupos de festivos** en la barra lateral izquierda.
2. Haz clic en **Agregar grupo de festivos** en la esquina superior derecha de la pantalla.



3. Cuando aparezca el panel **Agregar grupo de festivos**, escribe el nombre del grupo.



4. En la sección **Añadir días Festivos**, especifica el nombre y la fecha del feriado, y haz clic en **Agregar**.
   - Define el nombre y la fecha, y selecciona la opción **Repetir anualmente** para agregar un feriado público con fecha fija.
   - Define el nombre y la fecha, y selecciona la opción **Rango de fechas** para feriados que se repiten anualmente y abarcan un período determinado.
5. Agrega otros feriados de la misma forma.

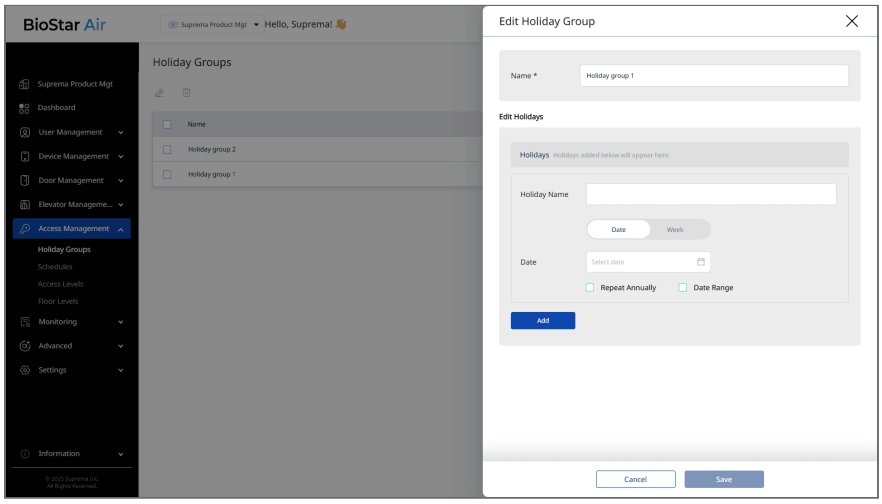


6. Haz clic en **Guardar** para guardar la configuración del grupo de feriados.

> **Información**
>
> - Los grupos de días festivos tienen prioridad sobre los horarios. Conceda acceso sin restricciones a los usuarios que siempre necesitan acceso.
> - Solo se puede aplicar un grupo de días festivos a una sola puerta.

Editar un grupo de días festivos

1. Haz clic en **Gestión de Acceso** → **Grupos de festivos** en la barra lateral izquierda.
2. Haga clic en el grupo de días festivos que desea editar en la lista. Alternativamente, seleccione la casilla del grupo de días festivos y, a continuación, haga clic en en la parte superior de la lista.
3. Cuando aparezca el panel **Editar grupos de vacaciones**, edite los elementos necesarios.



4. Haga clic en **Guardar** para guardar los cambios.

Eliminar un grupo de días festivos

1. Haz clic en **Gestión de Acceso** → **Grupos de festivos** en la barra lateral izquierda.
2. Seleccione la casilla del grupo de días festivos en la lista. Puede seleccionar varios grupos de días festivos.

3. Haga clic en en la parte superior de la lista.

4. Cuando aparezca un mensaje de advertencia, haga clic en **Sí**.

Administrar horarios

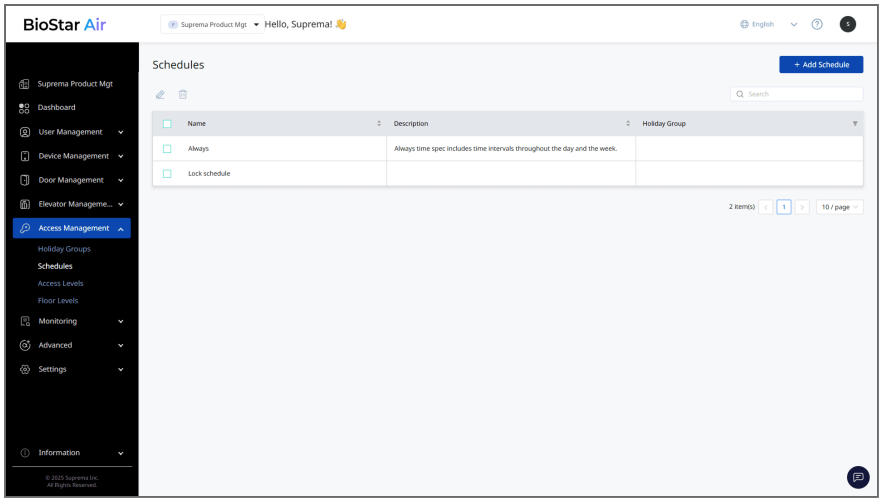
Crear horarios para permitir o restringir el acceso a puertas o ascensores en días y períodos de tiempo específicos. Úselos junto con grupos de días festivos para ajustar las reglas de acceso.

> **Información**
>
> - Los grupos de días festivos tienen prioridad sobre los horarios. Conceda acceso sin restricciones a los usuarios que siempre necesitan acceso.
> - Para obtener más información sobre la configuración de grupos de días festivos, consulte Gestionar grupos de días festivos.
> - Para obtener más información sobre cómo aplicar horarios a puertas, consulte Administrar horarios de las puertas.
> - Para obtener más información sobre cómo configurar horarios para controlar el acceso a cada piso del ascensor, consulte Ascensores.

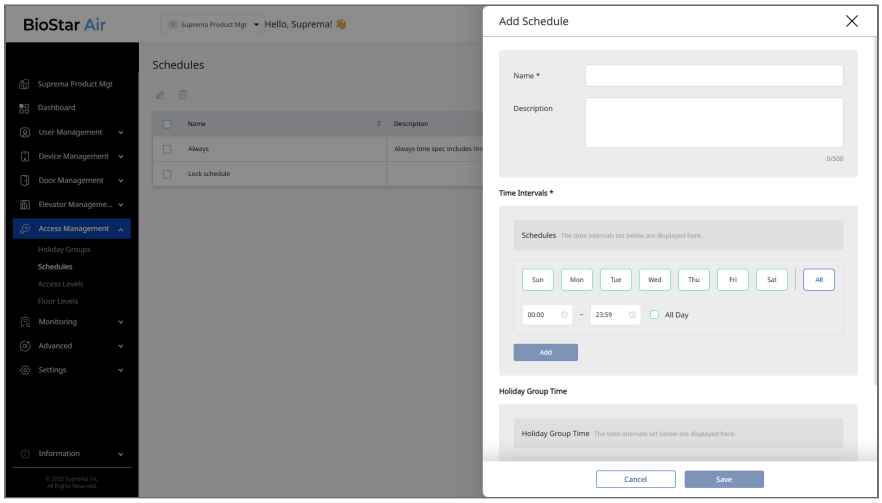
Agregar horario

1. Haz clic en **Gestión de Acceso** → **Horarios** en la barra lateral izquierda.

2. Haz clic en **Agregar Horarios** en la esquina superior derecha de la pantalla.



3. Cuando aparezca el panel **Agregar Horarios**, ingresa **Nombre** y **Descripción** (opcional).

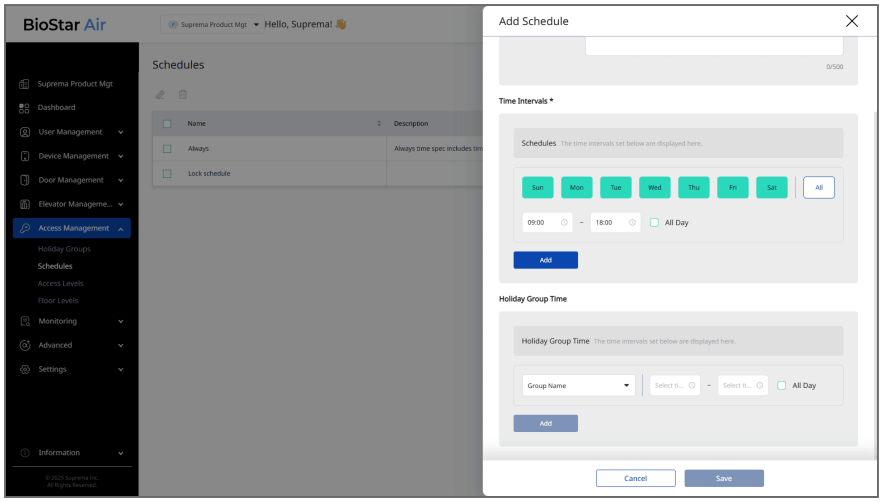


4. En la sección **Intervalos de tiempo ***, selecciona los días y los intervalos de tiempo.

> *Selecciona de lunes a viernes, de 9:00 a.m. a 6:00 p.m., para definir el horario laboral. Selecciona sábado y domingo, o de 6:00 p.m. a 9:00 a.m. todos los días, para definir un horario fuera de horario laboral.*

5. Haz clic en **Agregar** para aplicar el horario seleccionado.

6. En la sección **Tiempo de grupo de vacaciones**, selecciona el grupo de días festivos que se aplicará al horario y establece los intervalos de tiempo.



7. Haz clic en **Agregar** para aplicar el grupo de días festivos.

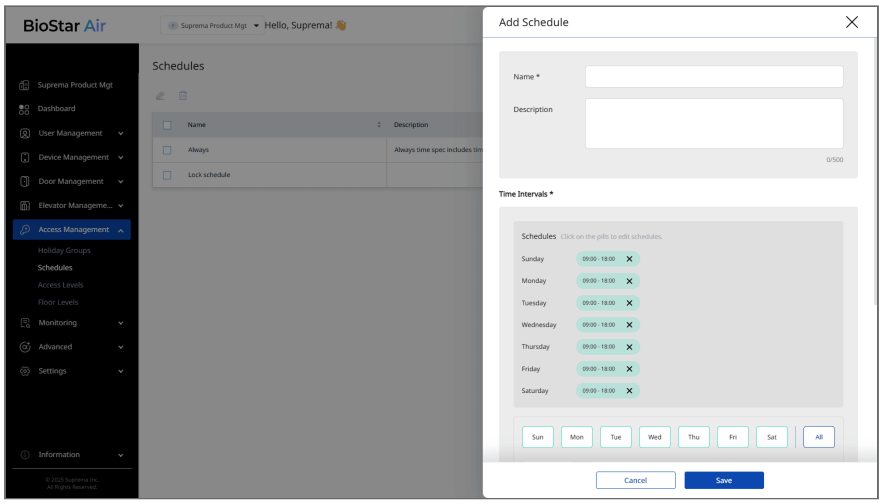
8. Haz clic en **Guardar** para agregar el horario.

Información

- Agregue horarios abiertos para permitir el acceso y horarios cerrados para restringirlo, y aplíquelos a las puertas. Para obtener más información sobre cómo aplicar horarios a puertas, consulte Administrar horarios de las puertas.
- Solo se puede asignar un único grupo de días festivos a un horario.
- Para obtener más información sobre cómo configurar horarios para controlar el acceso a cada piso del ascensor, consulte Ascensores.

Editar horario

1. Haz clic en **Gestión de Acceso** → **Horarios** en la barra lateral izquierda.
2. Haga clic en el horario que desea editar en la lista. Alternativamente, seleccione la casilla del horario y haga clic en en la parte superior de la lista.
3. Cuando aparezca el panel **Editar horarios**, actualice la información requerida o modifique el horario.



4. Haga clic en **Guardar** para guardar los cambios.

Eliminar horario

1. Haz clic en **Gestión de Acceso** → **Horarios** en la barra lateral izquierda.
2. Seleccione la casilla del horario que desea eliminar en la lista. Seleccione uno o más horarios.
3. Haga clic en en la parte superior de la lista.
4. Cuando aparezca un mensaje de advertencia, haga clic en **Sí**.

> **Información**
> Al eliminar un horario, este se quita de todas las secciones relacionadas. Por ejemplo, si se elimina un horario aplicado a una puerta o a un ascensor, ya no se aplicará a esa puerta o a ese ascensor.

Administrar Niveles de Acceso

Utilice los niveles de acceso para controlar con precisión el acceso de los usuarios. Los niveles de acceso definen quién puede acceder, dónde y cuándo. Un nivel de acceso consta de los siguientes elementos.

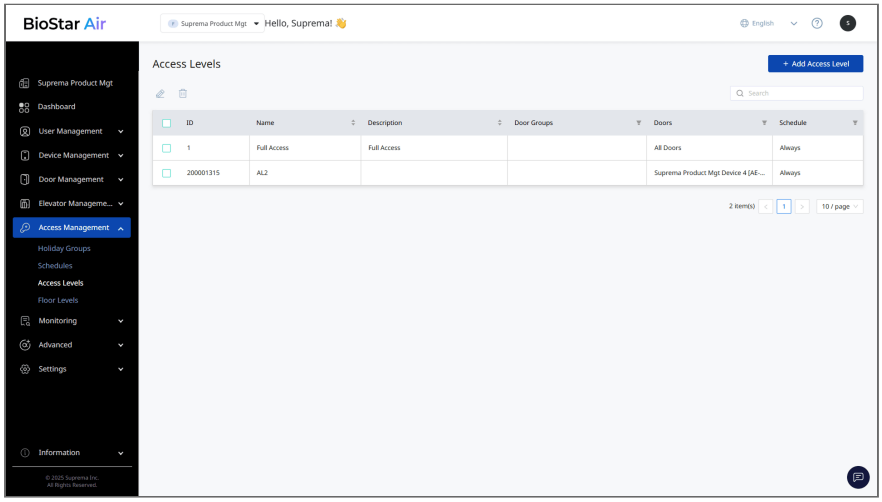
- **Puerta / grupo de puertas**: Ubicación donde se permite el acceso
- **Horario**: Período en el que se permite el acceso
- **Grupo de días festivos**: Fechas o períodos que restringen o ajustan el acceso

Configure los niveles de acceso antes de agregar usuarios para agilizar la gestión de usuarios.

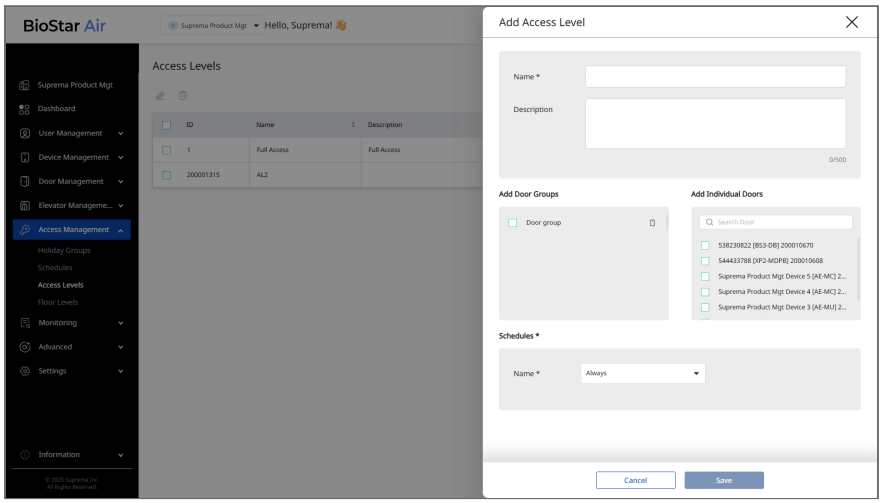
Agregar nivel de acceso

Utilice los niveles de acceso para establecer permisos de usuario según la puerta, el horario y el grupo de días festivos.

1. Haga clic en **Gestión de Acceso** → **Niveles de acceso** en la barra lateral izquierda.
2. Haga clic en **Agregar Nivel de Acceso** en la esquina superior derecha de la pantalla.



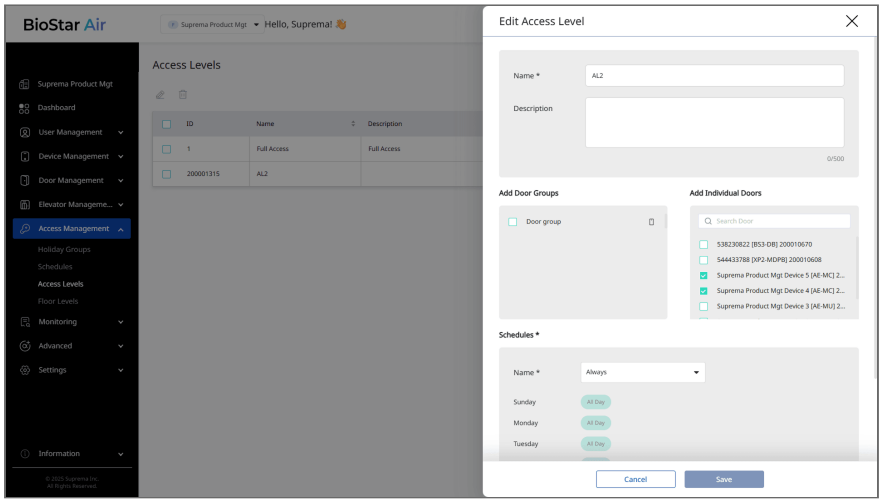
3. Cuando aparezca el panel **Agregar Nivel de Acceso**, ingrese **Nombre** y **Descripción** (opcional).



4. En la sección **Nombre del Grupo de Puerta** o **Añadir puertas individuales**, seleccione grupos de puertas o puertas individuales.
5. En la sección **Horarios**, seleccione el horario que se aplicará al nivel de acceso. Seleccione **Siempre** para permitir acceso sin restricciones.
6. Haga clic en **Guardar** para agregar el nivel de acceso.

Modificar nivel de acceso

1. Haga clic en **Gestión de Acceso** → **Niveles de acceso** en la barra lateral izquierda.
2. Haga clic en el nivel de acceso que desea modificar en la lista de niveles de acceso. Alternativamente, seleccione la casilla del nivel de acceso que desea modificar y haga clic en ✎ en la parte superior de la lista.



3. Cuando aparezca el panel **Editar Nivel de acceso**, edite la información requerida o cambie la configuración.
4. Haga clic en **Guardar** para guardar los cambios.

Eliminar nivel de acceso

1. Haga clic en **Gestión de Acceso** → **Niveles de acceso** en la barra lateral izquierda.
2. Marque la casilla del nivel de acceso que desea eliminar en la lista de niveles de acceso. Puede seleccionar más de un nivel de acceso.
3. Haga clic en en la parte superior de la lista.
4. Cuando aparezca un mensaje de advertencia, haga clic en **Sí**.

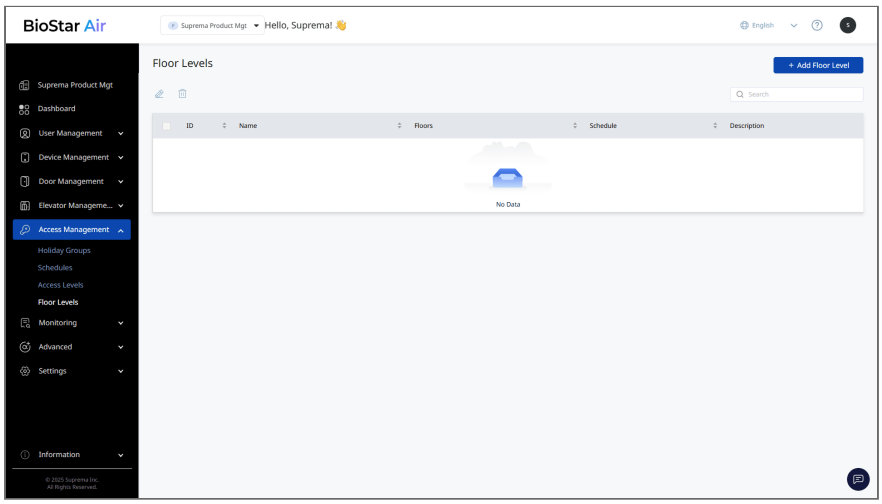
Gestionar Niveles de Piso

Los niveles de piso se utilizan en la configuración de control de acceso de los ascensores. Permiten un control más detallado de los permisos de acceso para cada piso. Por ejemplo, configure determinados grupos de usuarios para que solo puedan acceder a niveles de piso específicos.

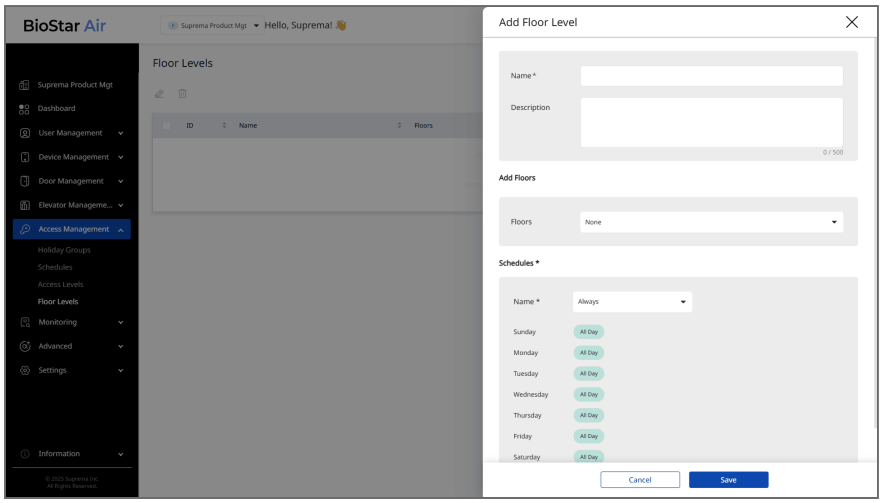
Agregar niveles de piso

Asigne usuarios o grupos que tendrán acceso a pisos específicos.

1. Haga clic en **Gestión de Acceso** → **Niveles de piso** en la barra lateral izquierda.
2. Haga clic en **Agregar nivel de piso** en la parte superior derecha de la pantalla.



3. Cuando aparezca el panel **Agregar nivel de piso**, ingrese **Nombre** y **Descripción** (opcional).



4. Seleccione los pisos a los que desea aplicar permisos en la sección **Agregar pisos**.

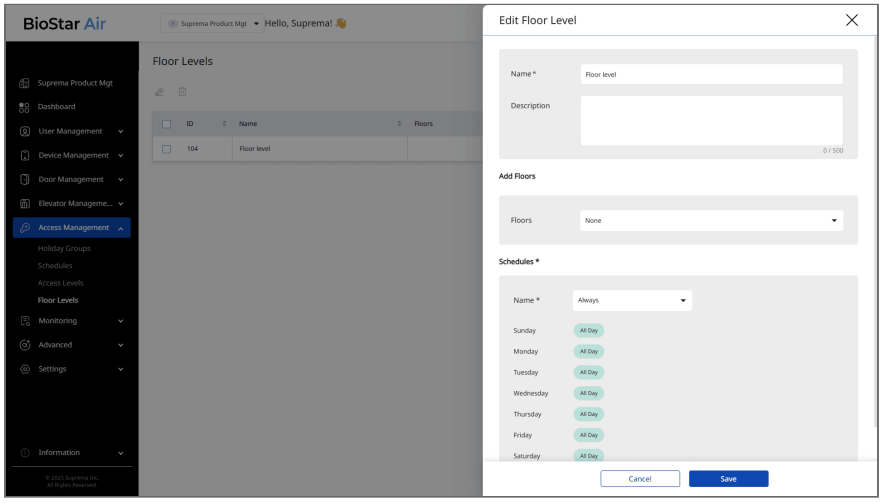
5. Seleccione el horario que se aplicará al nivel de piso en la sección **Horario**. Seleccione **Siempre** para permitir el acceso sin restricciones.

6. Haga clic en **Guardar** para agregar el nivel de piso.

Editar niveles de piso

1. Haga clic en **Gestión de Acceso** → **Niveles de piso** en la barra lateral izquierda.

2. Haga clic en el nivel de piso que desea editar en la lista. Como alternativa, seleccione la casilla de verificación del nivel de piso que desea editar y luego haga clic en en la parte superior de la lista.



3. Cuando aparezca el panel **Editar nivel de piso**, modifique la información necesaria o ajuste la configuración.

4. Haga clic en **Guardar** para guardar los cambios.

Eliminar niveles de piso

1. Haga clic en **Gestión de Acceso** → **Niveles de piso** en la barra lateral izquierda.

2. Seleccione la casilla de verificación del nivel de piso que desea eliminar de la lista. Puede seleccionar más de un nivel de piso.

3. Haga clic en en la parte superior de la lista.
4. Cuando aparezca un mensaje de advertencia, haga clic en **Sí**.

Administración de Zonas

Las zonas son agrupaciones lógicas de puertas y dispositivos. Se usan para anti-passback, estado en sitio, conteo de personas y otras aplicaciones futuras.

Comprender las zonas y el anti-passback (APB)

Al usar zonas para el anti-passback, el administrador debe definir puntos de entrada y puntos de salida para la zona. Estos puntos determinan cuándo un usuario con credencial está dentro o fuera de la zona. Un usuario con credencial no puede reingresar a la zona sin salir primero, aunque use una credencial diferente. El anti-passback también se usa para definir puntos claros de entrada y salida, y evita que los usuarios regresen y salgan por una entrada.

Zona perimetral

Al igual que el anti-passback, BioStar Air define una **zona perimetral** que determina el estado en sitio de un usuario con credencial. Esto es importante para las funciones **En sitio ahora** y **Pase de lista**. De forma opcional, se puede configurar la zona perimetral para anti-passback.

Consulte los siguientes documentos para saber cómo administrar las zonas y las infracciones de APB en el portal de BioStar Air.

Administrar Zonas
Con la feature **Zona** de BioStar Air, agrupe puertas en zonas lógicas. Aplique reglas de **Anti-Passback (APB)** para que los usuarios entren y salgan en el orden correcto. Aplique reglas de Anti-Passback por zona, de forma opcional. Las zonas sin APB aún pueden usar otras features de Zona, como Presencia, para ver quién está dentro. Las **zonas** pueden abarcar desde zonas de perímetro que cubren todo un sitio hasta áreas específicas dentro de un edificio.

Antes de comenzar

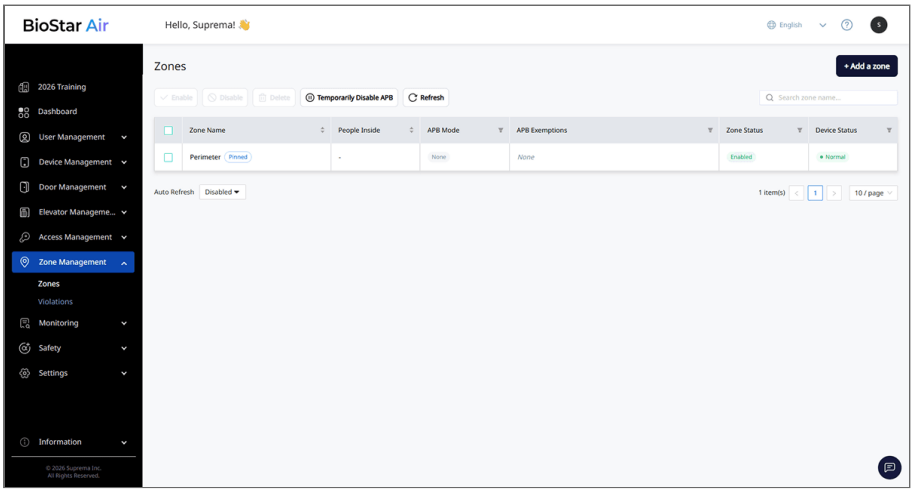
Revise lo siguiente antes de crear una zona.

- Agregue las puertas al sistema antes de asignarlas a una zona. Para obtener más información sobre el registro de puertas, consulte Administrar puertas registradas.
- Un dispositivo solo puede usarse en una zona a la vez.
- Cambiar los dispositivos de entrada y salida de la zona no cambia los ajustes de la puerta.
- Si los dispositivos de entrada y salida de la zona no se ajustan correctamente, el comportamiento de APB y el conteo de presencia pueden diferir del movimiento real.
- Los dispositivos sin conexión pueden aplicar los cambios más tarde que los dispositivos en línea. El sistema aplica los cambios primero a los dispositivos en línea. Los dispositivos sin conexión aplican los cambios después de volver a conectarse.
- El sistema solo asigna a una zona dispositivos con firmware **v2.13** o posterior. Verifique que el dispositivo asignado a la zona use el firmware más reciente.
- El sistema protege las puertas usadas en una zona APB para evitar conflictos de ajustes. Para cambiar los ajustes de la puerta que afectan el comportamiento de APB, primero quite la puerta de la zona.

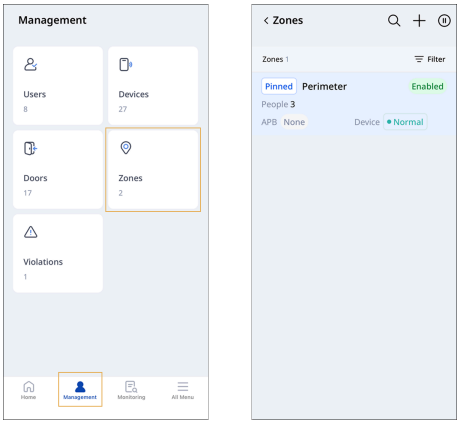
Explorar la lista de zonas

Web

Haz clic en **Gestión de zonas** → **Zonas** en la barra lateral izquierda.



Mobile



1. Abra la aplicación BioStar Air en su dispositivo móvil e inicie sesión.
2. Toque **Administrar** en la parte inferior de la pantalla.
3. Toque la tarjeta **Zonas**.

La lista de zonas muestra de un vistazo todas las zonas configuradas para el sitio.

- **Nombre de la zona**: Nombre de la zona. **Perímetro** muestra la insignia **Fijada** junto al nombre.
- **Personas dentro**: Número de usuarios registrados como presentes en la zona. Para obtener más información, consulte Comprobar personas en el interior.
- **Modo APB**: El modo APB aplicado a la zona (**Hard** / **Soft** / **Ninguno**).
- **Exenciones de APB**: El grupo de exención de APB asignado a la zona.
- **Estado de la zona**: Indica si la zona está activada.
- **Estado del dispositivo**: Indica si los dispositivos asignados a la zona están en línea.

Zonas perimetrales y zonas internas

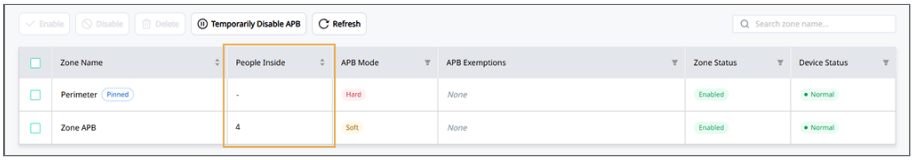
En la configuración inicial del sitio, el sistema proporciona **Perímetro** de forma predeterminada. **Perímetro** es como la puerta principal del sitio. Renombrar y eliminar no están disponibles, y la lista muestra la insignia **Fijada**.

- Los dispositivos de entrada y salida en **Perímetro** ayudan a calcular la presencia en **Panel de Control** > **Usuarios en el sitio** y **Seguridad** > **Presencia**.
- Cree zonas separadas para áreas que requieren control interno (p. ej., salas de servidores, ciertos pisos) además de zonas de perímetro, para habilitar un control de movimiento detallado en el sitio.

Comprobar personas en el interior

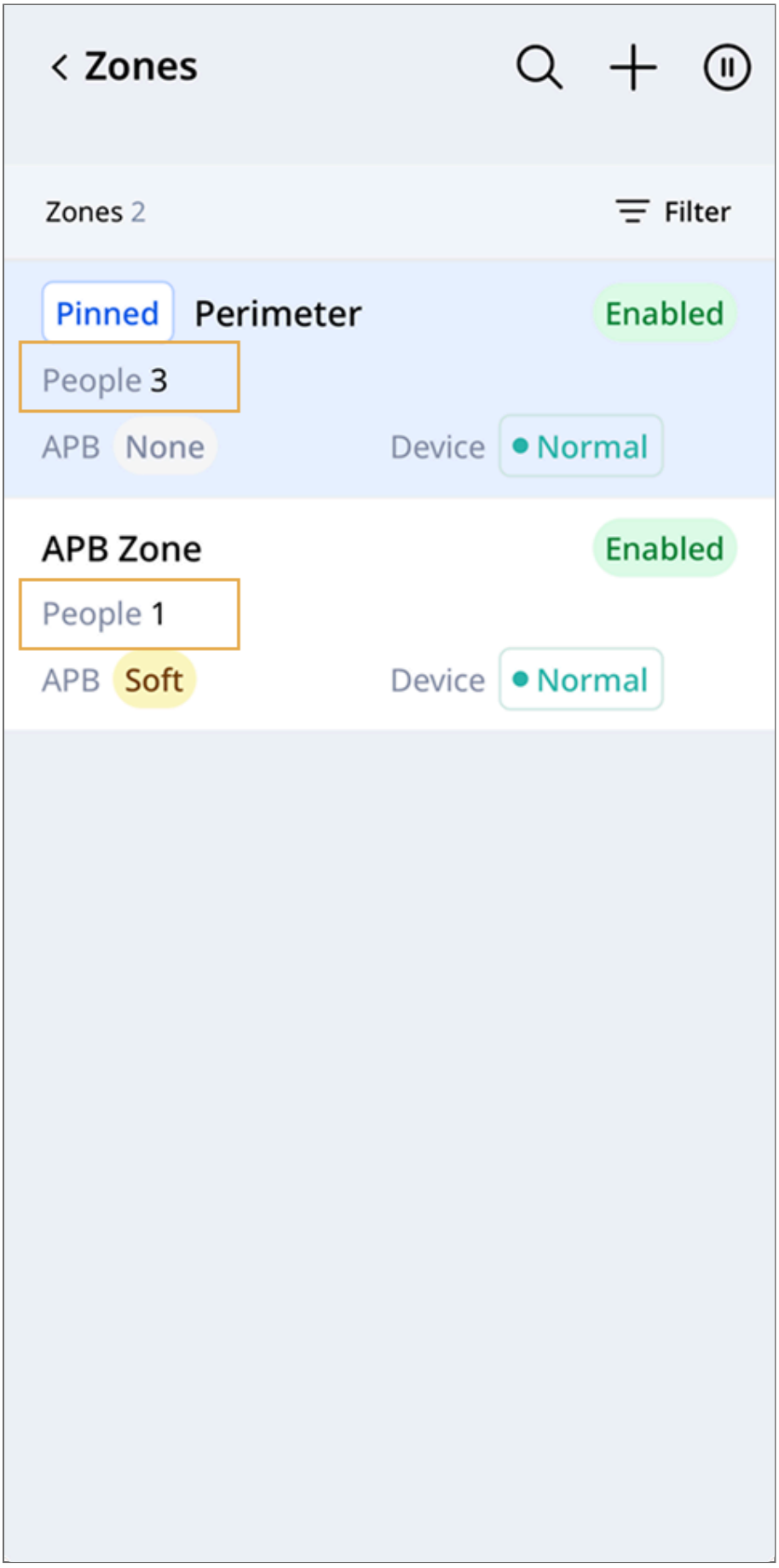
Web

Revise cuántas personas hay actualmente en cada zona en la columna **Personas dentro** de la lista de zonas.



Mobile

Revise cuántas personas hay actualmente en cada zona en la opción **People** de la lista de zonas.

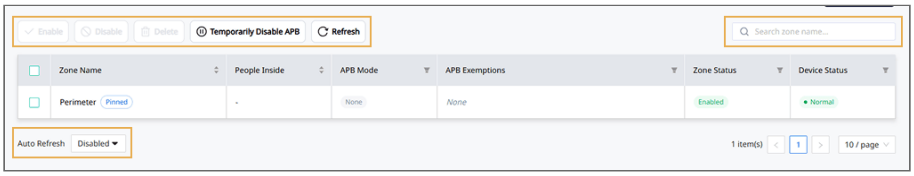


- El sistema calcula este número según los registros de autenticación de los dispositivos de entrada y salida definidos para la zona. Autentíquese en un dispositivo de entrada para aumentar el conteo, y autentíquese en un dispositivo de salida para disminuirlo.

- Los usuarios en un grupo de exención de APB no están sujetos a las reglas de APB, pero se incluyen en el recuento de personas dentro.
- Desactivar una zona inicializa el recuento de personas dentro de la zona en 0.
- Para mantener el valor más reciente, haga clic en **Actualizar** en la parte superior de la lista o defina un intervalo de actualización automática.

Feature para gestionar zonas

Use los features de gestión en la parte superior e inferior de la lista de zonas para completar las siguientes tareas.



- **Habilitar** / **Deshabilitar**: Habilite o deshabilite las zonas seleccionadas.
- **Eliminar**: Elimine las zonas seleccionadas. **Perímetro** no se puede eliminar.
- **Pausar APB**: Pausa APB para todas las zonas del sitio, incluida la zona de perímetro.
- **Actualizar**: Actualiza la lista de inmediato para mostrar el estado más reciente. En **Autorefrescar** en la parte inferior de la lista, seleccione un intervalo de actualización automática (**Desactivado** / **5 segundos** / **1 minuto**). El sistema actualiza la lista automáticamente según el intervalo establecido.
- **Buscar nombre de zona...**: Busca en la lista por nombre de zona.

Filtrar lista de zonas

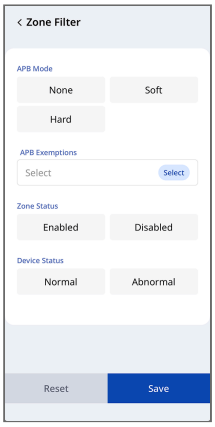
Web

En el encabezado de la lista, haga clic en el botón en la columna **Modo APB**, **Exenciones de APB**, **Estado de la zona** o **Estado del dispositivo** para filtrar la lista por esa condición.



> **Información**
> Haga clic en **Reiniciar** para borrar el filtro.

Mobile



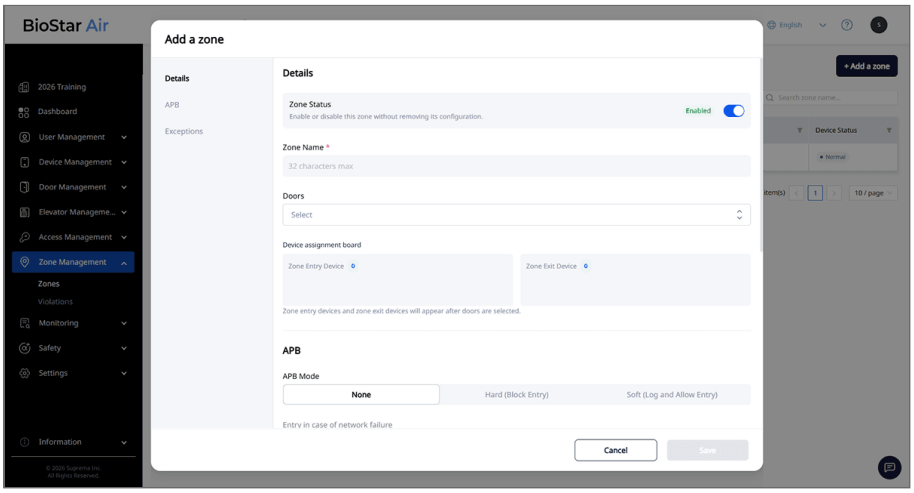
1. Toque **Filtros** en la esquina superior derecha de la lista de zonas.
2. Seleccione criterios en **Modo APB**, **Exenciones de APB**, **Estado de la zona** o **Estado del dispositivo**.
3. Toque **Guardar** para filtrar la lista según los criterios seleccionados.

> **Información**
> Toque **Reiniciar** para borrar el filtro.

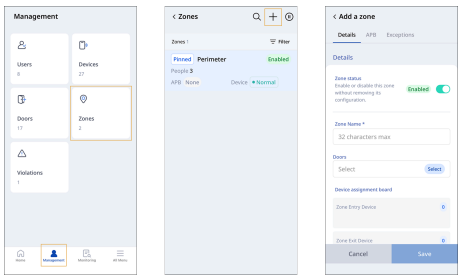
Agregar zonas

Web

Haz clic en **Gestión de zonas** → **Zonas** en la barra lateral izquierda. Haz clic en **+ Agregar una zona** en la esquina superior derecha de la pantalla.



Mobile

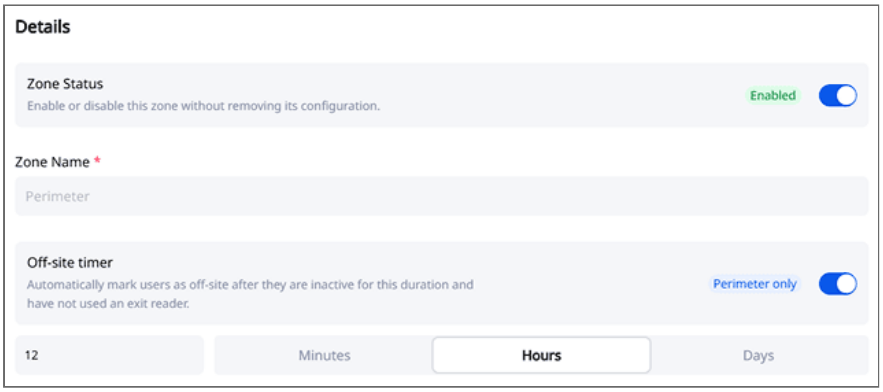


1. En la app BioStar Air, toque **Administrar** en la parte inferior de la pantalla.
2. Toque la tarjeta **Zonas**.
3. Toca + en la esquina superior derecha de la pantalla.

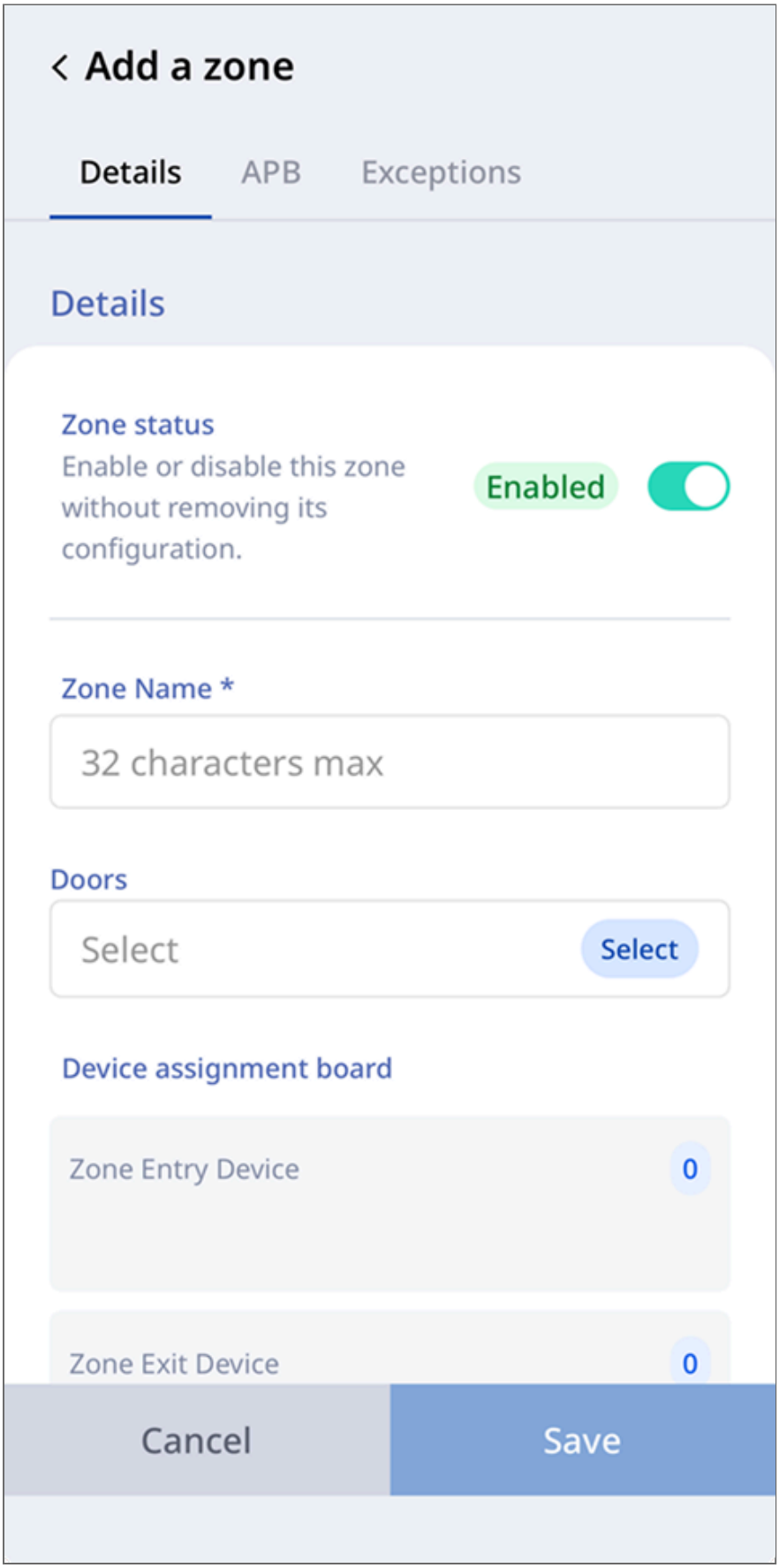
1 Ingresar información básica

Ingrese la información básica de la zona en la sección **Detalles**.

Web


Details
Zone Status
Enable or disable this zone without removing its configuration.
Enabled
Zone Name *
Perimeter
Off-site timer
Automatically mark users as off-site after they are inactive for this duration and have not used an exit reader.
Perimeter only
12
Minutes
Hours
Days

Mobile



- **Estado de la zona**: Seleccione si activa la zona de inmediato. Activa o desactiva la zona más adelante sin cambiar los ajustes.
- **Nombre de zona**: Ingrese hasta 32 caracteres. En sitios con varios edificios, usa un nombre que indique

claramente la ubicación.

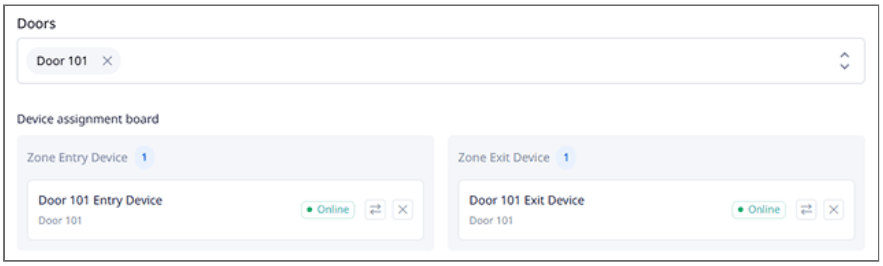
- **Temporizador de fuera del sitio**: Los usuarios sin actividad durante el tiempo establecido, y que no usaron un dispositivo de salida, cambian automáticamente al estado **Fuera del sitio**. Si no se asigna ningún dispositivo de salida a la zona de perímetro, establece esta opción.

> **Información**
> La opción **Temporizador de fuera del sitio** aparece solo al establecer una zona de perímetro.

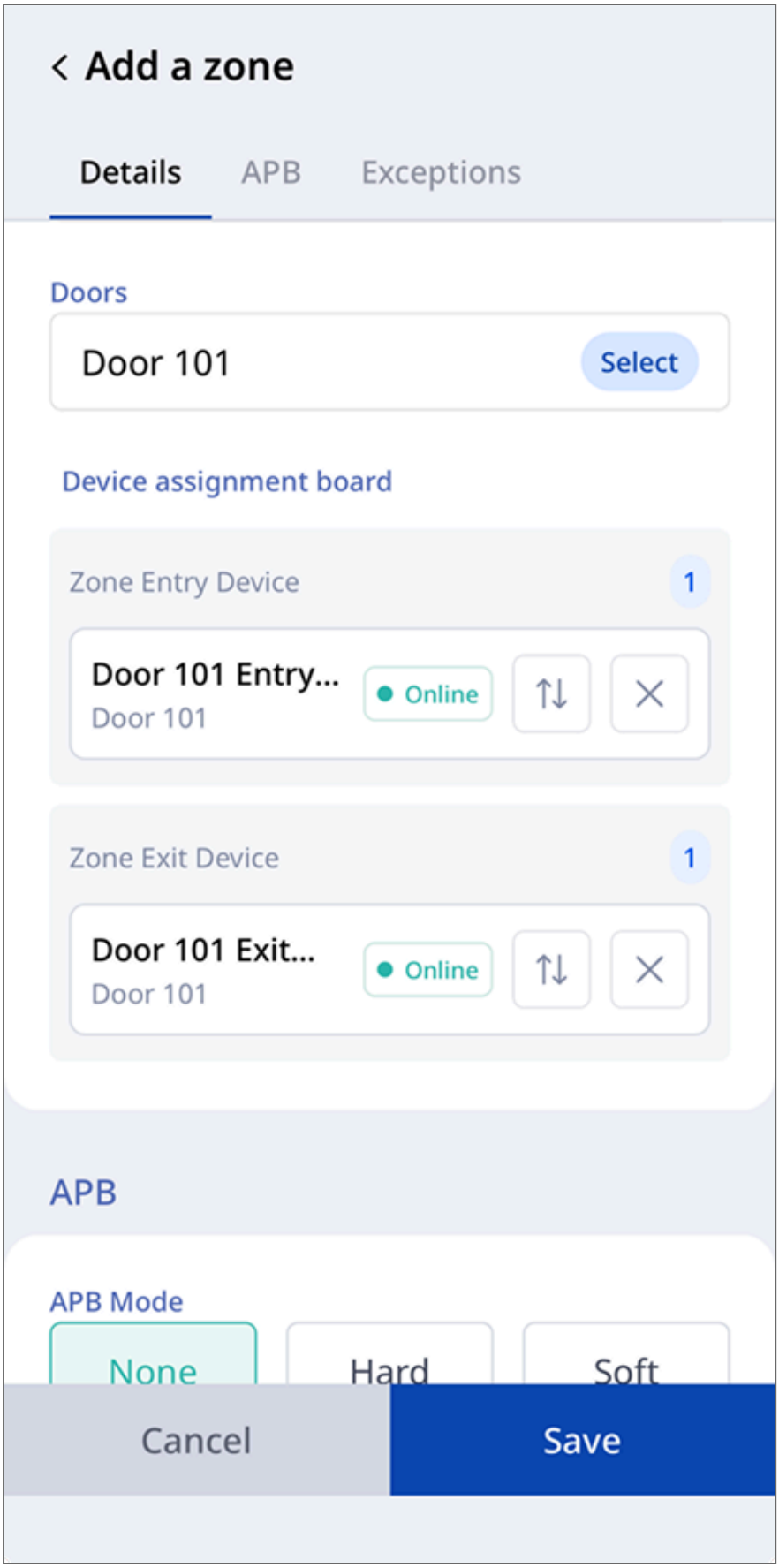
2 Asignar puertas y dispositivos

Seleccione las puertas y los dispositivos para asignarlos a la zona.

Web



Mobile



- **Puerta**: Seleccione las puertas para incluirlas en la zona. Se pueden seleccionar varias puertas. Seleccione una puerta. Sus dispositivos aparecen en **Panel de asignación de dispositivos**.
- **Panel de asignación de dispositivos**: Asigne cada dispositivo como **Dispositivo de entrada de zona** o

Dispositivo de salida de zona. Los dispositivos aparecen con **Identificación del dispositivo** para distinguirlos. Haga clic en el botón Mover (⇄) para establecer el dispositivo como dispositivo de entrada o salida.

Información

- Solo los dispositivos con firmware v2.13 o posterior aparecen en **Panel de asignación de dispositivos**. Verifique que el dispositivo asignado a la zona use el firmware más reciente.
- Para más información sobre la gestión de dispositivos, consulte Gestionar Grupos de Dispositivos y Paneles.
- Para obtener más información sobre la gestión de puertas registradas, consulte Administrar puertas registradas.

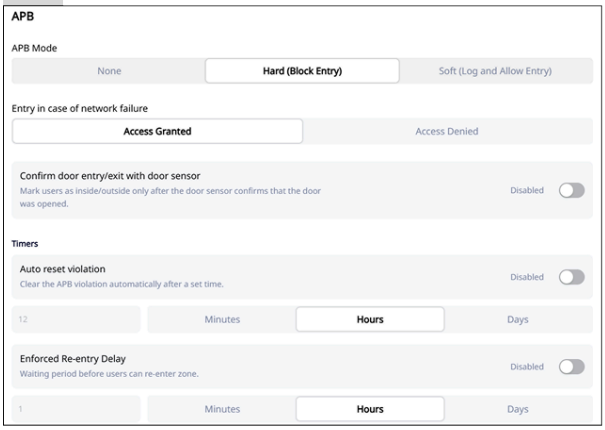
3 Establecer el modo APB

En la sección **APB**, establezca las reglas de antirretorno. Las reglas de Anti-Passback son opcionales. Si no necesita un control estricto, seleccione el modo **Ninguno** para usar las zonas solo para comprobaciones de Presencia.

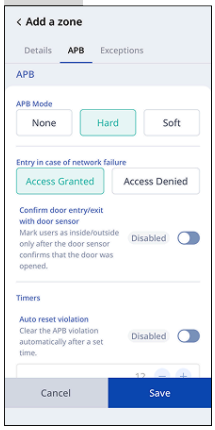
Hard

Hard (Bloquear entrada)

Web



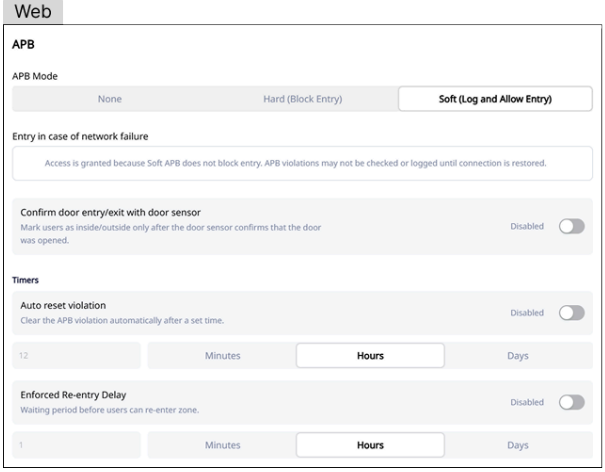
Mobile



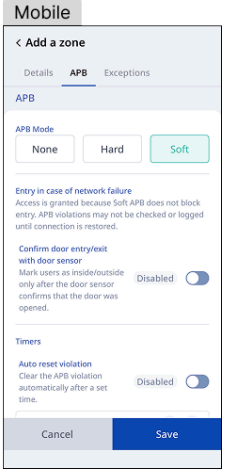
Soft

Soft (Registrar y permitir entrada)

Web



Mobile

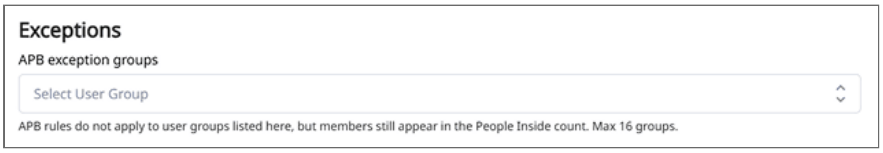


- **Modo APB**: Seleccione el modo APB.
  - **Hard (Bloquear entrada)**: Bloquea el acceso cuando un usuario infringe una regla APB y registra un evento de infracción.
  - **Soft (Registrar y permitir entrada)**: Permite el acceso, pero registra una infracción de APB en el registro de eventos.
  - **Ninguno**: No aplica APB a la zona. Las zonas sin un modo APB siguen contabilizando la presencia.
- **Entrada en caso de fallo de red**: Seleccione si permitir o denegar el acceso si el servidor BioStar Air no está disponible por una falla de red. El modo **Soft** no bloquea el acceso; siempre lo permite. El sistema quizá no verifique ni registre infracciones hasta que se recupere la conexión de red.
- **Confirmar entrada y salida con el sensor de puerta**: Cuando se habilita, el sensor de puerta debe confirmar que la puerta se abre antes de marcar a los usuarios como **En el sitio** o **Fuera del sitio**.
- **Temporizadores**
  - **Restablecer infracción automáticamente**: Borra automáticamente una infracción de APB después del tiempo establecido.
  - **Retraso de reingreso**: El tiempo de espera antes de que un usuario pueda entrar en la misma zona otra vez.

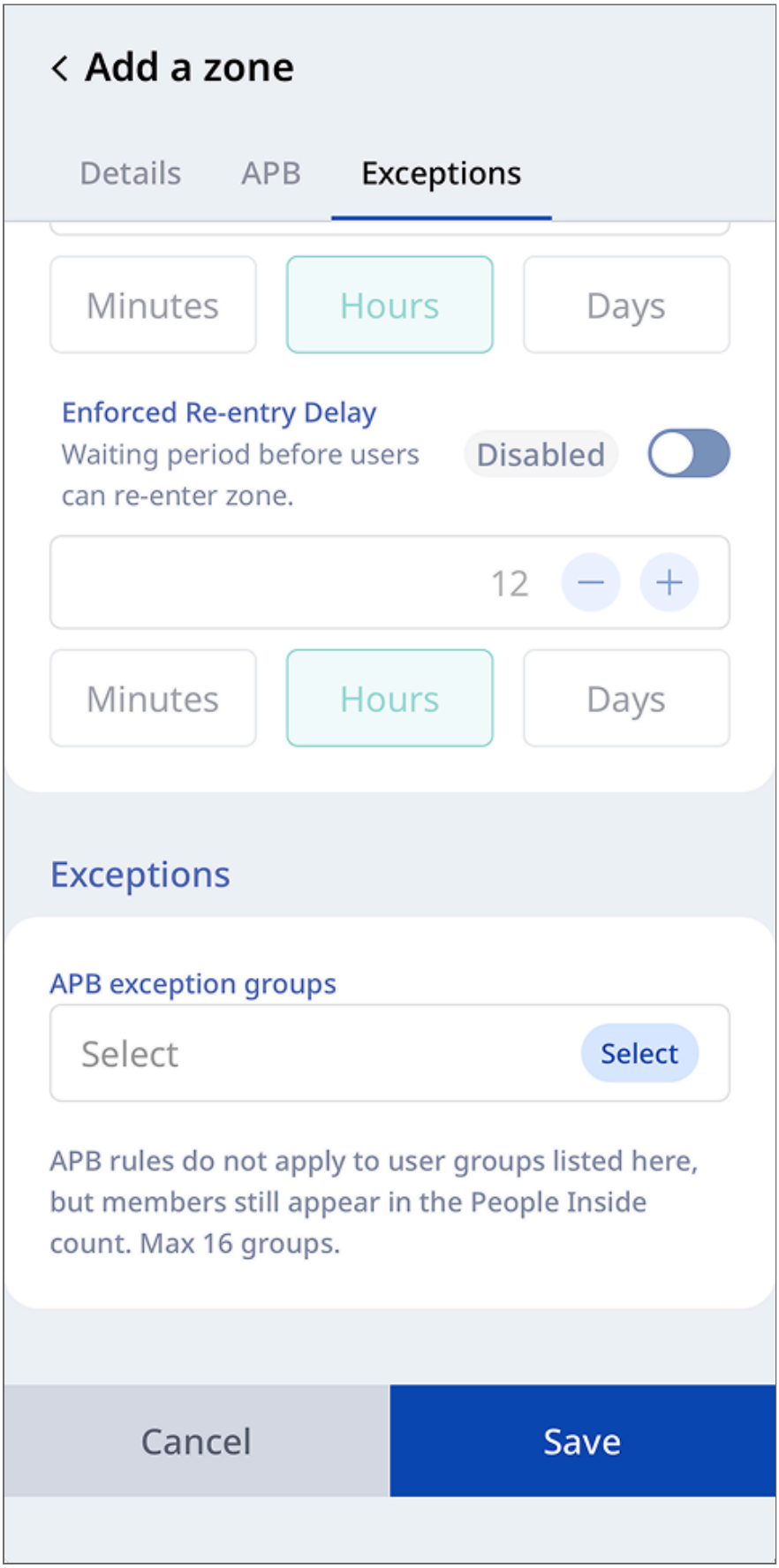
4 Establecer excepciones

En la sección **Excepciones**, seleccione grupos de usuarios exentos de las reglas de APB.

Web



Mobile



- Especifique hasta 16 grupos de usuarios como excepciones por zona.
- Los usuarios de un grupo de excepciones quedan exentos de las reglas de APB, pero permanecen en el conteo de presencia.

- Si **Modo APB** es **Ninguno**, el sistema deshabilita la sección **Excepciones**.

> **Información**
> Para obtener más información sobre la gestión de grupos de usuarios, consulta Administrar Grupos de Usuarios.

5 Guardar zona

Haga clic en **Guardar** para guardar los ajustes de la zona.

> **Notas para agregar una zona**
> - Las puertas ya asignadas a otra zona APB, las puertas sin dispositivo o las puertas dedicadas a Airfob Patch no aparecen en la lista de selección de puertas.
> - Habilite **Restablecer infracción automáticamente** (si la zona no es un perímetro) o **Temporizador de fuera del sitio** (si la zona es un perímetro) para guardar una zona sin un dispositivo de salida.
> - Las zonas deben tener nombres únicos.
> - Cambiar **Modo APB** a **Ninguno** inicializa todos los ajustes detallados guardados (**Modo APB**, **Temporizadores**, **Grupos de excepción de APB**) de la zona. Use la característica Deshabilitar zona o Pausar APB para pausar la aplicación de APB sin cambiar los ajustes.

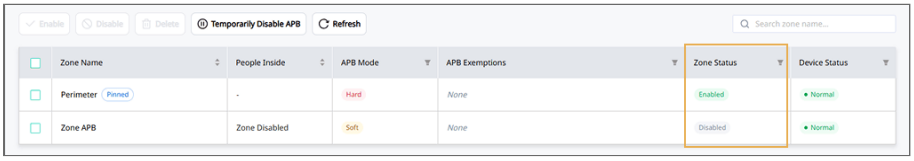
Habilitar o deshabilitar zonas

Esta característica permite a los administradores habilitar o deshabilitar zonas. Los ajustes no cambian. Deshabilitar una zona inicializa el conteo de presencia de la zona en 0. Sin embargo, las infracciones de APB existentes se mantienen. Elimínelas en el menú Revisar Infracciones De APB.

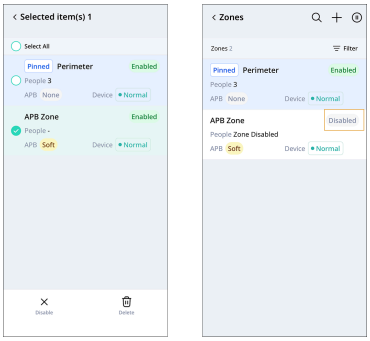
Web

1. Haga clic en la casilla de verificación de la zona para habilitarla o deshabilitarla en la lista. Seleccione una o más zonas.
2. Haga clic en **Habilitar** o **Deshabilitar** en la parte superior de la lista.
3. Cuando aparezca el mensaje de confirmación, haga clic en **Habilitar** o **Deshabilitar**.

Verifique el estado de cada zona en la columna **Estado de la zona** de la lista.



Mobile



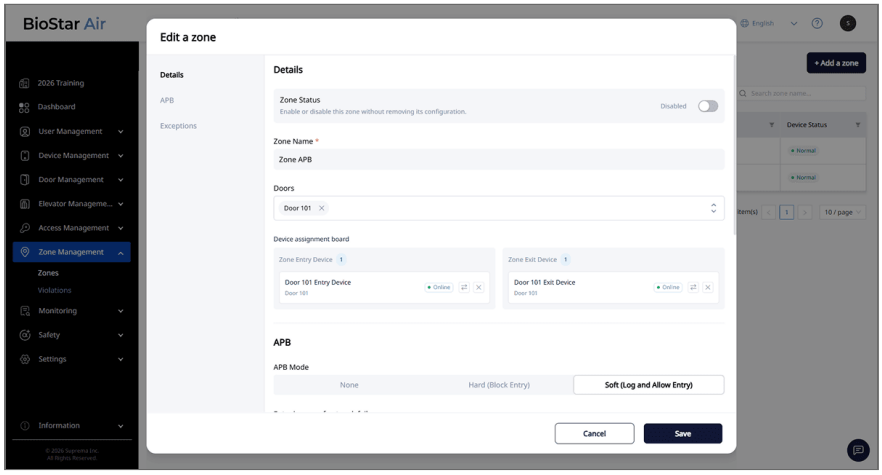
1. Mantenga presionada la zona para habilitarla o deshabilitarla en la lista.
2. Seleccione la zona para habilitarla o deshabilitarla. Seleccione una o más zonas.
3. Toque **Habilitar** o **Deshabilitar** en la parte inferior de la pantalla.
4. Cuando aparezca el mensaje de confirmación, haga clic en **Habilitar** o **Deshabilitar**.

Editar zona

Edita los detalles, los ajustes de APB y de excepciones de una zona existente.

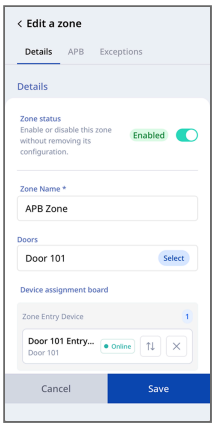
Web

1. Haga clic en la zona que desea editar en la lista.
2. Aparece la ventana **Editar una zona**.



3. Edite los campos obligatorios en la sección **Detalles**/**APB**/**Excepciones**.
4. Haga clic en **Guardar** para guardar los cambios.

Mobile



1. Toque la zona que va a editar en la lista.
2. Aparece la pantalla **Editar una zona**.
3. Edite los campos obligatorios en la sección **Detalles**/**APB**/**Excepciones**.
4. Para guardar los cambios, toque **Guardar**.

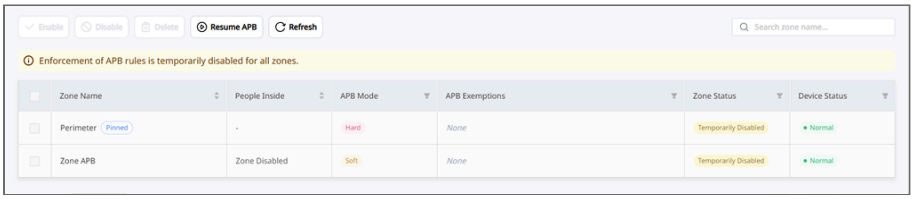
> **Información**
>
> Para obtener más información sobre los ajustes detallados en la sección **Detalles**/**APB**/**Excepciones**, consulte Agregar zonas.

Pausar APB

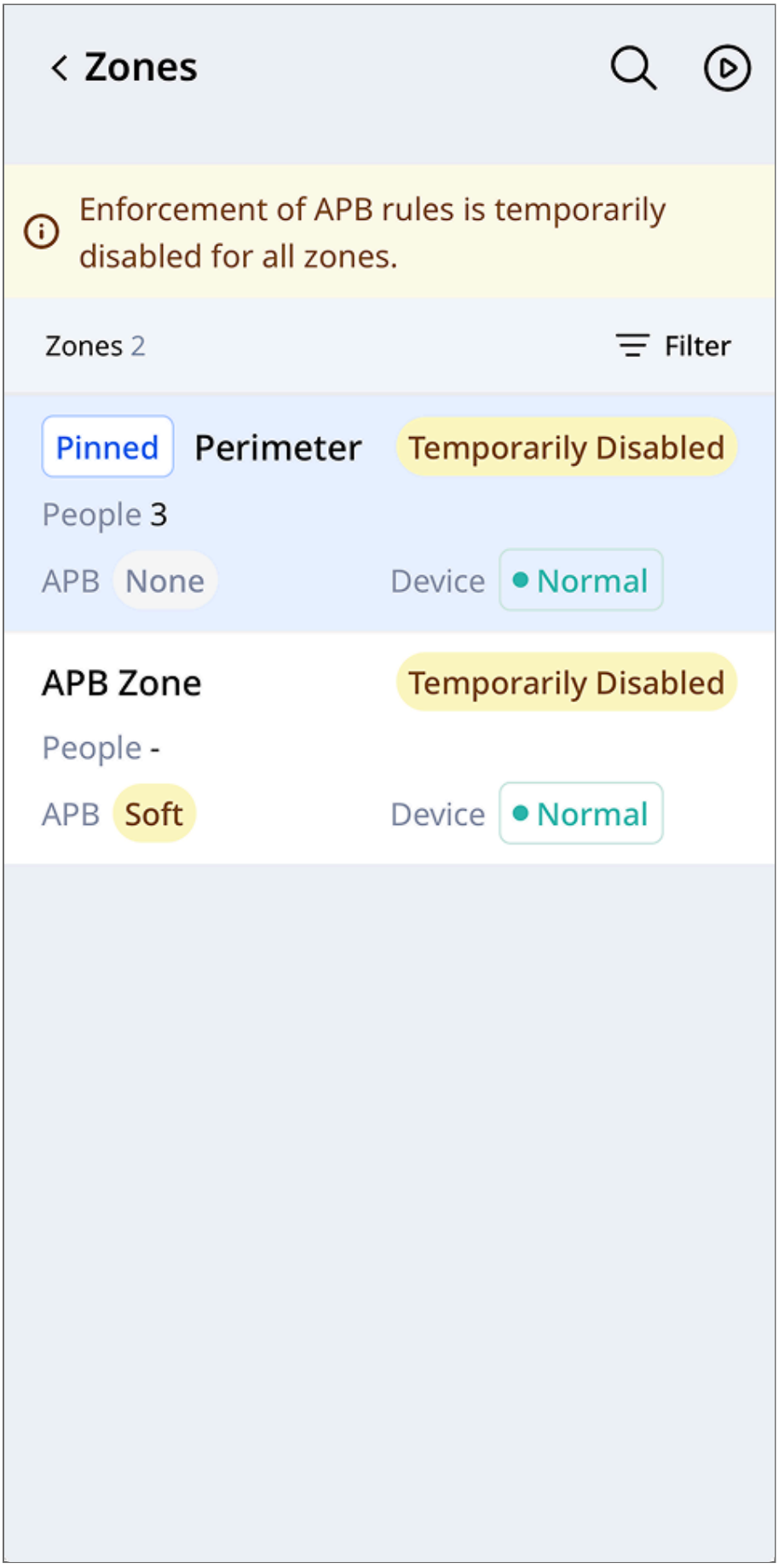
Seleccione **Pausar APB**(⏸) en la parte superior de la lista para pausar el APB en todo el sitio (para eventos especiales o tráfico pico). APB se pausa en todas las zonas, incluidas las zonas de perímetro. Después de reanudar, cada zona vuelve a su estado anterior. Durante la pausa, la lista de zonas se bloquea, así que no haga otros cambios.

Haga clic en **Reanudar**(▶) para reanudar el modo APB configurado para las zonas.

Web



Mobile

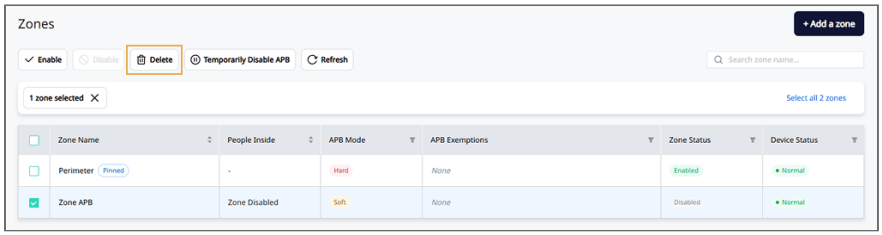

Zones
Enforcement of APB rules is temporarily disabled for all zones.
Zones 2
Filter
Pinned
Perimeter
Temporarily Disabled
People 3
APB None
Device Normal
APB Zone
Temporarily Disabled
People -
APB Soft
Device Normal

El sistema no permite habilitar una zona antipassback mientras un Roll Call está en curso. Inténtelo de nuevo cuando finalice el Roll Call. Para obtener más información sobre Roll Call, consulte Pase de lista.

Eliminar una zona

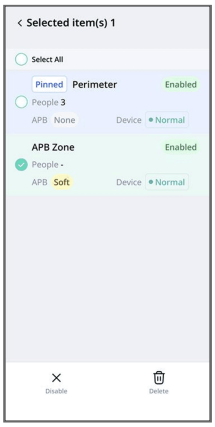
Web

1. Marque la casilla de la zona que va a eliminar en la lista. Seleccione una o más zonas.
2. Haz clic en **Eliminar** en la parte superior de la lista.



3. Haz clic en el botón **Eliminar** cuando aparezca la ventana del mensaje de confirmación.

Mobile



1. Mantenga presionada la zona que va a eliminar en la lista.
2. Seleccione la zona que va a eliminar. Seleccione una o más zonas.
3. Toque **Eliminar** en la parte inferior de la pantalla.
4. Cuando aparezca el mensaje de confirmación, haz clic en **Eliminar**.

Información

- **Perímetro** no se puede eliminar.
- El sistema elimina solo la zona seleccionada. Las puertas y los dispositivos asignados a la zona permanecen. La eliminación es irreversible.
- El sistema no puede eliminar una zona mientras los dispositivos asignados están sin conexión, sincronizando o actualizando el firmware. Espere hasta que los dispositivos se reconecten, o elimínelos de la zona y vuelva a intentarlo.

Revisar Infracciones De APB

En el menú **Gestión de zonas** → **Infracciones**, revise los usuarios que infringen las reglas de anti-passback (APB) de la zona. Borre las infracciones según sea necesario. Si aún no ha definido zonas ni el modo APB, consulte primero Administrar Zonas.

Cuando ocurren infracciones

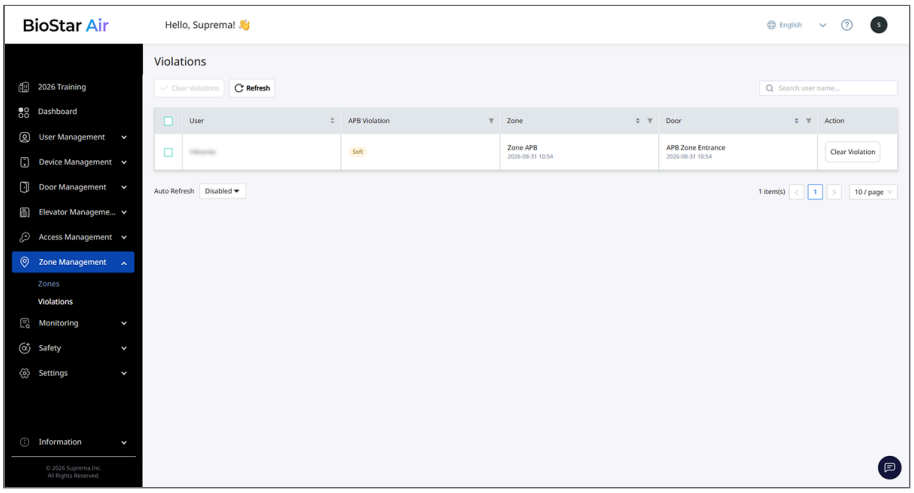
El sistema registra una infracción de APB cuando un usuario trata de entrar o salir fuera de secuencia, según el modo APB de la zona.

- En zonas con **modo estricto**, una infracción de APB bloquea el acceso y el sistema registra la infracción.
- En zonas con **modo flexible**, el sistema permite el acceso, pero registra una infracción de APB.
- Las reglas de APB no aplican a los usuarios del grupo de excepción de APB, así que no aparecen en la lista de infracciones.

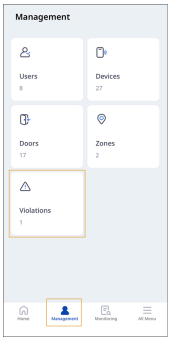
Revise la lista de infracciones

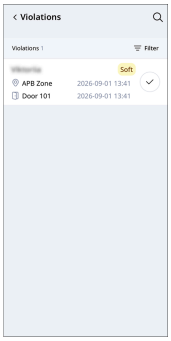
Web

En la barra lateral izquierda, haz clic en **Gestión de zonas** → **Infracciones**.



Mobile





1. Abra la aplicación BioStar Air en su dispositivo móvil e inicie sesión.
2. Toque **Administrar** en la parte inferior de la pantalla.
3. Toque la tarjeta **Infracciones**.

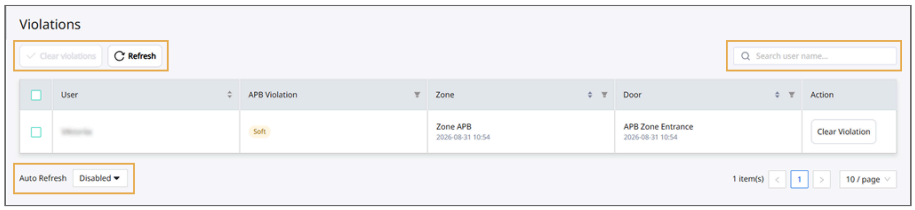
La lista muestra usuarios con infracciones de APB activas. Si no existen infracciones de APB activas, aparece una pantalla de estado vacío en lugar de la lista.

- **Usuario**: Usuario con una infracción de APB registrada.
- **Infracción de APB**: Modo (estricto/flexible) en el que ocurrió la infracción de APB.
- **Zona**: Zona donde ocurrió la infracción de APB.
- **Puerta**: Puerta donde ocurrió la infracción de APB.
- **Acción**: Borre una infracción de APB específica.

> **Información**
>
> Revise las infracciones de APB borradas y el historial de infracciones de APB anteriores en **Monitoreo** → **Registros de eventos**.

Administre la lista de infracciones

Use las características de administración de la parte superior e inferior de la lista para estas tareas.

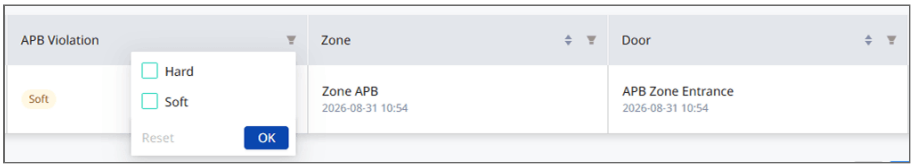


- **Borrar infracción**: Borre las infracciones de APB del usuario seleccionado en la lista. Para más información, consulte Borrar infracciones.
- **Actualizar**: Actualiza la lista de inmediato para mostrar el estado más reciente. En **Autorefrescar** en la parte inferior de la lista, seleccione un intervalo de actualización automática (**Desactivado** / **5 segundos** / **1 minuto**). El sistema actualiza la lista automáticamente según el intervalo establecido.
- **Buscar nombre de usuario...**: Buscar por nombre de usuario.

