Controlador de acceso

Guía de inicio rápido

V1.0.1

Prefacio

General

Este manual presenta la instalación y las operaciones básicas del controlador de acceso (en adelante, el "Dispositivo").

Las instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con un significado definido pueden aparecer en el manual.

Palabras de advertencia	Significado
 **PELIGRO**	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
 **ADVERTENCIA**	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 **PRECAUCIÓN**	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
 **NOTA**	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.1	Añadido proceso de inicialización.	diciembre 2021
V1.0.0	Primer lanzamiento.	agosto 2020

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcione la información de contacto requerida.

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.

- No somos responsables de las pérdidas sufridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si se produce algún problema durante el uso del dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del Dispositivo, la prevención de riesgos y prevención de daños a la propiedad. Lea atentamente antes de usar el Dispositivo, cumpla con las pautas cuando lo utilice y guarde el manual en un lugar seguro para consultarlo en el futuro.

Requisito de transporte

Transporte el Dispositivo en condiciones de humedad y temperatura permitidas.

Requisito de almacenamiento

Guarde el dispositivo en condiciones de humedad y temperatura permitidas.

requerimientos de instalación

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con el código y las normas locales de seguridad eléctrica. Asegúrese de que el voltaje ambiental sea estable y cumple con los requisitos de suministro de energía del dispositivo.
- No conecte el Dispositivo a dos o más tipos de fuentes de alimentación, para evitar daños al Dispositivo.
- El uso inadecuado de la batería puede provocar un incendio o una explosión.

- El personal que trabaje en alturas debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluidas usando casco y cinturones de seguridad.
- No coloque el Dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo en una superficie estable para evitar que se caiga.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o una fuente de alimentación de gabinete proporcionada por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumpla con la potencia nominal especificaciones.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en la norma IEC 62368-1 y no ser más alto que PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del dispositivo.

- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectado a una toma de corriente con puesta a tierra de protección.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de usar.
- No desconecte el cable de alimentación del lateral del dispositivo mientras el adaptador está encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Utilice el dispositivo en condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquido sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido. en el dispositivo para evitar que el líquido fluya hacia él.
- No desmonte el dispositivo sin instrucción profesional.

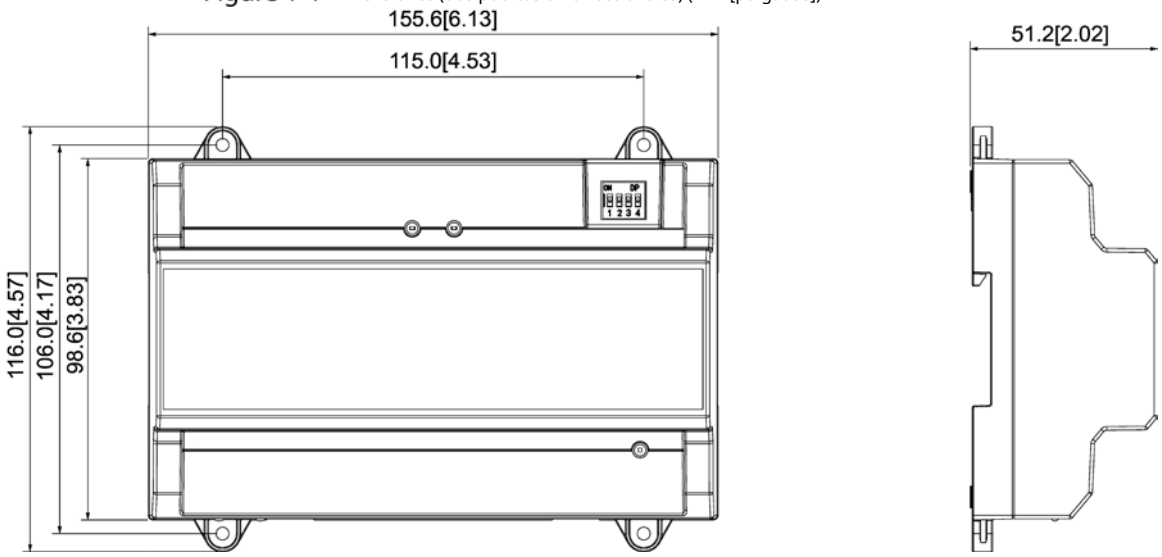
Tabla de contenido

El Dispositivo es un panel de control de acceso que compensa la videovigilancia y la intercomunicación visual. Tiene un diseño limpio y moderno con una gran funcionalidad, adecuado para edificios comerciales de alta gama, propiedades grupales y comunidades inteligentes.

1.1 Dimensiones

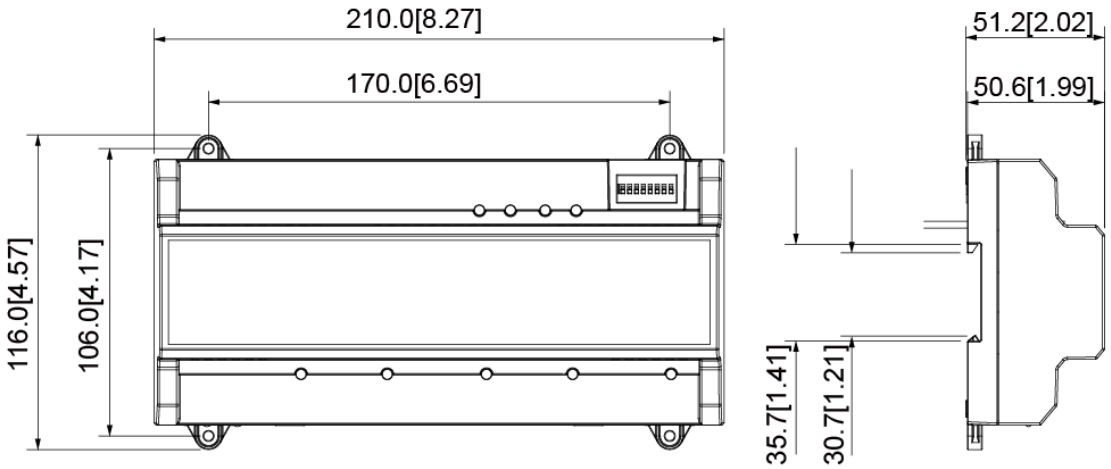
Controlador de acceso unidireccional de dos puertas

Figure 1-1 Dimensiones (dos puertas unidireccionales) (mm [pulgadas])



Controlador de acceso bidireccional de dos puertas/unidireccional de cuatro puertas

Figure 1-2 Dimensiones (dos puertas de dos vías/cuatro puertas de una vía) (mm [pulgadas])



1.2 Componentes

Controlador de acceso unidireccional de dos puertas

Figure 1-3 Componentes (dos puertas unidireccionales)

