suprema
BioStar

BioStar 1.3
Guía del administrador

suprema

Tabla de contenidos

Tabla de contenidos

Tabla de contenidos

Tabla de contenidos

Tabla de contenidos

Tabla de contenidos

Tabla de contenidos

Garantía y descargo de responsabilidad

Política de garantía de Suprema

Suprema garantiza al Comprador, en base a las limitaciones establecidas a continuación, que todos los productos funcionarán en conformidad con las especificaciones publicadas para el producto durante un período de un (1) año, a partir de la fecha de envío del producto ("Período de garantía"). Si el Comprador notifica a Suprema, por escrito y durante el Período de garantía, de algún defecto cubierto por esta garantía, Suprema deberá, a su elección, reparar o reemplazar el producto defectuoso que se enviará a Suprema durante el Período de garantía, debiendo pagar por adelantado el Comprador los costos de envío y del seguro. Dicha reparación o reposición deberá ser recurso exclusivo de Suprema en caso de incumplirse con las condiciones de la garantía del Producto. Esta garantía limitada no incluirá ningún producto que haya sido: (i) expuesto a cualquier esfuerzo, uso indebido, negligencia, accidente o abuso físico o eléctrico inusual; o dañado por cualquier otra causa externa; (ii) incorrectamente reparado, alterado o modificado a menos que dicha modificación haya sido aprobada por escrito por el Proveedor; (iii) incorrectamente instalado o utilizado incumpliendo las instrucciones provistas por Suprema.

Suprema será notificada por escrito de los defectos en el reporte RMA (Autorización de devolución de material) proporcionado por Suprema. Dicho reporte deberá ser enviado en un plazo no mayor a treinta días, después de que hayan aparecido los defectos mencionados, y a un año, contando a partir de la fecha de envío del Producto. El reporte deberá incluir los datos completos de cada uno de los productos defectuosos: número de modelo, número de factura y número de serie. Los productos que no tengan un número RMA proporcionado por Suprema no serán aceptados y todos los defectos deben ser reproducibles para el servicio de garantía.

Salvo que haya sido expresamente mencionado en el presente documento, los productos se proporcionan sin ningún tipo de garantía, ya sea de forma expresa o implícita, incluyendo, en forma enunciativa y no limitativa, las garantías o la mercantibilidad e idoneidad para un fin en particular.

Descargo de responsabilidad

La información del presente documento está relacionada con los productos de Suprema. Este documento no otorga ninguna licencia, expresa o implícita, por incumplimientos legales o, dicho de otro modo, ningún derecho de propiedad intelectual, salvo aquellos mencionados en los Términos y Condiciones de Suprema acerca de la venta de dichos productos.

Suprema no asume ningún tipo de responsabilidad y deniega cualquier garantía, expresa o implícita, en relación con la venta y/o uso de los productos de Suprema, incluyendo la responsabilidad o garantías relacionadas con la idoneidad para un fin en particular, la mercantibilidad o la infracción de cualquier patente, derecho de autor, o cualquier otro derecho de la propiedad intelectual.

Los productos de Suprema no están diseñados para uso médico, para salvar vidas, para aplicaciones de soporte vital ni para otras aplicaciones en las que un fallo producido en el producto de Suprema pueda originar una situación en la que se puedan ocasionar daños o la muerte de personas. En caso de que el Comprador adquiera o utilice los productos de Suprema para cualquiera de las aplicaciones no intencionadas ni autorizadas que han sido mencionadas anteriormente, el Comprador tendrá que indemnizar y mantener indemne a Suprema, así como a sus directivos, empleados, subsidiarios, afiliados y distribuidores, frente a cualquier denuncia, costo, daño, gasto y honorarios de abogados razonables que puedan surgir, directa o indirectamente, de cualquier denuncia presentada por daños personales o muerte asociados con dicho uso no intencionado ni autorizado, incluso en el caso de que dicha denuncia alegue negligencia por parte de Suprema en relación con el diseño o fabricación de la pieza.

Suprema se reserva el derecho a realizar cambios en las especificaciones y en las descripciones del producto, en cualquier momento y sin previo aviso, para mejorar cuestiones de seguridad, función o diseño. Los diseñadores no deben confiar en la ausencia o en las características de ninguna de las funciones o instrucciones marcadas como "reservadas" o "no definidas". Suprema se las reserva para definirlas en un futuro y no se hará responsable de los conflictos o incompatibilidades que surjan por realizar cambios futuros en ellas.

Favor de ponerse en contacto con Suprema, con los representantes locales de ventas de Suprema o con los distribuidores locales para obtener las últimas especificaciones antes de realizar su pedido.

1. Acerca del sistema BioStar

Aviso de Copyright

01 Acerca del sistema BioStar

BioStar es el sistema de control de acceso de última generación de Suprema, basado en conectividad IP y en seguridad biométrica. La mayoría de los dispositivos del sistema integran escáneres de huellas y lectores de tarjetas para múltiples niveles de autentificación de usuario. Sin embargo, los dispositivos biométricos de Suprema, instalados en cada puerta, funcionan no sólo como escáneres de tarjetas y huellas dactilares o lectores de tarjetas, sino también como controladores de acceso inteligente.

La edición estándar con licencia de BioStar se desbloquea con una llave USB. Sin la llave, BioStar funciona como una versión gratuita con capacidad limitada. Con la llave, BioStar ofrece mayor versatilidad y funciones adicionales, tal y como se muestra en la siguiente tabla:

	Edición estándar	Versión gratuita
# máximo de puertas	512	20
# máximo de clientes	32	2
Soporte de zona	Sí	No
Notificaciones por e-mail	Sí	No
Identificación de servidor	Sí	No
Tipos de turnos	Diarios y semanales	Sólo semanales
Placa de entradas/salidas (I/O)	Sí	No
Mapa visual	Sí	No

1. Acerca del sistema BioStar

La versión 1.3 de BioStar es compatible con los siguientes dispositivos:

- **BioStation (V1.5 o superior)**: BioStation es una terminal multifuncional con un teclado numérico y una pantalla LCD en color de 2.5 pulgadas que permite registrar usuarios y gestionar funciones directamente desde el dispositivo.

  BioStation se puede conectar a Internet mediante una red WLAN o Ethernet e incluye una entrada USB e interfazs de dispositivos para facilitar la transferencia de datos. Los modelos BioStation MIFARE (BSM) también permiten controlar la entrada mediante tarjetas inteligentes.

- **D-Station**: D-Station es una terminal multifuncional, con control de acceso basado en IP. Posee una cámara, una pantalla táctil y un escáner dual para huellas dactilares que permite numerosas combinaciones de autorización utilizando el reconocimiento de huellas (modo sencillo o dual), tarjetas de acceso MIFARE, User IDs (Id. de usuario) y reconocimiento facial. D-Station puede recibir energía directamente de una conexión Ethernet para eliminar así la necesidad de cableado o conexiones eléctricas adicionales.

- **BioEntry Plus (V1.2 o superior)**: BioEntry Plus es un dispositivo de control de acceso basado en IP que incluye tanto reconocimiento de huellas dactilares como entrada mediante una tarjeta de acceso. El dispositivo se puede controlar de forma independiente mediante tarjetas de comando o también se puede gestionar mediante la interfaz de BioStar. BioEntry Plus se puede conectar a cerraduras eléctricas para puertas mediante un relay interno o también se puede utilizar con el dispositivo Secure I/O para mayor seguridad y para una capacidad expandida.

- **BioLite Net (V1.0 o superior)**: BioLite Net es una terminal de huellas dactilares basado en IP diseñado específicamente para uso en exteriores. Con una estructura impermeable altamente resistente, clasificada como IP65, ofrece extra durabilidad para poder soportar la fuerza de los elementos. Ya sea como un sencillo control para puertas, o como parte de un entorno conectado en red complejo, BioLite Net es totalmente compatible con la funcionalidad de tiempo y asistencia y con las funciones de control de acceso de BioStar.

1. Acerca del sistema BioStar

- **Xpass**: Xpass es un lector/controlador de acceso basado en IP diseñado exclusivamente para utilizarlo con tarjetas RF. Ofrece muchas funciones parecidas a las del dispositivo BioEntry Plus, pero es impermeable (para uso en exteriores) y se puede conectar y alimentar con un único cable CAT5/6.

- **BioMini**: el dispositivo BioMini es un escáner de huellas dactilares que se puede utilizar para el registro de usuarios. La instalación del dispositivo es simple: conéctelo a un puerto USB de cualquier computadora que se encuentre conectada al servidor BioStar e instale el controlador.

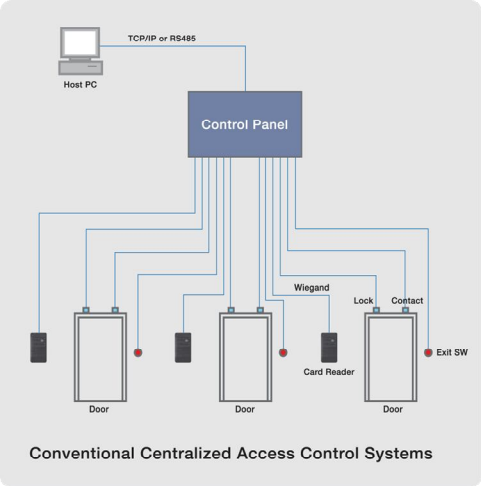
- **Secure I/O**: el dispositivo Secure I/O ofrece una forma conveniente de aumentar la seguridad de los dispositivos que hayan sido instalados en el exterior o de expandir las capacidades de su sistema. Cuando las puertas se controlan con un dispositivo Secure I/O, los intrusos no pueden abrir las puertas aunque logren desinstalar los dispositivos externos. Para aumentar aún más la seguridad, el dispositivo Secure I/O ofrece comunicaciones encriptadas entre los componentes de la puerta. El dispositivo Secure I/O posee cuatro interruptores de entrada y dos relays de salida para poder controlar varios componentes con tan sólo un dispositivo.

1.1 Configuración lógica

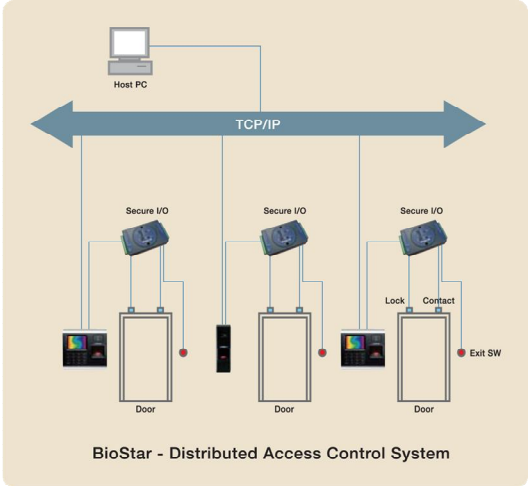
BioStar es un sistema de inteligencia distribuida. En lugar de los complejos controles cableados y centralizados que los sistemas de control de acceso convencionales necesitan, los dispositivos de control de acceso de Suprema se pueden conectar mediante TCP/IP o sin cables a una red de área local o también se pueden conectar mediante conexiones en serie. La información de usuario, las normas de acceso y cualquier otra información se pueden distribuir a cada uno de los dispositivos para acelerar el tiempo de autorización y ofrecer un funcionamiento continuo aún incluso cuando se haya perdido la conexión a la red.

Tal y como se muestra en la siguiente imagen, el sistema BioStar no necesita que los controladores de acceso se encuentren separados. Esta característica ofrece una ventaja distinta a otros sistemas de control de acceso, ya que los dispositivos BioStation o BioEntry Plus funcionan al mismo tiempo como controladores y como lectores. Como resultado, la propuesta de inteligencia distribuida de Suprema requiere de menos hardware y de menos cables que los sistemas de control de acceso centralizado convencionales.

1. Acerca del sistema BioStar



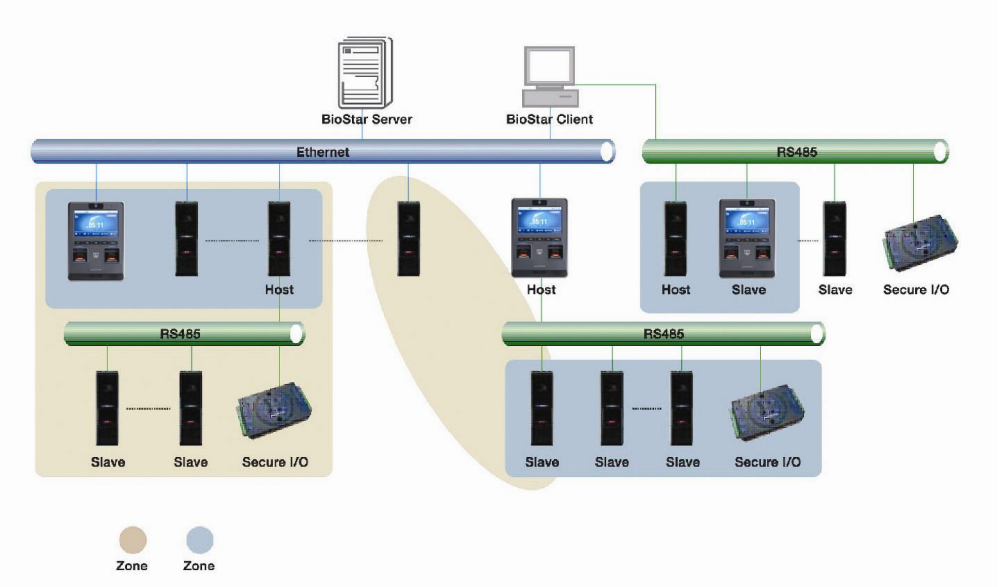
Conventional Centralized Access Control Systems



BioStar - Distributed Access Control System

BioStar es un programa servidor-cliente que permite hasta 32 clientes (máximo 2 clientes en la versión gratuita). Una configuración típica está formada por muchos dispositivos de control de acceso conectado a un servidor central mediante una conexión Ethernet, WLAN y/o RS485. BioStar es compatible con MS SQL Server y con bases de datos MySQL.

En general, el sistema permite un máximo de 512 puertas y 512 dispositivos (20 puertas y dispositivos en la versión gratuita). Los dispositivos conectados en red se pueden agrupar fácilmente para crear varias combinaciones de anti-passback o zonas de alarma, tal y como se muestra en la siguiente imagen.



1.2 Funciones de control de acceso

El sistema BioStar va un paso por delante de los sistemas de control de acceso convencionales, ya que combina la identificación biométrica única con la posibilidad de utilizar tarjetas de acceso configurables.

1.2.1 Autentificación de usuario

Los dispositivos de control de acceso de Suprema incorporan avanzados y premiados algoritmos de reconocimiento de huellas dactilares para ofrecer un control de acceso seguro. Cuando se utiliza el teclado numérico en las terminales BioStation y las funciones de reconocimiento facial en el dispositivo D-Station, el sistema permite una amplia variedad de modos de autentificación de usuario:

- **Huella dactilar o tarjeta de acceso**: se puede utilizar la lectura de una huella dactilar o una tarjeta de acceso para entrar.
- **Huella dactilar + tarjeta de acceso**: tanto la lectura de una huella dactilar como la tarjeta de acceso son necesarias para entrar.
- **Id. de usuario (User ID) + huella dactilar**: se utiliza una combinación de Id. de usuario y lectura de una huella dactilar; el id. de usuario identifica al usuario y la lectura de la huella se utiliza para la autorización.
- **Id. de usuario (User ID) + contraseña**: se utiliza una combinación de Id. de usuario y contraseña; el id. de usuario identifica al usuario y la contraseña se utiliza para la autorización.
- **Id. de usuario (User ID) + tarjeta + huella dactilar**: se utiliza una combinación de Id. de usuario, tarjeta de acceso y lectura de una huella dactilar.
- **Sólo huella dactilar**: el único método utilizado para entrar es la autentificación mediante la lectura de una huella dactilar.
- **Sólo tarjeta**: el único método utilizado para entrar es la autentificación mediante una tarjeta de entrada.
- **Huella dactilar + huella dactilar**: se utilizan dos huellas dactilares.
- **Huella dactilar + reconocimiento facial**: se utiliza una huella dactilar junto con la función de reconocimiento facial.
- **Huella dactilar + huella dactilar + reconocimiento facial**: se utilizan dos huellas dactilares junto con la función de reconocimiento facial.
- **Detectar rostro**: después de pasar con éxito el proceso de autentificación, se captura una imagen del rostro.

BioStar almacena dos plantillas para cada huella dactilar y hasta dos huellas dactilares por usuario (cuatro plantillas en total). Si lo desea, se puede utilizar una huella dactilar como señal de peligro. Así, es posible activar las alarmas o enviar alertas en situaciones en las que un usuario se vea obligado a acceder en contra de su propia voluntad. Si se duplican las plantillas para cada huella aumenta el rendimiento de la autentificación, ya que se reduce la posibilidad de falsos rechazos. Para obtener más información acerca de cómo registrar huellas dactilares, consulte la sección 3.5.2.

BioStar también proporciona a los administradores la posibilidad de leer tarjetas de proximidad EM4100 y HID, y de leer, expedir y formatear tarjetas de acceso MIFARE®. Para obtener más información acerca de las tarjetas de acceso, consulte la sección 3.5.4.

Los dispositivos D-Station permiten al sistema almacenar fotografías de usuarios y controlar el acceso mediante la función de reconocimiento facial, además de la autentificación mediante huella dactilar, tarjeta de acceso y Id. de usuario (User ID). Para obtener más información acerca del reconocimiento facial, consulte la sección 3.5.3.

1.2.2 Gestión de usuarios

BioStar permite gestionar usuarios de forma manual o automática. La sincronización manual está disponible para registrar diferentes subgrupos de usuarios en dispositivos particulares o cuando el número total de usuarios en la base de datos de BioStar supera los límites de un dispositivo BioStation, BioEntry Plus, BioLite Net, o D-Station. La sincronización automática está disponible cuando no es necesario, o no se desea, gestionar los registros de usuarios del dispositivo.

BioStar recopila los registros de los dispositivos y permite exportar los datos a un archivo de texto (.CSV) para reportes personalizados. El software permite un número ilimitado de registros de usuarios; la cantidad máxima de datos almacenados sólo depende de las capacidades de la base de datos subyacente y de la configuración del hardware. Para obtener más información acerca de la gestión de usuarios, consulte las secciones 4.1, 4.2, 4.3, 4.5, y 4.6.

1.2.3 Gestión del grupo de acceso

BioStar permite a los administradores crear grupos de acceso personalizados combinando permisos para zonas horarias y puertas. Con esta función, BioStar proporciona un control de acceso personalizable y programado.

BioStar permite hasta 128 zonas horarias que están formadas por un programa de siete días y dos programas vacacionales. Cada día de la zona horaria puede incluir hasta cinco períodos de tiempo diferentes.

En total, BioStar permite hasta 128 grupos de acceso que se pueden transferir a todos los dispositivos conectados. Para obtener más información acerca de los grupos de acceso, consulte la sección 3.7.

1.2.4 Gestión de dispositivos

Los administradores pueden controlar numerosos aspectos de los dispositivos a través del software BioStar. Además de los comportamientos de autentificación, BioStar permite configurar los relays, las acciones y los sonidos de entrada y salida. El sistema incluye opciones para personalizar la configuración de sonido y de pantalla de los dispositivos BioStation y D-Station, y la configuración del LED y del zumbido de otros dispositivos.

El sistema proporciona opciones de configuración para controlar dispositivos externos, tales como cerraduras de puertas y sirenas de alarma. BioStar también se puede conectar y comunicar con otros dispositivos utilizando una interfaz Wiegand. Para obtener más información acerca de la gestión de dispositivos, consulte las secciones 3.2 y 4.7.

1.2.5 Gestión de puertas

BioStar permite un control integral de puertas y dispositivos conectados, tales como los relays de puertas y alarmas, sensores de puertas e interruptores de salida. Todas las puertas se pueden controlar con hasta dos dispositivos y, cuando hay dos dispositivos conectados a una puerta, los administradores pueden aplicar controles anti-passback.

BioStar permite configurar de forma específica eventos de alarma para puertas que se hayan abierto de forma forzada o que hayan permanecido abiertas durante más tiempo del intervalo especificado, incluyendo la activación de sonidos de alarma para dispositivos individuales, el envío de señales a sirenas de alarma externas, la visualización de advertencias en la interfaz de usuario de BioStar y el envío de notificaciones por e-mail (no disponible en la versión gratuita). Además, los administradores o los operadores pueden bloquear y desbloquear las puertas o reiniciar las alarmas de forma remota. Para obtener más información acerca de la gestión de puertas, consulte las secciones 3.3, 4.3 y 4.4.

1.2.6 Gestión de zonas

El sistema BioStar proporciona a los administradores el control total de varias zonas (no disponible en la versión gratuita). Las zonas se pueden crear con los dispositivos conectados a través de una red Ethernet o RS485, pueden incluir un dispositivo maestro y hasta 65 dispositivos miembros. Además, los dispositivos individuales se pueden incluir hasta en cuatro zonas.

BioStar permite zonas para mayor control de acceso, tales como zonas anti-passback y de límite de entrada, así como también zonas que proporcionan control para entradas y acciones de alarma o de alarma de incendio. BioStar también permite a los administradores sincronizar la hora, los registros de eventos y los datos de usuarios de todos los dispositivos en una zona determinada. Para obtener más información acerca de la gestión de zonas, consulte la sección 3.4.

1.2.7 Tiempo y asistencia

La versión 1.2 de BioStar incluye funciones de tiempo y asistencia para permitir que los administradores definan categorías horarias, turnos, programas diarios y configuraciones vacacionales. Las capacidades de tiempo y asistencia de BioStar se pueden utilizar para reforzar el compromiso con los procedimientos de verificación de entradas y salidas, para restringir el acceso al personal que ha finalizado su jornada laboral y para elaborar reportes con datos de asistencia.

BioStar permite a los administradores personalizar las funciones de tiempo y asistencia de los dispositivos BioStation y D-Station y especificar la forma en que se registrarán los eventos. La interfaz de BioStar también permite a los administradores supervisar el estado de la entrada y de la salida de un usuario en tiempo real. Para obtener más información acerca del tiempo y de la asistencia, consulte las secciones 3.8 y 4.6.

02 Instalación del software BioStar

La instalación de BioStar es un proceso bastante sencillo, aunque es necesario cumplir con algunos requisitos antes de iniciar la instalación:

- En primer lugar, es necesario elegir una PC que pueda permanecer conectada de forma constante y que pueda funcionar como el servidor BioStar. El servidor recibirá y almacenará los datos de registro de los dispositivos conectados en tiempo real.
- En segundo lugar, es necesario elegir el tipo de base de datos que se va a utilizar. El servidor BioStar es compatible tanto con MySQL o MS SQL Server (incluyendo las versiones inferiores, como la base de datos gratuita MS SQL Server Express). Independientemente de la base de datos elegida, usted debe contar con suficientes derechos y privilegios de acceso para conectarse a la base de datos y para crear nuevas tablas.
- En tercer lugar, asegúrese de que las computadoras que vaya a utilizar, tanto para los programas del servidor como para las del cliente, cumplen con los requisitos enumerados en la sección 2.1.

El CD de instalación de BioStar incluye un instalador exprés de BioStar, un instalador del servidor BioStar y un instalador del cliente BioStar. El instalador exprés instalará los programas del servidor y del cliente con entrada mínima (consulte la sección 2.2). Sin embargo, es posible elegir entre la instalación de los programas del servidor y del cliente de forma independiente, en caso de que sea necesario especificar opciones adicionales de la base de datos y la instalación de los programas en computadoras separadas (consulte las secciones 2.3 y 2.4).

2. Instalación del software BioStar

2.1 Requisitos del sistema

BioStar es compatible con los siguientes sistemas operativos (sólo versiones de 32 bits)

- Windows 7
- Windows Vista
- Windows XP, Service Pack 1 o posterior
- Windows 2003
- Windows 2000, Service Pack 4 o posterior

Los requisitos mínimos del sistema para instalar y utilizar el software BioStar son los siguientes:

- CPU: Intel Pentium o procesador similar capaz de procesar velocidades de 1 GHz o superiores.
- RAM: 512 MB
- HDD: 5 GB

Sin embargo, Suprema recomienda la siguiente configuración de hardware para un rendimiento óptimo:

- CPU: Intel Pentium Dual Core o procesador similar capaz de procesar velocidades de 2GHz o superiores.
- RAM: 1 GB para Windows XP; 2 GB para otros sistemas operativos
- HDD: 10 GB

2.2 Ejecución del instalador exprés de BioStar

Ejecute el instalador exprés de BioStar si desea instalar los programas del servidor y del cliente en la misma computadora y utilizar la base de datos MS SQL Server Express con la configuración predeterminada. Sólo tendrá que intervenir en el proceso de instalación exprés cuando ya se encuentre instalada la base de datos MS SQL Server o una variación. En este caso, se le preguntará si desea o no instalar MS SQL Server Express. Si desea no instalar la versión exprés, se le pedirá que proporcione los datos correctos de autentificación, tal y como se describe en el paso 7 de la sección 2.3.

El instalador exprés instalará los siguientes componentes:

- Programa del servidor BioStar
- Librerías auxiliares: OpenSSL y Microsoft Visual C++ Redistributable
- MS SQL Server Express
- Programa cliente BioStar
- BADB Conv (herramienta para migrar bases de datos)

2. Instalación del software BioStar

Antes de ejecutar el instalador exprés de BioStar, cierre todos los demás programas. Si ya instaló anteriormente BioAdmin en el mismo equipo, asegúrese de haber cerrado el servidor BioAdmin antes de iniciar la instalación. Para ejecutar el instalador exprés:

1. Inserte el CD de instalación de BioStar en una unidad compatible.
2. Localice el directorio de instalación y ejecute BioStar 1.3 Express Setup.
3. Siga las instrucciones que aparecen en pantalla para iniciar la instalación.

2.3 Instalación del programa servidor BioStar

Si elige no utilizar el instalador exprés, deberá instalar los programas del servidor y del cliente BioStar por separado. Después de asegurarse de que su sistema cumple con los requisitos mínimos enumerados en la sección 2.1, y de cumplir con los prerrequisitos mencionados en la introducción de este capítulo, cierre todos los demás programas abiertos. Si ya instaló anteriormente BioAdmin en el mismo equipo, asegúrese de haber cerrado el servidor BioAdmin antes de iniciar la instalación.

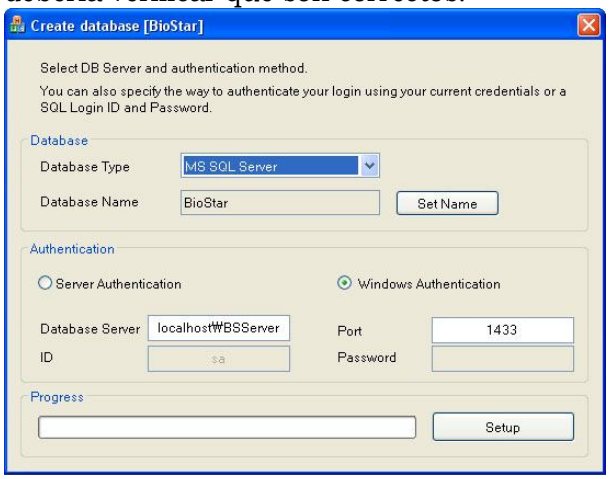
El instalador del servidor BioStar añadirá los siguientes componentes a su sistema:

- Programa del servidor BioStar
- MS SQL Server Express (opcional)
- Librerías auxiliares: OpenSSL y Microsoft Visual C++ 2005 Redistributable
- BADB Conv (herramienta para migrar bases de datos)

Para instalar el programa del servidor BioStar:

1. Inserte el CD de instalación de BioStar en una unidad compatible.
2. Localice el directorio de instalación y ejecute BioStar 1.3 Server Setup.
3. Siga las instrucciones que aparecen en pantalla para iniciar la instalación.
4. Durante la instalación, se le pedirá que acepte el contrato de licencia de OpenSSL y que seleccione una carpeta de destino para los archivos de programa de OpenSSL.
5. Se le preguntará si desea o no instalar MS SQL Server Express. En caso de que vaya a utilizar una versión anteriormente instalada de MS SQL Server, MySQL o Oracle, haga click en **No** cuando aparezca este mensaje. Si decide utilizar la versión exprés en este paso, puede ir al paso 7. El proceso de configuración de la base de datos será automático si instala la versión exprés.

6. Cuando aparezca la ventana Create Database [BioStar] (Crear base de datos [BioStar]), seleccione un tipo de base de datos (MS SQL Server, MySQL u Oracle). Los campos de la dirección del servidor de la base de datos (Database Server) y de los puertos (Port) se llenarán automáticamente; sin embargo, debería verificar que son correctos.



Nota: El nombre predeterminado de la base de datos siempre es "BioStar", para evitar instalar por equivocación varias bases de datos en el mismo sistema o en el mismo servidor de la base de datos. El nombre de la base de datos se puede cambiar editando el archivo DBSetup.exe. Al aplicar una revisión en el servidor de la base de datos, podrá seleccionar manualmente una base de datos.

7. Si elige MS SQL Server, deberá configurar también el método de autentificación (MySQL sólo permite la autentificación del servidor):
   - **Server authentication** (Autentificación del servidor): esta opción utiliza identificaciones y contraseñas para iniciar sesión y autentificar así a los usuarios que han sido creados y almacenados en el servidor SQL. Estas credenciales no se basan en las cuentas de usuario de Windows. Los usuarios que se conectan utilizando la autentificación del servidor, deben proporcionar sus credenciales siempre que se conectan.
   - **Windows authentication** (Autentificación de Windows): esta opción utiliza las cuentas de usuario de Windows para la autentificación. Cuando los usuarios se conectan mediante una cuenta de usuario de Windows, el servidor SQL valida el nombre y la contraseña de la cuenta utilizando el token principal de Windows en el sistema operativo. El servidor SQL no pide una contraseña y no valida de forma independiente la identificación de un usuario. La autentificación de Windows es el modo de autentificación predeterminado para MS SQL Server.

Nota: debe elegir el modo de autentificación compatible con la base de datos. También debe proporcionar las credenciales correspondientes para crear nuevas tablas en la base de datos.

8. Haga click en **Setup** (Instalar) para crear la base de datos SQL.
9. Una vez se haya completado la instalación de la base de datos SQL, haga click en **Finish** (Finalizar).
10. El programa de instalación realizará algunos procesos más antes de finalizar la instalación del servidor. Haga click en **Finish** (Finalizar).

2.3.1 Configuración de la base de datos MySQL

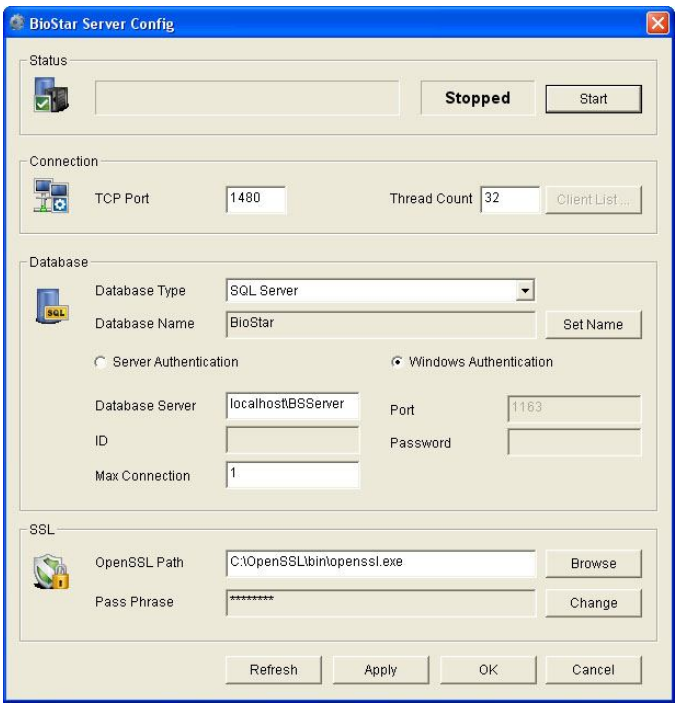
BioStar no puede utilizar la base de datos MySQL si el tamaño máximo del paquete es menor que 16 MB. Para configurar el tamaño máximo del paquete en el servidor MySQL, localice y abra un archivo de configuración para el servidor MySQL ("my.ini" en un sistema de Windows o "my.cnf" en un sistema de Linux). En [mysqld], agregue o edite el tamaño del paquete a 16 MB o mayor (por ejemplo: max_allowed_packet=16M). Cuando haya modificado y guardado el archivo, reinicie el servidor BioStar para aplicar los cambios.

2.3.2 Configuración del servidor BioStar

En algunos casos, es posible que necesite configurar manualmente el servidor BioStar. Si, por ejemplo, experimenta problemas al conectarse al servidor desde el programa cliente, es posible que necesite modificar la configuración del servidor. Además, debe cerrar y reiniciar el programa servidor para aplicar cualquier cambio que realice en la configuración del servidor o de la base de datos.

Para abrir la aplicación para configurar el servidor, localice y ejecute el archivo BSServerConfig.exe. De forma predeterminada, se agregará en el escritorio un acceso directo a esta aplicación durante la instalación del servidor BioStar. También puede localizar este archivo dentro de la carpeta "Server" (Carpeta), en donde se instaló el programa BioStar.

2. Instalación del software BioStar



La aplicación para configurar el servidor permite supervisar y controlar las siguientes opciones:

- **Status** (Estado): visualice y modifique el estado actual del servidor BioStar (*Stopped* (Detenido) o *Started* (Iniciado)). Usted puede detener e iniciar el servidor haciendo click en los botones **Start** (Iniciar) o **Stop** (Detener) de la izquierda.
- **Connection** (Conexión): visualice y modifique los detalles de la conexión entre el servidor y los dispositivos.
  - **TCP Port** (Puerto TCP): introduzca el puerto que los dispositivos y programas clientes van a utilizar para conectarse al servidor. Debería utilizar un puerto que no se comparta con ningún otro programa. En la mayoría de los casos, puede utilizar el puerto predeterminado (1480).
  - **Thread Count** (Número de subprocesos): introduzca el número máximo de subprocesos que el servidor BioStar puede crear. Puede introducir cualquier número entre 32 y 512. Sin embargo, recuerde que cuanto más alto sea el número de subprocesos, más recursos de sistema se consumirán.
  - **Client List** (Lista de clientes): haga click en este botón para ver una lista de los dispositivos conectados al servidor BioStar. La lista muestra la dirección IP de todos los dispositivos y si se ha emitido o no un certificado SSL para el dispositivo. Es posible emitir o eliminar certificados SSL directamente desde la aplicación.

- **Database** (Base de datos): visualice y modifique la configuración de la base de datos. Para obtener más información acerca de cómo modificar esta configuración, consulte el procedimiento para configurar el servidor BioStar en la sección 2.3.
  - **Max Connection** (Conexión máxima): especifique el número máximo de conexiones entre el servidor y la base de datos. En la mayoría de los casos, el valor predeterminado (1) es el adecuado.
- **SSL** (SSL): visualice y modifique la configuración para OpenSSL. Haga click en Browse (Examinar) para localizar la ruta del programa OpenSSL o haga click en Change (Cambiar) para cambiar la contraseña.

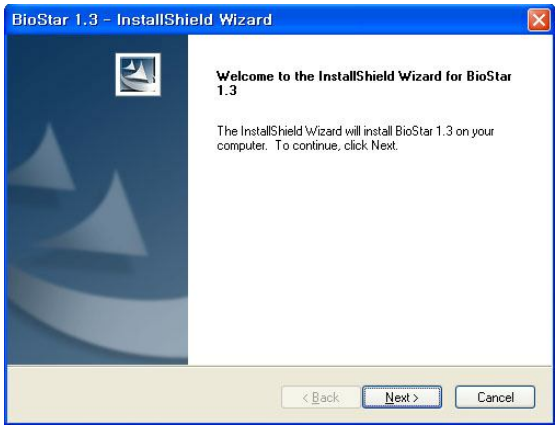
2.4 Instalación del programa cliente BioStar

Antes de instalar el programa cliente BioStar, cierre todos los demás programas abiertos. El instalador del programa cliente añadirá los siguientes componentes a su sistema:

- Programa cliente BioStar
- Librerías auxiliares: OpenSSL y Microsoft Visual C++ 2005 Redistributable

Para instalar el programa cliente BioStar:

1. Inserte el CD de instalación de BioStar en una unidad compatible.
2. Ejecute BioStar 1.3 Client Setup para iniciar el asistente de instalación.



3. Siga las instrucciones que aparecen en pantalla para instalar la terminal de usuario BioStar.

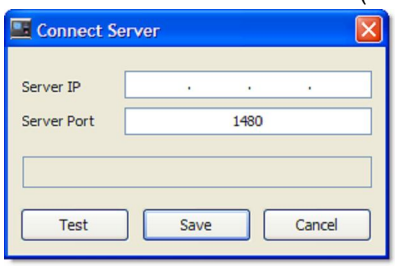
2.4.1 Inicio de sesión en BioStar por primera vez

Si reinicia el sistema después de la instalación, el servidor BioStar debería ejecutarse automáticamente de fondo. Si no ha reiniciado el sistema, es posible que se le pida conectarse manualmente al servidor antes de proceder (consulte la sección 2.3.2). Cuando inicie sesión en BioStar por primera vez, se le pedirá crear una cuenta de administrador.

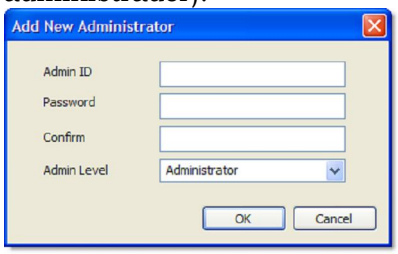
Para iniciar sesión por primera vez:

1. Inicie el programa BioStar. Si BioStar se conecta con éxito al servidor, aparecerá automáticamente la ventana Add New Administrator (Añadir nuevo administrador). En este caso, vaya al paso 6. Si BioStar no se puede conectar al servidor, la ventana Login (Inicio de sesión) se abrirá y mostrará el mensaje: “Cannot connect to server" (No se puede conectar al servidor).

2. Haga click en **Server Setting** (Configuración del servidor). Esta acción abrirá la ventana Connect Server (Conectar servidor).



3. Introduzca la dirección IP y el número de puerto del servidor BioStar.
4. Haga click en **Test** (Probar) para comprobar la conexión.
5. Haga click en **Save** (Guardar) para almacenar la configuración de la conexión. Esta acción abrirá la ventana Add New Administrator (Añadir nuevo administrador).



6. Introduzca una Id. de administrador (Admin ID) y una contraseña (Password) y elija un nivel de administración del menú desplegable.

7. Haga click en **OK** (Aceptar). Esto lo devolverá a la ventana de inicio de sesión.
8. Introduzca una Id. de usuario (User ID) y una contraseña (Password) y haga click en **Login** (Iniciar sesión).

2.5 Personalización de la interfaz de BioStar

No es necesario realizar ningún cambio en la interfaz para utilizar el sistema BioStar; la configuración predeterminada es suficiente para que se instale y funcione. Sin embargo, BioStar permite personalizar varios aspectos de la configuración para controlar la apariencia y la funcionalidad de la interfaz.

2.5.1 Cambio de tema

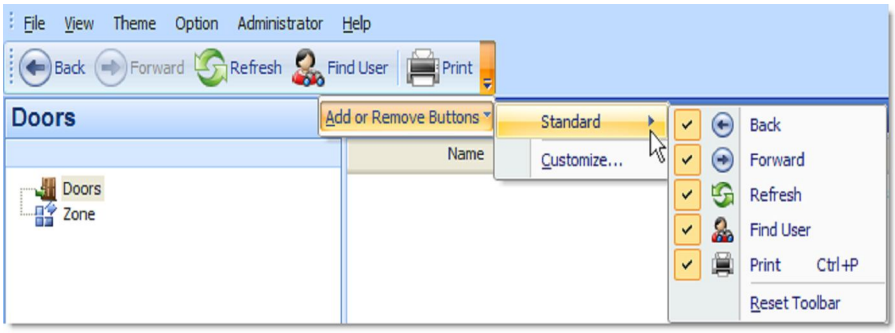
La interfaz de BioStar incluye dos temas predefinidos basados en los estilos de MS Office:

- Office 2003
- Office 2007

Para cambiar el tema, haga click en **Theme** (Tema) de la barra de menú y seleccione un tema.

2.5.2 Personalización de la barra de herramientas

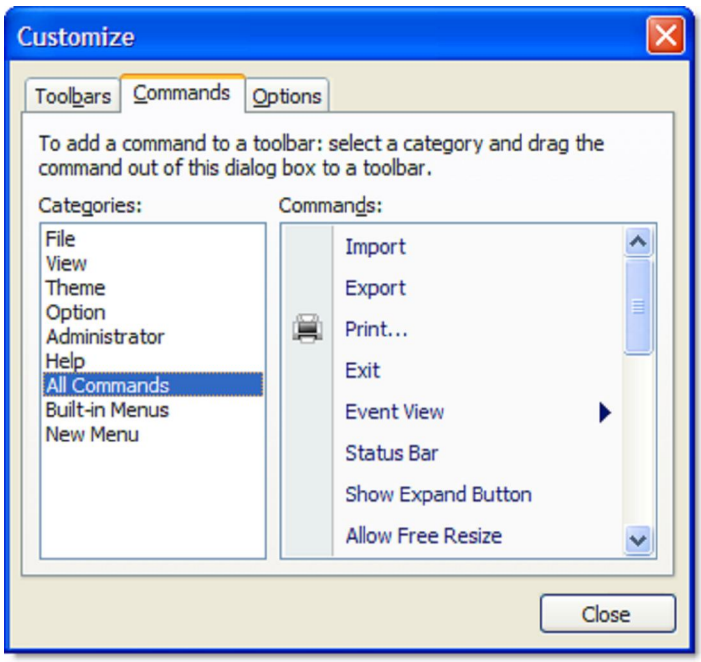
La interfaz de BioStar incluye una barra de herramientas estándar en la parte superior izquierda de la ventana. Los botones de la barra de herramientas estándar proporciona funciones parecidas a las de un navegador de Internet normal: Back (Regresar), Forward (Adelante), Refresh (Actualizar), Find User (búsqueda) (Encontrar usuario (búsqueda)), y Print (Imprimir).



Para personalizar la barra de herramientas:

1. Haga click en la flecha desplegable que se encuentra a la derecha de la barra de herramientas.
2. Haga click en **Add or Remove Buttons > Customize** (Añadir o eliminar botones > Personalizar). Esta acción abrirá la ventana Customize (Personalizar).

3. Haga click en la pestaña Commands (Comandos).
4. Haga click en *All Commands* (Todos los comando) para visualizar una lista con los botones disponibles.



5. Arrastre un comando a la barra de herramientas. Esto añadirá un nuevo botón para el comando.

2.5.3 Cambio de las vistas de eventos

BioStar permite cambiar los períodos de eventos predeterminados que se muestran en la pestaña Event (Evento) para usuarios o puertas y zonas. Es posible configurar la interfaz para que muestre los detalles de evento para 1 día, 3 días o 1 semana de forma predeterminada. Para cambiar la vista de eventos:

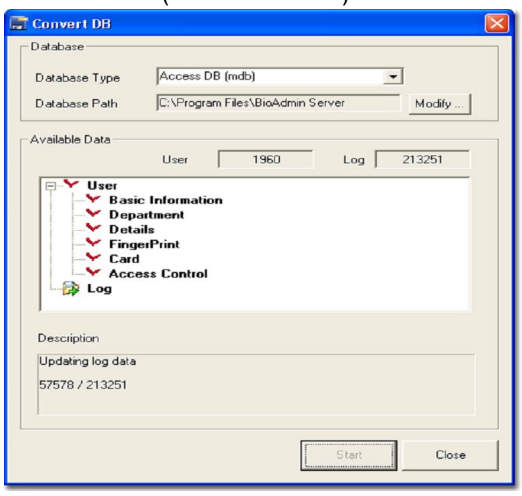
1. En la barra de menú, haga click en **View > Event View** (Ver > Vista de evento).
2. Haga click en el tipo de vista de evento que desea cambiar (*User* or *Doors/Zone* (Usuario o Puertas/Zona)).
3. Haga click en un período de eventos predeterminado (*1 day*, *3 day*, or *7 day*(1 día, 3 días o 7 días)).

2.6 Migración de una base de datos desde BioAdmin a BioStar

El programa de instalación de BioStar incluye una herramienta para migrar bases de datos llamada *BADB Conv*. Esta herramienta permite migrar una base de datos existente en BioAdmin a nuestro nuevo sistema BioStar.

Al migrar una base de datos, cualquier dato idéntico que exista en la base de datos de BioStar se sobrescribirá. Por ejemplo, si usted añade un usuario a BioStar que ya existía en BioAdmin, los datos del usuario se sobrescribirán con la información de la base de datos de BioAdmin. Por este motivo, debería migrar su antigua base de datos a BioStar antes de crear una cuenta de usuario nueva. Para migrar la información de BioAdmin a BioStar:

1. Localice y ejecute el programa de migración *BADBConv.exe*. De forma predeterminada, esta herramienta se instalará en la misma carpeta que el software BioStar.
2. Haga click en **Yes** (Sí) para aceptar el mensaje de aviso que le recuerda que la información idéntica en BioStar se sobrescribirá.
3. En caso de que ya se encuentre instalado, haga click en **Start** (Iniciar) para iniciar la instalación. Una vez se haya completado el proceso, la ventana Convert DB (Convertir BD) le mostrará los tipos de datos que se han migrado.



4. Haga click en **Close** (Cerrar) para salir de la herramienta de migración.

03 Configuración del sistema BioStar

Esta sección describe cómo añadir cuentas de administrador, dispositivos, puertas, zonas, departamentos, usuarios y grupos de acceso, y también cómo configurar el tiempo y la asistencia con el software BioStar. Esta guía del administrador no cubre los procedimientos para instalar los componentes físicos, el cableado de las puertas y dispositivos o para conectar los dispositivos a la red. Para obtener más información acerca de la instalación del hardware y la configuración física del sistema de control de acceso, consulte las guías de instalación de los dispositivos de control de acceso.

3.1 Creación de cuentas administrativas

Antes de añadir usuarios, le aconsejamos añadir y configurar las cuentas de los administradores y operadores del sistema. También resulta útil entender algunos conceptos generales relacionados con la administración del sistema BioStar.

3.1.1 Niveles administrativos

BioStar permite múltiples niveles de administración, funcionamiento e interacción con el sistema. Cada nivel administrativo posee diversos grados de privilegios y acceso a los menús del sistema User (Usuario), Doors (Puertas), Visual Map (Mapa visual), Access Control (Control de acceso), Monitoring (Supervisión), Devices (Dispositivos) y Time & Attendance (Tiempo y asistencia)). El sistema BioStar incluye tres niveles de administrador predeterminados además de los niveles de administrador personalizados:

- Administrador
- Operador
- Gerente
- Niveles de administrador personalizados

3. Configuración del sistema BioStar

Los administradores pueden añadir y configurar dispositivos, usuarios, puertas, zonas y grupos de acceso. También pueden gestionar las funciones de tiempo y asistencia, incluyendo las categorías para configurar la hora, los programas diarios, los turnos, las normas vacacionales y períodos de permiso, así como también crear, modificar y visualizar los reportes de tiempo y asistencia. Además, los administradores pueden crear niveles de administrador personalizados a los que se les otorga diversos privilegios para los menús del sistema BioStar.

Los operadores pueden supervisar y gestionar el sistema BioStar mediante una terminal de usuario remota. Los operadores poseen los mismos privilegios que los administradores, pero no poseen los privilegios para crear o eliminar otras cuentas de administrador u operador. Como ocurre con los administradores, los operadores pueden añadir y configurar dispositivos, usuarios, puertas, zonas y grupos de acceso. También pueden gestionar las funciones de tiempo y asistencia, incluyendo las categorías para configurar la hora, los programas diarios, los turnos, las normas vacacionales y períodos de permiso, así como también crear, modificar y visualizar los reportes de tiempo y asistencia.

Los gerentes poseen privilegios para leer toda la información de los menús. Sin embargo, no pueden crear, modificar o eliminar nada en los menús. Dependiendo de las necesidades de su organización, la posibilidad de ver eventos puede resultar útil para otros propósitos de gestión.

Al nivel de administrador personalizado se le pueden asignar privilegios completos o limitados en los siete menús. En cada menú, usted puede asignar uno de estos tres privilegios: All Rights (Todos los derechos), Modify (Modificación), o Read (Lectura). Dependiendo de las necesidades de su organización, el sistema BioStar se puede gestionar de forma más efectiva añadiendo niveles de administrador personalizados.

Una configuración típica consistirá en un administrador (o más, dependiendo del tamaño de la organización) con acceso total al sistema. Por debajo del nivel del administrador, varios operadores pueden realizar diversas funciones, como controlar de forma remota puertas y cerraduras, añadir usuarios, registrar huellas, expedir tarjetas de acceso, añadir grupos de acceso, definir zonas horarios y configurar eventos de alarma.

3.1.2 Adición y personalización de cuentas administrativas

De forma predeterminada, BioStar incluye una cuenta de administrador que se añade al instalar el software (consulte la sección 2.3). Puede elegir entre utilizar esta cuenta como el único administrador y otorgar privilegios de operador al resto de usuarios que gestionarán el sistema, o añadir varios administradores al sistema.

3.1.2.1 Adición de una cuenta administrativa

Para añadir una cuenta administrativa:

1. En la barra de menú, haga click en **Administrator > Admin Account** (Administrador > Cuenta de administrador) para abrir la ventana Admin Account List (Lista de cuentas de administrador).
2. Haga click en **Add New Administrator** (Añadir nuevo administrador).
3. En la ventana Add New Administrator (Añadir nuevo administrador), introduzca una Id. de administrador (Admin ID) y una contraseña (Password).
4. Confirme la contraseña volviéndola a introducir y seleccione un nivel de administrador (Admin Level) de la lista desplegable:
   - **Administrator** (Administrador): todos los privilegios.
   - **Operator** (Operador): todos los privilegios, excepto aquellos necesarios para crear o eliminar cuentas de administrador y operario.
   - **Manager** (Gerente): privilegio para leer toda la información.
5. Haga click en **OK** (Aceptar).

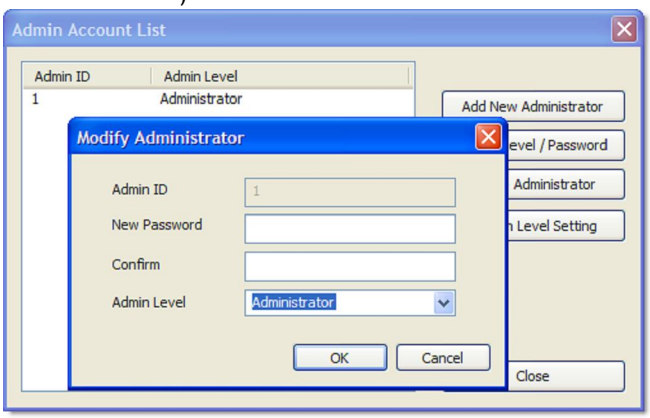
3.1.2.2 Cambio del nivel o de la contraseña de una cuenta administrativa

Si selecciona por accidente el nivel equivocado para una cuenta administrativa, o si necesita cambiar o volver a introducir una contraseña, puede hacerlo en el menú Administrator (Administrador).

Para cambiar un nivel administrativo o contraseña:

1. En la barra de menú, haga click en **Administrator > Admin Account** (Administrador > Cuenta de administrador) para abrir la ventana Admin Account List (Lista de cuentas de administrador).
2. Haga click en una cuenta de administrador de la lista que se encuentra en la parte izquierda de la ventana.
3. Haga click en **Modify Level/Password** (Modificar nivel/contraseña). Esta acción abrirá la ventana Modify Administrator (Modificar

administrador).



4. Edite la información necesaria de la cuenta:
   - Para cambiar el nivel administrativo, elija un nuevo nivel de la lista desplegable.
   - Para cambiar la contraseña, escriba una nueva contraseña en los campos New Password (Nueva contraseña) y Confirm (Confirmar).
5. Haga click en **OK** (Aceptar) para guardar los cambios.

3.1.2.3 Creación de un nivel de administración personalizado

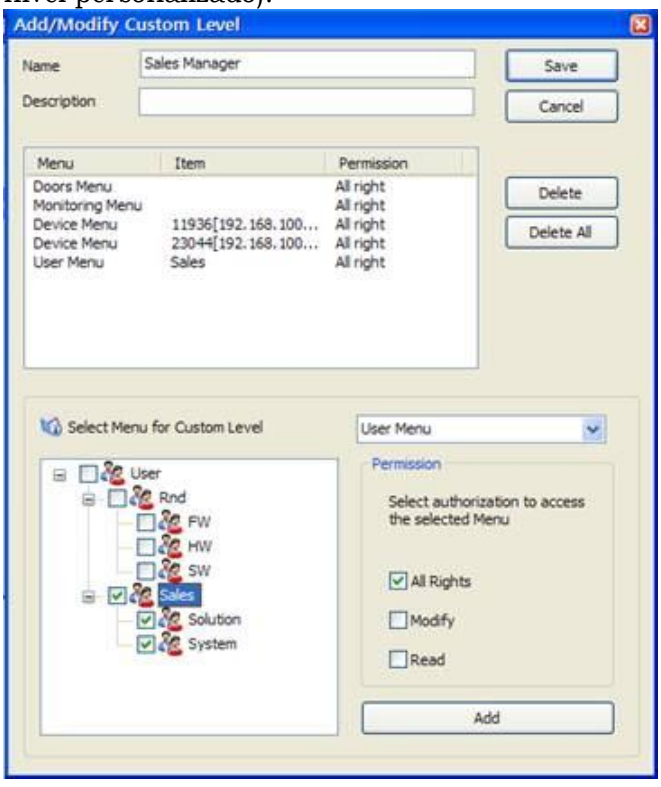
Si necesita definir un papel de administrador específico con privilegios particulares, puede añadir un nivel de administrador personalizado. Puede permitir el acceso total o limitado a cualquiera de los siete menús de BioStar para el nivel de administrador personalizado: User (Usuario), Doors (Puertas), Visual Map (Mapa visual), Access Control (Control de acceso), Monitoring (Supervisión), Devices (Dispositivos) y Time & Attendance (Tiempo y asistencia).

Al nivel de administrador personalizado se le puede asignar privilegios para usuarios y dispositivos específicos. Un administrador personalizado tendrá los privilegios que usted le asigne (All Rights (Todos los derechos), Modify (Modificación), o Read (Lectura)) sólo para aquellos usuarios o dispositivos que usted especifique, y por lo tanto, no podrá ver ni modificar otros usuarios o dispositivos. Al mismo tiempo que crea un nivel de administrador personalizado, en el menú User (Usuario), puede otorgar privilegios para usuarios en un área y subáreas. Sin embargo, asegúrese de que no puede seleccionar usuarios individuales, sino las áreas de primer o segundo nivel a las que pertenecen. En el menú Device (Dispositivo), usted puede otorgar privilegios para dispositivos específicos. Si un dispositivo posee un dispositivo esclavo, los privilegios para el dispositivo anfitrión también se aplicarán en los dispositivos esclavos. Los usuarios y dispositivos que no se seleccionen en los menús User (Usuario)

y Device (Dispositivo) no aparecerán en los menús Doors (Puertas), Visual Map (Mapa visual), Access Control (Control de acceso), Monitoring (Supervisión) y Time and Attendance (Tiempo y asistencia). Y, si una puerta o zona se encuentra asociada con dispositivos a los que no se les ha otorgado privilegios, la puerta o zona no aparecerá en el menú Doors (Puertas).

Para crear un nivel de administrador personalizado:

1. En la barra de menú, haga click en **Administrator > Admin Account** (Administrador > Cuenta de administrador) para abrir la ventana Admin Account List (Lista de cuentas de administrador).
2. Haga click en **Custom Level Setting** (Configuración del nivel personalizado).
3. En la ventana Custom Level List (Lista de niveles personalizados), haga click en **Add Custom Level** (Añadir nivel personalizado). Esta acción abrirá la ventana Add/Modify Custom Level (Añadir/Modificar nivel personalizado).



4. Escriba un nombre para el nivel personalizado en el campo Name (Nombre).
5. Si lo desea, añada una descripción adicional en el campo Description (Descripción).
6. Seleccione un menú de la lista desplegable.

7. Al seleccionar el menú usuario (User Menu) o el menú dispositivo (Device Menu), seleccione los usuarios o dispositivos a los que otorgará privilegios haciendo click en las casillas de validación de la lista de usuarios o dispositivos.
8. Seleccione un nivel de permisos All Rights (Todos los derechos), Modify (Modificación), o Read (Lectura)) haciendo click en las casillas de validación que se encuentran al lado de una opción.
9. Haga click en **Add** (Añadir) para incluir el permiso en el nivel personalizado.
10. Repita los pasos 6 y 9 tantas veces como sea necesario para añadir más permisos.
11. Una vez haya finalizado de personalizar el nivel, haga click en **Save** (Guardar).

Ahora puede crear nuevas cuentas administrativas con cualquiera de los niveles de administrador personalizados que creó.

3.2 Configuración de dispositivos

Esta sección describe cómo utilizar el asistente de dispositivos de BioStar para buscar y añadir nuevos dispositivos y cómo añadir dispositivos de RF de terceros. Además, los siguientes procedimientos describen la configuración básica de dispositivos en el sistema BioStar. Para obtener más información acerca de cómo configurar dispositivos, consulte las secciones 3.9.3 y 5.1.

3.2.1 Búsqueda y adición de dispositivos

BioStar incluye un asistente práctico para encontrar y añadir dispositivos. Antes de iniciar una búsqueda de nuevos dispositivos, verifique las conexiones de los dispositivos. Si tiene que añadir varios dispositivos, puede resultar útil preparar una lista con la localización, las identificaciones y las direcciones IP de los dispositivos antes de añadirlos.

Para buscar dispositivos y añadirlos al sistema BioStar:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Add Device* (Añadir dispositivo).
3. Cuando aparezca el asistente, haga click en el botón de radio que se encuentra al lado de uno de los tipos de conexión:
   - **LAN**: elija esta opción para buscar dispositivos conectados mediante Ethernet o WLAN.
   - **Serial** (En serie): elija esta opción para buscar dispositivos conectados a una computadora secundaria mediante RS485 y RS232, o dispositivos

esclavos conectados mediante RS485 a otro dispositivo conectado a una computadora secundaria (consulte la sección 3.2.2).

- **USB Device** (Dispositivo USB): elija esta opción para buscar dispositivos conectados a puertos USB.
- **Virtual USB Device** (Dispositivo USB virtual): elija esta opción para buscar dispositivos virtuales que haya añadido a una unidad virtual.

4. Haga click en **Next** (Siguiente).

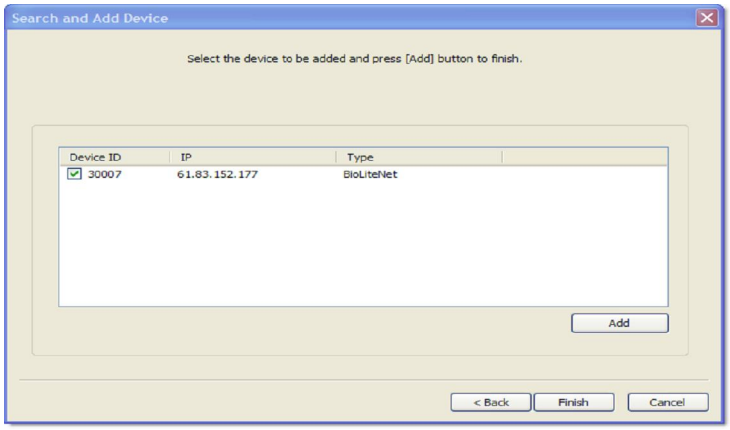
5. Para búsquedas USB o USB virtuales, vaya al paso 7. Si está buscando dispositivos conectados en red LAN o puertos en serie, establezca criterios de búsqueda avanzados:
   - LAN: seleccione si quiere buscar dispositivos utilizando los protocolos TCP o UDP. Si selecciona TCP, puede especificar un rango de dirección IP, el tipo de dispositivo que está buscando (BioStation/D-Station: 1470, BioEntry Plus/BioLite Net/Xpass: 1471, o Custom (Personalizado): introducir manualmente) y el puerto que busca. Si selecciona UDP, sólo puede buscar dispositivos en la misma subred.
   - Serial (En serie): especifique un puerto COM o seleccione *All port* (Todos los puertos) y una velocidad de transmisión.
6. Haga click en **Next** (Siguiente).
7. Cuando BioStar completa la búsqueda, puede especificar la configuración de red tal y como se describe a continuación. Haga click en un nombre de dispositivo de la lista que se encuentra a la izquierda y configure los parámetros como sea necesario:

   Nota: si cambia la configuración de red para un dispositivo en este punto, el dispositivo se eliminará de la lista de dispositivos. Para agregar el dispositivo en los siguientes pasos, deberá realizar de nuevo la búsqueda del dispositivo.

   No es necesario y no debe añadir dispositivos con el modo servidor. Los dispositivos se conectarán automáticamente al servidor y aparecerán en la lista del servidor BioStar en el árbol de dispositivos. Si intenta añadir dispositivos en modo servidor, se producirá un fallo en el proceso.

   - **DHCP or Static IP** (DHCP o IP estática): si elige utilizar la opción DHCP, el dispositivo obtendrá automáticamente la configuración de red del servidor DHCP. Si no utiliza DHCP, debe configurar los parámetros de red manualmente.
   - **Direct connection** (Conexión directa): esta es la opción de conexión predeterminada. Con esta opción, la terminal de usuario BioStar se conectará directamente al dispositivo. Si elige este tipo de conexión, se deberá ejecutar la terminal de usuario BioStar para obtener los registros del dispositivo.
   - **Server connection** (Conexión del servidor): si elige esta opción, el dispositivo se conectará automáticamente al servidor BioStar. Si configura correctamente la dirección IP y el puerto del servidor, los registros del dispositivo se almacenarán en el servidor, sin importar si la terminal de usuario BioStar se encuentra o no conectada. Esta opción también puede ser útil si la configuración de la red necesita que conecte dispositivos con direcciones IP privadas (por ejemplo, en una red WAN) a un servidor con una dirección IP pública. Esta opción también proporciona encriptación SSL para los dispositivos BioStation.

8. Haga click en **Next** (Siguiente).
9. Seleccione el dispositivo o dispositivos que va a añadir haciendo click en las casillas de validación que se encuentran al lado de el id. del dispositivo (Device ID).



10. Haga click en **Add** (Añadir) para añadir los dispositivos al sistema BioStar.
11. Cierre el mensaje de confirmación que aparece y haga click en **Finish** (Finalizar) para salir del asistente.

3.2.2 Búsqueda y adición de dispositivos esclavos

Una función característica de BioStar es que es compatible con dispositivos anfitriones y esclavos en redes RS485. Con esta función, sólo se debe conectar el dispositivo anfitrión a una computadora mediante una red LAN. La red se puede expandir fácilmente añadiendo dispositivos esclavos mediante conexiones RS485.

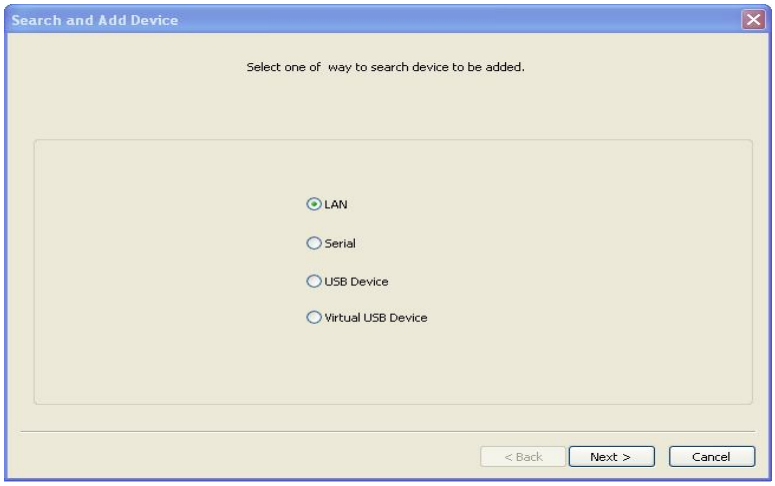
Si la configuración incluye dispositivos esclavos, deberá realizar una búsqueda adicional para localizarlos y agregarlos.

En primer lugar, configure el dispositivo anfitrión:

1. Busque y añada el dispositivo anfitrión tal y como se describe en la sección 3.2.1.
2. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
3. En el panel de navegación, haga click en el dispositivo anfitrión.
4. En el panel del dispositivo, haga click en la pestaña Network (Red).
5. Cambie la configuración en serie RS485 seleccionando la opción *Host* (Anfitrión) de la lista desplegable Mode (Modo).
6. Haga click en **Apply** (Aplicar) para guardar el cambio.

A continuación, busque y añada dispositivos esclavos:

1. En el panel de navegación, haga click con el botón secundario del ratón en el dispositivo anfitrión y haga click en **Add Device (Serial)** (Añadir dispositivo (en serie)). Esta acción abrirá la ventana Search and Add Device (Buscar y añadir dispositivo).