Filtrar la lista de infracciones

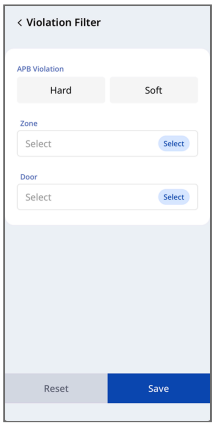
Web

En el encabezado de la lista, haga clic en el botón de la columna **Infracción de APB**, **Zona** o **Puerta** para filtrar la lista por esa condición.



> **Información**
>
> Haga clic en **Reiniciar** para borrar el filtro.

Mobile



1. Toque **Filtros** en la esquina superior derecha de la lista de infracciones.
2. Seleccione una condición de filtro en **Infracción de APB**, **Zona** o **Puerta**.
3. Toque **Guardar** para filtrar la lista según los criterios seleccionados.

> **Información**
> Toque **Reiniciar** para borrar el filtro.

Borrar infracciones

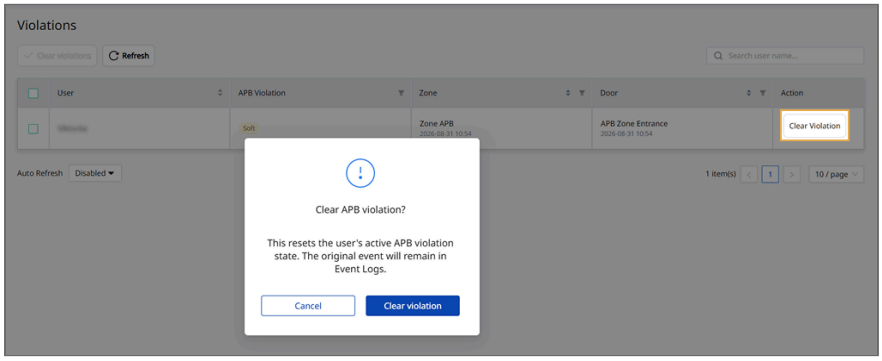
Borrar una infracción de APB inicializa el estado de infracción APB activa del usuario y restablece el acceso normal a la zona.

> **Información**
>
> - **Borrar infracción** inicializa solo el estado de infracción APB activa del usuario. El evento que activó la infracción de APB permanece en el registro de eventos.
> - Las infracciones de APB existentes permanecen después de deshabilitar la zona. Bórralas de la lista de infracciones.
> - Los usuarios en un grupo de excepciones de APB no aparecen en esta lista, pero siguen incluidos en el conteo de presencia de la zona.

Borrar una infracción de un usuario específico

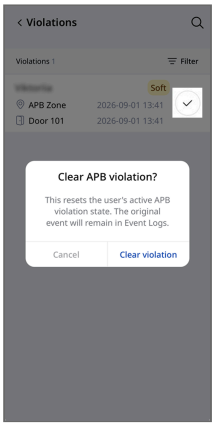
Web

1. En la lista, haga clic en **Borrar infracción** en la columna **Acción** para borrar la infracción de APB del usuario seleccionado.



2. Cuando aparezca el mensaje de confirmación, haga clic en **Borrar infracción**.

Mobile

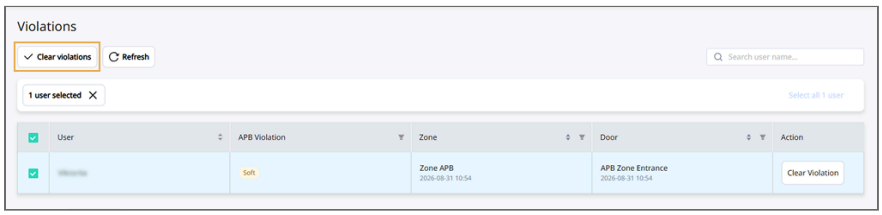


1. En la lista, toque ⌄ en la fila del usuario para borrar la infracción de APB.
2. Cuando aparezca el mensaje de confirmación, toque **Borrar infracción**.

Borrar infracciones de varios usuarios

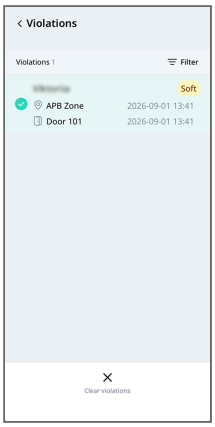
Web

1. Seleccione las casillas junto a los usuarios con infracciones de APB para borrarlas. Selecciona uno o más usuarios.
2. Haz clic en **Borrar infracciones** en la parte superior de la lista.



3. Cuando aparezca el mensaje de confirmación, haga clic en **Borrar infracciones**.

Mobile



1. Mantenga presionado un usuario en la lista.
2. Seleccione los usuarios cuyas infracciones va a borrar. Selecciona uno o más usuarios.
3. Toque **Borrar infracciones** en la parte inferior de la pantalla.
4. Cuando aparezca el mensaje de confirmación, toque **Borrar infracciones**.

Monitorizar

Usa el monitoreo de BioStar Air para rastrear y administrar en tiempo real las principales actividades del sistema: supervisar los registros de eventos y de cambios para analizar la actividad, comprobar el estado de las puertas y controlarlas de forma remota, y gestionar de manera integral la seguridad mediante las notificaciones e informes generados.

Usar registros de eventos

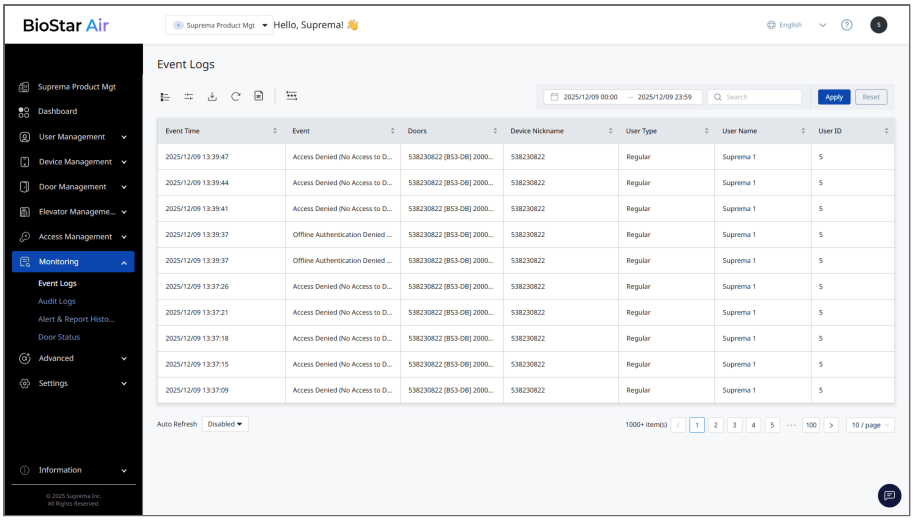
Una de las ventajas clave de una plataforma de control de acceso en la nube es la capacidad de monitorear la actividad del sitio en cualquier momento y desde cualquier lugar. Este documento explica cómo monitorear y analizar los registros de eventos en BioStar Air.

> **Consejo**
>
> Vea el siguiente video para un tutorial sobre los registros de eventos.

Ver registros de eventos

Web

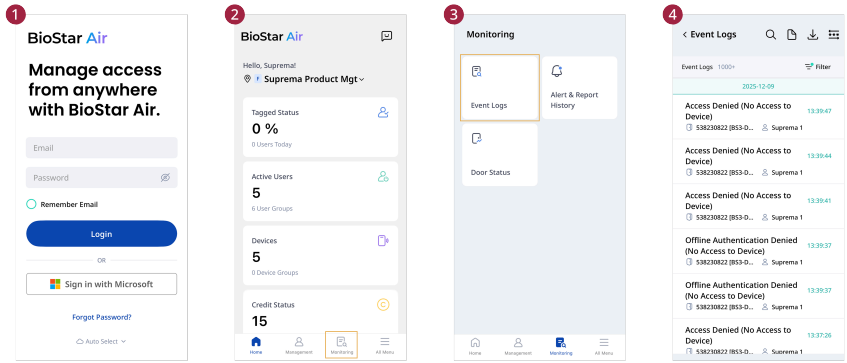
Vaya a **Registros de eventos** para ver los registros de eventos. Haga clic en **Monitoreo** → **Registros de eventos** en la barra lateral izquierda.



La pantalla **Registros de eventos** muestra una tabla con detalles que incluyen la hora del evento y su nombre, el nombre de la puerta, el alias del dispositivo, el tipo de usuario y el nombre de usuario.

Mobile

Esta guía explica cómo consultar el registro de eventos en la aplicación móvil.



1. Abra la aplicación BioStar Air en su dispositivo móvil e inicie sesión.
2. Toque **Monitoreo** en la parte inferior de la pantalla de inicio.
3. Toque la tarjeta **Registros de eventos**.

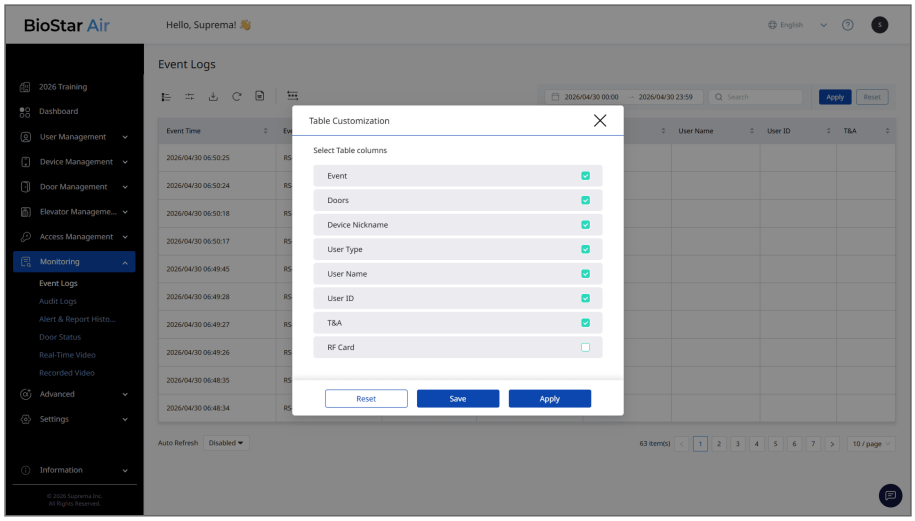
4. Desplácese por la lista de registros de eventos para ver su contenido.

Información

- **Filtros**: Filtrar registros de eventos.
- : Buscar por palabras clave específicas. Ingrese uno de los siguientes: ID de tarjeta RF, ID de usuario, correo electrónico o nombre.
- : Generar informes. Para obtener más información sobre la creación de informes, consulte Configurar informes.
- : Descargar informes en formato CSV o PDF.
- : Aplicar el enmascaramiento de datos personales.

Personalización de gráficos

Personalice las columnas de la tabla para mostrar u ocultar información. Reordene las columnas para colocar las que usa con frecuencia al principio. Haga clic en el botón en la parte superior de la lista de registros de eventos. Aparecerá la ventana **Personalización de gráficos**.



- Seleccione o deseleccione las casillas de las columnas para mostrarlas u ocultarlas.
- Para reordenar las columnas, haga clic y arrastre una columna a la posición deseada.
- Haga clic en **Guardar** para guardar la configuración de **Personalización de gráficos**.
- Haga clic en **Aplicar** para aplicar **Personalización de gráficos** a la lista de registros de eventos sin guardar.
- Haga clic en **Restablecer** para cancelar los cambios en **Personalización de gráficos** y restaurar el estado inicial.

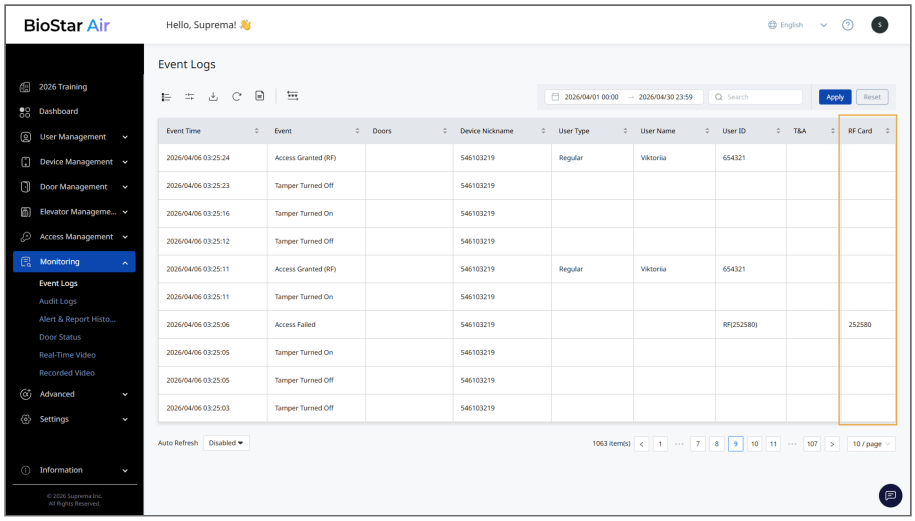
Información

- Al hacer clic en **Guardar**, la configuración se mantiene incluso después de navegar a otro menú. Al hacer clic en **Aplicar**, los cambios se aplican solo a la lista actual y se revierten al abandonar la página.
- **Registros de auditoría** no admite la **Personalización de gráficos**.

Mostrar columna de número de tarjeta RF.

Agregue la columna **Tarjeta RF** al registro de eventos para ver el número de la tarjeta RF cuando un usuario se autentica con una tarjeta RF.

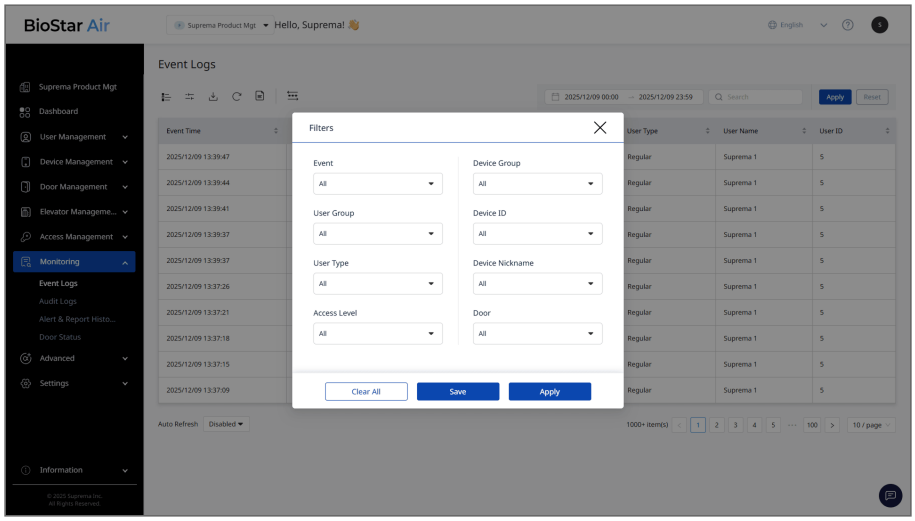
1. Haga clic en el botón en la parte superior de la lista de registros de eventos.
2. Cuando aparezca la ventana **Personalización de gráficos**, marque la casilla **Tarjeta RF** y arrástrela a la posición deseada.
3. Haga clic en el botón **Guardar** o en el botón **Aplicar**.
4. La columna **Tarjeta RF** aparece en la lista de registros de eventos.



> **Información**
>
> El número de tarjeta RF se muestra en el registro de eventos solo cuando el usuario tiene una sola tarjeta asignada. Si el usuario tiene varias tarjetas RF asignadas, el número no se mostrará.

Filtrar registros

Filtre los registros para encontrar rápidamente la información que necesita. Haga clic en en la parte superior de la lista de registros. Cuando aparezca la ventana **Filtros**, seleccione el valor deseado para cada elemento.



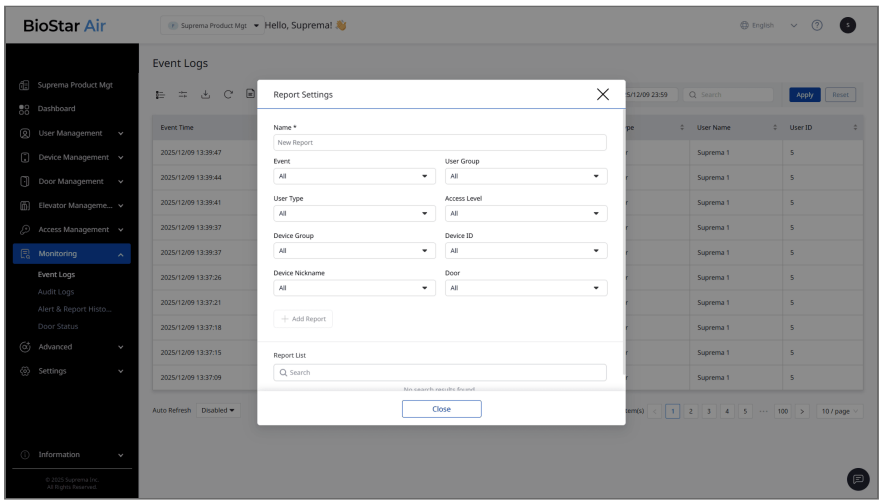
Información

- Haga clic en **Guardar** o **Guardar filtro** para guardar la configuración y que se mantenga al navegar a otro menú. Haga clic en **Aplicar** o **Aplicar filtro** para aplicar los cambios solo a la lista actual; se revertirán al salir.
- Haga clic en **Restablecer** o **Borrar filtros** para cancelar los cambios y volver al estado inicial.

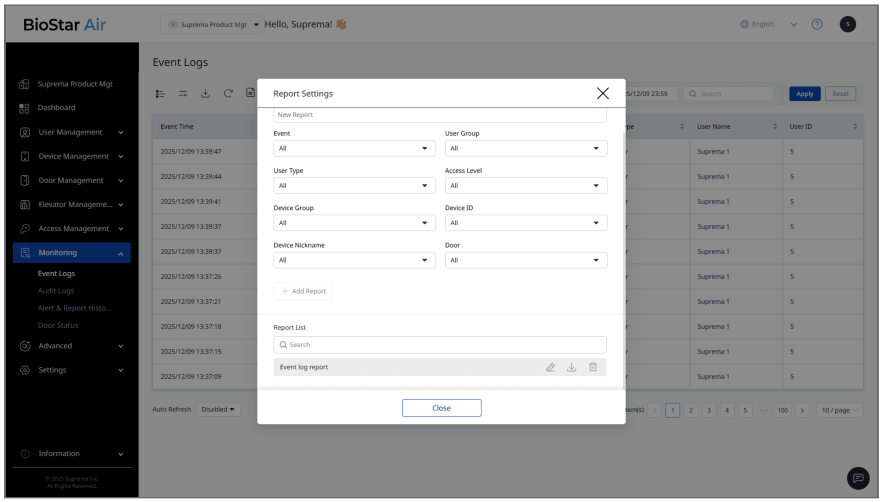
Configurar informes

Genere informes de los eventos ocurridos durante un período determinado, filtrando los datos de los registros.

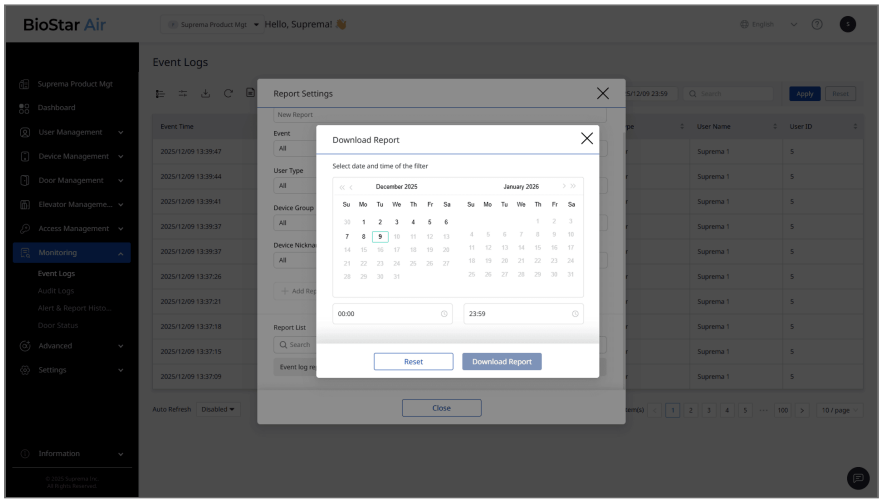
1. Haga clic en el botón en la parte superior de la lista de registros.
2. Cuando aparezca la ventana **Configuración de informes**, ingrese un nombre para el informe.



3. Seleccione los elementos que desea incluir en el informe.
4. Haga clic en **Agregar informe** para guardar el informe configurado.
5. Se crea un informe con el nombre establecido en **Lista de informes**.



6. Para descargar el informe generado, haga clic en el botón junto al nombre del informe.
7. Cuando aparezca la ventana **Descargar informe**, seleccione el período para consultar los eventos y haga clic en **Descargar informe**.



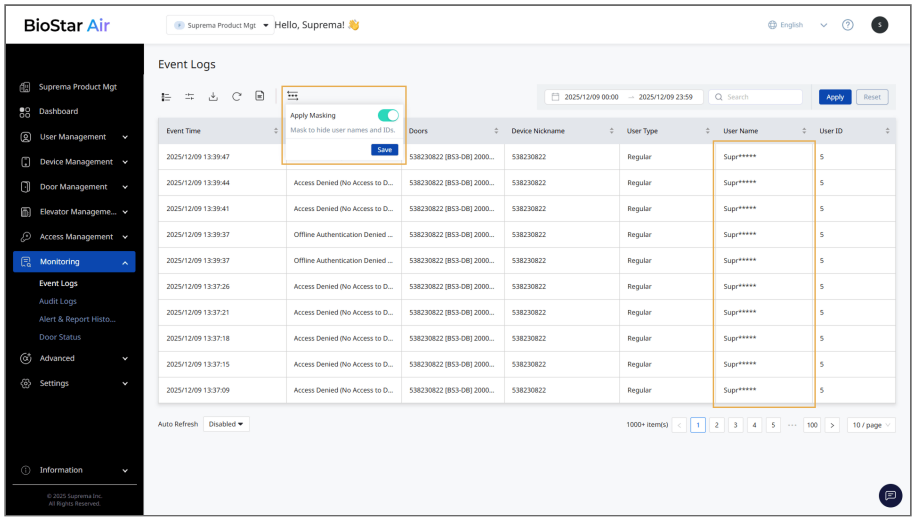
Se envía un enlace de descarga al correo electrónico del administrador.

> **Información**
>
> **Lista de informes** le permite buscar, editar, descargar o eliminar los informes creados.

Enmascarar datos personales

Enmascare los datos personales en los registros para proteger la información sensible. Cuando el enmascaramiento de datos personales está habilitado, información como los nombres de usuario, las direcciones de correo electrónico y los números de teléfono se oculta parcialmente.

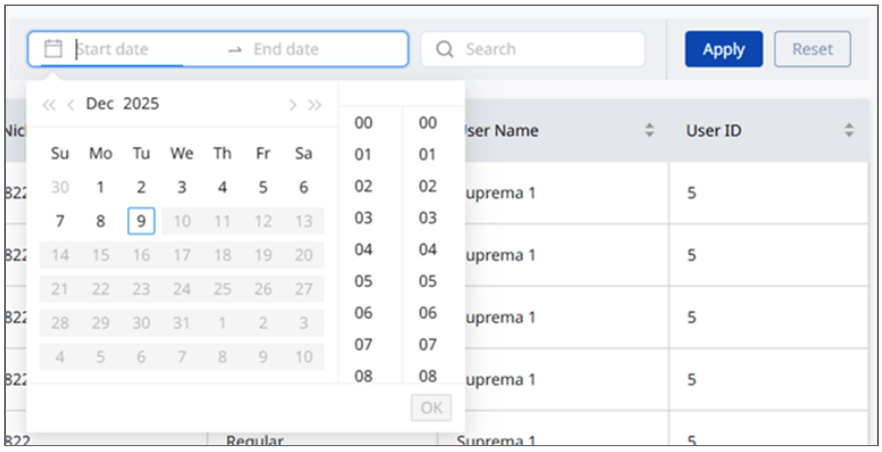
Para habilitar el enmascaramiento de datos personales, haga clic en el botón en la parte superior de la lista de registros. En el menú emergente, active **Aplicar enmascaramiento** y haga clic en **Guardar**.



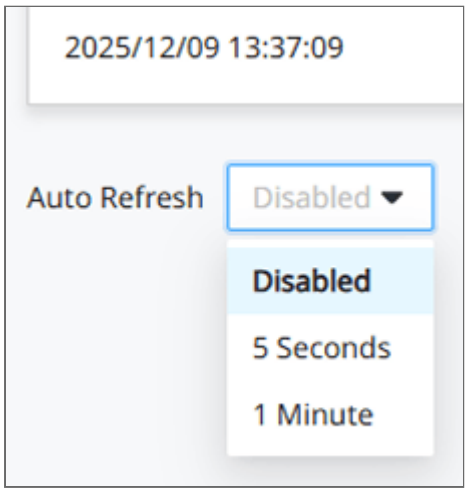
Otras funciones

Utilice la barra de herramientas en la parte superior de la lista para gestionar los registros de forma más eficiente.

- Para ordenar los registros por fecha, seleccione un rango de fecha y hora y, a continuación, haga clic en **Aplicar**. Haga clic en **Restablecer** para restablecer la fecha.



- En el campo de entrada **Búsqueda**, ingrese palabras clave específicas para buscar en los registros. Ingrese uno de los siguientes: ID de tarjeta RF, ID de usuario, correo electrónico o nombre.
- Haga clic en para guardar los registros como un archivo CSV o PDF.
- Haga clic en en la parte superior de la lista para actualizar los registros.
- Para actualizar a intervalos específicos, seleccione 5 segundos o 1 minuto en **Autorefrescar** en la parte inferior izquierda de la lista.



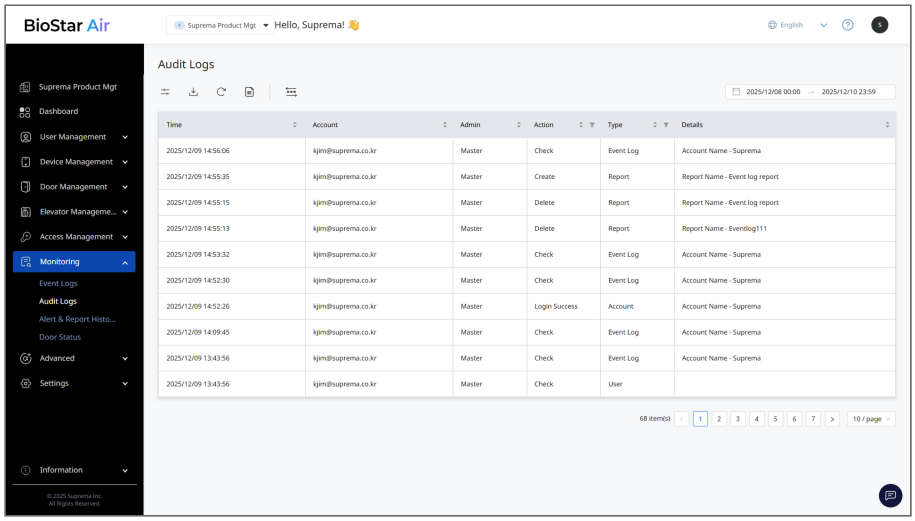
Usar registros de auditoría

Una de las principales ventajas de una plataforma de control de acceso en la nube es la capacidad de supervisar la actividad del sitio en todo momento y desde cualquier lugar. Este documento explica cómo supervisar y analizar los registros de auditoría en BioStar Air.

> **Consejo**
> Vea el siguiente video para un tutorial sobre los registros de auditoría.

Ver registros de auditoría

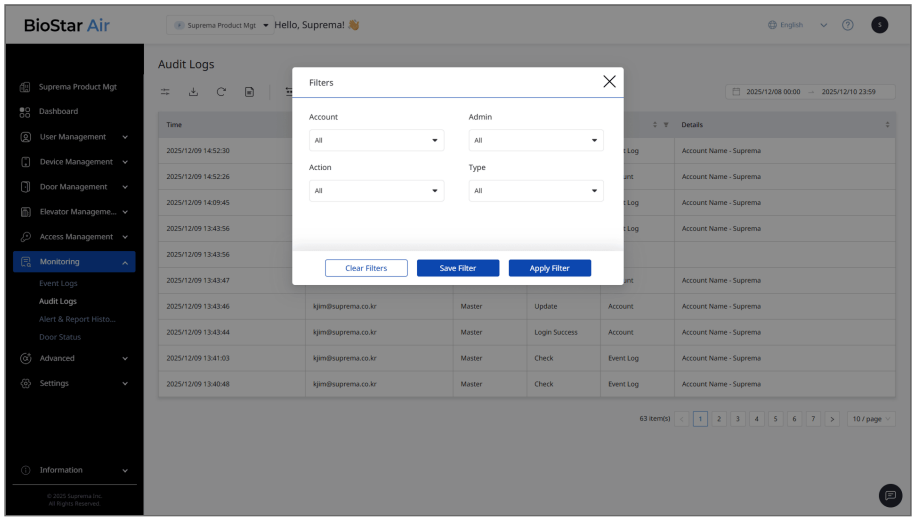
Vaya a **Registros de auditoría** para ver los registros de auditoría. Haga clic en **Monitoreo** → **Registros de auditoría** en la barra lateral izquierda.



Utilice **Registros de auditoría** para rastrear las acciones de los administradores. Cada registro en la lista muestra una tabla con información como la hora de la operación, la dirección de correo electrónico, los privilegios de administrador, el tipo de operación, la ruta del menú y los detalles de la operación.

Filtrar registros

Filtre los registros para encontrar rápidamente la información que necesita. Haga clic en en la parte superior de la lista de registros. Cuando aparezca la ventana **Filtros**, seleccione el valor deseado para cada elemento.



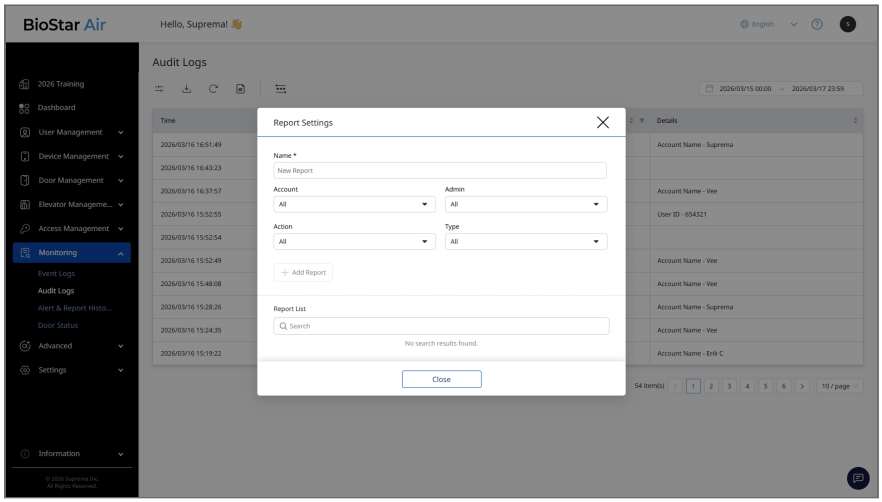
Información

- Haga clic en **Guardar** o **Guardar filtro** para guardar la configuración y que se mantenga al navegar a otro menú. Haga clic en **Aplicar** o **Aplicar filtro** para aplicar los cambios solo a la lista actual; se revertirán al salir.
- Haga clic en **Restablecer** o **Borrar filtros** para cancelar los cambios y volver al estado inicial.

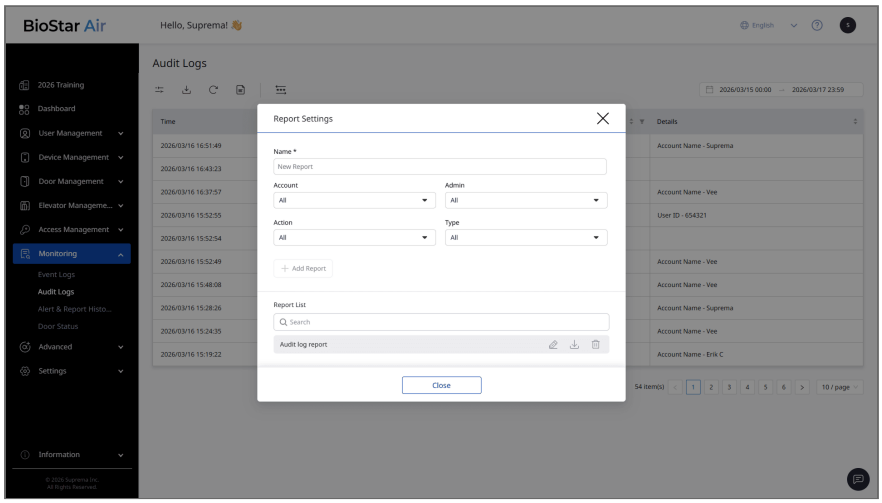
Configurar informes

Genere informes de los eventos ocurridos durante un período determinado, filtrando los datos de los registros.

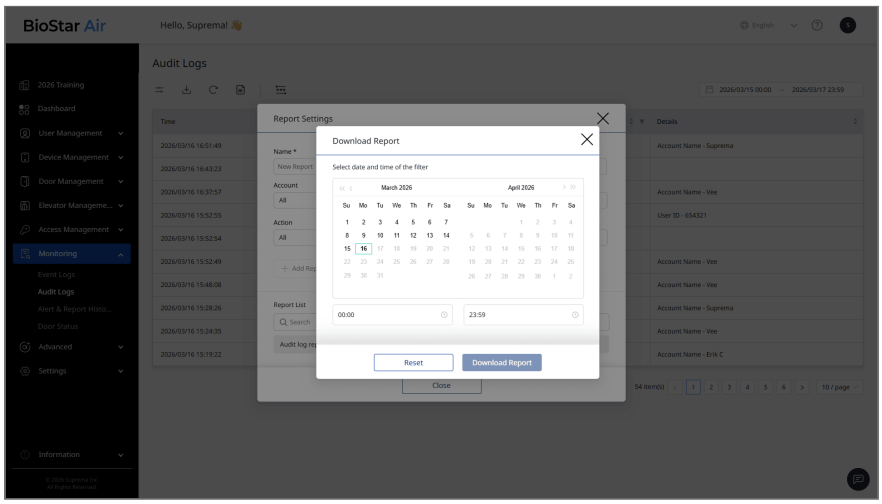
1. Haga clic en el botón en la parte superior de la lista de registros.
2. Cuando aparezca la ventana **Configuración de informes**, ingrese un nombre para el informe.



3. Seleccione los elementos que desea incluir en el informe.
4. Haga clic en **Agregar informe** para guardar el informe configurado.
5. Se crea un informe con el nombre establecido en **Lista de informes**.



6. Para descargar el informe generado, haga clic en el botón junto al nombre del informe.
7. Cuando aparezca la ventana **Descargar informe**, seleccione el período para consultar los eventos y haga clic en **Descargar informe**.



Se envía un enlace de descarga al correo electrónico del administrador.

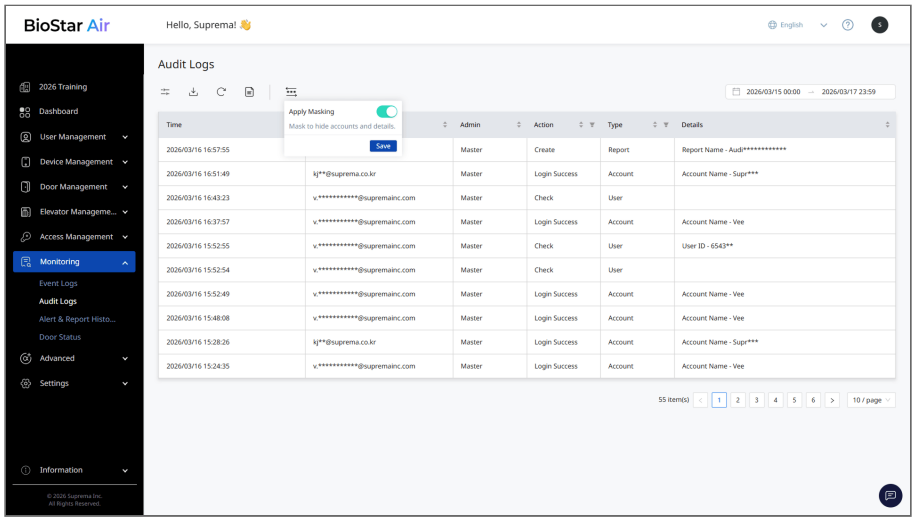
Información

Lista de informes le permite buscar, editar, descargar o eliminar los informes creados.

Enmascarar datos personales

Enmascare los datos personales en los registros para proteger la información sensible. Cuando el enmascaramiento de datos personales está habilitado, información como los nombres de usuario, las direcciones de correo electrónico y los números de teléfono se oculta parcialmente.

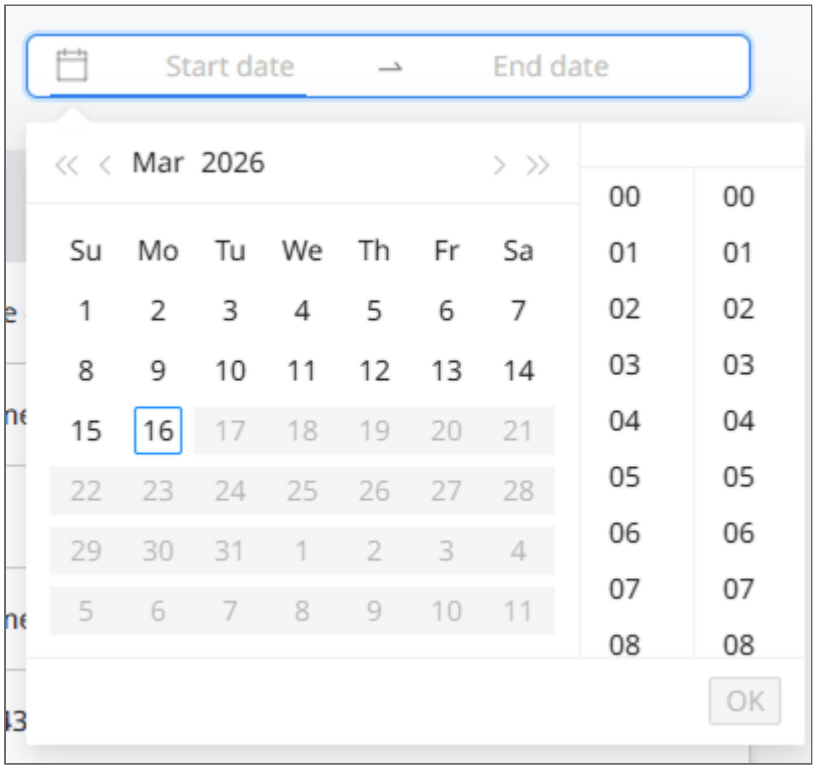
Para habilitar el enmascaramiento de datos personales, haga clic en el botón en la parte superior de la lista de registros. En el menú emergente, active **Aplicar enmascaramiento** y haga clic en **Guardar**.



Otras funciones

Utilice la barra de herramientas en la parte superior de la lista para gestionar los registros de forma más eficiente.

- Para ordenar los registros por fecha, seleccione un rango de fecha y hora, luego haga clic en **OK**.



- Haga clic en para guardar los registros como un archivo CSV o PDF.
- Haga clic en en la parte superior de la lista de registros para actualizarla.

Consultar historial de alertas e informes

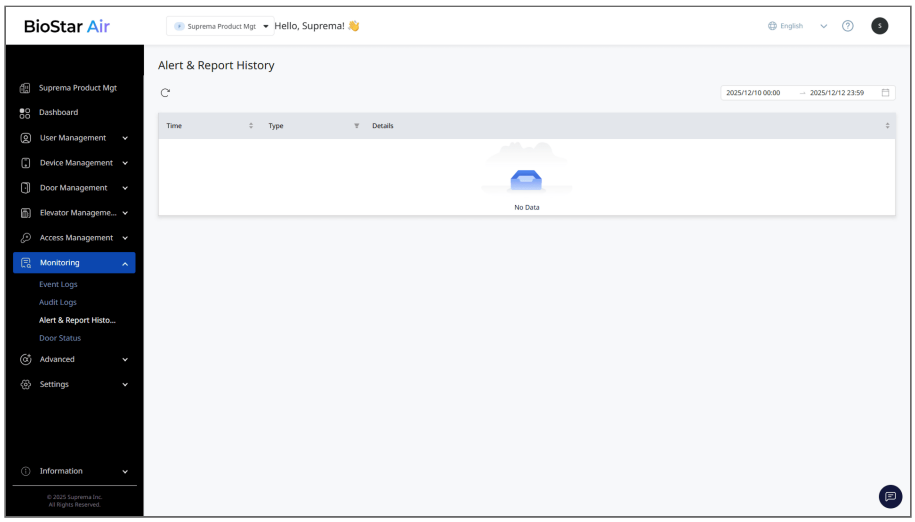
Aprende a consultar el historial de alertas e informes generados en BioStar Air. Los administradores pueden ver las alertas y los informes generados anteriormente a través del portal web y la aplicación móvil.

Antes de comenzar

El historial de alertas e informes muestra únicamente los elementos generados por las reglas de alertas e informes configuradas en **Ajustes** → **Historial de Alertas e Informes**. Para obtener más información sobre cómo establecer reglas para crear alertas e informes, consulta Configurar alertas y informes.

Consultar historial de alertas e informes

En la barra lateral izquierda, haz clic en **Monitoreo** → **Historial de Alertas e Informes**. Aparecerá el historial de alertas e informes.



- Consulta la hora, el tipo y los detalles de cada alerta o informe generado en la lista.
- Haz clic en el selector de rango de fechas en la esquina superior derecha de la pantalla, establece el período deseado y filtra el historial de alertas e informes para ese intervalo.
- Haz clic en ↻ en la parte superior de la lista para actualizarla.

Supervisar el estado de la puerta

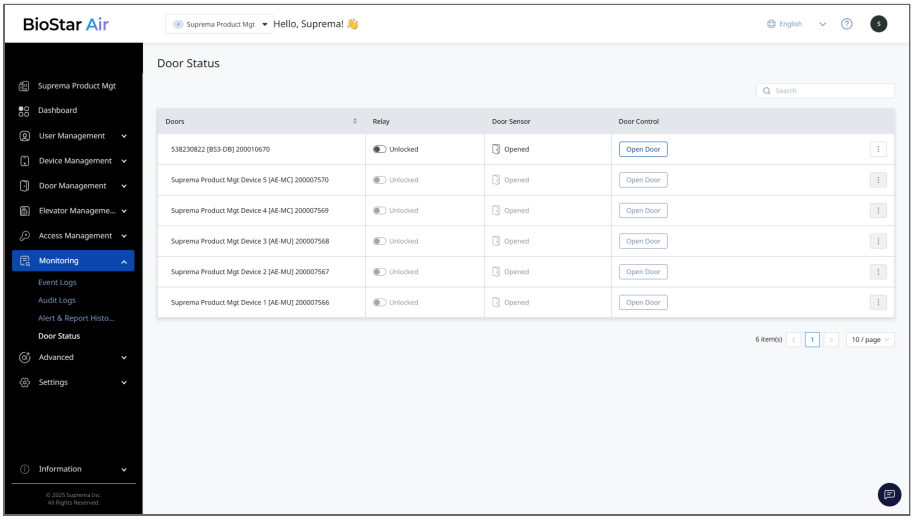
Supervise en tiempo real el estado de las puertas conectadas a BioStar Air. Compruebe si una puerta está bloqueada o desbloqueada y el estado de su sensor de relé, y bloquéela o desbloquéela de forma remota para controlar el acceso.

> **Consejo**
>
> Consulte el siguiente video para ver el tutorial sobre cómo supervisar el estado de las puertas.

Supervisión del estado de las puertas

Web

Supervise el estado de las puertas en el portal web de BioStar Air. Haga clic en **Monitoreo** → **Estado de puerta** en la barra lateral izquierda. Vea la lista de puertas registradas en BioStar Air.

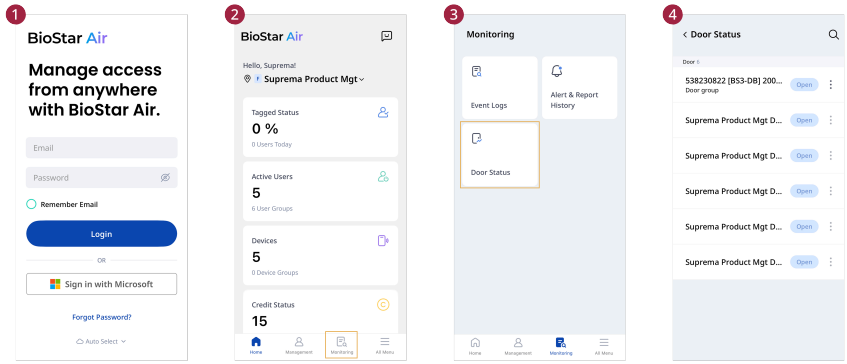


Revise los siguientes elementos para cada puerta.

- **Relé**: Indica si la puerta está bloqueada o desbloqueada.
- **Sensor de puerta**: Indica si la puerta está físicamente abierta o cerrada.

Mobile

Supervise el estado de las puertas desde la aplicación BioStar Air en un dispositivo móvil.



1. Abra la aplicación BioStar Air en su dispositivo móvil e inicie sesión.
2. Toque **Monitoreo** en la parte inferior de la pantalla de inicio.
3. Toque la tarjeta **Estado de puerta**.
4. Vea la lista de puertas registradas en BioStar Air.

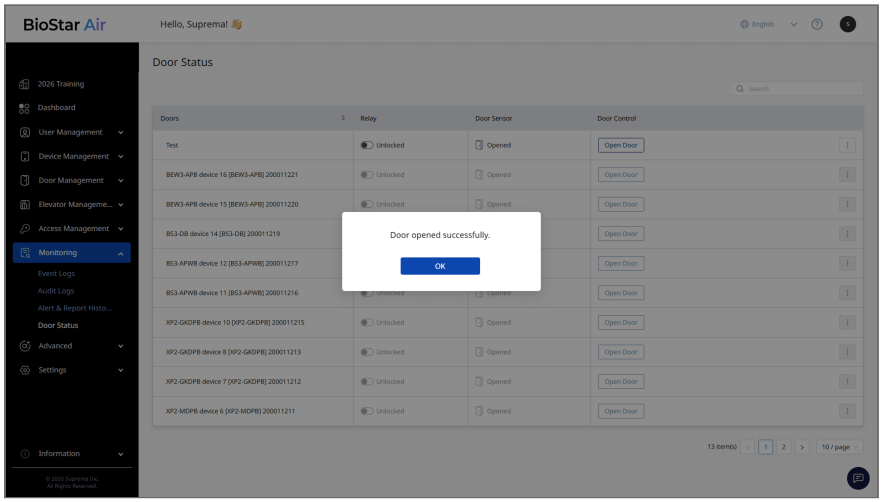
> **Información**
>
> Para obtener más información sobre el registro y la gestión de puertas, consulte Administrar puertas registradas.

Desbloquear una puerta

Desbloquee la puerta de forma remota cuando esté en línea y conectada a BioStar Air.

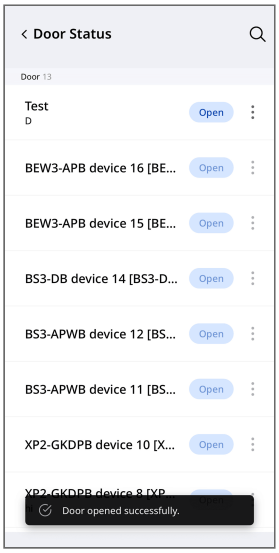
Web

1. En la columna **Control de puertas**, haga clic en **Puerta Abierta**.
2. El estado en la columna **Relé** cambia a desbloqueado y aparece un mensaje de éxito.



3. Después de que transcurra el tiempo configurado, la puerta vuelve a estar bloqueada.

Mobile



1. Toque **Puerta Abierta** para desbloquear la puerta de forma remota.
2. Aparecerá un mensaje de éxito en la parte inferior de la pantalla.
3. Después de que transcurra el tiempo configurado, la puerta vuelve a estar bloqueada.

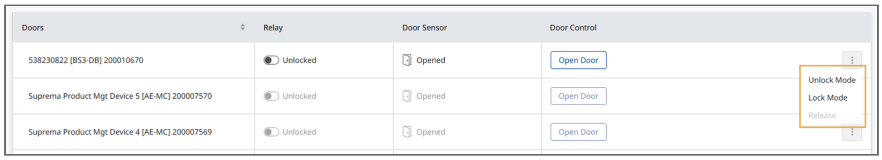
> **Información**
>
> Para obtener información sobre cómo configurar la duración durante la cual la puerta permanece abierta, consulte Administrar puertas registradas.

Activar modo siempre abierto

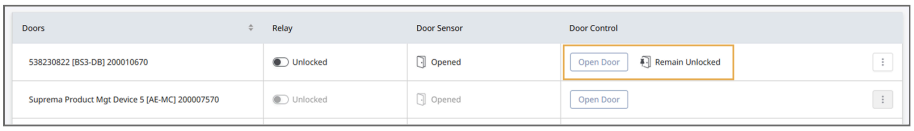
Mantenga una puerta desbloqueada indefinidamente. Úselo cuando se necesite acceso temporal o para visitantes.

Web

1. En la lista de puertas, haga clic en ⋮ en el extremo derecho de la puerta para mantenerla abierta.

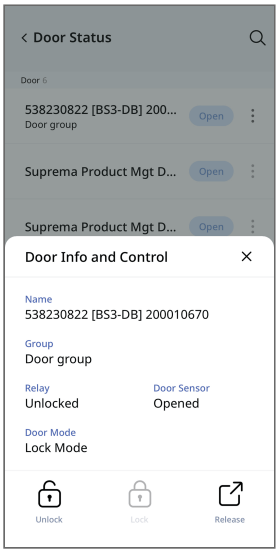


2. Haga clic en **Modo de desbloqueo** en el menú emergente.
3. El estado en la columna **Control de puertas** cambia a **Permanecer desbloqueada**.



Haga clic en ⋮ → **Liberación** para volver al funcionamiento normal.

Mobile



1. Toque ⋮ en el extremo derecho de la puerta.
2. Cuando aparezca la opción **Door Info and Control**, toque **Unlock**.
3. Aparecerá un mensaje de éxito en la parte inferior de la pantalla.

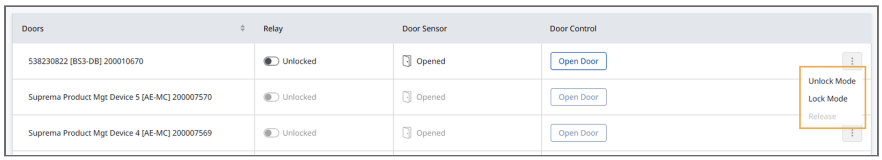
Toque ⋮ → **Liberación** para volver al funcionamiento normal.

Establecer el modo de bloqueo

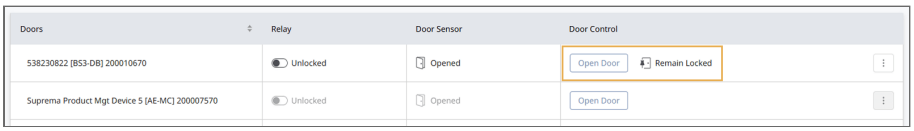
Mantenga la puerta bloqueada independientemente del horario actual. Úselo cuando se requiera mayor seguridad.

Web

1. En la lista de puertas, haga clic en ⋮ en el extremo derecho de la puerta para mantenerla bloqueada.

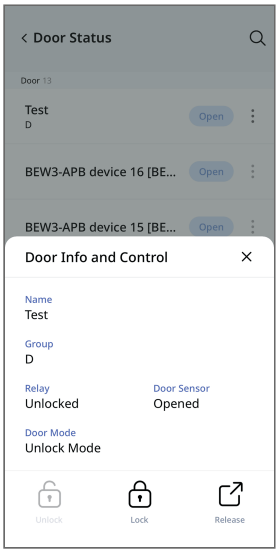


2. Haga clic en **Modo de bloqueo** en el menú emergente.
3. El estado en la columna **Control de puertas** cambia a **Permanecer bloqueada**.



Haga clic en ⋮ → **Liberación** para volver al funcionamiento normal.

Mobile



1. Toque ⋮ en el extremo derecho de la puerta.
2. Cuando aparezca la opción **Door Info and Control**, toque **Modo de bloqueo**.
3. Aparecerá un mensaje de éxito en la parte inferior de la pantalla.

Toque ⋮ → **Liberación** para volver al funcionamiento normal.

Seguridad

Las funcionalidades de administración de seguridad de BioStar Air ayudan a rastrear a las personas en el sitio durante las operaciones normales y a gestionar evacuaciones durante emergencias. Presencia, que incluye **En el sitio ahora** y **Zonas**, ofrece a los administradores una vista en tiempo real de los titulares de credenciales que están en el sitio y dónde se encuentran dentro del sitio. Los administradores también pueden actualizar manualmente el estado de presencia de una persona.

El pase de lista respalda evacuaciones ordenadas. Permite a los administradores designados hacerse responsables de ciertos puntos de reunión y supervisar la seguridad de las personas asignadas. Usa el mismo motor de presencia en el sitio que **En el sitio ahora**.

Consulte los siguientes documentos para saber cómo administrar Presencia y Roll Call en el portal de BioStar Air.

Comprobar Presencia

El menú **Seguridad** → **Presencia** muestra en tiempo real a los usuarios en el sitio. El sistema calcula el estado de presencia según los registros de autenticación de los dispositivos de entrada y salida definidos en **Perímetro**. Si Perímetro aún no está definido, consulte primero Administrar Zonas.

Cómo se determina el estado de presencia

Cuando los usuarios se autentican en un dispositivo de entrada en la zona de perímetro, su estado cambia a **En el sitio**. Cuando se autentican en un dispositivo de salida, su estado cambia a **Fuera del sitio**.

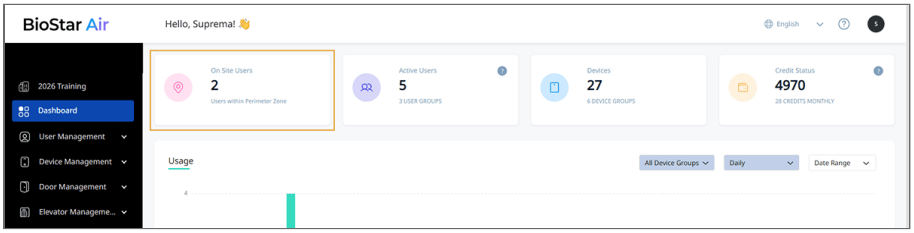
- Para sitios sin un dispositivo de salida en la zona de perímetro, establece siempre **Temporizador de fuera del sitio**. Si los usuarios permanecen inactivos durante el tiempo establecido, su estado cambia automáticamente a **Fuera del sitio**.
- Para saber cómo establecer los dispositivos de entrada y salida para la zona de perímetro y el ajuste **Temporizador de fuera del sitio**, consulte Administrar Zonas.
- Los administradores pueden ver la lista y la cantidad de personas en el sitio desde varios menús:
  - **Panel de Control** widget
  - **Seguridad** → **Presencia**

– **Gestión de zonas** → **Zonas** → **Personas dentro** (Perímetro)

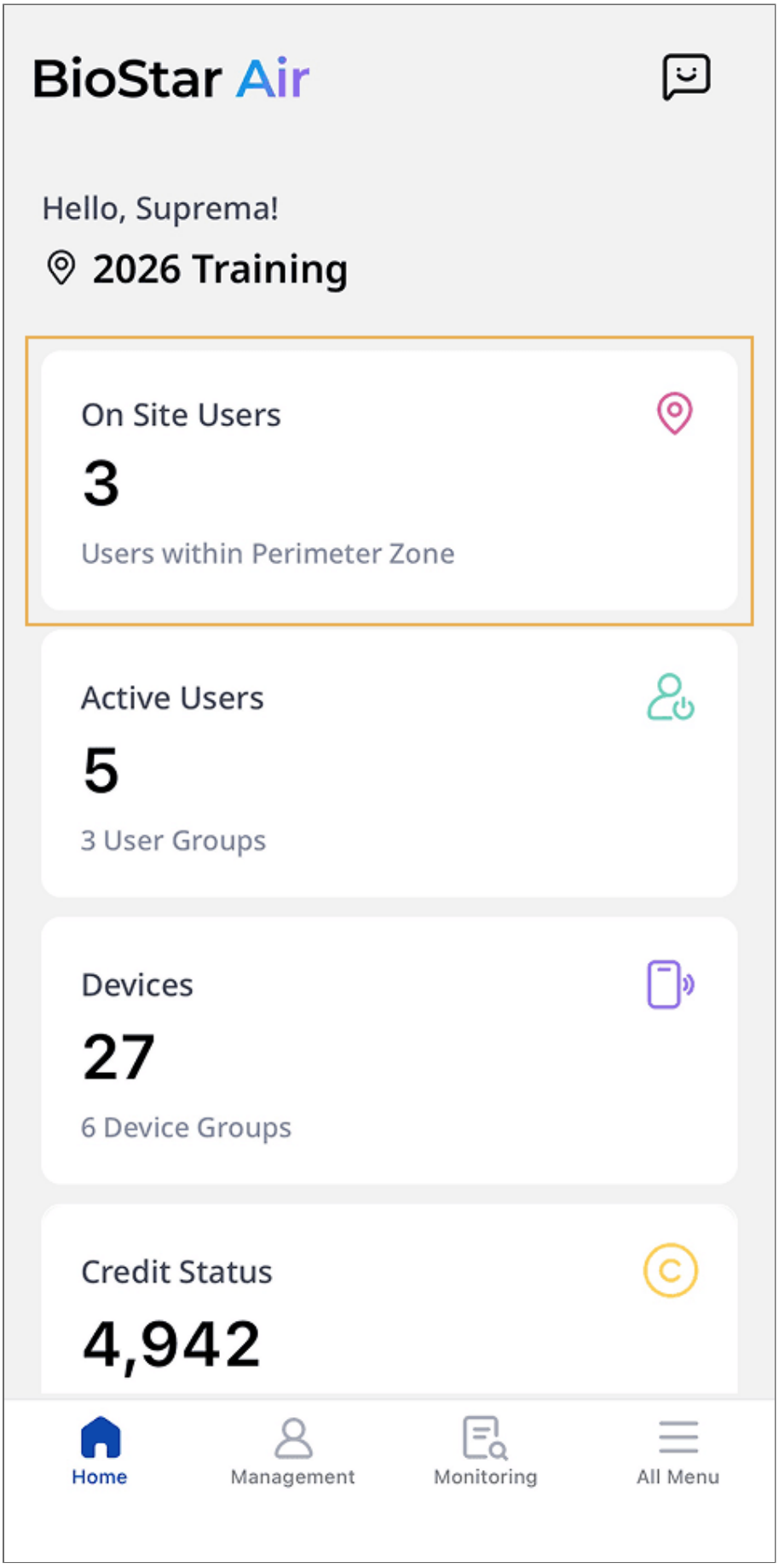
Comprobar en el panel

El menú **Panel de Control** también muestra el número de usuarios actualmente en el sitio en la tarjeta **Usuarios en el sitio**.

Web



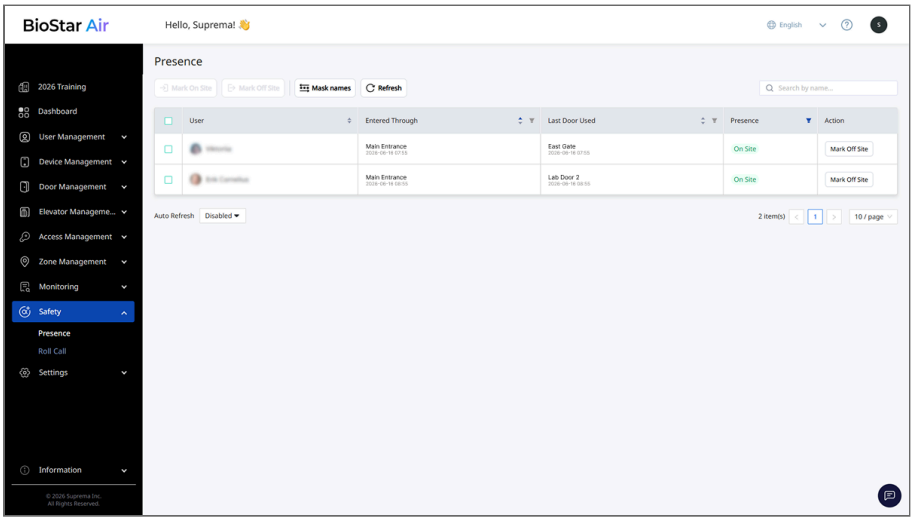
Mobile


BioStar Air
Hello, Suprema!
2026 Training
On Site Users
3
Users within Perimeter Zone
Active Users
5
3 User Groups
Devices
27
6 Device Groups
Credit Status
4,942
Home
Management
Monitoring
All Menu

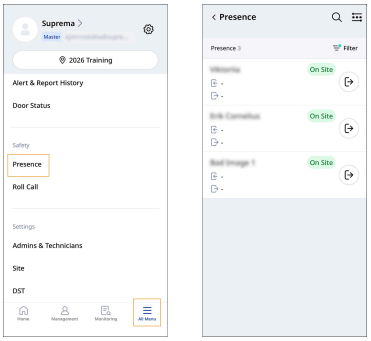
Explorar la lista de presencia

Web

En la barra lateral izquierda, haz clic en **Seguridad** → **Presencia**.



Mobile



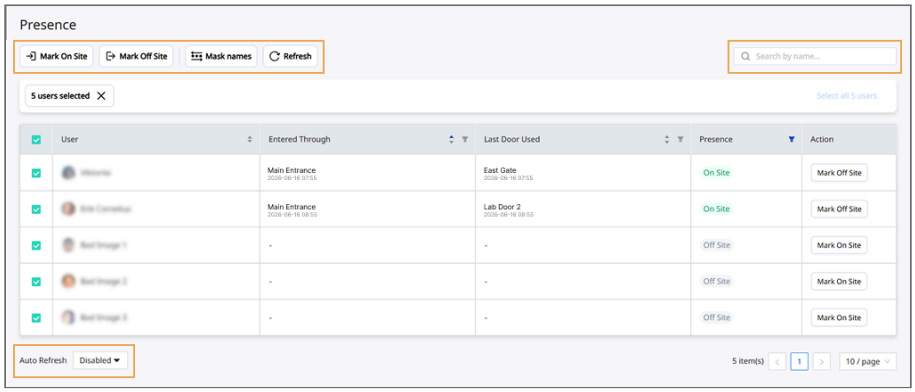
1. Abra la aplicación BioStar Air en su dispositivo móvil e inicie sesión.
2. Toque **All Menu** → **Presencia** en la parte inferior de la pantalla.

De forma predeterminada, la lista de presencia muestra solo a los usuarios con el estado **En el sitio**.

- **Usuario**: La foto de perfil y el nombre del usuario.
- **Entrada por**: El dispositivo de entrada y la hora en que el usuario se autenticó para entrar al sitio.
- **Ultima puerta usada**: La puerta más reciente y la hora.
- **Presencia**: El estado de presencia actual del usuario (**En el sitio** / **Fuera del sitio**).
- **Accion**: Cambia el estado de presencia del usuario.

Gestión de la lista de presencia

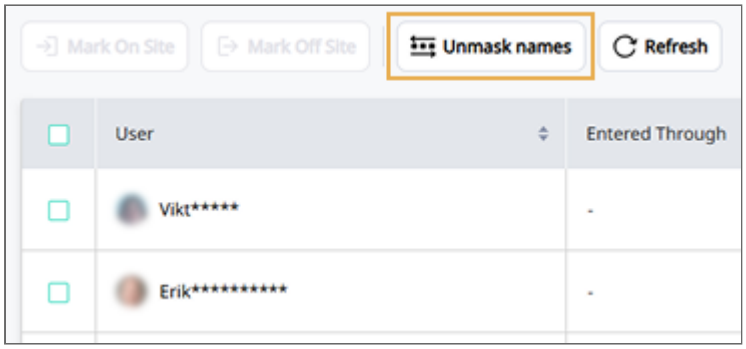
Use las características de administración de la parte superior e inferior de la lista para estas tareas.



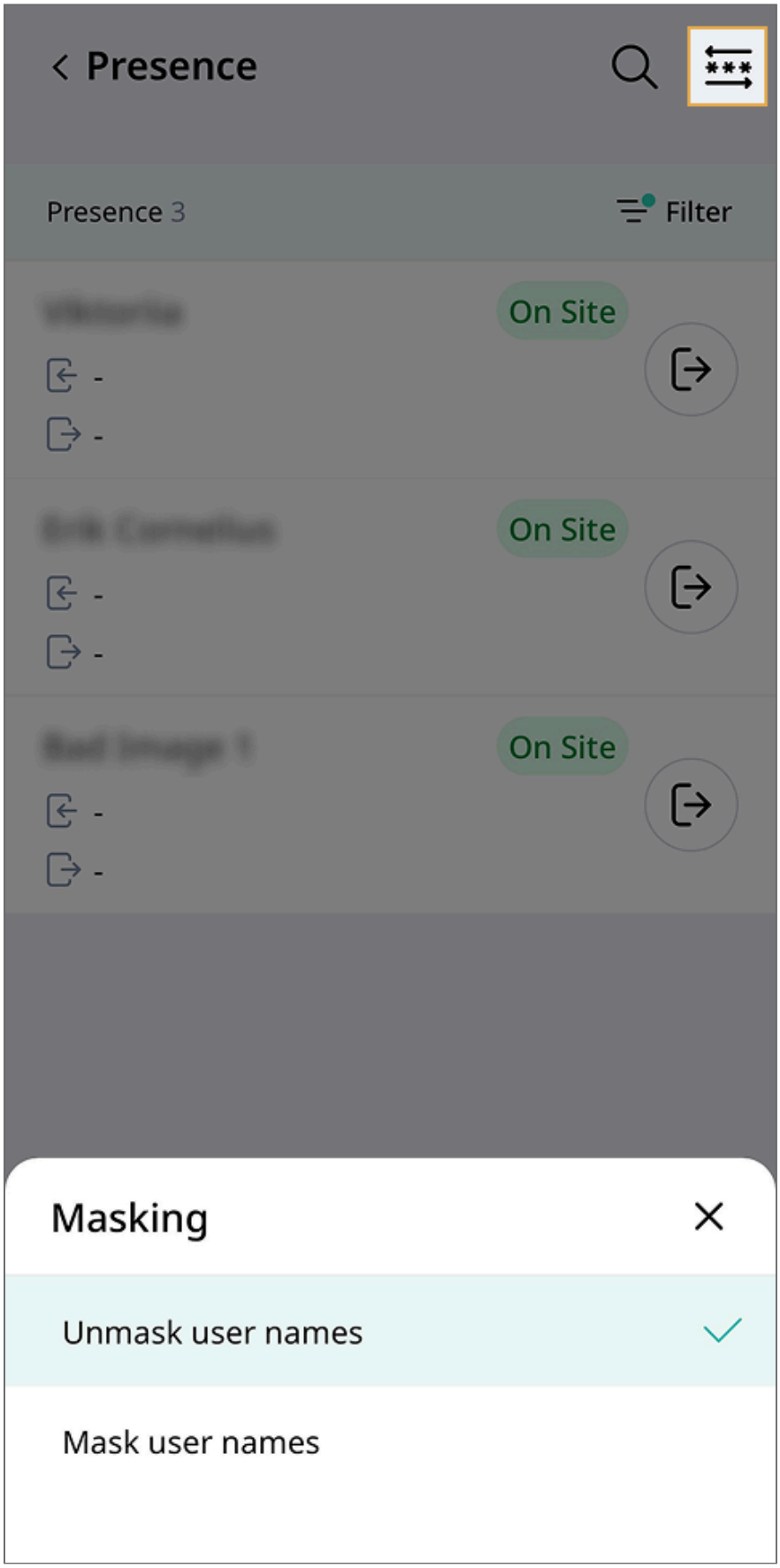
- **Marcar en sitio** / **Marcar fuera del sitio**: Cambia el estado de presencia del usuario a En el sitio o Fuera del sitio. Para más información, consulte Cambiar manualmente el estado de presencia.

- **Enmascarar nombres** / **Desenmascarar nombres** (): Oculta o muestra nombres de usuario. Útil al compartir la pantalla en entornos sensibles.

Web



Mobile

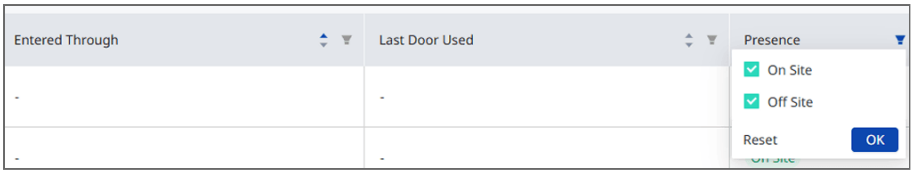


- **Actualizar**: Actualiza la lista de inmediato para mostrar el estado más reciente. En **Autorefrescar** en la parte inferior de la lista, seleccione un intervalo de actualización automática (**Desactivado** / **5 segundos** / **1 minuto**). El sistema actualiza la lista automáticamente según el intervalo establecido.
- **Buscar por nombre...**: Busca en la lista por nombre de usuario.

Filtrar lista de presencia

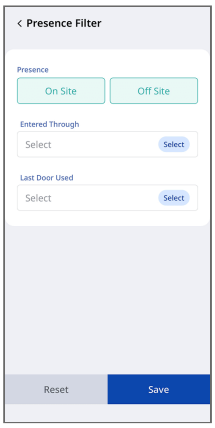
Web

En la columna **Presencia**, haga clic en el botón para filtrar la lista por **En el sitio**, **Fuera del sitio** o todos los usuarios. También filtra por los criterios seleccionados en las columnas **Entrada por** y **Ultima puerta usada**.



> **Información**
> Haga clic en **Reiniciar** para borrar el filtro.

Mobile



1. Toque **Filtros** en la esquina superior derecha de la lista de presencia.
2. Seleccione **En el sitio** o **Fuera del sitio**, o ambos.
3. Seleccione criterios en **Entered Through** y **Last Door Used**.
4. Toque **Guardar** para filtrar la lista según los criterios seleccionados.

> **Información**
> Toque **Reiniciar** para borrar el filtro.

> **Información**
>
> - Para ver a todos los usuarios, seleccione **En el sitio** y **Fuera del sitio** en la columna **Presencia**.
> - La lista de presencia muestra a los usuarios con el estado **En el sitio** de forma predeterminada.

Cambiar manualmente el estado de presencia

Cuando las condiciones reales difieren del estado de presencia registrado en el sistema, un administrador puede cambiarlo.

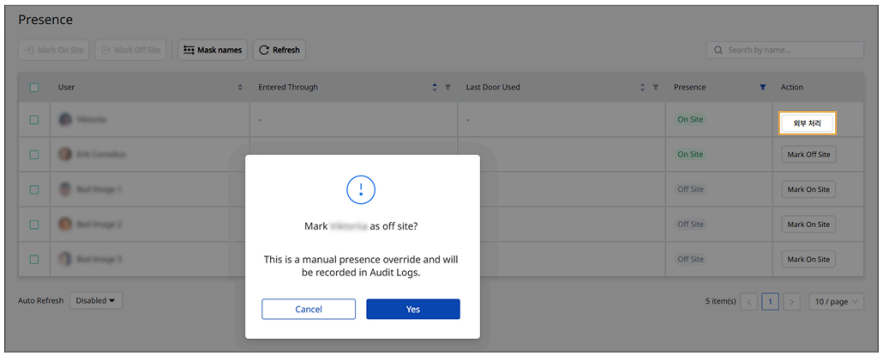
- La precisión de la presencia varía según la instalación de los dispositivos de entrada y salida del sitio. Los sitios con dispositivos de entrada y salida bien definidos proporcionan información de presencia más confiable.
- Si un dispositivo queda sin conexión o se retrasa la entrega de eventos, el estado de presencia se actualiza tras la sincronización.
- El estado de presencia difiere de los permisos de acceso. Los usuarios que aparecen como **En el sitio** no necesariamente pueden acceder a todas las puertas.
- Los usuarios con cuentas vencidas, inactivas o suspendidas no pueden cambiar el estado de presencia hasta que la cuenta esté activa.

> **Información**
>
> Los cambios manuales solo actualizan el estado registrado en el sistema. No verifican físicamente la ubicación del usuario. Consulte el historial de cambios en **Monitoreo** → **Registros de auditoría**.

Cambiar el estado de presencia de un usuario

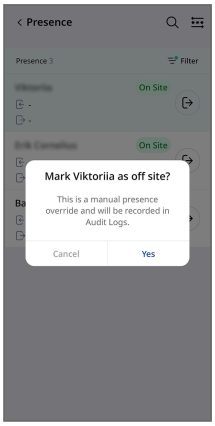
Web

1. En la columna **Accion** del usuario, haga clic en **Marcar en sitio** o **Marcar fuera del sitio**.



2. Cuando aparezca el mensaje de confirmación, haga clic en **Sí**.

Mobile

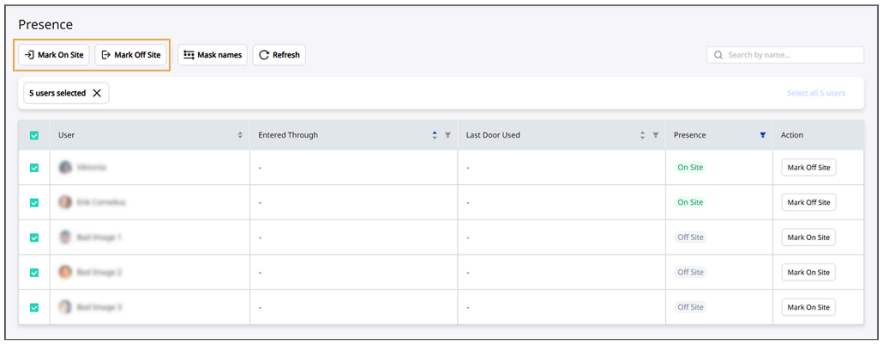


1. En la lista, toque ⎋ o ⎆ junto al usuario para cambiar el estado.
2. Cuando aparezca el mensaje de confirmación, toque **Sí**.

Cambiar el estado de presencia de varios usuarios

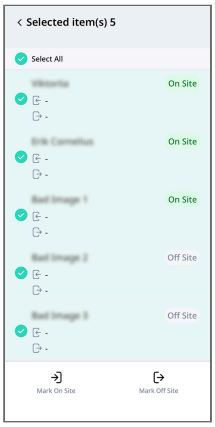
Web

1. Haga clic en la casilla de verificación de cada usuario para cambiar el estado de presencia. Selecciona uno o más usuarios.
2. Haga clic en **Marcar en sitio** o **Marcar fuera del sitio** en la parte superior de la lista.



3. Cuando aparezca el mensaje de confirmación, haga clic en **Sí**.

Mobile



1. Mantenga presionado al usuario en la lista para cambiar su estado.
2. Seleccione al usuario para cambiar el estado. Selecciona uno o más usuarios.
3. Toque **Mark On Site**( ) o **Mark Off Site**( ) en la parte inferior de la pantalla.
4. Cuando aparezca el mensaje de confirmación, haga clic en **Sí**.

Pase de lista

Con la feature Roll Call de BioStar Air, las organizaciones pueden supervisar qué usuarios evacuaron de forma segura durante una emergencia. Configure puntos de reunión y ejecute un Roll Call en la app móvil de BioStar Air. Los administradores identifican rápidamente a los usuarios en el sitio según la información de Presencia y confirman su seguridad.

Listas de reunión precisas basadas en Presencia

- Roll Call no asume que todos los usuarios están en el sitio. Use la información de Presencia para incluir solo a los usuarios confirmados en el sitio al momento de la emergencia como objetivos de Roll Call.
- Asigne grupos de usuarios a ciertos puntos de reunión y designe administradores dedicados. Los responsables de seguridad se enfocan en los usuarios asignados.
- La app Suprema Pass guía a los usuarios con credenciales móviles en el sitio al punto de reunión correcto y advierte a los usuarios fuera del sitio que no ingresen a la instalación durante una emergencia.

Información

- Asegúrese de que los puntos de reunión estén asignados correctamente a los grupos de usuarios para evitar confusiones.
- Pruebe regularmente la función de Roll Call para asegurar un funcionamiento sin problemas durante una emergencia real.
- Utilice los eventos de acceso para verificar la asistencia y cumplir con las normas de seguridad.

Consejo

Vea el siguiente video para obtener una guía sobre el Roll Call y los puntos de reunión.

Antes de comenzar

- La precisión de Roll Call depende de la detección de Presencia. Si configura **Perímetro** de forma incorrecta, la lista de Roll Call puede diferir del conteo real de personas en el sitio.
- Las notificaciones móviles requieren la app Suprema Pass. Los usuarios que usan solo tarjetas RF o credenciales biométricas no reciben notificaciones móviles de Roll Call.
- Los usuarios en el sitio sin un punto de reunión asignado podrían no recibir indicaciones.
- Si configura el ajuste **Administradores asignados** de forma incorrecta, la pantalla de Roll Call esperada podría no aparecer para los administradores.
- Si un dispositivo queda sin conexión o la entrega de eventos se retrasa, esto puede afectar la información de Presencia y la precisión de Roll Call.
- Los usuarios inactivos no reciben notificaciones de Roll Call.

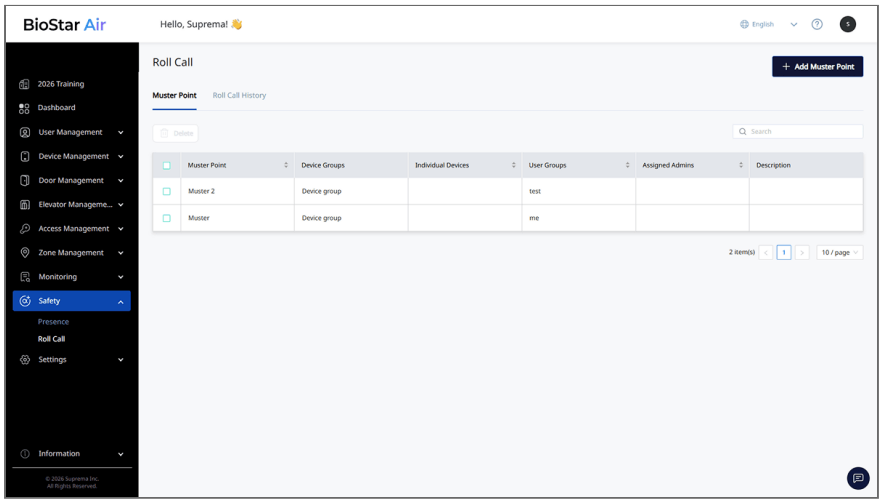
Información

Los usuarios y administradores que usan versiones anteriores de la app Suprema Pass o BioStar Air pueden seguir usando el método de Roll Call heredado. Actualice a la versión más reciente para usar las nuevas características.

