Barrera oscilante serie DS-K3B530X

Manual del usuario

Aviso legal

Acerca de este documento

Este documento incluye instrucciones para el uso y la gestión del producto. Las imágenes, gráficos y demás información adicional son solo para fines ilustrativos. La información contenida en este documento está sujeta a cambios sin previo aviso debido a actualizaciones del software u otros motivos . Consulte la versión más reciente del documento en el sitio web de Hikvision (www.hikvision.com) .). A menos que se acuerde lo contrario, Hangzhou Hikvision Digital Technology Co., Ltd. o sus empleados, ya sea expreso o implícito. (en adelante, "Hikvision") no ofrece ninguna garantía

• Utilice el Documento con la orientación y asistencia de profesionales capacitados en el uso del Producto.

Acerca de este producto

• Este producto solo se puede disfrutar una vez soporte de servicio en el país o región donde se encuentra realizada la compra.
• Si el producto que elige es un producto de video, escanee el siguiente código QR para obtenerlo Iniciativa sobre el Uso de Productos de Vídeo", y léala con atención.

Reconocimiento de los derechos de propiedad intelectual

• Hikvision posee los derechos de autor y/o patentes relacionados con la tecnología incorporada en el Productos descritos en este Documento, que pueden incluir licencias obtenidas de terceros. • Cualquier parte del Documento, incluyendo texto, imágenes, gráficos, etc., pertenece a Hikvision. Ninguna parte de este Documento puede ser extractada, copiada, traducida o modificada, total o parcialmente, por ningún medio sin el permiso escrito. y otras marcas comerciales y logotipos de Hikvision son
• HIKVISION propiedad de Hikvision en diversas rti.

• Otras marcas comerciales y logotipos son propiedad de sus respectivos propietarios.

AVISO LEGAL

• HASTA EL GRADO MÁXIMO PERMITIDO POR LA LEY APLICABLE, ESTE DOCUMENTO Y LA EL PRODUCTO DESCRITO, CON SU HARDWARE, SOFTWARE Y FIRMWARE, SE PROPORCIONA "TAL CUAL" Y "CON TODOS SUS FALLOS Y ERRORES". HIKVISION NO OFRECE GARANTÍAS, EXPRESAS O

IMPLÍCITAS, INCLUYENDO, SIN LIMITACIÓN, LA COMERCIABILIDAD, LA CALIDAD SATISFACTORIA O LA IDONEIDAD PARA UN PROPÓSITO PARTICULAR. EL USO DEL PRODUCTO POR SU PARTE ES BAJO SU PROPIA RESPONSABILIDAD.

EN NINGÚN CASO HIKVISION SERÁ RESPONSABLE ANTE USTED POR DAÑOS ESPECIALES, DERIVADOS, INCIDENTALES O INDIRECTOS, INCLUYENDO, ENTRE OTROS, DAÑOS POR PÉRDIDA DE BENEFICIOS COMERCIALES, INTERRUPCIÓN DE LA ACTIVIDAD COMERCIAL O PÉRDIDA DE DATOS, CORRUPCIÓN DE SISTEMAS O PÉRDIDA DE DOCUMENTACIÓN, YA SEA CON BASE EN INCUMPLIMIENTO DE CONTRATO, AGRAVIO (INCLUIDA LA NEGLIGENCIA), RESPONSABILIDAD DEL PRODUCTO O DE OTRO MODO, EN RELACIÓN CON EL USO DEL PRODUCTO, INCLUSO SI HIKVISION HA SIDO ADVERTIDO DE LA POSIBILIDAD DE DICHOS DAÑOS O PÉRDIDAS.

• USTED RECONOCE QUE LA NATURALEZA DE INTERNET CONLLEVA RIESGOS DE SEGURIDAD INHERENTES, Y HIKVISION NO ASUMIRÁ NINGUNA RESPONSABILIDAD POR FUNCIONAMIENTO ANORMAL, FUGA DE PRIVACIDAD U OTROS DAÑOS RESULTANTES DE ATAQUES CIBERNÉTICOS, ATAQUES DE PIRATAS INFORMÁTICOS, INFECCIÓN DE VIRUS U OTROS RIESGOS DE SEGURIDAD DE INTERNET; SIN EMBARGO, HIKVISION PROPORCIONARÁ SOPORTE TÉCNICO OPORTUNO SI ES NECESARIO.

• USTED ACEPTA UTILIZAR ESTE PRODUCTO EN CUMPLIMIENTO CON TODAS LAS LEYES APLICABLES Y ES EL ÚNICO RESPONSABLE DE ASEGURARSE DE QUE SU USO SE AJUSTE A LA LEY APLICABLE.

ESPECIALMENTE, USTED ES RESPONSABLE DE USAR ESTE PRODUCTO DE FORMA QUE NO INFRINJA LOS DERECHOS DE TERCEROS, INCLUYENDO, SIN LIMITACIÓN, LOS DERECHOS DE PUBLICIDAD, DE PROPIEDAD INTELECTUAL, DE PROTECCIÓN DE DATOS Y OTROS DERECHOS DE PRIVACIDAD. NO DEBERÁ UTILIZAR ESTE PRODUCTO PARA NINGÚN USO FINAL PROHIBIDO, INCLUYENDO EL DESARROLLO O LA PRODUCCIÓN DE ARMAS DE DESTRUCCIÓN MASIVA, EL DESARROLLO O LA PRODUCCIÓN DE ARMAS QUÍMICAS O BIOLÓGICAS, CUALQUIER ACTIVIDAD RELACIONADA CON CUALQUIER EXPLOSIVO NUCLEAR O CICLO DE COMBUSTIBLE NUCLEAR INSEGURO, O EN APOYO A ABUSOS DE LOS DERECHOS HUMANOS.

• EN CASO DE CONFLICTO ENTRE ESTE DOCUMENTO Y LA LEY APLICABLE, LA LO ÚLTIMO PREVALECE.

Datos norte

• Para proteger los datos, el desarrollo de los productos Hikvision incorpora la privacidad por diseño. Principios. Por ejemplo, para los Productos con rasgos faciales, los datos biométricos se almacenan mediante el método de cifrado; para los Productos de cifrado, solo se guardará la plantilla de cifrado, lo que impide reconstruir una imagen de cifrado. • Como responsable/ encargado del tratamiento de datos, usted puede procesar datos personales, incluyendo el almacenamiento, uso, procesamiento y divulgación de datos, así como las leyes aplicables y las normas relacionadas con la recopilación de datos personales, incluyendo la estaño, etc. Se recomienda pagar ntin y cumplir con aplicación de controles de seguridad para salvaguardar los datos personales, como la aplicación de controles de seguridad físicos y de mantenimiento razonables, la realización de revisiones periódicas y la evaluación de la eficacia de sus controles de seguridad.

Marco regulatorio

Nomenclatura de la FCC

Tenga en cuenta que los cambios o modificaciones no aprobados expresamente por la parte responsable del cumplimiento podrían anular la autoridad del usuario para operar el equipo.
Cumplimiento de la FCC: Este equipo ha sido probado y cumple con los límites para un dispositivo digital de Clase B, de conformidad con la parte 15 de las Normas de la FCC. Estos límites están diseñados para proporcionar una protección razonable contra interferencias perjudiciales en un entorno de recepción. Este equipo genera, utiliza y puede radiar energía de radiofrecuencia y, si no se instala y utiliza de acuerdo con la protección, puede causar interferencias perjudiciales en la comunicación de radio. Sin embargo, no hay garantía de que no se produzcan interferencias en un entorno de recepción. Si este equipo causa interferencias perjudiciales en la comunicación de radio o televisión, que pueden determinarse encendiendo el equipo, se recomienda al usuario que intente corregir la interferencia mediante una o más de las siguientes medidas: —Reorientar o reubicar la antena receptora.

—Aumentar la distancia entre el equipo y el receptor.
—Conecte el equipo a una toma de corriente en un circuito alejado de aquel al que está conectado el receptor.

—Consulte al distribuidor o a un técnico de radio/TV experimentado para obtener ayuda.
Este equipo debe instalarse y utilizarse con una distancia mínima de 20 cm entre el radiador y su cuerpo.

Normas de la

FCC Este dispositivo cumple con la parte 15 de las Normas de la FCC. Está sujeto a las dos siguientes normas: 1. Este dispositivo

no puede causar interferencias dañinas.
2. Este dispositivo debe aceptar cualquier interferencia recibida, incluidas las interferencias que puedan causar un funcionamiento no deseado.

Declaración de conformidad de la UE

CE

Este producto y, si corresponde, los accesorios suministrados también están marcados con "CE" y, por lo tanto, cumplen con las normas europeas armonizadas aplicables enumeradas

bajo la directiva EMC 2014/30/EU, la directiva RE 2014/53/EU y la directiva RoHS 2011/65/UE

2012/19/UE (Residuos de Aparatos Eléctricos y Electrónicos (RAEE)). Los productos marcados con este símbolo no pueden desecharse como residuos municipales sin clasificar en la Unión Europea. Para un reciclaje adecuado, devuelva este producto a su proveedor local tras la compra de un equipo nuevo equivalente o deséchelo en los puntos de reciclaje designados. Para obtener más información, consulte: www.recyclethis.info

2006/66/CE (recursos de reciclaje). Este producto contiene residuos que no pueden desecharse como residuos municipales sin clasificar en la Unión Europea. Consulte la etiqueta del producto para obtener información sobre residuos de reciclaje. El residuo está marcado con este símbolo. Símbolo, que puede incluir (Hg). rn para indicar cadmio (Cd), plomo (Pb) o mercurio Para un reciclaje adecuado, devuelva el producto a su proveedor o a un punto de reciclaje designado. Para más información, consulte: www.recyclethis.info

Instrucciones de Seguridad

Estas instrucciones están destinadas a garantizar que el usuario pueda utilizar el producto correctamente para evitar peligros o pérdidas de propiedad.

La medida de precaución se divide en Peligros y Peligros de la Nctin: La no

observación de cualquiera de las advertencias puede provocar lesiones graves o la muerte.

Cualquiera de los siguientes componentes puede provocar lesiones o daños al equipo.

⚠	⚠
Peligros: Siga estas precauciones para evitar lesiones graves o la muerte.	Siga estas instrucciones para evitar lesiones o daños materiales.

⚠ Peligro:

• Todos los equipos electrónicos deben cumplir estrictamente con las normas de seguridad eléctrica y otras normas relacionadas de su región local.

• Utilice el adaptador de corriente suministrado por la compañía eléctrica. El cable de alimentación... no puede ser menor que el valor requerido.

• No conecte varios dispositivos a un adaptador de corriente, ya que la sobrecarga del adaptador puede causar sobrecalentamiento. o peligro r.

• Asegúrese de que la alimentación esté desconectada antes de cablear, instalar o desmontar el dispositivo.

Si las tapas superiores deben estar abiertas y el dispositivo debe encenderse para realizar tareas de mantenimiento, asegúrese de que seguro:

1. Encienda el ventilador para evitar que el operador 2. No toque n herido accidentalmente. componentes desnudos de alto voltaje.

3. Asegúrese de que la secuencia de cableado del interruptor sea correcta para realizar el mantenimiento. • Asegúrese de que la alimentación esté desconectada antes de cablear, instalar o desmontar el interruptor. dispositivo.

• Cuando el producto se instala en la pared o el techo, el dispositivo debe estar rmy x • Si sale humo, olores o ruido del dispositivo, apague el dispositivo inmediatamente y desenchúfelo. cable y luego comuníquese con el centro de servicio.

• No ingerir. Peligro de quemaduras químicas.

Este producto contiene una célula cnbn bry. Si se ingiere la célula cnbn bry, puede causar quemaduras internas graves en solo 2 horas y puede provocar la muerte.

Mantenga el cepillo nuevo y usado fuera del alcance de los niños. Si el compartimento del cepillo no cierra bien, deje de usar el producto y manténgalo fuera del alcance de los niños. Si cree que el cepillo podría haber sido ingerido o introducido en alguna parte del cuerpo, busque atención médica inmediata. • Si el producto no funciona correctamente, comuníquese con su distribuidor o el centro de servicio más cercano.

Nunca desmonte el dispositivo usted mismo. (No asumimos ninguna responsabilidad por problemas causados por reparaciones o mantenimiento no autorizados).

⚠ Aviso

• El acero inoxidable puede corroerse en algunas circunstancias. Es necesario limpiar y cuidar el dispositivo.

Utilice el limpiador de acero inoxidable. Se recomienda limpiar el dispositivo mensualmente. • No deje caer el dispositivo ni lo someta a golpes, ni lo exponga a altas temperaturas.

Evite que el equipo permanezca sobre superficies o lugares calientes.

sujeto a descargas eléctricas (el desconocimiento puede provocar daños en el equipo).

• No coloque el dispositivo en una temperatura extremadamente caliente (consulte la etiqueta del dispositivo para obtener información detallada).

temperatura ambiente), frío, polvo o humedad y no lo exponga a altas temperaturas.

crmntic rtin

• La cubierta del dispositivo para uso en interiores debe mantenerse alejada de la lluvia y la humedad. • Exponer el equipo a la luz solar directa, a bajas temperaturas o a una fuente de calor como un calentador o

Está prohibido el uso del radiador (el desconocimiento puede suponer un peligro).

• No apunte el dispositivo al sol ni a lugares muy brillantes. Podría aparecer una capa o mancha.

De lo contrario (que sin embargo no es una mnctin), y al mismo ctin la resistencia del sensor en el tiempo

• Utilice el guante proporcionado al abrir la cubierta del dispositivo, evite el contacto directo con el

cubierta del dispositivo, ya que el sudor ácido del nr puede erosionar la superficie ctina del dispositivo cubrir.

• Utilice un paño limpio y seco para limpiar las superficies internas y externas de la cubierta del dispositivo. No utilice detergentes alcalinos. • Conserve todos los envoltorios después de desembalarlos para futuras consultas. En caso de avería, devuelva el dispositivo a fábrica

con el envoltorio original. Devolverlo sin el envoltorio original podría dañar el dispositivo y generar costes adicionales.

• El uso o reemplazo inadecuado de la batería puede provocar peligro de explosión. Reemplácela con la

Solo del mismo tipo o equivalente. Deseche el papel usado según las instrucciones proporcionadas por el fabricante.

• Los productos biométricos de rcntin no son completamente aplicables a entornos ntin. Si requiere un mayor nivel de seguridad, utilice los modos de rcntin de mti. • No permanezca en el carril cuando el dispositivo esté rbtin. • RIESGO DE EXPLOSIÓN SI SE SUSTITUYE LA BATERÍA POR UNA INCORRECTA. DESECHE LA BATERÍA USADA.

PILAS SEGÚN LAS INSTRUCCIONES.

• APTO PARA MONTAJE SOBRE HORMIGÓN U OTRAS SUPERFICIES NO COMBUSTIBLES SOLAMENTE. • La conexión requerirá la conexión del conductor de puesta a tierra reactiva del equipo al conductor de puesta a tierra reactiva de la red.

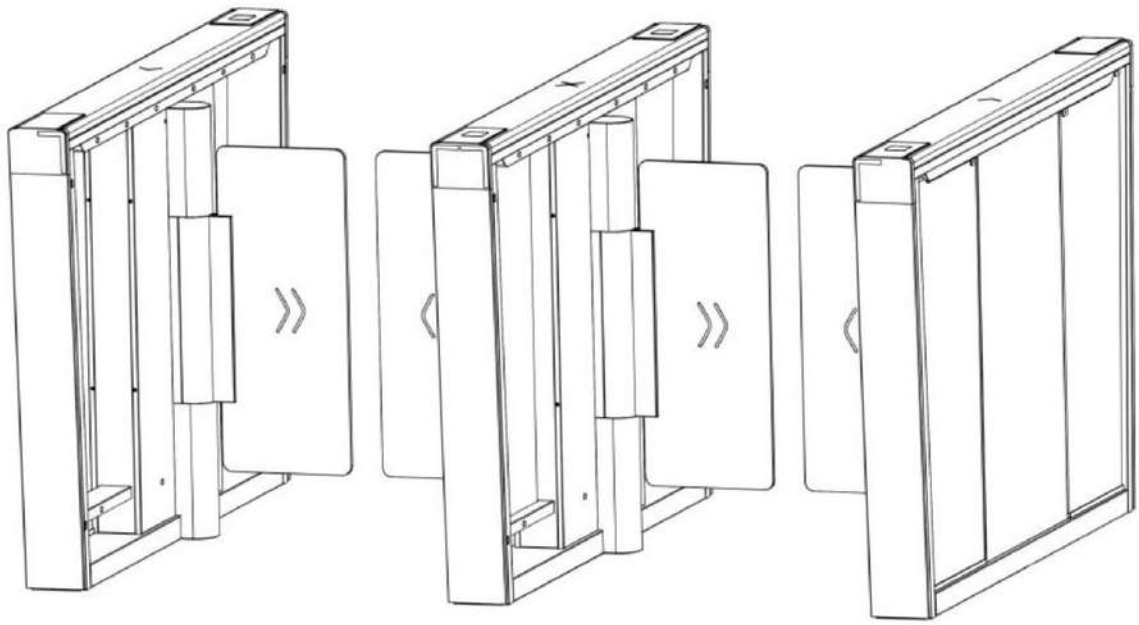
Modelos disponibles

Nombre del producto	Modelo	norte
Barrera oscilante	Pedestal DS-K3B530LX-L/DS-K3B530X-L/	pies
	DS-K3B530LX-M/DS-K3B530X-METRO	Pedestal central
	Pedestal derecho DS-K3B530LX-R/DS-K3B530X-R	

Contenido

Capítulo 1 Descripción general

1.1 nn



La barrera abatible con 14 luces infrarrojas está diseñada para detectar entradas o salidas no autorizadas. Al estaño integrarse con el sistema de control de acceso, la persona debe ser consciente de pasar.
a través del carril deslizando la tarjeta IC o de identificación, escaneando el código QR, etc. Se utiliza ampliamente en rctin estadios, recintos deportivos, residencias, etc.

1.2 Características principales

- Admite modo de control, modo nctiv, modo de paso libre, modo permanecer abierto y modo permanecer abierto. Modo cerrado tanto en la zona de entrada como en la de salida.
- anticorrupción

  La barrera reaccionará según el modo ft o el modo de protección al momento de realizar un acceso forzado.

- ctina Alarma ntic y mtic
- Se activará una alarma audible y visual cuando se produzca una intrusión. paso inverso de estaño, y escalar la barrera.
- El LED indica el estado de entrada/salida y paso.
- Paso de alarma de incendio

  Cuando se activa la alarma r, la barrera se abrirá automáticamente en caso de emergencia.
  vctin
- Pasaje válido rtin n

El sistema cancelará el permiso de paso si una persona no pasa por el carril dentro del carril de paso válido • Carril de entrada/salida

La velocidad de apertura y cierre de la barrera se puede ajustar según el tamaño del visitante.

• Comunicación de red TCP/IP

Los datos de cmmnctin están especialmente encriptados para aliviar la preocupación por la fuga de privacidad.

• Permisos vtin y ntitin • Apertura remota de barrera

mediante llavero y brctin mediante altavoz (brctin personalizado)

El contexto es compatible cuando se instala con la placa de control de acceso).

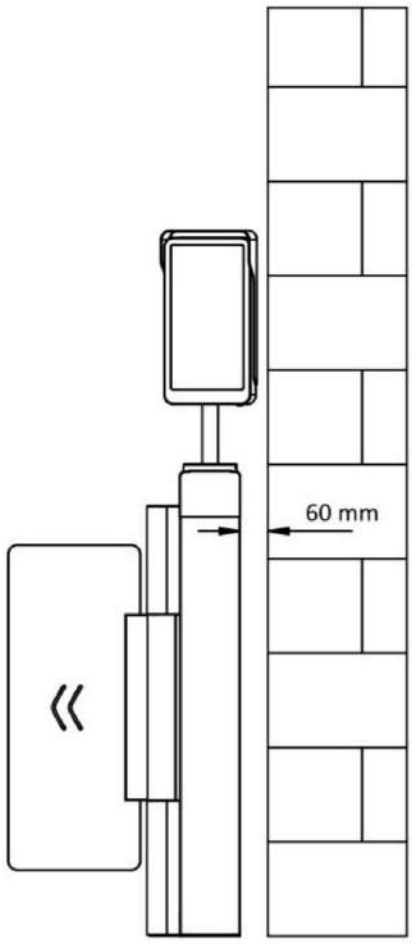
Capítulo 2 Cableado del sistema

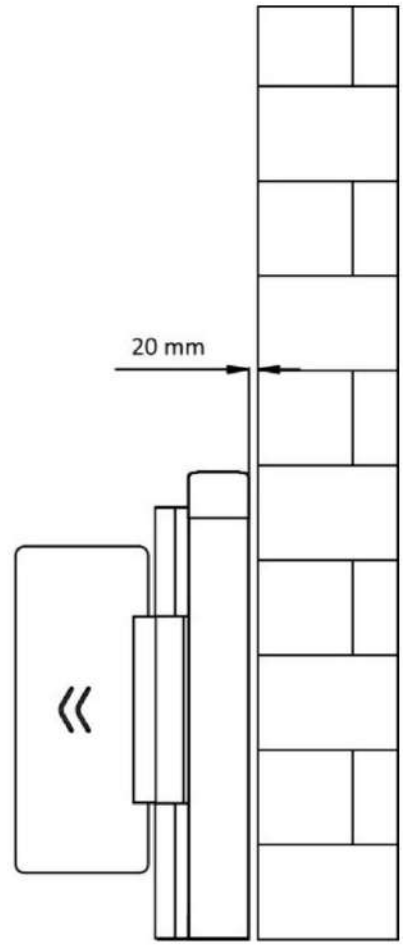
El cableado general.

Pasos

Nota

• El dispositivo debe instalarse sobre una superficie de concreto u otra superficie nnmmb. • Si el área ntin está demasiado cerca de la pared, asegúrese de que la distancia entre el pedestal y la pared no sea inferior a 20 mm (60 mm si tiene terminales rcntin frontales), o no podrá abrir el panel superior del pedestal o podría causar daños a los dispositivos.





• La dimensión es la siguiente.

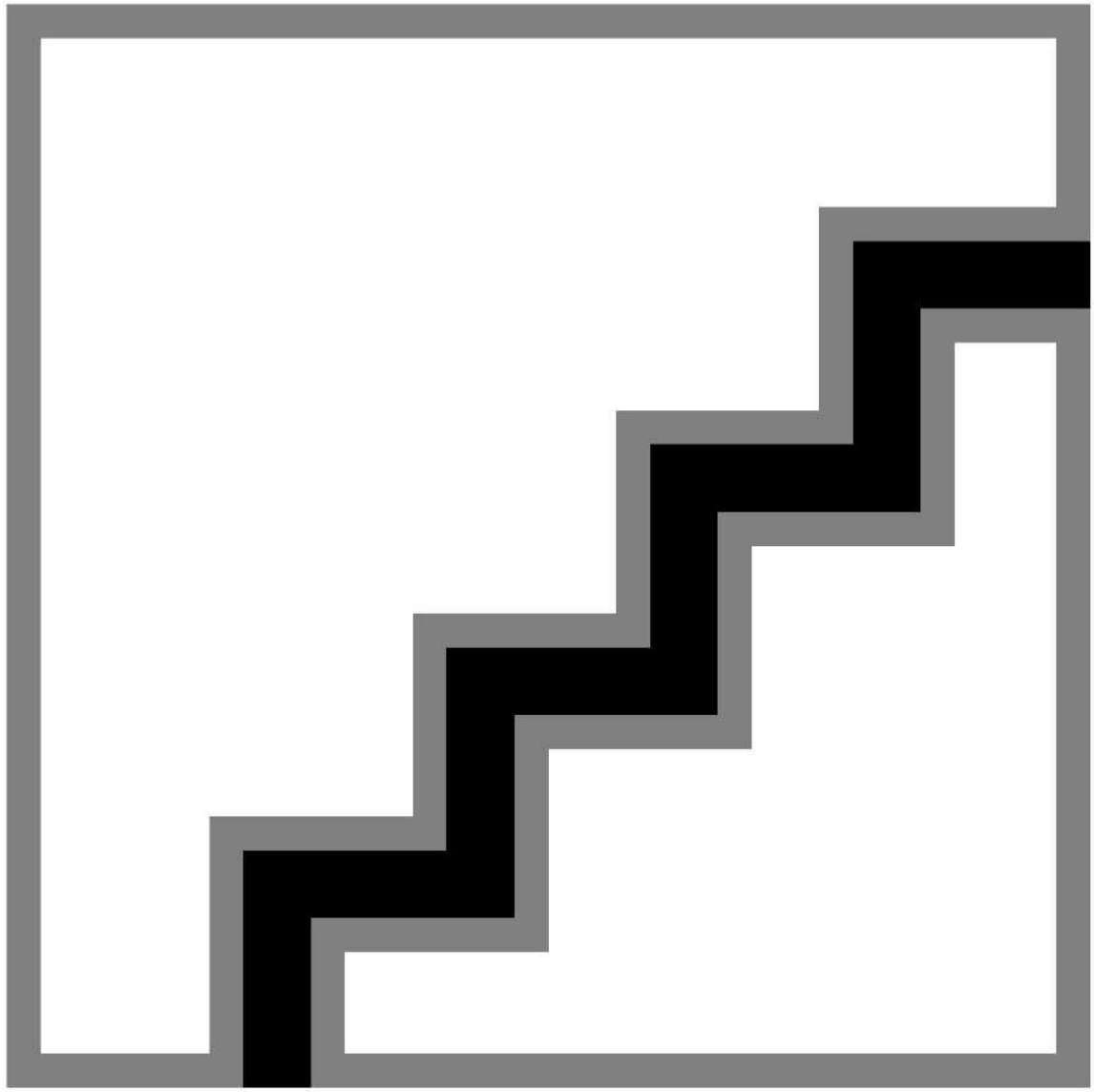


Figura 2-1 Dimensión

1. Dibuje una línea central en la superficie ntin del pedestal derecho o inferior.
2. Dibuje otras líneas paralelas para instalar los otros pedestales.

Nota

La distancia entre las dos líneas más cercanas es L + 272 mm. L representa el ancho del carril.

3. Haga una ranura en la superficie de la lámina y excave los orificios. Coloque 4 pernos de expansión M12*120. cada pedestal.

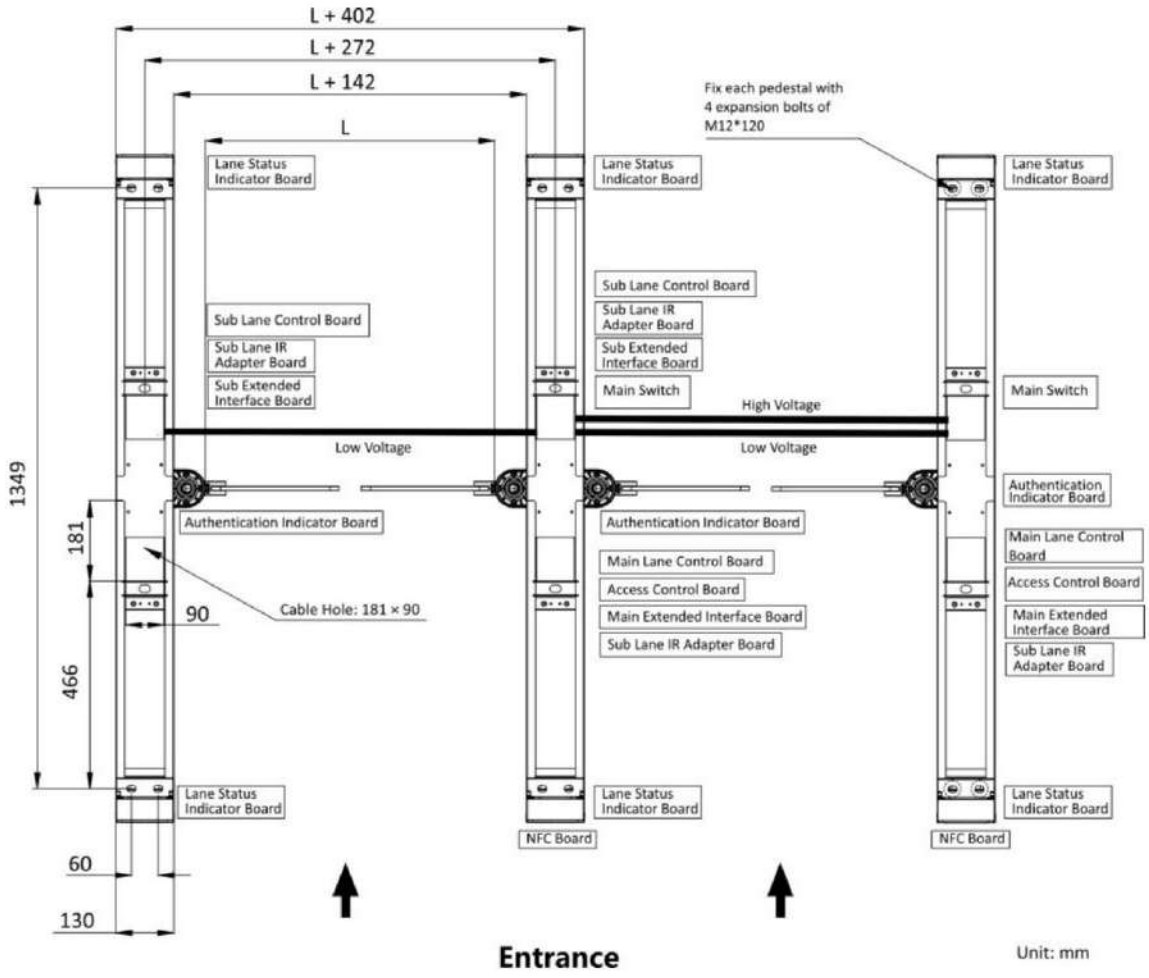


Figura 2-2 Agujero n y cableado del sistema

4. Entierre los cables. Cada carril entierra un cable de alta tensión y uno de baja tensión. Para más detalles, consulte la Diagrama de cableado del sistema del paso 3.

Nota

• Alto voltaje: entrada de alimentación de CA

Baja tensión: cable de conexión (cable de conexión y cable de alimentación de 24 V) y cable de conexión de red

• La longitud del cable de alimentación de 24 V suministrado es de 5 m y la longitud del cable de conexión es de 3 m. • El diámetro interior sugerido del conducto de baja tensión es mayor de 30 mm. • Si desea enterrar tanto el cable de alimentación de CA como el cable de baja tensión, los dos cables

Deben estar en conductos separados para evitar interferencias.

• Si se requieren más periféricos para conectar, debe aumentar el diámetro del conducto o enterrarlos.

Otro conducto para los cables externos.

• El cable de alimentación de CA externo debe tener doble aislamiento.

• El cable de red debe ser CAT5e o tener un rendimiento br.

Capítulo 3 Instalación de pedestales

Antes de comenzar

Prepare las herramientas ntin, verifique el dispositivo y los accesorios y limpie la base ntin.

Pasos

Nota

• El dispositivo debe instalarse sobre una superficie de concreto u otra superficie nnmmb. • Asegúrese de que el dispositivo esté encendido durante ntin y otros rtin. • Las herramientas ntin se colocan dentro del paquete del pedestal.

1. Prepárese para las herramientas ntin, verifique los componentes y prepárese para la base ntin.
2. Retire los 4 tornillos de cada pedestal que fijan los 2 paneles laterales.

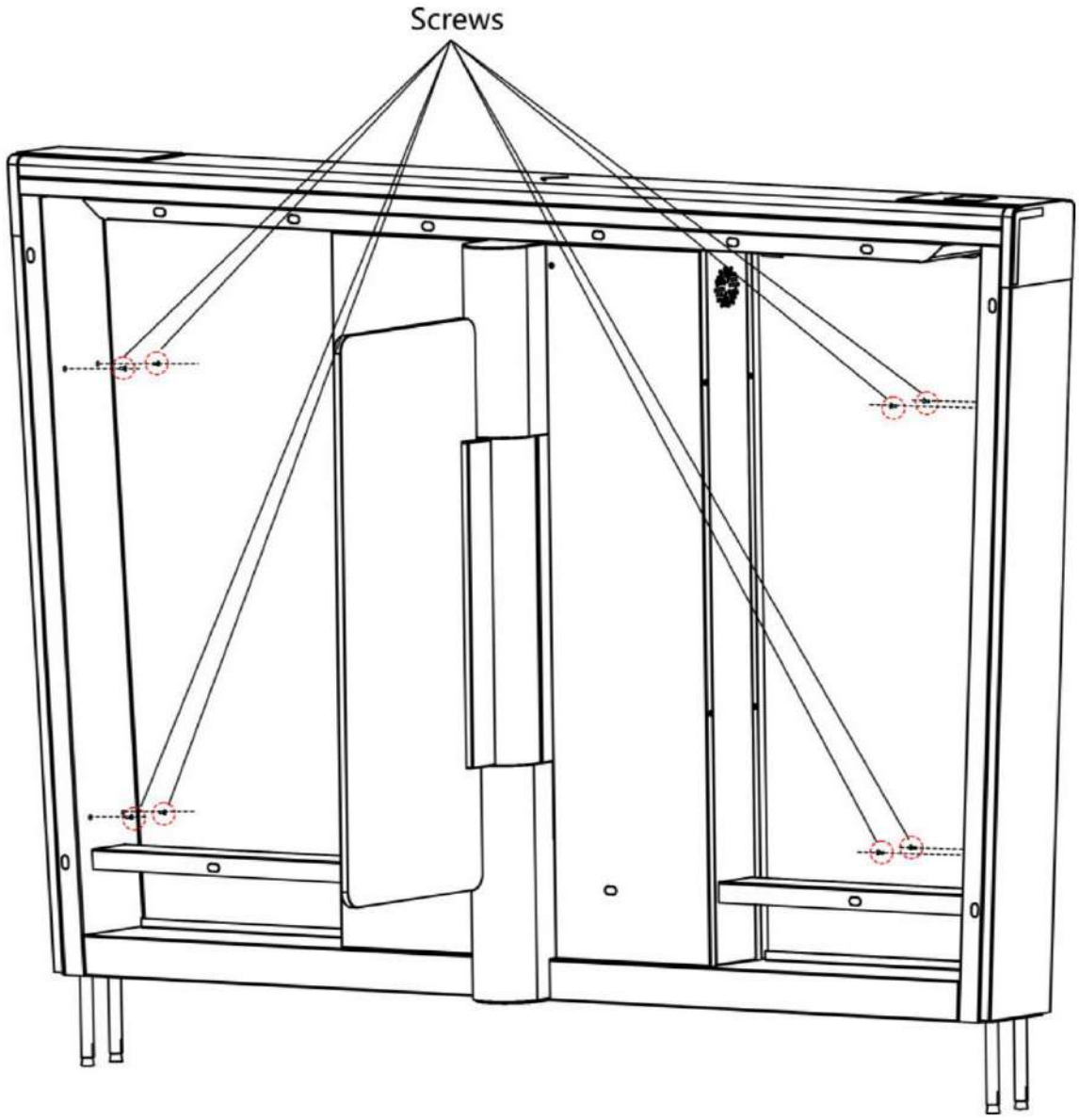


Figura 3-1 Retire los tornillos del panel lateral

3. Retire los paneles laterales y mueva los pedestales a los lugares correspondientes. estaño según el marcas de entrada y salida en los pedestales.

