Acceso independiente

Manual de usuario

V1.0.1

Prefacio

General

Este manual presenta la instalación y las operaciones básicas de Access Standalone (en lo sucesivo, "el Dispositivo").

Las instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Sentido
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, reducción del rendimiento o resultados impredecibles.
CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrar tiempo.
NOTA	Proporciona información adicional como suplemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.1	Se actualizaron las configuraciones del lector de tarjetas.	octubre 2021
V1.0.0	Primer lanzamiento	septiembre 2021

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 la prevención de daños a la propiedad. Lea atentamente antes de usar el dispositivo, cumpla con las pautas cuando lo use y guarde el manual en un lugar seguro para futuras consultas.

Requisitos de transporte

Transporte el Dispositivo en condiciones de humedad y temperatura permitidas.

Requisitos de almacenamiento

Guarde el dispositivo en condiciones de humedad y temperatura permitidas.

requerimientos de instalación

 **ADVERTENCIA**

- Conecte el dispositivo al adaptador antes de encenderlo.
- Cumpla estrictamente con las normas locales de seguridad eléctrica y asegúrese de que el voltaje en el área sea constante y cumpla con los requisitos de energía del dispositivo.
- No conecte el dispositivo a más de una fuente de alimentación. De lo contrario, el dispositivo podría dañarse.

- Observe todos los procedimientos de seguridad y use el equipo de protección requerido proporcionado para su uso mientras trabaja en alturas.
- Mantenga el dispositivo en un lugar estable para evitar que se caiga. No
- exponga el dispositivo a la luz solar directa ni a fuentes de calor. No
- instale el dispositivo en lugares húmedos, polvorientos o con humo.
- Instale el dispositivo en un lugar bien ventilado y no bloquee el ventilador del dispositivo. Utilice el adaptador de
- corriente o la fuente de alimentación de la carcasa proporcionada por el fabricante del dispositivo.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del dispositivo. Conecte los aparatos eléctricos
- de clase I a una toma de corriente con puesta a tierra de protección.

Requisitos operativos

- Asegúrese de que la fuente de alimentación del Dispositivo funcione correctamente antes de su
- uso. No extraiga el cable de alimentación del dispositivo mientras esté encendido.
- Utilice el dispositivo únicamente dentro del rango de potencia nominal.
- Utilice el dispositivo en condiciones de humedad y temperatura permitidas.
- Evite que los líquidos salpiquen o goteen sobre el dispositivo. Asegúrese de que no haya objetos llenos de líquido encima del dispositivo para evitar que fluyan líquidos hacia él.
- No desmonte el Dispositivo.

Tabla de contenido

1 Descripción general del producto

1.1 Introducción

Integrado con un potente procesador y un algoritmo de aprendizaje profundo, el dispositivo puede identificar huellas dactilares de forma instantánea y precisa. El Dispositivo también admite el desbloqueo de la puerta mediante tarjetas, contraseñas, huellas dactilares o sus combinaciones. Para satisfacer diferentes necesidades, también funciona con un software de gestión para realizar más funciones.

La función de huella digital está disponible en modelos selectos.

1.2 Características

- Pantalla LCD.
- Panel de PC + ABS/acrílico apto para exteriores.
- Admite modos de lector de tarjetas y controlador para adaptarse a diferentes situaciones.
- Admite el desbloqueo de la puerta de forma remota en SmartPSS AC, o mediante tarjetas, contraseñas, huellas dactilares o sus combinaciones.
- Admite múltiples tipos de alarma, como coacción, intrusión y manipulación.
- Admite varios tipos de usuarios, incluidos invitados, patrullas, listas de bloqueo, VIP, usuarios normales y otros tipos de usuarios.
- Puede iniciar sesión en el navegador web con una PC o un teléfono.
- Soporta timbre de puerta.
- Funciona con SmartPSS AC yDSS Pro.

1.3 Dimensiones

Figure 1-1 Dimensiones (1) (mm [pulgadas])

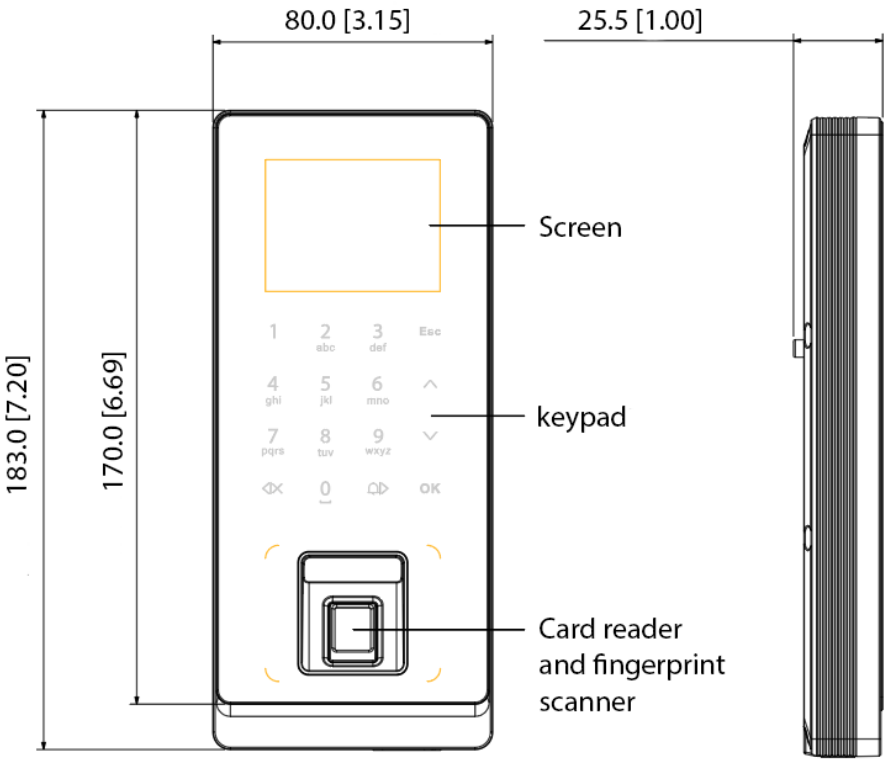
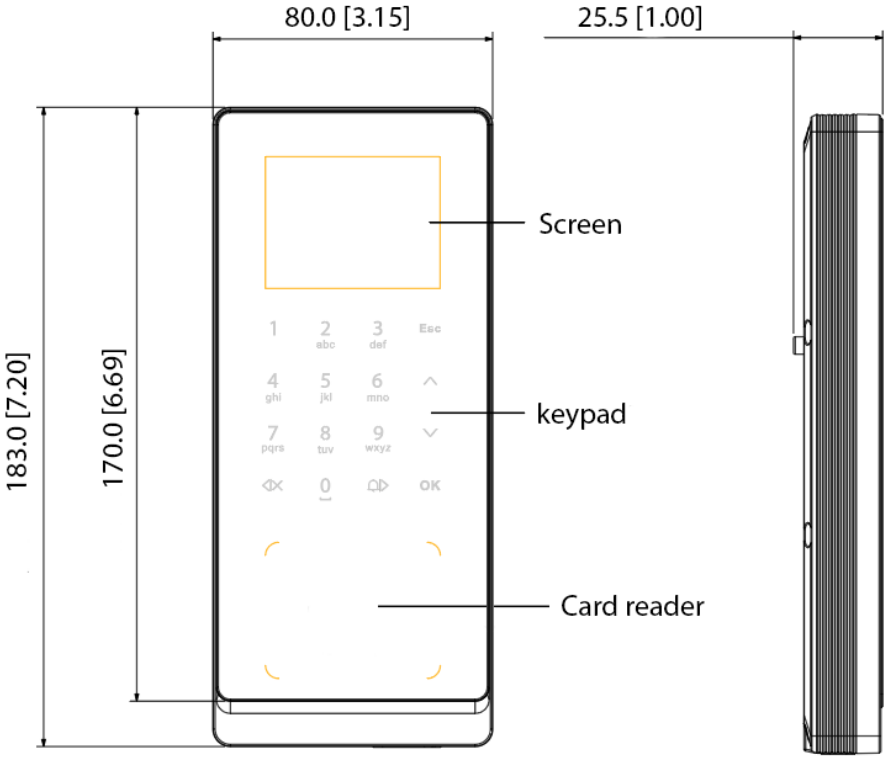


Figure 1-2 Dimensiones (2) (mm [pulgadas])

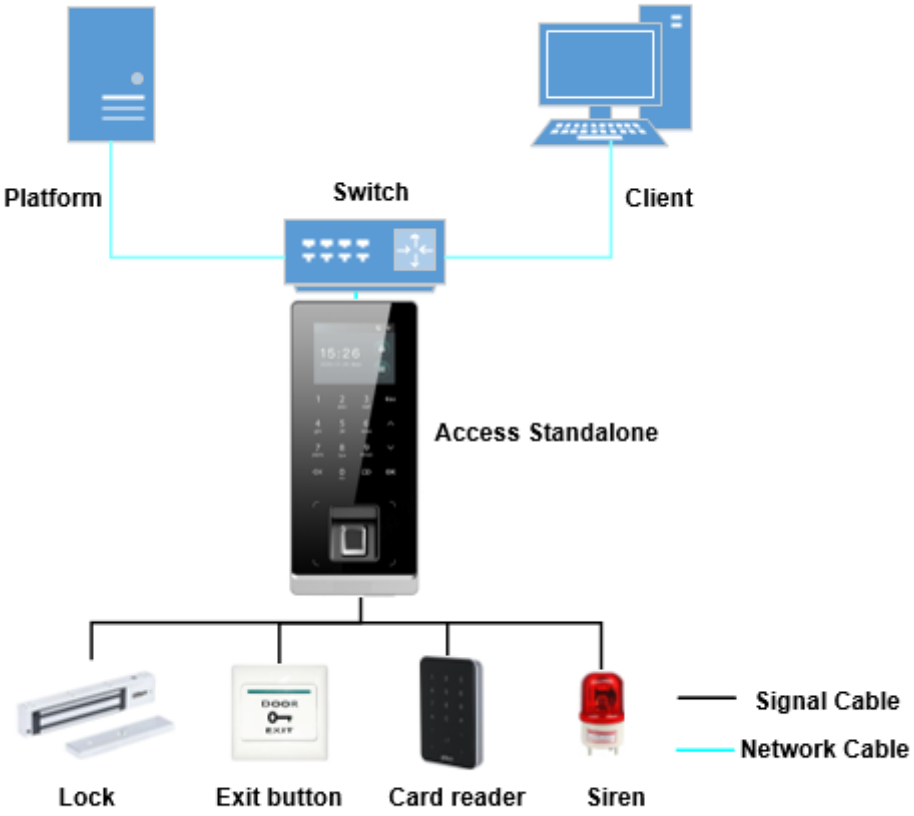


1.4 Solicitud

El Dispositivo es aplicable a una variedad de escenarios, como edificios de oficinas, escuelas, parques industriales, complejos de apartamentos, fábricas, estadios públicos y centros de negocios. Este manual de usuario describe principalmente el dispositivo con la función de huella digital en el modo de controlador.

