BioStar X

GUÍA DEL ADMINISTRADOR DE

Versión 1.0.3

Español

ES 102.00.BSX

suprema
SECURITY & BIOMETRICS

CONTENIDO

Resúmen 6

Mayor eficiencia operativa y seguridad 6

Ofrece gran escalabilidad y estabilidad 6

Antes de Comenzar 7

Dispositivos Compatibles 11

Requisitos Mínimos del Sistema 13

Primeros Pasos 17

Verificar la Prioridad de Red 17

Instalación Exprés 24

Instalación Personalizada 31

Actualizar 39

Instalar el Servidor de Comunicaciones Múltiples 47

Cómo Iniciar Sesión 54

Registrar Clave de Licencia 56

Guía de Configuración Inicial 59

Administración de Servidores 61

Iniciar y Detener el Servidor 61

Configuración del Servicio 62

Cambiar la dirección IP del servidor principal 65

Cambiar el Puerto 68

Cambiar la Base de Datos 69

Agregar Base de Datos Auxiliar 71

Desinstalar El Servidor BioStar X Y Restaurar Certificados De Seguridad 79

Lanzador 86

Usuario 87

Administrar Grupos de Usuarios 87

Registrar usuarios 91

Ingresar Información Básica del Usuario 93

Registrar Credencial del Usuario 95

Configurar Permisos de Usuario 119

Configura los Ajustes Avanzados del Usuario 123

Inscribir Y Editar Usuarios Al Escanear Un ID 124

Explorar Usuarios 128

Administrar Usuarios 133

Administrar Grupos de Acceso 143

Iniciar Sesión con Autenticación Multi-Factor 145

Inscribir Rostros por Lotes 148

Migracion Visual Face 152

Configurar Permisos de Apertura de Emergencia 155

Monitorizar 157

Monitorear Puertas 157

Monitorear Mapa 185

Monitorear Dispositivo 194

Supervisar Video 202

Supervisar Evento 209

Fecha 218

Generar Reporte 218

Programación Automática de Reportes 233

Ajustes 235

Tablero 237

Agregar Widgets 237

Editar Widget 243

Eliminar Widget 244

Ajustes 245

Administrar Dispositivos 245

Configuración del Dispositivo 269

Configuración de Registros de Imágenes 308

Configuración del Agente USB 312

Configuración de Administración de Conexión de Dispositivos 314

Administrar Puertas 317

Gestionar Permisos de Operación 330

Administrar Usuarios Inactivos A Largo Plazo 336

Configurar Escaneo De ID 341

Configuración de Control de Acceso 341

Ajustes de Horario 351

Configuración de Activadores y Acciones 354

Cómo Usar la Acción Rápida 356

Importar Registros de Eventos 360

Configuración de Alertas 361

Administrar Credenciales 363

Activar Licencia 386

Gestionar Registro De Auditoría 392

Configuración del Sistema 402

Configuración Avanzada 434

Administrar Ascensores 434

Configuración Avanzada de Control de Acceso 441

Configuración de Video 472

Administrar Mapa 495

Configurar Visitante 511

Configuración de Integración de Directorios 515

Configuración de Acceso Remoto 527

Integrar el Registro de Eventos de Dispositivos Virtuales 530

Conector 536

¿Qué son los conectores? 536

Conectores de BioStar X 536

Casos de uso clave 536

Registrar el plugin 536

Administración de conector 538

Cómo Usar Tiempo y Asistencia 539

Administrar Visitantes 586

Explorar la Interfaz 601

Aprender la Interfaz de Usuario Común 601

Usuario 602

Monitorizar 603

Tablero 604

Ajustes 604

Política de Licencias 606

licencia básica 606

Ampliación de capacidad 607

Complementos de funciones 608

Control de acceso avanzado 609

Licencia de dispositivo 390

Apéndices 611

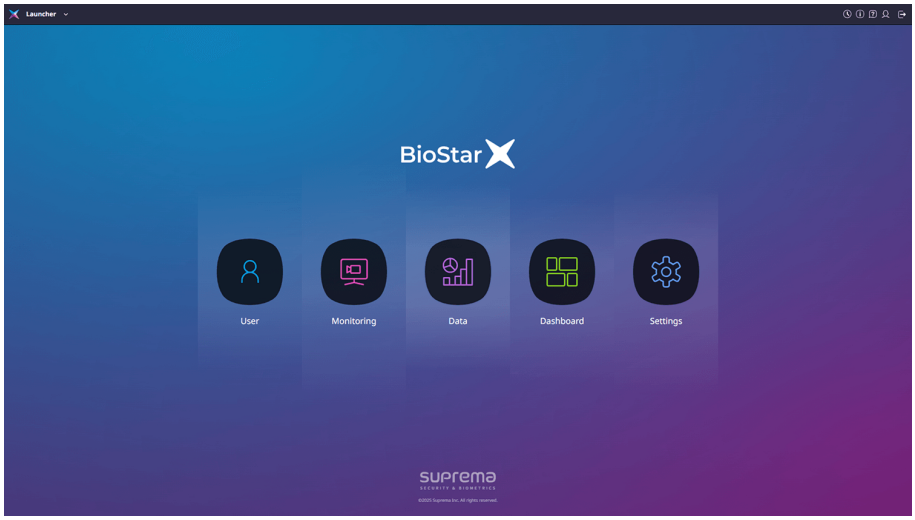
Descargos de responsabilidad 611

Aviso de derechos de autor 612

Licencia de código abierto 612

Resúmen

BioStar X es la plataforma de seguridad integrada de próxima generación de Suprema que combina el control de acceso basado en IA con el análisis de video inteligente. Una plataforma innovadora que puede integrar y gestionar de manera eficaz las operaciones de seguridad generales, más allá del simple control de acceso.



BioStar X, la culminación del control de acceso basado en IA y el análisis de video inteligente, está diseñada para utilizar la tecnología de IA para realizar la gestión de acceso en tiempo real, el monitoreo de video y la detección de comportamientos anómalos en una sola plataforma. Además del control de acceso, está equipada con varias funciones de análisis de video basadas en IA, como la detección de intrusiones, la detección de merodeo y la detección de caídas, lo que permite respuestas proactivas.

Asimismo, admite un monitoreo de seguridad más sofisticado en instalaciones grandes mediante funciones de conteo de personas, detección de tailgating, detección de listas negras y búsqueda de personas desaparecidas. Esta funcionalidad puede utilizarse eficazmente no solo en instalaciones de uso múltiple como escuelas, centros comerciales, aeropuertos y hospitales, sino también en edificios inteligentes.

Mayor eficiencia operativa y seguridad

BioStar X permite la gestión integrada de todos los elementos de seguridad en tiempo real desde una sola plataforma. Esto permite al personal de seguridad supervisar y controlar de manera eficiente los sistemas individuales desde una sola interfaz sin necesidad de gestionarlos por separado.

Además, el método de operación integrada optimiza al personal de monitoreo de seguridad y reduce los costos y el tiempo dedicados al mantenimiento. Sin necesidad de agregar un sistema de seguridad individual aparte, aprovechar la escalabilidad flexible de **BioStar X** le permite añadir fácilmente las funcionalidades necesarias, creando así un entorno de seguridad más seguro y eficiente.

Ofrece gran escalabilidad y estabilidad

En entornos empresariales, como grandes corporaciones o instituciones públicas, la escalabilidad y la estabilidad de los sistemas de seguridad son esenciales. **BioStar X** admite el registro de decenas de miles de usuarios y permite un funcionamiento estable incluso al conectar diversos dispositivos.

Además, facilita la gestión intuitiva de operaciones de seguridad complejas al proporcionar una UI·UX personalizada para los usuarios. Es posible configurar directamente el diseño de la interfaz de la pantalla de monitoreo, lo que permite comprobar de forma rápida y eficaz la información necesaria.

Solución de seguridad esencial BioStar X

Con la creciente variedad de amenazas de seguridad y la mayor complejidad de las operaciones de seguridad, **BioStar X**, que combina IA con tecnología de seguridad integrada, se está consolidando como una solución de seguridad esencial. Si su organización requiere tanto una seguridad sólida como operaciones eficientes, **BioStar X** es la opción óptima.

Antes de Comenzar

> **Consejo**
> Esta guía proporciona información importante que debe conocer antes de iniciar **BioStar X**. **BioStar X** es compatible con sistemas operativos de 64 bits. Verifique los requisitos del sistema de la PC donde desea instalar **BioStar X** y luego instálelo.

Notas previas a la instalación

Antes de instalar **BioStar X**, verifique lo siguiente y continúe con la instalación.

- **BioStar X** solo se puede instalar en un sistema operativo de 64 bits.
- Si está utilizando MS SQL 2012 Express, consulte el siguiente enlace para instalar el Service Pack 3.
- Si está utilizando MS SQL 2014 Express, consulte el siguiente enlace para instalar el Service Pack 2.
- Si está utilizando MS SQL Server, configure la opción `Collation` del servidor y de cada tabla en CI (sin distinción de mayúsculas).
- Al hacer una copia de seguridad de una base de datos de una versión anterior de **BioStar X**, desactive todos los servicios antes de continuar. Además, si no respalda y restaura juntas las bases de datos AC y TA, no podrá utilizar la base de datos TA.
- Si desea respaldar la base de datos de **BioStar X**, asegúrese de respaldar también el *enckey* en la carpeta *\Program Files\BioStar X\util* y los archivos *system.conf* y *setting.conf* en la carpeta *\Program Files\BioStar X*. De lo contrario, la base de datos no estará disponible.
- Para ver el puerto predeterminado que usa **BioStar X**, consulte Configuración del Servicio. Si otro programa ocupa el mismo puerto, **BioStar X** podría no funcionar correctamente.

Verificar la base de datos

Si está utilizando una base de datos configurada por el usuario, verifique los siguientes elementos antes de instalar **BioStar X**.

MariaDB

1. Cambie las siguientes opciones en la sección `[mysql]` del archivo *my.cnf*.

   my.cnf

```
character-set-server=utf8
collation-server=utf8_unicode_ci
max_connections = 600
```

2. Agregue las siguientes opciones en la sección `[mysql]` del archivo *my.cnf*.

   my.cnf

   ```
   log_bin_trust_function_creators = 1
   group_concat_max_len = 102400
   ```

3. Conéctese a MariaDB con privilegios de root y ejecute el siguiente comando.

   SQL

   ```
   GRANT SUPER ON . TO user_id@'localhost' IDENTIFIED BY "password";
   GRANT SUPER ON . TO user_id@'%' IDENTIFIED BY "password";
   ```

MS SQL Server

> **Información**
>
> - Configure las opciones de `Collation` para todas las bases de datos y tablas como insensibles a mayúsculas (CI).
> - Los nombres de base de datos solo pueden contener números, letras en inglés (distinguiendo mayúsculas y minúsculas) y los símbolos especiales `-` `_`.

Ajustes de puertos

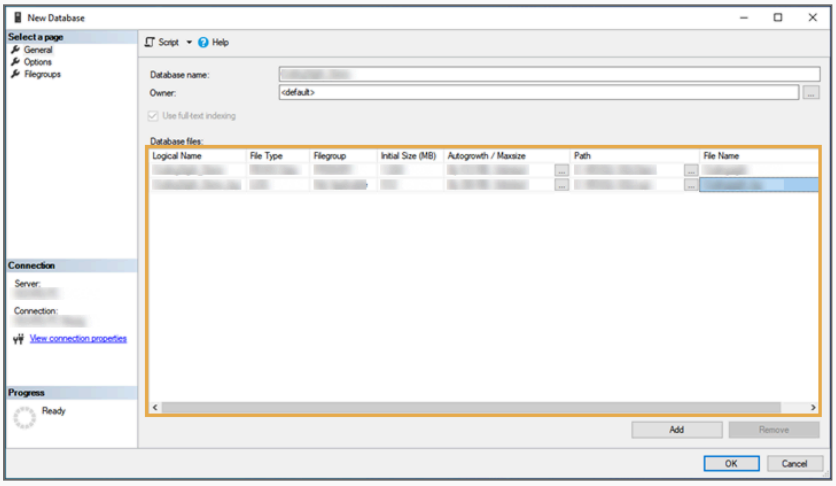
- Ejecute **SQL Server Configuration Manager** y establezca **TCP/IP Protocol** para **Protocols for SQLEXPRESS** en el número de puerto deseado.
- Reinicie los **SQL Server Services** para aplicar los ajustes.

Crear el usuario y la base de datos

1. Inicie sesión con la cuenta **sa** usando **SQL Server Authentication** en **SQL Server Management Studio**.
2. Haga clic derecho en **Security** y haga clic en **New Login**.
3. Ingrese el nombre deseado en el campo **Login Name** y seleccione **SQL Server Authentication**.
4. Ingrese la contraseña deseada en los campos **Password** y **Confirm password**, luego desmarque **Enforce password policy**.
5. Haga clic en **OK** para guardar los ajustes.
6. Haga clic derecho en **Database** y seleccione **New Database**.
7. Ingrese el nombre deseado en el campo Database Name.
8. Ingrese el nombre de inicio de sesión configurado en el paso **3** en el campo **Owner**.

Consejo

Establezca los siguientes valores recomendados en la sección **Database Files**. Configure **Autogrowth** usando tamaños fijos (MB/GB) en lugar de porcentajes y evite incrementos muy pequeños que puedan causar eventos de crecimiento frecuentes.



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

Pequeña (menos de 10 GB)

- Datos: **Initial Size** 1 - 5 GB, **Autogrowth** 100 - 512 MB
- Registro: **Initial Size** 512 MB - 2 GB, **Autogrowth** 100 - 512 MB
- TempDB: **Initial Size** 512 MB - 1 GB

> *p. ej. Datos 2 GB (**Autogrowth** 256 MB) / Registro 1 GB (**Autogrowth** 128 MB) / TempDB 512 MB*

Mediano (10 - 500 GB)

- Datos: **Initial Size** 10 - 50 GB, **Autogrowth** 512 MB - 1 GB
- Registro: **Initial Size** 5 - 10 GB, **Autogrowth** 512 MB - 1 GB
- TempDB: **Initial Size** 2 - 8 GB

> *p. ej. Datos 20 GB (**Autogrowth** 1 GB) / Registro 5 GB (**Autogrowth** 512 MB) / TempDB 4 GB*

Empresa (500 GB o más)

- Datos: **Initial Size** 100 GB o más, **Autogrowth** 1 - 4 GB
- Registro: **Initial Size** 20 ~ 100 GB, **Autogrowth** 1 ~ 4 GB
- TempDB: **Initial Size** 8 - 32 GB

> *p. ej. Datos 100 GB (**Autogrowth** 2 GB) / Registro 50 GB (**Autogrowth** 2 GB) / TempDB 16 GB*

Precaución

- No configure **Autogrowth** con incrementos muy pequeños ni deje **Maxsize** en **Unlimited**. En su lugar, establezca límites apropiados según el crecimiento esperado y supervise el uso.
- En entornos con muchas transacciones, respalde los registros periódicamente para evitar que el tamaño de los archivos de registro aumente.

Configurar la base de datos de autenticación de Windows

1 Ajustes previos

Si utiliza **Microsoft Windows Active Directory**, complete las configuraciones previas que se indican a continuación antes de configurar la base de datos de autenticación de Windows.

1. Inicie sesión con una cuenta de administrador en **SQL Server Management Studio**.
2. Haga clic derecho en **Security** y haga clic en **New Login**.
3. Seleccione **Windows Authentication** y luego haga clic en **Search**.
4. En la ventana **Select a user or group**, haga clic en Ubicación, seleccione la ruta de Active Directory y haga clic en **OK**.
5. Ingrese el nombre de usuario en el campo **Enter object name to select**, luego haga clic en **Check Names** > **OK**.
6. Haga clic en **Server Roles** en **Select a page**.
7. Seleccione **sysadmin** y luego haga clic en **OK**.
8. Haz clic en **User Mapping** en la página **Select**.
9. Selecciona **ac**, **master**, **ta**, **ve** y establece **Default Schema** en **dbo**.
10. Haga clic en **OK** para guardar los ajustes.

2 Configurar la autenticación de Windows de MS SQL con una cuenta de Active Directory

1. Ejecuta *services.msc*.
2. En la ventana **Properties** > **Logon** de la base de datos de SQL Server, selecciona **Specify account** e inicia sesión como usuario de dominio.
3. Agrega el puerto 1433 como excepción en el Firewall de Windows.
4. Crea las bases de datos vacías **ac**, **ta**, **ve** en SQL Server con autenticación **sysadmin**.
5. Configura al usuario de dominio para que use la autenticación de Windows en SQL Server y asigna todos los permisos excepto **sysadmin** a las bases de datos **ac**, **ta**, **ve**.
6. Conecta todos los servicios, excepto el equipo local, en *services.msc*.
7. Establece al usuario de dominio como administrador en el equipo de servicio local.
8. Conéctate a MS SQL ODBC.

3 Ajustes de la base de datos

1. Después de ejecutar **SQL Server Configuration Manager**, haz clic en **Client Protocol** en **SQL Native Client**.
2. Selecciona **TCP/IP** y verifica el puerto predeterminado.

3. Haz clic en **Protocols for SQL EXPRESS** en **SQL Server Network Configuration**.
4. Comprueba que el puerto ODBC en **TCP/IP** esté configurado con el mismo valor que el puerto predeterminado.
5. Inicie sesión con una cuenta de administrador en **SQL Server Management Studio**.
6. Haz clic en **Security** > **Log In**, luego haz doble clic en **NT AUTHORITY\SYSTEM**.
7. Haga clic en **Server Roles** en **Select a page**.
8. Selecciona **public** y **sysadmin**, luego haz clic en **OK**.
9. Haz clic en **User Mapping** en la página **Select**.
10. Selecciona las bases de datos **ac**, **ta**, **ve** y haz clic en **OK** para guardar.

Siguiente paso

Conoce los requisitos mínimos del sistema para instalar **BioStar X**.
Esta guía proporciona un método de instalación sencillo para usuarios primerizos.
Guía al usuario para configurar una instalación personalizada que se integre con una base de datos que ya haya instalado.

Dispositivos Compatibles

Los siguientes dispositivos son compatibles con la plataforma BioStar X.



BioStation 3 Max



XPass Q2



BioEntry W3



BioStation 2a



BioStation 3



X-Station 2



FaceStation F2



XPass 2



FaceLite



BioLite N2



XPass D2



BioEntry R2



BioEntry P2



FaceStation 2



BioEntry W2



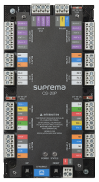
BioStation L2



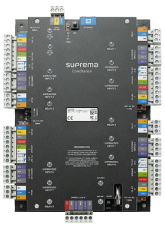
BioStation A2



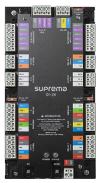
BioStation 2



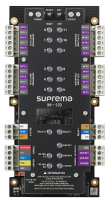
CoreStation 20



CoreStation



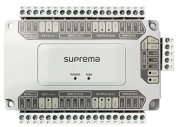
Door Interface



Input Module



Output Module



Door Module



Secure I/O 2

Requisitos Mínimos del Sistema

BioStar X ofrece una solución confiable y escalable de gestión de seguridad integrada para entornos empresariales grandes. El sistema puede gestionar eficientemente más de mil dispositivos mediante una arquitectura distribuida compuesta por un servidor principal y un Servidor de comunicaciones múltiples.

El servidor principal gestiona las funciones principales de administración del sistema. El servidor de comunicaciones múltiples gestiona la comunicación con los dispositivos, distribuye la carga y optimiza el rendimiento. Además, los administradores pueden acceder al sistema a través de un navegador web en los equipos cliente y realizar todas las tareas de gestión. Consulta los siguientes requisitos del sistema para configurar el entorno óptimo según el tamaño de tu organización.

> **Información**
> Para obtener más información sobre la configuración y optimización de licencias, comunícate con el Equipo de Soporte Técnico global de Suprema.

Servidor principal

El servidor principal es el servidor donde se instala el sistema de gestión central de **BioStar X**. El usuario accede al sistema mediante un navegador web para gestionarlo y realizar todas las tareas, como configurar la información de usuarios o los permisos de acceso. También se encarga de supervisar el estado general del sistema y de gestionar los registros de eventos o las alarmas.

Ítem		Pequeña	Medio	Corporativa
Entorno de uso	Total Dispositivos	1 a 50	51 a 100	101 a 1,000
Requisito del sistema	Sistema operativo	Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025		
	Base de datos	MariaDB 11.4.4, MS SQL Server 2012 SP3, MS SQL Server 2014 SP2, MS SQL Server 2016 SP1, MS SQL Server 2017, MS SQL Server 2019, MS SQL Server 2022		
	CPU	2.3 GHz de 6 núcleos	2.3 GHz de 8 núcleos	Mínimo 2.3 GHz Recomendado 4.0 GHz de 16 núcleos
	RAM	16 GB	32 GB	Mínimo 64 GB Recomendado 128 GB

Ítem		Pequeña	Medio	Corporativa
	SSD	512 GB	512 GB	1 TB
	HDD	Al utilizar la función **Image Log**, se requieren 200 GB para 10 millones de registros de imágenes.		

Información

- **BioStar X** solo se puede instalar en sistemas operativos de 64 bits.
- La seguridad de comunicación de MS SQL Server admite TLS 1.2.
- Si MS SQL Server y **BioStar X** se instalan en diferentes equipos, instala el Controlador Microsoft OLE DB para SQL Server en el equipo donde esté instalado **BioStar X**.
- Para entornos empresariales, se recomienda instalar una base de datos MS SQL Server.
- Si utilizas una base de datos MS SQL Server y **BioStar X T&A**, deberás instalar el Controlador Microsoft ODBC 17 para SQL Server correspondiente a tu entorno.
- El entorno virtual de Windows proporcionado por Boot Camp en macOS no es compatible.
- Hasta 1,000 dispositivos pueden conectarse a través de Ethernet (TCP/IP). Agrega un servidor de comunicaciones múltiples para conectar más dispositivos.

Requisitos de licencias de SQL Server

Si utilizas SQL Server como base de datos, se requiere una licencia adecuada de SQL Server según la cantidad de dispositivos conectados para el funcionamiento estable de **BioStar X**. Consulta las configuraciones de licencias recomendadas para cada entorno y selecciona la licencia adecuada al tamaño y las necesidades de tu organización.

Información

Para obtener más información sobre las licencias de SQL Server, consulta Microsoft SQL Server Licensing.

Uso general

Organización	Total Dispositivos	Cantidad de núcleos
Pequeña	1 a 50	4 - 6
Medio	50 - 300 dispositivos	8 - 12
Corporativa	300 - 1,000 dispositivos	16 - 24

Uso de la API de BioStar X

Organización	Total Dispositivos	Cantidad de núcleos
Pequeña	1 a 50	4 - 6
Medio	50 - 300 dispositivos	8 - 12
Corporativa	300 - 1,000 dispositivos	16 - 24

Servidor de Multi Comunicaciones

El servidor de comunicaciones múltiples gestiona la comunicación con dispositivos de control de acceso. Al instalarlo por separado del servidor principal, ayuda a gestionar muchos dispositivos de forma confiable. Un solo servidor de comunicaciones múltiples puede conectar hasta 1,000 dispositivos. Agregue varios servidores de comunicaciones múltiples según sea necesario.

Ítem		Especificación
Requisito del sistema	Sistema operativo	Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025
	CPU	Mínimo 2.3 GHz, recomendado 4.0 GHz de 16 núcleos
	RAM	Mínimo 64 GB, recomendado 128 GB
	SSD	1 TB

Información
Hasta 1,000 dispositivos pueden conectarse a través de Ethernet (TCP/IP).

Cliente

El cliente es el equipo desde el cual los administradores acceden a **BioStar X** a través de un navegador web para operar el sistema.

Ítem		Pequeña	Medio	Corporativa
Requisito del sistema	CPU	2.5 GHz	2.5 GHz	Mínimo 2.5 GHz
	RAM	16 GB	32 GB	Mínimo 32 GB
	GPU	Mínimo NVIDIA GeForce RTX 4060 al usar VMS		
	navegador web	Google Chrome versión 100 o superior		

Información

- **BioStar X** está optimizado para Google Chrome.
- La interfaz web de **BioStar X** no admite navegadores móviles.

Primeros Pasos

Guía de configuración esencial para usuarios primerizos de **BioStar X**. Guía paso a paso de los procedimientos clave necesarios para implementar y operar con éxito **BioStar X**, desde la elección de los métodos de instalación hasta el registro de licencias.

Verificar la Prioridad de Red

Instrucciones para verificar y configurar la prioridad de red del servidor antes de instalar **BioStar X**.

¿Cuándo se necesita?

Debe verificar y configurar la prioridad de red en las siguientes situaciones.

- Cuando el servidor tiene instalados dos o más adaptadores de red (tarjetas LAN)
- Cuando un adaptador de red específico debe utilizarse para el servicio de **BioStar X**
- Para evitar problemas de conexión de red después de instalar **BioStar X**

> **Información**
> Si ninguna de las situaciones anteriores aplica, no es necesario cambiar la prioridad de red. Omita este paso y continúe con la instalación de **BioStar X**. Para obtener más información sobre cómo instalar **BioStar X**, consulte Instalación Exprés.

> **Alerta**
> Durante la instalación de **BioStar X**, se seleccionará automáticamente el adaptador de red con una métrica más baja (mayor prioridad). Como puede ser difícil cambiar esta configuración después de la instalación, asegúrese de verificar y ajustar la prioridad de red antes de la instalación.

Verificar la Prioridad de Red

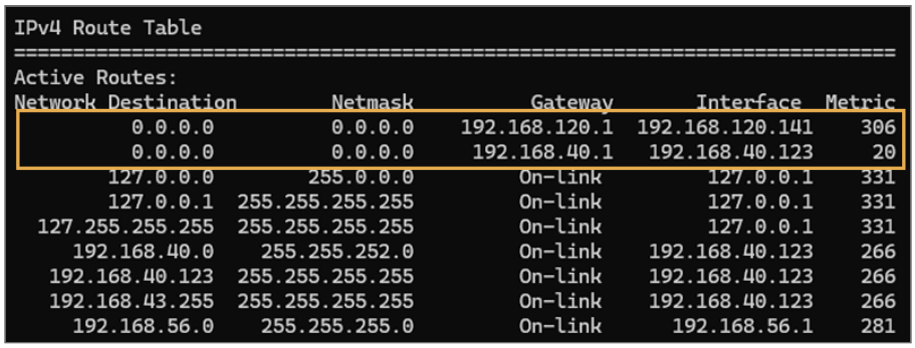
Verificar en el símbolo del sistema

1. Busque `cmd` en el menú **Inicio** y ejecute **Símbolo del sistema**.
2. Ingrese el siguiente comando.

```
route print
```

3. Busque entradas en la sección **IPv4 Route Table** donde **Network Destination** sea `0.0.0.0`.
4. Verifique el valor en la columna **Metric**. Cuanto menor sea el valor, mayor será la prioridad.

Ejemplo de salida:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.120.1  192.168.120.141     306
          0.0.0.0          0.0.0.0     192.168.40.1  192.168.40.123      20
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     331
     192.168.40.0    255.255.252.0         On-link     192.168.40.123     266
   192.168.40.123  255.255.255.255         On-link     192.168.40.123     266
   192.168.43.255  255.255.255.255         On-link     192.168.40.123     266
    192.168.56.0    255.255.255.0         On-link      192.168.56.1     281
```

En el ejemplo anterior, la interfaz `192.168.40.123` tiene un valor de métrica de **20**, lo que resulta en una prioridad más alta.

Verificar la información del adaptador de red

Verifique qué adaptador de red corresponde a cada interfaz.

1. En la ventana del **Símbolo del sistema**, ingrese el siguiente comando.

   ```
   ipconfig /all
   ```

2. Empareje la **dirección IPv4** de cada adaptador de red con la dirección **Gateway** identificada anteriormente para determinar de cuál se trata.

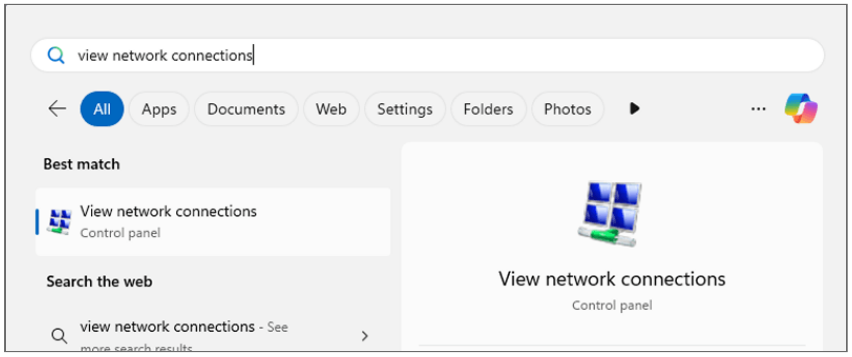
Cambiar la prioridad de red

Para aumentar la prioridad del adaptador de red deseado, siga los pasos a continuación.

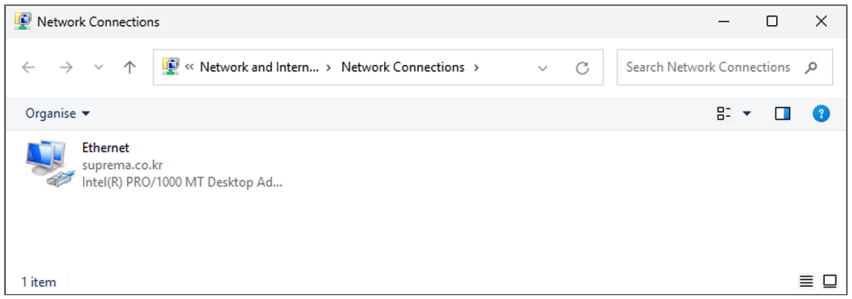
> **Información**
> Los siguientes pasos están basados en Windows 11. La ubicación del menú puede variar según la versión de Windows que esté utilizando.

1 Abrir la configuración de red

1. En el menú **Inicio**, escriba **Ver conexiones de red**.

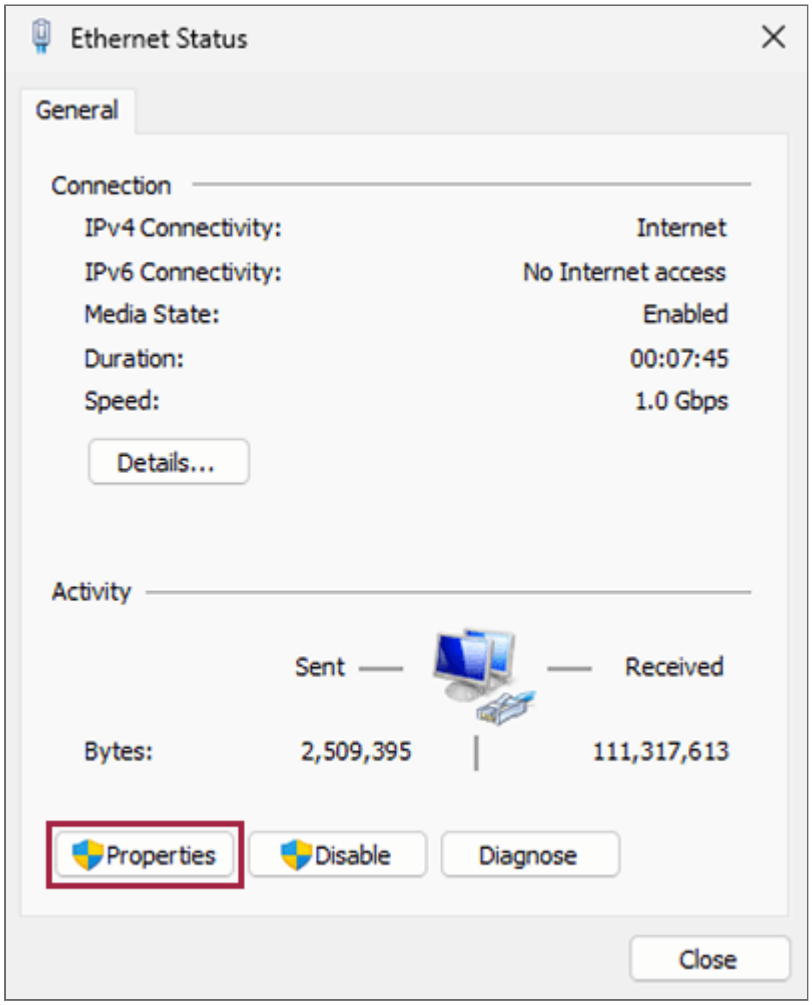


2. Haga clic en **Ver conexiones de red** en los resultados de la búsqueda.
3. Haga doble clic en el adaptador conectado a Internet en la lista.

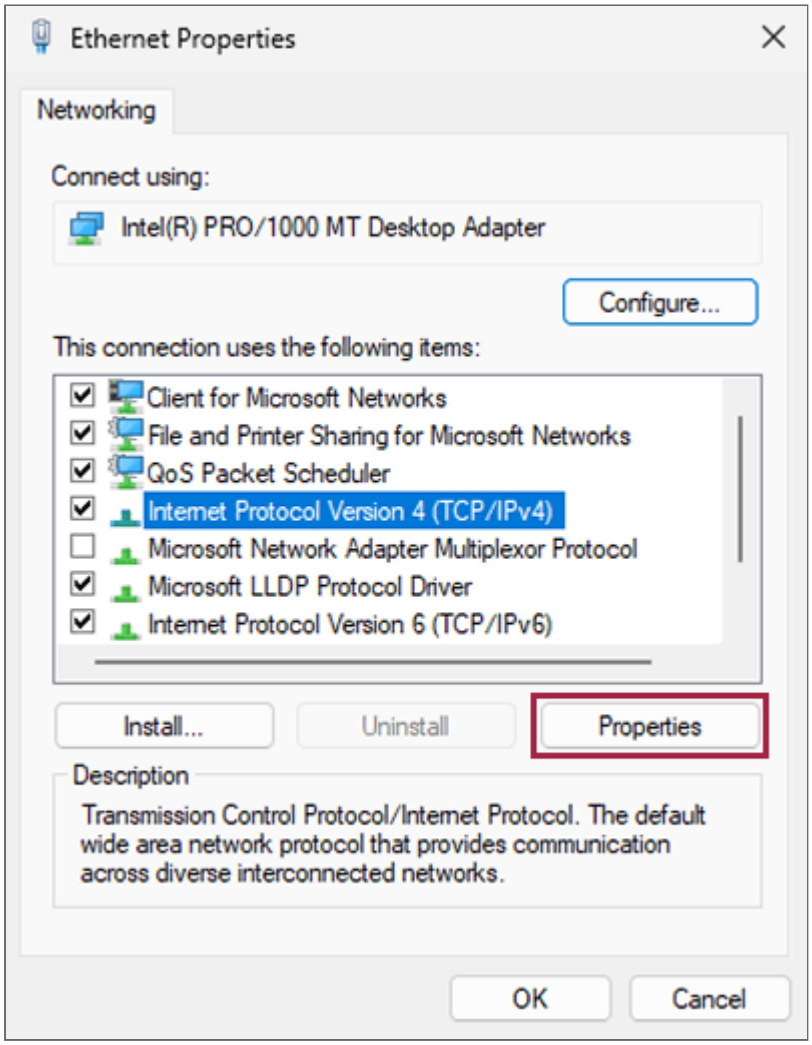


2 Abrir las opciones del adaptador

1. Cuando aparezca la ventana **Estado de Ethernet**, haga clic en el botón **Propiedades**.

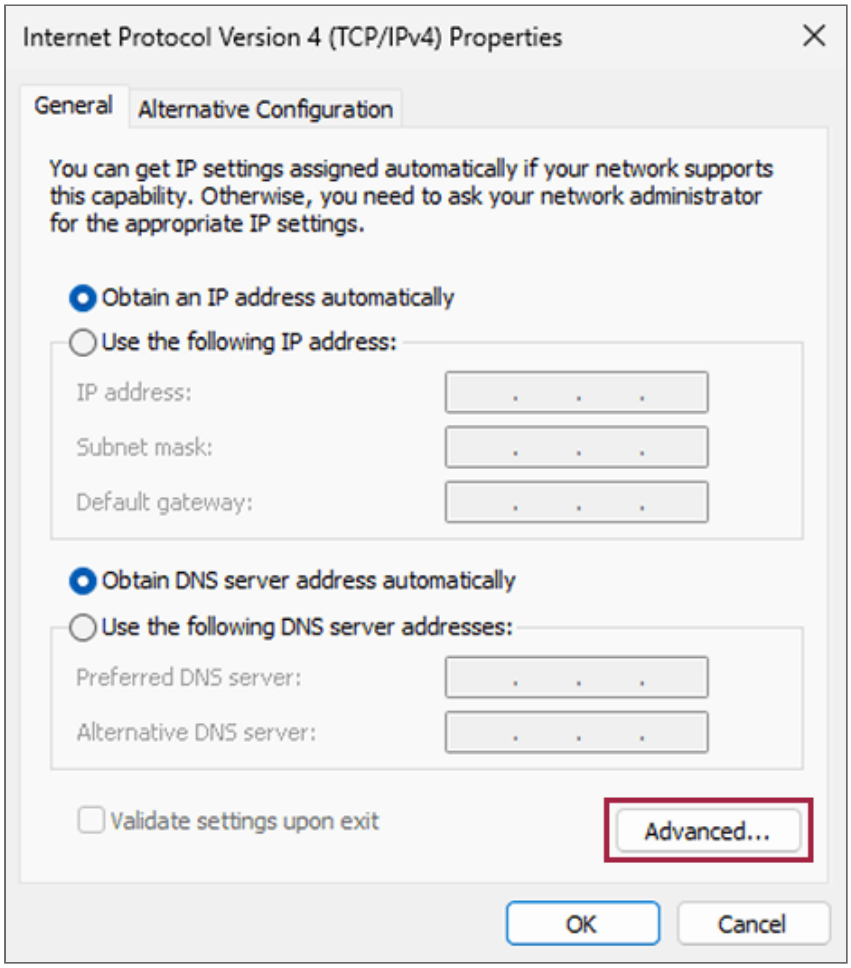


2. Cuando aparezca la ventana Propiedades de Ethernet, seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** en la lista.



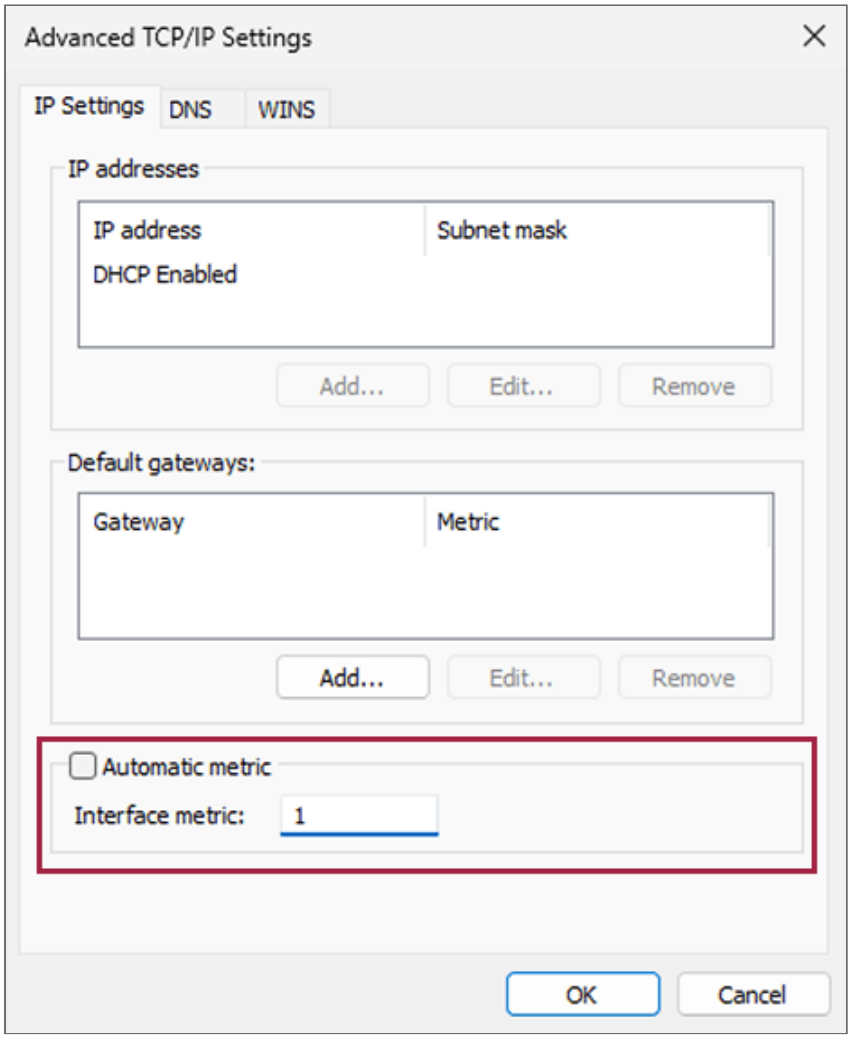
3. Haga clic en el botón **Propiedades**.

4. Cuando aparezca la ventana **Propiedades de Protocolo de Internet versión 4 (TCP/IPv4)**, haga clic en el botón **Avanzado**.



3 Configuración de métrica

1. Desmarque la casilla **Automatic Metric**.



2. Ingrese el valor deseado en el campo **Interface Metric**.
   - Si desea la prioridad más alta, ingrese `1`.
   - Si desea una prioridad mayor que la de otros adaptadores, ingrese un número menor que los valores de métrica de los demás adaptadores.
3. Para guardar la configuración y cerrar todas las ventanas, haga clic en el botón **OK**.

> **Información**
> Los valores que puede ingresar en **Interface Metric** van de `1` a `9999`. Cuanto menor sea el valor, mayor será la prioridad.

4 Verificar la configuración

1. Vuelva a abrir el **Símbolo del sistema** y ejecute el comando `route print`.
2. Verifique si el valor de la métrica ha cambiado.

Solución de Problemas

- Si la configuración no se aplica, reinicie el equipo o deshabilite y vuelva a habilitar el adaptador de red.

- Si se pierde la conexión de red, vuelva a la configuración original y habilite de nuevo la opción **Automatic Metric**. Comuníquese con su administrador de red para verificar la configuración correcta.

> **Información**
> Si necesita cambiar la configuración de red después de instalar **BioStar X**, se recomienda desinstalar por completo el programa y luego volver a instalarlo.

Siguiente paso

Esta guía proporciona un método de instalación sencillo para usuarios primerizos.
Guía al usuario para configurar una instalación personalizada que se integre con una base de datos que ya haya instalado.

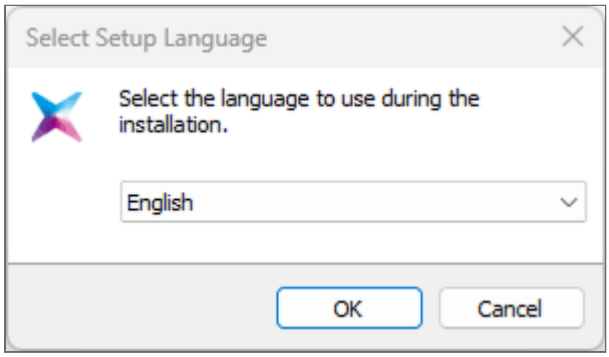
Instalación Exprés

Este procedimiento le guía paso a paso para instalar **BioStar X** con **Instalación exprés**. **Instalación exprés** instala automáticamente el servidor MariaDB integrado y crea la base de datos, lo que permite una instalación rápida sin configuración de base de datos por separado.

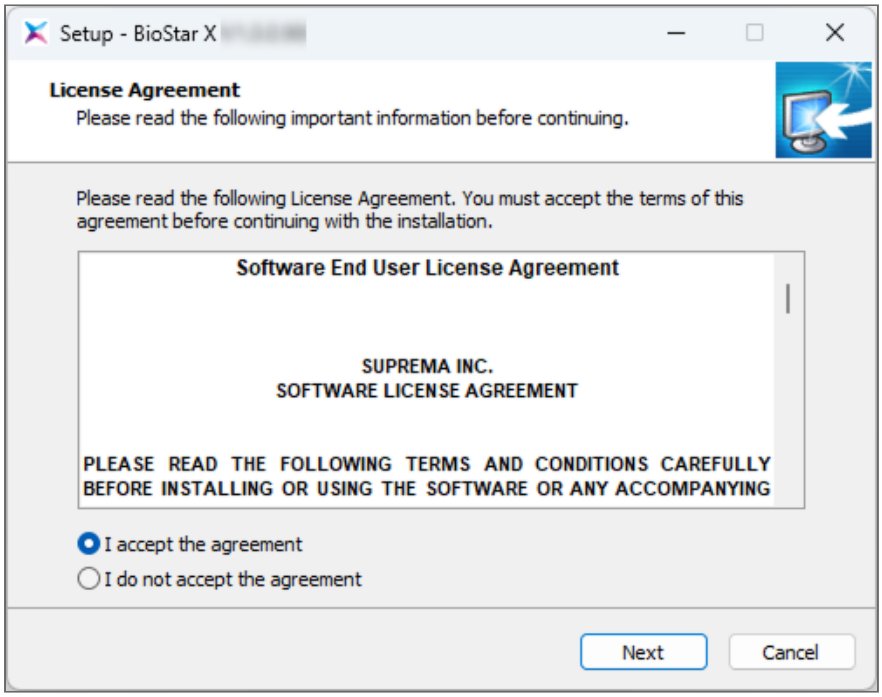
> **Información**
> Para conectarse a una base de datos ya instalada usando **Instalación personalizada**, consulte Instalación Personalizada.

Guía de instalación

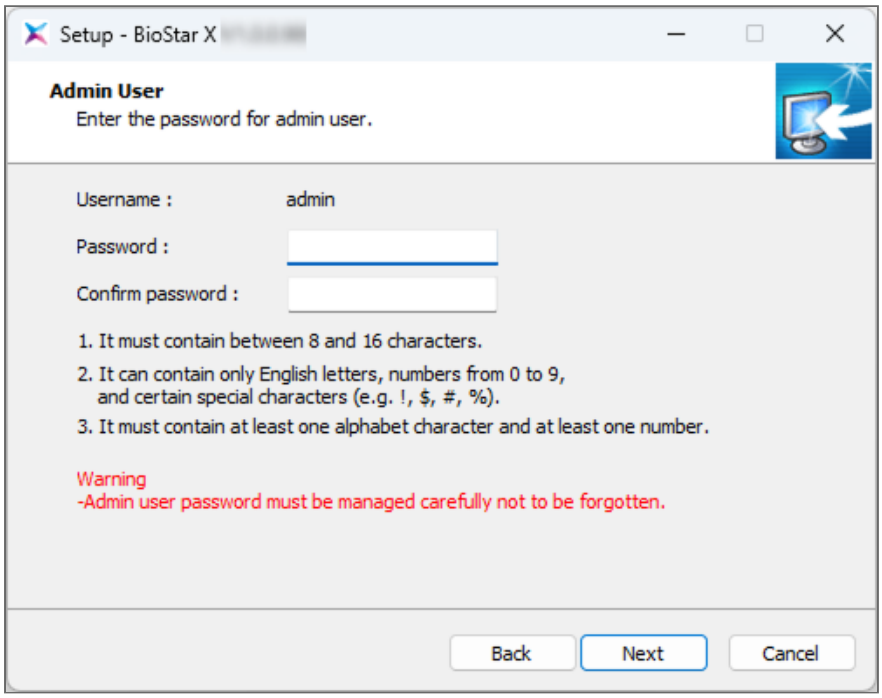
1. Vaya al Suprema Download Center, inicie sesión y descargue el paquete de instalación (*BioStar X Setup.X.Y.Z.BB.exe*).
2. Ejecute el archivo de instalación descargado.
3. Seleccione el idioma a usar y haga clic en el botón **Aceptar**.



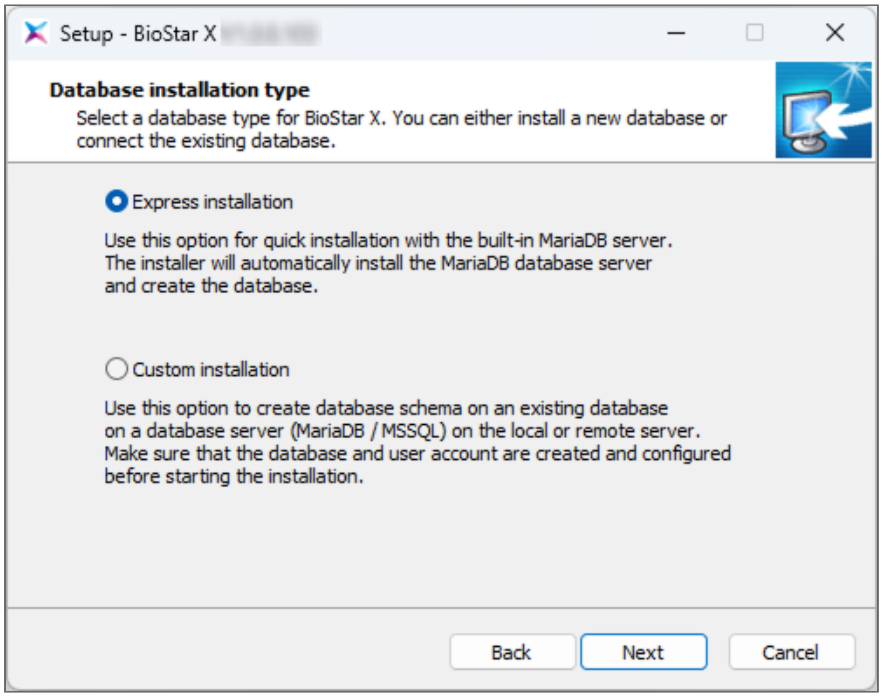
4. Para continuar con la instalación, seleccione **Acepto el acuerdo** y haga clic en el botón **Siguiente**.



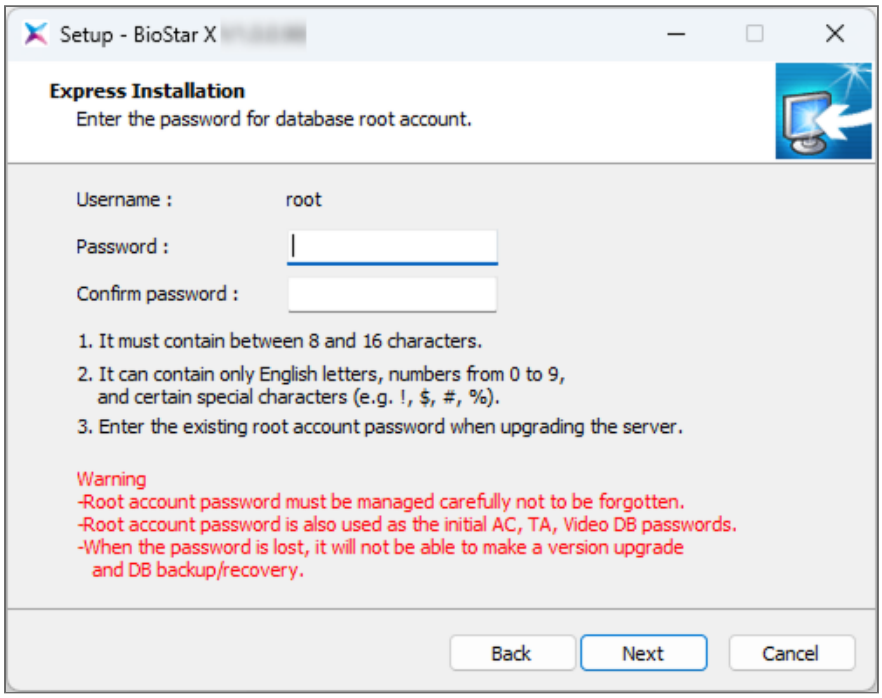
5. Ingrese la contraseña de la cuenta de administrador y haga clic en **Siguiente**.



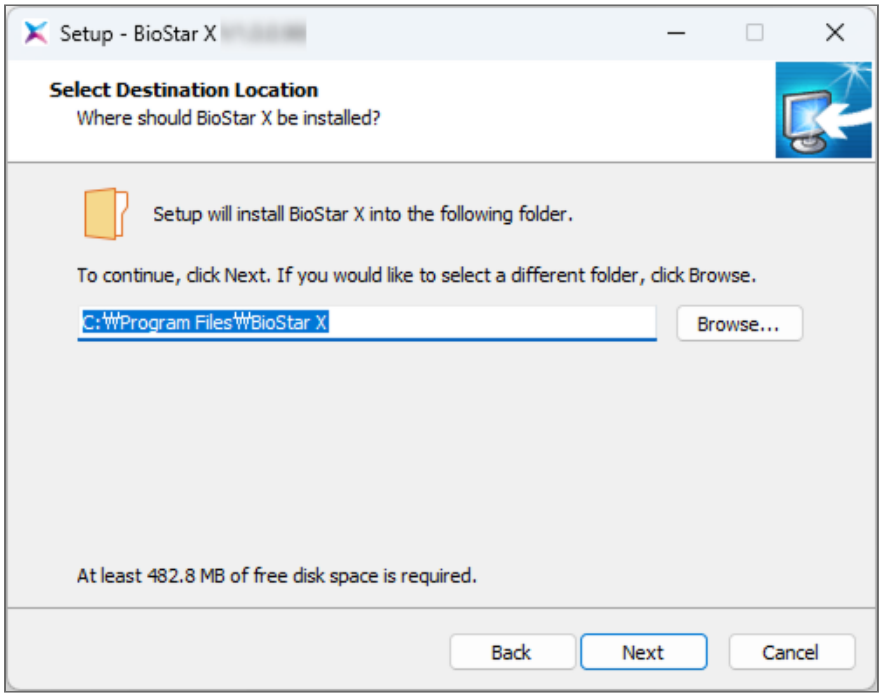
6. Seleccione **Instalación exprés** y haga clic en **Siguiente**.



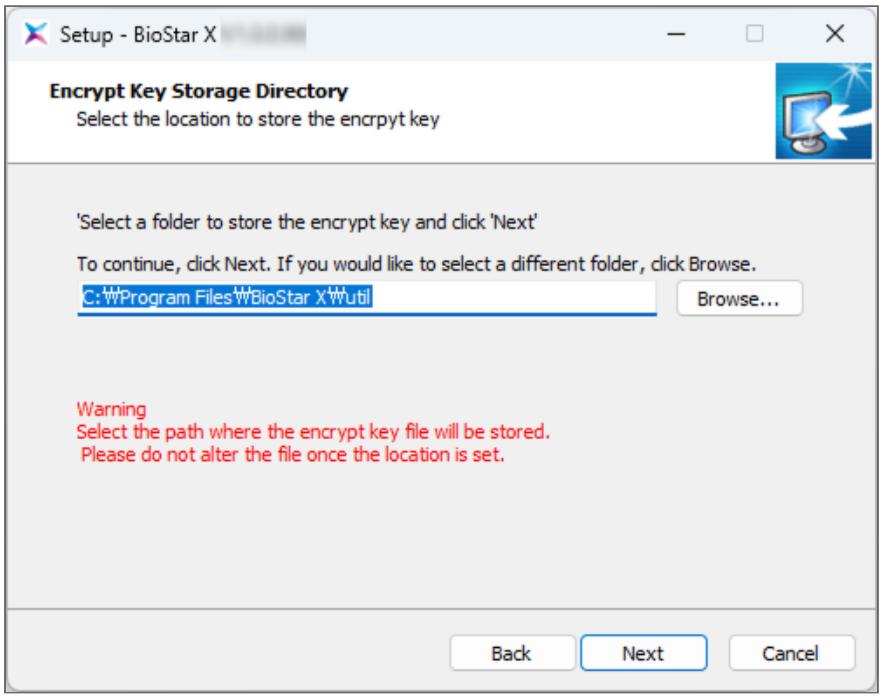
7. Ingrese la contraseña de la cuenta root de la base de datos y haga clic en el botón **Siguiente**.



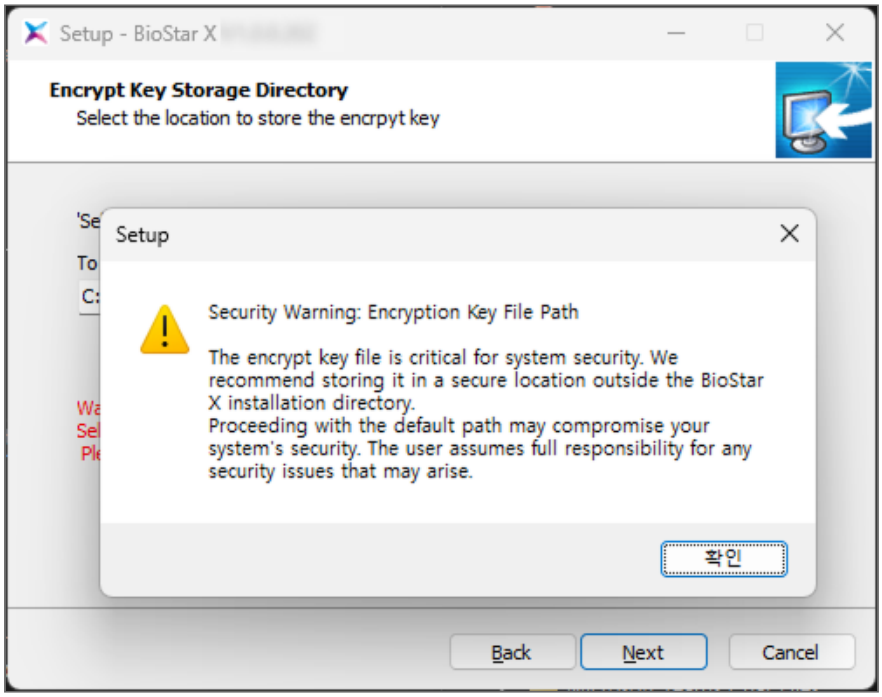
8. Establezca la ruta de instalación de **BioStar X** y haga clic en **Siguiente**.



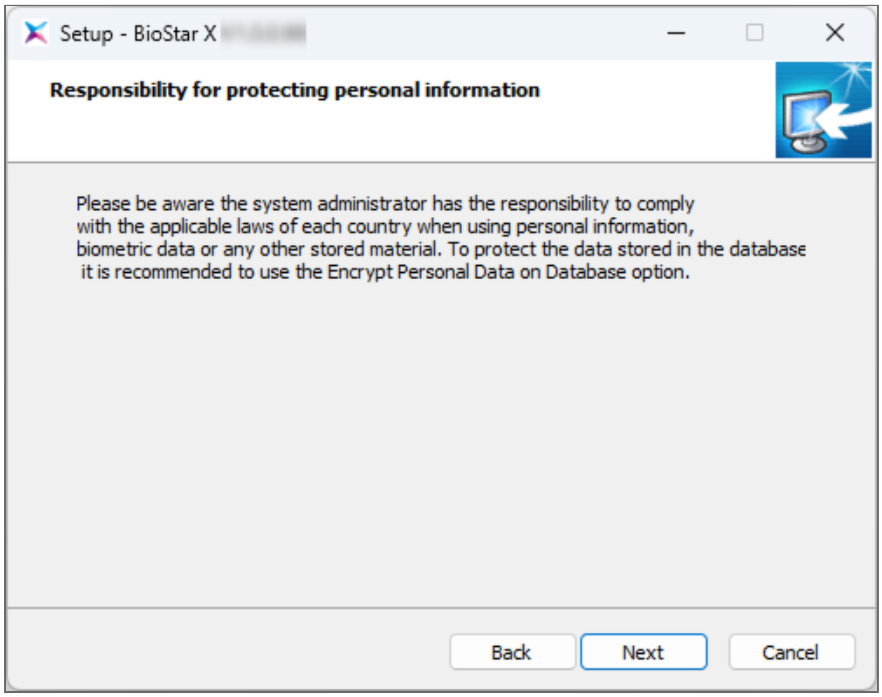
9. Establezca la ruta para almacenar la clave de cifrado y haga clic en **Siguiente**.



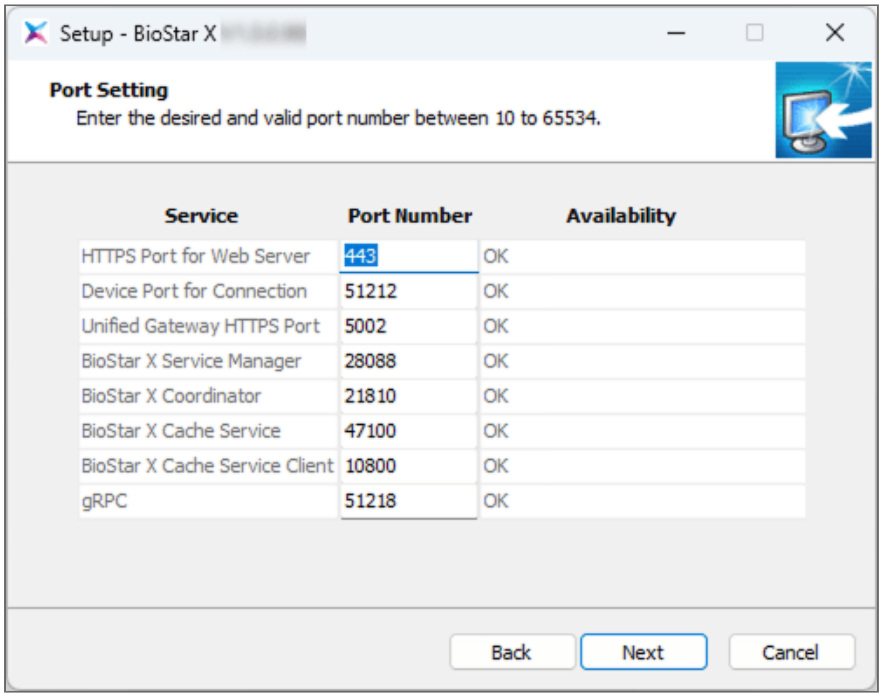
10. Revise el contenido del mensaje de advertencia de seguridad y haga clic en **Aceptar**.



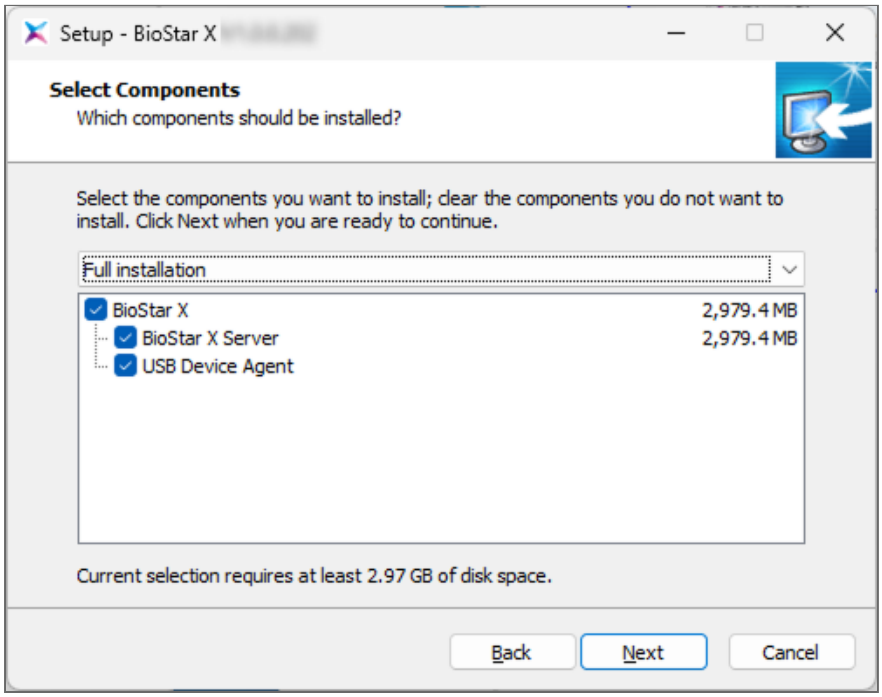
11. Lea la información sobre la gestión y la responsabilidad de los datos personales almacenados en la base de datos y haga clic en el botón **Siguiente** para continuar con la instalación.



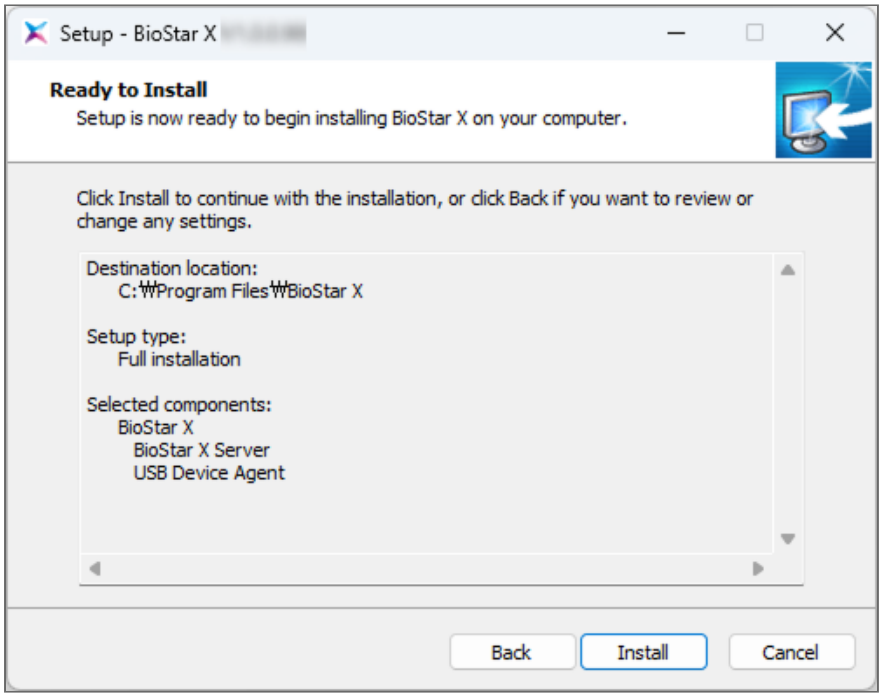
12. Configure el puerto de comunicación de **BioStar X** y haga clic en **Siguiente**.



13. Seleccione los componentes de **BioStar X** y haga clic en **Siguiente**. Al seleccionar **USB Device Agent**, se instalarán conjuntamente el USB Agent y el controlador para usar BioMini, BioMini Plus 2, BioMini Slim 2 y DUALi DE-620.



14. Cuando se completen todas las preparaciones para la instalación, haga clic en el botón **Instalar**.



15. Seleccione si instalar programas adicionales y haga clic en **Finish**.



16. Complete la instalación de **USB Device Agent** siguiendo las instrucciones en la pantalla de instalación.

Información

- En el nombre del archivo descargado, `X.Y.Z` es la información de la versión y `BB` es el número de compilación.
- La contraseña de la cuenta de administrador se usa al iniciar sesión por primera vez después de instalar **BioStar X**.
- La contraseña de la cuenta root de la base de datos se utiliza como contraseña inicial para AC, TA y Video DB.
- La ruta de almacenamiento de la clave de cifrado se puede cambiar. Si modificas o mueves el archivo de la clave de cifrado después de cambiar la ruta, puede ocurrir un error del sistema.
- Cuando se elimina **BioStar X**, el archivo de la clave de cifrado también se elimina.
- El certificado proporcionado del Agente de Dispositivo USB solo se puede aplicar a la red local.
- Si otro programa está usando el puerto 443, el programa BioStar X Setting se ejecuta automáticamente y permite cambiar el número de puerto. Para más información sobre cómo cambiar el número de puerto, consulta Cambiar el Puerto.
- Para más información sobre cómo cambiar la configuración de la base de datos, consulta Cambiar la Base de Datos.

Alerta

- Ten cuidado de no perder la contraseña de la cuenta de administrador o root de la base de datos.
- Si pierdes la contraseña, puede que no sea posible actualizar la versión ni hacer copias de seguridad o restaurar la BD.

Siguiente paso

Consulta cómo iniciar sesión en **BioStar X** a través de tu navegador web.
Verifica el estado del servidor de **BioStar X** y cómo apagarlo o reiniciarlo.

Instalación Personalizada

Este documento proporciona una guía paso a paso sobre cómo instalar **BioStar X** mediante el método **Instalación personalizada**. **Instalación personalizada** crea un esquema de base de datos junto con una base de datos existente (MariaDB, MS SQL Server) instalada en un servidor local o remoto. Prepare la base de datos y la cuenta de usuario que se vincularán antes de iniciar la instalación.

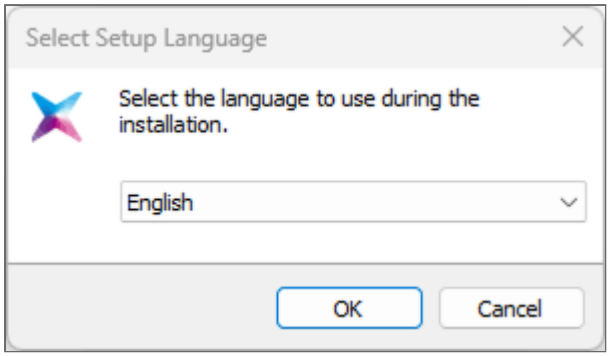
Antes de empezar

- Las bases de datos que se pueden usar en la integración con **BioStar X** son las siguientes.
  - MariaDB 11.4.4
  - MS SQL Server 2012 SP3
  - MS SQL Server 2014 SP2

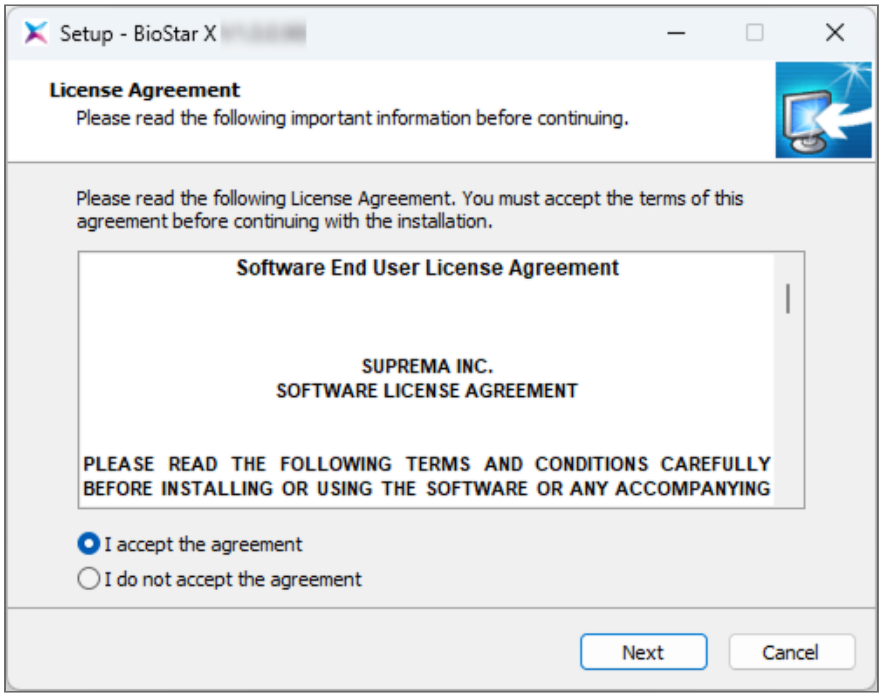
  - MS SQL Server 2016 SP1
  - MS SQL Server 2017
  - MS SQL Server 2019
  - MS SQL Server 2022
- La seguridad de comunicación de MS SQL Server admite TLS 1.2.
- Si la creación de tablas falla cuando se establece MS SQL Server como Tipo de base de datos, cree la tabla ejecutando el script en la carpeta *C:\Program Files\BioStar X\dbscript\mssql*.
- Al instalar con **Instalación personalizada**, **AC DB name**, **TA DB name** y **VE DB name** no pueden configurarse con el mismo nombre.
- Para usar la autenticación de Windows, se requiere Microsoft ODBC Driver 17 for SQL Server. Instale primero el controlador.

Guía de instalación

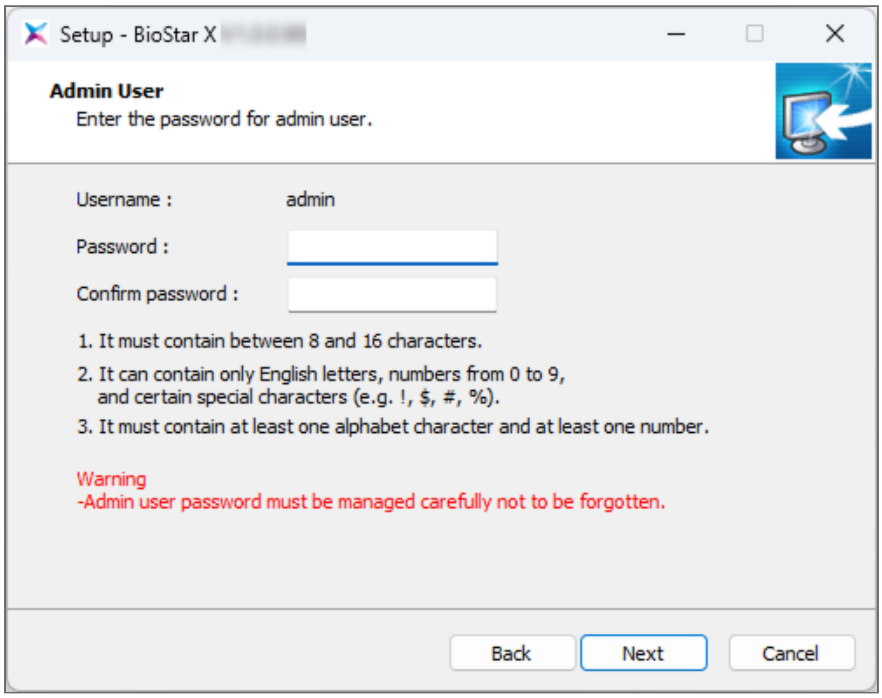
1. Vaya al Suprema Download Center, inicie sesión y descargue el paquete de instalación (*BioStar X Setup.X.Y.Z.BB.exe*).
2. Ejecute el archivo de instalación descargado.
3. Seleccione el idioma a usar y haga clic en el botón **Aceptar**.



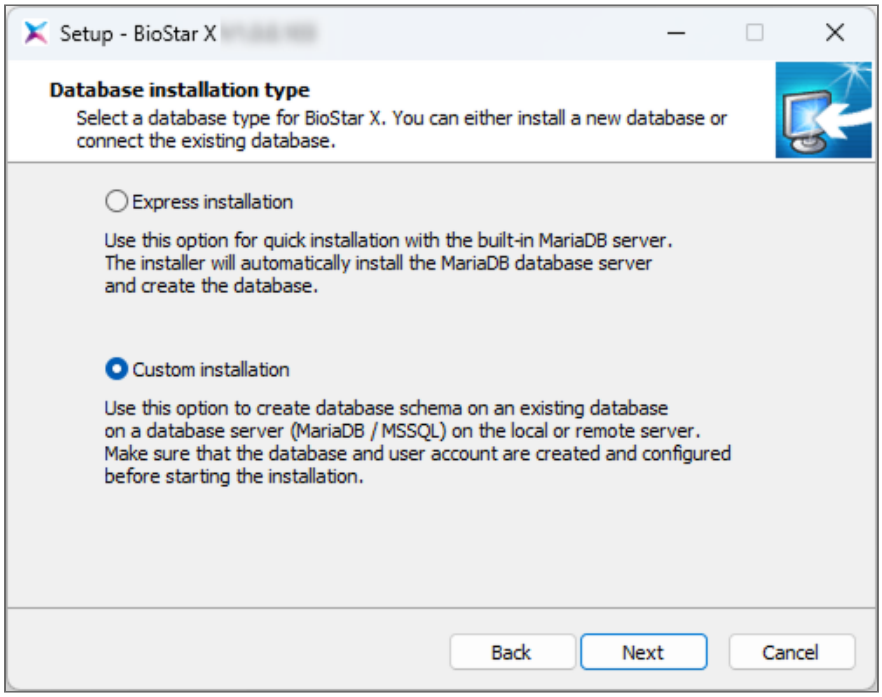
4. Para continuar con la instalación, seleccione **Acepto el acuerdo** y haga clic en el botón **Siguiente**.



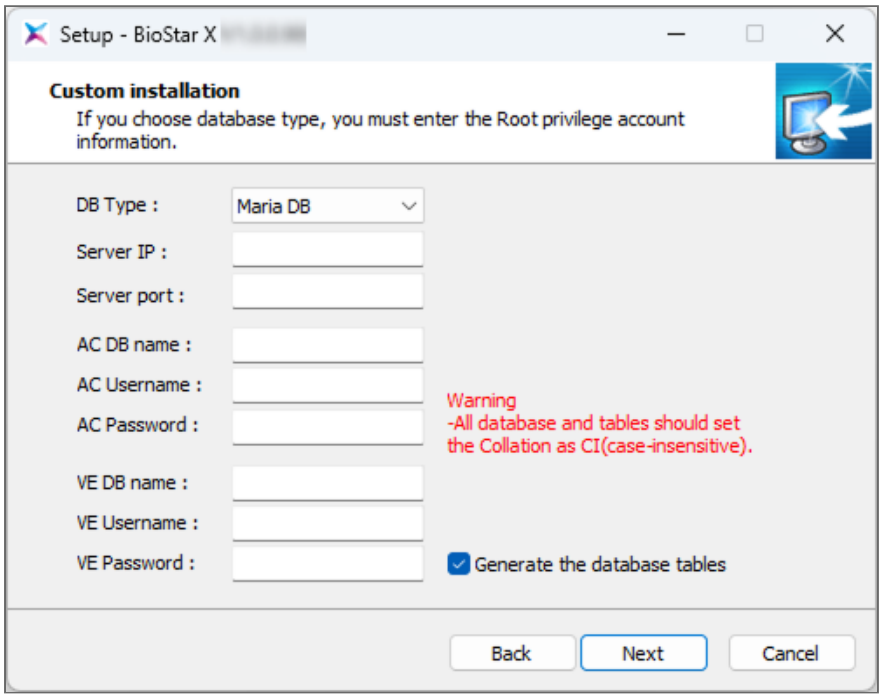
5. Ingrese la contraseña de la cuenta de administrador y haga clic en **Siguiente**.



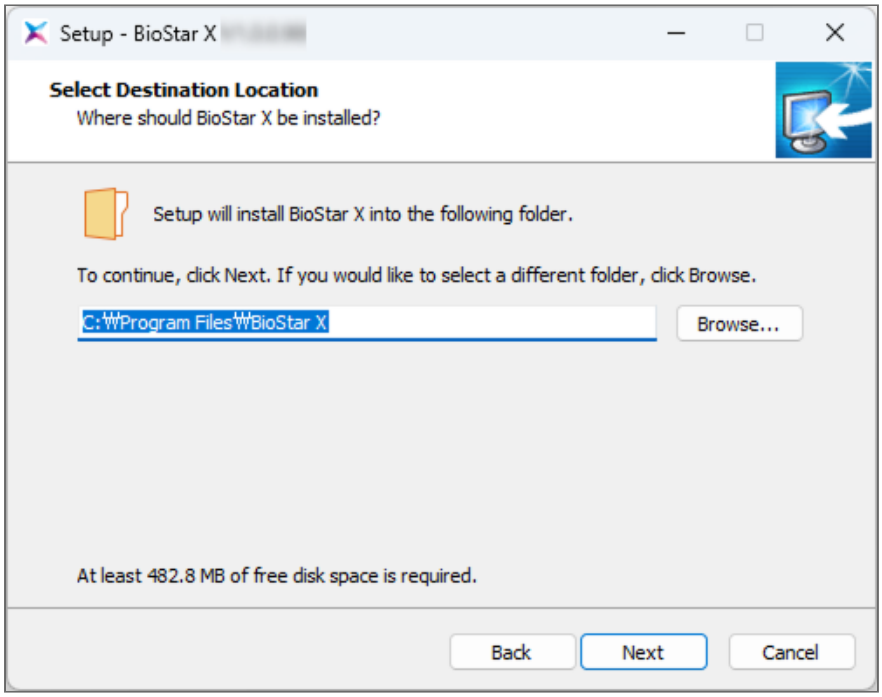
6. Seleccione **Instalación personalizada** y haga clic en **Siguiente**.



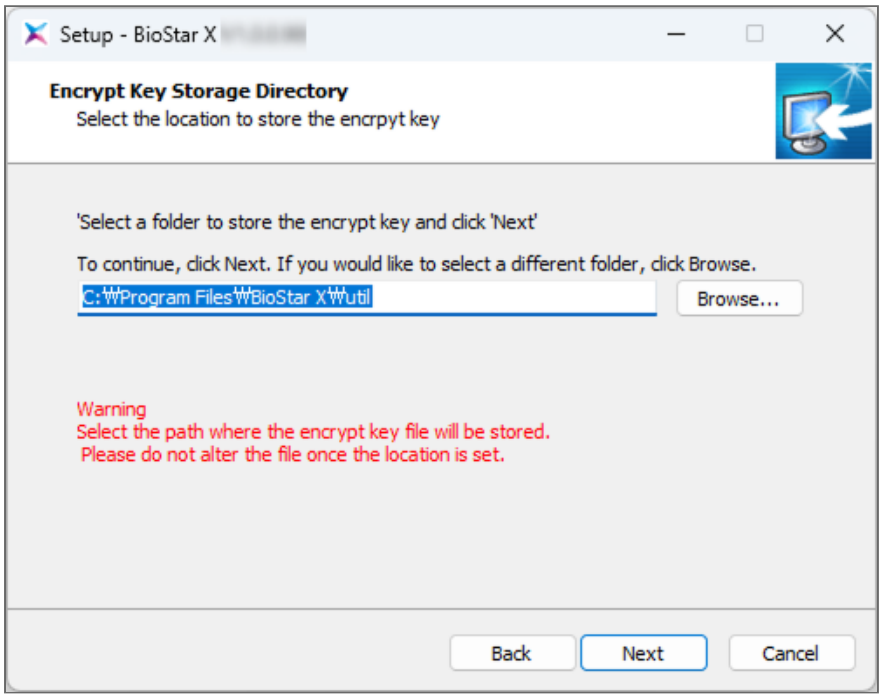
7. Introduzca los detalles de la base de datos preconfigurada y haga clic en **Siguiente**.



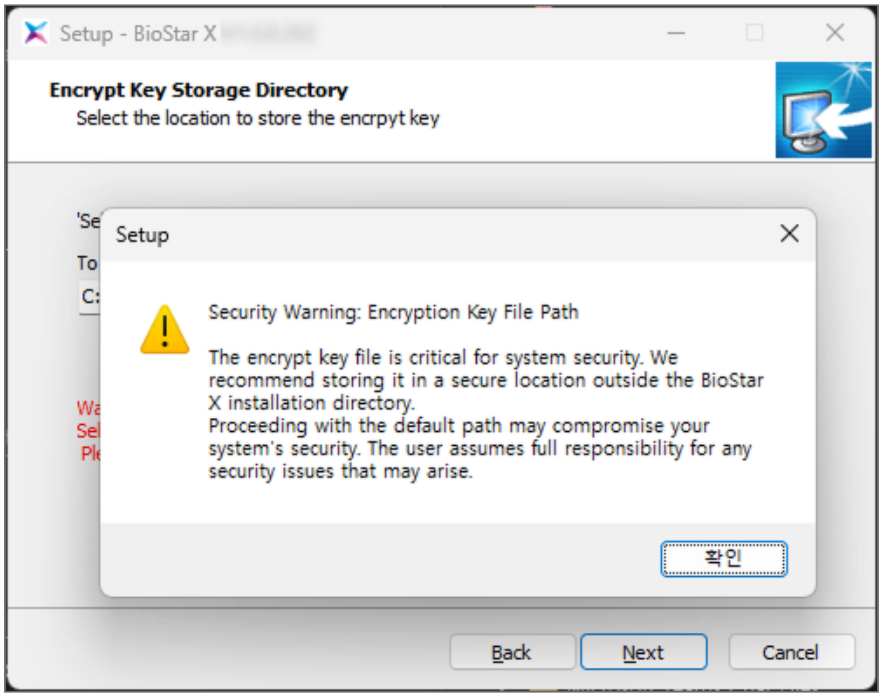
8. Establezca la ruta de instalación de **BioStar X** y haga clic en **Siguiente**.



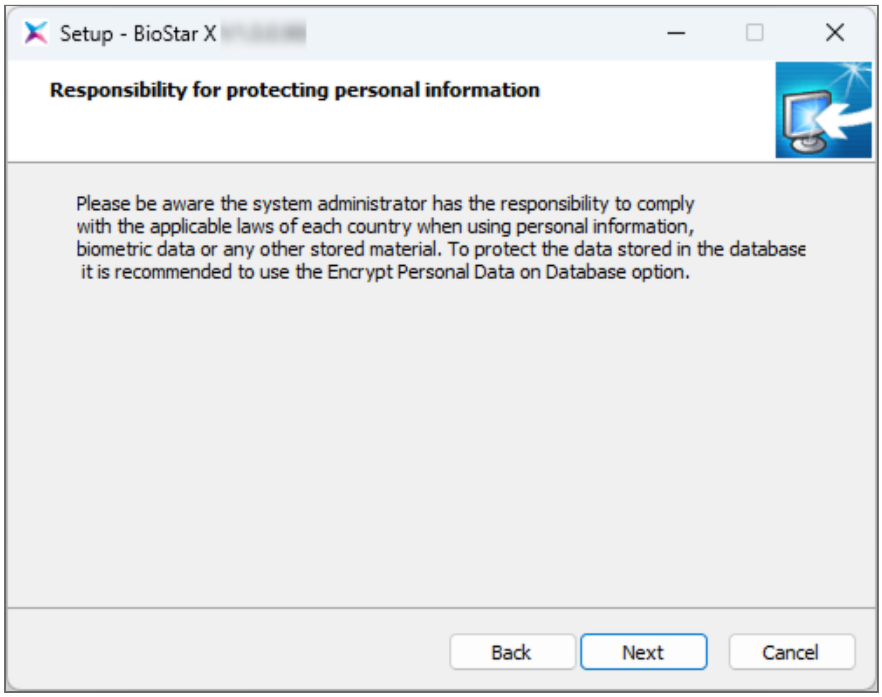
9. Establezca la ruta para almacenar la clave de cifrado y haga clic en **Siguiente**.



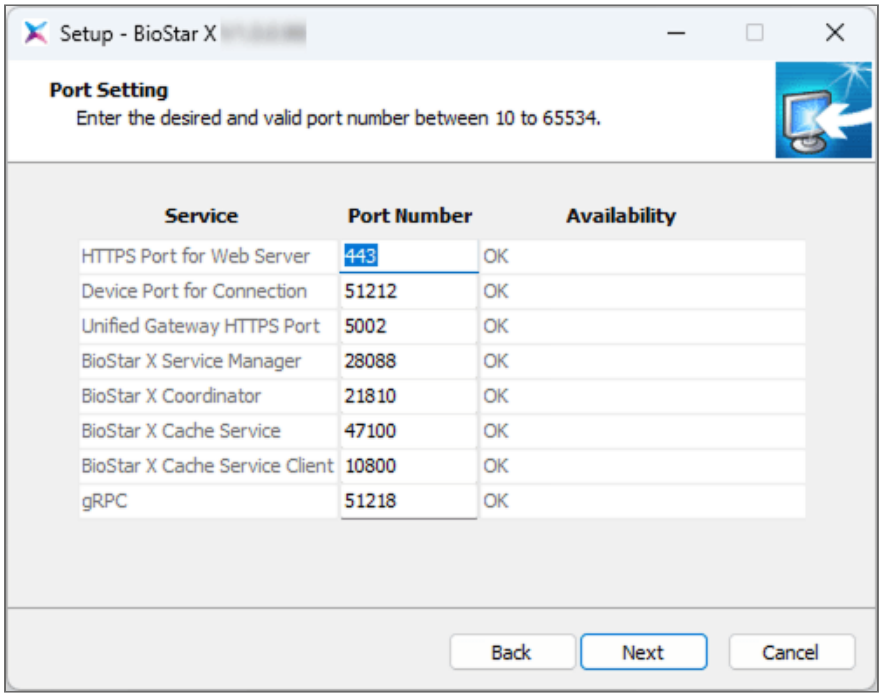
10. Revise el contenido del mensaje de advertencia de seguridad y haga clic en **Aceptar**.



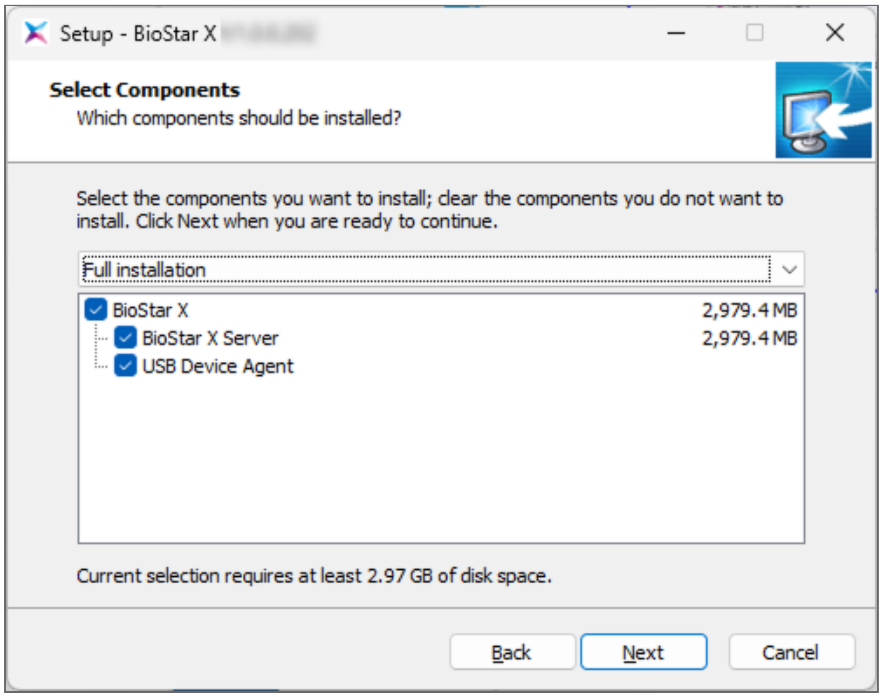
11. Lea la información sobre la gestión y la responsabilidad de los datos personales almacenados en la base de datos y haga clic en el botón **Siguiente** para continuar con la instalación.



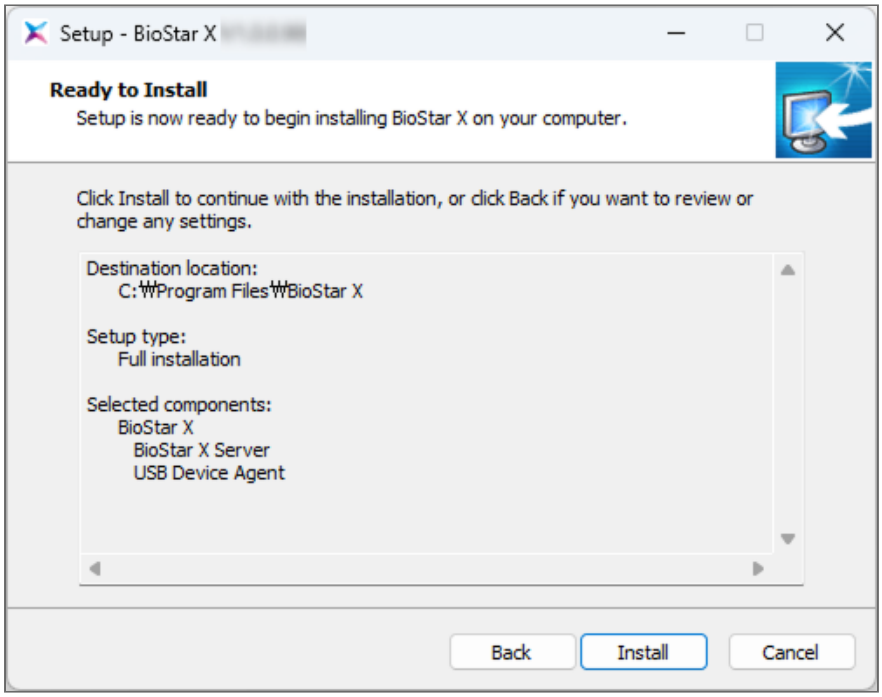
12. Configure el puerto de comunicación de **BioStar X** y haga clic en **Siguiente**.



13. Seleccione los componentes de **BioStar X** y haga clic en **Siguiente**. Al seleccionar **USB Device Agent**, se instalarán conjuntamente el USB Agent y el controlador para usar BioMini, BioMini Plus 2, BioMini Slim 2 y DUALi DE-620.



14. Cuando se completen todas las preparaciones para la instalación, haga clic en el botón **Instalar**.



15. Seleccione si instalar programas adicionales y haga clic en **Finish**.



16. Complete la instalación de **USB Device Agent** siguiendo las instrucciones en la pantalla de instalación.

Información

- En el nombre del archivo descargado, `X.Y.Z` es la información de la versión y `BB` es el número de compilación.
- La contraseña de la cuenta de administrador se usa al iniciar sesión por primera vez después de instalar **BioStar X**.
- La contraseña de la cuenta root de la base de datos se utiliza como contraseña inicial para AC, TA y Video DB.
- La ruta de almacenamiento de la clave de cifrado se puede cambiar. Si modificas o mueves el archivo de la clave de cifrado después de cambiar la ruta, puede ocurrir un error del sistema.
- Cuando se elimina **BioStar X**, el archivo de la clave de cifrado también se elimina.
- El certificado proporcionado del Agente de Dispositivo USB solo se puede aplicar a la red local.
- Si otro programa está usando el puerto 443, el programa BioStar X Setting se ejecuta automáticamente y permite cambiar el número de puerto. Para más información sobre cómo cambiar el número de puerto, consulta Cambiar el Puerto.
- Para más información sobre cómo cambiar la configuración de la base de datos, consulta Cambiar la Base de Datos.

Alerta

- Ten cuidado de no perder la contraseña de la cuenta de administrador o root de la base de datos.
- Si pierdes la contraseña, puede que no sea posible actualizar la versión ni hacer copias de seguridad o restaurar la BD.

Siguiente paso

Consulta cómo iniciar sesión en **BioStar X** a través de tu navegador web.
Verifica el estado del servidor de **BioStar X** y cómo apagarlo o reiniciarlo.

Actualizar

Este documento ofrece una guía paso a paso sobre cómo actualizar BioStar 2 a **BioStar X**. Verifique los requisitos del sistema y las precauciones antes de iniciar la actualización.

Antes de empezar

Verifique lo siguiente antes de actualizar de **BioStar 2** a **BioStar X**.

Información

Important

Requisitos mínimos

- Antes de continuar con la actualización, consulte Requisitos Mínimos del Sistema para confirmar que las especificaciones del servidor cumplen los requisitos.
- Si su entorno ejecuta BioStar 2 v2.9.11 o superior, puede actualizar a **BioStar X**.
  - Si utiliza una versión de BioStar 2 anterior a la v2.6.4, debe actualizarla de forma secuencial hasta la v2.9.11 antes de realizar la actualización. Para obtener instrucciones paso a paso sobre cómo actualizar BioStar 2, consulte la **Guía de administración de BioStar 2**.
  - No es posible actualizar las versiones de BioStar 2 inferiores a la v2.9.10.
- Si los siguientes dispositivos están conectados a BioStar 2, la actualización a **BioStar X** no está soportada.
  - XPass S2, XPass, BioEntry W, BioEntry Plus, BioLite Net

Licencia

- Debe contactar a su distribuidor para disponer de al menos una licencia de BioStar X antes de actualizar a **BioStar X**.
- Al actualizar a **BioStar X** se aplica una política de licenciamiento diferente a la de BioStar 2.
- Si realiza la actualización con una licencia BioStar 2 AC Advanced o superior activada, se eliminarán las siguientes funciones y ajustes del servicio.
  - Mapa Gráfico
  - Nube
- Para utilizar el servicio T&A de BioStar 2 en **BioStar X**, debe adquirir por separado la licencia **BioStar X T&A**.

Alerta

Verifica el certificado

Cuando actualizas de BioStar 2 a BioStar X, el archivo `biostar_cert.crt` en `nginx\conf` y el de `nginx\cert` pueden diferir. Actualizar en este estado causa los siguientes problemas.

- Ciertos registros de auditoría no se registran.
- Falla la creación de grupos de usuarios, la adición de Wiegand y la actualización del árbol.

Sigue estos pasos para hacer que los archivos de certificado coincidan antes de actualizar a BioStar X.

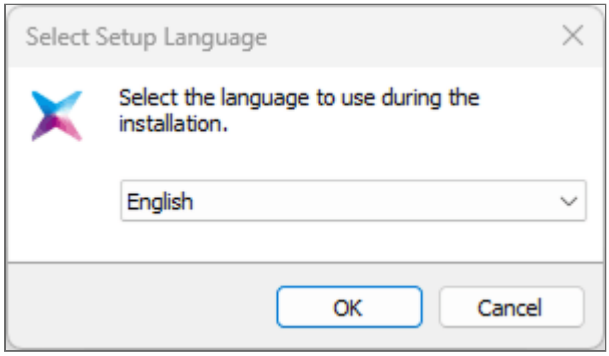
1. Detén el servicio de BioStar 2.
2. Sobrescribe los archivos `biostar_cert.crt` y `biostar_cert.key` en `nginx\cert` con los archivos de `nginx\conf`.
3. Reinicia el servicio de BioStar 2.

Guía de instalación de la actualización

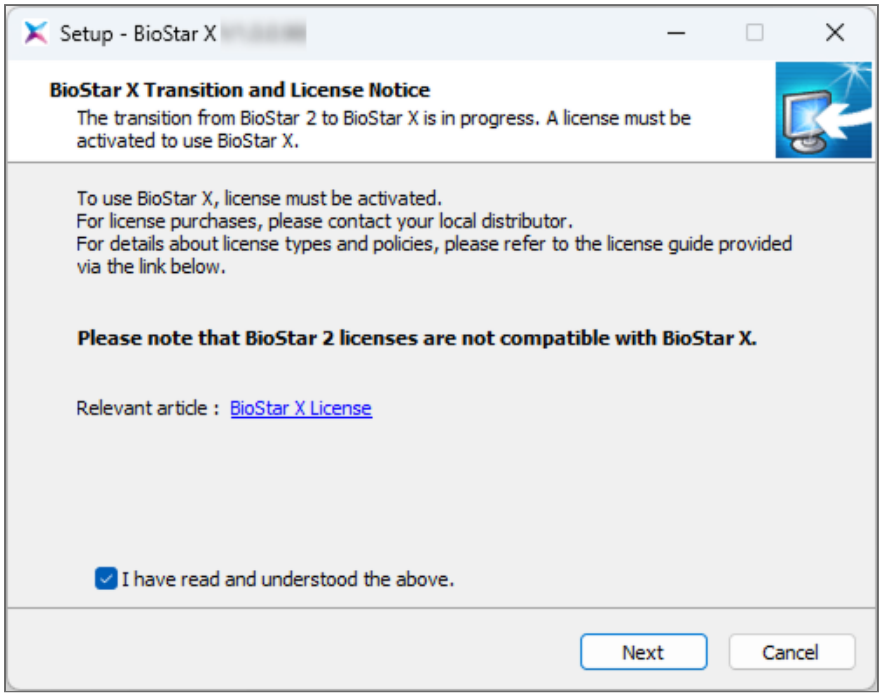
1. Vaya al Suprema Download Center, inicie sesión y descargue el paquete de instalación (*BioStar X Setup.X.Y.Z.BB.exe*).

2. Ejecute el archivo de instalación descargado.

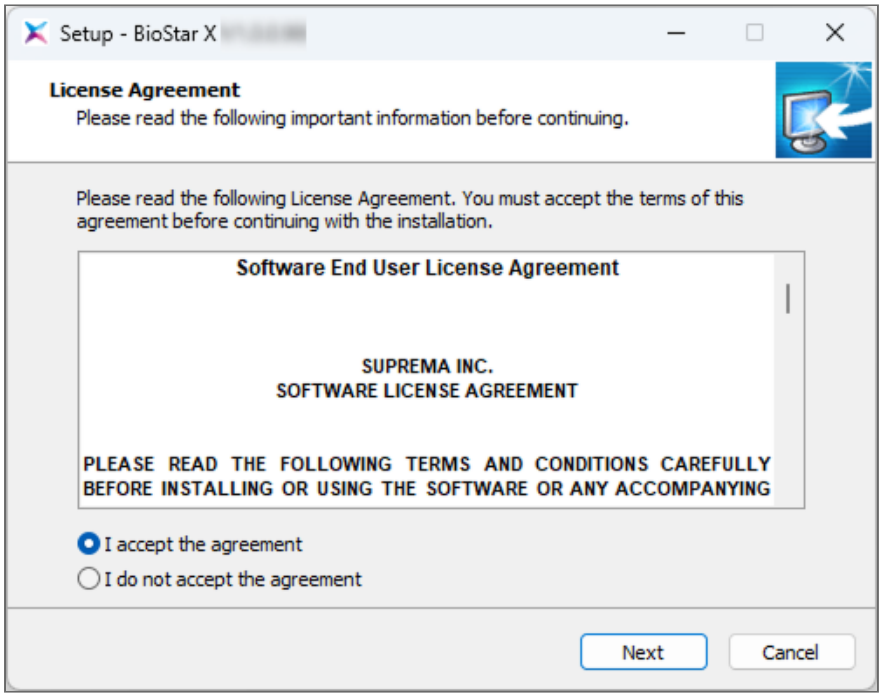
3. Seleccione el idioma a usar y haga clic en el botón **Aceptar**.



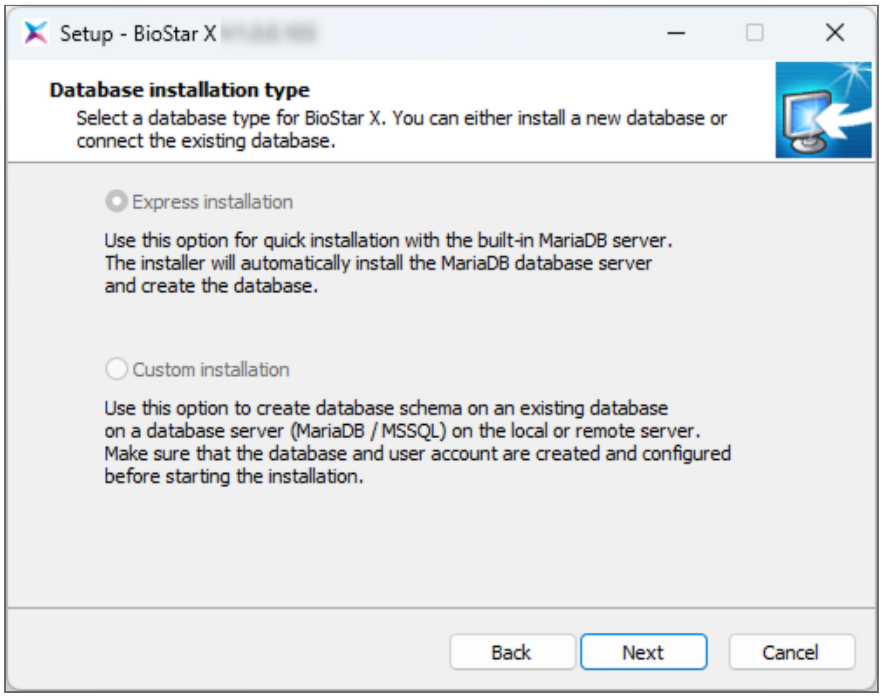
4. Acepte la política de licenciamiento de la transición de BioStar 2 a **BioStar X**. Marque la casilla y seleccione el botón **Siguiente**.



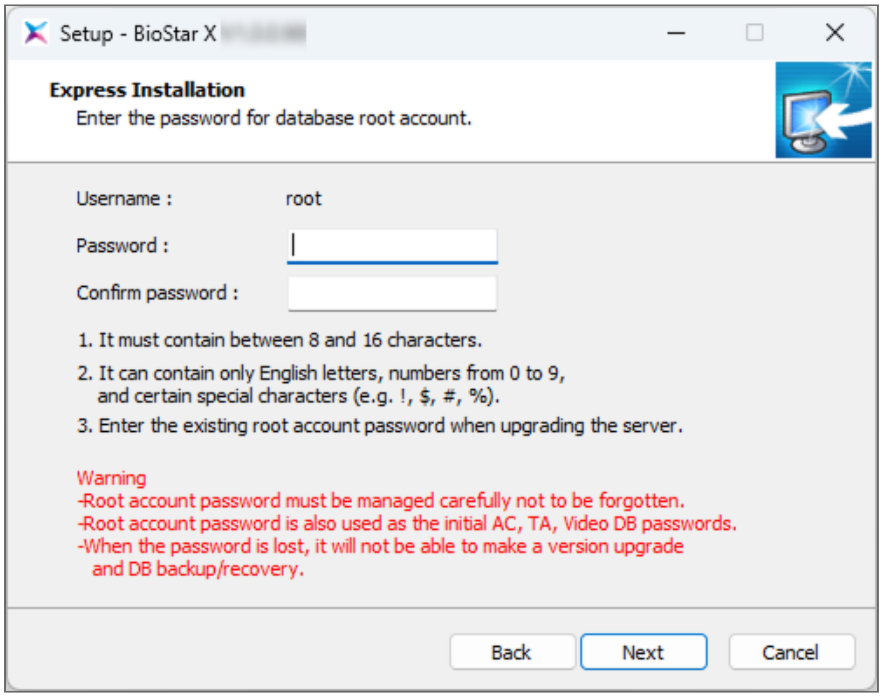
5. Para continuar con la instalación, seleccione **Acepto el acuerdo** y haga clic en el botón **Siguiente**.



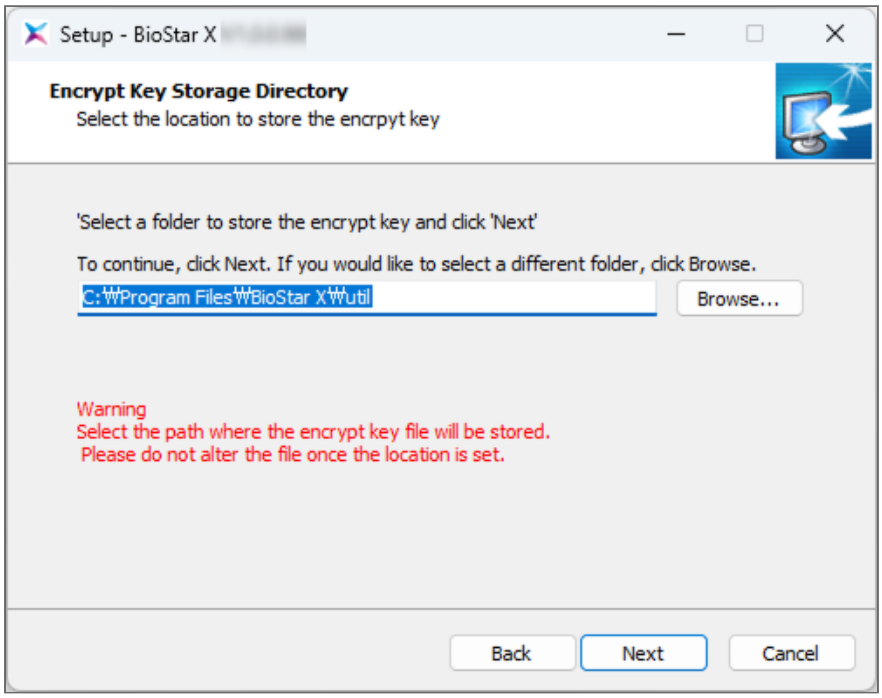
6. Al actualizar desde BioStar 2, la base de datos existente se conectará para continuar con la instalación. Seleccione el botón **Siguiente**.



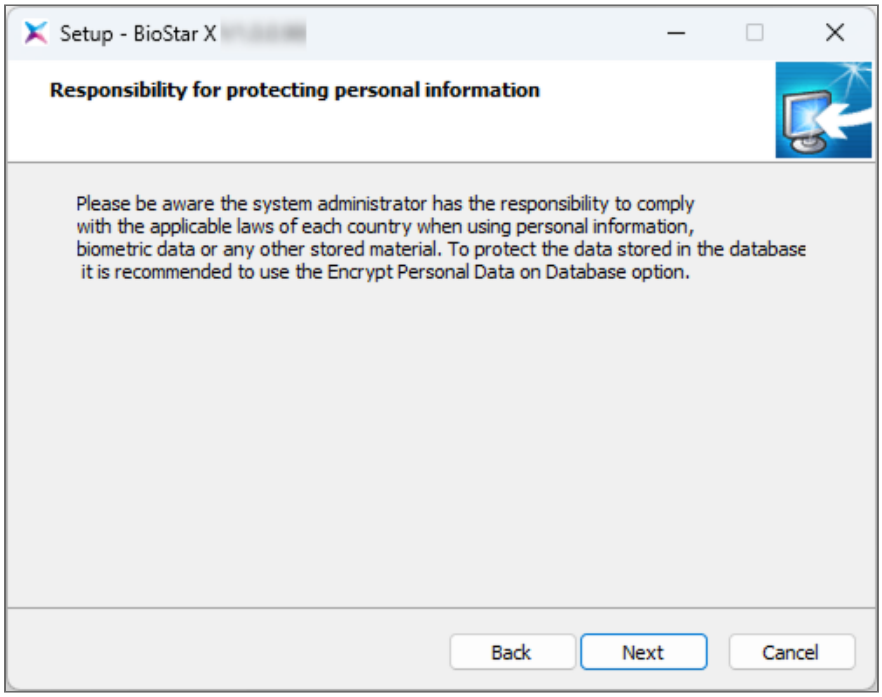
7. Ingrese la contraseña de la cuenta root de la base de datos existente y seleccione el botón **Siguiente**.



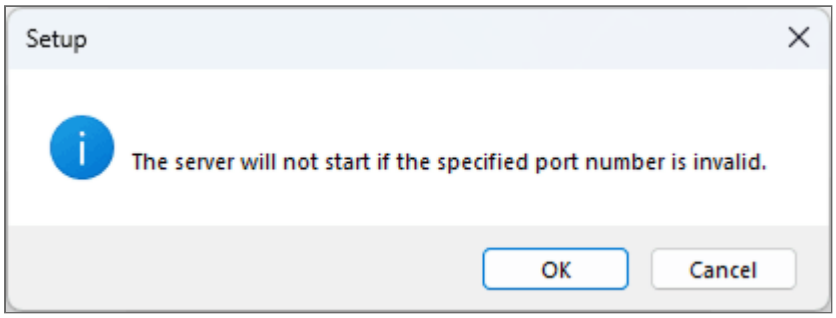
8. Establezca la ruta para almacenar la clave de cifrado y haga clic en **Siguiente**.



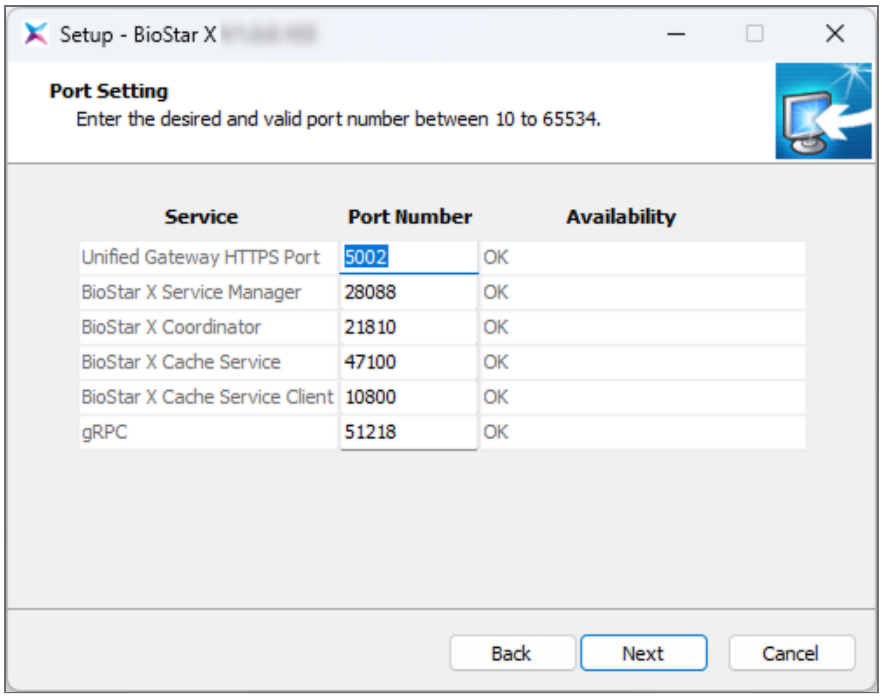
9. Lea la información sobre la gestión y la responsabilidad de los datos personales almacenados en la base de datos y haga clic en el botón **Siguiente** para continuar con la instalación.



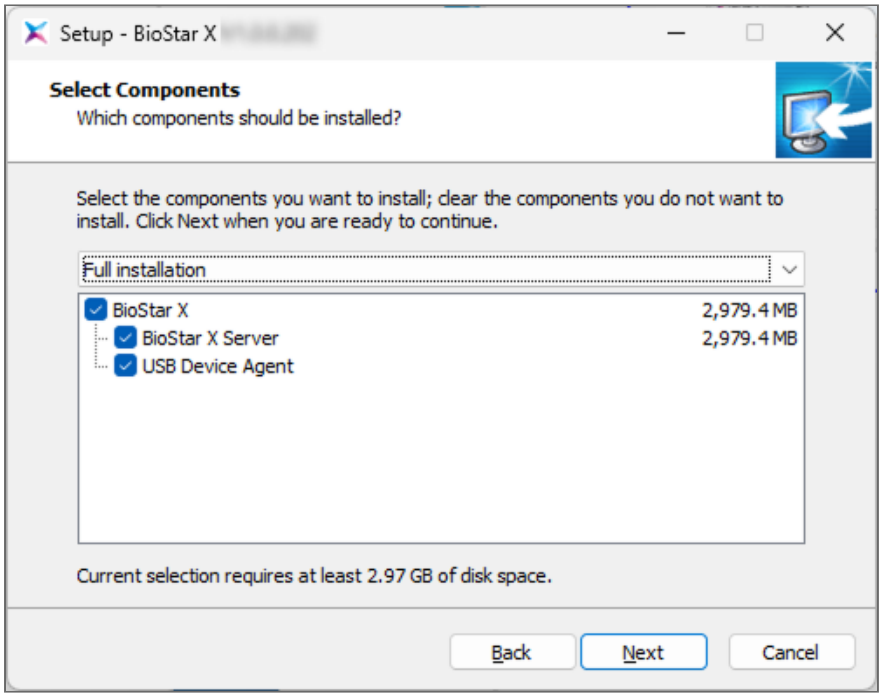
10. Si aparece un mensaje relacionado con el número de puerto, seleccione **Aceptar**.



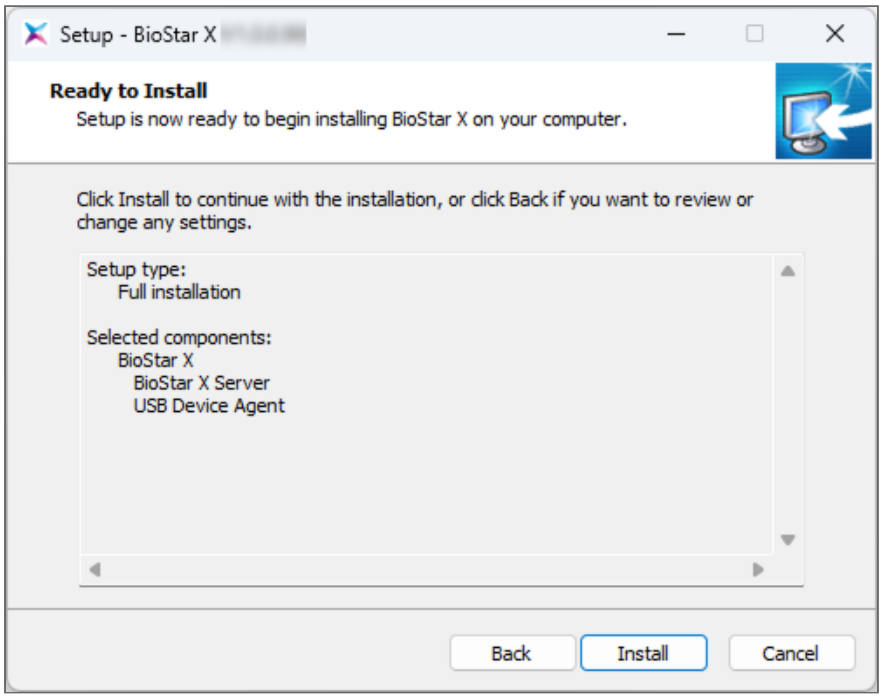
11. Configure el puerto de comunicación de **BioStar X** y haga clic en **Siguiente**.



12. Seleccione los componentes de **BioStar X** y haga clic en **Siguiente**. Al seleccionar **USB Device Agent**, se instalarán conjuntamente el USB Agent y el controlador para usar BioMini, BioMini Plus 2, BioMini Slim 2 y DUALi DE-620.



13. Cuando se completen todas las preparaciones para la instalación, haga clic en el botón **Instalar**.



14. Seleccione si instalar programas adicionales y haga clic en **Finish**.



15. Complete la instalación de **USB Device Agent** siguiendo las instrucciones en la pantalla de instalación.

Información

- En el nombre del archivo descargado, `X.Y.Z` es la información de la versión y `BB` es el número de compilación.
- La contraseña de la cuenta de administrador se usa al iniciar sesión por primera vez después de instalar **BioStar X**.
- La contraseña de la cuenta root de la base de datos se utiliza como contraseña inicial para AC, TA y Video DB.
- La ruta de almacenamiento de la clave de cifrado se puede cambiar. Si modificas o mueves el archivo de la clave de cifrado después de cambiar la ruta, puede ocurrir un error del sistema.
- Cuando se elimina **BioStar X**, el archivo de la clave de cifrado también se elimina.
- El certificado proporcionado del Agente de Dispositivo USB solo se puede aplicar a la red local.
- Si otro programa está usando el puerto 443, el programa BioStar X Setting se ejecuta automáticamente y permite cambiar el número de puerto. Para más información sobre cómo cambiar el número de puerto, consulta Cambiar el Puerto.
- Para más información sobre cómo cambiar la configuración de la base de datos, consulta Cambiar la Base de Datos.

Alerta

- Ten cuidado de no perder la contraseña de la cuenta de administrador o root de la base de datos.
- Si pierdes la contraseña, puede que no sea posible actualizar la versión ni hacer copias de seguridad o restaurar la BD.

Siguiente paso

Consulta cómo iniciar sesión en **BioStar X** a través de tu navegador web.
Verifica el estado del servidor de **BioStar X** y cómo apagarlo o reiniciarlo.

Instalar el Servidor de Comunicaciones Múltiples

Este documento explica cómo instalar el **BioStar X Servidor de Comunicaciones Múltiples**.

El servidor de comunicaciones múltiples gestiona la comunicación con dispositivos de control de acceso. Al instalarlo por separado del servidor principal, ayuda a gestionar muchos dispositivos de forma confiable. Un solo servidor de comunicaciones múltiples puede conectar hasta 1,000 dispositivos. Agregue varios servidores de comunicaciones múltiples según sea necesario.

> **Información**
> Hasta 1,000 dispositivos pueden conectarse a través de Ethernet (TCP/IP).

Antes de empezar

Antes de instalar el servidor de comunicaciones múltiples, verifique lo siguiente.

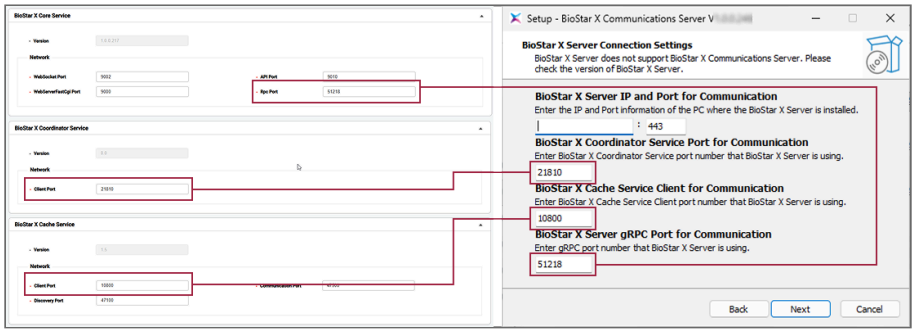
- El servidor de comunicaciones múltiples no puede instalarse en el mismo servidor que el servidor de **BioStar X**.
- El servidor de comunicaciones múltiples solo puede instalarse en un sistema operativo de 64 bits. Para obtener más información sobre los requisitos mínimos del sistema, consulte Requisitos Mínimos del Sistema.
- Necesita una licencia del servidor de comunicaciones múltiples para instalarlo y conectarlo. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Verificaciones previas a la instalación

Antes de instalar el servidor de comunicaciones múltiples, ejecute **BioStar X Service Manager** para comprobar la información necesaria durante la instalación.

1. Haz clic en Inicio → **BioStar X** → **BioStar X Service Manager** en Windows.
2. La ventana **BioStar X Service Manager** aparece.
3. Haga clic en **SERVICE SETTINGS**.

A continuación se muestra la información necesaria para instalar el servidor de comunicaciones múltiples. Revise y prepare cada elemento.



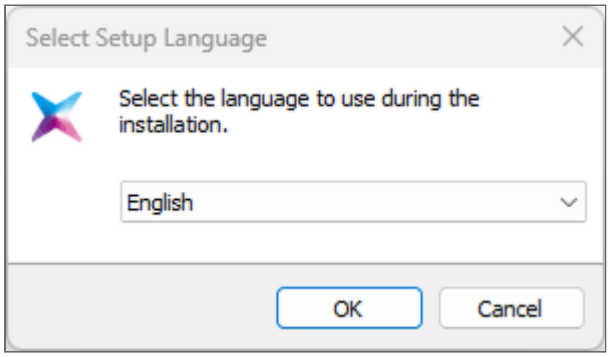
BioStar X Service Manager	Información requerida para la instalación del servidor de comunicaciones múltiples
BioStar X Core Service → RPC Port	Puerto gRPC del servidor BioStar X para comunicación
BioStar X Coordinator Service → Client Port	Puerto del servicio BioStar X Coordinator para comunicación
BioStar X Cache Service → Client Port	Cliente del servicio BioStar X Cache para comunicación

> **Información**
> Para obtener más información sobre **SERVICE SETTINGS**, consulte Configuración del Servicio.

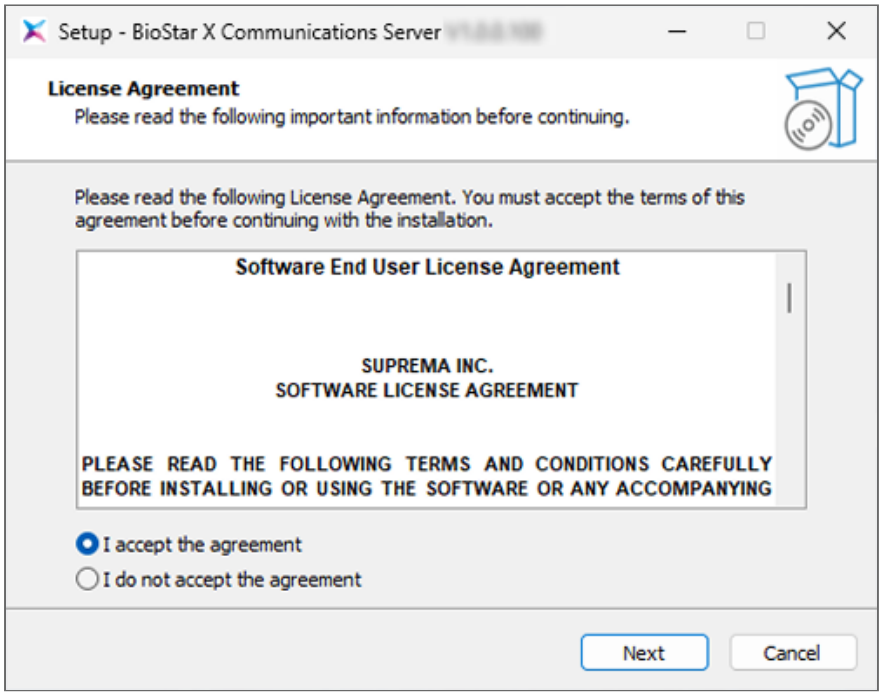
Guía de instalación

Siga los pasos a continuación para instalar el servidor de comunicaciones múltiples.

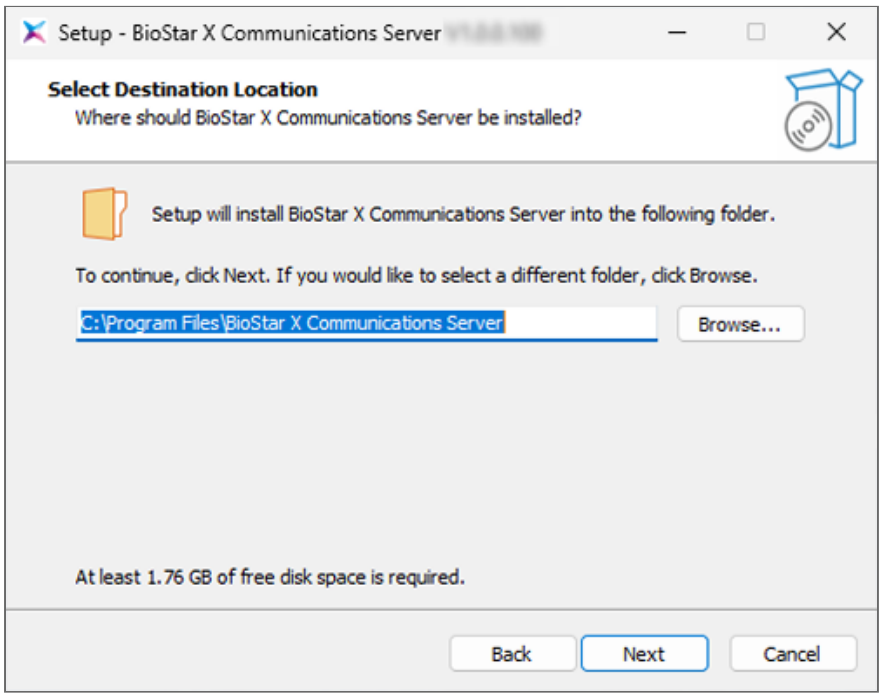
1. Acceda al Suprema Download Center, inicie sesión y descargue el paquete de instalación (*BioStar X Communications Server.X.Y.X.BB.exe*).
2. Ejecute el archivo de instalación descargado.
3. Seleccione el idioma a usar y haga clic en el botón **Aceptar**.



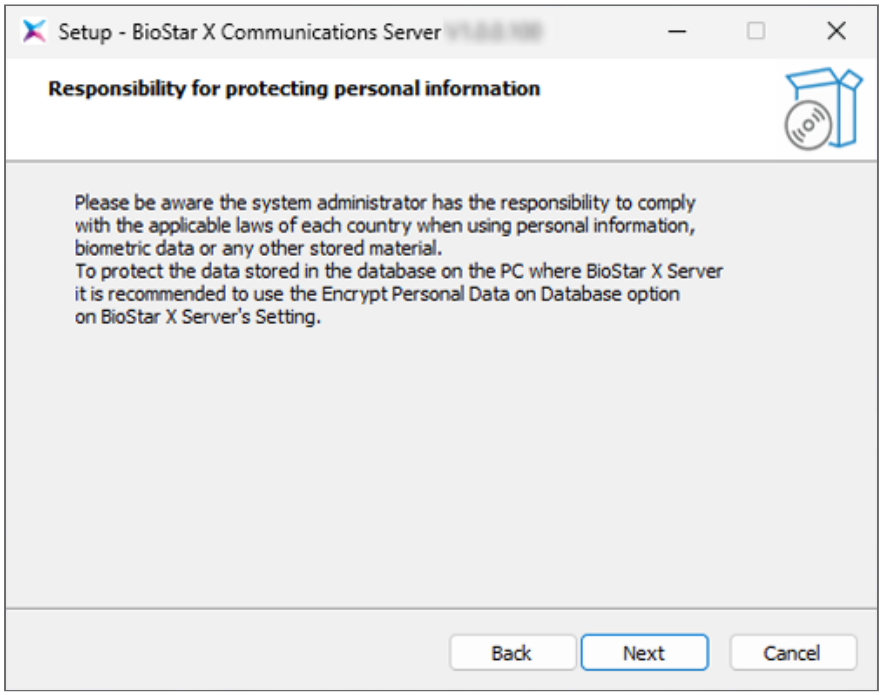
4. Para continuar con la instalación, seleccione **Acepto el acuerdo** y haga clic en el botón **Siguiente**.



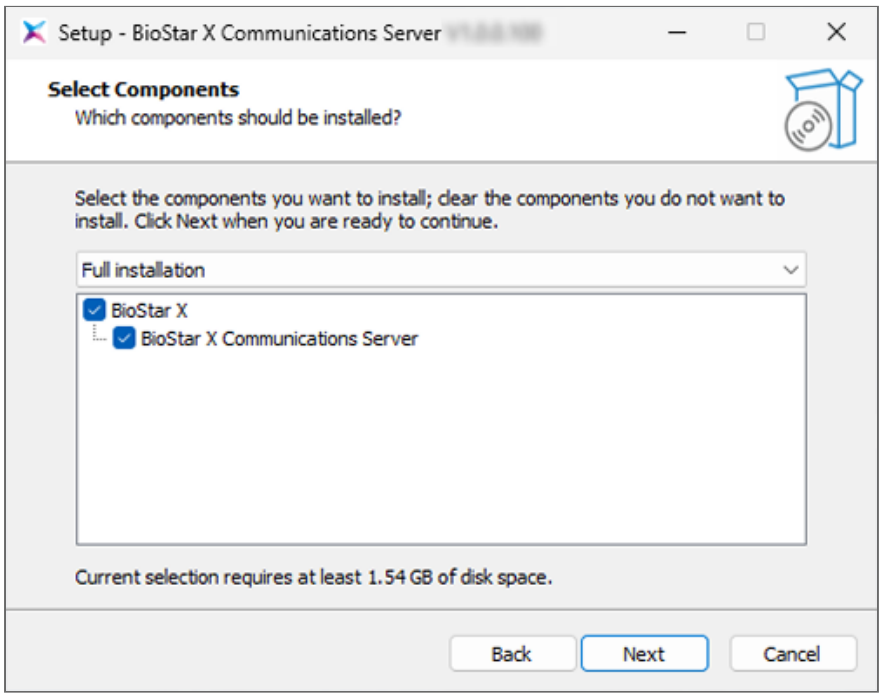
5. Defina la ruta de instalación del servidor de comunicaciones múltiples y haga clic en **Siguiente**.



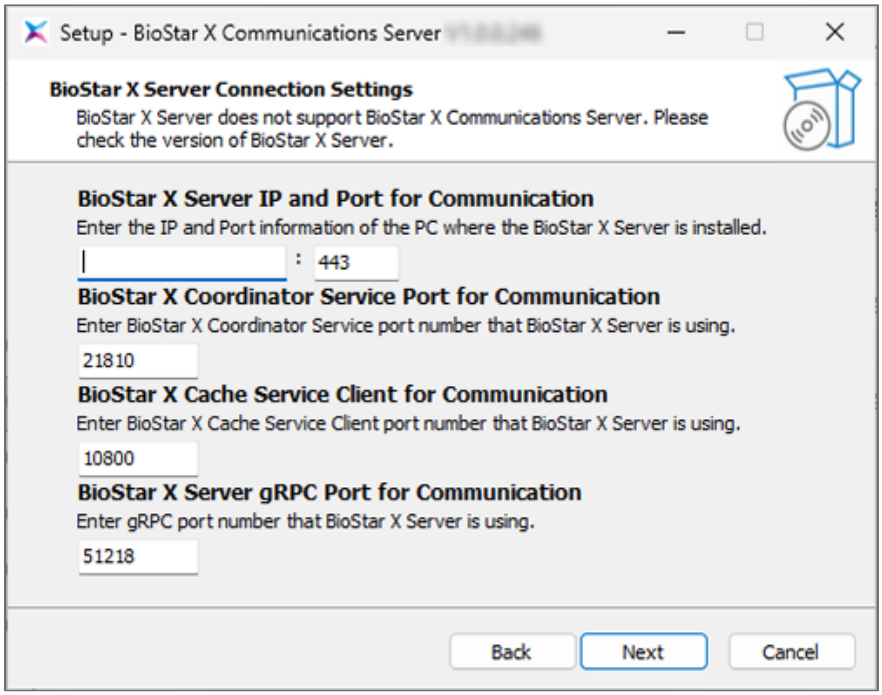
6. Revise los permisos y responsabilidades relacionados con la información personal y haga clic en **Siguiente** para continuar con la instalación.



7. Seleccione los componentes del servidor de comunicaciones múltiples y haga clic en **Siguiente**.

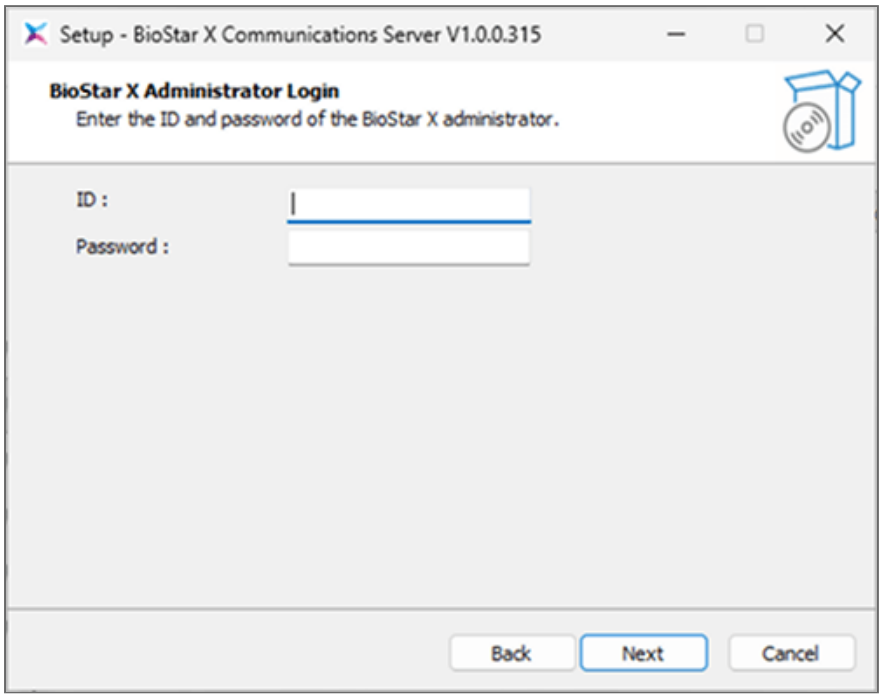


8. Ingrese la dirección IP y el número de puerto del servidor **BioStar X**, e introduzca los detalles para la conexión al servidor **BioStar X**. Complete su configuración y haga clic en **Siguiente**.

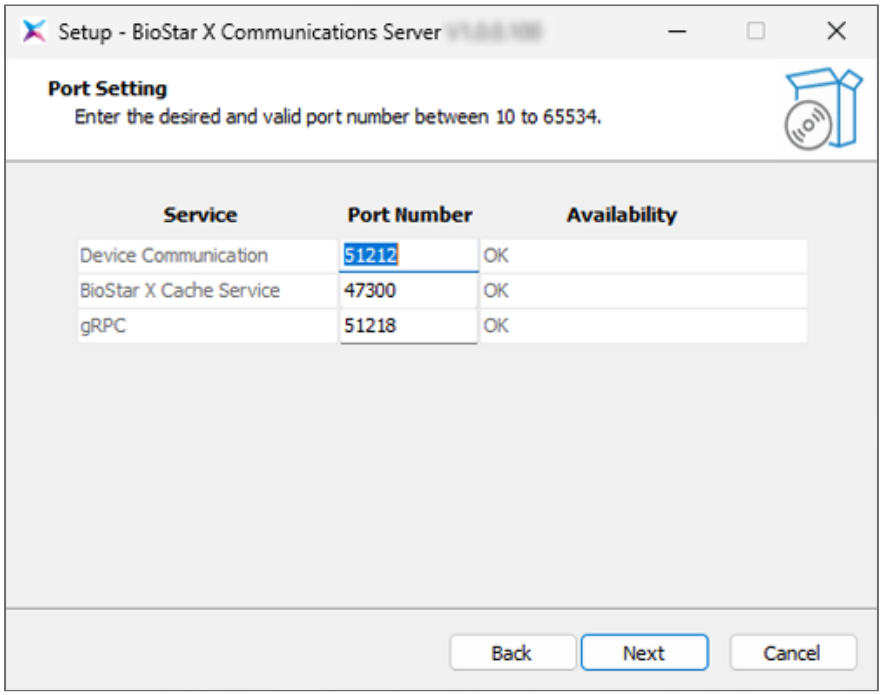


> Para obtener más información sobre cada campo de entrada, consulte Verificaciones previas a la instalación.

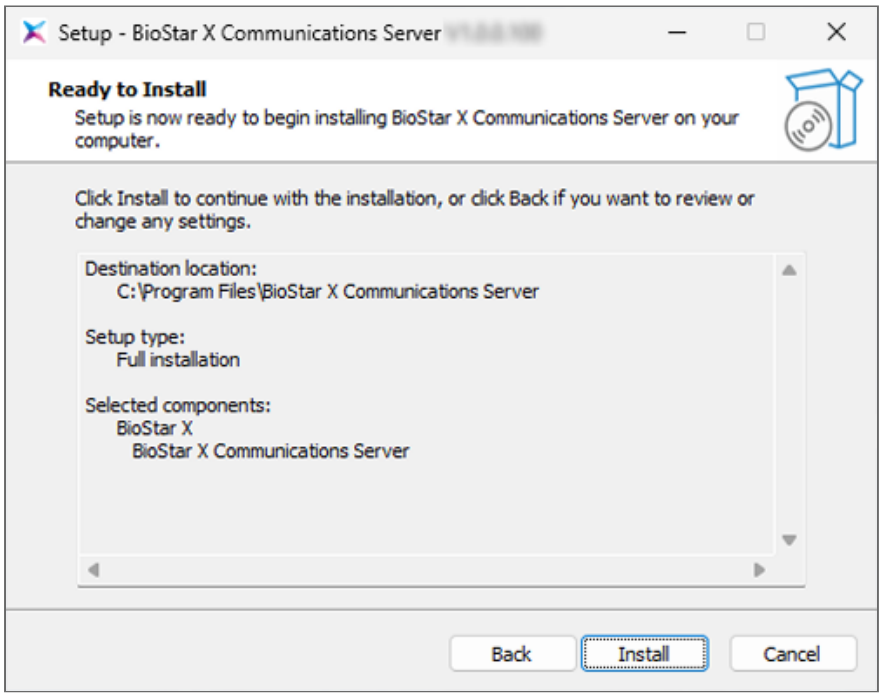
9. Ingrese el ID y la contraseña del administrador de **BioStar X**, luego haga clic en **Siguiente**.



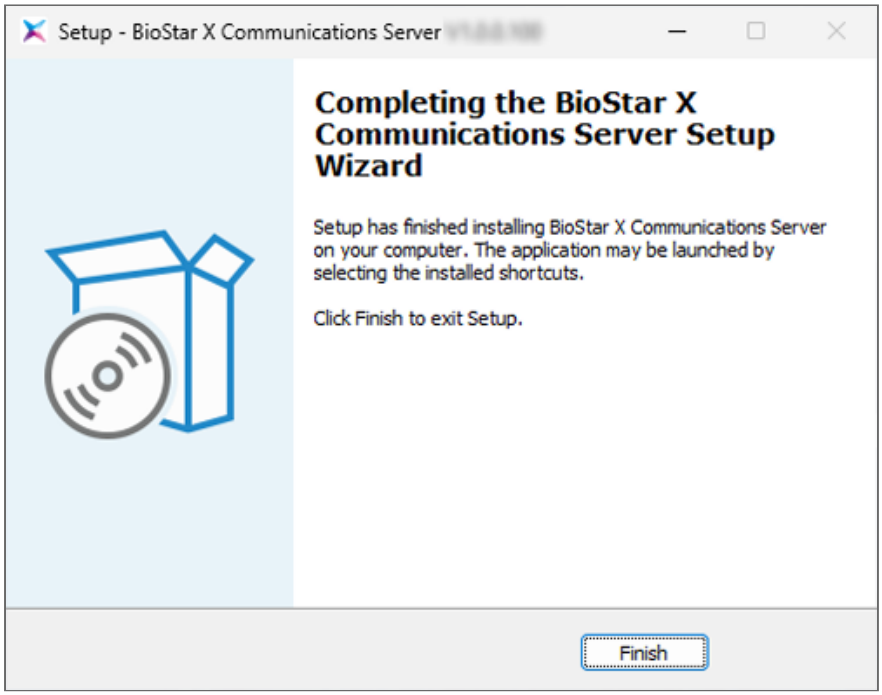
10. Configure el puerto para la comunicación y haga clic en **Siguiente**.



11. Cuando se completen todas las preparaciones para la instalación, haga clic en el botón **Instalar**. Proceda con la instalación.



12. Verifique el mensaje de finalización de instalación y haga clic en **Finalizar**.

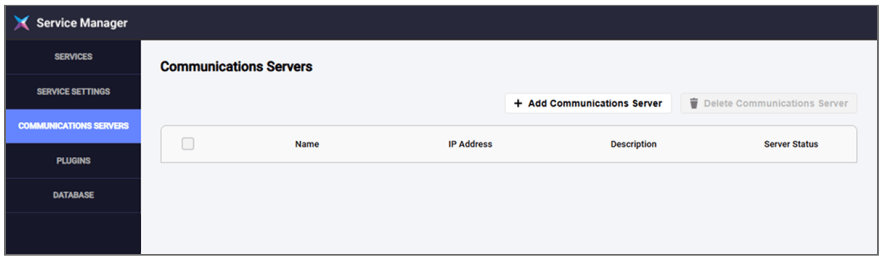


Complete la instalación del servidor de comunicaciones múltiples. Una vez finalizada la instalación, verifique la conexión entre el servidor de comunicaciones múltiples y el servidor principal de **BioStar X**.

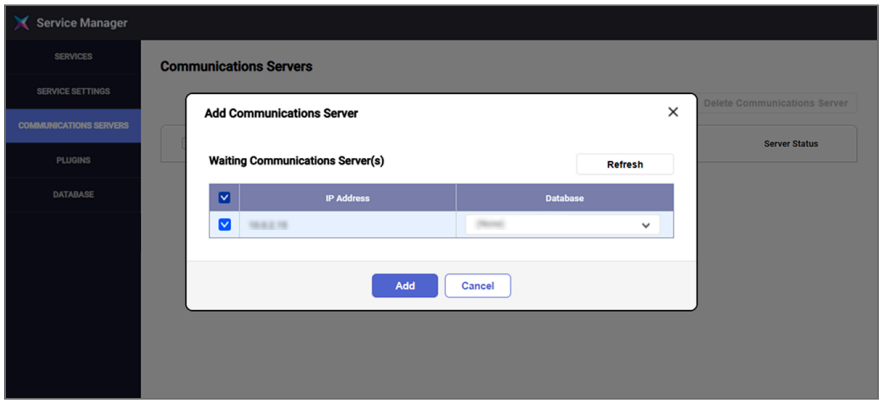
Verificaciones posteriores a la instalación

Después de instalar el servidor de comunicaciones múltiples, conéctelo al servidor principal en **BioStar X Service Manager**.

1. Haz clic en Inicio → **BioStar X** → **BioStar X Service Manager** en Windows.
2. La ventana **BioStar X Service Manager** aparece.
3. En la barra lateral izquierda, haga clic en el menú **COMMUNICATIONS**.

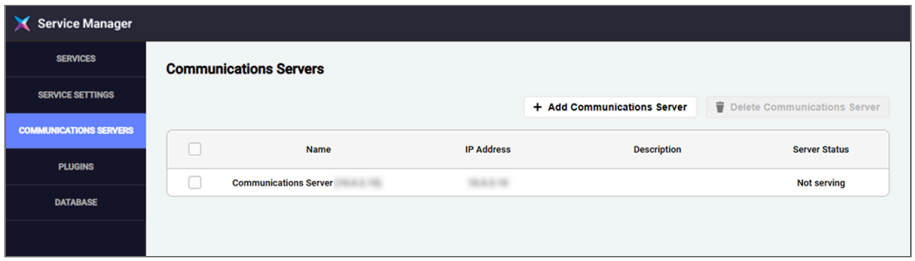


4. Haga clic en **Add Communication Server** en la esquina superior derecha de la pantalla.
5. Cuando aparezca la ventana **Add Communication Server**, marque la casilla que coincida con la dirección IP del servidor de comunicaciones múltiples instalado. En la columna **Database**, seleccione la base de datos que se usará.



6. Haga clic en el botón **Add**.

En la lista del servidor de comunicaciones múltiples, compruebe que **Server Status** muestre **Connected**.



Información

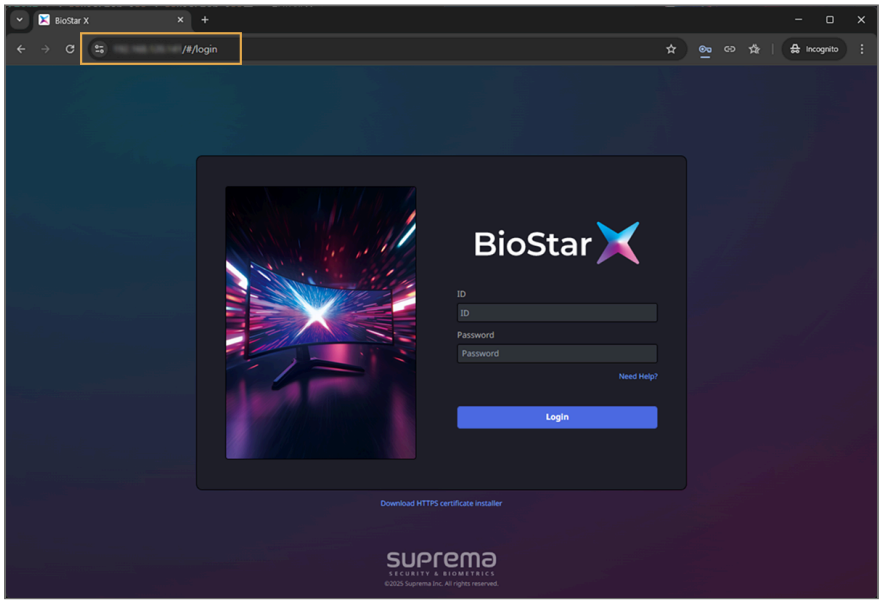
- El menú **COMMUNICATIONS** puede usarse cuando la licencia de multi-servidor de comunicación está activada. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.
- Para eliminar el servidor de comunicaciones múltiples, marque la casilla del servidor en la lista y haga clic en **Delete Communication Server** en la esquina superior derecha de la pantalla.
- Al agregar un servidor de comunicaciones múltiples, agregue una base de datos secundaria para reducir la carga en el servidor principal. Para obtener más información sobre cómo agregar una base de datos secundaria, consulte Agregar Base de Datos Auxiliar.

Cómo Iniciar Sesión

Si completaste la instalación de **BioStar X** mediante el paquete de instalación, accede desde un navegador web para comprobar que funciona correctamente. **BioStar X** ofrece un servicio basado en la web que permite el acceso en cualquier momento y lugar.

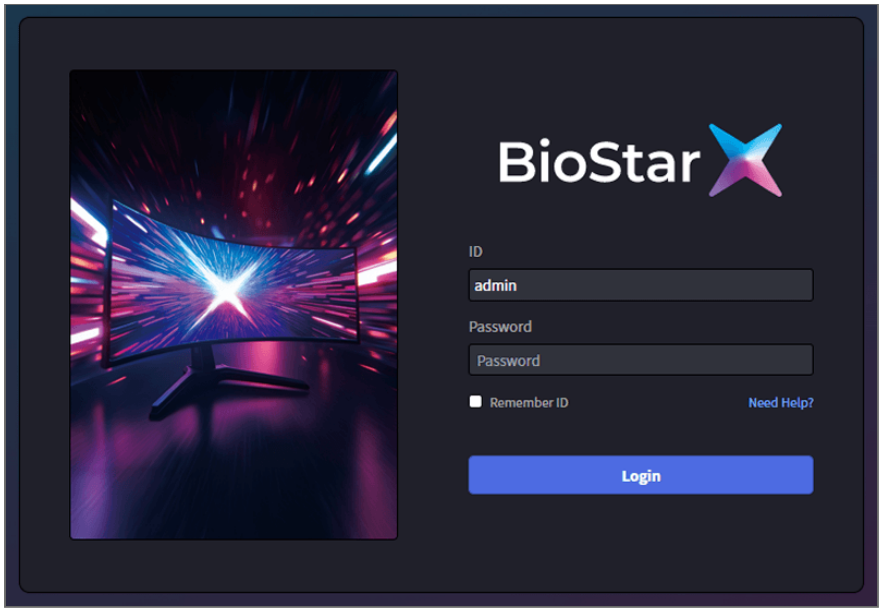
Iniciar sesión desde un navegador web

1. Haz clic en Inicio → **BioStar X** → **BioStar X** en Windows.
2. Conéctate a **BioStar X** a través de un navegador web.



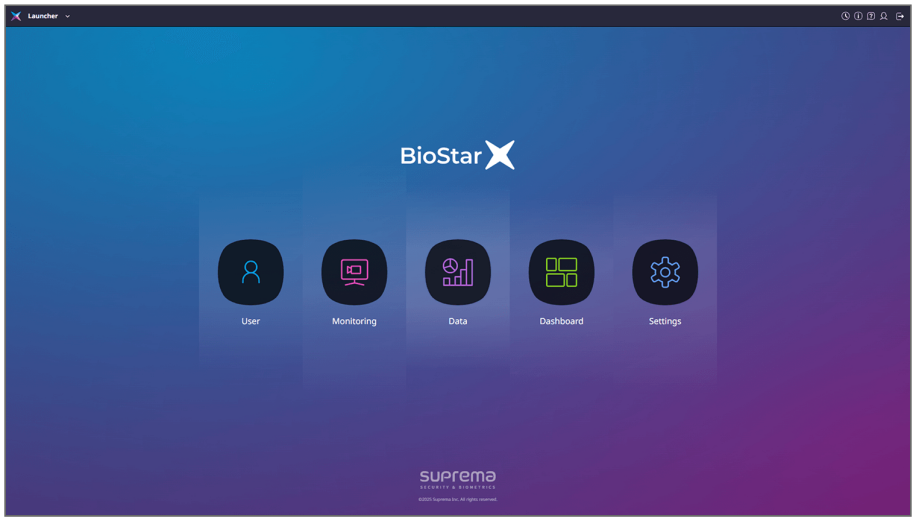
- Verifica la dirección de acceso de **BioStar X** en la barra de direcciones del navegador web.
- Si instalaste **BioStar X** en otra PC, ingresa la dirección IP de esa PC. p. ej. https://192.168.0.1
- No uses "localhost" como la dirección de acceso de **BioStar X**.
- **BioStar X** procesa todas las solicitudes a través del Unified Gateway. Por lo tanto, el acceso web y las llamadas de API se realizan a través del puerto de Unified Gateway (443 por defecto).

3. Cuando aparezca la pantalla de inicio de sesión, inicia sesión con la cuenta de administrador.



- El ID de administrador es **admin**.
- Si ves la advertencia **Not Secure** en la barra de direcciones del navegador web, debes instalar el certificado HTTPS. Para obtener más información sobre cómo instalar un certificado, consulta Instalar Certificado HTTPS.

Después de iniciar sesión, aparece la pantalla **Launcher**.



Información

- Se recomienda utilizar Chrome versión 100 o superior.
- Consulta la dirección IP externa de la PC donde está instalado **BioStar X** visitando este enlace.
- **BioStar X** utiliza el **puerto 443** por defecto. Si existe un programa que use el **puerto 443**, ciérralo y vuelve a intentar la conexión. Si no puedes cerrar el programa, ejecuta **BioStar X Service Manager** para cambiar el número de puerto. Para obtener más información, consulta Cambiar el Puerto.

Registrar Clave de Licencia

Si adquiriste la licencia de BioStar X, registra la clave de licencia para usar más funciones.

Ve a **Settings** → **License** → **BioStar X License**.

El método para activar **BioStar X License** varía según el entorno de red. Verifique el estado de la red y active la licencia según las instrucciones proporcionadas.

Información

- Ciertas características como añadir usuarios, puertas y puertos están restringidos cuando la licencia no está registrada.
- Para obtener más información sobre el menú **License**, consulte Activar Licencia.
- Para obtener más información sobre la política de licencias, consulte Política de Licencias.
- Para obtener información sobre los códigos de error de licencias, consulta el siguiente enlace.

Registrar en línea

Información

La clave de licencia acepta solo números y guiones (`-`). Ingrese hasta 16 dígitos en el formato `1111-1111-1111-1111`.

Registrar una sola licencia

Ingrese su nombre y la clave de licencia recibida y, a continuación, haga clic en **Activate** para activar la licencia de **BioStar X** mientras está en línea con una conexión a Internet.



Registrar varias licencias

Agregue hasta 30 licencias a la vez. Haga clic en el botón + **Add More License**. Después de ingresar todas las licencias, haga clic en **Activate**.



- Cuando la cantidad de campos llegue a 30, el botón + **Add More License** se desactiva. No puede agregar más licencias.
- Pegue varias claves de licencia en los campos a la vez. El sistema detecta solo las claves con el formato `1111-1111-1111-1111` y las divide en cada campo.
- Si las claves pegadas superan 30, el sistema ingresa automáticamente solo las primeras 30. El sistema ignora las claves adicionales.

Progreso de activación

Haga clic en **Activate** para abrir la ventana emergente de progreso. No cierre la página ni la ventana emergente hasta que finalice la activación.

Registrar sin conexión

Siga las instrucciones a continuación para activar la licencia de **BioStar X** en un entorno de red cerrado o en un estado sin conexión con acceso limitado a Internet.

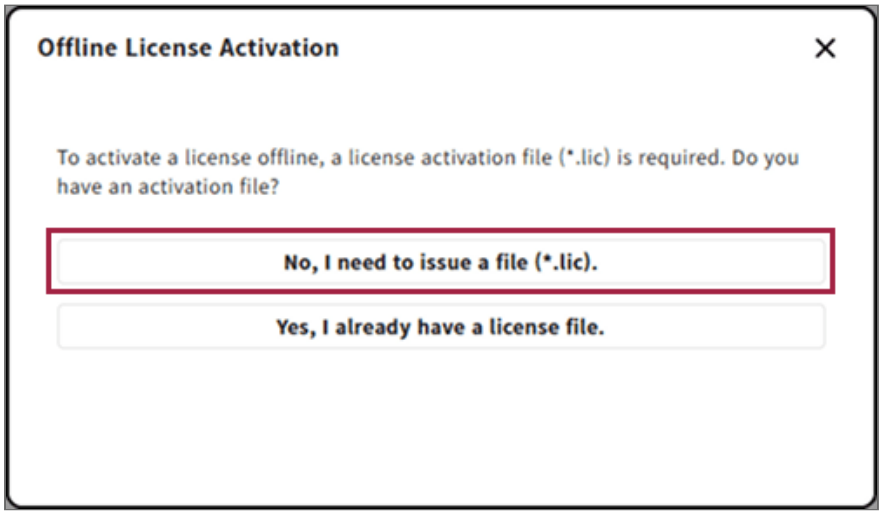
1. Ingrese cualquier nombre del administrador de inscripción y la clave de licencia en la sección **License Activation**.

   - La clave de licencia acepta solo números y guiones (`-`). Ingrese hasta 16 dígitos en el formato `1111-1111-1111-1111`.
   - Guarde o anote el nombre de administrador y la clave de licencia.
   - Si necesita varias licencias, haga clic en el botón + **Add More License** para agregarlas.

2. Haga clic en **Offline Activation**.

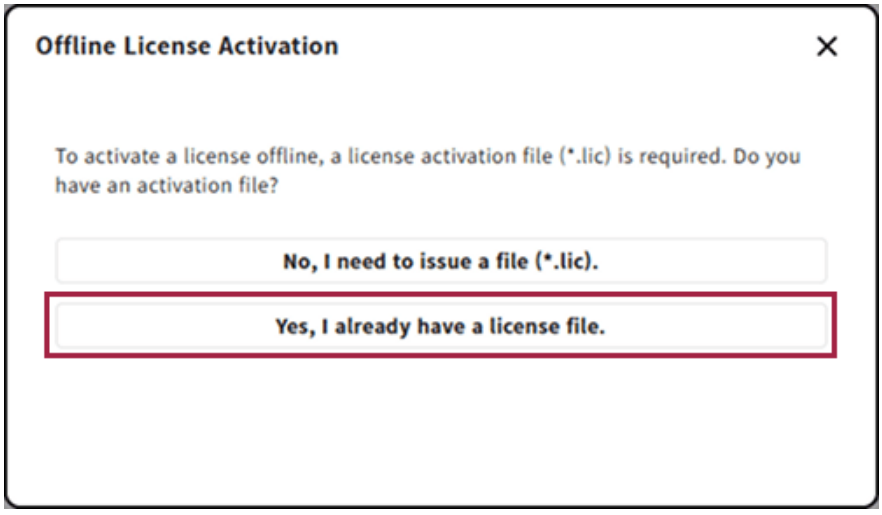


3. Cuando aparezca la ventana **Activate License Offline**, haga clic en **No, I need to issue a file (*.lic).**.



> Si tiene un archivo de licencia emitido, haga clic en **Yes, I already have a license file.** en esta pantalla y luego vaya al paso 9.

4. Cuando el sistema cree el archivo de solicitud de licencia (*.req), descárguelo en el disco local.
5. Envíe el archivo de solicitud descargado al revendedor y solicite un archivo de activación sin conexión (*.lic).
6. Tras recibir el archivo sin conexión, escriba el nombre de administrador y la clave del paso 1 en la sección **License Activation**.
7. Haga clic en **Offline Activation**.
8. Cuando aparezca la ventana **Activate License Offline**, haga clic en **Yes, I already have a license file.**.



9. Cuando aparezca la ventana Abrir archivo, seleccione el archivo de activación sin conexión (*.lic) o el comprimido (*.zip) almacenado localmente.

> Si solicita varias licencias, recibirá un archivo comprimido.

10. Aparece una ventana emergente con el estado del progreso. No cierre la página ni la ventana emergente hasta que finalice la activación.

Guía de Configuración Inicial

Se proporcionan configuraciones paso a paso para garantizar el funcionamiento adecuado de **BioStar X** después de la instalación inicial. Sigue cada paso secuencialmente para crear un entorno de control de acceso eficiente.

1 Registrar dispositivo

Registra un dispositivo para conectarlo a **BioStar X**. Configura modos de autenticación independientes según los dispositivos u asigna administradores a cada dispositivo.

Además, establece acciones según diversos eventos generados por el dispositivo (como fallas de autenticación, autenticación de huella digital bajo coacción, infracciones de anti-passback, etc.).

- Gestionar Grupos de Dispositivos
- Registrar dispositivo
- Registrar Credenciales Wiegand
- Registrar Esclavo
- Configuración del Dispositivo

> **Información**
> Obtenga una licencia **Device Manager** o superior para registrar dispositivos. Para obtener más información sobre la política de licencias, consulte Política de Licencias.

2 Registro y configuración de puertas

Registra la información de las puertas donde están instalados los dispositivos. Configura el relé, anti-passback, autenticación dual, alarmas y más.

- Administrar Grupo de Puertas
- Registrar Puerta

3 Configuración de niveles de acceso

Los niveles de acceso se crean combinando la información de puertas y horarios, lo que permite registrar varias puertas y horarios en un solo nivel de acceso.

Administrar Niveles de Acceso

4 Configuración de grupos de acceso

Los grupos de acceso se crean combinando niveles de acceso (puertas, horarios) e información de usuarios, lo que permite registrar múltiples niveles de acceso y usuarios en un solo grupo de acceso.

Administrar Grupos de Acceso

5 Registrar usuarios

Registra información como datos de usuarios y credenciales para usar en el control de acceso. La información de usuarios puede registrarse directamente en el dispositivo o en **BioStar X**. Además, la información de usuarios registrada en el dispositivo puede importarse a **BioStar X**, o la información registrada en **BioStar X** puede enviarse al dispositivo.

- Administrar Grupos de Usuarios
- Administrar Usuarios
- Registrar usuarios
- Registrar Credencial del Usuario

6 Configuración avanzada de control de acceso

Configura anti-passback y alarma de incendio, con opciones para ajustes locales y globales.

- Configuración Avanzada de Control de Acceso
- Monitorear Mapa

> **Información**
> Requiere una licencia **Esencial** o superior. Para obtener más información sobre la política de licencias, consulte Política de Licencias.

7 Monitorizar

Administra el sistema de control de acceso en tiempo real mediante diversas funciones de monitoreo como puertas, dispositivos y eventos.

- Monitorear Puertas
- Monitorear Dispositivo
- Supervisar Evento

Administración de Servidores

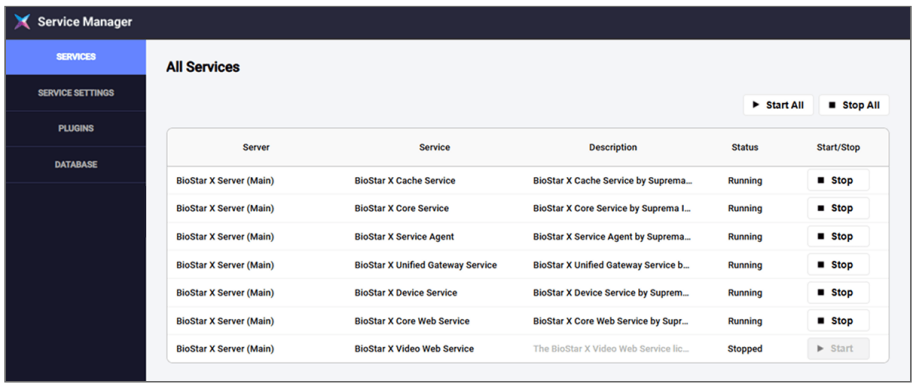
Después de instalar BioStar X, los usuarios pueden operar el sistema de forma eficiente mediante varias funciones de administración del servidor. Este documento le guía sobre las funciones de administración del servidor de BioStar X.

Iniciar y Detener el Servidor

Consulta cómo administrar los servicios del servidor BioStar X mediante **BioStar X Service Manager**. Inicia o detén servicios individuales.

Administrador de servicios de BioStar X

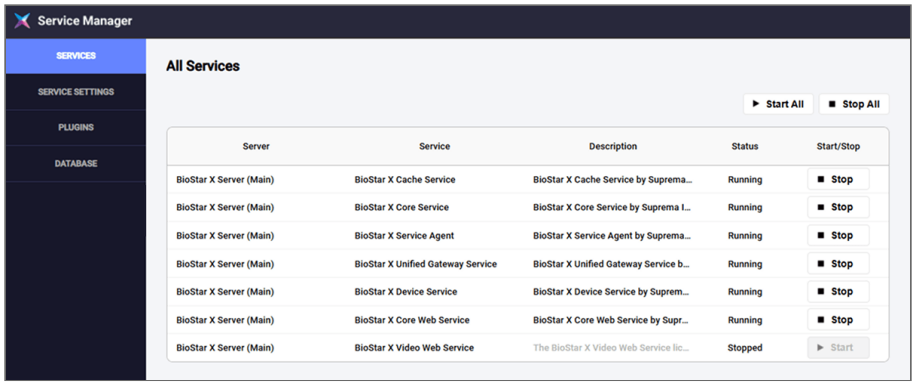
Proporciona una herramienta para administrar el estado del servidor **BioStar X**. Haz clic en Inicio → **BioStar X** → **BioStar X Service Manager** en Windows. La ventana **BioStar X Service Manager** aparece.



> **Información**
>
> Si no se reinicia, **BioStar X** podría no funcionar correctamente. Si cambiaste la configuración de hora del servidor **BioStar X**, detén y reinicia **BioStar X Core Service**.

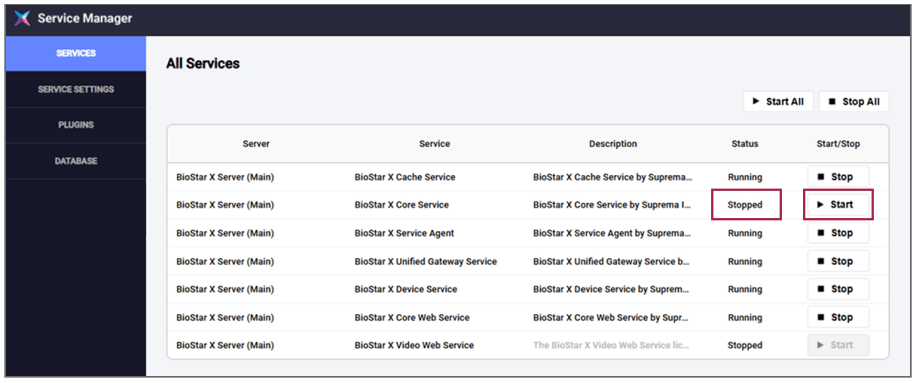
Detener servicio

Haz clic en el botón **Stop** de los servicios individuales en el menú **SERVICES** para apagar **BioStar X**. Para detener todos los servicios, haga clic en el botón **Stop All** en la esquina superior derecha de la pantalla.



Iniciar el servidor

Haz clic en **Start** del servicio en el menú **SERVICES** con estado **Stopped** en la columna **Status** para reiniciar **BioStar X**. Haga clic en el botón **Start All** en la esquina superior derecha para reiniciar todos los servicios.



Configuración del Servicio

Configure y gestione los servicios centrales del sistema en el menú **Service Settings** de **BioStar X Service Manager**. Configure cada servicio de forma independiente y verifique los puertos de red y la información de versión.

La **Service Settings** incluye los siguientes servicios principales.

- **BioStar X Core Web Service**: Servicio de interfaz web
- **BioStar X Core Service**: Funcionalidades centrales del sistema y servicio de comunicación API
- **Unified Gateway Service**: Servicio de puerta de enlace integrada basado en proxy inverso
- **BioStar X Coordinator Service**: Administración de la información de configuración del sistema distribuido y sincronización de servicios
- **BioStar X Server (Main)**: Servicio de servidor principal
- **BioStar X Cache Service**: Almacenamiento en caché de datos y mejora del rendimiento del sistema

Situaciones que requieren cambiar la configuración

Cambie la configuración del servicio en las siguientes situaciones.

- **Resolver conflictos de puertos**: cuando otra aplicación utiliza el mismo puerto y provoca conflictos
- **Cumplimiento de políticas de seguridad**: cuando la política de seguridad de la red de la organización solo permite puertos específicos
- **Configuración del firewall**: cuando sea necesario cambiar a puertos permitidos por el firewall corporativo
- **Cambios en el entorno del servidor**: al cambiar la dirección IP del servidor o la configuración de red
- **Optimización del rendimiento**: cuando se necesita separar puertos para distribuir el tráfico o equilibrar la carga

Cómo cambiar la configuración

1. Haga clic en el menú **SERVICE SETTINGS** en **BioStar X Service Manager**.

2. Vaya a la sección del servicio que desea cambiar.
3. Modifique el número de puerto o la dirección necesarios.
4. Para aplicar los cambios, haga clic en **Apply** en la esquina superior derecha de la pantalla.

- Reinicie el servicio correspondiente para aplicar los cambios tras modificar la configuración.
- La compatibilidad para cambiar el puerto varía según el servicio.

Precaución
Al cambiar los números de puerto, asegúrese de que no existan conflictos con otros servicios o aplicaciones.

Composición del servicio

BioStar X Core Web Service

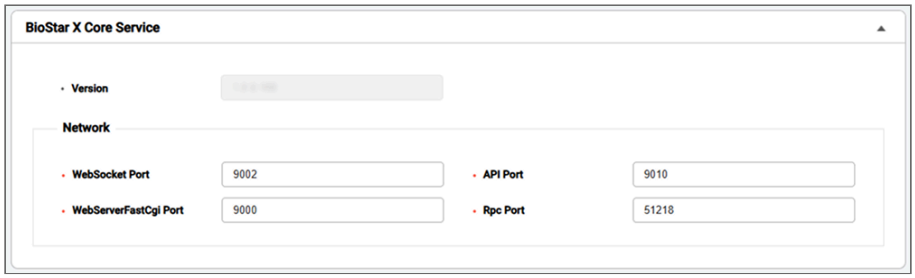
Este servicio es responsable de la interfaz de usuario basada en web.



- **HTTPS Port**: puerto de acceso a la interfaz web (predeterminado: 5002)
- **WebServerThrift Port**: puerto de comunicación del servidor web basado en el protocolo Thrift (predeterminado: 9310)

BioStar X Core Service

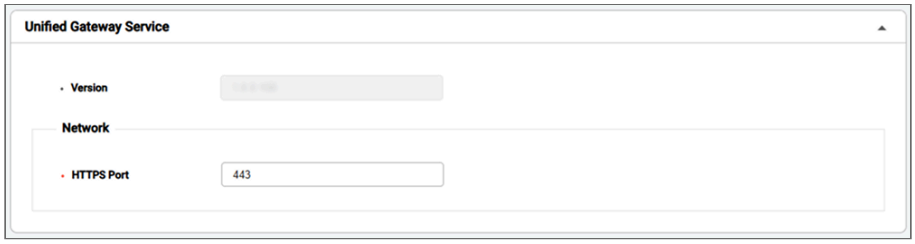
Este es el servicio principal que gestiona las funcionalidades centrales del sistema y las comunicaciones API externas.



- **WebSocket Port**: puerto WebSocket para comunicación bidireccional en tiempo real (predeterminado: 9002)
- **API Port**: puerto de comunicación de la API REST (predeterminado: 9010)
- **WebServerFastCgi Port**: puerto de comunicación del servidor web basado en protocolo FastCGI (predeterminado: 9000)
- **Rpc Port**: puerto de comunicación de llamada a procedimiento remoto (RPC) (predeterminado: 51218)

Unified Gateway Service

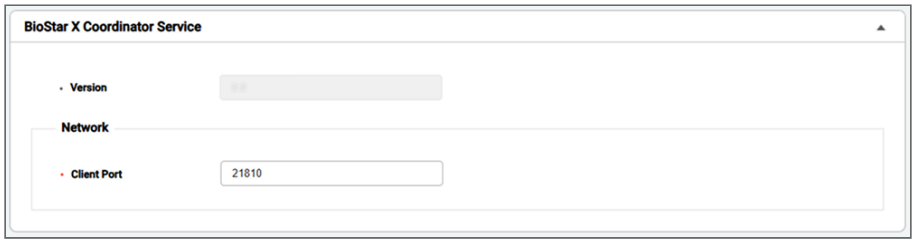
Procese eficientemente las solicitudes al servidor **BioStar X** mediante proxy inverso, mejore las vulnerabilidades de seguridad de los iframes y minimice los errores de certificado SSL.



- **HTTPS Port**: puerto de comunicación HTTPS de la puerta de enlace integrada (predeterminado: 443)

BioStar X Coordinator Service

Este servicio se encarga de administrar la información de configuración del sistema distribuido, supervisar el estado del servicio y sincronizar los servicios.

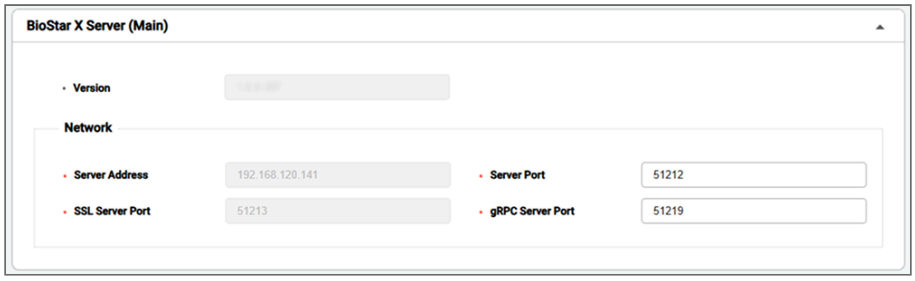


- **Client Port**: puerto de comunicación para conexiones de cliente (predeterminado: 21810)

> **Información**
>
> - Cambie el valor del **Client Port** y, luego, reinicie manualmente el **BioStar X Coordinator Service** en **Windows Services** (*services.msc*).
> - Después de reiniciar el **BioStar X Coordinator Service**, vaya a **BioStar X Service Manager** → **SERVICES** y reinicie todos los servicios.
>
> Haga clic en **Stop All** en la esquina superior derecha de la pantalla. Cuando todos los servicios estén detenidos y el botón **Start All** esté habilitado, haga clic en él.

BioStar X Server (Main)

Este es el servicio central que funciona como servidor principal del sistema.

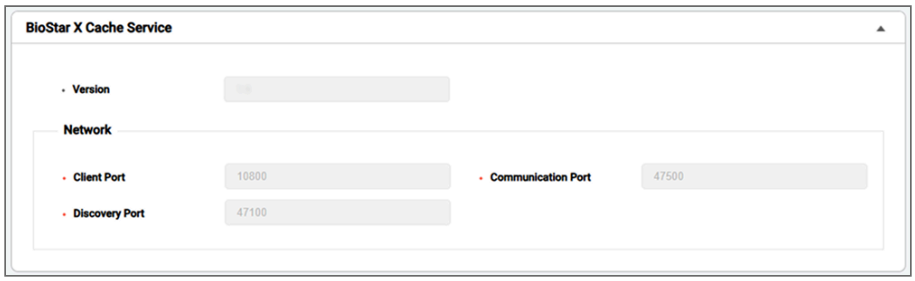


- **Server Address**: Dirección IP del servidor principal
- **Server Port**: puerto de comunicación general del servidor (predeterminado: 51212)

- **SSL Server Port**: puerto de comunicación segura cifrada SSL (predeterminado: 51213)
- **gRPC Server Port**: puerto de comunicación de alto rendimiento basado en el protocolo gRPC (predeterminado: 51219)

BioStar X Cache Service

Este servicio mejora la velocidad de procesamiento de datos y el rendimiento del sistema al almacenar en memoria los datos utilizados con frecuencia.



- **Client Port**: puerto de conexión de cliente del servicio de caché (predeterminado: 10800)
- **Communication Port**: puerto de comunicación interna entre nodos de caché (predeterminado: 47500)
- **Discovery Port**: puerto para el descubrimiento automático de nodos de caché distribuidos (predeterminado: 47100)

Siguiente paso

Aprenda paso a paso a cambiar el puerto predeterminado (443) de **BioStar X**.

Cambiar la dirección IP del servidor principal

Consulta este documento cuando cambie la red del servidor o debas cambiar la IP tras la configuración inicial. Esta guía explica cómo cambiar de forma segura la IP del servidor principal de **BioStar X**. También explica cómo reconfigurar el Servidor de comunicaciones múltiples conectado.

> **Información**
> La función de cambio de dirección IP del servidor principal es compatible con **BioStar X v1.0.2** y versiones posteriores.

Cambio de dirección IP

Primero, cambia la dirección IP en el servidor donde está instalado **BioStar X**. Cambia la dirección IP del adaptador de red conectado a la red externa.

> **Información**
> Para más información sobre cómo cambiar la dirección IP en Windows, consulta Microsoft Customer Support.

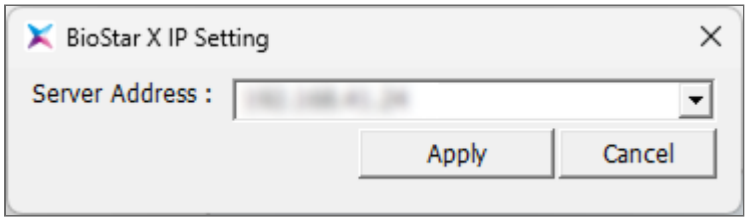
Aplicar la nueva dirección IP

Sigue los pasos siguientes para cambiar la dirección IP en el servidor donde está instalado **BioStar X**.

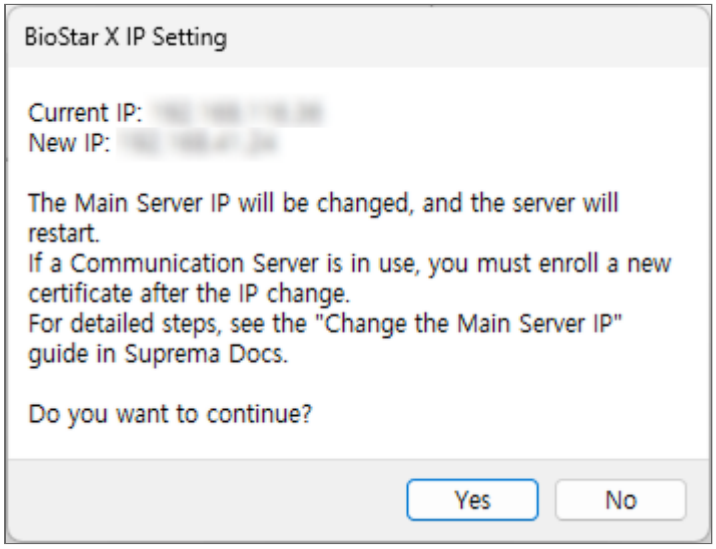
BioStar X IP Setting

Use la herramienta **BioStar X IP Setting** para cambiar la dirección IP.

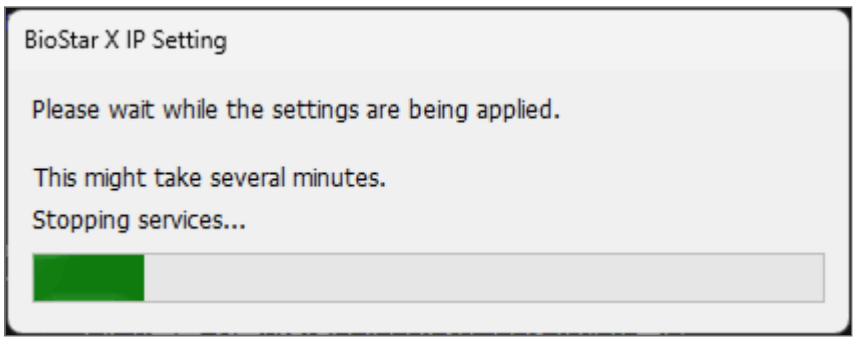
1. En Windows, haz clic en Inicio → **BioStar X** → **BioStar X IP Setting**.
2. Cuando aparezca la ventana **BioStar X IP Setting**, selecciona la dirección IP que deseas usar en **Server Address**.



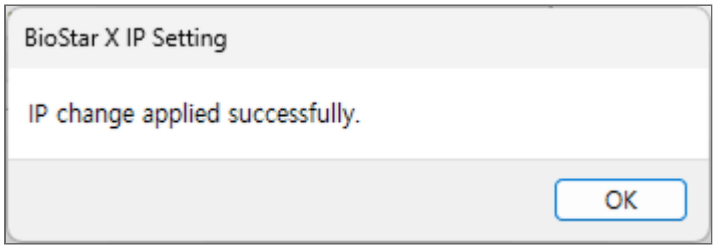
3. Haz clic en el botón **Apply**.
4. Si aparece un mensaje sobre el cambio de dirección IP, revísalo y haz clic en el botón **Yes**.



5. Espera hasta que finalice el proceso de cambio de dirección IP. Cuando se complete el proceso, aparecerá un mensaje de éxito.



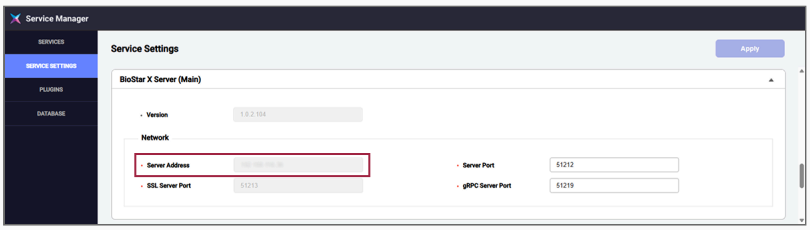
6. Si aparece el mensaje **IP change applied successfully**, haz clic en el botón **OK**.



Después de completar el cambio de dirección IP, reinicie todos los servicios.

Información

- La dirección IP no se puede introducir manualmente; selecciona una de las direcciones IP que figuran en **Server Address**.
- Puedes ver la nueva dirección IP en **BioStar X Service Manager** → **SERVICE SETTINGS** → **BioStar X Server (Main)**, en **Server Address**.



- Si un dispositivo está registrado en BioStar X con la opción **Device ▸ Server Connection**, el administrador debe actualizar manualmente la IP del servidor de ese dispositivo a la nueva dirección IP.

Modificar la configuración del servidor de base de datos

Si la base de datos está alojada en el mismo servidor que **BioStar X**, detenga todos los servicios y luego edite el archivo *system.conf* de **BioStar X**. Omita este paso si usa un servidor de base de datos externo.

1. Detenga todos los servicios relacionados con **BioStar X** en Servicios de Windows (service.msc).
2. Vaya a *C:\Program Files\BioStar X Server*.
3. Abra el archivo *system.conf* con un editor de texto como Notepad.
4. En la sección `database`, cambie el valor `server_ip` a la nueva dirección IP.
5. Guarde y cierre el archivo *system.conf*.
6. Reinicie todos los servicios relacionados con **BioStar X** en Servicios de Windows (service.msc).

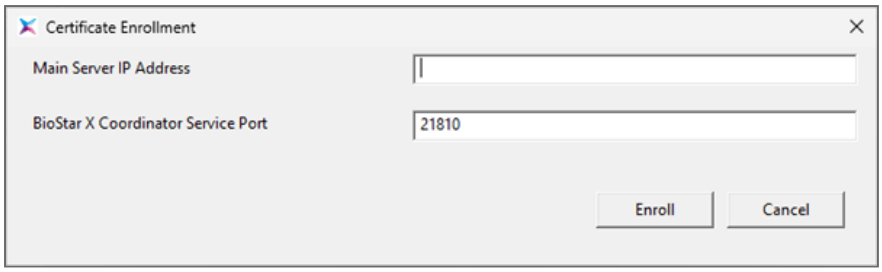
Abra un navegador web y verifique que puede acceder al servidor con la nueva dirección IP.

Actualizar Servidor de Multi Comunicaciones

Si instalaste un Servidor de comunicaciones múltiples adicional, actualiza sus ajustes para usar la nueva dirección IP del servidor principal. Ejecuta este paso en el servidor donde instalaste el Servidor de comunicaciones múltiples.

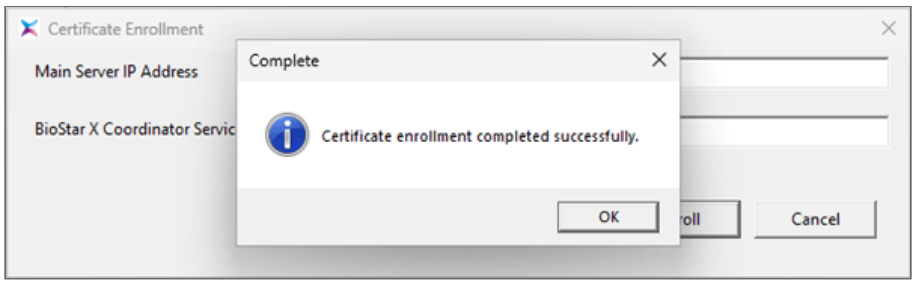
1. Ve a *C:\Program Files\BioStar X Communications Server*.
2. Ejecuta *biostar-device-cert-enroll.exe*.
3. Cuando aparezca la ventana **Certificate Enrollment**, introduce la nueva dirección IP del servidor principal en el campo

Main Server IP Address.



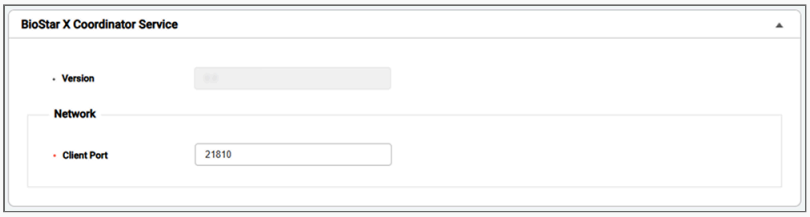
4. Si el número de puerto del servidor principal difiere del valor predeterminado (21810), introduce el nuevo número de puerto en el campo **BioStar X Coordinator Service Port**.
5. Haga clic en el botón **Enroll**.

Después de actualizar la dirección IP del servidor principal, se muestra un mensaje de confirmación.



Información

- Si no instalaste un Servidor de comunicaciones múltiples, omite este paso.
- Si cambió el número de puerto en el servidor principal donde está instalado BioStar X, ejecute **BioStar X Service Manager** y verifique el valor **Client Port** en **SERVICE SETTINGS** → **BioStar X Coordinator Service**.

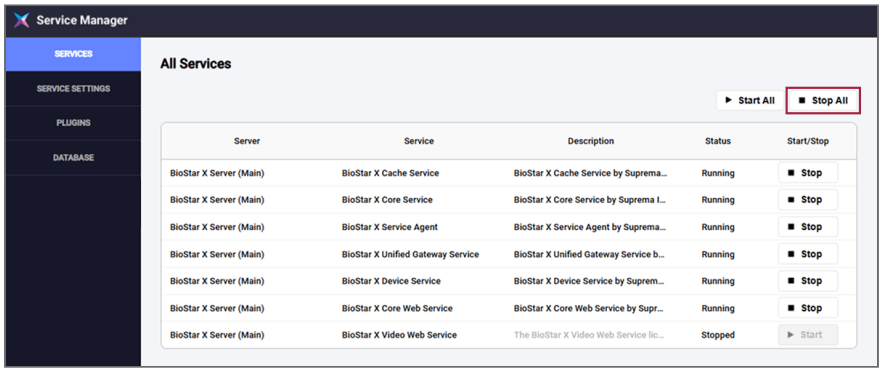


- Para más información sobre la instalación del Servidor de comunicaciones múltiples, consulta Instalar el Servidor de Comunicaciones Múltiples.

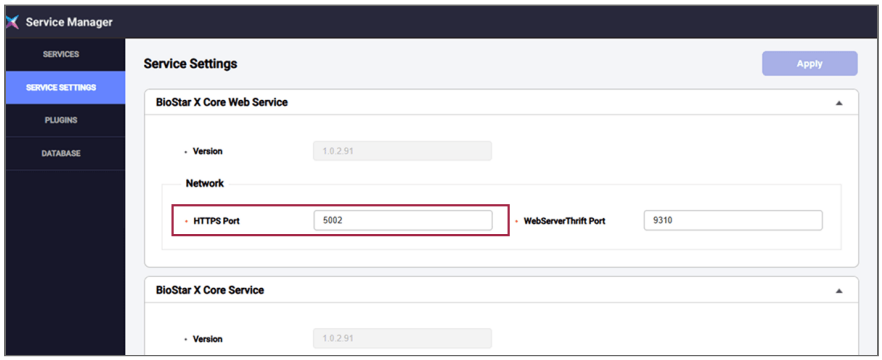
Cambiar el Puerto

Esta guía explica cómo cambiar el puerto cuando el puerto predeterminado (443) de **BioStar X** no está disponible.

1. Haz clic en Inicio → **BioStar X** → **BioStar X Service Manager** en Windows.
2. Cuando aparezca la ventana **BioStar X Service Manager** en el navegador web, haga clic en el menú **SERVICES**.
3. Para detener todos los servicios, haga clic en el botón **Stop All** en la esquina superior derecha de la pantalla.



4. Haga clic en **SERVICE SETTINGS** en la barra lateral izquierda.
5. Ingrese el número de puerto que desea cambiar en el campo de entrada **HTTPS Port** de la sección **Unified Gateway Service**.



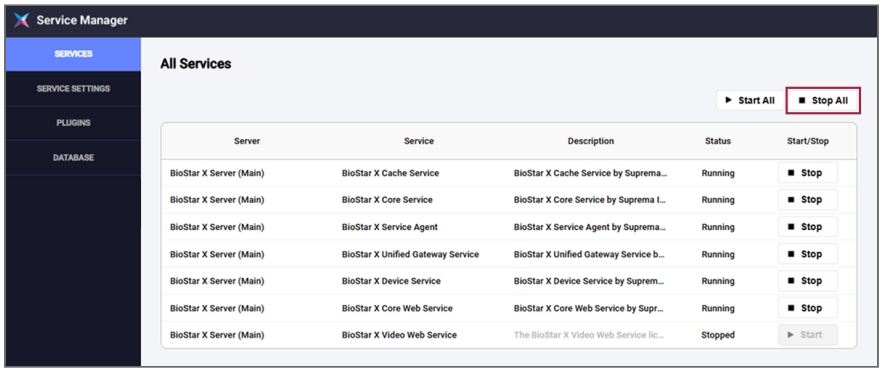
6. Haga clic en **Apply** en la esquina superior derecha de la pantalla.
7. Cuando aparezca el mensaje de confirmación, haga clic en **OK**.
8. Vaya a **SERVICES** y haga clic en **Start** para todos los servicios.
9. Acceda a **BioStar X** desde el navegador web.

> **Información**
>
> - Si cambió el número de puerto a 450, ingrese `https://{ip_address}:450` en la barra de direcciones.
> - La compatibilidad para cambiar el puerto varía según el servicio.

Cambiar la Base de Datos

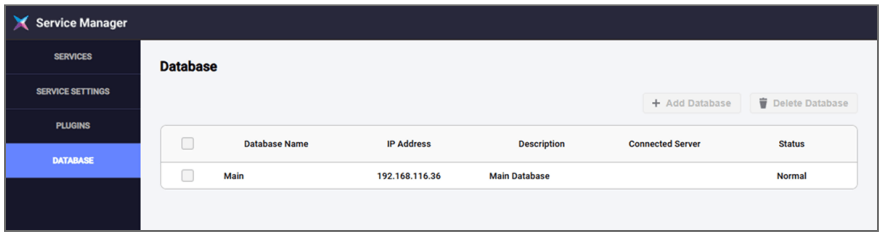
Cambie la configuración de la base de datos.

1. Haz clic en Inicio → **BioStar X** → **BioStar X Service Manager** en Windows.
2. Cuando aparezca la ventana **BioStar X Service Manager** en el navegador web, haga clic en el menú **SERVICES**.
3. Haga clic en **Stop** para todos los servicios.



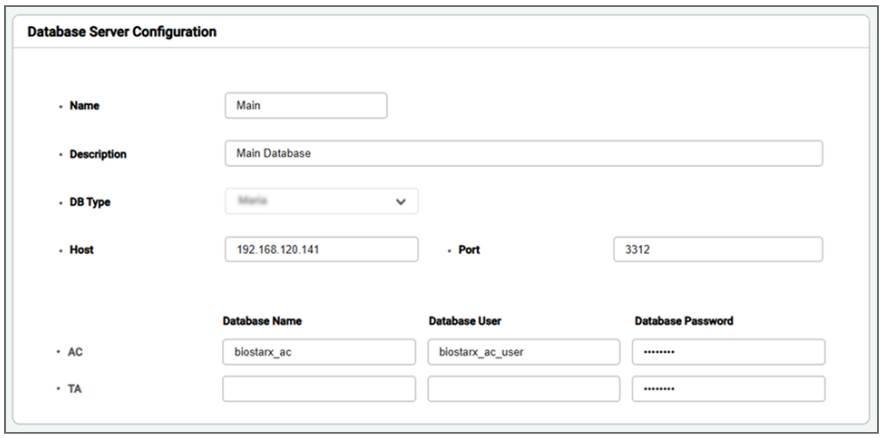
> Haga clic en **Stop All** para detener todos los servicios a la vez.

4. Haz clic en el menú **DATABASE** en la barra lateral izquierda.



5. Seleccione en la lista de bases de datos la base cuya configuración desea cambiar.

6. En la sección **Database Server Configuration**, cambie los siguientes ajustes:



- **Name**: Ingresa el nombre de la base de datos.
- **Description**: Ingresa la descripción de la base de datos.
- **DB Type**: Selecciona el tipo de base de datos. (MariaDB, MS SQL)
- **Host**: Ingresa el nombre de host o la dirección IP del servidor de bases de datos.
- **Port**: Ingresa el número de puerto del servidor de bases de datos.
- **AC** / **TA** / **Video**: Ingrese el nombre, el usuario y la contraseña de las bases de datos AC, TA y Video.

7. Haz clic en el botón **Test Connection** en la esquina superior derecha para comprobar si la base de datos está correctamente conectada.

8. Haz clic en **Save** en la parte superior derecha de la pantalla para guardar la configuración.

Agregar Base de Datos Auxiliar

Al agregar un servidor de comunicaciones múltiples, agrega y conecta una base de datos auxiliar. Esto reduce la carga en el servidor principal.

> **Información**
>
> - Necesitas una licencia de **servidor de comunicación múltiple** para agregar una base de datos auxiliar. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.
> - Para más información sobre la instalación del Servidor de comunicaciones múltiples, consulta Instalar el Servidor de Comunicaciones Múltiples.

Antes de comenzar

Si usas un dominio o nombre de host en lugar de una dirección IP para la comunicación entre bases de datos en un entorno MariaDB, asegúrate de revisar la siguiente guía.

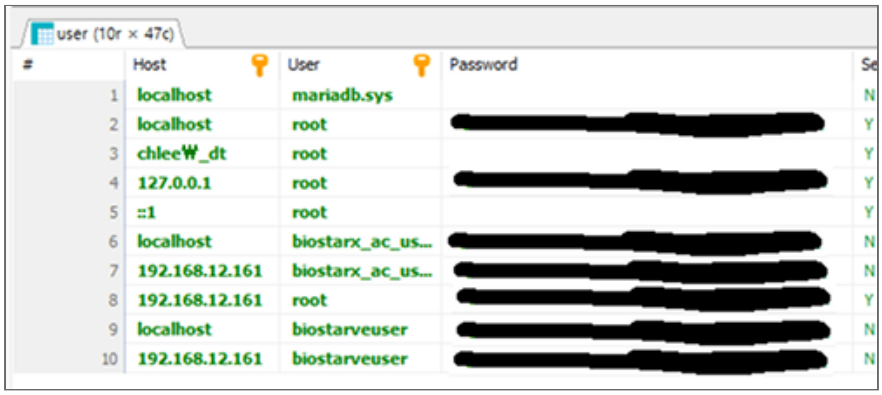
- Si no utilizas una dirección IP, puede que no sea posible ejecutar `Create user` o `Grant`.
- Si la comunicación se realiza mediante un dominio o nombre de host, asegura que el usuario y los permisos estén registrados para localhost.
- Si instalaste BioStar X mediante el método de instalación conveniente, la cuenta root está registrada solo para localhost, por lo que debes agregar la dirección IP del servidor o *127.0.0.1*.

Método de registro

Verifica si hay una contraseña establecida para la cuenta con Host *127.0.0.1* y Usuario root; si no existe, establece una contraseña y otorga permisos.

1. Verifica si hay una contraseña establecida para la cuenta con Host *127.0.0.1* y Usuario root.

```
SELECT * FROM mysql.user;
```



   Si está en blanco, la contraseña no está establecida; ejecuta la consulta en los siguientes elementos para agregar una contraseña y otorgar permisos.

2. Establece una contraseña y otorga permisos para la cuenta con Host *127.0.0.1* y Usuario root.

```
ALTER USER 'root'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO 'root'@'127.0.0.1';

CREATE USER '<Main DB AC User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB AC User>'@'127.0.0.1';
CREATE USER '<Main DB AC User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB AC User>'@'::1';

CREATE USER '<Main DB TA User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB TA User>'@'127.0.0.1';
CREATE USER '<Main DB TA User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB TA User>'@'::1';

CREATE USER '<Main DB VE User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB VE User>'@'127.0.0.1';
CREATE USER '<Main DB VE User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB VE User>'@'::1';

FLUSH PRIVILEGES;
```

Example

```
ALTER USER 'root'@'127.0.0.1' IDENTIFIED BY 'admin1234!';
GRANT ALL PRIVILEGES ON *.* TO 'root'@'127.0.0.1';
FLUSH PRIVILEGES;
```

Configuración de comunicación mediante dirección IP

Las siguientes configuraciones pueden forzar la comunicación mediante dirección IP.

1. Después de instalar **BioStar X**, dirígete a la siguiente ruta.

   > *C:\Program Files\BioStar X\ta\mariadb-11.4.4-winx64*

2. Abre el archivo *my.cnf* con permisos de propietario y agrega la opción `skip-name-resolve` a la sección [mysqld].

```
[mysqld]
port = 3312
character-set-server=utf8
collation-server=utf8_unicode_ci
socket = /tmp/mysql.sock
skip-external-locking
key_buffer_size = 32M
max_allowed_packet = 64M
...
skip-name-resolve
```

3. Reinicia el servicio de MariaDB.

Agregar base de datos auxiliar

Esta sección brinda orientación sobre cómo agregar una base de datos auxiliar. Según el tipo de base de datos que se utilice, existen dos métodos: MariaDB y SQL Server.

MariaDB

1 Base de datos principal

Otorga la cuenta y los permisos para acceder a la base de datos principal desde la nueva base de datos auxiliar.

```
CREATE USER '<Main DB AC Schema User>'@'<Sub DB IP>' IDENTIFIED BY '<Main DB AC Schema Password>';

GRANT ALL PRIVILEGES ON <Main DB AC Schema>.* TO '<Main DB AC Schema User>'@'<Sub DB IP>';
FLUSH PRIVILEGES;
```

Example

```
CREATE USER 'biostarx_ac_user'@'192.168.12.42' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON biostar2_ac.* TO 'biostarx_ac_user'@'192.168.12.42';
FLUSH PRIVILEGES;
```

2 Base de datos auxiliar

Otorga la cuenta y los permisos para acceder a la nueva base de datos auxiliar desde la base de datos principal.

```
CREATE USER '<Sub DB AC Schema User>'@'<Main DB IP>' IDENTIFIED BY '<Sub DB AC Schema Password>';

GRANT ALL PRIVILEGES ON <Sub DB AC Schema>.* TO '<Sub DB AC Schema User>'@'<Main DB IP>';
FLUSH PRIVILEGES;
```

Example

```
CREATE USER 'biostarx_ac_user'@'192.168.12.161' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON biostar2_ac.* TO 'biostarx_ac_user'@'192.168.12.161';
FLUSH PRIVILEGES;
```

3 Verificar el uso de FederatedX

Ejecuta el siguiente comando tanto en la base de datos principal como en la auxiliar para verificar si el motor de almacenamiento FederatedX está habilitado.

```
SHOW ENGINES;
```

Si el resultado de la consulta muestra `Engine : FEDERATED, Support : YES`, ya está instalado. Si el motor de almacenamiento FederatedX no está instalado, ejecuta la siguiente consulta.

```
INSTALL PLUGIN federated SONAME 'ha_federatedx';
```

> **Información**
> Verifica si el archivo *ha_federatedx.dll* existe en la carpeta *lib/plugin* en la ruta donde está instalada MariaDB. Normalmente, el archivo dll se encuentra en la ruta *C:\Program Files\MariaDB {version}\lib\plugin*.

4 Registrar alias de servidor

Registra un alias de servidor para que la tabla federatedX creada en la base de datos auxiliar pueda acceder a la tabla origen en la base de datos principal.

```
CREATE SERVER 'default' FOREIGN DATA WRAPPER mysql OPTIONS (HOST '<Main DB IP>', PORT <Main DB PORT>, DATABASE '<Main DB AC Schema>', USER '<Main DB AC USER>', PASSWORD '<Main DB AC USER Password>');

-- Confirm registration
SELECT * FROM mysql.servers;
```

Si necesitas cambiar la información de Host, Puerto, BD, Usuario o Contraseña del nombre de servidor registrado, puedes modificarla usando la instrucción `Alter`. También puedes cambiar solo cierta información.

```
ALTER SERVER 'default' OPTIONS (HOST '<Main DB IP>', PORT <Main DB PORT>, DATABASE '<Main DB AC Schema>', USER '<Main DB AC USER>', PASSWORD '<Main DB AC USER Password>');
```

Example

```
CREATE SERVER 'default' FOREIGN DATA WRAPPER mysql OPTIONS (HOST '192.168.12.161', PORT 3312, DATABASE 'biostar2_ac', USER 'biostarx_ac_user', PASSWORD 'password');

ALTER SERVER 'default' OPTIONS (HOST '192.168.12.161', PORT 3312, DATABASE 'biostar2_ac', USER 'biostarx_ac_usermt__fttid__', PASSWORD 'password');
```

5 Configuración de enlace de tablas

Sigue los pasos a continuación para enlazar las tablas necesarias en la base de datos auxiliar con las tablas en la base de datos principal.

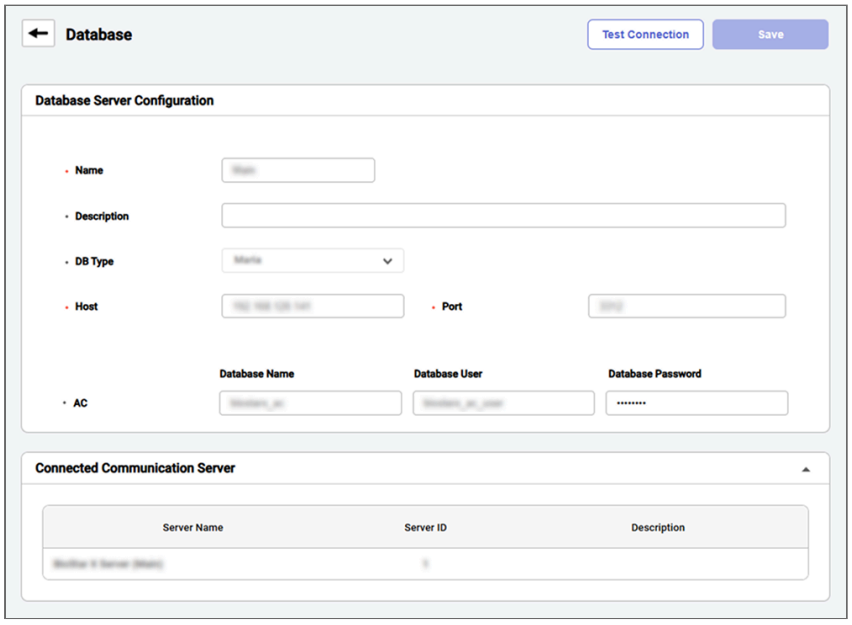
- A continuación se muestra la consulta para generar sentencias `CREATE TABLE` en la base de datos principal.

```
select
  concat(
     'CREATE TABLE IF NOT EXISTS <SubDB_AC_Database_Schema>.', table_name,
     ' ENGINE=FEDERATED ',
     'CONNECTION="default/', table_name, '";'
  ) as create_table_sql
from information_schema.TABLES
where TABLE_SCHEMA = '<MainDB_AC_Database_Schema>'
   AND TABLE_TYPE = 'BASE TABLE'
   AND NOT TABLE_NAME REGEXP '^t_lg[0-9]{6}$'
   AND NOT TABLE_NAME REGEXP '^t_almevt[0-9]{6}$'
   AND NOT TABLE_NAME REGEXP '^t_lgalmtrstrc[0-9]{6}$'
ORDER BY TABLE_NAME;
```

> **Información**
>
> Debido a la naturaleza de FederatedX, se recomienda establecer `Table_type` en 'BASE TABLE'. El `VIEW type` también es posible, pero no recomendado.

6 Configuración de Service Manager

1. Ejecuta **BioStar X Service Manager**. (Inicio → **BioStar X** → **BioStar X Service Manager**)
2. Haz clic en el menú **DATABASE** en la barra lateral izquierda.
3. Haz clic en **+ Add Database** en la esquina superior derecha de la pantalla.
4. Ingresa cada elemento en la pantalla de adición de base de datos.



- **Name**: Ingresa el nombre de la base de datos.
- **Description**: Ingresa la descripción de la base de datos.
- **DB Type**: Selecciona el tipo de base de datos. (Maria, MS SQL)

- **Host**: Ingresa el nombre de host o la dirección IP del servidor de bases de datos.
- **Port**: Ingresa el número de puerto del servidor de bases de datos.
- **AC** / **TA**: Ingresa el nombre, usuario y contraseña de las bases de datos AC y TA.

5. Haz clic en el botón **Test Connection** en la esquina superior derecha para comprobar si la base de datos está correctamente conectada.
6. Haz clic en **Save** en la parte superior derecha de la pantalla para guardar la configuración.

SQL Server

1 Otorgar permisos para la base de datos principal

Concede los siguientes permisos en la base de datos principal con una cuenta que tenga privilegios de sysadmin.

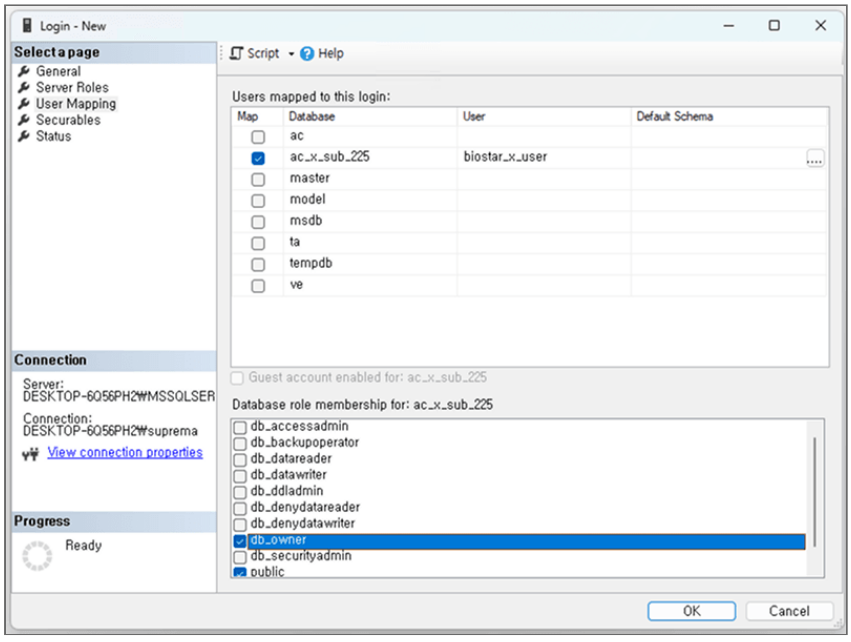
```
GRANT ALTER ANY LINKED SERVER TO [<MAIN DATABASE AC USER>];
GRANT ALTER ANY LOGIN TO [<MAIN DATABASE AC USER>];
```

Example

```
GRANT ALTER ANY LINKED SERVER TO [biostar_x_user];
GRANT ALTER ANY LOGIN TO [biostar_x_user];
```

2 Otorgar permisos para la base de datos auxiliar

1. Conecta User Mapping para las tablas y usuarios en la base de datos auxiliar con una cuenta que tenga privilegios de sysadmin. En este momento, es necesario agregar el rol `db_owner`.



2. Otorga los siguientes permisos a la base de datos que se va a agregar.

```
GRANT ALTER ANY LINKED SERVER TO [<SUB DATABASE AC USER>];
GRANT ALTER ANY LOGIN TO [<SUB DATABASE AC USER>];
```

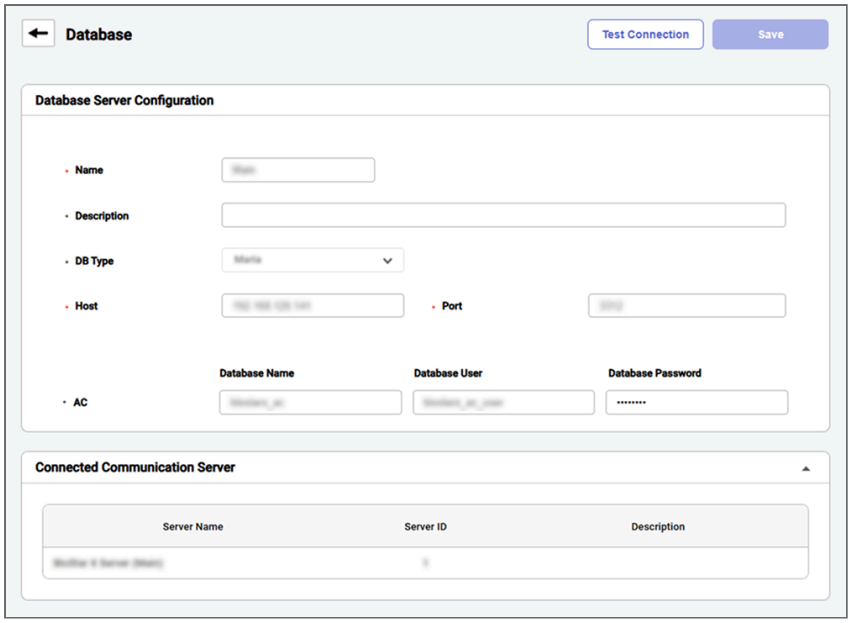
Example

```
GRANT ALTER ANY LINKED SERVER TO [biostar_x_user_sub];
GRANT ALTER ANY LOGIN TO [biostar_x_user_sub];
```

3 Configuración de Service Manager

Usa **BioStar X Service Manager** para agregar la base de datos auxiliar.

1. Ejecuta **BioStar X Service Manager**. (Inicio → **BioStar X** → **BioStar X Service Manager**)
2. Haz clic en el menú **DATABASE** en la barra lateral izquierda.
3. Haz clic en **+ Add Database** en la esquina superior derecha de la pantalla.
4. Ingresa cada elemento en la pantalla de adición de base de datos.



- **Name**: Ingresa el nombre de la base de datos.
- **Description**: Ingresa la descripción de la base de datos.
- **DB Type**: Selecciona el tipo de base de datos. (Maria, MS SQL)
- **Host**: Ingresa el nombre de host o la dirección IP del servidor de bases de datos.
- **Port**: Ingresa el número de puerto del servidor de bases de datos.
- **AC** / **TA**: Ingresa el nombre, usuario y contraseña de las bases de datos AC y TA.

5. Haz clic en el botón **Test Connection** en la esquina superior derecha para comprobar si la base de datos está correctamente conectada.

6. Haz clic en **Save** en la parte superior derecha de la pantalla para guardar la configuración.

> **Información**
>
> - Después de completar la configuración, los ajustes de Linked Server para ambas bases de datos, principal y auxiliar, se aplicarán automáticamente.
> - Incluso al modificar la información de la base de datos, los ajustes de Linked Server se cambiarán automáticamente. Al modificar la base de datos principal, los cambios se reflejarán en los ajustes de Linked Server de todas las bases de datos auxiliares registradas. Cuando se modifique la base de datos auxiliar, solo se reflejarán los cambios correspondientes a la base de datos principal y a esa base de datos auxiliar.

4 Generar la consulta de Linked Temp Table

Ejecuta la siguiente consulta en la base de datos principal para generar la consulta de Linked Temp Table que se creará en la base de datos auxiliar.