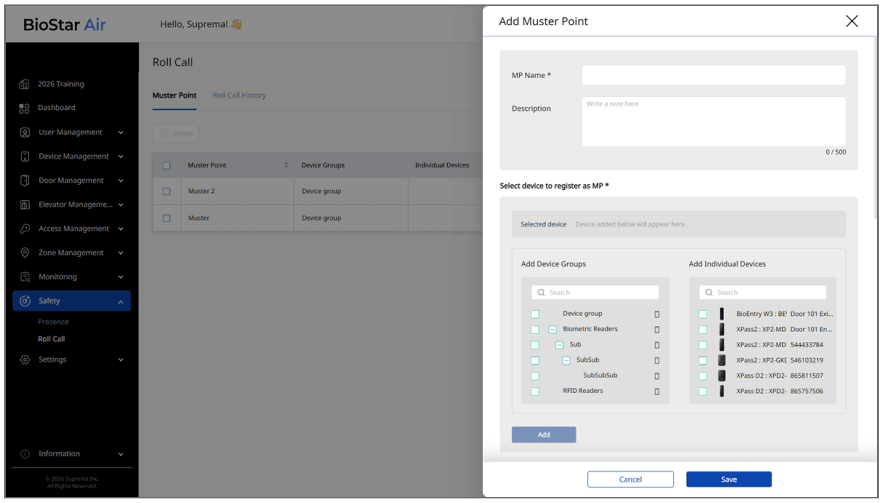
Configurar puntos de reunión

Un punto de reunión es un lugar designado donde los usuarios autentican sus credenciales para indicar que están seguros durante una emergencia.

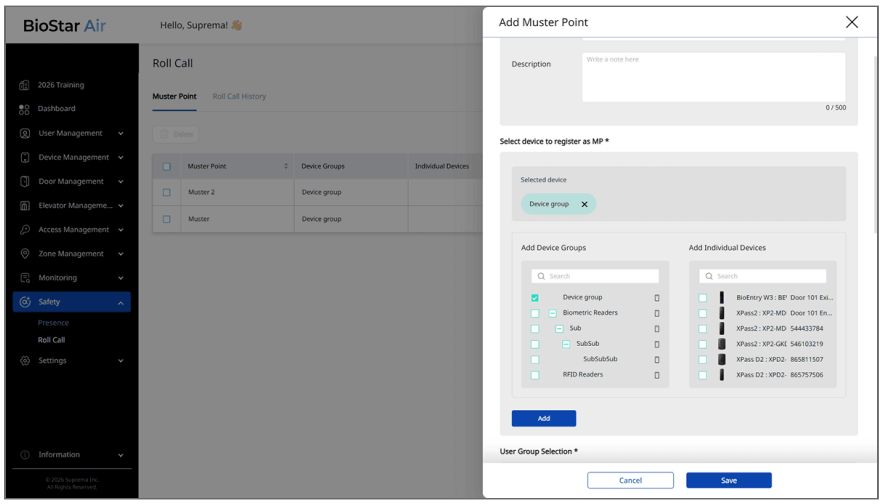
1. Haga clic en **Seguridad** → **Roll Call** en la barra lateral izquierda.
2. Haga clic en **Agregar punto de encuentro** en la esquina superior derecha de la pantalla.



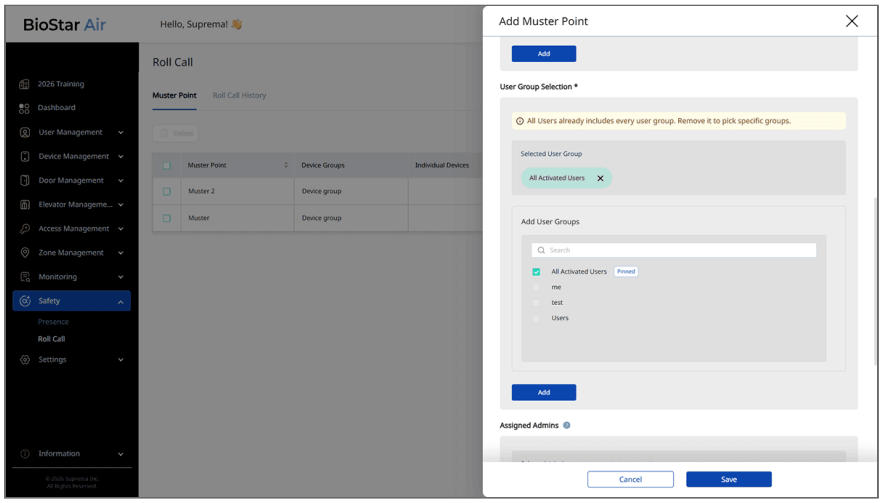
3. Ingrese el nombre del punto de reunión y la descripción (opcional) cuando aparezca el panel **Agregar punto de encuentro**.



4. En la sección **Seleccionar dispositivo para registrar como MP ***, agregue el grupo de dispositivos o el dispositivo para asignarlo al punto de reunión. Seleccione la casilla del grupo de dispositivos o del dispositivo y haga clic en **Agregar**.



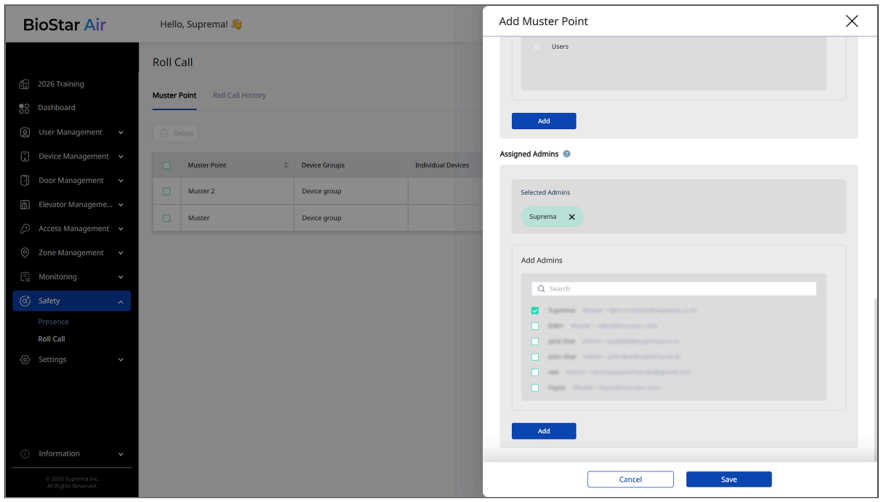
5. En la sección **Selección de grupo de usuarios ***, seleccione los grupos de usuarios que deben reportar cuando llegan al punto de reunión.



- Seleccione la casilla del grupo y haga clic en **Agregar**.
- **Todos los usuarios activos**: Asigna todos los usuarios activos del sitio de BioStar Air a un punto de reunión seleccionado. Ejecutar un Roll Call no supone que todos los usuarios activos estén en el sitio. Se dirige solo a los usuarios con estado en el sitio confirmado según la detección de presencia. Habilitar esta opción desactiva la selección de grupos de usuarios individuales. Primero deshabilite esta opción para seleccionar solo ciertos grupos

de usuarios.

6. En la sección **Administradores asignados**, seleccione la casilla del administrador que ejecutará el Roll Call en la ubicación de reunión y haga clic en **Agregar**.



- Si selecciona **Administradores asignados**, solo los administradores seleccionados pueden iniciar el Roll Call. Durante un Roll Call en curso, solo pueden ver y administrar a los usuarios de sus puntos de reunión asignados.
- Si no asigna **Administradores asignados**, los usuarios con el rol **Maestro**, **Administración** o **Operador** pueden iniciar el Roll Call.
- Un administrador no se puede asignar como administrador designado para varios puntos de reunión al mismo tiempo.

7. Haga clic en **Guardar** para guardar los ajustes del punto de reunión.

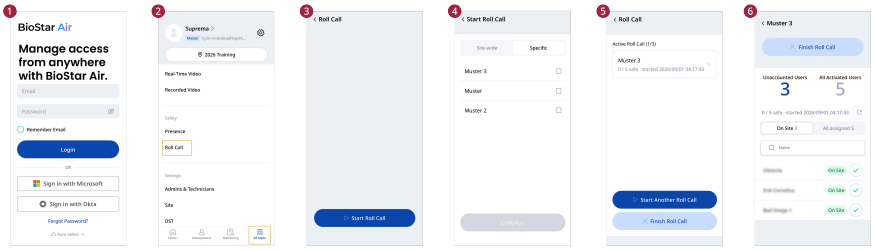
Mejores prácticas para los puntos de reunión

- Haga que el nombre y la descripción del punto de reunión sean claros y fáciles de entender. Por ejemplo, use nombres como "Estacionamiento Este" o "Vestíbulo del Edificio Principal".
- Al agregar varios dispositivos a un punto de reunión, seleccione un grupo de dispositivos en lugar de dispositivos individuales. Los grupos de dispositivos permiten administrar varios dispositivos a la vez. Para obtener más información sobre la administración de grupos de dispositivos, consulte Gestionar Grupos de Dispositivos y Paneles.
- En un campus grande con varios edificios, asigne **solo a los usuarios relevantes** a un punto de reunión específico.
- Los dispositivos de control de acceso cableados admiten tanto la autenticación móvil como por tarjeta, mientras que Airfob Tag y Airfob Patch admiten solo credenciales móviles.

Iniciar Roll Call

Iniciar en la aplicación móvil

Inicie una lista de asistencia y verifique la asistencia en la aplicación móvil BioStar Air.



1. Abra la aplicación BioStar Air en su dispositivo móvil e inicie sesión.
2. Toque **All Menu** → **Roll Call** en la parte inferior de la pantalla.
3. Toca **Start Roll Call**.
4. Seleccione el punto de reunión para iniciar Roll Call y, luego, toque **Continue**.

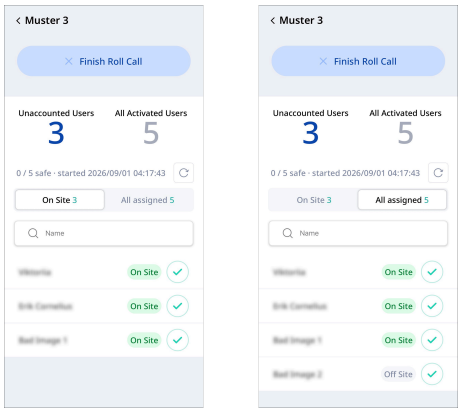
   Para ejecutar Roll Call en todos los puntos de reunión, seleccione **Site-wide** y, luego, toque **Continue**.
5. Seleccione un punto de reunión en la lista de Roll Call en curso.
6. Se muestra una lista con todos los usuarios que deben reunirse en el punto de encuentro.

Diferencias por rol de administrador

- Los usuarios **Maestro**, **Administración** y **Operador** pueden ver la lista de Roll Call. Esto aplica cuando no están asignados como **Administradores asignados** para el punto de reunión. Inician nuevos Roll Calls en el orden indicado arriba.
- **Administradores asignados** recibe una notificación cuando inicia el Roll Call en el punto de reunión asignado. Toque la notificación para ir directamente a la pantalla de progreso del punto de reunión asignado.

Explorar la pantalla de Roll Call activa

Cuando inicia el Roll Call, aparece el estado de progreso con el nombre del punto de reunión.

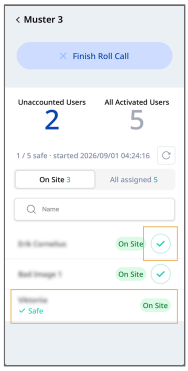


- En la parte superior de la pantalla, revisa el número de **Unaccounted Users** y **All Activated Users**.

  Debajo del conteo, aparecen **personas marcadas como seguras/total de personas** y la **hora de inicio del Roll Call**. Toca el botón de actualizar (↻) para revisar el estado más reciente.
- Cambia el rango de usuarios que se muestra en la lista.
  - **On Site**: Muestra solo a los usuarios cuyo estado de Presencia es En el sitio.
  - **All assigned**: Muestra todos los usuarios asignados a esta zona de reunión, sin importar el estado de presencia. Los usuarios marcados como Seguro se mueven al final de la lista.
- Usa la búsqueda para encontrar a un usuario específico.
- A la derecha de cada usuario en la lista, revisa el

estado de Presencia (**En el sitio** / **Fuera del sitio**).

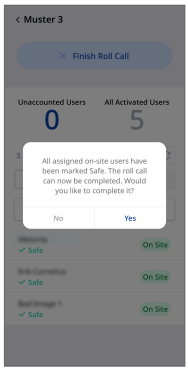
Marcar a los usuarios como seguros



Los administradores o los usuarios pueden marcarse como seguros de las siguientes formas.

- Un administrador puede mantener presionada la **marca de verificación** junto al nombre de un usuario en la app móvil para marcarlo como seguro.
- Los usuarios acercan su credencial a un dispositivo en la zona de reunión asignada.

Completar el pase de lista



Completa el pase de lista cuando se cumpla cualquiera de las siguientes condiciones.

- Cuando aparezca la ventana del mensaje de finalización porque el número de usuarios En el sitio —es decir, **Unaccounted Users**— incluidos en el alcance del Roll Call sea 0, toca el botón **Yes**
- Cuando el administrador marque manualmente a todos los usuarios como seguros y toque el botón **Finish Roll Call**
- Han pasado 24 horas

Finalizar alcance por rol

- El maestro del sitio puede finalizar los Roll Calls uno por uno, finalizar varios a la vez, o finalizar todos los Roll Calls en curso del sitio.
- Administración o Operador seleccionados en **Administradores asignados** solo pueden finalizar Roll Calls de las zonas que gestionan.

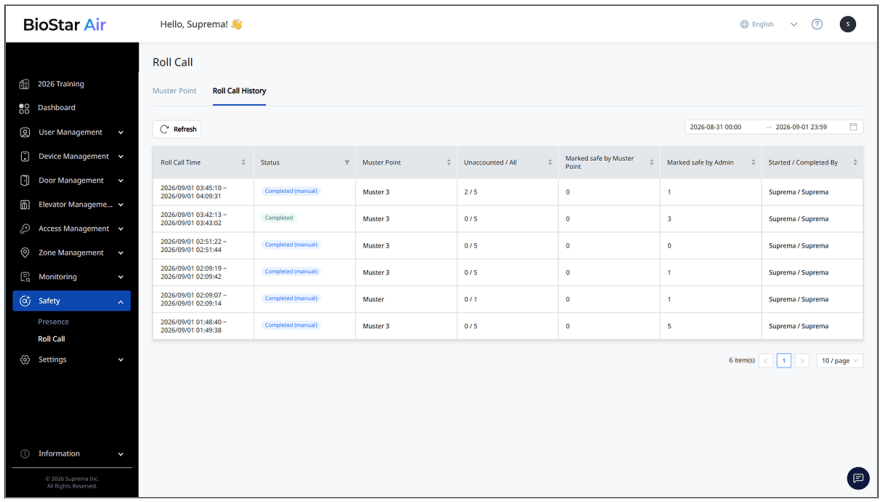
Información

Marque manualmente como a salvo a los usuarios con el estado **Fuera del sitio**. Por ejemplo, marque con anticipación como a salvo a los usuarios que trabajen desde casa ese día.

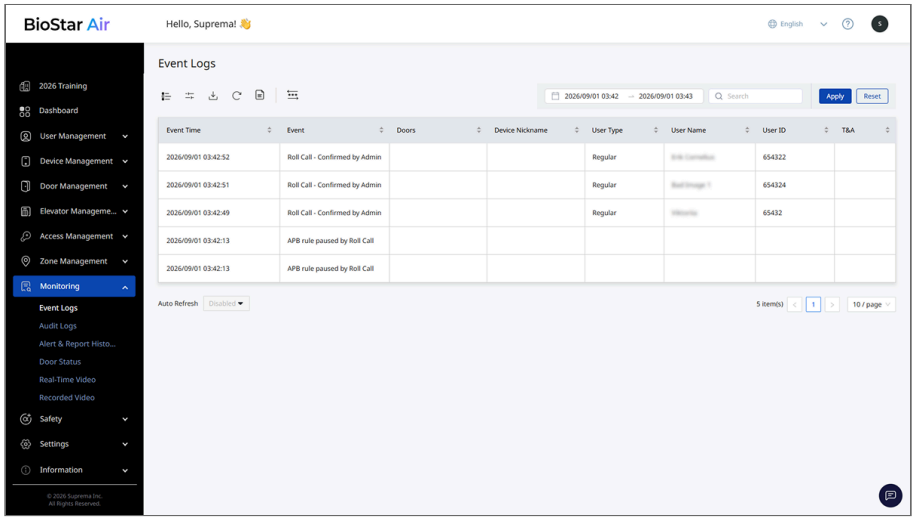
Ver el historial de pases de lista

Ver el historial de pases de lista anteriores.

1. Haga clic en **Seguridad** → **Roll Call** en la barra lateral izquierda.
2. Haz clic en la pestaña **Historial de Roll Call**.



3. Haz clic en una entrada de pase de lista completada para ver sus detalles.



- Ver la lista de todos los eventos de acceso registrados durante el pase de lista.
- Comprueba si cada usuario fue marcado como seguro o quedó sin confirmar.
- Comprueba las horas de inicio y fin del pase de lista.

Configurar ajustes del sitio

Gestione la configuración básica necesaria para operar BioStar Air. Configure el sistema para cumplir con los requisitos de la organización administrando las cuentas de administrador con privilegios operativos, estableciendo la información básica de la organización, configurando las zonas horarias y las alertas, personalizando las plantillas de correo electrónico y definiendo los formatos de tarjeta.

Consejo

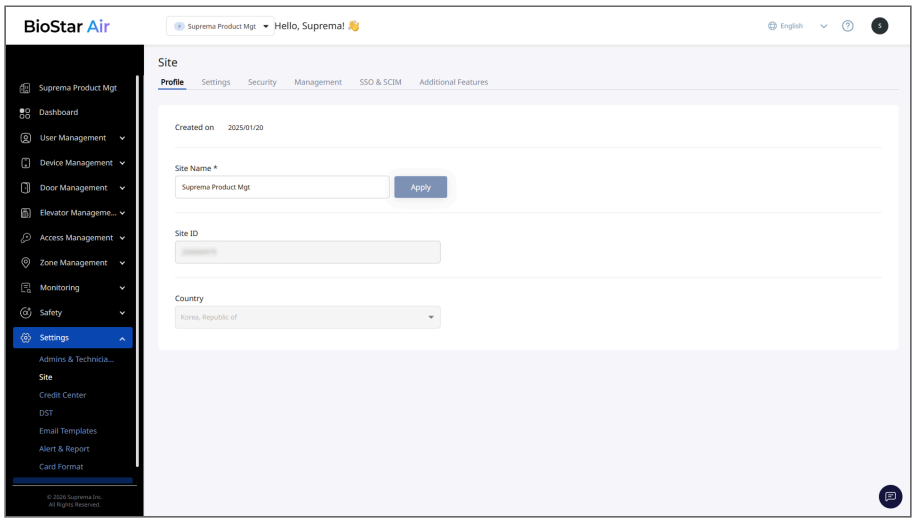
Vea el siguiente video para obtener una guía sobre la configuración del sitio.

Configuración del perfil

La información del sitio es la configuración más básica en BioStar Air. Esta guía explica cómo gestionar datos básicos, como el nombre y el identificador del sitio, y cómo eliminar un sitio cuando sea necesario.

Configurar la información del sitio

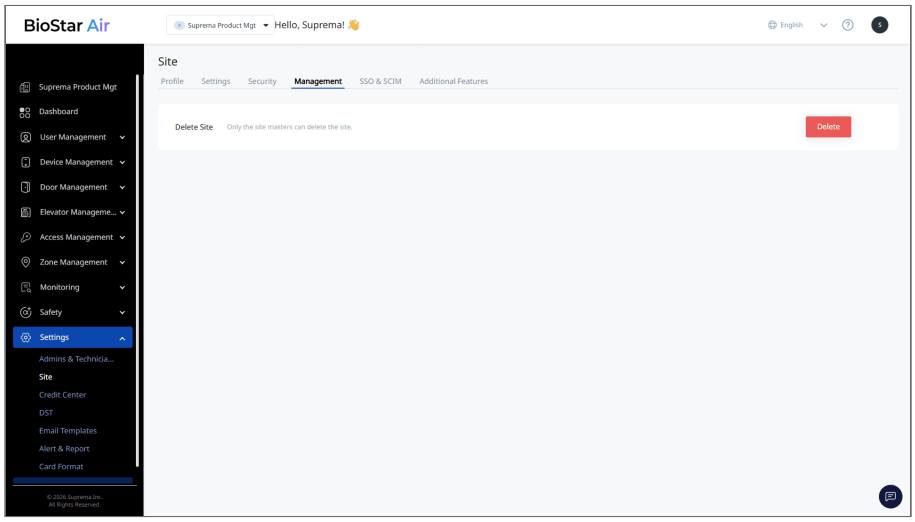
Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda. Utilice la pestaña **Perfil** para modificar la información básica del sitio.



- **Nombre del sitio**: El nombre del sitio. Escriba un nuevo nombre y haga clic en **Aplicar**. Puede cambiarlo en cualquier momento.
- **Identificación del sitio**: Identificador único requerido para solicitudes de soporte. Copie y proporcione el identificador del sitio al comunicarse con el equipo de MOCA.
- **País**: Se establece al crear el sitio y no se puede cambiar posteriormente. Solicite cambios a través del Portal de Socios de BioStar Air.

Eliminar el sitio

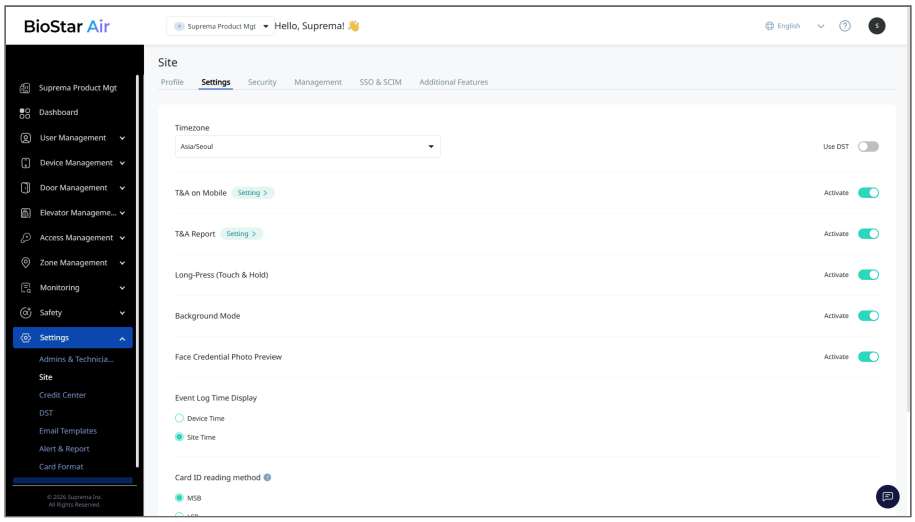
Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda. La única opción disponible en la pestaña **Administrar** es **Eliminar sitio**. Esta acción es irreversible, y solo el **administrador principal** puede eliminar un sitio.



Configuración Avanzada

Configure las opciones avanzadas para optimizar BioStar Air según el entorno laboral de su organización. Establezca la zona horaria y el horario de verano, habilite el control de tiempo y asistencia y ajuste los métodos de autenticación móvil y la visualización de los registros de eventos.

Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda. Utilice la pestaña **Settings** para configurar los ajustes del sitio.



- **Zona horaria**: Cambie la zona horaria en cualquier momento. El sistema registra los eventos y los registros según la zona horaria configurada. Para obtener más información, consulte Horario de Verano (DST).
  - **Usar DST**: Active o desactive el horario de verano para determinadas regiones.
- **T&A en dispositivos móviles**: Active la función de tiempo y asistencia (T&A). Tras activarla, haga clic en **Ajustes** para configurar los ajustes detallados. Para obtener más información, consulte Tiempo y asistencia (T&A).
- **Informe de tiempo y asistencia**: Genere informes de tiempo y asistencia (T&A). Después de activar la función de informes, haga clic en **Ajustes** para configurar las condiciones del informe. Para obtener más información, consulte Informe de tiempo y asistencia.
- **Pulsación prolongada (tocar y mantener)**: Active la función Long Touch para abrir puertas de forma remota desde cierta distancia.
- **Modo de fondo**: Permitir el uso de tarjetas móviles mientras la aplicación Suprema Pass se ejecuta en segundo plano. Cuando está activado, los usuarios pueden abrir una puerta sin abrir la aplicación.
- **Vista Previa de la Foto de la Cedencial Facial**: Mostrar una vista previa del rostro al emitir credenciales faciales.
- **Pantalla de tiempo de registro de eventos**: Establezca cómo se muestran las horas en los registros de eventos.
  - **Hora del dispositivo**: Mostrar los registros de eventos según la zona horaria de cada dispositivo.
  - **Hora del sitio**: Mostrar los registros según la zona horaria del sitio. Útil cuando todos los dispositivos están en una misma ubicación. Consulte la opción **Zona horaria**.
- **Método de lectura de ID de tarjeta**: Configure cómo se transmiten los datos de la tarjeta al usar Airfob Patch con lectores de terceros.

> Esta configuración se aplica únicamente a los dispositivos Patch y puede ajustarse para coincidir con el tipo de dispositivo de terceros al que está conectado el Patch.

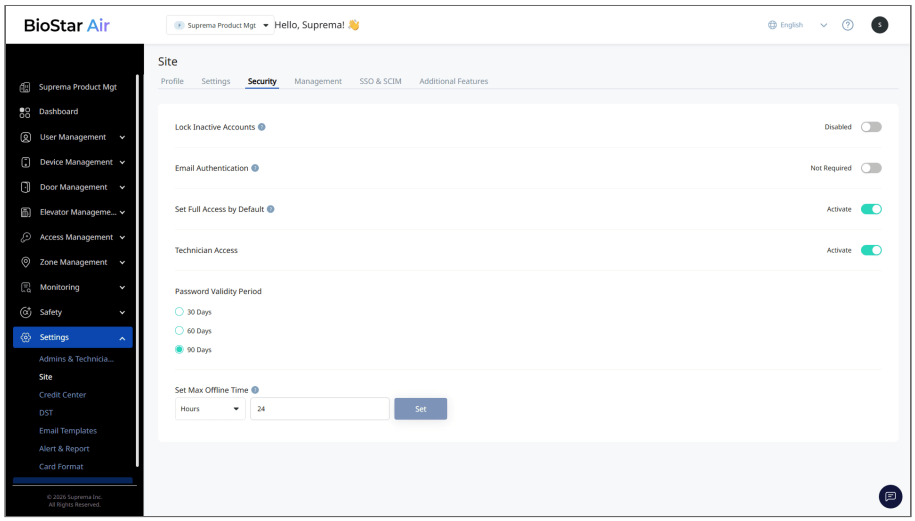
- **Período de validez para el enlace de activación/reemisión de tarjeta de acceso móvil**: Establezca el período de validez predeterminado para las credenciales móviles.

> Los administradores pueden establecer una fecha de caducidad distinta para las credenciales de cada usuario. Para obtener más información, consulte Agregar usuarios.

Configuración de seguridad

Configure correctamente las políticas de seguridad para evitar el acceso no autorizado y mantener el sitio protegido. Puede reforzar la seguridad bloqueando cuentas de administrador inactivas, habilitando la autenticación de 2 factores por correo electrónico y estableciendo intervalos para el cambio de contraseña.

Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda. Utilice la pestaña **Seguridad** para configurar los ajustes de seguridad del sitio.



- **Bloquear cuentas inactivas**: Bloquee las cuentas de administrador que hayan estado inactivas por más de 90 días.
- **Verificacion de Email**: Exija autenticación de dos factores por correo electrónico cada vez que un administrador inicie sesión.
- **Establecer acceso total de forma predeterminada**: Conceda 'acceso total' a los nuevos usuarios de forma predeterminada cuando no se seleccionen otros derechos de acceso. Si esta opción está deshabilitada, asigne los niveles de acceso manualmente. A los usuarios temporales no se les concede acceso total automáticamente, incluso si la opción anterior está activada.

> Para obtener más información sobre los niveles de acceso, consulte Administrar Niveles de Acceso.

- **Acceso de Técnico**: Permitir que las cuentas de técnicos accedan al sitio. Si esta configuración está deshabilitada, las cuentas de técnicos no podrán acceder al sitio.

> Para obtener más información sobre cómo gestionar el acceso al sitio para las cuentas de técnicos, consulte Asignar técnicos a un sitio.

- **Período de validez de la contraseña**: Exija el restablecimiento de la contraseña cada 30, 60 o 90 días.

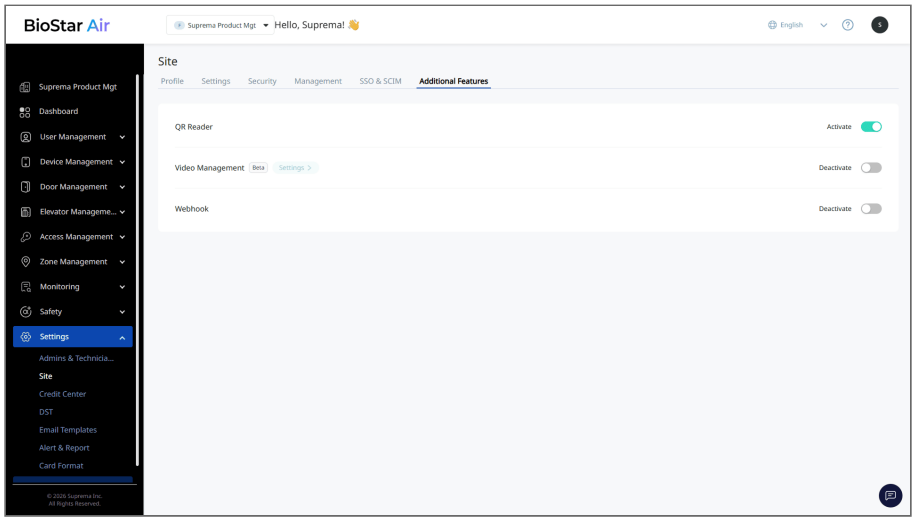
- **Establecer el tiempo máximo sin conexión**: Establezca cuánto tiempo permanecen válidas las credenciales móviles cuando el dispositivo está sin conexión.

  – El valor predeterminado es 5 minutos y se puede establecer entre 1 minuto y 8 días.
  – Esto ayuda a equilibrar la seguridad y la comodidad, especialmente en sitios remotos con conectividad de red limitada.

Configuración de funciones adicionales

Puede habilitar o deshabilitar funciones adicionales necesarias para el funcionamiento del sitio, como el soporte para lectores de códigos QR, la integración con cámaras IP compatibles con ONVIF y el reenvío de eventos a sistemas externos (webhooks).

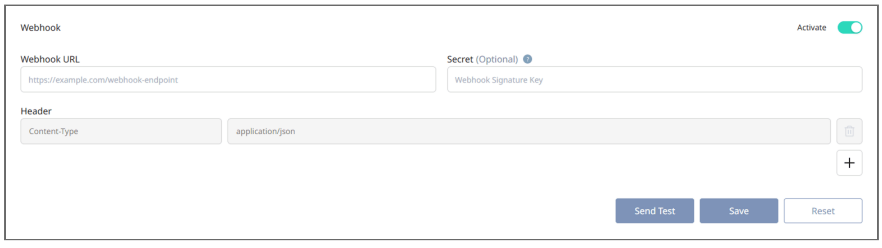
Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda. Utilice la pestaña **Adicionales** para habilitar o deshabilitar funciones adicionales.



- **Lector QR**: Admite lectores de códigos QR. Desactive esta opción si no utiliza un lector de códigos QR.
- **Gestión de Vídeos**: Admite cámaras IP compatibles con ONVIF. Habilite esta función para integrar BioStar Air con la videovigilancia. Después de habilitarla, haga clic en **Ajustes** para establecer el tiempo de reproducción del registro de eventos.

  Para obtener más información sobre la gestión de video, consulte Soporte y configuración de cámaras IP.

- **Webhook**: Habilite los webhooks para enviar eventos de BioStar Air a sistemas externos. Después de habilitar la función, configure los campos a continuación.



- **URL del Webhook**: Ingrese la dirección del endpoint del servidor externo que recibirá los eventos. Ejemplo: `https://example.com/webhook-endpoint`
- **Secreto**: Un token de seguridad usado para verificar que la solicitud del webhook proviene de un servidor de confianza. El servidor remitente cifra la carga útil con la clave de seguridad usando SHA-256 y la envía en el encabezado `X-Signature`.
- **Enviar Teste**: Verifique que el webhook funcione correctamente. Envíe un mensaje de prueba para confirmar que el servidor externo recibe y responde a la solicitud.

> **Información**
>
> - Después de introducir toda la información requerida, haga clic en **Guardar**.
> - Haga clic en **Reiniciar** para inicializar la información introducida.

Administrar cuentas y roles de administradores

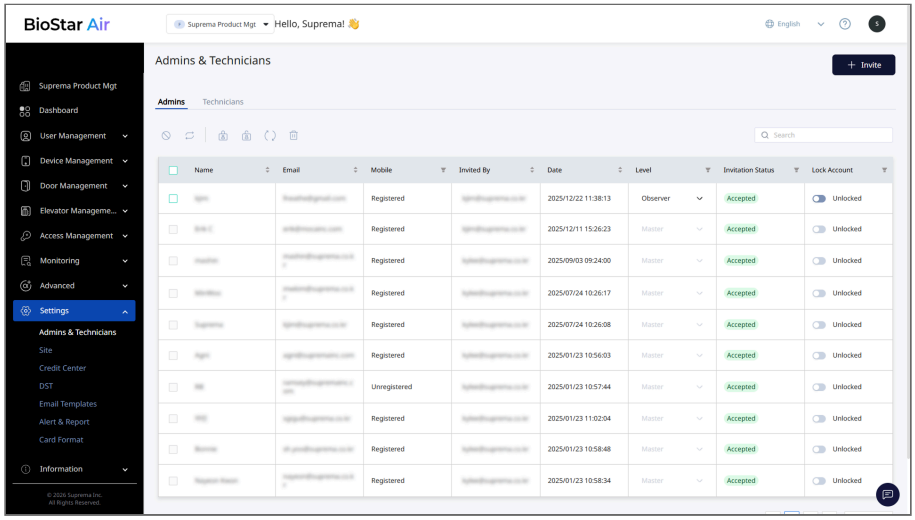
Use las funciones de administración y gestión de roles de BioStar Air para controlar eficazmente el acceso al sitio. Asigne los 4 roles — Observador, Operador, Administrador y Maestro — para otorgar a cada persona solo los permisos que necesita, garantizando seguridad y eficiencia operativa.

Este documento abarca todo el ciclo de vida de las cuentas de administrador: desde invitar administradores hasta asignar roles, gestionar permisos y bloquear cuentas.

> **Consejo**
>
> Mira el siguiente video para ver cómo gestionar administradores.

Ver administradores

Haga clic en **Ajustes** → **Administradores y técnicos** en la barra lateral izquierda.



Información

Habilitar la opción **Acceso de Técnico** cambia el menú **Ajustes** → **Administración** al menú **Administradores y técnicos**. Las pestañas **Administración** y **Técnicos** permiten administrar las cuentas de administrador y de técnico por separado.

Para más información sobre cómo habilitar **Acceso de Técnico**, consulte Administrar cuentas de técnicos..

Lista de administradores

El menú **Administradores y técnicos** muestra una lista de todos los administradores. La lista de administradores incluye la siguiente información.

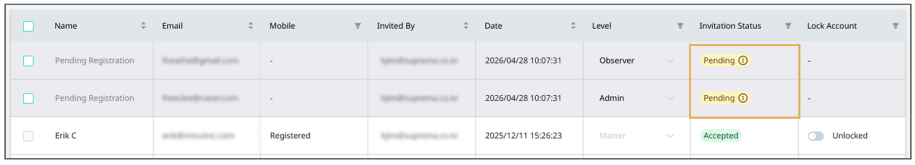
- **Nombre**: El nombre del administrador.
- **Correo Electrónico**: La dirección de correo electrónico del administrador.
- **Móvil**: El número de teléfono del administrador.
- **Invitado por**: La dirección de correo electrónico de la persona que invitó al administrador.
- **Fecha**: La fecha en que se invitó al administrador.
- **Nivel**: El nivel de permisos del administrador. Para más información, consulte Niveles de administrador.
- **Estado de la invitación**: El estado de la invitación de la cuenta de administrador. Para más información, consulte Estado de la invitación.
- **Bloquear cuenta**: El estado de bloqueo de la cuenta de administrador. Puede bloquear o desbloquear una cuenta. Para más información, consulte Bloquear o desbloquear administradores.

Estado de la invitación

La lista de administradores muestra el estado de la invitación de cada administrador.

Registro pendiente

El estado de un administrador invitado aparece como **Pendiente** hasta que acepta la invitación por correo electrónico y completa el registro. Un administrador invitado puede aceptar la invitación haciendo clic en el enlace del correo para registrarse o iniciar sesión y acceder al sitio.

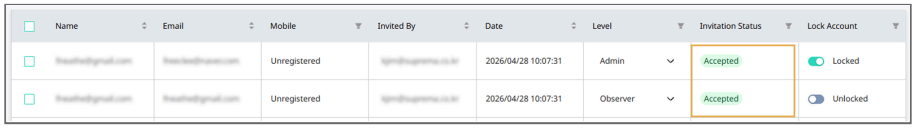


Información

Un administrador invitado tiene hasta 7 días para aceptar la invitación. Después de 7 días, la invitación expira y el estado cambia a **Venció**. Si la invitación expira, puede reenviar el enlace de invitación para que la cuenta invitada pueda registrarse de nuevo. Para más información sobre reenviar enlaces de invitación, consulte Reenviar enlace de invitación.

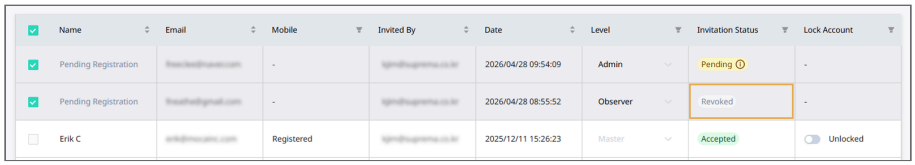
Registro completado

Cuando un administrador invitado acepta la invitación por correo y completa el registro, el estado de la invitación cambia a **Aceptado**. Tras completar el registro, el administrador inicia sesión en el sitio y accede a menús y funciones según su rol asignado.



Invitación revocada

Puede cancelar la invitación si la dirección de correo del administrador invitado es incorrecta o si la invitación ya no es necesaria. Al cancelar la invitación, su estado cambia a **revocado**. Para más información sobre cancelar invitaciones de administrador, consulte Invitación revocada.



Niveles de administrador

Cada nivel de administrador en BioStar Air tiene permisos específicos, y los niveles superiores heredan los permisos de los inferiores.

> **Información**
> Cada rol de administrador tiene permisos distintos en BioStar Air. **Observador** tiene el acceso más restringido y algunos menús no se muestran.

Comparar permisos

Función	Observador	Operador	Administrador	Maestro
Ver Panel/Registros	✔	✔	✔	✔
Exportar registros y generar informes	✔	✔	✔	✔
Gestión Usuarios	✕	✔	✔	✔
Administrar Grupos de Usuarios	✕	✔	✔	✔
Administrar Niveles de Acceso	✕	✔	✔	✔
Administrar horarios	✕	✔	✔	✔
Gestionar grupos de días festivos	✕	✔	✔	✔
Controlar y configurar dispositivos	✕	✕	✔	✔

Función	Observador	Operador	Administrador	Maestro
Invitar administradores	✕	✕	✔	✔
Asignar rol Maestro	✕	✕	✕	✔
Editar o eliminar administradores maestros	✕	✕	✕	✔
Crear subsitios	✕	✕	✕	✔
Configurar ajustes del sitio	✕	✕	✕	✔

Observador (Nivel más bajo)

- **Panel de Control** y los registros **se pueden ver**.
- **Exportar** registros y generar informes.
- **No puede modificar** la configuración, los usuarios ni los dispositivos.
- El acceso a los menús está restringido. La mayoría de los menús no se muestran en pantalla.

Operador

- Puede administrar **Usuarios**, **Grupos de Usuarios**, **Niveles de acceso**, **Horarios** y **Grupos de festivos**.
- **Sin acceso** al control de dispositivos ni a la configuración de administración.
- Adecuado para administrar la configuración diaria de usuarios y accesos.

Administración

- **Puede invitar** a nuevos administradores. Sin embargo, no puede asignar el rol **Maestro**.
- Cuenta con autoridad de **control total sobre los dispositivos** para modificar la configuración y gestionarlos.
- No puede eliminar ni modificar administradores con el rol **Maestro**.
- Este rol suele recomendarse para el personal de TI responsable de la gestión del sistema.

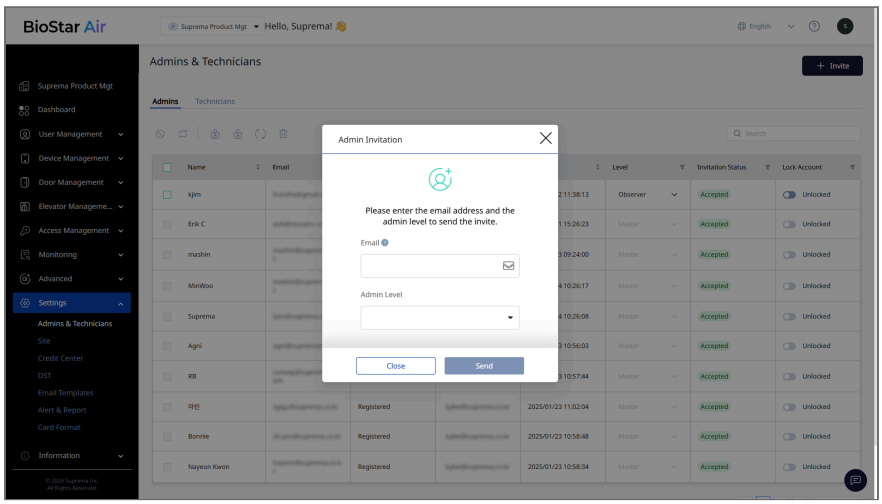
Maestro (Nivel más alto)

- Tiene **acceso total** a todas las configuraciones y funciones.
- No puede eliminarse ni modificarse por los **administradores**.
- Puede crear **subsitios** para gestionar distintas ubicaciones u organizaciones.
- Puede configurar los **ajustes del sitio**, incluyendo las configuraciones críticas a nivel del sistema.
- Responsable de aceptar los **términos** antes de que otros administradores inicien sesión.
- Generalmente asignado al propietario de la empresa o a un ejecutivo de máxima confianza.

Invitar a nuevos administradores

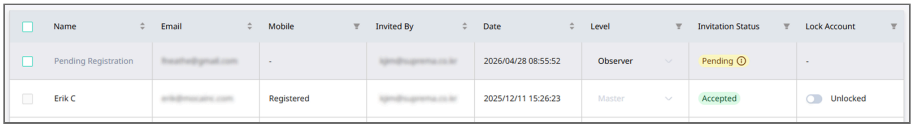
Agregar nuevos administradores.

1. Haga clic en **Ajustes** → **Administradores y técnicos** en la barra lateral izquierda.
2. Haga clic en **Invitar** en la esquina superior derecha de la pantalla.
3. Cuando aparezca la ventana **Invitación de administrador**, ingrese la dirección de correo electrónico.



4. En **Rol de administrador**, seleccione el rol que se asignará al nuevo administrador.
5. Haga clic en **Enviar** para enviar la invitación.

Las cuentas invitadas aparecen en la lista de administradores con **Estado de la invitación** establecido en **Pendiente**. Cuando una cuenta invitada acepta la invitación por correo, su **Estado de la invitación** cambia a **Aceptado**.

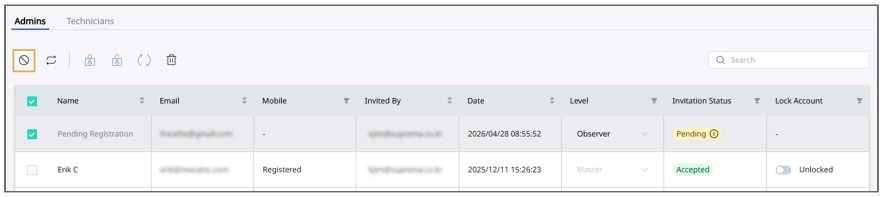


- Una cuenta invitada puede aceptar la invitación hasta por 7 días. Si pasan 7 días, la invitación expira y el estado de la cuenta cambia a **Venció**.
- Cada administrador debe tener una dirección de correo electrónico única. Si es necesario, use una dirección alias (por ejemplo, erik+training@example.com).
- Haga clic en el enlace del correo electrónico de invitación. Regístrese si el administrador no tiene una cuenta. Si el administrador ya tiene una cuenta, inicie sesión para acceder directamente al **sitio**.

Invitación revocada

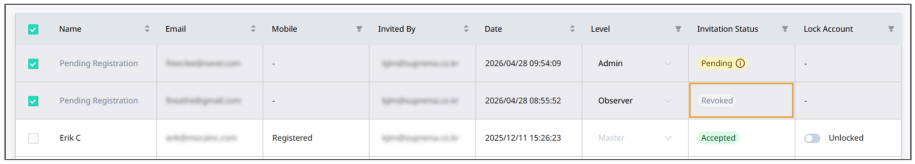
Si una cuenta invitada no ha aceptado la invitación, puede cancelarla. Cancelar la invitación impide que las cuentas pendientes se registren usando el enlace de invitación del correo.

1. Haga clic en la casilla de las cuentas con estado de invitación **Pendiente** en la lista de administradores. Seleccione 1 o más cuentas.
2. Haz clic en ⃠ en la parte superior izquierda de la lista de administradores.



3. Cuando aparezca un cuadro emergente, revisa el mensaje y haz clic en **Sí**.

Las cuentas en la lista de administradores cuyas invitaciones han sido revocadas cambian a **revocado**.

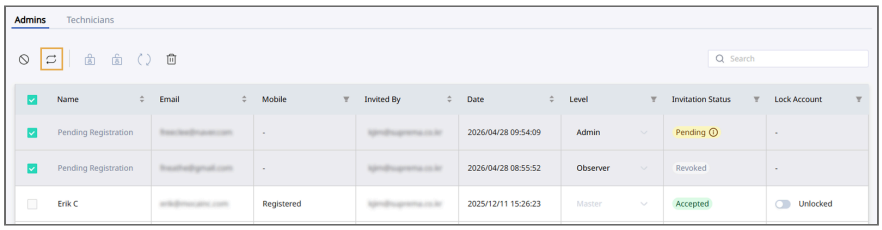


Reenviar enlace de invitación

Puede reenviar el enlace de invitación si una cuenta invitada no recibió o perdió el correo de invitación, o si el enlace ha expirado. Reenviar el enlace permite que el usuario se registre usando el nuevo enlace.

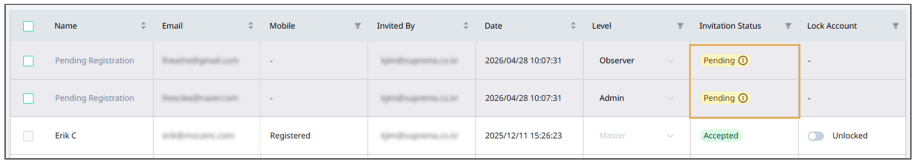
1. Haga clic en la casilla de las cuentas con estado de invitación **Pendiente**, **Venció** o **revocado** en la lista de administradores. Seleccione 1 o más cuentas.

2. Haz clic en ⟲ en la parte superior izquierda de la lista de administradores.



3. Cuando aparezca un cuadro emergente, revisa el mensaje y haz clic en **Sí**.

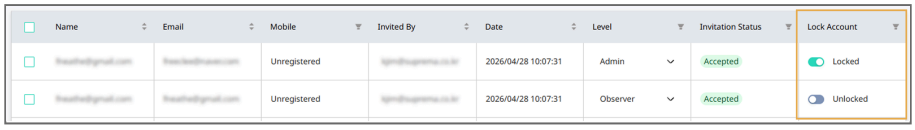
Las cuentas cuyo enlace de invitación se reenvíe cambiarán a **Pendiente**.



Bloquear o desbloquear administradores

Use la opción **Bloquear cuenta** para bloquear o desbloquear administradores que hayan completado el registro aceptando una invitación por correo. Bloquear una cuenta impide que el administrador inicie sesión. La información de la cuenta se conserva para que pueda reactivarse más tarde si es necesario.

En la columna **Bloquear cuenta**, los administradores bloqueados aparecen como **Bloqueado**, y los administradores desbloqueados aparecen como **Desbloqueado**.

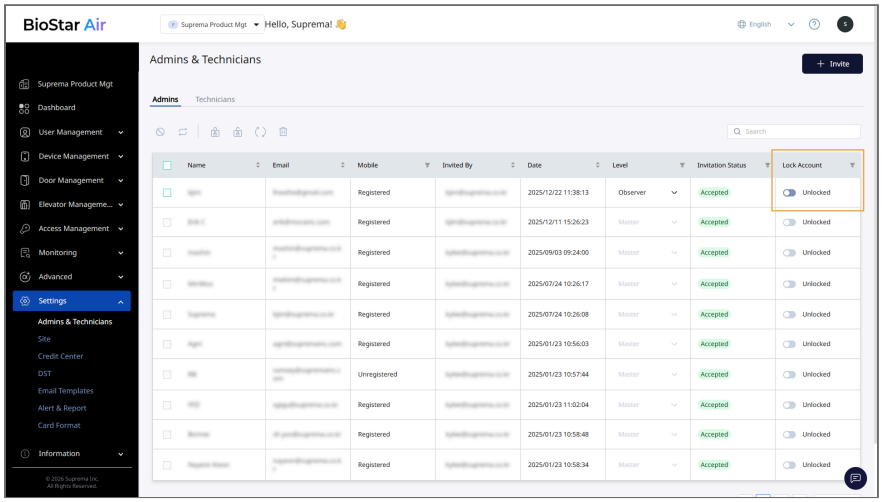


Información

- Solo se pueden bloquear o desbloquear cuentas de administrador que hayan completado el registro.
- La opción **Bloquear cuenta** puede estar restringida por el rol del administrador. Los administradores con el rol **Maestro** no pueden bloquear a otros administradores con el rol **Maestro**.

Bloquear o desbloquear a un administrador individual

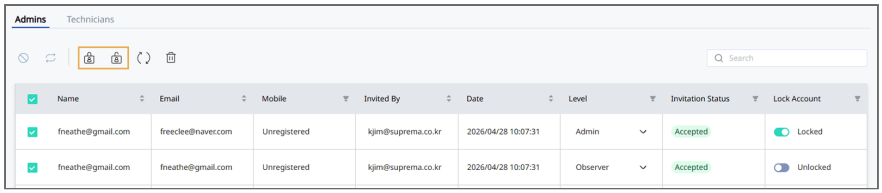
1. Busque al administrador que desea bloquear o desbloquear en la lista.
2. Haz clic en el interruptor de la columna **Bloquear cuenta**.



3. Cuando aparezca la ventana de mensajes, haz clic en el botón **Confirmar**.

Bloquear o desbloquear varios administradores

1. En la lista de administradores, haz clic en la casilla del administrador que quieras bloquear o desbloquear. Selecciona 1 o más administradores.
2. Haz clic en o en la esquina superior izquierda de la pantalla.

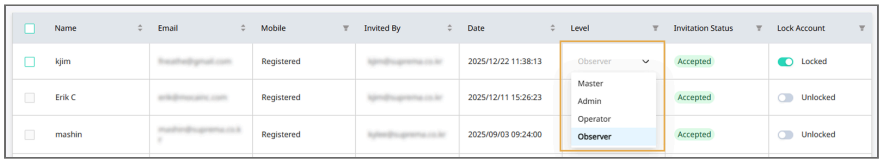


3. Cuando aparezca un cuadro emergente, revisa el mensaje y haz clic en **Sí**.

Cambiar el rol de un administrador

Los administradores pueden cambiar los roles de administradores de nivel inferior. Ajuste los roles cuando cambien las funciones de los empleados, cuando sus responsabilidades aumenten o disminuyan, o durante una reorganización. Reducir el nivel de un rol elimina el acceso del administrador a las funciones que tenía anteriormente.

1. Busque en la lista al administrador cuyo rol desea cambiar.
2. Selecciona el nuevo nivel de administrador en la columna **Nivel**.



3. Cuando aparezca la ventana de mensajes, haz clic en el botón **Confirmar**.

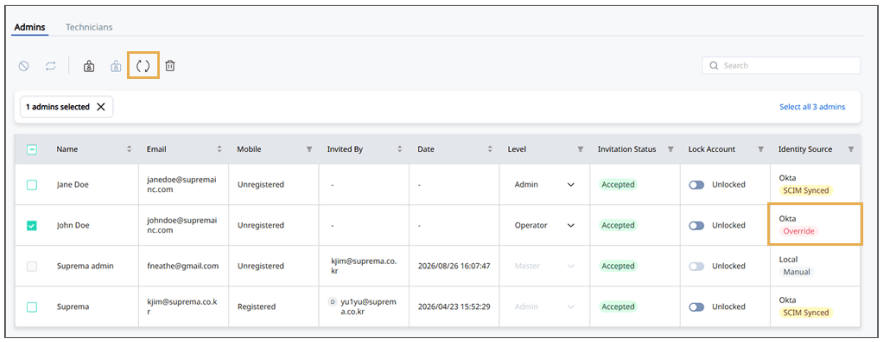
> Solo los administradores con el rol **Maestro** pueden asignar o modificar el rol **Maestro** para otros administradores.

Liberar el estado de sobrescritura

Cambiar manualmente los permisos o el estado de bloqueo de un administrador sincronizado con SCIM establece localmente **Anulación**. Cancela los cambios locales y restaura la gestión de SCIM.

1. En la lista de administradores, haz clic en la casilla junto al administrador cuyo estado sea **Anulación**. Selecciona 1 o más administradores.

2. Haz clic en ⟳ en la parte superior izquierda de la pantalla.



3. Cuando aparezca un cuadro emergente, revisa el mensaje y haz clic en **Sí**.

El sistema borra el estado **Anulación** de la cuenta de administrador seleccionada y lo cambia a **Sincronizado vía SCIM**.

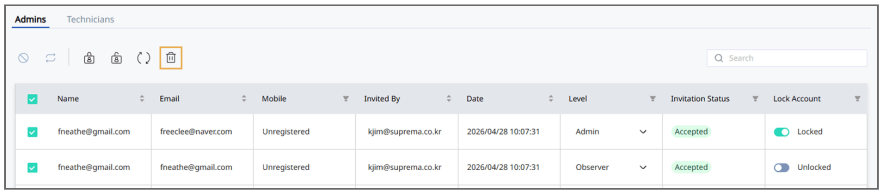
> **Información**
>
> Para obtener más información sobre los ajustes de SSO y SCIM, consulte Configurar SSO Y SCIM.

Eliminar cuenta de administrador

Si elimina una cuenta de administrador, ese administrador no podrá iniciar sesión en el sitio y la información de la cuenta eliminada no se podrá recuperar.

1. En la lista de administradores, haz clic en la casilla del administrador que quieras eliminar. Selecciona 1 o más administradores.

2. Haz clic en 🗑 en la parte superior izquierda de la pantalla.



3. Cuando aparezca un cuadro emergente, revisa el mensaje y haz clic en **Sí**.

Las cuentas de administrador eliminadas ya no aparecen en la lista de administradores.

Administrar cuentas de técnicos.

Un técnico es un profesional al que se le otorga acceso a un sitio del cliente. Para administrar cuentas de técnicos, invita a técnicos en el Partner Portal, asígnalos a sitios y establece sus niveles de permiso.

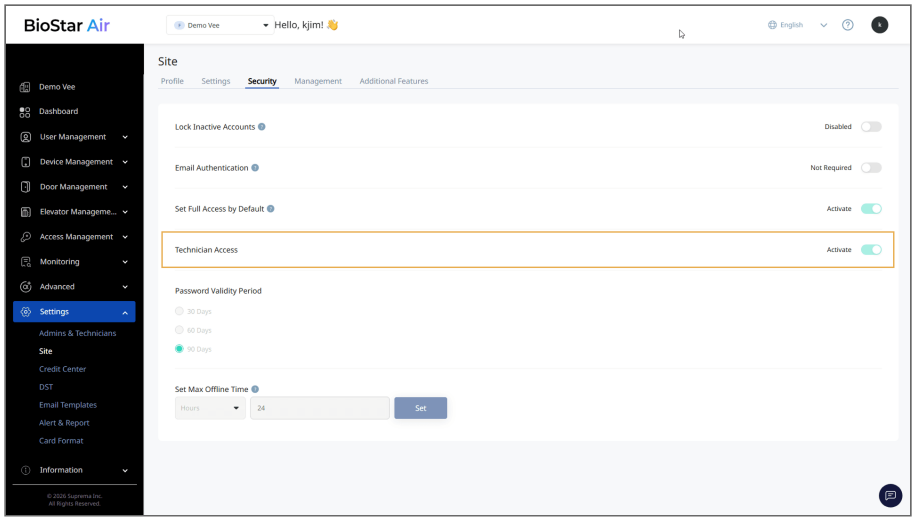
En el portal BioStar Air, modifica los permisos de acceso de un técnico invitado o bloquea/desbloquea su acceso al sitio. También puedes eliminar la cuenta de un técnico por completo para revocar su acceso al sitio.

> **Información**
>
> - Para más información sobre cómo invitar técnicos en el Partner Portal y asignarlos a sitios, consulta Administrar técnicos de socios.
> - Las actividades de los técnicos invitados se registran por cuenta y se pueden ver en **Monitoreo** → **Registros de eventos** / **Registros de auditoría**.

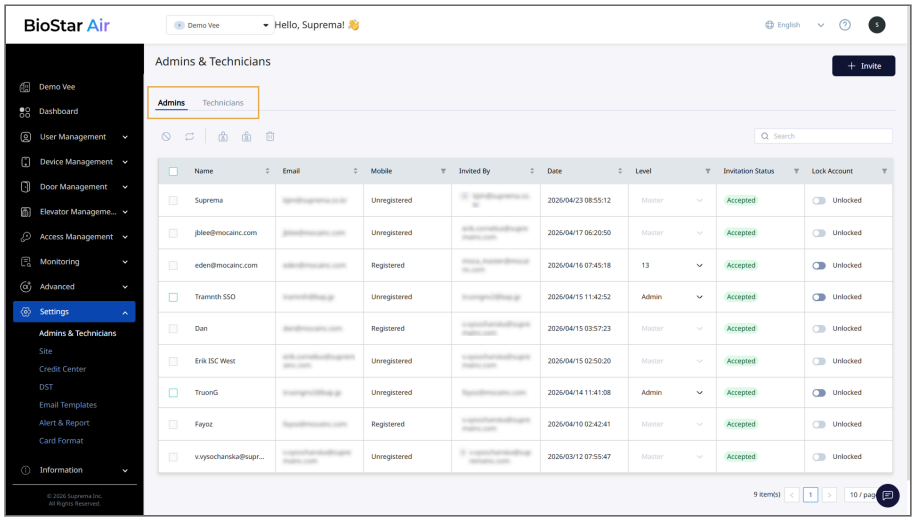
Antes de comenzar

Antes de administrar cuentas de técnicos, asegúrate de permitir que las cuentas de técnicos accedan al sitio en la configuración de seguridad del sitio. Si no lo permites, no podrás administrarlas.

1. Haz clic en **Ajustes** → **Sitio** en la barra lateral izquierda.
2. Haga clic en la pestaña **Seguridad**.
3. Habilite la opción **Acceso de Técnico**.



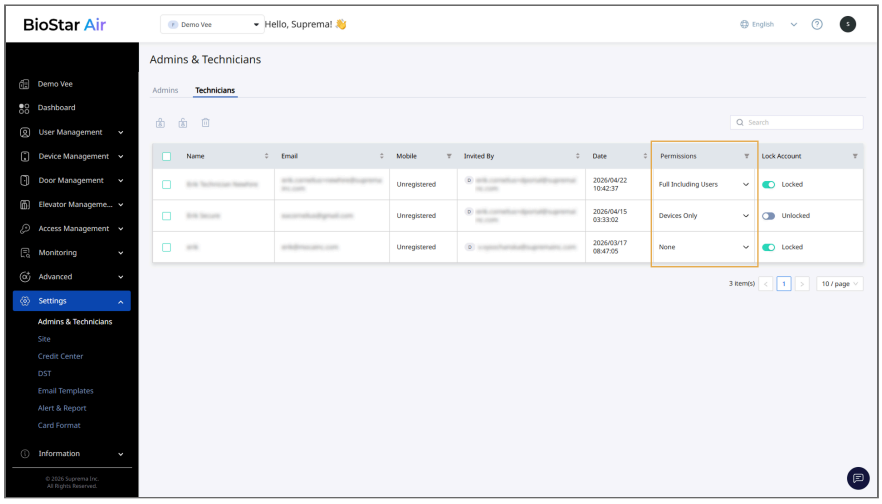
Habilitar la opción **Acceso de Técnico** cambia el menú **Ajustes** → **Administración** al menú **Administradores y técnicos**. Las pestañas **Administración** y **Técnicos** permiten administrar las cuentas de administrador y de técnico por separado.



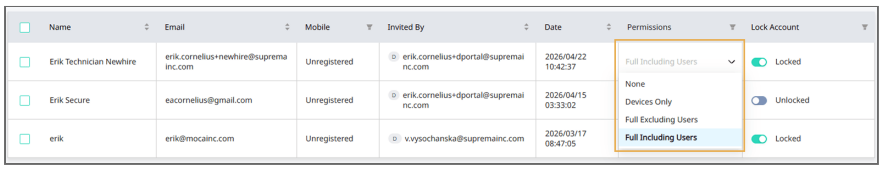
Cambiar permisos de técnicos

Sigue las instrucciones a continuación para cambiar los permisos de acceso de los técnicos invitados al sitio.

1. Haga clic en **Ajustes** → **Administradores y técnicos** en la barra lateral izquierda.
2. Haga clic en la pestaña **Técnicos**.
3. En la lista de técnicos, haz clic en la columna **Permisos** del técnico cuyos permisos de acceso quieres cambiar.



4. Selecciona el nivel de permiso deseado en el menú desplegable de acceso.



- : No puede iniciar sesión en el sitio.
- **Solo dispositivos**: Proporciona acceso solo a los menús **Panel de Control** y **Gestión de dispositivos**.
- **Completo excluyendo usuarios**: Proporciona acceso a todos los menús excepto **Gestión de usuarios**, pero el acceso a ciertas funciones de configuración está restringido.
- **Completo incluyendo usuarios**: Proporciona acceso a todos los menús, incluido **Gestión de usuarios**, pero el acceso a ciertas funciones de configuración está restringido.

5. Haz clic en **Sí** cuando aparezca la ventana de confirmación.

Los permisos de acceso del técnico se actualizan y aparece un mensaje de éxito en la parte superior de la pantalla.

> **Información**
>
> **Completo excluyendo usuarios** y **Completo incluyendo usuarios** tienen permiso de visualización pero no de edición para las siguientes rutas de menú.
>
> - **Ajustes** → **Administradores y técnicos**
> - **Ajustes** → **Sitio**

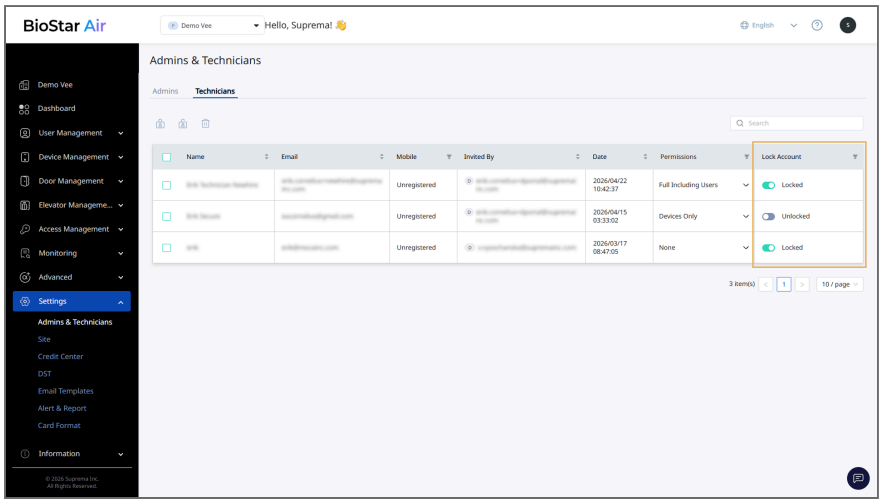
Bloquear o desbloquear cuentas de técnicos

Si ya no se necesita el soporte de un técnico o se debe restringir el acceso al sitio por razones de seguridad, bloquea la cuenta del técnico para impedir su acceso al sitio. Si necesitas el soporte del técnico de nuevo, desbloquea la cuenta para permitir su acceso al sitio.

Si bloqueas la cuenta de un técnico invitado, no podrá iniciar sesión en el sitio.

Bloquear o desbloquear la cuenta de un técnico individual

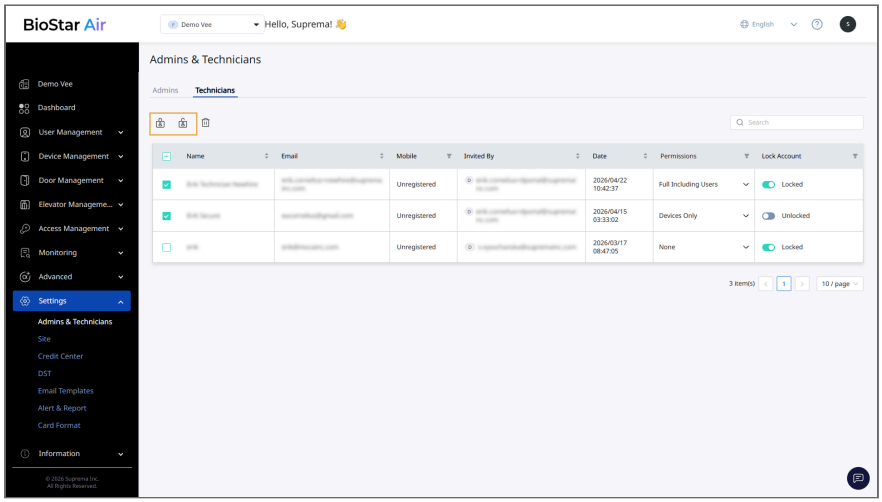
1. Haga clic en **Ajustes** → **Administradores y técnicos** en la barra lateral izquierda.
2. Haga clic en la pestaña **Técnicos**.
3. En la lista de técnicos, haz clic en el interruptor de la columna **Bloquear cuenta** del técnico cuya cuenta quieras bloquear o desbloquear.



4. Cuando aparezca un cuadro emergente, revisa el mensaje y haz clic en **Sí**.

Bloquear o desbloquear varias cuentas de técnicos

1. Haga clic en **Ajustes** → **Administradores y técnicos** en la barra lateral izquierda.
2. Haga clic en la pestaña **Técnicos**.
3. En la lista de técnicos, marca las casillas junto a los técnicos cuyas cuentas quieras bloquear o desbloquear. Selecciona 1 o más técnicos.
4. Haz clic en o en la parte superior de la lista de técnicos.



5. Cuando aparezca un cuadro emergente, revisa el mensaje y haz clic en **Sí**.

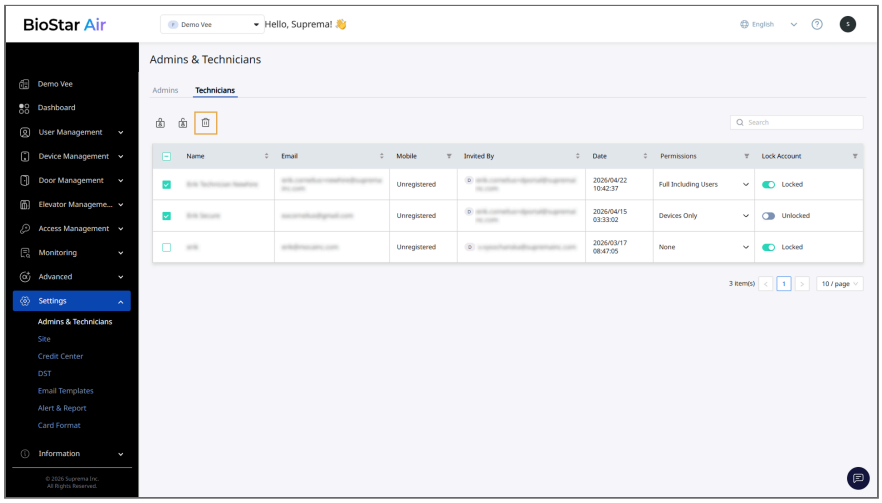
Las cuentas de los técnicos seleccionados se bloquean o desbloquean y aparece un mensaje de éxito en la parte superior de la pantalla.

> **Información**
>
> Si los técnicos seleccionados tienen estados de bloqueo mixtos, una acción masiva bloqueará o desbloqueará todas las cuentas.

Eliminar cuentas de técnicos

Eliminar la cuenta de un técnico invitado elimina por completo su acceso al sitio.

1. Haga clic en **Ajustes** → **Administradores y técnicos** en la barra lateral izquierda.
2. Haga clic en la pestaña **Técnicos**.
3. En la lista de técnicos, marca la casilla junto al técnico cuya cuenta quieras eliminar. Selecciona 1 o más técnicos.
4. Haz clic en en la parte superior de la lista de técnicos.



5. Cuando aparezca un cuadro emergente, revisa el mensaje y haz clic en **Sí**.

Después de eliminar las cuentas de los técnicos seleccionados, aparece un mensaje de éxito en la parte superior de la pantalla y esos técnicos ya no aparecen en la lista de técnicos.

Información

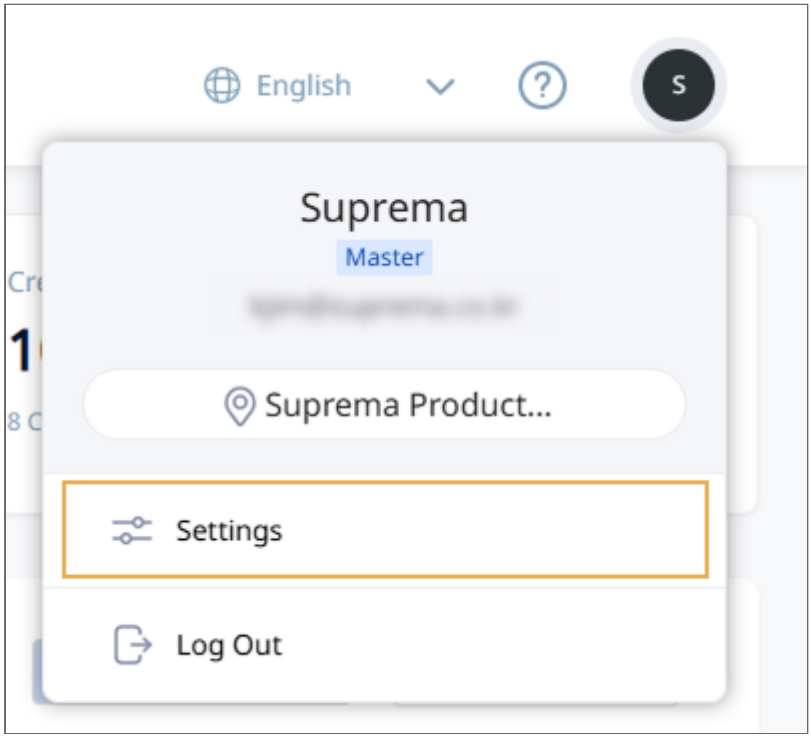
Una cuenta de técnico eliminada no se puede recuperar. Los técnicos que hayan sido removidos de un sitio pueden reasignarse a ese sitio a través del Partner Portal. Para más información sobre cómo asignar un técnico a un sitio en el Partner Portal, consulta Asignar técnicos a un sitio.

Configuración de la cuenta personal

Puede administrar los ajustes de su cuenta personal, por ejemplo cambiar la contraseña, configurar cómo recibe las alertas y ajustar la configuración del intercomunicador IP. También puede salir del sitio o eliminar su cuenta de forma permanente.

Acceda a los ajustes de la cuenta

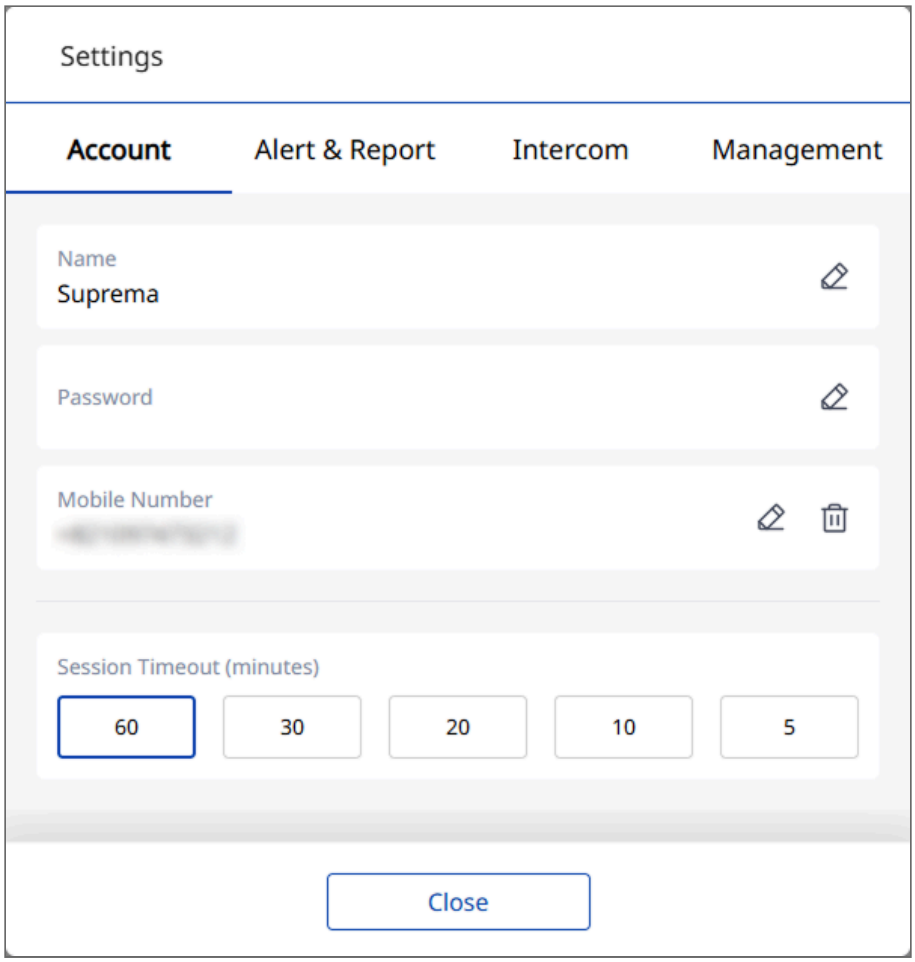
1. Inicia sesión en el portal de BioStar Air.
2. Haga clic en el icono de perfil de usuario en la parte superior derecha de la pantalla.
3. Haga clic en **Ajustes** en el menú desplegable.



4. Cuando aparezca la ventana **Ajustes**, configure las opciones deseadas.
   - **Cuenta**: Edite el nombre de usuario, la contraseña y el número de teléfono. Consulte Cambiar la información de la cuenta para más detalles.
   - **Alerta e informe**: Configure cómo se reciben las alertas. Consulte Configurar alertas para más detalles.
   - **Intercomunicador**: Administre la configuración del intercomunicador SIP. Consulte Configuración del intercomunicador para más detalles.
   - **Administrar**: Salga del sitio o elimine la cuenta. Consulte Salir del sitio o eliminar la cuenta para más detalles.

Cambiar la información de la cuenta

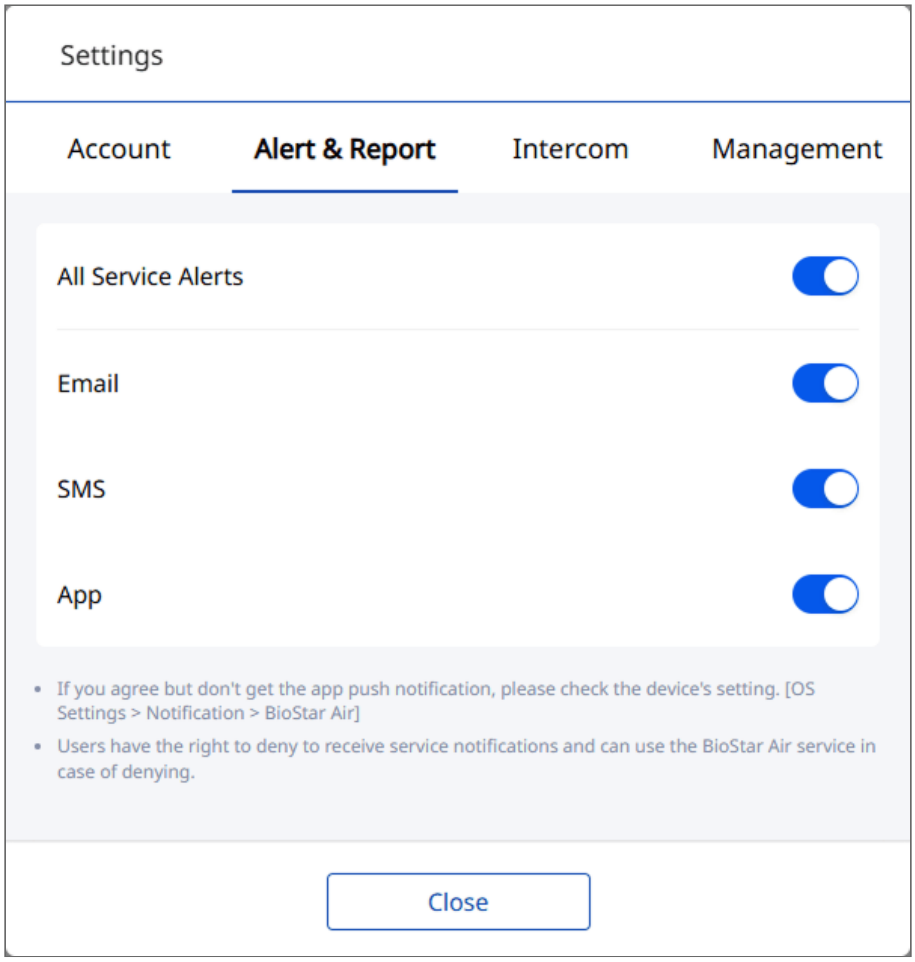
En la pestaña **Cuenta**, edite la información del usuario que ha iniciado sesión.