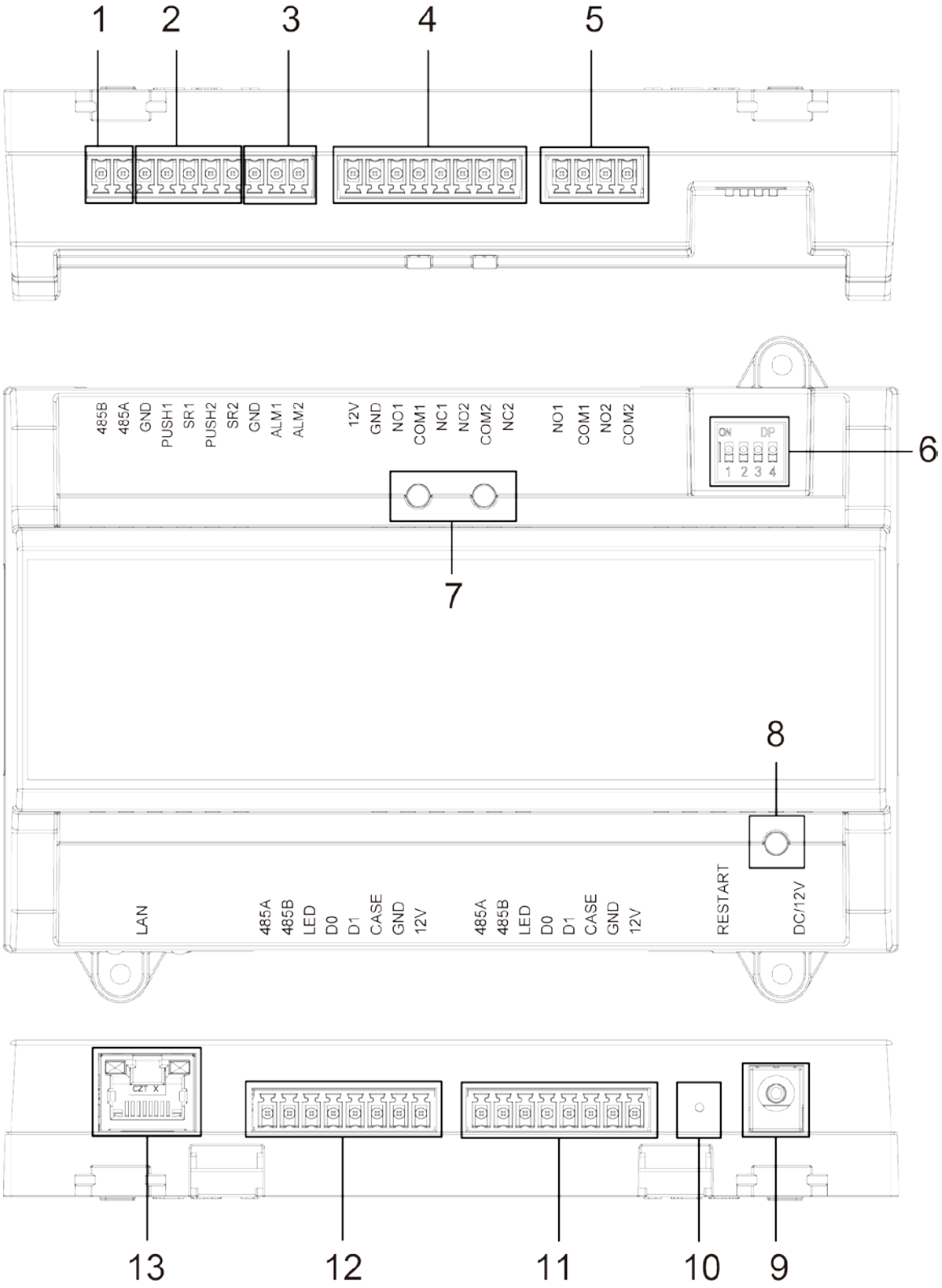


Tabla 1-1 Descripción de los componentes (dos puertas unidireccionales)

No.	Nombre	No.	Nombre
1	Puerto RS-485	8	Luz indicadora de poder
2	Botón de salida/puerto de contacto de puerta	9	Puerto de alimentación

3	Puerto de entrada de alarma	10	Botón de reinicio
4	Puerto de SALIDA de bloqueo de puerta	11	Puerto de lector de tarjetas de entrada de la puerta No.2
5	Puerto de SALIDA de alarma	12	Puerto de lector de tarjetas de entrada de la puerta No.1
6	Dip switch	13	puerto de red
7	Luz indicadora de la cerradura de la puerta	14	—

Controlador de acceso bidireccional de dos puertas

Figure 1-4 Componentes (dos puertas de dos vías)

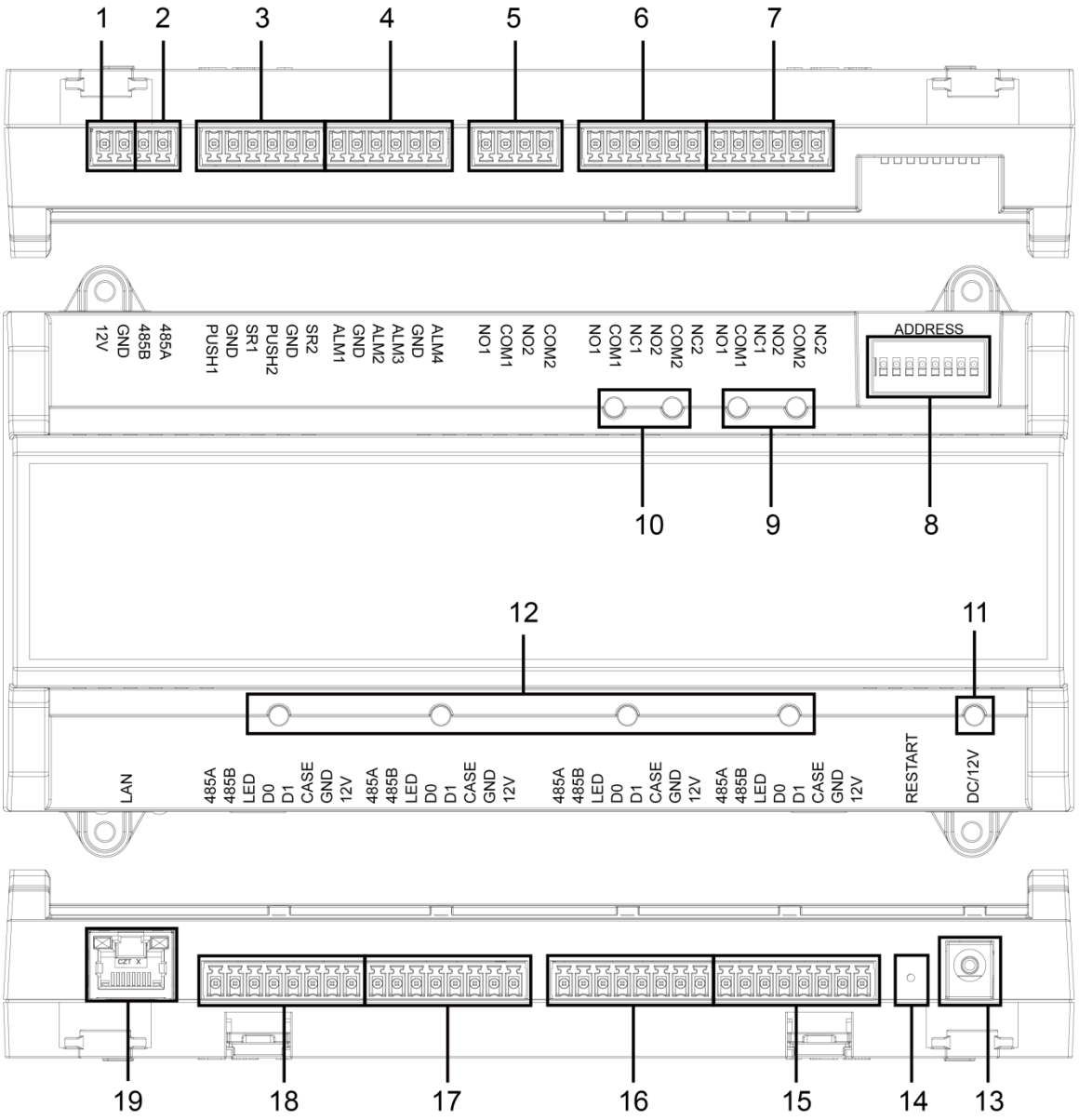


Tabla 1-2 Descripción de los componentes (dos puertas y dos vías)

No.	Nombre	No.	Nombre
1	Puerto de alimentación de bloqueo de puerta	11	Luz indicadora de poder
2	Puerto RS-485	12	Luz indicadora del lector de tarjetas
3	Botón de salida/puerto de contacto de puerta	13	Puerto de alimentación
4	Puerto de entrada de alarma externa	14	Botón de reinicio
5	Puerto de SALIDA de alarma externa	15	Salida del puerto del lector de tarjetas de la puerta No.2
6	Puerto de SALIDA de control de bloqueo de puerta	dieciséis	Puerto de lector de tarjetas de entrada de la puerta No.2

7	SALIDA de alarma interna	17	Salida del puerto del lector de tarjetas de la puerta No.1
8	Dip switch	18	Puerto de lector de tarjetas de entrada de la puerta No.1
9	Luz indicadora de alarma	19	puerto de red
10	Luz indicadora de bloqueo de puerta	—	—

Controlador de acceso unidireccional de cuatro puertas

Figure 1-5 Componentes (cuatro puertas unidireccionales)

