

Controlador de acceso con reconocimiento facial

Guía de inicio rápido



Prefacio

General

Este manual presenta las funciones, la conexión en red y las preguntas frecuentes del módulo de extensión de control de acceso (en adelante, "el módulo de extensión"). Lea atentamente antes de utilizar el dispositivo y guarde el manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
 DANGER	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
 WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducciones en el rendimiento o resultados impredecibles.
 TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
 NOTE	Proporciona información adicional como complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.4	Se actualizó el diagrama de cableado.	Marzo de 2024
Versión 1.0.3	Diagrama de red revisado.	Febrero de 2023
Versión 1.0.2	Revisado "Importante "Salvaguardias y advertencias".	Diciembre de 2022
Versión 1.0.1	Se revisó el nombre del manual.	Noviembre de 2022
Versión 1.0.0	Primer lanzamiento.	Marzo de 2022

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, es posible que recopile datos personales de otras personas, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y normativas 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 de la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del manual

- El manual es solo de referencia. Pueden existir ligeras diferencias entre el manual y el producto.

- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Pueden encontrarse 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 provocar 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 de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del Dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el Dispositivo y cumpla con las pautas al usarlo.

Requerimientos de transporte



Transporte, utilice y almacene el Dispositivo en condiciones de humedad y temperatura permitidas.

Requisito de almacenamiento



Guarde el dispositivo en condiciones de humedad y temperatura permitidas.

Requisitos de instalación



WARNING

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con los códigos y normas de seguridad eléctrica locales. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del dispositivo.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación, para evitar dañarlo.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.
- Siga los requisitos eléctricos para alimentar el dispositivo.
 - ◇ A continuación se detallan los requisitos para seleccionar un adaptador de corriente.
 - La fuente de alimentación debe cumplir con los requisitos de las normas IEC 60950-1 e IEC 62368-1.
 - El voltaje debe cumplir con los requisitos de SELV (voltaje extra bajo de seguridad) y no exceder los estándares ES-1.
 - Cuando la potencia del dispositivo no supere los 100 W, la fuente de alimentación debe cumplir los requisitos de LPS y no ser superior a PS2.
 - ◇ Recomendamos utilizar el adaptador de corriente provisto con el dispositivo.
 - ◇ Al seleccionar el adaptador de corriente, los requisitos de suministro de energía (como el voltaje nominal) están sujetos a la etiqueta del dispositivo.



- El personal que trabaja en altura debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de 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 sobre 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 armario proporcionada por el fabricante.

- Utilice los cables de alimentación recomendados para la región y que cumplan con las especificaciones de potencia nominal.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con conexión a tierra.

Requisitos de funcionamiento



- Compruebe si la fuente de alimentación es correcta antes de usarlo.
- **Conecte el dispositivo a tierra antes de encenderlo.**
- No desconecte el cable de alimentación del costado del dispositivo mientras el adaptador esté encendido.
- Utilice el dispositivo dentro del rango nominal de entrada y salida de energía.
- Utilice el dispositivo en las condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquidos sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el dispositivo que impida que el líquido fluya hacia él.
- **No desmonte el dispositivo sin instrucción profesional.**
- Este producto es un equipo profesional.
- El dispositivo no es adecuado para su uso en lugares donde es probable que haya niños.

Tabla de contenido

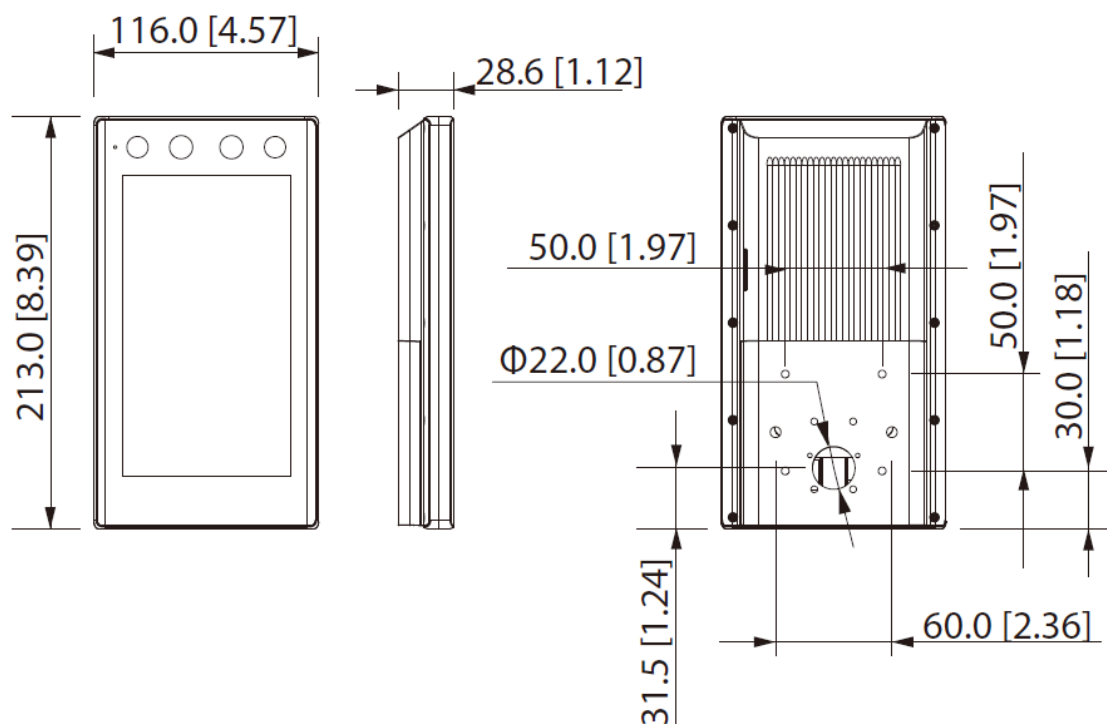
Prefacio.....	I Medidas de seguridad y advertencias importantes.....	III 1 Estructura
.....		1
2 Conexión e instalación.....		3
2.1 Cableado.....		3
2.2 Requisitos de instalación.....		4
2.3 Proceso de instalación.....		5
2.3.1 Instalación del controlador de acceso.....		5
2.3.1.1 Montaje en pared.....		5
2.3.1.2 (Opcional) Montaje del parasol.....		7
2.3.1.3 86 Montaje en caja.....		11
2.3.2 (Opcional) Instalación del módulo de extensión.....		13
3 Operaciones locales.....		15
3.1 Inicialización.....		15
3.2 Agregar nuevos usuarios.....		16
3.3 Configuración del módulo de extensión.....		18
4 Operaciones web.....		20
4.1 Inicialización.....		20
4.2 Iniciar sesión.....		20
Apéndice 1 Puntos importantes del funcionamiento del intercomunicador.....		22
Apéndice 2 Puntos importantes del escaneo de códigos QR.....		23
Apéndice 3 Instrucciones para el registro de huellas dactilares.....		24
Apéndice 4 Puntos importantes del registro facial.....		26
Apéndice 5 Recomendaciones de seguridad.....		29

1 Estructura

La apariencia frontal puede variar según los distintos modelos del controlador de acceso. Aquí tomamos como ejemplo el modelo Wi-Fi.

Controlador de acceso con reconocimiento facial

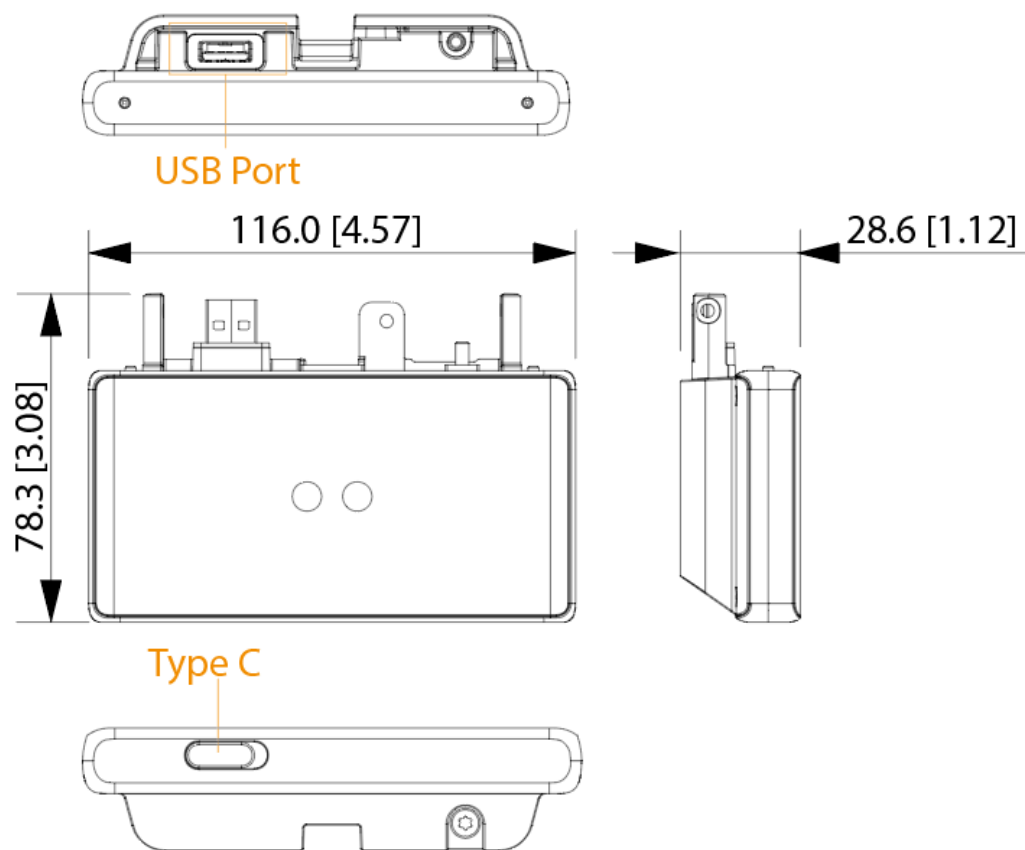
Figura 1-1 Estructura (unidad: mm [pulgada])



Módulo de extensión

Puede montar el módulo de extensión en el controlador de acceso según sus necesidades reales. Los módulos de extensión incluyen 3 tipos: módulo de código QR, módulo de huella dactilar, módulo de huella dactilar + código QR. Los módulos de extensión tienen las mismas dimensiones. Esta sección toma el módulo de código QR como ejemplo.