- Edite el nombre de usuario, la contraseña y el número de teléfono. Haga clic en para cada elemento.
- **Tiempo de espera de la sesión (minutos)**: Cierra sesión automáticamente cuando haya transcurrido el tiempo seleccionado. Seleccione el tiempo deseado.

Configurar alertas

En la pestaña **Alerta e informe**, configure cómo se reciben las alertas. Active la opción **Todas las alertas de servicio** para recibir todas las alertas. Desactive las alertas no deseadas individualmente.

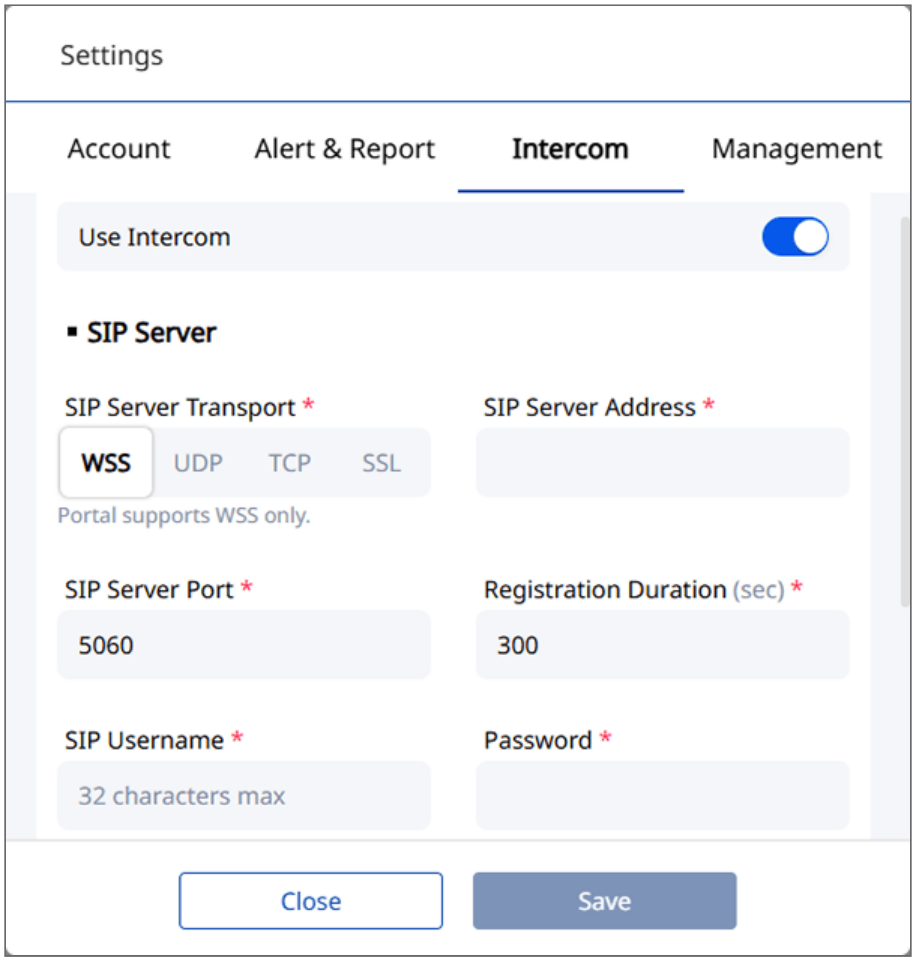


Información

- Si aceptó recibir alertas en la aplicación pero no aparecen, verifique la configuración del dispositivo móvil. Las alertas en la aplicación deben estar permitidas en dispositivos iOS o Android.
- Los usuarios pueden negarse a recibir alertas del servicio; hacerlo no restringe el uso del servicio.

Configuración del intercomunicador

En la pestaña **Intercomunicador**, administre la configuración del intercomunicador SIP.

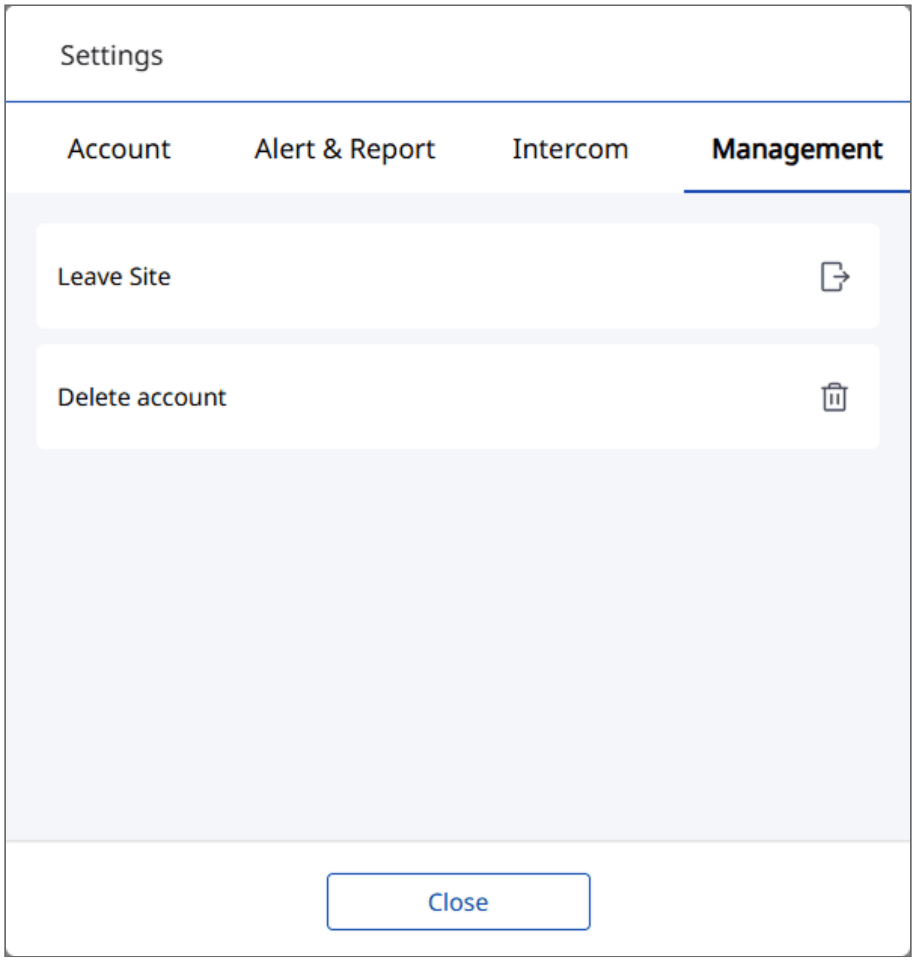


Información

Para obtener más información sobre la configuración del intercomunicador SIP, consulte Configurar el intercomunicador SIP en BioStation 3.

Salir del sitio o eliminar la cuenta

En la pestaña **Administrar**, sal del sitio o elimina la cuenta.



- **Abandonar el sitio**: Sal del sitio. Después de salir del sitio, tendrás que recibir una invitación del administrador del sitio para volver a unirte.
- **Borrar cuenta**: Elimina la cuenta de forma permanente. Al eliminarla, se borran de forma irreversible todos los datos personales y la configuración, y no se podrán recuperar.

Configurar SSO Y SCIM

Muchas organizaciones ya administran el acceso al sistema interno con Microsoft Entra ID u Okta, sin importar el tamaño de la empresa. BioStar Air se integra con estos proveedores para administrar cuentas de administrador y usuarios con credenciales desde una sola fuente.

SSO (inicio de sesión único) aplica las políticas de la organización al acceso a BioStar Air y mejora la seguridad. SCIM (gestión de identidades entre dominios) crea y elimina cuentas de usuario y reduce riesgos por cuentas activas sin acceso. Esto reduce el trabajo repetitivo de crear, editar y eliminar usuarios, grupos de usuarios y cuentas de administrador.

En la barra lateral izquierda, haz clic en **Ajustes** → **Sitio**. En la pestaña **SSO & SCIM**, selecciona la política de inicio de sesión y el proveedor de ID, y configúralos. Para los ajustes básicos, consulta Habilitar SSO y SCIM.

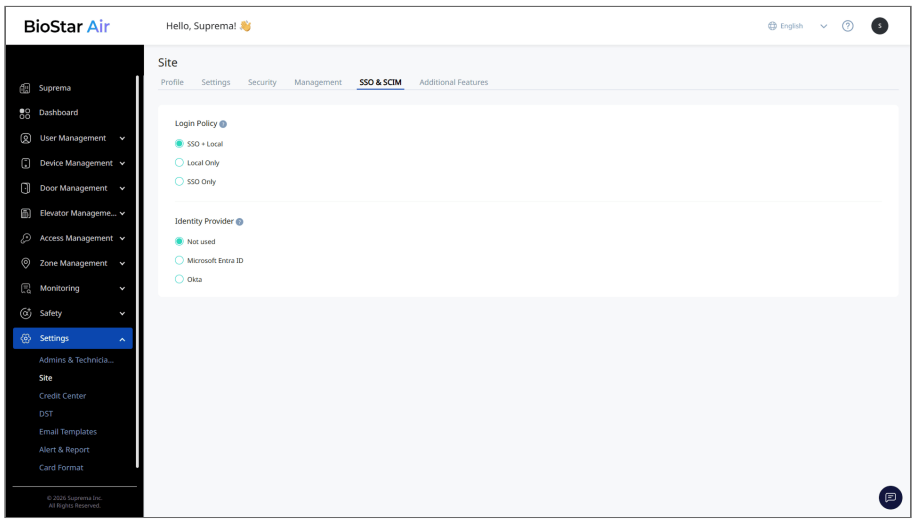
BioStar Air admite el aprovisionamiento de administradores del sitio y usuarios con credenciales mediante **Microsoft Entra ID** u **Okta**. Si usa uno de estos proveedores de identidad, use los siguientes documentos para configurar SSO y SCIM en los sitios de BioStar Air.

Requisitos mínimos

- Licencia de SSO y SCIM de BioStar Air
- Suscripción activa a Microsoft Entra AD u Okta
- Capacidad para crear nuevas aplicaciones en el IdP
- Capacidad para crear, sincronizar y asignar grupos en el IdP
- Gestione los permisos en BioStar Air

Habilitar SSO y SCIM

Haz clic en **Ajustes** → **Sitio** en la barra lateral izquierda. En la pestaña **SSO & SCIM**, seleccione la política de inicio de sesión y el proveedor de ID, o bórrelos.



Precaución

Antes de cambiar los ajustes del proveedor de ID, mantenga al menos una cuenta de administrador maestro que pueda iniciar sesión localmente. De lo contrario, los problemas de integración del proveedor de identidad pueden impedir que los administradores accedan al sitio.

Información

- Solo el administrador maestro del sitio puede administrar los ajustes de SSO y SCIM.
- Los usuarios con credenciales no inician sesión en BioStar Air; los ajustes de SSO y SCIM no los afectan.
- El Partner Portal no está incluido en el alcance de los ajustes de SSO y SCIM.

Política de inicio de sesión

En **Política de inicio de sesión**, defina cómo inician sesión los administradores de BioStar Air.

- **SSO**: Los administradores se autentican mediante un proveedor de identidad.

- **Local**: Los administradores se autentican con la dirección de correo electrónico y la contraseña definidas en BioStar Air.

Seleccione una de las tres opciones siguientes.

- **SSO + Local**: Permite el inicio de sesión con SSO y el inicio de sesión local.
- **Solo local**: Permite solo el inicio de sesión local.
- **Solo SSO**: Permite solo el inicio de sesión con SSO.

Ajustes de integración del proveedor de identidad

En **Proveedor de identidad**, seleccione un proveedor de ID externo para las cuentas de administrador de BioStar Air. Un sitio solo puede tener un proveedor de identidad activo a la vez.

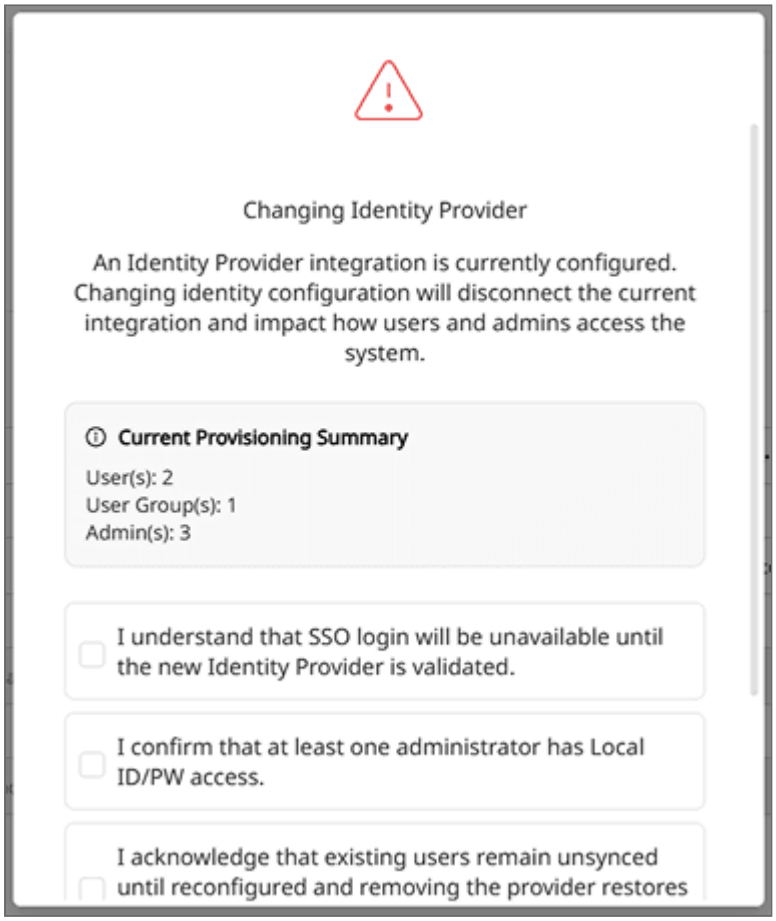
- **No utilizado**
- **Microsoft Entra ID**: Configurar La Integración De Microsoft Entra ID
- **Okta**: Configurar Integración con Okta

> **Información**
> Para cambiar el proveedor de ID conectado, seleccione **No utilizado** para desconectar y, luego, seleccione un nuevo proveedor de ID. Sin desconectarse, el sitio no puede cambiar directamente a otro proveedor de ID.

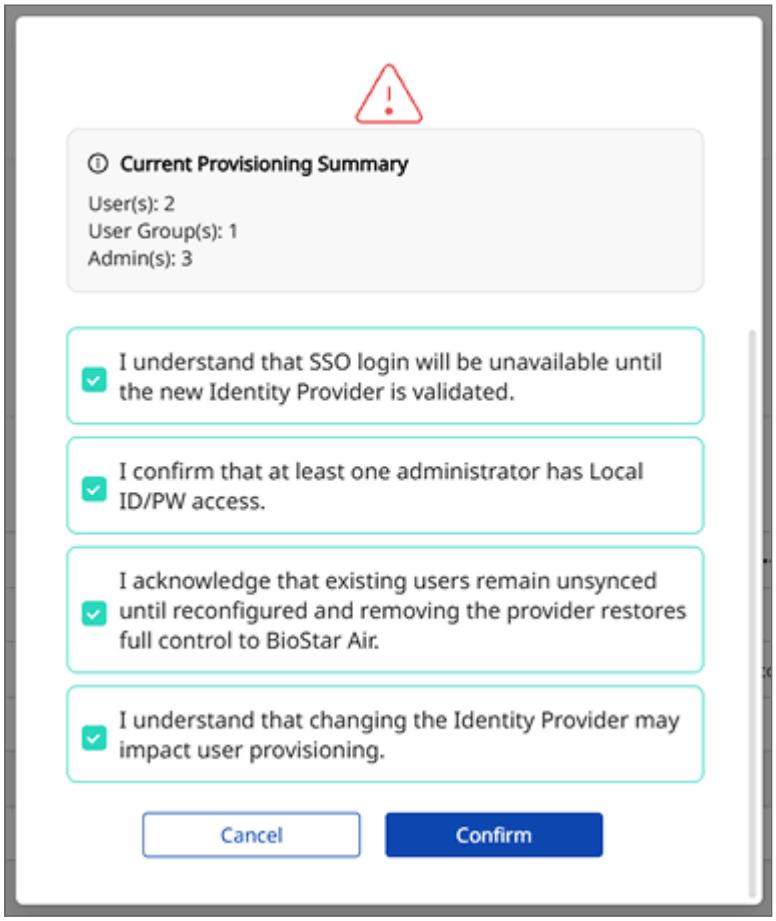
Desactivar ajustes de SSO y SCIM

Desactive la integración del proveedor de ID.

1. Seleccione **No utilizado** en la sección **Proveedor de identidad**.
2. Revise el mensaje en la ventana emergente de advertencia.



3. Revise el impacto del cambio de ajuste y marque la casilla de verificación.



4. Haga clic en **Confirmar**.

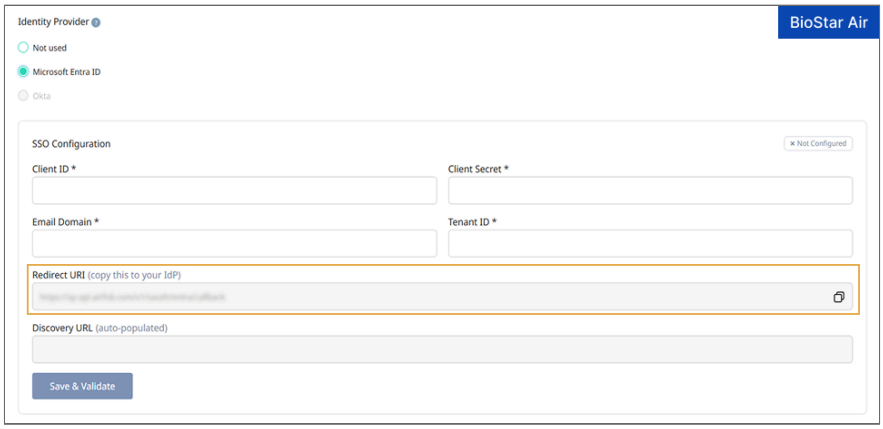
Configurar La Integración De Microsoft Entra ID

Para iniciar sesión en BioStar Air con Microsoft Entra ID, un administrador de Entra ID crea un registro de aplicación en Entra ID. Luego, el administrador lo vincula a los ajustes de SSO de BioStar Air.

Conectar SSO de Entra ID

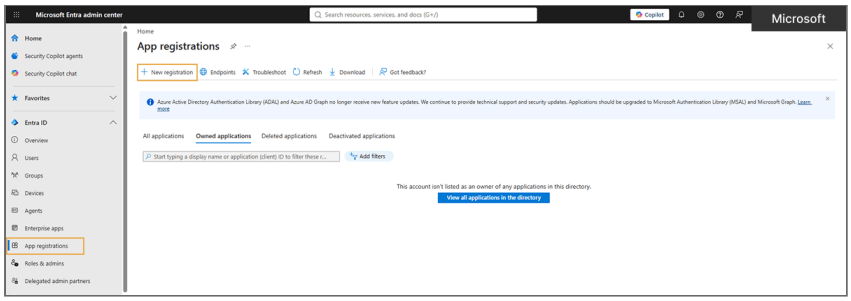
1 BioStar Air: Preparar URI de redirección

1. Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda de BioStar Air.
2. Haga clic en la pestaña **SSO & SCIM**.
3. En **Proveedor de identidad**, selecciona **Microsoft Entra ID**.
4. Copie el valor de URI que aparece en el campo **URI de redirección**.



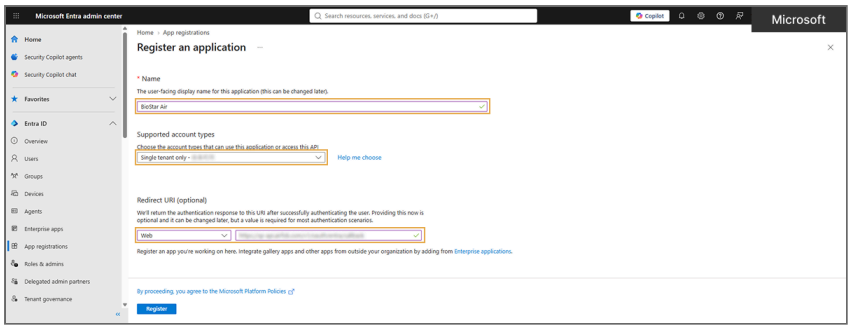
2 Centro de administración de Microsoft Entra: registrar aplicación

1. Inicia sesión en el Centro de administración de Microsoft Entra.
2. Ve a **Entra ID** → **App registrations**.
3. Haz clic en **New registration**.



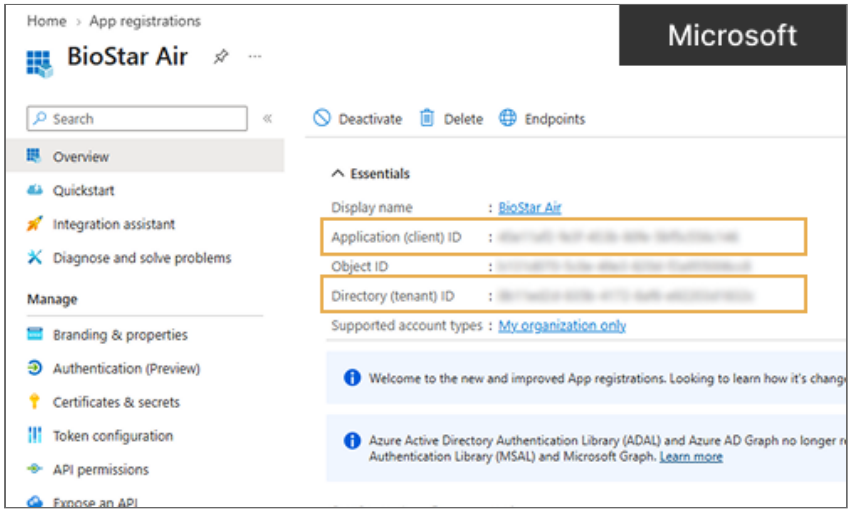
4. Ingresa 'BioStar Air' como nombre de la aplicación.
5. En **Supported account types**, selecciona **Single tenant only**.

6. En **Redirect URI**, selecciona **Web**. Pega el URI del paso BioStar Air: Preparar URI de redirección en el campo.



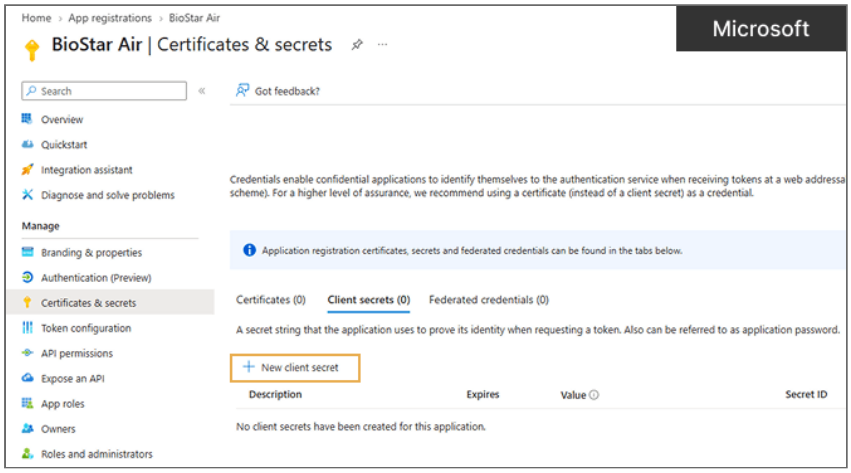
7. Haz clic en **Register**.

8. En **Overview** de la aplicación BioStar Air, copia los siguientes valores.

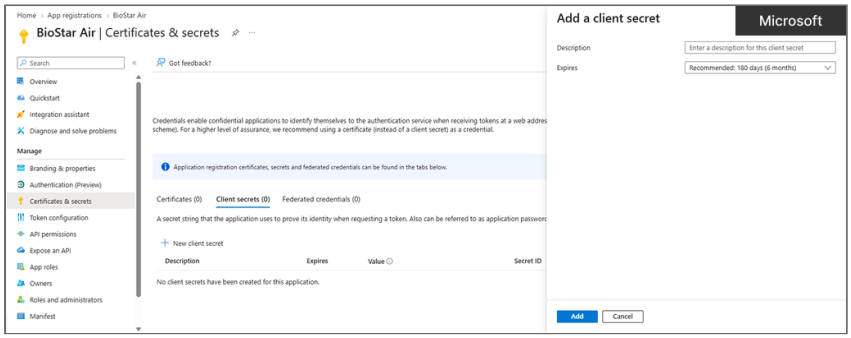


- **Application (client) ID**
- **Directory (tenant) ID**

9. En **Certificates & secrets** → **Client secrets**, haz clic en **New client secret**.

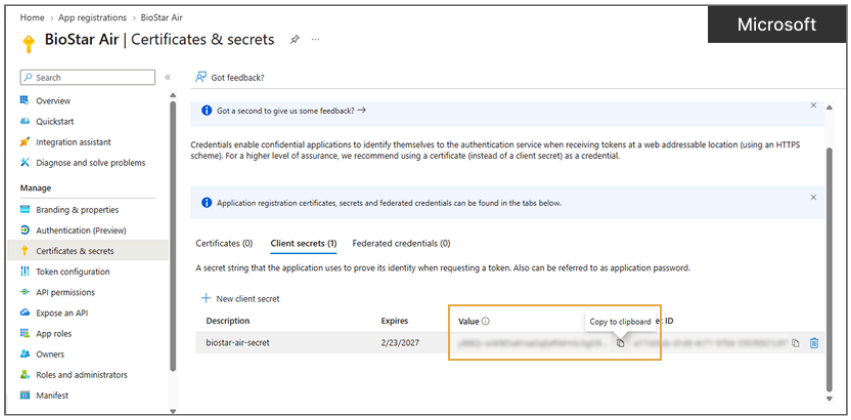


10. Ingresa una descripción y selecciona un período de expiración.



11. Haz clic en **Agregar**.

12. Copia el **Value** del secreto de cliente generado.



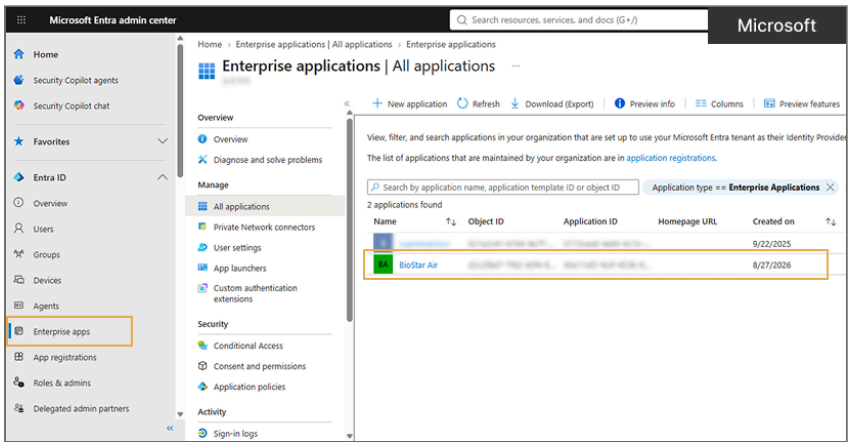
En el siguiente paso, ingresa el **Application (client) ID**, el **Directory (tenant) ID** y el **Value** copiados.

> **Precaución**
> Usa **Value**, no **Secret ID**. El **Value** aparece una sola vez, así que cópialo ahora.

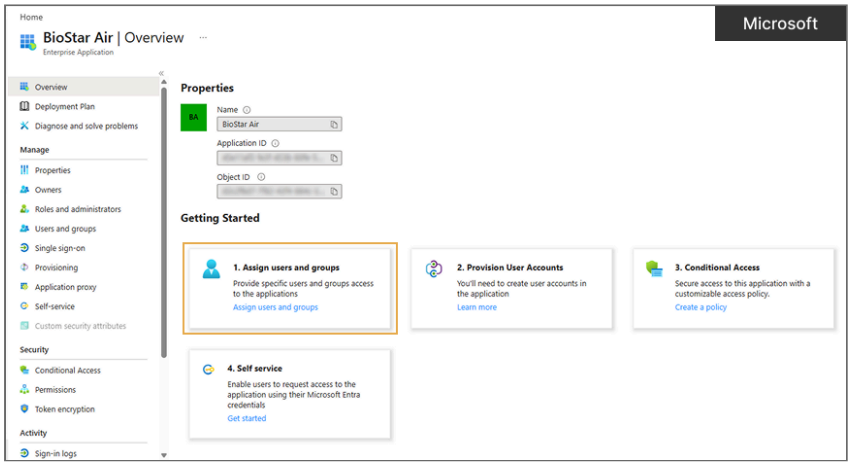
3 Centro de administración de Microsoft Entra: asignar usuarios y grupos

Crea usuarios y grupos antes de asignarlos.

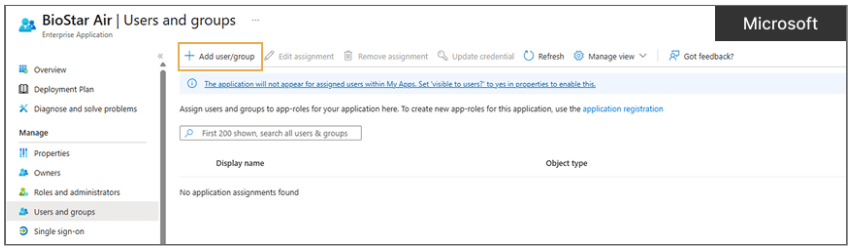
1. En **Enterprise apps**, haz clic en la aplicación creada antes (BioStar Air).



2. Haz clic en **Assign users and groups**.



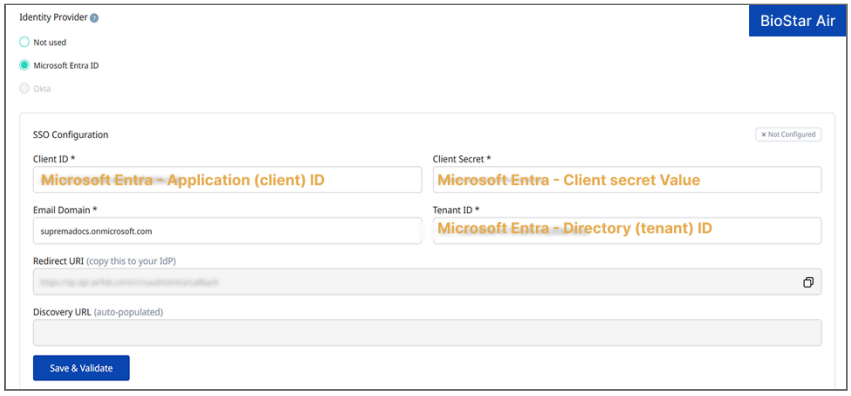
3. Haz clic en **Add user/group** para asignar usuarios y grupos.



4. Después de asignar usuarios y grupos, haz clic en **Assign**.

4 BioStar Air: Configurar SSO

1. Vuelve a la pantalla de configuración de BioStar Air e ingresa en cada campo los valores copiados en Centro de administración de Microsoft Entra: registrar aplicación.

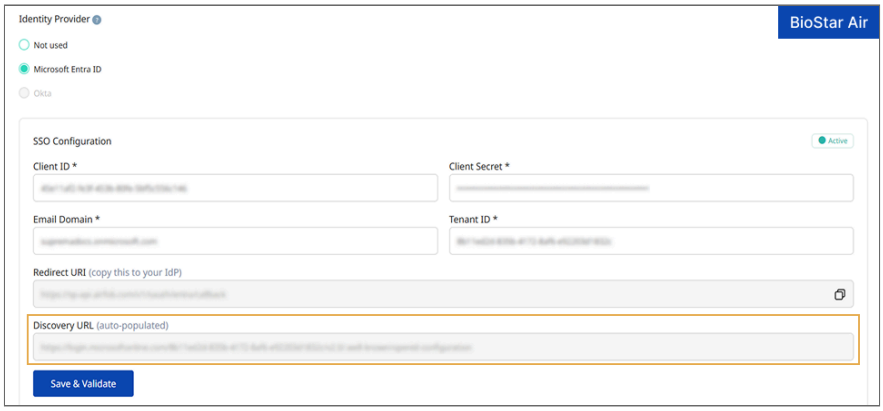


- **ID de cliente**: Application (client) ID
- **Secreto de cliente**: Value
- **ID de inquilino**: Directory (tenant) ID

2. En el campo **Dominio de correo electrónico**, escribe el dominio de correo electrónico de la organización.

3. Haz clic en **Guardar y Validar**.

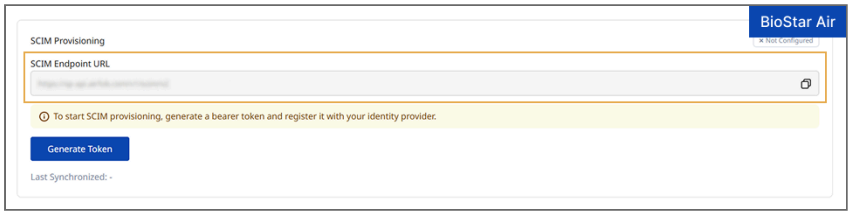
Cuando el sistema guarda y verifica correctamente, genera automáticamente el valor de **URL de descubrimiento**.



Conectar el aprovisionamiento SCIM de Entra ID

1 BioStar Air: Copiar el token SCIM

1. Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda de BioStar Air.
2. Haga clic en la pestaña **SSO & SCIM**.
3. En la sección **Aprovisionamiento SCIM**, copie el valor de **URL del endpoint SCIM**.

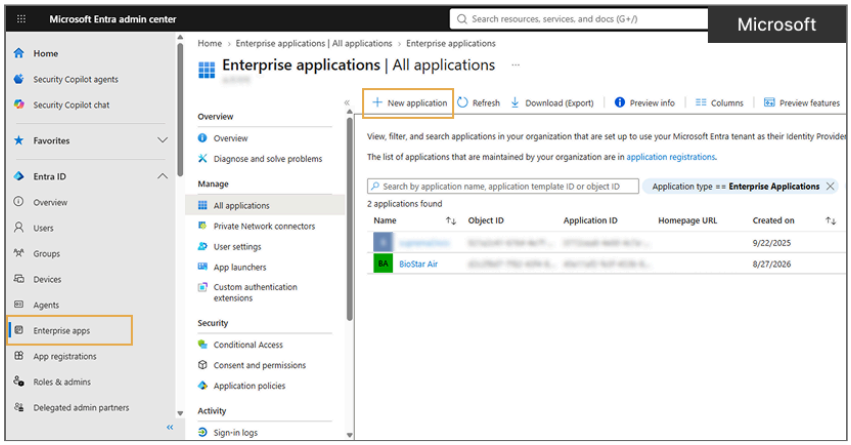


4. Haga clic en **Generar token**.
5. En el cuadro de diálogo Generación de token completada, copie el token.

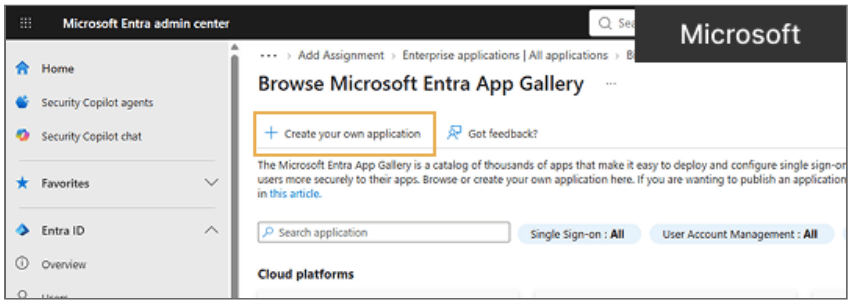
> **Información**
>
> - Copie el token generado de inmediato. Copie el token solo al generarlo. Después de cerrar el cuadro de diálogo, el sistema no permite copiar el token de nuevo.
> - Si pierde el token, haga clic en **Rotar token** para generar un nuevo token. Ingrese el nuevo token nuevamente en el proveedor de identidad.
> - En el siguiente paso, ingrese la URL del extremo de SCIM y el token copiado en este paso.

2 Centro de administración de Microsoft Entra: crear una aplicación de aprovisionamiento SCIM

1. En **Enterprise apps**, haz clic en **New application**.

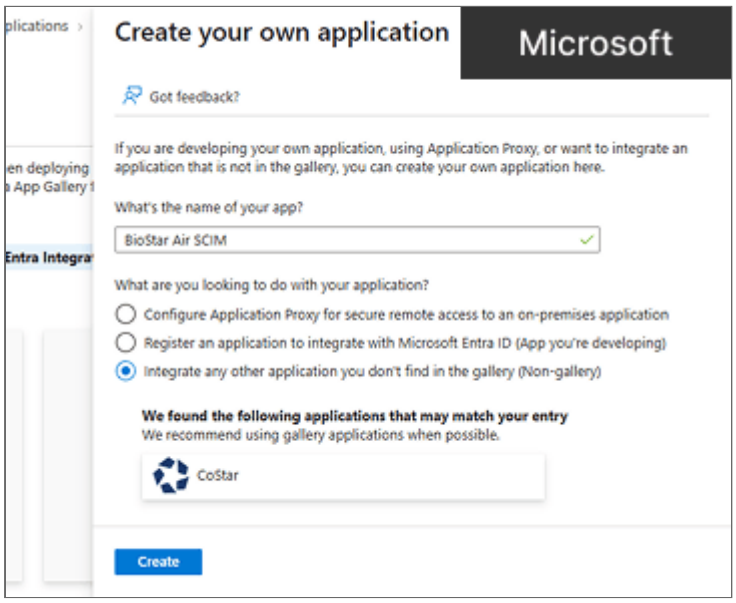


2. Haz clic en **Create your own application**.



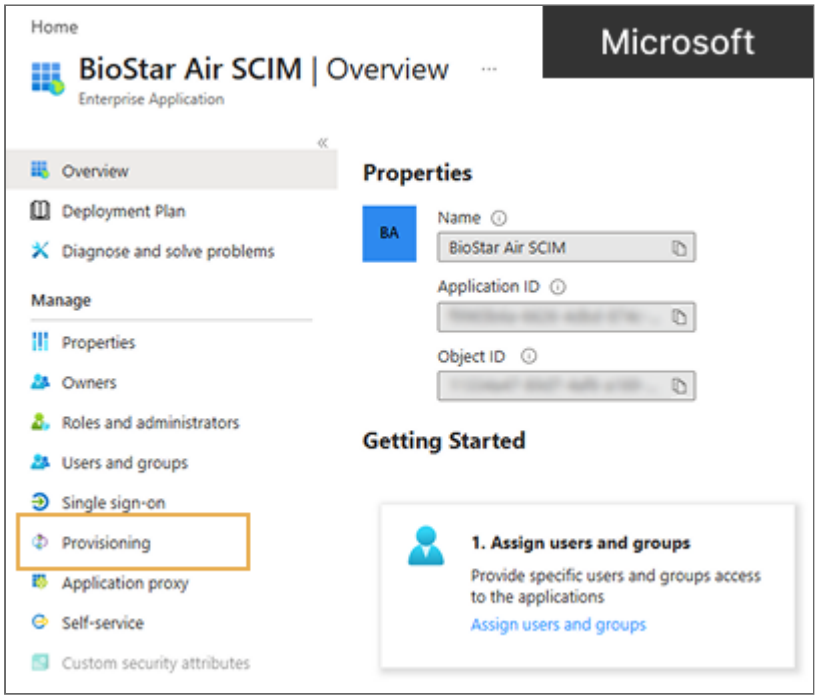
3. Ingresa el nombre de la aplicación como 'BioStar Air SCIM'.

4. Selecciona **Integrate any other application you don't find in the gallery (Non-gallery)**.



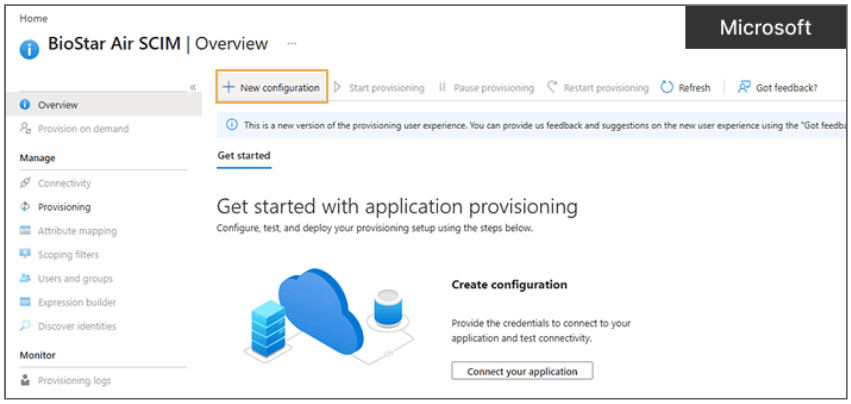
5. Haz clic en **Create**.

6. En la aplicación BioStar Air SCIM, haz clic en **Manage** → **Provisioning**.

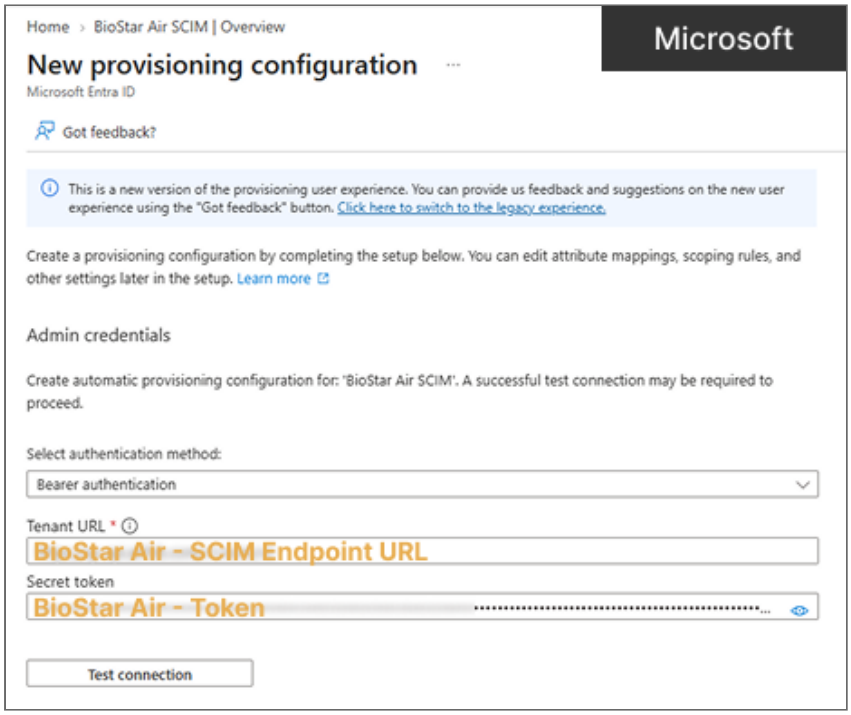


3 Centro de administración de Microsoft Entra: establecer credenciales de administrador e iniciar el aprovisionamiento

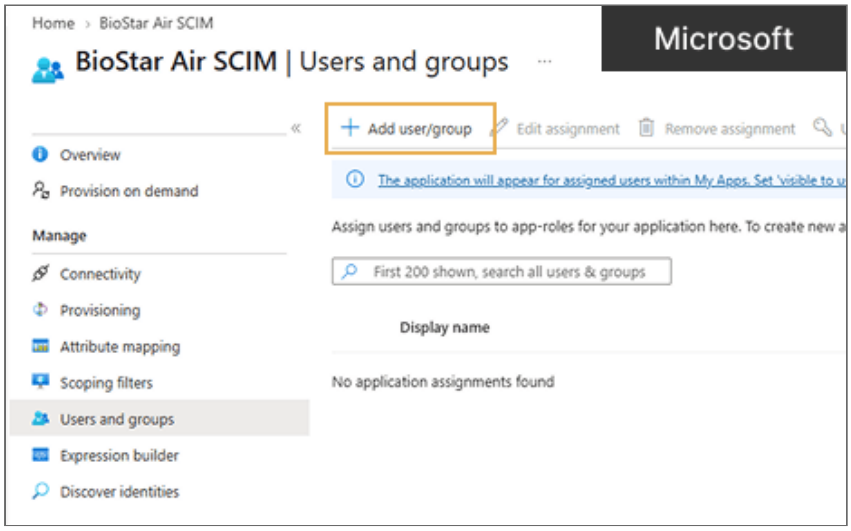
1. Haz clic en **New Configuration**.



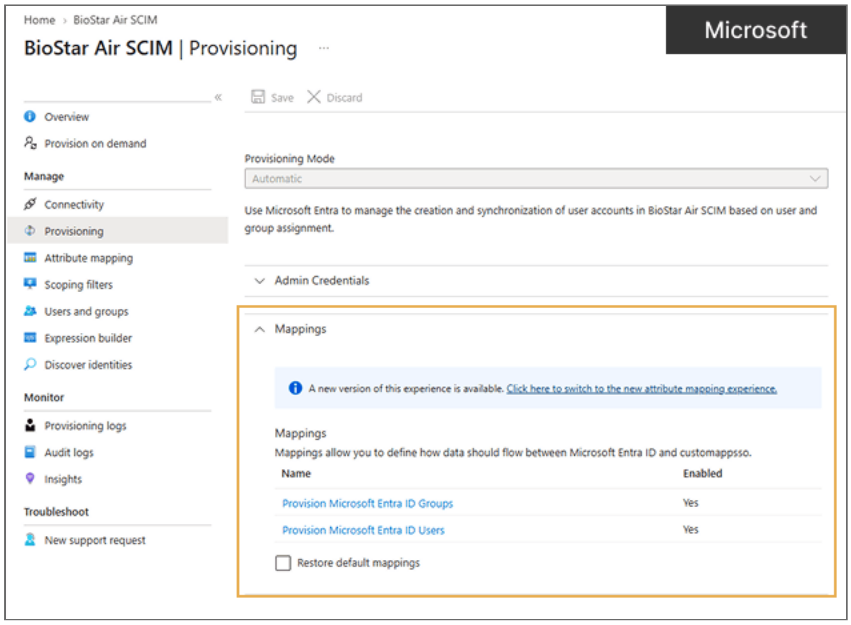
2. En **Admin credentials**, pega la URL del punto de conexión de SCIM y el token copiados en BioStar Air: Copiar el token SCIM en **Tenant URL** y **Secret token**.



3. Haz clic en **Test Connection** para probar la sincronización.
4. Haz clic en **Create**.
5. En **Users and groups**, haz clic en **Add user/group**.

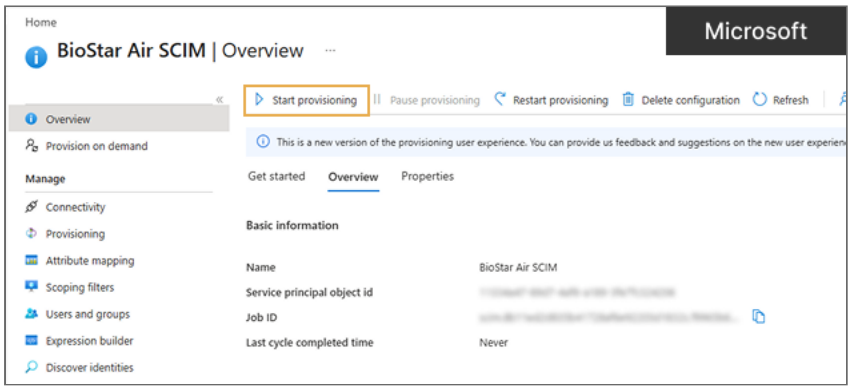


6. Asigna los usuarios y los grupos de seguridad que se aprovisionarán.
7. Haz clic en **Assign**.
8. Ve a **Provisioning** → **Mappings** y confirma que la sincronización de usuarios y grupos está habilitada.



9. Revisa las asignaciones antes de cambiar atributos.

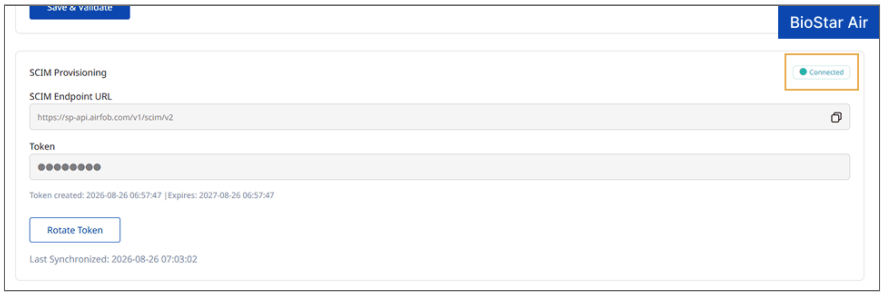
10. En **Overview** de la aplicación SCIM, haz clic en **Start provisioning**.



> **Información**
>
> Recomendamos empezar con un grupo de prueba pequeño. BioStar Air puede tardar hasta 40 minutos en reflejar cambios en la pertenencia al grupo.

4 BioStar Air: Compruebe la conexión

1. Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda de BioStar Air.
2. Haga clic en la pestaña **SSO & SCIM**.
3. En la sección **Aprovisionamiento SCIM**, verifique que aparezca el indicador **Conectado**.



Asignación de grupos

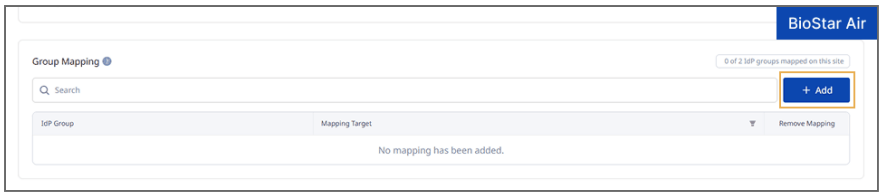
Después de conectar SSO y SCIM y enviar los grupos del IdP, el administrador del sitio debe asignarlos a grupos de BioStar Air.

Reglas de asignación

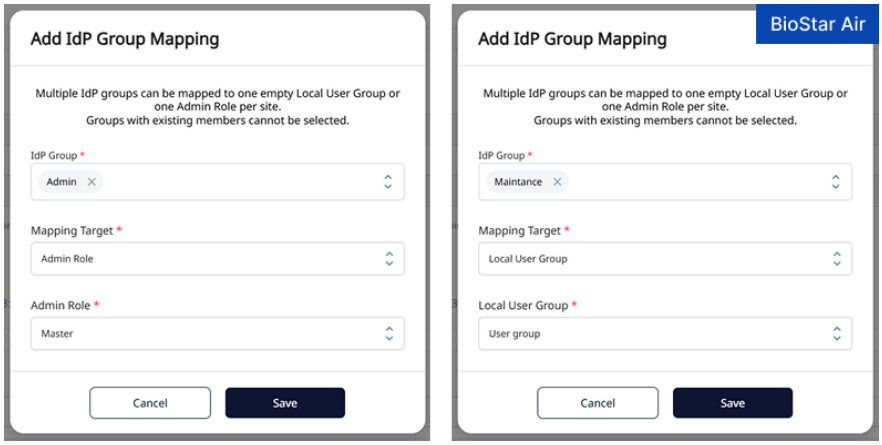
- Puede asignar varios grupos de IdP a un solo grupo de usuarios de BioStar Air.
- Un grupo de usuarios de BioStar Air debe estar vacío antes de la asignación.
- Los grupos de BioStar Air con miembros no pueden ser destinos de asignación.
- Solo el administrador maestro del sitio puede gestionar la asignación de grupos del IdP.
- El sistema bloquea el rol después de asignar un grupo del IdP al rol maestro.

Asignar roles de administrador y grupos de usuarios

1. Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda de BioStar Air.
2. Haga clic en la pestaña **SSO & SCIM**.
3. Vaya a la sección **Asignación de grupos** y haga clic en **Agregar**.

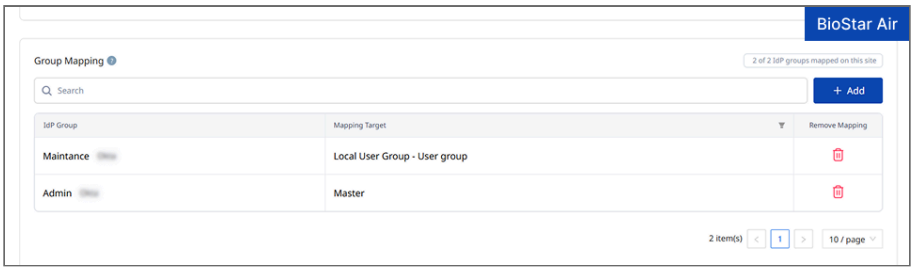


4. En **Grupo de IdP**, seleccione un grupo de IdP.
5. En **Destino de la asignación**, seleccione **Rol de administrador** o **Grupo de usuarios local** según el grupo de IdP seleccionado.
6. Según el destino de asignación, asigne un rol de administrador o seleccione un grupo de usuarios.



7. Haga clic en **Guardar** para guardar la asignación.

La sección **Asignación de grupos** muestra los grupos del IdP y los grupos de BioStar Air asignados.



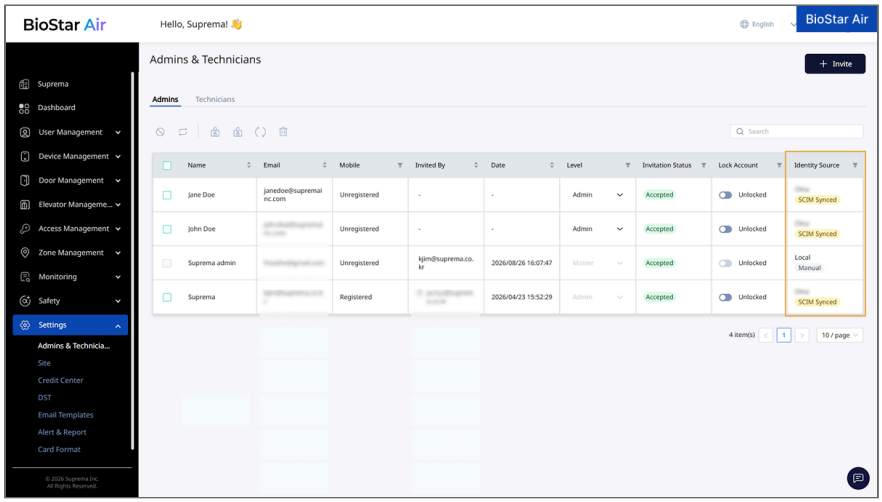
Información

- Para obtener más información sobre los roles de administrador, consulte Administrar cuentas y roles de administradores.
- Para obtener más información sobre los grupos de usuarios, consulte Administrar Grupos de Usuarios.

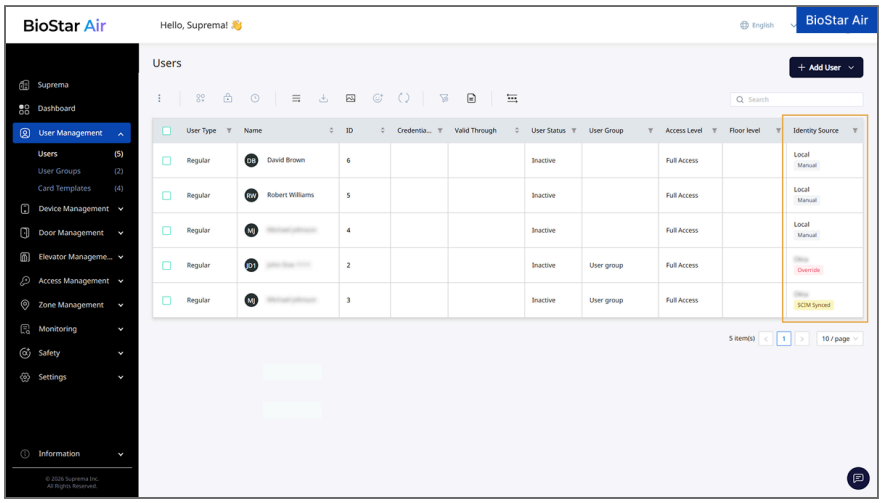
Administrar administradores, usuarios y grupos sincronizados

Con aprovisionamiento habilitado, BioStar Air indica si cada administrador, usuario y grupo es local o proviene del proveedor de identidad.

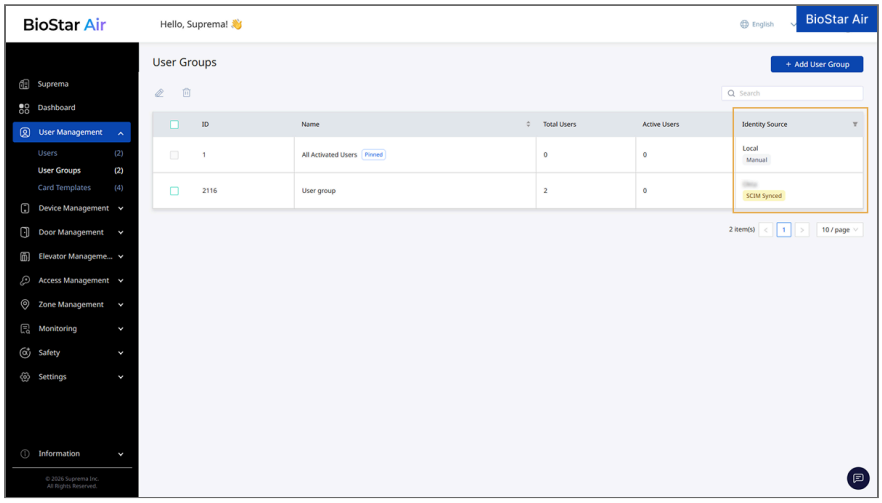
- En **Ajustes** → **Administradores y técnicos**, revise la columna **Fuente de identidad** en la lista de administradores.



- En **Gestión de usuarios** → **Usuarios**, revise la columna **Fuente de identidad** en la lista de usuarios.

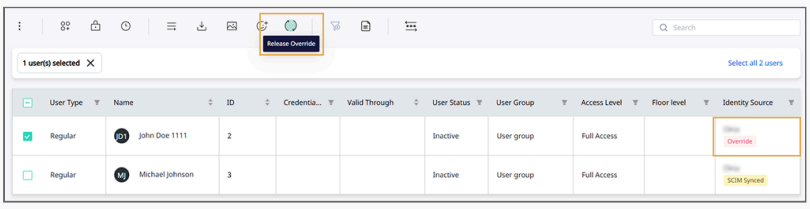


- En **Gestión de usuarios** → **Grupos de Usuarios**, revise la columna **Fuente de identidad** en la lista de grupos de usuarios.



Cómo funcionan las entradas sincronizadas con SCIM

- Los usuarios y administradores creados manualmente siguen gestionándose manualmente.
- BioStar Air evita la eliminación manual de entradas sincronizadas con SCIM.
- BioStar Air evita agregar o quitar manualmente usuarios de grupos sincronizados con SCIM.
- Cambiar manualmente una entrada sincronizada de forma local establece el estado en **Anulación**. Ejecute **Liberar anulación** para cancelar los cambios locales y devolver el registro a la administración de SCIM.

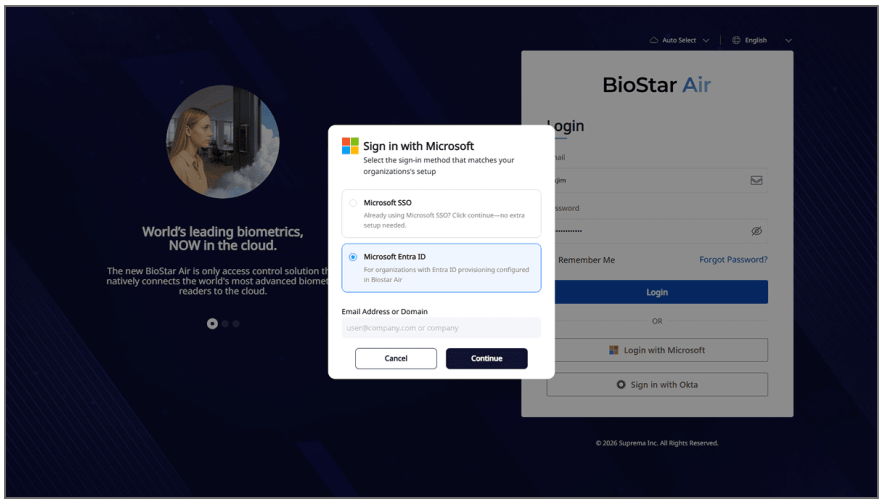


Iniciar sesión con Entra ID

Después de conectar SSO de Entra ID, los usuarios inician sesión en BioStar Air con una cuenta Microsoft.

1. En la pantalla de inicio de sesión de BioStar Air, haga clic en **Iniciar sesión con Microsoft**.

2. Selecciona **Microsoft Entra ID**.



> Si su organización ya usa SSO de Microsoft, seleccione **Microsoft SSO** para iniciar sesión sin ajustes adicionales.

3. Ingresa la dirección de correo electrónico o el dominio de la organización en el campo **Dirección de correo electrónico o dominio**. (Por ejemplo, `user@company.com` o `company`)
4. Haz clic en **Continuar**.
5. En la pantalla de inicio de sesión de Microsoft Entra ID, ingrese el correo y la contraseña de su organización.
6. Después de completar la autenticación, el sistema te redirige automáticamente a BioStar Air y finaliza el inicio de sesión.

> **Información**
> Aparece un mensaje de error si el dominio del correo ingresado no tiene SSO de Entra ID. Comuníquese con el administrador del sitio.

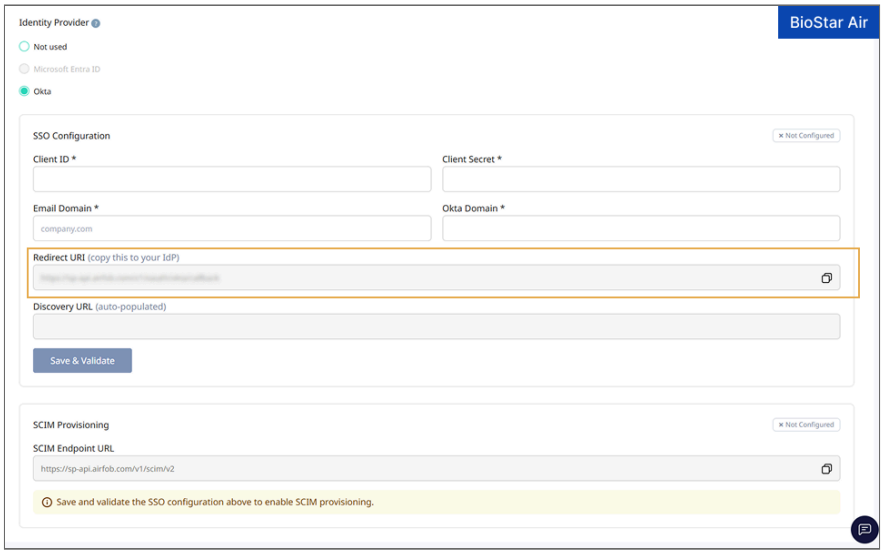
Configurar Integración con Okta

Para iniciar sesión en BioStar Air con Okta, el administrador de identidades debe crear una aplicación OIDC en Okta. Vincúlelo con los ajustes de SSO en BioStar Air.

Conectar SSO de Okta

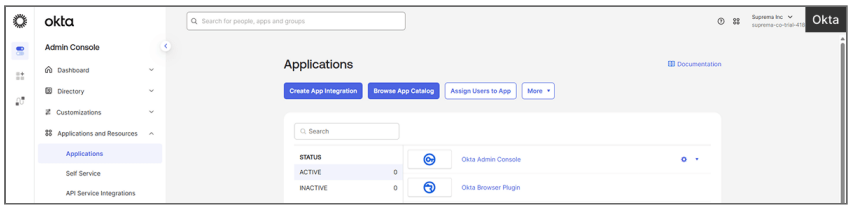
1 BioStar Air: Preparar URI de redirección

1. Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda de BioStar Air.
2. Haga clic en la pestaña **SSO & SCIM**.
3. Seleccione **Okta** en **Proveedor de identidad**.
4. Copie el valor de URI que aparece en el campo **URI de redirección**.

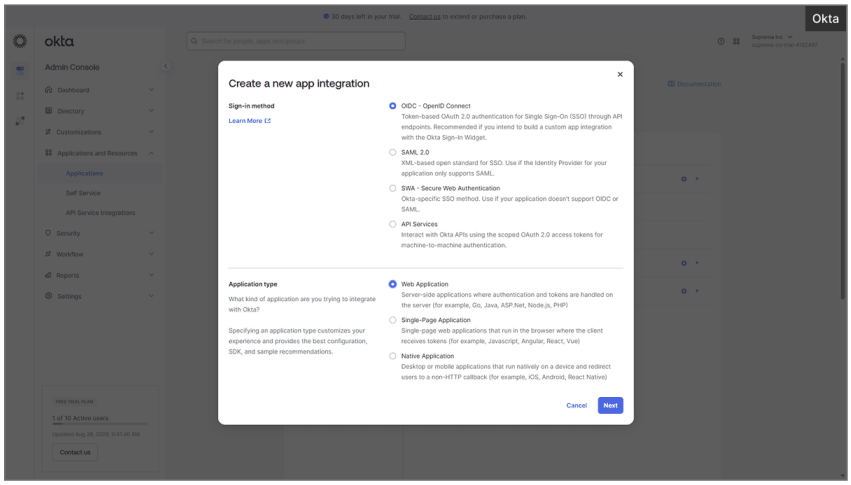


2 Okta: Crear una aplicación

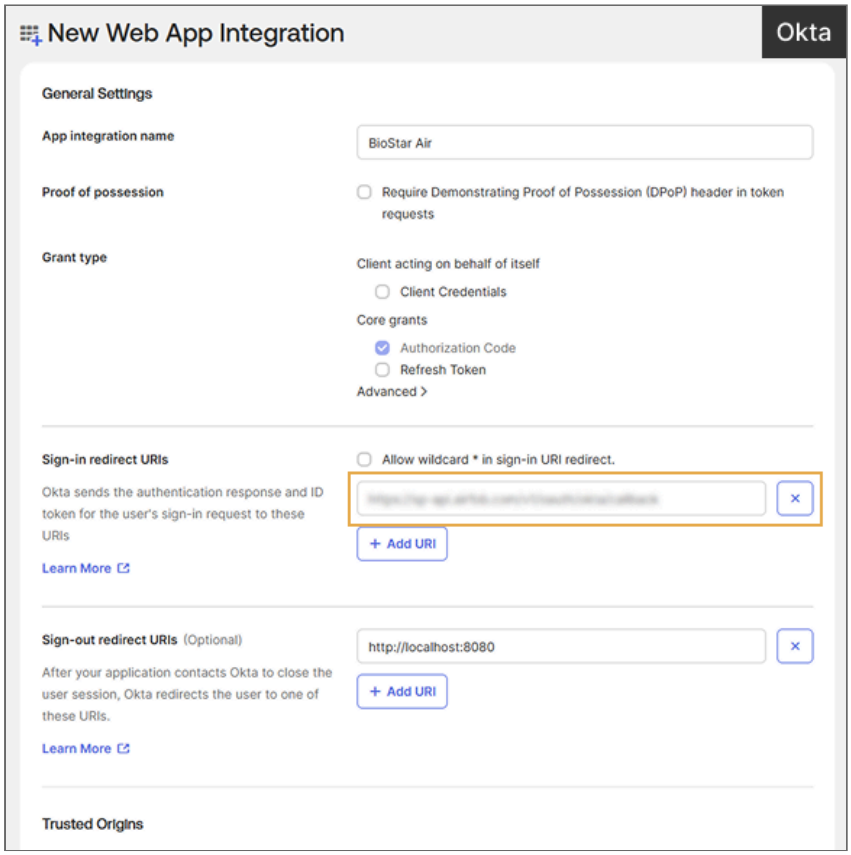
1. Inicie sesión en la **Okta Admin Console**.
2. Vaya a **Applications and Resources → Applications**.



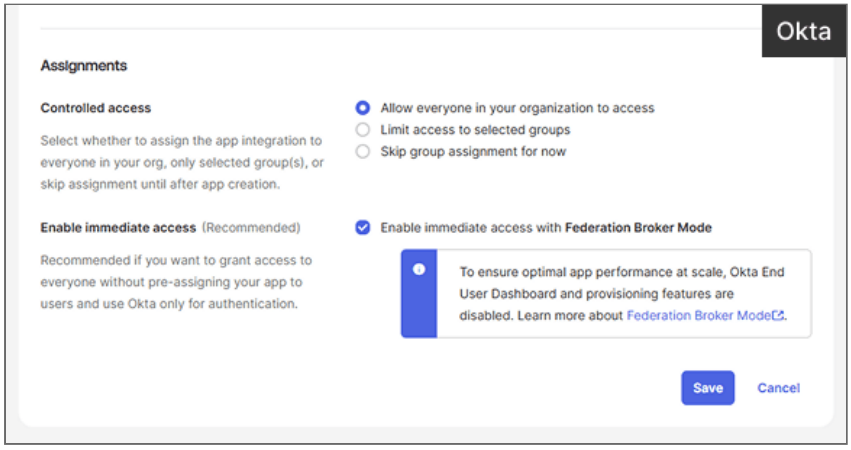
3. Haga clic en **Create App Integration**.
4. En **Sign-in method**, seleccione **OIDC - OpenID Connect**.
5. En **Application type**, selecciona **Web Application** para obtener un secreto de cliente.



6. Haga clic en **Next**.
7. En **App Integration name**, ingrese 'BioStar Air'.
8. Pegue el URI del paso BioStar Air: Preparar URI de redirección en el campo **Sign-in redirect URIs**.



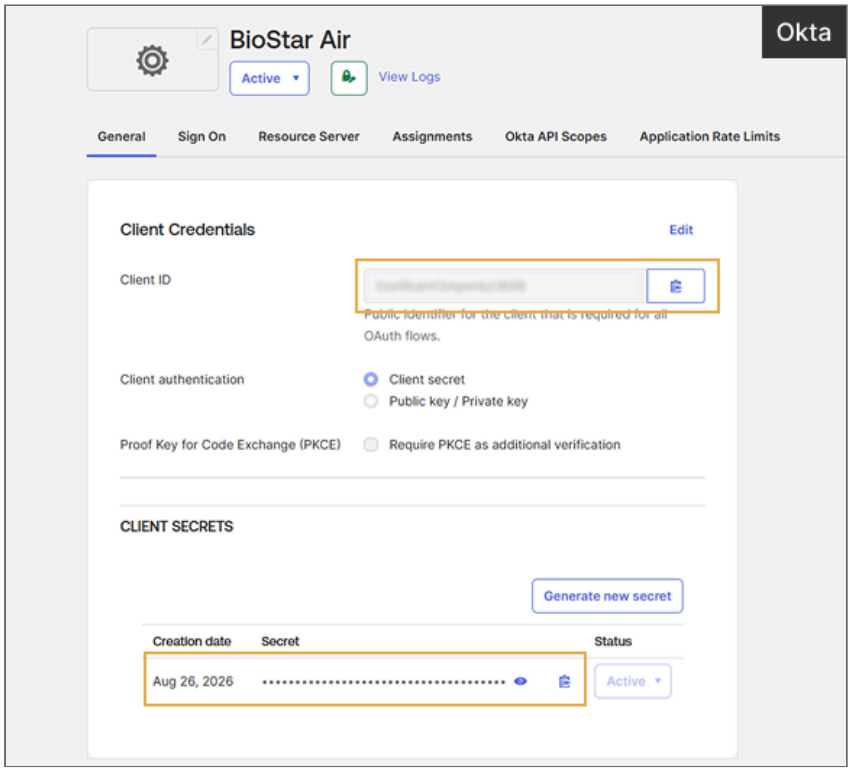
9. Vaya a **Assignments** y seleccione **Allow everyone in your organization to access**.



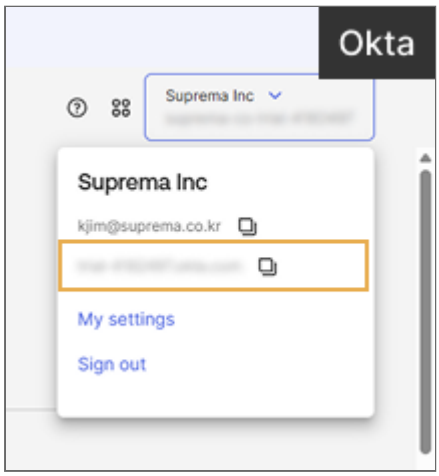
10. Haga clic en **Save**.

3 Okta: Copiar información del cliente de la aplicación

1. Después de crear la aplicación, copie **Client ID** y **Client Secret** desde la pestaña **General**.



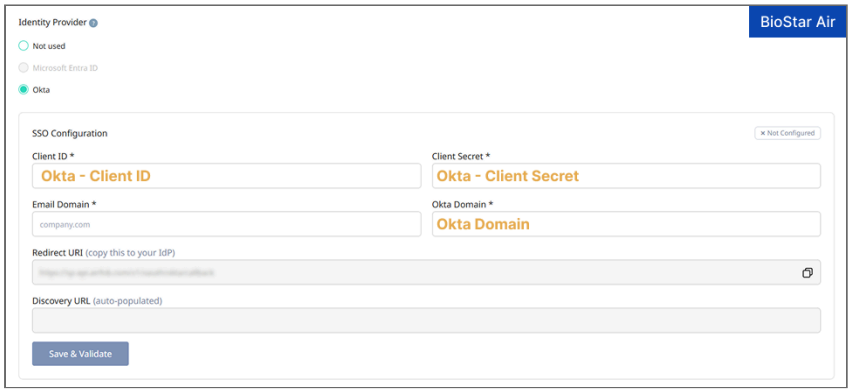
2. Haga clic en el perfil en la esquina superior derecha y copie **Okta Domain**.



Ingrese el **Client ID**, el **Client Secret** y el **Okta Domain** copiados en el siguiente paso.

4 BioStar Air: Configurar SSO

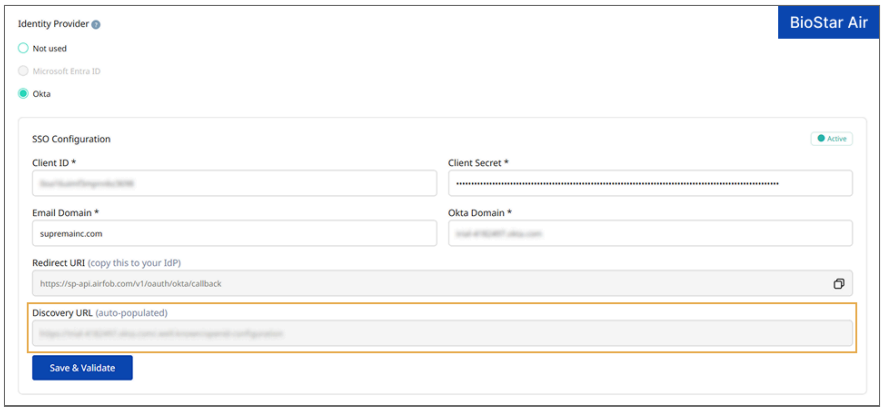
1. Vuelve a la página de ajustes de BioStar Air y escribe en cada campo los valores copiados en el paso Okta: Copiar información del cliente de la aplicación.



- **ID de cliente**: Client ID
- **Secreto de cliente**: Client Secret
- **Dominio de Okta**: Okta Domain

2. En el campo **Dominio de correo electrónico**, escribe el dominio de correo electrónico de la organización.
3. Haz clic en **Guardar y Validar**.

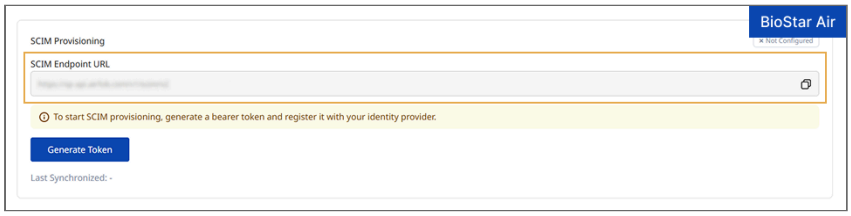
Cuando el sistema guarda y verifica correctamente, genera automáticamente el valor de **URL de descubrimiento**.



Conectar aprovisionamiento SCIM de Okta

1 BioStar Air: Copiar el token SCIM

1. Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda de BioStar Air.
2. Haga clic en la pestaña **SSO & SCIM**.
3. En la sección **Aprovisionamiento SCIM**, copie el valor de **URL del endpoint SCIM**.



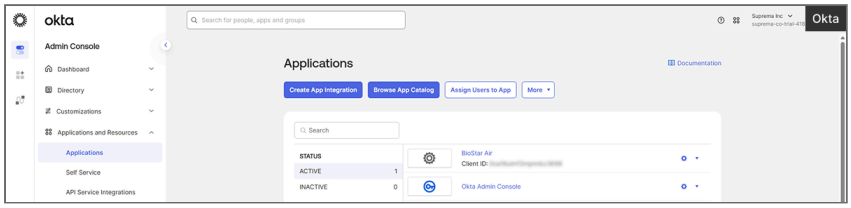
4. Haga clic en **Generar token**.

5. En el cuadro de diálogo Generación de token completada, copie el token.

> **Información**
>
> - Copie el token generado de inmediato. Copie el token solo al generarlo. Después de cerrar el cuadro de diálogo, el sistema no permite copiar el token de nuevo.
> - Si pierde el token, haga clic en **Rotar token** para generar un nuevo token. Ingrese el nuevo token nuevamente en el proveedor de identidad.
> - En el siguiente paso, ingrese la URL del extremo de SCIM y el token copiado en este paso.