El manual del usuario es solo para referencia y puede diferir del producto real.

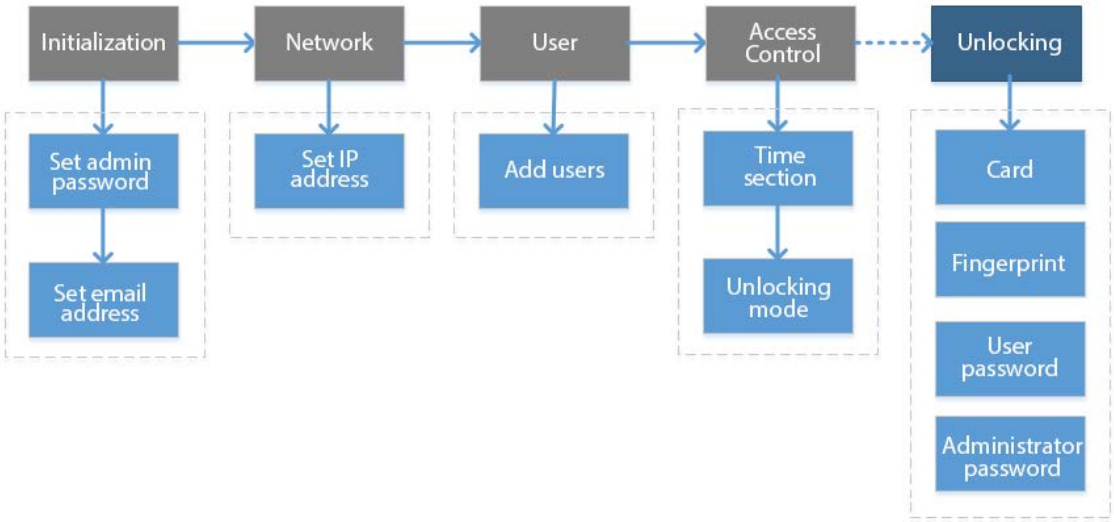
Figure 1-3 Diagrama de Red



2 Configuración local

2.1 Proceso de configuración

Figure 2-1 Flujo de trabajo de configuración



2.2 Función del teclado

Tabla 2-1 Descripción del teclado

Articulo	Descripción
Número o carta	Se utiliza para ingresar información o contraseña.
∧	Navega por la página.
∨	
Esc	Cancelar una operación o volver a la página anterior.
OK	Vaya a la página seleccionada o confirme su cambio.
	Vaya a la página de inicio de sesión del administrador.
	Retroceso.
	Toque el timbre (solo en la página de espera), navegue por la página o cambie el método de entrada.

2.3 Inicialización

Para el uso por primera vez o después de restaurar los valores predeterminados de fábrica, debe establecer una contraseña y asociar su dirección de correo electrónico para la cuenta de administrador. También debe configurar la zona horaria del dispositivo. Puedes usar el

cuenta de administrador para iniciar sesión en el menú principal del dispositivo, configurar el dispositivo e iniciar sesión en el navegador web y SmartPSS AC.

Figure 2-2 Inicialización

- Si olvida la contraseña de administrador, envíe una solicitud de restablecimiento a su dirección de correo electrónico asociada.
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo el indicador de seguridad de la contraseña.

2.4 Pantalla de espera

Puede desbloquear la puerta en la página de espera con su tarjeta, contraseña o huella digital.

- El dispositivo vuelve a la página de espera si no se realiza ninguna operación en 30 segundos.
- El dispositivo apaga la pantalla si permanece en la página de espera durante 30 segundos.
- La pantalla en el manual del usuario es solo para referencia.

Figure 2-3 pantalla de espera

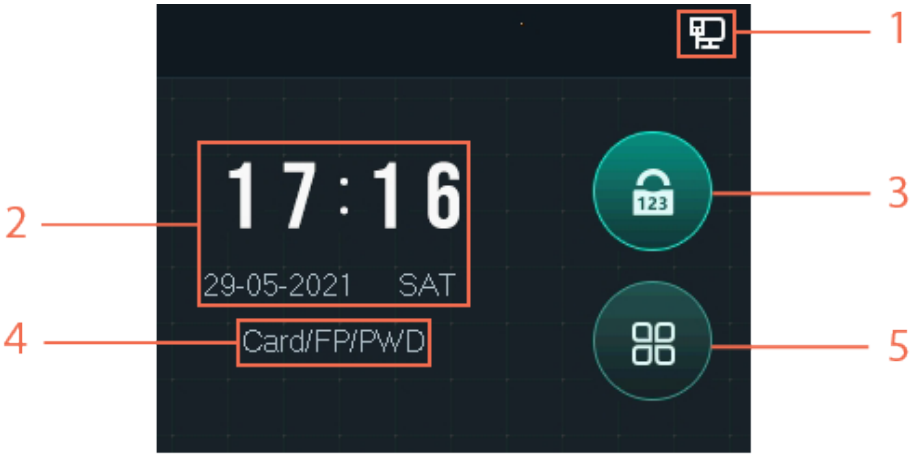


Tabla 2-2 Descripción de la página de espera

No.	Articulo	Descripción
1	Estado	Muestra el estado de Wi-Fi, la red cableada (si existe) y la unidad USB.
2	Fecha y hora	Hora y fecha.

No.	Articulo	Descripción
3	Desbloquear el puerta con clave	Ingrese la ID de usuario y la contraseña, o la contraseña del administrador (para obtener más información, consulte "2.6.4 Contraseña del administrador") para desbloquear la puerta.
4	Desbloqueo métodos	Muestra los métodos de desbloqueo que configuró.
5	Menú principal	Grifo para entrar en el menú principal. Solo administradores y usuarios con permiso de administrador puede iniciar sesión en el menú principal. Consulte "2.5 Inicio de sesión en el menú principal".

2.5 Iniciar sesión en el menú principal

Inicie sesión en el menú principal para configurar los parámetros del dispositivo. Por ejemplo, puede agregar usuarios de diferentes permisos y cambiar el modo de desbloqueo.

Solo el administrador y los usuarios administradores pueden iniciar sesión en el menú principal.

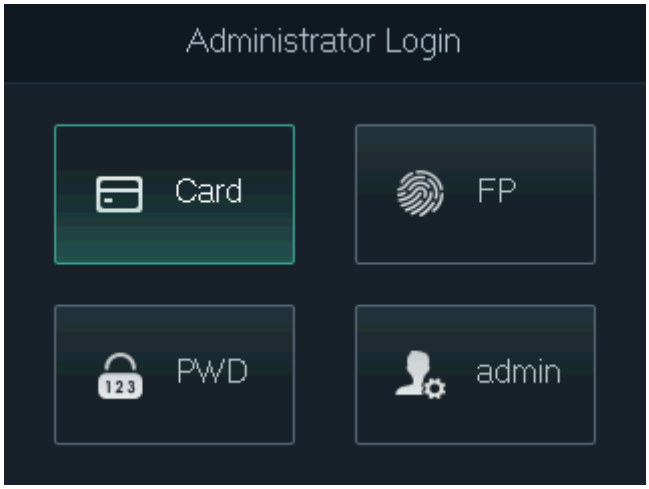
Step 1 En la pantalla de espera, toque .

Los métodos de verificación varían según el tipo de dispositivo.

Step 2 Inicie sesión en el menú principal.

- Inicie sesión como usuario con permiso de administrador utilizando una tarjeta, huella digital o contraseña.
- Iniciar sesión como**administración**: Grifo**administración**y luego ingrese la contraseña que configuró durante la inicialización.

Figure 2-4 Iniciar sesión como administrador



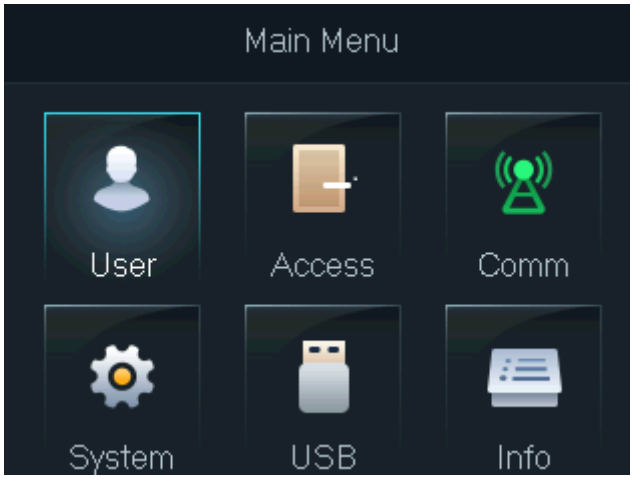
Step 3 En el menú principal, toque∧/∨para navegar por la página y luego toque**OK**para configurar los parámetros del Dispositivo.

Use los accesos directos para configurar parámetros simplemente tocando 1–6.

- Para configurar la gestión de usuarios, toque 1.
- Para configurar el control de acceso, toque 2.
- Para configurar la comunicación, toque 3.

- Para configurar el sistema, toque 4.
- Para configurar USB, toque 5.
- Para ver la información del sistema, toque 6.

Figure 2-5 Menú principal



2.6 Métodos de desbloqueo

2.6.1 Tarjeta

Pase su tarjeta para desbloquear la puerta.

Para la función Access Standalone with ID, si está conectado con un lector de tarjetas ID externo, el La distancia entre Access Standalone y el lector de tarjetas debe ser superior a 10 cm. De lo contrario, el lector de tarjetas podría funcionar mal porque está demasiado cerca del Access Standalone.

2.6.2 Huella digital

Presione su huella dactilar registrada en el escáner de huellas dactilares para desbloquear la puerta.

2.6.3 Contraseña de usuario

Introduzca el ID de usuario y la contraseña para desbloquear la puerta.

Step 1 Toque en la página de espera.

Step 2 Seleccione**PCD**y luego toque**OK**. Introduzca

Step 3 el ID de usuario y la contraseña.

- Para ingresar la ID de usuario, debe seleccionar el cuadro de entrada de ID de usuario y tocar**OK**.
- Puede introducir directamente la contraseña en el teclado.
- Grifo para cambiar el método de entrada.

Step 4 Seleccione**OK**y luego toque**OK**.

El sistema indicará que la puerta está desbloqueada.

2.6.4 Contraseña de administrador

Después de configurar su contraseña de administrador y habilitarla, puede desbloquear la puerta simplemente ingresando la contraseña de administrador. Uso de la contraseña de administrador para desbloquear la puerta sin estar sujeto a niveles de usuario, modos de desbloqueo, períodos, planes de vacaciones y anti-passback, excepto para puertas normalmente cerradas.

El dispositivo solo permite una contraseña de administrador.

Para usar la contraseña de administrador para el acceso a la puerta, debe habilitar la función. Ver "2.7.3 Configuración de la contraseña de administrador".