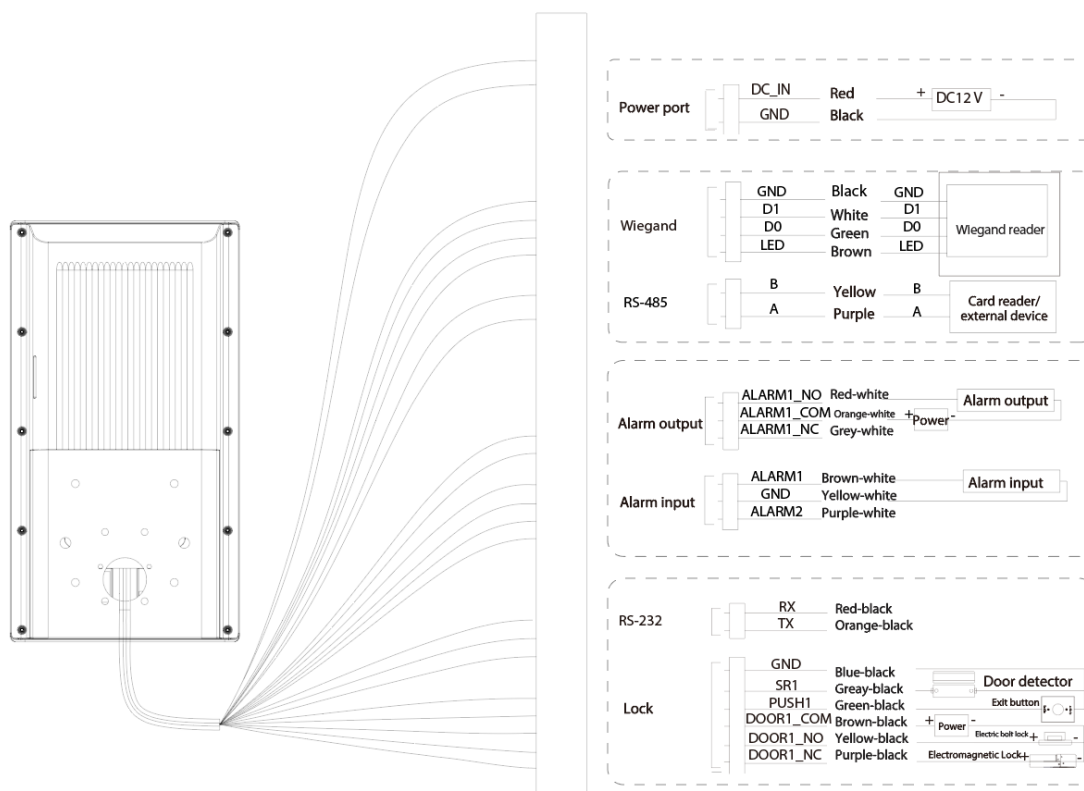
Figura 1-2 Modelo de código QR (unidad: mm [pulgada])



2 Conexión e instalación

2.1 Cableado

Figura 2-1 Cableado



- El panel posterior del controlador de acceso tiene un puerto de Internet, un puerto de extensión de audio y un puerto para tarjeta SD. y arnés de cableado. Los puertos pueden variar según los distintos modelos de controlador de acceso.
- Si desea conectar un altavoz externo, se requiere un cable adaptador de audio.
- Si desea conectar un módulo de seguridad, deberá adquirir un módulo de seguridad por separado. clientes. En el **Menú principal** Pantalla del controlador de acceso, seleccione **Conexión > Puerto serial > Módulo de seguridad**. El módulo de seguridad necesita una fuente de alimentación independiente.
- Cuando el módulo de seguridad está encendido, el botón de salida, la cerradura y la apertura de la puerta del enlace de alarma se activan. No efectivo.

2.2 Requisitos de instalación



- La luz a 0,5 metros de distancia del controlador de acceso no debe ser inferior a 100 Lux.
- Se recomienda instalar el controlador de acceso en interiores, al menos a 3 metros de distancia de ventanas y puertas, y a 2 metros de la fuente de luz.
- Evite la luz de fondo, la luz solar directa, la luz cercana y la luz oblicua.

Requisitos de iluminación ambiental

Figura 2-2 Requisitos de iluminación ambiental



Candle: 10Lux



Light bulb: 100Lux–850Lux



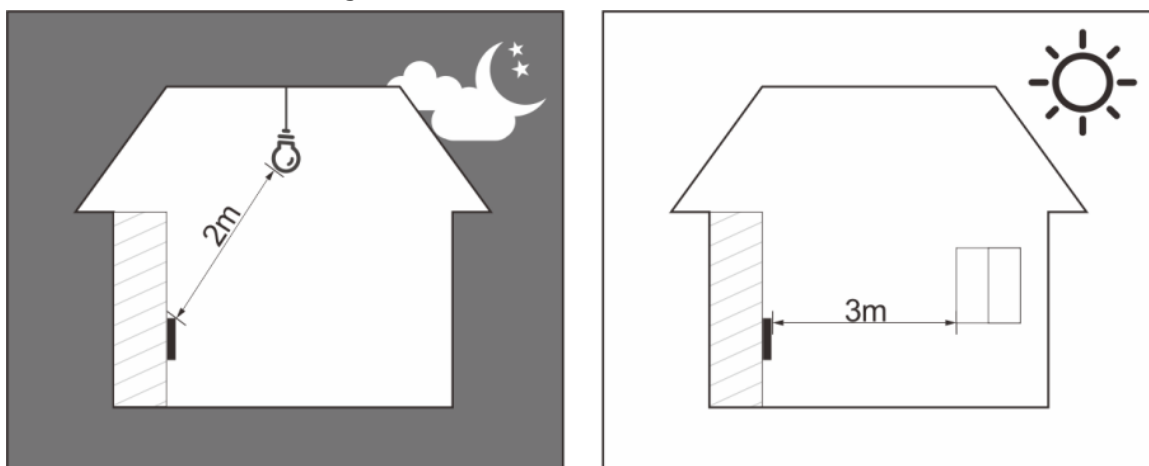
Sunlight: $\geq 1200\text{Lux}$

Requisitos de monitoreo de temperatura

- Se recomienda instalar el controlador de acceso en un entorno interior sin viento (un área relativamente cerrada) y donde la temperatura ambiente se mantenga entre 15 °C y 32 °C.
- Caliente el controlador de acceso durante más de 20 minutos después de encenderlo para permitir que la unidad de monitoreo de temperatura alcance el equilibrio térmico.
- Si no hay un entorno interior adecuado, incluidas las áreas orientadas directamente hacia áreas interiores y exteriores, y las puertas exteriores, configure una ubicación temporal con una temperatura ambiente estable para monitorear la temperatura.
- La luz del sol, el viento, el aire frío y el aire del aire acondicionado pueden afectar fácilmente la temperatura humana y el rendimiento del controlador de acceso, lo que provocará una desviación entre la temperatura monitoreada y la temperatura real.
- Factores que afectan el monitoreo de la temperatura:
 - ◇ Viento: El viento quitará el calor de la frente, lo que afectará la precisión del monitoreo de la temperatura.
 - ◇ Sudoración: la sudoración es una forma que tiene el cuerpo de enfriarse y disipar el calor de forma automática. Cuando el cuerpo suda, la temperatura también baja.
 - ◇ Temperatura ambiente: si la temperatura ambiente es demasiado baja, la temperatura corporal disminuirá. Si la temperatura ambiente es demasiado alta, el cuerpo humano sudará y afectará la precisión del control de temperatura.
 - ◇ La unidad de control de temperatura es sensible a ondas de luz con una longitud de onda de 10 μm a 15 μm . Evite instalar el controlador de acceso en lugares que tengan contacto con la luz solar directa, luz fluorescente, salidas de aire acondicionado, calefacción, salidas de aire frío y superficies de vidrio.