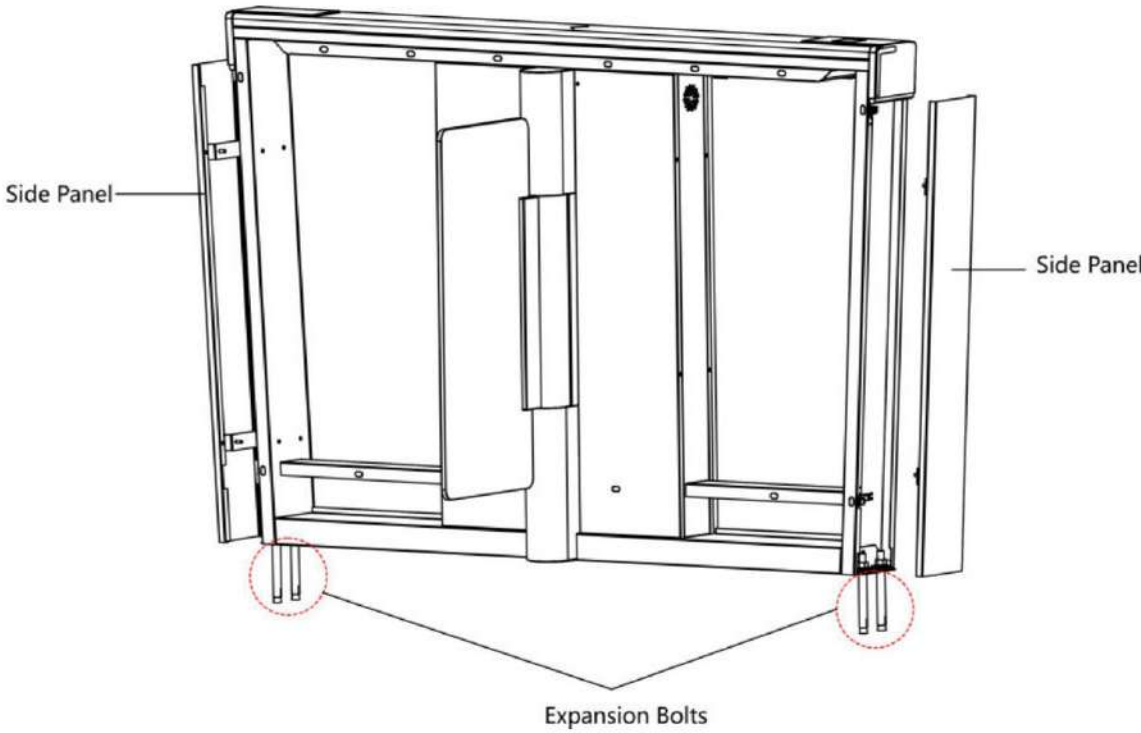


Figura 3-2 Retire los tornillos del panel lateral

Nota

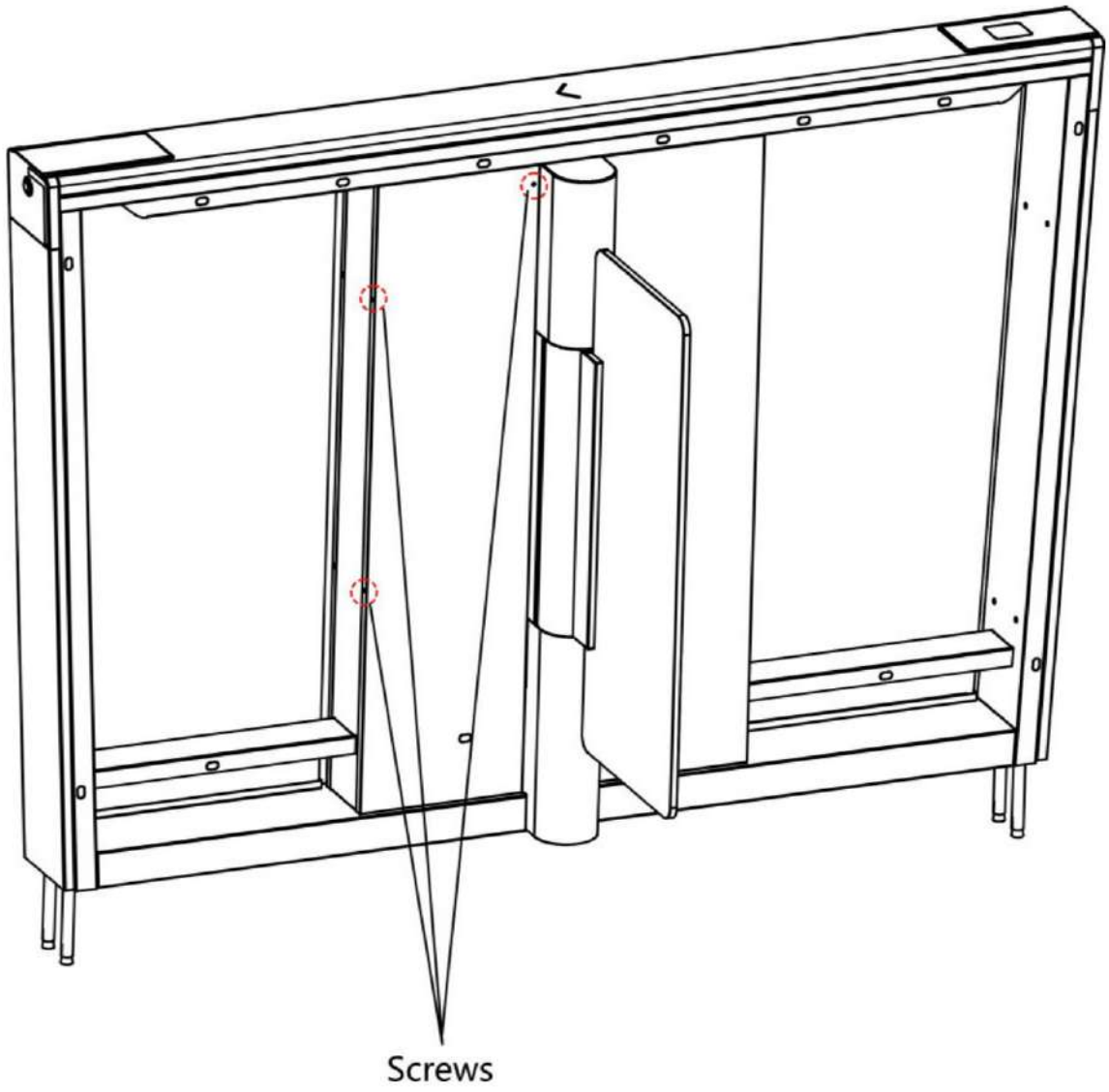
Para obtener información detallada sobre el cableado del sistema, consulte Cableado del sistema .

4. Fije los pedestales con pernos de expansión y fije los paneles laterales a su posición original. lata con tornillos.

Nota

• No sumerja el pedestal en agua. En circunstancias especiales, la altura de inmersión... no debe ser más de 150 mm.

5. Retire 3 tornillos para abrir cada puerta de mantenimiento para el cableado.


Screws

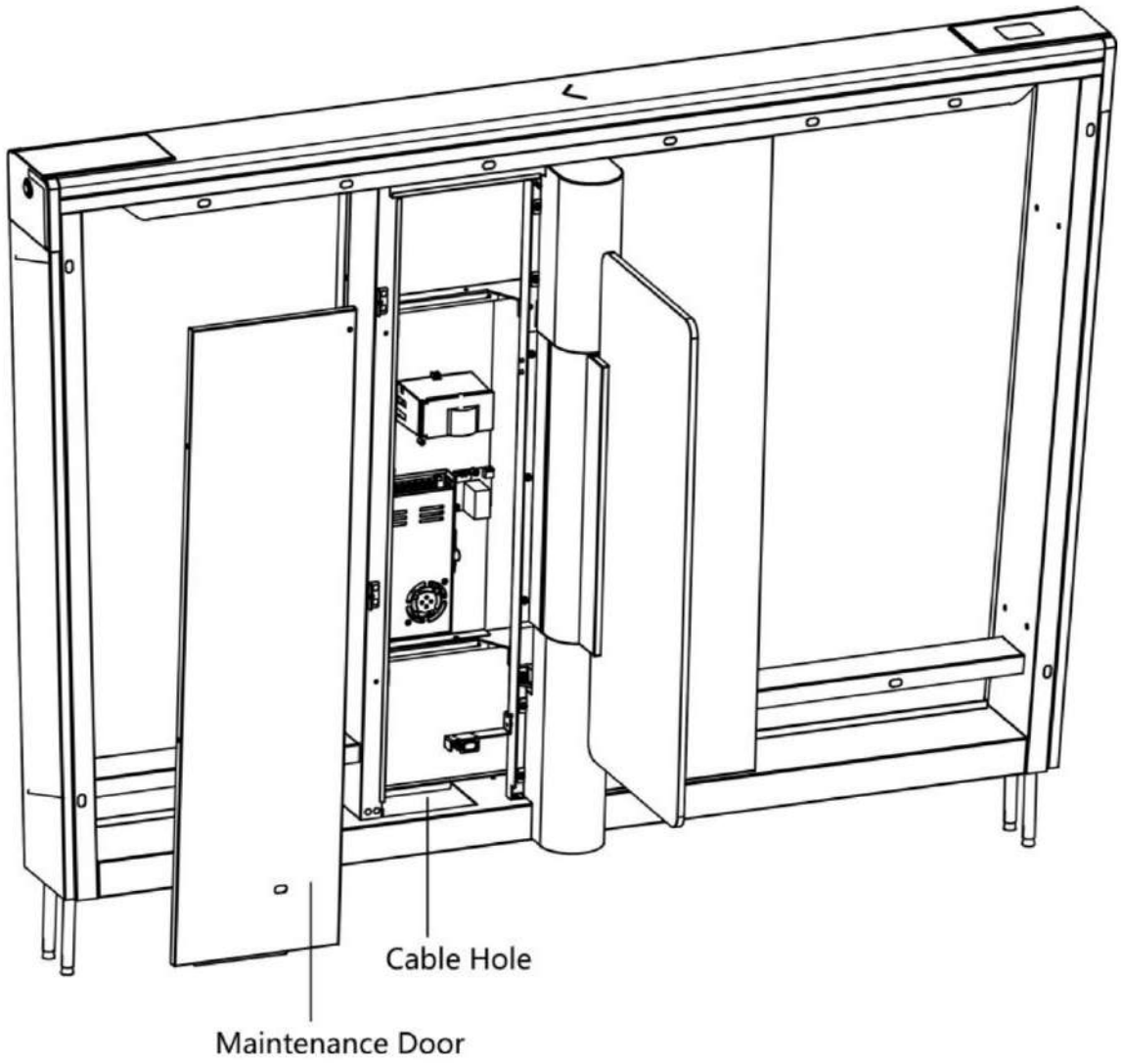


Figura 3-3 Retire la puerta de mantenimiento

Nota

Para obtener información detallada sobre los cables, consulte Cableado general .

Capítulo 4 Cableado general

Nota

• Cuando deba realizar mantenimiento o desmontar los módulos de alto voltaje, deberá retirar el Desconecte los cables de los periféricos antes de realizar tareas de mantenimiento para evitar daños en el dispositivo. • Al desmontar el módulo de alto voltaje, desconecte la alimentación para evitar lesiones. • Si solo se necesita cableado sin realizar tareas de mantenimiento, no retire los módulos de alto voltaje. • El interruptor y la placa de control principal ya están conectados. El cable de 14 AWG para la conexión entre la fuente de alimentación de CA y el interruptor debe adquirirse por separado.

• Se suministran 2 cables de conexión: cable de alimentación de 24 V y cable de conexión.

Cable de alimentación de 24 V: 5 m de largo, que se encuentra en el pedestal central y derecho.

Cable Cmmnctin: 4 m de largo, CAT5e, que se encuentra en el paquete del pedestal medio y derecho.

4.1 Componentes nn

De forma predeterminada, los componentes básicos del rnti están bien conectados. Los pedestales se comunican mediante los cables nrcnnctin. Además, el rnti admite el cableado de la fuente de alimentación de CA para todo el sistema.

Nota

La tensión ctin del suministro eléctrico está entre 100 VCA y 240 VCA, 50 a 60 Hz.

La imagen que se muestra a continuación describe el puerto serie en la entrada y salida rctin.

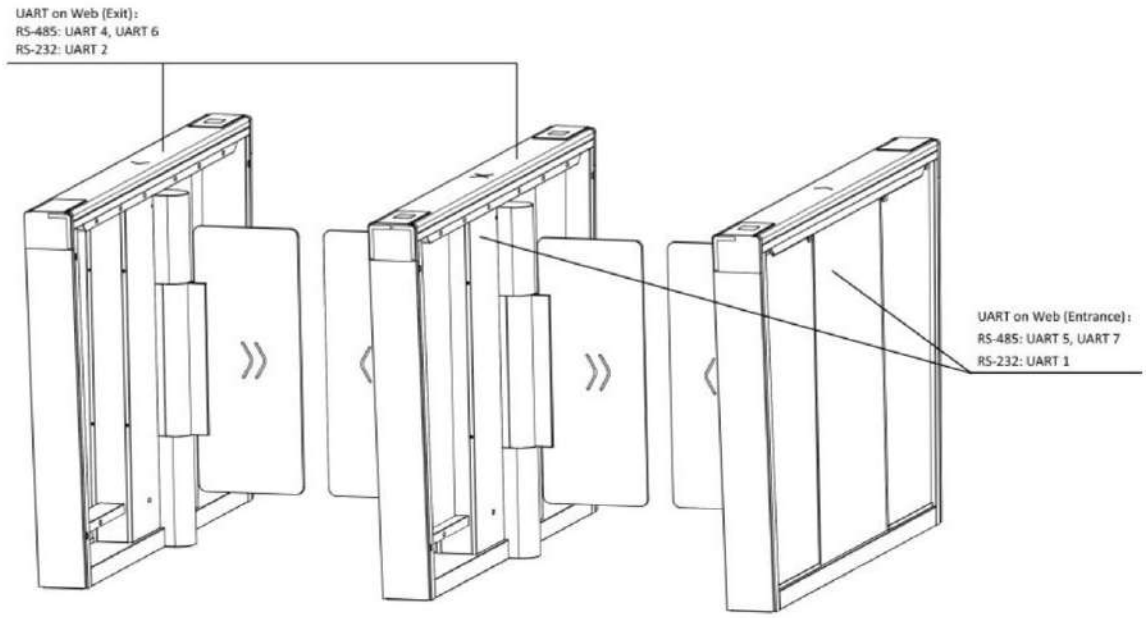


Figura 4-1 Puerto serie

La imagen que se muestra a continuación describe el módulo de envío/recepción de IR y su número correspondiente en el pedestal.

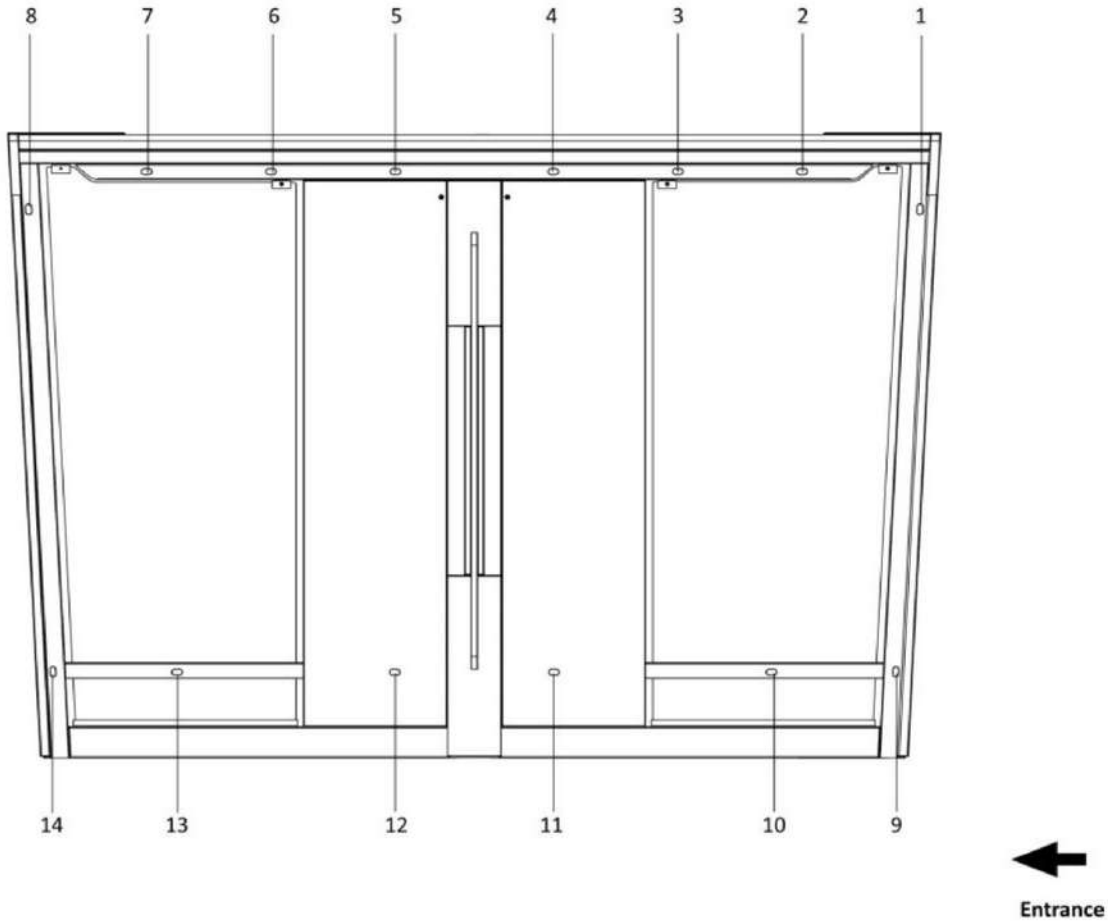


Figura 4-2 Módulo de envío/recepción de IR

Nota

De pie en la entrada del carril, los módulos IR a sus pies son los módulos de envío IR, los que están a su derecha son los módulos de recepción IR.

4.2 Cableado

Escanee el código QR para ver el vídeo guía.

4.3 Terminal norte

4.3.1 Cableado general

El cableado general de la placa de control de carril, la placa de control de acceso y la placa de interfaz extendida.

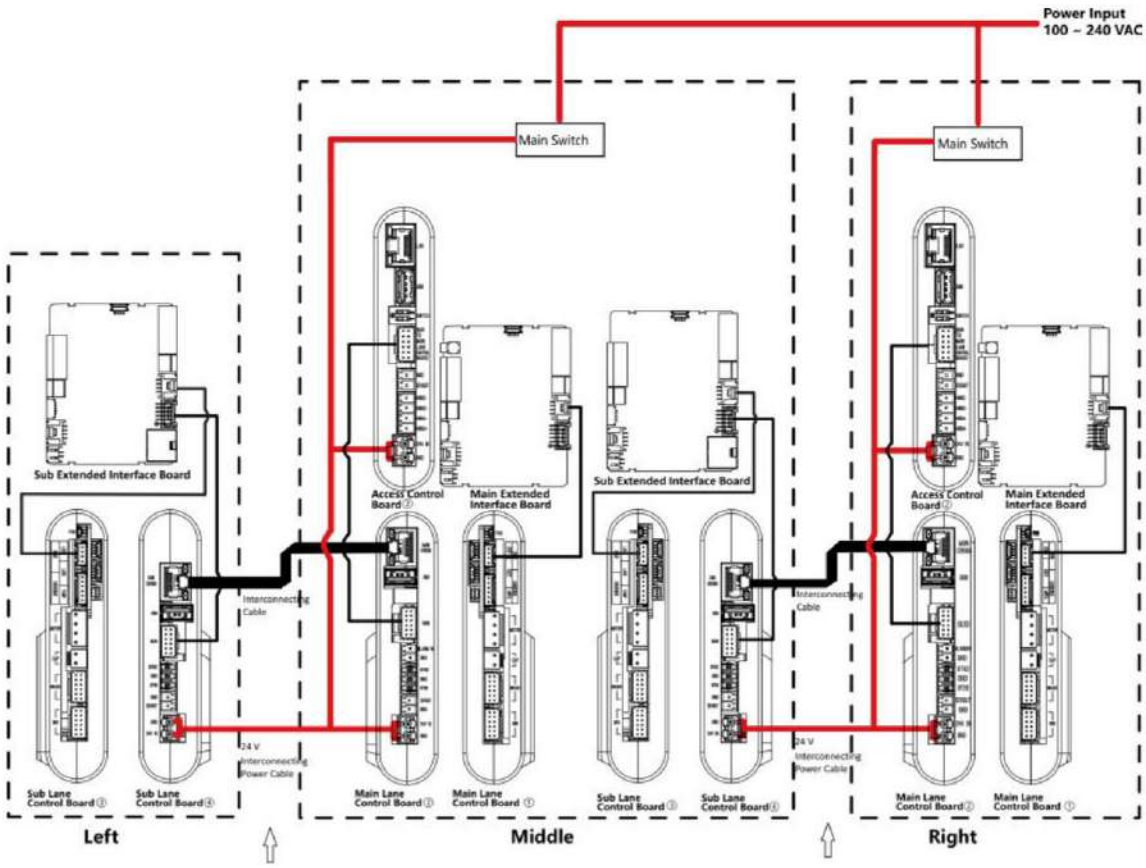


Figura 4-3 Cableado general

Nota

• El cable de alimentación de la fuente de alimentación al panel de control principal del carril está conectado. Deberá preparar el cable de alimentación de 14 AWG para conectar la entrada de CA a la fuente de alimentación.
• Los 2 cables de conexión suministrados deben conectarse en el sitio:
1. Cable de alimentación de 24 V de 14 AWG. El cable tiene una longitud de 5 m y se coloca dentro del pedestal derecho/central en la salida.
2. Cable de conexión CAT5e. El cable tiene 3 m de longitud y se coloca dentro del paquete del pedestal derecho/central. • y o y se refieren
a los dos lados de una misma placa. • Barrera que se abre en la entrada/salida: conectar a BTN1/ BTN2 y GND.

4.3.2 Terminal del tablero de control del carril principal norte

La placa de control del carril principal contiene una interfaz nrcnnctin, una interfaz de placa de control de acceso, una interfaz de entrada r, una interfaz bn de salida, una interfaz de salida de 12 VCC, una interfaz de entrada de 24 VCC, una interfaz de ventilador, una interfaz cmmnctin, una interfaz de codificador, una interfaz de fuente de alimentación para motor, una interfaz de supercondensador, una interfaz de freno principal, una interfaz de adaptador y una interfaz de manipulación.

La imagen que se muestra a continuación es el diagrama del tablero de control del carril principal.

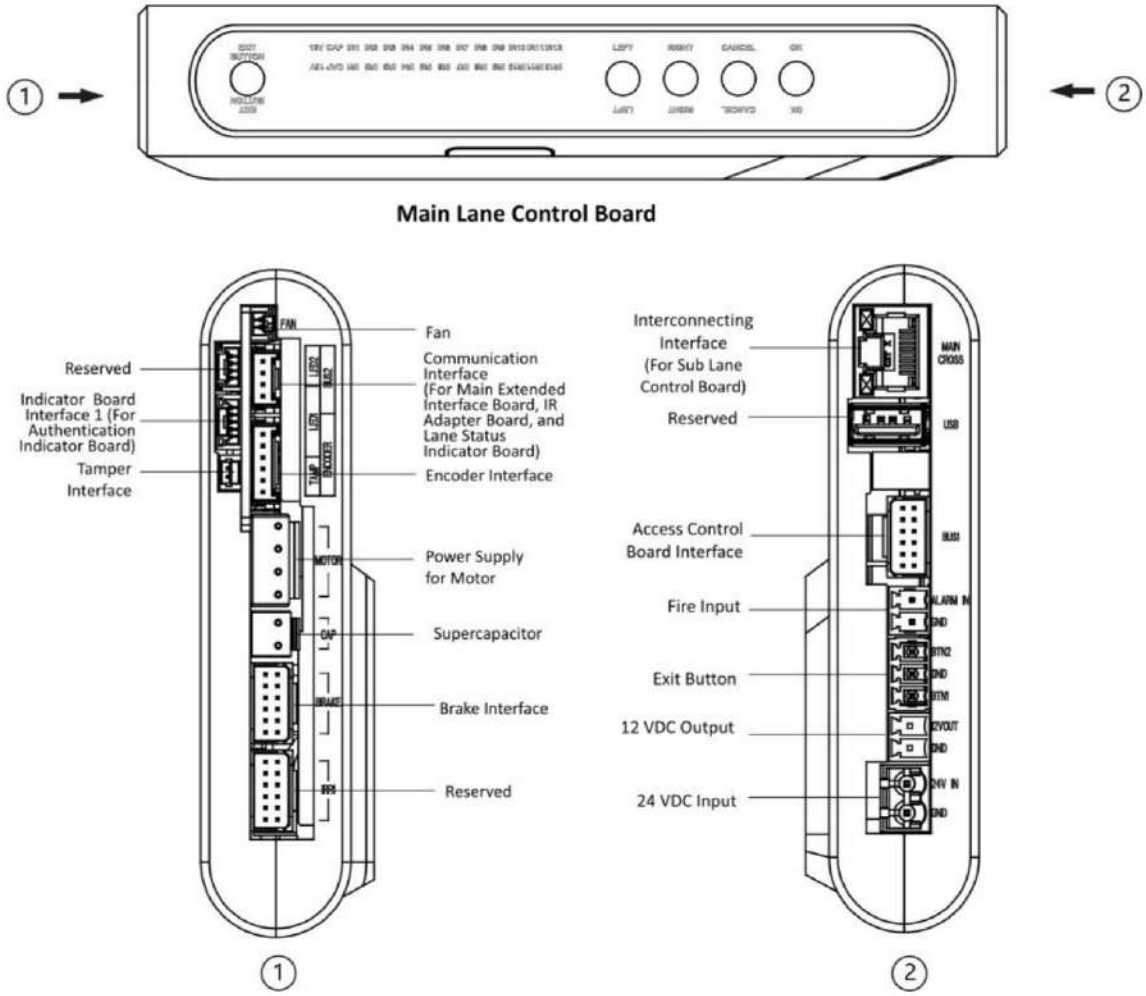


Figura 4-4 Terminales de la placa de control del carril principal

4.3.3 Terminal de la placa de control de subcarril norte

La placa de control de subcarril contiene una interfaz nrcnnctin, una interfaz BUS, una interfaz bn de salida, una interfaz de salida de 12 VCC, una interfaz de entrada de 24 VCC, una interfaz de ventilador, una interfaz cmmnctin, una interfaz de codificador, una interfaz de fuente de alimentación para motor, una interfaz de supercondensador, una interfaz de freno secundario, una interfaz de adaptador y una interfaz de manipulación.

La imagen que se muestra a continuación es el diagrama del tablero de control del subcarril.

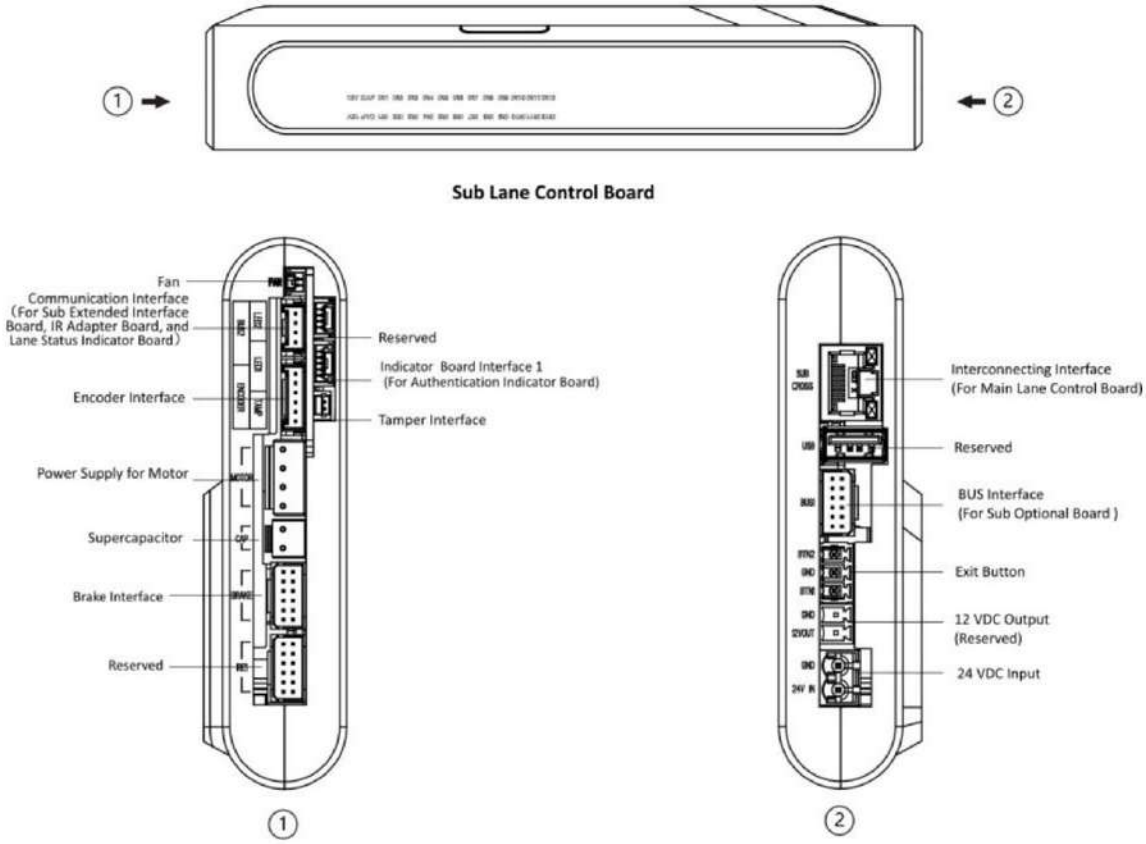


Figura 4-5 Terminales de la placa de control del subcarril

4.3.4 Terminal de la placa de control de acceso n (n)

El tablero de control de acceso se utiliza principalmente para la prohibición de autoridades en lugares con altos niveles de seguridad, como seguridad pública o lugares judiciales, acceso a dispositivos externos y comunicación con el controlador de carril y el controlador de carril superior.

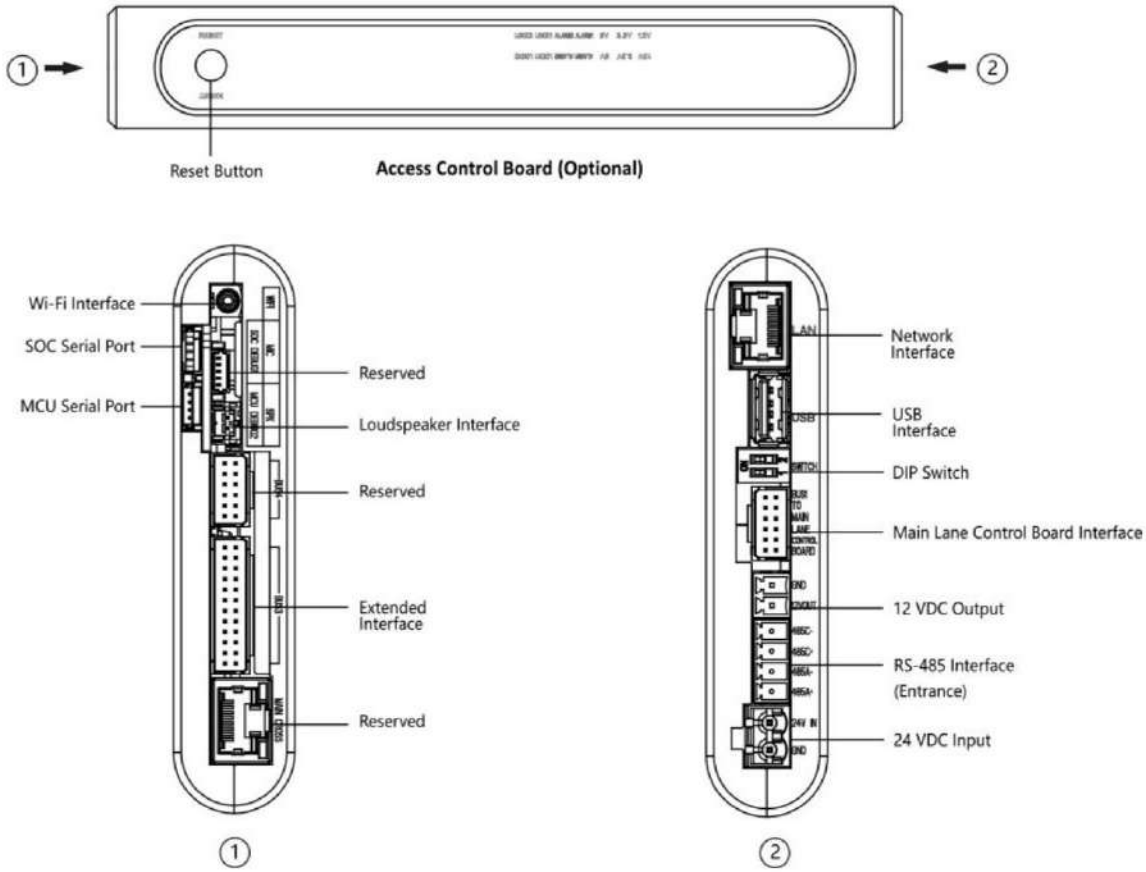


Figura 4-6 Placa de control de acceso

Nota

• RS-485A corresponde al puerto 5 en la web y es para el escáner de código QR que se encuentra en la entrada. predeterminado; RS-485C corresponde al puerto 7 en la web y es para la conexión del lector de tarjetas en la entrada de forma predeterminada.

• El puerto serie del SOC y del MCU es solo para mantenimiento y depuración. • Presione el botón de reinicio durante 5 segundos y el dispositivo comenzará a restaurarse a la configuración de fábrica. • El interruptor DIP es para el modo de estudio y el emparejamiento del llavero. Para obtener información detallada sobre... Interruptor DIP, ver Interruptor DIP .

El diagrama de cableado de la interfaz extendida de la placa de control de acceso se muestra a continuación.

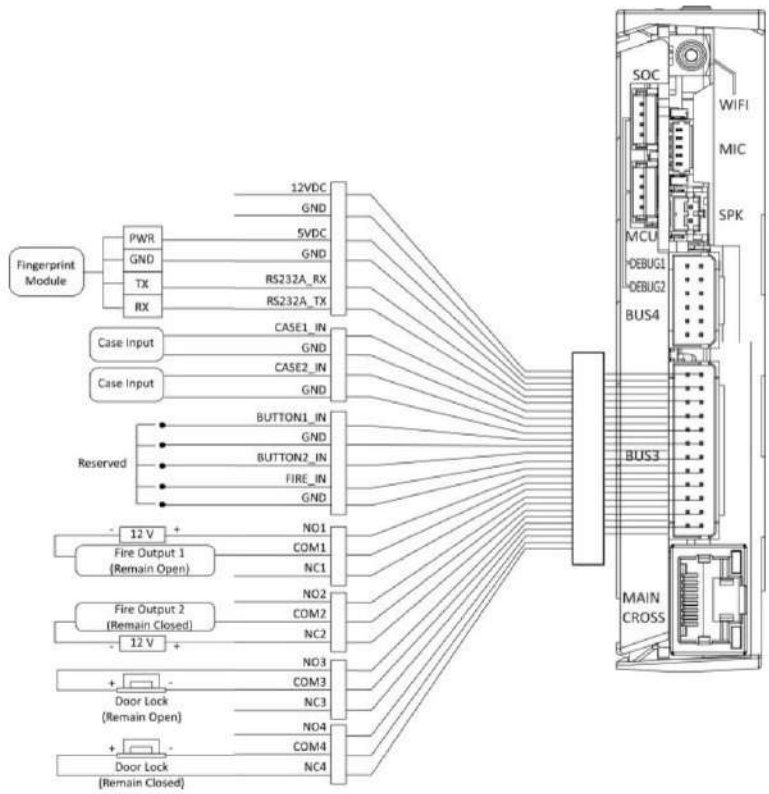


Figura 4-7 Diagrama de Wring de la interfaz BUS3

Nota

RS-232A corresponde al puerto 1 en la web.

4.3.5 Terminal de la placa de interfaz extendida principal norte

La placa de interfaz extendida principal contiene la interfaz de antena sub-1G, la interfaz de luz de barrera, la interfaz de altavoz, el puerto de depuración, la interfaz Wiegand/exit bn, la salida de 5 VCC y la interfaz cmmnctin.

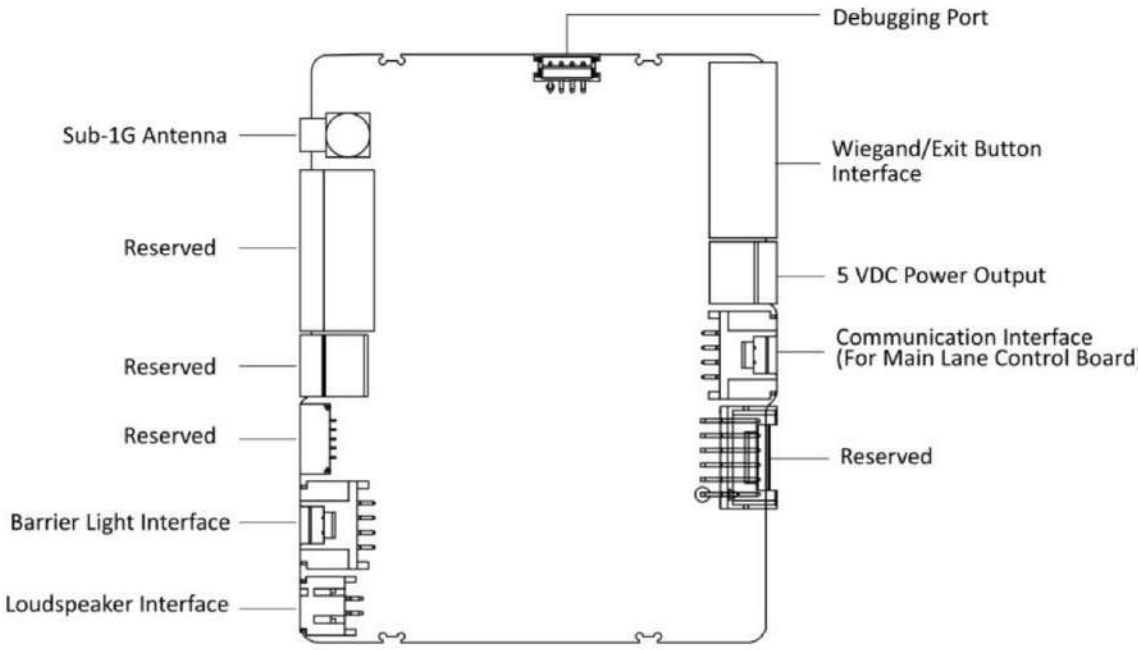


Figura 4-8 Terminal de la placa de interfaz extendida principal

Nota

Si el dispositivo se instala con una placa de control de acceso, el altavoz debe conectarse a esta. De lo contrario, debe conectarse a la placa de interfaz extendida principal.

4.3.6 Terminal de la placa del lector de tarjetas

La placa lectora de tarjetas se puede conectar a la placa de control de acceso a través de la interfaz RS-485.