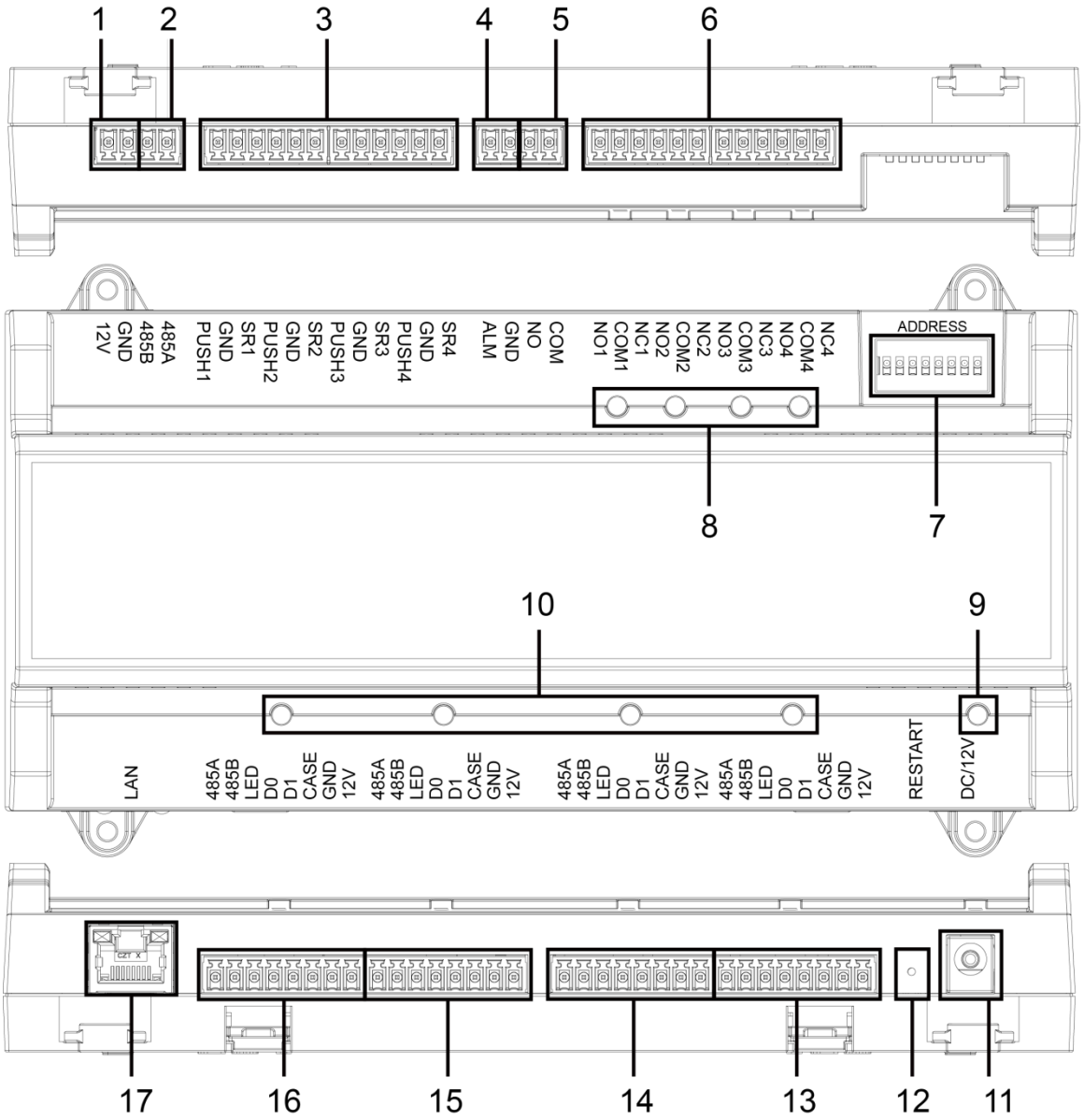


Tabla 1-3 Descripción de los componentes (cuatro puertas unidireccionales)

No.	Nombre	No.	Nombre
1	Puerto de alimentación de bloqueo de puerta	10	Luz indicadora del lector de tarjetas
2	Puerto RS-485	11	Puerto de alimentación
3	Botón de salida/puerto de contacto de puerta	12	Botón de reinicio
4	Puerto de entrada de alarma	13	Puerto de lector de tarjetas de entrada de la puerta No.4
5	Puerto de SALIDA de alarma	14	Puerto de lector de tarjetas de entrada de la puerta No.3
6	Puerto de SALIDA de control de bloqueo de puerta	15	Puerto de lector de tarjetas de entrada de la puerta No.2

7	Dip switch	dieciséis	Puerto de lector de tarjetas de entrada de la puerta No.1
8	Luz indicadora de bloqueo de puerta	17	puerto de red
9	Luz indicadora de poder	—	—

Puerto

Puerto autoadaptable de 10/100 Mbps y compatible con fuente de alimentación PoE.

Luz indicadora

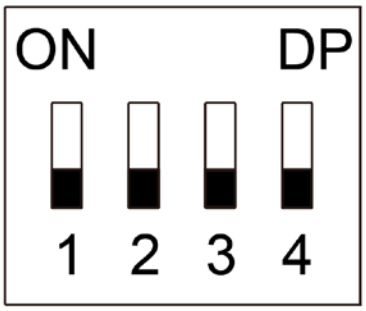
- Luz indicadora de poder
  - ◇ Verde: Funciona normalmente.
  - ◇ Rojo: Anomalía de energía.
  - ◇ Azul: Actualización.
- Luz indicadora de alarma
  - ◇ Encendido: se activa la alarma. Apagado:
  - ◇ la alarma no se dispara. Luz indicadora
- de cerradura de puerta
  - ◇ Encendido: la cerradura de la puerta está conectada.
  - ◇ Apagado: la cerradura de la puerta no está
- conectada. Lector de tarjetas Luz indicadora
  - ◇ Encendido: El lector de tarjetas está conectado.
  - ◇ Apagado: el lector de tarjetas no está conectado.

Dip switch

Realice la operación correspondiente a través del interruptor DIP.

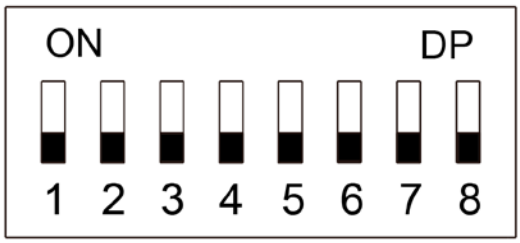
 Medios 1;  significa 0.

Figure 1-6 Interruptor DIP (controlador de acceso unidireccional de dos puertas)



- 1–4 son todos 0, el dispositivo se inicia normalmente después del encendido. 1–4 son
- todos 1, el dispositivo ingresa al modo de inicio después del encendido.
- 1 y 3 son 1, 2 y 4 son 0, el dispositivo se restaura a los valores predeterminados de fábrica después de reiniciar.
- 2 y 4 son 1, 1 y 3 son 0, el dispositivo se restaura a los valores predeterminados de fábrica después de reiniciar. Pero la información del usuario se conservará.

Figure 1-7 Interruptor DIP (controlador de acceso de dos puertas de dos vías/cuatro puertas de una vía)



- 1–8 son todos 0, el dispositivo se inicia normalmente después del encendido. 1–8 son
- todos 1, el dispositivo ingresa al modo de inicio después del encendido.
- 1, 3, 5 y 7 son 1, 2, 4, 6 y 8 son 0, el dispositivo se restaura a los valores predeterminados de fábrica después de reiniciar.
- 1, 2, 4, 6 y 8 son 1, 1, 3, 5 y 7 son 0, el dispositivo se restaura a los valores predeterminados de fábrica después de reiniciar. Pero

la información del usuario será retenida.

Reiniciar

Inserte una aguja en el orificio de REINICIO y presiónela para reiniciar el dispositivo.

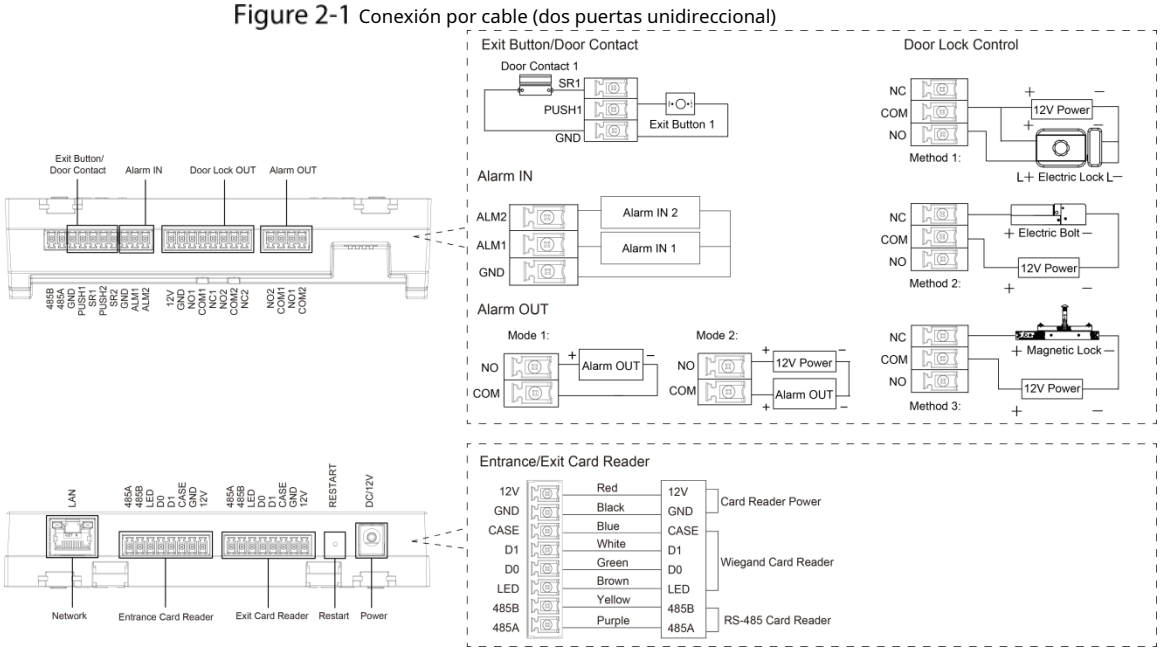
El botón de reinicio es para reiniciar el dispositivo, en lugar de modificar la configuración.