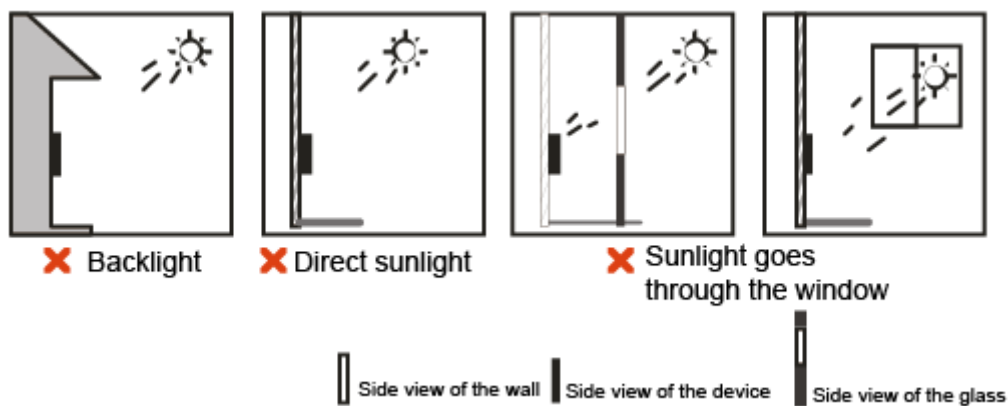
Ubicación recomendada

Figura 2-3 Ubicación recomendada



Ubicación no recomendada

Figura 2-4 Ubicación no recomendada



2.3 Proceso de instalación

2.3.1 Instalación del controlador de acceso

El controlador de acceso tiene cuatro métodos de instalación: montaje en pared, montaje en soporte de piso, montaje en torniquete y montaje en caja 86. Esta sección solo presenta el montaje en pared y el montaje en caja 86. Para obtener detalles sobre el montaje en soporte de piso y el montaje en torniquete, consulte el manual del usuario de los dispositivos correspondientes.

2.3.1.1 Montaje en pared

Procedimiento

- Paso 1** Según la posición de los orificios del soporte de instalación, taladre cuatro orificios y una salida de cable en la pared. Coloque pernos de expansión en los orificios.

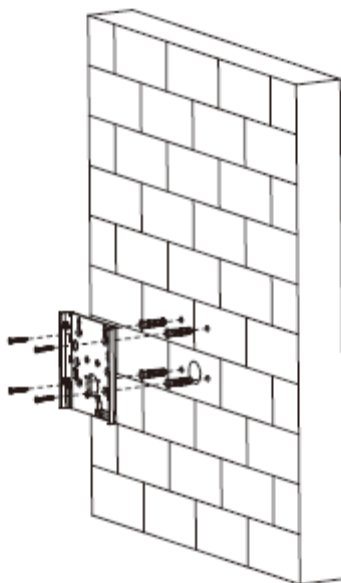


No se requiere salida de cable en el cableado montado en superficie.

Paso 2

Utilice los cuatro tornillos para fijar el soporte de instalación a la pared.

Figura 2-5 Fije el soporte de instalación a la pared



Paso 3

Conecte el controlador de acceso. Para obtener más información, consulte "2.1 Cableado".



Elija cableado en la pared o cableado montado en la superficie según sus necesidades reales.

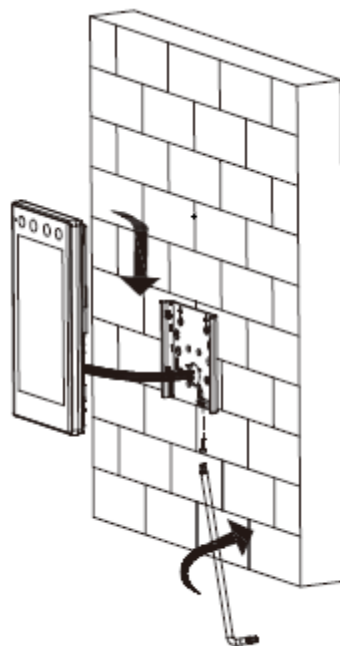
Paso 4

Fije el controlador de acceso en el soporte.

Paso 5

Atornille firmemente un tornillo de cabeza hueca en la parte inferior del controlador de acceso. La siguiente figura toma como ejemplo el cableado en la pared del controlador de acceso.

Figura 2-6 Cableado en la pared del controlador de acceso



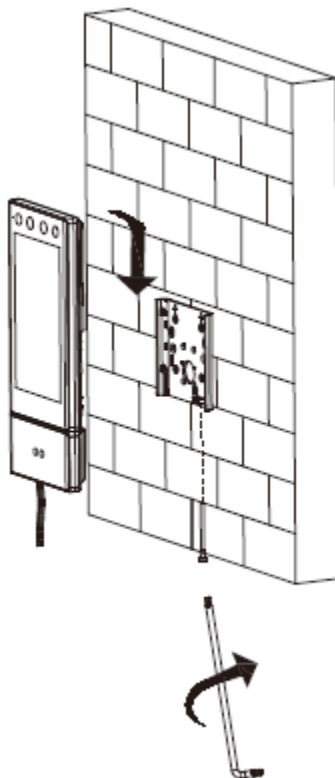


Si se monta un módulo de expansión en el controlador de acceso, seleccione un cabezal de zócalo adecuado

Tornillo de tapa según el tamaño del módulo de expansión. La siguiente figura toma como referencia la superficie.

cableado montado del módulo de extensión, por ejemplo.

Figura 2-7 Cableado montado en superficie del controlador de acceso (con módulo de extensión de código QR)



2.3.1.2 (Opcional) Montaje del parasol

Monte un parasol en el controlador de acceso según sus propias necesidades. El parasol debe adquirirse por separado por los clientes.

Procedimiento

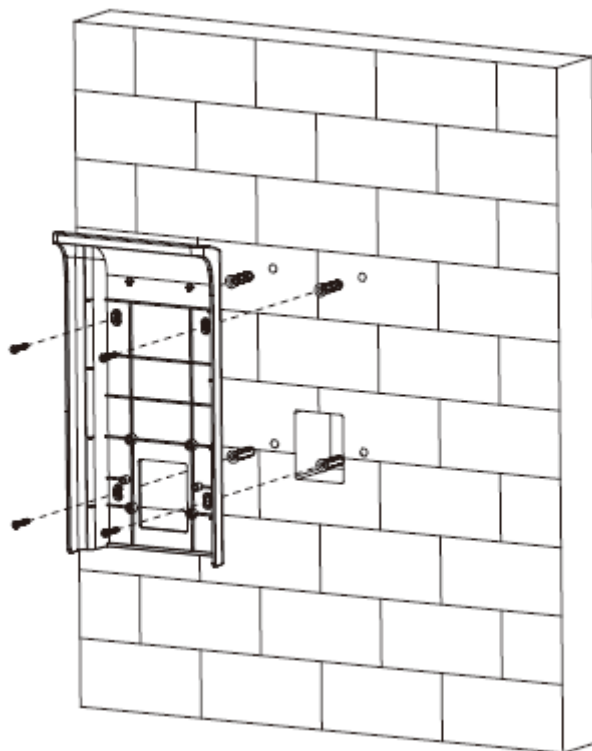
- Paso 1** Golpee suavemente los orificios con un destornillador para empujarlos lejos del parasol.



Un orificio ciego es una abertura parcialmente estampada que permite la entrada rápida de un cable o tornillos.

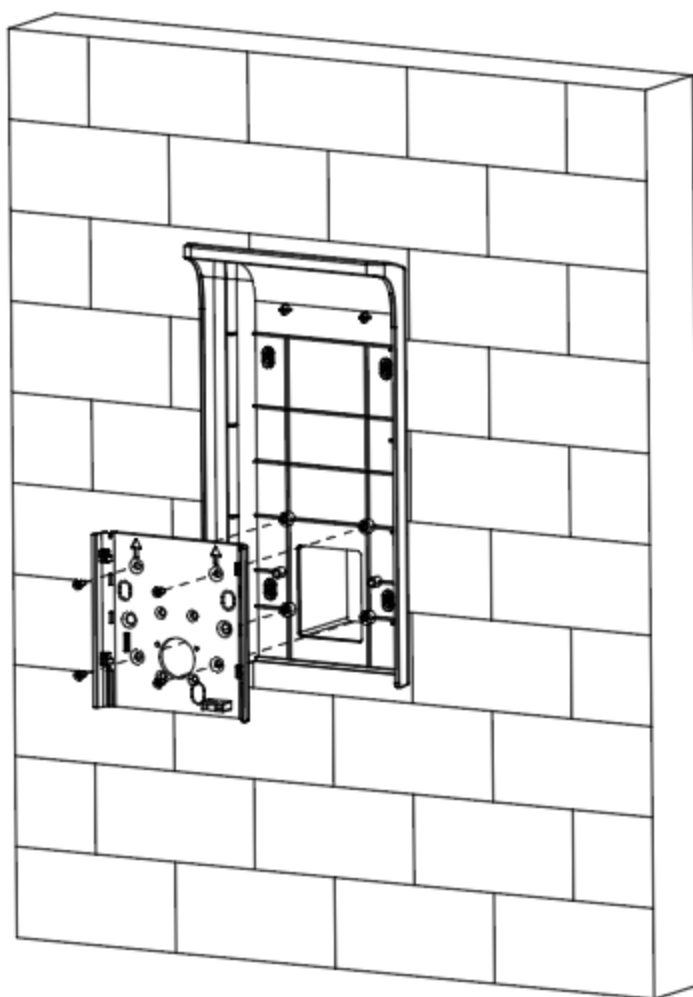
- Paso 2** Según la posición de los agujeros en el parasol, taladre cuatro agujeros y luego coloque pernos de expansión en los agujeros.
- Paso 3** Fije el parasol a la pared con cuatro tornillos.