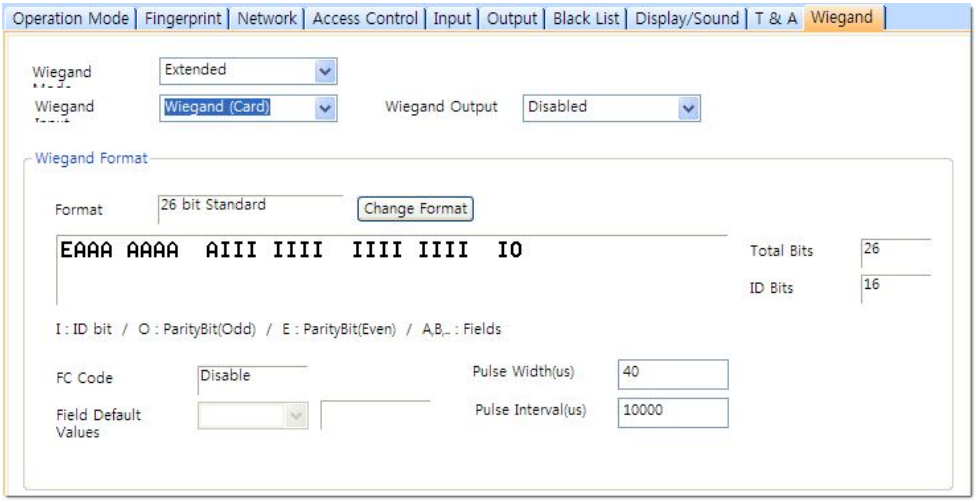
2. Haga click en **Next** (Siguiente) para iniciar la búsqueda.
3. Cuando BioStar complete la búsqueda, haga click en **Next** (Siguiente).
4. Seleccione el dispositivo o dispositivos que va a añadir haciendo click en las casillas de validación que se encuentran al lado de el id. del dispositivo (Device ID).
5. Haga click en **Add** (Añadir) para añadir el dispositivo.
6. Cierre el mensaje de confirmación que aparece y haga click en **Finish** (Finalizar) para salir del asistente.
7. En el panel de navegación, haga click en el dispositivo esclavo.
8. En el panel del dispositivo, haga click en la pestaña Network (Red).
9. Cambie la configuración en serie RS485 seleccionando la opción *Slave* (Esclavo) de la lista desplegable Mode (Modo).
10. Haga click en **Apply** (Aplicar) para guardar el cambio.

3.2.3 Adición de un dispositivo por RF

Antes de BioStar 1.2, los dispositivos de RF de terceros, conectados a los dispositivos de Suprema (los dispositivos BioStation, BioEntry Plus, and BioLite Net), sólo funcionaban como extensiones físicas de los dispositivos de Suprema. Como en BioStar 1.2, los dispositivos de RF de terceros conectados a los dispositivos de Suprema funcionan de forma independiente y se pueden asociar con puertas e incluso en zonas.

Para añadir un dispositivo de RF:

1. Conecte el dispositivo de RF a un dispositivo de Suprema.
2. Asegúrese de que el dispositivo de Suprema se añadió al sistema BioStar (consulte la sección 3.2.1).
3. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
4. En el panel de navegación, haga click en el nombre del dispositivo de Suprema.
5. Haga click en la pestaña Wiegand y especifique la configuración Wiegand tal y como se describe a continuación:



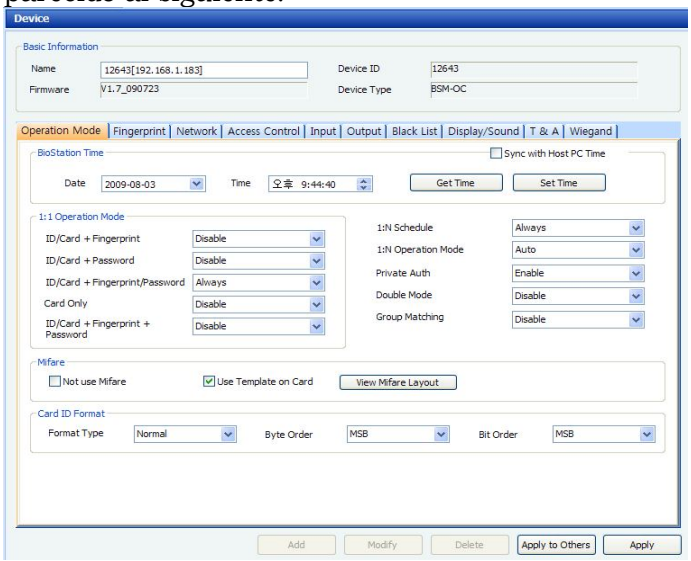
   a. Seleccione **Extended** (Extendido) en la lista desplegable del modo Wiegand (Wiegand Mode).
   b. Seleccione **Wiegand (Card)** (Wiegand (Tarjeta)) en la lista desplegable Wiegand Input (Entrada Wiegand).
   c. Haga click en **Apply** (Aplicar) al final del panel.
6. En el panel de navegación, haga click con el botón secundario del ratón en el nombre del dispositivo BioStation y luego haga click en *Add RF Device* (Añadir lector RF).

Nota: para obtener más información acerca de cómo utilizar lectores RF de terceros, consulte la guía de usuario del lector RF. El formato Wiegand se debe configurar correctamente para asegurar la compatibilidad con lectores RF de terceros.

3.2.4 Configuración de un dispositivo BioStation

Esta sección proporciona una visión general de la configuración de los dispositivos BioStation para que trabajen con el software BioStar. Para obtener más información, consulte las guías de instalación de los dispositivos. Para configurar un dispositivo BioStation:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. Haga doble click en el nombre de un dispositivo BioStation en el panel de navegación. Esta acción abrirá un panel, llamado Device (Dispositivo), parecido al siguiente:



3. Configure la información del dispositivo en las siguientes pestañas. Para una explicación de la configuración del dispositivo, consulte la sección 5.1.1.
   - **Operation mode** (Modo de funcionamiento): utilice esta pestaña para establecer la hora del dispositivo o para obtenerla de una computadora central y ajuste la configuración para los modos de funcionamiento.
   - **Fingerprint** (Huella dactilar): utilice esta pestaña para especificar la configuración de seguridad, calidad, identificación y tiempo de espera agotado para el reconocimiento de las huellas dactilares.
   - **Network** (Red): utilice esta pestaña para especificar la configuración de las conexiones en red LAN o en serie.
   - **Access Control** (Control de acceso): utilice esta pestaña para especificar los límites de entrada y los grupos de acceso predeterminados de un dispositivo.
   - **Input** (Entrada): utilice esta pestaña para añadir, modificar o eliminar la configuración de entrada del dispositivo.
   - **Output** (Salida): utilice esta pestaña para añadir, modificar o eliminar la configuración de salida del dispositivo.

- **Black List** (Lista negra): utilice esta pestaña para deshabilitar el acceso de tarjetas MIFARE en los dispositivos BioStation Mifare.
- **Display/Sound** (Pantalla/Sonido): utilice esta pestaña para ajustar la configuración de la pantalla o del sonido y añada imágenes de fondo y sonidos.
- **T&A** (Tiempo y asistencia): utilice esta pestaña para configurar los parámetros de tiempo y asistencia.
- **Wiegand**: utilice esta pestaña para configurar el formato Wiegand. Para obtener más información acerca de los formatos Wiegand, consulte la sección 3.2.9.

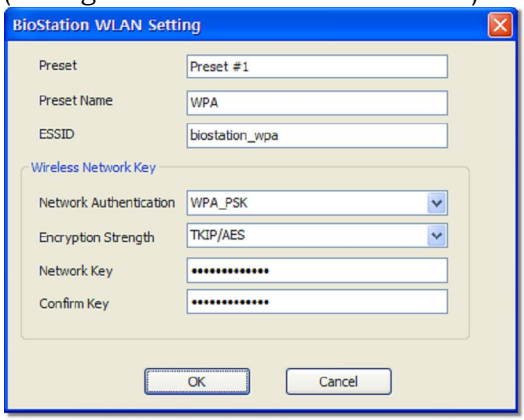
4. Cuando finalice de configurar el dispositivo, haga click en **Apply** (Aplicar) para guardar los cambios.
5. Para aplicar la misma configuración a otros dispositivos, haga click en **Apply to Others** (Aplicar a otros) y seleccione los otros dispositivos en la ventana Device Tree (Árbol de dispositivos).

3.2.4.1 Conexión de un dispositivo BioStation mediante una red WLAN

Algunos dispositivos BioStation son compatibles con conexiones en red WLAN. Para configurar los parámetros de una conexión WLAN:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. Haga click en el nombre de un dispositivo BioStation en el panel de navegación.
3. Haga click en la pestaña Network (Red), en el panel Device (Dispositivo).
4. Seleccione la opción “Wireless LAN" en la lista desplegable Lan Type (Tipos de redes LAN).
5. Seleccione una de las configuraciones predeterminadas en la sección WLAN (*Preset #1 - Preset #4*) (Predeterminada #1 - Predeterminada # 4).
6. Haga click en **Change Setting** (Cambiar configuración) en la sección WLAN. Esta acción abrirá la ventana BioStation WLAN Setting

(Configuración WLAN de BioStation).



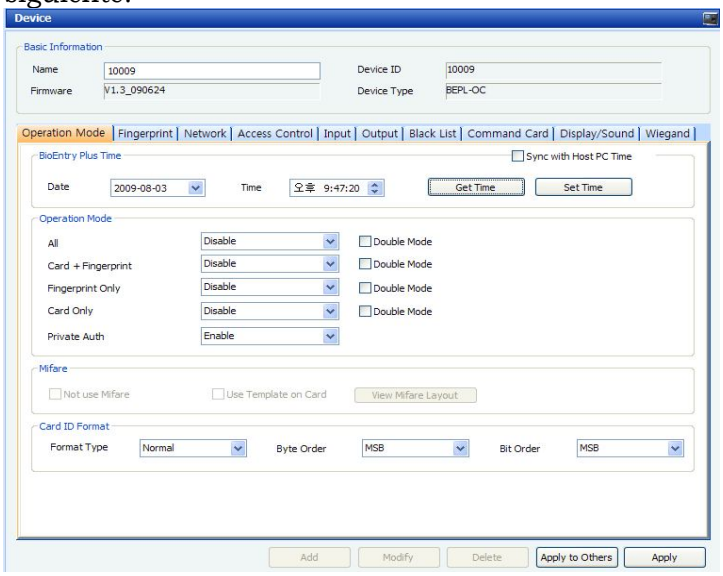
7. Configure los siguientes parámetros:
   - **Preset Name** (Predeterminar nombre): introduzca el nombre para la configuración que aparecerá en el dispositivo BioStation conectado a través de una red WLAN.
   - **ESSID**: introduzca el id. única del punto de acceso.
   - **Network Authentication** (Autentificación de red): seleccione un modo de autentificación de red de la lista desplegable (Open System (Sistema abierto), Shared Key (Clave compartida), o WPA-PSK). El modo de autentificación debe ser el mismo para el dispositivo y para el punto de acceso.
   - **Encryption Strength** (Fortaleza de la encriptación): seleccione una fortaleza de encriptación de la lista desplegable (las opciones disponibles dependen de la configuración de autentificación de red).
   - **Network Key** (Clave de red): introduzca una clave de red.
   - **Confirm Key** (Confirmar clave): vuelva a introducir la clave de red.
8. Haga click en **OK** (Aceptar) para guardar los cambios.

3.2.5 Configuración de un dispositivo BioEntry Plus

Para configurar un dispositivo BioEntry Plus:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. Haga doble click en el nombre de un dispositivo en el panel de navegación. Esta acción abrirá un panel, llamado Device (Dispositivo), parecido al

siguiente:

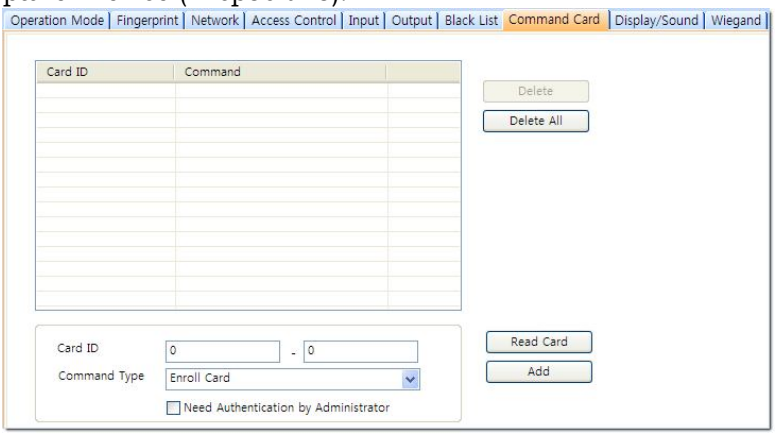


3. Configure la información del dispositivo en las siguientes pestañas. Para una explicación de la configuración del dispositivo, consulte la sección 5.1.2.
   - **Operation mode** (Modo de funcionamiento): utilice esta pestaña para establecer la hora del dispositivo o para obtenerla de una computadora central, ajuste la configuración para los modos de funcionamiento y ajuste las opciones para el reconocimiento de las huellas dactilares.
   - **Fingerprint** (Huella dactilar): utilice esta pestaña para especificar la configuración de seguridad, calidad, identificación y tiempo de espera agotado para el reconocimiento de las huellas dactilares.
   - **Network** (Red): utilice esta pestaña para especificar la configuración de las conexiones en red LAN o en serie.
   - **Access Control** (Control de acceso): utilice esta pestaña para especificar la configuración de los límites de entrada, grupos de acceso y modo de tiempo y asistencia.
   - **Input** (Entrada): utilice esta pestaña para añadir o modificar las entradas del dispositivo.
   - Output (Salida): utilice esta pestaña para añadir o modificar las salidas del dispositivo.
   - **Black List** (Lista negra): utilice esta pestaña para deshabilitar el acceso de tarjetas MIFARE en los dispositivos BioEntry Plus Mifare.
   - **Command Card** (Tarjeta de comando): utilice esta pestaña para expedir tarjetas de comando que puedan controlar dispositivos BioEntry Plus. Para obtener más información acerca de cómo expedir tarjetas de comando, consulte la sección 3.2.5.1.
   - **Display/Sound** (Pantalla/Sonido): utilice esta pestaña para configurar los parámetros del LED y del zumbido de acuerdo con el evento o estado.
   - **Wiegand**: utilice esta pestaña para configurar el formato Wiegand. Para obtener más información acerca de los formatos Wiegand, consulte la sección 3.2.9.
4. Cuando finalice de configurar el dispositivo, haga click en **Apply** (Aplicar) para guardar los cambios.
5. Para aplicar la misma configuración a otros dispositivos, haga click en **Apply to Others** (Aplicar a otros) y seleccione los otros dispositivos en la ventana Device Tree (Árbol de dispositivos).

3.2.5.1 Expedición de tarjetas de comando

Las tarjetas de comando le permiten registrar y eliminar usuarios directamente desde un dispositivo BioEntry Plus. Para obtener más información acerca de cómo registrar usuarios utilizando tarjetas de comando, consulte la sección 3.5.2.3. Para obtener más información acerca de cómo eliminar un solo usuario o todos los usuarios utilizando tarjetas de comando, consulte las secciones 4.5.1.1 y 4.5.1.2. Para expedir tarjetas de comando:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un dispositivo BioEntry Plus.
3. Haga click en la pestaña Command Card (Tarjeta de comando), en el panel Device (Dispositivo).

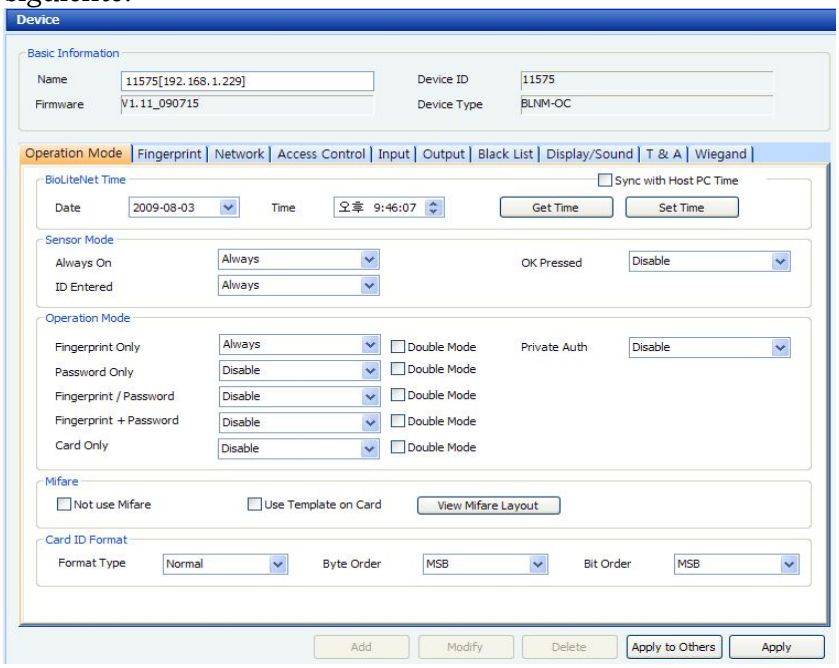


4. Haga click en **Read Card** (Leer tarjeta).
5. Coloque una tarjeta de comando en el dispositivo.
6. Seleccione un tipo de comando de la lista desplegable.
7. Si lo desea, configure la tarjeta de comando para que solicite la autentificación del administrador haciendo click en la casilla de validación que se encuentra al lado de la opción.
8. Haga click en **Add** (Añadir).

3.2.6 Configuración de un dispositivo BioLite Net

Para configurar un dispositivo BioLite Net:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. Haga doble click en el nombre de un dispositivo en el panel de navegación. Esta acción abrirá un panel, llamado Device (Dispositivo), parecido al siguiente:



3. Configure la información del dispositivo en las siguientes pestañas. Para una explicación de la configuración del dispositivo, consulte la sección 5.1.3.
   - **Operation mode** (Modo de funcionamiento): utilice esta pestaña para establecer la hora del dispositivo o para obtenerla de una computadora central, ajuste la configuración para los modos de funcionamiento y ajuste las opciones para el reconocimiento de las huellas dactilares.
   - **Fingerprint** (Huella dactilar): utilice esta pestaña para especificar la configuración de seguridad, calidad, identificación y tiempo de espera agotado para el reconocimiento de las huellas dactilares.
   - **Network** (Red): utilice esta pestaña para especificar la configuración de las conexiones en red LAN o en serie.
   - **Access Control** (Control de acceso): utilice esta pestaña para especificar los límites de entrada y los grupos de acceso.
   - **Input** (Entrada): utilice esta pestaña para añadir o modificar las entradas del dispositivo.
   - **Output** (Salida): utilice esta pestaña para añadir o modificar las salidas del dispositivo.

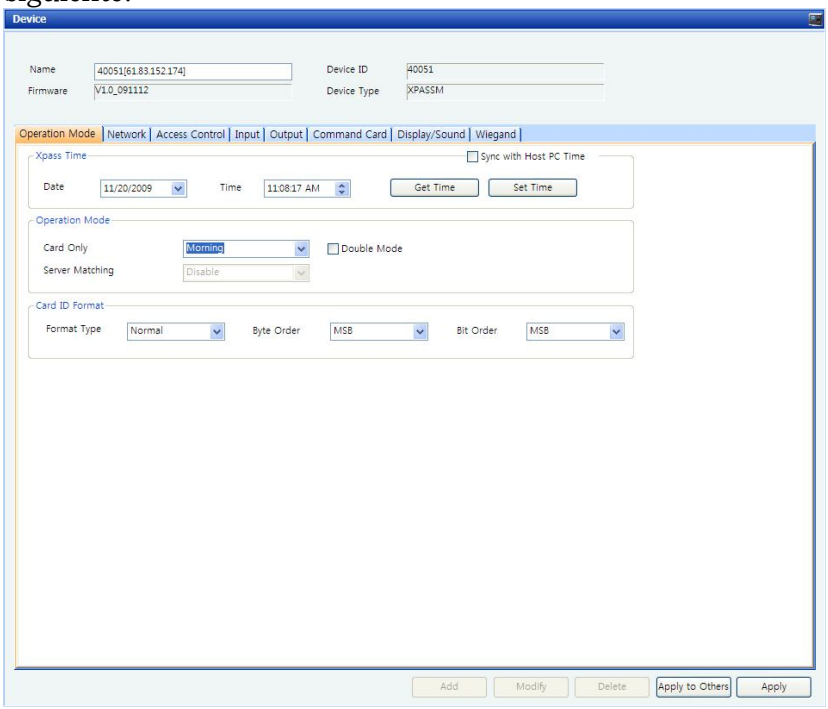
- **Black List** (Lista negra): utilice esta pestaña para deshabilitar el acceso de tarjetas MIFARE en los dispositivos BioLite Net Mifare.
- **Display/Sound** (Pantalla/Sonido): utilice esta pestaña para configurar los parámetros del LED y del zumbido de acuerdo con el evento o estado.
- **T&A** (Tiempo y asistencia): utilice esta pestaña para configurar los parámetros de tiempo y asistencia.
- **Wiegand**: utilice esta pestaña para configurar el formato Wiegand. Para obtener más información acerca de los formatos Wiegand, consulte la sección 3.2.9.

4. Cuando finalice de configurar el dispositivo, haga click en **Apply** (Aplicar) para guardar los cambios.
5. Para aplicar la misma configuración a otros dispositivos, haga click en **Apply to Others** (Aplicar a otros), seleccione los otros dispositivos en la ventana Device Tree (Árbol de dispositivos) y haga click en **Apply** (Aplicar).

3.2.7 Configuración de un dispositivo Xpass

Para configurar un dispositivo Xpass:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. Haga doble click en el nombre de un dispositivo en el panel de navegación. Esta acción abrirá un panel, llamado Device (Dispositivo), parecido al siguiente:



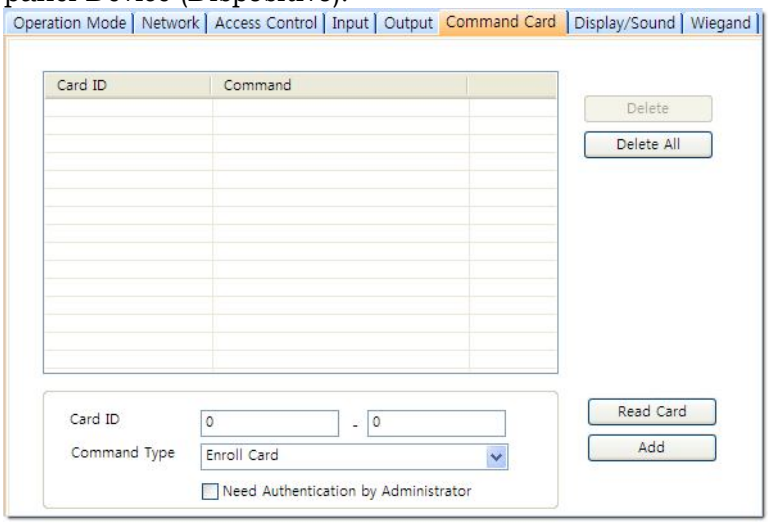
3. Configure la información del dispositivo en las siguientes pestañas. Para una explicación de la configuración del dispositivo, consulte la sección 5.1.4.
   - **Operation mode** (Modo de funcionamiento): utilice esta pestaña para establecer la hora del dispositivo o para obtenerla de una computadora central, ajuste la configuración para los modos de funcionamiento y ajuste los parámetros para los formatos de las Id. de las tarjetas (Card ID).
   - **Network** (Red): utilice esta pestaña para especificar la configuración de las conexiones en red LAN o en serie.
   - **Access Control** (Control de acceso): utilice esta pestaña para especificar los límites de entrada y los grupos de acceso.
   - **Input** (Entrada): utilice esta pestaña para añadir o modificar las entradas del dispositivo.
   - **Output** (Salida): utilice esta pestaña para añadir o modificar las salidas del dispositivo.
   - **Command Card** (Tarjeta de comando): utilice esta pestaña para expedir tarjetas de comando que puedan controlar dispositivos Xpass. Para obtener más información acerca de cómo expedir tarjetas de comando, consulte la sección 3.2.7.1.
   - **Display/Sound** (Pantalla/Sonido): utilice esta pestaña para configurar los parámetros del LED y del zumbido de acuerdo con el evento o estado.
   - **Wiegand**: utilice esta pestaña para configurar el formato Wiegand. Para obtener más información acerca de los formatos Wiegand, consulte la sección 3.2.9.
4. Cuando finalice de configurar el dispositivo, haga click en **Apply** (Aplicar) para guardar los cambios.
5. Para aplicar la misma configuración a otros dispositivos, haga click en **Apply to Others** (Aplicar a otros), seleccione los otros dispositivos en la ventana Device Tree (Árbol de dispositivos) y haga click en **Apply** (Aplicar).

3.2.7.1 Expedición de tarjetas de comando

Las tarjetas de comando permiten registrar y eliminar usuarios directamente desde un dispositivo Xpass. Para obtener más información acerca de cómo registrar usuarios utilizando tarjetas de comando, consulte la sección 3.5.2.3. Para obtener más información acerca de cómo eliminar un solo usuario o todos los usuarios utilizando tarjetas de comando, consulte las secciones 4.5.1.1 y 4.5.1.2. Para expedir tarjetas de comando:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.

2. En el panel de navegación, haga click en el nombre de un dispositivo Xpass.
3. Haga click en la pestaña Command Card (Tarjeta de comando), en el panel Device (Dispositivo).

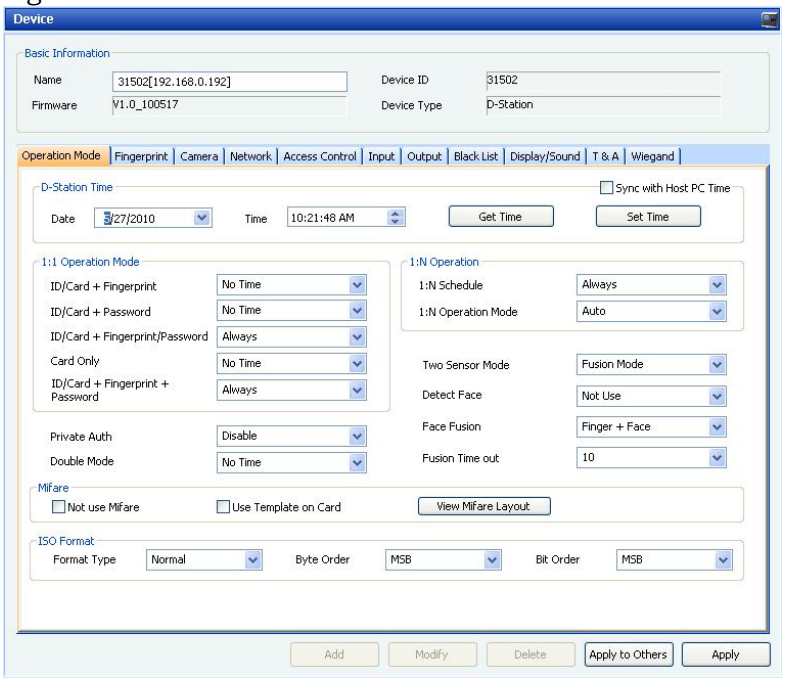


4. Haga click en **Read Card** (Leer tarjeta).
5. Coloque una tarjeta de comando en el dispositivo.
6. Seleccione un tipo de comando de la lista desplegable.
7. Si lo desea, configure la tarjeta de comando para que solicite la autentificación del administrador haciendo click en la casilla de validación que se encuentra al lado de la opción.
8. Haga click en **Add** (Añadir).

3.2.8 Configuración de un dispositivo D-Station

Para configurar un dispositivo D-Station:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. Haga doble click en el nombre de un dispositivo en el panel de navegación. Esta acción abrirá un panel, llamado Device (Dispositivo), parecido al siguiente:



3. Configure la información del dispositivo en las siguientes pestañas. Para una explicación de la configuración del dispositivo, consulte la sección 5.1.5.
   - **Operation mode** (Modo de funcionamiento): utilice esta pestaña para establecer la hora del dispositivo o para obtenerla de una computadora central y ajuste la configuración para los modos de funcionamiento.
   - **Fingerprint** (Huella dactilar): utilice esta pestaña para especificar la configuración de seguridad, calidad, identificación y tiempo de espera agotado para el reconocimiento de las huellas dactilares.
   - **Camera** (Cámara): utilice esta pestaña para asignar eventos, por zona horaria, que se pueden realizar a través de la cámara y la función de reconocimiento facial.
   - **Network** (Red): utilice esta pestaña para especificar la configuración de las conexiones en red LAN o en serie.
   - **Access Control** (Control de acceso): utilice esta pestaña para especificar los límites de entrada y los grupos de acceso predeterminados de un dispositivo.

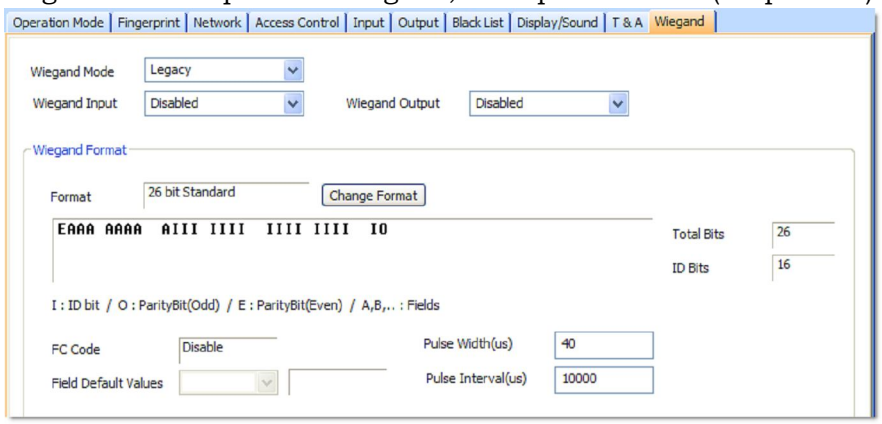
- **Input** (Entrada): utilice esta pestaña para añadir, modificar o eliminar la configuración de entrada del dispositivo.
- **Output** (Salida): utilice esta pestaña para añadir, modificar o eliminar la configuración de salida del dispositivo.
- **Black List** (Lista negra): utilice esta pestaña para deshabilitar el acceso de tarjetas MIFARE en los dispositivos D-Station.
- **Display/Sound** (Pantalla/Sonido): utilice esta pestaña para ajustar la configuración de la pantalla o del sonido y añada imágenes de fondo y sonidos.
- **T&A** (Tiempo y asistencia): utilice esta pestaña para configurar los parámetros de tiempo y asistencia.
- **Wiegand**: utilice esta pestaña para configurar el formato Wiegand. Para obtener más información acerca de los formatos Wiegand, consulte la sección 3.2.9.

4. Cuando finalice de configurar el dispositivo, haga click en **Apply** (Aplicar) para guardar los cambios.
5. Para aplicar la misma configuración a otros dispositivos, haga click en **Apply to Others** (Aplicar a otros) y seleccione los otros dispositivos en la ventana Device Tree (Árbol de dispositivos).

3.2.9 Cambio de los formatos Wiegand

En la interfaz de BioStar, puede configurar el formato Wiegand de un dispositivo para controlar las entradas y las salidas del dispositivo. Para configurar el formato Wiegand:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un dispositivo.
3. Haga click en la pestaña Wiegand, en el panel Device (Dispositivo).



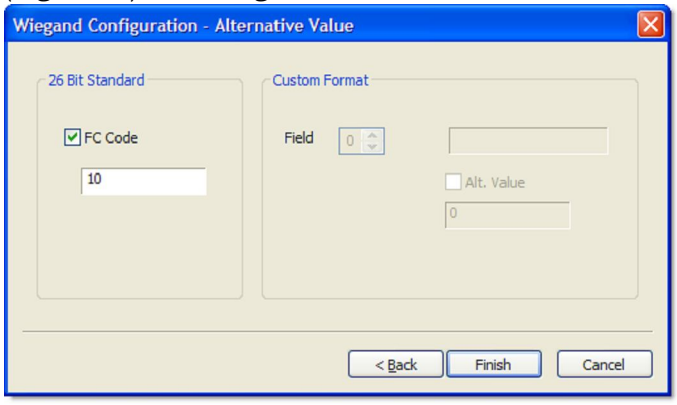
4. Haga click en **Change Format** (Cambiar formato). Esta acción abrirá el asistente de configuración Wiegand (Wiegand Configuration).

5. Haga click en un botón de radio para seleccionar uno de los siguientes formatos:
   - **26-bit Standard** (Estándar de 26 bits): este formato es el más común y consiste en un código FC de 8 bits y una Id. de 16 bits. No es posible cambiar la definición de bit del formato ni los bits de paridad de este formato.
   - **Pass-through** (Transferencia): utilice este formato para personalizar únicamente los bits de Id. Durante el proceso de verificación, si se reconoce el id., la cadena de entrada Wiegand pasará en su forma original. No es posible configurar los bits de paridad o los valores alternativos de este formato. En sí, el formato de transferencia se utiliza sólo cuando el modo de funcionamiento se configura como "uno a uno" (1:1). En el modo "uno a muchos" (1:N), los bits de no-Id. se establecen a 0.
   - **Custom** (Personalizar): con un formato personalizado, puede definir bits de Id., bits de paridad y valores alternativos. Durante el proceso de verificación, el dispositivo comprobará primero la paridad de una cadena de entrada. Si la paridad es correcta, el dispositivo comprobará el id. El dispositivo enviará una cadena de salida, que también se puede cambiar para que sea diferente a la cadena de entrada, únicamente cuando se complete todo el proceso de verificación.
6. Utilice el asistente de configuración Wiegand para personalizar el formato Wiegand de forma que se adapte a sus especificaciones (consulte las subsecciones siguientes para obtener más información).
7. Cuando haya terminado de realizar cambios con el asistente, haga click en **Apply** (Aplicar) para guardar los cambios.

3.2.9.1 Configuración de un formato Wiegand de 26 bits

Cuando selecciona un formato de 26 bits, lo único que se puede personalizar es el código FC:

1. Después de seleccionar el formato en el asistente, haga click en **Next** (Siguiente) hasta llegar a la ventana Alternative Value (Valor alternativo).

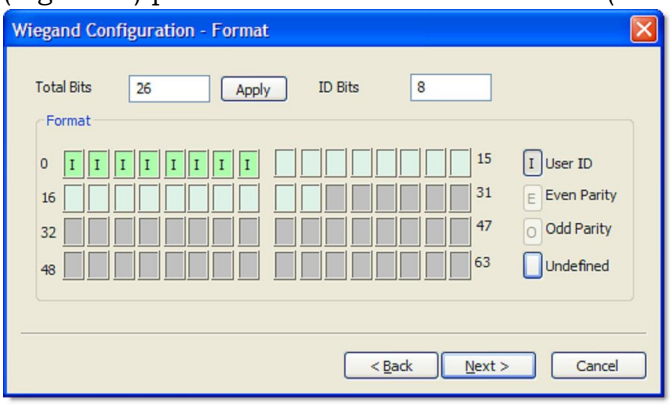


2. Haga click en la casilla de validación FC Code (Código FC) e introduzca un nuevo código FC.
3. Haga click en **Finish** (Finalizar) para cerrar el asistente.

3.2.9.2 Configuración de un formato Wiegand de transferencia

Cuando selecciona un formato de transferencia, puede alterar el número total de bits y asignar bits de Id.:

1. Después de seleccionar el formato en el asistente, haga click en **Next** (Siguiente) para avanzar a la ventana Format (Formato).

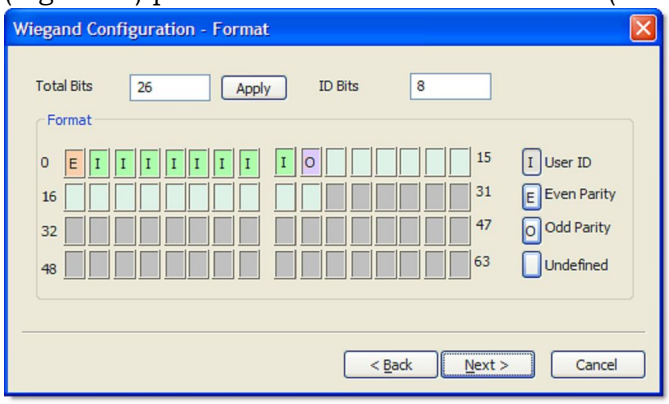


2. Si lo desea, introduzca un nuevo número total de bits y haga click en **Apply** (Aplicar).
3. Haga click en el botón (I) User ID (Id. de usuario) que se encuentra a la derecha.
4. Asigne bits de Id. haciendo click en los cuadrados correspondientes.
5. Haga click en Next (Siguiente) hasta llegar a la ventana Alternative Value (Valor alternativo).
6. Haga click en **Finish** (Finalizar) para cerrar el asistente.

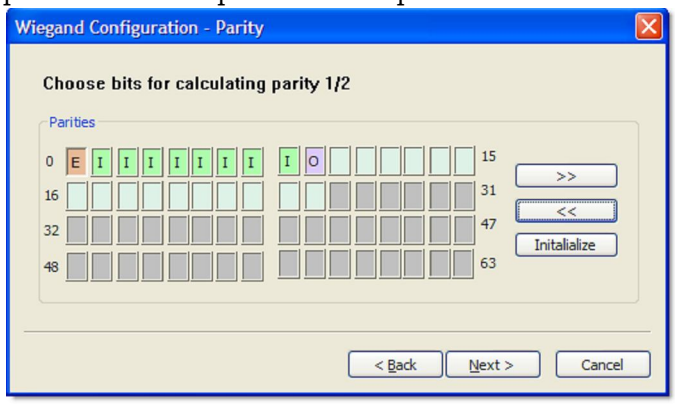
3.2.9.3 Configuración de un formato Wiegand personalizado

Cuando selecciona un formato personalizado, es posible personalizar el número total de bits, asignar bits de Id., definir bits de paridad y configurar valores alternativos para la cadena de salida.

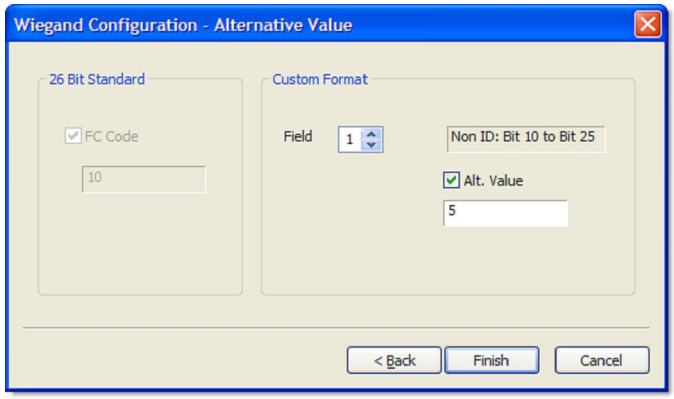
1. Después de seleccionar el formato en el asistente, haga click en **Next** (Siguiente) para avanzar a la ventana Format (Formato).



2. Si lo desea, introduzca un nuevo número total de bits y haga click en **Apply** (Aplicar).
3. Haga click en el botón (I) User ID (Id. de usuario) que se encuentra a la derecha y asigne bits de Id. haciendo click en los cuadrados correspondientes.
4. Haga click en el botón (E) Even Parity (Incluso paridad) que se encuentra a la derecha y asigne un bit de paridad haciendo click en los cuadrados correspondientes.
5. Haga click en el botón (O) Odd Parity (Paridad rara) que se encuentra a la derecha y asigne un bit de paridad rara haciendo click en los cuadrados correspondientes.
6. Haga click en **Next** (Siguiente).
7. En la ventana Parity (Paridad), seleccione los bits que se utilizarán para calcular el primer bit de paridad.



8. Haga click tantas veces como sea necesario en **>>** y seleccione los bits que se utilizarán para calcular bits de paridad adicionales. Debe repetir este paso para cada bit de paridad que usted asignó en los pasos 4 y 5. Si es necesario, puede hacer click en **Initialize** (Inicializar) para reiniciar la selección.
10. Haga click en **Next** (Siguiente).
11. En la ventana Alternative Value (Valor alternativo), seleccione el campo que desea personalizar (sólo bits de no-Id.).



11. Haga click en la casilla de validación Alt Value (Valor alternativo) e introduzca un nuevo valor para la cadena de salida.
12. Repita los pasos 10 y 11 tantas veces como sea necesario para personalizar el resto de la cadena de salida.
13. Haga click en **Finish** (Finalizar) para cerrar el asistente.

3.3 Configuración de puertas

Esta sección describe cómo configurar las puertas en el sistema BioStar. Para obtener más información acerca de cómo instalar dispositivos físicos e integrarlos en los componentes de la puerta, consulte la guía de usuario del dispositivo.

3.3.1 Adición de una puerta

Para añadir una puerta:

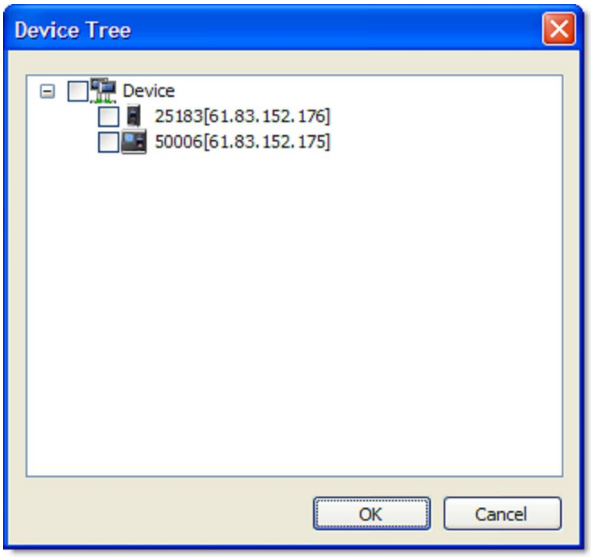
1. Haga click en **Doors** (Puertas) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Add New Door* (Añadir nueva puerta).
3. Haga click con el botón secundario del ratón en *New Door* (Nueva puerta), haga click en *Rename* (Renombrar) y escriba un nombre para la puerta.

3.3.2 Asociación de un dispositivo a una puerta

BioStar permite asociar un máximo de dos dispositivos a cada puerta. Cuando utilice dos dispositivos en una puerta, los dispositivos deben estar conectados entre sí mediante RS485. Consulte la sección 5.2 para una explicación acerca de cómo configurar puertas.

Para asociar un dispositivo a una puerta:

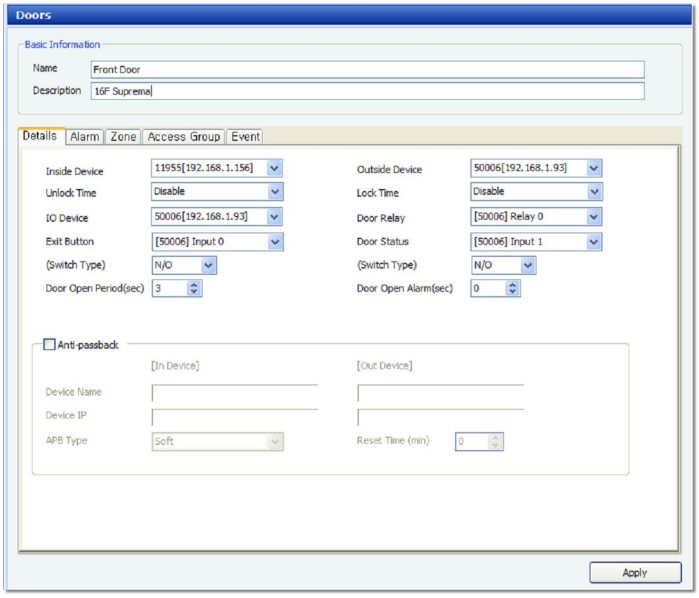
1. Haga click en **Doors** (Puertas) en el panel de acceso directo.
2. Haga click con el botón secundario del ratón y seleccione *Add Device* (Añadir dispositivo).
3. Seleccione un dispositivo de la ventana Device Tree (Árbol de dispositivos) haciendo click en la casilla de validación que se encuentra al lado del nombre del dispositivo.



4. Haga click en **OK** (Aceptar).

3.3.3 Configuración de una puerta

1. Haga click en **Doors** (Puertas) en el panel de acceso directo.
2. Haga click en el nombre de una puerta en el panel de navegación. Esta acción abrirá un panel, llamado Doors (Puertas), parecido al siguiente:



3. Configure la información de la puerta en las siguientes pestañas. Para una explicación de cómo configurar puertas, consulte la sección 5.2.
   - **Details** (Detalles): utilice esta pestaña para controlar la interacción entre puertas, dispositivos, cerraduras y botones de salida. Si añade dos dispositivos a una puerta, también puede utilizar esta pestaña para configurar los parámetros de anti-passback.
   - **Alarm** (Alarma): utilice esta pestaña para especificar qué acciones llevar a cabo cuando la puerta se fuerce o se deje abierta.
   - **Zone** (Zona): utilice esta pestaña para ver las zonas asociadas a una puerta.
   - **Access Control** (Control de acceso): utilice esta pestaña para ver los grupos de acceso asociados a una puerta.
   - **Event** (Evento): utilice esta pestaña para obtener y supervisar un registro de evento para la puerta.
4. Cuando finalice de configurar el dispositivo, haga click en **Apply** (Aplicar) para guardar los cambios.

3.3.4 Creación de un grupo de puertas

Es posible crear grupos de puertas para facilitar la gestión.

1. Haga click en **Doors** (Puertas) en el panel de acceso directo.

2. En el panel navegación, haga click con el botón secundario del ratón en *Doors* (Puertas) y haga click en *Add Door Group* (Añadir grupo de puertas).
3. Escriba el nombre del grupo y pulse Enter.
4. Para añadir una puerta al grupo, seleccione una puerta y arrástrela al grupo.

3.4 Configuración de zonas

BioStar permite proporcionar un control de acceso sofisticado con múltiples zonas. Las zonas se pueden utilizar para controlar el comportamiento de los dispositivos, puertas y otros componentes. Además, las zonas se pueden configurar para proporcionar diferentes tipos de restricciones, tales como anti-passback, anti-passback programado y límites de entrada. Las siguientes secciones describen cómo determinar qué zonas utilizar y cómo añadir y configurar zonas.

3.4.1 Determinación de las zonas que se van a utilizar

El sistema BioStar permite seis tipos de zonas en total:

- **Access zone** (Zona de acceso): utilice esta zona para sincronizar la información de usuario o registro. Si selecciona la opción de sincronización de usuario, los datos de usuario registrados en los dispositivos se propagarán automáticamente al resto de dispositivos conectados. Si selecciona la opción de sincronización de registro, todos los registros se escribirán en el dispositivo maestro (además de en el servidor), de manera que puede comprobar los registros de los dispositivos miembros. Para obtener más información acerca de cómo personalizar zonas de acceso, consulte la sección 5.3.5.
- **Anti-passback zone** (Zona anti-passback): utilice esta zona para evitar que un usuario pase su tarjeta a alguien más o utilice su huella dactilar para permitir que alguien más entre. Esta zona permite dos tipos de restricciones anti-passback: leve y fuerte. Cuando un usuario viola el protocolo anti-passback, la restricción leve registrará la acción en el registro del usuario. La restricción fuerte denegará el acceso y registrará el evento en el registro cuando se viole el protocolo anti-passback. Para obtener más información acerca de cómo personalizar zonas anti-passback, consulte la sección 5.3.1.
- **Entrance limit zone** (Zona límite de entrada): utilice esta zona para restringir el número de veces que un usuario puede entrar en una zona. El límite de entrada se puede asociar a una zona horaria, de manera que un usuario tendrá un número de entradas máximo durante un espacio de tiempo determinado. Es posible configurar también los límites de tiempo de reentrada para reforzar una restricción anti-passback programada. Para obtener más información acerca de cómo personalizar zonas límite de entrada, consulte la sección 5.3.2.

- **Alarm zone** (Zona de alarma): utilice esta zona para agrupar las entradas de varios dispositivos en una única zona de alarma. Los dispositivos en la zona de alarma se pueden armar o desarmar simultáneamente mediante una tarjeta o una clave de arme o desarme. Para obtener más información acerca de cómo configurar zonas de alarma, consulte las secciones 3.4.2.4, 3.4.2.5, 3.4.2.6 y 5.3.3.
- **Fire alarm zone** (Zona de alarma por incendio): utilice esta zona para controlar cómo responderán las puertas en caso de incendio. Se pueden realizar entradas externas en el sistema BioStar para abrir automáticamente las puertas o para realizar otras acciones. Para obtener más información acerca de cómo personalizar zonas de alarma por incendio, consulte la sección 5.3.4.
- **Muster zone** (Zona de reunión): utilice esta zona para supervisar y seguir la trayectoria de los empleados en una situación de emergencia o para pasar lista cuando sea necesario que los empleados se encuentren en un área determinada a una hora determinada. La zona de reunión permite a los administradores determinar si falta algún empleado en ella; y si es así, tomar las acciones necesarias para localizarlo. Para obtener más información acerca de cómo personalizar la zona de reunión, consulte la sección 5.3.6.

3.4.2 Adición y configuración de zonas

Cuando añade una zona, puede utilizar las cuatro pestañas del panel Zone (Zona) para configurar la zona. Para una explicación acerca de cómo configurar zonas, consulte la sección 5.3.

- **Details** (Detalles): añada dispositivos y especifique las entradas u otros parámetros de una zona.
- **Alarm** (Alarma): especifique acciones y salidas de alarma.
- **Access Group** (Grupo de acceso): aplique grupos de acceso a una zona (no disponible para zonas de alarma por incendio).
- **Event** (Evento): visualice eventos asociados a una zona.

3.4.2.1 Adición de una zona

Para añadir una zona nueva:

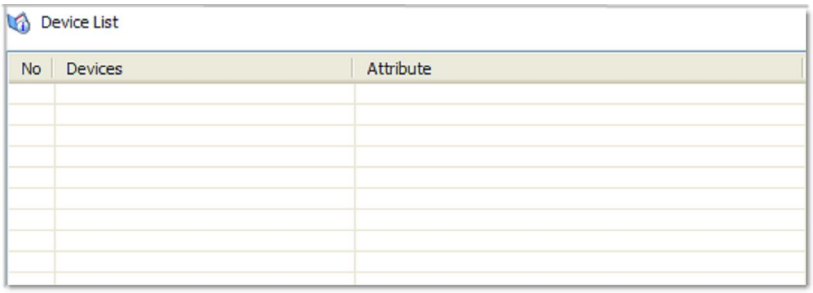
1. Haga click en **Doors** (Puertas) en el panel de acceso directo.
2. En el panel de navegación, haga click con el botón secundario del ratón en *Zone* (Zona).
3. Haga click en *Add Zone* (Añadir zona).
4. Escriba un nombre para la zona en el campo Name (Nombre).
5. Seleccione un tipo de zona de la lista desplegable (consulte la sección 3.4.1 para obtener información acerca de las descripciones de zona).

6. Pulse **OK** (Aceptar).

Aparecerá el panel Zone (Zona) en la parte derecha de la ventana.

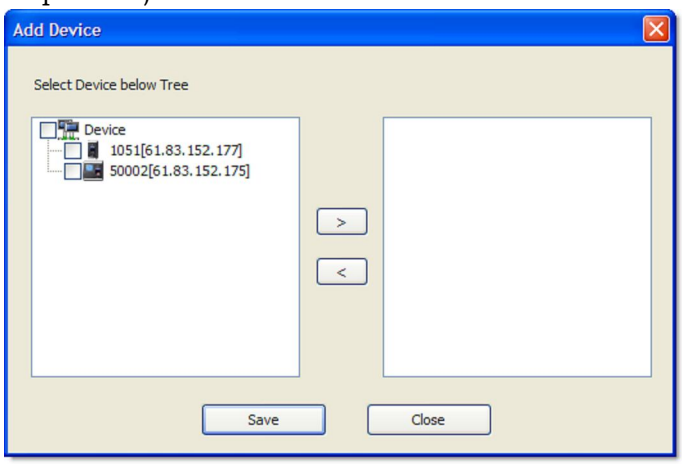
3.4.2.2 Adición de un dispositivo a una zona

Para implementar los protocolos de una zona, debe asociar dispositivos a la zona. La pestaña Details (Detalles), en el panel Zone (Zona), contiene una lista de dispositivos (Device List) que muestra todos los dispositivos asociados a una zona (consulte más adelante).



Para añadir un dispositivo a una zona:

1. Haga click en **Doors** (Puertas) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de una zona.
3. En la pestaña Zone (Zona), en la parte inferior de la lista de dispositivos (Device List), haga click en **Add Device** (Añadir dispositivo). Esta acción abrirá la ventana Add Device (Añadir dispositivo).



4. Seleccione un dispositivo (o varios dispositivos) de la lista y haga click en >.
   - **Anti-passback zones** (Zonas anti-passback): cuando aparezca la ventana Select Zone Attribute (Seleccione el atributo de zona), seleccione un atributo de la lista desplegable (*In Device* (Dispositivo de entrada) o *Out Device* (Dispositivo de salida)).

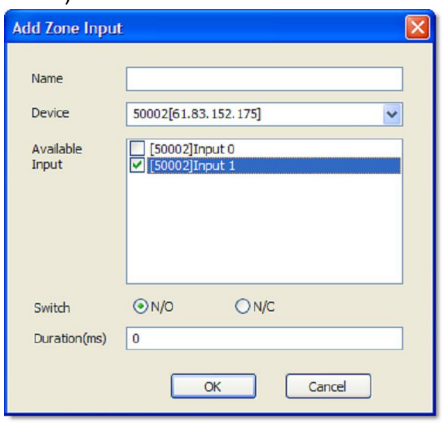
- **Alarm zones** (Zonas de alarma): cuando aparezca la ventana Select Zone Attribute/Type (Seleccione el atributo o tipo de zona), seleccione un atributo para el dispositivo de la lista desplegable (*General*, *Arm* (Armar), *Disarm* (Desarmar), o *Arm/Disarm* (Armar/Desarmar)). Si selecciona el atributo Arm (Armar) o Disarm (Desarmar) (o *Arm/Disarm* (Armar/Desarmar)), haga click en el botón de radio *Card* (Tarjeta) o *Key* (Clave) para especificar cómo armar o desarmar zonas; después pulse **OK** (Aceptar). Para obtener más información acerca de cómo armar o desarmar zonas, consulte la sección 3.4.2.5.

5. Pulse **Save** (Guardar) para añadir los dispositivos a la lista.

3.4.2.3 Configuración de entradas de zona

Cuando añada dispositivos a una zona de alarma, o a una zona de alarma por incendio, también es necesario configurar las entradas de zona. Para configurar entradas:

1. Haga click en **Doors** (Puertas) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de una zona.
3. En la pestaña Zone (Zona), en la parte inferior de la lista de dispositivos (Device List), haga click en **Add Input** (Añadir entrada). Esta acción abrirá la ventana Add Zone Inputs (Añadir entradas de zona).



4. Escriba un nombre para la entrada en el campo Name (Nombre).
5. Seleccione un dispositivo de la lista desplegable.
6. Seleccione una de las entradas disponibles haciendo click en la casilla de validación que se encuentra al lado de la entrada correspondiente.
7. Seleccione la posición normal de la entrada (*N/O: normalmente abierta* o *N/C: normalmente cerrada*).
8. Configure la duración (en milisegundos) de la señal de entrada.

10. Haga click en **OK** (Aceptar) para añadir la entrada a la lista de entradas.

3.4.2.4 Configuración de acciones y salidas de alarma

Configure acciones de alarma para especificar las alertas que se recibirán, en caso de que se produzcan, y los puertos y relays que se utilizarán para las entradas de alarma. La pestaña Alarm (Alarma), en el panel Zone (Zona), ofrece las siguientes opciones para todas las zonas, excepto para las zonas de acceso. Para obtener más información acerca de las alarmas, consulte las secciones 3.4.2.5 y 3.9.

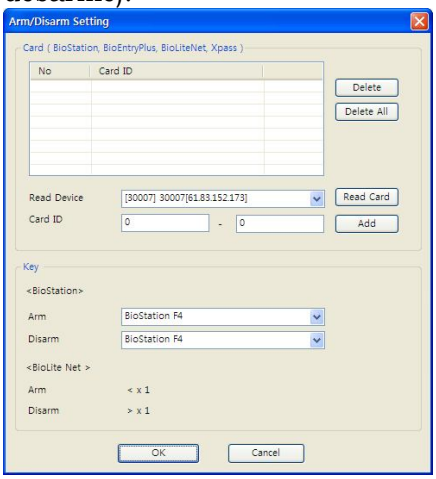
- **Program Sound** (Sonido del programa): configure el sonido que emitirá el software (en la computadora central o en el servidor BioStar). Para añadir sonidos personalizados, consulte la sección 3.9.1.2.
- **Device Sound** (Sonido del dispositivo): configure el sonido que emitirá un dispositivo determinado.
- **Send Email** (Enviar e-mail): cree una alerta de e-mail para enviarla cuando se active una alarma y seleccione los destinatarios o las alertas por e-mail. Para obtener más información acerca de las alertas por e-mail, consulte la sección 3.9.2.
- **Output Device** (Dispositivo de salida): especifique el dispositivo que enviará una señal de alarma a un dispositivo externo como, por ejemplo, una sirena de alarma.
- **Output Port** (Puerto de salida): especifique el puerto que se utilizará para la señal de salida.
- **Output Signal** (Señal de salida): especifique un tipo de señal de salida.

3.4.2.5 Configuración de los parámetros de arme y desarme

Después de añadir una zona de alarma, es posible configurar las acciones que armarán y desarmarán la zona. Para configurar los parámetros de arme y desarme:

1. Haga click en **Doors** (Puertas) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de una zona de alarma. Si es necesario, expanda primero el árbol de zonas.
3. Haga click en la pestaña Details (Detalles), en el panel Zone (Zona).

4. Haga click en la opción **Setup** (Configurar) que se encuentra a la derecha de Arm/Disarm Type (Tipo de arme/desarme). Esta acción abrirá la ventana Arm/Disarm Setting (Configuración de arme y desarme).



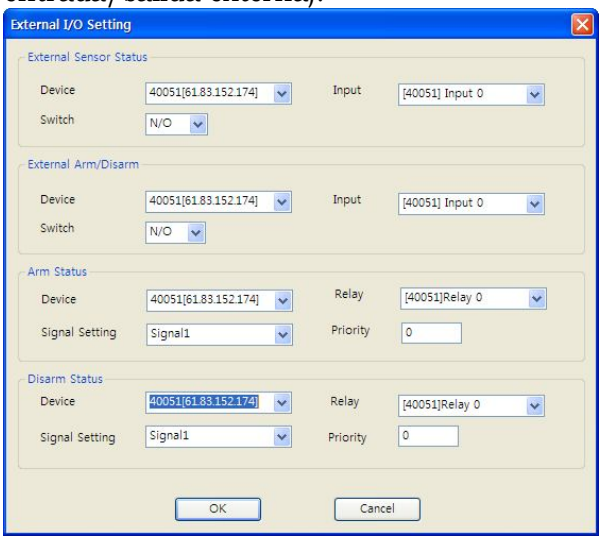
5. Para configurar tarjetas de arme o desarme de zonas:
   a. Seleccione un dispositivo de la lista desplegable Read Device (Leer dispositivo).
   b. Haga click en **Read Card** (Leer tarjeta). El LED del dispositivo que seleccionó comenzará a parpadear.
   c. Coloque la tarjeta en el dispositivo.
   d. Cuando se haya leído la tarjeta, haga click en **Add** (Añadir). La tarjeta se puede utilizar ahora para armar o desarmar dispositivos en la zona de alarma.
6. Para configurar las claves del dispositivo para armar o desarmar zonas (sólo con dispositivos BioStation):
   a. Seleccione de la primera lista desplegable una clave para armar los dispositivos.
   b. Seleccione de la segunda lista desplegable una clave para desarmar los dispositivos.
7. Cuando haya finalizado de configurar los parámetros de arme y desarme, haga click en **OK** (Aceptar).

3.4.2.6 Configuración de parámetros de entrada/salida externa

En lugar de armar o desarmar zonas de alarma manualmente, es posible configurar el sistema BioStar para que decida automáticamente cuándo armar o desarmar zonas basándose en el estado de una entrada determinada. También es posible evitar que el sistema BioStar arme una zona de alarma cuando una entrada supervisada no se encuentre preparada. Por último, es posible configurar el sistema para que envíe una señal determinada a una salida externa al armar o desarmar zonas de alarma. Los parámetros de entrada/salida externa están disponibles para BioStation V1.8, BioEntry Plus V1.4, BioLite Net V1.2, Xpass V1.0, y D-Station V1.0 o superior.

Para configurar parámetros de entrada/salida externa:

1. Haga click en **Doors** (Puertas) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de una zona de alarma. Si es necesario, expanda primero el árbol de zonas.
3. Haga click en la pestaña Details (Detalles), en el panel Zone (Zona).
4. Haga click en la opción **Setup** (Configurar) que se encuentra a la derecha de External Input/Out (Entrada/Salida externa). Esta acción abrirá la ventana External I/O Setting (Configuración de entrada/salida externa).



5. Configure los siguientes parámetros de entrada/salida como desee:
   - Para evitar que el sistema BioStar arme una zona de alarma:
     a. En External Sensor Status (Estado del sensor externo), seleccione un dispositivo de la lista de dispositivos desplegable.
     b. Seleccione una entrada de la lista de entradas desplegable.

c. Seleccione la posición de la entrada (*N/O: normalmente abierta* o *N/C: normalmente cerrada*) que evitará que el sistema arme la zona de alarma.

- Para permitir al sistema BioStar armar o desarmar automáticamente una zona de alarma:
  a. En External Arm/Disarm (Arme/desarme externo), seleccione un dispositivo de la lista de dispositivos desplegable.
  b. Seleccione una entrada de la lista de entradas desplegable.
  c. Seleccione la posición de la entrada (*N/O: normalmente abierta* o *N/C: normalmente cerrada*) que permitirá al sistema armar la zona de alarma. La otra posición permitirá al sistema desarmar la zona de alarma.
- Para enviar una señal de arme a un dispositivo externo como, por ejemplo, una señal de alarma:
  a. En Arm Status (Estado de arme), seleccione un dispositivo de la lista de dispositivos desplegable.
  b. Seleccione un relay de la lista de relays desplegable.
  c. Seleccione un tipo de señal de la lista desplegable Signal (Señal).
  d. Especifique un nivel de prioridad en el campo Priority (Prioridad).
- Para enviar una señal de desarme a un dispositivo externo como, por ejemplo, una señal de alarma:
  a. En Disarm Status (Estado de desarme), seleccione un dispositivo de la lista de dispositivos desplegable.
  b. Seleccione un relay de la lista de relays desplegable.
  c. Seleccione un tipo de señal de la lista desplegable Signal (Señal).
  d. Especifique un nivel de prioridad en el campo Priority (Prioridad).

6. Cuando haya finalizado de configurar los parámetros de entrada/salida, haga click en **OK** (Aceptar).

3.4.2.7 Selección de grupos de acceso

La pestaña Access Group (Grupo de acceso), en el panel Zone (Zona), permite especificar grupos de acceso que pueden eludir las restricciones normales establecidas para la zona. Por ejemplo, puede elegir que a un grupo de acceso determinado no le afecten las restricciones de una zona anti-passback. Para zonas de alarma, esta pestaña permite especificar grupos de acceso que pueden armar y desarmar alarmas. Para seleccionar un grupo de acceso, haga click en la casilla de validación que se encuentra junto al nombre de un grupo y luego haga click en **Apply** (Aplicar).

3.4.2.8 Visualización de eventos de zona

La pestaña Event (Evento), en el panel Zone (Zona), proporciona un listado con eventos registrados en una zona determinada. Es posible establecer un rango de fecha con los calendarios desplegables y ver un reporte de los eventos haciendo click en **Get Log** (Obtener registro). Para obtener más información acerca de cómo supervisar y visualizar registros de eventos, consulte la sección 4.1.

3.5 Configuración de usuarios

Necesitará utilizar un escáner de huellas dactilares para capturar cada una de las huellas dactilares de los usuarios. Por este motivo, puede resultar útil instalar una terminal conectada al sistema en un centro de registro como, por ejemplo, en la oficina de recursos humanos o de seguridad. Los dispositivos BioStation, BioEntry Plus, BioLite Net, o D-Station se pueden utilizar como escáneres de huellas dactilares cuando estén conectados en red al servidor BioStar. También se puede conectar el dispositivo BioMini USB a una terminal de usuario BioStar para que funcione como escáner de huellas dactilares en un centro de registro.

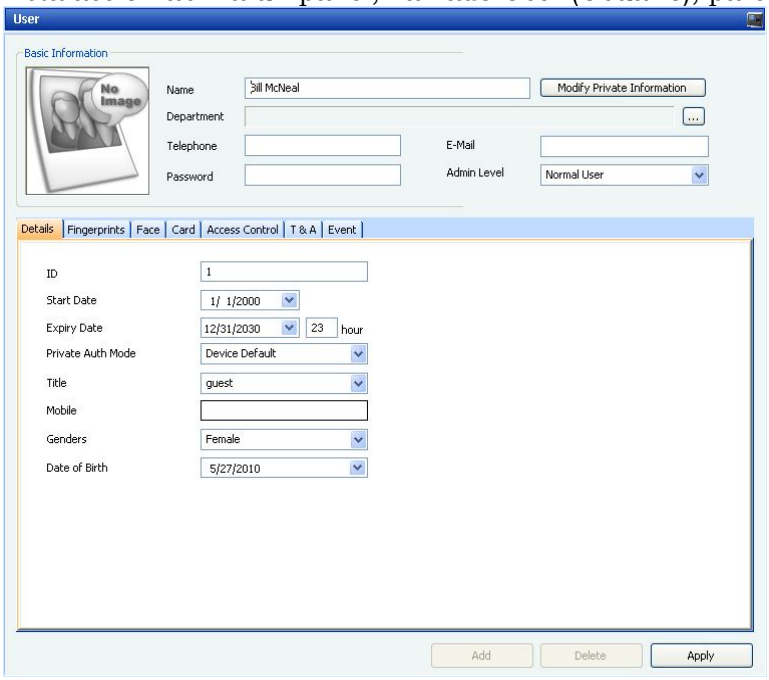
Al añadir usuarios, deberá crear en primer lugar una cuenta de usuario. Una vez que haya creado la cuenta, podrá registrar huellas dactilares y tarjetas de acceso o editar los datos de usuario como desee.