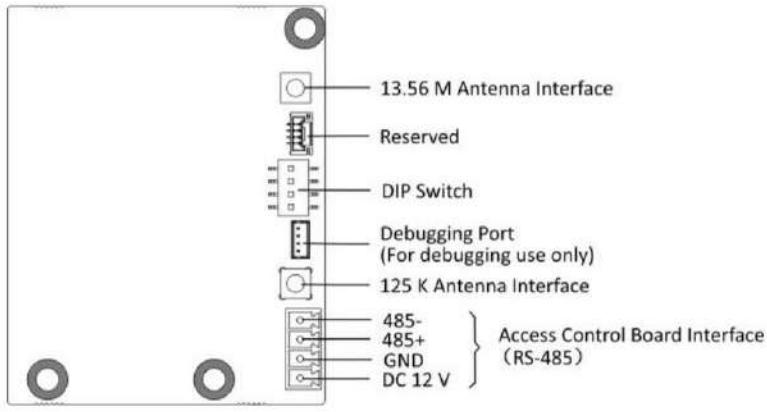


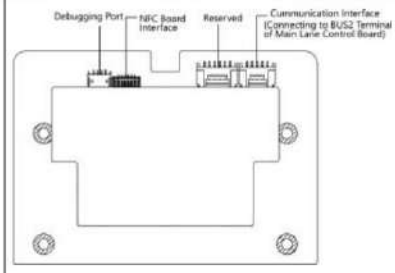
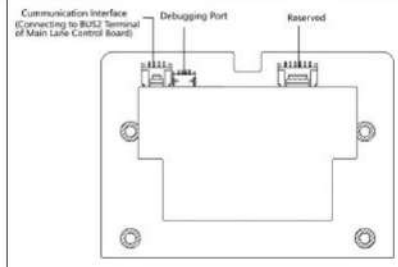
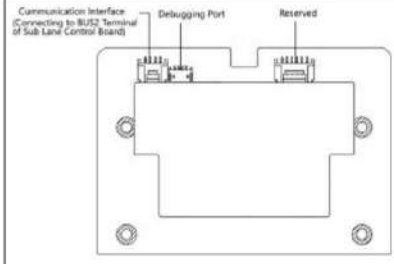
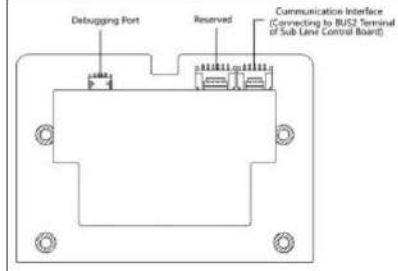
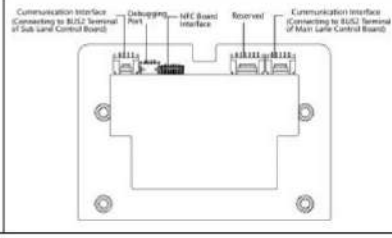
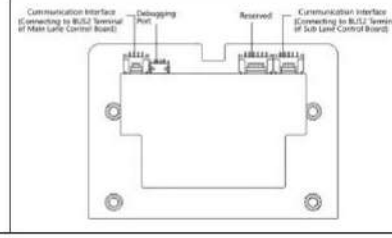
Figura 4-9 Placa del lector de tarjetas

4.3.7 Tablero indicador del estado del carril

Para obtener detalles sobre el indicador de estado del carril, consulte .

El tablero indicador del estado del carril en los pedestales rn se muestra de la siguiente manera.

Tabla 4-1 Tablero indicador de estado del carril

Pedestal	Entrada	Salida
Pedestal derecho		
Pedestal de pies		
Pedestal central		

4.3.8 Terminal de la placa indicadora nn

norte

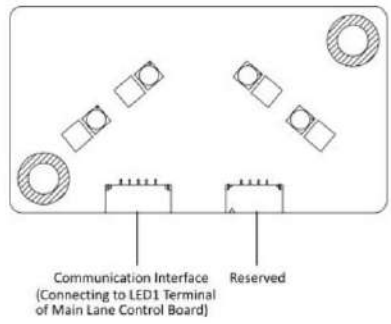


Figura 4-10 Placa indicadora nn

El La placa indicadora ntictin está conectada al terminal LED1 de la placa de control del carril principal.

4.3.9 Cableado RS-485

Se recomienda conectar las interfaces RS-485 de la placa de control de acceso y la placa de interfaz subextendida al módulo de reconocimiento facial o al lector de tarjetas. A continuación, se toma como ejemplo la conexión con un lector de tarjetas.

Nota

• La placa de control de acceso cuenta con dos interfaces RS-485 para la entrada. Consulte Control de Acceso. Terminal de la n (n) para más detalles.
placa. Hay dos interfaces RS-485 en la placa de interfaz subextendida para la salida. Consulte para obtener más detalles. • Si se conecta el RS-485 con un lector de tarjetas, por defecto, el interruptor DIP del lector de tarjetas debe...
se establecerá de la siguiente manera:

- Para ingresar, coloque el interruptor DIP de 4 dígitos número 1 en el lado ON.
- Para salir, coloque el interruptor DIP de 4 dígitos número 3 en el lado ON.

• Si hay otros dispositivos RS-485 conectados, no se puede controlar el ID del RS-485. • La interfaz de alimentación de 12 V conectada para el terminal de control frontal no se puede conectar con
Otros dispositivos de 12 V.

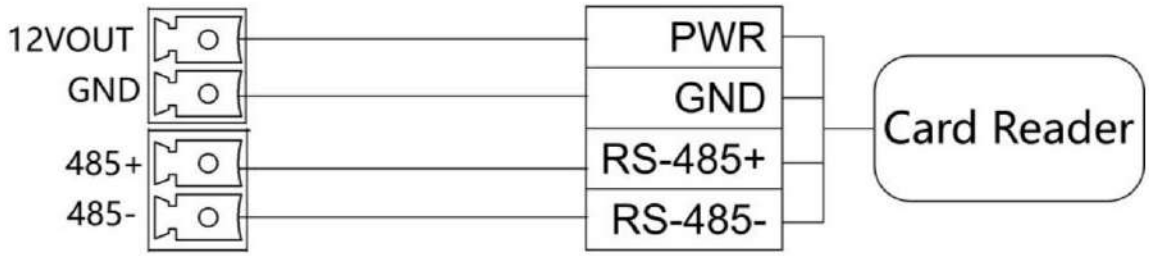


Figura 4-11 Cableado RS-485

4.3.10 Cableado RS-232

Nota

• Hay 1 interfaz RS-232 en la interfaz extendida de la placa de control de acceso, consulte Control de acceso Terminal de placa n (n) . El RS-232A corresponde al UART 1 en la web. • Hay una interfaz RS-232 en la placa de interfaz subextendida, consulte . El RS-232B corresponde
a UART 2 en la web.
La interfaz RS-232C está reservada.

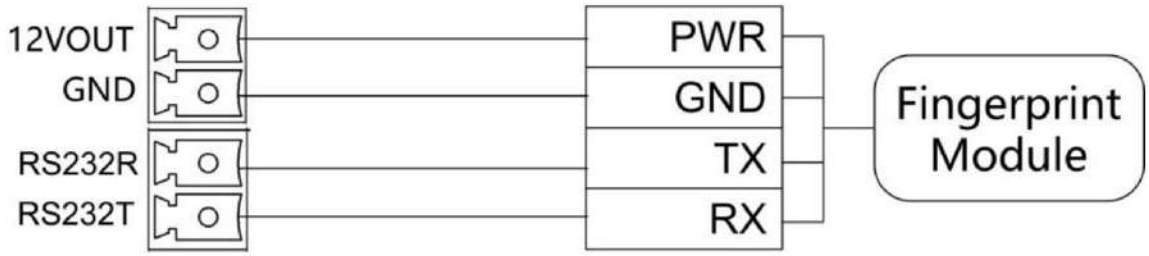


Figura 4-12 Cableado RS-232

4.3.11 Cableado de entrada de alarma

En el tablero de control del carril principal, puedes cablear la interfaz de entrada de alarma r.

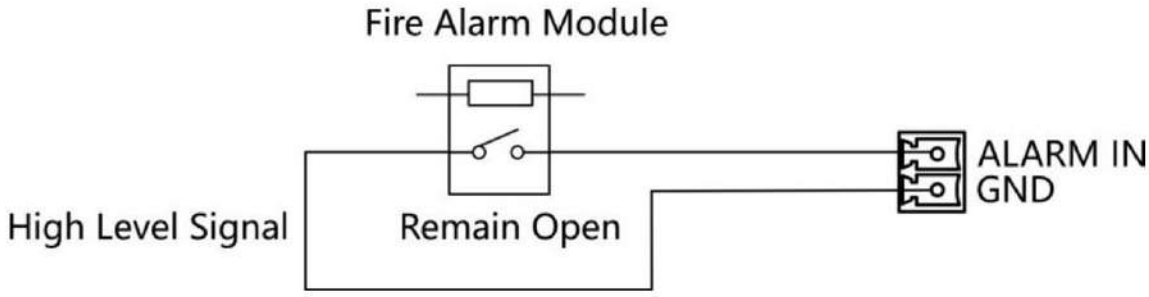


Figura 4-13 Permanecer abierto

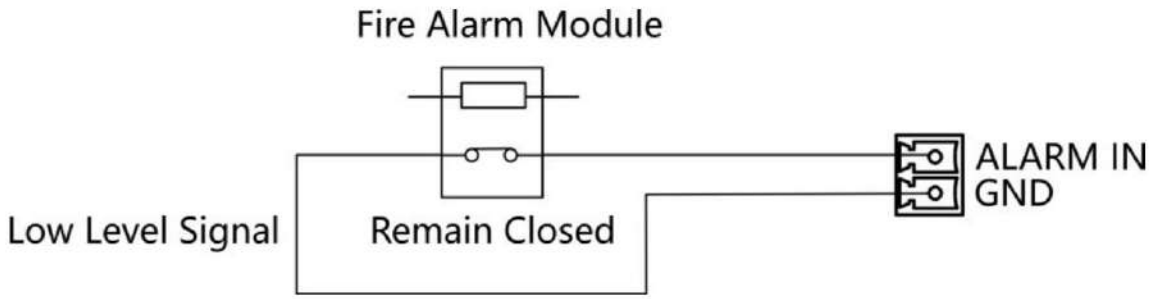


Figura 4-14 Permanecer cerrado

4.3.12 Cableado de salida Bn

La placa de control del carril principal y del carril secundario tiene cada una una interfaz bn, que se puede conectar a la salida bn o al dispositivo rcntin frontal.

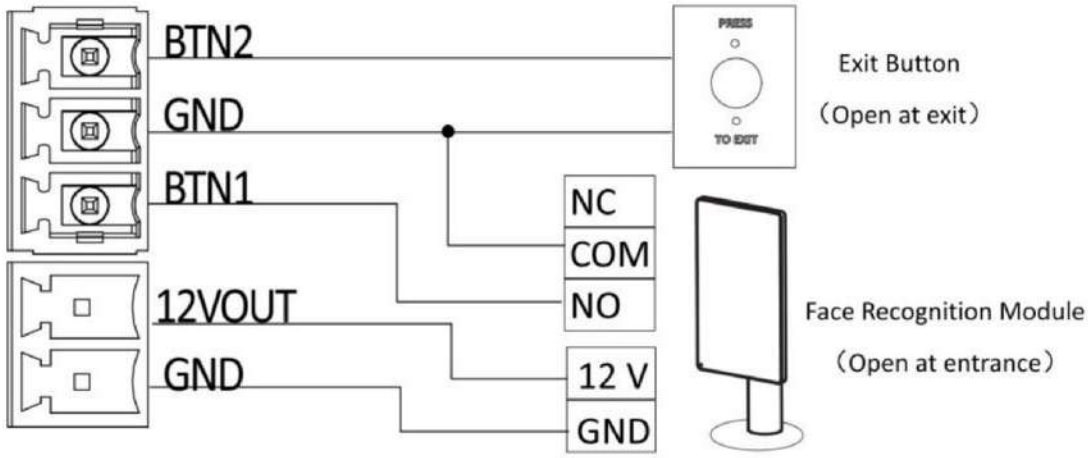


Figura 4-15 Cableado de salida Bn

Nota

• Los dispositivos face rcntin se alimentan a través de una interfaz de salida de energía de 12 VCC de la tablero de control de sub-carril.

• Barrera abierta en la entrada: conectar a BTN1 y GND. • Barrera abierta en la salida: conectar a BTN2 y GND.

4.4 Dispositivo n vía Bn

Puede controlar el dispositivo a través de bn en el tablero de control del carril principal o mediante el interruptor DIP en el tablero de control de acceso.

Fnn	Tablero de control del carril principal y Altavoz (conectado a Interfaz principal extendida Junta)	Tablero de control del carril principal y Tablero de control de acceso y Altavoz (conectado a Placa de control de acceso)
Modo de trabajo		
Modo normal/de estudio	Cnr vía bn (ver Establecer el modo de estudio mediante Bn)	Cnr a través del interruptor DIP (consulte Establecer el modo de estudio a través del interruptor DIP) Interruptor (n))
Emparejamiento de llavero	Cnr vía bn (ver Emparejar llavero mediante Bn)	Cnr a través del interruptor DIP (consulte Emparejar llavero a través del interruptor DIP (n))
Modo de pase	Cnr vía bn	Cnr vía bnwb

Modo	Tablero de control del carril principal y Altavoz (conectado a Interfaz principal extendida Junta)	Tablero de control del carril principal y Tablero de control de acceso y Altavoz (conectado a Placa de control de acceso)
Modo de memoria	Cnr vía bn	Cnr vía bnwb
Modo de control	Cnr vía bn	Cnr vía bnwb
Modo ctin	Cnr vía bn	Cnr vía bn
Parámetro nota		
Velocidad de apertura de la barrera Cnr vía bn		Cnr vía bnwb
Velocidad de cierre de la barrera	Cnr vía bn	Cnr vía bnwb
Lectura de tarjetas en la alarma Área	Cnr vía bn	Cnr vía bnwb
Ingrese rtin	Cnr vía bn	Cnr vía bnwb
Salir de la entrada	Cnr vía bn	Cnr vía bnwb
Detección de infrarrojos rtin	Cnr vía bn	Cnr vía bnwb
Intrusión rtin	Cnr vía bn	Cnr vía bnwb
Exceso de estancia	Cnr vía bn	Cnr vía bnwb
Tiempo de retraso para el cierre de la barrera Cnr vía bn		Cnr vía bnwb
Recuperación de barrera rtin Cnr vía bn		Cnr vía bn
Ajuste del volumen	Cnr vía bn	Cnr vía bn
Material de barrera	Cnr vía bn	Cnr vía bnwb
Longitud de la barrera	Cnr vía bn	Cnr vía bnwb
Altura de la barrera	Cnr vía bn	Cnr vía bnwb
Freno	Cnr vía bn	Cnr vía bn
Ángulo de freno	Cnr vía bn	Cnr vía bn
Detección por infrarrojos	Cnr vía bn	Cnr vía bnwb
Admirador	Cnr vía bn	Cnr vía bn
Brillo de la luz	Cnr vía bn	Cnr vía bnwb
Restaurar a valores predeterminados	Cnr vía bn	Cnr vía bnwb
Aviso de voz		

Modo	Tablero de control del carril principal y Altavoz (conectado a Interfaz principal extendida Junta)	Tablero de control del carril principal y Tablero de control de acceso y Altavoz (conectado a Placa de control de acceso)
Escalando la barrera	Habilitar o deshabilitar a través de bn	Habilitar o deshabilitar a través de bn
Pase inverso	Habilitar o deshabilitar a través de bn	Habilitar o deshabilitar a través de bn
Superando el paso rtin	Habilitar o deshabilitar a través de bn	Habilitar o deshabilitar a través de bn
Alarma de intrusión	Habilitar o deshabilitar a través de bn	Habilitar o deshabilitar a través de bn
Alarma de estaño	Habilitar o deshabilitar a través de bn	Habilitar o deshabilitar a través de bn
Alarma de sobrepasar el límite de permanencia	Habilitar o deshabilitar a través de bn	Habilitar o deshabilitar a través de bn
Nctina motora	Cnr vía bn	Cnr vía bn
Aviso de voz de autocomprobación	Habilitar o deshabilitar a través de bn	Habilitar o deshabilitar a través de bn
Aviso de voz del modo de estudio	Habilitar o deshabilitar a través de bn	Habilitar o deshabilitar a través de bn

Nota

- Consulte Bn Cnn n para obtener información detallada
- Si el dispositivo no está equipado con una placa de control de acceso, el altavoz se debe conectar a La placa de interfaz extendida principal.
- Si el dispositivo está equipado con una placa de control de acceso, el altavoz se debe conectar a la Placa de control de acceso. Puede configurar un contexto de brctin personalizado a través de la web. Para más detalles, consulte el Aviso Cronograma .

4.4.1 CNN vía Bn

Modo

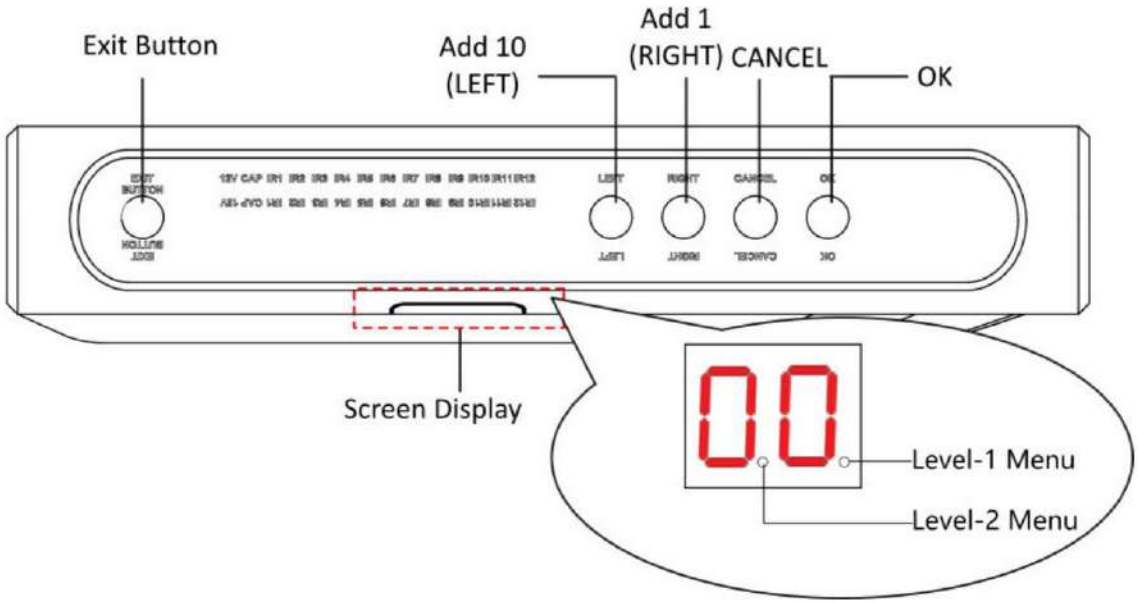


Figura 4-16 Bn

Salida Bn

• Presione para abrir la barrera desde la lata de entrada •
Presione dos veces para abrir la barrera desde la lata de salida

Parámetro Cnn Bn

• IZQUIERDA: Presione para agregar 10 datos a la
celda. • DERECHA: Presione para agregar 1 dato a
la celda. • CANCELAR: Regrese al menú de Nivel 1 o salga del menú de
Nivel 1. • ACEPTAR: Confirme n o ingrese al modo cnrtin, o ingrese al menú de Nivel 2.

Nota

• El número de la casilla se muestra mediante dos tubos
digitales. • Menú de nivel 1: Si el punto decimal a la derecha está activado, indica el menú de
nivel 1. El número representa el número de
la casilla. • Menú de nivel 2: Si el punto decimal en el centro está activado, indica el menú de nivel
2. El número representa el número de la casilla.

Procedimiento de Bn Cnn

Aquí se toma n intrusión rtin a 12 s como ejemplo:

Figura 4-17 Procedimiento

Pasos:

1. Mantenga pulsado el botón OK durante 3 s hasta que suene un pitido. El dispositivo entra en modo de reinicio. Nivel 1 El menú se ilumina. La pantalla muestra la orden n.º 1.
2. En el menú de Nivel 1, presione IZQUIERDA (más 10) una vez y presione DERECHA (más 1) dos veces para establecer el número de la tecla en 12. Presione OK n y entrar al menú de nivel 2. O puedes para guardar, presione CANCELAR para salir del menú actual o no realice ninguna operación durante 5 s para cancelar la operación y salir del menú actual.
3. Después de ingresar al menú de nivel 2, presione IZQUIERDA (más 10) una vez y DERECHA (más 1) dos veces para establecer el número de la tecla en 12. Presione OK para guardar o presione CANCELAR para salir del menú actual o no realice ninguna operación durante 5 s para cancelar la operación y salir del menú actual. menú.

Nota

- El n.° de transacción se mostrará en un ciclo.
- Cada número de transacción se refiere a una transacción. Para obtener detalles sobre el número de transacción y su nctin relacionado véase Bn Cnn n .

4.4.2 Modo de estudio n

Coloque la lata cerrada de la barrera del dispositivo.

Establecer el modo de estudio a través de Bn

Ingrese al modo de estudio a través de bn cnrtin para configurar el latín cerrado de la barrera del dispositivo.

Pasos

Nota

• Si el dispositivo está equipado con una placa de control de acceso, puede configurar el modo de estudio a través del interruptor DIP en la placa de control de acceso únicamente. • Para obtener más detalles sobre bn rtin, consulte .
Cnn a través de Bn • Para obtener más detalles sobre el n.º de cnrtin y su nctin relacionado, consulte Bn Cnn norte .

1. Ingrese al modo de estudio.
   1) Ingrese al modo cnrtin.
   2) Establezca el número de transacción en el Nivel 1 en 1. El dispositivo ingresará al modo de estudio.
   3) Establezca el número de transacción en el menú de Nivel 2 en 2. El dispositivo ingresará al modo de estudio.
2. Encienda el dispositivo y gire la barrera hasta que quede verticalmente hasta el pedestal.
3. Encienda el dispositivo.
   El dispositivo recordará la hora actual . Reinicie el dispositivo cuando escuche «Estudio completado». Por favor, reinicie.

Establecer el modo de estudio mediante el interruptor DIP (n)

Ingrese al modo de estudio a través de la conmutación DIP para configurar la lata cerrada de la barrera del dispositivo.

Pasos

1. Coloque el interruptor DIP de 2 dígitos n.° 1 en la placa de control de acceso en ON haciendo referencia a r para siguiente ingresar al modo de estudio.

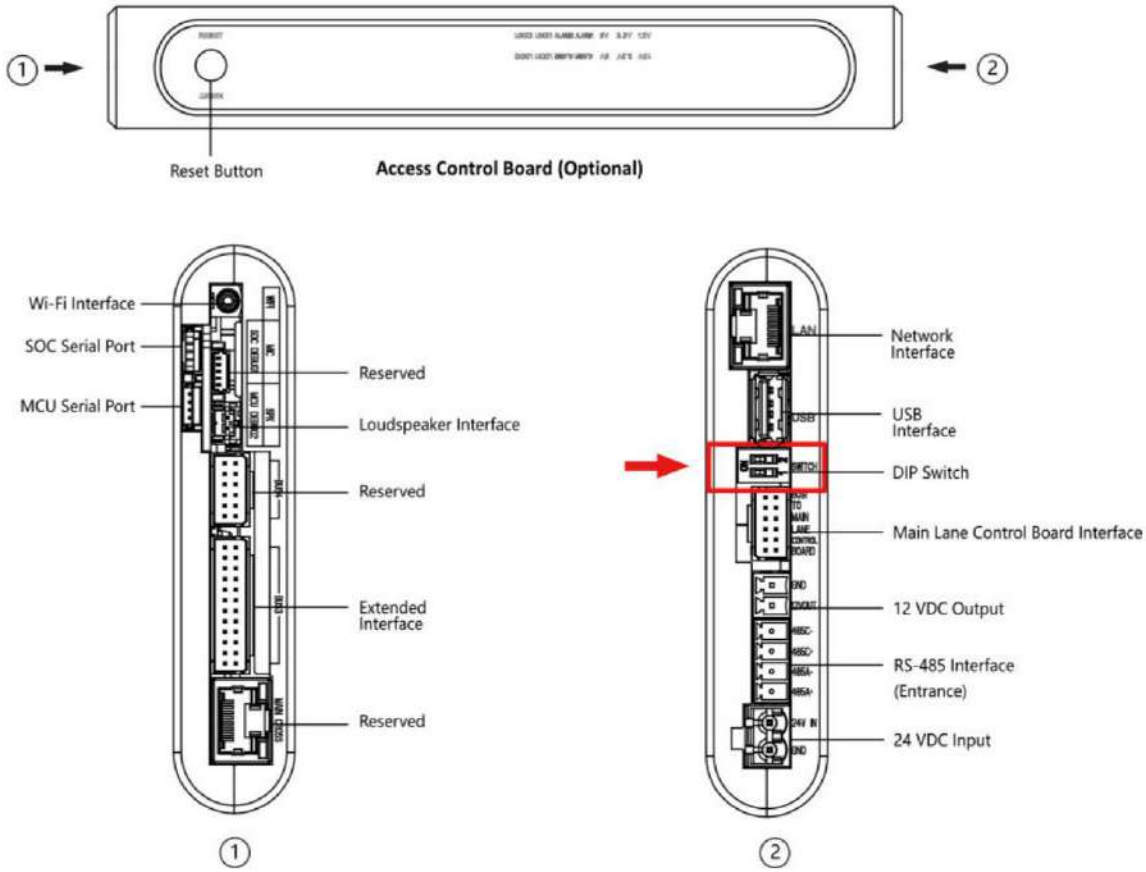


Figura 4-18 Interruptor DIP

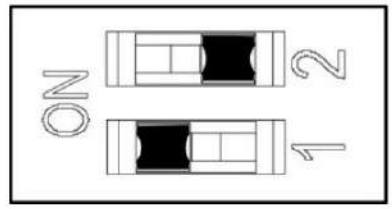


Figura 4-19 Modo de estudio

2. Ajuste la lata cerrada de la barrera.
3. Encienda el dispositivo.

   El dispositivo recordará la lata actual (cerrada) estaño) mticy
4. Encienda el dispositivo.
5. Configure los interruptores n.° 1 del interruptor DIP de 2 dígitos en la placa de interfaz extendida del usuario principal haciendo referencia a lo siguiente o

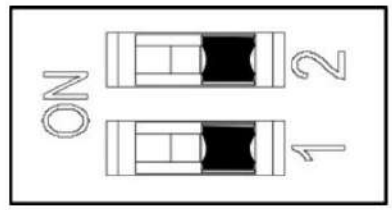


Figura 4-20 Modo normal

6. Encienda nuevamente el dispositivo.

Nota

Para obtener detalles sobre el valor y el significado del interruptor DIP, consulte Interruptor DIP .

La barrera se abrirá y volverá a la lata cerrada. En esta circunstancia, el dispositivo entra en el modo normal.

4.4.3 Emparejamiento del llavero

Empareje el llavero a través de bn o interruptor DIP.

Emparejar llavero mediante Bn

Empareje el llavero con el dispositivo a través de bn para abrir/cerrar la barrera de forma remota.

Antes de empezar

Consulte con nuestro soporte técnico o de ventas y adquiera el llavero.

Pasos

Nota

• Si el dispositivo está equipado con una placa de control de acceso, puede emparejar el llavero a través del interruptor DIP en el Solo placa de control de acceso.

• Para obtener detalles sobre bn rtin, consulte Cnn a través de Bn • Para obtener . detalles sobre el número de cnrtin y su nctin relacionado, consulte Bn Cnn norte .

• Para obtener detalles sobre el llavero rtin nrctin consulte el manual del usuario del llavero.

1. Ingrese al modo de emparejamiento del llavero.
   1) Ingrese al modo cnrtin.
   2) Establezca el número de contraseña en el Nivel 1 en 2. El dispositivo ingresará al modo de emparejamiento del llavero.
   3) Establezca el número de contraseña en el menú de Nivel 2 en 2. El dispositivo ingresará al emparejamiento del llavero. modo.
2. Mantenga presionado el botón Cerrar durante más de 10 segundos.

   El indicador del llavero se iluminará Si el emparejamiento se ha completado.

3. Salga del modo de emparejamiento del llavero.

1) Ingrese al modo cnrtin.

2) Establezca el número de contraseña en el Nivel 1 en 2. El dispositivo ingresará al modo de emparejamiento del llavero.

3) Establezca el número de contraseña en el menú de Nivel 2 en 1. El dispositivo saldrá del emparejamiento del llavero.
modo.

4. Reinicie el dispositivo para tomar do

Emparejar llavero mediante interruptor DIP (n)

Empareje el control remoto al dispositivo a través del interruptor DIP para abrir/cerrar la barrera de forma remota.

Antes de empezar

Consulte con nuestro soporte técnico o de ventas y adquiera el llavero.

Pasos

1. Encienda el rnti . 2. Coloque el

interruptor n.° 2 del interruptor DIP en la placa de control de acceso en el lado ON.

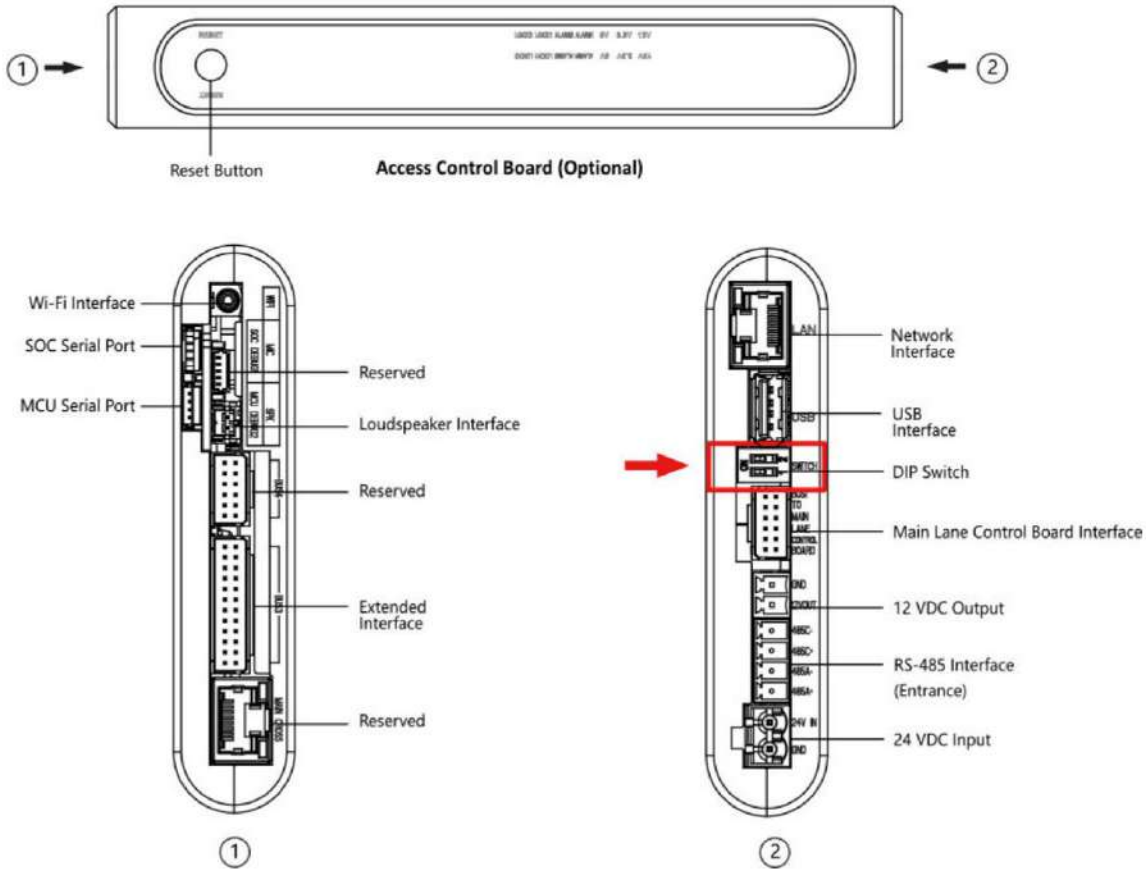


Figura 4-21 Interruptor DIP norte

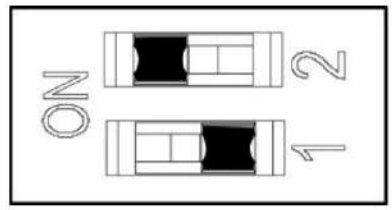


Figura 4-22 Habilitar el modo de emparejamiento del llavero

3. Encienda el rnti y entrará en el modo de emparejamiento del llavero.

4. Mantenga presionado el botón Cerrar durante más de 10 segundos.

El indicador del llavero estará 5. Coloque dos veces si se completa el emparejamiento. el interruptor n.° 2 en el lado APAGADO y reinicie el rnti para que funcione. do

Nota

- Solo un rnti puede emparejar el llavero. Si varios rnti están en modo de emparejamiento, El llavero seleccionará solo uno de ellos para emparejarlos.
- Para obtener detalles sobre el valor y el significado del interruptor DIP, consulte Interruptor DIP norte .

6. n Vaya a Sistema → Usuario → Usuario de llavero en la página de control remoto del cliente ftwr para borrar el llavero.

4.4.4 n Dispositivo

Pasos

1. Mantenga la tecla ntitin bn en el tablero de control de acceso durante 5 s.

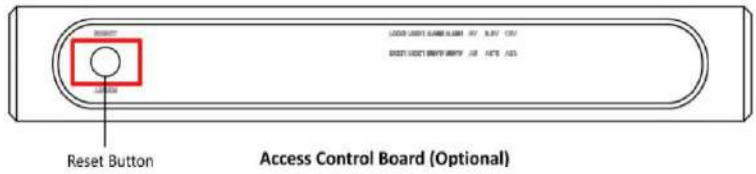


Figura 4-23 nn Bn n

2. El dispositivo comenzará a restaurarse a la configuración de norte

fábrica . 3. Cuando el proceso finalice, el dispositivo emitirá un pitido durante 3 s.

Cn

La ntin del dispositivo restaurará todos los parámetros a los valores predeterminados del n y todos los dispositivo, se eliminan los eventos.

Nota

Asegúrese de que no haya personas en el carril al encender el dispositivo.

Capítulo 5 Activacion

Debe activar el dispositivo antes de iniciar sesión. Después de encender el dispositivo, el sistema cambiará a la página de activación del dispositivo.

Se admite la actividad a través del dispositivo, la herramienta SADP y el cliente ftwr.

Los valores predeterminados del dispositivo son los siguientes:

• La dirección IP predeterminada: 192.0.0.64 • El

número de puerto predeterminado:
80 • El nombre de usuario predeterminado: admin

5.1 v a través del navegador web

Puede activar el dispositivo a través del navegador web.

Pasos

1. Ingrese la dirección IP predeterminada del dispositivo (192.0.0.64) en la barra de direcciones del navegador web y presione Ingresar.

   Nota

   Asegúrese de que la dirección IP del dispositivo y la de la computadora estén en el mismo segmento IP.

2. Cree una nueva contraseña (contraseña de administrador) y confirme la contraseña.

   Cn

   SE RECOMIENDA UNA CONTRASEÑA FUERTE: Le recomendamos encarecidamente que cree una contraseña segura de su elección (utilizando un mínimo de 8 caracteres, incluidas mayúsculas y minúsculas).

   números r y caracteres especiales) para aumentar la seguridad de su producto. Y

   Le recomendamos que restablezca su contraseña periódicamente, especialmente en el sistema de alta seguridad. Cambiar la contraseña mensual o semanalmente puede proteger su producto.

   Nota

   No se admite la configuración de caracteres que contengan admin y nimda como contraseña de ctivtin.

3. Haga clic en v.
4. Edite la dirección IP del dispositivo. Puede editar la dirección IP mediante la herramienta SADP, el dispositivo y el... cliente ftwr

5.2 v vía Web Móvil

Puede activar el dispositivo a través de la web móvil.

Pasos

1. Conéctese al punto de acceso del dispositivo con su teléfono móvil ingresando la contraseña del punto de acceso.

Nota

• Para los dispositivos nctiv, el punto de acceso está habilitado de forma predeterminada. • La contraseña del punto de acceso predeterminada es el número de serie del dispositivo.

Aparecerá la página de inicio de sesión.

2. Cree una nueva contraseña (contraseña de administrador) y confirme la contraseña.

Cn

SE RECOMIENDA UNA CONTRASEÑA FUERTE: Le recomendamos encarecidamente que cree una contraseña segura de su elección (utilizando un mínimo de 8 caracteres, incluidas mayúsculas y minúsculas).

números r y caracteres especiales) para aumentar la seguridad de su producto. Y

Le recomendamos que restablezca su contraseña periódicamente, especialmente en el sistema de alta seguridad. Cambiar la contraseña mensual o semanalmente puede proteger su producto.

Nota

No se admite la configuración de caracteres que contengan admin y nimda como contraseña de ctivtin.

3. Haga clic en v.

4. Edite la dirección IP del dispositivo. Puede editar la dirección IP mediante la herramienta SADP, el dispositivo y el... cliente ftwr

5.3 v vía SADP

SADP es una herramienta para detectar, activar y modificar la dirección IP del dispositivo a través de la LAN.

Antes de empezar

• Obtenga el SADP ftwr del disco suministrado o del sitio web c e instale el SADP wwwvnmn , según las instrucciones. • El dispositivo y la PC que ejecuta la herramienta SADP deben estar dentro de la misma subred.

Los siguientes pasos muestran cómo activar un dispositivo y modificar su dirección IP. Para obtener más información sobre la activación por lotes y la modificación de direcciones IP, consulte el Manual del usuario de SADP .