Figura 2-8 Fije el parasol a la pared



Paso 4 Fije el soporte de instalación al parasol con cuatro tornillos.

Figura 2-9 Fije el soporte de instalación al parasol



Paso 5 Conecte el controlador de acceso. Para obtener más información, consulte "2.1 Cableado"

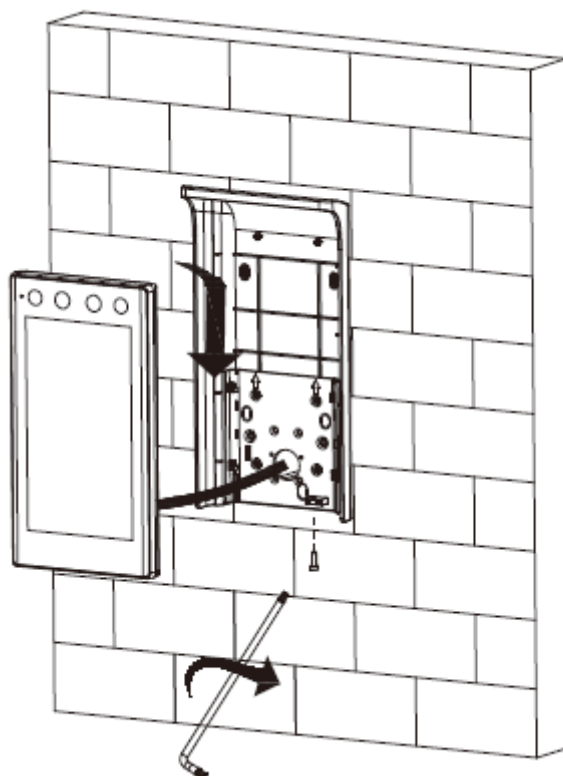


Elija cableado en la pared o cableado montado en la superficie según sus necesidades.

Paso 6 Fije el controlador de acceso en el soporte de instalación.

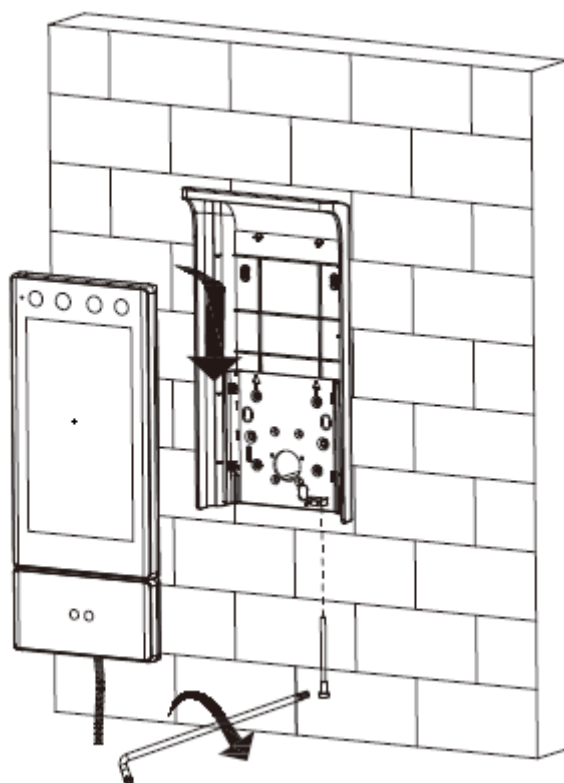
Paso 7 Atornille firmemente un tornillo de cabeza hueca en la parte inferior del controlador de acceso. La siguiente figura toma como ejemplo el cableado en la pared del controlador de acceso.

Figura 2-10 Cableado en la pared del controlador de acceso



Si se monta un módulo de expansión en el controlador de acceso, seleccione un cabezal de zócalo adecuado
Tornillo de tapa según el tamaño del módulo de expansión. La siguiente figura toma como referencia la superficie.
cableado montado del módulo de extensión de código QR, por ejemplo.

Figura 2-11 Cableado en la pared del controlador de acceso (con módulo de extensión de código QR)

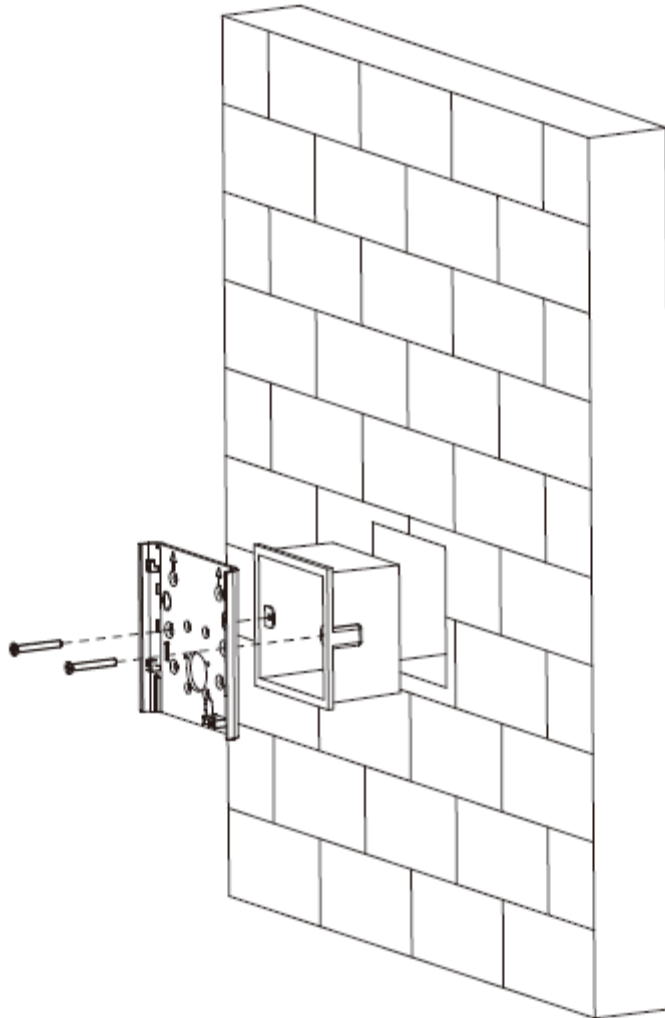


2.3.1.3 86 Montaje en caja

Procedimiento

- Paso 1 Coloque la caja 86 en la pared a una altura adecuada.
- Paso 2 Fije el soporte de instalación a la caja 86 con dos tornillos.

Figura 2-12 Fije el soporte a la caja 86



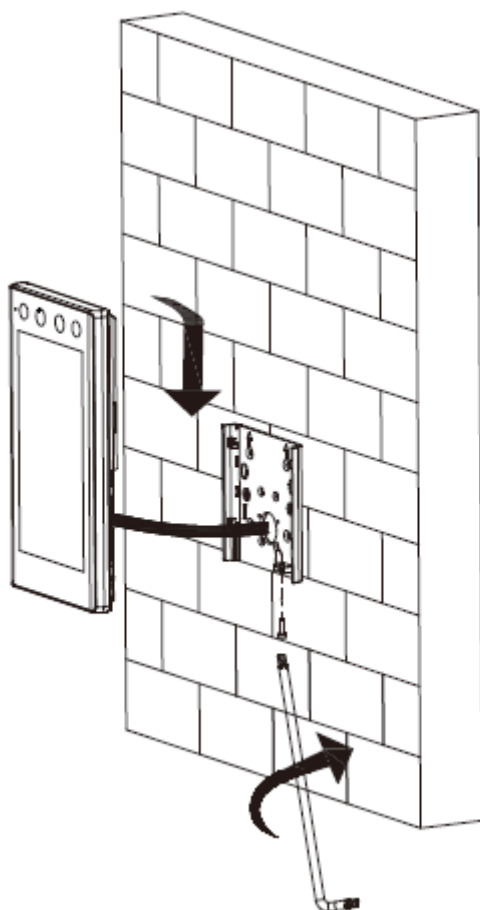
- Paso 3 Conecte el controlador de acceso. Para obtener más información, consulte "2.1 Cableado".



Elija cableado en la pared o cableado montado en la superficie según sus necesidades.

- Paso 4 Fije el controlador de acceso al soporte de instalación.
- Paso 5 Atornille firmemente un tornillo de cabeza hueca en la parte inferior del controlador de acceso. La siguiente figura toma como ejemplo el cableado en la pared del controlador de acceso.