3.5.1 Creación de una cuenta de usuario

Los datos de usuario se controlan a través de una cuenta de usuario. Es posible crear nuevas cuentas para usuarios u obtener datos de usuario desde un dispositivo. Para obtener datos de usuario desde un dispositivo, consulte la sección 3.5.4.3. Para migrar datos de usuario desde una base de datos existente en BioAdmin, consulte la sección 2.4.

Para crear nuevas cuentas de usuario:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel de navegación, haga click con el botón secundario del ratón en *User* (Usuario) o un nombre de área y haga click en*Add User* (Añadir usuario). Esta acción abrirá un panel, llamado User (Usuario), parecido al siguiente:



3. Añada los detalles de la cuenta de usuario en el panel User (Usuario):
   - **Name** (Nombre): introduzca el nombre de usuario.
   - **Department** (Área): introduzca un área o haga click en el botón de elipsis (...) para seleccionar una de las que ya se añadieron en el sistema BioStar.
   - **Telephone** (Teléfono): introduzca el número de teléfono del usuario (sólo números: no se permite ningún caracter en este campo).
   - **E-mail**: introduzca la dirección e-mail del usuario.
   - **Password** (Contraseña): introduzca la contraseña de usuario, si lo desea.
   - **Admin Level** (Nivel de administrador): seleccione el nivel de administrador BioStar del usuario (Normal User (Usuario normal) o Admin User (Usuario administrador).
   - **ID** (Id.): introduzca un número de identificación para el usuario.
   - **Start Date** (Fecha de inicio): establezca una fecha de inicio en la que el usuario obtendrá autorización mediante el sistema BioStar.
   - **Expiry Date** (Fecha de caducidad): establezca la fecha en la que la cuenta del usuario caducará (también puede especificar la hora en la que la cuenta caducará).

- **Title** (Título): seleccione un título para el usuario (Guest (Invitado), President (Presidente), Director, General Manager (Gerente general), Chief (Jefe), Assistant Manager (Subgerente) o un título personalizado).
- **Mobile** (Celular): introduzca un número de celular para el usuario.
- **Genders** (Género): introduzca el género del usuario.
- **Date of Birth** (Fecha de nacimiento): seleccione la fecha de nacimiento en el calendario desplegable.

Nota: se puede añadir una fotografía del usuario o un mensaje privado haciendo click en **Modify Private Information** (Modificar información privada).

4. Registre las huellas dactilares (consulte la sección 3.5.2, las imágenes faciales (consulte la sección 3.5.3) y las tarjetas de acceso (consulte la sección 3.5.4) como sea necesario.
5. Cuando haya terminado de añadir detalles a la cuenta de usuario, haga click en **Apply** (Aplicar).

3.5.2 Registro de huellas dactilares

BioStar proporciona una opción para encriptar plantillas de huellas dactilares. Si elige utilizar esta opción, debería configurar la encriptación *antes* de capturar huellas dactilares. Cualquier plantilla de huellas dactilares capturada anteriormente dejará de ser útil cuando active la encriptación. Para obtener más información acerca de cómo encriptar huellas dactilares, consulte la sección 4.7.

Al registrar huellas dactilares, es importante capturar imágenes de calidad. Antes de registrar huellas dactilares, asegúrese de que los dedos del candidato están limpios y secos. Puede que sea necesario pedirle al candidato que se limpie los dedos justo antes de realizar el registro. Si la piel de un candidato es excesivamente seca, pídale que se humedezca ligeramente la punta de los dedos soplando sobre ellos justo antes de realizar el registro.

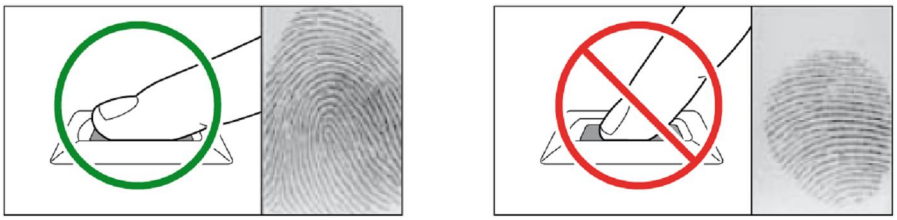
Al registrar huellas dactilares, recuerde los siguientes consejos:

- Debe registrar el mismo dedo dos veces (dos plantillas). Puede registrar hasta dos dedos (un total de cuatro plantillas) por usuario.
- Los dedos con cicatrices, las huellas dactilares maltratadas o con otro tipo de daño físico pueden generar un registro pobre.
- Puede que sea necesario eliminar y volver a capturar una imagen de una huella dactilar si el candidato experimenta tasas de aceptación bajas.

3.5.2.1 Colocación de los dedos en el sensor

Para garantizar huellas dactilares de calidad, los candidatos deben colocar la yema (la parte suave opuesta a la uña) en el sensor y cubrirlo tanto como se pueda. Suprema recomienda utilizar los dedos índice o medio ya que normalmente resultan ser para los usuarios los más fáciles de colocar en el sensor. Para colocar correctamente un dedo en el sensor, los candidatos deben poner la parte de la yema en posición horizontal, de manera que cubra el sensor tanto como sea posible. El dedo debe de estar ligeramente perpendicular en relación con el sensor.

La siguiente imagen ilustra la colocación correcta e incorrecta de un dedo en el sensor.



3.5.2.2 Registro de huellas dactilares

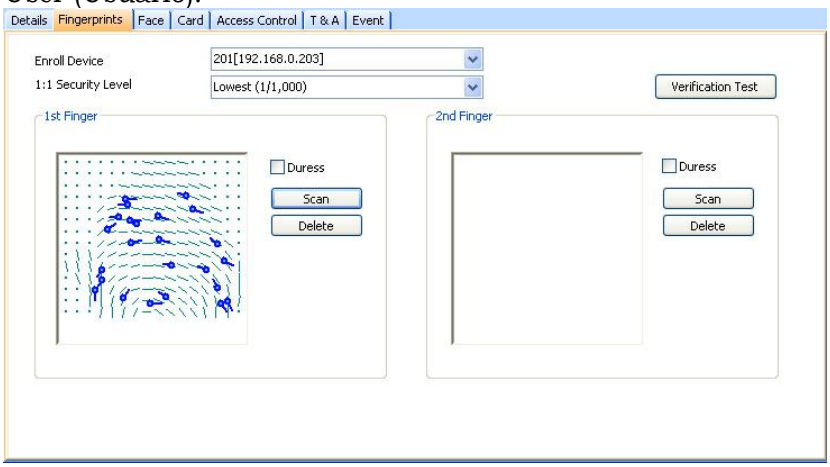
BioStar permite registrar hasta dos huellas dactilares por usuario. Si lo desea, una de las lecturas de la huella dactilar se puede utilizar como señal de peligro ya que activará las alarmas cuando un candidato se vea forzado a acceder a un área. Al registrar huellas dactilares de peligro, recuerde los siguientes consejos:

- Una huella dactilar de peligro no se puede utilizar como método de acceso normal.
- La huella dactilar de peligro debería parecer una elección natural (ej.: el dedo meñique no se elige normalmente y puede que el intruso se dé cuenta de que el candidato está activando una alarma).
- Los candidatos deberían ser educados acerca de lo que sucede cuando se utiliza la huella dactilar de peligro (ej.: la huella dactilar de peligro puede bloquear puertas o activar alarmas silenciosas automáticamente).

Para registrar huellas dactilares:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un usuario.

3. Haga click en la pestaña Fingerprints (Huellas dactilares), en el panel User (Usuario).



4. Seleccione de la lista desplegable Enroll Device (Dispositivo de registro) el dispositivo de registro que se utilizará para escanear las huellas dactilares.
5. Seleccione un nivel de seguridad (Security Level) de la lista desplegable.
6. En el área del primer dedo (1st Finger), pulse **Scan** (Escanear) y luego pida al usuario que coloque el dedo en el escáner dos veces, siguiendo las indicaciones de la interfaz de BioStar.
7. Si lo desea, haga click en la casilla de validación que se encuentra junto a la opción Duress (Peligro) para configurar esta huella dactilar como la señal de peligro.
8. Repita los pasos 5-7 en el área del segundo dedo (2nd Finger) para registrar una segunda huella dactilar.
10. Haga click en **Apply** (Aplicar) para guardar los cambios.

3.5.2.3 Registro de usuarios mediante tarjetas de comando

Después de expedir tarjetas de comando, puede registrar usuarios directamente desde un dispositivo BioEntry Plus o Xpass. Para obtener más información acerca de cómo expedir tarjetas de comando, consulte la sección 3.2.5.1 y 3.2.7.1.

Para registrar un usuario en un dispositivo BioEntry Plus utilizando una tarjeta de comando:

1. Coloque una tarjeta de registro (tarjeta de comando) en un dispositivo BioEntry Plus.
2. Si se necesita autorización, un administrador deberá escanear su huella dactilar para continuar.

3. Para capturar solo huellas dactilares, pida al usuario que coloque el dedo en el escáner dos veces (siguiendo las indicaciones del dispositivo).
4. Para capturar huellas dactilares y expedir una tarjeta de acceso, coloque primero la tarjeta en el dispositivo. Después, pida al usuario que coloque el dedo en el escáner dos veces (siguiendo las indicaciones del dispositivo).

Para registrar un usuario en un dispositivo Xpass utilizando una tarjeta de comando:

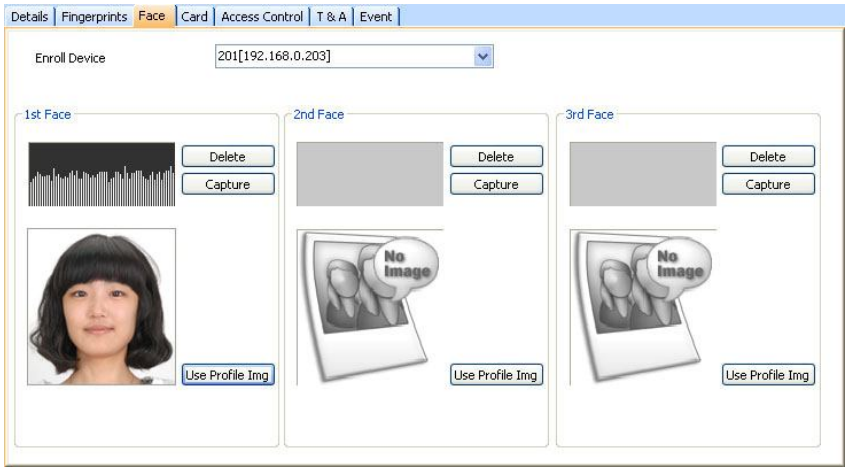
1. Coloque una tarjeta de registro (tarjeta de comando) en un dispositivo Xpass.
2. Si se necesita autorización, un administrador deberá colocar su tarjeta de acceso en el dispositivo para continuar.
3. Coloque la tarjeta de acceso del usuario en el dispositivo.
4. Coloque de nuevo la tarjeta de registro en el dispositivo para confirmar la acción.

3.5.3 Captura de imágenes faciales

Con dispositivos equipados con cámara, tales como D-Station, puede capturar imágenes de los rostros de los usuarios y utilizar esas imágenes para el proceso de autentificación mediante la tecnología de reconocimiento facial de BioStar. BioStar compara una imagen estática del rostro del usuario durante el proceso de autentificación con imágenes de rostros capturados en la base de datos del servidor BioStar. El reconocimiento facial se puede utilizar simultáneamente con el reconocimiento de huellas dactilares para un control de acceso más seguro. Para obtener más información acerca de la configuración del reconocimiento facial, consulte la sección 5.4.3.

Para capturar imágenes faciales:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un usuario.
3. Haga click en la pestaña Face (Rostro), en el panel User (Usuario).



4. Seleccione de la lista desplegable el dispositivo de registro que se utilizará para capturar las imágenes faciales.
5. En el área del primer rostro (1st Face), haga click en **Capture** (Capturar) y pídale al usuario que alinee su rostro con la cámara, siguiendo las indicaciones del dispositivo.
6. Si lo desea, haga click en **Use Profile Img** (Utilizar como imagen de perfil) para asignar la imagen deseada al perfil de usuario en lugar de capturar una nueva imagen.
7. Repita los pasos 5-7 en las áreas del segundo y tercer rostro (2nd Face y 3rd Face, respectivamente) para capturar imágenes faciales adicionales.
8. Haga click en **Apply** (Aplicar) para guardar los cambios.

3.5.4 Expedición de tarjetas de acceso

Suprema fabrica dispositivos de control de acceso que soportan múltiples tipos de tarjetas de acceso: EM4100, proximidad HID y tarjetas MIFARE®. Los dispositivos BioStation, BioEntry Plus y BioLite Net son compatibles con tarjetas EM4100; los dispositivos BioStation Mifare, BioEntry Plus Mifare, BioLite Net y D-Station son compatibles con tarjetas MIFARE; y los dispositivos BioStation HID son compatibles con tarjeta HID de proximidad.

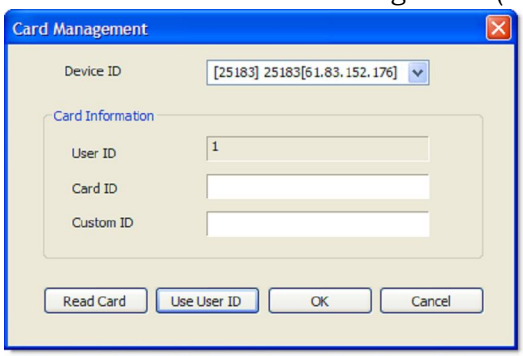
Las tarjetas EM4100 y HID solo necesitan una tarjeta de Id. para completar el proceso de registro, mientras que las tarjetas MIFARE son compatibles con dos modos de funcionamiento: los modos Card Serial Number (CSN) (Número de serie de tarjeta) y Template-on-Card (Tarjeta con plantilla). Al utilizar el modo CSN, es posible leer el número de serie tal y como lo haría para una tarjeta EM4100 o HID. Al utilizar el modo Template-on-Card (Tarjeta con plantilla), debe guardar la información de usuario directamente en la tarjeta, incluyendo las plantillas de huellas dactilares.

Siga los siguientes procedimientos para expedir el tipo de tarjeta adecuado y luego añadirla a la cuenta de usuario.

3.5.4.1 Expedición de tarjetas EM4100

Para registrar una tarjeta de usuario:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un usuario.
3. En el panel User (Usuario), haga click en la pestaña Card (Tarjeta).
4. Seleccione "EM4100" de la lista desplegable Card Type (Tipo de tarjeta).
5. Haga click en **Card Management** (Gestión de tarjetas). Esta acción abrirá la ventana Card Management (Gestión de tarjetas).



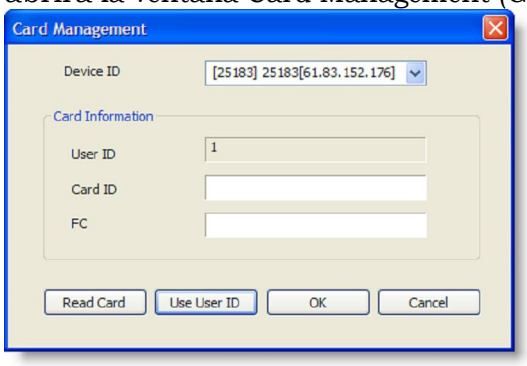
6. Seleccione el id. de un dispositivo de la lista desplegable.
7. Introduzca el id. de una tarjeta (32 bits) y una Id. personalizada (8 bits) ya sea manualmente o mediante la lectura de la tarjeta (también puede hacer click en **Use User ID** (Utilizar Id. de usuario) para insertar el id. de usuario en estos campos):
   - Para introducir los datos manualmente, escriba el id. de la tarjeta y el id. personalizada en los campos correspondientes, haga click en OK (Aceptar) y luego vaya al paso 8.
   - Para leer los datos de la tarjeta, haga click en Read Card (Leer tarjeta) (el LED del dispositivo que seleccionó comenzará a parpadear) y luego coloque la tarjeta en el dispositivo. Cuando se haya leído la tarjeta, haga click en **OK** (Aceptar).
8. Haga click en **Apply** (Aplicar) para guardar la tarjeta en la cuenta del usuario.

3.5.4.2 Expedición de tarjetas de proximidad HID

Para registrar una tarjeta de usuario:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un usuario.
3. En el panel User (Usuario), haga click en la pestaña Card (Tarjeta).
4. Seleccione "HID Prox" de la lista desplegable Card Type (Tipo de tarjeta).

5. Haga click en **Card Management** (Gestión de tarjetas). Esta acción abrirá la ventana Card Management (Gestión de tarjetas).



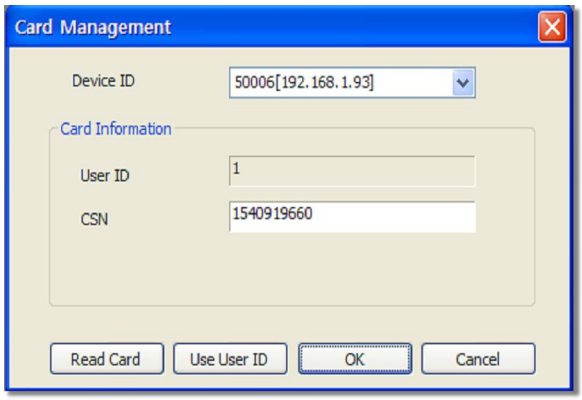
6. Seleccione el id. de un dispositivo de la lista desplegable.
7. Introduzca el id. de una tarjeta y el código de las instalaciones (FC) ya sea manualmente o mediante la lectura de la tarjeta (también puede hacer click en **Use User ID** (Utilizar Id. de usuario) para insertar el id. de usuario en estos campos):
   - Para introducir los datos manualmente, escriba el id. y el código de las instalaciones en los campos correspondientes, haga click en **OK** (Aceptar) y luego vaya al paso 8.
   - Para leer los datos de la tarjeta, haga click en **Read Card** (Leer tarjeta) (el LED del dispositivo que seleccionó comenzará a parpadear) y luego coloque la tarjeta en el dispositivo. Cuando se haya leído la tarjeta, haga click en **OK** (Aceptar).
8. Haga click en **Apply** (Aplicar) para guardar la tarjeta en la cuenta del usuario.

3.5.4.3 Expedición de tarjetas MIFARE CSN

Las tarjetas MIFARE CSN funcionan de forma parecida a las tarjetas EM4100 y HID, ya que todas ellas almacenan para un usuario un número de serie de tarjeta (CSN) que no se puede editar. Para registrar una tarjeta de usuario:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un usuario.
3. En el panel User (Usuario), haga click en la pestaña Card (Tarjeta).
4. Seleccione "Mifare CSN" de la lista desplegable Card Type (Tipo de tarjeta).

5. Haga click en **Card Management** (Gestión de tarjetas). Esta acción abrirá la ventana Card Management (Gestión de tarjetas).



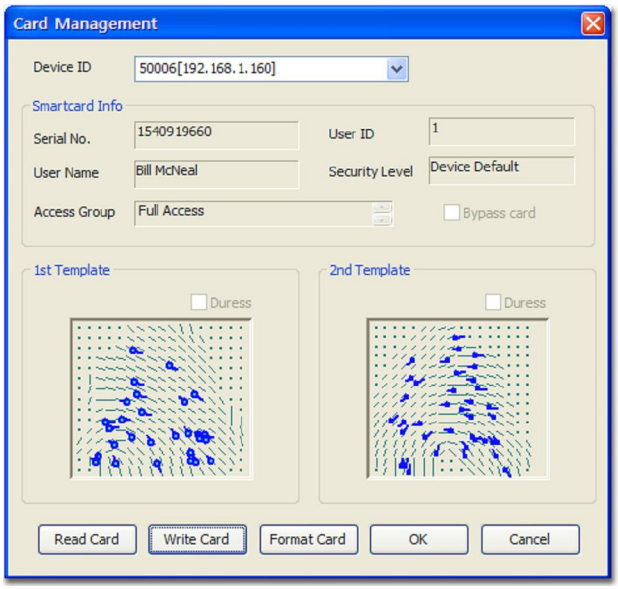
6. Seleccione el Id. de un dispositivo de la lista desplegable.
7. Introduzca el Id. de una tarjeta ya sea manualmente o mediante la lectura de la tarjeta (también puede hacer click en **Use User ID** (Utilizar Id. de usuario) para insertar el Id. de usuario en estos campos):
   - Para introducir los datos manualmente, escriba el Id. y el código de las instalaciones en los campos correspondientes, haga click en **OK** (Aceptar) y luego vaya al paso 8.
   - Para leer los datos de la tarjeta, haga click en Read Card (Leer tarjeta) (el LED del dispositivo que seleccionó comenzará a parpadear) y luego coloque la tarjeta en el dispositivo. Cuando se haya leído la tarjeta, haga click en **OK** (Aceptar).
8. Haga click en **Apply** (Aplicar) para expedir la tarjeta de la cuenta del usuario.

3.5.4.4 Expedición de tarjetas con plantilla MIFARE

Las tarjetas con plantilla MIFARE permiten almacenar información de usuario y plantillas de huellas dactilares directamente en la tarjeta. Para registrar una tarjeta de usuario:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un usuario.
3. En el panel User (Usuario), haga click en la pestaña Card (Tarjeta).
4. Seleccione "Mifare Template" de la lista desplegable.

5. Haga click en **Card Management** (Gestión de tarjetas). Esta acción abrirá la ventana Card Management (Gestión de tarjetas).



6. Seleccione el id. de un dispositivo o un dispositivo USB MIFARE (en caso de que esté conectado) de la lista desplegable.
7. Si lo desea, haga click en Bypass Card (Tarjeta de elusión) para permitir al usuario eludir la autentificación con huella dactilar.
8. Haga click en **Read Card** (Leer tarjeta). El LED del dispositivo que seleccionó comenzará a parpadear.
9. Coloque la tarjeta en el dispositivo.
10. Cuando se haya leído la tarjeta, haga click en **OK** (Aceptar).
11. Haga click en **Apply** (Aplicar) para expedir la tarjeta de la cuenta del usuario.

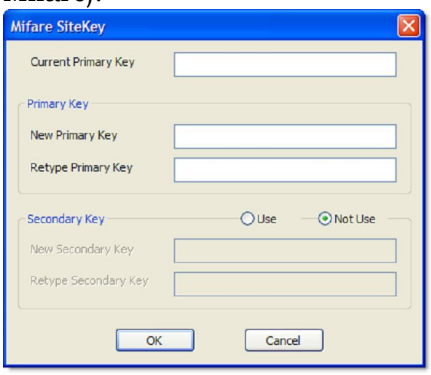
3.5.4.5 Cambio de la clave de sitio MIFARE

La encriptación de datos en las tarjetas MIFARE está determinada por una clave de sitio de 48 bits. Los dispositivos conectados solo pueden leer aquellas tarjetas con las claves de sitio adecuadas. BioStar permite definir hasta dos claves de sitio MIFARE (primaria y secundaria), de manera que puede cambiar la clave de sitio para tarjetas ya existentes.

Nota: las claves de sitio se deben guardar en un lugar seguro. Si se revela la clave del sitio, el sistema de seguridad podrá eludirse.

Para cambiar la clave de sitio MIFARE:

1. En la barra de menú, haga click en **Option > Mifare Card > Mifare Sitekey**. Esta acción abrirá la ventana Mifare Sitekey (Clave de sitio Mifare).



2. Introduzca una nueva clave primaria en el campo *New Primary Key* (Nueva clave primaria).
3. Introduzca de nuevo la clave en el campo *Retype Primary Key* (Vuelva a escribir la clave primaria).
4. Haga click en el botón de radio *Use* (Utilizar) para activar la función de clave secundaria. Esto permite leer las tarjetas con la clave de sitio antigua y reescribirlas con la nueva clave:
   a. Introduzca la antigua clave de sitio en el campo *New Secondary Key* (Nueva clave secundaria).
   b. Introduzca de nuevo la antigua clave de sitio en el campo *Retype Secondary Key* (Vuelva a escribir la clave secundaria).
5. Cuando haya finalizado de editar la clave de sitio, haga click en **OK** (Aceptar).

Nota: cuando la nueva clave de sitio se haya reescrito en todas las tarjetas, Suprema recomienda desactivar la función de la clave secundaria para evitar que se acceda utilizando tarjetas antiguas.

3.5.4.6 Edición de la distribución MIFARE

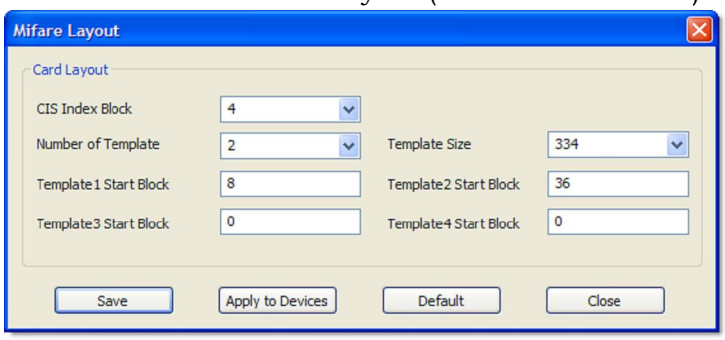
BioStar permite personalizar la distribución MIFARE que se utiliza para registrar la información de usuario y las plantillas de las huellas dactilares. Esta distribución se aplicará a todas las nuevas tarjetas MIFARE que se expidan en los dispositivos determinados (dispositivos BioStation Mifare, BioEntry Plus Mifare, BioLite Net o D-Station).

Las tarjetas MIFARE de 1 K se organizan en 16 sectores con 4 bloques de 16 bits cada uno. Las tarjetas MIFARE de 4 K se organizan en 32 sectores con 4 bloques y 8 sectores con 16 bloques. Las siguientes restricciones se aplican en la distribución MIFARE:

- El primer sector (del bloque 0 al bloque 3) está reservado y no se puede utilizar para almacenar otros datos.
- El último bloque de cada sector (bloques 3, 7, 11, etc.) está reservado para almacenar información de la clave de sitio.
- El sector de información de la tarjeta (CIS, por sus siglas en inglés) ocupa tres bloques contiguos y debería comenzar en el primer bloque disponible de un sector (bloques 4,8,12, etc.).
- Los datos de cada una de las plantillas no deberían solaparse.

Para editar la distribución MIFARE:

1. En la barra de menú, haga click en **Option > Mifare Card > Mifare Layout** (Opción > Tarjeta Mifare > Distribución Mifare). Esta acción abrirá la ventana Mifare Layout (Distribución Mifare).



2. Utilice las listas desplegables y los campos de entrada para configurar los siguientes parámetros de la distribución MIFARE:
   - **CIS Index Block** (Bloque de índices CIS): seleccione el índice de bloques que se utilizará para la información del encabezado (4, 8, 12, o 16).
   - **Number of Templates** (Número de plantillas): seleccione el número de plantillas que se incluirán en la distribución (de 0 a 4).
   - **Template Size** (Tamaño de plantilla): seleccione el número de bytes que se utilizarán en la plantilla. El tamaño predeterminado es de 334 bytes.
   - **Template 1-4 Start Block** (Bloque de inicio de la plantilla 1-4): introduzca el bloque de inicio para las plantillas de las huellas dactilares.
3. Para utilizar la distribución personalizada, haga click en **Apply to Devices** (Aplicar en dispositivo) y seleccione el número adecuado de dispositivos en la ventana Device Tree (Árbol de dispositivos).
4. Para guardar los cambios, haga click en **Save** (Guardar).

Nota: para reiniciar cualquier cambio que haya realizado, haga click en **Default** (Predeterminado). Para salir de la ventana sin guardar los cambios, haga click en **Close** (Cerrar).

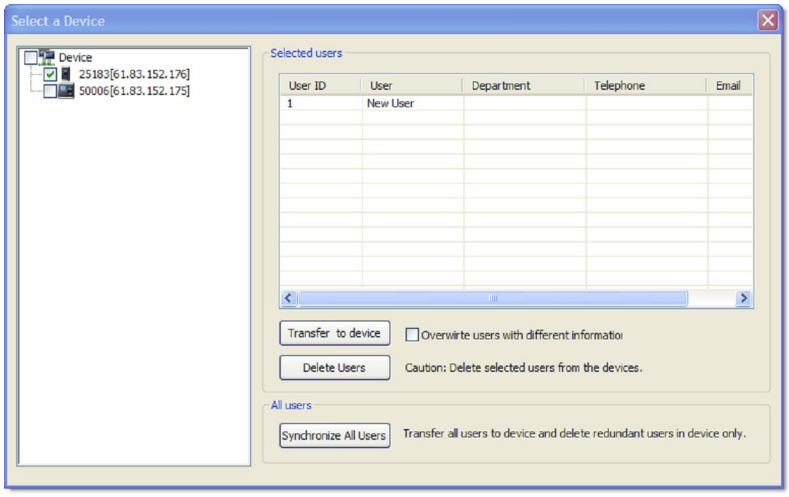
3.5.5 Transferencia de datos de usuario

BioStar permite transferir información de usuario automáticamente a dispositivos, seleccionando la opción "Auto" en la barra de menú (**Option > User > Transfer Mode > Auto**). Sin embargo, también se puede transferir datos a dispositivos manualmente. Cuando haga esto, puede transferir los usuarios seleccionados a los dispositivos seleccionados, o sincronizar todos los usuarios al mismo tiempo. BioStar también le perite obtener datos de un dispositivo y transferirlos al servidor BioStar.

3.5.5.1 Transferencia de un usuario a un dispositivo

Para transferir un solo usuario o usuarios seleccionados a un dispositivo o dispositivos:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Transfer Users to Device* (Transferir usuarios a dispositivo). Esta acción abrirá la ventana Select a Device (Seleccione un dispositivo).



3. Seleccione un dispositivo o dispositivos de la lista que se encuentra a la izquierda haciendo click en las casillas de validación que se encuentran junto a los nombres de los dispositivos.
4. Haga click en un nombre de usuario (puede dejar presionada la tecla Ctrl para seleccionar varios usuarios).
5. Si lo desea, haga click en la casilla de validación para sobrescribir los usuarios con otra información.
6. Haga click en **Transfer to Device** (Transferir a dispositivo) para enviar la información de usuario a los dispositivos seleccionados.

Nota: también puede eliminar usuarios de los dispositivos en este menú. Esta acción no se podrá deshacer, así que utilice esta función con cuidado. Para eliminar usuarios de un dispositivo, haga click en el nombre de un usuario y luego haga click en **Delete Users** (Eliminar usuarios).

3.5.5.2 Sincronización de todos los usuarios

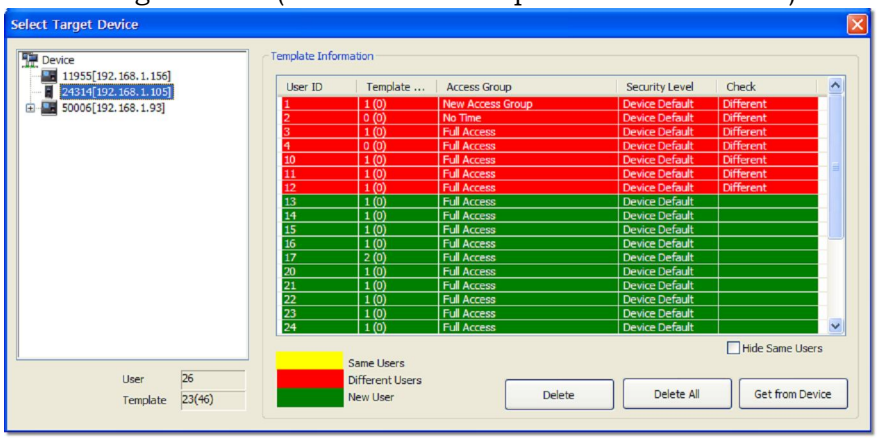
Para sincronizar la información de todos los usuarios entre el servidor BioStar y los dispositivos conectados:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Transfer Users to Device* (Transferir usuarios a dispositivo). Esta acción abrirá la ventana Select a Device (Seleccione un dispositivo) (consulte la sección 3.5.4.1).
3. Seleccione un dispositivo o dispositivos de la lista que se encuentra a la izquierda haciendo click en las casillas de validación que se encuentran junto a los nombres de los dispositivos.
4. Haga click en **Synchronize All Users** (Sincronizar todos los usuarios).

3.5.5.3 Obtención de los datos de usuario de un dispositivo

Para obtener los datos de un dispositivo:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en **Manage Users in Device** (Gestionar usuarios en dispositivo). Esta acción abrirá la ventana Select Target Device (Seleccione un dispositivo determinado).



3. Haga click en el nombre de un dispositivo de la lista de la izquierda para mostrar las plantillas de usuario del dispositivo.
4. Haga click en un usuario de la lista Template Information (Información de plantilla); los nuevos usuarios se resaltarán en amarillo.
5. Haga click en **Get From Device** (Obtener del dispositivo).

Nota: también puede eliminar usuarios de los dispositivos en este menú. Esta acción no se podrá deshacer, así que utilice esta función con cuidado. Para eliminar usuarios desde un dispositivo, haga click en el nombre de un usuario y luego haga click en **Delete** (Eliminar) (o haga click en **Delete All**(Eliminar todos) para eliminar todos los registros de usuarios al mismo tiempo).

Precaución: si existen los mismos usuarios en la base de datos de BioStar cuando se obtienen los datos de usuario de los dispositivos Xpass, los datos se

sobrescribirán sin los datos de huellas dactilares ya que los dispositivos Xpass no almacenan este tipo de datos.

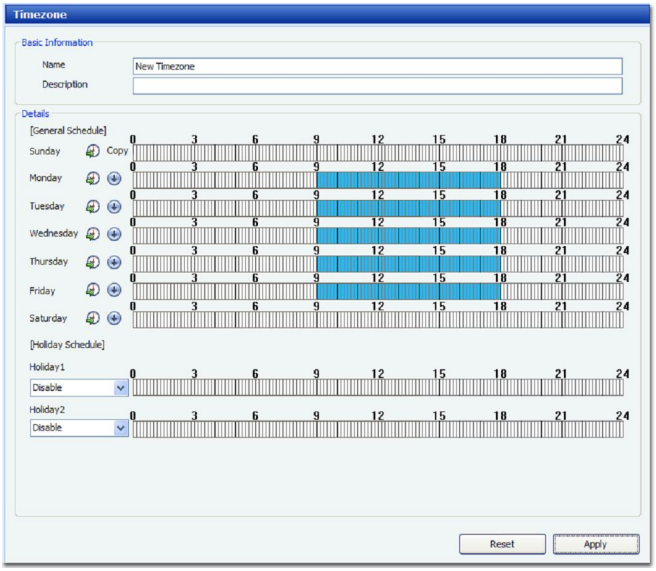
3.6 Configuración de zonas horarias

En el sistema BioStar, las zonas horarias se utilizan para programar permisos y restricciones. Es posible aplicar zonas horarias para restringir las horas en las que un usuario tiene permitido el acceso a una puerta, combinando puertas y zonas horarias en los grupos de acceso (consulte la sección 3.7).

3.6.1 Creación de una zona horaria

Para crear un programa de zonas horarias:

1. Haga click en **Access Control** (Control de acceso) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *New Timezone* (Nueva zona horaria).
3. Introduzca un nombre para la zona horaria.
4. En el panel Timezone (Zona horaria), cree un programa semanal resaltando las horas efectivas de cada día. Puede copiar un programa de un día a otro haciendo click en la flecha que se encuentra a la derecha del día.



5. Si lo desea, puede añadir hasta dos programas vacacionales a la zona horaria. Para crear programas vacacionales, consulte la sección 3.6.2.
6. Cuando haya finalizado de crear la zona horaria, haga click en **Apply** (Aplicar).
7. A continuación, transfiera los datos de la zona horaria a los dispositivos:
   a. En el panel Task (Tarea), haga click en *Transfer to Device* (Transferir a dispositivo). Esta acción abrirá la ventana del árbol de dispositivos.
   b. Seleccione un dispositivo, o dispositivos, haciendo click en las casillas de validación del árbol de dispositivos.

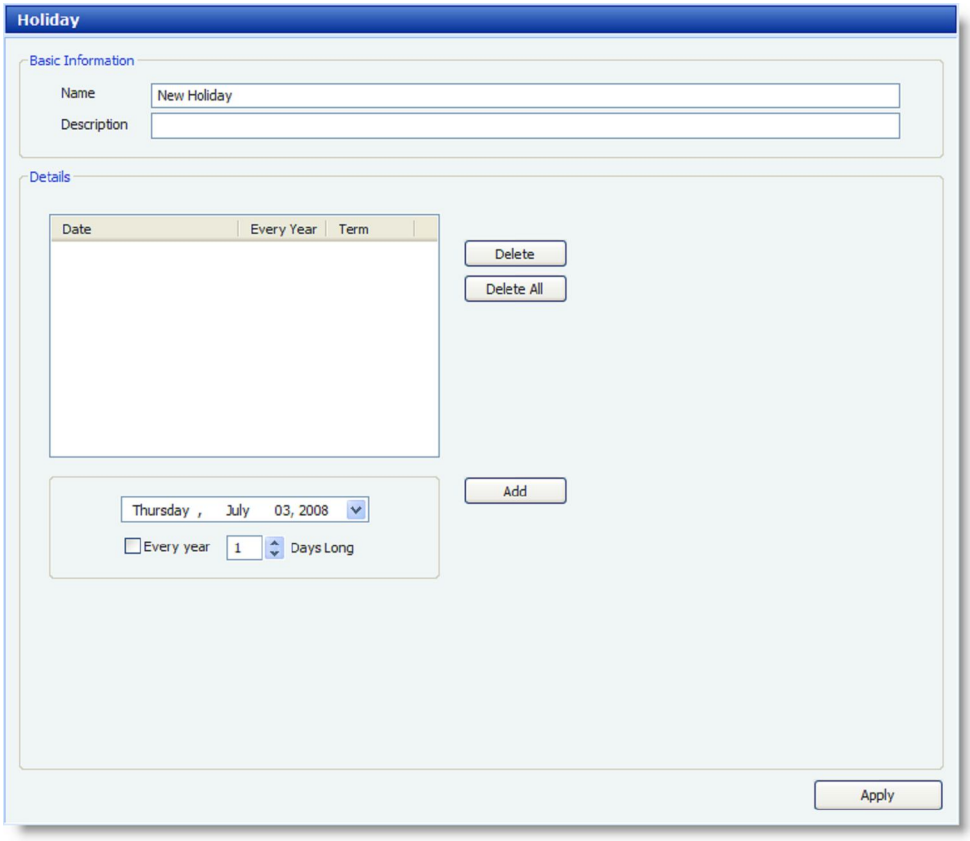
d. Haga click en **OK** (Aceptar).

Ahora es posible combinar la zona horaria con los permisos de una puerta para crear un grupo de acceso (consulte la sección 3.7).

3.6.2 Creación de un programa vacacional

Para crear un programa vacacional:

1. Haga click en **Access Control** (Control de acceso) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *New Holiday* (Nuevo período vacacional).
3. Introduzca un nombre para el período vacacional.
4. En el panel Holiday (Período vacacional), configure la fecha en la que comienza el período vacacional con el calendario desplegable.



5. Si el período vacacional se repite todos los años, haga click en la casilla de validación que se encuentra debajo de la lista desplegable.
6. Configure la duración del período vacacional (en días).
7. Haga click en **Add** (Añadir) para añadir los períodos vacacionales a la lista.
8. Haga click en **Apply** (Aplicar).

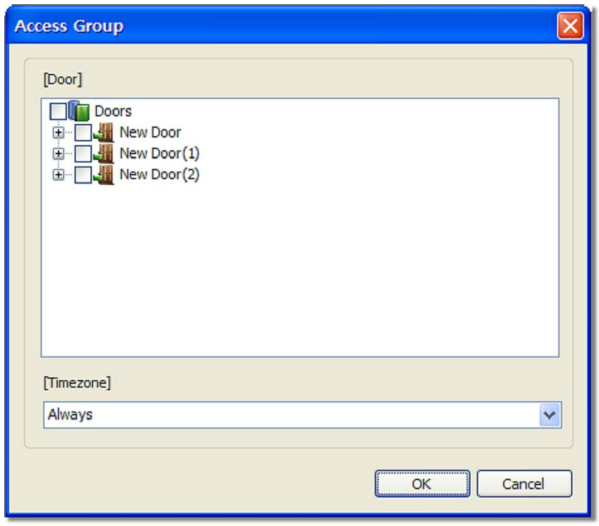
3.7 Configuración de los grupos de acceso

Los grupos de acceso permiten definir los parámetros de los permisos de acceso que pueden incluir puertas, usuarios y zonas horarias. Antes de añadir un grupo de acceso, debe configurar las puertas (consulte la sección 3.3) y las zonas horarias (consulte la sección 3.6). Después de crear los grupos de acceso, debe transferir manualmente los datos a los dispositivos correspondientes (consulte la sección 3.7.4).

3.7.1 Adición de un grupo de acceso

Para añadir un grupo de acceso:

1. Haga click en **Access Control** (Control de acceso) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *New Access Group* (Nuevo grupo de acceso).
3. Escriba un nombre para el nuevo grupo de acceso en el campo que aparece en el panel de navegación y pulse Enter.
4. En la pestaña Access Control (Control de acceso), en el panel Access Group (Grupo de acceso), haga click en **Add** (Añadir). Esta acción abrirá la ventana Access Group (Grupo de acceso).



5. Seleccione las puertas que va a añadir al grupo haciendo click en las casillas de validación que se encuentran al lado de los grupos de puertas o de puertas individuales.
6. Seleccione la zona horaria que se aplicará al grupo de la lista desplegable que se encuentra en la parte inferior de la ventana.
7. Repita los pasos 5 y 6 tantas veces como sea necesario para añadir varios conjuntos de puertas y zonas horarias al grupo de acceso.

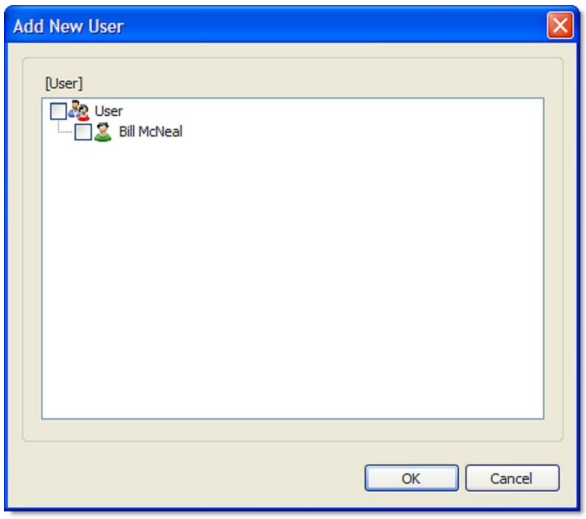
8. Haga click en **OK** (Aceptar) para añadir sus selecciones al grupo.

3.7.2 Adición de usuarios a un grupo de acceso

Después de añadir el grupo de acceso, debe añadir usuarios al grupo. Puede añadir usuarios a los grupos de acceso en la pestaña User (Usuario), tal y como se describe más arriba o asignando grupos de acceso a un usuario en el panel User (Usuario), tal y como se describe en la sección 3.7.3. Puede asignar hasta un máximo de cuatro grupos de acceso.

Para añadir usuarios a los grupos de acceso:

1. Haga click en **Access Control** (Control de acceso) en el panel de acceso directo.
2. En la pestaña User (Usuario), en el panel Access Group (Grupo de acceso), haga click en **Add** (Añadir).
3. En la ventana Add New User (Añadir nuevo usuario), seleccione los usuarios que desea añadir al grupo checando los grupos de usuarios o los usuarios individuales.



4. Haga click en **OK** (Aceptar).

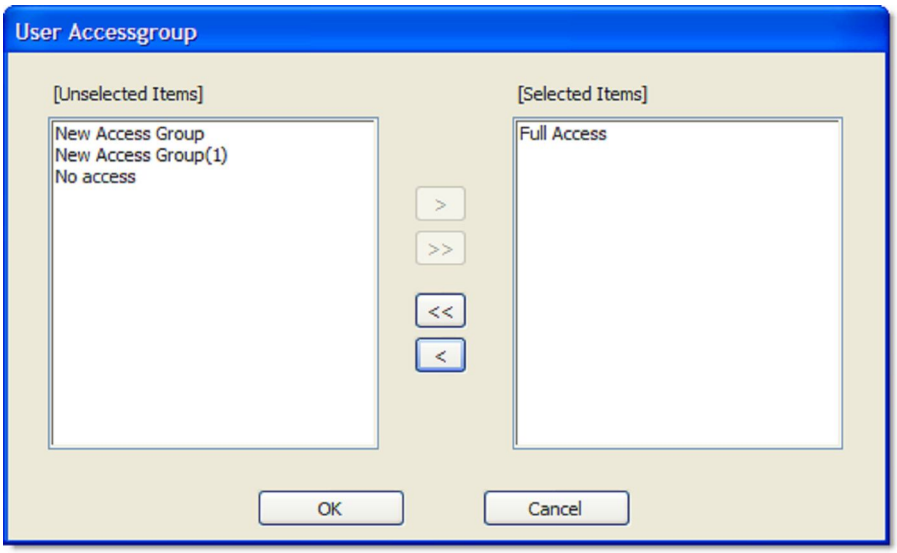
Si ha configurado grupos de usuarios, los usuarios aparecerán en sus grupos respectivos.

3.7.3 Asignación de grupos de acceso a usuarios

También es posible definir los grupos de acceso a los que un usuario pertenecerá (hasta un total de cuatro) en el panel User (Usuario). Para asignar un grupo de acceso a un usuario:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un usuario.

3. Haga click en la pestaña Access Control (Control de acceso), en el panel User (Usuario).
4. Haga click en **Add** (Añadir). Esta acción abrirá la ventana User Access Group (Grupo de acceso de usuario).



5. Haga click en el nombre de un grupo de acceso de la lista que se encuentra a la izquierda y luego haga click en **>**.
6. Repita el paso 5 tantas veces como sea necesario para asignar grupos de acceso adicionales.
7. Cuando haya finalizado de asignar grupos de acceso, haga click en **OK** (Aceptar).

3.7.4 Transferencia de grupos de acceso a dispositivos

Para transferir los datos de un grupo de acceso a los dispositivos:

1. Haga click en **Access Control** (Control de acceso) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Transfer to Device* (Transferir a dispositivo). Esta acción abrirá la ventana del árbol de dispositivos.
3. Seleccione un dispositivo, o dispositivos, haciendo click en las casillas de validación del árbol de dispositivos.
4. Haga click en **OK** (Aceptar).

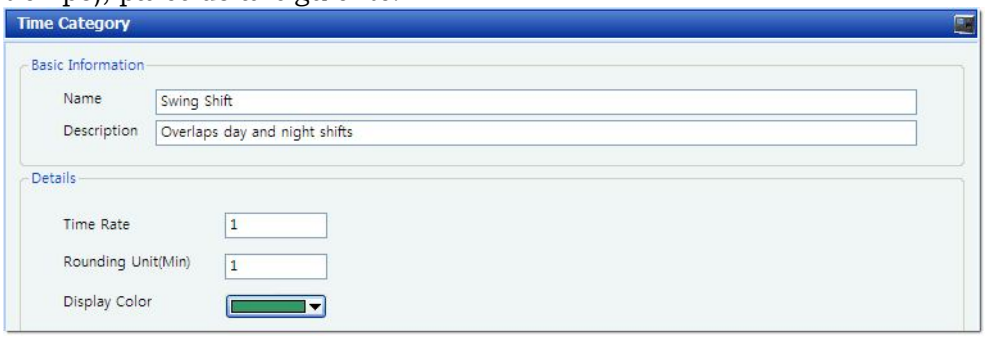
3.8 Configuración de tiempo y asistencia

Las funciones de tiempo y asistencia de BioStar permiten definir categorías de tiempo, turnos y normas vacacionales. Consulte los procedimientos en esta sección así como también los pasos de la sección 3.6.2 para configurar las opciones de tiempo y asistencia.

3.8.1 Adición de una categoría de tiempo

Para añadir una categoría de tiempo:

1. Haga click en la opción **Time and Attendance** (Tiempo y asistencia) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Add Time Category (Añadir categoría de tiempo).* Esta acción abrirá un panel, llamado Time Category (Categoría de tiempo), parecido al siguiente:

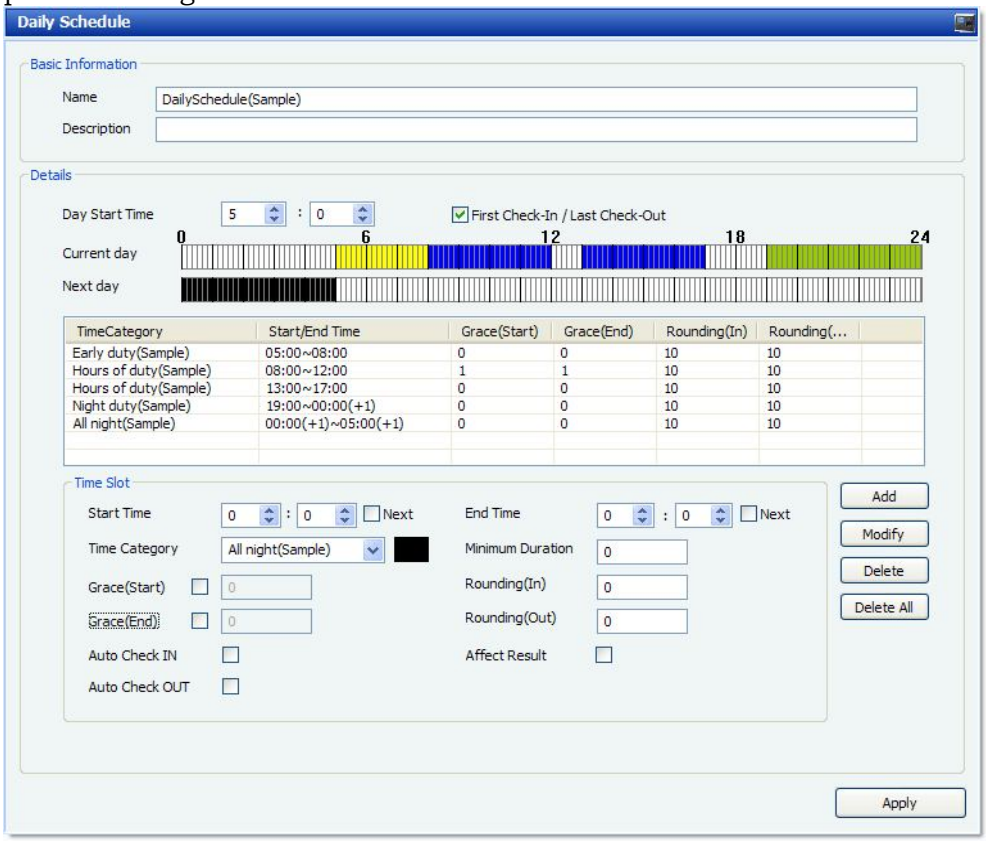


3. Introduzca un nombre y una descripción para la categoría de tiempo.
4. Añada los detalles para la categoría de tiempo:
   - **Time Rate** (Velocidad de tiempo): introduzca la velocidad a la que el tiempo se calculará para esta categoría de tiempo.
   - **Rounding Unit(Min)** (Unidad de redondeo (min.)): especifique en minutos cómo se redondeará el tiempo de trabajo de un usuario (por ejemplo, si lo configura en "5", el tiempo de trabajo de un usuario se redondeará y disminuirá al minuto 5 más cercano).
   - **Display Color** (Mostrar color): configure cómo aparecerá la categoría de tiempo en el programa diario.
5. Haga click en **Apply** (Aplicar) para guardar la categoría de tiempo.

3.8.2 Adición de un programa diario

Para añadir un programa diario:

1. Haga click en la opción **Time and Attendance** (Tiempo y asistencia) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Add Daily Schedule* (Añadir programa diario). Esta acción abrirá un panel, llamado Daily Schedule (Programa diario), parecido al siguiente:



3. Introduzca un nombre y una descripción para el programa diario.
4. Configure la hora de inicio (Start Time) del programa diario y, si lo desea, haga click en la casilla de validación que se encuentra a la derecha para permitir que BioStar registre la primera y la última actividad de los empleados, así como la llegada y la salida, mediante el sistema BioStar.
5. Defina el programa diario añadiendo uno o más espacios de tiempo:
   a. Especifique los detalles del espacio de tiempo:
      - **Start time** (Hora de inicio): establezca la hora de inicio del espacio de tiempo. Si el espacio de tiempo comienza al día siguiente del calendario, haga click en la casilla de validación "Next" (Siguiente) que se encuentra a la derecha.

- **End time** (Hora de finalización): establezca la hora de finalización del espacio de tiempo. Si el espacio de tiempo termina al día siguiente del calendario, haga click en la casilla de validación "Next" (Siguiente) que se encuentra a la derecha.
- **Time Category** (Categoría de tiempo): seleccione una categoría de tiempo de la lista desplegable. Consulte la sección 3.8.1 para definir las categorías de tiempo que aparecerán en esta lista.
- **Minimum Duration** (Duración mínima): establezca la duración mínima del espacio de tiempo (en minutos). Los empleados deberán chequear al menos la duración mínima; si no, el sistema no registrará ningún tiempo trabajado en el espacio de tiempo.
- **Grace (Start)** (Gracia (Inicio)): active y establezca un período de gracia para entrar al comienzo del espacio de tiempo (en minutos). Haga click en la casilla de validación para habilitar el período de gracia y luego especifique la duración en el campo correspondiente. Los empleados que chequen durante el período de gracia serán considerados como si hubiesen checado justo al comienzo del espacio de tiempo.
- **Grace (End)** (Gracia (Fin)): active y establezca un período de gracia para salir al comienzo del espacio de tiempo (en minutos). Haga click en la casilla de validación para habilitar el período de gracia y luego especifique la duración en el campo correspondiente. Los empleados que chequen durante el período de gracia serán considerados como si hubiesen salido justo al final del espacio de tiempo.
- **Rounding (In)** (Redondeo (Entrada)): especifique en minutos cómo se redondeará la hora de entrada de un usuario (por ejemplo, si lo configura en "5", la hora de un usuario se redondeará y disminuirá al minuto 5 más cercano).
- **Rounding (Out)** (Redondeo (Salida)): especifique en minutos cómo se redondeará la hora de salida de un usuario (por ejemplo, si lo configura en "5", la hora de un usuario se redondeará y disminuirá al minuto 5 más cercano).
- **Auto Check IN** (Entrada automática): habilite o deshabilite esta función para que se cheque automáticamente a un usuario que cometió un error a la hora de chequear la entrada en el espacio de tiempo.
- **Auto Check OUT** (Salida automática) - habilite o deshabilite esta función para que se cheque automáticamente a un usuario que cometió un error a la hora de chequear la salida en el espacio de tiempo.

- **Affect Result** (Afectar resultado): permita o prohíba que los datos de este espacio de tiempo se utilicen para determinar el resultado de tempo y asistencia general de un programa diario.

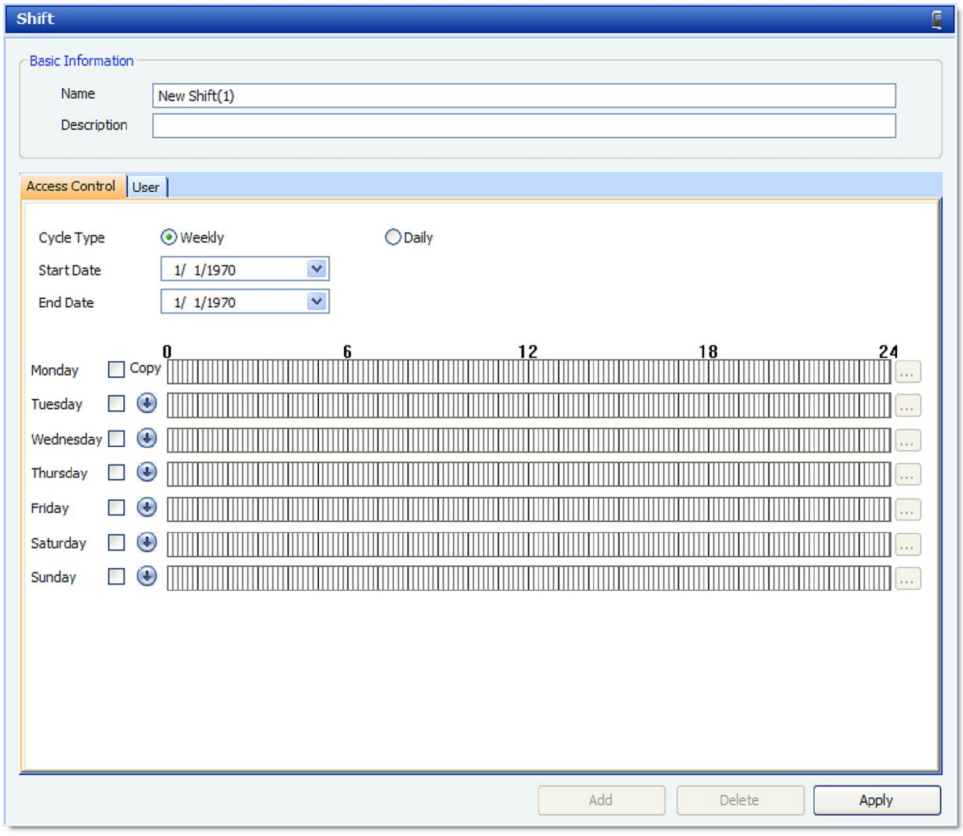
b. Haga click en **Add** (Añadir) para añadir el espacio de tiempo al programa diario.

6. Haga click en **Apply** (Aplicar) para guardar el programa diario.

3.8.3 Adición de un turno

Para añadir un turno:

1. Haga click en la opción **Time and Attendance** (Tiempo y asistencia) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Add Shift* (Añadir turno). Esta acción abrirá un panel, llamado Shift (Turno), parecido al siguiente:



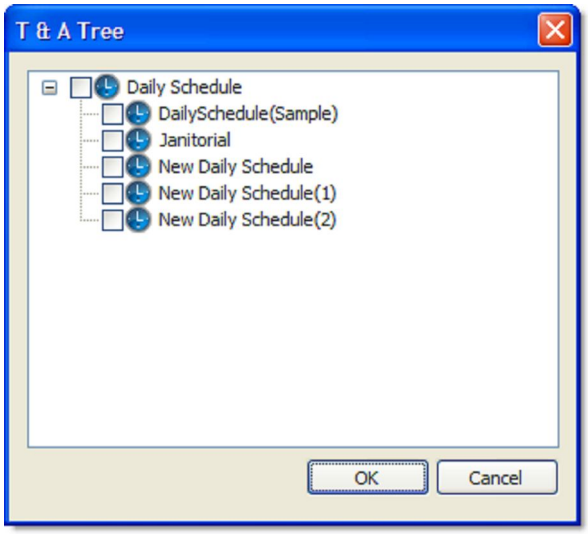
3. Haga click en los botones de radio para establecer el turno como parte de un ciclo diario o semanal. Si selecciona "weekly" (semanal), el ciclo estará formado por una semana del calendario. Si selecciona "daily" (diario), puede especificar cualquier número de días consecutivos (p. ej.: 5, 10 o 20 días) para formar un ciclo.

   Nota: el ciclo diario sólo está disponible en la edición estándar de BioStar.

4. Selecciona las fechas de inicio y finalización de los calendarios desplegables.

5. Active los días del ciclo haciendo click en las casillas de validación que se encuentran a la izquierda.

6. Haga click en el botón de elipsis (...) para seleccionar un programa diario. Esta acción abrirá la ventana T&A Tree (Árbol de tiempo y asistencia). Consulte la sección 3.8.2 para definir los programas diarios que aparecerán en esta ventana.



7. Seleccione un programa diario y haga click en **OK** (Aceptar) para aplicar el programa diario al turno.
8. Repita los pasos 5-7 tantas veces como sea necesario.

   Nota: Puede copiar un programa de un día a otro haciendo click en la flecha que se encuentra a la derecha del día.

9. Haga click en **Apply** (Aplicar) para guardar el turno.

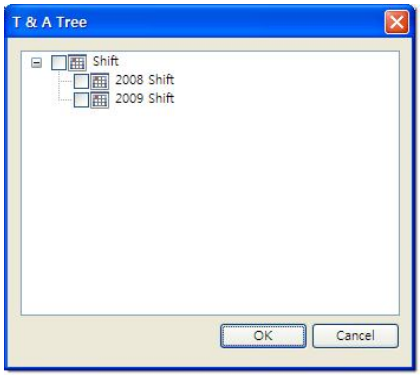
3.8.4 Asignación de usuarios a turnos

Asigne usuarios a turnos para que BioStar registre datos de tiempo y asistencia. Puede asignar usuarios individuales a turnos mediante el panel User (Usuario), o asignar múltiples usuarios a un turno mediante el panel Time and Attendance (Tiempo y asistencia).

Para asignar usuarios individuales a turnos mediante el panel User (Usuario):

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un usuario.
3. En el panel User (Usuario), haga click en la pestaña T&A (Tiempo y asistencia).

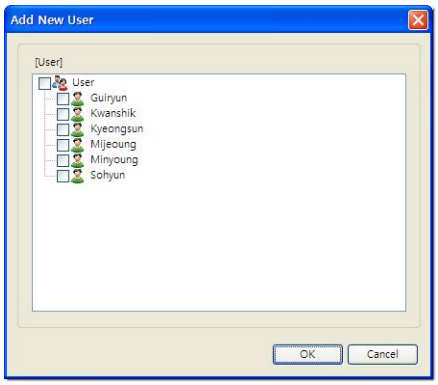
4. Haga click en el botón de radio que se encuentra junto a Shift Management (Gestión de turnos) y luego haga click en **Add** (Añadir), en la parte inferior del panel User (Usuario). Esta acción abrirá la ventana T&A Tree (Árbol de tiempo y asistencia).



5. Seleccione un turno y haga click en **OK** (Aceptar).
6. Haga click en **Apply** (Aplicar) para guardar la configuración de tiempo y asistencia del usuario.

Para asignar varios usuarios a un turno mediante el panel Time and Attendance (Tiempo y asistencia):

1. Haga click en la opción **Time and Attendance** (Tiempo y asistencia) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un turno.
3. En el panel Shift (Turno), haga click en la pestaña User (Usuario) y luego haga click en **Add** (Añadir), en la parte inferior del panel. Esta acción abrirá la ventana Add New User (Añadir nuevo usuario).

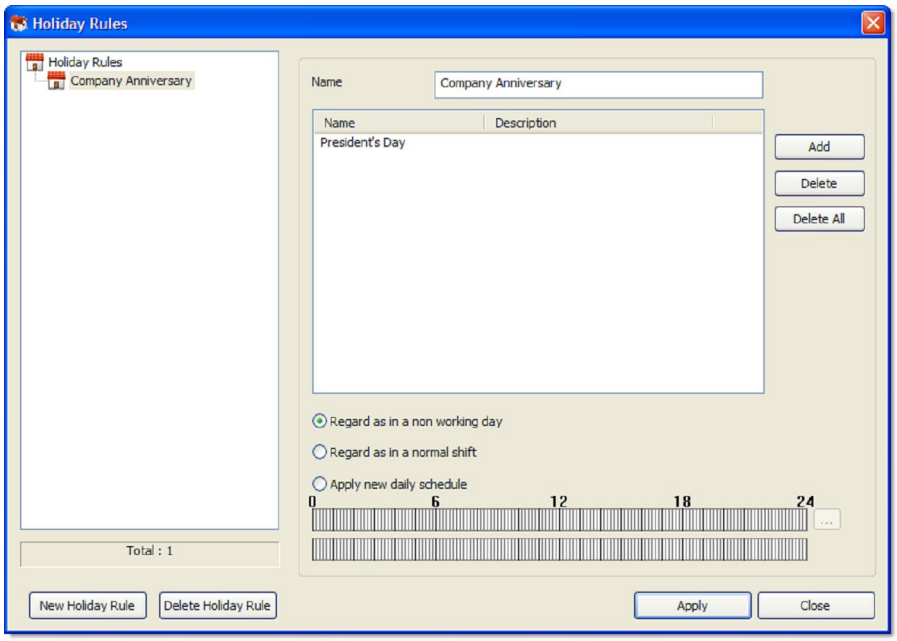


4. Seleccione uno o más usuarios y luego haga click en **OK** (Aceptar).
5. Haga click en **Apply** (Aplicar) para guardar la configuración de tiempo y asistencia del turno.