Step 1 Seleccione en la pantalla de espera.

Step 2 Seleccione**PCD del administrador**y luego toque

Step 3 **OK**. Introduzca la contraseña de administrador.

Step 4 Seleccione**OK**y luego toque**OK**. La puerta está desbloqueada.

2.7 Gestión de usuarios

Puede agregar nuevos usuarios, ver la lista de usuarios, la lista de administradores y modificar la supercontraseña en la**Usuario** pantalla.

2.7.1 Agregar nuevo usuario

Step 1 Seleccione en la pantalla de espera y luego toque**OK**.

Step 2 Inicie sesión con la cuenta de administrador y luego seleccione**Usuario > Nuevo Usuario**.

Las pantallas de este manual son solo de referencia y pueden diferir del producto real.

Figure 2-6 Agregar un nuevo usuario

Step 3 Configure los parámetros.

Tabla 2-3 Descripción de los parámetros de usuario

Parámetro	Descripción
IDENTIFICACIÓN	Cada ID de usuario es único. Puede ser de 18 caracteres de números, letras o su combinación.
Nombre	Introduzca el nombre (un máximo de 32 caracteres, incluidos números, símbolos y letras).
Huella dactilar	Cada usuario puede agregar hasta 3 huellas dactilares. Siga las indicaciones en pantalla y las indicaciones de voz para agregar huellas dactilares. Puede habilitar la función de huella digital bajo coacción debajo de cada huella digital. Después de habilitar la función de alarma de coacción, se activará una alarma si la puerta se desbloquea con la huella dactilar de coacción. - No recomendamos configurar la primera huella digital como huella digital de coacción. - Solo ciertos modelos admiten la función de huella digital.
Tarjeta	Puede registrar cinco tarjetas para cada usuario. En la página de registro de la tarjeta, deslice su tarjeta en el lector de tarjetas y luego el Dispositivo leerá la información de la tarjeta. Puede habilitar la función de tarjeta de coacción en la página de registro de la tarjeta. Una vez habilitada la función de alarma de coacción, se activará una alarma si la tarjeta de coacción desbloquea la puerta.
PCD	Introduzca la contraseña para desbloquear la puerta. La longitud máxima de los dígitos de identificación es 8.
Permiso	Puede seleccionar un permiso de usuario para el nuevo usuario. ● Los usuarios normales solo tienen permiso de desbloqueo de puertas. Los ● administradores pueden configurar el dispositivo y desbloquear la puerta.
Período	Un usuario solo puede tener acceso a la puerta dentro del período definido. El valor predeterminado es 255, lo que significa que no se configura ningún período.
Plan de vacaciones	Un usuario solo puede tener acceso a la puerta dentro de los días festivos programados. El valor predeterminado es 255, lo que significa que no se ha configurado ningún plan de vacaciones.
Fecha válida	Defina un período durante el cual el usuario tiene control de acceso a la puerta.
Tipo de usuario	● **General**: Los usuarios generales pueden desbloquear la puerta normalmente. ● **Lista de bloqueos**: cuando los usuarios de la lista de bloqueo desbloquean la puerta, el personal de servicio recibe una notificación. ● **Huésped**: Los invitados pueden desbloquear la puerta dentro de un período definido o por un cierto número de veces. Después de que vence el período definido o se agotan los tiempos de desbloqueo, no pueden desbloquear la puerta. ● **Patrulla**: Los usuarios de libertad condicional pueden hacer un seguimiento de su asistencia, pero no tienen permisos de desbloqueo. ● **VIP**: Cuando el VIP desbloquee la puerta, el personal de servicio recibirá una notificación. El usuario VIP no está restringido por modos de desbloqueo, como**multitarjeta**y **Sección de tiempo**. ● **Otros**: Cuando desbloqueen la puerta, la puerta permanecerá desbloqueada durante 5 segundos más. ● **Usuario personalizado 1/2**: Igual que**General**.

Step 4 Después de haber configurado todos los parámetros, toque**Esc**. Grifo

Step 5 **OK**para guardar los cambios.

2.7.2 Lista de usuarios/administradores

Puede ver y buscar todos los usuarios generales y usuarios administradores, y editar la información del usuario.

En el menú principal, seleccione**Usuario > Lista de usuarios/Lista de administradores**.

Figure 2-7 Lista de usuarios

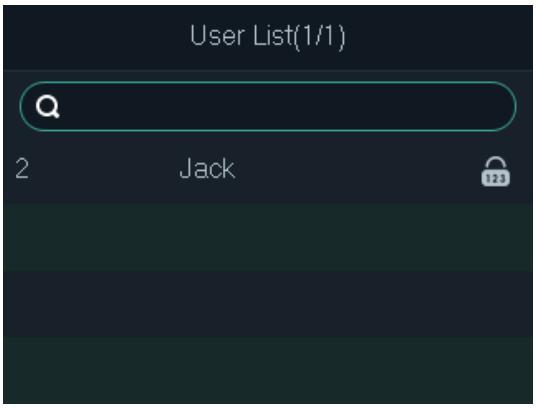
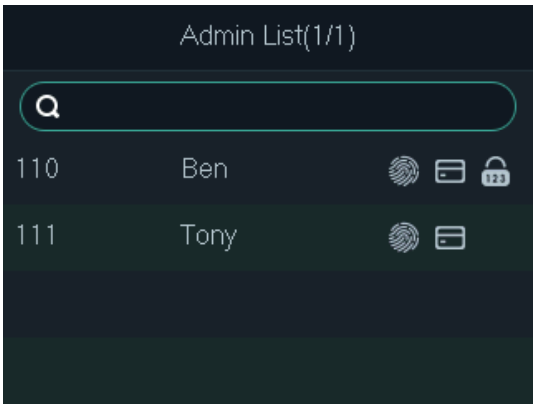


Figure 2-8 Lista de administradores



- Método de desbloqueo
  - ◇ : Huella dactilar.
  - ◇ : Tarjeta.
  - ◇ : Clave.

Edición de la información del usuario

Step 1 Seleccione el usuario y toque**OK**.

Step 2 Edite la información del usuario.

Step 3 Grifo**Esc**.

Step 4 Grifo**OK**para guardar los cambios.

Búsqueda de usuarios

Step 1 Seleccione y toque**OK**.

Step 2 Ingrese la ID de usuario, deslice una tarjeta o presione una huella digital para buscar al usuario.

Eliminación de usuarios

Seleccione el usuario, toque**OK**y luego seleccione  para eliminar el usuario.

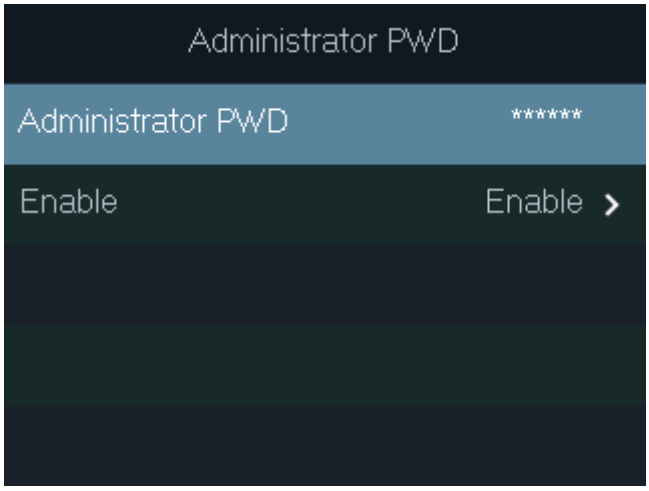
2.7.3 Configuración de la contraseña de administrador

El dispositivo permite solo una contraseña de administrador. Puede usarlo para desbloquear la puerta sin ingresar la ID de usuario.

Step 1 En el menú principal, seleccione**Usuario > Administrador PWD**.

Step 2 Ingrese la contraseña del administrador y luego toque**OK**.

Figure 2-9 Contraseña de administrador

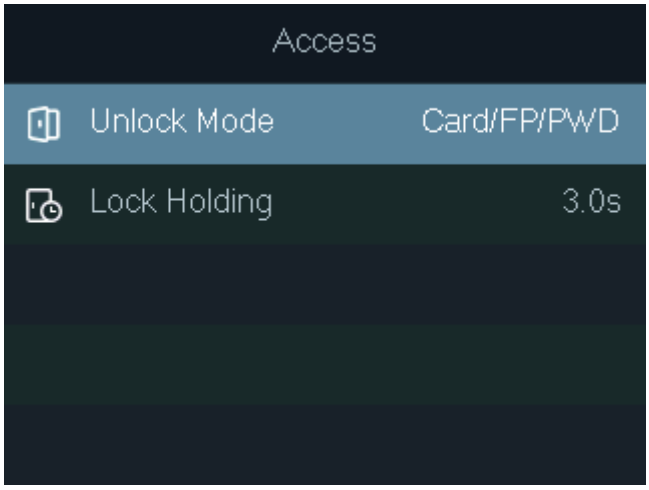


Step 3 Seleccione**Habilitar**y luego toque**OK**para habilitar la función.

2.8 Gestión de control de acceso

Configure el modo de desbloqueo y la duración del desbloqueo.

Figure 2-10 Gestión de control de acceso



2.8.1 Configuración del modo de desbloqueo

Configura las combinaciones de desbloqueo. Los métodos de desbloqueo varían con los diferentes tipos de dispositivos.

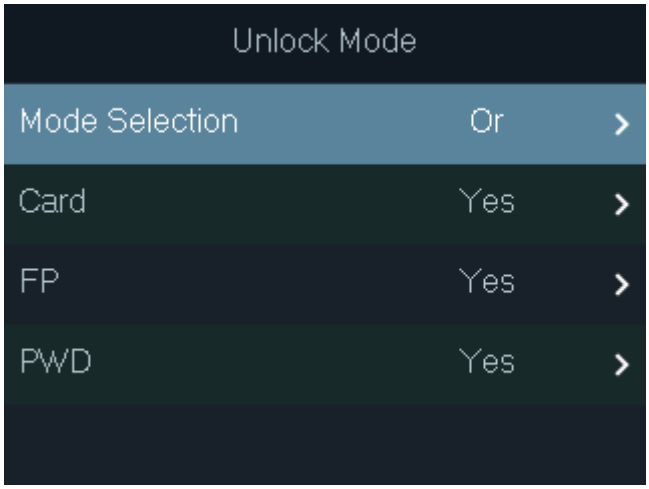
Use tarjeta, huella digital, contraseña o cualquiera de sus combinaciones para desbloquear la puerta.

Step 1 En el menú principal, seleccione**Acceso > Modo de desbloqueo**y luego toque**OK**.

Step 2 Grifo**OK**para configurar las combinaciones de desbloqueo.

- **Y**: Debe verificar todos los métodos de desbloqueo seleccionados para abrir la puerta. **O**:
- Puede verificar uno de los métodos de desbloqueo seleccionados para abrir la puerta.