Figura 2-13 Cableado en la pared del controlador de acceso



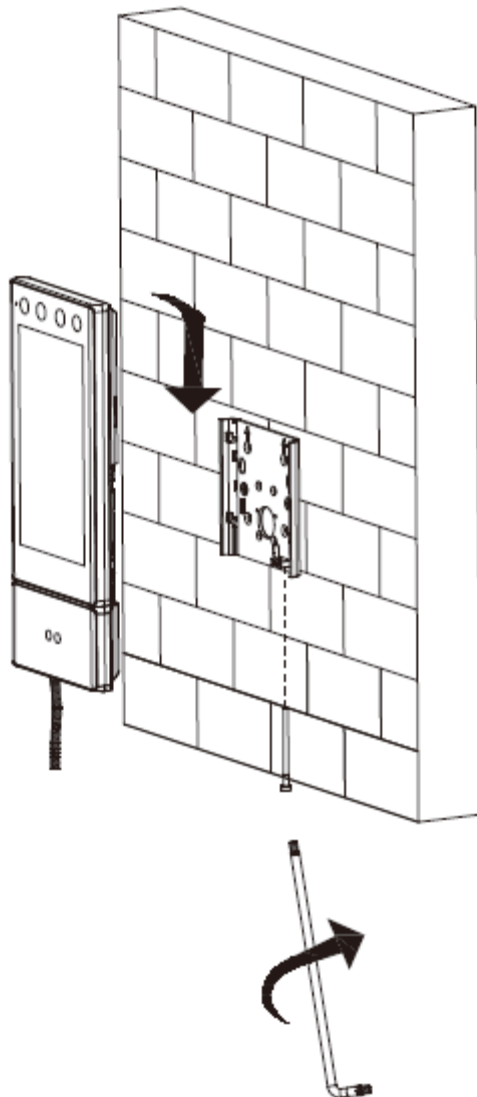


Si se monta un módulo de expansión en el controlador de acceso, seleccione un cabezal de zócalo adecuado

Tornillo de tapa según el tamaño del módulo de expansión. La siguiente figura toma como referencia la superficie.

cableado montado del módulo de extensión de código QR, por ejemplo.

Figura 2-14 Cableado en la pared del controlador de acceso (con módulo de extensión de código QR)



2.3.2 (Opcional) Instalación del módulo de extensión

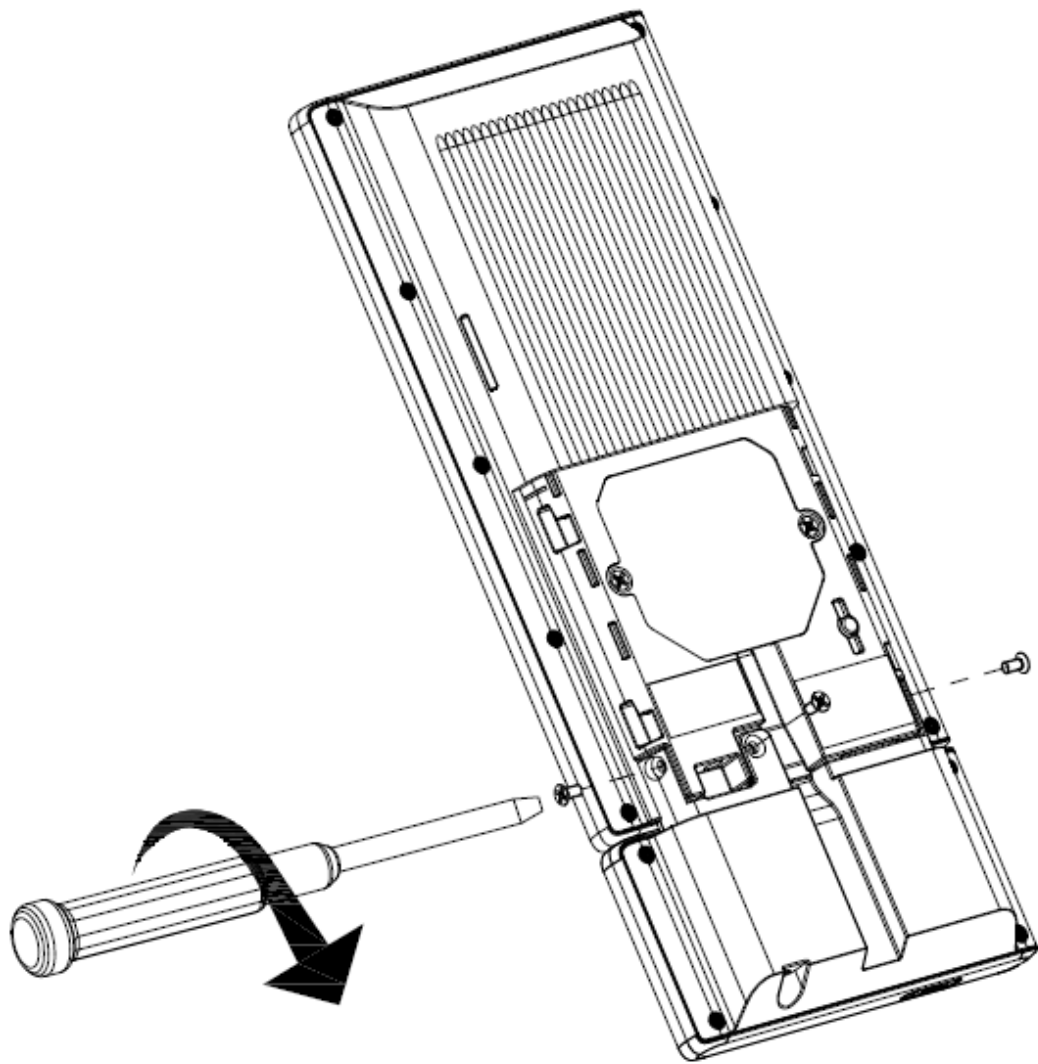
Puede montar el módulo de extensión en el controlador de acceso según sus necesidades reales. El cliente debe adquirir el módulo de extensión por separado.

Procedimiento

Paso 1 Inserte un USB en el controlador de acceso.

Paso 2 Atornille tres tornillos para fijar firmemente el módulo de extensión al controlador de acceso.

Figura 2-15 Fije el módulo de extensión

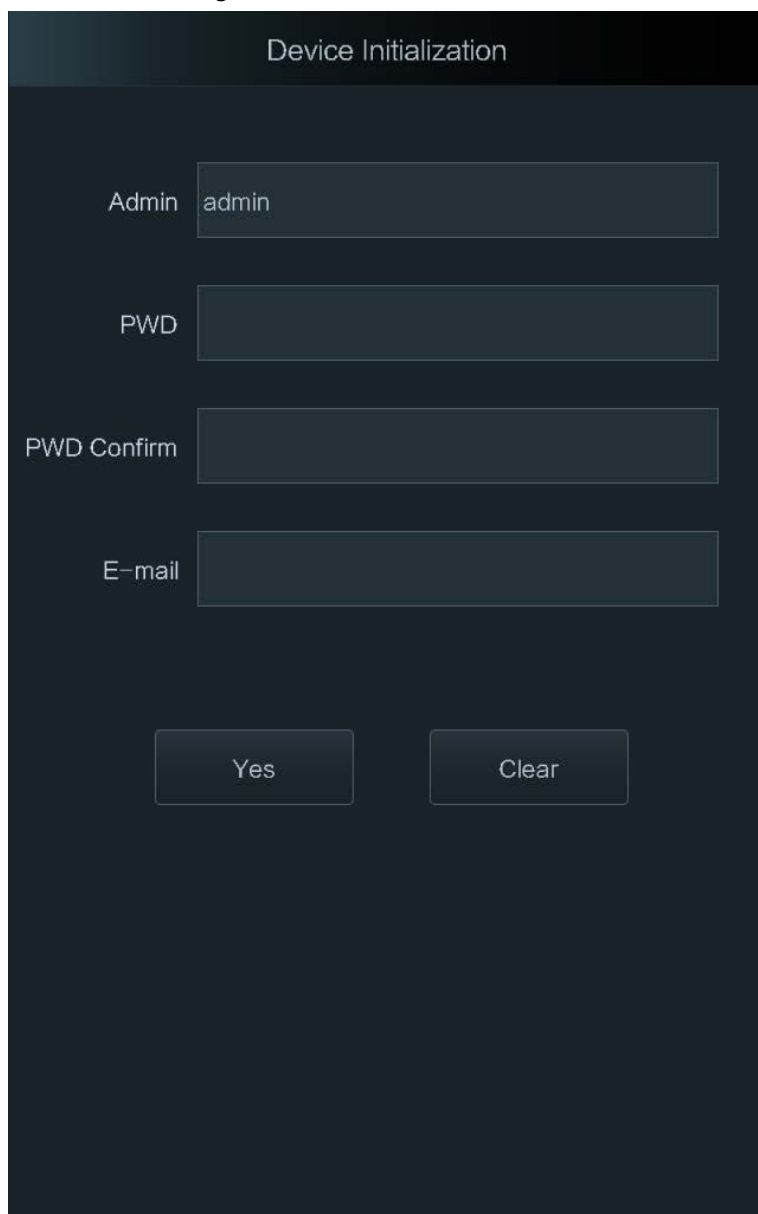


3 Operaciones locales

3.1 Inicialización

Para el primer uso o después de restaurar los valores predeterminados de fábrica, debe configurar una contraseña y una dirección de correo electrónico para la cuenta de administrador. Puede usar la cuenta de administrador para iniciar sesión en el menú principal del controlador de acceso y en la interfaz web.