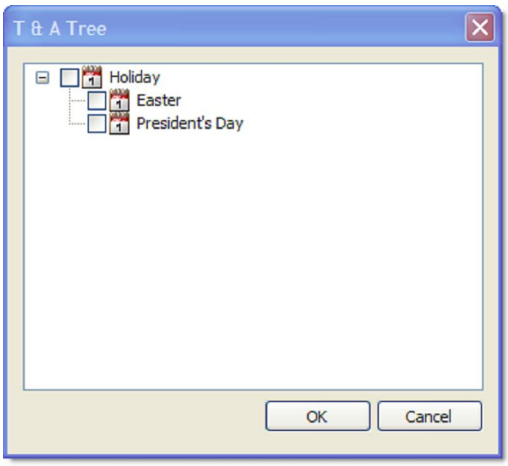
3.8.5 Adición de una norma vacacional

Para añadir una norma vacacional:

1. Haga click en la opción **Time and Attendance** (Tiempo y asistencia) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Holiday Management* (Gestión de vacaciones). Esta acción abrirá la ventana Holiday Rules (Normas vacacionales).



3. Haga click en New Holiday Rule (Nueva norma vacacional).
4. Introduzca un nombre para la norma.
5. Haga click en **Add** (Añadir). Esta acción abrirá la ventana T&A Tree (Árbol de tiempo y asistencia).



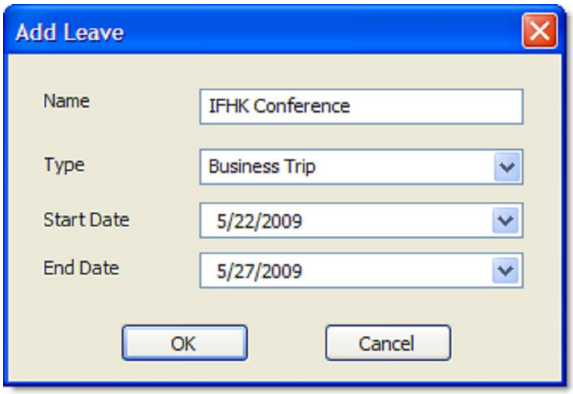
6. Seleccione un período vacacional de la lista y haga click en **OK** (Aceptar). Para definir un período vacacional, consulte la sección 3.6.2.

7. Haga click en uno de los botones de radio que se encuentran en la parte inferior de la ventana Holiday Rules (Normas vacacionales) y especifique cómo debería afectar el período vacacional a los programas de tiempo y asistencia:
   - **Regard as in a non-working day** (Contemplar como día no laborable): el tiempo trabajado en este día no se registra y no aparece en los reportes de tiempo y asistencia.
   - **Regard as in a normal shift** (Contemplar como en un turno normal): el tiempo trabajado en este día se registrará y calculará como en un turno normal.
   - **Apply a new daily schedule** (Aplicar un nuevo programa diario): el tiempo trabajado en este día se registrará y calculará por un programa diario seleccionado.
8. Si elige aplicar un nuevo programa diario, haga click en el botón de elipsis (...) para seleccionar un programa. Consulte la sección 3.8.2 para crear programas diarios.
9. Haga click en **Apply** (Aplicar) para guardar la norma vacacional.

3.8.6 Adición de un período de permiso

Añada períodos de permiso para definir tiempos en los que se prevé que los trabajadores estén fuera de la oficina, pero que se consideren como si estuvieran trabajando, como en días de vacaciones pagados o viajes de empresa. Para incluir un período vacacional programado de un usuario o un período de permiso en la configuración de tiempo y asistencia:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel User (Usuario), haga click en la pestaña T&A (Tiempo y asistencia).
3. Haga click en el botón de radio que se encuentra al lado de Leave Management (Gestión de permisos) y luego haga click en **Add** (Añadir). Esta acción abrirá la ventana Add Leave (Añadir permiso).



4. Si lo desea, introduzca un nombre para el período de permiso.
5. Seleccione un tipo de permiso de la primera lista desplegable.

6. Introduzca las fechas de inicio y finalización del permiso haciendo click en los calendarios desplegables.
7. Haga click en **OK** (Aceptar) para añadir el período de permiso a la configuración de tiempo y asistencia del usuario.
8. Haga click en **Apply** (Aplicar) para guardar la configuración de tiempo y asistencia del usuario.

3.9 Configuración de alarmas

BioStar puede proporcionar varios niveles de notificación de alarma. El sistema puede activar las alarmas del sistema al emitir sonidos de los dispositivos y de las computadoras conectadas. El sistema también se puede configurar para que envíe notificaciones por e-mail a ciertos destinatarios. Además, es posible configurar el sistema para que reciba entradas de dispositivos externos (como dispositivos de alarma en caso de incendio) o para que envíe salidas a dispositivos externos (como sirenas de alarma).

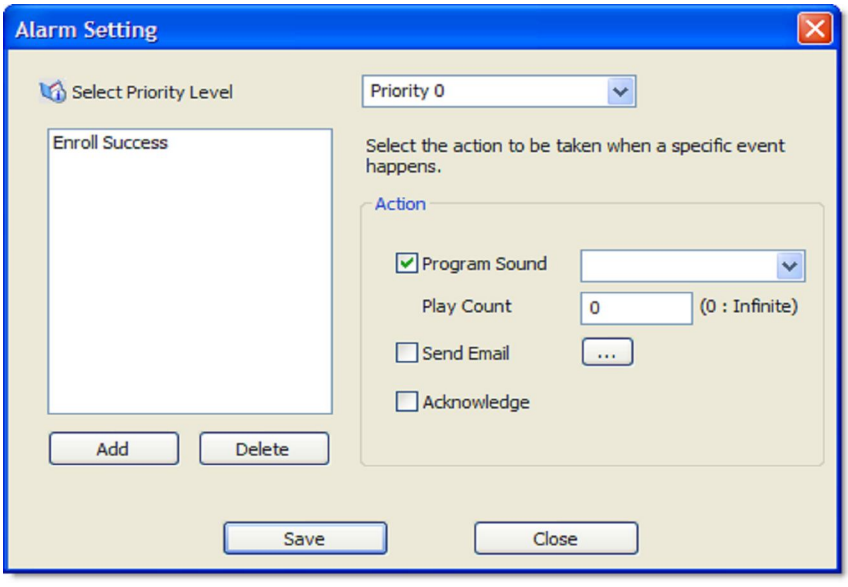
3.9.1 Configuración y sonidos de alarma

BioStar permite personalizar la respuesta del sistema ante eventos. Es posible configurar los parámetros de alarma creando niveles de prioridad personalizados y seleccionando la acción que se llevará a cabo ante un evento determinado. También es posible añadir sus propios sonidos de alarma para personalizar aún más el sistema.

3.9.1.1 Personalización de las acciones de alarma

Para personalizar las acciones de alarma:

1. En la barra de menú, haga click en **Option > Event > Alarm Setting** (Opción > Evento > Configuración de alarma).
   Esta acción abrirá la ventana Alarm Setting (Configuración de alarma).



2. Seleccione un nivel de prioridad de la lista desplegable y haga click en **Add** (Añadir). Esta acción abrirá una lista de eventos.
3. Seleccione los eventos que se incluirán en el nivel de prioridad y haga click en **OK** (Aceptar).
4. Seleccione una acción, o acciones, haciendo click en las casillas de validación de la derecha.
   - Si selecciona *Program Sound* (Programar sonido), elija un sonido de la lista desplegable y luego especifique la duración ("play count") del sonido en segundos. Si establece la opción Play Count (Reproducir durante) en 0, el sonido determinado se reproducirá hasta que alguien, con privilegios administrativos, detenga manualmente el sonido mediante la pestaña Realtime Monitoring (Supervisión en tiempo real) en el panel Monitoring (Supervisión). Para añadir sonidos personalizados a la lista, consulte la sección 3.9.1.2.
   - Si selecciona *Send Email* (Enviar e-mail), haga click en el botón de elipsis (...) que se encuentra a la derecha para seleccionar un destinatario. Para configurar notificaciones por e-mail, consulte la sección 3.9.2.
   - Al seleccionar Acknowledge (Acusar recibo) se activarán los mensajes de alerta en las computadoras secundarias.
5. Repita los pasos 2-4 tantas veces como sea necesario para personalizar otros niveles de prioridad.
6. Una vez finalizado, haga click en **Save** (Guardar).

3.9.1.2 Adición de sonidos de alarma personalizados

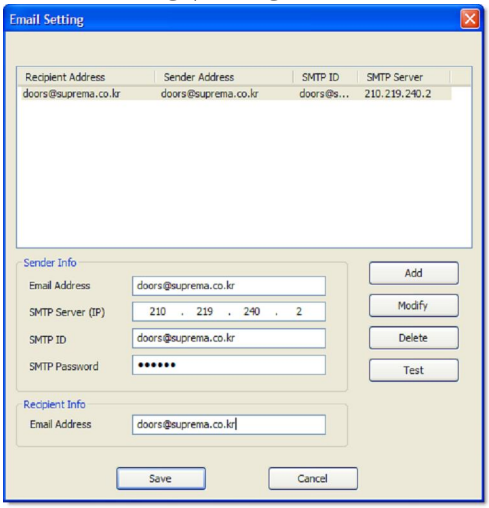
Para añadir sonidos de alarma personalizados:

1. En la barra de menú, haga click en **Option > Event > Sound Setting** (Opción > Evento > Configuración de sonido). Esta acción abrirá la ventana Sound Setting (Configuración de sonido).
2. Haga click en **Add** (Añadir).
3. Localice un archivo de forma de onda (.wav) en su computadora o red y haga click en **Open** (Abrir).
4. Si lo desea, haga click en un sonido y luego haga click en **Play** (Reproducir) para escuchar el sonido.
5. Una vez finalizado, haga click en **Save** (Guardar).

3.9.2 Configuración de las notificaciones por e-mail

BioStar puede enviar notificaciones por e-mail ante un evento (opción no disponible en la versión gratuita). Tal y como se explica en la sección 3.9.1.1, es posible personalizar los eventos que activarán alertas automáticas por e-mail. Para configurar una notificación por e-mail:

1. En la barra de menú, haga click en **Option > Event > E-mail Setting** (Opción > Evento > Configuración de e-mail). Esta acción abrirá la ventana Email Setting (Configuración de e-mail).



2. Escriba la dirección de e-mail, el servidor SMTP, el id. SMTP y la contraseña SMTP en la sección *Sender Info* (Información del remitente).
3. Escriba la dirección de e-mail en la sección *Recipient Info* (Información del destinatario).
4. Haga click en **Add** (Añadir) para añadir la configuración a la lista.
5. Repita los pasos 2-4 tantas veces como sea necesario para añadir otras configuraciones de e-mail.
6. Una vez finalizado, haga click en **Save** (Guardar).

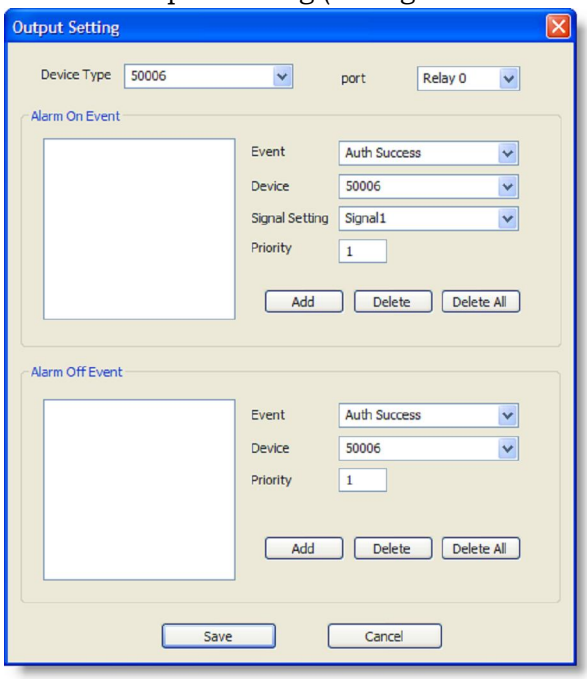
3.9.3 Configuración de los parámetros para dispositivos externos

Cuando se utilizan dispositivos externos con BioStar, debe configurar los parámetros para determinar las acciones que se llevarán a cabo en respuesta a las entradas. Para obtener más información acerca de cómo configurar dispositivos y los parámetros de los dispositivos, consulte las secciones 3.2 y 5.1.

3.9.3.1 Configuración de salidas a dispositivos externos

Puede elegir que ciertos dispositivos envíen señales a dispositivos externos, como sirenas de alarma, ante determinados eventos. Para configurar salidas:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un dispositivo.
3. En el panel Device (Dispositivo), haga click en la pestaña Output (Salida).
4. Haga click en **Add** (Añadir) al final del panel. Esta acción abrirá la ventana Output Setting (Configuración de salidas).



5. Configure las acciones que activarán (enviarán una señal a) un relay de salida específico:
   a. En la sección *Alarm On Event* (Evento para activar alarma), seleccione un evento de la primera lista desplegable.
   b. Seleccione el número del dispositivo o *All Device* (Todos los dispositivos) de la segunda lista desplegable.
   c. Seleccione una configuración de señal de la tercera lista desplegable.
   d. Introduzca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para encender una alarma (activar) de prioridad 2 solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.

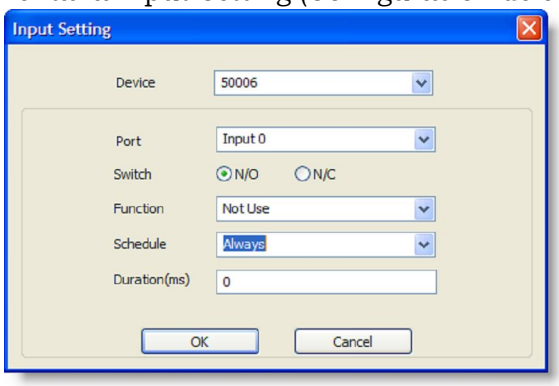
e. Haga click en **Add** (Añadir).

6. Configure las acciones que apagarán (detendrán el envío de una señal) un relay de salida activado:
   a. En la sección *Alarm Off Event* (Evento para desactivar alarma), seleccione un evento de la primera lista desplegable.
   b. Seleccione el número del dispositivo o *All Device* (Todos los dispositivos) de la segunda lista desplegable.
   c. Introduzca una prioridad para el evento.
   d. Haga click en **Add** (Añadir).
7. Una vez finalizado, haga click en **Save** (Guardar).

3.9.3.2 Configuración de entradas de dispositivos externos

Para integrar el control de puertas de BioStar con otros sistemas de alarma como, por ejemplo, los sistemas de alarma en caso de incendio, es posible especificar las acciones que BioStar llevará a cabo cuando reciba una entrada. También es posible configurar las entradas para que BioStar trabaje con los botones de salida manuales de las puertas y con otros tipos de dispositivos externos. Para configurar entradas:

1. Haga click en **Device** (Dispositivo) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un dispositivo.
3. En el panel Device (Dispositivo), haga click en la pestaña Input (Entrada).
4. Haga click en **Add** (Añadir) al final del panel. Esta acción abrirá la ventana Input Setting (Configuración de entradas).



5. Seleccione un puerto de entrada de la segunda lista desplegable.
6. Seleccione la posición normal del interruptor de entrada (*N/O: normalmente abierto* o *N/C: normalmente cerrado*).
7. Seleccione una función para la entrada (*Not Use* (No usar), *Generic Input* (Entrada genérica), *Emergency Open* (Apertura de emergencia),

Release All Alarms (Cancelar todas las alarmas), *Restart Device* (Reiniciar dispositivo) o *Disable Device* (Deshabilitar dispositivo)).

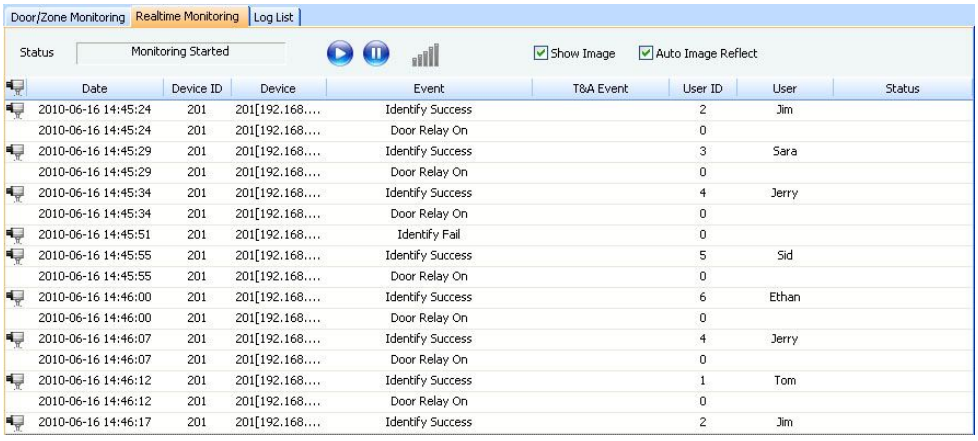
8. Seleccione un programa para aplicar la función (*Always* (Siempre), *Disable*(Desactivar) o programas personalizados).
10. Establezca la duración mínima (en milisegundos) que una entrada debe durar para activar la acción establecida.
11. Haga click en **OK** (Aceptar).

04 Gestión del sistema BioStar

Una vez que haya configurado el sistema BioStar correctamente, la gestión del mismo es muy sencilla. BioStar permite supervisar eventos en tiempo real, visualizar registros de eventos por fecha, controlar partes del sistema de forma remota, gestionar usuarios y actualizar el firmware de los dispositivos directamente desde la interfaz de BioStar. Además, es posible activar la encriptación de huellas dactilares, en caso de ser necesario, para proporcionar un nivel de seguridad y privacidad extra.

4.1 Supervisión de eventos en tiempo real

El sistema BioStar registra los eventos de todos los dispositivos conectados. Para supervisar eventos en tiempo real, haga click en **Monitoring** (Supervisión), en el panel de acceso directo, y luego haga click en la pestaña Realtime Monitoring (Supervisión en tiempo real).



Date	Device ID	Device	Event	T&A Event	User ID	User	Status
2010-06-16 14:45:24	201	201[192.168....	Identify Success		2	Jim	
2010-06-16 14:45:24	201	201[192.168....	Door Relay On		0		
2010-06-16 14:45:29	201	201[192.168....	Identify Success		3	Sara	
2010-06-16 14:45:29	201	201[192.168....	Door Relay On		0		
2010-06-16 14:45:34	201	201[192.168....	Identify Success		4	Jerry	
2010-06-16 14:45:34	201	201[192.168....	Door Relay On		0		
2010-06-16 14:45:51	201	201[192.168....	Identify Fail		0		
2010-06-16 14:45:55	201	201[192.168....	Identify Success		5	Sid	
2010-06-16 14:45:55	201	201[192.168....	Door Relay On		0		
2010-06-16 14:46:00	201	201[192.168....	Identify Success		6	Ethan	
2010-06-16 14:46:00	201	201[192.168....	Door Relay On		0		
2010-06-16 14:46:07	201	201[192.168....	Identify Success		4	Jerry	
2010-06-16 14:46:07	201	201[192.168....	Door Relay On		0		
2010-06-16 14:46:12	201	201[192.168....	Identify Success		1	Tom	
2010-06-16 14:46:12	201	201[192.168....	Door Relay On		0		
2010-06-16 14:46:17	201	201[192.168....	Identify Success		2	Jim	

Esta pestaña muestra todos los eventos que ocurrieron desde la última vez que inició sesión en el sistema. La pestaña muestra el estado de supervisión actual (*Monitoring Started* (Supervisión iniciada) o *Monitoring Paused* (Supervisión en pausa)) e incluye botones para iniciar (play) o detener (pause) la supervisión en tiempo real. El símbolo de barras de sonido que se encuentra a la izquierda muestra si se está reproduciendo el sonido de una alarma (barras verdes), o no (barras grises). Para detener el sonido de una alarma, haga click en el símbolo de barras de sonido.

Como en BioStar V1.3, los administradores pueden supervisar las ubicaciones y el estado de autentificación de los usuarios mediante la función Roll Call (Pasar lista). Esta función permite a los administradores determinar si los usuarios se encuentran presentes o no, o si entraron a áreas en las que no están autorizados.

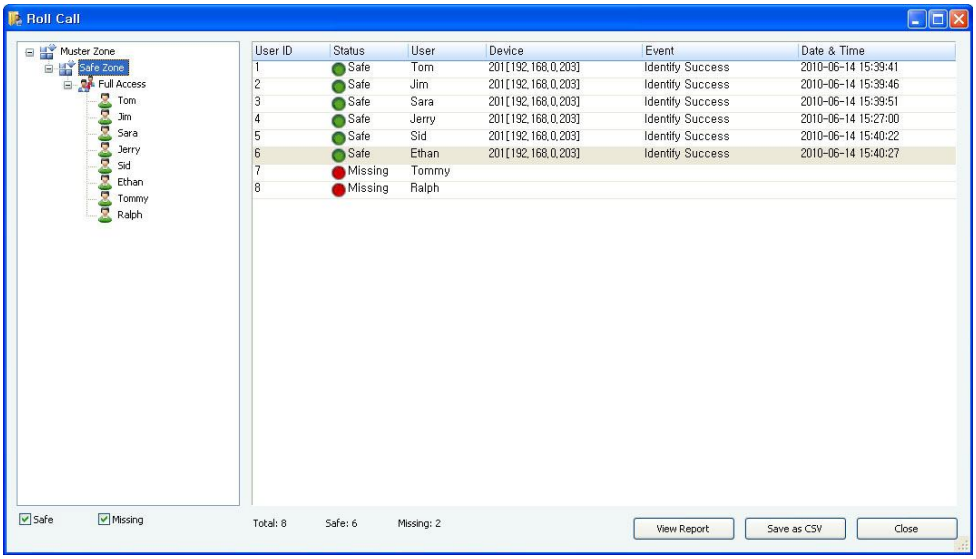
Junto con las funciones de reconocimiento fácil de D-Station, los administradores pueden verificar la identidad de los usuarios haciendo click en **Show Image** (Mostrar imagen) (para visualizar la fotografía almacenada del rostro del usuario) y **Auto Image Reflect** (Reflejar automáticamente imagen) (para visualizar la fotografía más reciente del rostro, capturada por el dispositivo local). Al hacer click en **Show Image** (Mostrar imagen) también se abrirá una ventana en la parte inferior donde se mostrará una fotografía del usuario. Haga click en **Real Size** (Tamaño real) para visualizar la imagen almacenada a tamaño real (640 x 480) en lugar de una miniatura y haga click en **Show Popup** (Mostrar en ventana) para abrir la imagen en una nueva ventana que se puede colocar en cualquier parte de la pantalla.

4.1.1 Supervisión de zonas de reunión en tiempo real

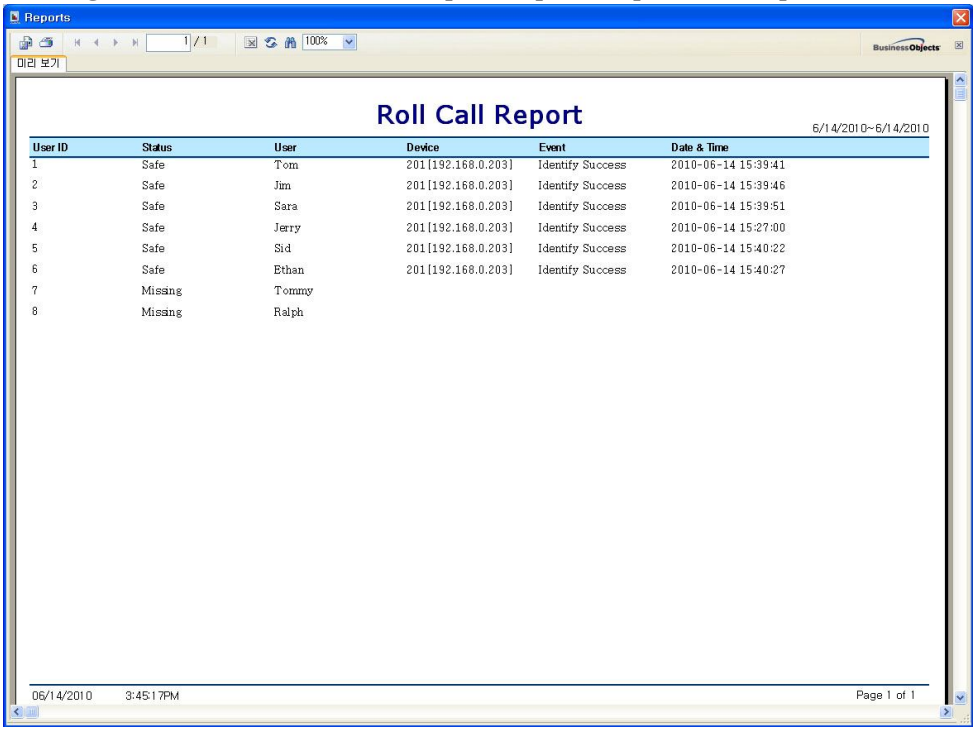
Es posible supervisar y seguir la trayectoria de los empleados en una situación de emergencia. Además, puede determinar si algún empleado no se ha reportado en el área de reunión.

Para supervisar y seguir la trayectoria de los empleados:

1. Haga click en **Monitoring** (Supervisión) en el panel de acceso directo.
2. Haga click en una zona de reunión en el panel Monitoring (Supervisión).
3. En el panel Task (Tarea), haga click en **Roll Call** (Pasar lista). Esta acción abrirá la ventana Roll Call (Pasar lista).



4. Haga click en **View Report** (Visualizar reporte) para visualizar la información como reporte. Esta acción abrirá el reporte de asistencia (Roll Call Report). Haga click en **Save as CSV** (Guardar como CSV) para guardar.
5. Haga click en el símbolo de impresora para imprimir el reporte de asistencia. Haga click en el símbolo de exportar para exportar el reporte de asistencia.



4.2 Visualización de los registros de eventos

BioStar permite visualizar los registros de eventos de usuarios, puertas y zonas. Puede acceder a los registros predefinidos en las pestañas Event (Evento) de los paneles de usuario, puerta y zona. También puede utilizar la pestaña Log List (Lista de registro) en el panel Monitoring (Supervisión) para especificar los parámetros de registro.

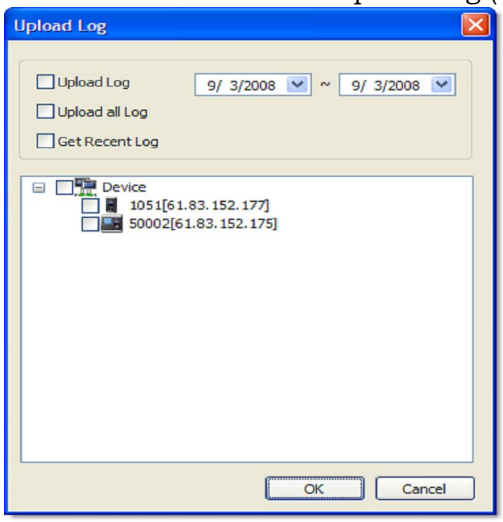
BioStar recopila automáticamente la información de registro de los dispositivos conectados siempre y cuando funcione el servidor. Sin embargo, si posee dispositivos que no se encuentren conectados con el servidor BioStar, deberá subir los registros manualmente antes de visualizarlos.

4.2.1 Subida de registros a BioStar

Para los dispositivos que no se encuentren conectados con el servidor BioStar, deberá subir los registros manualmente antes de visualizarlos.

Para subir registros a BioStar:

1. Haga click en **Monitoring** (Supervisión) en el panel de acceso directo.
2. Haga click en la pestaña Log List (Lista de registro), en el panel Monitoring (Supervisión).
3. En el panel Task (Tarea), haga click en **Upload Log** (Subir registro). Esta acción abrirá la ventana Upload Log (Subir registro).



4. Seleccione una opción de subida haciendo click en los campos correspondientes:
   a. **Upload Log** (Subir registro): utilice esta opción para subir los registros de un período de tiempo específico. Especifique el período con los calendarios desplegables.
   b. **Upload All Log** (Subir todo el registro): utilice esta opción para subir todos los registros.

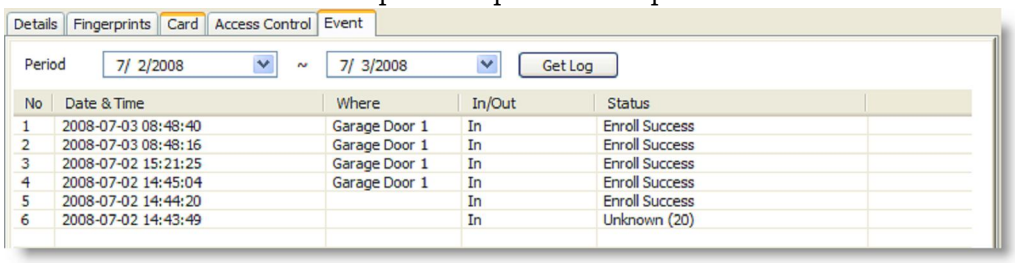
c. **Get Recent Log** (Obtener registro reciente): utilice esta opción para subir los registros realizados desde la anterior subida.

5. Seleccione los dispositivos desde los que subirán los registros haciendo click en las casillas de validación que se encuentran al lado de los números de los dispositivos.
6. Haga click en **OK** (Aceptar). BioStar descargará los registros de los dispositivos seleccionados y mostrará las actividades en la lista de registro.

4.2.2 Visualización de registros en paneles de usuario, puerta y zona

Para visualizar registros predefinidos:

1. Haga click en **User** (Usuario) o en **Doors** (Puertas) en el panel de acceso directo.
2. En el panel de navegación, haga click en el nombre de un usuario, puerta o zona.
3. En los paneles User (Usuario), Doors (Puertas) o Zone (Zona), haga click en la pestaña Event (Evento).
4. Establezca el período de un evento (fechas de inicio y de finalización) con los calendarios desplegables.
5. Haga click en **Get Log** (Obtener registro). Esto generará una lista de los eventos más destacados del período que usted especificó.



4.2.3 Visualización de registros desde el panel de supervisión

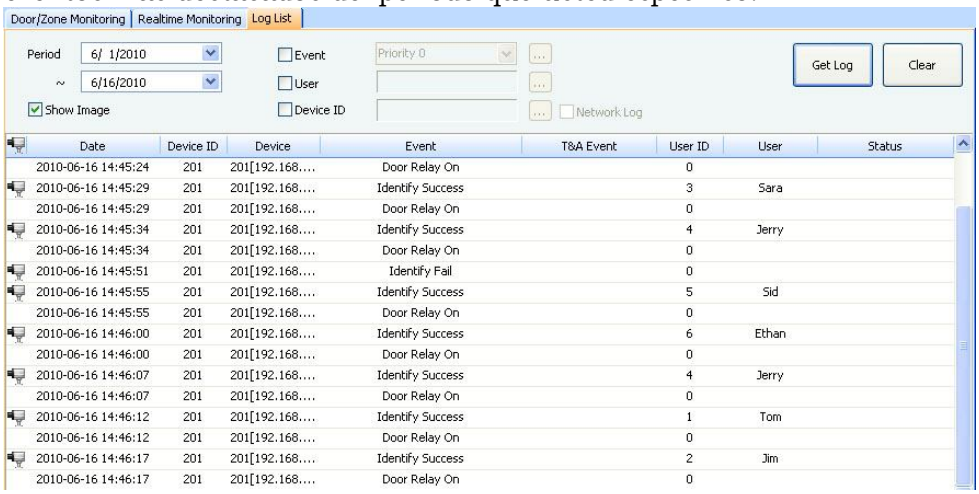
Para especificar filtros de registros o para visualizar registros de grupos de usuarios, puertas o zonas:

1. Haga click en **Monitoring** (Supervisión) en el panel de acceso directo.
2. En el panel Monitoring (Supervisión), haga click en la pestaña Log List (Lista de registro).
3. Establezca el período de un evento (fechas de inicio y de finalización) con los calendarios desplegables.
4. Configure los parámetros para generar un registro:
   - Para mostrar eventos por prioridad de alarma, haga click en la casilla de validación Event (Evento) y seleccione una prioridad de evento de la lista

desplegable. Para añadir una nueva prioridad de alarma, haga click en el botón de elipsis (...) para abrir la ventana Alarm Priority (Prioridad de alarma).

- Para mostrar eventos por usuario, haga click en la casilla de validación User (Usuario) y luego haga click en el botón de elipsis (...) para seleccionar un usuario, o usuarios, que aparece en la ventana User/Department Tree (Árbol de usuario/área). Puede seleccionar a todos los usuarios al mismo tiempo, si selecciona el nivel superior del árbol de usuarios.
- Para mostrar los eventos de un dispositivo en particular, haga click en la casilla de validación Device ID (Id. de dispositivo) y luego haga click en el botón de elipsis (...) para seleccionar un dispositivo de la ventana Device Tree (Árbol de dispositivos). Para mostrar sólo los eventos de red de un dispositivo, también puede hacer click en la casilla de validación Only Network History (Sólo historial de redes).
- Para mostrar todos los eventos, deje sin seleccionar todas las casillas de validación.
- Para mostrar la fotografía de un usuario en la parte inferior de la pestaña, haga click en **Show Image** (Mostrar imagen). Para obtener más información acerca de cómo visualizar fotografías de usuarios, consulte la sección 4.1.

5. Haga click en **Get Log** (Obtener registro). Esto generará una lista de los eventos más destacados del período que usted especificó.



4.3 Supervisión de eventos de puertas mediante un mapa visual

BioStar permite gestionar convenientemente las puertas en una representación visual del plano de la planta actual. En el mapa visual, puede personalizar el plano de la planta, añadir puertas y supervisar el estado y la actividad de éstas (por ejemplo: si una puerta está abierta o cerrada, los eventos de autentificación y

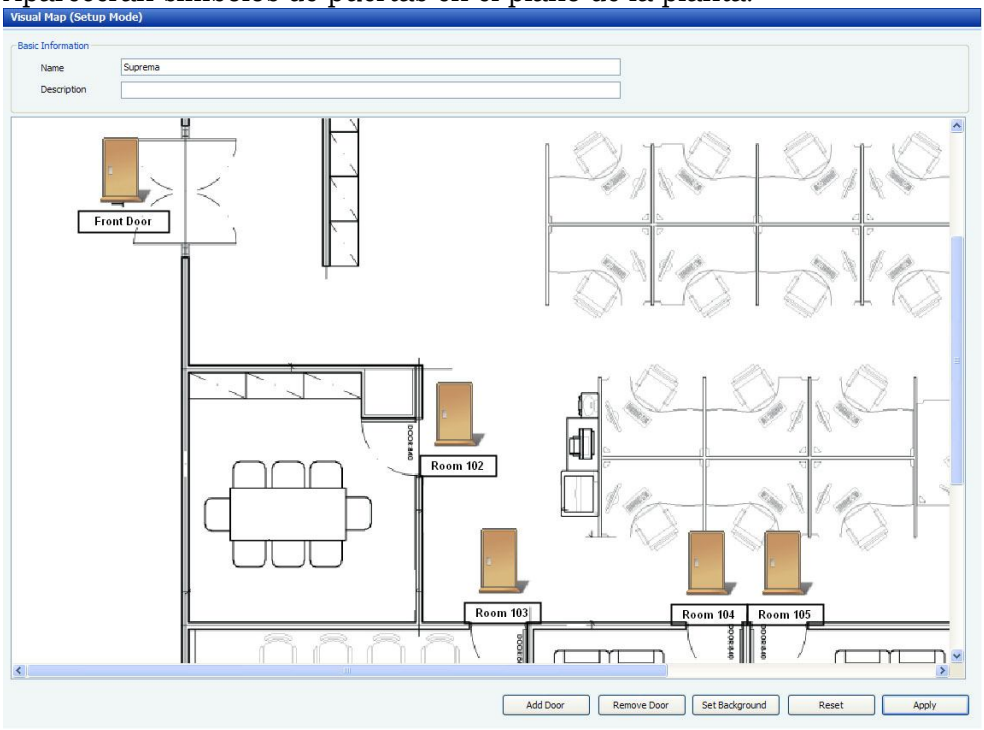
las alarmas de las puertas). Si el edificio posee más de una planta, puede crear mapas visuales adicionales para cada una de ellas. La función del mapa visual sólo está disponible en la edición estándar.

4.3.1 Creación de un mapa visual

En el modo de configuración, puede añadir el plano de la planta del edificio y ubicar puertas. Para añadir el plano de la planta y ubicar puertas:

1. En el panel de acceso directo, haga click en **Visual Map** (Mapa visual).
2. En el panel Task (Tarea), haga click en **Setup Mode** (Modo de configuración). Aparecerá “Monitor Mode” (Modo supervisor) en la barra del título de la ventana Visual Map (Mapa visual).
3. En el panel Task (Tarea), haga click en **Add Visual Map** (Añadir mapa visual). Esta acción abrirá una nueva ventana Visual Map (Mapa visual) en la parte derecha.
4. En la ventana Visual Map (Mapa visual), escriba un nombre para el mapa visual.
5. En la parte inferior de la ventana Visual Map (Mapa visual), haga click en **Set Background** (Configurar fondo) para añadir el plano de una planta. BioStar es compatible con imágenes con una resolución mayor a 730x470, solo en formato jpg, bmp, gif, o png.
6. Elija una imagen y haga click en **Open** (Abrir).
7. Haga click en **Add Door** (Añadir puertas) para añadir puertas. Esta acción abrirá una ventana con un listado de puertas.
8. Del listado de puertas, haga click en las casillas de validación que se encuentran al lado de las puertas para añadir y haga click en **Apply** (Aplicar).

Aparecerán símbolos de puertas en el plano de la planta.



9. Haga click en el símbolo de puerta y arrástrelo hacia la ubicación deseada en el plano de la planta. Puede reubicar o renombrar un símbolo de puerta de forma individual haciendo doble click en el símbolo o en el nombre de la puerta.
10. Para eliminar una puerta del plano de la planta, haga click en la puerta y luego haga click en **Remove Door** (Eliminar puerta).
11. Repita los pasos 7-10 tantas veces como sea necesario para añadir más puertas.
12. Una vez que haya finalizado de añadir puertas, haga click en **Apply** (Aplicar).

Nota: para eliminar todas las puertas del plano y comenzar de nuevo, haga click en **Reset** (Reiniciar).

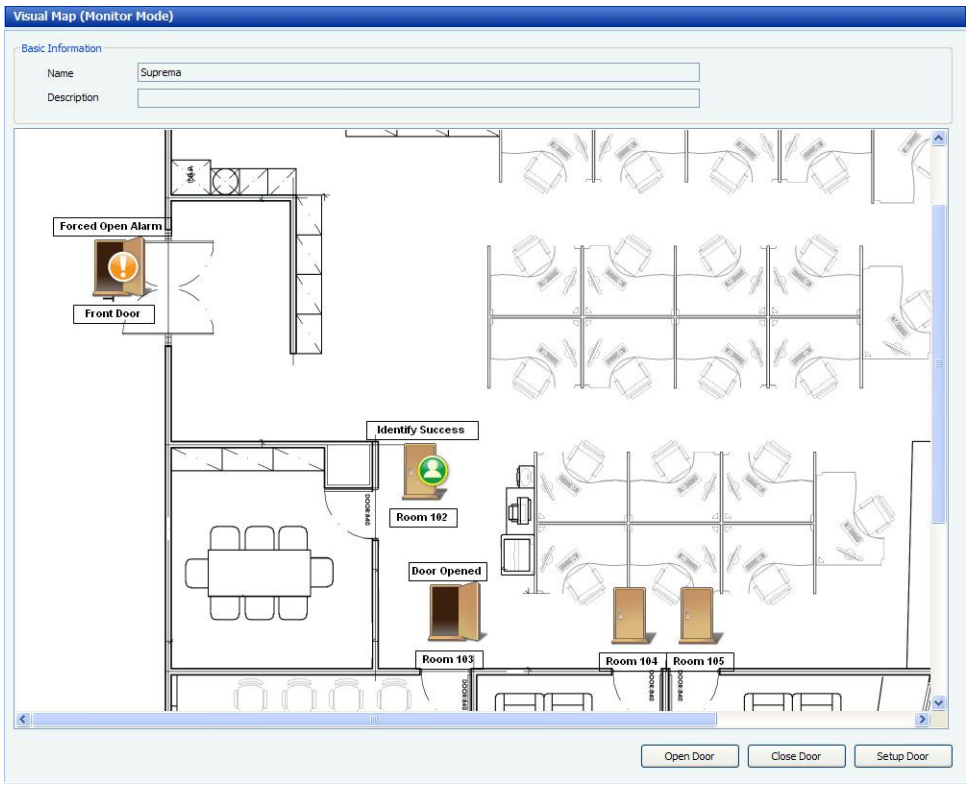
4.3.2 Supervisión de puertas en un mapa visual

En el modo supervisor, puede visualizar el estado y las actividades de todas las puertas en el mapa mejorado visualmente.

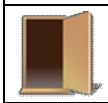
Para supervisar puertas:

1. En el panel Task (Tarea), haga click en **Monitor Visual Map** (Supervisar mapa visual). Aparecerá “Monitor Mode” (Modo supervisor) en la barra del título de la ventana Visual Map (Mapa visual).

3. Configuración del sistema BioStar



2. Supervise el estado y las actividades de las puertas, representados por símbolos, en el mapa visual. Las actividades de las puertas como, por ejemplo, las autentificaciones realizadas con éxito, las alarmas, etc., aparecerán representadas por los siguientes símbolos de puertas:

Símbolo	Actividad
	Puerta cerrada / Alarma de puerta apagada
	Puerta abierta
	Autentificación exitosa con puerta cerrada
	Autentificación exitosa con puerta abierta
	Autentificación fallida con puerta cerrada
	Autentificación fallida con puerta abierta
	Puerta mantenida abierta o forzada / Alarma por puerta mantenida abierta o forzada

Nota: los símbolos de puerta solo cambiarán cuando los sensores de las puertas se hayan asignado en el apartado de configuración de las puertas y se detecte el estado de la puerta. Dicho con otras palabras, los símbolos de puerta solo cambiarán cuando la puerta realmente se abra o se cierre, y no cuando usted haga click en **Open Door** (Abrir puerta) o **Close door** (Cerrar puerta). Para obtener más información acerca de la configuración de puertas, consulte la sección 5.2.1.

3. Para abrir o cerrar una puerta, haga click en una puerta y luego haga click en **Open Door** (Abrir puerta) o **Close Door** (Cerrar puerta).
4. Para cambiar la configuración de una puerta, haga click en una puerta y luego haga click en **Setup Door** (Configurar puerta).

4.4 Control remoto de puertas, alarmas y dispositivos

BioStar permite a los administradores y operadores controlar puertas, alarmas y dispositivos de forma remota. Puede abrir o cerrar puertas mediante una computadora conectada al sistema BioStar. También puede apagar (cancelar) alarmas de forma remota y bloquear y desbloquear dispositivos.

4.4.1 Apertura o cierre de puertas

En algunas situaciones, un administrador o un operador puede necesitar abrir o cerrar una puerta de forma remota. Para abrir o cerrar puertas:

1. Haga click en **Monitoring** (Supervisión) en el panel de acceso directo.
2. En la pestaña Door/Zone Monitoring (Supervisión de puerta/zona) se muestra una lista con los nombres de las puertas y sus estados. Para cambiar el estado de una puerta (abierta o cerrada), haga click en el nombre de la puerta y luego haga click en **Open Door** (Abrir puerta) o **Close Door** (Cerrar puerta).

También puede abrir o cerrar puertas cuando se encuentre supervisando un mapa visual. Para obtener más información, consulte la sección 4.3.2.

4.4.2 Cancelación de alarmas

Cuando un evento activa una alarma, los administradores y operadores pueden cancelar la alarma de forma remota. Para cancelar alarmas:

1. Haga click en **Monitoring** (Supervisión) en el panel de acceso directo.
2. En la pestaña Door/Zone Monitoring (Supervisión de puerta/zona) se muestra una lista con los nombres de las puertas y los eventos de alarma. Para cancelar una alarma, haga click en el nombre de la puerta y luego haga click en **Release Alarm** (Cancelar alarma).

4.4.3 Bloqueo o desbloqueo de dispositivos

BioStar permite bloquear y desbloquear dispositivos para evitar que se produzca un acceso no autorizado cuando BioStar no se encuentre funcionando. Esta acción bloquea la comunicación de los dispositivos. Puede bloquear dispositivos manualmente desde la interfaz de BioStar, o automáticamente cuando sale del software BioStar. Todos los dispositivos conectados se pueden bloquear o desbloquear simultáneamente, pero no se pueden bloquear o desbloquear los dispositivos que están conectados directamente al servidor BioStar.

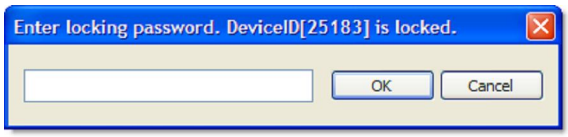
4.4.3.1 Bloqueo y desbloqueo de dispositivos conectados

Para bloquear todos los dispositivos conectados, en la barra de menú, haga click en **Option > Device > Lock All Devices** (Opción > Dispositivo > Bloquear todos los dispositivos).

Para desbloquear todos los dispositivos conectados:

1. En la barra de menú, haga click en **Option > Device > Unlock All Devices** (Opción > Dispositivo > Desbloquear todos los dispositivos).

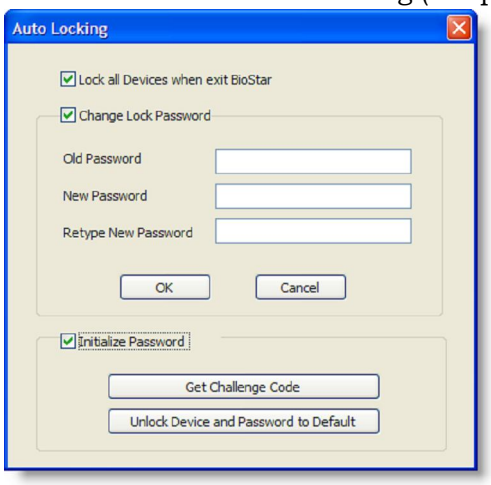
2. Si es necesario, introduzca una contraseña en la ventana Enter Locking Password (Introducir contraseña de bloqueo) y haga click en **OK** (Aceptar) (si no ha creado una contraseña de bloqueo, simplemente haga click en **OK**(Aceptar)). Consulte la sección 4.4.3.2 para crear una contraseña de bloqueo.



4.4.3.2 Configuración del bloqueo automático del dispositivo

Para configurar el bloqueo automático del dispositivo:

1. En la barra de menú, haga click en **Option > Device > Automatic Locking** (Opción > Dispositivo > Bloqueo automático). Esta acción abrirá la ventana Auto Locking (Bloqueo automático).

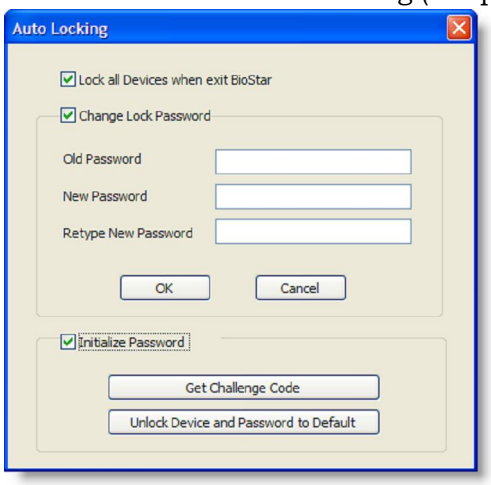


2. Haga click en la primera casilla de validación para bloquear todos los dispositivos al salir de BioStar.
3. Si lo desea, haga click en la segunda casilla de validación para cambiar la contraseña de bloqueo:
   a. Introduzca la contraseña anterior.
   b. Introduzca la contraseña nueva.
   c. Vuelva a escribir la nueva contraseña para confirmar.

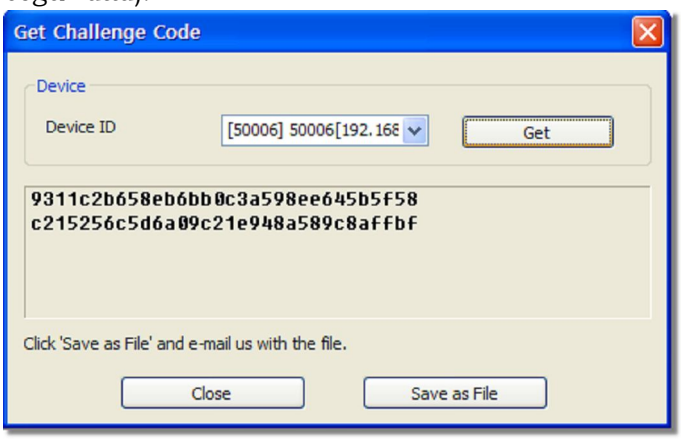
4.4.3.3 Reinicio de un dispositivo bloqueado

Si ha olvidado la contraseña de bloqueo de un dispositivo, el equipo de soporte técnico de Suprema puede enviarle un código de desbloqueo. Para solicitar el código:

1. En la barra de menú, haga click en **Option > Device > Automatic Locking** (Opción > Dispositivo > Bloqueo automático). Esta acción abrirá la ventana Auto Locking (Bloqueo automático).

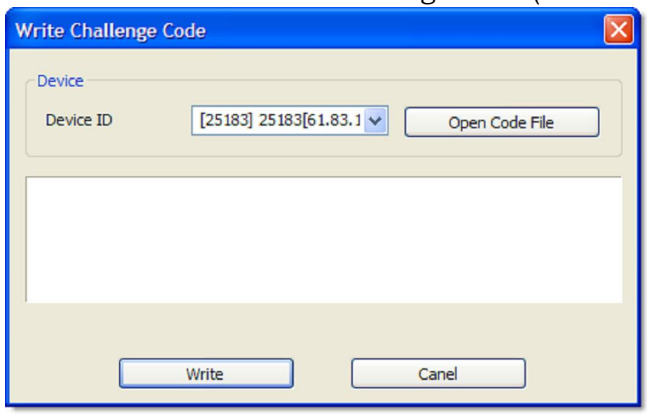


2. Haga click en la casilla de validación Initialize Password (Inicializar contraseña) para activar los botones que se encuentran en la parte inferior de la ventana.
3. Haga click en **Get Challenge Code** (Obtener código de seguridad). Esta acción abrirá la ventana Get Challenge Code (Obtener código de seguridad).



4. Seleccione el dispositivo apropiado de la lista desplegable y haga click en **Get** (Obtener).
5. Haga click en **Save as File** (Guardar como archivo) para guardar el código de seguridad en la computadora.

6. Envíe un e-mail con el código de seguridad a Suprema (*support@supremainc.com*). El personal del soporte técnico de Suprema le enviará un código de desbloqueo por e-mail.
7. Cuando reciba el código de Suprema, abra la ventana Auto Locking (Bloqueo automático) y active los botones (consulte los pasos 1-2).
8. Haga click en **Unlock Device and Password to Default** (Desbloquear dispositivo y predeterminar contraseña). Esta acción abrirá la ventana Write Challenge Code (Escribir código de seguridad).



9 Haga click en **Open Code File** (Abrir archivo con código) y localice el archivo que Suprema le envió.

10 Cuando haya abierto el archivo, haga click en **Write** (Escribir). Esto desbloqueará el dispositivo y devolverá la contraseña de bloqueo a su estado predeterminado (sin contraseña).

4.5 Gestión de usuarios

Con el sistema BioStar, puede eliminar usuarios, transferir usuarios a otras áreas y personalizar los campos que contienen información de usuario. También puede exportar o importar datos de usuario para crear informes personalizados, editar lotes u otras acciones.

4.5.1 Eliminación de usuarios

En caso de ser necesario, puede eliminar usuarios fácilmente desde el sistema BioStar. Para eliminar un usuario:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. Haga click con el botón secundario del ratón en el nombre de un usuario.
3. Haga click en *Delete User* (Eliminar usuario).
4. Haga click en **OK** (Aceptar) para confirmar la eliminación.

4.5.1.1 Eliminación de un usuario mediante tarjetas de comando

Después de expedir tarjetas de comando, puede eliminar un usuario directamente desde un dispositivo BioEntry Plus o Xpass. Para obtener más información acerca de cómo expedir tarjetas de comando, consulte la sección 3.2.5.1 y 3.2.7.1.

Para eliminar usuarios directamente desde un dispositivo BioEntry Plus utilizando tarjetas de comando:

1. Coloque una tarjeta de eliminación (tarjeta de comando) en un dispositivo BioEntry Plus.
2. Si se necesita autorización, un administrador deberá escanear su huella dactilar para continuar.
3. Coloque la tarjeta de acceso del usuario en el dispositivo y luego pida al usuario que coloque el dedo en el escáner (siguiendo las indicaciones del dispositivo).

Para eliminar usuarios directamente desde un dispositivo Xpass utilizando tarjetas de comando:

1. Coloque una tarjeta de eliminación (tarjeta de comando) en un dispositivo Xpass.
2. Si se necesita autorización, un administrador deberá colocar su tarjeta de acceso en el dispositivo para continuar.
3. Coloque la tarjeta de acceso del usuario en el dispositivo.
4. Coloque de nuevo la tarjeta de eliminación en el dispositivo para confirmar la acción.

4.5.1.2 Eliminación de todos los usuarios mediante tarjetas de comando

Después de expedir tarjetas de comando, puede eliminar todos los usuarios directamente desde un dispositivo BioEntry Plus o Xpass. Para obtener más información acerca de cómo expedir tarjetas de comando, consulte la sección 3.2.5.1 y 3.2.7.1.

Para eliminar todos los usuarios directamente desde un dispositivo BioEntry Plus utilizando tarjetas de comando:

1. Coloque una tarjeta de eliminación total (tarjeta de comando) en un dispositivo BioEntry Plus.
2. Si se necesita autorización, un administrador deberá escanear su huella dactilar para continuar.
3. Coloque de nuevo la tarjeta de eliminación total en el dispositivo para confirmar la acción.

Para eliminar todos los usuarios directamente desde un dispositivo Xpass utilizando tarjetas de comando:

1. Coloque una tarjeta de eliminación total (tarjeta de comando) en un dispositivo Xpass.
2. Si se necesita autorización, un administrador deberá colocar su tarjeta de acceso en el dispositivo para continuar.
3. Coloque de nuevo la tarjeta de eliminación total en el dispositivo para confirmar la acción.

4.5.2 Transferencia de usuarios a otra área

BioStar simplifica la transferencia de usuarios a otras áreas. Antes de transferir un usuario, deberá crear un área:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel de navegación, haga click con el botón secundario del ratón en *User* (Usuario).
3. Haga click en *Add Department* (Añadir área).
4. Introduzca un nombre para el área.

Para transferir usuarios a un área, simplemente haga click en el nombre de un usuario y arrástrelo hacia el nombre de un área.

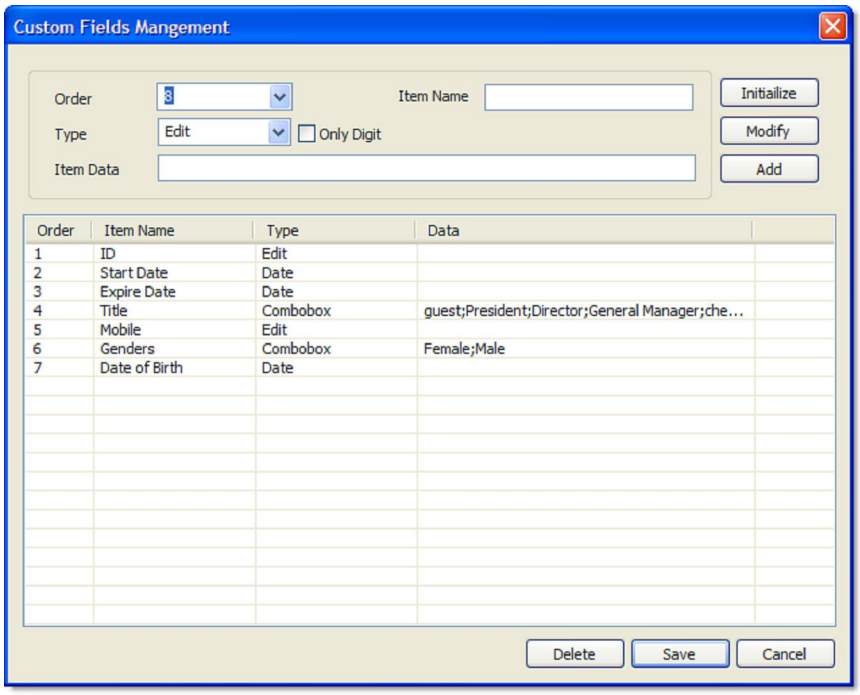
4.5.3 Personalización de los campos que contienen información de usuario

BioStar permite personalizar los campos que contienen información de usuario. Esto puede resultar útil para alterar los campos de información predeterminada o para crear nuevos campos.

4.5.3.1 Adición de nuevos campos de información

Para añadir nuevos campos de información:

1. En la barra de menú, haga click en **Option > User > Custom Field Setting** (Opción > Usuario > Configuración de campo personalizado). Esta acción abrirá la ventana Custom Fields Management (Gestión de campos personalizados).



2. Seleccione un número de orden de la primera lista desplegable (elija un número que no se encuentre en uso).
3. Seleccione un tipo de campo de la segunda lista desplegable. Para restringir el campo a valores numéricos, haga click en la casilla de validación Only Digit (Sólo dígitos)
4. Introduzca los datos y el nombre del campo (por ejemplo, los campos que aparecerán en un cuadro combinado).
5. Haga click en **Add** (Añadir).
6. Repita los pasos 2-5 tantas veces como desee para crear más campos de información.
7. Una vez finalizado, haga click en **Save** (Guardar).

4.5.3.2 Modificación de campos de información existentes

Para modificar campos de información existentes:

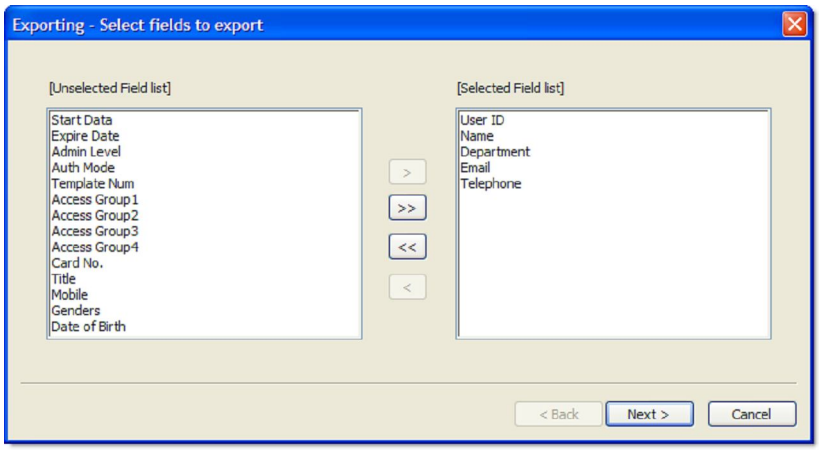
1. En la barra de menú, haga click en **Option > User > Custom Field Setting** (Opción > Usuario > Configuración de campo personalizado). Esta acción abrirá la ventana Custom Fields Management (Gestión de campos personalizados) (consulte la sección 4.5.3.1).
2. Haga click en el campo que desea modificar en la lista que se encuentra en la parte inferior. Los datos aparecerán en los campos de la parte superior de la ventana.
   Nota: los campos 1-4 son campos obligatorios y no se pueden modificar ni eliminar.
3. Modifique los datos como desee.

4. Haga click en **Modify** (Modificar).
5. Repita los pasos 2-4 tantas veces como desee para modificar más campos de información.
6. Una vez finalizado, haga click en **Save** (Guardar).

4.5.4 Exportación de datos de usuario

Los datos exportados de usuario son guardados en un archivo delimitado por comas(CSV) que se puede editar con un editor de texto o con Microsoft Excel. Para exportar datos de usuario:

1. Haga click en **User** (Usuario) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Export User* (Exportar usuario). Esta acción abrirá la ventana Exporting (Exportación).



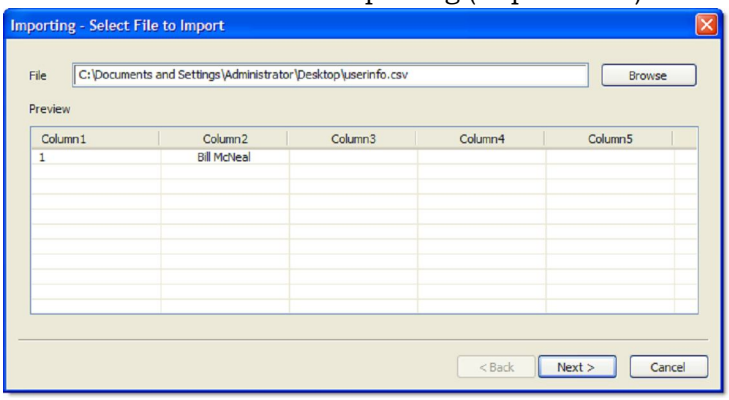
3. Seleccione los tipos de datos de usuario que desea exportar haciendo click en los campos de la lista de la izquierda y luego haciendo click en **>**.
4. Después de seleccionar todos los tipos de datos de usuario para exportar, haga click en **Next** (Siguiente).
5. Escriba una ruta y un nombre de archivo para los datos de usuario o haga click en **Browse** (Examinar) para seleccionar una ubicación en la que guardar el archivo.
6. Haga click en **Next** (Siguiente).
7. Haga click en **Export** (Exportar) para comenzar a exportar los datos de usuario.
8. Una vez se haya completado la exportación, haga click en **Finish** (Finalizar).

4.5.5 Importación de datos de usuario

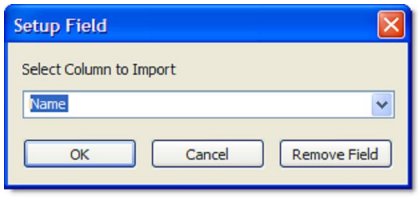
Los datos de usuario en formatos delimitados por comas (CSV) se pueden importar a BioStar. Para importar datos de usuario:

1. Haga click en **User** (Usuario) en el panel de acceso directo.

2. En el panel Task (Tarea), haga click en *Import User* (Importar usuario). Esta acción abrirá la ventana Importing (Importación).



3. Escriba la ruta y el nombre de archivo donde se encuentran ubicados los datos de usuario o haga click en **Browse** (Examinar) para seleccionar un archivo.
4. Haga click en **Next** (Siguiente). Los tipos de datos sin procesar se mostrarán y el campo de lista User (Usuario) volverá al estado predeterminado "Not Use. Click here to change." (No utilizar. Haga click aquí para cambiar.).
5. Haga click en la celda que se encuentra a la derecha de una muestra de datos Esta acción abrirá la ventana Setup Field (Campo de configuración), que permite relacionar los datos sin procesar con un campo de información de usuario en BioStar.



6. Relacione los datos con un campo seleccionando una etiqueta de campo de la lista desplegable y luego haga click en **OK** (Aceptar).
7. Repita los pasos 5 y 6 tantas veces como sea necesario para relacionar más datos.
8. Una vez que haya finalizado de relacionar los datos con los campos, haga click en **Next** (Siguiente).
9. Haga click en **Import** (Importar).
10. Si relaciona los datos con los campos en una cuenta de usuario ya existente, se le pedirá que confirme si desea sobrescribir los datos. Haga click en **Yes** (Sí) o en **Yes to All** (Sí a todo) para confirmar, o haga click en **No** o en **No to All** (No a todo) para denegar.
11. Haga click en **Finish** (Finalizar).

4.6 Gestión de tiempo y asistencia

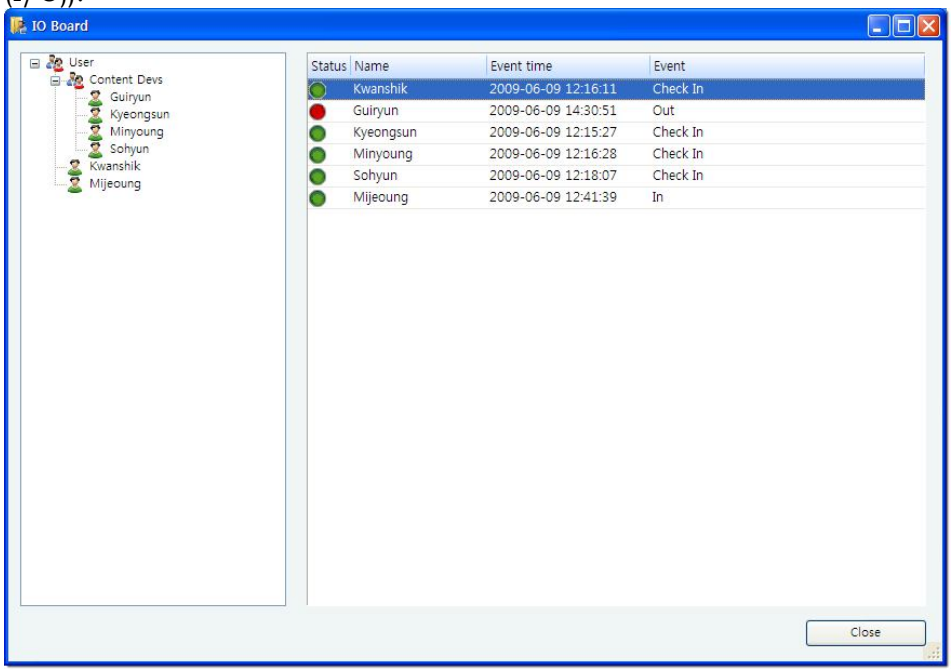
BioStar permite supervisar el estado de tiempo y asistencia de los usuarios y generar reportes de eventos de tiempo y asistencia, que puede editar o exportar según sea necesario.