```
USE [<AC Schema>];
GO
DECLARE @LinkedServer  sysname = N'default';
DECLARE @SourceSchema  sysname = N'dbo';
DECLARE @TargetSchema  sysname = N'dbo';

SELECT
    'IF OBJECT_ID(N''' + QUOTENAME(@TargetSchema,'') + '.' + QUOTENAME(t.name,'') + ''', ''SN'') IS NOT NULL '
  + 'DROP SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name) + ';'
  + 'CREATE SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name)
  + ' FOR ' + QUOTENAME(@LinkedServer) + '.' + QUOTENAME(DB_NAME()) + '.' + QUOTENAME(s.name) + '.' + QUOTENAME(t.name) + ';'
  AS recreate_synonym_sql
FROM sys.tables AS t
JOIN sys.schemas AS s
  ON s.schema_id = t.schema_id
WHERE s.name = @SourceSchema
  AND t.is_ms_shipped = 0
  AND t.name NOT LIKE 't_lg[0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_almevt[0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_lgalmtrstrc[0-9][0-9][0-9][0-9][0-9]'
ORDER BY t.name;
```

Example

```
-- Example
USE [main_ac_x_215];
GO
DECLARE @LinkedServer  sysname = N'default';  -- Linked Server name set in the sub DB
DECLARE @SourceSchema  sysname = N'dbo';      -- Schema to target in the main DB
DECLARE @TargetSchema  sysname = N'dbo';      -- Schema to create synonyms in the sub DB (reflected in the output string)

SELECT
    'IF OBJECT_ID(N''' + QUOTENAME(@TargetSchema,'') + '.' + QUOTENAME(t.name,'') + ''', ''SN'') IS NOT NULL '
  + 'DROP SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name) + ';'
  + 'CREATE SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name)
  + ' FOR ' + QUOTENAME(@LinkedServer) + '.' + QUOTENAME(DB_NAME()) + '.' + QUOTENAME(s.name) + '.' + QUOTENAME(t.name) + ';'
  AS recreate_synonym_sql
FROM sys.tables AS t
JOIN sys.schemas AS s
  ON s.schema_id = t.schema_id
WHERE s.name = @SourceSchema
  AND t.is_ms_shipped = 0
  AND t.name NOT LIKE 't_lg[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_almevt[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_lgalmtrstrc[0-9][0-9][0-9][0-9][0-9][0-9]'
ORDER BY t.name;
```

5 Ejecutar la consulta en la base de datos auxiliar.

Copia por completo la consulta `CREATE SYNONYM` generada previamente. Conéctate al servidor de base de datos auxiliar que se va a agregar, escribe la consulta como se muestra a continuación y ejecútala. Se almacenará en Synonyms del esquema AC de la base de datos auxiliar.

```
use [<Sub DB AC Database>];