Figura 3-1 Inicialización



The image shows a 'Device Initialization' screen with a dark background. It contains four input fields for configuration: 'Admin' (with the value 'admin'), 'PWD', 'PWD Confirm', and 'E-mail'. At the bottom, there are two buttons labeled 'Yes' and 'Clear'.

Device Initialization	
Admin	admin
PWD	
PWD Confirm	
E-mail	
Yes Clear	



- Si olvida la contraseña de administrador, envíe una solicitud de restablecimiento a su dirección de correo electrónico registrada.
- La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).

3.2 Agregar nuevos usuarios

Información de contexto



Este manual es solo de referencia. Es posible que se encuentren ligeras diferencias entre las interfaces de este manual y el dispositivo real.

Procedimiento

- Paso 1 En el **Menú principal** interfaz, seleccionar **Usuario>Nuevo**
- Paso 2 **usuario**. Configure los parámetros en la interfaz.

Figura 3-2 Nuevo usuario

The screenshot shows a 'New User' form with the following fields and values:

- User ID: 1
- Name: (empty)
- Face: 0
- Card: 0
- PWD: (empty)
- User Level: User
- Period: 255-Default
- Holiday Plan: 255-Default
- Valid Date: 2037-12-31
- User Type: General
- Use Time: Unlimited

Tabla 3-1 Descripción de los nuevos parámetros de usuario

Parámetro	Descripción
ID de usuario	Introduzca los identificadores de usuario. Los identificadores pueden ser números, letras y combinaciones de estos, y la longitud máxima del identificador es de 32 caracteres. Cada identificador es único.
Nombre	Ingrese un nombre con un máximo de 32 caracteres (incluidos números, símbolos y letras).
Rostro	Asegúrese de que su rostro esté centrado en el marco de captura de imágenes y se capturará y analizará automáticamente una imagen del rostro.

Parámetro	Descripción
Tarjeta	Un usuario puede registrar cinco tarjetas como máximo. Ingrese el número de su tarjeta o deslícela y luego el controlador de acceso leerá la información de la tarjeta. Puedes habilitar el Tarjeta de coacción Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta.  Sólo algunos modelos admiten el desbloqueo de tarjeta.
Personas con discapacidad	Introduzca la contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos.
Nivel de usuario	Puede seleccionar un nivel de usuario para los nuevos usuarios. ● Usuario: Los usuarios sólo tienen permiso de acceso a la puerta. ● Administración: Los administradores pueden desbloquear la puerta y configurar el controlador de acceso.
Período	Un usuario solo puede desbloquear la puerta dentro del período definido. El valor predeterminado es 255, lo que significa que el usuario puede desbloquear la puerta en cualquier momento.
Plan de vacaciones	Un usuario solo puede desbloquear la puerta dentro del plan de vacaciones definido. El valor predeterminado es 255, lo que significa que el usuario puede desbloquear la puerta en cualquier momento.
Fecha válida	Establecer un período durante el cual el permiso de acceso del usuario es válido.
Tipo de usuario	● General: Los usuarios generales pueden desbloquear la puerta. ● Lista de bloqueo: Cuando los usuarios en la lista de bloqueo desbloquean la puerta, el personal de servicio recibirá un aviso. ● Invitado: Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante una determinada cantidad de veces. Una vez que expire el período definido o se agote el tiempo de desbloqueo, no podrán desbloquear la puerta. ● Patrulla: Los usuarios de patrulla tendrán registrada su asistencia, pero no tendrán permisos de desbloqueo. ● personaje: Cuando el VIP desbloquee la puerta, el personal de servicio recibirá un aviso. ● Otros: Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más.
Usa el tiempo	Cuando el nivel de usuario es Invitado , establezca los tiempos máximos de acceso.

Paso 3 Grifo  para guardar la configuración.

3.3 Configuración del módulo de extensión

Si se monta un módulo de extensión en el controlador de acceso, configure primero el módulo de extensión.

Procedimiento

Paso 1 Toque la pantalla de espera.

Paso 2 Inicie sesión en el menú principal con la cuenta de administrador.

Paso 3 En el menú principal, seleccione **Características>Tipo de módulo externo**.

Paso 4 Seleccione el tipo de módulo de extensión.

Paso 5 Hacer clic **Sí**.

Después de reiniciar el dispositivo,



se muestra en la esquina superior derecha del modo de espera

pantalla, lo que significa que el módulo de extensión está configurado correctamente.

4 Operaciones web

4.1 Inicialización

Inicialice el controlador de acceso cuando inicie sesión en la página web por primera vez o después de que el controlador de acceso se restaure a los valores predeterminados de fábrica.

Prerrequisitos

Asegúrese de que la computadora utilizada para iniciar sesión en la página web esté en la misma LAN que el controlador de acceso.

Información de contexto

Establezca una contraseña y una dirección de correo electrónico antes de iniciar sesión en la página web por primera vez.

Procedimiento

Paso 1 Abra un navegador, vaya a la dirección IP (la dirección predeterminada es 192.168.1.108) del controlador de acceso.



Le recomendamos que utilice la última versión de Chrome o Firefox.

Paso 2 Establezca la contraseña y la dirección de correo electrónico de acuerdo con las instrucciones en pantalla.



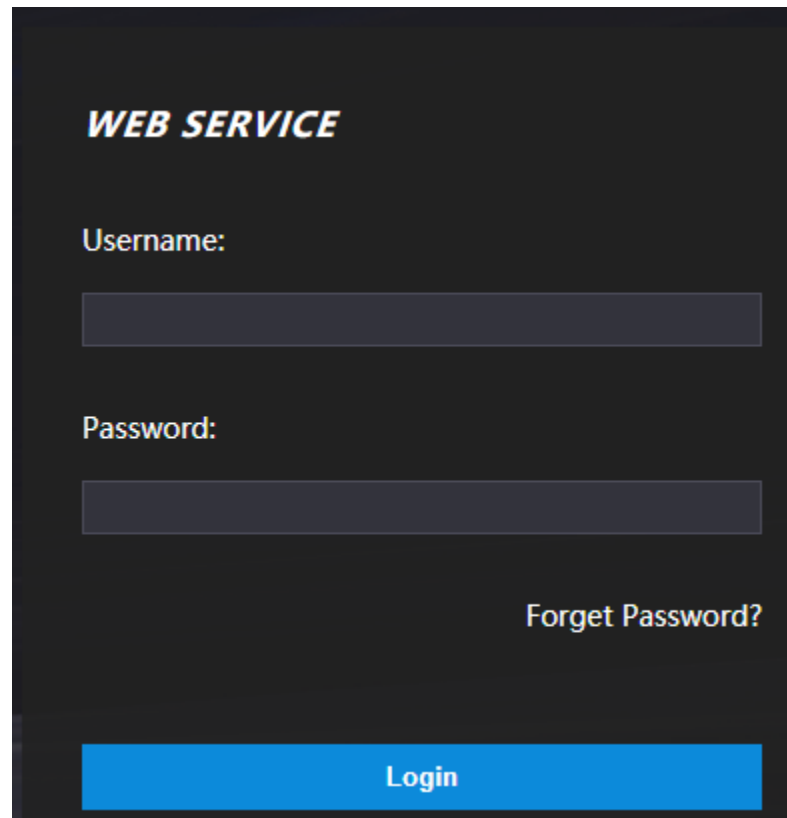
- La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &). Establezca una contraseña de alta seguridad siguiendo la contraseña Indicación de fuerza.
- Mantenga la contraseña segura después de la inicialización y cámbiela periódicamente para Mejorar la seguridad.

4.2 Iniciar sesión

Procedimiento

Paso 1 Abra un navegador, ingrese la dirección IP del Controlador de Acceso en el **DIRECCIÓN** barra y presione la tecla Enter.

Figura 4-1 Inicio de sesión



The image shows a login interface for a 'WEB SERVICE'. It has a dark background. At the top, the text 'WEB SERVICE' is displayed in a stylized, italicized font. Below this, there are two input fields: one for 'Username:' and one for 'Password:'. To the right of the password field, there is a link that says 'Forget Password?'. At the bottom of the form, there is a large blue button labeled 'Login'.

Paso 2 Introduzca el nombre de usuario y la contraseña.



- El nombre de administrador predeterminado es admin y la contraseña es la que usted configura. Durante la inicialización, le recomendamos que cambie la contraseña de administrador periódicamente. Para aumentar la seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en **¿Olvidaste tu contraseña?**.

Paso 3 Hacer clic **Acceso**.

Apéndice 1 Puntos importantes del intercomunicador

Operación

El controlador de acceso puede funcionar como VTO para realizar la función de intercomunicador.

Prerrequisitos

La función de intercomunicador se configura en el controlador de acceso y en el VTO.

Procedimiento

Paso 1 En la pantalla de espera, toque Ingresar 

Paso 2 número de habitación y luego toque .