2 Instalación

2.1 Conexión de cable

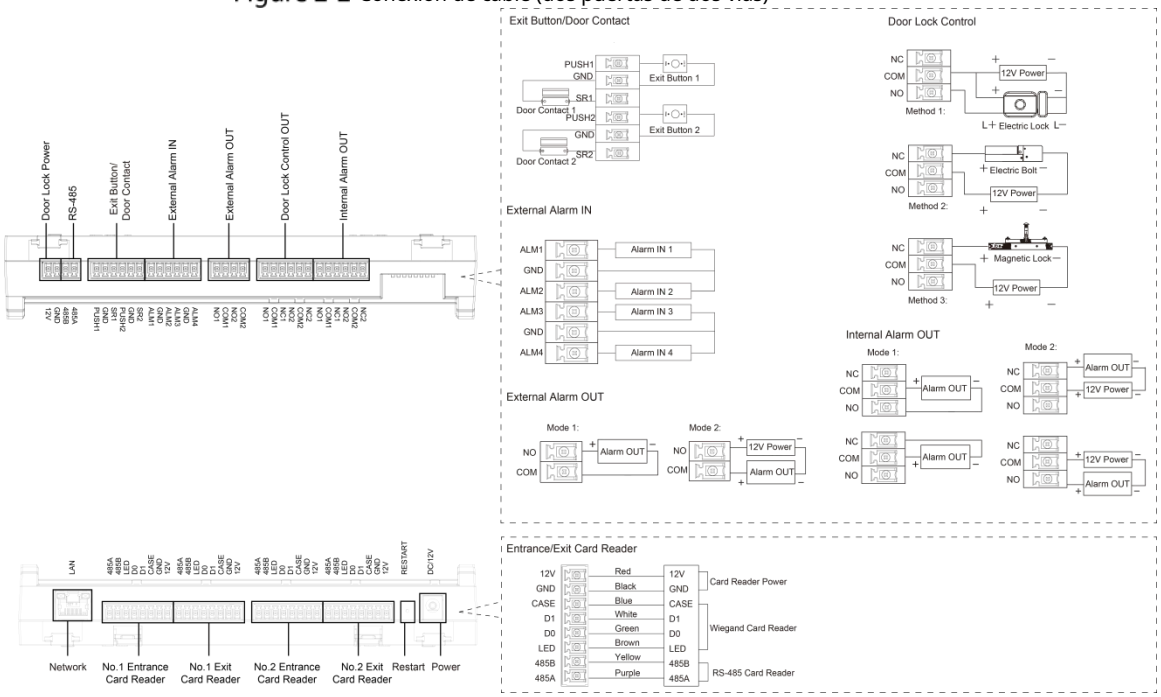
Controlador de acceso unidireccional de dos puertas

Figure 2-1 Conexión por cable (dos puertas unidireccional)



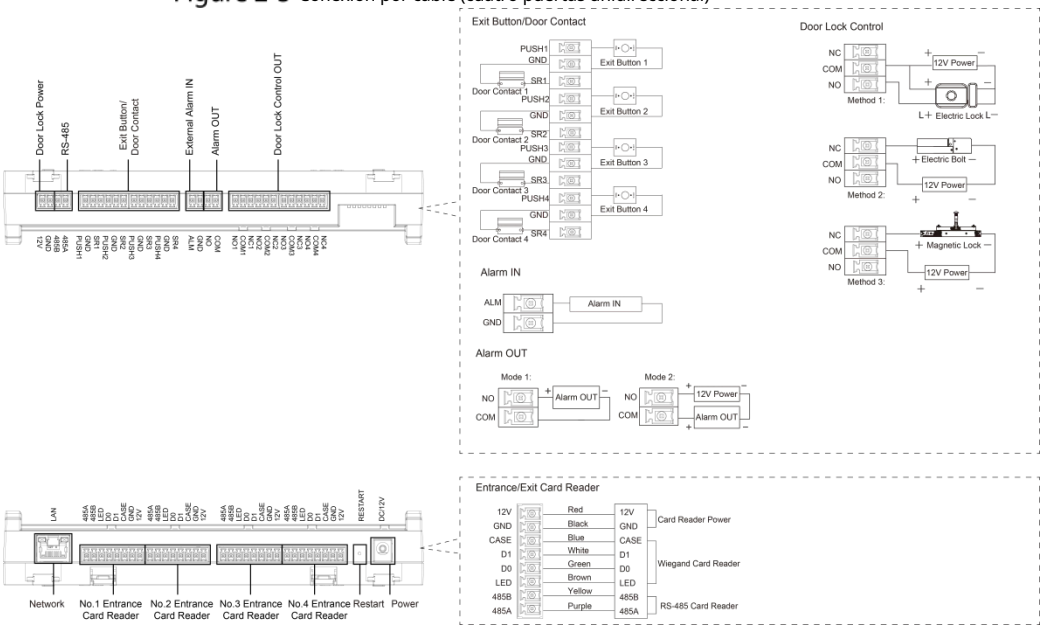
Controlador de acceso bidireccional de dos puertas

Figure 2-2 Conexión de cable (dos puertas de dos vías)



Controlador de acceso unidireccional de cuatro puertas

Figure 2-3 Conexión por cable (cuatro puertas unidireccional)



2.1.1 Conexión de cable de entrada de alarma

El puerto de entrada de alarma externa se puede conectar a detectores de humo, detectores de infrarrojos y más.

Tabla 2-1 Conexión de cable de entrada de alarma

Modelo	Canal de entrada de alarma	Descripción
Dos puertas de una sola mano	Entrada de alarma de 2 canales.	La alarma externa se puede vincular al estado de bloqueo/desbloqueo de la puerta. ● La alarma externa ALM1 vincula todas las puertas para que estén normalmente abiertas. ● La alarma externa ALM2 vincula todas las puertas para que estén normalmente cerradas.
Dos puertas bidireccional	Entrada de alarma de 4 canales.	La alarma externa se puede vincular al estado de bloqueo/desbloqueo de la puerta. ● La alarma externa ALM1–ALM2 vincula todas las puertas para que estén normalmente abiertas. ● La alarma externa ALM3–ALM4 vincula todas las puertas para que estén normalmente cerradas.
cuatro puertas de una sola mano	Entrada de alarma de 1 canal.	Cuando se dispara la alarma externa, todas las puertas están normalmente abiertas.

2.1.2 Conexión de cable de salida de alarma

La entrada de alarma interna o externa activa una alarma, y el dispositivo de salida de alarma emite una alarma durante 15 s.

Hay dos modos de conexión de salida de alarma. Seleccione el modo de conexión según el dispositivo de alarma. Por ejemplo, IPC puede usar el modo 1, y el dispositivo de luz y sonido puede usar el modo 2.

Cuando los controladores de acceso bidireccional de dos puertas están conectados al dispositivo de salida de alarma interna, seleccione NC/NO según el estado normalmente abierto o normalmente cerrado.

Tabla 2-2 Conexión de cable de salida de alarma

Modelo	Canal de salida de alarma	Puerto	Descripción
	Salida de alarma de 2 canales.	NO1	● ALM1 activa la salida de alarma.

Modelo	Canal de salida de alarma	Puerto	Descripción
Dos puertas de una sola mano		COM1	● Alarma de tiempo de espera de contacto de puerta y alarma de intrusión. ● Salida de alarma de sabotaje del lector de tarjetas de entrada de la puerta No.1.
		NO2	● ALM2 activa la salida de alarma. ● Salida de alarma de sabotaje del lector de tarjetas de entrada de la puerta No.2.
		COM2	
Dos puertas bidireccional	Salida de alarma externa de 2 canales.	NO1	Salida de alarma de activación ALM1/ALM2.
		COM1	
		NO2	Salida de alarma de activación ALM3/ALM4.
		COM2	
	Salida de alarma interna de 2 canales.	NC1	● Salida de alarma antisabotaje de los lectores de tarjetas de entrada y salida de la puerta n.º 1. ● Alarma de tiempo de espera de contacto de puerta y alarma de intrusión de la puerta n.º 1.
		COM1	
		NO1	
		NC2	● Salida de alarma de sabotaje de los lectores de tarjetas de entrada y salida de la puerta No.2. ● Alarma de tiempo de espera de contacto de puerta y alarma de intrusión de la puerta No.2.
		COM2	
		NO2	
cuatro puertas de una sola mano	Salida de alarma de 1 canal.	NO	● ALM activa la salida de alarma. ● Alarma de tiempo de espera de contacto de puerta y alarma de intrusión. ● Salida de alarma de manipulación del lector de tarjetas.
		COM	

2.1.3 Conexión del cable del lector de tarjetas

Una puerta solo admite un tipo de lector de tarjetas: RS-485 o Wiegand.

Tabla 2-3 Especificación del cable y longitud del lector de tarjetas

Tipo de lector de tarjetas	Modo de conexión	Largo
Lector de tarjetas RS-485	Cable de red CAT5e, conexión RS-485	100 metros
Lector de tarjetas Wiegand	Cable de red CAT5e, conexión Wiegand	30 metros

2.2 Instalación del dispositivo

Hay dos métodos de instalación.