Pasos

1. Ejecute SADP ftwr y busque los dispositivos en línea.

2. Busque y seleccione su dispositivo en la lista de dispositivos en línea.

3. Ingrese la nueva contraseña (contraseña de administrador) y confirme la contraseña.

Cn

SE RECOMIENDA UNA CONTRASEÑA FUERTE: Le recomendamos encarecidamente que cree una contraseña segura de su elección (utilizando un mínimo de 8 caracteres, incluidas mayúsculas y minúsculas).

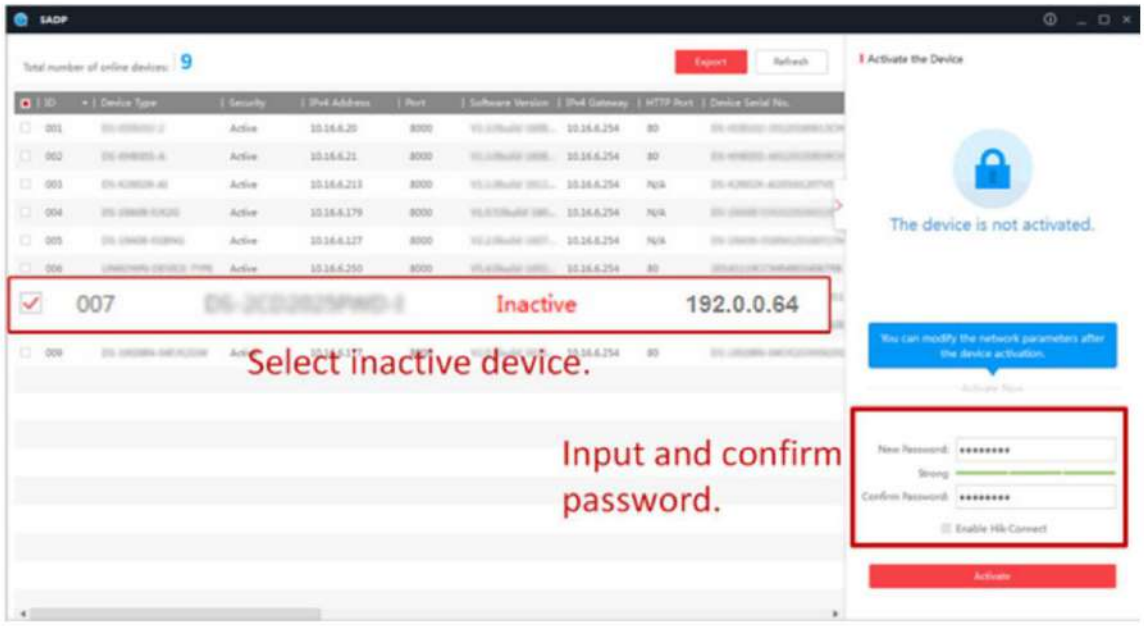
números r y caracteres especiales) para aumentar la seguridad de su producto. Y

Le recomendamos que restablezca su contraseña periódicamente, especialmente en el sistema de alta seguridad. Cambiar la contraseña mensual o semanalmente puede proteger su producto.

Nota

No se admite la configuración de caracteres que contengan admin y nimda como contraseña de ctivtin.

4. Haga clic v para iniciar activin



El estado del dispositivo pasa a ser v ftr exitoso activtin 5. Modifique la dirección IP del dispositivo.

1) Seleccione el dispositivo.
2) Cambie la dirección IP del dispositivo a la misma subred que su computadora modificando la dirección IP manualmente o marcando Habilitar DHCP.
3) Ingrese la contraseña de administrador y haga clic en Modificar para activar su dirección IP.

5.4 v Dispositivo a través del cliente iVMS-4200 ftw

Para algunos dispositivos, es necesario crear la contraseña para activarlos antes de que puedan agregarse al ftwr iVMS-4200 y funcionar correctamente.

Pasos

Nota

El dispositivo debería ser compatible con esta nctin.

1. Ingrese a la página de Administración de dispositivos.
2. Haga clic a la derecha de Administración de dispositivos y seleccione Dispositivo.
3. Haga clic en Dispositivo en línea para mostrar el área del dispositivo en línea.

   Los dispositivos en línea buscados se muestran en la lista.
4. Verifique el estado del dispositivo (que se muestra en la columna Nivel de seguridad) y seleccione un dispositivo nctiv.
5. Haga clic en v para abrir el cuadro de diálogo activtin.
6. Crea una contraseña en la contraseña y cnrm la contraseña.

   Cn

   La seguridad de la contraseña del dispositivo se puede comprobar con mticy. Le recomendamos encarecidamente que cambie la contraseña que elija (con un mínimo de 8 caracteres, incluyendo al menos tres tipos de las siguientes categorías: mayúsculas, números y caracteres especiales) para aumentar la seguridad de su producto. Le recomendamos que cambie su contraseña regularmente, especialmente en sistemas de alta seguridad. Cambiarla mensual o semanalmente puede proteger su producto.

   r minúscula

   Administración adecuada de todas las contraseñas y demás datos de seguridad del instalador y/o usuario final. n es responsabilidad de la

   Nota

   No se admite la configuración de caracteres que contengan admin y nimda como contraseña de ctivtin.
7. Haga clic en Aceptar para activar el dispositivo.

Capítulo 6 activacion a través del navegador web

6.1 Inicio de sesión

Puede iniciar sesión a través del navegador web o la consola remota del cliente ftwr

Nota

Asegúrese de que el dispositivo esté activo Para obtener información detallada sobre la actividad, consulte vn .

Iniciar sesión a través del navegador

web Ingrese la dirección IP del dispositivo en la barra de direcciones del navegador web y presione Entrar para ingresar a la página de inicio de sesión.

Ingrese el nombre de usuario y la contraseña del dispositivo. Haga clic en Iniciar sesión.

Iniciar sesión a través de CNN remoto del cliente ftw Descargue y abra

el cliente ftwr ftr agregando el dispositivo, haga clic para ingresar a la página Cnrtin.

6.2 Descripción general

Puede ver el estado de los componentes del dispositivo, el evento Rtim, el estado de la red de la nrmtin de persona, la nrmtin básica y la capacidad del dispositivo. También puede controlar la barrera de forma remota.

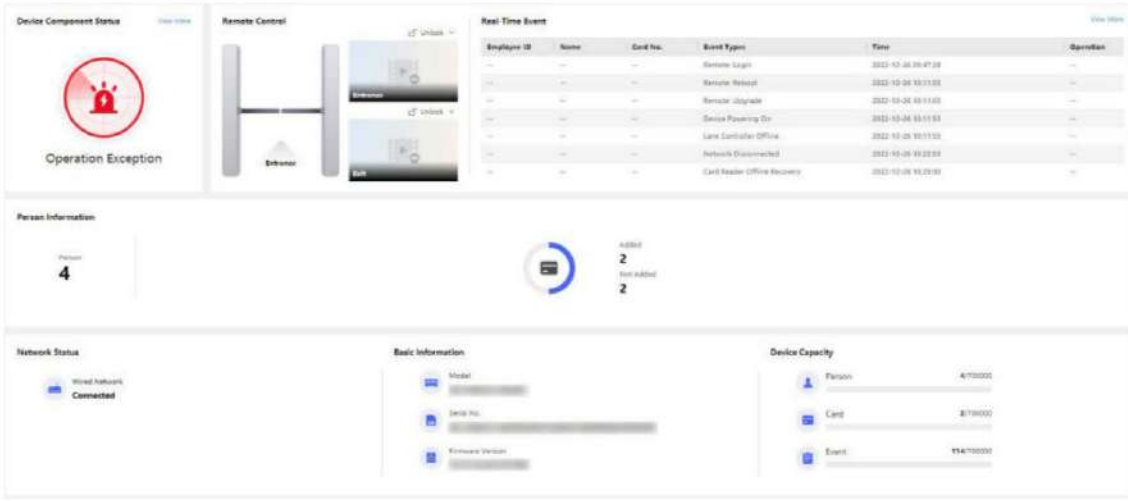


Figura 6-1 Descripción general

nctin crtin

Estado del componente del dispositivo

Puede comprobar si el dispositivo funciona correctamente. Haga clic en " Ver más" para ver el estado detallado del componente.

Mando a distancia

/ / /

La puerta se abre/se cierra/permanece abierta/permanece cerrada.

Evento en tiempo real

Puede ver el ID del empleado, el nombre, el número de tarjeta, el tipo de evento, la hora y la fecha del evento. También puede hacer clic en " Ver más" para ingresar el campo de búsqueda, incluyendo el tipo de evento, el ID del empleado, el nombre, el número de tarjeta, la hora de inicio y la hora de finalización, y hacer clic en "Buscar". Los resultados se mostrarán en el panel derecho.

Persona nmn

Puede ver los números agregados y no agregados de la persona y la tarjeta.

Estado de la red

Puede ver el estado de conexión de la red.

nmn básico

Puede ver el modelo, el número de serie y la versión rmwr.

Capacidad del

dispositivo Puede ver la capacidad de personas, tarjetas y eventos.

6.3 Gestión de personas

Haga clic en Agregar para agregar la nrmtin de la persona, incluida la crítica básica de la nrmtin.

ntictina y

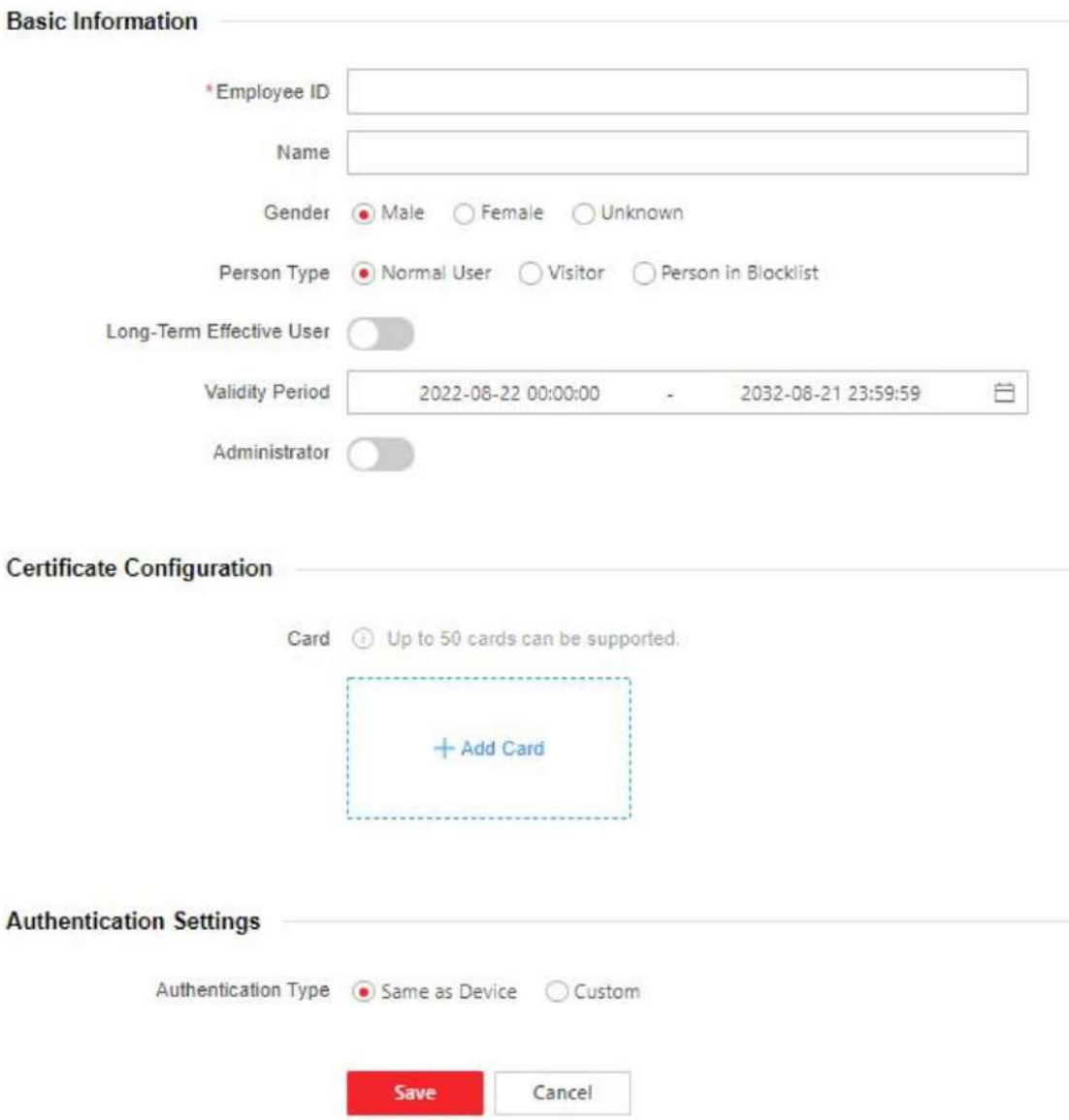


Figura 6-2 Agregar persona

Añadir nmn básico

Haga clic en Gestión de personas → Agregar para ingresar a la página Agregar persona.

Agregue la información básica de la persona, incluido el ID del empleado, el nombre de la persona y el tipo de persona.

Si selecciona Visitante como tipo de persona, puede establecer el tiempo de visita. Haga clic en Guardar para guardar la

Establecer tiempo de permiso

Haga clic en Gestión de personas → Agregar para ingresar a la página Agregar persona.

Habilite el largo plazo dentro v Usuario, o establecer Periodo de Validez y la persona solo puede tener el permiso del período de tiempo cnr según sus necesidades reales.

Haga clic en Guardar para guardar el note

Agregar tarjeta

Haga clic en Gestión de personas → Agregar para ingresar a la página Agregar persona.

Haga clic en Agregar tarjeta, ingrese el número de tarjeta y seleccione la propiedad, y haga clic en Aceptar para agregar la tarjeta.

Nota

Se pueden agregar hasta 50 tarjetas.

Haga clic en Guardar para guardar el note

nn n

Haga clic en Gestión de personas → Agregar para ingresar a la página Agregar persona.

Establezca el tipo nn como Igual que el dispositivo o Personalizado.

Haga clic en Guardar para guardar el note

Importar/Exportar datos de personas

Exportar datos de personas

Puede exportar datos de personas agregadas para realizar copias de seguridad o enviarlos a otros dispositivos.

Haga clic en "Exportar datos personales", establezca una contraseña de ncrytin y confírmela. Haga clic en "Aceptar".

Nota

• Los datos personales se descargarán a su PC. • La contraseña que configure será necesaria para ingresar los datos.

Datos personales de mn

Haga clic en Datos personales de mn y seleccione el Haga clic en Importar.

Ingrese la contraseña de ncrytin para importar y sincronizar los datos de la persona a los dispositivos.

6.4 Evento de búsqueda

Haga clic en Buscar eventos para ingresar a la página de búsqueda.

Figura 6-3 Evento de búsqueda

Ingrese el cuadro de búsqueda incluyendo el tipo de evento, el ID del empleado, el nombre, el número de tarjeta, la hora de inicio y la hora de finalización y haga clic en Buscar.

Los tipos de evento incluyen eventos de control de acceso y eventos de tarjeta de identificación. Si busca eventos de tarjeta de identificación, no necesitará ingresar el ID del empleado, el nombre ni el número de tarjeta.

Los resultados se mostrarán en el panel derecho.

6.5 Ver

6.5.1 Ver dispositivo

Haga clic en CNN → Sistema → Sistema n → nmn básico para ingresar al cnrtin página.

Puede ver el nombre del dispositivo, el idioma, el modelo, el número de serie, la versión, la entrada de E/S, la salida de E/S y la configuración local. Número RS-485.

Puede cambiar el nombre del dispositivo y hacer clic en Guardar.

Puede ver la capacidad del dispositivo, incluida la persona, la tarjeta y el evento.

6.5.2 Establecer hora

Establecer la hora del dispositivo

Haga clic en CNN → Sistema → Sistema n → Tiempo nota .

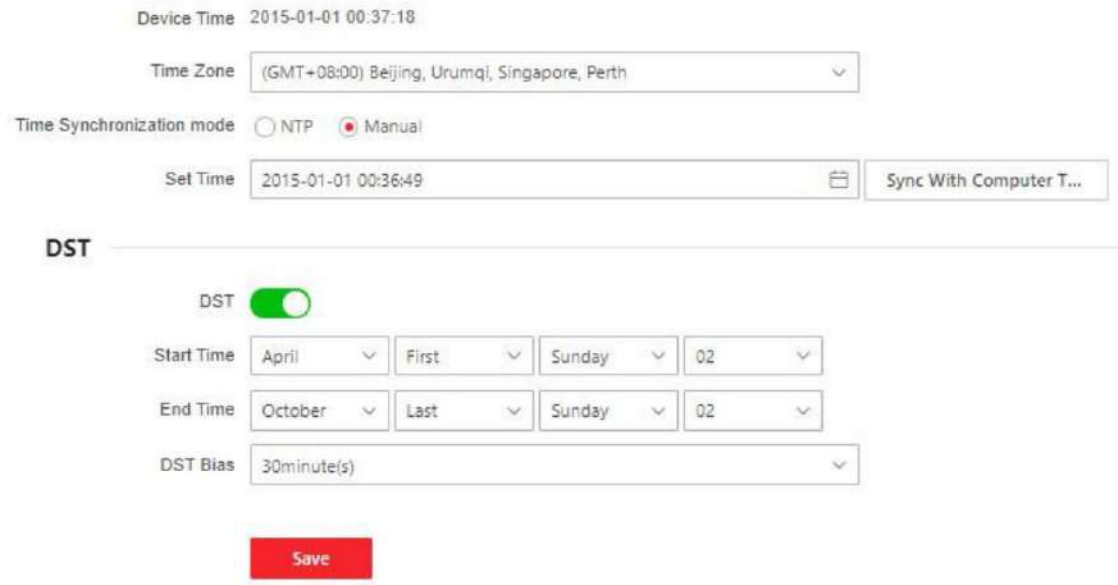


Figura 6-4 Tiempo nota

Haga clic en Guardar para guardar el n ftr la cubierta

Huso horario

Seleccione la zona horaria donde se encuentra el dispositivo en la lista desplegable.

Sincronización horaria.

Debe configurar la dirección IP, el número de puerto y el intervalo del servidor NTP.

Manual

De forma predeterminada, la hora del dispositivo debe sincronizarse manualmente. Puede configurar la hora del dispositivo manualmente o marcar la opción "Sincronizar con la hora del ordenador" para sincronizarla con la hora del ordenador. Tipo

de dirección del servidor/Dirección del servidor/Puerto NTP/Intervalo.

Puede configurar el tipo de dirección del servidor, la dirección del servidor, el puerto NTP y el intervalo.

6.5.3 Establecer el horario de verano

Pasos

1. Haga clic en CNN → Sistema → Sistema 2. Habilite el n → Tiempo norte .

horario de verano.

3. Establezca la hora de inicio y la hora de finalización del horario de verano y la hora de sesgo.

4. Haga clic en Guardar para guardar los cambios. norte

6.5.4 Cambiar la contraseña del administrador

Pasos

1. Haga clic en CNN → Administración de usuarios .

2. Haga .

clic en 3. Ingrese la contraseña anterior y cree una nueva contraseña.

4. Confirme la nueva contraseña.

5. Haga clic en Aceptar.

Cn

La seguridad de la contraseña del dispositivo se puede comprobar con mticy. Le recomendamos encarecidamente que cambie la contraseña que elija (con un mínimo de 8 caracteres, incluyendo al menos tres tipos de las siguientes categorías: mayúsculas, números y caracteres especiales) para aumentar la seguridad de su producto. Le recomendamos que cambie su contraseña r, minúscula regularmente, especialmente en sistemas de alta seguridad. Cambiarla mensual o semanalmente puede proteger su producto.

Administración adecuada de todas las contraseñas y demás datos de n es responsabilidad de la seguridad del instalador y/o usuario final.

6.5.5 Usuarios en línea

Se muestra el número de usuarios que inician sesión en el dispositivo.

Vaya a CNN → Sistema → Administración de usuarios → Usuarios en línea para ver la lista de usuarios en línea.
usuarios.

6.5.6 Ver dispositivo armado/desarmado nmn

Ver el tipo de armado del dispositivo y la dirección IP de armado.

Vaya a CNN → Administración de usuarios → Armado/desarmado nmn Puede ver el armado/desarmado ·
nrmtin del dispositivo. Haga clic en Actualizar para actualizar la página.

6.5.7 Red

Establecer parámetros TCP/IP, punto de acceso y HTTP(S).

Establecer parámetros básicos de red

Haga clic en CNN → Red → Red n → TCP/IP .

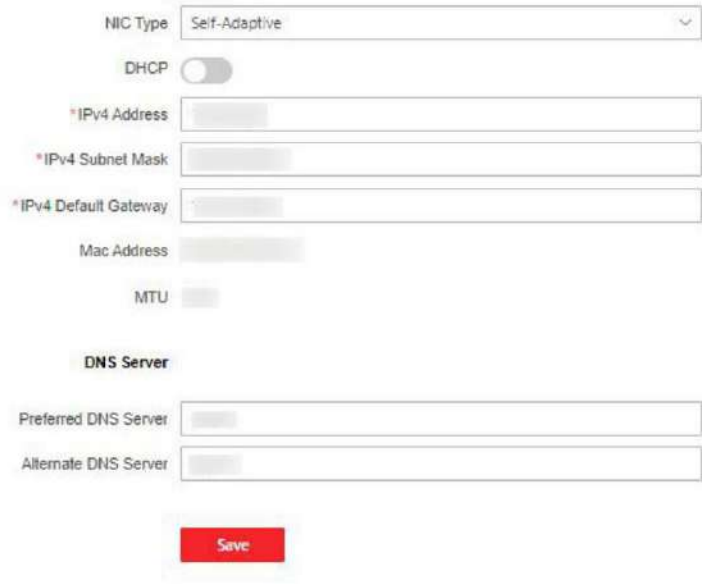


Figura 6-5 TCP/IP n Página

Establezca los parámetros y haga clic en Guardar para guardar los cambios.

Tipo de NIC

Seleccione un tipo de NIC en la lista desplegable. El valor predeterminado es Automático.

DHCP

Si desmarca nctin, debe configurar la dirección IPv4, la máscara de subred IPv4 y la IPv4 predeterminada.
puerta de enlace, dirección MAC y MTU.

Si marca nctin, el sistema asignará la dirección IPv4, la máscara de subred IPv4 y la puerta de enlace predeterminada IPv4 mticy.

Servidor DNS

Configure el servidor DNS preferido y el servidor DNS alternativo según sus necesidades reales.

Punto de acceso del dispositivo

Configurar el punto de acceso del dispositivo.

Haga clic en CNN → Red → Red n → Punto de acceso del dispositivo .

Haz clic para habilitar el punto de acceso del dispositivo. Establece el nombre y la contraseña del punto de acceso.

Haga clic en Guardar.

Establecer parámetros del puerto

Establezca los parámetros HTTP, HTTPS y HTTP Listening.

Haga clic en CNN → Red → Servicio de red → HTTP(S) .

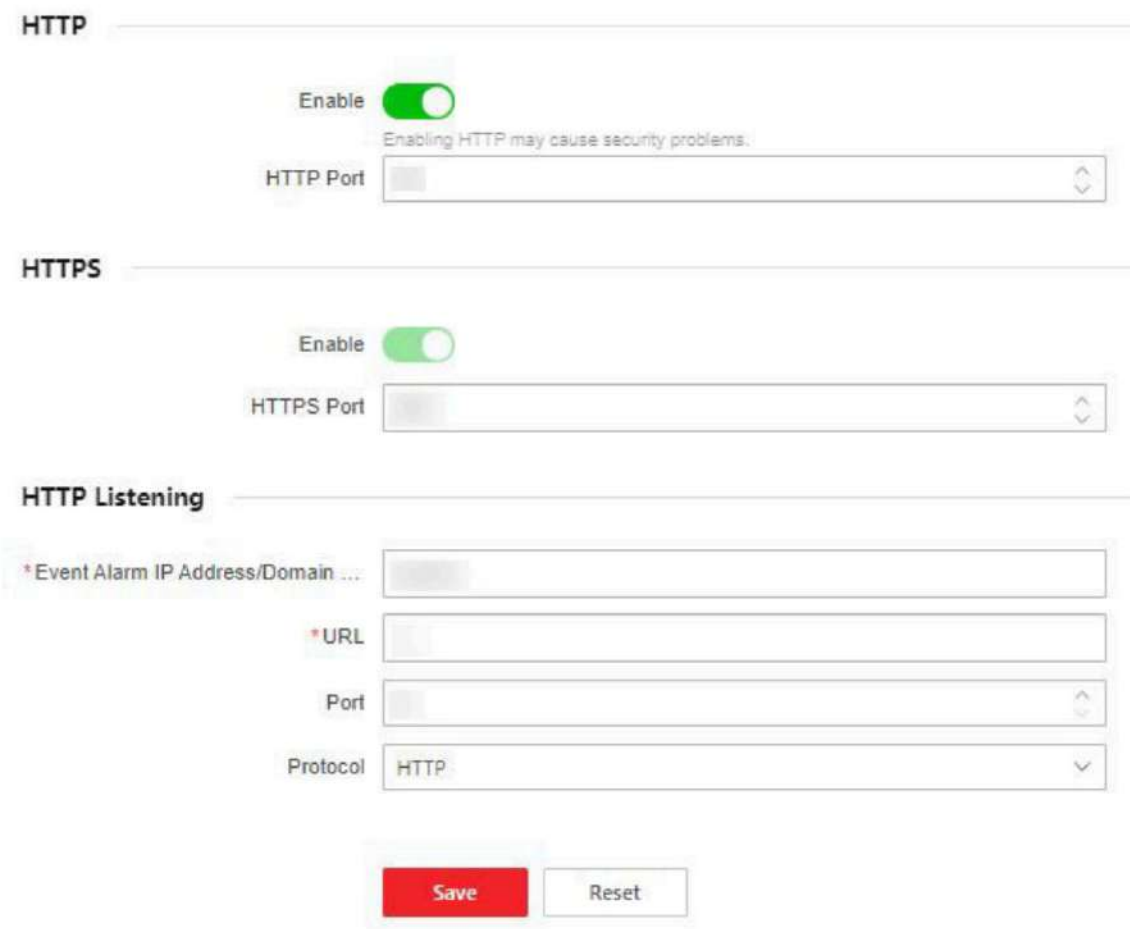


Figura 6-6 Servicio de red

HTTP

Se refiere al puerto a través del cual el navegador accede al dispositivo. Por ejemplo, si el puerto HTTP es de m a 81, debe ingresar 192006581 en el navegador para iniciar sesión.

HTTPS

Configurar HTTPS para acceder al navegador. Se requiere Crtic para acceder.

Escucha HTTP

El dispositivo puede enviar una notificación de alarma a la dirección IP o al nombre de dominio de la alarma de evento mediante el protocolo HTTP/HTTPS. Edite la dirección IP o el nombre de dominio de la alarma de evento, la URL, el puerto y el protocolo.

Nota

La dirección IP o el nombre de dominio de la alarma del evento deben ser compatibles con el protocolo HTTP/HTTPS para recibir el nrmtin de la alarma.

.

6.5.8 Establecer parámetros de audio

Establezca la calidad de la imagen, el rtin y el volumen del dispositivo.

Establecer parámetros de audio

Haga clic en CNN → Video/Audio → Audio .

Figura 6-7 Establecer parámetros de

audio Arrastre el bloque para ajustar el volumen de salida.
Haga clic en Guardar para guardar el texto en la columna.

También puede habilitar el mensaje de voz.

Nota

La nctin varía según el modelo de RN. Consulte el dispositivo para obtener más información.

6.5.9 Vinculación de eventos

Establecer ctin vinculado para eventos.

Pasos

1. Haga clic en CNN → Evento → Evento n → Enlace n para entrar a la página.

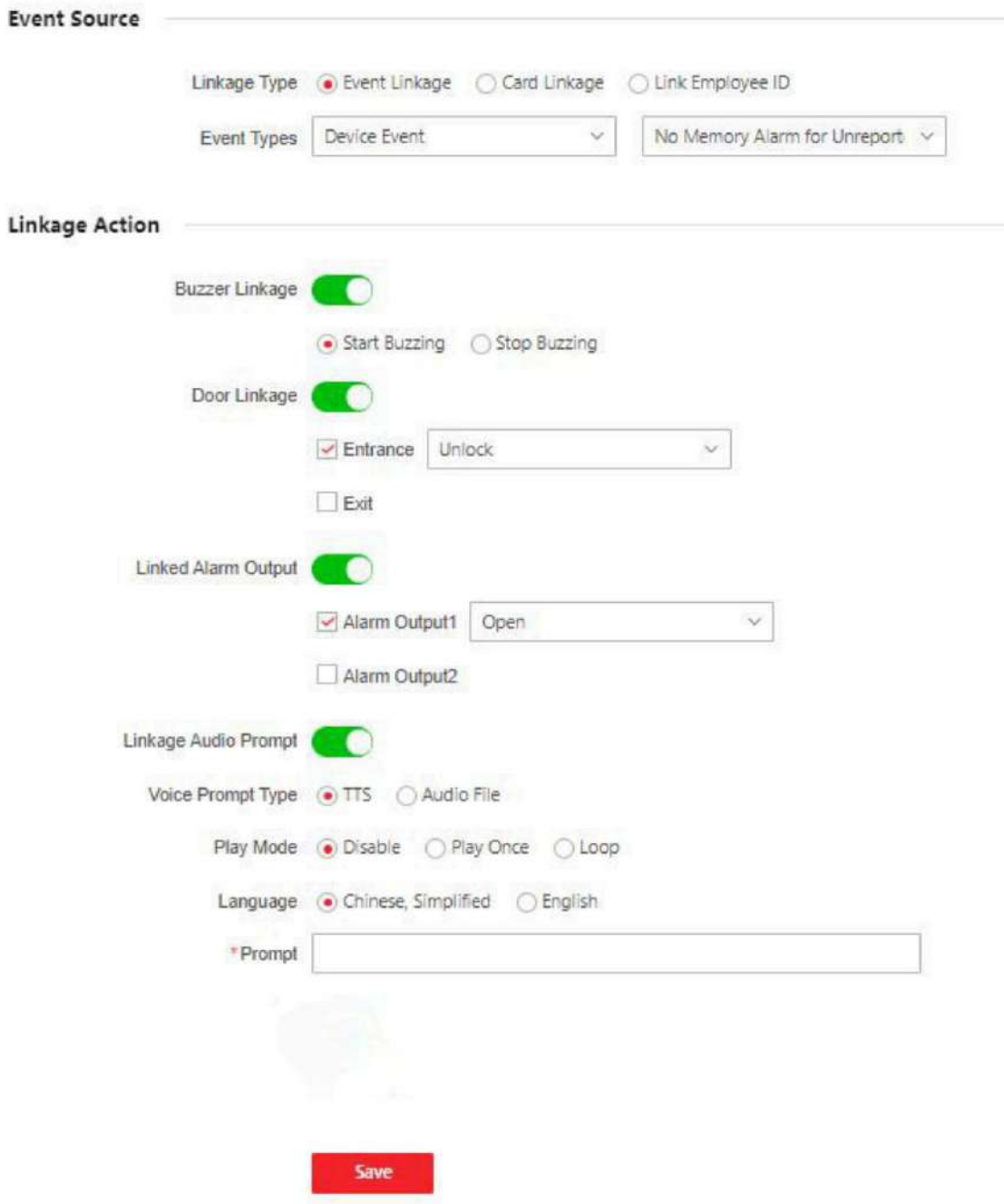


Figura 6-8 Vinculación de eventos

2. Establecer la fuente del evento.

- Si elige Tipo de vínculo como Vinculación de evento, debe seleccionar los tipos de evento en el menú desplegable.
  lista descendente.
- Si elige el Tipo de vinculación como Vinculación de tarjeta, debe ingresar el número de tarjeta y seleccionar la
  lector de tarjetas.

- Si elige el tipo de vinculación como Vinculación de ID de empleado, debe ingresar el ID del empleado y seleccionar el lector de tarjetas.

3. Establecer ctin vinculado

Zumbador vinculado

Habilite el zumbido vinculado y seleccione Iniciar zumbido o Detener zumbido para el evento de destino.

Puerta vinculada

Habilite Puerta Vinculada, marque Entrada o Salida y configure el estado de la puerta para el evento de destino.

Salida de alarma vinculada

Habilite la salida de alarma vinculada, marque la Salida de alarma 1 o la Salida de alarma 2 y configure el estado de salida de alarma para el evento de destino.

Aviso de audio vinculado

Habilite el aviso de audio vinculado y seleccione el modo de reproducción.

• Si elige TTS, debe configurar el idioma e ingresar el contenido del aviso. • Si elige Archivo de audio, debe seleccionar un audio disponible de la lista desplegable.

o haga clic en Enlace general n para agregar un nuevo audio

6.5.10 Control de acceso norte

Establecer nn parámetros

Haga clic en CNN → Control de acceso → nn n .

Nota

La nctin varía según el modelo de RN. Consulte el dispositivo para obtener más información.

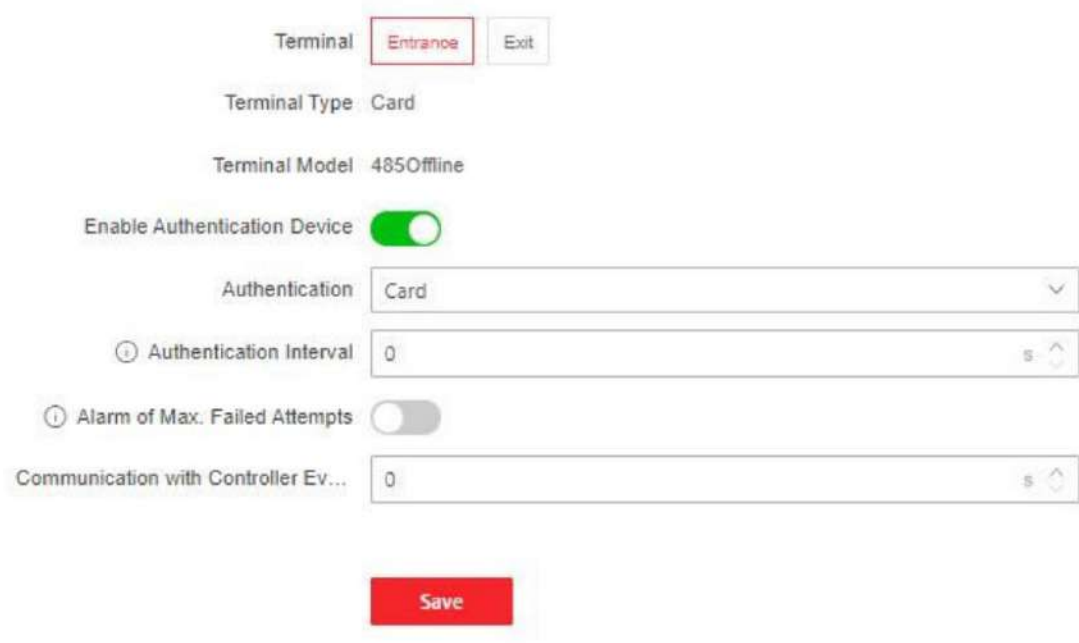


Figura 6-9 Establecer parámetros nn

Haga clic en Guardar para guardar el n ftr la cubierta

Terminal

Elija Entrada o Salida para

Tipo de terminal/modelo de terminal

Obtener terminal crtin Son de sólo lectura.

Habilitar dispositivo nn

Habilitar el ntictina nctina

nn

Seleccione un Modo anti-tictin según sus necesidades reales desde la lista desplegable.

nn Intervalo

Puedes configurar Intervalo de ntictin de la misma persona cuando ntic ntictin Lo mismo

que solo la persona una vez en el intervalo cnr. Un segundo La ntictina será

pueda fallar.

Alarma de Máx. Fallo m

Habilitar para informar una alarma cuando la lectura de la tarjeta m alcanza el valor establecido.

Máx. nn Falló m

Habilitar para informar una alarma cuando la lectura de la tarjeta m alcanza el valor establecido.

Cmmnn con el controlador cada

Cuando el dispositivo de control de acceso no puede conectarse con el lector de tarjetas durante más tiempo del establecido
El lector de tarjetas se encenderá automáticamente.

Nota

El El valor del intervalo de ntictina varía de 2 s a 255 s.

Establecer parámetros de la puerta

Haga clic en CNN → Control de acceso → Parámetros de la puerta .

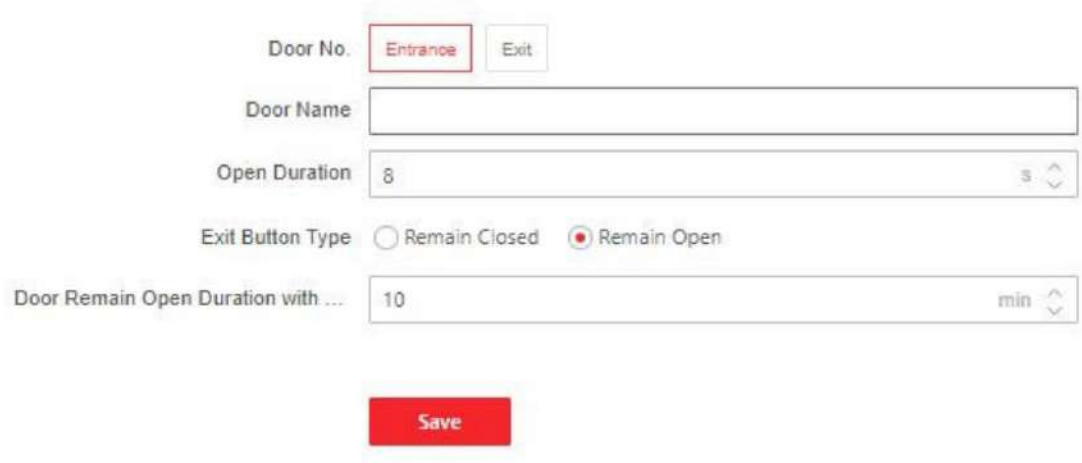


Figura 6-10 Parámetros de la puerta n Página

Haga clic en Guardar para guardar el n ftr la cubierta

Puerta N°

Seleccione Entrada o Salida para

Nombre de la puerta

Puedes crear un nombre para la puerta.