Apéndice 2 Puntos importantes del código QR

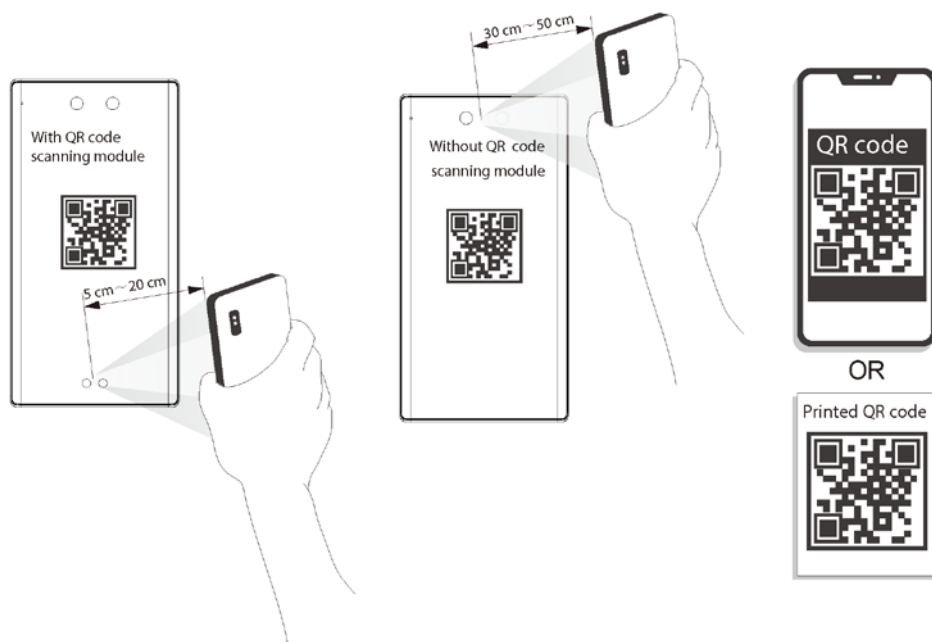
Exploración

- Controlador de acceso (con módulo de escaneo de código QR): coloque el código QR en su teléfono a una distancia de 3 cm a 5 cm de la lente de escaneo del código QR. Admite códigos QR de más de 30 mm × 30 mm - 5 cm × 5 cm y de menos de 100 bytes de tamaño.



La distancia de detección del código QR varía según los bytes y el tamaño del código QR.

Apéndice Figura 2-1 Escaneo de código QR



Apéndice 3 Instrucciones para el registro de huellas dactilares

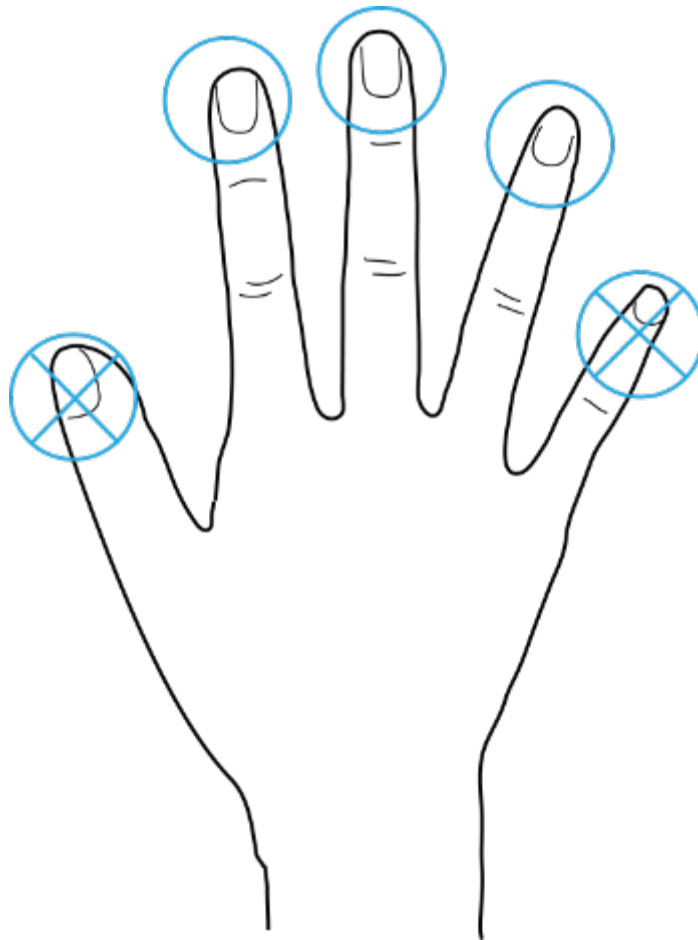
Al registrar la huella dactilar, preste atención a los siguientes puntos:

- Asegúrese de que sus dedos y la superficie del escáner estén limpios y secos.
- Presione su dedo en el centro del escáner de huellas dactilares.
- No coloque el sensor de huellas dactilares en un lugar con luz intensa, alta temperatura y alta humedad.
- Si sus huellas dactilares no están claras, utilice otros métodos de desbloqueo.

Se recomiendan los dedos

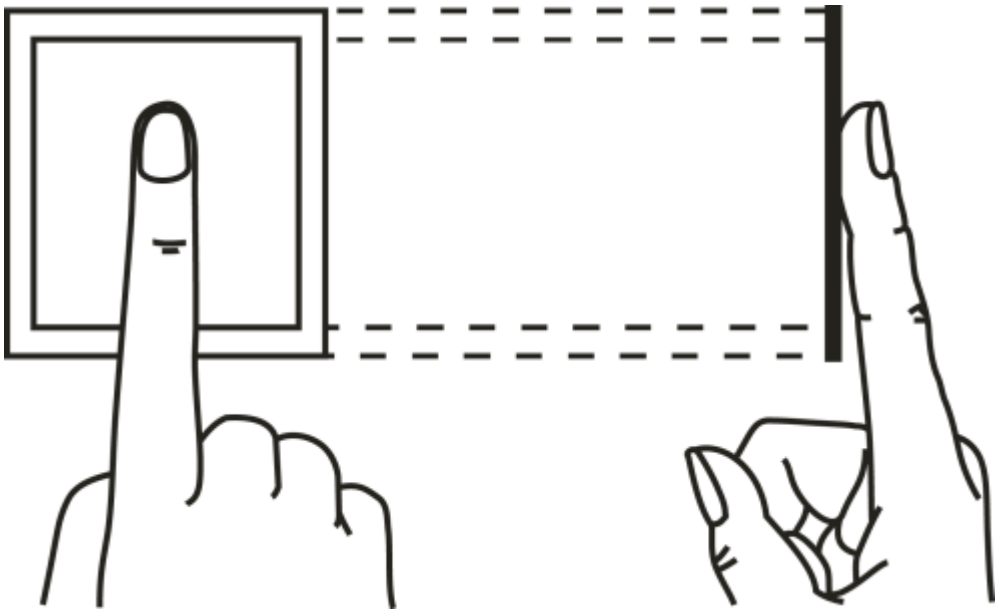
Se recomiendan los dedos índice, medio y anular. Los pulgares y meñiques no se pueden colocar fácilmente en el centro de la grabación.

Apéndice Figura 3-1 Dedos recomendados

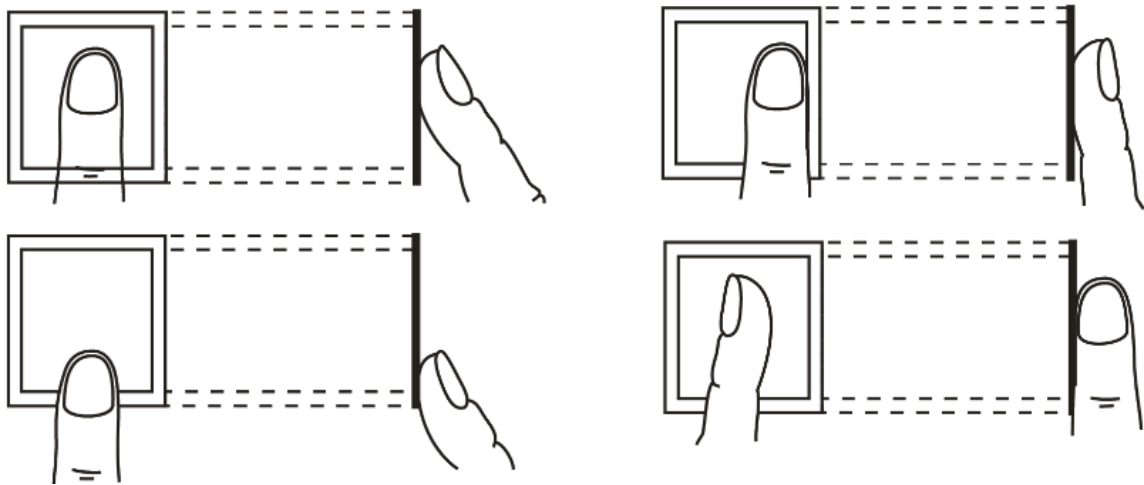


Cómo presionar su huella digital en el escáner

Apéndice Figura 3-2 Colocación correcta



Apéndice Figura 3-3 Colocación incorrecta



Apéndice 4 Puntos importantes del registro facial

Antes de la inscripción

- Las gafas, los sombreros y las barbas podrían influir en el rendimiento del reconocimiento facial.
- No te cubras las cejas cuando uses sombrero.
- No cambie mucho su estilo de barba si usa el dispositivo; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el dispositivo al menos a 2 metros de distancia de fuentes de luz y al menos a 3 metros de ventanas o puertas; de lo contrario, la luz de fondo y la luz solar directa podrían influir en el rendimiento de reconocimiento facial del controlador de acceso.