4.6.1 Supervisión del estado de tiempo y asistencia mediante IO Board (Placa de entradas/salidas (I/O))

La placa de entradas/salidas (I/O) muestra los eventos de tiempo y asistencia sólo para los eventos de entrada y salida realizados utilizando las teclas de función de tiempo y asistencia de los dispositivos de control de acceso. Esta función sólo está disponible en la edición estándar de BioStar.

Puede utilizar la tabla para verificar las actividades de tiempo y asistencia recientes o decidir rápidamente los usuarios que checan la entrada y la salida. Los usuarios pueden utilizar la tabla para visualizar sus propias actividades de tiempo y asistencia. Para supervisar el estado de tiempo y asistencia de los usuarios:

1. Haga click en la opción **Time and Attendance** (Tiempo y asistencia) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *IO Board* (Placa de entradas/salidas (I/O)). Esta acción abrirá la ventana IO Board (Placa de entradas/salidas (I/O)).

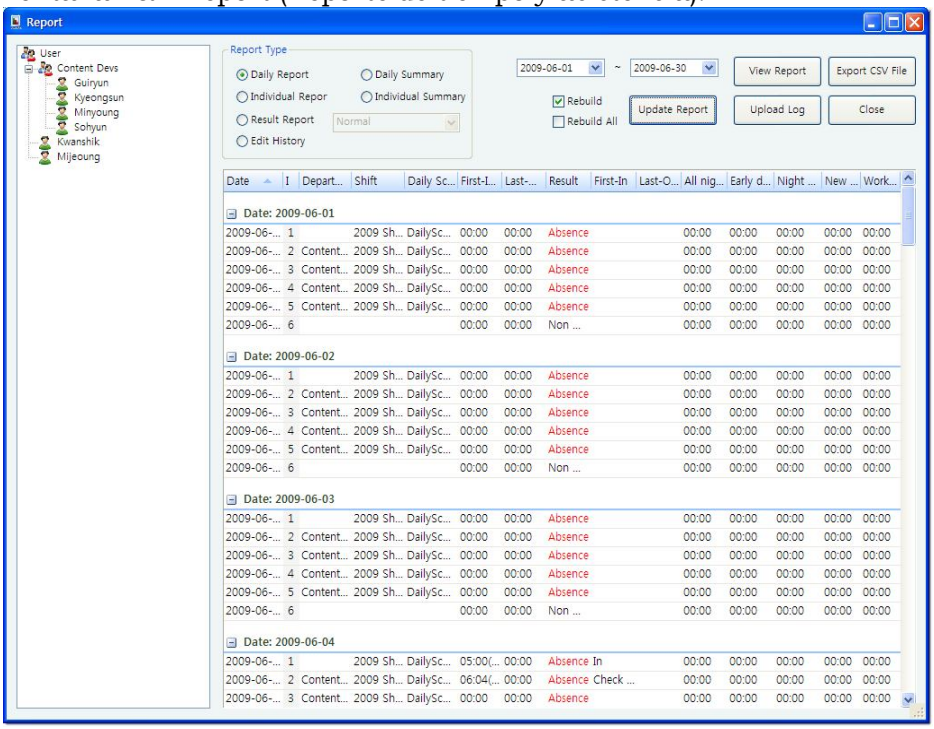


3. Haga click en **User** (Usuario), en el nombre de un usuario o en el nombre de un área del panel de la izquierda. Esta acción mostrará el estado de tiempo y asistencia correspondiente en el panel de la derecha.
4. Para cerrar la ventana, haga click en **Close** (Cerrar).

4.6.2 Generación de reportes de tiempo y asistencia

Puede generar reportes de tiempo y asistencia para visualizar diversos eventos de tiempo y asistencia de usuarios. También puede modificar e imprimir datos de tiempo y asistencia para otros usos como, por ejemplo, para calcular nóminas.
Para generar reportes de tiempo y asistencia:

1. Haga click en la opción **Time and Attendance** (Tiempo y asistencia) en el panel de acceso directo.
2. En el panel Task (Tarea), haga click en *Report* (Reporte). Esta acción abrirá la ventana T&A Report (Reporte de tiempo y asistencia).



3. Haga click en un botón de radio para seleccionar un tipo de reporte:
   - **Daily Report** (Reporte diario): es un reporte, clasificado por fecha, de todas las actividades para el período determinado.
   - **Individual Report** (Reporte individual): es un reporte, clasificado por Id. de usuario, de actividades para el período determinado.
   - **Result Report** (Reporte de resultado): es un reporte de actividades que se especifican utilizando la lista desplegable.
   - **Edit History** (Historial editado): es un reporte de entradas editadas.
   - **Daily Summary** (Resumen diario): es un resumen, clasificado por fecha, de actividades para el período determinado.
   - **Individual Summary** (Resumen individual): es un resumen, clasificado por Id. de usuario, de actividades para el período determinado.
4. Seleccione un período haciendo click en los calendarios desplegables.

5. Haga click en **View Report** (Visualizar informe) para obtener y mostrar los resultados.

Nota: haga click en **Upload Log** (Subir registro) para obtener los datos de todos los dispositivos conectados en red. Haga click en **Update Report** (Actualizar reporte) para actualizar el reporte con cualquier dato que haya modificado (consulte la sección 4.5.3).

Puede clasificar los datos del reporte haciendo click en cualquier encabezado de columna (la clasificación alternará entre orden ascendente y descendente). También puede reorganizar las columnas arrastrando y soltando los encabezados de columna en un nuevo lugar. Además, puede añadir o eliminar columnas mediante el menú que aparece cuando hace click con el botón secundario del ratón en cualquier encabezado de columna:

Para añadir una columna al reporte:

1. Haga click con el botón secundario del ratón en cualquier encabezado de columna.
2. Haga click en **Column** (Columna) y seleccione una columna para añadir al reporte.

Para eliminar una columna del reporte:

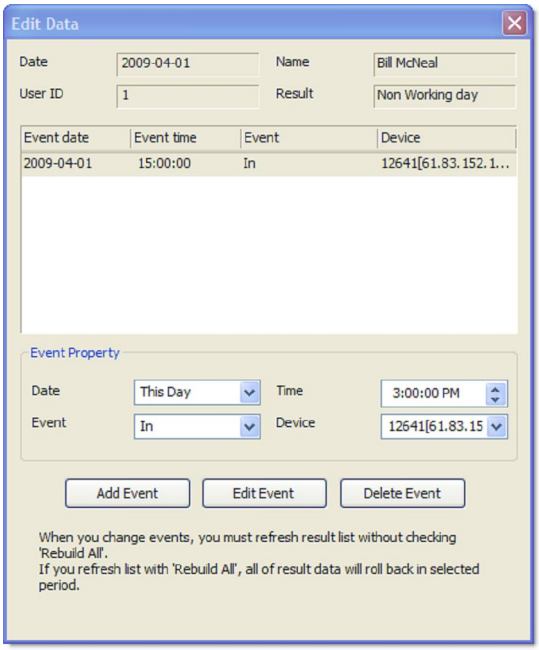
1. Haga click con el botón secundario del ratón en la columna que desea eliminar.
2. Haga click en **Remove column** (Eliminar columna).

4.6.3 Modificación de reportes de tiempo y asistencia

Los datos de tiempo y asistencia se pueden modificar con fines de reportes de tiempo o nóminas. Después de generar un reporte de tiempo y asistencia, puede localizar y hacer click en las celdas que desea modificar e introducir un nuevo valor o seleccionar una opción de la lista desplegable. Esta acción guardará la modificación realizada en el reporte, pero no sobrescribirá los datos originales recopilados de los dispositivos de control de acceso. Si desea generar el reporte con los datos originales, haga click en la casilla de validación que se encuentra junto a "Rebuild" (Reconstruir) y luego haga click en **Update Report** (Actualizar reporte).

Para modificar detalles en los datos del reporte:

1. Genere un reporte de tiempo y asistencia tal y como se describe en la sección 4.5.2.
2. Haga click con el botón secundario del ratón en una celda y haga click en *Detailed editing* (Edición detallada). Esta acción abrirá la ventana Edit Data (Editar datos).



3. Para editar un evento, cambie las siguientes propiedades de evento según sea necesario y luego haga click en **Edit Event** (Editar evento). Para añadir un evento, cambie las siguientes propiedades de evento según sea necesario y luego haga click en **Add Event** (Añadir evento). Para eliminar el evento, haga click en **Delete Event** (Eliminar evento).
   - **Date** (Fecha): seleccione si el evento ocurrió en este día o en el día siguiente.
   - **Event** (Evento): seleccione el tipo de evento.
   - **Time** (Hora): establezca la hora del evento.
   - **Device** (Dispositivo): establezca el dispositivo donde ocurrió el evento.
4. Cuando haya finalizado de modificar los datos de evento, haga click en "X", en la esquina superior derecha para cerrar la ventana.
5. En la ventana T&A Report (Reporte de tiempo y asistencia), asegúrese de que la casilla de validación "Rebuild" (Reconstruir) NO está seleccionada.
6. Haga click en **Update Report** (Actualizar reporte). El reporte mostrará los cambios realizados. Los cambios realizados mediante la edición detallada no se restaurarán aunque haga click en la casilla de validación que se encuentra junto a "Rebuild" (Reconstruir) y haga click en **Update Report** (Actualizar reporte). Si desea generar el reporte con los datos originales, haga click en las casillas de validación que se encuentran junto a "Rebuild" (Reconstruir) y "Rebuild All" (Reconstruir todo) y luego haga click en **Update Report** (Actualizar reporte).

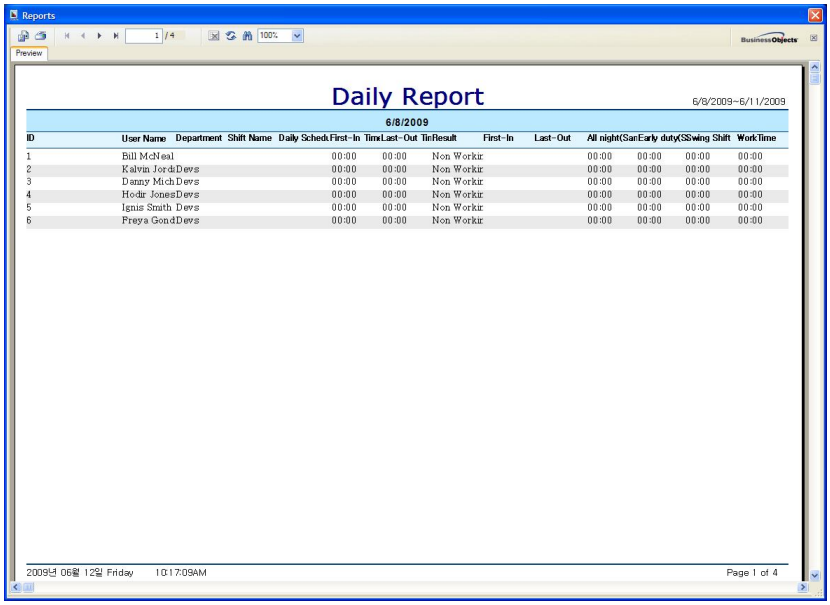
Nota: Puede clasificar los datos del reporte haciendo click en cualquier encabezado de columna (la clasificación alternará entre orden ascendente y descendente). También puede

reorganizar las columnas arrastrando y soltando los encabezados de columna en un nuevo lugar.

4.6.4 Impresión o exportación de los datos del reporte de tiempo y asistencia

Para imprimir o exportar los datos del reporte de tiempo y asistencia:

1. Genere un reporte de tiempo y asistencia tal y como se describe en la sección 4.5.2 y realice las modificaciones necesarias tal y como se describe en la sección 4.5.3.
2. Haga click en **View Report** (Visualizar reporte). Esta acción abrirá una ventana de vista previa, parecida a la siguiente:



4. Para imprimir el reporte, haga click en el símbolo de impresora en la barra de herramientas.
5. Para exportar los datos de reporte, haga click en el símbolo de exportar en la barra de herramientas y luego seleccione un formato y un destino de exportación. Puede exportar datos en los siguientes formatos:
   - Adobe Acrobat (PDF)
   - Crystal Report (RPT)
   - HTML 3.2 o 4.0
   - Microsoft Excel 97-2000 o Microsoft Excel 97-2000–solo datos (XLS)
   - Microsoft Word o Microsoft Word–editable (RTF)
   - Open Database Connectivity (ODBC)
   - Record Style–columnas con espacios (REC)
   - Definición de reporte (TXT)
   - Formato de texto enriquecido (RTF)
   - Valores separados por comas (CSV)

- Texto separado por tabuladores (TTX)
- Texto (TXT)
- XML

Nota: puede actualizar los datos del reporte haciendo click en el símbolo de actualización de la barra de herramientas. También puede buscar texto en el reporte haciendo click en el símbolo de búsqueda (binoculares) de la barra de herramientas.

4.7 Gestión de dispositivos

En caso de ser necesario, puede eliminar fácilmente los dispositivos y actualizar el firmware del dispositivo directamente desde la interfaz de BioStar. Cuando elimine dispositivos, primero asegúrese de que se haya transferido al servidor de BioStar cualquier dato nuevo que se haya podido añadir en la terminal.

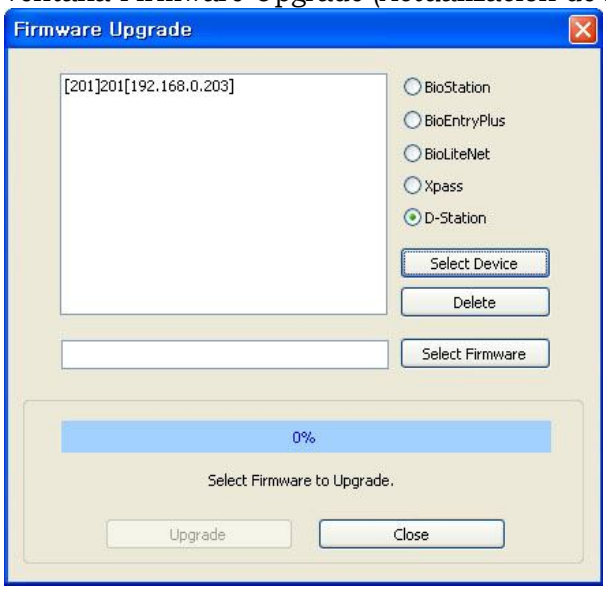
4.7.1 Eliminación de dispositivos

Si necesita eliminar un dispositivo del sistema BioStar, haga click en **Device** (Dispositivo) en el panel de acceso directo y luego haga click con el botón secundario del ratón en*Remove Device* (Eliminar dispositivo).

4.7.2 Actualización del firmware del dispositivo

A veces es necesario actualizar los dispositivos con la última versión del firmware. Para actualizar el firmware del dispositivo:

1. En la barra de menú, haga click en **Option > Device > Firmware Upgrade** (Opción > Dispositivo > Actualización de firmware). Esta acción abrirá la ventana Firmware Upgrade (Actualización de firmware).



2. Haga click en el botón de radio que se encuentra a lado del tipo de dispositivo que desea actualizar.

3. Haga click en **Select Device** (Seleccionar dispositivo) y seleccione uno o más dispositivos en la ventana Device Tree (Árbol de dispositivos).
4. Haga click en **OK** (Aceptar) para cerrar la ventana Device Tree (Árbol de dispositivos).
5. Haga click en **Select Firmware** (Seleccionar firmware).
6. Localice el archivo del firmware en la computadora o en la red y haga click en **Open** (Abrir).
7. Haga click en **Upgrade** (Actualizar).
8. Cuando la actualización del firmware se haya completado, espere a que el dispositivo se reinicie y luego haga click en **Close** (Cerrar).

4.7.3 Desactualizar el firmware del dispositivo

Los dispositivos pueden no trabajar adecuadamente si sufren una desactualización o una reversión de firmware. Suprema no recomienda la desactualización. Si los dispositivos requieren de una desactualización, póngase en contacto con el soporte técnico de Suprema (e-mail: support@supremainc.com) o con un distribuidor, directo o local, de Suprema.

4.8 Activación de la encriptación de huellas dactilares

La encriptación adicional de huellas dactilares se encuentra desactivada de forma predeterminada. En la mayoría de los casos no es necesario activar esta encriptación. Sin embargo, puede decidir activar la encriptación para proporcionar una seguridad o privacidad extra. Recuerde que la activación de la encriptación de huellas dactilares necesita administrar las claves de encriptación y solo usuarios avanzados deberían realizarla.

Activar la encriptación de huellas dactilares invalidará cualquier plantilla guardada anteriormente. Por lo tanto, es mejor activar la encriptación antes de registrar usuarios. Para activar la encriptación de huellas dactilares:

1. En la barra de menú, haga click en **Option > Fingerprint** (Opción > Huella dactilar). Esta acción abrirá la ventana Fingerprint (Huella dactilar).
2. Haga click en la casilla de validación que se encuentra en "Security Option" para activar la encriptación de la plantilla de huellas dactilares.
3. Haga click en **Yes** (Sí) para aceptar el mensaje de aviso.
4. Si lo desea, también puede cambiar la clave de encriptación:
   a. Haga click en **Encryption Key** (Clave de encriptación). Esta acción abrirá la ventana Change Encryption Key (Cambiar clave de encriptación).
   b. Introduzca una nueva clave de encriptación en el primer campo.
   c. Introduzca la clave en el segundo campo para confirmarla.

d. Haga click en **Change** (Cambiar).

5. Haga click en **Save** (Guardar). La opción elegida aparecerá en la pestaña Fingerprint (Huella dactilar) en el panel Device (Dispositivo).

4.9 Cambio de la plantilla de huellas dactilares

BioStar ofrece dos tipos de plantillas de huellas dactilares: el formato ISO 19794-2 o el formato propietario de Suprema. El formato de Suprema es el formato activo predeterminado. Cambiar las opciones de la plantilla de huellas dactilares invalidará cualquier plantilla guardada anteriormente. Por lo tanto, es mejor elegir una opción de plantilla antes de registrar usuarios. Para cambiar la opción de la plantilla de huellas dactilares:

1. En la barra de menú, haga click en **Option > Fingerprint** (Opción > Huella dactilar). Esta acción abrirá la ventana Fingerprint (Huella dactilar).
2. Haga click en la casilla de validación en “Template Format Option” (Opción de formato de plantilla) para seleccionar el formato ISO.
3. Haga click en **Yes** (Sí) para aceptar el mensaje de aviso.
4. Haga click en **Save** (Guardar).

05 Personalización de la configuración

Esta sección describe la configuración disponible en el software BioStar. BioStar proporciona un control preciso y una personalización del sistema de control de acceso mediante la configuración de las funciones de los dispositivos, los comportamientos de puertas y zonas, y las cuentas de usuario.

5.1 Personalización de la configuración de los dispositivos

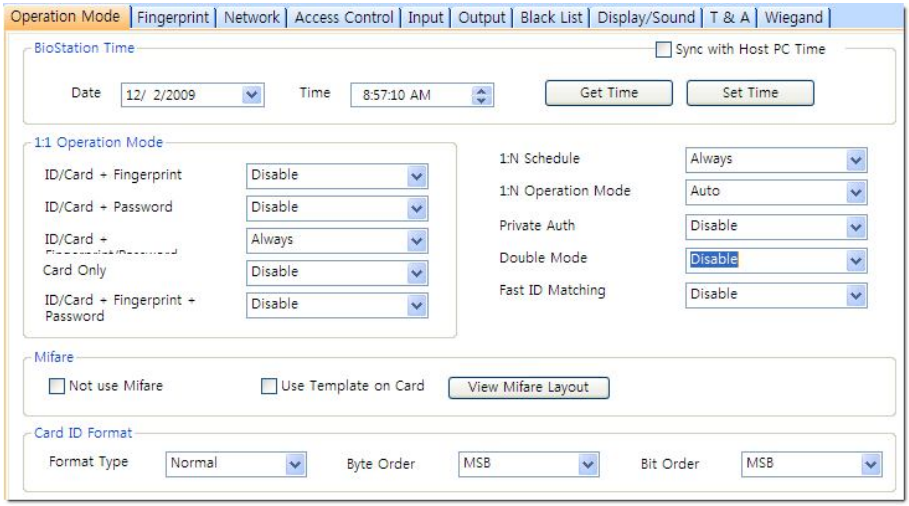
Mientras que la configuración de dispositivos es similar en BioStation, BioEntry Plus, BioLite Net, Xpass, y D-Station, estos presentan pequeñas diferencias. Las siguientes secciones describen la configuración por separado de cada uno de los dispositivos. Para acceder a las pestañas descritas a continuación, haga click en **Device** (Dispositivo) en el panel de acceso directo y luego haga click en el nombre de un dispositivo.

5.1.1 Personalización de la configuración para dispositivos BioStation

Las siguientes secciones describen la configuración disponible para los dispositivos BioStation. Personalice la forma en que funcionan los dispositivos BioStation cambiando la configuración para que estos se adapten al entorno y a las necesidades operacionales particulares.

5.1.1.1 Pestaña Operation Mode (Modo de funcionamiento)

La pestaña Operation Mode (Modo de funcionamiento) permite personalizar la configuración de la hora y de varios modos de funcionamiento en los dispositivos BioStation.



- **BioStation Time (Hora de BioStation)**
  - **Date** (Fecha): establezca manualmente la fecha del dispositivo en el calendario desplegable.
  - **Time** (Hora): establezca manualmente la hora del dispositivo.
  - **Sync with Host PC Time** (Sincronizar con la hora de la computadora central): seleccione esta casilla de validación para sincronizar automáticamente la hora del dispositivo con la hora de la computadora central.
  - **Get Time** (Obtener hora): obtenga la hora actual mostrada en el dispositivo.
  - **Set Time** (Establecer hora): establezca la hora del dispositivo.
- **1:1 Operation Mode** (Modo de funcionamiento 1:1): las listas desplegables de esta sección permiten controlar el modo de autentificación por programa. Por ejemplo, puede elegir un modo de autentificación normal para horas de trabajo, y un modo de autentificación más estricto para horas fuera del programa normal. Puede especificar modos de autentificación por dispositivo o por usuario (consulte la sección 5.4.1). A menos que se especifique un modo particular para un usuario, se aplicará el modo de autentificación del dispositivo.

- **ID/Card + Fingerprint** (Id./Tarjeta + Huella dactilar): configure el dispositivo para que solicite una Id. o una tarjeta además de la autorización con huella dactilar (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
- **ID/Card + Password** (Id./Tarjeta + Contraseña): configure el dispositivo para que solicite una Id. o una tarjeta además de la autorización con contraseña (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
- **ID/Card + Fingerprint/Password** (Id./Tarjeta + Huella dactilar/Contraseña): configure el dispositivo para que solicite una Id. o una tarjeta además de la autorización con huella dactilar o contraseña(*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
- **Card Only** (Solo tarjeta): configure el dispositivo para que solo solicite la autorización con tarjeta (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
- **ID/Card + Fingerprint + Password** (Id./Tarjeta + Huella dactilar + Contraseña): configure el dispositivo para que solicite una Id. o una tarjeta además de la autorización con huella dactilar y contraseña(*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).

• **Mifare** (solo disponible en dispositivos BioStation Mifare)
- **Not use Mifare** (No utilizar Mifare): seleccione esta casilla de validación para deshabilitar la autorización con tarjeta MIFARE.
- **Use Template on Card** (Utilizar plantilla en tarjeta): seleccione esta casilla de validación para que se utilice la plantilla en la tarjeta MIFARE en la autorización.
- **View Mifare Layout** (Visualizar distribución Mifare): haga click en este botón para visualizar la distribución MIFARE utilizada por el dispositivo. Para obtener más información acerca de cómo configurar la distribución MIFARE, consulte la sección 3.5.4.6.

• **Card ID Format (Formato de el id. de tarjeta)**
- **Format Type** (Tipo de formato): establezca el tipo de procesamiento previo de los datos de el id. de una tarjeta (*Normal* o *Wiegand*). Si se selecciona “Normal”, los datos de el id. de una tarjeta se procesarán en su forma original. Si se selecciona “Wiegand”, los dispositivos interpretarán los datos de el id. de una tarjeta según la configuración del formato Wiegand.

- **Byte Order** (Orden de bytes): especifique si desea intercambiar los datos de las tarjetas con Id. entre las tarjetas y los dispositivos por byte más significativo (*MSB*) o por byte menos significativo (*LSB*).
- **Bit Order** (Orden de bits): especifique si desea intercambiar los datos de las tarjetas con Id. entre las tarjetas y los dispositivos por bit más significativo (*MSB*) o por bit menos significativo (*LSB*).

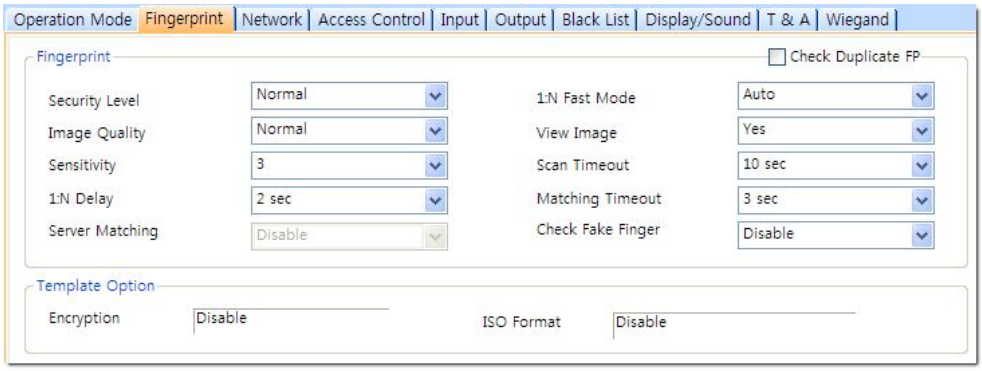
• **Otras opciones**

- **1:N Schedule** (Programa 1:N): establezca un programa para utilizar solamente la autentificación con huella dactilar (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
- **1:N Operation Mode** (Modo de funcionamiento 1:N): establezca un método para activar el sensor de huellas dactilares (*Auto* (Automático), *Ok/Function Key* (Aceptar/Clave de función), o *None* (Ninguno)).
- **Private Auth** (Autorización privada): configure el dispositivo para permitir un método de autorización privada (*Disable* (Deshabilitar) o *Enable* (Habilitar)). Si se habilita, el modo de autentificación del usuario se determinará por la configuración de la autorización (Authorization) de un usuario, que se encuentra en la pestaña Details (Detalles). Si se deshabilita, el modo de autentificación se determinará por la configuración del modo de funcionamiento del dispositivo.
- **Double Mode** (Modo doble): configure el dispositivo para que solicite la autentificación de dos tarjetas de acceso o huellas dactilares de usuarios (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)). El tiempo de espera para presentar la segunda autentificación es de 15 segundos.
- **Fast ID Matching** (Identificación de Id. rápida): configure el dispositivo para permitir una autentificación más rápida, solicitando a los usuarios que solo introduzcan los dos primeros dígitos de el id. de usuario y que solo escaneen una huella dactilar (*Enable* (Habilitar) o *Disable* (Deshabilitar)). Esta opción sirve para autentificar a un grupo más pequeño de usuarios (solo a aquellos con los mismos primeros dos dígitos en sus Id. de usuario) para aumentar la velocidad de la identificación.

  Nota: esta opción no es compatible con la identificación de servidor (consulte la sección 5.1.1.2). Cuando utilice las teclas de función para los eventos de tiempo y asistencia (consulte la sección 5.1.1.8), sólo estarán habilitadas las teclas F1-F4 (BioStation V1.7 y posterior).

5.1.1.2 Pestaña Fingerprint (Huella dactilar)

La pestaña Fingerprint (Huella dactilar) permite personalizar la configuración de la autorización con huella dactilar para los dispositivos BioStation.



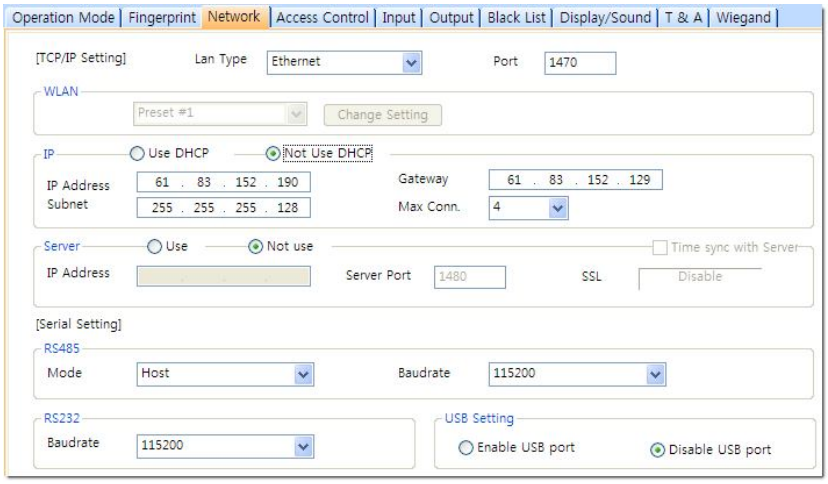
- **Fingerprint (Huella dactilar)**
  - **Security Level** (Nivel de seguridad): establezca el nivel de seguridad que utilizar para la autorización con huella dactilar (*Normal* (Normal), *Secure* (Seguro), or *Most Secure* (Muy seguro)). Recuerde que cuanto más alto sea el nivel de seguridad, más posibilidades hay de que se produzcan falsos rechazos.
  - **Image Quality** (Calidad de imagen): establezca la rigurosidad de la comprobación de calidad para las lecturas de las huellas dactilares (*Weak*(Débil), *Normal* (Normal), o *Strict* (Estricto)). Si la imagen de una huella dactilar está por debajo del nivel de calidad, será rechazada.
  - **Sensitivity** (Sensibilidad): configure la sensibilidad del escáner para huellas dactilares (de *0 [Min]* (0 [mín.]) a *7 [Max]* (7 [máx.]). Si se establece una mayor sensibilidad, las huellas dactilares se capturarán más fácilmente, pero también aumentará la sensibilidad al ruido externo.
  - **1:N Delay** (Retraso 1:N): establezca el retraso entre los escáneres cuando identifique las huellas dactilares (de *0 sec* (0 s) a *10 sec* (10 s)). Este retraso evitará que el escáner procese la misma huella dactilar más de una vez en caso de que un usuario no haya retirado para entonces su dedo del escáner.
  - **1:N Fast Mode** (Modo rápido 1:N): configure el dispositivo para utilizar el modo rápido y reducir así el tiempo requerido para identificar las huellas dactilares (*Auto* (Automático), *Normal*, *Fast* (Rápido) o *Fastest* (Muy rápido)). Si se establece en modo *Auto* (Automático), la velocidad de identificación se ajustará automáticamente según el número de plantillas registradas.

- **View Image** (Visualizar imagen): configure si quiere mostrar u ocultar las imágenes de las huellas dactilares en la pantalla de BioStation (*Yes* (Sí) o *No*).
- **Scan Timeout** (Tiempo de espera del escáner): configure el tiempo que debe transcurrir antes de que expire el tiempo del escáner de las huellas dactilares (de *1 sec* (1 s) a *20 sec* (20 s)). Si un usuario no coloca el dedo en el dispositivo durante el tiempo de espera, se producirá un fallo en la autorización.
- **Matching Timeout** (Tiempo de espera de la identificación): configure el tiempo que deberá transcurrir antes de que expire el tiempo del dispositivo para intentar identificar una huella dactilar (de *0 [Infinite]* (0 [Infinito] a *10 sec* (10 s)).
- **Server Matching** (Identificación de servidor): active esta opción para identificar una huella dactilar o el id. de una tarjeta en el servidor BioStar, en lugar de en el dispositivo. Cuando se activa este modo, los dispositivos envían las plantillas de las huellas dactilares o las Id. de la tarjeta al servidor para verificar la identificación. Este modo resulta útil cuando posee más usuarios de los que se pueden descargar a un dispositivo, o cuando la información de usuario no se puede distribuir por motivos de seguridad.
- **Check Fake Finger** (Comprobar dedo falso): configure el dispositivo para que detecte el uso de huellas dactilares falsas como, por ejemplo, las fabricadas con silicona o hule, y prevenir así un acceso no autorizado.

- **Check Duplicate FP** (Comprobar huellas dactilares duplicadas): configure el dispositivo para que determine si una huella dactilar ha sido o no registrada anteriormente. Si el dispositivo determina que una huella dactilar ha sido registrada anteriormente, se producirá un fallo en el proceso de registro.

5.1.1.3 Pestaña Network (Red)

La pestaña Network (Red) permite personalizar la configuración del servidor y de la red para los dispositivos BioStation.

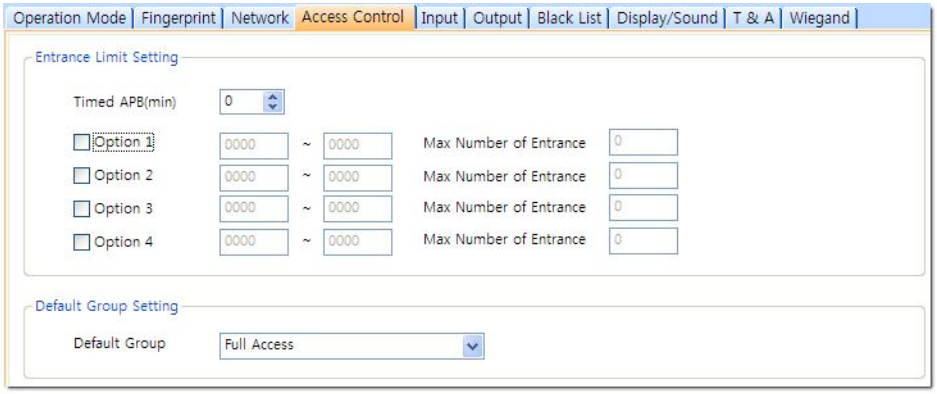


- **TCP/IP Setting (Configuración TCP/IP)**
  - **LAN Type** (Tipo de LAN): seleccione un tipo de conexión LAN de la lista desplegable (*Disable* (Deshabilitar), *Ethernet*, o *Wireless LAN*).
  - **Port** (Puerto): especifique un puerto para utilizar el dispositivo.
  - **WLAN** : seleccione una configuración de WLAN predeterminada de la lista desplegable. Esta opción solo está activa cuando se selecciona WLAN como la configuración de TCP/IP.
  - **Change setting** (Cambiar configuración): haga click para especificar los parámetros de una red de área local inalámbrica (WLAN). Esta opción solo está activa cuando se selecciona WLAN como la configuración de TCP/IP. Para obtener más información acerca de cómo configurar los parámetros de una conexión WLAN, consulte la sección 3.2.4.1.
  - **Use DHCP** (Utilizar DHCP): haga click en este botón de radio para habilitar el protocolo de configuración de host dinámico (DHCP) en el dispositivo.
  - **Not Use DHCP** (No utilizar DHCP): haga click en este botón de radio para deshabilitar el protocolo de configuración de host dinámico (DHCP) en el dispositivo.
  - **IP Address** (Dirección IP): especifique una dirección IP para el dispositivo.
  - **Subnet** (Subred): especifique una dirección de subred para el dispositivo.
  - **Gateway** (Puerta de enlace): especifique una puerta de enlace de red.

  - **Max Conn.** (Conexiones máximas): especifique el número máximo de conexiones permitidas.
- **Server (Servidor)**
  - **Use** (Utilizar): haga click en este botón de radio para habilitar el modo servidor.
  - **Not use** (No utilizar): haga click en este botón de radio para deshabilitar la configuración del servidor.
  - **IP Address** (Dirección IP): especifique una dirección IP para el servidor BioStar.
  - **Server Port** (Puerto del servidor): especifique el puerto utilizado para conectarse al servidor.
  - **SSL**: muestra el estado de SSL para la conexión del servidor.
  - **Time sync with Server** (Sincronizar hora con servidor): seleccione esta casilla de validación para sincronizar la hora del dispositivo con la hora del servidor.
- **RS485**
  - **Mode** (Modo): configure el modo de un dispositivo conectando mediante RS485 (*Disable* (Deshabilitar), *Host* (Anfitrión), *Slave* (Esclavo) o *PC Connection* (Conexión de PC)). Para obtener más información acerca de los modos RS485, consulte las secciones 3.2.1 y 3.2.2.
  - **Baudrate** (Velocidad de transmisión): configure la velocidad en baudios de un dispositivo conectado mediante RS485 (de *9600* a *115200*).
- **RS232** : configure la velocidad en baudios de un dispositivo conectado mediante RS232 (de 9600 a 115200).
- **USB Setting** (Configuración de USB): haga click en los botones de radio para habilitar o deshabilitar el puerto USB en el dispositivo BioStation.

5.1.1.4 Pestaña Access Control (Control de acceso)

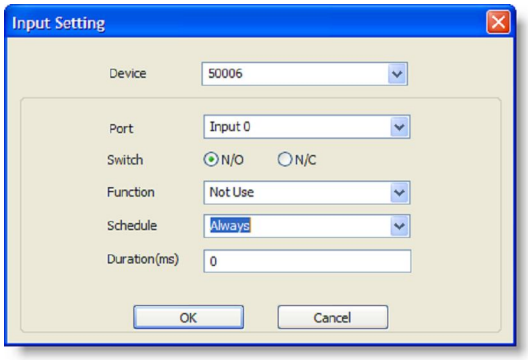
La pestaña Access Control permite personalizar la configuración del límite de entrada y de los grupos de acceso predeterminados para un dispositivo BioStation.



- **Entrance Limit Setting (Configuración del límite de entrada)**
  - **Timed APB (min)** (APB programado (min)): establezca el tiempo (en minutos) en que un usuario no podrá volver a entrar a una zona mediante el dispositivo. Una vez que un usuario haya conseguido entrar, el dispositivo rechazará la tarjeta o la huella dactilar del usuario durante el período de tiempo determinado aquí.
  - **Option 1-4** (Opción 1-4): haga click en la casilla de validación para habilitar el límite de entrada y luego especifique las horas efectivas para el mismo.
  - **Max Number of Entrance** (Número máximo de entradas): establezca el número máximo de entradas permitidas durante el límite de tiempo determinado.
- **Default Group Setting** (Configuración del grupo predeterminado): seleccione un grupo de acceso predeterminado para aplicar a los usuarios nuevos que no han sido asignados a ningún grupo de acceso.

5.1.1.5 Pestaña Input (Entrada)

La pestaña Input (Entrada) muestra los parámetros de entrada especificados para un dispositivo BioStation. Los botones que se encuentran en la parte inferior de la pestaña permiten añadir, modificar o eliminar parámetros de entrada. Para añadir o modificar los parámetros, debe especificarlos en la ventana Input Setting (Configuración de entrada). (Cerrar puerta). Para obtener más información acerca de cómo configurar los parámetros de entrada, consulte la sección 3.9.3.2.

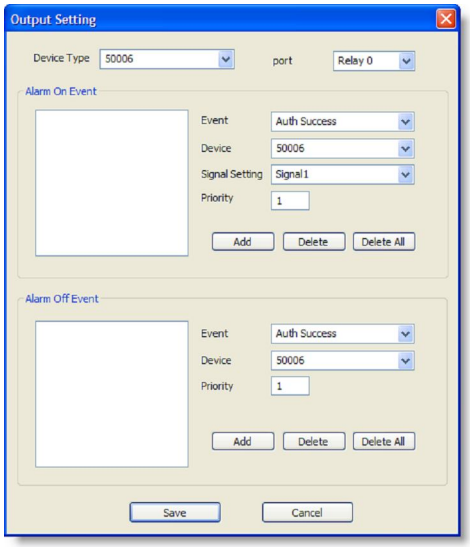


- **Device** (Dispositivo): seleccione el dispositivo BioStation (o Secure I/O) al que desea añadir o modificar los parámetros.
- **Port** (Puerto): seleccione un puerto de entrada (Input 0 (Entrada 0), Input 1 (Entrada 1), o Tamper (Alterar)). Para dispositivos Secure I/O, los siguientes parámetros están disponibles: Input 0 (Entrada 0), Input 1 (Entrada 1), Input 2 (Entrada 2), Input 3 (Entrada 3).
- **Switch** (Interruptor): haga click en los botones de radio para especificar la posición normal del interruptor de entrada (N/O: normalmente abierto o N/C: normalmente cerrado).
- **Function** (Función): seleccione la opción asociada a la entrada:
  - **Not Use** (No utilizar): el puerto de entrada no será supervisado.
  - **Generic Input** (Entrada genérica): el puerto de entrada se supervisará para una acción desencadenadora (para los eventos especificados con “Detect Input 0-3” (Detectar entrada 0-3), en la ventana Output settings (Configuración de salida), consulte la sección 5.1.1.6).
  - **Emergency Open** (Apertura de emergencia): abre las puertas controladas por este dispositivo. El período de apertura normal de puertas será ignorado y las puertas permanecerán abiertas hasta que un operador envíe la orden "Close Door" (Cerrar puerta) mediante la pestaña Door/Zone Monitoring (Supervisión de puerta/zona) (consulte la sección 4.4.1).
  - **Release All Alarms** (Cancelar todas las alarmas): cancela las alarmas asociadas a este dispositivo.
  - **Restart Device** (Reiniciar dispositivo): reinicia el dispositivo.
  - **Disable Device** (Deshabilitar dispositivo): deshabilita el dispositivo. Un dispositivo deshabilitado no se comunicará con el servidor BioStar ni procesará huellas dactilares ni tarjetas. Para habilitar de nuevo la comunicación, un administrador debe introducir la contraseña maestra para un dispositivo BioStar o proporcionar autentificación de forma local para un dispositivo BioEntry Plus.

- **Schedule** (Programa): configure el programa en el que se supervisarán las entradas (*Always* (Siempre), Disable (Deshabilitar), o Custom Schedule (programa personalizado)).
- **Duration (ms)** (Duración (ms)): establezca la duración (en milisegundos) que una entrada debe durar para activar la acción establecida.

5.1.1.6 Pestaña Output (Salida)

La pestaña Output (Salida) muestra los parámetros de salida especificados para un dispositivo BioStation. Los botones que se encuentran en la parte inferior de la pestaña permiten añadir, modificar o eliminar parámetros de salida. Para añadir o modificar los parámetros, debe especificarlos en la ventana Output Setting (Configuración de salida). Para obtener más información acerca de cómo configurar los parámetros de salida, consulte la sección 3.9.3.1.



- **Device Type** (Tipo de dispositivo): seleccione el tipo de dispositivo al que añadirá o modificará los parámetros.
- **Port** (Puerto): seleccione un puerto de salida (Relay 0). Para dispositivos Secure I/O, los siguientes parámetros están disponibles: Relay 0 o Relay 1.
- **Alarm On Event** (Evento para activar alarma): especifique la configuración y haga click en **Add** (Añadir) para añadir el evento a la lista Alarm On Event (Evento para activar alarma). Estos eventos activarán una alama.
  - **Event** (Evento): seleccione el evento que activará la alarma (*Auth Success* (Autorización con éxito), *Auth Fail* (Autorización fallida), *Auth Duress* (Autorización de peligro), *Anti-passback Fail*

(Antipassback fallido), *Access Not Granted* (Acceso no permitido), *Entrance Limited* (Entrada limitada), *Admin Auth Success* (Autorización de administrador con éxito), *Tamper On* (Alteración activada), *Door Opened* (Puerta abierta), *Door Close* (Puerta cerrada), *Forced Open Door* (Puerta forzada abierta), *Held Open Door* (Puerta mantenida abierta), *Detect Input #1-3* (Detectar entrada #1-3)).

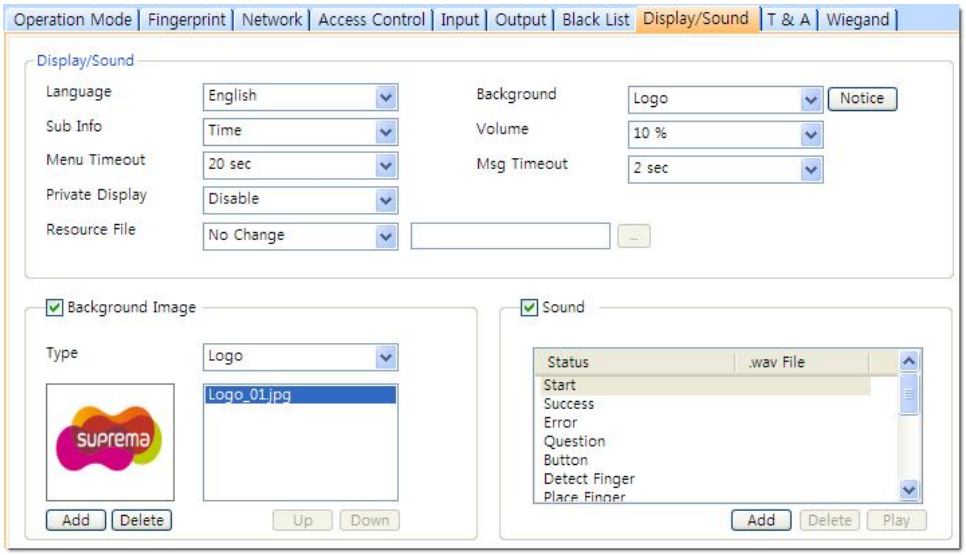
- **Device** (Dispositivo): seleccione el dispositivo supervisado para un evento de alarma.
- **Signal Setting** (Configuración de señal): seleccione una opción de señal anteriormente configurada en la barra de menú (**Option > Event > Output Port Setting** (Opción > Evento > Configuración del puerto de salida)).
- **Priority** (Prioridad): establezca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para encender una alarma (activar) de prioridad 2 solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.

• **Alarm Off Event** (Evento para desactivar alarma): especifique la configuración y haga click en **Add** (Añadir) para añadir el evento a la lista Alarm Off Event (Evento para desactivar alarma). Estos eventos desactivarán una alama.

- **Event** (Evento): seleccione el evento que desactivará la alarma (*Auth Success* (Autorización con éxito), *Auth Fail* (Autorización fallida), *Auth Duress* (Autorización de peligro), *Anti-passback Fail* (Antipassback fallido), *Access Not Granted* (Acceso no permitido), *Entrance Limited* (Entrada limitada), *Admin Auth Success* (Autorización de administrador con éxito), *Tamper On* (Alteración activada), *Door Opened* (Puerta abierta), *Door Close* (Puerta cerrada), *Forced Open Door* (Puerta forzada abierta), *Held Open Door* (Puerta mantenida abierta), *Detect Input #1-3* (Detectar entrada #1-3)).
- **Device** (Dispositivo): seleccione el dispositivo supervisado para un evento de alarma.
- **Priority** (Prioridad): establezca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para encender una alarma (activar) de prioridad 2 solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.

5.1.1.7 Pestaña Display/Sound (Pantalla/Sonido)

La pestaña Display/Sound (Pantalla/Sonido) permite personalizar la pantalla y los sonidos de eventos de BioStation. Para guardar los cambios realizados en la configuración de pantalla o sonido, debe hacer click en **Apply** (Aplicar) en la parte inferior de la pestaña. También puede aplicar la misma configuración a otros dispositivos haciendo click en **Apply to Others** (Aplicar a otros).



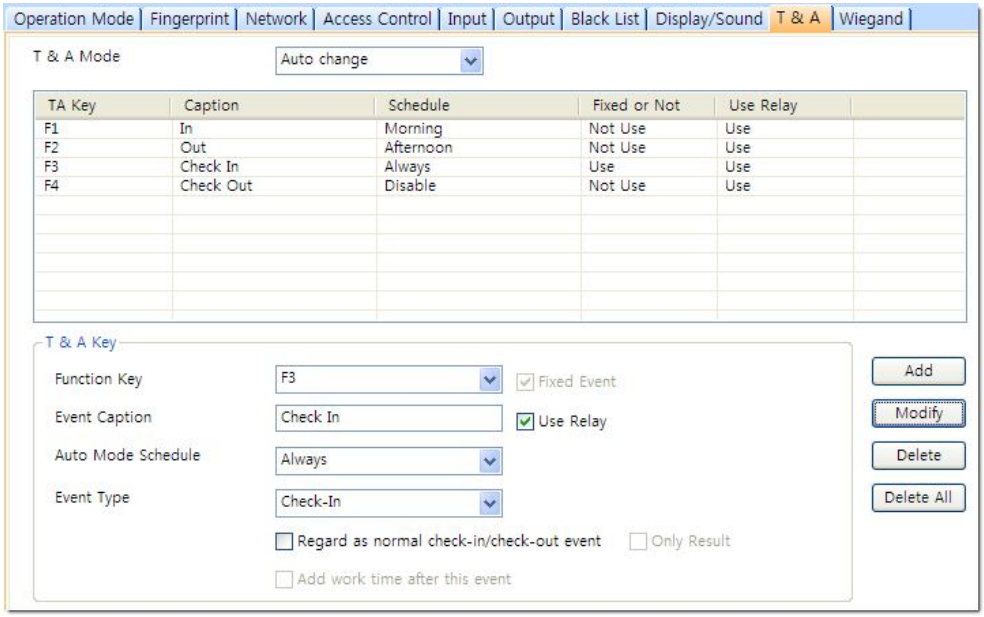
- **Display/Sound (Pantalla/Sonido)**
  - **Language** (Idioma): establezca el idioma utilizado en la pantalla (*Korean* (Coreano), *English* (Inglés) o *Custom* (Personalizado)).
  - **Sub Info** (Subinformación): configure la información que se mostrará en la parte inferior de la pantalla de BioStation (*Time* (Hora) o *None*(Ninguno)).
  - **Menu Timeout** (Tiempo de espera del menú): configure el tiempo de espera antes de que la pantalla cambie a modo inactivo (*Infinite* (Infinito), *10 sec* (10 s), *20 sec* (20 s) o *30 sec* (30 s)).
  - **Private Msg** (Mensaje privado): habilite o deshabilite la opción para mostrar un mensaje privado en la pantalla de BioStation (*Disable* (Deshabilitar) o *Enable* (Habilitar)). Puede añadir un mensaje privado en la pestaña Event (Evento) del panel User (Usuario): haga click en **Modify Private Information** (Modificar información privada), configure las opciones para el recuento y la duración de la pantalla, introduzca el texto en el campo Private Message (Mensaje privado) y luego haga click en **Save** (Guardar).

- **Resource** (Recurso): establezca el archivo de recursos lingüísticos que se utilizará para la interfaz de BioStar (*No Change* (No cambiar), *English* (Inglés), *Korean* (Coreano) o *Custom* (Personalizado)). Para utilizar un archivo de recursos lingüísticos diferente al de inglés o coreano, seleccione la opción *Custom* (Personalizado) y luego haga click en el botón de elipsis (...) para ubicar el archivo de recursos.
- **Background** (Fondo): configure el tipo de fondo para la pantalla de BioStation (*Logo*, *Notice* (Aviso) o *Slide Show* (Presentación)). Ninguno de los tipos de archivos compatibles (JPG, GIF, BMP y PNG) pueden exceder los 320x240 píxeles. Solo se puede utilizar una imagen como logo o aviso. Sin embargo, en una presentación pueden mostrarse hasta 16 imágenes (a un intervalo establecido).
- **Notice** (Aviso): haga click en este botón para crear el aviso que se mostrará en la pantalla de BioStation. Después de crear un aviso, puede hacer click en **Apply** (Aplicar), para aplicar el aviso al dispositivo actual, o en **Apply to Others** (Aplicar a otros) para aplicar el aviso a más dispositivos.
- **Volume** (Volumen): configure el volumen del dispositivo BioStation (del *10%* al *100%*).
- **Msg Timeout** (Tiempo de espera del mensaje): configure la duración en pantalla de un mensaje de confirmación o de error.

- **Background Image** (Imagen de fondo): haga click en esta casilla de validación para subir nuevas imágenes de fondo). Haga click en el signo (+) para ubicar y añadir un nuevo archivo de imagen.
- **Sound** (Sonido): haga click en la casilla de validación para habilitar y añadir sonidos de eventos personalizados. Haga click en un evento de la lista y luego haga click en el signo (+) para ubicar y añadir un nuevo archivo de sonido.

5.1.1.8 Pestaña T&A (Tiempo y asistencia)

La pestaña T&A permite configurar los parámetros del modo y de la clave para un dispositivo BioStation. Para guardar los cambios realizados en la configuración de tiempo y asistencia, debe hacer click en **Apply** (Aplicar) en la parte inferior de la pestaña. También puede aplicar la misma configuración a otros dispositivos haciendo click en **Apply to Others** (Aplicar a otros).



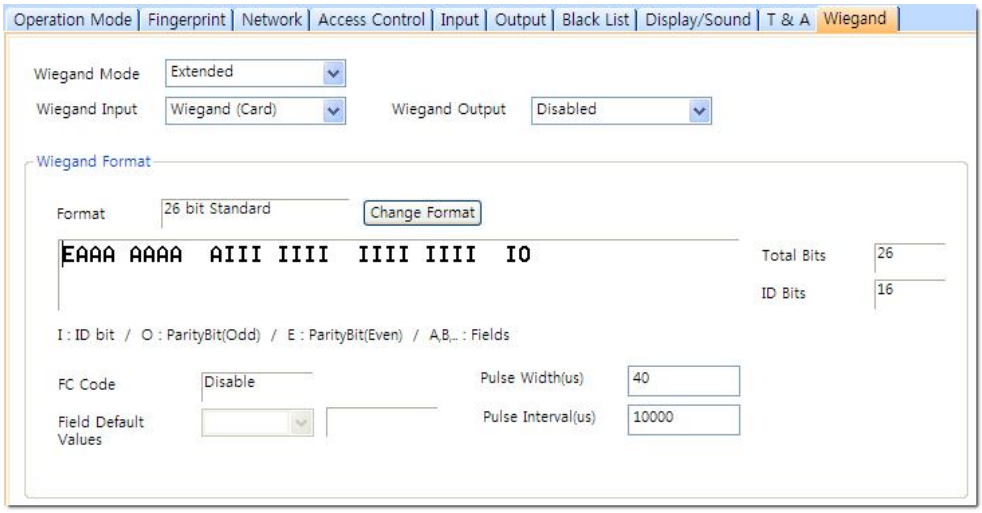
- **T&A Mode** (Modo de tiempo y asistencia): establezca el modo de tiempo y asistencia:
  - **Not Use** (No utilizar): deshabilita las funciones de tiempo y asistencia en este dispositivo.
  - **Manual** : los usuarios deben pulsar la tecla especificada cada vez que entren o salgan para registrar los eventos de tiempo y asistencia.
  - **Manual Fix** (Fijación manual): cuando se pulsa una tecla de tiempo y asistencia, el dispositivo permanecerá en este modo hasta que se pulse otra tecla de tiempo y asistencia.
  - **Auto change** (Cambio automático): el dispositivo cambiará automáticamente los modos de tiempo y asistencia para que se correspondan con las funciones especificadas para un período de tiempo.
  - **Event Fix** (Fijación de evento): el dispositivo solo realizará la función de tiempo y asistencia especificada.

- **T&A Key** (Tecla de tiempo y asistencia): especifique las teclas que se utilizarán para los eventos de tiempo y asistencia y los tipos de eventos asociados a ellas:
  - **Function Key** (Tecla de función): seleccione una tecla de función de la lista desplegable para asignar a un evento de tiempo y asistencia (*F1-F4*, *1-9*, *CALL*, *0*, o *ESC)*. Si utiliza el modo Event Fix (Fijación de eventos), puede hacer click en la casilla de validación que se encuentra a la derecha para designar un evento fijo.
  - **Event Caption** (Leyenda de evento): introduzca una leyenda para el evento.
  - **Auto Mode Schedule** (Programa de modo automático): cuando utilice el modo Auto Change (Cambio automático), puede especificar cuándo ocurrirá el evento, seleccionando una zona horaria de la lista desplegable. Para obtener más información acerca de cómo crear una zona horaria, consulte la sección 3.6.1.
  - **Event Type** (Tipo de evento): configure el tipo de evento que se asignará a la tecla (*Not Use* (No utilizar), *Check In* (Entrada), *Check Out* (Salida), *In* (Dentro) o *Out* (Fuera)). In/Out indican los eventos de entrada y salida generales durante un día, mientras que Check In/Out indican los eventos de entrada y salida formales a la llegada y a la partida del lugar de trabajo, o los eventos de la primera entrada y de la última salida del día. Cuando elija Check In o Check Out, puede habilitar la opción “Regard as normal check-in/check-out event” (Considerar como evento de entrada/salida normal).

    Si se habilita esta opción, los usuarios que pulsen las teclas adecuadas se considerarán como si llegasen o saliesen a tiempo del trabajo, aunque en realidad lleguen tarde o se vayan temprano. Si habilita la opción “Only Result” (Solo resultado), los usuarios aparecerán en los reportes de tiempo y asistencia como si hubieran llegado a tiempo, pero el tiempo de trabajo se calculará correctamente en base a las horas de entrada y salida reales. Si elige *Out* (Fuera), puede habilitar la opción "Add work time after this event” (Añadir tiempo de trabajo después de este evento). Si se habilita esta opción, los usuarios que pulsen las teclas adecuadas se considerarán como si se hubieran quedado a trabajar durante el tiempo restante, aunque abandonen la oficina antes.

5.1.1.9 Pestaña Wiegand

La pestaña Wiegand permite configurar el formato Wiegand para un dispositivo BioStation. Haga click en **Change Format** (Cambiar formato) para abrir el asistente de configuración Wiegand. Para obtener más información acerca de cómo configurar el formato Wiegand, consulte la sección 3.2.9.



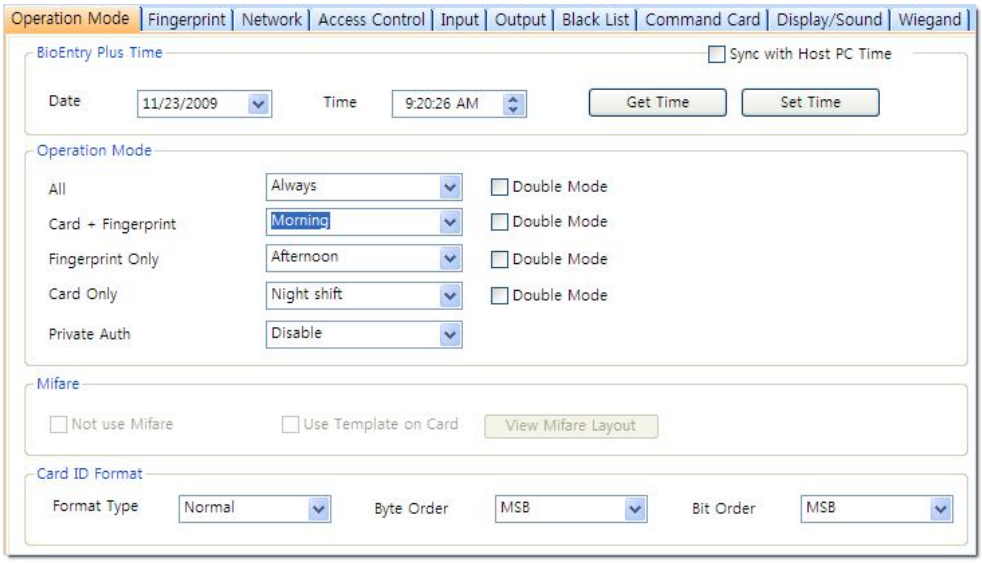
- **Wiegand Mode** (Modo Wiegand): configure el modo de entrada Wiegand que se utilizará cuando se lean los datos de Id. de una tarjeta (*Legacy* (Heredado) o *Extended* (Extendido)). El modo Legacy (Heredado) considerará a los dispositivos conectados mediante RFs como parte de los dispositivos anfitriones (esta función es típica de las anteriores versiones de BioStar). El modo Extended (Extendido) permitirá que los lectores de tarjetas por RFs funcionen de manera independiente, lo que permite asociarlos a puertas, incluidas en zonas, y guardar los registros con las propias Id. del dispositivo.
- **Wiegand Input** (Entrada Wiegand): asigne la entrada Wiegand:
  - **Disabled** (Deshabilitada): la entrada no se utilizará.
  - **Wiegand [Card]** (Wiegand [Tarjeta]): el campo de Id. de la cadena Wiegand se interpreta como el id. de una tarjeta.
  - **Wiegand [User]** (Wiegand [Usuario]): el campo de Id. de la cadena Wiegand se interpreta como el id. de un usuario.
- **Wiegand Output** (Salida Wiegand): asigne la salida Wiegand:
  - **Disabled** (Deshabilitada): la salida no se utilizará.
  - **Wiegand [Card]** (Wiegand [Tarjeta]): inserta el id. de la tarjeta del usuario autentificado en el campo de Id. de la cadena Wiegand.
  - **Wiegand [User]** (Wiegand [Usuario]): inserta el id. de usuario del usuario autentificado en el campo de Id. de la cadena Wiegand.

5.1.2 Personalización de la configuración para dispositivos BioEntry Plus

Las siguientes secciones describen la configuración disponible para los dispositivos BioEntry Plus. Personalice la forma en que funcionan los dispositivos BioEntry Plus cambiando la configuración para que estos se adapten al entorno y a las necesidades operacionales particulares.

5.1.2.1 Pestaña Operation Mode (Modo de funcionamiento)

La pestaña Operation Mode (Modo de funcionamiento) permite personalizar la configuración de la hora y de varios modos de funcionamiento en los dispositivos BioEntry Plus.



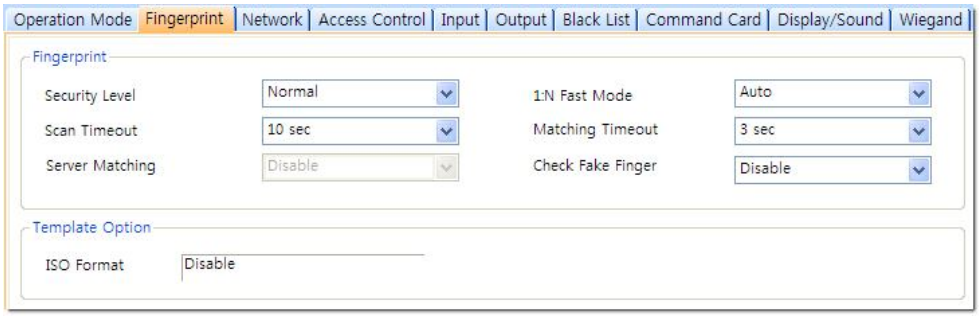
- **BioEntry Plus Time (Hora de BioEntry Plus)**
  - **Date** (Fecha): establezca manualmente la fecha del dispositivo en el calendario desplegable.
  - **Time** (Hora): establezca manualmente la hora del dispositivo.
  - **Sync with Host PC Time** (Sincronizar con la hora de la computadora central): seleccione esta casilla de validación para sincronizar automáticamente la hora del dispositivo con la hora de la computadora central.
  - **Get Time** (Obtener hora): obtenga la hora actual mostrada en el dispositivo.
  - **Set Time** (Establecer hora): establezca la hora del dispositivo.

- **Operation Mode** (Modo de funcionamiento): para todas las funciones siguientes, haga click en la casilla de validación correspondiente para habilitar el modo de verificación doble (Double Mode), que requiere la verificación de dos credenciales de usuario para permitir la entrada a una puerta.
  - **All** (Todos): configure el dispositivo para permitir todos los tipos de autorización (*Always* (Siempre), *Disable* (Deshabilitar) o Custom Schedule (programa personalizado)).
  - **Card + Fingerprint** (Tarjeta + Huella dactilar): configure el dispositivo para que solicite la autorización con tarjeta y con huella dactilar (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
  - **Only Fingerprint** (Solo huella dactilar): configure el dispositivo para que solo solicite la autorización con huella dactilar (*Always* (Siempre), *Disable* (Deshabilitar) o Custom Schedule (programa personalizado)).
  - **Only CARD** (Solo TARJETA): configure el dispositivo para que solo solicite la autorización con tarjeta (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
  - **Private Auth** (Autorización privada): configure el dispositivo para permitir un método de autorización privada (*Disable* (Deshabilitar) o *Enable* (Habilitar)). Si se habilita, el modo de autentificación del usuario se determinará por un parámetro de autorización de un usuario (Private Auth Mode (Modo de autorización privado)), que se encuentra en la pestaña Details (Detalles), en el panel User (Usuario). Si se deshabilita, el modo de autentificación se determinará por la configuración del modo de funcionamiento del dispositivo.
  - **Double Verification Mode** (Modo de verificación doble): configure el dispositivo para que solicite la verificación de dos usuarios durante un programa seleccionado (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
- **Mifare**
  - **Not use Mifare** (No utilizar Mifare): seleccione esta casilla de validación para deshabilitar la autorización con tarjeta MIFARE.
  - **Use Template on Card** (Utilizar plantilla en tarjeta): seleccione esta casilla de validación para que se utilice la plantilla en la tarjeta MIFARE en la autorización.
  - **View Mifare Layout** (Visualizar distribución Mifare): haga click en este botón para configurar la distribución MIFARE utilizada por el dispositivo. Para obtener más información acerca de cómo configurar la distribución MIFARE, consulte la sección 3.5.4.6.