- Fije directamente el dispositivo en la pared con tornillos.
- Instale el riel guía en forma de U (no incluido) en la pared y luego cuelgue el dispositivo en el riel guía.

Figure 2-4 Instalación (1)

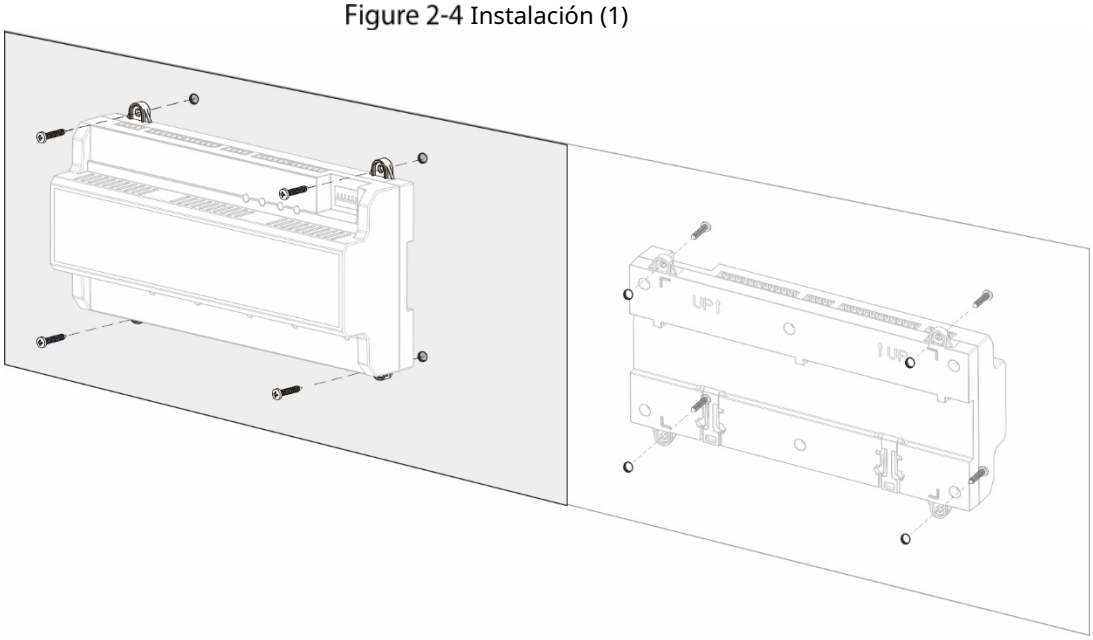
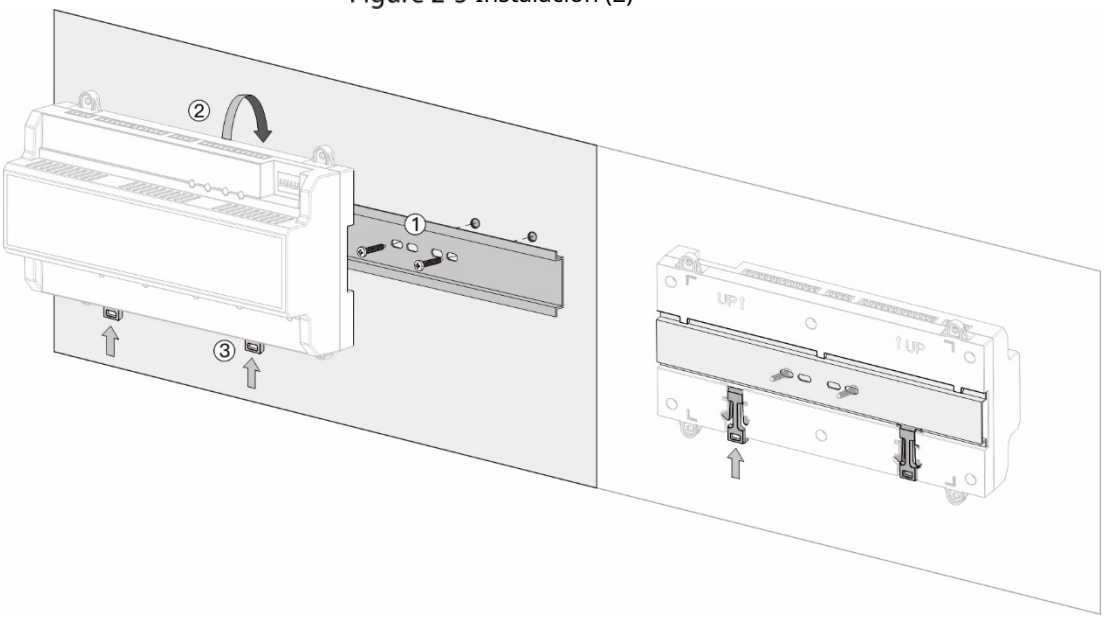


Figure 2-5 Instalación (2)



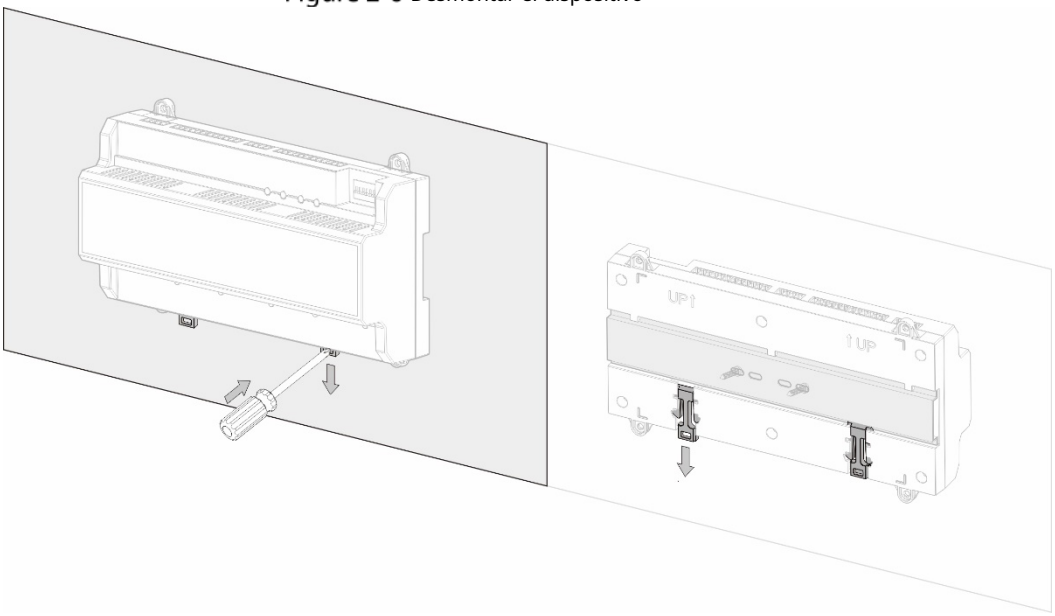
Step 1 Fije el riel guía en forma de U en la pared con tornillos.
Step 2 Abroche la parte trasera superior del dispositivo en el riel guía en forma de U. Empuje hacia
Step 3 arriba la hebilla en la parte inferior del dispositivo hasta que escuche un clic.

2.3 Quitar el dispositivo

Si el dispositivo se instala con el segundo método de instalación, consulte la Figura 2-6 cuando desee retirar el dispositivo.

Use un destornillador para presionar firmemente la hebilla y luego haga rebotar la hebilla para quitar el dispositivo.

Figure 2-6 Desmontar el dispositivo



3 Configuración de CA de SmartPSS

Puede administrar el dispositivo a través de SmartPSS AC. Esta sección presenta principalmente la configuración rápida de dispositivos. Para obtener más información, consulte el manual del usuario de SmartPSS AC.

Las capturas de pantalla del cliente Smart PSS AC en este manual son solo para referencia y pueden diferir de el producto real.

3.1 Acceso

Step 1 Instale el SmartPSS AC.