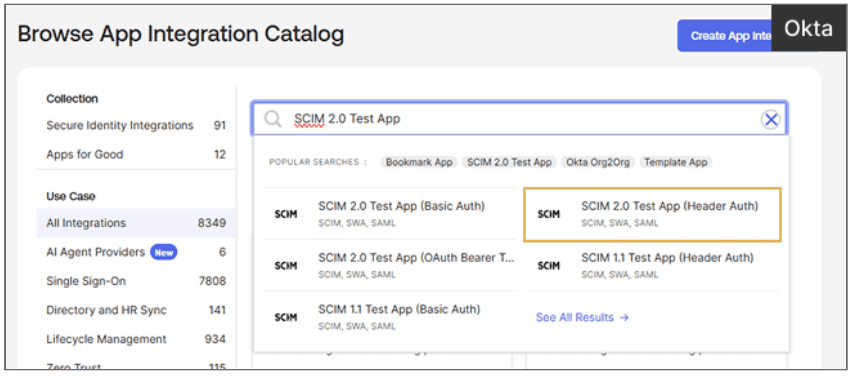
2 Okta: Crear una aplicación de aprovisionamiento SCIM

1. En la **Okta Admin Console**, ve a **Applications and Resources** → **Applications**.



2. Haz clic en **Browse App Catalog**.

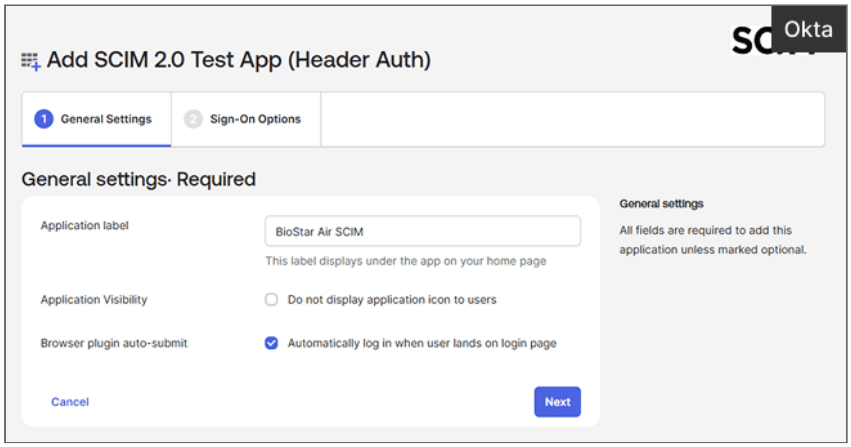
3. Busca 'SCIM 2.0 Test App'.



4. En los resultados de búsqueda, selecciona **SCIM 2.0 Test App (Header Auth)**.

5. Haz clic en **Add Integration**.

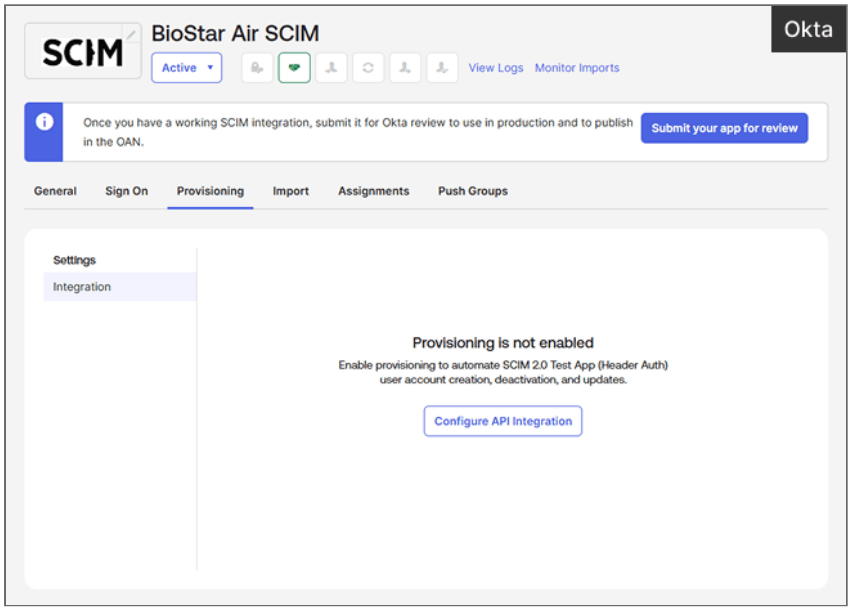
6. En el campo **Application label**, escribe 'BioStar Air SCIM'.



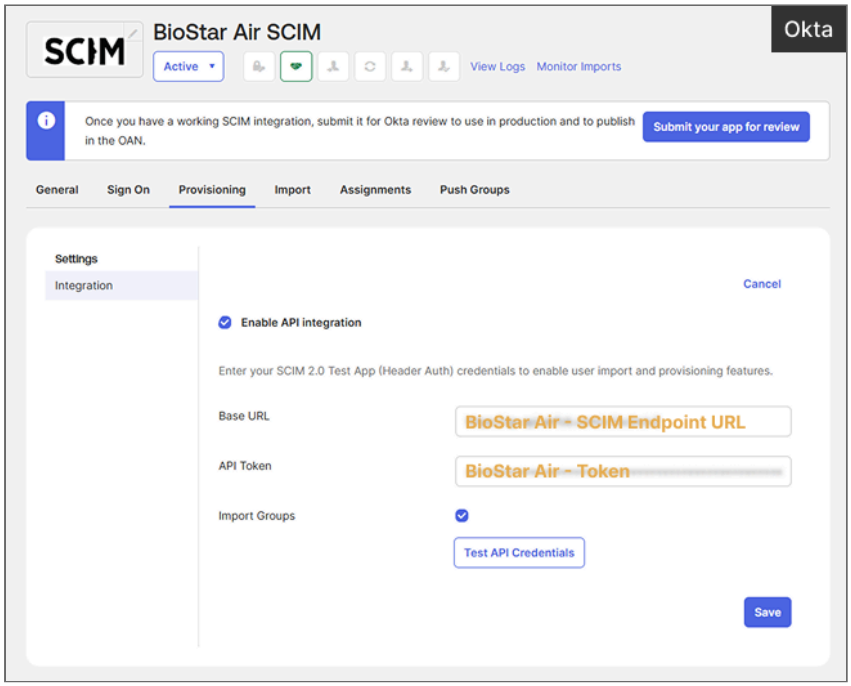
7. Haga clic en **Next**.
8. En **Sign-on options**, desplázate hacia abajo sin cambiar los ajustes y haz clic en **Done**.

3 Okta: Ajustes de integración de la API

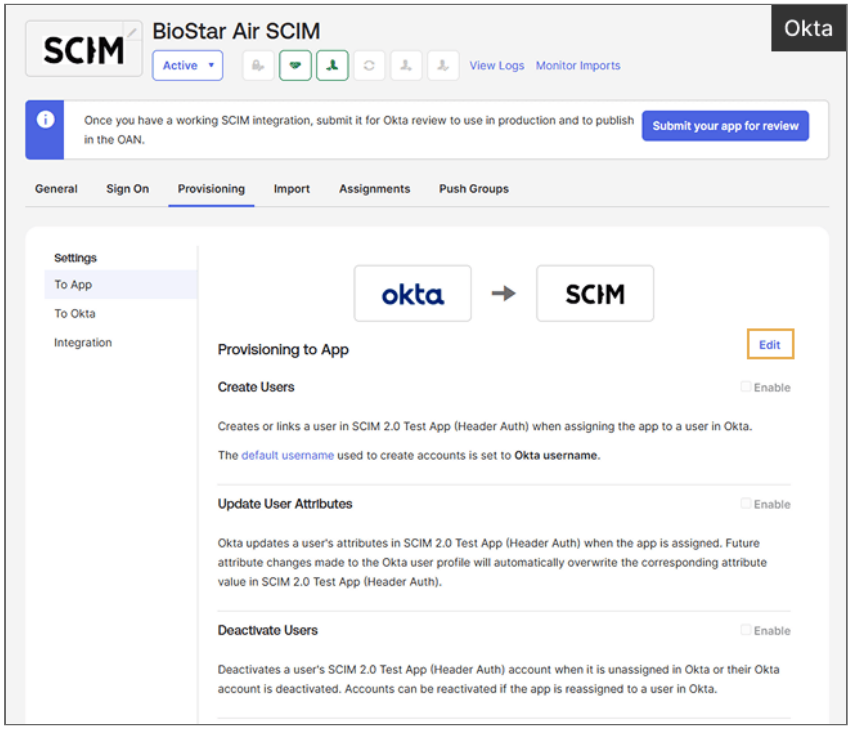
1. Después de crear la aplicación de aprovisionamiento, haz clic en la pestaña **Provisioning**.



2. Haz clic en **Configure API Integration**.
3. Haz clic en **Enable API integration**.
4. Introduce la URL del endpoint SCIM y el bearer token de BioStar Air: Copiar el token SCIM en **Base URL** y **API Token**.

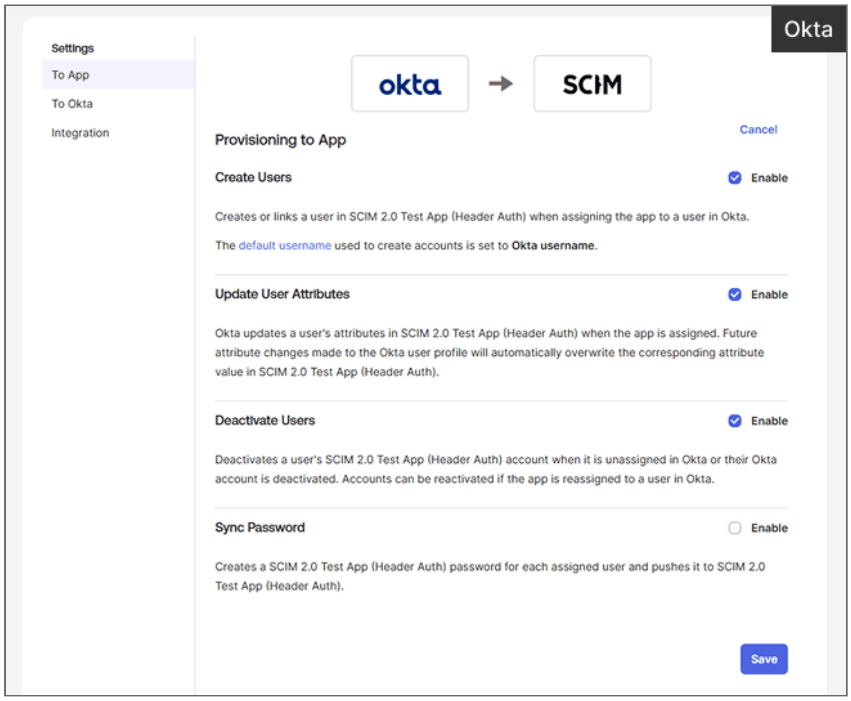


5. Para probar la sincronización, haz clic en **Test API Credentials**.
6. Haga clic en **Save**.
7. Haz clic en la pestaña **Provision** para definir el comportamiento de envío de grupos.
8. Haz clic en **Edit** y habilita los siguientes atributos.



- **Create Users**
- **Update User Attributes**
- **Deactivate Users**

9. Haz clic en **Save** para aplicar los cambios.

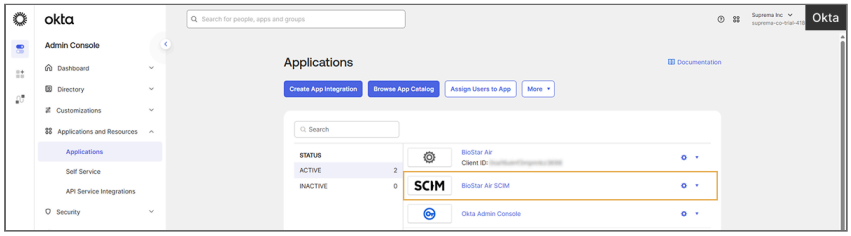


Enviar grupos de IdP a BioStar Air

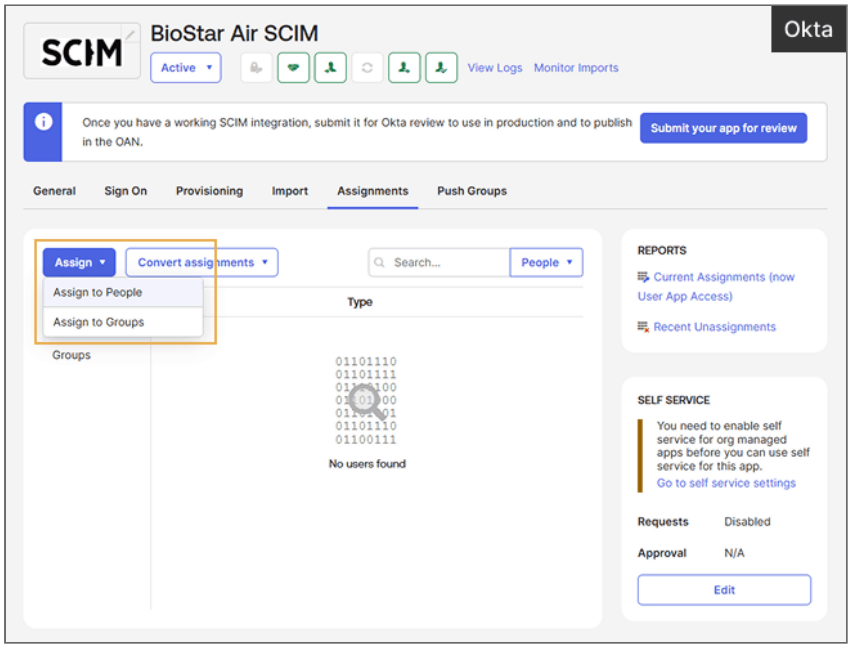
Para enviar grupos de IdP a BioStar Air, primero prepara los grupos de usuarios y los usuarios en Okta. Después de preparar los grupos de usuarios y los usuarios, envíalos a BioStar Air mediante SCIM.

1 Okta: Asignar grupos de usuarios

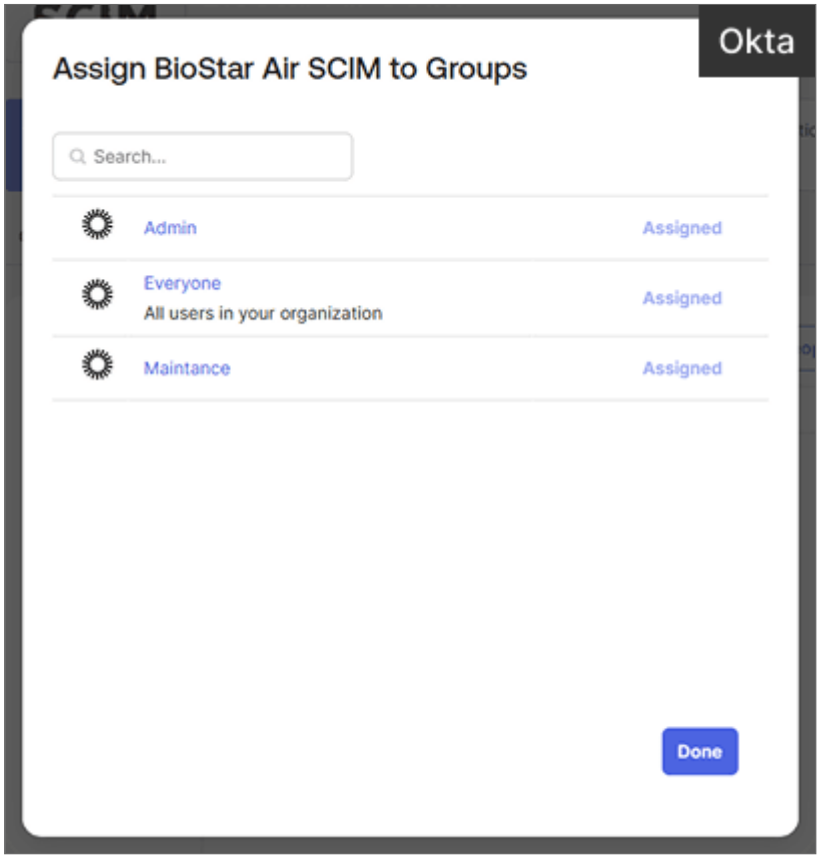
1. Inicie sesión en la **Okta Admin Console**.
2. Vaya a **Applications and Resources** → **Applications**.
3. Selecciona la aplicación SCIM.



4. Haz clic en la pestaña **Assignments**.
5. Haz clic en **Assign** → **Assign to Groups**.

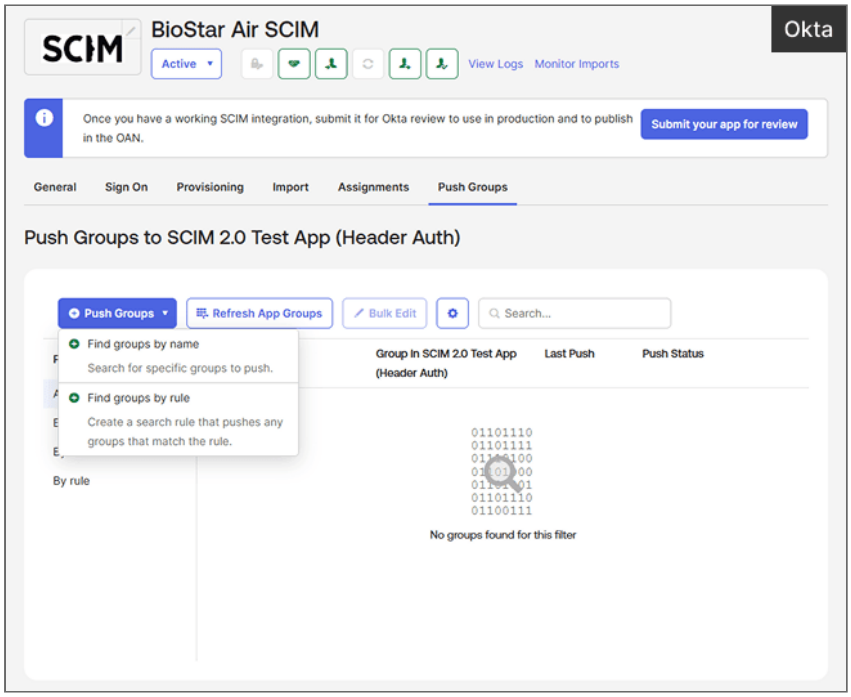


6. En el grupo de usuarios que asignarás a la aplicación SCIM, haz clic en **Assign**.
7. Después de asignar el grupo, haz clic en **Done**.

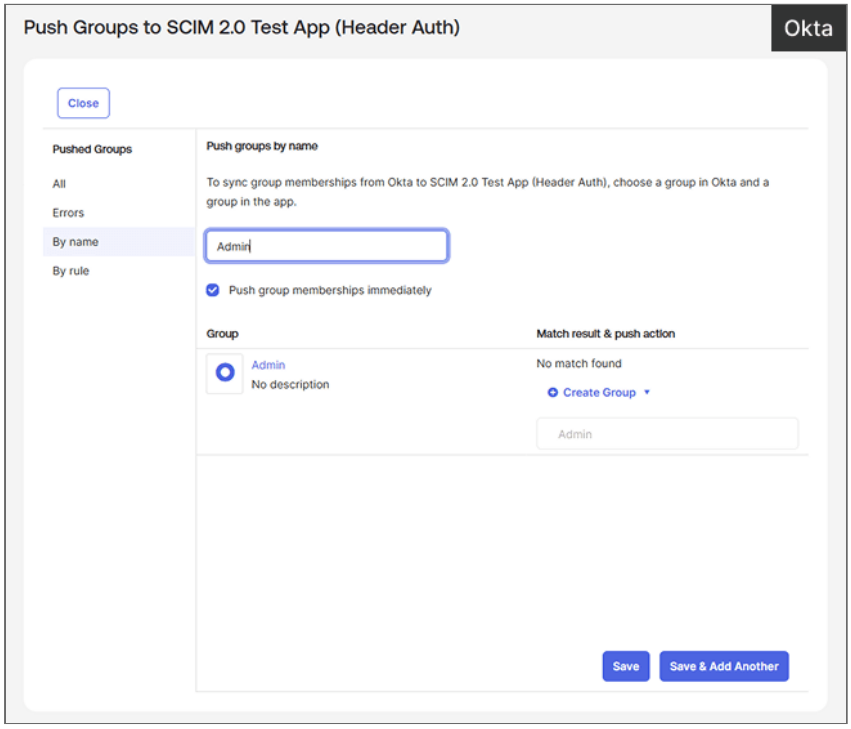


2 Okta: Enviar grupos de usuarios

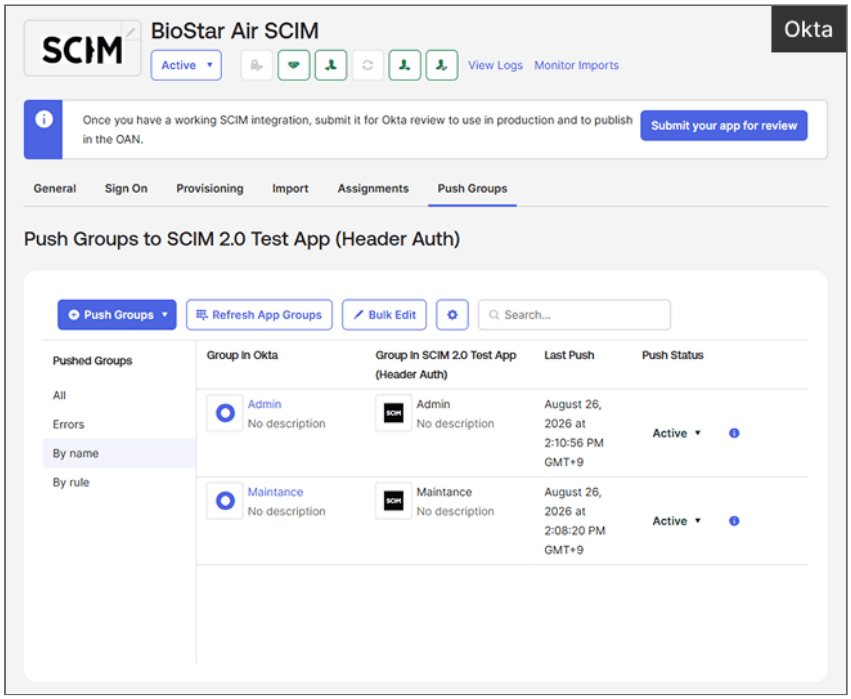
1. Haz clic en la pestaña **Push Groups**.
2. Haz clic en **Push Groups** → **Find groups by name**.



3. En el campo de entrada, ingresa el nombre del grupo que vas a enviar.
4. Cuando aparezca un grupo de usuarios coincidente, selecciónalo.

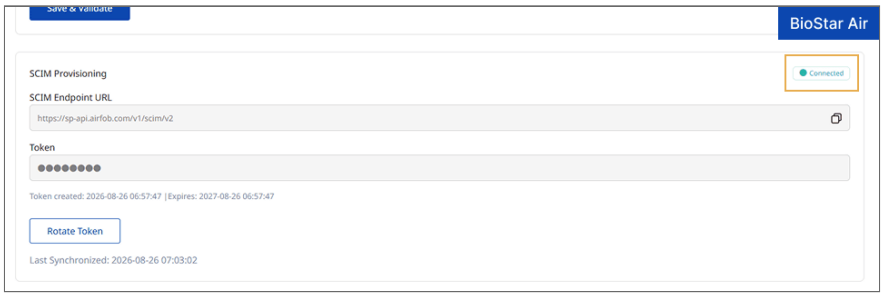


5. Después de seleccionar un grupo de usuarios, haz clic en **Save** o **Save & Another** para agregarlo.
6. Revisa los grupos de usuarios enviados en la pestaña **Push Groups**.



3 BioStar Air: Compruebe la conexión

1. Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda de BioStar Air.
2. Haga clic en la pestaña **SSO & SCIM**.
3. En la sección **Aprovisionamiento SCIM**, verifique que aparezca el indicador **Conectado**.



Asignación de grupos

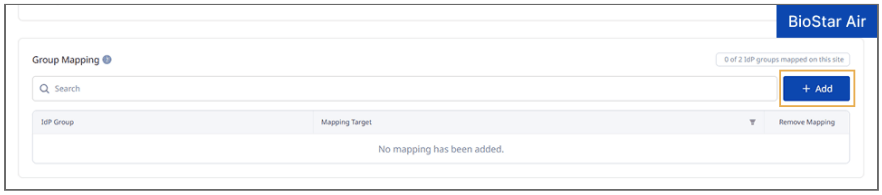
Después de conectar SSO y SCIM y enviar los grupos del IdP, el administrador del sitio debe asignarlos a grupos de BioStar Air.

Reglas de asignación

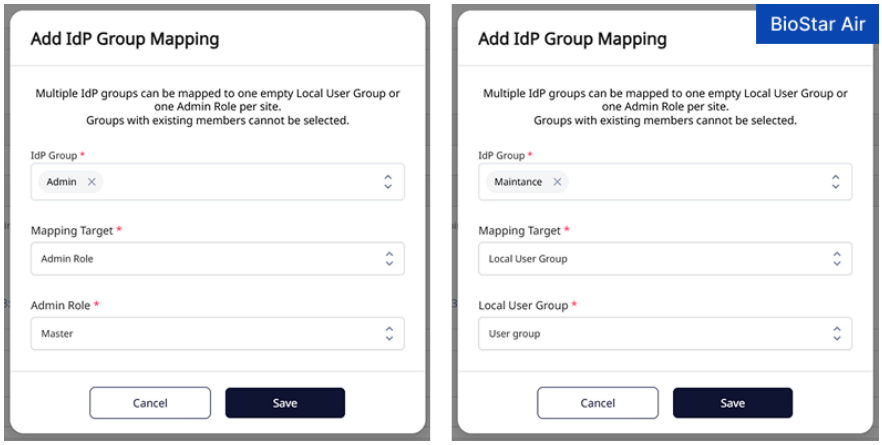
- Puede asignar varios grupos de IdP a un solo grupo de usuarios de BioStar Air.
- Un grupo de usuarios de BioStar Air debe estar vacío antes de la asignación.
- Los grupos de BioStar Air con miembros no pueden ser destinos de asignación.
- Solo el administrador maestro del sitio puede gestionar la asignación de grupos del IdP.
- El sistema bloquea el rol después de asignar un grupo del IdP al rol maestro.

Asignar roles de administrador y grupos de usuarios

1. Haga clic en **Ajustes** → **Sitio** en la barra lateral izquierda de BioStar Air.
2. Haga clic en la pestaña **SSO & SCIM**.
3. Vaya a la sección **Asignación de grupos** y haga clic en **Agregar**.

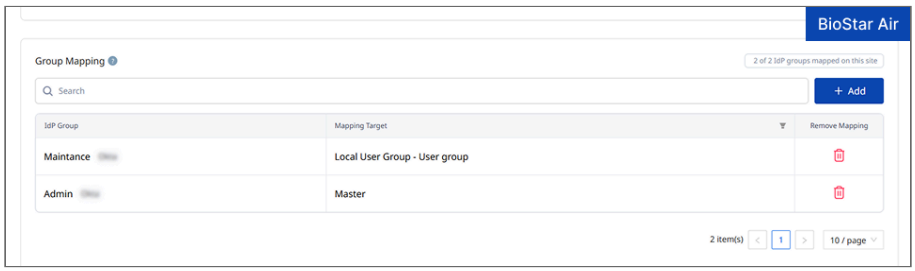


4. En **Grupo de IdP**, seleccione un grupo de IdP.
5. En **Destino de la asignación**, seleccione **Rol de administrador** o **Grupo de usuarios local** según el grupo de IdP seleccionado.
6. Según el destino de asignación, asigne un rol de administrador o seleccione un grupo de usuarios.



7. Haga clic en **Guardar** para guardar la asignación.

La sección **Asignación de grupos** muestra los grupos del IdP y los grupos de BioStar Air asignados.



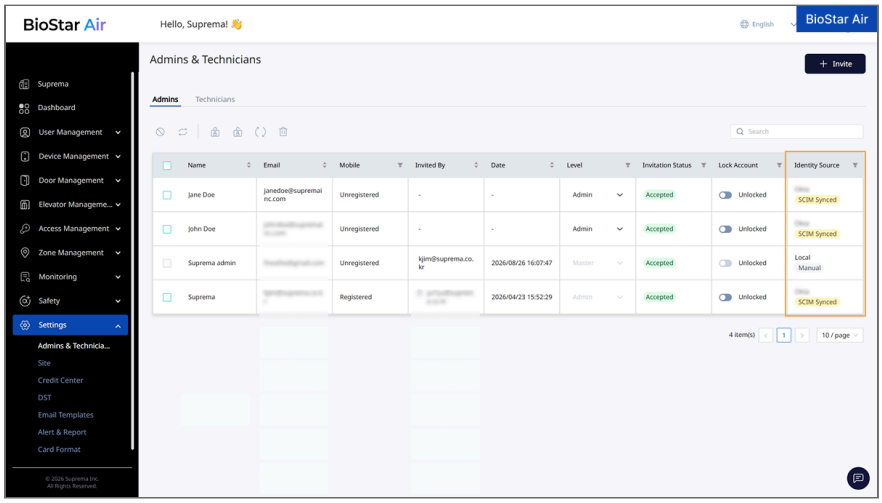
Información

- Para obtener más información sobre los roles de administrador, consulte Administrar cuentas y roles de administradores.
- Para obtener más información sobre los grupos de usuarios, consulte Administrar Grupos de Usuarios.

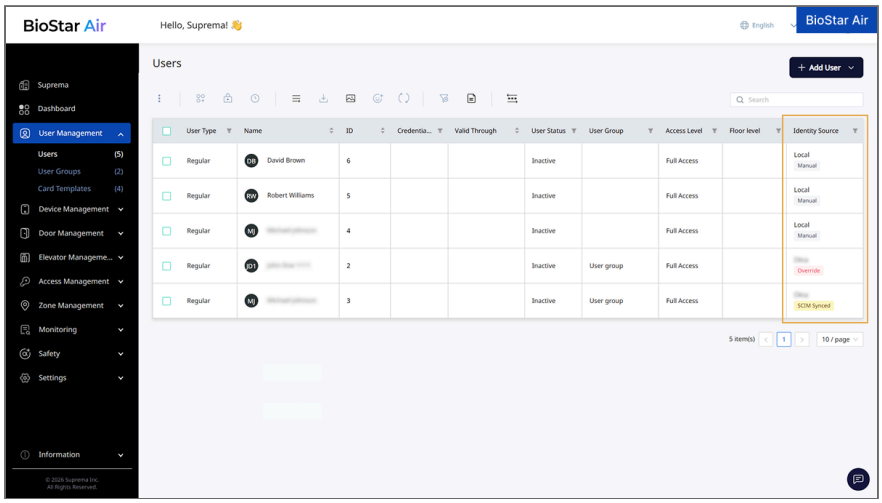
Administrar administradores, usuarios y grupos sincronizados

Con aprovisionamiento habilitado, BioStar Air indica si cada administrador, usuario y grupo es local o proviene del proveedor de identidad.

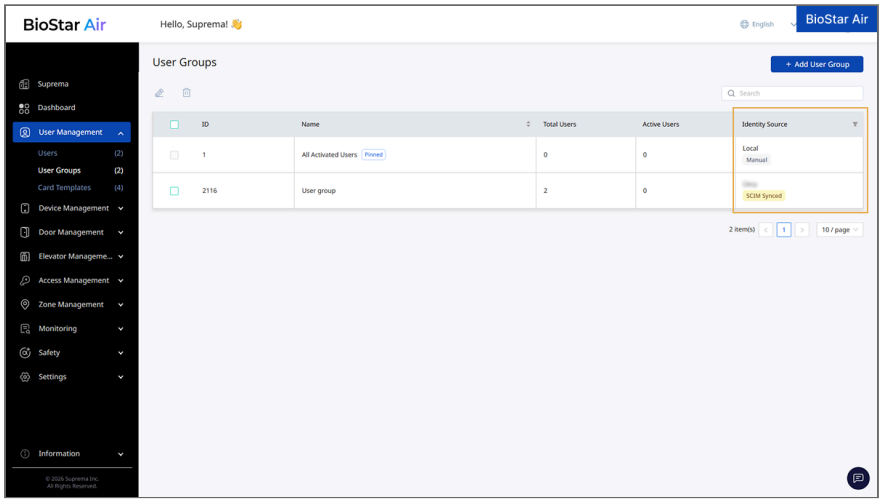
- En **Ajustes** → **Administradores y técnicos**, revise la columna **Fuente de identidad** en la lista de administradores.



- En **Gestión de usuarios** → **Usuarios**, revise la columna **Fuente de identidad** en la lista de usuarios.

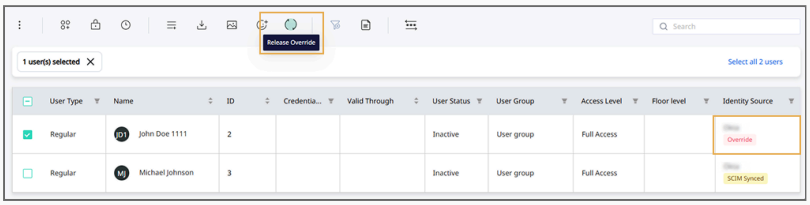


- En **Gestión de usuarios** → **Grupos de Usuarios**, revise la columna **Fuente de identidad** en la lista de grupos de usuarios.



Cómo funcionan las entradas sincronizadas con SCIM

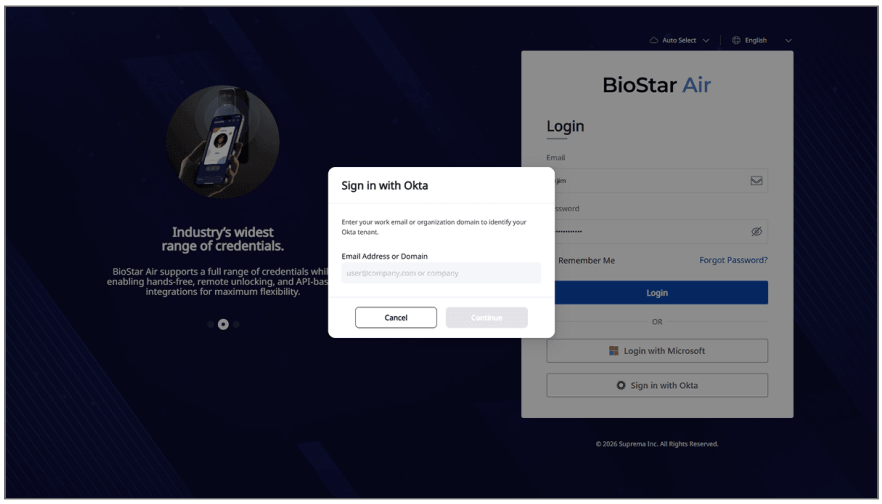
- Los usuarios y administradores creados manualmente siguen gestionándose manualmente.
- BioStar Air evita la eliminación manual de entradas sincronizadas con SCIM.
- BioStar Air evita agregar o quitar manualmente usuarios de grupos sincronizados con SCIM.
- Cambiar manualmente una entrada sincronizada de forma local establece el estado en **Anulación**. Ejecute **Liberar anulación** para cancelar los cambios locales y devolver el registro a la administración de SCIM.



Iniciar sesión en Okta

Tras completar la conexión SSO de Okta, los usuarios inician sesión con su cuenta de Okta en BioStar Air.

1. En la pantalla de inicio de sesión de BioStar Air, haz clic en **Iniciar sesión con Okta**.



2. Ingresa la dirección de correo electrónico o el dominio de la organización en el campo **Dirección de correo electrónico o dominio**. (Por ejemplo, `user@company.com` o `company`)
3. Haz clic en **Continuar**.
4. Cuando se abra la página de inicio de sesión de Okta, ingresa el correo electrónico y la contraseña de la cuenta de la organización.
5. Después de completar la autenticación, el sistema te redirige automáticamente a BioStar Air y finaliza el inicio de sesión.

Información

Si SSO de Okta no está configurado para el dominio de correo ingresado, aparece un mensaje de error. Comuníquese con el administrador del sitio.

Configuración adicional del sitio

Además de la configuración predeterminada del sitio, puede configurar funciones detalladas que afectan al servicio BioStar Air, como políticas horarias, plantillas de correo electrónico, métodos de entrega de alertas y registros de tiempo y asistencia. Puede agregar formatos personalizados de tarjetas Wiegand o configurar directamente la gestión del tiempo y la asistencia y la forma en que se generan los informes.

Horario de Verano (DST)

Utiliza la configuración del Horario de Verano (DST) para definir cómo el sitio ajusta la hora. Esto es especialmente importante para garantizar un registro coherente y preciso de la hora cuando gestionas un sitio con dispositivos y registros en distintas zonas horarias.

Para una gestión precisa del tiempo en BioStar Air, es necesario configurar los **ajustes de DST en tres lugares**:

- **Perfil de DST**: Define la fecha y la hora de inicio y fin del DST para cada zona horaria.
- **Hora del sitio**: Establece la zona horaria aplicada al sitio y a los registros de eventos.
- **Hora del dispositivo**: Configura cada lector individual para que ajuste correctamente su reloj.

Las tres opciones deben configurarse correctamente en los sitios ubicados en zonas horarias que observan el Horario de Verano.

Consejo

Consulta el siguiente video para obtener una guía sobre cómo configurar los ajustes del Horario de Verano (DST).

Información

Considera lo siguiente al revisar Registros de eventos.

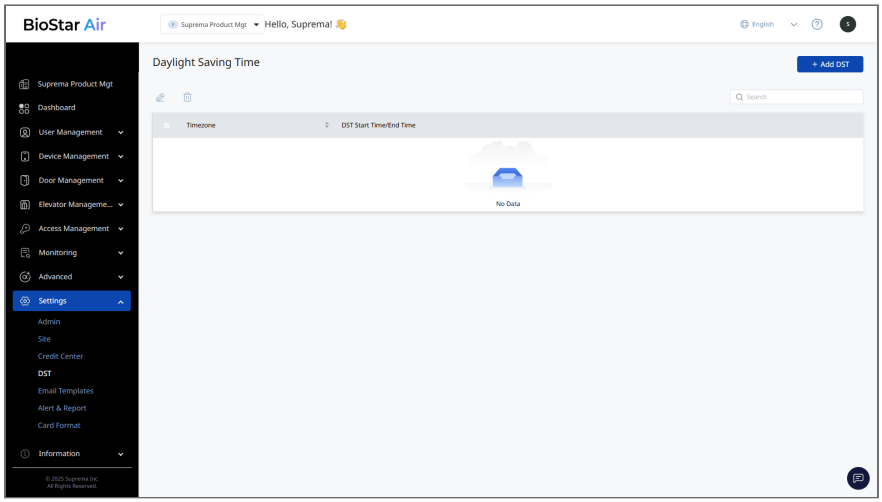
- Si la hora del dispositivo está configurada, las marcas de tiempo de los registros de eventos se ajustan al horario de verano de cada dispositivo.
- Si la hora del sitio está configurada, las marcas de tiempo se ajustan según la configuración de DST del sitio en lugar de la de cada dispositivo.

Paso 1: Crear perfil de DST

Un perfil de DST define la fecha y la hora en que el DST comienza y termina para una zona horaria específica. Debe crear un perfil de DST para cada zona horaria en la que se encuentren el sitio y los lectores.

Agregar nuevo perfil

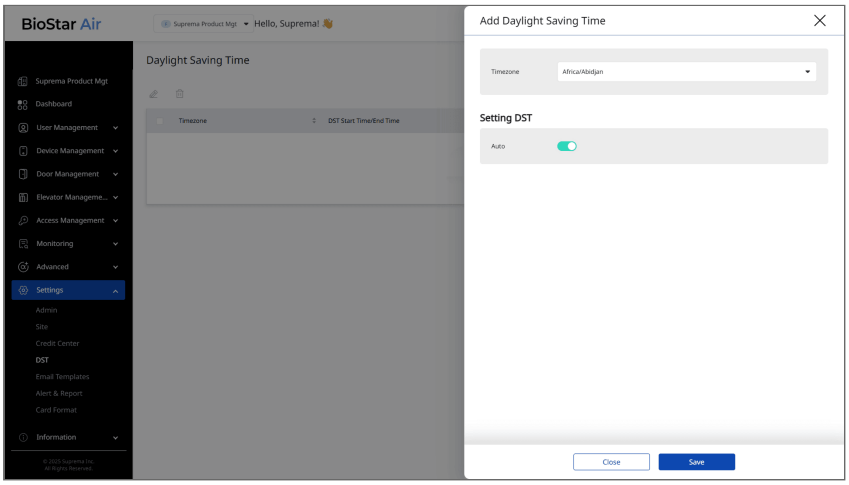
1. Haz clic en **Ajustes** → **DST** en la barra lateral izquierda.
2. Haz clic en **Agregar DST** en la parte superior derecha de la pantalla.



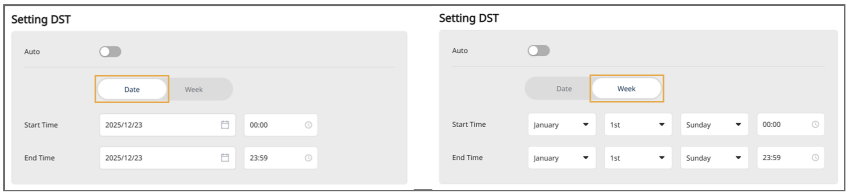
3. Selecciona el elemento deseado en **Zona horaria** cuando aparezca el panel **Agregar DST**.

4. Selecciona la configuración automática o manual en **Configuración de DST**.

   - **Automático**: La configuración de DST para la zona horaria seleccionada se agrega automáticamente. Las fechas de inicio y fin del DST se determinan según las reglas estándar de esa zona horaria.



   - **Manual**: Establece manualmente las horas de inicio y fin correspondientes para la zona horaria.



     – **Fecha**: Selecciona las fechas en las que el DST comienza y termina.

     – **Semana**: Selecciona las semanas en las que el DST comienza y termina.

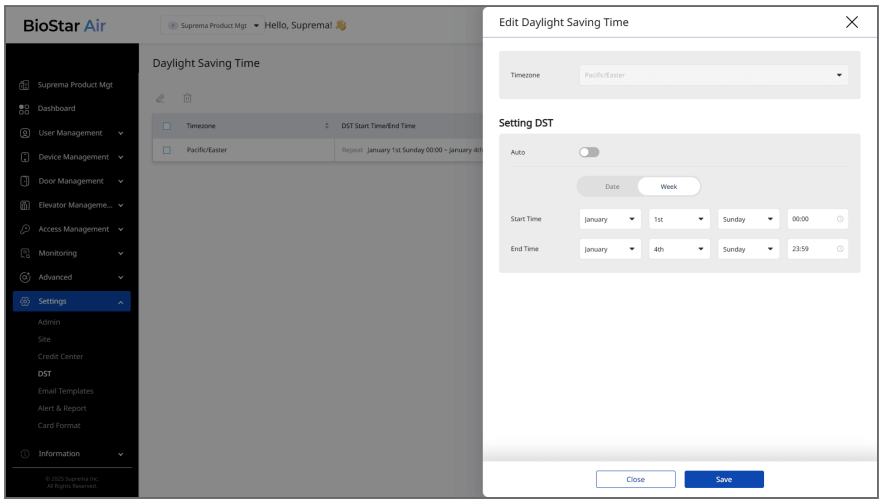
5. Haz clic en **Guardar** en la parte inferior para guardar el perfil DST.

Editar el perfil DST existente

1. Haz clic en **Ajustes** → **DST** en la barra lateral izquierda.

2. Haz clic en el perfil DST que quieras editar en la lista. Alternativamente, selecciona la casilla y haz clic en en la parte superior.

3. Modifica la hora de inicio y de finalización cuando aparezca el panel **Editar el horario de verano**.



La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

4. Haz clic en **Guardar** en la parte inferior para guardar los cambios.

Eliminar el perfil DST

1. Haz clic en **Ajustes** → **DST** en la barra lateral izquierda.
2. Haz clic en la casilla del perfil DST que quieras eliminar en la lista. Puedes seleccionar uno o más perfiles.
3. Haz clic en en la parte superior de la pantalla.
4. Cuando aparezca la ventana de mensajes, haz clic en el botón **Sí**.

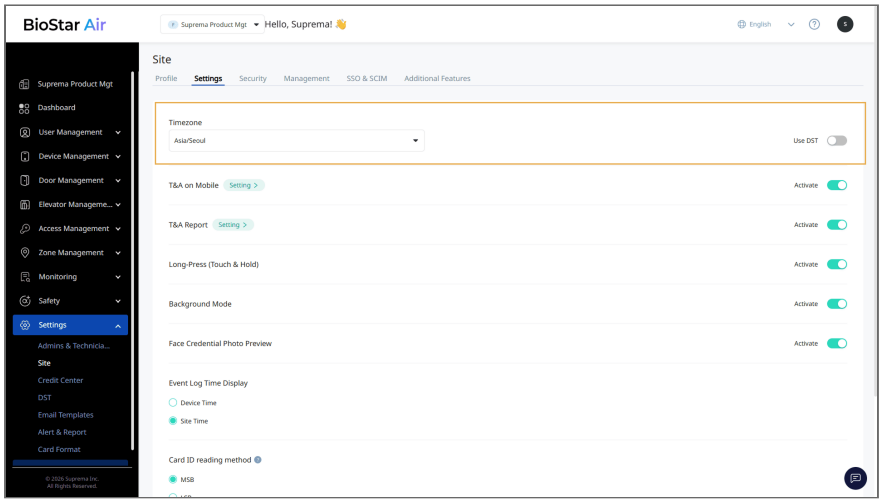
Paso 2: Configuración de la hora del sitio

La hora del sitio determina la zona horaria predeterminada que utiliza todo el sistema. Los siguientes elementos se ven afectados por esta configuración:

- Marcas de tiempo del registro de eventos
- Informes y datos de monitoreo
- Zona horaria predeterminada aplicada al registrar un nuevo dispositivo

Sigue las instrucciones a continuación para configurar la zona horaria del sitio y habilitar el horario de verano.

1. Haz clic en **Ajustes** → **Sitio** en la barra lateral izquierda.
2. Haz clic en la pestaña **Settings**.
3. Selecciona la zona horaria deseada en **Zona horaria**.



4. Habilita **Usar DST** para aplicar el horario de verano a la zona horaria seleccionada.

> **Precaución**
>
> Si la opción **Usar DST** no está habilitada en una zona horaria donde aplica el horario de verano, el sistema no ajustará la hora automáticamente y los registros de eventos pueden mostrarse de forma incorrecta.

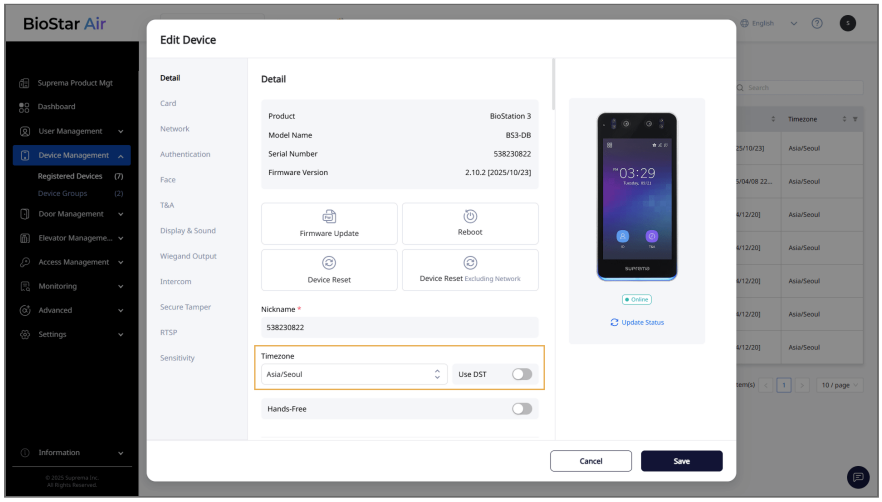
Paso 3: Habilitar el horario de verano para los dispositivos

Cada dispositivo conectado a BioStar Air mantiene su propio reloj, que se usa para el control de acceso y los registros de asistencia. Configura los ajustes de horario de verano para cualquier dispositivo ubicado en una zona horaria donde aplique el horario de verano.

Los dispositivos con pantalla, como BioStation 3, muestran la hora. Los dispositivos sin pantalla, como XPass 2, mantienen sus relojes internos para el control de acceso y los registros de tiempo y asistencia.

Configura el horario de verano en todos los dispositivos, tengan o no pantalla, para garantizar que los registros de eventos, los registros de acceso y los datos de asistencia se registren correctamente.

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. Haz clic en el dispositivo al que quieras aplicar los ajustes de horario de verano en la lista.
3. Selecciona la zona horaria deseada en la sección **Zona horaria** y activa la opción **Usar DST**.



> Esta opción está habilitada de forma predeterminada en las zonas horarias donde se aplica el horario de verano.

4. Haz clic en **Guardar** en la parte inferior para guardar los cambios.

> **Información**
> Si la hora del dispositivo no está configurada correctamente, pueden ocurrir los siguientes problemas:
> - **Error de acceso denegado**: La hora de acceso está configurada para comenzar a las 07:00 AM, pero si el dispositivo cree que son las 06:00 AM, se denegará el acceso al usuario.
> - **Error de programación**: El bloqueo/desbloqueo a la hora programada puede no ser preciso.
> - **Error en los registros**: Las horas en el registro de eventos y en los registros de tiempo y asistencia no coinciden con la hora real.

Lista de verificación

Para garantizar la precisión del horario en las regiones que observan el horario de verano (DST), asegúrate de haber completado las tres acciones siguientes.

- **Crear perfiles de DST**: ¿Has creado los perfiles de DST necesarios para cada zona horaria?
- **Configuración horaria del sitio**: ¿Has establecido la zona horaria del sitio y activado la opción **Usar DST**?
- **Ajustes de DST del dispositivo**: ¿Has configurado la zona horaria de cada dispositivo y activado la opción **Usar DST**?

Si las tres están configuradas correctamente, los registros de eventos, los horarios de acceso y los registros de asistencia mostrarán la hora correcta.

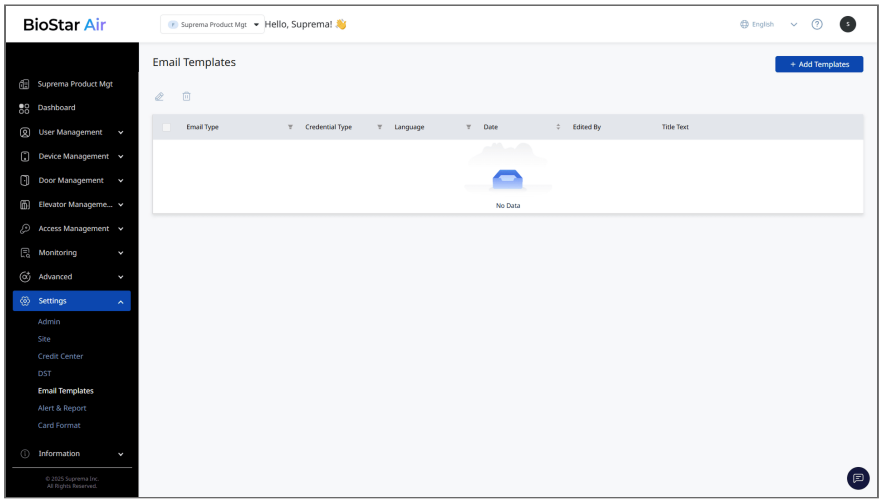
Personalizar plantillas de correo electrónico

Utilice la función de plantillas de correo electrónico para personalizar los correos enviados a los usuarios del sitio, de modo que reflejen la marca y el mensaje de su empresa. Las plantillas incluyen invitaciones, correos de activación y otras notificaciones.

> **Consejo**
> Vea el siguiente video para aprender a configurar las plantillas de correo electrónico.

Agregar plantillas de correo electrónico

1. Haga clic en **Ajustes** → **Plantillas de Email** en la barra lateral izquierda.
2. Haga clic en **Añadir Plantillas** en la parte superior derecha de la pantalla.

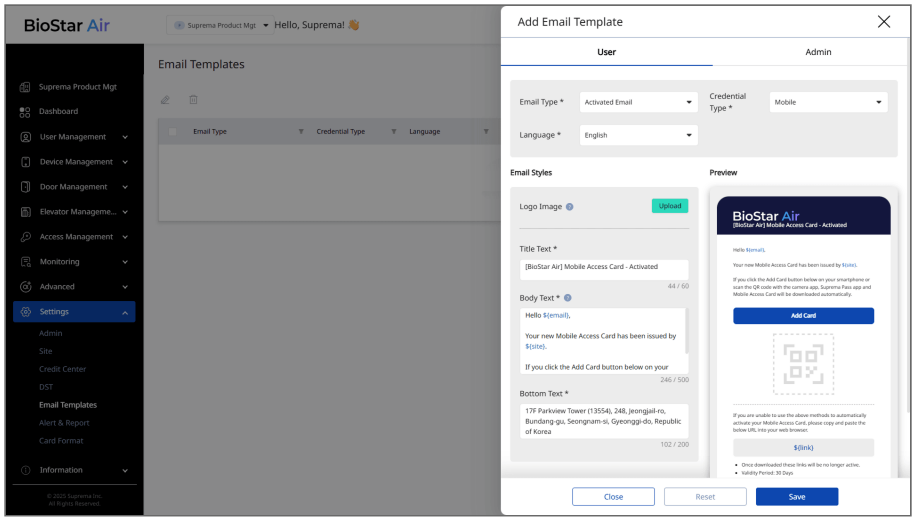


3. Cuando aparezca el panel **Agregar plantilla de Email**, configure cada elemento. Seleccione la pestaña **Usuario** o **Administración** para configurar las plantillas de correo electrónico de usuario o de administrador.

> **Información**
>
> Cree plantillas de correo electrónico separadas para cada idioma. Seleccione el idioma en **Idioma**. Los idiomas compatibles son los siguientes:
>
> > *English, 한국어, 日本語, Nederlands, Español, Português*
>
> Se admitirán más idiomas.

Usuario

Personalice las plantillas de correo electrónico enviadas a los usuarios.



- **Tipo de Email**: Seleccione el tipo de plantilla de correo electrónico que desea crear. Las opciones disponibles son las siguientes:
  - **Activada Email**: Se utiliza normalmente como invitación para descargar una tarjeta móvil.
  - **Correo electrónico reactivado**: Envía al usuario una notificación de que la tarjeta móvil ha sido reactivada.
  - **Reemitida Email**: Se utiliza al emitir una nueva tarjeta móvil.
  - **Eliminada Email**: Envía al usuario una notificación sobre la eliminación de la tarjeta.

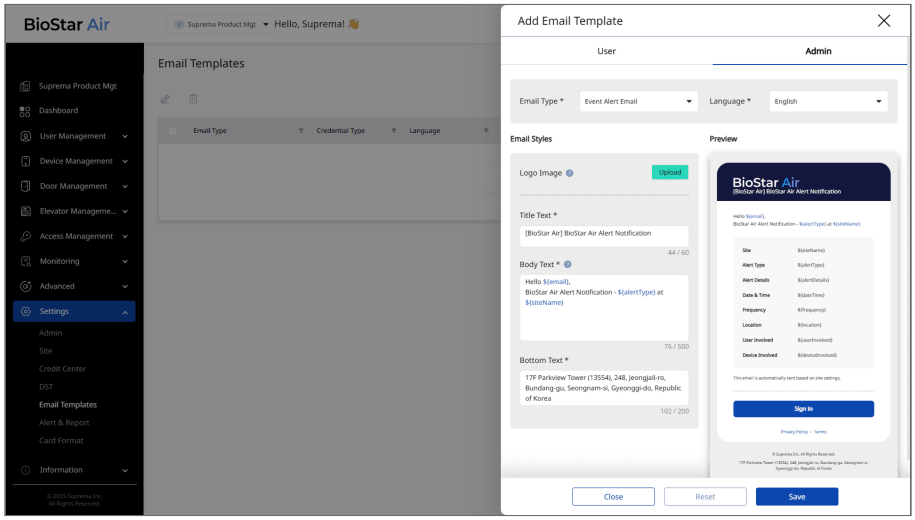
  - **Suspendida Email**: Notifica al usuario que la tarjeta ha sido suspendida.
  - **Correo Electrónico de Solicitud de Registro Facial**: Se usa para solicitar al usuario que suba una foto de su rostro.

- **Tipo de Credencial**: Se puede seleccionar para tipos de correo que permiten la descarga de la tarjeta móvil, como **Activada Email** y **Reemitida Email**.
  - **Mobile**
  - **Web QR**
  - **Pase de enlace**

> Para obtener más información sobre los tipos de credenciales, consulte Tipos de tarjetas y credenciales de usuario.

Administración

Personalice las plantillas de correo electrónico enviadas a los administradores.

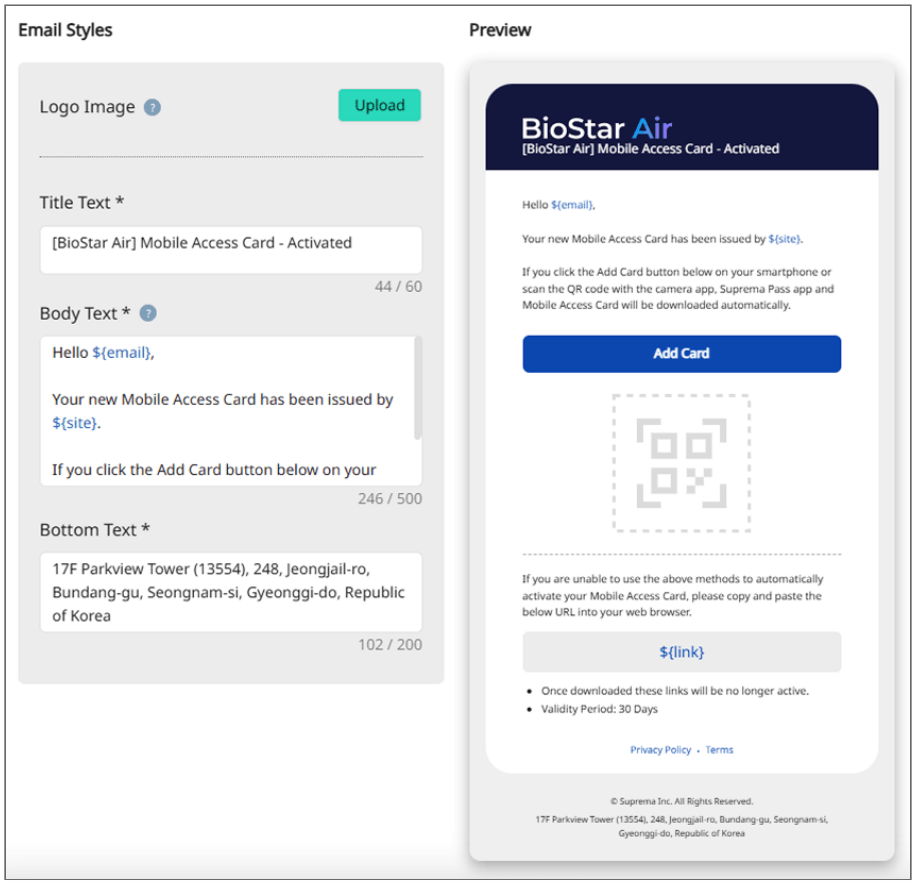


Tipo de Email: Seleccione el tipo de plantilla de correo electrónico que desea crear. Las opciones disponibles son las siguientes:

- **Correo electrónico de alerta de evento**: Envía a los administradores notificaciones sobre eventos en el sitio.
- **Correo electrónico de alerta del sistema**: Envía alertas del sistema a los administradores.
- **Correo de Alerta de Informe**: Envía a los administradores un enlace de descarga después de generar un informe.

Estilos de Emaill

Personalice el logotipo y el contenido del correo electrónico. Vea los cambios en tiempo real en **Vista previa**.



- **Imagen del Logo**: Cargue la imagen del logotipo que aparecerá en el correo electrónico.

  - Tipos de archivo: JPG, JPEG, PNG
  - Resolución mínima: 200 x 60
  - Tamaño del archivo: 1 MB o menos

- **Texto do Título**: Ingrese el asunto del correo electrónico.
- **Texto de Corpo**: Ingrese el mensaje que se mostrará en el cuerpo del correo electrónico.

El cuerpo del correo electrónico debe incluir claves HTML. Cada clave se reemplaza por la dirección de correo electrónico del destinatario, el nombre del sitio y otros valores. Las claves disponibles pueden variar según el valor seleccionado en **Tipo de Email**.

- Pestaña **Usuario**
- `${email}`: Dirección de correo electrónico
- `${siteName}`: Nombre del sitio
- Pestaña **Administrador**
- `${email}`: Dirección de correo electrónico
- `${siteName}`: Nombre del sitio
- `${alertType}`: Tipo de alerta
- `${alertDetails}`: Detalles de la alerta
- `${frequency}`: Frecuencia de la alerta
- `${location}`: Ubicación de la alerta
- `${userInvolved}`: Usuario involucrado en la alerta
- `${deviceInvolved}`: Dispositivo involucrado en la alerta
- `${dateTime}`: Fecha y hora de la alerta

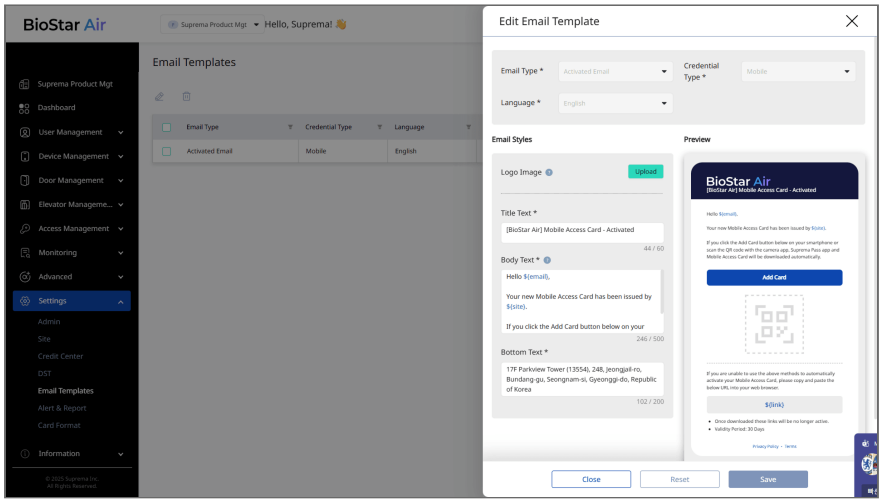
- **Texto Abaixo**: Ingrese información adicional que aparecerá en la parte inferior del correo electrónico. Agregue la dirección de la empresa o la información de contacto para el cumplimiento normativo o para proporcionar detalles de ubicación a los usuarios.

Información

- Verifique que la imagen del logotipo tenga el formato y tamaño adecuados para que aparezca correctamente en el correo electrónico.
- Si el idioma actual no es compatible, consulte las actualizaciones futuras. Se agregarán más idiomas.
- El campo de dirección es importante para el cumplimiento normativo y la claridad; ingréselo con precisión.
- Haga clic en **Guardar** en la parte inferior para guardar la plantilla de correo electrónico.
- Haga clic en **Reiniciar** en la parte inferior para restaurar el contenido original después de realizar cambios.

Editar plantillas de correo electrónico

1. Haga clic en **Ajustes** → **Plantillas de Email** en la barra lateral izquierda.
2. Haz clic en la plantilla de correo electrónico que quieres editar de la lista. O bien, marca la casilla y haz clic en en la parte superior.
3. Cuando aparezca el panel **Editar plantilla de Email**, edita los elementos necesarios.



4. Haz clic en **Guardar** en la parte inferior para guardar los cambios.

Eliminar plantillas de correo electrónico

1. Haga clic en **Ajustes** → **Plantillas de Email** en la barra lateral izquierda.
2. Marca la casilla de la plantilla de correo electrónico que quieres eliminar de la lista. Puedes seleccionar más de una plantilla.
3. Haz clic en en la parte superior de la lista.
4. Haga clic en **Borrar** cuando aparezca la ventana del mensaje.

Configurar alertas y informes

Configurar alertas e informes permite detectar y rastrear automáticamente eventos del sistema y situaciones de seguridad. Este artículo explica cómo configurar las opciones de alertas e informes en BioStar Air.

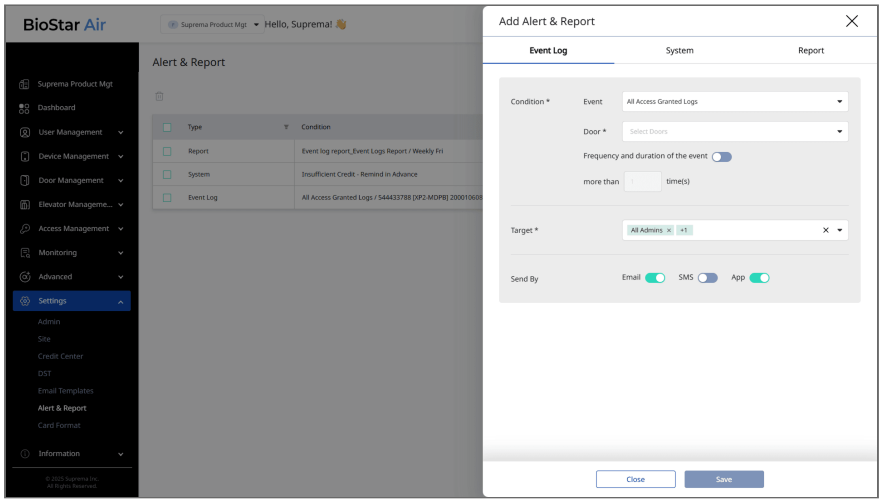
La configuración de alertas e informes ofrece los siguientes beneficios.

- Detecta de inmediato amenazas de seguridad o problemas del sistema y envía alertas en tiempo real a los administradores.
- Genera automáticamente informes sobre el estado del sistema y la actividad de los usuarios para mejorar la eficiencia en la gestión.

Agregar alertas

Configura alertas para registros de eventos específicos y para el estado del sistema en el sitio.

1. Haz clic en **Ajustes** → **Alerta e informe** en la barra lateral izquierda.
2. Haz clic en **Agregar alerta e informe** en la parte superior derecha de la pantalla.
3. Cuando aparezca el panel **Agregar alerta e informe**, elige la pestaña **Registro de eventos** o la pestaña **Sistema**.

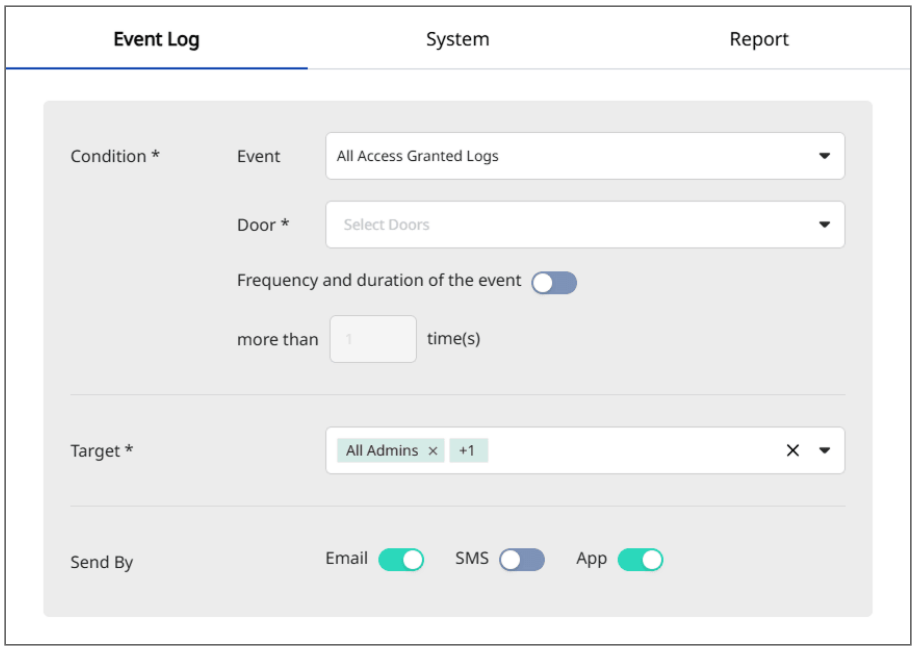


4. Después de configurar cada elemento, haz clic en **Guardar** para guardar.

Establecer condiciones

Registro de eventos

En la pestaña **Registro de eventos**, establece condiciones de alerta por tipo de evento.

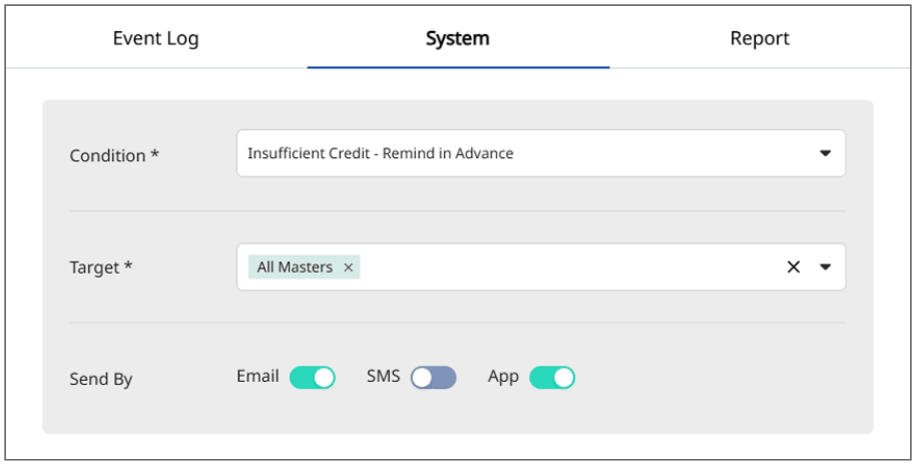


- **Eventos**: Selecciona los tipos de eventos para los que se enviará una alerta. También se puede seleccionar un **Eventos preestablecidos** predefinido.
- **Puerta**: Selecciona una puerta. Envía una alerta cuando ocurra un evento en la puerta seleccionada. Se pueden seleccionar varias puertas.
- **Frecuencia y duración del evento.**: Envía una alerta cuando los eventos ocurran con una frecuencia determinada dentro del período de tiempo definido. Por ejemplo, configura el sistema para que envíe una alerta si un evento ocurre tres veces en cinco minutos.

Consejo

En BioStar Air, a partir de la versión 2.12, es posible configurar alertas en tiempo real para eventos de desconexión de red de los dispositivos.

Sistema



En la pestaña **Sistema**, establece condiciones de alerta basadas en el estado del sistema. Las opciones disponibles son las siguientes.

- **Crédito insuficiente: recuérdelo con anticipación**
- **Crédito insuficiente: sitio suspendido**
- **Crédito insuficiente - SMS (menos de 10)**
- **La batería del APB está baja**
- **Hay un nuevo firmware disponible**
- **Red Desconectada (Detectado por el Dispositivo)**

Establecer destinatarios de alertas

Usa **Objetivo** para designar a los destinatarios de las alertas. Selecciona usuarios por rol de administrador o elige usuarios individuales.

Configurar método de envío

Selecciona el método de envío en **Enviado por**. Las alertas se envían por correo electrónico, SMS o notificación push de la aplicación.

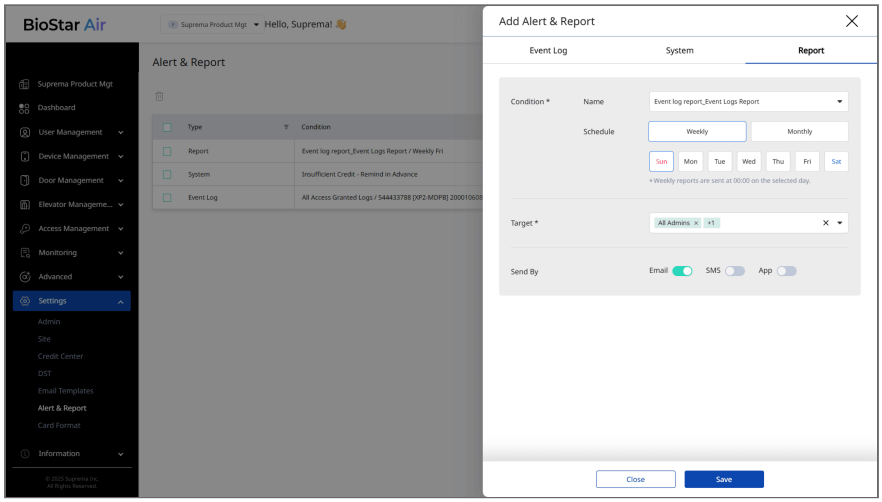
Información

Los mensajes de texto solo se pueden enviar después de recargar los créditos de SMS. Los créditos de SMS restantes se pueden consultar en **Ajustes** → **Centro de crédito**.

Generar informes

Genera informes automáticamente en intervalos definidos y envíalos a los administradores. Genera informes sobre la actividad del registro de eventos y el estado de los usuarios.

1. Haz clic en **Ajustes** → **Alerta e informe** en la barra lateral izquierda.
2. Haz clic en **Agregar alerta e informe** en la parte superior derecha de la pantalla.
3. Cuando aparezca el panel **Agregar alerta e informe**, selecciona la pestaña **Informe**.



4. Después de configurar cada elemento, haz clic en **Guardar** para guardar.

Configurar condiciones

Configura el tipo de informe y el intervalo de generación.

- **Nombre**: Selecciona el tipo de informe a generar.
  - **Informe de tiempo y asistencia**: Genera un informe sobre el estado de Tiempo y Asistencia de los usuarios para el período seleccionado.
  - **Informe de Registros de Auditoría**: Genera un informe sobre el estado del registro de auditoría para el período seleccionado.
  - **Informe de Registros de Eventos**: Genera un informe sobre la actividad del registro de eventos para el período seleccionado.
  - **Informe de Usuario**: Genera un informe sobre el estado de los usuarios para el período seleccionado.
- **Horario**: Selecciona el intervalo de generación de informes. Elige entre **Semanalmente** y **Mensual**.

Configurar destinatarios del informe

Usa **Objetivo** para designar a los destinatarios de las alertas. Selecciona usuarios por rol de administrador o elige usuarios individuales.

Configurar método de envío

Selecciona el método de envío en **Enviado por**.

> **Información**
>
> Los informes se entregan **únicamente por correo electrónico**. No se envían por SMS ni por notificación push de la aplicación.

Editar alertas e informes

1. Haz clic en **Ajustes** → **Alerta e informe** en la barra lateral izquierda.
2. Haz clic en la alerta o el informe que deseas editar en la lista.
3. Cuando aparezca el panel **Editar alerta** o **Editar informe**, edita los elementos necesarios.
4. Haz clic en **Guardar** en la parte inferior para guardar los cambios.

Eliminar alertas e informes

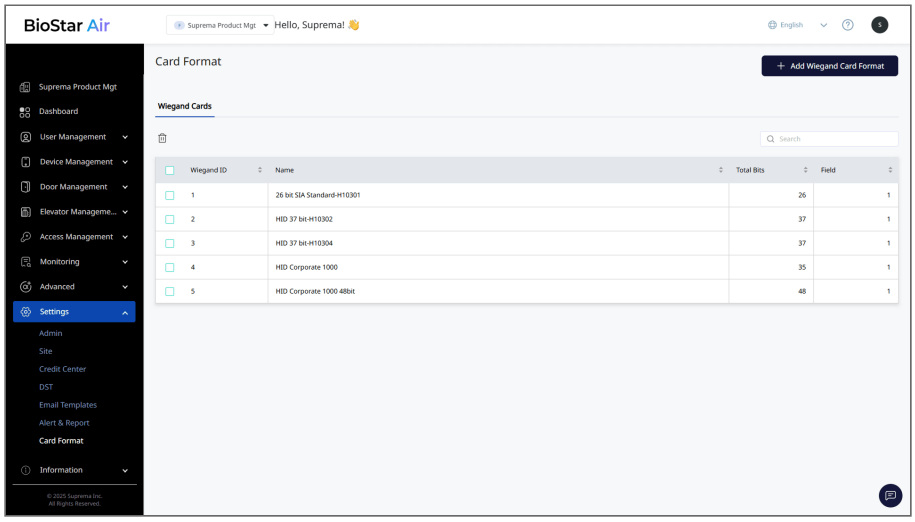
1. Haz clic en **Ajustes** → **Alerta e informe** en la barra lateral izquierda.
2. Selecciona la casilla de la alerta o del informe que deseas eliminar en la lista. Se puede seleccionar más de un elemento.
3. Haga clic en en la esquina superior izquierda de la lista.
4. Haga clic en **Borrar** cuando aparezca la ventana del mensaje.

Formato de tarjeta Wiegand personalizado

Cree y configure un formato de tarjeta Wiegand personalizado en BioStar Air v2.10, incluyendo códigos de instalación, segmentos de ID, bits de paridad y asignación de bits, para migrar sin contratiempos desde un sistema de control de acceso existente.

Lista de formatos de tarjeta Wiegand

Haga clic en **Ajustes** → **Formato de tarjeta** en la barra lateral izquierda. Cree, administre y vea formatos especiales de tarjeta, incluidos los formatos Wiegand, SIA y HID. Resulta útil para sitios que migran desde una solución de control de acceso existente con tarjetas emitidas previamente.

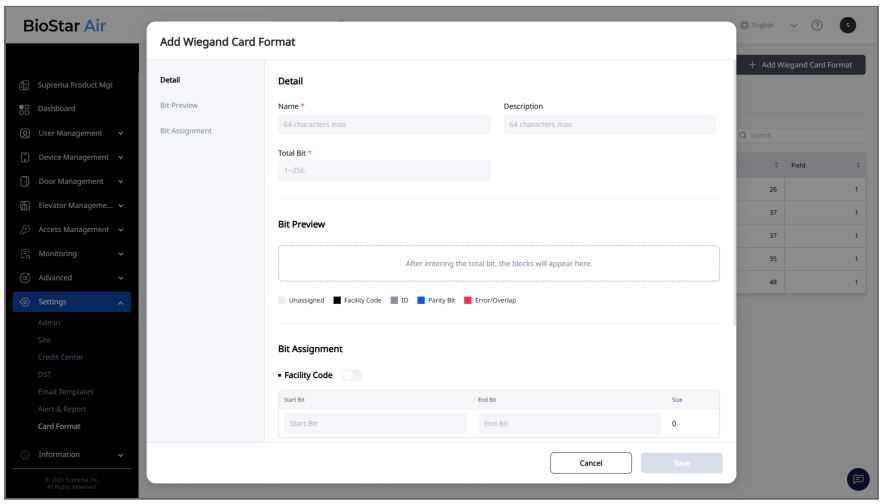


- Vea todos los formatos de tarjeta Wiegand registrados, incluidos los predeterminados de BioStar Air.
- Revise el nombre, la descripción, el total de bits, la vista previa y la asignación detallada de bits del formato.
- Configure un nuevo formato de tarjeta personalizado, incluyendo su nombre, descripción, total de bits y la asignación detallada de bits. El sistema ofrece una vista previa de los bits para su verificación visual.