- **Card ID Format (Formato de el id. de tarjeta)**
  - **Format Type** (Tipo de formato): establezca el tipo de procesamiento previo de los datos de el id. de una tarjeta (*Normal* o *Wiegand*). Si se selecciona "Normal", los datos de el id. de una tarjeta se procesarán en su forma original. Si se selecciona "Wiegand", los dispositivos interpretarán los datos de el id. de una tarjeta según la configuración del formato Wiegand.
  - **Byte Order** (Orden de bytes): especifique si desea intercambiar los datos de las tarjetas con Id. entre las tarjetas y los dispositivos por byte más significativo (*MSB*) o por byte menos significativo (*LSB*).
  - **Bit Order** (Orden de bits): especifique si desea intercambiar los datos de las tarjetas con Id. entre las tarjetas y los dispositivos por bit más significativo (*MSB*) o por bit menos significativo (*LSB*).

5.1.2.2 Pestaña Fingerprint (Huella dactilar)

La pestaña Fingerprint (Huella dactilar) permite personalizar la configuración de la autorización con huella dactilar para los dispositivos BioEntry Plus.



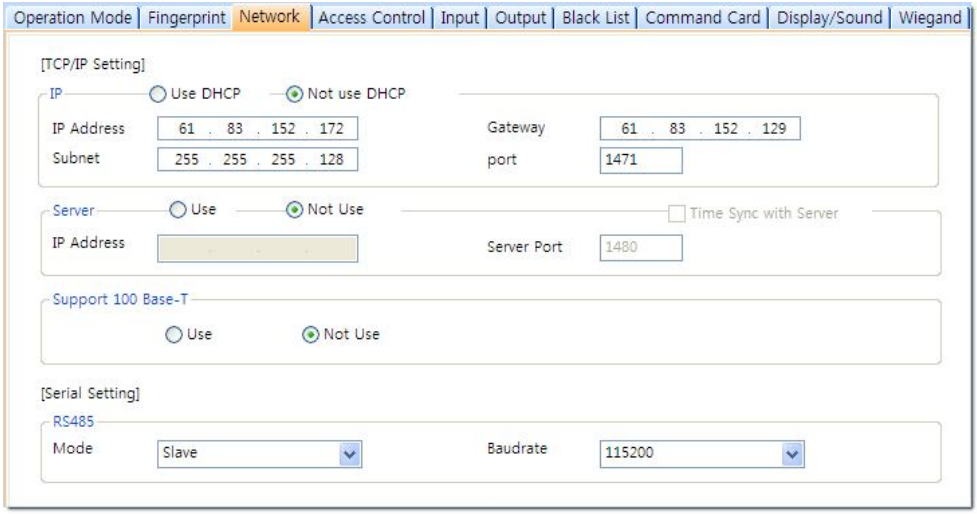
- **Fingerprint (Huella dactilar)**
  - **Security Level** (Nivel de seguridad): establezca el nivel de seguridad que utilizar para la autorización con huella dactilar (*Normal* (Normal), *Secure* (Seguro), or *Most Secure* (Muy seguro)). Recuerde que cuanto más alto sea el nivel de seguridad, más posibilidades hay de que se produzcan falsos rechazos.
  - **Scan Timeout** (Tiempo de espera del escáner): configure el tiempo que debe transcurrir antes de que expire el tiempo del escáner de las huellas dactilares (de *1 sec* (1 s) a *20 sec* (20 s)). Si un usuario no coloca el dedo en el dispositivo durante el tiempo de espera, se producirá un fallo en la autorización.
  - **Server Matching** (Identificación de servidor): active esta opción para identificar una huella dactilar o el id. de una tarjeta en el servidor BioStar, en lugar de en el dispositivo. Cuando se activa este modo,

los dispositivos envían las plantillas de las huellas dactilares o las Id. de la tarjeta al servidor para verificar la identificación. Este modo resulta útil cuando posee más usuarios de los que se pueden descargar a un dispositivo, o cuando la información de usuario no se puede distribuir por motivos de seguridad.

- **1:N Fast Mode** (Modo rápido 1:N): configure el dispositivo para utilizar el modo rápido y reducir así el tiempo requerido para identificar las huellas dactilares (*Auto* (Automático), *Normal*, *Fast* (Rápido) o *Fastest* (Muy rápido)). Si se establece en modo *Auto* (Automático), la velocidad de identificación se ajustará automáticamente según el número de plantillas registradas.
- **Matching Timeout** (Tiempo de espera de la identificación): configure el tiempo que deberá transcurrir antes de que expire el tiempo del dispositivo para intentar identificar una huella dactilar (de *0 [Infinite]* (0 [Infinito] a *10 sec* (10 s)).
- **Check Fake Finger** (Comprobar dedo falso): configure el dispositivo para que detecte el uso de huellas dactilares falsas como, por ejemplo, las fabricadas con silicona o hule, y prevenir así un acceso no autorizado.

5.1.2.3 Pestaña Network (Red)

La pestaña Network (Red) permite personalizar la configuración del servidor y de la red para los dispositivos BioEntry Plus.



- **TCP/IP**
  - **Use DHCP** (Utilizar DHCP): haga click en este botón de radio para habilitar el protocolo de configuración de host dinámico (DHCP) en el dispositivo.

- **Not Use DHCP** (No utilizar DHCP): haga click en este botón de radio para deshabilitar el protocolo de configuración de host dinámico (DHCP) en el dispositivo.
- **IP Address** (Dirección IP): especifique una dirección IP para el dispositivo.
- **Subnet** (Subred): especifique una dirección de subred para el dispositivo.
- **Gateway** (Puerta de enlace): especifique una puerta de enlace de red.
- **Port** (Puerto): especifique un puerto para utilizar el dispositivo.

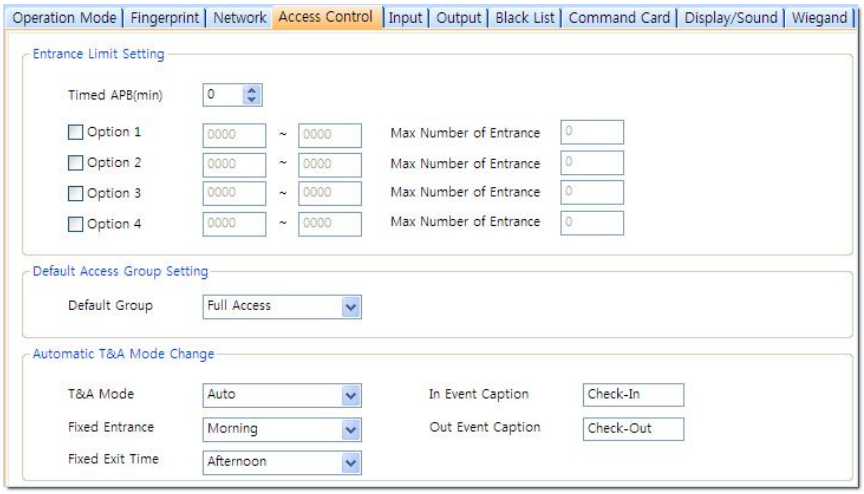
• **Server (Servidor)**
- **Use** (Utilizar): haga click en este botón de radio para utilizar los parámetros específicos del servidor.
- **Not use** (No utilizar): haga click en este botón de radio para deshabilitar la configuración del servidor.
- **IP Address** (Dirección IP): especifique una dirección IP para el servidor BioStar.
- **Time sync with Server** (Sincronizar hora con servidor): seleccione esta casilla de validación para sincronizar la hora del dispositivo con la hora del servidor.

• **Support 100 Base-T** (Compatibilidad con 100 Base-T): esta opción permite habilitar o deshabilitar una conexión rápida de Ethernet para el dispositivo. Cuando se encuentre habilitada esta opción, el dispositivo detectará la red Ethernet y establecerá automáticamente la mejor conexión. Si no se habilita, el dispositivo intentará establecer una conexión Ethernet de 10Base-T.
- **Use** (Utilizar): haga click en este botón de radio para habilitar la conexión 100base-T para el dispositivo.
- **Not Use** (No utilizar): haga click en este botón de radio para deshabilitar la conexión 100base-T para el dispositivo.

• **RS485**
- **Mode** (Modo): configure el modo de un dispositivo conectando mediante RS485 (*Disable* (Deshabilitar), *Host* (Anfitrión), *Slave* (Esclavo) o *PC Connection* (Conexión de PC)).
- **Baudrate** (Velocidad de transmisión): configure la velocidad en baudios de un dispositivo conectado mediante RS485 (de *9600* a *115200*).

5.1.2.4 Pestaña Access Control (Control de acceso)

La pestaña Access Control permite personalizar la configuración del límite de entrada, de los grupos de acceso predeterminados y del modo de tiempo y asistencia para un dispositivo BioEntry Plus.



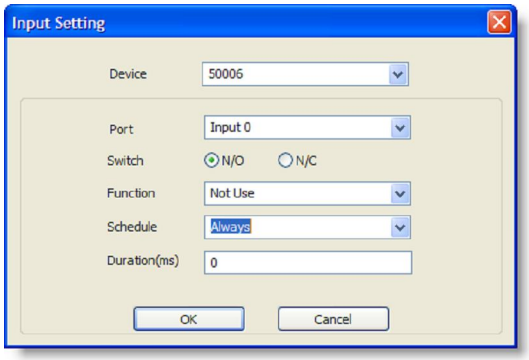
- **Entrance Limit Setting (Configuración del límite de entrada)**
  - **Timed APB (min)** (APB programado (min)): establezca el tiempo (en minutos) en que un usuario no podrá volver a entrar a una zona mediante el dispositivo. Una vez que un usuario haya conseguido entrar, el dispositivo rechazará la tarjeta o la huella dactilar del usuario durante el período de tiempo determinado aquí.
  - **Option 1-4** (Opción 1-4): haga click en la casilla de validación para habilitar el límite de entrada y luego especifique las horas efectivas para el mismo.
  - **Max Number of Entrance** (Número máximo de entradas): establezca el número máximo de entradas permitidas durante el límite de tiempo determinado.
- **Default Access Group Setting** (Configuración del grupo de acceso predeterminado): seleccione un grupo de acceso predeterminado para aplicar a los usuarios nuevos que no han sido asignados a ningún grupo de acceso.
- **Automatic T&A Mode Change (Cambio de modo de tiempo y asistencia automático)**
  - **T&A Mode** (Modo de tiempo y asistencia): configure el modo de tiempo y asistencia para el dispositivo (*Disable* (Deshabilitar), *Fixed In* (Entrada fija), *Fixed Out* (Salida fija) y *Auto* (Automático)).
  - **Fixed Entrance** (Entrada fija): cuando el modo de tiempo y asistencia "Auto" (Automático) está seleccionado, especifique cuándo se permitirán eventos de entrada seleccionando una zona

horaria (*Always* (Siempre), *Disable* (Deshabilitar) o zona horaria personalizada) de la lista desplegable. Para obtener más información acerca de cómo crear una zona horaria, consulte la sección 3.6.1.

- **Fixed Exit Time** (Hora de salida fija): cuando el modo de tiempo y asistencia "Auto" (Automático) está seleccionado, especifique cuándo se permitirán eventos de salida seleccionando una zona horaria (*Always* (Siempre), *Disable* (Deshabilitar) o zona horaria personalizada) de la lista desplegable. Para obtener más información acerca de cómo crear una zona horaria, consulte la sección 3.6.1.
- **In Event Caption** (Leyenda de evento de entrada): establezca una leyenda para la entrada.
- **Out Event Caption** (Leyenda de evento de salida): establezca una leyenda para la salida.

5.1.2.5 Pestaña Input (Entrada)

La pestaña Input (Entrada) muestra los parámetros de entrada especificados para un dispositivo BioEntry Plus. Los botones que se encuentran en la parte inferior de la pestaña permiten añadir, modificar o eliminar parámetros de entrada. Para añadir o modificar los parámetros, debe especificarlos en la ventana Input Setting (Configuración de entrada). (Cerrar puerta). Para obtener más información acerca de cómo configurar los parámetros de entrada, consulte la sección 3.9.3.2.

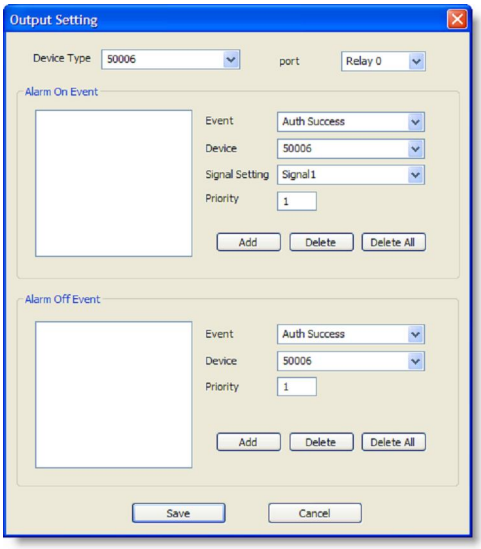


- **Device** (Dispositivo): seleccione el dispositivo BioEntry Plus (o Secure I/O) al que desea añadir o modificar los parámetros.
- **Port** (Puerto): seleccione un puerto de entrada (Input 0 (Entrada 0), Input 1 (Entrada 1), o Tamper (Alterar)). Para dispositivos Secure I/O, los siguientes parámetros están disponibles: Input 0 (Entrada 0), Input 1 (Entrada 1), Input 2 (Entrada 2), Input 3 (Entrada 3).

- **Switch** (Interruptor): haga click en los botones de radio para especificar la posición normal del interruptor de entrada (N/O: normalmente abierto o N/C: normalmente cerrado).
- **Function** (Función): seleccione la opción asociada a la entrada:
  - **Not Use** (No utilizar): el puerto de entrada no será supervisado.
  - **Generic Input** (Entrada genérica): el puerto de entrada se supervisará para una acción desencadenadora (para los eventos especificados con “Detect Input 1-3” (Detectar entrada 1-3), en la ventana Output settings (Configuración de salida), consulte la sección 5.1.2.6).
  - **Emergency Open** (Apertura de emergencia): abre las puertas controladas por este dispositivo. El período de apertura normal de puertas será ignorado y las puertas permanecerán abiertas hasta que un operador envíe la orden "Close Door" (Cerrar puerta) mediante la pestaña Door/Zone Monitoring (Supervisión de puerta/zona) (consulte la sección 4.4.1).
  - **Release All Alarms** (Cancelar todas las alarmas): cancela las alarmas asociadas a este dispositivo.
  - **Restart Device** (Reiniciar dispositivo): reinicia el dispositivo.
  - **Disable Device** (Deshabilitar dispositivo): deshabilita el dispositivo. Un dispositivo deshabilitado no se comunicará con el servidor BioStar ni procesará huellas dactilares ni tarjetas. Para habilitar de nuevo la comunicación, un administrador debe introducir la contraseña maestra para un dispositivo BioStar o proporcionar autentificación de forma local para un dispositivo BioEntry Plus.
- **Schedule** (Programa): configure el programa para las acciones de entrada (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
- **Duration (ms)** (Duración (ms)): establezca la duración (en milisegundos) que una entrada debe durar para activar la acción establecida.

5.1.2.6 Pestaña Output (Salida)

La pestaña Output (Salida) muestra los parámetros de salida especificados para un dispositivo BioEntry Plus. Los botones que se encuentran en la parte inferior de la pestaña permiten añadir, modificar o eliminar parámetros de salida. Para añadir o modificar los parámetros, debe especificarlos en la ventana Output Setting (Configuración de salida). Para obtener más información acerca de cómo configurar los parámetros de salida, consulte la sección 3.9.3.1.



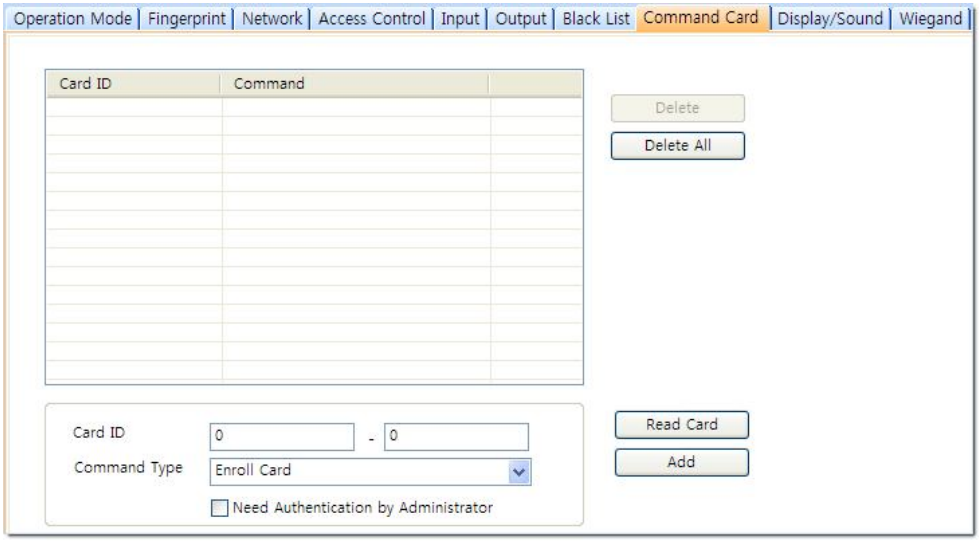
- **Device Type** (Tipo de dispositivo): seleccione el tipo de dispositivo al que añadirá o modificará los parámetros.
- **Port** (Puerto): seleccione un puerto de salida (*Relay 0*). Para dispositivos Secure I/O, los siguientes parámetros están disponibles: *Relay 0* o *Relay 1*.
- **Alarm On Event** (Evento para activar alarma): especifique la configuración y haga click en **Add** (Añadir) para añadir el evento a la lista Alarm On Event (Evento para activar alarma). Estos eventos activarán una alama.
  - **Event** (Evento): seleccione el evento que activará la alarma (*Auth Success* (Autorización con éxito), *Auth Fail* (Autorización fallida), *Auth Duress* (Autorización de peligro), *Anti-passback Fail* (Antipassback fallido), *Access Not Granted* (Acceso no permitido), *Entrance Limited* (Entrada limitada), *Admin Auth Success* (Autorización de administrador con éxito), *Tamper On* (Alteración activada), *Door Opened* (Puerta abierta), *Door Close* (Puerta cerrada), *Forced Open Door* (Puerta forzada abierta), *Held Open Door* (Puerta mantenida abierta), *Detect Input #1-3* (Detectar entrada #1-3)).
  - **Device** (Dispositivo): seleccione el dispositivo supervisado para un evento de alarma.
  - **Signal Setting** (Configuración de señal): seleccione una opción de señal anteriormente configurada en la barra de menú (**Option > Event > Output Port Setting** (Opción > Evento > Configuración del puerto de salida)).
  - **Priority** (Prioridad): establezca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para

encender una alarma (activar) de prioridad 2 solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.

- **Alarm Off Event** (Evento para desactivar alarma): especifique la configuración y haga click en **Add** (Añadir) para añadir el evento a la lista Alarm Off Event (Evento para desactivar alarma). Estos eventos desactivarán una alama.
  - **Event** (Evento): seleccione el evento que desactivará la alarma (*Auth Success* (Autorización con éxito), *Auth Fail* (Autorización fallida), *Auth Duress* (Autorización de peligro), *Anti-passback Fail* (Antipassback fallido), *Access Not Granted* (Acceso no permitido), *Entrance Limited* (Entrada limitada), *Admin Auth Success* (Autorización de administrador con éxito), *Tamper On* (Alteración activada), *Door Opened* (Puerta abierta), *Door Close* (Puerta cerrada), *Forced Open Door* (Puerta forzada abierta), *Held Open Door* (Puerta mantenida abierta), *Detect Input #1-3* (Detectar entrada #1-3)).
  - **Device** (Dispositivo): seleccione el dispositivo supervisado para un evento de alarma.
  - **Priority** (Prioridad): establezca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para encender una alarma (activar) solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.

5.1.2.7 Pestaña Command Card (Tarjeta de comando)

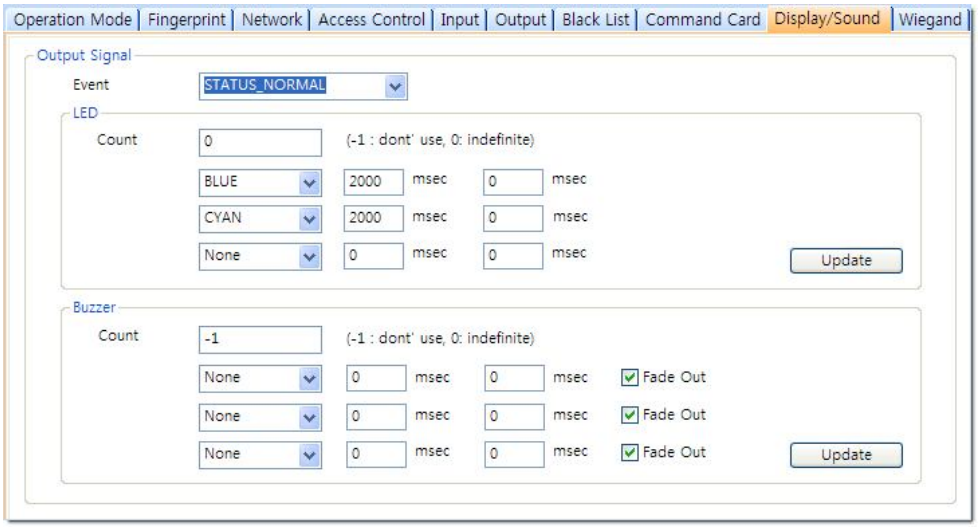
La pestaña Command Card (Tarjeta de comando) permite expedir tarjetas de comando. Para obtener más información acerca de las tarjetas de comando, consulte la sección 3.2.5.1.



- **Card ID** (Id. de tarjeta): introduzca el id. de la tarjeta o haga click en **Read Card** (Leer tarjeta) y coloque una tarjeta de comando en el lector para poblar automáticamente los campos.
- **Command Type** (Tipo de comando): seleccione el tipo de tarjeta de comando que desea expedir (*Enroll Card* (Tarjeta de registro), *Delete Card* (Tarjeta de eliminación) o *Delete All Card* (Tarjeta de eliminación total)).

5.1.2.8 Pestaña Display/Sound (Pantalla/Sonido)

La pestaña Display/Sound (Pantalla/Sonido) permite personalizar los comportamientos por evento del LED y del zumbido. Para guardar los cambios realizados en estos parámetros, deberá hacer click en **Update** (Actualizar) en la sección correspondiente para cada evento.

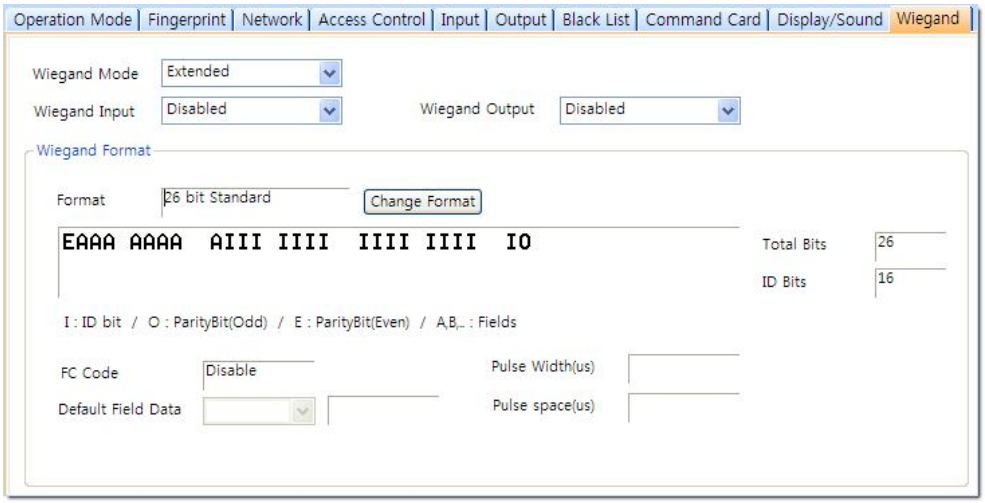


- **Event** (Evento):especifique el evento en cuestión seleccionándolo de la lista desplegable.
- **LED**:configure el comportamiento del LED para un evento determinado.
  - **Count** (Cuenta): introduzca el número de ciclos del LED para el evento determinado. Introduzca “0” para habilitar un ciclo infinito o “-1” para deshabilitar el LED.
  - **Colors** (Colores): especifique hasta tres colores de pantalla de la lista desplegable. El LED irá cambiando a estos colores en orden, de arriba a abajo. Al lado de cada color, introduzca el tiempo (en milisegundos) que el LED mostrará el color seleccionado y el tiempo (en milisegundos) que permanecerá apagado antes de cambiar al siguiente color del ciclo.

- **Buzzer** (Zumbido): configure el comportamiento del zumbido para un evento determinado.
  - **Count** (Cuenta): introduzca el número de ciclos del LED para el evento determinado. Introduzca "0" para habilitar un ciclo infinito o "-1" para deshabilitar el LED.
  - **Volume** (Volumen): configure hasta tres volúmenes de tono de la lista desplegable (*Low* (Bajo), *Middle* (Medio) o *High* (Alto)). El zumbido irá cambiando a estos volúmenes en orden, de arriba a abajo. Al lado de cada volumen, introduzca el tiempo (en milisegundos) que el zumbido se mantendrá en el volumen seleccionado y el tiempo (en milisegundos) que el zumbido se mantendrá apagado antes de cambiar al siguiente volumen del ciclo.
  - **Fade Out** (Fundido de salida): configure el volumen del tono al que le afectará el fundido de salida, antes de avanzar al siguiente volumen del ciclo, haciendo click en esta casilla de validación.

5.1.2.9 Pestaña Wiegand

La pestaña Wiegand permite configurar el formato Wiegand para un dispositivo BioEntry Plus. Haga click en **Change Format** (Cambiar formato) para abrir el asistente de configuración Wiegand. Para activar la función Wiegand en un dispositivo BioEntry Plus, haga click en la casilla de validación que se encuentra en la parte superior derecha de la pestaña. Para obtener más información acerca de cómo configurar el formato Wiegand, consulte la sección 3.2.9.



- **Wiegand Mode** (Modo Wiegand): configure el modo de entrada Wiegand que se utilizará cuando se lean los datos de Id. de una tarjeta (*Legacy* (Heredado) o *Extended* (Extendido)). El modo Legacy (Heredado) considerará a los dispositivos conectados mediante RFs

como parte de los dispositivos anfitriones (esta función es típica de las anteriores versiones de BioStar). El modo Extended (Extendido) permitirá que los lectores de tarjetas por RFs funcionen de manera independiente, lo que permite asociarlos a puertas, incluidas en zonas, y guardar los registros con las propias Id. del dispositivo.

- **Wiegand Input** (Entrada Wiegand): asigne la entrada Wiegand:
  - **Disabled** (Deshabilitada): la entrada no se utilizará.
  - **Wiegand [Card]** (Wiegand [Tarjeta]): el campo de Id. de la cadena Wiegand se interpreta como el id. de una tarjeta.
  - **Wiegand [User]** (Wiegand [Usuario]): el campo de Id. de la cadena Wiegand se interpreta como el id. de un usuario.
- **Wiegand Output** (Salida Wiegand): asigne la salida Wiegand:
  - **Disabled** (Deshabilitada): la salida no se utilizará.
  - **Wiegand [Card]** (Wiegand [Tarjeta]): inserta el id. de la tarjeta del usuario autentificado en el campo de Id. de la cadena Wiegand.
  - **Wiegand [User]** (Wiegand [Usuario]): inserta el id. de usuario del usuario autentificado en el campo de Id. de la cadena Wiegand.

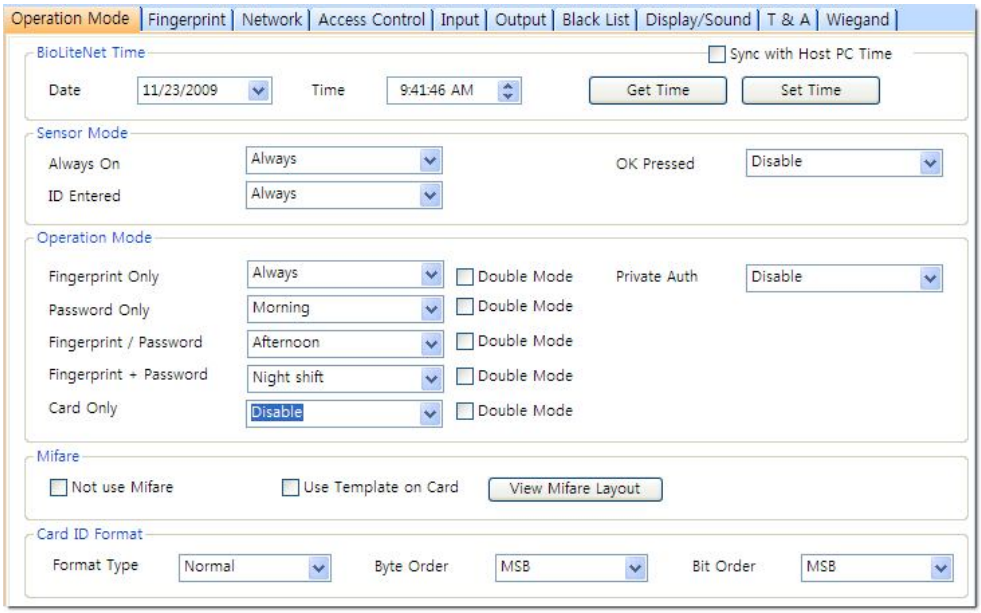
5.1.3 Personalización de la configuración para dispositivos BioLite Net

Las siguientes secciones describen la configuración disponible para los dispositivos BioLite Net. Personalice la forma en que funcionan los dispositivos BioLite Net cambiando la configuración para que estos se adapten al entorno y a las necesidades operacionales particulares.

5.1.3.1 Pestaña Operation Mode (Modo de funcionamiento)

La pestaña Operation Mode (Modo de funcionamiento) permite personalizar la configuración de la hora y de varios modos de funcionamiento en los dispositivos BioLite Net.

5. Personalización de la configuración



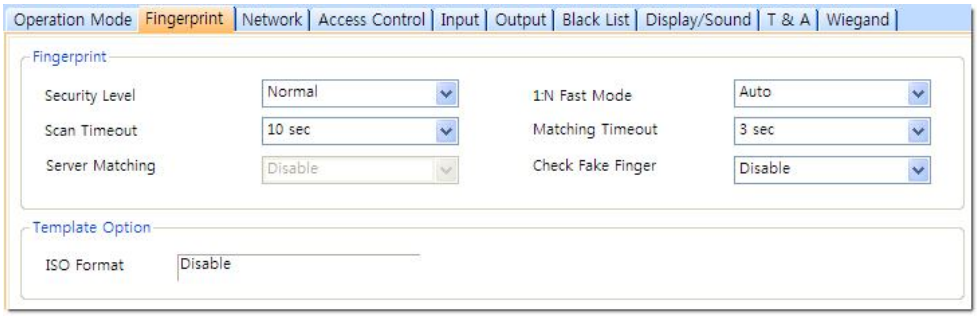
- **BioLiteNet Time (Hora de BioLite Net)**
  - **Date** (Fecha): establezca manualmente la fecha del dispositivo en el calendario desplegable.
  - **Time** (Hora): establezca manualmente la hora del dispositivo.
  - **Sync with Host PC Time** (Sincronizar con la hora de la computadora central): seleccione esta casilla de validación para sincronizar automáticamente la hora del dispositivo con la hora de la computadora central.
  - **Get Time** (Obtener hora): obtenga la hora actual mostrada en el dispositivo.
  - **Set Time** (Establecer hora): establezca la hora del dispositivo.
- **Sensor Mode (Modo del sensor)**
  - **Always On** (Siempre encendido): configure el sensor del dispositivo para que siempre esté disponible en modo de espera (*Always* (Siempre) o *Disable* (Deshabilitar)).
  - **ID Entered** (Id. introducida): configure el sensor del dispositivo para que esté disponible en modo de espera solo después de introducir una Id. válida (*Always* (Siempre) o *Disable* (Deshabilitar)).
  - **OK Pressed** (Tecla OK presionada): configure el sensor del dispositivo para que esté disponible en modo de espera solo después de pulsar la tecla OK (*Always* (Siempre) o *Disable* (Deshabilitar)).

- **Operation Mode** (Modo de funcionamiento): para todas las funciones siguientes, haga click en la casilla de validación correspondiente para habilitar el modo de verificación doble (Double Mode), que requiere la verificación de dos credenciales de usuario para permitir la entrada a una puerta.
  - **Fingerprint Only** (Solo huella dactilar): configure el dispositivo para que solo solicite la autorización con huella dactilar (*Always* (Siempre), *Disable* (Deshabilitar) o Custom Schedule (programa personalizado)).
  - **Password Only** (Solo contraseña): configure el dispositivo para que solo solicite la autorización con contraseña (*Always* (Siempre), *Disable* (Deshabilitar) o Custom Schedule (programa personalizado)).
  - **Fingerprint/Password** (Huella dactilar/Contraseña): configure el dispositivo para que solicite la autorización con huella dactilar o con contraseña (*Always* (Siempre), *Disable* (Deshabilitar) o Custom Schedule (programa personalizado)).
  - **Fingerprint+Password** (Huella dactilar+Contraseña): configure el dispositivo para que solicite la autorización con huella dactilar y contraseña (*Always* (Siempre), *Disable* (Deshabilitar) o Custom Schedule (programa personalizado)).
  - **Card Only** (Solo tarjeta): configure el dispositivo para que solo solicite la autorización con tarjeta (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
  - **Private Auth** (Autorización privada): configure el dispositivo para permitir un método de autorización privada (*Disable* (Deshabilitar) o *Enable* (Habilitar)). Si se habilita, el modo de autentificación del usuario se determinará por la configuración de la autorización (Authorization) de un usuario, que se encuentra en la pestaña Details (Detalles). Si se deshabilita, el modo de autentificación se determinará por la configuración del modo de funcionamiento del dispositivo.
- **Mifare**
  - **Not use Mifare** (No utilizar Mifare): seleccione esta casilla de validación para deshabilitar la autorización con tarjeta MIFARE.
  - **Use Template on Card** (Utilizar plantilla en tarjeta): seleccione esta casilla de validación para que se utilice la plantilla en la tarjeta MIFARE en la autorización.
  - **View Mifare Layout** (Visualizar distribución Mifare): haga click en este botón para configurar la distribución MIFARE utilizada por el dispositivo. Para obtener más información acerca de cómo configurar la distribución MIFARE, consulte la sección 3.5.4.6.

- **Card ID Format (Formato de el id. de tarjeta)**
  - **Format Type** (Tipo de formato): establezca el tipo de procesamiento previo de los datos de el id. de una tarjeta (*Normal* o *Wiegand*). Si se selecciona “Normal”, los datos de el id. de una tarjeta se procesarán en su forma original. Si se selecciona “Wiegand”, los dispositivos interpretarán los datos de el id. de una tarjeta según la configuración del formato Wiegand.
  - **Byte Order** (Orden de bytes): especifique si desea intercambiar los datos de las tarjetas con Id. entre las tarjetas y los dispositivos por byte más significativo (*MSB*) o por byte menos significativo (*LSB*).
  - **Bit Order** (Orden de bits): especifique si desea intercambiar los datos de las tarjetas con Id. entre las tarjetas y los dispositivos por bit más significativo (*MSB*) o por bit menos significativo (*LSB*).

5.1.3.2 Pestaña Fingerprint (Huella dactilar)

La pestaña Fingerprint (Huella dactilar) permite personalizar la configuración de la autorización con huella dactilar para los dispositivos BioLite Net.

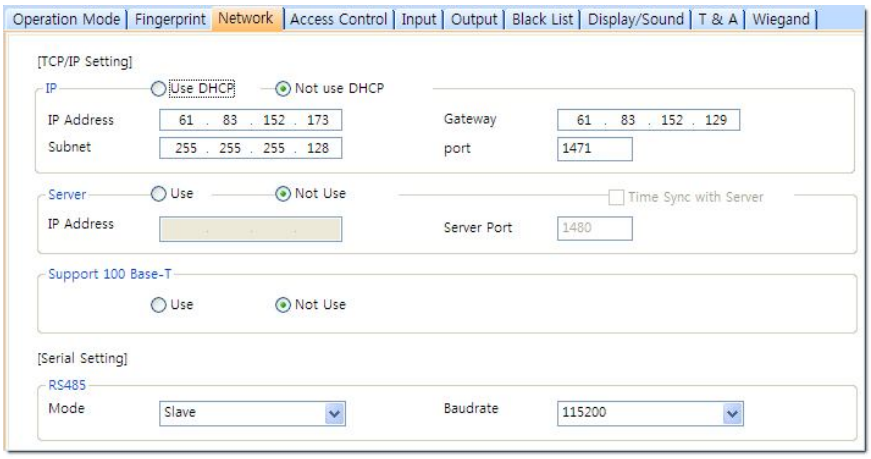


- **Fingerprint (Huella dactilar)**
  - **Security Level** (Nivel de seguridad): establezca el nivel de seguridad que utilizar para la autorización con huella dactilar (*Normal* (Normal), *Secure* (Seguro), or *Most Secure* (Muy seguro)). Recuerde que cuanto más alto sea el nivel de seguridad, más posibilidades hay de que se produzcan falsos rechazos.
  - **Scan Timeout** (Tiempo de espera del escáner): configure el tiempo que debe transcurrir antes de que expire el tiempo del escáner de las huellas dactilares (de *1 sec* (1 s) a *20 sec* (20 s)). Si un usuario no coloca el dedo en el dispositivo durante el tiempo de espera, se producirá un fallo en la autorización.

- **Server Matching** (Identificación de servidor): active esta opción para identificar una huella dactilar o el id. de una tarjeta en el servidor BioStar, en lugar de en el dispositivo. Cuando se activa este modo, los dispositivos envían las plantillas de las huellas dactilares o las Id. de la tarjeta al servidor para verificar la identificación. Este modo resulta útil cuando posee más usuarios de los que se pueden descargar a un dispositivo, o cuando la información de usuario no se puede distribuir por motivos de seguridad.
- **1:N Fast Mode** (Modo rápido 1:N): configure el dispositivo para utilizar el modo rápido y reducir así el tiempo requerido para identificar las huellas dactilares (*Auto* (Automático), *Normal*, *Fast* (Rápido) o *Fastest* (Muy rápido)). Si se establece en modo *Auto* (Automático), la velocidad de identificación se ajustará automáticamente según el número de plantillas registradas.
- **Matching Timeout** (Tiempo de espera de la identificación): configure el tiempo que deberá transcurrir antes de que expire el tiempo del dispositivo para intentar identificar una huella dactilar (de *0 [Infinite]* (0 [Infinito] a *10 sec* (10 s)).
- **Check Fake Finger** (Comprobar dedo falso): configure el dispositivo para que detecte el uso de huellas dactilares falsas como, por ejemplo, las fabricadas con silicona o hule, y prevenir así un acceso no autorizado.

5.1.3.3 Pestaña Network (Red)

La pestaña Network (Red) permite personalizar la configuración del servidor y de la red para los dispositivos BioLite Net.

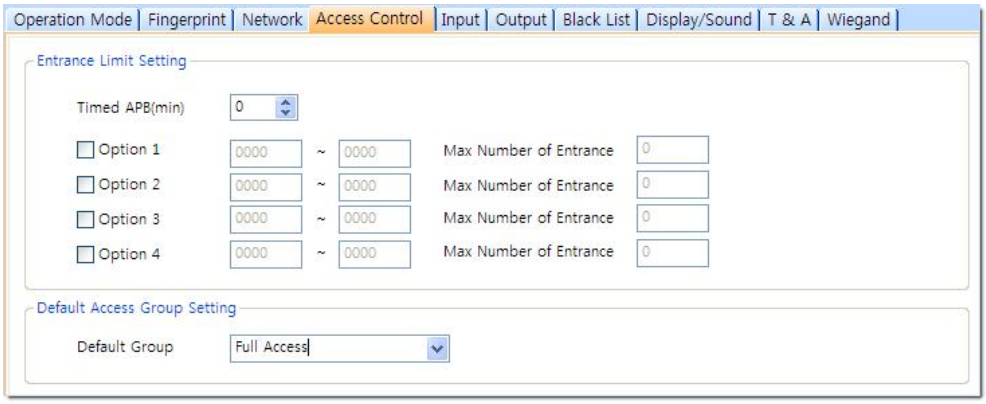


- **TCP/IP**
  - **Use DHCP** (Utilizar DHCP): haga click en este botón de radio para habilitar el protocolo de configuración de host dinámico (DHCP) en el dispositivo.
  - **Not Use DHCP** (No utilizar DHCP): haga click en este botón de radio para deshabilitar el protocolo de configuración de host dinámico (DHCP) en el dispositivo.
  - **IP Address** (Dirección IP): especifique una dirección IP para el dispositivo.
  - **Subnet** (Subred): especifique una dirección de subred para el dispositivo.
  - **Gateway** (Puerta de enlace): especifique una puerta de enlace de red.
  - **Port** (Puerto): especifique un puerto para utilizar el dispositivo.
- **Server (Servidor)**
  - **Use** (Utilizar): haga click en este botón de radio para utilizar los parámetros específicos del servidor.
  - **Not use** (No utilizar): haga click en este botón de radio para deshabilitar la configuración del servidor.
  - **IP Address** (Dirección IP): especifique una dirección IP para el servidor BioStar.
  - **Time sync with Server** (Sincronizar hora con servidor): seleccione esta casilla de validación para sincronizar la hora del dispositivo con la hora del servidor.
- **Support 100 Base-T** (Compatibilidad con 100 Base-T): esta opción permite habilitar o deshabilitar una conexión rápida de Ethernet para el dispositivo. Cuando se encuentre habilitada esta opción, el dispositivo detectará la red Ethernet y establecerá automáticamente la mejor conexión. Si no se habilita, el dispositivo intentará establecer una conexión Ethernet de 10Base-T.
  - **Use** (Utilizar): haga click en este botón de radio para habilitar la conexión 100base-T para el dispositivo.
  - **Not Use** (No utilizar): haga click en este botón de radio para deshabilitar la conexión 100base-T para el dispositivo.
- **RS485**
  - **Mode** (Modo): configure el modo de un dispositivo conectando mediante RS485 (*Disable* (Deshabilitar), *Host* (Anfitrión), *Slave* (Esclavo) o *PC Connection* (Conexión de PC)).

- **Baudrate** (Velocidad de transmisión): configure la velocidad en baudios de un dispositivo conectado mediante RS485 (de *9600* a *115200*).

5.1.3.4 Pestaña Access Control (Control de acceso)

La pestaña Access Control permite personalizar la configuración del límite de entrada y de los grupos de acceso predeterminados para un dispositivo BioLite Net.

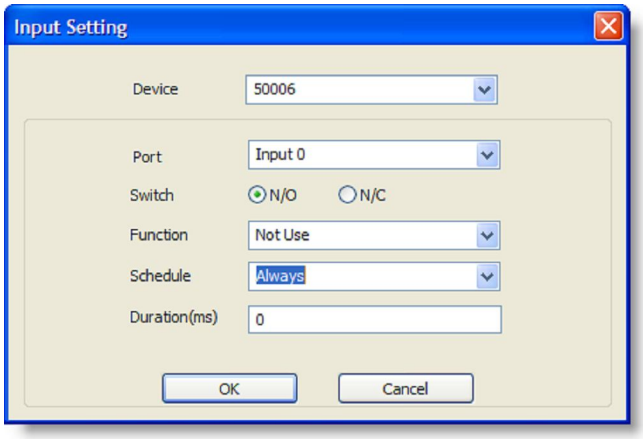


- **Entrance Limit Setting (Configuración del límite de entrada)**
  - **Timed APB (min)** (APB programado (min)): establezca el tiempo (en minutos) en que un usuario no podrá volver a entrar a una zona mediante el dispositivo. Una vez que un usuario haya conseguido entrar, el dispositivo rechazará la tarjeta o la huella dactilar del usuario durante el período de tiempo determinado aquí.
  - **Option 1-4** (Opción 1-4): haga click en la casilla de validación para habilitar el límite de entrada y luego especifique las horas efectivas para el mismo.
  - **Max Number of Entrance** (Número máximo de entradas): establezca el número máximo de entradas permitidas durante el límite de tiempo determinado.
- **Default Access Group Setting** (Configuración del grupo de acceso predeterminado): seleccione un grupo de acceso predeterminado para aplicar a los usuarios nuevos que no han sido asignados a ningún grupo de acceso.

5.1.3.5 Pestaña Input (Entrada)

La pestaña Input (Entrada) muestra los parámetros de entrada especificados para un dispositivo BioLite Net. Los botones que se encuentran en la parte inferior de la pestaña permiten añadir, modificar o eliminar parámetros de entrada. Para añadir o modificar los parámetros,

debe especificarlos en la ventana Input Setting (Configuración de entrada). (Cerrar puerta). Para obtener más información acerca de cómo configurar los parámetros de entrada, consulte la sección 3.9.3.2.



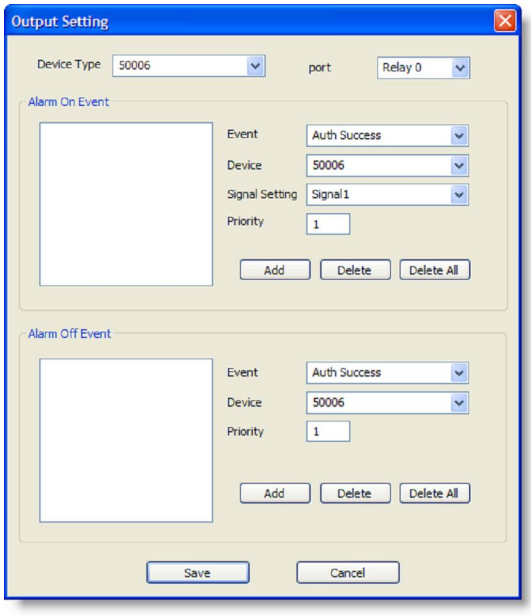
- **Device** (Dispositivo): seleccione el dispositivo BioLite Net (o Secure I/O) al que desea añadir o modificar los parámetros.
- **Port** (Puerto): seleccione un puerto de entrada (*Input 0* (Entrada 0), *Input 1* (Entrada 1), o *Tamper* (Alterar)). Para dispositivos Secure I/O, los siguientes parámetros están disponibles: *Input 0* (Entrada 0), *Input 1* (Entrada 1), *Input 2* (Entrada 2), *Input 3* (Entrada 3).
- **Switch** (Interruptor): haga click en los botones de radio para especificar la posición normal del interruptor de entrada (*N/O: normalmente abierto* o *N/C:* normalmente *cerrado*).
- **Function** (Función): seleccione la opción asociada a la entrada:
  - *Not Use* (No utilizar): el puerto de entrada no será supervisado.
  - *Generic Input* (Entrada genérica): el puerto de entrada se supervisará para una acción desencadenadora (para los eventos especificados con “Detect Input 1-3” (Detectar entrada 1-3), en la ventana Output settings (Configuración de salida), consulte la sección 5.1.3.6).
  - *Emergency Open* (Apertura de emergencia): abre las puertas controladas por este dispositivo. El período de apertura normal de puertas será ignorado y las puertas permanecerán abiertas hasta que un operador envíe la orden "Close Door" (Cerrar puerta) mediante la pestaña Door/Zone Monitoring (Supervisión de puerta/zona) (consulte la sección 4.4.1).
  - *Release All Alarms* (Cancelar todas las alarmas): cancela las alarmas asociadas a este dispositivo.
  - *Restart Device* (Reiniciar dispositivo): reinicia el dispositivo.
  - *Disable Device* (Deshabilitar dispositivo): deshabilita el dispositivo. Un dispositivo deshabilitado no se comunicará con el servidor

BioStar ni procesará huellas dactilares ni tarjetas. Para habilitar de nuevo la comunicación, un administrador debe introducir la contraseña maestra para un dispositivo BioStar o proporcionar autentificación de forma local para un dispositivo BioLite Net.

- **Schedule** (Programa): configure el programa para las acciones de entrada (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
- **Duration (ms)** (Duración (ms)): establezca la duración (en milisegundos) que una entrada debe durar para activar la acción establecida.

5.1.3.6 Pestaña Output (Salida)

La pestaña Output (Salida) muestra los parámetros de salida especificados para un dispositivo BioLite Net. Los botones que se encuentran en la parte inferior de la pestaña permiten añadir, modificar o eliminar parámetros de salida. Para añadir o modificar los parámetros, debe especificarlos en la ventana Output Setting (Configuración de salida). Para obtener más información acerca de cómo configurar los parámetros de salida, consulte la sección 3.9.3.1.



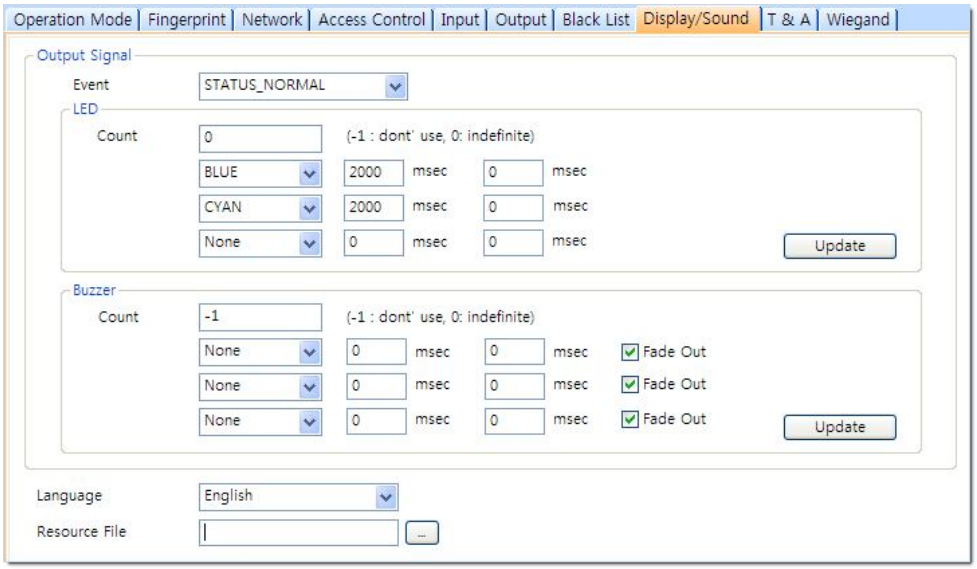
- **Device Type** (Tipo de dispositivo): seleccione el tipo de dispositivo al que añadirá o modificará los parámetros.
- **Port** (Puerto): seleccione un puerto de salida (*Relay 0*). Para dispositivos Secure I/O, los siguientes parámetros están disponibles: *Relay 0* o *Relay 1*.

- **Alarm On Event** (Evento para activar alarma): especifique la configuración y haga click en **Add** (Añadir) para añadir el evento a la lista Alarm On Event (Evento para activar alarma). Estos eventos activarán una alama.
  - **Event** (Evento): seleccione el evento que activará la alarma (*Auth Success* (Autorización con éxito), *Auth Fail* (Autorización fallida), *Auth Duress* (Autorización de peligro), *Anti-passback Fail* (Antipassback fallido), *Access Not Granted* (Acceso no permitido), *Entrance Limited* (Entrada limitada), *Admin Auth Success* (Autorización de administrador con éxito), *Tamper On* (Alteración activada), *Door Opened* (Puerta abierta), *Door Close* (Puerta cerrada), *Forced Open Door* (Puerta forzada abierta), *Held Open Door* (Puerta mantenida abierta), *Detect Input #1-3* (Detectar entrada #1-3)).
  - **Device** (Dispositivo): seleccione el dispositivo supervisado para un evento de alarma.
  - **Signal Setting** (Configuración de señal): seleccione una opción de señal anteriormente configurada en la barra de menú (**Option > Event > Output Port Setting** (Opción > Evento > Configuración del puerto de salida)).
  - **Priority** (Prioridad): establezca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para encender una alarma (activar) de prioridad 2 solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.
- **Alarm Off Event** (Evento para desactivar alarma): especifique la configuración y haga click en **Add** (Añadir) para añadir el evento a la lista Alarm Off Event (Evento para desactivar alarma). Estos eventos desactivarán una alama.
  - **Event** (Evento): seleccione el evento que desactivará la alarma (*Auth Success* (Autorización con éxito), *Auth Fail* (Autorización fallida), *Auth Duress* (Autorización de peligro), *Anti-passback Fail* (Antipassback fallido), *Access Not Granted* (Acceso no permitido), *Entrance Limited* (Entrada limitada), *Admin Auth Success* (Autorización de administrador con éxito), *Tamper On* (Alteración activada), *Door Opened* (Puerta abierta), *Door Close* (Puerta cerrada), *Forced Open Door* (Puerta forzada abierta), *Held Open Door* (Puerta mantenida abierta), *Detect Input #1-3* (Detectar entrada #1-3)).
  - **Device** (Dispositivo): seleccione el dispositivo supervisado para un evento de alarma.

- **Priority** (Prioridad): establezca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para encender una alarma (activar) solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.

5.1.3.7 Pestaña Display/Sound (Pantalla/Sonido)

La pestaña Display/Sound (Pantalla/Sonido) permite personalizar los comportamientos por evento del LED y del zumbido. Para guardar los cambios realizados en estos parámetros, deberá hacer click en **Update** (Actualizar) en la sección correspondiente para cada evento. También es posible personalizar el idioma utilizado en la pantalla del dispositivo.



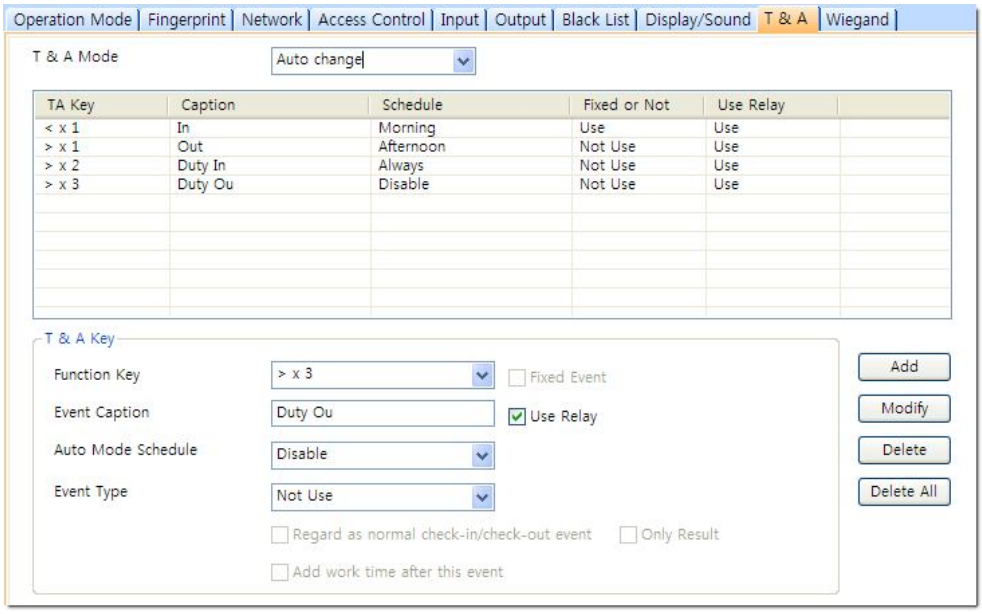
- **Event** (Evento):especifique el evento en cuestión seleccionándolo de la lista desplegable.
- **LED**:configure el comportamiento del LED para un evento determinado.
  - **Count** (Cuenta): introduzca el número de ciclos del LED para el evento determinado. Introduzca “0” para habilitar un ciclo infinito o “-1” para deshabilitar el LED.
  - **Colors** (Colores): especifique hasta tres colores de pantalla de la lista desplegable. El LED irá cambiando a estos colores en orden, de arriba a abajo. Al lado de cada color, introduzca el tiempo (en milisegundos) que el LED mostrará el color seleccionado y el tiempo (en milisegundos) que permanecerá apagado antes de cambiar al siguiente color del ciclo.
- **Buzzer** (Zumbido): configure el comportamiento del zumbido para un evento determinado.

- **Count** (Cuenta): introduzca el número de ciclos del LED para el evento determinado. Introduzca “0” para habilitar un ciclo infinito o “-1” para deshabilitar el LED.
- **Volume** (Volumen): configure hasta tres volúmenes de tono de la lista desplegable (*Low* (Bajo), *Middle* (Medio) o *High* (Alto)). El zumbido irá cambiando a estos volúmenes en orden, de arriba a abajo. Al lado de cada volumen, introduzca el tiempo (en milisegundos) que el zumbido se mantendrá en el volumen seleccionado y el tiempo (en milisegundos) que el zumbido se mantendrá apagado antes de cambiar al siguiente volumen del ciclo.
- **Fade Out** (Fundido de salida): configure el volumen del tono al que le afectará el fundido de salida, antes de avanzar al siguiente volumen del ciclo, haciendo click en esta casilla de validación.

- **Language** (Idioma): establezca el idioma utilizado en la pantalla (*Korean* (Coreano), *English* (Inglés) o *Custom* (Personalizado)).
- **Resource File** (Archivo de recursos): establezca el archivo de recursos lingüísticos, que se utilizará en la interfaz de BioStar, haciendo click en el botón de elipsis y localizando el archivo de recursos.

5.1.3.8 Pestaña T&A (Tiempo y asistencia)

La pestaña T&A permite configurar los parámetros del modo y de la clave para un dispositivo BioLite Net. Para guardar los cambios realizados en la configuración de tiempo y asistencia, debe hacer click en **Apply** (Aplicar) en la parte inferior de la pestaña. También puede aplicar la misma configuración a otros dispositivos haciendo click en **Apply to Others** (Aplicar a otros).



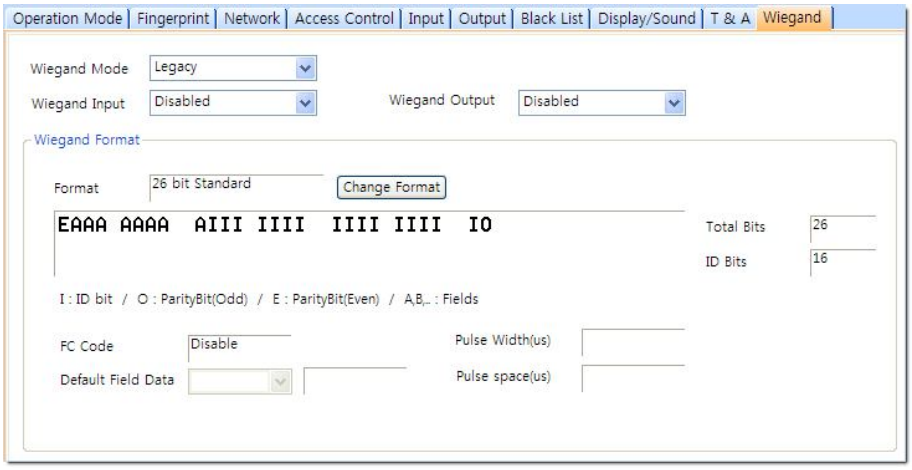
- **T&A Mode** (Modo de tiempo y asistencia): establezca el modo de tiempo y asistencia:
  - **Not Use** (No utilizar): deshabilita las funciones de tiempo y asistencia en este dispositivo.
  - **Manual** : los usuarios deben pulsar la tecla especificada cada vez que entren o salgan para registrar los eventos de tiempo y asistencia.
  - **Manual Fix** (Fijación manual): cuando se pulsa una tecla de tiempo y asistencia, el dispositivo permanecerá en este modo hasta que se pulse otra tecla de tiempo y asistencia.
  - **Auto change** (Cambio automático): el dispositivo cambiará automáticamente los modos de tiempo y asistencia para que se correspondan con las funciones especificadas para un período de tiempo.
  - **Event Fix** (Fijación de evento): el dispositivo solo realizará la función de tiempo y asistencia especificada.

- **T&A Key** (Tecla de tiempo y asistencia): especifique las teclas que se utilizarán para los eventos de tiempo y asistencia y los tipos de eventos asociados a ellas:
  - **Function Key** (Tecla de función): seleccione la tecla de función que se asignará al evento de tiempo y asistencia de la lista desplegable (**1-*15).* Si utiliza el modo Event Fix (Fijación de eventos), puede hacer click en la casilla de validación que se encuentra a la derecha para designar un evento fijo.
  - **Event Caption** (Leyenda de evento): introduzca una leyenda para el evento.
  - **Auto Mode Schedule** (Programa de modo automático): cuando utilice el modo Auto Change (Cambio automático), puede especificar cuándo ocurrirá el evento, seleccionando una zona horaria de la lista desplegable. Para obtener más información acerca de cómo crear una zona horaria, consulte la sección 3.6.1.
  - **Event Type** (Tipo de evento): configure el tipo de evento que se asignará a la tecla (*Not Use* (No utilizar), *Check In* (Entrada), *Check Out* (Salida), *In* (Dentro) o *Out* (Fuera)). In/Out indican los eventos de entrada y salida generales durante un día, mientras que Check In/Out indican los eventos de entrada y salida formales a la llegada y a la partida del lugar de trabajo, o los eventos de la primera entrada y de la última salida del día. Cuando elija Check In o Check Out, puede habilitar la opción “Regard as normal check-in/check-out event” (Considerar como evento de entrada/salida normal).

    Si se habilita esta opción, los usuarios que pulsen las teclas adecuadas se considerarán como si llegasen o saliesen a tiempo del trabajo, aunque en realidad lleguen tarde o se vayan temprano. Si habilita la opción “Only Result” (Solo resultado), los usuarios aparecerán en los reportes de tiempo y asistencia como si hubieran llegado a tiempo, pero el tiempo de trabajo se calculará correctamente en base a las horas de entrada y salida reales. Si elige *Out* (Fuera), puede habilitar la opción "Add work time after this event” (Añadir tiempo de trabajo después de este evento). Si se habilita esta opción, los usuarios que pulsen las teclas adecuadas se considerarán como si se hubieran quedado a trabajar durante el tiempo restante, aunque abandonen la oficina antes.

5.1.3.9 Pestaña Wiegand

La pestaña Wiegand permite configurar el formato Wiegand para un dispositivo BioLite Net. A diferencia de los dispositivos BioStation, solo se puede configurar un formato Wiegand a la vez (ya sea solo entrada o solo salida). Haga click en **Change Format** (Cambiar formato) para abrir el asistente de configuración Wiegand. Para activar la función Wiegand en un dispositivo BioLite Net, haga click en la casilla de validación que se encuentra en la parte superior derecha de la pestaña. Para obtener más información acerca de cómo configurar el formato Wiegand, consulte la sección 3.2.9.



- **Wiegand Mode** (Modo Wiegand): configure el modo de entrada Wiegand que se utilizará cuando se lean los datos de Id. de una tarjeta (*Legacy* (Heredado) o Extended (Extendido)). El modo Legacy (Heredado) procesará los datos de Id. de los dispositivos conectados en red y de los lectores de tarjetas por RFs de la misma forma (esta función es típica de las anteriores versiones de BioStar). El modo Extended (Extendido) permitirá que los lectores de tarjetas por RFs funcionen de manera independiente, lo que permite asociarlos a puertas, incluidas en zonas, y guardar los registros con las propias Id. del dispositivo.
- **Wiegand Input** (Entrada Wiegand): asigne la entrada Wiegand:
  - **Disabled** (Deshabilitada): la entrada no se utilizará.
  - **Wiegand [Card]** (Wiegand [Tarjeta]): el campo de Id. de la cadena Wiegand se interpreta como el id. de una tarjeta.
  - **Wiegand [User]** (Wiegand [Usuario]): el campo de Id. de la cadena Wiegand se interpreta como el id. de un usuario.

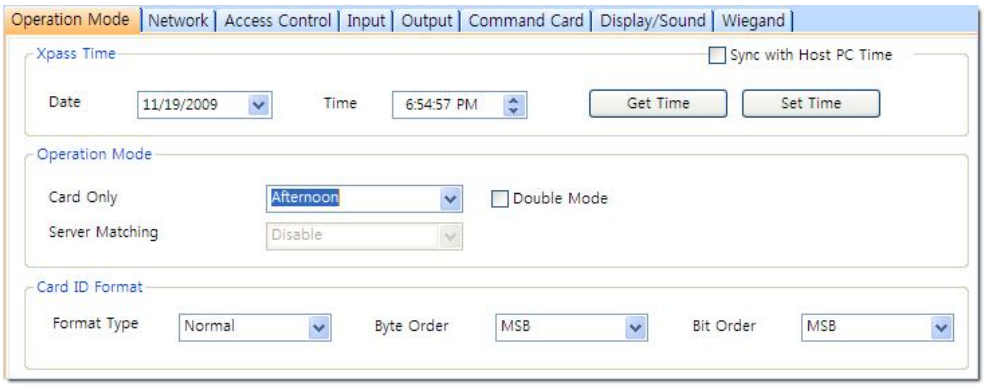
- **Wiegand Output** (Salida Wiegand): asigne la salida Wiegand:
  - **Disabled** (Deshabilitada): la salida no se utilizará.
  - **Wiegand [Card]** (Wiegand [Tarjeta]): inserta el id. de la tarjeta del usuario autentificado en el campo de Id. de la cadena Wiegand.
  - **Wiegand [User]** (Wiegand [Usuario]): inserta el id. de usuario del usuario autentificado en el campo de Id. de la cadena Wiegand.

5.1.4 Personalización de la configuración para dispositivos Xpass

Las siguientes secciones describen la configuración disponible para los dispositivos Xpass. Personalice la forma en que funcionan los dispositivos Xpass cambiando la configuración para que estos se adapten al entorno y a las necesidades operacionales particulares.

5.1.4.1 Pestaña Operation Mode (Modo de funcionamiento)

La pestaña Operation Mode (Modo de funcionamiento) permite personalizar la configuración de la hora y de varios modos de funcionamiento en los dispositivos Xpass.