Figure 2-11 Elemento (opción múltiple)



Step 3 Grifo**Esc**.

Step 4 Grifo**OK**para guardar los cambios.

2.8.2 Configuración del tiempo de retención de bloqueo

La puerta permanecerá desbloqueada durante el período definido.

Step 1 En el menú principal, seleccione**Acceso > Retención de bloqueo**. Grifo

Step 2 **OK**y, a continuación, introduzca la hora.

Grifo para cambiar el método de entrada.

2.9 Comunicación

Configure los parámetros de red, puerto serie y puerto Wiegand para conectar el dispositivo a la red u otros dispositivos.

2.9.1 Configuración de IP

Configure la dirección IP del dispositivo para conectarlo a la red. Después de eso, puede iniciar sesión en el portal web para configurar el dispositivo y agregarlo a SmartPSS AC.

Step 1 En el menú principal, seleccione**Comunicación > Dirección IP**y luego toque**OK**.

Step 2 Seleccione**Dirección IP**y toque**OK**para configurar parámetros.

Figure 2-12 Configurar IP

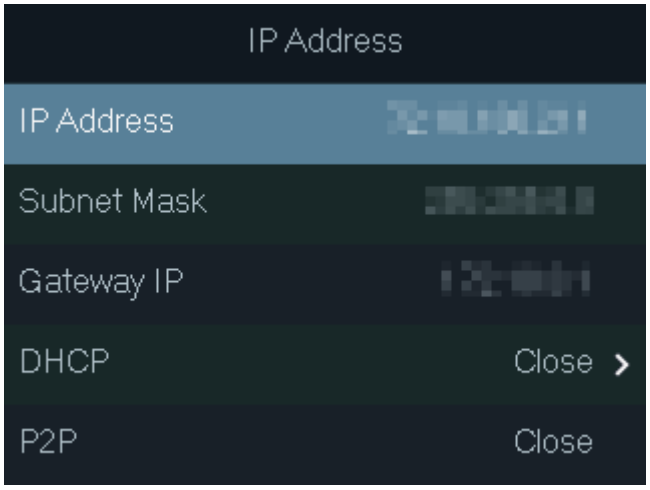


Tabla 2-4 Descripción de los parámetros de red

Parámetro	Descripción
Dirección IP, máscara de subred y puerta de enlace	La dirección IP, la máscara de subred y la dirección IP de la puerta de enlace deben estar en el mismo segmento de red. Grifo**Esc**para guardar las configuraciones.
DHCP	Significa Protocolo de configuración dinámica de host. Cuando está habilitado, el dispositivo obtendrá automáticamente una dirección IP.
P2P	Cuando está habilitado, puede administrar directamente el dispositivo sin un dominio dinámico, un servidor de retransmisión o una asignación de puertos.

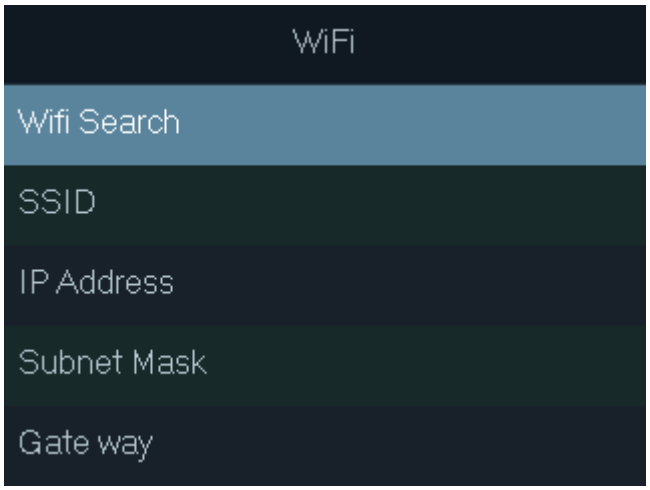
2.9.2 Configuración de WiFi

Conecte el dispositivo a una red inalámbrica.

Solo ciertos modelos admiten Wi-Fi.

Step 1 En el menú principal, seleccione**Comunicación > Wi-Fi**y luego toque**OK**.

Figure 2-13 Wifi



Step 2 Seleccione**Búsqueda Wifi**y luego toque**OK**.

Step 3 Seleccione**Wifi**y luego toque**OK**para habilitar la función Wi-Fi.

El dispositivo buscará y mostrará las redes inalámbricas disponibles.

Grifo O para ir a la página anterior o siguiente.

Step 4 Seleccione una red inalámbrica, toque**OK**e ingrese la contraseña.

2.9.3 Configuración de Wiegand

Configure la entrada o salida Wiegand para conectar un lector de tarjetas o un controlador de acceso. En el menú principal, seleccione**Comunicación > Wiegand**y luego toque**OK**.

- Seleccione**Entrada Wiegand**cuando necesite conectar un lector de tarjetas al Dispositivo.
- Seleccione**Salida Wiegand**cuando el dispositivo funciona como un lector de tarjetas y necesita conectarlo a otro controlador de acceso.

Figure 2-14 Wiegand

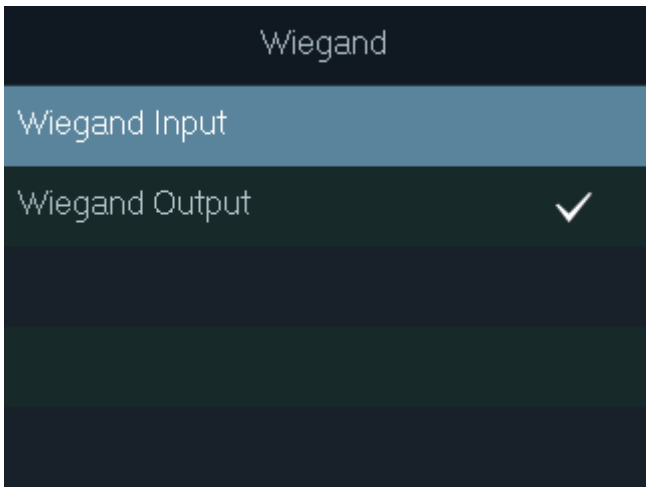


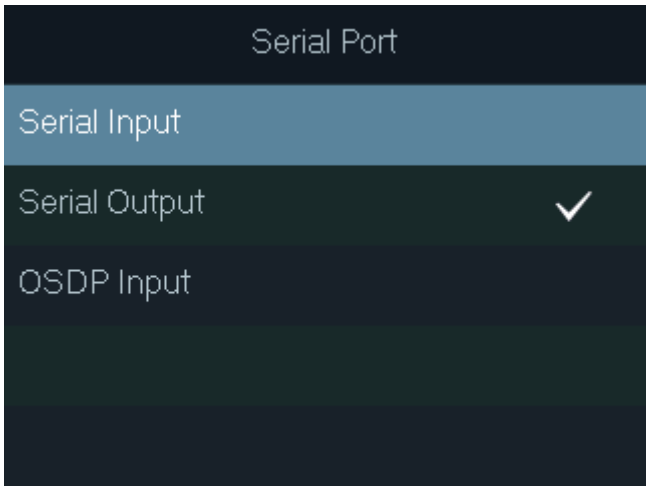
Tabla 2-5 Descripción de los parámetros de Wiegand

Parámetro	Descripción
Tipo de salida	Seleccione un formato Wiegand para leer números de tarjeta o números de identificación. ● **Wiegand26**: Lee 3 bytes o 6 dígitos. ● **Wiegand34**: Lee 4 bytes u 8 dígitos. ● **Wiegand66**: Lee 8 bytes o 16 dígitos.
Ancho de pulso	Introduzca el valor.
Intervalo de pulso	
Tipo de datos de salida	● **ID de usuario**: emite la ID del usuario que desliza una tarjeta. **número** ● **de tarjeta**: Muestra el número de tarjeta que se utiliza.

2.9.4 Configuración del puerto serie

En el menú principal, seleccione**Comunicaciones > Puerto serie**y luego toque**OK**.

Figure 2-15 Configuración del puerto serie



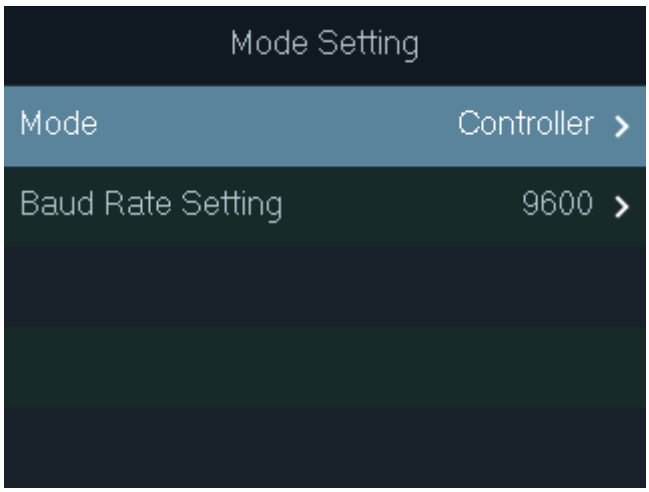
- Seleccione**Entrada en serie**cuando el dispositivo se conecta a un lector de tarjetas. El lector de tarjetas enviará el número de tarjeta al Dispositivo o SmartPSS AC.
- Seleccione**Salida en serie**cuando el Dispositivo funciona como un lector de tarjetas. El dispositivo enviará el número de tarjeta al controlador y el controlador controlará el acceso a la puerta.
  - ◇ **ID de usuario**: emite la ID del usuario que desliza una tarjeta. **número**
  - ◇ **de tarjeta**: Muestra el número de tarjeta que se utiliza.
- Seleccione**Entrada OSDP**cuando el Dispositivo conecta un lector de tarjetas a través del protocolo OSDP. El lector de tarjetas enviará la información de la tarjeta al Dispositivo o SmartPSS AC.

2.9.5 Modo de configuración

El dispositivo puede funcionar como un controlador o un lector de tarjetas.

En el menú principal, seleccione**Com > Configuración de modo**.

Figure 2-16 Configuración del puerto serie



- Modo
  - ◇ **Controlador**: El dispositivo funciona como un controlador de acceso. Puede conectarlo a un lector de tarjetas y el lector de tarjetas envía la información de la tarjeta al dispositivo o SmartPSS AC.
  - ◇ **Lector de tarjetas**: El Dispositivo funciona como un lector de tarjetas y se puede conectar a un controlador u otro acceso independiente.

    - La entrada del puerto serie no se puede configurar en el modo de lector de tarjetas.

- Para el modo de lector de tarjetas, consulte el método de cableado de un lector de tarjetas. Puedes conectarte el Dispositivo a un controlador externo u otro acceso independiente a través del protocolo RS485. Eso no es compatible con Wiegand.
- Para el modo lector de tarjetas, los dos cables A/B (RS-485) se conectan a los cables A/B del controlador. Para realizar la función de alarma de manipulación, DOOR1_COM y DOOR1_NC deben conectarse a los cables CASE y GND del controlador externo.