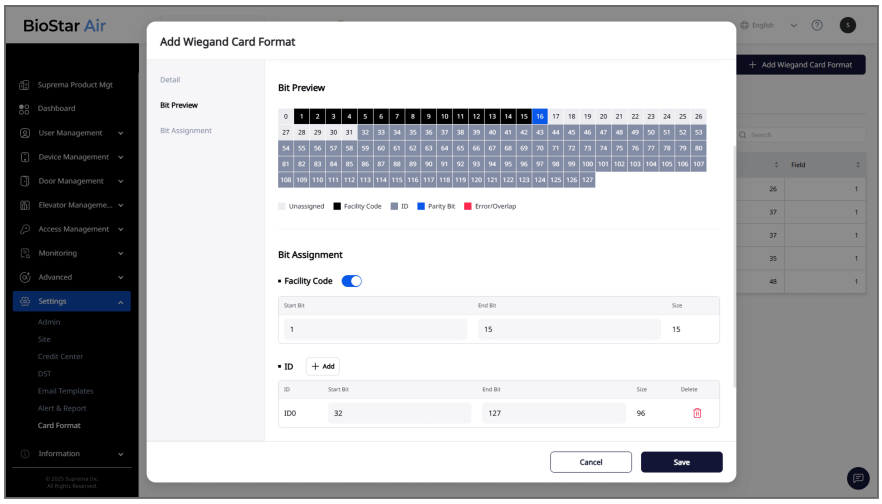
Agregar un formato de tarjeta

Agregue un nuevo formato de tarjeta Wiegand personalizado además de los formatos integrados.

1. Haga clic en **Ajustes** → **Formato de tarjeta** en la barra lateral izquierda.
2. Haga clic en **Añadir formato de tarjeta Wiegand** en la parte superior derecha de la pantalla.
3. Cuando aparezca la ventana **Añadir formato de tarjeta Wiegand**, ingrese el nombre, la descripción opcional y el número total de bits en la sección **Detalle**.



4. Ingrese el número total de bits para activar **Vista previa de bits**, luego configure la asignación de bits en la sección **Asignación de bits**.



La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

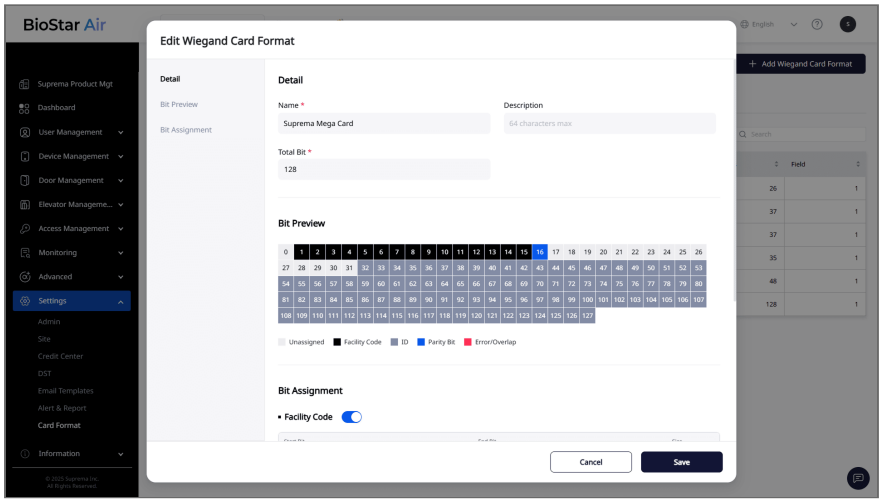
- **Código de instalación**: Haga clic en el interruptor para activar el código de instalación. Ingrese **Bit de inicio** y **Bit de fin**.
- **ID**: Especifique los bits de inicio y fin para agregar uno o más segmentos de ID.
- **Bit de paridad**: Especifique los bits de inicio y fin para agregar bits de paridad impar o par.

5. Haga clic en **Guardar** para agregar el nuevo formato de tarjeta.

Editar formato de tarjeta

Siga estos pasos para editar un formato de tarjeta Wiegand existente.

1. Haga clic en **Ajustes** → **Formato de tarjeta** en la barra lateral izquierda.
2. Haga clic en el formato de tarjeta para editarlo.
3. Cuando aparezca la ventana **Editar formato de tarjeta Wiegand**, edite los campos requeridos.



4. Haga clic en **Guardar** para guardar el formato de tarjeta editado.

Eliminar formato de tarjeta

1. Haga clic en **Ajustes** → **Formato de tarjeta** en la barra lateral izquierda.
2. Haga clic en la casilla de verificación del formato de tarjeta que desea eliminar. Seleccione uno o más formatos de tarjeta.
3. Haga clic en en la parte superior de la lista.
4. Cuando aparezca la ventana de mensaje, haga clic en **Sí**.

> **Información**
> No se pueden eliminar los cinco formatos de tarjeta Wiegand integrados.

Tiempo y asistencia (T&A)

BioStar Air registra los horarios de inicio y fin de turno y de descanso para ofrecer un seguimiento básico de **T&A**, e integrarse con sistemas externos de T&A o exportar los datos. BioStar Air no es un sistema completo de T&A, pero admite el registro de eventos y la integración mediante API con sistemas de nómina y T&A. También genera informes básicos de **horas trabajadas**.

> **Consejo**
> Consulta el siguiente video para ver una guía sobre la configuración de T&A.

Eventos de T&A

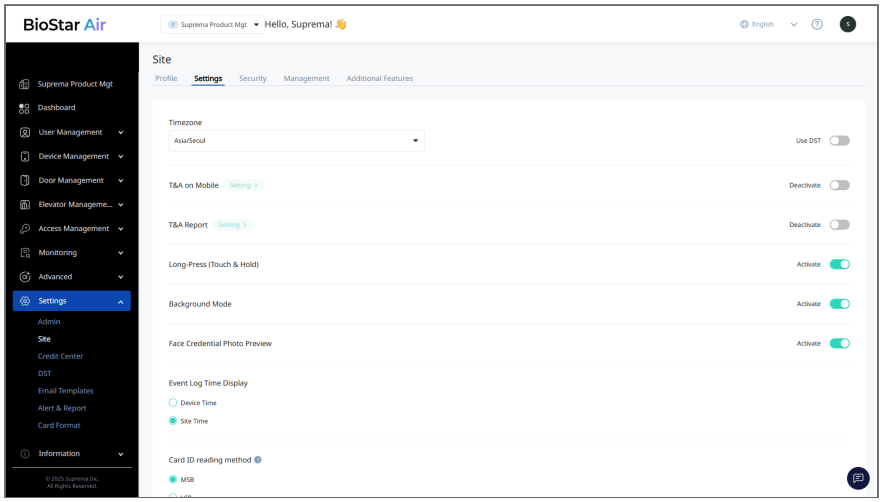
A continuación se indican los eventos de T&A que se pueden registrar. Estos eventos se guardan y pueden exportarse como un archivo CSV o recuperarse mediante la API.

- **Inicio del turno**
- **Fin del turno**
- **Inicio del descanso**
- **Fin del descanso**

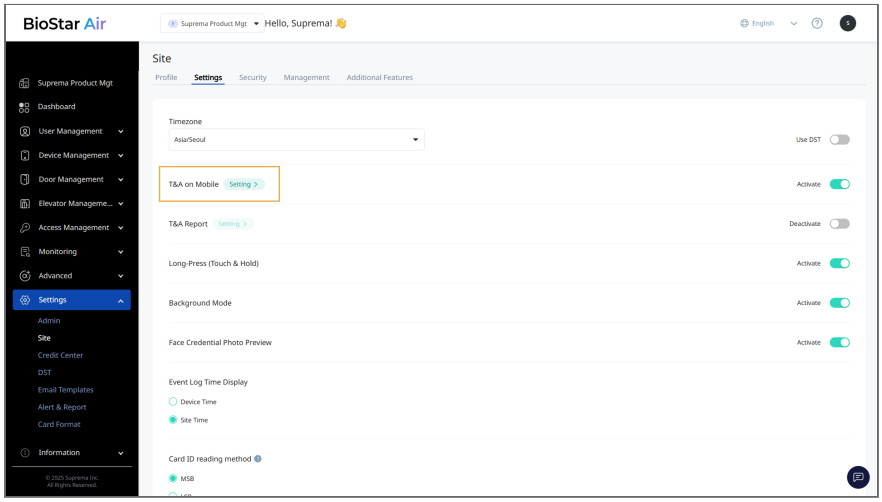
Configurar T&A

Sigue estos pasos para habilitar y configurar los ajustes de T&A.

1. Haz clic en **Ajustes** → **Sitio** en la barra lateral izquierda.
2. Haz clic en **Settings** en la parte superior de la pantalla.

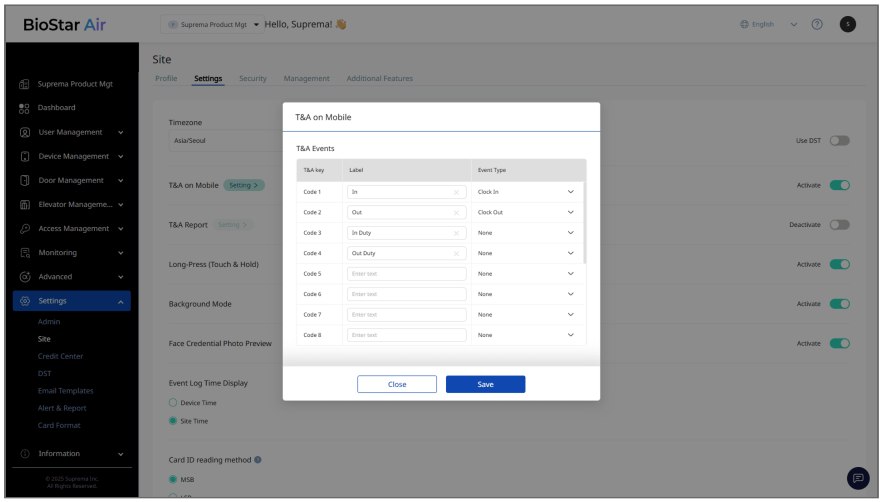


3. Activa **T&A en dispositivos móviles**.
4. Cuando aparezca la ventana de mensajes, haz clic en el botón **Confirmar**.
5. En **T&A en dispositivos móviles**, haz clic en **Ajustes**.



6. Cuando aparezca la ventana **T&A en dispositivos móviles**, establece la etiqueta para **Código T&A**.

> *Por ejemplo: Inicio del turno, Fin del turno, Inicio del descanso, Fin del descanso*

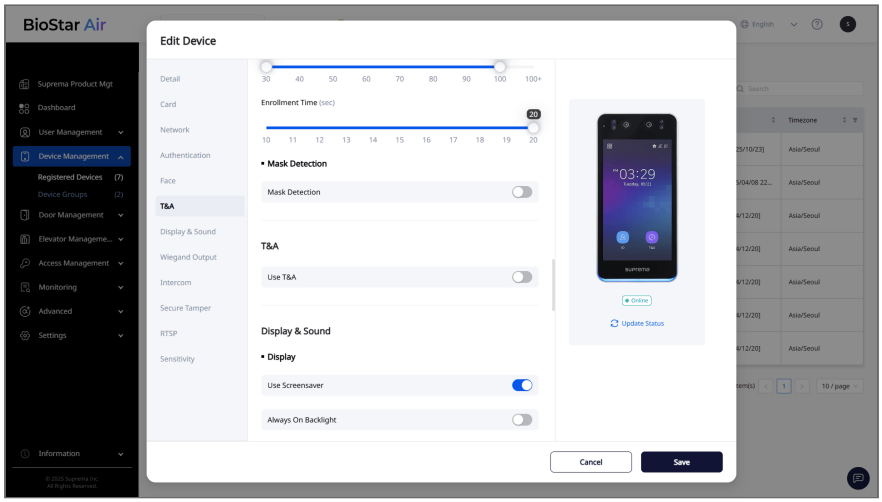


7. Selecciona si el tipo de evento para **Código T&A** es **Entrada** o **Salida**.
8. Haz clic en **Guardar** para guardar la configuración.

Configurar T&A en dispositivos

Tras activar **T&A en dispositivos móviles**, especifica los dispositivos que lo usarán.

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
2. En la lista de dispositivos, haz clic en el dispositivo que deseas configurar para T&A.
3. Cuando aparezca la ventana **Editar dispositivo**, ve a la sección **T&A**.



La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

4. Haz clic en el interruptor **Usar T&A** para habilitar T&A.
5. Haz clic en **Guardar** para guardar la configuración.

- Cuando **Modo T&A** esté configurado en **Móvil**, la opción **Se requiere T&A** estará disponible para la selección obligatoria de T&A durante la autenticación de acceso.
- Las etiquetas de eventos de T&A se gestionan a nivel de **sitio** y no se pueden cambiar por dispositivo.

Modo T&A

Un dispositivo registra eventos de T&A de distintas maneras. Selecciona el modo de asistencia deseado en **Modo T&A**.

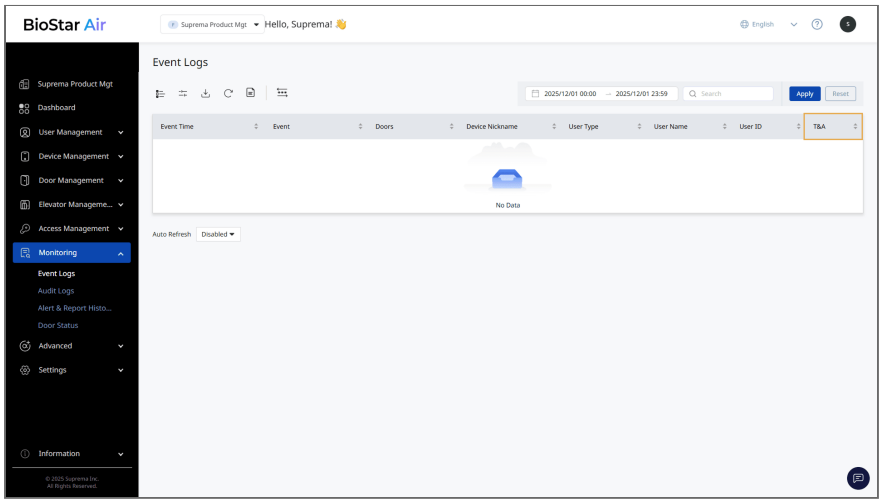
- **Selección manual**: Cuando la tecla de asistencia aparece en la pantalla, el usuario selecciona el evento de asistencia al autenticarse.
- **Por horario**: Registra las horas de entrada y salida según el horario definido. Por ejemplo, los eventos entre las 8:00 a. m. y las 12:00 p. m. se registran como **Entrada**, mientras que los eventos entre la 1:00 p. m. y las 5:00 p. m. se registran como **Salida**.
- **Última opción**: El usuario continúa usando el último evento de asistencia seleccionado.
- **Fijado**: Asigna un código de T&A fijo al dispositivo. Cada autenticación en ese dispositivo registrará el mismo evento de T&A. Usa esta opción para designar el dispositivo para marcar entrada o salida.
- **Móvil**: Requiere que el usuario seleccione un código de T&A antes de la autenticación. El evento de T&A seleccionado se registra en el registro de acceso.

> **Información**
>
> Los modos de gestión de asistencia compatibles pueden variar según el modelo de dispositivo. Para obtener más información, consulta los modos de T&A específicos del dispositivo en Opciones de Configuración de Dispositivos y Paneles.

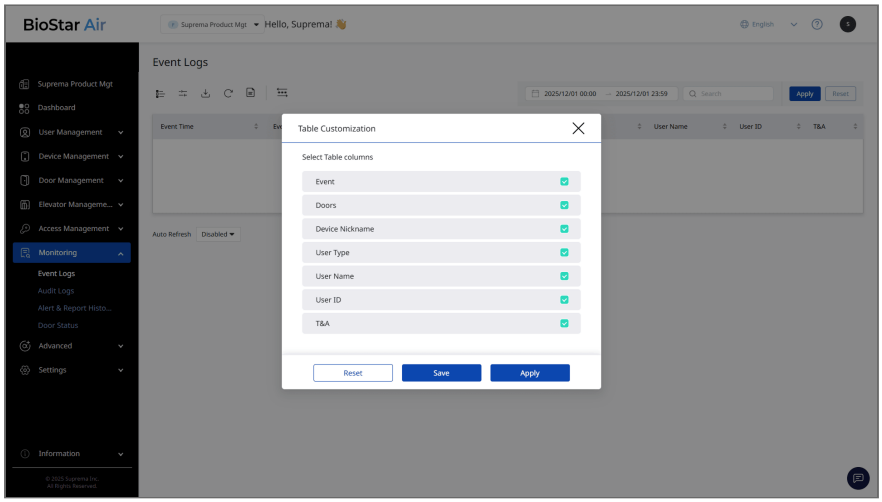
Ver y exportar registros de T&A

Los eventos de T&A se guardan en el registro de eventos y se pueden revisar o exportar a un archivo CSV.

1. Haz clic en **Monitoreo** → **Registros de eventos** en la barra lateral izquierda.
2. Ubica la columna **T&A** en la tabla de registros.



3. Haz clic en ☰ en la parte superior de la tabla de registros para personalizar la vista y mover la columna **T&A** para una mejor visibilidad.



4. Haz clic en y selecciona **Descargar CSV** para descargar los datos como un archivo CSV.

Informe de tiempo y asistencia

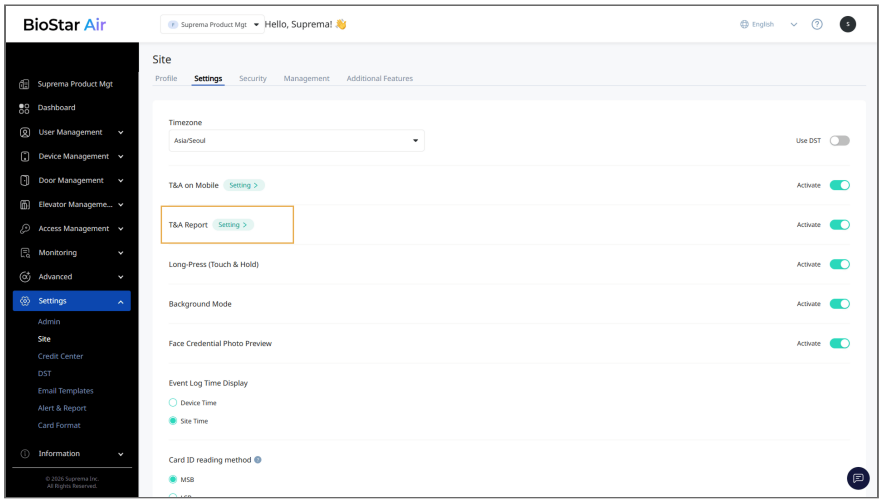
El informe de tiempo y asistencia (T&A) en BioStar Air es un informe sencillo sobre las **horas de trabajo presenciales**. Muestra las horas de entrada y salida de los empleados según los registros de eventos.

Esta función está diseñada para informes básicos sin opciones de configuración complejas. Los sistemas de tiempo y asistencia pueden tener requisitos diversos según la normativa local. Si el informe integrado de tiempo y asistencia no satisface las necesidades de tu organización, utiliza una solución T&A de terceros. Exporta los registros de eventos en **CSV** o integra directamente con software T&A de terceros mediante la API de BioStar Air.

> **Información**
>
> - El informe integrado de tiempo y asistencia es intencionalmente sencillo y puede no cumplir todos los requisitos normativos.
> - Si existen reglas complejas de T&A (por ejemplo, leyes laborales locales o esquemas de turnos), utiliza una solución T&A de terceros.
> - Exporta los registros de eventos en CSV para su procesamiento manual o utiliza la API para integrarlos automáticamente con otros sistemas.

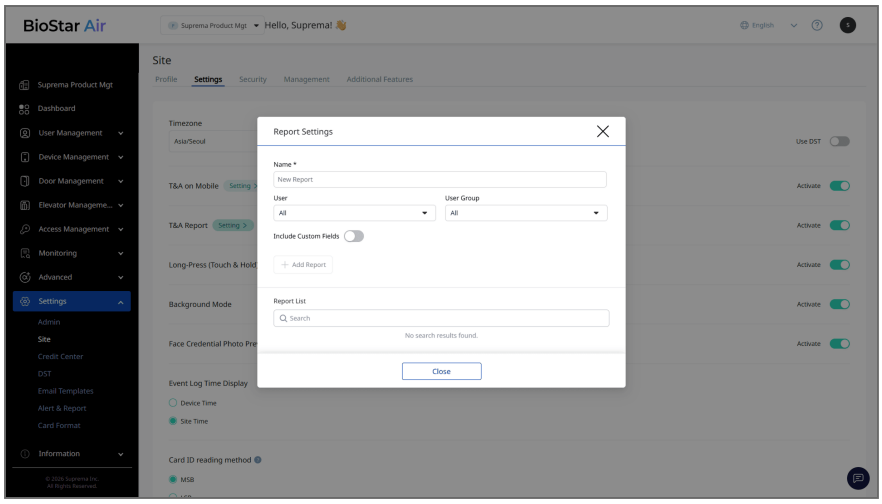
Sigue estos pasos para generar un informe de tiempo y asistencia (T&A).

1. Haz clic en **Ajustes** → **Sitio** en la barra lateral izquierda.
2. En la pestaña **Settings**, haz clic en **Informe de tiempo y asistencia** → **Ajustes**.

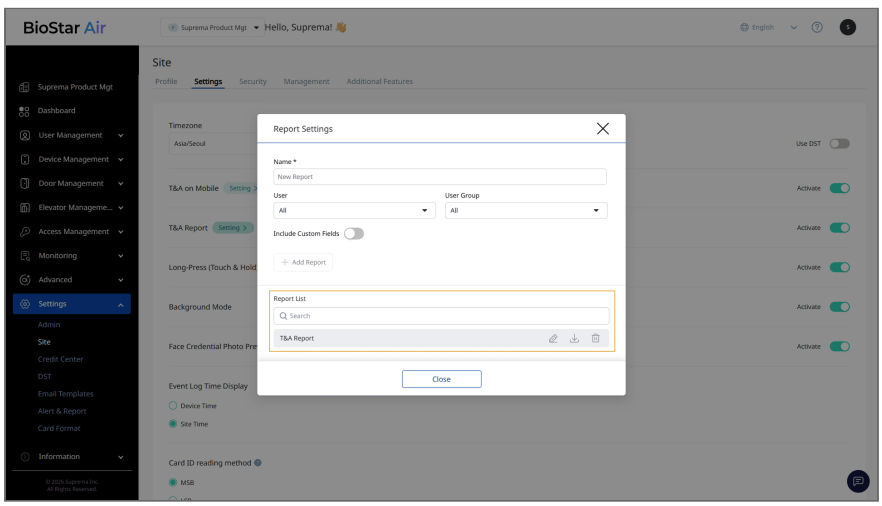


> Haz clic en el interruptor a la derecha para activar **Informe de tiempo y asistencia**.

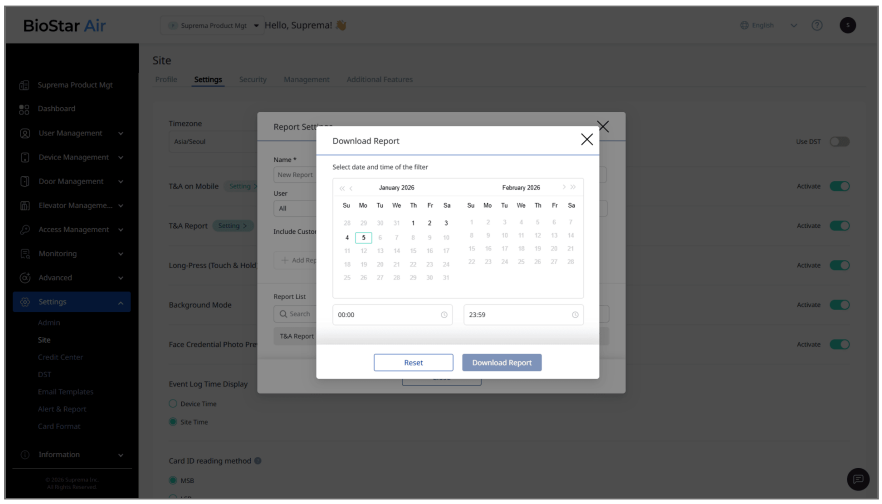
3. Cuando aparezca la ventana **Configuración de informes**, escribe un nombre para el informe.



4. Selecciona los usuarios o grupos de usuarios que deseas incluir en el informe.
5. Haz clic en **Agregar informe**.
6. Se genera un informe descargable en **Lista de informes**.



7. Haz clic en para descargar el informe.
8. Cuando aparezca la ventana **Descargar informe**, selecciona un rango de fecha y hora.



9. Haz clic en **Descargar informe**.

Una vez generado el informe, se envía un enlace de descarga al correo electrónico del administrador. Descarga el informe desde ese correo en formato PDF o CSV.

> **Información**
>
> - Activa **Elemento de plantilla de usuario** y selecciona los elementos de plantilla que quieras incluir en el informe.
> - El informe estará disponible para descargar durante 24 horas después de recibir el correo con el enlace de descarga. Tras ese período, ya no estará disponible.
> - Configura una programación automática en **Alerta e informe**. Para más información, consulta Configurar alertas y informes.

Crear y programar informes

En BioStar Air, los informes se pueden configurar desde diferentes páginas según el tipo. Este artículo explica cómo crear y programar informes de usuarios, de registros de eventos y de auditoría.

Acceder a la configuración de informes

La ruta de acceso varía según el tipo de informe.

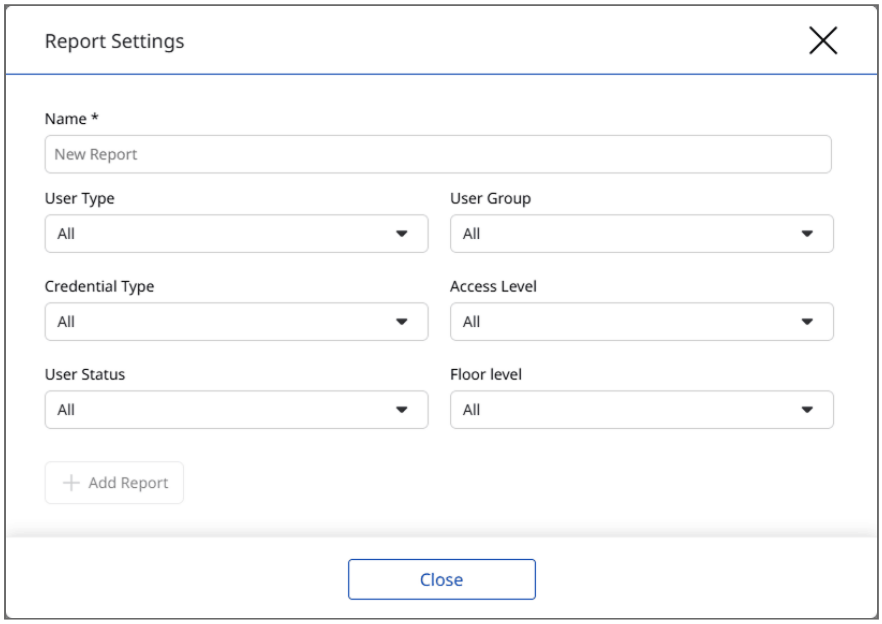
- Informe de usuarios: **Gestión de usuarios** → **Usuarios**
- Informe de registros de eventos: **Monitoreo** → **Registros de eventos**
- Informe de registros de auditoría: **Monitoreo** → **Registros de auditoría**

Haga clic en en la barra de herramientas en la parte superior de la lista. Aparece la página de configuración de informes.

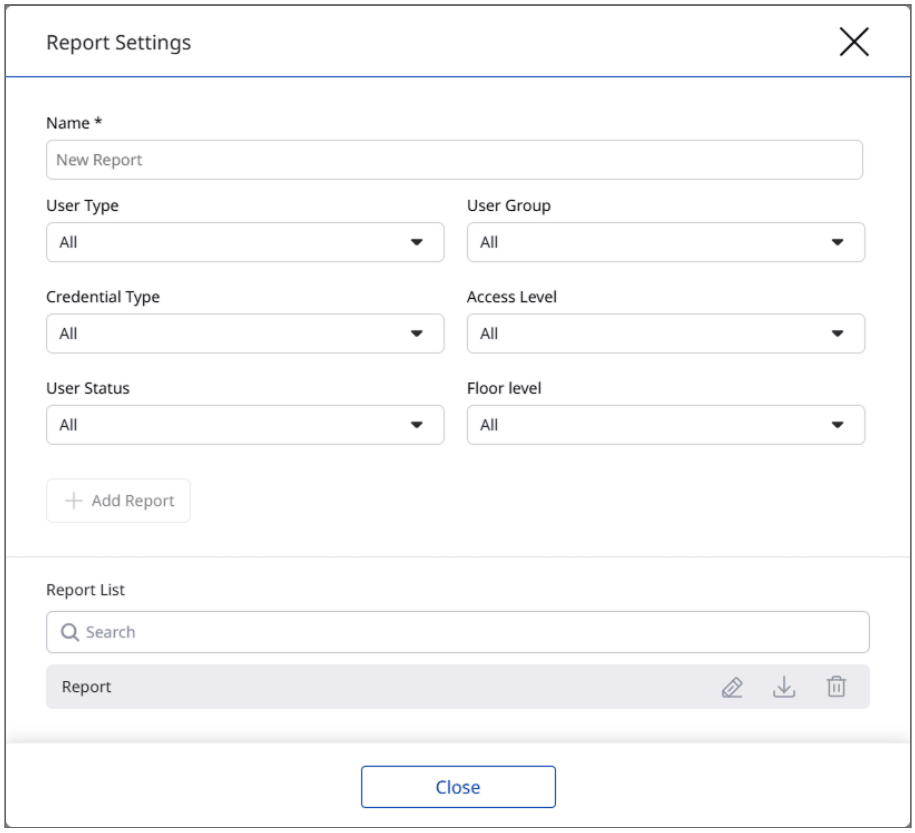
Configurar informes de usuarios

Configure un informe de usuarios para ver el estado actual de los usuarios registrados en el sitio.

1. Vaya a **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. En la barra de herramientas en la parte superior de la lista de usuarios, haga clic en .
3. Cuando aparezca la ventana **Configuración de informes**, ingrese un nombre para el informe.



4. Seleccione los elementos que desea incluir en el informe en cada opción de filtro.
5. Haga clic en **Agregar informe** para guardar el informe.
6. Se crea un **Lista de informes** en la parte inferior y se envía un enlace de descarga al correo electrónico del administrador.



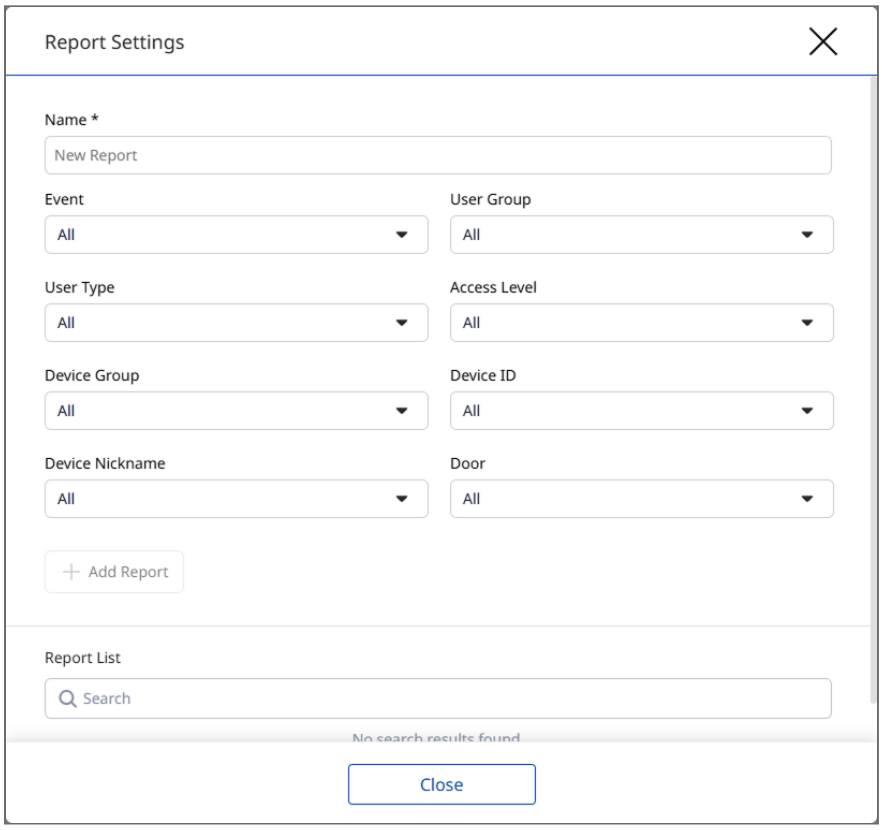
Información

- Haz clic en para editar el informe.
- Haz clic en para exportar el informe en formato PDF o CSV.
- Haz clic en para eliminar el informe.
- Para obtener más información sobre la gestión de usuarios, consulte Usuarios.

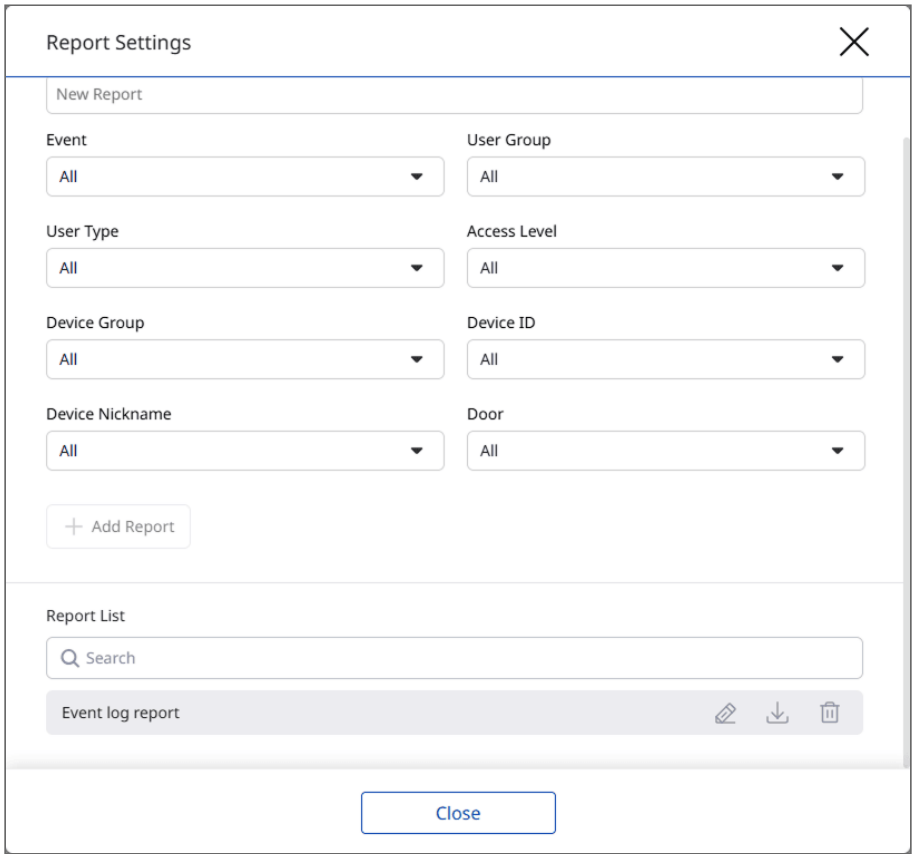
Configurar informes de registros de eventos

Configure un informe sobre los registros de eventos generados en el sitio.

1. Vaya a **Monitoreo** → **Registros de eventos** en la barra lateral izquierda.
2. En la barra de herramientas en la parte superior de la lista de registros, haga clic en .
3. Cuando aparezca la ventana **Configuración de informes**, ingrese un nombre para el informe.



4. Seleccione los elementos que desea incluir en el informe en cada opción de filtro.
5. Haga clic en **Agregar informe** para guardar el informe.
6. Se crea un **Lista de informes** en la parte inferior y se envía un enlace de descarga al correo electrónico del administrador.



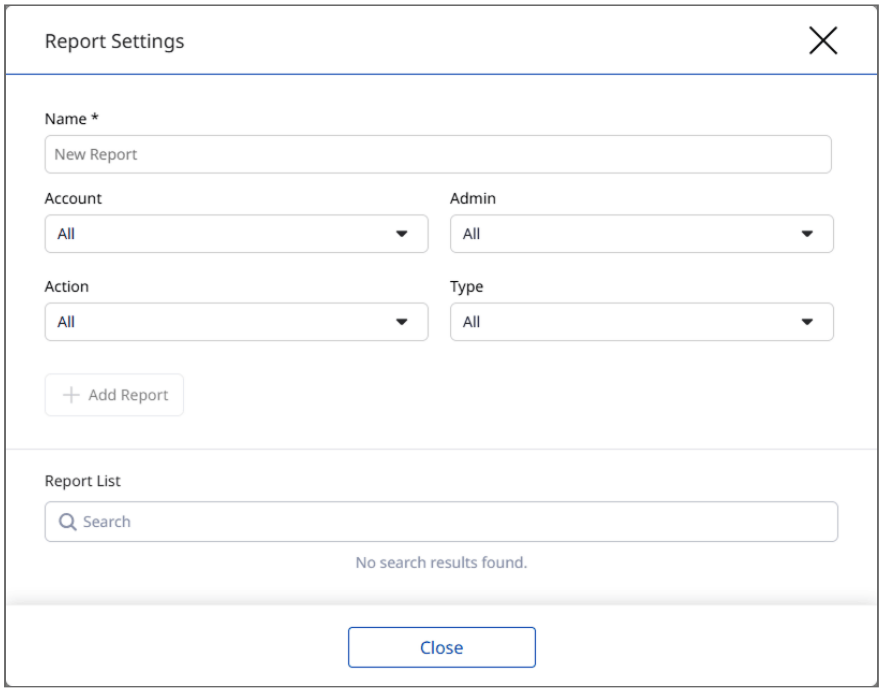
Información

- Haz clic en para editar el informe.
- Haz clic en para exportar el informe en formato PDF o CSV.
- Haz clic en para eliminar el informe.
- Para obtener más información sobre los registros de eventos, consulte Usar registros de eventos.

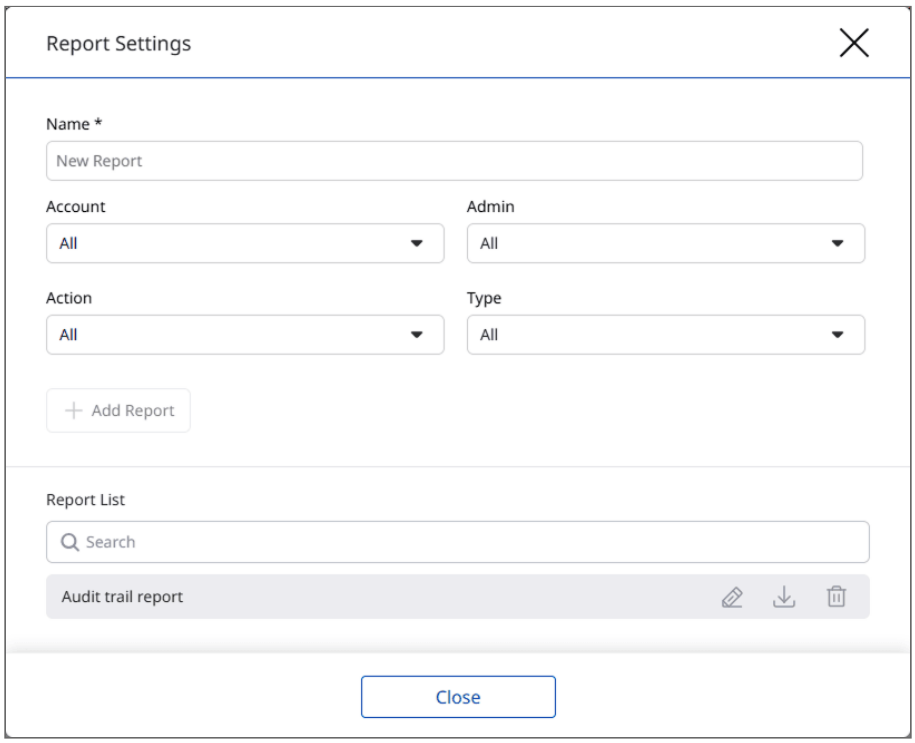
Configurar informes de registros de auditoría

Configure un informe de auditoría sobre los cambios realizados por los administradores.

1. Vaya a **Monitoreo** → **Registros de auditoría** en la barra lateral izquierda.
2. En la barra de herramientas en la parte superior de la lista de registros, haga clic en .
3. Cuando aparezca la ventana **Configuración de informes**, ingrese un nombre para el informe.



4. Seleccione los elementos que desea incluir en el informe en cada opción de filtro.
5. Haga clic en **Agregar informe** para guardar el informe.
6. Se crea un **Lista de informes** en la parte inferior y se envía un enlace de descarga al correo electrónico del administrador.



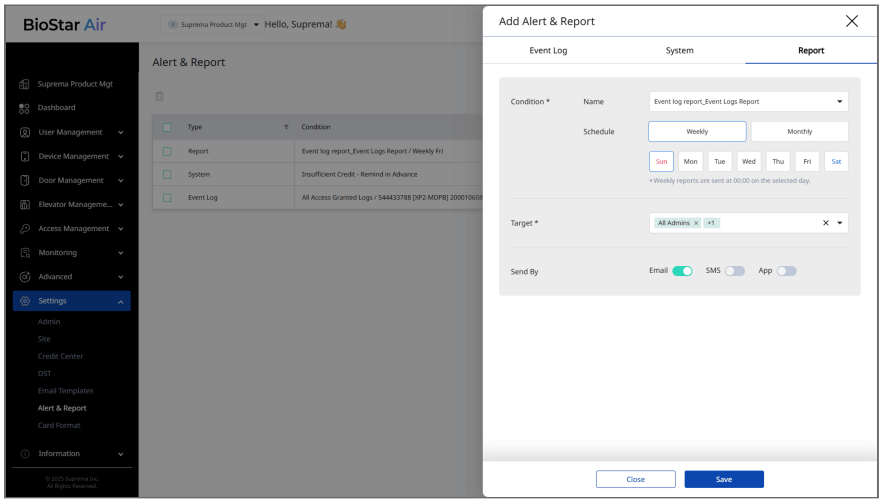
Información

- Haz clic en para editar el informe.
- Haz clic en para exportar el informe en formato PDF o CSV.
- Haz clic en para eliminar el informe.
- Para obtener más información sobre los registros de auditoría, consulte Usar registros de auditoría.

Programar informes

Genere informes automáticamente en intervalos definidos y envíelos a los administradores.

1. Vaya a **Ajustes** → **Alerta e informe** en la barra lateral izquierda.
2. Haz clic en **Agregar alerta e informe** en la parte superior derecha de la pantalla.
3. Cuando aparezca el panel **Agregar alerta e informe**, selecciona la pestaña **Informe**.



4. En la sección **Condición**, seleccione el tipo de informe a generar desde **Nombre**.
5. Seleccione la programación del informe desde **Horarios**.
   - Seleccione **Semanalmente** o **Mensual**.
   - Seleccione la fecha específica para enviar el informe.
   - Todos los informes se envían a la medianoche del día seleccionado.
6. Seleccione los destinatarios en **Objetivo**.
   - Todos los administradores de un nivel específico
   - Administrador individual
7. Selecciona el método de envío en **Enviado por**.
   - Los informes solo pueden enviarse por correo electrónico.
   - No se entregan por SMS ni por notificación push de la app.
8. Después de configurar cada elemento, haz clic en **Guardar** para guardar.

Información

Para obtener más información sobre la programación de la generación de informes, consulte Configurar alertas y informes.

Socios e Instaladores

El Portal de Socios de BioStar Air es una plataforma dedicada para revendedores de valor agregado (VAR) con acuerdos de distribución. Crea sitios de clientes, asigna créditos o configura sitios de federación para gestionar varias ubicaciones de forma centralizada.

Instala hardware en las instalaciones, como intercomunicadores SIP, cámaras IP y escáneres de códigos QR, y configura la red.

Usa el Portal de Socios

El Portal de Socios de BioStar Air es una herramienta exclusiva para revendedores de valor agregado (VAR) que les permite gestionar sitios de clientes, distribuir créditos y supervisar de forma eficiente las funciones administrativas.

Inicia sesión en el Portal de Socios para realizar las siguientes tareas.

- Crea nuevos sitios para clientes.
- Asigna y distribuye créditos a esos sitios.

> **Información**
>
> - El Portal de Socios es solo para revendedores de valor agregado (VAR) y no está destinado a administradores de sitio ni a clientes finales.
> - Si no recibes el correo de invitación, revisa la carpeta de spam o contacta al administrador del Portal de Socios.
> - Verifica que el correo utilizado para el registro sea correcto. Esto no se podrá cambiar más adelante.

> **Consejo**
> Mira el video a continuación para aprender a usar el Portal de Socios de BioStar Air.

Accede al Portal de Socios

El Portal de Socios está disponible solo como portal web. Accede a través del siguiente enlace:
https://partner.biostarair.com/

Regístrate en el Portal de Socios

1. Una vez firmado el acuerdo de distribución, se envía un correo de invitación para que te registres en el Portal de Socios.
2. Haz clic en **Inscribirse** en el correo electrónico.
3. Revisa y acepta la política de privacidad y los términos de uso.
4. Cuando aparezca la pantalla de registro con tu correo prellenado, ingresa la información requerida.

5. Completa el proceso de registro e inicia sesión en el Portal de Socios.

> **Información**
>
> - El Portal de Socios es solo para revendedores aprobados; los administradores del sitio y los usuarios finales no pueden acceder.
> - Si no recibes el correo de invitación, revisa la carpeta de spam o contacta al administrador del Portal de Socios.
> - Verifica que el correo utilizado para el registro sea correcto. Esto no se podrá cambiar más adelante.

Gestiona sitios

Inicia sesión en el Portal de Socios para ver la lista de sitios vinculados a tu cuenta.

- Revisa los detalles del sitio, como el nombre, el país y los créditos asignados.
- Supervisa los costos mensuales de cada sitio para determinar cuándo se necesitan créditos adicionales.
- Rastrear el número de usuarios y dispositivos registrados.
- Agregar notas para el seguimiento interno.

Editar detalles del sitio

Haga clic en el sitio que desea editar en la lista de sitios. En la pantalla de edición del sitio, realice las siguientes acciones.

- Actualizar detalles del sitio, incluida la zona horaria y la información del país.
- Agregar o editar notas relacionadas con el sitio.
- Ajustar el número de créditos asignados.
- Invitar a administradores adicionales al sitio.
- Eliminar el sitio si es necesario.

Rastrear el historial de créditos

Ver todos los cambios de crédito en la sección **Historial de créditos**.

- Establecer un rango de tiempo para revisar los cambios de crédito durante un período específico.
- Supervisar los créditos añadidos recientemente en los sitios de los clientes.

Gestionar administradores

Invitar a otros usuarios al Portal de Socios en la sección **Admin**.

1. Seleccione el nivel de administrador.
2. Ingrese la dirección de correo electrónico del usuario a invitar.
3. Haga clic en **OK** para enviar la invitación.

> **Información**
> No se deben agregar clientes finales al Portal de Socios. Solo los revendedores de valor agregado (VAR) deben encargarse de la creación de sitios y de la asignación de créditos.

Comprender los roles y permisos

El Portal de Socios tiene cuatro niveles de permiso.

- **Observador**: Puede ver la información del sitio pero no puede realizar cambios.
- **Operador**: Puede configurar nuevos sitios y asignar créditos, pero no puede modificar los permisos de administrador ni invitar a nuevos administradores.
- **Administración**: Puede invitar y gestionar a otros administradores, pero no puede eliminar a usuarios de nivel master.
- **Maestro**: Tiene control total del Portal de Socios, incluyendo la gestión de usuarios, la creación de sitios y la asignación de créditos. Solo los usuarios de nivel master pueden activar inicialmente la cuenta del Portal de Socios.

> **Información**
> Configura y activa una cuenta principal antes de que los usuarios con otros niveles de permiso puedan acceder al portal.

Administrar sitios federados

BioStar Air ofrece **sitios federados**, que permiten a un sitio primario gestionar sin problemas múltiples subsitios. Esta función es ideal para edificios con varios inquilinos u organizaciones con múltiples sucursales y proporciona control centralizado mediante la gestión distribuida de accesos.

Al aprovechar la función de sitios federados de BioStar Air, los administradores gestionan eficazmente el acceso en entornos complejos y ofrecen una experiencia segura, escalable y optimizada para todas las partes interesadas.

¿Qué es un sitio federado?

Los sitios federados admiten una estructura jerárquica en la que un **sitio primario** gestiona uno o más **subsitios**. Un administrador del sitio primario—denominado **administrador de la federación**—puede acceder y administrar directamente los subsitios desde la interfaz de BioStar Air.

Los sitios federados son útiles en las siguientes situaciones.

Edificio con múltiples inquilinos

Por ejemplo, en un edificio comercial donde cada piso está ocupado por una empresa diferente, configure el sistema de la siguiente manera.

- **Cuenta maestra** del edificio
- **Subcuenta** para cada empresa inquilina

Esta configuración autoriza únicamente a los empleados que tienen acceso a un piso específico, lo que simplifica la gestión del edificio.

Organización con múltiples sucursales

Una empresa con oficinas en varias ubicaciones puede configurar el sistema de la siguiente manera.

- Gestione la configuración global mediante una **cuenta maestra**
- Cree una **subcuenta** para cada sucursal

Por ejemplo, una empresa con diez oficinas en todo el mundo puede utilizar una estructura federada para agilizar la gestión.

Configurar sitios federados

1 Acceder al Portal de Socios

URL: https://partner.biostarair.com

- Solo socios e instaladores pueden usar el Portal de Socios de BioStar Air.
- Los clientes finales deben ponerse en contacto con un instalador para configurar esta función.

2 Crear sitio primario

1. Inicia sesión en el Portal de Socios.
2. Haz clic en y selecciona en .
   - Este paso **debe** realizarse al configurar el sitio por primera vez.
   - Un sitio estándar no puede convertirse en un sitio federado más adelante.
3. Agrega un administrador del sitio federado en la misma pantalla.
   - Un **administrador del sitio federado** agregado en el Portal de Socios puede acceder al sitio principal y a todos los subsitios.
   - Un **administrador general** agregado en BioStar Air solo puede administrar sitios individuales.

3 Agregar subsitios

1. Cuando el sitio principal se establece como sitio federado, el mostrará una opción para crear subsitios.
2. Haz clic en y configúralo como cualquier otro sitio.

Consideraciones importantes

Gestión de usuarios y dispositivos

- Agrega usuarios y dispositivos por separado a cada subsitio.
- Un dispositivo solo puede registrarse en un sitio a la vez. Selecciona el sitio principal o un subsitio.

Uso del sitio principal

- Ciertos clientes usan el sitio principal únicamente como punto de acceso para la gestión de subsitios y no registran usuarios ni dispositivos en el sitio principal.
- **Ejemplo 1**: Una empresa con tres sucursales configura un sitio principal sin dispositivos y crea un subsitio para cada sucursal.
- **Ejemplo 2**: Una empresa con sede central y tres sucursales registra usuarios y dispositivos en la sede central (el sitio principal) y crea subsitios para las sucursales.

Facturación

- La facturación se calcula según el número de dispositivos registrados (lectores) por sitio.
- No hay costo adicional por crear un sitio principal sin dispositivos registrados.

Invitar administradores de socios.

Guía para invitar cuentas de administradores de socios, asignar roles y gestionar permisos en el Portal de socios. Los administradores de socios controlan el acceso a los sitios de los clientes para mejorar la seguridad y la eficiencia operativa.

A los administradores de socios se les asigna uno de 4 roles: Observador, Operador, Administrador o Administrador principal; cada uno tiene permisos de acceso distintos. Este documento compara los permisos de cada rol y ofrece instrucciones paso a paso, desde invitar cuentas de administrador hasta gestionar permisos, bloquear/desbloquear cuentas y eliminar cuentas.

Comprender los roles y permisos de administrador

A los administradores del Portal de socios se les asigna uno de los siguientes 4 roles.

- **Observador**: Puede ver la información del sitio pero no puede realizar cambios.
- **Operador**: Puede configurar nuevos sitios y asignar créditos, pero no puede modificar los permisos de administrador ni invitar a nuevos administradores.
- **Administración**: Puede invitar y gestionar a otros administradores, pero no puede eliminar a usuarios de nivel master.
- **Maestro**: Tiene control total del Portal de Socios, incluyendo la gestión de usuarios, la creación de sitios y la asignación de créditos. Solo los usuarios de nivel master pueden activar inicialmente la cuenta del Portal de Socios.

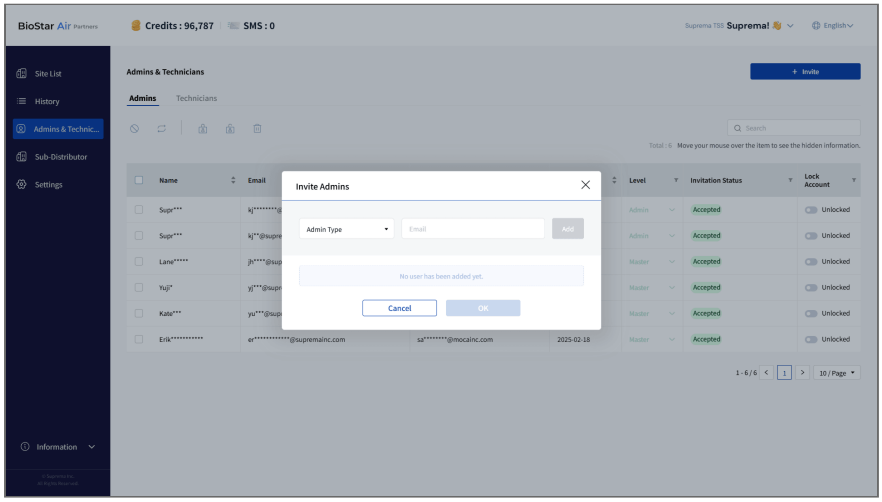
> **Información**
> Configura y activa una cuenta principal antes de que los usuarios con otros niveles de permiso puedan acceder al portal.

Invitar administradores

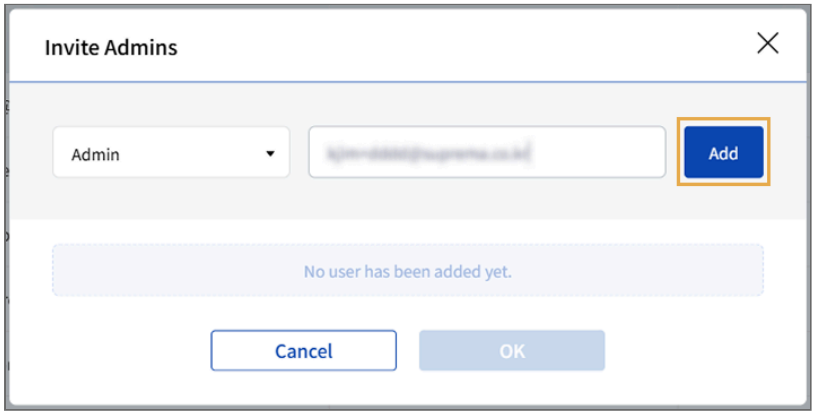
Sigue los pasos a continuación para invitar administradores.

1. Inicie sesión en el Partner Portal con una cuenta asignada el rol **Administración** o superior.
2. Haz clic en en la barra lateral izquierda.

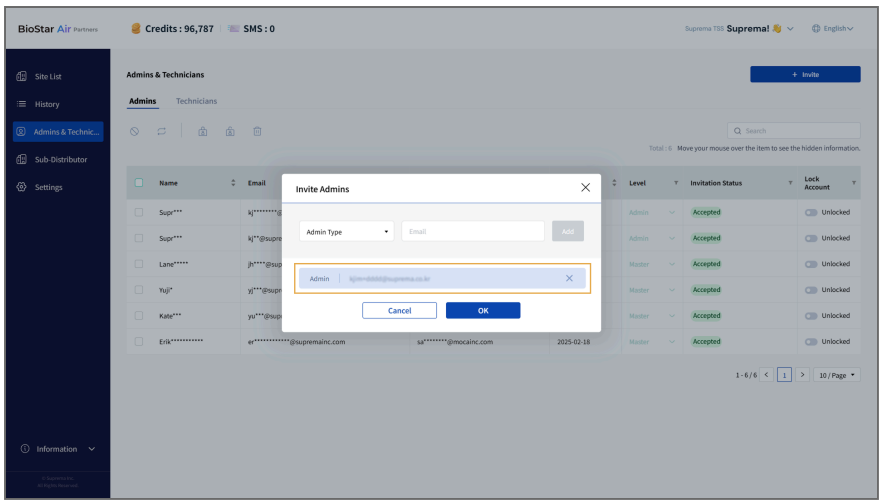
3. Haz clic en en la parte superior derecha de la pantalla.
4. Cuando aparezca la ventana , seleccione el rol de administrador a invitar en el campo .



5. Ingrese la dirección de correo electrónico del administrador a invitar.
6. Haga clic en cuando esté activo.



7. Los administradores agregados aparecen debajo del campo de dirección de correo electrónico. Repite los pasos 4–6 para invitar administradores adicionales.



8. Después de agregar todos los administradores, haga clic en **Aceptar**.
9. Cuando aparezca el mensaje de confirmación, haz clic en **Confirmar**.

> **Información**
>
> Invitar administradores al Portal de socios no otorga acceso a los sitios; invítalos en cada sitio por separado.

Estado de la invitación

Después de invitar administradores, consulta el estado de la invitación de cada cuenta invitada en la lista de administradores.

Registro pendiente

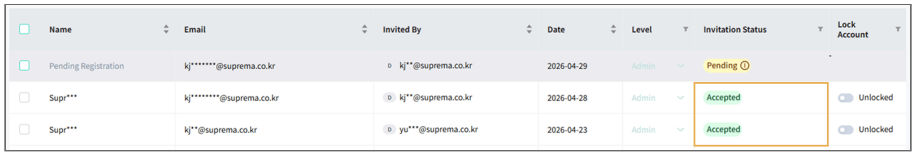
Los administradores invitados permanecen en el estado hasta que acepten la invitación por correo electrónico y activen su cuenta. Los administradores invitados pueden hacer clic en el enlace del correo para registrar su cuenta o iniciar sesión en el Portal de socios.



> **Información**
>
> Los administradores invitados tienen hasta 7 días para aceptar la invitación; después de 7 días la invitación expira y el estado cambia a . Si la invitación expira, reenvía el enlace de invitación para que la cuenta invitada pueda registrarse de nuevo. Para más información sobre reenvío de enlaces de invitación, consulta Reenviar enlace de invitación.

Registro completado

Cuando un administrador invitado acepta la invitación por correo electrónico y completa el registro, el estado de la invitación cambia a .



Invitación revocada

Cancela la invitación si la dirección de correo del administrador invitado es incorrecta o si la invitación ya no es necesaria. Si cancelas la invitación, su estado cambiará a . Para más información sobre cómo revocar invitaciones de administrador, consulta Invitación revocada.

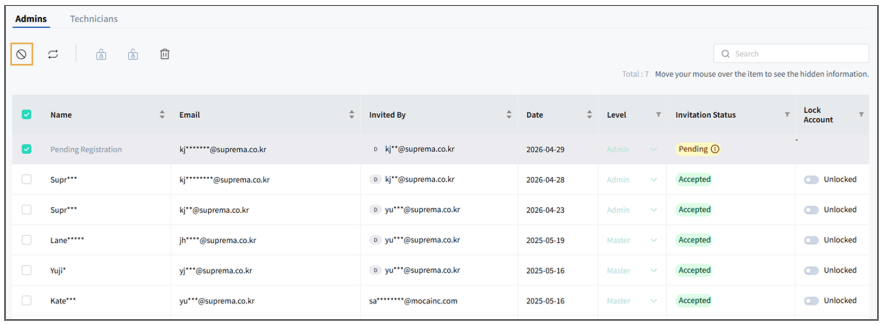


Invitación revocada

Cancela una invitación si un socio ingresó incorrectamente la dirección de correo de un administrador o si la invitación ya no es necesaria. Tras cancelar la invitación, el usuario no podrá usar el enlace para registrarse.

1. En la lista de administradores, haz clic en la casilla junto al administrador cuyo estado de invitación sea . Selecciona 1 o más administradores.

2. Haz clic en ⃠ en la parte superior izquierda de la lista de administradores.



> Solo los administradores con el estado pueden tener su invitación cancelada.

3. Si aparece un mensaje emergente, revíselo y haga clic en .

4. Cuando aparezca el mensaje de éxito por la invitación cancelada, haga clic en **Cerrar**.

En la lista de administradores, el estado de invitación de un administrador cuya invitación fue cancelada cambia a .

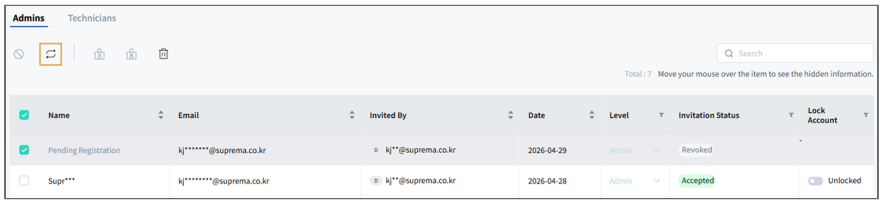


Reenviar enlace de invitación

Reenvía el enlace de invitación si un administrador invitado no recibió el correo, lo perdió o si el enlace ha expirado.

1. En la lista de administradores, haz clic en la casilla junto a cualquier administrador cuyo estado de invitación sea , o . Selecciona 1 o más administradores.

2. Haz clic en ⟲ en la parte superior izquierda de la lista de administradores.



3. Si aparece un mensaje emergente, revíselo y haga clic en .

4. Cuando aparezca el mensaje de éxito por reenvío del enlace de invitación, haga clic en **Cerrar**.

En la lista de administradores, el estado de invitación de un administrador cuyo enlace fue reenviado cambia a .



Gestión de administradores

Después de que un administrador invitado acepte la invitación por correo y complete el registro, gestiona al administrador desde la lista de administradores. Bloquea o desbloquea la cuenta de un administrador, o cambia su rol. Si un

administrador ya no es necesario, elimina su cuenta.

Bloquear o desbloquear una cuenta de administrador

Bloquea o desbloquea una cuenta usando la opción para administradores que han aceptado la invitación por correo y completado el registro. Cuando una cuenta está bloqueada, el administrador no puede iniciar sesión en el Portal de socios. La información de la cuenta se conserva para poder reactivarla más adelante si es necesario.

Para administradores bloqueados, la columna muestra ; para administradores desbloqueados muestra .



Información

- Las cuentas de los administradores que completaron el registro están desbloqueadas por defecto.
- Las cuentas con el rol **Administración** o superior no se pueden bloquear ni desbloquear.

Bloquear o desbloquear a un administrador individual

Haz clic en el interruptor de la columna de la lista de administradores para bloquear o desbloquear cuentas de administradores individuales.

1. Haz clic en el interruptor de la columna de la lista de administradores.



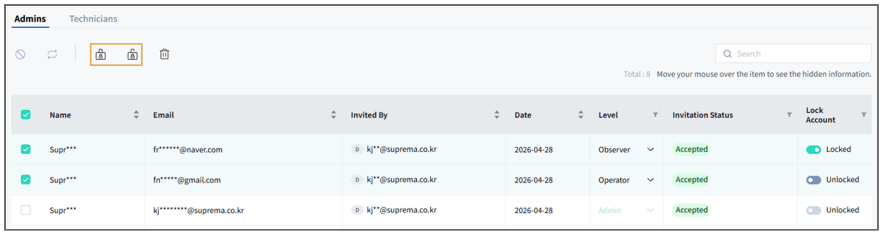
2. Si aparece un mensaje emergente, revíselo y haga clic en **Confirmar**.

Bloquear o desbloquear varios administradores

Para bloquear o desbloquear varias cuentas de administrador a la vez, selecciónalas en la lista de administradores.

1. En la lista de administradores, haz clic en la casilla del administrador que quieras bloquear o desbloquear. Selecciona 1 o más administradores.

2. Haz clic en o en la esquina superior izquierda de la pantalla.



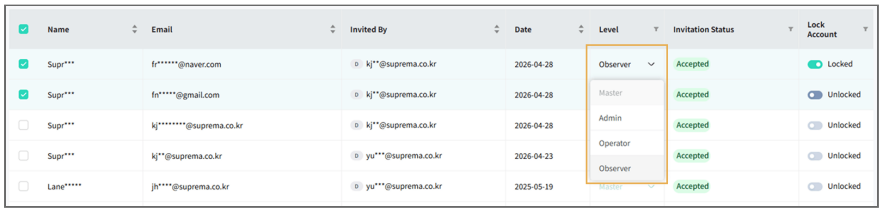
3. Si aparece un mensaje emergente, revíselo y haga clic en .

4. Cuando aparezca el mensaje de éxito que confirma el bloqueo o desbloqueo de la cuenta, haz clic en **Cerrar**.

Cambiar el rol de administrador

Cambia el rol de un administrador. Para más información sobre los roles de administrador, consulta Comprender los roles y permisos de administrador.

1. En la lista de administradores, haz clic en la columna del administrador cuyo rol quieras cambiar.



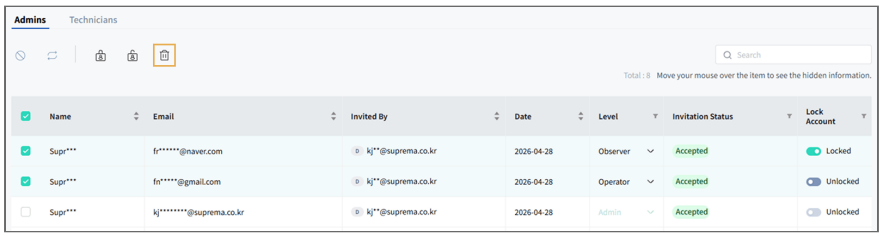
2. Selecciona el permiso que deseas cambiar de la lista.
3. Cuando aparezca un mensaje emergente, haz clic en **Confirmar**.

Los permisos del usuario se actualizan en la lista de administradores.

Eliminar cuenta de administrador

Elimina una cuenta de administrador cuando ya no sea necesaria. Eliminar una cuenta de administrador impide que el administrador inicie sesión en el Portal de socios, y la información de la cuenta se elimina de forma permanente y no se puede restaurar.

1. En la lista de administradores, haz clic en la casilla del administrador que quieras eliminar. Selecciona 1 o más administradores.
2. Haz clic en en la parte superior izquierda de la pantalla.



3. Si aparece un mensaje emergente, revíselo y haga clic en **Confirmar**.
4. Cuando aparezca el mensaje de éxito de eliminación de la cuenta, haz clic en **Cerrar**.

Las cuentas de administrador eliminadas ya no aparecen en la lista de administradores.

Invitar a un administrador del sitio.

Los socios pueden invitar administradores a los sitios de clientes y configurar permisos. Administre niveles de acceso granulares para cada administrador para garantizar la seguridad y la eficiencia operativa de los sitios de los clientes.

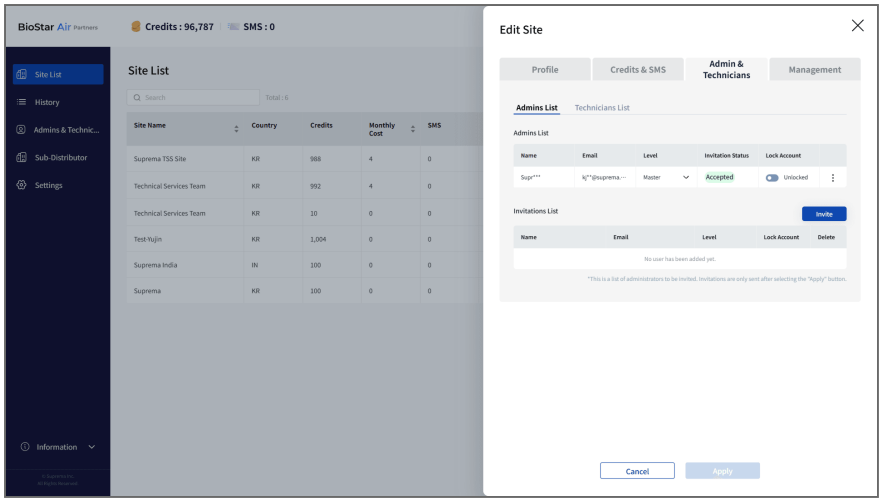
Información

- Para obtener más información sobre los niveles y roles de administrador, consulte Administrar cuentas y roles de administradores.
- Para obtener más información sobre cómo invitar administradores y asignar roles en el portal BioStar Air, consulte Administrar cuentas y roles de administradores.

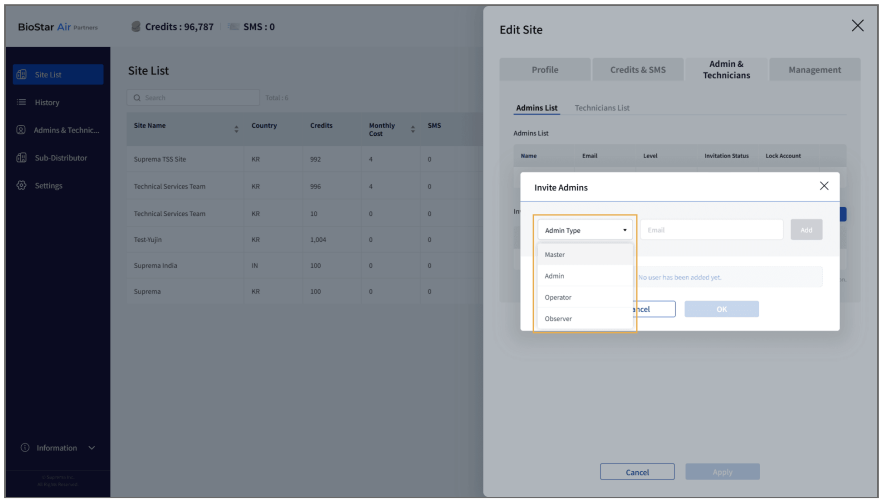
Invitar a un administrador del sitio

Aprenda a invitar administradores a los sitios de clientes y a configurar permisos en el Portal de Socios.

1. Inicie sesión en el Partner Portal con una cuenta asignada el rol **Administración** o superior.
2. Haga clic en en la barra lateral izquierda.
3. En la lista de sitios, haga clic en el sitio al que desea asignar un administrador.
4. Cuando aparezca el panel , haga clic en → en ese orden.

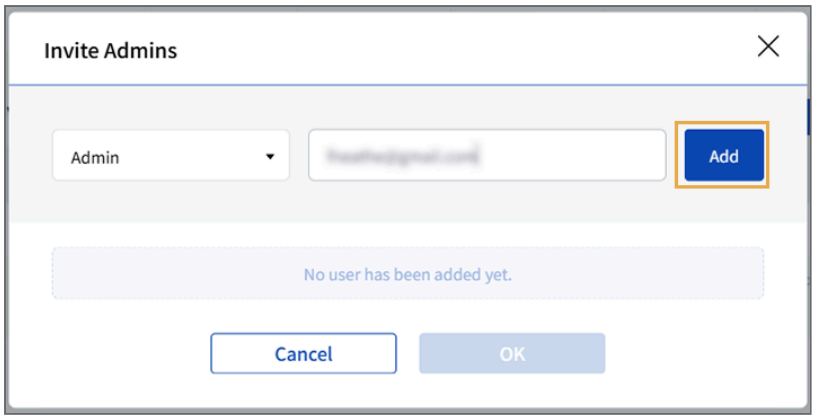


5. Haga clic en .
6. Cuando aparezca la ventana , seleccione el rol de administrador a invitar en el campo .

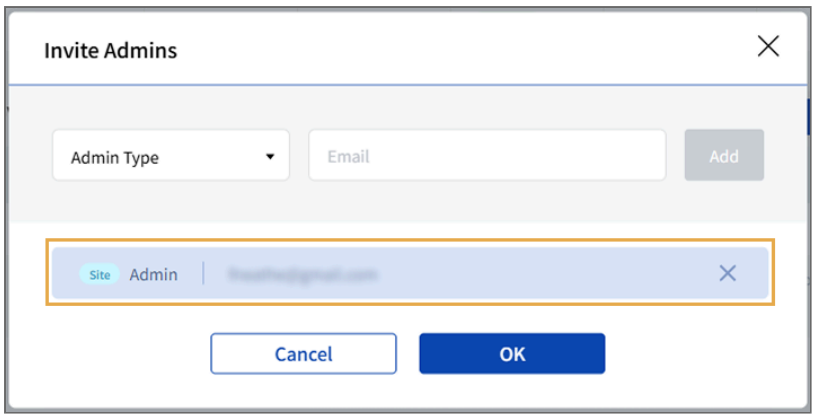


7. Ingrese la dirección de correo electrónico del administrador a invitar.

8. Haga clic en cuando esté activo.



9. Los administradores agregados aparecen debajo del campo de dirección de correo electrónico. Repita los pasos 6–8 para invitar administradores adicionales.



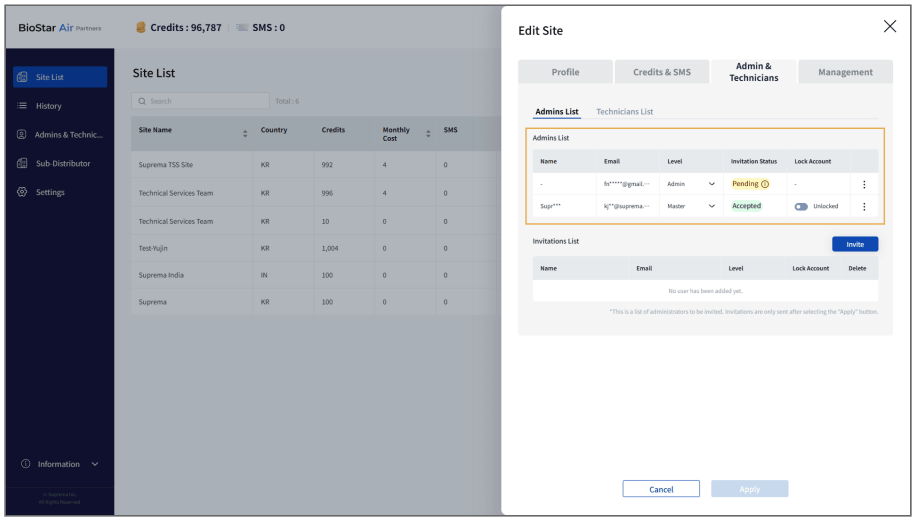
10. Después de agregar todos los administradores, haga clic en **Aceptar**.
11. Revise los administradores agregados en y, a continuación, haga clic en para enviar el correo de invitación.
12. Cuando aparezca el mensaje de éxito, haga clic en **Confirmar**.

Verificar el estado de la invitación

Verifique el estado de invitación de los administradores invitados al sitio. El estado de invitación es hasta que el administrador invitado acepte el correo de invitación. Los administradores invitados tienen hasta 7 días para aceptar la invitación; después de 7 días la invitación expira y el estado cambia a .

1. En la lista de sitios, haga clic en el sitio donde invitó a un administrador.
2. Cuando aparezca el panel , haga clic en → en ese orden.
3. Verifique el estado de la invitación en .

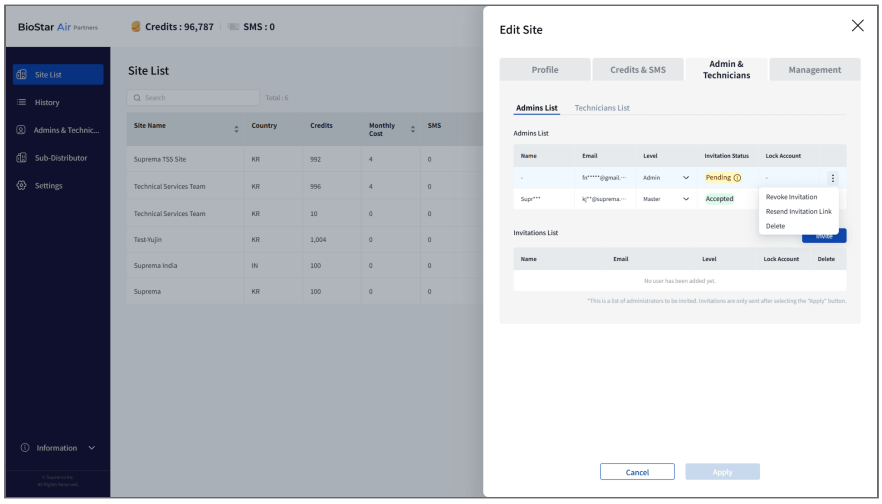
Cuando un administrador invitado completa la inscripción en el sitio, el estado cambia de a .



Invitación revocada

Cancele la invitación si la dirección de correo electrónico del administrador invitado se ingresó incorrectamente o si el administrador ya no es necesario.

1. En la lista de sitios, haga clic en el sitio donde invitó a un administrador.
2. Cuando aparezca el panel , haga clic en → en ese orden.
3. En , para cualquier administrador con estado , haga clic en ⋮ en el extremo derecho.



4. Haga clic en en el menú emergente.
5. Si aparece un mensaje emergente, revíselo y haga clic en .
6. Cuando aparezca el mensaje de éxito por la invitación cancelada, haga clic en **Cerrar**.