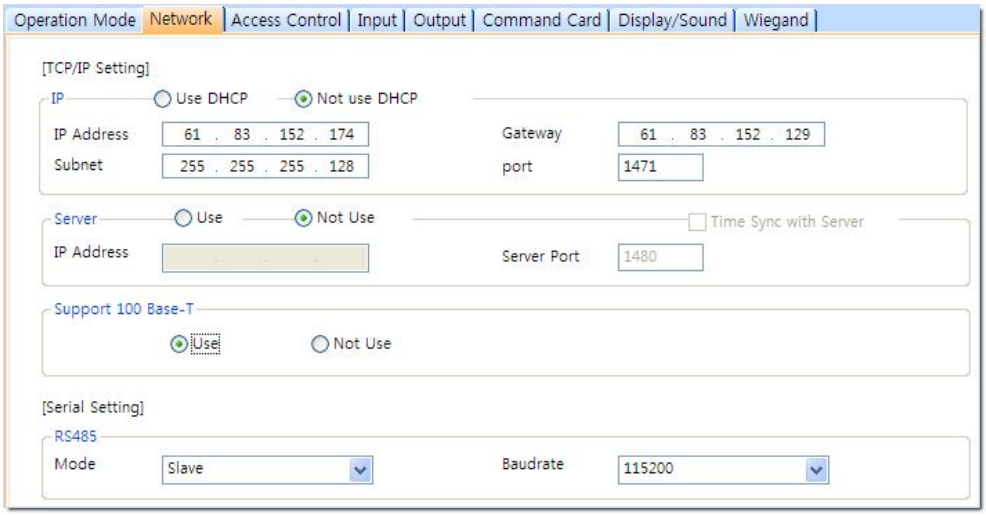


- **Xpass Time (Hora de Xpass)**
  - **Date** (Fecha): establezca manualmente la fecha del dispositivo en el calendario desplegable.
  - **Time** (Hora): establezca manualmente la hora del dispositivo.
  - **Sync with Host PC Time** (Sincronizar con la hora de la computadora central): seleccione esta casilla de validación para sincronizar automáticamente la hora del dispositivo con la hora de la computadora central.
  - **Get Time** (Obtener hora): obtenga la hora actual mostrada en el dispositivo.
  - **Set Time** (Establecer hora): establezca la hora del dispositivo.

- **Operation Mode** (Modo de funcionamiento): para todas las funciones siguientes, haga click en la casilla de validación correspondiente para habilitar el modo de verificación doble (Double Mode), que requiere la verificación de dos credenciales de usuario para permitir la entrada a una puerta.
  - **Card Only** (Solo tarjeta): configure el dispositivo para que solo solicite la autorización con tarjeta (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
  - **Server Matching** (Identificación de servidor): habilite esta opción para identificar el id. de una tarjeta en el servidor BioStar, en lugar de en el dispositivo. Cuando se activa este modo, el dispositivo envía el id. de la tarjeta al servidor para verificarla. Este modo resulta útil cuando posee más usuarios de los que se pueden descargar a un dispositivo, o cuando la información de usuario no se puede distribuir por motivos de seguridad.
- **Card ID Format (Formato de el id. de tarjeta)**
  - **Format Type** (Tipo de formato): establezca el tipo de procesamiento previo de los datos de el id. de una tarjeta (*Normal* o *Wiegand*). Si se selecciona “Normal”, los datos de el id. de una tarjeta se procesarán en su forma original. Si se selecciona “Wiegand”, los dispositivos interpretarán los datos de el id. de una tarjeta según la configuración del formato Wiegand.
  - **Byte Order** (Orden de bytes): especifique si desea intercambiar los datos de las tarjetas con Id. entre las tarjetas y los dispositivos por byte más significativo (*MSB*) o por byte menos significativo (*LSB*).
  - **Bit Order** (Orden de bits): especifique si desea intercambiar los datos de las tarjetas con Id. entre las tarjetas y los dispositivos por bit más significativo (*MSB*) o por bit menos significativo (*LSB*).

5.1.4.2 Pestaña Network (Red)

La pestaña Network (Red) permite personalizar la configuración del servidor y de la red para los dispositivos Xpass.

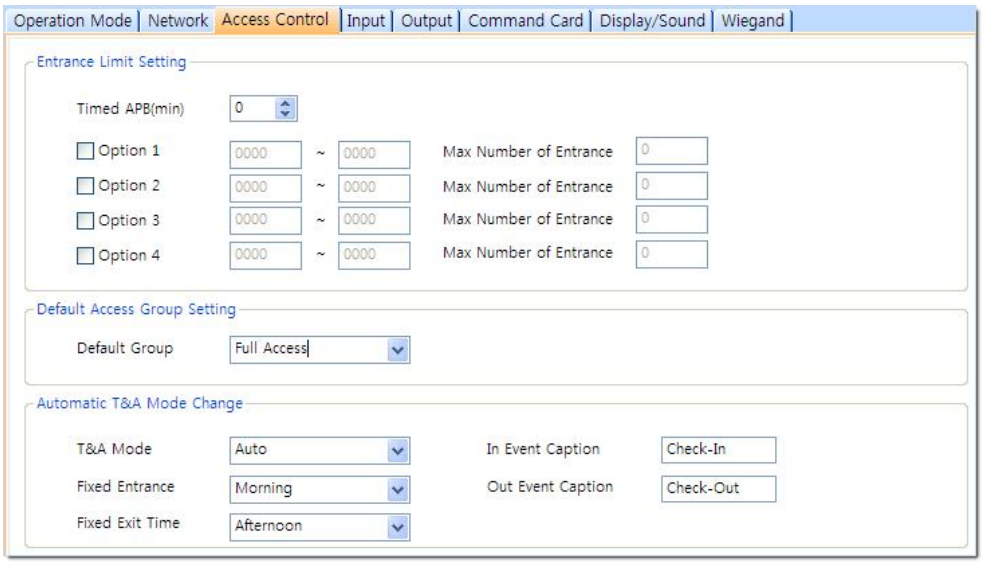


- **TCP/IP**
  - **Use DHCP** (Utilizar DHCP): haga click en este botón de radio para habilitar el protocolo de configuración de host dinámico (DHCP) en el dispositivo.
  - **Not Use DHCP** (No utilizar DHCP): haga click en este botón de radio para deshabilitar el protocolo de configuración de host dinámico (DHCP) en el dispositivo.
  - **IP Address** (Dirección IP): especifique una dirección IP para el dispositivo.
  - **Subnet** (Subred): especifique una dirección de subred para el dispositivo.
  - **Gateway** (Puerta de enlace): especifique una puerta de enlace de red.
  - **Port** (Puerto): especifique un puerto para utilizar el dispositivo.
- **Server (Servidor)**
  - **Use** (Utilizar): haga click en este botón de radio para utilizar los parámetros específicos del servidor.
  - **Not use** (No utilizar): haga click en este botón de radio para deshabilitar la configuración del servidor.
  - **IP Address** (Dirección IP): especifique una dirección IP para el servidor BioStar.
  - **Time sync with Server** (Sincronizar hora con servidor): seleccione esta casilla de validación para sincronizar la hora del dispositivo con la hora del servidor.

- **Support 100 Base-T** (Compatibilidad con 100 Base-T): esta opción permite habilitar o deshabilitar una conexión rápida de Ethernet para el dispositivo. Cuando se encuentre habilitada esta opción, el dispositivo detectará la red Ethernet y establecerá automáticamente la mejor conexión. Si no se habilita, el dispositivo intentará establecer una conexión Ethernet de 10Base-T.
  - **Use** (Utilizar): haga click en este botón de radio para habilitar la conexión 100base-T para el dispositivo.
  - **Not Use** (No utilizar): haga click en este botón de radio para deshabilitar la conexión 100base-T para el dispositivo.
- **RS485**
  - **Mode** (Modo): configure el modo de un dispositivo conectando mediante RS485 (*Disable* (Deshabilitar), *Host* (Anfitrión), *Slave* (Esclavo) o *PC Connection* (Conexión de PC)).
  - **Baudrate** (Velocidad de transmisión): configure la velocidad en baudios de un dispositivo conectado mediante RS485 (de *9600* a *115200*).

5.1.4.3 Pestaña Access Control (Control de acceso)

La pestaña Access Control permite personalizar la configuración del límite de entrada, de los grupos de acceso predeterminados y del modo de tiempo y asistencia para los dispositivos Xpass.



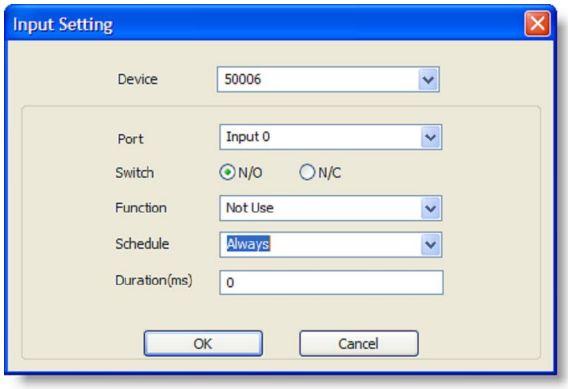
- **Entrance Limit Setting (Configuración del límite de entrada)**
  - **Timed APB (min)** (APB programado (min)): establezca el tiempo (en minutos) en que un usuario no podrá volver a entrar a una zona mediante el dispositivo. Una vez que un usuario haya conseguido entrar, el dispositivo rechazará la tarjeta o la huella dactilar del usuario durante el período de tiempo determinado aquí.

- **Option 1-4** (Opción 1-4): haga click en la casilla de validación para habilitar el límite de entrada y luego especifique las horas efectivas para el mismo.
- **Max Number of Entrance** (Número máximo de entradas): establezca el número máximo de entradas permitidas durante el límite de tiempo determinado.

- **Default Access Group Setting** (Configuración del grupo de acceso predeterminado): seleccione un grupo de acceso predeterminado para aplicar a los usuarios nuevos que no han sido asignados a ningún grupo de acceso.
- **Automatic T&A Mode Change (Cambio de modo de tiempo y asistencia automático)**
  - **T&A Mode** (Modo de tiempo y asistencia): configure el modo de tiempo y asistencia para el dispositivo (*Disable* (Deshabilitar), *Fixed In* (Entrada fija), *Fixed Out* (Salida fija) y *Auto* (Automático)).
  - **Fixed Entrance** (Entrada fija): cuando el modo de tiempo y asistencia "Auto" (Automático) está seleccionado, especifique cuándo se permitirán eventos de entrada seleccionando una zona horaria (*Always* (Siempre), *Disable* (Deshabilitar) o zona horaria personalizada) de la lista desplegable. Para obtener más información acerca de cómo crear una zona horaria, consulte la sección 3.6.1.
  - **Fixed Exit Time** (Hora de salida fija): cuando el modo de tiempo y asistencia "Auto" (Automático) está seleccionado, especifique cuándo se permitirán eventos de salida seleccionando una zona horaria (*Always* (Siempre), *Disable* (Deshabilitar) o zona horaria personalizada) de la lista desplegable. Para obtener más información acerca de cómo crear una zona horaria, consulte la sección 3.6.1.
  - **In Event Caption** (Leyenda de evento de entrada): establezca una leyenda para la entrada.
  - **Out Event Caption** (Leyenda de evento de salida): establezca una leyenda para la salida.

5.1.4.4 Pestaña Input (Entrada)

La pestaña Input (Entrada) muestra los parámetros de entrada especificados para un dispositivo Xpass. Los botones que se encuentran en la parte inferior de la pestaña permiten añadir, modificar o eliminar parámetros de entrada. Para añadir o modificar los parámetros, debe especificarlos en la ventana Input Setting (Configuración de entrada). (Cerrar puerta). Para obtener más información acerca de cómo configurar los parámetros de entrada, consulte la sección 3.9.3.2.



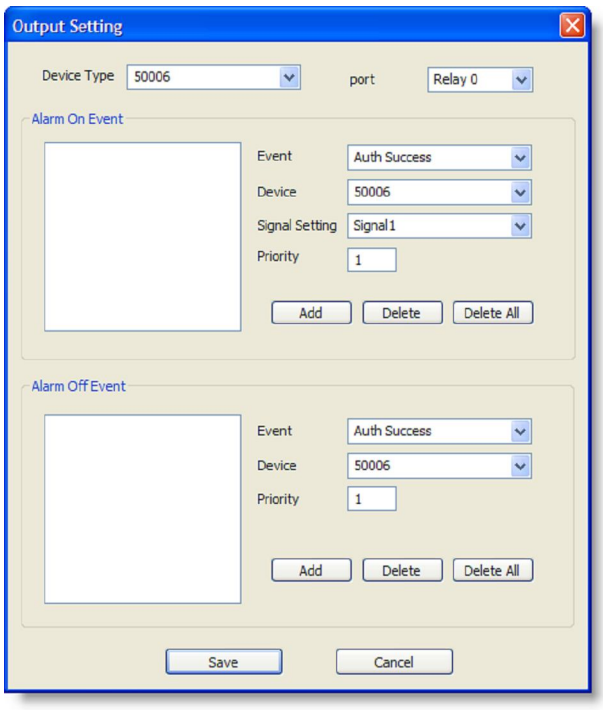
- **Device** (Dispositivo): seleccione el dispositivo Xpass (o Secure I/O) al que desea añadir o modificar los parámetros.
- **Port** (Puerto): seleccione un puerto de entrada (Input 0 (Entrada 0), Input 1 (Entrada 1), o Tamper (Alterar)). Para dispositivos Secure I/O, los siguientes parámetros están disponibles: Input 0 (Entrada 0), Input 1 (Entrada 1), Input 2 (Entrada 2), Input 3 (Entrada 3).
- **Switch** (Interruptor): haga click en los botones de radio para especificar la posición normal del interruptor de entrada (N/O: normalmente abierto o N/C: normalmente cerrado).
- **Function** (Función): seleccione la opción asociada a la entrada:
  - **Not Use** (No utilizar): el puerto de entrada no será supervisado.
  - **Generic Input** (Entrada genérica): el puerto de entrada se supervisará para una acción desencadenadora (para los eventos especificados con “Detect Input 1-3” (Detectar entrada 1-3), en la ventana Output settings (Configuración de salida), consulte la sección 5.1.4.5).
  - **Emergency Open** (Apertura de emergencia): abre las puertas controladas por este dispositivo. El período de apertura normal de puertas será ignorado y las puertas permanecerán abiertas hasta que un operador envíe la orden "Close Door" (Cerrar puerta) mediante la pestaña Door/Zone Monitoring (Supervisión de puerta/zona) (consulte la sección 4.4.1).

- **Release All Alarms** (Cancelar todas las alarmas): cancela las alarmas asociadas a este dispositivo.
- **Restart Device** (Reiniciar dispositivo): reinicia el dispositivo.
- **Disable Device** (Deshabilitar dispositivo): deshabilita el dispositivo. Un dispositivo deshabilitado no se comunicará con el servidor BioStar ni procesará huellas dactilares ni tarjetas. Para habilitar de nuevo la comunicación, un administrador debe introducir la contraseña maestra para un dispositivo BioStar o proporcionar autentificación de forma local para un dispositivo BioEntry Plus.

- **Schedule** (Programa): configure el programa para las acciones de entrada (*Always* (Siempre), *Disable* (Deshabilitar), o Custom Schedule (programa personalizado)).
- **Duration (ms)** (Duración (ms)): establezca la duración (en milisegundos) que una entrada debe durar para activar la acción establecida.

5.1.4.5 Pestaña Output (Salida)

La pestaña Output (Salida) muestra los parámetros de salida especificados para un dispositivo Xpass. Los botones que se encuentran en la parte inferior de la pestaña permiten añadir, modificar o eliminar parámetros de salida. Para añadir o modificar los parámetros, debe especificarlos en la ventana Output Setting (Configuración de salida). Para obtener más información acerca de cómo configurar los parámetros de salida, consulte la sección 3.9.3.1.



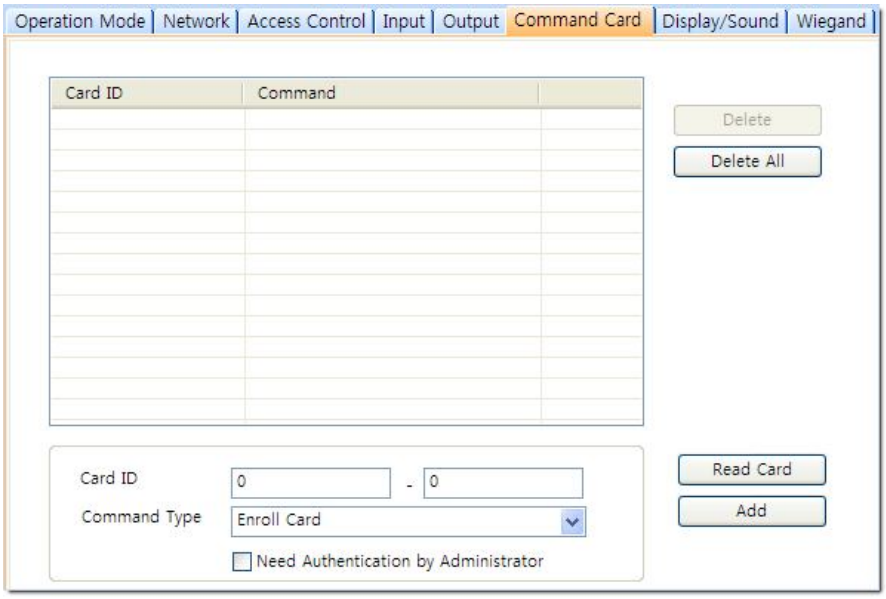
- **Device Type** (Tipo de dispositivo): seleccione el tipo de dispositivo al que añadirá o modificará los parámetros.
- **Port** (Puerto): seleccione un puerto de salida (*Relay 0*). Para dispositivos Secure I/O, los siguientes parámetros están disponibles: *Relay 0* o *Relay 1*.
- **Alarm On Event** (Evento para activar alarma): especifique la configuración y haga click en **Add** (Añadir) para añadir el evento a la lista Alarm On Event (Evento para activar alarma). Estos eventos activarán una alama.
  - **Event** (Evento): seleccione el evento que activará la alarma (*Auth Success* (Autorización con éxito), *Auth Fail* (Autorización fallida), *Auth Duress* (Autorización de peligro), *Anti-passback Fail* (Antipassback fallido), *Access Not Granted* (Acceso no permitido), *Entrance Limited* (Entrada limitada), *Admin Auth Success* (Autorización de administrador con éxito), *Tamper On* (Alteración activada), *Door Opened* (Puerta abierta), *Door Close* (Puerta cerrada), *Forced Open Door* (Puerta forzada abierta), *Held Open Door* (Puerta mantenida abierta), *Detect Input #1-3* (Detectar entrada #1-3)).
  - **Device** (Dispositivo): seleccione el dispositivo supervisado para un evento de alarma.
  - **Signal Setting** (Configuración de señal): seleccione una opción de señal anteriormente configurada en la barra de menú (**Option > Event > Output Port Setting** (Opción > Evento > Configuración del puerto de salida)).
  - **Priority** (Prioridad): establezca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para encender una alarma (activar) de prioridad 2 solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.
- **Alarm Off Event** (Evento para desactivar alarma): especifique la configuración y haga click en **Add** (Añadir) para añadir el evento a la lista Alarm Off Event (Evento para desactivar alarma). Estos eventos desactivarán una alama.
  - **Event** (Evento): seleccione el evento que desactivará la alarma (*Auth Success* (Autorización con éxito), *Auth Fail* (Autorización fallida), *Auth Duress* (Autorización de peligro), *Anti-passback Fail* (Antipassback fallido), *Access Not Granted* (Acceso no permitido), *Entrance Limited* (Entrada limitada), *Admin Auth Success* (Autorización de administrador con éxito), *Tamper On* (Alteración activada), *Door Opened* (Puerta abierta), *Door Close* (Puerta cerrada),

Forced Open Door (Puerta forzada abierta), *Held Open Door* (Puerta mantenida abierta), *Detect Input #1-3* (Detectar entrada #1-3)).

- **Device** (Dispositivo): seleccione el dispositivo supervisado para un evento de alarma.
- **Priority** (Prioridad): establezca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para encender una alarma (activar) solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.

5.1.4.6 Pestaña Command Card (Tarjeta de comando)

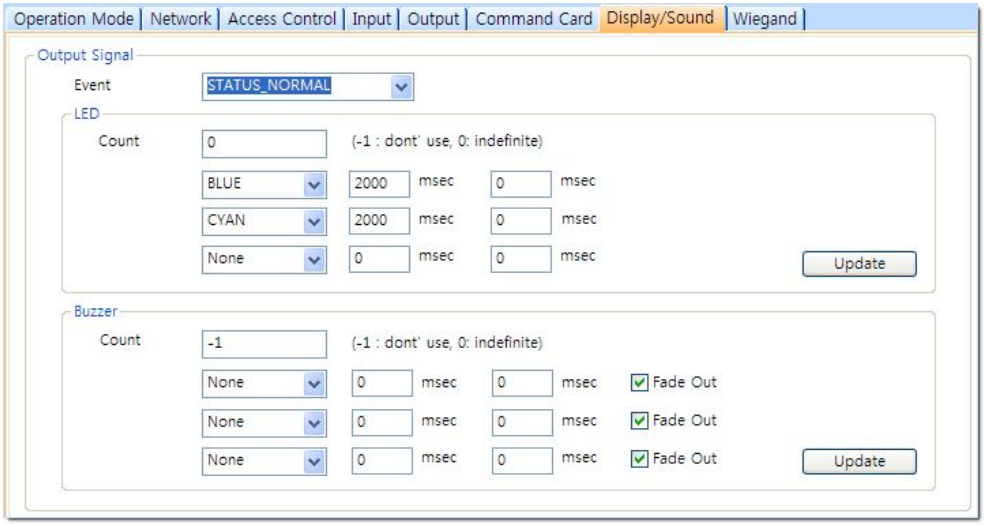
La pestaña Command Card (Tarjeta de comando) permite expedir tarjetas de comando. Para obtener más información acerca de las tarjetas de comando, consulte la sección 3.2.7.1.



- **Card ID** (Id. de tarjeta): introduzca el id. de la tarjeta o haga click en **Read Card** (Leer tarjeta) y coloque una tarjeta de comando en el lector para poblar automáticamente los campos.
- **Command Type** (Tipo de comando): seleccione el tipo de tarjeta de comando que desea expedir (*Enroll Card* (Tarjeta de registro), *Delete Card* (Tarjeta de eliminación) o *Delete All Card* (Tarjeta de eliminación total)).

5.1.4.7 Pestaña Display/Sound (Pantalla/Sonido)

La pestaña Display/Sound (Pantalla/Sonido) permite personalizar los comportamientos por evento del LED y del zumbido. Para guardar los cambios realizados en estos parámetros, deberá hacer click en **Update** (Actualizar) en la sección correspondiente para cada evento.



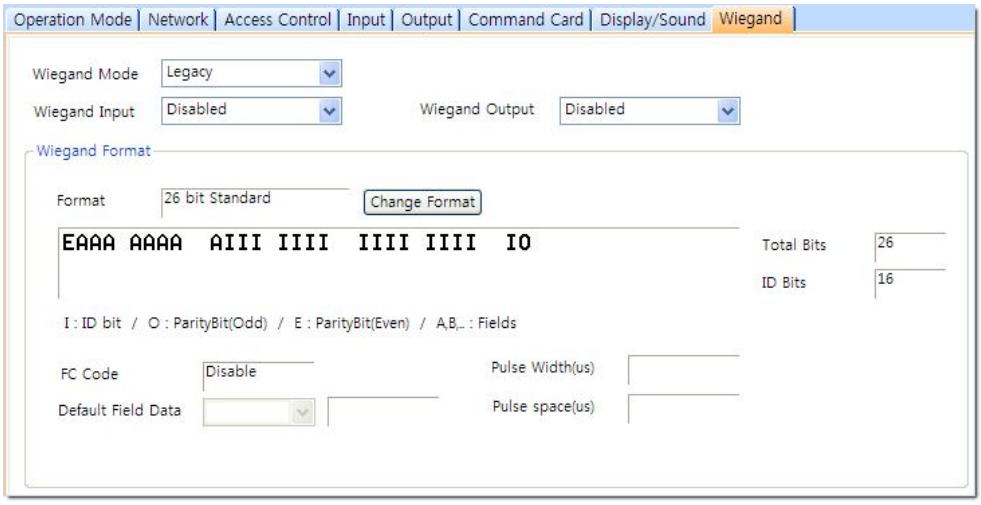
- **Event** (Evento):especifique el evento en cuestión seleccionándolo de la lista desplegable.
- **LED**:configure el comportamiento del LED para un evento determinado.
  - **Count** (Cuenta): introduzca el número de ciclos del LED para el evento determinado. Introduzca “0” para habilitar un ciclo infinito o “-1” para deshabilitar el LED.
  - **Colors** (Colores): especifique hasta tres colores de pantalla de la lista desplegable. El LED irá cambiando a estos colores en orden, de arriba a abajo. Al lado de cada color, introduzca el tiempo (en milisegundos) que el LED mostrará el color seleccionado y el tiempo (en milisegundos) que permanecerá apagado antes de cambiar al siguiente color del ciclo.
- **Buzzer** (Zumbido): configure el comportamiento del zumbido para un evento determinado.
  - **Count** (Cuenta): introduzca el número de ciclos del LED para el evento determinado. Introduzca “0” para habilitar un ciclo infinito o “-1” para deshabilitar el LED.
  - **Volume** (Volumen): configure hasta tres volúmenes de tono de la lista desplegable (*Low* (Bajo), *Middle* (Medio) o *High* (Alto)). El zumbido irá cambiando a estos volúmenes en orden, de arriba a abajo. Al lado de cada volumen, introduzca el tiempo (en

milisegundos) que el zumbido se mantendrá en el volumen seleccionado y el tiempo (en milisegundos) que el zumbido se mantendrá apagado antes de cambiar al siguiente volumen del ciclo.

- **Fade Out** (Fundido de salida): configure el volumen del tono al que le afectará el fundido de salida, antes de avanzar al siguiente volumen del ciclo, haciendo click en esta casilla de validación.

5.1.4.8 Pestaña Wiegand

La pestaña Wiegand permite configurar el formato Wiegand para un dispositivo Xpass. Haga click en **Change Format** (Cambiar formato) para abrir el asistente de configuración Wiegand. Para activar la función Wiegand en un dispositivo Xpass, haga click en la casilla de validación que se encuentra en la parte superior derecha de la pestaña. Para obtener más información acerca de cómo configurar el formato Wiegand, consulte la sección 3.2.9.



- **Wiegand Mode** (Modo Wiegand): configure el modo de entrada Wiegand que se utilizará cuando se lean los datos de Id. de una tarjeta (*Legacy* (Heredado) o *Extended* (Extendido)). El modo Legacy (Heredado) considerará a los dispositivos conectados mediante RFs como parte de los dispositivos anfitriones (esta función es típica de las anteriores versiones de BioStar). El modo Extended (Extendido) permitirá que los lectores de tarjetas por RFs funcionen de manera independiente, lo que permite asociarlos a puertas, incluidas en zonas, y guardar los registros con las propias Id. del dispositivo.
- **Wiegand Input** (Entrada Wiegand): asigne la entrada Wiegand:
  - **Disabled** (Deshabilitada): la entrada no se utilizará.
  - **Wiegand [Card]** (Wiegand [Tarjeta]): el campo de Id. de la cadena Wiegand se interpreta como el id. de una tarjeta.

- **Wiegand [User]** (Wiegand [Usuario]): el campo de Id. de la cadena Wiegand se interpreta como el id. de un usuario.

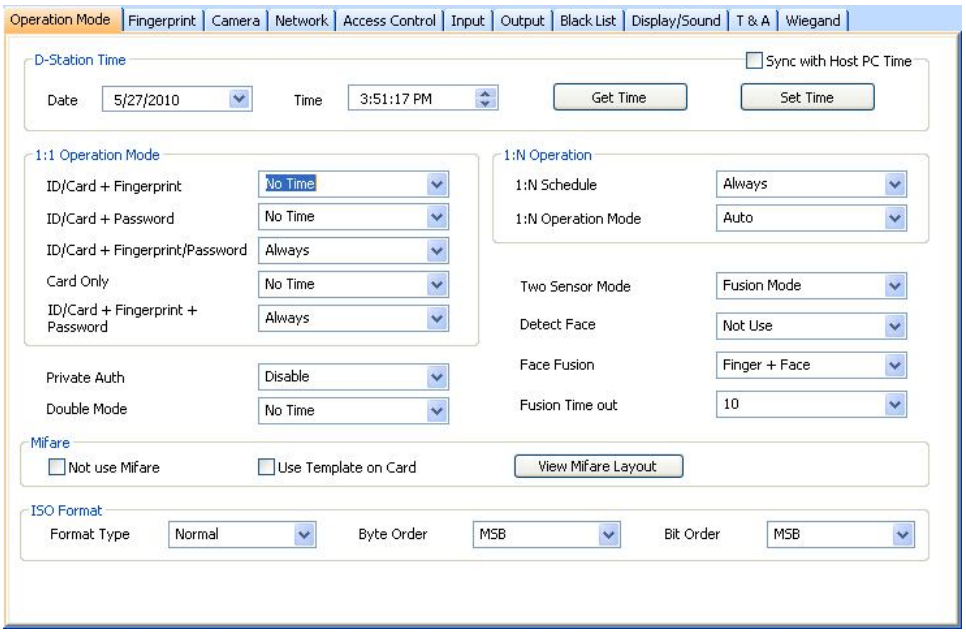
- **Wiegand Output** (Salida Wiegand): asigne la salida Wiegand:
  - **Disabled** (Deshabilitada): la salida no se utilizará.
  - **Wiegand [Card]** (Wiegand [Tarjeta]): inserta el id. de la tarjeta del usuario autentificado en el campo de Id. de la cadena Wiegand.
  - **Wiegand [User]** (Wiegand [Usuario]): inserta el id. de usuario del usuario autentificado en el campo de Id. de la cadena Wiegand.

5.1.5 Personalización de la configuración para dispositivos D-Station

Las siguientes secciones describen la configuración disponible para los dispositivos D-Station. Personalice la forma en que funcionan los dispositivos D-Station cambiando la configuración para que estos se adapten al entorno y a las necesidades operacionales particulares.

5.1.5.1 Pestaña Operation Mode (Modo de funcionamiento)

La pestaña Operation Mode (Modo de funcionamiento) permite personalizar la configuración de la hora y de varios modos de funcionamiento en los dispositivos D-Station.



- **D-Station Time (Hora de D-Station)**
  - **Date** (Fecha): establezca manualmente la fecha del dispositivo en el calendario desplegable.
  - **Time** (Hora): establezca manualmente la hora del dispositivo.

- **Sync with Host PC Time** (Sincronizar con la hora de la computadora central): seleccione esta casilla de validación para sincronizar automáticamente la hora del dispositivo con la hora de la computadora central.
- **Get Time** (Obtener hora): obtenga la hora actual mostrada en el dispositivo.
- **Set Time** (Establecer hora): establezca la hora del dispositivo.

- **1:1 Operation Mode** (Modo de funcionamiento 1:1): las listas desplegables de esta sección permiten controlar el modo de autentificación por programa. Por ejemplo, puede elegir un modo de autentificación normal para horas de trabajo, y un modo de autentificación más estricto para horas fuera del programa normal. Puede especificar modos de autentificación por dispositivo o por usuario (consulte la sección 5.4.1). A menos que se especifique un modo particular para un usuario, se aplicará el modo de autentificación del dispositivo.
  - **ID/Card + Fingerprint** (Id./Tarjeta + Huella dactilar): configure el dispositivo para que solicite una Id. o una tarjeta además de la autorización con huella dactilar (*Always* (Siempre) o *No Time* (Nunca)).
  - **ID/Card + Password** (Id./Tarjeta + Contraseña): configure el dispositivo para que solicite una Id. o una tarjeta además de la autorización con contraseña (*Always* (Siempre) o *No Time* (Nunca)).
  - **ID/Card + Fingerprint/Password** (Id./Tarjeta + Huella dactilar/Contraseña): configure el dispositivo para que solicite una Id. o una tarjeta además de la autorización con huella dactilar o contraseña (*Always* (Siempre) o *No Time* (Nunca)).
  - **Card Only** (Solo tarjeta): configure el dispositivo para que solo solicite la autorización con tarjeta (*Always* (Siempre) o *No Time* (Nunca)).
  - **ID/Card + Fingerprint + Password** (Id./Tarjeta + Huella dactilar + Contraseña): configure el dispositivo para que solicite una Id. o una tarjeta además de la autorización con huella dactilar y contraseña (*Always* (Siempre) o *No Time* (Nunca)).
- **1:N Operation (Funcionamiento 1:N)**
  - **1:N Schedule** (Programa 1:N): establezca un programa para utilizar solamente la autentificación con huella dactilar (*Always* (Siempre) o *No Time*(Nunca)).
  - **1:N Operation Mode** (Modo de funcionamiento 1:N): establezca un método para activar el sensor de huellas dactilares (*Auto* (Automático), *Ok/Function Key* (Aceptar/Clave de función), o *None* (Ninguno)).
- **Two Sensor Mode (Modo de dos sensores)**

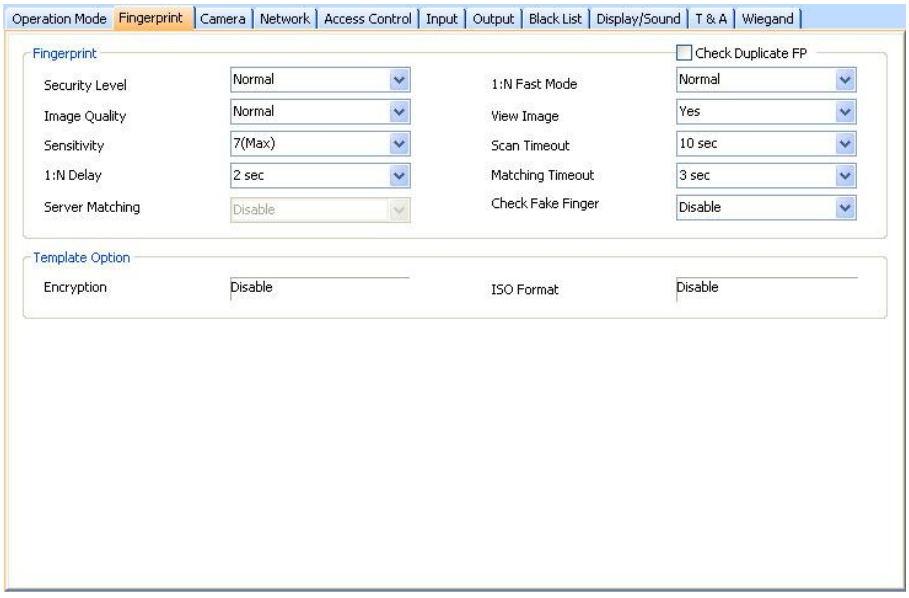
- **Fast Mode** (Modo rápido): el dispositivo proporcionará la autentificación más rápida.
- **Fusion Mode** (Modo fusión): la autentificación se realiza utilizando un algoritmo que permite que los usuarios escaneen dos dedos registrados, aumentando el índice de autentificación de cada dedo.
- **Twin Mode** (Modo gemelos): cada sensor trabaja de forma independiente para autentificar simultáneamente hasta dos usuarios.

- **Detect Face (Detección de rostro)**
  - configure el dispositivo para que capture la imagen de un rostro. Después de que se realice con éxito una autentificación, la imagen capturada se almacena en el registro de eventos y se podrá utilizar más tarde con fines de verificación.
- **Face Fusion (Fusión de rostro)**
  - configure el dispositivo para que utilice la fusión de rostro en la autentificación. Esta configuración puede mejorar los índices de autentificación de algunos usuarios. También se puede utilizar en conjunto con el modo rápido (Fast Mode) o con el modo fusión (Fusion Mode) en la configuración del modo de dos sensores (Two Sensor Mode).
- **Fusion Time out (Tiempo de espera de fusión)**
  - configure el dispositivo para que se acabe el tiempo de espera después de un número determinado de minutos, en caso de que no se realice con éxito la autentificación (1-20).
- **Otras opciones**
  - **Private Auth** (Autorización privada): configure el dispositivo para permitir un método de autorización privada (*Disable* (Deshabilitar) o *Enable* (Habilitar)). Si se habilita, el modo de autentificación del usuario se determinará por la configuración de la autorización (Authorization) de un usuario, que se encuentra en la pestaña Details (Detalles). Si se deshabilita, el modo de autentificación se determinará por la configuración del modo de funcionamiento del dispositivo.
  - **Double Mode** (Modo doble): configure el dispositivo para que solicite la autentificación de dos tarjetas de acceso o huellas dactilares de usuarios (*Always* (Siempre) o *No Time* (Nunca)). El tiempo de espera para presentar la segunda autentificación es de 15 segundos.

- **Mifare**
  - **Not use Mifare** (No utilizar Mifare): seleccione esta casilla de validación para deshabilitar la autorización con tarjeta MIFARE.
  - **Use Template on Card** (Utilizar plantilla en tarjeta): seleccione esta casilla de validación para que se utilice la plantilla en la tarjeta MIFARE en la autorización.
  - **View Mifare Layout** (Visualizar distribución Mifare): haga click en este botón para visualizar la distribución MIFARE utilizada por el dispositivo. Para obtener más información acerca de cómo configurar la distribución MIFARE, consulte la sección 3.5.4.6.
- **ISO Format (Formato ISO)**
  - **Format Type** (Tipo de formato): establezca el tipo de procesamiento previo de los datos de el id. de una tarjeta (*Normal* o *Wiegand*). Si se selecciona "Normal", los datos de el id. de una tarjeta se procesarán en su forma original. Si se selecciona "Wiegand", los dispositivos interpretarán los datos de el id. de una tarjeta según la configuración del formato Wiegand.
  - **Byte Order** (Orden de bytes): especifique si desea intercambiar los datos de las tarjetas con Id. entre las tarjetas y los dispositivos por byte más significativo (*MSB*) o por byte menos significativo (*LSB*).
  - **Bit Order** (Orden de bits): especifique si desea intercambiar los datos de las tarjetas con Id. entre las tarjetas y los dispositivos por bit más significativo (*MSB*) o por bit menos significativo (*LSB*).

5.1.5.2 Pestaña Fingerprint (Huella dactilar)

La pestaña Fingerprint (Huella dactilar) permite personalizar la configuración de la autorización con huella dactilar para los dispositivos D-Station.

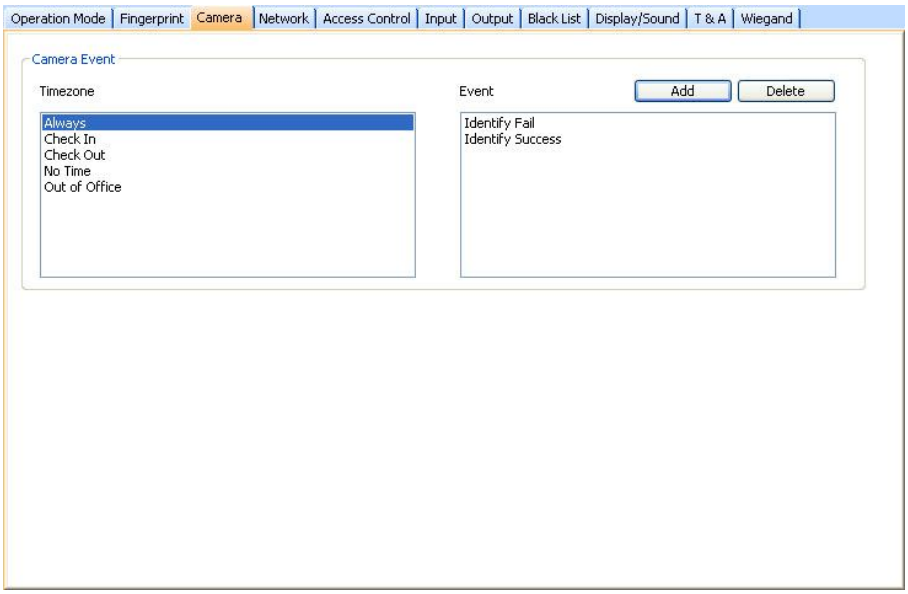


- **Fingerprint (Huella dactilar)**
  - **Security Level** (Nivel de seguridad): establezca el nivel de seguridad que utilizar para la autorización con huella dactilar (*Normal* (Normal), *Secure* (Seguro), or *Most Secure* (Muy seguro)). Recuerde que cuanto más alto sea el nivel de seguridad, más posibilidades hay de que se produzcan falsos rechazos.
  - **Image Quality** (Calidad de imagen): establezca la rigurosidad de la comprobación de calidad para las lecturas de las huellas dactilares (*Weak*(Débil), *Normal* (Normal), o *Strict* (Estricto)). Si la imagen de una huella dactilar está por debajo del nivel de calidad, será rechazada.
  - **Sensitivity** (Sensibilidad): configure la sensibilidad del escáner para huellas dactilares (de *0 [Min]* (0 [mín.]) a *7 [Max]* (7 [máx.]). Si se establece una mayor sensibilidad, las huellas dactilares se capturarán más fácilmente, pero también aumentará la sensibilidad al ruido externo.
  - **1:N Delay** (Retraso 1:N): establezca el retraso entre los escáneres cuando identifique las huellas dactilares (de *0 sec* (0 s) a *10 sec* (10 s)). Este retraso evitará que el escáner procese la misma huella dactilar más de una vez en caso de que un usuario no haya retirado para entonces su dedo del escáner.
  - **Server Matching** (Identificación de servidor): active esta opción para identificar una huella dactilar o el id. de una tarjeta en el servidor BioStar, en lugar de en el dispositivo. Cuando se activa este modo, los dispositivos envían las plantillas de las huellas dactilares o las Id. de la tarjeta al servidor para verificar la identificación. Este modo resulta útil cuando posee más usuarios de los que se pueden descargar a un dispositivo, o cuando la información de usuario no se puede distribuir por motivos de seguridad.
  - **1:N Fast Mode** (Modo rápido 1:N): configure el dispositivo para utilizar el modo rápido y reducir así el tiempo requerido para identificar las huellas dactilares (*Auto* (Automático), *Normal*, *Fast* (Rápido) o *Fastest* (Muy rápido)). Si se establece en modo *Auto* (Automático), la velocidad de identificación se ajustará automáticamente según el número de plantillas registradas.
  - **View Image** (Visualizar imagen): configure si quiere mostrar u ocultar las imágenes de las huellas dactilares en la pantalla de BioStation (*Yes* (Sí) o *No*).

- **Scan Timeout** (Tiempo de espera del escáner): configure el tiempo que debe transcurrir antes de que expire el tiempo del escáner de las huellas dactilares (de *1 sec* (1 s) a *20 sec* (20 s)). Si un usuario no coloca el dedo en el dispositivo durante el tiempo de espera, se producirá un fallo en la autorización.
- **Matching Timeout** (Tiempo de espera de la identificación): configure el tiempo que deberá transcurrir antes de que expire el tiempo del dispositivo para intentar identificar una huella dactilar (de *0 [Infinite]* (0 [Infinito] a *10 sec* (10 s)).
- **Check Fake Finger** (Comprobar dedo falso): configure el dispositivo para que detecte el uso de huellas dactilares falsas como, por ejemplo, las fabricadas con silicona o hule, y prevenir así un acceso no autorizado.
- **Template Option** (Opción de plantilla): muestra la configuración de las plantillas de huellas dactilares. Para obtener más información acerca de las plantillas de huellas dactilares, consulte la sección 4.9.

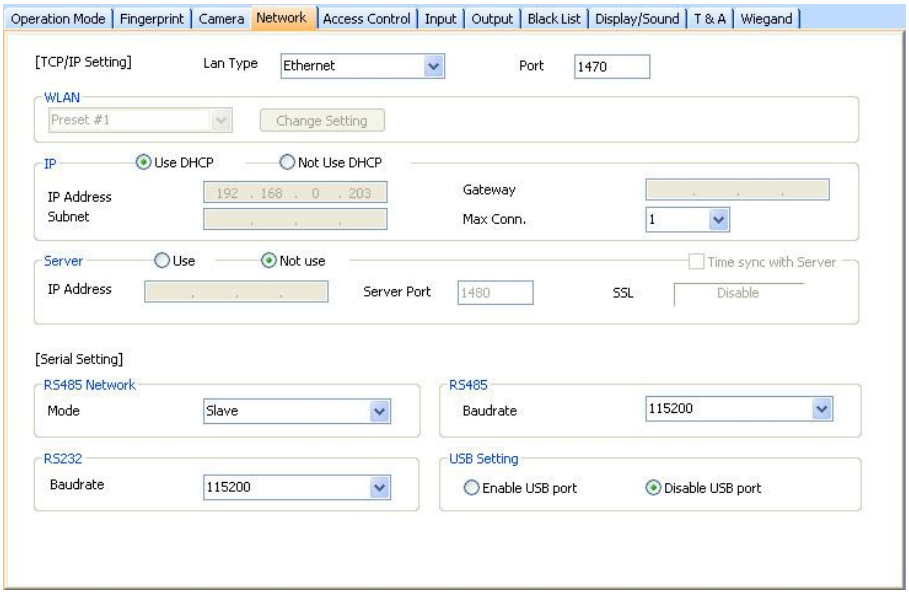
5.1.5.3 Pestaña Camera (Cámara)

La pestaña Camera (Cámara) permite controlar la forma en que se utiliza la cámara con fines de autorización. En el campo Timezone (Zona horaria), seleccione una zona horaria para el evento especificado. Haga click en **Add** (Añadir) para seleccionar el evento que activará la cámara. Haga click en **Apply** (Aplicar) para guardar los cambios.



5.1.5.4 Pestaña Network (Red)

La pestaña Network (Red) permite personalizar la configuración del servidor y de la red para los dispositivos D-Station.



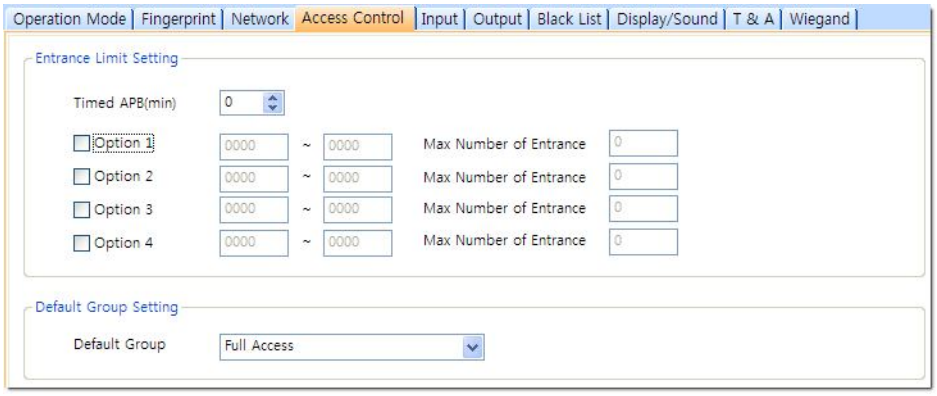
- **TCP/IP Setting (Configuración TCP/IP)**
  - **LAN Type** (Tipo de LAN): seleccione un tipo de conexión LAN de la lista desplegable (*Disable* (Deshabilitar), *Ethernet*, o *Wireless LAN*).
  - **Port** (Puerto): especifique un puerto para utilizar el dispositivo.
- **WLAN**
  - **Change setting** (Cambiar configuración): haga click para especificar los parámetros de una red de área local inalámbrica (WLAN). Esta opción solo está activa cuando se selecciona WLAN como la configuración de TCP/IP. Para obtener más información acerca de cómo configurar los parámetros de una conexión WLAN, consulte la sección 3.2.4.1.
- **IP**
  - **Use DHCP** (Utilizar DHCP): haga click en este botón de radio para habilitar el protocolo de configuración de host dinámico (DHCP) en el dispositivo.
  - **Not Use DHCP** (No utilizar DHCP): haga click en este botón de radio para deshabilitar el protocolo de configuración de host dinámico (DHCP) en el dispositivo.
  - **IP Address** (Dirección IP): especifique una dirección IP para el dispositivo.
  - **Subnet** (Subred): especifique una dirección de subred para el dispositivo.

- **Gateway** (Puerta de enlace): especifique una puerta de enlace de red.
- **Max Conn.** (Conexiones máximas): especifique el número máximo de conexiones permitidas.

- **Server (Servidor)**
  - **Use** (Utilizar): haga click en este botón de radio para habilitar el modo servidor.
  - **Not use** (No utilizar): haga click en este botón de radio para deshabilitar la configuración del servidor.
  - **IP Address** (Dirección IP): especifique una dirección IP para el servidor BioStar.
  - **Server Port** (Puerto del servidor): especifique el puerto utilizado para conectarse al servidor.
  - **SSL**: muestra el estado de SSL para la conexión del servidor.
  - **Time sync with Server** (Sincronizar hora con servidor): seleccione esta casilla de validación para sincronizar la hora del dispositivo con la hora del servidor.
- **RS485 Network (Red RS485)**
  - **Mode** (Modo): configure el modo de un dispositivo conectando mediante RS485 (*Disable* (Deshabilitar), *Host* (Anfitrión) o *Slave* (Esclavo)). Para obtener más información acerca de los modos RS485, consulte las secciones 3.2.1 y 3.2.2.
- **RS485**
  - **Baudrate** (Velocidad de transmisión): configure la velocidad en baudios de un dispositivo conectado mediante RS485 (de *9600* a *115200*).
- **RS232**
  - **Baudrate** (Velocidad de transmisión): configure la velocidad en baudios de un dispositivo conectado mediante RS232 (de *9600* a *115200*).
- **USB Setting** (Configuración de USB): haga click en los botones de radio para habilitar o deshabilitar el puerto USB en el dispositivo D-Station.

5.1.5.5 Pestaña Access Control (Control de acceso)

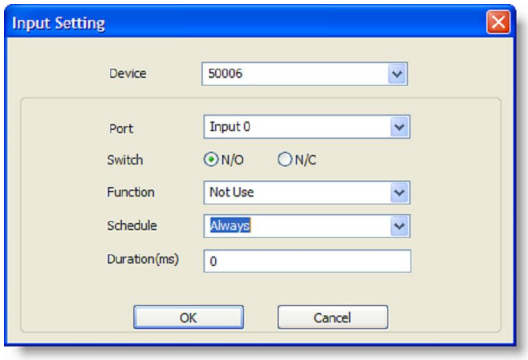
La pestaña Access Control permite personalizar la configuración del límite de entrada y de los grupos de acceso predeterminados para un dispositivo D-Station.



- **Entrance Limit Setting (Configuración del límite de entrada)**
  - **Timed APB (min)** (APB programado (min)): establezca el tiempo (en minutos) en que un usuario no podrá volver a entrar a una zona mediante el dispositivo. Una vez que un usuario haya conseguido entrar, el dispositivo rechazará la tarjeta o la huella dactilar del usuario durante el período de tiempo determinado aquí.
  - **Option 1-4** (Opción 1-4): haga click en la casilla de validación para habilitar el límite de entrada y luego especifique las horas efectivas para el mismo.
  - **Max Number of Entrance** (Número máximo de entradas): establezca el número máximo de entradas permitidas durante el límite de tiempo determinado.
- **Default Group Setting** (Configuración del grupo predeterminado): seleccione un grupo de acceso predeterminado para aplicar a los usuarios nuevos que no han sido asignados a ningún grupo de acceso.

5.1.5.6 Pestaña Input (Entrada)

La pestaña Input (Entrada) muestra los parámetros de entrada especificados para un dispositivo D-Station. Los botones que se encuentran en la parte inferior de la pestaña permiten añadir, modificar o eliminar parámetros de entrada. Para añadir o modificar los parámetros, debe especificarlos en la ventana Input Setting (Configuración de entrada). (Cerrar puerta). Para obtener más información acerca de cómo configurar los parámetros de entrada, consulte la sección 3.9.3.2.

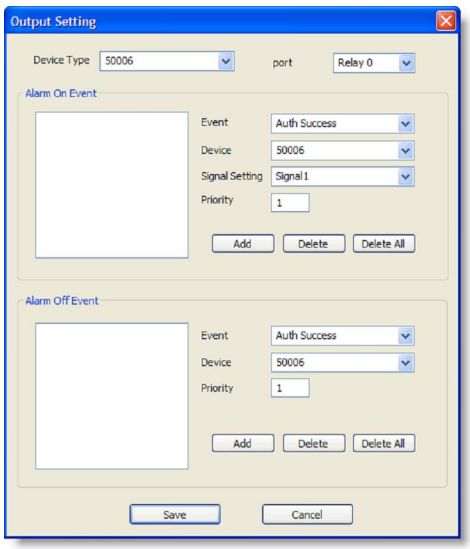


- **Device Type** (Tipo de dispositivo): seleccione el dispositivo D-Station al que añadirá o modificará los parámetros.
- **Port** (Puerto): seleccione un puerto de entrada (Input 0 (Entrada 0), Input 1 (Entrada 1), o Tamper (Alterar)). Para dispositivos Secure I/O, los siguientes parámetros están disponibles: Input 0 (Entrada 0), Input 1 (Entrada 1), Input 2 (Entrada 2), Input 3 (Entrada 3).
- **Switch** (Interruptor): haga click en los botones de radio para especificar la posición normal del interruptor de entrada (N/O: normalmente abierto o N/C: normalmente cerrado).
- **Function** (Función): seleccione la opción asociada a la entrada:
  - **Not Use** (No utilizar): el puerto de entrada no será supervisado.
  - **Generic Input** (Entrada genérica): el puerto de entrada se supervisará para una acción desencadenadora (para los eventos especificados con “Detect Input 0-3” (Detectar entrada 0-3), en la ventana Output settings (Configuración de salida), consulte la sección 5.1.1.6).
  - **Emergency Open** (Apertura de emergencia): abre las puertas controladas por este dispositivo. El período de apertura normal de puertas será ignorado y las puertas permanecerán abiertas hasta que un operador envíe la orden "Close Door" (Cerrar puerta) mediante la pestaña Door/Zone Monitoring (Supervisión de puerta/zona) (consulte la sección 4.4.1).
  - **Release All Alarms** (Cancelar todas las alarmas): cancela las alarmas asociadas a este dispositivo.
  - **Restart Device** (Reiniciar dispositivo): reinicia el dispositivo.
  - **Disable Device** (Deshabilitar dispositivo): deshabilita el dispositivo. Un dispositivo deshabilitado no se comunicará con el servidor BioStar ni procesará huellas dactilares ni tarjetas. Para habilitar de nuevo la comunicación, un administrador debe autentificarse en el dispositivo.

- **Schedule** (Programa): configure el programa en el que se supervisarán las entradas (*Always* (Siempre) o *No Time* (Nunca)).
- **Duration (ms)** (Duración (ms)): establezca la duración (en milisegundos) que una entrada debe durar para activar la acción establecida.

5.1.5.7 Pestaña Output (Salida)

La pestaña Output (Salida) muestra los parámetros de salida especificados para un dispositivo D-Station. Los botones que se encuentran en la parte inferior de la pestaña permiten añadir, modificar o eliminar parámetros de salida. Para añadir o modificar los parámetros, debe especificarlos en la ventana Output Setting (Configuración de salida). Para obtener más información acerca de cómo configurar los parámetros de salida, consulte la sección 3.9.3.1.



- **Device Type** (Tipo de dispositivo): seleccione el tipo de dispositivo al que añadirá o modificará los parámetros.
- **Port** (Puerto): seleccione un puerto de salida (Relay 0). Para dispositivos Secure I/O, los siguientes parámetros están disponibles: Relay 0 o Relay 1.
- **Alarm On Event** (Evento para activar alarma): especifique la configuración y haga click en **Add** (Añadir) para añadir el evento a la lista Alarm On Event (Evento para activar alarma). Estos eventos activarán una alama.
  - **Event** (Evento): seleccione el evento que activará la alarma (*Auth Success* (Autorización con éxito), *Auth Fail* (Autorización fallida), *Auth Duress* (Autorización de peligro), *Anti-passback Fail* (Antipassback fallido), *Access Not Granted* (Acceso no permitido),

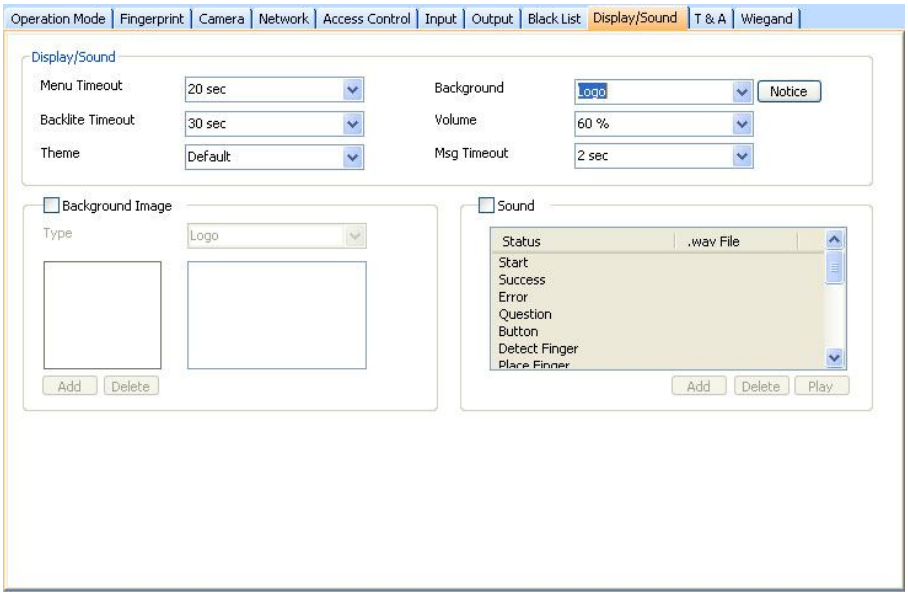
Entrance Limited (Entrada limitada), *Admin Auth Success* (Autorización de administrador con éxito), *Tamper On* (Alteración activada), *Door Opened* (Puerta abierta), *Door Close* (Puerta cerrada), *Forced Open Door* (Puerta forzada abierta), *Held Open Door* (Puerta mantenida abierta), *Detect Input #1-3* (Detectar entrada #1-3)).

- **Device** (Dispositivo): seleccione el dispositivo supervisado para un evento de alarma.
- **Signal Setting** (Configuración de señal): seleccione una opción de señal anteriormente configurada en la barra de menú (**Option > Event > Output Port Setting** (Opción > Evento > Configuración del puerto de salida)).
- **Priority** (Prioridad): establezca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para encender una alarma (activar) de prioridad 2 solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.

- **Alarm Off Event** (Evento para desactivar alarma): especifique la configuración y haga click en **Add** (Añadir) para añadir el evento a la lista Alarm Off Event (Evento para desactivar alarma). Estos eventos desactivarán una alama.
  - **Event** (Evento): seleccione el evento que desactivará la alarma (*Auth Success* (Autorización con éxito), *Auth Fail* (Autorización fallida), *Auth Duress* (Autorización de peligro), *Anti-passback Fail* (Antipassback fallido), *Access Not Granted* (Acceso no permitido), *Entrance Limited* (Entrada limitada), *Admin Auth Success* (Autorización de administrador con éxito), *Tamper On* (Alteración activada), *Door Opened* (Puerta abierta), *Door Close* (Puerta cerrada), *Forced Open Door* (Puerta forzada abierta), *Held Open Door* (Puerta mantenida abierta), *Detect Input #1-3* (Detectar entrada #1-3)).
  - **Device** (Dispositivo): seleccione el dispositivo supervisado para un evento de alarma.
- **Priority** (Prioridad): establezca una prioridad para el evento. Sólo se puede invalidar un evento anterior con un evento de igual o mayor prioridad (1 es el valor más alto). Por ejemplo, un evento para encender una alarma (activar) de prioridad 2 solo se puede cancelar con un evento para apagar una alarma (desactivar) de prioridad 1 o 2.

5.1.5.8 Pestaña Display/Sound (Pantalla/Sonido)

La pestaña Display/Sound (Pantalla/Sonido) permite personalizar la pantalla y los sonidos de eventos de D-Station. Para guardar los cambios realizados en la configuración de pantalla o sonido, debe hacer click en **Apply** (Aplicar) en la parte inferior de la pestaña. También puede aplicar la misma configuración a otros dispositivos haciendo click en **Apply to Others** (Aplicar a otros).



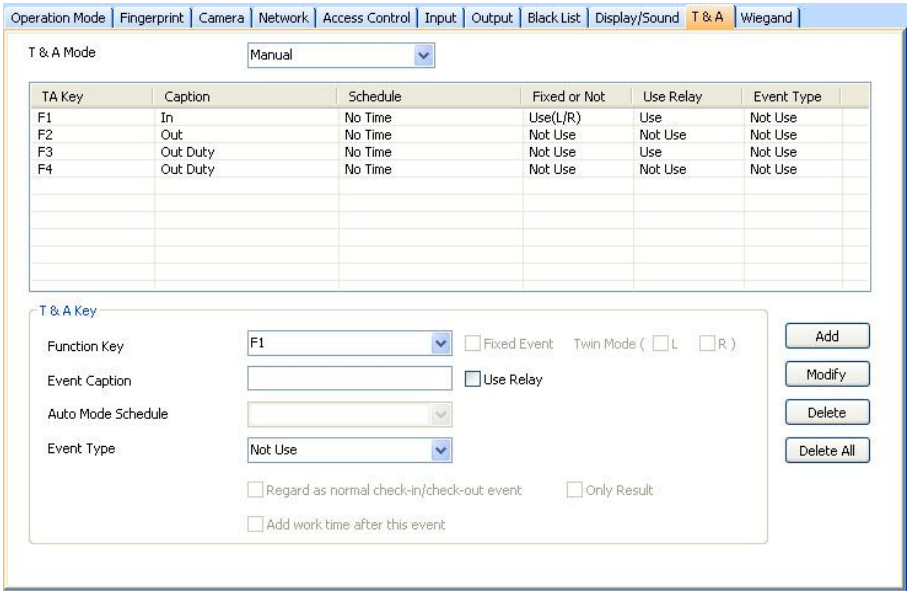
- **Display/Sound (Pantalla/Sonido)**
  - **Menu Timeout** (Tiempo de espera del menú): configure el tiempo de espera antes de que la pantalla cambie a modo inactivo.
  - **Backlite Timeout** (Tiempo de espera de retroiluminación): configure el período de tiempo que deberá transcurrir antes de que la pantalla se oscurezca.
  - **Theme** (Tema): configure un tema de pantalla.
  - **Background** (Fondo): configure el tipo de fondo para la pantalla de BioStation (*Logo*, *Notice* (Aviso) o *Slide Show* (Presentación)). Ninguno de los tipos de archivos compatibles (JPG, GIF, BMP y PNG) pueden exceder los 320x240 píxeles. Solo se puede utilizar una imagen como logo o aviso. Sin embargo, en una presentación pueden mostrarse hasta 16 imágenes (a un intervalo establecido).
  - **Notice** (Aviso): haga click en este botón para crear el aviso que se mostrará en la pantalla de BioStation. Después de crear un aviso, puede hacer click en **Apply** (Aplicar), para aplicar el aviso al dispositivo actual, o en **Apply to Others** (Aplicar a otros) para aplicar el aviso a más dispositivos.

  - **Volume** (Volumen): configure el volumen del dispositivo BioStation (del *10%* al *100%*).
  - **Msg Timeout** (Tiempo de espera del mensaje): configure la duración en pantalla de un mensaje de confirmación o de error.
- **Background Image** (Imagen de fondo): haga click en esta casilla de validación para subir nuevas imágenes de fondo). Haga click en el signo (+) para ubicar y añadir un nuevo archivo de imagen.
  - **Type** (Tipo): configure el tipo de fondo para la pantalla de BioStation (*Logo* o *Notice* (Aviso)). Ninguno de los tipos de archivos compatibles (JPG, GIF, BMP y PNG) pueden exceder los 800x427 píxeles para avisos, y 800x327 píxeles para logos. Solo se puede utilizar una imagen a la vez como logo o aviso.
- **Sound** (Sonido): haga click en la casilla de validación para habilitar y añadir sonidos de eventos personalizados. Haga click en un evento de la lista y luego haga click en el signo (+) para ubicar y añadir un nuevo archivo de sonido. Haga click en **Add** (Añadir) para añadir nuevos archivos de sonido, **Delete** (Eliminar) para eliminar archivos de sonido o **Play** (Reproducir) para previsualizar un archivo de sonido seleccionado.

5.1.5.9 Pestaña T&A (Tiempo y asistencia)

La pestaña T&A permite configurar los parámetros del modo y de la clave para un dispositivo D-Station. Para guardar los cambios realizados en la configuración de tiempo y asistencia, debe hacer click en **Apply** (Aplicar) en la parte inferior de la pestaña. También puede aplicar la misma configuración a otros dispositivos haciendo click en **Apply to Others** (Aplicar a otros).