Abierto

Configurar el tiempo de desbloqueo de la puerta Si la puerta no se abre durante el tiempo establecido, se desbloqueó.
Bloqueado.

Nota

El tiempo de apertura varía entre 5 s y 60 s.

Tipo de salida Bn

Puede configurar la salida bn como Permanecer abierta o Permanecer cerrada según sus necesidades reales.

De forma predeterminada, la opción permanece abierta.

La puerta permanece abierta n con Primera Persona

Establezca la puerta abierta cuando una persona esté dentro. Si la persona está autorizada, permite que varias personas accedan a la puerta u otros ntictina ctina

Nota

El tiempo de respuesta varía entre 1 s y 1440 s.

Puerto serie norte

Establecer parámetros del puerto serie.

Pasos

1. Haga clic en CNN → Control de acceso → Puerto serie CNN .

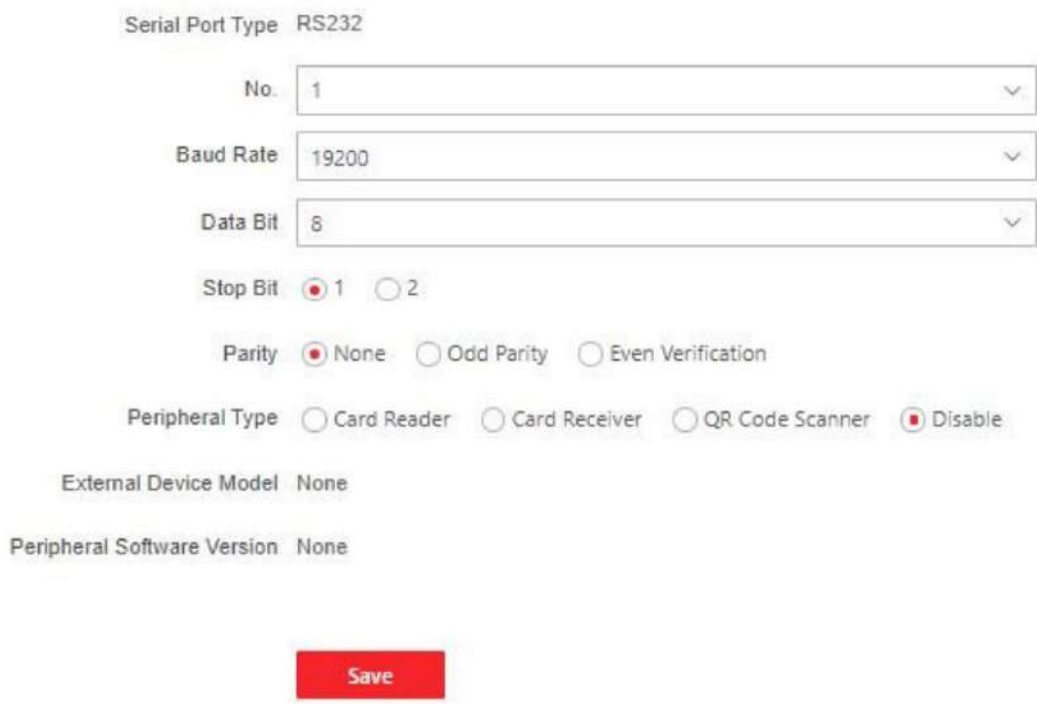


Figura 6-11 Puerto serie norte

2. Configure el N.°, la velocidad en baudios, el bit de datos, el bit de parada y la paridad.
3. Configure el tipo de periférico como Lector de tarjetas, Escáner de código QR o Desactivar.
4. Puede ver el tipo de puerto serie, el modelo del dispositivo conectado y la versión ftwr del periférico.
5. Haga clic en Guardar.

Establecer parámetros Wiegand

Puede configurar la transmisión Wiegand rctin

Pasos

Nota

Algunos modelos de dispositivos no son compatibles con esta nctin. Consulte los productos reales al conectar.

1. Haga clic en CNN → Control de acceso → Wiegand 2. Seleccione norte .
Entrada o Salida.

3. Habilite Wiegand nctin 4. La
transmisión Wiegand rctin se establece en Entrada de manera predeterminada.

Nota

Entrada: el dispositivo puede conectar un lector de tarjetas Wiegand.

5. Haga clic en Guardar para guardar el norte

Nota

Si cambia el periférico y luego guarda los parámetros del dispositivo, este se reiniciará.
mticy

Parámetros del host

Establecer contacto de puerta n y protocolo RS-485.

Pasos

1. Haga clic en CNN → Control de acceso → Parámetros de host para ingresar a la página.

2. Establecer el contacto de la puerta.

Nota

Puede configurar el contacto de la puerta como Puerta Abierta o Puerta Cerrada según sus necesidades. Por defecto, es Puerta Abierta.

3. Configure el protocolo RS-485.

4. Haga clic en Guardar.

Establecer parámetros del terminal

Establecer el modo de trabajo y la vrctin remota

Pasos

1. Haga clic en CNN → Control de acceso → Parámetros del terminal para ingresar a la página.

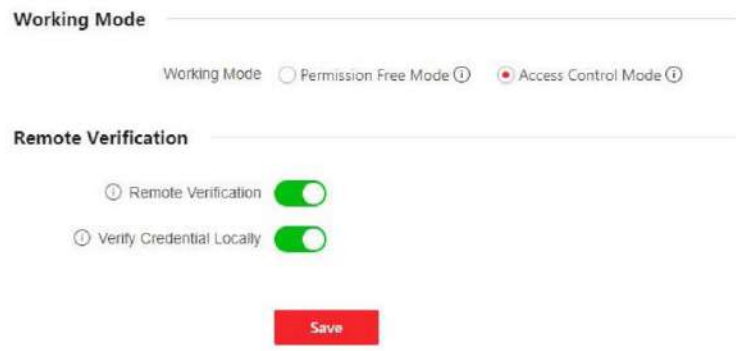


Figura 6-12 Parámetros del terminal

2. Configure el modo de funcionamiento del dispositivo.

Modo sin permisos

El dispositivo no verificará el permiso de la persona, sino solo su período de validez. Si la persona se encuentra dentro del período de validez, la barrera se abrirá.

Puede habilitar Verificar CN localmente. Al habilitar nctin, el dispositivo solo verificará el permiso de la persona sin la plantilla de programación, etc.

Modo de control de acceso

El dispositivo funciona normalmente y verificará el permiso de la persona para abrir la barrera.

3. Configurar vrctin remoto 1)

Habilitar remoto norte.

Nota

El dispositivo cargará la voluntad de la nctictin nrmtin al tfrm El tfrm persona para juzgar si abre o no la barrera. 2)

n Habilitar Verificar Cn Localmente.

Nota

Al habilitar nctin, el dispositivo solo verificará el permiso de la persona sin la plantilla de programación, etc.

4. Haga clic en Guardar para completar la configuración del parámetro del terminal. norte

6.5.11 n

Parámetros básicos

Establecer parámetros básicos de rnti.

Pasos

1. Haga clic en CNN → n → Básico 2. Vea el tipo de dispositivo, n para entrar a la página.

el modelo del dispositivo y el estado de funcionamiento.

3. Configure el material de la barrera, el ancho del carril, la altura de la barrera, la velocidad de apertura de la barrera y el cierre de la barrera.

Velocidad.

4. Establezca el modo de paso.

- Si elige Paso General, puede seleccionar el estado de la barrera para la entrada y salida de

la lista desplegable.

Nota

Si configura el modo sin barreras, la barrera permanecerá abierta y se cerrará cuando falle. ntictina

- Si elige Programación semanal, puede establecer una programación semanal para las barreras de entrada y salida.

5. Haga clic en Guardar.

llavero

Establecer parámetros del llavero.

Pasos

1. Haga clic en Cnn → n → Keyfob para ingresar a la página.

Figura 6-13 Llavero 2.

Establezca el modo de trabajo como Uno a uno o Uno a muchos.

3. Añade el llavero.

1) Haga clic en Agregar y aparecerá la ventana para agregar el llavero.

2) Ingrese el nombre y el número de serie.

3) Marque para habilitar el permiso Permanecer abierto según sus necesidades reales.

4) Haga clic en Aceptar para agregar el llavero.

n Seleccione un llavero y haga clic en Eliminar para eliminarlo. 4.

5. Haga clic en Guardar.

Detector de infrarrojos

Establecer detector de infrarrojos.

Pasos

1. Haga clic en Cnn → n → Detector IR para ingresar a la página.

Figura 6-14 Detector de infrarrojos

2. Configure el modo de entrada y salida nctiv como Activado único o Activado simultáneamente.

3. Configure el modo de detector de infrarrojos personalizado.

Habilitar el modo de emergencia IR

Si algunos rayos infrarrojos no funcionan correctamente, puede protegerlos para restablecer el carril. Sin embargo, este rayo podría impactar a una persona y causarle lesiones.

Habilitar nn personalizado para el cierre de puertas

La función ntinc para el cierre de puertas indica que la barrera no se cerrará si el dispositivo detecta a una persona en el carril. La barrera solo se cerrará cuando la persona salga del carril. Si activa la función ntinc, puede bloquear partes de los rayos infrarrojos para el cierre de la barrera con antelación. Sin embargo, esta función podría golpear a una persona y causarle lesiones.

4. Haga clic en Guardar.

Gente CNN

Establecer personas cntin.

Pasos

1. Haga clic en CNN → n → People CNN para ingresar a la página.

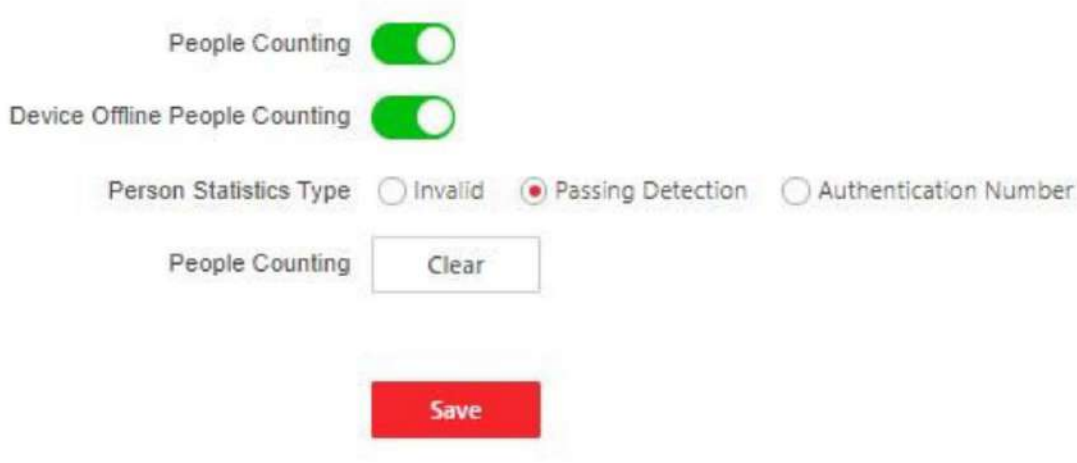


Figura 6-15 People CNN 2. Marque para

habilitar People CNN.

3. Habilite Device ffln People Cnn según sus necesidades reales.

4. Seleccione el tipo de CNN de personas como no válido, pasando el número n o nn. n Haga clic en borrar para borrar todos los CNN de personas nrmtin 5.

Establecer color del indicador

Establezca el color de los indicadores.

Pasos

1. Haga clic en Cnn → n → Luz 2. Configure el color de la luz n para entrar a la página.

para el indicador de estado del carril.

1) Configure el brillo de la luz como Automático o Brillo fijo. Si elige Brillo fijo, puede arrastrar el bloque o ingrese el valor para ajustar el brillo de la luz manualmente.

2) Establezca el color de luz de nctiv prohibido y de paso de autenticación.

3. Establecer el color de la luz de barrera.

1) Marque para habilitar la Luz encendida en modo de espera según sus necesidades reales.

2) Establezca el color de la luz de barrera.

4. Haga clic en Guardar.

Otro norte

Establecer otros parámetros.

Pasos

1. Haga clic en CNN → n → Otro 2. Configure la salida de alarma n para entrar a la página.

norte.

Nota

El rango de salida de alarma rtin va de 0 s a 3599 s.

3. Establecer la unidad de temperatura.

4. Marque para habilitar la opción No abrir la barrera cuando el carril no esté despejado.

5. Arrastre el bloque o ingrese el valor para ajustar el brillo del tablero de luz.

6. Configure el timbre de la alarma para que suene durante el retardo de cierre de la puerta y la intrusión durante el tiempo de permanencia.
rtin e IR obstruidos rtin 7. Marque para

habilitar el modo de memoria según sus necesidades reales.

Nota

Se permite el uso de tarjetas MTI para el paso de personas MTI al habilitar el modo de memoria. Cuando el número de personas que pasan supera el número de tarjetas MTI, o si pasa la última persona sin que nadie pase dentro de la puerta abierta, la puerta se cerrará. 8. Seleccione el modo de control.

Modo ft

La barrera se cerrará después de que la persona haya pasado a través de la barrera cuando haya seguimiento, acceso forzado, etc.

Modo Guardia

La barrera se cerrará inmediatamente cuando haya 9. Establezca el tipo acceso forzado al estaño, etc.
de entrada r.

10. Haga clic para habilitar la prueba automática del motor y elija el carril principal o el carril secundario para iniciar el motor.
lata

11. Haga clic en Guardar.

6.5.12 Tarjeta norte

Establecer la seguridad de la tarjeta

Haga clic en CNN → Tarjeta n → Tipo de tarjeta para ingresar n página.

Establezca los parámetros y haga clic en Guardar.

Habilitar tarjeta NFC

Para evitar que el teléfono móvil acceda a los datos del control de acceso, puede desactivar la tarjeta NFC para aumentar el nivel de seguridad de los datos.

Habilitar tarjeta M1

Habilitar la tarjeta M1 y La tarjeta ntictin by rntin M1 está disponible.

Tarjeta M1 nyn
Sector

La tarjeta M1 ncrytin puede mejorar el nivel de seguridad. Habilite ntictina ncrytin y configure el sector ncrytin. El sector 13 está cifrado por defecto. Se recomienda cifrar el sector 13.

Habilitar tarjeta EM

Habilitar tarjeta EM y La tarjeta EM ntictin by rntin está disponible.

Nota

Si el lector de tarjetas periféricas admite la tarjeta EM rntin, también se admite nctin.

Habilitar/deshabilitar la tarjeta EM nctin

Habilitar tarjeta CPU

Habilitar la tarjeta CPU y La tarjeta CPU ntictin de rntin está disponible.

Contenido de lectura de la tarjeta CPU

ftr habilita la lectura del contenido de la tarjeta CPU nctin el dispositivo puede leer el contenido de la tarjeta CPU.

Habilitar la tarjeta FeliCa

El dispositivo puede leer los datos de la tarjeta FeliCa al habilitar la tarjeta FeliCa nctin

Establecer parámetros de la tarjeta nn

Establezca el contenido de lectura de la tarjeta cuando ntic A través de tarjeta en el dispositivo.

Ir a CNN → Tarjeta n → N.º de tarjeta nn n .

Seleccione una tarjeta Modo anti-tictin y habilite el número de tarjeta invertido según sus necesidades. Haga clic en Guardar.

6.5.13 Establecer parámetros de privacidad

Establecer el tipo de almacenamiento de eventos.

Vaya a CNN → Seguridad → Privacidad. El tipo de norte almacenamiento de eventos es vrwrtin por defecto. El 5% de los primeros eventos se eliminará cuando... El sistema detecta que los eventos almacenados han superado el 95% del espacio total.

6.5.14 Programación rápida

Personalice el contenido de audio de salida cuando ntictin tuvo éxito y fracasó.

Pasos

1. Haga clic en CNN → Preferencias → Programación de avisos .

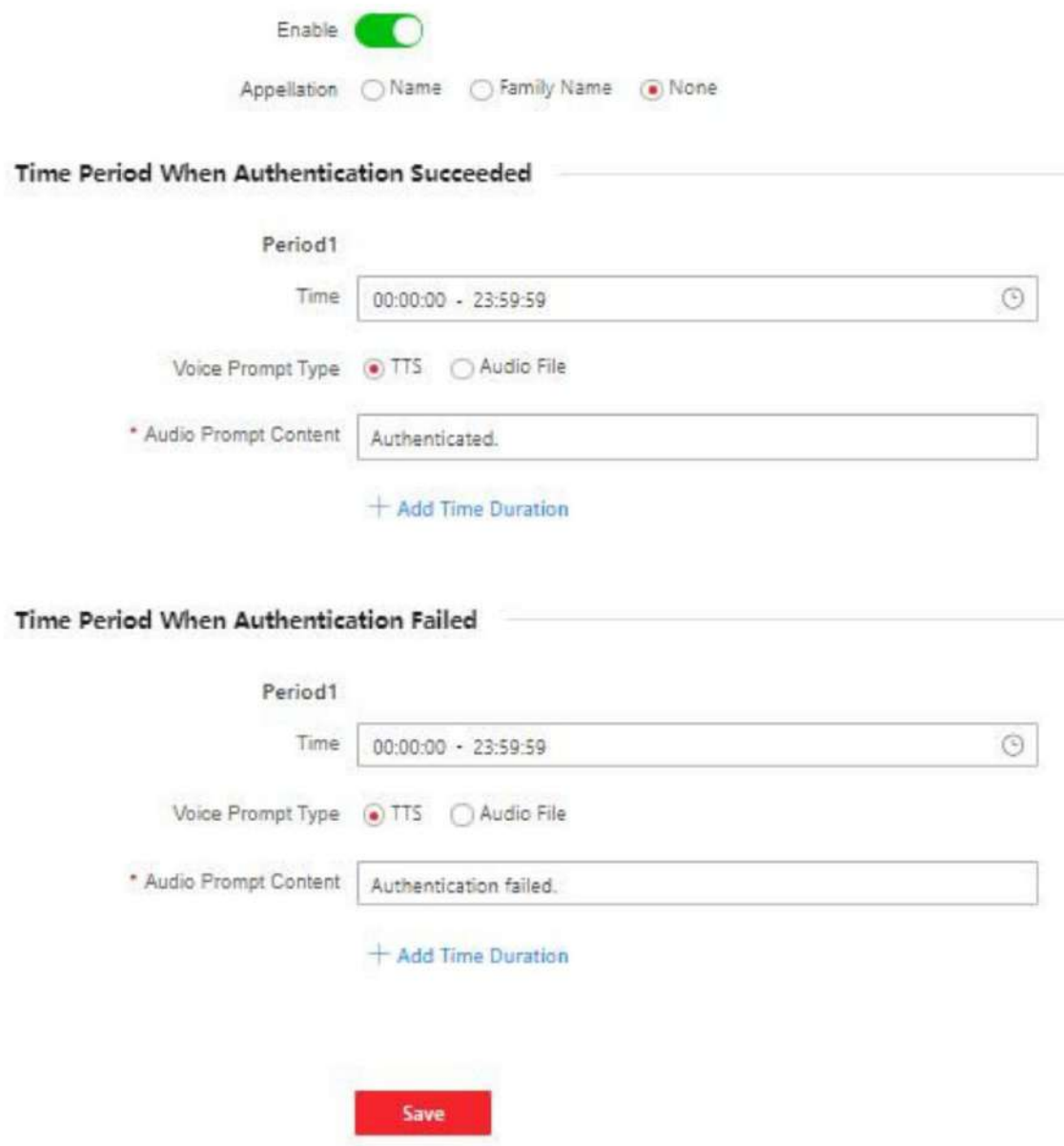


Figura 6-16 Personalizar el contenido de audio

2. Seleccione el horario.

3. Habilitar nctin

4. Establezca estaño

el 5. Establezca el período de tiempo ntictin tuvo éxito.

cuando 1) Haga clic en norte.

Agregar tiempo 2) Establezca el tiempo rtin

Nota

Si ntictin tiene éxito en el cnr tim rtin el dispositivo transmitirá el contenido cnr.

3) Establezca el contenido de audio.

TTS

Si elige TTS, debe configurar el idioma e ingresar el contenido del mensaje.
Éxito de ntictin.

Archivo de audio

Si elige audio o hace clic Debes seleccionar un audio disponible de la lista desplegable en Administración de archivos de audio para agregar uno nuevo

Nota

El audio El formato debe ser wav y el tamaño debe ser inferior a 200 KB.

4) n Repita los pasos 1 a 3.

5) n Haga clic para eliminar el cnr tim rtin

6. Establezca el tiempo rtin cuando 1) La ntictina falló.

Haga clic en Agregar.

2) Establezca el tiempo rtin

Nota

Si La ntictin ha fallado en el cnr tim rtin, el dispositivo transmitirá el contenido cnr.

3) Establecer el contenido de audio.

TTS

Si elige TTS, debe configurar el idioma e ingresar el contenido del mensaje.
insuficiencia de tictina.

Archivo de audio

Si elige audio o hace clic Debes seleccionar un audio disponible de la lista desplegable en Administración de archivos de audio para agregar uno nuevo

Nota

El formato de audio debe ser wav y el tamaño debe ser inferior a 200 KB.

4) n Repita los subpasos 1 a 3.

5) n Haga clic para eliminar el cnr tim rtin

7. Haga clic en Guardar para guardar el

6.5.15 Actualización y mantenimiento

Reiniciar el dispositivo, restaurar los parámetros del dispositivo y actualizar la versión del dispositivo.

Reiniciar el dispositivo

Haga clic en Mantenimiento y seguridad → Mantenimiento → Reiniciar .
Haga clic en Reiniciar para reiniciar el dispositivo.

Actualizar

Haga clic en Mantenimiento y seguridad → Mantenimiento → Actualizar .
Seleccione un tipo de actualización en la lista desplegable. Haga clic y seleccione la actualización desde su PC local. Haga clic en Actualizar para iniciar la actualización.

Nota

No encienda durante la actualización.

Restaurar parámetros

Haga clic en Mantenimiento y seguridad → Mantenimiento → Copia de seguridad y restablecimiento .

Restaurar todo

Todos los parámetros se restaurarán a los valores de fábrica. n Debe activar el dispositivo antes uso.

Restaurar

El dispositivo se restaurará al nrmtin predeterminado n excepto los parámetros de red y el usuario

Parámetros de importación y exportación Haga clic en Mantenimiento y seguridad → Mantenimiento → Copia de seguridad y restablecimiento .

Exportar

Haga clic en Exportar para exportar los parámetros del dispositivo.

Nota

Puede importar los parámetros del dispositivo exportados a otro dispositivo.

Importar

Haga clic y seleccione el Para importar. Haga clic en Importar para iniciar la importación.

6.5.16 Depuración del dispositivo

Puede configurar los parámetros de depuración del dispositivo.

Pasos

1. Haga clic en Mantenimiento y seguridad → Mantenimiento → Depuración del dispositivo .
2. Puede configurar los siguientes parámetros.

Habilitar SSH

Para aumentar la seguridad de la red, desactive el servicio SSH. El cnrtin solo se usa para depurar el dispositivo para profesionales.

Registro de

impresión Puede hacer clic en Exportar para exportar el registro.

6.5.17 Estado del componente

Puede ver el estado del carril principal y del carril secundario.

Estado del carril principal

Componente del dispositivo

Puede ver el estado del tablero de control de acceso, el tablero de control de carril, el tablero de interfaz extendida del usuario y el tablero indicador de modo de adelantamiento.

Periférico

Puede visualizar el estado del lector de tarjetas RS-485 y la entrada de manipulación.

TemperaturaPuedes

ver la temperatura del pedestal.

Movimiento

Puede ver el estado de funcionamiento del codificador del motor.

Estado del subcarril

Componente del dispositivo

Puede ver el estado del tablero de control de carril, el tablero indicador de modo de adelantamiento y el adaptador IR superior.

Periférico

Puede visualizar el estado del lector de tarjetas RS-485, del receptor de tarjetas RS-232 y de la entrada de manipulación.

Movimiento

Puede ver el estado de funcionamiento del codificador del motor.

Otros

Modo de pase

Puede ver el modo de entrada y salida.

Estado del detector de infrarrojos

Puede ver el estado de cada par de sensores de haz infrarrojo.

Estado de entrada y salida Puede

ver el estado de la entrada/salida de evento, entrada/salida de alarma y alarma.

Otro estado

Puede visualizar el estado de la barrera y del módulo receptor del llavero.

6.5.18 Consulta de registro

Puede buscar y ver los registros del dispositivo.

Vaya a Mantenimiento y seguridad → Mantenimiento → Registro .

Establezca el tipo principal y secundario del registro. Establezca la hora de inicio y la hora de finalización de la búsqueda.
Haga clic en Buscar.

Los resultados se mostrarán a continuación, incluyendo el n.°, el tiempo, el tipo principal y el tipo secundario.
el número de canal, el número de usuario local/remoto, la IP del host remoto, etc.

6.5.19 C Gestión

Ayuda a administrar la crítica del servidor/cliente y la crítica de la CA.

Nota

El nctin solo es compatible con ciertos modelos de dispositivos.

Crear e instalar un C autofirmado

Pasos

1. Vaya a Mantenimiento y seguridad → Seguridad → C 2. En el Gestión .
área Archivos C , seleccione un C 3. Haga clic en Escriba de la lista desplegable.
Crear.

4. Entrada crítica nrmtin

5. Haga clic en Aceptar para guardar e instalar el crítico.

La crítica creada se muestra en C La crítica se Área de detalles .
guardará automáticamente

6. Descargue la crítica y guárdela en una solicitud. 7. Envíe la en la computadora local.
solicitud a una autoridad de crítica para su firma.

8. Importar el crítico firmado

1) Seleccione un tipo de crítico en el área Importar contraseñas y seleccione un crítico del local.
y haga clic en Instalar.

2) Seleccione un tipo crítico en la Cmdte. Importar Cmdte. área y seleccione un crítico
desde el local y haga clic en Instalar.

Instalar otro C autorizado

Si ya tienes un crítico autorizado (no creado por el dispositivo), puedes importarlo al dispositivo directamente.

Pasos

1. Vaya a Mantenimiento y seguridad → Seguridad → C 2. Gestión . áreas,
En Importar contraseñas e Importar Cmmnn C seleccionar tipo crítico
y subir critic 3. Haga
clic en Instalar.

Instalar CA C

Antes de comenzar

Prepare una crítica de CA con antelación.

Pasos

1. Vaya a Mantenimiento y seguridad → Seguridad → C 2. Gestión .
Cree un ID en la CA de importación C área.

 Nota

El ID de crítico de entrada no puede ser el mismo que el de xtin.

3. Sube un crítico. 4. Del local.
Haz clic en Instalar.

Capítulo 7 Conecte el dispositivo a través del móvil Navegador

7.1 Inicio de sesión

Puede iniciar sesión a través del navegador móvil.

Nota

Asegúrese de que el dispositivo esté activo

Puede iniciar sesión mediante los siguientes métodos:

• Si el punto de acceso del dispositivo está desactivado, asegúrese de que su teléfono móvil y el dispositivo estén conectados a la misma red. Coloque el teléfono en el área NFC y se abrirá la página de inicio de sesión. Si el punto de acceso del dispositivo está activado, coloque el teléfono en el área NFC e ingrese el nombre y la contraseña.

• Cuando el punto de acceso del dispositivo está habilitado, puede conectarse al punto de acceso del dispositivo y a la página de inicio de sesión. aparecerá.

Ingrese el nombre de usuario y la contraseña del dispositivo. Haga clic en Iniciar sesión. • Cuando el punto de acceso del dispositivo esté habilitado, coloque su teléfono en el área NFC y el nombre y la contraseña Se obtendrá la contraseña del punto de acceso del dispositivo mticy

Nota

Sistema Android Se recomienda rtin NFC nctin. El sistema IOS no es compatible.

7.2 Descripción general

Puede ver el estado del dispositivo, realizar control remoto, etc.

Puede ver el estado del dispositivo. Si hay xctin, puede tocar para ver los detalles del componente.

Puede controlar la barrera de forma remota tocando los íconos.

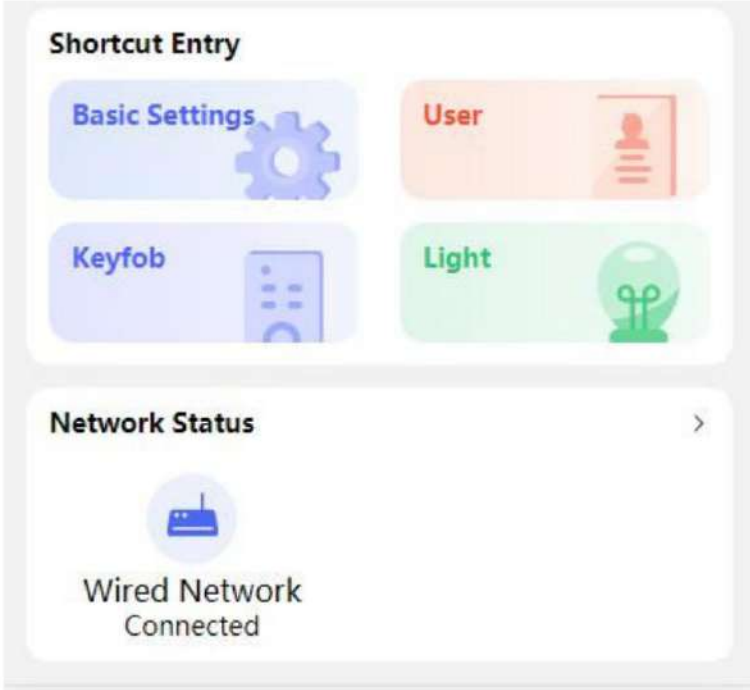


Figura 7-1 Entrada de acceso directo y estado de la red

Puede tocar para ingresar rápidamente a la página Página n, página de usuario, página de llavero, página de luz y página de red básica.

7.3 CNN

7.3.1 norte Parámetros básicos

Puede configurar los parámetros básicos del rnti

Toque Básico n de la entrada de acceso directo en la página de descripción general.

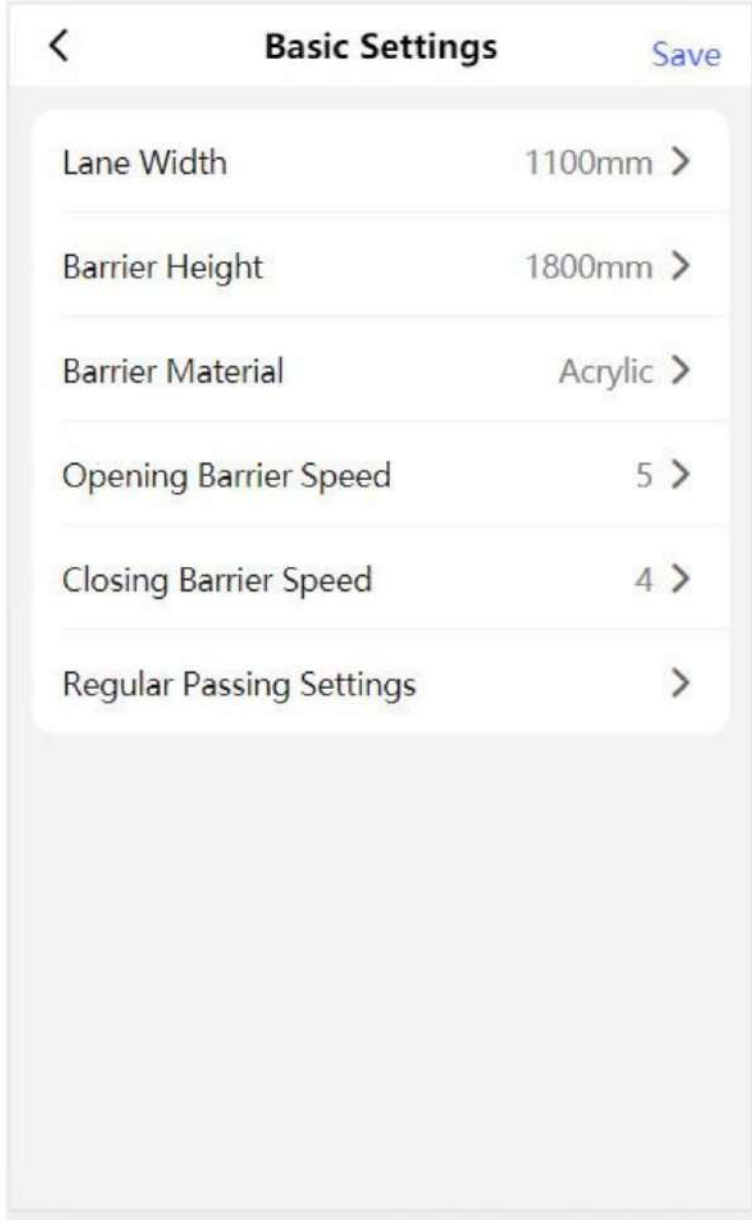


Figura 7-2 n Parámetros básicos

Establecer el ancho del carril, la altura de la barrera, la altura de la barrera, la velocidad de apertura de la barrera y la velocidad de cierre de la barrera.

Establecer el modo de paso regular para la entrada y la salida.

Pulse Guardar.

7.3.2 Gestión de usuarios

Puede agregar, editar, eliminar y buscar usuarios a través del navegador web móvil.

Pasos

1. Pulse Usuario para ingresar n página.

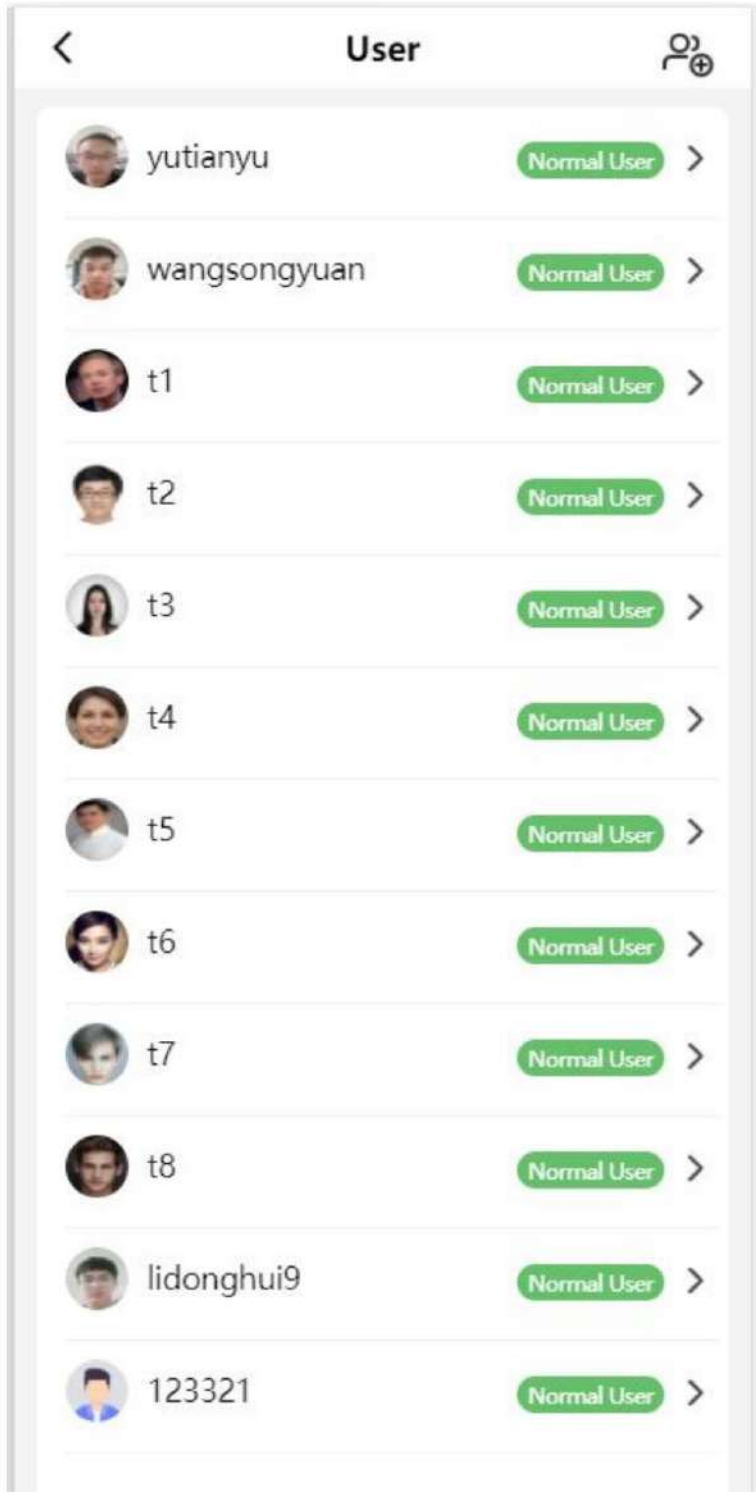


Figura 7-3 Agregar usuario

2. Agregar usuario.

1) Toque

2) Establezca los siguientes parámetros.

ID de empleado :

Ingrese el ID de empleado. El ID de empleado no puede tener más de 32 caracteres. Puede ser una combinación de mayúsculas y minúsculas. r y números.