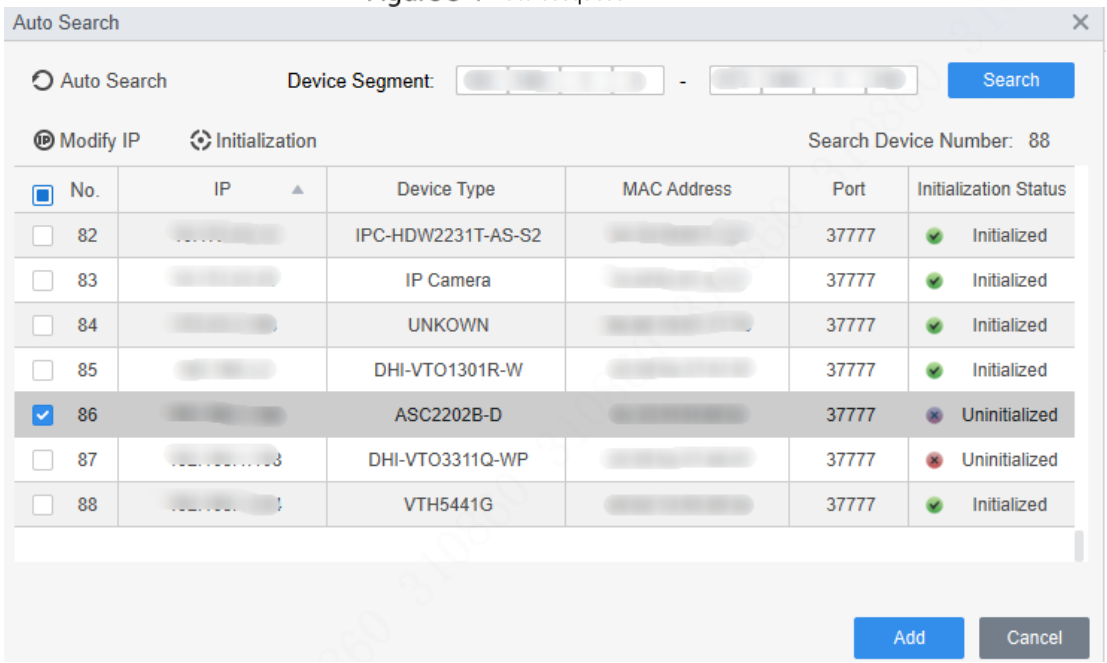
Step 2 Haga doble clic y luego siga las instrucciones para finalizar la inicialización e iniciar sesión.

3.2 Inicialización

Antes de la inicialización, asegúrese de que el dispositivo y la computadora estén en la misma red.

Step 1 En la página de inicio, seleccione**Administrador de dispositivos**y luego haga clic en**Auto búsqueda**.

Figure 3-1 Auto búsqueda



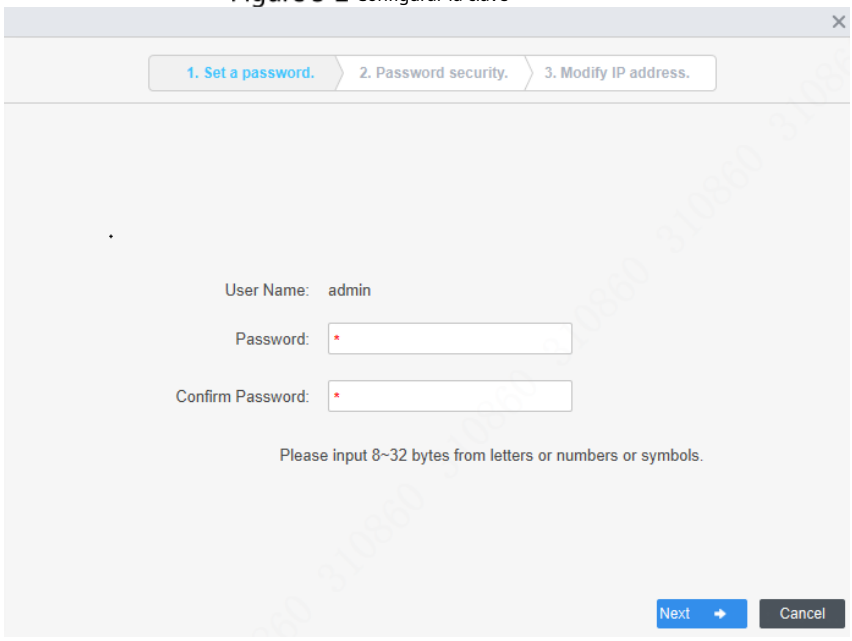
Step 2 Ingrese un rango de segmento de red y luego haga clic en**Búsqueda**.

Step 3 Seleccione el dispositivo y luego haga clic en**Inicialización**. Establezca la

Step 4 contraseña de administrador y luego haga clic en**próximo**.

Si olvida la contraseña, use el interruptor DIP para restaurar los valores predeterminados de fábrica.

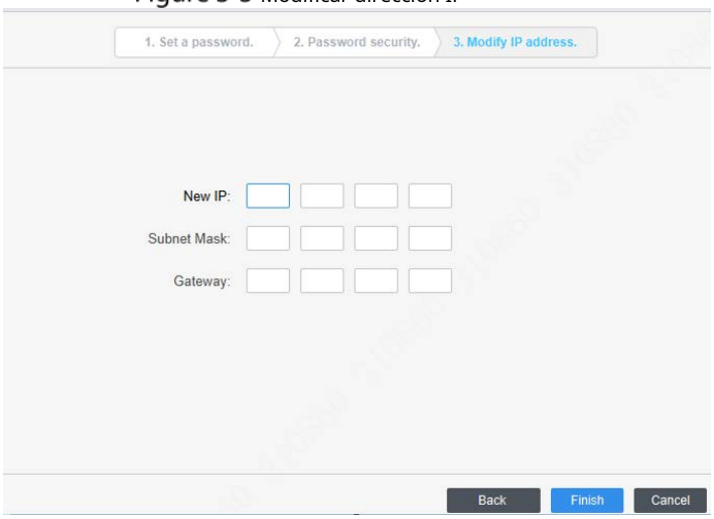
Figure 3-2 Configurar la clave



Step 5 Asocie el número de teléfono y luego haga clic en**próximo**. Ingrese la

Step 6 nueva IP, máscara de subred y puerta de enlace.

Figure 3-3 Modificar dirección IP



Step 7 Hacer clic**Terminar**.

3.3 Adición de dispositivos

Debe agregar el dispositivo a SmartPSS AC. Puede agregar dispositivos en lotes mediante la búsqueda automática o agregar dispositivos individualmente.

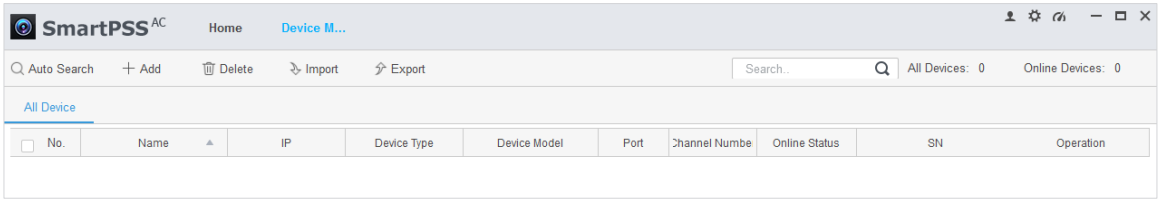
3.3.1 Búsqueda automática

Le recomendamos que agregue dispositivos mediante la búsqueda automática cuando necesite agregar dispositivos en lotes en el mismo segmento de red, o cuando conozca el rango del segmento de red en lugar de la dirección IP exacta.

Step 1 Inicie sesión en SmartPSS AC.

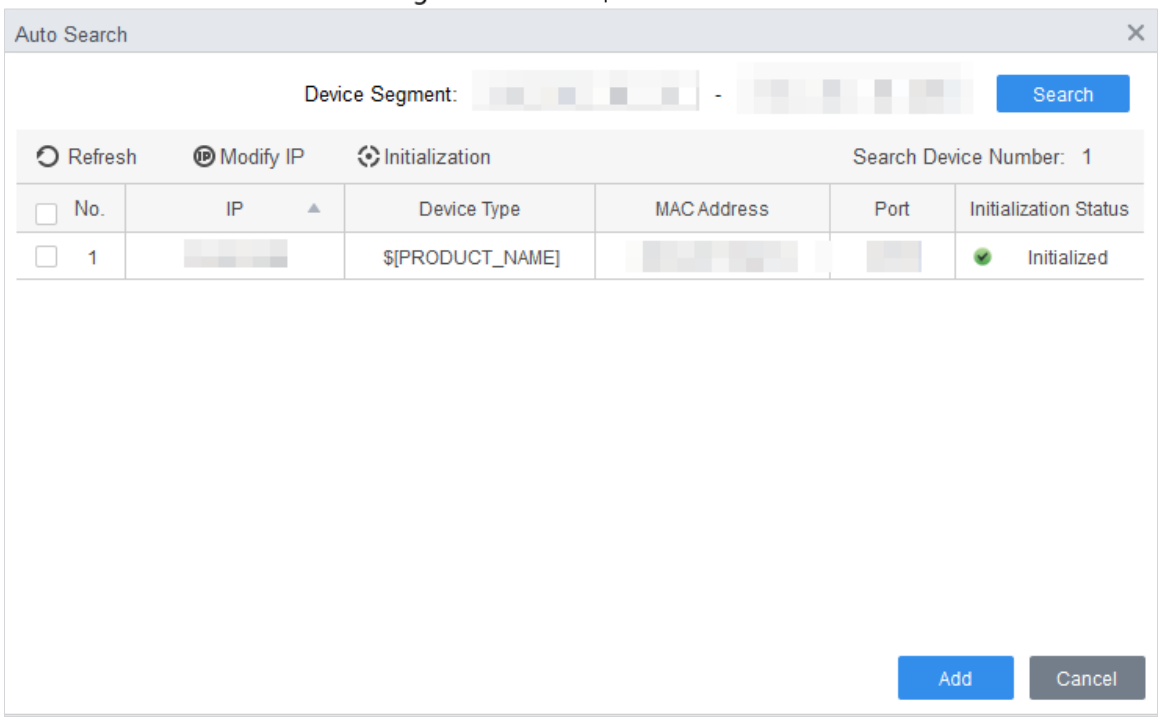
Step 2 Hacer clic**Administrador de dispositivos**en la esquina inferior izquierda.