5. Personalización de la configuración



- **T&A Mode** (Modo de tiempo y asistencia): establezca el modo de tiempo y asistencia:
  - **Not Use** (No utilizar): deshabilita las funciones de tiempo y asistencia en este dispositivo.
  - **Manual** : los usuarios deben pulsar la tecla especificada cada vez que entren o salgan para registrar los eventos de tiempo y asistencia.
  - **Manual Fix** (Fijación manual): cuando se pulsa una tecla de tiempo y asistencia, el dispositivo permanecerá en este modo hasta que se pulse otra tecla de tiempo y asistencia.
  - **Auto change** (Cambio automático): el dispositivo cambiará automáticamente los modos de tiempo y asistencia para que se correspondan con las funciones especificadas para un período de tiempo.
  - **Event Fix** (Fijación de evento): el dispositivo solo realizará la función de tiempo y asistencia especificada. En este modo, cada sensor funciona de forma independiente. Puede configurar un evento para cada sensor.
- **T&A Key** (Tecla de tiempo y asistencia): especifique las teclas que se utilizarán para los eventos de tiempo y asistencia y los tipos de eventos asociados a ellas:
  - **Function Key** (Tecla de función): seleccione la tecla de función que se asignará al evento de tiempo y asistencia de la lista desplegable (*F1-F4, EXT01-EXT12).* Si utiliza el modo Event Fix (Fijación de eventos), puede hacer click en la casilla de validación que se encuentra a la derecha para designar un evento fijo.

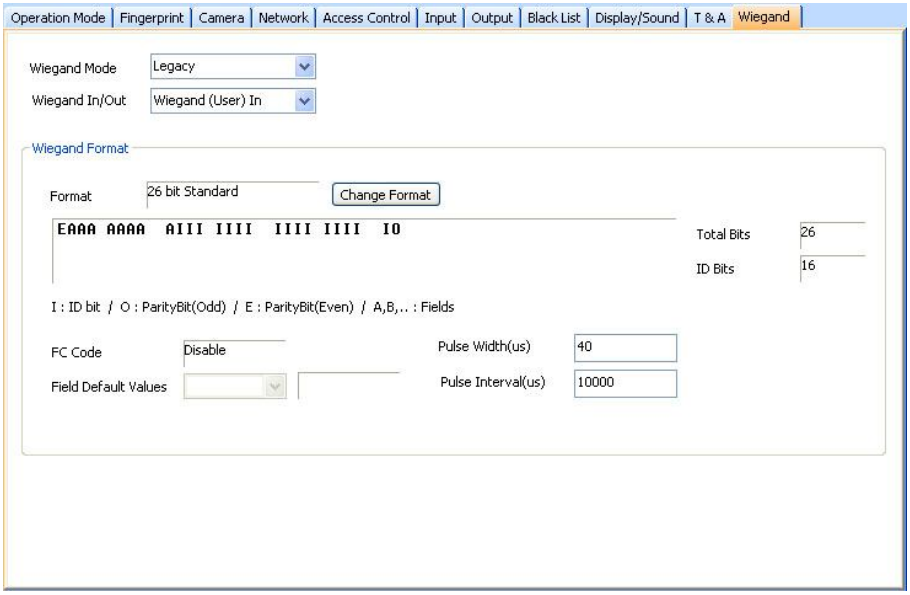
- **Event Caption** (Leyenda de evento): introduzca una leyenda para el evento.
- **Auto Mode Schedule** (Programa de modo automático): cuando utilice el modo Auto Change (Cambio automático), puede especificar cuándo ocurrirá el evento, seleccionando una zona horaria de la lista desplegable. Para obtener más información acerca de cómo crear una zona horaria, consulte la sección 3.6.1.
- **Event Type** (Tipo de evento): configure el tipo de evento que se asignará a la tecla (*Not Use* (No utilizar), *Check In* (Entrada), *Check Out* (Salida), *In* (Dentro) o *Out* (Fuera)). In/Out indican los eventos de entrada y salida generales durante un día, mientras que Check In/Out indican los eventos de entrada y salida formales a la llegada y a la partida del lugar de trabajo, o los eventos de la primera entrada y de la última salida del día. Cuando elija Check In o Check Out, puede habilitar la opción “Regard as normal check-in/check-out event” (Considerar como evento de entrada/salida normal).

  Si se habilita esta opción, los usuarios que pulsen las teclas adecuadas se considerarán como si llegasen o saliesen a tiempo del trabajo, aunque en realidad lleguen tarde o se vayan temprano. Si habilita la opción “Only Result” (Solo resultado), los usuarios aparecerán en los reportes de tiempo y asistencia como si hubieran llegado a tiempo, pero el tiempo de trabajo se calculará correctamente en base a las horas de entrada y salida reales. Si elige *Out* (Fuera), puede habilitar la opción "Add work time after this event” (Añadir tiempo de trabajo después de este evento). Si se habilita esta opción, los usuarios que pulsen las teclas adecuadas se considerarán como si se hubieran quedado a trabajar durante el tiempo restante, aunque abandonen la oficina antes.

5.1.5.10 Pestaña Wiegand

La pestaña Wiegand permite configurar el formato Wiegand para un dispositivo D-Station. Haga click en **Change Format** (Cambiar formato) para abrir el asistente de configuración Wiegand. Para obtener más información acerca de cómo configurar el formato Wiegand, consulte la sección 3.2.9.

5. Personalización de la configuración



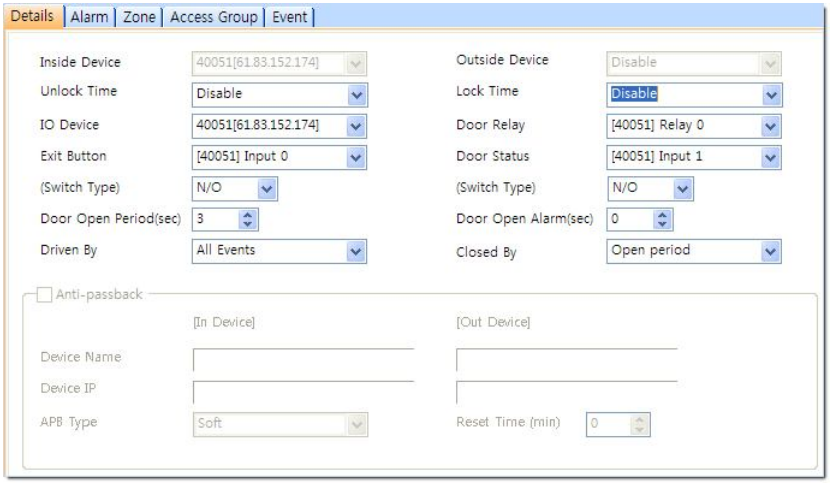
- **Wiegand Mode** (Modo Wiegand): configure el modo de entrada Wiegand que se utilizará cuando se lean los datos de Id. de una tarjeta (*Legacy* (Heredado) o *Extended* (Extendido)). El modo Legacy (Heredado) considerará a los dispositivos conectados mediante RF como parte de los dispositivos anfitriones (esta función es típica de las anteriores versiones de BioStar). El modo Extended (Extendido) permitirá que los lectores de tarjetas por RF funcionen de manera independiente, lo que permite asociarlos a puertas, incluidas en zonas, y guardar los registros con las propias Id. del dispositivo.
- **Wiegand In/Out** (Entrada/salida Wiegand): asigne la entrada o salida Wiegand:
  - **Wiegand (User) In** (Entrada (de usuario) Wiegand): el campo de Id. de la cadena Wiegand se interpreta como el id. de un usuario.
  - **Wiegand (Card) In** (Entrada (de la tarjeta) Wiegand): el campo de Id. de la cadena Wiegand se interpreta como el id. de una tarjeta.
  - **Wiegand (User) Out** (Salida (del usuario) Wiegand): inserta el id. de usuario del usuario autentificado en el campo de Id. de la cadena Wiegand.
  - **Wiegand (Card) Out** (Salida (de la tarjeta) Wiegand): inserta el id. de la tarjeta del usuario autentificado en el campo de Id. de la cadena Wiegand.

5.2 Personalización de la configuración de puertas

Las siguientes secciones describen la configuración disponible para las puertas que se añadieron al sistema BioStar. Personalice la forma en que dichas puertas funcionan cambiando la configuración para que estas se adapten al entorno y a las necesidades operacionales particulares. Para acceder a las pestañas siguientes, haga click en **Doors** (Puertas) en el panel de acceso directo, y luego haga click en el nombre de una puerta.

5.2.1 Pestaña Details (Detalles)

La pestaña Details (Detalles) permite especificar qué dispositivos se utilizan en el interior o exterior de una puerta, cómo controlan los dispositivos la puerta y las funciones anti-passback. Cuando conecte dos dispositivos a una sola puerta, los dispositivos deberán estar conectados entre sí mediante RS485. En este caso, únicamente se pueden utilizar los puertos I/O de un solo dispositivo. Especifique qué puertos de entrada/salida (I/O) del dispositivo se van utilizar en la lista despegable "IO Device" (Dispositivo de entrada/salida (IO)).



- **Inside Device** (Dispositivo interno): seleccione el dispositivo que se utilizará en el interior de la puerta.
- **Outside Device** (Dispositivo externo): seleccione el dispositivo que se utilizará en el exterior de la puerta.
- **Unlock Time** (Hora de desbloqueo): seleccione el programa en el que la puerta se deberá desbloquear normalmente. Durante este tiempo, los relays de la puerta están activos.
- **Lock Time** (Hora de bloqueo): seleccione el programa en el que la puerta se deberá bloquear normalmente. Durante este tiempo, los relays de la puerta están inactivos.
- **IO Device** (Dispositivo de entrada/salida (I/O)): cuando se utilicen dos dispositivos en una puerta, especifique los puertos de entrada/salida (I/O) del dispositivo utilizados.
- **Door Relay** (Relay de puerta): seleccione el relay de una puerta.
- **Exit Button** (Botón de salida): seleccione la entrada de un dispositivo para utilizarla para un botón de salida (Disable (Deshabilitar) o Input 0 (Entrada 0) yInput 1 (Entrada 1) para cada dispositivo añadido).
- **(Switch Type)** (Tipo de interruptor): configure la posición normal de la entrada utilizada para un botón de salida (*N/O: normalmente abierto* o *N/C: normalmente cerrado*).
- **Door Status** (Estado de puerta): establezca una entrada para un sensor que detecte el estado actual de la puerta.
- **(Switch Type)** (Tipo de interruptor): configure la posición normal de la entrada utilizada para el sensor de estado de una puerta (N/O: normalmente abierto o N/C: normalmente cerrado).

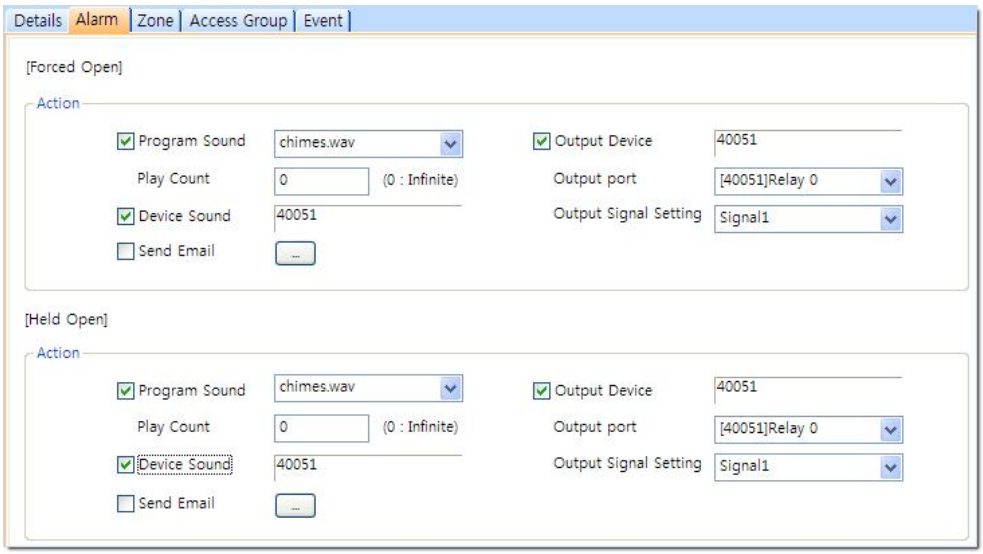
- **Door Open Period (sec)** (Período de puerta abierta (s)): establezca el tiempo (en segundos) que un relay debe permanecer activado cuando se abra una puerta. Después de este tiempo, el relay dejará de enviar la señal para abrir la puerta. El tiempo predeterminado es de tres segundos.
- **Door Open Alarm (sec)** (Alarma de puerta abierta (s)): establezca el tiempo (en segundos) que puede permanecer abierta una puerta antes de que suene una alarma.
- **Driven by** (Conducido por): seleccione los tipos de eventos que los dispositivos asociados activarán para abrir la puerta.
  - **All Events (default)** (Todos los eventos (predetermidado)): los dispositivos asociados abrirán la puerta en cualquier evento de autorización realizada con éxito.
  - **TNA + AUTH** (TNA + autorización): los dispositivos asociados abrirán la puerta en eventos de autorización con credencial o de tiempo y asistencia exitosa, o en eventos de autorización de tiempo y asistencia. Para utilizar esta opción, debe seleccionar la casilla de validación Use Relay (Utilizar relay) en la pestaña de tiempo y asistencia. Esta opción solo se encuentra disponible para dispositivos BioStation, D-Station y BioLite Net. Para obtener más información acerca de cómo configurar los parámetros de tiempo y asistencia, consulte las secciones 5.1.1.8 y 5.1.3.7.
  - **AUTH** (Autorización): los dispositivos asociados solo abrirán la puerta en eventos de autorización con credencial realizada con éxito.
  - **TNA**: los dispositivos asociados solo abrirán la puerta en eventos de autorización de tiempo y asistencia realizada con éxito. Para utilizar esta opción, debe seleccionar la casilla de validación Use Relay (Utilizar relay) en la pestaña de tiempo y asistencia. Esta opción solo se encuentra disponible para dispositivos BioStation, D-Station y BioLite Net. Para obtener más información acerca de cómo configurar los parámetros de tiempo y asistencia, consulte las secciones 5.1.1.8 y 5.1.3.7.
  - **Disabled** (Deshabilitado): los dispositivos asociados no abrirán la puerta, sin importar los eventos de autorización intentados.
- **Closed by** (Cerrado por): seleccione una opción para cerrar la puerta.
  - **Open period** (Período abierto): el sistema BioStar cerrará la puerta después del período de tiempo determinado en el campo *Door Open Period (sec)* (Período de apertura de puertas (s)).
  - **Open period+Status** (Período abierto+Estado): el sistema BioStar intentará cerrar la puerta basándose en el estado de ésta (si conectó los sensores de la puerta y si el sistema puede detectar que la puerta se encuentra abierta). Si los sensores de la puerta no están conectados, o si el sistema no es capaz de detectar el estado de la puerta, el sistema la cerrará después del

período determinado en el campo *Door Open Period (sec)* (Período de apertura de puertas (s)). Esta configuración es útil cuando se utiliza con puertas giratorias, por ejemplo, para evitar que alguien entre detrás de una persona autorizada.

- **Anti-passback**: haga click en la casilla de validación para activar la función anti-passback (solo disponible cuando se utilizan el dispositivo interno y el dispositivo externo).
  - **Device Name** (Nombre del dispositivo): este campo se poblará automáticamente.
  - **Device IP** (IP del dispositivo): este campo se poblará automáticamente.
  - **APB Type** (Tipo APB): establezca el tipo de restricción anti-passback que desea utilizar (Soft (Leve) o Hard (Fuerte)).
  - **Reset Time (min)** (Tiempo de reinicio (min)): establezca el tiempo (en minutos) que debe pasar antes de que se reinicie el estado anti-passback. Si en esta configuración, el tiempo de reinicio predeterminado es 0, el estado anti-passback no se reiniciará.

5.2.2 Pestaña Alarm (Alarma)

La pestaña Alarm (Alarma) permite especificar acciones de alarma para puertas forzadas o para puertas que se mantienen abiertas. Una alarma para puertas forzadas se activa cuando una puerta se abre a la fuerza sin ninguna autentificación en el dispositivo. Una alarma por puerta mantenida abierta se activa cuando una puerta permanece abierta por un período de tiempo más largo que el determinado en la configuración del sistema.



- **Action (Acción)**
  - **Program Sound** (Programar sonido): active y seleccione de la lista desplegable el sonido que emitirá el programa BioStar. Luego especifique la duración ("play count") del sonido en segundos. Si establece la opción Play Count (Reproducir durante) en 0, el sonido determinado se reproducirá hasta que alguien, con privilegios administrativos, detenga manualmente el sonido mediante la pestaña Realtime Monitoring (Supervisión en tiempo real) en el panel Monitoring (Supervisión). Para añadir sonidos personalizados a la lista, consulte la sección 3.9.1.2.
  - **Device Sound** (Sonido del dispositivo): active y seleccione el sonido que emitirán los dispositivos conectados a la puerta.
  - **Send Email** (Enviar e-mail): active y configure los e-mails que el sistema enviará. Para obtener más información acerca de cómo enviar alertas por e-mail, consulte la sección 3.9.2.
  - **Output Device** (Dispositivo de salida): active y seleccione el dispositivo que enviará una señal de alarma.
  - **Output Port** (Puerto de salida): seleccione el puerto de salida que se utilizará cuando se envíe la señal de alarma.
  - **Output Signal** (Señal de salida): seleccione la señal de salida que se enviará.

5.3 Personalización de la configuración de zonas

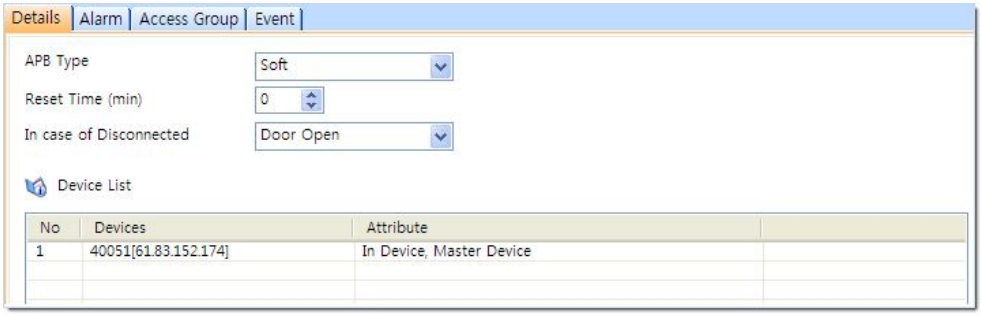
Personalice la forma en que funcionan las zonas cambiando la configuración para que estas se adapten al entorno y a las necesidades operacionales particulares. Para acceder a las pestañas descritas a continuación, haga click en **Doors** (Puertas) en el panel de acceso directo, y luego haga click en el nombre de una zona.

5.3.1 Personalización de la configuración para zonas anti-passback

Las siguientes secciones describen la configuración disponible para las zonas anti-passback. Personalice la forma en que funciona la zona, cambiando la configuración para que se adapte al entorno y a las necesidades operacionales particulares.

5.3.1.1 Pestaña Details (Detalles)

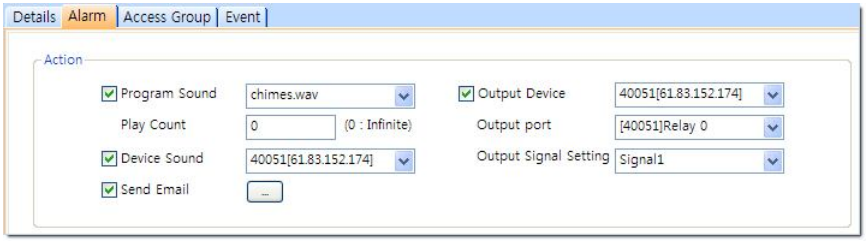
La pestaña Details (Detalles) permite especificar qué tipo de anti-passback utilizar para una zona y el período de reinicio para la función anti-passback.



- **APB Type** (Tipo APB): establezca el tipo de restricción anti-passback que desea aplicar (*Soft* (Leve) o *Hard* (Fuerte)).
- **Reset Time (min)** (Tiempo de reinicio (min)): establezca el tiempo (en minutos) que debe pasar antes de que se reinicie el estado anti-passback. Si en esta configuración, el tiempo de reinicio predeterminado es 0, el estado anti-passback no se reiniciará.
- **In case of Disconnected** (En caso de desconexión): establezca cómo deben comportarse las zonas en caso de que se pierda la comunicación entre los dispositivos maestros y los dispositivos miembros.

5.3.1.2 Pestaña Alarm (Alarma)

La pestaña Alarm (Alarma) permite especificar las acciones de alarma y un dispositivo de salida para una zona anti-passback.

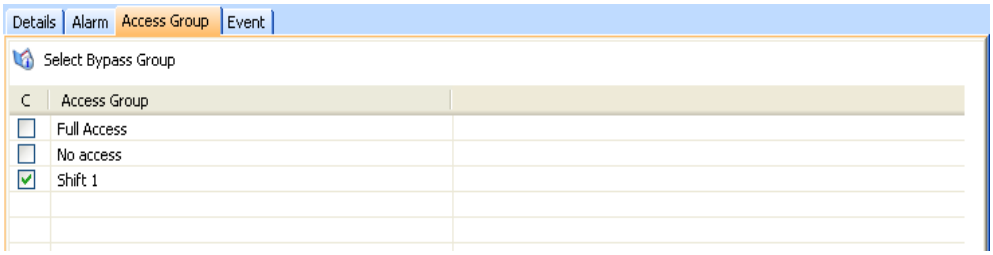


- **Action (Acción)**
  - **Program Sound** (Programar sonido): active y seleccione de la lista desplegable el sonido que emitirá el programa BioStar. Luego especifique la duración ("play count") del sonido en segundos. Si establece la opción Play Count (Reproducir durante) en 0, el sonido determinado se reproducirá hasta que alguien, con privilegios administrativos, detenga manualmente el sonido mediante la pestaña Realtime Monitoring (Supervisión en tiempo real) en el panel Monitoring (Supervisión). Para añadir sonidos personalizados a la lista, consulte la sección 3.9.1.2.
  - **Device Sound** (Sonido del dispositivo): active y seleccione el sonido que emitirán los dispositivos conectados a la puerta.
  - **Send Email** (Enviar e-mail): active y configure los e-mails que el sistema enviará. Para obtener más información acerca de cómo enviar alertas por e-mail, consulte la sección 3.9.2.

- **Output Device** (Dispositivo de salida): active y seleccione el dispositivo que enviará una señal de alarma.
- **Output Port** (Puerto de salida): seleccione el puerto de salida que se utilizará cuando se envíe la señal de alarma.
- **Output Signal** (Señal de salida): seleccione la señal de salida que se enviará.

5.3.1.3 Pestaña Access Group (Grupo de acceso)

La pestaña Access Group (Grupo de acceso) permite especificar los grupos de acceso que pueden eludir las restricciones normales para la zona. Para otorgar derechos de elusión a un grupo de acceso, seleccione un grupo y haga click en **Apply** (Aplicar) en la parte inferior de la derecha del panel Zone (Zona).

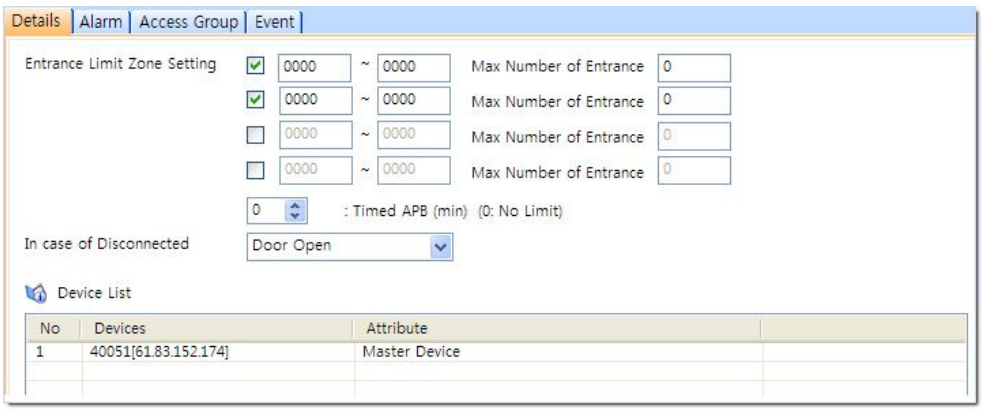


5.3.2 Personalización de la configuración para zonas de límites de entrada

Las siguientes secciones describen la configuración disponible para zonas de límites de entrada. Personalice la forma en que funciona la zona, cambiando la configuración para que se adapte al entorno y a las necesidades operacionales particulares.

5.3.2.1 Pestaña Details (Detalles)

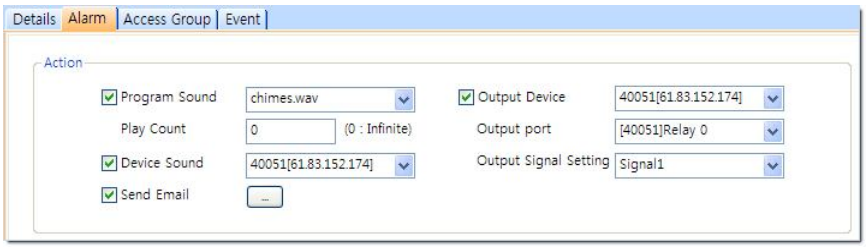
La pestaña Details (Detalles) permite especificar los límites de entrada y un programa para las restricciones de zona.



- **Entrance Limit Zone Setting** (Configuración del límite de entrada): haga click en la casilla de validación para habilitar una configuración de límites de entrada y luego especifique las horas efectivas para el mismo.
- **Max Number of Entrance** (Número máximo de entradas): establezca el número máximo de entradas permitidas durante el límite de tiempo determinado.
- **Timed APB (min)** (APB programada(min)): especifique un límite de tiempo para volver a entrar en una zona.
- **In case of Disconnected** (En caso de desconexión): establezca cómo deben comportarse las zonas en caso de que se pierda la comunicación entre los dispositivos maestros y los dispositivos miembros.

5.3.2.2 Pestaña Alarm (Alarma)

La pestaña Alarm (Alarma) permite especificar las acciones de alarma y un dispositivo de salida para una zona de límites de entrada.

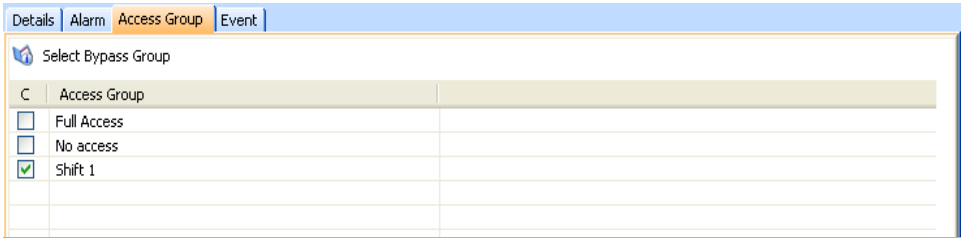


- **Action (Acción)**
  - **Program Sound** (Programar sonido): active y seleccione de la lista desplegable el sonido que emitirá el programa BioStar. Luego especifique la duración (“play count”) del sonido en segundos. Si establece la opción Play Count (Reproducir durante) en 0, el sonido determinado se reproducirá hasta que alguien, con privilegios administrativos, detenga manualmente el sonido mediante la pestaña Realtime Monitoring (Supervisión en tiempo real) en el panel Monitoring (Supervisión). Para añadir sonidos personalizados a la lista, consulte la sección 3.9.1.2.
  - **Device Sound** (Sonido del dispositivo): active y seleccione el sonido que emitirán los dispositivos conectados a la puerta.
  - **Send Email** (Enviar e-mail): active y configure los e-mails que el sistema enviará. Para obtener más información acerca de cómo enviar alertas por e-mail, consulte la sección 3.9.2.
  - **Output Device** (Dispositivo de salida): active y seleccione el dispositivo que enviará una señal de alarma.

- **Output Port** (Puerto de salida): seleccione el puerto de salida que se utilizará cuando se envíe la señal de alarma.
- **Output Signal** (Señal de salida): seleccione la señal de salida que se enviará.

5.3.2.3 Pestaña Access Group (Grupo de acceso)

La pestaña Access Group (Grupo de acceso) permite especificar los grupos de acceso que pueden eludir las restricciones normales para la zona. Para otorgar derechos de elusión a un grupo de acceso, seleccione un grupo y haga click en **Apply** (Aplicar) en la parte inferior de la derecha del panel Zone (Zona).

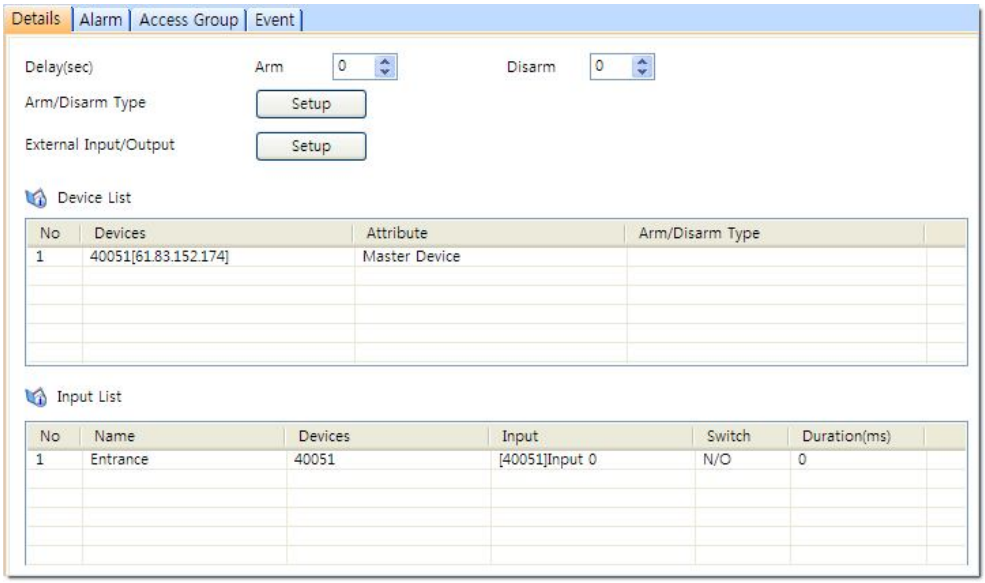


5.3.3 Personalización de la configuración para zonas de alarma

Las siguientes secciones describen la configuración disponible para zonas de alarma. Personalice la forma en que funciona la zona, cambiando la configuración para que se adapte al entorno y a las necesidades operacionales particulares.

5.3.3.1 Pestaña Details (Detalles)

La pestaña Details (Detalles) permite especificar los retrasos de alarma y los tipos de arme y desarme para las zonas de alarma.



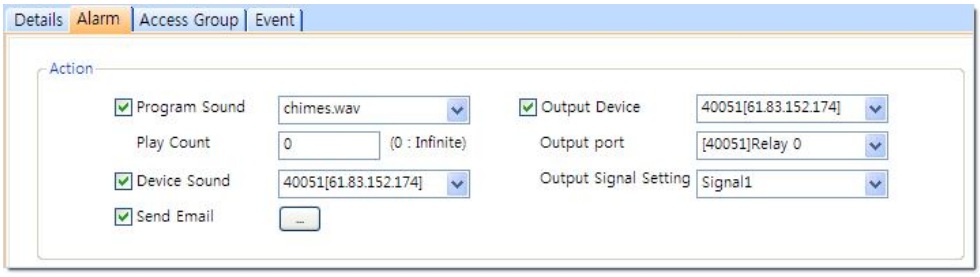
- **Delay (sec) (Retraso (s))**

- **Arm** (Arme): establezca el tiempo (en segundos) que debe transcurrir antes de armar la zona.
- **Disarm** (Desarme): establezca el tiempo (en segundos) que debe transcurrir antes de desarmar la zona.

- **Arm/Disarm Type** (Tipo de arme/desarme): especifique la configuración para armar o desarmar zonas. Para obtener más información acerca de cómo configurar los parámetros de arme y desarme, consulte la sección 3.4.2.5. Para obtener más información acerca de cómo configurar alarmas, consulte la sección 3.9.
- **External Input/Out** (Entrada/Salida externa): especifique la configuración para permitir que el sistema BioStar arme o desarme zonas automáticamente. Para obtener más información acerca de cómo configurar los parámetros de entrada/salida externa, consulte la sección 3.4.2.6. Para obtener más información acerca de cómo configurar alarmas, consulte la sección 3.9.

5.3.3.2 Pestaña Alarm (Alarma)

La pestaña Alarm (Alarma) permite especificar las acciones de alarma y un dispositivo de salida para una zona de alarma.

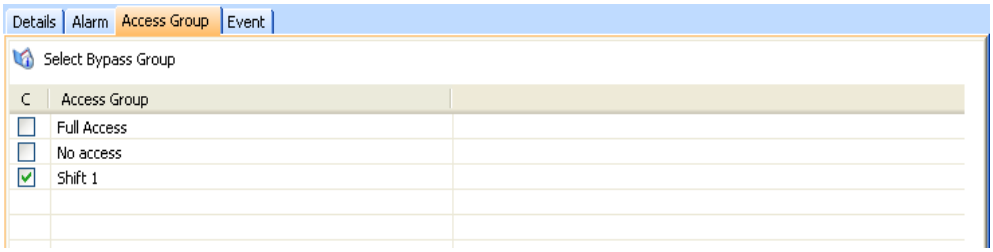


- **Action (Acción)**
  - **Program Sound** (Programar sonido): active y seleccione de la lista desplegable el sonido que emitirá el programa BioStar. Luego especifique la duración (“play count”) del sonido en segundos. Si establece la opción Play Count (Reproducir durante) en 0, el sonido determinado se reproducirá hasta que alguien, con privilegios administrativos, detenga manualmente el sonido mediante la pestaña Realtime Monitoring (Supervisión en tiempo real) en el panel Monitoring (Supervisión). Para añadir sonidos personalizados a la lista, consulte la sección 3.9.1.2.
  - **Device Sound** (Sonido del dispositivo): active y seleccione el sonido que emitirán los dispositivos conectados a la puerta.

- **Send Email** (Enviar e-mail): active y configure los e-mails que el sistema enviará. Para obtener más información acerca de cómo enviar alertas por e-mail, consulte la sección 3.9.2.
- **Output Device** (Dispositivo de salida): active y seleccione el dispositivo que enviará una señal de alarma.
- **Output Port** (Puerto de salida): seleccione el puerto de salida que se utilizará cuando se envíe la señal de alarma.
- **Output Signal** (Señal de salida): seleccione la señal de salida que se enviará.

5.3.3.3 Pestaña Access Group (Grupo de acceso)

La pestaña Access Group (Grupo de acceso) permite especificar los grupos de acceso que pueden armar y desarmar alarmas. Para otorgar autorización de desarme a un grupo de acceso, seleccione un grupo y haga click en **Apply** (Aplicar) en la parte inferior de la derecha del panel Zone (Zona).

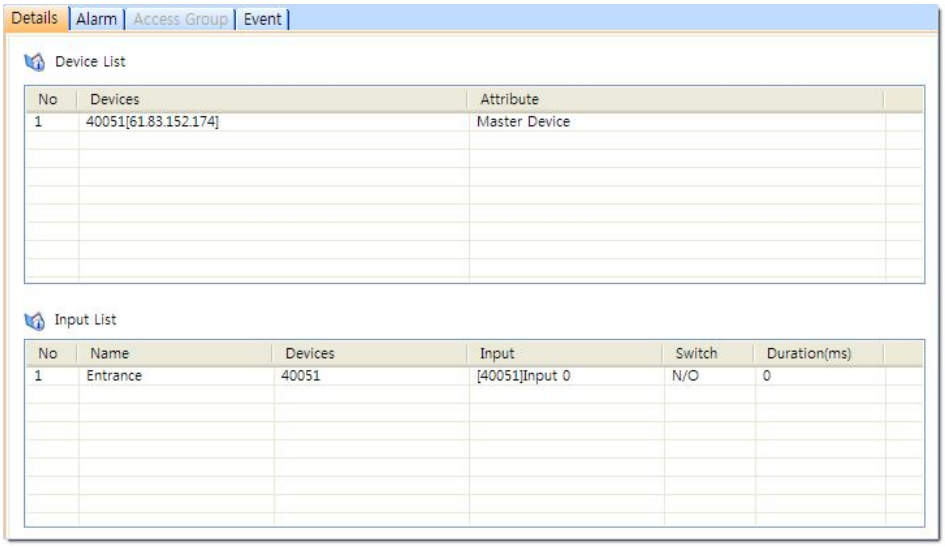


5.3.4 Personalización de la configuración para zonas de alarma por incendio

Las siguientes secciones describen la configuración disponible para zonas de alarma por incendio. Personalice la forma en que funciona la zona, cambiando la configuración para que se adapte al entorno y a las necesidades operacionales particulares.

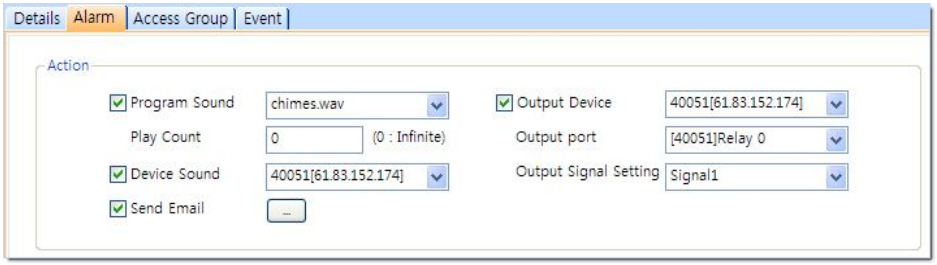
5.3.4.1 Pestaña Details (Detalles)

La pestaña Details (Detalles) permite añadir o eliminar dispositivos en la lista de dispositivos (Device List) y entradas en la lista de entradas (Input List). Para añadir o eliminar dispositivos consulte la sección 3.4.2.2.



5.3.4.2 Pestaña Alarm (Alarma)

La pestaña Alarm (Alarma) permite especificar las acciones de alarma y un dispositivo de salida para una zona de alarma por incendio.



- **Action (Acción)**
  - **Program Sound** (Programar sonido): active y seleccione de la lista desplegable el sonido que emitirá el programa BioStar. Luego especifique la duración (“play count”) del sonido en segundos. Si establece la opción Play Count (Reproducir durante) en 0, el sonido determinado se reproducirá hasta que alguien, con privilegios administrativos, detenga manualmente el sonido mediante la pestaña Realtime Monitoring (Supervisión en tiempo real) en el panel Monitoring (Supervisión). Para añadir sonidos personalizados a la lista, consulte la sección 3.9.1.2.
  - **Device Sound** (Sonido del dispositivo): active y seleccione el sonido que emitirán los dispositivos conectados a la puerta.
  - **Send Email** (Enviar e-mail): active y configure los e-mails que el sistema enviará. Para obtener más información acerca de cómo enviar alertas por e-mail, consulte la sección 3.9.2.
  - **Output Device** (Dispositivo de salida): active y seleccione el dispositivo que enviará una señal de alarma.

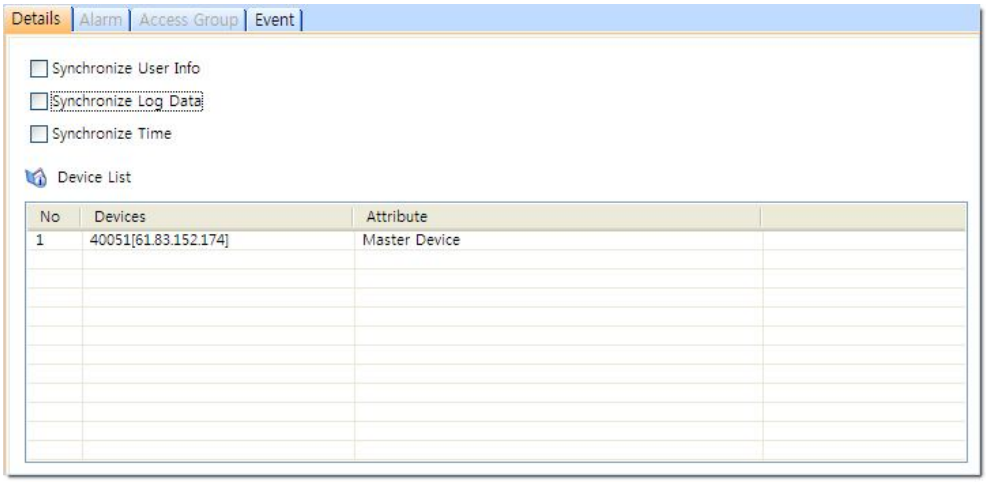
- **Output Port** (Puerto de salida): seleccione el puerto de salida que se utilizará cuando se envíe la señal de alarma.
- **Output Signal** (Señal de salida): seleccione la señal de salida que se enviará.

5.3.5 Personalización de la configuración para zonas de acceso

Las siguientes secciones describen la configuración disponible para zonas de acceso. Estas zonas se utilizan para sincronizar datos del usuario; por lo tanto, las pestañas Alarm (Alarma) y Access Group (Grupo de acceso) no están disponibles. Personalice la forma en que funciona la zona, cambiando la configuración para que se adapte al entorno y a las necesidades operacionales particulares.

5.3.5.1 Pestaña Details (Detalles)

La pestaña Details (Detalles) permite añadir dispositivos a la lista de dispositivos (Device List).



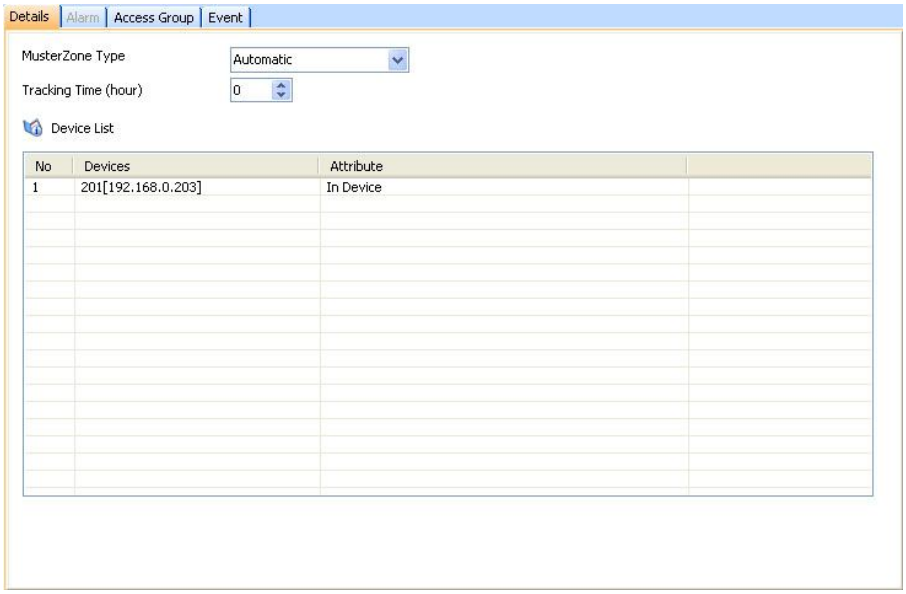
- **Synchronize User Info** (Sincronizar información de usuario): haga click en esta casilla de validación para propagar automáticamente la información de usuario a otros dispositivos.
- **Synchronize Log Data** (Sincronizar datos de registro): haga click en esta casilla de validación para pasar automáticamente todos los registros al dispositivo maestro (para los dispositivos miembros en la zona).
- **Synchronize Time** (Sincronizar hora): haga click en esta casilla de validación para sincronizar la hora de los dispositivos en la zona.

5.3.6 Personalización de la configuración para zonas de reunión

Las siguientes secciones describen la configuración disponible para zonas de reunión. Estas zonas se utilizan para supervisar la ubicación de los usuarios; por lo tanto, la pestaña Alarm (Alarma) no se encuentra disponible. Personalice la forma en que funciona la zona, cambiando la configuración para que se adapte al entorno y a las necesidades operacionales particulares.

5.3.6.1 Pestaña Details (Detalles)

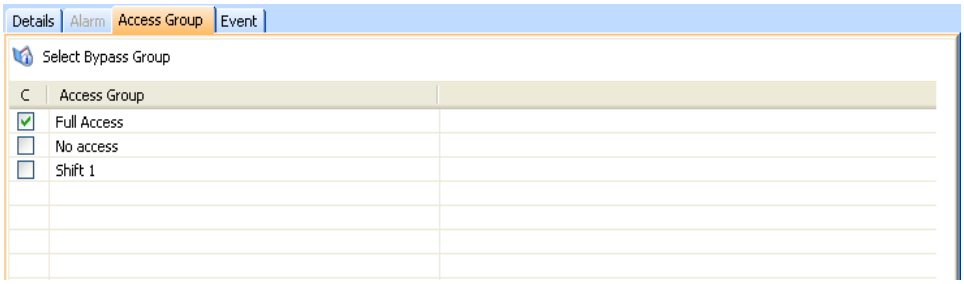
La pestaña Details (Detalles) permite añadir dispositivos a la lista de dispositivos (Device List).



- **Muster Zone Type** (Tipo de zona de reunión): establezca el tipo de supervisión (*automatic* (automática) o *manual* (manual)).
- **Tracking Time (hour)** (Tiempo de seguimiento (h)): establezca el número de horas para supervisar la zona.

5.3.6.2 Pestaña Access Group (Grupo de acceso)

La pestaña Access Group (Grupo de acceso) permite especificar los grupos de acceso que pueden armar y desarmar alarmas. Para otorgar autorización de desarme a un grupo de acceso, seleccione un grupo y haga click en **Apply** (Aplicar) en la parte inferior de la derecha del panel Zone (Zona).

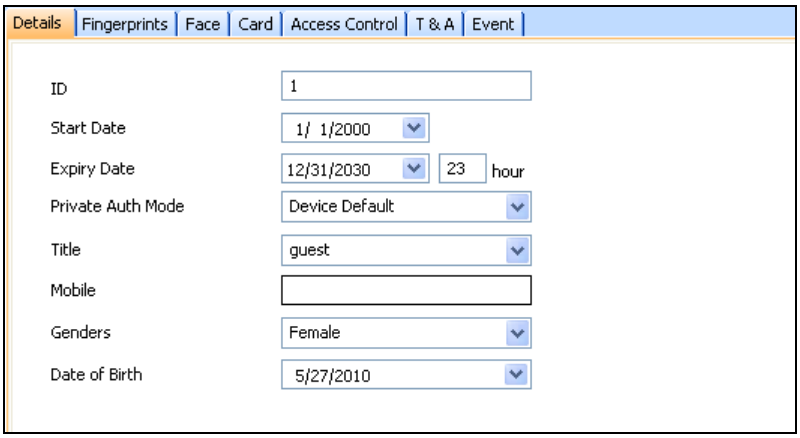


5.4 Personalización de la configuración de usuario

Personalizar varias configuraciones para usuarios, incluyendo detalles personales, información de huellas dactilares e información de la tarjeta de acceso. Para acceder a las pestañas descritas a continuación, haga click en **User** (Usuario) en el panel de acceso directo y luego haga click en el nombre de un usuario.

5.4.1 Pestaña Details (Detalles)

La pestaña Details (Detalles) permite especificar la información personal de un usuario y las fechas válidas de una cuenta de usuario. Para editar estos campos consulte la sección 4.4.3.



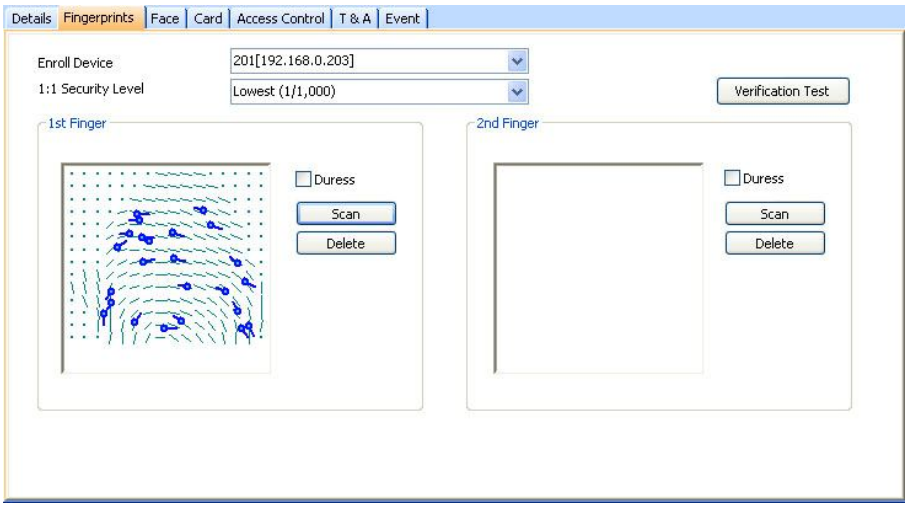
- **ID** (Id.): introduzca un número de identificación para el usuario.
- **Start Date** (Fecha de inicio): establezca una fecha de inicio en la que el usuario obtendrá autorización mediante el sistema BioStar.
- **Expiry Date** (Fecha de caducidad): establezca la fecha en la que la cuenta del usuario caducará (también puede especificar la hora en la que la cuenta caducará).
- **Private Auth Mode** (Modo de autorización privado): establezca el método de autorización para el usuario (*Device Default* (Dispositivo predeterminado), *Finger Only* (Solo huella dactilar), *Password Only* (Solo contraseña), *Finger or Password* (Dedo o contraseña), *Card Only* (Solo tarjeta) o *Finger and Password* (Dedo y contraseña)). Si establece el método en "Device Default" (Dispositivo

predeterminado), el modo autentificación se determinará por la configuración del modo de funcionamiento del dispositivo.

- **Title** (Título): seleccione un título para el usuario (*Guest (Invitado)*, *President (Presidente)*, *Director*, *General Manager (Gerente general)*, *Chief (Jefe)*, *Assistant Manager (Subgerente)* o un título personalizado).
- **Mobile** (Celular): introduzca un número de celular para el usuario.
- **Genders** (Género): introduzca el género del usuario.
- **Date of Birth** (Fecha de nacimiento): seleccione la fecha de nacimiento en el calendario desplegable.

5.4.2 Pestaña Fingerprints (Huellas dactilares)

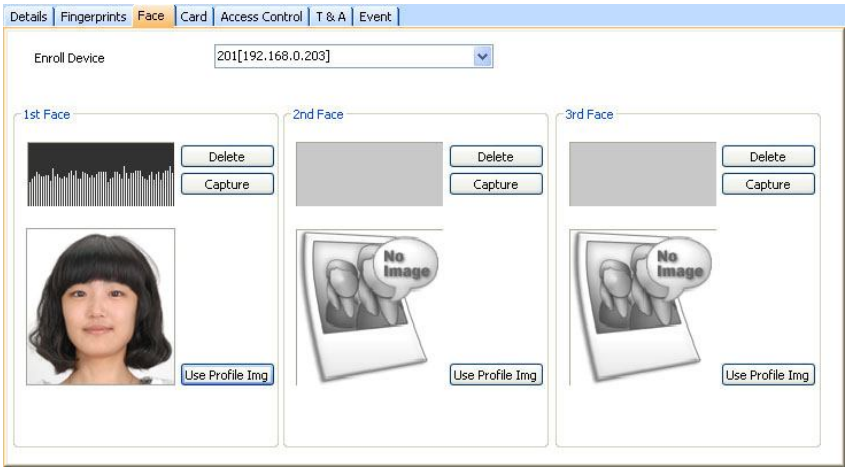
La pestaña Fingerprints (Huellas dactilares) permite especificar el tipo de escáner que se utilizará para el registro y el nivel de seguridad aplicado. Esta pestaña también se puede utilizar para comprobar huellas dactilares y registrar huellas dactilares de peligro. Para obtener más información acerca de cómo registrar huellas dactilares, consulte la sección 3.5.2.



- **Enroll Device** (Dispositivo de registro): seleccione el dispositivo que se utilizará para escanear las huellas dactilares.
- **1:1 Security Level** (Nivel de seguridad 1:1): seleccione el nivel de seguridad que se utilizará en la autorización con huella dactilar (*Device Default* (Dispositivo predeterminado) y de *Lowest [1/1,000]* (El menor [1/1,000]) a *Highest [1/10,000,000]* (El mayor [1/10,000,000])). Recuerde que cuanto más alto sea el nivel de seguridad, más posibilidades hay de que se produzcan falsos rechazos.
- **Duress** (Peligro): establezca la plantilla de huella dactilar que se utilizará como dedo de peligro (cuando se utilice el dedo de peligro para entrar, se activarán las alarmas).

5.4.3 Pestaña Face (Rostro)

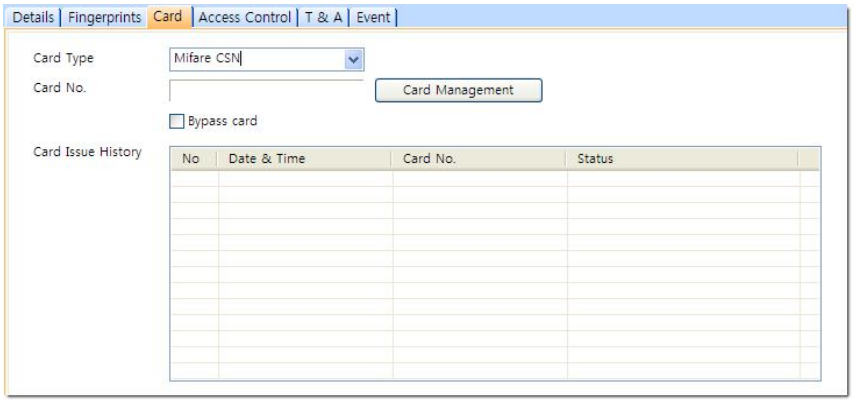
La pestaña Face (Rostro) permite especificar el dispositivo D-Station que se utilizará para hacer fotografías de los rostros de los usuarios. Para obtener más información acerca de cómo hacer fotografías faciales, consulte la sección 3.5.3.



- **Enroll Device** (Dispositivo de registro): seleccione el dispositivo que se utilizará para hacer fotografías faciales.

5.4.4 Pestaña Card (Tarjeta)

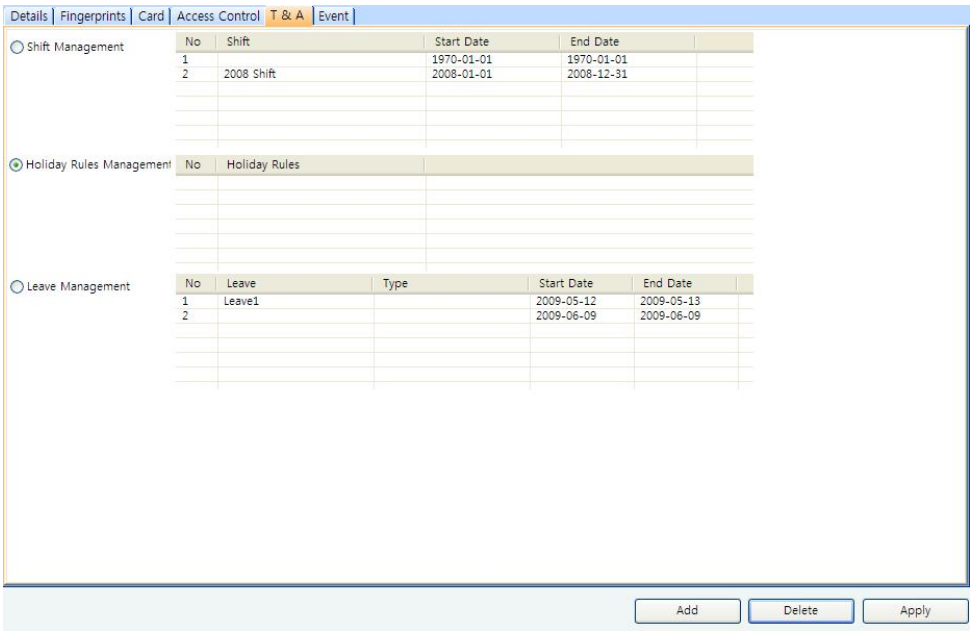
La pestaña Card (Tarjeta) permite especificar los tipos de tarjeta y las Id., y expedir tarjetas para los usuarios. Para obtener más información acerca de cómo expedir tarjetas de acceso, consulte la sección 3.5.3.



- **Card Type** (Tipo de tarjeta): seleccione el tipo de tarjeta de acceso que desea expedir (*Mifare Card* (Tarjeta Mifare), *EM 4100 Card* (Tarjeta EM 4100) o *HID Prox Card* (Tarjeta de proximidad HID)).
- **Card ID** (Id. de tarjeta): muestra el número de el id. de la tarjeta cuando se expide una tarjeta.

5.4.5 Pestaña T&A (Tiempo y asistencia)

La pestaña T&A (Tiempo y asistencia) permite especificar los turnos, las normas vacacionales y los períodos de permisos que se van a aplicar a un usuario. Para añadir nuevos detalles, haga click en **Add** (Añadir) en la parte inferior de la pestaña. Para guardar los cambios realizados en la configuración de tiempo y asistencia, debe hacer click en **Apply** (Aplicar) en la parte inferior de la pestaña. También puede eliminar entradas seleccionándolas y haciendo click en **Delete** (Eliminar). Para obtener más información acerca de cómo configurar el tiempo y la asistencia, consulte la sección 3.8.



- **Shift Management** (Gestión de turnos): especifique los turnos que se aplicarán al usuario.
- **Holiday Rules Management** (Gestión de normas vacacionales): especifique las normas vacacionales que se aplicarán al usuario.
- **Leave Management** (Gestión de permisos): especifique el permiso para el usuario.

06

Solución de problemas

Si experimenta problemas con el software BioStar, póngase en contacto con el soporte técnico de Suprema por e-mail: **support@supremainc.com**. Cuando escriba un e-mail al soporte técnico, incluya la siguiente información:

- La versión de BioStar que está utilizando.
- Los dispositivos de Suprema que presentan el problema, en caso de que haya.
- El mensaje de error que aparece, en caso de que haya.
- Una descripción completa (pero concisa) del problema que está experimentando.
- Su nombre y título.
- Su información de contacto.
- La mejor hora y método para contactarle.

Glosario

tarjeta de acceso: una tarjeta que se puede utilizar para otorgar o restringir el acceso a un área específica.
BioStar es compatible con las tarjetas MIFARE® y EM4100, y con las tarjetas de proximidad HID. Consulte también: tarjeta de proximidad.

sistema de control de acceso: un sistema de mecanismos y controles físicos que permite o deniega el acceso a un recurso o área física en particular. BioStar es un sistema de control de acceso biométrico basado en conectividad IP.

zona de alarma: un grupo de dispositivos que se utiliza para proteger un área física. BioStar
supervisa puntos de entrada en una zona de alarma y activa las alarmas cuando se detecta una intrusión o alteración.

anti-passback: un protocolo de seguridad que evita que un usuario proporcione entrada no autorizada a otro usuario mediante una tarjeta de acceso o una huella dactilar. Consulte también: anti-passback programado.

biométrico: biométrico se refiere al uso de características físicas en una verificación o autorización. BioStar incorpora la galardonada tecnología de reconocimiento de huellas dactilares para proporcionar autentificación biométrica de la identidad de un usuario y autorización para acceder a áreas restringidas.

grupo de elusión: un grupo de usuarios que pueden eludir las restricciones normales de una zona.

cliente: el software cliente de BioStar permite a un operador conectarse al servidor BioStar y controlar los dispositivos conectados de forma remota. Son necesarias el id. y la contraseña de un operador para acceder al sistema a través de un cliente.

área: una parte de una organización utilizada para agrupar empleados. No es necesario utilizar áreas, pero puede ser de gran ayuda a la hora de organizar números elevados de empleados.

Glosario

dispositivo: en esta guía, la palabra "dispositivo" se refiere a cualquier producto de Suprema compatible con el sistema BioStar. Los dispositivos compatibles incluyen las terminales BioStation, BioEntry Plus y BioMini USB, así como también el dispositivo Secure I/O.

inteligencia distribuida : en el sistema BioStar, la base de datos de la autorización se distribuye a cada terminal, de manera que la autorización se vuelve un proceso más rápido y puede seguir funcionando incluso cuando otras partes del sistema se encuentran desactivadas.

puerta: las puertas son barreras físicas que dan entrada a un edificio o espacio. Al menos debe de haber conectado un dispositivo a una puerta para proporcionar control de acceso. Además, se pueden conectar dos dispositivos para activar la función anti-passback y otras como, por ejemplo, los relays de puerta, los relays de alarma, los interruptores de salida y los sensores.

dedo de peligro: este término se refiere a una huella dactilar registrada que activará alarmas silenciosas cuando un usuario se vea amenazado. En la típica situación de peligro, un intruso fuerza y amenaza al usuario para que acceda. El usuario accede utilizando su dedo de peligro y así accede y desencadena las acciones de alerta que usted especifique.

registro el proceso de crear una cuenta de usuario, capturar imágenes de las huellas dactilares o expedir tarjetas de acceso.

límite de entrada: el número máximo de veces que un usuario puede acceder a un área especificada. El límite de entrada puede estar relacionado a un período de tiempo en el que los usuarios están limitados a un número específico de entradas durante horas de oficina, por ejemplo.

ESSID: ESSID (Extended Service Set ID) es el nombre de un punto de acceso de red inalámbrica. Permite distinguir claramente una red inalámbrica de otra. ESSID es un tipo de SSID (el otro tipo es BSSID).

índice de aceptación falsa: el índice de aceptación falsa (FAR, por sus siglas en inglés) es un parámetro que mide las posibilidades que un sistema de seguridad biométrico tiene de aceptar de forma incorrecta un intento de acceso por parte de un usuario no autorizado. Un índice de aceptación falsa está conformado normalmente por el número de falsas aceptaciones y el número de intentos de identificación.

índice de falsos rechazos: el índice de falsos rechazos (FRR, por sus siglas en inglés) es un parámetro que mide las posibilidades que un sistema de seguridad biométrico tiene de rechazar de forma incorrecta un intento de acceso por parte de un usuario autorizado. Un índice de aceptación falsa está conformado normalmente por el número de falsos rechazos y el número de intentos de identificación.

Glosario

reconocimiento de huella dactilar: es la comprobación automática de dos huellas dactilares humanas: una previamente registrada y otra proporcionada en el momento de la autentificación por el usuario. BioStar incorpora los algoritmos galardonados de Suprema para el reconocimiento de huellas dactilares.

sensor de huellas dactilares: un sensor de huellas dactilares es un dispositivo electrónico utilizado para capturar una imagen digital del patrón de una huella dactilar. La imagen capturada se llama exploración real. Esta exploración real se procesa digitalmente para crear una plantilla biométrica (una colección de características extraídas) que se almacenan y utilizan para el reconocimiento de huellas dactilares.

zona de alarma por incendio: es una zona que se utiliza para interactuar con alarmas de incendio o puertas de control cuando se detecta un incendio.

anfitrión: un anfitrión es el dispositivo que sirve como maestro en una red RS485. El dispositivo anfitrión transmite por relays paquetes de datos entre los dispositivos externos (o una red más grande) y los dispositivos esclavos conectados a la red RS485.

señal de entrada: es la señal enviada a un dispositivo por un objeto externo como, por ejemplo, un botón de salida.

operador: los operadores son empleados que poseen derechos para utilizar los clientes BioStar. BioStar incluye tres clases predeterminadas de operadores: administradores, operadores y gerentes. BioStar también permite hasta 16 clases personalizadas de operador.

señal de salida: es la señal enviada a un dispositivo externo como, por ejemplo, la sirena de una alarma o la cerradura eléctrica de una puerta.

tarjeta de proximidad: las tarjetas de proximidad (o tarjetas "prox") son dispositivos con circuitos integrados sin contacto para accesos de seguridad. Los dispositivos BioStation son compatibles con tarjetas HID y EM4100, mientras que los dispositivos BioEntry Plus son compatibles con las tarjetas EM4100.

lectores RF: son dispositivos de lectura por RF de corto alcance que se utilizan para acceder a las puertas. El sistema BioStar permite añadir al sistema lectores RF de terceros para incorporar hardware que ya existe en la configuración del control de acceso.

nivel de seguridad: consulte *índice de aceptación falsa.*

tiempo y asistencia (T&A): este término se refiere a los procesos y funciones que supervisan y reportan las actividades de entrada y salida de los empleados y permiten a los administradores definir lotes de tiempo y programas. La información recopilada por el sistema BioStar se puede utilizar junto con sistemas externos para reportar tiempos y para controlar la asistencia de los empleados.

anti-passback programado: es un protocolo de seguridad que evita que un usuario vuelva a acceder por un período de tiempo específico. Consulte también: *anti-passback.*

timezone (zona horaria): es un programa personalizable que se puede utilizar para permitir o restringir el acceso durante las horas especificadas. Las zonas horarias se pueden combinar con puertas para crear grupos de acceso.

usuario: un usuario es cualquier persona con derechos de acceso. Los derechos de acceso de un usuario están compuestos de derechos individuales (nivel de usuario), de la pertenencia a grupos de acceso y de las restricciones de tiempo.

interfase Wiegand: la interfase Wiegand es un estándar con cables utilizado para conectar un mecanismo para leer tarjetas a un sistema de entrada electrónico. La interfase utiliza tres cables, uno es un cable de tierra común y los otros dos son cables de transmisión de datos llamados normalmente DATA0 y DATA1, aunque algunas veces también se les llama Data High y Data Low.

zona: una zona está compuesta por dos o más dispositivos agrupados. BioStar incluye varias clasificaciones de zonas: zonas anti-passback, zonas de limitación de entrada, zonas alarma y zonas de alarma por incendio.

Índice

Índice

Índice

Índice

suprema

BioStar

Suprema Inc.

16F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863 Corea

Tlfn.: +82-31-783-4502 **Fax**: +82-31-783-4503

E-mail: sales@supremainc.com **Página de Internet**: www.supremainc.com