IF OBJECT_ID(N'[dbo].[T_ACSGR]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGR];CREATE SYNONYM [dbo].[T_ACSGR] FOR
[default].[main_ac_x_215].[dbo].[T_ACSGR];
IF OBJECT_ID(N'[dbo].[T_ACSGRLVLS]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRLVLS];CREATE SYNONYM [dbo].[T_ACSGRLVLS]
FOR [default].[main_ac_x_215].[dbo].[T_ACSGRLVLS];
IF OBJECT_ID(N'[dbo].[T_ACSGRSENT]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRSENT];CREATE SYNONYM
[dbo].[T_ACSGRSENT] FOR [default].[main_ac_x_215].[dbo].[T_ACSGRSENT];
IF OBJECT_ID(N'[dbo].[T_ACSGRUSS]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRUSS];CREATE SYNONYM [dbo].[T_ACSGRUSS]
FOR [default].[main_ac_x_215].[dbo].[T_ACSGRUSS];
...
```

Desinstalar El Servidor BioStar X Y Restaurar Certificados De Seguridad

Esta sección explica cómo desinstalar el servidor **BioStar X** de una computadora. Si **Secure communication with device** no se usa, desinstale **BioStar X** sin respaldar ni restaurar certificados.

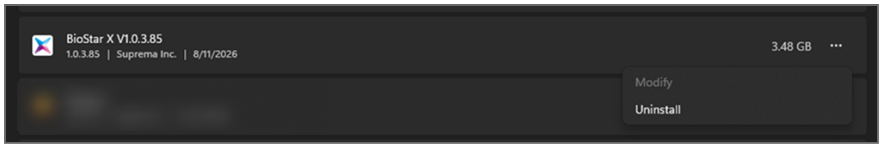
Si **Secure communication with device** se usa, respalde el conjunto de certificados de seguridad del servidor (CA raíz/ certificado del servidor/clave) antes de desinstalar **BioStar X**. Este respaldo es la única forma de volver a conectar los dispositivos existentes después de reinstalar el mismo servidor. Para reutilizar solo los certificados de comunicación segura

y conservar la base de datos y los ajustes, consulte Restaurar certificados de seguridad respaldados. Esto difiere de la característica de restauración del sistema.

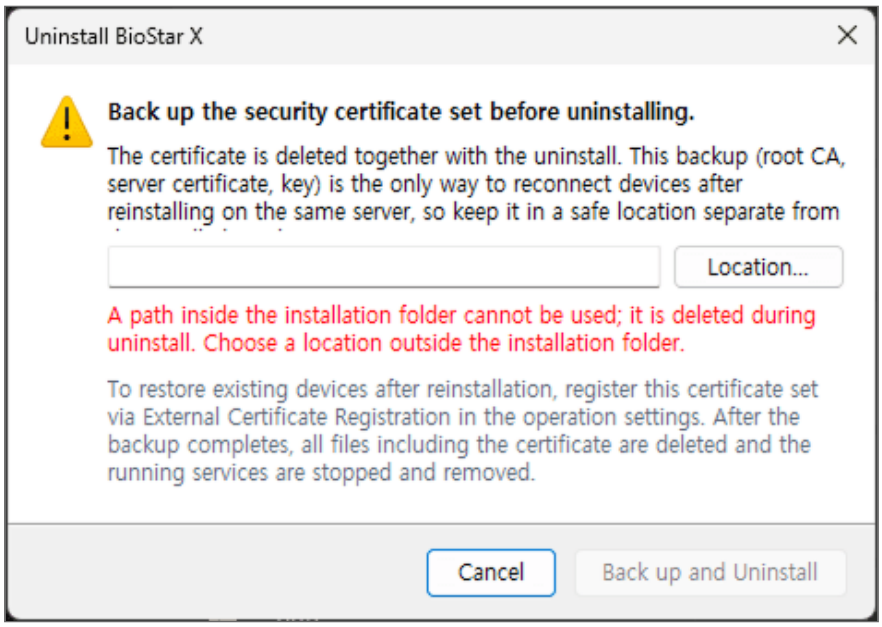
Desinstalar el servidor BioStar X

> **Precaución**
> Desinstalar **BioStar X** elimina todos los archivos de instalación, incluidos los certificados, y también puede eliminar contenido (información de usuarios). Para conservar la base de datos, los ajustes y las claves, respalde el sistema antes de desinstalarlo. Consulte Respaldo de Sistema.

1. En Windows, vaya a **Configuración** → **Aplicaciones** → **Aplicaciones instaladas**.
2. Busque **BioStar X** en la lista, haga clic en ••• y seleccione **Desinstalar**.

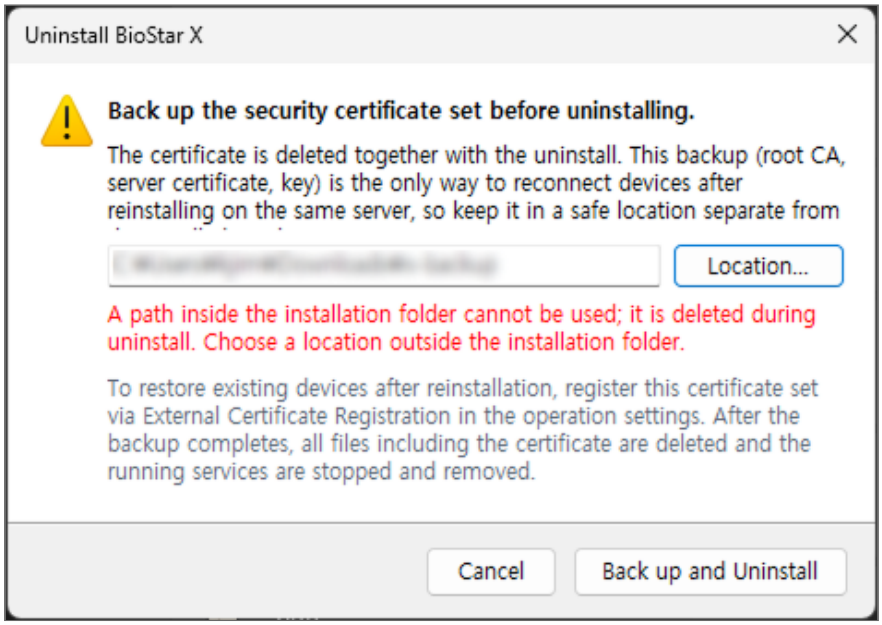


3. Si **Secure communication with device** se usa, aparece el cuadro de diálogo de respaldo de certificados. Haga clic en **Ubicación...** y defina la ruta de respaldo. Si esta opción no se usa, continúe con el paso 7 sin el procedimiento de respaldo de certificados.

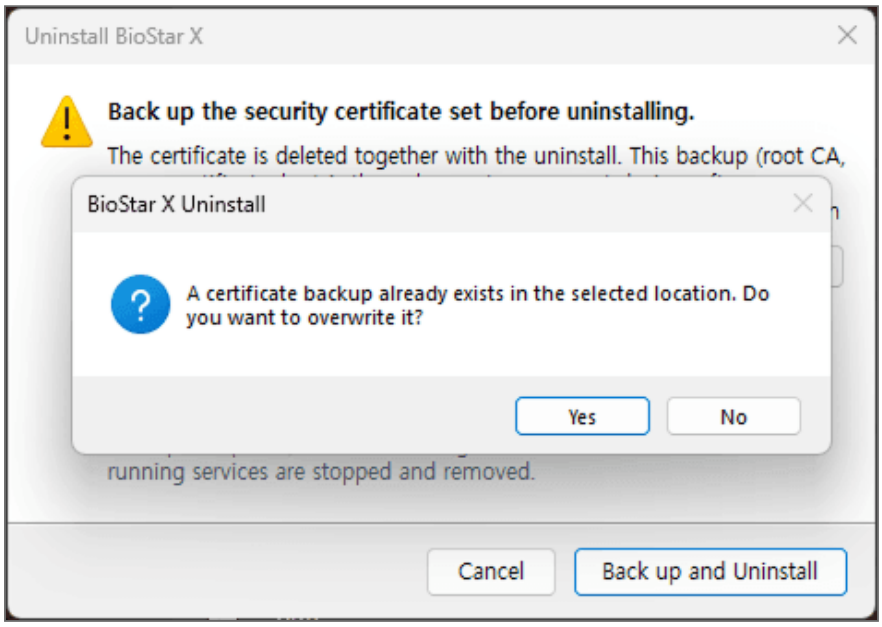


> **Precaución**
> No use la ruta de instalación de **BioStar X** como ubicación de respaldo. Desinstalar **BioStar X** lo elimina junto con la carpeta de instalación de **BioStar X**. Seleccione una ruta distinta de la ruta de instalación de **BioStar X**.

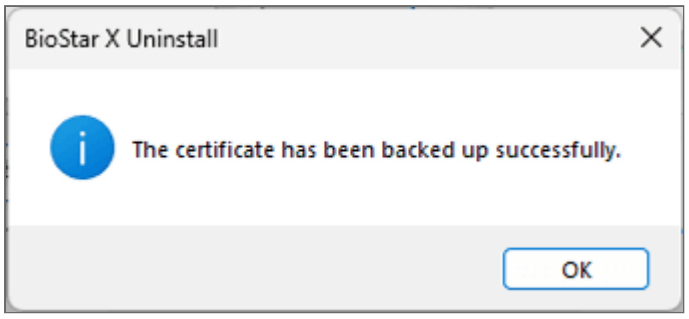
4. Después de seleccionar una ruta, haga clic en **Respaldar y desinstalar** cuando se active.



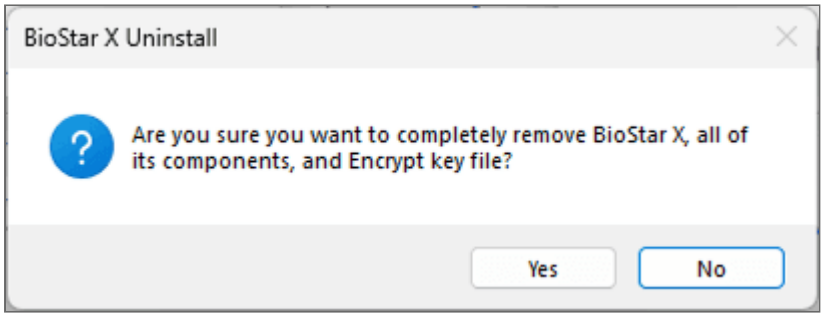
5. Si ya existe un archivo de respaldo de certificados en la ubicación seleccionada, un cuadro de diálogo pregunta si debe sobrescribirlo. Para sobrescribir el respaldo existente, haga clic en **Sí**. Para seleccionar otra ruta, haga clic en **No**.



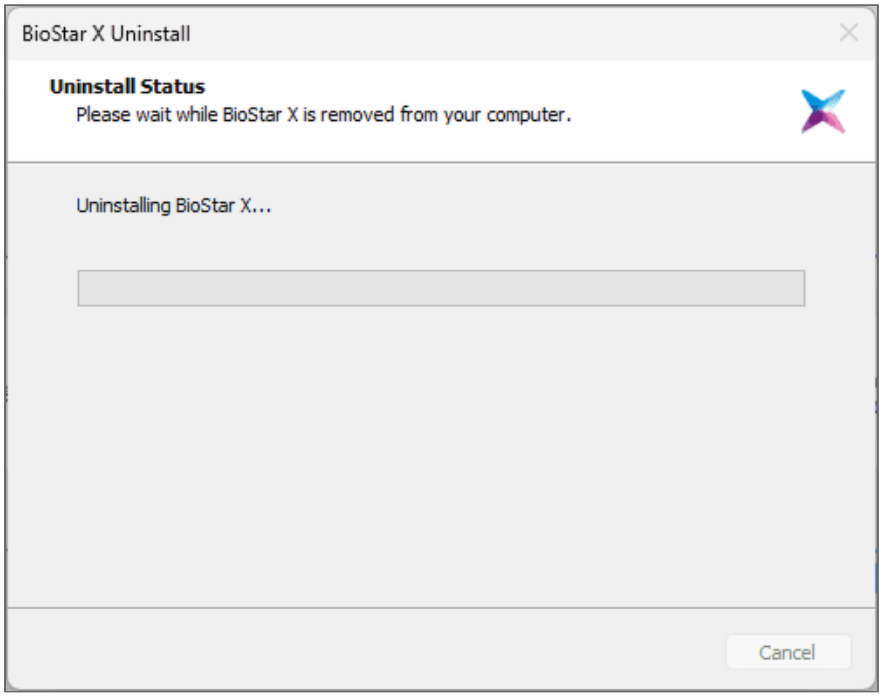
6. Cuando finalice el respaldo de certificados, aparece un cuadro de diálogo informativo. Haga clic en **OK** para guardar los ajustes.



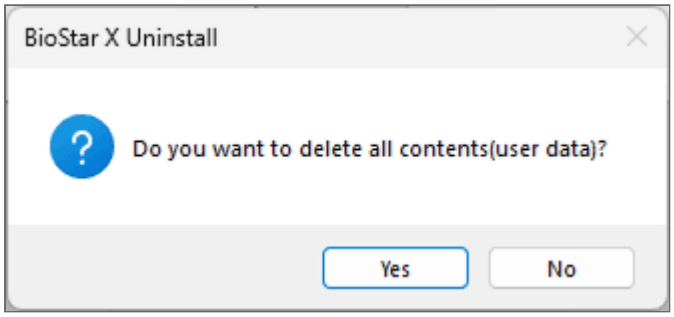
7. Cuando se le solicite confirmar la desinstalación de **BioStar X** y todos los componentes relacionados, haga clic en **Sí**.



8. Espere mientras se completa la desinstalación.

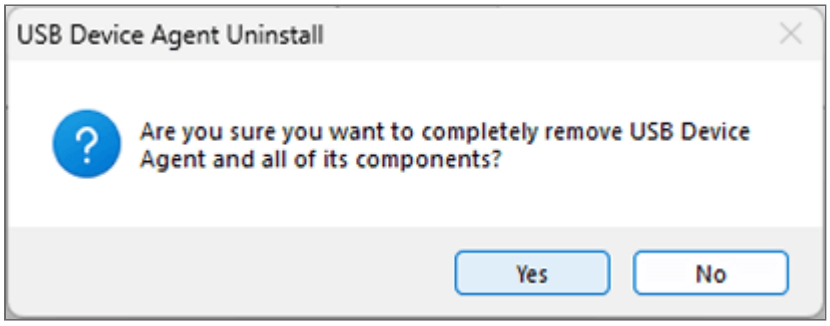


9. Aparece un cuadro de diálogo para confirmar si debe eliminar todo el contenido (información del usuario). Para eliminar todos los datos, incluida la información del usuario almacenada en la base de datos, haga clic en **Sí**. Para conservar los datos, haga clic en **No**.



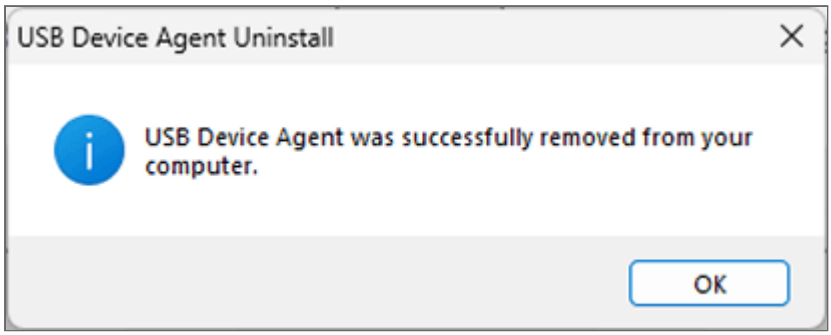
> **Precaución**
>
> Haga clic en **Sí** para eliminar todos los datos, incluida la información del usuario almacenada en la base de datos. No es posible recuperar los datos. Para conservar los datos, haga clic en **No**. Antes de quitar **BioStar X**, haga una copia de seguridad del sistema. Consulte Respaldo de Sistema.

10. Si **USB Device Agent** está instalado, aparece un cuadro de diálogo que pregunta si también debe quitarlo. Haga clic en **Sí**.



> Según los componentes en uso, pueden aparecer cuadros de diálogo adicionales para desinstalar controladores relacionados. Siga las instrucciones en pantalla para completar la desinstalación.

11. Cuando finalice la eliminación de componentes, aparece un cuadro de diálogo. Haga clic en **OK** para guardar los ajustes.



12. Después de que el sistema elimine **BioStar X**, aparece un cuadro de diálogo. Haga clic en **OK** para guardar los ajustes.



Restaurar certificados de seguridad respaldados

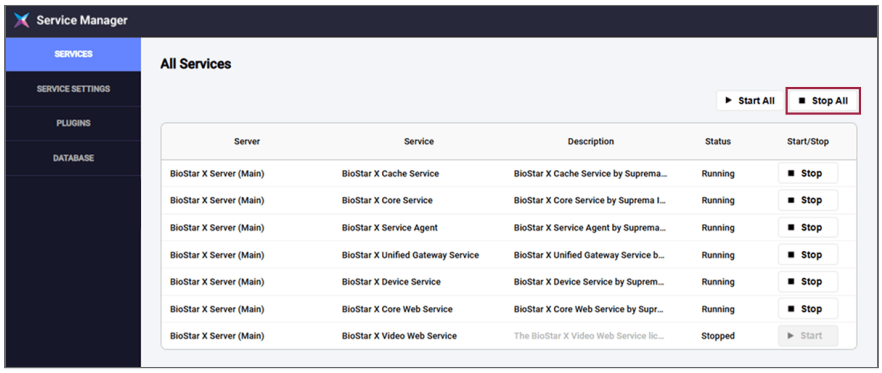
Después de reinstalar el servidor que usó la opción **Secure communication with device**, restaure el certificado de comunicación segura. Esto permite reconectar los dispositivos existentes. La herramienta de restauración del sistema restaura todo el sistema, incluida la base de datos y los ajustes, a un estado anterior. Use este método para reutilizar solo el certificado de comunicación segura sin una restauración del sistema. Sin una herramienta dedicada, restaure los archivos de certificados respaldados directamente en la ruta de instalación.

> **Información**
>
> En un entorno con un servidor principal y un Multi Communication Server, cada servidor usa su propio certificado de comunicación segura. Después de restaurar el certificado, instale y agregue el Multi Communication Server. El sistema copia su certificado automáticamente, por lo que no necesita una restauración aparte.

1. Instale **BioStar X** de nuevo. Para obtener instrucciones de instalación, consulte Instalación Exprés o Instalación

Personalizada.

2. Después de instalar **BioStar X**, haga clic en Inicio → **BioStar X** → **BioStar X Service Manager** en Windows.
3. Cuando aparezca la ventana **BioStar X Service Manager** en el navegador web, haga clic en el menú **SERVICES**.
4. Para detener todos los servicios, haga clic en **Detener todo** en la esquina superior derecha de la pantalla.



5. Copie todos los archivos de certificado respaldados (CA raíz, certificado del servidor y clave) en la carpeta *cert* en la ruta de instalación de **BioStar X**.

   > *Ejemplo: C:\Program Files\BioStar X\cert*

   > Los nombres de archivo coinciden con los certificados creados durante la nueva instalación. Cuando aparezca un aviso para sobrescribir archivos, haga clic en **Sí** para reemplazar los archivos existentes.

6. En **SERVICIOS**, haga clic en **Iniciar todo** para reiniciar todos los servicios.
7. Si usa el Servidor de comunicaciones múltiples, instálelo en un entorno independiente. Para ver las instrucciones de instalación, consulte Instalar el Servidor de Comunicaciones Múltiples.
8. En **BioStar X Service Manager** del servidor principal, agregue el Servidor de comunicaciones múltiples. Para obtener instrucciones sobre cómo agregar el Servidor de comunicaciones múltiples, consulte Instalar el Servidor de Comunicaciones Múltiples.

Cuando agrega el Servidor de comunicaciones múltiples, el sistema copia los archivos del certificado de seguridad desde la carpeta *cert* del servidor principal. Los copia automáticamente en el Servidor de comunicaciones múltiples.

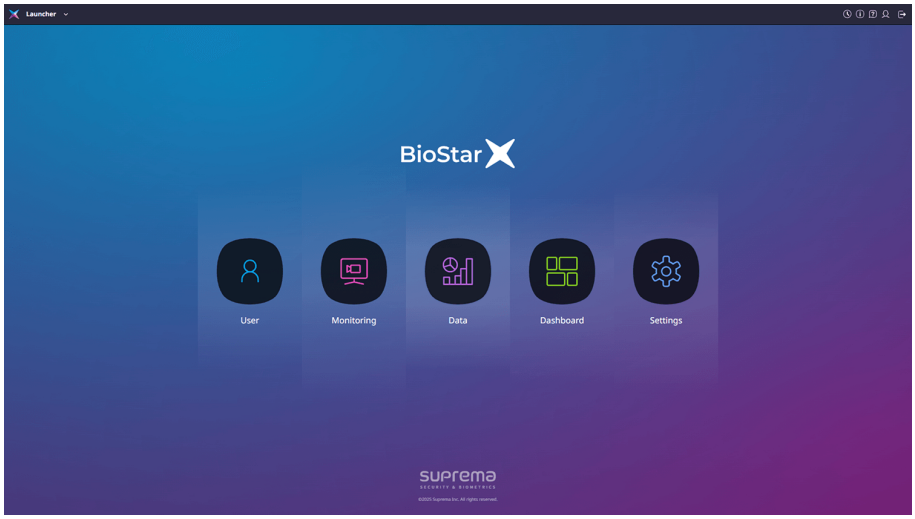
> **Precaución**
>
> Si agregó el Servidor de comunicaciones múltiples antes de restaurar el certificado (pasos 4~6), ya tiene el certificado anterior. En ese caso, reemplace el certificado del Servidor de comunicaciones múltiples por separado. Siga el procedimiento a continuación.
>
> 1. En el servidor donde está instalado el Servidor de comunicaciones múltiples, ejecute **BioStar X Service Manager** y detenga todos los servicios.
> 2. Copie los archivos de certificado respaldados en la carpeta *cert* en la ruta de instalación del Servidor de comunicaciones múltiples.
>
>   > *Ejemplo: C:\Program Files\BioStar X Communications Server\cert*
>
> 3. En el servidor principal y en el Servidor de comunicaciones múltiples, reinicie todos los servicios en **BioStar X Service Manager**.

Información

- Para obtener más información sobre el uso de **BioStar X Service Manager**, consulte Iniciar y Detener el Servidor.
- Para más información sobre la opción **Secure communication with device**, consulta Mejorar la Seguridad del Sistema.
- Necesita una licencia del servidor de comunicaciones múltiples para instalarlo y conectarlo. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Lanzador

La página **Launcher** es la página de inicio inicial de **BioStar X** que los usuarios encuentran después de iniciar sesión y sirve como centro para acceder a las funciones principales de **BioStar X**. Esta página está diseñada para que los usuarios naveguen y utilicen fácilmente todas las funciones de **BioStar X**. Los componentes de la IU de la página Lanzador son los siguientes.



La página **Launcher** proporciona vínculos a las páginas **User**, **Monitoring**, **Data**, **Dashboard** y **Settings**.

- **User**: Administre usuarios de forma eficiente mediante funciones como gestión de grupos de usuarios, gestión de usuarios, gestión de plantillas de usuarios y verificación de usuarios por permisos de acceso, lo que refuerza la seguridad a través de los permisos. Para obtener más información, consulte Usuario.
- **Monitoring**: Supervise puertas, dispositivos, video y eventos de diversas maneras. Controle funciones relacionadas y supervise a través de video en tiempo real. Para obtener más información, consulte Monitorizar.
- **Data**: Consulte información de usuarios o eventos según los criterios deseados y genere informes en una programación establecida. Para obtener más información, consulte Fecha.
- **Dashboard**: Los usuarios pueden agregar y organizar widgets basados en datos seleccionados de los diversos datos que proporciona **BioStar X** para crear el panel que deseen. Para obtener más información, consulte Tablero.
- **Settings**: Configure **BioStar X**, optimizado para los entornos de los usuarios, mediante diversos ajustes para dispositivos, control de acceso, permisos de usuario, idioma y hora. Para obtener más información, consulte Ajustes.

Información

- Para obtener más información sobre el área del encabezado en la parte superior de la pantalla, consulte Aprender la Interfaz de Usuario Común.
- En la parte inferior de la pantalla se puede acceder a las funciones instaladas mediante conectores adicionales. Se requiere una licencia de conector para utilizar las funciones de conector.
  - Para obtener más información sobre el uso de complementos, consulte Conector.
  - Para obtener más información sobre la política de licencias, consulte Política de Licencias.

Usuario

Esta guía abarca las funciones disponibles en la página **User**, una de las funciones fundamentales de BioStar X. Esta página presenta varias funciones para gestionar eficazmente a los usuarios mediante la gestión de grupos de usuarios, la gestión de usuarios, la gestión de plantillas de usuarios y la verificación de usuarios por permisos de acceso, así como métodos para mejorar la seguridad mediante permisos. Utilice las distintas funciones para sacar el máximo partido a **BioStar X**.

Haga clic en **User** en la página **Launcher** o seleccione **User** en la lista de accesos directos de la esquina superior izquierda de la pantalla.

Administrar Grupos de Usuarios

Los grupos de usuarios pueden compartir propiedades y permisos comunes. Cuando un usuario se convierte en miembro de un grupo, automáticamente se le otorgan todas las propiedades de ese grupo. Un usuario solo puede pertenecer a un grupo de usuarios.

- En lugar de establecer permisos de acceso para usuarios individuales, cree grupos de usuarios por departamento o rol y aplique los mismos permisos de acceso de una sola vez.
- Al modificar los permisos de acceso del grupo, estos se aplican automáticamente a todos los usuarios que pertenecen a ese grupo, lo que reduce la carga administrativa. Ajuste rápidamente los permisos cuando haya cambios organizativos o nuevos proyectos.
- Evite accesos innecesarios y aumente la seguridad estableciendo permisos por grupo.
- Analice por separado los registros de acceso de grupos específicos, lo que facilita las auditorías de seguridad y la gestión de registros.
- Los grupos de usuarios pueden aplicar políticas detalladas, como horarios límite de acceso y áreas restringidas, en integración con el nivel de acceso.

Agregar grupo

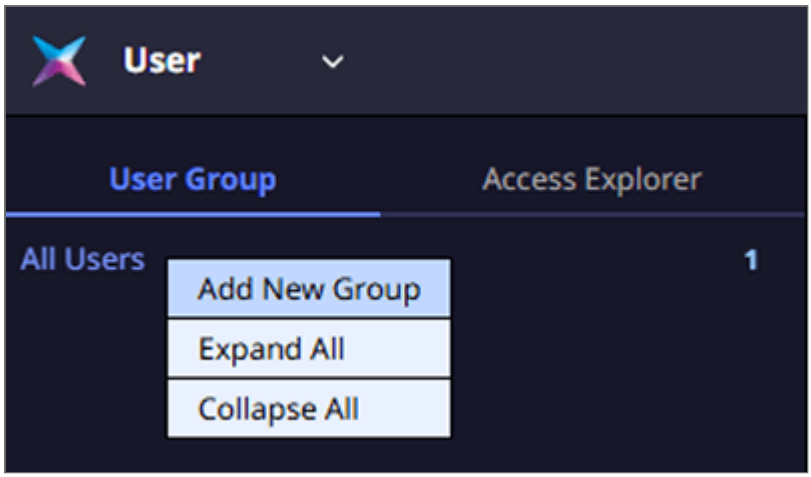
Cree grupos para gestionar varios usuarios de forma eficiente. Registre un nombre, como la organización a la que pertenece el usuario, para gestionarlo cómodamente.

> **Información**
>
> - Registrar el nombre del grupo como el nombre de la organización o departamento al que pertenece el usuario facilita la gestión.
> - Cree subgrupos del grupo de forma secuencial hasta 8 niveles.
> - El nombre del grupo de usuarios puede tener hasta 48 caracteres.
> - Seleccione un grupo de la lista de grupos de usuarios para que en la lista de usuarios aparezcan únicamente los pertenecientes a ese grupo.

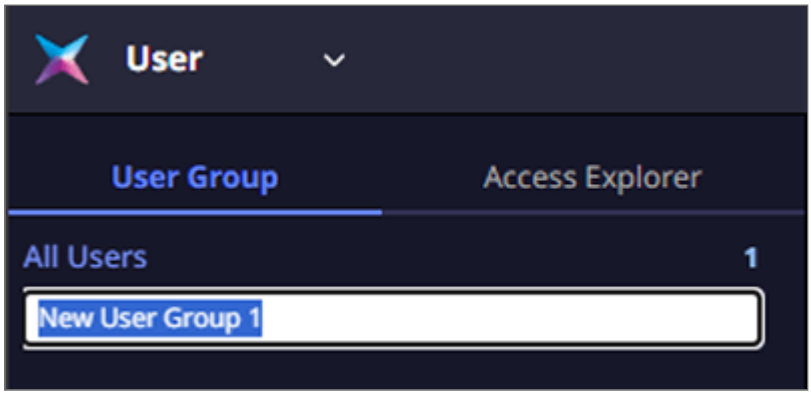
Crear grupo de nivel superior

1. Haz clic en **User** en la página **Launcher**.

2. En la barra lateral izquierda de la pantalla, seleccione **All Users** en la pestaña **User Group** y haga clic derecho.

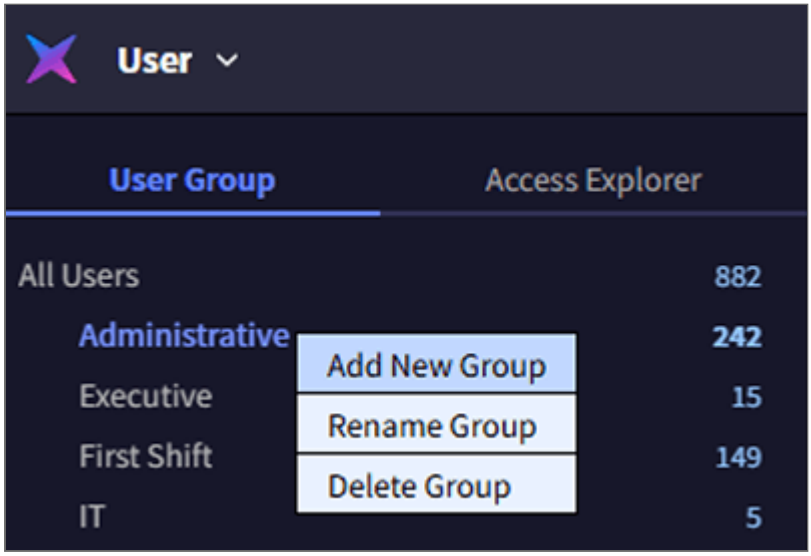


3. Haga clic en **Add New Group** en el menú emergente.
4. Una vez creado el grupo, ingrese el nombre de grupo deseado.



Crear subgrupo

1. En la pestaña **User Group** de la barra lateral izquierda de la pantalla, seleccione el grupo padre y haga clic derecho.



2. Haga clic en **Add New Group** en el menú emergente.
3. Una vez creado el grupo, ingrese el nombre de grupo deseado.

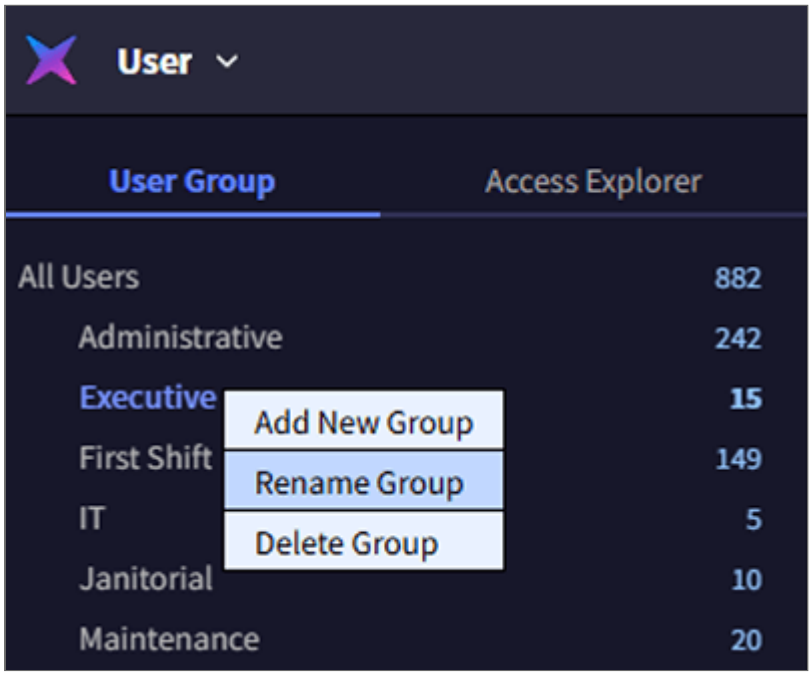
Información

- Al crear un subgrupo, debe seleccionar un grupo padre y puede crear hasta 8 niveles.
- Establezca un grupo como subgrupo del grupo de destino arrastrándolo a otro grupo. Mover un grupo a **All Users** permite configurarlo como grupo de nivel superior.

Cambiar nombre de grupo

Cambie el nombre del grupo al que pertenece el usuario. Se recomienda cambiar el nombre del grupo cuando cambie el nombre de la organización o del departamento.

1. Haz clic en **User** en la página **Launcher**.
2. En la lista **User Group** de la barra lateral izquierda, seleccione el grupo que desea renombrar y haga clic derecho.



3. Haga clic en **Rename Group** en el menú emergente.
4. Cambie el nombre del grupo según desee.

Verifique los cambios en la lista **User Group**.

Información

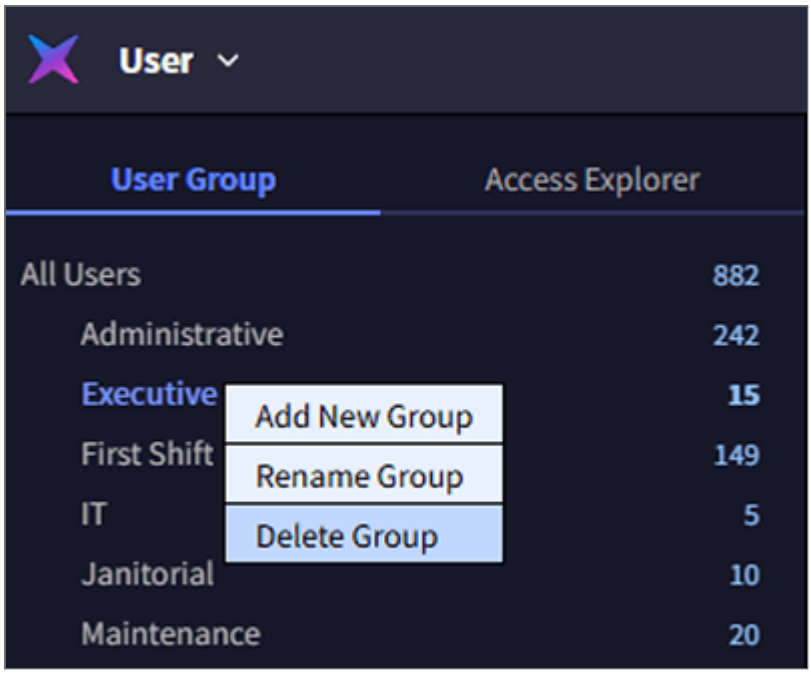
El nombre del grupo de usuarios puede tener hasta 48 caracteres.

Eliminar grupo

Elimine el grupo al que pertenece el usuario.

1. Haz clic en **User** en la página **Launcher**.
2. En la lista **User Group** de la barra lateral izquierda, seleccione el grupo que desea eliminar y haga clic derecho.

3. Haga clic en **Delete Group** en el menú emergente.

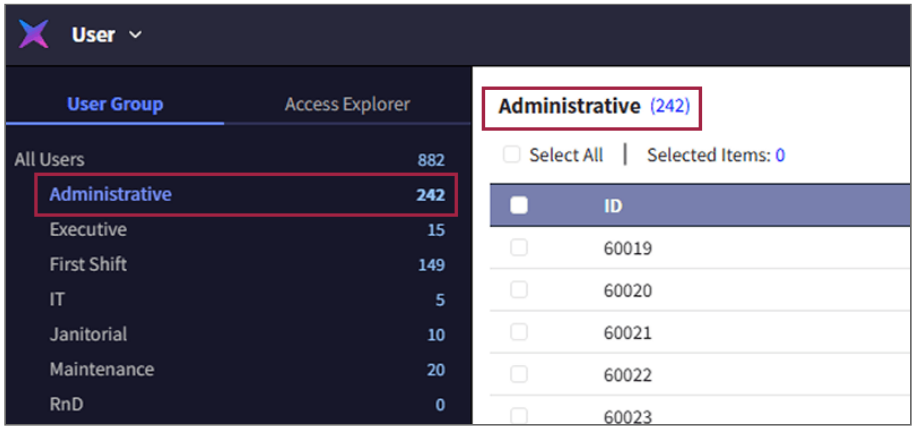


4. Cuando aparezca el mensaje de confirmación, haga clic en el botón **Yes**.

En la lista **User Group**, confirme que el grupo seleccionado se ha eliminado.

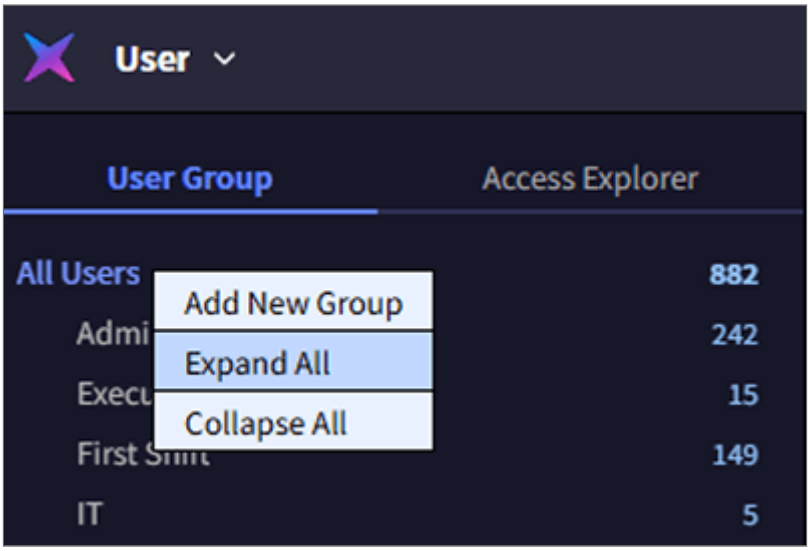
Ver usuarios por grupo

Vea los usuarios que pertenecen al grupo de usuarios. En la página **User**, seleccione el grupo de usuarios deseado en la barra lateral izquierda. Los usuarios del grupo seleccionado se mostrarán en la lista.

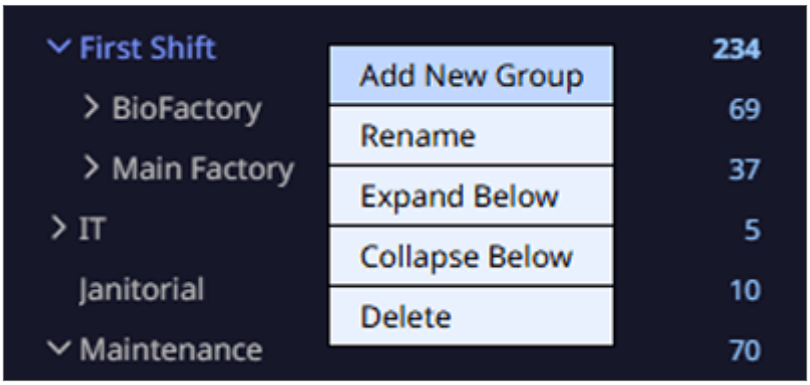


Expandir/contraer lista de grupos

Expanda o contraiga la lista de grupos de usuarios. En la pestaña **User Group**, seleccione **All Users** y haga clic derecho. Haga clic en **Expand All** o **Collapse All** en el menú emergente.



Si hay subgrupos dentro del grupo, puede expandirlos o contraerlos. Seleccione el grupo padre y haga clic derecho. Haga clic en **Expand Below** o **Collapse Below** en el menú emergente.



Registrar usuarios

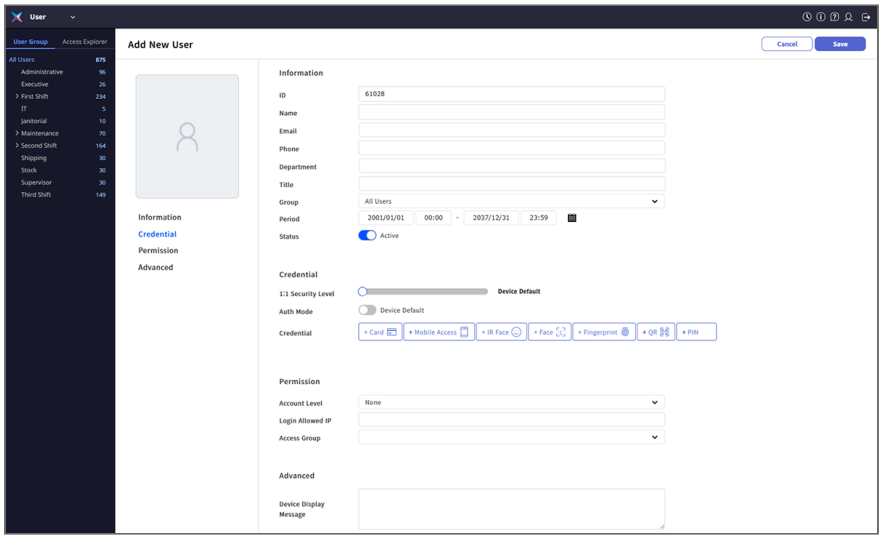
Pautas para registrar nuevos usuarios. Ingrese información como la foto, el nombre, el correo electrónico y el número de teléfono del usuario, y configure los permisos de acceso y la información biométrica del usuario.

Ingrese la información del usuario y configure los permisos de acceso; luego, inscriba las credenciales.

1. Haz clic en **User** en la página **Launcher**.
2. Haga clic en **New User** en la esquina superior derecha de la página **User**.



3. Ingrese la información del usuario en la pantalla **Add New User**.



4. Ingrese la información básica del usuario en la sección **Information**.
5. Inscriba la información biométrica del usuario en la sección **Credential**.
6. Configure los permisos de operación y acceso de **BioStar X** para el usuario en la sección **Permission**.
7. En la sección **Advanced**, ingrese un mensaje que se mostrará en el dispositivo cuando el usuario acceda.
8. Ingrese toda la información y haga clic en **Save** en la esquina superior derecha de la pantalla.

El usuario registrado aparece en la lista de usuarios. Para obtener información detallada sobre la entrada y la configuración por sección, consulte lo siguiente.

Ingrese la información básica del usuario en la sección **Information**. Revise la información detallada de cada campo.
Inscriba las credenciales del usuario y configure el método de autenticación de acceso en la sección **Credential**.
Consulte cómo configurar los permisos de acceso del usuario en la sección **Permission**.
En la sección **Advanced**, configure el mensaje que se mostrará en el dispositivo cuando el usuario acceda o excluya a ese usuario de la sincronización al vincular con Directory Service.
Inscriba o edite un usuario escaneando un pasaporte.

Información

- Los permisos de acceso y la información biométrica son opcionales. Modifique o agregue después de guardar la información básica.
- Haga clic en **Print Card** en la esquina superior derecha de la pantalla para imprimir la información del usuario como tarjeta usando la plantilla de tarjetas. Para obtener más información, consulte Impresora de Tarjetas.
- Haga clic en **Cancel** en la esquina superior derecha de la pantalla para cancelar el registro del usuario.

Ingresar Información Básica del Usuario

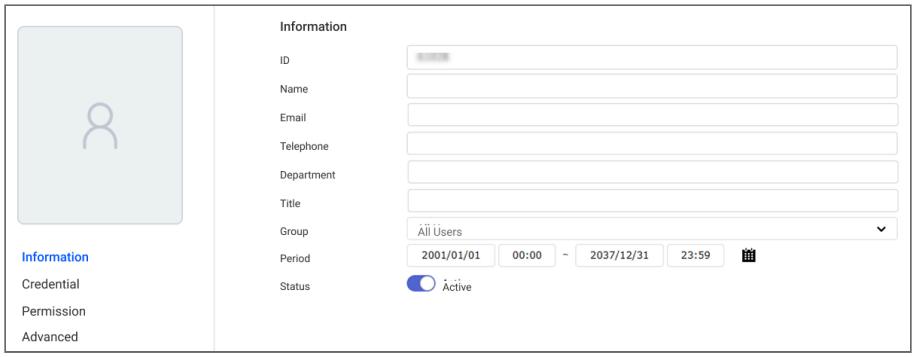
Esta sección describe cómo ingresar la información básica del usuario. La información de usuario ingresada se utiliza para búsqueda y gestión. Gestionar la información de los usuarios ayuda claramente a cumplir con las políticas de seguridad y privacidad de la organización.

- Al ingresar de forma sistemática información básica como nombre, departamento, puesto y grupo, se puede buscar, clasificar y gestionar a los usuarios fácilmente.
- Se pueden perfeccionar los derechos de acceso según la afiliación, el puesto y la información de grupo del usuario.
- Es ventajoso para la seguridad y las auditorías porque permite el seguimiento preciso de actividades, registros de acceso, etc., por usuario.

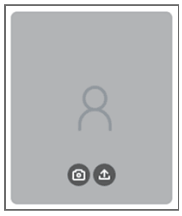
Vaya a la página **Launcher** → **User**. Hay dos maneras de ingresar la información del usuario.

- **Nuevo usuario**: Haz clic en **New User** en la esquina superior derecha de la pantalla. Aparece la ventana **New User**.
- **Usuario existente**: Haz doble clic en un usuario de la lista de usuarios. O haz clic en el usuario y luego haz clic en **See More** en la pantalla de vista previa que aparece en el lado derecho de la pantalla. Aparece una ventana para editar la información del usuario.

Los campos que se pueden configurar en la sección **Information** son los siguientes. Ingrese la información del usuario según la descripción de cada campo.



- **Foto**: Registre la foto del usuario. Puede tomar una foto con la cámara web o cargar una desde su PC. Al colocar el cursor sobre el perfil, se muestran las herramientas disponibles.



  - : Si hay una cámara web conectada al PC, haga clic en el botón para tomar y registrar una foto.
  - : Puede cargar un archivo de imagen guardado en su PC.

  Para obtener más información, consulte Registrar Cara.

- **ID**: Ingrese la identificación única que asignará al usuario.
- **Name**: Ingrese el nombre del usuario.
- **Email**: Ingrese la dirección de correo electrónico.
- **Phone**: Ingrese el número de teléfono.
- **Department**: Ingrese el departamento al que pertenece el usuario.
- **Title**: Ingrese el puesto del usuario.

- Seleccione **Group**: Seleccione el grupo del usuario. Para obtener más información sobre cómo agregar y administrar grupos de usuarios, consulte Administrar Grupos de Usuarios.
- **Period**: Defina un período para usar la cuenta de usuario. Puede hacer clic en el área de fecha y hora para ingresarlas manualmente o hacer clic en para seleccionar la fecha y hora deseadas.
- **Status**: Puede deshabilitar temporalmente la cuenta de usuario.

Haga clic en **Save** en la esquina superior derecha de la pantalla para guardar la información básica ingresada.

Reglas para ingresar el ID de usuario y el nombre

- El valor de **ID** no puede incluir espacios.
- **ID** puede incluir un punto (`.`), pero no puede consistir únicamente en un punto (`.`) o dos puntos (`..`).
- El nombre de usuario puede tener hasta 48 caracteres, incluidos los caracteres especiales.

  > *Caracteres especiales:* `~` `!` `@` `#` `$` `%` `^` `&` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}` `;` `.` `'`

- Los ID de usuario y los nombres no pueden incluir los siguientes caracteres. `₩` `/` `:` `*` `?` `"` `<` `>` `|` `` ` ``
- Los ID de usuario tampoco pueden incluir un apóstrofo (`'`).
- El nombre de usuario no puede comenzar con `&@~` de forma consecutiva. Sin embargo, un nombre de usuario puede comenzar solo con `&`, `@` o `~`.

Información

- Los valores disponibles para **ID** varían según la opción **User ID Type** en el menú **Settings** → **System** → **Server**. Para obtener más información, consulte Configuración Detallada del Servidor.
  - **Number**: Ingrese un número del 1 al 4294967294.
  - **Alphanumeric**: Ingrese una combinación de letras y números.
- Para mostrar la foto, el departamento y el puesto del usuario en la tarjeta de acceso móvil, asegúrese de agregar una foto e ingresar el departamento y el puesto.
- Los nombres de puesto y departamento pueden tener hasta 64 caracteres, incluidos los caracteres especiales, `espacios` y `_`.
- Si usa una tarjeta de acceso móvil, asegúrese de ingresar el correo electrónico del usuario al enviarla por correo electrónico.
- Para usar el enrolamiento facial móvil o BioStar X QR, asegúrese de ingresar la dirección de correo electrónico del usuario.

Consejo

Además de los campos básicos proporcionados por **BioStar X**, puede agregar campos personalizados mediante la función **Custom User Field** para ingresar información adicional del usuario. **Custom User Field** es una función útil que permite ampliar la información del usuario según los requisitos de la organización.

Para obtener más información sobre cómo agregar **Custom User Field**, consulte Configuración Detallada del Servidor.

Siguiente paso

Inscriba las credenciales del usuario y configure el método de autenticación de acceso en la sección **Credential**.
Consulte cómo configurar los permisos de acceso del usuario en la sección **Permission**.
En la sección **Advanced**, configure el mensaje que se mostrará en el dispositivo cuando el usuario acceda o excluya a ese usuario de la sincronización al vincular con Directory Service.
Consulte cómo editar la información del usuario.

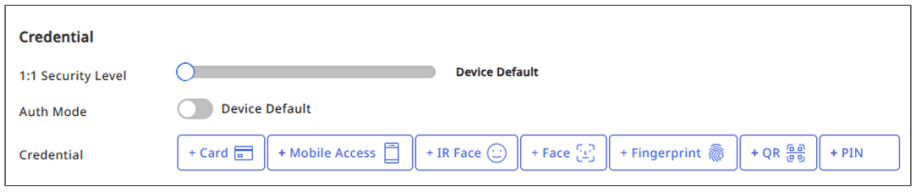
Registrar Credencial del Usuario

Este documento proporciona orientación sobre cómo inscribir credenciales de usuario. Los usuarios pueden inscribir sus fingerprints, faces, información de card y PINs como credenciales. Las credenciales se pueden añadir o modificar al registrar o actualizar un usuario.

Vaya a la página **Launcher** → **User** y inscriba, añada o modifique credenciales de las dos siguientes maneras:

- **Nuevo usuario**: Haz clic en **New User** en la esquina superior derecha de la pantalla. Aparece la ventana **New User**.
- **Usuario existente**: Haz doble clic en un usuario de la lista de usuarios. O haz clic en el usuario y luego haz clic en **See More** en la pantalla de vista previa que aparece en el lado derecho de la pantalla. Aparece una ventana para editar la información del usuario.

En la sección **Credential**, se pueden configurar los siguientes elementos. Consulte las descripciones de cada elemento para configurar los permisos de usuario adecuados.



Inscriba credenciales y establezca el nivel de seguridad apropiado en el campo **1:1 Security Level**. Un nivel de seguridad más alto puede resultar en una menor tasa de autenticación o una mayor tasa de rechazo falso (FRR).

크리덴셜(Credential): 사용자의 신원을 확인하기 위한 데이터입니다. 일반적으로 디지털 서명, 스마트카드, 바이오 정보, 사용자 이름과 비밀번호 등이 있습니다.

Información

- Vincule las tarjetas de acceso móvil al portal Airfob para usarlas. Para obtener más información sobre la integración con el portal de Airfob y el uso de las tarjetas de acceso móvil, consulte Administrar Tarjetas de Acceso Móvil.

Inscribir credenciales

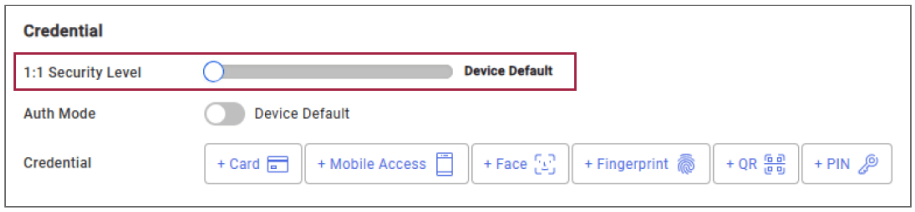
El método para inscribir credenciales de usuario es el siguiente. Las credenciales pueden inscribirse en varias formas, como fingerprints, faces, cards y contraseñas.

Siguiente paso

Consulte cómo configurar los permisos de acceso del usuario en la sección **Permission**.
En la sección **Advanced**, configure el mensaje que se mostrará en el dispositivo cuando el usuario acceda o excluya a ese usuario de la sincronización al vincular con Directory Service.
Consulte cómo editar la información del usuario.

Configurar Nivel de Seguridad

Otorgue niveles de seguridad independientes a los usuarios, independientemente del nivel de seguridad biométrico 1:N configurado en el dispositivo. Si los usuarios fallan con frecuencia la autenticación cuando el nivel de seguridad 1:N del dispositivo es alto, reduzca **1:1 Security Level** para mitigar las autenticaciones fallidas.



Establezca el nivel deseado en el campo **1:1 Security Level**. Los valores disponibles son los siguientes:

- **Device Default**
- **Lowest**
- **Low**
- **Normal**
- **High**
- **Highest**

Haga clic en **Save** en la esquina superior derecha de la pantalla para guardar la configuración.

Información

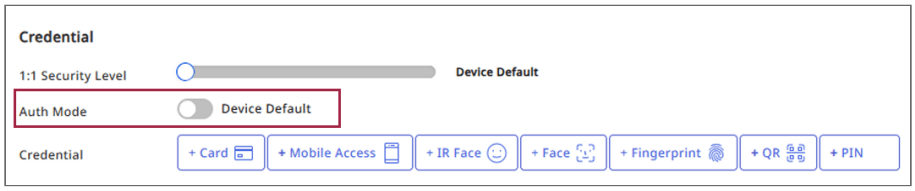
- Si se establece **Private Auth Mode** en la sección **Credential** como **Biometrics**, no es posible aplicar el nivel de seguridad 1:1 porque el usuario ingresado no se puede identificar; el nivel de seguridad 1:1 solo se puede aplicar cuando en el modo de autenticación se configura una tarjeta o ID que permita identificar al usuario. Para obtener más información sobre **Private Auth Mode**, consulte Configuración del Modo de Autenticación.
- Establezca un nivel de seguridad apropiado. Un nivel de seguridad más alto puede dar como resultado tasas de autenticación de huella dactilar más bajas o tasas de rechazo falso (FRR) más altas.

Configuración del Modo de Autenticación

Los usuarios pueden configurar los métodos de autenticación de manera flexible. Utilice el método de autenticación predeterminado configurado en el dispositivo o asigne modos de autenticación individuales adaptados a cada usuario. Además, el modo de autenticación extendida, que incluye autenticación facial y de huellas dactilares, mejora el nivel de seguridad.

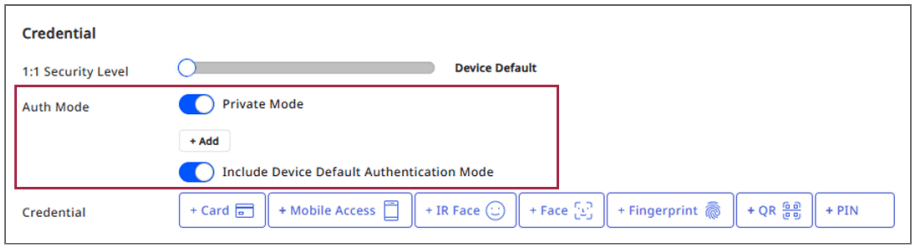
Valores predeterminados del dispositivo

Configurar la opción **Auth Mode** en **Device Default** permite la autenticación según el método configurado en el dispositivo.



Modo de autenticación privada

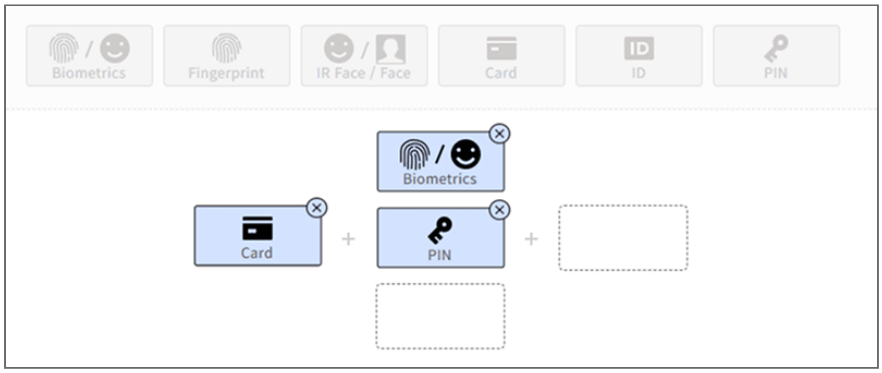
Configurar la opción **Auth Mode** en **Private Mode** permite diferentes métodos de autenticación para cada usuario.



Haga clic en **+ Add** para abrir la ventana **Add New Auth Mode**. Configure los métodos de autenticación deseados.



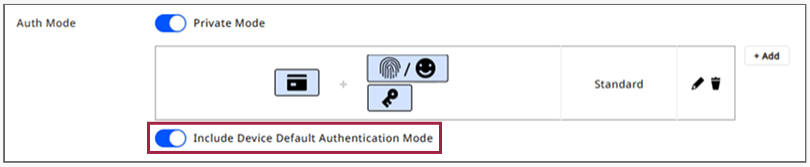
- **Extended Auth Mode**: Configure si se utiliza el modo de autenticación extendida. El modo de autenticación extendida permite combinar los métodos de autenticación facial y de huellas dactilares.
- **Auth Mode**: Configure los métodos de autenticación mediante arrastrar y soltar.



Para inscribir los métodos de autenticación configurados, haga clic en **Apply**.

Información

- La opción **Extended Auth Mode** está disponible en los modelos BioStation 3 Max, BioEntry W3, BioStation 3 y FaceStation F2.
- Configurar **Include Device Default Authentication Mode** permite utilizar tanto los modos de autenticación establecidos en el dispositivo como los modos de autenticación privados configurados en **BioStar X**.



- Configurar **Exclude Device Default Authentication Mode** permite usar únicamente los modos de autenticación privados establecidos en **BioStar X**.

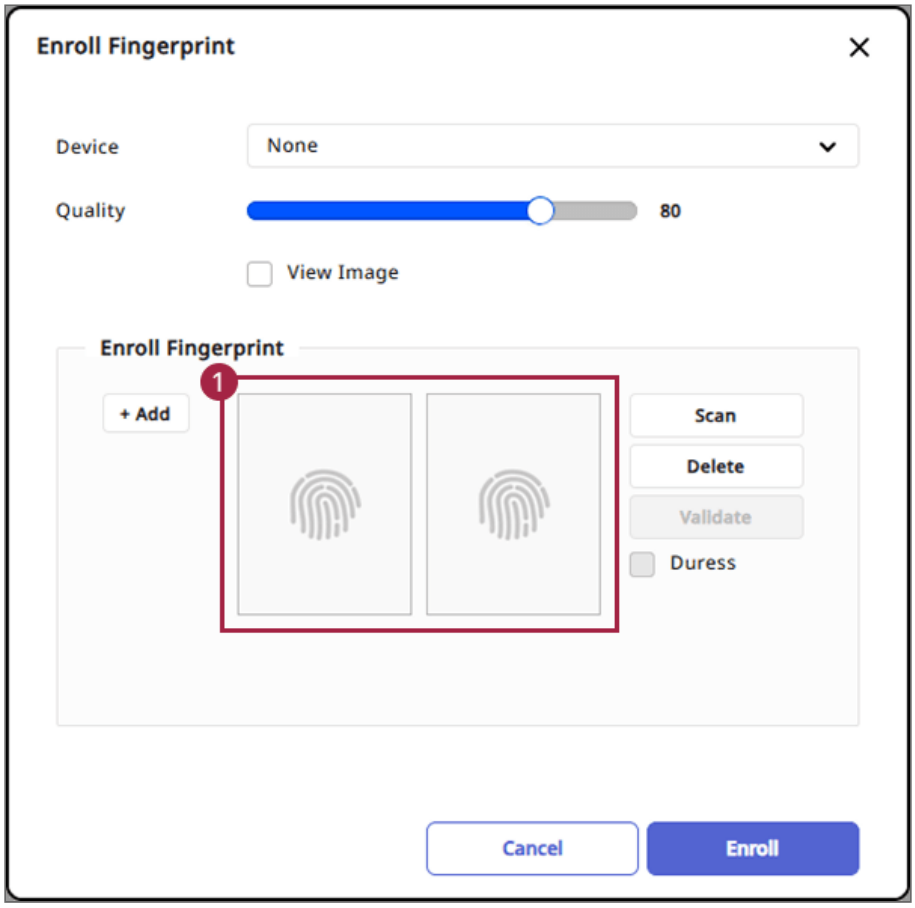
Inscribir Huella Dactilar

Inscriba la huella digital del usuario como medio de autenticación para el control de acceso. Inscriba la información de la huella digital del usuario mediante un dispositivo que admita autenticación por huella digital. Escanee huellas digitales en dispositivos equipados con lectores de huellas digitales.

Antes de inscribir huellas digitales...

- Asegúrese de que la huella digital del usuario esté limpia y seca.
- No inscriba huellas digitales lesionadas o borrosas.

En **Credential**, haga clic en **+ Fingerprint**. Cuando aparezca la ventana **Enroll Fingerprint**, configure cada elemento y haga clic en **Enroll**.



- **Device**: Seleccione el dispositivo para inscribir la huella digital.
- **Quality**: Ajuste la calidad de inscripción de huella digital. No se puede inscribir la información de la huella digital si no cumple el nivel de calidad configurado.
- **View Image**: Vea la imagen original de la huella digital escaneada en el área 1.
- **+ Add**: Haga clic para añadir una huella digital. Se pueden inscribir hasta 10 huellas digitales.
- **Scan**: Seleccione el número de huella digital añadido y haga clic. Coloque el dedo en el lector de huellas digitales o en el sensor del dispositivo para escanear la huella.



- **Delete**: Permite eliminar una huella digital inscrita. Seleccione el número de huella digital que desea eliminar y haga clic.
- **Validate**: Verifique si la huella digital ya está inscrita.
- **Duress**: Para inscribir una huella digital como huella digital de coacción, seleccione esta opción y escanee la huella. Si lo amenazan o lo obligan a abrir la puerta, use esa huella digital para enviar una notificación.

Información

- No use la huella digital que utiliza para el acceso diario como huella de coacción.
- Al activar la opción **View Image**, se muestra la imagen de la huella digital, pero no se almacena en **BioStar**.
- Si la tasa de autenticación de huella digital es baja, elimine la huella digital y inscriba una nueva.
- Cubra toda la superficie del sensor de reconocimiento de huellas digitales con el dedo para obtener una huella de buena calidad. Utilice las huellas digitales del dedo índice o medio.



Inscribirse IR Face

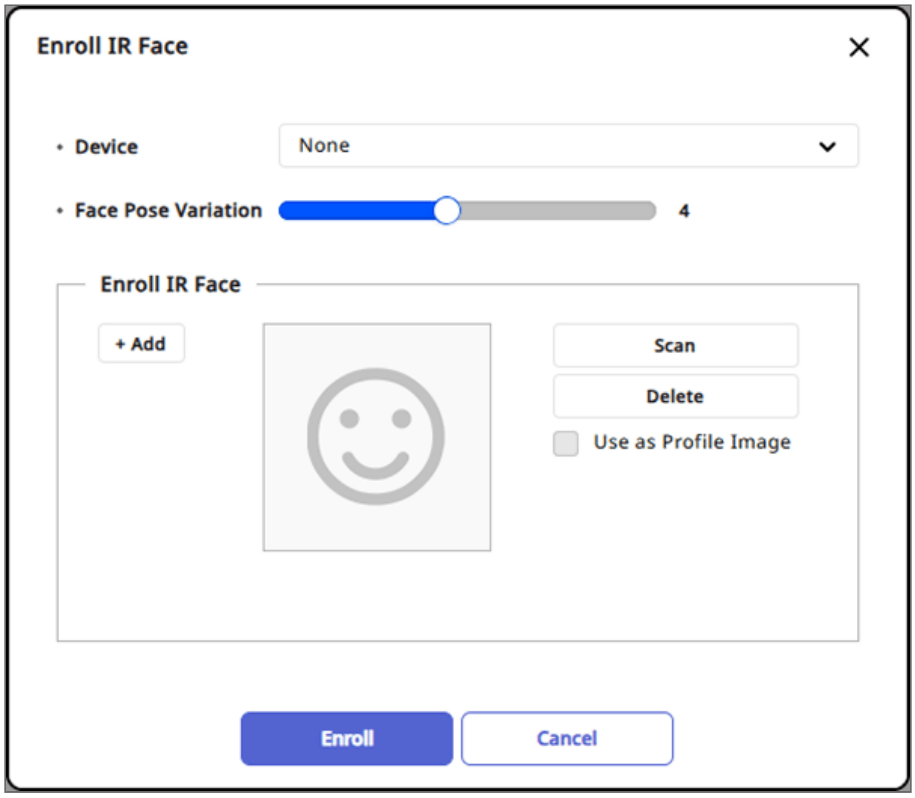
Registra el rostro del usuario como medio de autenticación para el control de acceso. El registro de rostro IR es un método de autenticación que captura el rostro del usuario utilizando una cámara infrarroja.

Precauciones al registrar rostro IR

- Mantén una distancia de 60 a 100 cm entre el dispositivo y tu rostro al enrolar tu rostro.
- No cambies tu expresión facial.
- No uses mascarillas, sombreros ni parches para los ojos.
- No enroles un rostro con mascarilla. Podría aumentar la tasa de aceptación errónea (FAR) si se enrolan rostros con y sin mascarilla.
- No inclines la cabeza hacia arriba ni hacia abajo.
- No uses maquillaje pesado.
- No cierres los ojos.
- Asegúrate de que ambos hombros aparezcan correctamente en la pantalla.
- Permanece quieto y enrola tu rostro mirando fijamente la pantalla.
- Asegúrate de que no aparezcan dos rostros en la pantalla. Enrola a una persona a la vez.
- Si no sigues las instrucciones en pantalla, el enrolamiento facial podría tardar más o fallar.

Registrar por dispositivo

Haga clic en **+ IR Face** en la sección **Credential**. Cuando aparezca la ventana **Enroll IR Face**, establezca cada campo y haga clic en **Enroll**.



- **Device**: Seleccione el dispositivo para registrar el rostro IR.
- **Face Pose Variation**: Defina la sensibilidad a la posición, ángulo y distancia del rostro al registrar el rostro IR. Defínala alta para obtener una plantilla de rostro IR precisa.
- **+ Add**: Haga clic para registrar el rostro IR. Agregue hasta cinco rostros IR.
- **Scan**: Haga clic en el botón **Nth** agregado para escanear el rostro IR. Sigue las instrucciones en pantalla para escanear el rostro.



- **Use as Profile Image**: Active esta opción para usar la imagen de rostro IR registrada como imagen de perfil.
- **Delete**: Elimine la credencial de rostro IR. Selecciona el número a eliminar y haz clic en el botón.

Información

- Los dispositivos que pueden registrar rostro IR son los siguientes:
  - FaceStation 2
  - FaceLite
- Si la tasa de autenticación facial es baja, elimina la información de rostro y registra un nuevo rostro.

Registrar Cara

Registra el rostro del usuario como medio de autenticación para el control de acceso. El registro facial es un método de autenticación que captura el rostro del usuario con una cámara. Registra de forma remota en un dispositivo móvil la información facial del usuario capturada por la cámara.

Precauciones al registrar el rostro

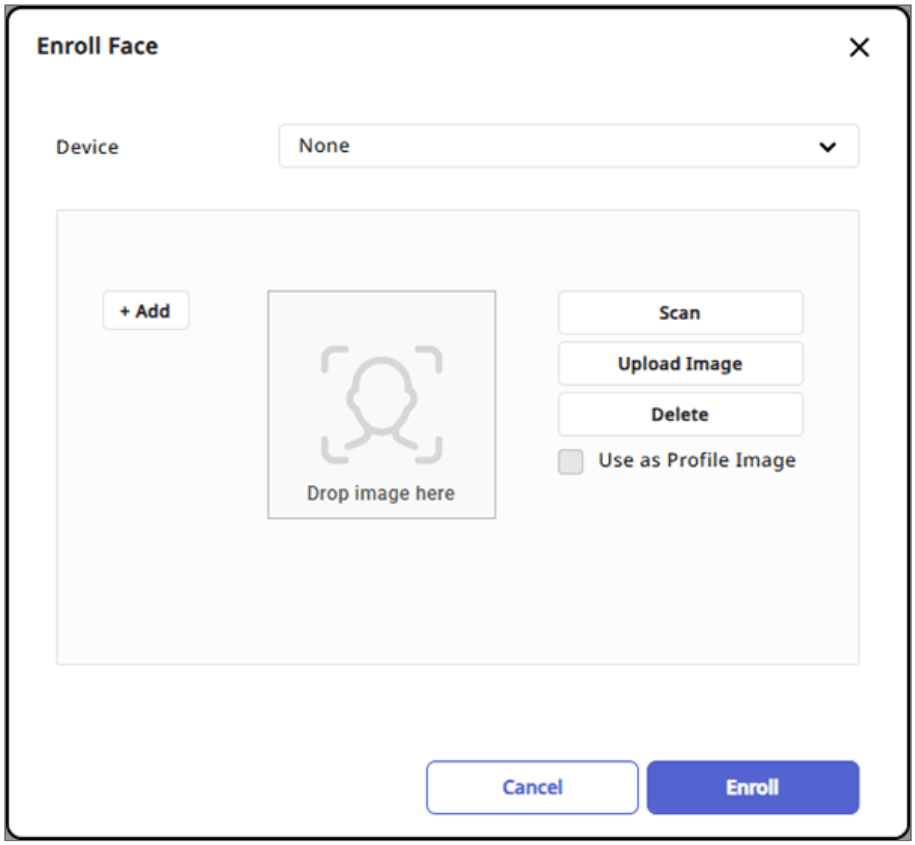
- Mantén una distancia de 60 a 100 cm entre el dispositivo y tu rostro al enrolar tu rostro.
- No cambies tu expresión facial.
- No uses mascarillas, sombreros ni parches para los ojos.
- No enroles un rostro con mascarilla. Podría aumentar la tasa de aceptación errónea (FAR) si se enrolan rostros con y sin mascarilla.
- No inclines la cabeza hacia arriba ni hacia abajo.
- No uses maquillaje pesado.
- No cierres los ojos.
- Asegúrate de que ambos hombros aparezcan correctamente en la pantalla.
- Permanece quieto y enrola tu rostro mirando fijamente la pantalla.
- Asegúrate de que no aparezcan dos rostros en la pantalla. Enrola a una persona a la vez.
- Si no sigues las instrucciones en pantalla, el enrolamiento facial podría tardar más o fallar.

Información

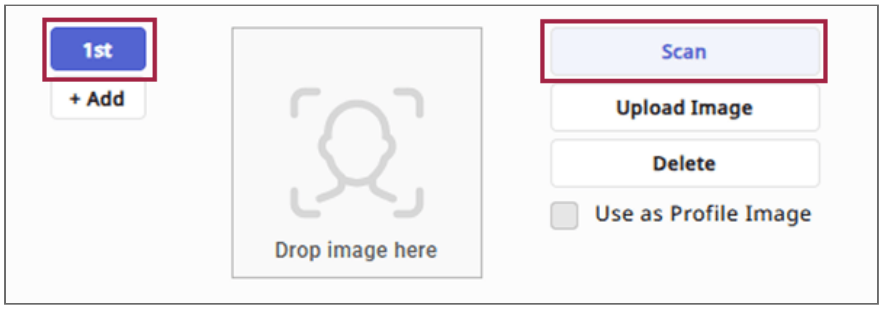
Utiliza la función de importación desde CSV para registrar varios rostros a la vez o envía un enlace por correo electrónico a varios usuarios para que registren su rostro directamente en un dispositivo móvil. Para más información, consulte Inscribir Rostros por Lotes.

Registrar por dispositivo

Haz clic en **+ Face** en la sección **Credential**. Cuando aparezca la ventana **Enroll Face**, configure cada elemento y haga clic en **Enroll**.



- **Device**: Selecciona el dispositivo para registrar el rostro.
- **+ Add**: Haz clic para registrar el rostro. Añade hasta 2 rostros.
- **Scan**: Haz clic en el botón **N-th** añadido para escanear el rostro. Sigue las instrucciones en pantalla para escanear el rostro.



- **Upload Image**: Carga una imagen de rostro sin escanear.

  – El tamaño máximo de archivo para los tipos de imagen admitidos es de 10MB.
  – Los formatos de imagen admitidos incluyen JPG, JPEG y PNG.

- **Use as Profile Image**: Seleccione esta opción para usar la imagen facial inscrita como imagen de perfil.
- **Delete**: Elimina la credencial de rostro. Selecciona el número a eliminar y haz clic en el botón.

Información

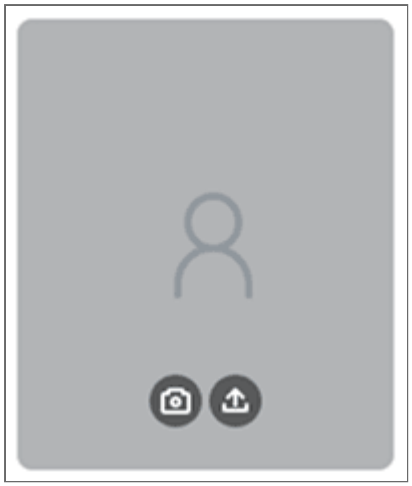
- Los dispositivos que pueden registrar rostros son los siguientes:
  - BioStation 3 Max
  - BioEntry W3
  - BioStation 3
  - FaceStation F2
- Si la tasa de autenticación facial es baja, elimina la información de rostro y registra un nuevo rostro.

Inscribir con una cámara web o una foto

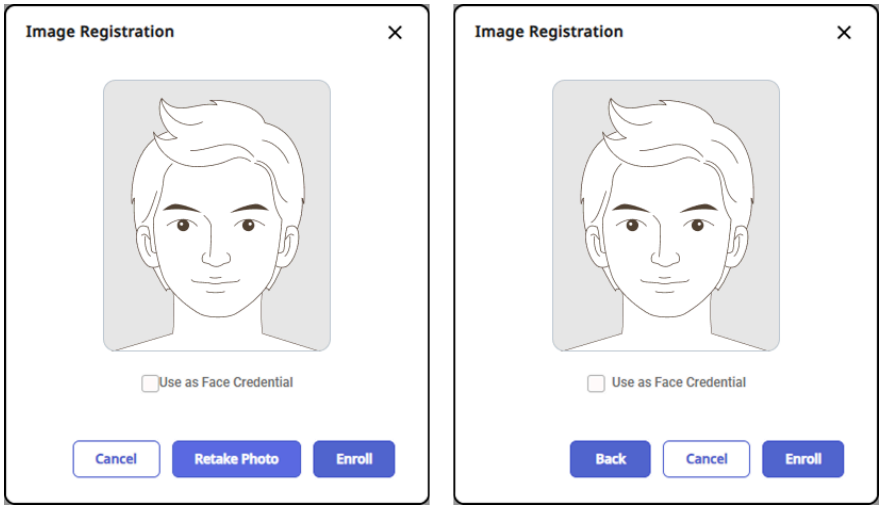
Toma una foto con una webcam conectada a tu PC, establece la foto capturada como imagen de perfil del usuario y registra el rostro como credencial. O registra la foto cargada como credencial de rostro.

1. Conecta la webcam al PC.
2. Coloca el cursor sobre el área de imagen de perfil en la parte superior derecha de la pantalla y haz clic en el botón que aparece.

   Para cargar una imagen guardada en tu PC, haz clic en el botón .



3. Cuando aparezca la ventana **Image Registration**, haz clic en **Take Photo** o **Upload Photo**.
4. Si tomas una foto con la webcam, se mostrará la foto; si cargas una foto desde el PC, se mostrará la foto cargada.



5. Para registrar la foto tomada con la webcam o la foto cargada como credencial de rostro, marca la casilla de la opción **Use as Face Credential**.

6. Haz clic en **Enroll** para completar el registro facial.

Información

- Si utilizas la webcam por primera vez, aparecerá una ventana emergente del navegador solicitando permiso para la cámara. Para utilizar la funcionalidad de la webcam, otorga permiso a la cámara del navegador.
- El proceso para permitir el acceso a la cámara puede variar según el navegador.
- Pueden transcurrir unos segundos desde que haces clic en **Take Photo** hasta que se toma la foto.
- Se recomienda usar Google Chrome versión 100 o superior.
- El tamaño máximo del archivo de imagen a cargar es de 10MB.
- Los formatos de imagen admitidos incluyen JPG, JPEG y PNG.
- Precauciones para registrar un rostro visual con una webcam
  - Mantén una distancia adecuada de la webcam.
  - Registra tu rostro de frente sin moverte.
  - No cambies tu expresión facial.
  - No uses mascarillas, sombreros ni parches para los ojos.
  - No inclines la cabeza hacia arriba ni hacia abajo.
  - No uses maquillaje pesado.
  - No cierres los ojos.
  - Asegúrate de que ambos hombros sean visibles.
  - Asegúrate de que no aparezcan dos rostros en la pantalla. Enrola a una persona a la vez.

Inscribir Tarjeta de Acceso

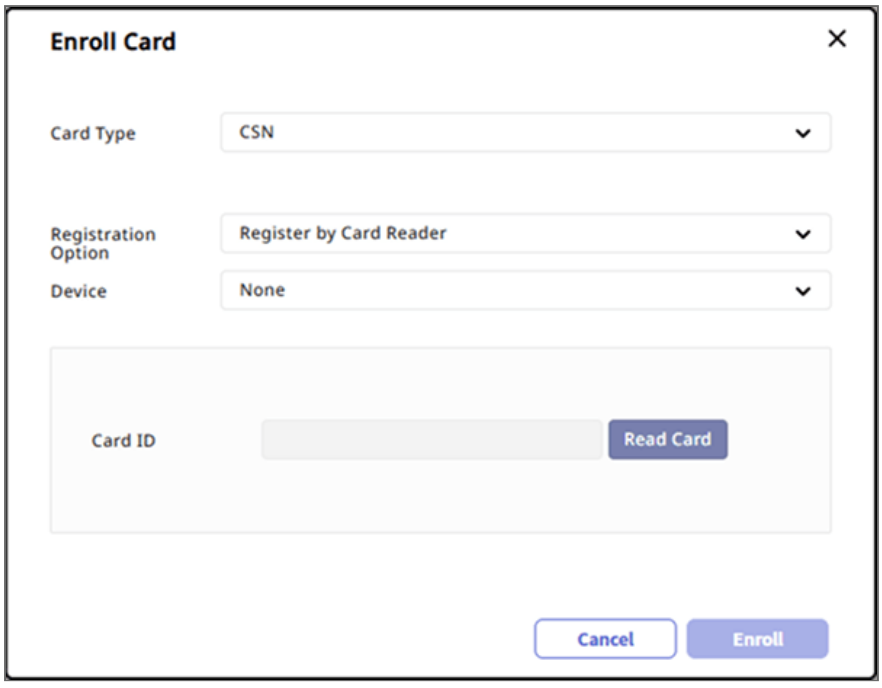
Guía a los usuarios sobre cómo registrar tarjetas de acceso. Explica los métodos de registro para tarjetas CSN, tarjetas Wiegand y tarjetas inteligentes, así como las funciones de lectura y formateo de tarjetas. Consulta el manual del dispositivo para conocer los tipos de tarjetas compatibles con el dispositivo.

Registro de tarjetas mediante un agente USB

Tipo Tarjeta	CSN	Wiegand	Tarjeta Inteligente
EM	✕	✕	✕
MIFARE	✓	✕	✓
DESFire	✓	✕	✓
FeliCa	✓	✕	✕
HID Prox	✕	✕	✕
HID iCLASS	✕	✕	✕

Tarjeta CSN

1. En la sección **Credential**, haz clic en el botón **+ Card**.
2. Cuando aparezca la ventana **Enroll Card**, selecciona **CSN** en las opciones de **Card Type**.

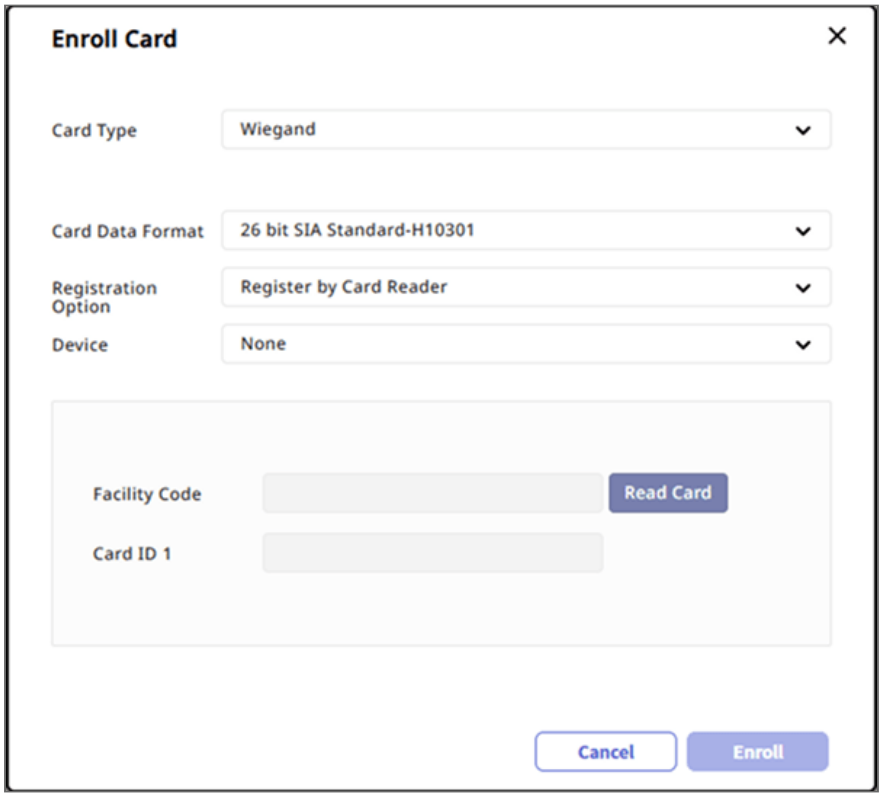


3. Selecciona el método de registro de tarjetas deseado en el campo **Registration Option**.
   - **Register by Card Reader**: Selecciona el dispositivo de la lista **Device** para escanear la tarjeta y haz clic en el botón **Read Card**.
   - **Assign Card**: Selecciona de la lista la tarjeta que deseas asignar al usuario. Busca en el campo de entrada.
   - **Enter Manually**: Ingresa el número de tarjeta manualmente o haz clic en el botón **Use User ID**.

4. Haga clic en **Enroll**.

Tarjeta Wiegand

1. En la sección **Credential**, haz clic en el botón **+ Card**.
2. Cuando aparezca la ventana **Enroll Card**, selecciona **Wiegand** en las opciones de **Card Type**.



3. Selecciona el formato deseado en el campo **Card Data Format**.
4. Selecciona el método de registro de tarjetas deseado en el campo **Registration Option**.
   - **Register by Card Reader**: Selecciona el dispositivo de la lista **Device** para escanear la tarjeta y haz clic en el botón **Read Card**.
   - **Assign Card**: Selecciona de la lista la tarjeta que deseas asignar al usuario. Busca en el campo de entrada.
   - **Enter Manually**: Ingresa manualmente el código de instalación y el ID de la tarjeta.
5. Haga clic en **Enroll**.

> **Información**
> Si el formato de datos de la tarjeta que desea no está disponible en las opciones de **Card Data Format**, consulte Configurar Formato de Tarjeta Wiegand.

Tarjeta inteligente

Inscriba una tarjeta access-on, una tarjeta de credencial segura o una tarjeta inteligente personalizada.

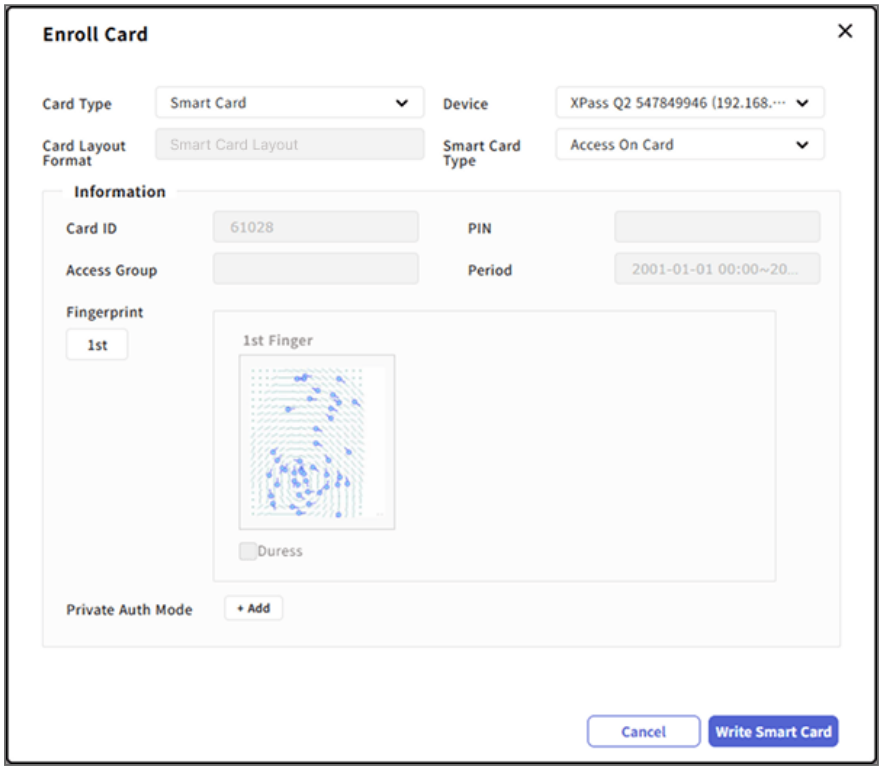
Información

- Para emitir una tarjeta inteligente, se debe configurar el tipo de tarjeta correcto. Para obtener más información sobre los formatos de tarjeta, consulte Configurar Formato de Tarjeta Inteligente.
- La información del usuario almacenada en la tarjeta inteligente utiliza la información almacenada en **BioStar X**. Si no se almacena la información actualizada del usuario, puede que se almacene información incorrecta en la tarjeta inteligente. Además, si la información de usuario actualizada no se sincroniza con el dispositivo, este podría no realizar la autenticación.
- Para usar una plantilla facial, selecciona **Use Face Template** en la sección **Layout** al agregar una nueva tarjeta inteligente en el menú **Settings** → **Credential** → **Card Format**. Para obtener más información sobre el diseño de la tarjeta, consulte Configurar Formato de Tarjeta Inteligente.
- Consulte Configuración de Autenticación para configurar el diseño de la tarjeta inteligente en el dispositivo.
- Consulte Leer/formatear tarjeta para formatear la tarjeta inteligente y reescribir sus datos.

Access On Card

Seleccione **Access On Card** para almacenar información del usuario en la tarjeta. Incluye el ID de tarjeta, el PIN, el grupo de acceso, el período, la plantilla de huella digital, la plantilla facial y el modo de autenticación personal.

1. En la sección **Credential**, haz clic en el botón **+ Card**.
2. Cuando aparezca la ventana **Enroll Card**, selecciona **Smart Card** en las opciones de **Card Type**.
3. Selecciona el dispositivo para el registro de tarjetas en el campo **Device**.
4. Una vez seleccionado, aparecerá el formato de diseño de tarjeta configurado en el campo **Card Layout Format**.
5. Seleccione **Access On Card** en las opciones de **Smart Card Type**.



6. Seleccione una plantilla de huella digital si está disponible. Si no tiene una plantilla disponible, omita este paso.

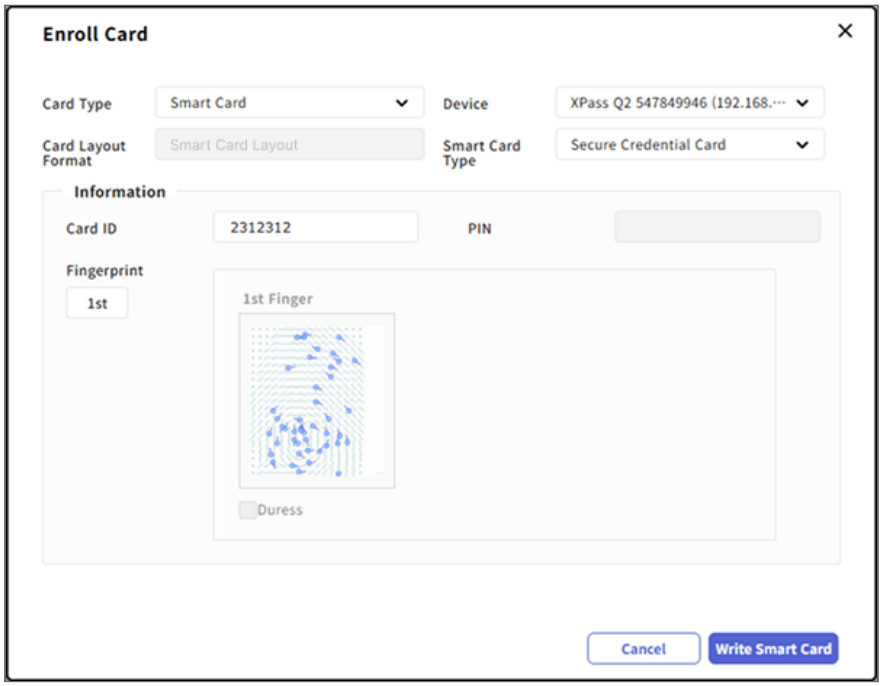
7. Haz clic en el botón **Write Smart Card**.

> **Información**
> Access On Card no puede configurar el ID de la tarjeta manualmente.

Secure Credential Card

Seleccione **Secure Credential Card** para almacenar información del usuario en la tarjeta. Incluye el ID de tarjeta, el PIN, la plantilla de huella digital y la plantilla facial.

1. En la sección **Credential**, haz clic en el botón **+ Card**.
2. Cuando aparezca la ventana **Enroll Card**, selecciona **Smart Card** en las opciones de **Card Type**.
3. Selecciona el dispositivo para el registro de tarjetas en el campo **Device**.
4. Una vez seleccionado, aparecerá el formato de diseño de tarjeta configurado en el campo **Card Layout Format**.
5. Seleccione **Secure Credential Card** en las opciones de **Smart Card Type**.



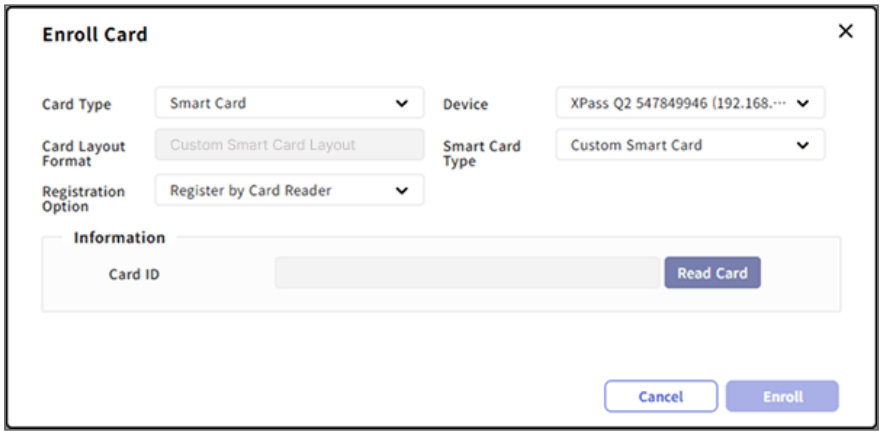
6. Ingrese directamente **Card ID**.
7. Seleccione una plantilla de huella digital o una plantilla facial si está disponible. Si no tiene una plantilla disponible, omita este paso.
8. Haz clic en el botón **Write Smart Card**.

Custom Smart Card

Seleccione **Custom Smart Card** para inscribir una tarjeta inteligente de terceros.

1. En la sección **Credential**, haz clic en el botón **+ Card**.
2. Cuando aparezca la ventana **Enroll Card**, selecciona **Smart Card** en las opciones de **Card Type**.

3. Selecciona el dispositivo para el registro de tarjetas en el campo **Device**.
4. Una vez seleccionado, aparecerá el formato de diseño de tarjeta configurado en el campo **Card Layout Format**.
5. Seleccione **Custom Smart Card** en las opciones de **Smart Card Type**.



6. Selecciona el método de registro de tarjetas deseado en el campo **Registration Option**.
   - **Register by Card Reader**: Selecciona el dispositivo de la lista **Device** para escanear la tarjeta y haz clic en el botón **Read Card**.
   - **Assign Card**: Selecciona de la lista la tarjeta que deseas asignar al usuario. Busca en el campo de entrada.
   - **Enter Manually**: Ingrese el número de tarjeta manualmente en formato de base 10 (decimal).
7. Haga clic en **Enroll**.

Información

Para los dispositivos y versiones de firmware que admiten Custom Smart Card, consulta la lista siguiente.

▼ **Ver dispositivos y versiones de firmware que admiten tarjetas inteligentes personalizadas**

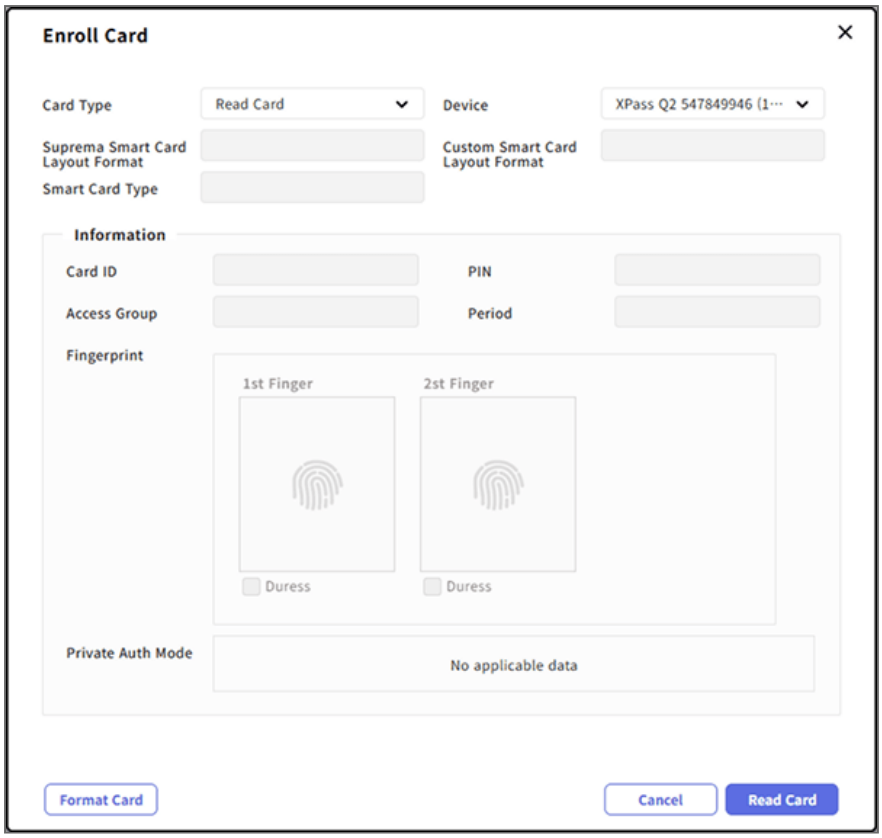
- Firmware de BioStation 3 Max, versión 1.0.0 o posterior
- Firmware de XPass Q2, versión 1.0.0 o posterior
- BioEntry W3 versión de firmware 1.0.0 o superior
- BioStation 2a versión de firmware 1.1.0 o superior
- BioStation 3 versión de firmware 1.3.0 o superior
- X-Station 2 versión de firmware 1.3.0 o superior
- BioLite N2 versión de firmware 1.6.2 o superior
- XPass D2 versión de firmware 1.7.1 o superior
- BioEntry P2 versión de firmware 1.5.1 o superior
- BioEntry W2 versión de firmware 1.8.0 o superior

Leer/formatear tarjeta

Formatea tarjetas inteligentes y reescribe información.

1. En la sección **Credential**, haz clic en el botón **+ Card**.

2. Cuando aparezca la ventana **Enroll Card**, selecciona **Read Card** en las opciones de **Card Type**.

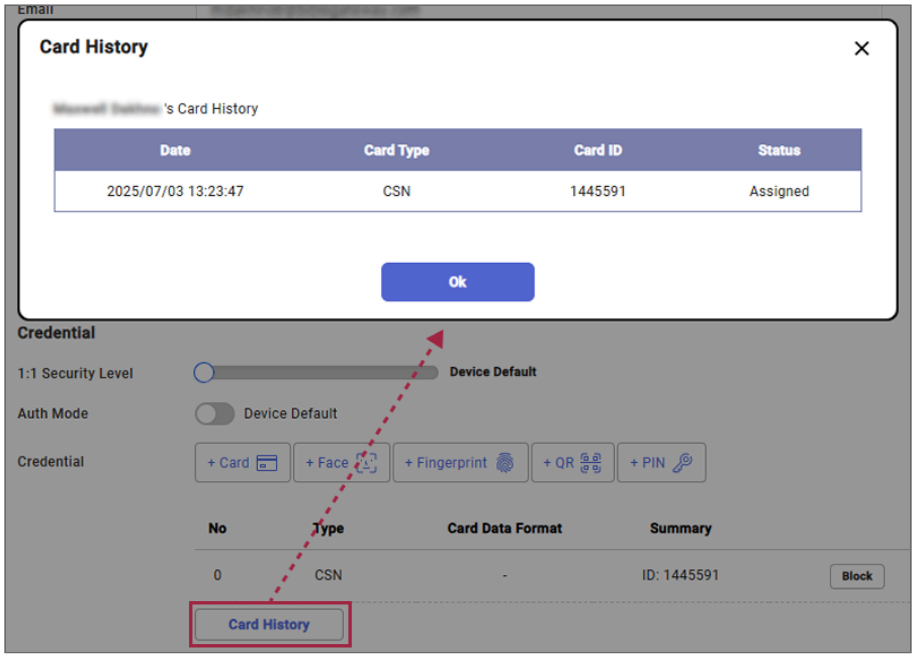


3. Selecciona en el campo **Device** el dispositivo capaz de leer tarjetas inteligentes.
4. Selecciona **Smart Card Type**.
5. Haz clic en el botón **Read Card**.
6. Verifica la información de la tarjeta y haz clic en el botón **Format Card**.

> **Información**
>
> - La lista de dispositivos en el campo **Device** se muestra solo cuando se ha configurado el diseño de la tarjeta inteligente. Para obtener más información sobre esta configuración, consulte Configuración de Autenticación.
> - Las tarjetas inteligentes personalizadas no se pueden formatear.

Confirmación de información de tarjeta asignada

Para ver la información de la tarjeta asignada al usuario, haz clic en el botón **Card History** en la sección **Credential**. Revisa la fecha de asignación de la tarjeta, el tipo de tarjeta, el ID de la tarjeta y el estado.



Registrar Credenciales Móviles

La integración con el portal Airfob de Suprema permite emitir credenciales móviles a los usuarios. Los usuarios pueden registrar credenciales móviles de forma individual o usar la función de importación CSV para registrar a varios usuarios a la vez.

Debe ingresar el correo electrónico del usuario según el método de envío de credenciales móviles configurado en el portal Airfob.

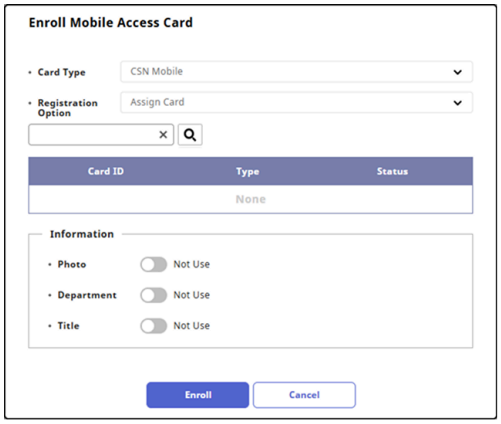
> **Información**
>
> - Solo se puede usar una de las dos opciones: **CSN Mobile Card** o **Template on Mobile**.
> - Esta función solo se puede usar cuando está vinculada con el portal Airfob. Para obtener más información sobre la integración con el portal de Airfob y el uso de las tarjetas de acceso móvil, consulte Administrar Tarjetas de Acceso Móvil.

CSN móvil

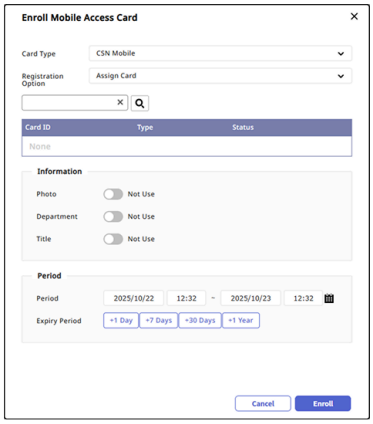
Puede emitir credenciales móviles CSN a los usuarios.

Asignación de tarjeta

1. Haga clic en **Mobile Access** en la sección **Credential**.
2. Cuando aparezca la ventana **Enroll Mobile Access Card**, seleccione la opción **Card Type** y elija **CSN Mobile**.
3. En las opciones de **Registration Option**, seleccione **Assign Card**.



Airfob portal site: Regular



Airfob portal site: Dynamic

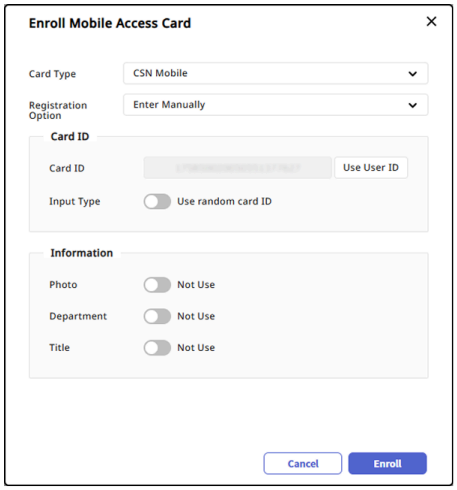
> El elemento **Period** se activa al configurar un sitio **Dinámico** durante la creación del sitio en el portal Airfob. Configura la duración de vencimiento y el período de uso de las Credenciales Móviles. Para obtener más información sobre el portal Airfob, consulta el siguiente enlace.

4. Seleccione o busque en la lista la tarjeta que desea asignar.
5. Configure **Info** y **Period**.
6. Haga clic en **Enroll**.

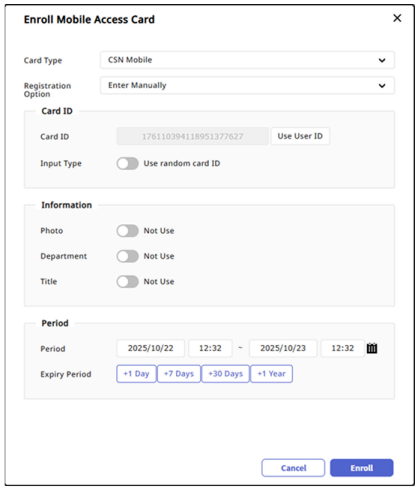
> **Información**
>
> - Si ha habilitado las opciones **Photo**, **Department** y **Title** en la sección **Info**, esa información puede mostrarse en la tarjeta de credenciales móviles del usuario. Los elementos que se muestran en este momento se basan en la información ingresada por el usuario. Para obtener más información sobre cómo ingresar la información básica del usuario, consulte Ingresar Información Básica del Usuario.
> - El sistema restringe la emisión si el nombre de usuario contiene caracteres especiales incompatibles con la tarjeta de acceso móvil. Solo se permiten `@` `-` `_` `+` `[` `]` `,` `.`.
> - Si el nombre de usuario incluye una comilla simple(`'`), aparece un aviso. El sistema envía el valor sin la comilla simple al guardar el usuario. Cuando aparece este aviso, el sistema ya creó el registro de la tarjeta. Cancelar el aviso detiene solo la transferencia al portal Airpop, y la tarjeta sigue inutilizable. En este caso, el sistema guarda el resto de la información del usuario sin vincular la tarjeta inutilizable.

Ingresar manualmente

1. Haga clic en **Mobile Access** en la sección **Credential**.
2. Cuando aparezca la ventana **Enroll Mobile Access Card**, seleccione la opción **Card Type** y elija **CSN Mobile**.
3. Seleccione **Enter Manually** en las opciones de **Registration Option**.



Airfob portal site: Regular



Airfob portal site: Dynamic

> El elemento **Period** se activa al configurar un sitio **Dinámico** durante la creación del sitio en el portal Airfob. Configura la duración de vencimiento y el período de uso de las Credenciales Móviles. Para obtener más información sobre el portal Airfob, consulta el siguiente enlace.

4. Seleccione **Input Type**.
   - **Use random card ID**: Genera automáticamente un ID de tarjeta.
   - **Use User ID**: Usa el ID de usuario como ID de tarjeta. Use esto solo cuando el ID de usuario sea numérico.
   - **Enter manually**: Permite ingresar manualmente el ID de tarjeta.
5. Configure **Info** y **Period**.
6. Haga clic en **Enroll**.

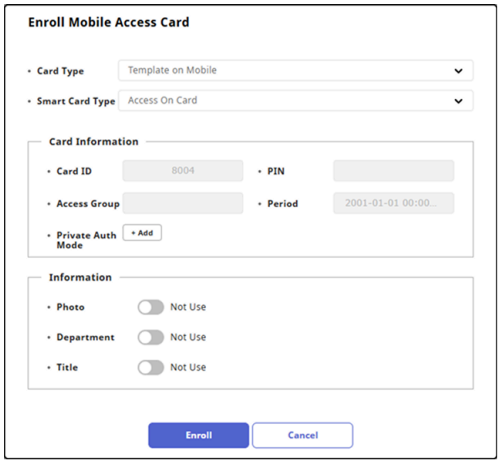
> **Información**
>
> - Si ha habilitado las opciones **Photo**, **Department** y **Title** en la sección **Info**, esa información puede mostrarse en la tarjeta de credenciales móviles del usuario. Los elementos que se muestran en este momento se basan en la información ingresada por el usuario. Para obtener más información sobre cómo ingresar la información básica del usuario, consulte Ingresar Información Básica del Usuario.
> - El sistema restringe la emisión si el nombre de usuario contiene caracteres especiales incompatibles con la tarjeta de acceso móvil. Solo se permiten `@` `-` `_` `+` `[` `]` `,` `.`.
> - Si el nombre de usuario incluye una comilla simple(`'`), aparece un aviso. El sistema envía el valor sin la comilla simple al guardar el usuario. Cuando aparece este aviso, el sistema ya creó el registro de la tarjeta. Cancelar el aviso detiene solo la transferencia al portal Airpop, y la tarjeta sigue inutilizable. En este caso, el sistema guarda el resto de la información del usuario sin vincular la tarjeta inutilizable.
> - Si el usuario perdió o eliminó el enlace de activación enviado por correo electrónico, haga clic en el botón **Reenviar** para volver a emitir el enlace de activación.
> - Para obtener más información sobre la aplicación móvil CSN, consulte el siguiente enlace.

Template on Mobile

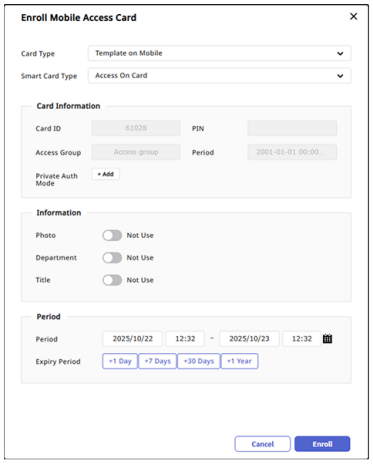
Template on Mobile es una credencial móvil que almacena la plantilla biométrica del usuario en un dispositivo móvil. Autentica biométricamente sin almacenar los datos del usuario en el servidor **BioStar X**, el portal Airfob ni en el dispositivo.

Esta función es útil para entornos que desean usar biometría como credencial pero no pueden almacenar información biométrica en el servidor ni en el dispositivo por motivos de privacidad. Como la emisión de **Template on Mobile** y el proceso de registro de la plantilla biométrica se realizan por separado, los usuarios pueden registrar su rostro directamente en dispositivos compatibles con **Template on Mobile** sin interactuar con un administrador.

1. Haga clic en **Mobile Access** en la sección **Credential**.
2. Cuando aparezca la ventana **Enroll Mobile Access Card**, seleccione la opción **Card Type** y elija **Template on Mobile**.



Airfob portal site: Regular



Airfob portal site: Dynamic

> El elemento **Period** se activa al configurar un sitio **Dinámico** durante la creación del sitio en el portal Airfob. Configura la duración de vencimiento y el período de uso de las Credenciales Móviles. Para obtener más información sobre el portal Airfob, consulta el siguiente enlace.

3. Seleccione el tipo de tarjeta deseado en **Smart Card Type**.
   - **Access On Card**: La información del usuario (ID de tarjeta, PIN, grupo de acceso, duración, modo de autenticación privada) puede almacenarse en la tarjeta.
   - **Secure Credential Card**: Tarjeta de credencial segura. Se pueden almacenar el ID de tarjeta del usuario y el PIN.
4. Configure **Info** y **Period**.
5. Haga clic en **Enroll**.

Se enviará un correo electrónico de emisión a la dirección de correo electrónico registrada del usuario. El usuario debe instalar la aplicación Airfob Pass mediante el enlace del correo electrónico para completar la emisión de **Template on Mobile**.

> **Consejo**
>
> **Cómo autenticarse con Template on Mobile**
>
> El usuario acerca el dispositivo móvil que contiene **Template on Mobile** al dispositivo de autenticación y sigue las indicaciones en pantalla para autenticar su rostro.

Información

- Si ha habilitado las opciones **Photo**, **Department** y **Title** en la sección **Info**, esa información puede mostrarse en la tarjeta de credenciales móviles del usuario. Los elementos que se muestran en este momento se basan en la información ingresada por el usuario. Para obtener más información sobre cómo ingresar la información básica del usuario, consulte Ingresar Información Básica del Usuario.
- El sistema restringe la emisión si el nombre de usuario contiene caracteres especiales incompatibles con la tarjeta de acceso móvil. Solo se permiten `@` `-` `_` `+` `[` `]` `,` `.`.
- Si el nombre de usuario incluye una comilla simple(`'`), aparece un aviso. El sistema envía el valor sin la comilla simple al guardar el usuario. Cuando aparece este aviso, el sistema ya creó el registro de la tarjeta. Cancelar el aviso detiene solo la transferencia al portal Airpop, y la tarjeta sigue inutilizable. En este caso, el sistema guarda el resto de la información del usuario sin vincular la tarjeta inutilizable.
- Para obtener información sobre los dispositivos y las versiones de firmware que admiten **Template on Mobile**, consulte la siguiente lista.
  - Firmware de BioStation 3 Max, versión 1.0.0 o posterior
  - BioEntry W3 versión de firmware 1.0.0 o superior
  - BioStation 3 versión de firmware 1.2.0 o superior
  - FaceStation F2 versión de firmware 2.2.0 o superior
- Solo se puede emitir una credencial móvil: **CSN mobile card** o **Template on Mobile**.

Inscribir QR/código de Barras

Guía para registrar códigos QR o códigos de barras como métodos de autenticación de usuario. Inscriba los códigos QR generados directamente por **BioStar X** y los códigos QR/códigos de barras emitidos externamente.

Información

- Los dispositivos que pueden usar la autenticación con QR/Barcode mediante el escáner son los siguientes.
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- Los dispositivos que pueden usar la autenticación con QR/Barcode mediante la cámara son los siguientes.
  - Firmware de BioStation 3 Max, versión 1.0.0 o posterior
  - Firmware de XPass Q2, versión 1.0.0 o posterior
  - Versión de firmware 1.1.0 o posterior para BioStation 3
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) versión de firmware 1.2.0 o superior
  - X-Station 2 (XS2-QDPB, XS2-QAPB) versión de firmware 1.4.1 o superior
- Se requiere una licencia de dispositivo independiente para utilizar la autenticación mediante QR/código de barras con una cámara. Para obtener más información, consulte Licencia de dispositivo.

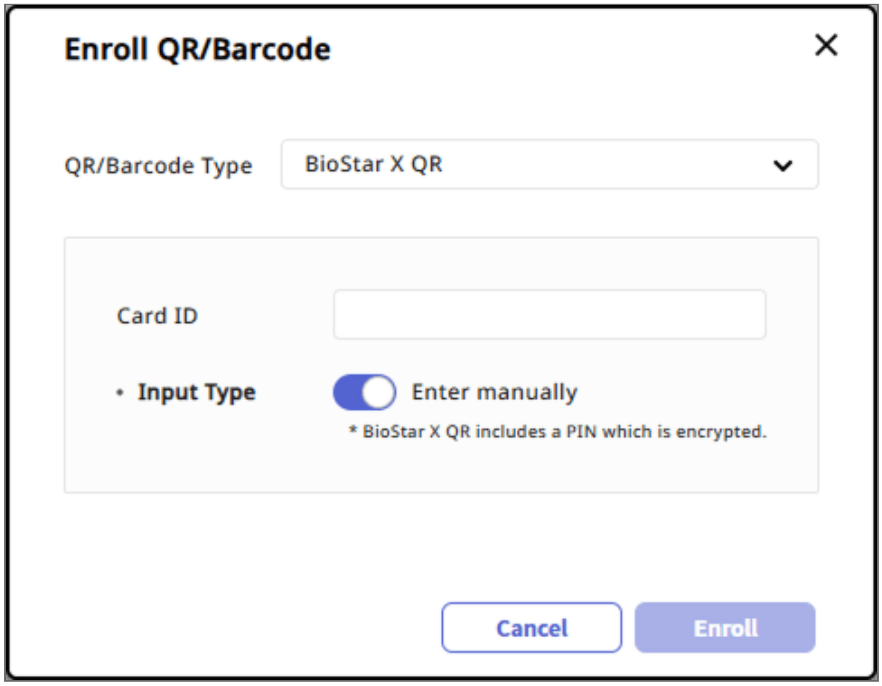
BioStar X QR

Emita un código QR que contenga un PIN cifrado para permitir el acceso del usuario.

Antes de comenzar

- Complete la configuración de la información de correo electrónico, incluida la configuración SMTP, antes de usar **BioStar QR**. Para obtener más información, consulta Configuración de Correo Electrónico.
- Para emitir **BioStar QR**, debe registrar una dirección de correo electrónico en la información del usuario. Para obtener más información, consulte Ingresar Información Básica del Usuario.

1. Haga clic en **+ QR/Barcode** en la sección **Credential**.
2. Cuando aparezca la ventana **Enroll QR/Barcode**, seleccione **BioStar QR** en **QR/Barcode Type**.



3. Seleccione **Input Type**.
   - **Use random card ID**: Genera automáticamente un ID de tarjeta.
   - **Enter manually**: Ingrese el ID de la tarjeta manualmente.
4. Haga clic en **Enroll**.

Luego, cuando un usuario se autentica, se emiten códigos QR y se envían a la dirección de correo electrónico registrada en la información del usuario. El usuario puede escanear el código QR incluido en el correo electrónico en el dispositivo para obtener acceso.

Información

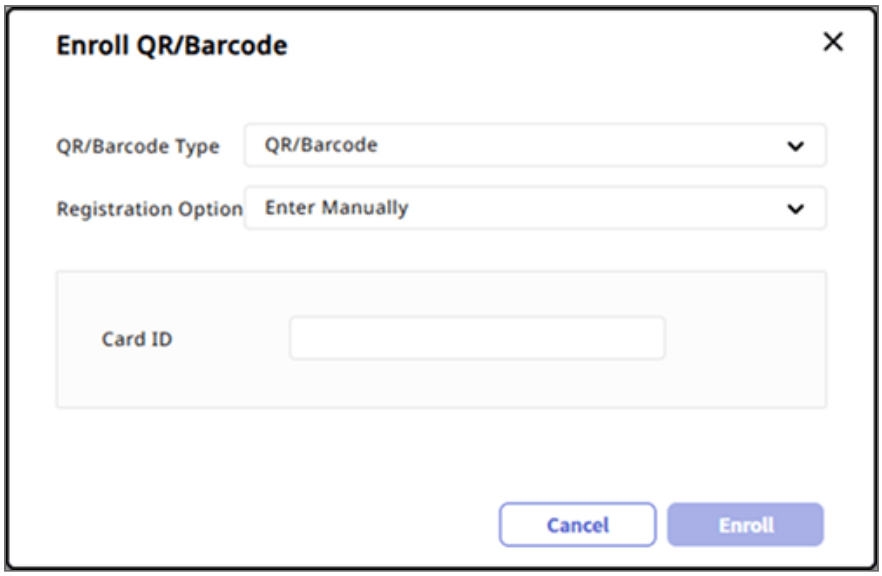
Para evitar la creación de ID de tarjeta duplicados, se recomienda configurar **Input Type** en **Use random card ID**.

QR/código de barras

Registre un código QR/código de barras emitido por emisores externos para los usuarios.

1. Haga clic en **+ QR/Barcode** en la sección **Credential**.

2. Cuando aparezca la ventana **Enroll QR/Barcode**, seleccione **QR/Barcode** en las opciones de **QR/Barcode Type**.



3. Seleccione **Enter Manually** en las opciones de **Registration Option**.
4. Introduzca directamente el ID del código QR/código de barras emitido previamente en la opción **Card ID**.
5. Haga clic en **Enroll**.

> **Información**
> En la opción **Card ID**, puede ingresar hasta 32 caracteres, incluidas letras en inglés, números y caracteres especiales.

Inscribir PIN

Guíe al usuario sobre cómo inscribir un PIN para que pueda acceder ingresándolo en el dispositivo. Inscriba un PIN para usuarios individuales o inscriba a varios usuarios en lote mediante la importación CSV.

Inscribir PIN

1. Haga clic en **PIN** en la sección **Credential**.



2. Cuando se active el campo de entrada, ingrese la contraseña.
3. Ingrese la misma contraseña en **Confirm PIN**.

4. Haga clic en **Enroll**.

> **Información**
>
> - El PIN debe tener una longitud de 4~16 dígitos y contener solo números.
> - Inscriba como máximo una credencial de PIN por usuario.

Inscribir PIN mediante importación CSV

Use la función de importación CSV para inscribir a varios usuarios a la vez.

1. Agregue una columna `pin` al archivo CSV que se importará.
2. Ingrese el PIN del usuario en la columna `pin` y guarde el archivo CSV.
3. Vaya a la página **User**.
4. Haz clic en ••• en la parte superior derecha de la pantalla y selecciona **Import** → **CSV**.
5. Siga las indicaciones en pantalla para seleccionar el archivo CSV y configurar las opciones de importación.

> **Información**
>
> - Inscriba como máximo una credencial de PIN por usuario.
> - Para obtener más información sobre la función de importación de archivos CSV, consulte Exportar/Importar Información de Usuarios.

Configurar Permisos de Usuario

De acuerdo con la política de seguridad de la organización, puede diferenciar los privilegios operativos específicos del usuario y los permisos de acceso para **BioStar X**. Restrinja el acceso a los menús principales mediante niveles de administrador y controle el acceso a los espacios físicos mediante grupos de acceso. También puede mejorar la seguridad mediante restricciones de dirección IP y autenticación multifactor.

Ve a la página **Launcher** → **User** y establece permisos de acceso con los dos métodos siguientes.

- **Nuevo usuario**: Haz clic en **New User** en la esquina superior derecha de la pantalla. Aparece la ventana **New User**.
- **Usuario existente**: Haz doble clic en un usuario de la lista de usuarios. O haz clic en el usuario y luego haz clic en **See More** en la pantalla de vista previa que aparece en el lado derecho de la pantalla. Aparece una ventana para editar la información del usuario.

En la sección **Permission**, se pueden configurar los siguientes elementos. Consulte las descripciones de cada elemento para configurar los permisos de usuario adecuados.



Seleccione el nivel de administrador

Los menús accesibles se limitarán según el nivel de administrador seleccionado. Seleccione el nivel de administrador del usuario en la sección **Permission**, bajo el elemento **Account Level**. Consulte la siguiente lista para conocer los niveles de administrador que se pueden asignar a los usuarios.

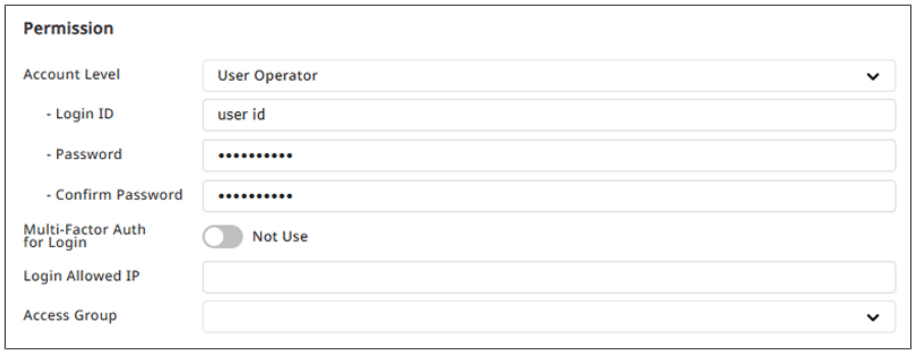
- **Administrator**: Este es un nivel de administrador que puede usar todos los menús.
- **User Operator**: El menú **User** tiene permisos de **lectura** y **edición**. Otros grupos de ajustes no tienen permisos, excepto el menú **User**.
- **Monitoring Operator**: Los menús **Monitoring** y **Data** tienen permisos de **lectura** y **edición**, y el menú **Dashboard** tiene permiso de **lectura**.
- **T&A Operator**: El menú **TIME ATTENDANCE** tiene permisos de **lectura** y **edición**, y el menú **User** tiene permiso de **lectura**.
- **Visitor Operator**: El menú **VISITOR** tiene permisos de **lectura** y **edición**.

Información

- Seleccione **None** si no desea establecer un nivel de administrador. En este caso, el usuario no puede iniciar sesión en **BioStar X**.
- El permiso de **edición** del menú **Monitoring** permite agregar pestañas o controlar las entradas del árbol de estado.
- El permiso de **edición** del menú **Data** permite guardar informes, agregar programaciones automáticas de informes y acceder a los ajustes.
- Para obtener más información sobre cómo agregar permisos de usuario personalizados, consulte Agregar Permisos Personalizados.
- Los permisos de las cuentas predeterminadas no se pueden modificar ni eliminar.
- Niveles como **T&A Operator** y **Visitor Operator** requieren licencias por separado. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Configurar ID de inicio de sesión y contraseña

Si seleccionó un nivel de administrador, debe establecer el ID y la contraseña que se utilizarán cuando el usuario inicie sesión en **BioStar X**.



Información

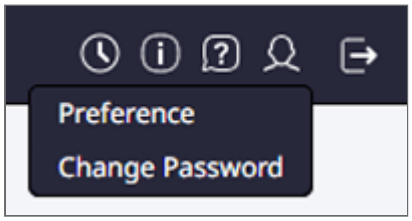
Precauciones al establecer ID y contraseña

- Establezca el ID como una combinación de letras, números y un punto (.) de entre 8~32 caracteres. No utilice comillas simples (').
- Para obtener más información sobre cómo configurar las políticas de contraseñas, consulte Mejorar la Seguridad del Sistema.
- Evite usar contraseñas vulnerables en términos de seguridad.
  - Caracteres o números consecutivos (por ejemplo, abcd, 1234)
  - Palabras o patrones comunes (por ejemplo, qwerty, password)

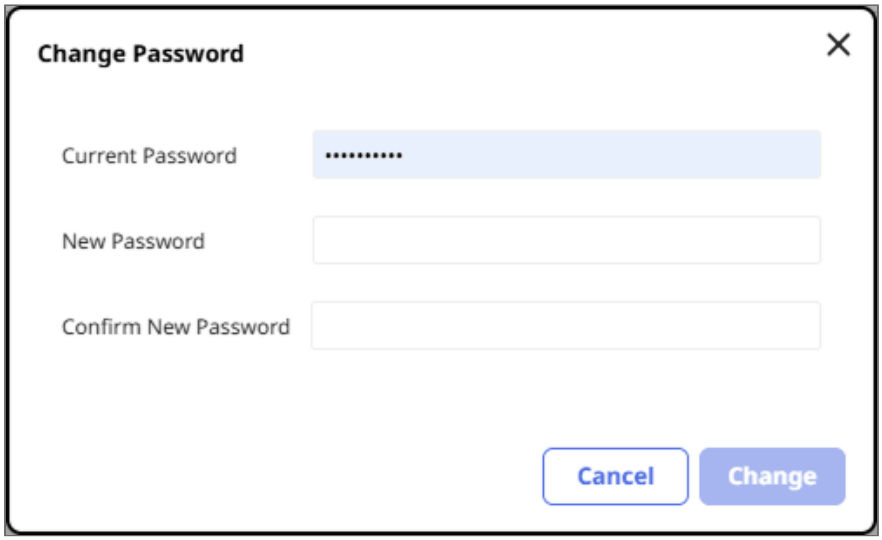
Cambiar la contraseña del usuario de inicio de sesión

Cambia tu contraseña después de iniciar sesión en **BioStar X**.

1. Inicia sesión en **BioStar X**.
2. Haz clic en en la esquina superior derecha de la pantalla.



3. Haz clic en **Change Password** en el menú desplegable.
4. Cuando aparezca la ventana **Change Password**, ingresa la contraseña actual y una nueva.



5. Después de ingresar todos los campos, haz clic en **Change**.

Configuración de autenticación de múltiples factores

Al habilitar **Multi-Factor Auth for Login**, los usuarios podrán iniciar sesión en **BioStar X** con autenticación de huella digital adicional.

> **Información**
> Para obtener más información sobre cómo configurar la **autenticación multifactor**, consulte Iniciar Sesión con Autenticación Multi-Factor.

Configuración de inicio de sesión con dirección IP del usuario

Si registra una dirección IP de usuario, solo podrá iniciar sesión en el PC cuando la información de IP coincida con la registrada en su cuenta. Esto mejora la seguridad. Ingrese la dirección IP del usuario en el campo **Login Allowed IP** de la sección **Permission**.

> **Información**
> - Las direcciones IP pueden introducirse en el formato xxx.xxx.xxx.xxx, y cada octeto debe contener un número en el rango de 0–255.
> - Si la dirección IP no está registrada, se permitirá el inicio de sesión en el PC independientemente de la información de IP.

Seleccione el grupo de acceso

Configure el grupo de acceso del usuario para restringir el acceso por organización o departamento. En la sección **Permission**, seleccione el grupo de acceso desde **Access Group**.

Información

Para obtener más información sobre cómo agregar y configurar grupos de acceso, consulte Administrar Grupos de Acceso.

Siguiente paso

En la sección **Advanced**, configure el mensaje que se mostrará en el dispositivo cuando el usuario acceda o excluya a ese usuario de la sincronización al vincular con Directory Service.
Consulte cómo editar la información del usuario.

Configura los Ajustes Avanzados del Usuario

Configura mensajes para que aparezcan en el dispositivo cuando el usuario ingrese o excluye al usuario de la sincronización durante Directory Service integration. Configura esta función al agregar o editar un usuario.

Ve a la página **Launcher** → **User** y establece permisos de acceso con los dos métodos siguientes.

- **Nuevo usuario**: Haz clic en **New User** en la esquina superior derecha de la pantalla. Aparece la ventana **New User**.
- **Usuario existente**: Haz doble clic en un usuario de la lista de usuarios. O haz clic en el usuario y luego haz clic en **See More** en la pantalla de vista previa que aparece en el lado derecho de la pantalla. Aparece una ventana para editar la información del usuario.

Configura los siguientes elementos en la sección **Advanced**.



- **Device Display Message**: Ingresa un mensaje que aparezca en el dispositivo cuando el usuario ingrese. Ingresa hasta 128 caracteres para el mensaje.
- **Exclude from Directory Integration**: Excluye al usuario de la sincronización durante la integración de Directory Service.

Información

- La opción **Exclude from Directory Integration** está disponible como complemento para licencias **Essential** o superiores. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.
- Para obtener más información sobre la configuración de la integración con directorios, consulte Configuración de Integración de Directorios.

Siguiente paso

Consulte cómo editar la información del usuario.

Inscribir Y Editar Usuarios Al Escanear Un ID

En lugar de ingresar los datos del usuario uno por uno, escanea un ID para obtener el nombre y la foto del ID del usuario y, luego, inscribe o edita al usuario.

Antes de comenzar

- Conecta el escáner de ID DESKO a la PC cliente para usar Escanear ID.
- Antes de inscribir a un usuario mediante un escaneo de ID, selecciona los datos que se obtendrán del ID. Para obtener más información sobre los ajustes de Escanear ID, consulta Configurar Escaneo De ID.

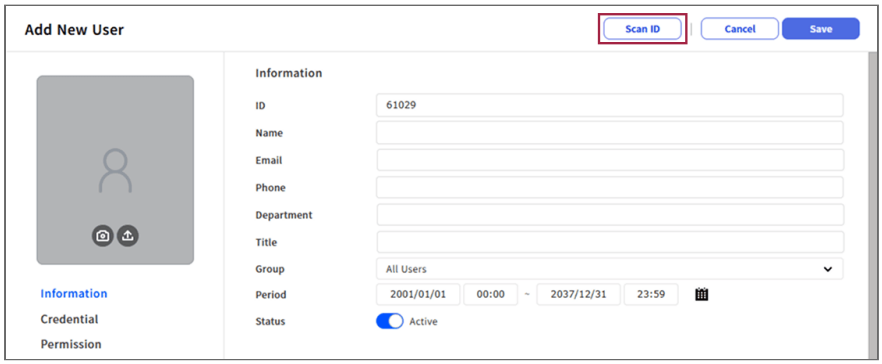
> **Información**
> La característica **Scan ID** actualmente solo admite escaneos de pasaporte.

Inscribir un usuario mediante un escaneo de ID

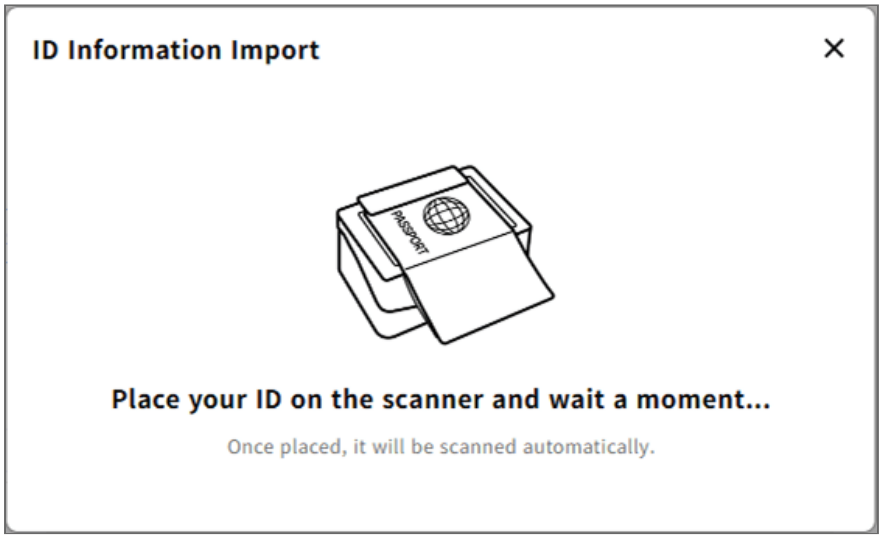
1. Haz clic en **User** en la página **Launcher**.
2. Haz clic en **New User** en la esquina superior derecha de la página **User**.



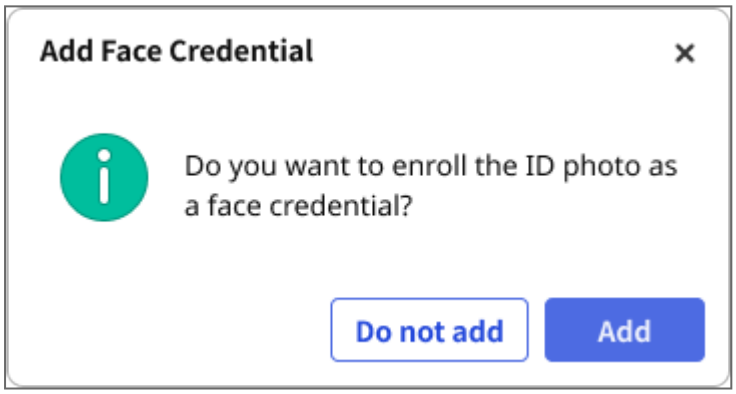
3. Haz clic en **Scan ID** en la esquina superior derecha de la pantalla **Add New User**.



4. Cuando aparezca la ventana **ID Information Import**, coloca el ID en el escáner.



5. Después de que aparezca el mensaje de escaneo de ID exitoso, selecciona si inscribes la foto del ID como credencial facial.

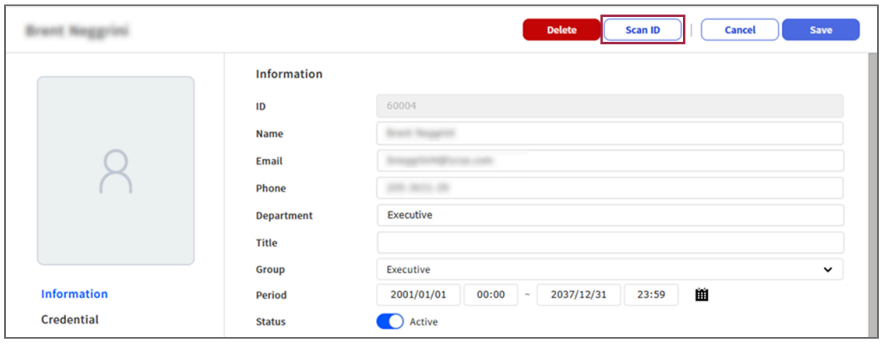


> Este mensaje aparece cuando **Face Credential** se establece en **Require Confirmation** en **Settings** → **Account** → **ID Scanning**. Si establece la opción **Do Not Ask**, este mensaje no aparece y el sistema inscribe la foto de inmediato como credencial facial.

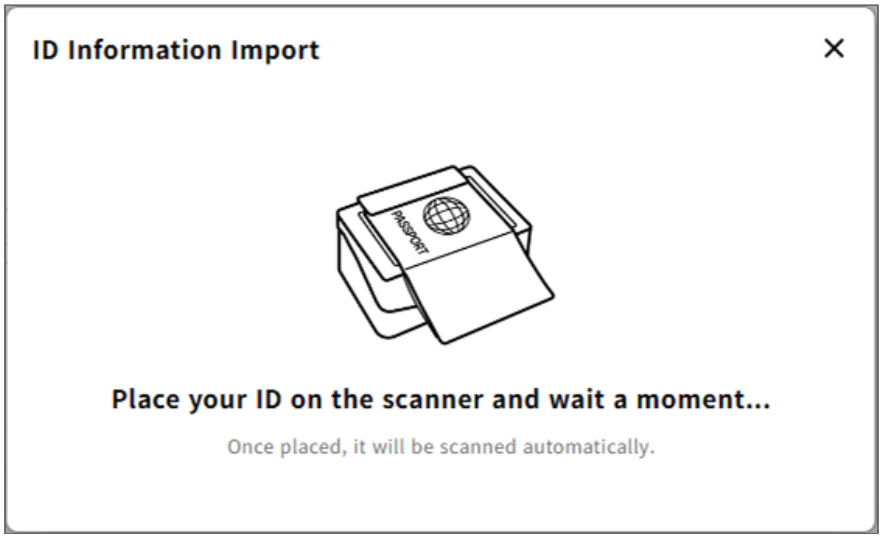
6. Revisa la información del escaneo de ID y edítala si es necesario.
7. Haz clic en **Save** en la esquina superior derecha de la pantalla para guardar al usuario.

Editar un usuario mediante un escaneo de ID

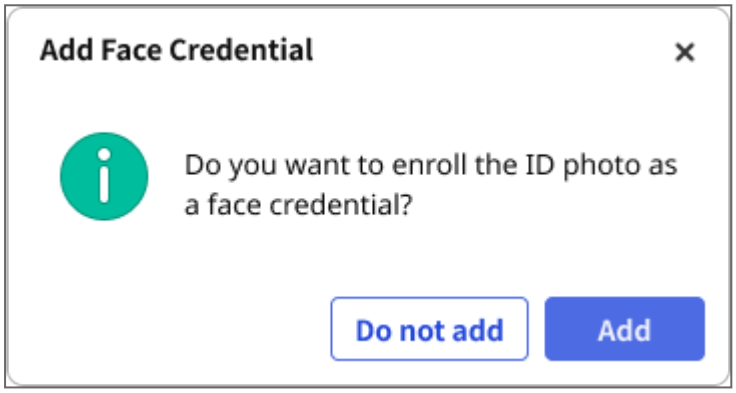
1. Haz clic en **User** en la página **Launcher**.
2. En la lista de usuarios, haz doble clic en el usuario para editarlo mediante un escaneo de ID.
3. Haz clic en **Scan ID** en la esquina superior derecha de la pantalla de edición de usuario.



4. Cuando aparezca la ventana **ID Information Import**, coloca el ID en el escáner.



5. Después de que aparezca el mensaje de escaneo de ID exitoso, selecciona si inscribes la foto del ID como credencial facial.



> Este mensaje aparece cuando **Face Credential** se establece en **Require Confirmation** en **Settings** → **Account** → **ID Scanning**. Si establece la opción **Do Not Ask**, este mensaje no aparece y el sistema inscribe la foto de inmediato como credencial facial.

6. Revisa la información del escaneo de ID y edítala si es necesario.

7. Haz clic en **Save** en la esquina superior derecha de la pantalla para guardar las actualizaciones del escaneo.

Información

Si el usuario tiene 2 o más credenciales faciales inscritas, la edición mediante un escaneo de ID sobrescribe la primera credencial facial inscrita.

Mensajes de error

Si ocurre un problema al escanear un ID, el sistema muestra un mensaje con la causa y la solución. Usa la información a continuación para resolver el error.

Falló el escaneo

Si ocurre un problema cuando el sistema lee automáticamente el ID en el escáner, aparece uno de los siguientes mensajes.

Causa	Mensaje de error
Característica de seguridad del ID (patrón UV, etc.) la verificación falló	**Invalid ID. Check the ID and try again.**
El sistema no reconoció el ID dentro del tiempo especificado	**The ID was not scanned in time. Please try again.**
Otros errores de escaneo, como que el ID se mueva durante el escaneo o falle la detección de páginas	**Unable to scan the ID. Check the ID and scanner, then try again.**

Si aparece este mensaje, haga clic en **Retry** y escanee de nuevo. Comprueba que el ID esté colocado correctamente en el escáner y vuelve a intentarlo.

Información

Haga clic en **Retry** para reiniciar el reconocimiento automático siguiendo las instrucciones de **Place your ID on the scanner and wait a moment...**.

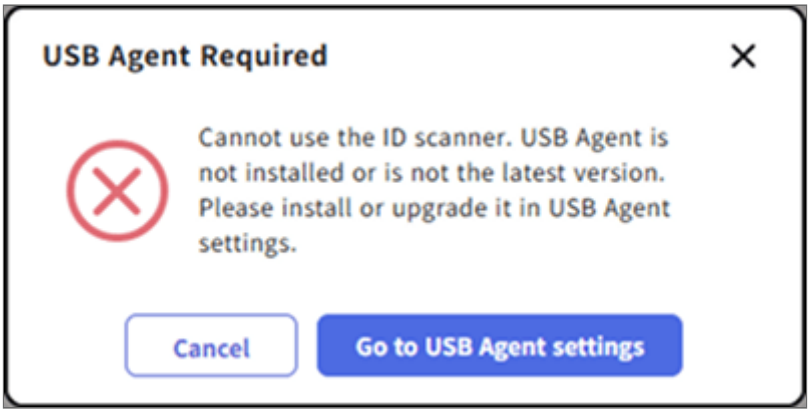
Error de conexión del escáner

Si falla la conexión del escáner, aparece el siguiente mensaje. Este error no incluye un botón para reintentar. Siga las instrucciones y, luego, haga clic en **Scan ID** de nuevo para iniciar el escaneo desde el principio.

Escenario	Mensaje de error	Solución
El escáner no está conectado a la PC cliente	**The scanner is not connected. Please check the device connection and try again.**	Verifique la conexión entre el Escáner de ID y la PC cliente.

Agente USB requerido

Instale la versión más reciente del Agente USB antes de usar el Escáner de ID. Si falta el Agente USB o está desactualizado, aparece un cuadro de diálogo de error después de hacer clic en el botón **Scan ID**.



- **Cancel**: Cierre la ventana de error y no escanee.
- **Go to USB Agent settings**: Vaya a **Settings** → **Device** → **USB Agent**. En esa pantalla, actualice el Agente USB a la versión más reciente y luego vuelva a escanear.

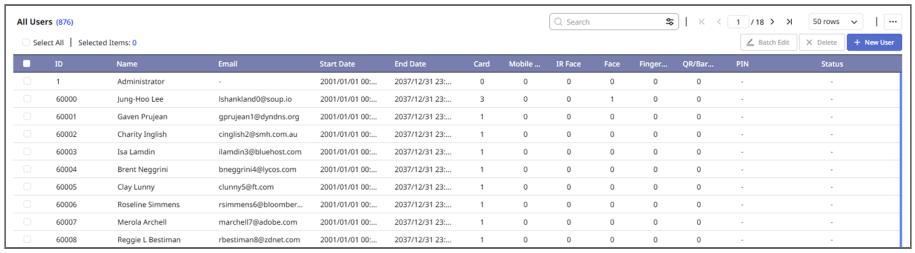
Explorar Usuarios

Esta guía explica cómo ver y administrar los usuarios registrados en la página de lista de usuarios. Busque rápidamente los usuarios deseados mediante búsquedas generales y avanzadas, y use funciones como el ordenamiento de listas, la configuración de columnas y la impresión.

Haga clic en **User** en el **Launcher** o seleccione **User** en el menú de la esquina superior izquierda de la pantalla para acceder a la página **User**.

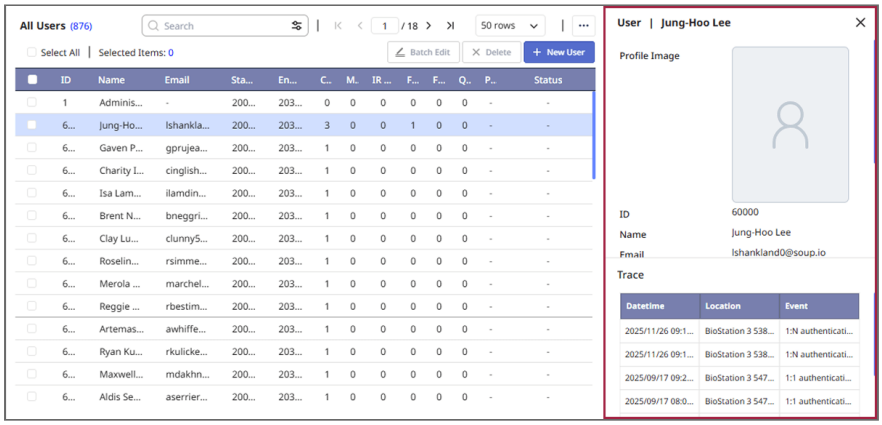
Ver lista de usuarios

En la página de lista de usuarios, consulte la información básica y el estado de los usuarios, y vea o edite la información detallada de cada uno.



La lista de usuarios muestra todos los usuarios registrados y permite verificar el ID, nombre, dirección de correo electrónico, duración y estado de las credenciales inscritas de cada usuario. Los usuarios se enumeran en orden según su ID.

- Haga clic en el usuario deseado en la lista para ver su información detallada. La información del perfil del usuario aparece en el lado derecho de la pantalla. Haga clic en **See More** en la información del perfil del usuario para ir a la página de edición de la información detallada.



- Haga doble clic en el usuario deseado de la lista para editar su información detallada. Vaya a la página de edición de la información detallada del usuario.

> **Información**
>
> - Para obtener más información sobre cómo editar la información del usuario, consulte Editar Información del Usuario.
> - Cambie el diseño de columnas en la lista de usuarios. Para obtener más información sobre cómo cambiar la disposición de las columnas, consulte Explorar Usuarios.

Seleccionar opciones de vista

Cambie las opciones de visualización de la lista de usuarios mediante el botón de herramientas en la esquina superior derecha de la pantalla.

Ir a la lista de usuarios

De forma predeterminada, la lista de usuarios muestra 10 usuarios. Haga clic en el botón en la parte superior de la pantalla para ir a otra página.



- |< : Ir a la primera página de la lista de usuarios.
- < : Ir a la página anterior de la lista de usuarios.
- > : Ir a la página siguiente de la lista de usuarios.
- >| : Ir a la última página de la lista de usuarios.
- Vaya a la página deseada, ingrese el número de página en el campo numérico y presione `Enter`.

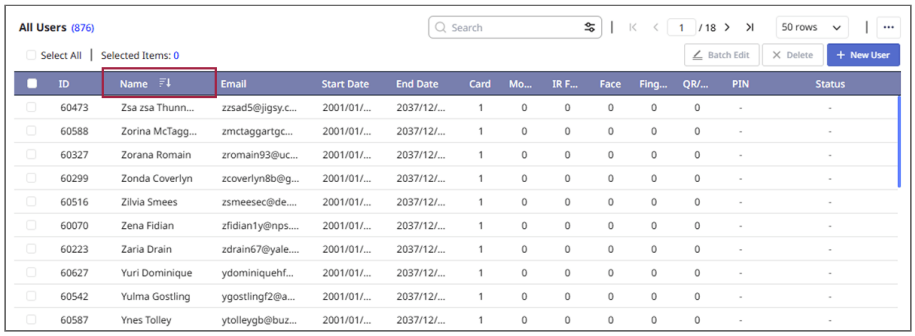
Cambiar la cantidad de usuarios mostrados en la lista

Cambie la cantidad de usuarios que se muestran en la lista. Seleccione la cantidad deseada de usuarios en el cuadro de lista de la esquina superior derecha de la pantalla. Las opciones disponibles son 50, 100 o 200 usuarios.



Ordenar lista de usuarios

Cambie el criterio de ordenamiento de la lista de usuarios. Haga clic en el encabezado de columna en la parte superior de la lista para ordenar en orden ascendente o descendente. Por ejemplo, al hacer clic en el encabezado **Name**, los nombres de los usuarios se ordenan en orden ascendente o descendente. El elemento seleccionado mostrará un ícono de ascendente ( ) o descendente ( ).



> **Información**
> Algunos elementos podrían no ordenarse según el tipo de columna.

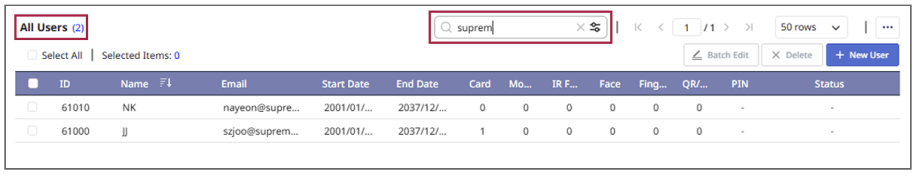
Buscar usuario

Ofrece orientación sobre cómo buscar usuarios específicos. Encuentre rápidamente a los usuarios deseados mediante la función de búsqueda en la página de lista de usuarios.

> **Información**
>
> - Los términos de búsqueda no distinguen mayúsculas de minúsculas.
> - La información básica del usuario debe ingresarse para buscarlos. Para obtener más información sobre cómo ingresar la información básica del usuario, consulte Ingresar Información Básica del Usuario.

Búsqueda general

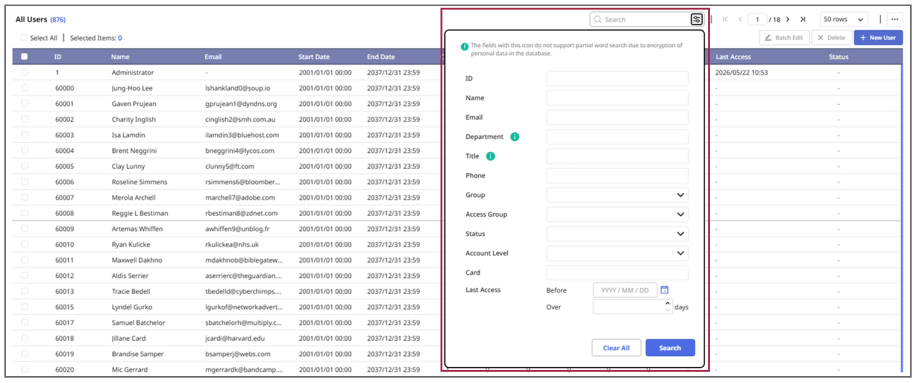
Busque por ID, nombre o correo electrónico del usuario. Introduzca las palabras clave en el campo de búsqueda en la parte superior de la pantalla y presione `Enter`. Los usuarios que coincidan con la palabra clave especificada aparecerán en la lista. Verifique la cantidad de resultados de búsqueda en la parte superior de la lista.



Búsqueda avanzada

Busque IDs de usuario, nombres, direcciones de correo electrónico, etc.

1. Haga clic en ⚙ junto al campo de búsqueda en la parte superior de la pantalla.
2. Cuando se abra la ventana de búsqueda avanzada, ingrese los criterios deseados y haga clic en **Search**.



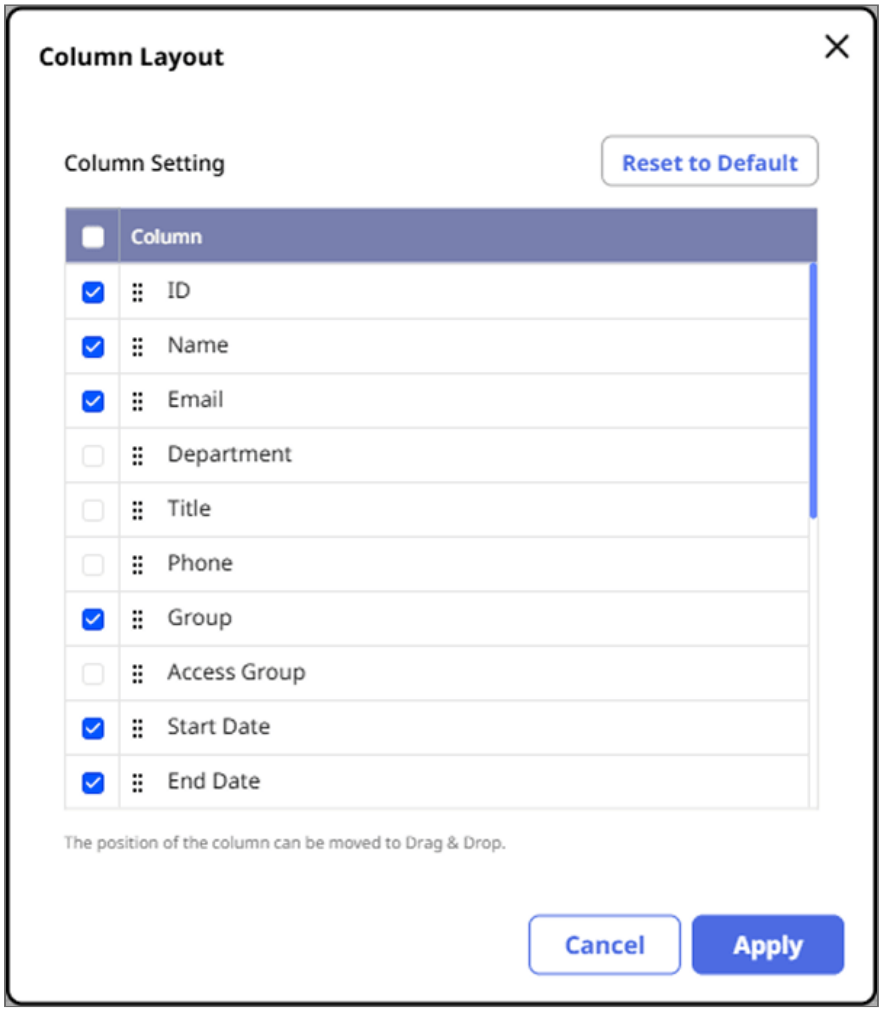
Información

- Los campos con el ícono ! no admiten búsqueda de palabras parciales debido al cifrado de datos personales en la base de datos.
- Para restablecer los criterios ingresados en la ventana de búsqueda avanzada, haga clic en **Clear All**.
- La búsqueda avanzada admite la búsqueda de **Custom User Field**. Para obtener más información sobre **Custom User Field**, consulte Configuración Detallada del Servidor.

Ajustes de columnas de la lista de usuarios

Cambie la configuración de columnas que se muestran en la lista de usuarios. En los ajustes de columnas, seleccione las columnas que aparecerán o cambie su orden.

1. Haga clic en ••• en la esquina superior derecha de la pantalla de la lista de usuarios.
2. Haga clic en **Column Layout**.
3. Cuando aparezca la ventana **Column Layout**, seleccione o deseleccione las columnas deseadas.



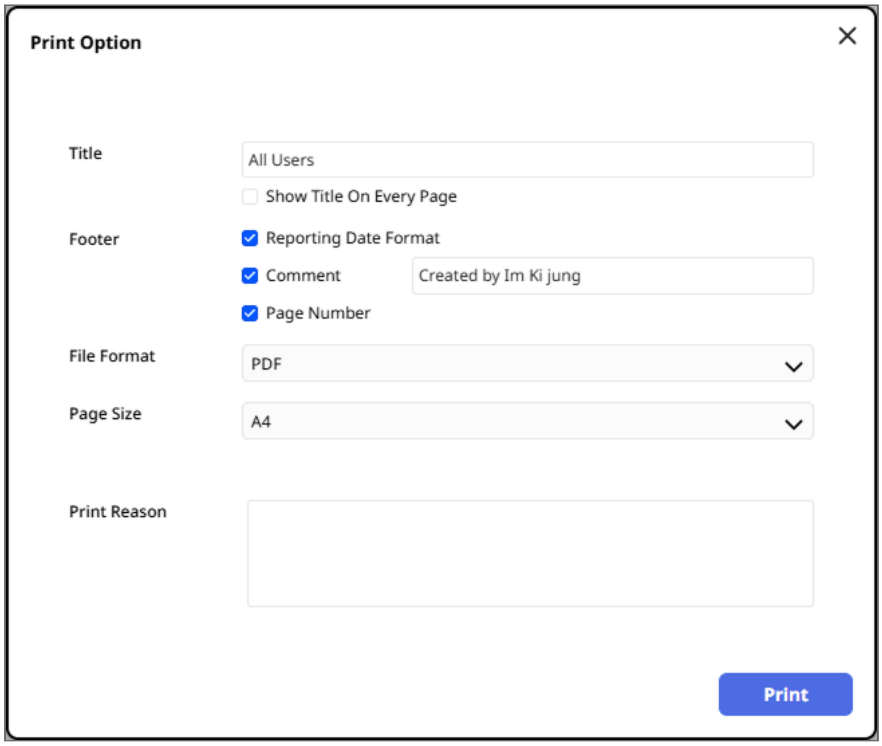
4. Haga clic y arrastre la columna deseada para cambiar su posición.
5. Haga clic en **Apply** para guardar la configuración.

> **Información**
>
> - La configuración de columnas se guarda para cada cuenta de usuario.
> - Haga clic en **Default Column** para restablecer el diseño de columnas.

Imprimir lista de usuarios

Guarde la lista de usuarios que está viendo como archivo PDF o SVG.

1. Haga clic en ••• en la esquina superior derecha de la pantalla de la lista de usuarios.
2. Haga clic en **Print**.
3. Cuando aparezca la ventana **Print Option**, seleccione el formato deseado en las opciones **File Format** y configure las demás opciones.



4. Ingresa **Print Reason** (opcional) y haz clic en **Print**.

Imprima el archivo PDF o SVG que se abre en el navegador.

> **Información**
> **Print Reason** es opcional. Verifique los registros de **Print Reason** en **Settings** → **Audit Trail** → **AC Audit Log**.

Administrar Usuarios

Guía cómo gestionar eficazmente a los usuarios registrados. Explica paso a paso las funciones clave necesarias para la gestión de usuarios, incluida la modificación y eliminación de información de usuario, la sincronización de datos con dispositivos, el seguimiento del historial de acceso y la exportación/importación de datos de usuario.

Editar Información del Usuario

Guía cómo modificar la información de usuarios registrados. Modifica la información básica, los permisos de acceso o las credenciales de usuarios individuales o edita en lote la información de varios usuarios.

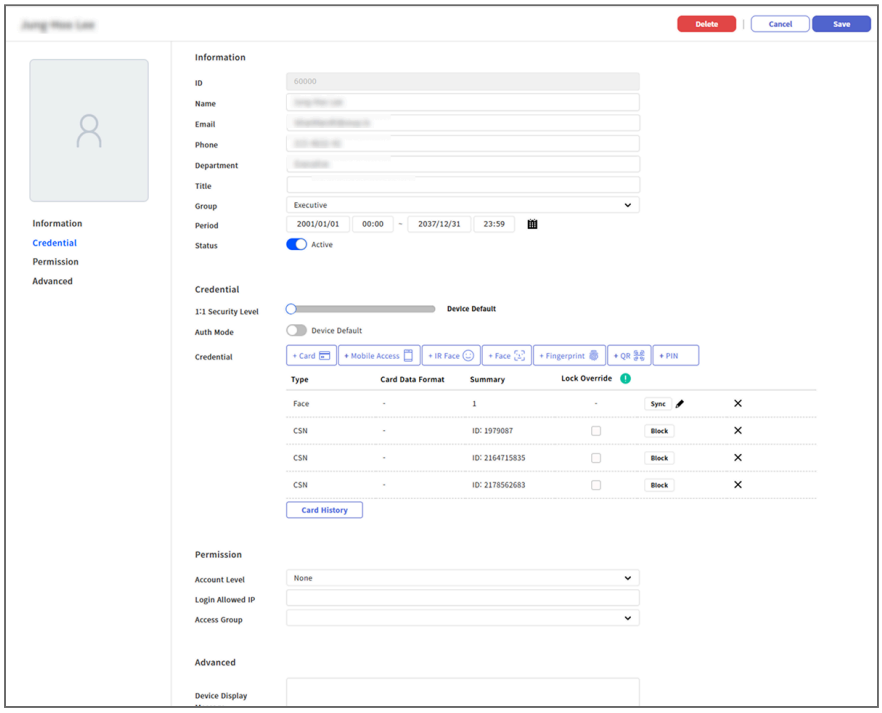
> **Información**
> Un usuario con el ID original `1` no puede ser modificado por otros administradores. Solo el usuario que ha iniciado sesión en esta cuenta puede modificar su propia información.

Editar información del usuario

1. Haz clic en **User** en la página **Launcher**.
2. Selecciona al usuario que deseas editar de la lista de usuarios.

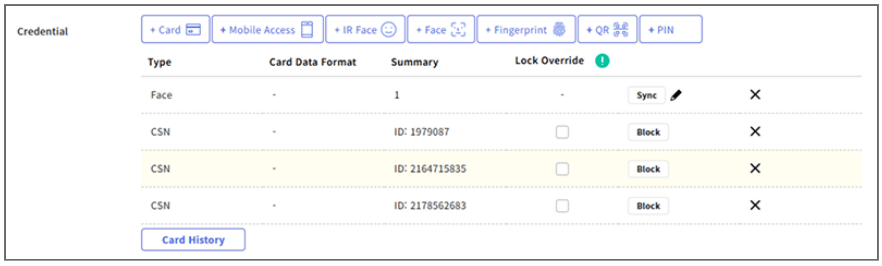
3. Haz doble clic en el usuario o haz clic en el botón **See More** cuando la información del perfil del usuario aparezca en el lado derecho de la pantalla.

4. Aparece una ventana para editar la información del usuario.



5. Modifique los elementos deseados.

6. Haz clic en el botón ✎ para modificar elementos de credenciales y en el botón ✕ para eliminarlos.



7. Para guardar los cambios, haz clic en **Save** en la esquina superior derecha de la pantalla.

Información

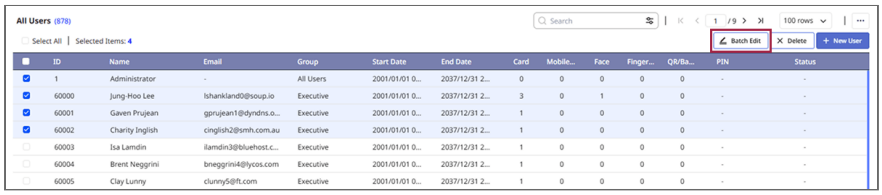
- Para obtener más información sobre cada campo de la sección **Information**, consulte Ingresar Información Básica del Usuario.
- Para obtener más información sobre cada campo de la sección **Credential**, consulte Registrar Credencial del Usuario.
- Para obtener más información sobre cada campo de la sección **Permission**, consulte Configurar Permisos de Usuario.
- Ingresa el mensaje personal del usuario en la sección **Advanced**.

Editar información del usuario por lotes

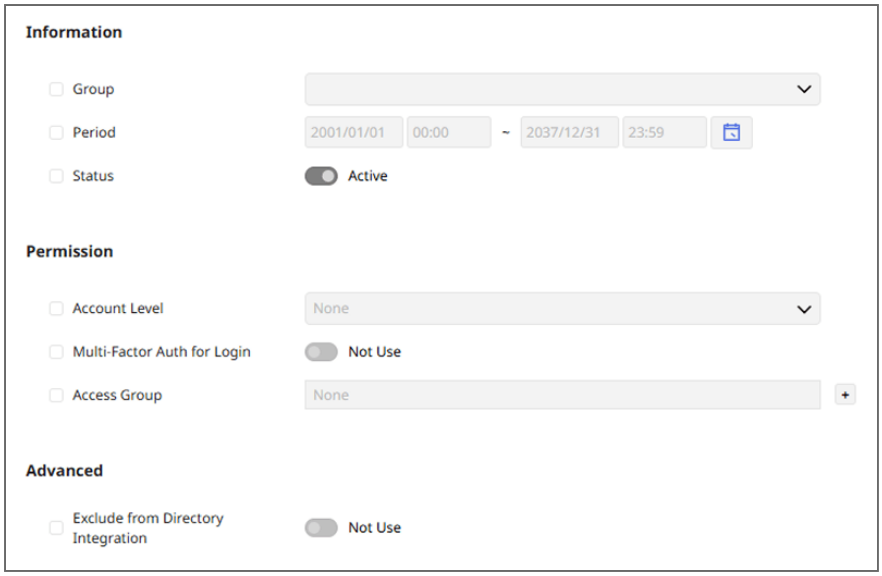
Edita la información o los permisos de acceso de varios usuarios a la vez. Esta función es útil al establecer los mismos

permisos de acceso o grupos para varios usuarios.

1. Haz clic en **User** en la página **Launcher**.
2. Haz clic en la casilla a la izquierda del usuario que deseas editar en la lista de usuarios. Selecciona dos o más usuarios.
3. Haz clic en **Batch Edit** en la esquina superior derecha de la pantalla.



4. Cuando aparezca la pantalla **Batch Edit**, marca la casilla del elemento deseado y realiza las modificaciones.



5. Haz clic en el botón **Save** en la esquina superior derecha de la pantalla para guardar la información editada.

> **Información**
>
> - El ID, nombre, correo electrónico, número de teléfono y credenciales del usuario no se pueden editar por lotes.
> - Haz clic en el botón **Cancel** en la esquina superior derecha de la pantalla para cancelar la información editada.

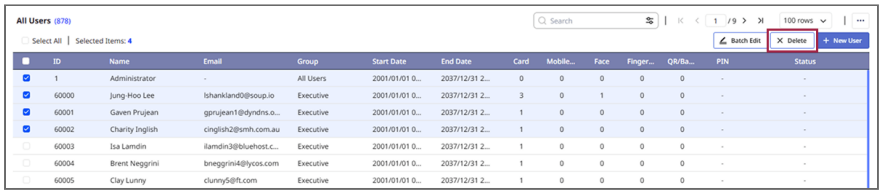
Siguiente paso

Enrola las credenciales del usuario y establece el método de autenticación de acceso.
Consulta cómo establecer los permisos de acceso del usuario.
Si cambiaste la información del usuario, envíala al dispositivo. Consulta cómo enviar la información del usuario al dispositivo.

Borrar Usuario

Para eliminar a un usuario registrado en **BioStar X** por renuncia, terminación de contrato o violación de seguridad, sigue los pasos a continuación.

1. Haz clic en **User** en la página **Launcher**.
2. Haz clic en la casilla de verificación a la izquierda del usuario que deseas eliminar de la lista de usuarios. Selecciona más de un usuario.
3. Haz clic en **Delete** en la parte superior derecha de la pantalla.



4. Haz clic en **Delete** para confirmar en el mensaje que aparece.

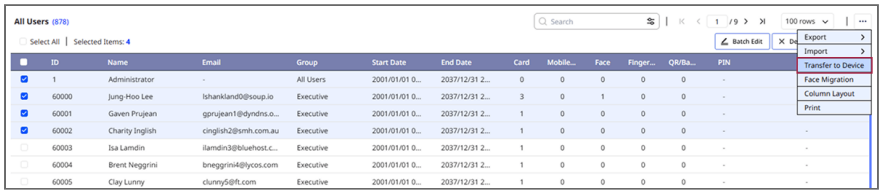
Confirma que el usuario seleccionado se haya eliminado de la lista de usuarios.

> **Información**
>
> - El usuario con ID `1` no se puede eliminar.
> - Para obtener más información sobre cómo eliminar la información del usuario del dispositivo, consulta Administrar Usuarios Registrados en el Dispositivo.

Transferir Información de Usuario al Dispositivo

Proporciona una función para transmitir al dispositivo la información de usuario registrada en el servidor **BioStar X** para el control de acceso. Cuando se envía la información de usuario al dispositivo, este utiliza los datos del usuario para determinar los permisos de acceso y puede realizar autenticación incluso en entornos sin conexión.

1. Haz clic en **User** en la página **Launcher**.
2. Haz clic en la casilla de verificación a la izquierda del usuario cuya información deseas enviar desde la lista de usuarios. Selecciona más de un usuario.
3. Selecciona el botón [•••] en la esquina superior derecha de la pantalla y haz clic en **Transfer to Device**.



4. Cuando aparezca la ventana **Transfer to Device**, selecciona el dispositivo de la lista al que deseas transferir la información de usuario.



5. Si la información difiere para el mismo ID, marca la casilla de la opción **Overwrite users with different information** para sobrescribirla con el contenido del servidor **BioStar X**.

6. Después de seleccionar todos los dispositivos a los que deseas transferir, haz clic en **Apply**.

Transfiriendo la información de usuario al dispositivo seleccionado.

> **Información**
>
> - Busca dispositivos ingresando palabras clave en el campo de búsqueda.
> - El dispositivo debe estar conectado al servidor **BioStar X** para transferir la información de usuario.
> - Si cambias la información de un usuario que ya está registrado en el dispositivo, debes volver a enviar la información de usuario para que los cambios se reflejen en el dispositivo. Para obtener información sobre cómo usar la opción **Automatic User Synchronization** para sincronizar la información del usuario con el dispositivo, consulte Configuración Detallada del Servidor.
> - Existe un límite en la cantidad de usuarios que se pueden registrar en cada dispositivo. Verifica la cantidad de usuarios que se pueden registrar en el dispositivo.

Rastrear Historial de Acceso de Usuarios

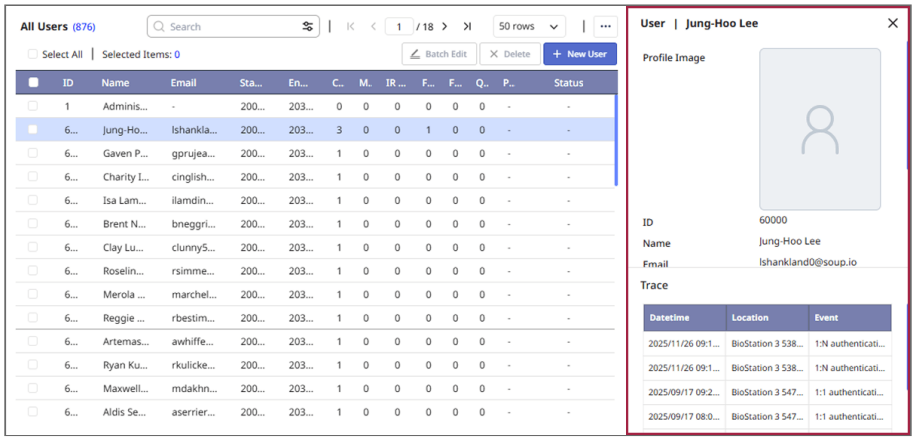
Rastrear y verificar el historial de acceso de los usuarios es crucial para mejorar la seguridad y optimizar la eficiencia operativa. El historial de acceso permite prevenir amenazas de seguridad y optimizar las operaciones. Identifique a los usuarios que intentan acceder a áreas restringidas o en horarios no autorizados. Esto permite responder rápidamente a las amenazas de seguridad. Al identificar señales anómalas, como fallas de autenticación repetidas o accesos desde zonas horarias inusuales, es posible detectar las amenazas de seguridad de forma temprana.

Verifique el historial de acceso del usuario siguiendo estos pasos.

1. Haz clic en **User** en la página **Launcher**.

2. En la lista de usuarios, haga clic en el usuario cuyo historial de acceso desea verificar.

3. La información de perfil del usuario seleccionado aparece en el lado derecho de la pantalla.



Verifique el historial de acceso del usuario en la sección **Trace** debajo de la pantalla de vista previa.

> **Información**
>
> - Consulte los eventos de acceso en tiempo real en la página **Monitoring**. Para obtener más información, consulte Supervisar Evento.
> - Consulte los eventos de acceso anteriores en la página **Data**. Para obtener más información, consulte Fecha.

Exportar/Importar Información de Usuarios

Utiliza la información de usuarios de una versión anterior o de otro servidor exportando o importando los datos de usuario.

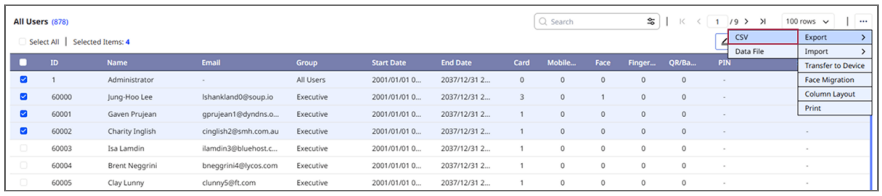
Exportar o importar CSV

Guarda la información de usuarios seleccionada como un archivo CSV o carga archivos CSV guardados. Transfiere fácilmente la información de usuarios mediante archivos CSV.

> **Información**
>
> - Si existen campos de usuario personalizados que no se han añadido a **BioStar X**, el archivo CSV no se importará correctamente. Para obtener más información sobre cómo agregar campos de usuario personalizados, consulte Configuración Detallada del Servidor.
> - Si la información de usuarios se introduce en un idioma distinto del inglés o el coreano, guarda el archivo CSV en formato UTF-8.

Exportar CSV

1. Haz clic en **User** en la página **Launcher**.
2. Selecciona la casilla junto a los usuarios que deseas guardar como archivo CSV en la lista de usuarios. Selecciona más de un usuario.
3. Haz clic en el botón [•••] en la esquina superior derecha de la pantalla y selecciona **Export** → **CSV**.



4. Cuando aparezca la ventana **CSV Export**, ingresa **Export Reason** (opcional) y haz clic en **Download**.



5. Guarda el archivo CSV en la ubicación deseada de tu ruta local.

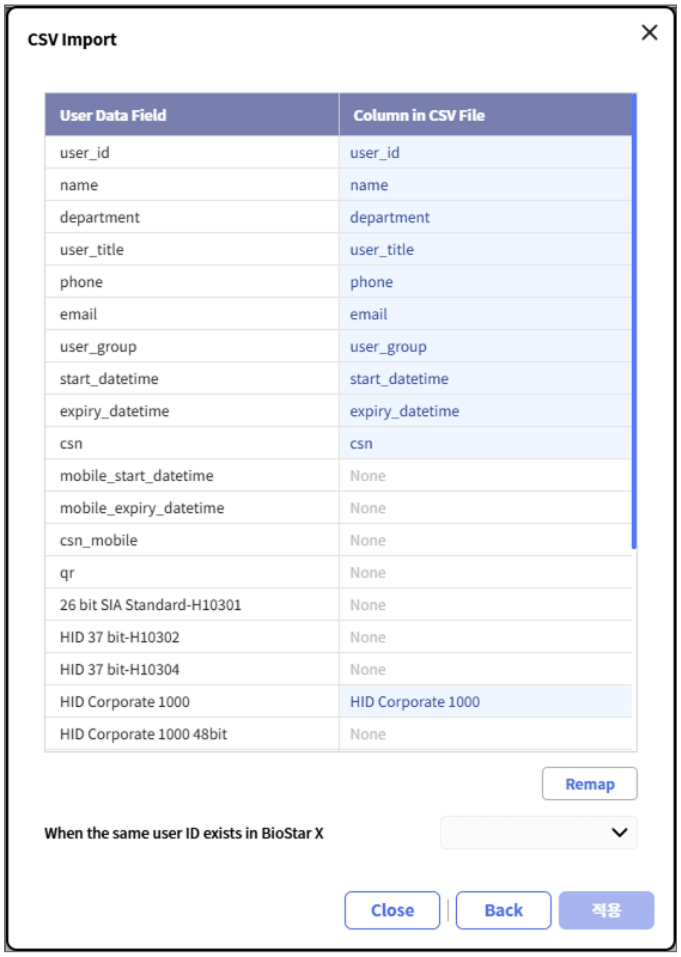
> **Información**
>
> **Export Reason** es opcional. Verifique los registros de motivos de exportación en **Settings** → **Audit Trail** → **AC Audit Log**.

Importar CSV

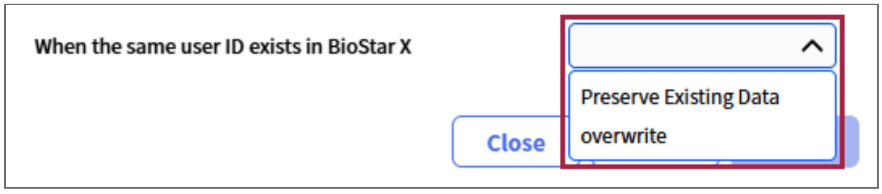
1. Haz clic en **User** en la página **Launcher**.
2. Haz clic en ••• en la parte superior derecha de la pantalla y selecciona **Import** → **CSV**.
3. Selecciona el archivo CSV guardado localmente.
4. Configura **Start import at row** en la ventana **CSV Import** y haz clic en **Next**.



5. Los campos de datos de usuario del archivo CSV se asignarán automáticamente a los campos correspondientes en **BioStar X**. Haz clic en **Remap** para reasignar campos con el mismo nombre.



6. Selecciona conservar datos de usuarios inscritos por ID en **BioStar X** o sobrescribirlos con el CSV y haz clic en **Apply**.



Si ocurre un error al importar el archivo CSV, puedes volver a revisar y subir solo los datos CSV que provocaron el error.

Información

- Las tarjetas de acceso móvil se pueden emitir mediante la importación de CSV. Al utilizar el sitio regular, se descontará un crédito del Airfob Portal por cada tarjeta de acceso móvil emitida al completar la importación. Para evitar emitir tarjetas de acceso móvil, desactiva la asignación.
- Si el archivo CSV contiene datos idénticos a las tarjetas de acceso móvil ya emitidas a los usuarios registrados en **BioStar X**, puedes elegir mantener o sobrescribir los datos; en ese caso, se conservarán las tarjetas de acceso móvil existentes.
- Si el archivo CSV contiene datos diferentes de las tarjetas de acceso móvil emitidas a los usuarios registrados en **BioStar X**, mantener los datos conservará las tarjetas actuales, mientras que sobrescribir emitirá nuevas tarjetas de acceso móvil a los usuarios correspondientes.
- Al emitir tarjetas de acceso móvil mediante la importación de CSV en un sitio dinámico, asegúrate de introducir valores en los campos `mobile_start_datetime` y `mobile_expiry_datetime`.
- Los códigos QR de **BioStar X** no se pueden emitir mediante la importación de CSV.
- Los datos faciales de usuarios se pueden inscribir mediante la importación de CSV. Para obtener más información, consulte Inscribir Rostros por Lotes.
- Los PIN de usuario se pueden inscribir mediante la importación de CSV. Para obtener más información, consulte Inscribir PIN.
- Si añades columnas que no coinciden con el archivo CSV guardado, no podrás importar el archivo en **BioStar X**.
- Si un nombre de usuario empieza con `&@~`, la importación de esa entrada del CSV falla.
- Establece el período de validez (fecha y hora de vencimiento) hasta 2037-12-31 23:59:59. La importación falla para las entradas con valores posteriores a esta fecha.
- Evita abrir el archivo CSV exportado directamente en programas de hojas de cálculo como Excel. Si un nombre de usuario empieza con el carácter `=`, el programa puede tratarlo como una fórmula y mostrar un valor diferente.

Exportar o importar archivos de datos

La información de usuarios se puede almacenar en un dispositivo de almacenamiento externo (USB) para importarla a **BioStar X** o a los dispositivos. Se pueden transferir hasta 500,000 registros de usuarios del servidor a los dispositivos o entre dispositivos.

Información

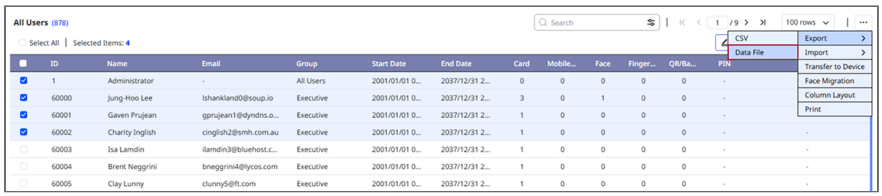
- Los datos exportados desde dispositivos con firmware obsoleto no se pueden importar a **BioStar X**. Utiliza siempre la versión más reciente del firmware.
- No se pueden importar datos si se utilizan formatos de plantilla de huella dactilar diferentes. Por ejemplo, los datos exportados desde dispositivos que utilizan el formato de plantilla de huella dactilar Suprema no se pueden importar en dispositivos que utilizan el formato de plantilla ISO.
- Al importar datos de usuario, si ya existen credenciales de huella y rostro almacenadas en el servidor **BioStar X**, se sobrescribirán con los datos existentes.
- No se pueden importar datos desde dispositivos con versiones de firmware obsoletas. Actualiza el firmware del dispositivo a una versión compatible.

  ▼ Ver dispositivos y versiones de firmware compatibles

  – BioStation 2 versión de firmware 1.9.0 o superior
  – BioStation A2 versión de firmware 1.8.0 o superior
  – FaceStation 2 versión de firmware 1.4.0 o superior
  – FaceStation F2 versión de firmware 2.2.0 o superior
  – X-Station 2 versión de firmware 1.0.0 o superior
  – BioStation 3 versión de firmware 1.3.1 o superior
  – BioStation 2a versión de firmware 1.0.0 o superior

Exportar datos

1. Haz clic en **User** en la página **Launcher**.
2. Selecciona la casilla junto a los usuarios que deseas exportar de la lista de usuarios. Selecciona más de un usuario.
3. Haz clic en ••• en la esquina superior derecha de la pantalla y selecciona **Export** → **Data File**.



4. En la ventana **Data File Export**, selecciona el dispositivo al que aplicar el archivo de datos.



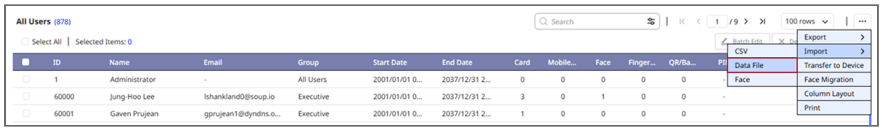
5. Ingresa **Export Reason** (opcional) y haz clic en **Apply**.
6. Guarda el archivo de datos en la ruta local deseada.

> **Información**
>
> - La exportación del archivo de datos incluye fotos de perfil de usuario, IDs, nombres, periodos de validez, grupos de acceso, PIN, modos de autenticación privada, credenciales (rostro, huella, tarjeta, tarjeta móvil, rostro, QR/Barcode) e información de nivel de seguridad uno a uno.
> - Seleccionar un dispositivo incorrecto para aplicar el archivo de datos puede hacer que el dispositivo no lo reconozca.
> - **Export Reason** es opcional. Verifique los registros de motivos de exportación en **Settings** → **Audit Trail** → **AC Audit Log**.

> **Precaución**
>
> Para importar en los dispositivos un archivo exportado desde **BioStar X**, cambia el nombre del archivo como se indica a continuación para que el dispositivo lo reconozca. El formato de nombre de archivo se ajustará para que sea reconocido automáticamente en futuras actualizaciones de firmware del dispositivo.
>
> ***BioStarX**_YYYYMMDD_HHMMSS.tgz* → ***BioStar2**_YYYYMMDD_HHMMSS.tgz*

Importar datos

1. Haz clic en **User** en la página **Launcher**.
2. Haz clic en [•••] en la esquina superior derecha de la pantalla y selecciona **Import** → **Data File**.



3. Seleccione el archivo de datos (*.tgz*) guardado localmente.

Aparecerá un mensaje en la pantalla si el archivo de datos se importa correctamente.

Administrar Grupos de Acceso

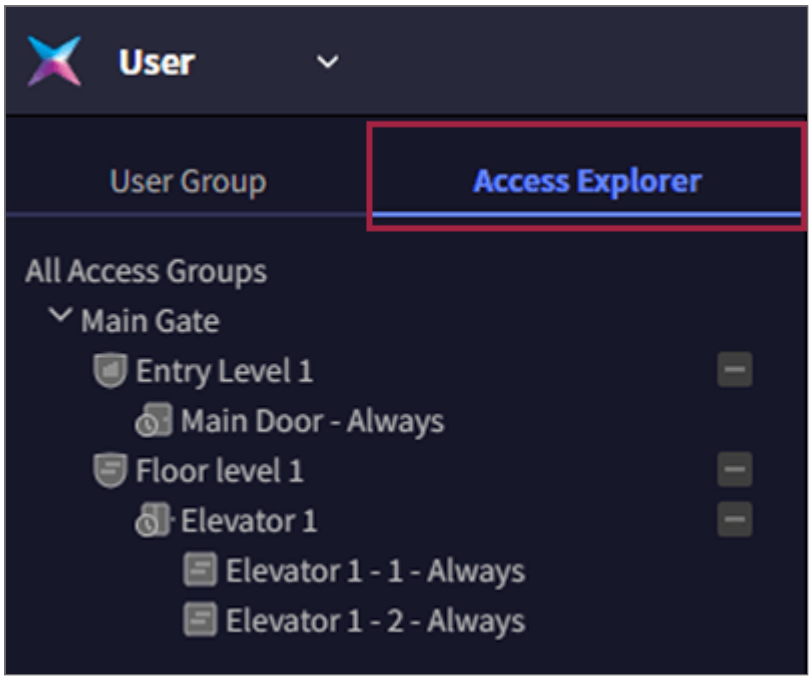
Esta guía muestra cómo consultar y administrar usuarios basados en grupos de acceso. Usa **Access Explorer** para verificar los usuarios registrados por grupo de acceso y explorar la jerarquía de permisos de acceso mediante la estructura de árbol.

> **Información**
>
> Configura la función de control de acceso para verificar las puertas o pisos que pertenecen a un grupo de acceso en **Access Explorer**. Para obtener más información, consulte Configuración de Control de Acceso.

Consulta a los usuarios por grupo de acceso

1. Haz clic en **User** en la página **Launcher**.

2. Haz clic en la pestaña **Access Explorer** en el menú de la estructura de árbol.



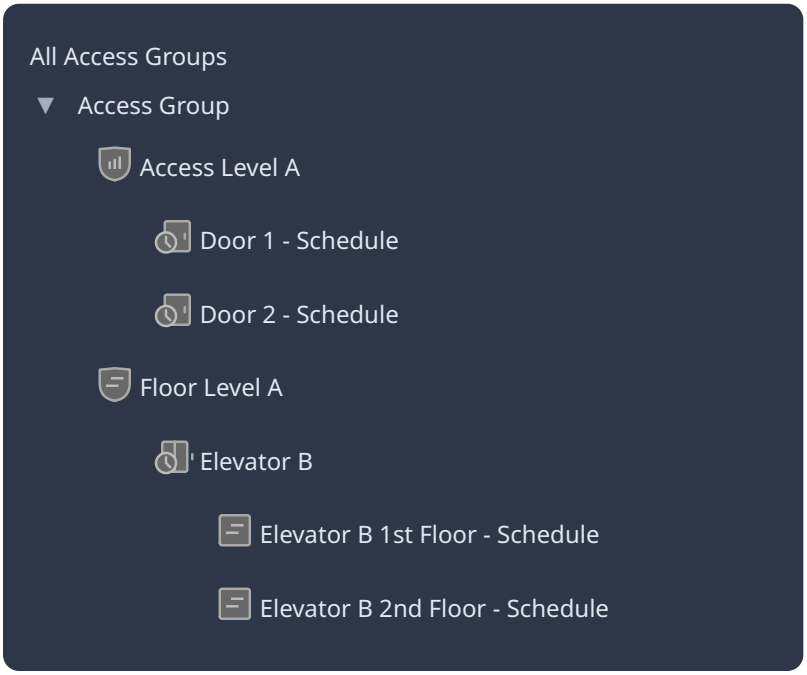
3. Haz clic en el grupo de permisos de acceso deseado en **All Access Groups**.

Puedes ver los usuarios que pertenecen al grupo de permisos de acceso seleccionado en la lista de usuarios.

> **Información**
> Haz clic en + o − para expandir o contraer los niveles de acceso o de piso bajo el grupo de acceso.

Conoce la estructura en árbol

El menú de la estructura de árbol se compone de la siguiente jerarquía.



- El **grupo de acceso** es la capa superior que incluye niveles de acceso, niveles de piso, grupos de usuarios y usuarios. Puedes administrar los permisos de acceso a través del **grupo de acceso**. Consulte Administrar Grupos de Acceso para obtener más información sobre la creación de grupos de acceso.
- El **nivel de acceso** define los horarios en los que los usuarios pueden ingresar y concede permiso para acceder a las puertas durante ese periodo. Consulte Administrar Niveles de Acceso para obtener más información sobre la creación de niveles de acceso.
- Puedes gestionar los pisos a los que los usuarios pueden acceder mediante ascensores a través del **nivel de piso**. Consulte Gestionar Niveles de Piso para obtener más información sobre la creación de pisos.
- El **horario** es una función que opera de forma eficaz el control de acceso y la gestión de asistencia mediante la configuración de horarios de acceso y festivos. Consulte Ajustes de Horario para obtener más información sobre cómo registrar horarios.
- Puedes registrar ascensores y gestionar los pisos accesibles a través de ellos. Consulte Registrar Ascensor para obtener más información sobre cómo registrar un ascensor.

Información

La característica de registro de ascensor está disponible como opción adicional con una licencia **Essential** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Iniciar Sesión con Autenticación Multi-Factor

Use la función **Autenticación multifactor** para mejorar la seguridad al iniciar sesión en **BioStar X**. Al habilitar **Multi-Factor Auth for Login** se añade un paso de autenticación por huella digital mediante un lector de huellas a la combinación de ID de usuario y contraseña.

Información

- Los usuarios que deseen utilizar la función **Multi-Factor Auth for Login** deben registrar su huella digital y configurar su nombre de usuario, contraseña y nivel de operador.
- Para usar la función **Multi-Factor Auth for Login**, debe conectarse al PC cliente de **BioStar X** un lector de huellas que admita inicio de sesión con autenticación multifactor. Consulte la siguiente lista para ver los dispositivos compatibles con el lector de huellas.
  - BioMini
  - BioMini Plus 2
  - BioMini Slim 2
- Si utiliza la cuenta Directory Service con la opción **Use for BioStar X Login**, no podrá usar la función **Multi-Factor Auth for Login**.
- Los administradores que configuren **Multi-Factor Auth for Login** no podrán autenticarse en los servicios de **BioStar X** (gestión de asistencia y video) distintos al control de acceso. Para usar el servicio, inicie sesión después de desactivar el ajuste **Multi-Factor Auth for Login**. Luego puede volver a activar el ajuste **Multi-Factor Auth for Login**.

Precaución

- Después de configurar la función de autenticación multifactor para la cuenta de administrador principal (ID 1), tenga en cuenta que no podrá iniciar sesión con esa cuenta si la autenticación por huella digital deja de estar disponible.
- Si el inicio de sesión se vuelve imposible debido a problemas con la huella digital, comuníquese con Equipo de Soporte Técnico global de Suprema.

Configuración de autenticación multifactor

Siga los pasos a continuación para configurar **Multi-Factor Auth for Login**.

1. Haz clic en **User** en la página **Launcher**.
2. Haga doble clic en el usuario al que desea configurar **Multi-Factor Auth for Login** en la lista de usuarios.

   Como alternativa, seleccione un usuario y haga clic en el botón **See More** en el perfil que se muestra en la pantalla derecha.
3. Cuando aparezca la pantalla de vista previa del usuario, establezca el elemento **Multi-Factor Auth for Login** en **Use** en la sección **Permission**.



4. Haga clic en **Save** en la parte superior derecha de la pantalla.

Configuración de autenticación multifactor completada.

Configuración masiva de autenticación multifactor

Antes de comenzar

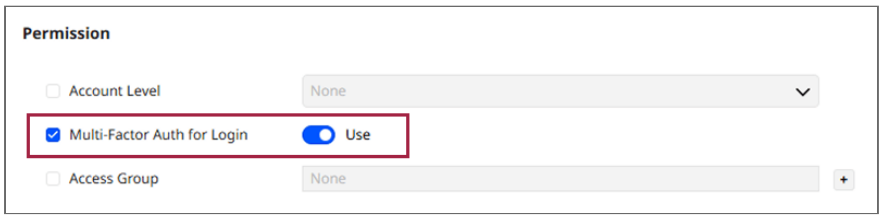
Para usar la función de inicio de sesión con autenticación multifactor, debe cumplir las siguientes condiciones.

- El usuario debe tener registrada la autenticación por huella digital.
- Se deben configurar **Operator**, **Login ID** y **Password**. Para obtener más información, consulta Configurar Permisos de Usuario.

Puede usar la función de edición masiva para aplicar **Multi-Factor Auth for Login** a varios usuarios.

1. Haz clic en **User** en la página **Launcher**.
2. En la lista de usuarios, marque la casilla a la izquierda del usuario al que desea configurar la autenticación multifactor.
3. Haz clic en **Batch Edit** en la esquina superior derecha de la pantalla.

4. Cuando aparezca la ventana de edición masiva, marque la casilla de la opción **Multi-Factor Auth for Login** en la sección **Permission** y establézcala en **Use**.



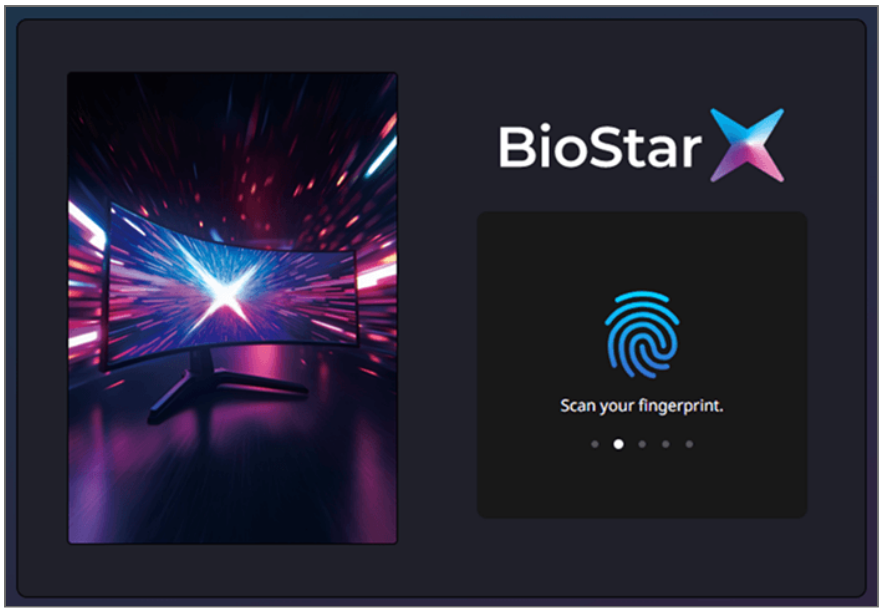
5. Haga clic en **Save** en la parte superior derecha de la pantalla.

Configuración de autenticación multifactor completada para varios usuarios seleccionados.

> **Información**
>
> Los usuarios seleccionados que no cumplan con las condiciones necesarias para activar la función **Multi-Factor Auth for Login** se pueden verificar mediante el mensaje emergente de **Not applicable user(s)**. Verifique las condiciones requeridas para la configuración e inténtelo de nuevo.

Iniciar sesión con autenticación multifactor

1. Acceda a la pantalla de inicio de sesión de **BioStar X** mediante un navegador web.
2. Introduzca su ID de usuario y contraseña, y luego haga clic en el botón **Login**.
3. Cuando aparezca la pantalla de ingreso de huella, escanee su huella digital con el lector de huellas.



Inicio de sesión completado.

Información

- El tiempo límite de escaneo está fijado en 18 segundos y no se puede cambiar.
- El escaneo de huella digital se puede intentar hasta tres veces consecutivas. Si la huella digital no se escanea correctamente dentro de estos tres intentos, la autenticación fallará.
- Si la autenticación falla, haga clic en el botón **Retry** para volver a intentar la autenticación por huella digital. Se permiten hasta dos intentos de reintento. Si la autenticación falla después de los intentos de reintento, el proceso volverá al paso de inicio de sesión con ID y contraseña.

Inscribir Rostros por Lotes

Aprende a inscribir rostros de usuarios por lotes. Inscribe los rostros de varios usuarios a la vez mediante la función de importación con un archivo CSV o cargando fotografías de rostro cuyos nombres de archivo coincidan con los ID de usuario. Como alternativa, envía enlaces de inscripción de rostro por correo electrónico a varios usuarios, lo que les permitirá inscribir sus rostros directamente desde sus dispositivos móviles.

Antes de comenzar

Prepara las imágenes de rostro de los usuarios antes de comenzar la inscripción por lotes.

- Los archivos de imagen de rostro deben almacenarse en una sola carpeta. Los nombres de archivo de las imágenes de rostro deben coincidir con los ID de usuario.
- El tamaño máximo de archivo para los tipos de imagen admitidos es de 10MB.
- Los formatos de imagen admitidos incluyen JPG, JPEG y PNG.

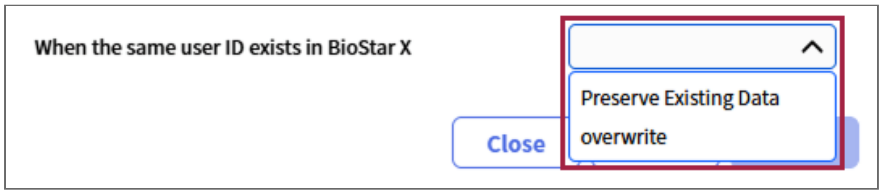
Inscribir con importación de archivo CSV

Inscribe rostros de usuarios en bloque mediante la función de importación CSV.

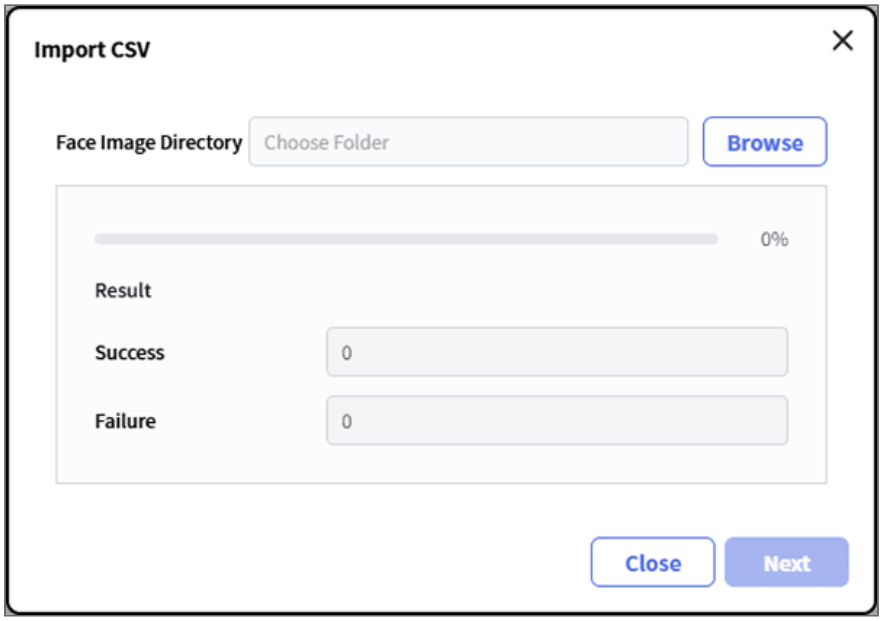
1. Haz clic en **User** en la página **Launcher**.
2. En la lista de usuarios, marca la casilla del usuario cuyo rostro deseas inscribir. Selecciona más de un usuario.
3. Haz clic en el botón ••• en la esquina superior derecha de la pantalla y selecciona **Export** → **CSV**.
4. Cuando aparezca la ventana de exportación CSV, haz clic en **Download**.
5. Guarda el archivo CSV en la ubicación deseada de tu ruta local.
6. Abre el archivo CSV y agrega las columnas `face_image_file1`, `face_image_file2`.
7. Ingresa los nombres de archivo de las imágenes de rostro, incluidas las extensiones, en las columnas agregadas y guarda.
8. Haz clic en ••• en la parte superior derecha de la pantalla y selecciona **Import** → **CSV**.
9. Selecciona el archivo CSV modificado.
10. Cuando aparezca la ventana de importación CSV, establece **Start import at row** y haz clic en **Next**.



11. Elige si deseas sobrescribir los datos de usuario ya registrados en **BioStar X** con la información del archivo CSV y haz clic en **Apply**.



12. Haz clic en el botón **Browse** en **Face Image Directory**.



13. Selecciona la ruta donde se almacenan las imágenes de rostro y haz clic en **Upload**.

14. Para completar la importación CSV, haz clic en **Next**.

Si ocurre un error al importar el archivo CSV, puedes volver a revisar y subir solo los datos CSV que provocaron el error.

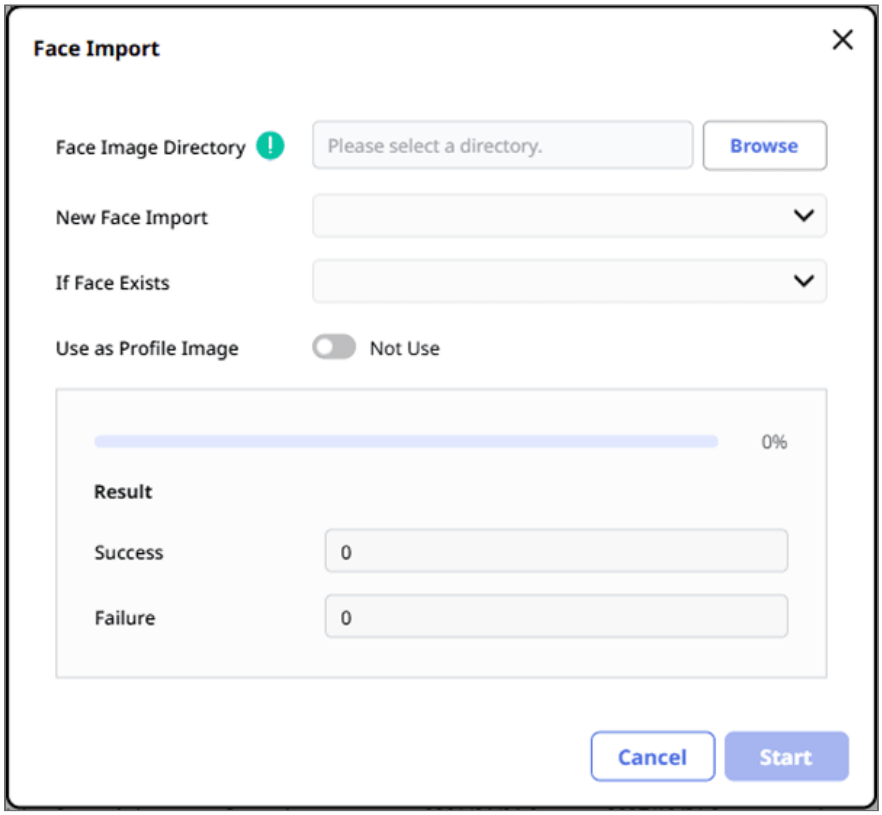
> **Información**
> Se recomienda usar la misma ruta para el archivo CSV y los archivos de imágenes de rostro que se van a importar.

Importar rostro

Puedes importar imágenes de rostro con nombres de archivo que coincidan con los ID de usuario e inscribirlas para

autenticación facial. Prepara los archivos de imágenes de rostro de los usuarios antes de comenzar. Los nombres de archivo de las imágenes de rostro deben coincidir con los ID de usuario.

1. Haz clic en **User** en la página **Launcher**.
2. Haz clic en ••• en la esquina superior derecha de la pantalla y selecciona **Import** → **Face**.
3. Cuando aparezca la ventana **Face Import**, haga clic en **Browse**.



4. Selecciona la ruta donde se almacenan las imágenes de rostro.
5. Selecciona el método para cargar imágenes de rostro en la opción **New Face Import**.
   - **Import image files whose name matches user ID**: Carga imágenes cuyos nombres de archivo coinciden con los ID de usuario.
   - **Import image files whose name matches user ID + Add new user by using file name as user ID**: Si los ID de usuario registrados coinciden con los nombres de archivo de las imágenes de rostro, se cargan las imágenes; si no coinciden, se crea un nuevo usuario usando el nombre de archivo como ID de usuario y se inscribe como método de autenticación facial.
6. En la opción **If Face Exists**, selecciona **Preserve data** o **Overwrite**.
   - **Preserve**: Conserva las imágenes de rostro de los usuarios registrados.
   - **Overwrite**: Sobrescribe las imágenes de rostro de los usuarios registrados con las nuevas imágenes importadas.
7. Para usar las imágenes de rostro importadas como imágenes de perfil, haz clic en la opción **Use as Profile Image** para habilitarla.
8. Haz clic en **Start**.

Si ocurre un error al importar un archivo de imagen de rostro, aparece una lista de fotos con errores. Revisa la lista y vuelve a intentar.

Información

Se puede importar un máximo de 1 imagen de rostro por ID de usuario.

Inscribir rostros con un dispositivo móvil

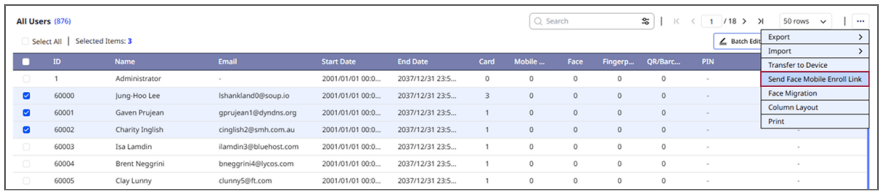
Envía enlaces de inscripción de rostro a los usuarios por correo electrónico. Los usuarios pueden acceder al enlace en sus dispositivos móviles para inscribir sus rostros directamente.

Antes de comenzar

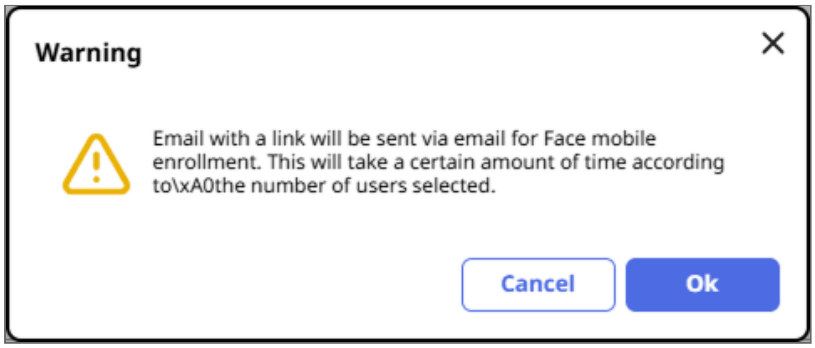
- Completa la configuración de información de correo electrónico, incluyendo la configuración SMTP, antes de usar la función de inscripción facial móvil. Para obtener más información, consulta Configuración de Correo Electrónico.
- Debes habilitar la función **Remote Access** para usar la inscripción facial móvil. Para obtener más información sobre **Remote Access**, consulta Configuración de Acceso Remoto.

Enviar enlace de inscripción de rostro

1. Haz clic en **User** en la página **Launcher**.
2. En la lista de usuarios, marca la casilla del usuario cuyo rostro deseas inscribir. Selecciona más de un usuario.
3. Haz clic en el botón ••• en la esquina superior derecha de la pantalla y selecciona **Send Face Mobile Enroll Link**.



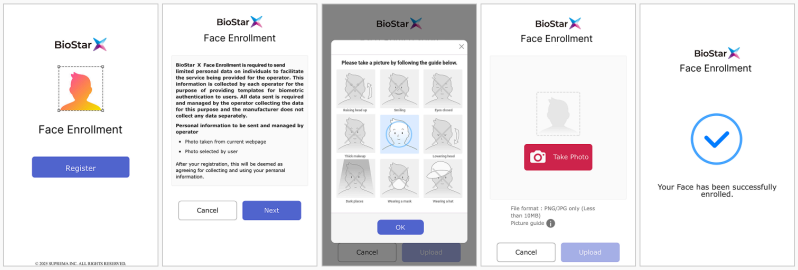
4. Cuando aparezca la ventana de mensaje, haga clic en **Ok**.



El enlace de inscripción de rostro se envía al correo electrónico de los usuarios seleccionados. Una vez que los usuarios completen la carga, su credencial de rostro se añade a sus perfiles de usuario.

Información

- Puedes comprobar el estado de envío de correos electrónicos en **Audit Trail**. Para obtener más información sobre el registro de auditoría del sistema, consulta Gestionar Registro De Auditoría.
- El idioma que se muestra en la página a la que se accede mediante el enlace móvil de inscripción de rostro sigue la configuración de idioma del navegador utilizado en el dispositivo móvil.
- Cuando el usuario abra el enlace móvil de registro facial que se le envió, se ejecutará el servicio de registro facial como se muestra a continuación. Sigue las instrucciones en la pantalla.



- El tamaño máximo de archivo para los tipos de imagen admitidos es de 10MB.
- Los formatos de imagen admitidos incluyen JPG, JPEG y PNG.
- El enlace móvil de inscripción de rostro enviado caducará después de 24 horas.
- Una vez que el proceso de inscripción móvil de rostro se complete correctamente tras cargar una fotografía de rostro, aparece un mensaje de éxito de inscripción en la pantalla. Si la inscripción falla, se muestra un mensaje de error y el motivo, y el usuario puede volver a intentar la inscripción facial visual con una fotografía de rostro diferente.

Migracion Visual Face

Actualice las caras registradas en la versión anterior de **BioStar X** para mejorar el rendimiento de autenticación mediante el algoritmo más reciente. El protocolo de sincronización se ha mejorado para transmitir solo plantillas, excluyendo las imágenes reales durante la sincronización de usuarios. Además, esto ayuda a reducir significativamente el tiempo de sincronización y a prevenir problemas relacionados con la privacidad.

Antes de comenzar

Antes de ejecutar la función de migración de caras, revise los siguientes puntos.

¿Qué es la migración de caras?

Es una función que genera dos tipos de plantillas faciales a partir de las imágenes de usuario ya almacenadas en el servidor de BioStar X. Ejecute **Face Migration** para sincronizar solo la plantilla de autenticación facial durante la sincronización de usuarios.

Dispositivos y versiones de firmware compatibles

Consulte la lista a continuación para conocer los dispositivos que pueden sincronizar la cara con la plantilla.

- Firmware del BioStation 3 Max v1.0.0 o posterior

- Firmware BioEntry W3 v1.0.0 o posterior
- Firmware BioStation 3 v1.3.1 o posterior
- Firmware FaceStation F2 v2.2.0 o posterior

▼ Aviso sobre el fin de soporte del firmware FaceStation F2 v1.x.x

BioStar X optimizó el rendimiento de la sincronización al cambiar para enviar solo plantillas al sincronizar la cara del usuario con el dispositivo. Por lo tanto, el soporte para el firmware FaceStation F2 v1.x.x, que solo puede extraer plantillas desde el dispositivo, se descontinuará. Si actualmente utiliza el firmware FaceStation F2 versión 1.x.x, actualice al firmware más reciente para usar **BioStar X** con FaceStation F2.

Puede descargar el firmware más reciente desde el Centro de descargas de Suprema.

Notas sobre los tipos de plantillas faciales

Diferencias en los tipos de plantillas faciales para BioStation 3 Max, BioEntry W3, BioStation 3 y FaceStation F2.

- **Tipo NPU**: BioStation 3 Max, BioEntry W3, BioStation 3
- **Tipo GPU**: FaceStation F2

- **Tiempo de sincronización entre dispositivos con diferentes tipos de plantillas faciales**

  Antes de ejecutar **Face Migration**, tenga en cuenta que si agrega BioStation 3 Max, BioEntry W3 o BioStation 3 a un entorno que anteriormente solo utilizaba FaceStation F2 y luego sincroniza, el tipo de plantilla cambiará y se extraerán plantillas de tipo NPU de las imágenes. Esto puede llevar bastante tiempo, dependiendo del número de rostros registrados en el servidor.

- **Recomendaciones para registrar caras en BioStar X**

  Al registrar caras sin usar la opción **Store Face Image** en el dispositivo, solo se sincroniza la plantilla con **BioStar X**. Como resultado, no se puede sincronizar a dispositivos con tipos de plantillas faciales diferentes. Por lo tanto, se recomienda registrar las caras mediante **BioStar X**.

Avisos relacionados con dispositivos

Al exportar archivos de datos desde FaceStation F2 y BioStation 3, los archivos solo se pueden exportar con versiones de firmware superiores a las siguientes:

El archivo de datos de usuario exportado desde **BioStar X** contiene solo plantillas sin imágenes, por lo que no se puede importar en FaceStation F2 y BioStation 3 que utilizan firmware existente.

- Firmware FaceStation F2 v2.2.0 o posterior
- Firmware BioStation 3 v1.3.1 o posterior

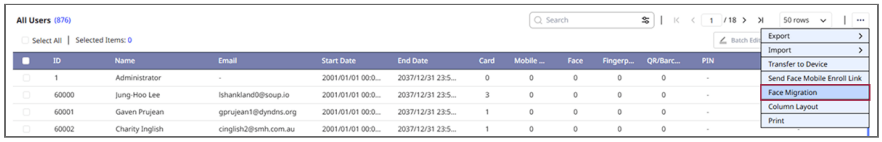
Precaución

Al utilizar FaceStation F2 o BioStation 3, se recomienda actualizar a la versión de firmware más reciente. Puede descargar el firmware más reciente desde el Centro de descargas de Suprema.

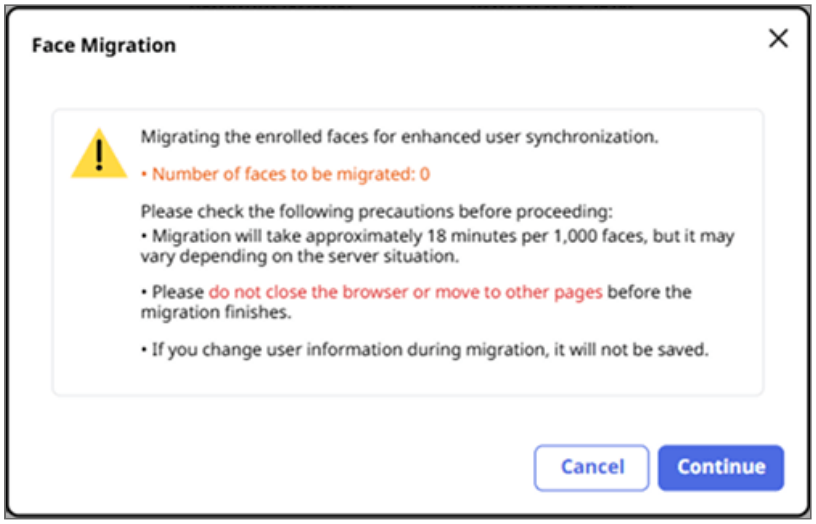
Cómo realizar la migración de caras

1. Haz clic en **User** en la página **Launcher**.

2. Seleccione ••• en la esquina superior derecha de la pantalla y haga clic en **Face Migration**.



3. Revise el contenido de la ventana emergente de advertencia y haga clic en **Continue**.



Migración de caras en curso. Cuando la migración de caras finalice, aparecerá una ventana emergente con los resultados. Mostrará el número total de caras registradas, así como la cantidad de caras migradas correctamente y las que fallaron.

- Después de una migración exitosa, sincronice la información del usuario con el dispositivo para aplicar los cambios. Para obtener más información sobre cómo transferir la información del usuario al dispositivo, consulte Transferir Información de Usuario al Dispositivo.

- Si la migración de caras falla, descargue una lista de usuarios fallidos en un archivo CSV. Haga clic en **Delete** para eliminar todas las caras cuya migración falló.

Información

- Solo la cuenta de administrador con ID de usuario **1** puede usar esta función.
- No salga de la página actual mientras la migración esté en curso.
- Cuanto mayor sea el tamaño de las imágenes faciales registradas por usuario, más tiempo tomará generar las plantillas.
- Para aproximadamente 1,000 caras, el proceso tarda alrededor de 18 minutos, aunque puede variar según el rendimiento del servidor.
- Para obtener más información sobre cómo almacenar únicamente la plantilla, sin guardar la imagen del rostro del usuario en el servidor, consulte Configuración Detallada del Servidor.

Configurar Permisos de Apertura de Emergencia

Configure permisos de apertura de emergencia para permitir que usuarios específicos accedan a todas las puertas en situaciones de emergencia. Si se abre una puerta con una tarjeta que tiene configurado el permiso de acceso de emergencia, la puerta permanece abierta y permite que cualquiera entre.

Antes de comenzar

Primero agregue las credenciales de tarjeta antes de configurar los permisos de apertura de emergencia. Para obtener más información sobre cómo agregar credenciales de tarjeta, consulte Inscribir Tarjeta de Acceso.

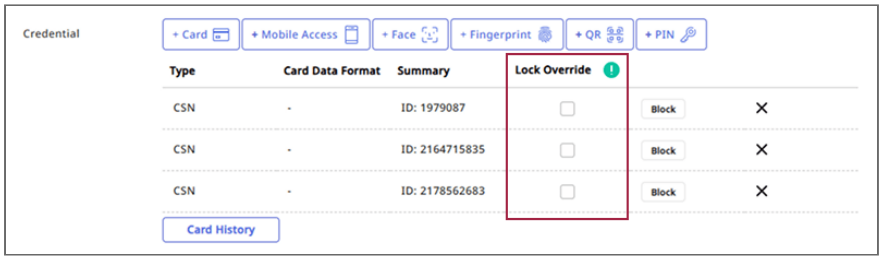
Información

- No se admiten credenciales distintas de las credenciales de tarjeta.
- Se admiten todas las credenciales de tarjeta excepto las tarjetas inteligentes (AoC) y las tarjetas de acceso móvil ToM (ToM AoC).
- Según el dispositivo, es posible que la función de apertura de emergencia no esté admitida. Consulte los dispositivos y versiones de firmware compatibles a continuación.
  - Firmware del BioStation 3 Max v1.0.0 o posterior
  - Firmware del XPass Q2 v1.0.0 o posterior
  - Firmware BioStation 3 v1.4.0 o superior

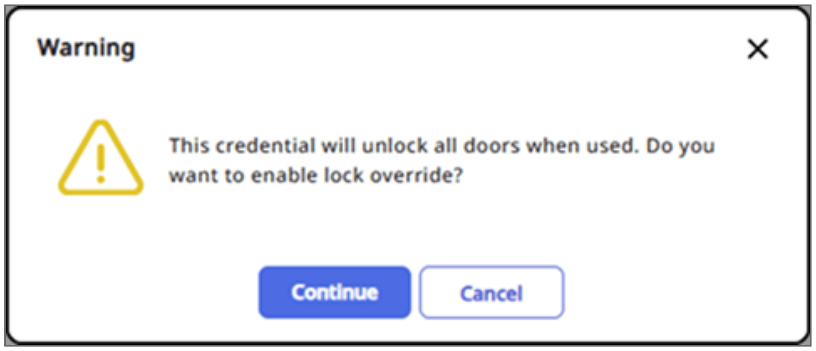
Configurar permisos de apertura de emergencia

1. Haz clic en **User** en la página **Launcher**.
2. Haga doble clic en el usuario al que desea configurar permisos de apertura de emergencia en la lista de usuarios.

   Como alternativa, seleccione un usuario y haga clic en el botón **See More** en el perfil que se muestra en la pantalla derecha.
3. Cuando aparezca la pantalla de detalles del usuario, vaya a la sección **Credential**.
4. Haga clic en la casilla de verificación del elemento **Lock Override** para las credenciales de tarjeta que desea autorizar para la apertura de emergencia.



5. Cuando aparezca un mensaje de advertencia, revise el contenido y haga clic en **Continue**.



6. Haga clic en **Save** en la parte superior derecha de la pantalla.

Complete la configuración de los permisos de apertura de emergencia.

Precaución

Los usuarios pueden abrir todas las puertas con una tarjeta de acceso configurada con permiso de emergencia.

Información

- Seleccione una o más credenciales de tarjeta para otorgar permiso de acceso de emergencia.
- Para revocar el permiso de acceso de emergencia, vuelva a hacer clic en la casilla de verificación del elemento **Lock Override** de la credencial de tarjeta seleccionada.

Monitorizar

Esta guía abarca las funciones disponibles en la página **Monitoring**, una de las funciones principales de **BioStar X**.

Haga clic en **Monitoring** en la página **Launcher** o seleccione **Monitoring** en la lista de accesos directos en la esquina superior izquierda de la pantalla.

Monitorear Puertas

Supervisar la puerta es una de las funciones principales del sistema de seguridad, lo que permite verificar y controlar en tiempo real el estado de la puerta. Este documento guía sobre cómo supervisar y controlar puertas, elevadores y control de acceso avanzado. Esto permite una gestión de seguridad eficiente y una respuesta rápida.

Verifica el estado

Supervise el estado de puertas, elevadores y control de acceso avanzado en tiempo real para operar el sistema de seguridad de forma confiable. Usa los íconos de estado en **Monitoring** para revisar alarmas y estados anómalos de un vistazo. Revisa solo las entradas que requieren acción y responde de inmediato.

Haga clic en **Monitoring** en la página **Launcher** o seleccione **Monitoring** en la lista de accesos directos en la esquina superior izquierda de la pantalla. Revisa el estado de cada elemento en la pestaña **Door** en la barra lateral izquierda de la pantalla.

Antes de comenzar

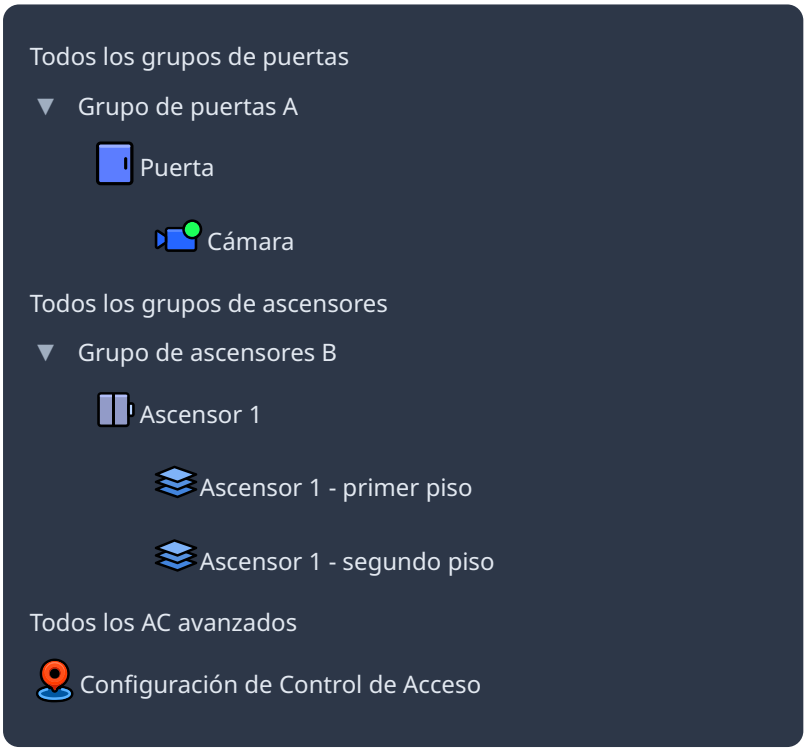
Asegúrate de que los dispositivos conectados a la puerta estén configurados correctamente. Comprueba que el dispositivo esté conectado a la red y actualizado con el firmware más reciente. En caso de un problema, primero verifica el estado de alimentación y la conexión de red del dispositivo.

Información

- Para más información sobre cómo agregar y configurar dispositivos, consulte Administrar Dispositivos.
- Para más información sobre cómo agregar y configurar puertas, consulte Administrar Puertas.
- La función **Log Upload** debe estar habilitada para supervisar o controlar el estado de la puerta de acceso. Habilita esta función en **Settings** → **System** → **Server** en la sección **General**.
- La función para conectar cámaras a puertas mediante el servidor VMS está disponible como opción adicional con una licencia **Essential** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Conoce la estructura del árbol

La estructura de árbol en la pestaña **Door** de la barra lateral izquierda se organiza de la siguiente manera.



Información

- Para más información sobre cómo agregar y configurar dispositivos, consulte Administrar Dispositivos.
- Para más información sobre cómo agregar y configurar puertas, consulte Administrar Puertas.
- Para más información sobre cómo agregar y configurar ascensores, consulte Administrar Ascensores.
- Para más información sobre la configuración avanzada de control de acceso, consulte Configuración Avanzada de Control de Acceso.
- Para más información sobre cómo vincular puertas y cámaras, consulte Configurar Reglas de Video.

Verifica el estado

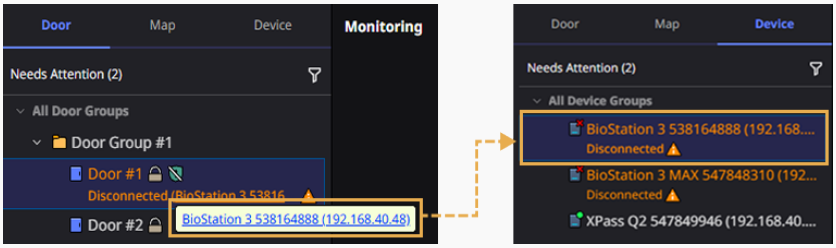
Verificar errores de conexión y alarmas

Verifica el estado de la puerta o del ascensor para confirmar su correcto funcionamiento. Consulta la información siguiente para el estado de cada icono.

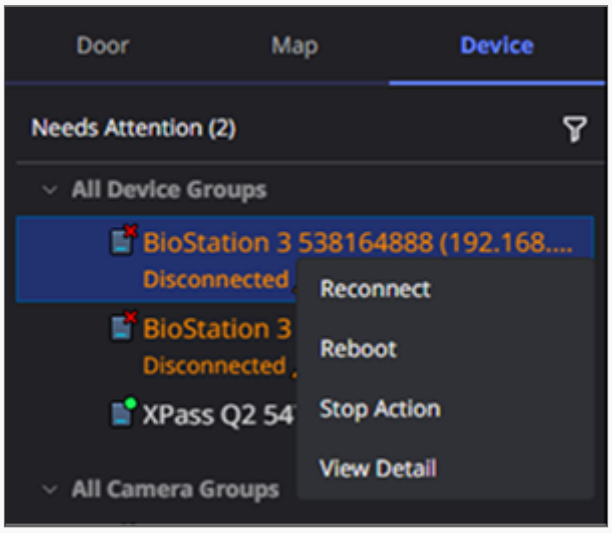
Ícono de estado	Descripción
⚠	Muestra estados anómalos del dispositivo, como desconexión, errores del servidor de comunicaciones múltiples y errores de sincronización.
🚨	Muestra el estado de puertas de entrada, elevadores, control de acceso avanzado y alarmas de análisis de video con IA.

Consejo

Haz clic en un icono de estado para ver información detallada en una descripción emergente. Haz clic en el enlace del mensaje de error de la descripción emergente para ir a la lista de dispositivos conectados a la puerta o al ascensor.



Haz clic derecho en el dispositivo y selecciona la opción **Reconnect** o **Reboot**.

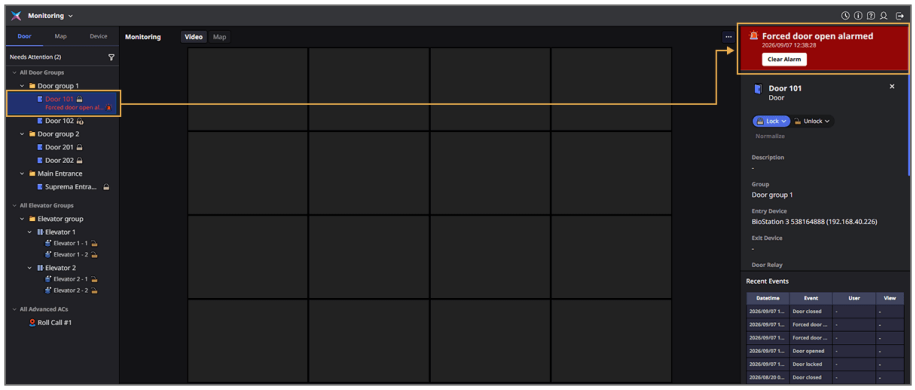


Información

- Configura las alarmas provenientes de la puerta o del ascensor mediante los siguientes ajustes.
  - Ajustes de alarma de puerta
  - Ajustes de alarma de ascensor
  - Ajustes avanzados de control de acceso
- Conecta la puerta de entrada y la cámara en las reglas de video para configurar alarmas. Para más información sobre cómo configurar las reglas de video, consulte Configurar Reglas de Video.
- Cuando está vinculado con el servidor VMS, las alarmas de eventos de IA para videos pueden enviarse a **BioStar X**. Para obtener más información, consulta el manual del servidor VMS.
- Para más información sobre cómo reconocer alarmas, consulte Supervisar Evento.

Revisa las alarmas en el panel de vista previa

En la pestaña **Door**, selecciona una puerta, un elevador o un área de control de acceso avanzado con el icono de alarma( ). Revisa los detalles de la alarma en la parte superior del panel de vista previa de la derecha. En puertas y elevadores, en la parte superior del panel también aparece el estado anómalo ( ).



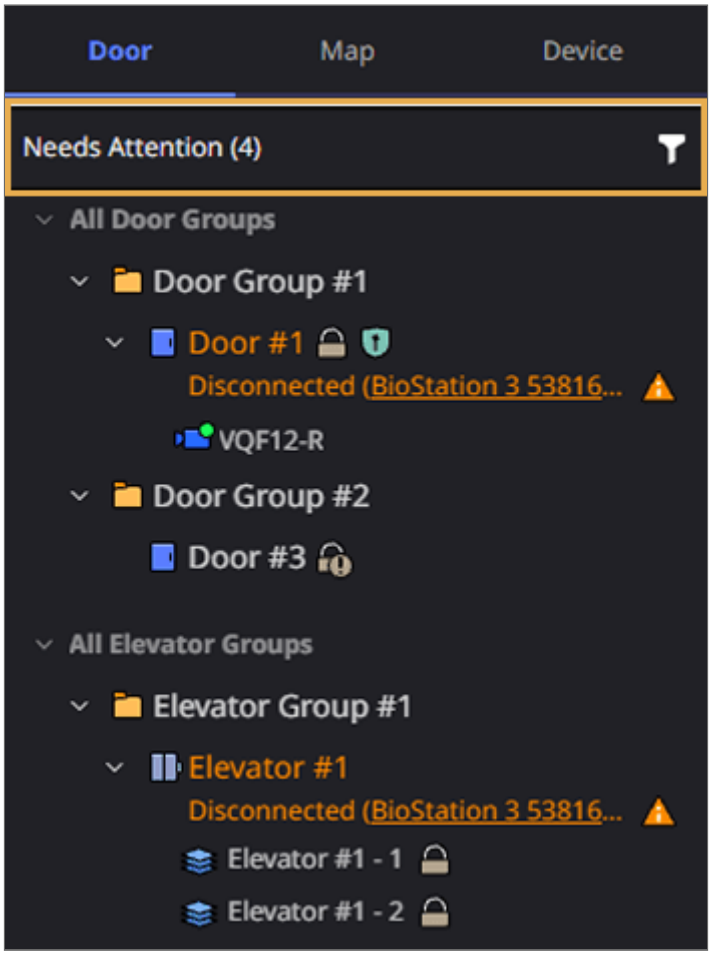
Un banner en la parte superior del panel muestra los detalles del estado actual, como el nombre y la hora de la alarma. También incluye botones para ejecutar la acción adecuada.

Información

- Si ocurren varias alarmas al mismo tiempo, el banner muestra solo 1 alarma: la más reciente.
- En puertas o elevadores, las alarmas que se activan cuando el dispositivo está desconectado muestran solo el tipo de alarma, sin marca de tiempo.
- Los botones del banner varían según el tipo de alarma. Haz clic en un botón para ejecutar la acción de la alarma.
- Los controles de puerta, como bloquear y desbloquear, siguen disponibles mientras aparece una alarma. Para obtener más información sobre el control de puertas, consulta Control de Puerta.

Ver entradas que requieren atención

Los administradores pueden ver solo las puertas y los elevadores que requieren acción de un vistazo. En la barra lateral izquierda, haz clic en **Needs Attention**. Revisa el estado de puertas y elevadores, y toma medidas de inmediato cuando ocurran problemas.



> **Información**
> Consulta Criterios de atención para ver las condiciones que marcan puertas y elevadores como elementos que requieren atención.

Criterios de atención

Puerta

Una puerta requiere atención si se cumple alguna de las condiciones siguientes.

Cambio de modo de la puerta

Esto incluye puertas bloqueadas o desbloqueadas por un administrador, un horario o una emergencia.

Motivo	Indicador de estado
Operación manual por un administrador	**Locked by Operator** / **Unlocked by Operator**
Horario	**Locked by Schedule** / **Unlocked by Schedule**
Emergencia	**Locked by Emergency** / **Unlocked by Emergency**

Alarma

Si una alarma permanece sin borrar, el sistema la marca como una alarma que requiere atención. Las alarmas de apertura forzada, puerta mantenida abierta, y anti-passback se clasifican como alarmas, no como estados anormales.

Tipos de alarma	Descripción
Apertura de puerta forzada	Puerta abierta a la fuerza sin desbloquear
Puerta mantenida abierta demasiado tiempo	La puerta permanece abierta más tiempo del establecido
Alarma anti-passback (APB)	Regla anti-passback infringida
Alarma anti-passback temporizada	Se infringió la regla de anti-passback basada en el tiempo
Alarma de anulación del bloqueo	Desbloqueado mediante autenticación con tarjeta de anulación de bloqueo en estado bloqueado (bloqueado por un administrador o por horario)
Alarma de analítica de video con IA	Alarmas basadas en analítica de video, como acceso por seguimiento, merodeo, intrusión, caídas, y objetos abandonados

Estado anormal

El sistema lo determina según el estado de conexión de los dispositivos conectados a la puerta.

Tipo de estado anormal	Descripción
Desconectado	El dispositivo está desconectado de la red
Error de sincronización	Conectado, pero los datos no están sincronizados
Error de Multi Communications Server	El Multi Communications Server del dispositivo presenta un error

Información

- El filtro **Needs Attention** incluye el bloqueo del dispositivo y el bloqueo por fallas de autenticación consecutivas (Auth Fail Lockout), además de los estados anormales anteriores.
- Si una alarma y un estado anormal ocurren juntos, ambos íconos aparecen en una fila sin superponerse.
- Los estados anormales de los dispositivos secundarios se consolidan en el nodo de puerta principal. Siga la jerarquía para encontrar el problema con el filtro activado.

Elevador

Evalúe los ascensores en las mismas condiciones que las puertas. Sin embargo, las condiciones de estado anormal y alarma difieren de la siguiente manera.

- **Cambio de modo**: Igual que en las puertas. El sistema marca el ascensor como requiere atención si un administrador, un horario o una emergencia lo bloquea o desbloquea.
- **Estado anormal**: Use los criterios de la puerta. Sin embargo, los ascensores no tienen estado de apertura forzada ni de apertura prolongada, así que exclúyalos de la evaluación.
- **Alarma**: Los ascensores tienen alarmas dedicadas que difieren de las alarmas de puerta. Consulte lo siguiente.

Tipos de alarma	Descripción
Alarma del ascensor disparada	Alarma del ascensor activada
Alarma de entrada del ascensor	Alarma activada por una señal de entrada externa
Alarma de desbloqueo de todos los pisos del ascensor	Apertura forzada de todos los pisos

Información

- Los pisos aparecen como nodos independientes debajo del nodo del ascensor, y cada piso solo tiene estado bloqueado ( ) o desbloqueado ( ).
- Las alarmas y los estados anormales aparecen en el nodo del ascensor principal, no en los pisos. Al expandir el ascensor, solo aparecen los pisos que requieren acción, y el sistema oculta los pisos normales.

Control de acceso avanzado

El sistema también incluye entradas de control de acceso avanzado (anti-passback, incendio, intrusión, recuento, límite de ocupación e interbloqueo). Esto ayuda a decidir si se requiere acción. A diferencia de puertas o elevadores, los cambios de modo y los estados anormales no aplican. Si una alarma sigue sin restablecerse, aparece como que requiere acción.

Tipos de alarma	Descripción
Alarma anti-passback (APB)	Regla anti-passback infringida
Alarma de incendios	Alarma activada al detectar un incendio
Alarma de cierre programado	Alarma activada cuando el cierre programado está activo
Alarma de intrusión	Alarma activada al detectar una intrusión
Alarma de esclusa	Incumplimiento de la regla de esclusa
Alarma de reunión	Alarma activada durante un evento de reunión

Información

- El estado de armado y las entradas deshabilitadas no aparecen como que requieren acción. Armado significa que la zona opera normalmente, y Deshabilitado significa que está desactivada intencionalmente.
- Cada entrada aparece directamente bajo el grupo de control de acceso avanzado. El árbol no despliega puertas debajo del grupo. Solo las entradas que requieren acción permanecen en el árbol. Si ninguna entrada requiere acción, el sistema quita del árbol el grupo de control de acceso avanzado.

Verificar el estado de la puerta

Verifique si la puerta está cerrada, abierta o en estado anormal. Consulta lo siguiente para el estado de la puerta.

Ícono de estado	Descripción
	La puerta está cerrada.
	La puerta está abierta.
	El sensor de la puerta no está configurado.

Verificar el estado del bloqueo de la puerta

Verifica el estado de bloqueo de la puerta mediante el estado del relé de la puerta. Consulta lo siguiente para el estado del relé de la puerta.

Ícono de estado	Descripción
	La puerta de entrada está bloqueada.
	El sistema bloquea la puerta mediante la opción **Timed** o **Permanent**.
	La puerta de entrada está abierta.
	El sistema desbloquea la puerta mediante la opción **Timed** o **Permanent**.

Información

Para obtener más información sobre las opciones de control de puertas, consulte Control de Puerta.

Verificar el estado de la cámara

Verifica el estado de la cámara para asegurarte de que funcione con normalidad. Consulta lo siguiente para el estado de la cámara.

Ícono de estado	Descripción
	La cámara está conectada.
	La cámara está apagada o desconectada.

Información

- Si no ves la cámara vinculada a la puerta de acceso, comprueba los permisos del grupo de cámaras. Si el administrador de un permiso personalizado no ha configurado los permisos del grupo de cámaras, la cámara podría no ser visible. Para obtener más información sobre cómo configurar los permisos de los grupos de cámaras, consulte Configurar la Cámara.
- Para vincular una puerta a una cámara, agrega una regla de video. Para más información, consulte Configurar Reglas de Video.

Verificar el estado de armado

Verifica el estado de seguridad de la puerta de entrada o de los ajustes avanzados de control de acceso.

Ícono de estado	Descripción
	La puerta está armada.
	La puerta está desarmada.

Información

El estado de seguridad se muestra solo cuando la puerta de entrada está configurada como **guard**. Para más información sobre la configuración de alarmas de intrusión, consulte Alarma de intrusión.

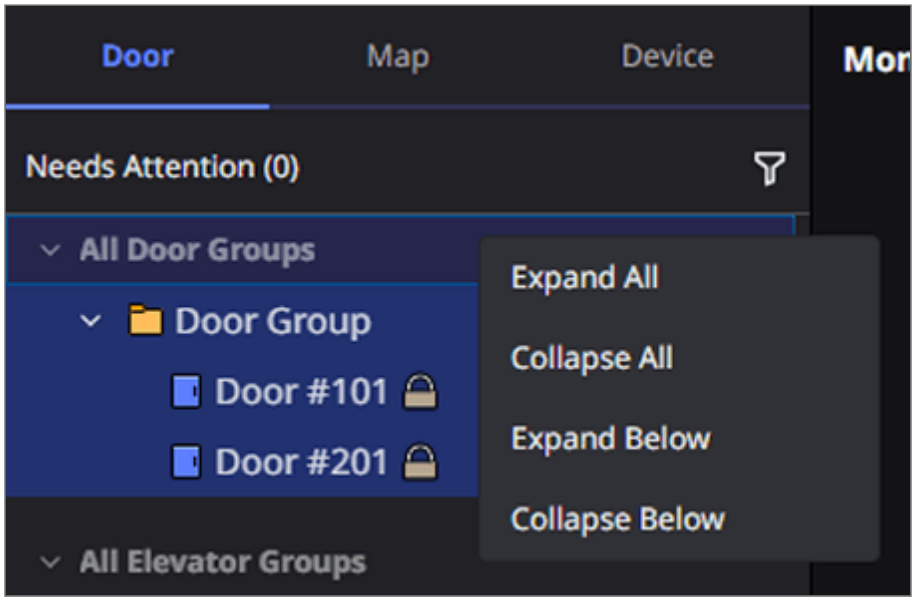
Verificar el estado del ascensor

Verifica el estado del control de acceso por piso a través del ascensor.

Ícono de estado	Descripción
	El piso correspondiente está bloqueado a través del ascensor.
	El piso correspondiente está desbloqueado a través del ascensor.

Expandir/contraer lista de grupos

Expande o contrae la lista mediante el grupo de nivel superior o el subgrupo.



Grupo de nivel superior

1. En la pestaña **Door**, selecciona **All Door Groups** o **All Elevator Groups**, **All Advanced ACs** y haz clic derecho.
2. Elige **Expand All** o **Collapse All** en el menú emergente.

Todas las sublistas pueden expandirse o contraerse según el grupo de nivel superior seleccionado.

Subgrupo

1. Para expandir o contraer la lista de subgrupos en cada grupo de nivel superior, selecciona el subgrupo y haz clic derecho.
2. Selecciona la opción **Expand Below** o **Collapse Below** en el menú emergente.

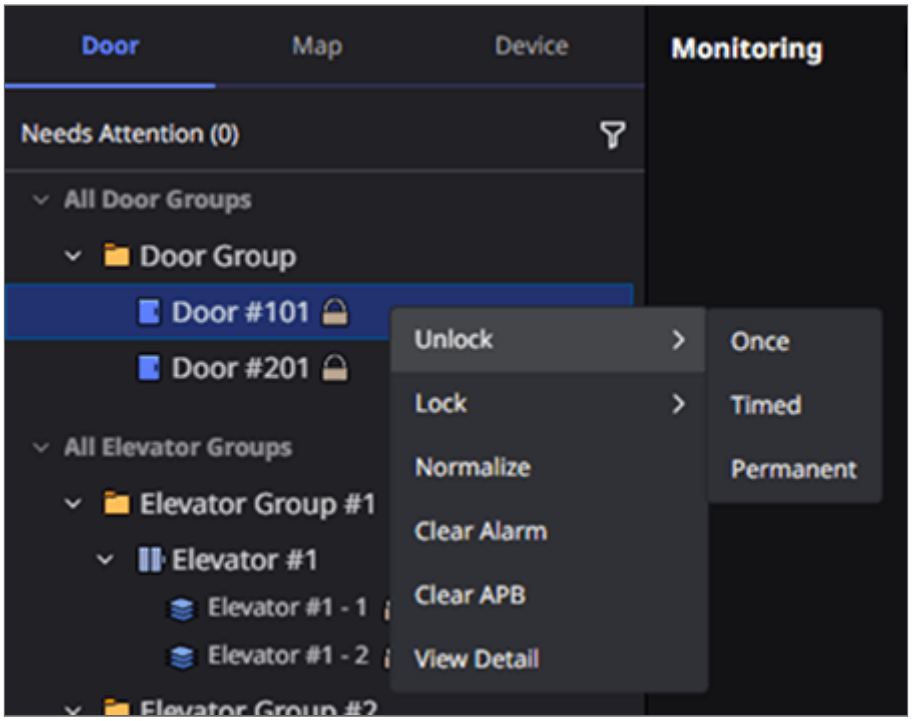
Puedes expandir o contraer la lista del subgrupo seleccionado.

Control de Puerta

Esta guía describe cómo controlar puertas. Bloquea la puerta durante un periodo determinado, verifica la cámara conectada a la puerta y borra las alarmas que se hayan generado.

- Controla la puerta de forma remota para administrar el acceso. Configura la puerta para que permanezca abierta o bloqueada durante un periodo específico.
- Monitorea en tiempo real las situaciones de acceso mediante la cámara conectada a la puerta.
- La función anti-passback evita el acceso no autorizado y gestiona los registros de acceso con precisión.

Haga clic en **Monitoring** en la página **Launcher** o seleccione **Monitoring** en la lista de accesos directos en la esquina superior izquierda de la pantalla. Selecciona la puerta que deseas controlar y haz clic derecho. Seleccione la función deseada en el menú emergente.

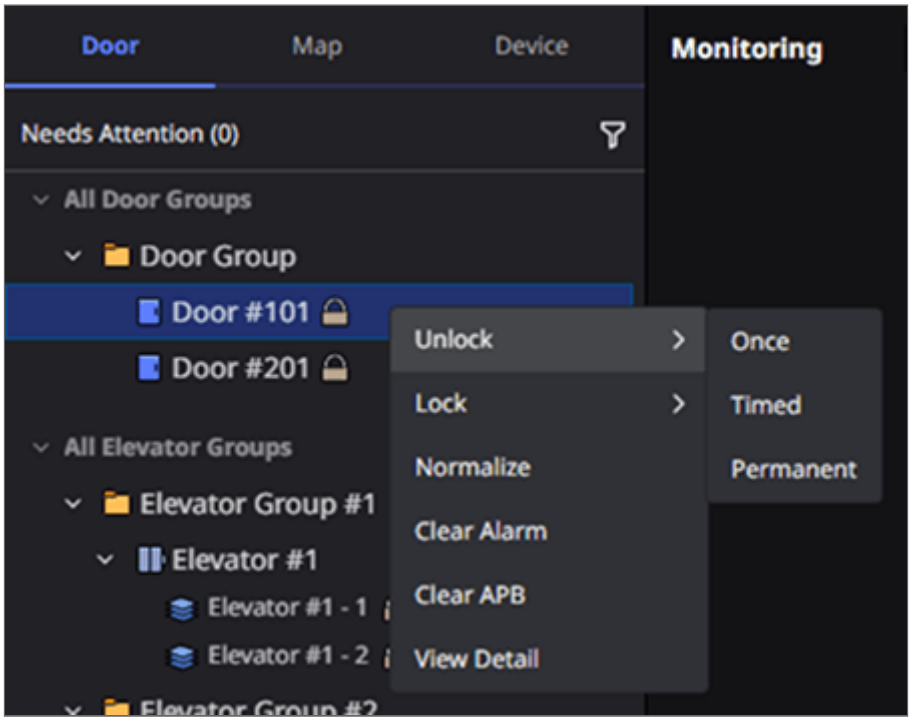


Información

- La función **Log Upload** debe estar habilitada para supervisar o controlar el estado de la puerta de acceso. Habilita esta función en **Settings** → **System** → **Server** en la sección **General**.
- La opción **Open Video** está vinculada al VMS y requiere la integración de la puerta de acceso y la cámara para poder usarse. Además, esta funcionalidad está disponible mediante la compra de opciones adicionales con una licencia **Essential** o superior. Para obtener más información sobre la política de licencias, consulte Política de Licencias.
- Para controlar varias puertas a la vez, consulte Control Masivo.

Abrir puerta

Cualquiera puede acceder a la puerta cuando está abierta. Haga clic en **Unlock** en el menú emergente y seleccione la opción deseada.



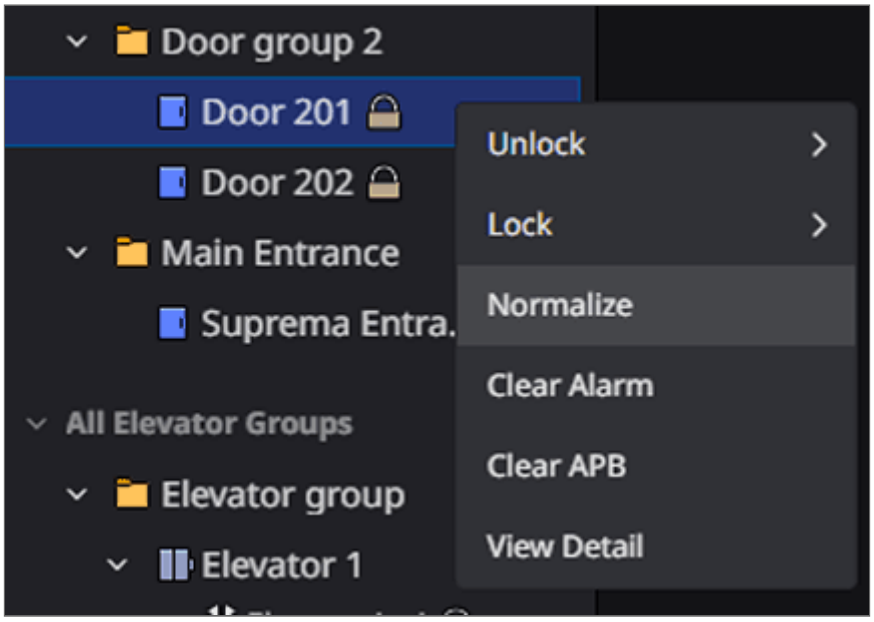
- **Once**: Desbloquea la puerta una vez.
- **Timed**: Abre la puerta durante un tiempo determinado. Ingresa el tiempo deseado en segundos.
- **Permanent**: Desbloquea la puerta sin límite de tiempo.

Al abrir temporalmente la puerta, el icono del relé de la puerta cambia de a . Al abrir la puerta con la opción **Timed** o **Permanent**, el icono cambia a .

> **Consejo**
> La puerta puede abrirse temporalmente para la comodidad de los visitantes externos. Después de abrir la puerta, cambia al modo **Normalize**.

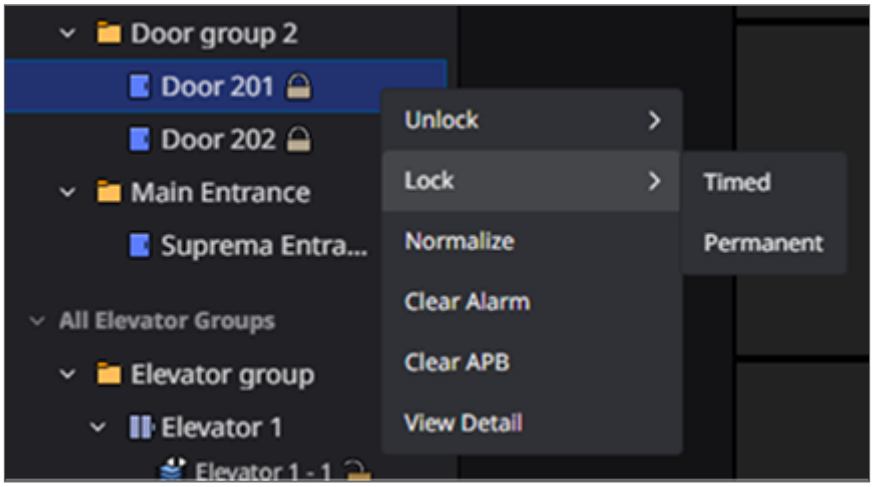
Normalizar puerta

Cambiar la puerta al estado **Normalize** permitirá el acceso solo a usuarios autorizados. Haga clic en **Normalize** en el menú emergente.



Bloquear puerta

Cambiar la puerta al estado **Lock** impedirá el acceso a cualquier persona. Haz clic en **Lock** en el menú emergente y selecciona la opción deseada.

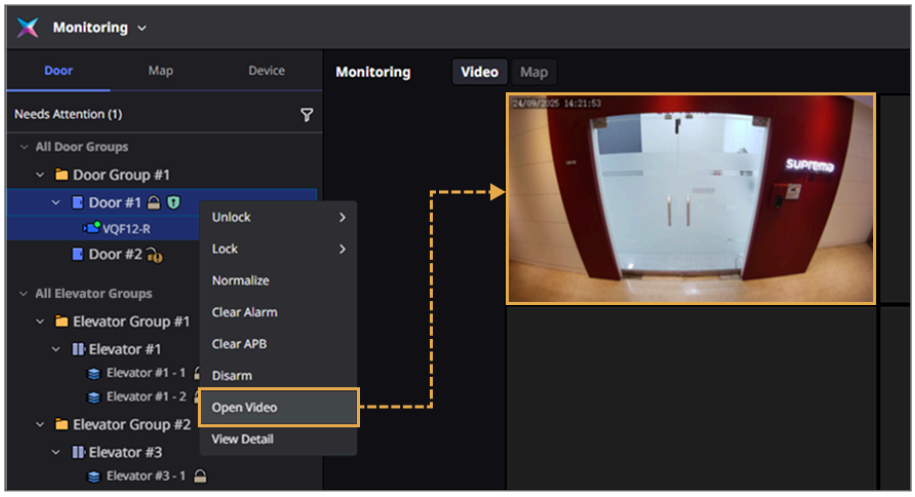


- **Timed**: Cambia la puerta a un estado bloqueado durante un período determinado. Ingresa el tiempo deseado en segundos.
- **Permanent**: Cambia la puerta a un estado bloqueado sin límite de tiempo.

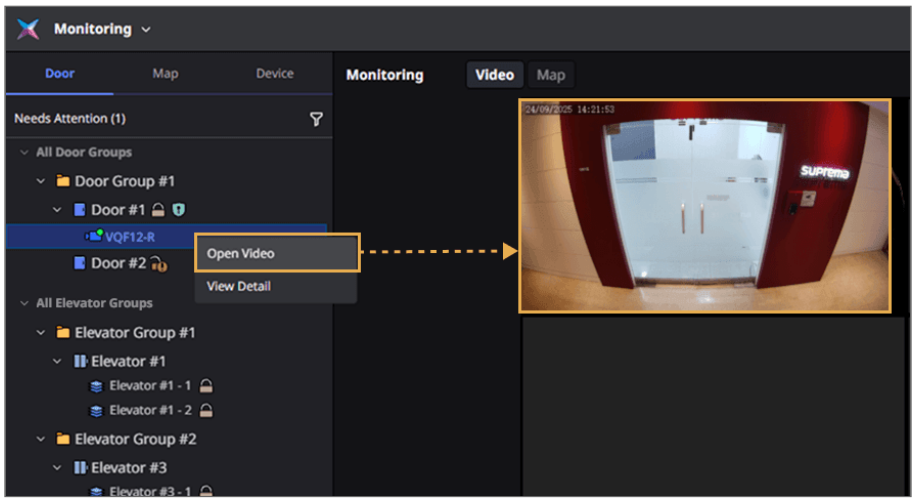
Al bloquear la puerta, el icono del relé de la puerta cambia a .

Ver cámara de la puerta

Consulta la cámara conectada a la puerta. Haz clic en **Open Video** en el menú emergente. Agrega y reproduce el metraje de la cámara seleccionada en la sección de mosaicos de video de **Monitoring**.



O selecciona la cámara deseada y haz clic con el botón derecho del ratón. Haz clic en **Open Video** en el menú emergente para añadir y reproducir la grabación de la cámara seleccionada.

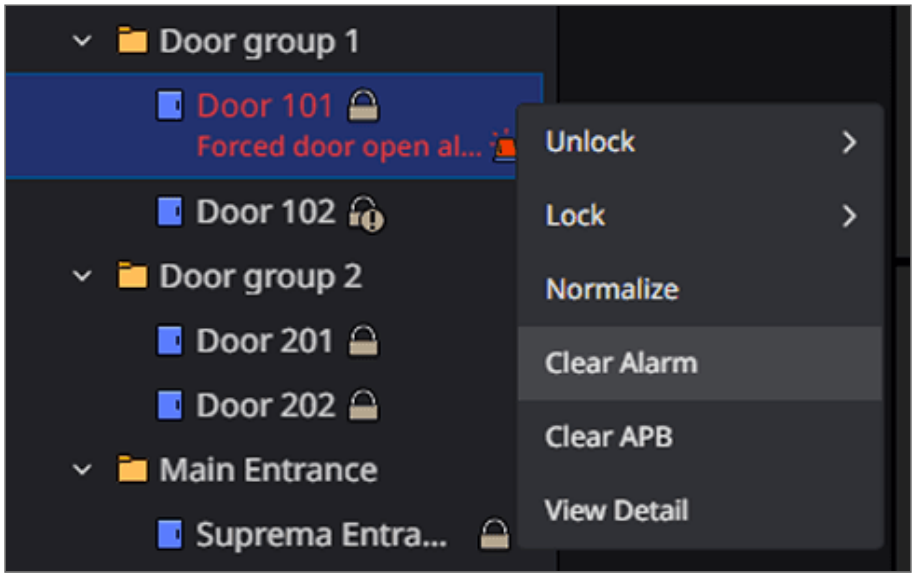


Información

- Si hay más de una cámara conectada a la puerta de acceso, la primera cámara conectada aparece en el mosaico de video.
- Los mosaicos de video se añaden en orden desde la parte superior izquierda de la pantalla. Si no hay espacio para añadir más, aparece un mensaje de error.
- Para obtener más información sobre el monitoreo de video, consulte Supervisar Video.
- Si no ves la cámara vinculada a la puerta de acceso, comprueba los permisos del grupo de cámaras. Si el administrador de un permiso personalizado no ha configurado los permisos del grupo de cámaras, la cámara podría no ser visible. Para obtener más información sobre cómo configurar los permisos de los grupos de cámaras, consulte Configurar la Cámara.
- Esta característica está disponible al comprar opciones adicionales con una licencia **Essential** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Restablecer alarma

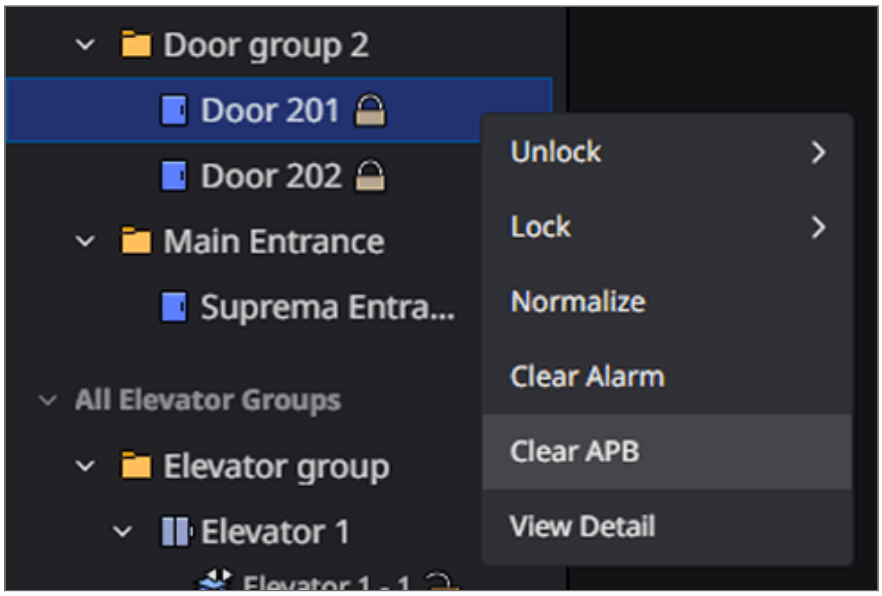
Desactiva la alarma que se generó en la puerta. Haga clic en **Clear Alarm** en el menú emergente. Un mensaje de alarma aparece en la esquina superior derecha de la pantalla.



Restablecer anti-passback

Desactiva la alarma APB cuando se produzca una violación de anti-passback.

1. Haz clic en **Clear APB** en el menú emergente.



2. Cuando aparezca la ventana **Clear APB**, revisa la lista de todos los usuarios.



3. Selecciona al usuario que violó la regla anti-passback y haz clic en **Apply**.

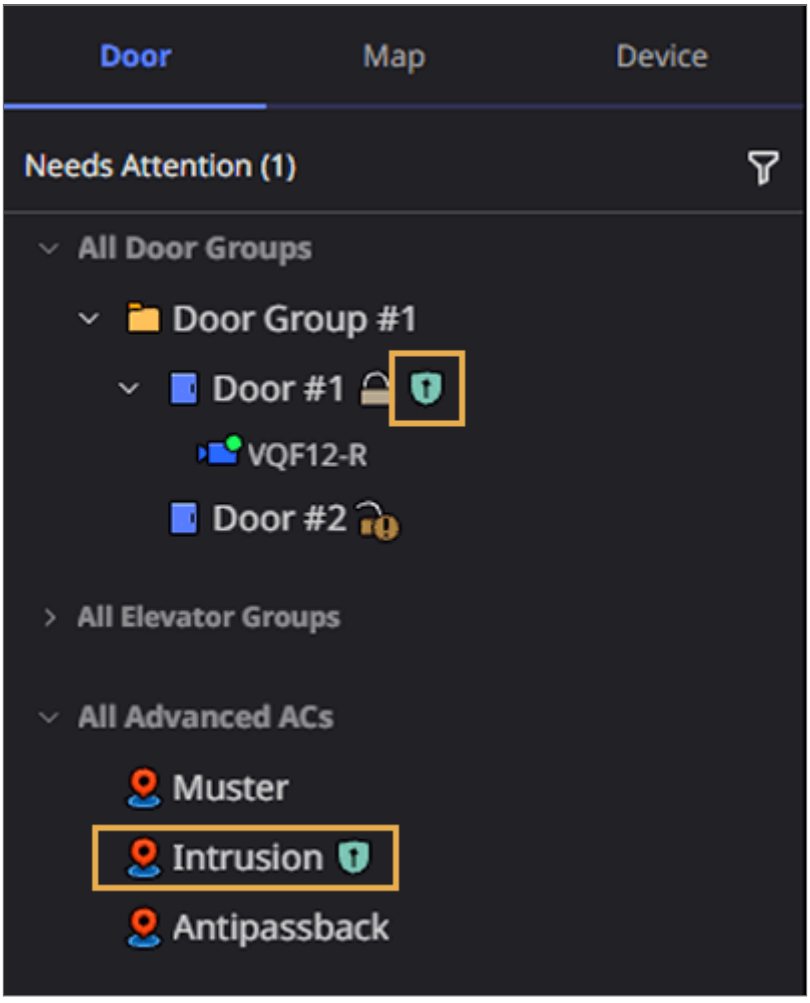
Un mensaje de finalización aparece en la esquina superior derecha de la pantalla.

Información

- **안티패스백(Anti-Passback)**: 출입 통제를 위해 구조적인 방법으로서, 출입문 안쪽/바깥쪽에 출입 통제 장치를 설치하여 구역에 출입할 때 반드시 인증을 통해 출입해야 하는 기능입니다. 카드를 사용해 출입할 때 리더기에 카드를 인식하지 않고 앞 사람을 따라 입실했다면, 퇴실할 때 출입문이 열리지 않으며 **안티패스백** 이벤트가 발생합니다. **안티패스백**은 Hard APB와 Soft APB로 구분합니다. **안티패스백** 위반 시 Hard APB는 **안티패스백** 이벤트를 생성하고 출입할 수 없으며, Soft APB는 **안티패스백** 이벤트를 생성하고 출입은 가능합니다.
- Para obtener más información sobre cómo configurar el **anti-passback** para una puerta, consulte Registrar Puerta.

Activar o desactivar la alarma

Si la puerta está configurada en modo seguridad, activa o desactiva la seguridad. Haz clic en **Arm** o **Disarm** en el menú emergente.

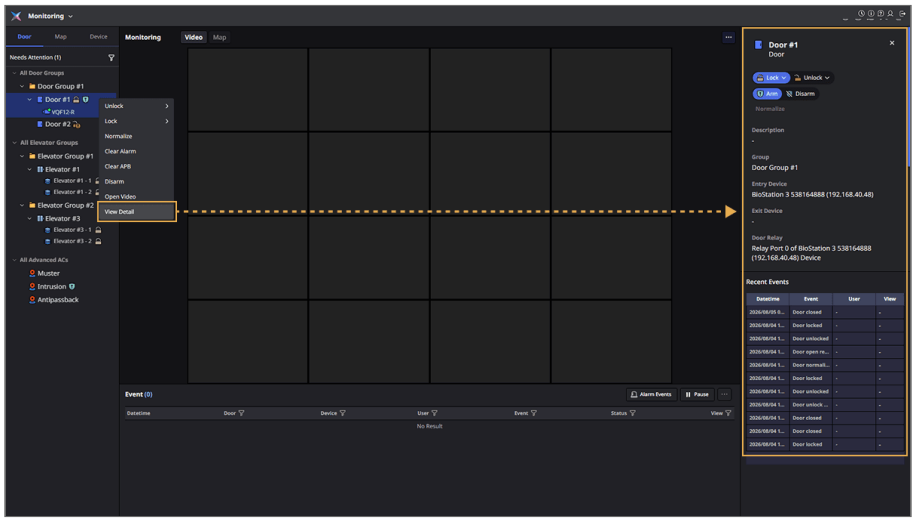


Una puerta armada cambia el icono de estado de armado de a . El icono también se aplica al ajuste de control de acceso correspondiente.

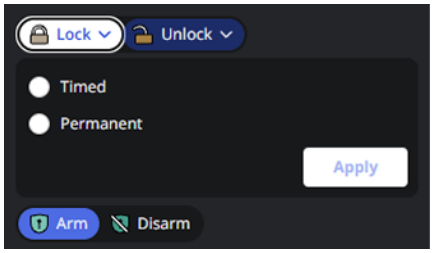
> **Información**
>
> Esta funcionalidad está disponible al adquirir opciones adicionales con una licencia **Essential** o con una licencia **Enterprise** o superior. Para obtener más información sobre la política de licencias, consulte Política de Licencias.

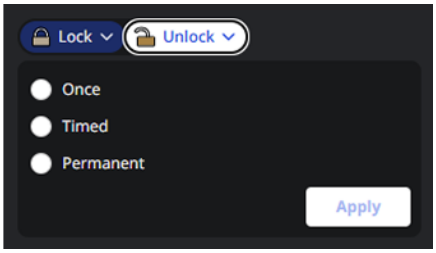
Ver detalles

Consulta la información detallada de la puerta y el historial de eventos. Haga clic en **View Detail** en el menú emergente. Aparece un panel en el lado derecho de la pantalla que muestra el control de la puerta, los detalles de la puerta y el historial de eventos.



- **Control de la puerta**: Cambie el estado de la puerta a bloqueada, abierta, armada o desarmada.





- **Normalize**: Use esta opción si un administrador abre o bloquea la puerta manualmente.
- **Información detallada de la puerta**: Consulta el nombre, la ubicación, el estado y la información de los subdispositivos conectados a la puerta.
- **Recent Events**: Consulta la lista de eventos recientes que se produjeron en la puerta de acceso seleccionada.

> **Información**
>
> Para obtener más información sobre cada elemento de la sección de detalles de la puerta, consulte Registrar Puerta.

Controlar Ascensores

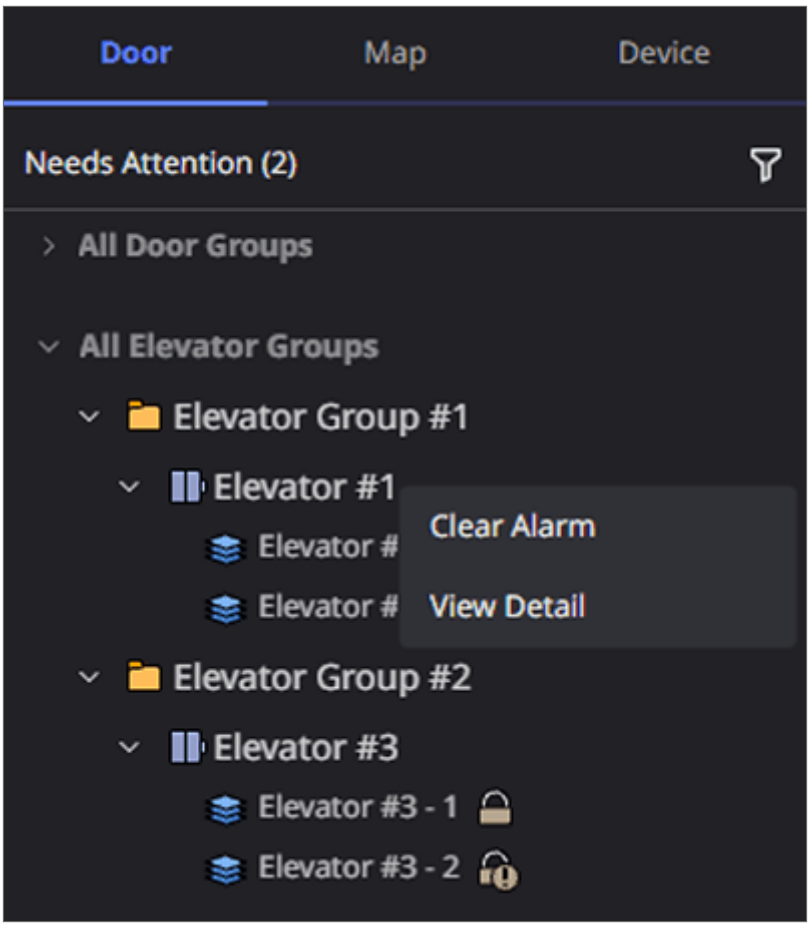
Esta guía describe cómo controlar el ascensor. Controle el ascensor o verifique información detallada mediante las funciones proporcionadas.

1. Haga clic en **Monitoring** en la página **Launcher** o seleccione **Monitoring** en la lista de accesos directos en la esquina superior izquierda de la pantalla.
2. En la pestaña **Door** de la barra lateral izquierda, vaya a **All Elevator Groups**.
3. Seleccione el ascensor en el grupo deseado y haga clic con el botón derecho. Seleccione la función deseada en el menú emergente.

> **Información**
>
> - Para más información sobre cómo configurar los ascensores y los grupos, consulte Administrar Ascensores.
> - Para controlar varios ascensores y pisos a la vez, consulte Control Masivo.

Controlar Ascensores

Reconozca o verifique detalles de las alarmas activadas por el ascensor.

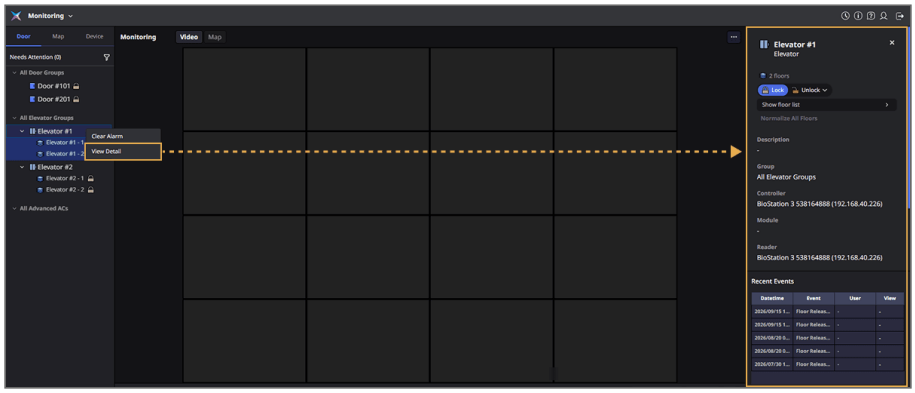


Borrar alarma

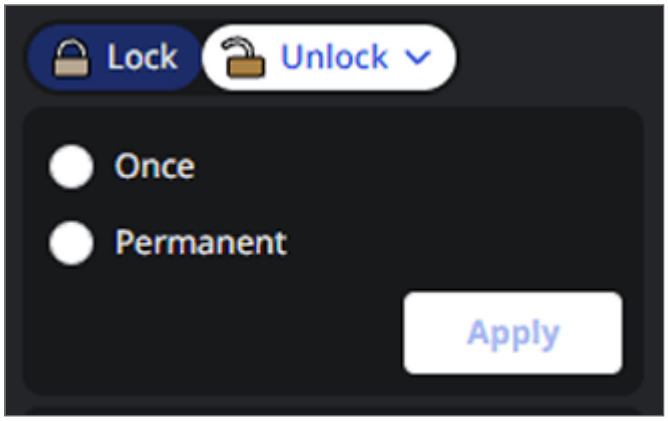
Desactive la alarma que se produjo en este ascensor. Haga clic en **Clear Alarm** en el menú emergente. Un mensaje de finalización aparece en la esquina superior derecha de la pantalla.

Ver detalles

Verifique información detallada sobre el ascensor y el historial de eventos. Haga clic en **View Detail** en el menú emergente. La información detallada y el historial de eventos del ascensor aparecen en el lado derecho de la pantalla.



- **Control del ascensor**: Establezca el ascensor como bloqueado o abierto.



- **Show floor list**: Muestra la lista de pisos configurados para el ascensor.

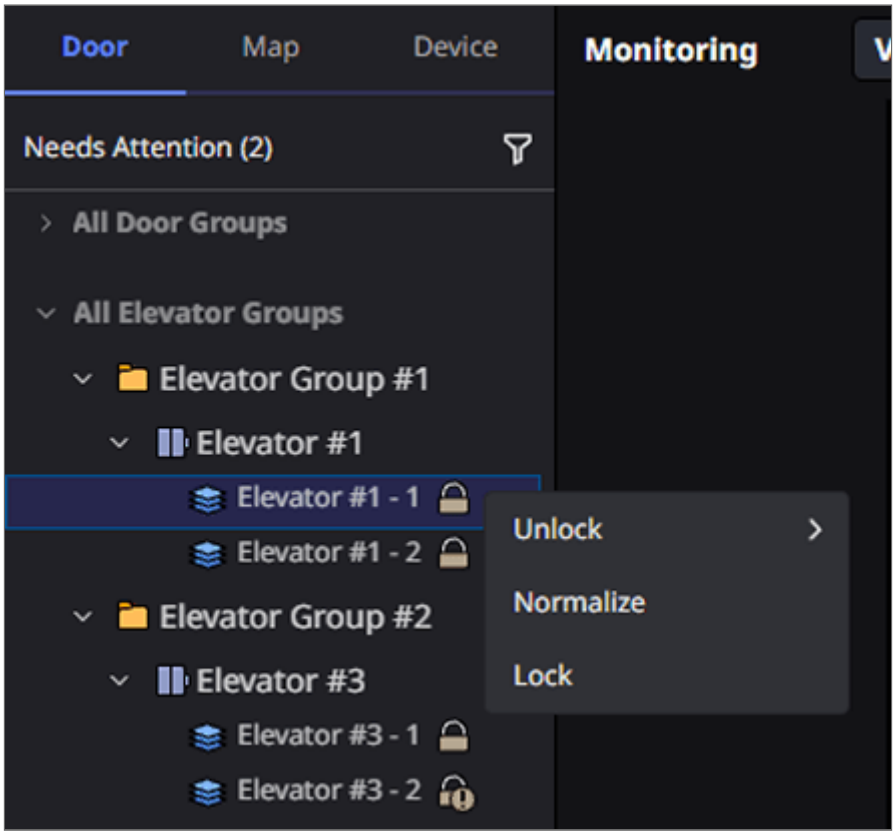


- **Normalize All Floors**: Úselo cuando un administrador abre o bloquea manualmente todos los pisos.
- **Ver detalles**: Verifique el nombre, la ubicación, la información de estado y más del ascensor.
- **Recent Events**: Verifique la lista de eventos recientes que ocurrió en el ascensor seleccionado.

> **Información**
> Para más información sobre cada elemento de la sección Detalles del ascensor, consulte Registrar Ascensor.

Control de acceso a pisos

Controle los pisos a los que se puede acceder desde el ascensor. Haga clic en el relé del piso configurado en el ascensor y haga clic con el botón derecho. Seleccione la función deseada en el menú emergente.



Abrir piso

Cualquier persona puede acceder al piso abierto. Haga clic en **Unlock** en el menú emergente y seleccione la opción deseada.

- **Once**: Abre el piso una vez.
- **Permanent**: Abre el piso sin restricciones de tiempo.

> **Consejo**
> El piso puede abrirse temporalmente para la comodidad de los visitantes externos cuando lleguen. Después de abrir el piso, cambie al modo **Normalize**.

Normalizar piso

Al cambiar el piso al estado **Normalize**, solo los usuarios autorizados podrán acceder. Haga clic en **Normalize** en el menú emergente.

Bloquear piso

Al cambiar el piso al estado **Lock**, se evitará el acceso de cualquier persona. Haga clic en **Lock** en el menú emergente.

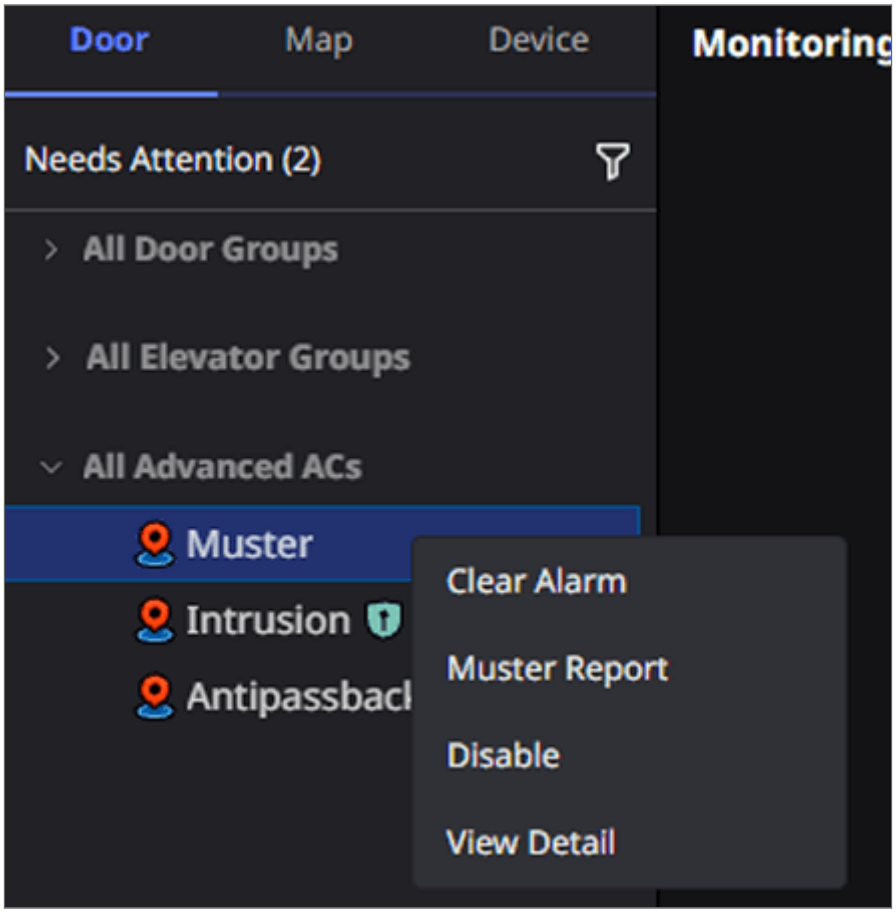
Gestionar el Control de Acceso Avanzado

Esta guía explica cómo controlar puertas o dispositivos configurados con control de acceso avanzado. Las funciones proporcionadas permiten respuestas rápidas y una gestión eficiente en caso de problemas.

1. Haga clic en **Monitoring** en la página **Launcher** o seleccione **Monitoring** en la lista de accesos directos en la esquina superior izquierda de la pantalla.

2. Vaya a la pestaña **Door** en la barra lateral izquierda de la pantalla y seleccione **All Advanced ACs**.

3. Seleccione el control de acceso avanzado configurado y haga clic derecho. Seleccione la función deseada en el menú emergente.



Información

- Las funciones ofrecidas varían según el tipo de control de acceso avanzado. Los tipos de control de acceso avanzado son los siguientes.
  - **Anti-Passback**
  - Alarma de incendios
  - Bloqueo/desbloqueo programado
  - Alarma de intrusión
  - Esclusa
  - Reunión
  - Límite de ocupación
  - Pase de lista
- Para más información sobre cada función de control de acceso avanzado, consulte Configuración Avanzada de Control de Acceso.
- Para seleccionar y controlar varios ajustes de control de acceso avanzado a la vez, consulte Control Masivo.

Borrar anti-passback

Borre la alarma APB de la puerta o dispositivo configurado con **Anti-Passback**. Haz clic en **Clear APB** en el menú emergente. Un mensaje de finalización aparece en la parte superior de la pantalla.

Información

- La función **Clear APB** solo está disponible para **Anti-Passback**.
- Para obtener más información sobre la configuración de **Anti-Passback**, consulte Anti-retorno.
- Para obtener más información sobre **Anti-Passback**, consulte Glosario.

Borrar alarma

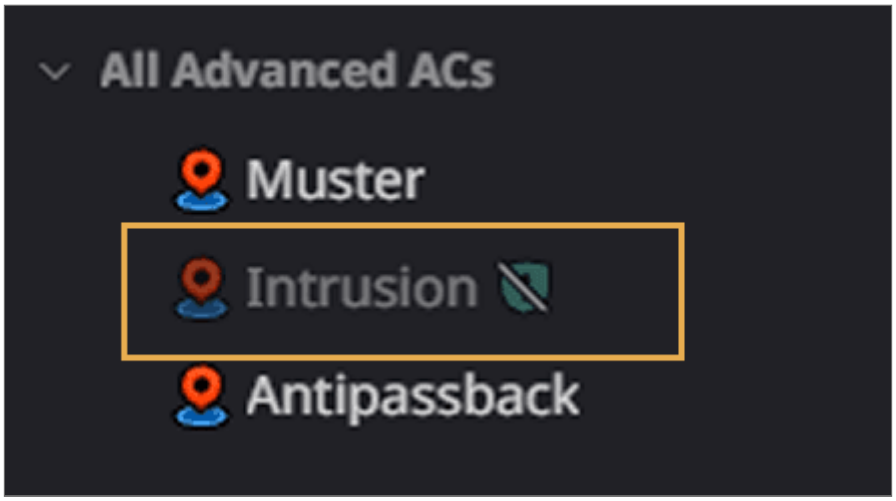
Borre la alarma que ocurrió en la puerta o dispositivo. Haga clic en **Clear Alarm** en el menú emergente. Un mensaje de finalización aparece en la parte superior de la pantalla.

Información

Clear Alarm no se puede usar en la función de límite de ocupación.

Activar/desactivar

Active el control de acceso avanzado o desactive las funciones que no se usen. El control de acceso avanzado desactivado aparece atenuado. Haga clic en **Enable** o **Disable** en el menú emergente.



Seguridad/desarmar

Active o desactive la seguridad de la puerta o dispositivo. Haz clic en **Arm** o **Disarm** en el menú emergente.

Información

- **Arm** o **Disarm** solo pueden usarse en controles de acceso avanzado configurados para seguridad.
- Para más información sobre la configuración de alarmas de intrusión, consulte Alarma de intrusión.

Ver informe de reunión

Haga clic en **Muster Report** para revisar el informe de reunión. En la nueva ventana, verifique las horas de entrada y salida de los usuarios y si el tiempo de estancia se ha excedido, mediante la lista de usuarios y los dispositivos configurados con la función de reunión.

> **Información**
>
> - La función **Muster Report** solo está disponible en los reunión.
> - Para obtener más información sobre la función de control de presencia, consulte Reunión.

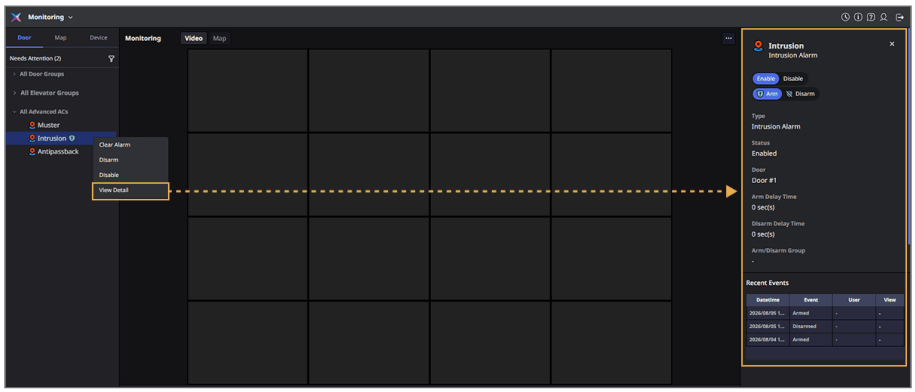
Monitorear límite de ocupación

Verifique el estado de los dispositivos configurados con la función de límite de ocupación. Haga clic en **Occupancy Monitoring** en el menú emergente. En la nueva ventana, vaya al menú **Settings** → **Access Management** → **Advanced AC**. Verifique el estado en la lista **Occupancy Limit**.

> **Información**
>
> - La función **Occupancy Monitoring** solo está disponible para elementos configurados con la función de límite de ocupación.
> - Para obtener más información sobre la configuración del límite de ocupación, consulte Límite de Ocupación.

Ver detalles

Verifique la información detallada y el historial de eventos del control de acceso avanzado. Haga clic en **View Detail** en el menú emergente. La información detallada y el historial de eventos se muestran en el panel derecho de la pantalla.



- **Control de acceso avanzado**: Controle el tipo de control de acceso avanzado seleccionado.
- **Información detallada**: Verifique el nombre y el estado de la función de control de acceso avanzado, la información del dispositivo, etc.
- **Recent Events**: Verifique la lista de eventos recientes ocurridos en el control de acceso avanzado seleccionado.

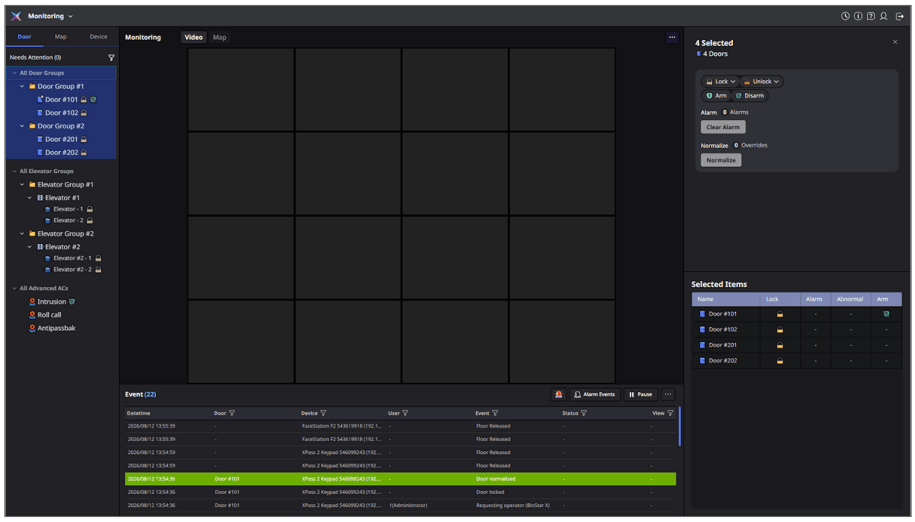
> **Información**
>
> Para obtener más información sobre cada elemento en la sección de detalles del control de acceso avanzado, consulte Configuración Avanzada de Control de Acceso.

Control Masivo

Esta guía explica cómo seleccionar varias puertas, ascensores o ajustes avanzados de control de acceso y ejecutar Desbloquear, Bloquear o Borrar alarma a la vez.

- Si selecciona dos o más entradas en el árbol de estado, el panel de control masivo aparece en el lado derecho de la pantalla. Ejecute comandos a la vez sin controlar cada entrada por separado.
- Responda rápidamente durante emergencias o al controlar varias entradas al mismo tiempo.
- Seleccione puertas, elevadores (pisos) o ajustes avanzados de control de acceso de forma masiva y contrólelos. El sistema no permite el control masivo para tipos mixtos.

Haga clic en **Monitoring** en la página **Launcher** o seleccione **Monitoring** en la lista de accesos directos en la esquina superior izquierda de la pantalla. Si selecciona dos o más entradas en el árbol de estado de la barra lateral izquierda, el panel de control masivo aparece en el lado derecho de la pantalla.



> **Información**
>
> - El control masivo no incluye cámaras. Si selecciona cámaras junto con otras entradas, el sistema las quita de la lista de selección.
> - Este documento explica cómo controlar varias entradas a la vez. Para controlar una sola puerta, un elevador o un ajuste avanzado de control de acceso, consulte el siguiente documento.
>   - Control de Puerta
>   - Controlar Ascensores
>   - Gestionar el Control de Acceso Avanzado

Seleccionar varias entradas

Para seleccionar puertas, elevadores, pisos o control de acceso avanzado en el árbol de estado de la barra lateral izquierda, siga estos pasos. Funciona igual que seleccionar varios archivos en el Explorador de archivos de Windows.

- **Clic**: Seleccione una entrada. Esto borra la selección anterior.
- `Ctrl` + **clic**: Agregue a la lista de selección la entrada en la que hizo clic o quítela. Esto mantiene el resto de la selección.
- `Shift` + **clic**: Seleccione el rango visible desde la última entrada en la que hizo clic hasta la entrada actual. Reemplace la selección actual por este rango.

- Ctrl + Shift + **clic**: Agregue un rango sin borrar la selección actual. Use esto para seleccionar varias entradas no adyacentes.

- **Clic en un grupo**: Seleccione el nombre de un grupo ( ) para seleccionar todas las puertas, elevadores, pisos y ajustes avanzados de control de acceso de ese grupo. Para expandir o contraer un grupo, haz clic en la flecha (›) antes del nombre del grupo.

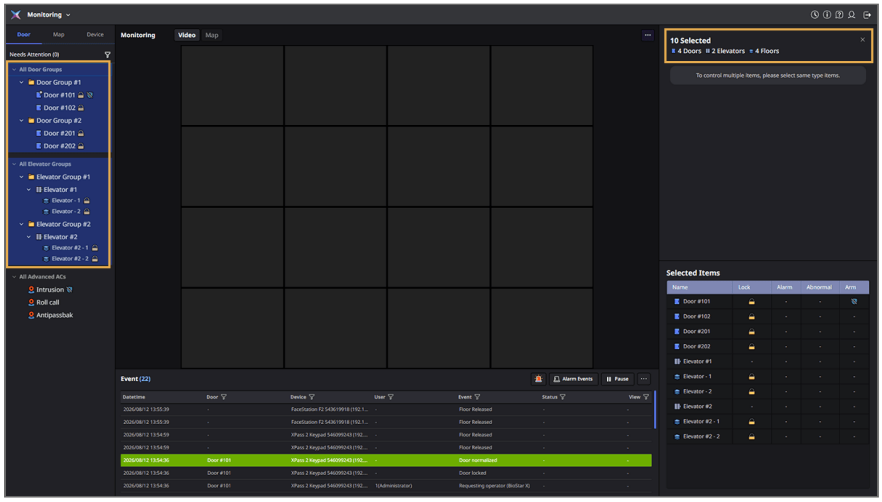
> **Información**
>
> El panel de control masivo no se abre cuando no seleccionas ninguna entrada o solo una. Cuando solo queda una entrada seleccionada, aparece la vista detallada. Cuando borras todas las selecciones, el panel derecho desaparece.

Diseño del panel de control masivo

Selecciona varias entradas en el árbol de estado de la barra lateral izquierda. El panel de control masivo aparece a la derecha de la siguiente manera.

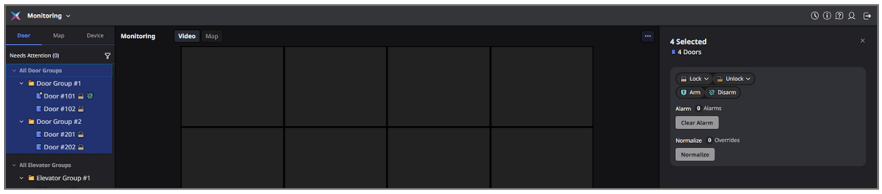
- **Cantidad y tipos de selección**: Por ejemplo, si seleccionas 4 puertas, 2 elevadores y 4 pisos, aparece de la siguiente manera.

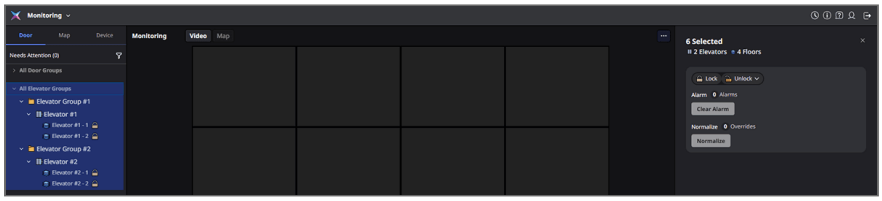
  > ***10 Selected** / **4 Doors 2 Elevators 4 Floors***



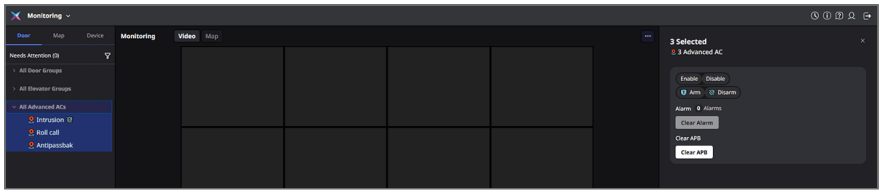
  > Las características de control no están disponibles cuando seleccionas tipos diferentes juntos.

- **Control de puertas/elevadores**: Muestra las características de control disponibles para puertas y elevadores.

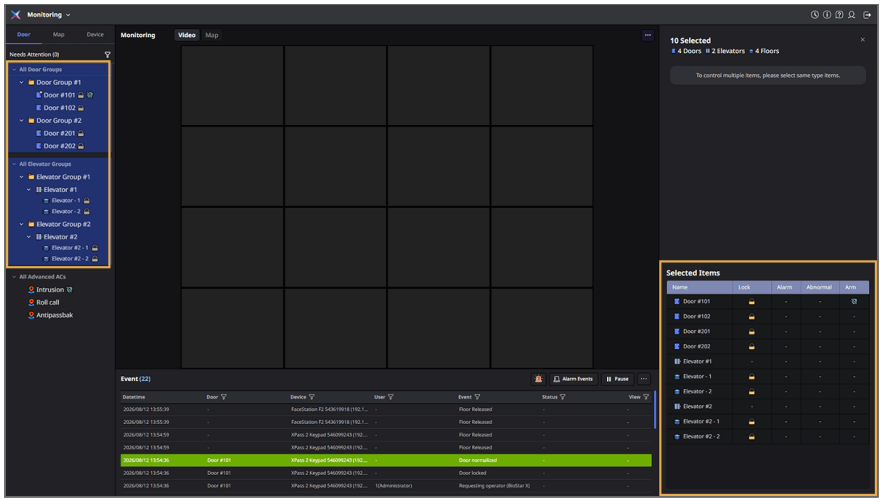




- **Control de acceso avanzado**: Muestra las características de control disponibles en el control de acceso avanzado.

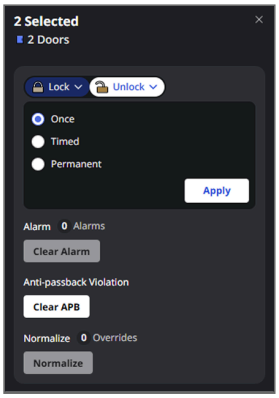


- **Tabla de resumen de entradas seleccionadas**: La parte inferior del panel derecho muestra el nombre y el estado de cada entrada seleccionada. Arrastra el divisor entre el área de control y la tabla de resumen hacia arriba o hacia abajo para ajustar sus alturas. Si seleccionas muchas entradas, arrastra el divisor para expandir el área de la tabla de resumen.



Control masivo de puertas

Cuando seleccionas al menos dos puertas, usa los mismos controles básicos y avanzados que en el control de una sola puerta.



Control básico

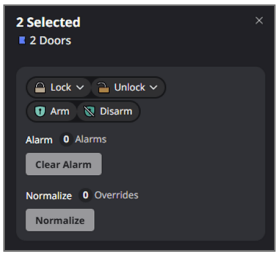
- **Once**: Aplica el estado de desbloqueo una vez.
- **Timed**: Mantiene el estado bloqueado o desbloqueado durante el tiempo especificado.
- **Permanent**: Establece el estado bloqueado o desbloqueado sin límite de tiempo.

Selecciona un comando para aplicar y haz clic en **Apply**.

Control avanzado

Usa los siguientes botones cuando al menos una entrada seleccionada cumple las condiciones que se indican a continuación.

- **Clear Alarm**: Disponible cuando al menos una puerta seleccionada tiene



una alarma activa.

- **Clear APB**: Disponible cuando al menos una puerta seleccionada tiene el antirretorno habilitado. Para más información, consulte Control de Puerta.
- **Normalize**: Disponible cuando un administrador desbloquea o bloquea una puerta manualmente. Esto excluye estados cambiados por horarios o emergencias.
- **Arm** / **Disarm**: Aparece solo cuando la puerta se establece en alarma de intrusión, un ajuste avanzado de control de acceso.

Información

- Haga clic en **Clear Alarm** o **Normalize**. Aparece una ventana emergente. En la ventana emergente, haga clic en **Normalize** o **Normalize** para borrarlos. En cambio, **Arm**/**Disarm** cambia el estado sin un cuadro de diálogo de confirmación.
- Los ajustes avanzados de control de acceso están disponibles al comprar un complemento con una licencia **Essential**, o con una licencia **Enterprise** o superior. Para obtener más información sobre la política de licencias, consulte Política de Licencias.

Control masivo de ascensores y pisos

Seleccione un ascensor para controlar todos los pisos configurados en conjunto. Para controlar solo ciertos pisos, seleccione los pisos directamente.

Las diferencias con las puertas son las siguientes.

Característica de control	Puerta	Ascensor, piso
Unlock	**Once**, **Timed**, **Permanent**	**Once**, **Permanent**
Lock	**Timed**, **Permanent**	**Permanent**
Normalize	Soportado	Soportado
Clear Alarm	Soportado	Aparece cuando la selección incluye un ascensor; no aparece si solo se seleccionan pisos
Clear APB	Soportado	No compatible

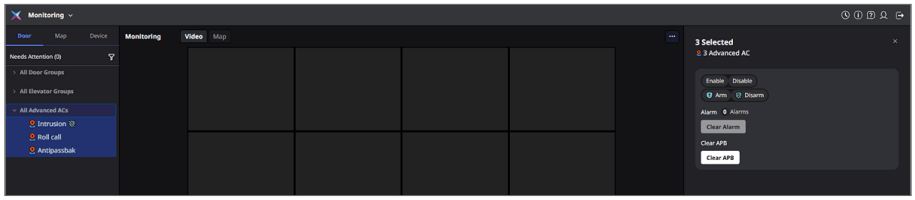
Información

Si selecciona un ascensor y sus pisos, el sistema envía un comando de desbloqueo/bloqueo por ascensor.

Control masivo del control de acceso avanzado

Seleccione varios ajustes de control de acceso avanzado para controlarlos a la vez. Al seleccionar dos o más, el panel derecho cambia al panel de control masivo. Las acciones de selección, rango y filtro son iguales para puertas y elevadores.

Los ajustes avanzados de control de acceso no incluyen relés de bloqueo ni bloqueo/desbloqueo del operador, por lo que las opciones difieren de puertas y elevadores. Los siguientes botones de control aparecen según el tipo de ajuste seleccionado.

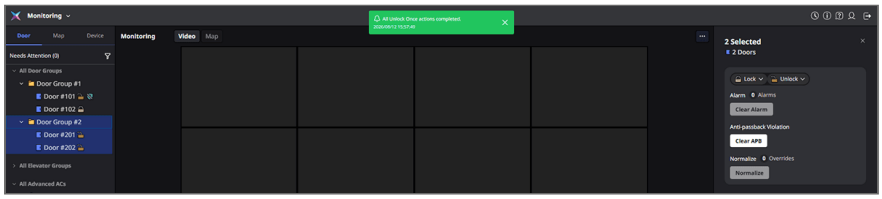


- **Enable**/**Disable**: Aparece para todos los ajustes avanzados de control de acceso.
- **Arm**/**Disarm**: Aparece solo cuando la selección se establece en alarma de intrusión.
- **Clear Alarm**: Aparece solo cuando la selección incluye ajustes que activan alarmas (anti-passback, alarma de incendio, bloqueo programado, alarma de intrusión, interbloqueo o muster). No aparece si selecciona solo ajustes sin alarma, como límite de ocupación o verificación de recuento.
- **Clear APB**: Aparece solo cuando la selección incluye el ajuste de anti-passback. Haz clic en este botón. En la ventana de selección de usuarios, selecciona un usuario que incumplió el ajuste de anti-passback y borra la alarma de APB. Para obtener más información, consulte Gestionar el Control de Acceso Avanzado.

> **Información**
>
> - El control masivo no incluye **Lock**, **Unlock** ni **Normalize**. El panel de control masivo también excluye funciones que abren otras pantallas, como el informe de muster y el monitoreo del límite de ocupación. Use estas funciones en la pantalla de detalles cuando seleccione un solo ajuste.
> - Para más información sobre el control de acceso avanzado, consulte Gestionar el Control de Acceso Avanzado.

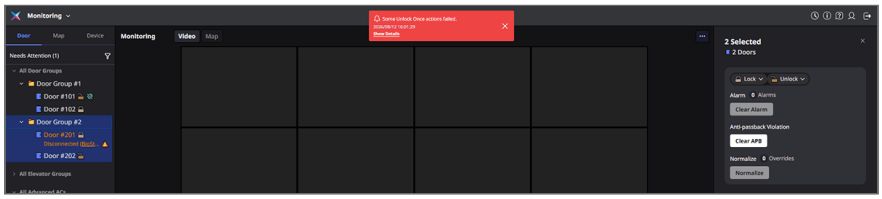
Verifique los resultados de ejecución

- Si todas las entradas seleccionadas se ejecutan correctamente, aparece un mensaje de éxito en la parte superior de la pantalla.



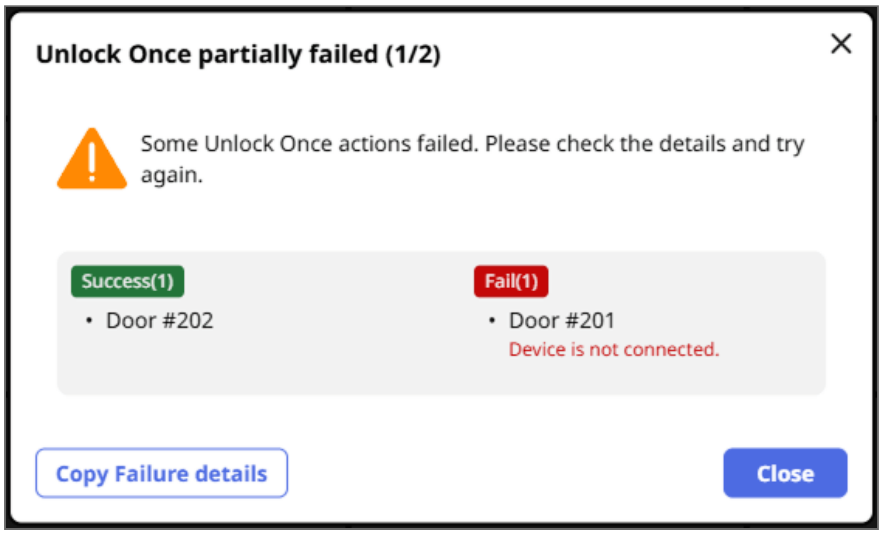
La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

- Si alguna entrada falla, aparece un mensaje de fallo con el botón **Show Details**.



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

Haga clic en **Show Details** para ver los resultados agrupados en **Success**, **Failure** y **Skipped**. Haga clic en **Copy Failure details** para copiar al portapapeles los nombres y los motivos de las entradas fallidas.



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

Monitorear Mapa

Esta guía explica cómo monitorear y controlar el estado en tiempo real de puertas y cámaras por zona y piso mediante la función de monitoreo de mapas. El monitoreo de mapas permite navegar fácilmente por áreas y pisos a través de una interfaz visual integrada con Google Maps, habilitando funciones como el control de puertas de acceso y la reproducción de video de cámaras.

Para acceder a la página **Monitoring**, haz clic en **Monitoring** en **Launcher** o selecciona **Monitoring** en el menú de la parte superior izquierda de la pantalla.

En **BioStar X** se pueden configurar múltiples instalaciones dentro de una sola área. Cada instalación puede tener varios pisos configurados. En un piso, puede configurar la puerta y la cámara según el plano para su monitoreo. Consulte lo siguiente.



Puede acceder al área configurada en el mapa GIS en el orden Área → Instalación → Piso, como se muestra en la imagen,

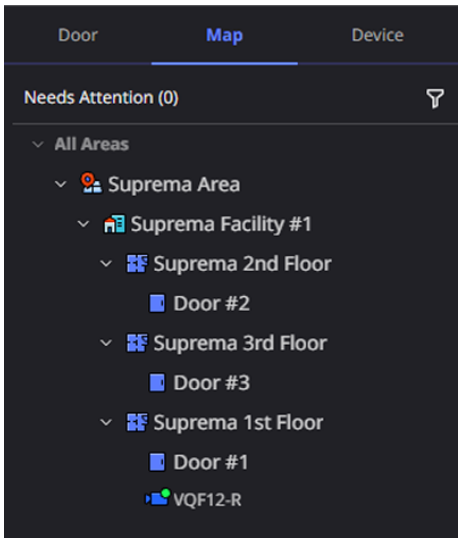
para monitorear y controlar puertas y cámaras. Esta estructura también se puede ver en la barra lateral de la página **Monitoring**.

> **Información**
>
> - Para obtener más información sobre cómo configurar el mapa, consulte Administrar Mapa.
> - El área **Monitoring** permanece deshabilitada si el sistema no tiene cámaras registradas o no tiene componentes del mapa registrados (áreas, instalaciones o pisos).
> - La característica de monitoreo de mapas integrada con GIS está disponible como complemento con una licencia **Essential** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Componentes y opciones

Componentes del árbol del mapa

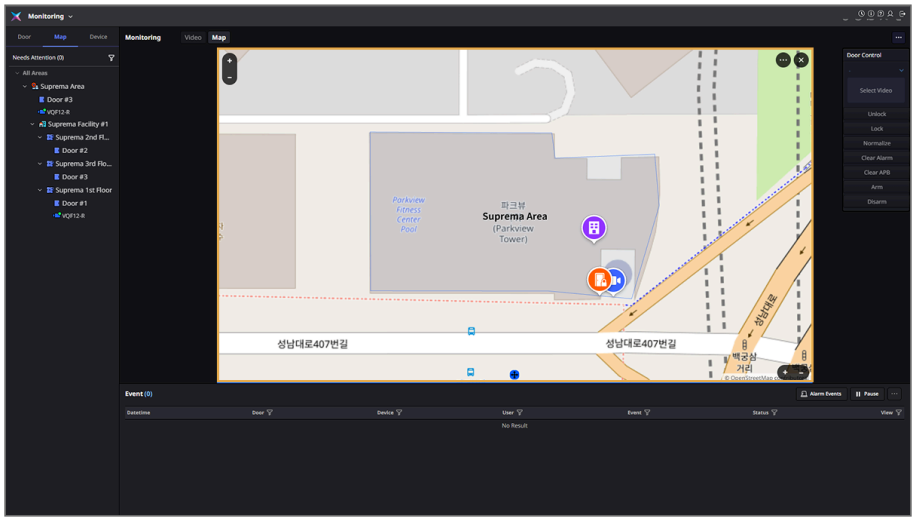
La barra lateral izquierda muestra los componentes del árbol del mapa. Cada ícono de componente en el árbol del mapa indica si es una zona, una instalación, un piso, una puerta o una cámara.



Ícono	Nombre
	Área
	Instalación
	Planta
	Puerta
	Cámara

Componentes del área del mapa

Los componentes que se muestran en el mapa incluyen el área, las instalaciones y las cámaras conectadas a las instalaciones. Puede acceder al piso a través de la instalación. Puede verificar la puerta y la cámara en el piso.



Componente	Descripción
	**Instalación**: Haga clic en una instalación ubicada en el mapa para ingresar al piso configurado correspondiente.
	**Puerta**: Haga clic en una puerta ubicada en el mapa para mostrar un menú emergente y controlar esa puerta. Para obtener más información sobre las funciones disponibles, consulte Control de Puerta.
	**Cámara**: Haga clic en la cámara para reproducir el video de la instalación o piso correspondiente.
	**Error de cámara**: Este mensaje aparece cuando la cámara no está conectada o está apagada.
	**Puerta abierta**: La puerta ubicada en el piso está en estado abierto.
	**Puerta bloqueada**: La puerta ubicada en el piso está bloqueada.

Opciones

Las opciones disponibles en el mapa o la capa son las siguientes.

Función	Descripción
	Puede acercar o alejar haciendo clic en los botones ubicados en la parte superior izquierda y en la inferior derecha del mapa. También puede usar la rueda del ratón para acercar o alejar el mapa.

Función	Descripción
	Puede acercar o alejar haciendo clic en los botones ubicados en la parte inferior derecha del piso.
	Haga clic en el botón para acceder a funciones adicionales.
	Para cerrar el mapa o el piso situado en la ventana de video, haga clic en el botón de la parte superior derecha.
	Al hacer clic y arrastrar mientras mantiene presionado el icono, puede mover el mapa a otra ubicación.

Información

- Puede mover la posición arrastrando el ratón mientras hace clic en el mapa. Puede acercar o alejar usando la rueda del ratón.
- Haga doble clic en el mapa para expandirlo a pantalla completa. Haga doble clic nuevamente o presione la tecla `ESC` para volver al tamaño original.

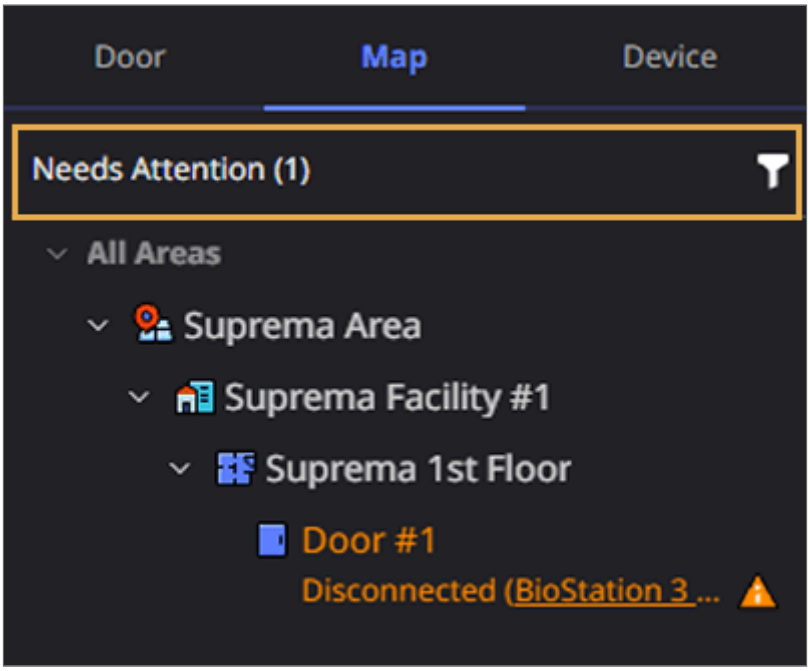
Verifica el estado

En la barra lateral izquierda, verifique el estado de cada puerta y cámara de las instalaciones o pisos. Consulta la información siguiente para el estado de cada icono.

Ícono de estado	Descripción
	Error del servidor de comunicaciones múltiples o conexión perdida.
	Se ha producido una alarma en la puerta. Si se detecta merodeo o intrusión, se mostrará el icono correspondiente.
	La cámara está conectada.
	La cámara está apagada o desconectada.

Ver entradas que requieren atención

Los administradores pueden filtrar la lista para mostrar solo las entradas que requieren acción. En la barra lateral izquierda, haz clic en **Needs Attention**. Verifique el estado de las puertas por área, instalación y piso, y actúe sobre las puertas con problemas.



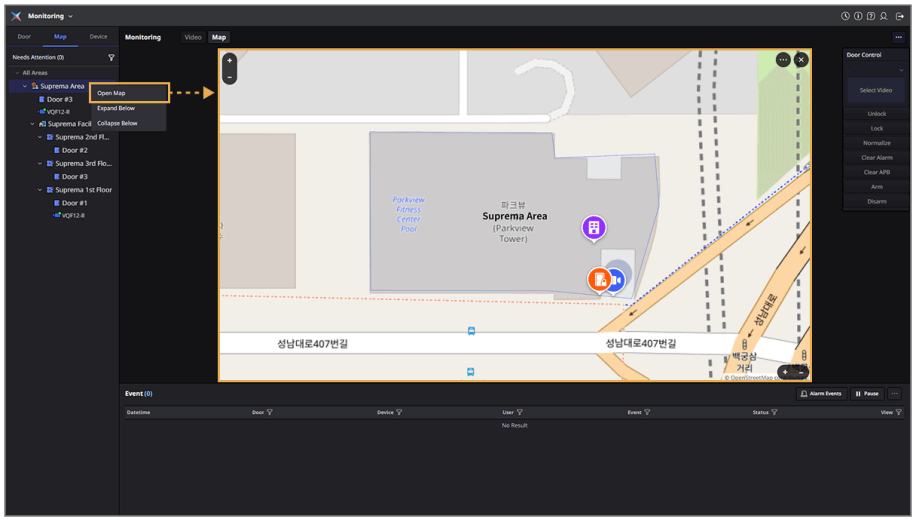
> **Información**
> Para conocer los criterios que determinan las acciones de la puerta, consulte Verifica el estado.

Abrir mapa

Si el área está vinculada al mapa GIS, puede mostrar el mapa en la sección **Monitoring**.

1. En la barra lateral izquierda, seleccione la instalación para verla en el mapa.
2. Haga clic con el botón derecho.
3. Haga clic en **Open Map** en el menú emergente.

El mapa del área seleccionada se mostrará en la ventana de video de la sección **Monitoring**.

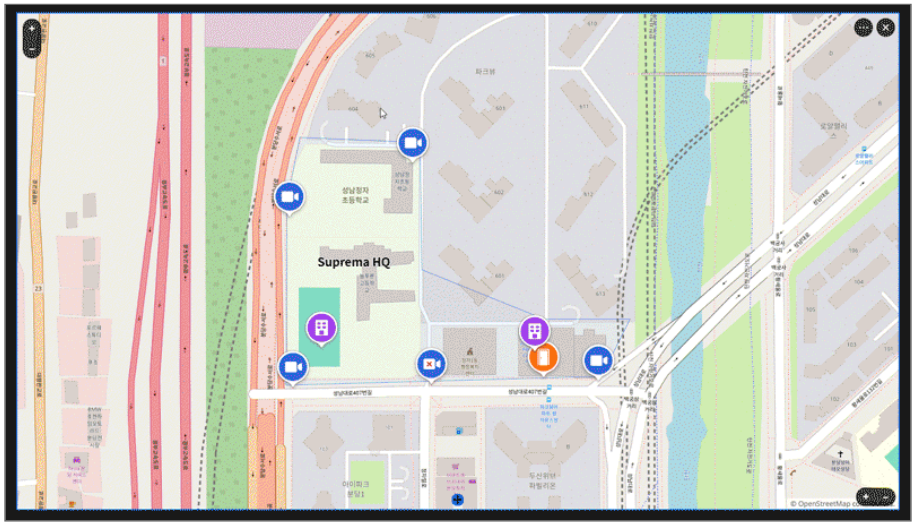


Información

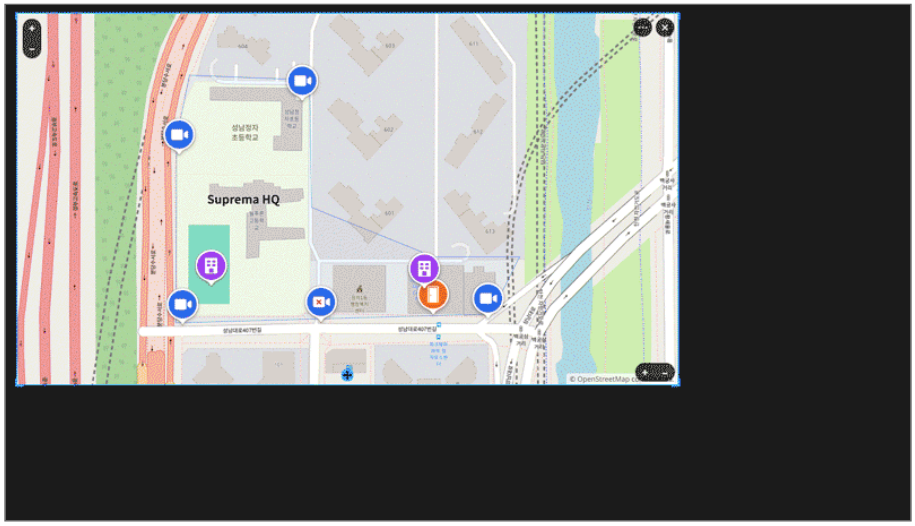
- Haga doble clic en la instalación en la barra lateral izquierda para abrir el mapa donde se encuentra la instalación.
- La imagen es una pantalla de ejemplo. La pantalla real puede diferir.
- Para obtener más información sobre cómo configurar las áreas vinculadas al mapa GIS, consulte Configurar Área.

Ajuste de tamaño y reubicación del mapa

Para ajustar el tamaño del mapa, haga clic en un área vacía del mapa. En cada esquina aparecerán manijas para cambiar el tamaño. Haga clic y arrastre la manija para ajustarla al tamaño deseado.



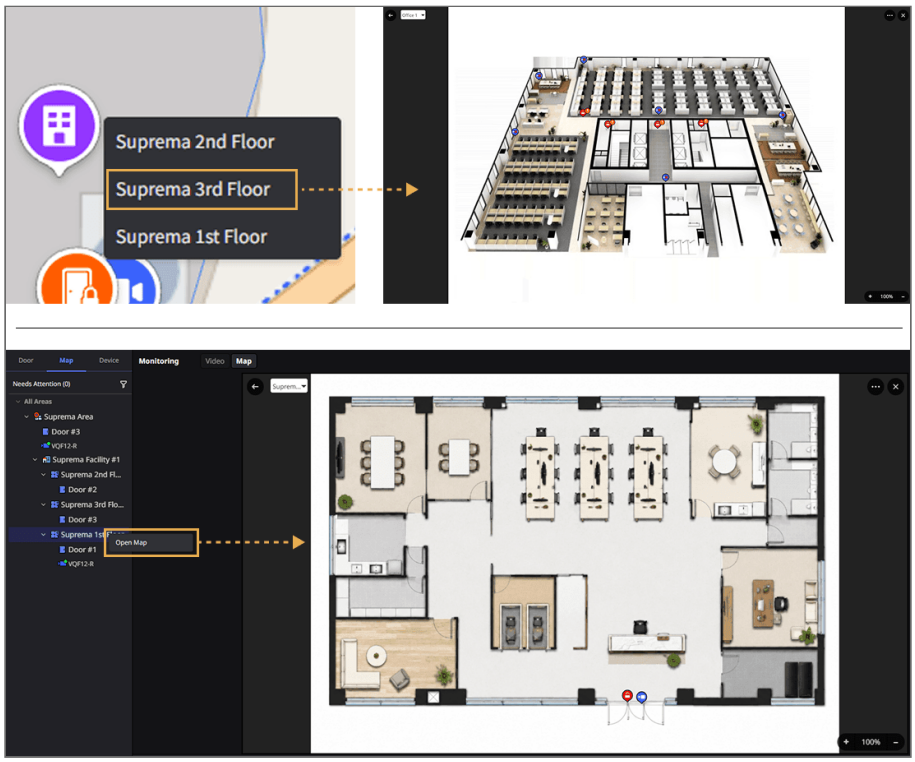
Para mover el mapa a otra ubicación mientras cambia su tamaño, haga clic en el icono sobre el mapa y arrástrelo a la posición deseada.



Entrar al piso

Para ingresar a un piso en el mapa, haga clic en la instalación. Cuando se muestre la lista de pisos accesibles desde el menú emergente, seleccione el piso deseado. Puede verificar los planos, las puertas y las cámaras en el piso seleccionado.

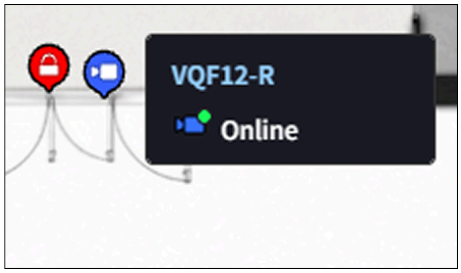
O bien, haga doble clic en el piso en la barra lateral izquierda o haga clic con el botón derecho y seleccione **Open Map** en el menú emergente.



Componente	Descripción
	**Puerta abierta**: La puerta ubicada en el piso está en estado abierto.
	**Puerta bloqueada**: La puerta ubicada en el piso está bloqueada.
	**Cámara**: Haga clic en la cámara para reproducir el video de la instalación o piso correspondiente.

- Pase el cursor sobre una puerta o cámara para verificar su estado actual.

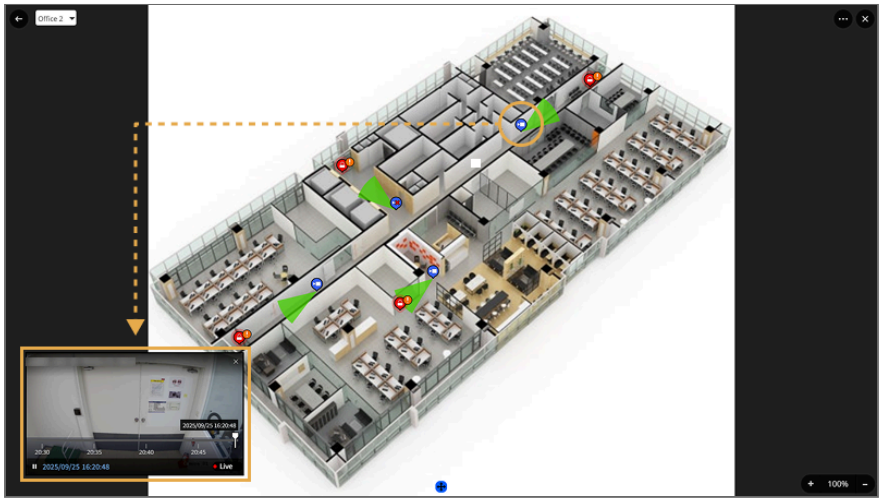




- Al hacer clic en la puerta se mostrará un menú emergente que le permite controlar esa puerta. Para obtener más información sobre las funciones disponibles, consulte Control de Puerta.



- Al hacer doble clic en la cámara, se reproduce la transmisión en vivo.



Información

- Para navegar al mapa que muestra la instalación, haga clic en ← en la parte superior izquierda.
- Para obtener más información sobre cómo configurar puertas y cámaras en un piso (Floor), consulte Configurar Pisos.
- Para obtener más información sobre los controles de vídeo y las herramientas que aparecen en él, consulte Supervisar Video.
- La imagen es una pantalla de ejemplo. La pantalla real puede diferir.

Moverse a otro piso

Para moverse a otro piso, haga clic en la opción de selección en la esquina superior izquierda del mapa y seleccione el piso al que desea ir.

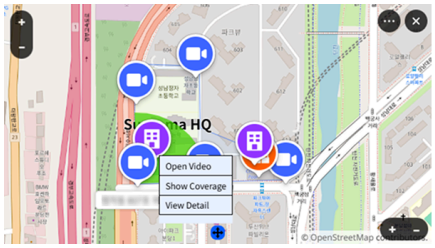


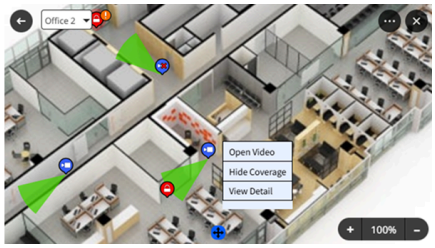
Información

- Para navegar al mapa que muestra la instalación, haga clic en ← en la parte superior izquierda.
- La opción de selección de piso en la parte superior izquierda del mapa muestra solo los pisos configurados para la instalación. Si el piso no está configurado en la instalación, no aparecerá en la lista. Para obtener más información sobre cómo configurar los pisos de una instalación, consulte Configurar Instalación.

Controlar la cámara

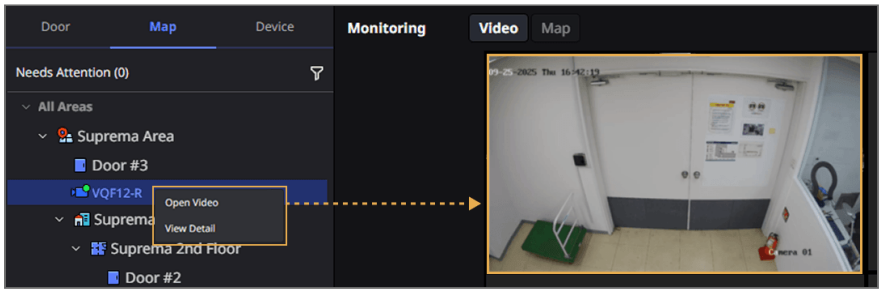
- Para controlar la cámara en el mapa o piso, haga clic en el ícono de la cámara. Seleccione la función deseada en el menú emergente.





  - **Open Video**: Puede ver el video de la cámara en tiempo real.
  - **Show Coverage** / **Hide Coverage**: Puede mostrar u ocultar el rango de cobertura de la cámara.
  - **View Detail**: Puede ver información detallada sobre la cámara. Muestra el nombre, grupo, ID, dirección IP, etc., de la cámara en el panel derecho.

- Para colocar y reproducir la transmisión de la cámara en el mosaico de video, haga doble clic en la cámara en la lista **Map** en la barra lateral izquierda de la pantalla. O haga clic derecho y seleccione **Open Video** en el menú emergente.



Para ver información detallada como el nombre y el grupo de la cámara, haga clic en **View Detail** en el menú emergente.

Información

- Los mosaicos de video se añaden en orden desde la parte superior izquierda de la pantalla. Si no hay espacio para añadir más, aparece un mensaje de error.
- Para obtener más información sobre los controles de vídeo y las herramientas que aparecen en él, consulte Supervisar Video.
- Si una cámara no se muestra en el mapa, compruebe los permisos del grupo de cámaras. Si el administrador de un permiso personalizado no ha configurado los permisos del grupo de cámaras, la cámara podría no ser visible. Para obtener más información sobre cómo configurar los permisos de los grupos de cámaras, consulte Configurar la Cámara.

Monitorear Dispositivo

Este documento proporciona orientación sobre cómo usar las funciones de supervisión de dispositivos y cámaras. Puedes verificar el estado de dispositivos y cámaras, ver información detallada y reproducir video de la cámara en tiempo real, entre otras funciones. Además, revisa los eventos recientes para gestionar de manera eficiente el estado de dispositivos y cámaras.

Para acceder a la página **Monitoring**, haz clic en **Monitoring** en **Launcher** o selecciona **Monitoring** en el menú de la parte superior izquierda de la pantalla.

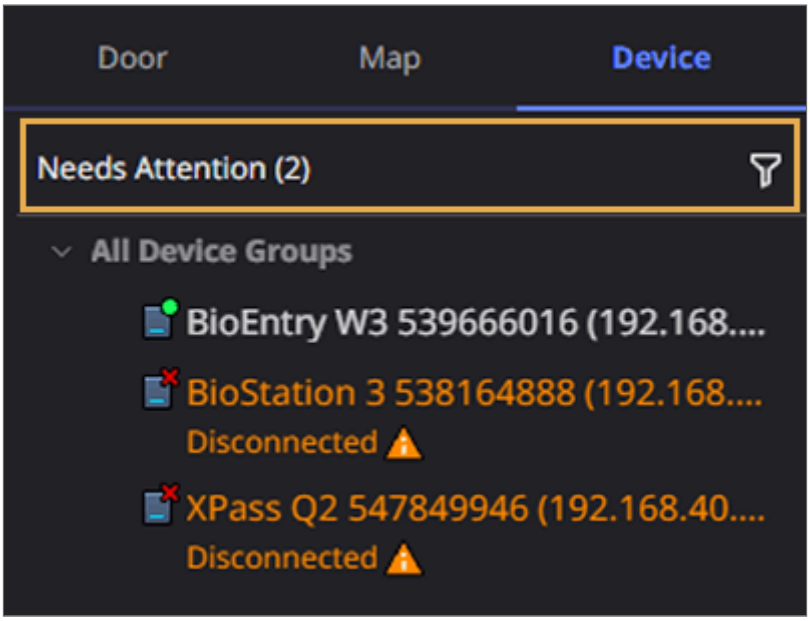
Verificar estado de dispositivos y cámaras

Haz clic en la pestaña **Device** en la barra lateral izquierda. Puedes verificar el estado de todos los dispositivos y cámaras. Consulta lo siguiente para conocer el estado de los dispositivos y cámaras.

Ícono de estado	Descripción
	El dispositivo está conectado correctamente.
	El dispositivo está apagado o desconectado.
	La cámara está conectada.
	La cámara está apagada o desconectada.

Ver dispositivos que requieren atención

Los administradores pueden ver solo los dispositivos que requieren acción en una lista. En la barra lateral izquierda, haz clic en **Needs Attention**. Revise el estado del dispositivo y tome medidas en dispositivos con problemas.



Criterios para dispositivos que requieren acción

En el árbol de dispositivos, el sistema marca los dispositivos anómalos como dispositivos que requieren acción.

Tipo de estado anormal	Indicador de estado	Descripción
Desconectado	**Disconnected**	El dispositivo está desconectado de la red
Error de sincronización	**Sync Error**	Conectado, pero los datos no están sincronizados
Error de Multi Communications Server	**Communications Server Error**	El Multi Communications Server del dispositivo presenta un error
Bloquear dispositivo	**Device Locked**	El dispositivo está bloqueado debido a las condiciones y acciones del trabajo
Bloqueo por fallo de autenticación	**Auth Failure Lockout**	El dispositivo se bloquea cuando la autenticación falla más del número especificado de veces

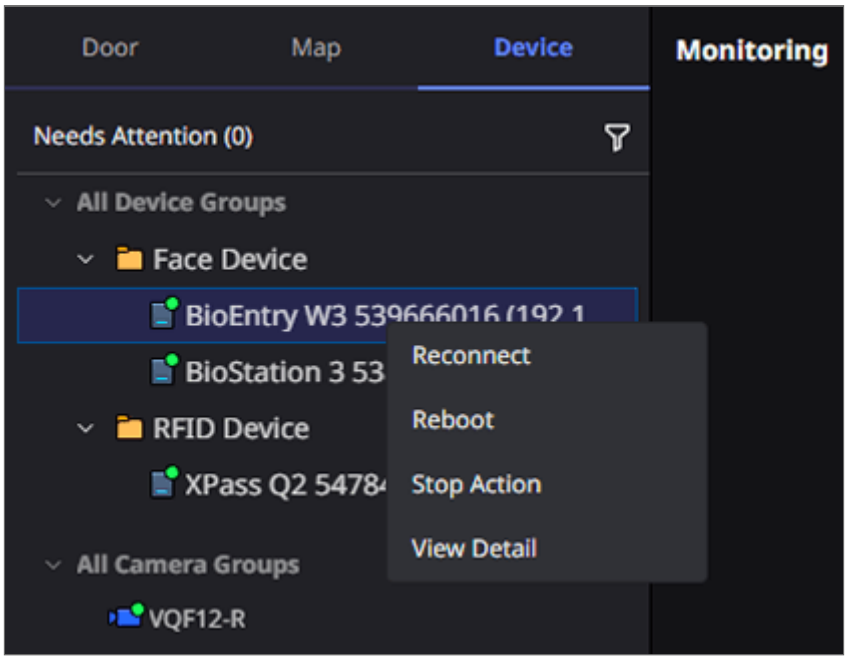
Información

- La condición **Device Locked** depende de las condiciones y acciones del trabajo establecidas en Configuración de Activadores y Acciones. Para obtener información sobre cómo revisar y liberar este estado, consulte Desbloquear el dispositivo.
- Configure la condición **Auth Failure Lockout** en los ajustes del dispositivo. Para obtener detalles, consulte Configuración de Autenticación. Para obtener información sobre cómo revisar y liberar este estado, consulte Borrar el bloqueo por fallas de autenticación.

Control del dispositivo

Selecciona el dispositivo deseado de la lista en la barra lateral izquierda y haz clic derecho. Seleccione la función deseada en

el menú emergente.



Las características de control que aparecen pueden variar según el tipo de dispositivo.

Tipo de dispositivo	Característica de control
Dispositivo maestro, un dispositivo principal que se conecta directamente al servidor sin esclavos	**Stop Action**, **Reboot**, **Unlock Device**, **Release Auth Failure Lockout**, **Reconnect**(solo cuando el servidor se conecta al dispositivo)
Dispositivo esclavo	**Stop Action**, **Reboot**, **Unlock Device**, **Release Auth Failure Lockout**
Dispositivo de comunicación OSDP	**Unlock Device**, **Reconnect** (depende del método de conexión)
Dispositivo Wiegand	**Unlock Device**
Módulos de expansión (Secure I/O 2, DM-20, OM-120, IM-120)	**Stop Action**
Dispositivos que usan conexiones de dispositivo a servidor	**Stop Action**, **Reboot**, **Unlock Device**, **Release Auth Failure Lockout**
Módulo de antena inalámbrica	Ninguno

Reconectar dispositivo

Independientemente del estado de conexión del dispositivo, haga clic en **Reconnect** en el menú emergente. Úselo para volver a conectar dispositivos desconectados o reenviar ajustes y borrar estados anómalos en dispositivos conectados.

Cuando el dispositivo se reconecta, el ícono de estado cambia al estado normal ( ).

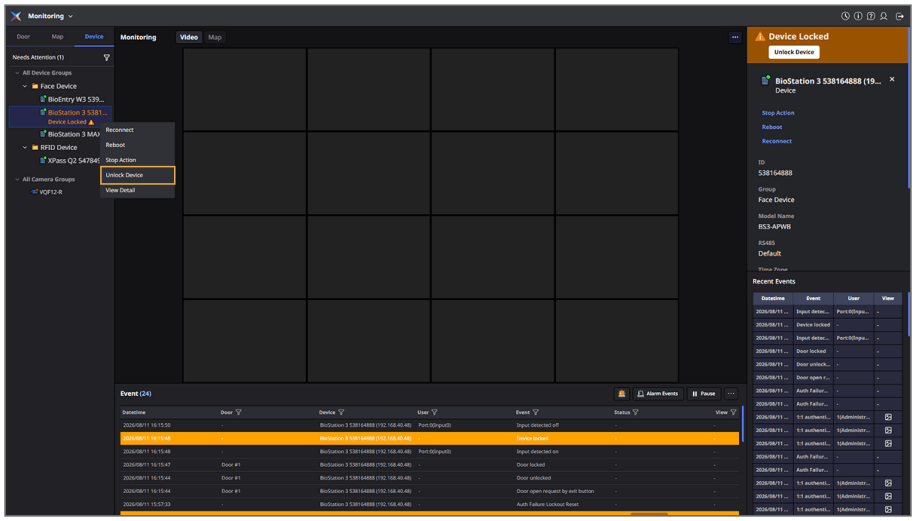
> **Información**
>
> La característica **Reconnect** no es compatible con dispositivos conectados mediante la opción **Device ▸ Server Connection**. Para obtener más información sobre el registro de dispositivos, consulte Registrar dispositivo.

Reiniciar dispositivo

Para reiniciar el dispositivo, haz clic en **Reboot** en el menú emergente. Cuando aparezca la ventana de mensaje de advertencia, haga clic en **Ok**.

Desbloquear el dispositivo

Cuando el dispositivo se bloquea según condiciones definidas por el administrador, **Device Locked** aparece debajo del nombre del dispositivo en la barra lateral izquierda. Al seleccionar el dispositivo, el panel de vista previa derecho muestra el mismo banner en la parte superior.



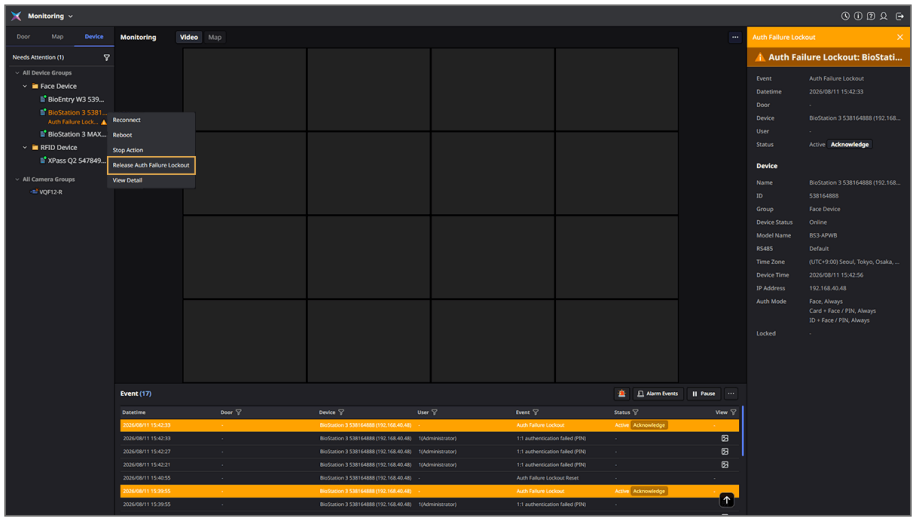
- El menú emergente muestra **Unlock Device** solo cuando el dispositivo está bloqueado. Seleccione el dispositivo bloqueado y, luego, haga clic en **Unlock Device** en el menú emergente.
- Seleccione el dispositivo bloqueado. En el banner en la parte superior del panel de vista previa derecho, haga clic en **Unlock Device**.

> **Información**
>
> Solo los usuarios con privilegios de **Administrator** o **Monitoring Operator** ven **Unlock Device**.

Borrar el bloqueo por fallas de autenticación

Si la autenticación falla la cantidad de veces establecida en **Auth Failure Lockout**, el dispositivo cambia al estado bloqueado. Cuando el dispositivo está en bloqueo por fallas de autenticación, **Auth Failure Lockout** aparece debajo del nombre del dispositivo en la barra lateral izquierda. Al seleccionar el dispositivo, el panel de vista previa derecho muestra el mismo banner en la parte superior. El banner muestra la hora del evento y la información del dispositivo.

El menú emergente muestra **Release Auth Failure Lockout** solo cuando el dispositivo está en bloqueo por fallas de autenticación. Seleccione el dispositivo bloqueado y, luego, haga clic en **Release Auth Failure Lockout** en el menú emergente.



Información

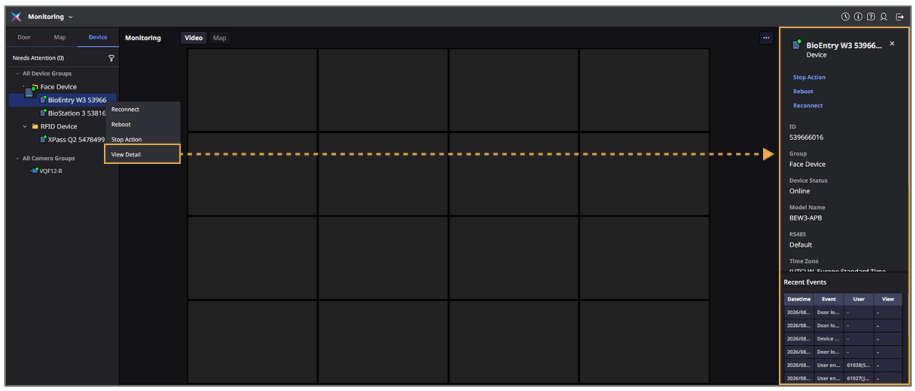
- Solo los usuarios con privilegios de **Administrator** o **Monitoring Operator** ven el menú **Release Auth Failure Lockout**.
- Después de que transcurra el tiempo de bloqueo establecido (**1st Lockout Duration**/**2nd Lockout Duration**), el dispositivo se desbloquea automáticamente. El dispositivo elimina el bloqueo sin acciones adicionales. Para más información sobre condiciones y ajustes del tiempo de bloqueo, consulte Configuración de Autenticación.

Detener acción

Para detener todas las acciones basadas en alarmas y activadores del dispositivo, haga clic en **Stop Action** en el menú contextual. Aparecerá un mensaje de éxito en la parte superior de la pantalla indicando que la acción se detuvo.

Vista detallada del dispositivo

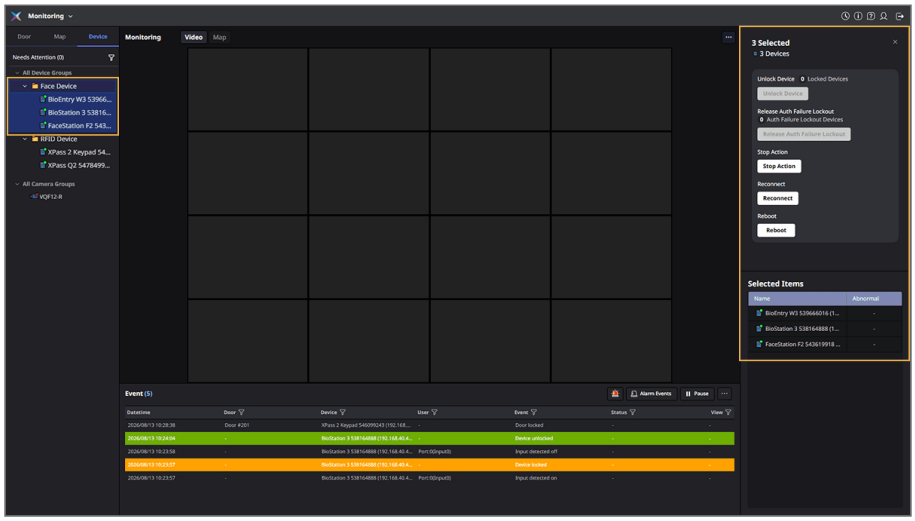
Para ver información detallada del dispositivo, haz clic en **View Detail** en el menú emergente. O haz doble clic en el dispositivo. La información detallada del dispositivo aparecerá en el lado derecho de la pantalla.



- **Control del dispositivo**: Use los controles para detener tareas, reiniciar o reconectar.
- **Detalles del dispositivo**: Verifique el ID del dispositivo, el grupo, el nombre del modelo, el tiempo de actividad y la dirección IP.
- **Recent Events**: Vea la lista de eventos recientes en el dispositivo seleccionado.

Controle varios dispositivos a la vez

Esta sección describe cómo seleccionar varios dispositivos y ejecutar comandos como reconectar, reiniciar o desbloquear. Seleccione dos o más dispositivos en la pestaña **Device** de la barra lateral izquierda. El panel de control por lotes aparece a la derecha.



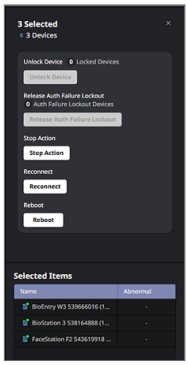
> **Información**
>
> El control masivo no incluye cámaras. Para el control de la cámara, consulte Controlar la cámara.

Seleccione varios dispositivos

Use los siguientes métodos para seleccionar dispositivos en la pestaña **Device** de la barra lateral izquierda.

- `Ctrl` + **clic**: Agregue o quite de la lista de selección el dispositivo en el que hizo clic. Esto mantiene el resto de la selección.
- `Shift` + **clic**: Seleccione un rango desde el último dispositivo en el que hizo clic hasta el dispositivo en el que hizo clic. La selección de rango excluye los grupos de dispositivos.
- **Haga clic en un grupo (** **)**: Haga clic en el nombre de un grupo para agregar a la lista de selección todos los dispositivos del grupo. Mantenga seleccionados los dispositivos ya seleccionados.

> **Información**
>
> - Si selecciona solo un grupo vacío sin dispositivos, el panel derecho se cierra.
> - La aplicación abre el panel de detalles del dispositivo al seleccionar un dispositivo. La aplicación cambia al panel de control por lotes al seleccionar dos o más dispositivos.



Diseño del panel de control por lotes

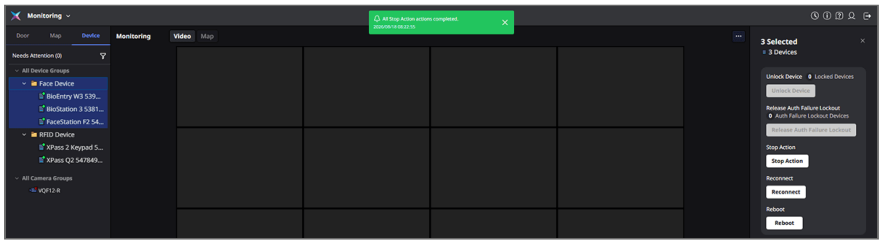
- **Unlock Device**, **Release Auth Failure Lockout**: Estos botones se activan cuando los dispositivos seleccionados están bloqueados o en bloqueo por fallas de autenticación. La cantidad de dispositivos objetivo aparece junto a cada botón.
- **Stop Action**, **Reconnect**, **Reboot**: Estos botones se activan si los dispositivos seleccionados admiten este control. No muestran la cantidad de dispositivos objetivo.
- **Control del dispositivo**: Use estos botones: **Unlock Device**, **Release Auth Failure Lockout**, **Stop Action**, **Reconnect** y **Reboot**.
- **Divisor**: Arrastre el divisor entre el control del dispositivo y **Selected Items** hacia arriba o abajo para ajustar la altura de cada área.
- **Selected Items**: Verifique el estado de conexión, el nombre y el estado anormal de los dispositivos seleccionados. Consulte Criterios para dispositivos que requieren acción para ver los tipos de estado anormal.

Haga clic en cada botón para abrir el cuadro de diálogo de confirmación. En el cuadro de diálogo de confirmación, haz clic en **Cancel** para cerrar sin ejecutar la característica seleccionada. Haz clic en el botón de la característica seleccionada para ejecutarla en todos los dispositivos seleccionados.

> **Información**
>
> Si la selección incluye distintos tipos de dispositivos, el sistema muestra los controles compatibles combinados. El sistema no muestra botones para controles que ninguno de los dispositivos seleccionados admite. Si no hay controles compatibles, el sistema muestra solo el texto de orientación y la tabla de la lista de dispositivos seleccionados.

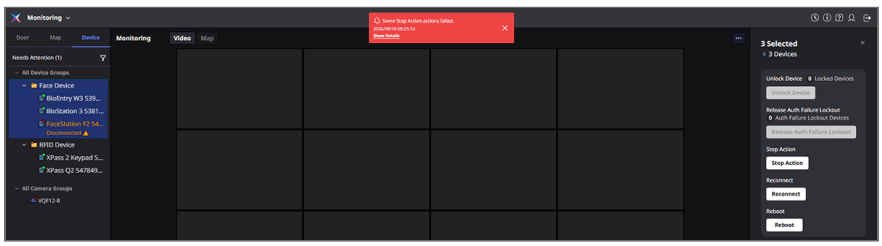
Revisar resultados de ejecución

- Si la ejecución tiene éxito en todos los dispositivos seleccionados, el sistema muestra solo un mensaje de éxito.



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

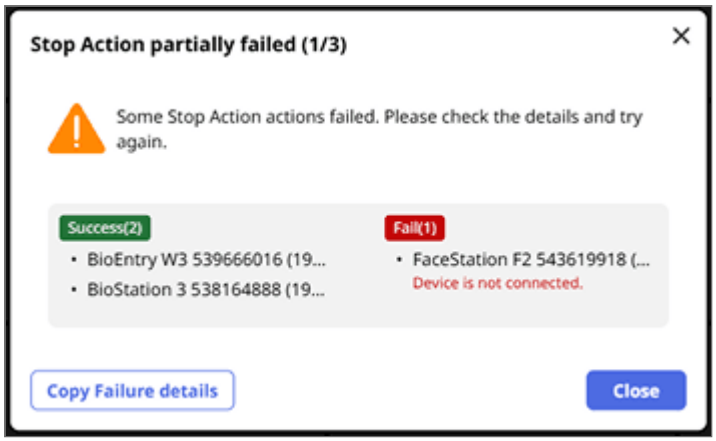
- Si falla algún dispositivo, el sistema muestra un mensaje de fallo junto con el botón **Show Details**.



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

Haga clic en **Show Details** para ver los resultados agrupados en **Success**, **Failure** y **Skipped**. Haga clic en **Copy Failure**

details para copiar al portapapeles los nombres y los motivos de las entradas fallidas.



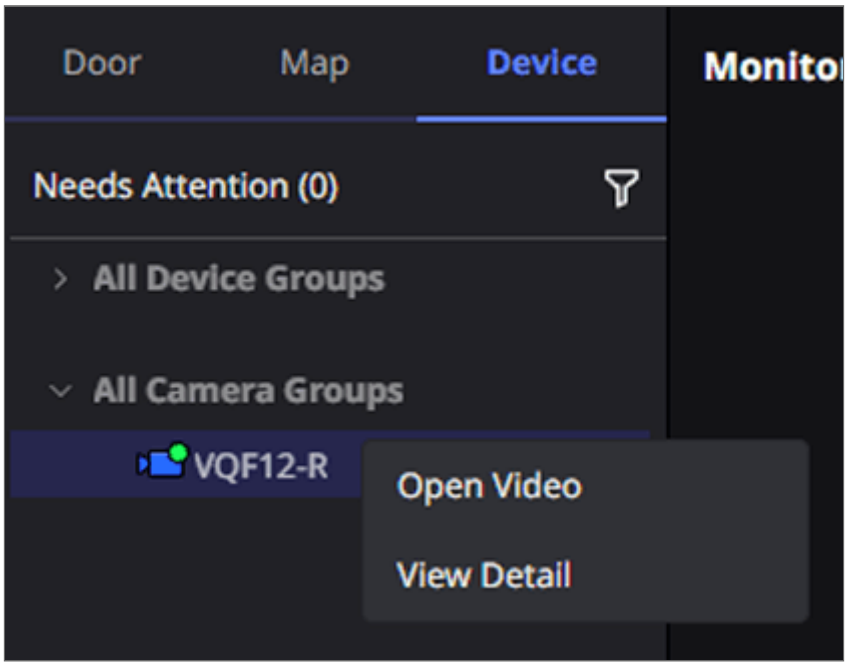
La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

Información

- El botón **Reconnect** es una excepción. Después de que el sistema acepte la solicitud, solo muestra un mensaje de éxito. No proporciona el estado de fallo ni una ventana de resultados detallados. Revisa el árbol de estado para confirmar si la conexión se completó correctamente.
- El sistema ejecuta **Unlock Device** y **Release Auth Failure Lockout** por separado y muestra ventanas de resultados independientes.

Controlar la cámara

Selecciona la cámara deseada de la lista en la barra lateral izquierda y haz clic derecho. Seleccione la función deseada en el menú emergente.



Reproducir video de la cámara

Para colocar el video de la cámara en el mosaico de video y supervisarlo en tiempo real, haz clic en **Open Video** en el menú emergente.

También puedes añadir video de la cámara a los mosaicos de video de las siguientes maneras:

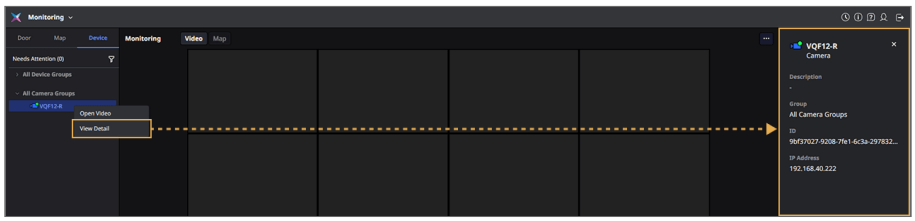
- Haz doble clic en la cámara para reproducir su video desde la barra lateral izquierda.
- También puedes añadir video arrastrando y soltando la cámara en el área de mosaicos de video.

Información

- Los mosaicos de video se añaden en orden desde la parte superior izquierda de la pantalla. Si no hay espacio para añadir más, aparece un mensaje de error.
- Para obtener más información sobre los controles de video y las herramientas que se muestran en el video, consulte Supervisar Video.
- Si una cámara no aparece en la lista **All Camera Groups**, revisa los permisos del grupo de cámaras. Si el administrador de un permiso personalizado no ha configurado los permisos del grupo de cámaras, la cámara podría no ser visible. Para obtener más información sobre cómo configurar los permisos de los grupos de cámaras, consulte Configurar la Cámara.

Vista detallada de la cámara

Haz clic en **View Detail** en el menú emergente para ver los detalles de la cámara. Puedes verificar el grupo, la descripción, el ID y la dirección IP de la cámara.

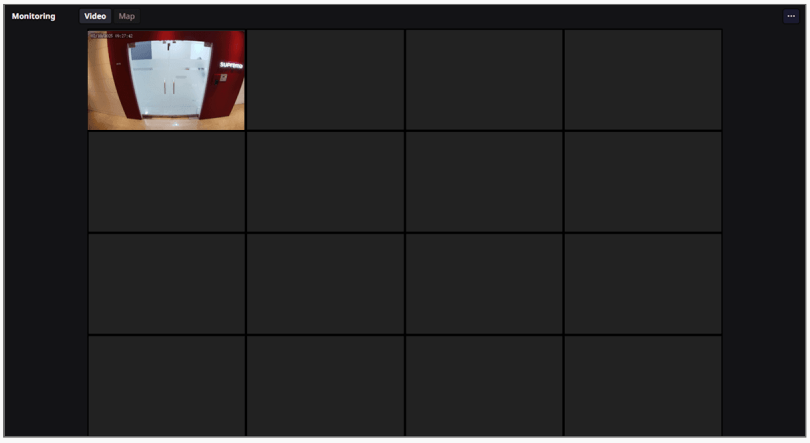


Supervisar Video

Supervise y controle en tiempo real los videos de cámaras vinculadas a puertas, áreas y dispositivos mediante la función de monitoreo de video. Este documento ofrece orientación sobre cómo usar los mosaicos de video para agregar videos de cámaras, cambiar su tamaño, cambiar su posición, verlos en pantalla completa y realizar varias tareas. Además, admite una respuesta rápida a situaciones de seguridad mediante funciones de gestión como comprobar y borrar estados de alarma.

Información

- **Video Tile** es el área en el centro de la pantalla donde aparece el video de la cámara. Es un componente de la interfaz que permite colocar y supervisar simultáneamente varios videos de cámaras. Los usuarios pueden cambiar el tamaño o la posición del video en el video tile y cerrarlo o pasarlo a pantalla completa según sea necesario.



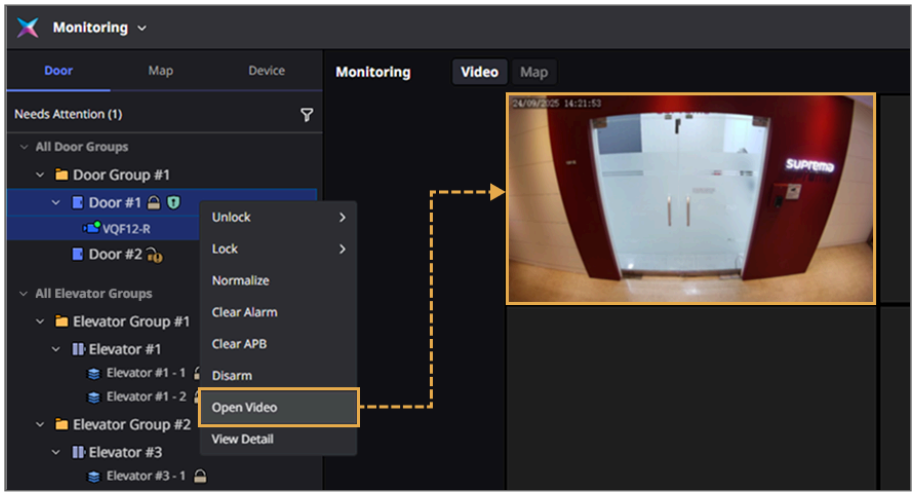
- El área **Monitoring** permanece deshabilitada si el sistema no tiene cámaras registradas o no tiene componentes del mapa registrados (áreas, instalaciones o pisos).
- Para obtener más información sobre la integración con el VMS y cómo agregar y administrar cámaras, consulte Configuración de Video.
- Si se produce un error de carga al reproducir grabaciones desde el VMS, instale el certificado en el servidor VMS e instale el certificado del servidor VMS en la PC cliente. Para obtener más información, consulta lo siguiente.
  - Instalar el certificado en el servidor VMS
  - Instalar el certificado del servidor VMS en la PC cliente
- Si las cámaras asociadas a esta área no son visibles, verifique los permisos del grupo de cámaras. Si el administrador de un permiso personalizado no ha configurado los permisos del grupo de cámaras, la cámara podría no ser visible. Para obtener más información sobre cómo configurar los permisos de los grupos de cámaras, consulte Configurar la Cámara.
- El monitoreo de video está disponible como una opción adicional con la licencia **Essential** (Essential) o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Reproducir video

Agregue videos de cámaras al video tile para su monitoreo. El video tile se encuentra en el centro de la pantalla y permite supervisar simultáneamente varios videos de cámaras.

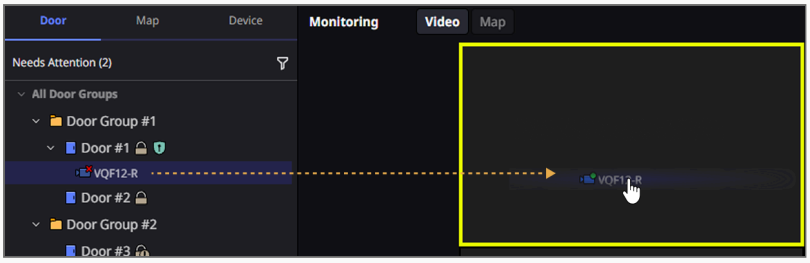
1. Seleccione la cámara que desea ver desde las pestañas **Door** o **Map**, **Device** en la barra lateral izquierda.
2. Haga clic con el botón derecho.
3. Haz clic en **Open Video** en el menú emergente.

El video de la cámara seleccionada se puede colocar en el video tile ubicado en el centro de la pantalla.



Información

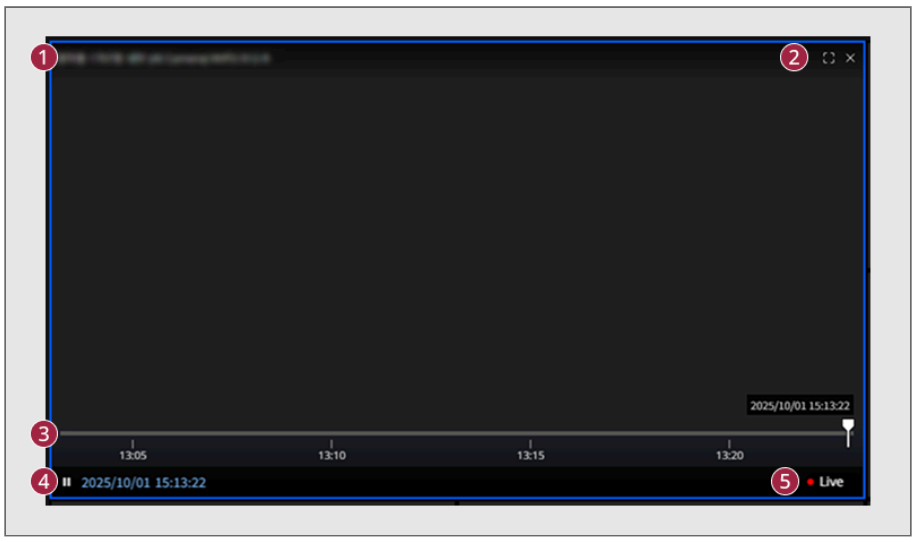
- Seleccione cámaras de la lista en la barra lateral y arrástrelas al área del video tile.



- Los mosaicos de video se añaden en orden desde la parte superior izquierda de la pantalla. Si no hay espacio para añadir más, aparece un mensaje de error.

Controlar video

De forma predeterminada, los videos colocados en el video tile se reproducen en tiempo real. Utilice las herramientas de reproducción para ajustar la reproducción del video o ver grabaciones anteriores.



1. Este es el nombre de la cámara.
2. Este botón permite reproducir el video en pantalla completa (⛶) o excluirlo del video tile (✕).
3.

Este control deslizante permite ajustar la posición de reproducción del video. Al arrastrar el control deslizante, se pueden ver videos anteriores.

4. Para reproducir o pausar el video, haga clic en el botón ▶ o ⏸.

5. Este icono indica que el video actual se reproduce en tiempo real. Para volver al video en vivo mientras reproduce video anterior, haga clic en este icono.

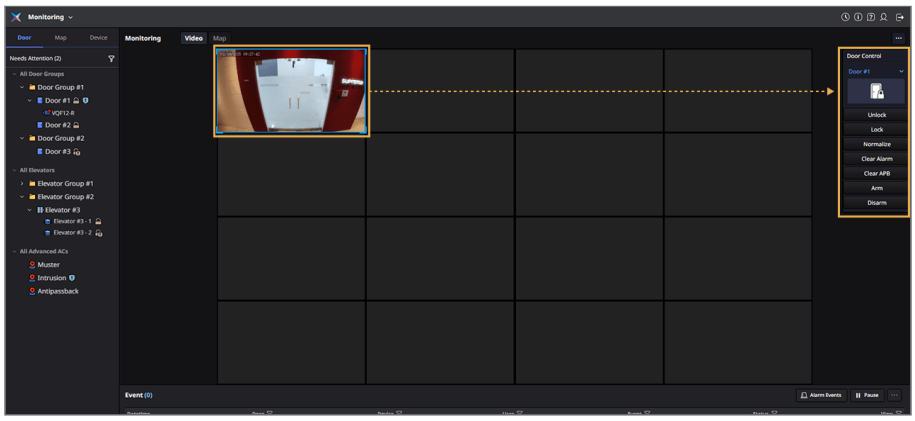
Retención de la reproducción de video grabado y aviso de falla

Salga de la pestaña **Video** (por ejemplo, vaya a otra página, cambie a la pestaña **Map** o actualice). Cuando vuelva a la pestaña **Video**, mantiene el estado de reproducción del video grabado. Cada mosaico de video vuelve a cargar el video en el orden en que aparece.

> **Información**
>
> La falla de reproducción puede aparecer en cada mosaico en momentos distintos porque los tiempos de respuesta varían. Sin embargo, los mosaicos que no se reproducen suelen aparecer al final del orden.

Herramienta de control de puerta

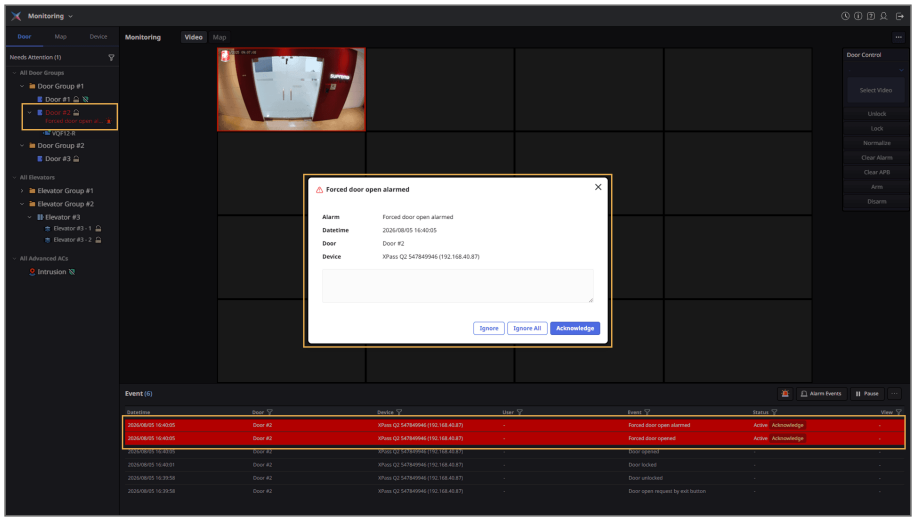
Después de agregar un video, use la herramienta **Door Control** para realizar acciones adicionales. Al seleccionar la cámara vinculada a la puerta desde el video tile se activa la herramienta **Door Control** que permite controlar la puerta. Use funciones como abrir o bloquear la puerta, desbloquear y desactivar la alarma.



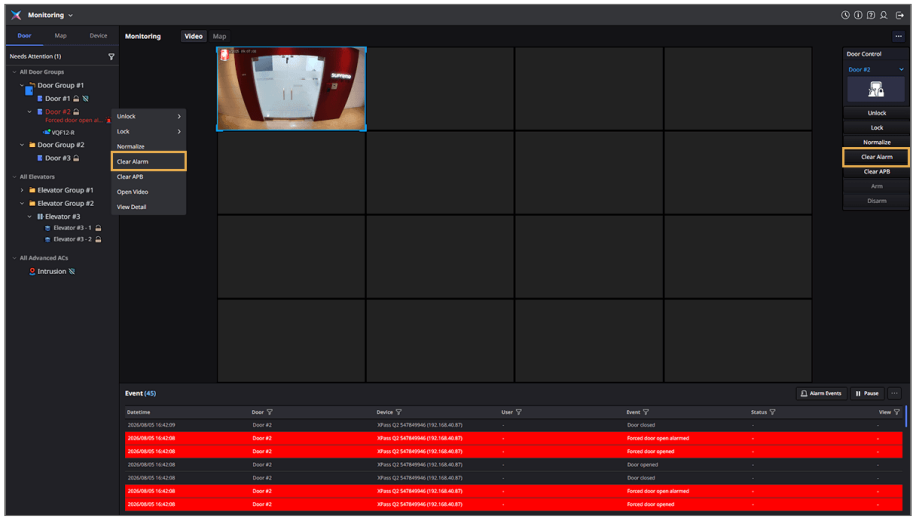
> **Información**
>
> - La herramienta **Door Control** se puede usar cuando no hay nada abierto en el panel derecho. Si la información detallada está abierta en el panel derecho, ciérrela para usar la herramienta.
> - Esta función requiere que una cámara esté vinculada a la puerta. Para obtener más información sobre cómo vincular cámaras con puertas, consulte Configurar Reglas de Video.
> - Para obtener más información sobre las funciones disponibles en la herramienta **Door Control**, consulte Control de Puerta.

Comprobar alarma de video

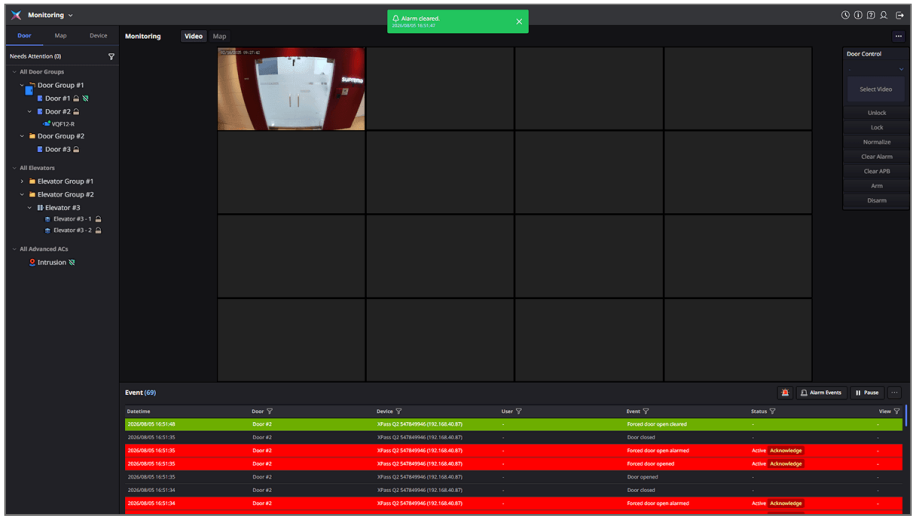
Cuando se activa un estado de alarma para una de las puertas vinculadas a la cámara, aparece un icono de alarma sobre el video. Para que el icono de alarma desaparezca, deben borrarse todas las alarmas vinculadas a la puerta.



Para borrar la alarma de la puerta, haga clic con el botón derecho en la puerta de la lista y haga clic en **Clear Alarm** en el menú emergente. Como alternativa, haga clic en la herramienta **Door Control** y luego en **Clear Alarm**.



Un mensaje de éxito o error aparecerá en la parte superior de la pantalla.

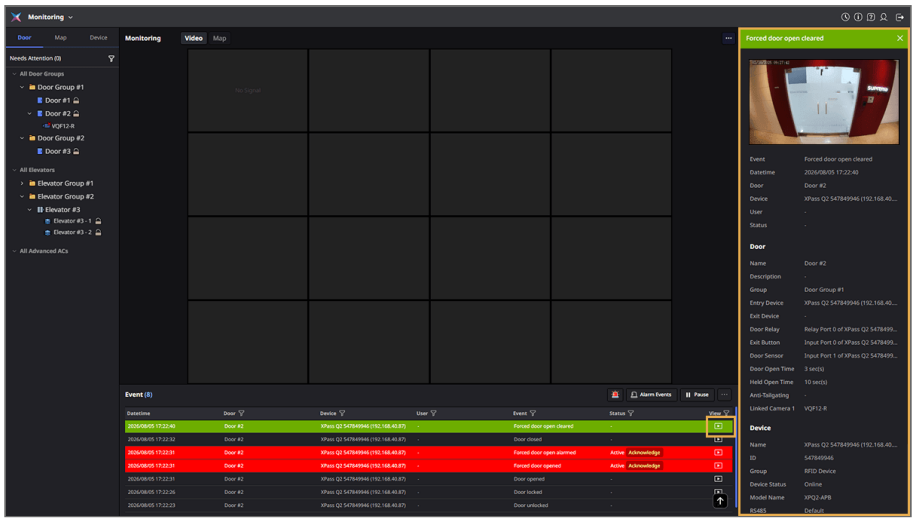


Información

Para obtener más información sobre la sección **Event** en la parte inferior de la pantalla, consulte Supervisar Evento.

Comprobar registro de video

Cuando se produce un evento específico en una puerta establecido por una regla, el elemento de evento correspondiente en la lista de la sección **Event** mostrará un icono de registro de video ( ). Al hacer clic en el elemento de evento con el icono de registro de video, se muestra información detallada en el lado derecho de la pantalla, lo que le permite ver el video del momento en que ocurrió el evento específico. Compruebe el video del momento en que ocurrió un evento específico.



Información

- El icono de registro de video se muestra solo cuando una cámara está vinculada a la puerta. Para obtener más información sobre cómo vincular cámaras con puertas, consulte Configurar Reglas de Video.
- La primera cámara conectada tiene prioridad de reproducción según las reglas de configuración de eventos. Para ver el video en una pantalla más grande, haga doble clic en él.
- Vincule hasta 4 cámaras a una puerta y haga clic en el botón de cámara en la parte inferior del video para reproducir el video de la cámara deseada. Si solo hay una cámara vinculada, el botón de cámara no se mostrará.
- Para obtener más información sobre la sección **Event** en la parte inferior de la pantalla, consulte Supervisar Evento.

Configurar diseño de mosaicos de video

Cambie el tamaño o la posición del video colocado en el video tile según sea necesario. Ajuste el tamaño y la posición del video según su importancia para el monitoreo.

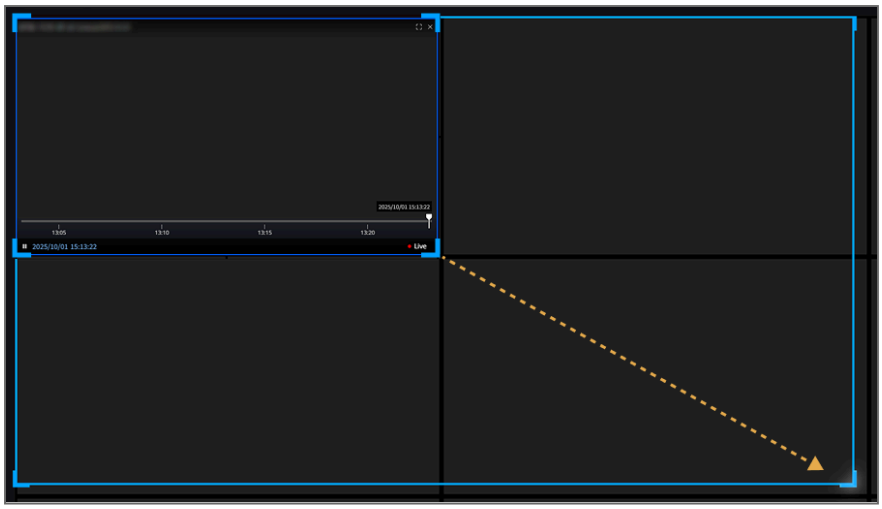
Cambiar tamaño del video

1. Haga clic en el video cuyo tamaño desea cambiar para activar el marco del video seleccionado.

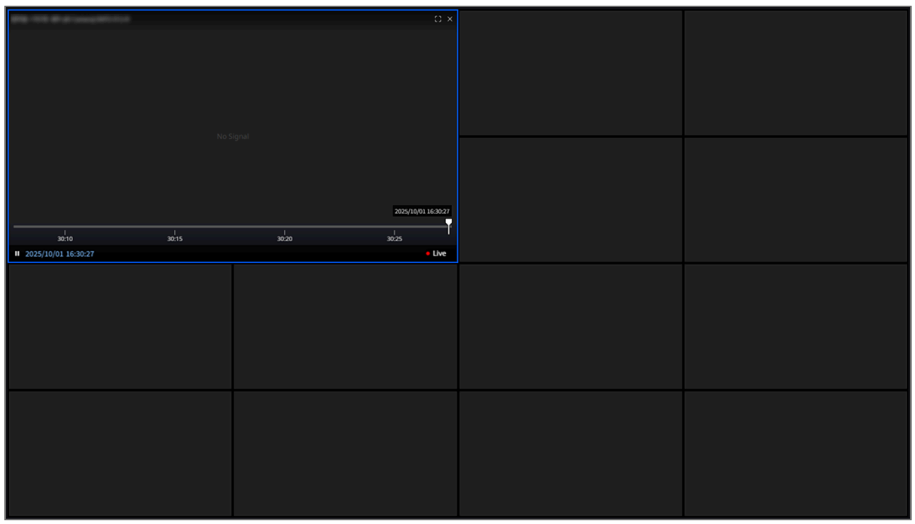


2. Mueva el cursor del mouse sobre los bordes del marco para que adopte la forma de redimensionamiento.

3. Haga clic en una esquina y arrastre hasta el tamaño deseado.

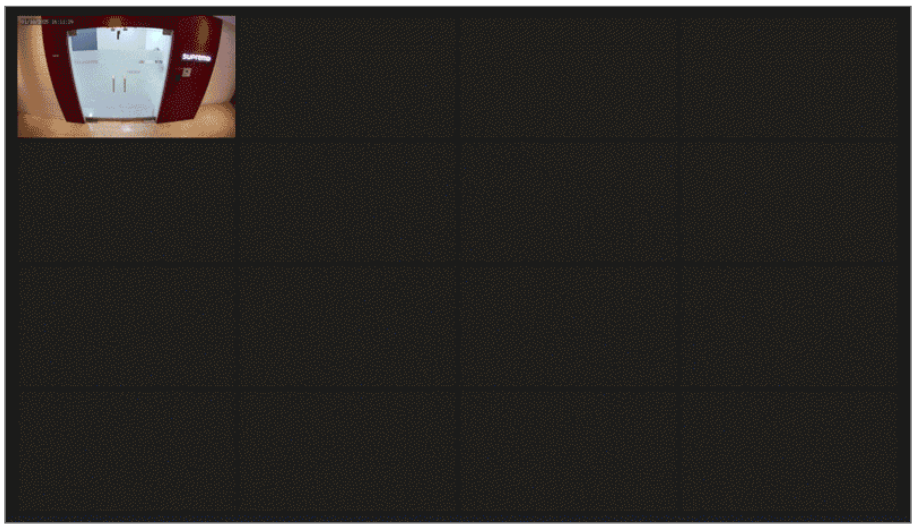


El tamaño del video puede ajustarse proporcionalmente al tamaño del mosaico colocado. De manera inversa, también es posible reducir el tamaño del video.



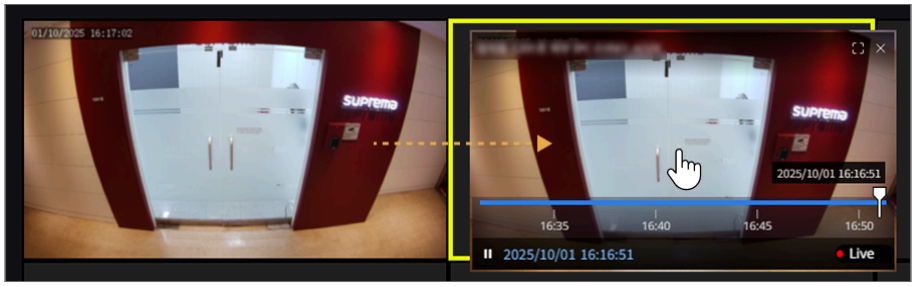
Ampliar tamaño del video

Para ampliar el video al tamaño completo del video tile, haga doble clic en el video. El video se ampliará hasta el tamaño del video tile.

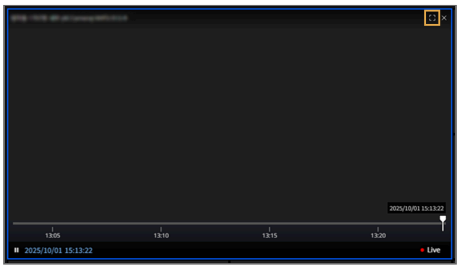


Cambiar ubicación del video

Haga clic en el video para moverlo y arrástrelo hasta la ubicación deseada. Es posible cambiar la posición del video seleccionado.



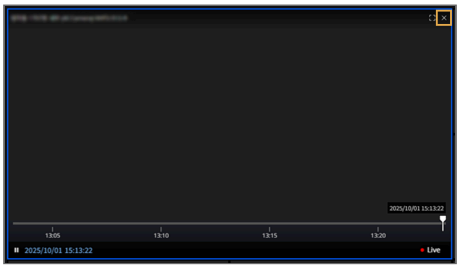
Vista de pantalla completa



Haz clic en ⛶ en la esquina superior derecha del video para verlo en pantalla completa.

Haz clic en ⛶ en la esquina superior derecha de la pantalla para salir de pantalla completa. O presiona la tecla en el teclado.

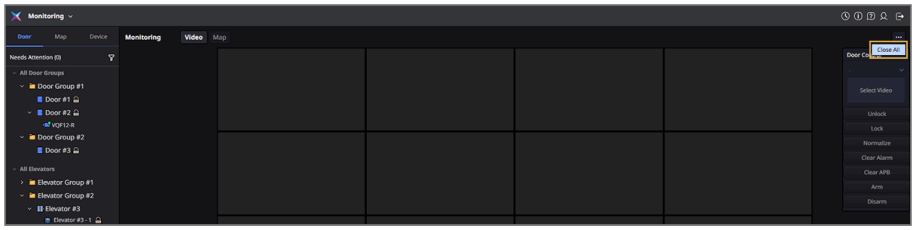
Cerrar video



Haz clic en ✕ en la esquina superior derecha del video para cerrarlo.

Cerrar todos los videos

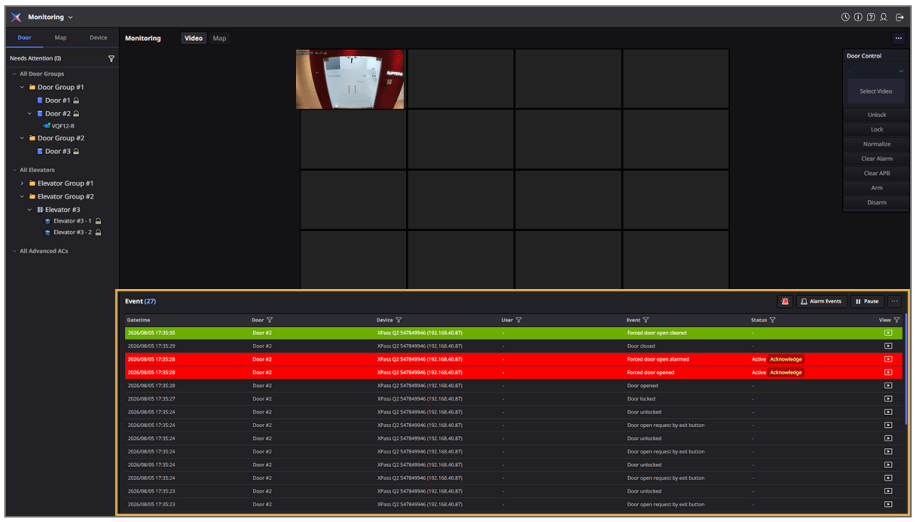
Haz clic en ••• en la esquina superior derecha de la pantalla para cerrar todos los videos. Haz clic en **Close All** en el menú emergente.



Supervisar Evento

En la sección **Event** en la parte inferior de la página de supervisión, revise y gestione eventos en tiempo real. Gestione

eventos de forma eficiente mediante funciones como estado de eventos, manejo de eventos de alarma, filtrado y codificación por colores. Supervise en tiempo real los eventos relacionados con puertas, dispositivos y usuarios y tome medidas rápidas según sea necesario.



Revisar la lista de eventos

En la sección **Event**, visualice los eventos a medida que ocurren en tiempo real. Cada evento incluye la siguiente información:



- **Datetime**: Fecha y hora en que ocurrió el evento.
- **Door**: Puerta donde ocurrió el evento.
- **Device**: Dispositivo en el que ocurrió el evento.
- **User**: Usuario que generó el evento.
- **Event**: Información detallada del evento.
- **Status**: Estado del evento. Los eventos activos se muestran como **Active**. Los eventos de alarma muestran un botón **Acknowledge**. Haga clic en **Acknowledge** para resolver el evento.



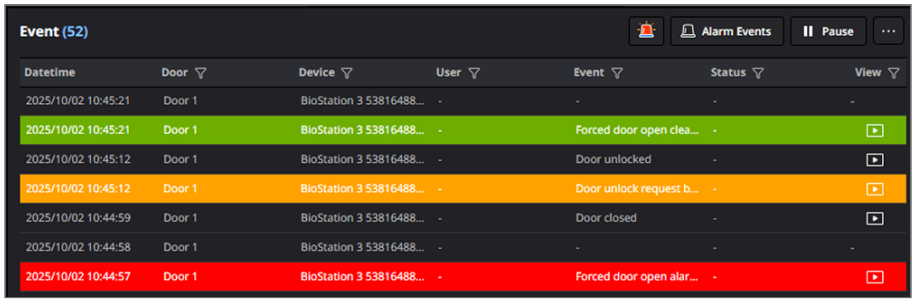
- **View**: Si el evento incluye información de video de la cámara conectada a la puerta, se muestra un ícono de video ( ). Haga clic en este ícono para ver el video.

Información

- Haga clic en un evento individual para mostrar información detallada en el lado derecho de la pantalla. Esta información detallada incluye la hora del evento, área, puerta, dispositivo, grupo de usuarios, usuario, puerto y detalles del evento.
- Si el evento incluye información de video o imágenes de una cámara conectada a la puerta, también podrá ver los registros de video e imágenes.

Distinguir eventos por color

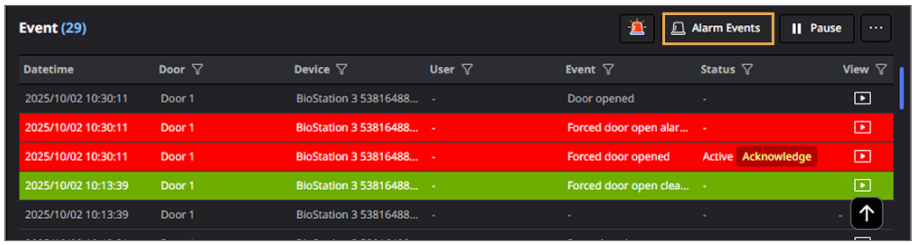
Los eventos en la lista se pueden distinguir por color:



- **Sin color**: Evento normal.
- Naranja: Evento de precaución. Indica eventos que requieren atención, como intentos de acceso no autorizado en áreas restringidas o puertas que quedan abiertas.
- Rojo: Evento de alarma. Indica un evento de advertencia que requiere acción en el sistema.
- Verde: Evento de alarma resuelto.

Revisar eventos de alarma

Solo los eventos de alarma se pueden ver en la sección **Event**. Haga clic en **Alarm Events** en la esquina superior derecha de la sección **Event**. La lista mostrará solo eventos de alarma, los cuales se indican en rojo. Los eventos de alarma se muestran en rojo.



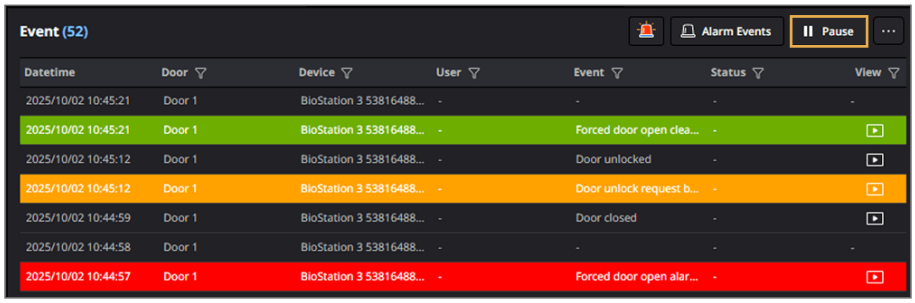
Información

Para ver todos los eventos, haga clic en **All Events** en la esquina superior derecha de la sección **Event**.

Eventos en tiempo real

Revise los eventos a medida que ocurren en tiempo real en la lista de la sección **Event**. Para detener los eventos en tiempo

real, haga clic en ⏸ **Pause** en la esquina superior derecha de la sección **Event**. Haga clic en ▶ **Play** para reanudar los eventos en tiempo real.

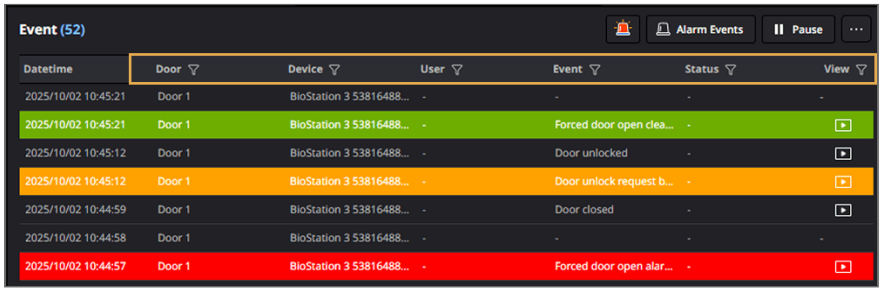


Filtrar eventos

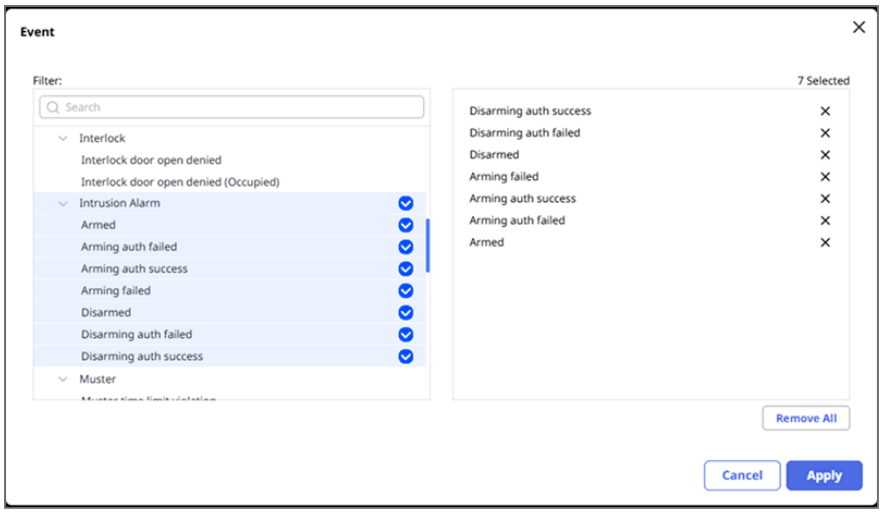
Aplicar filtros

Los usuarios pueden filtrar la lista de eventos según los criterios deseados, lo que permite identificar rápidamente los eventos relevantes. Esto le permite revisar rápidamente los eventos según las condiciones deseadas.

1. Haga clic en ▽ en cada columna de encabezado de la sección **Event**.



2. Cuando aparezca la ventana de filtro, seleccione el elemento deseado de la lista izquierda.



   - Selecciona una opción principal para seleccionar todas las opciones secundarias.
   - Haz clic en ✕ para deseleccionar la opción seleccionada. Para borrar todos los elementos, haga clic en **Remove All**.

3. Una vez que haya terminado la configuración, haga clic en **Apply**.

Solo se mostrarán en la lista los eventos que cumplan las condiciones establecidas.

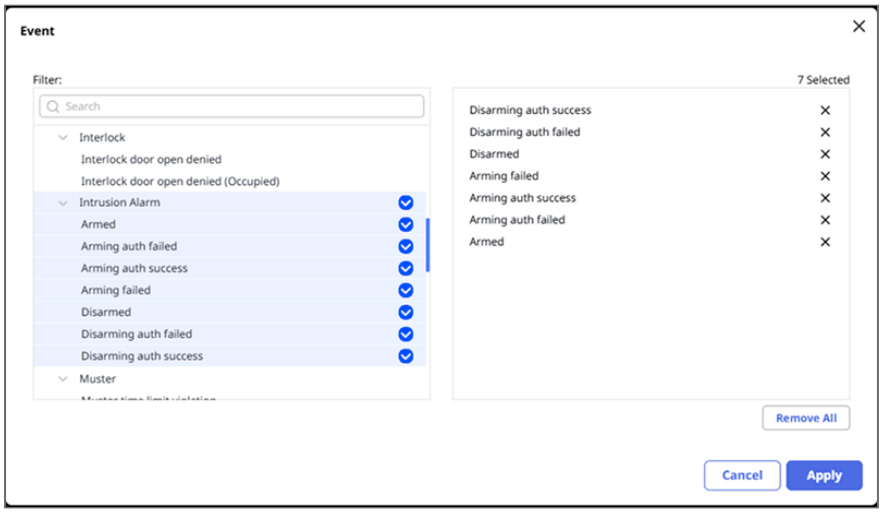
Información

- También puede buscar rápidamente los elementos deseados usando el campo de búsqueda en la ventana de filtro.
- Se pueden definir múltiples condiciones para cada columna de encabezado; si se especifica más de una condición, se aplicará la condición AND. Al establecer más de una condición, se aplica la condición AND.
- Los elementos que se pueden filtrar pueden variar según la columna de encabezado.
- Cuando defines condiciones de filtrado, el ícono en la columna de encabezado cambia de color.

Eliminar filtros

Puede borrar las condiciones de filtro aplicadas.

1. En la lista de la sección **Event**, haz clic en el ícono de la columna de encabezado con filtros aplicados.
2. Cuando aparezca la ventana de filtro, haz clic en a la derecha de la opción que vas a deseleccionar en la lista de la derecha. Para borrar todos los filtros, haga clic en **Remove All**.



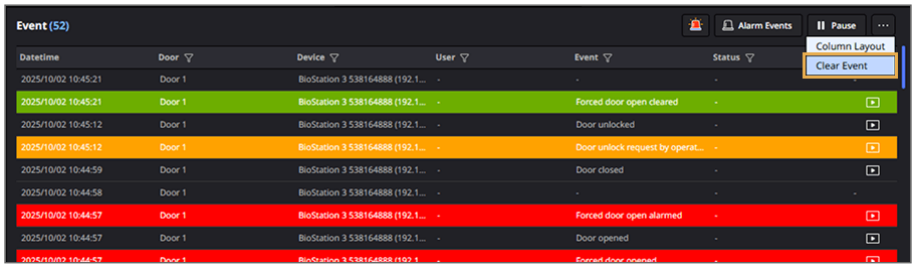
3. Una vez que haya configurado todas las condiciones a borrar, haga clic en **Apply**.

Información

- También puede buscar rápidamente los elementos deseados usando el campo de búsqueda en la ventana de filtro.
- Cuando se borran las condiciones de filtrado, el color del ícono en la columna de encabezado vuelve a su estado original.

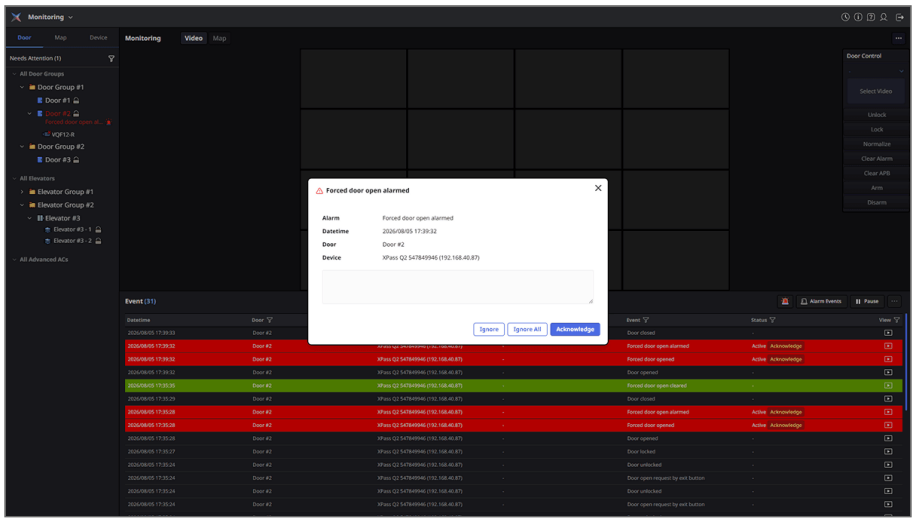
Borrar la lista de eventos

En la sección **Event**, borre eventos. Haga clic en en la esquina superior derecha de la sección **Event** y seleccione **Clear Event** en el menú emergente. Si hay muchos eventos innecesarios acumulados en la lista, utilice la función **Clear Event** para limpiarla.



Confirmar alarma y registrar acción

Cuando ocurre un evento de alarma, como la apertura forzada de la puerta, aparece una ventana de mensaje de alarma. La ventana de mensaje de alarma incluye información detallada sobre el evento de alarma activado. En este momento, el administrador puede registrar su confirmación del evento de alarma activado y las acciones realizadas.



> **Información**
>
> El botón **Ignore All** se muestra solo cuando ocurren dos o más eventos de alarma.

Registrar acción para el evento de alarma

Ingresa las acciones relacionadas con el evento de alarma en el campo de entrada de mensaje. Ingresa hasta 500 caracteres. Ingresa las acciones y haz clic en **Acknowledge**. Registra la confirmación y las acciones relacionadas con el evento de alarma. La ventana de mensaje de alarma se cerrará.



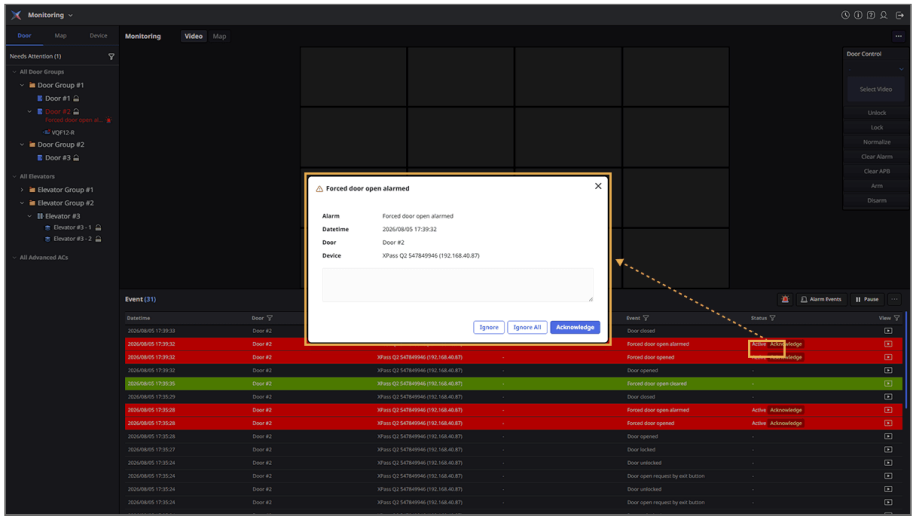
Aplazar la confirmación de un evento de alarma

Aplaza la confirmación del evento de alarma haciendo clic en **Ignore**. Se pueden registrar las acciones realizadas. La ventana de mensaje de alarma se cerrará. Los eventos de alarma aplazados se muestran en la lista de eventos con el estado **Active**, y se puede usar el botón **Acknowledge**.



Verificar eventos de alarma en la lista de eventos

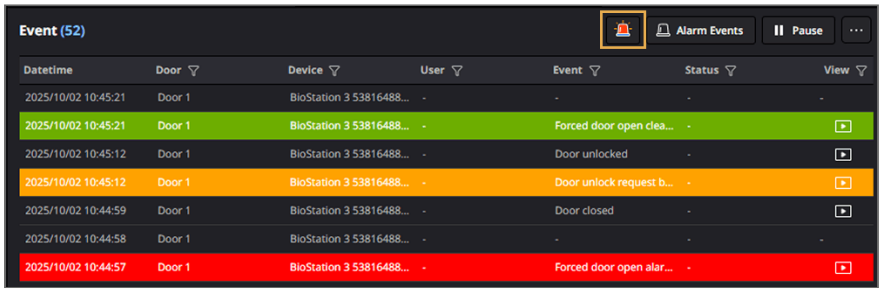
Haz clic en **Acknowledge** que aparece en la columna **Status** de la lista de eventos para registrar la confirmación y las acciones relacionadas con los eventos de alarma activados. Completa tu entrada y haz clic en **Acknowledge**.



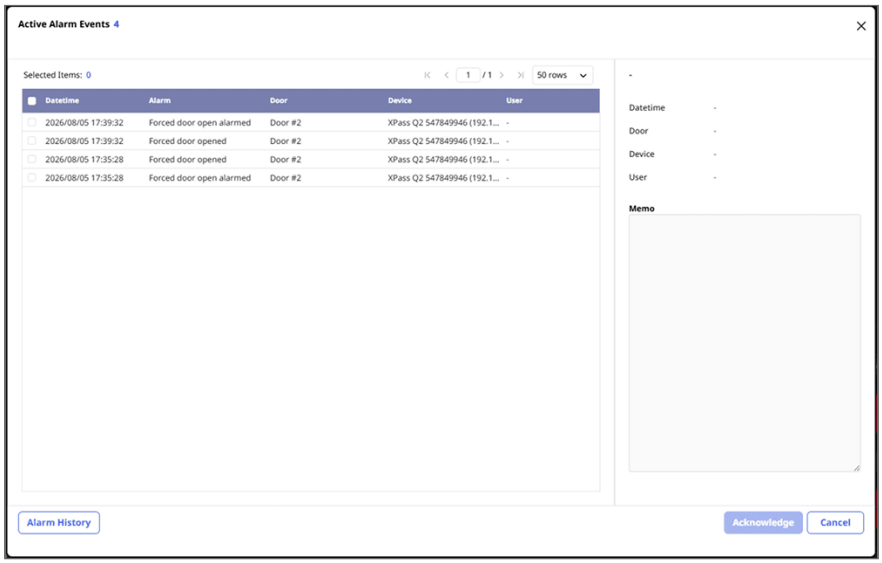
Ver eventos de alarma sin confirmar

Esta función muestra todos los eventos de alarma sin confirmar a la vez y permite registrar las acciones realizadas. Es especialmente útil cuando ocurren múltiples eventos de alarma idénticos.

1. Haz clic en en la esquina superior derecha de **Event**.



2. Cuando aparezca la ventana **Active Alarm Events**, selecciona en la lista izquierda el evento de alarma para registrar las acciones. Para seleccionar todos los eventos, haz clic en la casilla de verificación ubicada en el extremo izquierdo de la columna de encabezado.



3. Ingresa las acciones relacionadas con el evento de alarma en el campo de entrada **Memo**.

4. Haz clic en **Acknowledge**.

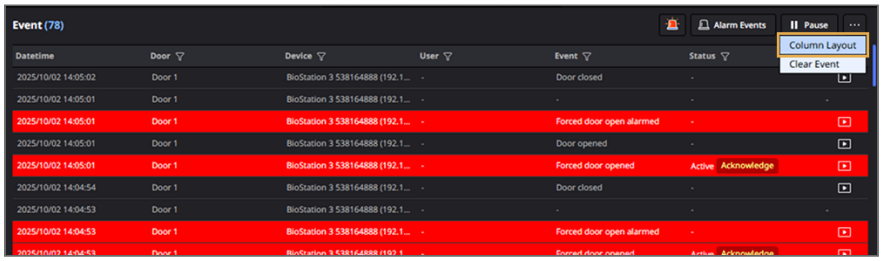
Registra las acciones realizadas para el evento seleccionado. Aparecerá una ventana emergente para ingresar la confirmación del evento de alarma y las acciones realizadas.

> **Información**
>
> Selecciona más de un evento de la lista de eventos de alarma para activar el botón **Acknowledge**.

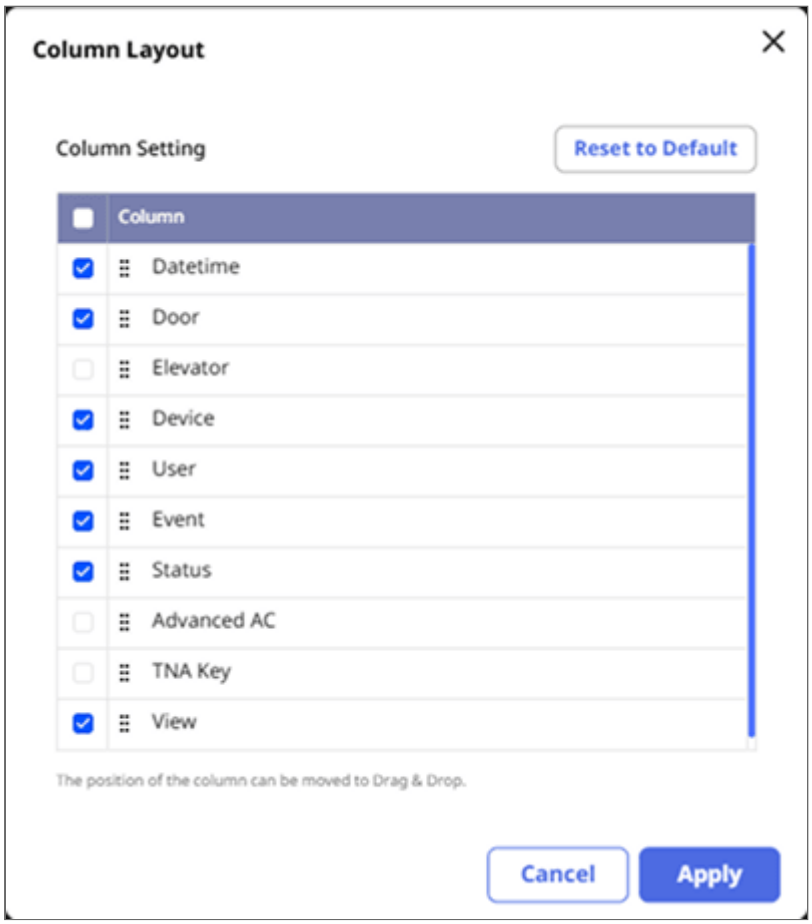
Configurar columnas de la lista de eventos

Agrega columnas para mostrar en la lista de eventos, reordénalas y ocúltalas según sea necesario.

1. Haz clic en ••• → **Column Layout** en la esquina superior derecha de **Event**.



2. Cuando aparezca la ventana **Column Layout**, haz clic en las casillas de las columnas para mostrarlas u ocultarlas. También cambia el orden de las columnas mediante arrastrar y soltar.



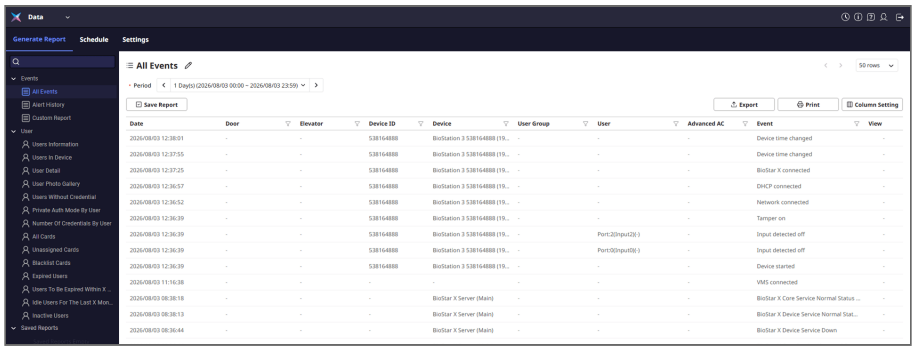
3. Después de realizar todos los cambios en la configuración de columnas, haz clic en **Apply**.

> **Información**
> Haz clic en el botón **Default Column** para inicializar la configuración de columnas.

Fecha

Con el menú **Data**, puede consultar la información de los usuarios registrada en **BioStar X** o los eventos que cumplan criterios específicos y generar informes con una programación periódica. Puede generar automáticamente el informe deseado de forma periódica si es necesario, y el informe generado se puede exportar como archivos CSV o PDF o imprimir.

Haga clic en **Data** o seleccione **Data** en la lista de accesos directos en la parte superior izquierda de la pantalla en la página **Launcher**.



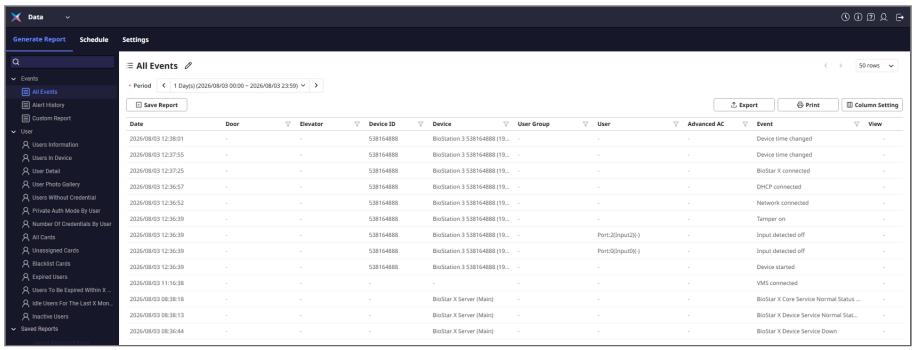
Generar Reporte

Puede ver todos los eventos que ocurrieron en **BioStar X** o solo el historial de alarmas. Puede filtrar y generar informes personalizados según las condiciones definidas por el usuario.

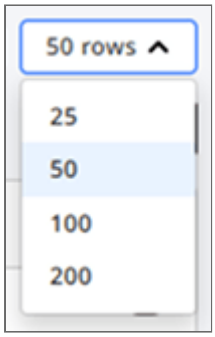
Haga clic en **Data** o seleccione **Data** en la lista de accesos directos en la parte superior izquierda de la pantalla en la página **Launcher**.

Ver todos los eventos

Puede ver todos los eventos que ocurrieron en **BioStar X**. Haga clic en **Events** → **All Events** en la barra lateral izquierda de la pantalla.

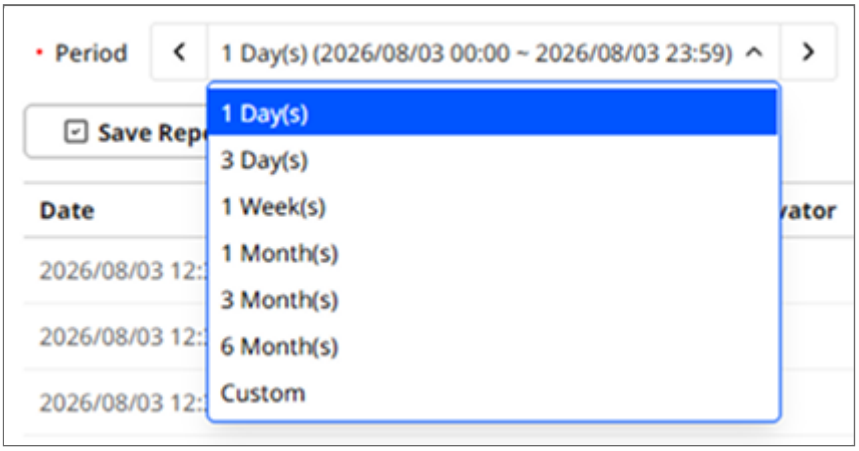


- Para revisar la página anterior o siguiente de los resultados listados, haga clic en ‹ o › en la esquina superior derecha de la pantalla.
- Para cambiar la cantidad de filas que se muestran en la lista, haga clic en el menú desplegable en la esquina superior derecha de la pantalla y seleccione el valor deseado. Puede seleccionar un mínimo de 25 filas y un máximo de 200 filas.

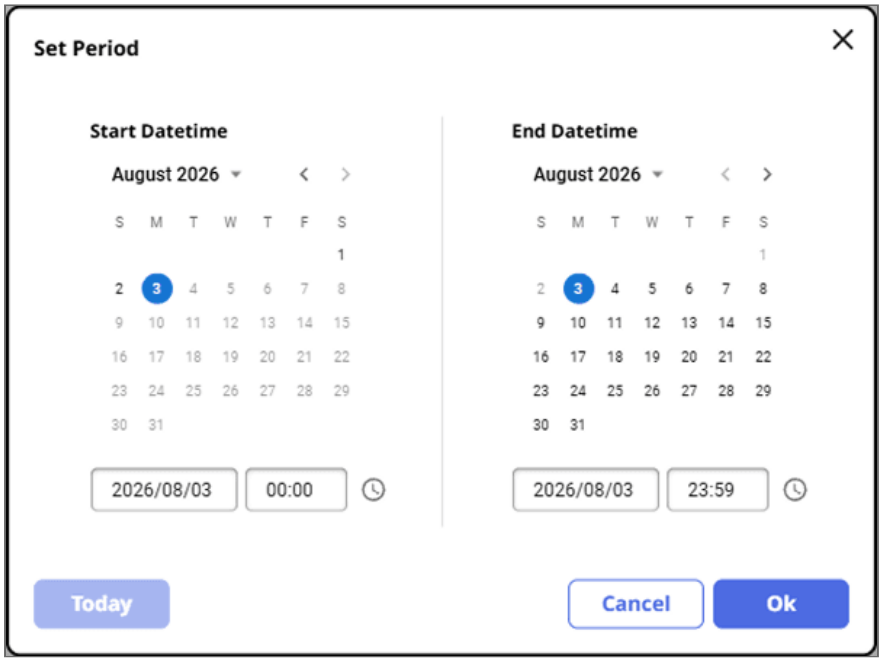


Establecer período

Establezca el período deseado en la opción **Period** en la esquina superior izquierda de la pantalla. Haga clic en el área de fecha.



- Seleccione períodos predefinidos desde hoy, de 1 a 6 meses. La lista muestra automáticamente los eventos ocurridos durante el período seleccionado.
- Seleccione **Custom** para establecer manualmente el período deseado. En la ventana de selección de período, defina inicio, fin y hora; luego haga clic en **Ok**. La lista muestra automáticamente los eventos ocurridos durante el período establecido.

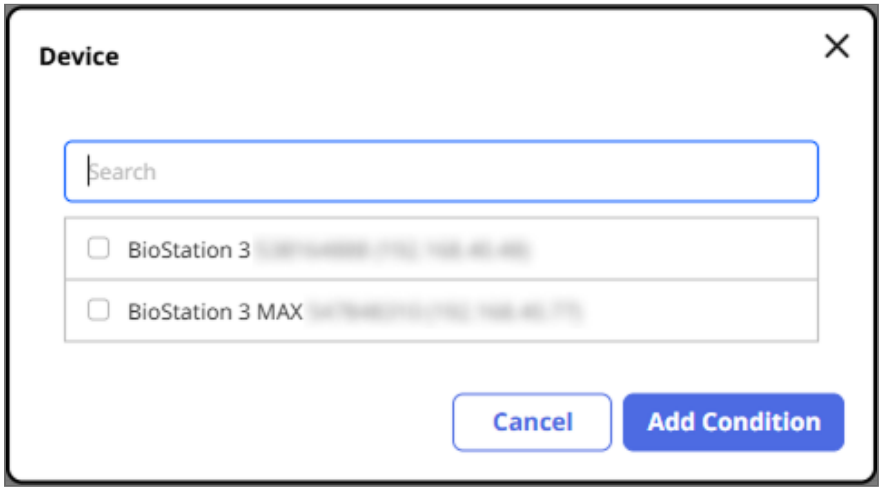


> **Información**
> Para seleccionar la fecha de hoy, haga clic en **Today**.

Establecer condiciones de consulta

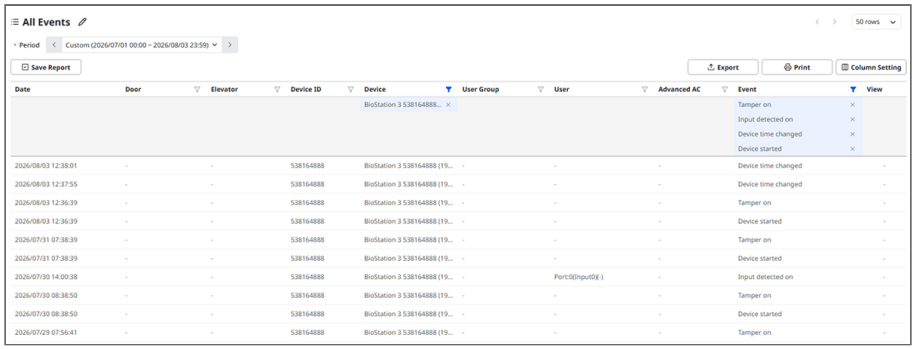
Puede filtrar la lista estableciendo las condiciones deseadas en la sección de encabezado de la lista de consulta. Puede establecer condiciones para todos los elementos excepto las fechas.

1. En la sección de encabezado de la lista de eventos, haga clic en el botón de la columna deseada.
2. Cuando aparezca la ventana de condiciones de filtro, seleccione los elementos deseados.



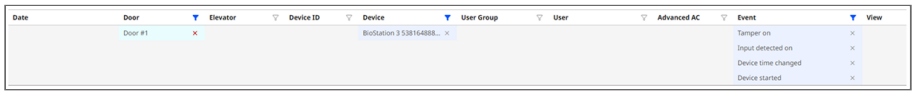
3. Una vez completada la selección, haga clic en el botón **Add Condition**.

Solo se mostrarán en la lista los eventos que coincidan con las condiciones seleccionadas.



Borrar condiciones de consulta

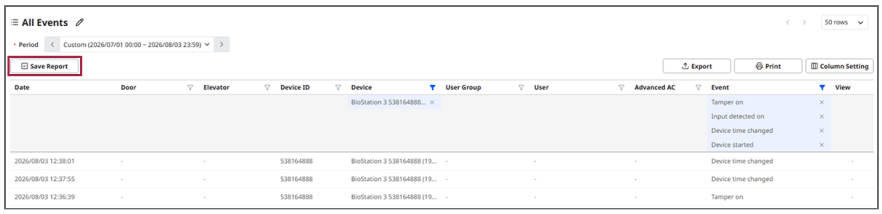
Para borrar las condiciones de consulta establecidas, haga clic en el botón en el conjunto de condiciones debajo de la sección de encabezado. Las condiciones establecidas se borrarán y todos los eventos se mostrarán nuevamente en la lista.



Guardar informe

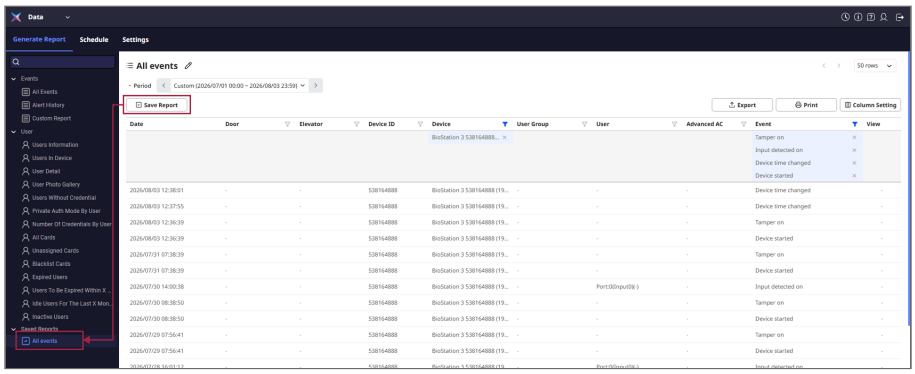
Guarde los eventos como un informe con el período de consulta y las condiciones que estableció.

1. Haga clic en **Save Report** en la parte superior izquierda de la lista de eventos.



2. Cuando un mensaje confirme que la plantilla del informe se guardó correctamente, haga clic en **Ok**.

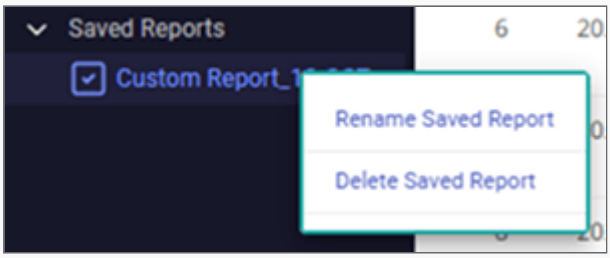
3. Consulte los informes guardados en **Saved Reports** en la barra lateral izquierda.



El sistema almacena los informes guardados como plantillas para reutilizarlos al generar informes en las mismas condiciones.

Información

- Haga clic en el botón ✎ en la parte superior del informe para editar el título del informe guardado, los elementos de evento, el período y las condiciones de filtro.
- Cambie también el título del informe en **Saved Reports** en la barra lateral izquierda de la pantalla. Seleccione el informe personalizado cuyo título desee cambiar y haga clic con el botón derecho. Seleccione **Rename Saved Report** en el menú emergente.



- Para obtener más información sobre cómo gestionar informes, consulte Gestión de informes.

Ver video del evento

Si una cámara está conectada al dispositivo del evento, la columna **View** muestra el icono ▶ para ese evento. Al hacer clic en el icono, vea el video del momento en que ocurrió el evento en una ventana emergente.



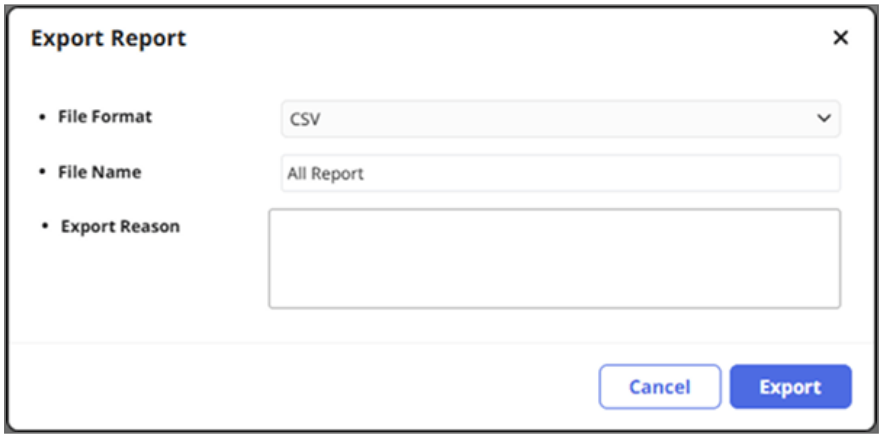
Información

- Si conecta varias cámaras en los ajustes de reglas de cámara, el sistema reproduce el video de la primera cámara. Para obtener más información sobre cómo configurar las reglas para cámaras, consulte Configurar Reglas de Video.
- Para obtener más información sobre cómo vincular cámaras con puertas, consulte Configurar Reglas de Video.
- Esta característica está disponible al comprar opciones adicionales con una licencia **Essential** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Exportar a CSV

Puede exportar la lista de eventos consultados como un archivo CSV.

1. Haga clic en **Export** en la esquina superior derecha de la pantalla.
2. Cuando aparezca la ventana **Export Report**, seleccione **CSN** en **File Format**.



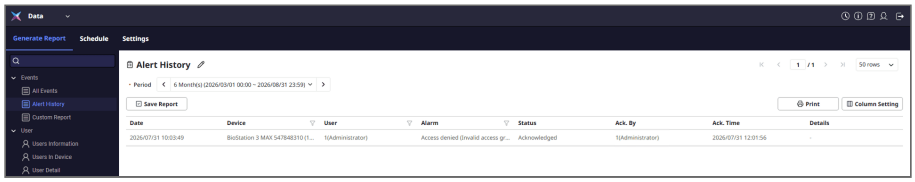
3. Edite el nombre del archivo que se guardará en **File Name**.
4. Ingrese **Export Reason** (opcional) y haga clic en **Export**.

5. Guarda el archivo CSV en la ubicación deseada de tu ruta local.

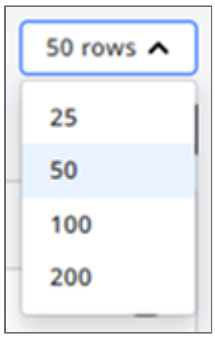
> **Información**
>
> **Export Reason** es opcional. Verifique los registros de motivos de exportación en **Settings** → **Audit Trail** → **AC Audit Log**.

Ver historial de alarmas

Solo puede ver el historial de alarmas (alertas). Haga clic en **Events** → **Alert History** en la barra lateral izquierda de la pantalla.



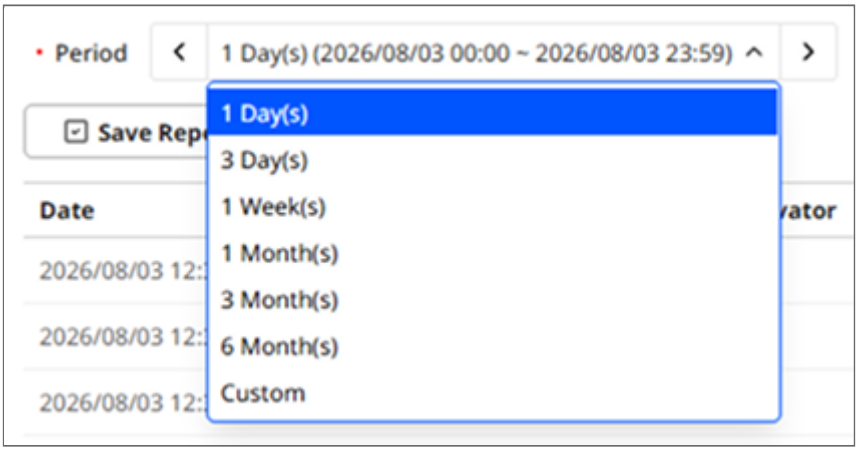
- Para revisar la página anterior o siguiente de los resultados listados, haga clic en ‹ o › en la esquina superior derecha de la pantalla.
- Para ir a la primera o última página de la lista consultada, haga clic en |‹ o ›| en la esquina superior derecha de la pantalla.
- Para cambiar la cantidad de filas que se muestran en la lista, haga clic en el menú desplegable en la esquina superior derecha de la pantalla y seleccione el valor deseado. Puede seleccionar un mínimo de 25 filas y un máximo de 200 filas.



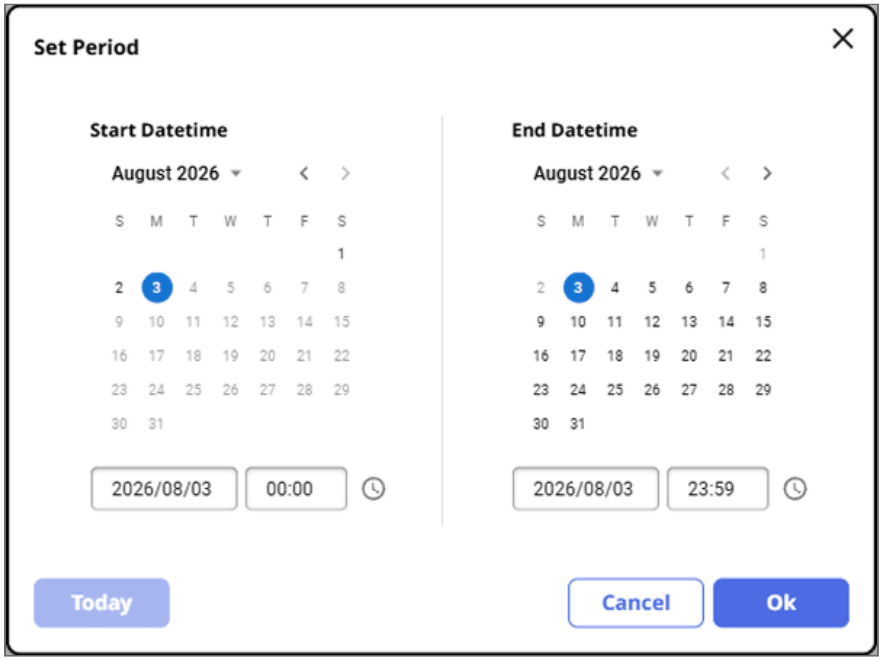
> **Información**
>
> Para obtener más información sobre cómo visualizar eventos de alarma (alerta) en el monitoreo de eventos, consulte Supervisar Evento.

Establecer período

Establezca el período deseado en la opción **Period** en la esquina superior izquierda de la pantalla. Haga clic en el área de fecha.



- Seleccione períodos predefinidos desde hoy, de 1 a 6 meses. La lista muestra automáticamente los eventos ocurridos durante el período seleccionado.
- Seleccione **Custom** para establecer manualmente el período deseado. En la ventana de selección de período, defina inicio, fin y hora; luego haga clic en **Ok**. La lista muestra automáticamente los eventos ocurridos durante el período establecido.

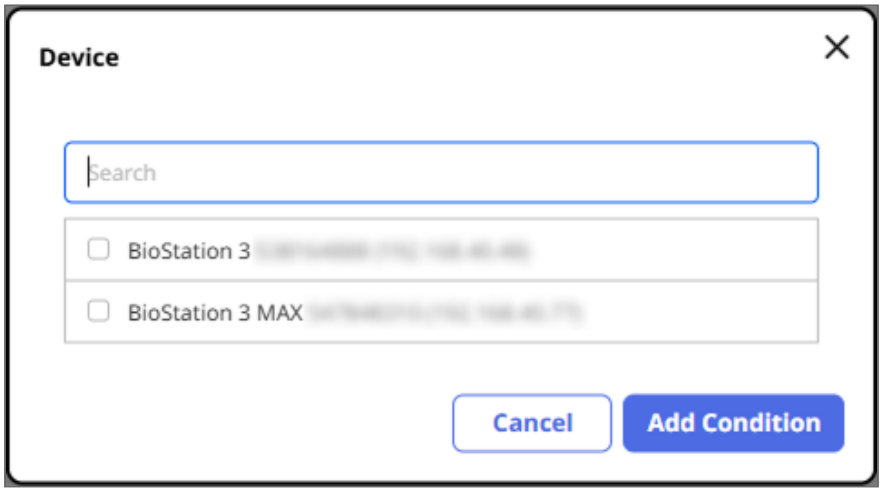


> **Información**
> Para seleccionar la fecha de hoy, haga clic en **Today**.

Establecer condiciones de consulta

Puede filtrar la lista estableciendo las condiciones deseadas en la sección de encabezado de la lista de consulta. Puede establecer condiciones para todos los elementos excepto las fechas.

1. En la sección de encabezado de la lista de eventos, haga clic en el botón de la columna deseada.
2. Cuando aparezca la ventana de condiciones de filtro, seleccione los elementos deseados.



3. Una vez completada la selección, haga clic en el botón **Add Condition**.

Solo se mostrarán en la lista los eventos que coincidan con las condiciones seleccionadas.



Borrar condiciones de consulta

Para borrar las condiciones de consulta establecidas, haga clic en el botón ✕ en el conjunto de condiciones debajo de la sección de encabezado. Las condiciones establecidas se borrarán y todos los eventos se mostrarán nuevamente en la lista.



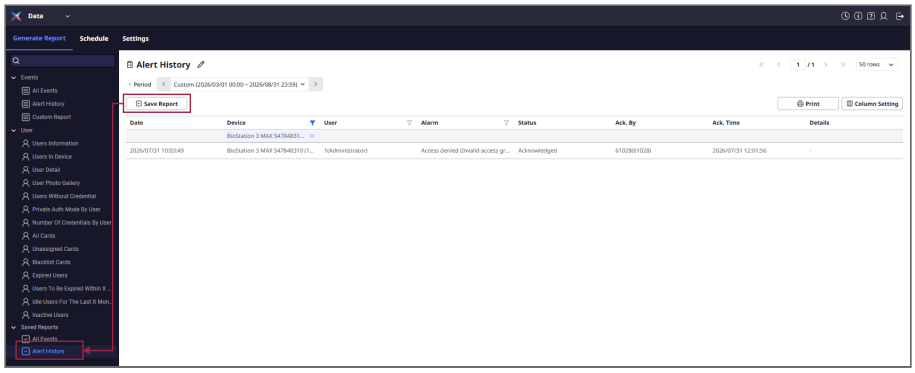
Guardar informe

Guarde el historial de alarmas como informe con el período de consulta y las condiciones que estableció.

1. Haga clic en **Save Report** en la parte superior izquierda de la lista del historial de alarmas.



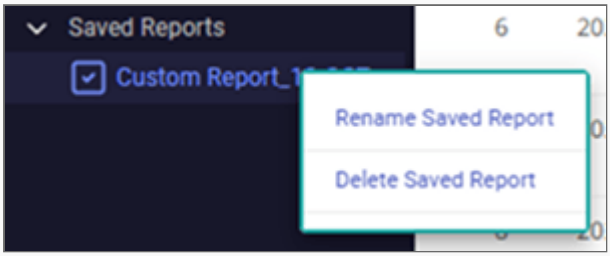
2. Cuando un mensaje confirme que la plantilla del informe se guardó correctamente, haga clic en **Ok**.
3. Consulte los informes guardados en **Saved Reports** en la barra lateral izquierda.



El sistema almacena los informes guardados como plantillas para reutilizarlos al generar informes en las mismas condiciones.

Información

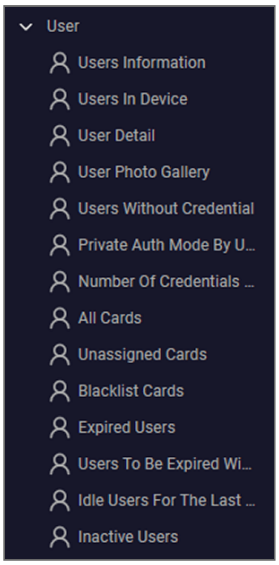
- Haga clic en el botón en la parte superior del informe para editar el título del informe guardado, los elementos de evento, el período y las condiciones de filtro.
- Cambie también el título del informe en **Saved Reports** en la barra lateral izquierda de la pantalla. Seleccione el informe personalizado cuyo título desee cambiar y haga clic con el botón derecho. Seleccione **Rename Saved Report** en el menú emergente.



- Para obtener más información sobre cómo gestionar informes, consulte Gestión de informes.

Ver informes de usuarios

Puede seleccionar plantillas relacionadas con usuarios para generar informes. En la barra lateral izquierda de la pantalla, haga clic en la plantilla deseada bajo **User**.



- **Users Information**: Puede ver información detallada del usuario en formato de lista.
- **Users In Device**: Puede ver información de los usuarios registrados en el dispositivo.
- **User Detail**: Puede ver información detallada del usuario en formato de tarjeta.
- **User Photo Gallery**: Puede ver las fotos de perfil de los usuarios en formato de galería.
- **Users Without Credential**: Puede ver a los usuarios que no han configurado credenciales.
- **Private Auth Mode By User**: Puede ver la configuración de modos de autenticación privada específicos de cada usuario.
- **Number Of Credentials By User**: Puede ver la cantidad de credenciales

configuradas para el usuario.

- **All Cards**: Puede ver usuarios según las tarjetas enroladas.
  - **Unassigned Cards**: Puede ver las tarjetas que no se han asignado a usuarios.
  - **Blacklist Cards**: Puede ver las tarjetas deshabilitadas.
- **Expired Users**: Puede ver a los usuarios cuya fecha de vencimiento ha pasado.
- **Users To Be Expired Within X Days**: Puede ver a los usuarios cuya fecha de vencimiento se aproxima en N días. Puede ingresar directamente el número de días antes de generar el informe.
- **Idle users for the last N months**: Puede ver a los usuarios que no han tenido registros de acceso durante los últimos N meses. Puede ingresar directamente el número de meses antes de generar el informe.
- **Inactive Users**: Puede ver a los usuarios inactivos.

Información

- El informe generado se puede guardar en **Saved Reports**. Haga clic en el botón **Save Report** en la esquina superior izquierda del informe.
- Para obtener más información sobre cómo gestionar informes, consulte Gestión de informes.

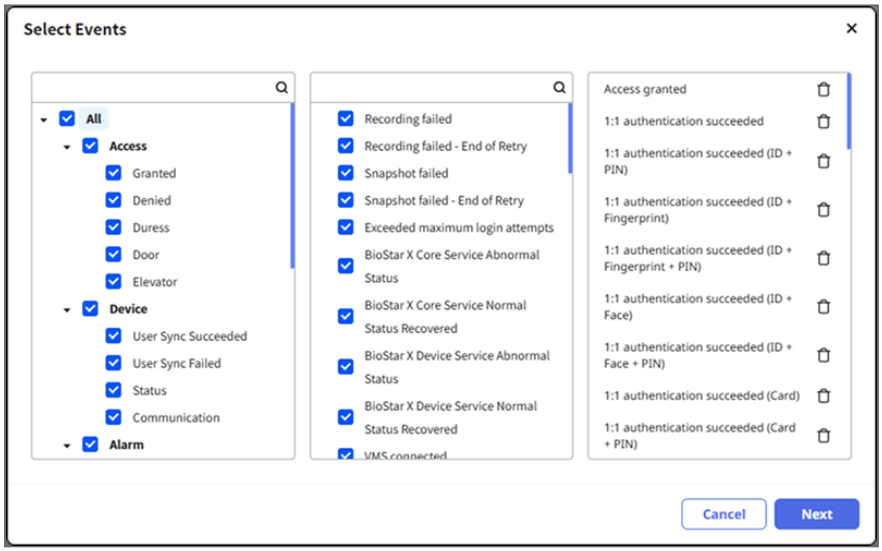
Generar un informe personalizado

Puede filtrar y generar informes personalizados según las condiciones deseadas. Guarde el informe generado como plantilla para utilizarlo fácilmente cuando genere informes con las mismas condiciones en el futuro.

1. Haga clic en **Events** → **Custom Report** en la barra lateral izquierda de la pantalla.
2. En la ventana **Select Events**, seleccione los eventos deseados.

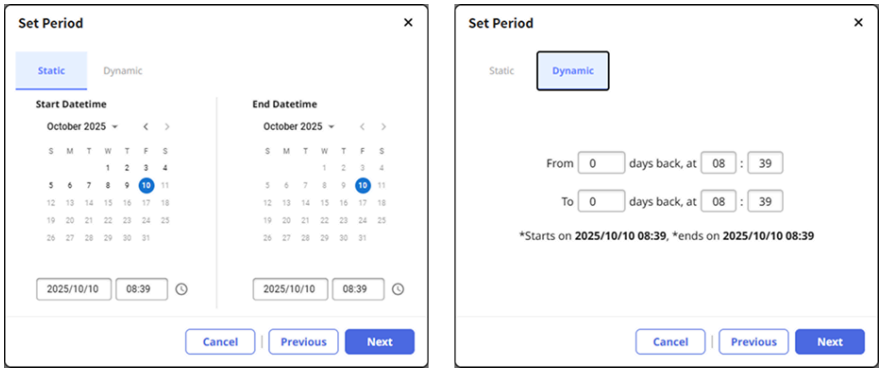


3. Después de completar la selección de eventos, haga clic en **Next**.



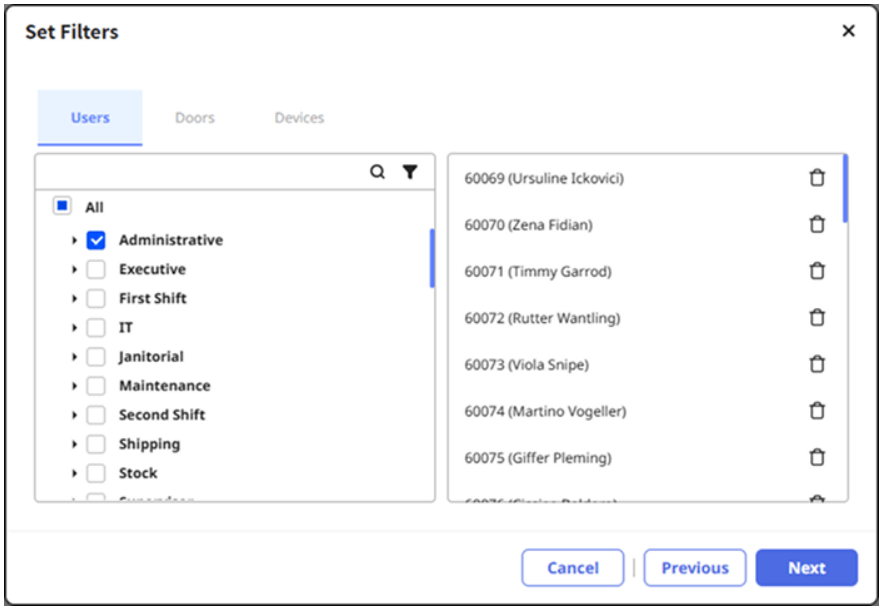
- Busque los elementos deseados en el campo de búsqueda (🔍).
- Haga clic en 🗑 en la lista de la derecha para excluir los elementos seleccionados.

4. Establezca el periodo de consulta y haga clic en **Next**.



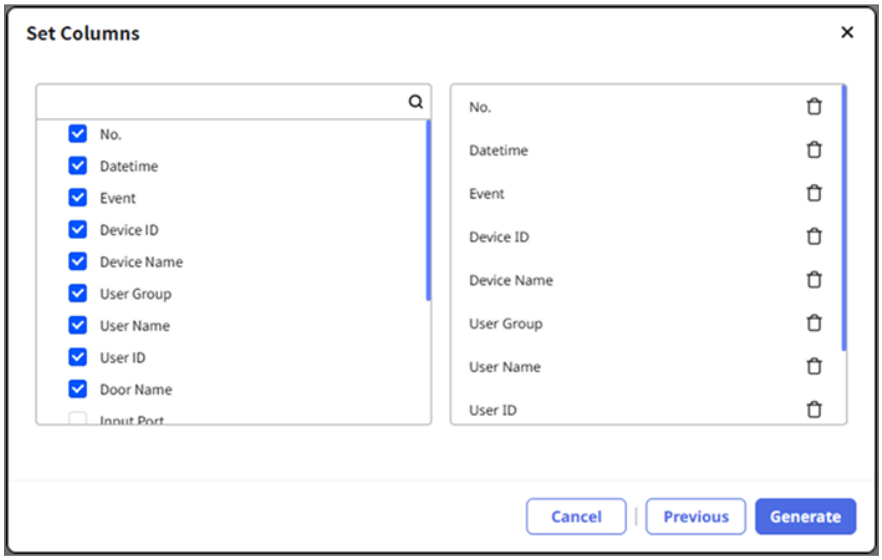
- **Static**: Establezca una fecha y hora específicas para definir el periodo de consulta.
- **Dynamic**: Establezca la fecha de inicio, la fecha de finalización y la hora basadas en hoy. Es útil al generar informes de forma repetitiva para un periodo específico.

5. Configure las condiciones según usuarios, puertas y dispositivos, agrupados o individualmente.

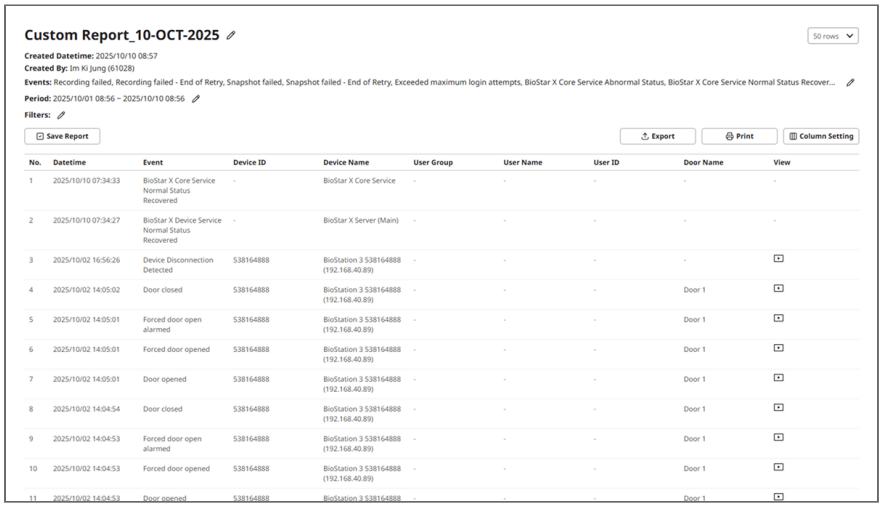


- Haga clic en 🗑 en la lista de la derecha para excluir los elementos seleccionados.

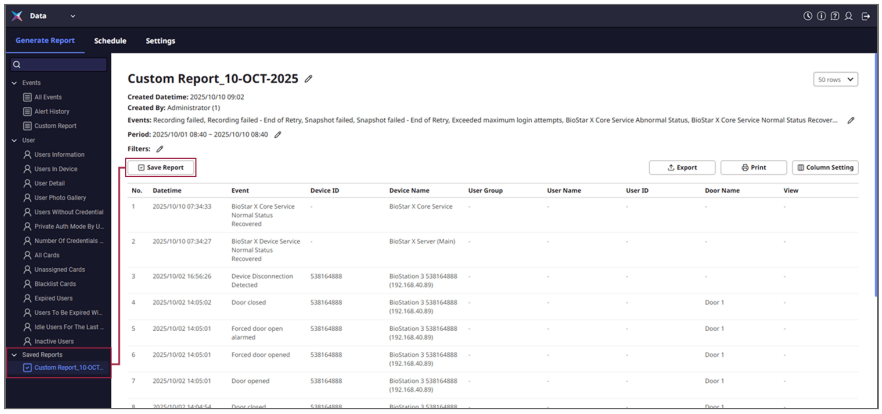
6. Seleccione las condiciones deseadas y haga clic en **Next**.
7. En la ventana de configuración de columnas, seleccione las columnas que se mostrarán en el informe.



8. Después de seleccionar las columnas, haga clic en **Generate**.
9. Genere un informe según las condiciones que estableció.



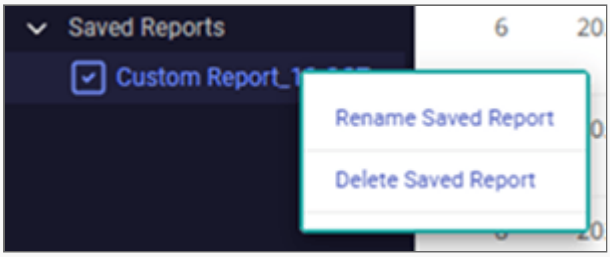
10. Haga clic en **Save Report** en la parte superior izquierda de la lista para guardar el informe generado como plantilla. Consulte los informes guardados en **Saved Reports** en la barra lateral izquierda de la pantalla.



El sistema almacena los informes guardados como plantillas para reutilizarlos al generar informes en las mismas condiciones.

Información

- Haga clic en el botón ✎ en la parte superior del informe para editar el título del informe guardado, los elementos de evento, el período y las condiciones de filtro.
- Cambie también el título del informe en **Saved Reports** en la barra lateral izquierda de la pantalla. Seleccione el informe personalizado cuyo título desee cambiar y haga clic con el botón derecho. Seleccione **Rename Saved Report** en el menú emergente.

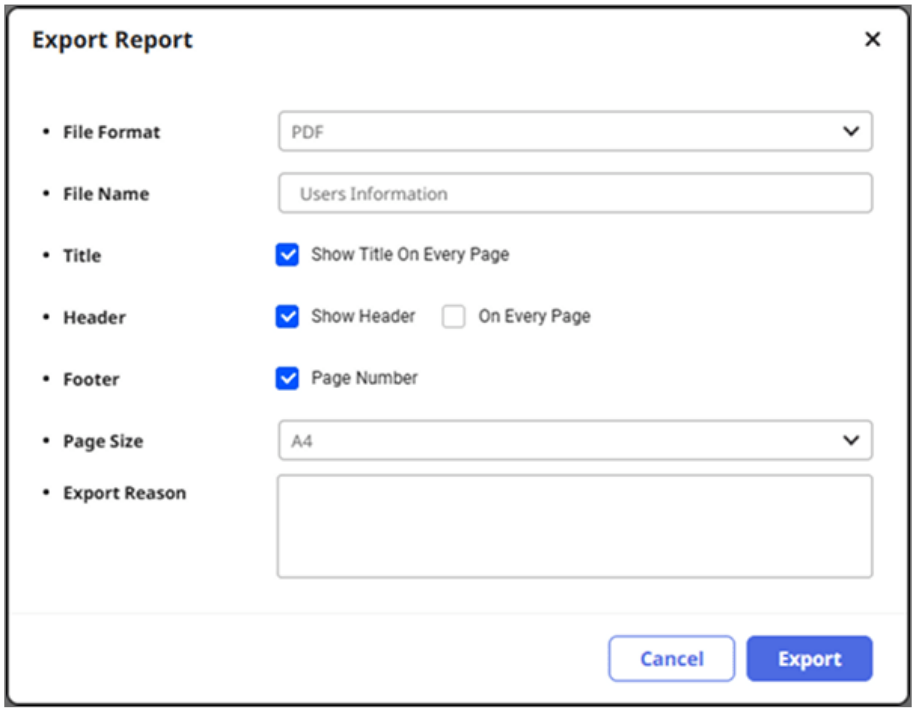


- Para obtener más información sobre cómo gestionar informes, consulte Gestión de informes.

Gestión de informes

Guardar archivo de informe

Haga clic en **Export** para exportar el informe como archivo PDF o CSV. Cuando aparezca la ventana **Export Report**, configure cada campo y haga clic en **Export**.

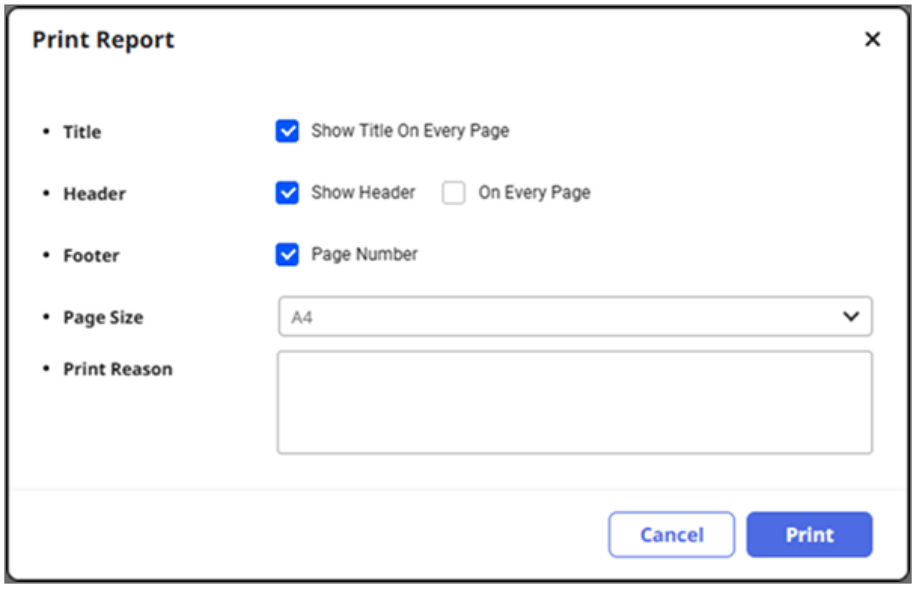


Información

Export Reason es opcional. Verifique los registros de motivos de exportación en **Settings** → **Audit Trail** → **AC Audit Log**.

Imprimir informe

Haga clic en **Print** para imprimir el informe con una impresora conectada a su PC. Cuando aparezca la ventana **Print Report**, configure cada opción y haga clic en **Print**.

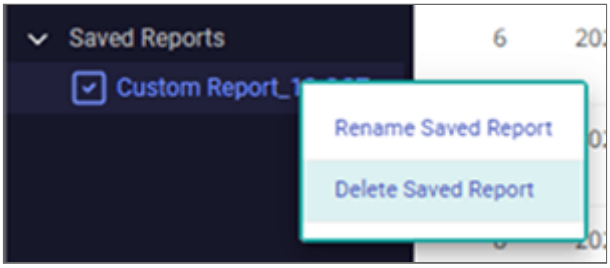


La pantalla de vista previa de impresión aparece en una pestaña nueva del navegador web. Haga clic en el botón Imprimir en la parte superior derecha de la pantalla para iniciar la impresión.

> **Información**
> **Print Reason** es opcional. Verifique los registros de motivos de impresión en **Settings** → **Audit Trail** → **AC Audit Log**.

Eliminar informe

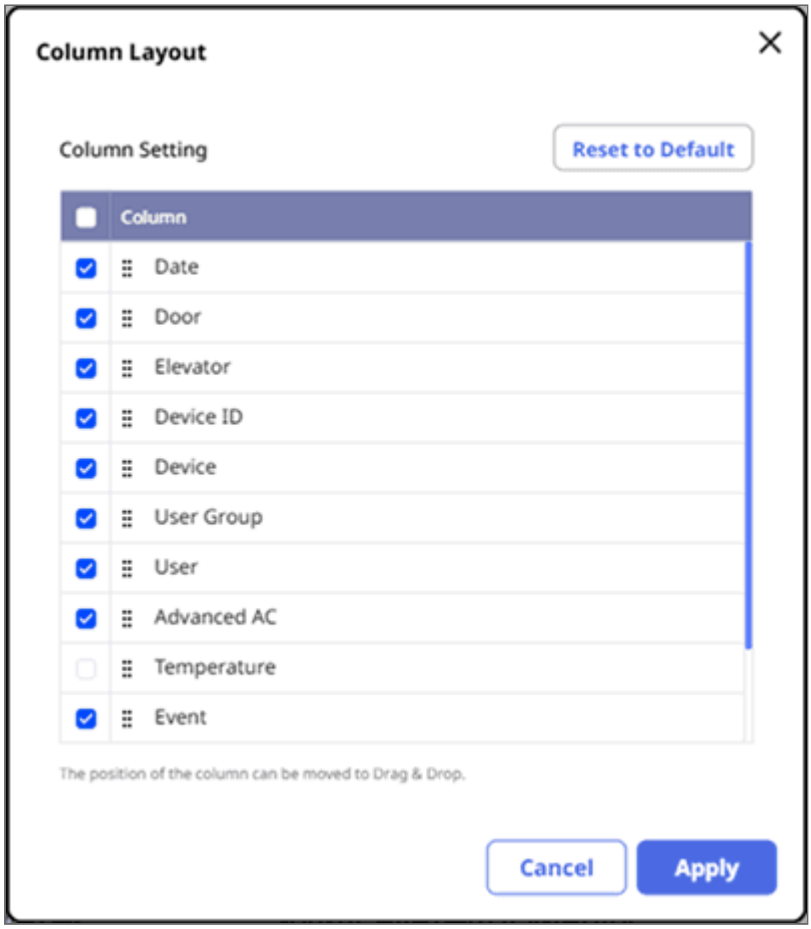
Seleccione el informe guardado que desea eliminar en **Saved Reports** en la barra lateral izquierda y haga clic con el botón derecho. Seleccione **Delete Saved Report** en el menú emergente.



Configurar columnas

Cambie los ajustes de las columnas que aparecen en el informe. En los ajustes de columnas, seleccione las columnas que aparecerán o cambie su orden.

1. Haga clic en **Set Columns** en la parte superior derecha del informe.
2. Cuando aparezca la ventana **Column Layout**, seleccione o deseleccione las columnas deseadas.



3. Haga clic y arrastre la columna deseada para cambiar su posición.
4. Haga clic en **Apply** para guardar la configuración.

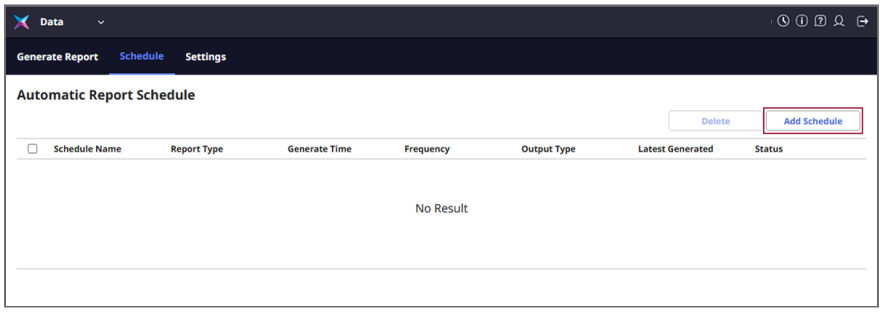
> **Información**
>
> - Haga clic en **Default Column** para restablecer el diseño de columnas.
> - Según el informe generado, las columnas que se puedan seleccionar o deseleccionar pueden variar.

Programación Automática de Reportes

Configure una programación para generar automáticamente **Custom Report** creados al establecer el período DYNAMIC.

Agregar programación automática

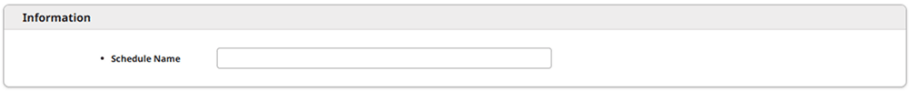
1. Haga clic en **Data** o seleccione **Data** en la lista de accesos directos en la parte superior izquierda de la pantalla en la página **Launcher**.
2. Haz clic en la pestaña **Schedule**.
3. Haga clic en **Add Schedule** en la parte superior derecha de la pantalla.



4. Cuando aparezca la pantalla **Add Automatic Report Schedule**, configure cada elemento.

Configuración de información

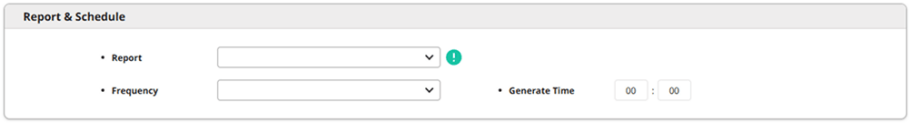
Configure la información básica de la programación de informes automáticos.



- **Schedule Name**: Ingrese el nombre de la programación.

Configuración de informes y programación

Configure la programación que se generará automáticamente para cada informe.

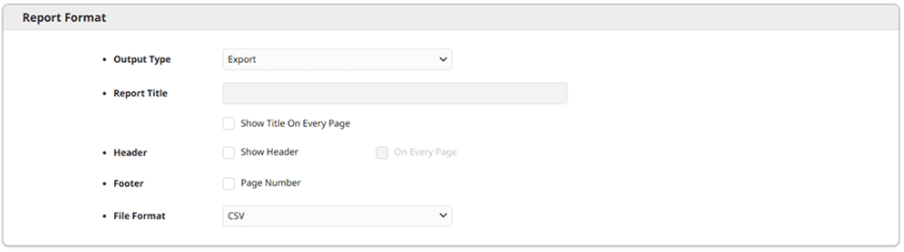


- **Report**: Seleccione un informe personalizado para generar automáticamente. Solo aparecerán los informes personalizados configurados con período DYNAMIC.
- **Frequency**: Configure la frecuencia para generar informes automáticamente.
- **Generate Time**: Configure la hora para generar informes automáticamente.

> **Información**
> Para obtener más información sobre cómo crear informes personalizados, consulte Generar Reporte.

Configuración del formato de informe

Configure el formato para cada informe.



- **Output Type**: Configure el método de generación automática de informes.

- **Report Title**: Seleccione **Show Title On Every Page** para mostrar el nombre del informe como título en cada página.
- **Header**: Si se selecciona **Show Header**, el encabezado se muestra cuando se crea el informe. Seleccione **On Every Page** para mostrar el encabezado en cada página.

> **Información**
> El encabezado puede variar según los informes.

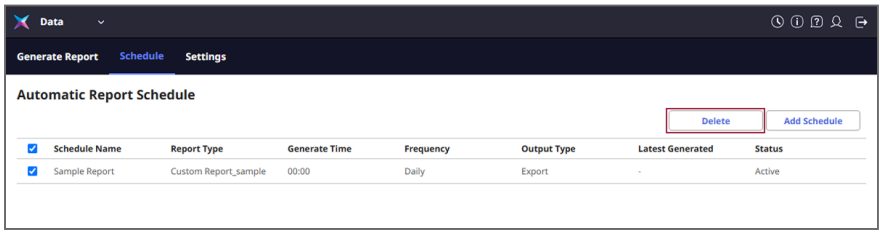
- **Footer**: Configure si se mostrarán números de página.
- **File Format**: Configure el formato de archivo para exportar informes.

3. Haga clic en **Apply** para guardar la configuración.

> **Información**
> Cuando todas las configuraciones estén completas, establezca la ruta para guardar el informe. Para obtener más información, consulte Ajustes.

Eliminar programación automática

1. Haga clic en **Data** o seleccione **Data** en la lista de accesos directos en la parte superior izquierda de la pantalla en la página **Launcher**.