- Configuración de la tasa de baudios
  - ◇ **9600**: Por defecto.
  - ◇ **115200**: Aplicable al controlador y al lector de tarjetas con esta velocidad en baudios.

  - Para el modo de lector de tarjetas, la velocidad en baudios se ajustará automáticamente de acuerdo con la controlador externo. Te recomendamos no modificar otras configuraciones en la web portal y en el dispositivo.
  - Para el modo de controlador, debe configurar manualmente la misma velocidad en baudios que el externo dispositivo.

2.10 Sistema

2.10.1 Hora

Configure la hora del dispositivo, como fecha, hora y formato de fecha.

Step 1 En el menú principal, seleccione**Sistema > Hora**y luego toque**OK**.

Step 2 Seleccione un parámetro y luego toque**OK**.

Figure 2-17 Ajustes de hora

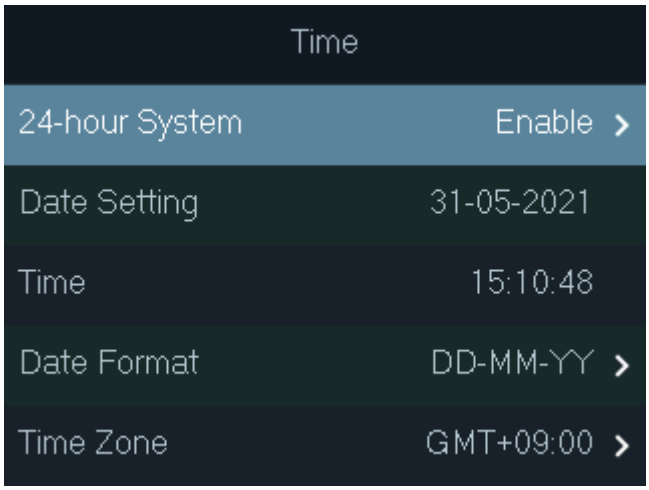


Tabla 2-6 Descripción de los parámetros de tiempo

Parámetro	Descripción
Sistema 24 horas	Habilite el formato de 24 horas.
Configuración de la fecha	Configura la fecha.
Hora	Configura el tiempo.
Formato de fecha	Seleccione un formato de fecha.
Zona horaria	Seleccione una zona horaria.

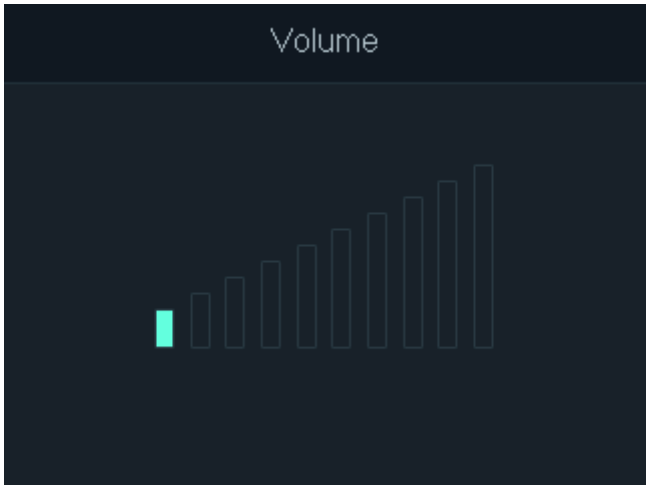
2.10.2 Volumen

Ajuste el volumen del mensaje de voz.

Step 1 En el menú principal, seleccione**Sistema > Volumen**y luego toque**OK**. Toque

Step 2 la flecha hacia arriba o hacia abajo para ajustar el volumen.

Figure 2-18 Ajusta el volumen



2.10.3 Restauración de la configuración predeterminada

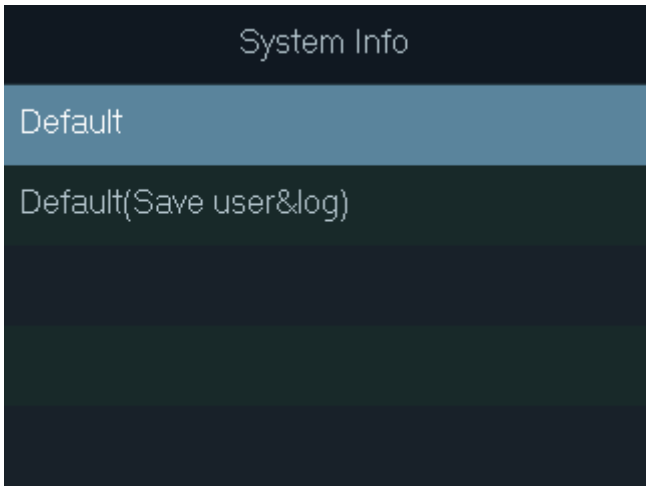
Los datos se perderán si restaura el dispositivo a los valores predeterminados de fábrica. Por favor tenga en cuenta.

Step 1 En el menú principal, seleccione**Sistema > Restaurar fábrica**y luego toque**OK**.

Step 2 Seleccione una opción y luego toque**OK**.

- **Por defecto**: restaura los valores predeterminados de fábrica y elimina todos los datos, incluidos los usuarios, la información del dispositivo y los registros.
- **Predeterminado (Guardar usuario y registro)**: restaura los valores predeterminados de fábrica y elimina todos los datos excepto la información del usuario y los registros.

Figure 2-19 Restaurar a la configuración predeterminada



2.10.4 Reinicio del dispositivo

En el menú principal, seleccione**Sistema > Reiniciar**y luego toque**OK**para reiniciar el dispositivo.

2.11 Gestión USB

- Asegúrese de que haya una unidad flash USB insertada en el dispositivo antes de exportar la información del usuario o sistema de actualización. Para evitar fallas, no extraiga la unidad flash USB ni realice ninguna operación durante el proceso.
- Si desea importar datos de un dispositivo a otro, debe exportar los datos a una memoria flash USB conducir primero.

Puede usar una unidad flash USB para actualizar el dispositivo y exportar o importar información del usuario.

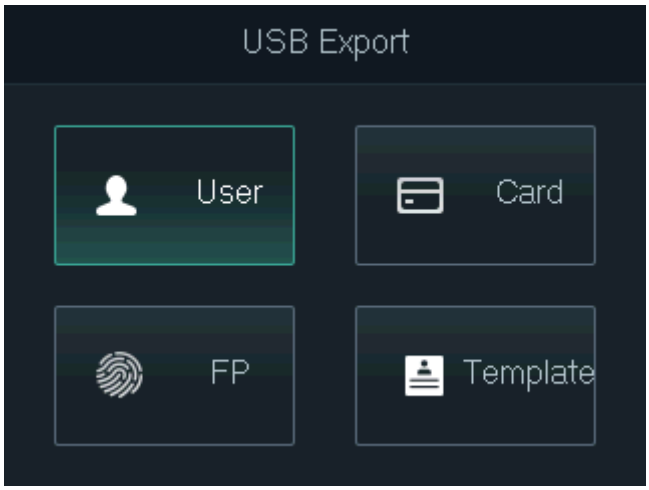
2.11.1 Exportando a USB

Exporte datos del dispositivo a una unidad flash USB. Los datos exportados están encriptados y no se pueden editar.

Step 1 En el menú principal, seleccione**USB > Exportación USB**y luego toque**OK**.

Step 2 Seleccione el tipo de datos que desea exportar y luego toque**OK**.

Figure 2-20 Exportar datos a la unidad USB



Step 3 Grifo**OK**.

Los datos seleccionados se exportan a la unidad flash USB.

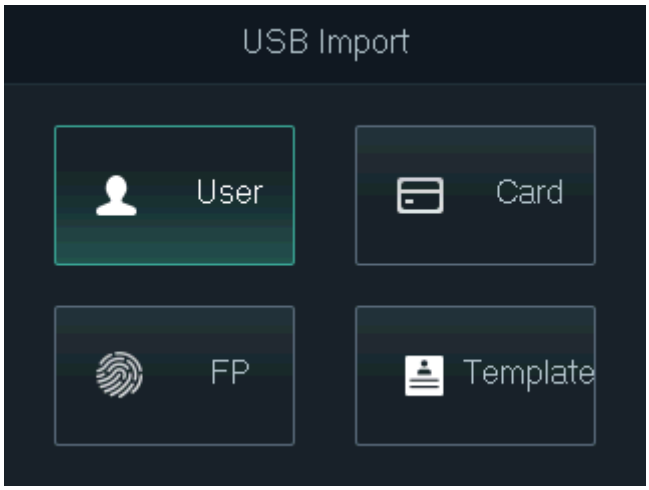
2.11.2 Importación desde USB

Puede importar datos desde USB al dispositivo.

Step 1 En el menú principal, seleccione**USB > Importación USB**y luego toque**OK**.

Step 2 Seleccione el tipo de datos que desea importar y luego toque**OK**.

Figure 2-21 Importar datos desde la unidad flash USB



Step 3 Grifo**OK**.

Los datos seleccionados se importan al dispositivo.

2.11.3 Sistema de actualización

Puede usar una unidad flash USB para actualizar el sistema del Dispositivo.

Step 1 Cambie el nombre del archivo de actualización a "update.bin", colóquelo en el directorio raíz de la unidad flash USB y luego inserte la unidad flash USB en el dispositivo.

Step 2 En el menú principal, seleccione**USB > Actualización USB**.

Step 3 Grifo**OK**.

El dispositivo se reiniciará cuando se complete la actualización.

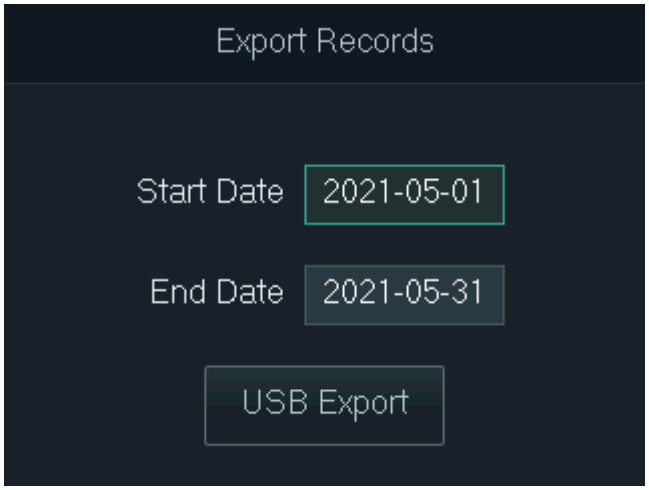
2.11.4 Exportación de registros de desbloqueo

Exporte registros de desbloqueo a una unidad flash USB.

Step 1 En el menú principal, seleccione**USB > Exportar registros**y luego toque**OK**.

Step 2 Selecciona la hora.

Figure 2-22 Exportar registros de desbloqueo



Step 3 Seleccione**Exportación USB**y luego toque**OK**.