Figure 3-4 Dispositivos



Step 3 Hacer clic**Auto búsqueda**.

Figure 3-5 Auto búsqueda



Step 4 Ingrese el segmento de red y luego haga clic en**Búsqueda**.

- Hacer clic**Actualizar**para actualizar la información del dispositivo.
- Seleccione un dispositivo, haga clic en**Modificar IP**para modificar la dirección IP del Dispositivo.

Step 5 Seleccione los dispositivos que desea agregar a SmartPSS AC y luego haga clic en**Agregar**. Ingrese el

Step 6 nombre de usuario y la contraseña de inicio de sesión para iniciar sesión.

- El nombre de usuario es admin y la contraseña es admin123 por defecto. Te recomendamos modificar la contraseña después de iniciar sesión.
- Después de un inicio de sesión exitoso, se muestra el estado del dispositivo**En línea**. De lo contrario, muestra**Desconectado**.

3.3.2 Adición manual

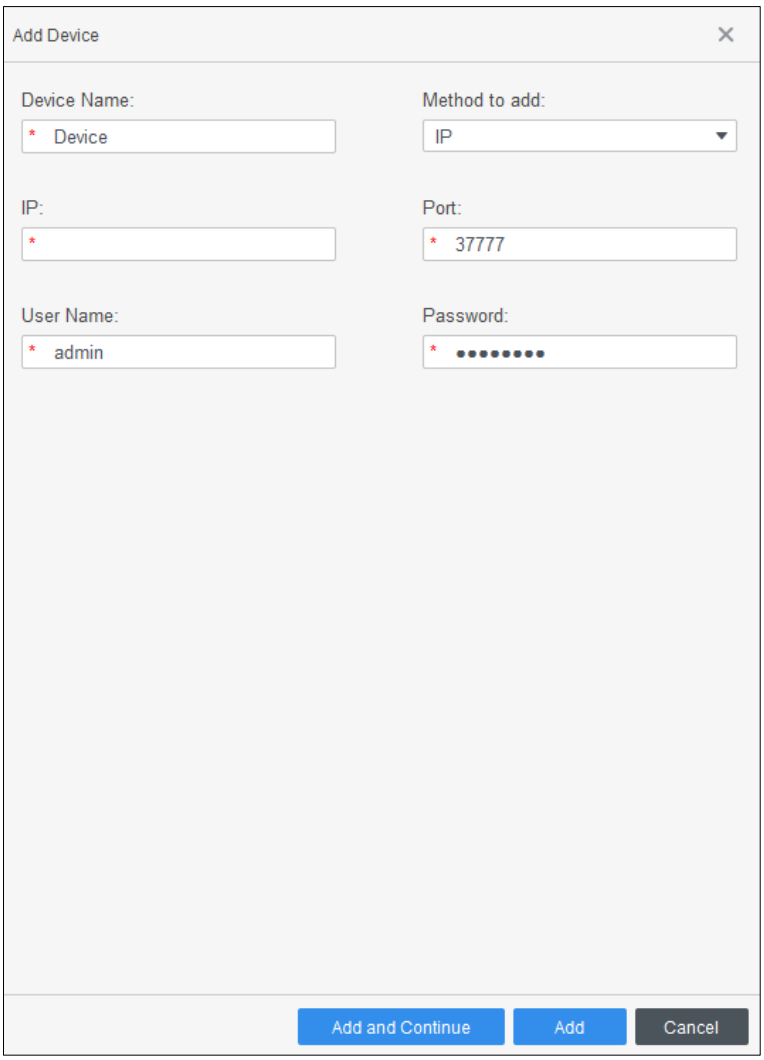
Puede agregar dispositivos manualmente. Debe conocer las direcciones IP y los nombres de dominio del controlador de acceso que desea agregar.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Administrador de dispositivos**en la esquina inferior izquierda.

Step 3 Hacer clic**Agregar**sobre el**Administrador de dispositivos**página

Figure 3-6 Adición manual



Step 4 Ingrese la información detallada del Dispositivo.

Tabla 3-1 Parámetros

Parámetro	Descripción
Nombre del dispositivo	Ingrese un nombre del dispositivo. Se recomienda nombrar el dispositivo con el área de instalación para una fácil identificación.
Método para agregar	Seleccione**IP**para agregar el dispositivo a través de la dirección IP.
IP	Ingrese la dirección IP del dispositivo. Es 192.168.1.108 por defecto.
Puerto	Introduzca el número de puerto del dispositivo. El número de puerto predeterminado es 37777.
Nombre de usuario, Clave	Ingrese el nombre de usuario y la contraseña del dispositivo agregado. El nombre de usuario es admin y la contraseña es admin123 por defecto. Se recomienda modificar la contraseña después de iniciar sesión.

Step 5 Hacer clic**Agregar**, y luego puede ver el dispositivo agregado en la**Dispositivos**página.

Después de agregar, SmartPSS AC inicia sesión en el dispositivo automáticamente. Después de un inicio de sesión exitoso, se muestra el estado**En línea**. De lo contrario, muestra**Desconectado**.

4 Configuración de la herramienta de configuración

ConfigTool se utiliza principalmente para configurar y mantener el dispositivo.

No use ConfigTool y SmartPSS AC al mismo tiempo, de lo contrario puede causar resultados anormales cuando buscas dispositivos.

4.1 Inicialización

Antes de la inicialización, asegúrese de que el dispositivo y la computadora estén en la misma red.

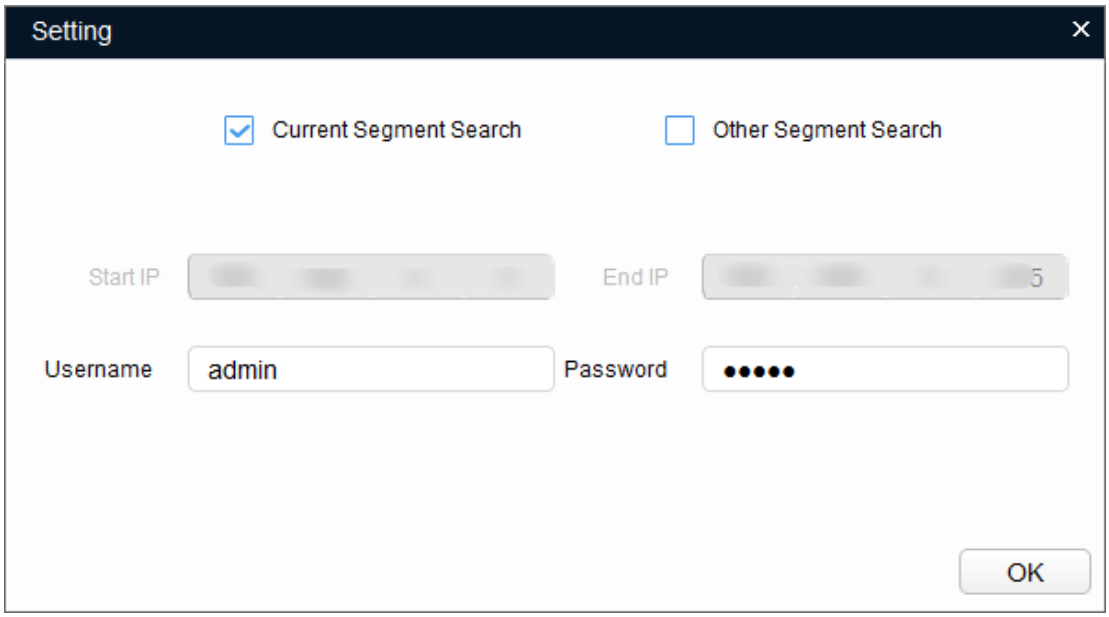
Step 6 Busque el dispositivo a través de ConfigTool. 1)

Haga doble clic en ConfigTool para abrirlo.

1) Haga clic**Configuración de búsqueda**, ingrese el rango del segmento de red y luego haga clic en**DE ACUERDO**.

2) Seleccione el dispositivo no inicializado y luego haga clic en**Inicializar**.

Figure 4-1 Buscar el dispositivo



Step 7 Seleccione dispositivos no inicializados y luego haga clic en**Inicializar.** Hacer clic**DE**

Step 8 **ACUERDO**.

El sistema inicia la inicialización. indica el éxito de la inicialización, indica inicialización falló.

Step 9 Hacer clic**Terminar**.