2. Haz clic en la pestaña **Schedule**.
3. Haga clic en la casilla de verificación de la programación que desea eliminar de la lista de programación automática.

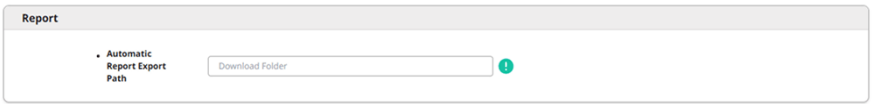


4. Haga clic en **Delete** en la parte superior derecha de la pantalla.

Ajustes

Configure la ruta donde se guardará el informe si ha configurado **Schedule**.

1. Haga clic en **Settings**.
2. Ingrese la ruta donde desea guardar el informe.



- **Automatic Report Export Path**: El informe se guardará en la ruta especificada; si no se ingresa ninguna ruta, se guardará automáticamente en la carpeta *Documents\BioStarX* de la PC del usuario.

3. Haga clic en **Apply** para guardar la configuración.

Tablero

El panel se puede personalizar para adaptarse a las preferencias individuales, lo que permite que cada usuario seleccione la información que desee, agregue widgets y configure y organice libremente los widgets.

> **Información**
>
> - Cada usuario puede configurar **Dashboard** de forma individual.
> - La información disponible en **Dashboard** puede variar según **Account Level**.

Agregar Widgets

El panel de **BioStar X** es una pantalla de monitoreo personalizable donde los usuarios pueden organizar libremente la información que deseen. Agrega distintos widgets para configurar la información clave del sistema de control de acceso según tu entorno de trabajo.

Los tipos de widgets disponibles son los siguientes.

- **Gráfico**: Visualiza los datos de eventos de acceso en gráficos de barras, líneas o pastel
- **Contador**: Muestra la cantidad de eventos por día o semana en números
- **Eventos en tiempo real**: Monitorea todos los eventos que ocurren en **BioStar X** en tiempo real
- **Monitoreo de acceso en tiempo real**: Muestra en tiempo real la información del usuario que se autentica correctamente en dispositivos específicos
- **Estado de uso del sistema**: Muestra en números el estado de registro de usuarios, dispositivos, puntos de acceso, etc.
- **Control de puertas**: Verifica el estado de los puntos de acceso seleccionados y contrólalos de forma remota
- **Texto**: Coloca texto personalizado, como anuncios o títulos de widgets

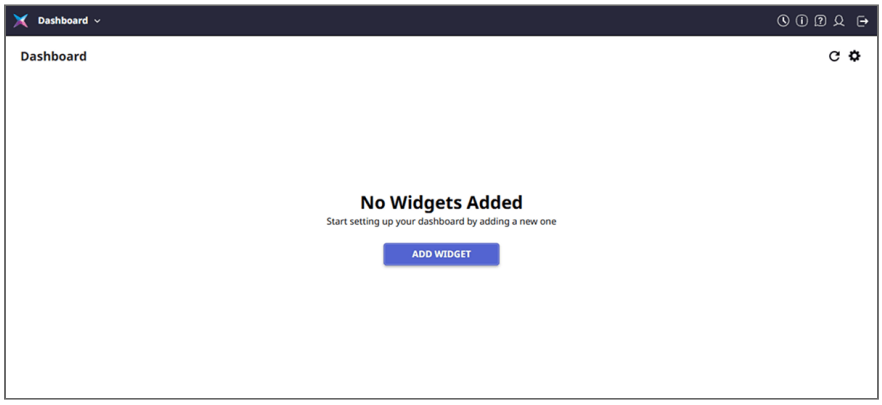
Los widgets colocados en el panel ofrecen las siguientes ventajas.

- **Configuración personalizada**: Selecciona solo la información necesaria para el trabajo y organízala en una sola pantalla
- **Monitoreo en tiempo real**: Verifica al instante los eventos de acceso y el estado del sistema
- **Visualización intuitiva**: Representa los datos mediante gráficos y contadores
- **Gestión eficiente**: Mejora la eficiencia del trabajo al integrar funciones de monitoreo y control

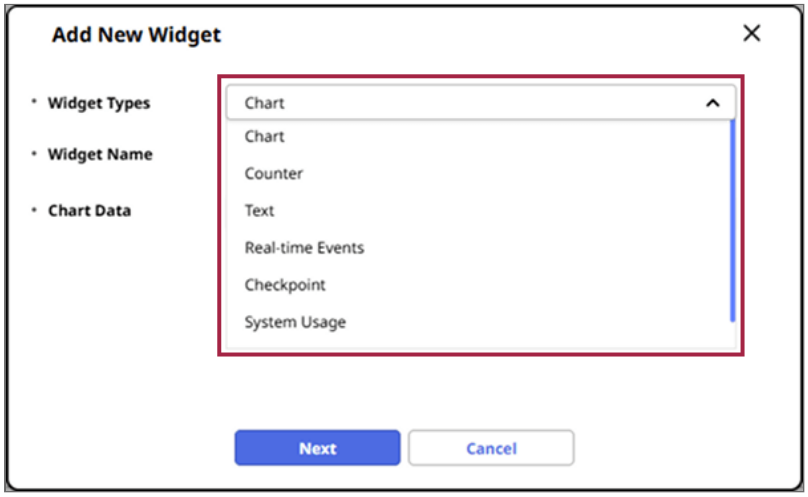
Agregar widgets

Agrega widgets en **Dashboard** para consultar la información que necesites.

1. Haz clic en **Dashboard** en la página **Launcher**.
2. Haga clic en **Add Widget**.



3. Cuando aparezca la ventana **Add New Widget**, selecciona el elemento deseado en **Widget Type** e ingresa o define los campos requeridos.

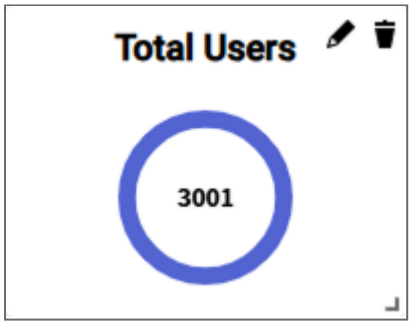


4. Completa la configuración del widget y haz clic en **Apply**.
5. Una vez creado el widget en el área de visualización, ajusta su tamaño o colócalo en la ubicación deseada.
6. Una vez que hayas completado todos los ajustes, haz clic en **Apply** en la esquina superior derecha de la pantalla.

> **Información**
>
> Si ya agregaste un widget, haz clic en el ícono ⚙ en la esquina superior derecha de la pantalla. Una vez que entres en el modo **Dashboard Settings**, haz clic en **Add Widget**.

Tipos de widgets

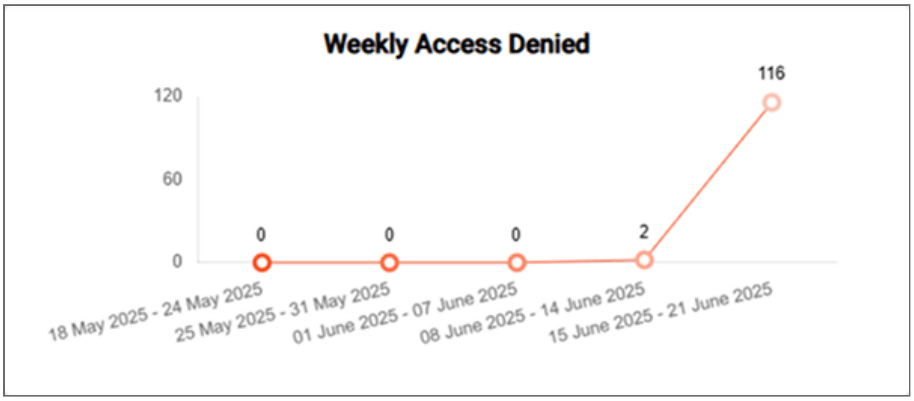
- El tamaño predeterminado varía según el widget y está optimizado para verse mejor en ese tamaño.
- Todos los widgets se pueden redimensionar arrastrando la esquina inferior derecha.



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

Gráfico

Al seleccionar los datos de gráfico deseados, se muestra en el gráfico la cantidad de eventos ocurridos.



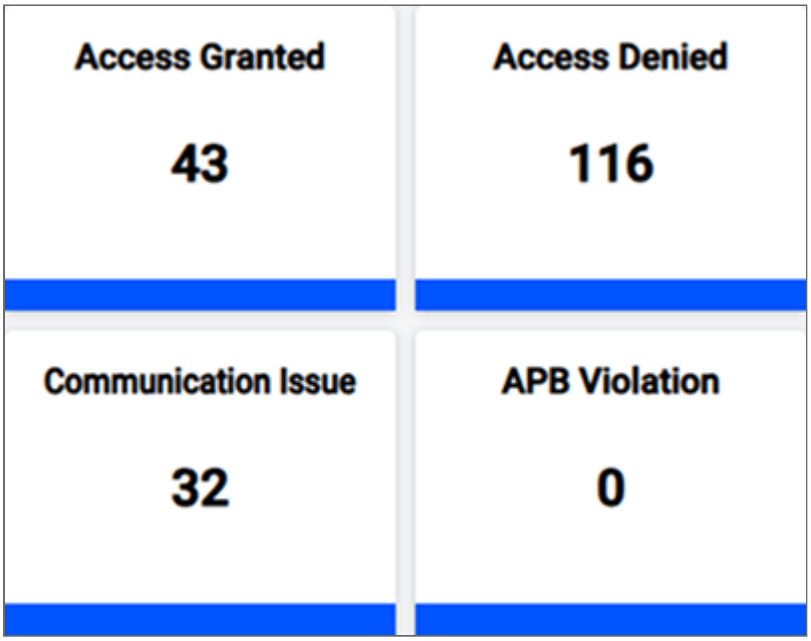
La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

- **Chart Data**: En la lista de eventos diarios o semanales, selecciona los datos de gráfico deseados.
  - **Daily Access Granted**, **Daily Access Denied**, **Daily Communication Issue**, **Daily APB Violation**, **Weekly Access Granted**, **Weekly Access Denied**, **Weekly Communication Issue**, **Weekly APB Violation**
- **Chart Type**: Selecciona el tipo deseado entre **Vertical Bar**, **Horizontal Bar**, **Line**, y **Pie**.
- **Color Schemes**: Selecciona el color deseado entre los 5 esquemas de color.

> **Información**
>
> Los gráficos que se muestran al seleccionar **Color Schemes** utilizan valores aleatorios para la vista previa; no son valores reales.

Contador

Al seleccionar los datos de contador deseados, se muestra como número la cantidad de eventos ocurridos.

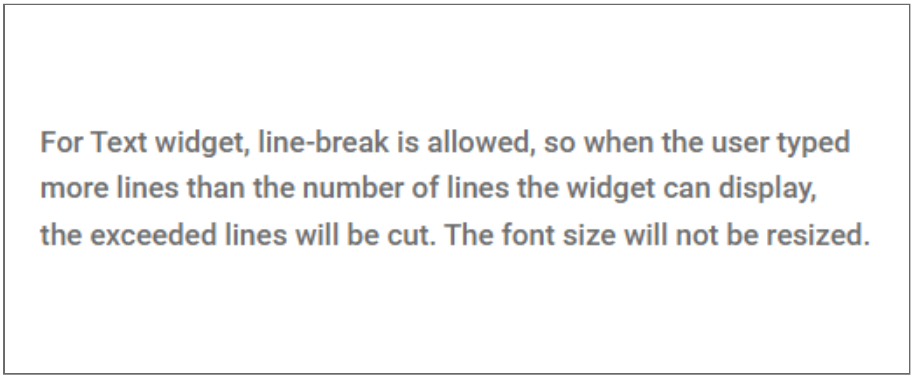


La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

- **Counter Data**: En la lista de eventos diarios o semanales, selecciona los datos de contador deseados.
  - **Daily Access Granted**, **Daily Access Denied**, **Daily Communication Issue**, **Daily APB Violation**, **Weekly Access Granted**, **Weekly Access Denied**, **Weekly Communication Issue**, **Weekly APB Violation**

Texto

Ingresa y coloca el texto deseado en el área de widgets de **Dashboard**. Después de crearlo, colócalo en la ubicación necesaria y úsalo como título de un widget o como aviso.

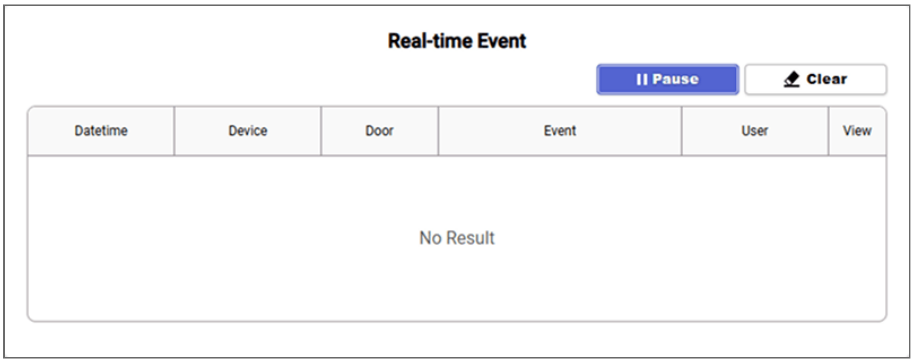


La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

> **Información**
> Si seleccionas la opción **Remove Background** al crear un widget **Text**, se aplicará transparencia al fondo.

Eventos en tiempo real

Muestra los eventos que ocurren en **BioStar X** en tiempo real. Verifica eventos filtrando eventos específicos, usuarios, puertas y dispositivos.



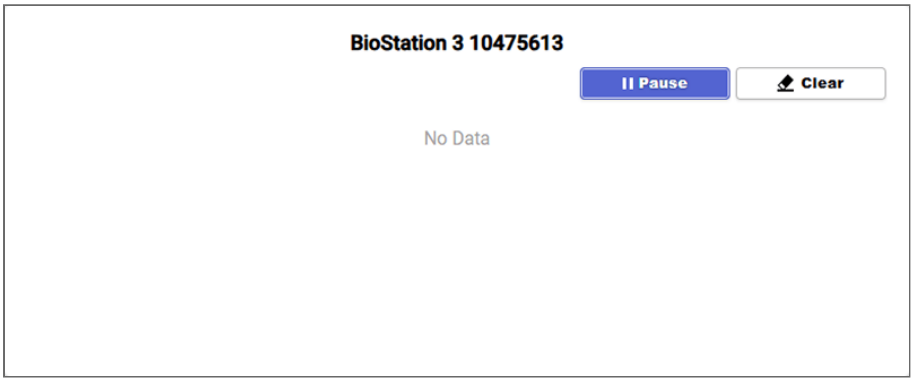
La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

- **Pause**: Pausar el evento en tiempo real.
- **Play**: Reanudar el evento en tiempo real que se detuvo.
- **Clear**: Se eliminará todo el registro capturado.

> **Información**
> Si navegas a otra página y regresas a **Dashboard**, la lista se borrará y los eventos se registrarán nuevamente.

Monitoreo de acceso en tiempo real

Selecciona un dispositivo y muestra la foto de perfil e información (**User**, **Date**, **Device**) del usuario que se autentique correctamente en tiempo real.



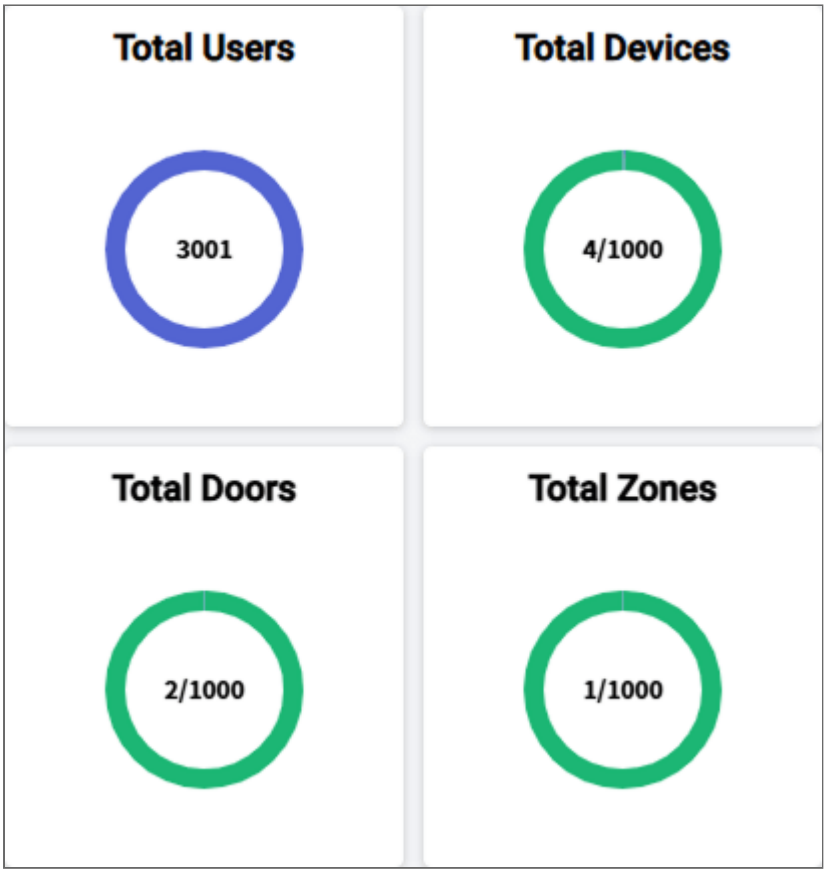
La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

- **Pause**: Pausar el punto de control.
- **Play**: Reanudar el punto de control que se pausó.
- **Clear**: Se eliminará todo el registro capturado.

> **Información**
> Se registran hasta 5 personas en **Checkpoint**.

Estado de uso del sistema

Los distintos estados de uso de BioStar X se muestran en números.



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

Los **System Usage** que se pueden mostrar son los siguientes:

- **Total Users**, **Total Cards**, **Total Fingerprints**, **Total Faces**, **Total Faces**, **Total QR/Barcode**, **Total Mobile Access**, **Total Devices**, **Total Doors**, **Total Advanced ACs**, **Total Access Groups**, **Total User Groups**, **Total Device Groups**, **IR Face**

Control de puertas

Selecciona una puerta para verificar y controlar su estado.



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

Los siguientes elementos se pueden controlar con los botones **Actions**:

- **Open**, **Normalize**, **Manual Lock**, **Manual Unlock**, **Clear Alarm**, **Clear APB**

Información

El nombre del widget **Door Control** se asigna automáticamente al nombre de la puerta y no puede modificarse.

Definir intervalo de actualización de datos del widget

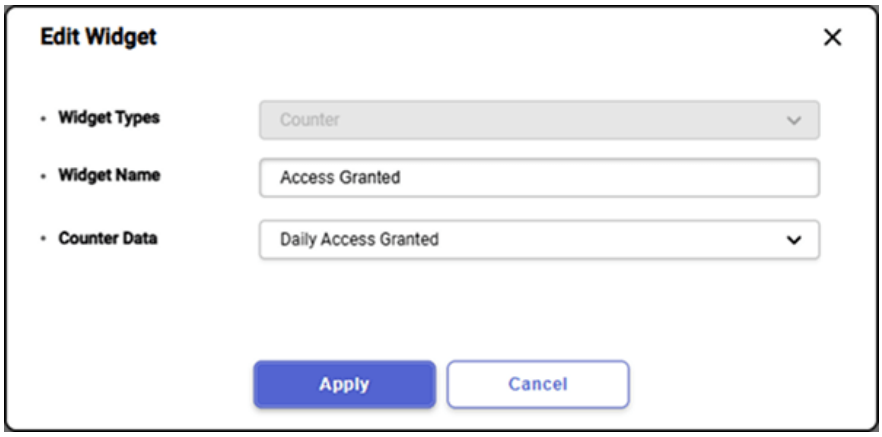
Puede configurar el intervalo de actualización de datos de los widgets agregados al panel.

1. Haz clic en **Dashboard** en la página **Launcher**.
2. Haz clic en el icono ⚙ en la esquina superior derecha de la pantalla.
3. Una vez que ingrese al modo **Dashboard Settings**, configure **Auto Refresh Interval** en la configuración general en la parte inferior de la pantalla.

Editar Widget

Edita los widgets agregados al tablero.

1. Haz clic en **Dashboard** en la página **Launcher**.
2. Haz clic en el icono ⚙ en la esquina superior derecha de la pantalla.
3. Después de ingresar al modo **Dashboard Settings**, haz clic en ✎ en la esquina superior derecha del **widget** que deseas editar.
4. Cuando aparezca la ventana **Edit Widget**, modifica los elementos deseados.



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

5. Haz clic en **Apply** después de completar las modificaciones.
6. Haz clic en **Apply** en la esquina superior derecha de la pantalla **Dashboard Settings**.

Confirma que los cambios realizados en el panel se hayan aplicado.

Información

- El **Widget Types** no puede cambiarse en **Edit Widget**.
- **Text**, **System Usage** y **Door Control** que usan un nombre específico no pueden modificar el **Widget Name**.

Eliminar Widget

Elimina los widgets añadidos al panel.

1. Haz clic en **Dashboard** en la página **Launcher**.
2. Haz clic en el icono ⚙ en la esquina superior derecha de la pantalla.
3. Al entrar en el modo **Dashboard Settings**, haz clic en 🗑 en la esquina superior derecha del **Widget** que deseas eliminar.
4. Revisa la ventana emergente de confirmación de eliminación y haz clic en **Yes**.



5. Haz clic en **Apply** en la esquina superior derecha de la pantalla **Dashboard Settings**.

Confirma que los cambios realizados en el panel se hayan aplicado.

Ajustes

Esta guía describe las distintas funciones que se pueden configurar en la página **Settings** de **BioStar X**. Agregue dispositivos y explore diversas opciones para personalizar el entorno de usuario, como permisos, idioma, fecha y hora y administración de tarjetas de acceso.

Haga clic en **Settings** en la página **Launcher** o seleccione **Settings** en la lista de accesos directos en la esquina superior izquierda de la pantalla.

> **Información**
> Las funciones que se pueden configurar pueden variar según los permisos del usuario. Algunas funciones solo pueden ser utilizadas por usuarios con permiso de administrador. Para obtener más información sobre los menús accesibles en cada nivel de permiso de usuario, consulte Configurar Permisos de Usuario.

Administrar Dispositivos

Esta guía describe cómo gestionar la adición, eliminación y modificación de dispositivos. Importe la información de usuario registrada en el dispositivo al servidor **BioStar X** o actualice el firmware de forma remota.

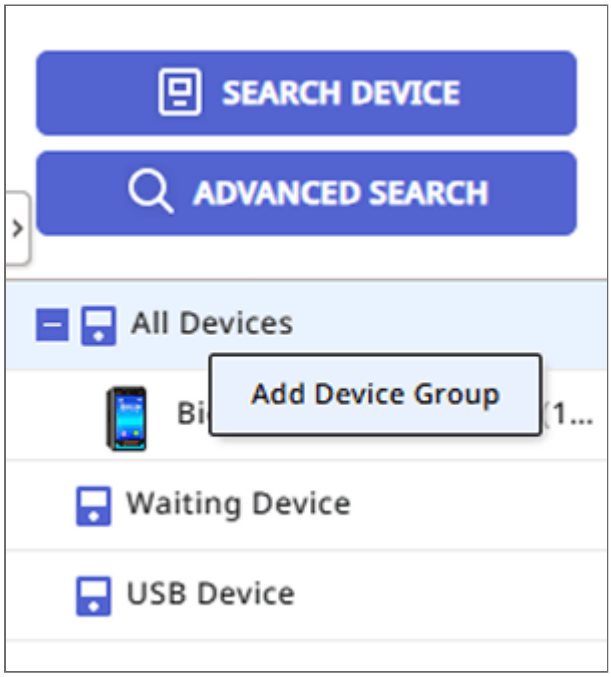
Gestionar Grupos de Dispositivos

Esta guía describe la función de grupos de dispositivos para gestionar varios dispositivos de manera eficiente. Este documento ofrece orientación sobre la función de grupos de dispositivos que permite gestionar varios dispositivos de forma eficiente.

> **Consejo**
> Nombrar los grupos de dispositivos según la ubicación o el propósito de los dispositivos facilita la gestión. Por ejemplo, los grupos pueden designarse como "Entrada del primer piso", "Oficina del segundo piso", "Sala de conferencias", etc.

Crear un grupo de dispositivos

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haga clic con el botón derecho en **All Devices** en la lista de dispositivos.

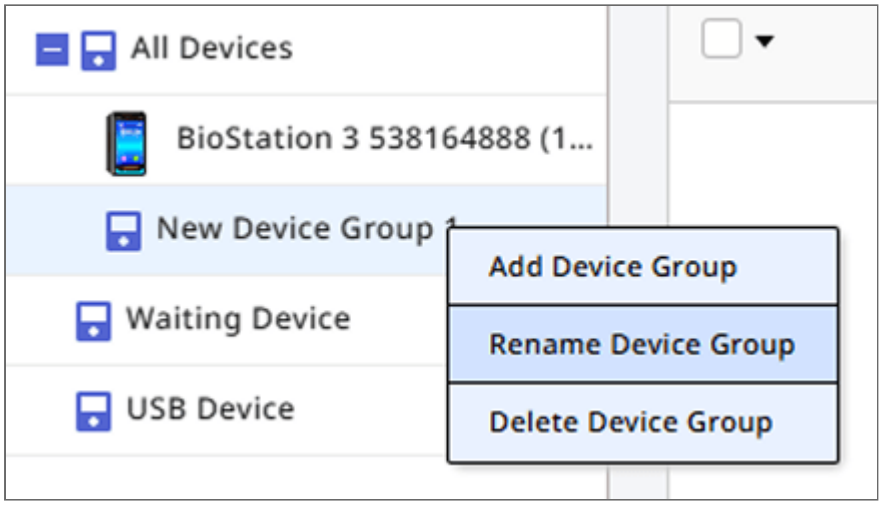


4. Haga clic en **Add Device Group** en el menú emergente.
5. Introduzca el nombre de grupo deseado.

> **Información**
>
> - Puede crear grupos de dispositivos con hasta 8 niveles de subgrupos.
> - Los nombres de los grupos de dispositivos pueden tener hasta 48 caracteres.
> - Al seleccionar un grupo de dispositivos de la lista de dispositivos, aparecerán solo los dispositivos que pertenecen a ese grupo.

Modificar el nombre de un grupo de dispositivos

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. En la sublista de **All Devices**, seleccione el grupo de dispositivos cuyo nombre desea cambiar y haga clic con el botón derecho.

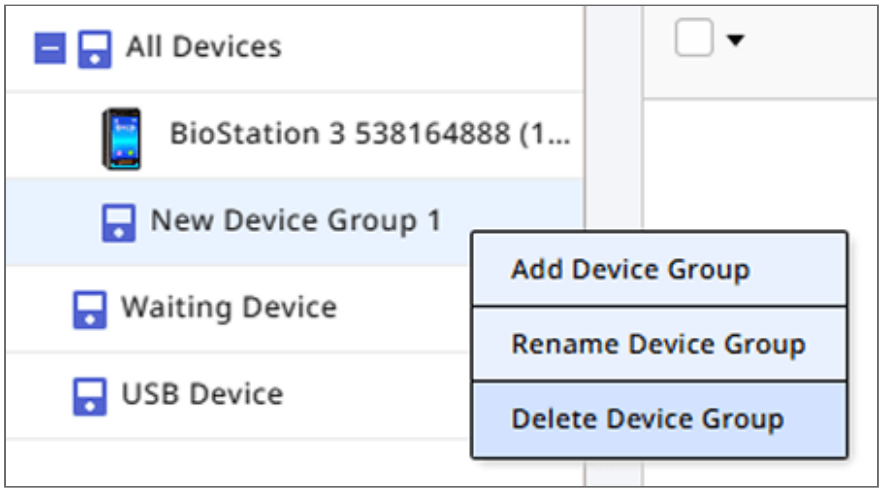


4. Haga clic en **Rename Device Group** en el menú emergente.
5. Introduzca el nuevo nombre para el grupo.

> **Información**
> Los nombres de los grupos de dispositivos pueden tener hasta 48 caracteres.

Eliminar un grupo de dispositivos

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. En la sublista de **All Devices**, seleccione el grupo de dispositivos que desea eliminar y haga clic con el botón derecho.



4. Haga clic en **Delete Device Group** en el menú emergente.

> **Precaución**
> Eliminar un grupo de dispositivos quitará todos los dispositivos que pertenecen a ese grupo.

Registrar dispositivo

Esta guía explica cómo registrar un dispositivo en **BioStar X**. Registrar un dispositivo permite que **BioStar X** supervise y administre el estado de ese dispositivo. Asegúrese de que el dispositivo esté correctamente conectado antes de buscarlo. Es conveniente conocer de antemano la ubicación, el ID, la dirección IP y otros detalles al agregar varios dispositivos a la vez.

Información

- Al registrar un nuevo dispositivo, cambie el valor de la clave del dispositivo por el valor de la clave de cifrado de datos del servidor. Todos los datos de usuario del dispositivo se eliminarán durante la conversión de clave.
- Haga clic en **Delete Data & Sync Device** para eliminar toda la información de configuración y los datos de usuario almacenados en el dispositivo y volver a enviarlos. Encuentre la opción **Delete Data & Sync Device** seleccionando el dispositivo en la lista y haciendo clic en el botón [•••].
- Haga clic con el botón derecho en el nombre del grupo **Waiting Device** y luego haga clic en **Add All Waiting Devices** para registrar todos los dispositivos del grupo. Haga clic con el botón derecho en el nombre del dispositivo y luego haga clic en **Add Waiting Device** para registrarlo individualmente.
- Si el tipo de ID de usuario en **BioStar X** difiere del del dispositivo, cambie la configuración del dispositivo según la configuración de ID de usuario de **BioStar X**.
- Si el tipo de ID de usuario en **BioStar X** está configurado como alfanumérico, es posible que algunos dispositivos no se puedan usar o tengan restricciones. Para obtener más información, consulte Configuración Detallada del Servidor.
- Para registrar un dispositivo y configurar sus detalles, consulte Configuración del Dispositivo.
- Hasta 1,000 dispositivos pueden conectarse a través de Ethernet (TCP/IP).
- Obtenga una licencia **Device Manager** o superior para registrar dispositivos. Para obtener más información sobre la política de licencias, consulte Política de Licencias.

Antes de comenzar

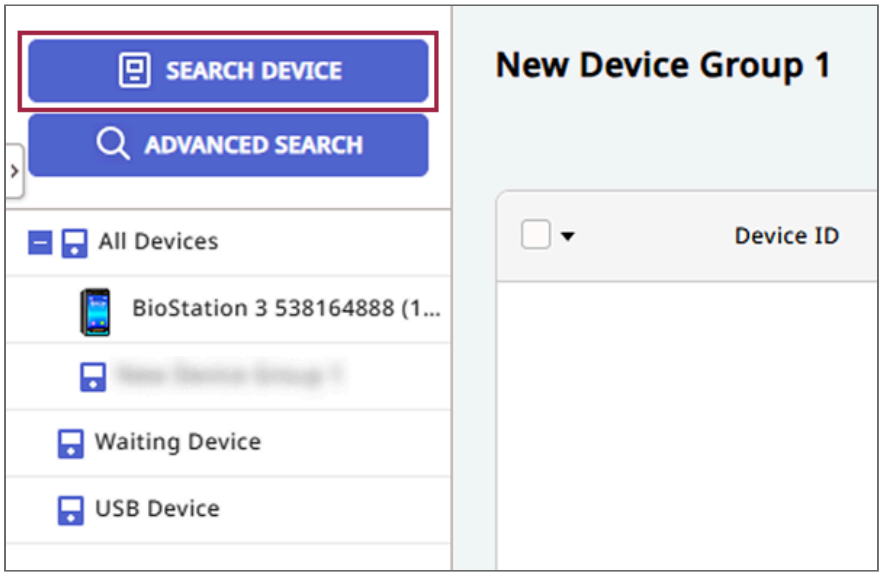
Revise lo siguiente antes de registrar el dispositivo.

- Configure los niveles de acceso, grupos de acceso y niveles de piso para el control de acceso. Para obtener más información, consulte Configuración de Control de Acceso.
- Cree un grupo para administrar los dispositivos de forma eficiente. Para obtener más información, consulte Gestionar Grupos de Dispositivos.

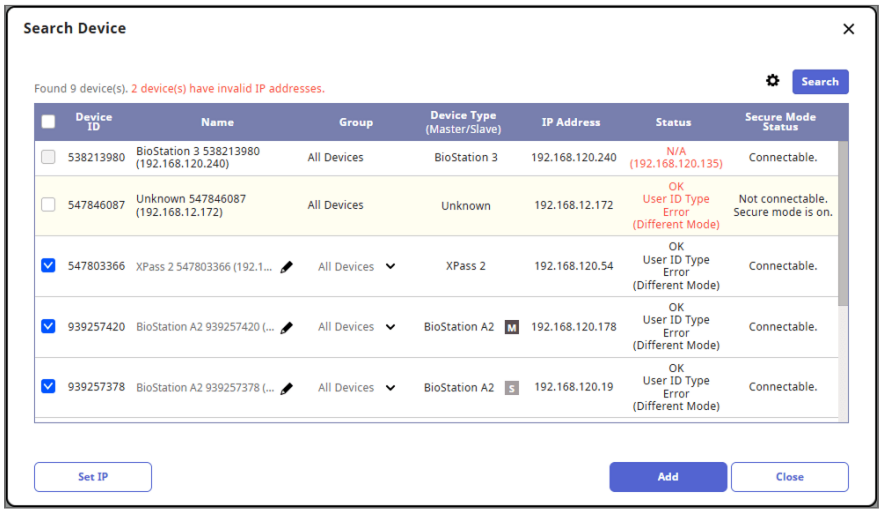
Registro rápido

Los dispositivos en la misma red que **BioStar X** se pueden buscar y registrar automáticamente.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haga clic en **Search Device** en la lista de dispositivos.

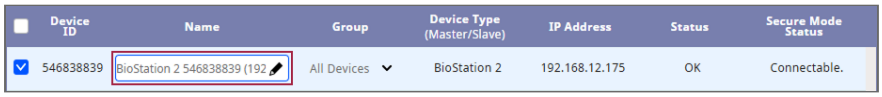


4. Cuando aparezca la ventana **Search Device**, se mostrará una lista de todos los dispositivos que se pueden registrar. Si el dispositivo deseado no está en la lista, haga clic en **Search** en la esquina superior derecha.

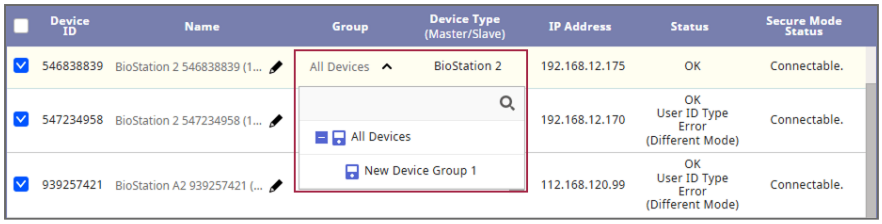


5. Seleccione en la lista los dispositivos que desee registrar o desmarque los que no quiera registrar.

6. Haga clic en ✎ en la columna **Name** para cambiar el nombre del dispositivo que se registrará y realice el cambio.

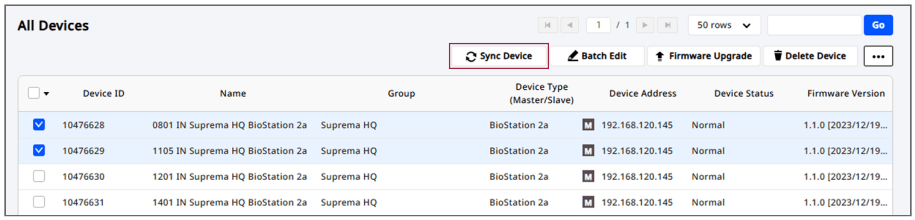


7. Seleccione el grupo del dispositivo que se registrará en la columna **Group**.



8. Cuando haya terminado de configurar todos los dispositivos seleccionados, haga clic en **Add**.

Los dispositivos añadidos aparecerán en la lista de dispositivos. Seleccione el dispositivo añadido y haga clic en **Sync Device**.

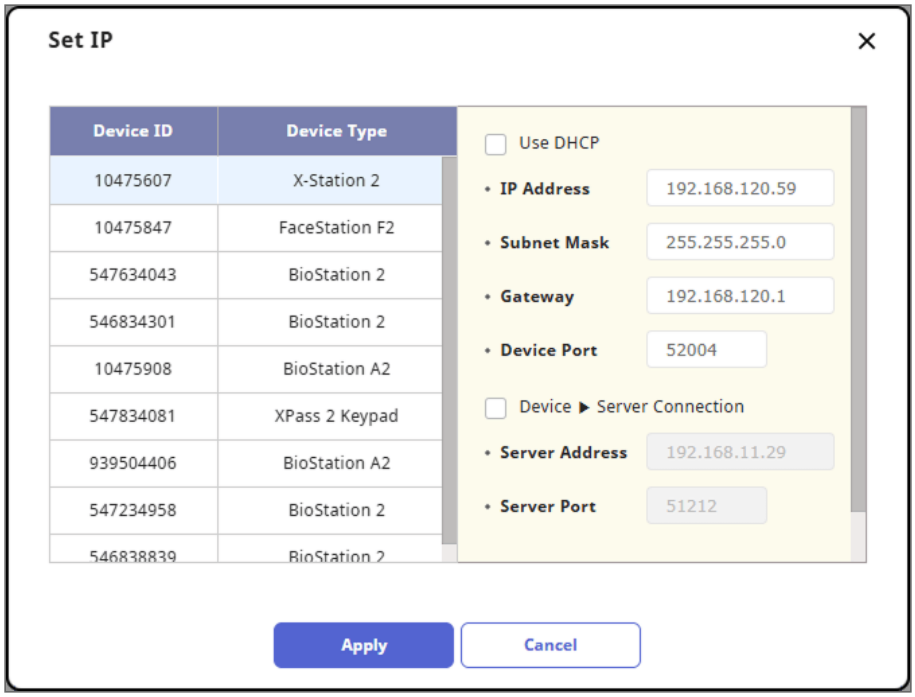


Información

Modifique los dispositivos cuya dirección IP no esté disponible o deba cambiarse haciendo clic en **Set IP**. Para obtener más información, consulte Configuración de dirección IP.

Configuración de dirección IP

Cambie la dirección IP del dispositivo que se registrará. Haga clic en **Set IP** en la parte inferior izquierda de la ventana **Search Device**. Cuando aparezca la ventana **Set IP**, seleccione el dispositivo al que desea cambiar la dirección IP.



- **Use DHCP**: Seleccione esta opción para que el dispositivo obtenga automáticamente una dirección IP mediante DHCP. Al seleccionar esta opción, es posible que la dirección IP cambie cada vez que el dispositivo se conecte a la red.

  Para introducir manualmente la dirección IP, la máscara de subred, la puerta de enlace, etc., desmarque esta opción.

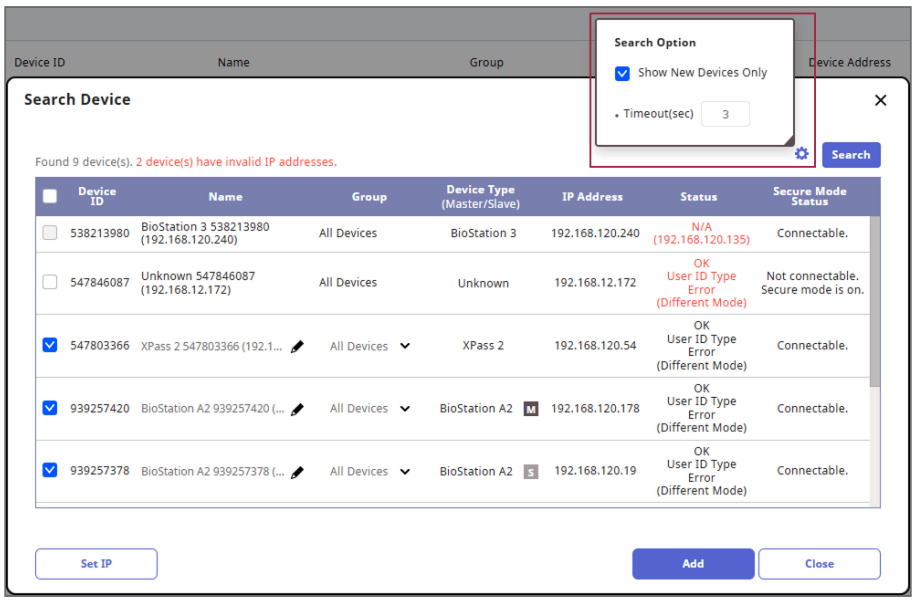
- **Device ▸ Server Connection**: Seleccione esta opción para configurar el dispositivo para que se conecte al servidor de **BioStar X**. Deberá introducir la dirección IP y el número de puerto del servidor donde está instalado **BioStar X**.

Información

Después de completar toda la configuración de IP y guardar los cambios, haga clic en **Apply**. Para cancelar los cambios, haga clic en **Cancel**.

Opciones de búsqueda de dispositivos

Configure las opciones de búsqueda de dispositivos haciendo clic en ⚙ en la esquina superior derecha de la ventana **Search Device**.

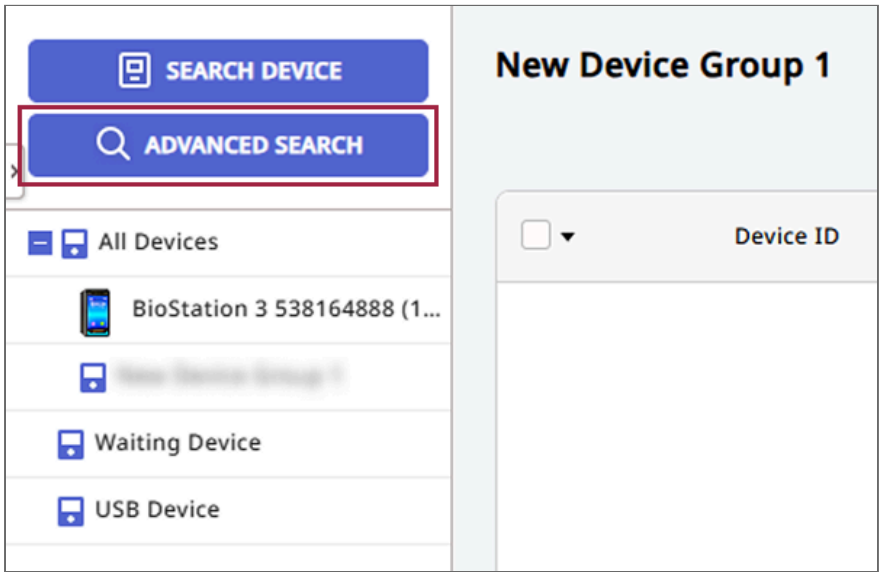


- **Show New Devices Only**: Seleccione esta opción para mostrar solo los dispositivos recién detectados en la lista de búsqueda.
- **Timeout(sec)**: Establezca el tiempo deseado para excluir de la lista de búsqueda los dispositivos que no respondan durante un periodo determinado. Este valor puede configurarse en segundos, con un valor predeterminado de 3 segundos.

Búsqueda avanzada

Puede especificar la dirección IP y el número de puerto de un dispositivo específico para registrarlo.

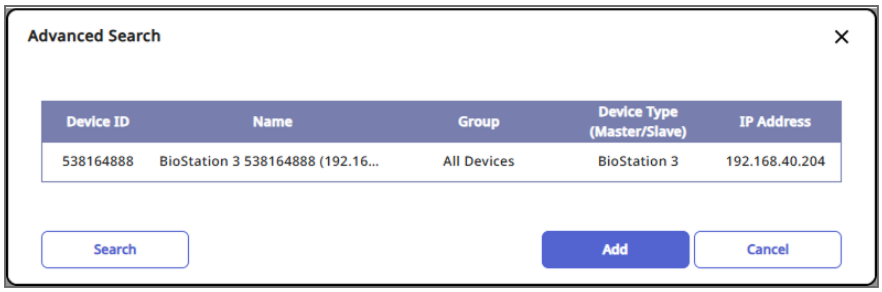
1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haga clic en **ADVANCED SEARCH** en la lista de dispositivos.



4. Cuando aparezca la ventana **ADVANCED SEARCH**, introduzca la dirección IP y el número de puerto del dispositivo que se va a registrar.



5. Haga clic en **Search** para mostrar los dispositivos que coincidan con los criterios introducidos.



6. Para registrar el dispositivo, haga clic en **Add**.

Los dispositivos añadidos aparecerán en la lista de dispositivos. Seleccione el dispositivo añadido y haga clic en **Sync Device**.

Registrar dispositivos en espera

Los dispositivos con la opción **Device → Server** configurada tratan de conectarse al servidor **BioStar X** mediante la dirección IP y el puerto del servidor. **BioStar X** no registra automáticamente estos dispositivos en la lista de dispositivos activos. Estos dispositivos aparecen en el grupo **Waiting Device**, y un administrador autorizado debe registrarlos manualmente.

1. En la opción **Device → Server** del dispositivo, establezca la dirección IP y el número de puerto de **BioStar X**.
2. Haz clic en **Settings** en la página **Launcher**.
3. Haz clic en **Device → Device** en la barra lateral izquierda.
4. Marque los dispositivos que aparecen en el grupo **Waiting Device**.



5. Haga clic con el botón derecho en el nombre del dispositivo en el grupo **Waiting Device** para registrarlo individualmente.

Para registrar todos los dispositivos en el grupo **Waiting Device**, haga clic con el botón derecho en el grupo **Waiting Device**.



6. En el menú emergente, haga clic en **Add Waiting Device**(dispositivo individual) o **Add All Waiting Devices**(todos los dispositivos).

Después de que un administrador registre un dispositivo en el grupo **Waiting Device**, el dispositivo pasa a la lista **All Devices**.

Información

- Configure la opción **Device** → **Server** del dispositivo en **SETTINGS** → **NETWORK** → **Server**. Las rutas de menú pueden variar según el dispositivo.
- Configure este ajuste también en **BioStar X** mediante **Set IP** → **Device** ▸ **Server Connection** (Configuración de dirección IP).
- **BioStar X** no sincroniza los dispositivos que permanecen en el grupo **Waiting Device**. El sistema transfiere los datos de usuario, los niveles de acceso, los grupos de acceso y los ajustes del dispositivo solo después de registrar el dispositivo y sincronizarlo.

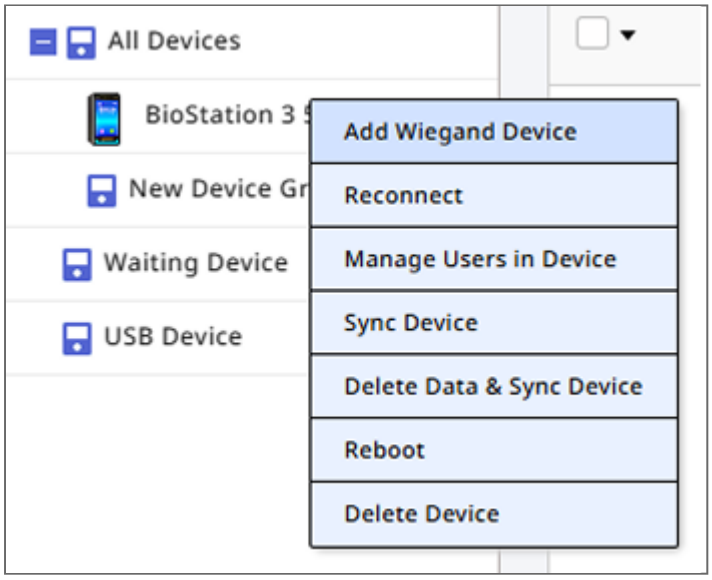
Registrar Credenciales Wiegand

Esta guía describe cómo agregar un dispositivo Wiegand al dispositivo maestro o esclavo registrado.

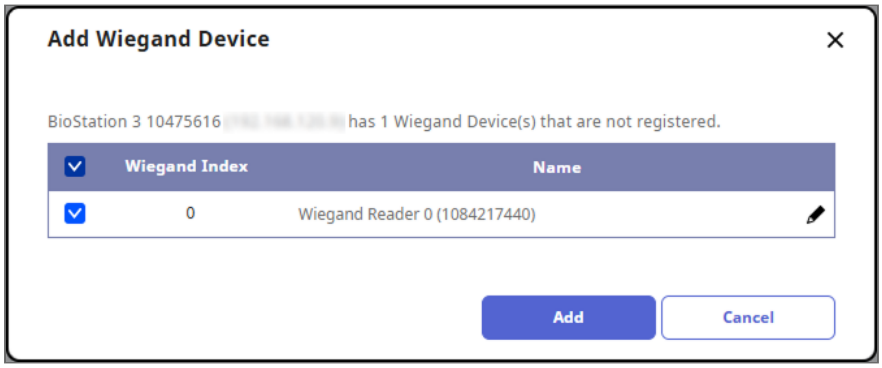
Información

- **마스터(Master) 장치**: RS-485로 연결한 장치 중 컨트롤러 역할을 수행하는 장치입니다. 슬레이브 장치를 주기적으로 모니터링하여 데이터를 처리합니다. 호스트(Host) 장치라고도 부릅니다.
- **슬레이브(Slave) 장치**: RS-485로 연결한 장치 중 리더 또는 입출력 기능만 수행하는 장치입니다. 사용자 정보를 갖고 있지 않으며 마스터 장치에 의해 제어됩니다.
- **Wiegand**: Wiegand는 두 개의 신호선(DATA0, DATA1)을 사용하여 데이터를 전송하는 통신 방식입니다. 주로 출입 통제 시스템에서 리더(Reader)와 컨트롤러 간의 통신에 사용되며, 간단한 구조와 낮은 비용으로 구현할 수 있습니다. 다만, 전송 거리가 짧고 데이터 전송 속도가 느린 한계가 있습니다.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haz clic con el botón derecho en el dispositivo maestro o esclavo en la lista **All Devices**.



4. Haz clic en **Add Wiegand Device** en el menú emergente.
5. Cuando aparezca la lista de dispositivos Wiegand conectados al dispositivo maestro, selecciona el dispositivo que deseas registrar.



6. Haz clic en **Add**.
7. Cuando aparezca el mensaje de confirmación del registro del dispositivo, haz clic en **Apply**.

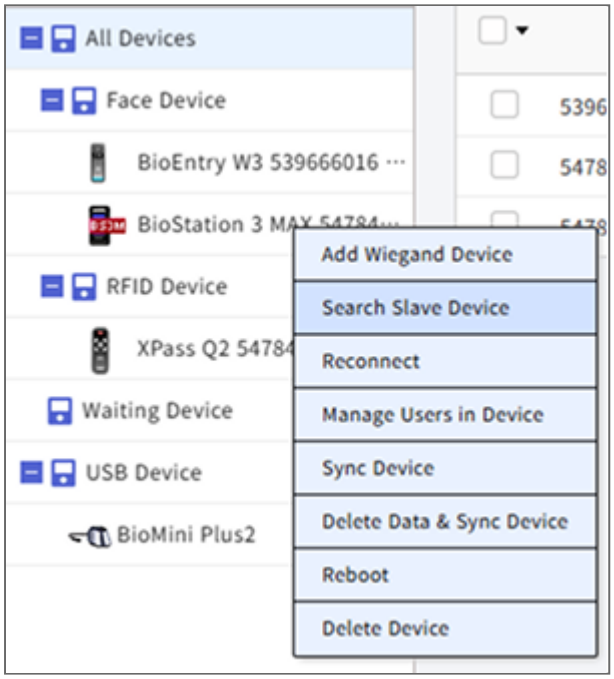
El dispositivo Wiegand registrado aparecerá debajo del dispositivo seleccionado.



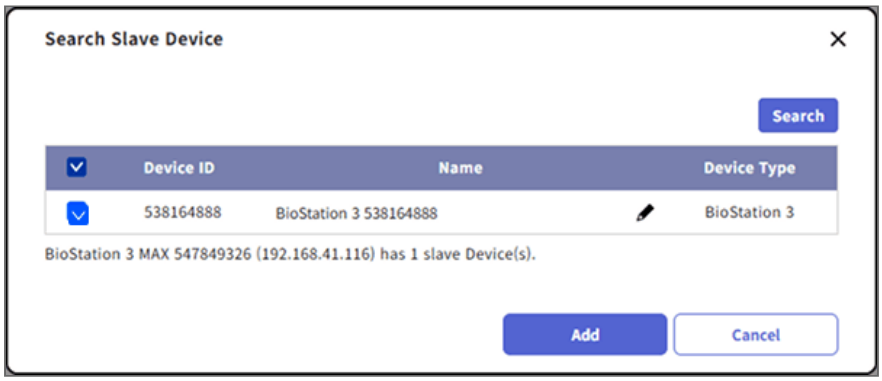
Registrar Esclavo

Amplía fácilmente la red del sistema de control de acceso añadiendo un dispositivo esclavo al dispositivo maestro registrado. Los dispositivos maestro y esclavo pueden conectarse mediante comunicación RS-485. Además de los dispositivos, también pueden conectarse y utilizarse dispositivos complementarios como Secure I/O 2.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haz clic con el botón derecho en el dispositivo maestro o esclavo en la lista **All Devices**.

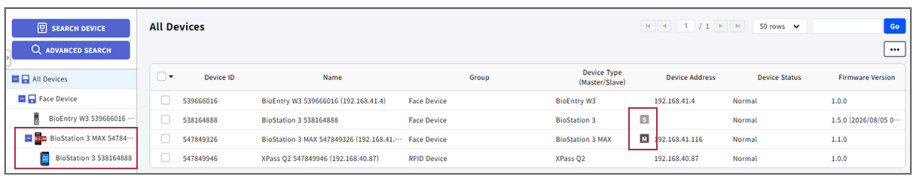


4. Haz clic en **Search Slave Device** en el menú emergente.
5. Cuando aparezca la lista de dispositivos esclavos conectados al dispositivo maestro, selecciona el dispositivo que se va a registrar. Si el dispositivo deseado no aparece en la lista, haz clic en **Search** en la esquina superior derecha.



6. Haz clic en **Add**.
7. Cuando aparezca el mensaje de confirmación del registro del dispositivo, haz clic en **Ok**.

El dispositivo esclavo registrado aparecerá debajo del dispositivo seleccionado. En la lista de dispositivos, el maestro muestra el icono y el esclavo muestra el icono .



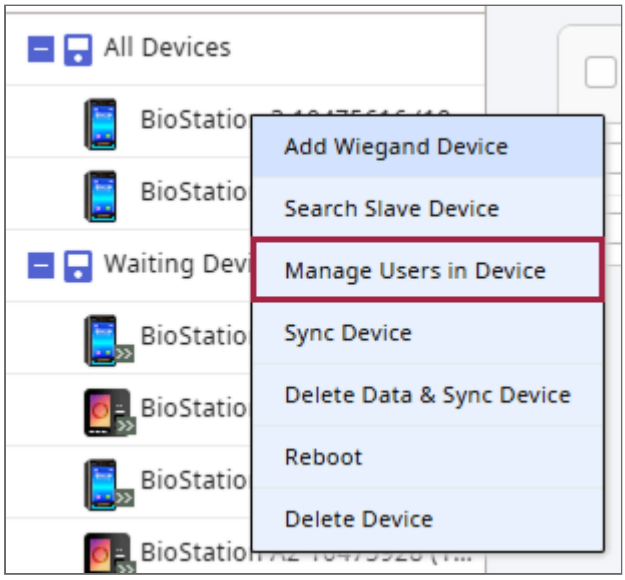
Información

- No es posible añadir un dispositivo de autenticación facial como esclavo cuando el dispositivo maestro es de autenticación por huella digital.
- No es posible añadir un dispositivo de autenticación facial como esclavo si el dispositivo maestro es de autenticación facial y ya se añadió otro dispositivo esclavo.
- Solo se puede añadir un dispositivo de autenticación facial como esclavo cuando el dispositivo maestro es de autenticación facial.
- Cuando el dispositivo maestro es de autenticación facial, se puede conectar además un Secure I/O 2 y un DM-20.
- El número máximo de dispositivos esclavos que se pueden conectar varía según el método de autenticación, el número de usuarios y el número de dispositivos. Ten en cuenta también que la cantidad de dispositivos esclavos afecta el rendimiento de autenticación.

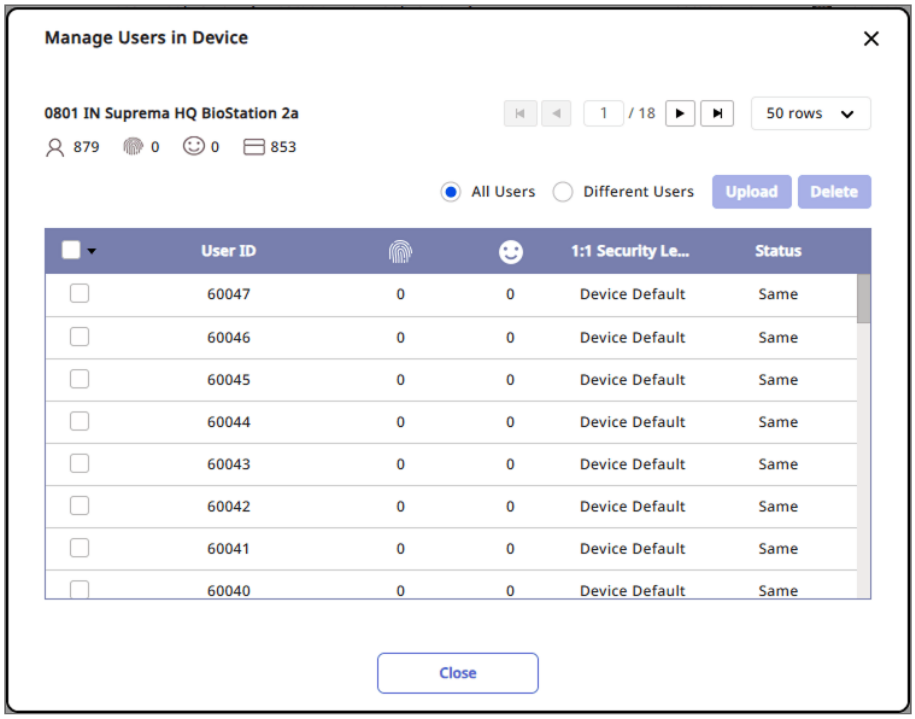
Administrar Usuarios Registrados en el Dispositivo

Comprueba la cantidad de usuarios, huellas, rostros y tarjetas almacenados en el dispositivo. Compara la información de los usuarios no registrados en **BioStar X** con la información de los usuarios registrados y envíala o elimínala en el servidor de **BioStar X**.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Selecciona el dispositivo en la lista **All Devices** y haz clic con el botón derecho.
4. Haz clic en **Manage Users in Device** en el menú emergente.



Cuando aparezca la ventana **Manage Users in Device**, compara la información de usuario registrada en el dispositivo con la información de usuario registrada en **BioStar X**.



Consulta los valores que aparecen en la columna **Status** para decidir si eliminas la información de usuario del dispositivo o la envías al servidor de **BioStar X**. Los valores de la columna **Status** son los siguientes:

- **Same**: Usuario con la misma información registrada en el servidor de **BioStar X**
- **Different**: Usuario con información diferente de la registrada en el servidor de **BioStar X**
- **New User**: Usuario de **BioStar X** que no está almacenado en el servidor

Selecciona al usuario y haz clic en el botón **Delete** para eliminar su información del dispositivo. Haz clic en el botón **Upload** para enviar la información de usuario al servidor de **BioStar X**.

> **Información**
>
> - La función **Manage Users in Device** solo se puede usar con un dispositivo seleccionado.
> - Al hacer clic en **Upload**, si **BioStar X** ya tiene un usuario con el mismo ID, el sistema lo actualiza con la información del dispositivo.
> - La información de usuario eliminada se quita solo del dispositivo y se conserva en el servidor de **BioStar X**.
> - Para obtener más información sobre la configuración del dispositivo, consulta Configuración del Dispositivo.

Actualizar Firmware

Los dispositivos conectados a **BioStar X** pueden actualizar su firmware fácilmente sin conexiones ni operaciones adicionales. Mantener el firmware del dispositivo actualizado resuelve vulnerabilidades de seguridad y permite acceder a nuevas funciones.

Antes de comenzar

Antes de actualizar el firmware del dispositivo, prepare la nueva versión del archivo de firmware. Guarde el archivo de firmware descargado en la ruta siguiente y extráigalo. Cree una nueva carpeta si la carpeta *firmware* no existe.

> *C:\Program Files\BioStar X\firmware*

Información

Busque el nombre del modelo de su dispositivo en el Centro de descargas de Suprema para descargar la última versión del archivo de firmware.

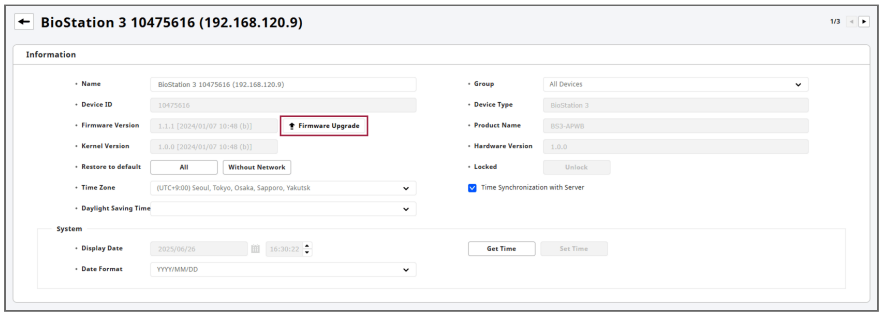
Actualización de firmware

Precaución

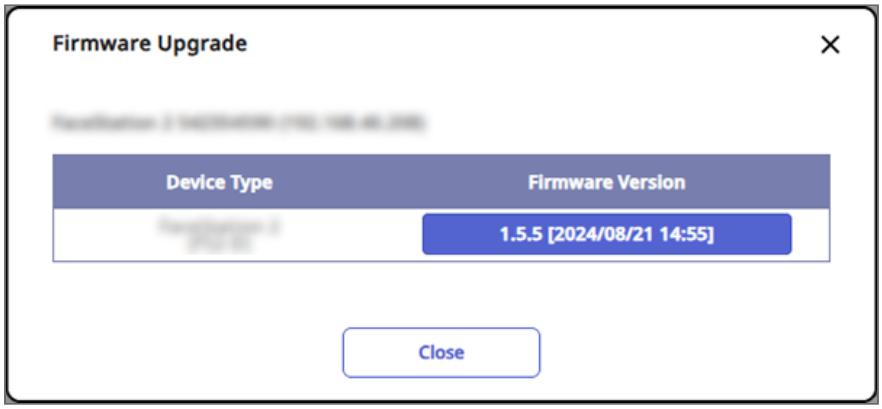
- Antes de actualizar el firmware, asegúrese de que el dispositivo tenga alimentación y conectividad de red. En particular, asegúrese de que la alimentación no se interrumpa durante la actualización.
- Según el tipo y el modo del dispositivo, puede tardar hasta 1 hora o más. Además, no se puede usar el dispositivo durante la actualización.
- No apague el dispositivo durante la actualización del firmware. Cuando finalice la actualización, el dispositivo se reinicia automáticamente.

Actualizar firmware para un solo dispositivo

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haga clic en el dispositivo que desea actualizar en la lista de dispositivos.
4. En la pantalla de detalles del dispositivo, en la sección **Information**, haga clic en **Firmware Upgrade**.



5. Cuando aparezca la ventana **Firmware Upgrade**, haga clic en la versión de firmware.

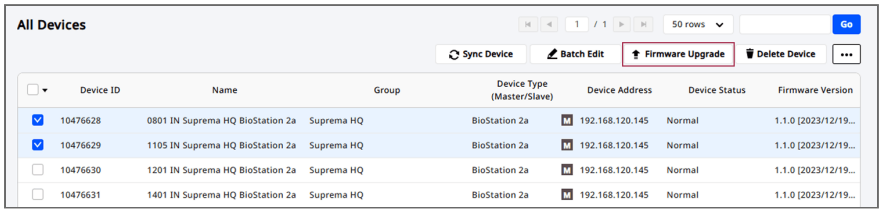


6. Cuando aparezca la ventana del mensaje de advertencia, haga clic en **Continue**.

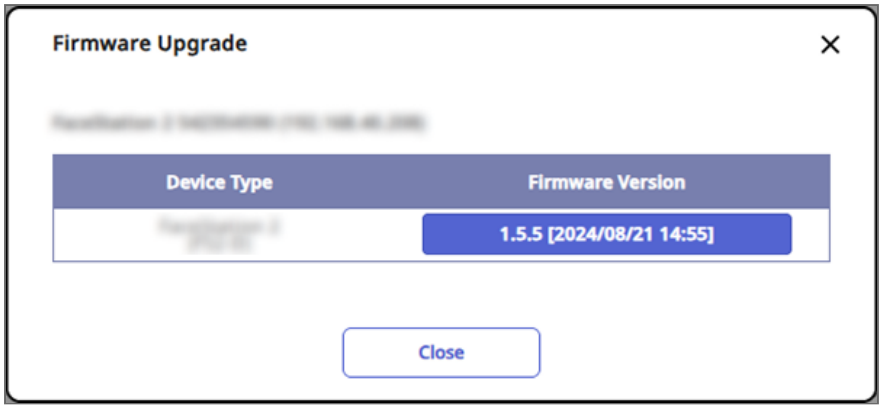
Esto inicia la actualización de firmware del dispositivo.

Actualizar firmware para varios dispositivos

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Seleccione la casilla situada completamente a la izquierda de los dispositivos que desea actualizar en la lista de dispositivos. Puede seleccionar varios dispositivos.
4. Haga clic en **Firmware Upgrade** en la esquina superior derecha de la lista de dispositivos.



5. Cuando aparezca la ventana **Firmware Upgrade**, haga clic en la versión de firmware.



6. Cuando aparezca la ventana del mensaje de advertencia, haga clic en **Continue**.

Esto inicia la actualización de firmware de los dispositivos seleccionados.

> **Información**
>
> - El botón **Firmware Upgrade** se activa solo después de seleccionar un dispositivo de la lista de dispositivos.
> - Los dispositivos con el mismo modo RS-485 pueden actualizarse simultáneamente en grupos. Por ejemplo, los dispositivos maestros pueden actualizar varios dispositivos maestros a la vez, y los dispositivos esclavos pueden actualizar varios dispositivos esclavos a la vez.
> - Los dispositivos maestros o los esclavos sin maestro pueden actualizarse simultáneamente en grupos.
> - Los dispositivos esclavos conectados al mismo dispositivo maestro no pueden actualizarse simultáneamente.

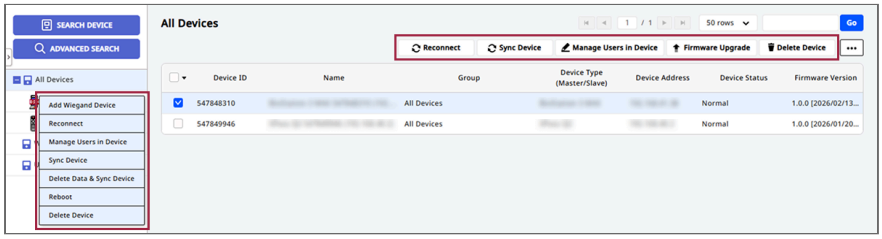
Usar la Función de Administración de Dispositivos

Esta guía explica cómo usar funciones adicionales de **BioStar X**. Esta sección explica cómo reconectar dispositivos, sincronizar, editar en lote la información de los dispositivos, eliminar dispositivos, y exportar o importar ajustes. También explica cómo eliminar certificados de comunicación segura al eliminar dispositivos.

Administrar un dispositivo

Siga los pasos a continuación para administrar un solo dispositivo.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Selecciona el dispositivo en la lista **All Devices** y haz clic con el botón derecho. O haga clic en la casilla de verificación junto al dispositivo que desea en la lista de dispositivos.



4. Seleccione la acción deseada en el menú emergente o en la parte superior de la lista de dispositivos.

Consulte las funciones que se indican a continuación. Las funciones disponibles pueden variar según el dispositivo.

- **Reconnect**: Reconectar el dispositivo seleccionado. Esta opción está disponible cuando se selecciona un dispositivo. En general, el dispositivo vuelve automáticamente a estar en línea cuando se restablece la conexión de red, sin intervención del usuario. Use esta característica cuando el dispositivo no se reconecte automáticamente después de restablecer la conexión de red.

  > **Información**
  >
  > Esta función no es compatible con los dispositivos conectados con la opción **Device ▸ Server Connection**. Para obtener más información sobre el registro de dispositivos, consulte Registrar dispositivo.

- **Sync Device**: Sincronizar toda la información de usuario registrada en el dispositivo con **BioStar X**. Esta sincronización se basa en la base de datos de **BioStar X** y eliminará la información de usuario registrada únicamente en el dispositivo. Utiliza la función **Manage Users in Device** para cargar la información de usuario en **BioStar X**.
- **Delete Data & Sync Device**: Eliminar toda la información de configuración y de usuario almacenada en el dispositivo y volver a enviarla. Esta función también está disponible al seleccionar el dispositivo en la lista y hacer clic en el botón [•••].
- **Manage Users in Device**: Cargar o eliminar la información de usuario registrada en el dispositivo en **BioStar X**. Para obtener más información, consulte Administrar Usuarios Registrados en el Dispositivo.
- **Firmware Upgrade**: Actualizar fácilmente el firmware del dispositivo. Para obtener más información, consulte Actualizar Firmware.
- **Reboot**: Reiniciar el dispositivo seleccionado. Utiliza esta función cuando el dispositivo no funcione con normalidad.
- **Delete Device**: Eliminar el dispositivo seleccionado de la lista. Los dispositivos configurados como puertas o zonas no se pueden eliminar. Para más información, consulte Eliminar dispositivos.

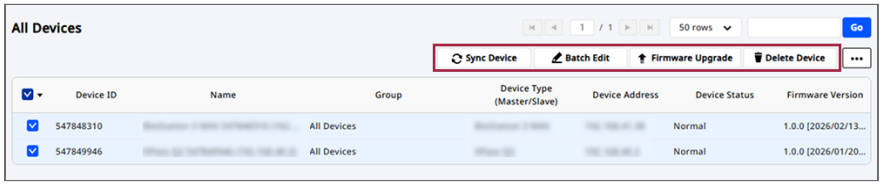
Información

- Para obtener más información sobre la función **Add Wiegand Device**, consulte Registrar Credenciales Wiegand.
- Para obtener más información sobre la función **Search Slave Device**, consulte Registrar Esclavo.

Administrar varios dispositivos

Siga los pasos a continuación para administrar uno o más dispositivos.

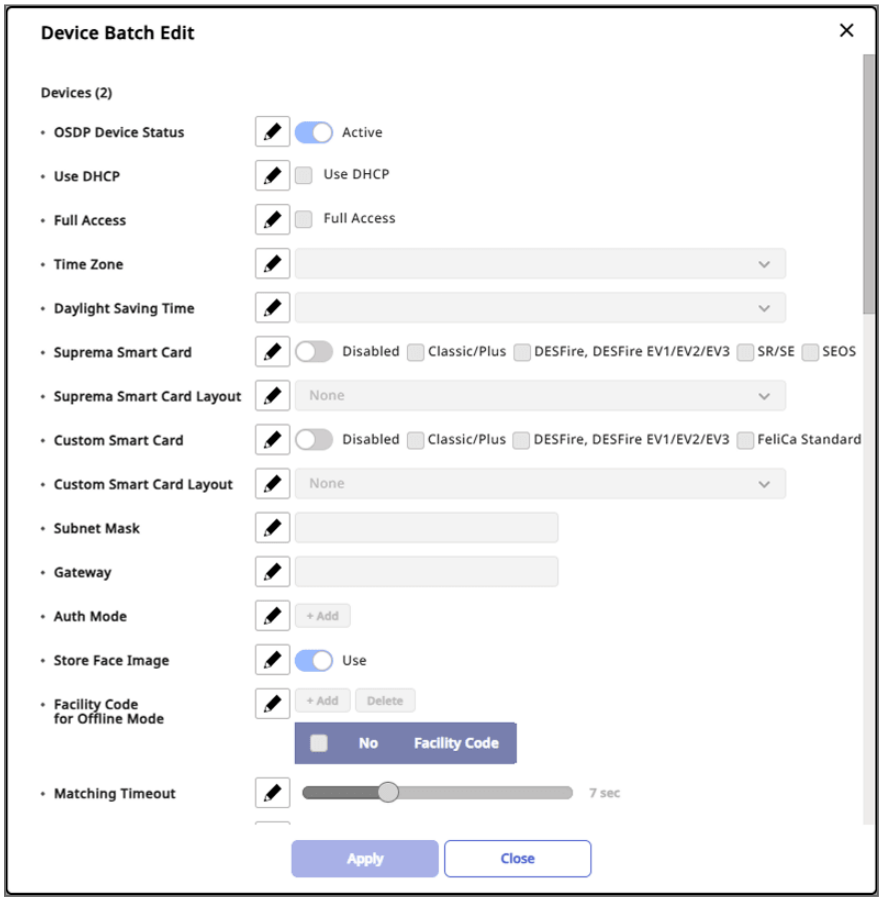
1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haga clic en la casilla de verificación junto al dispositivo que desea en la lista de dispositivos. Puede seleccionar 1 o más dispositivos.



4. Seleccione la función deseada en la parte superior de la lista de dispositivos.

Consulte las funciones que se indican a continuación. Las funciones disponibles pueden variar según el dispositivo.

- **Sync Device**: Sincronizar toda la información de usuario registrada en el dispositivo con **BioStar X**. Esta sincronización se basa en la base de datos de **BioStar X** y eliminará la información de usuario registrada únicamente en el dispositivo.
- **Batch Edit**: Editar por lotes la información de los dispositivos seleccionados. Haga clic en el botón para abrir la ventana **Device Batch Edit**.



Información

- Los detalles que se muestran en la ventana **Device Batch Edit** pueden variar según los tipos de dispositivo seleccionados.
- Al seleccionar un dispositivo maestro y dispositivos esclavos simultáneamente para la edición por lotes, solo se pueden modificar ciertos elementos dentro de **Authentication** y **Display/Sound**.
- **Auth Mode** solo se puede editar por lotes cuando se seleccionan dispositivos con el mismo nombre de modelo.

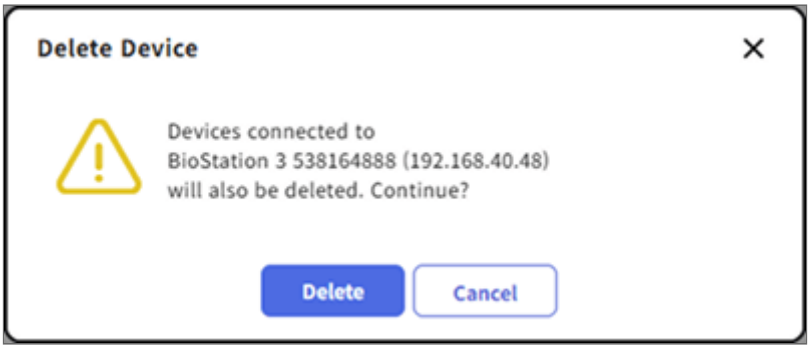
- **Firmware Upgrade**: Actualizar fácilmente el firmware del dispositivo. Para obtener más información, consulte Actualizar Firmware.
- **Delete Device**: Eliminar el dispositivo seleccionado de la lista. Los dispositivos configurados como puertas o zonas no se pueden eliminar. Para más información, consulte Eliminar dispositivos.

Eliminar dispositivos

Use **Delete Device** para eliminar dispositivos de la lista. Las opciones que aparecen durante la eliminación dependen de si **Secure communication with device** está habilitado.

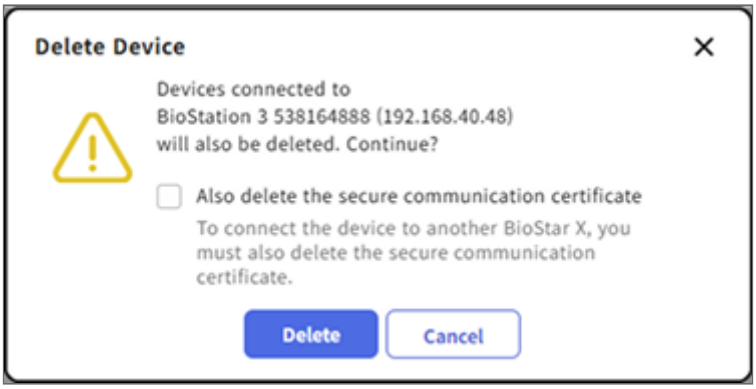
Cuando la comunicación segura está deshabilitada

Cuando **Secure communication with device** está establecido en **Not Use**, elimine el dispositivo seleccionado sin opciones adicionales.



Cuando la comunicación segura está habilitada

Cuando **Secure communication with device** está establecido en **Use**, el cuadro de diálogo **Delete Device** muestra la opción **Also delete the secure communication certificate**.



- Si **Also delete the secure communication certificate** está desmarcada (predeterminado), elimine solo el dispositivo y conserve el certificado.
- Si **Also delete the secure communication certificate** está seleccionada, elimine también el certificado de comunicación segura almacenado en el dispositivo. Use esta opción para conectar el dispositivo a otro servidor **BioStar X** después de eliminarlo.

Precaución

Si un dispositivo se desconecta de **BioStar X**, no puede eliminar su certificado. Si **Also delete the secure communication certificate** está seleccionada, falla la eliminación del dispositivo. Para eliminar el dispositivo, desmarque la opción o reconecte el dispositivo y vuelva a intentarlo.

Información

- Si **Secure communication with device** está habilitado, al eliminar el dispositivo sin seleccionar **Also delete the secure communication certificate**, el certificado permanece en el dispositivo. Luego, cambie la opción **Secure communication with device** a **Not Use** y vuelva a inscribir el dispositivo en **BioStar X**. El dispositivo no se conecta porque el certificado permanece en el dispositivo. Si usa el certificado predeterminado, cambie la opción **Secure communication with device** de nuevo a **Use**.
- Si todos los dispositivos seleccionados son dispositivos secundarios o no admiten comunicación segura, elimine los dispositivos sin la opción **Also delete the secure communication certificate**.
- La opción **Also delete the secure communication certificate** aparece solo cuando **Secure communication with device** está habilitado. Para más información, consulte Mejorar la Seguridad del Sistema.

Exportar/importar la configuración del dispositivo

Exporte la configuración de un dispositivo a un archivo y luego impórtela y aplíquela a otro dispositivo del mismo modelo. En lugar de repetir la configuración en varios dispositivos, cree un archivo desde uno configurado y aplíquelo a los demás.

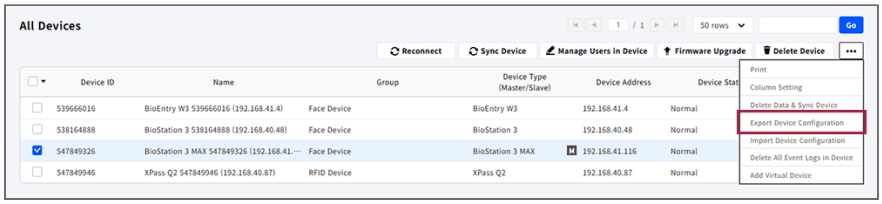
Información

- El mismo modelo significa que el nombre detallado del modelo y el número de parte coinciden (por ejemplo, XXX en XPD2-XXX).
- La característica de exportar/importar la configuración está disponible para administradores con permisos completos para los ajustes del dispositivo. Para obtener más información sobre la configuración de permisos de administrador, consulte Gestionar Permisos de Operación.

Exportar la configuración del dispositivo

Para descargar las configuraciones de un solo dispositivo como archivo, siga estos pasos.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. En la lista de dispositivos, seleccione la casilla del dispositivo cuya configuración se exportará. Seleccione solo un dispositivo.
4. Haga clic en ••• → **Export Device Configuration** en la parte superior de la lista de dispositivos.



5. Cuando aparezca la ventana de descarga, guarde el archivo de configuración localmente.

Precaución

La exportación de configuraciones no está disponible para los siguientes dispositivos.

- Dispositivos desconectados de **BioStar X** o con tiempo de espera de respuesta
- Dispositivo Virtual
- Dispositivos sin modo de comunicación RS-485 (por ejemplo, dispositivos Wiegand, módulos de E/S, interfaz de puerta, módulos de puerta, módulos Secure y antena/lector OSDP)

Información

- No puede ejecutar esta característica a menos que seleccione exactamente un dispositivo.
- El sistema establece el nombre del archivo automáticamente en este orden: nombre del modelo, ID del dispositivo, modo de comunicación RS-485 (Master/Default/Slave) y fecha de exportación. La fecha sigue el formato de fecha establecido en **Settings** → **System** → **Preferences**.

  Por ejemplo, si el nombre del modelo es BS3-DB, el ID del dispositivo es 538001234, el modo de comunicación serial es **Master**, y la fecha de exportación es 6/23/2026, el archivo se guarda como `BS3-DB_538001234_Master_20260623.json`.

Configuraciones excluidas de la exportación

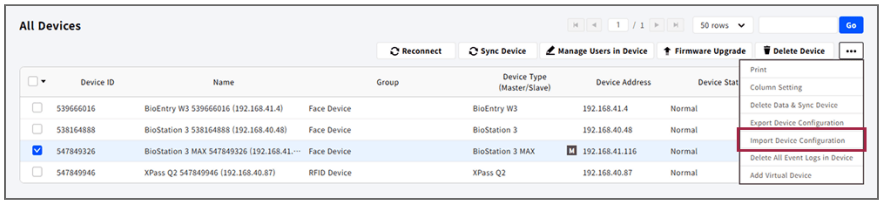
El archivo de exportación no incluye las siguientes configuraciones porque deben ser únicas por dispositivo, se guardan solo en el dispositivo o contienen información confidencial, como credenciales.

- Configuraciones específicas del dispositivo: Name, Group, red cableada e inalámbrica, conexión al servidor, identificador OSDP y Trigger & Action
- Estas configuraciones se guardan solo en el dispositivo. No es posible trasladarlas a otro dispositivo: recursos de idioma, pantalla de inicio y opciones de sonido en Display/Sound, la clave SCB para comunicación serial y opciones de video agregadas a BioStation 3 Max
- Credenciales e información confidencial: nombres de usuario y contraseñas para el intercomunicador IP y RTSP, Master Admin y la opción Two-step Authentication

Importar la configuración del dispositivo

Para aplicar el archivo de configuración exportado a uno o más dispositivos del mismo modelo, siga estos pasos.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. En la lista de dispositivos, seleccione la casilla del dispositivo que recibirá las configuraciones. Seleccione uno o más dispositivos.
4. Haga clic en ••• → **Import Device Configuration** en la parte superior de la lista de dispositivos.



5. Cuando aparezca la ventana Abrir en el navegador web, seleccione el archivo de configuración guardado localmente.
6. Cuando aparezca el mensaje de resultado de Importar configuraciones del dispositivo, revíselo y haga clic en **Ok**.

Precaución

El sistema acepta como válidos los archivos de configuración creados en otros sitios o servidores, sin verificar el origen ni mostrar una advertencia. Verifique que una fuente confiable haya creado el archivo que importará.

Información

Seleccione al menos un dispositivo para ejecutar esta característica.

Al ejecutar Importar, el sistema verifica lo siguiente, en este orden, antes de aplicar la configuración. Si falla alguna verificación, el sistema no aplica las configuraciones y muestra el motivo.

- Si todos los dispositivos seleccionados tienen el mismo nombre de modelo (incluido el número de parte)
- Si el modo de comunicación RS-485 coincide entre los dispositivos seleccionados y el archivo
- Si el nombre de modelo guardado en el archivo (incluido el número de parte) coincide con los nombres de modelo de los dispositivos seleccionados (incluido el número de parte)
- Si alguno de los dispositivos seleccionados es un dispositivo virtual (Virtual Device)

Si las verificaciones se completan, el sistema aplica las configuraciones, excepto Configuraciones excluidas de la exportación, a dispositivos seleccionados.

Información

- Importar un archivo de un dispositivo no compatible pone la característica en Desactivado y desactiva las opciones habilitadas. Importar un archivo de un dispositivo compatible en uno no compatible omite la funcionalidad y aplica los ajustes restantes. En ambos casos, el sistema no marca la importación como fallida ni la agrega a la lista de fallas.
- Los ajustes que requieren una licencia del dispositivo no se aplican a dispositivos sin esa licencia. Importar un archivo de un dispositivo sin licencia establece el ajuste en "Desactivado" y desactiva las opciones habilitadas. En ambos casos, el sistema no marca la importación como fallida ni la agrega a la lista de fallas.
- El sistema muestra un mensaje de éxito después de que aplica los ajustes a todos los dispositivos. Si el sistema no aplica los ajustes, aparece un mensaje con el recuento de fallas y un enlace al CSV. El archivo enumera el ID, el nombre y el motivo de cada dispositivo con error (desconectado o porque los grupos de acceso bloquean los permisos de acceso completo).

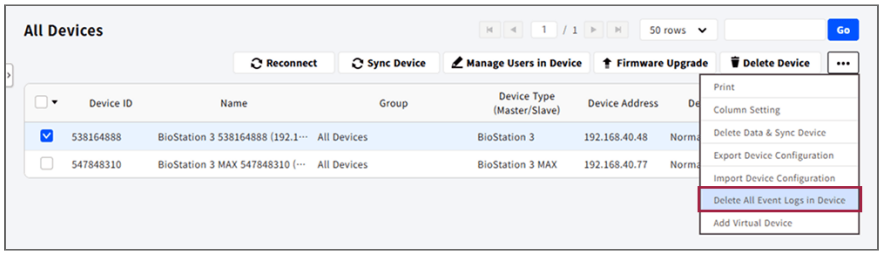
  > *Por ejemplo, si ejecuta una importación a las 15:45:30 el 6/23/2026 y falla, el nombre del archivo es `Device_Template_Import_Error_20260623T154530.csv`.*

- También se incluyen los dispositivos CoreStation.
- Vea el historial de exportación e importación de ajustes del dispositivo en **Settings** → **Audit Trail** → **AC Audit Log**.

Eliminar registros de eventos de un dispositivo

Puede eliminar los registros de eventos almacenados en el dispositivo.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haga clic en la casilla de verificación junto al dispositivo que desea en la lista de dispositivos. Puede seleccionar 1 o más dispositivos.
4. Haga clic en ••• → **Delete All Event Logs in Device** en la parte superior de la lista de dispositivos.



5. Si aparece un cuadro de diálogo de advertencia, revise el mensaje y haga clic en el botón **Continue**.

Cuando se complete la eliminación de los registros de eventos del dispositivo, aparecerá un mensaje emergente. Vea la cantidad de dispositivos objetivo, los exitosos y los que fallaron.

Precaución

Los registros de eventos eliminados de un dispositivo no se pueden recuperar ni reenviar desde el servidor al dispositivo. Antes de proceder con la eliminación, confirme que los registros de eventos del dispositivo están almacenados en el servidor. Además, si entre los dispositivos seleccionados hay dispositivos esclavos, virtuales o Wiegand, estos no almacenan registros y se excluyen de la eliminación de registros.

Información

- Solo los usuarios con el permiso **Administrator Role** pueden usar esta función.
- Vea el historial de eliminación de registros de eventos del dispositivo en **Settings** → **Audit Trail** → **AC Audit Log**.

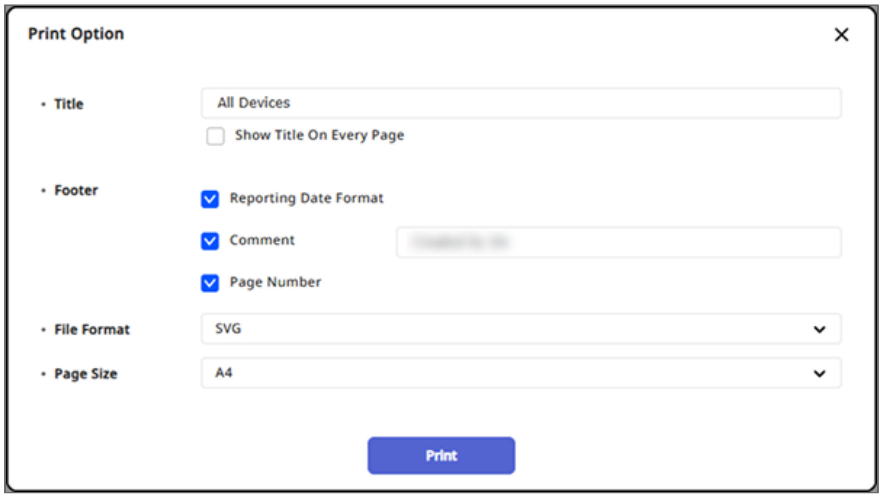
Funciones adicionales

Utilice funciones adicionales, como imprimir la lista de dispositivos o cambiar la configuración de las columnas.

Imprimir la lista de dispositivos

Guarde la lista de dispositivos como un archivo PDF o SVG para imprimir.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haga clic en [•••] en la parte superior de la lista de dispositivos.
4. Haga clic en **Print** en el menú emergente.
5. Cuando aparezca la ventana **Print Option**, seleccione el formato deseado en las opciones **File Format** y configure las demás opciones.



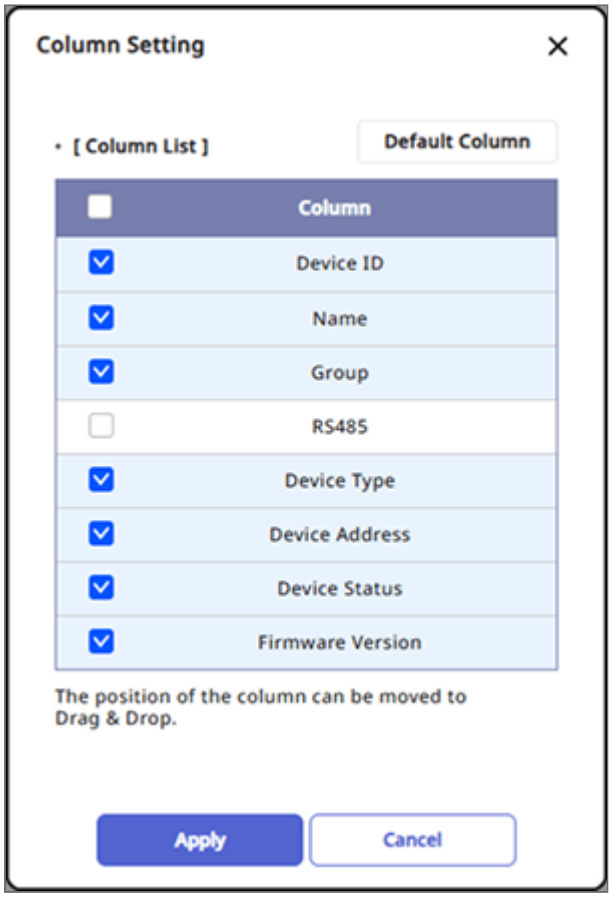
6. Haga clic en **Print**.

Imprima el archivo PDF o SVG que se abre en el navegador.

Configuración de la columna (Columna) de la lista de dispositivos

Puede cambiar la configuración de la columna (Columna) que se muestra en la lista de dispositivos. En los ajustes de columnas, seleccione las columnas que aparecerán o cambie su orden.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haga clic en ••• en la parte superior de la lista de dispositivos.
4. Haga clic en **Column Setting** en el menú emergente.
5. Cuando aparezca la ventana **Column Setting**, seleccione o deseleccione las columnas deseadas.



6. Haga clic y arrastre la columna deseada para cambiar su posición.
7. Haga clic en **Apply** para guardar la configuración.

> **Información**
> Haz clic en **Default Column** para inicializar la configuración de columnas.

Configuración del Dispositivo

Esto proporciona instrucciones sobre cómo configurar y gestionar las funciones detalladas del dispositivo registrado. Puede configurar detalles como la información del dispositivo, la configuración de red, la autenticación y la configuración avanzada. Los detalles pueden variar según los tipos de conexión RS-485 o los modelos de dispositivo.

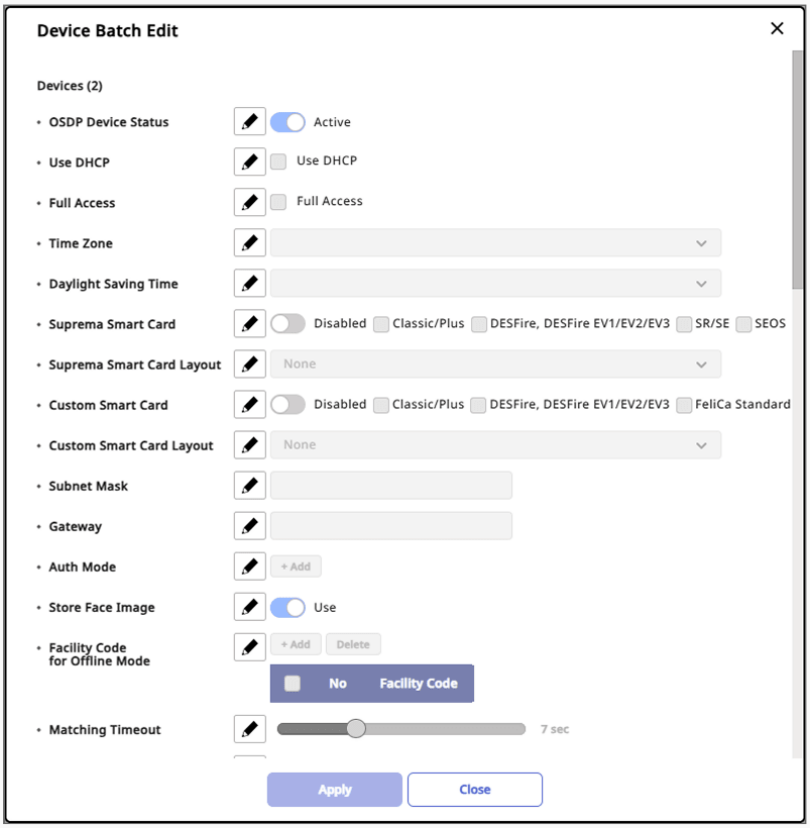
1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Seleccione el dispositivo que desea configurar de la lista de dispositivos.
4. Consulte los detalles en cada sección para configurar la información del dispositivo.
   - **Information**: Verifique y modifique el nombre y grupo del dispositivo, la zona horaria, el hardware y las versiones de firmware. Para obtener más información, consulte Ajuste de Información Básica.
   - **Network**: Configure la configuración de red del dispositivo para TCP/IP, RS-485 y comunicación con el servidor. Para obtener más información, consulte Configuración de Red.

- **Authentication**: Configure las opciones relacionadas con la autenticación de usuarios para el dispositivo. Para obtener más información, consulte Configuración de Autenticación.
- **Advanced**: Puede configurar el Administrador maestro, la gestión del dispositivo, pantalla/sonido, condiciones de funcionamiento y acciones. Para obtener más información, consulte Configuración Avanzada.
- **Thermal & Mask** / **Mask**: Configure los detalles relacionados con el uso de la cámara térmica y la mascarilla. Para obtener más información, consulte Configuración Térmica y de Máscara.
- **Intercom**: Configure los detalles para usar el intercomunicador IP. Para obtener más información, consulte Configuración del Intercomunicador.
- **RTSP**: Establezca los detalles para la transmisión **Real Time Streaming Protocol** (RTSP). Para obtener más información, consulte Configuración de RTSP.

5. Una vez completados todos los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.

Información

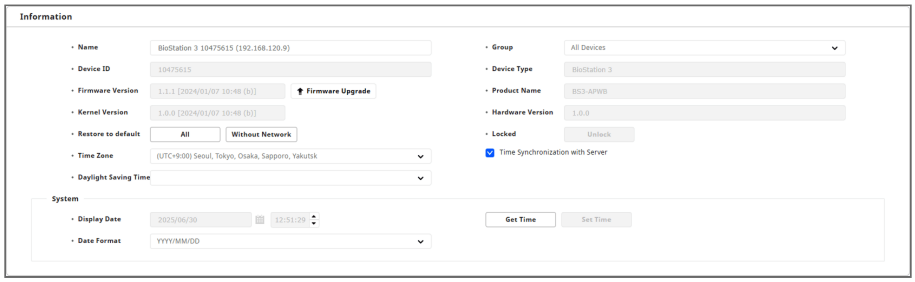
- También puede modificar la información de varios dispositivos a la vez. Seleccione dos o más dispositivos y luego haga clic en **Batch Edit** en la esquina superior derecha de la pantalla.



- Los detalles que se muestran en la ventana **Device Batch Edit** pueden variar según los tipos de dispositivo seleccionados.
- Al seleccionar un dispositivo maestro y dispositivos esclavos simultáneamente para la edición por lotes, solo se pueden modificar ciertos elementos dentro de **Authentication** y **Display/Sound**.
- **Auth Mode** solo se puede editar por lotes cuando se seleccionan dispositivos con el mismo nombre de modelo.

Ajuste de Información Básica

La sección **Information** permite configurar la información básica del dispositivo. Permite comprobar el nombre y el grupo del dispositivo, la zona horaria y las versiones de hardware y firmware. Permite cambiar el nombre y el grupo del dispositivo o actualizar su firmware.



Estos son los ajustes de información predeterminados del dispositivo que no se pueden modificar.

- **Device ID**: Permite comprobar el ID del dispositivo.
- **Device Type**: Permite comprobar el tipo de dispositivo.
- **Product Name**: Permite comprobar el nombre del modelo del dispositivo.
- **Kernel Version**: Permite comprobar la versión del kernel del dispositivo.
- **Hardware Version**: Permite comprobar la versión de hardware del dispositivo.

> **Información**
>
> Si el usuario ha realizado cambios, haga clic en **Apply**. Los cambios no se aplicarán al dispositivo si no se guardan.

Cambiar el nombre del dispositivo

Permite cambiar el nombre predeterminado del dispositivo. Introduzca el nombre deseado del dispositivo en el campo **Name**. Puede introducir un nombre de dispositivo de hasta 48 caracteres. El nombre del dispositivo puede tener hasta 48 caracteres y se usa para identificar el dispositivo en la lista de dispositivos.

Cambiar el grupo del dispositivo

Permite cambiar el grupo al que pertenece el dispositivo. Seleccione el grupo de dispositivos deseado en el campo **Group**.

> **Información**
>
> Para obtener más información sobre cómo crear, renombrar o eliminar grupos de dispositivos, consulte Gestionar Grupos de Dispositivos.

Actualización de firmware

Puede comprobar la versión de firmware del dispositivo en la sección **Firmware Version**. Haga clic en **Firmware Upgrade** para actualizar el firmware.

Información

Para obtener más información sobre cómo actualizar el firmware del dispositivo, consulte Actualizar Firmware.

Configurar la fecha y la hora del dispositivo

Permite configurar la fecha y la hora del dispositivo mediante las opciones siguientes.

- **Time Zone**: Permite seleccionar la zona horaria estándar donde se encuentra el dispositivo.
- **Time Synchronization with Server**: Permite sincronizar la hora del dispositivo con el servidor **BioStar X**.
- **Daylight Saving Time**: Permite aplicar al dispositivo el horario de verano configurado por el usuario. Para agregar un nuevo horario de verano, consulte Horario de Verano (DST).
- **Display Date**: Permite configurar manualmente la fecha y la hora del dispositivo. Después de configurar fecha y hora, haga clic en **Set Time**.

  Esta función se puede utilizar cuando la opción **Time Synchronization with Server** no está seleccionada.

- **Date Format**: Permite seleccionar el formato de fecha que se muestra en el dispositivo.
- **Get Time**: Permite obtener la hora configurada en el dispositivo.

Precaución

La fecha y la hora configuradas se registrarán en el registro de eventos y en tiempo real. Si la fecha y la hora del dispositivo son incorrectas, los registros pueden ser inexactos.

Desbloquear el dispositivo

Cuando el dispositivo esté bloqueado debido a condiciones de funcionamiento y acciones, haga clic en **Locked Unlock** para desbloquearlo. Permite desbloquear el dispositivo.

Información

Para obtener más información sobre las condiciones de activación y la configuración de acciones, consulte Configuración de Activadores y Acciones.

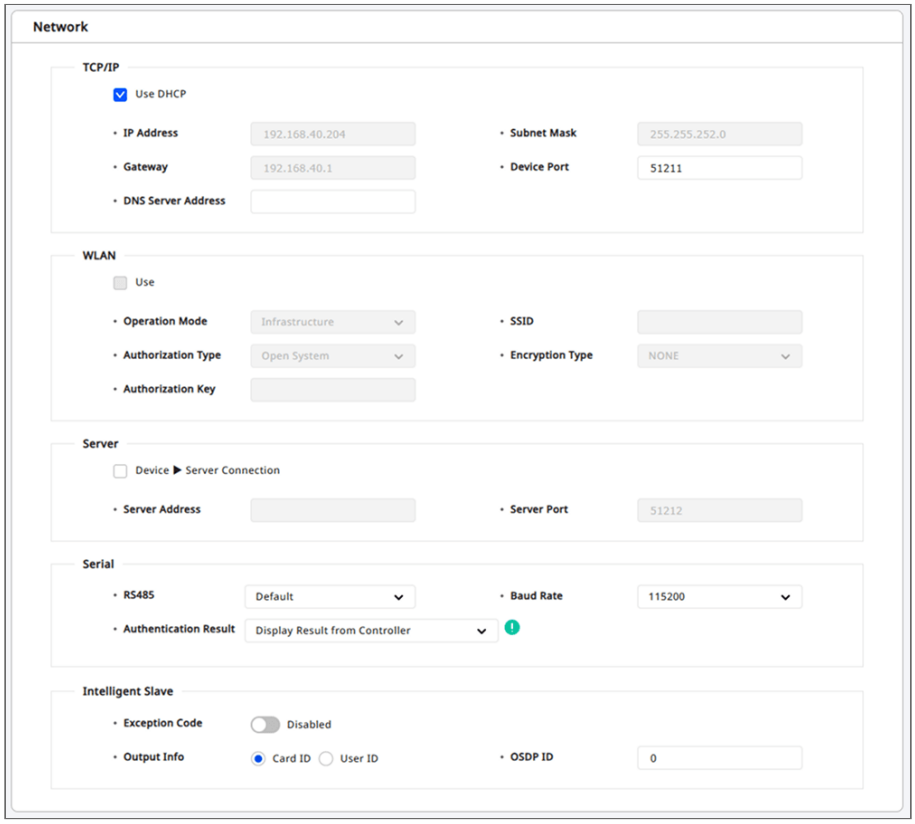
Inicializar el dispositivo

Para inicializar los ajustes del dispositivo, seleccione una de las siguientes funciones en el campo **Restore to default**.

- **All**: Inicializa todos los ajustes del dispositivo.
- **Without Network**: Mantiene los ajustes de red e inicializa los demás ajustes.

Configuración de Red

A continuación se muestran los ajustes de red del dispositivo registrado. En la sección **Network**, configure la red TCP/IP, RS-485 y la comunicación con el servidor del dispositivo.



Información

- Las opciones de red disponibles pueden variar según el tipo de dispositivo.
- Si el usuario ha realizado cambios, haga clic en **Apply**. Los cambios no se aplicarán al dispositivo si no se guardan.

Ajustes de TCP/IP

En el grupo **TCP/IP**, configure la dirección IP del dispositivo.

Información

Para obtener más información sobre la configuración de la dirección IP al registrar un dispositivo, consulte Registrar dispositivo.

Ajustes de IP dinámica

Seleccione la casilla de la opción **Use DHCP** para configurar el dispositivo con IP dinámica. El dispositivo recibirá automáticamente una dirección IP del servidor DHCP, la cual puede cambiar. En ese caso, la dirección IP del dispositivo puede cambiar.

Ajustes de IP estática

Desactive la casilla de la opción **Use DHCP** para asignar una dirección IP estática al dispositivo. Ingrese la información de red del dispositivo en los campos siguientes.

- **OSDP ID**: Ingrese la dirección OSDP del dispositivo. Debe ser un número entre 0 y 126.
- **Subnet Mask**: Ingrese la máscara de subred del dispositivo.
- **Gateway**: Ingrese la dirección de puerta de enlace del dispositivo.
- **Device Port**: Ingrese el número de puerto del dispositivo.
- **DNS Server Address**: Ingrese la dirección del servidor DNS del dispositivo.

▼ **Ver dispositivos y versiones de firmware que pueden aceptar direcciones de servidor DNS**

- Firmware de BioStation 3 Max, versión 1.0.0 o posterior
- Firmware de XPass Q2, versión 1.0.0 o posterior
- BioEntry W3 versión de firmware 1.0.0 o superior
- BioStation 3 firmware 1.0.0 o superior
- X-Station 2 versión de firmware 1.0.0 o superior
- FaceStation F2 versión de firmware 1.0.0 o superior
- Firmware de XPass 2 1.0.0 o posterior
- Firmware de FaceLite 1.0.0 o posterior
- Firmware de BioLite N2 1.0.0 o posterior
- Firmware de FaceStation 2 1.0.0 o posterior
- Firmware de BioStation L2 1.0.0 o posterior
- Firmware de BioStation A2 1.0.0 o posterior
- Firmware de BioStation 2 1.2.0 o posterior

Ajustes de LAN inalámbrica

En el grupo **WLAN**, active o desactive los ajustes de LAN inalámbrica del dispositivo. Los ajustes detallados están disponibles en la guía del usuario del dispositivo.

Información

Consulte los siguientes dispositivos que admiten ajustes de LAN inalámbrica:

- BioStation 2
- BioStation A2
- FaceStation 2
- BioStation 3

Ajustes de comunicación con el servidor

En el grupo **Server**, configure cómo se comunica el dispositivo con el servidor **BioStar X**.

- **Device ▸ Server Connection**: Al seleccionar esta opción, ingrese la dirección IP y el número de puerto del servidor **BioStar X** al que se conectará el dispositivo.
- **Server Address**: Ingrese la dirección IP o el nombre de dominio del servidor **BioStar X**.
- **Server Port**: Ingrese el número de puerto del servidor **BioStar X**.

> **Consejo**
> Esta función es útil cuando cambia la dirección IP del servidor **BioStar X**. Si configura previamente esta opción en varios dispositivos antes de cambiar la dirección IP del servidor, los dispositivos se conectarán automáticamente a la dirección IP actualizada.

▼ **Ver dispositivos y versiones de firmware que permiten ingresar nombres de dominio en Server Address**

- Firmware de BioStation 3 Max, versión 1.0.0 o posterior
- Firmware de XPass Q2, versión 1.0.0 o posterior
- BioEntry W3 versión de firmware 1.0.0 o superior
- BioStation 3 firmware 1.0.0 o superior
- X-Station 2 versión de firmware 1.0.0 o superior
- FaceStation F2 versión de firmware 1.0.0 o superior
- Firmware de XPass 2 1.0.0 o posterior
- Firmware de FaceLite 1.0.0 o posterior
- Firmware de BioLite N2 1.0.0 o posterior
- Firmware de BioEntry P2 1.0.0 o posterior
- Firmware de FaceStation 2 1.0.0 o posterior
- Firmware de BioEntry W2 1.0.0 o posterior
- Firmware de BioStation L2 1.0.0 o posterior
- Firmware de BioStation A2 1.0.0 o posterior
- Firmware de BioStation 2 1.2.0 o posterior

Configuración de comunicación serial

En el grupo **Serial**, configure el modo, el rendimiento de transmisión y la visualización de resultados de autenticación para dispositivos conectados mediante RS-485.

- **RS485**: Configure el modo RS-485.
- **Baud Rate**: Configure el rendimiento de comunicación RS-485.
- **Authentication Result**: Seleccione el resultado de autenticación que se mostrará en la pantalla del dispositivo cuando se utilice con un controlador de terceros.
  - **Display Result from Controller**: Permite mostrar en el dispositivo el resultado de autenticación del controlador de terceros.
  - **Display Device Matching Result**: Permite mostrar el resultado de autenticación del propio dispositivo.

Información

La opción **Authentication Result** se habilita cuando la opción **RS485** está configurada en **Slave** o **Default**.

Ajustes de esclavo inteligente

En el grupo **Intelligent Slave**, cuando un usuario se autentica con huella digital en un entorno donde los dispositivos Suprema están conectados a controladores de terceros, el resultado de la autenticación se envía como datos de tarjeta OSDP (Open Supervised Device Protocol) para admitir numerosos emparejamientos 1:1 o 1:N.

- **Exception Code**: Cuando utilice el esclavo inteligente, si ocurre una excepción, como un fallo de autenticación, ingrese el código de excepción en formato decimal (0-18446744073709551615) o hexadecimal (0-FFFFFFFFFFFFFFFF) para registrar un log preciso. El valor hexadecimal puede introducirse con números o letras.



- **Output Info**: Permite enviar el ID de tarjeta o el ID de usuario tras una autenticación exitosa.
- **OSDP ID**: Ingrese la dirección OSDP del dispositivo. Debe ser un número entre 0 y 126.

Información

- Puede introducir datos de hasta 8 bytes en **Exception Code**.
- La opción **Intelligent Slave** se habilita cuando la opción **RS485** está configurada en **Default**.

▼ Ver dispositivos y versiones de firmware que admiten la opción Intelligent Slave

- Firmware de BioStation 3 Max, versión 1.0.0 o posterior
- Firmware de XPass Q2, versión 1.0.0 o posterior
- BioEntry W3 versión de firmware 1.0.0 o superior
- BioStation 3 firmware 1.0.0 o superior
- Firmware de X-Station 2 1.1.0 o superior
- Firmware de FaceStation F2 1.1.2 o superior
- Firmware de XPass 2 1.2.3 o superior
- Firmware de BioLite N2 1.4.1 o superior
- Firmware de BioEntry P2 1.4.1 o superior
- Firmware de BioEntry W2 1.6.3 o posterior
- Firmware de BioStation L2 1.6.1 o posterior

Configuración de Autenticación

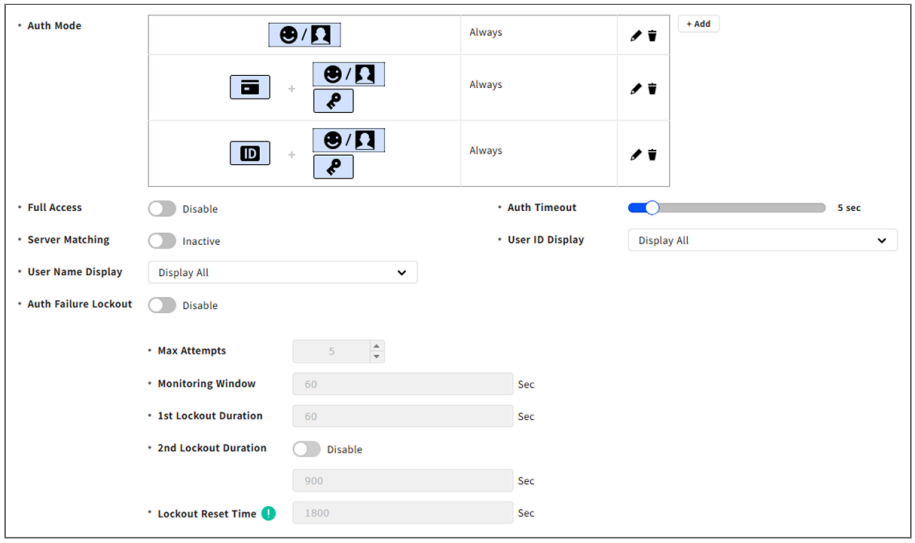
Se proporcionan instrucciones para varios ajustes relacionados con la autenticación de usuarios en el dispositivo. La sección

Authentication ofrece información paso a paso sobre los métodos de autenticación y las principales opciones de autenticación compatibles con el dispositivo. Tenga en cuenta que los cambios en los ajustes se aplicarán al dispositivo real y configure la política de autenticación según su entorno, consultando las características y precauciones de cada opción.

> **Información**
>
> - Las opciones de red disponibles pueden variar según el tipo de dispositivo.
> - Si el usuario ha realizado cambios, haga clic en **Apply**. Los cambios no se aplicarán al dispositivo si no se guardan.

Ajustes del método de autenticación

Configure el modo de autenticación del dispositivo, los permisos, la autenticación en servidor y el tiempo de espera de autenticación.



- **Auth Mode**: Configure el modo de autenticación del dispositivo combinando una o más credenciales. Para obtener más información, consulte Agregar modo de autenticación.
  - Haga clic en para modificar el modo de autenticación agregado.
  - Haga clic en para eliminar el modo de autenticación agregado.
- **Full Access**: A los usuarios registrados en el dispositivo se les pueden otorgar todos los permisos de acceso sin definir ajustes de grupo de acceso.

  > **Información**
  >
  > Cuando esta opción está configurada en **Use**, el dispositivo no se puede registrar en **Access Level** ni en **Floor Level**.

- **Auth Timeout**: Es el tiempo de espera para autenticar la segunda credencial cuando se utilizan varias credenciales en la opción **Auth Mode**. Si la credencial no se autentica dentro del tiempo especificado, la autenticación fallará.
- **Server Matching**
  - **Active**: Activa la autenticación en servidor. Configure la función de autenticación en servidor para autenticar con la información de usuario almacenada en el servidor donde está instalado **BioStar X**.

- **Inactive**: Desactiva la autenticación en servidor. En este caso, la autenticación se realiza utilizando la información de usuario registrada en el dispositivo.

▼ **Ver los dispositivos y versiones de firmware que admiten la función Server Matching**

- Firmware de BioStation 3 Max, versión 1.0.0 o posterior
- Firmware de XPass Q2, versión 1.0.0 o posterior
- BioEntry W3 versión de firmware 1.0.0 o superior
- BioStation 3 firmware 1.0.0 o superior
- X-Station 2 versión de firmware 1.0.0 o superior
- FaceStation F2 versión de firmware 1.0.0 o superior
- Firmware de XPass 2 1.0.0 o posterior
- Firmware de BioLite N2 1.0.0 o posterior
- Versión de firmware de XPass D2 1.0.0 o superior
- Firmware de BioEntry P2 1.0.0 o posterior
- FaceStation 2 versión de firmware 1.4.0 o superior
- Firmware de BioEntry W2 1.0.0 o posterior
- Firmware de BioStation L2 1.0.0 o posterior
- Firmware de BioStation A2 1.0.0 o posterior
- Firmware de BioStation 2 1.2.0 o posterior
- Versión de firmware de CoreStation 1.0.0 o superior
- FaceLite no admite la función de autenticación en servidor.
- Los dispositivos BioStation 3, BioEntry W3 y FaceStation F2 no pueden usar la verificación en servidor para la autenticación facial.

- **Face Detection Level**: Establezca los pasos del algoritmo para reconocer rostros con la cámara integrada cuando el usuario se autentique.
  - **Normal**: Detecta rostros a una distancia equivalente a la longitud del brazo de una persona.
  - **High**: Requiere que el usuario esté más cerca que la longitud del brazo de una persona para detectar un rostro.
  - **Not Use**: No utiliza la funcionalidad de reconocimiento facial.

> **Información**
> Esta opción es compatible con BioStation A2.

- **User ID Display**: Controle si se muestra u oculta la ID de usuario en el dispositivo cuando la autenticación es exitosa.
  - **Display All** / **Mask All but First Letter** / **Hide All**
- **User Name Display**: Controle si se muestra u oculta el nombre de usuario en el dispositivo cuando la autenticación es exitosa.
  - **Display All** / **Mask All but First Letter** / **Hide All**
- **Auth Failure Lockout**: Si la autenticación falla repetidamente en poco tiempo, el dispositivo se bloquea durante un período determinado. Esto bloquea ataques de fuerza bruta. Establezca esta opción en **Enable** para configurar los

ajustes siguientes. El valor predeterminado es **Disable**.

- **Max Attempts**: Establezca la cantidad de fallas de autenticación permitidas antes del bloqueo en 3~15 intentos. El valor predeterminado es 5 intentos.
- **Monitoring Window**: Establezca la ventana de tiempo para contar fallas de autenticación en 30~300 segundos. El valor predeterminado es 60 segundos.
- **1st Lockout Duration**: Establezca en 30~900 segundos el tiempo de bloqueo que se aplica cuando las fallas llegan a **Max Attempts**. El valor predeterminado es 60 segundos y el valor es obligatorio.
- **2nd Lockout Duration**: Tiempo del 2.º bloqueo. El dispositivo lo aplica si las fallas de autenticación continúan incluso después de que se haya levantado el 1.º bloqueo. Establezca esta opción en **Use** para ingresar un valor entre 900~3,600 segundos. El valor predeterminado es 900 segundos.

  > Establezca esta opción en **Disable** para aplicar repetidamente solo el 1.º bloqueo, sin un 2.º bloqueo.

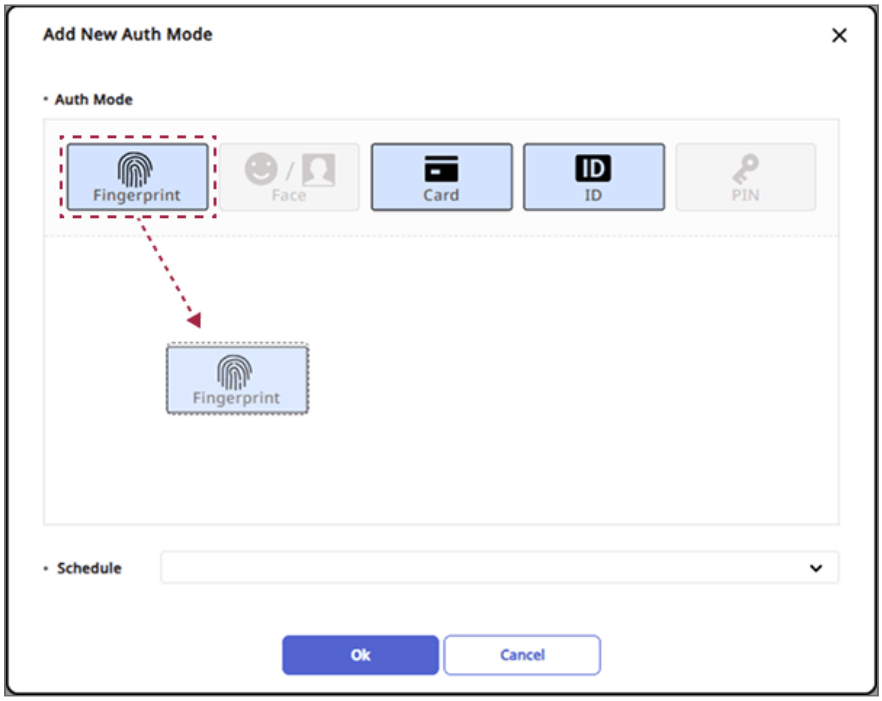
- **Lockout Reset Time**: Si no ocurren fallas adicionales dentro de este tiempo después de la última falla, el dispositivo inicializa el conteo acumulado de fallas. Configúrelo en 600~3,600 segundos. El valor predeterminado es 1,800 segundos.

> **Información**
>
> - Si el dispositivo está bloqueado, cambie **Auth Failure Lockout** a **Disable** y guarde. El dispositivo se desbloquea de inmediato. Sin embargo, cambiar **2nd Lockout Duration** a **Disable** y guardar no desbloquea el dispositivo.
> - Se incluye soporte para la opción **Auth Failure Lockout** en el firmware de BioStation 3 1.5.0 o posterior.

Agregar modo de autenticación

Configure el modo de autenticación del dispositivo en la opción **Auth Mode**. Configure el modo de autenticación combinando credenciales como huella digital, ID, tarjeta, PIN y rostro.

1. En la opción **Auth Mode**, haga clic en + **Add**.
2. Cuando aparezca la ventana **Add New Auth Mode**, arrastre el modo de autenticación deseado al área central.



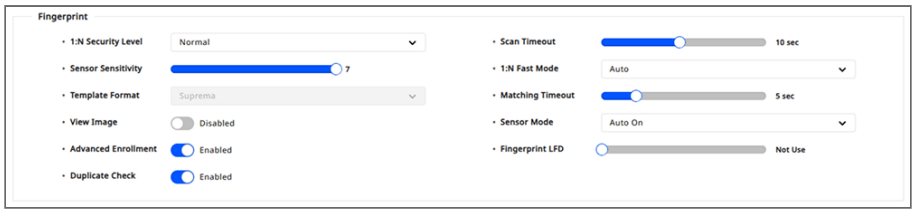
Agregue hasta cinco modos de autenticación.

3. Seleccione el elemento deseado en la opción **Schedule**.
4. Cuando finalices la configuración, haz clic en **Apply**.

> **Información**
>
> Si el horario deseado no está disponible en la opción **Schedule**, haga clic en + **Add New Schedule** para agregar un nuevo horario. Agregue un nuevo horario. Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

Configuración de autenticación de huellas dactilares

En el grupo **Fingerprint**, configure los detalles relacionados con la autenticación de huellas dactilares del dispositivo.



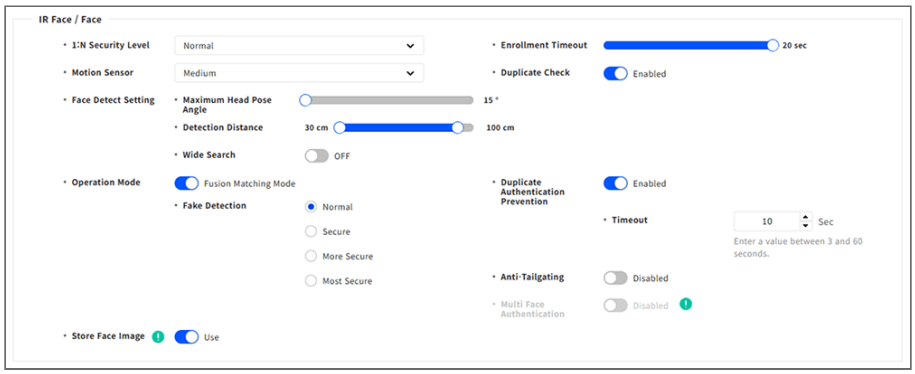
- **1:N Security Level**: Establezca el nivel de seguridad utilizado para autenticar huellas dactilares. Los niveles de seguridad más altos incrementan la tasa de rechazo falso (FRR) pero disminuyen la tasa de aceptación falsa (FAR).
- **Scan Timeout**: Establezca el tiempo de espera para el escaneo de huellas dactilares. Si no se escanea dentro del tiempo establecido, la autenticación fallará.
- **Sensor Sensitivity**: Establezca la sensibilidad del sensor de reconocimiento de huellas dactilares. Establece la sensibilidad más alta para obtener información de huella dactilar precisa.
- **1:N Fast Mode**: Establezca la velocidad de autenticación de huellas dactilares. Cuando se selecciona **Automatic**, se ajusta el rendimiento de la autenticación según el total de plantillas de huellas dactilares registradas en el dispositivo.

- **Template Format**: Vea el formato de plantilla de huella dactilar configurado.
- **Matching Timeout**: Establezca el tiempo de espera para la comparación de huellas dactilares. Si la autenticación no se completa dentro del tiempo especificado, fallará.
- **View Image**: Muestre las imágenes de huellas dactilares en la pantalla durante la autenticación.
- **Sensor Mode**: Establezca el modo de funcionamiento del sensor de huellas dactilares.
  - **Auto On**: El sensor de huellas dactilares se enciende al reconocer el dedo del usuario.
  - **Always On**: El sensor de huellas dactilares permanece siempre encendido.
- **Advanced Enrollment**: Evalúe la calidad de las huellas dactilares escaneadas para guardar información de alta calidad. Establézcalo en **Use** para notificar al usuario si la calidad de la huella dactilar es baja y ayudar a escanearla correctamente.
- **Fingerprint LFD**: Establezca el nivel para la detección de huellas dactilares falsas. Niveles más altos de detección de huellas falsas pueden aumentar las tasas de rechazo de las huellas reales.
- **Duplicate Check**: Verifique registros duplicados al enrolar huellas dactilares.

> **Información**
>
> - Las opciones disponibles para la configuración pueden variar según el tipo de dispositivo.
> - Cambiar la opción **Template Format** en los ajustes de autenticación por huella digital hará que todas las huellas almacenadas previamente queden inutilizables. Asegúrate de seleccionar una plantilla en la opción **Template Format** antes de enrolar las huellas de los usuarios.
> - La opción **View Image** es compatible con BioStation 3 Max (BS3M-ODB, BS3M-OAPB), X-Station 2 (XS2-ODPB, XS2-OAPB), FaceStation F2 (FSF2-ODB), BioLite N2, BioStation L2, BioStation A2 y BioStation 2.
> - La opción **Fingerprint LFD** es compatible con BioStation 3 Max (BS3M-ODB, BS3M-OAPB), X-Station 2 (XS2-ODPB, XS2-OAPB), FaceStation F2 (FSF2-ODB), BioLite N2, BioStation L2, BioStation A2 y BioEntry W2.

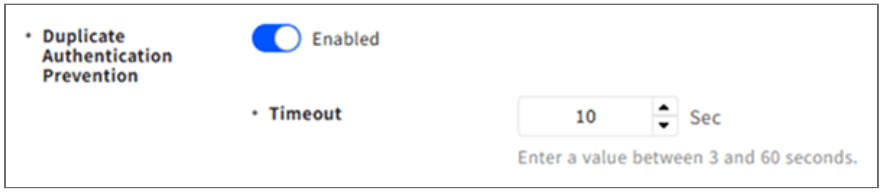
Ajustes de autenticación facial

En el grupo **IR Face / Face** o **Face**, puedes configurar los ajustes de autenticación facial del dispositivo.



- **1:N Security Level**: Define el nivel de seguridad utilizado para autenticar rostros. Los niveles de seguridad más altos incrementan la tasa de rechazo falso (FRR) pero disminuyen la tasa de aceptación falsa (FAR).
- **Enrollment Timeout**: Si el rostro del usuario no se enrola dentro del tiempo establecido al registrarlo, el enrolamiento se cancelará.
- **Motion Sensor**: Define la sensibilidad para detectar movimiento alrededor del dispositivo.

- **Ambient Brightness**: El dispositivo puede detectar la luminosidad ambiental y ajustar la intensidad del LED IR.
- **Enhanced fake face enrollment block**: Ajusta el nivel de detección de rostros falsos. Incrementar el nivel de detección de rostros falsos puede aumentar la tasa de rechazo de rostros reales.
- **Light Brightness**: Ajusta manualmente el brillo de la luz del dispositivo. Define el brillo seleccionando **Normal** o **High**, o selecciona **Not Use** para apagar la luz.
- **Quick Enrollment**: Define si se habilita el enrolamiento rápido de rostros.
  - **Enable**: Configura el procedimiento de enrolamiento de rostros en un solo paso.
  - **Disabled**: Configura el procedimiento de enrolamiento de rostros en 3 pasos. Establece **Disabled** para enrolar plantillas de rostros de alta calidad.
- **Duplicate Check**: Verifica registros duplicados al enrolar rostros.
- **Face Detect Setting**: Configura los ajustes ambientales para reconocer el rostro del usuario durante la autenticación.
  - **Maximum Head Pose Angle**: Define el ángulo máximo de rotación permitido para el rostro.
  - **Detection Distance**: Define las distancias mínima y máxima para reconocer el rostro.
  - **Wide Search**: Establece **ON** para permitir el reconocimiento facial en toda la vista de la cámara.
- **Operation Mode**: Define el modo de operación del dispositivo durante la autenticación facial.
  - **Fusion Matching Mode**: Realiza emparejamiento visual e infrarrojo para mejorar la precisión de la autenticación facial.
  - **Fast Matching Mode**: Permite la autenticación rápida de usuarios que caminan dentro del rango de autenticación del dispositivo.
- **Fake Detection**: Evita la autenticación de usuarios mediante rostros falsos, como fotografías. Se activa cuando la opción **Operation Mode** está configurada en **Fusion Matching Mode**.
- **Store Face Image**: Almacena tanto la imagen facial real como una plantilla que contiene únicamente los datos de las características extraídas. Desactive esta opción si no desea almacenar la imagen real.
- **Duplicate Authentication Prevention**: Configure la opción para evitar autenticaciones duplicadas cuando el dispositivo detecta de nuevo el rostro del mismo usuario pronto. Configure esta opción como **Enable** y configure **Timeout** en 3~60 segundos.



> Este ajuste se aplica a **Anti-Tailgating** y **Multi Face Authentication**, independientemente de la opción que habilite.

- **Anti-Tailgating**: Si la cámara detecta 2 o más rostros al mismo tiempo dentro del rango de captura de la cámara del dispositivo, lo considera tailgating y detiene la autenticación.
- **Multi Face Authentication**: Autentica a varios usuarios en secuencia dentro de la vista de la cámara.

- Esta opción requiere una licencia de dispositivo independiente. Los dispositivos sin licencia no pueden habilitar esta opción. Para obtener más información, consulte Licencia de dispositivo.
- Configure esta opción en **Use** para usar solo autenticación facial, independientemente del ajuste **Auth Mode**.
- Los dispositivos que usan esta opción no pueden usar **T&A** ni **Server Private Message**.

Información

- Las opciones disponibles para la configuración pueden variar según el tipo de dispositivo.
- Las opciones **Ambient Brightness**, **Enhanced fake face enrollment block** y **Quick Enrollment** son compatibles con los modelos FaceStation 2 y FaceLite.
- La opción **Light Brightness** es compatible con firmware FaceStation F2 versión 1.1.0 o superior.
- Las opciones **Face Detect Setting** y **Operation Mode** son compatibles con los modelos BioStation 3 Max, BioStation 3 y FaceStation F2.
- No configure **Anti-Tailgating** y **Multi Face Authentication** en **Use** al mismo tiempo. Configure una opción en **Use**; la otra cambia automáticamente a **Not Use**.
- Configure **Duplicate Authentication Prevention** y **Multi Face Authentication** solo en el dispositivo maestro. Configure la opción **Anti-Tailgating** por separado en los dispositivos maestro y esclavo.
- El soporte para **Duplicate Authentication Prevention**, **Anti-Tailgating** y **Multi Face Authentication** puede variar según el modelo del dispositivo y la versión de firmware.
  - Versión de firmware 1.5.0 o posterior para BioStation 3

Ajustes de QR/código de barras

En el grupo **QR/Barcode**, puedes configurar los detalles para la autenticación mediante QR/código de barras en el dispositivo.



- **Use QR/Barcode through Camera** / **Use QR/Barcode**: Establece si se usará la autenticación por código QR o código de barras mediante la cámara del dispositivo.
- **Camera Timeout** / **Scan Timeout**: Establece el tiempo de espera del escaneo de la cámara. Si un QR/barcode no se escanea dentro del tiempo especificado, la autenticación fallará.
- **Use QR as Card**: Configura la autenticación de códigos QR con los mismos datos que las tarjetas CSN o Wiegand emitidas a los usuarios.
- **Motion Sensor**: Define la sensibilidad para detectar movimiento e iniciar el escaneo de la cámara.
- **Use QR/Barcode through Scanner**: Define si se utiliza el escáner del dispositivo para la autenticación QR/código de barras.
- **Scanner Timeout**: Define el tiempo de espera de escaneo. Si un QR/barcode no se escanea dentro del tiempo especificado, la autenticación fallará.
- **LED Light**: Establece si se utilizará la iluminación LED del dispositivo al autenticar códigos QR.

Información

- La opción **Use QR/Barcode through Camera** requiere una licencia de dispositivo independiente. Para obtener más información, consulte Licencia de dispositivo.
- Los dispositivos que admiten las opciones **Use QR/Barcode through Camera**, **Camera Timeout**, **Use QR as Card** y **Motion Sensor** son los siguientes.
  - BioStation 3 Max: versión de firmware 1.0.0 o superior
  - Versión de firmware 1.1.0 o posterior para BioStation 3
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) versión de firmware 1.2.0 o superior
  - X-Station 2 (XS2-QDPB, XS2-QAPB) versión de firmware 1.4.1 o superior
- Los dispositivos que admiten las opciones **Use QR/Barcode through Scanner** y **Scanner Timeout** son los siguientes.
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- Las opciones **Use QR/Barcode**, **Scan Timeout** y **LED Light** son compatibles con los siguientes dispositivos.
  - Firmware de XPass Q2, versión 1.0.0 o posterior

Ajustes de autenticación con tarjeta

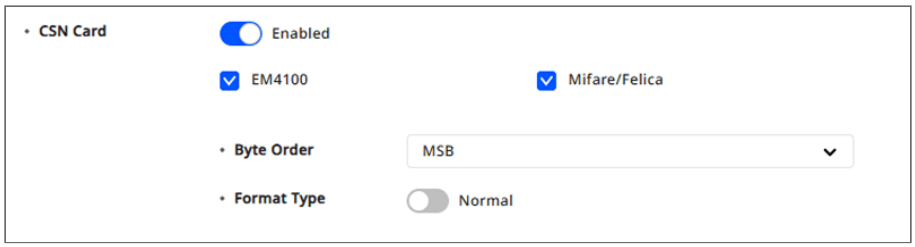
En el grupo **Card Type**, puedes definir los tipos de tarjetas que se usarán en el dispositivo.

Información

Solo se mostrarán en el grupo **Card Type** los tipos de tarjeta compatibles con el dispositivo.

CSN Card

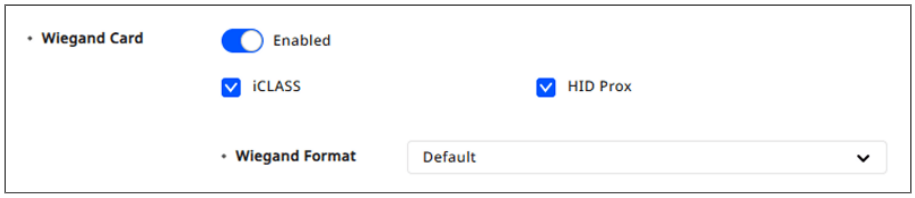
Puedes seleccionar los tipos y formatos de tarjetas CSN y definir el orden de bytes.



- **Byte Order**
  - **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).
- **Format Type**
  - **Normal**: Lee y muestra el número de serie (CSN) de la tarjeta sin conversión adicional.
  - **Wiegand**: Transforma y muestra el número de serie (CSN) de la tarjeta según el formato Wiegand definido por el usuario. Consulte Configurar Formato de Tarjeta Wiegand para configurar un nuevo formato Wiegand.

Wiegand Card

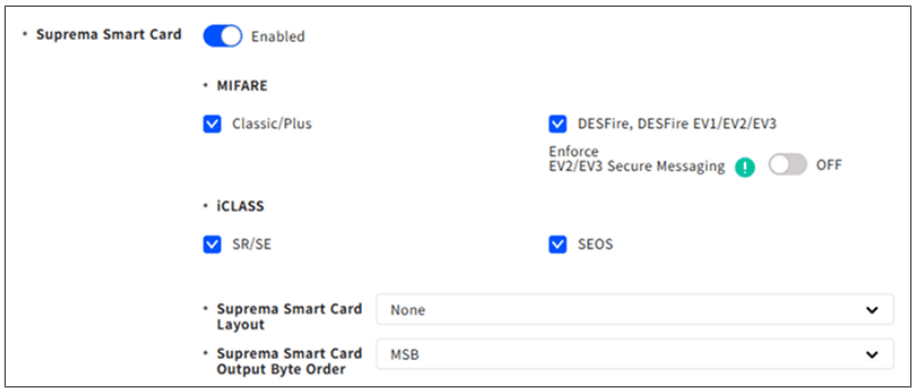
Selecciona los tipos de tarjetas Wiegand y define los formatos Wiegand. Elija el formato Wiegand que se utilizará en la opción **Wiegand Format**.



> **Información**
>
> Consulte Configurar Formato de Tarjeta Wiegand para configurar un nuevo formato Wiegand.

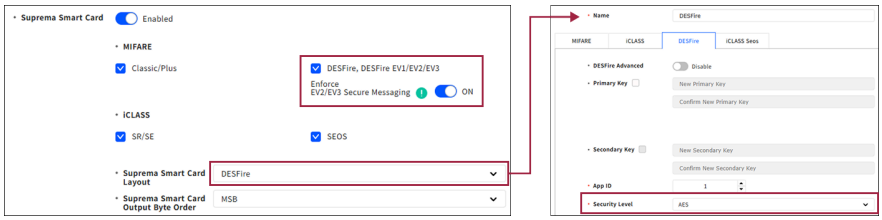
Suprema Smart Card

Seleccione los tipos de tarjetas inteligentes Suprema y configure la estructura y el orden de bytes de la tarjeta.



- **Enforce EV2/EV3 Secure Messaging**: Establezca esta opción en **ON** para autenticar solo con tarjetas compatibles con mensajería segura EV2 (DESFire EV2/EV3). El dispositivo rechaza las tarjetas DESFire EV1 que no admiten mensajería segura EV2.

  Esta opción está disponible cuando selecciona **DESFire, DESFire EV1/EV2/EV3** y el **Security Level** de la **Suprema Smart Card** seleccionada es **AES**. Si **Suprema Smart Card** no está en uso, esta opción aparece como **OFF**.

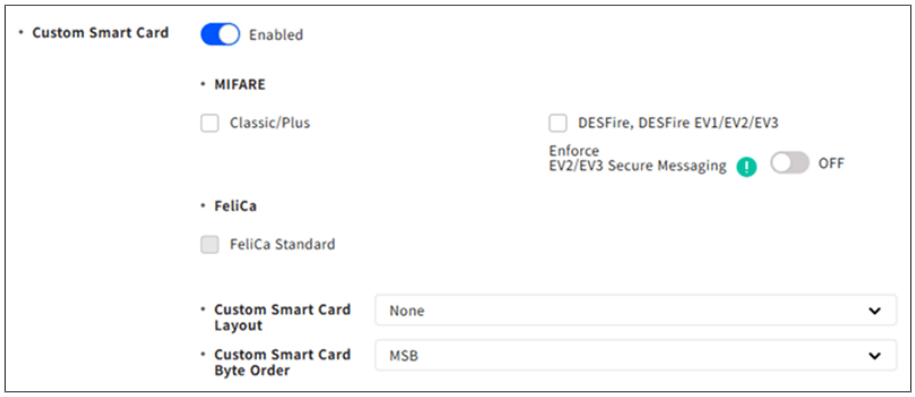


- **Suprema Smart Card** y **Custom Smart Card** comparten los mismos ajustes. Si alguno está en uso, aparece un mensaje de confirmación al cambiar cualquiera de los valores. Haga clic en **Ok** en el cuadro de diálogo para cambiar ambas opciones a la vez. Si alguna de las opciones no usa una tarjeta inteligente, cambie el valor sin un cuadro de diálogo de confirmación.
- La mensajería segura está disponible solo en tarjetas DESFire EV2 y EV3. Habilite DESFire y establezca el tipo de cifrado del diseño de la tarjeta en AES.
- Si el dispositivo no admite mensajería segura EV2, no aparece la opción **Enforce EV2/EV3 Secure Messaging**.
- Para establecer esta opción en varios dispositivos, use **Device Batch Edit**. La edición por lotes excluye automáticamente los dispositivos que no admiten mensajería segura EV2.

- **Suprema Smart Card Layout**: Elija la estructura de tarjeta inteligente Suprema. Consulte Configurar Formato de Tarjeta Inteligente para configurar un nuevo formato de tarjeta inteligente.
- **Suprema Smart Card Output Byte Order**
  - **MSB**: Procesa los datos de la tarjeta en orden de unidades de bytes grandes a pequeñas.
  - **LSB**: Procesa los datos de la tarjeta en orden de unidades de bytes pequeñas a grandes.

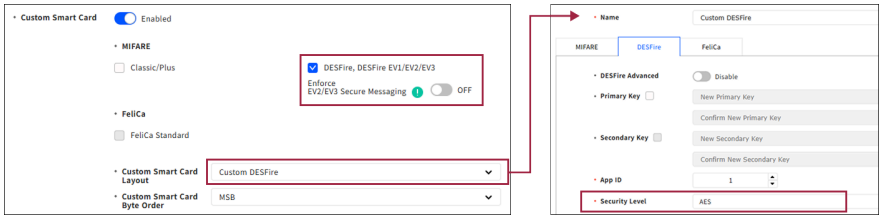
Custom Smart Card

Seleccione los tipos de tarjetas inteligentes personalizadas emitidas por terceros y configure la estructura y el orden de bytes de la tarjeta.



- **Enforce EV2/EV3 Secure Messaging**: Establezca esta opción en **ON** para autenticar solo con tarjetas compatibles con mensajería segura EV2 (DESFire EV2/EV3). El dispositivo rechaza las tarjetas DESFire EV1 que no admiten mensajería segura EV2.

  Esta opción está disponible cuando selecciona **DESFire, DESFire EV1/EV2/EV3** y el **Security Level** de la **Custom Smart Card** seleccionada es **AES**. Si **Custom Smart Card** no está en uso, esta opción aparece como **OFF**.



- **Suprema Smart Card** y **Custom Smart Card** comparten los mismos ajustes. Si alguno está en uso, aparece un mensaje de confirmación al cambiar cualquiera de los valores. Haga clic en **Ok** en el cuadro de diálogo para cambiar ambas opciones a la vez. Si alguna de las opciones no usa una tarjeta inteligente, cambie el valor sin un cuadro de diálogo de confirmación.
- La mensajería segura está disponible solo en tarjetas DESFire EV2 y EV3. Habilite DESFire y establezca el tipo de cifrado del diseño de la tarjeta en AES.
- Si el dispositivo no admite mensajería segura EV2, no aparece la opción **Enforce EV2/EV3 Secure Messaging**.
- Para establecer esta opción en varios dispositivos, use **Device Batch Edit**. La edición por lotes excluye automáticamente los dispositivos que no admiten mensajería segura EV2.

- **Custom Smart Card Layout**: Elija la estructura de tarjeta inteligente personalizada. Consulte Configurar Formato de Tarjeta Inteligente para configurar un nuevo formato de tarjeta inteligente.
- **Custom Smart Card Byte Order**
  - **MSB**: Procesa los datos de la tarjeta en orden de unidades de bytes grandes a pequeñas.
  - **LSB**: Procesa los datos de la tarjeta en orden de unidades de bytes pequeñas a grandes.

▼ Ver dispositivos y versiones de firmware que admiten tarjetas inteligentes personalizadas

- BioStation 3 Max: versión de firmware 1.3.0 o superior
- Firmware de XPass Q2, versión 1.0.0 o posterior
- BioEntry W3 versión de firmware 1.0.0 o superior
- BioStation 2a versión de firmware 1.1.0 o superior
- BioStation 3 versión de firmware 1.3.0 o superior
- X-Station 2 versión de firmware 1.3.0 o superior
- BioLite N2 versión de firmware 1.6.2 o superior
- XPass D2 versión de firmware 1.7.1 o superior
- BioEntry P2 versión de firmware 1.5.1 o superior
- BioEntry W2 versión de firmware 1.8.0 o superior

CSN Mobile

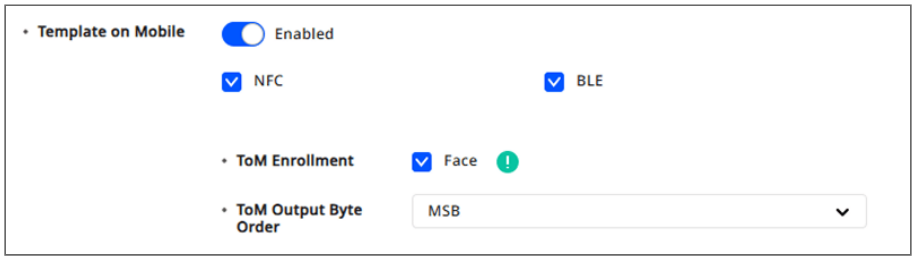
Configure el método para reconocer tarjetas móviles.



- **NFC**: Reconoce tarjetas móviles mediante comunicación NFC desde dispositivos móviles.
- **BLE**: Reconoce tarjetas móviles mediante comunicación Bluetooth Low Energy (BLE).

Template on Mobile

Especifique cómo funciona el reconocimiento en Template on Mobile y configure el orden de bytes para los biométricos enrolados directamente por el usuario en el dispositivo.



- **ToM Output Byte Order**
  - **MSB**: Procesa los datos de la tarjeta en orden de unidades de bytes grandes a pequeñas.
  - **LSB**: Procesa los datos de la tarjeta en orden de unidades de bytes pequeñas a grandes.

▼ **Ver dispositivos y versiones de firmware que admiten plantillas en el móvil**
- Firmware de BioStation 3 Max, versión 1.0.0 o posterior
- BioEntry W3 versión de firmware 1.0.0 o superior
- BioStation 3 versión de firmware 1.2.0 o superior

Configuración de autenticación por PIN

En el grupo **PIN**, active o desactive la opción **Scramble Keypad** para la autenticación por PIN del dispositivo.



Información

La opción **Scramble Keypad** solo está disponible en los productos Suprema que admiten interfaces de usuario a través de la pantalla LCD.

Configuración Avanzada

Esta sección ofrece orientación para configurar elementos en los ajustes de **Advanced**. Consulte cómo configurar diversas funciones avanzadas, como Master Administrator, gestión de permisos de administrador, eventos de asistencia, pantalla y sonido, condiciones de funcionamiento y acciones, registros de imágenes, Wiegand, tamper de seguridad y el significado de cada opción. Aplique los ajustes adecuados para su entorno para gestionar el dispositivo de forma eficaz.

Información

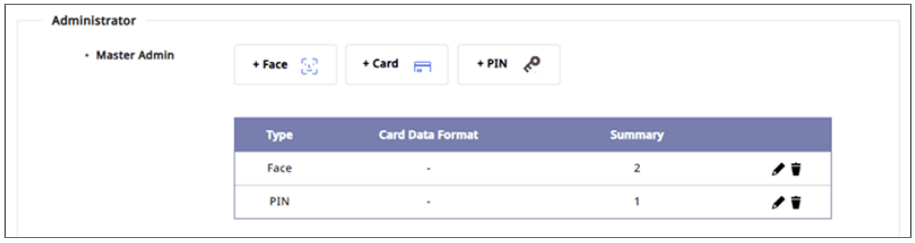
- Las opciones de red disponibles pueden variar según el tipo de dispositivo.
- Si el usuario ha realizado cambios, haga clic en **Apply**. Los cambios no se aplicarán al dispositivo si no se guardan.

Agregar administrador maestro productos CE

La función **Master Admin** mejora los permisos de administrador global del dispositivo para aumentar la seguridad y evitar el acceso y los cambios de ajustes no autorizados. Un dispositivo nuevo debe registrar un Master Administrator mediante

esta función, y solo el Master Administrator registrado puede acceder al menú de administrador y cambiar ajustes.

Seleccione dos tipos de credenciales para enrolar en el menú **Advanced** → **Administrator Master Admin**.



Las credenciales que se pueden enrolar como **Master Admin** son las siguientes:

Tipo de credencial	Número de enrolamientos	Condiciones
tarjeta	Hasta 4	Solo admite los tipos CSN y Wiegand y no puede enrolar duplicados del mismo tipo.
Rostro	Hasta 2	Solo se puede enrolar en dispositivos equipados con el mismo algoritmo.
Huella	Hasta 2	-
PIN	1	Debe ingresar al menos 8 dígitos.

- Para cambiar la credencial enrolada, haga clic en el botón ✎ a la derecha de esa credencial.
- Para eliminar la credencial enrolada, haga clic en el botón 🗑 a la derecha de esa credencial.

Precaución

Esta característica está disponible solo en **productos CE** que admiten una interfaz de usuario LCD. Para obtener más información sobre los dispositivos compatibles y las versiones de firmware, consulte Guía de configuración de Master Admin.

Condiciones de enrolamiento

- Debe enrolar al menos dos tipos de credenciales.
- Estas mismas condiciones se aplican a todos los dispositivos con firmware actualizado que admiten administradores maestros.
- Todas las credenciales compatibles con el dispositivo pueden utilizarse como medios de autenticación.

Información

- Esta función solo está disponible en productos Suprema que admiten interfaces de usuario mediante pantallas LCD.
- Los dispositivos existentes que han tenido su firmware actualizado no muestran el menú **Master Admin** en la configuración del dispositivo de BioStar X.
- Ciertos dispositivos no incluyen el ajuste **Master Admin** (por ejemplo, dispositivos con firmware actualizado). Use la opción **Two-step Authentication** para mejorar los permisos de administrador. Según el dispositivo, la opción **Two-step Authentication** puede no aparecer.
- El dispositivo almacena las credenciales del administrador maestro por separado y las gestiona independientemente de los PIN de usuario. Cambiar o eliminar un PIN de usuario no afecta las credenciales del administrador maestro.

Configuración de autenticación en dos pasos

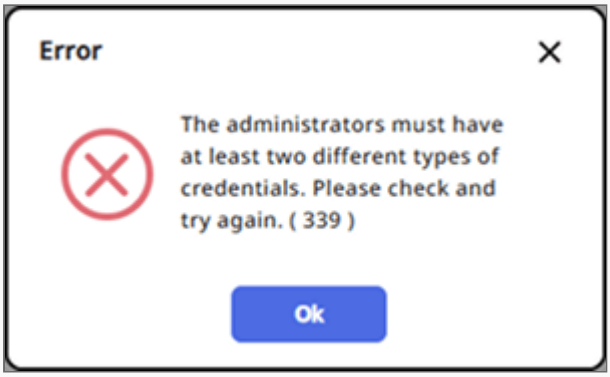
Después de actualizar el firmware en un dispositivo global que no admite **Master Admin**, habilite la opción **Two-step Authentication**. Esto otorga permisos completos de administrador y mejora la seguridad.



Si configura la opción **Two-step Authentication** en **Use**, deberá utilizar dos o más credenciales para la autenticación de administrador global en el dispositivo. Por ejemplo, si se han enrolado una tarjeta y un PIN, deberá escanear la tarjeta e ingresar el PIN para autenticar correctamente durante la autenticación de administrador global.

Información

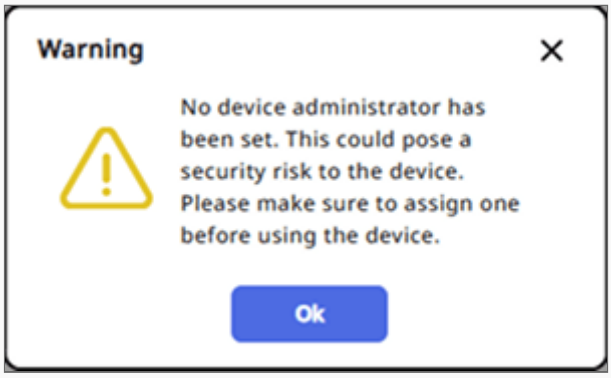
- Si los administradores tienen menos de 2 tipos de credenciales enroladas, la activación falla y aparece un mensaje de error. Enrole 2 o más tipos de credenciales para todos los administradores e inténtelo nuevamente.



- Según el dispositivo, **Two-step Authentication** puede no aparecer, pero el ajuste habilitado previamente permanece activo. BioStar X no permite desactivar este ajuste. Póngase en contacto con Equipo de Soporte Técnico global de Suprema.

Precaución

Si el administrador global no está establecido en el dispositivo, aparecerá el siguiente mensaje emergente. Agregue administradores para todos los permisos en **Advanced** → **Administrator**.

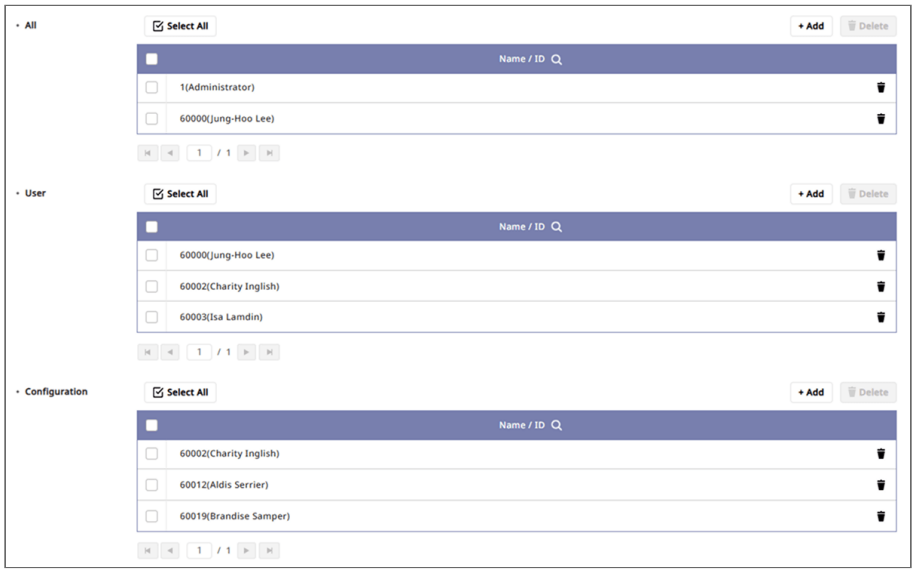


Alerta

Si se activa **Two-step Authentication** y luego se eliminan las credenciales de todos los administradores hasta quedar con menos de dos tipos, no se podrá acceder al menú de administrador en el dispositivo cuando no sea posible conectarse a **BioStar X**. Por lo tanto, tenga especial cuidado al eliminar credenciales de administrador.

Agregar administradores

En el grupo **Administrator**, gestione los administradores del dispositivo por nivel de permiso.



Para agregar un administrador por nivel de permiso, haga clic en el botón **+ Add**. Cuando aparezca la lista de usuarios, seleccione el usuario deseado. Busque también al usuario deseado haciendo clic en el botón en la lista de usuarios.

Consulte los permisos para cada nivel a continuación.

Nivel	Gestión de información del usuario	Configuración del Dispositivo
All	✔	✔

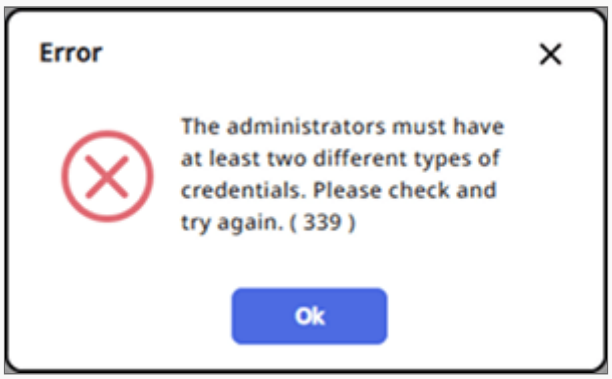
Nivel	Gestión de información del usuario	Configuración del Dispositivo
User	✔	✕
Configuration	✕	✔

Información

- Se pueden agregar hasta 1,000 administradores. La cantidad de administradores que se pueden agregar puede variar según la versión del firmware del dispositivo.
- Para buscar al usuario enrolado, haga clic en el botón en **Name / ID**.
- **Device Settings** permite cambiar ajustes de pantalla y sonido, red, RS-485, etc.
- Para eliminar un administrador, haga clic en el botón a la derecha del administrador.
- Los administradores establecidos para cada dispositivo no afectan los permisos de **BioStar X**.
- Si un administrador enrolado en un dispositivo con administradores maestros (**productos CE**) tiene un PIN de menos de 8 dígitos. Enrole el PIN de nuevo con al menos 8 dígitos. Para más información sobre cómo enrollar códigos PIN, consulte Inscribir PIN.
- Primero, elimine al usuario de los roles de administrador en todos los dispositivos. Luego, cambie el PIN a 4 dígitos para el usuario con permisos de **Configuration**.

Precaución

Si el usuario que se asigna como administrador del dispositivo tiene menos de 2 tipos de credenciales enrolladas, aparece un mensaje de error. Enrole 2 o más tipos de credenciales para todos los administradores e inténtelo nuevamente.



Gestionar el enrolamiento de administradores para usuarios eliminados

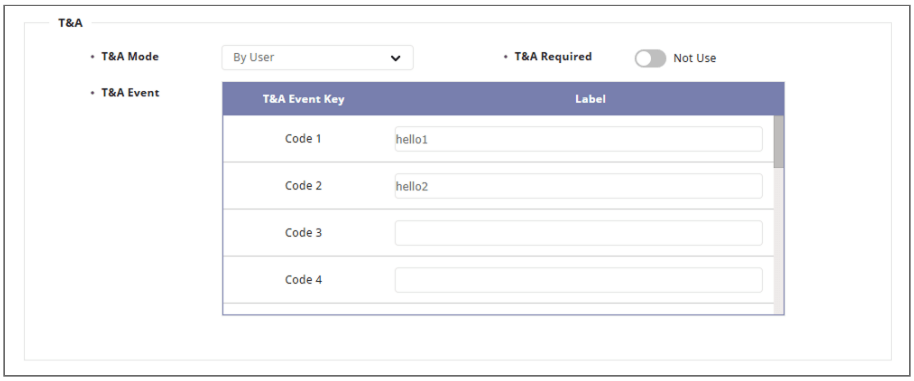
Si la lista de administradores del dispositivo incluye un usuario eliminado de **BioStar X**, aparece una ventana emergente al guardar los ajustes. Haga clic en **Apply** en la parte inferior de la pantalla.



- **Yes**: Elimine el usuario eliminado de la lista de administradores y guarde los ajustes.
- **No**: Cancele el guardado.

Gestión de asistencia

El grupo **T&A** permite cambiar los nombres de eventos de asistencia o establecer modos de asistencia.

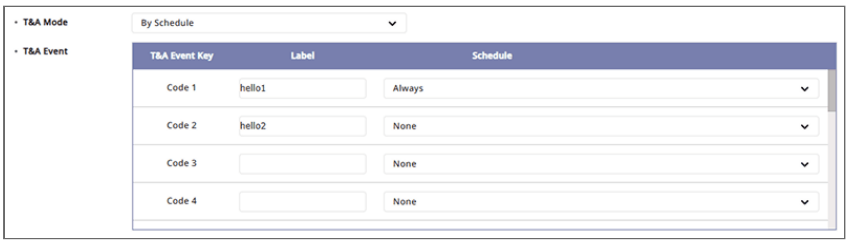


- **T&A Mode**: Establece cómo se registran los eventos de asistencia.
  - **Not Use**: No se pueden registrar eventos de asistencia.
  - **By User**: El usuario puede seleccionar el evento de asistencia deseado al autenticarse.
  - **By Schedule**: Los eventos de asistencia cambian automáticamente según un horario establecido. Seleccione un horario para aplicar a los eventos de asistencia.
  - **Last Choice**: El último evento de asistencia utilizado puede seguir usándose.
  - **Fixed**: Solo se puede usar el evento de asistencia seleccionado. Elija el evento de asistencia fijo que desea usar.
- **T&A Required**: Configura que se requiera al usuario registrar un evento de asistencia al autenticarse.

  > Esta opción puede usarse cuando la opción **T&A Mode** está configurada en **By User**.

- **T&A Event**: Modifique los nombres de los eventos de asistencia o agregue horarios cuando la opción **T&A Mode** esté configurada en **By Schedule**.
  - **T&A Event Key**: Lista de claves que se pueden usar para registrar asistencia.
  - **Label**: Cambie el nombre del evento de asistencia según **T&A Event Key**.

– **Schedule**: Configure un horario para cambios automáticos cuando la opción **T&A Mode** esté configurada en **By Schedule**.



Información

- Los dispositivos sin pantalla LCD pueden establecer los modos de asistencia en **Fixed** y **By Schedule** y pueden registrar eventos de asistencia fijos o eventos de asistencia que cambien según un horario preestablecido. Los dispositivos compatibles son XPass Q2, XPass 2, XPass D2, BioEntry P2 y BioEntry W2.
- Para obtener más información sobre cómo configurar un nuevo horario, consulte Ajustes de Horario.
- Establecer **Multi Face Authentication** en **Use** en el dispositivo desactiva la gestión de tiempo y asistencia. Para obtener más información sobre **Multi Face Authentication**, consulta Configuración de Autenticación.

Ajustes de pantalla y sonido

Cambie los ajustes relacionados con la pantalla y el sonido del dispositivo. Las opciones disponibles pueden variar según el dispositivo.

▼ **XPass 2, XPass D2, BioEntry P2, BioEntry W2**

- **Sound**: Active o desactive el sonido.
- **LED/Buzzer**: Seleccione y configure los elementos de evento que activarán el LED o el zumbador.
- **Keypad Backlight**: Active o desactive la retroiluminación del teclado. Cuando esta opción está activada, la luz detrás del teclado se enciende, lo que facilita identificar las teclas en entornos oscuros. Identifique fácilmente las teclas incluso en entornos oscuros.

La opción **Keypad Backlight** está disponible en el hardware XPass D2 V02M y en la versión de firmware 1.7.1 o superior.

▼ **FaceLite, BioLite N2, BioStation L2, BioStation 2**

- **Language**: Configure el idioma que se mostrará en la pantalla del dispositivo. Haga clic en **Update Resource** para enviar archivos de recursos de idioma al dispositivo.
- **Device Volume**: Defina el nivel de sonido predeterminado que produce el dispositivo.
- **Menu Timeout**: Defina el tiempo que tarda en pasar de la pantalla de menú a la pantalla inactiva.
- **Theme**: Cambie el estilo de la pantalla de inicio del dispositivo.
- **Backlight Timeout**: Establezca el tiempo antes de que la luz de la pantalla se apague automáticamente.
- **Message Timeout**: Establezca el tiempo antes de que los mensajes desaparezcan automáticamente.
- **Voice Instruction**: Utilice la guía por voz en lugar de tonos de notificación.

- **Background**: Defina los elementos que se mostrarán en el fondo de la pantalla de inicio del dispositivo.
  - **Logo**: Los usuarios pueden mostrar las imágenes que registraron en la pantalla de inicio del dispositivo. Haga clic en **Add** para registrar una imagen.
  - **Notice**: Los administradores pueden mostrar sus entradas en la pantalla de inicio.
  - **Slide Show**: Los usuarios pueden mostrar hasta 10 imágenes registradas como presentación de diapositivas en la pantalla de inicio. Haga clic en **Add** para registrar una imagen.

  > – Haga clic en **Update** para reflejar los cambios en tiempo real en el dispositivo.
  > – Si cambia el tipo de fondo de pantalla, hacer clic en **Update** no lo aplicará al dispositivo. En la parte inferior de la pantalla, haga clic en **Apply**.
  > – Las opciones **Notice** y **Slide Show** son compatibles con el modelo BioStation 2.

- **Sound**: Configure los efectos de sonido que se reproducirán al iniciar, al autenticar correctamente y al fallar la autenticación. Seleccione archivos **.wav* de hasta 500 Kb de tamaño. Haga clic en **Browse**.

  > Haga clic en **Update** para reflejar los cambios en tiempo real en el dispositivo.

▼ **BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceStation 2, BioStation A2**

- **Language**: Configure el idioma que se mostrará en la pantalla del dispositivo. Haga clic en **Update Resource** para enviar archivos de recursos de idioma al dispositivo.
- **Device Volume**: Defina el nivel de sonido predeterminado que produce el dispositivo.
- **Intercom Speaker Volume**: Defina el volumen de salida de sonido del dispositivo cuando utilice la función de intercom IP.
- **Intercom Microphone Volume**: Defina el volumen de entrada de sonido al dispositivo cuando utilice la función de intercom IP.
- **Menu Timeout**: Defina el tiempo que tarda en pasar de la pantalla de menú a la pantalla inactiva.
- **Backlight Timeout**: Establezca el tiempo antes de que la luz de la pantalla se apague automáticamente.
- **Message Timeout**: Establezca el tiempo antes de que los mensajes desaparezcan automáticamente.
- **Server Private Message**: Defina si se utilizará un mensaje privado que se mostrará en pantalla cuando el usuario se autentique.

  > Establecer **Multi Face Authentication** en **Use** en el dispositivo desactiva esta opción. Para obtener más información sobre **Multi Face Authentication**, consulta Configuración de Autenticación.

- **Voice Instruction**: Utilice la guía por voz en lugar de tonos de notificación.
- **Home Screen**: Defina los elementos que se mostrarán en el fondo de la pantalla de inicio del dispositivo.
  - **Normal**: Muestra la imagen predeterminada en la pantalla de inicio.
  - **Logo**: Los usuarios pueden mostrar las imágenes que registraron en la pantalla de inicio del dispositivo. Haga clic en **Add** para registrar una imagen.
  - **Notice**: Los administradores pueden mostrar sus entradas en la pantalla de inicio.

> – Haga clic en **Update** para reflejar los cambios en tiempo real en el dispositivo.
> – Si cambia el tipo de fondo de pantalla, hacer clic en **Update** no lo aplicará al dispositivo. En la parte inferior de la pantalla, haga clic en **Apply**.
> – Configurar la pantalla de inicio como **Logo** y **Slide Show** permite mostrar hasta 10 imágenes como presentación de diapositivas en la pantalla de inicio. Haga clic en **Add** para registrar una imagen.

- **Sound**: Configure los efectos de sonido que se reproducirán al iniciar, al autenticar correctamente y al fallar la autenticación. Seleccione archivos **.wav* de hasta 500 Kb de tamaño. Haga clic en **Browse**.

> Haga clic en **Update** para reflejar los cambios en tiempo real en el dispositivo.

- **Default Idle Screen**: Seleccione la pantalla en espera que aparece cuando el dispositivo no está en uso.
  – **Screen Saver**: Muestra el protector de pantalla como pantalla en espera.
  – **Home Screen**: Muestra la opción seleccionada en **Home Screen**.

> – Esta opción es compatible con BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2 y FaceStation 2.
> – Para obtener más información sobre la opción **Play Video**, consulte Reproducir un video en la pantalla en espera.

▼ XPass Q2

LED/Buzzer: Seleccione y configure los elementos de evento que activarán el LED o el zumbador.

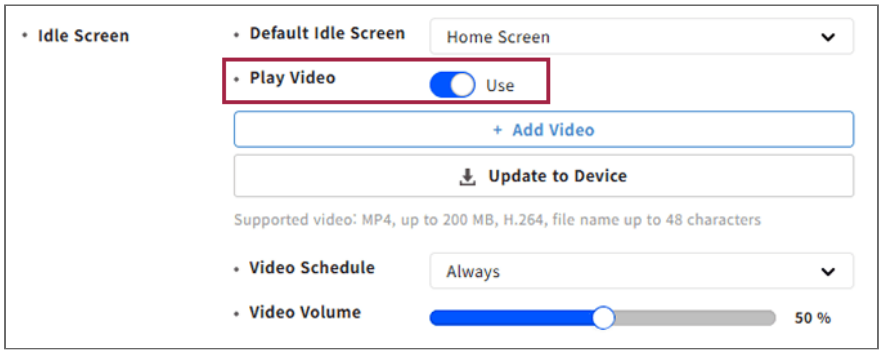
Reproducir un video en la pantalla en espera

> El firmware 1.1.0 o posterior de **BioStation 3 Max** admite el feature de reproducir videos en la pantalla en espera. Prepare el video antes de enviarlo al dispositivo.

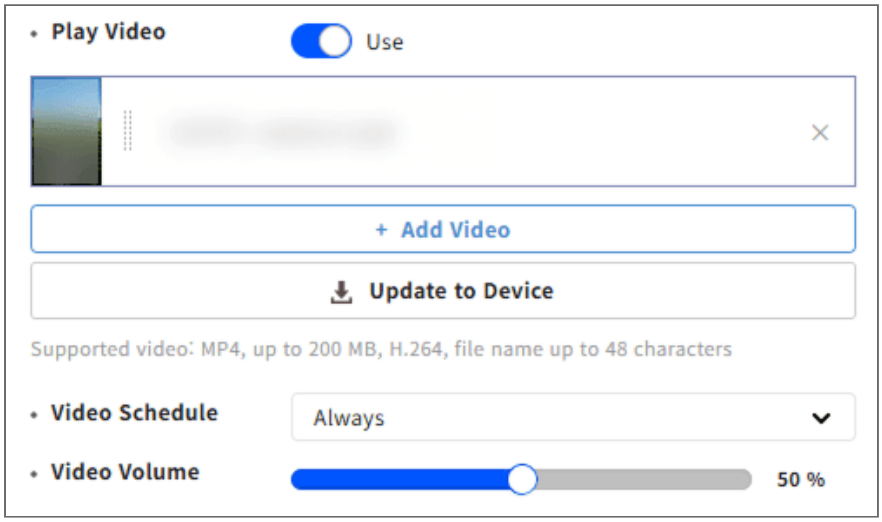
Agrega un video y transfiérelo al dispositivo

Configura el dispositivo para reproducir contenido específico en la pantalla de inactividad.

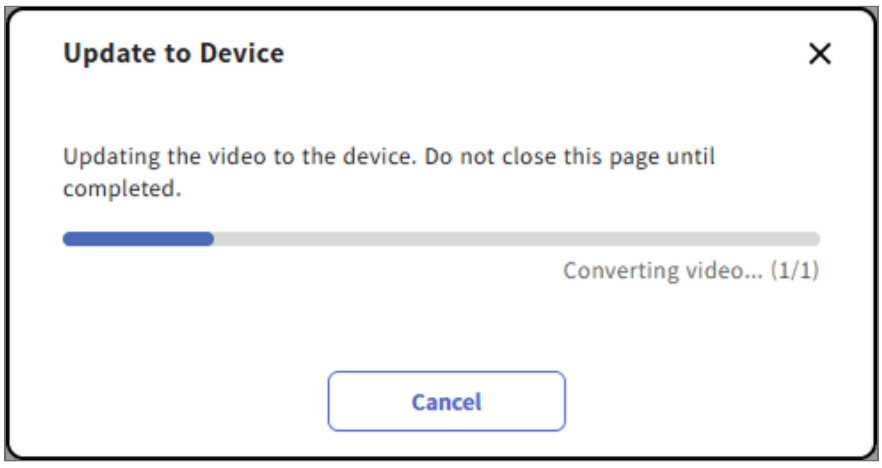
1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. En la lista de dispositivos, haz clic en **BioStation 3 Max**.
4. Ve a la sección **Advanced** → **Display/Sound**.
5. Opción **Idle Screen** → **Play Video**: configúrala como **Use**.



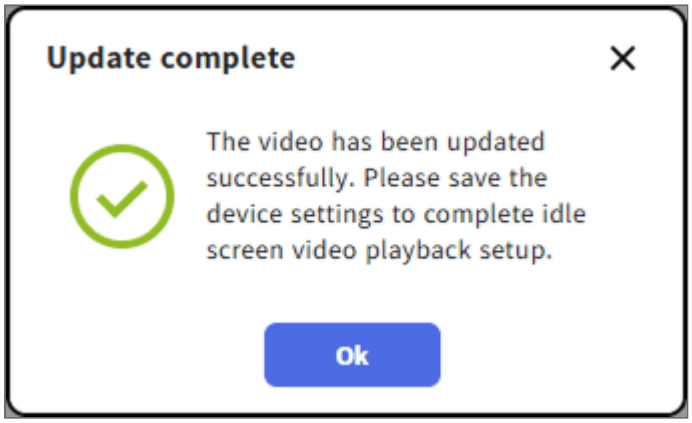
6. Haz clic en **Add Video**.
7. Selecciona el video guardado localmente.
8. Después de cargar el video, configura **Video Schedule** y **Video Volume**.



9. Haz clic en **Update to Device** para transferir el video cargado al dispositivo.
10. Aparece la ventana emergente de progreso de actualización. No cierres la página hasta que finalice la carga.



11. Cuando aparezca el mensaje de carga completada, haz clic en **Ok**.



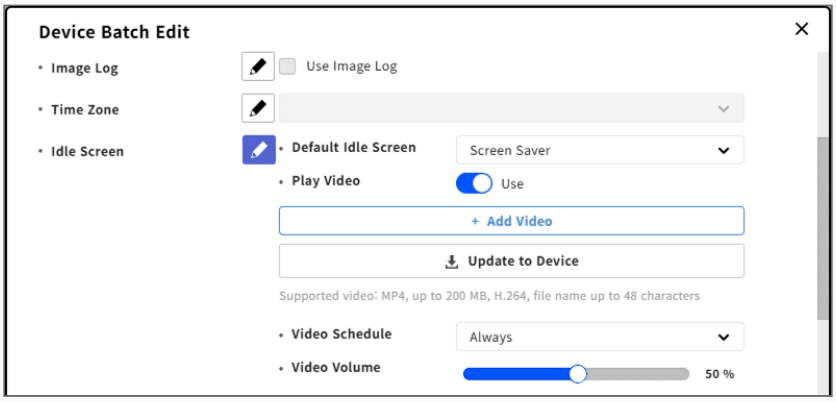
12. Haz clic en **Apply** en la parte inferior de la pantalla para guardar los cambios.

Información

- Los videos se reproducen solo cuando **Play Video** está configurado en **Use**, registras al menos 1 video y configuras el horario en **Video Schedule**. En los horarios que no cumplen estas condiciones, aparece la pantalla seleccionada en **Default Idle Screen**.
- El tamaño máximo del archivo de video compatible es de 200 MB y el formato es MP4 (H.264).
- El nombre del archivo de video puede tener hasta 48 caracteres. El nombre del archivo no puede incluir caracteres como punto(`.`), apóstrofo(`'`) o acento grave(`` ` ``).
- Agrega hasta 3 videos. Cuando agregas 3 videos, el botón **Add Video** se desactiva.
- Si el dispositivo se conecta como esclavo (mediante RS-485), no puedes agregar, eliminar ni transferir videos.
  - Si el dispositivo maestro admite la reproducción de videos, la pantalla del esclavo muestra la lista del maestro en modo de solo lectura. La lista es de solo lectura. Agrega, elimina, transfiere y reordena videos solo en el dispositivo maestro.
  - Si el dispositivo maestro no admite la reproducción de video, la pantalla esclava solo muestra **Default Idle Screen**.

Consejo

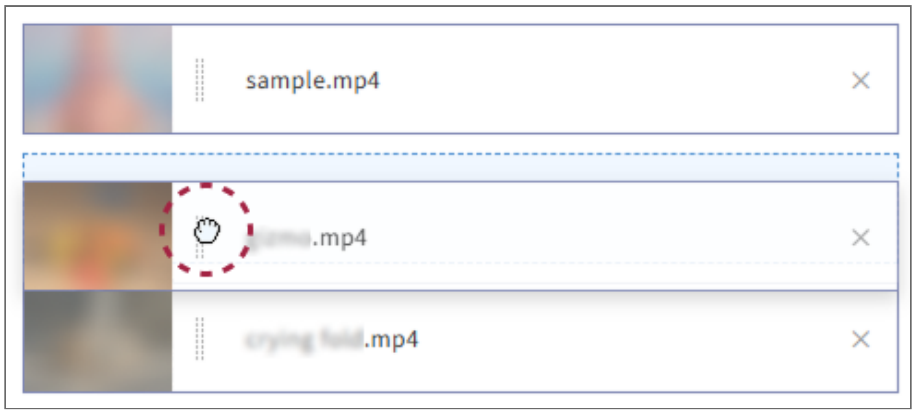
Use **Batch Edit** para agregar y transferir videos a varios dispositivos a la vez. Para obtener más información sobre la característica **Batch Edit**, consulte Usar la Función de Administración de Dispositivos.



Cambiar el orden de reproducción de videos

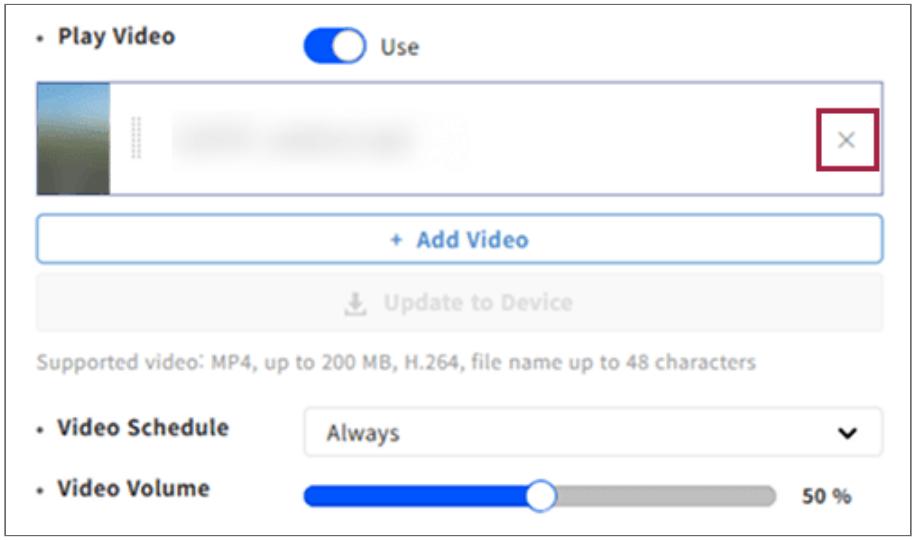
Arrastre el área a la derecha de una miniatura de video para cambiar el orden de reproducción. Para guardar los cambios,

haga clic en **Apply** en la parte inferior de la pantalla.



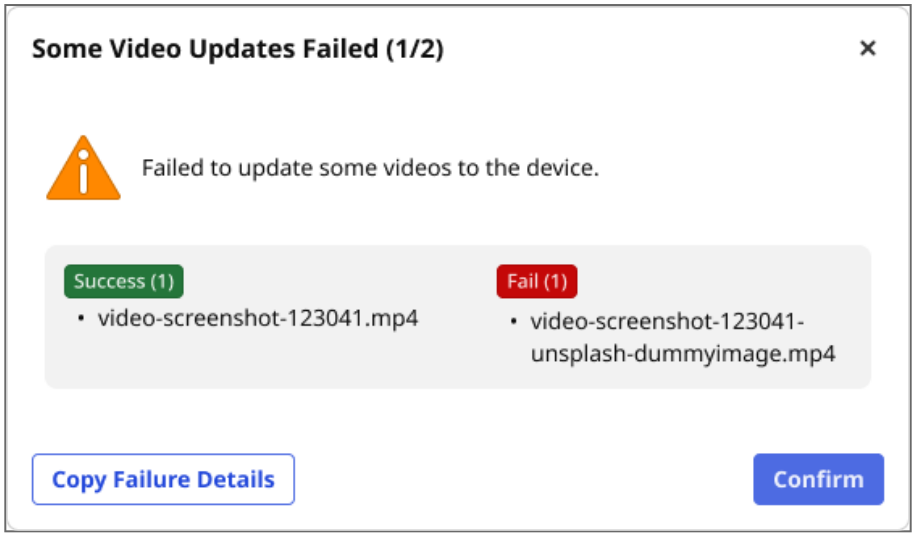
Eliminar videos

En **Idle Screen** → **Play Video**, haga clic en ✕ del video que va a eliminar. Luego, haga clic en **Update to Device**. Haz clic en **Apply** en la parte inferior de la pantalla para guardar los cambios.



Falla de transferencia de video

Si falla la transferencia del video al dispositivo, una ventana emergente muestra el nombre del video cuya transferencia falló.



Los principales motivos de la falla de transferencia son los siguientes.

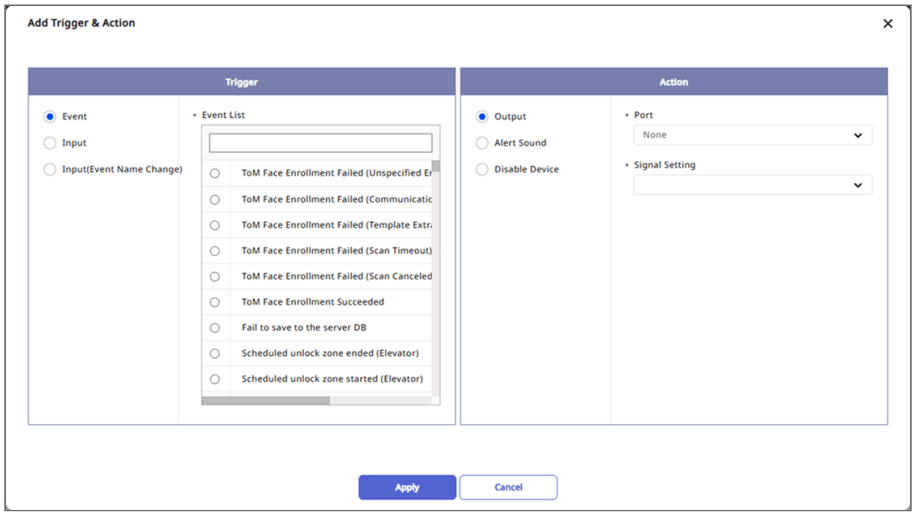
- Cuando ocurre un error al procesar la respuesta del dispositivo
- Cuando ocurre un error por motivos distintos a los anteriores

> **Consejo**
> Si la transferencia por lotes de video a varios dispositivos mediante la característica **Batch Edit** falla solo en ciertos dispositivos, haga clic en **Copy Failure Details** en la ventana emergente de resultados para copiar la lista de dispositivos con fallas y los motivos al portapapeles.

Ajustes de condiciones y acciones de activación

En el grupo **Trigger & Action**, defina las condiciones y acciones según situaciones específicas. Por ejemplo, configure todas las alarmas para que suenen cuando falle la autenticación o para que el dispositivo quede inutilizable si se pierde la conexión RS-485.

Registre eventos seleccionándolos como condiciones o acciones, o configure condiciones y acciones según las preferencias del usuario. Haga clic en el grupo **Trigger & Action** y luego haga clic en + **Add** a la derecha.



Trigger

Puede seleccionar eventos predefinidos o agregar condiciones personalizadas.

- **Event**: Seleccione un evento predefinido.
- **Input**: Establezca condiciones personalizadas seleccionando cada elemento dentro de la opción.
- **Input(Event Name Change)**: Establezca condiciones personalizadas seleccionando cada elemento dentro de la opción. Puede configurarlo para que solo detecte entradas sin acciones adicionales.

Información

- Cuando **Trigger** se establece en **Event**, solo puede seleccionar un evento de la lista de eventos.
- Al seleccionar las opciones **Input** o **Input(Event Name Change)** para establecer condiciones personalizadas, si el horario deseado no está disponible, haga clic en **+ Add Schedule**. Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.
- Si el nombre de evento deseado no está disponible al seleccionar la opción **Input(Event Name Change)** para establecer condiciones personalizadas, haga clic en **Add Event Name**. Cuando ocurra este evento, el nombre del evento se mostrará en el registro de eventos y en el registro en tiempo real.
- Los nombres de eventos pueden tener un máximo de 64 caracteres.

Action

Puede seleccionar acciones predefinidas o agregar acciones personalizadas.

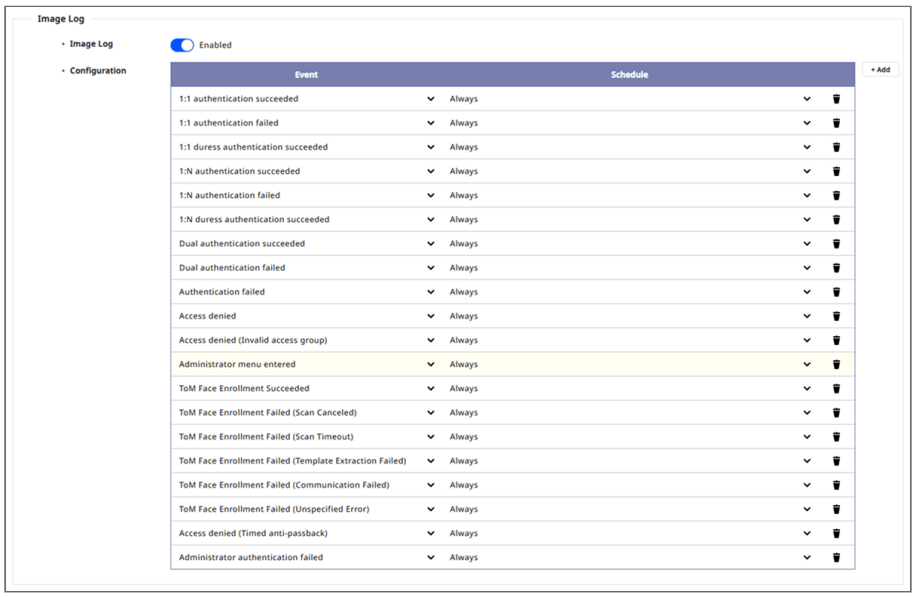
Información

- Si selecciona la opción **Output** para establecer acciones personalizadas y la configuración de señal deseada no está disponible, haga clic en **+ Add Signal** para configurarla.
- Si seleccionó **Trigger** como **Input(Event Name Change)**, puede establecer **Action** como **Port None**.

Ajustes del registro de imágenes

En el grupo **Image Log**, puede configurar los eventos y horarios del registro de imágenes utilizados por el dispositivo.

1. Establezca la opción **Image Log** en **Use**.
2. Haga clic en **Configuration** y luego en **+ Add** para configurar los eventos y horarios deseados.



Información

- Esta función es compatible con BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceStation 2 y BioStation A2.
- Para obtener más información sobre la configuración predeterminada del registro de imágenes, consulte Configuración de Registros de Imágenes.

Ajustes de Wiegand

En el grupo **Wiegand**, puede configurar los detalles de entrada y salida relacionados con los dispositivos Wiegand.



- **Input/Output**: Seleccione el modo de entrada y salida.
- **Pulse Width(µs)**: Establezca el ancho de pulso para la señal Wiegand.
- **Wiegand Input Format**: Cambie el formato Wiegand asignado al dispositivo.
- **Pulse Interval(µs)**: Establezca el intervalo de pulso para la señal Wiegand.
- **Output Mode**: Configure el modo de salida de la señal Wiegand.
  - **Normal**: Escanee tarjetas usando el formato Wiegand configurado. Puede establecer códigos de error y seleccionar valores que se enviarán si la autenticación de la tarjeta Wiegand falla.
  - **Bypass**: Envíe CSN independientemente de la autenticación Wiegand. Configure esto si lo usa como un dispositivo sin funcionalidad de control de puertas.
- **Output info**: Seleccione la información que se enviará al dispositivo durante la autenticación.

Información

Para obtener más información sobre la configuración del formato Wiegand, consulte Configurar Formato de Tarjeta Wiegand.

Ajustes de manipulación de seguridad

Si ocurre un evento de manipulación en el dispositivo, puede configurarlo para eliminar toda la información de usuario, los registros y las claves de seguridad almacenadas en el dispositivo. Para activar la función **Secure Tamper**, establézcala en **On**.



Ajustes de intercomunicador analógico

Puede configurar si se utilizará un intercomunicador analógico. Para usar el intercomunicador conectado al dispositivo, haga clic en el grupo **Interphone** y seleccione **Use**.

Información

Esta función es compatible solo con el modelo BioStation 2.

Ajustes de la cámara

Puede establecer la frecuencia de la cámara. Configurar incorrectamente la frecuencia en entornos con luces fluorescentes puede causar parpadeo en las imágenes. Establezca la frecuencia para el área local en el grupo **Camera**.

Información

- Esta función es compatible con los modelos FaceStation F2 y BioStation A2 con versión de firmware 2.1.4 o superior.
- Las frecuencias de la cámara varían según la ubicación geográfica. Estados Unidos suele usar 60 Hz, mientras que la mayoría de las demás regiones usan 50 Hz. Para conocer la frecuencia de la cámara en su área, consulte a su distribuidor.

Configuración Térmica y de Máscara

En las secciones **Thermal & Mask** o **Mask**, puede configurar parámetros detallados para la cámara térmica y el uso de máscaras.

- La cámara térmica puede vincularse al dispositivo de autenticación facial de Suprema para medir la temperatura de los usuarios que pasan por la puerta y restringir el acceso de aquellos que superen la temperatura umbral.
- El sistema detecta máscaras y restringe el acceso a los usuarios que no lleven máscara.

Información

- La función de configuración **Thermal Camera** es compatible con los modelos FaceStation 2 y FaceStation F2. Consulte las cámaras térmicas compatibles a continuación.
  - TCM10-FS2
  - TCM10-FSF2
- La configuración **Mask Detection** está disponible en los modelos FaceStation F2, BioStation 3, BioEntry W3 y BioStation 3 Max.
- Si el usuario ha realizado cambios, haga clic en **Apply**. Los cambios no se aplicarán al dispositivo si no se guardan.

Configuración de máscara

En el grupo **Mask Configuration**, puede definir si se utiliza la detección de máscara.

- **Mask Detection**: Seleccione si usar la detección de máscara.
  - **Use (Deny access when failed to detect mask)**: A los usuarios sin máscara se les niega la autenticación y se registran eventos de no uso de máscara.
  - **Use (Allow access after leaving log when failed to detect mask)**: Los usuarios sin máscara pueden autenticarse, pero se registran eventos de no uso de máscara.

  - **Not Use**: No se utiliza la detección de máscara.

- **Mask Detect Level**: Seleccione la sensibilidad de la detección de máscara.

> **Información**
> Para obtener más información sobre la opción **Mask Check Mode**, consulte Métodos de verificación térmica y de mascarilla.

Configuración de la cámara térmica

En el grupo **Thermal Camera**, puede establecer el uso de la cámara térmica y sus parámetros.

- **Thermal Camera Use**: Configure si se utiliza la cámara térmica.
  - **Use (Deny access when exceeded threshold temperature)**: A los usuarios que superen la temperatura umbral se les niega la autenticación y se registran eventos de temperatura excedida.
  - **Use (Allow access after leaving log when exceeded threshold temperature)**: Los usuarios que superen la temperatura umbral pueden autenticarse, pero se registran eventos de temperatura excedida.
- **Celsius/Fahrenheit**: Defina la unidad de visualización de temperatura.
- **Threshold Temp. (℃)** / **Threshold Temp. (℉)**: Establezca los valores mínimo y máximo de la temperatura umbral que restringe el acceso.

  Los usuarios con una temperatura superficial por debajo del valor **Low** o por encima del valor **High** se restringirán de entrar según la opción **Thermal Camera Use**. Puede establecer el rango de 1 ℃ a 45 ℃ y el valor **Low** no puede ser mayor que el valor **High**.
- **Save Temp. Data**: Configure si se guarda el registro de temperatura del usuario.
  - **Enabled**: Registra tanto el éxito de autenticación como el valor de temperatura del usuario.
  - **Disable**: Solo registra el éxito de autenticación.
- **Temp. Fail Sound**: Configure si se notifica el fallo de autenticación debido a superar la temperatura umbral.
- **Show Infrared Image**: Configure si se muestran imágenes infrarrojas en la pantalla del dispositivo.
- **Camera Configuration**: Configure opciones detalladas para la cámara térmica.
  - **Temp. Correction (℃)**: Ajuste la temperatura para medir de forma consistentemente más alta o más baja según el entorno de uso del producto. Por ejemplo, si las temperaturas se miden constantemente 0.1 ℃ más altas, establezca el valor de compensación de temperatura en -0.1 ℃.
  - **Distance(cm)**: Establezca la distancia entre el usuario y la cámara térmica.
  - **Emissivity**: Establezca la emisividad infrarroja.
  - **Dynamic ROI**: Si hay otras fuentes de luz en el entorno, configure la cámara térmica para medir automáticamente la temperatura del usuario sin interferencia de luces cercanas.
  - **ROI X(%)** / **ROI Y(%)** / **ROI Width(%)** / **ROI Height(%)**: Si la opción **Dynamic ROI** está configurada en **Disable**, establezca manualmente la ROI (Región de interés). Ajuste la ubicación y el tamaño de la ROI para especificar el área donde la cámara térmica medirá la temperatura.

Información

- La configuración de los valores **Low** y **High** de la opción **Threshold Temp.** es compatible a partir de las siguientes versiones de firmware.
  - FaceStation 2 versión de firmware 1.4.2 o superior
  - FaceStation F2 versión de firmware 1.0.2 o superior
- Para un rendimiento óptimo, se recomienda usar la configuración predeterminada para las subopciones en **Camera Configuration**. Los valores predeterminados para las opciones de cada dispositivo se enumeran a continuación.

Ítem	FaceStation 2	FaceStation F2
Distance(cm)	100	100
Emissivity	0.98	0.98
ROI X(%)	47	30
ROI Y(%)	45	25
ROI Width(%)	15	50
ROI Height(%)	10	55

Métodos de verificación térmica y de mascarilla

En el grupo **Thermal & Mask Check Mode** o **Mask Check Mode**, establezca la opción **Mask Detection** o **Thermal Camera Use** en **Use** para configurar el método de verificación según el uso previsto del dispositivo.

- **Check after authentication**: Comprueba el uso de mascarilla del usuario o mide la temperatura después de la autenticación.
- **Check before authentication**: Comprueba el uso de mascarilla del usuario o mide la temperatura antes de la autenticación. En este caso, los usuarios que no lleven mascarilla o superen la temperatura umbral no podrán autenticarse.
- **Check without authentication**: El dispositivo solo se puede usar para verificar el uso de mascarilla o medir la temperatura. Los usuarios que lleven mascarilla o tengan una temperatura por debajo del umbral pueden ingresar independientemente de la autenticación.

Configuración del Intercomunicador

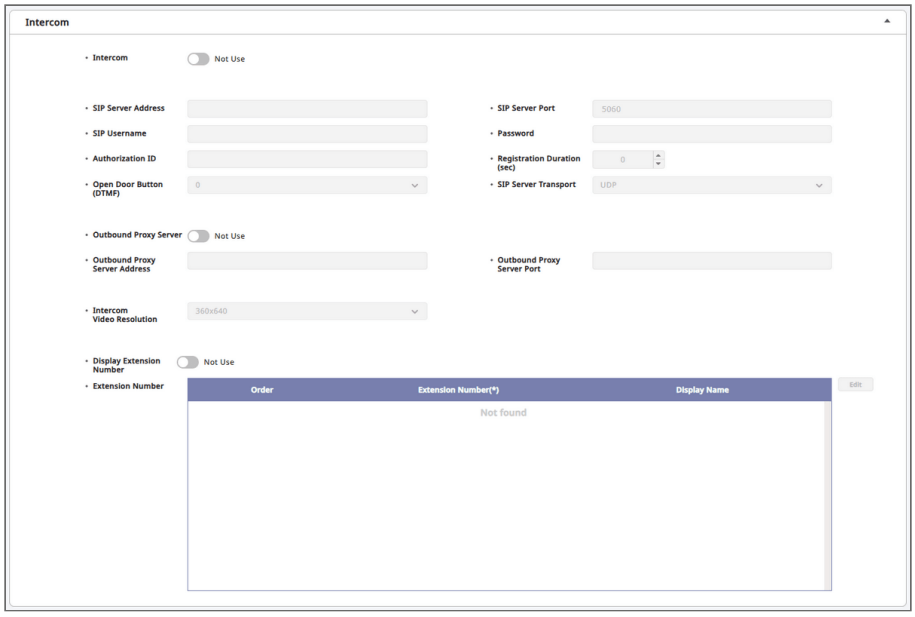
En la sección **Intercom**, configure opciones detalladas para usar el intercomunicador.

Información

- Esta función es compatible con los modelos BioStation 3 Max, BioStation 3, FaceStation 2 y BioStation A2.
- Si el usuario ha realizado cambios, haga clic en **Apply**. Los cambios no se aplicarán al dispositivo si no se guardan.

Configuración del intercomunicador

Configure cada opción para registrar el dispositivo en el servidor SIP (Session Initiation Protocol).



- **Intercom**: Para usar el dispositivo como intercomunicador, configúrelo en **Enabled**.
- **SIP Server Address**: Ingrese la dirección del servidor SIP.
- **SIP Server Port**: Ingrese el puerto del servidor SIP. El valor predeterminado es 5060.
- **SIP Username**: Ingrese el nombre de usuario de la cuenta SIP.
- **Password**: Ingrese la contraseña de la cuenta SIP.
- **Authorization ID**: Ingrese el ID de autorización de la cuenta SIP.
- **Registration Duration (sec)**: Ingrese la duración del registro en segundos. El dispositivo intenta registrarse en el servidor SIP cada vez que vence la duración del registro.
- **Open Door Button (DTMF)**: Especifique un botón para abrir la puerta de entrada durante una llamada.
- **SIP Server Transport**: Elija el método de transporte SIP al configurar los ajustes del servidor SIP del intercomunicador.
- **Outbound Proxy Server**: Establézcalo en **Enabled** si utiliza servicios SIP a través de un servidor proxy de salida independiente.
  - **Outbound Proxy Server Address**: Ingrese la dirección del servidor proxy de salida.
  - **Outbound Proxy Server Port**: Ingrese el puerto del servidor proxy de salida.
- **Intercom Video Resolution**: Seleccione la resolución de la salida de video cuando use el intercomunicador. El valor predeterminado es **360 x 640**.

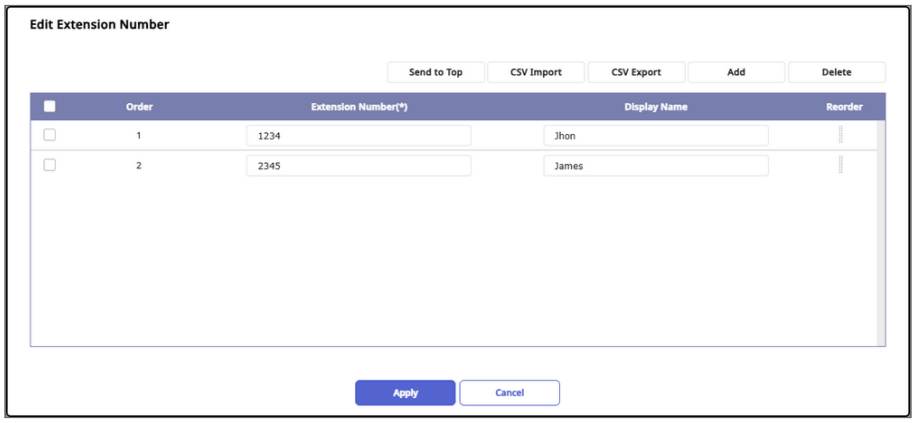
- **Display Extension Number**: Establézcalo en **Disable** para evitar que el dispositivo muestre el número de extensión. Si no se muestra el número de extensión, no podrá distinguir al destinatario en la pantalla de llamada.
- **Extension Number**: Puede registrar hasta 128 números de extensión. Para agregar o editar números de extensión, haga clic en el botón **Edit**. Para obtener más información, consulte Editar números de extensión.

Información

- Las opciones **SIP Username** y **Authorization ID** solo pueden incluir números, letras inglesas (distingue mayúsculas y minúsculas) y caracteres especiales.
- La opción **Registration Duration (sec)** se puede configurar entre 60 y 600 segundos.
- Las opciones **SIP Server Transport** y **Intercom Video Resolution** son compatibles con el firmware versión 1.3.0 y posteriores de BioStation 3.
- **Session Initiation Protocol** (SIP) es un protocolo de comunicación basado en protocolos de Internet para diversas comunicaciones multimedia, como VoIP y videoconferencias. El servidor SIP gestiona dichas comunicaciones y establece conexiones.

Editar números de extensión

Orientación sobre las funciones proporcionadas en la ventana **Edit Extension Number**.



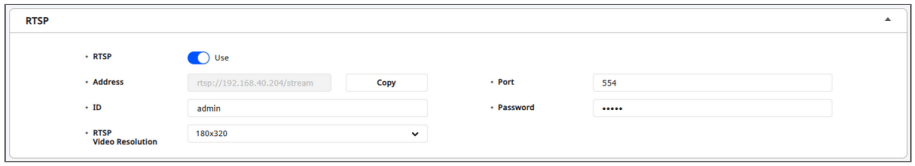
- **Send to Top**: Mueva el número de extensión seleccionado al principio de la lista.
- **CSV Import**: Importe un archivo CSV que contenga los números de extensión.
- **CSV Export**: Exporte los números de extensión guardados a un archivo CSV.
- **Add**: Agregue un número de extensión.
- **Delete**: Elimine un número de extensión.
- **Reorder**: Cambie el orden de los números de extensión arrastrándolos con el mouse.

Información

- Los modelos FaceStation 2 y BioStation A2 pueden guardar hasta 16 números de extensión.
- No puede importar un archivo CSV que contenga más números de extensión que el máximo permitido.
- Los números de extensión solo pueden incluir números, letras inglesas (distingue mayúsculas y minúsculas) y caracteres especiales.

Configuración de RTSP

En la sección **RTSP**, configure los detalles de la transmisión **Real Time Streaming Protocol** (RTSP). La cámara del dispositivo puede transmitir video en vivo.

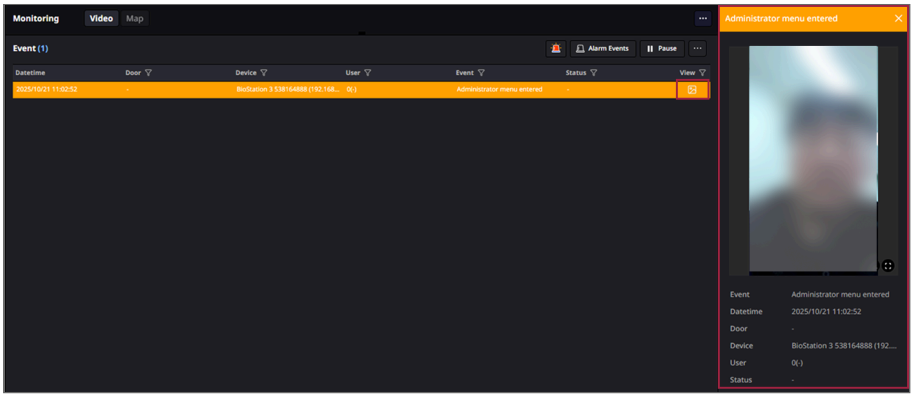


- **RTSP**: Active la transmisión RTSP configurando **Enabled**.
- **Address**: La dirección del servidor RTSP es fija. Haga clic en **Copy** para copiar la dirección RTSP.
- **Port**: Configure el puerto RTSP.
- **ID**: Ingrese el ID del servidor RTSP.
- **Password**: Ingrese la contraseña del servidor RTSP.
- **RTSP Video Resolution**: Seleccione la resolución de salida de video cuando use RTSP. El valor predeterminado es **180 x 320**.

> **Información**
>
> - Esta función es compatible con los modelos BioStation 3 Max, BioStation 3 y BioEntry W3.
> - La opción **RTSP Video Resolution** es compatible con el firmware BioStation 3 versión 1.3.0 o superior.
> - Si el usuario ha realizado cambios, haga clic en **Apply**. Los cambios no se aplicarán al dispositivo si no se guardan.

Configuración de Registros de Imágenes

Image Log permite la verificación por imágenes de los eventos que ocurren en dispositivos con cámara. Puede registrar imágenes faciales de los usuarios que pasan por las puertas o situaciones durante la ocurrencia de eventos usando la cámara del dispositivo. Las imágenes registradas se pueden visualizar en los eventos en tiempo real en la página **Monitoring**.



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

Al configurar el registro de imágenes, se creará un registro de imágenes del evento en la lista **Event**. Haz clic en a la derecha del elemento del evento. Visualiza la imagen capturada cuando ocurrió el evento en el panel derecho.

Información

- Esta función es compatible con BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceStation 2 y BioStation A2.
- Para obtener más información sobre cómo ver los registros de eventos en la página **Monitoring**, consulta Supervisar Evento.

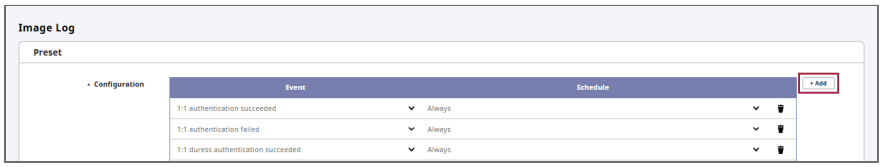
Precaución

El dispositivo no aplica los ajustes del menú **Settings** → **Device** → **Image Log**. Habilite la opción **Image Log** en cada dispositivo. Para más información, consulte Configuración Avanzada.

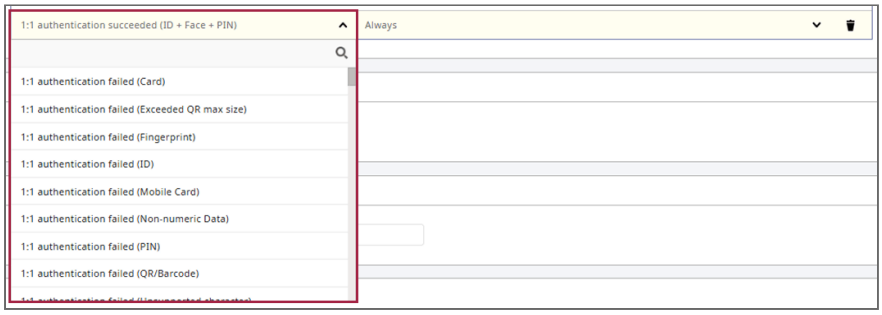
Agregar ajustes básicos

Configure los ajustes básicos que entran en vigor cuando habilita **Image Log** en un dispositivo. Configure eventos y horarios para crear registros de imágenes. Se generará un registro de imágenes cuando se cumplan las condiciones de eventos y horarios.

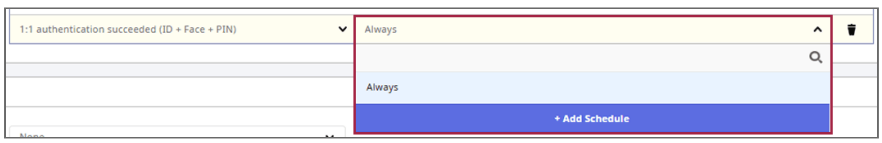
1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Device** → **Image Log** en la barra lateral izquierda.
3. Haga clic en **+ Add** a la derecha de la sección **Preset**.



4. Cuando agregue un evento al final de la lista, haga clic en ⌄ para el evento deseado y seleccione las opciones.



5. Haga clic en ⌄ en el horario del evento seleccionado y elija la opción deseada.



6. Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.

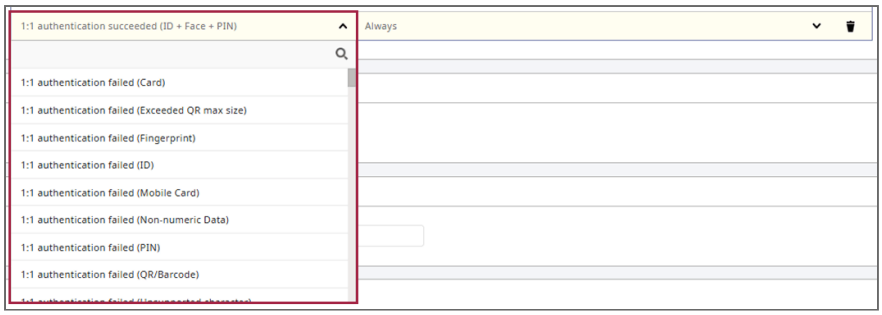
Información

Si el horario deseado no está disponible, haz clic en **+ Add Schedule** para agregar uno. Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

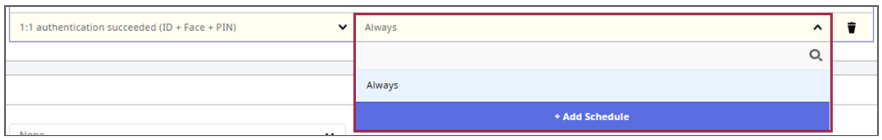
Modificar ajustes básicos

Cambia los eventos y horarios de los registros de imágenes existentes.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Device** → **Image Log** en la barra lateral izquierda.
3. En la lista de la sección **Preset**, haga clic en ⌄ para el evento que desea modificar y seleccione las opciones.



4. Haga clic en ⌄ en el horario del evento seleccionado y elija la opción deseada.



5. Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.

Información

- Si el horario deseado no está disponible, haz clic en **+ Add Schedule** para agregar uno. Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.
- Los ajustes básicos modificados solo afectan a los dispositivos agregados a partir de ahora. Estos cambios no afectan a los dispositivos donde **Image Log** ya está habilitado. Agregue los cambios en los ajustes de cada dispositivo.

Eliminar ajustes básicos

Elimina los eventos y horarios de los registros de imágenes existentes.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Device** → **Image Log** en la barra lateral izquierda.
3. En la lista de la sección **Preset**, haga clic en 🗑 para el evento que desea eliminar.



4. Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.

Delete Option

Configura opciones de eliminación para que los archivos de registro de imágenes no ocupen espacio en el servidor **BioStar X**. Los registros de imágenes que superen el tamaño de archivo o la duración establecidos se eliminarán automáticamente.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Device** → **Image Log** en la barra lateral izquierda.
3. Configura las condiciones para eliminar registros de imágenes en la sección **Delete Option**.



- **Delete Option**: Elige la unidad de tamaño de archivo (**MB**/**GB**) o la unidad de duración (**Day**/**Week**/**Month**).
- **Amount of Image Log**: Define la unidad de la condición establecida en **Delete Option**.
- **Delete Cycle**: Selecciona el ciclo para eliminar registros de imágenes.

4. Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.

Storage Path Settings

Configura la ruta donde se almacenan los registros de imágenes.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Device** → **Image Log** en la barra lateral izquierda.
3. Ingresa la ruta para almacenar los registros de imágenes en el campo **Image Log File Path** de la sección **Storage Path Settings**.



4. Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.

Información

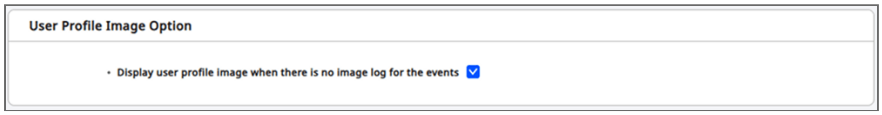
- La ruta de almacenamiento no se crea automáticamente; debe crearse previamente para almacenar registros de imágenes.
- Por ejemplo, si ingresas `.\imagelog\`, los registros de imágenes se almacenarán en la ruta donde está instalado BioStar X.

  > *C:\Program Files\BioStar X\imagelog*

User Profile Image Option

Configura el dispositivo para mostrar la foto de perfil del usuario al monitorizar registros de eventos y registros en tiempo real si el dispositivo no puede capturar registros de imágenes.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Device** → **Image Log** en la barra lateral izquierda.
3. Marca la casilla de **Display user profile image when there is no image log for the events** en la sección **User Profile Image Option**.



4. Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.

Información

- Cuando esta opción está habilitada, si se genera un registro de imágenes, no se mostrará la foto de perfil del usuario y se mostrará el registro de imágenes grabado.
- Para obtener más información sobre cómo ver los registros de eventos en la página **Monitoring**, consulta Supervisar Evento.

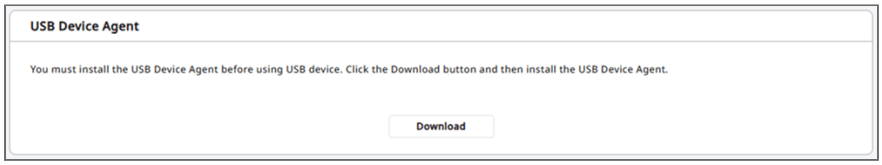
Configuración del Agente USB

Al acceder a **BioStar X** desde una PC cliente, asegúrese de que los dispositivos USB de enrolamiento de huellas y de tarjetas estén disponibles. Instale el agente de dispositivo USB para hacerlo. Este documento brinda orientación sobre cómo instalar y configurar el agente de dispositivo USB.

Instale el agente del dispositivo USB

Debe instalar el agente de dispositivo USB para acceder a **BioStar X** desde una PC cliente y usar los dispositivos USB de enrolamiento de huellas y tarjetas.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Device** → **USB Agent** en la barra lateral izquierda.
3. Haga clic en **Download** en la sección **USB Device Agent**.



4. Ejecute el archivo descargado y siga las instrucciones en pantalla para completar la instalación.

> **Información**
> Si **User Account Control** está habilitado en Windows, el agente USB no se puede iniciar automáticamente. Desactive User Account Control o ejecútelo directamente con privilegios administrativos.

Configure el orden de bytes del dispositivo de tarjeta USB

Configure el orden de bytes del dispositivo de tarjeta USB.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Device** → **USB Agent** en la barra lateral izquierda.
3. Configure la opción **Byte Order of USB Card Device** en la sección **Byte Order**.



   - **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).

4. Una vez completados todos los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.

> **Información**
> La opción **Byte Order** se aplica solo a tarjetas CSN.

Configure el puerto del agente USB

Configure el puerto usado por el agente USB.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Device** → **USB Agent** en la barra lateral izquierda.
3. Ingrese el número de puerto en **USB Agent Port Number** en la sección **USB Agent Port**.



4. Una vez completados todos los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.

> **Información**
> El agente USB es un programa que opera por cliente y la configuración del número de puerto permite que el servidor se comunique a través de ese puerto.

Configuración de Administración de Conexión de Dispositivos

El **Device Connection Manager** de **BioStar X** es una función diseñada para administrar de manera eficiente una gran cantidad de dispositivos en empresas o edificios grandes. Anteriormente, un único servidor podía conectar un máximo de 1,000 dispositivos, pero ahora puede instalar varios servidores de **comunicación** en varias computadoras para administrar hasta 3,000 dispositivos de red.

> **Información**
>
> - Esta función requiere que la licencia de **Device Manager** esté activada. Para obtener más información sobre la política de licencias, consulte Política de Licencias.
> - Para obtener más información sobre las especificaciones y la instalación del Servidor de comunicaciones múltiples, consulte lo siguiente:
>   - Requisitos Mínimos del Sistema
>   - Instalar el Servidor de Comunicaciones Múltiples

Funciones clave

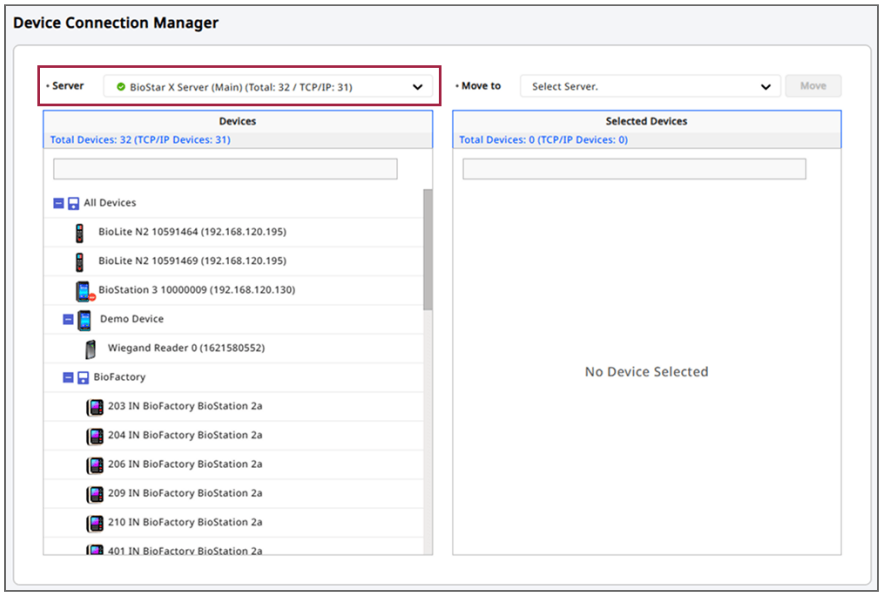
- **Expansión de servidor**: Instale servidores de comunicación en computadoras adicionales además de la principal para conectar más dispositivos.
- **Operación con múltiples servidores**: Use hasta tres servidores en conjunto para admitir un total de 3,000 dispositivos.
- **Gestión conveniente de dispositivos**: Al agregar nuevos dispositivos, elija a qué servidor conectarlos; también puede mover dispositivos existentes a otro servidor.
- **Soporte para entornos grandes**: Opere una gran cantidad de dispositivos de forma fiable en sitios corporativos o edificios grandes.

El Servidor de comunicaciones múltiples es un servicio dedicado que separa la conexión de dispositivos del servidor integrado de BioStar X. Se centra solo en una comunicación confiable con los dispositivos y mejora el rendimiento general del sistema.

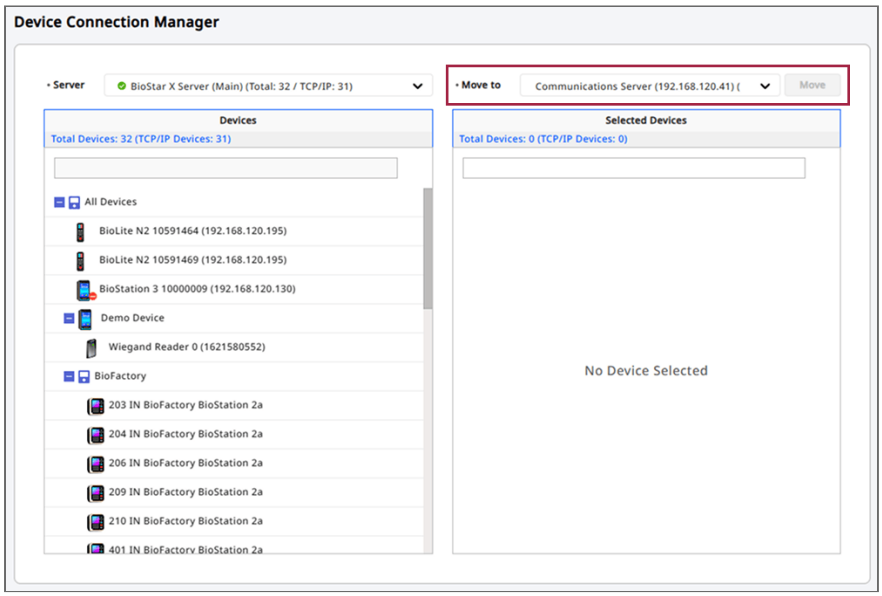
Mover dispositivos a otro servidor

Use esta característica para mover dispositivos del servidor principal o de otro Servidor de comunicaciones múltiples a otro. Esta función ayuda a mantener el estado de conexión de los dispositivos mientras se trasladan entre servidores.

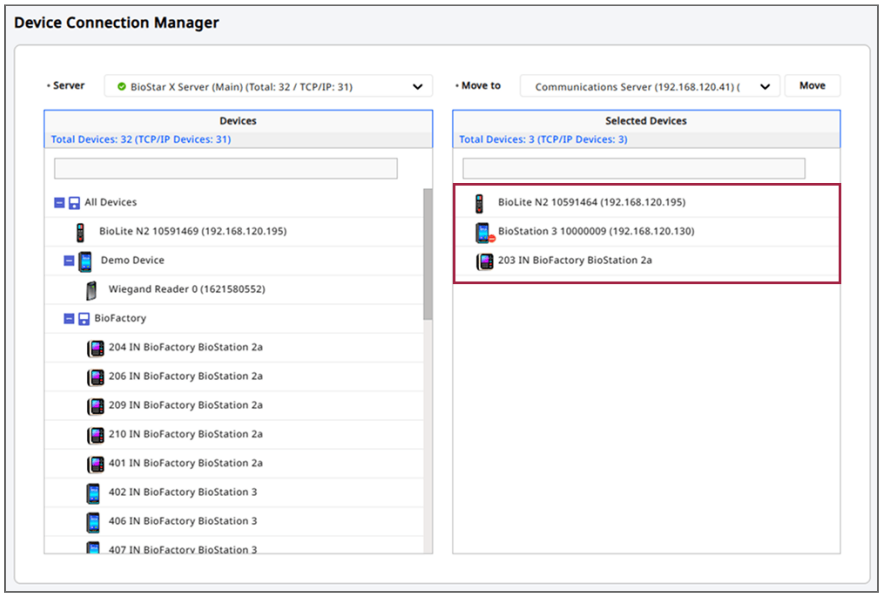
1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device Connection Manager** en la barra lateral izquierda.
3. En la sección **Server** de la izquierda, seleccione el servidor donde está registrado el dispositivo que desea mover.



4. En la sección **Move to** de la derecha, seleccione el servidor de destino al que desea trasladar los dispositivos.

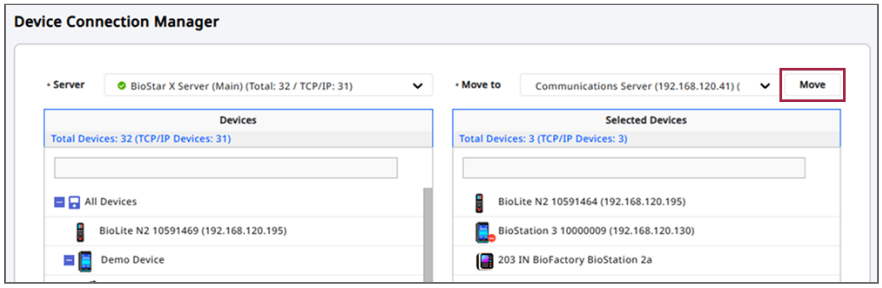


5. Seleccione los dispositivos que desea mover de la lista de dispositivos. Puede seleccionar varios dispositivos.



> Para buscar un dispositivo específico, ingrese palabras clave en el campo de entrada superior. Puede buscar por nombre del dispositivo o número de serie.

6. Haga clic en **Move** para mover el dispositivo al servidor de destino.



7. Verifique el número total de dispositivos a mover, la cantidad de dispositivos conectados por TCP/IP, el nombre del servidor al que se trasladarán y la dirección IP en la ventana de mensajes.

8. Haga clic en **Yes**.

Una vez completada la transferencia, puede verificar el número total de dispositivos trasladados, la cantidad de dispositivos conectados por TCP/IP, y el nombre y la dirección IP del servidor de destino en la ventana de mensajes.

Si hay dispositivos que no se pudieron mover, la ventana de mensajes mostrará la cantidad de dispositivos que no se movieron y la cantidad de dispositivos conectados por TCP/IP. Para ver una lista de los dispositivos que no se pudieron mover y los motivos de la falla en un archivo CSV, haga clic en el botón **Download**.

> **Información**
>
> - Si no hay servidores de extensión conectados, **Move to** en el lado derecho de la pantalla no se mostrará.
> - Al seleccionar un servidor, puede ver todos los dispositivos registrados, incluidos los dispositivos conectados por Wiegand y RS-485 en ese servidor.
> - Al seleccionar un dispositivo o grupo de dispositivos, también se trasladarán los dispositivos subordinados conectados al dispositivo y los dispositivos incluidos en el grupo.
> - Los dispositivos que no están conectados mediante TCP/IP no se pueden mover.

Administrar Puertas

Esta guía describe cómo configurar y administrar la información de la puerta de acceso del dispositivo registrado. Configure la información relativa a los relés del dispositivo, la autenticación dual, el anti-passback, la apertura forzada de la puerta y las alarmas de puerta abierta prolongada; la información de puerta configurada se usará como componentes de los niveles de acceso.

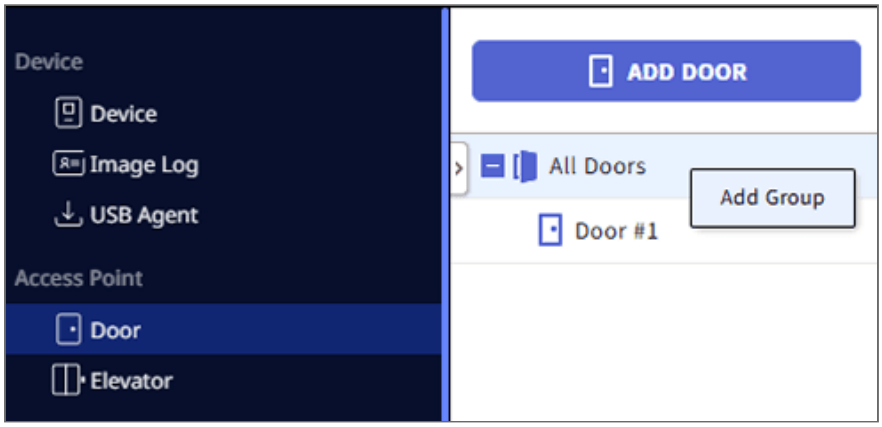
Administrar Grupo de Puertas

Esta guía describe cómo configurar grupos para administrar fácilmente varias puertas. Un grupo de puertas es una característica que te permite gestionar varias puertas como un grupo. Si configura un grupo, puede configurar múltiples puertas a la vez.

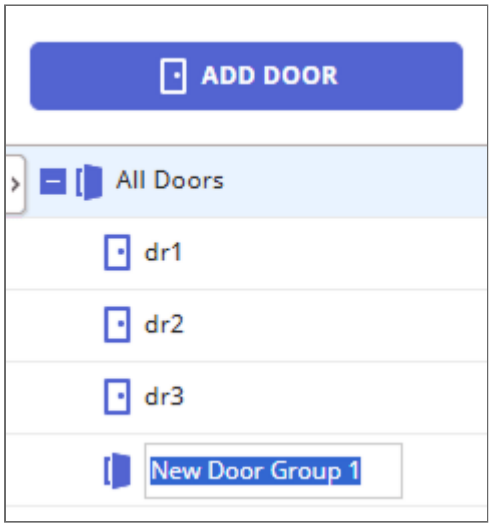
> **Consejo**
> Registre nombres de grupos mediante ubicaciones de puertas o nombres de oficinas para facilitar la administración.

Agregar grupo de puertas

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Door** en la barra lateral izquierda.
3. Haga clic derecho en **All Doors** de la lista de puertas.



4. Haga clic en **Add Group** en el menú emergente.

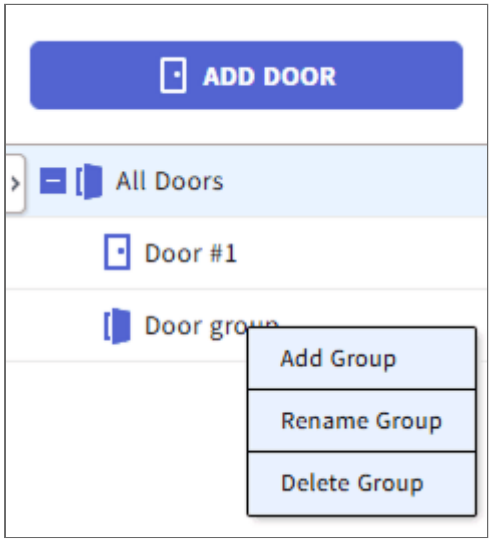


5. Introduzca el nombre de grupo deseado.

> **Información**
>
> - Cree hasta 8 niveles de grupos de puertas.
> - El nombre del grupo de puertas puede tener hasta 48 caracteres.

Renombrar grupo de puertas

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Door** en la barra lateral izquierda.
3. Haga clic derecho en el grupo que desea renombrar en la lista de puertas.



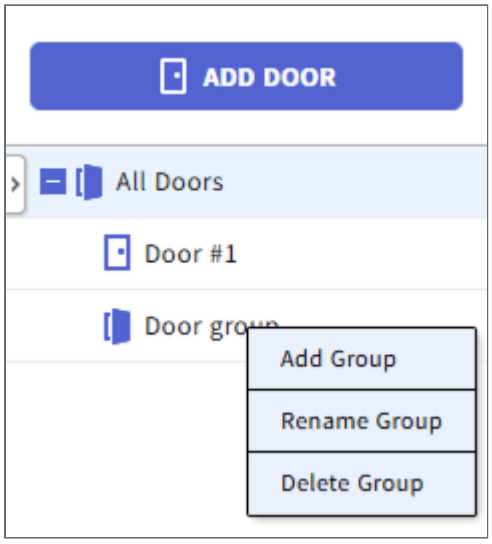
4. Haga clic en **Rename Group** en el menú emergente.
5. Ingrese el nuevo nombre del grupo.

Información

El nombre del grupo de puertas puede tener hasta 48 caracteres.

Eliminar grupo de puertas

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Door** en la barra lateral izquierda.
3. Haga clic derecho en el grupo que desea eliminar en la lista de puertas.



4. Haga clic en **Delete Group** en el menú emergente.

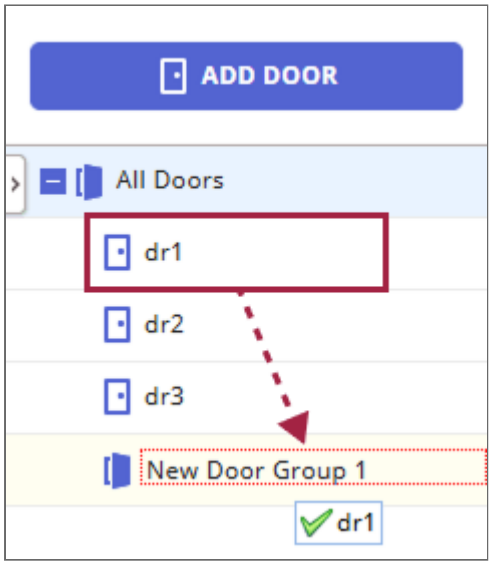
Precaución

Eliminar un grupo de puertas elimina todas las puertas incluidas en el grupo. Para evitar eliminar las puertas, muévalas a otro grupo antes de eliminar el grupo.

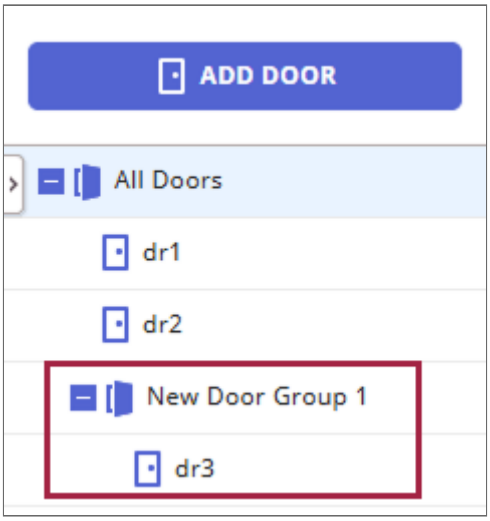
Agregar puerta al grupo

Agregar desde la lista de puertas

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Door** en la barra lateral izquierda.
3. Seleccione la puerta que desea agregar a un grupo en la lista de puertas y arrástrela al grupo deseado.

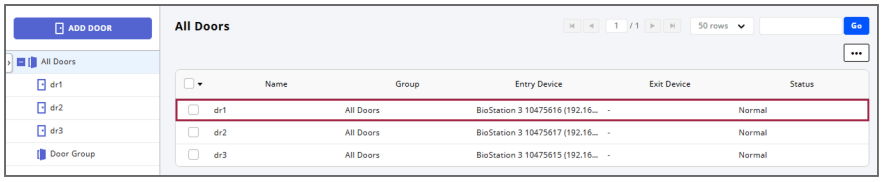


La puerta seleccionada se mueve al grupo.

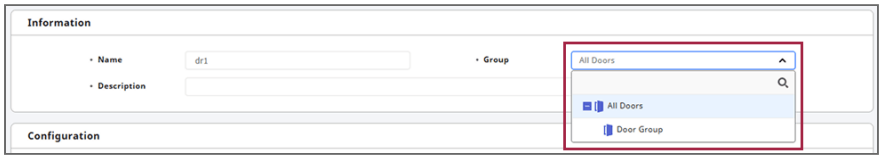


Agregar desde la información de la puerta

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Door** en la barra lateral izquierda.
3. Haga clic en la puerta que desea agregar a un grupo en la lista en el lado derecho de la pantalla.



4. Cuando aparezca la pantalla de edición de información de la puerta, haga clic en la opción **Group** en la sección **Information**.



5. Seleccione el grupo deseado.

6. Haga clic en **Apply** en la parte inferior de la pantalla.

Registrar Puerta

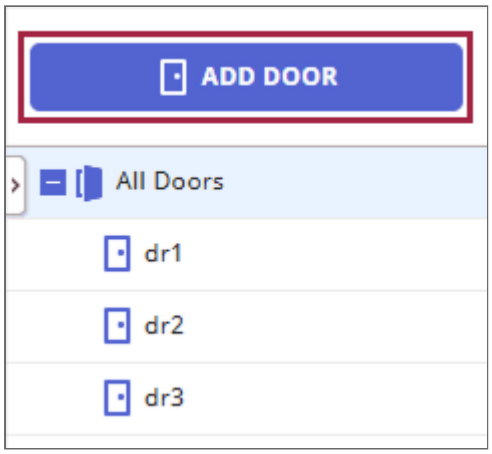
Esta guía describe cómo registrar y configurar puertas. Conecte dispositivos de entrada y salida para cada puerta y configure funciones de seguridad como anti-passback y autenticación dual para establecer un entorno de gestión de acceso sistemático. Además, configure alarmas basadas en el estado de la puerta para prevenir incidentes de seguridad con anticipación.

Antes de comenzar

- Configure los niveles de acceso, los grupos de acceso y los niveles de piso para el control de acceso antes de registrar puertas. Para obtener más información, consulte Configuración de Control de Acceso.
- Registre los dispositivos antes de registrar puertas. Para obtener más información sobre el registro de dispositivos, consulte lo siguiente.
  - Registrar dispositivo
  - Registrar Credenciales Wiegand
  - Registrar Esclavo

Registrar puerta

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Door** en la barra lateral izquierda.
3. Haga clic en **ADD DOOR**.



4. Cuando aparezca la pantalla **Add New Door**, configure cada elemento de la sección en orden.
   - **Information**: Configure la información básica de la puerta. Para obtener más información, consulte Configurar información básica.
   - **Configuration**: Configure los dispositivos conectados a la puerta, los botones de entrada y salida y los sensores de puerta. Para obtener más información, consulte Configurar los ajustes de la puerta.
   - **Option**: Configure opciones adicionales. Para obtener más información, consulte Configurar opciones adicionales.
   - **Anti PassBack**: Configure la función anti-passback para gestionar el historial de acceso y mejorar la seguridad. Para obtener más información, consulte Configurar anti-passback.

- **Timed Anti PassBack**: Configure el tiempo de inicialización para la función anti-passback. Para obtener más información, consulte Configurar anti-passback temporizado.
- **Alarm**: Configure la alarma para activar o bloquear el uso del dispositivo cuando ocurra una violación de anti-passback. Para obtener más información, consulte Configurar alarmas.

5. Una vez completados todos los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.

Configurar información básica

En la sección **Information**, ingrese o cambie el nombre, el grupo y la descripción de la puerta.

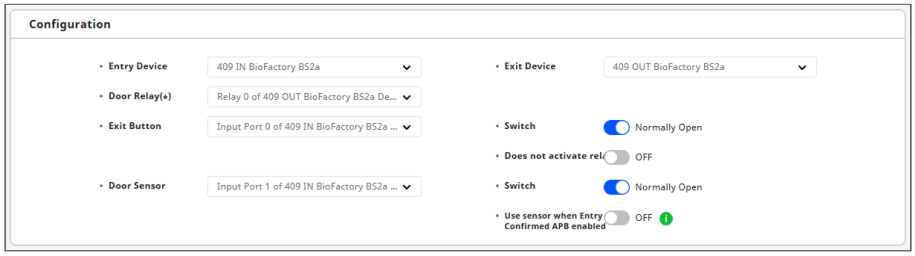


- **Name**: Ingrese el nombre de la puerta. Ingrese un nombre que permita una gestión conveniente.
- **Group**: Seleccione el grupo de la puerta.
- **Description**: Ingrese una descripción breve de la puerta.

> **Información**
>
> - El nombre de la puerta puede tener hasta 48 caracteres.
> - Para obtener más información sobre cómo registrar grupos de puertas, consulte Administrar Grupo de Puertas.

Configurar los ajustes de la puerta

En la sección **Configuration**, configure los dispositivos conectados a la puerta, los botones de salida y los sensores de puerta.



- **Entry Device**: Seleccione el dispositivo que se utilizará para la entrada. Si el dispositivo no está en la lista, regístrelo primero.
- **Door Relay**: Elija el relevador que funcionará como mecanismo de cierre de la puerta.
- **Exit Button**: Seleccione el puerto que se utilizará como botón de salida.
  - **Switch**: Se puede configurar en **N/C** (Normalmente Cerrado) o **N/O** (Normalmente Abierto).
  - **Does not activate relay**: Configure para que una entrada del botón de salida genere un registro de solicitud de apertura de puerta sin activar el relevador.
- **Door Sensor**: Elija el puerto para confirmar el estado de la puerta. Si se establece en **None**, se deshabilitará el uso de la sección **Alarm**.

  - **Switch**: Se puede configurar en **N/C** (Normalmente Cerrado) o **N/O** (Normalmente Abierto).
  - **Use sensor when Entry Confirmed APB enabled**: Configure si se utilizará el sensor de puerta al usar la opción **Entry Confirmed APB**.

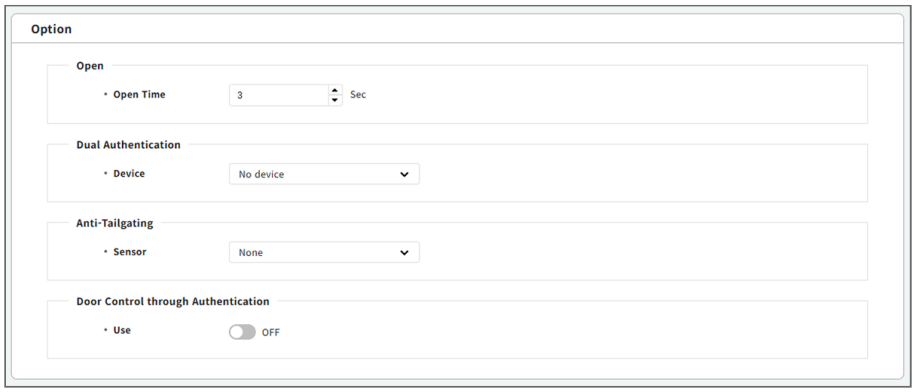
> Si **Timed Anti PassBack** está habilitado, no se podrá usar la opción **Use sensor when Entry Confirmed APB enabled**.

- **Exit Device**: Seleccione el dispositivo que se utilizará para la salida.

> **Información**
>
> - Si seleccionó una cerradura de puerta inalámbrica para **Entry Device**, también debe seleccionar una cerradura de puerta inalámbrica para **Exit Device**.
> - Si seleccionó una cerradura de puerta inalámbrica para **Entry Device**, no podrá usar la opción **Door Relay**.
> - Los modelos CoreStation no se pueden usar como dispositivos de entrada ni de salida.

Configurar opciones adicionales

En la sección **Option**, configure opciones adicionales para la puerta.



- **Open**: Configure las opciones de apertura de la puerta.
  - **Open Time**: Configure la duración durante la cual la puerta permanece abierta después de completar la autenticación. La puerta se bloqueará automáticamente después de este tiempo.
  - **Lock when door is closed**: La puerta se bloqueará cuando el sensor detecte que se ha cerrado. Si se establece en **On**, no se podrá usar la opción **Use Automatic Door**.
  - **Use Automatic Door**: Si se usa una puerta automática, el relevador puede operar independientemente del estado del sensor de puerta. Si se establece en **On**, no se podrá usar la opción **Lock when door is closed**.

> El valor de **Open Time** puede variar según el tipo de dispositivo de cierre de puerta que se use.

- **Dual Authentication**: Configura para requerir que dos personas (un usuario regular y un administrador) autentiquen credenciales para abrir la puerta.
  - **Device**: Selecciona el dispositivo que se usará para la autenticación dual. **Device**: Selecciona el dispositivo que se usará para la autenticación dual.

  - **Schedule**: Selecciona el horario para usar la autenticación dual. Si el horario deseado no está disponible, haz clic en **+ Add Schedule** para agregar uno.
  - **Approval Type**: Define el orden de la autenticación del administrador.
    - **None**: Se requieren dos autenticaciones sin importar el grupo de autenticación.
    - **Last**: El usuario general debe autenticarse primero, seguido de un usuario autenticado incluido en el grupo de autenticación establecido.
  - **Approval Group**: Define el grupo al que pertenece el administrador. Esta opción está disponible cuando **Approval Type** se establece en **Last**.
  - **Timeout**: Define el tiempo de espera entre la primera y la segunda autenticación. Si la segunda autenticación no se completa dentro del tiempo establecido, la puerta no se abrirá.

> - Modifique los ajustes en el siguiente menú para cambiar la autenticación dual del dispositivo configurado para los ajustes de límite de ocupación. **Settings** → **Access Management** → **Advanced AC** → **Occupancy Limit**
>
>   Para obtener más información sobre la configuración de **Occupancy Limit**, consulte Configuración Avanzada de Control de Acceso.
> - Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

- **Anti-Tailgating**: Configura para detectar tailgating cuando una persona no autorizada sigue a una autorizada para entrar.
  - **Sensor**: Selecciona un sensor para detectar tailgating.
- **Door Control through Authentication**: Permite que la puerta permanezca desbloqueada cuando un usuario autorizado realiza un Double Badge (Double Badge). Para más información, consulte Configurar El Control De Puerta Mediante Autenticación.

> Este ajuste no está disponible en la pantalla Agregar puerta porque la puerta no está en un grupo de acceso. Guarda la puerta, agrégala a un grupo de acceso y, luego, configura este ajuste en la pantalla Editar información de la puerta.

Configurar anti-passback

Anti-passback se usa para gestionar el historial de acceso y mejorar la seguridad. Previene situaciones en las que un usuario entrega su tarjeta de entrada a otro después de ingresar y detiene a personas externas que siguen a usuarios con privilegios de acceso.

Consulta a continuación para completar la configuración en la sección **Anti PassBack**.

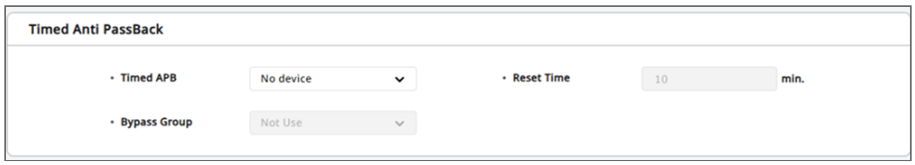
- **Type**: Elige el tipo de anti-passback.
  - **None**: No utiliza la función de anti-passback.
  - **Soft APB**: Durante una violación de anti-passback, se permite la entrada pero se activa una alarma o se crea un registro en **BioStar X**.
  - **Hard APB**: Durante una violación de anti-passback, la entrada no está permitida y se activará una alarma o se creará un registro en **BioStar X**.

- **Reset Time**: Define el tiempo hasta que se reinicie la función de anti-passback. Admite hasta 7 días (10080 minutos); si se establece en 0, no se reinicia.

> **Información**
>
> - Funciona únicamente cuando se instalan dispositivos de entrada y salida; si en la sección **Configuration** la opción **Exit Device** se establece en **None**, quedará inutilizable. Para obtener más información sobre cómo configurar el dispositivo de salida, consulte Configurar los ajustes de la puerta.
> - La sección **Anti PassBack** requiere un dispositivo maestro configurado vía RS-485 y un dispositivo esclavo.
> - Si se habilita la sección **Timed Anti PassBack**, **Anti PassBack** no estará disponible.

Configurar anti-passback temporizado

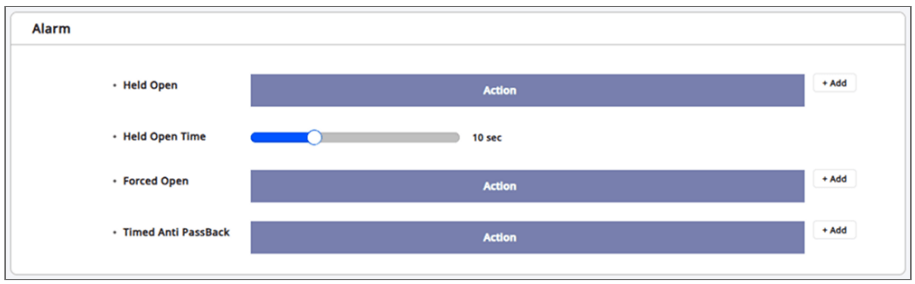
Cuando un usuario intenta volver a autenticarse en el mismo dispositivo después de la autenticación de ingreso, la función de anti-passback impide la reautenticación inmediata. La sección **Timed Anti PassBack** define el tiempo de inicialización de la función de anti-passback para limitar de forma efectiva las entradas frecuentes de los usuarios.



- **Timed APB**: Selecciona el dispositivo que usará la función de anti-passback temporizado.
- **Reset Time**: Define el tiempo hasta que se reinicie la función de anti-passback. La unidad de entrada es minutos (min) y el valor predeterminado es 10 minutos. Admite un máximo de 60 minutos.
- **Bypass Group**: Selecciona los grupos de acceso que siempre pueden pasar sin estar sujetos al anti-passback temporizado.

Configurar alarmas

En la sección **Alarm**, configura que se active una alarma o se bloquee el uso del dispositivo cuando la puerta se abra por la fuerza, quede abierta o ocurra una violación de anti-passback. Haz clic en **+ Add** en la opción para agregar una alarma.



- **Held Open**: Configura las acciones de alarma cuando la puerta quede abierta.
- **Held Open Time**: Define el tiempo para que suene la alarma cuando la puerta haya estado abierta durante un periodo prolongado. Determina el tiempo máximo que la puerta puede permanecer abierta.
- **Forced Open**: Configura las acciones de alarma cuando la puerta se abra por la fuerza.
- **Anti PassBack** / **Timed Anti PassBack**: Configura las acciones de alarma para violaciones de anti-passback o anti-passback temporizado.

Información

La opción **Anti PassBack** está disponible únicamente si el dispositivo de salida está registrado.

Modificar la Información de la Puerta

Esta guía describe cómo modificar la información de configuración de la puerta de acceso registrada. Cambie la configuración detallada de puertas individuales o seleccione varias puertas para modificar en lote los elementos comunes.

Modificar la información de una puerta

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Door** en la barra lateral izquierda.
3. Haga clic en la puerta que desea modificar en la lista de puertas.
4. Modifique los detalles en cada sección.
5. Una vez completados todos los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.

Información

- Para obtener más información sobre cada sección de la pantalla 'Editar información de la puerta', consulte Registrar Puerta.
- Después de agregar una puerta a un grupo de acceso, configure la característica **Door Control through Authentication**. Para más información, consulte Configurar El Control De Puerta Mediante Autenticación.

Editar varias puertas en lote

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Door** en la barra lateral izquierda.
3. Haga clic en las casillas de las puertas que desea modificar en la lista de puertas. Seleccione dos o más puertas.
4. Haga clic en **Batch Edit** en la parte superior derecha de la pantalla.
5. Cuando aparezca la ventana **Batch Edit**, configure las opciones deseadas.



- **Open Time**: Configure la duración durante la cual la puerta permanece abierta después de completar la autenticación. La puerta se bloqueará automáticamente después de este tiempo.

6. Después de completar todas las configuraciones, haga clic en **Apply**.

> **Información**
> **Batch Edit** se activa solo cuando se seleccionan dos o más puertas de la lista de puertas.

Configurar El Control De Puerta Mediante Autenticación

El control de puerta mediante autenticación cambia una puerta a siempre abierta cuando un usuario designado se autentica dos veces seguidas (Double Badge) con la misma tarjeta en un dispositivo compatible. En el modo Siempre abierta, pase la tarjeta dos veces de nuevo. La puerta vuelve a su modo original cuando termina el horario permitido.

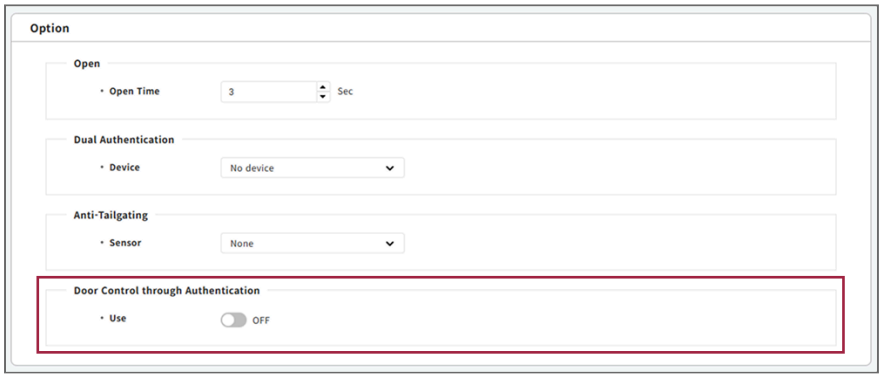
Antes de comenzar

- La puerta debe pertenecer a un grupo de acceso. En la pantalla Agregar puerta, esta característica no está disponible porque la puerta todavía no está en un grupo de acceso. Guarde la puerta, agréguela a un grupo de acceso, y configure esta característica en la pantalla Editar información de puerta. Para obtener más información sobre la configuración de grupos de acceso, consulte Configuración de Control de Acceso.
- Para obtener más información sobre agregar puertas y editar información de puerta, consulte los siguientes documentos.
  - Registrar Puerta
  - Modificar la Información de la Puerta

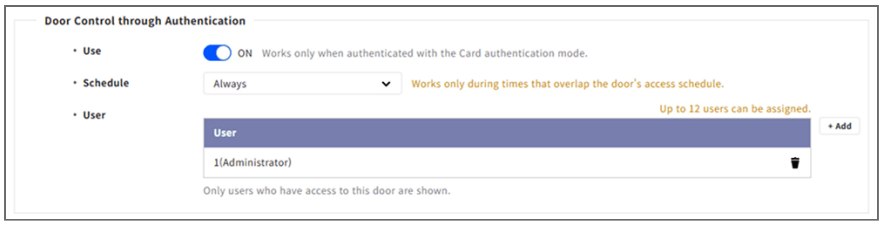
> **Información**
> - El soporte para el control de puerta mediante autenticación comienza con los siguientes dispositivos y versiones de firmware. Use esta característica solo en puertas que usen dispositivos compatibles.
>   - XPass 2 versión de firmware 1.5.3 o superior
>   - FaceStation F2 versión de firmware 2.3.0 o superior
> - Esta característica funciona solo con credenciales de tipo tarjeta (CSN, Wiegand, tarjetas inteligentes, y CSN/ToM de tarjeta móvil). Esta característica no aplica a credenciales de plantilla ni a autenticación biométrica, como huella digital y autenticación facial. El sistema las procesa como autenticación de acceso estándar.
> - El control de puerta mediante autenticación funciona solo cuando el modo de autenticación del dispositivo se establece en Tarjeta. **BioStar X** no verifica el modo de autenticación del dispositivo. Verifique el modo de autenticación del dispositivo antes de usar esta característica.
> - El dispositivo reconoce una doble credencial solo cuando ambas autenticaciones ocurren dentro de 3 segundos. Si el intervalo supera 3 segundos, el dispositivo trata cada autenticación como una autenticación de acceso independiente.

Configurar el control de puerta mediante autenticación

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Door** en la barra lateral izquierda.
3. En la lista de puertas, haz clic en la puerta que vas a configurar.
4. En la sección **Option**, ve a **Door Control through Authentication**.

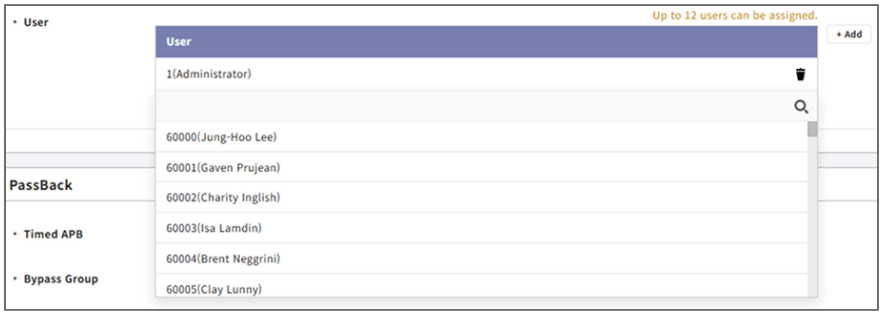


5. Establezca la opción **Use** en **ON**.



6. En **Schedule**, seleccione el horario para usar esta función. El valor predeterminado es **Siempre**. Si el horario no está disponible, agregue un horario primero.

7. Para agregar usuarios que pueden controlar la puerta con Double Badge, haga clic en **+ Add** y seleccione usuarios en la lista de **User**.



- La lista de **User** muestra solo usuarios con acceso a la puerta. Verifique los grupos de acceso y los niveles de acceso en **Settings** → **Access Management** → **Access Control**.
- Especifique hasta 12 usuarios.
- Haga clic en Q para buscar un usuario específico.
- Seleccione solo usuarios individuales. La selección de grupos de usuarios no está disponible.

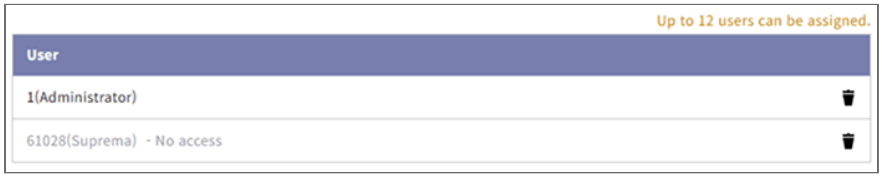
8. Una vez completados todos los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.

Información

- Para obtener más información sobre cómo agregar horarios, consulte Ajustes de Horario.
- Para obtener más información sobre cómo establecer grupos de acceso y niveles de acceso, consulte Configuración de Control de Acceso.

Notas

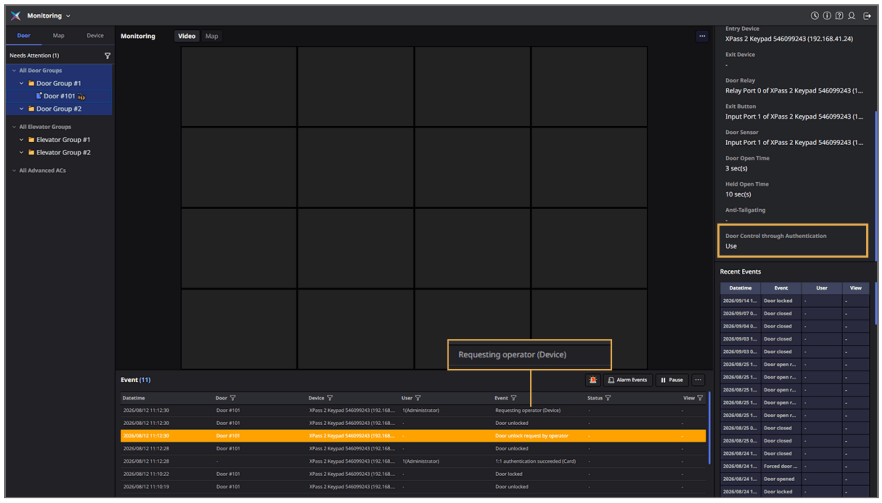
- Las puertas que usan control de puerta mediante autenticación no pueden cambiar el dispositivo de entrada o salida por un modelo no compatible. Antes de cambiar el dispositivo, establezca **Door Control through Authentication** en **OFF**.
- Si un usuario de control pierde el acceso a la puerta, la lista lo marca como **No access**. Este estado impide guardar. Otorgue el acceso de nuevo o elimine al usuario de la lista.



- Guardar requiere al menos un usuario de control.
- Si se elimina el horario seleccionado, el campo **Schedule** muestra **Deleted Schedule**. Este estado impide guardar. Seleccione otro horario.
- En el modo estricto, el sistema niega el acceso cuando ocurre una infracción de antirretorno, por lo que el control de puerta mediante autenticación no funciona. En el modo flexible, el sistema permite el acceso, por lo que sí funciona.
- Cuando se aplican otras funciones avanzadas de control de acceso, tienen prioridad.

Información relacionada

- Verifique el control de puerta mediante autenticación en el panel de vista previa de la puerta en **Monitoring**. Los eventos relacionados aparecen como **Requesting operator** en **Event**. Para obtener más información sobre el monitoreo de puertas, consulte Monitorear Puertas.



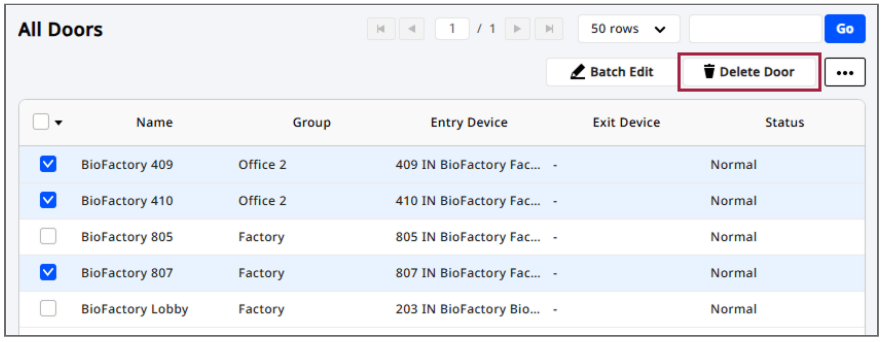
- El registro de auditoría registra los cambios en los ajustes. Para más información, consulte Ver Registros de Auditoría de Control de Acceso.

Borrar Puerta

Esta guía describe cómo eliminar puertas registradas.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Door** en la barra lateral izquierda.

3. Haz clic en la casilla de la puerta que deseas eliminar de la lista.
4. Haga clic en **Delete Door** en la esquina superior derecha de la pantalla.



5. Haga clic en **Yes** cuando aparezca la ventana del mensaje de confirmación.

La puerta seleccionada se eliminará. Las puertas eliminadas no se pueden recuperar.

> **Información**
> El sistema habilita **Delete Door** solo cuando hay una o más puertas seleccionadas en la lista de puertas de acceso.

Gestionar Permisos de Operación

Esta guía describe cómo asignar permisos de operador y añadir y configurar permisos personalizados a los usuarios registrados. Los permisos de operador controlan las tareas que un usuario puede realizar en **Biostar X**. **Los permisos personalizados** permiten establecer permisos adicionales más allá de los permisos de operador predeterminados.

Comprobar tipos de permisos

Haz clic en **Settings** en la página **Launcher**. Haga clic en **Account** → **Account** en la barra lateral izquierda. Consulta las cuentas proporcionadas según los niveles de permiso.

- **Administrator**: Este es un nivel de administrador que puede usar todos los menús.
- **User Operator**: El menú **User** tiene permisos de **lectura** y **edición**. Otros grupos de ajustes no tienen permisos, excepto el menú **User**.
- **Monitoring Operator**: Los menús **Monitoring** y **Data** tienen permisos de **lectura** y **edición**, y el menú **Dashboard** tiene permiso de **lectura**.
- **T&A Operator**: El menú **TIME ATTENDANCE** tiene permisos de **lectura** y **edición**, y el menú **User** tiene permiso de **lectura**.
- **Visitor Operator**: El menú **VISITOR** tiene permisos de **lectura** y **edición**.

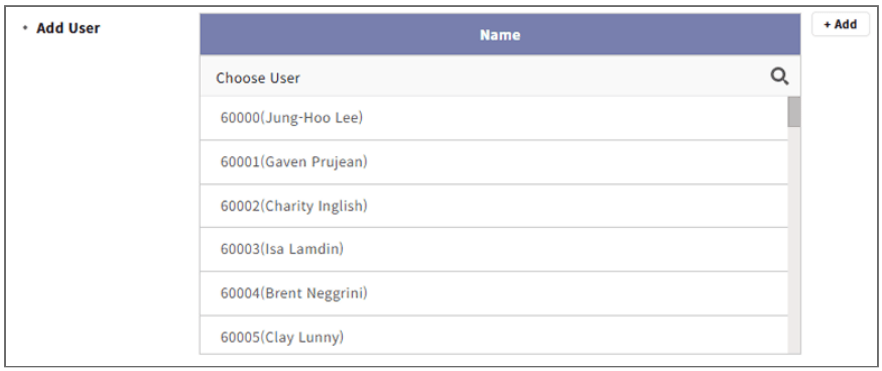
Información

- El permiso de **edición** del menú **Monitoring** permite agregar pestañas o controlar las entradas del árbol de estado.
- El permiso de **edición** del menú **Data** permite guardar informes, agregar programaciones automáticas de informes y acceder a los ajustes.
- Para obtener más información sobre cómo agregar permisos de usuario personalizados, consulte Agregar Permisos Personalizados.
- Los permisos de las cuentas predeterminadas no se pueden modificar ni eliminar.
- Niveles como **T&A Operator** y **Visitor Operator** requieren licencias por separado. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Conceder permisos de operador a los usuarios

Guía para conceder permisos de operador a usuarios generales.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Account** → **Account** en la barra lateral izquierda.
3. Haz clic en el elemento deseado de la lista de cuentas.
4. Haz clic en **+ Add** en la opción **Add User**.



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

5. Selecciona en la lista de usuarios al usuario al que deseas conceder permisos de operador.
6. Después de seleccionar todos los usuarios deseados, haz clic en **Apply** en la parte inferior de la pantalla.

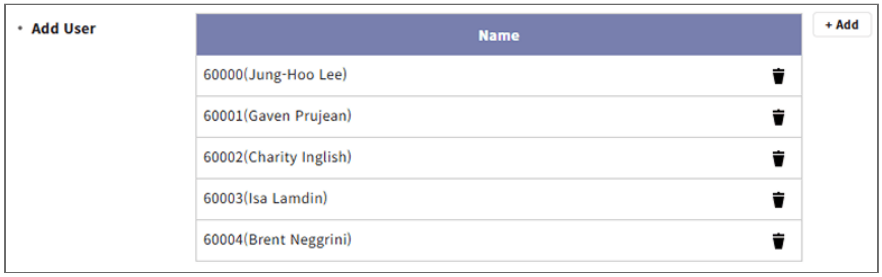
Información

- Si resulta difícil encontrar usuarios debido a su cantidad, haz clic en 🔍 para buscarlos y seleccionar el usuario deseado.
- Los permisos de operador también se pueden conceder al añadir o modificar la información del usuario. Para obtener más información, consulta Configurar Permisos de Usuario.
- Si los permisos ya se configuraron al añadir o modificar la información del usuario, se incluirán en la opción **Add User**.

Excluir permisos de operador

Guía para excluir los permisos de operador concedidos a los usuarios.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Account** → **Account** en la barra lateral izquierda.
3. Haz clic en el tipo de cuenta deseado de la lista de cuentas.
4. Haz clic en para el usuario que se excluirá de la operación en la opción **Add User**.

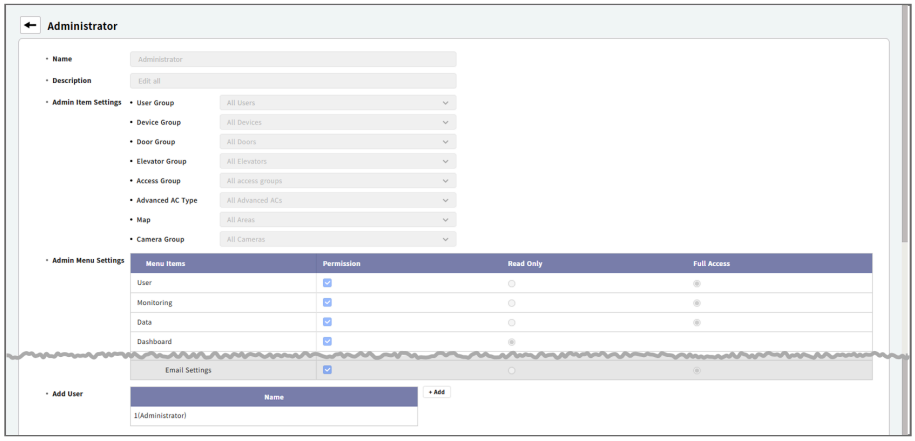


La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

5. Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.

Comprobar detalles de permisos de operador

Haz clic en una cuenta de la lista del menú **Account** para ver los detalles de permisos de operador.



- **Name**: Nombre del permiso de operador seleccionado.
- **Description**: Descripción breve del permiso.
- **Admin Item Settings**: Permite ver los grupos con permisos concedidos, elemento por elemento.
- **Admin Menu Settings**: Permite ver los permisos concedidos para acceder al menú.
  - **Read Only**: Concede permiso para añadir, editar o eliminar opciones del menú.
  - **Full Access**: Concede permiso para entrar al menú y solo ver los ajustes.
- **Add User**: Permite ver los usuarios con permisos concedidos.

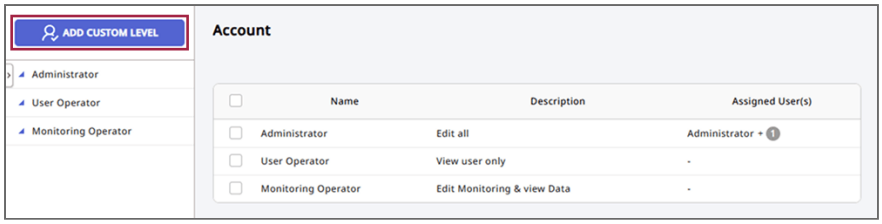
> **Información**
>
> Para obtener más información sobre cómo conceder permisos a un usuario específico, consulta Conceder permisos de operador a los usuarios.

Agregar Permisos Personalizados

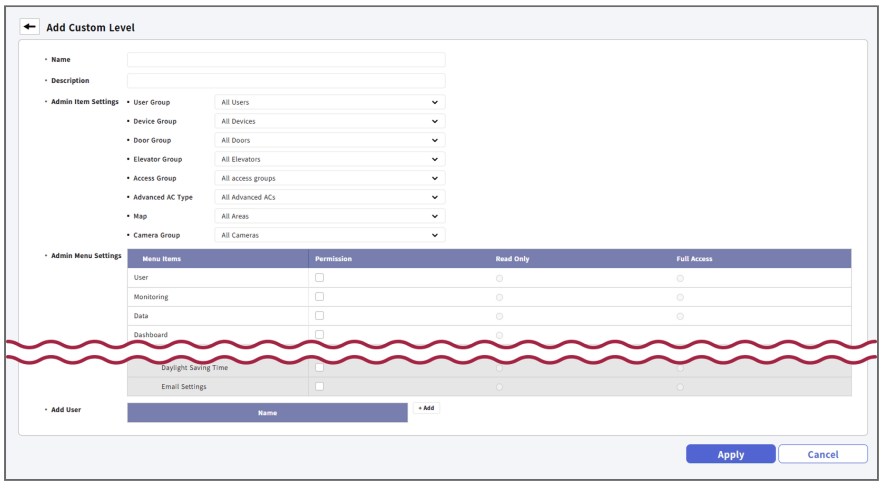
Esta guía describe cómo agregar el nivel de permiso deseado. Los permisos personalizados son funciones que el usuario puede personalizar y que permiten permisos adicionales más allá de los permisos operativos predeterminados.

Agregar permisos personalizados

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Account** → **Account** en la barra lateral izquierda.
3. Haga clic en **Add Custom Level**.



4. Ingrese un nombre y una descripción para el permiso recién creado.



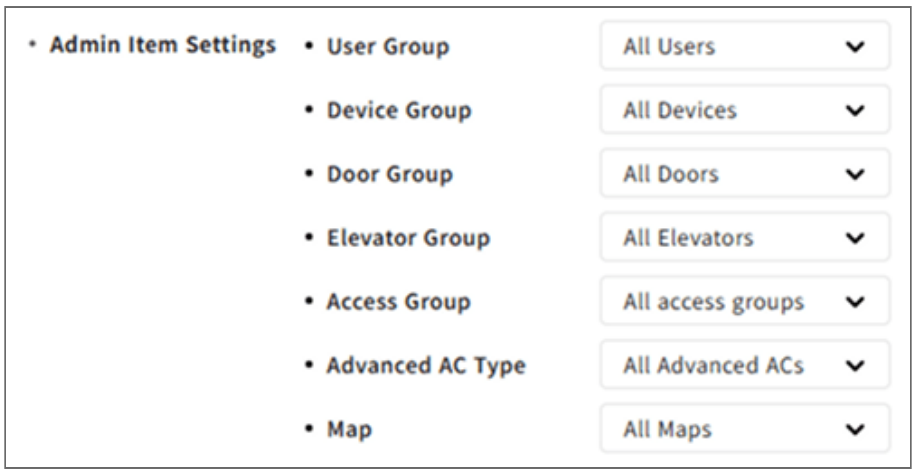
5. Complete o seleccione cada uno de los elementos restantes.
6. Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.

Información

- Los tipos de ajustes de **Admin Menu Settings** que puede configurar pueden variar según el tipo de licencia activada.
- Para obtener más información sobre **Admin Item Settings**, consulte detailSetting.
- Para obtener más información sobre **Admin Menu Settings**, consulte menuSetting.
- Para obtener más información sobre **Add User**, consulte addUser.

Admin Item Settings

Configure permisos detallados para los elementos. Seleccione grupos para otorgar permisos de edición y visualización para cada menú. Establezca permisos de elementos para **User Group**, **Device Group**, **Door Group**, **Access Group** basándose en la información de los grupos ya creados en cada menú.

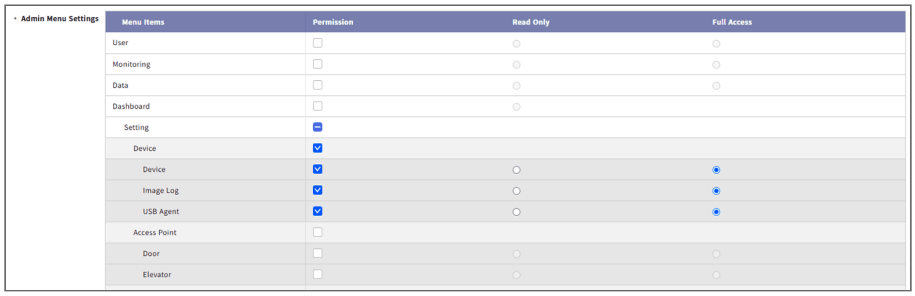


Información

- Si el grupo que desea no está disponible, diríjase al menú correspondiente para agregar un nuevo grupo. Para más información sobre cómo agregar grupos, consulte lo siguiente:
  - Administrar Grupos de Usuarios
  - Gestionar Grupos de Dispositivos
  - Administrar Grupo de Puertas
  - Administrar Grupo de Ascensores
  - Administrar Grupos de Acceso
- El permiso **Map** está disponible con una licencia **Essential** o superior. Para obtener más información sobre la política de licencias, consulte Política de Licencias.
- Los permisos **Elevator Group**, **Advanced AC Type**, **Camera Group** están disponibles como una opción adicional con una licencia **Essential** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Admin Menu Settings

Seleccione **Read Only** o **Full Access** para cada menú. Asigne permisos diferentes a cada menú. Haga clic en la casilla **Permission** y luego seleccione **Read Only** o **Full Access**.



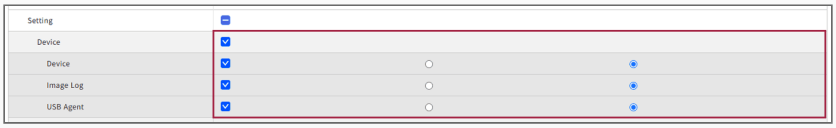
- **Read Only**: Concede permiso para entrar al menú y solo ver los ajustes.
- **Full Access**: Concede permiso para añadir, editar o eliminar entradas en el menú.

Información

- En el menú **Monitoring**, **Full Access** permite agregar pestañas o controlar las entradas del árbol de estados.
- En el menú **Data**, **Full Access** permite guardar informes, agregar programaciones automáticas de informes y acceder a los ajustes.
- En el menú **Dashboard**, el permiso **Read Only** permite crear nuevos dashboards y widgets.
- Los menús que no aparecen en **Menu Items** son accesibles independientemente de los permisos.

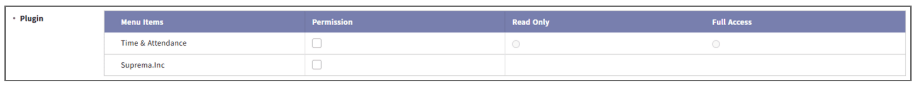
Consejo

Haga clic en un permiso del menú principal para habilitar los permisos en todos los submenús.



Conector

Después de agregar un plugin, configure los permisos del plugin. Los usuarios sin permisos del plugin no pueden acceder al plugin, y el plugin no aparece en la pantalla de inicio ni en el lanzador.

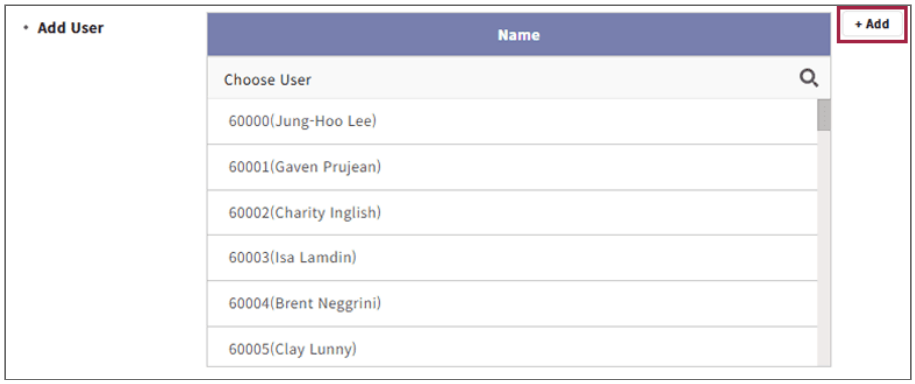


Información

- Se requiere una licencia de conector para utilizar las funciones de conector. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.
- Aplique **Read Only** o **Full Access** solo al plugin **Time & Attendance**.

Add User

Agregue o verifique la información del usuario para otorgar permisos. Haga clic en **+ Add** para agregar un usuario. Seleccione el usuario al que desea otorgar permisos de la lista de usuarios.



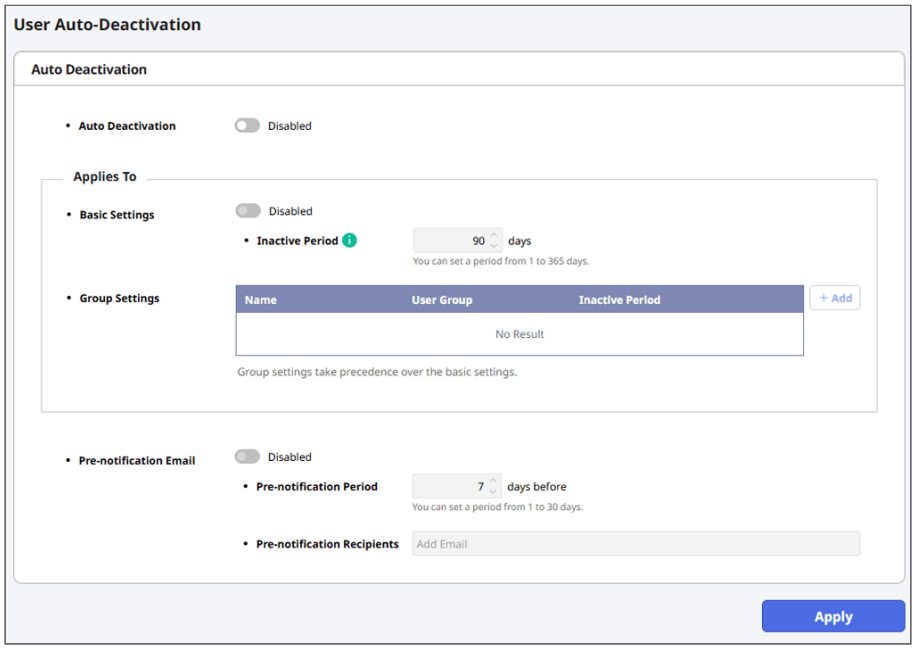
Información

Al hacer clic en junto a un usuario en la lista de usuarios, se excluirá a ese usuario de los permisos.

Administrar Usuarios Inactivos A Largo Plazo

Mantener activas las credenciales de usuarios que no han accedido durante mucho tiempo, como tras una renuncia o una licencia, puede generar riesgos de seguridad, como robo de credenciales y acceso no autorizado. La función de desactivación automática desactiva a los usuarios tras un período desde su último acceso. Los administradores gestionan las cuentas sin limpiar manualmente cada vez. Antes de la desactivación automática, el sistema envía un correo electrónico de aviso previo a los destinatarios especificados. Esto da tiempo para revisar o crear excepciones.

Haz clic en **Settings** en la página **Launcher**. Haga clic en **Account** → **User Auto-Deactivation** en la barra lateral izquierda.

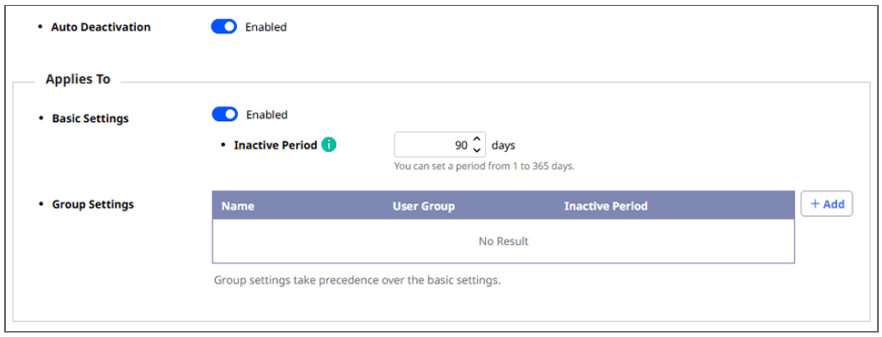


Información

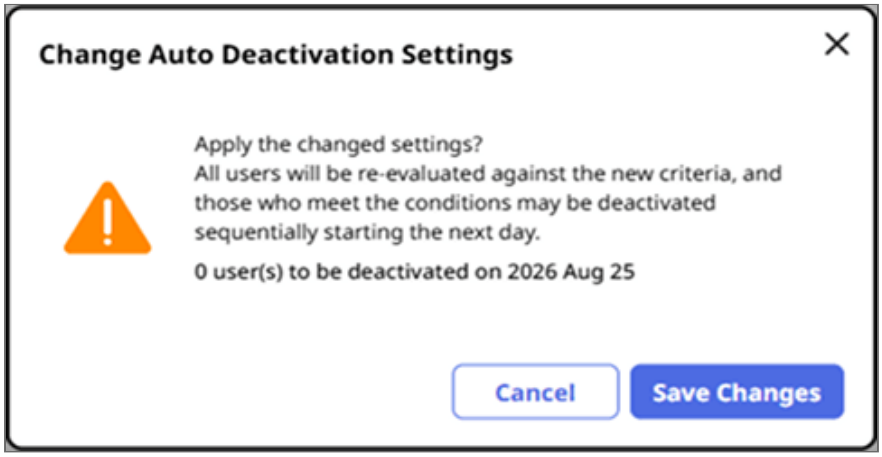
Solo los administradores con permiso para este menú pueden acceder a **Account** → **User Auto-Deactivation**. Para otorgar permiso a un administrador para un menú específico, consulte Gestionar Permisos de Operación.

Configurar la desactivación automática

1. En **Auto Deactivation**, haga clic en el interruptor para activarlo.
2. En la sección **Applies To**, defina los usuarios a los que se aplica la desactivación automática.



   - Para aplicar los mismos criterios a todos los usuarios, active **Basic Settings** e ingrese **Inactive Period**. Establezca un valor de 1 a 365 días.
   - Para aplicar criterios diferentes a ciertos grupos de usuarios, agregue **Group Settings**. Para obtener más información, consulte Aplicar criterios diferentes por grupo.
3. Cuando complete los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.
4. Cuando aparezca la ventana de confirmación, revise la próxima fecha de procesamiento automático y los usuarios programados para desactivación. Luego haga clic en **Save Changes**.



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

Información

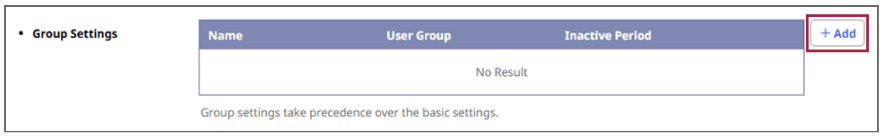
- Para enviar un correo electrónico a los destinatarios especificados antes de que el sistema desactive automáticamente a un usuario, configure **Pre-notification Email**. Consulte Ajustes del correo electrónico de notificación previa para obtener más detalles.
- Activar la opción **Auto Deactivation** no activa automáticamente **Basic Settings**. Para crear la política solo con **Group Settings**, mantenga desactivada **Basic Settings**.
- La desactivación automática usa la hora de autenticación del último acceso. El sistema excluye a los usuarios sin historial de acceso o con solo historial de acceso antes de la inscripción.
- Si un usuario cumple con **Basic Settings** y **Group Settings**, **Inactive Period** en **Group Settings** tiene prioridad. Si el usuario pertenece a 2 o más **Group Settings**, el sistema aplica el **Inactive Period** más corto.
- La desactivación automática se ejecuta 1 vez al día (medianoche). El sistema aplica los cambios de ajuste en el siguiente tiempo de procesamiento y no afecta las programaciones de avisos anticipados ya enviadas.
- Al establecer la opción **Auto Deactivation** en inactivo, el sistema la guarda de inmediato sin un cuadro de diálogo de confirmación.

Aplicar criterios diferentes por grupo

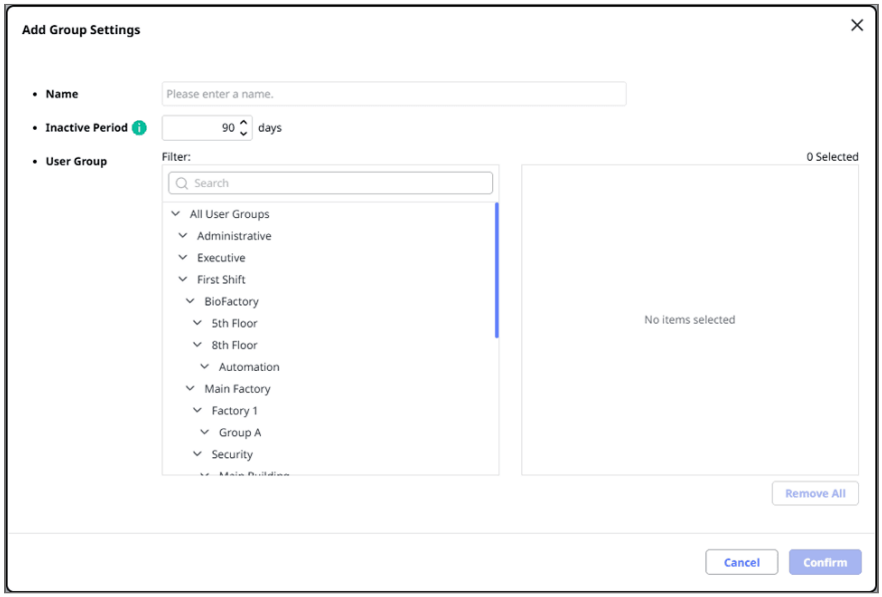
Aplica a ciertos grupos de usuarios un **Inactive Period** diferente al de **Basic Settings**.

Agregar ajustes de grupo

1. Haz clic en **+ Add** a la derecha de la lista **Group Settings**.



2. Cuando aparezca la ventana **Add Group Settings**, configura cada campo.



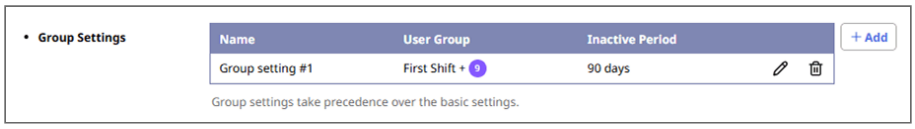
- **Name**: Ingresa un nombre que no se repita en otros ajustes de grupo. Las mayúsculas y minúsculas, y los espacios al inicio o al final, no importan.
- **Inactive Period**: Configura de 1 a 365 días.

- **User Group**: Selecciona los grupos de usuarios a los que aplica este ajuste. Al seleccionar un grupo, el sistema también selecciona sus subgrupos.

3. Después de seleccionar los grupos de usuarios, haz clic en **Confirm**.
4. Haz clic en **Apply** en la parte inferior de la pantalla para guardar los ajustes.
5. Cuando aparezca la ventana de confirmación, revise la próxima fecha de procesamiento automático y los usuarios programados para desactivación. Luego haga clic en **Save Changes**.

> **Información**
>
> - En **User Group**, los grupos de usuarios fuera del alcance de permisos del administrador aparecen deshabilitados, pero siguen visibles en la lista. Expande este grupo. Selecciona los subgrupos dentro del alcance de permisos.
> - Los administradores con privilegios configurados en **Todos los usuarios**, o los administradores completos, no tienen límites en la selección de grupos de usuarios. Para obtener más información sobre los roles de administrador, consulta Gestionar Permisos de Operación.

Editar y eliminar ajustes de grupo



- Para editar, en la lista **Group Settings**, haz clic en ✎ en la fila deseada, cambia el valor y haz clic en **Confirm**.
- Haz clic en 🗑 en la fila que deseas eliminar. Cuando aparezca el mensaje de confirmación, haga clic en **Delete**.

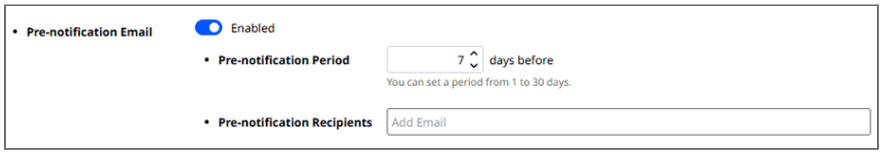
Para guardar sus ediciones o eliminaciones, haga clic en **Apply** en la parte inferior de la pantalla. Cuando aparezca la ventana de confirmación, revise la próxima fecha de procesamiento automático y los usuarios programados para desactivación. Luego haga clic en **Save Changes**.

> **Información**
>
> - Si **Group Settings** incluye grupos de usuarios fuera del alcance de permisos del administrador, la lista todavía los muestra. El sistema desactiva la edición y la eliminación.
> - **Group Settings** tiene prioridad sobre **Basic Settings**.
> - Eliminar **Group Settings** no reactiva a los usuarios ya desactivados. Después de la eliminación, el sistema cambia a otra configuración aplicable (como **Basic Settings**).

Ajustes del correo electrónico de notificación previa

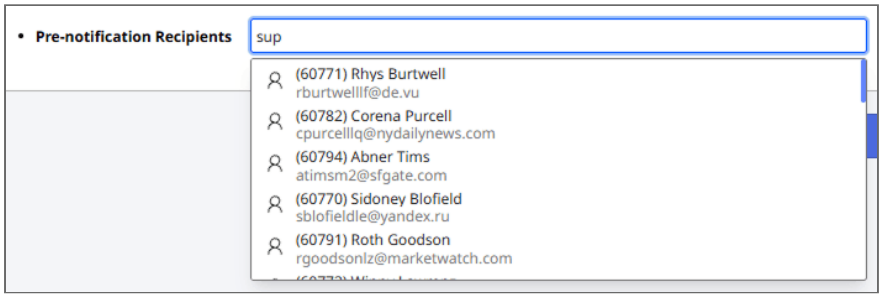
Esta característica envía un aviso por correo electrónico a destinatarios específicos antes de que el sistema desactive automáticamente a los usuarios.

1. Haga clic en el interruptor de la opción **Pre-notification Email** para activarla.



2. Ingrese un valor para **Pre-notification Period**. El sistema envía correos electrónicos de aviso de desactivación automática durante el período ingresado. Establezca el período de 1 a 30 días.

3. En el campo **Pre-notification Recipients**, busque y seleccione un usuario por nombre, ID o correo electrónico, o ingrese una dirección de correo electrónico y luego presione `Enter`.



4. Cuando complete los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.

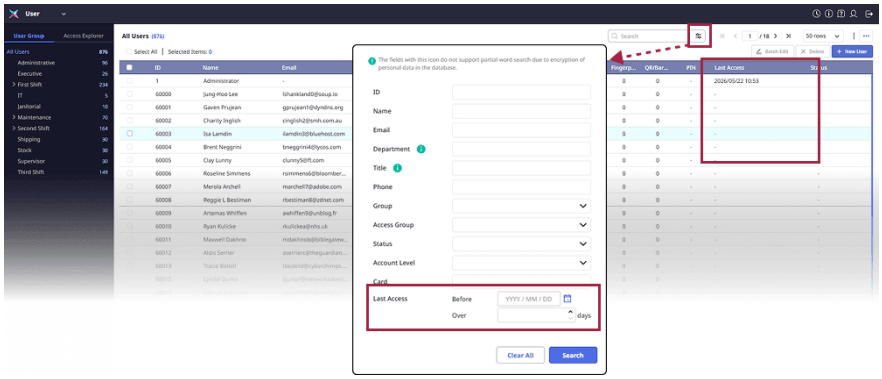
5. Cuando aparezca la ventana de confirmación, revise la próxima fecha de procesamiento automático y los usuarios programados para desactivación. Luego haga clic en **Save Changes**.

Información

- Configure los ajustes de SMTP para usar correos electrónicos de notificación previa. Para obtener más información, consulta Configuración de Correo Electrónico.
- Establezca **Pre-notification Period** en un valor menor que el período de inactividad de **Basic Settings** y de cada **Group Settings**.
- Agregue direcciones de correo electrónico que no estén en **BioStar X** como destinatarios.
- El sistema envía un correo electrónico consolidado 1 vez al día, no correos separados para cada usuario.
- Si **Basic Settings** está desactivado y no existe **Group Settings**, el sistema no envía correos electrónicos porque no hay destinatarios al activar solo **Pre-notification Email**.

Información relacionada

- Vea los usuarios inactivos a largo plazo en la columna **Last Access** de la lista de usuarios, o use Búsqueda avanzada. Para obtener más información sobre cómo seleccionar las opciones de visualización, consulte Explorar Usuarios.

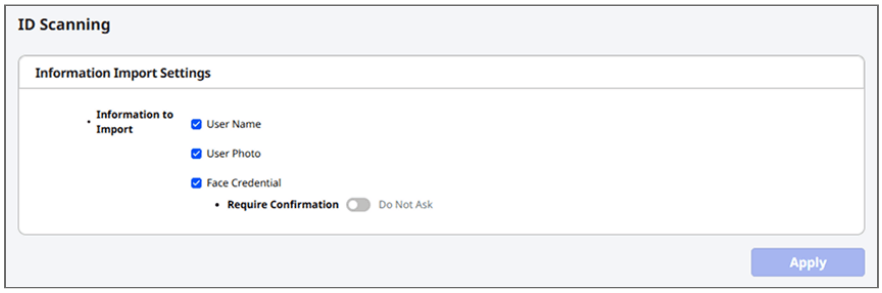


- Revise el historial de usuarios desactivados automática o manualmente en el informe **Inactive Users**. Para obtener más información sobre cómo seleccionar las opciones de visualización, consulte Generar Reporte.

Configurar Escaneo De ID

Antes de inscribir usuarios con el escaneo de ID, elige nombre de usuario e imagen de perfil para importar. Luego, selecciona el método de inscripción de credenciales faciales. Este artículo explica cómo configurar el escaneo de ID.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Account** → **ID Scanning** en la barra lateral izquierda.



3. Selecciona los datos que se importarán al escanear un ID.
   - **User Name**: Importa el nombre impreso en el ID.
   - **User Photo**: Importa la imagen de perfil impresa en el ID.
   - **Face Credential**: Inscribe la imagen facial impresa en el ID como una credencial facial.
     - **Require Confirmation**: Siempre solicita confirmación al inscribir la imagen facial impresa en el ID como una credencial facial.
     - **Do Not Ask**: Inscribe la imagen facial impresa en el ID como una credencial facial sin solicitar confirmación.
4. Haga clic en **Apply** para guardar la configuración.

> **Información**
>
> - Selecciona **User Photo** para activar **Face Credential**.
> - Para obtener más información sobre inscribir o actualizar usuarios con el escaneo de ID, consulta Inscribir Y Editar Usuarios Al Escanear Un ID.

Configuración de Control de Acceso

Esta guía describe cómo configurar el sistema de control de acceso. Establezca puntos de entrada y horarios de entrada para crear niveles de acceso y configure grupos de acceso usando los niveles de acceso y la información de grupos de usuarios. Use los grupos de acceso configurados para la configuración del control de acceso.

Administrar Niveles de Acceso

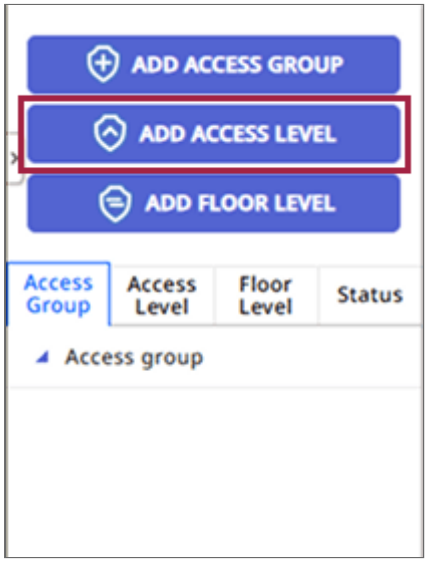
Los niveles de acceso permiten a los usuarios establecer horarios de entrada y conceder permiso para acceder a las puertas durante esos horarios. Los niveles de acceso son un elemento clave para configurar grupos de acceso.

Antes de comenzar

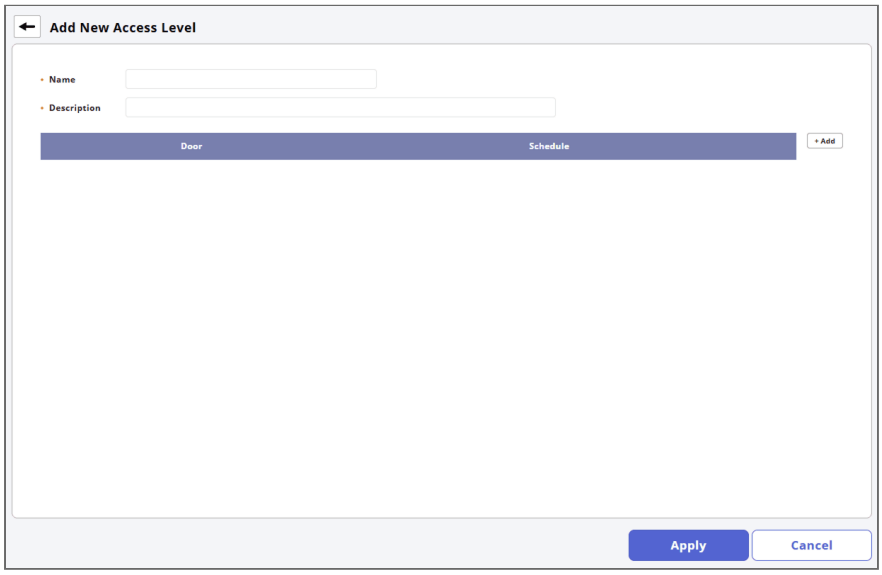
- Inicializa las puertas antes de registrar niveles de acceso. Para obtener más información sobre el registro de puertas, consulte Registrar Puerta.
- Predefine los horarios que se aplicarán a los niveles de acceso mediante los ajustes de programación. Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

Inscribir nivel de acceso

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Access Control** en la barra lateral izquierda.
3. Haz clic en **ADD ACCESS LEVEL**.



4. Ingresa **Name** y **Description** en la pantalla **Add New Access Level**.



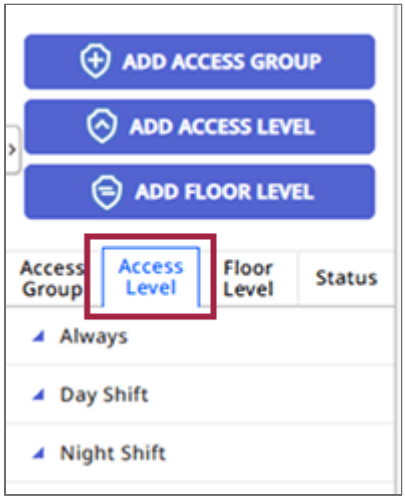
5. Selecciona la puerta a la que se aplicará el nivel de acceso en el campo **Door**.
6. Selecciona el horario que se aplicará al nivel de acceso en el campo **Schedule**.
7. Haz clic en **Apply** en la parte inferior de la pantalla para registrar el nivel de acceso.

Información

- Se pueden registrar hasta 128 niveles de acceso por grupo de acceso.
- Haz clic en en los campos **Door** y **Schedule** para buscar las puertas y horarios deseados.
- Haz clic en para eliminar los elementos añadidos en los campos **Door** y **Schedule**.
- Si la puerta deseada no está disponible, registra una nueva puerta. Para obtener más información sobre el registro de puertas, consulte Registrar Puerta.
- Si el horario deseado no está disponible, haz clic en **+ Add Schedule** para agregar uno. Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

Modificar nivel de acceso

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Access Control** en la barra lateral izquierda.
3. Haz clic en la pestaña **Access Level**.



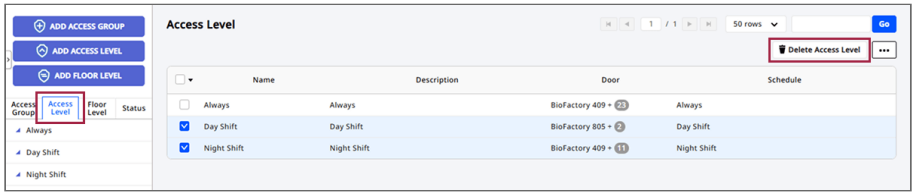
4. Haz clic en el nivel de acceso que desees modificar en la lista de niveles de acceso.
5. Modifique los elementos deseados.
6. Una vez que complete las modificaciones, haga clic en **Apply** en la parte inferior de la pantalla.

Eliminar nivel de acceso

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Access Control** en la barra lateral izquierda.
3. Haz clic en la pestaña **Access Level**.

4. Marca la casilla del nivel de acceso que desees eliminar de la lista de niveles de acceso.

5. Haz clic en **Delete Access Level** en la parte superior derecha de la pantalla.



Administrar Grupos de Acceso

Esta guía describe cómo configurar grupos de acceso mediante niveles de acceso e información de grupos de usuarios. Los grupos de acceso son elementos cruciales que definen el permiso para acceder a las puertas. Configurar grupos de acceso permite administrar los permisos de los usuarios para acceder a las puertas.

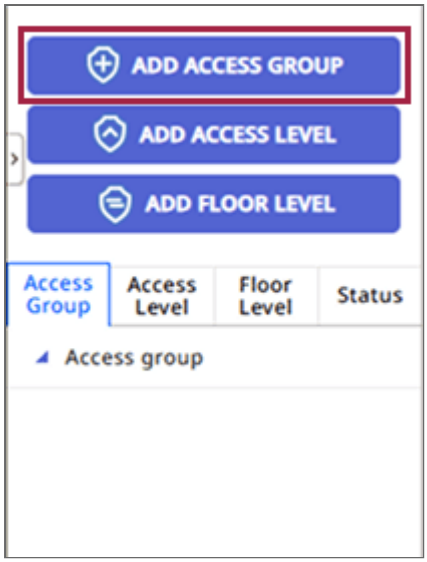
Antes de comenzar

Confirme lo siguiente antes de registrar grupos de acceso.

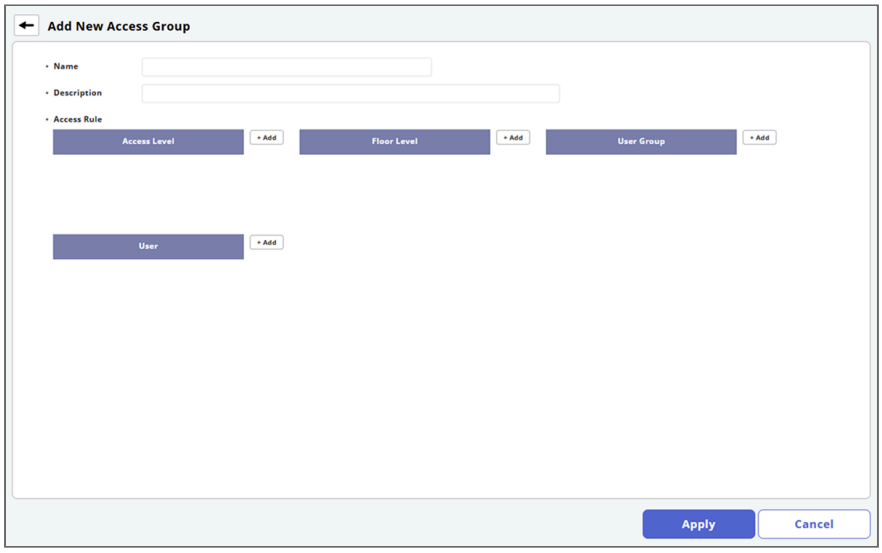
- Configure niveles de acceso. Para obtener más información sobre cómo registrar niveles de acceso, consulte Administrar Niveles de Acceso.
- Configure niveles de piso. Para obtener más información sobre cómo registrar los niveles de planta, consulte Gestionar Niveles de Piso.
- Configure grupos de usuarios. Para obtener más información sobre cómo registrar los grupos de usuarios, consulte Administrar Grupos de Usuarios.

Registrar grupos de acceso

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Access Control** en la barra lateral izquierda.
3. Haga clic en **ADD ACCESS GROUP**.



4. En la pantalla **Add New Access Group**, ingrese **Name** y **Description**.



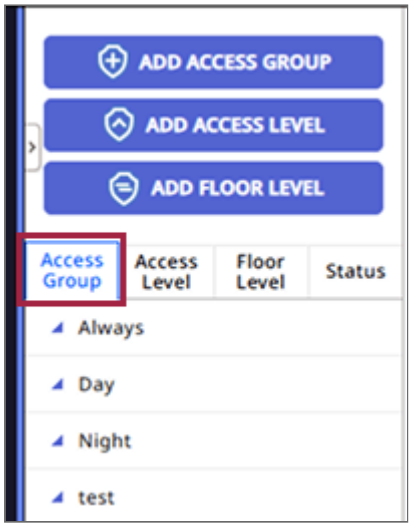
5. En el campo **Access Level**, haga clic en **+ Add** para seleccionar los niveles de acceso que se aplicarán al grupo de acceso.
6. En el campo **Floor Level**, haga clic en **+ Add** para seleccionar los niveles de piso que se aplicarán al grupo de acceso.
7. En el campo **User Group**, haga clic en **+ Add** para seleccionar los grupos de usuarios que se aplicarán al grupo de acceso.
8. En el campo **User**, haga clic en **+ Add** para seleccionar los usuarios para el grupo de acceso.
9. Haga clic en **Apply** en la parte inferior de la pantalla para registrar el grupo de acceso.

Información

- Si el nivel de acceso deseado no está disponible, deberá registrar uno nuevo. Para obtener más información sobre cómo registrar niveles de acceso, consulte Administrar Niveles de Acceso.
- Si el nivel de piso deseado no está disponible, deberá registrar uno nuevo. Para obtener más información sobre cómo registrar los niveles de planta, consulte Gestionar Niveles de Piso.
- Haga clic en para eliminar los elementos agregados.
- Haga clic en para buscar el elemento deseado.

Editar grupos de acceso

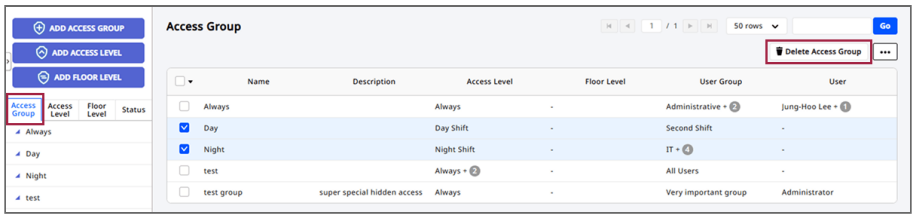
1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Access Control** en la barra lateral izquierda.
3. Haga clic en la pestaña **Access Group**.



4. Haga clic en el grupo de acceso que desea editar de la lista.
5. Modifique los elementos deseados.
6. Una vez que complete las modificaciones, haga clic en **Apply** en la parte inferior de la pantalla.

Borrar grupos de acceso

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Access Control** en la barra lateral izquierda.
3. Haga clic en la pestaña **Access Group**.
4. Marque la casilla del grupo de acceso que desea borrar de la lista.
5. Haga clic en **Delete Access Group** en la esquina superior derecha de la pantalla.



Gestionar Niveles de Piso

Esta guía describe cómo definir los niveles de piso con la información de elevador y piso configurada. Los niveles de piso son elementos importantes que se pueden aplicar a los grupos de acceso. Al definir los niveles de piso, gestiona los pisos a los que los usuarios pueden acceder mediante el elevador.

> **Información**
>
> Las licencias **Essential** y superiores incluyen características de nivel de piso mediante opciones complementarias. Para obtener más información sobre la política de licencias, consulte Política de Licencias.

Antes de comenzar

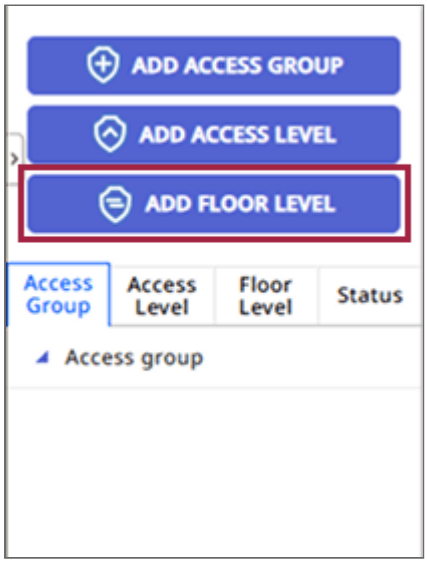
- Configure el elevador antes de registrar los niveles de piso. Consulte Registrar Ascensor para obtener más información

sobre cómo registrar un ascensor.

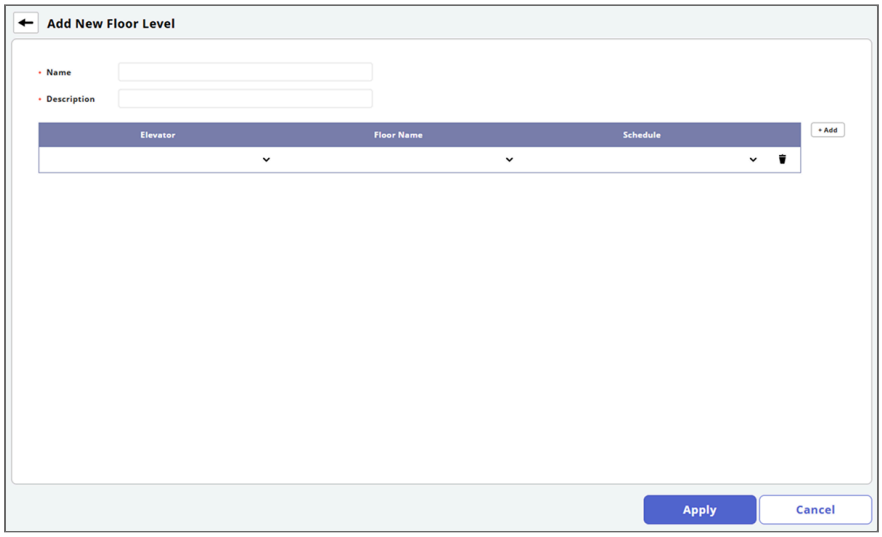
- Defina con antelación el horario que se aplicará al nivel de piso mediante la configuración de horarios. Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

Registrar niveles de piso

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Access Control** en la barra lateral izquierda.
3. Haga clic en **ADD FLOOR LEVEL**.



4. En la pantalla **Add New Floor Level**, ingrese **Name** y **Description**.



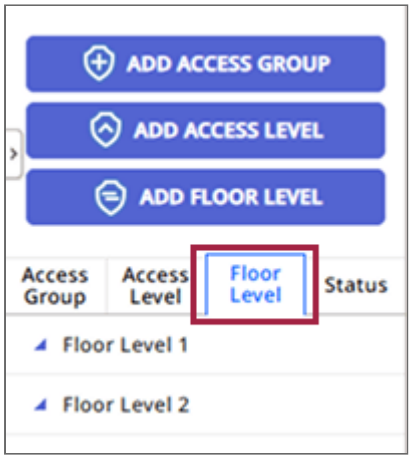
5. Seleccione el elevador que se aplicará al nivel de piso en el elemento **Elevator**.
6. Seleccione el piso que se aplicará al nivel de piso en el elemento **Floor Name**.
7. Seleccione el horario que se aplicará al nivel de piso en el elemento **Schedule**.
8. Haga clic en **Apply** en la parte inferior de la pantalla para registrar el nivel de piso.

Información

- Si el nivel de acceso deseado no está disponible, deberá registrar uno nuevo. Para obtener más información sobre cómo registrar niveles de acceso, consulte Administrar Niveles de Acceso.
- Registre un nuevo elevador si el deseado no está disponible. Consulte Registrar Ascensor para obtener más información sobre cómo registrar un ascensor.
- Si el horario deseado no está disponible, haz clic en **+ Add Schedule** para agregar uno. Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.
- Haga clic en para eliminar los elementos agregados.
- Haga clic en para buscar el elemento deseado.

Editar niveles de piso

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Access Control** en la barra lateral izquierda.
3. Haga clic en la pestaña **Floor Level**.



4. Haga clic en el nivel de piso que desea editar en la lista de niveles de piso.
5. Modifique los elementos deseados.
6. Una vez que complete las modificaciones, haga clic en **Apply** en la parte inferior de la pantalla.

Eliminar niveles de piso

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Access Control** en la barra lateral izquierda.
3. Haga clic en la pestaña **Floor Level**.
4. Seleccione la casilla de verificación del nivel de piso que desea eliminar de la lista de niveles de piso.
5. Haga clic en **Delete Floor Level** en la parte superior derecha de la pantalla.

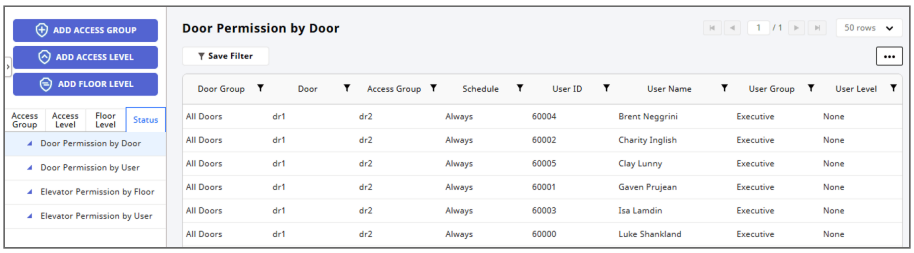


Verificar Estado de Permisos de Acceso

Esta guía explica cómo verificar la lista de puertas a las que pueden acceder los usuarios. Al verificar el estado de los permisos de acceso, podrá administrar las puertas a las que un usuario puede acceder y los permisos para esas puertas. Utilice la función de filtro para ordenar los resultados deseados y guardar la lista en un archivo CSV.

Verificar estado de permisos de acceso

Los permisos de acceso pueden visualizarse por puerta o piso, o por usuario.



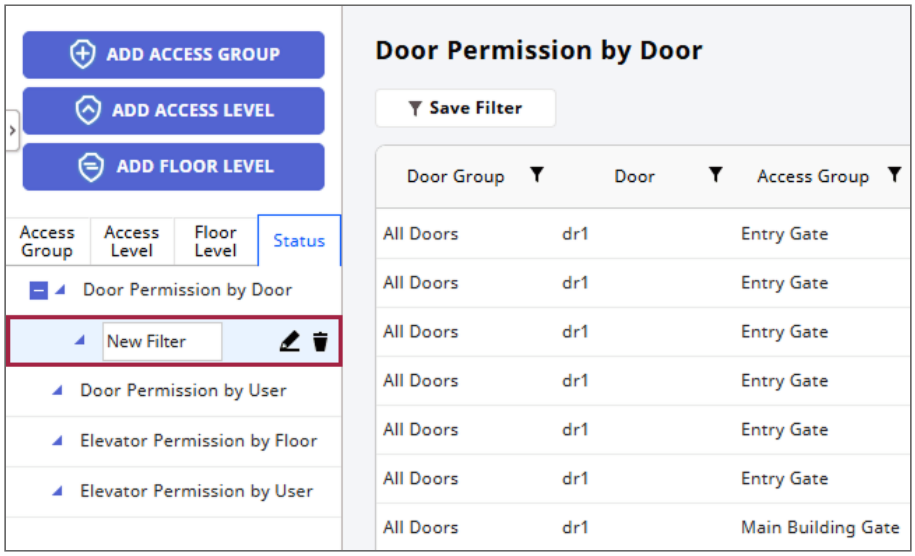
1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Access Control** en la barra lateral izquierda.
3. Haga clic en la pestaña **Status**.
4. Haga clic en el elemento deseado de la lista de estados en la pestaña **Status**.
   - **Door Permission by Door**
   - **Door Permission by User**
   - **Elevator Permission by Floor**
   - **Elevator Permission by User**

Podrá verificar el estado de permisos de acceso del elemento seleccionado.

Guardar filtro

Haga clic en el botón ▼ en el encabezado de la tabla de lista de permisos de acceso para ordenar los resultados deseados. Puede añadir condiciones de filtro.

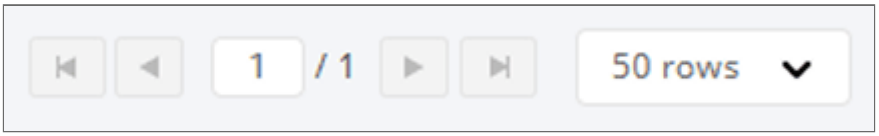
Después de configurar el filtro, podrá guardarlo. Haga clic en **Save Filter**. El filtro guardado se puede consultar en la lista de estados de la pestaña **Status**.



- Haga clic en para cambiar el nombre del filtro.
- Haga clic en para eliminar el filtro.

Navega por la página de lista

Desplácese entre páginas o establezca la cantidad de elementos que aparecerán en cada página. Utiliza la herramienta de navegación de página en la esquina superior derecha de la pantalla.



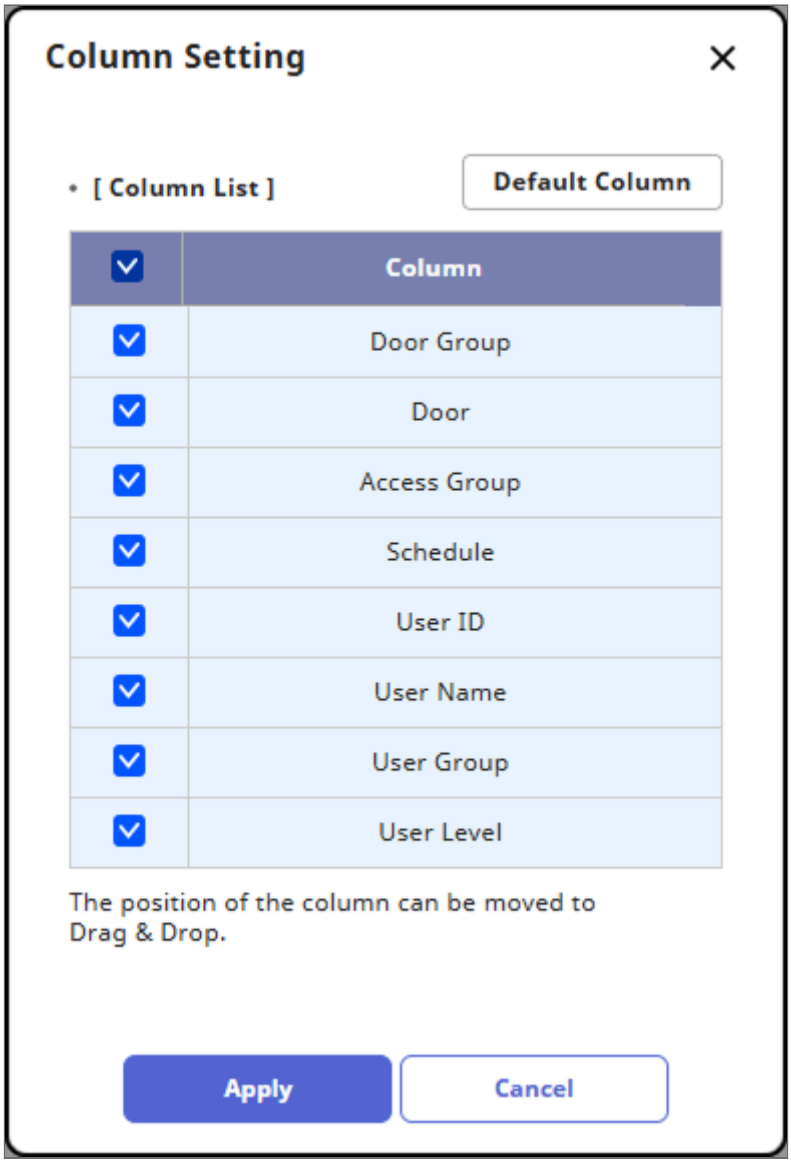
- : Ir a la primera página.
- : Ir a la página anterior.
- : Ir a la página siguiente.
- : Ir a la última página.
- Ingresa el número de página en el campo de entrada para ir a la página deseada.
- Haz clic en el cuadro de selección de filas para establecer la cantidad de elementos que se muestran en cada página.

Exportar a CSV

Puede exportar la lista actual de estado de permisos de acceso como archivo CSV. Haga clic en en la esquina superior derecha de la pantalla y seleccione **CSV Export**.

Configurar columnas

Puede ocultar o mostrar las columnas deseadas en la tabla de la lista de estado de permisos de acceso. Haga clic en en la esquina superior derecha de la pantalla y seleccione **Column Setting**.



- Seleccione las columnas que se mostrarán desde **Column List**. Las columnas seleccionadas aparecerán en la tabla de la lista. Las columnas no seleccionadas se ocultarán de la tabla de la lista.
- Haga clic en **Default Column** para inicializar la configuración.

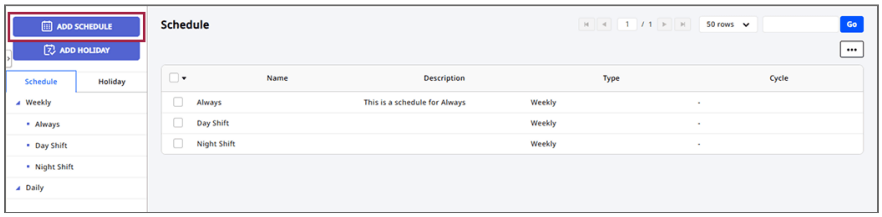
Una vez completada toda la configuración, haga clic en **Apply**.

Ajustes de Horario

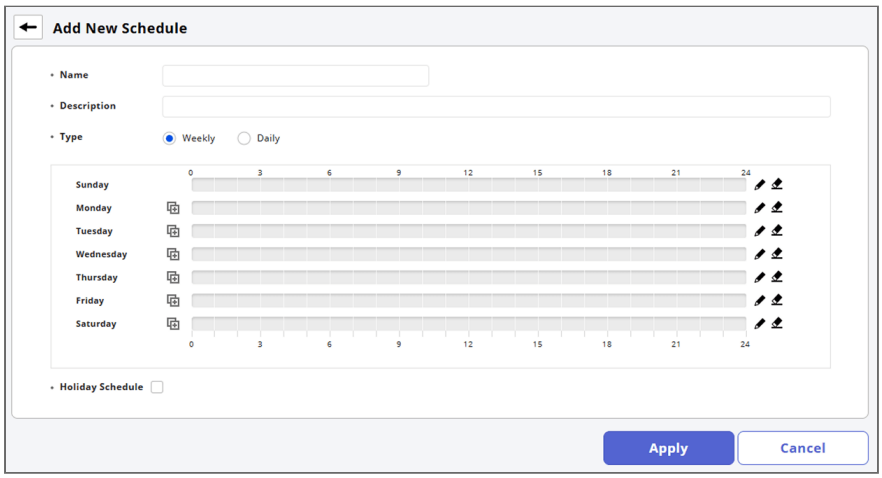
Esta guía describe cómo operar de manera eficiente el control de acceso y la gestión de asistencia configurando horarios de acceso y festivos. Los horarios son un factor importante que se puede aplicar al control de acceso, lo que permite gestionar los tiempos de acceso de los usuarios y los días festivos.

Registrar horario

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Schedule** en la barra lateral izquierda.
3. Haga clic en **ADD SCHEDULE** en la parte superior izquierda de la pantalla.



4. Introduzca o configure cada elemento en la pantalla **Add New Schedule**.

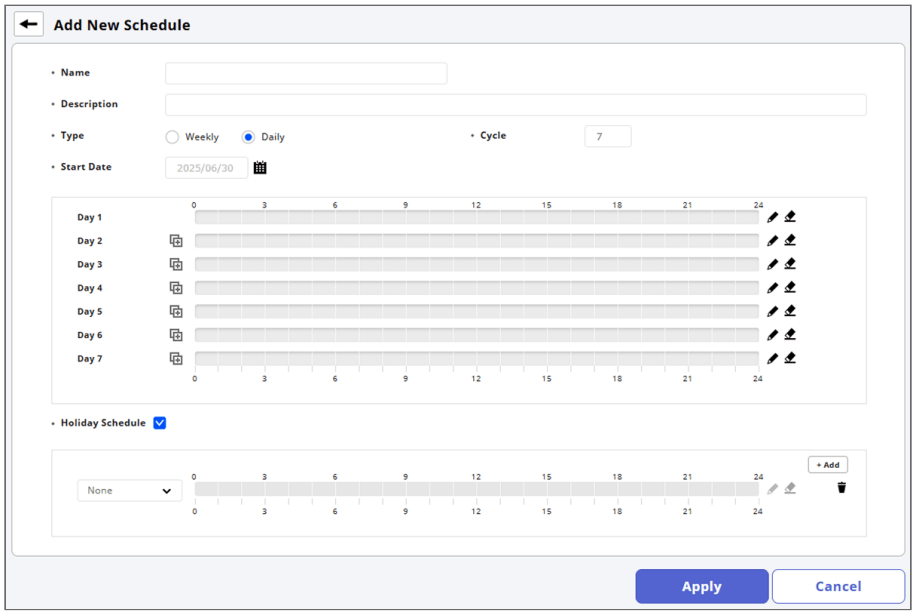


5. Cuando complete todos los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.

> **Información**
>
> Para obtener más información sobre los elementos individuales en la pantalla **Add New Schedule**, consulte Opciones para añadir un nuevo horario.

Opciones para añadir un nuevo horario

Guía de los elementos individuales que se pueden configurar en la pantalla **Add New Schedule**.

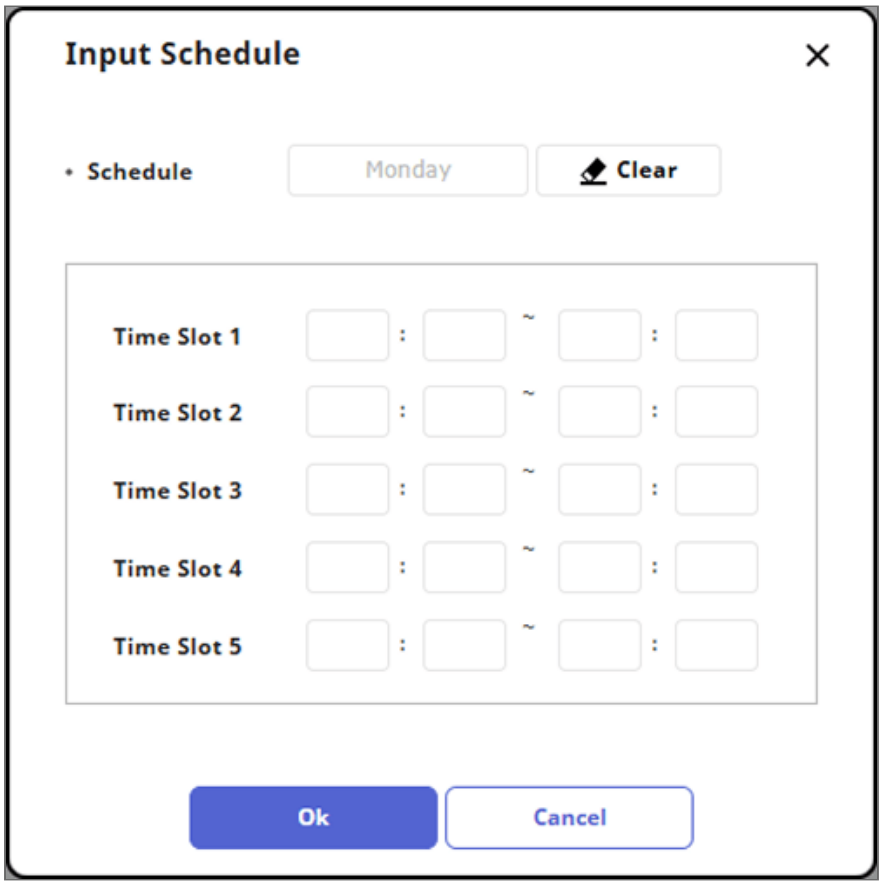


- **Name**: Introduzca el nombre del horario.
- **Description**: Introduzca una breve descripción del horario.

- **Type**: Elija un horario semanal o diario. Al seleccionar **Daily**, puede seleccionar **Cycle** y **Start Date**.



- Haga clic en **Time segment** en el área central para establecer la hora deseada. Cuando termine, haga clic en **Apply**.



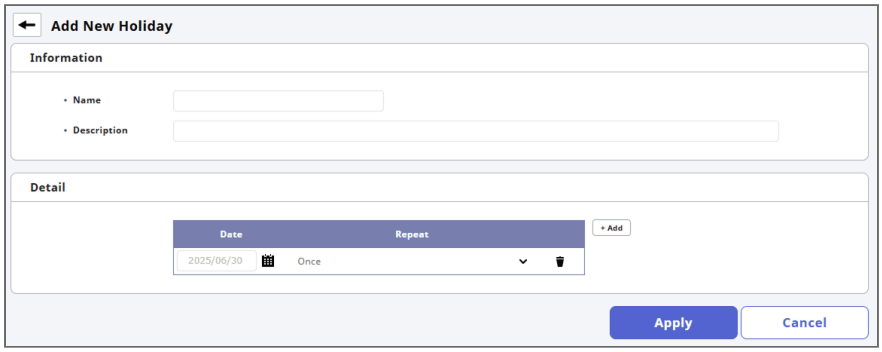
  - Puede configurar hasta cinco franjas horarias por día o por semana.
  - Prográmelas y haga clic en para copiar las franjas horarias establecidas arriba.
  - Haga clic en para modificar una franja horaria. Haga clic en para eliminar una franja horaria establecida.

- **Holiday Schedule**: Elija si desea aplicar horarios de festivos. Al seleccionar un elemento, se habilitan los ajustes detallados.
  - Seleccione la casilla **None** para elegir los festivos preestablecidos. Para añadir más festivos, haga clic en **+ Add** y establezca los festivos.
  - **Franjas horarias de festivos**: Haga clic en las franjas horarias para establecer las que se aplicarán en los festivos.

> **Información**
>
> - Haga clic en para modificar una franja horaria. Haga clic en para eliminar una franja horaria establecida.
> - Haga clic en para eliminar los festivos añadidos.
> - Para obtener más información sobre cómo agregar un horario de días festivos, consulte Añadir horario de festivos.

Añadir horario de festivos

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Schedule** en la barra lateral izquierda.
3. Haga clic en **ADD HOLIDAY** en la parte superior izquierda de la pantalla.
4. Introduzca **Name** y **Description** en la pantalla **Add New Holiday**.



5. Haga clic en **+ Add** en la sección **Detail**.
6. Haga clic en para seleccionar la fecha y establecer el número de repeticiones y la duración.
7. Haga clic en **Apply** para registrar el horario de festivos establecido.

> **Información**
>
> Haga clic en para eliminar un horario de festivos.

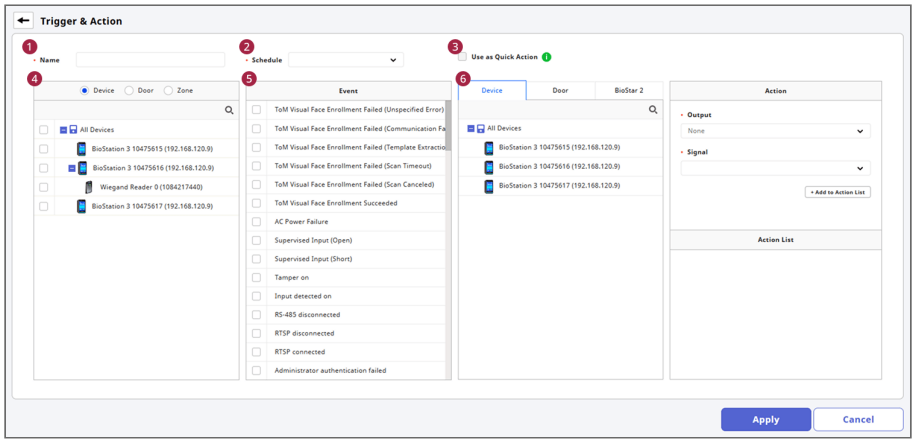
Configuración de Activadores y Acciones

Configure el dispositivo o **BioStar X** para realizar acciones deseadas cuando ocurran eventos específicos en un dispositivo, puerta o área.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Trigger & Action** en la barra lateral izquierda.
3. Haga clic en **Access Management** → **ADD TRIGGER & ACTION** en la esquina superior izquierda de la pantalla.



Siga las instrucciones en pantalla para configurar los detalles.



1 Ingrese el nombre

Name: Ingrese el nombre para las condiciones y las acciones.

2 Configurar horario

Schedule: Configure el horario en el que se aplicarán las condiciones y acciones.

> **Información**
>
> - Haga clic en **+ Add Schedule** para definir un horario si no existe uno adecuado al seleccionar **Input** y crear condiciones personalizadas.
> - Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

3 Usar como Acción Rápida

El ajuste **Quick Action** permite controlar varias puertas a la vez con **Quick Action** en la pantalla principal de **BioStar X**. Haga clic en la casilla **Use as Quick Action**.

> **Información**
>
> - Esta función solo está disponible cuando la opción **Schedule** se configura en **Always**.
> - Configura **Quick Action** en **Settings** → **Access Management** → **Quick Action**. Para obtener más información sobre **Quick Action**, consulte Cómo Usar la Acción Rápida.

4 Seleccionar dispositivo, puerta, control de acceso avanzado

Seleccione los elementos para enviar señales de eventos. Se pueden seleccionar varios dispositivos y funcionarán de forma independiente incluso si se pierde la conexión con **BioStar X**.

> **Información**
>
> Una licencia **Essential** o superior permite habilitar la opción **Advanced AC** como opción adicional. Para obtener más información sobre la política de licencias, consulte Política de Licencias.

5 Configurar condiciones de evento

Configure los eventos de condición. Debe seleccionar uno o más eventos.

> **Información**
>
> Según las opciones seleccionadas en el paso anterior, se activarán listas de eventos distintas.

6 Configurar acciones

Seleccione el dispositivo que realizará las acciones. Elija acciones para dispositivos, puertas o **BioStar X**.

En la sección **Action**, configure las señales que se enviarán cuando ocurran los eventos de condición seleccionados. Configure esto en **BioStar X** para recibir registros por correo electrónico.

> **Información**
>
> - Al hacer clic en **Device**, **Door**, o **BioStar X** se cambiará el contenido de la sección de acciones.
> - Para configurar la información del servidor de correo electrónico, haga clic en ⚙ en la pestaña **BioStar X**. Cuando aparezca la ventana **SMTP Option**, ingrese la información del servidor de correo electrónico y haga clic en **Apply**. Para obtener más información, consulte Configuración de Correo Electrónico.
> - Para información detallada sobre la configuración del servidor de correo electrónico, contacte a su administrador del sistema.

Cuando finalices la configuración, haz clic en **Apply**.

Cómo Usar la Acción Rápida

Acciones rápidas es una función que automatiza procedimientos de control complejos durante emergencias. Ejecuta al instante las acciones de varios dispositivos predefinidos con un solo botón para responder con rapidez.

Agregue un botón de acción rápida en el menú **Quick Action**. Haga clic en el botón en la pantalla principal de **BioStar X** para controlar varias puertas a la vez.

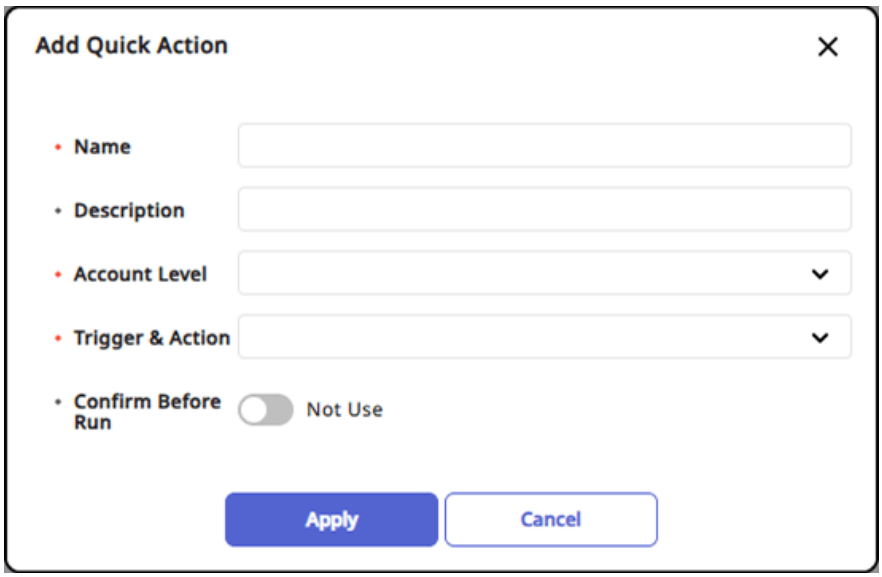
> **Información**
>
> Para agregar el **Quick Action** como acción rápida, consulte Configuración de Activadores y Acciones.

Agregar botón de Acción rápida

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Quick Action** en la barra lateral izquierda.



3. Haga clic en **+ Add** en la sección **Quick Action Layout**.
4. Cuando aparezca la ventana **Add Quick Action**, ingrese y configure cada elemento.



- **Account Level**: Seleccione el **Account Level** que puede ejecutar la Acción rápida que desea agregar. Es posible seleccionar varias opciones.
- **Trigger & Action**: Seleccione el **Trigger & Action** que se ejecutará. Es posible seleccionar varias opciones.
- **Confirm Before Run**: Si habilita esta opción, aparecerá una ventana de confirmación cuando presione el botón **Quick Action** para preguntar si desea ejecutarlo.

5. Haga clic en **Apply** para guardar la configuración.
6. Haz clic en **Apply** en la parte inferior derecha de la pantalla.

Se creará el botón **Quick Action** agregado en el área del encabezado superior derecho de la pantalla de **BioStar X**. Haga clic en el botón **Quick Action** creado para verificar que funcione según lo configurado en **Quick Action**.

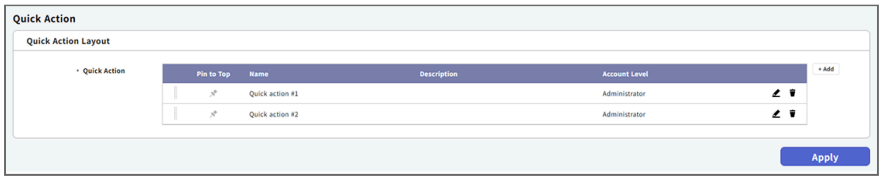


Información

- Es posible agregar hasta cuatro botones **Quick Action** en el área del encabezado superior de la pantalla. Permanece fijo para su uso en cualquier página.
- Los botones **Quick Action** disponibles pueden variar según los ajustes configurados para el usuario **Account Level**.

Editar botón de acción rápida

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Quick Action** en la barra lateral izquierda.
3. Haga clic en el botón a la derecha del botón de Acción rápida que desea modificar.



4. Cuando aparezca la ventana emergente de edición, modifique el elemento deseado y haga clic en **Apply**.
5. Para guardar las modificaciones, haga clic en **Apply** en la parte inferior derecha de la pantalla.

Cambiar el orden de las acciones rápidas

1. Haz clic en **Settings** en la página **Launcher**.
2. En la barra lateral izquierda, haga clic en **Access Management** → **Quick Action**.
3. En la lista de acciones rápidas, mantenga presionada la columna de más a la izquierda y arrástrela a la posición deseada.



4. Haga clic en **Apply** en la esquina inferior derecha de la pantalla para guardar el nuevo orden.

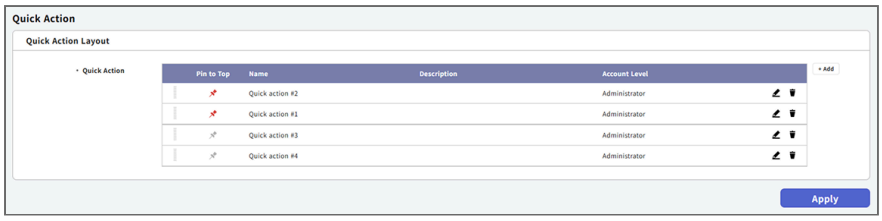
La lista de acciones rápidas en la esquina superior derecha de la pantalla muestra el orden actualizado.



Fijar botones en el encabezado

Coloque las acciones rápidas que requieren acceso rápido en el área del encabezado.

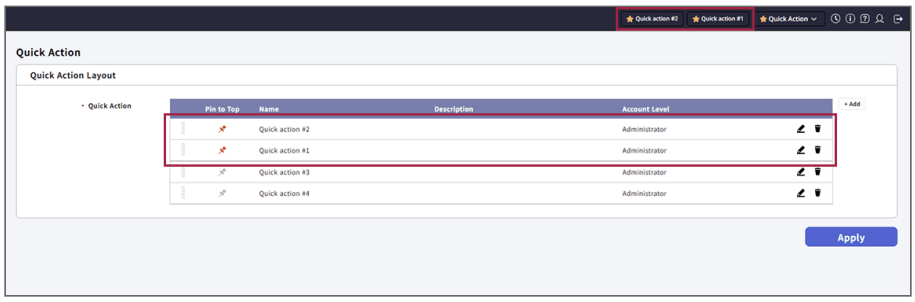
1. Haz clic en **Settings** en la página **Launcher**.
2. En la barra lateral izquierda, haga clic en **Access Management** → **Quick Action**.
3. Haga clic en **Pin to Top**( ) para fijar la acción rápida en el área del encabezado.



> Arrastre la columna de más a la izquierda para cambiar el orden. Haga clic en **Pin to Top** de nuevo para quitar la fijación.

4. Seleccione todas las acciones rápidas para fijarlas en el área del encabezado. Haga clic en **Apply** en la esquina inferior derecha.

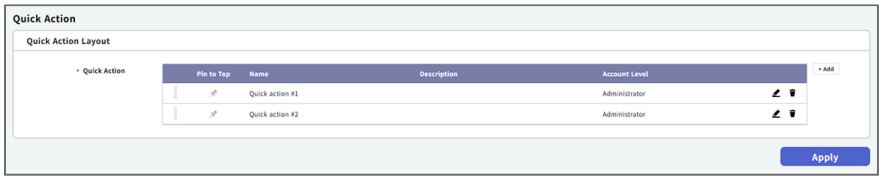
Las acciones rápidas fijadas aparecen a la izquierda del botón **Quick Action** en la esquina superior derecha de la pantalla.



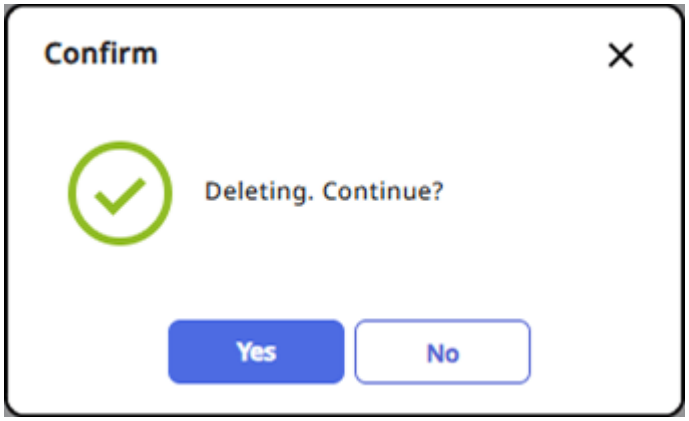
> **Información**
>
> - Fije hasta 4 acciones rápidas en el área del encabezado. Cuando ya hay 4 acciones rápidas fijadas, no es posible fijar más. Quite la fijación de otra entrada y vuelva a intentarlo.
> - Cuando la ventana del navegador se estrecha, desaparecen todos los botones individuales del encabezado.
>
> Busque las acciones rápidas fijadas con el icono de chincheta ( ) en la lista desplegable del botón **Quick Action**.
> - Si todas las acciones rápidas agregadas están fijadas en el área del encabezado, el botón **Quick Action** no aparece. Quite la fijación de ciertas entradas para que el botón vuelva a aparecer.

Eliminar el botón de acción rápida

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Access Management** → **Quick Action** en la barra lateral izquierda.
3. Haga clic en a la derecha del botón de acción rápida que desea eliminar.



4. En la ventana emergente de confirmación de eliminación, haga clic en **Yes**.



5. Para aplicar los cambios, haga clic en **Apply** en la parte inferior derecha de la pantalla.

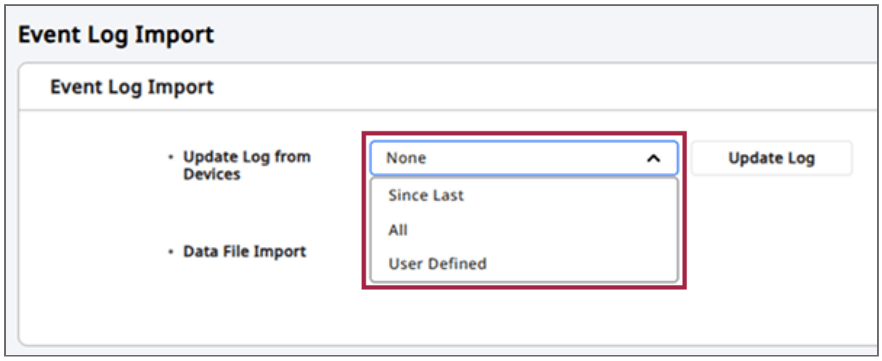
Importar Registros de Eventos

Importa los registros del dispositivo al servidor **BioStar X** para revisar eventos. Esta función está disponible cuando la opción **Log Upload** se establece en **Manual** en los ajustes de **Server**.

> **Información**
> Para obtener más información sobre la opción **Log Upload**, consulte Configuración Detallada del Servidor.

Importar manualmente

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Event** → **Event Log Import** en la barra lateral izquierda.
3. Selecciona el periodo para obtener registros en **Update Log from Devices**.



- **Since Last**: Importa los registros desde la fecha del último registro guardado en el servidor **BioStar X**.
- **All**: Importa todos los registros del dispositivo.

- **User Defined**: Selecciona las fechas de inicio y fin para importar registros.

4. Haz clic en **Update Log** para importar los registros.

Importar desde almacenamiento externo

Carga los registros de eventos almacenados en un dispositivo de almacenamiento externo (USB) en **BioStar X**.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Event** → **Event Log Import** en la barra lateral izquierda.
3. Haz clic en **Browse** para **Data File Import**.



4. Seleccione el archivo de datos (*.tgz*) guardado localmente.

Aparecerá un mensaje en la pantalla si el archivo de datos se importa correctamente.

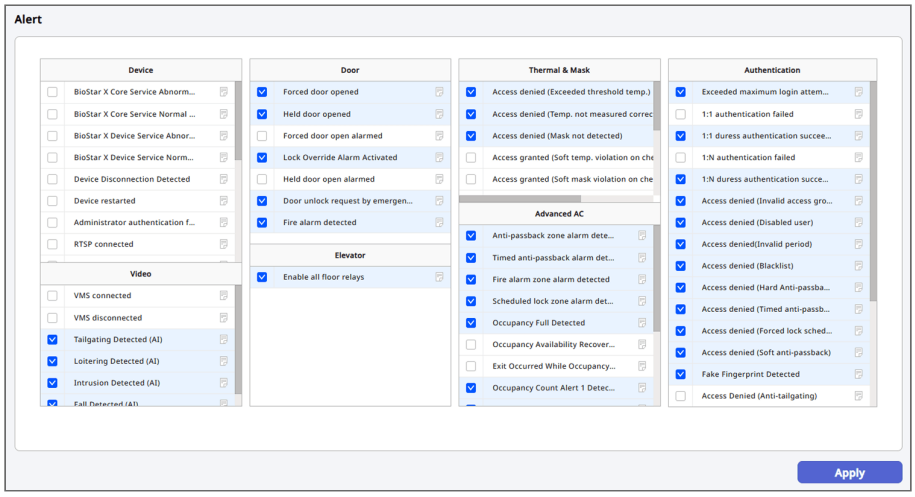
> **Información**
>
> - Los datos exportados desde dispositivos con una versión de firmware desactualizada no se pueden importar en **BioStar X**. Utiliza siempre la versión más reciente del firmware.
> - Solo se pueden importar archivos de datos exportados por los siguientes modelos: BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceLite, FaceStation 2, BioStation A2 y BioStation 2.
> - Si los registros de eventos importados no provienen de puntos de acceso, ascensores o zonas configuradas en el sistema **BioStar X**, cierta información puede aparecer en blanco.

Configuración de Alertas

Establece los tipos de alerta y los mensajes que aparecerán en la pantalla cuando ocurran eventos en el dispositivo, la puerta o el área. Además, configura la reproducción de un archivo de sonido cargado por el usuario cuando se produzca la alerta.

Configuración de Alertas

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Event** → **Alert** en la barra lateral izquierda de la pantalla.
3. Selecciona el evento que se mostrará en la pantalla desde la lista de eventos de cada categoría.
4. Cuando finalices la configuración, haz clic en **Apply**.



Editar mensaje de alerta

Haz clic en en la lista de eventos para editar el mensaje de alerta. Cuando aparezca la ventana **Alert Message**, ajusta cada elemento y haz clic en **Apply**.



- **Name**: Cambia el nombre del mensaje de alerta.
- **Message**: Ingresa el mensaje que aparecerá en la pantalla.
- **Sound Name**: Si cargaste un archivo de sonido para reproducir en el evento, selecciónalo de la lista.
- **Play Options**: Si seleccionaste un archivo de sonido, elige cuántas veces se reproducirá.

> **Información**
> Si no tienes un archivo de sonido para reproducir, consulta Configurar Preferencias para ver cómo subirlo.

Administrar Credenciales

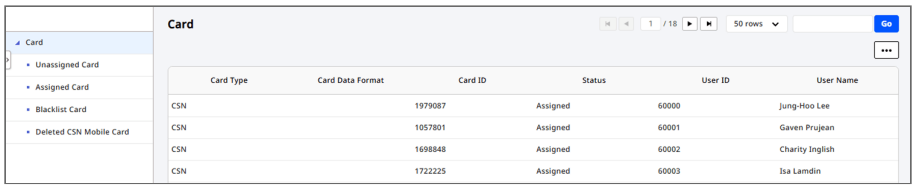
Esta guía describe cómo administrar credenciales para la autenticación de acceso. Verifique el estado de emisión de tarjetas, los titulares de tarjetas y la lista negra, y configure formatos Wiegand y de tarjetas inteligentes. Esta guía también cubre la impresión de tarjetas con cardPresso, la gestión de tarjetas de acceso móvil con Airfob Portal (Airfob Portal) y la configuración de coincidencia de grupos de IR Face.

Administrar Tarjetas

Puede verificar el estado de emisión de la tarjeta, cambiar el formato de datos de tarjetas Wiegand y gestionar el historial de eliminación de tarjetas móviles CSN.

Gestión de tarjetas

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Credential** → **Card** en la barra lateral izquierda.
3. Puede ver las tarjetas registradas en la pantalla de lista de tarjetas.



Haga clic en el estado de emisión en el lado izquierdo de la pantalla para filtrar por estado de emisión de la tarjeta. Los estados de emisión de tarjetas son los siguientes:

- **Unassigned Card**: Tarjeta que no está asignada a ningún usuario.
- **Assigned Card**: Tarjeta asignada a un usuario específico. Puede verificar el ID y el nombre del usuario asignado en la lista de tarjetas.
- **Blacklist Card**: Tarjeta registrada en la lista negra. El titular de la tarjeta no puede autenticarse para acceder.
- **Deleted CSN Mobile Card**: Tarjeta de acceso móvil eliminada.

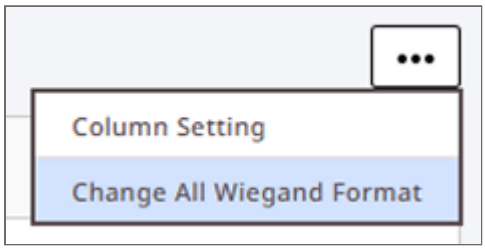
> **Información**
>
> Si ha bloqueado la tarjeta de un usuario, puede consultar la información de la tarjeta en la lista **Blacklist Card**. Para desbloquear, seleccione la tarjeta deseada y haga clic en **Unblocked**.

Cambiar formato de datos de tarjeta Wiegand

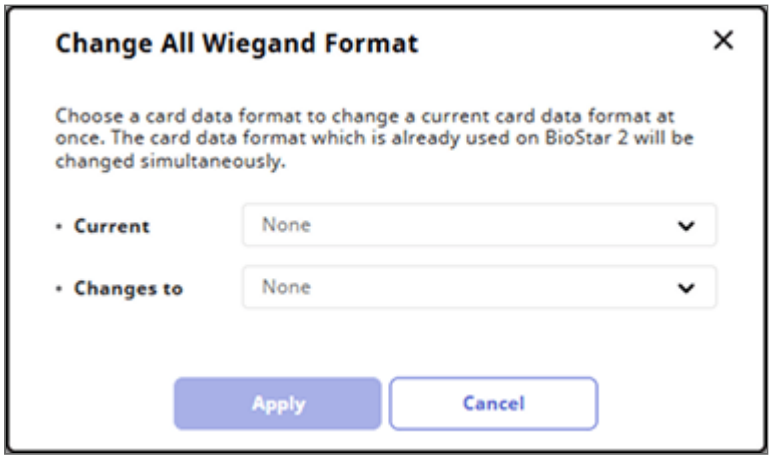
Cambie el formato de datos de tarjeta Wiegand en uso de forma simultánea.

> **Precaución**
>
> El cambio de formato de datos de las tarjetas ya asignadas a usuarios también se realizará, así que tenga precaución.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Credential** → **Card** en la barra lateral izquierda.
3. Haga clic en ••• en la parte superior derecha de la lista de tarjetas y seleccione **Change All Wiegand Format**.



4. Cuando aparezca la ventana **Change All Wiegand Format**, seleccione el formato de datos de tarjeta que desea cambiar en la lista **Current**.



5. Seleccione el formato de datos de tarjeta deseado en la lista **Changes to**.
6. Haga clic en **Apply** para cambiar el formato de datos de tarjeta.

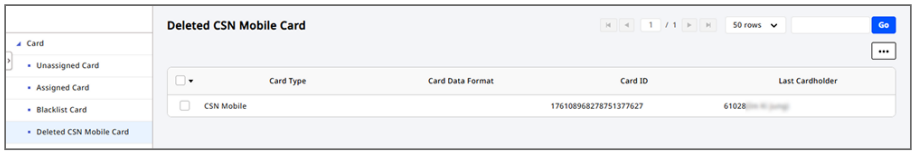
Pautas para la gestión de eliminación de tarjetas móviles CSN

Al usar tarjetas móviles CSN integradas con el sitio regular de Airfob Portal en **BioStar X**, si un usuario elimina una tarjeta, el mismo ID de tarjeta podría volver a emitirse a otro usuario. Sin embargo, esto podría ocasionar que el titular original de la tarjeta aún pueda acceder a las instalaciones incluso después de que la tarjeta haya sido reemitida.

Para solucionar este problema, **BioStar X** ofrece la función de gestionar el historial de eliminación después de eliminar tarjetas móviles CSN.

Gestión separada de tarjetas móviles CSN eliminadas

El sistema registra las tarjetas móviles CSN eliminadas en la lista **Deleted CSN Mobile Card** en **Settings** → **Credential** → **Card**. En esta lista, puede ver **Card Type**, **Card Data Format**, **Card ID**, y **Last Cardholder**.

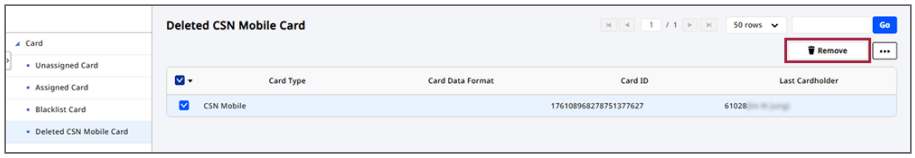


Evitar la reemisión de IDs de tarjetas eliminadas

Si existe un historial de eliminación de una tarjeta móvil CSN, el sistema impedirá que ese ID de tarjeta sea reemitido a otro

usuario.

Si desea emitir una tarjeta con un ID de tarjeta eliminado, solo podrá hacerlo después de excluir la tarjeta móvil CSN correspondiente de la lista **Deleted CSN Mobile Card**.



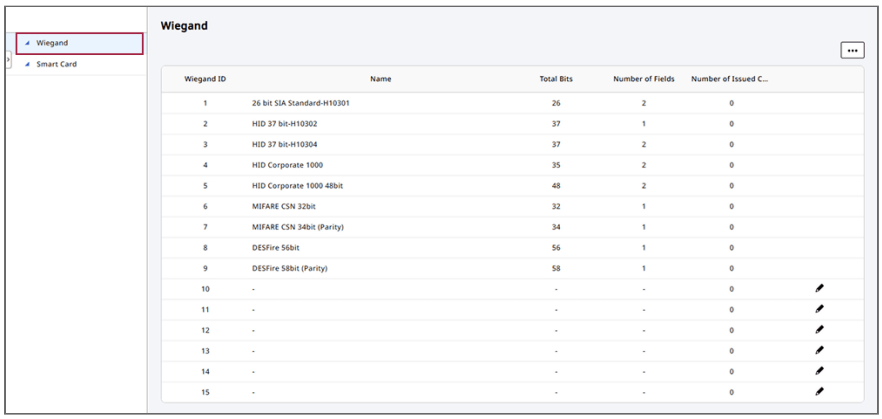
> **Información**
>
> Las tarjetas móviles CSN incluidas en la lista **Deleted CSN Mobile Card** no pueden eliminarse desde la lista **Unassigned Card**.
>
> Para eliminar una tarjeta de la lista **Unassigned Card**, primero retire la tarjeta de la lista **Deleted CSN Mobile Card** y luego proceda con la eliminación.

Configurar Formato de Tarjeta Wiegand

Configure el formato de lectura de datos de la tarjeta. Los datos de la tarjeta se procesan según el formato Wiegand configurado.

Configurar formato de tarjeta Wiegand

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Credential** → **Card Format** en la barra lateral izquierda.
3. Haga clic en **Wiegand** en la lista de formatos de tarjeta de la izquierda.



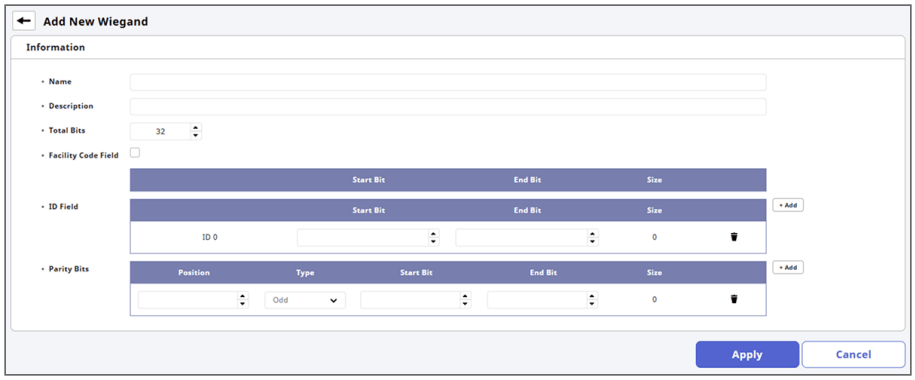
4. Haga clic en el botón ✎ del elemento sin nombre en la lista de formatos Wiegand.
5. Cuando aparezca la pantalla **Add New Wiegand**, configure cada elemento. Para obtener más información, consulte Guía de opciones de ajuste.
6. Haga clic en **Apply** para agregar el formato Wiegand configurado.

Información

- Se pueden usar hasta 15 formatos Wiegand.
- Los formatos predefinidos no se pueden modificar ni eliminar.

Guía de opciones de ajuste

Consulte los siguientes elementos para establecer la configuración de bits al agregar o editar un formato de tarjeta Wiegand.



- **Name**: Ingrese el nombre del formato Wiegand.
- **Description**: Ingrese una descripción breve del formato Wiegand.
- **Total Bits**: Ingrese el número total de bits.
- **Facility Code Field**: Establezca si se usará el código de identificación. Para usar el código de identificación, marque la casilla y escriba **Start Bit** y **End Bit**.
- **ID Field**: Ingrese **Start Bit** y **End Bit** para la ID que desea usar. Haga clic en **+ Add** para agregar un campo de ID.
- **Parity Bits**: Haga clic en **+ Add** para ingresar el número de bits de paridad. Ingrese la posición de los bits de paridad y los bits inicial y final.

Información

Para agregar bits de paridad, se debe ingresar la opción **Total Bits**.

Configurar Formato de Tarjeta Inteligente

Configura el diseño de tarjetas inteligentes como MIFARE, iCLASS, DESFire e iCLASS Seos.

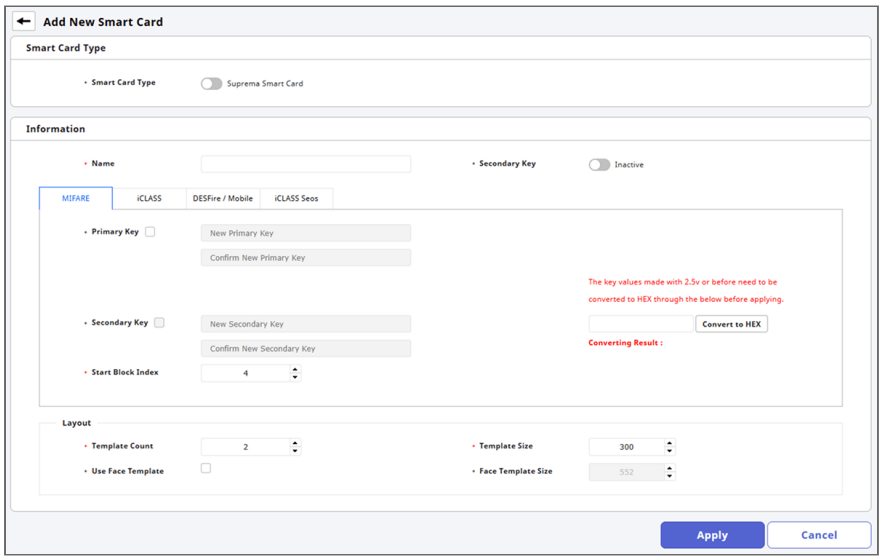
Agregar tarjeta inteligente

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Credential** → **Card Format** en la barra lateral izquierda.
3. Haz clic en **Smart Card** en la lista de formatos de tarjeta de la izquierda.



4. Haz clic en **Add Smart Card** en la parte superior izquierda de la pantalla.

5. Cuando aparezca la pantalla **Add New Smart Card**, configura cada elemento. Para obtener más información, consulta Tipos de tarjeta inteligente.

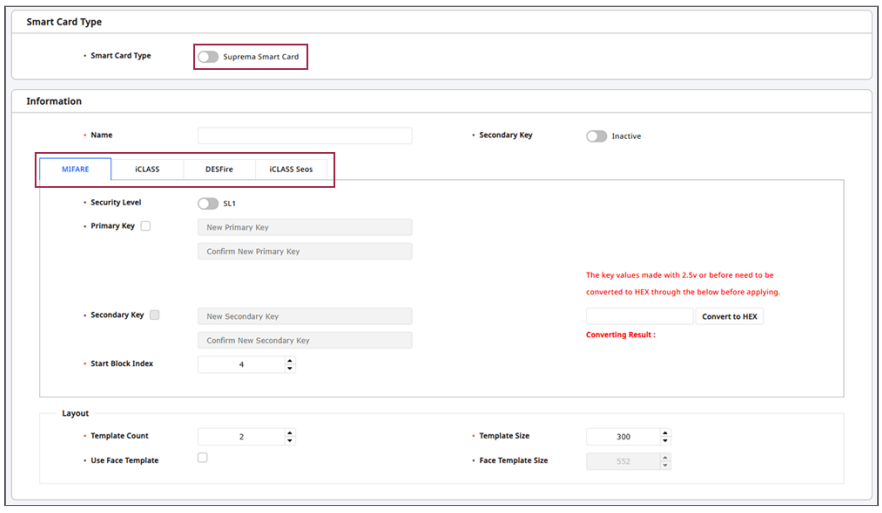


6. Una vez que completes todos los ajustes, haz clic en **Apply**.

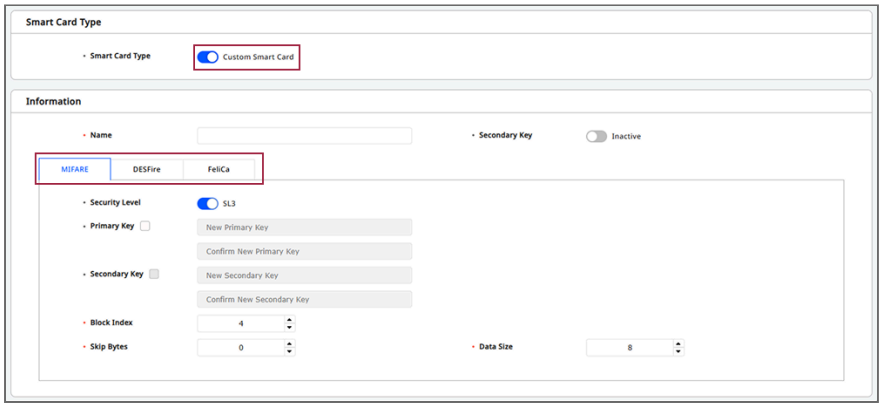
Tipos de tarjeta inteligente

Define el tipo de tarjeta inteligente deseado en la opción **Smart Card Type**.

- **Suprema Smart Card**



- **Custom Smart Card**

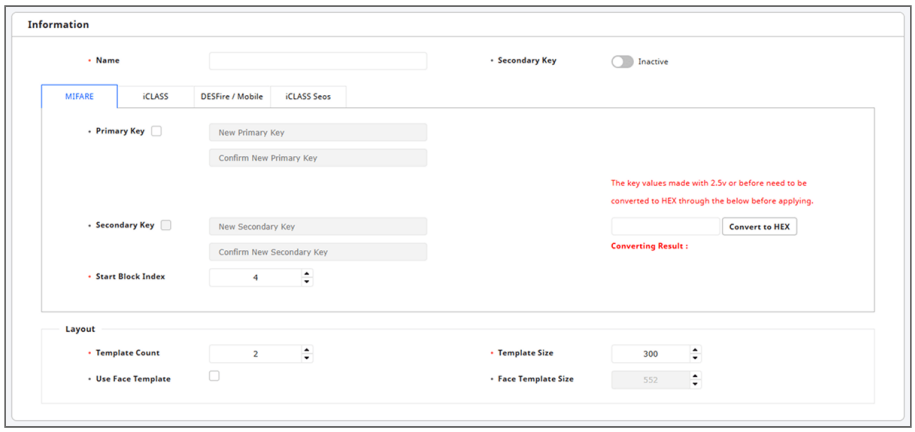


Información

- Las tarjetas inteligentes personalizadas solo admiten MIFARE, DESFire y FeliCa.
- FeliCa solo se admite en el firmware BioStation 3 versión 1.3.0 o superior.

Guía de opciones de ajuste

Configura el diseño de la tarjeta en la sección **Info**.

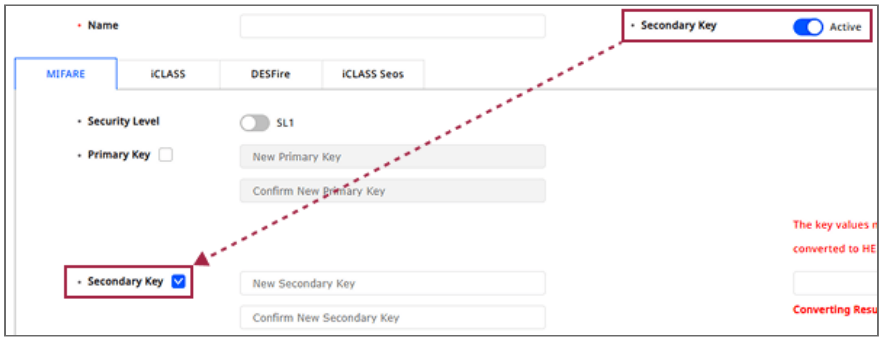


Información

- Los campos **Primary Key** y **Secondary Key** admiten solo hexadecimal. Ingresa los valores de la clave en el campo derecho y haz clic en **Convert to HEX**. Usa el valor convertido como clave del sitio.
- **Convert to HEX** está disponible solo cuando la opción **Smart Card Type** es **Suprema Smart Card**.

Configurar información básica

- **Name**: Ingresa el nombre de la tarjeta inteligente.
- **Secondary Key**: Configura si se usará una clave secundaria del sitio. Establécelo en **Active** para habilitar la configuración de la clave secundaria del sitio. Cuando se configura una clave secundaria del sitio, se utilizará para la autenticación cuando la clave primaria de la tarjeta no coincida.



Configurar tarjeta inteligente

Configura la estructura de la tarjeta inteligente.

Tarjeta inteligente Suprema

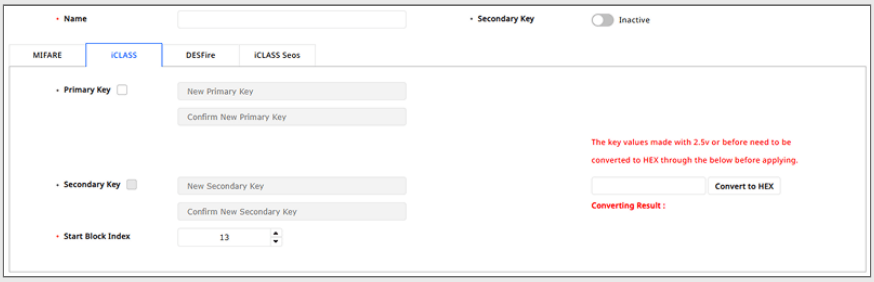
Los campos **Primary Key** y **Secondary Key** admiten solo hexadecimal. Ingresa el valor de la clave en cada campo y haz clic en **Convert to HEX**. Usa el valor convertido como clave del sitio.

▼ **MIFARE**



- **Security Level**: Configure el tipo de cifrado en **SL1** o **SL3**.
- **Primary Key**: Clave que cifra las comunicaciones entre la tarjeta inteligente y el lector de tarjetas.
- **Secondary Key**: Se usa para la autenticación cuando la clave de sitio primaria de la tarjeta no coincide. La clave de sitio secundaria solo se puede ingresar después de activar la opción **Secondary Key** en la parte superior de la sección.
- **Start Block Index**: Seleccione el bloque inicial donde se guardará cada plantilla. Este bloque es el índice del bloque donde se almacena la información del usuario; configúrelo en un bloque almacenable si el usuario ya usa la tarjeta inteligente.

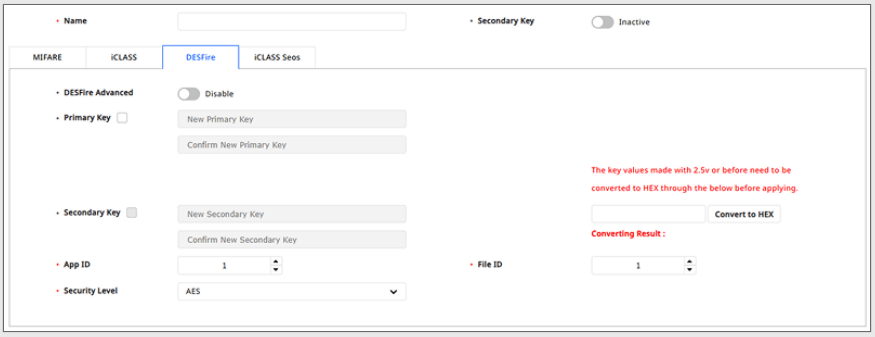
▼ **iCLASS**



- **Primary Key**: Clave que cifra las comunicaciones entre la tarjeta inteligente y el lector de tarjetas.
- **Secondary Key**: Se usa para la autenticación cuando la clave de sitio primaria de la tarjeta no coincide. La clave de sitio secundaria solo se puede ingresar después de activar la opción **Secondary Key** en la parte superior de la sección.

- **Start Block Index**: Seleccione el bloque inicial donde se guardará cada plantilla. Este bloque es el índice del bloque donde se almacena la información del usuario; configúrelo en un bloque almacenable si el usuario ya usa la tarjeta inteligente.

▼ **DESFire**



- **DESFire Advanced**: Utilice tarjetas DESFire emitidas por terceros. Solo se puede configurar DESFire.
- **Primary Key**: Clave que cifra las comunicaciones entre la tarjeta inteligente y el lector de tarjetas.
- **Secondary Key**: Se usa para la autenticación cuando la clave de sitio primaria de la tarjeta no coincide. La clave de sitio secundaria solo se puede ingresar después de activar la opción **Secondary Key** en la parte superior de la sección.
- **ID Field**: Configure para leer un área específica de la tarjeta. Funciona como un directorio que contiene **File ID**.
- **File ID**: Configure el ID de archivo.
- **Security Level**: Configure el tipo de cifrado en **DES/3DES** o **AES**.

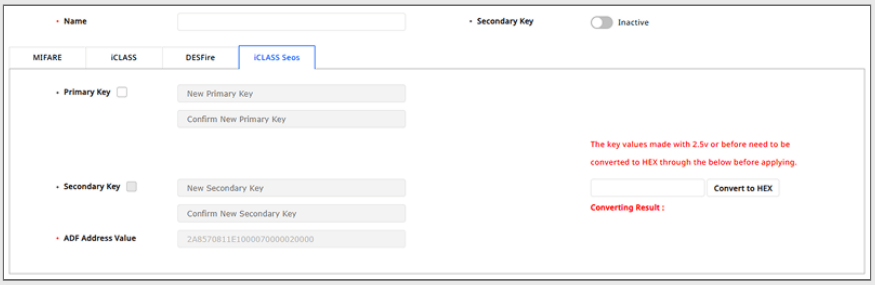
Información

Al cambiar un diseño de tarjeta guardado con cifrado **AES** a **DES/3DES**, aparece esta advertencia.

> ***Changing the Encryption Type to DES/3DES makes Enforce EV2/EV3 Secure Messaging unavailable on devices that use this card layout.***

Haz clic en el botón **Ok** para guardar los cambios. El sistema desactiva automáticamente la opción **Enforce EV2/EV3 Secure Messaging** en los dispositivos que usan este diseño de tarjeta. Para más información sobre la opción **Enforce EV2/EV3 Secure Messaging**, consulta Configuración de Autenticación.

▼ **iClass Seos**



- **Primary Key**: Clave que cifra las comunicaciones entre la tarjeta inteligente y el lector de tarjetas.
- **Secondary Key**: Se usa para la autenticación cuando la clave de sitio primaria de la tarjeta no coincide. La clave de sitio secundaria solo se puede ingresar después de activar la opción **Secondary Key** en la parte superior de la sección.

- **ADF Address Value**: Dirección ADF donde se almacenan las credenciales digitales.

Diseño

Modifica el diseño que registra la información del usuario, facial y de huellas digitales.

- **Template Count**: Establece el número de plantillas de huellas digitales que se incluirán en el diseño.
- **Template Size**: Define la cantidad de bytes que usa cada plantilla de huellas digitales.
- **Use Face Template**: Elige si se usará la plantilla facial.
- **Face Template Size**: Establece la cantidad de bytes que usa la plantilla facial.

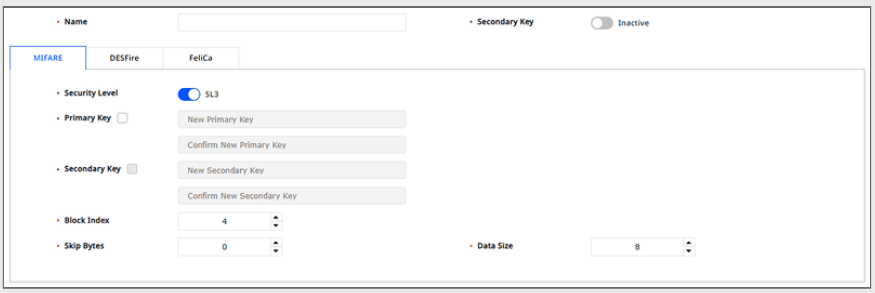
> **Información**
> **Use Face Template** está disponible en los modelos BioStation 3 Max, BioEntry W3, BioStation 3 y FaceStation F2.

Tarjeta inteligente personalizada

Las tarjetas inteligentes personalizadas solo admiten MIFARE, DESFire y FeliCa.

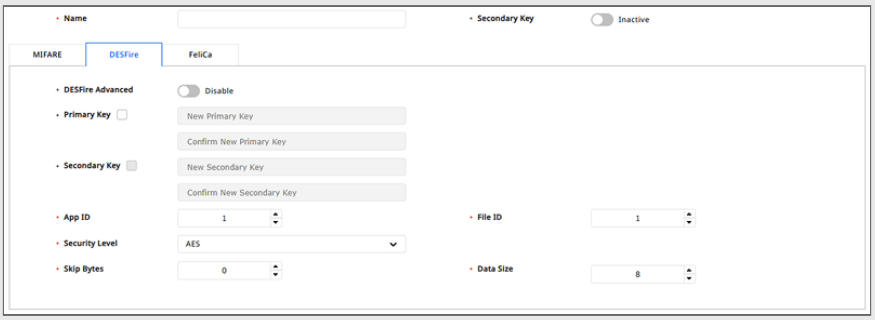
> **Información**
> FeliCa solo se admite en el firmware BioStation 3 versión 1.3.0 o superior.

▼ MIFARE



- **Security Level**: Configure el tipo de cifrado en **SL1** o **SL3**.
- **Primary Key**: Clave que cifra las comunicaciones entre la tarjeta inteligente y el lector de tarjetas.
- **Secondary Key**: Se usa para la autenticación cuando la clave de sitio primaria de la tarjeta no coincide. La clave de sitio secundaria solo se puede ingresar después de activar la opción **Secondary Key** en la parte superior de la sección.
- **Block Index**: Seleccione el bloque inicial donde se guardará cada plantilla. Este bloque es el índice del bloque donde se almacena la información del usuario; configúrelo en un bloque almacenable si el usuario ya usa la tarjeta inteligente.
- **Skip Bytes**: Configure el punto de inicio para leer el número de tarjeta.
- **Data Size**: (Cuando los valores configurados de **Primary Key** y **Secondary Key** coinciden con la configuración de la tarjeta) Configure el tamaño de los datos de la tarjeta que se leerán.

▼ DesFire



- **DESFire Advanced**: Utilice tarjetas DESFire emitidas por terceros. Solo se puede configurar DESFire.
- **Primary Key**: Clave que cifra las comunicaciones entre la tarjeta inteligente y el lector de tarjetas.
- **Secondary Key**: Se usa para la autenticación cuando la clave de sitio primaria de la tarjeta no coincide. La clave de sitio secundaria solo se puede ingresar después de activar la opción **Secondary Key** en la parte superior de la sección.
- **ID Field**: Configure para leer un área específica de la tarjeta. Funciona como un directorio que contiene **File ID**.
- **File ID**: Configure el ID de archivo.
- **Security Level**: Configure el tipo de cifrado en **DES/3DES** o **AES**.

Información

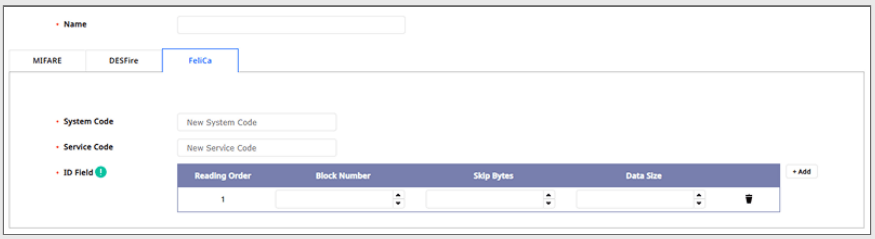
Al cambiar un diseño de tarjeta guardado con cifrado **AES** a **DES/3DES**, aparece esta advertencia.

> ***Changing the Encryption Type to DES/3DES makes Enforce EV2/EV3 Secure Messaging unavailable on devices that use this card layout.***

Haz clic en el botón **Ok** para guardar los cambios. El sistema desactiva automáticamente la opción **Enforce EV2/EV3 Secure Messaging** en los dispositivos que usan este diseño de tarjeta. Para más información sobre la opción **Enforce EV2/EV3 Secure Messaging**, consulta Configuración de Autenticación.

- **Skip Bytes**: Configure el punto de inicio para leer el número de tarjeta.
- **Data Size**: (Cuando los valores configurados de **Primary Key** y **Secondary Key** coinciden con la configuración de la tarjeta) Configure el tamaño de los datos de la tarjeta que se leerán.

▼ Felica



- **System Code**: Ingrese el código de sistema para leer tarjetas FeliCa en hexadecimal, con un máximo de 4 caracteres.
- **Service Code**: Ingrese el código de servicio para leer tarjetas FeliCa en hexadecimal, con un máximo de 4 caracteres.
- **ID Field**: Configure para leer un área determinada de la tarjeta. Configure hasta 8 bloques para lectura haciendo clic en **+ Add**.

  Block Number: Configure el bloque que se leerá de la tarjeta. (0-150)

Impresora de Tarjetas

Imprima tarjetas con el diseño deseado integrando **BioStar X** y cardPresso. cardPresso es un software profesional para el diseño e impresión de tarjetas. Con cardPresso cree diversas plantillas de tarjetas y organice la información del usuario en consecuencia.

Antes de comenzar

Instale el programa cardPresso y conéctelo a **BioStar X** para usar la función de impresora de tarjetas de **BioStar X**. Se requiere una licencia de la edición XXL de cardPresso para utilizar la función de servidor de impresión web del programa.

Información

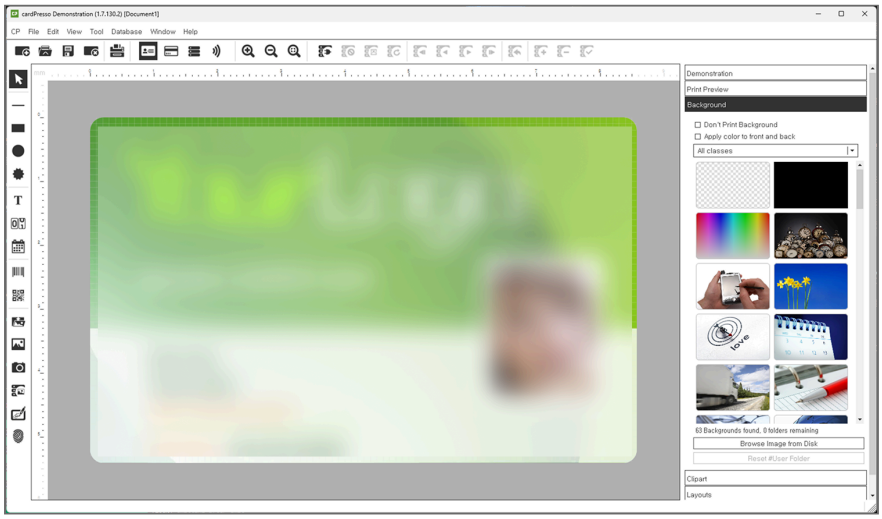
- Para obtener más información sobre los tipos de licencias del programa cardPresso, consulte el siguiente enlace.
- La función de servidor de impresión web solo es compatible con sistemas operativos Windows.

Instalar y configurar cardPresso

Siga los pasos siguientes para instalar el programa cardPresso y configurar el servidor de impresión web.

La ruta del menú o la pantalla pueden variar según la versión de instalación.

1. Descargue la última versión de cardPresso compatible con el sistema operativo del PC que operará como servidor de impresión web desde cardPresso Download.
2. Instale el programa y active la licencia emitida por cardPresso.
3. Después de ejecutar cardPresso, cree una plantilla de tarjeta.

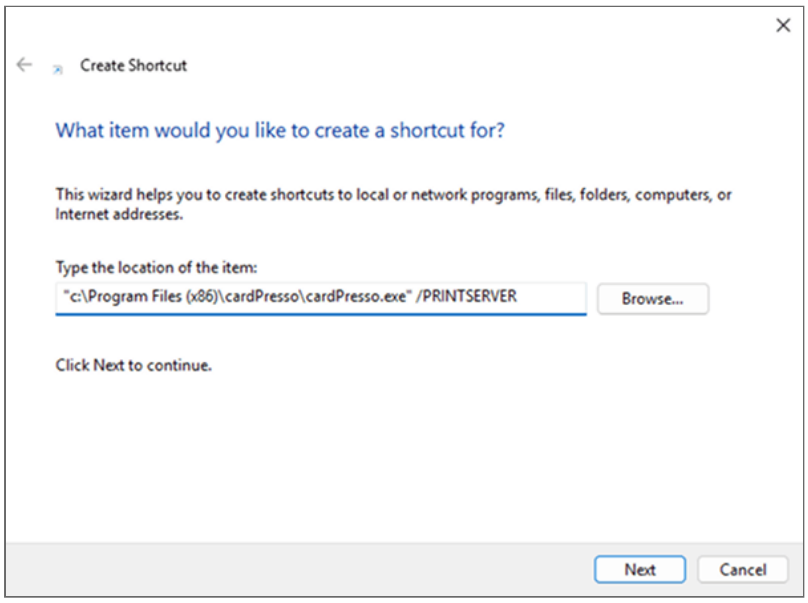


La imagen anterior es una pantalla de ejemplo y puede diferir de la pantalla real.

4. Guarde la plantilla de tarjeta creada en la ubicación deseada en el servidor donde está instalado **BioStar X**. *C:\template\example.card*)
5. Haga clic con el botón derecho en el escritorio del PC donde está instalado cardPresso y luego seleccione **New** → **Shortcut** en el menú emergente.

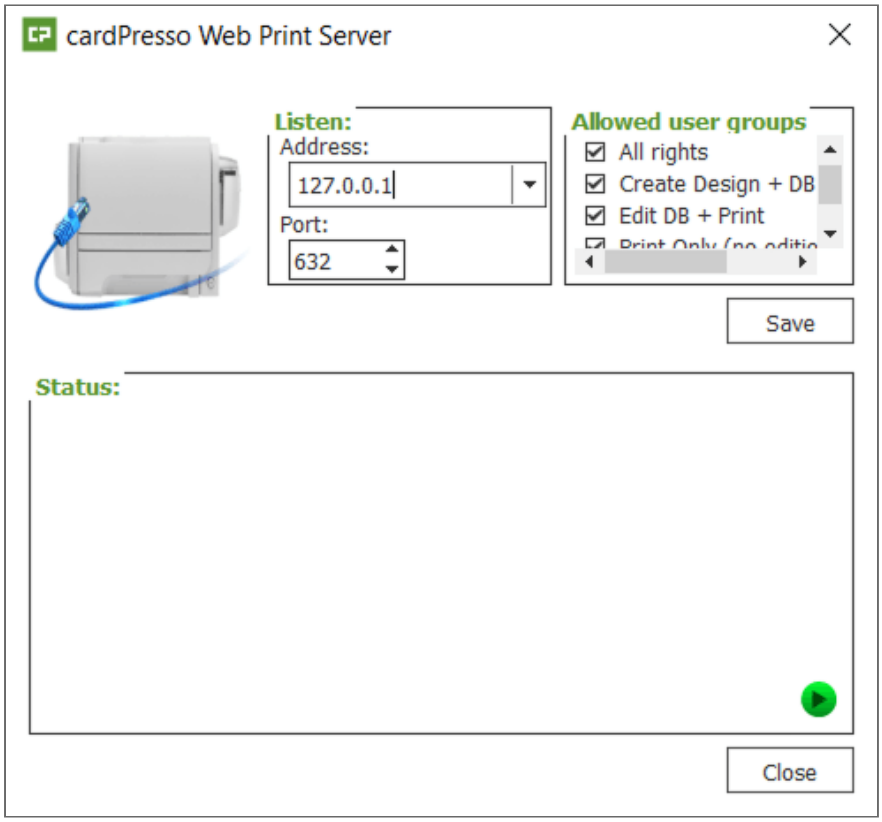
6. Introduzca lo siguiente en el campo **Ubicación del elemento** y luego haga clic en el botón **Siguiente**.