Nombre

Ingrese su nombre. El nombre admite números, mayúsculas y minúsculas en inglés, y caracteres. Se recomienda que el nombre tenga un máximo de 32 caracteres.

Rol de usuario

Seleccione su rol de usuario.

Tarjeta

Agregar tarjeta. Pulse Tarjeta → Agregar tarjeta. , Ingrese el número de la tarjeta y seleccione el tipo de tarjeta.

3) Pulse Guardar.

3. Toque el usuario que necesita ser editado en la lista de usuarios para editar el nrmtin

7.3.3 Llavero norte

Toque el llavero de la entrada de acceso directo en la página de descripción general.

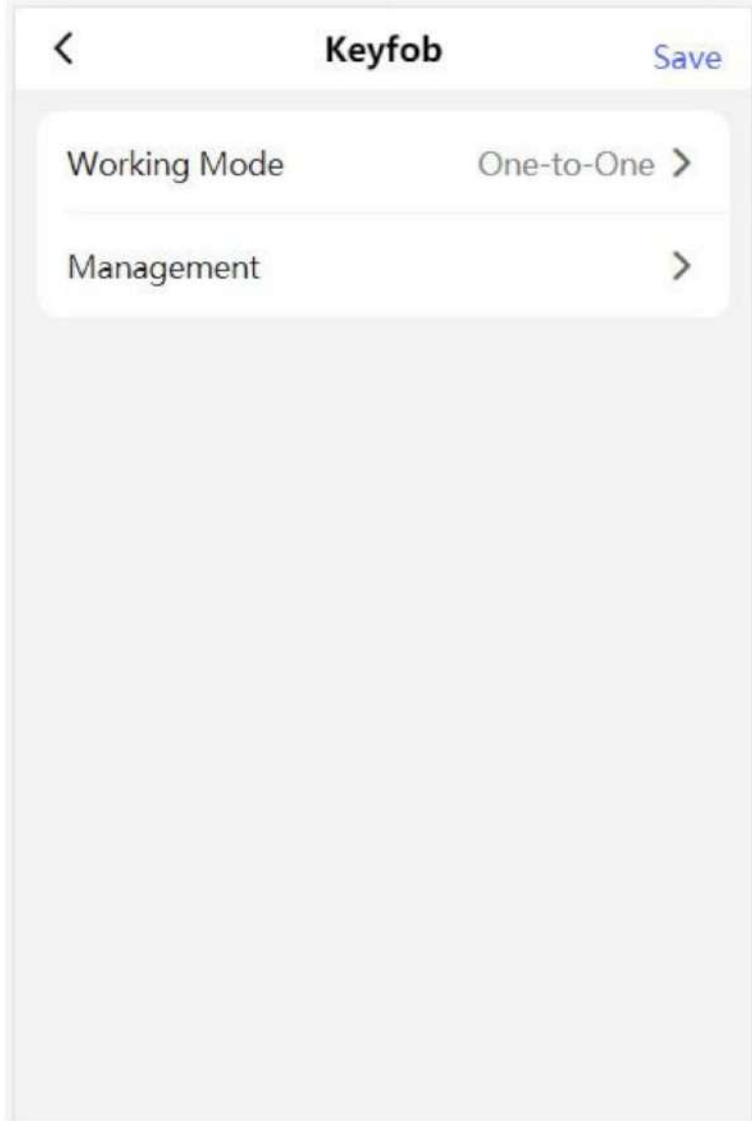


Figura 7-4 Llavero

Establezca el modo de trabajo como Uno a uno o Uno a muchos.

Pulse "Administración" para acceder a la página. Pulse "+" para añadir un llavero. Configure el nombre, el número de serie y el permiso para mantenerlo abierto.

7.3.4 Luz

Toque la luz de la entrada de acceso directo en la página de descripción general.

Indicador de estado del carril

Figura 7-5 Indicador de estado del carril

El brillo de la luz está configurado en Manual por defecto. Introduzca el valor para ajustarlo manualmente.

Establecer el color de la luz para nctivrmn abierto, permanecer cerrado y modo controlado/sin barreras rctivy

Luz de barrera

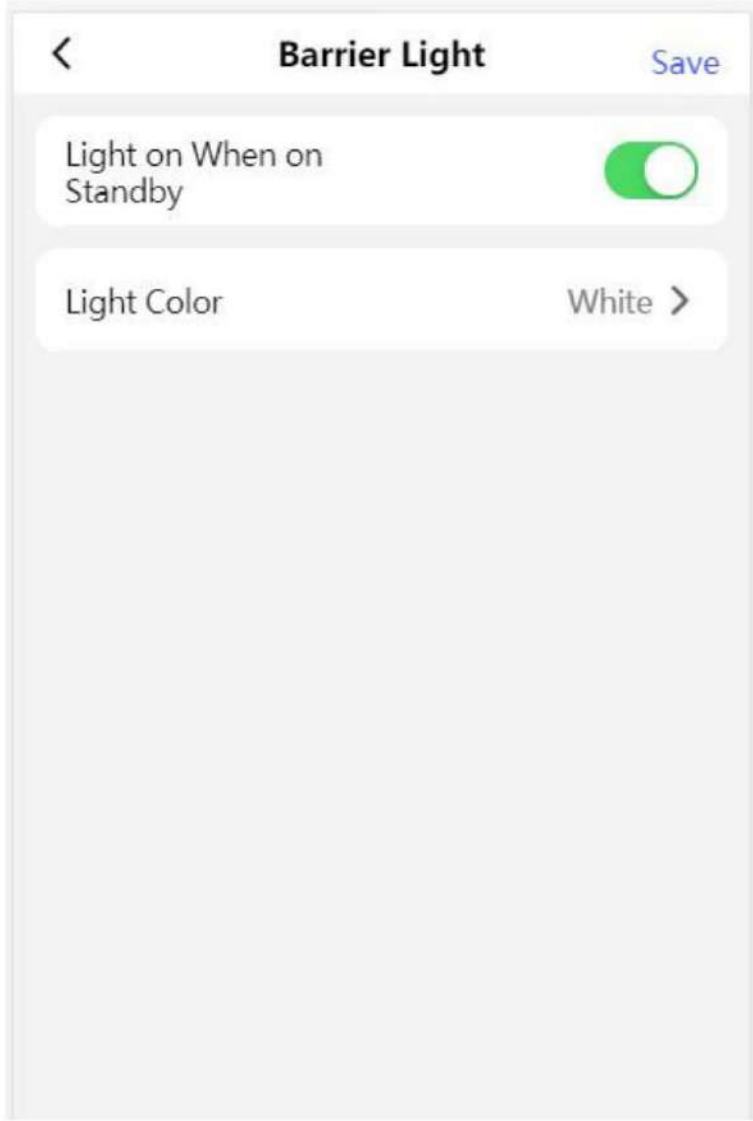


Figura 7-6 Luz de barrera

Toque para habilitar la luz encendida cuando esté en espera según sus necesidades reales y configure el color de la luz de barrera.

7.3.5 Red

Puede configurar la red cableada, el punto de acceso del dispositivo y el puerto.

Red cableada

Establecer red cableada.

Toque CNN → Cmmnn n → Red cableada para ingresar a la página CNN.

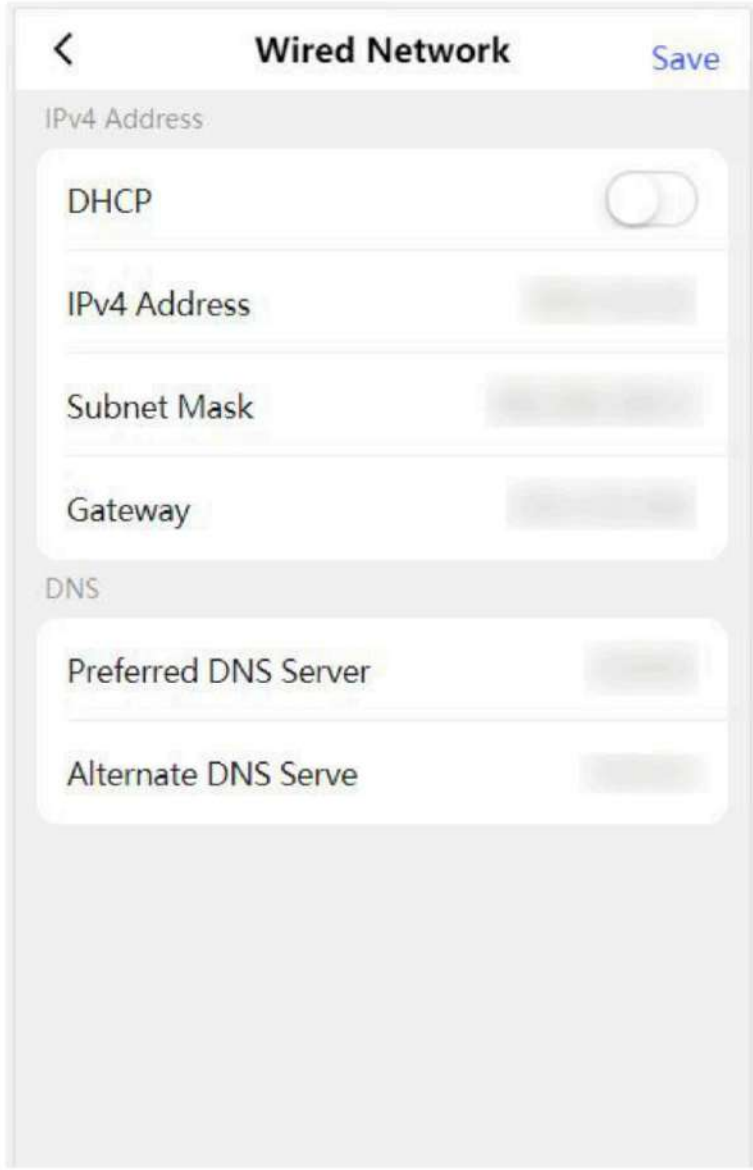


Figura 7-7 Red cableada

DHCP

Si deshabilita nctin, debe configurar la dirección IPv4, la máscara de subred IPv4 y la puerta de enlace predeterminada IPv4.

Si habilita nctin, el sistema asignará la dirección IPv4, la máscara de subred IPv4 y la puerta de enlace predeterminada IPv4 mticy.

Servidor DNS

Configure el servidor DNS preferido y el servidor DNS alternativo según sus necesidades reales.

Punto de acceso del dispositivo

Establecer el punto de acceso del dispositivo.

Toque Cnn → Cmmnn n → Punto de acceso del dispositivo para ingresar a la página de Cnrtin.

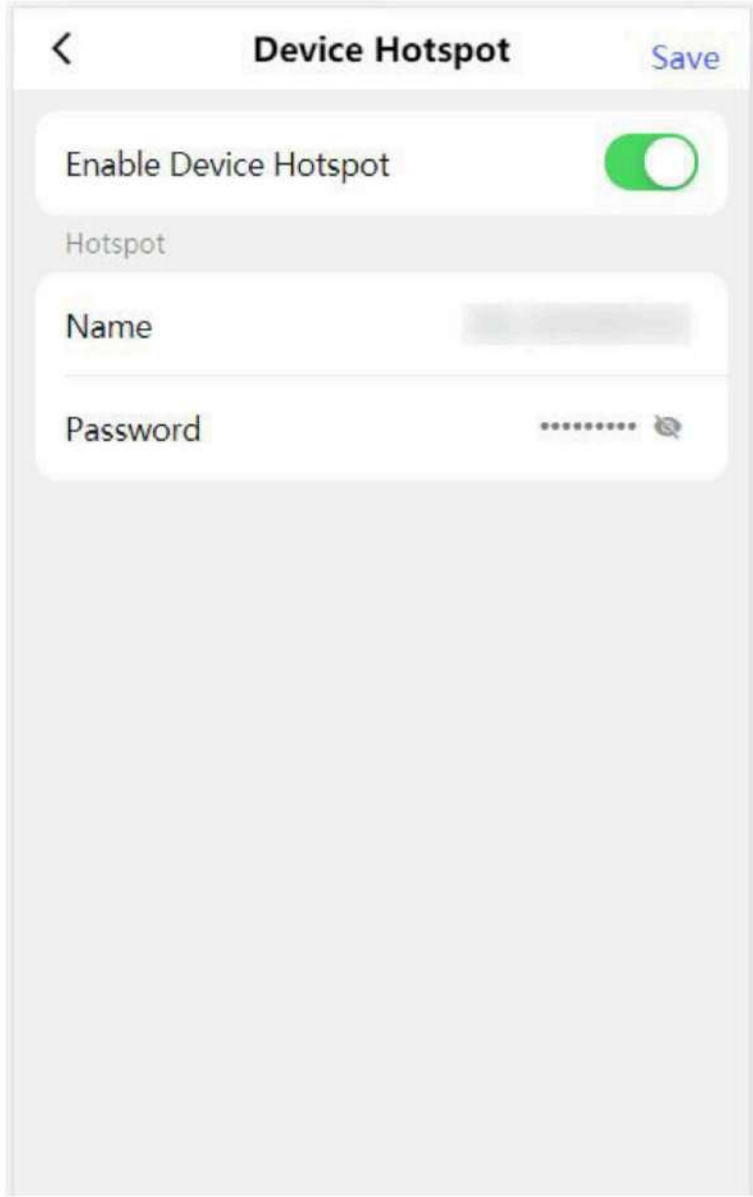


Figura 7-8 Punto de acceso del dispositivo

Pulsa para habilitar el punto de acceso del dispositivo. Establece el nombre y la contraseña del punto de acceso.

Haga clic en Guardar.

CNN de puerto serie

Establecer puerto serie.

Toque Cnn → Cmmnn n → Puerto serie Cnn para ingresar a la página Cnrtin.

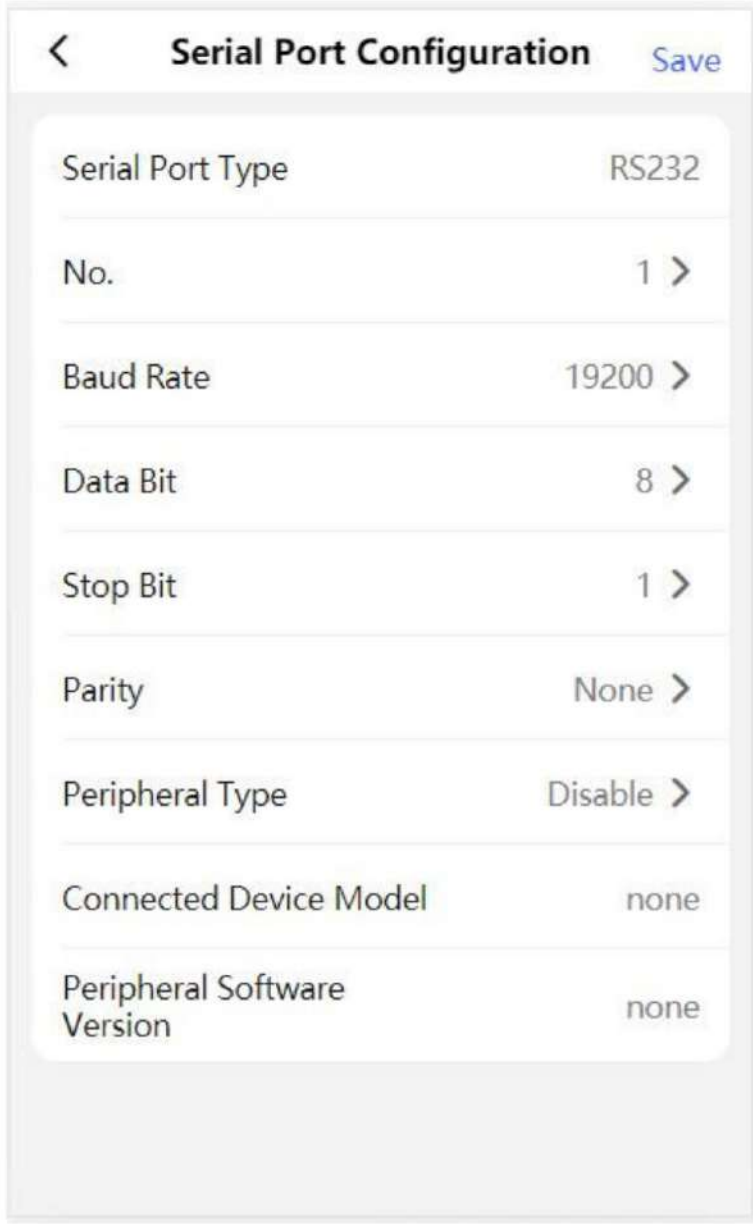


Figura 7-9 Puerto serie CNN

Seleccione el número de puerto y configure la velocidad en baudios, el bit de datos, el bit de parada y la paridad.

Configure el tipo de periférico como Lector de tarjetas, Receptor de tarjetas, Escáner de código QR o Desactivar.

Pulse Guardar.

7.3.6 Dispositivo básico norte

Establecer audio, horario de suspensión y privacidad.

Toque CNN → Básico n para ingresar a la página de contracción.

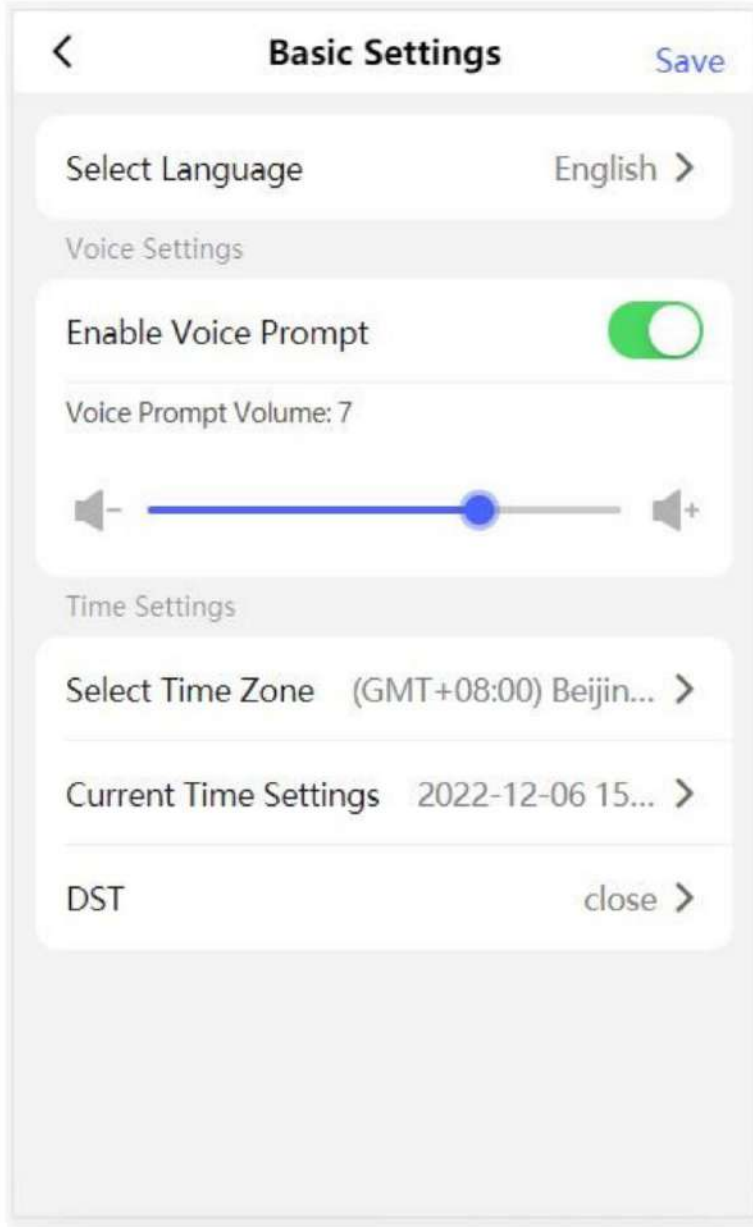


Figura 7-10 CNN básica

Idioma

El idioma predeterminado es inglés.

Voz norte

Toque para habilitar la indicación de voz, seleccione la entrada o la salida para configurar la indicación de voz y arrastre para configurarla.
volumen.

Tiempo norte

Toque para seleccionar la zona horaria y la hora del dispositivo.

Pulse "DST" para acceder a la página "DST n". Active el horario de verano y configure su hora de inicio, fin y sesgo.
tiempo

7.3.7 Control de acceso norte

Establecer parámetros de la puerta

Toque CNN → Control de acceso → Parámetros de la puerta .

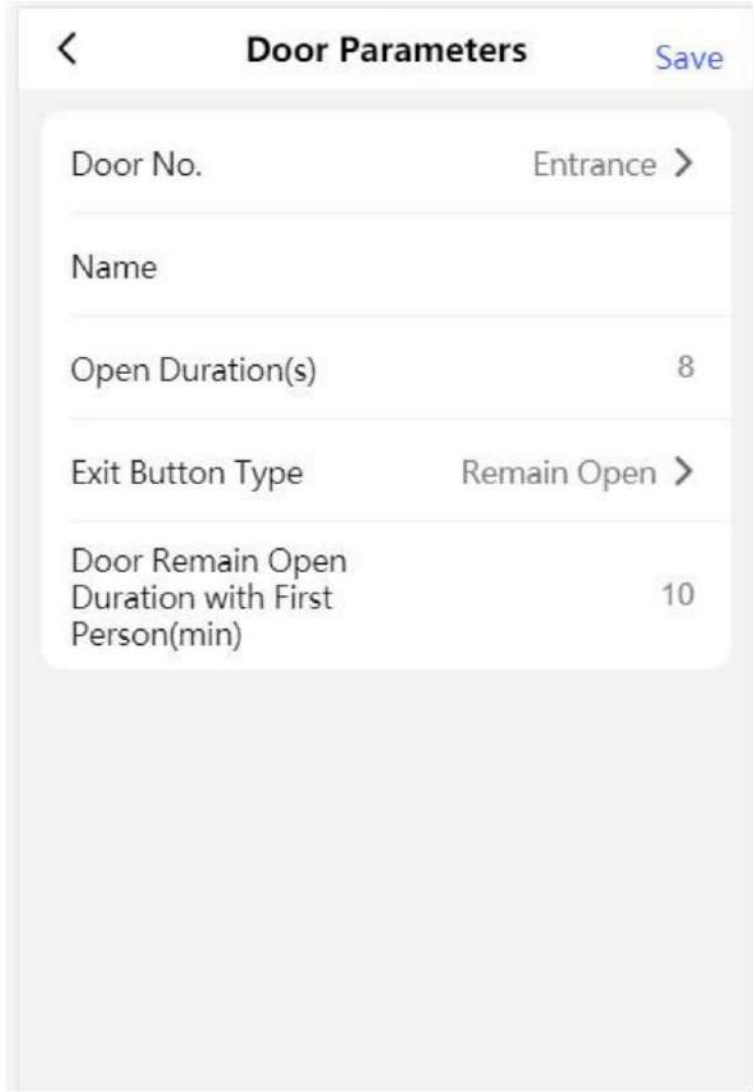


Figura 7-11 Parámetros de la puerta n Página

Haga clic en Guardar para guardar el n ftr la cubierta

Puerta N°

Seleccione el dispositivo al que corresponde el número de puerta.

Nombre

Puedes crear un nombre para la puerta.

Abierto norte

Configurar el tiempo de desbloqueo de la puerta Si la puerta no se abre durante el tiempo establecido, se desbloqueó.
Bloqueado.

Tipo de salida Bn

Puede configurar la salida bn como Permanecer abierta o Permanecer cerrada según sus necesidades reales.

De forma predeterminada, la opción permanece abierta.

La puerta permanece abierta n con Primera Persona

Establezca la puerta abierta rtin cuando la persona r esté dentro. Si la persona r está autorizada, permite
Las personas mti acceden a la puerta u otro ntictina ctina

Establecer nn parámetros

Colocar Parámetros de ntictin.

Pasos

1. Pulse CNN → Control de acceso → nn n .

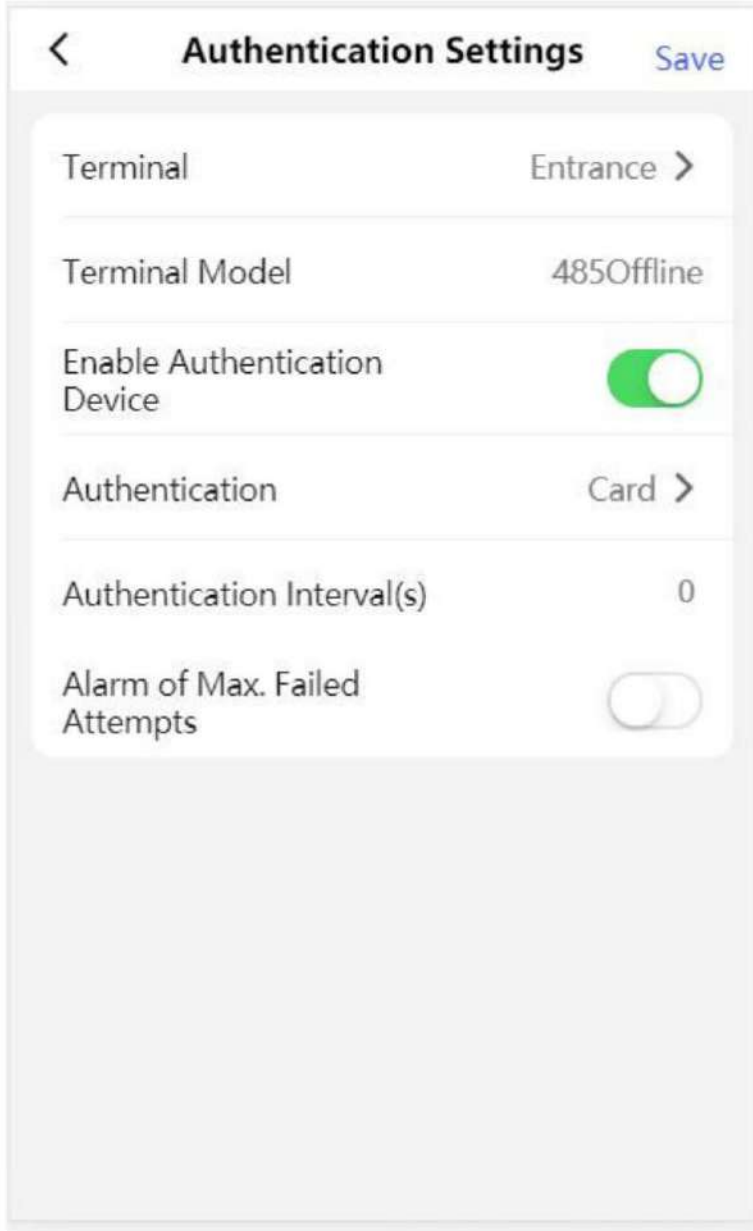


Figura 7-12 nn n

2. Pulse Guardar.

Terminal

Elija Entrada o Salida para

Modelo de terminal

El modelo de terminal es de sólo lectura.

Habilitar dispositivo nn

Habilitar el ntictina nctina

nn

ntictin mediante tarjeta por defecto.

nn Intervalo

Puedes configurar que solo la persona pueda fallar.

Intervalo de ntictin de la misma persona cuando ntic una vez en el intervalo cnr. Un segundo

nntictin Lo mismo La ntictina será

Alarma de Máx. Fallo m

Habilitar para informar una alarma cuando la lectura de la tarjeta m alcanza el valor establecido.

Establecer la seguridad de la tarjeta

Toque CNN → Control de acceso → Seguridad de la tarjeta para ingresar n página.

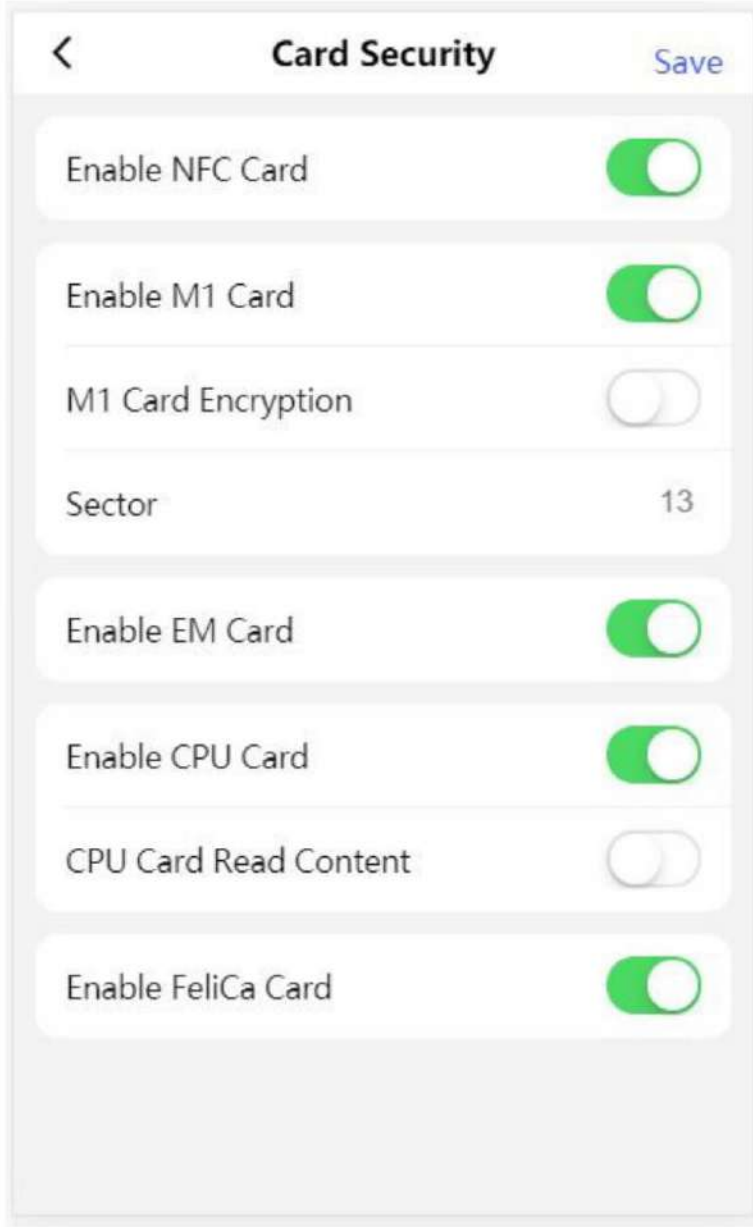


Figura 7-13 Seguridad de la tarjeta

Establezca los parámetros y haga clic en Guardar.

Habilitar tarjeta NFC

Para evitar que el teléfono móvil acceda a los datos del control de acceso, puede desactivar la tarjeta NFC para aumentar el nivel de seguridad de los datos.

Habilitar tarjeta M1

Habilitar la tarjeta M1 y La tarjeta ntictin by rntin M1 está disponible.

Tarjeta M1 nyn

La tarjeta M1 ncrytin puede mejorar el nivel de seguridad de ntictina

Sector

Habilite nctin y configure el sector ncrytin. El sector 13 está cifrado por defecto. Se recomienda cifrar el sector 13.

Habilitar tarjeta EM

Habilitar tarjeta EM y La tarjeta EM ntictin by rntin está disponible.

Nota

Si el lector de tarjetas periféricas admite la tarjeta EM rntin, también se admite nctin para habilitar o deshabilitar la nctin de la tarjeta EM.

Habilitar tarjeta CPU

El dispositivo puede leer los datos de la tarjeta CPU al habilitar la tarjeta CPU nctin

Contenido de lectura de la tarjeta CPU

ftr habilita la lectura del contenido de la tarjeta CPU nctin el dispositivo puede leer el contenido de la tarjeta CPU.

Habilitar la tarjeta FeliCa

El dispositivo puede leer los datos de la tarjeta FeliCa al habilitar la tarjeta FeliCa nctin

Terminal norte

Establecer el modo de trabajo.

Toque CNN → Control de acceso → Parámetros del terminal para ingresar n página.

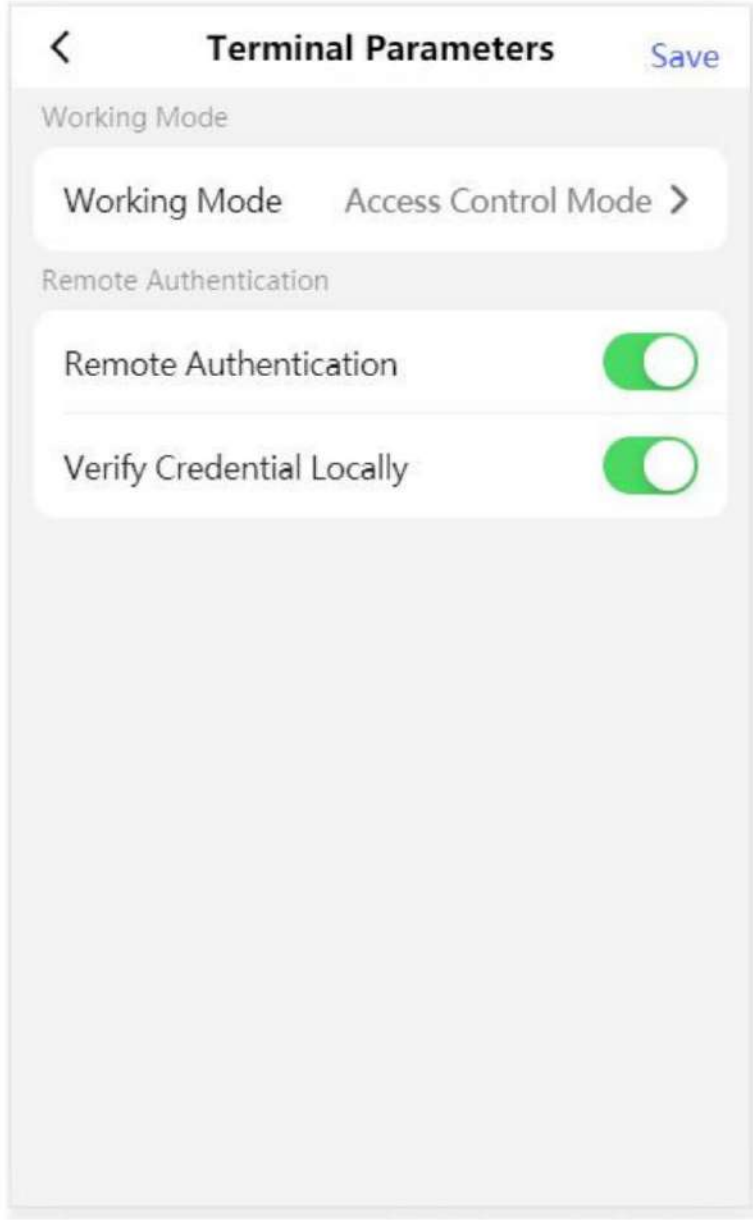


Figura 7-14 Parámetros del terminal

Modo sin permisos

El dispositivo no verificará el permiso de la persona, sino solo su período de validez. Si la persona se encuentra dentro del período de validez, la barrera se abrirá.

Puede habilitar Verificar CN localmente. Al habilitar nctin, el dispositivo solo verificará el permiso de la persona sin la plantilla de programación, etc.

Modo de control de acceso

El dispositivo funciona normalmente y verificará el permiso de la persona para abrir la barrera.

Nn remoto

El dispositivo cargará la voluntad de la persona y juzgará si abre o no la barrera. ntictin nrmtin al tfrm El tfrm

Verificar CN localmente El

dispositivo solo verificará el permiso de la persona sin la plantilla de programación, etc.

7.3.8 Ver dispositivo nmn

Ver el nombre del dispositivo, idioma, modelo, número de serie, versión, etc.

Toque Cnn → Sistema nmn para ingresar a la página cnrtin.

Puede ver el idioma, el modelo, el número de serie, la versión, el número de entrada y salida IO, el número RS-485 local, la dirección MAC y la licencia de código abierto.

Puedes cambiar el nombre del dispositivo. Pulsa Guardar.

7.3.9 Capacidad del dispositivo

Toque CNN → Capacidad del dispositivo para ingresar a la página.

Puede ver la cantidad de usuarios, tarjetas y eventos.

7.3.10 Exportación de registros

Toque CNN → Exportar registro para ingresar a la página.

Seleccione un tipo de registro y toque Exportar.

7.3.11 Restaurar y reiniciar

Reinicie el dispositivo y restaure los parámetros del dispositivo.

Restaurar

Toque CNN → Restaurar .

Todos los parámetros se restaurarán a los valores de fábrica.

Reiniciar dispositivos

Toque CNN → Reiniciar dispositivos .

Pulse Reiniciar para reiniciar el dispositivo.

Capítulo 8 Cliente ftp

Puede llamar a la línea directa para obtener el paquete ftp ntin del cliente iVMS-4200.