Los registros de desbloqueo se exportan a la unidad flash USB.

2.11.5 Exportación/Importación de información de usuario

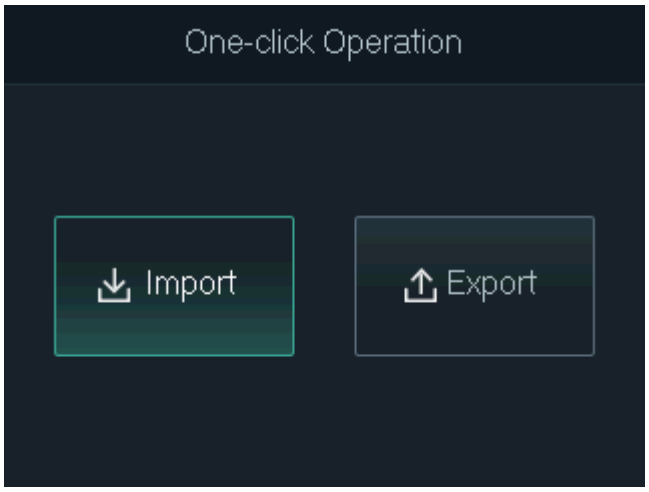
Puede utilizar la función de un clic para importar o exportar información de usuario, incluidas tarjetas y huellas dactilares.

Step 1 En el menú principal, seleccione**USB > Operación con un clic**y luego toque**OK**.

- **Importar**: importe la información del usuario, incluidas las tarjetas y las huellas dactilares.
- **Exportar**: exporte la información del usuario, incluidas las tarjetas y las huellas dactilares.

Step 2 Seleccione**Importar**o**Exportar**y luego toque**OK**.

Figure 2-23 Operación con un solo clic



2.12 Información del sistema

En el menú principal, seleccione**Información**y luego toque**OK**. Puede ver la capacidad de datos y la información del sistema del dispositivo.

- **Capacidad de datos**: muestra el número de usuarios generales, usuarios administradores, tarjetas, huellas dactilares, registros de desbloqueo y registros de alarma que se han almacenado, y la capacidad de almacenamiento.
- **Versión del dispositivo**: muestra información de software y hardware del dispositivo.

3 Configuración Web

Abra el navegador web en su computadora o teléfono. Inicie sesión en la página web para configurar y actualizar el dispositivo.

3.1 Web en computadora

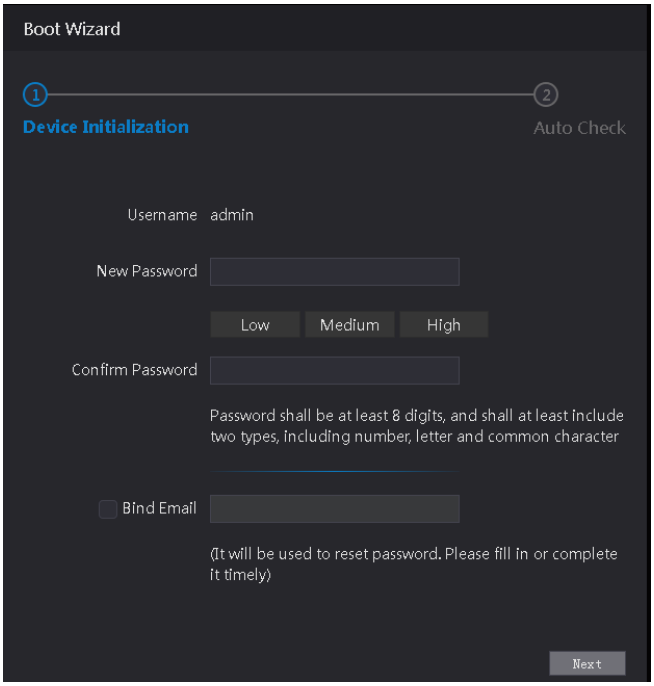
3.1.1 Inicialización

Debe establecer una contraseña y vincular una dirección de correo electrónico antes de iniciar sesión en la web por primera vez.

Step 1 Vaya a la dirección IP (192.168.1.108 por defecto) del Dispositivo en el navegador.

Asegúrese de que la computadora esté en la misma LAN que el dispositivo.

Figure 3-1 Inicialización

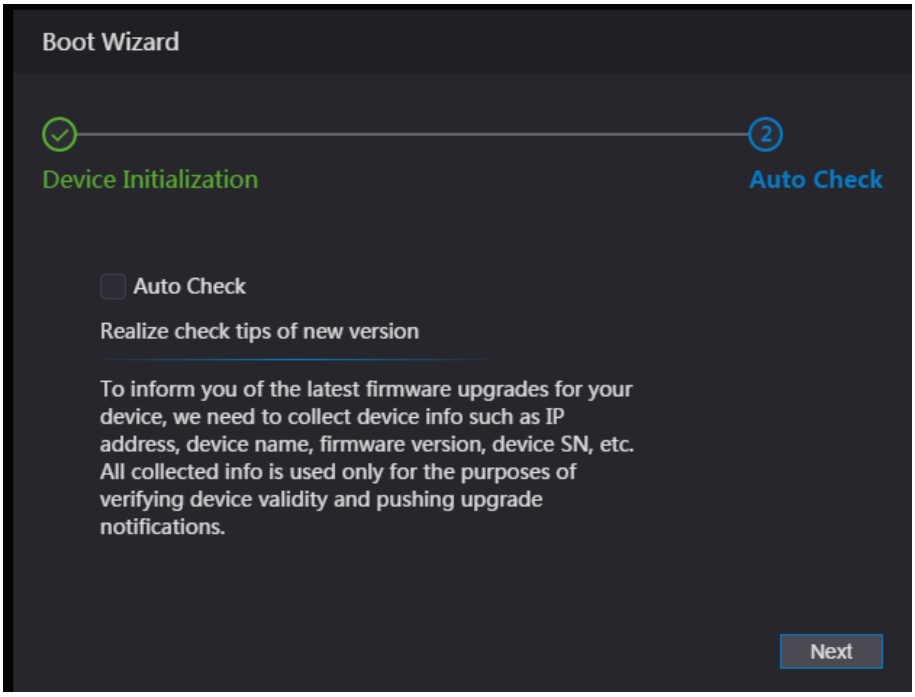


Step 2 Ingrese la nueva contraseña, confirme la contraseña, habilite**Vincular correo electrónico**, ingrese una dirección de correo electrónico y luego haga clic en**Próximo**.

- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: Mayúsculas, minúsculas, números y especiales caracteres (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo la contraseña indicador de fuerza.
- Mantenga la contraseña correctamente después de la inicialización y cámbiela regularmente para mejorar la seguridad
- Cuando necesite restablecer la contraseña de administrador escaneando el código QR, necesita la dirección de correo electrónico asociada para recibir el código de seguridad.

Step 3 Hacer clic**Próximo**.

Figure 3-2 Verificación automática

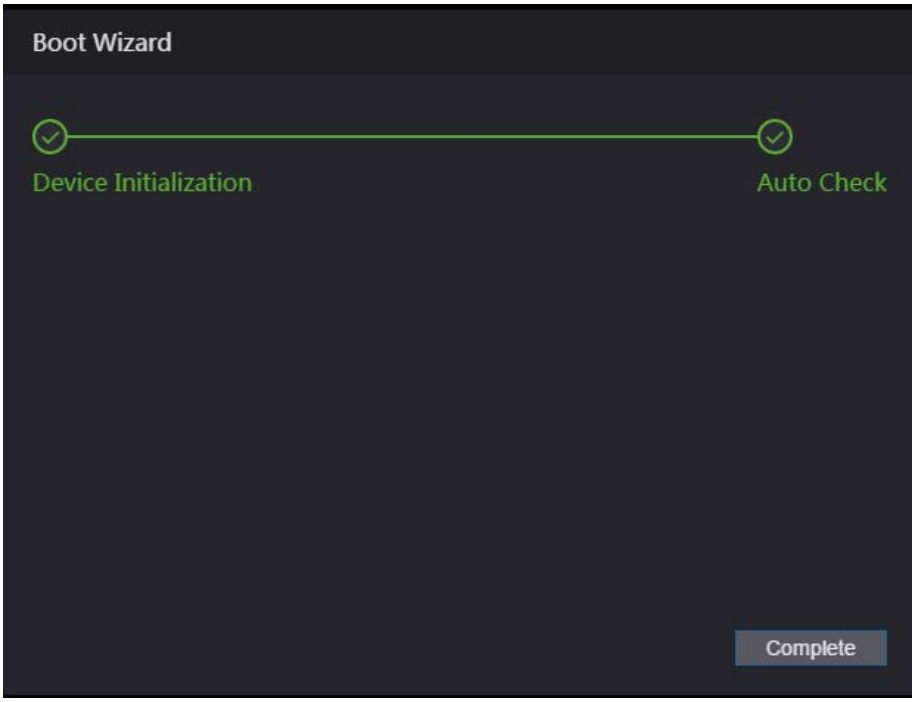


Step 4 (Opcional) Seleccionar**Verificación automática**.

Le recomendamos que seleccione**Verificación automática**para obtener la última versión a tiempo.

Step 5 Hacer clic**Próximo**.

Figure 3-3 Configuración finalizada



Step 6 Hacer clic**Completo**.

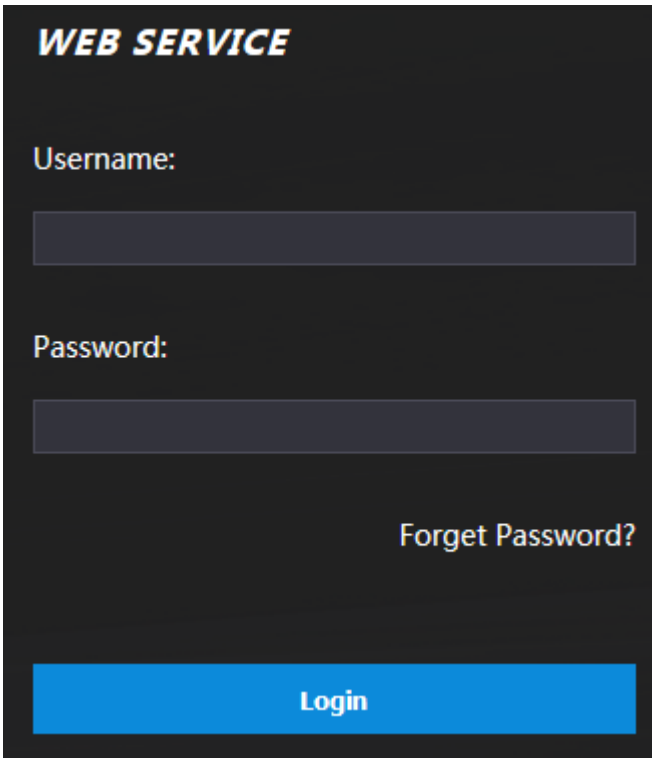
3.1.2 Iniciar sesión

Step 1 Vaya a la dirección IP (192.168.1.108 por defecto) del Dispositivo en el navegador, y presione el

Introducir clave.