```
"C:\Program Files (x86)\cardPresso\cardPresso.exe" /PRINTSERVER
```



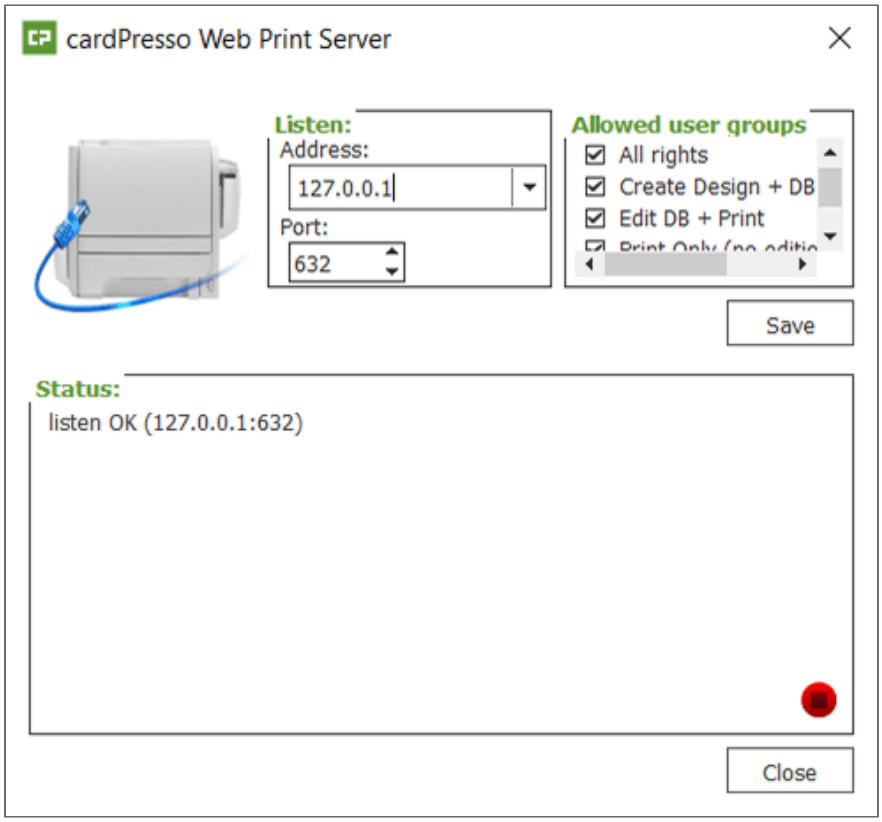
> La ruta donde está instalado cardPresso puede variar según el entorno de instalación. Después de confirmar la ruta donde está instalado cardPresso, modifíquela según corresponda conforme a la ruta anterior.

7. Introduzca un nombre para el acceso directo y haga clic en el botón **Finalizar**.
8. Haga doble clic en el icono de acceso directo del servidor de impresión web de cardPresso creado en el escritorio para ejecutarlo.
9. Cuando aparezca la ventana del servidor de impresión web de cardPresso, haga clic en el icono **Configuración**.



- **Dirección**: Introduzca la dirección IP del equipo que actúa como servidor de impresión web.
- **Puerto**: Número de puerto en el que cardPresso recibe las operaciones de impresión.
- **Grupos de usuarios permitidos**: Seleccione un grupo de usuarios que tenga acceso al servidor de impresión web.

10. Haga clic en **Guardar** cuando finalice la configuración.
11. Haga clic en en la esquina inferior derecha para iniciar el servicio. Si la configuración es correcta, el icono cambia a y aparece el mensaje **listen OK**.

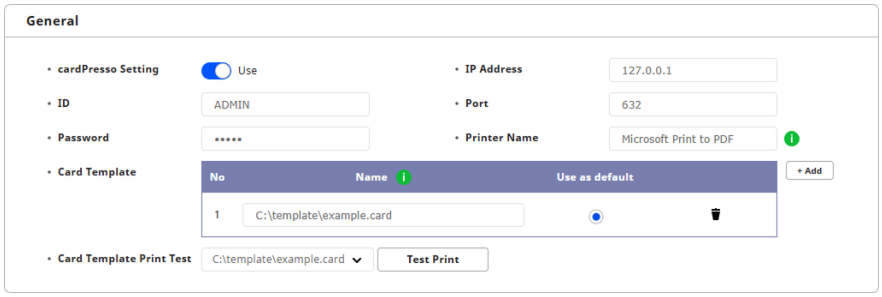


No cierre la ventana hasta que la impresión de tarjetas se haya completado.

Conectar cardPresso con BioStar X

Configure cardPresso como se muestra a continuación para conectarlo a **BioStar X**.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Credential** → **Card Printer** en la barra lateral izquierda.
3. Active **cardPresso Setting** en **Use** y luego complete cada elemento.



- **ID**: Introduzca su ID de inicio de sesión de cardPresso. (predeterminado: ADMIN)
- **Password**: Introduzca su contraseña de inicio de sesión de cardPresso. (predeterminado: admin)
- **IP Address**: Introduzca la dirección IP del PC que ejecuta el servidor de impresión web de cardPresso.
- **Port**: Introduzca el número de puerto que cardPresso utiliza para recibir operaciones de impresión.
- **Printer Name**: Introduzca el nombre de la impresora que se utilizará como impresora de tarjetas. Se encuentra en

el **Panel de control** de Windows → **Dispositivos e impresoras**.

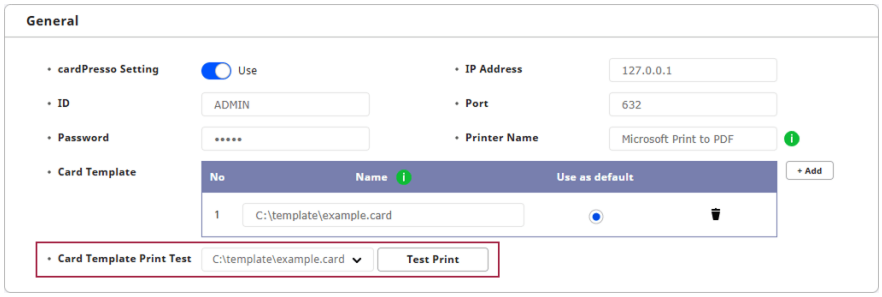
- **Card Template**: Haga clic en **+ Add** para añadir un **Card Template**. En el elemento **Name**, introduzca la ruta completa, incluido el nombre de archivo y la extensión de la plantilla de tarjeta.
  - El nombre de archivo de la plantilla de tarjeta puede contener caracteres alfanuméricos y especiales.
  - Se admiten hasta 20 plantillas de tarjetas.
  - Ruta de ejemplo: C:\template\example.card
- **Card Template Print Test**: Imprima de prueba la plantilla de tarjeta.

4. Una vez que complete la configuración, haga clic en **Apply**.

Imprimir de prueba la plantilla de tarjeta

Imprima de prueba una plantilla de tarjeta con información del administrador.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Credential** → **Card Printer** en la barra lateral izquierda.
3. Seleccione la plantilla de tarjeta que desea imprimir y luego haga clic en el botón **Test Print**.

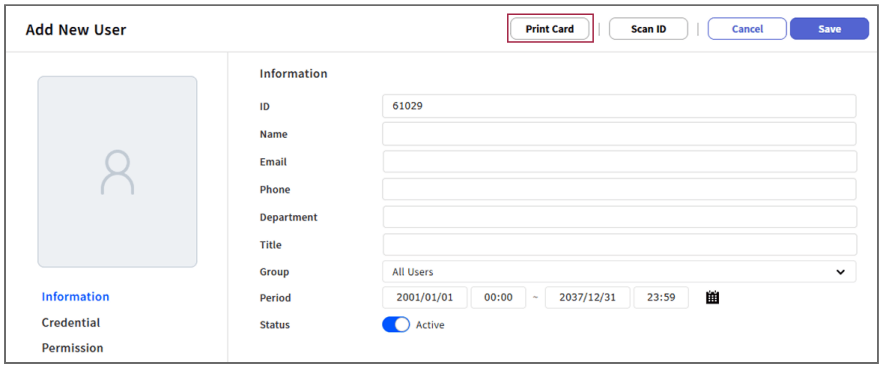


4. Se imprime la plantilla de tarjeta con información del administrador.

Imprimir plantillas de tarjetas por usuario

Imprima tarjetas con plantillas de tarjetas por usuario.

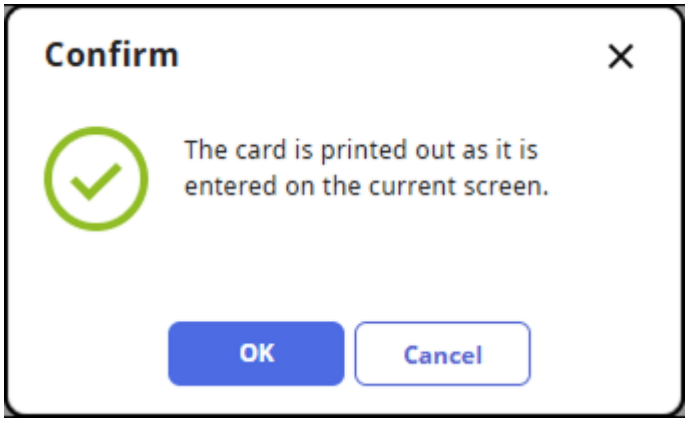
1. Haz clic en **User** en la página **Launcher**.
2. Haga clic en el botón **New User** en la parte superior derecha de la pantalla. Aparece la ventana **New User**.
3. Complete el formulario y haga clic en el botón **Print Card**.
   - Cada elemento puede contener caracteres alfanuméricos y especiales.



4. Seleccione la plantilla de tarjeta que desea imprimir y haga clic en el botón **Print**.



5. Cuando aparezca la ventana emergente que pregunta si desea imprimir la tarjeta, haga clic en el botón **OK**.

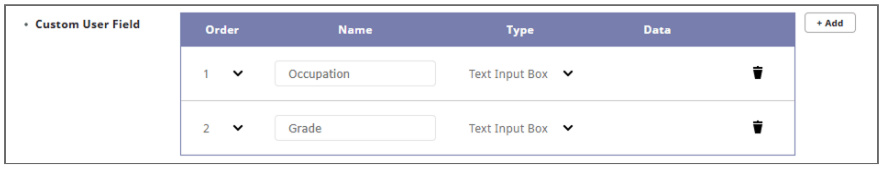


Se creará un nuevo usuario y se imprimirá una tarjeta como plantilla de tarjeta con la información del usuario.

Añadir campos de usuario personalizados

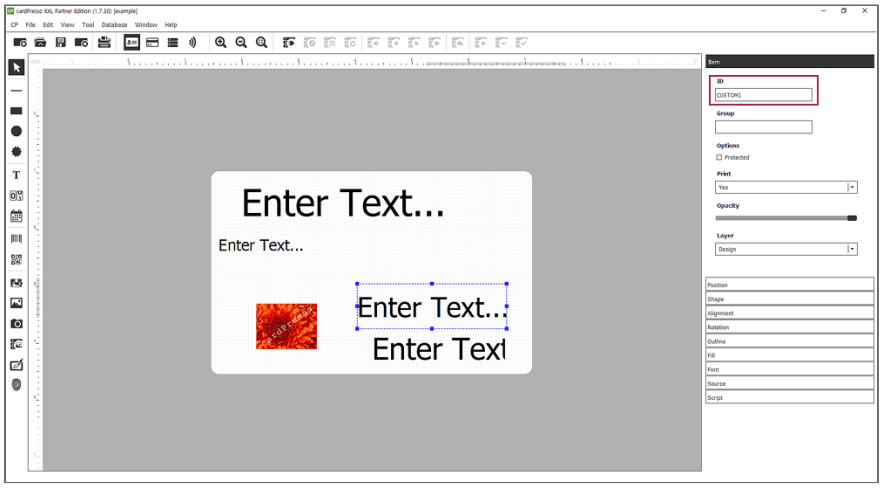
Imprima una tarjeta con una plantilla de tarjeta que incluya un campo de usuario personalizado.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **System** → **Server** en la barra lateral izquierda.
3. En la sección **User/Device Management**, haz clic en **+ Add** en **Custom User Field** para ingresar un **Name** y seleccionar un **Type**. El orden en que agregues **Custom User Field** determina el **ID** del elemento de la plantilla de tarjetas.



Según el ID de elemento de BioStar X, **Orden 1** equivale a **CUSTOM1**. Para obtener más información sobre los identificadores de atributos de BioStar X, consulte ID del atributo de la plantilla de tarjeta.

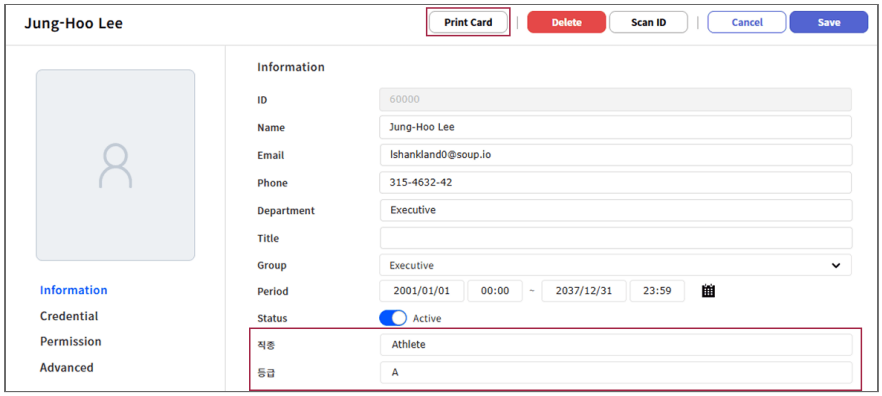
4. Una vez que completes la configuración, haz clic en **Apply** en la parte inferior de la pantalla.
5. Haz clic en **File** → **Open Template** en el programa cardPresso para abrir el archivo de plantilla de tarjeta. Agrega un nuevo elemento e ingresa el **ID** como **XML item ID name** en el orden de IDs de elementos de BioStar X.



6. Cuando finalices la configuración, haz clic en **File** → **Save**.

7. Regresa a **BioStar X** y selecciona el usuario al que aplicarás la plantilla de tarjeta en la página **User**.

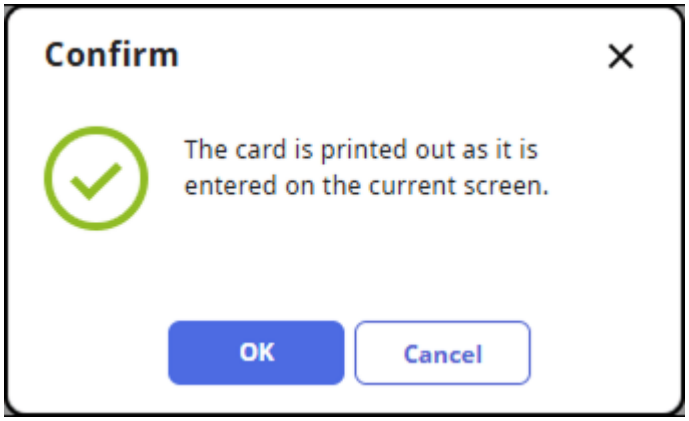
8. Verifica los campos de usuario personalizados que agregaste. Completa según el formulario y haz clic en **Print Card**.



9. Seleccione la plantilla de tarjeta que desea imprimir y haga clic en el botón **Print**.



10. Cuando aparezca la ventana emergente que pregunta si desea imprimir la tarjeta, haga clic en el botón **OK**.



La información del usuario se guarda y la tarjeta se imprime como una plantilla con los campos de usuario personalizados.

ID del atributo de la plantilla de tarjeta

Los IDs de atributos compatibles en **BioStar X** son los siguientes. Asegúrate de ingresar **XML item ID name** como ID de elemento al crear una plantilla de tarjetas.

Índice	Datos de usuario de BioStar X	Nombre de ID de elemento XML
1	ID Usuario	ID
2	Nombre Usuario	NAME
3	Email	EMAIL
4	Departamento	DEPARTMENT
5	Teléfono	TELEPHONE
6	Filtro Grupo Usuarios	GROUP
7	Foto de perfil	PHOTO
8	Campo personalizado 1	CUSTOM1
9	Campo personalizado 2	CUSTOM2
10	Campo personalizado 3	CUSTOM3
11	Campo personalizado 4	CUSTOM4
12	Campo personalizado 5	CUSTOM5
13	Campo personalizado 6	CUSTOM6
14	Campo personalizado 7	CUSTOM7
15	Campo personalizado 8	CUSTOM8

Índice	Datos de usuario de BioStar X	Nombre de ID de elemento XML
16	Campo personalizado 9	CUSTOM9
17	Campo personalizado 10	CUSTOM10

Administrar Tarjetas de Acceso Móvil

Integra el Airfob Portal para emitir o eliminar tarjetas de acceso móvil para los usuarios en **BioStar X**.

Los usuarios pueden recibir tarjetas de acceso móvil mediante un enlace enviado a su correo electrónico sin registrarse en Airfob Portal ni inscribirse por separado para las tarjetas de acceso móvil.

Información

- Solo se puede usar una de las siguientes para tarjetas de acceso móvil: **CSN Mobile** o **Template on Mobile**.
- Consulta lo siguiente para ver los dispositivos y versiones de firmware que admiten la tarjeta **CSN Mobile**.

  ▼ Ver dispositivos y versiones de firmware que admiten la tarjeta CSN Mobile

  – Firmware de BioStation 3 Max, versión 1.0.0 o posterior
  – Firmware de XPass Q2, versión 1.0.0 o posterior
  – BioEntry W3 versión de firmware 1.0.0 o superior
  – BioStation 3 firmware 1.0.0 o superior
  – X-Station 2 versión de firmware 1.0.0 o superior
  – FaceStation F2 versión de firmware 1.0.0 o superior
  – XPass 2 versión de firmware 1.1.0 o superior
  – FaceLite versión de firmware 1.2.0 o superior
  – BioLite N2 versión de firmware 1.3.0 o superior
  – XPass D2 (Rev 2) versión de firmware 1.4.0 o superior
  – FaceStation 2 versión de firmware 1.4.0 o superior
  – BioEntry W2 (Rev 2) versión de firmware 1.6.0 o superior
  – BioStation A2 versión de firmware 1.8.0 o superior (modelo con NFC)
  – BioStation 2 versión de firmware 1.9.0 o superior (modelo con NFC)

- Consulta lo siguiente para ver los dispositivos y versiones de firmware que admiten **Template on Mobile**.
  – Firmware de BioStation 3 Max, versión 1.0.0 o posterior
  – BioEntry W3 versión de firmware 1.0.0 o superior
  – BioStation 3 versión de firmware 1.2.0 o superior

Define si se usarán tarjetas de acceso móvil y administra los ajustes relacionados con la integración de Airfob Portal. Registra también los dispositivos que usarán tarjetas de acceso móvil. Después de registrarte en Airfob Portal, administra las tarjetas de acceso móvil en **BioStar X**.

1 Regístrate en Airfob Portal y crea un sitio

Configura las tarjetas de acceso móvil y los dispositivos registrados en Airfob Portal y administra tu sitio y créditos.

1. Accede al Airfob Portal.
2. Haz clic en **Get Started** para continuar con el registro y la creación del sitio.
3. Introduce la dirección de correo electrónico del administrador de Airfob Portal en el campo de correo electrónico y luego haz clic en **Get Started**. Se enviará un código de verificación a la dirección de correo electrónico ingresada.
4. Introduce el código de verificación recibido por correo electrónico en el campo correspondiente y luego haz clic en **Confirm**.

   > El código de verificación es un número de 6 dígitos.

5. Revisa la política de privacidad y los términos, luego haz clic en **Agree**.
6. Establece una contraseña y un apodo para Airfob Portal y luego haz clic en **Create Account**. La creación de la cuenta se completará.
7. Una vez que se haya completado la creación de la cuenta, haz clic en **Sign In**.
8. Introduce tu correo electrónico y contraseña y luego haz clic en **Sign In**.
9. Haz clic en **Create Site** para continuar con la creación del sitio.

   > **Site** se refiere a la organización o empresa que utiliza tarjetas de acceso móvil.

10. Define el nombre y el país del sitio y luego haz clic en **Next**.
11. Selecciona el tipo de sitio.

    > Seleccione el tipo de tarjeta **Dynamic** o **Regular** según el tipo de sitio.
    > - **Dynamic**: Tipo que deduce créditos según el dispositivo y la duración de uso, y permite acciones de gestión como revocación, suspensión, reemisión y definición de fecha de vencimiento incluso después de emitida la tarjeta. Este tipo es adecuado para instalaciones de membresía como gimnasios o salas de estudio, así como espacios de coworking.
    > - **Regular**: Tipo que deduce créditos según la cantidad de tarjetas emitidas y está disponible de forma permanente hasta que el administrador elimine las tarjetas en **BioStar X**. Este tipo es adecuado para que empresas o grupos lo utilicen como credenciales de empleado y tarjetas de acceso.

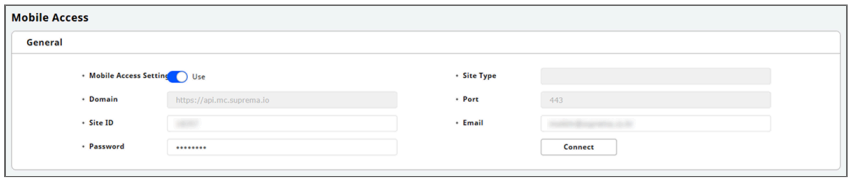
12. Haz clic en **Create**. La creación del sitio se completará.
13. Haz clic en el nombre del sitio para acceder a Airfob Portal de ese sitio.

> **Información**
> Para obtener más información sobre el uso de Airfob Portal, consulta el siguiente enlace.

2 Configura la tarjeta de acceso móvil en BioStar X

Después de registrarte en Airfob Portal, administra las tarjetas de acceso móvil en **BioStar X**. Para usar las tarjetas de acceso móvil de Suprema, regístrate en Airfob Portal y crea un sitio.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Credential** → **Mobile Access** en la barra lateral izquierda.
3. Edite los campos necesarios.



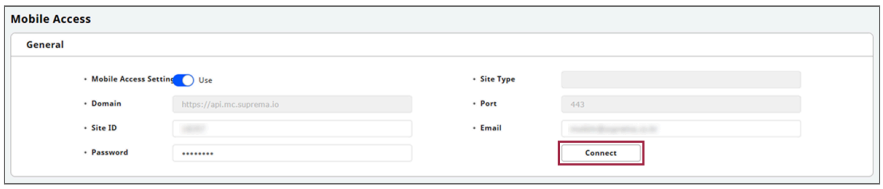
- **Mobile Access Setting**: Establece si se usarán tarjetas de acceso móvil. Configura en **Use** para emitir tarjetas de acceso móvil a los usuarios.
- **Site ID**: Introduce el ID del sitio creado en Airfob Portal. El ID del sitio se encuentra en la ruta **Settings** → **Site** dentro de Airfob Portal.
- **Email**: Introduce la dirección de correo electrónico de la cuenta administradora de las tarjetas de acceso móvil.
- **Password**: Introduce la contraseña de la cuenta administradora de las tarjetas de acceso móvil.

4. Haz clic en **Connect** cuando hayas terminado de configurar todo.

> **Información**
>
> Para usar tarjetas de acceso móvil en **BioStar X**, completa primero el registro y la configuración inicial de Airfob Portal. Para obtener más información, consulta Regístrate en Airfob Portal y crea un sitio.

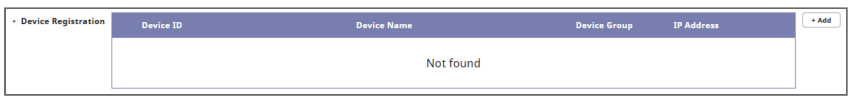
3 Inscribir dispositivo

Registra los dispositivos que usarán tarjetas de acceso móvil directamente desde la aplicación Airfob Pass o desde **BioStar X**.



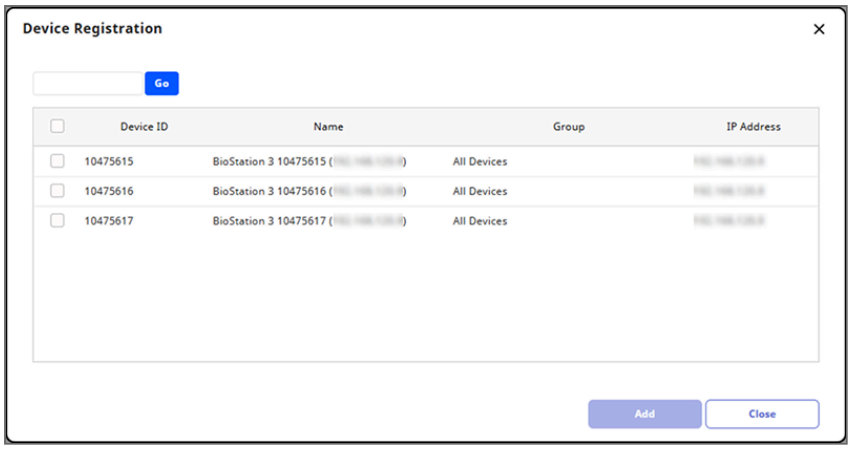
Una vez que hayas terminado de configurar la integración con Airfob Portal, haz clic en **Connect**. La opción **Device Registration** estará disponible.

1. Para añadir un dispositivo que usará tarjetas de acceso móvil, haz clic en **+ Add**.



2. En la lista de dispositivos de la ventana **Device Registration**, selecciona la casilla del dispositivo que usará la

tarjeta de acceso móvil.



3. Después de seleccionar todos los dispositivos, haz clic en **Add**.

Verifica los dispositivos añadidos en la lista de dispositivos.

- Haz clic en para reenviar el certificado de la tarjeta de acceso móvil.
- Haz clic en para eliminar un dispositivo registrado.

Información

- Consulta la siguiente información para conocer los dispositivos y las versiones de firmware que pueden usar tarjetas de acceso móvil.

  ▼ Ver dispositivos y versiones de firmware que pueden usar tarjetas de acceso móvil

  – Firmware de BioStation 3 Max, versión 1.0.0 o posterior
  – Firmware de XPass Q2, versión 1.0.0 o posterior
  – BioEntry W3 versión de firmware 1.0.0 o superior
  – BioStation 3 firmware 1.0.0 o superior
  – X-Station 2 versión de firmware 1.0.0 o superior
  – FaceStation F2 versión de firmware 1.0.0 o superior
  – XPass 2 versión de firmware 1.1.0 o superior
  – FaceLite versión de firmware 1.2.0 o superior
  – BioLite N2 versión de firmware 1.3.0 o superior
  – XPass D2 (Rev 2) versión de firmware 1.4.0 o superior
  – FaceStation 2 versión de firmware 1.4.0 o superior
  – BioEntry W2 (Rev 2) versión de firmware 1.6.0 o superior
  – BioStation A2 versión de firmware 1.8.0 o superior (modelo con NFC)
  – BioStation 2 versión de firmware 1.9.0 o superior (modelo con NFC)

- Registra dispositivos también mediante la aplicación Airfob Pass.
- Eliminar un dispositivo registrado quitará el certificado de la tarjeta de acceso móvil enviado a ese dispositivo.

4 Emitir tarjeta de acceso móvil

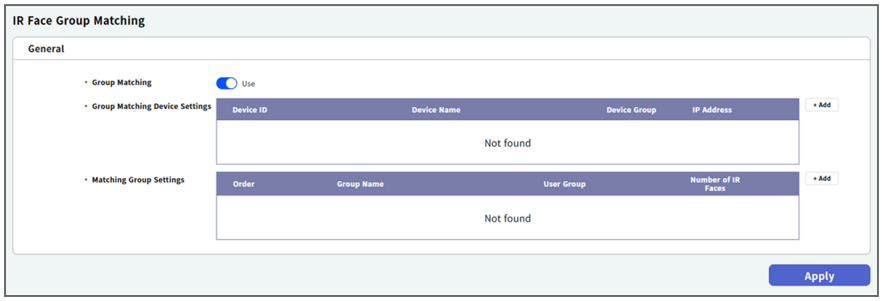
Emite tarjetas de acceso móvil a los usuarios registrados en **BioStar X**. Ingresa la información esencial del usuario según el método de envío para emitir una tarjeta de acceso móvil al usuario. Para obtener más información, consulta lo siguiente.

- Registrar usuarios
- Registrar Credenciales Móviles

Configurar Grupos Identificación Facial IR

IR Face Group Matching autentica a los usuarios mediante la configuración de grupos de coincidencia basados en grupos de usuarios. Utilice esta función para permitir el acceso mediante autenticación IR facial solo a los usuarios de ciertos grupos de usuarios.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Credential** → **IR Face Group Matching** en la barra lateral izquierda.
3. Establezca la opción **Group Matching** en **Use**.



4. Haz clic en **+ Add** en **Group Matching Device Settings**.
5. Cuando aparezca la ventana **Group Matching Device Settings**, seleccione el dispositivo y haga clic en **Add**.

> Sólo se puede seleccionar FaceStation 2.

6. Haz clic en **+ Add** en **Matching Group Settings**.
7. Configure los campos **Group Name** y **User Group**.
8. Haga clic en **Apply** en la parte inferior derecha de la pantalla para guardar los ajustes.

Información

- Se pueden crear hasta 10 grupos de coincidencia.
- Cada grupo puede contener hasta 3,000 plantillas de rostro IR.
- Se pueden asignar múltiples grupos de usuarios a un solo grupo de coincidencia.
- El número total de plantillas IR faciales en un grupo de coincidencia no puede exceder 5,000.
- Si un grupo de usuarios contiene más de 3,000 plantillas IR faciales, no se puede establecer como grupo de coincidencia.
- Esta función es compatible solo con el modelo FaceStation 2.
- Elimine todos los dispositivos configurados y los ajustes de grupo para desactivar la función de coincidencia de grupos.

Activar Licencia

Esta guía explica cómo activar la licencia de **BioStar X** y las licencias de dispositivo.

Licencia Biostar X

Active la licencia de **BioStar X** adquirida.

La forma de activar **BioStar X License** varía según el entorno de red. Verifique el estado de la red y active la licencia según las instrucciones proporcionadas.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **License** → **BioStar X License** en la barra lateral izquierda.

Información

- Para obtener más información sobre la política de licencias, consulte Política de Licencias.
- Para obtener información sobre los códigos de error de licencias, consulta el siguiente enlace.

Registrar en línea

Información

La clave de licencia acepta solo números y guiones (`-`). Ingrese hasta 16 dígitos en el formato `1111-1111-1111-1111`.

Registrar una sola licencia

Ingrese su nombre y la clave de licencia recibida y, a continuación, haga clic en **Activate** para activar la licencia de **BioStar X** mientras está en línea con una conexión a Internet.



Registrar varias licencias

Agregue hasta 30 licencias a la vez. Haga clic en el botón + **Add More License**. Después de ingresar todas las licencias, haga clic en **Activate**.



- Cuando la cantidad de campos llegue a 30, el botón + **Add More License** se desactiva. No puede agregar más licencias.
- Pegue varias claves de licencia en los campos a la vez. El sistema detecta solo las claves con el formato `1111-1111-1111-1111` y las divide en cada campo.
- Si las claves pegadas superan 30, el sistema ingresa automáticamente solo las primeras 30. El sistema ignora las claves adicionales.

Progreso de activación

Haga clic en **Activate** para abrir la ventana emergente de progreso. No cierre la página ni la ventana emergente hasta que finalice la activación.

Registrar sin conexión

Siga las instrucciones a continuación para activar la licencia de **BioStar X** en un entorno de red cerrado o en un estado sin conexión con acceso limitado a Internet.

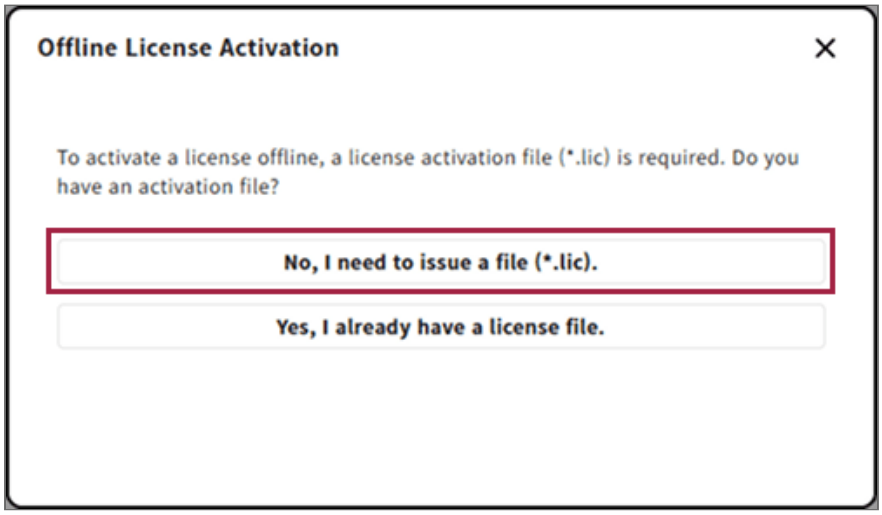
1. Ingrese cualquier nombre del administrador de inscripción y la clave de licencia en la sección **License Activation**.

   - La clave de licencia acepta solo números y guiones (`-`). Ingrese hasta 16 dígitos en el formato `1111-1111-1111-1111`.
   - Guarde o anote el nombre de administrador y la clave de licencia.
   - Si necesita varias licencias, haga clic en el botón + **Add More License** para agregarlas.

2. Haga clic en **Offline Activation**.

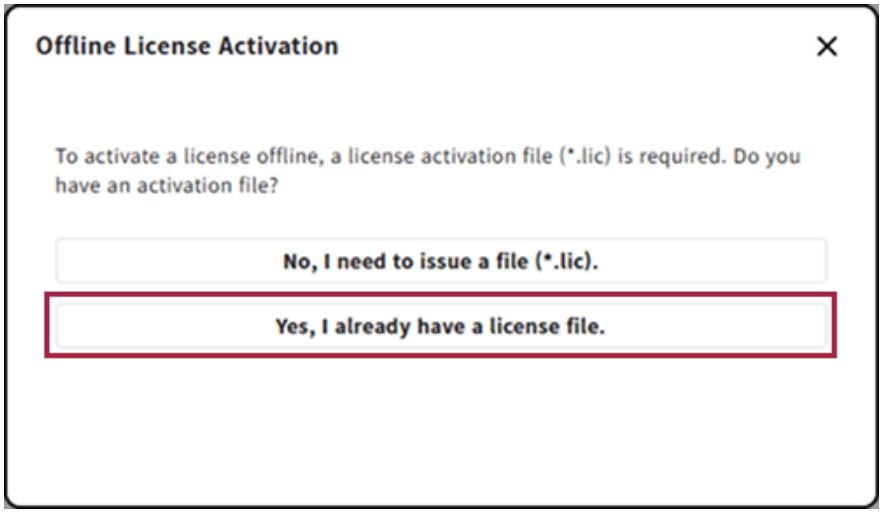


3. Cuando aparezca la ventana **Activate License Offline**, haga clic en **No, I need to issue a file (*.lic).**.



> Si tiene un archivo de licencia emitido, haga clic en **Yes, I already have a license file.** en esta pantalla y luego vaya al paso 9.

4. Cuando el sistema cree el archivo de solicitud de licencia (*.req), descárguelo en el disco local.
5. Envíe el archivo de solicitud descargado al revendedor y solicite un archivo de activación sin conexión (*.lic).
6. Tras recibir el archivo sin conexión, escriba el nombre de administrador y la clave del paso 1 en la sección **License Activation**.
7. Haga clic en **Offline Activation**.
8. Cuando aparezca la ventana **Activate License Offline**, haga clic en **Yes, I already have a license file.**.



9. Cuando aparezca la ventana Abrir archivo, seleccione el archivo de activación sin conexión (*.lic) o el comprimido (*.zip) almacenado localmente.

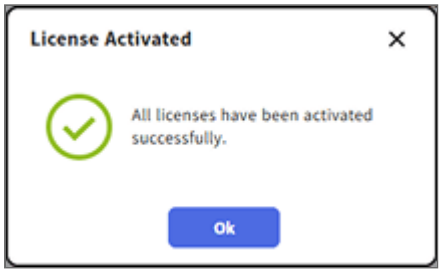
> Si solicita varias licencias, recibirá un archivo comprimido.

10. Aparece una ventana emergente con el estado del progreso. No cierre la página ni la ventana emergente hasta que finalice la activación.

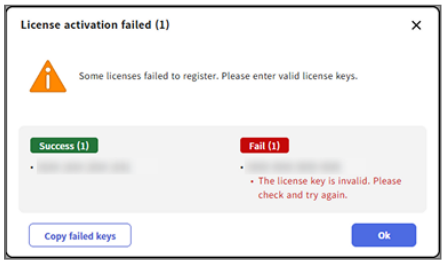
Verifique los resultados de activación de la licencia

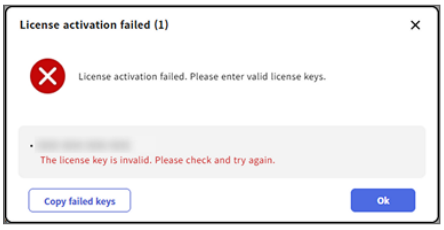
Según los resultados de activación de la clave de licencia ingresada, aparece el siguiente mensaje.

- Si todas las claves de licencia ingresadas son válidas, aparece un mensaje de éxito.



- Si el sistema activa solo ciertas claves o no activa todas, revise el estado y el motivo de falla de cada clave. El sistema borra los campos de las claves activadas y mantiene las fallidas para volver a ingresarlas.





- Si todas las claves fallan sin conexión a Internet, aparece un mensaje para verificar la conexión y reintentar. Aparece el botón **Offline Activation**. Si la red está aislada, haga clic en este botón para activar sin conexión.

> **Información**
>
> Haga clic en **Copy failed keys** para copiar las claves fallidas.

Verificar licencia activada

Consulte la información de la licencia de **BioStar X** activada en **Activated License**.



Licencia de dispositivo

Activa **Device License** emitida por Suprema para usar las características específicas asociadas a la licencia.

Device License permite activar la licencia de dispositivo mediante **BioStar X** y una memoria USB.

> **Información**
>
> - Contacta al lugar de compra para obtener una licencia de dispositivo.
> - Hay una función disponible por licencia de dispositivo.
> - Es posible incluir varias licencias de dispositivo en un solo archivo de licencia de dispositivo. (Admite hasta 100)
> - El archivo de licencia del dispositivo está cifrado y no puede modificarse de forma arbitraria.
> - Las licencias de dispositivo se emiten según el ID del dispositivo. Si el ID del dispositivo se cambia de manera inusual, no se proporciona servicio de garantía para la licencia.
> - Para obtener información sobre los códigos de error de licencias, consulta el siguiente enlace.

Antes de comenzar

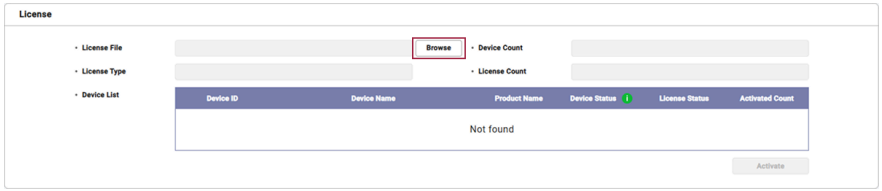
Antes de activar la licencia de dispositivo, verifica lo siguiente.

- Prepara un archivo de licencia de dispositivo válido. Solicita el archivo de licencia de dispositivo en el lugar de compra.
- Asegúrate de que el dispositivo de destino esté registrado en **BioStar X**. Para obtener más información sobre cómo agregar dispositivos, consulta Registrar dispositivo.

Aplicar licencia de dispositivo

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **License** → **Device License** en la barra lateral izquierda.

3. Haz clic en **Browse**.



4. Carga el archivo de licencia de dispositivo desde la ruta donde está guardada la licencia.

5. La información correspondiente a la licencia cargada aparece en **License Type**, **Device Count**, **Device List**.



6. Marca **Device List**, y para activar la licencia del dispositivo, haz clic en **Activate**.

> **Información**
> Si la activación de la licencia falla, aparece un mensaje de error. Intenta activar la licencia nuevamente.

Información de la licencia de dispositivo

Cuando cargas el archivo de licencia de dispositivo, aparece la siguiente información.

- **License Type**: Verifica el tipo de licencia incluido en el archivo de licencia de dispositivo.
  - **Camera QR**

    Los dispositivos que pueden usar **Camera QR** son los siguientes.
    - Firmware de BioStation 3 Max, versión 1.0.0 o posterior
    - Firmware de XPass Q2, versión 1.0.0 o posterior
    - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) versión de firmware 1.2.0 o superior
    - X-Station 2 (XS2-QDPB, XS2-QAPB) versión de firmware 1.4.1 o superior
    - Versión de firmware 1.1.0 o posterior para BioStation 3

  - **Multi Face Authentication**

    Los siguientes dispositivos pueden usar la licencia **Multi Face Authentication**.
    - Versión de firmware 1.5.0 o posterior para BioStation 3

    Establece la opción **Multi Face Authentication** en los dispositivos con esta licencia habilitada. Consulta Configuración de Autenticación.

- **Cerradura inalámbrica**

> – La antena OSDP y la cerradura inalámbrica compatibles son las siguientes:
> – Antena OSDP U&Z: CX8936
> – Cerradura inalámbrica U&Z: CX217x (Manija), CX212x (Perilla)
> – Se puede emitir una licencia de dispositivo para hasta 12 dispositivos, equivalente al número de cerraduras inalámbricas que se deseen conectar.
> – El número máximo de cerraduras inalámbricas que se puede conectar con una licencia de dispositivo es 12. Aunque se activen varias licencias de dispositivo, no es posible superar 12 dispositivos.

- **Device Count**: Verifica la cantidad de dispositivos incluidos en el archivo de licencia de dispositivo.
- **License Count**: Verifica la cantidad de cerraduras inalámbricas que se pueden activar con una licencia de dispositivo.
- **Device List**: Permite consultar la información detallada de los dispositivos incluidos en el archivo de licencia de dispositivo.
  - **Device ID**: ID único que identifica el dispositivo.
  - **Device Name**: Nombre del dispositivo.
  - **Product Name**: Nombre del modelo del dispositivo.
  - **Device Status**: Estado actual del dispositivo. Solo los dispositivos en estado **Normal** pueden activar licencias.
    - **Normal**, **Disconnected**, **Not Supported**, **Unregistered**

> Si el dispositivo es un modelo que no admite la función de licencia o si la versión de firmware es baja, **Device Status** se mostrará como **Not Supported**. Verifica los modelos y las versiones de firmware compatibles con esa función.

  - **License Status**: Indica si la licencia está activada. Solo los dispositivos **Not Activated** pueden activar licencias.
    - **Not Activated**, **Activated**, **N/A**
  - **Activated Count**: Estado de conexión de las cerraduras inalámbricas.

> **Información**
>
> - La información de **License Count** y **Activated Count** solo aparece cuando se carga la licencia de dispositivo de la cerradura inalámbrica.

Gestionar Registro De Auditoría

La característica **Audit Trail** registra y rastrea todas las actividades del sistema. Registra actividades como inicio/cierre de sesión, cambios de ajustes y tareas de administración del sistema. Estos registros se usan para auditorías de seguridad y monitoreo del sistema.

El grupo **Audit Trail** en la barra lateral izquierda incluye los siguientes menús.

- **AC Audit Log**: Registra actividades de control de acceso, como crear, actualizar, eliminar, ver, exportar, importar y acciones administrativas relacionadas con usuarios, dispositivos y puertas.
- **Audit Settings**: Define el período de retención del registro de auditoría y si se registra el historial de visualización.

> **Información**
>
> Para obtener más información sobre **T&A Audit Log**, consulte Ver Registros de Auditoría de Tiempo y Asistencia. El menú **T&A Audit Log** solo aparece con una licencia activa de control de tiempo y asistencia (T&A).

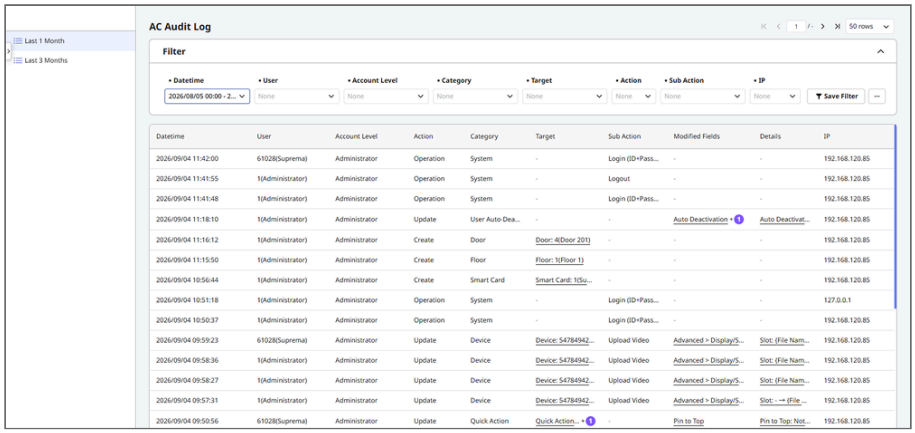
Ver Registros de Auditoría de Control de Acceso

La característica **AC Audit Log** registra la actividad de control de acceso para usuarios, dispositivos y puertas: crear, actualizar, eliminar, ver, exportar, importar y operaciones. Cada registro muestra cuándo ocurrió, quién hizo el cambio, qué cambió y cómo, para respaldar auditorías y la resolución de problemas.

- **Auditoría de seguridad**: Detectar intentos de acceso no autorizado o abuso de privilegios.
- **Solución de problemas**: Supervisar cuándo ocurren errores del sistema y revisar cambios de ajustes.
- **Cumplimiento**: Conservar registros de acceso, incluido el historial de acceso a datos personales, y crear informes de auditoría.

Consultar registros de auditoría de control de acceso

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Audit Trail** → **AC Audit Log** en la barra lateral izquierda.
3. La lista de registros de auditoría aparece en la pantalla.



Información

- Para cambiar las políticas del registro de auditoría, como el período de retención, consulta Administrar Ajustes de Retención del Registro de Auditoría.
- Después de actualizar a la versión 1.0.3, el sistema cifra los nuevos registros de auditoría, independientemente de la opción **Encrypt Personal Data on Database** en **Settings** → **System** → **Security**.
- Si el sistema no registra ciertos registros de auditoría después de la actualización de BioStar 2 a **BioStar X**, consulte Actualizar.

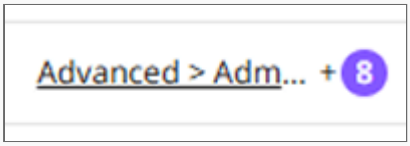
Diseño de la tabla

La tabla de la lista de registros de auditoría tiene 10 columnas y muestra los registros en orden descendente por **Datetime**.

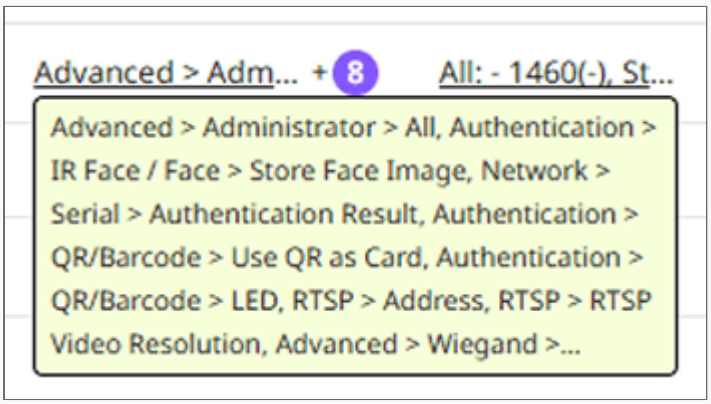
Columna	Descripción
Datetime	Fecha y hora en que ocurrió el evento.
User	Usuario que realizó el evento. Aparece en el formato **id(nombre)**.
Account Level	El nivel de administrador del usuario que realizó el evento.
Action	El tipo de acción ejecutada. Se clasifica como **Create**, **Update**, **Delete**, **Read**, **Export**, **Import** o **Operation**.
Category	La categoría de dominio del objetivo del evento (por ejemplo, usuarios, dispositivos y puertas).
Target	Destino al que se aplica la acción. Aparece en el formato **type: id(name)**.
Sub Action	Aparece solo cuando hay un nombre de acción detallado, como el método de inicio de sesión o el desarmado de alarma.
Modified Fields	Nombre del campo que cambió o se consultó.
Details	Información detallada de cada acción. (p. ej., valores cambiados, motivos y criterios de búsqueda)
IP	Dirección IP desde la cual el usuario accedió. El sistema muestra los registros emitidos automáticamente como **127.0.0.1**.

Información

- Si el valor de **Target** o **Modified Fields** tiene 2 entradas o más, solo se muestra la primera y el resto se contrae en una insignia con el conteo restante a la derecha (p. ej., **+208**). Si el conteo restante es de 1,000 o más, la insignia muestra **+999**. Revise el conteo total exacto en el título de la ventana emergente de detalles. Haga clic en la insignia para abrir la ventana emergente de detalles de esa celda.

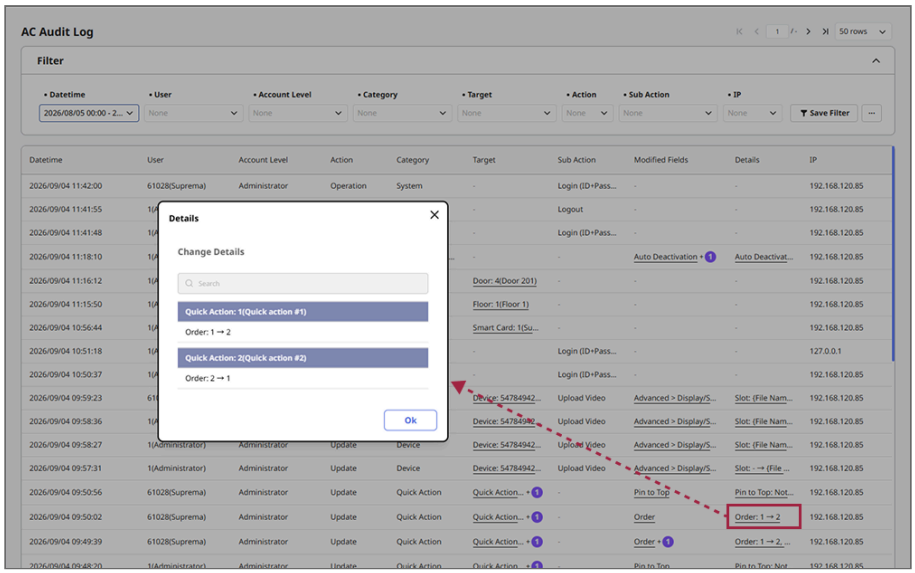


- Los valores largos de las celdas se truncan a una línea con puntos suspensivos. Pase el cursor sobre el valor para ver el texto completo en la información sobre herramientas. La información sobre herramientas trunca el texto excedente como `...`.



Ver detalles

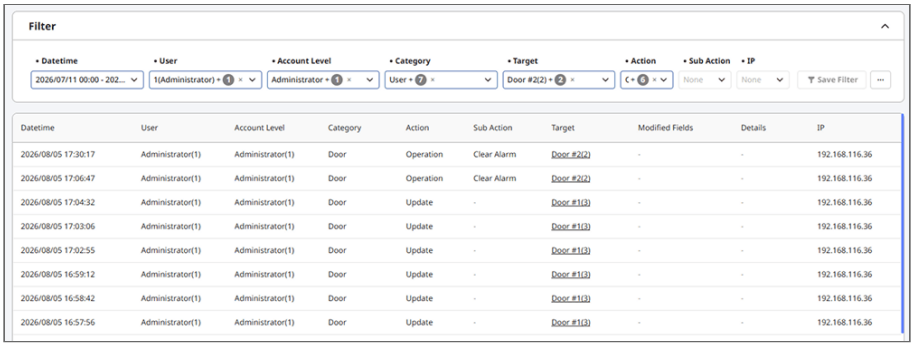
Las columnas **Target**, **Modified Fields** y **Details** aparecen subrayadas y permiten hacer clic cuando tienen valores. Haga clic en un valor de la columna para abrir la ventana emergente de detalles específica de la acción. Para cerrar la ventana emergente, haga clic en **OK** o ✕.



Escriba una palabra clave en el campo **Search** en la parte superior de la ventana emergente para resaltar o filtrar las entradas coincidentes. Al buscar, la ventana emergente de destino actualiza los grupos y el recuento por grupo. El total del título no cambia.

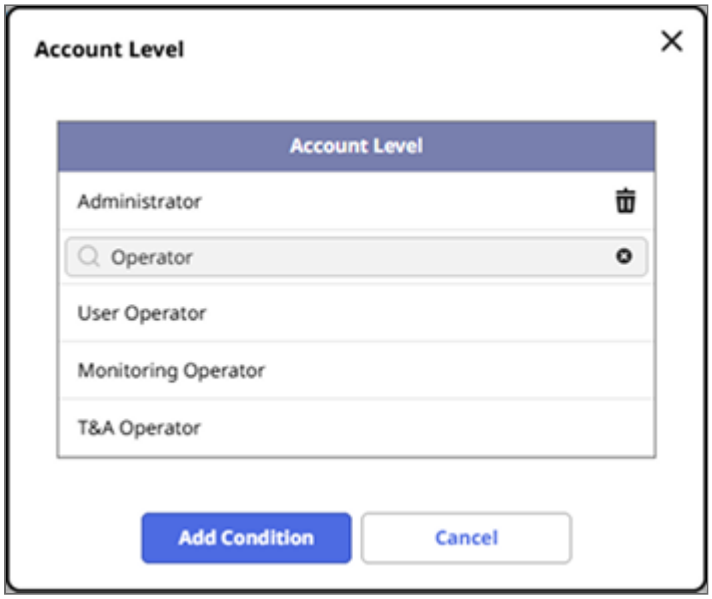
Buscar registros con filtros

Combine los filtros en la sección **Filter** para acotar y encontrar los registros que necesita. Seleccione varios valores en un filtro para combinarlos con `OR`. Aplique varios filtros a la vez para combinarlos con `AND`.

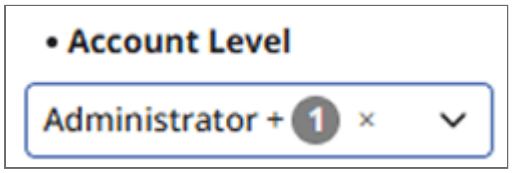


Filtrar	Cómo funciona
Datetime	Establezca las fechas y horas de inicio y fin. No se aplica un límite de duración al período de búsqueda.
User	Escriba un término de búsqueda y presione `Enter` para encontrar usuarios coincidentes. La lista está vacía cuando la abre por primera vez.
Account Level	Escriba un término de búsqueda y presione `Enter` para encontrar niveles de administrador coincidentes.
Category	Seleccione una o más categorías de la lista de casillas de verificación con búsqueda.
Target	Escriba un término de búsqueda y presione `Enter` para encontrar objetivos coincidentes.
Action	Seleccione una o más acciones de la lista de casillas de verificación.
Sub Action	Seleccione una acción detallada de la lista con búsqueda.
IP	Escriba un término de búsqueda y luego presione `Enter` para encontrar direcciones IP coincidentes.

- Si no aplica filtros, aparecen de forma predeterminada los registros de los últimos 30 días.
- Seleccione un valor en cada ventana emergente de filtro y luego haga clic en **Add Condition** para aplicarlo a la búsqueda de inmediato. Haga clic en **Cancel** para cancelar la selección y cerrar la ventana emergente.



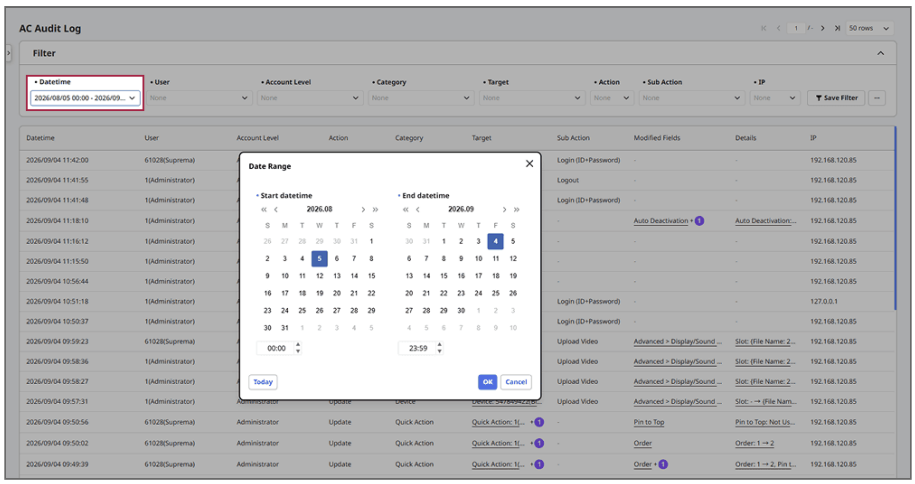
- Los filtros aplicados aparecen como el primer filtro y la cantidad de filtros adicionales. Haga clic en ✕ para desactivar solo ese filtro. Los filtros sin un valor seleccionado aparecen como **None**.



> **Información**
>
> Escriba un término de búsqueda para ver resultados de los filtros **User**, **Account Level**, **Target** y **IP**. La búsqueda admite coincidencias parciales; escriba parte de un nombre o ID. La búsqueda incluye destinos eliminados y los marca como **Deleted**.

Configurar período de consulta

Haga clic en **Datetime** para abrir la ventana **Date Range**.

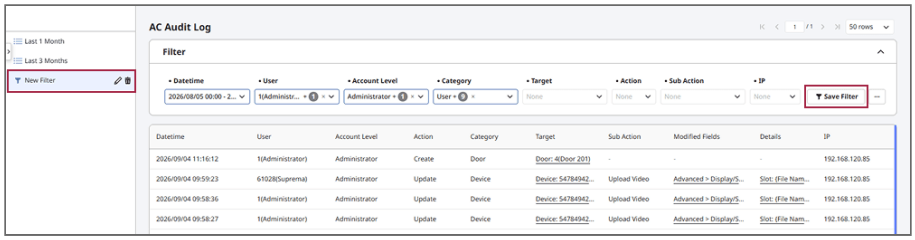


1. Configure la fecha y la hora de **Start datetime** y **End datetime**. Haga clic en **Today** para ir a hoy.
2. Haga clic en **OK** para aplicar el período de consulta.

Guardar filtro

Guarde las condiciones de búsqueda de uso frecuente en **Saved Filters** y cárguelas cuando sea necesario.

1. Configure los filtros para que coincidan con las condiciones requeridas.
2. Haga clic en **Save Filter** en la sección **Filter**.
3. El sistema agrega **New Filter** a la lista de filtros de la izquierda.



- Haga clic en ✎, escriba un nombre nuevo y presione Enter para cambiar el nombre del filtro.
- Haga clic en 🗑 para eliminar el filtro.

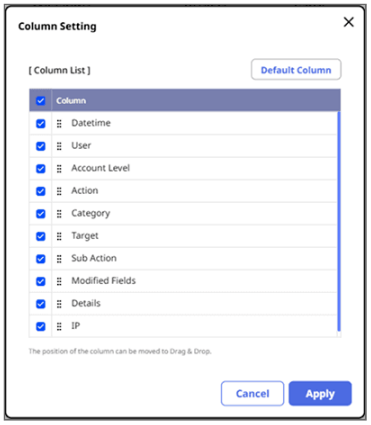
> **Información**
> El sistema permite guardar hasta 20 filtros. El navegador almacena los filtros guardados, por lo que no aparecen en otras PC ni en otros navegadores.

Navegación de páginas

Desplácese entre páginas o establezca la cantidad de elementos que aparecerán en cada página.

- |<: Ir a la primera página.
- <: Ir a la página anterior.
- >: Ir a la página siguiente.
- >|: Ir a la última página.
- 50 rows: Seleccione la cantidad de filas por página.

Configurar columnas



Cambie la posición de las columnas u oculte columnas en la tabla del registro de auditoría. En el lado derecho de la sección **Filter**, haga clic en ••• → **Column Setting**.

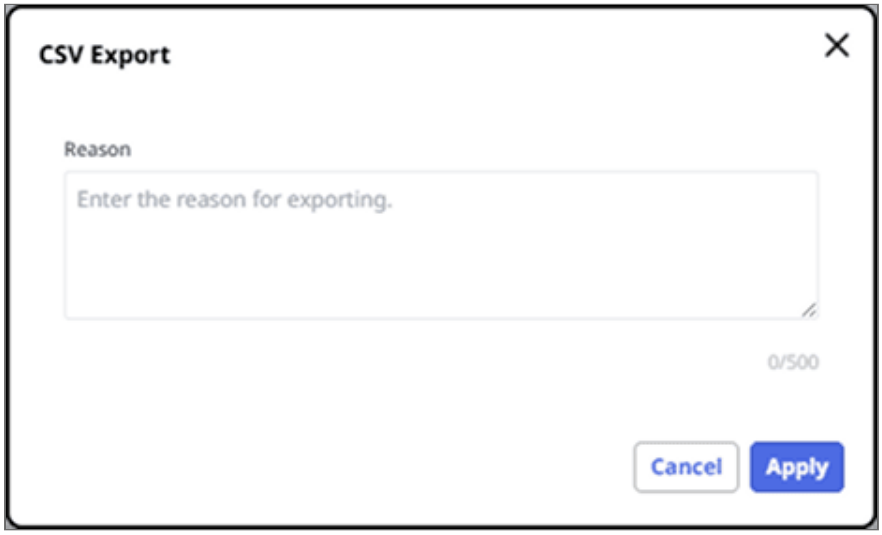
- En **[Column List]**, desmarque la casilla de la columna para ocultarla.
- Arrastre una columna para cambiar el orden de las columnas.
- Haga clic en **Default Column** para inicializar la configuración de columnas.

Haga clic en **Apply** para guardar la configuración.

Exportar a CSV

Exporte los registros de auditoría a un archivo CSV para utilizarlo con herramientas de análisis externas.

1. En la sección **Filter**, configure filtros si es necesario.
2. Haga clic en ••• → **CSV Export** en el lado derecho de la sección.
3. Cuando aparezca la ventana **CSV Export**, ingresa **Export Reason** (opcional) y haz clic en **Apply**.



El CSV exportado incluye 10 columnas, una fila por registro, y pone entre comillas todos los valores. Los valores con varios destinos usan una barra vertical (|) (p. ej., **User: 7(Kim)|User: 8(Lee)**). El valor **Details** incluye todos los destinos y campos sin truncar.

> **Precaución**
> El archivo CSV incluye los valores tal cual, incluidos los que una hoja de cálculo puede interpretar como fórmulas. No abra el archivo CSV descargado directamente en una hoja de cálculo. Si es necesario, ábralo con la característica de importación de texto.

> **Consejo**
> Si configura filtros, la exportación incluye solo los resultados filtrados en el archivo CSV.

Revisar registros de BioStar 2

La misma tabla también muestra registros de versiones anteriores (BioStar 2). Los registros de BioStar 2 aparecen de la siguiente manera.

- **User** y **Target** mantienen el formato original **name(id)** (incluidas las variaciones de espacios).
- **Modified Fields** siempre muestra un guion (-).
- también puede buscar registros de BioStar 2 con los filtros proporcionados, y **User** y **Target** coinciden con el nombre y el ID.

Información

Los registros heredados pueden incluir criterios de búsqueda no compatibles. Cuando cargas un filtro guardado, aparece un aviso si se excluyen ciertos criterios.

Administrar Ajustes de Retención del Registro de Auditoría

Los registros de auditoría aumentan con el tiempo. Gestiona el período de retención para ahorrar almacenamiento y proteger la privacidad. En **Audit Settings**, defina el período de retención de los registros **AC Audit Log** y decida si conserva el historial de consultas.

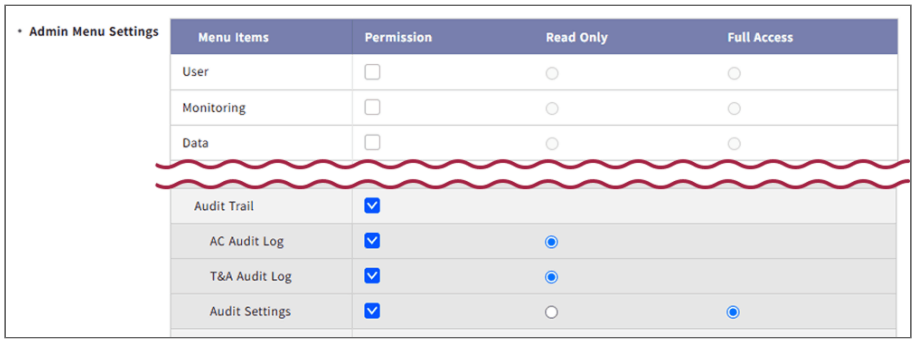
Información

Un documento independiente describe la política de retención de los registros de auditoría de Tiempo y Asistencia (T&A).

Información de privilegios

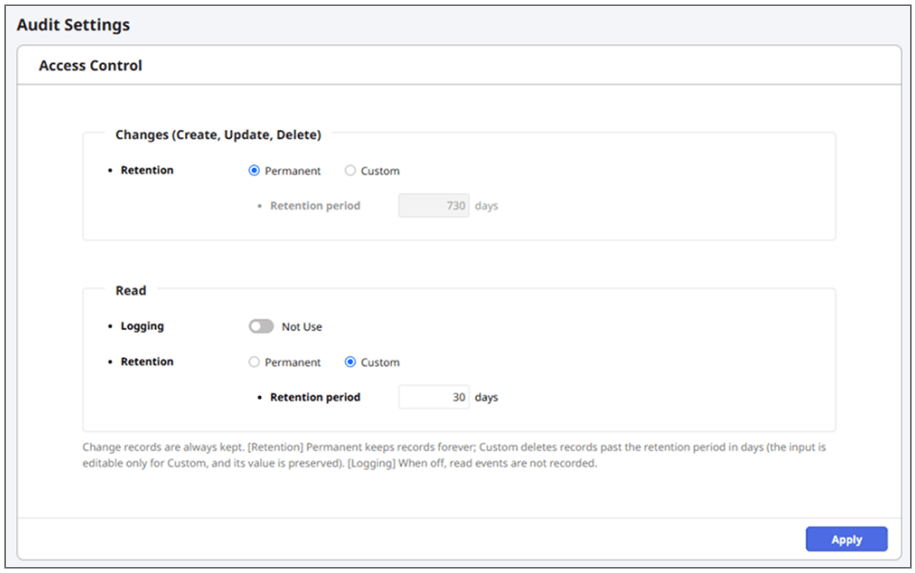
Administrator siempre puede ver y cambiar los ajustes en el menú **Audit Settings**. Para un administrador con privilegios personalizados, en **Admin Menu Settings**, establezca **Audit Settings** en **Read Only** para solo lectura, o en **Full Access** para ver y cambiar.

Settings → ***Account*** → ***Account*** → ***Add Custom Level***



Abrir ajustes de auditoría

1. Haz clic en **Settings** en la página **Launcher**.
2. En la barra lateral izquierda, haz clic en **Audit Trail** → **Audit Settings**.



Ajustes de la política de retención

La sección **Access Control** consta de los siguientes dos grupos.

- **Changes (Create, Update, Delete)**: Registros de creación, actualización y eliminación. El sistema siempre los registra. No puede activar ni desactivar el registro.
- **Read**: Ver registros. Defina si el sistema crea registros.

> **Información**
>
> - Ingrese **Retention period** como un número entero entre 1 y 2,147,483,647 días.
> - Seleccione **AC Audit Log** para ver los registros de auditoría de cambios de ajustes en la sección **Access Control**.

Registros de cambios

Como el sistema siempre registra el grupo **Changes (Create, Update, Delete)**, seleccione el ajuste **Retention**.

- **Permanent**: Conserve los registros de forma permanente sin eliminación automática.
- **Custom**: Seleccione esta opción para limitar el período de retención por cumplimiento o política interna. Cuando se active el campo **Retention period**, ingrese el período de retención en días.

Ver registros

En el grupo **Read**, defina si el sistema conserva los registros de visualización.

- **Logging**: Establezca esta opción en **Use** para conservar los registros de visualización. Si no se necesita, establézcalo en **Not Use**.
- **Retention**: Seleccione un método de retención.
  - **Permanent**: Conserve los registros de visualización de forma permanente sin eliminación automática.
  - **Custom**: Activa el campo **Retention period**. Ingrese el período de retención en días.

> **Información**
> Cuando **Logging** está en **Not Use**, el sistema no registra eventos de visualización. Después de cambiarlo a **Use**, el sistema no muestra los registros anteriores.

Guardar configuración

Después de completar los ajustes de **Changes (Create, Update, Delete)** y **Read**, haz clic en el botón **Apply** en la parte inferior de la sección **Access Control**. Guarda ambos ajustes de grupo juntos.

Cómo funciona la eliminación automática

El servidor ejecuta esta tarea todos los días a la 1 a. m. La tarea elimina los registros que superan el período de retención establecido en **Custom**, sin importar las acciones del usuario. La tarea evalúa y elimina los registros al mismo tiempo. La tarea se ejecuta solo una vez al día.

> *Por ejemplo, establece los registros de **Read** en 30 días en **Custom**. A la 1 a. m., la tarea elimina los registros con más de 30 días de antigüedad. Los registros que acaban de superar el período de retención permanecen hasta que se ejecute la siguiente tarea de la 1 a. m.*

Cuando **Retention** se establece en **Permanent**, la tarea de eliminación automática no se ejecuta y los registros se conservan permanentemente.

Configuración del Sistema

Explica los ajustes para un funcionamiento estable del sistema **BioStar X**. Configura servidor y certificados HTTPS; protege datos con copia de seguridad y restauración; usa políticas de contraseñas y cifrado. Configura ajustes básicos, como el horario de verano, las notificaciones por correo electrónico, el idioma y la zona horaria.

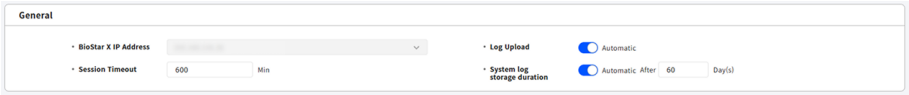
Configuración Detallada del Servidor

Cambie la configuración de información básica del servidor BioStar X, la gestión de usuarios y dispositivos, la autenticación en servidor, los niveles de registro del sistema y la configuración para guardar imágenes faciales.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **System** → **Server** en la barra lateral izquierda.
3. Configure los elementos deseados en cada sección.
    - **General**: Configure la dirección IP, el número de puerto, el tiempo de expiración de la sesión, el método de carga de registros de eventos y el período de retención de registros.
    - **User/Device Management**: Cambie la configuración de gestión de usuarios y dispositivos.
    - **System Log Level Settings**: Cambie la configuración del nivel de registro del sistema.
    - **Expert Settings**: Configure para guardar tanto la imagen real como la plantilla del rostro, o guardar solo la plantilla sin almacenar la imagen real.
4. Haga clic en **Apply** en la parte inferior derecha de la pantalla para guardar los ajustes.

Configuración de información básica

Verifique o configure la información básica de **BioStar X** en la sección **General**.

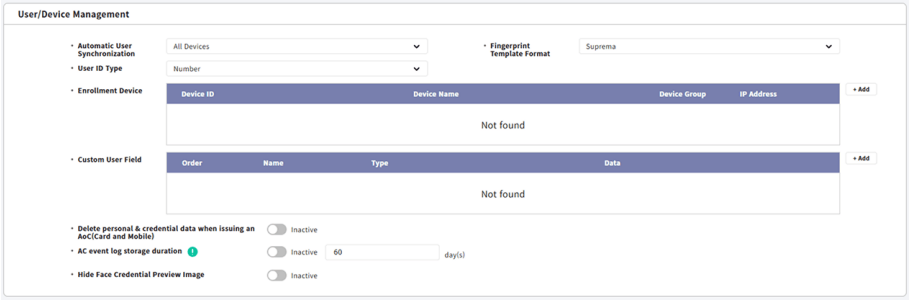


- **BioStar X IP Address**: Verifique la dirección IP del servidor.
- **Log Upload**: Seleccione un método de carga de registros de eventos. Si la comunicación en tiempo real con el servidor es difícil, configure esta opción en **Manual**.
- **System log storage duration**: Establezca el período de retención de registros de 1 a 120 días.
- **Session Timeout**: Configure un período de expiración de sesión. Si no hay operación después de iniciar sesión en BioStar X durante el tiempo configurado, la sesión se cerrará automáticamente.

> **Información**
>
> Si establece **Log Upload** en **Automatic**, el dispositivo carga automáticamente los registros de eventos al servidor cuando se pierde y se restablece la conexión entre el servidor y el dispositivo.

Gestión de usuarios y dispositivos

En la sección **User/Device Management**, configure los métodos de sincronización y autenticación entre usuarios y dispositivos.



Automatic User Synchronization

En la opción **Automatic User Synchronization**, elija cómo sincronizar la información de usuario entre el servidor y los dispositivos. La sincronización incluye los niveles de acceso y los grupos de acceso asignados a los usuarios. Si cambia los niveles de acceso o los grupos de acceso en el servidor **BioStar X**, los cambios se aplican automáticamente a los dispositivos relacionados.

- **All Devices**: La información de usuario se sincroniza automáticamente entre el servidor y todos los dispositivos registrados.
- **All Devices(Including user update from device)**: La información de usuario del servidor se sincroniza con todos los dispositivos registrados en el servidor. Sin embargo, la información de usuario modificada en el dispositivo no se sincroniza con el servidor; solo la información de usuario añadida en el dispositivo se sincroniza con el servidor.
- **Specific Devices(Only devices belonging to the access group)**: Solo los dispositivos que pertenecen a un grupo de acceso con cambios se sincronizan automáticamente con el servidor.

Información

- Si selecciona la opción **Specific Devices(Only devices belonging to the access group)**, los usuarios guardados en dispositivos que no pertenecen al grupo de acceso no podrán ser gestionados por el servidor. Vaya a **Settings** → **Device** → **Device**, seleccione cada dispositivo y haga clic en **Delete Data & Sync Device** para iniciar la sincronización. Para obtener más información sobre la función **Delete Data & Sync Device**, consulte Usar la Función de Administración de Dispositivos.
- Incluso si selecciona la opción **Specific Devices(Only devices belonging to the access group)**, los grupos de acceso especiales designados para fines específicos se sincronizarán independientemente del grupo de acceso del dispositivo.
  - Grupo de acceso de autenticación dual configurado en Dispositivos y Elevadores.
  - Grupo Always pass para la configuración anti-passback
  - Grupo Always pass para la configuración de bloqueo programado
  - Grupo de acceso de autenticación abierta para la configuración de apertura programada
  - Grupo Access/Deactivate para la configuración de guardia
- Incluso si selecciona la opción **Specific Devices(Only devices belonging to the access group)**, los usuarios designados como administradores del dispositivo se sincronizarán independientemente del grupo de acceso.

Fingerprint Template Format

En la opción **Fingerprint Template Format**, elija el formato de plantilla de huella digital. Seleccione entre los siguientes elementos.

- **SUPREMA**: Formato de plantilla de huella digital de Suprema. Se utiliza al enrolar huellas digitales en dispositivos Suprema.
- **ISO**: Formato internacional de plantilla de huella digital ISO.
- **ANSI378**: Formato de plantilla de huella digital definido por el American National Standards Institute (ANSI).

Información

Si existen plantillas de huellas digitales de usuario en el dispositivo, no se pueden cambiar a otro formato.

User ID Type

En la opción **User ID Type**, seleccione el tipo de ID de usuario como **Number** o **Alphanumeric**. Revise la lista de dispositivos registrados en el servidor **BioStar X** y seleccione la configuración compatible.

▼ **Ver los dispositivos y las versiones de firmware que pueden cambiar User ID Type**

- Firmware de BioStation 3 Max, versión 1.0.0 o posterior
- Firmware de XPass Q2, versión 1.0.0 o posterior
- BioStation 3 firmware 1.0.0 o superior
- X-Station 2 versión de firmware 1.0.0 o superior
- Firmware de XPass 2 1.0.0 o posterior
- Firmware de FaceLite 1.0.0 o posterior

- Firmware de BioLite N2 1.0.0 o posterior
- Versión de firmware de XPass D2 1.0.0 o superior
- BioEntry R2 FW 1.0.0 o posterior
- Firmware de BioEntry P2 1.0.0 o posterior
- Firmware de FaceStation 2 1.0.0 o posterior
- BioEntry W2 FW 1.1.0 o posterior
- BioStation L2 FW 1.2.0 o posterior
- BioStation A2 FW 1.3.0 o posterior
- BioStation 2 FW 1.4.0 o posterior
- Versión de firmware de CoreStation 1.0.0 o superior

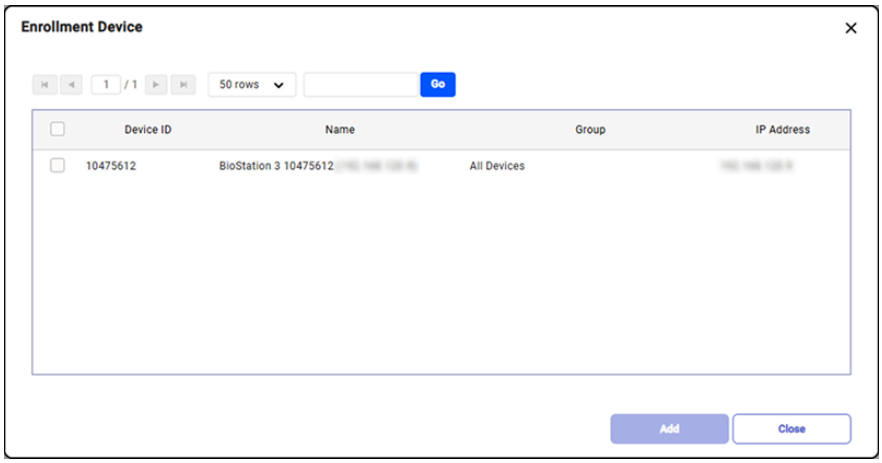
Información

Cambiar de **Alphanumeric** a **Number** requiere eliminar toda la información de usuario registrada en **BioStar X**.

Enrollment Device

Para mayor comodidad, añada dispositivos usados con frecuencia para enrolar huellas digitales, rostros o tarjetas en la opción **Enrollment Device**.

1. Haga clic en **+ Add** para agregar un dispositivo.
2. Cuando aparezca la ventana **Enrollment Device**, haga clic en la casilla de verificación del dispositivo deseado en la lista.



3. Haga clic en **Add** para agregar el dispositivo seleccionado.
4. Haga clic en **Apply** en la esquina inferior derecha de la pantalla para guardar la configuración del dispositivo añadido.

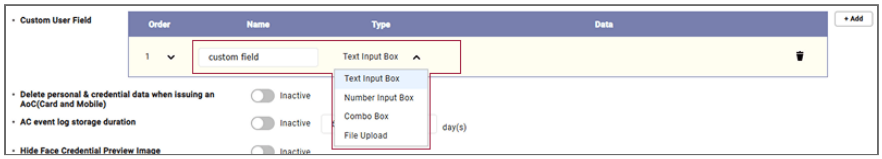
Información

- Si resulta difícil localizar un dispositivo registrado en la lista debido a la gran cantidad, ingrese palabras clave en el campo de búsqueda para encontrar dispositivos. Ingrese el ID del dispositivo, el nombre del dispositivo, el grupo de dispositivos y la dirección IP.
- Para obtener más información sobre cómo enrolar credenciales de huella dactilar, rostro o tarjeta, consulte lo siguiente:
  - Inscribir Huella Dactilar
  - Registrar Cara
  - Inscribir Tarjeta de Acceso
  - Registrar Credenciales Móviles

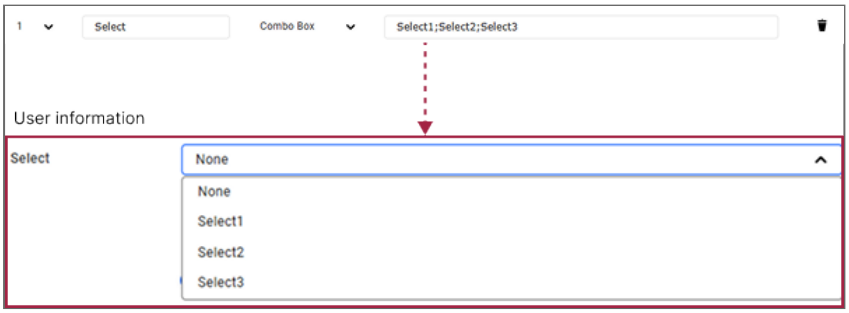
Custom User Field

En la opción **Custom User Field**, agregue campos para ingresar información adicional del usuario. Los campos agregados se mostrarán en la pantalla de información del usuario.

1. Haga clic en **+ Add** para agregar un campo de usuario personalizado.
2. Ingrese el nombre del campo de usuario personalizado y seleccione el tipo de elemento deseado.



- **Number Input Box**: Permite ingresar valores de 0 a 4294962795; no se pueden ingresar caracteres.
- **Text Input Box**: Permite ingresar hasta 32 caracteres entre números y letras.
- **Combo Box**: Permite agregar hasta 20 elementos de 32 caracteres; cada elemento se separa con punto y coma (;). (p. ej., Seleccion1;Seleccion2;Seleccion3)



- **File Upload**: Permite agregar un campo para cargar archivos.

- El tamaño máximo del archivo es 1MB.
- El nombre del archivo puede contener un mínimo de 1 carácter y un máximo de 120 caracteres.
- Requisitos del nombre de archivo: el nombre debe usar caracteres alfanuméricos, guiones bajos (_) y guiones (-), y debe usar un punto (.) para separar la extensión.
- No hay restricciones en las extensiones de archivos, y los archivos subidos son cifrados y almacenados en la base de datos.

3. Haga clic en **Apply** en la parte inferior derecha de la pantalla para guardar el campo de usuario personalizado agregado.

Información

- Modifique los números en la columna **Order** para cambiar el orden de los campos de usuario personalizados. La posición de ese campo cambiará.
- Después de modificar los campos de usuario personalizados, haga clic en **Apply** en la parte inferior derecha de la pantalla.
- Haga clic en para eliminar un campo de usuario personalizado. Los campos eliminados no se pueden recuperar.
- Para obtener más información sobre cómo registrar y editar la información de usuario, consulte Usuario.
- La información del usuario con campos personalizados añadidos se puede imprimir en una tarjeta. Para obtener más información sobre cómo agregar campos de usuario personalizados, consulte Impresora de Tarjetas.

Configuración de tarjetas AoC

Habilite la opción **Delete personal & credential data when issuing an AoC(Card and Mobile)** para emitir una credencial Access on Card (AoC) que almacena las credenciales del usuario en una tarjeta y elimina la información personal y los datos de credenciales del servidor **BioStar X**.

Información

▼ **Ver dispositivos que admiten tarjetas móviles NFC**

- Sistema operativo del dispositivo móvil: Android 7.0 o posterior
- BioStar X Móvil
- BioStation 3 Max
- XPass Q2
- XPass 2
- FaceLite
- BioLite N2
- XPass D2
- BioEntry R2
- BioEntry P2
- FaceStation 2
- BioEntry W2
- BioStation L2: BSL2-OM
- BioStation A2: BSA2-OMPW, BSA2-OIPW
- BioStation 2: BS2-OMPW, BS2-OIPW

▼ **Ver dispositivos que admiten tarjetas móviles BLE**

- Sistema operativo del dispositivo móvil: Android 7.0 o posterior / iOS 13.0 o posterior
- BioStar X Móvil
- BioStation 3 Max
- XPass Q2
- XPass 2
- FaceLite: FL-DB
- BioLite N2
- XPass D2
- FaceStation 2: FS2-AWB

- Las funciones **Mobile Access Card** y **Mobile Access** no se pueden utilizar al mismo tiempo.

Otros ajustes

- **AC event log storage duration**: Configure el período de retención de los registros de eventos de control de acceso.

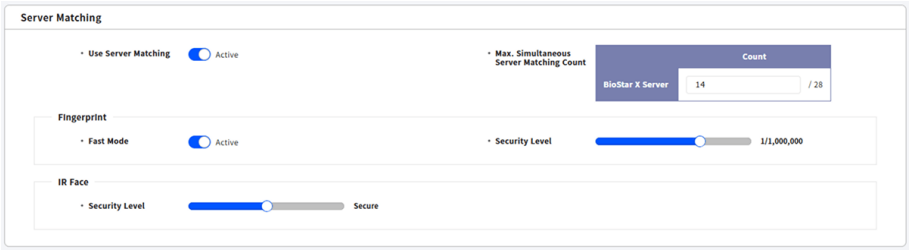
Información

El ajuste de retención del registro de eventos de control de acceso solo se aplica a los registros del servidor. Este ajuste no se aplica a los registros de eventos del dispositivo. Vaya a **Settings** → **Device** → **Device** y elimine los registros de eventos del dispositivo de forma individual.

- **Hide Face Credential Preview Image**: Para proteger la información personal de los usuarios, la imagen de vista previa se puede ocultar durante el registro de credenciales faciales. Cuando esta opción está habilitada, la pantalla de vista previa no se mostrará al enrolar credenciales faciales de los usuarios.

Autenticación en servidor

En la sección **Server Matching**, configure la función de autenticación en servidor para autenticar la información del usuario en **BioStar X** sin autenticarla en el dispositivo.



- **Use Server Matching**: Activa/desactiva la función de autenticación en servidor.
- **Max. Simultaneous Server Matching Count**: Configure cuántas coincidencias pueden realizarse simultáneamente.

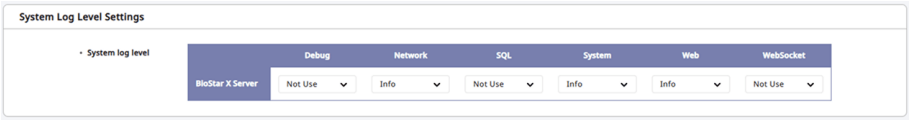
  > Esta opción puede variar según el rendimiento de la CPU de la PC servidor donde esté instalado **BioStar X**.

- **Fingerprint**
  - **Fast Mode**: Configure la velocidad de coincidencia de huellas dactilares.
  - **Security Level**: Configure el nivel de seguridad de coincidencia del servidor para huellas dactilares. Cuanto más alto sea el nivel de seguridad, mayor puede ser la tasa de rechazo falso (FRR).
- **IR Face**
  - **Security Level**: Configure el nivel de seguridad de coincidencia del servidor para rostros IR. Cuanto más alto sea el nivel de seguridad, mayor puede ser la tasa de rechazo falso (FRR).

> **Información**
>
> La característica **Server Matching** está disponible como opción adicional con una licencia **Essential** o superior. Para obtener más información sobre la política de licencias, consulte Política de Licencias.

Configuración del nivel de registro del sistema

En la sección **System Log Level Settings**, configure el nivel de registros del sistema que se almacenan en la base de datos.



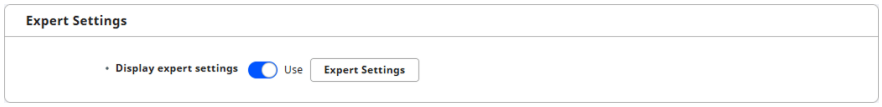
Los registros del sistema se gestionan según categorías predefinidas, y los niveles de registro se clasifican en **Trace**, **Debug**, **Info**, **Warning** y **Error**. El nivel más alto incluye todos los registros de los niveles inferiores. Por ejemplo, al seleccionar **Trace**, se incluirán y guardarán todos los registros de los niveles inferiores **Debug**, **Info**, **Warning** y **Error**.

Guardar imágenes faciales

Al inscribir un rostro como credencial, se puede configurar para guardar tanto la imagen real como la plantilla, o guardar solo la plantilla sin la imagen real.

> **Antes de usar**
>
> Antes de habilitar la opción **Display expert settings**, guarde los cambios en el menú **Server**. Haz clic en **Apply** en la parte inferior derecha de la pantalla.

1. En la sección **Expert Settings**, establece la opción **Display expert settings** en **Use**.



2. Haga clic en **Expert Settings**.
3. Al ingresar a la pantalla **Expert Settings**, configura la opción **Store Face Image**.



   - **Use**: Este es el valor predeterminado. Guarda tanto la imagen real como la plantilla de la credencial de rostro.
   - **Not Use**: No guarda la imagen real de la credencial de rostro y guarda solo la plantilla. Lee detenidamente la ventana emergente de advertencia que aparece al seleccionar esta opción antes de configurarla.
4. Haga clic en **Apply** para guardar la configuración.

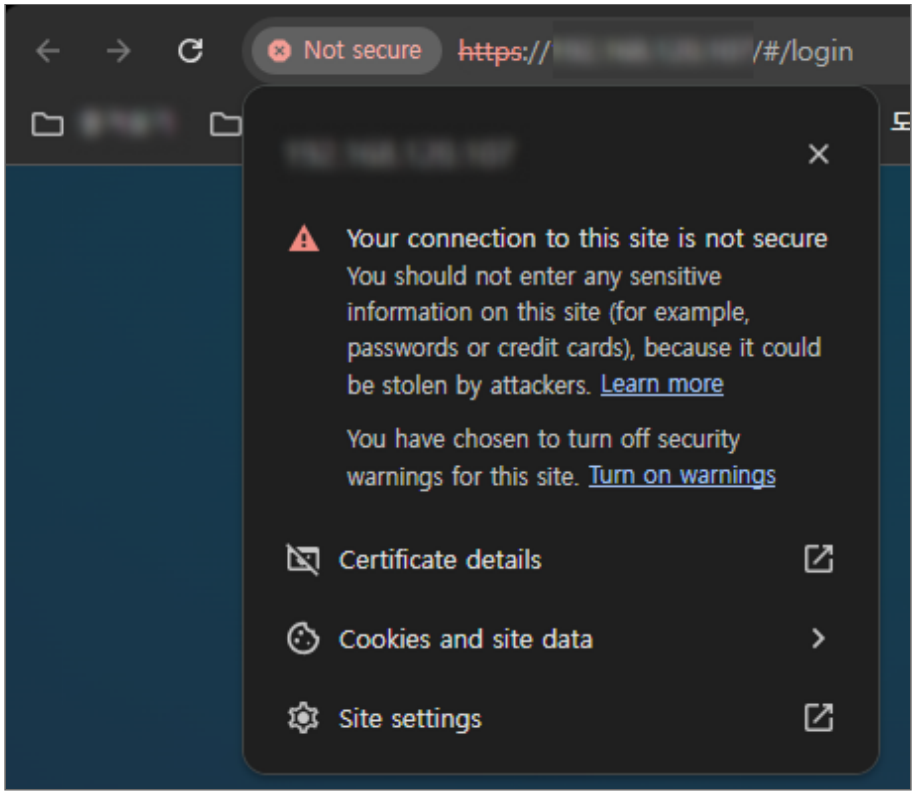
> **Precaución**
>
> **Precauciones al desactivar la opción Store Face Image**
>
> - Si desactivas esta función, se eliminarán todas las imágenes faciales almacenadas y las futuras inscripciones de rostro guardarán solo las plantillas, excluyendo las imágenes.
> - No es posible desactivar esta función si las imágenes faciales inscritas no tienen ambos tipos de plantillas. Para obtener más información sobre la función **Face Migration**, consulte Migracion Visual Face.
> - Después de desactivar esta función, si incluyes plantillas de imagen facial inválidas en **Data File Import**, no podrás importar el archivo de datos. Para resolver este problema, habilita temporalmente esta función antes de importar el archivo de datos.

Instalar Certificado HTTPS

Para conectar **BioStar X** mediante HTTPS, debe registrar la dirección IP del servidor donde está instalado **BioStar X** para instalar el certificado.

Cuándo se requiere la instalación del certificado

Si accede a **BioStar X** sin tener instalado el certificado HTTPS, aparecerá una advertencia de seguridad como la siguiente en su navegador web.

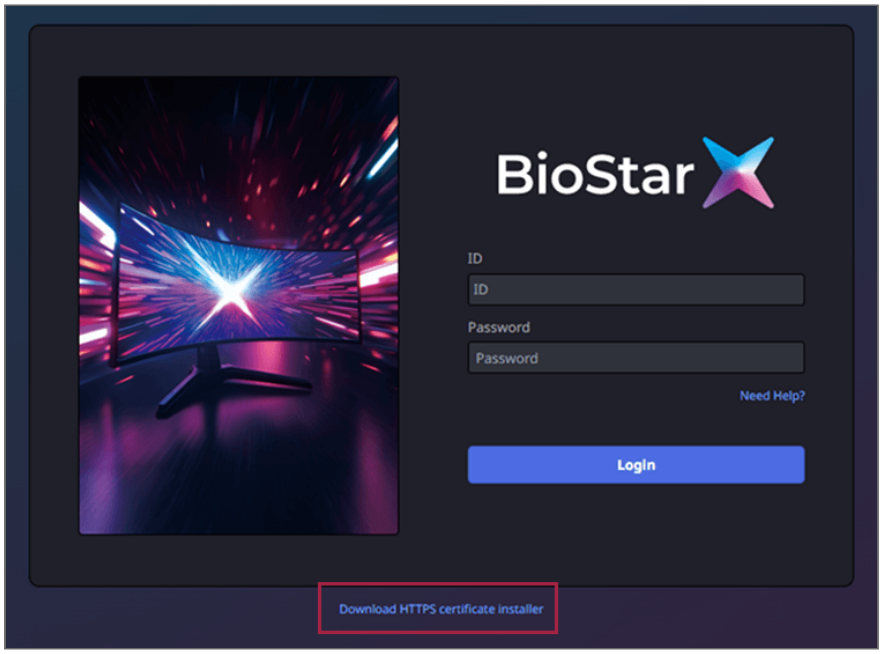


Estas advertencias aparecen porque el navegador no puede verificar la identidad del servidor. La instalación del certificado hará que el navegador confíe en el servidor **BioStar X**, lo que permitirá una conexión HTTPS segura sin advertencias de seguridad.

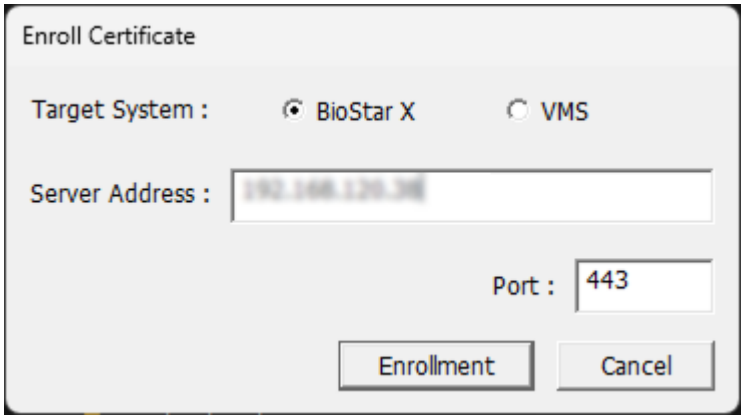
Instalación del certificado

Instale el certificado antes de utilizar **BioStar X** para garantizar la conectividad de red correcta.

1. Acceda a la página de inicio de sesión de **BioStar X**.
2. Haga clic en el enlace **Download HTTPS certificate installer** en la parte inferior de la pantalla.



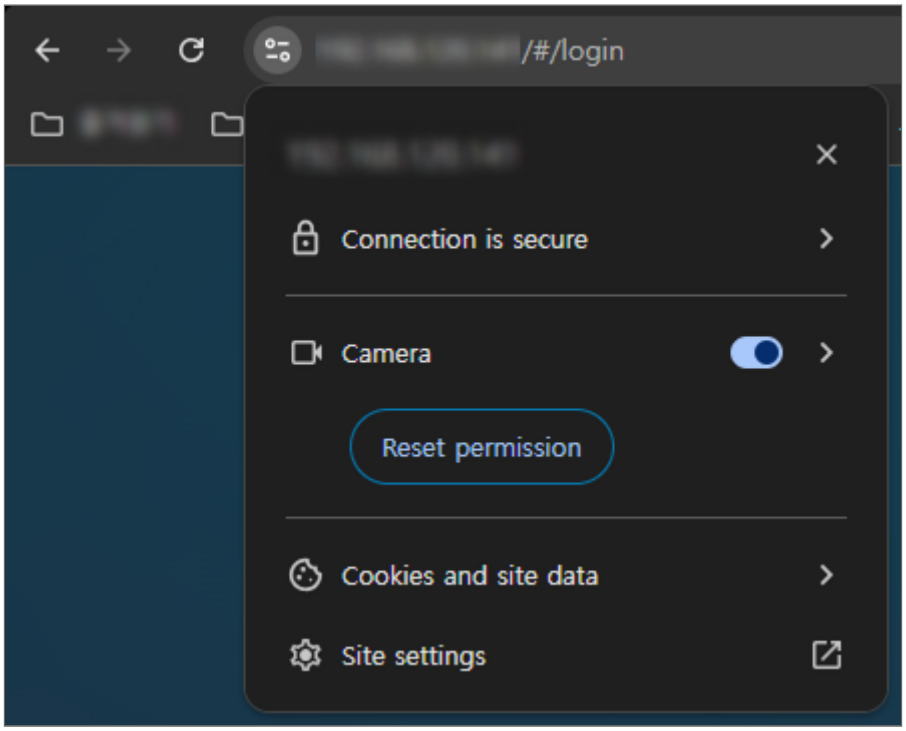
3. Guarde el archivo *cert-register.zip* localmente.
4. Extraiga el archivo descargado y ejecute el archivo *cert-register.exe*. Se ejecuta el programa **Enroll Certificate**.
5. Seleccione **BioStar X** en **Target System**, introduzca la dirección IP del PC donde está instalado **BioStar X** en **Server Address** y haga clic en **Enrollment**.



> El número de puerto predeterminado para **BioStar X** es 443. Si cambió el número de puerto, introduzca el nuevo número en **Port**.

6. Verifique el mensaje de advertencia de seguridad y haga clic en **Yes**.

Reinicie el navegador web e introduzca la dirección IP registrada para acceder a la página de **BioStar X**. Al hacer clic en el ícono a la izquierda de la barra de direcciones, aparecerá el mensaje **Esta conexión es segura**.

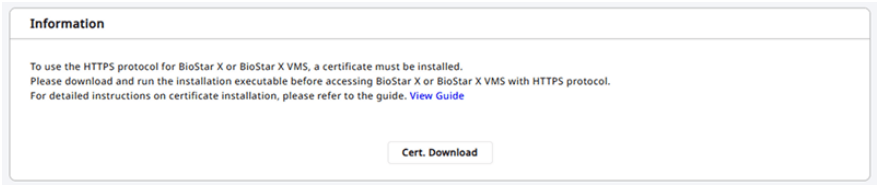


Información

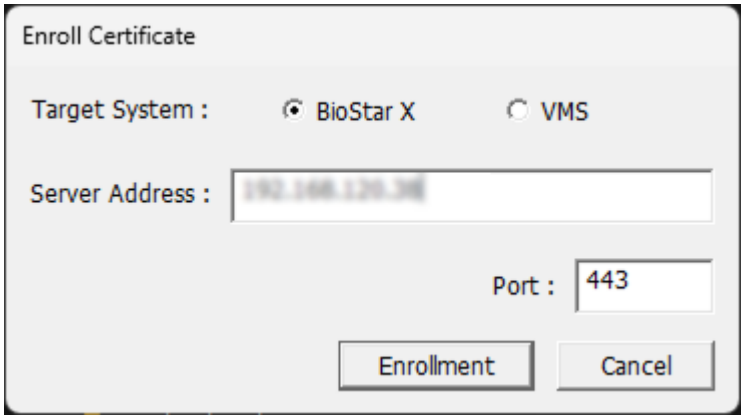
La dirección IP introducida en **Enroll Certificate** debe ser la misma que la establecida en **BioStar X**. Compruébela en la ruta de menú **Settings** → **System** → **Server** en **BioStar X IP Address**.

Instalación del certificado en la configuración del servidor

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **System** → **HTTPS** en la barra lateral izquierda.
3. Haga clic en **Cert. Download**.



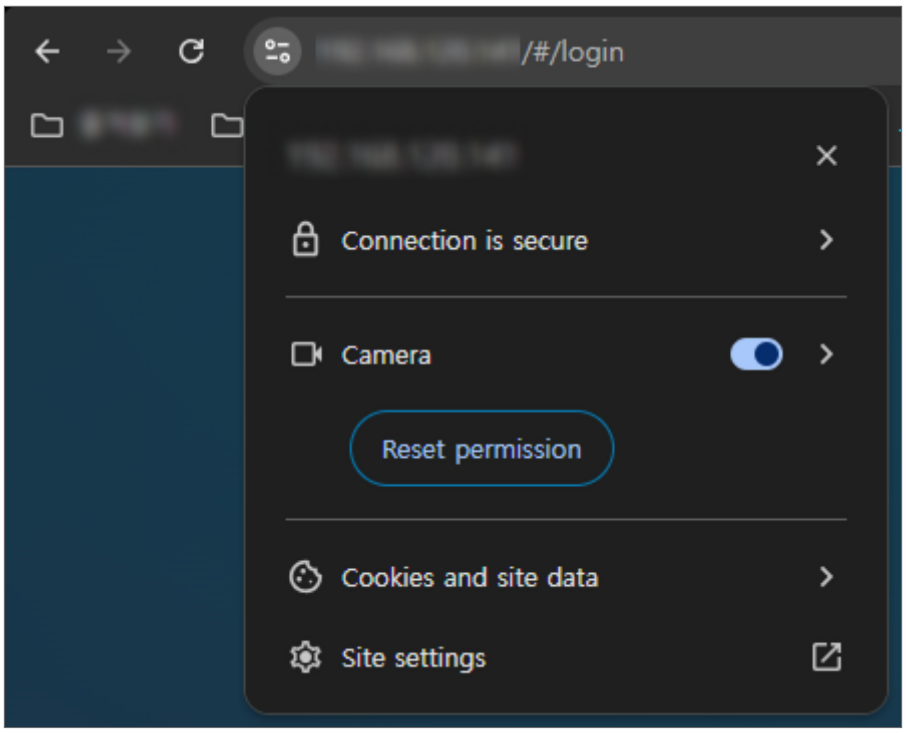
4. Guarde el archivo *cert-register.zip* localmente.
5. Descomprima el archivo descargado y ejecute el archivo **cert-register.exe**. Se ejecuta el programa **Enroll Certificate**.
6. Seleccione **BioStar X** en **Target System**, introduzca la dirección IP del PC donde está instalado **BioStar X** en **Server Address** y haga clic en **Enrollment**.



> El número de puerto predeterminado para **BioStar X** es 443. Si cambió el número de puerto, introduzca el nuevo número en **Port**.

7. Verifique el mensaje de advertencia de seguridad y haga clic en **Yes**.

Reinicie el navegador web e introduzca la dirección IP registrada para acceder a la página de **BioStar X**. Al hacer clic en el ícono a la izquierda de la barra de direcciones, aparecerá el mensaje **Esta conexión es segura**.



Instalación del certificado para el servidor VMS

Si se presentan las siguientes situaciones, instala el certificado desde el servidor VMS en el PC cliente para resolver el problema.

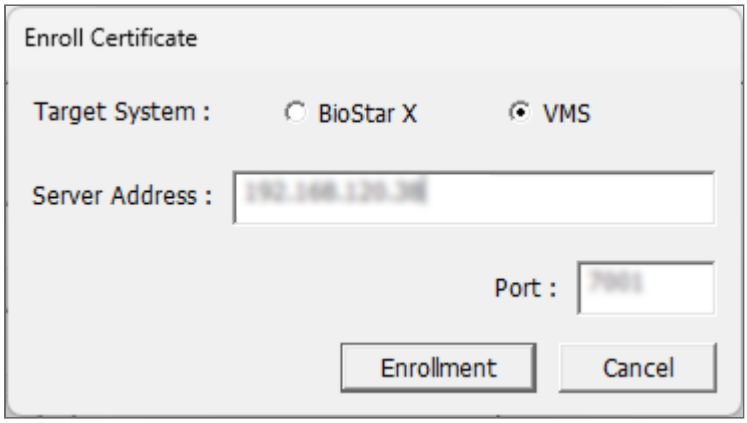
- Al acceder al **Sistema de Gestión de Video** (VMS) a través del navegador y aparece una advertencia "No es seguro"
- Cuando el video en tiempo real se reproduce en la página **Monitoring** pero el video grabado no se reproduce
- Al instalar el servidor VMS y **BioStar X** en el mismo servidor

Información

- Para obtener más información sobre cómo instalar el certificado en el servidor VMS, consulte Integrar VMS.
- La función para integrar con el servidor VMS debe comprarse por separado en un paquete de opciones adicional. Para obtener más información sobre la política de licencias, consulte Política de Licencias.

Instalar el certificado en la PC cliente

1. En una PC cliente **BioStar X**, descarga el instalador del certificado HTTPS (*cert-register.zip*) en la pantalla de inicio de sesión o en **Settings** → **System** → **HTTPS**.
2. Descomprima el archivo descargado y ejecute el archivo **cert-register.exe**. Se ejecuta el programa **Enroll Certificate**.
3. Seleccione **VMS** en **Target System** e ingrese la siguiente información.



   - **Server Address**: dirección IP del servidor VMS
   - **Port**: número de puerto del servidor VMS
4. Haga clic en **Inscripción**.
5. Verifique el mensaje de advertencia de seguridad y haga clic en **Yes**.

Reinicie el navegador web y verifique que el video grabado del servidor VMS se reproduzca normalmente en la página **Monitoring**.

Respaldo de Sistema

Realice copias de seguridad de información clave, como la base de datos de **BioStar X**, diversos ajustes y claves. Los archivos de copia de seguridad también incluyen configuraciones definidas por el usuario, como la clave de cifrado (enc key) y la ruta del registro de imágenes. Utilice la función **System Backup** para evitar la pérdida de datos en el servidor o al transferirlos a un nuevo equipo.

Los métodos de copia de seguridad compatibles son los siguientes.

- **Copia de seguridad manual**: El usuario crea el archivo de copia de seguridad manualmente.
- **Copia de seguridad automática**: El sistema crea archivos de copia de seguridad automáticamente en intervalos predefinidos.

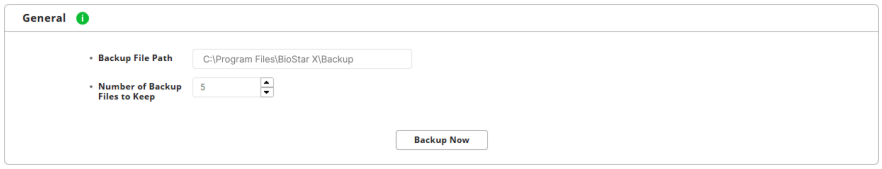
Información

- Al restaurar **BioStar X** desde un archivo de copia de seguridad creado en un equipo anterior a uno nuevo, vuelva a emitir la licencia.
- Si la base de datos de SQL Server y **BioStar X** están instalados en servidores diferentes, no se puede usar la copia de seguridad y restauración del sistema de **BioStar X**.
- Para obtener más información sobre la restauración del sistema, consulte Restauración del Sistema.

Copia de seguridad manual

Los usuarios pueden crear archivos de copia de seguridad de forma manual.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **System** → **System Backup** en la barra lateral izquierda.
3. En la sección **General**, configure la ruta para guardar el archivo de copia de seguridad y el número máximo de archivos de copia de seguridad.



   - **Backup File Path**: Ingrese la ruta donde se guardará el archivo de copia de seguridad. Ingrese una ruta de directorio que ya exista para la ubicación de guardado.
   - **Number of Backup Files to Keep**: Defina el número máximo de archivos de copia de seguridad.
4. Para crear un archivo de copia de seguridad, haz clic en **Backup Now**.
5. Si aparece un mensaje de advertencia, revíselo y haga clic en **Continue**.

Los archivos de copia de seguridad se guardan en formato *zip* en la ruta especificada en la opción **Backup File Path**. El nombre del archivo se genera con el formato `BioStar_X_Backup_YYYYMMDD_HHMMSS.zip`. Aquí, `YYYYMMDD` representa la fecha de la copia de seguridad y `HHMMSS` representa la hora.

Información

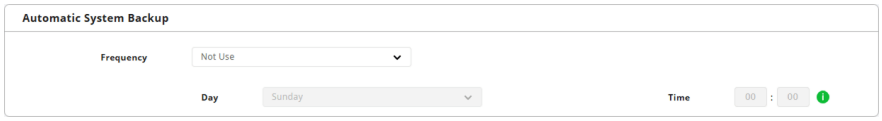
- Si se supera el número máximo de copias de seguridad, los archivos de copia de seguridad más antiguos se eliminan automáticamente.
- En **Number of Backup Files to Keep**, solo se ingresan números entre 1 y 100.

Configuración de copia de seguridad automática

Cuando configure la copia de seguridad automática, el sistema creará archivos de copia de seguridad en intervalos predefinidos.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **System** → **System Backup** en la barra lateral izquierda.

3. En la sección **Automatic System Backup**, seleccione la opción **Frequency**.



   - **Daily**: Realiza copias de seguridad diariamente de forma automática. Configure la hora de la copia de seguridad en la opción **Time**.
   - **Weekly**: Realiza copias de seguridad semanalmente de forma automática. Configure el día para la copia de seguridad automática en la opción **Day** y establezca la hora en la opción **Time**.
   - **Monthly**: Realiza copias de seguridad mensualmente de forma automática. Configure la fecha para la copia de seguridad automática en la opción **Date** y establezca la hora en la opción **Time**.

4. Haga clic en **Apply** para guardar la configuración.

Después de habilitar la copia de seguridad automática, las copias de seguridad se ejecutarán a intervalos regulares. Si falla una copia de seguridad automática, dicho fallo quedará registrado en el registro de eventos y en la pista de auditoría. La información detallada sobre la causa está disponible en los archivos de registro.

Los archivos de copia de seguridad se guardan en formato *zip* en la ruta especificada en la opción **Backup File Path** de la sección **General**. El nombre del archivo se genera con el formato `BioStar_X_Backup_YYYYMMDD_HHMMSS.zip`. Aquí, `YYYYMMDD` representa la fecha de la copia de seguridad y `HHMMSS` representa la hora.

> **Información**
>
> - Si selecciona la frecuencia de copia de seguridad automática como **Monthly** y establece la fecha en 29, 30 o 31, no se realizarán copias de seguridad automáticas en los meses que no tengan ese día.
> - La hora se basa en la zona horaria estándar configurada en **Preferences**. Para obtener más información sobre la configuración de la zona horaria, consulte Configurar Preferencias.

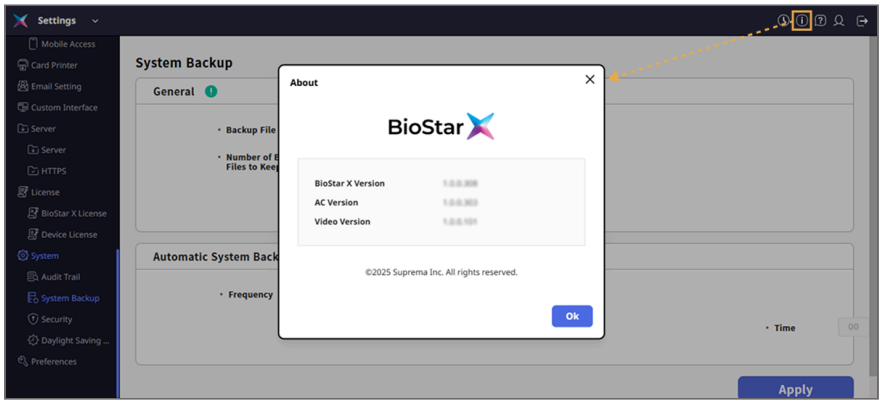
Restauración del Sistema

Use un archivo de copia de seguridad del sistema para restaurar cuando haya un problema con **BioStar X** o necesite volver a un estado anterior. La función de restauración permite devolver la base de datos, la configuración y la información de licencias al estado que tenían en el momento de la copia de seguridad.

Antes de comenzar

Antes de comenzar la restauración del sistema, verifique lo siguiente.

- La restauración no puede continuar si la versión de **BioStar X** en el momento de la copia de seguridad es diferente de la versión actual. Haga clic en ⓘ en la esquina superior derecha de la pantalla para comprobar la versión de **BioStar X**.



- Para comprobar la versión de **BioStar X** en el momento de la copia de seguridad, extraiga el archivo de copia de seguridad y verifique el valor `biostarVersion` en el archivo *sysbackup.conf*.
- Si la base de datos de SQL Server y **BioStar X** están instalados en servidores diferentes, no se puede usar la copia de seguridad y restauración del sistema de **BioStar X**.
- Si la dirección IP del servidor de destino de la restauración difiere de la del servidor de copia de seguridad:
  - **BioStar X v1.0.2 o posterior**: durante la restauración, BioStar X detecta la dirección IP del servidor de destino y reemite el certificado automáticamente en función de la nueva dirección IP. Una vez reemitido el certificado, los servicios que lo usan se vuelven a conectar automáticamente, por lo que no se requiere ninguna acción adicional.
  - **BioStar X v1.0.1 o anterior**: la restauración puede fallar. Verifique la dirección IP del servidor antes de continuar con la restauración.
- Aunque la clave de cifrado o la ruta del registro de imágenes hayan cambiado, la restauración seguirá las rutas de configuración actuales del **BioStar X** de destino. Si no se especifica una ruta personalizada, la restauración utilizará la ruta predeterminada del **BioStar X** de destino.
- Al realizar una restauración, los datos actuales se respaldan automáticamente. Si la restauración falla, puede volver al estado anterior a la restauración.

> **Información**
>
> Para obtener más información sobre cómo crear una copia de seguridad del sistema, consulte Respaldo de Sistema.

Restauración del Sistema

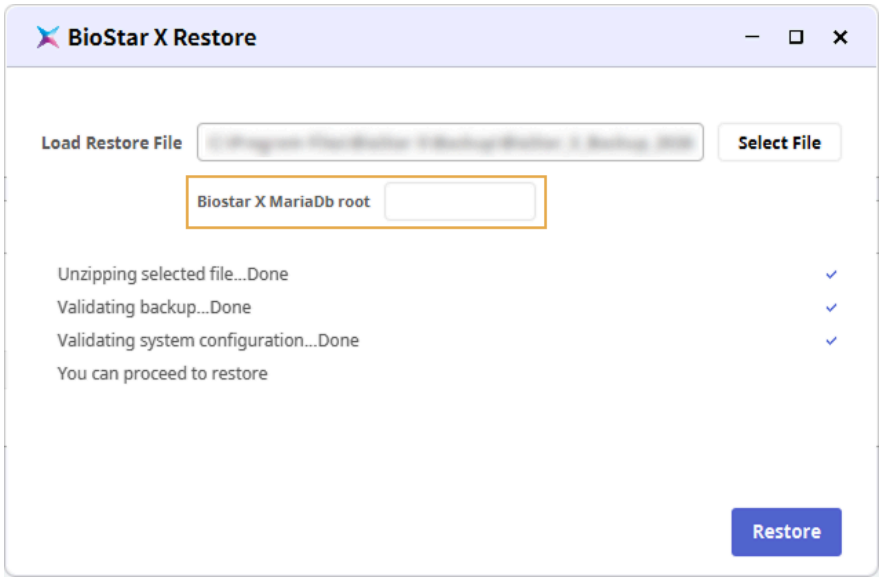
1. En Windows, ejecute Inicio → **BioStar X** → **BioStar X Restore**.

   > *Ruta del programa: C:\Program Files\BioStar X\biostar-restore.exe*

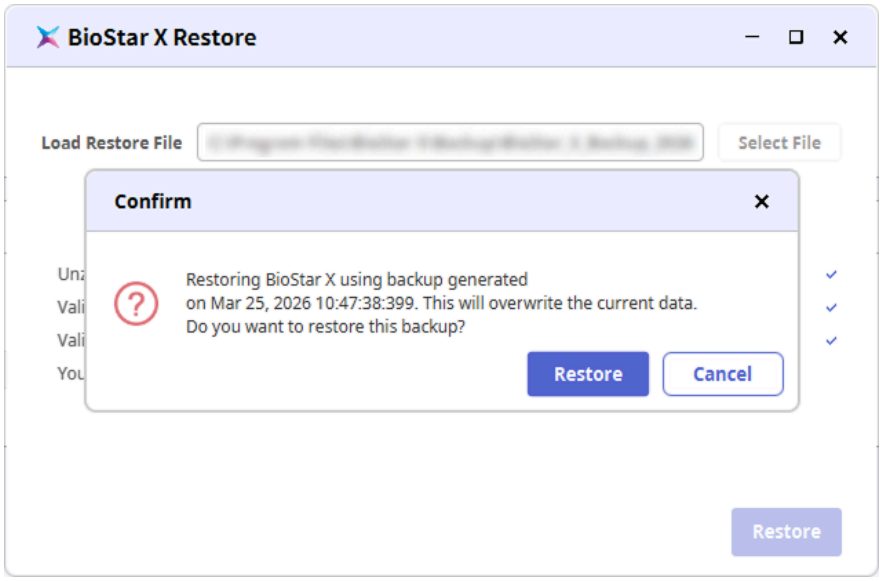
2. Haga clic en **Select File** y elija el archivo de copia de seguridad para restaurar.



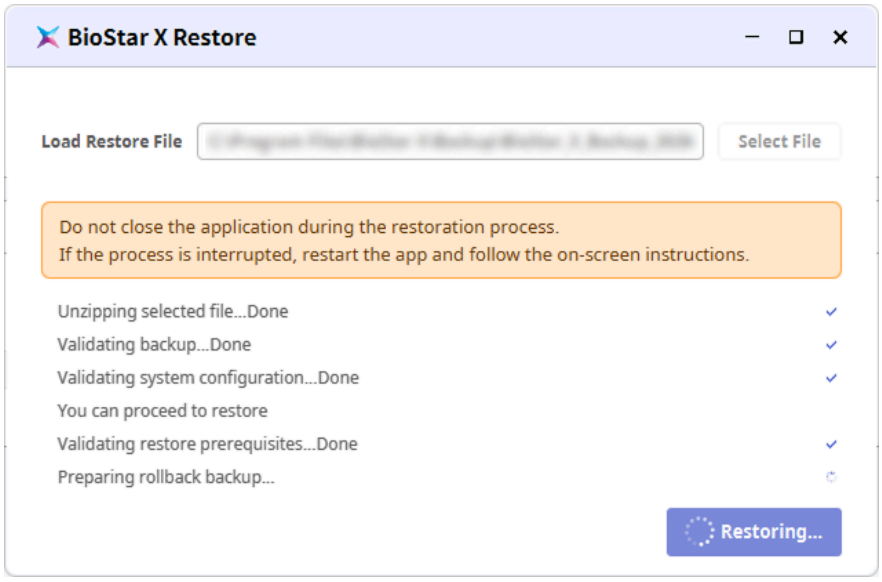
3. Haga clic en **Restore** para iniciar la restauración.
4. Valide el archivo de copia de seguridad.
5. Cuando aparezca el mensaje **Puede proceder con la restauración**, ingrese la contraseña de la base de datos y haga clic en **Restaurar**.



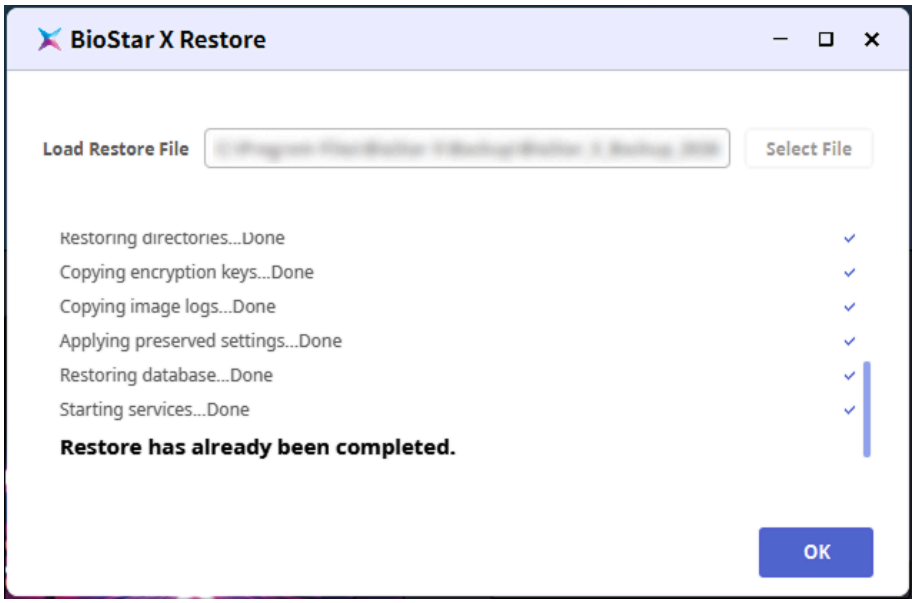
6. Haga clic en **Restaurar** para confirmar y continuar con la restauración.



7. Aparece un mensaje que muestra el progreso de la restauración. Espere a que se complete la restauración.



Si aparece el mensaje **La restauración ya se ha completado**, la restauración ya ha finalizado. Acceda a **BioStar X** para verificar los datos restaurados.



Información

- Si el PC se apaga inesperadamente durante la restauración, ejecute **BioStar X Restore** nuevamente para reintentar la restauración.
- Si la IP del servidor de restauración difiere de la IP del servidor de respaldo al usar un servidor de comunicaciones múltiples, vuelva a emitir el certificado. Para obtener más información sobre cómo volver a emitir el certificado del servidor de comunicaciones múltiples, consulte Cambiar la dirección IP del servidor principal.

Mejorar la Seguridad del Sistema

Configure los ajustes de seguridad de **BioStar X** según la política de seguridad de la organización. Configure de forma selectiva la política de contraseñas, el cifrado de datos personales, la seguridad de comunicación entre dispositivos y el control de accesos concurrentes.

Información

Verifique la política y las regulaciones de seguridad de la organización antes de mejorar la seguridad del sistema.

Usar la seguridad del sistema

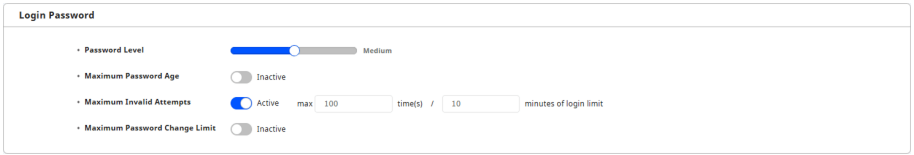
1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **System** → **Security** en la barra lateral izquierda.
3. Configure cada elemento relacionado con la seguridad.
   - **Login Password**: Configure el nivel de seguridad relacionado con la contraseña de inicio de sesión. Para obtener más información, consulte Configurar la política de contraseñas.
   - **Advanced Security Settings**: Mejore la seguridad de comunicación entre la información personal y los dispositivos. Para obtener más información, consulte Ajustes de seguridad avanzados.
   - **Session Security**: Mejore la seguridad de la sesión. Para obtener más información, consulte Control de acceso concurrente.
4. Haga clic en **Apply** en la parte inferior derecha de la pantalla para guardar los ajustes.

Información

Solo la primera cuenta de administrador con ID **1** puede usar el menú **Advanced Security Settings**.

Configurar la política de contraseñas

La sección **Login Password** establece el nivel de seguridad relacionado con la contraseña de inicio de sesión. Configure la política de contraseñas según los requisitos de seguridad de la organización.



Configurar la complejidad de la contraseña

Configure la complejidad de las contraseñas de los usuarios. Ajuste el control deslizante de la opción **Password Level** para definir el nivel de seguridad.

- **Low**: Permite ingresar hasta 32 caracteres.
- **Medium**: Al establecer una contraseña, se requiere una combinación de 8 a 32 caracteres alfabéticos (mayúsculas o minúsculas) y números.
- **Strong**: Al establecer una contraseña, se requiere una combinación de 10 a 32 caracteres alfabéticos (mayúsculas y minúsculas, con al menos una mayúscula), números y caracteres especiales.

Configurar el ciclo de cambio de contraseña

Para limitar el período de uso de las contraseñas, cambie el botón de la opción **Maximum Password Age** al estado **Active**. Los usuarios deben cambiar su contraseña periódicamente según lo establecido. Si se supera el ciclo de cambio de contraseña, aparecerá un mensaje solicitando el cambio durante el inicio de sesión.

> **Información**
> Puede configurarse de 1 a 180 días.

Configurar el límite de intentos fallidos de inicio de sesión

Configure la cantidad de intentos fallidos permitidos y el tiempo de restricción de inicio de sesión. Si se supera la cantidad de intentos definida en la opción **Maximum Invalid Attempts**, no podrá iniciar sesión durante un tiempo limitado después de ingresar una contraseña incorrecta.

> **Información**
> Esta opción está activada de forma predeterminada y restringe el inicio de sesión durante 10 minutos después de 100 intentos fallidos. Ajuste los valores o desactívelos según sea necesario.

Configurar el límite de cambio de contraseña

Para limitar la cantidad de cambios de contraseña que un usuario puede realizar en un día, cambie el botón de la opción **Maximum Password Change Limit** al estado **Active**. Los usuarios pueden cambiar la contraseña hasta el número especificado de veces.

> **Información**
> Puede configurarse hasta un máximo de 10 veces.

Ajustes de seguridad avanzados

En la sección **Advanced Security Settings**, puede mejorar la seguridad de la información personal y la comunicación entre dispositivos.



Información

La sección **Advanced Security Settings** se activa solo cuando inicia sesión con la cuenta inicial de administrador.

Mejorar la protección de datos personales

Para minimizar el riesgo de filtraciones de datos, configure las siguientes opciones para cifrar la información personal sensible.

- **Encrypt Personal Data on Database**
  - **Use**: Cifra y almacena los datos personales del usuario, incluidos los datos de credenciales.
  - **Not Use**: Almacena la información personal del usuario sin cifrado. Los datos que ya están cifrados se almacenarán descifrados y los nuevos datos no se cifrarán.
- **Personal Data Encryption Key**: Se utiliza para cifrar o descifrar la información almacenada en la base de datos y proteger de forma segura la información personal del usuario. Haga clic en **Change** y establezca un nuevo valor de clave de cifrado. Cambiar la clave de cifrado vuelve a cifrar los datos que previamente estaban cifrados.

Información

- No inicie el servidor de forma forzada durante el proceso de cifrado o descifrado de la base de datos de datos personales. Pueden producirse errores como fallos de inicio de sesión o corrupción de datos. Puede tardar cierto tiempo según el tamaño de la base de datos y el rendimiento del servidor.

  ▼ Ver los elementos de cifrado de datos personales

  - Imagen de perfil
  - ID Usuario
  - Nombre
  - Número de teléfono
  - USER IP
  - Información de correo electrónico del remitente y de los destinatarios
  - ID Inicio Sesión
  - Contraseña de inicio de sesión
  - Plantilla de rostro
  - Plantilla de huella dactilar
  - ID Tarjeta
  - Clave de layout de tarjeta inteligente
  - Información personalizada para usuario y visitante
  - Archivos de registros de imágenes
- Puede introducir **Personal Data Encryption Key** utilizando caracteres alfanuméricos y símbolos, para un total de 32 caracteres.
- Después de actualizar a la versión 1.0.3, el sistema cifra los nuevos registros de auditoría sin importar la opción **Encrypt Personal Data on Database**.

Configurar la comunicación segura entre dispositivos

Proteja la comunicación entre el servidor **BioStar X** y los dispositivos de control de acceso con certificados para mejorar la seguridad. Un sistema **BioStar X** recién instalado establece la opción **Secure communication with device** en **Use** de forma predeterminada. No requiere pasos adicionales de activación. Al actualizar un sistema existente, mantiene los ajustes anteriores, reutiliza el certificado de seguridad y vuelve a conectar los dispositivos inscritos.

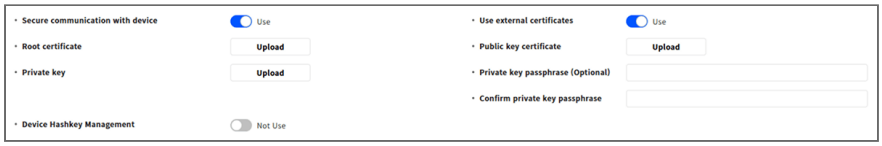
- **Secure communication with device**: Proteja la comunicación entre el servidor **BioStar X** y los dispositivos de control de acceso con certificados. Si establece esta opción en **Use**, el servidor genera automáticamente un certificado, lo envía a los dispositivos y cifra toda la comunicación a partir de entonces. Los dispositivos usan este certificado para establecer un canal seguro al intercambiar datos con el servidor **BioStar X**.

  Para usar un certificado externo, establezca la opción **Use external certificates** en **Use** y registre lo siguiente.

  – Cargue los archivos **Root certificate**, **Public key certificate** y **Private key** por separado.

  – Si la clave privada tiene una frase de contraseña, escriba el mismo valor en **Private key passphrase (Optional)** y **Confirm private key passphrase**. (Opcional)

  > Para restaurar el certificado de seguridad respaldado durante la eliminación del servidor, cópielo directamente en la ruta de instalación de **BioStar X**. Para obtener instrucciones para respaldar y restaurar certificados de seguridad, consulte Desinstalar El Servidor BioStar X Y Restaurar Certificados De Seguridad.



- **Device Hashkey Management**: Administre manualmente la clave hash aplicada a los dispositivos. Establezca esta opción en **Use** para verificar y cambiar el valor de **Device Hashkey**. Haga clic en **Change** y establezca un nuevo valor de clave hash.

> **Precaución**
>
> Antes de habilitar la opción **Device Hashkey Management**, verifique lo siguiente.
>
> - Al habilitarla, el dispositivo elimina datos de usuario, registros y claves de cifrado cuando ocurre un evento de manipulación (Tamper), para mejorar la seguridad; úsela con precaución.
> - Si un usuario distinto de la cuenta Administrator Role tiene una contraseña o un PIN, el sistema no puede aplicar la clave hash. Elimine la contraseña o el PIN de inicio de sesión y vuelva a intentarlo. El sistema cifra las contraseñas y los PIN de forma irreversible para cumplir los requisitos de seguridad.
> - Cambiar la clave hash del dispositivo elimina la información del PIN del administrador principal almacenada en el dispositivo. Tenga especial cuidado, porque eliminar credenciales puede impedir el acceso al menú Administrador de dispositivos.
> - Los ajustes **Encrypt Personal Data on Database** y **Device Hashkey Management** no se pueden habilitar al mismo tiempo. Deshabilite una de las dos opciones y luego establezca la otra.

Información

- **BioStar X** conserva el certificado predeterminado generado por el servidor después de cambiar **Secure communication with device** a **Not Use**. Al volver a cambiar la opción a **Use**, el sistema reutiliza el certificado existente. Crea uno nuevo solo si no existe ninguno. Cambiar **Use** → **Not Use** → **Use** conserva el mismo certificado. Los dispositivos agregados previamente vuelven a conectarse sin pasos adicionales. Al cambiar a **Not Use** mientras se usa un certificado externo, el sistema elimina el certificado externo (certificado raíz, certificado de clave pública y clave privada) del servidor. También elimina la contraseña de la clave privada del servidor.
- Cambie **Secure communication with device** y **Use external certificates** solo cuando todos los dispositivos agregados y el servidor de multicomunicación estén conectados al servidor. Si un dispositivo se desconecta o el servidor de multicomunicación no está conectado, el sistema rechaza el cambio y muestra un mensaje de error. Vuelva a conectar el dispositivo o el servidor de multicomunicación, luego intente de nuevo. Si ya no usa el dispositivo, elimínelo de la lista de dispositivos y vuelva a intentarlo.
- Si un dispositivo conectado anteriormente no se conecta por una discrepancia de certificado, **BioStar X** lo registra en el registro del sistema. Si el dispositivo deja de conectarse de repente, revise el registro del sistema. Luego, inicialice el dispositivo o vuelva a inscribir el conjunto de certificados exportado con **Use external certificates**. Si elimina y vuelve a instalar el servidor, consulte Desinstalar El Servidor BioStar X Y Restaurar Certificados De Seguridad.
- Para ver instrucciones para respaldar los certificados al eliminar un servidor, consulte Desinstalar El Servidor BioStar X Y Restaurar Certificados De Seguridad.

▼ Ver los dispositivos y versiones de firmware compatibles con la función Secure communication with device

- Firmware de BioStation 3 Max, versión 1.0.0 o posterior
- Firmware de XPass Q2, versión 1.0.0 o posterior
- BioStation 3 firmware 1.0.0 o superior
- BioStation 2a firmware 1.0.0 o superior
- X-Station 2 versión de firmware 1.0.0 o superior
- Firmware de XPass 2 1.0.0 o posterior
- Firmware de FaceLite 1.0.0 o posterior
- Firmware de BioLite N2 1.0.0 o posterior
- BioEntry P2 FW 1.1.0 o posterior
- FaceStation 2 FW 1.1.0 o posterior
- BioEntry W2 FW 1.2.0 o posterior
- BioStation L2 FW 1.3.0 o posterior
- BioStation A2 FW 1.5.0 o posterior
- BioStation 2 FW 1.6.0 o posterior
- CoreStation FW 1.1.0 o posterior

Control de acceso concurrente

En la sección **Session Security**, limite los inicios de sesión duplicados para la misma cuenta para mejorar la seguridad. Establezca la opción **Simultaneous Connection Allow** en **Inactive**. Cuando haya intentos de inicio de sesión concurrentes para la misma cuenta, se cerrará la sesión de los usuarios existentes.



Horario de Verano (DST)

Establece el horario de verano (DST) para ajustar automáticamente la hora del sistema a la hora legal local. Esto garantiza la precisión de los registros de acceso y evita problemas de sincronización horaria con otros sistemas.

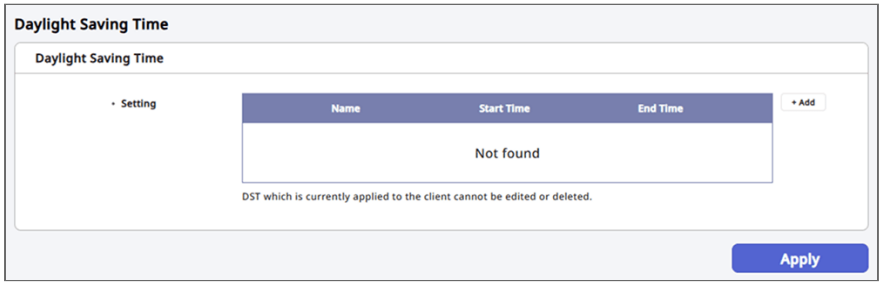
Información

Configura el horario de verano en los siguientes casos.

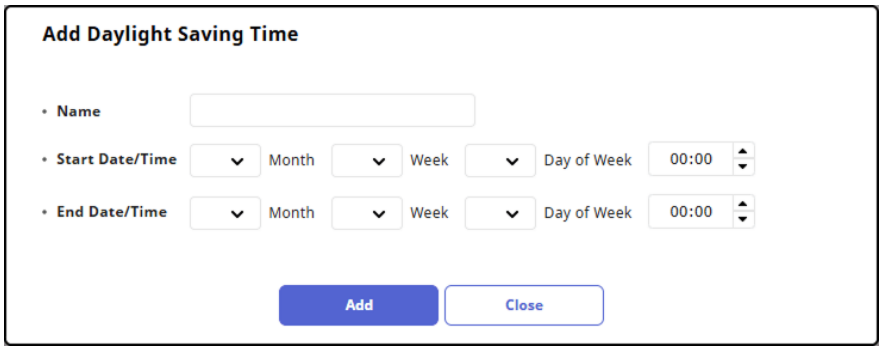
- Si operas el sistema en países o regiones que adoptan el horario de verano
- Si necesitas registrar horarios de acceso precisos integrados con sistemas de gestión de asistencia
- Si administras un sistema de seguridad consolidado que funciona en múltiples zonas horarias

Agregar horario de verano

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **System** → **Daylight Saving Time** en la barra lateral izquierda.
3. Haz clic en **+ Add**.



4. Configura cada elemento y haz clic en **Add**.



5. Haz clic en **Apply** en la esquina inferior derecha de la pantalla para guardar los ajustes añadidos.

Información

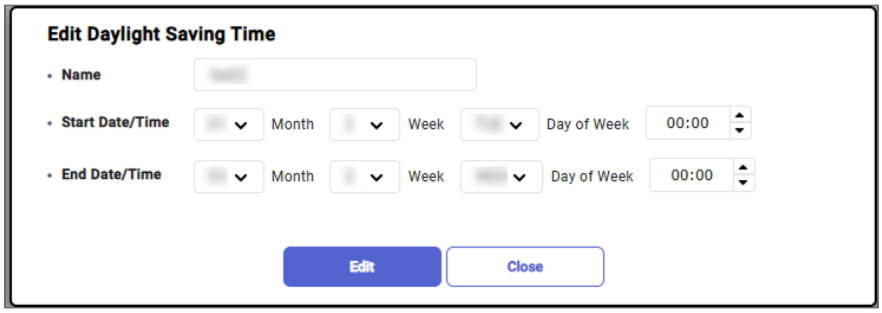
- Los ajustes actuales de horario de verano no se pueden modificar ni eliminar. Consulta los ajustes actuales de horario de verano en el menú **Settings** → **System** → **Preferences**.
- Para obtener más información sobre cómo aplicar al sistema los ajustes de horario de verano recién añadidos, consulte Configurar Preferencias.

Editar horario de verano

Información

Los ajustes en uso actualmente no se pueden modificar. Para modificarlos, primero desmarca la selección en la sección **Language / Time Zone** del menú **Settings** → **System** → **Preferences**.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **System** → **Daylight Saving Time** en la barra lateral izquierda.
3. Haz clic en el botón del elemento que deseas modificar en la lista de horario de verano.
4. Cuando aparezca la ventana **Edit Daylight Saving Time**, modifica el elemento deseado.



5. Al finalizar la edición, haz clic en **Edit**.
6. Haz clic en **Apply** en la esquina inferior derecha de la pantalla para guardar los ajustes modificados.

Información

Para obtener más información sobre cómo aplicar los ajustes de horario de verano al sistema, consulte Configurar Preferencias.

Borrar horario de verano

Borra los ajustes de horario de verano que no se utilizan.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **System** → **Daylight Saving Time** en la barra lateral izquierda.
3. Haz clic en el botón del elemento que deseas borrar en la lista de horario de verano.
4. Cuando aparezca el mensaje de confirmación, haz clic en **Yes**.

5. Haz clic en **Apply** en la esquina inferior derecha de la pantalla para guardar la eliminación de ajustes.

Configuración de Correo Electrónico

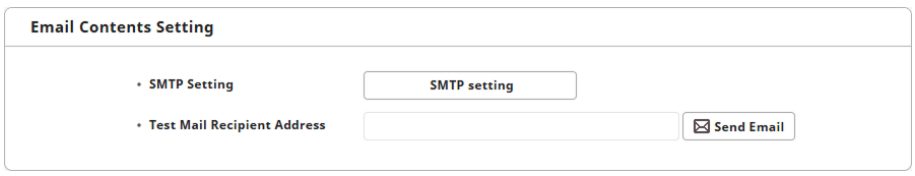
Configure información como la línea de asunto del correo electrónico que enviará el enlace móvil para el enrolamiento facial, el nombre de la empresa, el logotipo de la empresa y los datos de contacto.

> **Información**
>
> - Registre la dirección de correo electrónico del usuario en la información del usuario para enviar el enlace móvil de enrolamiento facial o para emitir un QR/código de barras. Para obtener más información sobre los datos del usuario, consulte Ingresar Información Básica del Usuario.
> - Los dispositivos que pueden realizar **autenticación facial** son los siguientes.
>   - FaceStation F2, BioStation 3, BioEntry W3, BioStation 3 Max
> - Los dispositivos que incluyen **soporte para autenticación QR/Barcode mediante escáner** son los siguientes.
>   - X-Station 2 (XS2-QDPB, XS2-QAPB)
> - Los dispositivos que incluyen **soporte para autenticación QR/Barcode mediante cámara** son los siguientes.
>   - Firmware de BioStation 3 Max, versión 1.0.0 o posterior
>   - Versión de firmware 1.1.0 o posterior para BioStation 3
>   - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) versión de firmware 1.2.0 o superior
>   - X-Station 2 (XS2-QDPB, XS2-QAPB) versión de firmware 1.4.1 o superior
> - Usar **Use QR/Barcode through Camera** requiere una licencia de dispositivo independiente. Para obtener más información sobre las licencias de dispositivos, consulte Licencia de dispositivo.

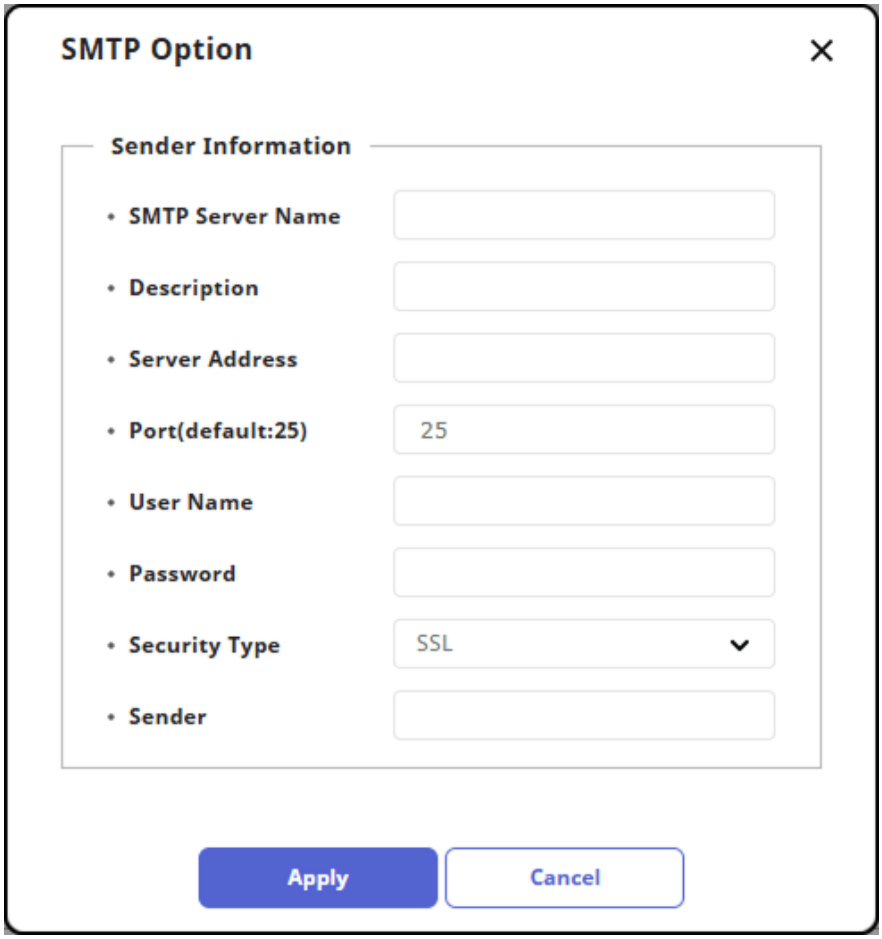
1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **System** → **Email Settings** en la barra lateral izquierda.
3. Edite los campos necesarios.
4. Haga clic en **Apply** para guardar la configuración.

Configurar contenido del correo electrónico

Ingrese la información del servidor SMTP para enviar correos electrónicos.



- **SMTP Setting**: Configure el SMTP (Simple Mail Transfer Protocol) para enviar correos electrónicos. Haga clic en **SMTP setting** para abrir la ventana de configuración de **SMTP Setting**.



- **SMTP Server Name**: Ingrese el nombre del servidor SMTP.
- **Description**: Ingrese la descripción.
- **Server Address**: Ingrese la dirección del servidor SMTP. La dirección del servidor SMTP usa el formato `smtp.{email-service-provider}.com`. Confírmela en la pantalla de ajustes del correo electrónico utilizado como servidor SMTP.
- **Port(default:25)**: Ingrese el número de puerto del servidor SMTP. Confírmela en la pantalla de ajustes del correo electrónico utilizado como servidor SMTP.
- **User Name**: Ingrese la cuenta del servicio SMTP.
- **Password**: Ingrese la contraseña del servicio SMTP.
- **Security Type**: Seleccione el tipo de seguridad.
- **Sender**: Ingrese la dirección de correo electrónico del remitente.

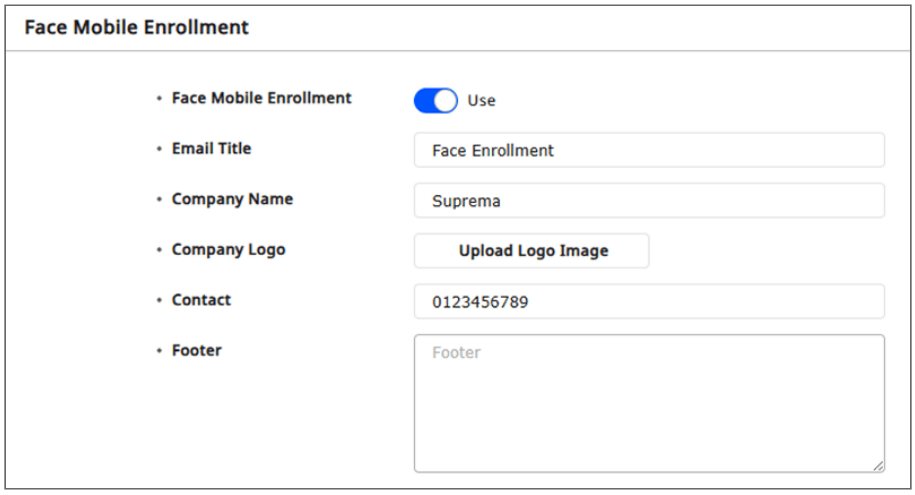
Información

- Para obtener más información sobre SMTP, contacte al administrador del sistema.
- Al usar el servidor SMTP como cuenta de correo con autenticación de dos factores y cambiar la contraseña de la cuenta, tenga en cuenta lo siguiente: Una vez que configure la autenticación de dos factores, la contraseña SMTP es la misma que la contraseña de la aplicación generada mediante la autenticación de dos factores, no la contraseña de la cuenta de correo.
  - Al configurar la autenticación en dos pasos, la contraseña SMTP usa la contraseña de aplicación generada por la autenticación en dos pasos, no la contraseña de la cuenta de correo.
  - En ese momento, si se cambia la contraseña de la cuenta de correo, la contraseña de la aplicación se elimina automáticamente y la contraseña SMTP deja de estar disponible.
  - Al cambiar la contraseña de la cuenta de correo, genere nuevamente la contraseña de la aplicación y luego configure otra vez la contraseña SMTP.

- **Test Mail Recipient Address**: Para comprobar si existen problemas con la configuración SMTP, ingrese la dirección de correo electrónico que recibirá el mensaje y haga clic en **Send Email**.

Configurar enlace móvil para el enrolamiento facial

Establezca en **Use** para enviar al usuario un enlace móvil de enrolamiento facial por correo electrónico.



- **Email Title**: Ingrese la línea de asunto del correo electrónico para enviar el enlace móvil de enrolamiento facial.
- **Company Name**: Ingrese el nombre de la empresa.
- **Company Logo**: Cargue la imagen del logotipo de la empresa.

Información

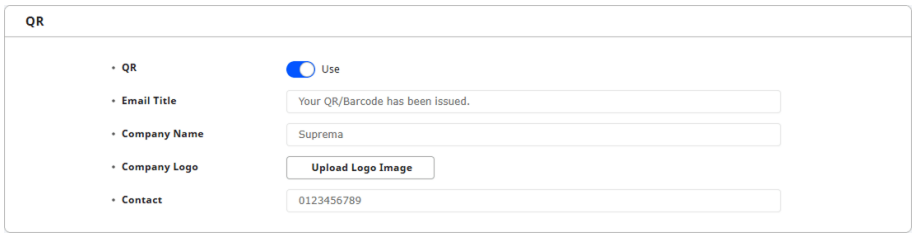
- Los formatos de archivo de imagen admitidos son GIF, JPG, JPEG, JPE, JFIF, PNG.
- El tamaño de archivo de imagen soportado es de hasta 5MB.

- **Contact**: Ingrese la información de contacto de la persona responsable.
- **Footer**: Ingrese el contenido que se notificará a los usuarios que se enrolen con su rostro, como avisos legales. Se mostrará en la parte inferior del correo electrónico enviado con el enlace móvil para el enrolamiento facial.

> **Información**
> El pie de página puede tener hasta 5,000 caracteres.

Configuración de QR/código de barras

Para usar el QR/código de barras, configúrelo en **Use**.



- **Email Title**: Ingrese el título del correo electrónico.
- **Company Name**: Ingrese el nombre de la empresa.
- **Company Logo**: Cargue la imagen del logotipo de la empresa.

> **Información**
> – Los formatos de archivo de imagen admitidos son GIF, JPG, JPEG, JPE, JFIF, PNG.
> – El tamaño de archivo de imagen soportado es de hasta 5MB.

- **Contact**: Ingrese la información de contacto de la persona responsable.

Configurar Preferencias

Para utilizar **BioStar X** de manera eficaz, son necesarios los ajustes adecuados para su entorno de uso. A continuación se indican los ajustes necesarios para diversas situaciones.

- Ajustes iniciales para el recién instalado **BioStar X**
- Cambiar al idioma preferido
- Configurar la hora según la zona horaria local
- Personalizar el sonido de notificación de eventos

Accede a preferencias

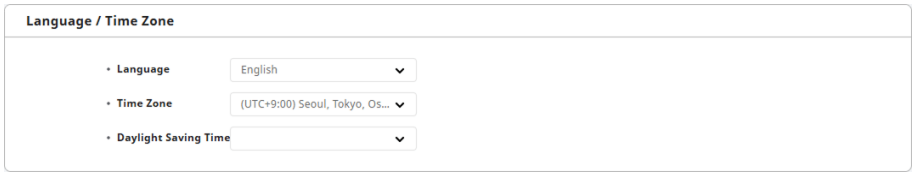
1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **System** → **Preferences** en la barra lateral izquierda.
3. Configure las opciones deseadas en cada sección.
   - **Language / Time Zone**: Idioma de la interfaz y zona horaria, horario de verano
   - **Date/Time**: Formato de fecha y hora

- **Sound**: Sonido de notificación de eventos

4. Después de completar todos los ajustes, haga clic en **Apply** en la parte inferior derecha de la pantalla.

Configura el idioma y la zona horaria

Puede configurar el idioma de la interfaz de **BioStar X**, la zona horaria y las reglas de horario de verano.



- **Language**: Seleccione el idioma de la interfaz que desea usar.
- **Time Zone**: Seleccione la zona horaria que corresponde a su ubicación actual.
- **Daylight Saving Time**: Elija las reglas de horario de verano que se aplicarán al servidor **BioStar X**. Si el elemento que busca no está disponible, consulte Horario de Verano (DST) para obtener instrucciones sobre cómo añadirlo.

Haga clic en **Apply** en la parte inferior derecha de la pantalla para guardar los ajustes.

Configura el formato de fecha y hora

Puede configurar el formato de visualización de fecha y hora que se utilizará en todo el sistema.



- **Date Format**: Cambia el formato de fecha.
  - **mm/dd/yyyy**: 01/31/2025
  - **yyyy/mm/dd**: 2025/01/31
  - **dd/mm/yyyy**: 31/01/2025
- **Time Format**: Cambia el formato de hora.
  - **hh:mm**: 23:59, formato de 24 horas
  - **hh:mm a**: 11:59 PM, formato de 12 horas
  - **a hh:mm**: PM 11:59, formato de 12 horas

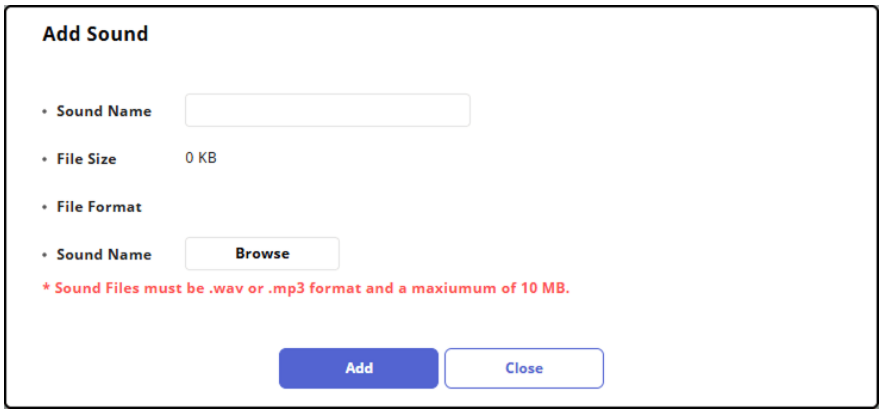
Haga clic en **Apply** en la parte inferior derecha de la pantalla para guardar los ajustes.

Configura el sonido de notificación de eventos

Puede cargar un archivo de sonido que se utilizará cuando ocurra un evento.



1. Haga clic en **+ Add**.
2. Cuando aparezca la ventana **Add Sound**, haga clic en **Browse**.



3. Seleccione el archivo *.wav* o *.mp3* que desea cargar y haga clic en **Abrir**.
4. Haz clic en **Add** para cargar el archivo de sonido.

Haga clic en **Apply** en la parte inferior derecha de la pantalla para guardar los ajustes.

Información

- Solo se pueden cargar archivos de sonido en formato *.wav* o *.mp3*.
- El tamaño máximo del archivo es 10MB.
- Para saber cómo aplicar el archivo de sonido cargado cuando se produzca un evento, consulte Configuración de Alertas.

Configuración Avanzada

Proporciona orientación sobre la funcionalidad de ajustes avanzados disponible con una licencia **Essential** al comprar opciones adicionales, o con una licencia **Enterprise** o superior.

Administrar Ascensores

Esta guía describe cómo agrupar, registrar y administrar ascensores. Controle los derechos de acceso a pisos específicos mediante la configuración de control de acceso relacionada con los ascensores. Esto mejora la seguridad y la comodidad.

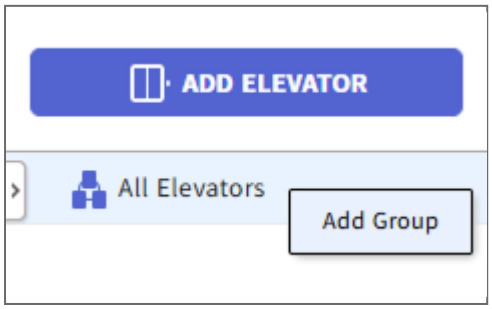
Administrar Grupo de Ascensores

Esta guía describe cómo configurar grupos para administrar varios elevadores fácilmente. Un grupo de ascensores es una función que permite gestionar varios ascensores como una sola unidad. Si configura un grupo, puede configurar varios ascensores al mismo tiempo.

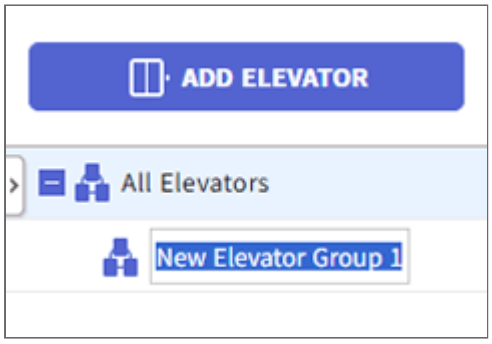
> **Consejo**
> Registrar el nombre del grupo según la ubicación del elevador facilita la administración.

Agregar grupo de elevadores

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Elevator** en la barra lateral izquierda.
3. Selecciona **All Elevators** en la lista de elevadores y haz clic con el botón derecho.



4. Haga clic en **Add Group** en el menú emergente.
5. Introduzca el nombre de grupo deseado.

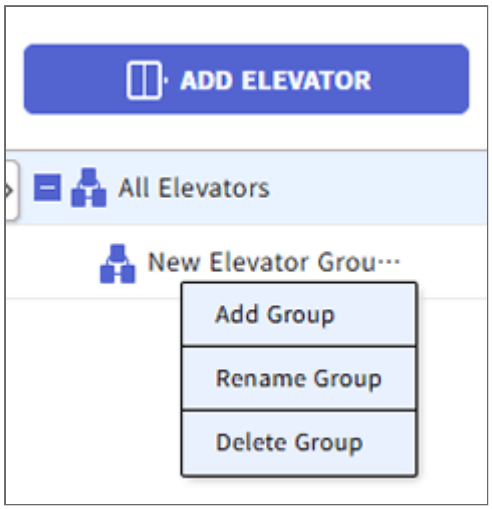


Información

- Se pueden crear como máximo 8 niveles para los grupos de elevadores.
- El nombre del grupo de elevadores puede tener hasta 48 caracteres.

Cambiar nombre del grupo de elevadores

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Elevator** en la barra lateral izquierda.
3. Selecciona el grupo cuyo nombre deseas cambiar de la lista de elevadores y haz clic con el botón derecho.



4. Haga clic en **Rename Group** en el menú emergente.
5. Ingrese el nuevo nombre del grupo.

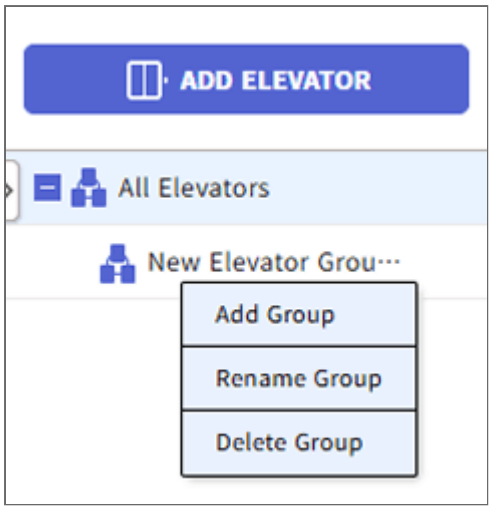
Información

El nombre del grupo de elevadores puede tener hasta 48 caracteres.

Eliminar grupo de elevadores

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Elevator** en la barra lateral izquierda.

3. Selecciona el grupo que deseas eliminar de la lista de elevadores y haz clic con el botón derecho.



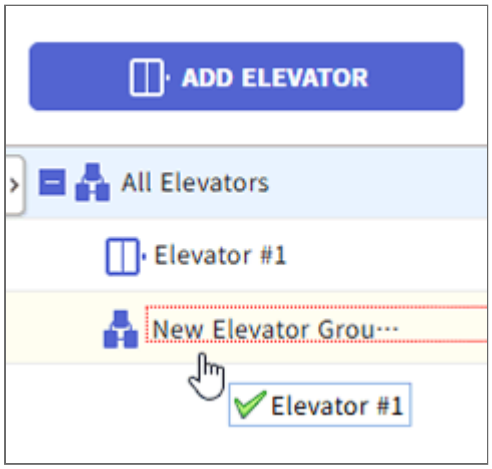
4. Haga clic en **Delete Group** en el menú emergente.

> **Precaución**
> Eliminar un grupo de elevadores quitará todos los elevadores incluidos en el grupo. Para evitar eliminar elevadores, muévelos primero a otro grupo antes de eliminar el grupo.

Agregar elevador al grupo

Agregar desde la lista de elevadores

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Elevator** en la barra lateral izquierda.
3. Selecciona el elevador que deseas agregar al grupo en la lista de elevadores y arrástralo al grupo deseado.



El elevador seleccionado se mueve al grupo.

Agregar desde la información del elevador

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Elevator** en la barra lateral izquierda.

3. Haz clic en el elevador que deseas agregar al grupo en la lista de elevadores del lado derecho.
4. Cuando aparezca la pantalla de modificación de la información del elevador, haz clic en la opción **Group** en la sección **Information**.



5. Seleccione el grupo deseado.
6. Haga clic en **Apply** en la parte inferior de la pantalla.

Registrar Ascensor

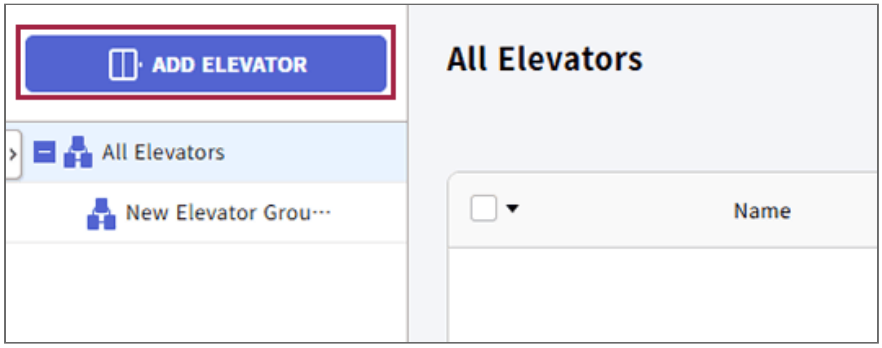
Este documento ofrece orientación sobre cómo registrar y configurar un ascensor. El ascensor se utiliza para el control de pisos y forma parte del sistema de control de acceso junto con la puerta de entrada. Registrar el ascensor permite controlar los permisos de acceso para pisos específicos.

Antes de comenzar

- Configure el nivel de acceso, el grupo de acceso y el nivel de piso para el control de acceso antes de registrar el ascensor. Para obtener más información, consulte Configuración de Control de Acceso.
- Registre el dispositivo antes de registrar el ascensor. Para obtener más información sobre el registro de dispositivos, consulte lo siguiente.
  - Registrar dispositivo
  - Registrar Credenciales Wiegand
  - Registrar Esclavo

Registrar ascensor

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Elevator** en la barra lateral izquierda.
3. Haz clic en **ADD ELEVATOR** en la parte superior izquierda de la pantalla.



4. Cuando aparezca la pantalla **Add New Elevator**, configure cada elemento de la sección en orden.
   - **Information**: Configure la información básica del ascensor. Para obtener más información, consulte Configurar información básica.
   - **Detail**: Configure la información detallada del ascensor. Para obtener más información, consulte Configurar

información detallada.

- **Option**: Configure opciones adicionales. Para obtener más información, consulte Configurar opciones adicionales.
- **Alarm**: Configure la alarma para activar o bloquear el uso del dispositivo cuando ocurra una violación de anti-passback. Para obtener más información, consulte Configurar alarmas.

5. Una vez completados todos los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.

Configurar información básica

En la sección **Information**, ingrese o cambie el nombre, el grupo y la descripción del ascensor.

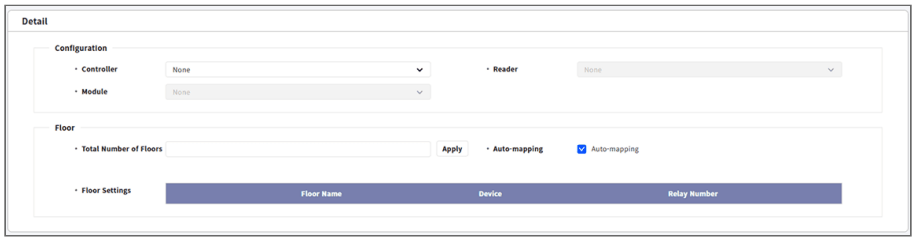


- **Name**: Ingrese el nombre del ascensor. Es conveniente ingresar un nombre que especifique la ubicación del ascensor para facilitar la gestión.
- **Group**: Seleccione el grupo del ascensor.
- **Description**: Ingrese una descripción breve del ascensor.

> **Información**
>
> - El nombre del ascensor puede tener hasta 48 caracteres.
> - Para obtener más información sobre cómo registrar grupos de ascensores, consulte Administrar Grupo de Ascensores.

Configurar información detallada

En la sección **Detail**, configure la información detallada del ascensor, como los dispositivos conectados al ascensor y la información de los pisos. Configure la información de dispositivos y pisos para conectarlos al ascensor.



- **Controller**: Seleccione el dispositivo que controlará los permisos de acceso del ascensor.
- **Reader**: Seleccione el dispositivo que se utilizará para la autenticación.
- **Module**: Seleccione el dispositivo que controlará el relé del botón del ascensor.
- **Total Number of Floors**: Ingrese el número total de pisos a los que el ascensor puede acceder. Ingrese hasta 192 pisos.
- **Auto-mapping**: Seleccione si desea usar el mapeo automático. El mapeo automático asigna números de relé de forma secuencial.
- **Floor Settings**: Configure los nombres de los pisos y los números de relé que los controlarán.

Información

- Solo se pueden seleccionar dispositivos maestro para la opción **Controller**.
- Para la opción **Reader**, solo se pueden seleccionar dispositivos maestro, dispositivos esclavo y dispositivos Wiegand, con un máximo de 4 selecciones permitidas.

  El modelo OM-120 no se puede configurar como lector.
- Para la opción **Module**, solo se pueden seleccionar los modelos OM-120, DM-20, IM-120 y SIO2.

Configurar opciones adicionales

En la sección **Option**, configure las opciones adicionales del ascensor.



- **Relay Control**: Configure las opciones para el relé del botón de piso.
  - **Open Time**: Configure el tiempo durante el cual el botón de piso permanece activo después de completar la autenticación. Después de este tiempo, el relé no activará el botón de piso.
- **Dual Authentication**: Configure para que dos personas (un usuario general y un administrador) deban autenticar sus credenciales para activar el botón de piso.
  - **Device**: Selecciona el dispositivo que se usará para la autenticación dual. Para no usar autenticación dual, seleccione **None**.
  - **Schedule**: Selecciona el horario para usar la autenticación dual. Si el horario deseado no está disponible, haz clic en **+ Add Schedule** para agregar uno.
  - **Approval Type**: Define el orden de la autenticación del administrador.
  - **None**: Se requieren dos autenticaciones sin importar el grupo de autenticación.
  - **Last**: El usuario general debe autenticarse primero, seguido de un usuario autenticado incluido en el grupo de autenticación establecido.
  - **Approval Group**: Define el grupo al que pertenece el administrador. Esta opción está disponible cuando **Approval Type** se establece en **Last**.
  - **Timeout**: Define el tiempo de espera entre la primera y la segunda autenticación. Si la segunda autenticación no se completa dentro del tiempo establecido, el botón de piso no se activará.

> **Información**
>
> – Modifique los ajustes en el siguiente menú para cambiar la autenticación dual del dispositivo configurado para los ajustes de límite de ocupación. **Settings** → **Access Management** → **Advanced AC** → **Occupancy Limit**
>
> Para obtener más información sobre la configuración de **Occupancy Limit**, consulte Configuración Avanzada de Control de Acceso.
>
> – Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

- **Tamper**: Configure el puerto para emitir la señal de sabotaje.

Configurar alarmas

En la sección **Alarm**, configure las acciones a realizar cuando se detecten entradas de sabotaje o señales de entrada independientes. Haz clic en **+ Add** para agregar condiciones de trabajo y acciones.



- **Trigger**: Configure la detección de entradas de sabotaje o señales de entrada independientes.
- **Action**: Configure las acciones a realizar según las condiciones establecidas. Active todos los botones de piso del ascensor u emita señales específicas.

Editar Información del Ascensor

Esta guía describe cómo editar la información de configuración del ascensor registrado. Cambie la configuración detallada de ascensores individuales o seleccione varios ascensores para aplicar cambios masivos a elementos comunes.

Editar información de un ascensor

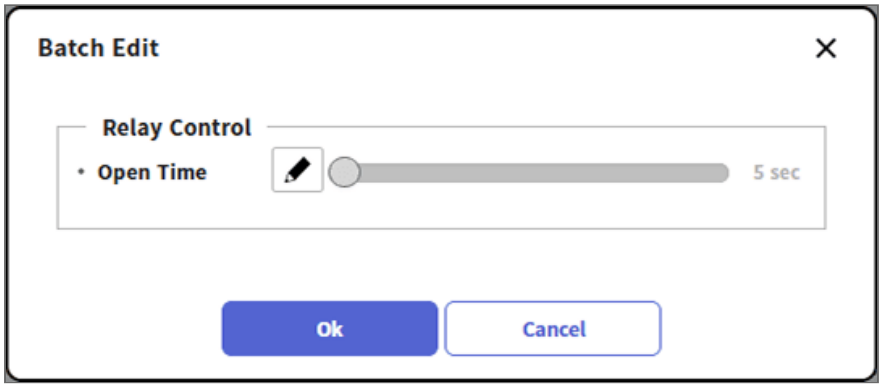
1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Elevator** en la barra lateral izquierda.
3. Haga clic en el ascensor que desea editar en la lista de ascensores.
4. Modifique los detalles en cada sección.
5. Una vez completados todos los ajustes, haga clic en **Apply** en la parte inferior de la pantalla.

> **Información**
>
> Para obtener más información sobre cada sección de la pantalla Editar información del ascensor, consulte Registrar Ascensor.

Editar varios ascensores por lotes

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Elevator** en la barra lateral izquierda.

3. Marque las casillas de los ascensores que desea editar en la lista de ascensores. Seleccione dos o más ascensores.
4. Haga clic en **Batch Edit** en la parte superior derecha de la pantalla.
5. Cuando aparezca la ventana **Batch Edit**, configure las opciones deseadas.



6. Después de completar todas las configuraciones, haga clic en **Apply**.

> **Información**
>
> - **Batch Edit** se activará solo cuando se seleccionen dos o más ascensores de la lista de ascensores.
> - En la edición por lotes, modifique solo la opción **Open Time**.

Borrar Ascensor

Esta guía describe cómo eliminar ascensores registrados.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Point** → **Elevator** en la barra lateral izquierda.
3. Haz clic en la casilla de verificación del ascensor que deseas eliminar de la lista de ascensores.
4. Haz clic en **Delete Elevator** en la esquina superior derecha de la pantalla.

El ascensor seleccionado se eliminará. Los ascensores eliminados no se pueden recuperar.

> **Información**
>
> Selecciona uno o más ascensores en la lista de ascensores para activar **Delete Elevator**.

Configuración Avanzada de Control de Acceso

Controle el acceso mediante la configuración avanzada de control de acceso. Configure diversas funciones avanzadas de control de acceso según los requisitos de seguridad y los entornos operativos. Evite la reentrada no autorizada con anti-passback, responda a emergencias como incendios o intrusiones, controle automáticamente las puertas según los horarios y restrinja y supervise al personal en ubicaciones específicas.

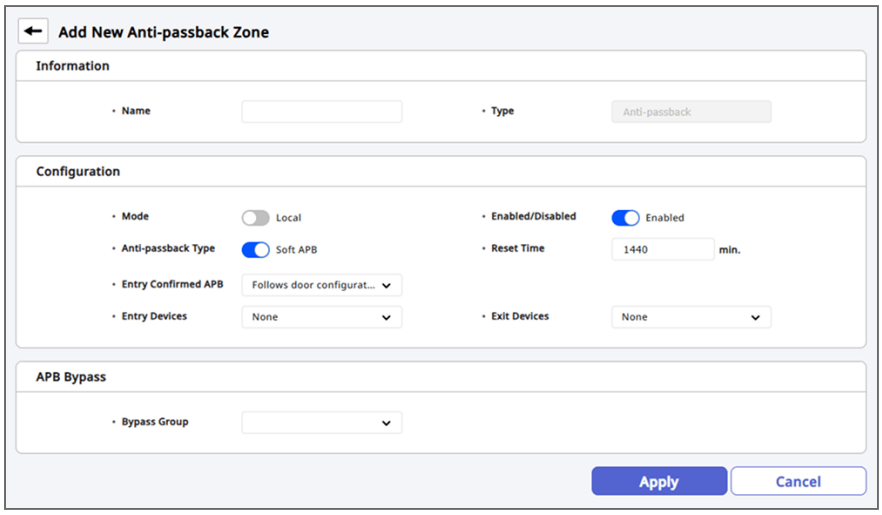
Anti-retorno

El anti-passback ofrece funciones mejoradas en comparación con el anti-passback generado a partir de puertas o dispositivos. Configure el anti-passback para obligar a los usuarios a utilizar las puertas y los dispositivos designados al ingresar y salir. Esto evita el reingreso no autorizado y mejora la seguridad.

> **Información**
> **안티패스백(Anti-Passback)**: 출입 통제를 위해 구조적인 방법으로서, 출입문 안쪽/바깥쪽에 출입 통제 장치를 설치하여 구역에 출입할 때 반드시 인증을 통해 출입해야 하는 기능입니다. 카드를 사용해 출입할 때 리더기에 카드를 인식하지 않고 앞 사람을 따라 입실했다면, 퇴실할 때 출입문이 열리지 않으며 **안티패스백** 이벤트가 발생합니다.
> 안티패스백은 Hard APB와 Soft APB로 구분합니다. **안티패스백** 위반 시 Hard APB는 **안티패스백** 이벤트를 생성하고 출입할 수 없으며, Soft APB는 **안티패스백** 이벤트를 생성하고 출입은 가능합니다.

Registrar anti-passback

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **ADD ADVANCED AC**.
4. Seleccione **Anti-passback** y haga clic en **Apply**.
5. Ingrese el nombre de la función adicional de anti-passback en la sección **Info**.



6. Configure los detalles de la función de anti-passback en la sección **Settings**. Para obtener más información, consulte Guía de opciones de ajuste.
7. Configure las acciones a realizar cuando se produzca una violación de anti-passback en la sección **Alarm**.
8. Seleccione los grupos de ingreso que pueden omitir el anti-passback en la sección **APB Bypass**. Los usuarios que pertenezcan a este grupo pueden omitir el anti-passback.
9. Después de completar todas las configuraciones, haz clic en **Apply** en la parte inferior de la pantalla.

> **Información**
> La sección **Alarm** solo puede utilizarse después de configurar tanto **Entry Devices** como **Exit Devices**.

Guía de opciones de ajuste

Los detalles de la configuración de anti-passback son los siguientes.

- **Mode**: Establece el alcance de aplicación.
  - **Local**: Se puede configurar con dispositivos de entrada conectados mediante RS-485.
  - **Global**: Se puede configurar en todos los dispositivos registrados en **BioStar X**.
- **Enabled/Disabled**: Puedes activar o desactivar temporalmente la configuración.
- **Anti-passback Type**: Seleccione el tipo de anti-passback.
  - **Hard APB**: Crea eventos de anti-passback y no permite el ingreso.
  - **Soft APB**: Crea eventos de anti-passback y permite el ingreso.
- **Reset Time**: Establezca el tiempo de espera hasta que se permita el reingreso después de que un usuario viole las reglas de anti-passback. Después de que transcurra el tiempo especificado tras una alarma, se permitirá automáticamente el acceso del usuario.
  - Se puede configurar en un rango de **1** minuto a **10080** minutos (7 días).
  - Si se establece en **0** minutos, la alarma no se borrará automáticamente hasta que el administrador la borre manualmente.
- **Entry Confirmed APB**: Configure el alcance en el que se aplican las reglas de anti-passback.
  - **ON**: Las reglas de anti-passback se aplican según la operación real de los dispositivos de entrada y salida.
  - **OFF**: Las reglas se aplican según la autenticación del usuario, independientemente del funcionamiento de la puerta.
  - **Follows door configuration**: Al usar APB basado en la entrada de la puerta correspondiente, las reglas de anti-passback se aplican según la opción de uso del sensor.
- **Entry Devices**: Selecciona el dispositivo que se utilizará al entrar. Puedes elegir de la lista de dispositivos registrados.
- **Exit Devices**: Selecciona el dispositivo que se utilizará al salir. Puedes elegir de la lista de dispositivos registrados.
- **Network Failure Action**: Configure la acción de la puerta cuando se interrumpa la comunicación con dispositivos configurados con anti-passback en **BioStar X**. Esta función está disponible cuando la opción **Mode** se establece en **Global**.
  - **Open by auth**: La puerta se abre cuando el usuario se autentica normalmente.
  - **Open by auth & record APB log**: Se genera una alarma de violación de anti-passback y la puerta se abre.
  - **Door locked & record APB log**: Se genera una alarma de violación de anti-passback y la puerta no se abre.

Información

Para obtener más información sobre el registro de dispositivos, consulte lo siguiente.

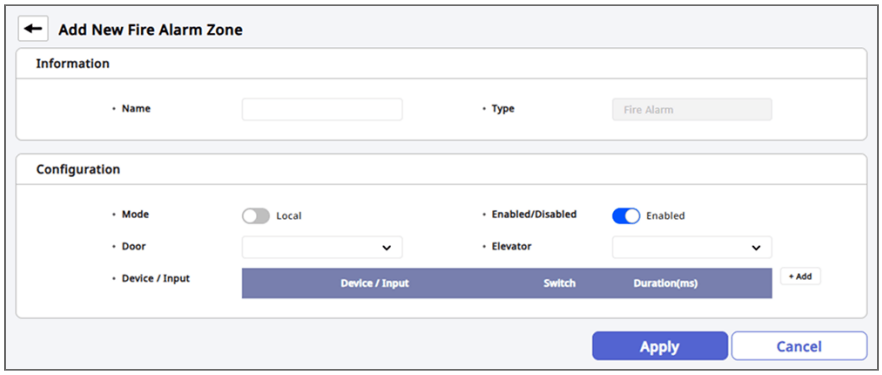
- Registrar dispositivo
- Registrar Credenciales Wiegand
- Registrar Esclavo

Alarma de incendios

Guía para configurar las alarmas contra incendios. La alarma contra incendios es una función que permite abrir o bloquear todas las puertas de acceso o los ascensores cuando se produce un incendio.

Registrar alarma contra incendios

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **ADD ADVANCED AC**.
4. Selecciona **Fire Alarm** y haz clic en **Apply**.
5. Ingresa el nombre de la alarma contra incendios que deseas agregar en la sección **Info**.



6. Configura los detalles de la alarma contra incendios en la sección **Settings**. Para obtener más información, consulte Guía de opciones de ajuste.
7. Configura las acciones que se ejecutarán cuando se active una alarma contra incendios en la sección **Alarm**.
8. Después de completar todas las configuraciones, haz clic en **Apply** en la parte inferior de la pantalla.

> **Información**
> La sección **Alarm** debe configurar **Door** para que sea utilizable.

Guía de opciones de ajuste

Los detalles para configurar la alarma contra incendios son los siguientes.

- **Mode**: Establece el alcance de aplicación.
  - **Local**: Solo se puede configurar en dispositivos conectados vía RS-485 con dispositivos de entrada.
  - **Global**: Se puede configurar en todos los dispositivos registrados en **BioStar X**.
- **Enabled/Disabled**: Puedes activar o desactivar temporalmente la configuración.
- **Door**: Selecciona las puertas que se designarán para la regla de alarma contra incendios.
- **Elevator**: Selecciona el ascensor que se designará para las reglas de alarma contra incendios.
- Haz clic en **+ Add** y configura los dispositivos que activarán las señales de alarma contra incendios con **Device / Input**.

Información

- Configurar la opción **Mode** en **Local** permite aplicar la función de alarma contra incendios solo a una puerta de acceso o a un ascensor.
- Configurar la opción **Mode** en **Global** permite aplicar la función de alarma contra incendios tanto a las puertas de acceso como a los ascensores de forma simultánea.
- Para obtener más información sobre el registro de dispositivos, consulte lo siguiente.
  - Registrar dispositivo
  - Registrar Credenciales Wiegand
  - Registrar Esclavo

Cierre Programado

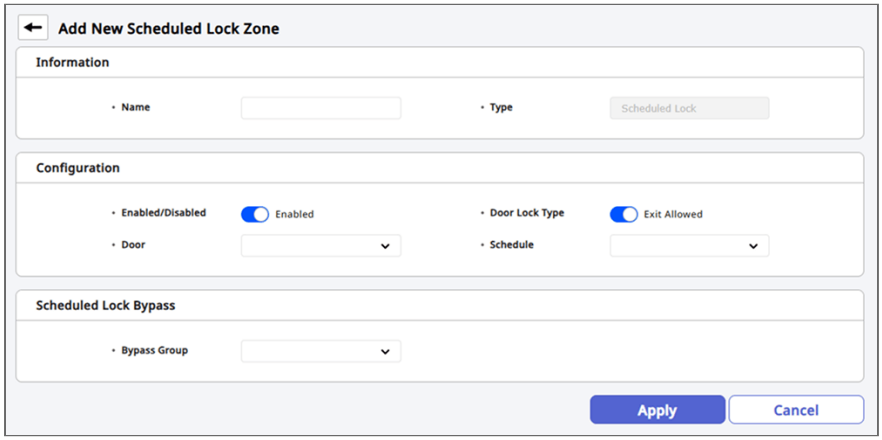
Guía para configurar el bloqueo programado. El bloqueo programado permite bloquear puertas en horarios específicos. Esta función mejora el control de acceso y resulta útil para restringir el acceso durante ciertos períodos.

Información

La configuración de bloqueo programado solo admite el modo **Local**.

Registrar bloqueo programado

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **ADD ADVANCED AC**.
4. Selecciona **Scheduled Lock** y haz clic en **Apply**.
5. Ingresa el nombre de la función de bloqueo programado que deseas agregar en la sección **Info**.



6. Configura los detalles de la función de bloqueo programado en la sección **Settings**. Para obtener más información, consulte Guía de opciones de ajuste.
7. Configura la acción a realizar cuando se produzca una violación del bloqueo programado en la sección **Alarm**.
8. Selecciona el grupo de acceso que puede omitir el bloqueo programado en la sección **Scheduled Lock Bypass**. Los

usuarios de este grupo pueden omitir el bloqueo programado.

9. Después de completar todas las configuraciones, haz clic en **Apply** en la parte inferior de la pantalla.

> **Información**
> La sección **Alarm** debe configurar **Door** para que sea utilizable.

Guía de opciones de ajuste

Los detalles para configurar el bloqueo programado son los siguientes.

- **Enabled/Disabled**: Puedes activar o desactivar temporalmente la configuración.
- **Door Lock Type**: Puedes configurarlo para bloquear solo el dispositivo de entrada o ambos dispositivos de entrada y salida.
- **Door**: Selecciona las puertas para especificar las reglas de bloqueo programado.
- **Schedule**: Selecciona un horario. Si el horario deseado no está disponible, haz clic en **+ Add Schedule** para agregar uno.

> **Información**
> - Puedes seleccionar varias puertas para configurar la función de bloqueo programado en el modo **Local**.
> - Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

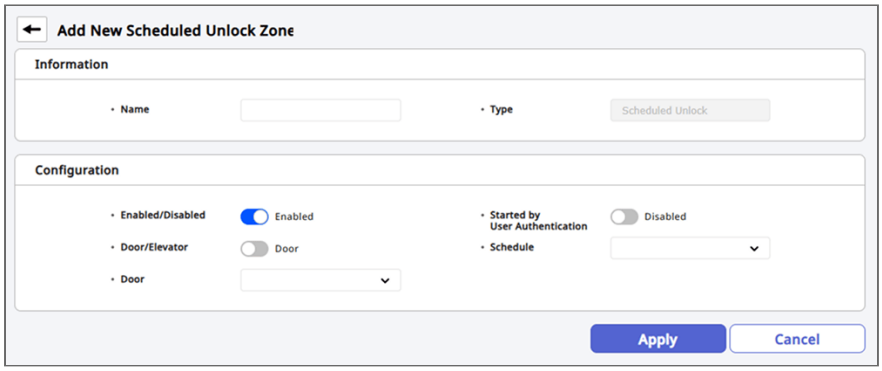
Apertura Programada

Pautas para la configuración de desbloqueo programado. El desbloqueo programado permite abrir puertas en horarios específicos. Esta función mejora el control de acceso y es útil para permitir el ingreso durante determinados períodos de tiempo.

> **Información**
> El desbloqueo programado solo admite el modo **Local**.

Registrar desbloqueo programado

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **ADD ADVANCED AC**.
4. Seleccione **Scheduled Unlock** y haga clic en **Apply**.
5. Introduzca el nombre de la función de desbloqueo programado que se va a añadir en la sección **Info**.



6. Configure los detalles de la función de desbloqueo programado en la sección **Settings**. Para obtener más información, consulte Guía de opciones de ajuste.

7. Seleccione el grupo de acceso que puede iniciar el desbloqueo programado en la sección **Scheduled Unlock Authentication**.

8. Después de completar todas las configuraciones, haz clic en **Apply** en la parte inferior de la pantalla.

Guía de opciones de ajuste

Los detalles de la configuración de desbloqueo programado son los siguientes.

- **Enabled/Disabled**: Puedes activar o desactivar temporalmente la configuración.
- **Started by User Authentication**: Si se define en **Enabled**, aparecerá la sección **Scheduled Unlock Authentication**. Los usuarios del grupo de usuarios seleccionado en **Access Group** deben autenticarse según el horario especificado para iniciar el desbloqueo programado.
- **Door/Elevator**: Seleccione la puerta o el ascensor al que se aplicará la función de desbloqueo programado.
  - Al seleccionar **Door**, se activa la lista de puertas. Seleccione la puerta a la que se aplicará la función de desbloqueo programado. Se pueden seleccionar varias puertas.
  - Al seleccionar **Elevator**, se activa la lista de ascensores. Seleccione el ascensor al que se aplicará la función de desbloqueo programado. Se pueden seleccionar varios ascensores.

> La opción **Door/Elevator** aparece cuando se registra un ascensor. Si no hay ascensores registrados, solo aparecerá la opción **Door**. Consulte Registrar Ascensor para obtener más información sobre cómo registrar un ascensor.

- **Schedule**: Selecciona un horario. Si el horario deseado no está disponible, haz clic en **+ Add Schedule** para agregar uno.
- **Floor**: Puede seleccionar los pisos para el ascensor seleccionado.

> **Información**
>
> - En el modo **Local**, puede seleccionar varias puertas para configurar la función de desbloqueo programado.
> - Si selecciona un ascensor que ya forma parte de otra configuración de desbloqueo programado, no podrá duplicar los ajustes en el mismo piso.
> - Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

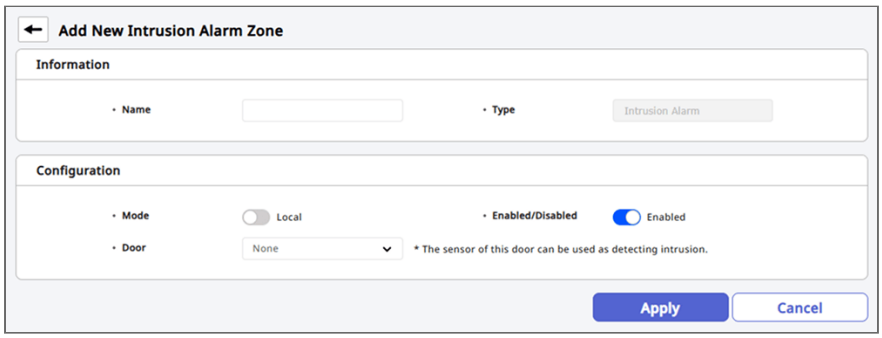
Alarma de intrusión

Esta guía muestra cómo configurar la seguridad. Los ajustes de la alarma de intrusión permiten bloquear puertas o activar alarmas cuando se detecta una intrusión.

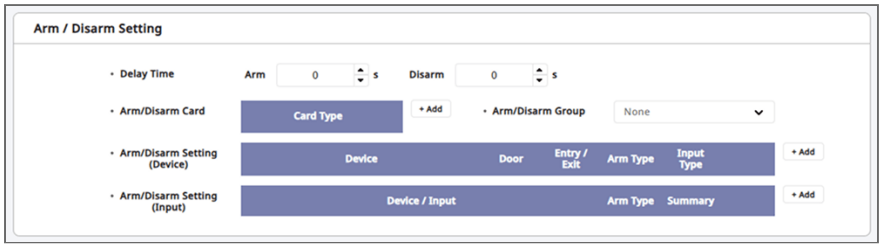
> **Información**
> **경비 구역:** 경비 개시 후 허가받지 않은 사람이 침입을 시도하면 경고음을 출력하거나 릴레이 신호를 출력하도록 설정한 구역입니다. 주로 업무 종료 이후 경비를 개시하며, 경비 개시 이후 출입을 시도하면 설정된 알람이나 신호를 출력합니다.

Agregar alarma de intrusión

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **ADD ADVANCED AC**.
4. Seleccione **Intrusion Alarm** y haga clic en **Apply**.
5. Introduzca el nombre del ajuste de alarma de intrusión que desea agregar en la sección **Info**.



6. Configure los detalles de los ajustes de alarma de intrusión en la sección **Settings**. Para obtener más información, consulte Guía de opciones de ajuste.
7. Agregue ajustes de autenticación para el armado y desarmado en la sección **Arm / Disarm Setting**. Para obtener más información, consulte Ajustes de armado o desarmado.



> La sección **Arm / Disarm Setting** aparece cuando selecciona una puerta en la sección **Info**.

8. Configure las señales de detección de intrusión en la sección **Intrusion Setting**. Para obtener más información, consulte Ajustes de detección de intrusión.



9. Configure las acciones que se realizarán cuando ocurran eventos específicos en la sección **Alarm**.
10. Después de completar todas las configuraciones, haz clic en **Apply** en la parte inferior de la pantalla.

> **Información**
> Las secciones **Arm / Disarm Setting**, **Intrusion Setting** y **Alarm** están disponibles solo si la opción **Door** está configurada en la sección **Settings**.

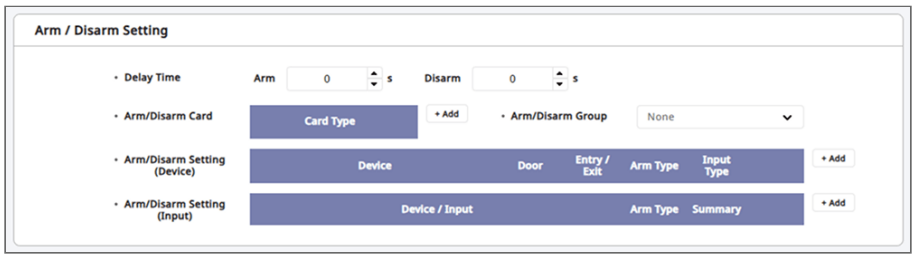
Guía de opciones de ajuste

Los detalles para los ajustes de alarma de intrusión son los siguientes.

- **Mode**: Establece el alcance de aplicación. Los ajustes de alarma de intrusión solo admiten el modo **Local** y solo se pueden configurar con dispositivos conectados mediante RS-485 y dispositivos de entrada.
- **Enabled/Disabled**: Puedes activar o desactivar temporalmente la configuración.
- **Door**: Seleccione la puerta a la que se aplicará la función de alarma de intrusión.

Ajustes de armado o desarmado

Agregue ajustes de autenticación para el armado y desarmado.

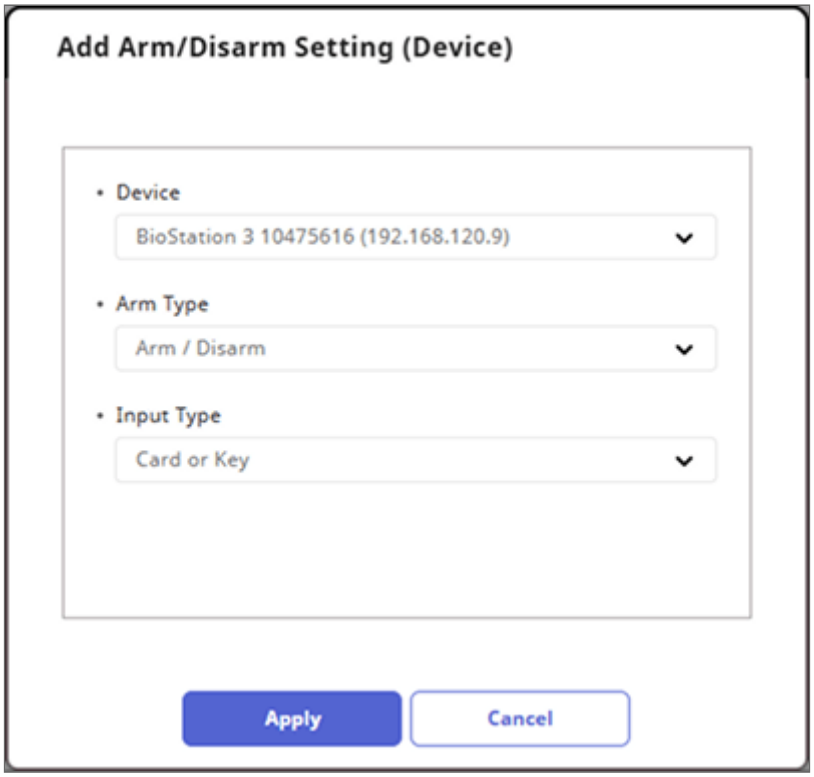


- Configure el tiempo de retraso para el armado o desarmado con **Delay Time**. Esto significa que el armado es el tiempo de retraso después de la autenticación hasta que inicia la alarma, y el desarmado es el tiempo de retraso antes de que se active la alarma después de que se detecta una intrusión.
- Agregue tarjetas autorizadas para el armado o desarmado con **Arm/Disarm Card**. Registre hasta 128 tarjetas de armado/desarmado.
- Seleccione los grupos autorizados para el armado o desarmado con **Arm/Disarm Group**. Registre hasta 128 grupos de armado/desarmado.
- Configure el armado/desarmado mediante el dispositivo o señal de entrada con **Arm/Disarm Setting**. Haga clic en el botón **+ Add** y configure cada elemento.

Agregar armado/desarmado por dispositivo

Haga clic en el botón **+ Add** en la opción **Arm/Disarm Setting** (**Device**). Seleccione el dispositivo para controlar la función de alarma de intrusión y elija **Arm Type**.

En **Input Type** puede seleccionar **Card**, **Key** o **Card or Key**. Los dispositivos sin pantalla LCD solo pueden usar **Card** como tipo de entrada.



Agregar armado/desarmado por señal de entrada

Haga clic en el botón **+ Add** en la opción **Arm/Disarm Setting** (**Input**). Seleccione el dispositivo para controlar la función de alarma de intrusión. Haga clic en **Port** para elegir el puerto de entrada del dispositivo seleccionado.

Después de elegir **Arm Type**, establezca el tipo de interruptor y la duración de la señal.



Ajustes de detección de intrusión

Configure las señales de detección de intrusión. Haga clic en **+ Add** y configúrelo como se muestra a continuación para reconocer una intrusión cuando un sensor N/O conectado al puerto de entrada 0 del dispositivo BioStation 3 envíe una señal durante 100 (ms).



Esclusa

El esclusa es un método de control de acceso utilizado en áreas donde la seguridad es importante. Cuando se configura el esclusa en un lugar con dos o más puertas, funciona de la siguiente manera.

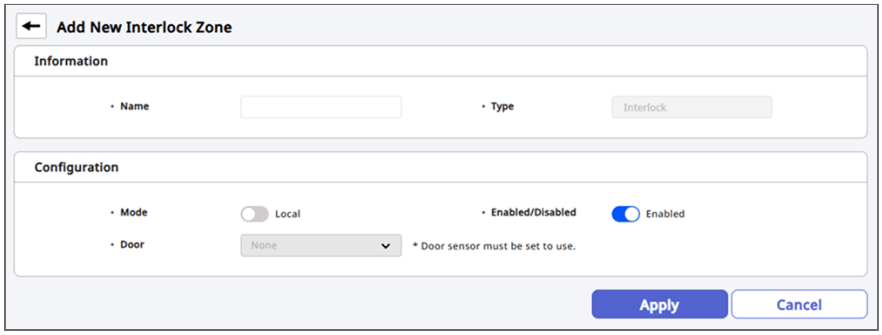
- Supervisa el estado de cada puerta en tiempo real mediante sensores y relés de puerta.
- Si una puerta está abierta o desbloqueada, todas las demás puertas pasan automáticamente a estado bloqueado.
- Configura para bloquear el acceso adicional mientras haya un usuario presente en la ubicación.

Este método mejora la seguridad al evitar que varias puertas se abran simultáneamente.

> **Información**
>
> - Una sola configuración de esclusa puede incluir hasta 4 puertas.
> - Solo se puede configurar el esclusa en puertas compuestas por dispositivos conectados a CoreStation.
> - Los dispositivos asignados a un esclusa no pueden utilizarse en otras configuraciones de esclusa.
> - Las puertas asignadas a un esclusa no pueden utilizarse en otras configuraciones, excepto en los ajustes de alarma contra incendios.

Registre el interbloqueo

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **ADD ADVANCED AC**.
4. Selecciona **Interlock** y haz clic en **Apply**.
5. Ingresa el nombre de la configuración de esclusa que se añadirá en la sección **Info**.



6. Configura los detalles de la configuración de esclusa en la sección **Settings**. Para obtener más información, consulte Guía de opciones de ajuste.
7. Establece que no se permita el acceso cuando haya un usuario presente en la sección **Option**.
8. En la sección **Alarm**, define las acciones que se ejecutarán cuando ocurran eventos específicos en la configuración de esclusa.

> **Información**
> Las secciones **Option** y **Alarm** solo pueden utilizarse si la opción **Door** está configurada en la sección **Settings**.

Guía de opciones de ajuste

Los detalles de las configuraciones de esclusa son los siguientes.

- **Mode**: Establece el alcance de aplicación. Las configuraciones de esclusa solo admiten el modo **Local** y solo pueden configurarse con dispositivos conectados a CoreStation mediante RS-485.
- **Enabled/Disabled**: Puedes activar o desactivar temporalmente la configuración.
- **Door**: Selecciona la puerta que se designará para esclusa. Debes seleccionar al menos 2 puertas, y solo se pueden añadir puertas con sensores de puerta conectados.

Reunión

La reunión es un ajuste necesario para la gestión eficaz del personal y la garantía de seguridad durante emergencias. Esta función permite a los administradores designar una ubicación específica como punto de reunión para predefinir dónde se reunirán los usuarios durante emergencias.

El ajuste de reunión cumple los siguientes propósitos:

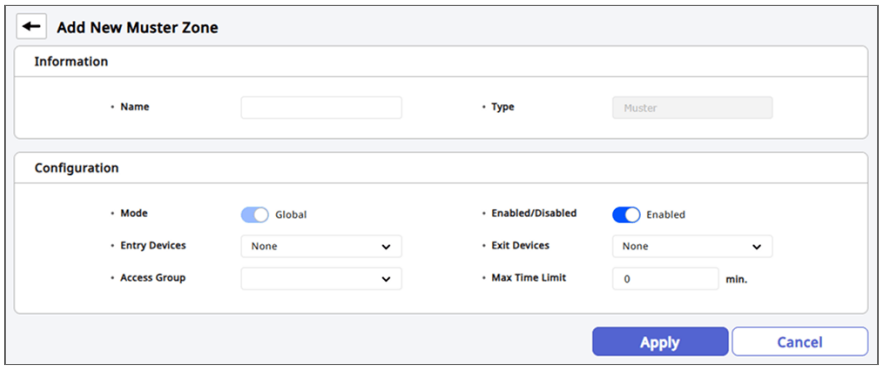
- **Respuesta ante emergencias**: Designa una ubicación donde los usuarios puedan reunirse de forma segura en caso de emergencias, como incendios o terremotos.

- **Supervisión de personal**: Verifica en tiempo real el número actual de personas y la lista de ingresantes en una ubicación específica.
- **Detección de estancia prolongada**: Detecta a los usuarios que permanecen en una ubicación específica más allá del tiempo establecido y envía notificaciones al administrador.
- **Seguridad mejorada**: Supervisa continuamente el acceso a ubicaciones sensibles para mejorar los niveles de seguridad.

A través de estas funciones, los administradores pueden establecer un marco de gestión de seguridad más sistemático y eficiente.

Registrar punto de reunión

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **ADD ADVANCED AC**.
4. Selecciona **Muster** y haz clic en **Apply**.
5. Ingresa el nombre del ajuste de reunión que se agregará en la sección **Info**.



6. Configura los detalles de los ajustes de reunión en la sección **Settings**. Para obtener más información, consulte Guía de opciones de ajuste.
7. Configura las acciones que se realizarán cuando ocurran eventos específicos en los ajustes de reunión en la sección **Alarm**.
8. Después de completar todas las configuraciones, haz clic en **Apply** en la parte inferior de la pantalla.

> **Información**
> La sección **Alarm** solo puede utilizarse después de configurar tanto **Entry Devices** como **Exit Devices**.

Guía de opciones de ajuste

Los detalles de los ajustes de reunión son los siguientes:

- **Mode**: Puedes verificar el alcance de aplicación. El ajuste de reunión solo admite el modo **Global** y puede configurarse con todos los dispositivos registrados en **BioStar X**.
- **Enabled/Disabled**: Puedes activar o desactivar temporalmente la configuración.
- **Entry Devices**: Selecciona el dispositivo que se utilizará al entrar. Puedes elegir de la lista de dispositivos registrados.

- **Exit Devices**: Selecciona el dispositivo que se utilizará al salir. Puedes elegir de la lista de dispositivos registrados.
- **Access Group**: Establece el grupo de acceso para los usuarios que se quedarán en la ubicación de reunión. Establece hasta 16 grupos de acceso.
- **Max Time Limit**: Establece el tiempo máximo permitido para permanecer en la ubicación de reunión. Se puede configurar hasta un máximo de 4320 minutos y se activará una alarma si un usuario permanece en la ubicación de reunión más allá del tiempo especificado.

> **Información**
>
> Para obtener más información sobre el registro de dispositivos, consulte lo siguiente.
>
> - Registrar dispositivo
> - Registrar Credenciales Wiegand
> - Registrar Esclavo

Límite de Ocupación

La función de límite de ocupación es una característica clave de control de acceso para garantizar la seguridad y la eficiencia de los espacios. Esta función permite a los administradores definir un número máximo de personas que pueden ingresar simultáneamente en cada ubicación, evitando la sobrepoblación y posibilitando una gestión del espacio más sistemática.

Las principales aplicaciones del ajuste de límite de ocupación son las siguientes.

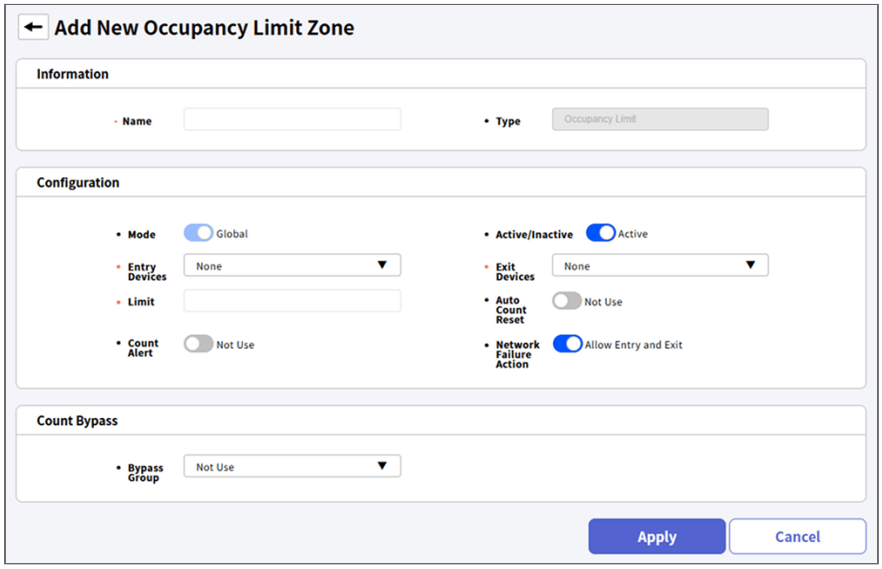
- **Gestión de seguridad**: Prevención de incidentes de seguridad mediante la limitación del número máximo de ocupantes según las normas contra incendios o la capacidad del edificio.
- **Eficiencia del espacio**: Optimización del entorno de trabajo manteniendo una ocupación adecuada en salas de reuniones, laboratorios y áreas de trabajo.
- **Respuesta ante enfermedades infecciosas**: Gestión del personal en situaciones que requieren distanciamiento social o restricciones de densidad de personas.
- **Supervisión en tiempo real**: Verifique la ocupación actual y el estado de entrada/salida de cada ubicación en tiempo real.
- **Alertas automáticas**: Notificaciones inmediatas a los administradores cuando se alcanza el límite de ocupación establecido, lo que permite respuestas rápidas.

Al utilizar estas funciones, los administradores pueden establecer políticas de gestión de personal adaptadas a las características de cada espacio, garantizando operaciones de las instalaciones seguras y eficientes.

> **Información**
>
> - Agregue hasta 100 ajustes de límite de ocupación.
> - Los dispositivos y versiones de firmware que se pueden configurar para el ajuste de límite de ocupación son los siguientes.
>   - FaceStation F2 versión de firmware 1.1.0 o superior
>   - FaceStation 2 versión de firmware 1.5.0 o superior

Establecer límite de ocupación

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **ADD ADVANCED AC**.
4. Seleccione **Occupancy Limit** y haga clic en **Apply**.
5. Ingrese el nombre del ajuste de límite de ocupación que desea añadir en la sección **Info**.



6. Configure los detalles del ajuste de límite de ocupación en la sección **Configuration**. Para obtener más información, consulte Guía de opciones de ajuste.
7. En la sección **Count Bypass**, seleccione los grupos de acceso que siempre puedan omitir el ajuste de límite de ocupación. Para obtener más información, consulte Ajuste de conteo de personas para paso siempre permitido.
8. Después de completar todas las configuraciones, haz clic en **Apply** en la parte inferior de la pantalla.

> **Información**
> **Name** puede contener hasta 48 caracteres y no puede utilizar el mismo nombre que otras configuraciones.

Guía de opciones de ajuste

Los detalles del ajuste de límite de ocupación son los siguientes.

- **Mode**: Puedes verificar el alcance de aplicación. Configure hasta 2 límites de **Global** y solo se podrán ingresar números menores que el límite.
- **Active/Inactive**: Active o desactive temporalmente los ajustes.
- **Entry Devices**: Selecciona el dispositivo que se utilizará al entrar. Puedes elegir de la lista de dispositivos registrados.
- **Exit Devices**: Selecciona el dispositivo que se utilizará al salir. Puedes elegir de la lista de dispositivos registrados.
- **Limit**: Ingrese el número de personas a limitar para la entrada. El ingreso se restringe si el número de personas alcanza el límite de ocupación establecido. Ingrese un número de 0 a 10,000; si lo establece en 0, el acceso será ilimitado.

- **Auto Count Reset**: Defina la hora para inicializar automáticamente el conteo de ocupación almacenado. Cada día a la hora establecida, se restablecerán el conteo de ocupación y el número de personas que siempre omiten el límite.
- **Count Alert**: Envíe una alerta al administrador o registre un evento antes de que el número de personas que ingresan alcance el límite establecido. Cuando las prealertas de ocupación están habilitadas, el campo de entrada **Alert 1** se activa. Para configurar **Alert 2**, haga clic en el botón +.
- **Network Failure Action**: Determine si se permite la entrada y salida cuando se produce un error de red en el dispositivo configurado. Si se establece permitir entrada y salida, la restricción de ingreso se detiene cuando el dispositivo pierde la conexión de red y los usuarios pueden ingresar incluso si el número real supera el límite.

Información

- No se puede establecer el mismo dispositivo tanto para **Entry Devices** como para **Exit Devices** al mismo tiempo.
- Seleccione hasta 128 dispositivos para **Entry Devices** y **Exit Devices**.
- Un dispositivo configurado con **Dual Authentication** en una puerta no puede ser asignado a **Entry Devices** ni a **Exit Devices**.
- Configure la hora para la opción **Auto Count Reset** teniendo en cuenta la zona horaria estándar de la ubicación real. Por ejemplo, si el servidor **BioStar X** está ubicado en una región UTC+1:00 y la hora de restablecimiento automático se establece a las 00:00, el cliente **BioStar X** en la región UTC+2:00 restablecerá automáticamente la ocupación a las 01:00.
- Configure hasta 2 límites de **Count Alert** y solo se podrán ingresar números menores que el límite. **Alert 1** y **Alert 2** no pueden configurarse con el mismo valor.
- Para obtener más información sobre el registro de dispositivos, consulte lo siguiente.
  - Registrar dispositivo
  - Registrar Credenciales Wiegand
  - Registrar Esclavo

Ajuste de conteo de personas para paso siempre permitido

Seleccione los grupos de acceso que siempre pueden omitir el ajuste de límite de ocupación. Los usuarios que pertenecen al grupo exento pueden entrar y salir independientemente del conteo de ocupación y no se contabilizarán en las cifras de ocupación. Los miembros activos actualmente exentos se muestran en la columna de ocupantes exentos de la lista de ajustes de límite de ocupación.

Información

- Al usar una cámara térmica conectada al dispositivo, configurar **Thermal & Mask Check Mode** en **Check without authentication** no funcionará, incluso si se han establecido personas exentas.
- Configure hasta 16 grupos de **Bypass Group**.

Verifique el estado de la lista de ocupación

Revise la lista de ajustes de límite de ocupación. Revise el estado de cada ajuste y el conteo de ocupación, y cambie los ajustes según sea necesario.

- **Name**: Revise el nombre.

- **Status**: Revise el estado.
  - **Normal**: Indica que el número de usuarios en la zona es inferior al establecido por **Limit**, **Count Alert**(**Alert 1**, **Alert 2**). Los usuarios pueden entrar en esta ubicación.
  - **Count Alert**: Indica que el número de usuarios presentes ha alcanzado el valor establecido en **Alert 1** o **Alert 2**.
  - **Full**: Indica que el número de usuarios presentes ha alcanzado el límite establecido. Se restringen más ingresos.
- **Count/Limit**: Revise el número actual de ocupantes en comparación con la capacidad. Si hay una discrepancia entre la ocupación registrada y el número real de usuarios presentes debido a situaciones como errores de red, el administrador puede hacer clic en + o − o hacer clic en el conteo de ocupación para modificarlo directamente.
- **Count Bypass**: Revise el número de usuarios que actualmente están en el grupo exento.
- **Device Status**: Revise el estado de los dispositivos configurados.
  - **Normal**: La red de todos los dispositivos configurados funciona con normalidad.
  - **Network Failure**: Indica que uno o más dispositivos están experimentando errores de red.
- **Full Screen**: Puede ver el estado de la configuración del límite de ocupación en pantalla completa.

> **Información**
> Cuando se establece **Limit**, puede ingresar conteos de ocupación de hasta 50,000 como máximo. Si **Limit** no está establecido, puede ingresar conteos de hasta 999,999 como máximo. No puede ingresar números que superen el valor máximo permitido y, si la ocupación real supera este valor, el excedente no se registrará en la base de datos.

Inicializar ocupación

Puede restablecer el conteo de ocupación y el número de personas con paso siempre permitido. Al continuar con el restablecimiento de la ocupación se eliminará toda la información de entrada y salida de los usuarios, y la precisión del conteo de ocupación puede variar según el estado de la conexión de red.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haga clic en **Occupancy Limit** en la lista.
4. Haga clic en la casilla de verificación de la configuración que desea inicializar en la lista de configuraciones de límite de ocupación.
5. Haga clic en **Reset Count** en la esquina superior derecha de la pantalla.
6. Cuando aparezca el mensaje de confirmación, haga clic en **Apply**.

Activar/desactivar

Puede activar una configuración de límite de ocupación desactivada o desactivar una configuración activa. Al desactivar las configuraciones se restablecerán **Current Occupancy** y **Bypass Count**.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.

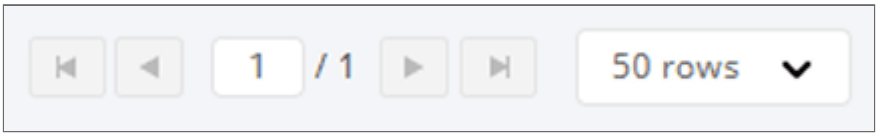
3. Haga clic en **Occupancy Limit** en la lista.
4. Haga clic en la casilla de verificación del elemento en la lista de configuraciones de límite de ocupación para activarlo o desactivarlo.
5. Haga clic en **Activate** o **Deactivate** en la esquina superior derecha de la pantalla.

Eliminar

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haga clic en **Occupancy Limit** en la lista.
4. Haga clic en la casilla de verificación del elemento que desea eliminar de la lista de configuraciones de límite de ocupación.
5. Haga clic en **Delete** en la esquina superior derecha de la pantalla.
6. Cuando aparezca el mensaje de confirmación, haga clic en **Apply**.

Navega por la página de lista

Desplácese entre páginas o establezca la cantidad de elementos que aparecerán en cada página. Utiliza la herramienta de navegación de página en la esquina superior derecha de la pantalla.



- ⏮: Ir a la primera página.
- ◀: Ir a la página anterior.
- ▶: Ir a la página siguiente.
- ⏭: Ir a la última página.
- Ingresa el número de página en el campo de entrada para ir a la página deseada.
- Haz clic en el cuadro de selección de filas para establecer la cantidad de elementos que se muestran en cada página.

Pase de lista

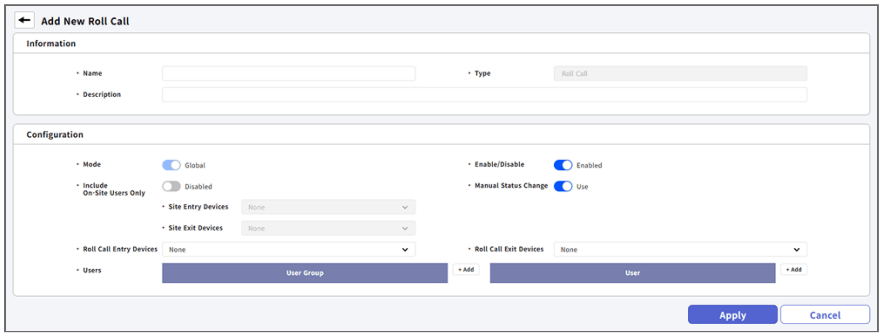
Roll Call genera rápidamente una lista de personal según los registros de entrada en un tiempo y lugar específicos. Cuando ocurre una emergencia, el sistema puede determinar si un usuario llegó al punto de lista de asistencia al autenticarse en el dispositivo de entrada o salida en una ubicación predefinida.

Puede utilizarse para la respuesta a emergencias, verificaciones de seguridad y para proporcionar información al equipo de rescate. Esto permite la gestión eficiente del estado del personal utilizando registros de entrada y salida.

> **Información**
>
> Los ajustes de Roll Call están disponibles mediante una opción adicional con una licencia **Essential** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Registrar lista de asistencia

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **ADD ADVANCED AC**.
4. Selecciona **Roll Call** y haz clic en **Apply**.
5. Ingresa el nombre y la descripción de la configuración de lista de asistencia que deseas añadir en la sección **Info**.

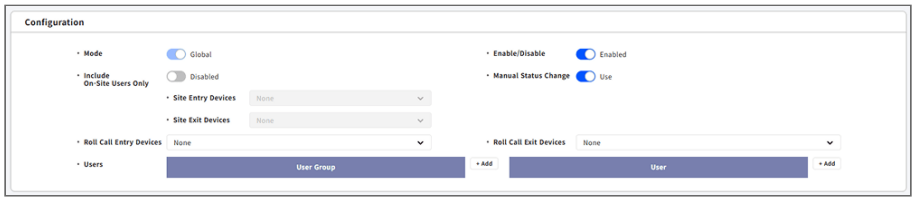


6. Configura los detalles en la sección **Configuration**. Para obtener más información, consulte Guía de opciones de ajuste.
7. Después de completar todas las configuraciones, haz clic en **Apply** en la parte inferior de la pantalla.

> **Información**
>
> **Name** puede contener hasta 48 caracteres y no puede utilizar el mismo nombre que otras configuraciones.

Guía de opciones de ajuste

Los detalles de las configuraciones de lista de asistencia son los siguientes.



- **Mode**: Puedes verificar el alcance de aplicación. Las configuraciones de lista de asistencia solo se admiten en modo **Global** y pueden configurarse para todos los dispositivos registrados en **BioStar X**.
- **Enabled/Disabled**: Puedes activar o desactivar temporalmente la configuración.
- **Include On-Site Users Only**: Establezca en **Use**. Al iniciar la lista de asistencia, el sistema fija como objetivos a los **usuarios autenticados por última vez en un dispositivo de entrada en sitio**. El valor predeterminado es **Not Use**. En este caso, todos los usuarios configurados (grupos de usuarios y usuarios individuales) pasan a ser objetivos de la lista

de asistencia.

> El sistema determina si cada usuario está en sitio según los registros de autenticación de dispositivos de entrada o salida en sitio de los últimos 7 días. Si la autenticación más reciente antes del inicio de la lista de asistencia ocurrió en un dispositivo de entrada en sitio, el sistema considera que el usuario está en sitio. Si ocurrió en un dispositivo de salida en sitio, el sistema considera que el usuario está fuera de sitio. El sistema considera que los usuarios sin registros de autenticación en los últimos 7 días están fuera de sitio y los excluye de la lista de usuarios objetivo.
>
> La lista de usuarios objetivo se finaliza una sola vez cuando inicia la lista de asistencia, y no cambia si los usuarios entran o salen mientras la lista de asistencia está en curso.

Las siguientes opciones están disponibles cuando **Include On-Site Users Only** está establecido en **Use**.

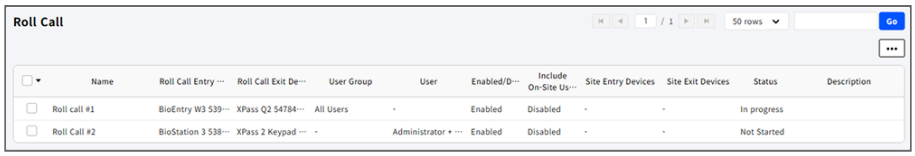
  - **Site Entry Devices**: Seleccione el dispositivo para la autenticación de entrada en sitio.
  - **Site Exit Devices**: Seleccione el dispositivo para la autenticación de salida en sitio.

- **Manual Status Change**: Puedes configurarlo para cambiar el estado manualmente.
- **Roll Call Entry Devices**: Seleccione el dispositivo que se usará al entrar. Puedes elegir de la lista de dispositivos registrados.
- **Roll Call Exit Devices**: Seleccione el dispositivo que se usará al salir. Puedes elegir de la lista de dispositivos registrados.
- **Users**: Puedes seleccionar grupos de usuarios o usuarios individuales que tengan permiso para entrar.

> **Información**
>
> - No se puede establecer el mismo dispositivo tanto para **Roll Call Entry Devices** como para **Roll Call Exit Devices** al mismo tiempo.
> - Seleccione hasta 10 dispositivos para **Roll Call Entry Devices** y **Roll Call Exit Devices**.
> - Para obtener más información sobre el registro de dispositivos, consulte lo siguiente.
>   - Registrar dispositivo
>   - Registrar Credenciales Wiegand
>   - Registrar Esclavo

Verifique el estado de la lista de asistencia

La lista de asistencia muestra los detalles y el estado de cada ajuste de lista de asistencia.



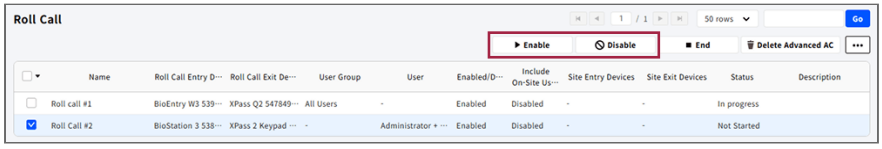
- **Name**: Muestra el nombre.
- **Roll Call Entry Devices** / **Roll Call Exit Devices**: Muestra los dispositivos seleccionados.
- **User Group** / **Users**: Muestra los usuarios objetivo seleccionados.

- **Enabled/Disabled**: Muestra el estado de activación.
- **Include On-Site Users Only**: Muestra si está habilitado.
- **Site Entry Devices** / **Site Exit Devices**: Muestra los dispositivos de entrada o salida en sitio seleccionados.
- **Status**: Muestra el estado del pase de lista (**Not Started**, **In progress**, etc.).
- **Description**: Muestra la descripción.

Activar/desactivar

Puedes activar configuraciones de lista de asistencia deshabilitadas o desactivar configuraciones activadas.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **Roll Call** en la lista.
4. Haz clic en la casilla de verificación del elemento que deseas activar o desactivar en la lista de configuraciones de lista de asistencia.

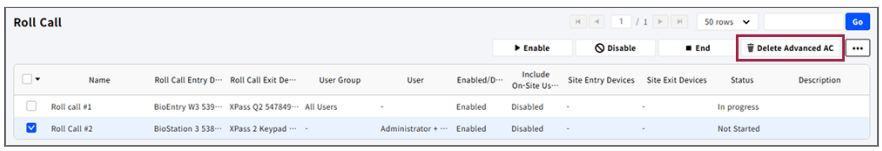


5. Haz clic en **Enable** o en **Disable** en la esquina superior derecha de la pantalla.

> **Información**
>
> - Seleccione **Disable**, y verá un mensaje de confirmación. Seleccione **Yes** o **No**.
> - No se puede desactivar un pase de lista en curso. Verifique y vuelva a intentarlo.

Eliminar

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **Roll Call** en la lista.
4. Haz clic en la casilla de verificación del elemento que deseas eliminar de la lista de configuraciones de lista de asistencia.



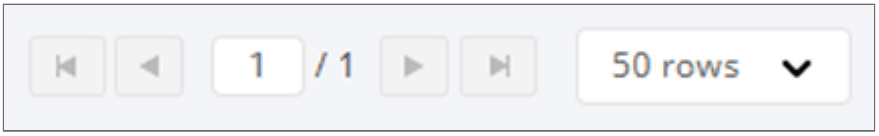
5. Haz clic en **Delete Advanced AC** en la esquina superior derecha de la pantalla.
6. Cuando aparezca el mensaje de advertencia, haz clic en el botón **Continue**.

Información

No se puede eliminar un pase de lista en curso. Finalice el pase de lista y vuelva a intentar.

Navega por la página de lista

Desplácese entre páginas o establezca la cantidad de elementos que aparecerán en cada página. Utiliza la herramienta de navegación de página en la esquina superior derecha de la pantalla.



- ⏮: Ir a la primera página.
- ◀: Ir a la página anterior.
- ▶: Ir a la página siguiente.
- ⏭: Ir a la última página.
- Ingresa el número de página en el campo de entrada para ir a la página deseada.
- Haz clic en el cuadro de selección de filas para establecer la cantidad de elementos que se muestran en cada página.

Usar la lista de asistencia en la aplicación móvil

La función de lista de asistencia está disponible en la aplicación móvil **BioStar X**.

Información

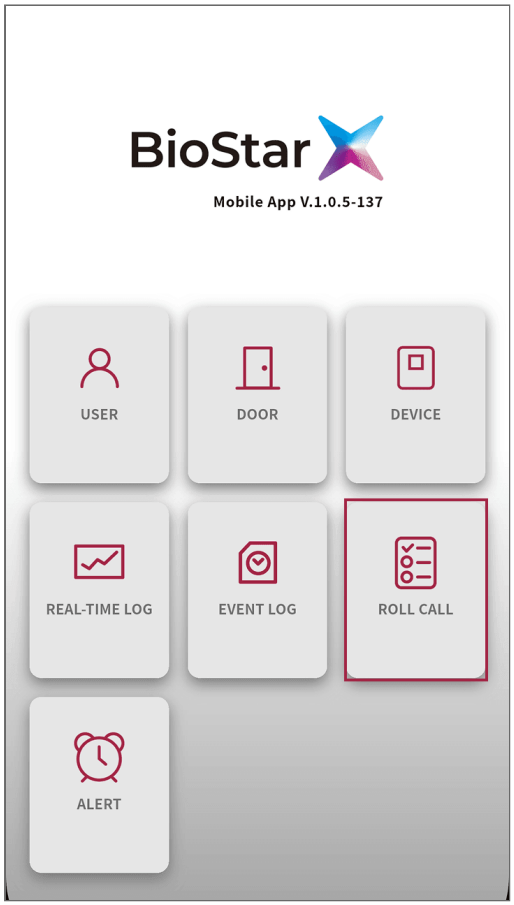
Puedes instalar la aplicación móvil **BioStar X** mediante los siguientes enlaces.

- iOS: Apple App Store
- Android: Google Play'

Iniciar la lista de asistencia

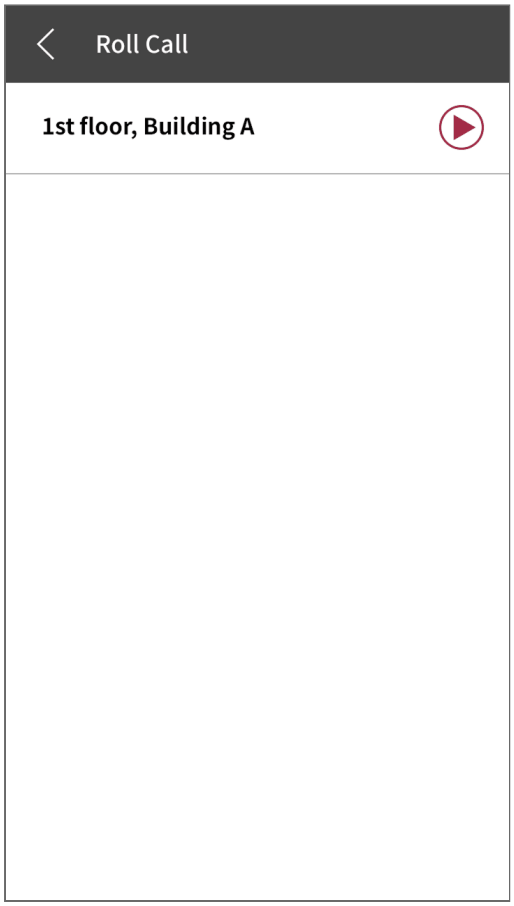
Para iniciar la función de lista de asistencia en la aplicación móvil, sigue estos pasos.

1. Abre la aplicación móvil **BioStar X** en tu dispositivo móvil.
2. Desde la pantalla principal de la app, toca **ROLL CALL**.



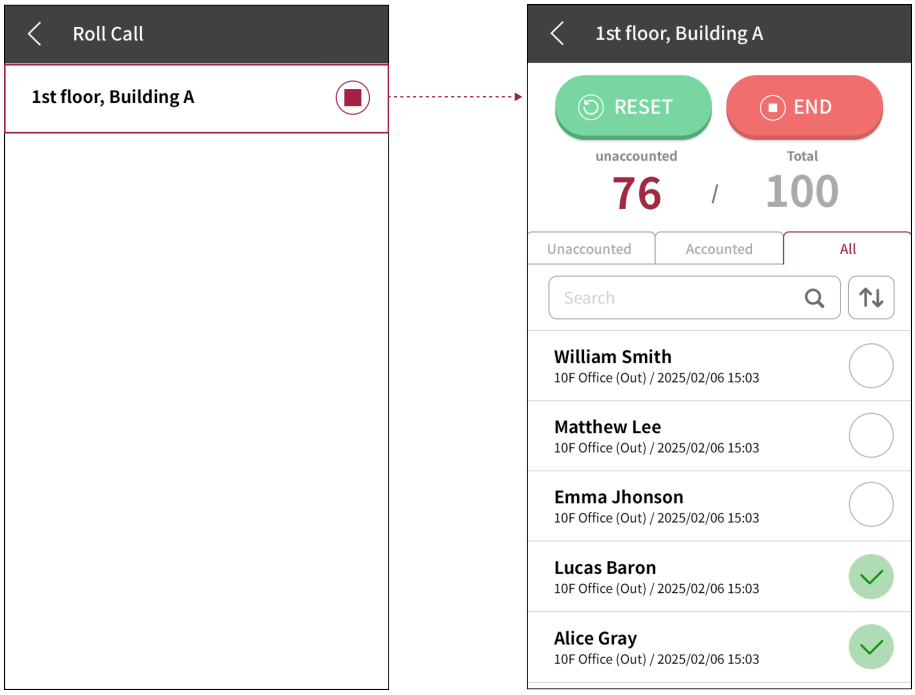
> También puedes acceder a ella desde el menú lateral. Toca ☰ → **Monitoring** → **Roll Call**.

3. En la lista de Roll Call, toca ▶ del elemento para ejecutar la lista de asistencia.



4. Cuando aparezca el mensaje de confirmación, toca **Yes**.

La lista de asistencia se iniciará y, al tocar el elemento de lista de asistencia en curso, podrás comprobar su estado.



Controlar una lista de asistencia en curso

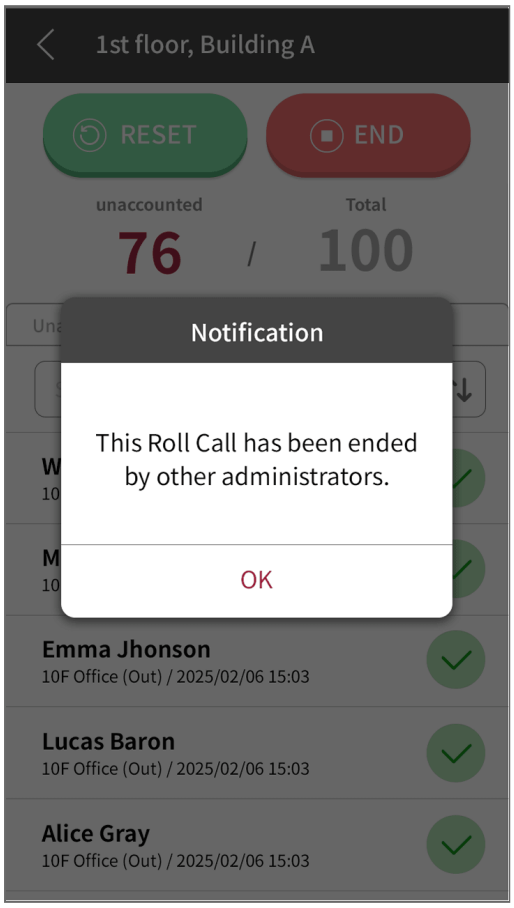
- Los usuarios que ingresen se marcarán con el ícono . Cuando todos los usuarios hayan ingresado, aparecerá un mensaje que indica que la lista de asistencia ha finalizado. Para finalizar la lista de asistencia, toca **Yes**.

- El administrador puede cambiar manualmente la entrada o el estado del usuario. Mantén presionado el botón redondo en el extremo derecho del usuario cuyo estado deseas cambiar en la lista de usuarios.



- Para reiniciar la lista de asistencia, toca **Reset**. Todo el progreso se descarta y la lista de asistencia se reinicia desde el inicio.

- Si otro administrador finaliza la lista de asistencia, aparecerá un mensaje de notificación.

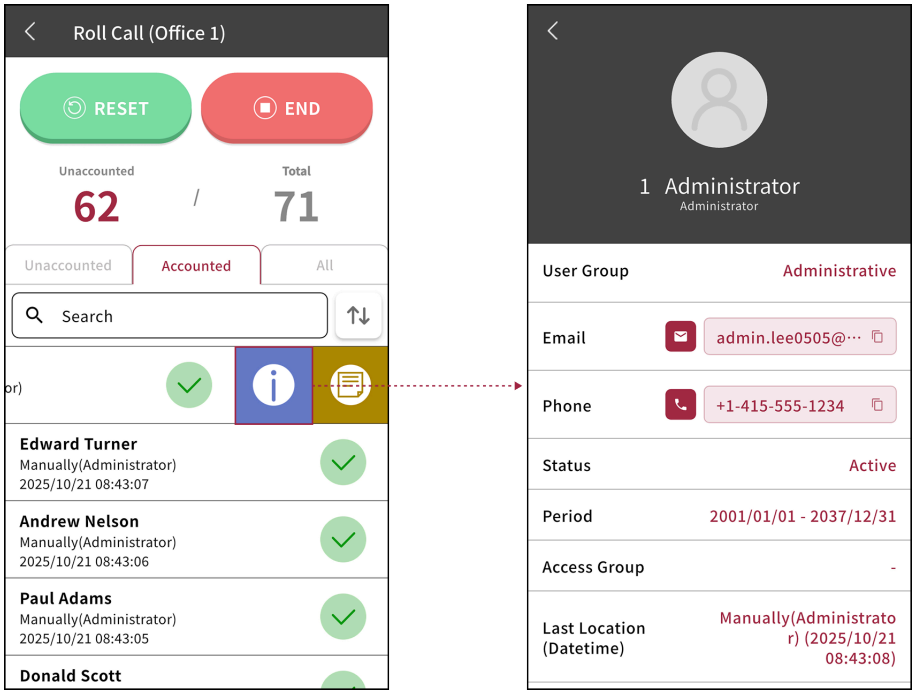


- Después de completar la lista de asistencia, puedes consultar los informes relacionados en **Data** → **Generate Report** → **Roll Call**. Para obtener más información, consulte Ver informes de pase de lista.

Información del usuario durante la lista de asistencia

Durante la lista de asistencia en la aplicación móvil, puedes consultar la información de cada usuario. Consulta detalles como la información de contacto del contacto de emergencia y la última ubicación conocida del usuario.

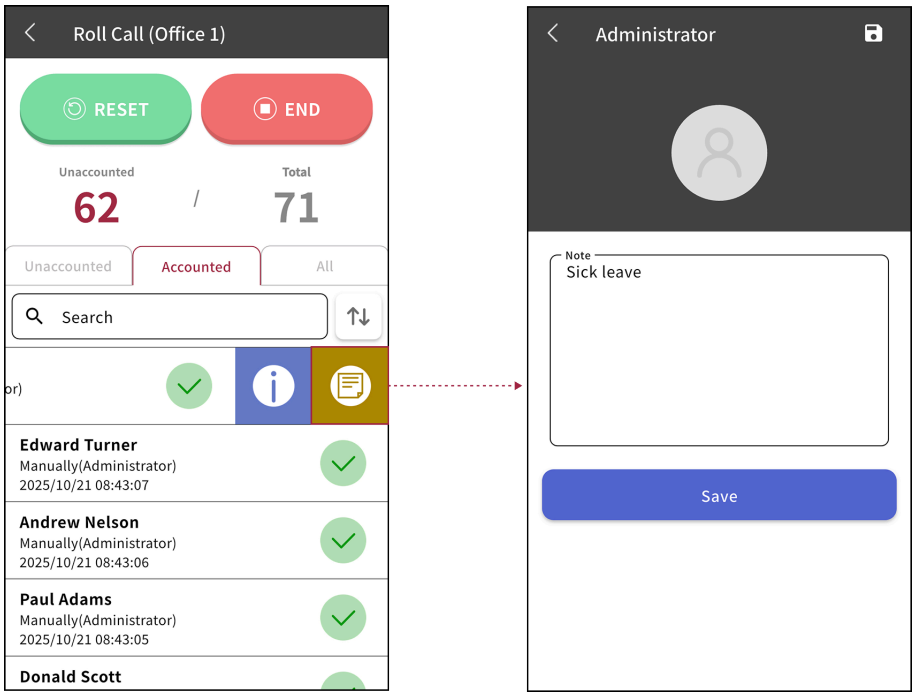
Desliza hacia la izquierda sobre el elemento de usuario del que quieras ver detalles durante la lista de asistencia. Luego, toca ⓘ.



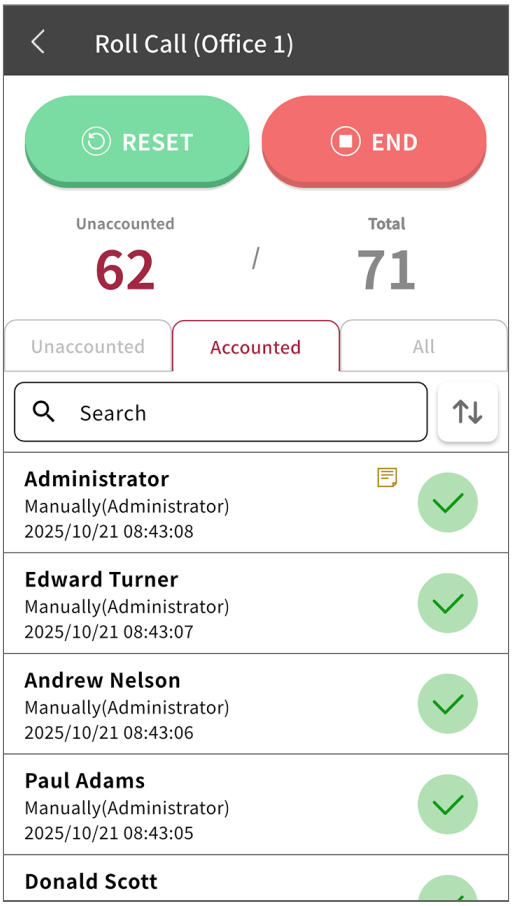
Dejar una nota para usuarios durante la lista de asistencia

Si un usuario específico no ha ingresado durante la lista de asistencia en la aplicación móvil, puedes dejarle una nota.

Desliza hacia la izquierda sobre el elemento de usuario donde quieras ingresar una nota durante la lista de asistencia. Luego, toca . En la pantalla de ingreso de notas, escribe el contenido y toca **Save**.



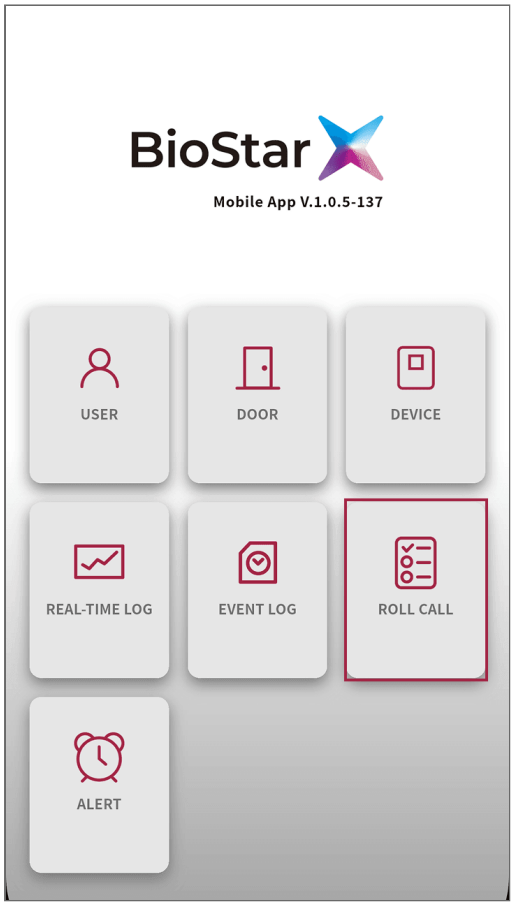
Los usuarios que hayan ingresado notas se marcarán con el ícono en la lista de asistencia.



Ver detalles de la lista de asistencia

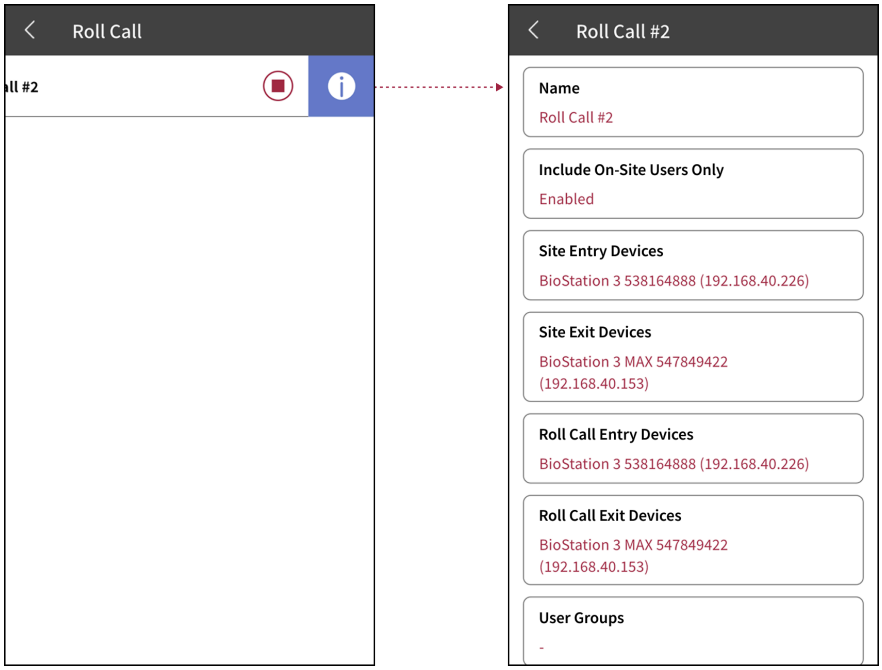
Consulta los detalles de la configuración del pase de lista en la aplicación móvil.

1. Abre la aplicación móvil **BioStar X** en tu dispositivo móvil.
2. Desde la pantalla principal de la app, toca **ROLL CALL**.



> También puedes acceder a ella desde el menú lateral. Toca ☰ → **Monitoring** → **Roll Call**.

3. Desliza el elemento hacia la izquierda para consultar los detalles en la lista y, luego, toca ⓘ.

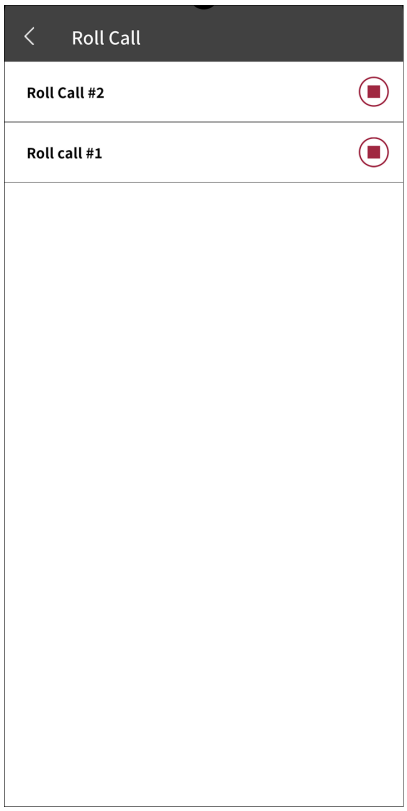


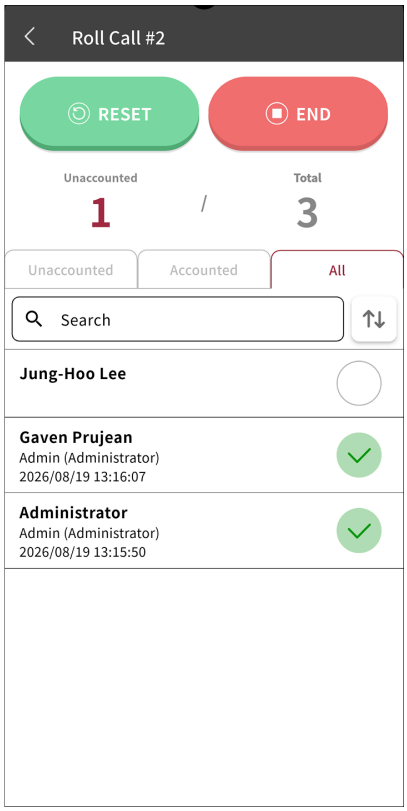
Finalizar lista de asistencia

Finaliza listas de asistencia en curso tanto en la aplicación móvil **BioStar X** como en la web.

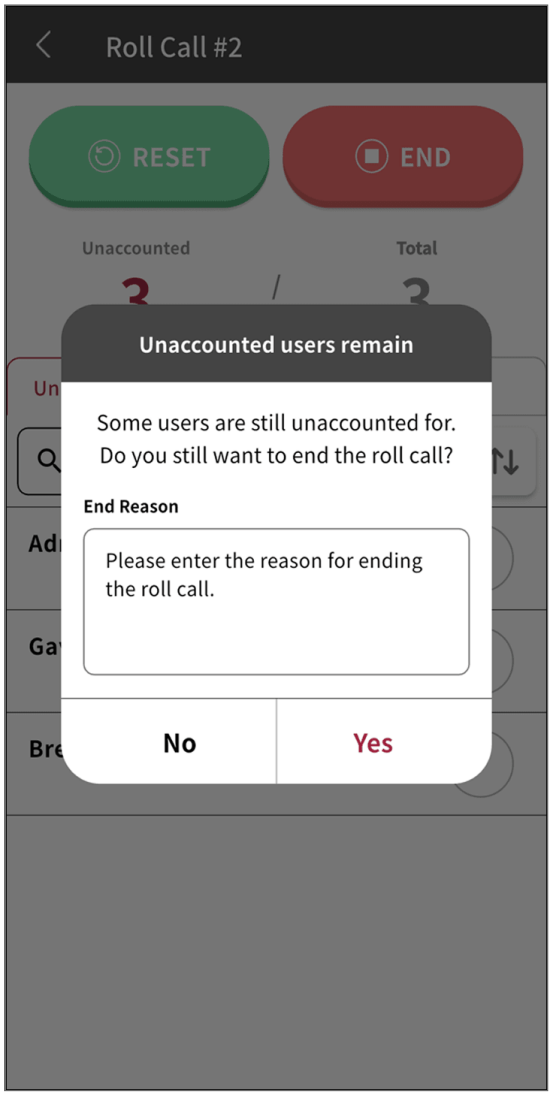
Finalizar en la aplicación móvil

1. Para finalizar una lista de asistencia, toca el botón en la pantalla de lista o el botón **END** en la pantalla de estado.



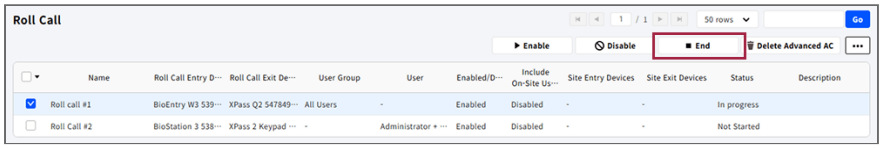


2. Si quedan usuarios no contabilizados, aparece una ventana emergente de advertencia. Ingresa un motivo de finalización y toca **Sí**.



Finalizar en la web

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Access Management** → **Advanced AC** en la barra lateral izquierda.
3. Haz clic en **Roll Call** en la lista.
4. En la lista de listas de asistencia, marca la casilla de la lista que vas a finalizar.



5. Haz clic en **End** en la esquina superior derecha de la pantalla.
6. Cuando aparezca el mensaje de confirmación, haz clic en **Yes**.

Una lista de asistencia sin usuarios no contabilizados finaliza de inmediato. En una lista de asistencia con usuarios no contabilizados, aparece un cuadro de diálogo con la lista **Unaccounted Users** y el campo **End Reason**. Ingresa un motivo y haz clic en **End Roll Call** para finalizar la lista de asistencia.



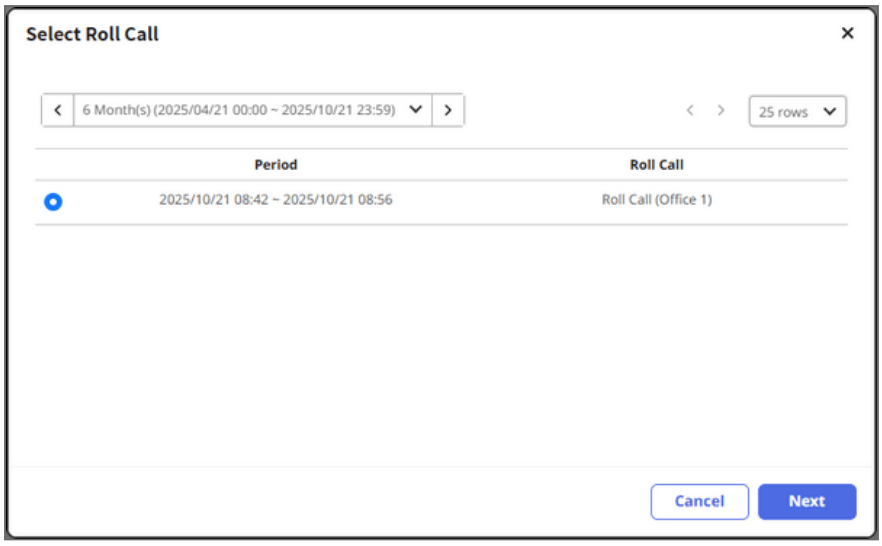
Información

- **End Reason**: Ingresa hasta 500 caracteres.
- El sistema no puede finalizar varias listas de asistencia si alguna tiene usuarios no contabilizados. Finaliza las listas de asistencia una a la vez.

Ver informes de pase de lista

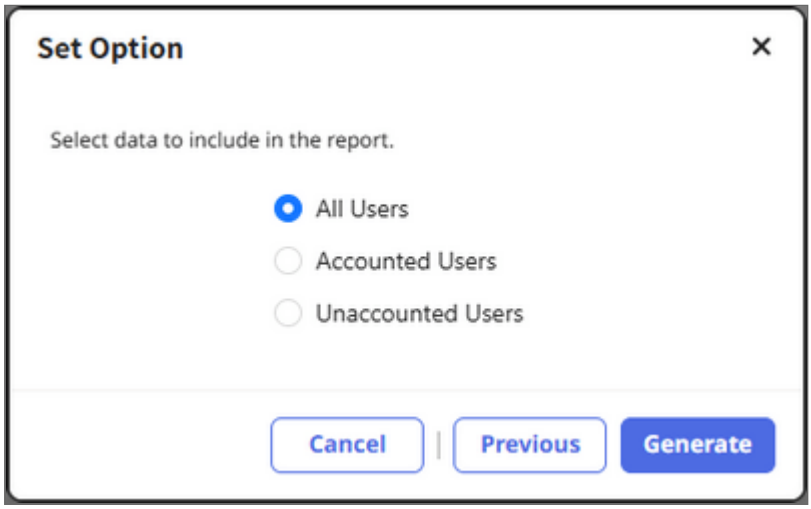
Sigue estos pasos para consultar el informe de pase de lista.

1. Haz clic en **Data** en **Launcher**.
2. Haz clic en **Events** → **Roll Call** en la barra lateral izquierda.
3. Cuando aparezca la ventana **Select Roll Call**, selecciona el elemento de pase de lista que deseas consultar en el informe y, luego, haz clic en el botón **Next**.

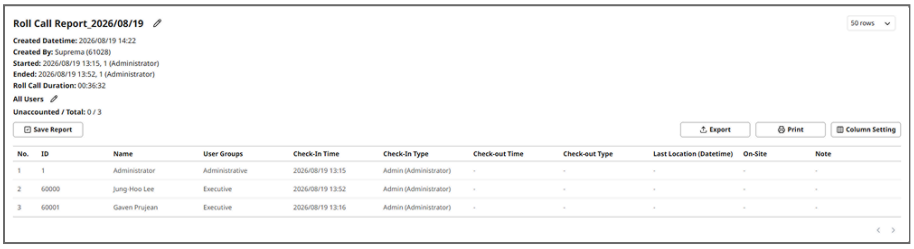


> Si no ves el elemento de pase de lista deseado, ajusta el período en la parte superior de la pantalla.

4. En la ventana de configuración de opciones, selecciona los datos que se van a incluir en el informe y, luego, haz clic en el botón **Generate**.

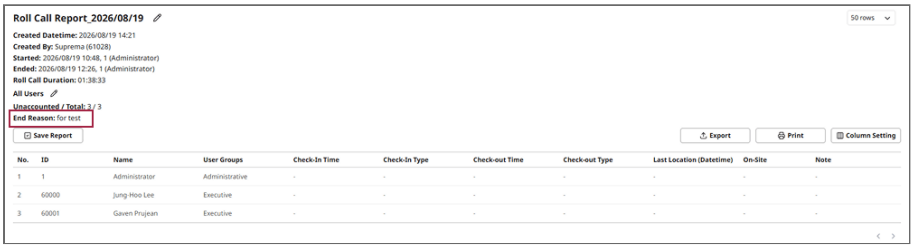


Generando el informe. El informe proporciona información de cada usuario, incluida la hora de entrada, la hora de salida, la última ubicación y las notas.



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

Revise **End Reason** en los informes de pase de lista con usuarios sin confirmar.



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

Configuración de Video

La función de ajustes de video de **BioStar X** permite gestionar de forma integrada el control de acceso y la seguridad por video. Al integrarse con un **Video Management System** (VMS), utilice potentes funciones de gestión de seguridad, como la supervisión de video en tiempo real, la grabación vinculada a eventos y la generación automática de marcadores.

> **Información**
>
> La licencia **Esencial** o superior habilita la función de ajustes de video mediante opciones adicionales. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Descripción general de los ajustes de video

Los ajustes de video constan de los siguientes tres pasos.

1 Integrar servidor VMS

Configure la conexión entre el servidor VMS y **BioStar X** y los certificados. Un paso esencial para crear un sistema integrado de gestión de seguridad por video. Para obtener más información, consulte Integrar VMS.

2 Configurar la Cámara

Seleccione las cámaras necesarias entre las conectadas al VMS y cree grupos para una gestión eficiente. Para obtener más información, consulte Configurar la Cámara.

3 Configurar reglas

Cree reglas que vinculen los eventos de acceso con video para utilizar funciones avanzadas, como marcadores automáticos y registro de eventos. Para más información, consulte Configurar Reglas de Video.

Funciones clave

- **Supervisión integrada**: Gestione el control de acceso y la seguridad por video desde una sola interfaz.
- **Registro automático de eventos**: Grabe automáticamente el video asociado y genere etiquetas cuando se produzcan eventos de acceso.
- **Búsqueda eficiente**: Busque rápidamente videos y reúna evidencia mediante marcadores y etiquetas de eventos.
- **Respuesta en tiempo real**: Verifique al instante las grabaciones de las cámaras pertinentes cuando surjan situaciones de seguridad.

Integrar VMS

El **Sistema de Gestión de Video** (VMS) es un sistema de gestión de video que integra y administra video de múltiples cámaras, lo que permite la grabación y la reproducción. La integración de BioStar X con VMS permite gestionar el control de acceso y la seguridad de video en una sola plataforma.

La integración con VMS ofrece las siguientes funciones.

- **Monitoreo en tiempo real**: Visualiza video en tiempo real de las cámaras conectadas a las puertas.
- **Gestión de eventos integrada**: Comprende las situaciones de seguridad enlazando los eventos de acceso con video.
- **Recopilación de evidencia eficiente**: Busca y reproduce rápidamente video grabado de momentos específicos.

- **Función de marcadores**: Agrega etiquetas de video a momentos de eventos importantes para facilitar su búsqueda y revisión.

Antes de comenzar

Antes de integrar el **Sistema de Gestión de Video** (VMS), verifica lo siguiente.

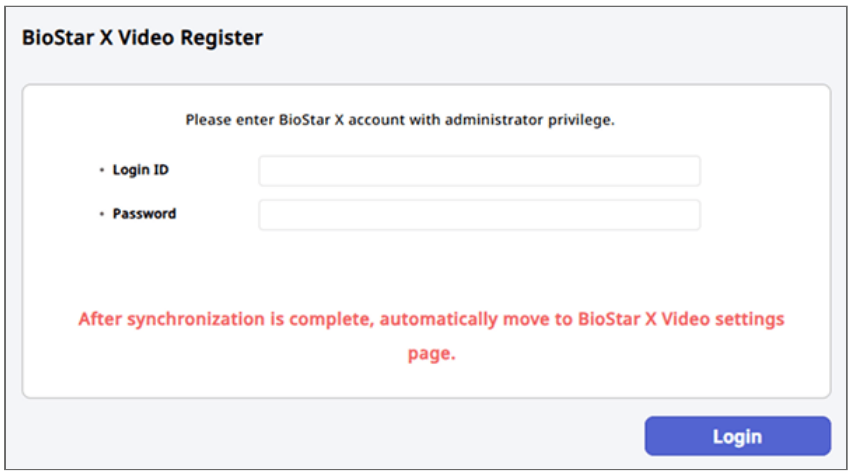
- La característica de integración con VMS está disponible como complemento para licencias **Essential** o superiores. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.
- Asegúrate de que el servidor VMS esté instalado y configurado correctamente. El servidor VMS debe estar en un estado que permita la conexión en línea con **BioStar X**.
- Utiliza un VMS compatible con **BioStar X**. Puede usar BioStar X VMS o las series de VMS **Nx Witness v5.1.5** y **v6.x.x**.
- Prepara la dirección IP, el número de puerto y la información de la cuenta de administrador del servidor VMS. Esta información es necesaria para conectar el servidor VMS con **BioStar X**.

Configuración de integración del servidor VMS

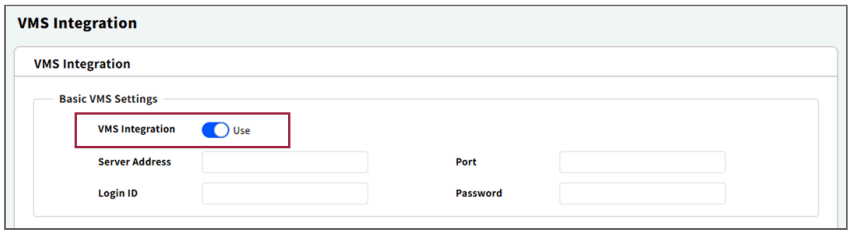
Sigue los pasos a continuación para integrar el servidor VMS con **BioStar X**.

1 Activar la integración de VMS

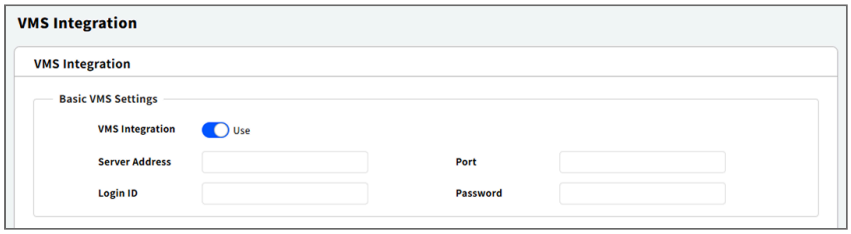
1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Video** → **VMS Integration** en la barra lateral izquierda.
3. Si es la primera vez que accedes, inicia sesión con la cuenta de administrador de **BioStar X**.



4. Establece la opción **VMS Integration** en **Use**.



5. Ingresa la información del servidor VMS.



- **Server Address**: Ingresa la dirección IP del servidor VMS.
- **Port**: Ingresa el número de puerto del servidor VMS.
- **Login ID**: Ingresa el ID de la cuenta de administrador del servidor VMS.
- **Password**: Ingresa la contraseña de la cuenta de administrador del servidor VMS.

6. Después de ingresar toda la información del servidor VMS, haz clic en el botón **Apply** en la parte inferior derecha de la pantalla.

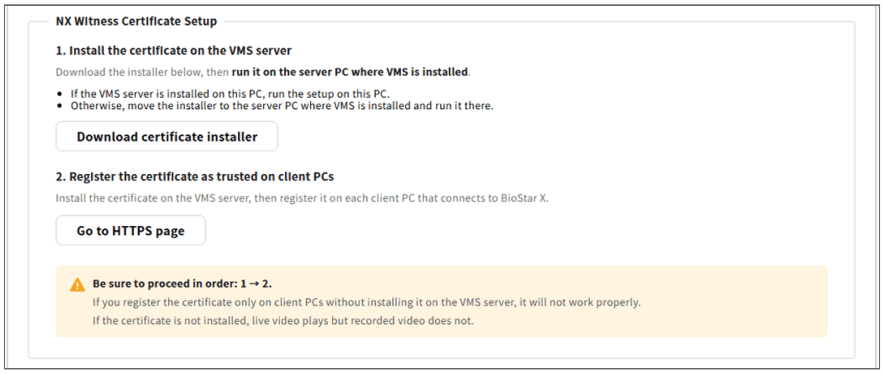
> **Información**
>
> - Si la integración con el servidor VMS falla y aparece un mensaje de error, verifica nuevamente la dirección del servidor y la información de la cuenta de administrador. También es necesario comprobar si el servidor VMS está en línea y si las conexiones de red están bloqueadas por la configuración del firewall.
> - Para obtener más información sobre la configuración en la sección **VMS Event/Bookmark**, consulte Configuración de eventos y marcadores de VMS.

2 Instalar el certificado en el servidor VMS

Para reproducir video grabado desde el servidor VMS, se debe usar el protocolo HTTPS. Los certificados SSL estándar se emiten para nombres de dominio, por lo que no son válidos si se accede al servidor VMS mediante su dirección IP. Por lo tanto, debes crear un certificado aparte que incluya la dirección IP del servidor VMS.

> **Información**
>
> Debes instalar un certificado tanto si el servidor VMS y **BioStar X** están instalados en el mismo servidor como si están en servidores distintos.

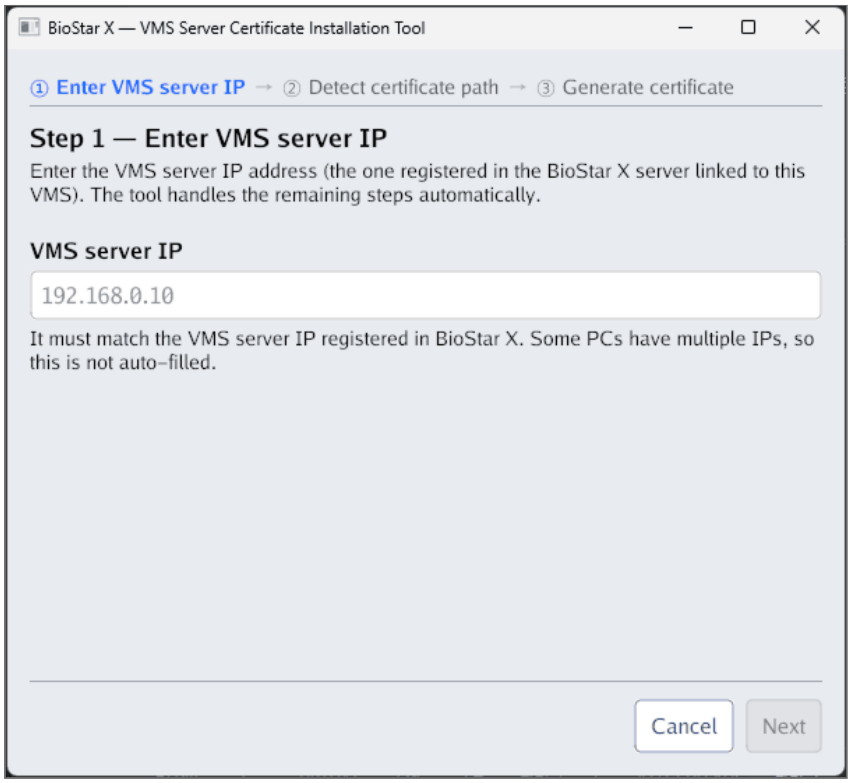
La sección **NX Witness Certificate Setup** está disponible solo cuando la opción **VMS Integration** está configurada en **Use**.



1. En el servidor donde está instalado VMS, haga clic en **Download certificate installer** para descargar el instalador del certificado.

2. Ejecute el archivo *vmsCertMaker.exe* descargado.

3. Ingrese la dirección IP en el campo **IP del servidor VMS**.

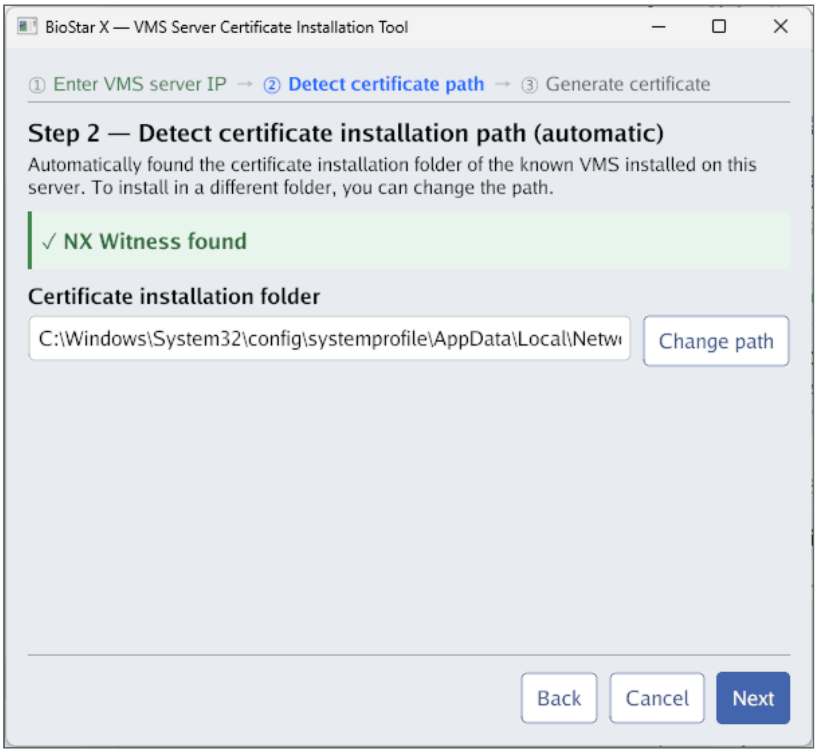


> Use el formato de dirección IPv4. por ejemplo, 192.168.0.10

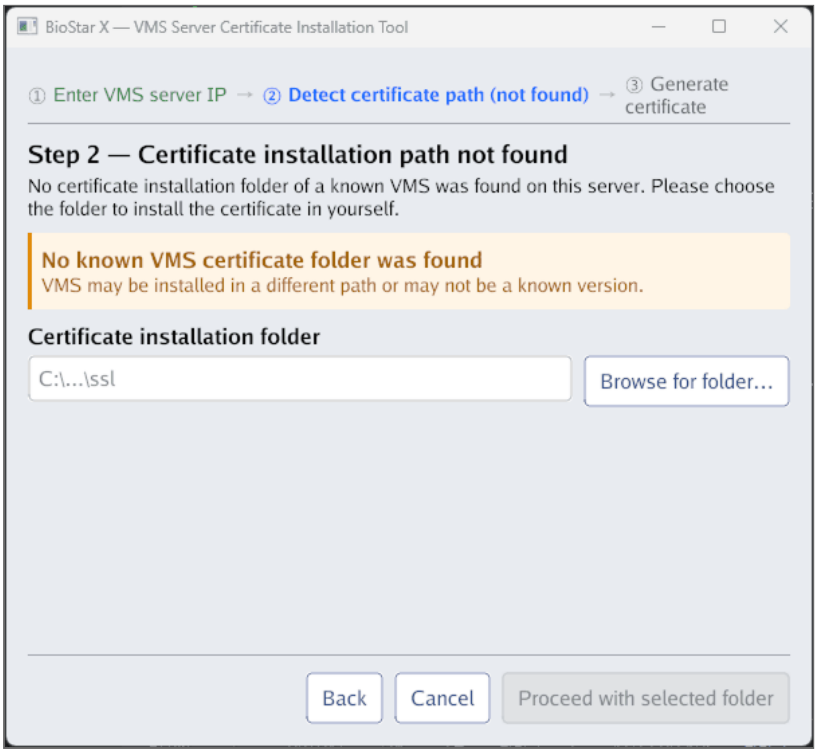
4. Ingrese una dirección IP con el formato correcto para habilitar el botón **Siguiente**. Haga clic en **Next**.

5. Seleccione la ruta de instalación del certificado VMS.

   - Para VMS compatibles, el instalador detecta la ruta de instalación automáticamente.

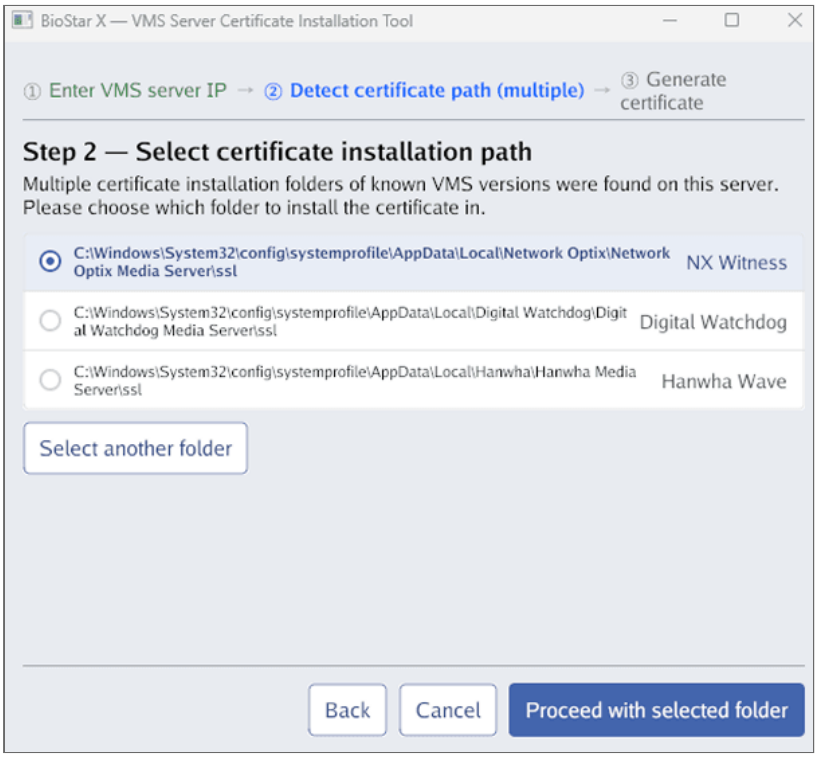


- Si el instalador no detecta la ruta de instalación automáticamente, haga clic en **Buscar carpeta** y seleccione la ruta manualmente.

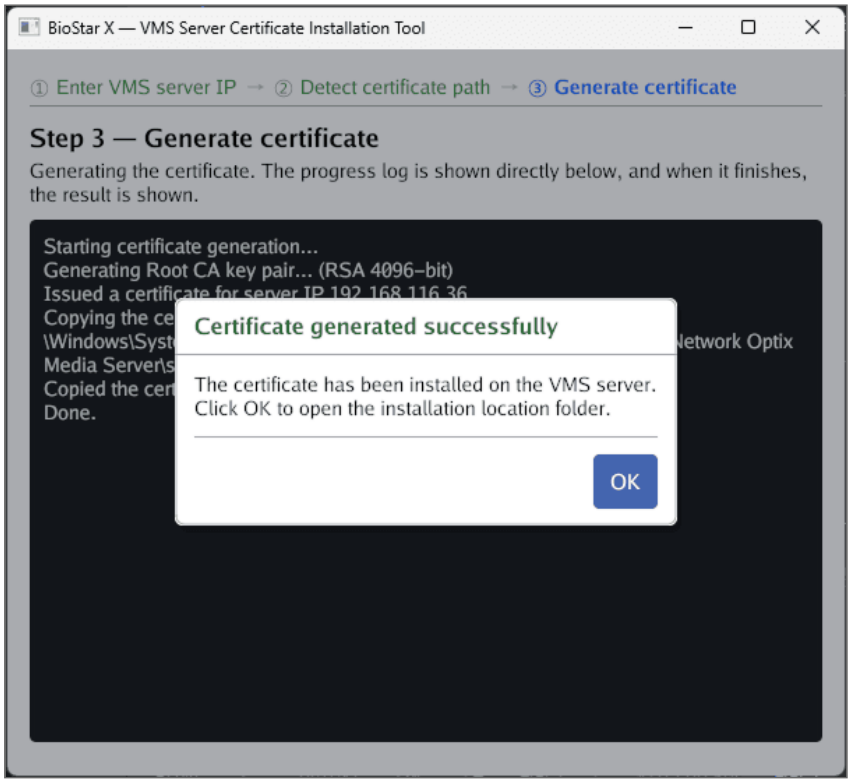


> La ruta de instalación del certificado puede variar según el sistema VMS. Consulte los ejemplos a continuación.
> - **BioStar 2 VMS**: *C:\Windows\System32\config\systemprofile\AppData\Local\Suprema Inc\Suprema Inc. Media Server\ssl*
> - **Digital Watchdog**: *C:\Windows\System32\config\systemprofile\AppData\Local\Digital Watchdog\Digital Watchdog Media Server\ssl*
> - **Hanwha Wave**: *C:\Windows\System32\config\systemprofile\AppData\Local\Hanwha\Hanwha Media Server\ssl*
> - **NX**: *C:\Windows\System32\config\systemprofile\AppData\Local\Network Optix\Network Optix Media Server\ssl*

- Si existen varias rutas de certificados de VMS, aparecen todas. Haga clic en **Seleccionar otra carpeta** y seleccione la ruta deseada.

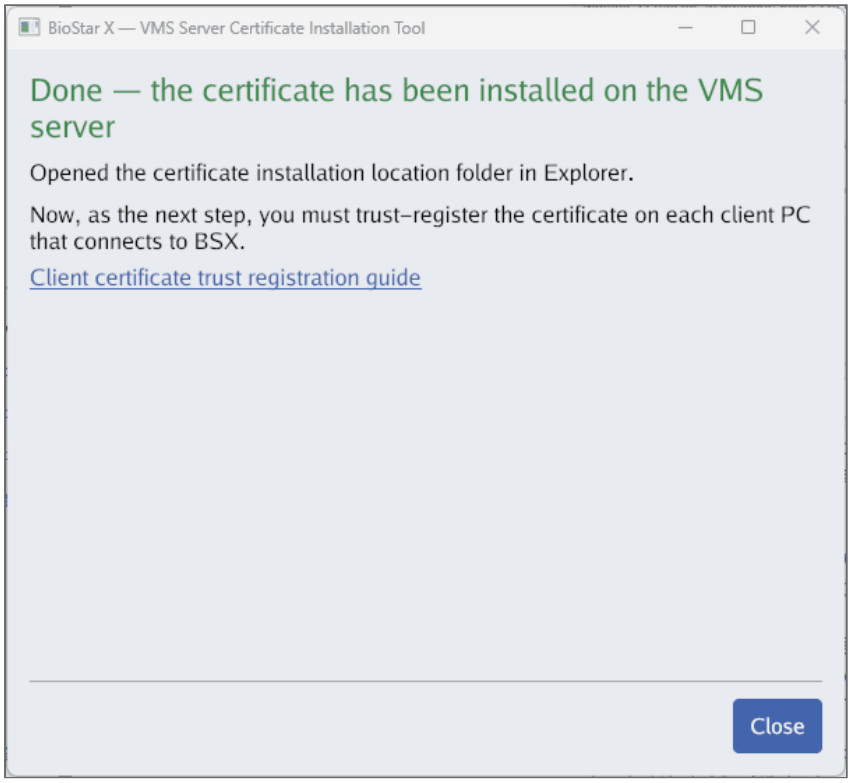


6. Haga clic en **Siguiente** o en **Continuar con la carpeta seleccionada**.
7. Cuando finaliza la generación del certificado, aparece el mensaje **Certificado generado correctamente**.



8. La ruta de instalación del certificado aparece al hacer clic en **Aceptar**. Confirme que el archivo de certificado (*cert.pem*) existe.

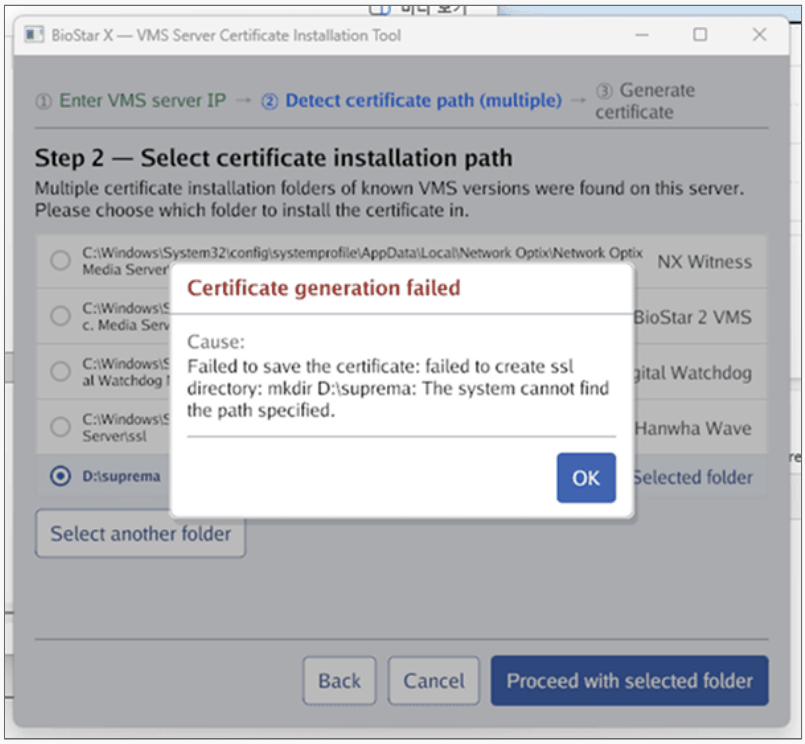
9. Cuando finaliza la instalación del certificado, haga clic en **Cerrar**.



10. Reinicia el servidor VMS.

Información

Si falla la instalación del certificado, el mensaje muestra el motivo. Revise el mensaje y luego realice la acción requerida.



3 Instalar el certificado en la PC cliente

Si se presentan las siguientes situaciones, instala el certificado desde el servidor VMS en el PC cliente para resolver el problema.

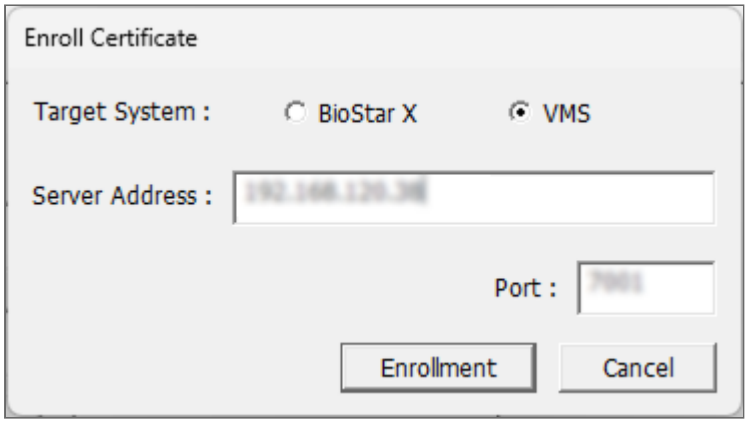
- Al acceder al **Sistema de Gestión de Video** (VMS) a través del navegador y aparece una advertencia "No es seguro"
- Cuando el video en tiempo real se reproduce en la página **Monitoring** pero el video grabado no se reproduce

Precaución

Inscribir el certificado solo en la PC cliente, sin instalarlo en el servidor VMS, impide el funcionamiento normal.

---

1. Acceda a **BioStar X** desde el navegador web.
2. Descargue el instalador del certificado HTTPS (*cert-register.zip*) desde la pantalla de inicio de sesión o desde **Settings** → **System** → **HTTPS**.
3. Descomprima el archivo descargado y ejecute el archivo **cert-register.exe**. Aparece la ventana **Enroll Certificate**.
4. Seleccione **VMS** en **Target System** e ingrese la siguiente información.



- **Server Address**: dirección IP del servidor VMS
- **Puerto**: número de puerto del servidor VMS (predeterminado: 7001)

5. Haga clic en **Inscripción**.
6. Verifique el mensaje de advertencia de seguridad y haga clic en **Yes**.

Reinicie el navegador web y verifique que el video grabado del servidor VMS se reproduzca normalmente en la página **Monitoring**.

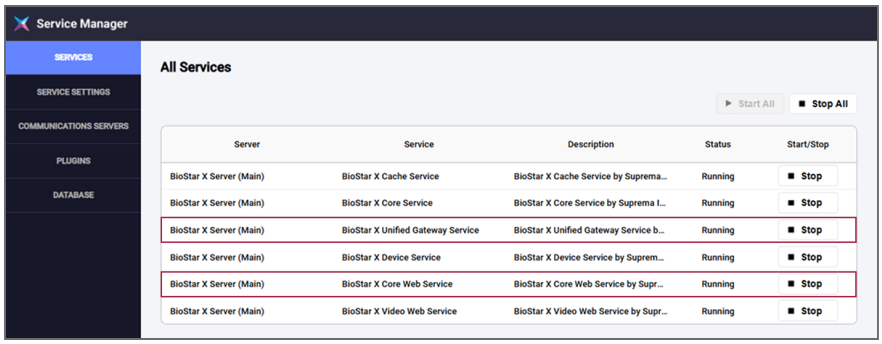
4 Revise y ajuste la cámara

Si el servidor VMS se integra correctamente, verifica las cámaras conectadas en el menú **Video** → **Video**. Para obtener más información, consulte Configurar la Cámara.

Solución de problemas

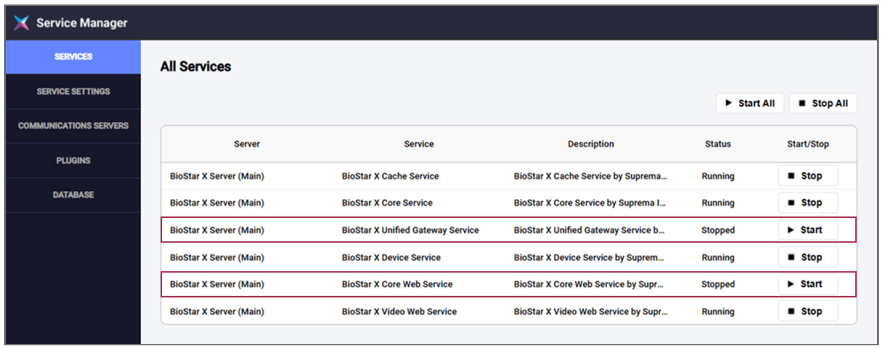
Si el servicio no funciona después de la primera integración con el servidor VMS, reinícielo manualmente de la siguiente manera.

1. Haz clic en Inicio → **BioStar X** → **BioStar X Service Manager** en Windows.
2. En la lista **Todos los servicios**, haga clic en **Detener** para los siguientes servicios.



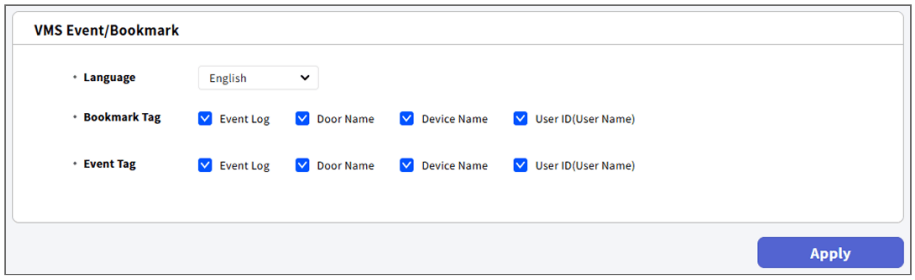
- **BioStar X Unified Gateway Service**
- **BioStar X Core Web Service**

3. Cuando el estado del servicio solicitado cambie de **Pendiente** a **Detenido**, haga clic en **Iniciar** para reiniciar el servicio.



Configuración de eventos y marcadores de VMS

Transmita etiquetas de marcador e información de etiquetas de eventos al servidor VMS integrado. En este punto, elija transmitir también los registros de eventos, nombres de puertas, nombres de dispositivos e ID de usuario. Seleccione las opciones deseadas y haga clic en **Apply** en la parte inferior derecha de la pantalla.



- **Language**: Elija el idioma de las etiquetas de eventos y marcadores que se enviarán al servidor VMS. Seleccione coreano o inglés.
- **Bookmark Tag**: Las etiquetas de marcador permiten ubicar y revisar fácilmente los videos almacenados en el servidor VMS mediante designaciones y nombres para una identificación rápida. Seleccione la información que se enviará con la etiqueta de marcador.
- **Event Tag**: Transmita los eventos ocurridos en momentos específicos al servidor VMS para su registro. Seleccione la información que se enviará con la etiqueta de evento.

Información

- Para obtener más información sobre la función de marcadores en VMS, consulte el siguiente enlace.
- Para obtener más información sobre la función de eventos en VMS, consulte el siguiente enlace.
- Si las etiquetas de marcadores o eventos incluyen los siguientes caracteres, el sistema los elimina antes de enviarlas al servidor VMS.
  - Etiqueta de evento: `\` `'` `,` `#` `%` `=` `&` `<` `>`
  - Etiqueta de marcador: `<` `'`

Desconectar la integración del servidor VMS

Siga los siguientes pasos para desconectar el servidor VMS integrado. Al desconectar la integración de VMS se eliminarán todos los ajustes de video, cámaras registradas y reglas.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Video** → **VMS Integration** en la barra lateral izquierda.

3. Configure la opción **VMS Integration** en **Not Use**.
4. Haga clic en **Apply** en la esquina inferior derecha de la pantalla.
5. Revise el contenido de la ventana de mensajes y haga clic en **Yes**.

Configurar la Cámara

Después de completar la integración con VMS, selecciona y configura las cámaras que se usarán en BioStar X. La configuración adecuada de las cámaras permite utilizar las siguientes funciones de gestión de seguridad.

- **Supervisión opcional**: Agrega a **BioStar X** solo las cámaras necesarias de todas las cámaras del VMS.
- **Gestión eficiente**: Gestiona las cámaras de forma sistemática agrupándolas por ubicación o propósito.

> **Información**
>
> - Para obtener más información sobre cómo integrarse con el servidor VMS, consulte Integrar VMS.
> - Se requiere el permiso de grupo de cámaras para agregar cámaras o configurar grupos. Para obtener más información sobre los permisos de los grupos de cámaras, consulte Configuración de permisos de grupos de cámaras.

Configuración y gestión de cámaras

Después de la integración con VMS, configura y gestiona las cámaras en el menú **Settings** → **Video** → **Video**.

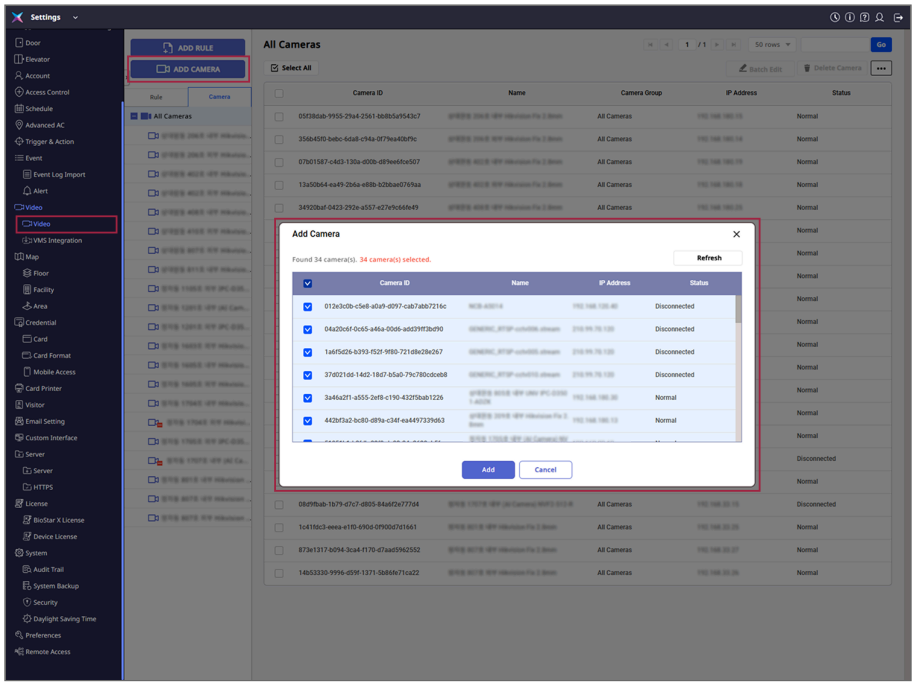
Añadir cámara

Cuando esté integrado con VMS, agrega a **BioStar X** las cámaras conectadas al servidor VMS y reproduce video en vivo y grabaciones en la página **Monitoring**.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.
3. Haz clic en **ADD CAMERA**.
4. Cuando aparezca la ventana **Add Camera**, selecciona las cámaras que quieras excluir de la lista.

   Si la cámara deseada no aparece, haz clic en **Refresh** para actualizar la lista de cámaras.
5. Después de seleccionar las cámaras, haz clic en **Add** en la esquina inferior derecha de la pantalla.

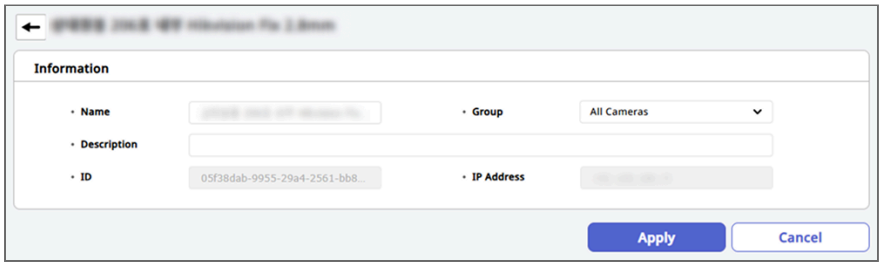
Verifica las cámaras añadidas en la lista de cámaras.



Editar información de la cámara

Edita la información de las cámaras añadidas. Cambia el nombre, grupo, descripción, etc., de la cámara.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.
3. Haz clic en la pestaña **Camera** en la esquina superior izquierda de la pantalla.
4. Haz clic en la cámara que deseas editar en la lista de cámaras.
5. Cuando se muestre la pantalla con la información de la cámara, edita los elementos deseados.



6. Después de editar toda la información de la cámara, haz clic en **Apply** en la esquina inferior derecha de la pantalla.

> **Información**
> El ID y la dirección IP de la cámara no se pueden modificar.

Eliminar cámara

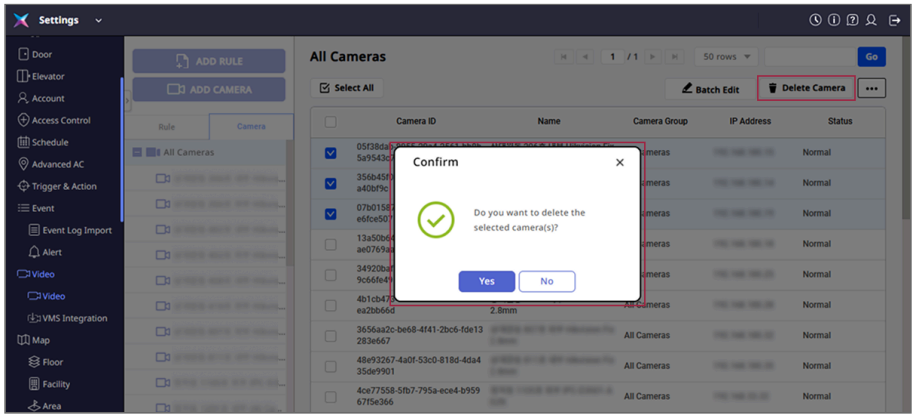
Elimina las cámaras añadidas.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.

3. Haz clic en la casilla ubicada a la izquierda de la cámara que deseas eliminar en la lista de cámaras. Selecciona más de una cámara.

4. Haz clic en **Delete Camera** en la esquina superior derecha de la pantalla.

5. Revisa el mensaje y haz clic en **Yes**.



Información

Si la cámara que deseas eliminar está incluida en una regla, no podrás eliminarla. Quita la cámara de la regla e inténtalo de nuevo. Para obtener más información sobre la creación y gestión de reglas, consulte Configurar Reglas de Video.

Configuración y gestión de grupos de cámaras

Puedes agrupar varias cámaras para gestionarlas de manera sistemática según su ubicación o finalidad. Sigue los pasos que aparecen a continuación para crear y gestionar grupos de cámaras.

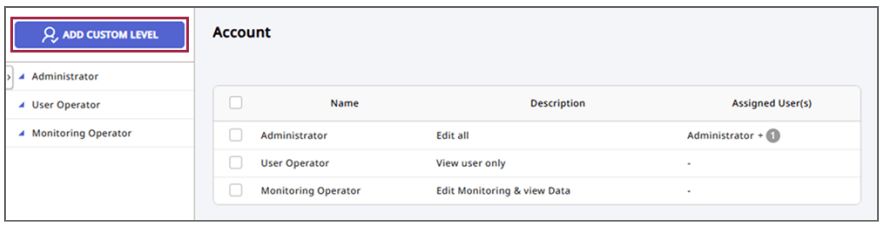
Configuración de permisos de grupos de cámaras

Los administradores necesitan el permiso de grupo de cámaras para añadir cámaras o configurar grupos. Los administradores del sistema, los administradores de usuarios y los administradores de monitoreo tienen acceso a todos los grupos de cámaras. Si necesitas una configuración de permisos distinta, agrega un permiso personalizado para configurar el acceso a los grupos de cámaras.

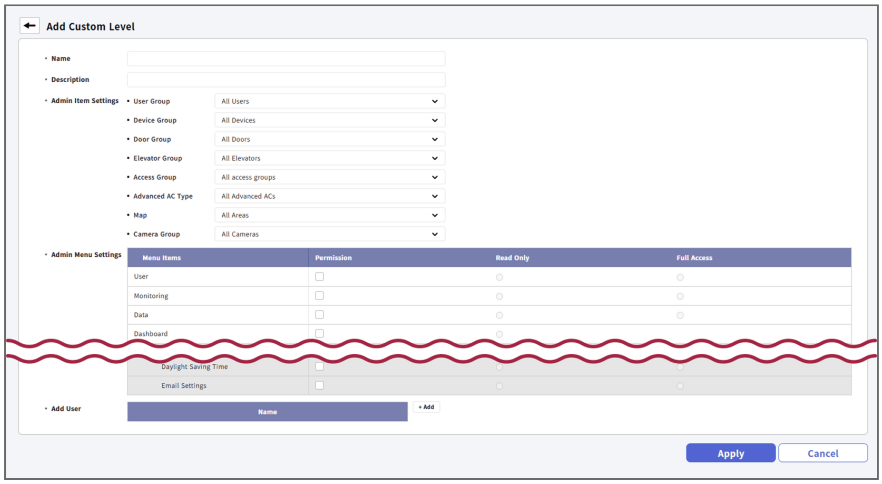
1. Haz clic en **Settings** en la página **Launcher**.

2. Haga clic en **Account** → **Account** en la barra lateral izquierda.

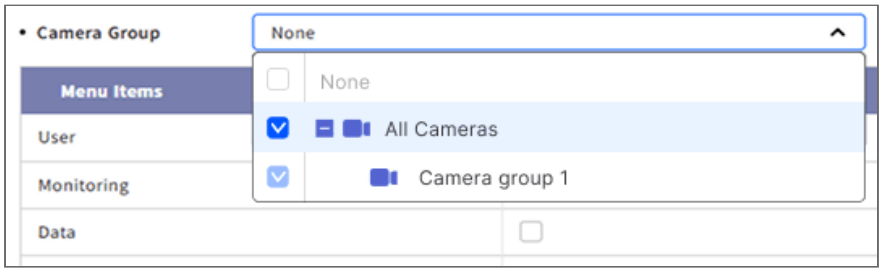
3. Haga clic en **Add Custom Level**.



4. Ingrese un nombre y una descripción para el permiso recién creado.



5. En **Admin Item Settings**, bajo **Camera Group**, selecciona el grupo de cámaras al que asignar permisos.



   - Selecciona **All Cameras** para otorgar permisos a todos los grupos de cámaras.
   - Para otorgar permisos a un grupo de cámaras individual, selecciona el grupo deseado de la lista de grupos de cámaras. Puedes seleccionar uno o más grupos.

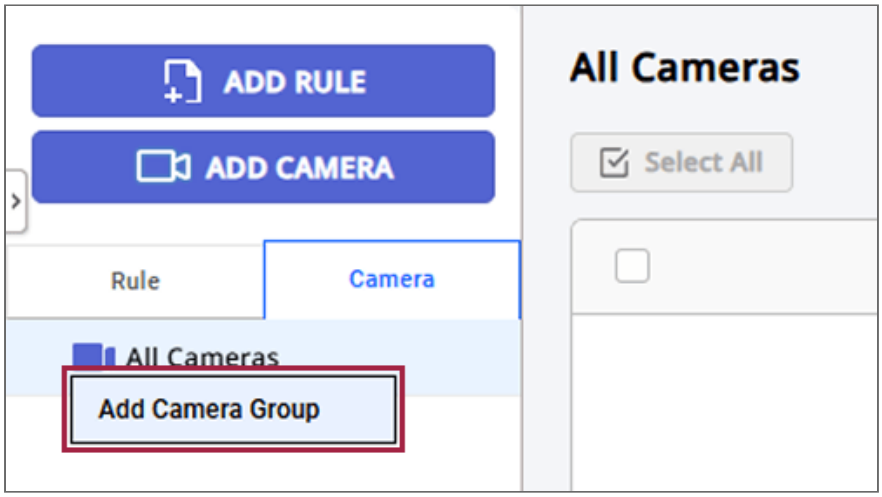
6. En **Add User**, haz clic en **+ Add** y selecciona los usuarios a los que asignar permisos.
7. Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.

> **Información**
> Si no tienes permiso para un grupo de cámaras específico, no podrás ver las cámaras de ese grupo.

Agregar grupo de cámaras

Agrupa varias cámaras para gestionarlas añadiendo un grupo de cámaras.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.
3. Haz clic en la pestaña **Camera** en la esquina superior izquierda de la pantalla.
4. Selecciona **All Cameras** y haz clic con el botón derecho.



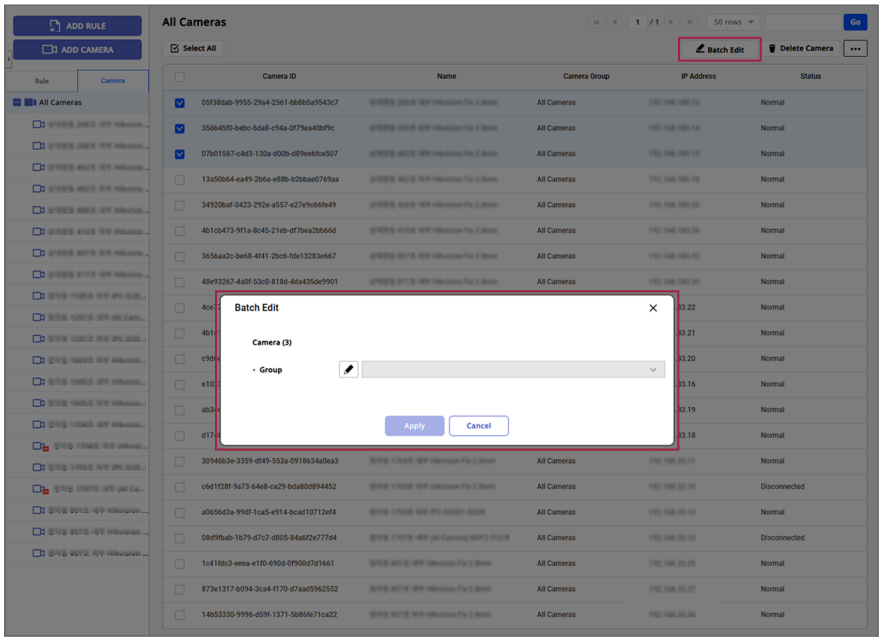
5. Haz clic en **Add Camera Group** en el menú emergente.
6. Ingresa el nombre de grupo deseado y presiona la tecla `Enter`.

> **Información**
>
> - Crea grupos de cámaras con hasta 8 subgrupos.
> - Los nombres de grupos de cámaras pueden tener hasta 48 caracteres.
> - Al seleccionar un grupo de cámaras en la lista, solo se mostrarán las cámaras que pertenecen a ese grupo.

Agregar varias cámaras al grupo

Añade más de una cámara al grupo.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.
3. Haz clic en la casilla ubicada a la izquierda de las cámaras que se añadirán al grupo en la lista de cámaras. Selecciona más de una cámara.
4. Si seleccionas más de una cámara, se activa **Batch Edit** en la esquina superior derecha de la pantalla. Haz clic en **Batch Edit**.



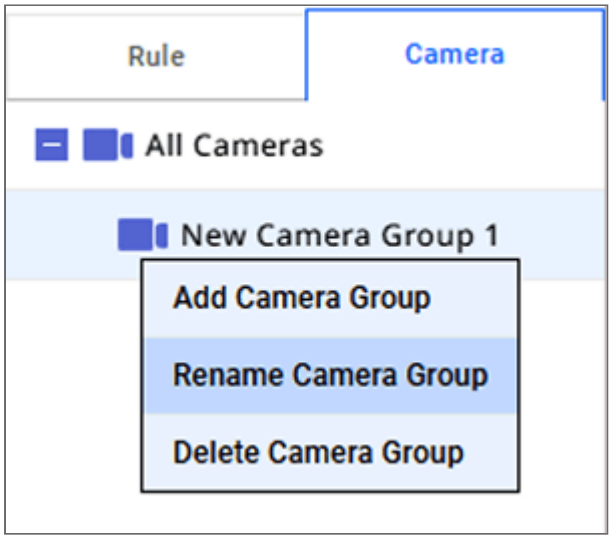
5. Cuando aparezca la ventana **Batch Edit**, haz clic en el botón **Group** del elemento ✎.
6. Selecciona el grupo deseado de la lista.
7. Haz clic en **Apply**.

> **Información**
> Desde la lista de cámaras de la pestaña **Camera**, también añade cámaras al grupo mediante arrastrar y soltar.



Editar nombre del grupo de cámaras

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.
3. Haz clic en la pestaña **Camera**.
4. Selecciona el grupo que deseas renombrar y haz clic con el botón derecho.
5. Haz clic en **Rename Camera Group** en el menú emergente.



6. Ingresa el nombre de grupo deseado y presiona la tecla `Enter`.

Eliminar grupo de cámaras

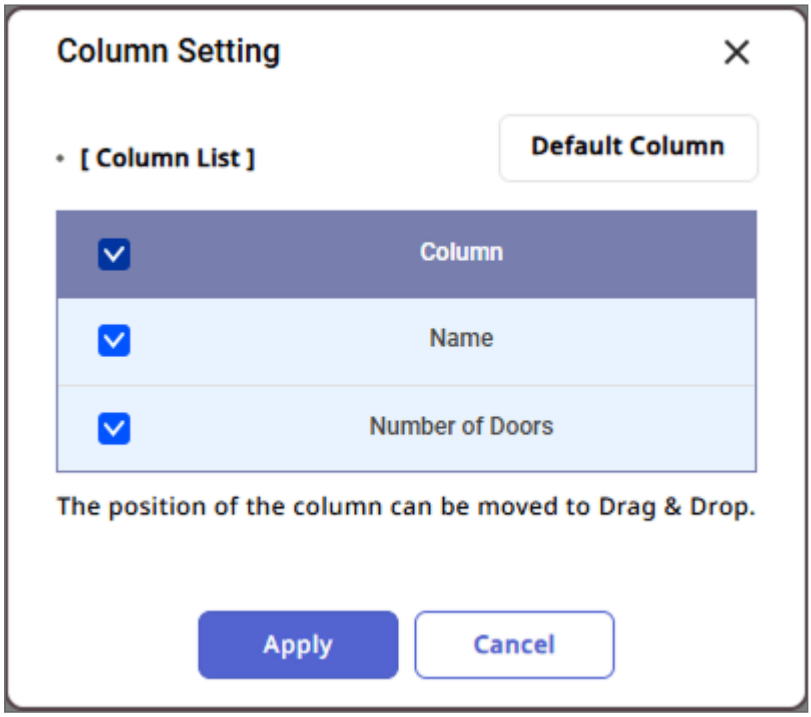
1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.
3. Haz clic en la pestaña **Camera**.
4. Selecciona el grupo que deseas renombrar y haz clic con el botón derecho.
5. Haz clic en **Delete Camera Group** en el menú emergente.
6. Lee el mensaje de advertencia y haz clic en **Yes**.

> **Información**
> Si el grupo de cámaras contiene cámaras, no podrás eliminar el grupo. Mueve las cámaras que pertenecen al grupo a otro grupo o quítalas del grupo e inténtalo de nuevo.

Configuración de columnas

Agrega columnas, cambia su orden en la lista o configúralas como ocultas.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.
3. En la esquina superior derecha de la lista **All Cameras**, haz clic en ••• → **Column Setting**.
4. Cuando aparezca la ventana **Column Setting**, selecciona las casillas de las columnas que quieras mostrar para agregarlas o configúralas como ocultas. También cambia el orden de las columnas mediante arrastrar y soltar.



5. Cuando hayas terminado de cambiar la configuración de columnas, haz clic en **Ok**.

> **Información**
> Haz clic en **Default Column** para inicializar la configuración de columnas.

Configurar Reglas de Video

Las reglas son ajustes para enviar eventos y marcadores al servidor VMS combinando los eventos que ocurren en la cámara y la puerta. Una configuración adecuada de las reglas de video permite utilizar varias funciones de gestión de seguridad.

- **Creación automática de marcadores**: Crea marcadores automáticamente cuando ocurren eventos de acceso específicos para encontrar fácilmente videos importantes.
- **Supervisión eficiente**: Supervisa las imágenes en vivo de las cámaras conectadas a las puertas y comprueba los eventos al instante cuando ocurren.
- **Gestión integrada de eventos**: Vincula eventos de acceso e imágenes para comprender de manera integral las situaciones de seguridad.

> **Información**
>
> - La característica de reglas de video está disponible con una licencia **Esencial** o superior mediante opciones adicionales. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.
> - Para vincular una puerta a una cámara, debes tener permiso del grupo al que pertenece la cámara. Para obtener más información sobre cómo configurar los permisos de los grupos de cámaras, consulte Configurar la Cámara.

Agregar regla

1. Haz clic en **Settings** en la página **Launcher**.

2. Haz clic en **Video** → **Video** en la barra lateral izquierda.

3. Haz clic en **ADD RULE** en la parte superior izquierda de la pantalla.

Cuando aparezca la pantalla **Add New Rule**, configura las reglas según las siguientes instrucciones. Haz clic en **Apply** en la parte inferior de la pantalla para completar y guardar todos los ajustes.

Ingresar información de la regla

En la sección **Information**, ingresa el nombre y la descripción de la nueva regla.



> **Información**
> **Description** es opcional. Úsalo para ingresar una descripción sencilla y comprender fácilmente el propósito o las características de la regla.

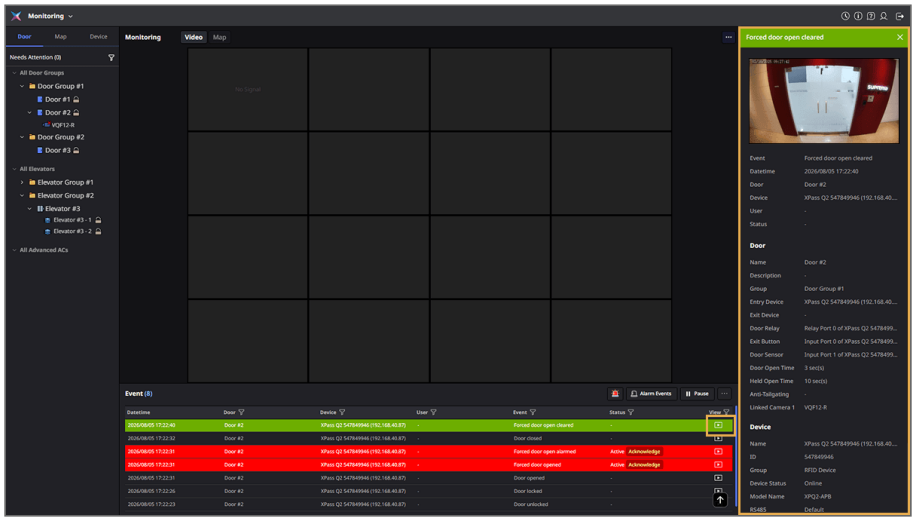
Ajustes de registro de video

Video Log es una función que graba automáticamente video antes y después de que ocurra un evento específico. Conserva las grabaciones durante un período determinado para comprender el contexto antes y después de los eventos.



- **Video Log**: Define el uso de Video Log en la regla actual.
  - **Enabled**: Graba automáticamente video desde antes y después de que ocurran los eventos.
  - **Disabled**: Desactiva la función Video Log.
- **Video Log Length**: Define el rango de grabación alrededor de diez segundos antes y después del evento. Se puede configurar hasta un máximo de 60 segundos.

Habilita la opción **Video Log**. El icono de registro de video (▶) aparece junto a los eventos en el panel de eventos de la pantalla de Supervisión. Al hacer clic en el elemento de evento con el icono de registro de video, se muestra información detallada en el lado derecho de la pantalla, lo que le permite ver el video del momento en que ocurrió el evento específico. Compruebe el video del momento en que ocurrió un evento específico.

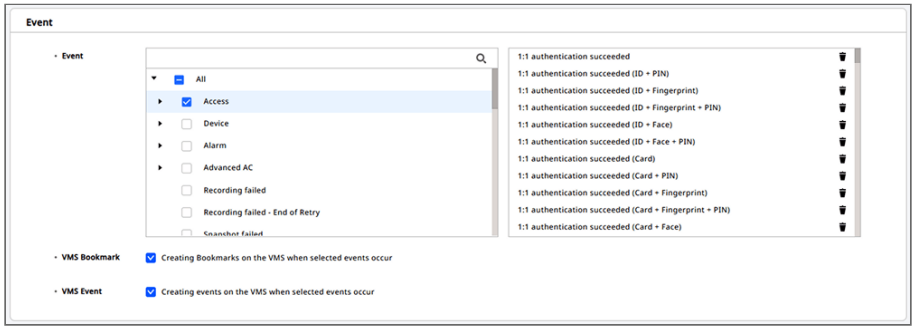


Información

Cuanto mayor sea el rango establecido de **Video Log Length**, más espacio de almacenamiento puede requerir. Ten en cuenta el rendimiento del sistema y la capacidad de almacenamiento al definir una duración adecuada.

Ajustes de eventos que se registrarán en VMS

En la sección **Event**, puedes seleccionar los eventos que se registrarán en el servidor VMS y definir si se enviarán marcadores o eventos.



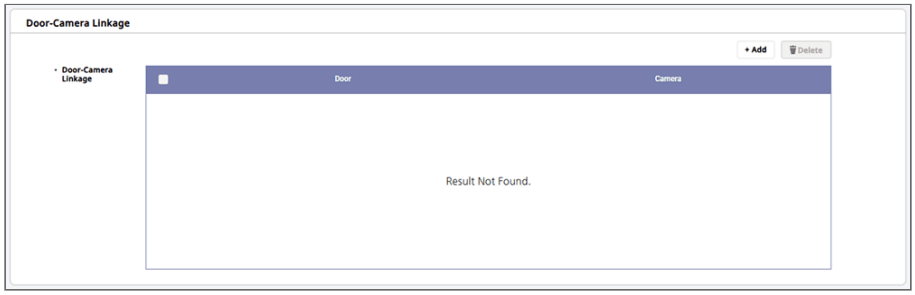
- **Event**: Selecciona el tipo de evento que se enviará al servidor VMS. Cuando selecciones el evento deseado de la lista de eventos de la izquierda, se añadirá a la lista de la derecha.
- **VMS Bookmark**: Puedes definir si se creará un marcador en el servidor VMS cuando ocurra el evento seleccionado en la lista.
- **VMS Event**: Puedes definir si se crearán registros de eventos en el servidor VMS cuando ocurra el evento seleccionado en la lista.

Información

- Seleccionar eventos no es obligatorio.
- Puedes encontrar rápidamente el evento deseado utilizando el campo de búsqueda en la parte superior de la lista de eventos de la izquierda.
- Para eliminar un evento de la lista de la derecha, haz clic en .
- Puedes establecer el idioma del mensaje al enviar marcadores y eventos al servidor VMS. Para obtener más información, consulta Integrar VMS.

Enlazar puerta y cámara

En la sección **Door-Camera Linkage**, enlaza puertas con cámaras para enviar grabaciones de las cámaras conectadas junto con los eventos que ocurren en las puertas al servidor VMS. Esto permite ver fácilmente las grabaciones relacionadas con eventos de acceso.



1. Haz clic en **+ Add** en la parte superior derecha.
2. Cuando aparezca la ventana **Add Linkage**, selecciona la puerta y luego la cámara asociada.



3. Después de seleccionar la puerta y la cámara, haz clic en **Add**.

Consulta en la lista las cámaras enlazadas a la puerta.



Información

- Los administradores que no tienen permisos en un grupo de cámaras no pueden ver ni seleccionar las cámaras de dicho grupo. Para obtener más información sobre cómo configurar los permisos de los grupos de cámaras, consulte Configurar la Cámara.
- Una sola puerta puede tener hasta cuatro cámaras añadidas.
- Las puertas incluidas en una regla no pueden usarse en otras reglas.
- Puede vincular cámaras a varias puertas sin restricciones y también puede reutilizar cámaras ya vinculadas a otras puertas.
- Para eliminar la regla de enlace de puertas y cámaras, marca la casilla de las reglas que vas a eliminar. Luego, haz clic en **Delete** en la parte superior derecha.
- Las cámaras enlazadas a las puertas pueden visualizarse como una subestructura de las puertas en la lista de puertas de la página **Monitoring**. Para obtener más información, consulta Verifica el estado.
- Haz clic en **Apply** en la parte inferior de la pantalla para completar y guardar todos los ajustes.

Editar regla

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.
3. Haz clic en la regla que deseas editar en la lista **All Rules**.
4. Cuando aparezca la pantalla de edición de la regla, modifica los elementos deseados.
5. Para guardar la regla modificada, haz clic en **Apply** en la parte inferior derecha de la pantalla.

> **Información**
> Para obtener más información sobre cada sección de la pantalla de edición de reglas, consulta Agregar regla.

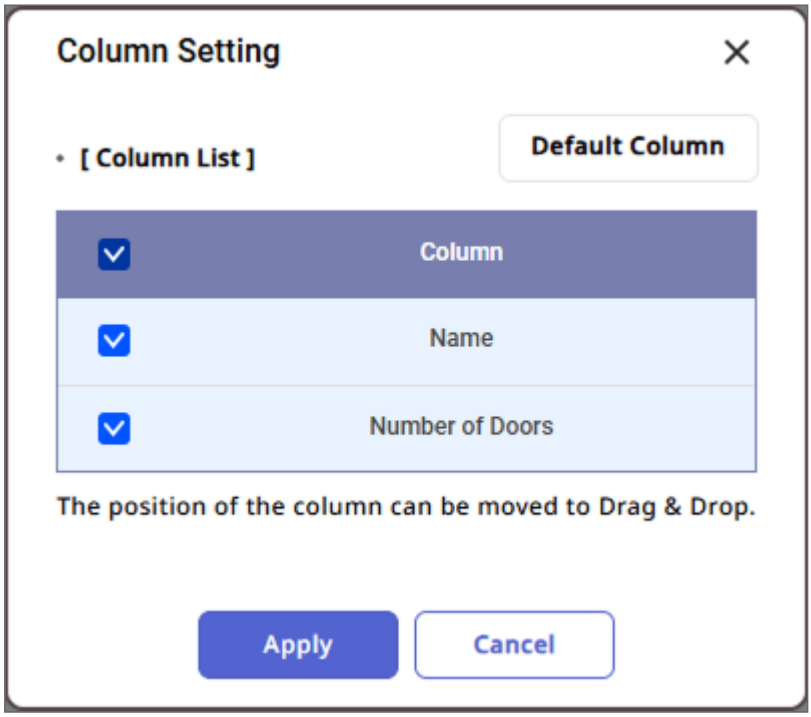
Borrar Regla

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.
3. Marca la casilla de la regla que deseas eliminar en la lista **All Rules**. Se puede seleccionar una o más reglas.
4. Haz clic en **Delete Rule** en la parte superior derecha de la pantalla.
5. Revisa el mensaje y haz clic en **Yes**.

Configuración de columnas

Agrega columnas, cambia su orden en la lista o configúralas como ocultas.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Video** → **Video** en la barra lateral izquierda.
3. En la parte superior derecha de la lista **All Rules**, haz clic en ••• → **Column Setting**.
4. Cuando aparezca la ventana **Column Setting**, selecciona las casillas de las columnas que quieras mostrar para agregarlas o configúralas como ocultas. También cambia el orden de las columnas mediante arrastrar y soltar.



5. Cuando hayas terminado de cambiar la configuración de columnas, haz clic en **Ok**.

> **Información**
> Haz clic en **Default Column** para inicializar la configuración de columnas.

Administrar Mapa

Los ajustes de mapa permiten configurar y administrar pisos, instalaciones y zonas en conjunto con el mapa. Utilice esta función para ver un mapa segmentado por zonas, instalaciones y pisos en la página **Monitoring**.

> **Información**
> Para obtener más información sobre cómo monitorear mapas, consulte Monitorear Mapa.

Configurar Pisos

Configura los pisos antes de configurar zonas y instalaciones. Carga el plano del piso como imagen y coloca puertas y cámaras para la gestión visual. Después de configurar un piso, verifica las puertas y cámaras de ese piso en la página **Monitoring**.



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

Información

- Registra puertas antes de configurar pisos. Para obtener más información sobre el registro de puertas, consulte Registrar Puerta.
- Para obtener más información sobre cómo monitorear mapas, consulte Monitorear Mapa.
- Las características "Agregar piso" y "Ajustes de piso" están disponibles con una licencia **esencial** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Agregar piso

Carga un plano del piso o una imagen 3D en vista aérea para agregar un piso y colocar puertas y cámaras.

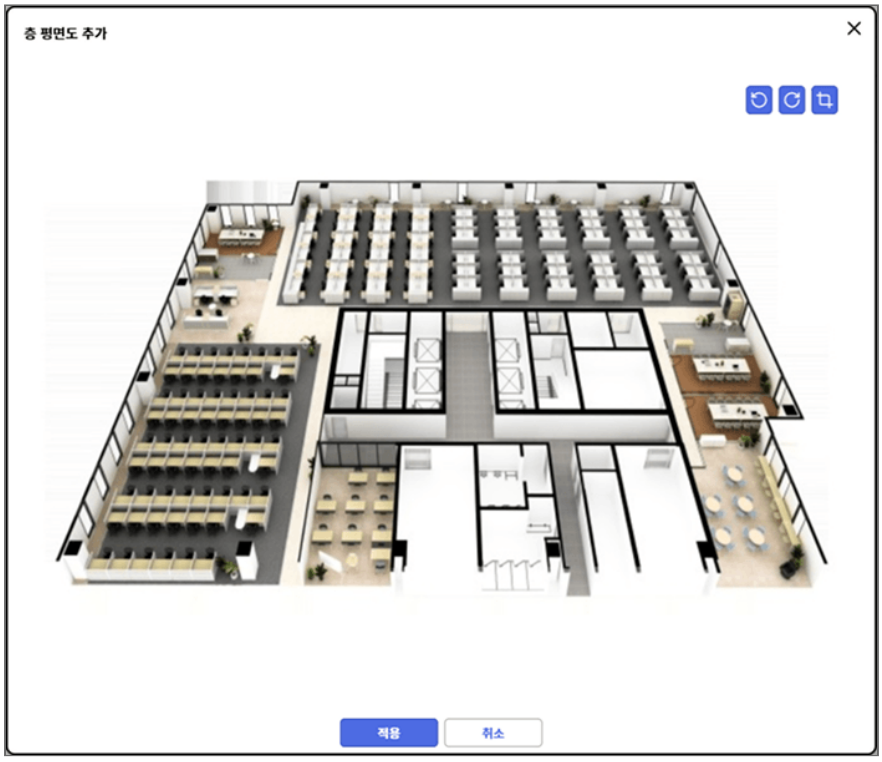
1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Map** → **Floor** en la barra lateral izquierda.
3. Haz clic en **New Floor** en la esquina superior derecha de la pantalla de lista de pisos.



4. Ingresa el nombre y la descripción del piso que deseas agregar en la sección **Information** de la pantalla **Add New Floor**.
5. Haz clic en **Floor Plan** en la sección **Floor Configuration** o arrastra y suelta la imagen para cargarla.

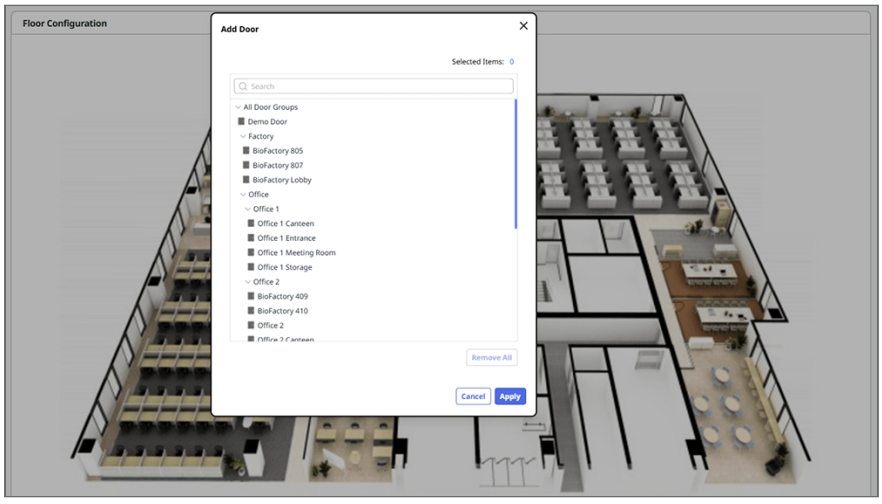
   Los formatos de imagen admitidos son PNG, JPEG y JPG.

6. Confirma la imagen cargada en la ventana **Add Floor Plan** y continúa con la configuración.

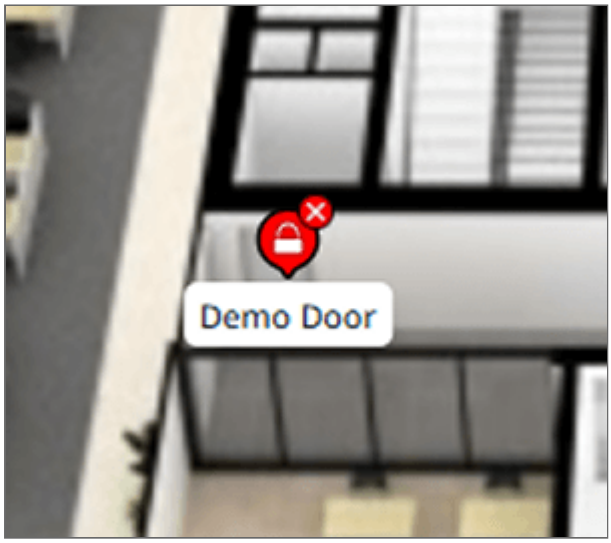


- Para rotar la imagen, haz clic en ↺ o ↻.
- Para recortar la imagen, haz clic en ⧉.

7. Después de completar la configuración de la imagen, haz clic en **Apply**.
8. Para agregar una puerta a la imagen cargada en la sección **Floor Configuration**, haz clic derecho en la ubicación deseada de la imagen y selecciona **Add Door**.
9. Cuando aparezca la ventana **Add Door**, selecciona una de las puertas registradas.

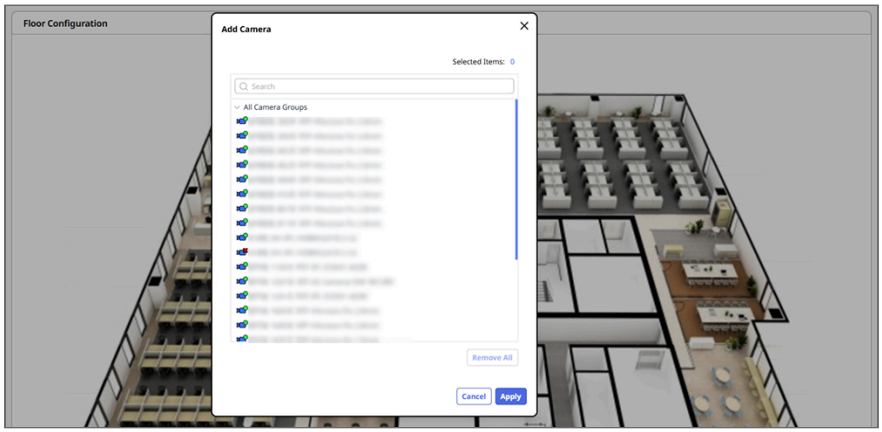


10. Para colocar la puerta en la imagen, haz clic en **Apply**.



11. Para agregar una cámara a la imagen cargada, haz clic derecho en la ubicación deseada de la imagen y selecciona **Add Camera**.

12. Cuando aparezca la ventana **Add Camera**, selecciona una de las cámaras registradas.



13. Para colocar la cámara en la imagen, haz clic en **Apply**.



14. Coloca puertas y cámaras adicionales según sea necesario en el piso real.

15. Después de completar todos los ajustes y guardar el piso configurado, haz clic en **Apply**.

Información

- Para cambiar la posición de las puertas y cámaras colocadas en el piso, haz clic y arrastra la puerta o cámara correspondiente hasta la ubicación deseada.
- Para obtener más información sobre los íconos y el estado de las puertas y las cámaras en el piso, consulta Monitorear Mapa.

Modificar configuración del piso

Puedes modificar el diseño del piso con las puertas y cámaras añadidas. Al modificar el diseño del piso, puedes cambiar o eliminar las posiciones de puertas y cámaras.

1. Haz clic en **Settings** en la página **Launcher**.
2. En la barra lateral izquierda, haz clic en **Map** → **Floor**.
3. Haz clic en el piso que deseas modificar de la lista.

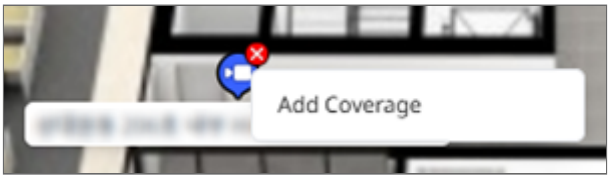
Después de completar todos los ajustes y guardar el piso configurado, haz clic en **Apply**.

Eliminar puerta/cámara

Haz clic en el ícono de la puerta o cámara que deseas eliminar de la imagen del piso. Puedes eliminar la puerta o cámara correspondiente.

Configurar rango de captura de la cámara

Haz clic derecho en la cámara a la que deseas ajustar el rango de captura en la imagen del piso. Haz clic en **Add Coverage** en el menú emergente.



- Para cambiar el rango de captura, mueve el puntero del mouse dentro del área verde. Cuando el puntero del mouse cambie a forma de cruz, haz clic y arrastra hasta la ubicación deseada manteniendo presionado el botón del mouse.



- Para ajustar el área de cobertura, sujeta el borde del rango y arrastra para redimensionar.

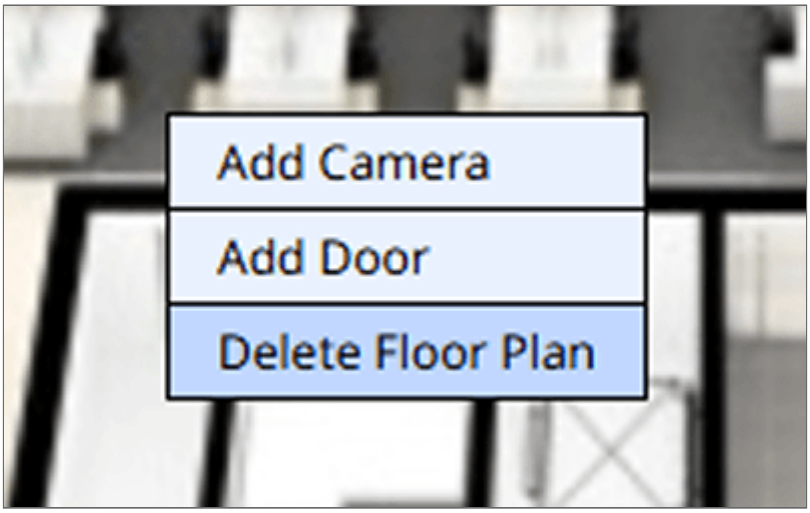


- Para eliminar el área de cobertura, haz clic en el ícono .

> **Precaución**
> Los ajustes realizados por el usuario son solo funciones proporcionadas para la comodidad de la gestión de seguridad y no reflejan el rango de captura real de la cámara.

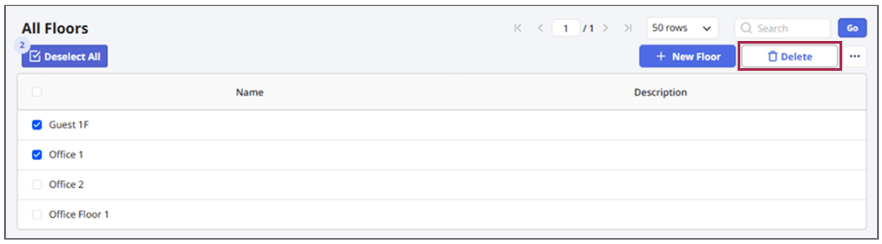
Eliminar imagen del piso

Para eliminar la imagen del piso, haz clic derecho sobre la imagen del piso y selecciona **Delete Floor Plan** en el menú emergente.



Eliminar piso

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Map** → **Floor** en la barra lateral izquierda.
3. Marca la casilla del piso que deseas eliminar de la lista. Puedes seleccionar más de un piso.

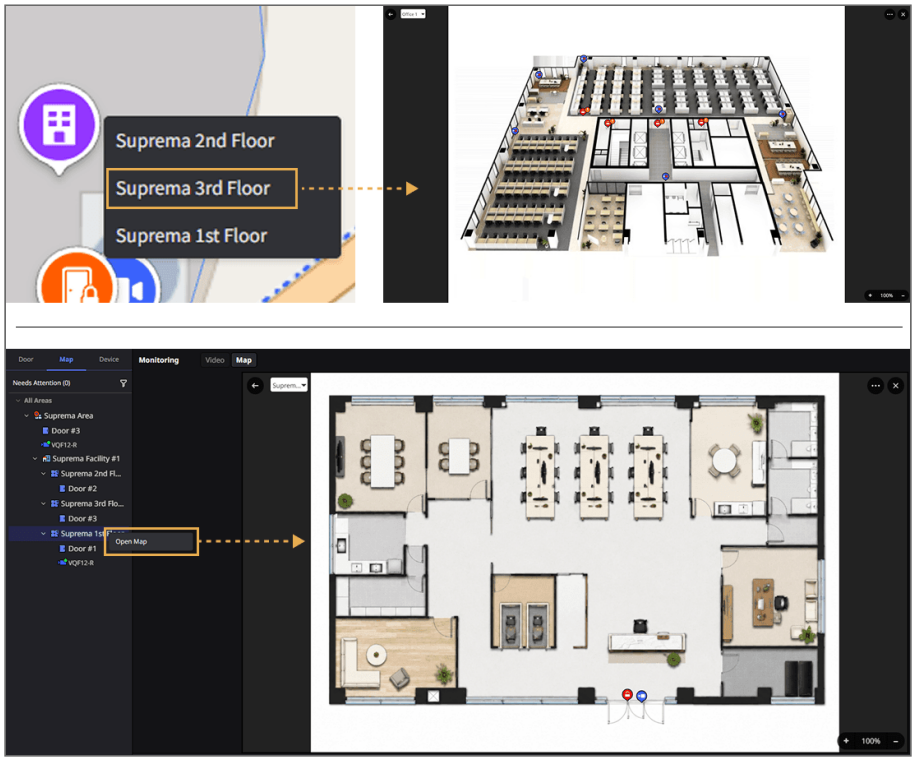


4. Haz clic en **Delete** en la parte superior derecha de la pantalla.

Los pisos seleccionados se eliminarán de la lista. Los pisos eliminados no se pueden recuperar.

Configurar Instalación

Configura la instalación y organiza los pisos. Organiza los pisos de forma secuencial para representar la distribución real de la instalación. La configuración de instalaciones permite seleccionar las instalaciones ubicadas en el mapa en la página **Monitoring** y acceder a cada piso para supervisión.



Información

- Registra los pisos antes de configurar las instalaciones. Para obtener más información sobre cómo registrar pisos, consulte Configurar Pisos.
- Para obtener más información sobre cómo monitorear mapas, consulte Monitorear Mapa.
- La característica para agregar y configurar instalaciones está disponible con una licencia **Essential** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Agregar instalación

Sigue estos pasos para diseñar la estructura agregando pisos a la instalación.

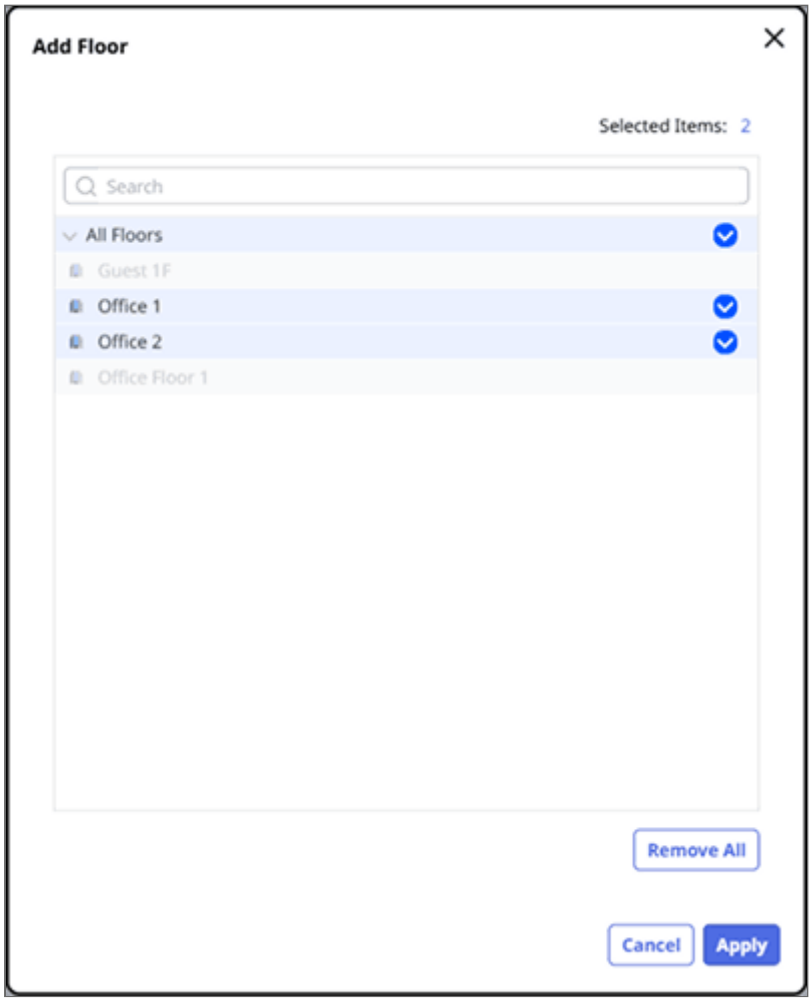
1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Map** → **Facility** en la barra lateral izquierda.
3. Haz clic en **New Facility** en la parte superior derecha de la pantalla de lista de instalaciones.



4. Ingresa el nombre y la descripción de la instalación que deseas agregar en la sección **Information** de la pantalla **Add New Facility**.
5. Haz clic en **Add** en **Facility Configuration**.



6. Cuando aparezca la ventana **Add Floor**, selecciona el piso que deseas agregar de la lista de pisos.



- También puedes buscar pisos ingresando palabras clave en el campo de entrada.
- Para seleccionar todos los pisos, elige **All Floors**.

7. Si seleccionaste todos los pisos, haz clic en **Apply**.
8. Para revisar los pisos agregados a la lista de puertas de acceso y cambiar el orden, arrastra ⠿ en la columna **Order** para cambiar el orden.
9. Para finalizar la configuración de la instalación y guardar, haga clic en **Apply** en la parte inferior derecha de la pantalla.

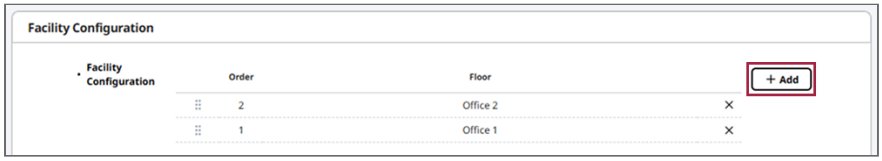
Modificar instalación

Agregar pisos a instalaciones existentes

Agrega pisos a una instalación ya creada.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Map** → **Facility** en la barra lateral izquierda.

3. Selecciona la instalación a la que deseas agregar pisos de la lista de instalaciones.
4. Haz clic en **Add** en **Facility Configuration**.



5. Cuando aparezca la ventana **Add Floor**, haz clic en la casilla de verificación del piso que deseas seleccionar.
6. Si seleccionaste todos los pisos, haz clic en **Apply**.
7. Para revisar los pisos agregados a la lista de puertas de acceso y cambiar el orden, arrastra ⠿ en la columna **Order** para cambiar el orden.
8. Para finalizar la configuración de la instalación y guardar, haga clic en **Apply** en la parte inferior derecha de la pantalla.

Eliminar pisos de la instalación

Elimina pisos de una instalación ya creada.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Map** → **Facility** en la barra lateral izquierda.
3. Selecciona la instalación de la que deseas eliminar pisos en la lista de instalaciones.
4. Haz clic en ✕ del piso que deseas eliminar en **Facility Configuration**.
5. Para completar la eliminación del piso y guardar, haga clic en **Apply** en la parte inferior derecha de la pantalla.

Eliminar instalación

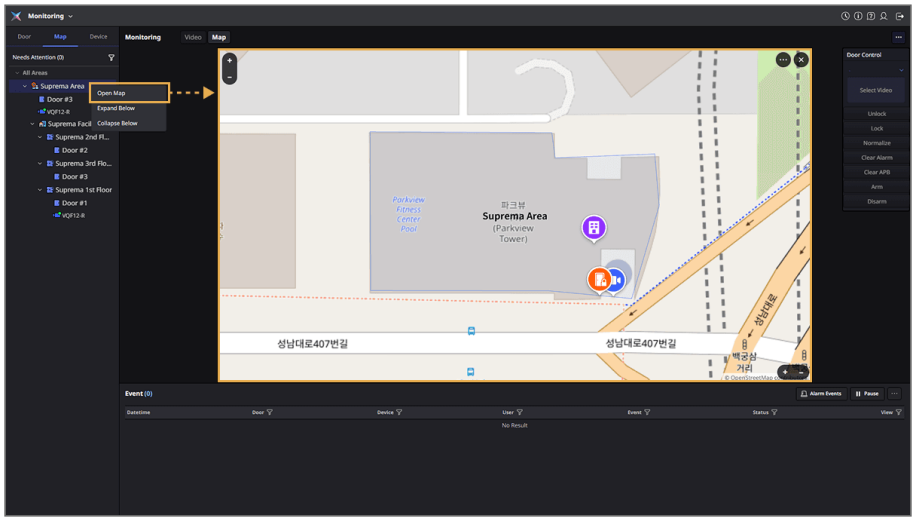
1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Map** → **Facility** en la barra lateral izquierda.
3. Haz clic en la casilla de verificación de la instalación que deseas eliminar en la lista de instalaciones.



4. Haz clic en **Delete** en la parte superior derecha de la pantalla.
5. Cuando aparezca la ventana de mensaje de confirmación, haz clic en **Yes**.

Configurar Área

Completa la configuración de pisos e instalaciones para definir el área. Verifica las áreas seguras en el mapa. La configuración de zonas permite acceder y supervisar las instalaciones y los pisos de la zona correspondiente en la página **Monitoring**.



Información

- Registra pisos e instalaciones antes de configurar las zonas. Para obtener más información sobre cómo registrar pisos e instalaciones, consulta lo siguiente:
  - Configurar Pisos
  - Configurar Instalación
- Para obtener más información sobre cómo monitorear mapas, consulte Monitorear Mapa.
- La característica de añadir zonas y ajustes está disponible como opción adicional con una licencia **Esencial** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Añadir zona

Configura y administra las zonas de las áreas de seguridad que gestionas actualmente mediante el mapa.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Map** → **Area** en la barra lateral izquierda.
3. Haz clic en **New Area** en la parte superior derecha de la pantalla de lista de áreas.



4. Ingresa el nombre y la descripción del área que deseas añadir en la sección **Information** de la pantalla **Add New Area**.
5. Define la ubicación de la zona que vas a añadir en el mapa, en la sección **Area Configuration**.
6. Haz clic derecho en el mapa y selecciona **Set Area**.

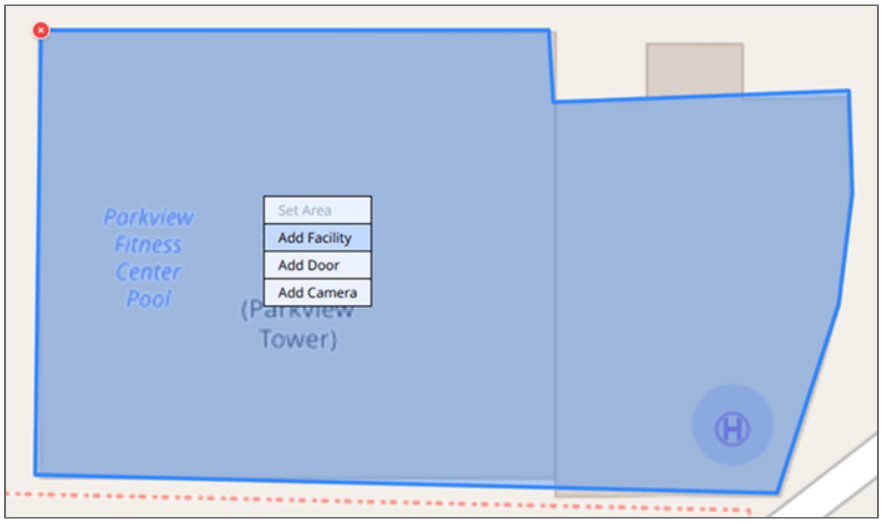


7. Define la zona con la forma deseada. Haz clic para comenzar a dibujar y arrastra para definir la zona.



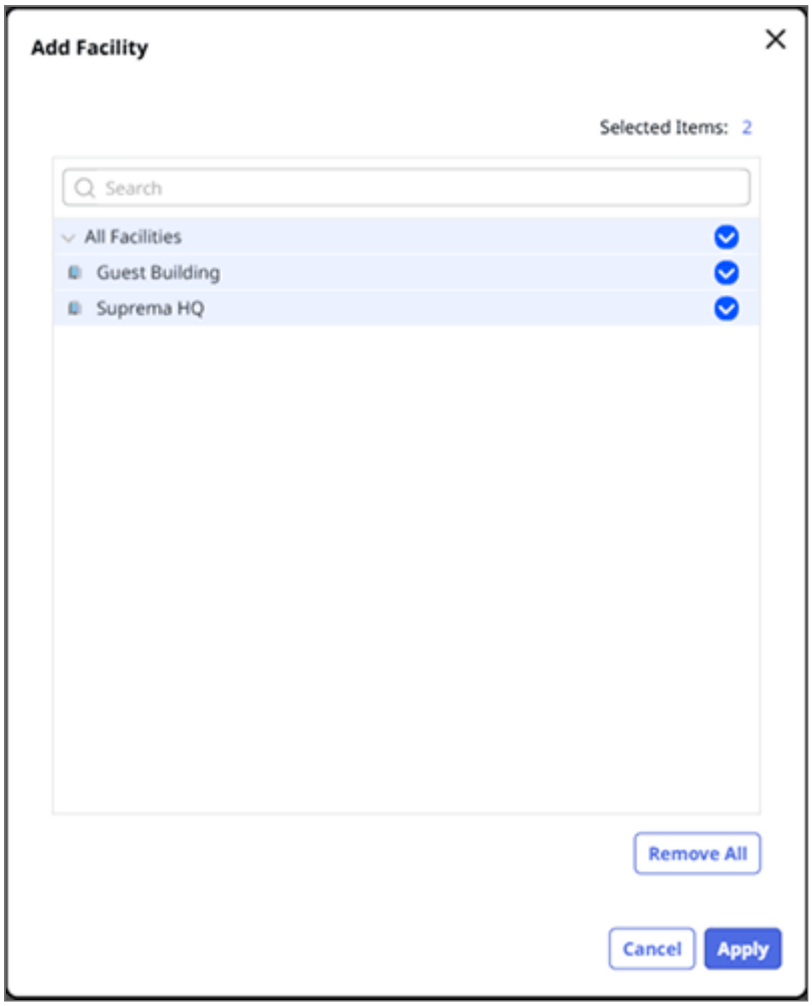
> Para restablecer el área, debes eliminar la zona configurada. Haz clic en para eliminar el área.

8. Para añadir instalaciones al área configurada, haz clic derecho y selecciona **Add Facility**.



> Al añadir una zona, debes configurar al menos una instalación, entrada o cámara.
> - Para añadir una entrada, haz clic derecho y selecciona **Add Door**.
> - Para añadir una cámara, haz clic derecho y selecciona **Add Camera**.

9. Cuando aparezca la ventana **Add Facility**, selecciona la instalación que deseas añadir y haz clic en **Apply**.



> Al añadir una entrada o una cámara, también aparecerá la ventana **Add Door** o **Add Camera**. Selecciona el elemento que quieres añadir y haz clic en **Apply**.

10. Una vez completados los ajustes del área, haz clic en **Apply** en la parte inferior derecha de la pantalla.

> **Información**
>
> - Busca la ubicación deseada usando el campo de entrada en la parte superior izquierda del mapa. Haz clic en para volver a la ubicación actual.
>
> 
>
>
> - Al añadir una zona en el mapa, solo puede establecerse como un único polígono. Al definir una zona, asegúrate de que los puntos de inicio y fin sean los mismos. Una vez configurada, la forma de la zona no se puede cambiar. Para modificar la zona, debes eliminarla y volver a añadirla.
> - Las posiciones de las instalaciones, entradas y cámaras añadidas pueden cambiarse mediante arrastrar y soltar en el mapa.

Editar zona

Elimina y reconfigura zonas existentes o añade o elimina instalaciones, entradas y cámaras.

Restablecer zona

Para restablecer una zona en el mapa, debes eliminar la zona existente y volver a añadirla.

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Map** → **Area** en la barra lateral izquierda.
3. Selecciona la zona que deseas restablecer de la lista de zonas.
4. En el mapa, en la sección **Area Configuration**, haz clic en en la esquina superior izquierda del área ya creada.



5. Haz clic derecho en el mapa y selecciona **Set Area** en el menú emergente.

6. Define el área según sea necesario y haz clic en **Apply** en la parte inferior derecha para guardar.

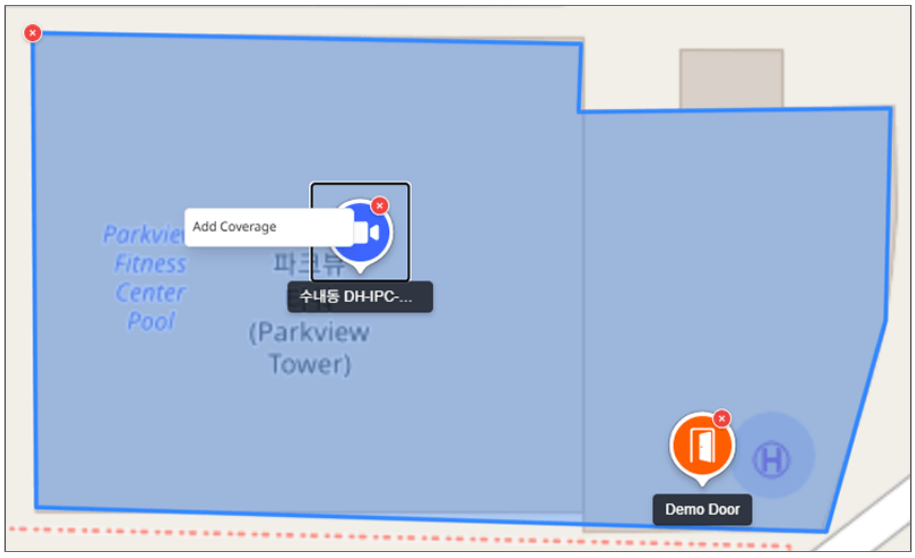
Eliminar instalación/entrada/cámara

Haz clic en la instalación, entrada o cámara que quieras eliminar en el mapa. Aparecerá el ícono . Haz clic en el ícono para eliminar la instalación seleccionada.

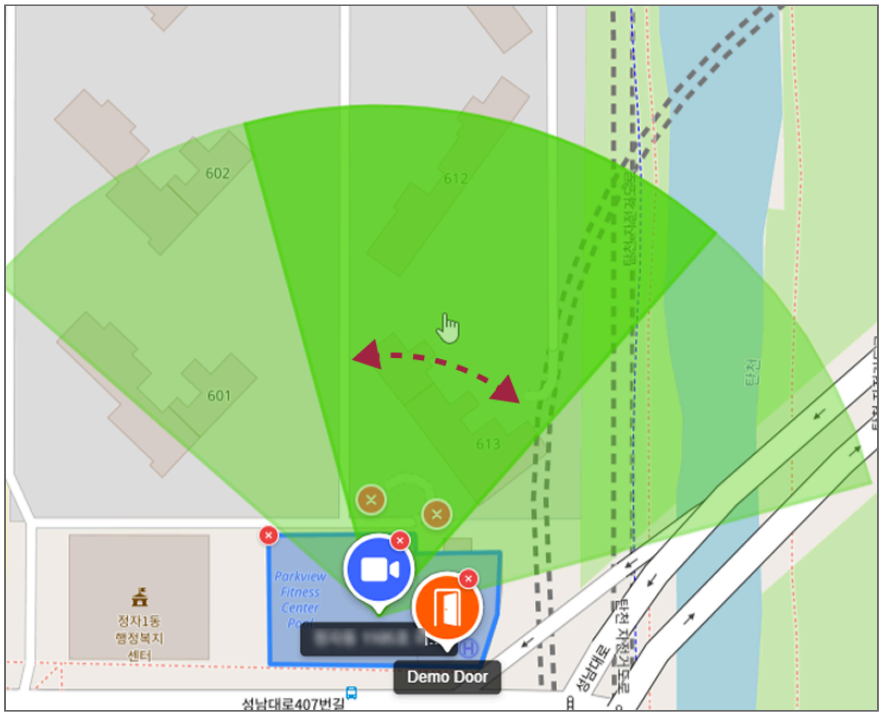


Configurar rango de captura de la cámara

Define el área de cobertura de la cámara en el mapa. Haz clic derecho en el ícono donde está ubicada la cámara y selecciona **Add Coverage**.



- Para cambiar el rango de disparo, haz clic y arrastra el rango de la zona verde en la dirección deseada.



- Para ajustar el área de cobertura, sujeta el borde del rango y arrastra para redimensionar.



- Para eliminar el área de cobertura, haz clic en el ícono .

> **Precaución**
> Los ajustes realizados por el usuario son solo funciones proporcionadas para la comodidad de la gestión de seguridad y no reflejan el rango de captura real de la cámara.

Eliminar zona

1. Haz clic en **Settings** en la página **Launcher**.

2. Haz clic en **Map** → **Area** en la barra lateral izquierda.
3. Marca la casilla de la zona que deseas eliminar en la lista de zonas.



4. Haz clic en **Delete** en la parte superior derecha de la pantalla.
5. Cuando aparezca la ventana de mensaje de confirmación, haz clic en **Yes**.

Configurar Visitante

Configura los sitios y PC de visita. Además, configura los términos y condiciones para los visitantes. Crea los campos de información que necesites de los visitantes mediante el campo personalizado de visitante.

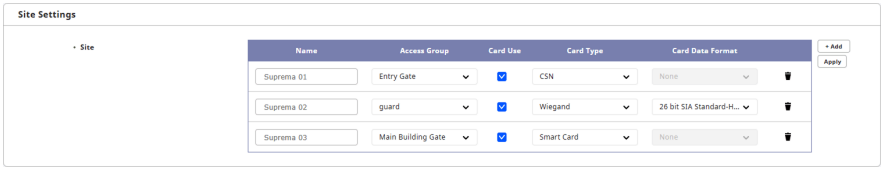
> **Información**
>
> - La configuración **Visitor** está disponible mediante opciones adicionales con una licencia **Esencial** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.
> - Activa la opción **Automatic User Synchronization** o **Use Server Matching** para usar **Visitor**. Para obtener más información, consulte Configuración Detallada del Servidor.

Configuración de visitante

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Visitor** → **Visitor** en la barra lateral izquierda.
3. Sigue las instrucciones a continuación para configurar los ajustes de visitante.

1 Configuración del sitio de visitante

Define el grupo de acceso que se utilizará en la PC de visita y la PC de administración de cada sitio. También define si se usarán tarjetas. Si usas tarjetas, configura también el tipo de tarjeta y el formato de datos de tarjeta.



- **Name**: Define el nombre del sitio.

> **Información**
>
> – Se pueden ingresar hasta 48 caracteres para el nombre del sitio.

- **Access Group**: Selecciona el grupo de acceso que se asignará al visitante.

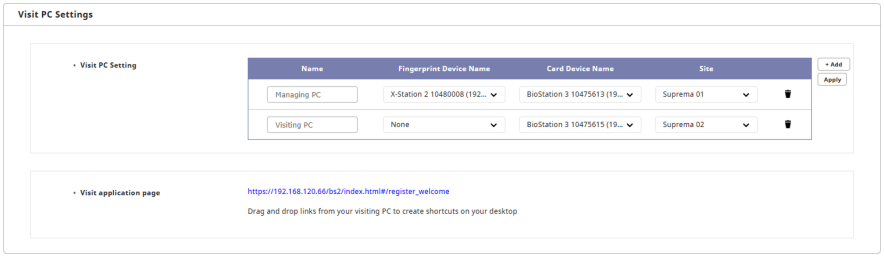
> **Información**
>
> Preconfigurar los grupos de acceso para visitantes facilita la administración. Para obtener más información sobre la configuración de grupos de acceso, consulte Administrar Grupos de Acceso.

- **Card Use**: Define si se usará una tarjeta.
- **Card Type**: Selecciona el tipo de tarjeta que se usará en el sitio. El tipo de tarjeta se activa solo cuando seleccionas **Card Use**.
- **Card Data Format**: Configura el formato para leer los datos de la tarjeta. **Card Data Format** se activa solo cuando estableces **Card Type** en **Wiegand**.

Haz clic en **Apply** para guardar la configuración del sitio de visitante.

2 Configuración de PC de visitante

Configura la PC de visita y la PC de administración.



- **Name**: Define el nombre de la PC de visita y de la PC de administración.
- **Fingerprint Device Name**: Selecciona un dispositivo para inscribir las huellas digitales de los visitantes cuando accedan al sitio mediante autenticación de huella.
- **Card Device Name**: Selecciona un dispositivo para emitir tarjetas a los visitantes cuando accedan al sitio mediante autenticación con tarjeta. El nombre del dispositivo de tarjeta se activa solo si configuraste una visita en la que seleccionaste usar tarjeta.
- **Site**: Selecciona un sitio para gestionar la visita en la PC de visita.

Haz clic en **Apply** para guardar la configuración de la PC de visita.

> **Información**
>
> - Se pueden ingresar hasta 48 caracteres para el nombre de la PC de visita.
> - Se pueden usar simultáneamente los dispositivos de huella y de tarjeta. Solo se puede seleccionar uno por tipo.
> - Solo se puede seleccionar un sitio por PC.

3 Seleccionar PC de visitante

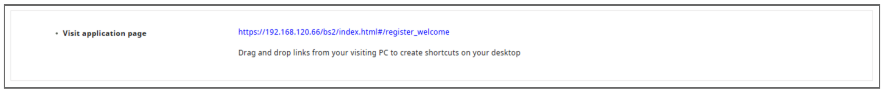
Selecciona la PC configurada en **Visit PC Setting** y asígnala a la PC actual.



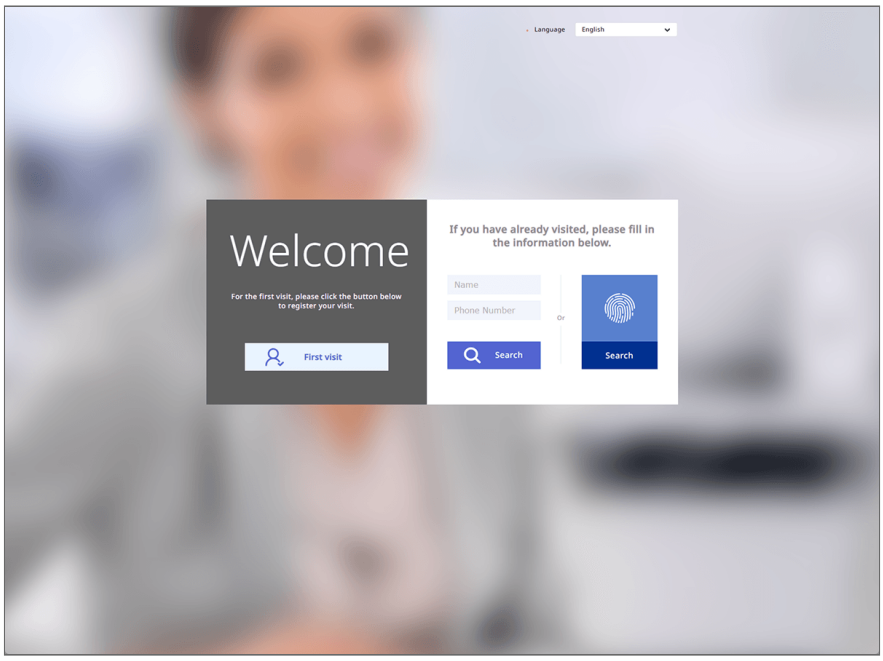
Haz clic en **Apply** para guardar la configuración.

4 Acceso directo a la página de la aplicación de visitantes

Crea un ícono de acceso directo a la página de aplicación de visitante en el escritorio de la PC de aplicación. Arrastra la URL del elemento **Visit application page** al escritorio.

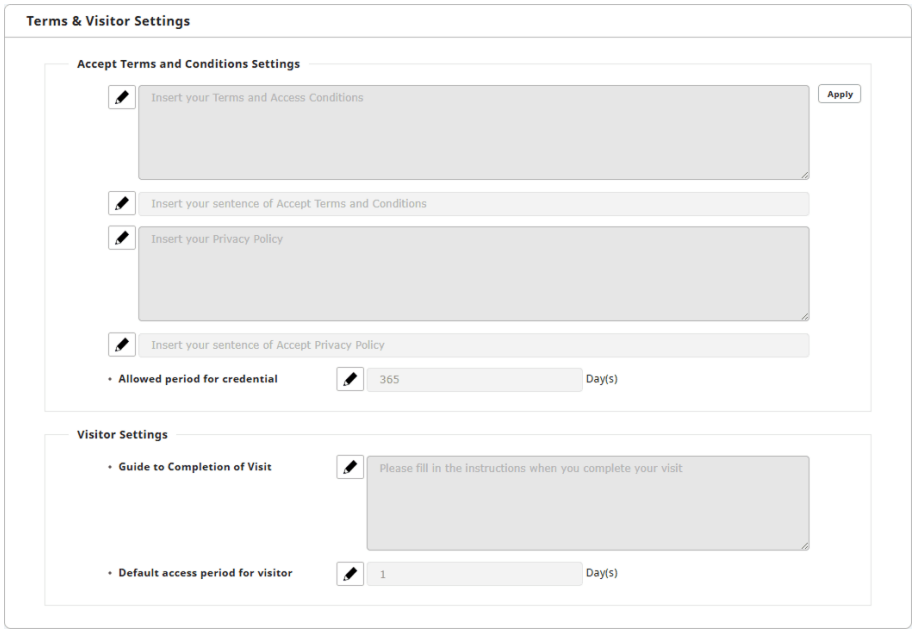


Accede a la página de aplicación de visitante conectándote a la URL en un navegador web.



Establecer términos y configuración de visitantes

Administra los ajustes clave de visitante como los términos de entrada, la política de privacidad y los mensajes de guía.



- **Términos y condiciones**: Configura los términos y condiciones para los visitantes. Haz clic en ✎ para activar el campo de entrada e introducir el contenido de los términos y condiciones.

  > **Información**
  >
  > – Se pueden ingresar hasta 65,535 caracteres para la redacción de los términos y condiciones.
  >
  > – Se pueden ingresar hasta 64 caracteres para la frase de aceptación de términos y condiciones.

- **Política de privacidad**: Configura la política de privacidad para los visitantes. Haz clic en ✎ para activar el campo de entrada e introducir la política de privacidad.

  > **Información**
  >
  > – Se pueden ingresar hasta 65,535 caracteres para la redacción de la política de privacidad.
  >
  > – Se pueden ingresar hasta 64 caracteres para la frase de aceptación de la política de privacidad.

- **Allowed period for credential**: Define el período de conservación de los datos personales que los visitantes proporcionan al registrarse. Haz clic en ✎ para activar el campo de entrada e introducir el número de días de conservación de los datos personales.

  > **Información**
  >
  > – Elimina a los visitantes cuyo período de datos personales haya expirado en el menú **Visitor**.

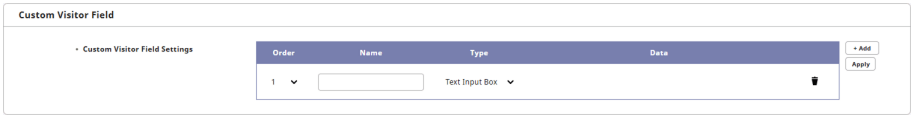
- **Guide to Completion of Visit**: Configura la guía que aparecerá en pantalla como ventana emergente cuando un visitante complete una solicitud de visita. Haz clic en ✎ para activar el campo de entrada e introducir la guía para los visitantes.

> **Información**
>
> – Se pueden ingresar hasta 65,535 caracteres para la redacción de la guía.
>
> – Si no se ingresa la redacción de la guía, no se mostrará nada en pantalla cuando los visitantes completen su solicitud de visita.

- **Default access period for visitor**: Define el período de acceso para los visitantes. Haz clic en para activar el campo de entrada e ingresar el período de acceso predeterminado para visitantes.

Configura los campos personalizados de visitantes

Agrega campos personalizados de visitantes para información adicional; estos campos aparecen en la página de solicitud de visitas.



- **Order**: Establece el orden del campo personalizado de visitantes.
- **Name**: Establece el nombre del campo personalizado de visitantes.
- **Type**: Elige la caja de texto, la caja numérica o el cuadro combinado.
- **Data**: Ingresa las opciones que aparecerán en los cuadros combinados. Separa cada elemento con un punto y coma (;). Los datos solo se activan cuando **Type** está configurado en **Combo Box**.

Haz clic en **Apply** para guardar la configuración.

> **Información**
>
> - En una **Text Input Box**, se permiten caracteres y números.
> - En una **Number Input Box**, se permiten números y no se permiten caracteres.
> - En un **Combo Box**, los elementos configurados para el campo se muestran como elementos. Si deseas configurar un campo de cuadro combinado como se muestra en la captura de pantalla siguiente, ingresa **Option 1**; **Option 2**; **Option 3**; **Option 4** en el campo de datos.

Configuración de Integración de Directorios

Este documento ofrece orientación sobre cómo sincronizar y administrar usuarios mediante la integración de **Microsoft Entra ID** (en adelante, **Entra ID**) o **Active Directory** con **BioStar X**.

La integración con **Entra ID** o **Active Directory** ofrece las siguientes funciones prácticas, mejorando la seguridad y la usabilidad. Esto mejora la seguridad y la comodidad.

- Inicia sesión en BioStar 2 con la cuenta de **Entra ID** mediante inicio de sesión único (SSO) proporcionado por **Entra ID**.
- Inicia sesión en **BioStar X** mediante la autenticación Lightweight Directory Access Protocol (LDAP) proporcionada por **Active Directory**.
- Los usuarios y los grupos configurados en **Entra ID** o **Active Directory** se pueden sincronizar con **BioStar X**.

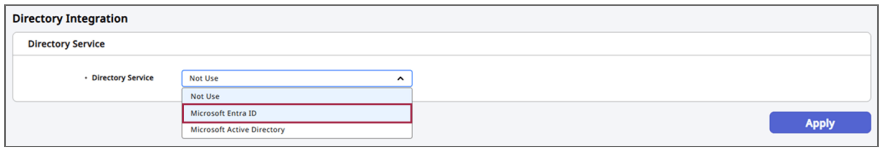
- Asigna información del usuario, como cargo, departamento y grupo, utilizada en **Entra ID** o **Active Directory**, a los campos personalizados de **BioStar X**.

> **Información**
>
> La función de ajustes de **Entra ID** o **Active Directory** está disponible como complemento con la licencia **Essential** o superior. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Ajustes de integración del directorio

Entra ID

1. Inicia sesión en **BioStar X** con una cuenta de administrador.
2. Haz clic en **Settings** en la página **Launcher**.
3. Haga clic en **System** → **Directory Integration** en la barra lateral izquierda.
4. Selecciona **Microsoft Entra ID** en **Directory Service**.



5. Configura cada elemento como se indica a continuación.

> **Información**
>
> Para integrar con Entra ID, vaya a **System** → **Server** y establezca **User ID Type** en **Alphanumeric**.

1 Directory Server

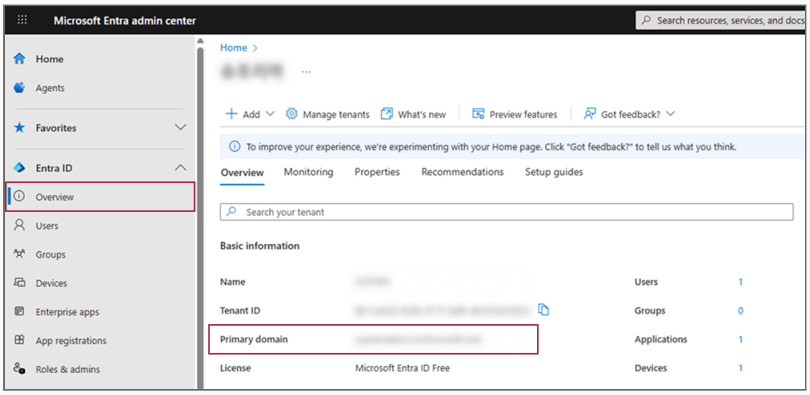
Ingresa la información del servidor de **Entra ID** y haz clic en **Connect** en **Directory Server**.



- **Client ID**: Ingresa el **Client ID** de la aplicación registrada en **Entra ID**.
- **Client Secret**: Ingresa el **Client secret** agregado en **Certificates & secrets** de la aplicación registrada en **Entra ID**.
- **Primary Domain**: Ingresa el nombre de dominio principal que se ingresó al crear la organización en **Entra ID**.

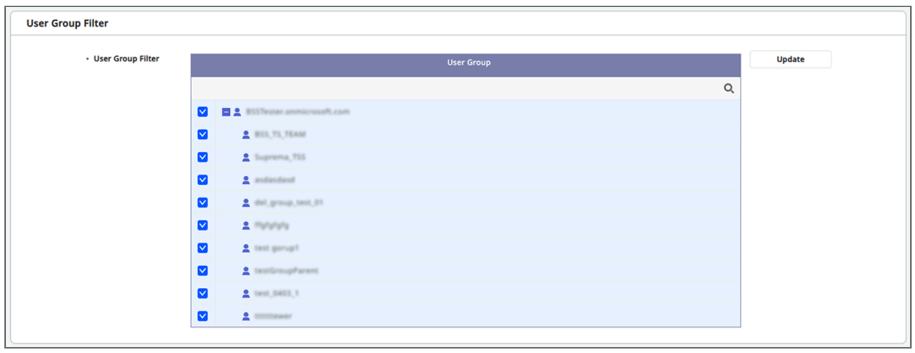
Información

- Para obtener más información sobre cómo registrar una aplicación en **Entra ID**, consulta el siguiente enlace.
- Para obtener más información sobre cómo configurar **Certificates & secrets** en **Entra ID**, consulta el siguiente enlace.
- **Tenant ID** se puede encontrar en **Overview** de la aplicación registrada en **Entra ID**.
- La información de **Primary Domain** se puede verificar en **Overview** de **Entra ID**.



1 User Group Filter

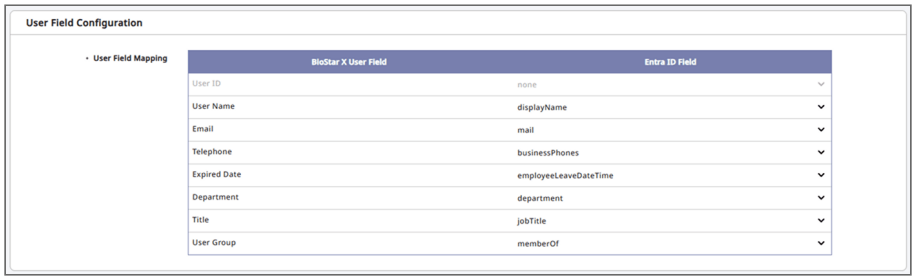
Después de completar la configuración en **Directory Server** y hacer clic en **Connect**, la información de los grupos de usuarios de se recuperará en **User Group Filter**. Desmarque los grupos de usuarios que no se sincronizarán con **BioStar X**.



- **Update**: Haga clic para actualizar la información de grupos de usuarios.
- Haga clic en el ícono para buscar el grupo de usuarios deseado.

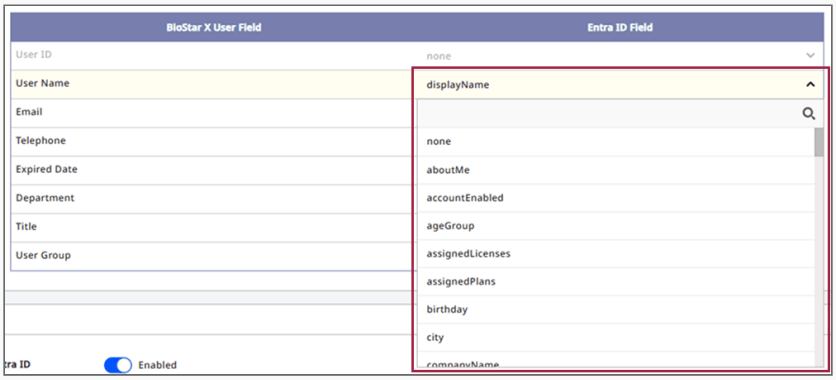
1 User Field Configuration

Configura el campo de para asignarlo a los campos de usuario de **BioStar X**. Selecciona el campo de que se usará como campo de usuario de **BioStar X** en la sección **User Field Configuration**.



Información

De forma predeterminada, **BioStar X** asigna cada campo de usuario a un campo de información de usuario coincidente en . Para usar un valor de campo distinto del predeterminado, haga clic en una entrada de la columna **Entra ID Field** y seleccione otro valor de campo.

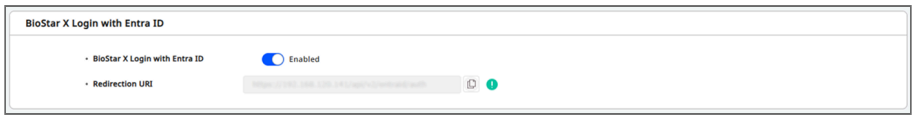


Precaución

El campo **User ID** no se puede asignar al integrar con **Entra ID**. **User ID** se genera y aplica automáticamente en **BioStar X**.

1 BioStar X Login with Entra ID

Cambia **BioStar X Login with Entra ID** a **Enabled** para habilitar el inicio de sesión en **BioStar X** mediante **Entra ID SSO**.



Copia el URI de redirección del campo **Redirection URI** ( ) y pégalo en la configuración de redirección SSO en el portal de **Entra ID**. Cuando un usuario inicie sesión correctamente con **Entra ID**, será redirigido a esta dirección.

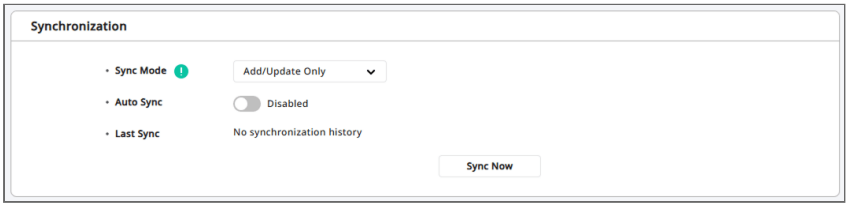
Información

- Para obtener más información sobre cómo registrar una aplicación en **Entra ID** y agregar un URI de redirección, consulta los siguientes enlaces.
  - Registrar una aplicación en Microsoft Entra ID
  - Cómo agregar un URI de redirección a tu aplicación
- La dirección de redirección se puede encontrar en **Overview** de la aplicación registrada en **Entra ID**.

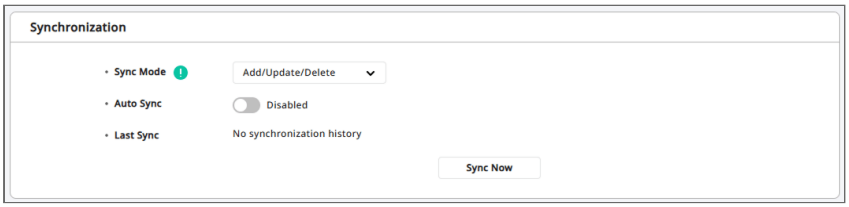
1 Synchronization

Sincroniza la información de los usuarios modificada en .

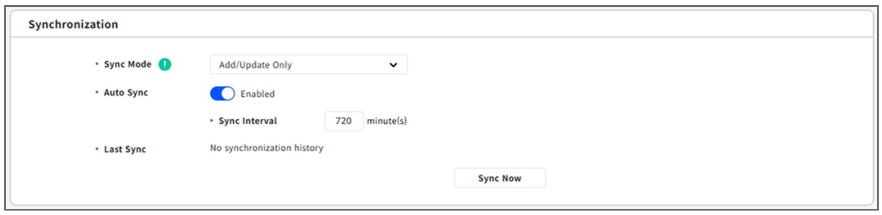
- **Sync Mode**: Seleccione el modo de sincronización deseado.
  - **Add/Update Only**: Al sincronizar usuarios desde el servicio de directorio integrado, se agregarán los usuarios que no estén en **BioStar X** y se actualizarán los usuarios cuya información haya cambiado. Sin embargo, los siguientes usuarios no serán eliminados.
    - Usuarios registrados únicamente en **BioStar X**
    - Usuarios eliminados de



  - **Add/Update/Delete**: Sincroniza la información de los usuarios de **BioStar X** para que coincida exactamente con la del servicio de directorio integrado. Sincroniza los usuarios, incluidos aquellos registrados únicamente en **BioStar X** y los eliminados de , para mantener los datos idénticos en ambos sistemas.



- **Auto Sync**: Establece el intervalo de sincronización automática. La sincronización se ejecuta automáticamente en el intervalo establecido en **Sync Interval**. Ingrese el intervalo en minutos. El valor mínimo es de **30** minutos y el máximo es de **10,080** minutos (7 días).



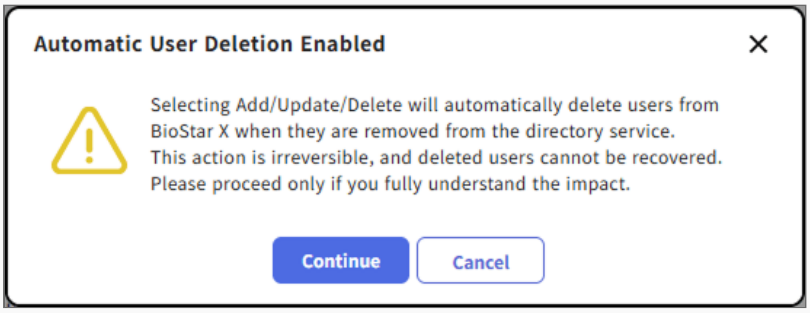
- **Last Sync**: Revisa la fecha y la hora de la sincronización más reciente.

Precaución

- Al usar el modo **Add/Update Only**, si existe un grupo con el mismo nombre, ese grupo se conserva en lugar de eliminarse.
- Modo **Add/Update/Delete**:
  - **Si ya existe un grupo con el mismo nombre**: no se crea el grupo y se conserva la información del grupo existente. Sin embargo, todos los usuarios de ese grupo se eliminan y luego se vuelven a agregar para reflejar la información más reciente del servicio de directorio. Sin embargo, los usuarios de ese grupo que comparten el mismo nombre se conservan.
  - **Usuarios creados en BioStar X**: Los usuarios creados directamente en **BioStar X** no están vinculados al servicio de directorio. Al sincronizar, actualiza estos usuarios para que su información quede vinculada al servicio de directorio.
  - **Limitaciones**: Después de la sincronización, si ya existe un grupo con el mismo nombre, la información y los miembros de ese grupo pueden no sincronizarse correctamente.
- Si actualizas a **BioStar X v1.0.2** con la integración de directorio habilitada, el modo de sincronización predeterminado será **Add/Update/Delete**.

Información

- Al hacer clic en **Sync Now**, la información de los usuarios se sincroniza con el servicio de directorio según el modo de sincronización seleccionado.
- Al seleccionar el modo **Add/Update/Delete**, aparecerá un mensaje de advertencia. Haz clic en **Continue** para continuar. Haz clic en **Cancel** para cancelar.



- Para excluir usuarios específicos de la sincronización al integrar, consulta Excluir de la integración del directorio.
- Si un identificador de usuario sincronizado o un nombre de usuario contiene caracteres que **BioStar X** no permite, inscríbalo después de eliminar solo esos caracteres. Sin embargo, **BioStar X** no cambia un punto (`.`) en un ID de usuario ni un punto (`.`) o un apóstrofo (`'`) en un nombre de usuario. Para obtener más información sobre los caracteres no permitidos, consulta Reglas para ingresar el ID de usuario y el nombre.

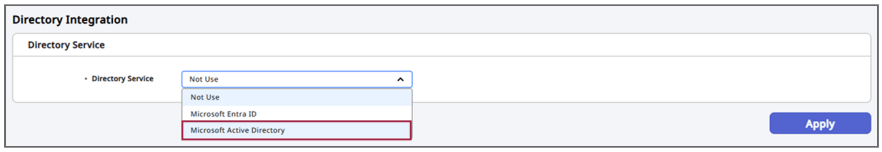
1 Guardar configuración

Después de completar todos los ajustes de **Directory Integration**, haz clic en **Apply** en la parte inferior de la pantalla para guardar. Para ver los resultados de la configuración, consulte Verificar los resultados de los ajustes.

Active Directory

1. Inicia sesión en **BioStar X** con una cuenta de administrador.

2. Haz clic en **Settings** en la página **Launcher**.
3. Haga clic en **System** → **Directory Integration** en la barra lateral izquierda.
4. Selecciona **Microsoft Active Directory** en **Directory Service**.



5. Configura cada elemento como se indica a continuación.

> **Información**
>
> - Active Directory está disponible para entornos de sistema con Windows Server 2008 R2 o posterior.
> - Para integrar con Active Directory, vaya a **System** → **Server** y establezca **User ID Type** en **Alphanumeric**.

1 Directory Server

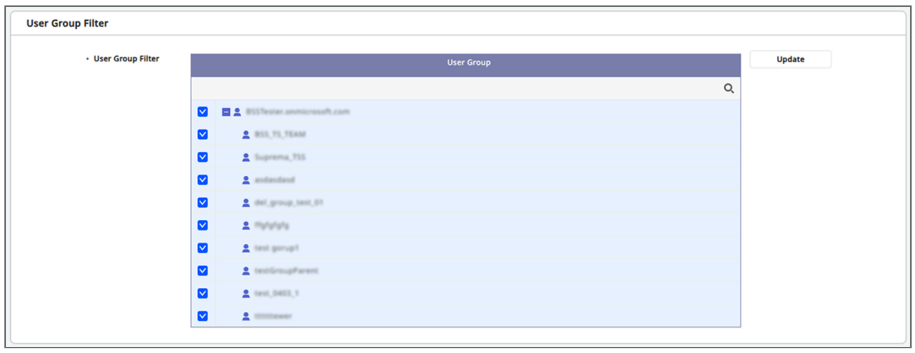
Ingresa la información del servidor de **Active Directory** y haz clic en **Connect** en **Directory Server**.



- **Server Address**: Ingresa la dirección del servidor de Windows Active Directory.
- **User Name**: Ingresa el nombre de usuario que utiliza Windows Active Directory.
- **Password**: Ingresa la contraseña que utiliza Windows Active Directory.
- **Base Domain Name**: Ingresa el nombre de dominio base para Windows Active Directory. Encuentra el nombre de dominio base mediante los siguientes pasos:
  1. Ejecuta **Active Directory Administrative Center**.
  2. Haz clic derecho en el nodo donde se almacenan los datos de usuario y luego haz clic en **Property**.
  3. En la ventana **property**, selecciona **Expand** y luego haz clic en **Attribute Editor**.
  4. Consulta el valor de **distinguishedName**.
- **Secure Transfer**: Usa cifrado al comunicarte con el servidor Windows Active Directory. Para instalar Active Directory Certificate Services y configurar el **Keystore Password**, consulte Cifrado de Active Directory.
  - **Keystore Password**: Ingresa la contraseña del almacén de claves de cifrado del servidor Windows Active Directory. Ingresa la contraseña cuando **Secure Transfer** esté establecido en **Enabled**.

1 User Group Filter

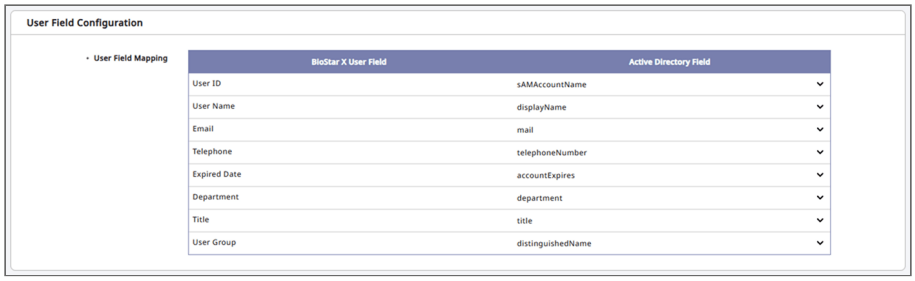
Después de completar la configuración en **Directory Server** y hacer clic en **Connect**, la información de los grupos de usuarios de se recuperará en **User Group Filter**. Desmarque los grupos de usuarios que no se sincronizarán con **BioStar X**.



- **Update**: Haga clic para actualizar la información de grupos de usuarios.
- Haga clic en el ícono para buscar el grupo de usuarios deseado.

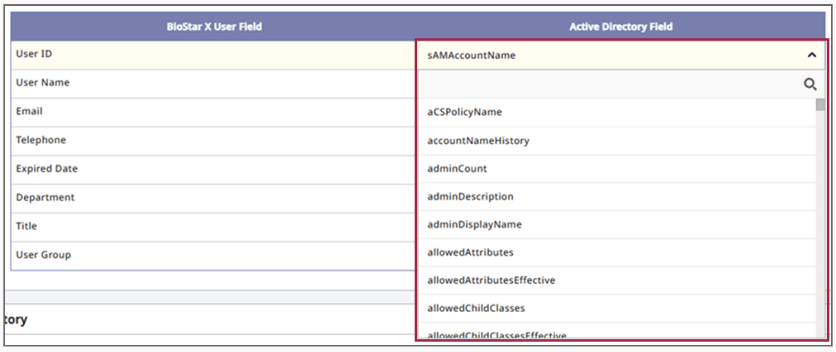
1 User Field Configuration

Configura el campo de para asignarlo a los campos de usuario de **BioStar X**. Selecciona el campo de que se usará como campo de usuario de **BioStar X** en la sección **User Field Configuration**.



Información

De forma predeterminada, **BioStar X** asigna cada campo de usuario a un campo de información de usuario coincidente en . Para usar un valor de campo distinto del predeterminado, haga clic en una entrada de la columna **Active Directory Field** y seleccione otro valor de campo.



1 BioStar X Login with Active Directory

Para configurar el inicio de sesión en **BioStar X** usando el ID de usuario del servidor Active Directory, cambia **BioStar X Login with Active Directory** a **Enabled**. El valor del campo `sAMAccountName` del servidor Active Directory se asignará al ID de inicio de sesión de **BioStar X**.

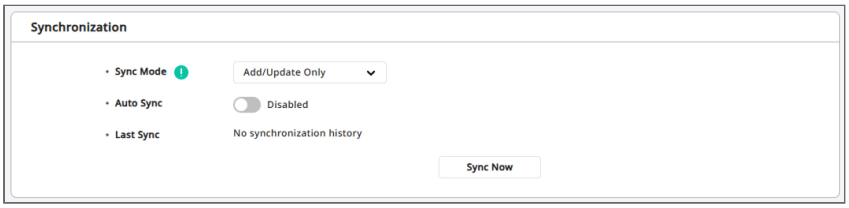
> **Precaución**
>
> El campo `sAMAccountName` no puede contener caracteres especiales. El inicio de sesión podría fallar si no cumple con la política de ID de inicio de **BioStar X**.



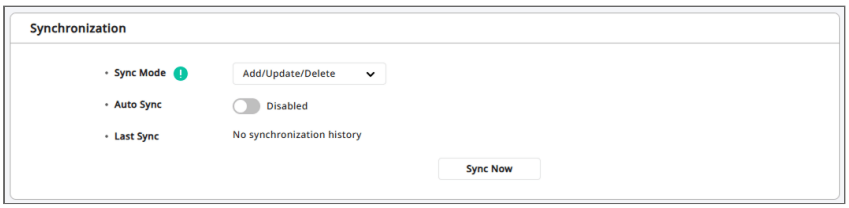
1 Synchronization

Sincroniza la información de los usuarios modificada en .

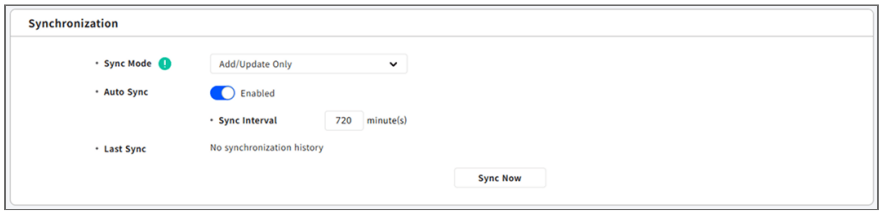
- **Sync Mode**: Seleccione el modo de sincronización deseado.
  - **Add/Update Only**: Al sincronizar usuarios desde el servicio de directorio integrado, se agregarán los usuarios que no estén en **BioStar X** y se actualizarán los usuarios cuya información haya cambiado. Sin embargo, los siguientes usuarios no serán eliminados.
    - Usuarios registrados únicamente en **BioStar X**
    - Usuarios eliminados de



  - **Add/Update/Delete**: Sincroniza la información de los usuarios de **BioStar X** para que coincida exactamente con la del servicio de directorio integrado. Sincroniza los usuarios, incluidos aquellos registrados únicamente en **BioStar X** y los eliminados de , para mantener los datos idénticos en ambos sistemas.



- **Auto Sync**: Establece el intervalo de sincronización automática. La sincronización se ejecuta automáticamente en el intervalo establecido en **Sync Interval**. Ingrese el intervalo en minutos. El valor mínimo es de **30** minutos y el máximo es de **10,080** minutos (7 días).



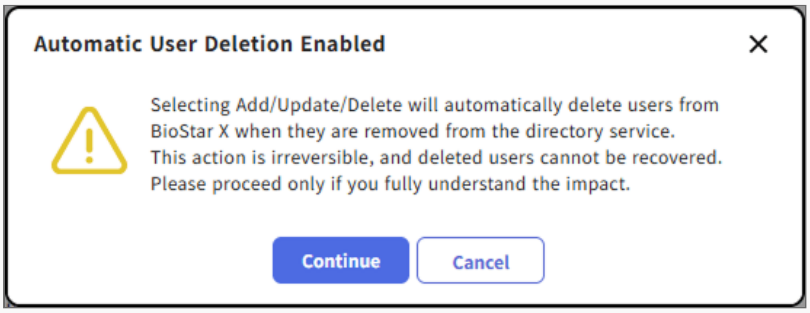
- **Last Sync**: Revisa la fecha y la hora de la sincronización más reciente.

Precaución

- En el modo **Add/Update Only**, los grupos de usuarios con el mismo nombre y los usuarios con el mismo ID de usuario no se eliminan; se conservan.
- Modo **Add/Update/Delete**:
  - **Si ya existe un grupo con el mismo nombre**: no se crea el grupo y se conserva la información del grupo existente. Sin embargo, todos los usuarios de ese grupo se eliminan y luego se vuelven a agregar para reflejar la información más reciente del servicio de directorio. Sin embargo, los usuarios de ese grupo que comparten el mismo nombre se conservan.
  - **Usuarios creados en BioStar X**: Los usuarios creados directamente en **BioStar X** no están vinculados al servicio de directorio. Al sincronizar, actualiza estos usuarios para que su información quede vinculada al servicio de directorio.
  - **Limitaciones**: Después de la sincronización, si ya existe un grupo con el mismo nombre, la información y los miembros de ese grupo pueden no sincronizarse correctamente.
- Si actualizas a **BioStar X v1.0.2** con la integración de directorio habilitada, el modo de sincronización predeterminado será **Add/Update/Delete**.

Información

- Al hacer clic en **Sync Now**, la información de los usuarios se sincroniza con el servicio de directorio según el modo de sincronización seleccionado.
- Al seleccionar el modo **Add/Update/Delete**, aparecerá un mensaje de advertencia. Haz clic en **Continue** para continuar. Haz clic en **Cancel** para cancelar.



- Para excluir usuarios específicos de la sincronización al integrar, consulta Excluir de la integración del directorio.
- Si un identificador de usuario sincronizado o un nombre de usuario contiene caracteres que **BioStar X** no permite, inscríbalo después de eliminar solo esos caracteres. Sin embargo, **BioStar X** no cambia un punto (`.`) en un ID de usuario ni un punto (`.`) o un apóstrofo (`'`) en un nombre de usuario. Para obtener más información sobre los caracteres no permitidos, consulta Reglas para ingresar el ID de usuario y el nombre.

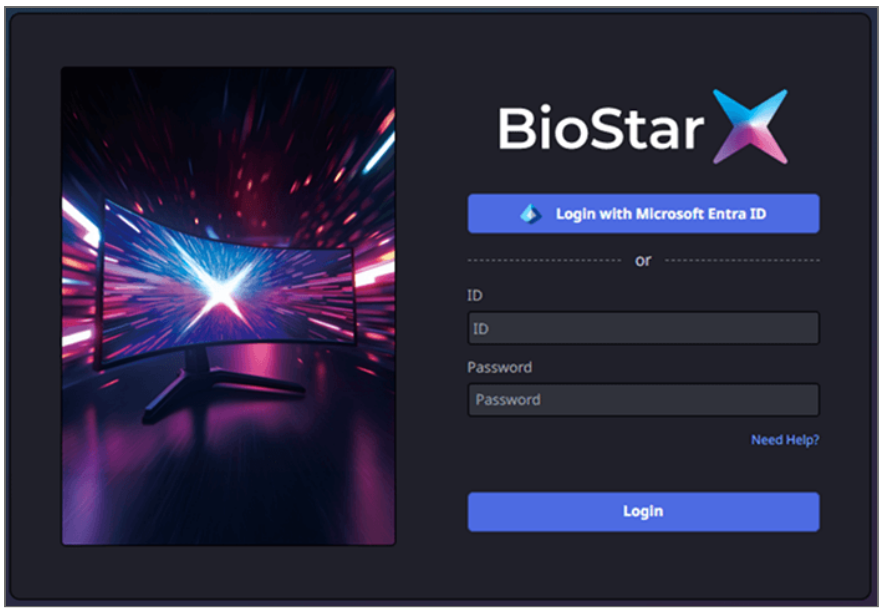
1 Guardar configuración

Después de completar todos los ajustes de **Directory Integration**, haz clic en **Apply** en la parte inferior de la pantalla para guardar. Para ver los resultados de la configuración, consulte Verificar los resultados de los ajustes.

Verificar los resultados de los ajustes

Haga clic en **Apply** en la parte inferior de la pantalla para aplicar la configuración de integración con **Entra ID** o **Active Directory**. Consulte lo siguiente para verificar la configuración sincronizada.

- Revise la lista de usuarios sincronizados en el menú **User**.
- Tras completar la configuración de inicio de sesión con **Entra ID** o **Active Directory**, aparece **Login with Microsoft Entra ID** al iniciar sesión en **BioStar X**.



Gestionar caracteres no compatibles

Si un ID de usuario o nombre en **Entra ID** o **Active Directory** incluye caracteres no compatibles, el sistema sincroniza al usuario después de eliminarlos.

> *Por ejemplo, si el id de usuario del servicio de directorio es `john/doe` y el nombre de usuario es `John<Doe>`, **BioStar X** los registra como `johndoe` y `JohnDoe`.*

Información

- El sistema excluye los puntos(.) y los apóstrofos(') de los caracteres no compatibles en los nombres de usuario y guarda los valores originales del servicio de directorio.

  > *Ejemplo: `O'Brien`, `John.Doe` → El sistema los guarda con los valores originales del servicio de directorio*

- El sistema excluye los puntos(.) de los caracteres no compatibles en los ID de usuario y guarda los valores originales del servicio de directorio, pero elimina los apóstrofos(') porque los ID de usuario no pueden incluirlos.

  > *Ejemplos de ID de usuario del servicio de directorio:*
  > – `O'Brien` → *El sistema lo guarda como* `OBrien`
  > – `john.doe` → *El sistema lo guarda como* `john.doe`

- Para obtener más información sobre las reglas de entrada de ID de usuario y nombre, consulta Ingresar Información Básica del Usuario.

Excluir de la integración del directorio

Al integrar **Entra ID** o **Active Directory** mediante la función **Directory Integration**, los usuarios que no existan en el servicio de directorio podrían eliminarse de **BioStar X**. Si hay usuarios que no desea que se eliminen, exclúyalos de la integración con el siguiente método.

1. Inicia sesión en **BioStar X** con una cuenta de administrador.
2. Vaya al menú **User**.
3. Haga clic en el usuario que desea excluir de la integración en la lista **All Users**.
4. Cuando aparezca la pantalla de detalles del usuario seleccionado, en la sección **Advanced**, habilite la opción **Exclude from Directory Integration**.



5. Haz clic en **Apply**.

Los usuarios seleccionados se excluirán de la integración al usar la función **Directory Integration**.

Información

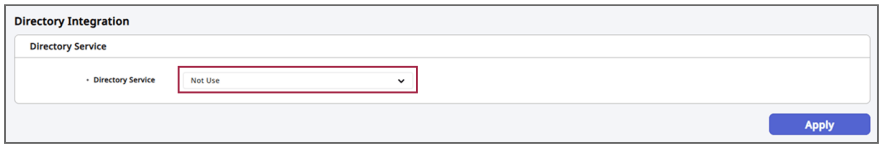
El sistema excluye automáticamente a estos usuarios de la integración.

- Cuando un nombre de usuario empieza con `&@~` al inicio
- El id de usuario o el nombre de usuario está en blanco
- El ID de usuario (hasta 32 caracteres) o el nombre de usuario (hasta 48 caracteres) supera el límite de longitud
- el id de usuario coincide con un valor reservado por el sistema, como `admin`
- El ID de usuario es un punto (`.`) o dos puntos (`..`)

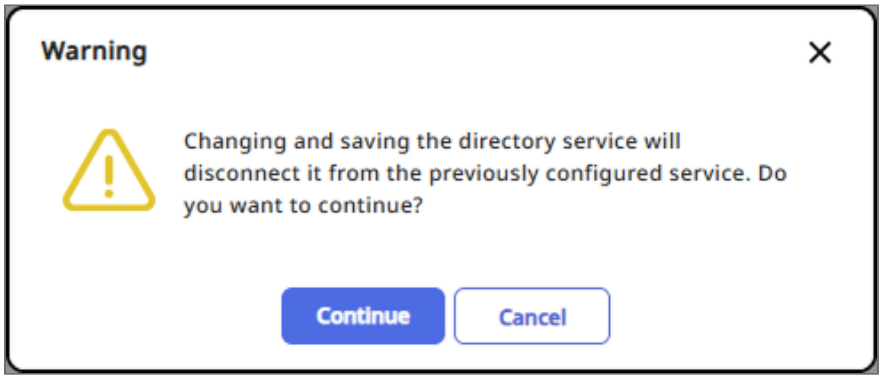
Deshabilitar la integración del directorio

Siga estos pasos para deshabilitar la función **Directory Service**:

1. Inicia sesión en **BioStar X** con una cuenta de administrador.
2. Haga clic en **System** → **Directory Integration**.
3. Seleccione **Not Use** en **Directory Service**.



4. Cuando aparezca el mensaje **Warning**, haga clic en **Continue**.



5. Haga clic en **Apply** en la parte inferior de la pantalla.

Precaución

Cuando **Directory Service** se configure en **Not Use**, se eliminará toda la configuración de integración con **Entra ID** o **Active Directory** en **BioStar X**. La información integrada de usuarios y grupos no se eliminará, pero dejará de sincronizarse. Asegúrese de verificar antes de deshabilitar la integración.

Configuración de Acceso Remoto

El acceso remoto a través de ngrok permite acceder de forma segura a redes internas desde redes externas. Esta función

permite acceder al servidor **BioStar X** de forma remota sin configuraciones de firewall ni reenvío de puertos.

Información

- La función de acceso remoto está disponible como una opción adicional. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias. La licencia de acceso remoto es una suscripción anual.
- Al adquirir la licencia de acceso remoto, Suprema genera una cuenta de bot, un endpoint y un documento de licencia para el uso de acceso remoto en el sitio ngrok de Suprema.

Precaución

- El acceso remoto se proporciona mediante el servicio de túnel de terceros de ngrok. Antes de usar esta función, revise Remote Access Feature Agreement.
- BioStar X solo admite la conexión llamando a la API de ngrok, pero la seguridad y continuidad de la conectividad a Internet dependen completamente del servicio ngrok. Por lo tanto, Suprema no asume ninguna responsabilidad por incidentes de seguridad, pérdida de datos o vulneraciones del sistema que puedan ocurrir durante el uso de esta función.

¿Cuándo usarlo?

Use la función de acceso remoto en las siguientes situaciones.

- Cuando necesite conectarse al servidor **BioStar X** desde una red externa
- Cuando sea difícil conectarse directamente debido a firewalls o entornos NAT
- Cuando desee configurar rápidamente el acceso remoto sin configuraciones de red complejas
- Cuando necesite proporcionar derechos de acceso externos de manera temporal

Configuración del acceso remoto

1 Activar licencia de acceso remoto

1. Inicie sesión con su ID de administrador de **BioStar X**.
2. Haz clic en **Settings** en la página **Launcher**.
3. Haga clic en **License** → **BioStar X License** en la barra lateral izquierda.
4. Introduzca la clave de licencia de acceso remoto y el nombre de administrador proporcionados por Suprema y, a continuación, haga clic en **Activate**.

Información

Para obtener más información sobre el registro de licencias, consulte Licencia Biostar X.

2 Activar acceso remoto

1. Inicie sesión con su ID de administrador de **BioStar X**.
2. Haz clic en **Settings** en la página **Launcher**.
3. Haga clic en **System** → **Remote Access** en la barra lateral izquierda.
4. En la sección **Remote Access with ngrok**, cambie la opción **Remote Access** a **Use**.



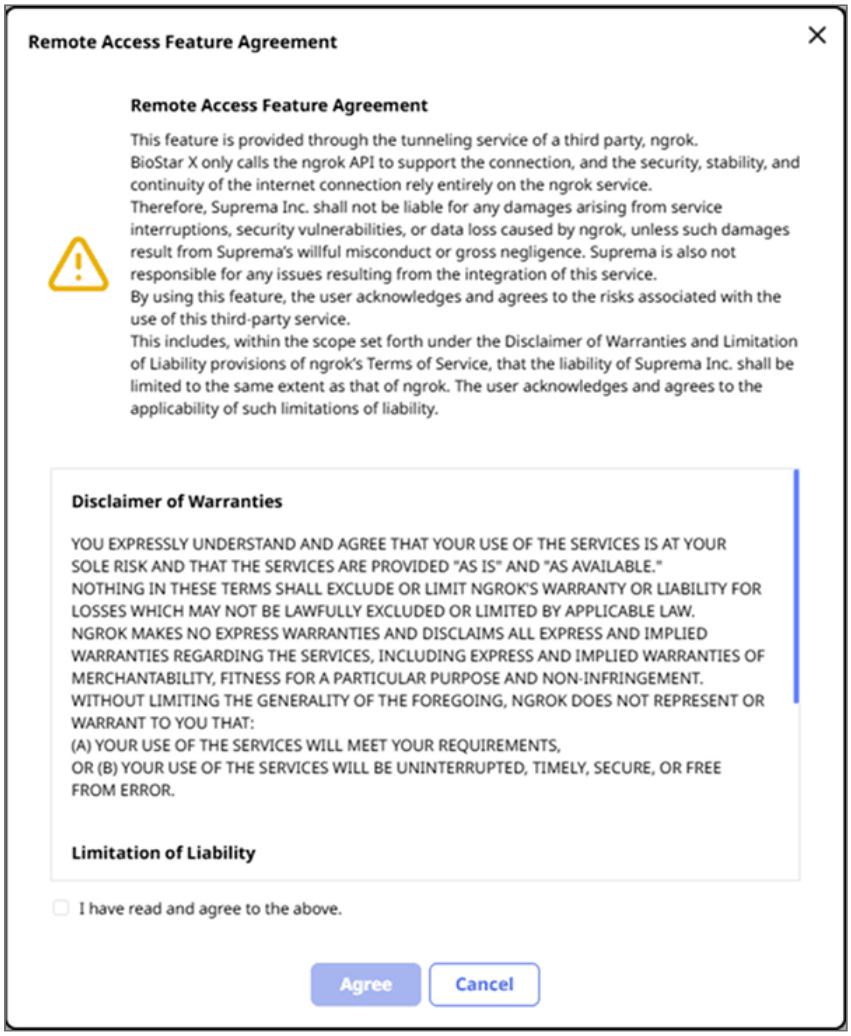
3 Introducir la información de configuración de ngrok

Introduzca la información de configuración de ngrok proporcionada por Suprema.

- **Authtoken**: Ingrese su **token de autenticación**.
- **URL**: Ingrese la URL del endpoint. La URL tiene el formato `https://subdomain.bsx.ngrok.app`.

> **Información**
>
> El subdominio (`subdomain`) debe cumplir las reglas que se indican a continuación. No se pueden usar subdominios que no cumplan con las reglas.
>
> - Solo se permiten letras del alfabeto inglés (A-Z, a-z), números (0-9) y guiones (`-`).
> - No se permiten caracteres especiales ni espacios.

1. Después de introducir toda la información, haga clic en **Apply**.
2. Cuando aparezca la ventana **Remote Access Feature Agreement**, revise el contenido.



3. Seleccione la casilla para aceptar los términos, luego haga clic en **Agree**.

Acceder a la URL del endpoint

Después de completar la configuración, verifique si puede acceder al servidor **BioStar X** desde una red externa usando la URL del endpoint que introdujo en **URL**.

> **Información**
>
> - Conéctese a la URL del endpoint. Luego vaya a **Settings** → **Audit Trail** → **AC Audit Log** para consultar los registros de acceso.
>
> *Ejemplo: [Acceso remoto] 192.168.1.100*
>
> - Si no puede acceder mediante la URL del endpoint desde una red externa, póngase en contacto con el punto de venta o distribuidor que emitió su licencia.

Integrar el Registro de Eventos de Dispositivos Virtuales

Al usar la función de dispositivo virtual, es posible registrar eventos como entradas y salidas directamente en **BioStar X** desde aplicaciones móviles o servicios de terceros al integrar la función de gestión de asistencia. Es posible gestionar sistemáticamente los registros de eventos sin un dispositivo físico, lo cual resulta útil para la integración con sistemas externos.

¿Cuándo usarlo?

Utilice la función de integración de registro de eventos de dispositivos virtuales en las siguientes situaciones.

- Al gestionar eventos del sistema externo de gestión de T&A en **BioStar X**
- Cuando necesite guardar registros de acceso (Punch Log) desde la aplicación móvil o un sistema externo directamente en **BioStar X** (registrar eventos de entrada/salida sin vinculación de base de datos)
- Cuando sea necesario enviar eventos directamente mediante la API de **BioStar X** desde aplicaciones o servicios de terceros

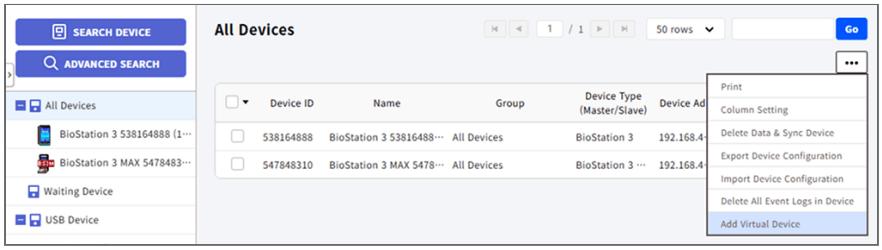
Antes de comenzar

Debe activarse la licencia **Event Log API**. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

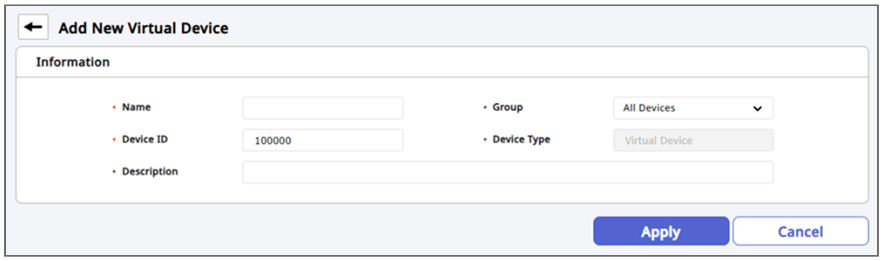
> **Información**
> Para obtener más información sobre cómo aplicar licencias, consulte Licencia Biostar X.

Registrar dispositivo virtual

1. Haz clic en **Settings** en la página **Launcher**.
2. Haz clic en **Device** → **Device** en la barra lateral izquierda.
3. Haga clic en [•••] en la parte superior derecha de la lista de dispositivos y seleccione **Add Virtual Device**.



4. Ingrese la información de configuración cuando aparezca la pantalla **Add Virtual Device**.



- **Name**: Ingrese el nombre del dispositivo virtual.
- **Group**: Seleccione el grupo para asignar el dispositivo virtual.
- **Device ID**: Ingrese el ID único del dispositivo virtual. Debe especificarse dentro de un rango que no duplique un ID de dispositivo existente.
- **Description**: Ingrese la descripción del dispositivo virtual.

5. Haga clic en **Apply** en la parte inferior derecha de la pantalla para registrar el dispositivo virtual.

> **Información**
>
> - El **Device ID** puede especificarse dentro del rango de 100000 - 999999. Debe especificarse dentro de un rango que no duplique un ID de dispositivo Suprema existente.
> - El valor de **Device ID** que ya se ha creado no puede modificarse.

Gestionar grupos de dispositivos

Los dispositivos virtuales pueden usar la función de grupos de dispositivos igual que los dispositivos normales.

- Ubique el dispositivo en el mismo grupo que los dispositivos existentes.
- Si el usuario tiene permisos de grupo, puede otorgar permisos a los dispositivos virtuales dentro de ese grupo.

> **Información**
> Para obtener más información sobre los grupos de dispositivos, consulte Gestionar Grupos de Dispositivos.

Limitaciones de dispositivos virtuales

- Los dispositivos virtuales aparecen solo en el siguiente menú.
  - **Settings** → **Device** → **Device**
  - Vea todos los registros de eventos y la vista previa de eventos en **Monitoring**
  - Recupere registros de eventos desde **Data**
- El dispositivo virtual no puede usar las funciones de control de acceso en la puerta ni en **Advanced AC**.
- No puede especificarse como dispositivo para la configuración de **T&A**.
- Los dispositivos virtuales no aparecen en la lista de dispositivos de la barra lateral del menú **Monitoring**.
- No es posible usar la función de control del dispositivo.
- No se incluyen en el número de dispositivos de la licencia **Multi Communication Server**.

Registrar eventos mediante API

Tipo de evento admitido

Solo pueden registrarse los siguientes tipos de eventos.

- **Acceso concedido** (`4088`)
- **Acceso denegado** (`6400`)

Parámetros de la API

Debe proporcionar los siguientes parámetros al registrar eventos.

Parámetro	Descripción	Obligatorio
dev_id	Solo se permiten ID de dispositivos virtuales registrados	Si
evt	Acceso concedido o acceso denegado	Si
fecha y hora	Hora de ocurrencia del evento	Si
user_id	ID Usuario	Si
tna_key	Disponible únicamente para la entrada con el valor especificado	Opción

Request example