Durante el registro

- Puedes registrar rostros a través del Dispositivo o a través de la plataforma. Para el registro a través de la plataforma, consulta el manual de usuario de la plataforma.
- Centra tu cabeza en el marco de captura de fotos. La imagen de tu rostro se capturará automáticamente.



- No mueva la cabeza ni el cuerpo, de lo contrario el registro podría fallar.
- Evite que aparezcan 2 caras en el cuadro de captura al mismo tiempo.

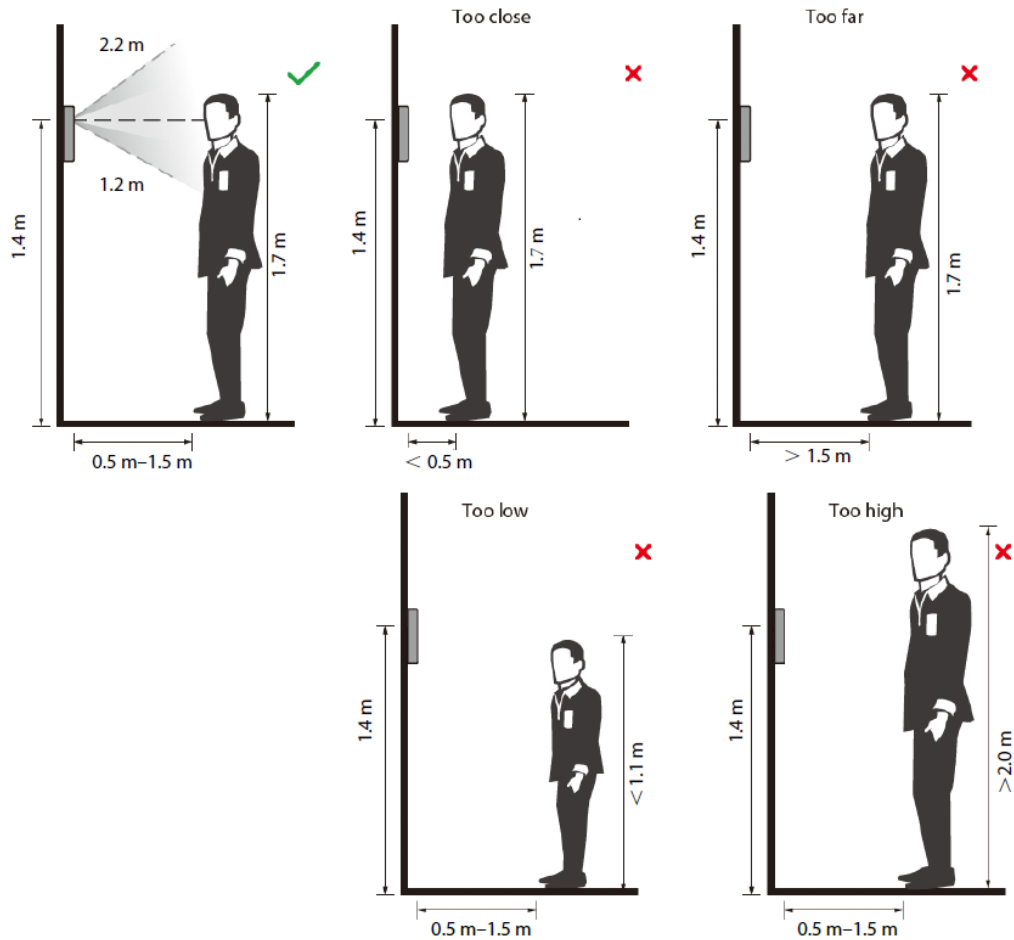
Posición de la cara

Si su cara no está en la posición adecuada, la precisión del reconocimiento facial podría verse afectada.



La posición de la cara que se muestra a continuación es solo de referencia y puede diferir de la situación real.

Apéndice Figura 4-1 Posición adecuada de la cara



Requisitos de las caras

- Asegúrese de que la cara esté limpia y la frente no esté cubierta de pelo.
- No use gafas, sombreros, barbas pobladas ni otros adornos faciales que influyan en la grabación de imágenes del rostro.
- Con los ojos abiertos, sin expresiones faciales y dirigiendo la cara hacia el centro de la cámara.
- Al grabar su rostro o durante el reconocimiento facial, no mantenga su rostro demasiado cerca ni demasiado lejos de la cámara.

Apéndice Figura 4-2 Posición de la cabeza





- Al importar imágenes de rostros a través de la plataforma de administración, asegúrese de que la imagen
La resolución está dentro del rango de 150 × 300 píxeles a 600 × 1200 píxeles. Se recomienda que
La resolución debe ser mayor a 500 × 500 píxeles, el tamaño de la imagen debe ser menor a 100 KB y
El nombre de la imagen y la identificación de la persona deben ser los mismos.
- Asegúrese de que el rostro ocupe más de 1/3 pero no más de 2/3 del área total de la imagen.
y la relación de aspecto no exceda de 1:2.

Apéndice 5 Recomendaciones de seguridad

Gestión de cuentas

1. Utilice contraseñas complejas

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Cambie las contraseñas periódicamente

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que sea adivinada o descifrada.

3. Asignar cuentas y permisos de forma adecuada

Agregue usuarios de forma adecuada según los requisitos de servicio y administración y asigne conjuntos de permisos mínimos a los usuarios.

4. Habilitar la función de bloqueo de cuenta

La función de bloqueo de cuenta está habilitada de forma predeterminada. Se recomienda mantenerla habilitada para proteger la seguridad de la cuenta. Después de varios intentos fallidos de ingresar la contraseña, se bloquearán la cuenta correspondiente y la dirección IP de origen.

5. Establecer y actualizar la información de restablecimiento de contraseña de manera oportuna

El dispositivo admite la función de restablecimiento de contraseña. Para reducir el riesgo de que esta función sea utilizada por actores maliciosos, si hay algún cambio en la información, modifíquela a tiempo. Al configurar las preguntas de seguridad, se recomienda no utilizar respuestas fáciles de adivinar.

Configuración del servicio

1. Habilitar HTTPS

Se recomienda que habilite HTTPS para acceder a servicios web a través de canales seguros.

2. Transmisión cifrada de audio y vídeo

Si el contenido de sus datos de audio y video es muy importante o confidencial, se recomienda utilizar la función de transmisión encriptada para reducir el riesgo de que sus datos de audio y video sean espiados durante la transmisión.

3. Desactiva los servicios no esenciales y utiliza el modo seguro

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, AP hotspot, etc., para reducir las superficies de ataque.

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

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

4. Cambiar HTTP y otros puertos de servicio predeterminados

Se recomienda cambiar el puerto predeterminado de HTTP y otros servicios a cualquier puerto entre 1024 y 65535 para reducir el riesgo de ser adivinado por actores de amenazas.

Configuración de red

1. Habilitar lista de permitidos

Se recomienda activar la función de lista de permitidos y permitir que solo las direcciones IP de la lista de permitidos accedan al dispositivo. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del dispositivo compatible a la lista de permitidos.

2. Vinculación de dirección MAC

Se recomienda vincular la dirección IP de la puerta de enlace a la dirección MAC del dispositivo para reducir el riesgo de suplantación de ARP.

3. Construir un entorno de red seguro

Para garantizar mejor la seguridad de los dispositivos y reducir los posibles riesgos cibernéticos, se recomienda lo siguiente:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde la red externa;
- De acuerdo con las necesidades reales de la red, particione la red: si no hay demanda de comunicación entre las dos subredes, se recomienda utilizar VLAN, puerta de enlace y otros métodos para particionar la red para lograr el aislamiento de la red;
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal a terminales de la red privada.

Auditoría de seguridad

1. Comprobar usuarios en línea

Se recomienda revisar periódicamente a los usuarios en línea para identificar usuarios ilegales.

2. Comprobar el registro del dispositivo

Al ver los registros, puede obtener información sobre las direcciones IP que intentan iniciar sesión en el dispositivo y las operaciones clave de los usuarios registrados.

3. Configurar el registro de red

Debido a la capacidad de almacenamiento limitada de los dispositivos, el registro almacenado es limitado. Si necesita guardar el registro durante un período prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos se sincronicen con el servidor de registro de red para realizar el seguimiento.

Seguridad del software

1. Actualizar el firmware a tiempo

De acuerdo con las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión a tiempo para garantizar que el dispositivo tenga las últimas funciones y seguridad. Si el dispositivo está conectado a la red pública, se recomienda habilitar la función de detección automática de actualizaciones en línea, para obtener la información de actualización de firmware publicada por el fabricante de manera oportuna.

2. Actualice el software del cliente a tiempo

Se recomienda descargar y utilizar el software de cliente más reciente.

Protección física

Se recomienda realizar protección física para los dispositivos (especialmente los dispositivos de almacenamiento), como colocar el dispositivo en una sala de máquinas y un gabinete dedicados, y tener control de acceso y administración de claves para evitar que personal no autorizado dañe el hardware y otros equipos periféricos (por ejemplo, disco flash USB, puerto serial).