- Asegúrese de que la computadora esté en la misma LAN que el dispositivo .
- La dirección IP predeterminada es 192.168.1.108.

Figure 3-4 Acceso



Step 2 Introduzca el nombre de usuario y la contraseña.

- El nombre de administrador predeterminado es admin, y la contraseña es la que estableció durante inicialización Le recomendamos que cambie la contraseña de administrador regularmente para aumentar la seguridad.
- Si olvidó la contraseña de administrador, haga clic en**¿Contraseña olvidada?**para restablecerlo. Ver "3.3 Restablecimiento de la contraseña ".

Step 3 Hacer clic**Acceso**.

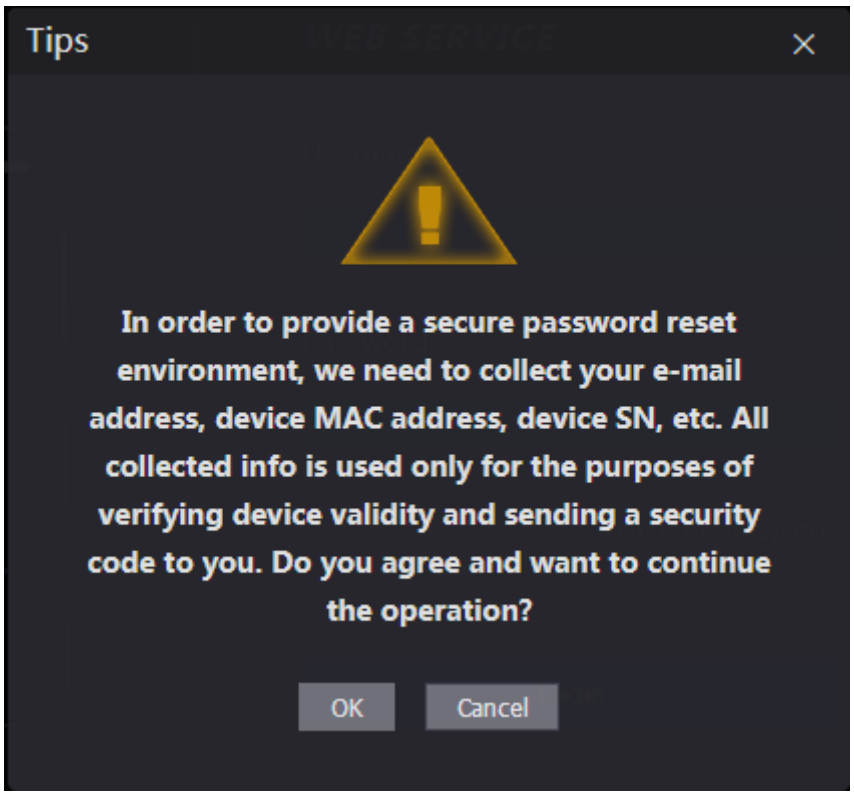
3.1.3 Restablecimiento de la contraseña

Al restablecer la contraseña de la cuenta de administrador, se requiere su dirección de correo electrónico.

Step 1 En la página de inicio de sesión, haga clic en**Has olvidado tu**

Step 2 **contraseña**. Lea atentamente el mensaje y haga clic en**OK**.

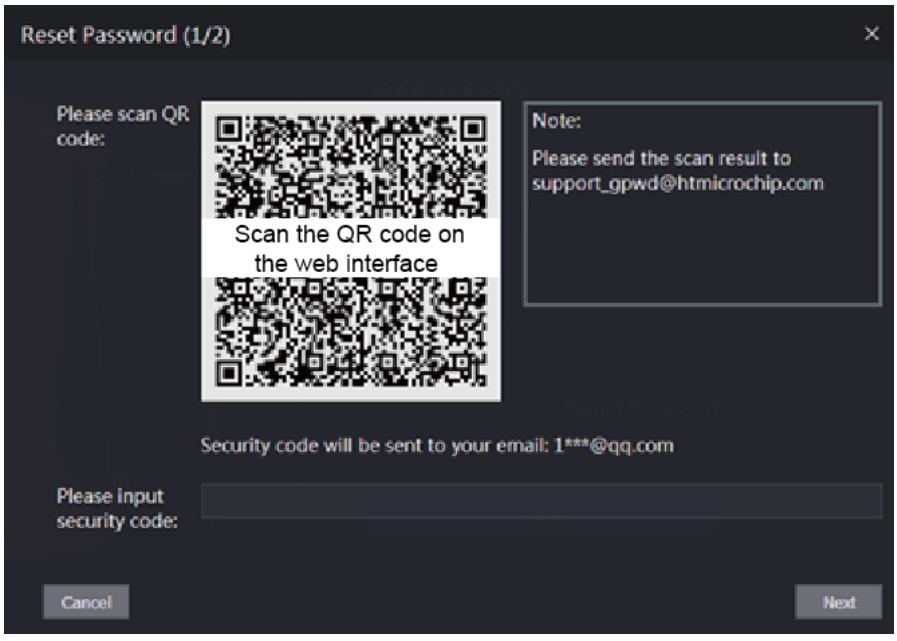
Figure 3-5 Aviso de reinicio



Step 3 Escanee el código QR en la ventana y obtendrá el código de seguridad.

- Se generarán un máximo de dos códigos de seguridad escaneando el mismo código QR. Si los códigos de seguridad dejan de ser válidos, actualice el código QR y vuelva a escanear.
- Después de escanear el código QR, envíe el contenido que recibió a la persona designada dirección de correo electrónico, y luego recibirá un código de seguridad.
- Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, se convertirá inválido. Si se ingresan códigos de seguridad incorrectos cinco veces consecutivas, el administrador se congelará durante cinco minutos.

Figure 3-6 Restablecer la contraseña



Step 4 Introduzca el código de seguridad que ha recibido. Hacer

Step 5 clic**Próximo**.

Step 6 Restablece y confirma la nueva contraseña.

La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo el indicador de seguridad de la contraseña.

Step 7 Hacer clic**OK**para completar el restablecimiento.

3.1.4 Configuración de parámetros de puerta

Configure los parámetros de control de acceso.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Parámetro de la puerta**.

Figure 3-7 Figura 3-9 Parámetro de puerta

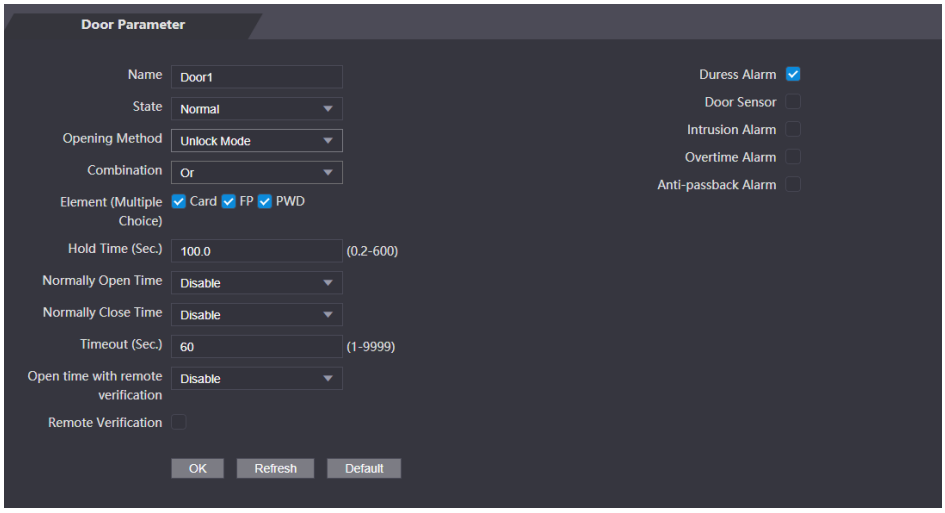


Tabla 3-1 Descripción de los parámetros de la puerta

Parámetro	Descripción
Nombre	Introduzca un nombre para la puerta que controla el dispositivo.
Estado	Seleccione**CAROLINA DEL NORTE**para normalmente cerrado, o**NO**para normalmente abierto. Si se selecciona cualquiera, el método de apertura definido no será efectivo.
Apertura Método	● **Sección de tiempo:**Establezca un método de desbloqueo diferente para períodos definidos. **multitarjeta**: ● El usuario puede desbloquear la puerta cuando múltiples usuarios y múltiples grupos de usuarios otorgan acceso. ● **Modo de desbloqueo**: establecer combinaciones de desbloqueo.
Tiempo de espera (seg.)	Duración del desbloqueo. La puerta se bloqueará nuevamente después de la duración. Va de 0,2 a 600 segundos.
Normalmente abierto Hora	La puerta permanece abierta o cerrada durante el tiempo definido.
normalmente cerrado Hora	

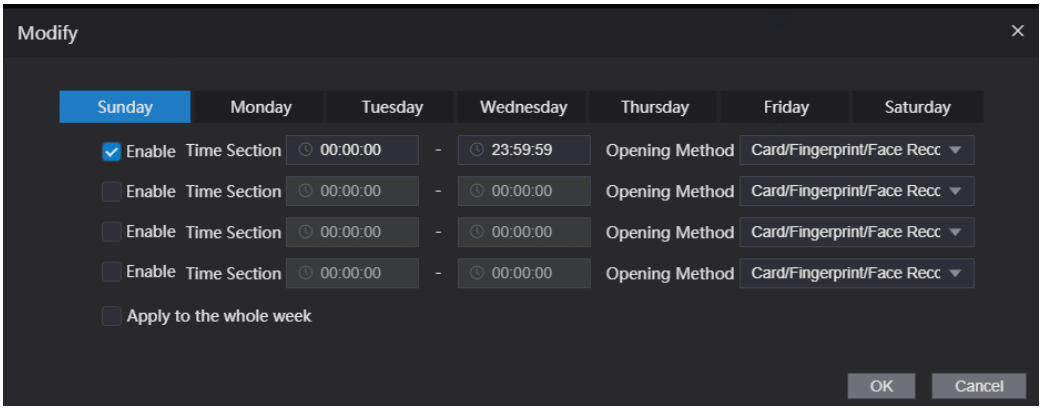
Parámetro	Descripción
Tiempo de espera (seg.)	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante más tiempo que este valor.
Remoto Verificación	Configure el período de apertura de la puerta de verificación remota. Para obtener más información, consulte "3.6.1 Configuración de la sección Hora". Cuando se autoriza la apertura de una puerta en el dispositivo, debe confirmarse en la plataforma antes de que se pueda abrir.
alarma de coacción	Se activará una alarma cuando se use una tarjeta de coacción o una contraseña de coacción para desbloquear la puerta.
sensor de puerta	Las alarmas de intrusión y horas extras pueden activarse solo después de**sensor de puerta**está habilitado.
Alarma de intrusión	Cuándo**sensor de puerta**está habilitado, se activará una alarma de intrusión si la puerta se abre de manera anormal.
Alarma de horas extras	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante más tiempo que el**Tiempo de espera (seg)**, que va de 1 a 9999 segundos.
Anti-passback Alarma	Si está habilitado, los usuarios deben verificar las identidades tanto para la entrada como para la salida; de lo contrario, se activará una alarma. ● Si una persona ingresa con verificación y sale sin verificación, se activará una alarma cuando intente desbloquear nuevamente y se negará el acceso al mismo tiempo. ● Si una persona ingresa sin verificación y sale con verificación, se activará una alarma cuando intente desbloquear nuevamente y se negará el acceso al mismo tiempo.