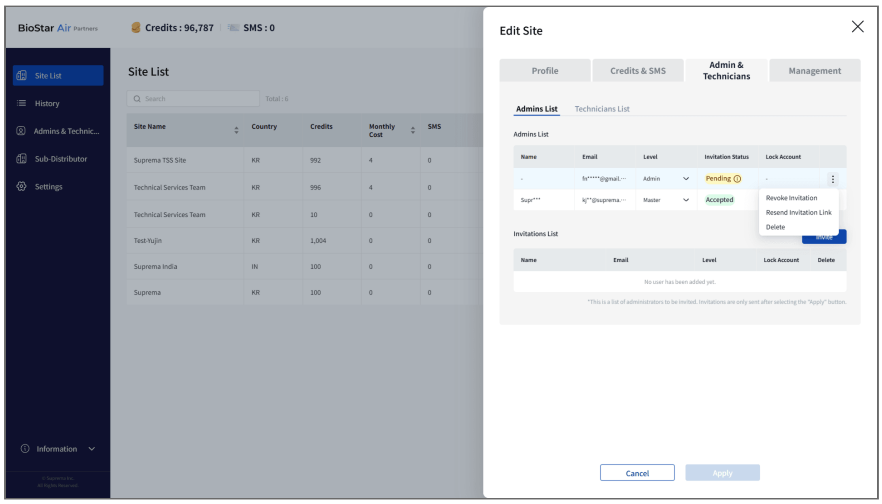
Cuando se cancela una invitación, el estado de la invitación cambia de a .

Reenviar enlace de invitación

Reenvíe el enlace de invitación si el administrador invitado no recibió el correo de invitación o lo perdió.

1. En la lista de sitios, haga clic en el sitio donde invitó a un administrador.

2. Cuando aparezca el panel , haga clic en → en ese orden.
3. En , para administradores con estado , o , haga clic en ⋮ en el extremo derecho.

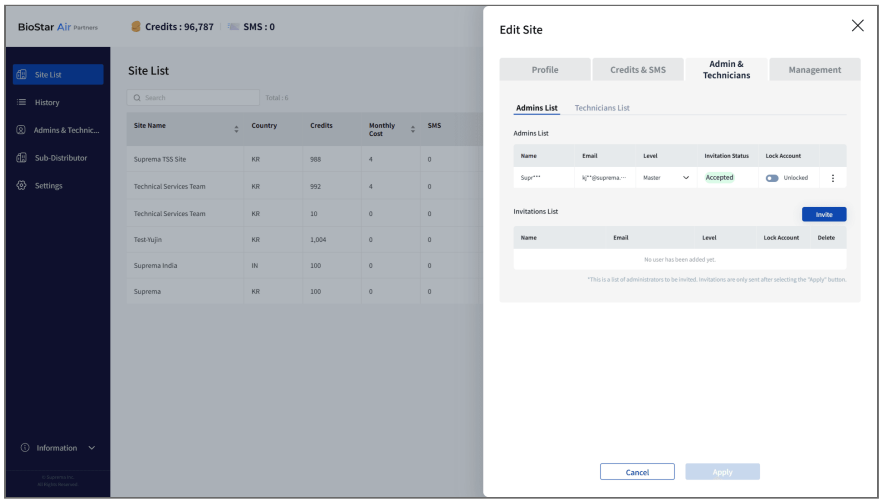


4. Haga clic en en el menú emergente.
5. Si aparece un mensaje emergente, revíselo y haga clic en .
6. Cuando aparezca el mensaje de éxito por reenvío del enlace de invitación, haga clic en **Cerrar**.

Bloquear o desbloquear una cuenta de administrador

Bloquear o desbloquear cuentas de administrador asignadas a un sitio.

1. Haga clic en en la barra lateral izquierda.
2. En la lista de sitios, haga clic en el sitio para administrar el acceso de administradores.
3. Cuando aparezca el panel , haga clic en → en ese orden.

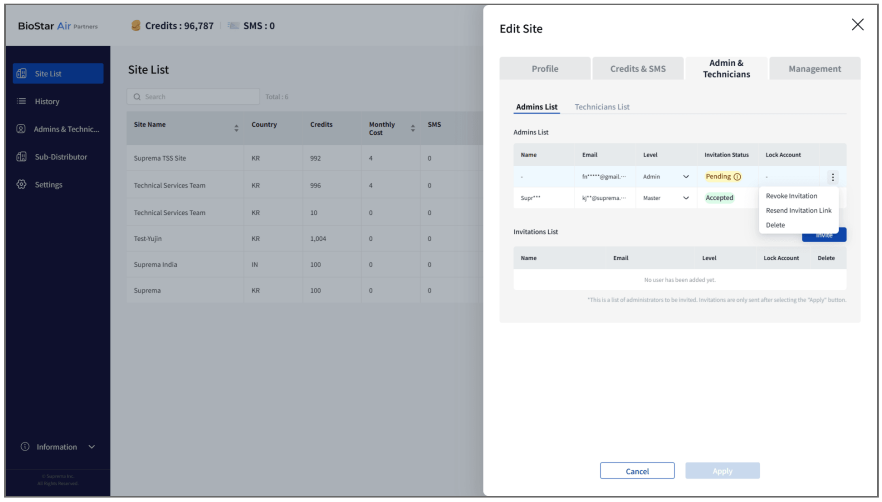


4. En , haga clic en el botón de alternancia en la columna para bloquear o desbloquear una cuenta de administrador.
5. Haz clic en en la parte inferior para aplicar los cambios.

Eliminar administrador

Elimine la cuenta de un administrador invitado. Cuando se elimina la cuenta de un administrador, ya no podrá iniciar sesión en el sitio y su acceso se revocará por completo. Una vez eliminada la cuenta de administrador, no se puede recuperar.

1. En la lista de sitios, haga clic en el sitio donde invitó a un administrador.
2. Cuando aparezca el panel , haga clic en → en ese orden.
3. En , haga clic en ⋮ al extremo derecho del administrador que desea eliminar.



4. Haga clic en **Borrar** en el menú emergente.
5. Si aparece un mensaje emergente, revíselo y haga clic en **Confirmar**.
6. Cuando aparezca el mensaje de éxito que confirma la eliminación del administrador, haga clic en **Cerrar**.

Administrar técnicos de socios

Las cuentas de técnico permiten que socios e instaladores brinden soporte a sitios de clientes sin compartir una cuenta de administrador. Los socios invitan a técnicos a través del portal de socios y los asignan a sitios específicos. Tras la asignación, los clientes y los administradores del sitio pueden activar o actualizar los permisos de los técnicos en el portal de administración de BioStar Air. Esto permite controlar el acceso de soporte de los socios, mantener registros de auditoría y limitar el acceso únicamente a los sitios necesarios.

Beneficios de la gestión de técnicos

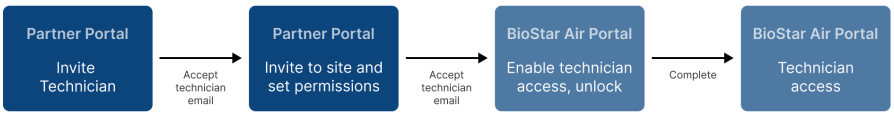
Las cuentas de técnico están diseñadas para profesionales que realizan instalación, mantenimiento y soporte técnico en varios sitios de clientes. Los socios pueden definir el rol y nivel de permisos de cada técnico para implementar lo siguiente.

- **Mayor seguridad**: Reduce el riesgo de acceso no autorizado eliminando cuentas de administrador compartidas
- **Cumplimiento**: Cumple con las normas de privacidad; opción de excluir el acceso a los datos de los usuarios
- **Gestión eficiente**: Rastrea y audita las actividades de cada técnico en varios sitios
- **Control de permisos flexible**: Permisos granulares por técnico y por sitio

Limitaciones

- **Se requieren cuentas separadas para el portal de socios y el portal de BioStar Air**: Cada portal requiere un proceso de registro separado. Las contraseñas no se sincronizan entre portales.
- **Sin caducidad ni control de acceso por tiempo**: El acceso de los técnicos no caduca automáticamente. Los administradores del sitio deben bloquear o eliminar el acceso manualmente.
- **Permisos de acceso fijos**: Solo hay 4 niveles de permiso predefinidos. No se pueden crear roles personalizados ni permisos más granulares.
  - **Ninguna** / **Solo dispositivos** / **Completo excluyendo usuarios** / **Completo incluyendo usuarios**
- **Se requiere activación por el cliente al asignar técnicos**: Los técnicos asignados por los socios deben ser desbloqueados por el administrador del sitio antes de poder acceder al sitio. La falta de comunicación clara puede retrasar el soporte o la instalación.
- **Sin asignación masiva**: Los técnicos deben asignarse individualmente por sitio.
- **Los roles de técnico y administrador no pueden compartir la misma dirección de correo electrónico**: Una dirección de correo electrónico que ya esté registrada como técnico en el portal de socios no puede ser invitada como administrador. Al cambiar de rol, debe eliminarse la cuenta existente y volver a invitar al usuario con el nuevo rol.

Proceso general



Invitar técnicos al Portal de Socios

Con cuentas de técnico, otorga a socios e instaladores acceso limitado a sitios sin una cuenta de administrador compartida. Los técnicos se administran de forma central en el Portal de Socios y pueden asignarse a sitios individuales.

Beneficios clave de las cuentas de técnico

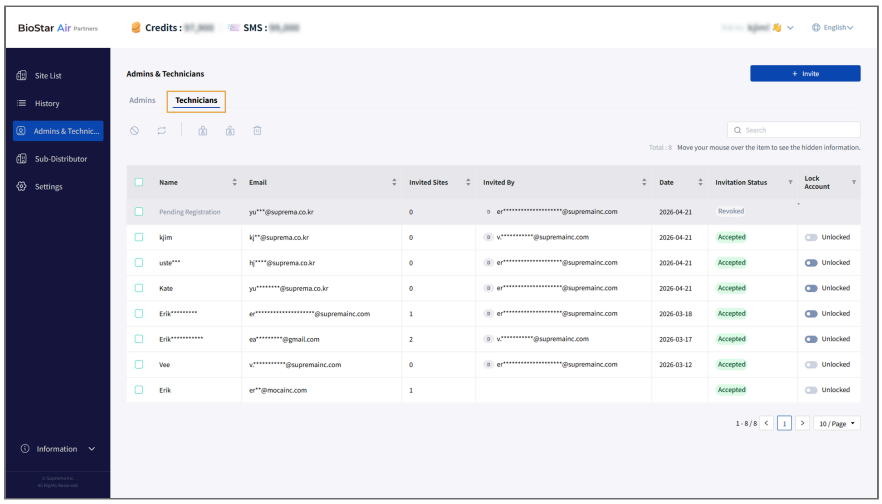
- **Mayor seguridad**: Reduce el riesgo de acceso no autorizado eliminando cuentas de administrador compartidas
- **Cumplimiento**: Ayuda a cumplir las normas de privacidad (por ejemplo, GDPR) y ofrece la opción de restringir el acceso a los datos de usuarios
- **Control de acceso**: Configura permisos granulares, desde acceso a dispositivos hasta privilegios de administrador completos
- **Registro de auditoría**: Registra las actividades individuales de los técnicos en los registros de auditoría para rastrear la responsabilidad
- **Mayor eficiencia**: Asigna y administra técnicos en múltiples sitios sin conflictos de inicio de sesión
- **Revocación inmediata**: Revoca el acceso de un técnico de forma inmediata, en cualquier momento

Invitar técnicos

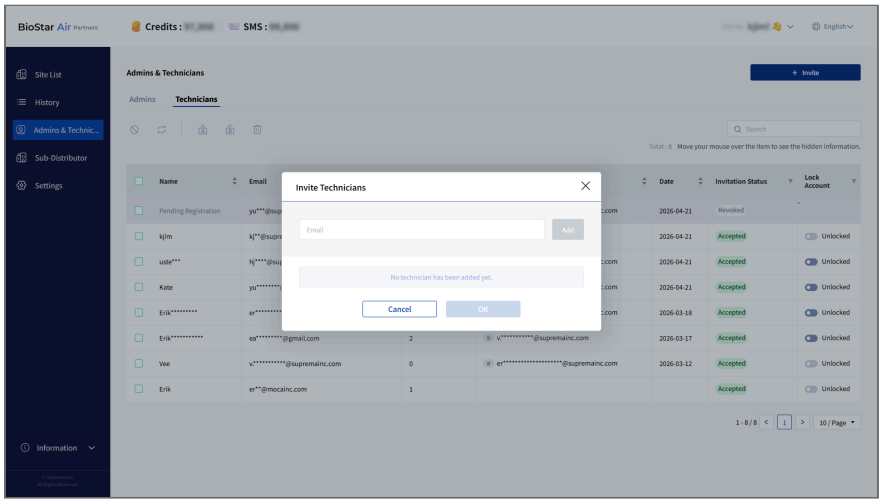
Los socios deben invitar a los técnicos para crear cuentas de técnico antes de otorgar acceso a un sitio. Las cuentas de

técnico se crean con una dirección de correo electrónico. Los técnicos invitados activan sus cuentas aceptando la invitación enviada a su correo.

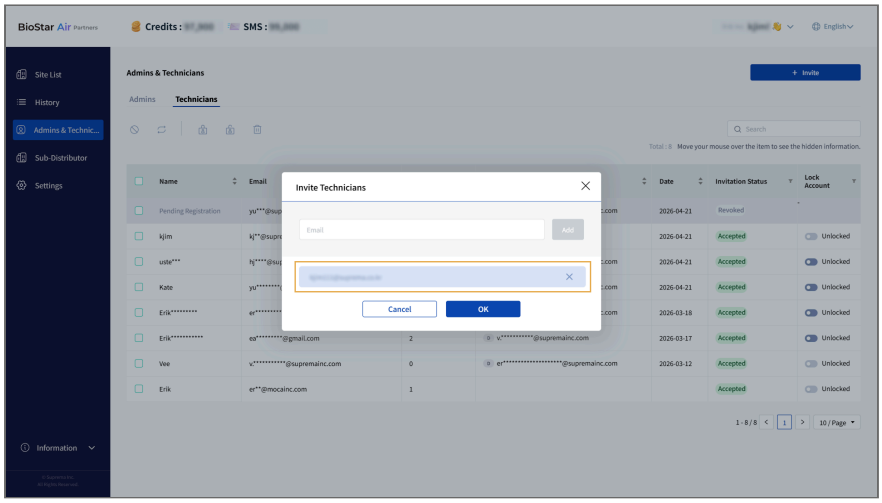
1. Inicia sesión en el Portal de Socios.
2. Haz clic en en la barra lateral izquierda.
3. Haz clic en la pestaña .



4. Haz clic en en la parte superior derecha de la pantalla.
5. Cuando aparezca la ventana , ingresa la dirección de correo electrónico del técnico a invitar.



6. Haga clic en cuando esté activo.
7. Los técnicos agregados aparecen debajo del campo de entrada de correo electrónico. Repite los pasos 5–6 para invitar técnicos adicionales.



8. Después de agregar a todos los técnicos, haz clic en **Aceptar**.
9. Cuando aparezca el mensaje de confirmación, haz clic en **Confirmar**.

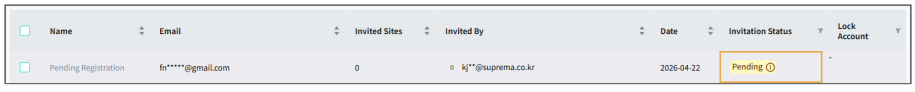
> **Información**
>
> - Invitar técnicos al Portal de Socios no les otorga acceso a los sitios; debes invitar a los técnicos a cada sitio por separado. Para más información sobre cómo invitar a un técnico a un sitio, consulta Asignar técnicos a un sitio.
> - Los técnicos que se registran mediante el correo de invitación pueden iniciar sesión en el Portal de Socios, pero su acceso a los menús es limitado. Solo pueden cambiar su propia contraseña, eliminar su cuenta y seleccionar su idioma.

Estado de la invitación

Después de invitar a los técnicos, los socios pueden verificar el estado de la invitación de cada técnico en la lista de técnicos.

Registro pendiente

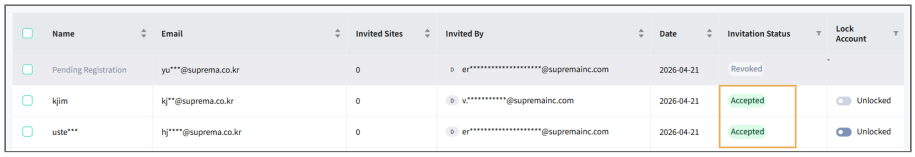
El estado de la invitación se muestra como hasta que el técnico invitado acepta la invitación. Los técnicos invitados pueden hacer clic en el enlace del correo para crear una cuenta o iniciar sesión en el Portal de Socios.



> **Información**
>
> Los técnicos invitados tienen hasta 7 días para aceptar la invitación. Tras 7 días, la invitación expira y el estado cambia a . Si una invitación expira, los socios pueden reenviar el enlace de invitación para que el técnico vuelva a registrarse. Para más información sobre cómo reenviar enlaces de invitación, consulta Reenviar enlace de invitación.

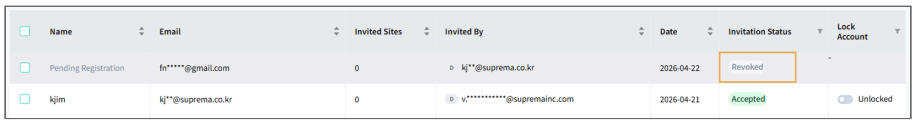
Registro completado

Cuando un técnico acepta la invitación por correo y completa el registro, el estado de la invitación cambia a .



Invitación revocada

Los socios pueden cancelar una invitación si ingresaron mal el correo del técnico, o si el problema se resolvió y la invitación ya no es necesaria. El estado de la invitación cambia a . Para más información sobre cómo revocar la invitación de un técnico, consulta Invitación revocada.



Invitación revocada

Los socios pueden cancelar una invitación si ingresaron mal el correo del técnico, o si el problema se resolvió y la invitación ya no es necesaria. Después de cancelar la invitación, el usuario no podrá usar el enlace de invitación para registrarse.

1. En la lista de técnicos, selecciona la casilla de cada técnico cuyo estado de invitación sea . Selecciona 1 o más técnicos.
2. Haz clic en en la parte superior izquierda de la lista de técnicos.



> Solo los técnicos con estado pueden tener su invitación revocada.

3. Si aparece un mensaje emergente, revíselo y haga clic en .
4. Cuando aparezca el mensaje de éxito por la invitación cancelada, haga clic en **Cerrar**.

El estado de la invitación de un técnico revocado cambia a en la lista de técnicos.



Reenviar enlace de invitación

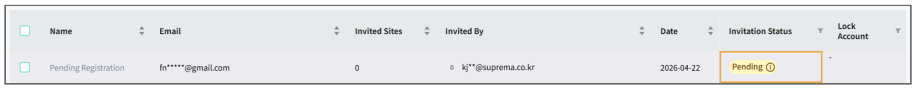
Reenvía el enlace de invitación si un técnico invitado no recibió el correo, lo perdió o el enlace de invitación expiró.

1. En la lista de técnicos, selecciona la casilla de cada técnico cuyo estado de invitación sea , o . Selecciona 1 o más técnicos.
2. Haz clic en en la parte superior izquierda de la lista de técnicos.



3. Si aparece un mensaje emergente, revíselo y haga clic en .
4. Cuando aparezca el mensaje de éxito por reenvío del enlace de invitación, haga clic en **Cerrar**.

Después de reenviar el enlace de invitación de un técnico, su estado de invitación cambia a en la lista de técnicos.



Administrar técnicos

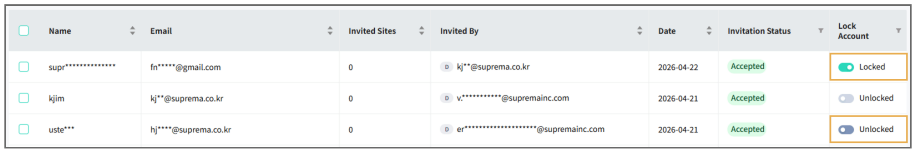
Después de que el técnico invitado acepte la invitación por correo y complete el registro, los socios pueden administrar los siguientes elementos en la lista de técnicos.

- Bloquear o desbloquear cuentas de técnicos
- Editar acceso al sitio
- Eliminar cuentas de técnicos

Bloquear o desbloquear cuentas de técnicos

Los socios pueden bloquear o desbloquear cuentas de técnico usando la opción . Bloquear una cuenta de técnico impide que el técnico inicie sesión en el Portal de Socios y en los sitios asignados. Se conserva la información de la cuenta, permitiendo su reactivación cuando sea necesario.

En la columna , los técnicos bloqueados se muestran como y los técnicos desbloqueados se muestran como .



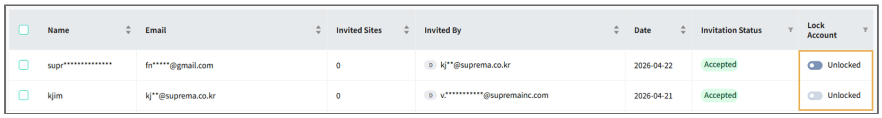
Información

- Las cuentas de los técnicos que han completado el registro están desbloqueadas por defecto.
- Aunque una cuenta de administrador del Portal de Socios pueda aparecer en la lista de técnicos si tiene acceso de técnico a ciertos sitios, esa cuenta de administrador no puede ser bloqueada o desbloqueada desde la lista de técnicos.

Bloquear o desbloquear la cuenta de un técnico individual

En la lista de técnicos, haz clic en el botón de alternancia en la columna para bloquear o desbloquear la cuenta de un técnico.

1. En la lista de técnicos, haz clic en el interruptor en la columna .



2. Si aparece un mensaje emergente, revíselo y haga clic en .
3. Cuando aparezca el mensaje de éxito que confirma el bloqueo o desbloqueo de la cuenta, haz clic en **Cerrar**.

Bloquear o desbloquear varias cuentas de técnicos

Selecciona varias cuentas de técnicos en la lista para bloquearlas o desbloquearlas en lote.

1. En la lista de técnicos, marca la casilla de cada técnico que quieras bloquear o desbloquear. Selecciona 1 o más técnicos.
2. Haz clic en o en la esquina superior izquierda de la pantalla.



3. Si aparece un mensaje emergente, revíselo y haga clic en .
4. Cuando aparezca el mensaje de éxito que confirma el bloqueo o desbloqueo de la cuenta, haz clic en **Cerrar**.

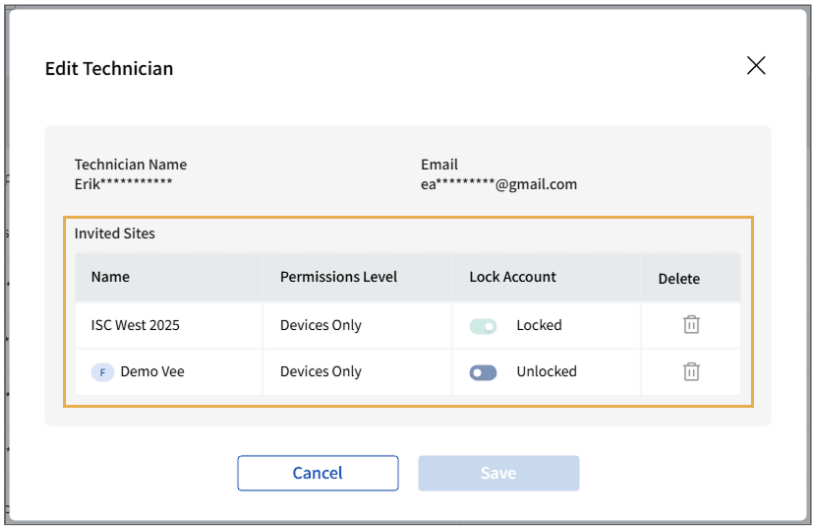
Editar acceso al sitio

Modifica el acceso de un técnico al sitio.

1. En la lista de técnicos, haz clic en un técnico cuya columna indique 1 o más sitios.



2. Cuando aparezca la ventana , revisa la lista de sitios a los que el técnico está invitado en .



3. Haz clic en el botón de alternancia en la columna para permitir o bloquear el acceso al sitio.
4. Haz clic en para guardar los cambios.
5. Cuando aparezca el mensaje de éxito que confirma los cambios en el acceso al sitio, haz clic en **Cerrar**.

> **Información**
>
> - Una vez que un técnico se asigna a un sitio y los permisos se configuran en el Portal de Socios, solo una cuenta de administrador puede cambiar esos permisos en el portal de administración de BioStar Air.
> - Si un administrador del sitio bloquea el acceso de un técnico al sitio en el portal de BioStar Air, no se puede desbloquear desde el Portal de Socios. Para modificar el acceso de un técnico al sitio, usa una cuenta con privilegios de administrador para ese sitio en el portal de BioStar Air.
> - Para más información sobre cómo otorgar acceso a un técnico a un sitio, consulta Asignar técnicos a un sitio.

Eliminar cuentas de técnicos

Si ya no necesitas el soporte del técnico, puedes eliminar su cuenta. Eliminar una cuenta de técnico impide que el técnico inicie sesión en el Portal de Socios y elimina permanentemente toda la información asociada con la cuenta del sistema.

1. En la lista de técnicos, marca la casilla del técnico que deseas eliminar. Selecciona 1 o más técnicos.
2. Haz clic en en la parte superior izquierda de la pantalla.



3. Si aparece un mensaje emergente, revíselo y haga clic en **Confirmar**.
4. Cuando aparezca el mensaje de éxito de eliminación de la cuenta, haz clic en **Cerrar**.

Las cuentas de técnicos eliminadas ya no aparecen en la lista de técnicos.

Asignar técnicos a un sitio

Los socios pueden asignar técnicos a los sitios de clientes y definir permisos. Gestione niveles de acceso granulares para cada técnico y proteja la información personal sensible.

Funciones clave al asignar técnicos a sitios

- **Ajustes de acceso granular**: Opciones flexibles, desde acceso a dispositivos hasta permisos de administrador completos
- **Protección de datos de usuarios**: Cumpla con las normativas de privacidad usando la opción para excluir el acceso a datos de usuario
- **Gestión eficiente**: Administre técnicos en cada sitio según los niveles de permiso definidos por el socio

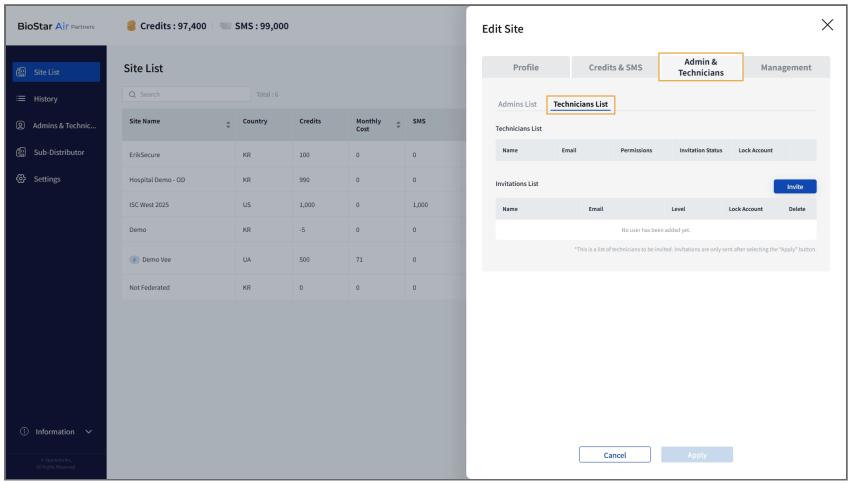
> **Información**
>
> - Antes de asignar técnicos a un sitio, invite sus cuentas en el Portal de Socios. Para obtener más información, consulte Invitar técnicos al Portal de Socios.
> - Para obtener más información sobre cómo asignar técnicos a un sitio en el portal de administración de BioStar Air, consulte Administrar cuentas de técnicos..

Asignar técnicos a un sitio

Después de invitar a un técnico en el Partner Portal, asigne al técnico a cada sitio individual para que pueda acceder a esos sitios. Siga los pasos siguientes para asignar un técnico a un sitio.

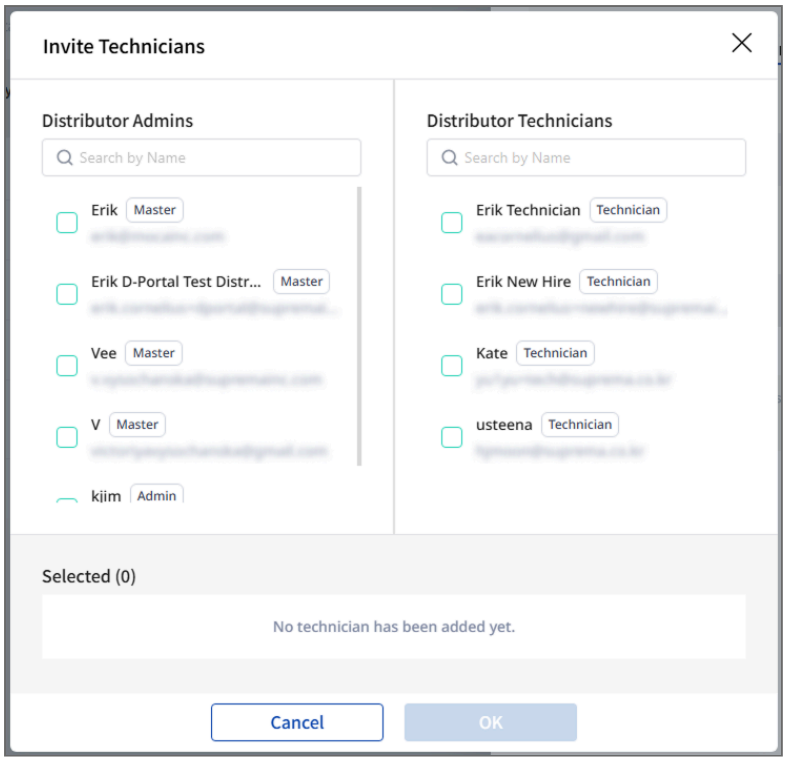
1 Ir a la lista de sitios

1. Inicia sesión en el Portal de Socios.
2. Haga clic en en la barra lateral izquierda.
3. En la lista de sitios, haga clic en el sitio al que asignará un técnico.
4. Cuando aparezca el panel , selecciona la pestaña y luego la pestaña .

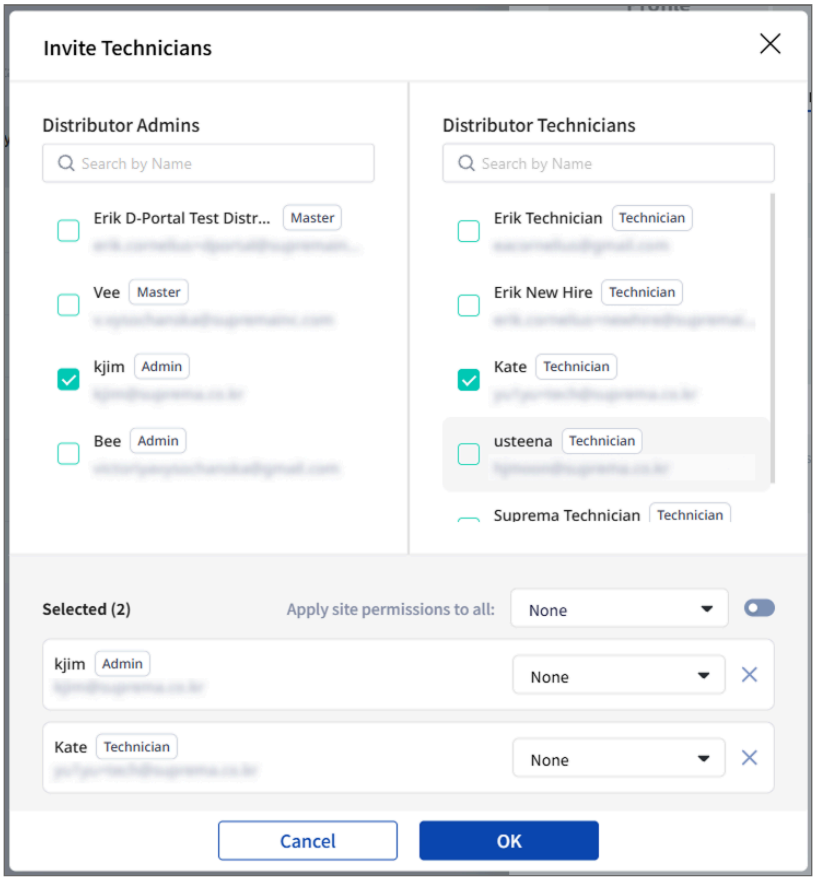


5. Haga clic en .

6. Cuando aparezca la ventana , seleccione la cuenta deseada de la lista o .



Las cuentas seleccionadas aparecen en la lista en la parte inferior.



Información

- Ingrese el nombre de un administrador o de un técnico en el campo de búsqueda por nombre.
- Para cancelar la cuenta seleccionada, en la lista , haga clic en ✕ a la derecha de la cuenta.
- Las cuentas que estén registradas como administradores del sitio o ya asignadas como técnicos al sitio no aparecerán en la lista.

2 Establecer permisos de acceso al sitio

Después de seleccionar todos los técnicos para invitar, aplique los permisos de acceso al sitio. Los permisos disponibles son:

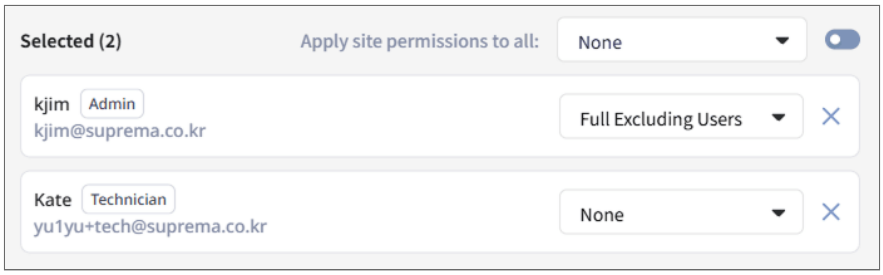
- : Puede agregarse al sitio pero no puede iniciar sesión.
- : Solo puede acceder a los menús **Panel de Control** y **Gestión de dispositivos**.
- : Puede acceder a todos los menús excepto el menú **Gestión de usuarios**, pero el acceso a ciertos ajustes está restringido.
- : Puede acceder a todos los menús, incluido el menú **Gestión de usuarios**, pero el acceso a ciertos ajustes está restringido.

Información

- y tienen acceso de solo lectura a la siguiente ruta de menú.
  - **Ajustes** → **Administradores y técnicos**
  - **Ajustes** → **Sitio**
- Una vez que un técnico se asigna a un sitio y los permisos se configuran en el Portal de Socios, solo una cuenta de administrador puede cambiar esos permisos en el portal de administración de BioStar Air.

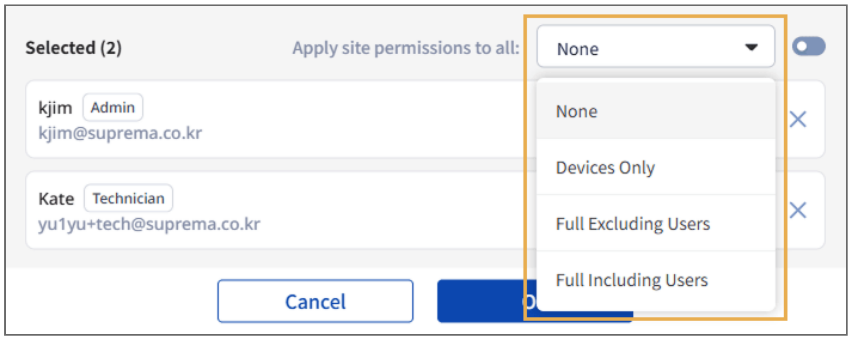
3 Establecer permisos para técnicos individuales

Asigne distintos permisos a técnicos individuales. A la derecha de cada cuenta, seleccione el nivel de permiso deseado.

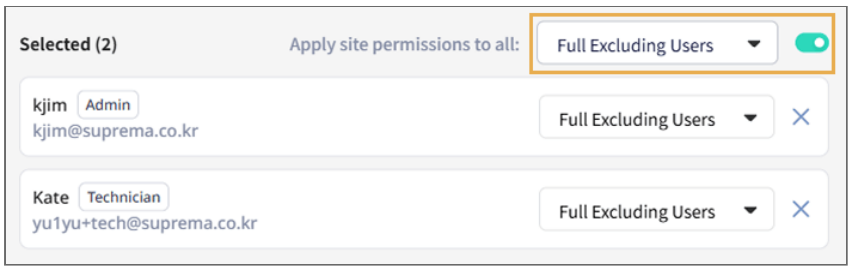


4 Aplicar los mismos permisos a todos los técnicos

1. Elija el nivel de permiso deseado en la opción , luego active el interruptor a la derecha para aplicar los mismos permisos a todas las cuentas seleccionadas.

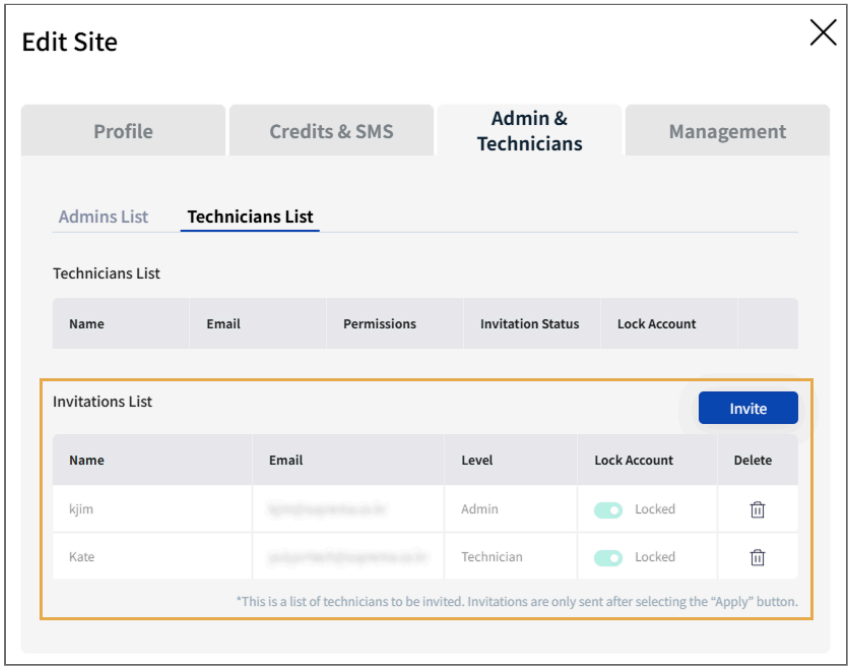


2. Cuando aparezca el mensaje de confirmación, haga clic en .
3. El permiso seleccionado se aplica a todas las cuentas de la lista .



5 Invitación de técnico completada

1. Después de completar las invitaciones a técnicos y la configuración de permisos, haga clic en **Confirmar** en la ventana .
2. La ventana se cierra y los técnicos invitados aparecen en dentro del panel .



3. Para enviar los correos de invitación y permitir el acceso de los técnicos al sitio, haga clic en en la parte inferior del panel .

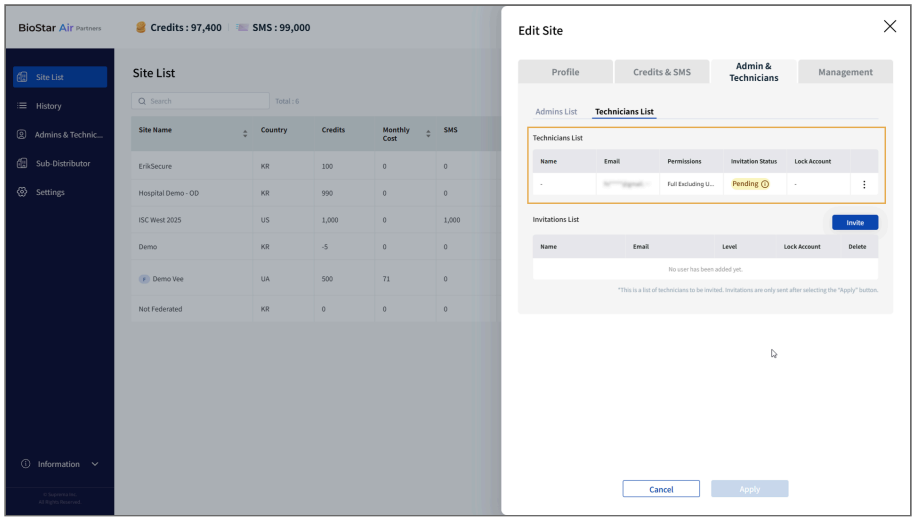
Verificar el estado de la invitación

Compruebe el estado de invitación de los técnicos invitados al sitio. El estado se muestra como hasta que el técnico invitado

acepte la invitación. Los técnicos invitados tienen hasta 7 días para aceptar la invitación. Pasados 7 días, la invitación expira y el estado cambia a .

1. En la lista de sitios, haga clic en el sitio donde invitó al técnico.
2. Cuando aparezca el panel , selecciona la pestaña y luego la pestaña .
3. : Compruebe el estado de la invitación.

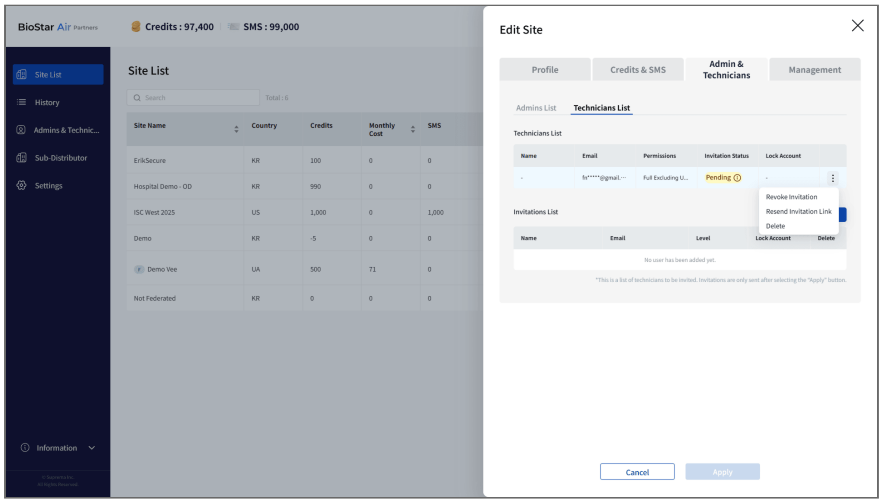
Cuando un técnico completa el registro en el sitio, su estado cambia de a .



Invitación revocada

Cancele la invitación si la dirección de correo electrónico del técnico invitado se ingresó incorrectamente o si el problema se resolvió y la invitación ya no es necesaria.

1. En la lista de sitios, haga clic en el sitio donde invitó al técnico.
2. Cuando aparezca el panel , selecciona la pestaña y luego la pestaña .
3. En , para el técnico cuyo estado sea , haga clic en ⋮ en el extremo derecho.



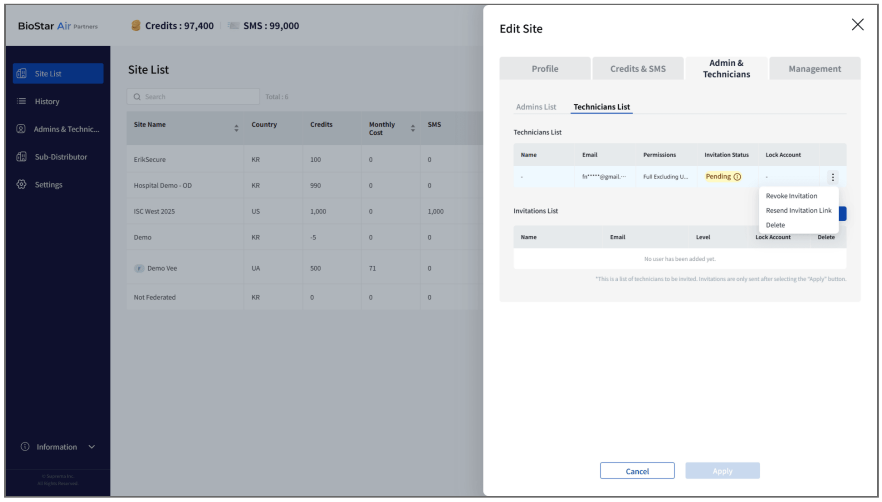
4. Haga clic en en el menú emergente.
5. Si aparece un mensaje emergente, revíselo y haga clic en .
6. Cuando aparezca el mensaje de éxito por la invitación cancelada, haga clic en **Cerrar**.

Cuando se cancela una invitación, el estado del técnico cambia de a .

Reenviar enlace de invitación

Reenvíe el enlace de invitación si un técnico invitado no recibió el correo de invitación o lo perdió.

1. En la lista de sitios, haga clic en el sitio donde invitó al técnico.
2. Cuando aparezca el panel , selecciona la pestaña y luego la pestaña .
3. En , para el técnico cuyo estado sea , o , haga clic en ⋮ en el extremo derecho.

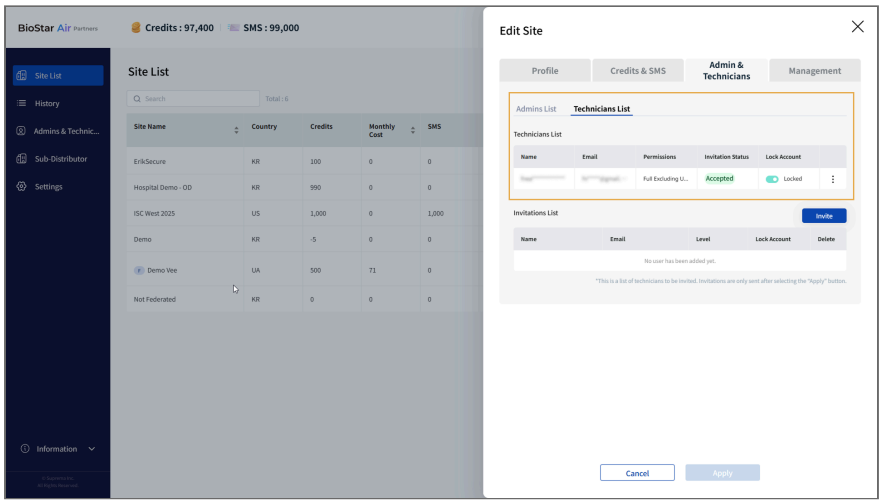


4. Haga clic en en el menú emergente.
5. Si aparece un mensaje emergente, revíselo y haga clic en .
6. Cuando aparezca el mensaje de éxito por reenvío del enlace de invitación, haga clic en **Cerrar**.

Bloquear o desbloquear cuentas de técnicos

Bloquee o desbloquee cuentas de técnicos asignados a un sitio.

1. Haga clic en en la barra lateral izquierda.
2. En la lista de sitios, haz clic en el sitio donde quieras administrar el acceso de técnicos.
3. Cuando aparezca el panel , selecciona la pestaña y luego la pestaña .



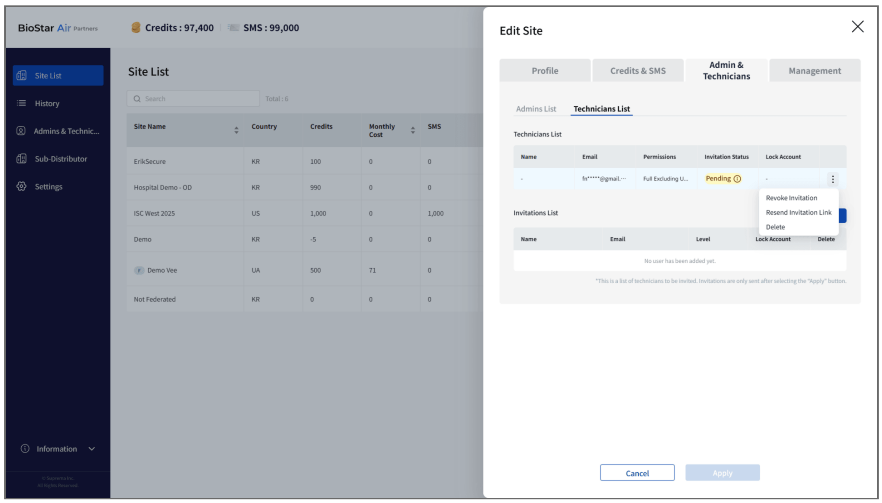
4. En , haga clic en el botón de alternar en la columna para bloquear o desbloquear la cuenta de un técnico.
5. Haz clic en en la parte inferior para aplicar los cambios.

> **Información**
> Las cuentas de técnicos recién registradas tienen el acceso al sitio establecido en . Para desbloquear el estado , use una cuenta con derechos de administrador para ese sitio en el portal de BioStar Air.

Eliminar cuentas de técnicos

Es posible eliminar la cuenta de un técnico invitado al sitio. Cuando se elimina la cuenta de un técnico, este no puede iniciar sesión en el sitio y se revoca su acceso.

1. En la lista de sitios, haga clic en el sitio donde invitó al técnico.
2. Cuando aparezca el panel , selecciona la pestaña y luego la pestaña .
3. En , haga clic en ⋮ en el extremo derecho del técnico que va a eliminar.



4. Haga clic en **Borrar** en el menú emergente.
5. Si aparece un mensaje emergente, revíselo y haga clic en **Confirmar**.
6. Cuando aparezca el mensaje de éxito que confirma la eliminación de la cuenta del técnico, haga clic en **Cerrar**.

> **Información**
> Eliminar la cuenta de un técnico no borra la cuenta por completo; solo revoca el acceso a ese sitio. Vuelva a invitar al técnico eliminado al sitio para restaurar su acceso.

Instalar el hardware

Esta es una guía de instalación y configuración de hardware para configurar correctamente el sistema BioStar Air. Estos documentos explican cómo conectar y configurar cada dispositivo, incluyendo interfaces SIP, cámaras IP, Los escáneres QR y Airfop Patch, así como cómo configurar los puertos de red y la configuración del módulo de seguridad.

Configurar el intercomunicador SIP en BioStation 3

A partir de **BioStar Air v2.10**, **BioStation 3** (BS3) es compatible con la función de intercomunicador SIP. Esto permite realizar llamadas de voz bidireccionales entre el dispositivo y los administradores, así como la apertura remota de puertas.

> **Información**
> Es necesario un servidor SIP para usar esta función; adquiere y configura el servidor por separado. Suprema no ofrece servicios SIP.

SIP

El **Session Initiation Protocol** (SIP) es un protocolo de comunicación ampliamente utilizado para iniciar, mantener y finalizar llamadas de voz y vídeo en tiempo real sobre redes IP. En este contexto, SIP permite que BioStation 3 actúe como punto final de intercomunicador, pudiendo realizar y recibir llamadas a través de un servicio SIP compatible.

Recibir llamadas

Responde las llamadas recibidas desde BioStation 3 de las siguientes maneras.

- **BioStar Air Web**: Recibe llamadas directamente en un navegador web
- **BioStar Air Mobile App** (iOS / Android): Recibe llamadas desde cualquier lugar

Control remoto de puertas

Al responder una llamada SIP, utiliza los **comandos DTMF** para abrir la puerta:

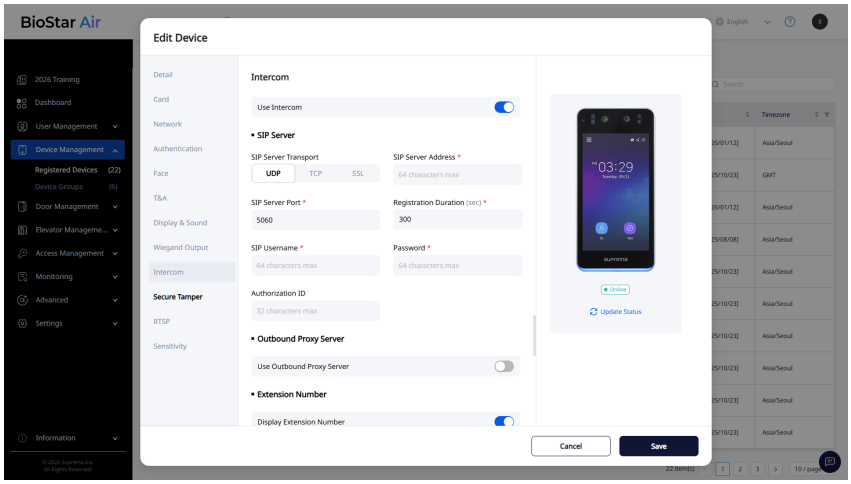
- Teléfono SIP físico
- Aplicación móvil BioStar Air
- Interfaz web de BioStar Air

Pasos de configuración

Configura esto en la configuración del dispositivo y en los ajustes de la cuenta del administrador.

1 Configuración del dispositivo

1. Inicia sesión en el portal de BioStar Air.
2. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
3. En la lista de dispositivos, haz clic en **BioStation 3**.
4. Ve a la sección **Intercomunicador** y habilita la opción **Usar intercomunicador**.
5. Ingresa la información del servidor SIP.



La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

- **Dirección del servidor SIP**
- **Puerto del servidor SIP**
- **Nombre de usuario SIP** / **Clave**

6. Haz clic en **Guardar** para guardar los cambios.

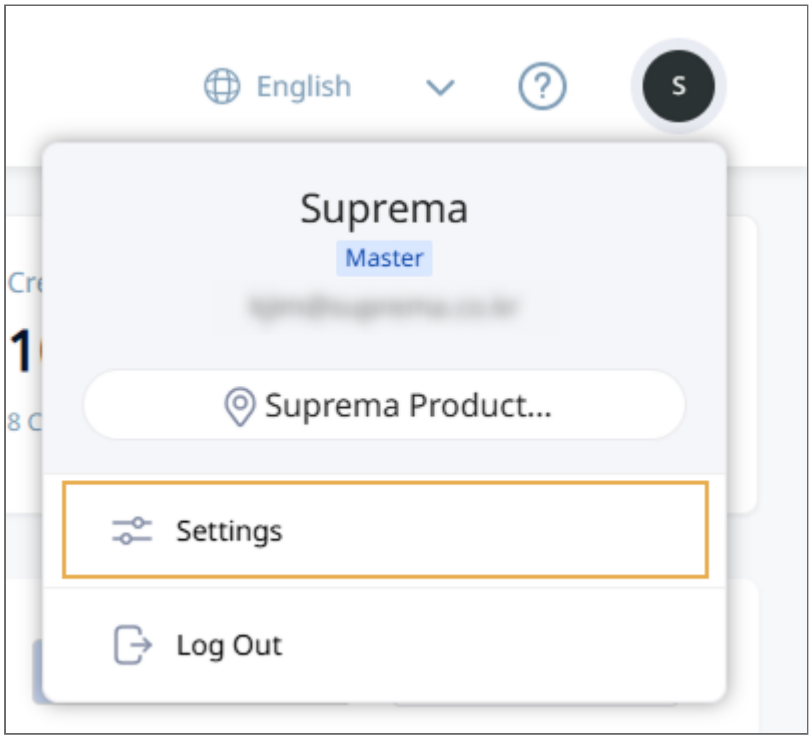
2 Ajustes de la cuenta

Dirige las llamadas desde BioStation 3 a un navegador o a la aplicación.

1. Cada administrador que necesite recibir llamadas debe iniciar sesión en el portal de BioStar Air o en la aplicación móvil.
2. Ve a **Configuración de la cuenta**.

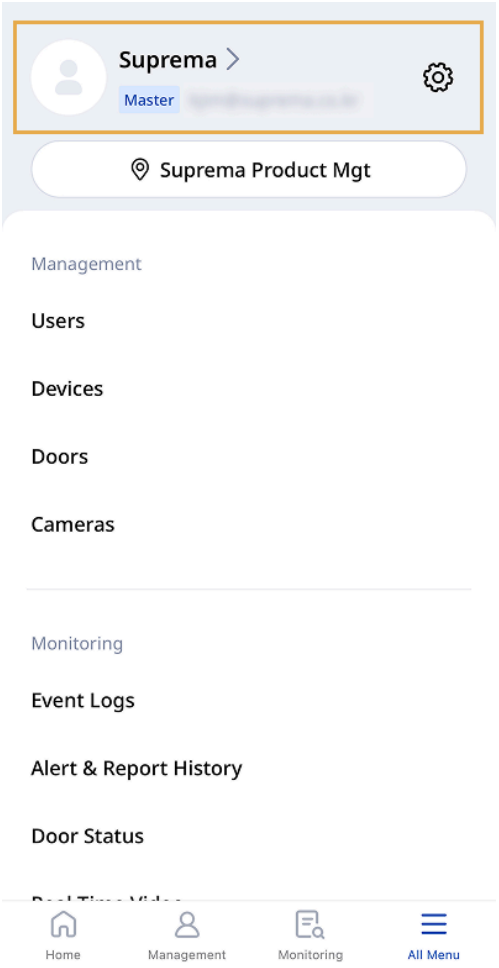
Web

Haz clic en el icono de perfil de usuario en la esquina superior derecha de la pantalla y selecciona **Ajustes**.



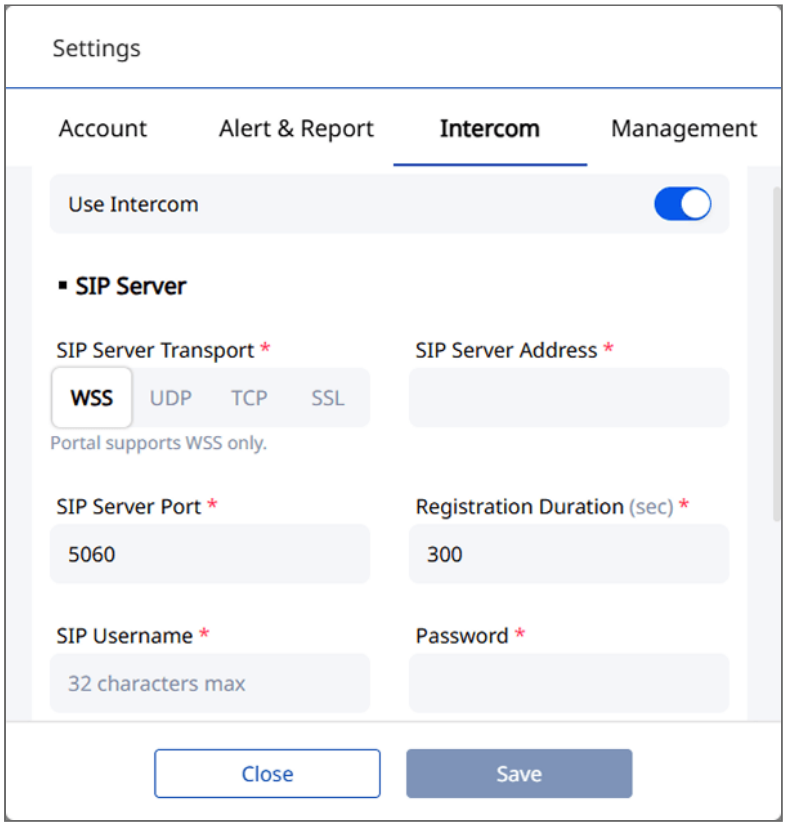
Mobile

En la pantalla principal, toca **All Menu** en la parte inferior, y luego toca el área del perfil de usuario.

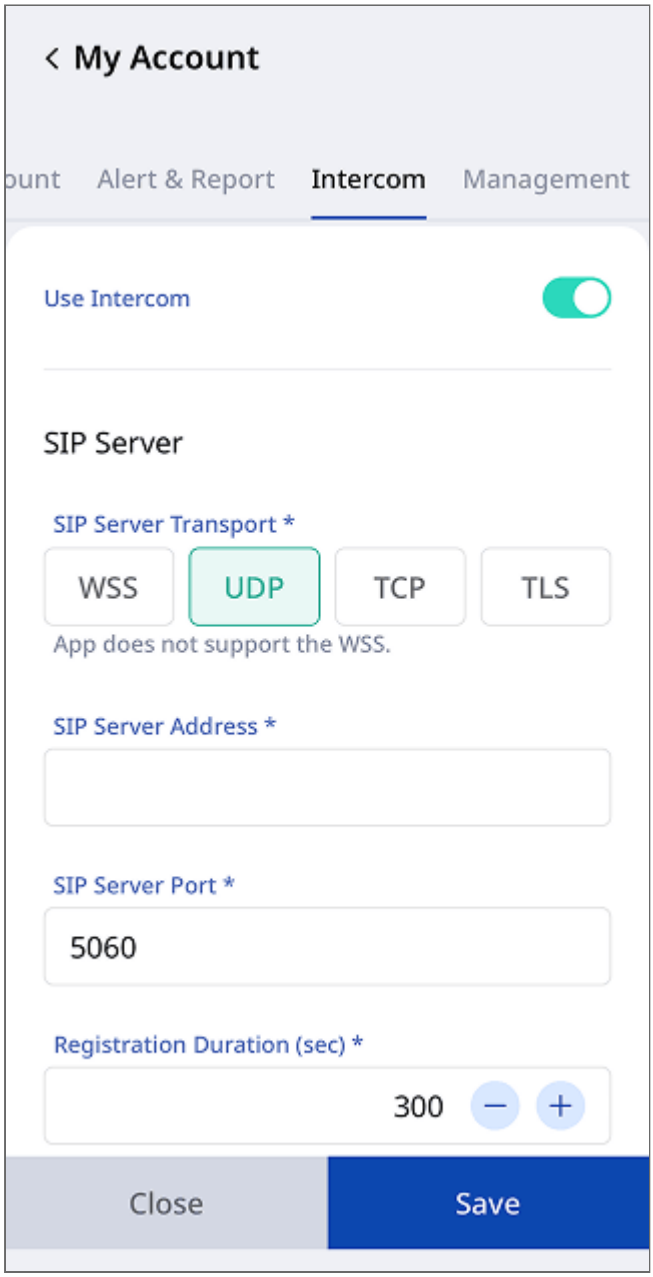


3. Cuando aparezca la ventana **Ajustes**, haz clic en la pestaña **Intercomunicador** y añade la información de inicio de sesión del servidor SIP.

Web


Settings
Account
Alert & Report
Intercom
Management
Use Intercom
SIP Server
SIP Server Transport *
WSS
UDP
TCP
SSL
Portal supports WSS only.
SIP Server Address *
SIP Server Port *
5060
Registration Duration (sec) *
300
SIP Username *
32 characters max
Password *
Close
Save

Mobile



4. Haz clic en **Guardar** para guardar la configuración.

Proveedores SIP verificados

BioStation 3 ha sido probado y se ha comprobado que funciona correctamente con los proveedores que se indican a continuación.

- RingCentral
- FreePBX
- Linphone
- Linhome

Soporte y configuración de cámaras IP

BioStar Air detecta automáticamente las cámaras IP conectadas a la misma red que los lectores compatibles con BioStar Air.

Como las cámaras utilizan el dispositivo como puerta de enlace, no se requiere un grabador de video en red (NVR); en su lugar, las cámaras emplean el almacenamiento integrado en la tarjeta SD.

Con un lector compatible con BioStar Air instalado, BioStar Air puede mostrar las siguientes transmisiones en vivo simultáneas.

- Hasta dos cámaras en resolución Full HD (1080p)
- Hasta cuatro cámaras en resolución HD (720p)

Estas especificaciones se duplican cuando se utiliza la X-Station 2.

> **Información**
> Si un video grabado no se reproduce después de registrar la cámara en BioStar Air, consulte Solución de problemas de reproducción de video.

Compatibilidad

- **Perfiles ONVIF**: La cámara IP debe ser compatible con el perfil ONVIF S o G.
  - **Perfil Onvif S**: transmisión de video en vivo
  - **Perfil ONVIF G**: video grabado almacenado en la tarjeta SD
- **Tarjeta SD**: La cámara IP debe tener una tarjeta SD integrada para que las grabaciones puedan reproducirse posteriormente.

  > Utilice SanDisk microSDXC Class10 Max Endurance de 256 GB o 512 GB.

- **Codificación**: La cámara debe soportar H.264 (AVC) y este debe configurarse como el códec activo. BioStar Air actualmente no es compatible con H.265.
- **Marcas recomendadas**: Las cámaras HanwhaVision, Hikvision y Dahua son altamente compatibles. La compatibilidad con otras marcas puede variar según el cumplimiento del perfil Onvif. Para conocer la lista de dispositivos probados y verificados, consulte Lista de dispositivos probados y verificados.
- Comuníquese con el equipo de servicio para probar otras marcas de cámaras.

Resumen de la funcionalidad

Realice las siguientes acciones en el portal de BioStar Air o en la aplicación móvil.

- Ver transmisiones en vivo.
- Ver grabaciones de las cámaras.
- Acceder a grabaciones de las cámaras relacionadas con eventos de acceso.

Instrucciones

1 Conectar cámaras IP

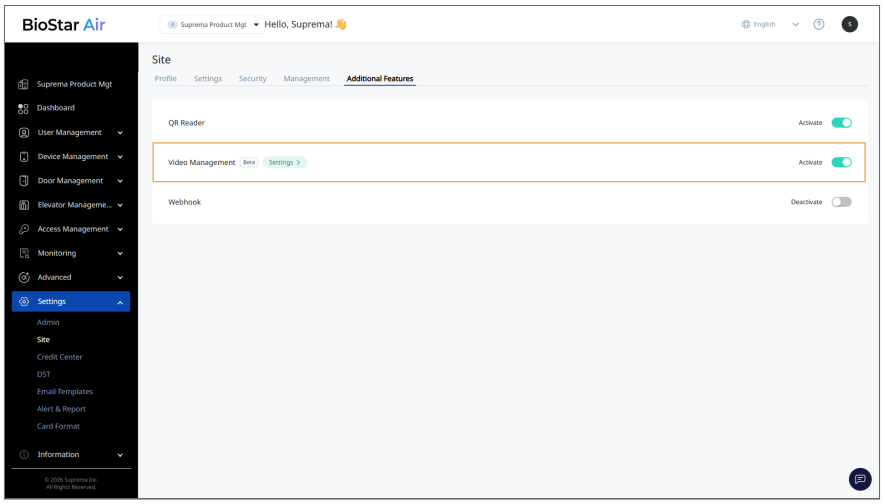
- **Conexión de red**: Asegúrese de que la cámara IP esté en la misma red que el lector compatible con BioStar Air.
- **Habilitar Onvif**: Asegúrese de que Onvif esté activado en la cámara.
- **Registro del dispositivo**: Asegúrese de que el dispositivo esté registrado en el portal de BioStar Air.

2 Iniciar sesión en BioStar Air

Los administradores con rol **master** pueden cambiar la configuración del sitio, como habilitar la gestión de video. Inicie sesión en el portal de BioStar Air con privilegios de **master**.

3 Habilitar la gestión de video

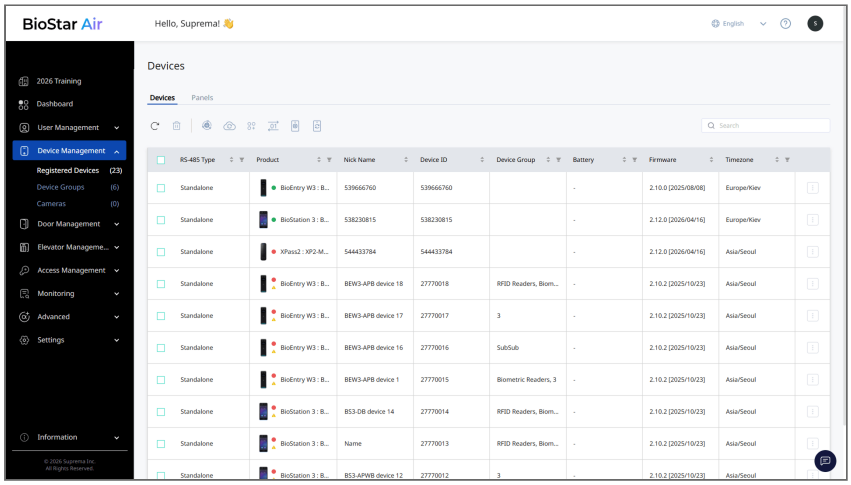
1. Haz clic en **Ajustes** → **Sitio** en la barra lateral izquierda.
2. Haz clic en la pestaña **Adicionales**.
3. Habilitar **Gestión de Vídeos**.



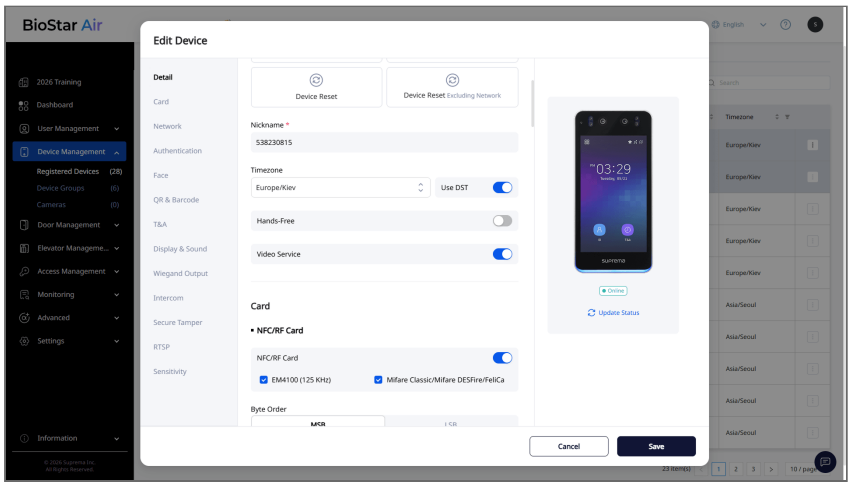
> **Información**
> Solo los administradores con nivel **master** pueden habilitar esta función.

4 Habilitar el servicio de video

1. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.



2. Haga clic en el dispositivo (por ejemplo, BioStation 3) compatible con BioStar Air en la lista.
3. Aparece la ventana **Editar dispositivo**.
4. Habilite **Servicio de Video** en la sección **Detalle**.

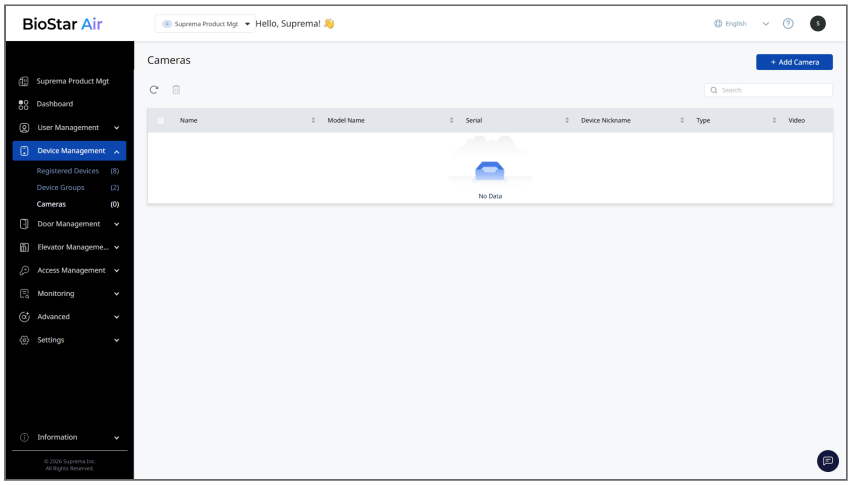


5. Haz clic en **Guardar** en la parte inferior para guardar los cambios.

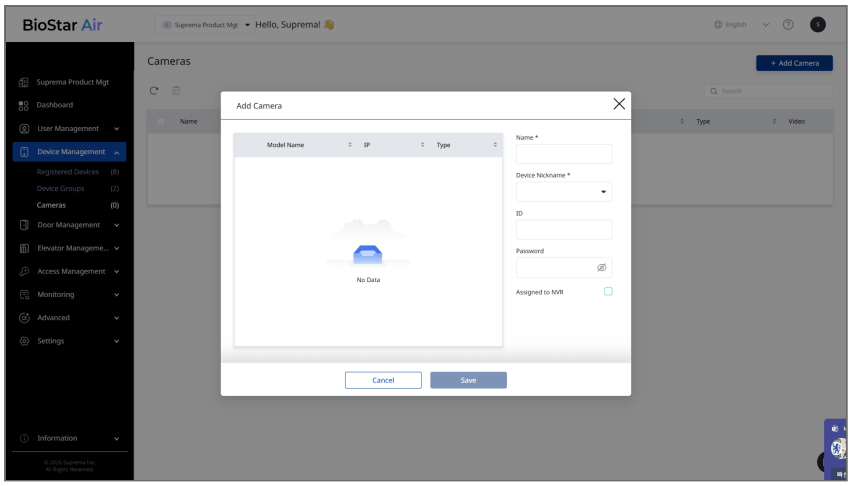
> **Información**
> El dispositivo debe ejecutar la versión de firmware 2.5.1 o posterior y estar en la misma red que la cámara.

5 Añadir cámara

1. Haz clic en **Gestión de dispositivos** → **Cámaras** en la barra lateral izquierda.



2. Haz clic en **Agregar Cámara** en la esquina superior derecha de la pantalla.
3. Cuando aparezca la ventana **Agregar Cámara**, seleccione el dispositivo que actuará como puerta de enlace.



La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

4. Ingrese la siguiente información para agregar la cámara.
   - **Nombre**: Ingrese el nombre de la cámara.
   - **Apodo del dispositivo**: Seleccione un nombre para identificar la cámara.
   - **ID**: Ingrese el ID para conectarse a la cámara.
   - **Contraseña**: Ingrese la contraseña para conectarse a la cámara.
5. Haz clic en **Guardar** para agregar la cámara seleccionada.

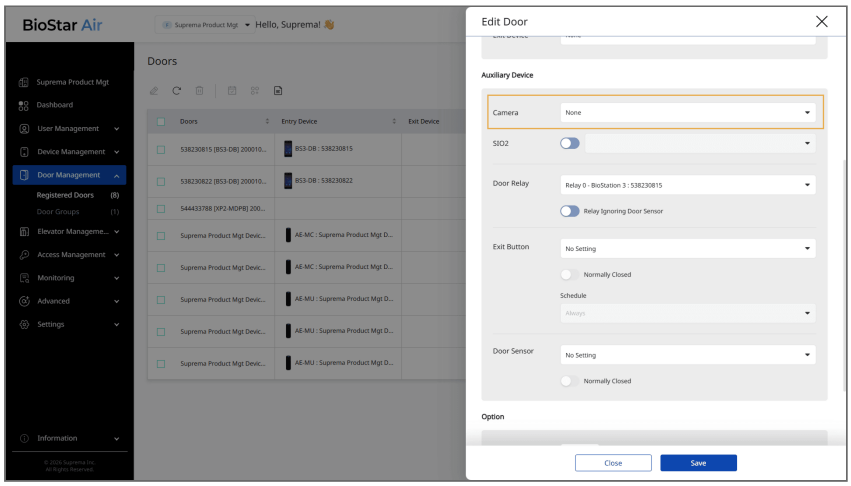
Información

- El dispositivo debe ejecutar la versión de firmware 2.5.1 o posterior y estar en la misma red que la cámara.
- BioStar Air detecta automáticamente las cámaras en la red.

6 Vincular a una puerta

Vincule la cámara agregada a una puerta para asociar el video con los eventos de acceso.

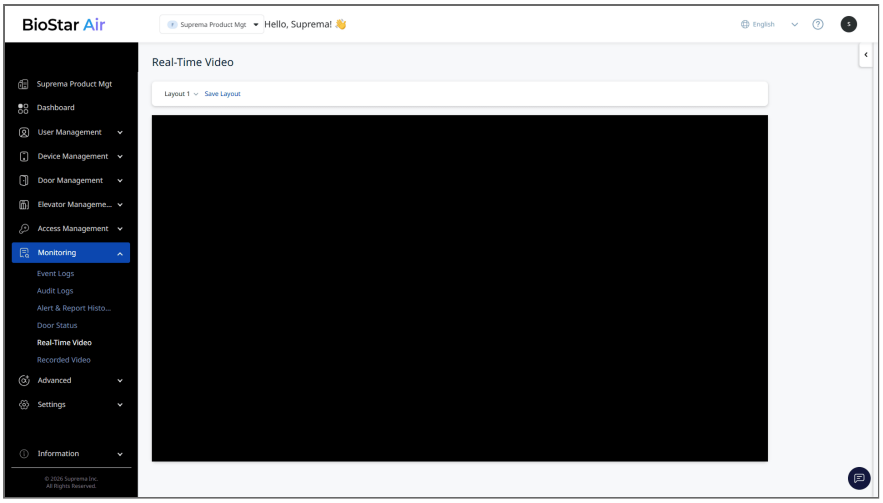
1. Haga clic en **Gestión de Puerta** → **Registrados Puerta** en la barra lateral izquierda.
2. Haz clic en la puerta en la lista para asignarle una cámara.
3. Cuando aparezca el panel **Editar puerta**, desplácese hasta **Dispositivo auxiliar**.
4. Seleccione la cámara que agregó en **Cámara**.



5. Haz clic en **Guardar** para guardar los cambios.

7 Ver video en vivo de la cámara

Ver video en vivo de las cámaras agregadas. Haz clic en **Monitoreo** → **Vídeo en Tiempo Real** en la barra lateral izquierda.



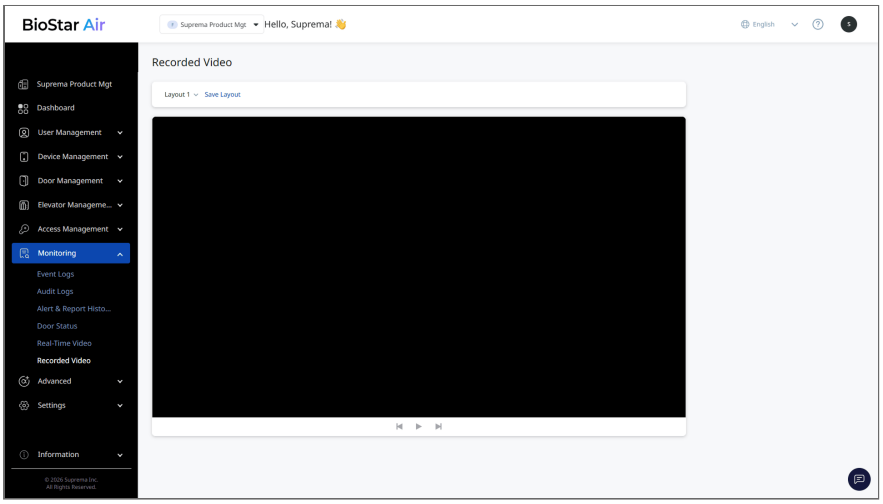
La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

- Ver hasta dos transmisiones en vivo Full HD (1080p) por cada lector instalado compatible con BioStar Air.
- Agrega más dispositivos o reduce la resolución de la cámara para ver más transmisiones en vivo.

  > ***Gestión de dispositivos*** → ***Cámaras*** → *Haz clic en la cámara de la lista* → ***Perfil de video***

8 Ver video grabado de la cámara

Ver transmisiones de video grabadas. Haz clic en **Monitoreo** → **Vídeo Grabado** en la barra lateral izquierda.