```
{
  "packet_device_id" : 100003, // required
  "is_virtual_device" : "true", // required
  "events":[ //4088 access granted, 6400 access denied
    {
      "dev_id": 100003, // required
      "evt": 6400, // required
      "datetime": "2025-08-21T14:12:00Z", // required
      "user_id": "2", // required
      "tna_key": "1"
    },
    {
      "dev_id": 100003,
      "evt": 6400,
      "datetime": "2025-08-21T14:13:01Z",
      "user_id": "2",
      "tna_key": "1"
    }
  ]
}
```

Response example

```
{
  "Response": {
    "code": "0",
    "link": "https://support.supremainc.com/en/support/home",
    "message": "Success"
  }
}
```

Información

- Es posible registrar múltiples eventos para un solo dispositivo virtual a la vez con una sola llamada a la API.
- Para obtener más información sobre el uso de la API, consulte la API de BioStar X.

Recuperar registro de eventos

Recupere los registros de eventos grabados mediante el dispositivo virtual en el menú.

- **Monitoring**: Recupere y filtre todos los eventos, vista previa de eventos
- **Data**: Recupere y filtre todos los eventos

Información

- Para obtener más información sobre cómo ver eventos en el menú **Monitoring**, consulte Supervisar Evento.
- Para obtener más información sobre el menú **Data**, consulte Generar Reporte.

Registro auditoría

El rastro de auditoría se registra como se muestra en el siguiente ejemplo cuando se registran eventos.