4.2 Adición de dispositivos

Puede agregar uno o varios dispositivos según sus necesidades reales. Esta sección utiliza como ejemplo la adición manual del dispositivo por dirección IP.

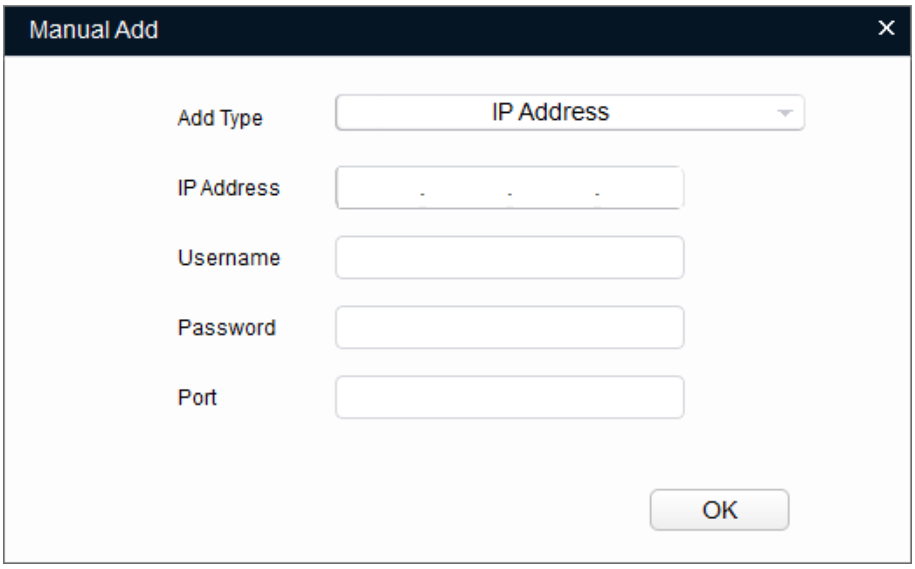
Asegúrese de que el Dispositivo y la PC donde está instalado ConfigTool estén conectados; de lo contrario el La herramienta no puede encontrar el dispositivo.

Step 1 Hacer clic .

Step 2 Haga clic en Añadir manualmente.

Step 3 Seleccione**Dirección IP**desde**Añadir tipo**lista.

Figure 4-2 Adición manual



Step 4 Configure los parámetros del dispositivo.

Tabla 4-1 Parámetros de adición manual

Añadir método	Parámetro	Descripción
Dirección IP	Dirección IP	La dirección IP del Dispositivo. Es 192.168.1.108 por defecto.
	Nombre de usuario	El nombre de usuario y la contraseña para iniciar sesión en el Dispositivo.
	Clave	
	Puerto	El número de puerto del dispositivo.

Step 5 Hacer clic**DE ACUERDO**.

El dispositivo recién agregado se muestra en la lista de dispositivos.

4.3 Configuración del controlador de acceso

Las capturas de pantalla y los parámetros pueden ser diferentes según los tipos y modelos de dispositivos.

Step 1 Hacer clic en el menú principal.

Step 2 Haga clic en el controlador de acceso que desea configurar en la lista de dispositivos y luego haga clic en**Obtener información del dispositivo**.

Step 3 (Opcional) Si aparece la página de inicio de sesión, ingrese el nombre de usuario y la contraseña, y luego haga clic en**DE ACUERDO**.

Step 4 Establecer los parámetros del controlador de acceso.

Figure 4-3 Configurar controlador de acceso

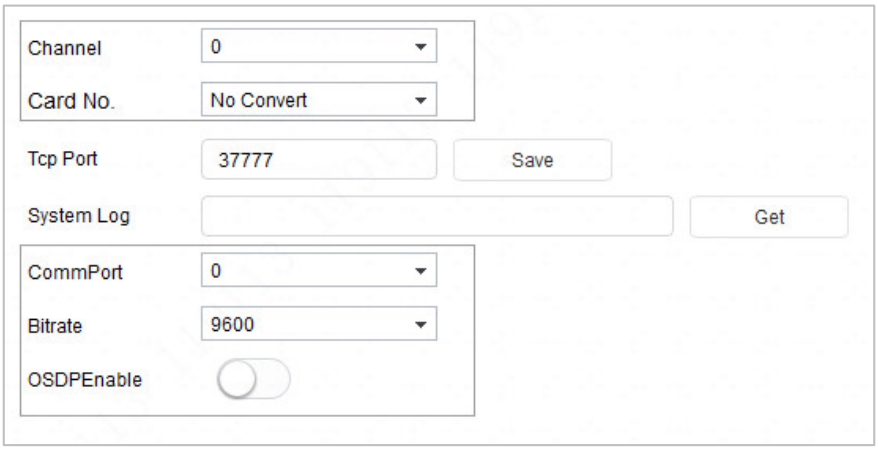


Tabla 4-2 Parámetros del controlador de acceso

Parámetro	Descripción
Canal	Seleccione el canal para configurar los parámetros.
número de tarjeta	Configure la regla de procesamiento del número de tarjeta del controlador de acceso. Está**Sin conversión** por defecto. Cuando el resultado de la lectura de la tarjeta no coincida con el número de tarjeta real, seleccione **Reversión de bytes**o**Convertir HIDpro**. ● **Reversión de bytes**: Cuando el controlador de acceso funciona con lectores de terceros y el número de tarjeta leído por el lector de tarjetas está en orden inverso al número de tarjeta real. Por ejemplo, el número de tarjeta leído por el lector de tarjetas es hexadecimal 12345678 mientras que el número de tarjeta real es hexadecimal 78563412, y puede seleccionar**Reversión de bytes**. ● **Convertir HIDpro**: Cuando el controlador de acceso funciona con lectores HID Wiegand y el número de tarjeta leído por el lector de tarjetas coincide con el número de tarjeta real, puede seleccionar HIDpro Revert para que coincidan. Por ejemplo, el número de tarjeta leído por el lector de tarjetas es hexadecimal 1BAB96 mientras que el número de tarjeta real es hexadecimal 78123456,
Puerto TCP	Modifique el número de puerto TCP del dispositivo.
Registro del sistema	Hacer clic**Conseguir**para seleccionar una ruta de almacenamiento para los registros del sistema.
Puerto de comunicaciones	Seleccione el lector para establecer la tasa de bits y habilitar OSDP.
tasa de bits	Si la lectura de la tarjeta es lenta, puede aumentar la tasa de bits. Es 9600 por defecto.
Habilitar OSDP	Cuando el controlador de acceso funciona con lectores de terceros a través del protocolo ODSP, habilite ODSP.

Step 5 (Opcional) Haga clic en**Aplicar para**, seleccione los dispositivos a los que necesita aplicar los parámetros configurados y luego haga clic en**Configuración**.

indica el éxito de la aplicación; indica que la aplicación falló. Puede hacer clic en ellos para ver detalles.

Appendix 1 Recomendaciones de ciberseguridad

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo: 1. Use contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres.
- Incluya al menos dos tipos de caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No contenga el nombre de la cuenta o el nombre de la cuenta en orden
- inverso. No utilice caracteres continuos, como 123, abc, etc.
- No utilice caracteres superpuestos, como 111, aaa, etc.

2. Actualice el firmware y el software del cliente a tiempo

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función de "verificación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala y gabinete de computadoras especiales, e implemente un permiso de control de acceso y una administración de claves bien hechos para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB). , puerto serie), etc.

2. Cambie las contraseñas regularmente

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3. Establezca y actualice la información de restablecimiento de contraseñas a tiempo

El dispositivo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

4. Habilitar bloqueo de cuenta

La función de bloqueo de cuenta está habilitada de forma predeterminada y le recomendamos que la mantenga activada para garantizar la seguridad de la cuenta. Si un atacante intenta iniciar sesión varias veces con la contraseña incorrecta, la cuenta correspondiente y la dirección IP de origen se bloquearán.

5. Cambiar HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio a cualquier conjunto de números entre 1024 y 65535, lo que reduce el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6. Habilitar HTTPS

Le sugerimos que habilite HTTPS, para que visite el servicio web a través de un canal de comunicación seguro.

7. Enlace de dirección MAC

Le recomendamos vincular la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así

el riesgo de suplantación de ARP.

8. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente y asígneles un conjunto mínimo de permisos.

9. Deshabilite los servicios innecesarios y elija modos seguros

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir los riesgos.

Si es necesario, se recomienda encarecidamente que utilice modos seguros, incluidos, entre otros, los siguientes servicios:

- SNMP: elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.
- SMTP: Elija TLS para acceder al servidor de buzones.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de encriptación WPA2-PSK y configure contraseñas seguras.

10. Transmisión encriptada de audio y video

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión encriptada para reducir el riesgo de robo de datos de audio y video durante la transmisión.

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

11. Auditoría segura

- Verifique a los usuarios en línea: le sugerimos que verifique a los usuarios en línea regularmente para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se usaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12. Registro de red

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

13. Construya un entorno de red seguro

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts que pueden acceder al dispositivo.