8.1 Flujo CNN del cliente ftw

Siga el diagrama w a continuación para cnr en el cliente ftwr

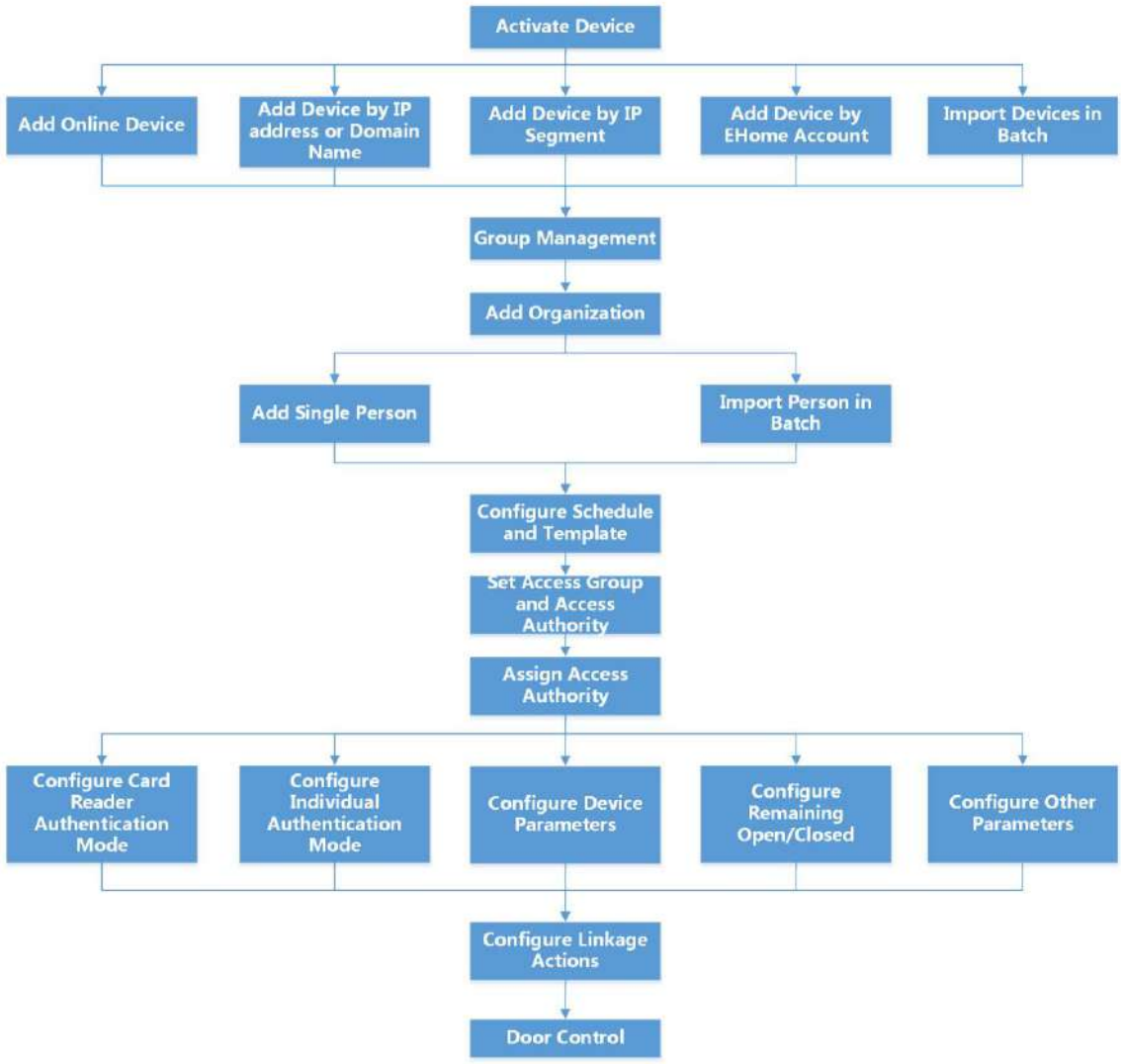


Figura 8-1 Diagrama de flujo de CNN en el cliente ftw

8.2 Administración de dispositivos

El cliente admite la gestión de dispositivos de control de acceso y dispositivos de videoportero.

Ejemplo

Puede controlar la entrada y salida y administrar nnc ftr agregando dispositivos de control de acceso al cliente; puede realizar intercomunicación de video con la lata interior y la lata de la puerta.

8.2.1 Agregar dispositivo

El cliente ofrece tres modos de agregar dispositivos: por IP/dominio, segmento IP y protocolo ISUP. También admite la adición de dispositivos mrtin mti por lotes cuando se requiere agregar una gran cantidad de dispositivos.

Agregar dispositivo por dirección IP o nombre de dominio

Si conoce la dirección IP o el nombre de dominio del dispositivo que desea agregar, puede agregar dispositivos al cliente especificando la dirección IP (o nombre de dominio), el nombre de usuario, la contraseña, etc.

Pasos

1. Ingrese al módulo Administración de dispositivos.
2. Haga clic en la pestaña Dispositivo en la parte superior del panel derecho.

   Los dispositivos agregados se muestran en el panel derecho.
3. Haga clic en Agregar para abrir la ventana Agregar y luego seleccione IP/Dominio como modo de adición.
4. Ingrese el nrmtin requerido

   Nombre

   Crea un nombre crítico para el dispositivo. Por ejemplo, puedes usar un apodo que muestre la función o el nombre del dispositivo.

   DIRECCIÓN

   La dirección IP o el nombre de dominio del dispositivo.

   Puerto

   Los dispositivos que se van a agregar comparten el mismo número de puerto. El valor predeterminado es 8000.

   Nota

   Para algunos tipos de dispositivos, puede ingresar 80 como número de puerto. Este nctin debería ser compatible con el dispositivo.

   Nombre de usuario

   Introduzca el nombre de usuario del dispositivo. Por defecto, el nombre de usuario es admin.

   Contraseña

Introduzca la contraseña del dispositivo.

Cn

Se puede comprobar la seguridad de la contraseña del dispositivo con mticy. Recomendamos encarecidamente cambia la contraseña de tu elección (utilizando un mínimo de 8 caracteres, incluidos al menos tres tipos de las siguientes categorías: mayúsculas y minúsculas, números, y caracteres especiales) para aumentar la seguridad de su producto. Y recomendamos cambia tu contraseña regularmente, especialmente en el sistema de alta seguridad, cambiando la La contraseña mensual o semanal puede proteger su producto.
El mantenimiento adecuado de todas las contraseñas y otras medidas de seguridad es responsabilidad del usuario. instalador y/o usuario final.

5. n Marque la casilla Transmisión nyn (TLS) para habilitar la transmisión ncrytin mediante TLS (Transport Layer Security) Protocolo con fines de seguridad.

Nota

• El dispositivo debe ser compatible con esta nctin.
Si ha habilitado la función de control de acceso de Crtic, haga clic en Abrir C para abrir la Directorio a carpeta predeterminada y copie el directorio de Crtic para exportado desde el dispositivo a este valor predeterminado reforzar la seguridad. Consulte para obtener más información sobre cómo habilitar la función de control de acceso de Crtic.
• Puede iniciar sesión en el dispositivo para obtener el crítico. por navegador web.

6. Marque Sincronizar hora para sincronizar la hora del dispositivo con la PC que ejecuta el cliente ftr agregando el dispositivo al cliente.
7. n Marque Importar al grupo para crear un grupo por nombre del dispositivo e importar todos los canales del dispositivo a este grupo.

Ejemplo

Para el dispositivo de control de acceso, sus puntos de acceso, entradas/salidas de alarma y canales de codificación (si existen) se importarán a este grupo.

8. Termine de agregar el dispositivo.
- Haga clic en Agregar para agregar el dispositivo y regresar a la página de la lista de dispositivos.
- Haga clic en Agregar y Nuevo para guardar la n y cntin para agregar otro dispositivo.

Importar dispositivos en un lote

Puede agregar dispositivos mti al cliente en un lote ingresando los parámetros del dispositivo en ar en CSV

Pasos

1. Ingrese al módulo Administración de dispositivos.
2. Haga clic en la pestaña Dispositivo en la parte superior del panel derecho.
3. Haga clic en Agregar para abrir la ventana Agregar y luego seleccione Importación por lotes como modo de adición.
4. Haga clic en Exportar plantilla y luego guarde la plantilla rn (CSV) en su PC.

5. Abra la plantilla exportada e ingrese el nrmtin requerido de los dispositivos que se agregarán en la columna correspondiente.

Nota

Para una descripción detallada de lo requerido Consulte la nrctin en la plantilla.

Modo de adición

Introduzca 0 , 1 o 2.

DIRECCIÓN

Editar la dirección del dispositivo.

Puerto

Introduzca el número de puerto del dispositivo. El puerto predeterminado es 8000.

Nombre de usuario

Introduzca el nombre de usuario del dispositivo. Por defecto, el nombre de usuario es admin.

Contraseña

Introduzca la contraseña del dispositivo.

Cn

La seguridad de la contraseña del dispositivo se puede comprobar con mticy. Le recomendamos encarecidamente que cambie la contraseña que elija (con un mínimo de 8 caracteres, incluyendo al menos tres tipos de mayúsculas, minúsculas, números y caracteres especiales) para aumentar la seguridad de su producto. Le recomendamos que cambie su contraseña regularmente, especialmente en sistemas de alta seguridad. Cambiarla mensual o semanalmente puede proteger su producto.

El mantenimiento adecuado de todas las contraseñas y otros datos de seguridad es responsabilidad del instalador y/o del usuario final.

Importar al grupo

Introduzca 1 para crear un grupo por nombre de dispositivo. Todos los canales del dispositivo se importarán al grupo correspondiente por defecto. Introduzca 0 para desactivar esta función.

6. Haga clic y seleccione la plantilla. 7. Haga clic en Agregar para importar los dispositivos.

8.2.2 Restablecer la contraseña del dispositivo

Si olvidó la contraseña de los dispositivos en línea detectados, puede restablecer la contraseña del dispositivo a través del cliente.

Pasos

1. Ingrese a la página de Administración de dispositivos.
2. Haga clic en Dispositivo en línea para mostrar el área del dispositivo en línea.

Todos los dispositivos en línea que comparten la misma subred se mostrarán en la lista.

3. Seleccione el dispositivo de la lista y haga clic en la columna rtin.

4. Restablezca la contraseña del dispositivo.

- Haga clic en Generar para que aparezca la ventana del Código QR y haga clic en Descargar para guardar el código QR en Tu PC. También puedes tomar una foto del código QR para guardarla en tu teléfono. Envía la foto a nuestro soporte técnico.

Nota

Para el siguiente rtin para rn la contraseña, póngase en contacto con nuestro soporte técnico.

Cn

La seguridad de la contraseña del dispositivo se puede comprobar con mticy. Le recomendamos encarecidamente que cambie la contraseña que elija (con un mínimo de 8 caracteres, incluyendo al menos tres tipos de las siguientes categorías: mayúsculas, números y caracteres especiales) para aumentar la seguridad de su producto. Le recomendamos que cambie su contraseña regularmente, especialmente en sistemas de alta seguridad. Cambiarla mensual o semanalmente puede proteger su producto.

r minúscula

Administración adecuada de todas las contraseñas y demás datos de seguridad del instalador y/o usuario final. n es responsabilidad de la

8.2.3 Administrar dispositivos agregados

Al agregar dispositivos a la lista de dispositivos, puede administrar los dispositivos agregados, incluidos los parámetros del dispositivo, la visualización remota del estado del dispositivo, etc.

Tabla 8-1 Administrar dispositivos agregados

Editar dispositivo	Haga clic para editar el nombre del dispositivo, incluido el nombre del dispositivo, la dirección, el nombre de usuario, la contraseña, etc.
Eliminar dispositivo	Marque uno o más dispositivos y haga clic en Eliminar para eliminar los dispositivos seleccionados.
Control remoto: Haga clic para configurar el control remoto del dispositivo correspondiente. Para más detalles, consulte el manual del usuario del dispositivo.	
Ver el estado del dispositivo	Haga clic para ver el estado del dispositivo, incluido el número de puerta, el estado de la puerta, etc. Nota Para los dispositivos rn, verá rn nrmtin acerca del dispositivo estado.

Ver usuario en línea	Haga clic para ver los detalles del usuario en línea que accede al dispositivo, incluido el nombre de usuario, el tipo de usuario, la dirección IP y la hora de inicio de sesión.
Actualizar nrmtin del dispositivo	Haga clic para actualizar y obtener la última versión del dispositivo.

8.3 Gestión de grupos

El cliente proporciona grupos para administrar los recursos añadidos en grupos rn. Puede agrupar los recursos en grupos rn según su ctin.

Ejemplo :

Por ejemplo, en el primer piso, Allí se montaron 16 puertas, 64 entradas de alarma y 16 salidas de alarma. se pueden organizar estos recursos en un grupo (llamado "Primer piso") para una gestión más sencilla. Se puede controlar el estado de las puertas y realizar otras tareas de los dispositivos al administrar los recursos por grupos.

8.3.1 Agregar grupo

Puede agregar un grupo para organizar el dispositivo agregado para una administración conveniente.

Pasos

1. Ingrese al módulo Administración de dispositivos.
2. Haga clic en Administración de dispositivos → Grupo para ingresar a la página de administración de grupos.
3. Crea un grupo.
   - Haga clic en Agregar grupo e ingrese el nombre del grupo que desee.
   - Haga clic en Crear grupo por nombre de dispositivo y seleccione un dispositivo agregado para crear un nuevo grupo con el nombre del dispositivo seleccionado.

   Nota

   Los recursos (como entradas/salidas de alarma, puntos de acceso, etc.) de este dispositivo se importarán al grupo de forma predeterminada.

8.3.2 Importar recursos al grupo

Puede importar los recursos del dispositivo (como entradas/salidas de alarma, puntos de acceso, etc.) al grupo agregado en un lote.

Antes de empezar:

Agrega un grupo para administrar dispositivos. Consulta " Agregar grupo" .

Pasos

1. Ingrese al módulo Administración de dispositivos.

2. Haga clic en Administración de dispositivos → Grupo para ingresar a la página de administración de grupos.

3. Seleccione un grupo de la lista de grupos y seleccione el tipo de recurso como Punto de acceso, Entrada de alarma, Salida de alarma, etc.

4. Haga clic en Importar.

5. Seleccione las miniaturas/nombres de los recursos en la vista de miniaturas/lista.

Nota

Puede hacer clic en para cambiar el modo de visualización de recursos a vista de miniatura o vista de lista.

6. Haga clic en Importar para importar los recursos seleccionados al grupo.

8.4 Gestión de personas

Puede agregar un número de persona al sistema para funciones adicionales, como control de acceso, videoportero, tim y nnc, etc. Puede administrar las personas agregadas, como emitirles tarjetas en un lote, números de persona mrtin y xrtin en un lote, etc.

8.4.1 Agregar nn

Puede agregar una rntin e importar la nrmtin de persona a la rntin para gestionar las personas. activo También puede agregar una rntin subordinada para la persona agregada.

Pasos

1. Ingresar al módulo Persona .

2. Seleccione una ruta principal en la columna ft y haga clic en Agregar en la esquina rft para agregar una. rntin

3. Crea un nombre para el rntin agregado

Nota

Se pueden agregar hasta 10 niveles de rntin. n Realice

4. el siguiente rtin()

Editar nn Pase el mouse sobre una rntin agregada y haga clic para editar su nombre.

Borrar nn Pase el mouse sobre una entrada agregada y haga clic para eliminarla.

Nota

- El rntin de nivel inferior también se eliminará si elimina un rntin
- Asegúrese de que no haya ninguna persona agregada en el registro o el registro no se podrá eliminar.

Mostrar personas en Sub nn Marque Mostrar personas en sub nn y seleccione una ruta para mostrar personas en su subruta

8.4.2 Importación y Exportación Persona

Puede importar el nrmtin y las imágenes de personas mti al cliente ftwr en un lote.
Mientras tanto, también puedes exportar la información de la persona y las imágenes y guardarlas en tu PC.

Importar persona

Puede ingresar el nrmtin de mti personas en una plantilla rn (CSV/Excel) e importar el nrmtin al cliente en) a un lote.

Pasos

1. Ingresar al módulo Persona.
2. Seleccione una entrada agregada en la lista o haga clic en Agregar en la esquina inferior derecha para agregar una. rntin y luego selecciónelo.
3. Haga clic en Importar para abrir el panel Importar.
4. Seleccione Persona nmn como modo mrtin.
5. Haga clic en Descargar plantilla para mn Person para descargar la plantilla.
6. Ingrese el nombre de la persona en la plantilla descargada.

Nota

• Si la persona tiene tarjetas mti, separe el número de tarjeta con punto y coma. • Los elementos con asterisco son obligatorios. •
De forma predeterminada, la fecha de contratación es la fecha actual.

7. Haga clic para seleccionar el CSV/Excel con la información de la persona desde la PC local.
8. Haga clic en Importar para iniciar mrtin

Nota

• Si ya existe un número de persona en la base de datos del cliente, elimine el xtin nrmtin antes Mrtin
• Puedes importar un número máximo de 2.000 personas.

Importar imágenes de personas

Fotos de rostros de las personas añadidas al cliente. Las personas en las fotos pueden ser importadas por una terminal anti de reconocimiento facial. Puede importar las fotos de las personas una por una.
uno, o importe imágenes mti a la vez según su necesidad.

Antes de comenzar

Asegúrese de haber importado la información de persona al cliente de antemano.

Pasos

1. Ingresar al módulo Persona.

2. Seleccione una entrada agregada en la lista o haga clic en Agregar en la esquina inferior derecha para agregar una.
rntin y luego selecciónelo.

3. Haga clic en Importar para abrir el panel Importar y marque Cara. 4.

n Habilite Verificar por dispositivo para verificar si el dispositivo de reconocimiento facial administrado en el

El cliente puede reconocer la cara en la fotografía.

5. Haga clic para seleccionar una imagen de rostro.

Nota

La carpeta de fotos faciales debe estar en formato ZIP. Cada imagen debe estar en formato JPG y no debe superar los 200 KB. Cada imagen debe llamarse "ID de persona_Nombre". El ID de persona debe ser el mismo que el de la persona importada. 6. Haga clic en Importar para iniciar la importación. Se mostrarán el progreso y el resultado de la importación.

Persona de exportación nmn

Puede exportar la información de las personas agregadas a la PC local como CSV/Excel

Antes de empezar

• Asegúrese de haber agregado personas a una lista • Asegúrese de haber habilitado la opción Exportar persona para mostrar la lista Exportar
bn Ver para más detalles.

Pasos

1. Ingresar al módulo Persona.
2. n Seleccione una ruta en la lista.

Nota

Se exportarán los datos de todas las personas si no selecciona ningún dato. 3. Haga clic en Exportar.

4. Ingrese el nombre de superusuario y la contraseña para vrctin

Se muestra el panel Exportar.

5. Marque Persona nmn como el contenido a exportar.
6. Marque los elementos que desea exportar.
7. Haga clic en Exportar para guardar el archivo exportado. en CSV/Excel en su PC.

Exportar imágenes de personas

Puedes exportar fotos de la cara. de las personas agregadas y guardar en tu PC.

Antes de empezar

• Asegúrese de haber agregado personas y sus fotos de rostro a una lista • Asegúrese de haber habilitado la opción Exportar persona para mostrar la lista Exportar
bn Ver para más detalles.

Pasos

1. Ingresar al módulo Persona.
2. n Seleccione una ruta en la lista.

Nota

Se exportarán las imágenes de los rostros de todas las personas si no selecciona ninguna opción.

3. Haga clic en Exportar en la barra de menú superior.
4. Ingrese el nombre de superusuario y la contraseña para vrctin

Se muestra el panel Exportar.

5. Marque Cara como el contenido a exportar.
6. Haga clic en Exportar y configure una clave ncrytin para cifrar el archivo exportado.

Nota

• La imagen del está en formato ZIP.
rostro exportada se denomina "Person ID_Name_0" ("0" es para un rostro frontal completo).

8.4.3 Obtener el nmn de persona del dispositivo de control de acceso

Si el dispositivo de control de acceso se ha cifrado con el número de persona (incluidos los detalles de la persona, el número y el número de tarjeta emitida), puede obtener el número de persona del dispositivo agregado e importarlo al cliente para su posterior cifrado.

Pasos

Nota

• Si el nombre de la persona almacenado en el dispositivo está vacío, el nombre de la persona será con el emitido
Tarjeta No. ftr mrtin al cliente.

• Las personas serán hombres de forma
predeterminada. • Si el número de tarjeta o el ID de persona (ID de empleado) almacenado en el dispositivo ya existe en la base de datos del cliente, la persona con este número de tarjeta o ID de persona no se importará al cliente.

1. Ingrese al módulo Persona .
2. Seleccione una ruta para importar las personas.
3. Haga clic en Obtener del dispositivo.
4. Seleccione un dispositivo de control de acceso agregado o la lata de inscripción de la lista desplegable.

Nota

Si selecciona la opción de registro deberá hacer clic en Iniciar sesión e ingresar la dirección IP, el número de puerto, el nombre de usuario y la contraseña del dispositivo.

5. Seleccione el modo Gn.

Nota

El El modo n varía según los dispositivos rn. El dispositivo de control de acceso admite cada uno.
En la persona nrmtin por ID de empleado. Se pueden c hasta 5 ID de empleado.
tiempo

6. Haga clic en Importar para comenzar a importar la información de la persona al cliente.

Nota

Se pueden importar hasta 2.000 personas y 5.000 tarjetas.

El nrmtin de la persona, incluidos los detalles de la persona, el nrmtin de la persona (si es cnr) y las tarjetas vinculadas (si es cnr) se importarán al nrmtin seleccionado.

8.4.4 Emitir tarjetas a personas por lotes

El cliente proporciona una forma conveniente de emitir tarjetas a personas mti en un lote.

Pasos

1. Ingresar al módulo Persona .
2. Haga clic en Emitir tarjetas por lotes.

En el panel derecho se mostrarán todas las personas agregadas sin tarjeta emitida. r la(s) persona(s)
n Ingrese palabras clave (nombre o ID de la persona) en el cuadro de entrada que necesitan 3.
para emitir
4. tarjetas. n Haga clic en Para configurar los parámetros de emisión de tarjetas. Para más detalles,
5. Haga clic en consulte . Para configurar la tarjeta de registro o el lector de tarjetas para que esté listo para la emisión.
n tarjetas.
6. Haga clic en la columna Número de tarjeta e ingrese el número de tarjeta.
- Coloque la tarjeta en la lata de inscripción de tarjetas. - Pase
la tarjeta por el lector de tarjetas.
- Introduzca manualmente el número de tarjeta y presione la tecla Enter .

A las personas que figuran en la lista se les expedirá(n) tarjeta(s).

8.4.5 Pérdida de la tarjeta de informe

Si la persona perdió su tarjeta, puede reportar la pérdida de la tarjeta para que se active la función de acceso relacionada con la misma.

Pasos

1. Ingresar al módulo Persona .
2. Seleccione la persona cuya pérdida de tarjeta desea reportar y haga clic en Editar para abrir la ventana Editar persona.
3. En el panel Cn → Tarjeta , haga clic en la tarjeta agregada para establecerla como tarjeta perdida.

En caso de pérdida de tarjeta, el acceso de esta tarjeta será inválido y no activo. Otra persona que obtenga esta tarjeta no podrá acceder a las puertas deslizándola. Si se encuentra la tarjeta perdida, puede hacer clic

4. para cancelar la pérdida. Al cancelar la pérdida de tarjeta, el acceso de la persona

será válido y activo. 5. Si la tarjeta perdida se agrega a un grupo de acceso y el grupo de acceso se aplica al dispositivo.

ya, tras la pérdida de la tarjeta o la cancelación de la pérdida de la tarjeta, aparecerá una ventana que le pedirá que aplique los cambios al dispositivo. tras aplicarlos al dispositivo, estos cambios pueden tener lugar en el c en el dispositivo.

8.4.6 Establecer parámetros de emisión de tarjetas

El cliente ofrece dos modos de lectura del número de tarjeta: mediante la tarjeta de registro o mediante el lector del dispositivo de control de acceso. Si dispone de una tarjeta de registro, conéctela al PC que ejecuta el cliente mediante una interfaz USB o COM y coloque la tarjeta en la tarjeta de registro para leer el número. De lo contrario, también puede deslizar la tarjeta por el lector del dispositivo de control de acceso añadido para obtener el número. Por lo tanto, antes de emitir una tarjeta a una persona, debe configurar los parámetros de emisión, incluyendo el modo de emisión y los parámetros relacionados.

Al agregar una tarjeta a una persona, haga clic en n para abrir la Emisión de Tarjetas n ventana.

Modo local: Emisión de tarjeta por inscripción. Conecte una lata norte

de inscripción de tarjeta al PC que ejecuta el cliente. Puede colocar la tarjeta sobre la lata para obtener el número.

Inscripción de tarjeta norte

Seleccione el modelo de la lata de inscripción de la tarjeta conectada

Nota

Actualmente, los modelos de lata de inscripción de tarjetas compatibles incluyen DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E y DS-K1F180-D8E.

Tipo de tarjeta

Este solo está disponible cuando el modelo es DS-K1F100-D8E o DS-K1F180-D8E.

Seleccione el tipo de tarjeta como tarjeta EM o tarjeta IC según el tipo de tarjeta real.

Puerto serie

Sólo está disponible cuando el modelo es DS-K1F100-M.

Seleccione el COM al cual se conecta la tarjeta de inscripción.

Zumbido

Habilitar o deshabilitar el zumbido cuando se lee correctamente el número de tarjeta.

Número de tarjeta Tipo

Seleccione el tipo de número de tarjeta según las necesidades reales.

Tarjeta M1 nyn

Este solo está disponible cuando el modelo es DS-K1F100-D8, DS-K1F100-D8E o DS-K1F180-D8E.

Si la tarjeta es una tarjeta M1 y necesita habilitar la ncrytin nctin de la tarjeta M1, debe
Habilite este nctin y seleccione el sector de la tarjeta que desea cifrar.

Modo remoto: Emitir tarjeta mediante lector de tarjetas

Seleccione un dispositivo de control de acceso agregado en el cliente y deslice la tarjeta en su lector de tarjetas para leer el número de tarjeta.

8.5 Cn Programa y Plantilla

Puede copiar la plantilla, incluidos los días festivos y el calendario semanal. ftr en la plantilla,
Puede adoptar la plantilla cnr para acceder a los grupos cuando n los grupos de acceso, de modo que
El grupo de acceso tomará c en el tim rtin de la plantilla.

Nota

Para el grupo de acceso nota Consulte Establecer grupo de acceso para asignar acceso n a Personas .

8.5.1 Agregar vacaciones

Puede crear días festivos y establecer los días de los días festivos, incluida la fecha de inicio, la fecha de finalización y el día festivo.
rtin en un día.

Pasos

Nota

Puede agregar hasta 64 días festivos en el sistema ftwr.

1. Haga clic en Control de acceso → Programación → Vacaciones para ingresar a la página de Vacaciones.
2. Haga clic en Agregar en el panel ft.
3. Crea un nombre para la festividad.
4. n Ingrese la fecha o alguna anécdota de este feriado en el cuadro de Observaciones.
5. Agregue un período de vacaciones a la lista de vacaciones y haga clic en el período de vacaciones.

   Nota

   Es posible añadir hasta 16 periodos de vacaciones a un día festivo.

   1) Haga clic en Agregar en la lista de vacaciones

2) Arrastre el cursor para dibujar el rtin de tiempo, lo que significa que en ese rtin de tiempo el
El grupo de acceso cnr está activo

Nota

Se pueden configurar hasta 8 tim rtin para un período de vacaciones.

3) n Realice el siguiente rtin para editar el tim rtin

• Mueva el cursor al tim rtin y arrastre el tim rtin en la barra de tiempo hasta el tim deseado cuando el cursor cambie a .

• Haga clic en el tim rtin y edite directamente el tiempo de inicio/fin en el cuadro de diálogo que aparece.

• Mueva el cursor al inicio o al final del tim rtin y arrástrelo para alargarlo o acortarlo cuando el cursor cambie a n . Seleccione el tim rtin() que necesita eliminarse y .

4) luego haga clic en la columna rtin para eliminar el tim rtin() seleccionado. en el

5) n Haga clic en la columna rtin para borrar todo el tiempo rtin() en la barra de tiempo. 6) n Haga clic en la columna rtin para eliminar este período de vacaciones agregado de la lista de vacaciones.

6. Haga clic en Guardar.

8.5.2 Agregar plantilla

La plantilla incluye el horario semanal y los días festivos. Puede configurar el horario semanal y asignar el horario de acceso para cada persona o grupo. También puede seleccionar los elementos añadidos.
vacaciones para la plantilla.

Pasos

Nota

Puede agregar hasta 255 plantillas en el sistema ftwr.

1. Haga clic en Control de acceso → Programación → Plantilla para ingresar a la página Plantilla.

Nota

Hay dos plantillas predeterminadas: Autorizada todo el día y Denegada todo el día, y no se pueden editar ni eliminar.

Autorizado todo el día

El rtin de acceso es válido todos los días de la semana y no tiene festivos.

Todo el día denegado

El rtin de acceso no es válido en todos los días de la semana y no tiene días festivos.

2. Haga clic en Agregar en el panel ft para crear una nueva plantilla.
3. Crea un nombre para la plantilla.
4. Ingrese la letra o algún carácter de esta plantilla en el cuadro Observaciones.
5. Edite el cronograma semanal para aplicarlo a la plantilla.

1) Haga clic en la pestaña Programación semanal en el panel inferior.

2) Seleccione un día de la semana y dibuje tim rtin() en la barra de tiempo.

Nota

Se pueden configurar hasta 8 tiempos rtin() para cada día del cronograma de la semana.

3) n Realice el siguiente rtin para editar el tim rtin

- Mueva el cursor al tim rtin y arrástrelo en la barra de timn hacia el lata deseada cuando el cursor cambia a .
- Haga clic en el botón tim rtin y edite directamente la hora de inicio/finalización en el cuadro de diálogo que aparece.
- Mueva el cursor al inicio o al final del tiempo rtin y arrástrelo para alargarlo o acortarlo el tim rtin cuando el cursor cambia a .

4) Repite los dos pasos anteriores para dibujar más tim rtin en los demás días de la semana.

6. Agrega un día festivo para aplicarlo a la plantilla.

Nota

Se pueden agregar hasta 4 días festivos a una plantilla.

1) Haga clic en la pestaña Vacaciones .

2) Seleccione un día festivo en la lista ft y se agregará a la lista seleccionada en el panel derecho.

3) n Haga clic en Agregar para agregar un nuevo día festivo.

Nota

Para obtener detalles sobre cómo agregar un feriado, consulte Agregar feriado .

4) n Seleccione un día festivo seleccionado en la lista de la derecha y haga clic en para eliminar el seleccionado, o Borrar para borrar todos los días festivos seleccionados en la lista de la derecha.

7. Haga clic en Guardar para guardar la n y la n agregando la plantilla.

8.6 Establecer grupo de acceso para asignar acceso n a Personas

Después de agregar a la persona y acceder a su crnti, puede crear los grupos de acceso.

n qué persona(s) puede(n) tener acceso a qué puerta(s) y luego aplicar el grupo de acceso a la(s)

Para acceder al dispositivo de control para tomar do

Antes de empezar

- Agregar persona al cliente.
- Agregar un dispositivo de control de acceso a los puntos de acceso del cliente y del grupo. Para más detalles, consulte Grupo Gestión .
- Agregar plantilla.

Pasos

Cuando el grupo de acceso n se modifican, es necesario aplicar los grupos de acceso a los dispositivos vuelve a tomar c Los cambios del grupo de acceso incluyen cambios de plantilla, grupo de acceso de la persona del grupo de acceso n y datos de la persona relacionada (incluido el número de tarjeta, el rostro y la dirección)

imagen, vínculo entre el número de tarjeta y nrrn vínculo entre el número de tarjeta y
contraseña de la tarjeta nrrn, período de actividad de la tarjeta, etc.).

1. Haga clic en Control de acceso n → Grupo de acceso para ingresar a la interfaz del Grupo de acceso.

→ 2. Haga clic en Agregar para abrir la ventana Agregar.

3. En el texto Nombre, cree un nombre para el grupo de acceso como desee.

4. Seleccione una plantilla para el grupo de acceso.

Nota

Debes cnr la plantilla antes de acceder al grupo y a la Plantilla para obtener n Consulte el programa Cn más detalles.

5. En la lista ft de Seleccionar persona, seleccione la(s) persona(s) a las que asignar autoridad de acceso.

6. En la lista ft de Seleccionar punto de acceso Seleccione puerta(s), puerta tin() o r() para la Personas seleccionadas para acceder.

7. Haga clic en Guardar.

Puede ver las personas seleccionadas y los puntos de acceso seleccionados en el lado derecho de la interfaz.

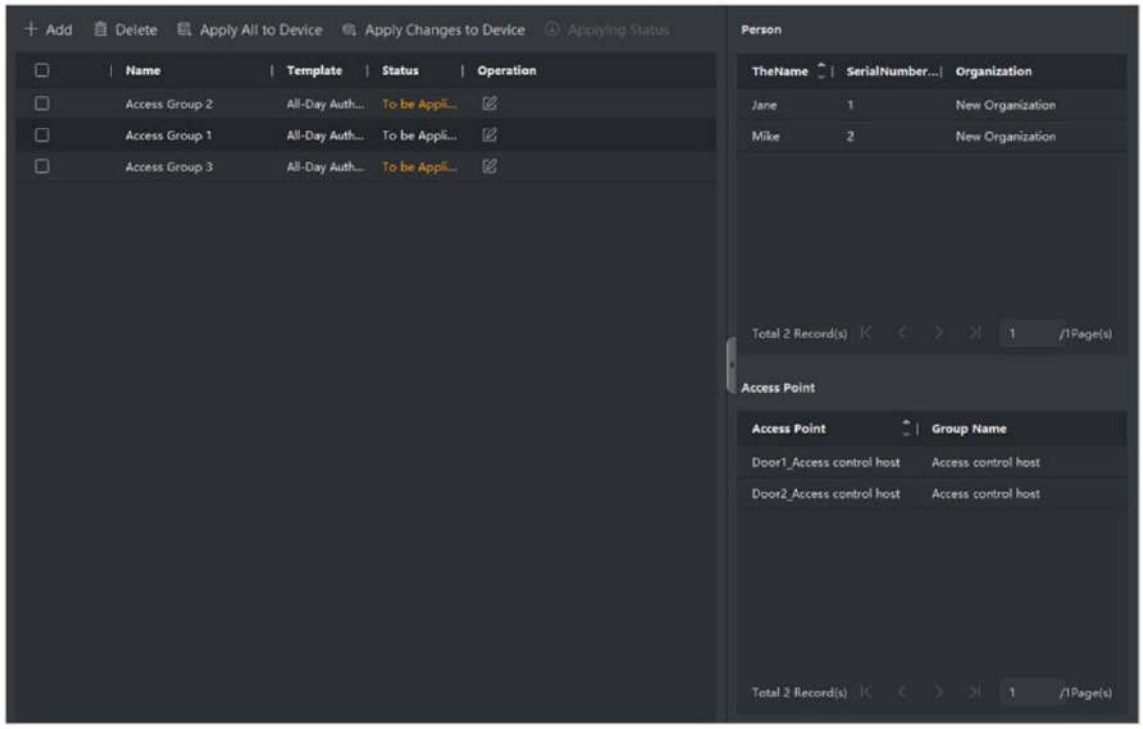


Figura 8-2 Mostrar las personas seleccionadas y los puntos de acceso

8. Después de agregar los grupos de acceso, debe aplicarlos al dispositivo de control de acceso para tomarlos.

do

1) Seleccione el o los grupos de acceso que se aplicarán al dispositivo de control de acceso.
2) Haga clic en Aplicar todo a los dispositivos para comenzar a aplicar todos los grupos de acceso seleccionados al control de acceso. dispositivo o puerta de hojalata

3) Haga clic en Aplicar todo a los dispositivos o Aplicar cambios a los dispositivos.

Aplicar todo a los dispositivos

Esta rtin borrará todos los grupos de acceso existentes de los dispositivos seleccionados y luego aplicará el nuevo grupo de acceso al dispositivo.

Aplicar cambios a los dispositivos

Esta rtin no borrará los grupos de acceso existentes de los dispositivos seleccionados y solo aplicará la parte modificada de los grupos de acceso seleccionados a los dispositivos.

4) Vea el estado de la solicitud en la columna Estado o haga clic en Estado de la solicitud para ver todas las solicitudes. grupo(s) de acceso.

Nota

Puede marcar Solo falla de visualización para r los resultados de la aplicación.

Las personas seleccionadas en los grupos de acceso aplicados tendrán el derecho de ingresar/salir de las puertas/ grupos de acceso seleccionados con su(s) tarjeta(s) vinculada(s) o nrrn n Haga clic

9. para editar el grupo de acceso si es necesario.

Nota

Si cambia el número de acceso de las personas u otro número relacionado, verá el mensaje Grupo de acceso a aplicar en la esquina derecha del cliente.

Puede hacer clic en el mensaje para aplicar los datos modificados al dispositivo. Puede seleccionar " Aplicar ahora" o "Aplicar más tarde".

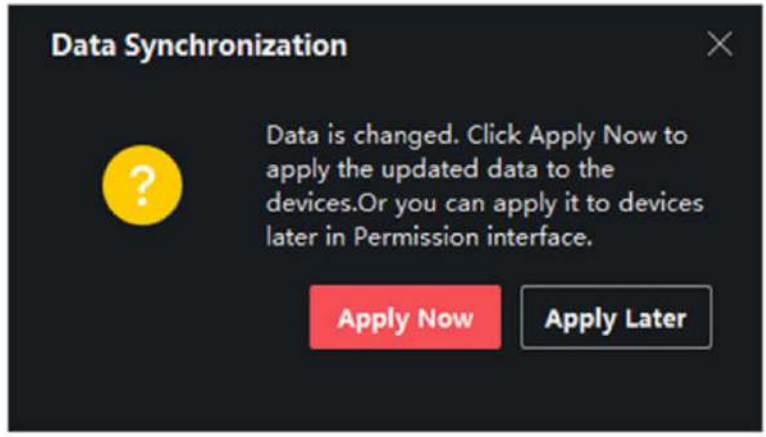


Figura 8-3 Datos ynnn

8.7 Cn Función avanzada

Puede activar la función avanzada de control de acceso para cumplir con algunos requisitos especiales en escena rn, como mticr ntictin ntibc etc.