```
Access granted, 2025/08/05 03:37:49, outside access door on 12th floor, Administrator(1)
```

Información

- Incluso si los eventos se registran por lotes, se crea una entrada de auditoría individual para cada evento.
- Para obtener más información sobre **Audit Trail**, consulte Gestionar Registro De Auditoría.

Solución de Problemas

Si el botón **Add Virtual Device** no es visible

Verifique si la licencia **Event Log API** está activada.

Cuando falla la llamada a la API

- Verifique si la licencia **Event Log API** está activada.
- Verifique que el ID de dispositivo sea un dispositivo virtual registrado.
- Verifique que el formato de los parámetros de la API sea correcto.

Cuando no se recuperan los eventos

- Verifique que el dispositivo registrado sea el ID de dispositivo virtual correcto.
- Verifique que el dispositivo virtual esté seleccionado en el filtro de eventos.
- Compruebe los registros de auditoría para garantizar que no se produjeron errores al registrar eventos.

Conector

¿Qué son los conectores?

Los conectores de **BioStar X** son extensiones de la plataforma **BioStar X** que proporcionan funciones adicionales para cumplir con los requisitos de los clientes o integrarse con sistemas existentes.

> **Información**
>
> - Se requiere una licencia de conector para utilizar las funciones de conector. Para obtener más información sobre la política de licencias, consulte Política de Licencias.
> - Para obtener más información sobre cómo desarrollar complementos, consulte Guía de Desarrollador de conector de BioStar X.

Conectores de BioStar X

Lista de complementos disponibles a través de opciones de licencia adicionales.

- Cómo Usar Tiempo y Asistencia
- Administrar Visitantes

> **Información**
> Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

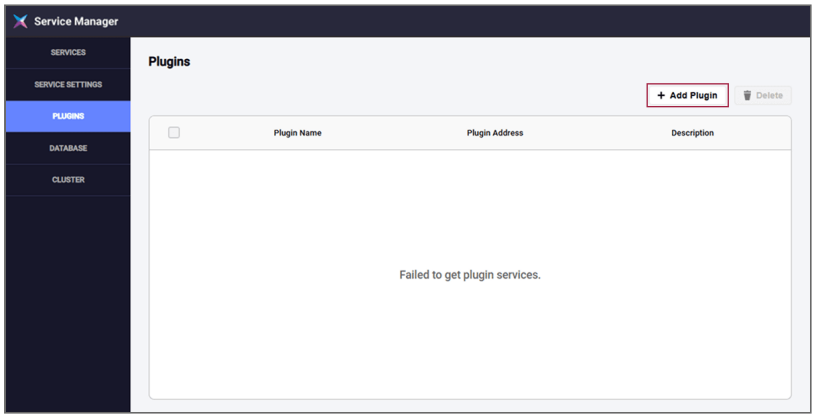
Casos de uso clave

Integre diversos sistemas externos mediante el sistema de conector de **BioStar X**. Los casos de uso representativos son los siguientes.

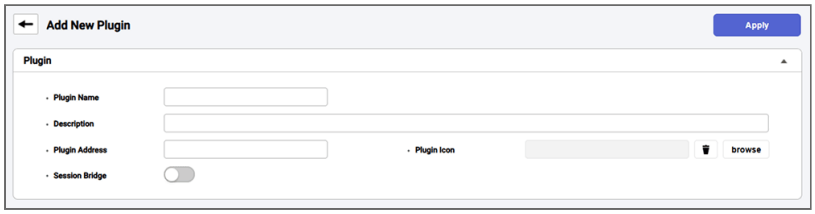
- **Sistema de gestión de asistencia**: Integración con soluciones externas de T&A (tiempo y asistencia)
- **Sistema de gestión de visitantes**: Integración con sistemas independientes de registro y gestión de visitantes
- **Solución de informes**: Integración con herramientas de informes y análisis personalizables
- **Integración con sistemas de terceros**: Integración de datos con sistemas empresariales existentes como ERP y HRM

Registrar el plugin

1. Haz clic en Inicio → **BioStar X** → **BioStar X Service Manager** en Windows.
2. Haz clic en **PLUGINS** en el menú lateral izquierdo.
3. Haz clic en **Add Plugin** en la esquina superior derecha.



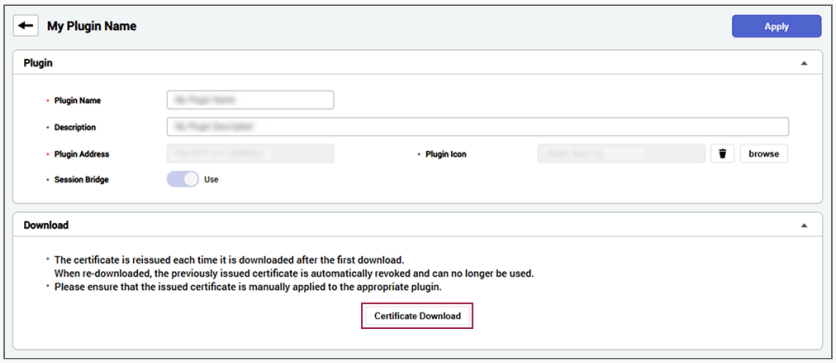
4. Introduzca la información del conector en la pantalla **Add New Plugin**.



5. Introduzca la información del conector y haz clic en **Apply** para completar el registro.

Información

Si activaste **Session Bridge**, descarga el certificado en la parte inferior de la pantalla. Se requiere el certificado para la comunicación segura entre **BioStar X** y el conector. Si pierdes el certificado, descárgalo de nuevo. En ese momento, el certificado existente se invalidará.



Introduzca información del conector

- **Plugin Name**: Introduzca el nombre del conector. Ingresa hasta 48 caracteres. No uses un nombre ya registrado por otro conector.
- **Description**: Ingresa una descripción del conector. Ingresa hasta 500 caracteres.
- **Plugin Address**: Ingresa la dirección del conector. Debe ser una URL válida que comience con `http://` o `https://`, y no se debe usar la misma dirección de un conector ya registrado.
- **Plugin Icon**: Carga el ícono del conector.
  - Los formatos compatibles son JPEG, PNG, SVG y GIF.
  - El tamaño máximo del archivo es de 1 MB y no se pueden cargar archivos vacíos de 0 KB.

  - Las imágenes cargadas se redimensionarán automáticamente a 104×104 píxeles.

- **Session Bridge**: Activa Session Bridge. Usar esta característica hereda automáticamente los permisos para los usuarios de BioStar X, por lo que no es necesario iniciar sesión separada al acceder al conector.

> **Información**
>
> - Si no cargas un ícono, se generará automáticamente uno a partir de la primera letra del nombre del conector. Para eliminar el ícono cargado, haz clic en el botón ; al eliminarlo se reemplazará por el ícono generado automáticamente.
> - Una vez que **Session Bridge** esté activado, no se podrá desactivar ni cambiar la dirección del conector por razones de seguridad.

Verificar en la pantalla del lanzador

Los conector agregados aparecen en la pantalla **Launcher** de **BioStar X**.



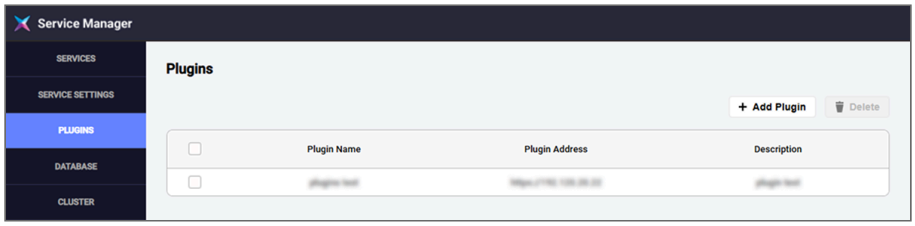
Administración de conector

Administra los conectores instalados a través de **BioStar X Service Manager**.

Haz clic en Inicio → **BioStar X** → **BioStar X Service Manager** en Windows. Haz clic en **PLUGINS** en el menú del sitio de la pantalla de **BioStar X Service Manager**.

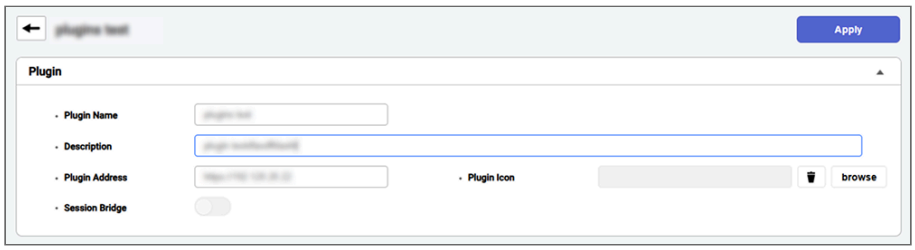
Revisar la lista de conector

Consulta todos los conectores registrados por el usuario.



Editar conector

Haz clic en el conector que deseas editar en la lista de conectores. Aparece la pantalla de edición de información del conector. Edita el nombre del conector (**Plugin Name**), la descripción (**Description**) y el ícono (**Plugin Icon**).



> **Información**
> No se puede editar **Plugin Address** cuando **Session Bridge** está habilitado.

Eliminar conector

1. Selecciona el conector que deseas eliminar haciendo clic en la casilla de verificación ubicada en el extremo izquierdo de la lista de conectores.
2. Haz clic en y luego en **Delete** en la esquina superior derecha de la pantalla.
3. Cuando aparezca el mensaje de confirmación, haga clic en **OK**.

> **Información**
> - El conector de tiempo y asistencia (T&A) añadido con la licencia de tiempo y asistencia no se puede eliminar.
> - El conector de gestión de tiempo y asistencia está disponible como opción adicional. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Cómo Usar Tiempo y Asistencia

Configure las reglas de gestión de asistencia y consulte el historial de trabajo registrado a través del dispositivo o expórtelo como informe. La función T&A se ofrece como conector y requiere una licencia independiente.

> **Información**
> La característica T&A está disponible mediante una opción complementaria. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.

Antes de comenzar

Para usar la función T&A, aplique la licencia y descargue el archivo de instalación independiente.

Aplicar licencia

Instrucciones para aplicar la licencia de T&A. Después de adquirir la licencia T&A a través de un proveedor de **BioStar X**, siga las instrucciones para aplicarla.

1. Inicie sesión con la cuenta de administrador de **BioStar X**.
2. Haz clic en **Settings** en la página **Launcher**.
3. Haga clic en **License** → **BioStar X License** en la barra lateral izquierda.
4. Ingrese **License Activation** en secuencia con **Activated by** y **License Key**.



5. Haga clic en **Activate**.

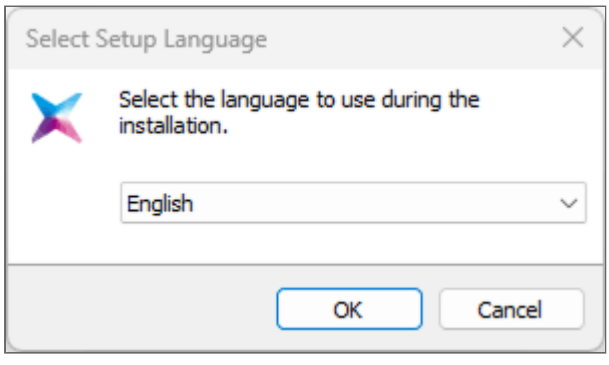
Verifique las licencias registradas en **Activated License**.

> **Información**
> Para activar su licencia en un entorno de red cerrado o cuando el acceso a Internet esté restringido o no esté disponible, consulte Licencia Biostar X.

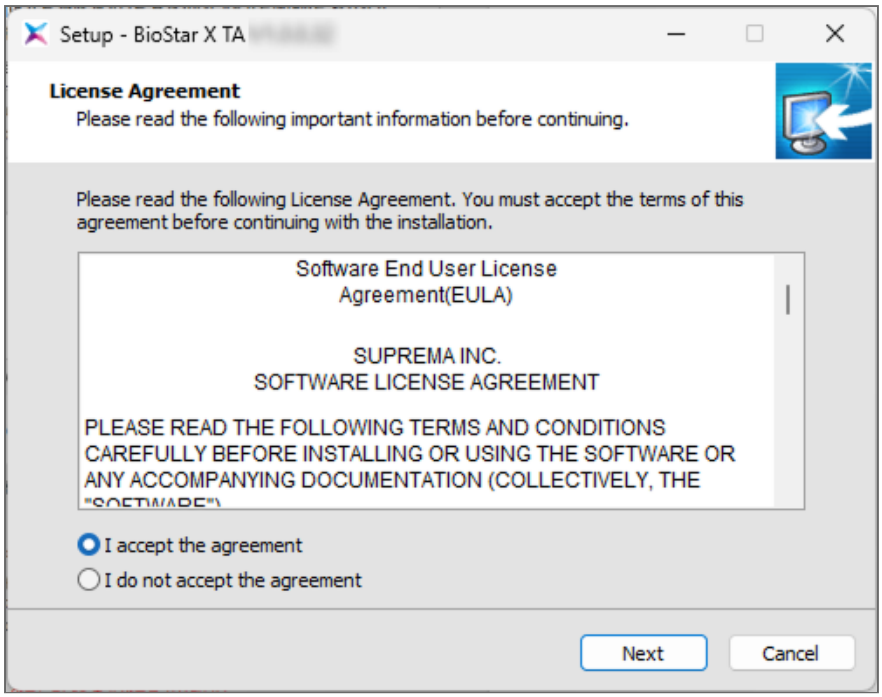
Instalar conector

Para usar la función T&A, se debe descargar e instalar un archivo de instalación independiente. Siga las instrucciones para instalar el conector.

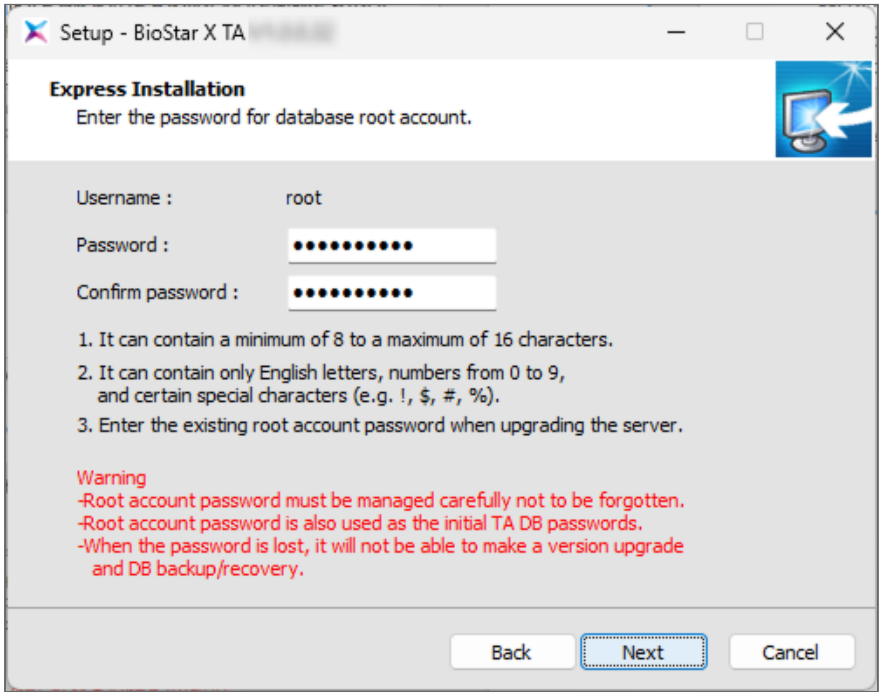
1. Acceda al Suprema Download Center y descargue el archivo de instalación del conector T&A (*BioStar X TA.X.Y.Z.BB.exe*).
2. Ejecute el archivo de instalación y complete la instalación siguiendo las instrucciones.
3. Ejecute el archivo de instalación descargado.
4. Seleccione el idioma a usar y haga clic en el botón **Aceptar**.



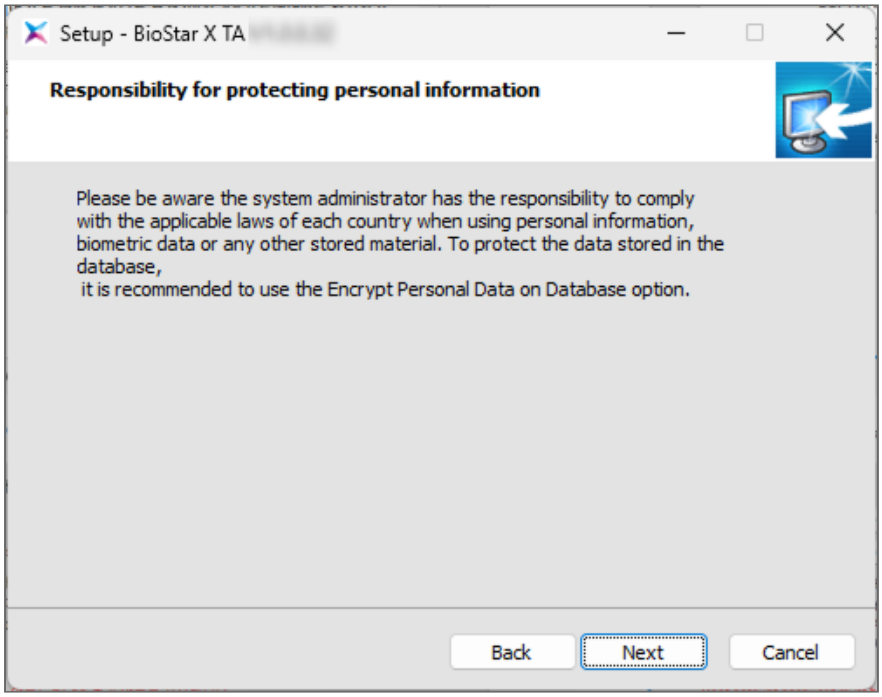
5. Para continuar con la instalación, seleccione **Acepto el acuerdo** y haga clic en el botón **Siguiente**.



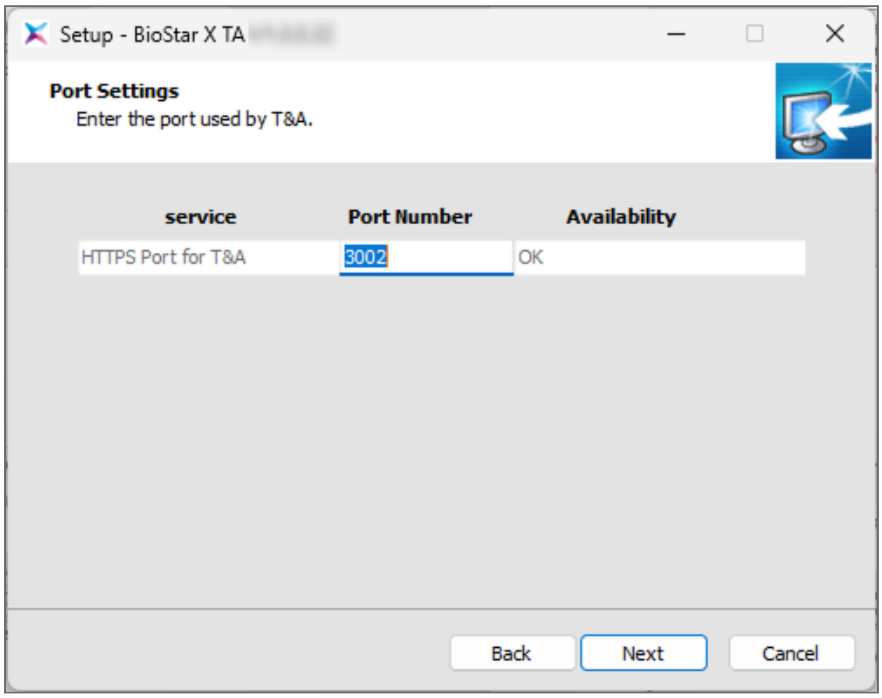
6. Ingrese la contraseña de la cuenta root de la base de datos y haga clic en el botón **Siguiente**.



7. Lea la información sobre la gestión y la responsabilidad de los datos personales almacenados en la base de datos y haga clic en el botón **Siguiente** para continuar con la instalación.

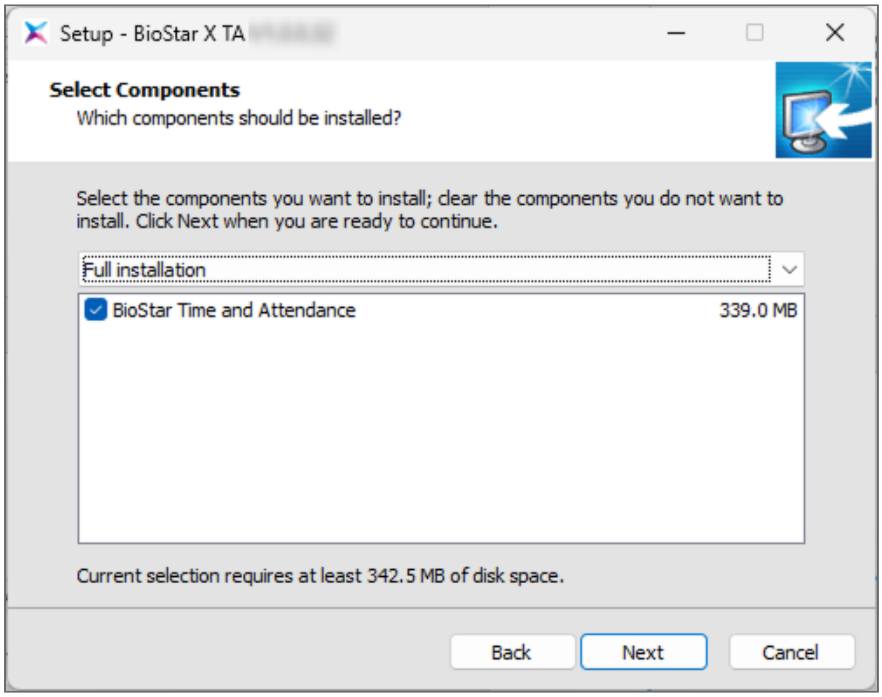


8. Configure el puerto para la comunicación con **BioStar X** y haga clic en **Siguiente**.

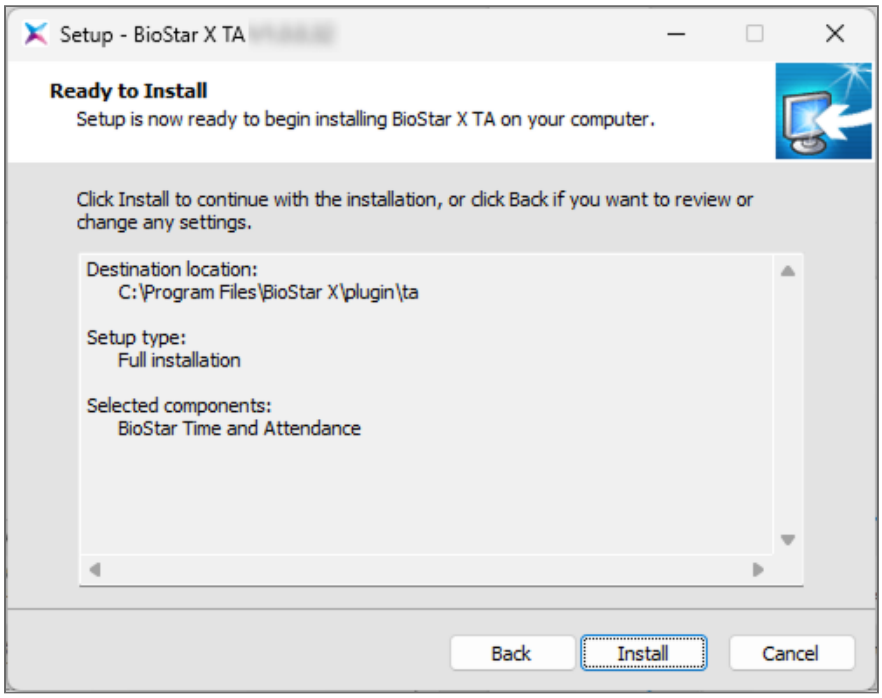


> Puede usar el número de puerto predeterminado (3002) o cambiarlo por otro. Si cambia el número de puerto, asegúrese de que el puerto correspondiente esté abierto en el firewall.

9. Seleccione los componentes de instalación y haga clic en **Siguiente**.



10. Cuando se completen todas las preparaciones para la instalación, haga clic en el botón **Instalar**.

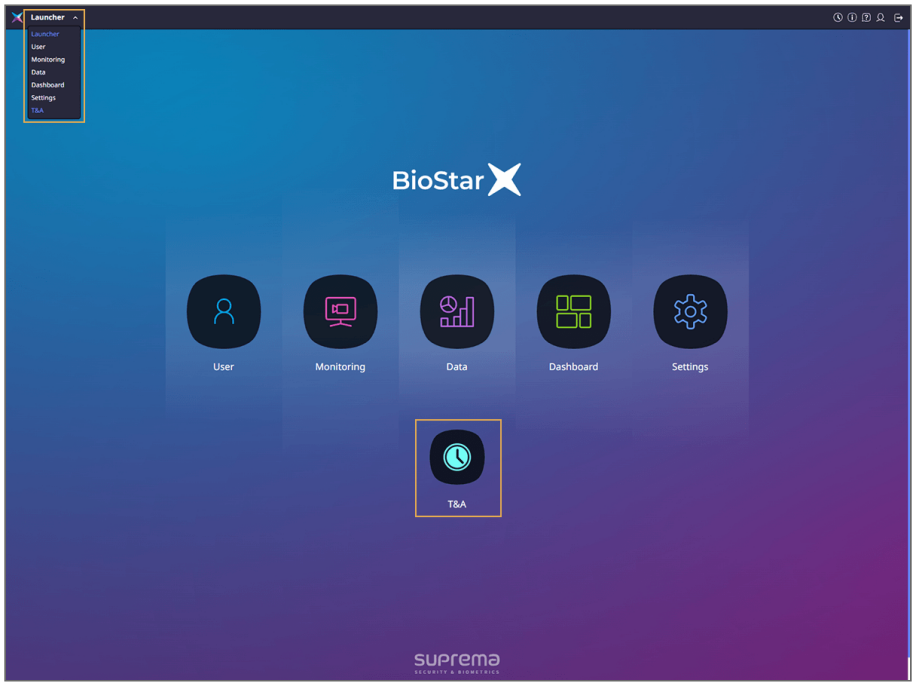


Información

- En el nombre del archivo descargado, `X.Y.Z` es la información de la versión y `BB` es el número de compilación.
- Use la contraseña de la cuenta root de la base de datos que se usó al instalar **BioStar X**.

Menú **T&A**

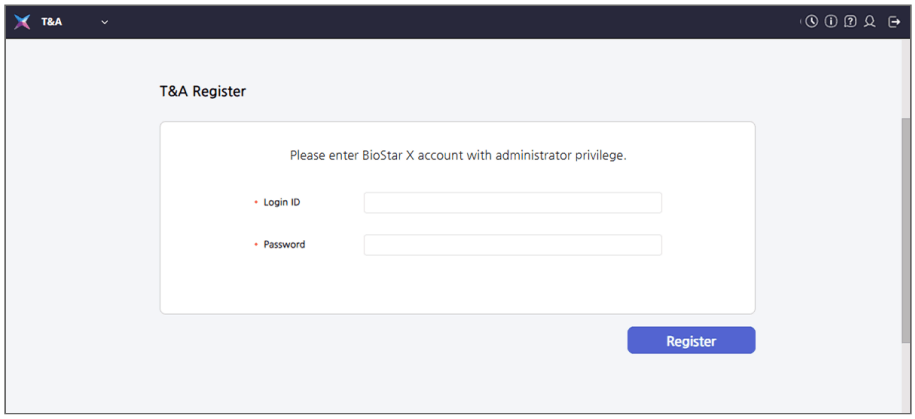
Una vez completada la instalación del conector y la licencia T&A, la página **Launcher** incluirá el menú **T&A**.



Haga clic en el ícono **T&A** en la página **Launcher** o seleccione **T&A** en la lista de accesos directos en la esquina superior izquierda de la pantalla.

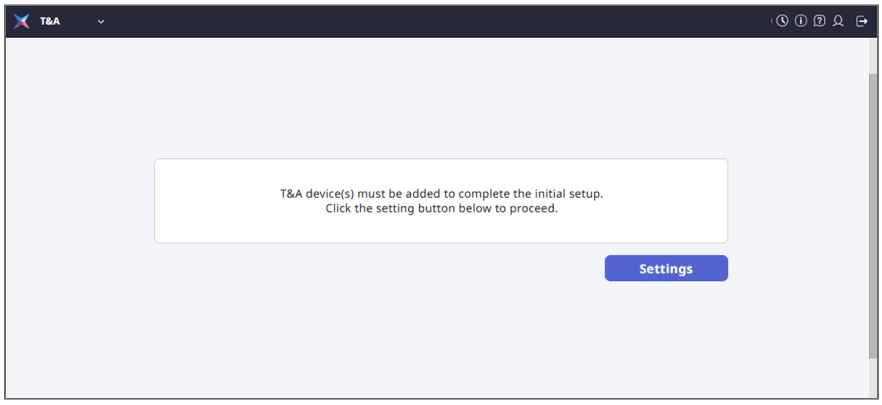
Inicio de sesión de **T&A**

Aparecerá una pantalla de inicio de sesión independiente la primera vez que ingrese a la función T&A. Inicie sesión con la cuenta de administrador de **BioStar X**. Cuando inicie sesión en la función T&A con la cuenta de administrador, podrá usar la función T&A posteriormente sin un proceso de inicio de sesión separado.

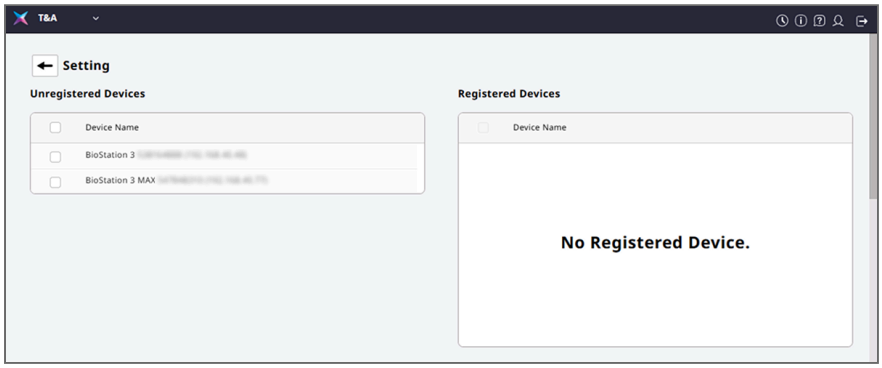


Configuración inicial

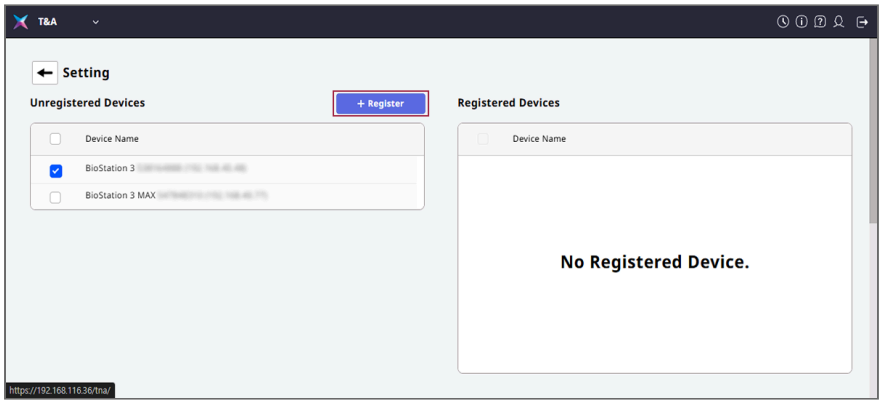
1. La primera vez que inicie sesión en la función T&A, debe agregar un dispositivo para la gestión de asistencia como parte de la configuración inicial. Haga clic en el botón **Settings** en la pantalla.



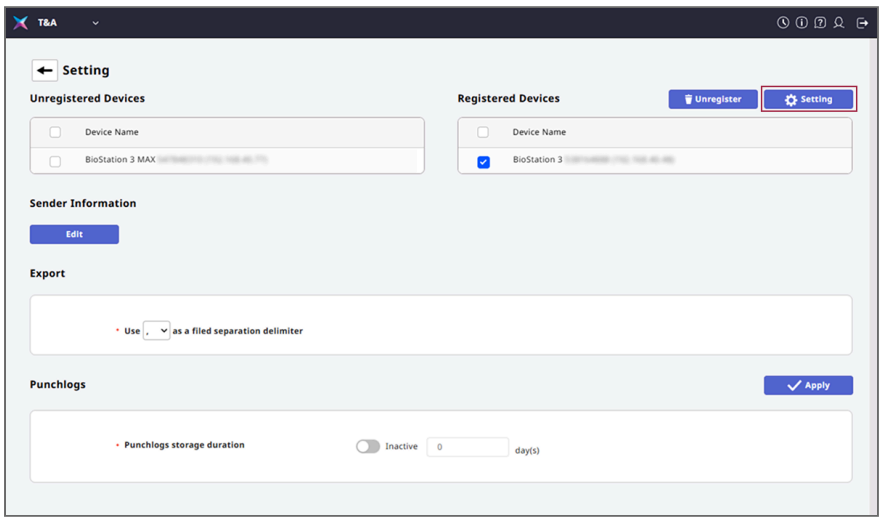
2. Seleccione un dispositivo para la gestión de asistencia en la lista de dispositivos.



3. Haga clic en el botón activado + **Register**.



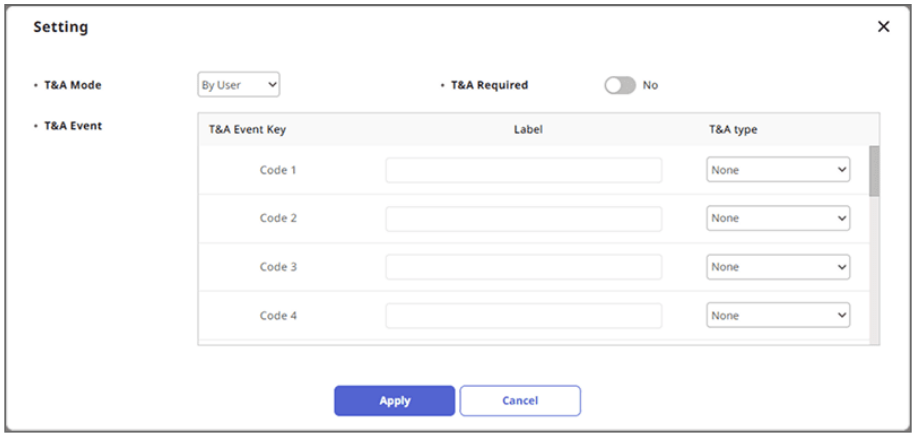
4. Si el dispositivo seleccionado aparece en la lista **Registered Devices**, haga clic en el botón **Setting**.



5. Cuando aparezca la ventana **Setting**, complete la configuración básica de gestión de asistencia.

Configurar modo de asistencia

Continúe con la configuración del modo de asistencia y de los eventos de asistencia.



- **T&A Mode**: Elija cómo registrar los eventos de asistencia.
  - **By User**: Los usuarios pueden seleccionar eventos de asistencia durante la autenticación.
  - **By Schedule**: Los eventos de asistencia cambian automáticamente según un horario establecido. Seleccione un horario para aplicar a los eventos de asistencia.
  - **Last Choice**: El último evento de asistencia utilizado puede seguir usándose.
  - **Fixed**: Solo se puede usar el evento de asistencia seleccionado.
  - **Not Use**: No registra eventos de asistencia.
- **T&A Required**: Puede configurarlo para requerir el registro de eventos de asistencia durante la autenticación. Se puede usar cuando **T&A Mode** está configurado en **By User**.
- **T&A Event**: Puede modificar el nombre de los eventos de asistencia o agregar horarios cuando configure **T&A Mode** en **By Schedule**.
  - **T&A Event Key**: Lista de claves que se pueden usar para registrar asistencia.
  - **Label**: Puede cambiar el nombre de los eventos de asistencia según la tecla de asistencia.
  - **Schedule**: Si configura **T&A Mode** en **By Schedule**, puede establecer automáticamente el horario para que cambie. Para obtener más información sobre la configuración de horarios, consulte Ajustes de Horario.

Información

- Los dispositivos que no son compatibles con pantallas LCD pueden configurar **T&A Mode** en **By Schedule** y **Fixed**. Puede registrar eventos de asistencia fijos o cambiar eventos de asistencia según configuraciones programadas previamente.
- Estos modelos son compatibles con los modos **By Schedule** y **Fixed**: XPass Q2, XPass 2, XPass D2, BioEntry W3, BioEntry P2 y BioEntry W2.
- Para obtener más información sobre el menú **Setting**, consulte Configurar Tiempo y Asistencia.

Configurar Turno

Esta guía explica cómo configurar las reglas de gestión de asistencia mediante el establecimiento del horario laboral en unidades horarias, diarias y semanales.

Si es la primera vez que registra reglas de trabajo, siga los pasos a continuación para configurarlas.

1 Time Code

Puede establecer reglas de tiempo para la gestión de registros de asistencia, horas extra y ausencias. Puede definir ponderaciones horarias y asignarles código de color para facilitar la identificación.

Para obtener más información sobre la configuración de Time Code, consulte Establecer Código de Tiempo.

2 Shift

Configura reglas de trabajo diarias basadas en un periodo de 24 horas. Las reglas de trabajo incluyen ajustes de reglas por hora, ajustes de hora de inicio diaria y reglas de redondeo de tiempo.

Para obtener más información sobre la configuración de Shift, consulte Configurar Turno Diario.

3 Schedule Template

Configure reglas de trabajo semanales basadas en las reglas diarias configuradas. Configure reglas de trabajo semanales de forma semanal o diaria.

Para obtener más información sobre la configuración de Schedule Template, consulte Configurar Turnos Semanales.

4 Rule

Esto puede ser útil cuando no ha añadido reglas de horas extra a las reglas de trabajo diarias. Las horas extra establecidas en las reglas de trabajo diarias tienen horas de inicio y fin, pero **Rule** calcula el tiempo total que supera el horario laboral regular. **Rule** puede utilizarse cómodamente para gestionar el total de horas extra diarias/semanales/mensuales y, si configura **Rule**, se aplicará en lugar de la regla de horas extra añadida a las reglas de trabajo.

Para obtener más información sobre la configuración de Rule, consulte Configurar Otras Reglas de Trabajo.

5 Horario de trabajo

Puede establecer el periodo para aplicar el horario de trabajo configurado en el paso anterior, junto con los usuarios, otras reglas de trabajo y los calendarios de ausencias.

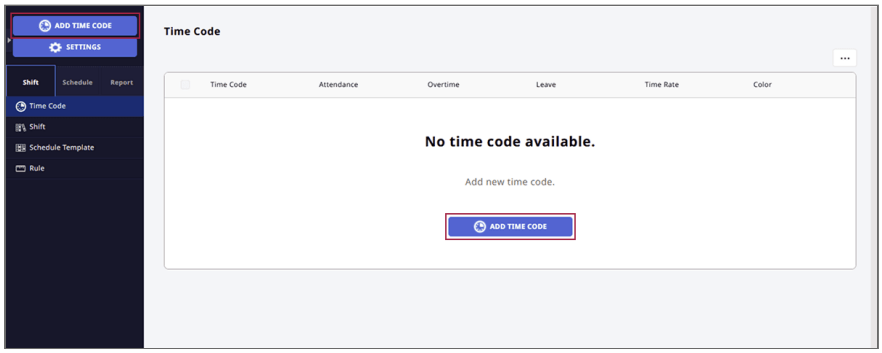
Para obtener más información sobre la configuración de Schedule, consulte Configurar el Horario.

Establecer Código de Tiempo

Esta guía describe la configuración de los ajustes de Time Code utilizados para el cálculo de horas laborales. Configura códigos de tiempo estándar, de horas extra y de ausencias. Cada Time Code se puede utilizar con diferentes ponderaciones horarias.

ADD TIME CODE

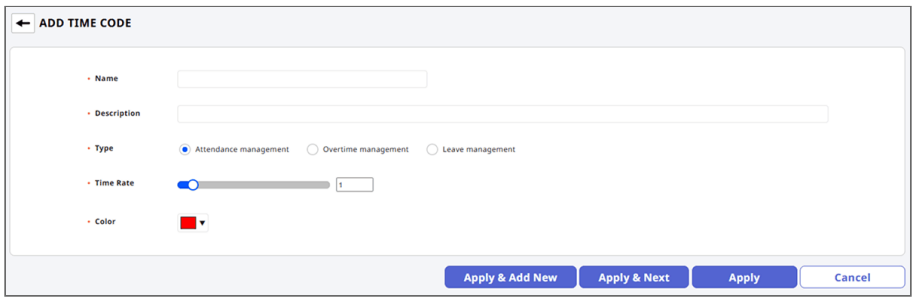
1. Haga clic en **T&A** en la página **Launcher**.
2. Haz clic en **Shift** → **Time Code** en la barra lateral izquierda.
3. Haz clic en **ADD TIME CODE**.



4. Cuando aparezca la pantalla **ADD TIME CODE**, configura cada campo.

> **Información**
>
> - Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.
> - Para agregar Shift, haz clic en **Apply & Next**.
> - Después de guardar los ajustes, haz clic en **Apply & Add New** para agregar otra **Time Code**.

Guía de opciones de configuración



- **Name**: Ingresa el nombre del Time Code.
- **Description**: Ingresa una descripción para el Time Code.
- **Type**: Selecciona el tipo de Time Code.
  - **Attendance management**: Configura como el Time Code que se utilizará para la asistencia normal.
  - **Overtime management**: Configura como el Time Code que se utilizará para horas extra.
  - **Leave management**: Configura como el Time Code que se utilizará para ausencias, viajes de negocios, etc.
- **Time Rate**: Establece la ponderación por hora según el Time Code. **1** es la ponderación base y, si se establece en **2**, el Time Code configurado calculará las horas laborales al doble por hora.
- **Color**: Establece el color para distinguir el Time Code.

Siguiente paso

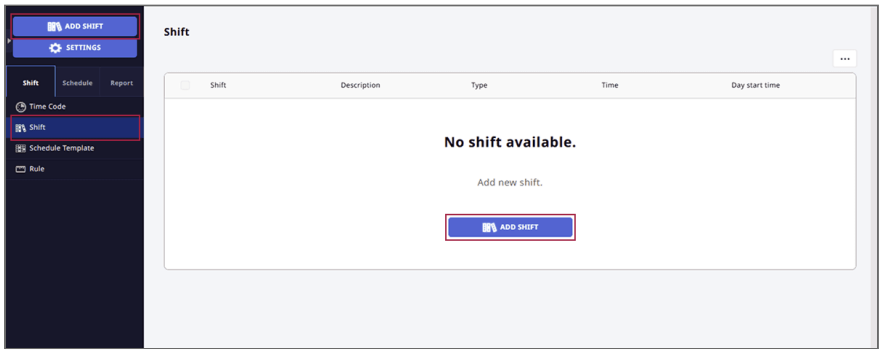
Configura reglas de trabajo diarias basadas en un periodo de 24 horas. Las reglas de trabajo incluyen ajustes de reglas por hora, ajustes de hora de inicio diaria y reglas de redondeo de tiempo.

Configurar Turno Diario

Cree reglas de trabajo aplicando diferentes reglas horarias durante un período de 24 horas. Seleccione entre opciones de trabajo fijo, flexible o flotante y configure la hora de inicio del día, las reglas de redondeo, etc.

ADD SHIFT

1. Haga clic en **T&A** en la página **Launcher**.
2. Haz clic en **Shift** → **Shift** en la barra lateral izquierda.
3. Haga clic en **ADD SHIFT**.



4. Cuando aparezca la pantalla **ADD SHIFT**, configure cada elemento.

Información

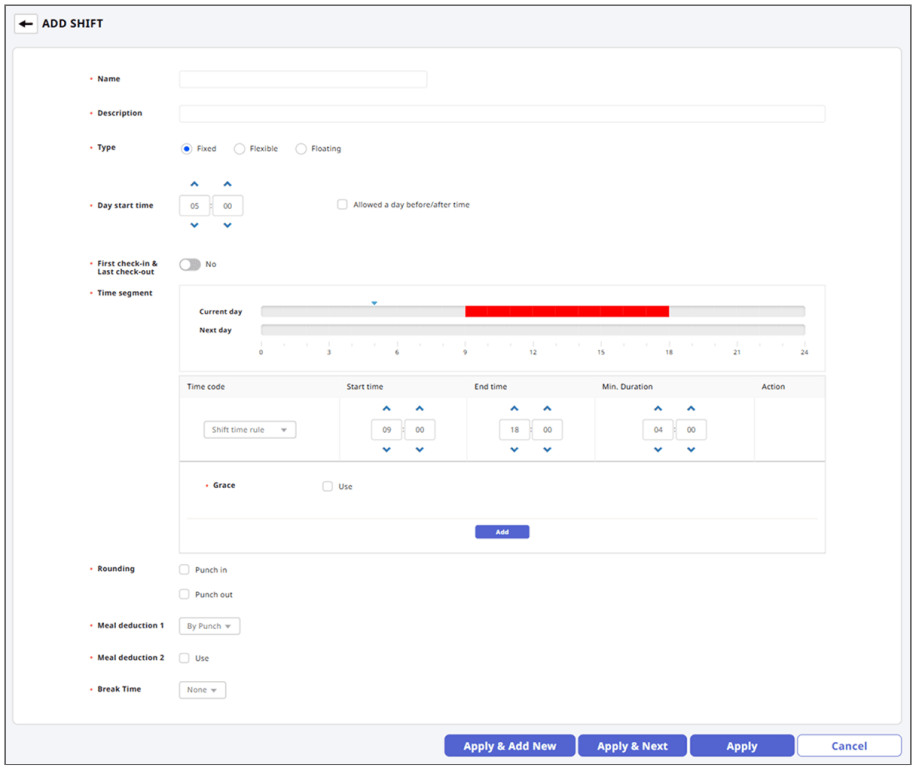
- Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.
- Haga clic en **Apply & Next** para seguir agregando reglas de trabajo semanales.
- Después de guardar la configuración, haga clic en **Apply & Add New** para agregar otro **Shift**.

Guía de opciones de configuración

Según el tipo de regla de trabajo, seleccione **Fixed**, **Flexible** o **Floating**. Las opciones de configuración pueden variar según el tipo de regla de trabajo seleccionado.

Fixed

Es una regla de trabajo para llegada y salida en horas establecidas. Ingrese el nombre y la descripción de Shift y seleccione **Type** como **Fixed**.



- **Day start time**: Establece la hora de inicio de la jornada laboral.

  Allowed a day before/after time permite definir reglas de trabajo para las horas trabajadas en exceso de 24 horas según la hora de inicio del día establecida. Se puede configurar por un máximo de 6 horas.

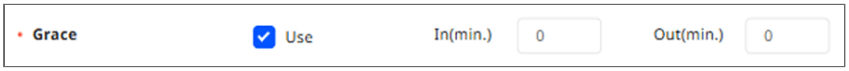


- **First check-in & Last check-out**: Cuando esta opción está activada, la primera hora autenticada se registra como la hora de inicio y la última hora autenticada se registra como la hora de fin.

> **Información**
>
> Cuando esta opción está activada, configura **Break by Punch** para registrar los descansos de los usuarios.

- **Time segment**: Después de seleccionar los elementos configurados en la columna **Time code** para los registros de asistencia, establece **Start time**, **End time** y **Min. Duration**.

  – **Grace**: Configura el tiempo de gracia para permitir trabajo normal cuando se llegue tarde o se salga temprano respecto a la hora establecida.



- **Rounding**: Redondea automáticamente las horas de inicio y fin. Configura las unidades y los estándares para las horas de inicio y fin.



  – **Unit(min)**: Define reglas para redondear la hora registrada cuando los eventos de entrada se registran antes o después de la hora de inicio establecida.

- **Point(min)**: Define reglas para redondear la hora registrada cuando los eventos de salida se registran antes o después de la hora de fin establecida.

> **Consejo**
>
> Por ejemplo, si la hora de entrada se establece a las 09:00 y **Unit(min)** se establece en 15 minutos y **Point(min)** se establece en 8 minutos, el redondeo se hará de la siguiente manera.
>
> - Entrada a las 09:07 → se redondea hacia abajo a 09:00 (menos de 8 minutos)
> - Entrada a las 09:08 → se redondea hacia arriba a 09:15 (8 minutos o más)

> **Información**
>
> La regla **Rounding** tiene prioridad sobre **Grace**.

- **Meal deduction 1** / **Meal deduction 2**: Configura las deducciones por tiempo de comida de las horas laborales diarias.
  - **By Punch**: Configura para deducir según los registros de tiempo en el dispositivo de asistencia sin establecer horarios fijos de comida.
  - **Auto**: Configura para deducir automáticamente los tiempos de comida definiendo **Deduction time** y **Minimal hours before deduction**.
  - **Fixed**: Configura para deducir tiempos fijos definiendo **Start time** y **End time**.

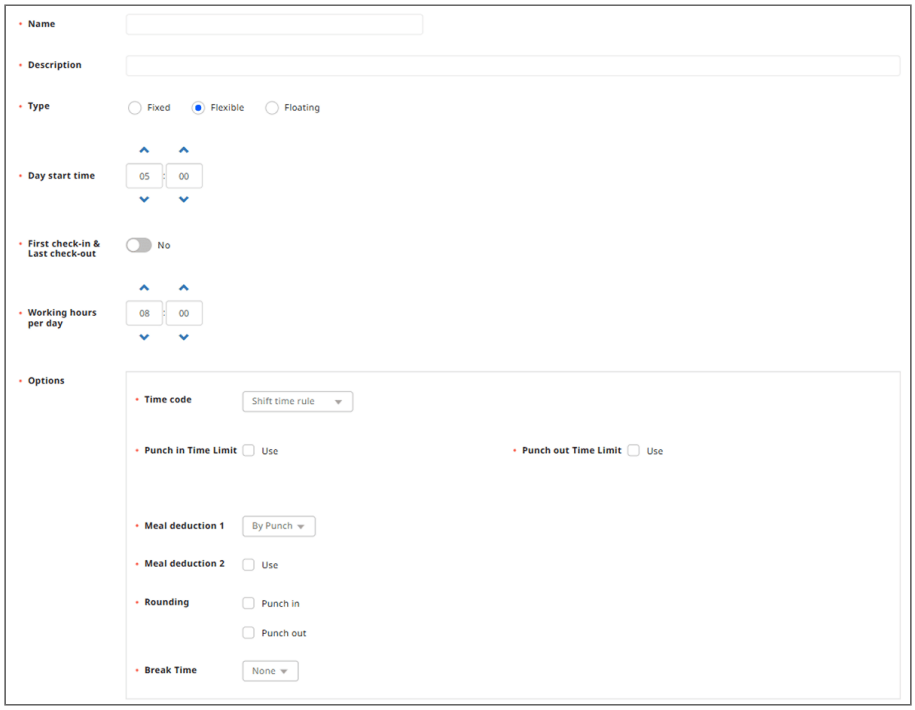
> **Información**
>
> - Usar **Meal deduction 2** permite deducir dos tiempos de comida de las horas laborales diarias.
> - Si los tipos de deducción de comida son **Auto** o **Fixed**, entonces **Meal deduction 1** y **Meal deduction 2** solo pueden configurarse con el mismo tipo.

- **Break Time**: Configura los tiempos de descanso.
  - **By Punch**: Configura para seguir los registros de tiempo del dispositivo de asistencia sin horarios de descanso fijos. Cuando esta opción está activada, configura **Max. allowed break time(min.)**.
  - **Fixed**: Establece **Start time** y **End time** como horarios fijos para los descansos de los usuarios.

> **Información**
>
> - Solo es posible agregar un conjunto de reglas de tiempo establecido como **Attendance management** a Shift.
> - Configure **Start time**, **End time**, **Min. Duration** y **Rounding** para un conjunto de reglas de tiempo establecido como **Overtime management**.

Trabajo flexible

Es una regla de trabajo que establece las horas laborables diarias y ajusta de forma flexible las horas de llegada y salida según la hora de inicio del día. Ingrese el nombre y la descripción de Shift y seleccione **Type** como **Flexible**.



- **Day start time**: Establece la hora de inicio de la jornada laboral.
- **First check-in & Last check-out**: Cuando esta opción está activada, la primera hora autenticada se registra como la hora de inicio y la última hora autenticada se registra como la hora de fin.

> **Información**
> Cuando esta opción está activada, configura **Break by Punch** para registrar los descansos de los usuarios.

- **Working hours
per day**: Establece el total de horas de trabajo del día.
- **Time code**: Selecciona los elementos para los registros de asistencia.
- **Punch in Time Limit** / **Punch out Time Limit**: Configura el rango de tiempo en el que los usuarios pueden autenticar sus horas de entrada y salida.



- **Meal deduction 1** / **Meal deduction 2**: Configura las deducciones por tiempo de comida de las horas laborales diarias.
  - **By Punch**: Configura para deducir según los registros de tiempo en el dispositivo de asistencia sin establecer horarios fijos de comida.
  - **Auto**: Configura para deducir automáticamente los tiempos de comida definiendo **Deduction time** y **Minimal hours before deduction**.
  - **Fixed**: Configura para deducir tiempos fijos definiendo **Start time** y **End time**.

> **Información**
>
> – Usar **Meal deduction 2** permite deducir dos tiempos de comida de las horas laborales diarias.
>
> – Si los tipos de deducción de comida son **Auto** o **Fixed**, entonces **Meal deduction 1** y **Meal deduction 2** solo pueden configurarse con el mismo tipo.

- **Rounding**: Redondea automáticamente las horas de inicio y fin. Configura las unidades y los estándares para las horas de inicio y fin.



  – **Unit(min)**: Define reglas para redondear la hora registrada cuando los eventos de entrada se registran antes o después de la hora de inicio establecida.

  – **Point(min)**: Define reglas para redondear la hora registrada cuando los eventos de salida se registran antes o después de la hora de fin establecida.

> **Consejo**
>
> Por ejemplo, si la hora de entrada se establece a las 09:00 y **Unit(min)** se establece en 15 minutos y **Point(min)** se establece en 8 minutos, el redondeo se hará de la siguiente manera.
>
> – Entrada a las 09:07 → se redondea hacia abajo a 09:00 (menos de 8 minutos)
>
> – Entrada a las 09:08 → se redondea hacia arriba a 09:15 (8 minutos o más)

> **Información**
>
> La regla **Rounding** tiene prioridad sobre **Grace**.

- **Break Time**: Configura los tiempos de descanso.

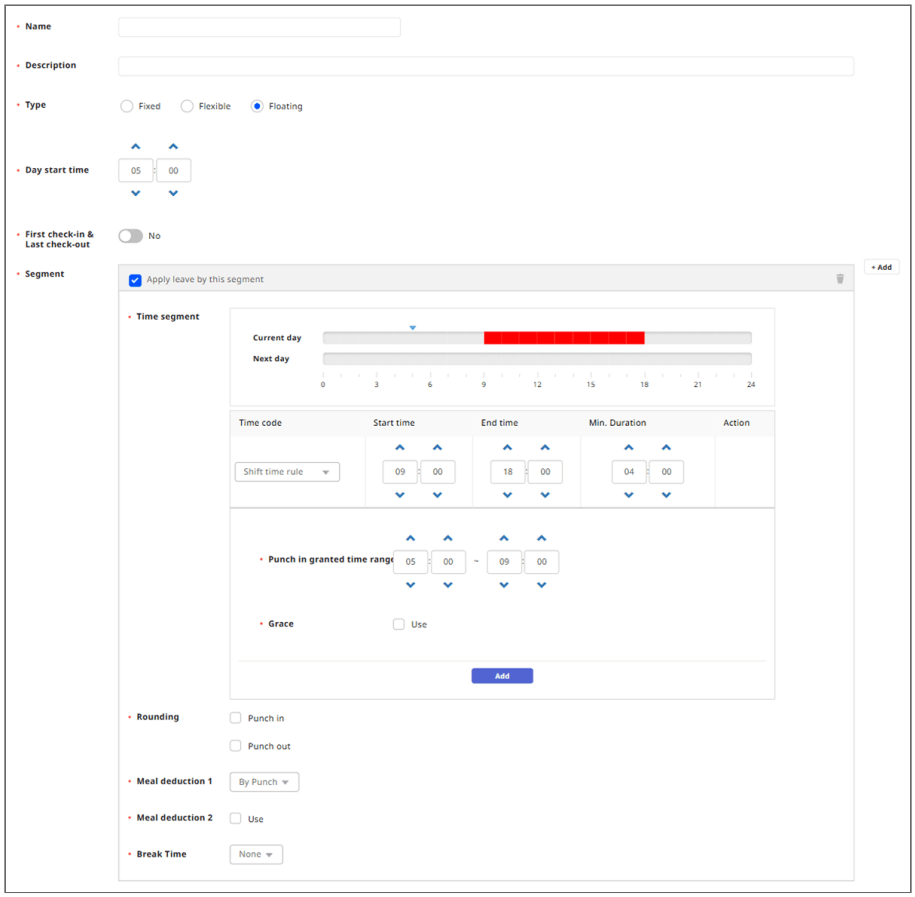
  – **By Punch**: Configura para seguir los registros de tiempo del dispositivo de asistencia sin horarios de descanso fijos. Cuando esta opción está activada, configura **Max. allowed break time(min.)**.

  – **Fixed**: Establece **Start time** y **End time** como horarios fijos para los descansos de los usuarios.

> **Información**
>
> No se puede agregar un conjunto de reglas de tiempo configurado como **Overtime management**.

Turno flotante

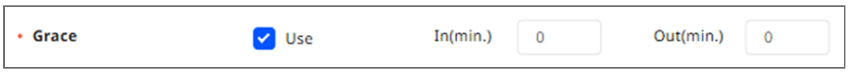
Es una regla de trabajo que permite configurar de manera flexible las horas de llegada y salida. Ingrese el nombre y la descripción de Shift y seleccione **Type** como **Floating**.



- **Day start time**: Establece la hora de inicio de la jornada laboral.
- **First check-in & Last check-out**: Cuando esta opción está activada, la primera hora autenticada se registra como la hora de inicio y la última hora autenticada se registra como la hora de fin.

> **Información**
> Cuando esta opción está activada, configura **Break by Punch** para registrar los descansos de los usuarios.

- **Time segment**: Después de seleccionar los elementos configurados en la columna **Time code** para los registros de asistencia, establece **Start time**, **End time** y **Min. Duration**.
  - **Punch in granted time range**: Configura el rango horario que se considerará trabajo normal cuando se llegue antes o se salga después de la hora de inicio o fin establecida.
  - **Grace**: Configura el tiempo de gracia para permitir trabajo normal cuando se llegue tarde o se salga temprano respecto a la hora establecida.



- **Rounding**: Redondea automáticamente las horas de inicio y fin. Configura las unidades y los estándares para las horas de inicio y fin.



  - **Unit(min)**: Define reglas para redondear la hora registrada cuando los eventos de entrada se registran antes o después de la hora de inicio establecida.

  - **Point(min)**: Define reglas para redondear la hora registrada cuando los eventos de salida se registran antes o después de la hora de fin establecida.

> **Consejo**
>
> Por ejemplo, si la hora de entrada se establece a las 09:00 y **Unit(min)** se establece en 15 minutos y **Point(min)** se establece en 8 minutos, el redondeo se hará de la siguiente manera.
>
> - Entrada a las 09:07 → se redondea hacia abajo a 09:00 (menos de 8 minutos)
> - Entrada a las 09:08 → se redondea hacia arriba a 09:15 (8 minutos o más)

> **Información**
>
> La regla **Rounding** tiene prioridad sobre **Grace**.

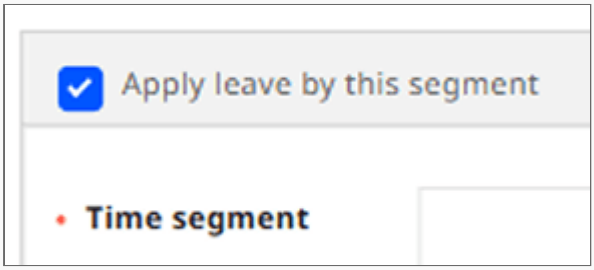
- **Meal deduction 1** / **Meal deduction 2**: Configura las deducciones por tiempo de comida de las horas laborales diarias.
  - **By Punch**: Configura para deducir según los registros de tiempo en el dispositivo de asistencia sin establecer horarios fijos de comida.
  - **Auto**: Configura para deducir automáticamente los tiempos de comida definiendo **Deduction time** y **Minimal hours before deduction**.
  - **Fixed**: Configura para deducir tiempos fijos definiendo **Start time** y **End time**.

> **Información**
>
> - Usar **Meal deduction 2** permite deducir dos tiempos de comida de las horas laborales diarias.
> - Si los tipos de deducción de comida son **Auto** o **Fixed**, entonces **Meal deduction 1** y **Meal deduction 2** solo pueden configurarse con el mismo tipo.

- **Break Time**: Configura los tiempos de descanso.
  - **By Punch**: Configura para seguir los registros de tiempo del dispositivo de asistencia sin horarios de descanso fijos. Cuando esta opción está activada, configura **Max. allowed break time(min.)**.
  - **Fixed**: Establece **Start time** y **End time** como horarios fijos para los descansos de los usuarios.

Información

- Los turnos de trabajo pueden consistir en hasta cinco franjas horarias. Haga clic en **+ Add** para agregar una franja horaria.
- Al configurar ausencias, debe seleccionarse la opción **Apply leave by this segment**. Se puede seleccionar **Apply leave by this segment** entre las franjas horarias configuradas en los turnos de trabajo.



- Configure **Start time**, **End time**, **Min. Duration** y **Rounding** para un conjunto de reglas de tiempo establecido como **Overtime management**.

Siguiente paso

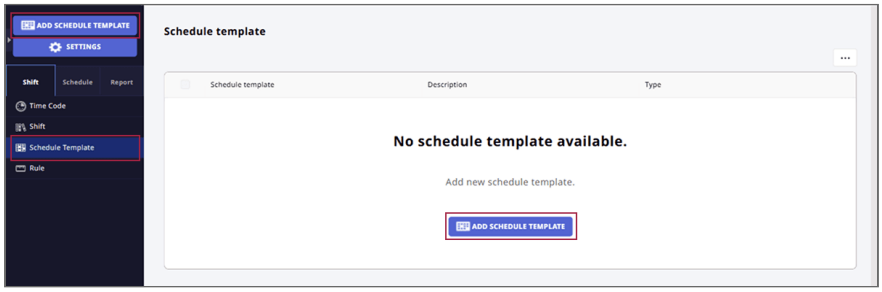
Configure reglas de trabajo semanales basadas en las reglas diarias configuradas. Configure reglas de trabajo semanales de forma semanal o diaria.

Configurar Turnos Semanales

Esta guía explica cómo crear reglas de turno semanales basadas en las Shift configuradas.

ADD SCHEDULE TEMPLATE

1. Haga clic en **T&A** en la página **Launcher**.
2. Haz clic en **Shift** → **Schedule Template** en la barra lateral izquierda.
3. Haz clic en **ADD SCHEDULE TEMPLATE**.

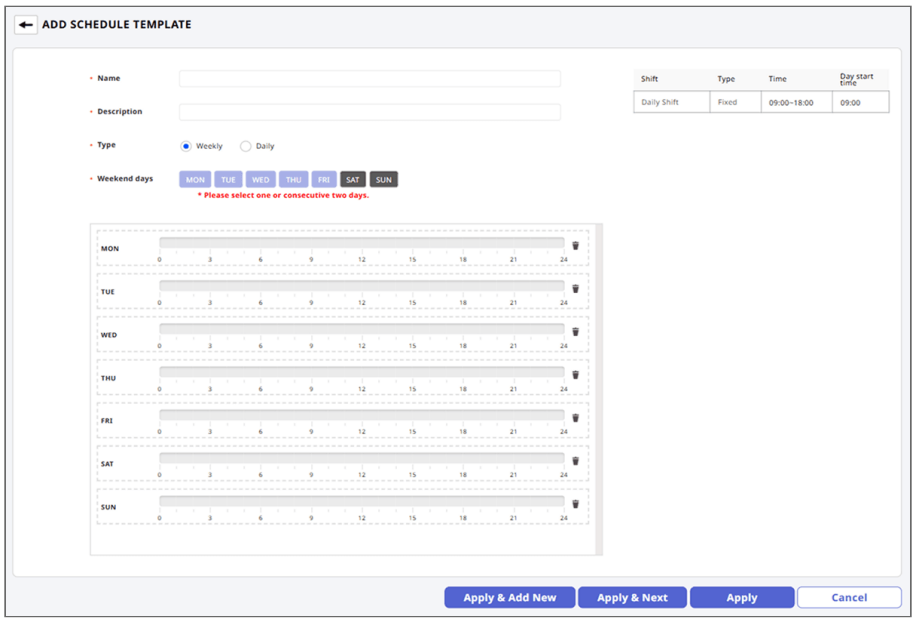


4. Cuando aparezca la pantalla **ADD SCHEDULE TEMPLATE**, configura cada elemento.

Información

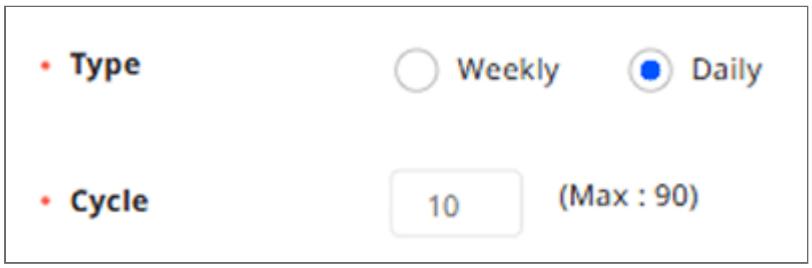
- Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.
- Para seguir agregando el horario de trabajo, haz clic en **Apply & Next**.
- Después de guardar la configuración, haz clic en **Apply & Add New** para agregar otra **Schedule Template**.

Guía de opciones de configuración



- **Name**: Ingresa el nombre de Schedule Template.
- **Description**: Ingresa una descripción para Schedule Template.
- **Type**: Establece Schedule Template como **Weekly** o **Daily**.

  Al seleccionar **Daily**, podrás establecer el período de uso repetido (**Cycle**).



- **Weekend days**: Establece los días que se designarán como fines de semana.
- **Shift**: Consulta la lista de reglas Shift configuradas.
- Horario semanal/diario: Arrastra y suelta las Shift configuradas.



Información

- Para aplicar a todos de lunes a domingo, haz clic en **Copy All**.
- Para eliminar la Shift aplicada, haz clic en el botón 🗑.
- Al aplicar la Shift establecida con **Allowed a day before/after time**, no se puede establecer un exceso de tiempo que se sitúe más de 24 horas antes de la hora de inicio de las reglas de turno diarias.

Siguiente paso

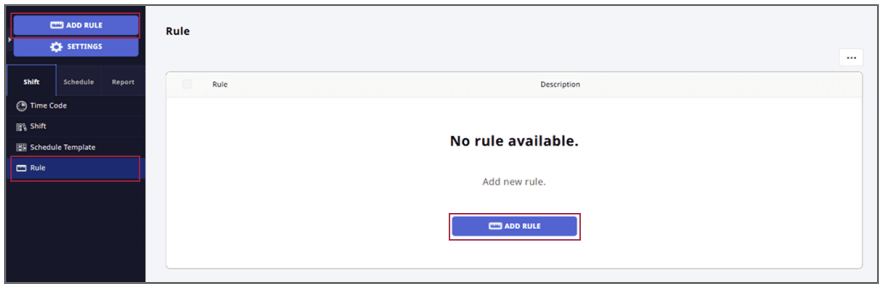
Esta guía explica cómo crear reglas de turno flexibles aplicando reglas de horas extra adicionales a las reglas de turno diarias.

Configurar Otras Reglas de Trabajo

Esto es útil cuando las reglas de horas extra no se añaden a Shift. Los ajustes de horas extra en Shift tienen horas de inicio y fin, mientras que Rule calcula el total de horas más allá del horario laboral regular. Rule es conveniente para gestionar el total de horas extra de forma diaria, semanal o mensual. Cuando se configura Rule, reemplaza las reglas de horas extra añadidas a Shift.

ADD RULE

1. Haga clic en **T&A** en la página **Launcher**.
2. Haz clic en **Shift** → **Rule** en la barra lateral izquierda.
3. Haz clic en **ADD RULE**.



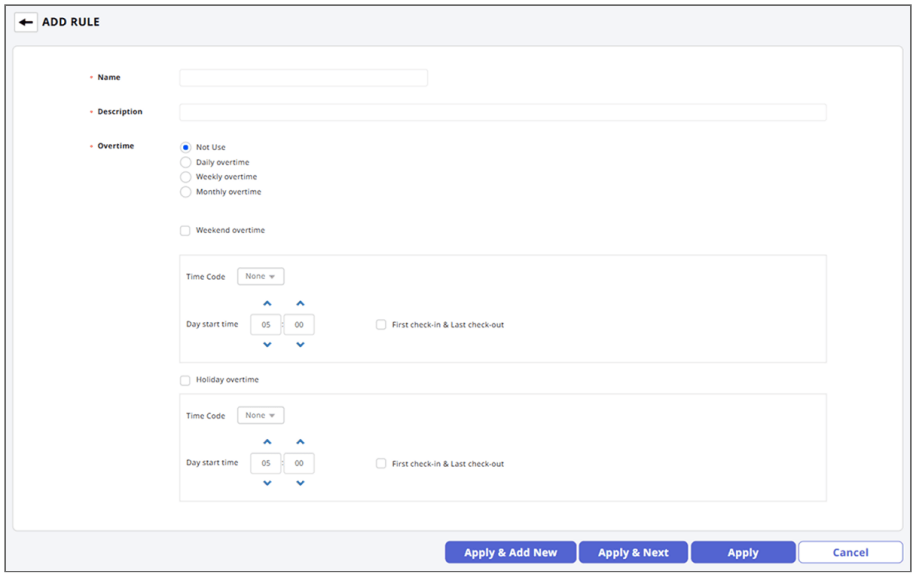
4. Cuando aparezca la pantalla **ADD RULE**, configure cada elemento.

Información

- Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.
- Para seguir agregando el horario de trabajo, haz clic en **Apply & Next**.
- Después de guardar los ajustes, haz clic en **Apply & Add New** para agregar otra **Rule**.

Guía de opciones de configuración

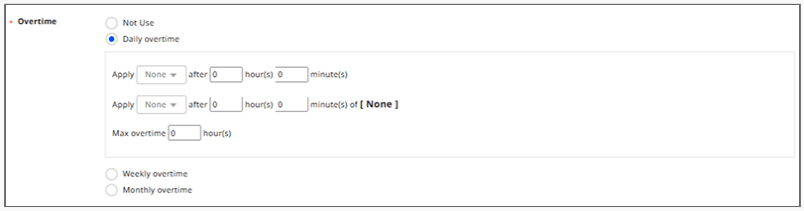
Configure Rule. Puede establecer reglas de horas extra para aplicar de forma diaria, semanal o mensual.



- **Name**: Ingrese el nombre de Rule.
- **Description**: Ingrese una descripción para Rule.
- **Overtime**: Seleccione las reglas de horas extra que se aplicarán después del horario laboral regular de forma diaria, semanal o mensual. Puede aplicar otras reglas de horas extra después de un cierto período de tiempo. También puede establecer un límite máximo de horas extra para restringir la cantidad de horas extra que un empleado puede trabajar.

Consejo

Si se configura como se indica a continuación, la regla de tiempo **Overtime(1.5)** se aplicará de 5:00 p. m. a 11:00 p. m. cuando el horario laboral regular sea de 8:00 a. m. Además, las horas extra diarias están limitadas a un máximo de 9 horas, y solo los registros hasta las 2:00 a. m. se utilizarán para calcular los salarios diarios.



> **Información**
> El total de horas trabajadas no incluye pausas ni tiempos de comida.

- **Weekend overtime** / **Holiday overtime**: Configure las reglas de trabajo que se aplicarán los fines de semana o días festivos.
  - **Time Code**: Seleccione el Time Code que se aplicará.
  - **Day start time**: Configure la hora de inicio del trabajo.
  - **First check-in & Last check-out**: Registra la hora en que el primer usuario se autenticó como hora de inicio y la hora en que el último usuario se autenticó como hora de fin.

Siguiente paso

Esto lo guía sobre cómo configurar su horario de trabajo mediante la configuración del período, usuarios, otras reglas de trabajo y calendarios de vacaciones.

Configurar el Horario

Cree horarios de trabajo especificando Shift, Rule, la duración y los días festivos.

También agregue horarios temporales o licencias personales al horario de trabajo creado.

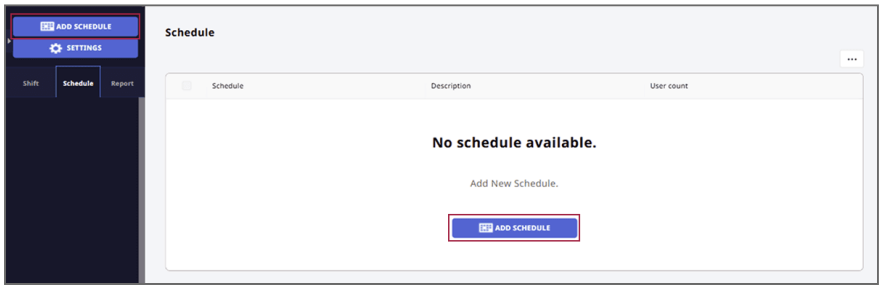
> **Información**
> Antes de crear el horario, asegúrese de haber creado correctamente Time Code, Shift, Shift y los días festivos.
> - Para obtener más información sobre la configuración de reglas de trabajo, consulte lo siguiente:
>   - Establecer Código de Tiempo
>   - Configurar Turno Diario
>   - Configurar Turnos Semanales
>   - Configurar Otras Reglas de Trabajo
> - Para obtener más información sobre la configuración de días festivos, consulte Ajustes de Horario.

Horario de trabajo

Agregar un horario

Agregue el horario de trabajo para los usuarios registrados como se indica a continuación.

1. Haga clic en **T&A** en la página **Launcher**.
2. Haga clic en la pestaña **Schedule** en la barra lateral izquierda de la pantalla.
3. Haz clic en **ADD SCHEDULE**.

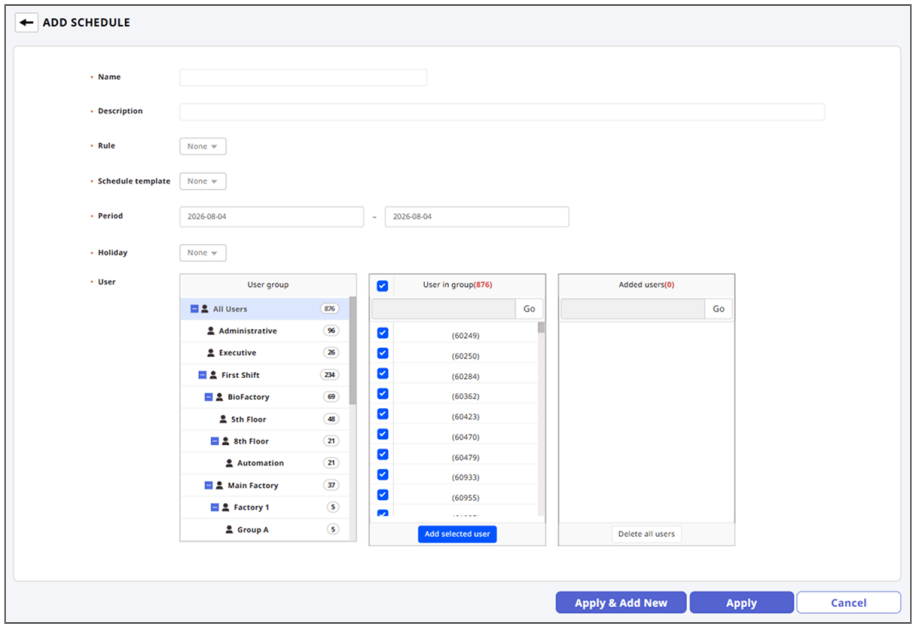


4. Cuando aparezca la pantalla **ADD SCHEDULE**, configure cada elemento.

> **Información**
>
> - Haz clic en **Apply** en la parte inferior de la pantalla para guardar la configuración.
> - Después de guardar los ajustes, haz clic en **Apply & Add New** para agregar otra **Schedule**.

Guía de opciones de configuración

Guía de opciones de configuración del horario de trabajo.



- **Name**: Ingrese el nombre del horario de trabajo.
- **Description**: Ingrese una descripción para el horario de trabajo.
- **Rule**: Seleccione el Rule configurado. Configurar Rule ignora las reglas de horas extra establecidas en Shift. Seleccione **None** si no se utiliza.

  > **Información**
  >
  > Si el Rule deseado no está disponible, agrégalo. Para obtener más información, consulte Configurar Otras Reglas de Trabajo.

- **Schedule template**: Seleccione la Schedule template configurada. Una vez configurada, Schedule template no se puede modificar.

> **Información**
> Si la Schedule template deseada no está disponible, agréguela. Para obtener más información, consulte Configurar Turnos Semanales.

- **Period**: Defina el periodo para recopilar eventos de asistencia.

> **Información**
> La fecha de inicio no se puede cambiar una vez establecida. La fecha de finalización se puede cambiar más adelante y, si se cambia a una fecha anterior a la establecida, se eliminarán los eventos de asistencia del periodo modificado.

- **Holiday**: Seleccione el calendario de días festivos configurado. Seleccione **None** si no se utiliza.

> **Información**
> Si el calendario de días festivos deseado no está disponible, agréguelo. Para obtener más información sobre la configuración de días festivos, consulte Ajustes de Horario.

- **User**: Agregue usuarios para aplicar las reglas.

> **Información**
> La cantidad de usuarios incluida en el horario de trabajo general no puede exceder el máximo admitido por su licencia registrada de gestión de asistencia. El número máximo de usuarios por licencia se detalla en Política de Licencias.

Editar un horario

Guía para modificar horarios de trabajo registrados.

1. Haga clic en **T&A** en la página **Launcher**.
2. Haga clic en la pestaña **Schedule** en la barra lateral izquierda de la pantalla.
3. Haga clic en el elemento que desea modificar de la lista **Schedule**. Como alternativa, haz clic en ✎ en la opción que vas a modificar en la barra lateral izquierda de la pantalla.
4. Modifica la opción y haz clic en **Apply**.

Eliminar un horario

Guía para eliminar horarios de trabajo registrados.

1. Haga clic en **T&A** en la página **Launcher**.
2. Haga clic en la pestaña **Schedule** en la barra lateral izquierda de la pantalla.
3. Haga clic en la casilla de verificación del elemento que desea eliminar de la lista **Schedule**.



4. Haz clic en **Delete schedule** en la esquina superior derecha de la pantalla. Como alternativa, haz clic en 🗑 en la opción que vas a eliminar en la barra lateral izquierda de la pantalla.

5. Cuando aparezca el mensaje de confirmación, haz clic en **Yes**.

Agregar un horario temporal

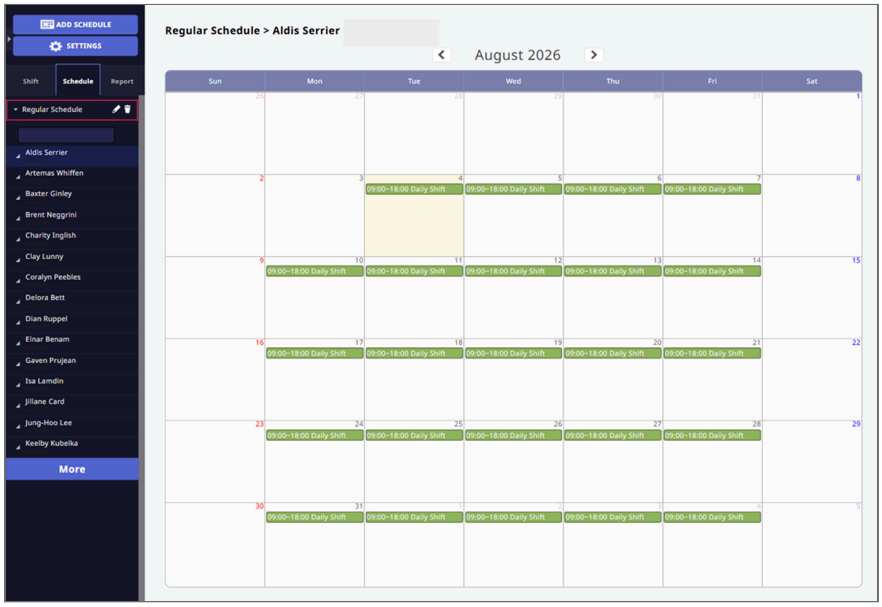
Si ya hay un horario registrado, se puede aplicar al usuario una regla de trabajo temporal diferente.

1. Haga clic en **T&A** en la página **Launcher**.

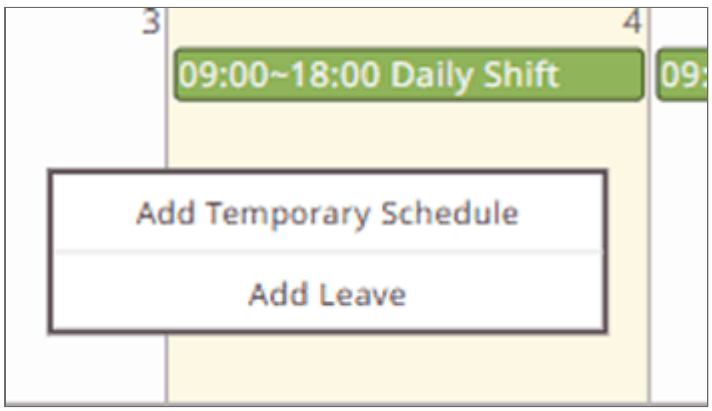
2. Haga clic en la pestaña **Schedule** en la barra lateral izquierda de la pantalla.

3. Haz clic en ▶ en el horario deseado de la lista del lado izquierdo de la pantalla.

4. Aparecerá una lista de usuarios asignados al horario y, al seleccionar un usuario para aplicar un horario temporal, se mostrará el calendario.

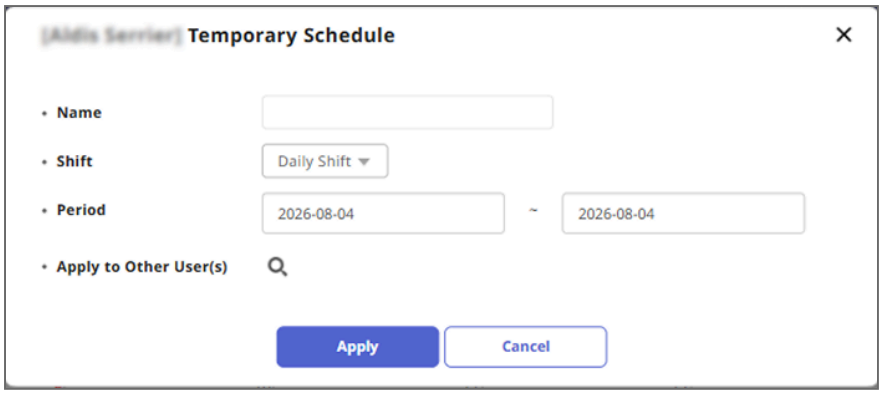


5. Haga clic en la fecha del calendario a la que desea agregar un horario temporal.



6. Haga clic en **Add Temporary Schedule** en el menú emergente.

7. Cuando aparezca la ventana de configuración **Add Temporary Schedule**, configure cada elemento.



Para aplicar el mismo horario de trabajo a otros usuarios, haz clic en y selecciona los usuarios.

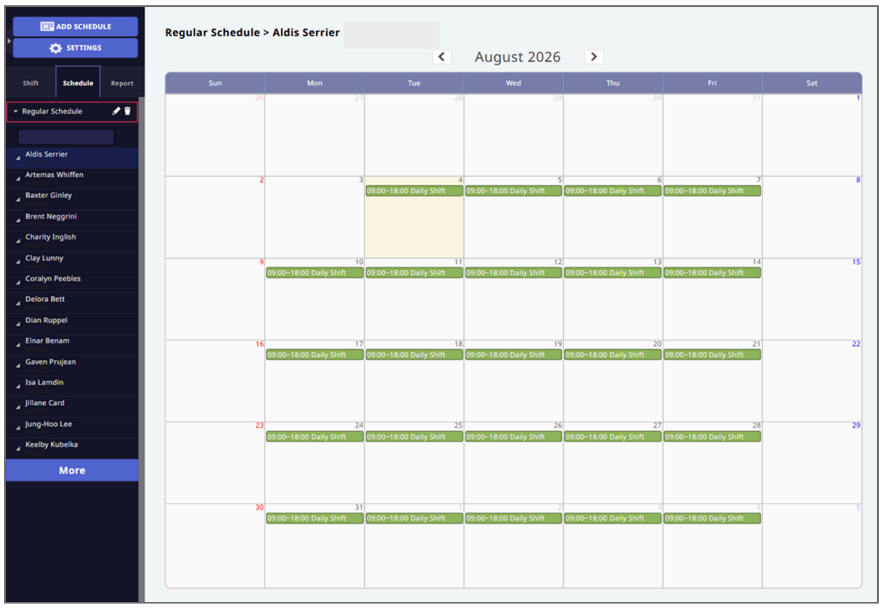
8. Haz clic en **Apply** para aplicar las reglas de trabajo establecidas.

> **Información**
> Para eliminar el horario temporal aplicado al usuario, haga clic en el horario temporal establecido en el calendario. Haga clic en **Yes** cuando aparezca la ventana del mensaje de confirmación.

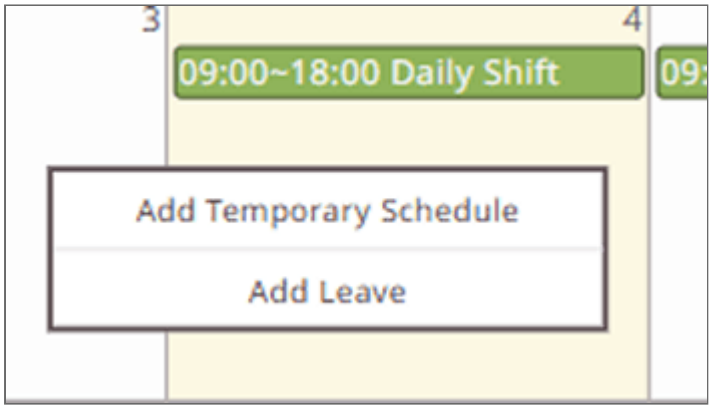
Agregar y eliminar una ausencia

Agregue el horario de ausencia personal de un usuario.

1. Haga clic en **T&A** en la página **Launcher**.
2. Haga clic en la pestaña **Schedule** en la barra lateral izquierda de la pantalla.
3. Haz clic en ▶ en el horario deseado de la lista del lado izquierdo de la pantalla.
4. Aparecerá una lista de usuarios asignados al horario y, al seleccionar un usuario para aplicar el horario de ausencia, se mostrará el calendario.

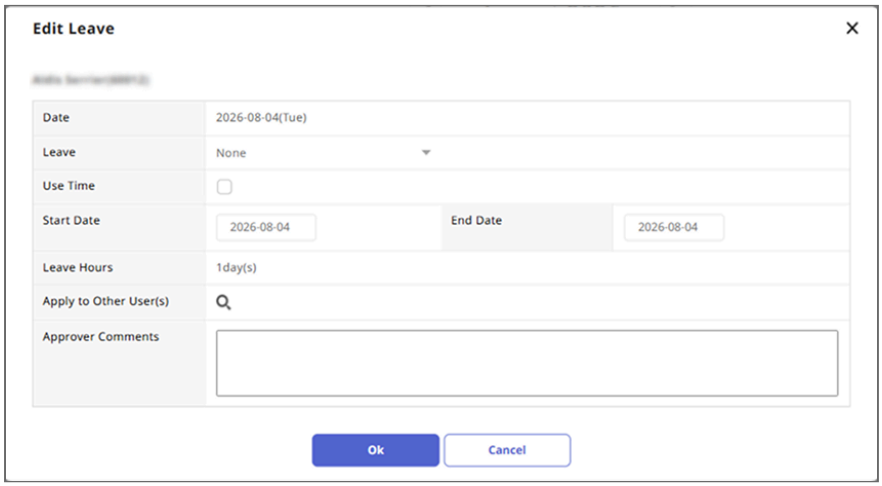


5. Haga clic en la fecha del calendario para agregar el horario de ausencia del usuario.



6. Haga clic en **Add Leave** en el menú emergente.

7. Cuando aparezca la ventana de configuración **Edit Leave**, configure cada elemento.

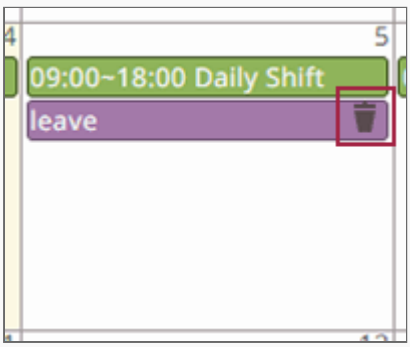


Para aplicar el mismo horario de ausencia a otros usuarios, haz clic en 🔍 y selecciona los usuarios.

8. Haz clic en **Apply** para aplicar el horario de ausencia establecido.

Información

- Si las reglas de tiempo de gestión de ausencias deseadas no están disponibles, agréguelas. Para obtener más información sobre cómo agregar reglas de tiempo, consulte Establecer Código de Tiempo.
- Para eliminar el horario de ausencia aplicado al usuario, haz clic en 🗑 del horario de ausencia establecido en el calendario. Haga clic en **Yes** cuando aparezca la ventana del mensaje de confirmación.



Ver el Informe

Puede generar informes de T&A a partir de los eventos de asistencia de los usuarios recopilados en el sistema y editar los registros de tiempo o exportarlos como archivos CSV o PDF.

Utilice fácilmente los siete filtros de informe predefinidos; además, los administradores pueden configurar sus propios filtros.

Antes de comenzar

Antes de usar el informe multilingüe

BioStar X admite coreano e inglés de forma predeterminada. Para utilizar informes multilingües, configure el idioma deseado según las siguientes instrucciones.

1. Vaya a la siguiente ruta. *C:\Program Files\BioStar X\plugin\ta\dist\setup\report_fonts*
2. Cree una carpeta con el nombre del idioma que desea usar. Consulte las normas ISO 639-1 para los nombres de idiomas. Por ejemplo, para usar español, cree una carpeta llamada "es".
3. Copie y pegue las fuentes en la carpeta creada. Solo se admite una fuente TrueType.

Antes de actualizar el informe

BioStar X utiliza MariaDB como base de datos predeterminada. Si utiliza la base de datos MS SQL Server, verifique primero los siguientes elementos.

Al usar **BioStar X** con MS SQL Server, si hay muchos usuarios registrados, el uso de memoria en la PC puede acumularse cada vez que se actualiza el informe. Restablezca la memoria máxima del servidor de la base de datos MS SQL Server.

1. Ejecute **Microsoft SQL Server Management Studio**.
2. Haga clic derecho en la base de datos **BioStar X** en el explorador de objetos.
3. Haga clic en **Propiedades** en el menú emergente.
4. Haga clic en **Memory** y reduzca el valor de **Maximum server memory**.

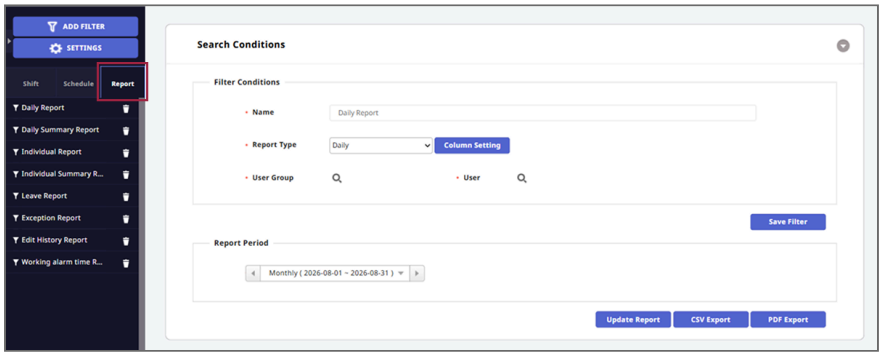
> **Información**
> Para obtener más información sobre la configuración de MariaDB y MS SQL Server durante la instalación de **BioStar X**, consulte Instalación Personalizada.

Comprobar el informe

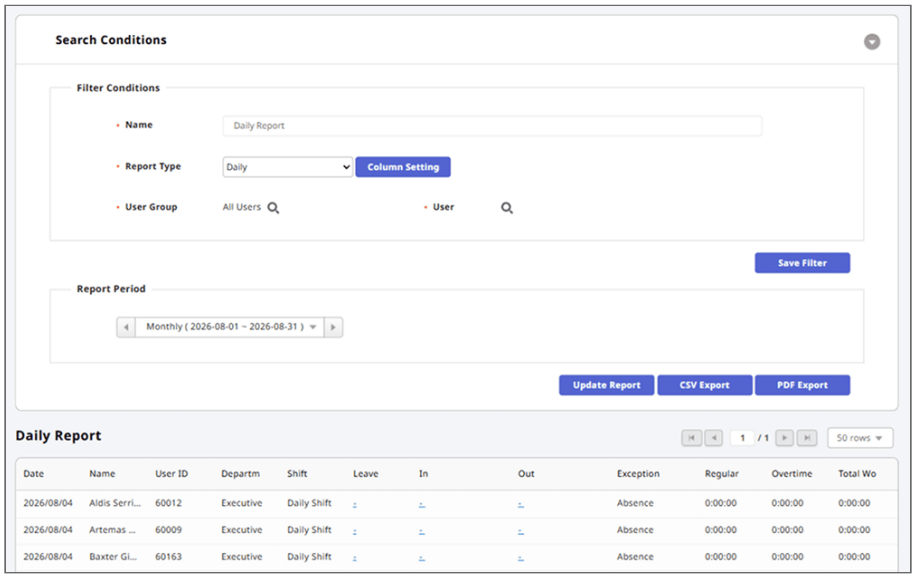
Generar el informe

Aquí se proporcionan instrucciones para generar informes de registros de asistencia de usuarios registrados.

1. Haga clic en **T&A** en la página **Launcher**.
2. Haga clic en la pestaña **Report** en la barra lateral izquierda de la pantalla.

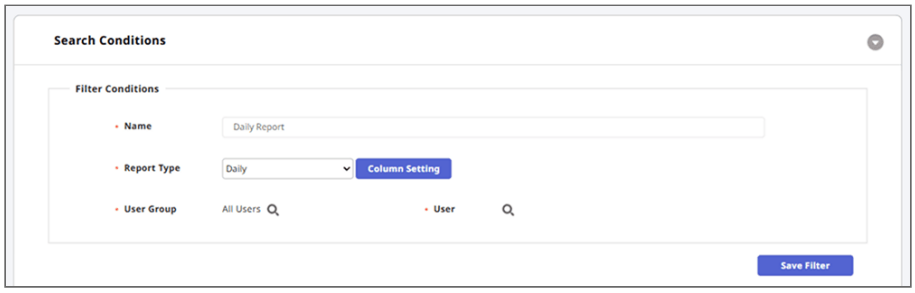


3. Haga clic en el filtro de informe deseado en la barra lateral izquierda de la pantalla.
4. En **User Group** o **User**, haga clic en el botón 🔍 y luego especifique el grupo o usuario.
5. Para generar el informe, haga clic en el botón **Update Report**.
6. Cuando la lista de informes aparezca en la parte inferior de la pantalla, puede hacer clic en el elemento deseado para ver los detalles.



Configurar las condiciones de filtro

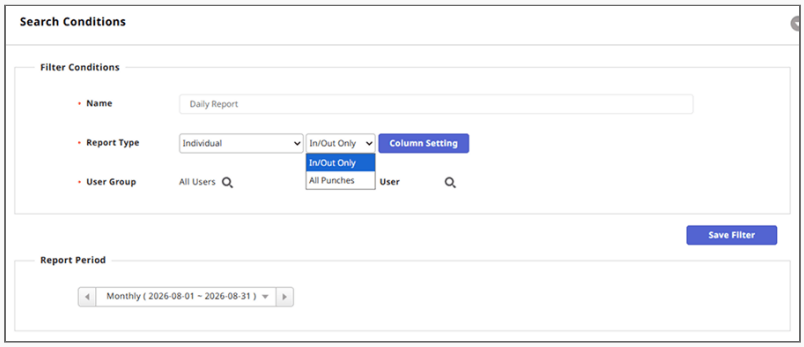
Puede configurar condiciones de filtro para generar un nuevo informe de registros de T&A.



- **Name**: Ingrese el nombre del informe.
- **Report Type**: Seleccione el tipo de informe deseado. Los tipos de informe disponibles son los siguientes.
  - **Daily**, **Daily Summary**, **Individual**, **Individual Summary**, **Leave**, **Exception**, **Modified Punch Log History**, **Working alarm time**

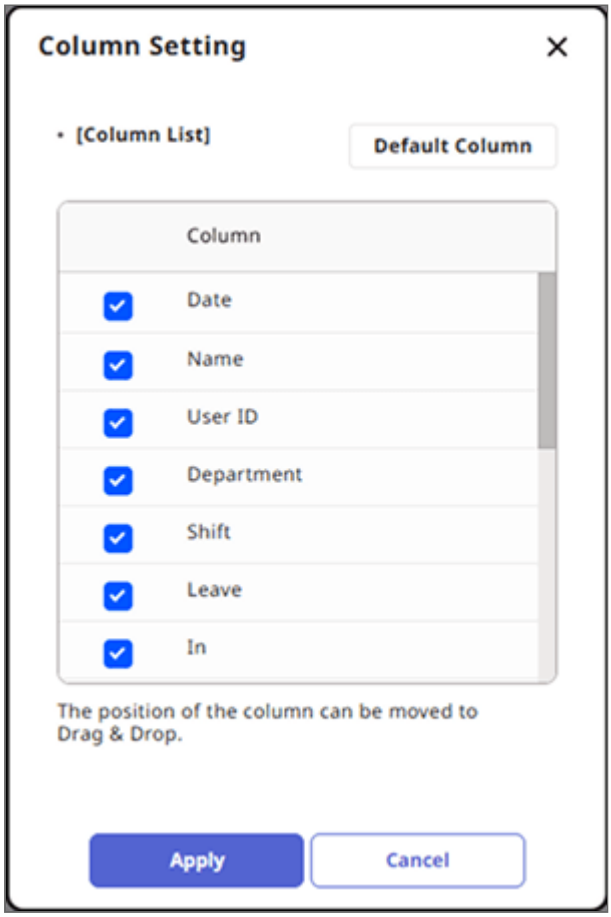
Información

Al seleccionar **Report Type** como **Individual**, puede configurar si se mostrarán los registros de entrada del usuario.



- **In/Out Only**: Esto solo muestra los registros de entrada y salida del usuario en el informe.
- **All Punches**: Esto muestra todos los registros de entrada del usuario en el informe.

- **Column Setting**: Puede cambiar el orden de las columnas de la tabla de informe u ocultarlas.

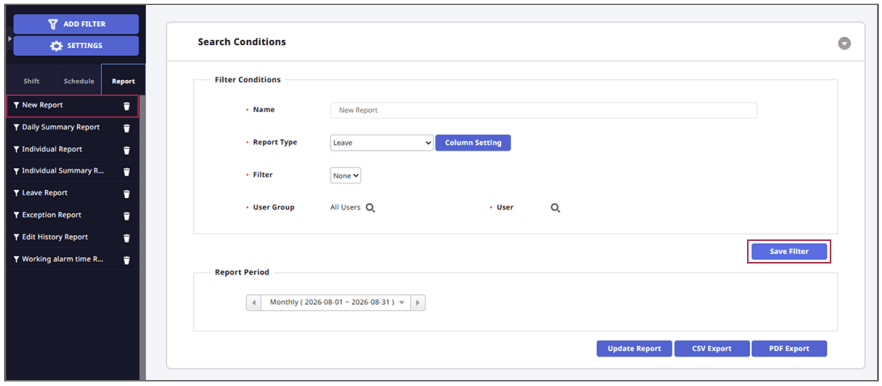


Información

Después de cambiar el orden de las columnas, haga clic en el botón **Default Column** para restaurar los valores predeterminados.

- **Filter**: Esto solo se activará cuando **Report Type** esté configurado como **Leave** o **Exception**, y puede elegir condiciones específicas para registros de ausencias o excepciones.

- **User Group** / **User**: Seleccione el grupo de usuarios o usuario para generar el informe.
- **Save Filter**: Puede guardar el informe de asistencia configurado como un filtro.



Configurar período del informe

Aquí se proporcionan instrucciones para configurar el período del informe.



Puede establecer el período del informe como **Daily**, **Weekly** o **Monthly**. Para generar un informe para un período específico, seleccione **Custom**.

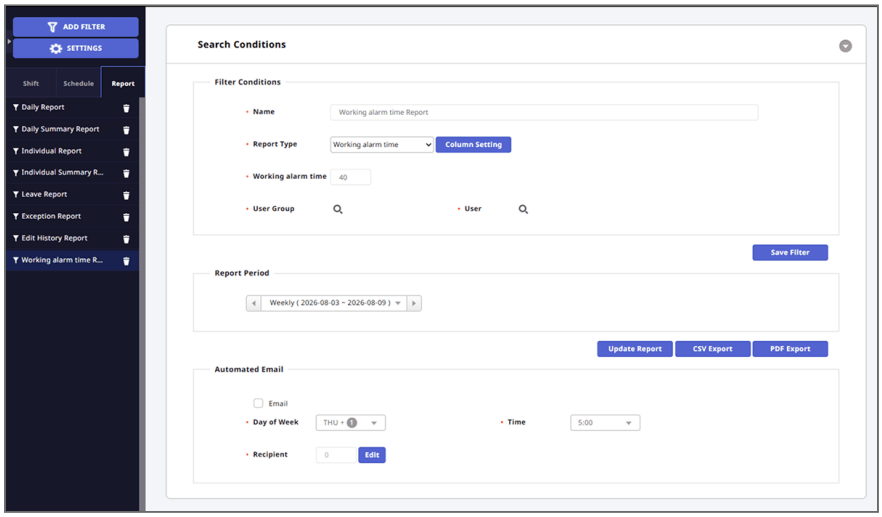
Exportar informe

- **CSV Export**: Puede guardar el informe generado como un archivo CSV.
- **PDF Export**: Puede guardar el informe generado como un archivo PDF.

Generar informe de horas de alarma de trabajo

Puede generar informes de T&A para los usuarios que hayan alcanzado las horas laborales designadas o notificar al administrador por correo electrónico. El informe de horas laborales de alerta se genera semanalmente.

1. Haga clic en **T&A** en la página **Launcher**.
2. Haga clic en la pestaña **Report** en la barra lateral izquierda de la pantalla.
3. Haga clic en **Working Alarm Time Report** en la lista de filtros de la barra lateral izquierda.



4. Configure cada elemento en **Filter Conditions** y **Report Period**.

5. Para generar el informe, haga clic en el botón **Update Report**.

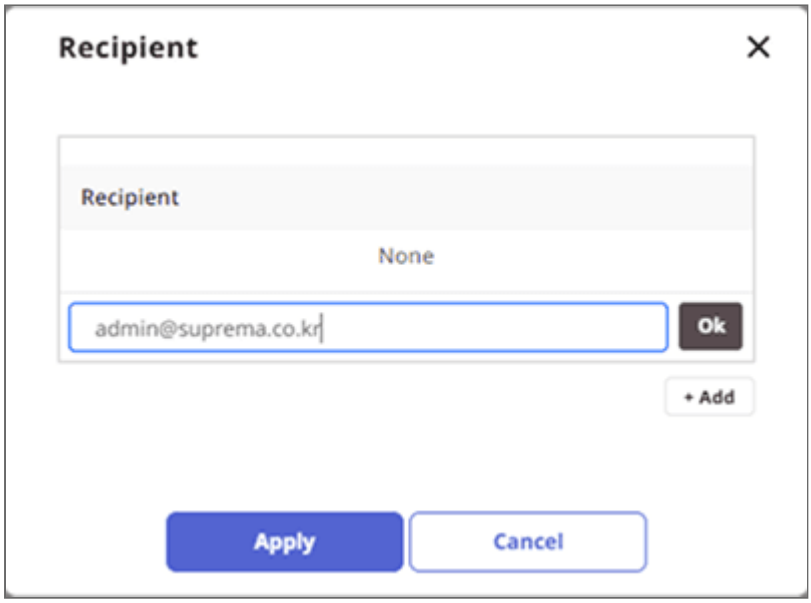
> **Información**
>
> Para enviar notificaciones al administrador por correo electrónico para los usuarios que hayan alcanzado las horas laborales designadas, configure **Automated Email**. Para obtener más información, consulte Configuración del envío automático de correos electrónicos.

Configuración del envío automático de correos electrónicos

Puede enviar automáticamente correos electrónicos de alarma al administrador para los usuarios que hayan alcanzado las horas laborales designadas.



- **Email**: Marque la casilla para enviar correos electrónicos automáticamente al administrador.
- **Day of Week**: Seleccione el día de la semana para enviar correos electrónicos al administrador.
- **Time**: Configure la hora para enviar correos electrónicos al administrador.
- **Recipient**: Puede especificar el administrador que recibirá el correo electrónico. Haga clic en **Edit** para abrir la ventana **Recipient**. Ingrese la dirección de correo electrónico. Puede especificar más de un administrador.



Información

- Establezca las condiciones de filtro y luego guarde el filtro para configurar la función **Automated Email**.
- Configure la información del remitente de los correos electrónicos enviados automáticamente en **Setting**(⚙) → **Sender Information** en la barra lateral izquierda de la pantalla. Para obtener más información, consulte Configurar Tiempo y Asistencia.

Editar Informe de T&A

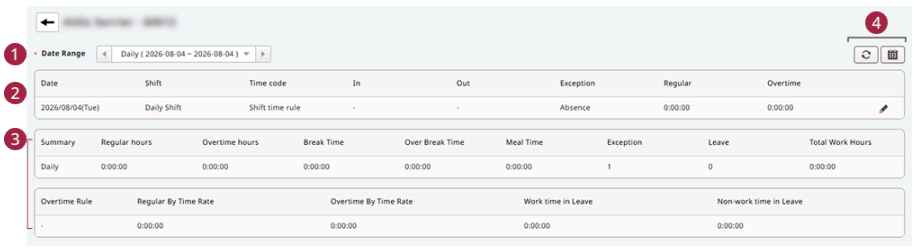
Haz clic en la tabla del informe generado para modificar los registros de asistencia.

Información

- Primero debes generar un informe para modificar los registros de asistencia. Para obtener más información sobre la generación de informes, consulte Ver el Informe.
- No se pueden modificar los registros de los usuarios sin un horario de asistencia.

1. Haz clic en el elemento de la lista de informes generados para modificar el registro.
2. Modifica los registros de asistencia o agrega ausencias según sea necesario.

Editar en la lista



1. **Date Range**: Configura el período de los registros de asistencia que se mostrará en la lista.
2.

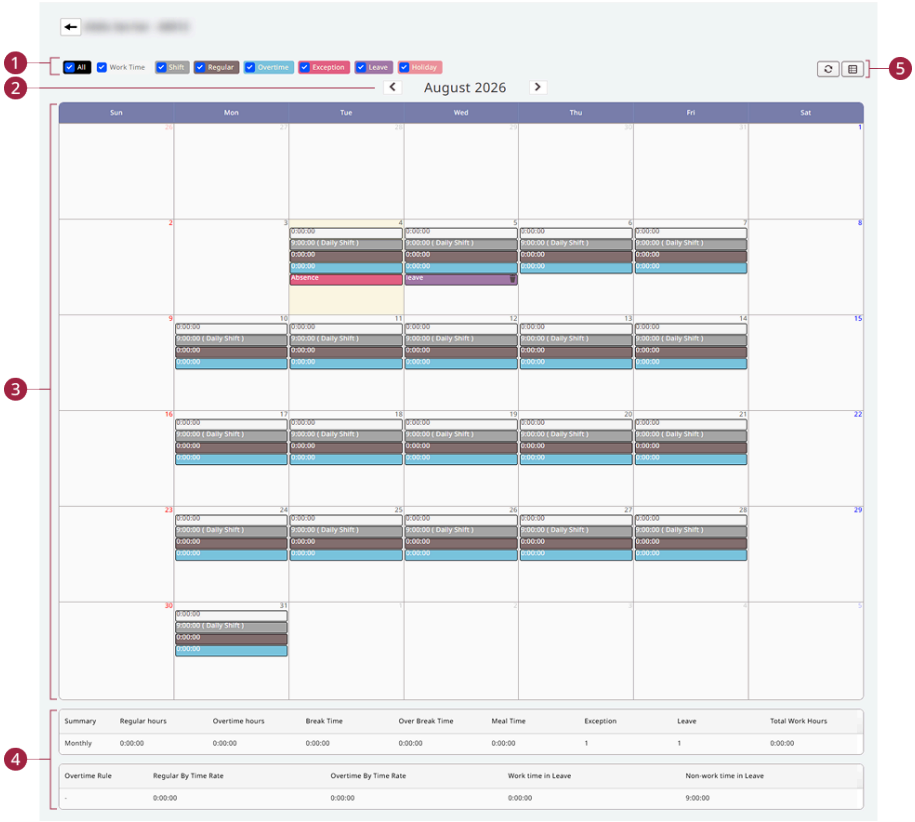
Registro diario de asistencia: Muestra el registro diario de asistencia.

- Haz clic en las horas de entrada/salida para agregar, modificar o eliminar registros de asistencia. Después de hacer clic en las horas de entrada/salida, haga clic en para modificar el registro de asistencia y haga clic en **Apply** para guardar los cambios.
- Haga clic en para agregar una ausencia. Necesitas un código de tiempo configurado como ausencia para agregar vacaciones. Haz clic en en la ausencia agregada del usuario para eliminarla.

3. **Resumen de registros de asistencia**: Revisa los registros de asistencia del período especificado.
4. **Actualizar / Ver en calendario**
   - : Actualiza la lista de registros de asistencia.
   - : Visualiza los registros de asistencia en formato de calendario.

> **Información**
> Para obtener más información sobre la creación de reglas de horario, consulte Establecer Código de Tiempo.

Editar en el calendario



1. **Tipo de evento**: Selecciona u oculta los tipos de evento que aparecerán en el calendario.
2. **Mes**: Haz clic en < o > para moverte al mes anterior o siguiente.
3. **Registro diario de asistencia**: Muestra el registro diario de asistencia.
   - Haz clic en el horario de trabajo (en blanco) para agregar, modificar o eliminar registros de asistencia. Haga clic

en ✎ para modificar el registro de asistencia y haga clic en **Apply** para guardar los cambios.

- Haz clic en las reglas de trabajo (en gris) para agregar gestión de ausencias de usuario. Necesitas un código de tiempo configurado como ausencia para agregar una ausencia de usuario. Haz clic en 🗑 en la ausencia agregada del usuario para eliminarla.

4. **Registro diario de asistencia**: Muestra el registro diario de asistencia.
5. **Actualizar / Ver en lista**
   - ⟳: Actualiza la lista de registros de asistencia.
   - ▤: Visualiza los registros de asistencia en formato de lista.

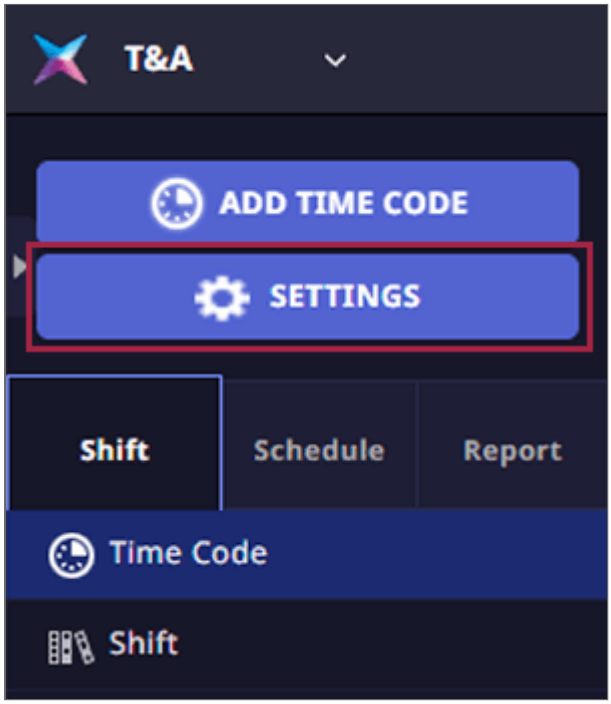
> **Información**
> Para obtener más información sobre la creación de reglas de horario, consulte Establecer Código de Tiempo.

Configurar Tiempo y Asistencia

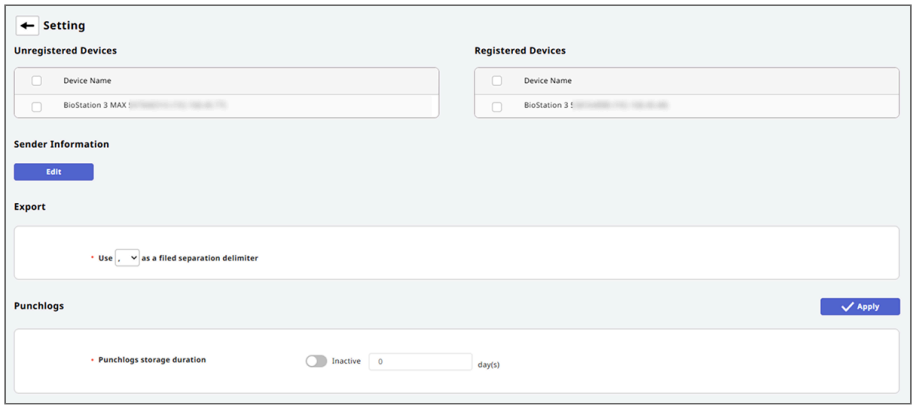
Puede registrar dispositivos para usarlos en la gestión de asistencia o establecer la información del remitente que se utilizará al enviar correos electrónicos de notificación. También puede establecer el delimitador de documentos para exportar informes de asistencia en formato CSV.

Acceder a la configuración de gestión de asistencia

1. Haga clic en **T&A** en la página **Launcher**.
2. Haga clic en ⚙ **Settings** en la barra lateral izquierda.



3. Edite los campos necesarios.



Configuración de gestión de asistencia

Unregistered Devices

Lista de dispositivos que se pueden usar para la gestión de asistencia. Para registrarlo como dispositivo de gestión de asistencia, seleccione el dispositivo deseado y haga clic en **Register**.



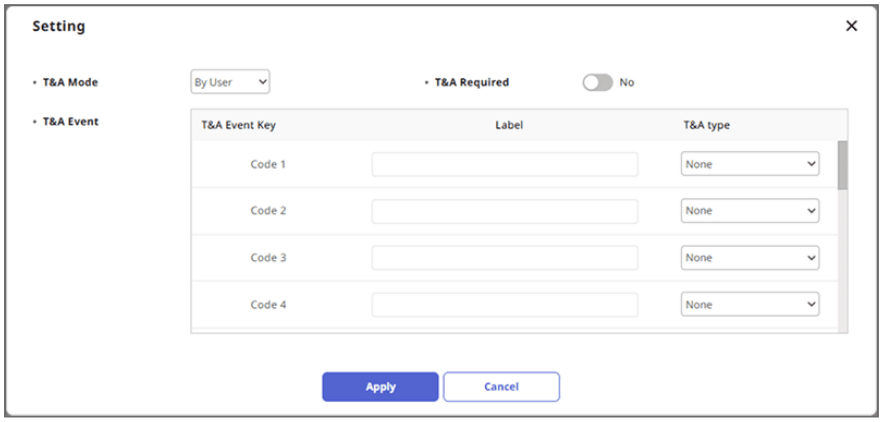
Registered Devices

Lista de dispositivos que se utilizan actualmente para la gestión de asistencia.

- Para darlo de baja, seleccione el dispositivo deseado y haga clic en **Unregister**.



- Para editar la configuración de asistencia de un dispositivo registrado, haga clic en **Setting**. Para obtener más información sobre la configuración de asistencia, consulte Configuración Avanzada.



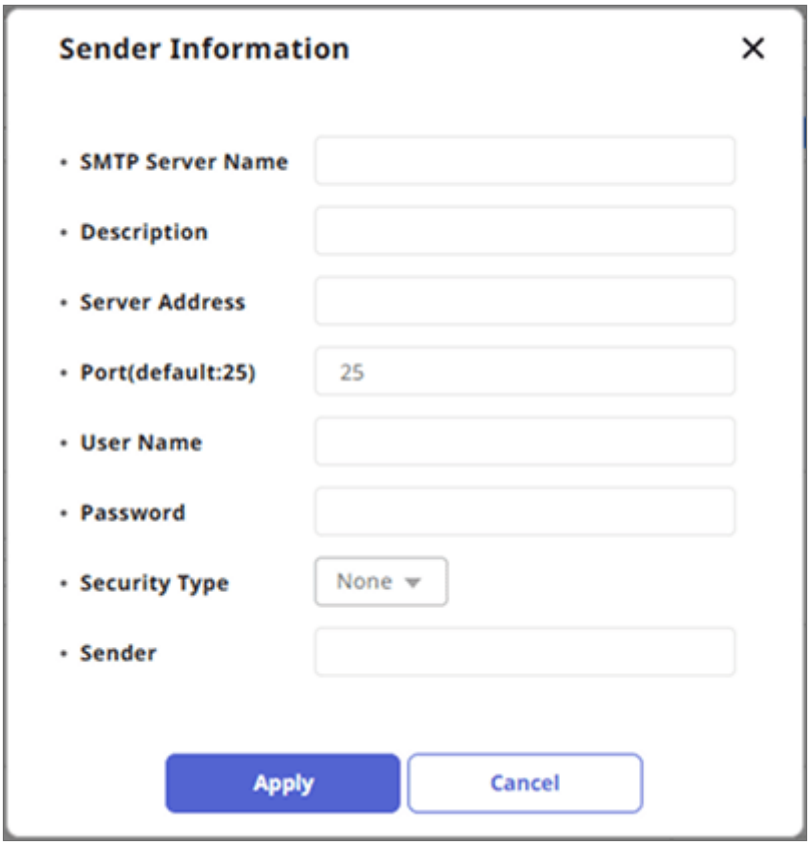
T&A type es una configuración para asignar **T&A Event Key** con los tipos de eventos de asistencia. Los tipos de eventos de asistencia son los siguientes:

- **Check In**
- **Check Out**
- **Break Start**
- **Break End**
- **Meal Time Start**
- **Meal Time End**

> **Información**
>
> - Solo puede editar la configuración de asistencia de un dispositivo cuando esté conectado a él.
> - Si elimina un dispositivo registrado del menú **Settings** → **Device** → **Device**, el sistema también elimina automáticamente el dispositivo de gestión de asistencia registrado.
> - Si establece la opción **Multi Face Authentication** en **Use**, el dispositivo no incluye soporte para la gestión de asistencia. Para obtener más información sobre **Multi Face Authentication**, consulta Configuración de Autenticación.

Sender Information

Puede establecer la información del remitente que se utilizará al enviar correos electrónicos de notificación. Haga clic en **Edit**.



- **SMTP Server Name**: Ingrese el nombre del servidor SMTP.
- **Description**: Ingrese la descripción.
- **Server Address**: Ingrese la dirección del servidor SMTP. La dirección del servidor SMTP usa el formato `smtp.{email-service-provider}.com`. Confírmela en la pantalla de ajustes del correo electrónico utilizado como servidor SMTP.

- **Port(default:25)**: Ingrese el número de puerto del servidor SMTP. Confírmela en la pantalla de ajustes del correo electrónico utilizado como servidor SMTP.
- **User Name**: Ingrese la cuenta del servicio SMTP.
- **Password**: Ingrese la contraseña del servicio SMTP.
- **Security Type**: Seleccione el tipo de seguridad.
- **Sender**: Ingrese la dirección de correo electrónico del remitente.

Información

- Para obtener más información sobre SMTP, contacte al administrador del sistema.
- Al usar el servidor SMTP como cuenta de correo con autenticación de dos factores y cambiar la contraseña de la cuenta, tenga en cuenta lo siguiente: Una vez que configure la autenticación de dos factores, la contraseña SMTP es la misma que la contraseña de la aplicación generada mediante la autenticación de dos factores, no la contraseña de la cuenta de correo.
  - Al configurar la autenticación en dos pasos, la contraseña SMTP usa la contraseña de aplicación generada por la autenticación en dos pasos, no la contraseña de la cuenta de correo.
  - En ese momento, si se cambia la contraseña de la cuenta de correo, la contraseña de la aplicación se elimina automáticamente y la contraseña SMTP deja de estar disponible.
  - Al cambiar la contraseña de la cuenta de correo, genere nuevamente la contraseña de la aplicación y luego configure otra vez la contraseña SMTP.

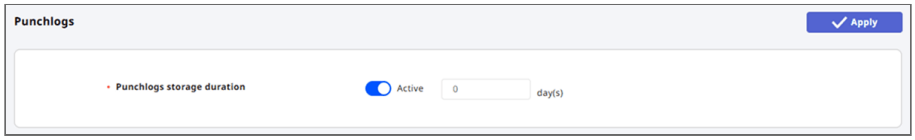
Export

Con la función **CSV Export**, puede elegir el delimitador de documentos al exportar informes de asistencia.



Punchlogs

Puede establecer el período de almacenamiento de los registros de asistencia. Establezca la opción **Punchlogs storage duration** en **Active** e ingrese el período. Para guardar la configuración, haga clic en **Apply**.



Ver Registros de Auditoría de Tiempo y Asistencia

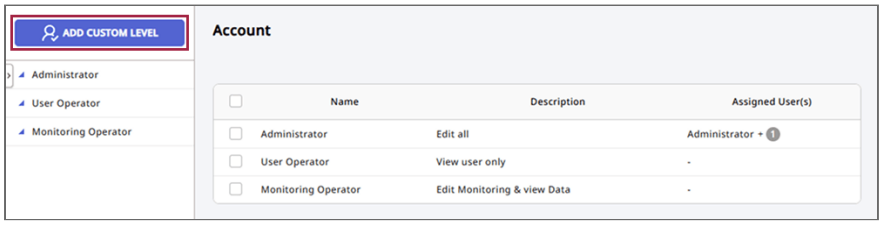
La característica **T&A Audit Log** registra todas las actividades relacionadas con la gestión de tiempo y asistencia, como trabajo, horarios e informes. Cada registro muestra cuándo ocurrió, quién hizo el cambio, qué cambió y cómo, para respaldar auditorías y la resolución de problemas.

Información

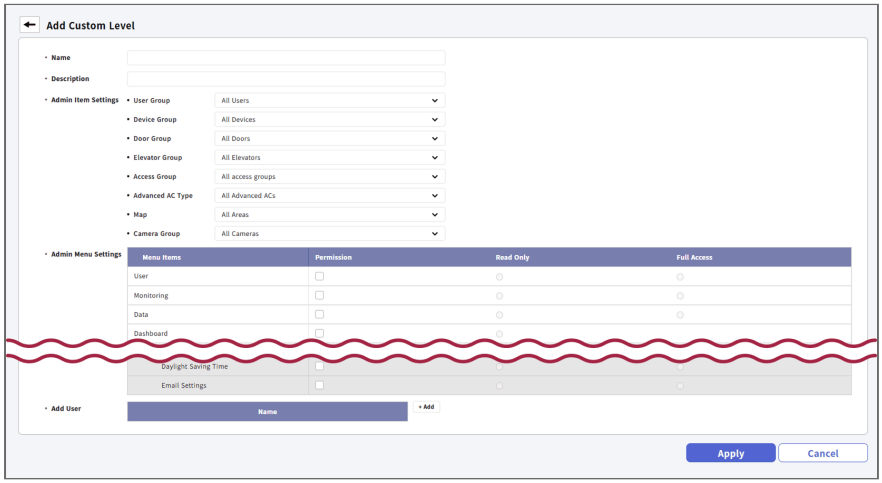
El menú **T&A Audit Log** requiere una licencia activa de Tiempo y Asistencia (T&A) y permiso de administrador de operaciones. La cuenta **T&A Operator** creada de forma predeterminada durante la instalación del complemento de Tiempo y Asistencia no incluye este permiso. Agregue y asigne un permiso personalizado.

Agregar permiso de auditoría de tiempo y asistencia

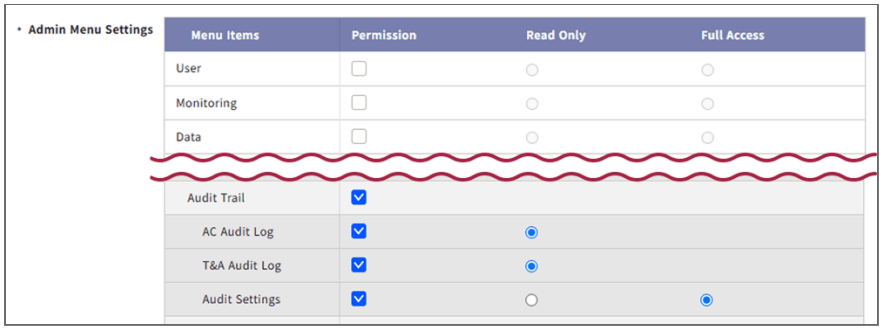
1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Account** → **Account** en la barra lateral izquierda.
3. Haga clic en **Add Custom Level**.



4. Ingrese un nombre y una descripción del permiso para ver los registros de auditoría de tiempo y asistencia.



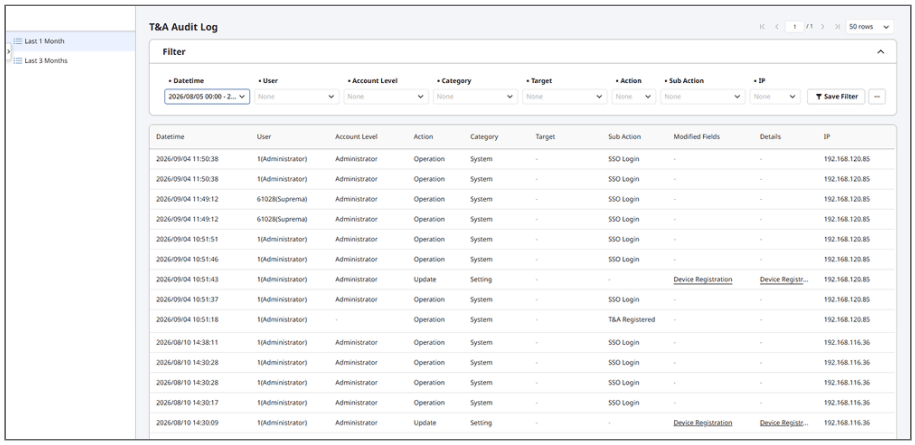
5. En **Admin Menu Settings**, establezca permisos para **T&A Audit Log** y **Audit Settings** en el menú **Audit Trail**.



6. En **Add User**, haga clic en **+ Add** y seleccione un grupo de usuarios o usuarios individuales.
7. Haga clic en **Apply** en la parte inferior de la pantalla para guardar el permiso personalizado.

Ver registros de auditoría de tiempo y asistencia

1. Haz clic en **Settings** en la página **Launcher**.
2. Haga clic en **Audit Trail** → **T&A Audit Log** en la barra lateral izquierda.
3. La lista de registros de auditoría de tiempo y asistencia aparece en la pantalla.



> **Información**
>
> - Para cambiar las políticas del registro de auditoría, como el período de retención, consulte Configurar Auditoría de Tiempo y Asistencia.
> - Después de actualizar a la versión 1.0.3, el sistema cifra los nuevos registros de auditoría, independientemente de la opción **Encrypt Personal Data on Database** en **Settings** → **System** → **Security**.
> - Si el sistema no registra ciertos registros de auditoría después de la actualización de BioStar 2 a **BioStar X**, consulte Actualizar.

Diseño de la tabla

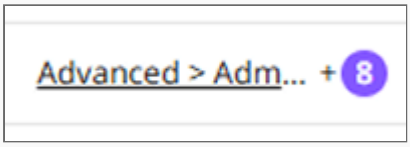
La tabla de la lista de registros de auditoría tiene 10 columnas y muestra los registros en orden descendente por **Datetime**.

Columna	Descripción
Datetime	Fecha y hora en que ocurrió el evento.
User	Usuario que realizó el evento. Aparece en el formato **id(nombre)**.
Account Level	El nivel de administrador del usuario que realizó el evento. Deje este campo en blanco para las acciones que el sistema ejecuta automáticamente.
Action	El tipo de acción ejecutada. Este campo muestra **Create**, **Update**, **Delete**, **Read**, **Export** o **Operation**.
Category	Categoría de dominio del destino del evento. (**Shift**, **Schedule**, **Report**, **T&A Audit Log**, **Setting**, **System**)
Target	Destino al que se aplica la acción. Aparece en el formato **type: id(name)**.

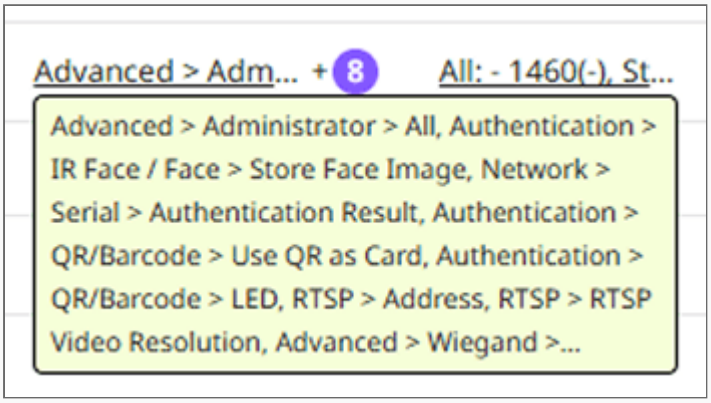
Columna	Descripción
Sub Action	Nombre detallado de la acción que aparece solo para las acciones **Operation**, **Read** y **Export**.
Modified Fields	Nombre del campo que cambió o se consultó. Deje siempre **Operation** en blanco.
Details	Información detallada de cada acción. (Valores cambiados, condiciones de consulta, instantáneas de campos y más)
IP	Dirección IP desde la cual el usuario accedió. El sistema muestra los registros emitidos automáticamente como **127.0.0.1**.

Información

- Los registros en los que **Action** es **Update** siempre se refieren a 1 solo destino. Time and Attendance no incluye la edición masiva que cambia varios destinos a la vez. Por eso, los destinos nunca aparecen como grupo.
- Los nombres que aparecen en **User**, **Target** y **Change Details** conservan el valor del momento en que ocurrió el registro. Si el nombre cambia después o se elimina el destino, el nombre que aparece en los registros anteriores se mantiene.
- Si el valor de **Target** o **Modified Fields** tiene 2 entradas o más, solo se muestra la primera y el resto se contrae en una insignia con el conteo restante a la derecha (p. ej., **+208**). Si el conteo restante es de 1,000 o más, la insignia muestra **+999**. Revise el conteo total exacto en el título de la ventana emergente de detalles. Haga clic en la insignia para abrir la ventana emergente de detalles de esa celda.

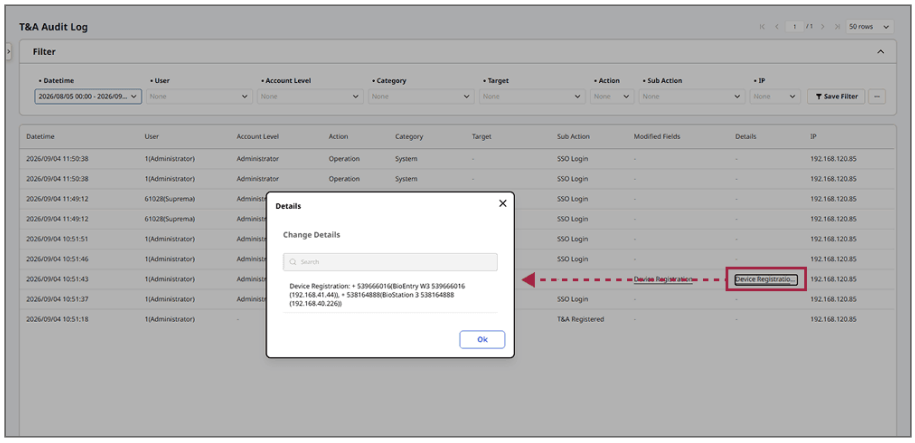


- Los valores largos de las celdas se truncan a una línea con puntos suspensivos. Pase el cursor sobre el valor para ver el texto completo en la información sobre herramientas. La información sobre herramientas trunca el texto excedente como ...



Ver detalles

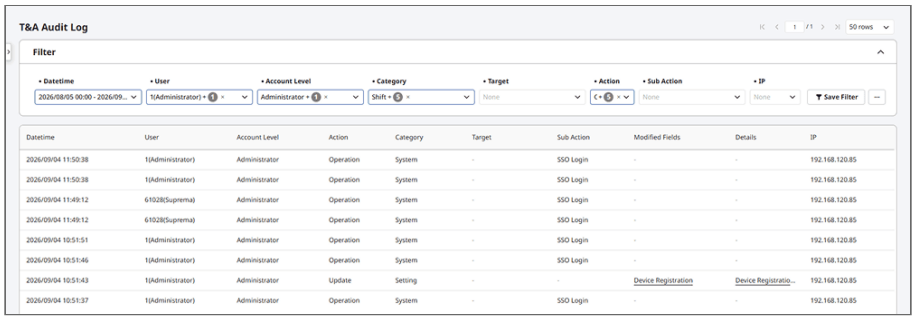
Las celdas con valores en **Target**, **Modified Fields** o **Details** aparecen subrayadas y permiten hacer clic. Haga clic en una celda para abrir la ventana emergente de detalles de la acción de esa fila. Ciérrela con **OK** o ✕.



Escriba una palabra clave en el campo **Search** en la parte superior de la ventana emergente para resaltar o filtrar las entradas coincidentes. Al buscar, la ventana emergente de destino actualiza los grupos y el recuento por grupo. El total del título no cambia.

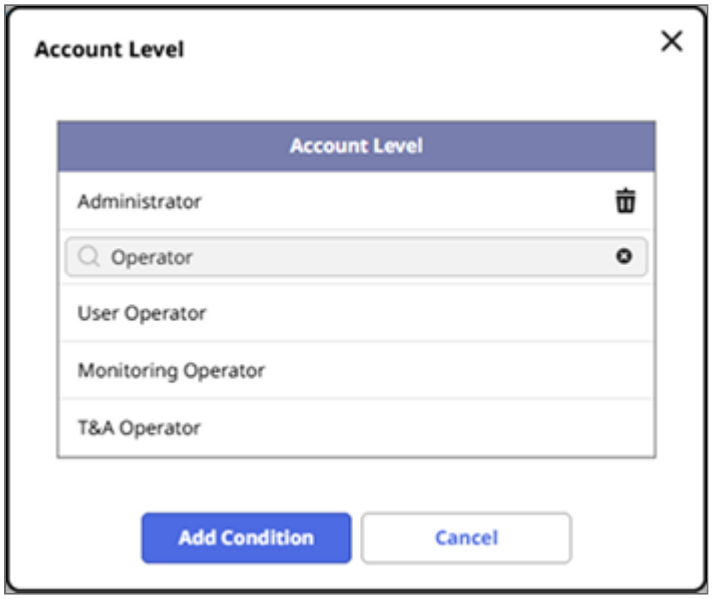
Buscar registros con filtros

Combine los filtros en la sección **Filter** para acotar y encontrar los registros que necesita. Seleccione varios valores en un filtro para combinarlos con `OR`. Aplique varios filtros a la vez para combinarlos con `AND`.

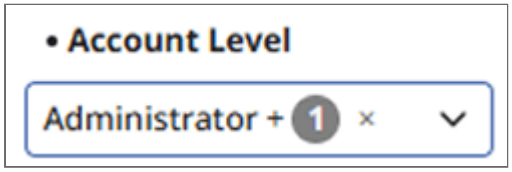


Filtrar	Cómo funciona
Datetime	Establezca las fechas y horas de inicio y fin. No se aplica un límite de duración al período de búsqueda.
User	Escriba un término de búsqueda y presione `Enter` para encontrar usuarios coincidentes. La lista está vacía cuando la abre por primera vez.
Account Level	Escriba un término de búsqueda y presione `Enter` para encontrar niveles de administrador coincidentes.
Category	Seleccione una o más categorías de la lista de casillas de verificación con búsqueda.
Target	Escriba un término de búsqueda y presione `Enter` para encontrar objetivos coincidentes.
Action	Seleccione una o más acciones de la lista de casillas de verificación.
Sub Action	Seleccione una acción detallada de la lista con búsqueda.
IP	Escriba un término de búsqueda y luego presione `Enter` para encontrar direcciones IP coincidentes.

- Si no aplica filtros, aparecen de forma predeterminada los registros de los últimos 30 días.
- Seleccione un valor en cada ventana emergente de filtro y luego haga clic en **Add Condition** para aplicarlo a la búsqueda de inmediato. Haga clic en **Cancel** para cancelar la selección y cerrar la ventana emergente.



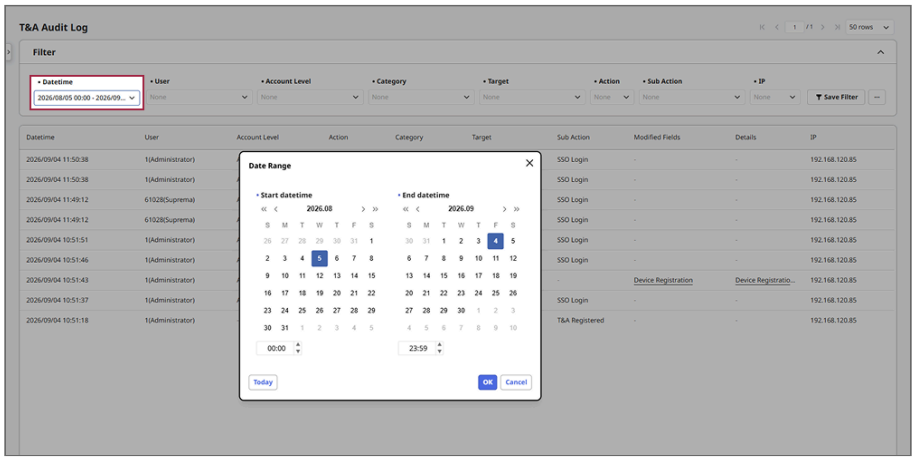
- Los filtros aplicados aparecen como el primer filtro y la cantidad de filtros adicionales. Haga clic en ✕ para borrar solo ese filtro. Los filtros sin un valor seleccionado aparecen como **None**.



> **Información**
>
> Escriba un término de búsqueda para ver resultados de los filtros **User**, **Account Level**, **Target** y **IP**. La búsqueda admite coincidencias parciales; escriba parte de un nombre o ID. La búsqueda incluye destinos eliminados y los marca como **Deleted**.

Configurar período de consulta

Haga clic en **Datetime** para abrir la ventana **Date Range**.

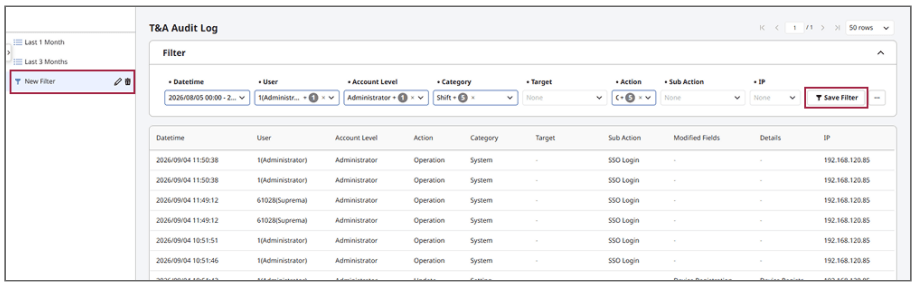


1. Configure la fecha y la hora de **Start datetime** y **End datetime**. Haga clic en **Today** para ir a hoy.
2. Haga clic en **OK** para aplicar el período de consulta.

Guardar filtro

Guarde las condiciones de búsqueda de uso frecuente en **Saved Filters** y cárguelas cuando sea necesario.

1. Configure los filtros para que coincidan con las condiciones requeridas.
2. Haga clic en **Save Filter** en la sección **Filter**.
3. El sistema agrega **New Filter** a la lista de filtros de la izquierda.



- Haga clic en ✎, escriba un nombre nuevo y presione `Enter` para cambiar el nombre del filtro.
- Haga clic en 🗑 para eliminar el filtro.

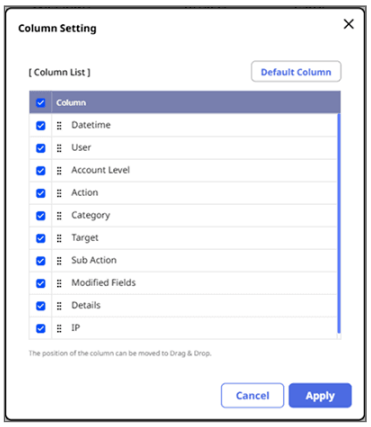
> **Información**
>
> El sistema permite guardar hasta 20 filtros. El navegador almacena los filtros guardados, por lo que no aparecen en otras PC ni en otros navegadores.

Registros adicionales por eliminación en cascada

Editar o eliminar un horario de trabajo también puede eliminar horarios temporales y ausencias de usuarios que lo usan. El sistema registra cada horario temporal y ausencia eliminados por separado del cambio o la eliminación del horario de trabajo.

- Si la eliminación en cascada no elimina nada, el sistema no crea registros adicionales.
- **Target** incluye 1 horario de trabajo que causó la eliminación y solo los usuarios cuyas entradas se eliminaron realmente. No incluye a todos los usuarios del horario.
- **Details** muestra la cantidad de eliminaciones. Al eliminar un horario de trabajo, también muestra el período afectado.

Configurar columnas



Cambie la posición de las columnas u oculte columnas en la tabla del registro de auditoría. En el lado derecho de la sección **Filter**, haga clic en [•••] → **Column Setting**.

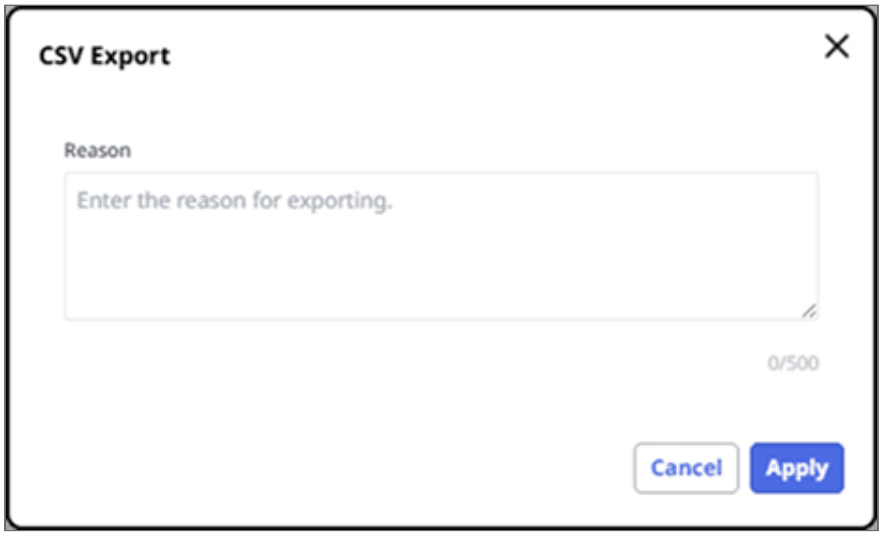
- En **[Column List]**, desmarque la casilla de la columna para ocultarla.
- Arrastre una columna para cambiar el orden de las columnas.
- Haga clic en **Default Column** para inicializar la configuración de columnas.

Haga clic en **Apply** para guardar la configuración.

Exportar a CSV

Exporte los registros de auditoría a un archivo CSV para utilizarlo con herramientas de análisis externas.

1. En la sección **Filter**, configure filtros si es necesario.
2. Haga clic en [•••] → **CSV Export** en el lado derecho de la sección.
3. Cuando aparezca la ventana **CSV Export**, ingresa **Export Reason** (opcional) y haz clic en **Apply**.



El archivo CSV exportado incluye las 10 columnas, una línea por registro. Agrega comillas solo a las celdas que contienen comas. Use una barra vertical (|) para separar varios valores en celdas como **Target** y **Modified Fields** (ejemplo: **Horario: 7(Horario del equipo)| Usuario: 12(Robert)**). En los registros donde **Action** es **Update**, **Details** incluye todos los campos sin puntos suspensivos.

> **Precaución**
>
> El archivo CSV incluye los valores tal cual, incluidos los que una hoja de cálculo puede interpretar como fórmulas. No abra el archivo CSV descargado directamente en una hoja de cálculo. Si es necesario, ábralo con la característica de importación de texto.

Consejo

Si configura filtros, la exportación incluye solo los resultados filtrados en el archivo CSV.

Configurar Auditoría de Tiempo y Asistencia

Los registros de auditoría aumentan con el tiempo. Gestiona el período de retención para ahorrar almacenamiento y proteger la privacidad. En **Audit Settings**, define el período de retención de **T&A Audit Log** y si conserva el historial de vistas.

Información de privilegios

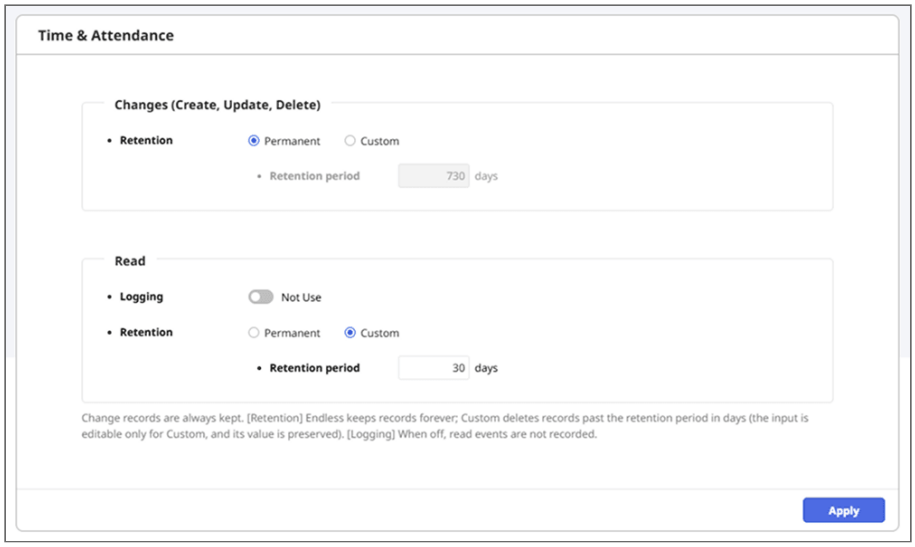
Administrator siempre puede ver y cambiar los ajustes en el menú **Audit Settings**. Para un administrador con privilegios personalizados, en **Admin Menu Settings**, establezca **Audit Settings** en **Read Only** para solo lectura, o en **Full Access** para ver y cambiar.

Información

- La cuenta de administrador predeterminada de Tiempo y Asistencia no tiene este permiso. El sistema crea esta cuenta cuando instalas el complemento de Tiempo y Asistencia. Concede el permiso por separado si es necesario.
- Para obtener más información sobre cómo agregar permisos de auditoría de Tiempo y Asistencia, consulta Ver Registros de Auditoría de Tiempo y Asistencia.

Abrir ajustes de auditoría

1. Haz clic en **Settings** en la página **Launcher**.
2. En la barra lateral izquierda, haz clic en **Audit Trail** → **Audit Settings**.
3. Desplázate hacia abajo hasta la sección **Time & Attendance**.



Ajustes de la política de retención

La sección **Time & Attendance** consta de los siguientes dos grupos.

- **Changes (Create, Update, Delete)**: Registros de creación, actualización y eliminación. El sistema siempre los registra. No puede activar ni desactivar el registro.
- **Read**: Ver registros. Defina si el sistema crea registros.

> **Información**
>
> - Ingrese **Retention period** como un número entero entre 1 y 2,147,483,647 días.
> - Seleccione **T&A Audit Log** para ver los registros de **Update** de cambios de ajustes en la sección **Time & Attendance**.

Registros de cambios

Como el sistema siempre registra el grupo **Changes (Create, Update, Delete)**, seleccione el ajuste **Retention**.

- **Permanent**: Conserve los registros de forma permanente sin eliminación automática.
- **Custom**: Seleccione esta opción para limitar el período de retención por cumplimiento o política interna. Cuando se active el campo **Retention period**, ingrese el período de retención en días.

Ver registros

En el grupo **Read**, defina si el sistema conserva los registros de visualización.

- **Logging**: Establezca esta opción en **Use** para conservar los registros de visualización. Si no se necesita, establézcalo en **Not Use**.
- **Retention**: Seleccione un método de retención.
  - **Permanent**: Conserve los registros de visualización de forma permanente sin eliminación automática.
  - **Custom**: Activa el campo **Retention period**. Ingrese el período de retención en días.

> **Información**
>
> Cuando **Logging** está en **Not Use**, el sistema no registra eventos de visualización. Después de cambiarlo a **Use**, el sistema no muestra los registros anteriores.

Guardar configuración

Después de completar los ajustes de **Changes (Create, Update, Delete)** y **Read**, haz clic en el botón **Apply** en la parte inferior de la sección **Time & Attendance**. Guarda ambos ajustes de grupo juntos.

Cómo funciona la eliminación automática

El servidor ejecuta esta tarea todos los días a la 1 a. m. La tarea elimina los registros que superan el período de retención establecido en **Custom**, sin importar las acciones del usuario. La tarea evalúa y elimina los registros al mismo tiempo. La tarea se ejecuta solo una vez al día.

> *Por ejemplo, establece los registros de **Read** en 30 días en **Custom**. A la 1 a. m., la tarea elimina los registros con más de 30 días de antigüedad. Los registros que acaban de superar el período de retención permanecen hasta que se ejecute la siguiente tarea de la 1 a. m.*

Cuando **Retention** se establece en **Permanent**, la tarea de eliminación automática no se ejecuta y los registros se

conservan permanentemente.

Administrar Visitantes

Utilice la función **Visitor** para crear una página de solicitud de visitantes en la PC de solicitudes y gestione el acceso de visitantes en la PC de administración.

Información

- La licencia **Esencial** o superior incluye la característica **Visitor** como opción adicional. Para obtener más información sobre las políticas de licencia, consulte Política de Licencias.
- Después de activar la función de visitantes mediante la licencia, consulte Configurar Visitante para obtener instrucciones detalladas sobre la configuración.

Aplicar la licencia de visitantes

Esta guía explica cómo aplicar la licencia de visitantes. Después de comprar la licencia Visitor al distribuidor de **BioStar X**, siga las instrucciones a continuación para aplicar la licencia.

1. Inicie sesión con la cuenta de administrador de **BioStar X**.
2. Haz clic en **Settings** en la página **Launcher**.
3. Haga clic en **License** → **BioStar X License** en la barra lateral izquierda.
4. Ingrese **License Activation** en secuencia con **Activated by** y **License Key**.



5. Haga clic en **Activate**.

Verifique las licencias registradas en **Activated License**.

Información

Para activar su licencia en un entorno de red cerrado o cuando el acceso a Internet esté restringido o no esté disponible, consulte Licencia Biostar X.

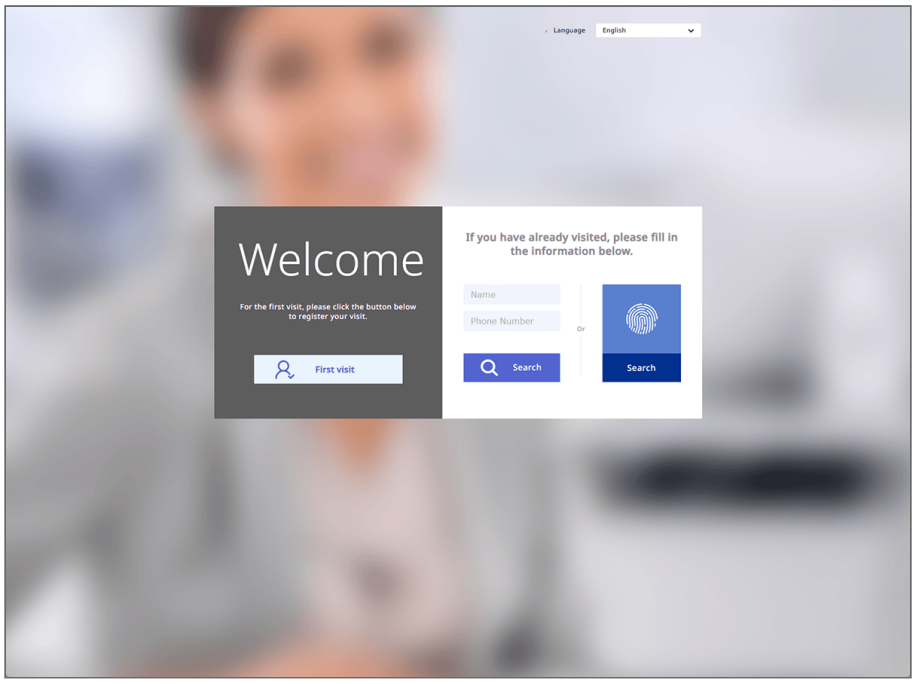
Consejo

Aplicar la licencia de visitantes activa el menú **Settings** → **Visitor**, y agrega un enlace a la página de gestión de **Visitor** en la lista de accesos directos en la esquina superior izquierda de la pantalla.

Configuración de la página de solicitud de visitantes

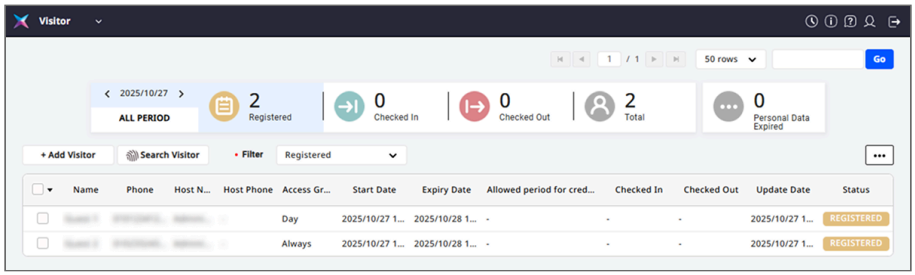
La página de solicitud de visitantes puede usarse después de priorizar la configuración de visitantes. Para obtener más información sobre cómo configurar la página de solicitud de visitantes, consulte Configurar Visitante.

Se puede acceder a la página de solicitud de visitantes desde una PC dedicada a solicitudes, lo que permite a los visitantes enviar solicitudes de acceso. Para obtener más información sobre el registro de visitantes, consulte Solicitar Visita.



Gestión de acceso de visitantes

Verifique el historial de solicitudes de visitantes y gestione el acceso de visitantes. Para obtener más información sobre cómo gestionar el acceso de visitantes, consulte Administrar Visitantes.



Solicitar Visita

Esta guía explica cómo los visitantes externos que no son usuarios internos solicitan la entrada mediante la PC de solicitud de visitas.

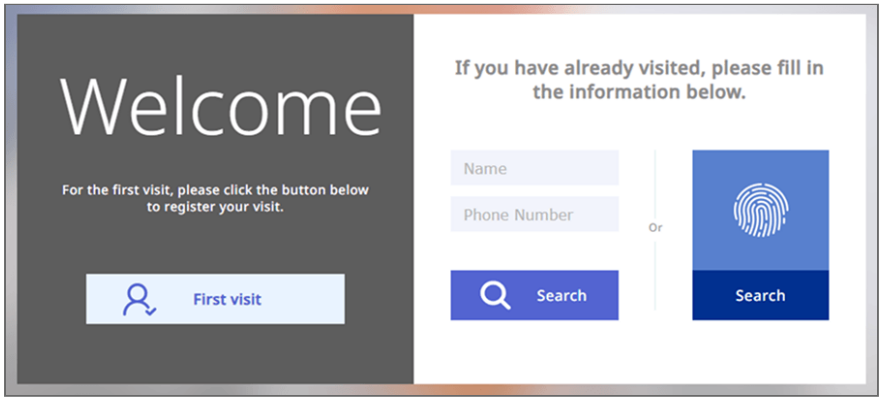
Información

- La PC de solicitud de visitas debe configurarse por separado y la configuración de visitantes debe realizarse previamente. Para obtener más información sobre la configuración de visitantes, consulte Configurar Visitante.
- Si la página de la aplicación de visitantes no tiene un icono de acceso directo en la PC, consulte Configurar Visitante para crear uno.

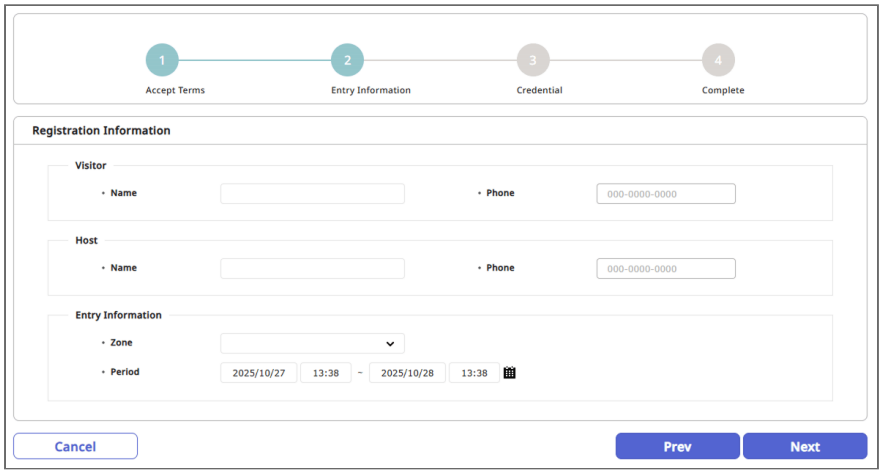
Nueva solicitud de visita

Esta guía explica cómo los visitantes que vienen por primera vez solicitan la entrada mediante la PC de solicitud de visitas.

1. Abra la página de solicitud de visitas en la PC de solicitud de visitas. La dirección URL de la página de solicitud de visitas tiene el formato `https://{biostar_x_server_ip}/#/register-welcome`.



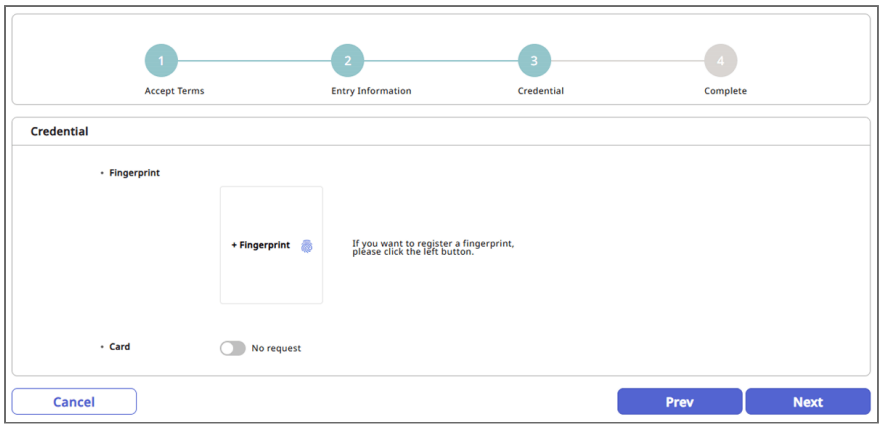
2. Haga clic en **First visit** en el centro de la pantalla.
3. Después de aceptar los términos y la política de privacidad relacionados con el acceso al departamento visitado, haga clic en el botón **Next** en la esquina inferior derecha de la pantalla.
4. Ingrese la información requerida para la solicitud de visita.



- **Visitor**: Ingrese el nombre y el número de teléfono del visitante.
- **Host**: Ingrese el nombre y el número de teléfono de la persona responsable en el destino de la visita.
- **Entry Information**: Configure el área de acceso y la duración de la visita.

5. Después de ingresar la información, haga clic en el botón **Next** en la esquina inferior derecha de la pantalla.

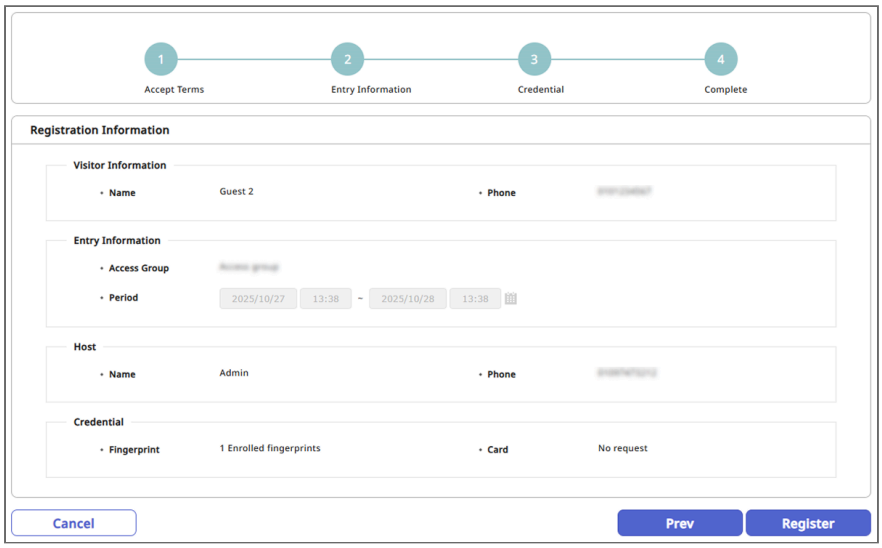
6. Configure el medio de entrada.



- **Fingerprint**: Para usar autenticación por huella digital, haga clic en el botón **+ Fingerprint** y luego registre su huella.
- **Card**: Para usar autenticación mediante tarjeta, configúrela con **Request** y reciba una tarjeta del administrador.

7. Después de completar la configuración, haga clic en el botón **Next** en la esquina inferior derecha de la pantalla.

8. Después de confirmar toda la información proporcionada, haga clic en el botón **Register** en la esquina inferior derecha de la pantalla.



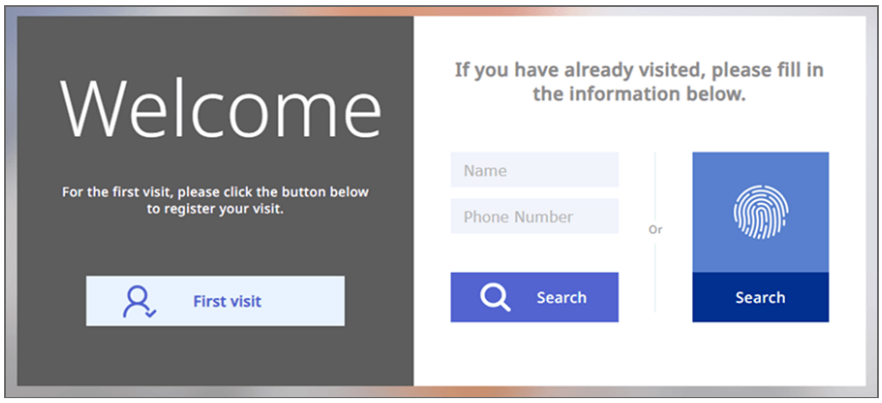
Información

- Para obtener más información sobre cómo crear los términos de uso y la política de privacidad para el acceso de visitantes, consulte Configurar Visitante.
- El nombre puede tener hasta 48 caracteres.
- Para obtener más información sobre cómo agregar campos personalizados a la información del visitante, consulte Configurar Visitante.
- Solo se pueden seleccionar los grupos de acceso asignados al departamento visitado para la PC de visitas. Para obtener más información, consulte Configurar Visitante.
- Para obtener más información sobre los grupos de acceso, consulte Administrar Grupos de Acceso.
- Para volver al paso anterior y modificar la información de la visita, haga clic en el botón **Prev**.
- Para escanear huellas digitales, se debe conectar un dispositivo de registro de huellas digitales a la PC de solicitud de visitas.

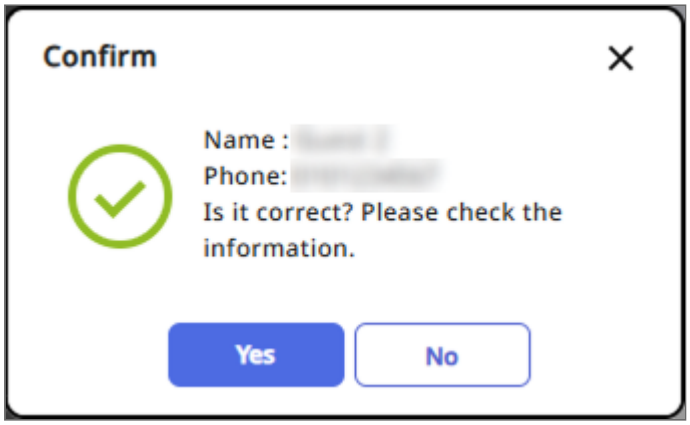
Solicitar usando información existente

Si una huella digital está registrada en el lugar de la visita, puede buscar la huella y solicitar una visita usando la información de visita existente.

1. Abra la página de solicitud de visitas en la PC de solicitud de visitas. La dirección URL de la página de solicitud de visitas tiene el formato `https://{biostar_x_server_ip}/#/register-welcome`.



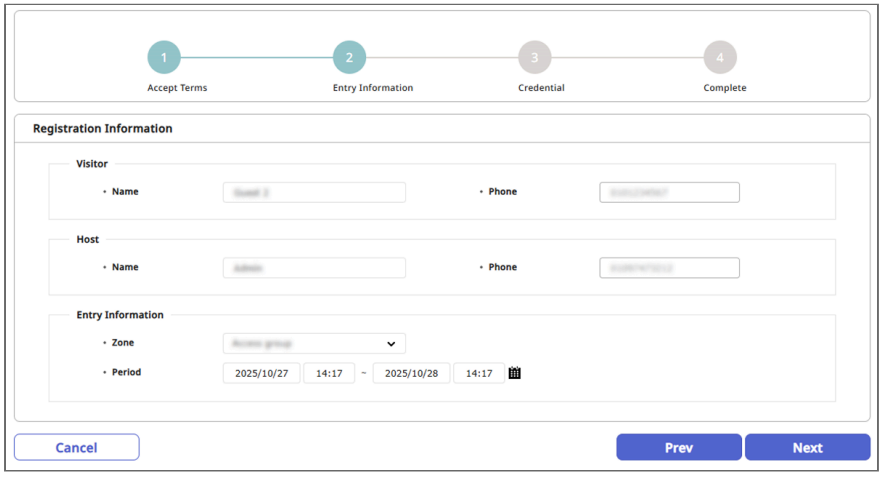
2. Haga clic en **Search** debajo del ícono de huella digital en el centro de la pantalla.
3. Escanee su huella digital en el dispositivo de escaneo de huellas digitales. Use la huella digital escaneada para buscar usuarios registrados.
4. Si la huella digital coincide con un visitante registrado previamente, aparecerá un mensaje de confirmación.



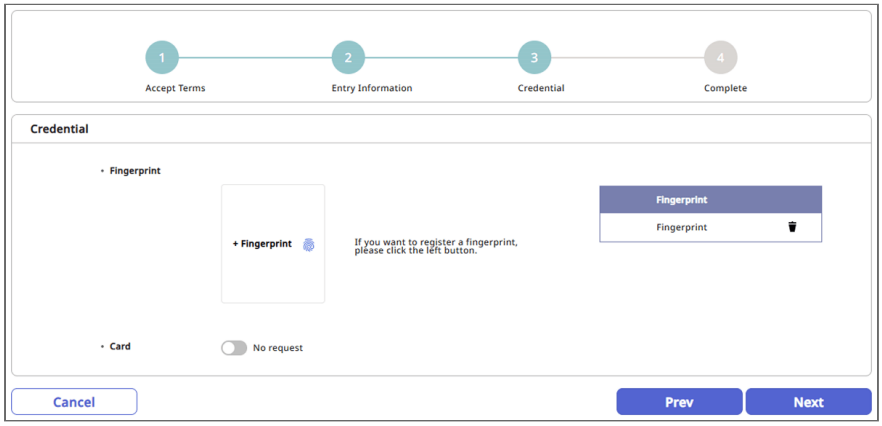
5. Si el visitante encontrado es correcto, haga clic en el botón **Yes**.

6. Después de aceptar los términos y la política de privacidad relacionados con el acceso al departamento visitado, haga clic en el botón **Next** en la esquina inferior derecha de la pantalla.

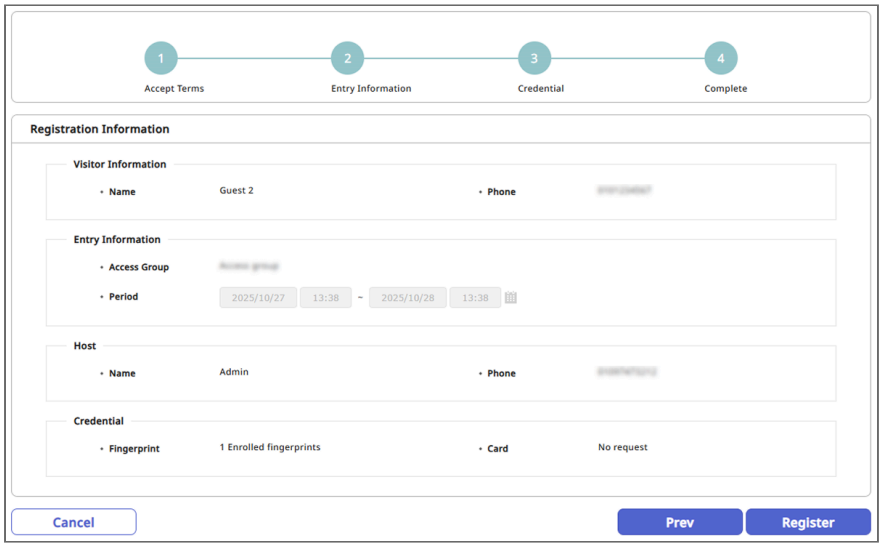
7. Confirme la información de la visita establecida durante la visita anterior. Para modificar la información existente, edite cada elemento y luego haga clic en el botón **Next** en la esquina inferior derecha de la pantalla.



8. Confirme el medio de entrada establecido durante la visita anterior. Para cambiar el medio de entrada existente, edite el elemento que desea cambiar y luego haga clic en el botón **Next** en la esquina inferior derecha de la pantalla.



9. Después de confirmar toda la información proporcionada, haga clic en el botón **Register** en la esquina inferior derecha de la pantalla.



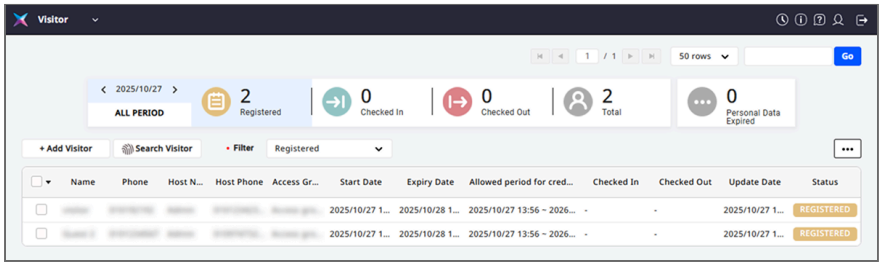
Administrar Visitantes

Apruebe o modifique solicitudes de visitantes. Los administradores también pueden agregar o eliminar visitantes directamente.

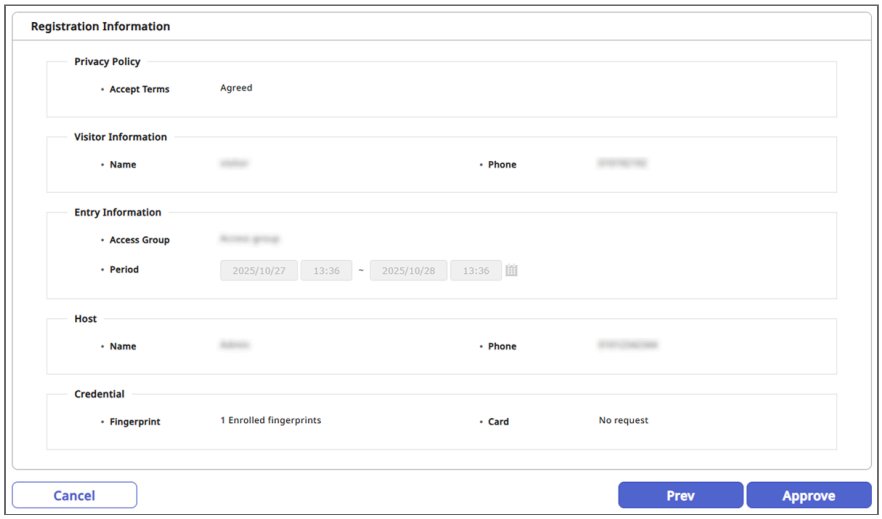
Aprobación de visitantes

Esta guía muestra cómo revisar las solicitudes de visitantes y aprobar su acceso.

1. Haz clic en **Visitor** en **Launcher**.
2. Haga clic en el visitante que desea aprobar en la lista de visitantes.



3. Después de revisar la información del visitante, corrija los elementos necesarios y haga clic en **Edit**.
4. Haga clic en **Check in** en la esquina inferior derecha de la pantalla.
5. Revise el contenido de **Registration Information** y, para aprobar la visita, haga clic en **Approve** en la parte inferior derecha de la pantalla.

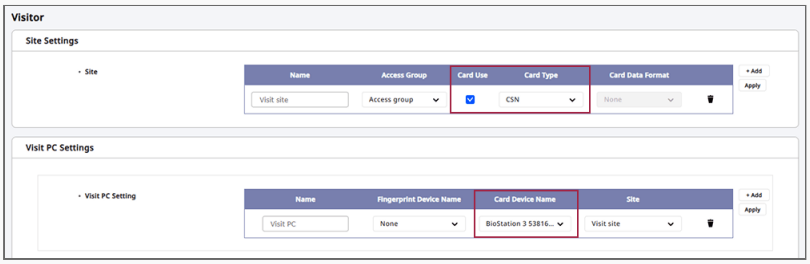


Información

- Si el solicitante no ha aceptado los términos de acceso para visitantes, **Approve** estará deshabilitado. Haga clic en **View terms** para mostrar los términos de acceso al visitante y obtener su consentimiento. Si el visitante no acepta los términos de acceso, la visita se restringirá.



- Si en la PC del visitante hay un dispositivo de registro de tarjetas configurado, **Approve and register card** se activará. Haga clic en **Approve and register card** para aprobar al visitante y emitir una tarjeta de acceso. Para obtener más información, consulte Aprobar y enrolar tarjeta.
- Configure el uso de tarjetas en la PC del visitante desde **Settings** → **Visitor** y asegúrese de aplicar los siguientes ajustes mínimos. Para obtener más información, consulte Configurar Visitante.

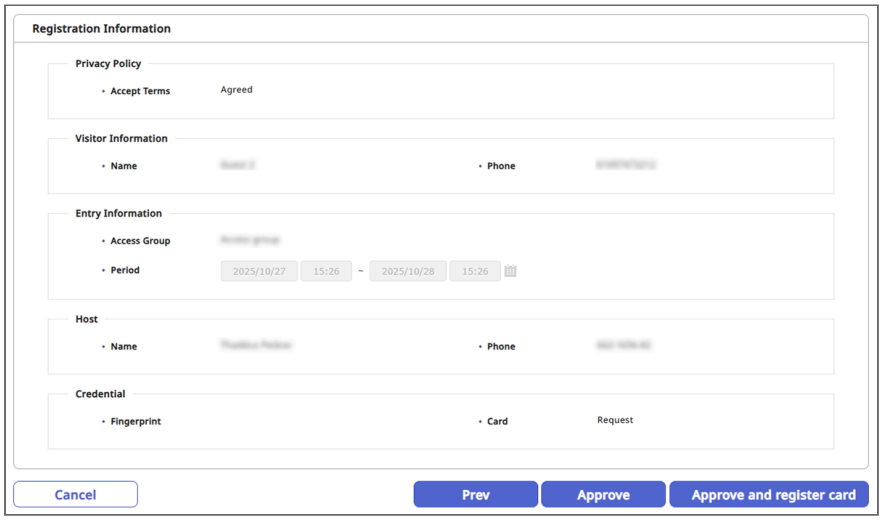


  - **Site Settings** → **Card Use** / **Card Type**
  - **Visit PC Visit PC Setting** → **Card Device Name**

Aprobar y enrolar tarjeta

Esta guía muestra cómo aprobar solicitudes de visitantes y emitir tarjetas de acceso.

1. En la pantalla **Registration Information**, haga clic en **Approve and register card** en la parte inferior derecha de la pantalla.



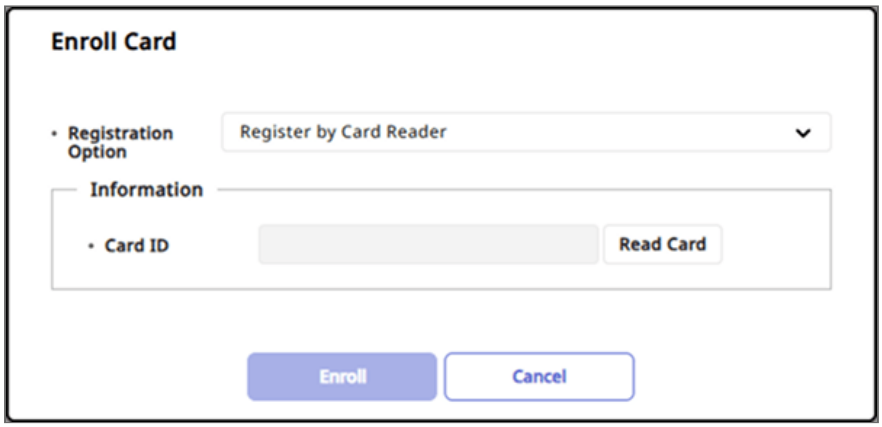
2. Cuando aparezca la ventana de registro de tarjetas, seleccione el método de registro deseado.

   - **Register by Card Reader**
   - **Enter Manually**

Register by Card Reader

Escanee la información de la tarjeta con un dispositivo conectado a la PC del visitante.

1. Seleccione **Register by Card Reader** en **Registration Option**.

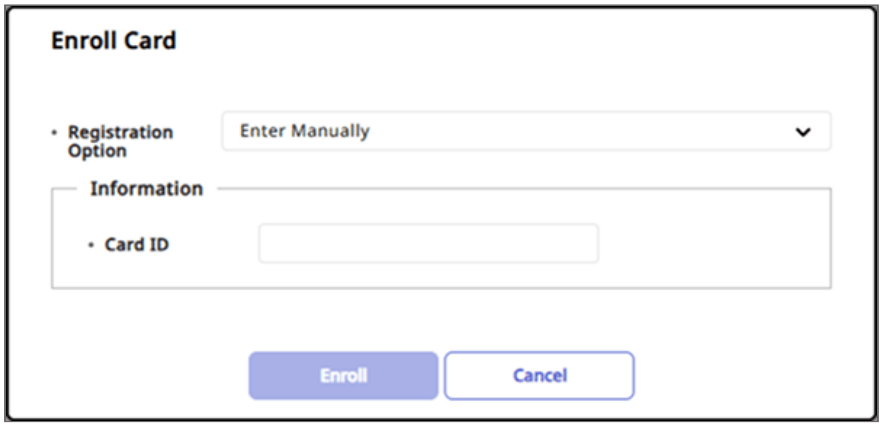


2. Para escanear la tarjeta a enrolar, haga clic en **Read Card**.
3. Para enrolar la tarjeta, haga clic en **Enroll**.

Enter Manually

Enrole ingresando directamente el número de tarjeta.

1. Seleccione **Enter Manually** en **Registration Option**.

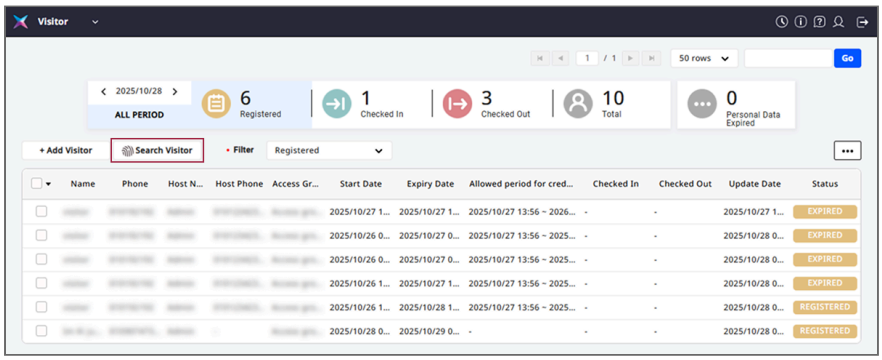


2. Ingrese directamente **Card ID**.
3. Para enrolar la tarjeta, haga clic en **Enroll**.

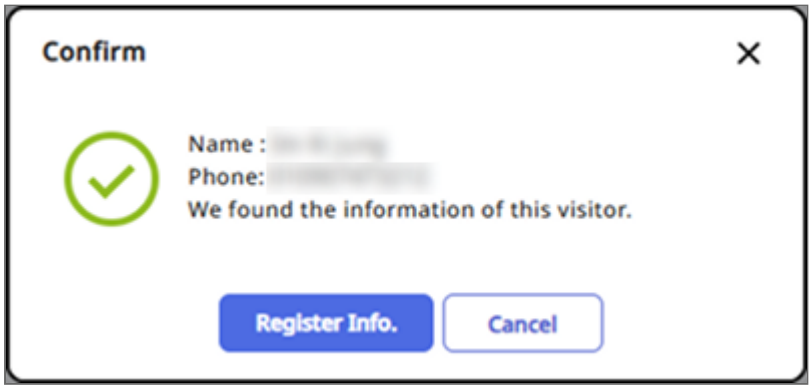
Búsqueda de huella digital para aprobación de visitantes

Busque visitantes con huellas digitales enroladas y procese su aprobación.

1. Haz clic en **Visitor** en **Launcher**.
2. Haga clic en **Search Visitor** en la parte superior izquierda de la lista de solicitudes de visitantes.



3. Escanee la huella digital del visitante en el dispositivo de escaneo de huellas.
4. Si se encuentra un visitante que coincida con la huella, aparecerá un mensaje de confirmación. Haga clic en **Register Info.**.



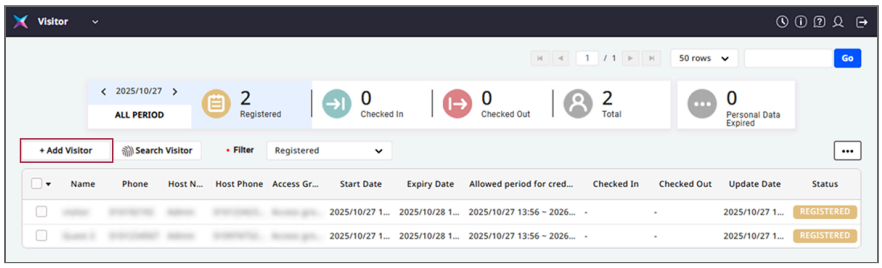
5. Después de revisar la información del visitante, corrija los elementos necesarios y haga clic en **Edit**.
6. Haga clic en **Check in** en la esquina inferior derecha de la pantalla.
7. Revise el contenido de **Registration Information** y, para aprobar la visita, haga clic en **Approve** en la parte inferior

derecha de la pantalla.

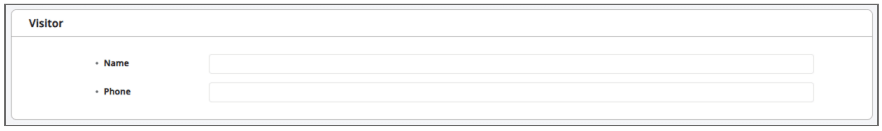
Agregar visitante

Esta guía muestra cómo un administrador puede agregar visitantes directamente.

1. Haz clic en **Visitor** en **Launcher**.
2. Haga clic en + **Add Visitor** en la parte superior izquierda de la lista de visitantes.



3. Ingrese el nombre y número de teléfono del visitante en la sección **Visitor**.

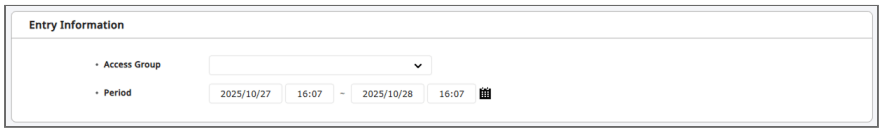


4. Ingrese el nombre y número de teléfono de la persona responsable de la visita en la sección **Host**.



> Al ingresar un nombre o número de teléfono, se mostrará una lista de usuarios que coinciden con la información ingresada. Para seleccionar el usuario deseado, haga clic en **Choose**.

5. Configure el grupo de acceso y la duración de la visita en la sección **Entry Information**.



> Solo se pueden seleccionar los grupos de acceso asignados al departamento visitado para la PC de visitas. Para obtener más información, consulte Configurar Visitante.

6. Configure el medio de acceso en la sección **Credential**.



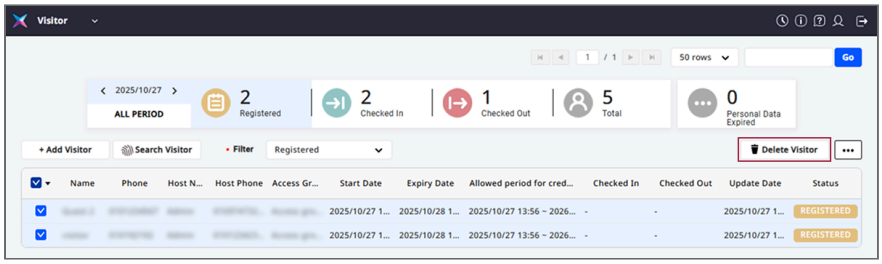
- **Card**: Para usar autenticación con tarjeta, configúrelo en **Request**.
- **Fingerprint**: Para usar autenticación con huella digital, haga clic en **+ Fingerprint** y luego enrole la huella del visitante.

7. Para finalizar la adición del visitante, haga clic en **Register** en la parte inferior derecha de la pantalla.

> **Información**
>
> - El nombre puede tener hasta 48 caracteres.
> - Para obtener más información sobre cómo agregar campos personalizados a la información del visitante, consulte Configurar Visitante.

Eliminar visitante

1. Haz clic en **Visitor** en **Launcher**.
2. Marque la casilla del visitante que desea eliminar de la lista de solicitudes de visitantes.



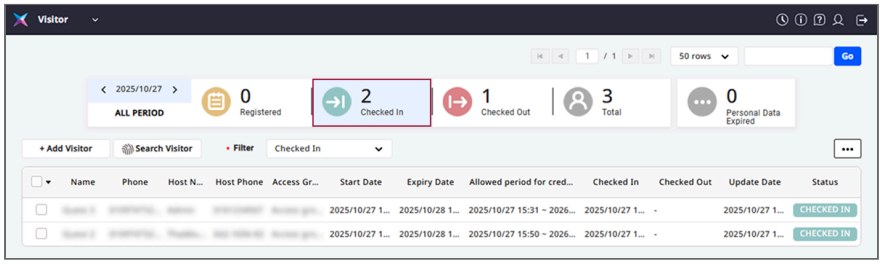
3. Haga clic en **Delete Visitor** en la esquina superior derecha de la pantalla.
4. Cuando aparezca el mensaje de confirmación, haz clic en **Yes**.

> **Información**
>
> - **Delete Visitor** se activará cuando se marque la casilla de un visitante.
> - Los visitantes solo se pueden eliminar desde la lista de solicitudes de visitantes.

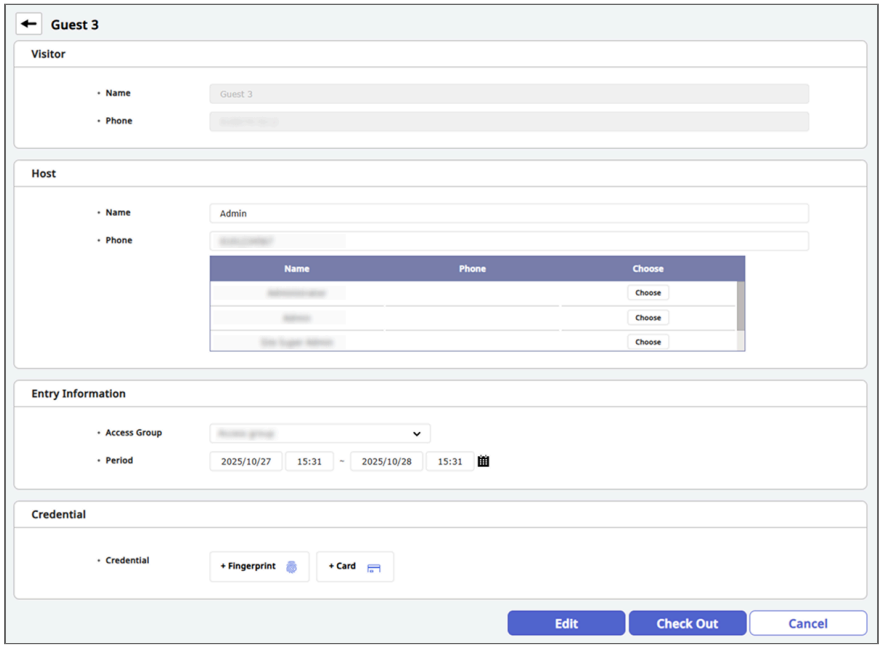
Administrar Visitantes en Check-in

Revisa los visitantes en estado de check-in y modifica la información de la visita o procesa el check-out.

1. Haz clic en **Visitor** en **Launcher**.
2. Haz clic en **Check in** en la parte superior de la pantalla.



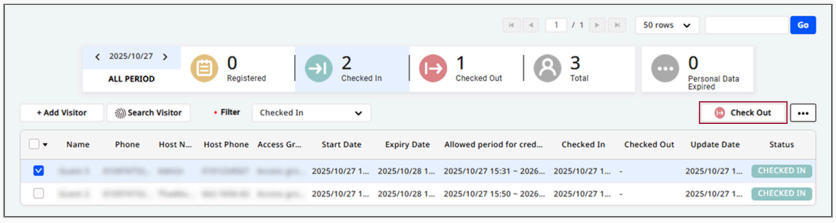
3. Haz clic en el visitante de la lista para modificarlo o realizar el check-out.
4. Verifica la información de solicitud de visita del visitante.



- Haz clic en **Edit** en la esquina inferior derecha de la pantalla para modificar y guardar elementos individuales.
- Haz clic en **Check Out** en la esquina inferior derecha de la pantalla para procesar el check-out.

Información

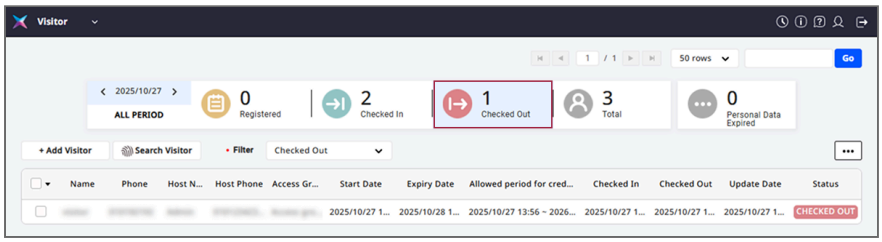
Selecciona también visitantes para hacer check-out desde la lista **Check in**. Selecciona la casilla del visitante para hacer check-out en la lista y luego haz clic en **Check Out** en la esquina superior derecha de la pantalla.



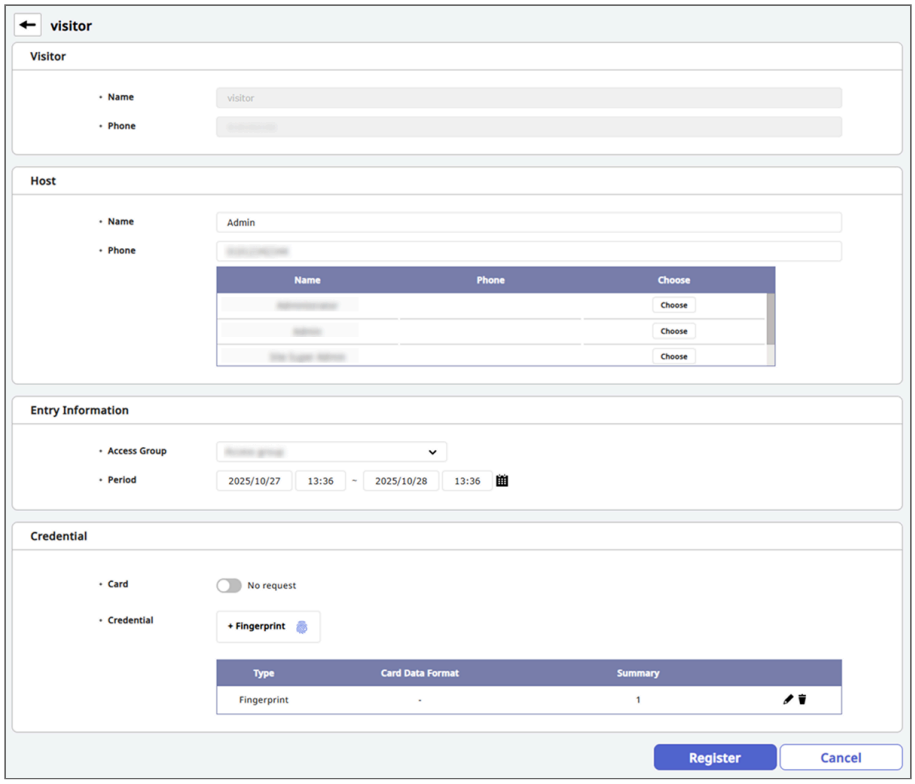
Gestionar las Salidas de Visitantes

Revisa a los visitantes en estado de salida y usa su información de solicitud de visita para registrar una visita recurrente.

1. Haz clic en **Visitor** en **Launcher**.
2. Haz clic en la pestaña **Check out** en la parte superior de la pantalla.



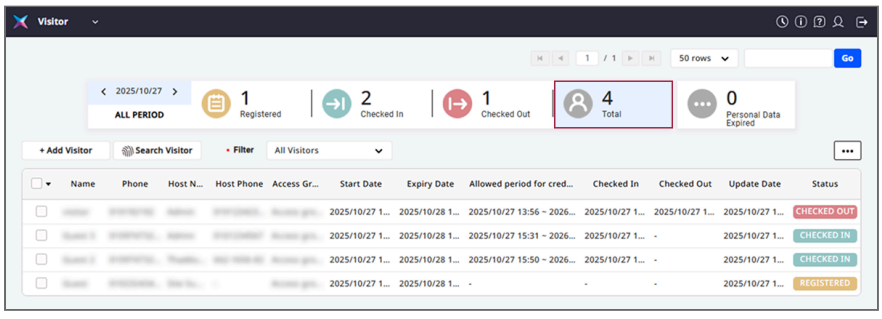
3. Haz clic en el visitante que desees volver a registrar en la lista de visitantes.
4. Haga clic en **Edit** en la esquina inferior derecha de la pantalla.
5. Si hay elementos que necesitan corrección, modifica los elementos individuales y luego haz clic en el botón **Enroll**.



El visitante vuelto a registrar se añadirá a la lista de solicitudes de visita. Haz clic en la pestaña **Register** en la parte superior de la pantalla para comprobar.

Gestionar Todos los Visitantes

1. Haz clic en **Visitor** en **Launcher**.
2. Haz clic en la pestaña **Total** en la parte superior de la pantalla.



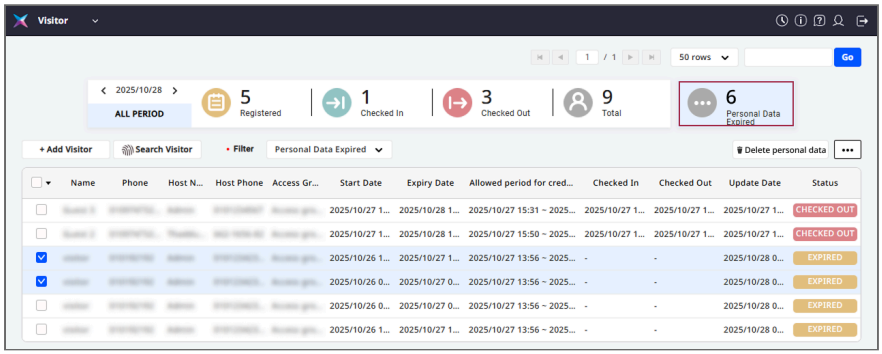
Información

- Aprueba las solicitudes de visitantes o agrega visitantes desde la lista general de visitantes. Para obtener más información sobre el registro de visitantes, consulte Solicitar Visita.
- Gestiona a los visitantes con estado de entrada o salida desde la lista general de visitantes. Para obtener más información, consulta lo siguiente.
  - Administrar Visitantes en Check-in
  - Gestionar las Salidas de Visitantes

Eliminar Datos Personales Vencidos

Elimina la información de visitantes cuyo periodo de retención de datos personales haya vencido.

1. Haz clic en **Visitor** en **Launcher**.
2. Haz clic en la pestaña **Personal Data Expired** en la parte superior de la pantalla.
3. Cuando se muestre la lista de visitantes cuyo periodo de retención de datos personales haya vencido, haz clic en la casilla de verificación del visitante que deseas eliminar. Selecciona más de uno.



4. Haz clic en el botón **Delete personal data** en la parte superior derecha de la lista de visitantes.
5. Cuando aparezca el mensaje de confirmación, haz clic en **Yes**.

Información

- Solo los usuarios con permisos de **Administrator** pueden ver la lista de visitantes con datos personales vencidos. Para obtener más información sobre los permisos de usuario, consulta Registrar usuarios.
- Para obtener más información sobre cómo configurar el período de retención de datos personales, consulta Configurar Visitante.

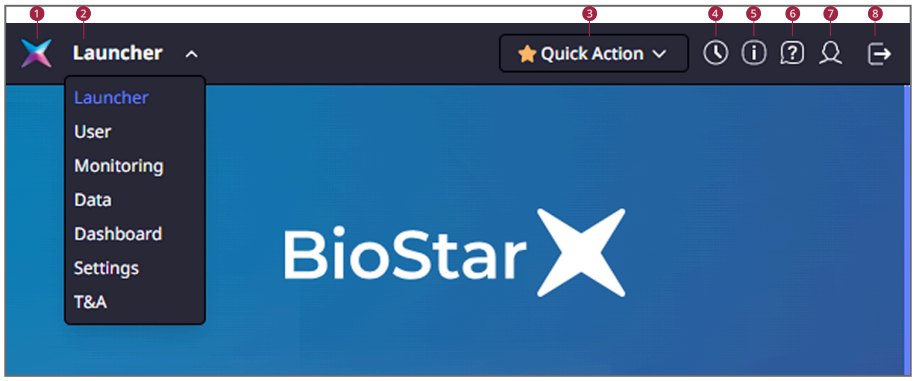
Explorar la Interfaz

Explore la interfaz de usuario de cada página de BioStar X y obtenga una guía sobre cómo usarla. BioStar X ofrece varias funciones, cada una fácilmente accesible a través de la interfaz de usuario (UI). Al examinar la interfaz de usuario de cada página, podrá comprender y utilizar las funciones de BioStar X con mayor facilidad. A continuación se muestra una visión general de las páginas principales de BioStar X y sus componentes de interfaz de usuario.

Aprender la Interfaz de Usuario Común

La interfaz de usuario (UI) de **BioStar X** está diseñada para permitir que los usuarios naveguen y utilicen el sistema con facilidad. Este documento presenta los componentes comunes de la UI de **BioStar X**. Comprenda la UI de **BioStar X** y utilice el sistema con mayor eficiencia.

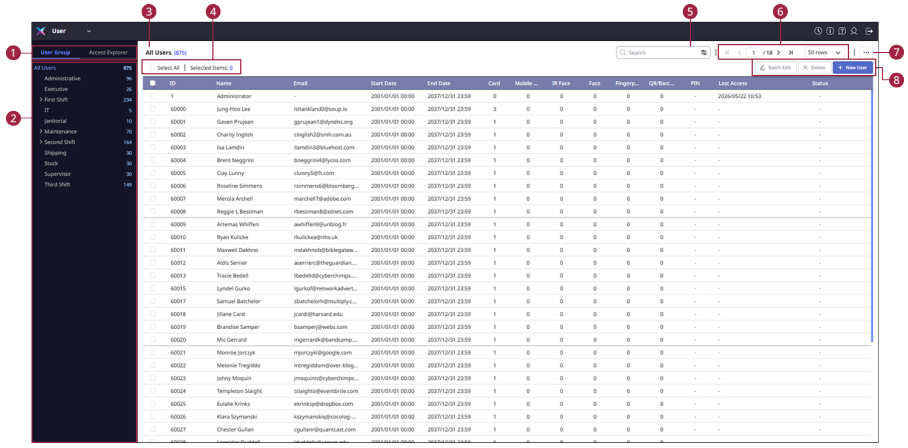
El área de encabezado de la pantalla se utiliza en todas las páginas y ofrece botones de enlace para acceder a varias funciones de **BioStar X**.



1. **Logo de BioStar X**: Botón de enlace que permite a los usuarios regresar a la página **Launcher** de **BioStar X**.
2. **Accesos directos**: Proporciona enlaces a las páginas principales que ofrece **BioStar X**.
3. **Quick Action**: Ejecuta la función **action** configurada por el usuario del servidor. Al hacer clic en el botón se muestra la lista de acciones. Para obtener más información, consulte Cómo Usar la Acción Rápida.
4. **Hora del servidor**: Compruebe la hora actual del servidor en ejecución de **BioStar X**. Al pasar el mouse sobre el botón se muestra la hora actual del servidor.
5. **Información**: Verifique la información de versión de **BioStar X** instalado.
6. **Ayuda**: Botón de enlace que dirige a la página de ayuda de **BioStar X**.
7. **Cuenta**: Ve a **Preferences** o cambia la contraseña del usuario que inició sesión actualmente.
   - Para obtener más información sobre el menú **Preferences**, consulte Configurar Preferencias.
   - Para obtener más información sobre cómo cambiar la contraseña del usuario que ha iniciado sesión, consulte Configurar Permisos de Usuario.
8. **Cerrar sesión**: Finaliza la sesión del usuario conectado y cierra la sesión.

Usuario

El menú **User** de la página **User** permite una gestión eficiente de usuarios mediante varias funciones, como la administración de grupos de usuarios, la administración de usuarios y la consulta de usuarios por derechos de acceso, lo que mejora la seguridad mediante permisos. Los componentes de la IU de la página **User** son los siguientes:



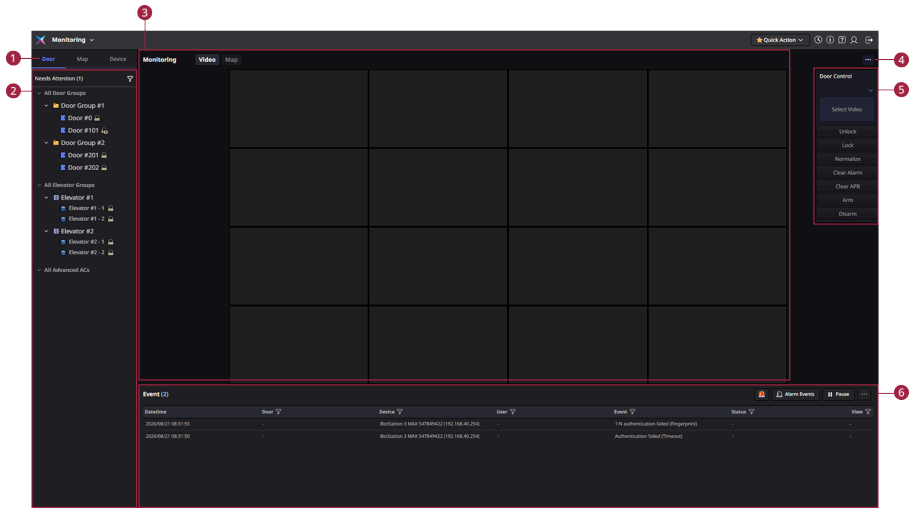
1. Compruebe los grupos de usuarios o los grupos de acceso.
   - Para obtener más información sobre **User Group**, consulta Administrar Grupos de Usuarios.
   - Para obtener más información sobre **Access Explorer**, consulta Administrar Grupos de Acceso.
2. Vea los grupos de usuarios o grupos de acceso en formato de estructura de árbol. Expanda o contraiga la estructura de árbol y haga clic en cada grupo para verificar los usuarios que pertenecen a ese grupo.
3. Verifique la cantidad de usuarios en el grupo de usuarios seleccionado desde el menú lateral.
4. Haga clic en **Select All** para seleccionar todos los usuarios mostrados en la lista de usuarios. La cantidad de usuarios seleccionados aparece en **Selected Items**.
5. Ingrese palabras clave para buscar usuarios. Para obtener más información sobre cómo buscar usuarios, consulte Explorar Usuarios.
6. Haga clic en el botón de navegación de página ubicado en la parte superior derecha de la pantalla para ver las listas de usuarios siguiente o anterior. Especifique también la página a la que desea moverse. Para obtener más información sobre cómo seleccionar las opciones de visualización, consulte Explorar Usuarios.
7. Haga clic en ⋯ para acceder a varias funciones relacionadas con los usuarios.
   - **Export**: Guarde la lista de usuarios en formato de archivo CSV o de datos. Para obtener más información sobre cómo exportar o importar la información de los usuarios, consulte Exportar/Importar Información de Usuarios.
   - **Import**: Importe listas de usuarios en formato de archivo CSV o de datos, o importe información de autenticación facial. Para obtener más información sobre cómo exportar o importar la información de los usuarios, consulte Exportar/Importar Información de Usuarios.
   - **Transfer to Device**: Función para enviar la información de usuarios registrados al dispositivo. Para obtener más información sobre cómo transferir la información de los usuarios a un dispositivo, consulte Transferir Información de Usuario al Dispositivo.
   - **Face Migration**: Mejore el rendimiento de autenticación actualizando los rostros inscritos en versiones anteriores de **BioStar X** con el algoritmo más reciente. Para obtener más información, consulte Migracion Visual Face.

- **Column Layout**: Cambie los elementos de encabezado de las columnas en la lista de usuarios. Para obtener más información sobre la configuración de las columnas de la lista de usuarios, consulte Explorar Usuarios.
- **Print**: Imprima la lista de usuarios.

8. Utilice las funciones para el registro de usuarios y la modificación o eliminación por lotes.
   - **Batch Edit**: Modifique información o derechos de acceso para varios usuarios a la vez. Para obtener más información sobre la edición masiva de la información de los usuarios, consulte Editar Información del Usuario.
   - **Delete**: Elimine los usuarios seleccionados. Para obtener más información sobre la eliminación de usuarios, consulte Borrar Usuario.
   - **New User**: Registre nuevos usuarios. Para obtener más información, consulte Registrar usuarios.

Monitorizar

Esta guía describe la interfaz de usuario (UI) de la página **Monitoring**. Puede monitorear el estado de seguridad en tiempo real según puertas, mapas y dispositivos en la página **Monitoring**. También puede revisar eventos en tiempo real y tomar las acciones necesarias. Los componentes de la UI de la página **Monitoring** son los siguientes.



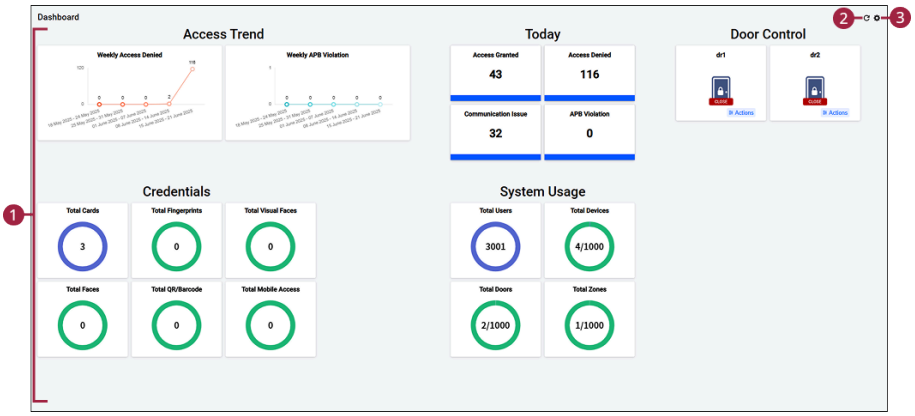
1. Ingrese palabras clave en el campo de búsqueda para obtener dispositivos, puertas, cámaras y otros elementos deseados.
2. Supervise la estructura en árbol de los grupos revisando **Door**, **Map** y **Device**.
   - Para obtener más información sobre cómo monitorear **Door**, consulte Monitorear Puertas.
   - Para obtener más información sobre cómo monitorear **Map**, consulte Monitorear Mapa.
   - Para obtener más información sobre cómo monitorear **Device**, consulte Monitorear Dispositivo.
3. El **mosaico de video** le permite revisar video en tiempo real o mapas de puertas, cámaras y áreas. Puede supervisar múltiples transmisiones de cámaras simultáneamente.
   - Para obtener más información sobre cómo monitorear las transmisiones de las cámaras, consulte Supervisar Video.
   - Para obtener más información sobre cómo monitorear mapas, consulte Monitorear Mapa.
4. Haga clic en ••• y seleccione **Close All** para cerrar todos los elementos del mosaico de video.

5 El **panel de control** le permite controlar las funciones de la puerta o dispositivo seleccionados. Para obtener más información, consulte Control de Puerta.

6 La **lista de eventos** le permite revisar eventos en tiempo real en orden cronológico. Puede ver información detallada, estado, usuarios relacionados e información del dispositivo para cada evento y tomar medidas inmediatas si es necesario. Para obtener más información, consulte Supervisar Evento.

Tablero

Esta guía describe la interfaz de usuario (UI) de la página **Dashboard**.



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

1 **Área de widgets**: Zona donde se muestran los widgets añadidos por el usuario.

- El tamaño de cada widget se puede ajustar libremente dentro de los límites de tamaño de cada widget.
- Los widgets solo se pueden colocar en áreas vacías y no pueden superponerse entre sí.

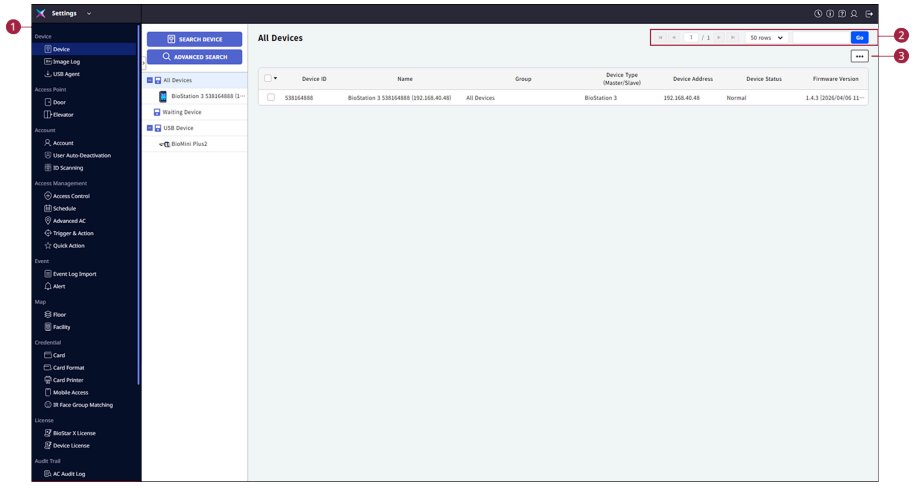
2 **Actualizar**: Actualiza la página del panel para actualizar los datos del widget modificado.

Establece el ciclo de actualización en **Auto Refresh Interval** en **Dashboard Settings**.

3 **Dashboard Settings**: Agrega nuevos widgets o configura los datos y la apariencia de los widgets añadidos.

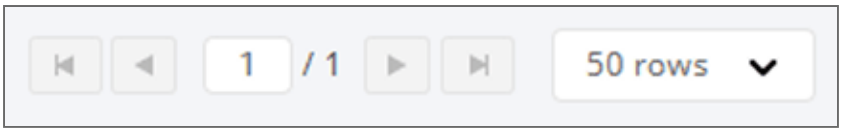
Ajustes

En la página **Settings**, administra varios ajustes de **BioStar X**. Los componentes de la interfaz de usuario de esta página son los siguientes:



1. Revisa los distintos menús de ajustes que se ofrecen en el menú **Settings**. Para obtener más información, consulte Ajustes.

2. Una herramienta para navegar por la lista de páginas. Desplázate entre páginas o ve a la página deseada.



- ⏮: Ir a la primera página.
- ◀: Ir a la página anterior.
- ▶: Ir a la página siguiente.
- ⏭: Ir a la última página.
- Ingresa el número de página en el campo de entrada para ir a la página deseada.
- Haz clic en el cuadro de selección de filas para establecer la cantidad de elementos que se muestran en cada página.

> **Información**
> La compatibilidad puede variar según el menú de ajustes.

3. Haz clic en [•••] para acceder a opciones adicionales.

> **Información**
> Las funciones compatibles pueden variar según el menú de ajustes.

Política de Licencias

BioStar X es el software de control de acceso de próxima generación desarrollado como sucesor de **BioStar 2**. Admite diversos entornos de implementación actuales y futuros gracias a una arquitectura de sistema mejorada, funciones ampliadas y un modelo de licenciamiento más flexible.

BioStar X ofrece un total de cinco niveles de licencia escalables que van desde **Starter** hasta **Élite**, lo que permite elegir según distintos entornos, desde pequeñas empresas hasta grandes corporaciones. Diseñado con una estructura modular, puede añadir diversas funciones opcionales como integración de video, acceso móvil y soporte para múltiples servidores.

Usa el **BioStar X License Calculator** para resolver requisitos de licenciamiento complejos. La herramienta ayuda a determinar el tipo y la cantidad de licencias requeridas.

licencia básica

La licencia básica es un componente esencial para activar y operar el sistema. Esta licencia sirve como base para aplicar funciones adicionales o actualizaciones.

	Device Manager	Inicial	Esencial	Avanzado	Corporativa	Élite
Número máximo de puertas	0	5	32	128	500	2000
Número máximo de usuarios	200	100	1,000	50,000	100,000	500,000
Número máximo de operadores	1	1	10	20	40	100
Número máximo de dispositivos IP conectados	1,000	1,000	1,000	1,000	1,000	1,000
Mapas	✕	✕	✔	✔	✔	✔
Video	✕	✕	Complemento	Complemento	Complemento	Complemento

	Device Manager	Inicial	Esencial	Avanzado	Corporativa	Élite
Control de acceso avanzado *(Anti-passback, alarma de incendio, alarma de intrusión, reunión, límite de ocupación, elevador, esclusa)*	✕	✕	Complemento	Complemento	✔	✔
Ampliación de capacidad *(Puertas/ Usuarios/ Operadores)*	Usuarios y Operadores únicamente	✕	Complemento	Complemento	Complemento	Complemento

- La licencia **Device Manager** es necesaria para los clientes que utilizan software o sistemas de terceros y desean administrar de manera eficiente los dispositivos Suprema a través de **BioStar X**.
- **Operadores máximos** se refiere a la cantidad de usuarios a quienes se les conceden permisos de acceso al sistema.
- Si el número máximo de dispositivos IP conectados supera 1,000, se recomienda utilizar el servidor **Multi Communications**.

Ampliación de capacidad

Las actualizaciones de licencia están disponibles para los titulares de licencias **Esencial**, **Avanzado**, **Corporativa** y **Élite**. Los titulares de licencia de **Device Manager** solo pueden comprar actualizaciones de Usuarios y Operadores.

	Cantidad
Puertas	32
Usuarios	5,000
Operadores	10

Complementos de funciones

Las siguientes opciones están disponibles para compra individual y se pueden agregar a los niveles de licencia **Esencial**, **Avanzado**, **Corporativa** y **Élite**.

Función	Tipo de Licencia	Observaciones
Multi Communications Server Init	Licencia básica	Incluye 1 servidor de comunicaciones Multi. Admite hasta 1,000 dispositivos IP.
Multi Communications Server Add-on	Servidor adicional	Necesario para añadir 1 servidor de comunicaciones Multi adicional. Amplía la capacidad de dispositivos IP en 1,000 por cada complemento.
Mapa GIS	Sistema	Puede usar el mapa GIS para configurar áreas, instalaciones y pisos.
Video	Cámara	Requerido para integrar VMS de terceros. Admite hasta 1,000 cámaras integradas por sistema.
Autenticación en servidor	ID, tarjeta, huella digital, rostro IR	El método de autenticación en servidor compara el ID, la tarjeta, la huella digital y el rostro IR almacenados en el dispositivo con las credenciales almacenadas en la base de datos del servidor.
Visitante	Sistema	Los administradores y operadores pueden rastrear o controlar el acceso de visitantes.
Integración de directorio	Sistema	Admite la integración con servicios de directorio para la gestión centralizada de usuarios.
Llamada de lista	Sistema	-

> No todas las cámaras conectadas al VMS necesitan integrarse con BioStar X. Por ejemplo, incluso si el VMS admite 32 cámaras, los usuarios solo deben comprar una licencia para la cámara específica que desean integrar con **BioStar X** y no es necesario adquirir una licencia para todas las cámaras.

Los siguientes ítems se pueden comprar individualmente y se pueden añadir independientemente de la licencia básica.

Función	Tipo de Licencia	Observaciones
Aplicación móvil	Sistema	-

Función	Tipo de Licencia	Observaciones
API de registro de eventos	Sistema	El sistema puede recibir y registrar eventos mediante una API externa. Esto permite que aplicaciones o servicios de terceros inserten datos de eventos directamente en el sistema de control de acceso para registro y generación de informes centralizados.
Acceso Remoto	Sistema (facturado anualmente)	Proporciona una función de túnel seguro que permite acceder al servidor **BioStar X** desde una red externa. **BioStar X** también actúa como una puerta de enlace para el acceso de red externa a móvil y API. Necesario para usar la función **Send Face Mobile Enroll Link**.
Conector de BioStar X	Sistema	Admite la integración de conector externos. Se pueden usar hasta 10 conectores personalizados por sistema. Para obtener más información, consulta Conector.
Gestión de asistencia (T&A)	Estándar	Admite hasta 500 usuarios.
	Corporativa	No hay límite en la cantidad de usuarios.

Información

Los usuarios de **time & attendance** (T&A) siguen el límite básico de licencias y tienen permitido hasta el número máximo de usuarios permitido por la edición de **time & attendance**. (p. ej., 500 usuarios para la edición Standard)

Control de acceso avanzado

El **control de acceso avanzado** consta de las siguientes 7 funcionalidades individuales. Seleccione y compre solo las que necesita. Los niveles de licencia **Esencial** y **Avanzado** las ofrecen como complementos, mientras que **Corporativa** y **Élite** incluyen las 7 funcionalidades de forma predeterminada.

Función	Tipo de Licencia	Observaciones
APB (Anti-passback)	Sistema	-
Alarma de incendio	Sistema	-
Alarma de intrusión	Sistema	-
Reunión	Sistema	-
Límite de ocupación	Sistema	-
Elevador	Sistema	-

Función	Tipo de Licencia	Observaciones
Esclusa	Sistema	-

- Bloqueo programado (Scheduled Lock) y desbloqueo programado (Scheduled Unlock) son funcionalidades básicas sin licencia y siempre están disponibles aparte de las 7 anteriores.
- Los clientes que compraron previamente el paquete de control de acceso avanzado pueden seguir usándolo. Las compras nuevas permiten seleccionar y comprar las 7 funcionalidades de forma individual.

Licencia de dispositivo

Las licencias de dispositivos se pueden comprar individualmente y se pueden agregar independientemente de la licencia básica. Las licencias de dispositivos se emiten según el número de serie (S/N). Esta función solo se puede activar en dispositivos que requieran licencia.

Función	Tipo de Licencia	Modelos compatibles	Observaciones
Camera QR	Dispositivo	BioStation 3 Max, XPass Q2, BioStation 3, X-Station 2	-
Multi Face Authentication	Dispositivo	BioStation 3	-
Cerradura inalámbrica	Dispositivo	CoreStation 40	-

Apéndices

Incluye avisos legales contenidos en el producto.

Descargos de responsabilidad

- La información de este sitio web se proporciona en relación con los productos de Suprema.
- El derecho de uso se reconoce únicamente para los productos de Suprema incluidos en los términos y condiciones de uso o venta de dichos productos garantizados por Suprema. Este sitio web no otorga ninguna licencia, expresa o implícita, por impedimento legal ni de ningún otro tipo, sobre ninguna propiedad intelectual.
- Salvo lo expresamente establecido en un acuerdo entre usted y Suprema, Suprema no asume ninguna responsabilidad y rechaza toda garantía, expresa o implícita, incluidas, entre otras, las relativas a la idoneidad para un fin particular, la comerciabilidad o la no infracción.
- Todas las garantías quedan ANULADAS si los productos de Suprema han sido: 1) instalados incorrectamente o si los números de serie, la fecha de garantía o las etiquetas de control de calidad del hardware han sido alterados o retirados; 2) utilizados de una manera distinta a la autorizada por Suprema; 3) modificados, alterados o reparados por un tercero que no sea Suprema o un tercero autorizado por Suprema; o 4) operados o mantenidos en condiciones ambientales inadecuadas.
- Los productos de Suprema no están destinados a usos médicos, de salvamento, de soporte vital ni a otras aplicaciones en las que la falla del producto de Suprema pudiera ocasionar lesiones personales o la muerte. Si compra o utiliza productos de Suprema para cualquiera de estas aplicaciones no previstas ni autorizadas, deberá indemnizar y eximir de responsabilidad a Suprema y a sus directores, empleados, subsidiarias, afiliadas y distribuidores por todos los reclamos, costos, daños y gastos, incluidos los honorarios razonables de abogados, derivados directa o indirectamente de cualquier reclamo por lesiones personales o muerte asociado con dicho uso no previsto o no autorizado, incluso si el reclamo alega que Suprema fue negligente en el diseño o la fabricación de la pieza.
- Suprema se reserva el derecho de realizar cambios en las especificaciones y descripciones de los productos en cualquier momento y sin previo aviso para mejorar la confiabilidad, la función o el diseño.
- La información personal, en forma de mensajes de autenticación y otra información relacionada, puede almacenarse en los productos de Suprema durante su uso. Suprema no se hace responsable de ninguna información, incluida la información personal, almacenada dentro de los productos de Suprema que no esté bajo el control directo de Suprema o según lo establecido en los términos y condiciones correspondientes. Cuando se utilice cualquier información almacenada, incluida la información personal, es responsabilidad de los usuarios del producto cumplir con la legislación nacional (como el RGPD) y garantizar su manipulación y tratamiento adecuados.
- No debe confiar en la ausencia o las características de ninguna función o instrucción marcada como "reservada" o "indefinida". Suprema las reserva para su definición futura y no tendrá ninguna responsabilidad por conflictos o incompatibilidades derivados de cambios posteriores en ellas.
- Salvo que se disponga expresamente en el presente documento y en la medida máxima permitida por la ley, los productos de Suprema se venden "tal cual".
- Comuníquese con la oficina de ventas local de Suprema o con su distribuidor para obtener las especificaciones más recientes y antes de realizar su pedido.

Aviso de derechos de autor

Los derechos de autor de este sitio web pertenecen a Suprema. Los derechos sobre otros nombres de productos, marcas comerciales y marcas registradas pertenecen a las personas u organizaciones propietarias.

Licencia de código abierto

Este producto contiene software de código abierto. El código fuente sujeto a las licencias GPL, LGPL, MPL y otras licencias de código abierto que requieren la distribución del código fuente puede solicitarse al Equipo de Soporte Técnico global de Suprema.

El código fuente de este producto puede solicitarse al Equipo de Soporte Técnico global de Suprema durante 3 años a partir de la fecha de entrega final del producto.

Si desea obtener el código fuente en un medio físico, podría cobrarse el costo de dicha distribución. Esta oferta es válida para cualquier persona que reciba esta información.

Las licencias de código abierto y los términos de licencia correspondientes para el software de código abierto incluido en este producto son los siguientes: enlace

ffmpeg

BioStar X incluye ffmpeg (https://ffmpeg.org) para convertir y sondear archivos de video. Incluye dos binarios de línea de comandos de ffmpeg: *ffmpeg.exe* y *ffprobe.exe*. Ambos se compilan a partir del tarball único de código fuente upstream de ffmpeg que se indica abajo (ffprobe forma parte del proyecto ffmpeg, no es un componente aparte).

- Component: ffmpeg (ffmpeg.exe, ffprobe.exe)
- Version: 8.1
- License: GNU Lesser General Public License v2.1

  Texto completo: consulte COPYING.LGPLv2.1
- Source code: ffmpeg-8.1.tar.xz
- Upstream URL: ffmpeg-8.1.tar.xz
- SHA-256: b072aed6871998cce9b36e7774033105ca29e33632be5b6347f3206898e0756a

Build configuration:

```
./configure \
  --arch=x86_64 \
  --target-os=mingw64 \
  --disable-gpl \
  --disable-nonfree \
  --disable-libx264 \
  --disable-libx265 \
  --disable-libxvid \
  --enable-mediafoundation \
  --enable-libmp3lame \
  --disable-doc \
  --disable-debug \
  --enable-small \
  --pkg-config-flags=--static \
  --extra-ldflags="-static"
```

Modificaciones: ninguna. Binario compilado a partir del tarball de código fuente upstream sin modificaciones.

Codificadores que usa **BioStar X**:

- h264_mf (H.264 via Windows Media Foundation)
- libmp3lame (MP3 audio, LGPL)

libmp3lame

BioStar X usa libmp3lame para la codificación de audio MP3.

- Component: libmp3lame (LAME MP3 Encoder)
- Version: 3.100
- License: GNU Lesser General Public License v2.1

  Texto completo: consulte COPYING.LGPLv2.1 (la misma versión LGPL v2.1 que ffmpeg)
- Source code: lame-3.100.tar.gz
- Upstream URL: lame-3.100.tar.gz
- SHA-256: ddfe36cab873794038ae2c1210557ad34857a4b6bdc515785d1da9e175b1da1e

Modificaciones: ninguna. Tarball de código fuente upstream sin modificaciones, vinculado estáticamente a *ffmpeg.exe* y *ffprobe.exe* con `--enable-libmp3lame` durante la compilación.

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.