La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

9 Ver video del evento

Haz clic en **Monitoreo** → **Registros de eventos** en la barra lateral izquierda. Busca un registro de evento con un clip de video asociado y haz clic en reproducir para verlo.

Lista de dispositivos probados y verificados

No	Fabricante	Número de modelo	Tipo de dispositivo	Perfil Onvif	Resolución
1	Hanwha Techwin	QNV-C8011R	Cámara	S, G, T, M	2592x1944
2	Hanwha Techwin	QND-6022R	Cámara	S, G, T	1920x1080
3	Hanwha Techwin	MMI-600R	Cámara	S, T	1920x1080
4	HIKVISION	DS-2CD2025FWD-I	Cámara	S, G, T	1920x1080
5	HIKVISION	DS-2CD2166G2-I	Cámara	S, G, T	3200×1800
6	HIKVISION	DS-2CD1121-I	Cámara	S	1920x1080
7	Dahua	DHI-NVR2104HS-P-S3	NVR	S, G, T	12MP
8	Dahua	IPC-HDBW3249E-AS-NI	Cámara	S, G, T	1920×1080
9	Dahua	SD22204UEN-GN	Cámara	S, G, T	1920×1080
10	Dahua	DH-IPC-HFW1230DT-STW-VN	Cámara	S, T	1920×1080
11	Marruy	IPC-A32E-L	Cámara	S, T	2304×1296

No	Fabricante	Número de modelo	Tipo de dispositivo	Perfil Onvif	Resolución
12	TP-Link	Tapo C210	Cámara	S	2304×1296

Habilitar ONVIF en una cámara IP

1. Abre un navegador web e ingresa la dirección IP de la cámara.
2. Autentícate con credenciales de administrador e inicia sesión.
3. Ve a la sección **Red** o **Configuración**.
4. Activa ONVIF o la interfaz abierta de video en red.
5. Crea un perfil de usuario solo para ONVIF si es necesario.
6. Guarda la configuración y prueba la conexión ONVIF en BioStar Air.

Consejo

- **Actualización de firmware**: Actualiza la cámara y el dispositivo al firmware más reciente.
- **Redirección de puertos**: Configura la redirección de puertos para ONVIF si es necesario.
- **Herramientas de terceros**: Usa ONVIF Device Manager para verificar la configuración y el funcionamiento de la cámara.

Instalar Airfob Patch

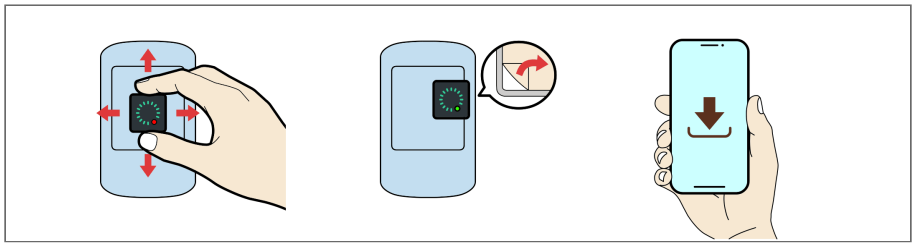
Esta guía explica cómo instalar Airfob Patch. Airfob Patch actualiza un sistema de control de acceso existente para que funcione con credenciales móviles de BioStar Air.

Información

- Airfob Patch es compatible con la tecnología MIFARE 1K, pero no es compatible con lectores de **baja frecuencia** de 125 kHz.
- Airfob Patch autentica credenciales Bluetooth cifradas de BioStar Air y emula una señal RFID MIFARE para el lector. Se fija a los lectores de control de acceso con cinta y no requiere cableado.
- Para obtener más información sobre cómo enrollar un Airfob Patch en la aplicación BioStar Air, consulte Configurar Airfob Patch y Tag.

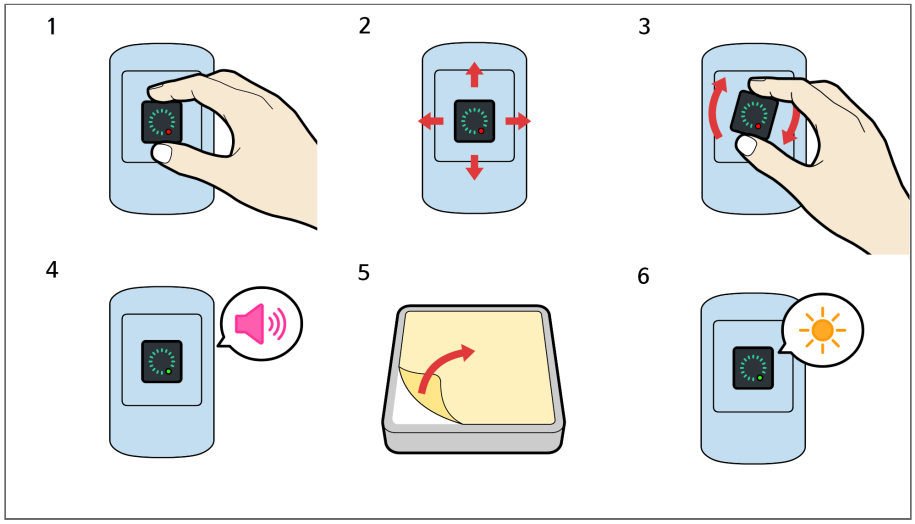
Resumen de instalación

Encuentre la ubicación donde el lector alimenta el Airfob Patch mediante su campo RF.



Verifique la ubicación de instalación del Airfob Patch

Antes de fijar permanentemente el Airfob Patch al lector de control de acceso con la cinta adhesiva incluida, encuentre la mejor ubicación en el lector siguiendo las acciones del diagrama y las instrucciones a continuación.



1. Coloque el Airfob Patch sobre el lector de control de acceso para que se toquen.
2. Encuentre un punto donde el LED del Airfob Patch parpadee en verde al menos una vez por segundo.
3. Sostenga el Airfob Patch sobre el lector o fíjelo temporalmente con cinta removible. Enrolle el Airfob Patch con la aplicación BioStar Air. Para obtener más información, consulte Configurar Airfob Patch y Tag.
4. Realice al menos cinco autenticaciones de prueba con una credencial móvil de Airfob o BioStar Air.
5. Retire la película protectora de la cinta adhesiva de doble cara en la parte posterior del Airfob Patch.
6. Fije permanentemente el Airfob Patch al lector de control de acceso.

Información

- El Airfob Patch no requiere una fuente de alimentación adicional. Al fijarlo al lector de control de acceso, el dispositivo se enciende.
- Cuando fije el Airfob Patch a un lector con la cinta adhesiva de doble cara incluida, considérelo permanente. Si retira el Airfob Patch, podría dañarlo y hacer imposible volver a usarlo.

Solución de Problemas

▼ P. El lector de control de acceso no emite cinco pitidos consecutivos.

Si el lector de control de acceso no emite cinco pitidos consecutivos, reinicie el Airfob Patch.

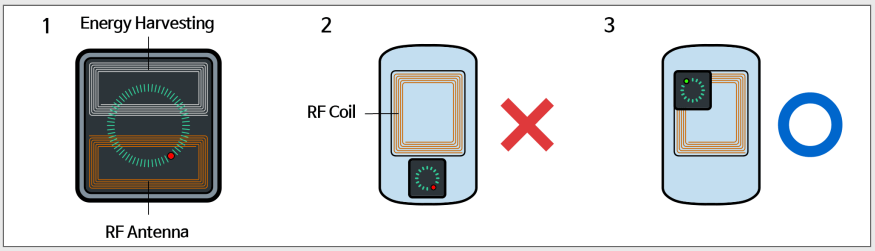
1. Desconecte el Airfob Patch del lector de control de acceso.
2. Cuando se apaga la alimentación, el LED del Airfob Patch parpadea en rojo durante unos 6 segundos y luego se apaga.
3. Asegúrese de que el Airfob Patch esté apagado y luego comience de nuevo.

▼ P. El LED del Airfob Patch parpadea en rojo.

Si el LED del Airfob Patch parpadea en rojo, ajuste la posición del parche.

1. Mueva el Airfob Patch a otra ubicación en el lector de control de acceso y verifique si el LED parpadea en verde.
2. Si la intensidad de la alimentación es alta, el LED parpadea a intervalos de 0.5 segundos o 1 segundo.
3. Si cambia la posición del Airfob Patch, reinícielo y comience de nuevo.

▼ P. El lector de control de acceso no reconoce el Airfob Patch.



- Los dos dispositivos funcionan correctamente cuando la posición de la bobina RF del lector de control de acceso coincide con la posición de la antena RF del Airfob Patch.
- Si no se conceden derechos de acceso válidos cuando toca el lector de control de acceso con un dispositivo móvil, ajuste o rote el Airfob Patch para encontrar una ubicación en la que funcione correctamente.
- La posición y la orientación del Airfob Patch pueden variar según el lector de control de acceso.
- El rango de funcionamiento del Airfob Patch puede ser pequeño o grande según la intensidad de la señal RF del lector de control de acceso y la posición y el tamaño de la bobina RF.

Configurar el módulo seguro SIO2

El módulo seguro SIO2 mejora la seguridad del sistema de control de acceso al actuar como intermediario entre el lector compatible con BioStar Air y los relés. Se comunica con el lector mediante un **cable RS485** y evita brechas de seguridad a través de comunicación cifrada.

> **Precaución**
> Consulte el diagrama de cableado incluido en el paquete del producto para obtener instrucciones precisas de instalación del **módulo seguro SIO2**. Dado que los métodos de instalación pueden variar según el entorno, solicite asistencia profesional a un distribuidor de Suprema.

Habilitar SIO2 en el portal BioStar Air

Habilite la opción **SIO2** siguiendo estos pasos para integrar correctamente el módulo seguro SIO2 y mejorar la seguridad del sistema de control de acceso.

> **Información**
> Si SIO2 está instalado pero no se modifican los ajustes en el portal BioStar Air, podría no funcionar.

1 Registrar el lector

- Verifique que el lector, el SIO2 y el relé de la puerta estén conectados correctamente.
- Registre el lector en el sitio a través de la **aplicación BioStar Air**.

2 Verificar la conexión del dispositivo

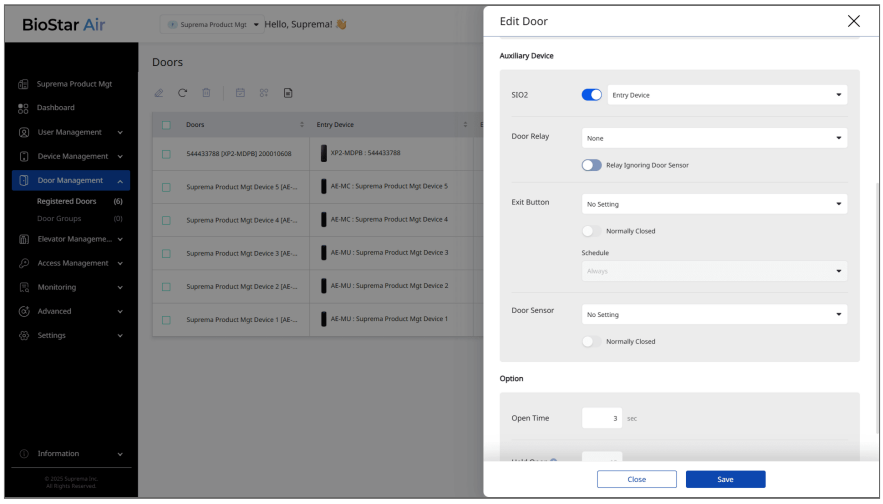
1. Acceda al portal BioStar Air.
2. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
3. En la lista de dispositivos, verifique que el dispositivo aparezca en **verde** (🟢) para confirmar la conexión.

3 Asignar SIO2 a una puerta

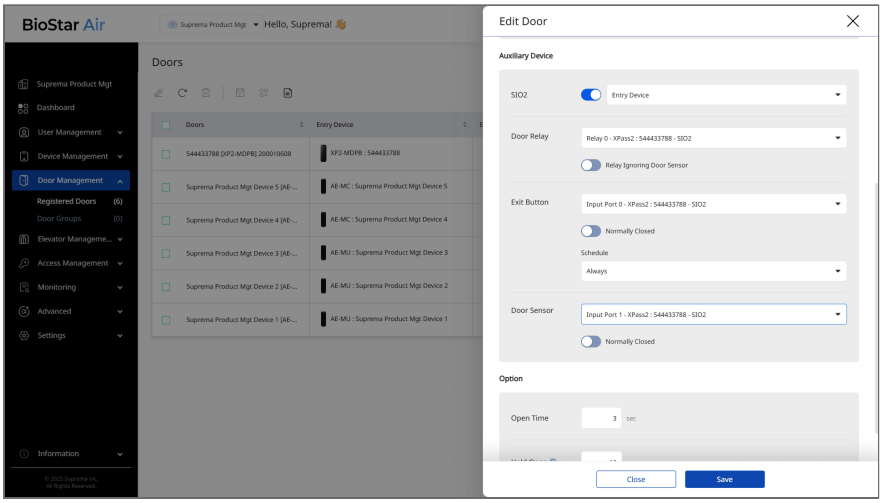
1. Haga clic en **Gestión de Puerta** → **Registrados Puerta** en la barra lateral izquierda.
2. Haga clic en la puerta vinculada al dispositivo en la lista. Al registrar el dispositivo, se crea automáticamente una puerta.

4 Habilitar SIO2

1. Cuando aparezca el panel **Editar puerta**, vaya a **Dispositivo auxiliar**.
2. Habilite la opción **SIO2**.



5 Configurar relé y sensores



La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

- Para **Relé de puerta**, seleccione **Relay 0**.

> El módulo SIO2 solo tiene un puerto de relé de puerta.

- Para **Sin ajustes**, seleccione el número de puerto de entrada del SIO2 conectado.
- Si **Botón de salida** está conectado, seleccione el puerto de entrada correspondiente en el SIO2.
- Si se utiliza otro tipo de dispositivo de salida, seleccione **Dispositivo de salida**.

6 Guardar la configuración

- Haga clic en **Guardar** para aplicar la configuración.
- El módulo seguro SIO2 ahora funciona con normalidad.

Cableado y configuración del escáner QR E200

Paso 1: Cablear

Conecta el escáner QR de la serie E200 usando el cable adaptador incluido como se muestra a continuación.

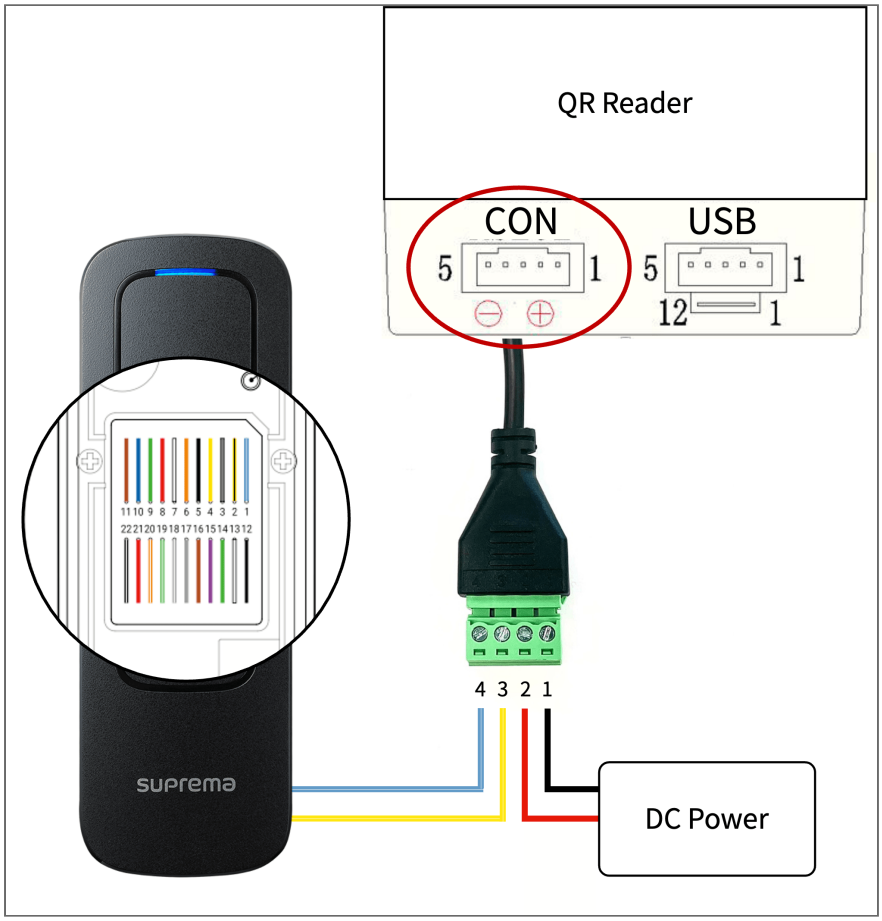
- El bloque de terminales verde tiene pines etiquetados del **1 al 4**, dispuestos de **derecha a izquierda** cuando estés frente al conector.

Pin	Color del cable	Función
1	Negro	Negativo / Tierra
2	Rojo	Positivo (V+)
3	Amarillo (franja blanca)	RS-485 TRXN

Pin	Color del cable	Función
4	Azul (franja blanca)	RS-485 TRXP

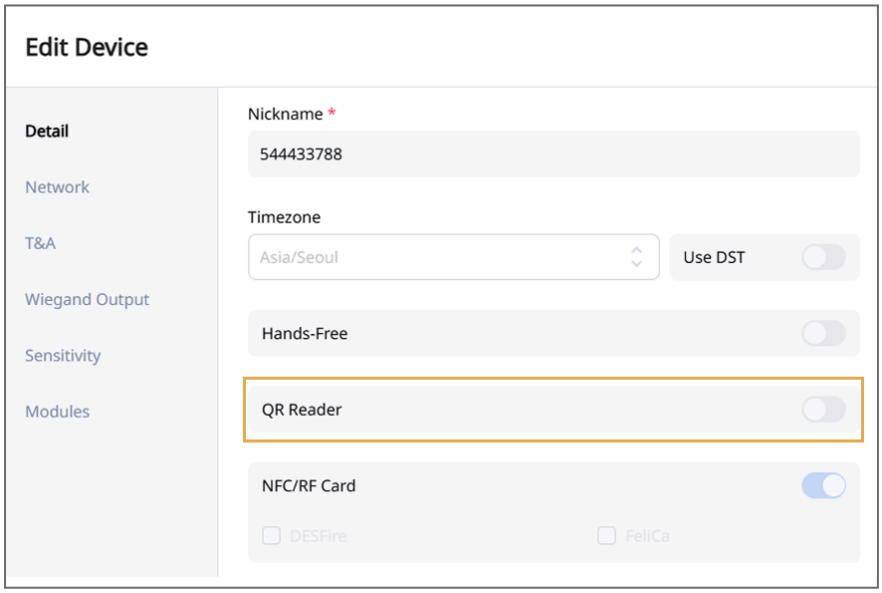
> **Información**
> La dirección del cableado es exactamente opuesta a la de muchos otros conectores. Verifica la orientación nuevamente antes de cablear.

- Conecta el conector de 4 pines al puerto CON en la parte inferior del escáner QR. Como el conector está **polarizado** (con muesca), solo encaja en una posición.



Paso 2: Habilitar el lector QR

1. Inicia sesión en el portal de BioStar Air (web o app).
2. Haz clic en **Gestión de dispositivos** → **Dispositivos registrados** en la barra lateral izquierda.
3. Haz clic en el dispositivo que tiene conectado el escáner QR E200.
4. Habilita la opción **Lector QR** en la sección **Detalle**.



5. Haz clic en **Guardar** para guardar los cambios.

> **Información**
> Habilitar el lector QR impide que uses otros dispositivos RS-485 (por ejemplo, un SIO2) en el mismo lector.

Paso 3: Configurar el escáner QR

Por defecto, el **escáner QR E200** viene configurado con una velocidad de baudios de **115,200**. Cambia la velocidad de baudios a **9,600** para usarlo con dispositivos Suprema.

Conecta el escáner QR al dispositivo y **escanea el código de barras a continuación** para aplicar la nueva velocidad de baudios.



Cuando el cableado sea correcto y el dispositivo Suprema esté conectado a la red, utiliza las **credenciales QR dinámicas** proporcionadas a través de BioStar Air.

Identificar puertos y dispositivos de red

BioStar Air y los dispositivos compatibles deben acceder a puertos de red específicos para garantizar una conexión fluida. Estos puertos permiten la comunicación segura entre los dispositivos compatibles, los servicios en la nube y las aplicaciones de los usuarios. En ciertos casos, los administradores necesitan determinar la dirección MAC de un dispositivo compatible con BioStar Air a partir de su número de serie para realizar tareas de configuración de red.

Puertos de red necesarios

Verifique que los siguientes puertos estén abiertos en el firewall de la red.

- **6379**, **6381**: Puertos de Redis

  Se utilizan para sincronizar la información de usuario, gestionar el registro rápido de eventos, administrar sesiones y actuar como un intermediario de mensajes para la señalización entre los dispositivos y la nube.

- **5671**: AMQP sobre TLS (RabbitMQ)

  Proporciona un protocolo de mensajería seguro para la comunicación en tiempo real entre servicios.

- **443**: HTTPS (TLS)

  Se utiliza para el tráfico web estándar y seguro y es necesario para los siguientes servicios:

  – Acceso a la aplicación web del portal de administración desde un navegador

  – Aplicación móvil BioStar Air (iOS/Android)

  – Llamadas a la API

  – Actualizaciones de firmware de los dispositivos a través de la nube

  – Servicios de inicio de sesión y autenticación para dispositivos

- Al usar la función integrada de gestión de video de BioStar Air:

  – Dominio WebSocket: eu-wss-api.airfob.com

  – Puerto WebSocket: 3500

  – Puertos TURN/STUN: 80, 443, 3478, 5349

> **Información**
> Verifique el acceso a los siguientes puntos de conexión para el inicio de sesión y la autenticación de dispositivos.
> - https://e-afs-api.airfob.com/v1/device/login (Europe)
> - https://afs-api.airfob.com/v1/device/login (Rest del mundo)

Comprobar la dirección MAC a partir del número de serie

En algunos casos, los administradores necesitan determinar la dirección MAC de un lector compatible con BioStar Air utilizando únicamente su número de serie. Esto resulta útil para tareas como añadir el dispositivo a una lista blanca antes de conectarlo a la red.

Pasos

1. **Localice el número de serie**:

   Localice el número de serie de 9 dígitos en la parte posterior del dispositivo.

2. **Convierta el número de serie a hexadecimal**:

   Utilice una calculadora o una herramienta en línea para convertir el número de serie de decimal a hexadecimal.

3. **Extraiga los últimos 3 bytes**:

   Tome los últimos seis caracteres del valor hexadecimal; estos seis caracteres representan los últimos 3 bytes.

4. **Construya la dirección MAC**:

   La dirección MAC siempre comienza con `00:17:FC:`. Añada los últimos 3 bytes (seis caracteres) del valor hexadecimal, separando cada par con dos puntos.

Ejemplo

1. **Número de serie**: 546089489
2. **Hexadecimal**: 208CAA11
3. **Últimos 3 bytes**: 8CAA11
4. **Dirección MAC**: 00:17:FC:8C:AA:11

Estos pasos permiten identificar con precisión un lector compatible con BioStar Air en la red mediante su número de serie.

Convertidor de direcciones MAC

Ingrese a continuación el número de serie del dispositivo para obtener su dirección MAC al instante.

Credencial de usuario

Con la aplicación Suprema Pass puedes abrir puertas usando solo tu smartphone. Esta guía cubre las funciones clave de la aplicación — desde la elección de los métodos de autenticación Bluetooth, NFC o código QR y la configuración de la autenticación en 2 pasos, hasta el ajuste de la sensibilidad de detección del Bluetooth.

Uso de credenciales móviles

Utilice credenciales móviles en lugar de tarjetas RFID plásticas para abrir las puertas con la app Suprema Pass. Acerque el dispositivo móvil al lector mediante Bluetooth o NFC, mantenga presionada la tarjeta o escanee un código QR para abrir las puertas.

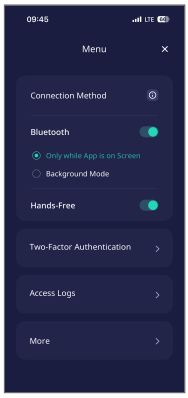
> **Información**
>
> La app Suprema Pass actúa como interfaz de usuario del sistema BioStar Air y funciona principalmente como una billetera digital para credenciales móviles. Los usuarios emiten y almacenan en la app las tarjetas de acceso móviles para ingresar a áreas seguras con sus dispositivos móviles.

Requisitos y preparación

Cumpla los siguientes requisitos para abrir puertas con credenciales móviles.

- Debe instalarse un dispositivo de control de acceso compatible con las credenciales móviles de Suprema Pass.
- Instale la app Suprema Pass en el dispositivo móvil.
  - iOS
  - Android
- Active Bluetooth o NFC en el dispositivo móvil.
- Activar la autenticación en dos pasos desactiva **Modo en segundo plano**.
- El administrador debe habilitar la autenticación QR en el portal de BioStar Air.
- Verifique que el sitio admita el método de acceso manos libres.

> **Información**
>
> - Los servicios de ubicación son necesarios para autenticar la tarjeta de acceso móvil en Suprema Pass. Consulte las preguntas frecuentes relacionadas en ¿Por qué se me solicita activar los servicios de ubicación?.
> - Siga las instrucciones proporcionadas para solucionar el problema si la tarjeta móvil se autentica con el dispositivo pero la puerta no se abre. Consulte las preguntas frecuentes relacionadas en Solucionar problemas con la tarjeta móvil.



Establecer método de conexión

Seleccione entre dos modos de funcionamiento en la app Suprema Pass. En la pantalla de inicio de la app Suprema Pass, toque ☰ en la esquina superior derecha y luego seleccione el modo deseado en **Método de conexión**.

- **Solo mientras la app esté en pantalla**: Abra la puerta solo cuando la app aparezca en pantalla y la tarjeta móvil sea visible.
- **Modo en segundo plano**: Abra la puerta incluso si el teléfono está bloqueado cuando la app se ejecuta en segundo plano.

> **Información**
> Independientemente del modo, acerque el dispositivo móvil al lector para autenticarse.

Abrir puertas

Use la app Suprema Pass para abrir puertas de varias formas.

Acerque su dispositivo móvil a un lector

Acerca el dispositivo móvil a un lector compatible con BioStar Air y autentícate mediante Bluetooth o NFC para abrir la puerta.

1. Asegúrate de que la app Suprema Pass esté abierta.
2. Acerca la zona de la antena Bluetooth o NFC del dispositivo móvil al lector.
3. La puerta se abre cuando la credencial móvil se autentica.

> **Información**
> - Elige entre dos modos de comunicación. Para más información, consulta Configurar funciones avanzadas.
>   - **Modo Bluetooth**: El dispositivo móvil se comunica de forma inalámbrica con el lector.
>   - **Modo NFC**: Disponible solo en dispositivos Android; acerca el dispositivo móvil al lector para autenticarte.
> - La ubicación de la antena Bluetooth o NFC varía según el modelo. Consulta las especificaciones del dispositivo para conocer el punto de contacto óptimo.

Toca y mantén presionada la tarjeta móvil

Toque y mantenga presionada la tarjeta móvil en la app Suprema Pass para abrir la puerta.

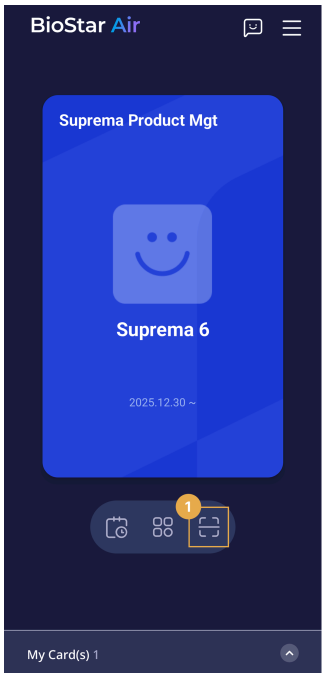
1. Muestra la pantalla principal de la app Suprema Pass.
2. Toque y mantenga presionada la tarjeta móvil cerca de un lector compatible con BioStar Air durante 2–3 segundos.
3. La puerta se abre cuando la credencial móvil se autentica.

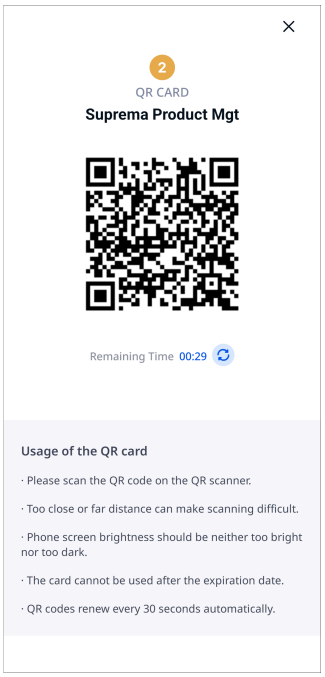
Información

- Selecciona **Modo en segundo plano** en **Método de conexión** para usar esta función. Para más información, consulta Establecer método de conexión.
- Por motivos de seguridad, **el administrador del sitio puede deshabilitar esta función**.
- **El alcance efectivo** varía según la potencia Bluetooth del dispositivo móvil.
- Los lectores de control de acceso cercanos pueden provocar autenticaciones no deseadas.

Autenticación QR

Si el administrador habilita la opción **Lector QR** en el portal BioStar Air, puedes abrir la puerta escaneando el código QR desde la app Suprema Pass con un lector de códigos QR. En la pantalla principal de la app Suprema Pass, toca el icono debajo de la tarjeta móvil.





Información

- Para más información sobre la opción **Lector QR**, consulta Configuración de funciones adicionales.
- La autenticación QR está disponible únicamente en puertas equipadas con un lector de códigos QR.

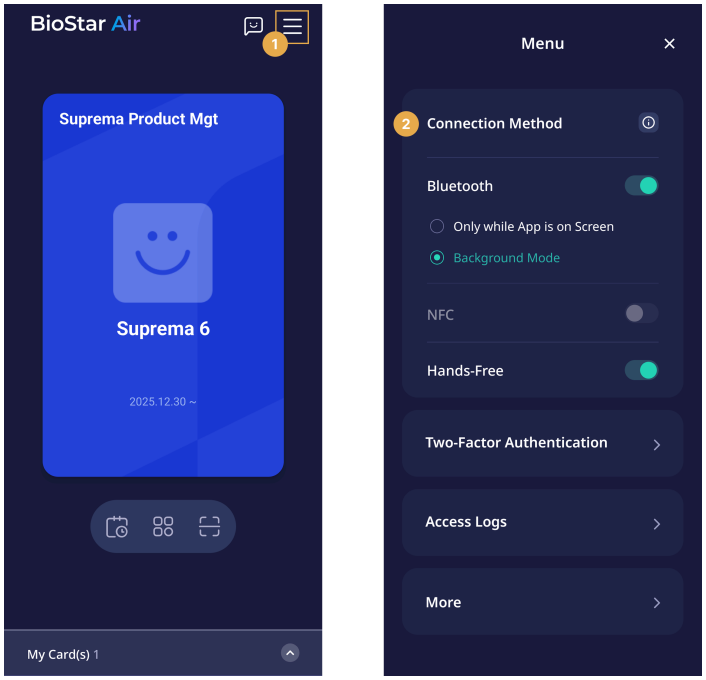
Configurar funciones avanzadas

La app Suprema Pass incluye ajustes avanzados y opciones de seguridad para mejorar la experiencia del usuario y las funciones de control de acceso. Los usuarios pueden configurar los métodos de autenticación, habilitar la autenticación de dos factores, revisar los registros de acceso, reportar problemas y usar las opciones de soporte.

Configurar método de conexión

Seleccione un método de conexión preferido para comunicarse con el dispositivo de control de acceso. En la pantalla

principal de la app Suprema Pass, toque ☰ en la esquina superior derecha, luego seleccione el modo deseado en **Método de conexión**.



Bluetooth

Elija entre dos modos de autenticación por Bluetooth.

- **Solo mientras la app esté en pantalla**: autenticar con la tarjeta móvil únicamente cuando la app esté abierta en el dispositivo. Este modo ahorra batería, pero requiere abrir la app manualmente antes de acercarse a la puerta.
- **Modo en segundo plano**: autenticar con la tarjeta móvil incluso si la pantalla del dispositivo está apagada cuando la app se ejecuta en segundo plano. Este modo es más cómodo pero consume más batería. Si la app se cierra, vuelva a abrirla para reanudar las funciones en segundo plano.

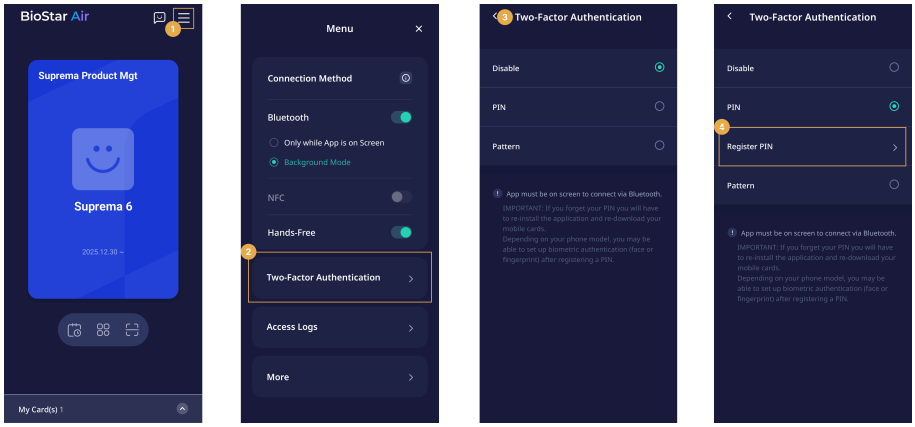
NFC

La autenticación por NFC está disponible solo en dispositivos Android. Utilice NFC solo o junto con Bluetooth para un acceso más rápido.

> **Información**
> Los usuarios de Android con un dispositivo compatible con NFC pueden usar NFC junto con Bluetooth.

Autenticación de dos factores (2FA)

Habilite la autenticación de dos factores con un **PIN, un patrón o autenticación biométrica** (reconocimiento facial o huella dactilar) para mayor seguridad.



Información

- Esta función no es compatible con las conexiones en **Modo en segundo plano** porque la pantalla de la app debe permanecer abierta durante la autenticación de acceso.
- Si se olvida el PIN o el patrón, reinstale la app y reactive la tarjeta móvil.
- Las funciones compatibles pueden variar según el dispositivo móvil.

Usuarios de iOS

1. En la pantalla principal de la app Suprema Pass, toque ☰ en la esquina superior derecha.
2. Establezca el método de conexión en **Solo mientras la app esté en pantalla**.
3. Toque **Autenticación de dos factores**.
4. Toque **Registrar PIN**.
5. Ingrese el PIN de seis dígitos.
6. Cuando aparezca la notificación de éxito, toque **Aceptar**.

Información

- Toque **Cambiar PIN**, luego ingrese el nuevo PIN para cambiarlo.
- Active **Autenticación Biométrica** y siga las instrucciones de configuración para usar la biometría.

Usuarios Android

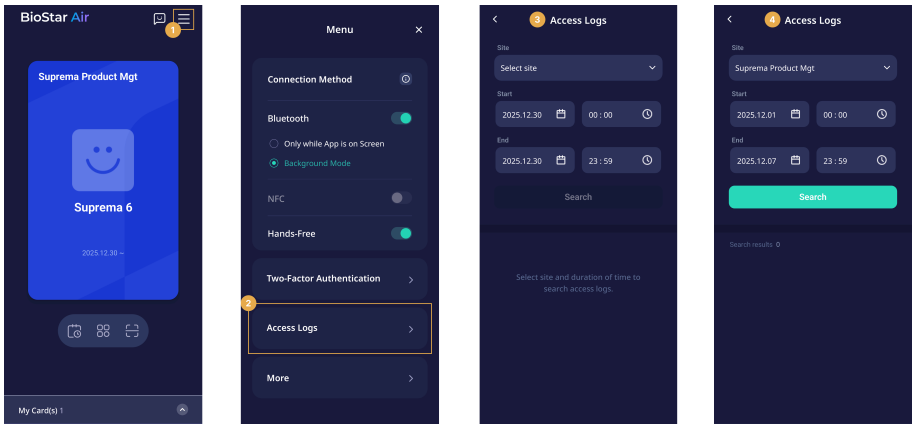
1. En la pantalla principal de la app Suprema Pass, toque ☰ en la esquina superior derecha.
2. Configure el método de conexión en **Solo mientras la aplicación esté en pantalla** o **NFC**.
3. Toque **Autenticación de dos factores**.
4. Toque **PIN** → **Registrar PIN** o **Patrón** → **Registrar Patrón**.
5. Ingrese el PIN o patrón seleccionado.
6. Cuando aparezca la notificación de éxito, toque **Aceptar**.

Información

- Toque **Cambiar PIN**, luego ingrese el nuevo PIN para cambiarlo.
- Toque **Cambiar Patrón**, luego ingrese el nuevo patrón para cambiarlo.
- Active **Autenticación Biométrica** y siga las instrucciones de configuración para usar la biometría.

Registros de acceso

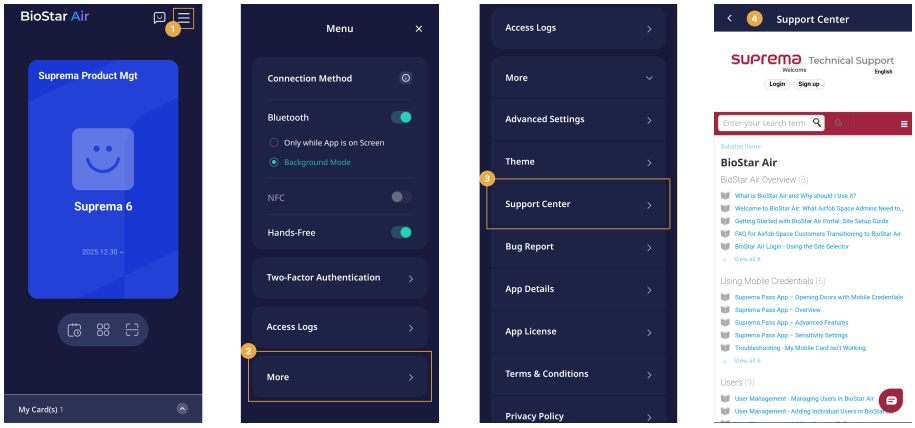
Utilice los registros de acceso para rastrear intentos de acceso y solucionar problemas relacionados con el acceso.



1. En la pantalla principal de la app Suprema Pass, toque ☰ en la esquina superior derecha.
2. Toque **Registros de acceso**.
3. Seleccione un sitio y luego establezca las fechas de inicio y fin.
4. Toque **Buscar**.

Centro de soporte

Vaya a **Centro de soporte** para obtener asistencia adicional.



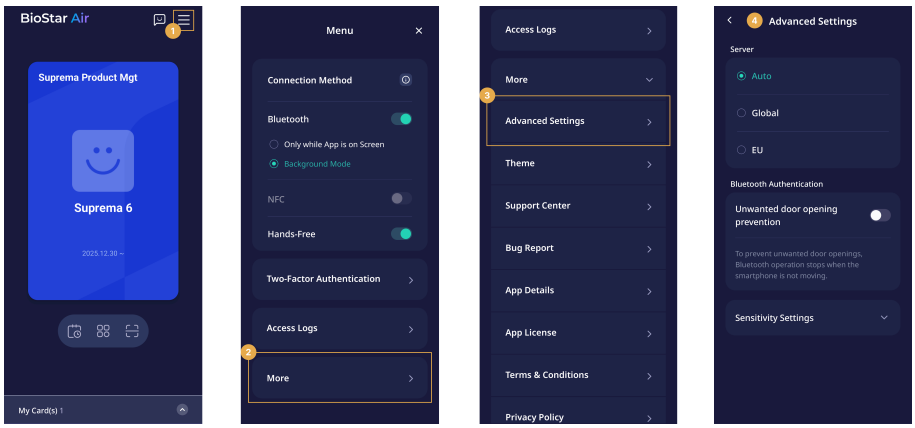
1. En la pantalla principal de la app Suprema Pass, toque ☰ en la esquina superior derecha.
2. Toque **Más**.
3. Toque **Centro de soporte**.

4. Vaya a la página **Soporte técnico de Suprema**.

- Busque preguntas o revise las preguntas frecuentes.
- Si necesita asistencia, toque el icono de chat en la esquina inferior derecha para enviar un ticket al equipo de MOCA Systems.

Configuración Avanzada

Toque ☰ en la esquina superior derecha de la pantalla de inicio de la aplicación Suprema Pass, luego seleccione **Más** → **Configuración Avanzada** para usar las siguientes funciones adicionales.



- **Configuración de ubicación**: Seleccione el servidor **Global** o **EU** según su ubicación. Seleccione **Auto** para que la app detecte su ubicación y elija el servidor adecuado.
- **Autenticación Bluetooth**: Active **Prevención de apertura no deseada** para bloquear la autenticación Bluetooth cuando el dispositivo móvil está inmóvil.
- **Configuración de Sensibilidad**: Ajuste la sensibilidad Bluetooth entre el dispositivo móvil y el lector compatible con BioStar Air. Para más información, consulte Ajustar la sensibilidad Bluetooth.

Funciones adicionales

Toca ☰ en la esquina superior derecha de la pantalla principal de la app Suprema Pass, luego selecciona **Más** para acceder a las siguientes funciones.

- **Tema**: Establece el modo de color de la app. Selecciona **Claro**, **Oscuro** o **Sistema**.
- **Informe de errores**: Escribe información detallada, como el contexto en el que ocurrió el error y los pasos para reproducirlo, para enviar el informe al desarrollador.
- **Detalles de la app**: Consulta el nombre del modelo, la versión del sistema operativo y el soporte y el estado de BLE del dispositivo móvil.
- **Licencia de la app**: Consulta la información sobre las licencias de código abierto utilizadas en la app Suprema Pass.
- **Términos y condiciones**: Consulta los términos de uso de la plataforma BioStar Air.

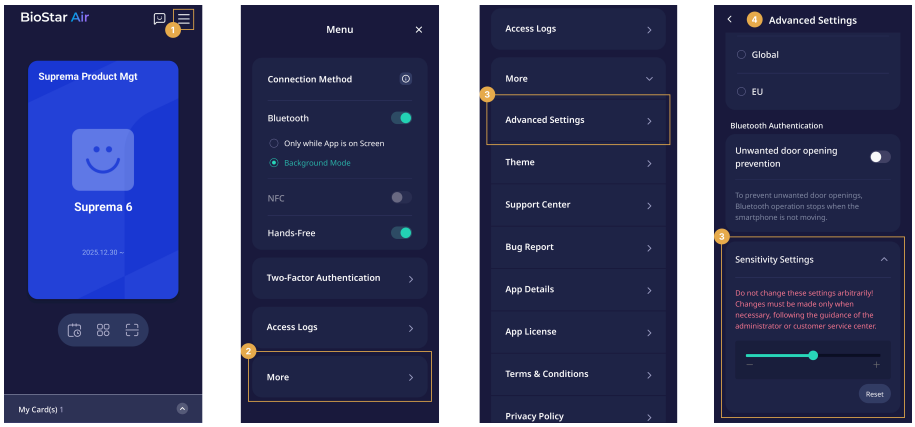
Ajustar la sensibilidad Bluetooth

Con la función **Ajustes de sensibilidad** puede ajustar la sensibilidad Bluetooth entre el dispositivo móvil y el lector compatible con BioStar Air. Esta función ayuda a garantizar autenticaciones fluidas y reduce intentos de acceso no autorizados y fallos de autenticación.

> **Información**
>
> Dado que la intensidad de la señal Bluetooth varía según el modelo de dispositivo móvil, los usuarios pueden experimentar distintos rangos de detección. Factores ambientales, como paredes, interferencias o la ubicación de los lectores compatibles con BioStar Air, también pueden afectar la detección Bluetooth.

Ajuste la configuración de sensibilidad

Los usuarios pueden ajustar con precisión la sensibilidad de la autenticación Bluetooth según la intensidad de la señal del dispositivo móvil y sus preferencias.



1. En la pantalla principal de la app Suprema Pass, toque ☰ en la esquina superior derecha.
2. Toque **Más**.
3. Toque **Ajustes avanzados**.
4. Toque **Ajustes de sensibilidad**, luego mueva el control deslizante para ajustar la sensibilidad.

> **Información**
>
> - Mueva el control deslizante hacia − para disminuir la sensibilidad y bloquear autenticaciones no deseadas.
>
> *Por ejemplo, cuando el dispositivo móvil está sobre un escritorio*
>
> - Si la autenticación falla, mueva el control deslizante hacia + para aumentar la sensibilidad. Sin embargo, el dispositivo móvil debe estar muy cerca de un lector compatible con BioStar Air.

Consejo

Consejos para usuarios de iOS

Si acerca un iPhone con Apple Pay a un lector compatible con BioStar Air, Apple Pay se activará. Esto ocurre porque se detecta la zona NFC del dispositivo móvil junto con la autenticación de la tarjeta móvil.

Solución: Ajuste la configuración de sensibilidad hacia + para que un lector compatible con BioStar Air detecte antes la señal Bluetooth del dispositivo móvil, eliminando la necesidad de contacto físico con el dispositivo. Esto permite un acceso fluido y evita que se active Apple Pay.

Desarrollador

BioStar Air ofrece una API RESTful en la nube que puedes utilizar para integrarla con sistemas externos, automatizar el ciclo de vida de los usuarios y gestionar las credenciales. Configura un entorno de demostración y comprende el flujo de autenticación; a continuación, implementa la integración con la API de gestión de usuarios.

Inicio rápido

Esta guía explica cómo configurar el sitio de demostración de BioStar Air, conectar y registrar dispositivos compatibles y probar la integración de la API en la nube. Si has trabajado con BioStar 2 antes, muchos conceptos te resultarán familiares. BioStar Air está completamente basado en la nube.

Requisitos previos

Antes de comenzar, comprueba lo siguiente.

- Prepara un **dispositivo compatible con BioStar Air** con el firmware en estado de fábrica.
  - XP2-AIR, XS2-AIR, BEW3-AIR, BS3-AIR, BLN2-AIR
  - Los dispositivos pueden comprarse a través de distribuidores autorizados de Suprema.
- El dispositivo debe estar conectado a Internet mediante Ethernet.
- Permite el acceso saliente en la red.
  - Puerto 443 (HTTPS)
  - Puerto 5671 (MQTT sobre TLS)

Configura el entorno de demostración y la clave de API

1 Regístrate e inicia sesión

1. Ve a BioStar Air Developer.
2. Haz clic en **Regístrate**, completa el formulario y espera la aprobación.
3. Después de la aprobación, inicia sesión con el correo electrónico y la contraseña de tu cuenta del Portal de desarrolladores.

> **Información**
> La dirección de correo electrónico y la contraseña utilizadas en el Portal de desarrolladores no se pueden usar en el Portal de demostración.

2 Crea una aplicación de demostración

1. Ve a **API** → **Gestión**.
2. Haz clic en **+ Registrar**.
3. Selecciona **Demo** como tipo de aplicación.
4. Introduce un nombre para la aplicación y haz clic en **Registrar**.
5. Después de registrar la aplicación de demostración, puedes descargar el archivo *site_info.csv*.

> **Información**
>
> - El archivo *site_info.csv* contiene el alias de correo electrónico y la contraseña.
> - Al iniciar sesión en el portal de demostración, asegúrate de usar este alias de correo electrónico y la contraseña.
> - **No uses el correo electrónico y la contraseña del Portal de desarrolladores en el Portal de demostración.**

3 Generar una clave API

1. Ve a **API** → **Gestión**.
2. Haz clic en la aplicación que registraste.
3. Desplázate hasta **Gestión de API**.
4. Haz clic en **Agregar**.
5. Introduce un nombre y confirma.
6. Copia la clave API generada y guárdala de forma segura.

Esta clave API se usa para autenticar las llamadas a la API en el entorno de demostración.

4 Inicia sesión en el portal de demostración

1. Haz clic en **Portal de demostración** en el menú del Portal de desarrolladores o ve directamente a https://demo.airfobspace.com/login.
2. Inicia sesión con el alias de correo electrónico y la contraseña del archivo *site_info.csv*.

> **Información**
>
> **No uses el correo electrónico y la contraseña del Portal de desarrolladores en el Portal de demostración.**

Registrar dispositivos

Usa la aplicación BioStar Air Demo (solo Android) en tu dispositivo móvil.

1. Ve al enlace BioStar Air Developers y descarga la aplicación de demostración.
2. Abre la aplicación de demostración e inicia sesión con el alias de correo electrónico y la contraseña del archivo *site_info.csv*.
3. Acerca tu dispositivo Android al lector (dentro del alcance BLE).
   - En **Menú principal** → **Dispositivos**, pulsa el botón + en la esquina superior derecha.
   - Busca el dispositivo y pulsa **Registrar**.
4. El dispositivo emite un pitido, se reinicia y aparece en la lista de dispositivos registrados.

> **Información**
> Los dispositivos solo se pueden registrar a través de la aplicación móvil. No es posible registrar dispositivos desde el portal web. El registro mediante API requiere un certificado de cifrado que no se proporciona a los socios.

Gestión Dispositivos

Gestiona los dispositivos desde la app Demo o desde el portal web de demostración.

- **BioStar Air Demo App**
- **Portal web de demostración:** https://demo.airfobspace.com/login

Demo vs producción

- Un sitio **Demo** para pruebas se crea a través del Portal de desarrolladores.
- Un sitio de producción se crea a través del Portal de socios y requiere un ID de sitio, correo electrónico de usuario y contraseña. Solo los revendedores autorizados o las sucursales de Suprema pueden crear un sitio de producción.

> **Información**
> - Los ID de usuario y los ID de cuenta son diferentes. No los confundas.
> - Si administra varios sitios, guarde las contraseñas de forma segura.
> - Utilice siempre el token Bearer más reciente.
> - Un token Bearer copiado del navegador puede reutilizarse en Postman.

¿Necesita ayuda?

Abra un ticket en el Portal de Soporte Técnico de Suprema. https://support.supremainc.com

Autenticación de la API

La API de BioStar Air Cloud utiliza autenticación basada en tokens Bearer (JWT). Debe obtener un token mediante el proceso de inicio de sesión antes de hacer llamadas a la API e incluirlo en el encabezado Authorization de cada solicitud.

URLs base de la API

Entorno	URL base	Descripción
Demo (prueba)	https://sp-demo-api.airfob.com/v1	Cuando el tipo de aplicación esté registrado como "Demo", puede descargar el sitio del entorno de demostración y la información de la cuenta maestra del sitio en un archivo csv.
Producción (en vivo)	https://sp-api.airfob.com/v1	(**Auto-Routing**) Selecciona automáticamente el servidor global o el de la UE según la región del cliente.
	https://sp-a-api.airfob.com/v1	(**Global Dedicated**) Se conecta al entorno del servidor global.
	https://sp-e-api.airfob.com/v1	(**EU Dedicated**) Se conecta al entorno del servidor EU(Europe).

> El entorno **Auto-Routing** puede ocasionar un enrutamiento inesperado según la detección de la región.

Flujo de inicio de sesión de la API

Realice llamadas a la API con Postman o de forma programática.

Iniciar sesión

- **Endpoint**: `login`
- **Payload**:

```
{
  "username": "your_email",
  "password": "your_password"
}
```

Devuelve un token Bearer (JWT).

Obtener información de la cuenta

- **Endpoint**: `getSelfAccounts`
- **Authorization**: token Bearer

Devuelve una lista de sitios y cuentas a los que puede acceder.

Iniciar sesión en una cuenta

- **Endpoint:** `loginAccount`
- **Authorization:** token Bearer

Devuelve un token específico del sitio.

Cómo obtener un token Bearer desde un navegador web

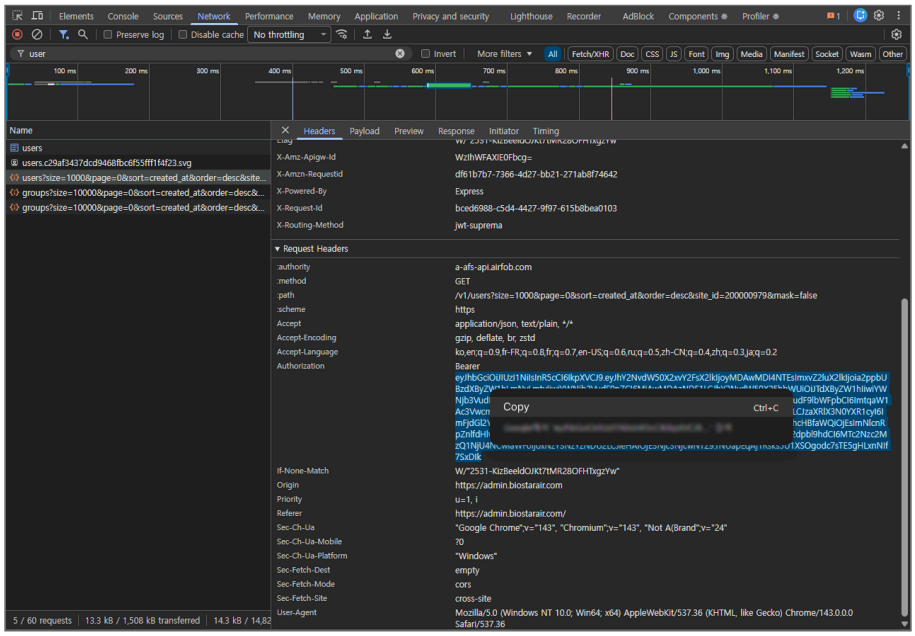
Puede obtener el token Bearer directamente desde el navegador usando las herramientas de desarrollo, sin necesidad de Postman.

Chrome/Edge (Windows o Mac)

1. En el navegador web, presione `F12` o `Ctrl/Cmd + Shift + I`.
2. Vaya a la pestaña **Network**.
3. Actualice la página.
4. Busque llamadas a la API.

   > *p. ej.,* `groups`, `login`

5. Haga clic en la petición en la lista.
6. Vaya a la pestaña **Headers**.
7. En los encabezados de la petición, busque `Authorization: Bearer ...`.
8. Haga clic con el botón derecho en el token y cópielo.



Safari (Mac)

1. Active el menú **Developer**. En Safari, vaya a Preferences → Advanced y marque **Show Develop menu**.
2. Vaya a **Develop → Show Web Inspector**.

3. Vaya a la pestaña **Network**.
4. Actualice la página.
5. Filtre e inspeccione las llamadas a la API.
6. Copie el token `Authorization: Bearer` de los encabezados de la petición.

> **Información**
> Un token Bearer copiado del navegador puede reutilizarse en Postman. Use siempre el token Bearer más reciente.

Uso de la API de gestión de usuarios

Después de obtener un token de autenticación, puedes gestionar el ciclo de vida de los usuarios a través de la API. Utiliza los endpoints para recuperar, crear, actualizar y desactivar usuarios y así automatizar la gestión de usuarios en tu sitio de BioStar Air.

Alcance recomendado para la integración con la API

Limita la integración con la API al alcance que se muestra a continuación, siempre que sea posible.

- Gestión del ciclo de vida de los usuarios (crear/actualizar/eliminar)
- Gestión de credenciales (móvil, tarjeta RF, biométrica)

Permite que los administradores sigan usando las aplicaciones web y móviles de gestión de BioStar Air.

- Nivel de acceso
- Horarios
- Configuración de puertas y dispositivos
- Configuración del sitio

Llamadas a la API de gestión de usuarios

Después de iniciar sesión, utiliza los siguientes endpoints para gestionar usuarios.

- `getUsers`
- `createUser`
- `updateUser`
- `suspendUsers`

Incluye siempre un token Bearer en el encabezado Authorization.

Para activar a un usuario, asigna al menos un tipo de credencial.

> *p. ej., tarjeta RF, móvil, LinkPass*

Aplicación de ejemplo

El siguiente código de ejemplo es una aplicación en Python que sube un archivo CSV a través de la API y desactiva usuarios en masa.

Python

```
import requests
import csv
import getpass
from pathlib import Path

def select_server():
    servers = {
        "1": ("Demo", "https://demo-afs-api.airfob.com/v1"),
        "2": ("Global", "https://a-afs-api.airfob.com/v1"),
        "3": ("EU", "https://e-afs-api.airfob.com/v1")
    }

    print("Please select a server:")
    for key, (name, _) in servers.items():
        print(f"{key}: {name}")

    choice = input("Enter server number: ").strip()
    return servers.get(choice, (None, None))[1]

def login(base_url, username, password):
    url = f"{base_url}/login"
    payload = {"username": username, "password": password}
    response = requests.post(url, json=payload)
    response.raise_for_status()
    data = response.json()
    token = data.get("access_token")
    if not token:
        raise ValueError("Login succeeded but no access_token returned.")
    print("✅ Login successful.")
    return token

def login_to_account(base_url, token, account_id):
    url = f"{base_url}/login/{account_id}"
    headers = {"Authorization": f"Bearer {token}"}
    response = requests.post(url, headers=headers)
    response.raise_for_status()
    new_token = response.json().get("access_token")
    if new_token:
        print(f"✅ Switched to account ID: {account_id}")
        return new_token
    return token

def get_accounts(base_url, token):
    url = f"{base_url}/accounts/self"
    headers = {"Authorization": f"Bearer {token}"}
    response = requests.get(url, headers=headers)
    response.raise_for_status()
    accounts = response.json().get("accounts", [])
    return [{"id": acc["id"], "name": acc["site"]["name"]} for acc in accounts]

def suspend_users_from_csv(base_url, csv_path, token):
    if not Path(csv_path).exists():
        print(f"❌ File not found: {csv_path}")
        return

    headers = {"Authorization": f"Bearer {token}"}
```

```
    with open(csv_path, newline='', encoding='utf-8-sig') as f:
        reader = csv.DictReader(f)

        # Normalize headers
        reader.fieldnames = [field.strip().lower() for field in reader.fieldnames]
        if 'email' not in reader.fieldnames:
            print("❌ Missing required 'email' column in CSV.")
            return

        for row in reader:
            email = row.get("email")
            if not email:
                print("⚠️ Skipping row with missing email.")
                continue

            # Search user
            search_url = f"{base_url}/users/search"
            payload = {"filters": [{"field": "email", "equals": email}]}
            search_resp = requests.post(search_url, headers=headers, json=payload)
            if search_resp.status_code != 200:
                print(f"❌ Failed to search user {email}: {search_resp.text}")
                continue

            users = search_resp.json().get("users", [])
            if not users:
                print(f"❌ No user found with email: {email}")
                continue

            user_id = users[0]["id"]

            # Suspend user
            suspend_url = f"{base_url}/users/suspend"
            suspend_payload = {
                "ids": [user_id],
                "certify_by": "none",
                "use_site_template": True
            }
            suspend_resp = requests.post(suspend_url, headers=headers, json=suspend_payload)
            if suspend_resp.status_code == 200:
                print(f"✅ Suspended user: {email}")
            else:
                print(f"❌ Failed to suspend user {email}: {suspend_resp.text}")

def main():
    base_url = select_server()
    if not base_url:
        print("❌ Invalid selection. Exiting.")
        return

    print("\n🔑 BioStar Air Login")
    username = input("Email: ")
    password = getpass.getpass("Password: ")

    token = login(base_url, username, password)
    accounts = get_accounts(base_url, token)

    print("\n🌐 Available Sites:")
```

```
    for i, acc in enumerate(accounts):
        print(f"{i}: {acc['name']} (ID: {acc['id']})")

    selected = int(input("\nSelect site number to log into: "))
    account_id = accounts[selected]["id"]
    token = login_to_account(base_url, token, account_id)

    csv_path = input("Enter path to CSV file with user emails: ").strip()
    suspend_users_from_csv(base_url, csv_path, token)

if __name__ == "__main__":
    main()
```

Solución de Problemas

¿Has tenido un problema inesperado al usar BioStar Air? Este documento identifica los problemas más comunes que podrías encontrar y explica cómo solucionarlos.

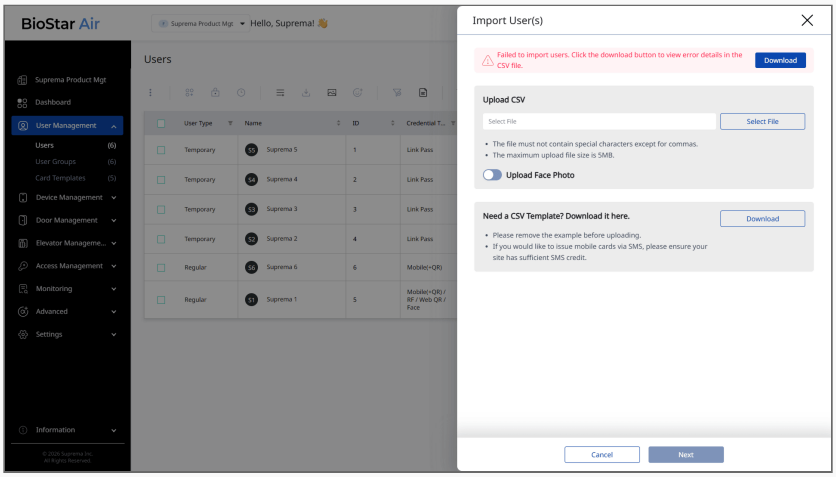
Selecciona un problema a continuación para ver las soluciones paso a paso.

Solución de problemas al agregar usuarios en masa

Varios clientes y socios han informado problemas al agregar listas de usuarios en masa. La mayoría de estos problemas se deben a archivos CSV con formato incorrecto. Siga exactamente las instrucciones a continuación para asegurarse de que la función de adición masiva funcione como se espera.

Información

A partir de la versión v2.10, BioStar Air genera un informe de validación cuando se carga un archivo CSV que contiene entradas no válidas. Corrija los errores y vuelva a cargar el archivo.



Preparar el archivo CSV

Descargar la plantilla CSV

1. Vaya a **Gestión de usuarios** → **Usuarios** en la barra lateral izquierda.
2. Haga clic en **Añadir nuevo usuario** → **Importar usuarios** en la esquina superior derecha de la pantalla.
3. Cuando aparezca el panel **Importar usuarios**, haga clic en **Descargar**.
4. Guarde el archivo de plantilla CSV (*biostar-import-user-csv-example.csv*) localmente.

Usar el formato exacto de la plantilla CSV

- **No agregue ni elimine columnas manualmente**. Una columna inesperada puede causar un error.
- Si necesita incluir campos adicionales (por ejemplo, ID de empleado o departamento), utilice la función **Plantilla de**

Usuario(☰+) en la parte superior de la lista de usuarios para agregarlos. Cuando se agrega un campo, el archivo CSV descargado incluye automáticamente la columna correspondiente.

Ingrese los datos correctamente consultando los requisitos de cada columna.

Clave de usuario

- Un ID numérico único para cada usuario.
- La columna **Clave de usuario puede dejarse en blanco**, y el sistema asigna un valor automáticamente.
- Si ingresa los ID de usuario manualmente
  - Utilice **solo números**.
  - Utilice un **valor único**.
  - No incluya letras, espacios, guiones ni caracteres especiales.

> **Precaución**
> Si debe usar un ID de empleado específico de la empresa que incluya letras, no utilice el campo **Clave de usuario**. En su lugar, cree un campo de usuario personalizado con la función **Plantilla de Usuario**.

Correo electrónico

- Utilice un formato de correo electrónico válido. Consulte las fórmulas de validación para verificar el formato del correo electrónico.
  - No se permiten espacios.
  - Debe incluir el signo arroba (`@`).
  - El dominio debe incluir un punto (`.`) y un dominio de nivel superior.

    Ejemplo: example.com, gmail.com, suprema.co.kr
  - No debe haber ningún punto adicional después de la dirección.
  - No se permiten caracteres especiales ni ocultos.
  - Debe ser una dirección de correo electrónico. Pueden aparecer errores como 'Not provided'.
- La dirección de correo electrónico **debe ser única**. No se permiten duplicados ni en el archivo ni entre los usuarios existentes.
- Se requiere una dirección de correo electrónico para emitir las credenciales que aparecen a continuación.
  - **Tarjeta Móvil**
  - **Web QR**
  - **Pase de enlace**
- Los usuarios que solo tienen una tarjeta RFID no necesitan proporcionar una dirección de correo electrónico.

Móvil

- Proporcionar un número de teléfono es opcional cuando la credencial no se entrega vía SMS.

- Al igual que la dirección de correo electrónico, el número de teléfono **debe ser único** y no se permiten duplicados ni en el archivo ni entre los usuarios existentes.
- Utilice el correo electrónico para enviar las credenciales cuando sea posible. Los SMS generan cargos adicionales.

Fechas (**Fecha de inicio / Fecha de caducidad**)

Todos los campos de fecha deben seguir exactamente el formato que se muestra a continuación.

```
YYYY-MM-DDTHH:MM:SS.sssZ

Example:
1995-05-09T00:00:00.000Z
```

Incluso pequeñas diferencias—por ejemplo, omitir la 'Z', usar barras (`/`) en lugar de guiones (`—`), o no incluir la hora—pueden causar que la carga falle.

Requisitos de credenciales

Tipo de credencial	Correo electrónico o número de teléfono
Solo **Tarjeta RF**	No.
Tarjeta Móvil / **Web QR** / **Pase de enlace**	Sí, se requiere una.

- Las credenciales deben entregarse a una dirección de correo electrónico o a un número de teléfono.
- Se pueden proporcionar ambos, pero las **credenciales móviles** requieren al menos uno.
- El correo electrónico es gratuito. Los SMS generan cargos.

Fórmulas de Excel para la prevalidación

Antes de cargar los datos, utilice las siguientes fórmulas en las **columnas auxiliares** para verificar los datos.

Validación de correos electrónicos o números de teléfono duplicados

Detect Duplicate Emails or Phone Numbers

```
=IF(E2="", "", IF(COUNTIF(E$2:E2, E2)>1, "Duplicate", "First Occurrence"))
```

Validación del formato de fecha

Validate ISO 8601 Date Format (Column Q)

```
=IF(Q2="", "", IF(AND(LEN(Q2)=24,
  ISNUMBER(VALUE(MID(Q2,1,4))), MID(Q2,5,1)="-",
  ISNUMBER(VALUE(MID(Q2,6,2))), MID(Q2,8,1)="-",
  ISNUMBER(VALUE(MID(Q2,9,2))), MID(Q2,11,1)="T",
  ISNUMBER(VALUE(MID(Q2,12,2))), MID(Q2,14,1)=":",
  ISNUMBER(VALUE(MID(Q2,15,2))), MID(Q2,17,1)=":",
  ISNUMBER(VALUE(MID(Q2,18,2))), MID(Q2,20,1)=".",
  ISNUMBER(VALUE(MID(Q2,21,3))), RIGHT(Q2,1)="Z"),
  "Valid", "Invalid"))
```

Validación del formato de correo electrónico

Validate Email Format (Column E)

```
=IF(TRIM(E2)="", "", IF(AND(
  ISNUMBER(FIND("@", E2)),
  ISNUMBER(FIND(".", E2)),
  FIND("@", E2) > 1,
  FIND(".", E2, FIND("@", E2)) > FIND("@", E2) + 1,
  LEN(E2) - LEN(SUBSTITUTE(E2, "@", "")) = 1,
  ISERROR(FIND(" ", E2))
), "Valid", "Invalid"))
```

¿Aparecen errores?

- ¿Descargó la plantilla correcta y no agregó columnas adicionales?
- ¿Se han completado todos los campos obligatorios para los usuarios que recibirán una credencial móvil?
- ¿La dirección de correo electrónico y el número de teléfono son únicos tanto en el archivo como entre los usuarios existentes?
- ¿Los formatos de fecha y de correo electrónico son correctos según lo indicado arriba?

Información

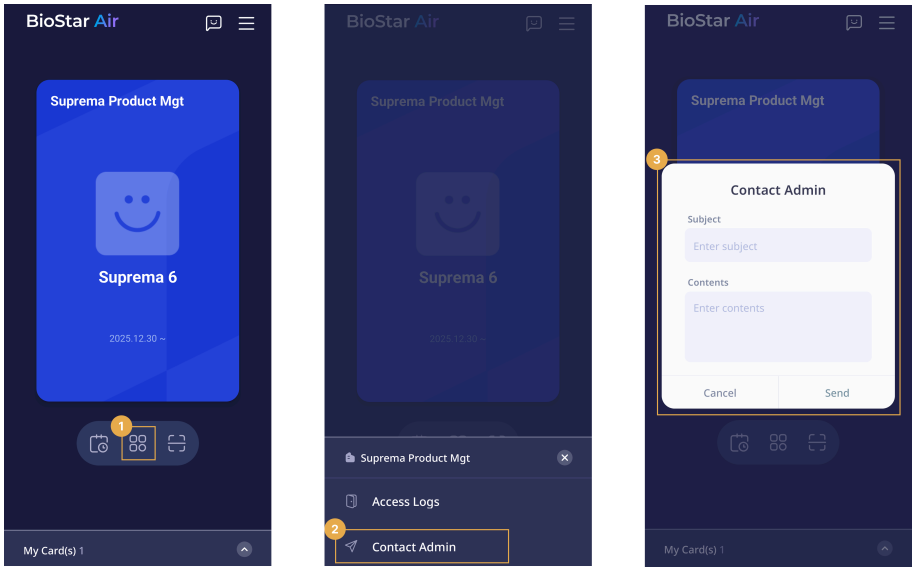
- El equipo de soporte no ofrece edición de archivos. Si el archivo no se sube, utilice las herramientas de validación anteriores para identificar y resolver el problema.
- Este documento está diseñado para permitir cargas exitosas sin intervención manual por parte del equipo de soporte.

Solucionar problemas con la tarjeta móvil

Si la tarjeta móvil se autentica con el dispositivo pero la puerta no se abre, siga estos pasos para resolver el problema.

Contacte al administrador de BioStar Air

El administrador del sitio puede ayudar con la reemisión de tarjetas móviles, problemas temporales del dispositivo móvil y problemas de configuración.



1. En la app Suprema Pass en su dispositivo móvil, toque el icono debajo de la tarjeta móvil.
2. Cuando aparezca el panel inferior, toque **Contactar al administrador**.
3. Cuando aparezca la ventana emergente, ingrese un título y un mensaje.
4. Toque **Enviar** para enviar un mensaje al administrador.

¿Se eliminó la tarjeta móvil?

Si cambió su dispositivo móvil o reinstaló la app Suprema Pass, todas las tarjetas móviles se eliminaron por motivos de seguridad. Comuníquese con los siguientes contactos para solicitar la reemisión de las tarjetas móviles.

- **Company Spaces**: Recursos Humanos, TI, seguridad u operaciones
- **Shared Spaces**: administrador regional o equipo de servicio al cliente

> **Información**
> Cuando un administrador reemite las credenciales de un usuario en BioStar Air, las credenciales móviles previamente emitidas y los códigos QR y LinkPasses son revocados y reemplazados. El usuario recibirá un correo electrónico o SMS, dependiendo de la configuración del sitio, que contenga un enlace a las credenciales actualizadas. El usuario debe seguir el enlace para descargar la nueva credencial móvil en la aplicación Suprema Pass o acceder al nuevo código QR o LinkPass. Los intentos de acceso usando credenciales móviles revocadas, códigos QR o LinkPasses fallarán.

Guía de solución de problemas paso a paso

1 ¿Apareció un mensaje de error en la app Suprema Pass?

- Si la puerta no se abre, intente autenticarse nuevamente en la app Suprema Pass.
- Si aparece un mensaje de error, haga una captura de pantalla y compártala con el administrador del sitio.

2 ¿Está activado el Bluetooth en su dispositivo móvil?

La tarjeta móvil depende de la comunicación por Bluetooth entre el dispositivo móvil y el controlador de acceso.

- Asegúrese de que el Bluetooth esté activado.
- Apague y vuelva a encender el Bluetooth.
- Reinicie el dispositivo móvil si es necesario.

3 Conceder permiso de ubicación a la app Suprema Pass

La autenticación por Bluetooth y por NFC requiere permiso de ubicación.

1. Vaya a **Configuración** → **Aplicaciones** en el dispositivo móvil.
2. Seleccione la aplicación **Suprema Pass**.
3. En **Permisos** → **Ubicación**, configure el acceso a la ubicación en **Permitir siempre** o **Permitir solo mientras se usa la aplicación**.

4 Verifique las conexiones de red celular y Wi-Fi

Se requiere una conexión estable de red celular o Wi-Fi para la autenticación con tarjeta móvil.

5 ¿Está usando el método de conexión seleccionado?

Verifique el método de conexión en la aplicación Suprema Pass.

- En la pantalla principal de la aplicación Suprema Pass, toque ☰ en la esquina superior derecha.
- Verifique el modo de autenticación en **Método de conexión**.
- Mantenga la aplicación abierta en segundo plano al usar **Modo en segundo plano**.

6 ¿El dispositivo móvil vibró durante la autenticación?

- Si el dispositivo móvil vibró pero la puerta no se abrió, abra la aplicación Suprema Pass e intente autenticarse de nuevo.
- Si aparece un mensaje de error, haga una captura de pantalla y compártala con el administrador del sitio.

¿Por qué se me solicita activar los servicios de ubicación?

En Suprema Pass, los servicios de ubicación son necesarios para autenticarse con la tarjeta de acceso móvil. Esto garantiza una comunicación segura por Bluetooth entre el dispositivo móvil y el equipo de control de acceso.

Q. ¿Necesito cambiar de Airfob Space a BioStar Air?

No. Si ya eres cliente de Airfob Space, puedes seguir usando la plataforma tal y como está. No hay una migración forzada por el momento.

Q. ¿Se verán afectados mis dispositivos o mis datos?

No. Ambas plataformas comparten el mismo backend. Los dispositivos, los datos de los usuarios y las configuraciones siguen siendo completamente compatibles en ambos servicios.

Q. ¿Debería empezar a usar Suprema Pass en lugar de la app de Airfob Space?

No es necesario migrar a los usuarios que ya tienen credenciales móviles a BioStar Air. Si usas la URL app.airfobspace.com o la app Airfob Pro para administrar usuarios y emitir credenciales móviles, esos usuarios recibirán una invitación que apunta a la app Airfob Space. Si usas admin.biostarair.com o la app BioStar Air para administrar usuarios y emitir credenciales móviles, esos usuarios recibirán una invitación que apunta a la app Suprema Pass.

Q. ¿Cambiarán el soporte o la facturación?

No habrá cambios inmediatos en tus procesos de soporte o facturación. Sin embargo, con el tiempo, BioStar Air se convertirá en la marca principal para la documentación, el soporte y los anuncios de nuevas funciones.

Q. ¿Puedo cambiar a BioStar Air si quiero?

Sí. Dado que comparten el backend, la transición es sencilla, aunque podrían existir diferencias en la imagen de marca y en la disponibilidad de funciones. Simplemente comienza a usar admin.biostarair.com y la app BioStar Air para administrar tu sitio. Las credenciales de administrador existentes de app.airfobspace.com funcionarán sin inconvenientes.

Q. ¿Cuáles son los beneficios de BioStar Air?

BioStar Air es la marca orientada al futuro. Recibirá mejoras continuas, como integraciones mejoradas, actualizaciones de la interfaz y nuevas funciones que quizá no se incorporen a Airfob Space.

Q. ¿Las futuras funciones serán compatibles con Airfob Space?

Algunas sí funcionarán, pero no todas. Es posible que las nuevas funciones sean exclusivas de BioStar Air. Para una experiencia y soporte óptimos, las nuevas implementaciones deberían usar BioStar Air.

Solución de problemas de reproducción de video

Siga estos pasos para diagnosticar y resolver el problema cuando el video grabado no se reproduce tras registrar una cámara en BioStar Air. Estos pasos solucionan problemas de reproducción de video y garantizan el correcto funcionamiento en BioStar Air.

Información

Para obtener más información sobre el registro de cámaras, consulte Soporte y configuración de cámaras IP.

Q. ¿Necesito cambiar de Airfob Space a BioStar Air?

No. Si ya eres cliente de Airfob Space, puedes seguir usando la plataforma tal y como está. No hay una migración forzada por el momento.

Q. ¿Se verán afectados mis dispositivos o mis datos?

No. Ambas plataformas comparten el mismo backend. Los dispositivos, los datos de los usuarios y las configuraciones siguen siendo completamente compatibles en ambos servicios.

Q. ¿Debería empezar a usar Suprema Pass en lugar de la app de Airfob Space?

No es necesario migrar a los usuarios que ya tienen credenciales móviles a BioStar Air. Si usas la URL app.airfobspace.com o la app Airfob Pro para administrar usuarios y emitir credenciales móviles, esos usuarios recibirán una invitación que apunta a la app Airfob Space. Si usas admin.biostarair.com o la app BioStar Air para administrar usuarios y emitir credenciales móviles, esos usuarios recibirán una invitación que apunta a la app Suprema Pass.

Q. ¿Cambiarán el soporte o la facturación?

No habrá cambios inmediatos en tus procesos de soporte o facturación. Sin embargo, con el tiempo, BioStar Air se convertirá en la marca principal para la documentación, el soporte y los anuncios de nuevas funciones.

Q. ¿Puedo cambiar a BioStar Air si quiero?

Sí. Dado que comparten el backend, la transición es sencilla, aunque podrían existir diferencias en la imagen de marca y en la disponibilidad de funciones. Simplemente comienza a usar admin.biostarair.com y la app BioStar Air para administrar tu sitio. Las credenciales de administrador existentes de app.airfobspace.com funcionarán sin inconvenientes.

Q. ¿Cuáles son los beneficios de BioStar Air?

BioStar Air es la marca orientada al futuro. Recibirá mejoras continuas, como integraciones mejoradas, actualizaciones de la interfaz y nuevas funciones que quizá no se incorporen a Airfob Space.

Q. ¿Las futuras funciones serán compatibles con Airfob Space?

Algunas sí funcionarán, pero no todas. Es posible que las nuevas funciones sean exclusivas de BioStar Air. Para una

experiencia y soporte óptimos, las nuevas implementaciones deberían usar BioStar Air.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

Para obtener más información sobre las sucursales globales de Suprema,
visite la página web a continuación escaneando el código QR.
http://www.supremainc.com/en/about/contact-us.asp

© 2026 Suprema Inc. Suprema y los números y los nombres que identifican productos mencionados en este documento son marcas comerciales registradas de Suprema, Inc. Todas las marcas y los nombres de productos que no pertenecen a Suprema son marcas comerciales o marcas comerciales registradas de sus respectivas compañías. La apariencia del producto, el estado de la estructura o las especificaciones están sujetas a cambio sin previo aviso.