Nota

• Para la nctin relacionada con la tarjeta (tipo de control de acceso crmticr ntictin), solo se incluirán las tarjetas con grupo de acceso aplicado al agregar tarjetas.

• El dispositivo debe ser compatible con nctin avanzado. • Coloque el cursor sobre nctin avanzado y luego haga clic para personalizar el nctin() avanzado que se mostrará.

8.7.1 Parámetros del dispositivo Cn

Al agregar el dispositivo de control de acceso, puede cambiar los parámetros del dispositivo de control de acceso (controlador de acceso), puntos de control de acceso (puerta o calle), entradas de alarma, salidas de alarma, lectores de tarjetas y controlador de carril.

Parámetros CN para el dispositivo de control de acceso

Al agregar el dispositivo de control de acceso, puede cambiar sus parámetros, incluida la superposición de nombres de usuario en la imagen, la carga de imágenes para capturarlas, el guardado de imágenes capturadas, etc.

Antes de comenzar

Agregue un dispositivo de control de acceso al cliente.

Pasos

1. Haga clic en Control de acceso → Función avanzada → Parámetros del dispositivo .

Nota

Si no puede seleccionar el parámetro del dispositivo en la lista de opciones avanzadas, pase el cursor sobre Opciones avanzadas y haga clic para seleccionar el parámetro del dispositivo que se mostrará.

2. Seleccione un dispositivo de acceso para mostrar sus parámetros en la página derecha.
3. Gire el interruptor a ON para habilitar la nctin correspondiente.

Nota

• Los parámetros mostrados pueden variar para los dispositivos de control de acceso rn. • Algunos de los siguientes parámetros no aparecen en la página de acceso básico; haga clic en Más para editar los parámetros.

Redundancia de comunicación RS-485

Debe habilitar este nctin si conecta el lector de tarjetas RS-485 al dispositivo de control de acceso de forma redundante.

Mostrar rostro detectado

Mostrar imagen del rostro al ntictina

mostrar el número de tarjeta

Mostrar el número de tarjeta cuando ntictina

Mostrar persona nmn

Mostrar la persona nrmtin cuando ntictina

Superposición de información de la persona en la imagen

Muestra la identificación de la persona en la imagen capturada.

Aviso de voz: Si

activa esta función, el aviso de voz se activará en el dispositivo. Podrá escucharlo al iniciar sesión en el dispositivo.

Subir imagen con captura vinculada

Sube las imágenes capturadas por la cámara vinculada al sistema mticy Guardar imagen. ft

Captura vinculada

Si habilita esta nctin, puede guardar la imagen capturada por la cámara vinculada al dispositivo.

Presione la tecla para ingresar el número de tarjeta

Si habilita esta nctin, puede ingresar el número de tarjeta presionando la tecla.

Sonda Wi-Fi

Si habilita esta nctin, el dispositivo puede sondear los dispositivos cmmnctin circundantes.

Dirección MAC y cargarla al sistema. Si la dirección MAC coincide con la dirección MAC c, el sistema puede activar la conexión 3G/4G. Si habilita esta conexión, el dispositivo podrá

comunicarse en la red 3G/4G.

NFC nCnn

Si habilita esta nctin, no podrá usar la tarjeta clonada para mejorar la seguridad. ntictina y más

4. Haga clic en

5. Aceptar. n Haga clic en Copiar a y, a continuación, seleccione el dispositivo o los dispositivos de control de acceso en los que desea copiar los parámetros. la página al dispositivo(s) seleccionado(s).

Parámetros Cn para puerta/ascensor

Después de agregar el dispositivo de control de acceso, puede cambiar su punto de acceso (puerta o r) parámetros.

Antes de comenzar

Agregue un dispositivo de control de acceso al cliente.

Pasos

1. Haga clic en Control de acceso → Función avanzada → Parámetros del dispositivo .
2. Seleccione un dispositivo de control de acceso en el panel ft y luego haga clic para mostrar las puertas o el r de dispositivo seleccionado.

3. Seleccione una puerta o r para mostrar sus parámetros en la página derecha. parámetros

4. Edite la puerta o r.

Nota

• Los parámetros mostrados pueden variar para los dispositivos de control de acceso rn. • Algunos de los siguientes parámetros no aparecen en la página de acceso básico; haga clic en Más para editar los parámetros.

Nombre

Edite el nombre del lector de tarjetas como desee.

Contacto de puerta

Puedes configurar el sensor de la puerta para que permanezca cerrado o abierto. Normalmente, permanece cerrado.

Tipo de salida Bn

Puede configurar la salida bn como cerrada o abierta. Normalmente, permanece abierta.
abierto.

Tiempo de puerta cerrada

Al pasar la tarjeta normal y el relé ctin, el temporizador para bloquear la puerta comienza a funcionar.

Abierto extendido norte

El contacto de la puerta se puede habilitar con un retraso apropiado cuando una persona con necesidades de acceso extendido pasa su tarjeta.

Alarma de tiempo de espera por puerta abierta

La alarma se puede activar si la puerta no se ha cerrado durante un período de tiempo determinado. Si se establece en 0, no se activará ninguna alarma.

Bloquear la puerta cuando esté cerrada

La puerta se puede bloquear una vez cerrada incluso si no se alcanza el tiempo de bloqueo de la puerta .

Código de coacción

La puerta se puede abrir con el código de coacción cuando hay coacción. Al mismo tiempo, el cliente puede reportar el evento de coacción.

Supercontraseña La

persona cc puede abrir la puerta con nn la supercontraseña.

Código de despido

Cree un código de descarte que pueda usarse para detener el timbre del lector de tarjetas (ingresando el código de descarte en el teclado).

Nota

• El código de coacción, el supercódigo y el código de despido deben ser rn • El código de coacción, la supercontraseña y el código de despido deben ser rn de la contraseña de ntictin. • La longitud del código de coacción, la supercontraseña y el código de despido depende del dispositivo. Generalmente debe contener de 4 a 8 dígitos.

5. Haga clic en Aceptar. n Haga , y luego seleccione rr() para copiar los parámetros en la página a clic en Copiar a 6. el rr() seleccionado

Nota

La puerta o El estado r rtin n también se copiará al rr() seleccionado.

Parámetros Cn para el lector de tarjetas

Al agregar el dispositivo de control de acceso, puede cambiar sus parámetros del lector de tarjetas.

Antes de comenzar

Agregue un dispositivo de control de acceso al cliente.

Pasos

1. Haga clic en Control de acceso → Función avanzada → Parámetros del dispositivo .
2. En la lista de dispositivos en el pie, haga clic para expandir la puerta, seleccione un lector de tarjetas y podrá editarlo. Parámetros del lector de tarjetas a la derecha.
3. Edite los parámetros básicos del lector de tarjetas en la página Nrmtin básico.

Nota

Los parámetros mostrados pueden variar según el dispositivo de control de acceso. Algunos de los parámetros se listan a continuación. Consulte el manual del usuario del dispositivo para obtener más detalles. Algunos de los siguientes parámetros no aparecen en la página de configuración básica. Haga clic en "Más" para editarlos.

Nombre

Edite el nombre del lector de tarjetas como desee.

Polaridad del LED OK/Polaridad del LED de error/Polaridad del zumbador: Configure la polaridad del LED OK/Polaridad del LED de error/Polaridad del zumbador de la placa base según los parámetros del lector de tarjetas. Generalmente, se adopta el valor predeterminado.

Intervalo mínimo de deslizamiento de tarjeta

Si el intervalo entre pasadas de la misma tarjeta es menor que el valor establecido, la pasada no es válida. Puede configurarlo entre 0 y 255.

Intervalo máximo al ingresar PWD

Al ingresar la contraseña en el lector de tarjetas, si el intervalo entre presionar dos dígitos es mayor que el valor establecido, se borrarán los dígitos que presionó anteriormente.

Alarma de Máx. Fallo m

Habilitar para informar una alarma cuando la lectura de la tarjeta m alcanza el valor establecido.

Máx. veces falla de la tarjeta

Establezca el fallo máximo m de la tarjeta de lectura.

Manipulación norte

Habilite ntimr ctin para el lector de tarjetas.

Comunicarse con el controlador cada

Cuando el dispositivo de control de acceso no puede conectarse con el lector de tarjetas durante un tiempo mayor al establecido, el lector de tarjetas se apagará automáticamente.

Tiempo de

zumbido Configure el tiempo de zumbido del lector de tarjetas. El tiempo disponible varía de 0 a 5999 s. 0 representa cntin zumbido.

Tipo de lector de tarjetas/lector de norte

tarjetas Obtenga el tipo de lector de tarjetas y crtin Son de solo lectura.

Nivel de huella dactilar nn

Seleccione el nivel de rcntin nrrn en la lista desplegable.

Modo nn del lector de tarjetas predeterminado

Ver el lector de tarjetas predeterminado modo ntictin.

Capacidad de huellas dactilares

Ver el número máximo de nrrn disponibles

xn Número de huella dactilar

Ver el número de nrrn existentes en el dispositivo.

Puntaje

El dispositivo calificará la imagen capturada según el ángulo de guiñada, el ángulo de cabeceo y la distancia pupilar. Si la puntuación es inferior al valor cnr, la detección de rostros será incorrecta.

Valor de tiempo de espera de Face nn

Si el tiempo rcntin es mayor que el tiempo cnr, el dispositivo se lo recordará.

Intervalo de cara nn

El intervalo de tiempo entre dos cntin es de 2s. cara rcntin cuando ntictin Por defecto,

Umbral de coincidencia de cara 1:1

Establezca el umbral de coincidencia ntictina mediante el modo de coincidencia 1:1. Cuanto mayor sea el valor, cuando sea menor la tasa de aceptación falsa y mayor la tasa de aceptación falsa cuando ntictina

Nivel de seguridad 1:N

Establezca el nivel de seguridad correspondiente ntictina a través del modo de coincidencia 1:N. Cuanto mayor sea el cuando el valor sea menor, la tasa de aceptación falsa y mayor la tasa de recepción falsa cuando ntictina

Cara viva norte

Habilitar o deshabilitar el live face ctin nctin Si habilita el nctin el dispositivo puede reconocer si la persona está viva o no.

Cara viva n Nivel de seguridad

ftr habilitando Live Face ctin nctin puede configurar el nivel de seguridad correspondiente cuando actuando en vivo ntictina

Máx. Falló m para autenticación facial.

Establezca el máximo de minutos ctin falló m El sistema bloqueará la cara del usuario durante 5 de cara en vivo si la cara en vivo ctin ha fallado por más de cnr m Lo mismo

El usuario no ntic A través de la cara falsa en 5 minutos. En esos 5 minutos, el usuario...

poder puede ntic A través de la cara real dos veces cntiny para desbloquear.

Bloqueo nn Cara fallida

ftr habilitando Live Face ctin falla ctin nctin el sistema bloqueará la cara del usuario durante 5 minutos si la cara en vivo por más de cnr m Lo mismo

el usuario no puede ntic A través de la cara falsa en 5 minutos. En esos 5 minutos, el usuario...

poder ntic A través de la cara real dos veces cntiny para desbloquear.

Modo n

Puede seleccionar el modo interior u otros modos ctin según el entorno real.

4. Haga clic en Aceptar.

5. n Haga clic en Copiar a y, a continuación, seleccione el/los lector(es) de tarjetas a los que desea copiar los parámetros en la página. el(los) lector(es) de tarjetas seleccionados.

Parámetros Cn para salida de alarma

Después de agregar el dispositivo de control de acceso, si el dispositivo se vincula a las salidas de alarma, puede cnr el parámetros.

Antes de empezar

Agregue un dispositivo de control de acceso al cliente y asegúrese de que el dispositivo admita la salida de alarma.

Pasos

1. Haga clic en Control de acceso → Función avanzada → Parámetros del dispositivo para ingresar al control de acceso. parámetro cnrtin página.
2. En la lista de dispositivos en el pie, haga clic para expandir la puerta, seleccione una entrada de alarma y podrá editar Los parámetros de entrada de alarma a la derecha.
3. Configure los parámetros de salida de alarma.

Nombre

Edite el nombre del lector de tarjetas como desee.

Salida de alarma v Tiempo

¿Cuánto tiempo durará la salida de alarma una vez activada?

4. Haga clic

5. en Aceptar. n Coloque el interruptor en la esquina superior derecha en ON para activar la salida de alarma.

Parámetros Cn para el controlador de carril

Al agregar el controlador de carril al cliente, puede cambiar sus parámetros para pasar por el carril.

Antes de comenzar

Agregue un dispositivo de control de acceso al cliente.

Pasos

1. Haga clic en Control de acceso → Función avanzada → Parámetro del dispositivo para ingresar el parámetro página.
2. En la lista de dispositivos en la parte inferior, seleccione un controlador de carril y podrá editarlo. parámetros a la derecha.
3. Edite los parámetros.

Modo de pase

Seleccione el controlador que controlará el estado de la barrera del dispositivo.

- Si selecciona Según el DIP n del controlador de carril, el dispositivo seguirá el carril n para controlar la barrera. DIP del controlador n en el ftwr no será válido. n de
- Si selecciona Según n del controlador principal, el dispositivo seguirá la n del controlador de carril y no El ftwr para controlar la barrera. El DIP será válido.

Paso libre nn

Si habilita esta nctin cuando el modo de barrera de entrada y salida está en Permanecer abierto, los peatones deberían activarse. ntic cada vez que pasa por el carril. O sonará una alarma.

Velocidad de apertura/cierre de la barrera

Establezca la velocidad de apertura y cierre de la barrera. Puede seleccionar entre 1 y 10. Cuanto mayor sea el valor, mayor será la velocidad.

Nota

El valor recomendado es 6.

Aviso audible

Establezca cuánto durará el audio que se reproduce cuando se activa una alarma.

Nota

0 se refiere a que el audio de la alarma se reproducirá hasta que finalice la alarma.

Unidad de temperatura

Seleccione la unidad de temperatura que se muestra en el estado del dispositivo.

4. Haga clic en Aceptar.

8.7.2 Otros parámetros de Cn

Al agregar el dispositivo de control de acceso, puede configurar sus parámetros, como parámetros de red, parámetros de captura, parámetros RS-485, parámetros Wiegand, etc.

Establecer parámetros para la terminal Face nn

Para la terminal face rcntin, puede configurar sus parámetros, incluida la base de datos de imágenes faciales y el código QR. ntictina etc.

Pasos

Nota

El dispositivo debería ser compatible con esta nctin.

1. Ingrese al módulo de Control de Acceso.
2. En la barra nvtin de la parte inferior, ingrese Función avanzada → Más parámetros .
3. Seleccione un dispositivo de control de acceso en la lista de dispositivos y haga clic en Terminal Face nn.
4. Establezca los parámetros.

Nota

Estos parámetros mostrados varían según los modelos de dispositivo rn.

COM

Seleccione un puerto COM para cnrtin COM1 se refiere a la interfaz RS-485 y COM2 se refiere a la interfaz RS-232.

Base de datos de imágenes de rostros

Seleccione Deep Learning como base de datos de imágenes faciales.

nortio por código QR

Si está habilitado, la cámara del dispositivo puede escanear el código QR si ntic Por defecto, el nctin está deshabilitado.

Lista de bloqueo nn

Si está habilitado, el dispositivo comparará a la persona que desea acceder con las personas en la lista de bloqueo.

Si coincide (la persona está en la lista de bloqueo), se denegará el acceso y el dispositivo cargará una alarma al cliente.

Si no coincide (la persona no está en la lista de bloqueo), se concederá el acceso.

Guardar imagen de cara nn

Si está habilitado, la imagen del rostro capturado cuando ntictin se guardará en el dispositivo.

Versión MCU

Ver la versión MCU del dispositivo.

5. Haga clic en Guardar.

Establecer parámetros RS-485

Puede configurar los parámetros RS-485 del dispositivo de control de acceso, incluidos la velocidad en baudios, el bit de datos, el bit de parada, el tipo de paridad, el tipo de control w, el modo cmmnctin, el modo de trabajo y el modo cnnctin.

Antes de comenzar

Agregue el dispositivo de control de acceso al cliente y asegúrese de que el dispositivo admita la interfaz RS-485.

Pasos

1. Ingrese al módulo de Control de Acceso.
2. En la barra nvtin de la parte inferior, ingrese Función avanzada → Más parámetros .
3. Seleccione un dispositivo de control de acceso en la lista de dispositivos y haga clic en RS-485 para ingresar al RS-485 página.
4. Seleccione el número de puerto serie de la lista desplegable para configurar los parámetros RS-485.
5. Configure la velocidad en baudios, el bit de datos, el bit de parada, el tipo de paridad, el modo de comunicación, el modo de trabajo y modo cnnctin en la lista desplegable.

Nota

Cuando el modo de conexión es Conectar dispositivo de control de acceso, puede seleccionar N.° de tarjeta o ID de persona como tipo de salida.

6. Haga clic en Guardar.

• Los parámetros cnr se aplicarán al dispositivo mticy • Cuando cambie el modo de trabajo o el modo cnnctin, el dispositivo se reiniciará

mticy

Establecer parámetros Wiegand

Puede configurar el canal Wiegand del dispositivo de control de acceso y el modo de comunicación. Según los parámetros Wiegand, el dispositivo se puede conectar al lector de tarjetas Wiegand a través del modo de comunicación Wiegand.

Antes de comenzar

Agregue el dispositivo de control de acceso al cliente y asegúrese de que el dispositivo sea compatible con Wiegand.

Pasos

1. Ingrese al módulo de Control de Acceso.
2. En la barra nvtin de ft ingrese Función avanzada → Más parámetros .

3. Seleccione un dispositivo de control de acceso en la lista de dispositivos y haga clic en Wiegand para ingresar al Wiegand n página.
4. Coloque el interruptor en encendido para habilitar Wiegand nctin para el dispositivo.
5. Seleccione el número de canal Wiegand y el modo de comunicación de la lista desplegable.

Nota

Si configura Cmmnn n como Envío, deberá configurar el Modo Wiegand como Wiegand 26 o Wiegand 34.

6. Haga clic en Guardar. • Los parámetros cnr se aplicarán al dispositivo mticy • Al cambiar la cmmnctin rctin, el dispositivo se reiniciará mticy

Habilitar tarjeta M1 nyn

La tarjeta M1 ncrytin puede mejorar el nivel de seguridad de ntictina

Pasos

Nota

El nctin debe ser compatible con el dispositivo de control de acceso y el lector de tarjetas.

1. Ingrese al módulo de Control de Acceso.
2. En la barra nvtin de ft ingrese Función avanzada → Más parámetros .
3. Seleccione un dispositivo de control de acceso en la lista de dispositivos y haga clic en M1 Card nyn para ingresar a la página M1 Card ncrytin.
4. Coloque el interruptor en encendido para habilitar la tarjeta M1 ncrytin nctin 5.

Configure el ID del sector.

El ID del sector varía de 1 a 100.

6. Haga clic en Guardar para guardar el

8.8 Control de puertas y ascensores

En el módulo de Monitoreo, puede ver el estado de las puertas o ascensores gestionados por el dispositivo de control de acceso añadido. También puede controlar las puertas y ascensores, como abrirlas o cerrarlas, o mantenerlas abiertas o cerradas, a través del cliente de forma remota. Los eventos de acceso de Rtim se muestran en este módulo. Puede ver los detalles de acceso y de la persona.

Nota

El usuario con permiso para controlar puertas y ascensores puede acceder al módulo de Monitoreo y controlarlos. De lo contrario, los iconos utilizados para el control no se mostrarán. Para obtener el permiso, en el usuario consulte .

8.8.1 Estado de la puerta de control

Puede controlar el estado de las puertas, incluido desbloquear la puerta, bloquear la puerta, mantener la puerta desbloqueada, mantener la puerta bloqueada, mantener todas desbloqueadas, etc.

Antes de empezar

• Agregue una persona y asigne un permiso de acceso a la persona designada, quien tendrá el permiso de acceso a los puntos de acceso (puertas). Para más detalles, consulte Administración y configuración de personas.

Grupo de acceso para asignar acceso • n a Personas .

Asegúrese de que el usuario rtin tenga permiso para los puntos de acceso (puertas). Para más detalles, consulte a .

Pasos

1. Haga clic en Monitoreo para ingresar a la página de monitoreo de estado.
2. Seleccione un grupo de puntos de acceso en la esquina superior derecha.

Nota

Para administrar el grupo de puntos de acceso, consulte Administración de grupos .

Se mostrarán las puertas del grupo de control de acceso seleccionado.

3. Haga clic en el icono de una puerta para seleccionarla o presione Ctrl y seleccione puertas mti.

Nota

Para permanecer todo desbloqueado y permanecer todo bloqueado, ignore este paso.

4. Haga clic en el siguiente bn para controlar la puerta.

Descubrir

Cuando la puerta esté bloqueada, desbloquéela y se abrirá por una vez. Después de abrirla, la puerta se cerrará y se bloqueará nuevamente.

Cerrar

Cuando la puerta esté desbloqueada, bloquéela y se cerrará. La persona que tiene el acceso rtin puede acceder a la puerta con crnti

Permanecer desbloqueado

La puerta estará desbloqueada (no se puede abrir ni cerrar). Cualquier persona podrá acceder sin necesidad de contraseña.

Permanecer bloqueado

La puerta estará cerrada con llave. Nadie podrá acceder, incluso con la credencial autorizada, excepto los superusuarios.

Permanecer todo desbloqueado

Todas las puertas del grupo estarán desbloqueadas (no se podrán abrir ni cerrar). Todos podrán acceder a ellas sin necesidad de contraseña.

Permanecer todo bloqueado

Todas las puertas del grupo estarán cerradas con llave. Nadie podrá acceder a ellas, incluso con la credencial autorizada, excepto los superusuarios.

Captura

Capturar una imagen manualmente.

Nota

La captura bn está disponible cuando el dispositivo admite la captura nctin. La imagen se guarda en la PC que ejecuta el cliente. Para En la ruta de guardado, consulte .

Resultado

El icono de las puertas cambiará en rtim de acuerdo al rtin si el rtin es exitoso.

8.8.2 Verificar registros de acceso en tiempo real

Los registros de acceso rtim se pueden mostrar en el cliente, incluidos registros de deslizamiento de tarjetas, registros de reconocimiento facial, registros de temperatura de la superficie de la piel, etc. Además, puede ver el registro de la persona y ver la imagen capturada durante el acceso.

Antes de empezar, ha

añadido personas y dispositivos de control de acceso al cliente. Para más información, consulte " Administración de personas y añadir dispositivos" .

Pasos

1. Haga clic en Monitoreo para ingresar al módulo de monitoreo.

Los registros de acceso temporal se muestran en la base de datos de la página. Puede ver los detalles del registro y el incluyendo número de tarjeta, nombre de la persona, hora del evento, temperatura de la puerta, tipo de ntictin. etc.

Figura 8-4 m Registros de acceso

Nota

Puede hacer clic derecho en el nombre de la columna de la tabla de eventos de acceso para mostrar u ocultar la columna según las necesidades reales.

2. n Seleccione un grupo de puntos de acceso de la lista desplegable en la esquina superior derecha para Mostrar los registros de acceso en tiempo real del grupo seleccionado.
3. n Verifique el tipo de evento y el estado del evento.

   Los eventos detectados con tipo y estado verificados se mostrarán en la lista a continuación.
4. n Marque Mostrar último evento para ver el último registro de acceso.

   La lista de registros se ordenará en orden cronológico inverso.
5. n Marque Habilitar aviso de temperatura anormal para habilitar la temperatura anormal de la superficie de la piel. Indicador de temperatura.

   Nota

   Cuando está habilitado, si hay una temperatura anormal, se activa un aviso de temperatura anormal.
   Aparece una ventana cuando ingresas al módulo de Monitoreo, mostrando la foto de la persona y la superficie de la piel. temperatura, número de tarjeta, nombre de la persona, etc.
6. n Haga clic en un evento para ver fotos de personas (incluidas fotos capturadas y r)

   Nota

   En la imagen de captura vinculada . Puede hacer doble clic en la imagen capturada para verla ampliada.
7. n Haga clic para ver los detalles de monitoreo (incluida la información detallada de la persona y el imagen capturada).

   Nota

   En la ventana emergente, puede hacer clic para ver los detalles de monitoreo en pantalla completa.

Apéndice A. Interruptor DIP

A.1 Interruptor DIP

norte

El interruptor DIP está en la placa de control de acceso. Los números 1 y 2 van del bit bajo al bit alto.

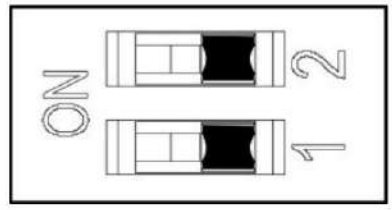


Figura A-1 Interruptor DIP

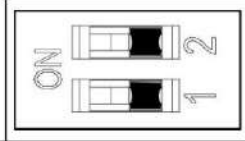
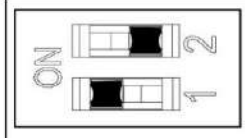
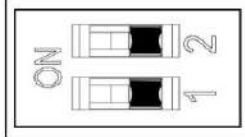
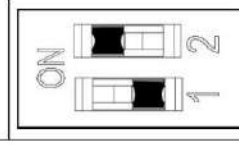
Cuando el interruptor está en la posición ON, significa que el interruptor está habilitado, de lo contrario, el interruptor está en la posición ON.

A.2 Interruptor DIP Fnn correspondiente

Nota

ftr En el interruptor DIP, debe reiniciar el dispositivo o el nctin no podrá tomar do

Los interruptores DIP de 2 bits correspondientes a nctin en la placa de control de acceso son los siguientes:

Poco	Valor decimal de Fnn del modo de dispositivo			Interruptor DIP Diagrama de direcciones
1	Modo de trabajo	Modo normal 0		
		Modo de estudio	1	
2	Emparejamiento de llavero Modo	Desactivar llavero Modo de emparejamiento	0	
		Habilitar llavero Modo de emparejamiento	1	

Apéndice B. Activacion

Consulte la tabla a continuación para conocer la activación del dispositivo a través de bn en el tablero de control del carril principal.

CNN de nivel 1 No.	norte	Número y fin de CNN de nivel 1	Notas
1	Modo de estudio	1-Salir del modo de estudio/ Modo normal Modo 2-Estudio Nota De forma predeterminada, se mostrará 1 en la pantalla.	Si el dispositivo está equipado con una placa de control de acceso, solo se puede configurar mediante el interruptor DIP.
2	Modo de emparejamiento del llavero	1: Modo normal Modo de emparejamiento 2 Nota De forma predeterminada, se mostrará 1 en la pantalla.	Si el dispositivo está equipado con una placa de control de acceso, solo se puede configurar mediante el interruptor DIP.
3	Modo de pase	1-Ambos lados bajo control Nota De forma predeterminada, se mostrará 1 en la pantalla. 2-Entrada bajo control; salida prohibida 3-Entrada bajo control; salida en modo nctiv 4-Ambos lados en modo nctiv	

CNN de nivel 1 No.	norte	Número y fin de CNN de nivel 1	Notas
		5-Entrada en modo nctiv; salida bajo control 6-Entrada en modo nctiv; salida prohibida 7-Ambas partes prohibidas 8-Entrada prohibida; salida bajo control 9-Entrada prohibida; salida en modo nctiv 10-Entrada bajo control; salida restante abierto 11-Entrada bajo control; salida en modo libre 12-Entrada en modo nctiv; la salida permanece abierta 13-Entrada en modo nctiv; salida en modo libre 14-Entrada prohibida; salida abierta 15-Entrada prohibida; salida en modo libre 16-Entrada abierta; salida bajo control 17-Entrada abierta; salida en modo nctiv	

CNN de nivel 1 No.	norte	Número y fin de CNN de nivel 1	Notas
		18-Entrada abierta; salida abierta abierto 19-Entrada abierta; salida en modo libre 20-Entrada abierta; salida prohibida 21-Entrada en modo libre; salida bajo control 22-Entrada en modo libre; salida en modo nctiv 23-Entrada en modo libre; salida permaneciendo abierta 24-Entrada en modo libre; salida en modo libre 25-Entrada en modo libre; salida prohibida	
4	Modo de memoria	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 2 en la pantalla.	
5	Control remoto llavero 1-uno a uno	2-uno a mti Nota De forma predeterminada, se mostrará 1 en la pantalla.	

CNN de nivel 1 No.	norte	CNN de nivel 1 No. y Fnn	Notas
6	Velocidad de apertura de la barrera	1-1, 2-2, …10-10 Nota Por defecto, será 5 se muestra en el pantalla de visualización.	
7	Velocidad de cierre de barrera	1-1, 2-2, …10-10 Nota Por defecto, será 5 se muestra en el pantalla de visualización.	
8	Lectura de cartas en el Área de alarma	1-No abrir 2-Abierto Nota Por defecto, 2 será se muestra en el pantalla de visualización.	
9	Ingrese rtin	5-5s, 6-6s, 7-7s, ..., 60- Años 60 Nota Por defecto, será 5 se muestra en el pantalla de visualización.	
10	Salir de la entrada	5-5s, 6-6s, 7-7s, ..., 60- Años 60 Nota Por defecto, será 5 se muestra en el pantalla de visualización.	
11	Detección IR rtin	0-0s,1-1s,2-2s,..., 25- 25 años	

CNN de nivel 1 No.	norte	CNN de nivel 1 No. y Fnn	Notas
		Nota De forma predeterminada, será 0 se muestra en el pantalla de visualización.	
12	Intrusión rtin	0-0s, 1-1s, 2-2s,..., 20-años 20 Nota De forma predeterminada, será 0 se muestra en el pantalla de visualización.	
13	Exceso de estancia	0-0s, 1-1s, 2-2s,..., 20-años 20 Nota De forma predeterminada, será 0 se muestra en el pantalla de visualización.	
14	Tiempo de retardo para la barrera Cierre	0-0s, 1-1s, 2-2s, 3-3s, 4-4s, 5-5s Nota De forma predeterminada, será 0 se muestra en el pantalla de visualización.	
15	Modo de control	1 mil millones de Cnrtin Interruptor 2-DIP en el acceso Tablero de control Nota Por defecto, 1 será se muestra en el pantalla de visualización.	
18	Número de carril	1-Carriles dobles	No se puede cambiar

CNN de nivel 1 No.	norte	Número y fin de CNN de nivel 1	Notas
		2-Carril único Nota De forma predeterminada, se mostrará 1 en la pantalla.	
19	Motor estaño	1-En sentido horario 2nticcw Nota De forma predeterminada, se mostrará 1 en la pantalla.	No se puede cambiar
21	Volumen	1-0, 2-1, 3-2, 4-3, 5-4 Nota De forma predeterminada, se mostrará 2 en la pantalla.	El dispositivo se silenciará cuando se configure en "1".
22	ntic	Pasando 1-Deshabilitar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	No se puede cambiar a través de bn
23	Número de tarjeta no válido	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	No se puede cambiar a través de bn

CNN de nivel 1 No.	norte	Número y fin de CNN de nivel 1	Notas
24	Huella dactilar no coincidente 1-	Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	No se puede cambiar a través de bn
25	Escalar la barrera 1 - Desactivar	2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	
26	Pase inverso	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	
27	Superando el paso rtin	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	
28	Alarma de intrusión	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	

CNN de nivel 1 No.	norte	Número y fin de CNN de nivel 1	Notas
29	Paso forzado	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	No se puede cambiar a través de bn
30	Alarma de estaño	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	
31	Paso no autorizado	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	No se puede cambiar a través de bn
32	Exceder la dosis de ntictin	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	No se puede cambiar a través de bn
33	Fallido ntictin	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	No se puede cambiar a través de bn

CNN de nivel 1 No.	norte	Número y fin de CNN de nivel 1	Notas
34	Crnti vencido	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	No se puede cambiar a través de bn
35	Alarma de sobrepasar el límite de permanencia	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 1 en la pantalla.	
36	Material de barrera	1-Acrílico 2-Acero inoxidable 3 vasos	
37	Longitud de la barrera	1-550 2-600 3-650 4-700 5-750 6-800 7-850 8-900 9-950 10-1000 11-1100 12-1200 13-1300 14-1400	

CNN de nivel 1 No.	norte	Número y fin de CNN de nivel 1	Notas
		Nota De forma predeterminada, se mostrará 8 en la pantalla.	
38	Nctina motora	1-Desactivar 2-Habilitar en carril principal 3-Habilitar en subcarril Nota De forma predeterminada, se mostrará 1 en la pantalla.	
39	Brillo de la luz	0-0, 1-1, 2-2, …, 10- 10 Nota De forma predeterminada, se mostrará 3 en la pantalla.	Cuanto mayor sea el valor, más brillante será la luz.
40	Voz de autocomprobación Inmediato	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 2 en la pantalla.	
41	Voz en modo estudio Inmediato	1-Desactivar 2-Habilitar Nota De forma predeterminada, se mostrará 2 en la pantalla.	

CNN de nivel 1 No.	norte	CNN de nivel 1 No. y Fnn	Notas
42	do	4-4,6-6,8-8, Nota Por defecto, 4 será se muestra en el pantalla de visualización.	No se puede cambiar a través de bn
43	Modo ctin	1-A prueba de viento 2-Interior Por defecto, 1 será se muestra en el pantalla de visualización.	
44	Recuperación de barrera rtin	1-Velocidad normal 2-Recuperación rápida Por defecto, 1 será se muestra en el pantalla de visualización.	
45	Freno	1-Desactivar Estaño de 2 barreras xctina 3-Intrusión Por defecto, 2 será se muestra en el pantalla de visualización.	
46	Ángulo de freno	1-5° 2-10° 3-15° Por defecto, 1 será se muestra en el pantalla de visualización.	
47	Detección por infrarrojos	1-Disparado único 2-Disparado Simultáneamente	

CNN de nivel 1 No.	norte	Número y fin de CNN de nivel 1	Notas
		De forma predeterminada, se mostrará 1 en la pantalla.	
48	Admirador	1-Discapacitado 2-Habilitado De forma predeterminada, se mostrará 2 en la pantalla.	
49	Altura de la barrera	1-700 2-1200 3-1400 4-1600 5-1800 De forma predeterminada, se mostrará 5 en la pantalla.	
99	Restaurar a valores predeterminados	1- Predeterminado 2- Inicio Nota De forma predeterminada, se mostrará 1 en la pantalla.	

Apéndice C. Tipos de eventos y alarmas

Evento	Tipo de alarma
estaño	Visual y audible
Pase inverso	Visual y audible
Acceso forzado	Ninguno
Escalar la barrera	Visual y audible
Permanecer demasiado tiempo	Visual y audible
Pase de tiempo muerto	Ninguno
Intrusión	Visual y audible
Pase libre ntictin falló	Visual y audible
Barrera obstruida	Ninguno

Apéndice D. Tabla de índice de audio Contenido relacionado

Nota

- Si el dispositivo no está equipado con una placa de control de acceso, el altavoz se debe conectar a La placa de interfaz extendida principal.
- Si el dispositivo está equipado con una placa de control de acceso, el altavoz se debe conectar a la Panel de control de acceso. Puede configurar un contexto de brctin personalizado a través de la web.

Contenido
Escalando la barrera.
Pase inverso.
El paso del tiempo
Intrusión.
estaño
Permanecer demasiado tiempo.

Apéndice E. Código de error

norte

La barrera abatible mostrará el código de error en la pantalla de siete segmentos si se produjo un error. Consulte a la tabla de abajo para n la crtin de cada numero.

Motivo del error	Código	Motivo del error	Código
El primer haz de infrarrojos activado	01	El decimotercer haz de infrarrojos Motivado	13
El segundo haz de infrarrojos se activó	02	El decimocuarto haz de infrarrojos Motivado	14
Se activó el tercer haz de infrarrojos	03	Tablero indicador de tictina (Entrada) ffln	49
El cuarto haz de infrarrojos se disparó	04	Tablero indicador de tictina (Salida) ffln	50
El haz de infrarrojos ft se activa	05	Placa adaptadora IR ffln	51
Se activó el sexto haz de infrarrojos	06	nrcnnctin xctin	53
El séptimo haz de infrarrojos se activó	07	No estudiar	54
El octavo haz de infrarrojos se activó	08	brctin	55
Se activó el noveno haz de infrarrojos	09	Exceder el rango de estudio	56
Se activó el décimo haz de infrarrojos	10	Codificador xctin	57
El undécimo haz de infrarrojos se activó	11	Extractor de motor	58
El haz de infrarrojos wft se disparó	12	Placa de interfaz extendida ffln (Si el tablero no está instalado, el código de error de "49" aparecerá pero el dispositivo nctin normalmente)	59

Apéndice F. Matriz y comando de dispositivo

Matriz Cmmnn

Escanee el siguiente código QR para obtener la matriz de cmmnctin del dispositivo.

Tenga en cuenta que la matriz contiene todos los puertos de comunicación de los dispositivos de control de acceso y videoportero de Hikvision.

Figura F-1 Código QR de la matriz Cmmnn

Comando de dispositivo

Escanee el siguiente código QR para obtener los comandos del puerto serie común del dispositivo.

Tenga en cuenta que la lista de comandos contiene todos los comandos de puertos seriales comúnmente utilizados para todos los dispositivos de control de acceso y videoportero de Hikvision.

Figura F-2 Comando del dispositivo

ventas@rosarioseguridad.com.ar
+54 9 341 6708000
+54 9 341 6799822

rosarioseguridadok
Rosario Seguridad
Rosario Seguridad

Grupo Instaladores
https://www.facebook.com/groups/591852618012744/
+54 9 341 6591429
+54 9 341 4577532

Avenida Pellegrini 4820-Presidente Perón 3998
Rosario - Santa Fe - Argentina