Step 3 Configure el método de desbloqueo.

- Sección de tiempo

1) En el**Método de apertura**lista, seleccione**Sección de tiempo**y luego haga clic en .

Figure 3-8 Parámetro de sección de tiempo



2) Configurar la hora y el método de apertura de un tramo horario. Puede configurar hasta cuatro tramos de tiempo para un solo día.

3) (Opcional) Seleccionar**Aplica para toda la semana**para copiar la configuración al resto de días.

4) Haga clic**OK**.

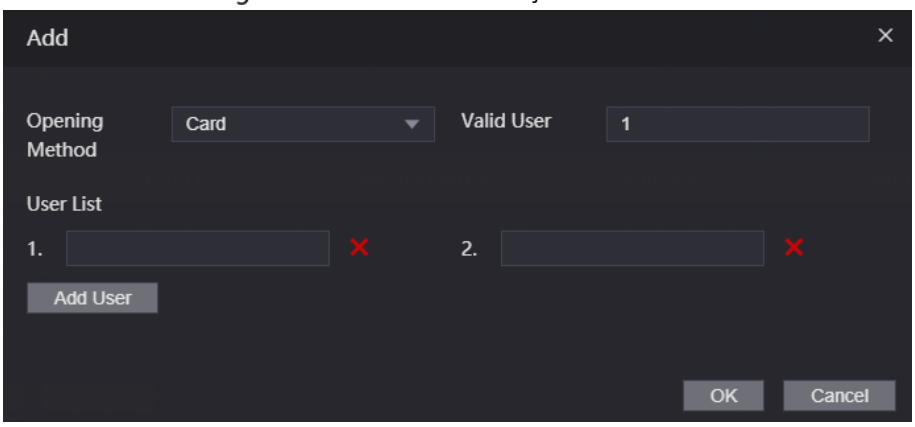
- multitarjeta

1) En el**Método de apertura**lista, seleccione**multitarjeta**y luego haga clic en .

2) Haga clic**Agregar**.

3) Seleccione un método de desbloqueo en el**Método de apertura**list., e ingrese un número para el usuario válido.

Figure 3-9 Parámetro multitarjeta



4) En el**Lista de usuarios**área, ingrese la ID de usuario. Para obtener más información, consulte "2.7.1 Agregar nuevo usuario".

- No se pueden agregar usuarios VIP, patrulla y lista de bloqueo.
- Todos los usuarios en diferentes grupos deben verificar sus identidades en el grupo para poder quitale el seguro a la puerta.

- Modo de desbloqueo

1) En el**Método de apertura**lista, seleccione**Modo de desbloqueo**.

2) En el**Combinación**lista, seleccione**O**o**Y**.

- **Y**significa que debe utilizar todos los métodos seleccionados para abrir la puerta. **O**
- significa que puede abrir la puerta con cualquiera de los métodos seleccionados.

3) En el**Elemento**lista, seleccione el método de desbloqueo.

Step 4 Configurar otros parámetros.

Step 5 Hacer clic**OK**.

3.1.5 Enlace de alarma

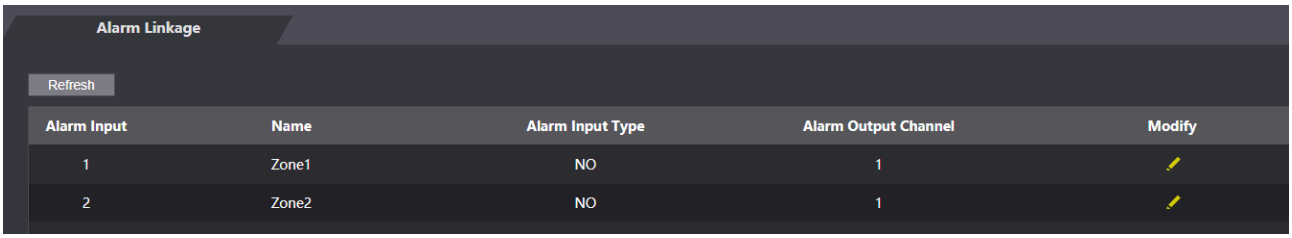
3.1.5.1 Configuración de enlace de alarma

Los dispositivos de entrada de alarma se pueden conectar al dispositivo y se pueden modificar los parámetros de enlace de alarma.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Enlace de alarma**>**Enlace de alarma**.

Figure 3-10 Enlace de alarma



Step 3 Hacer clic para configurar el enlace de alarma.

Figure 3-11 Modificar parámetros de vinculación

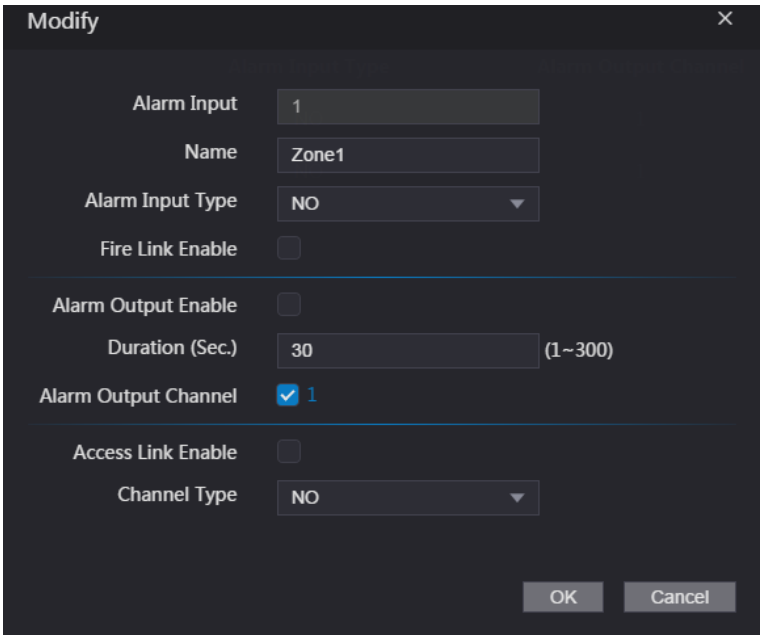


Tabla 3-2 Descripción de los parámetros de vinculación de alarmas

Parámetro	Descripción
Entrada de alarma	No puede modificar el valor. Manténgalo predeterminado.
Nombre	Introduzca un nombre de zona.
Tipo de entrada de alarma	Seleccione el tipo según el dispositivo de alarma. ● **NO**: El circuito del dispositivo de alarma normalmente está abierto y se cierra cuando se activa una alarma. ● **CAROLINA DEL NORTE**: El circuito del dispositivo de alarma normalmente está cerrado y se abre cuando se activa una alarma.
Habilitar enlace de fuego	Si el enlace de incendio está habilitado, el dispositivo generará alarmas de incendio cuando se active. Los mensajes de alarma se muestran en el registro de alarmas. Si el enlace de incendio está habilitado, la salida de alarma y el enlace de acceso son NO por defecto.
Habilitar salida de alarma	Si la salida de alarma está habilitada, el relé puede generar mensajes de alarma.
Duración (seg.)	Duración de la alarma. Va desde 1 s hasta 300 s.
Canal de salida de alarma	El dispositivo tiene un solo canal de salida. Seleccione el canal de salida de acuerdo con su dispositivo de alarma.
Habilitar enlace de acceso	Si el enlace de acceso está habilitado, el dispositivo estará normalmente encendido o normalmente cerrado cuando haya señales de alarma de entrada.
Tipo de canal	Hay dos opciones: NO y NC.

Step 4 Hacer clic**OK**para guardar los cambios.

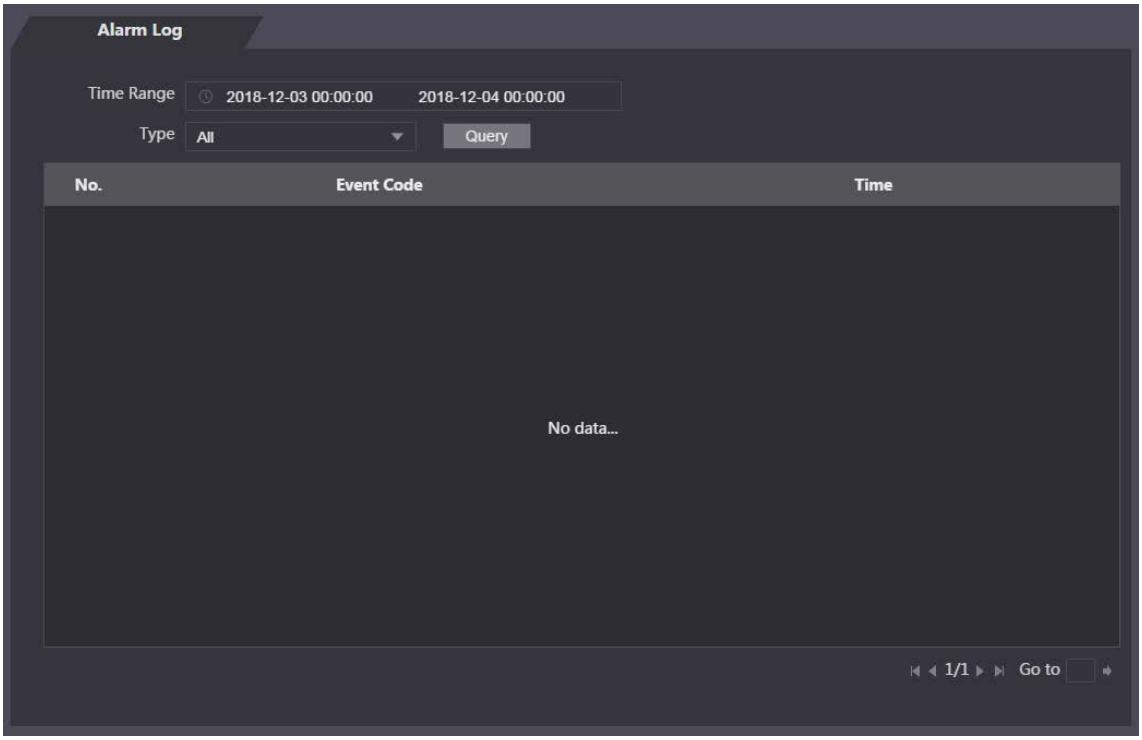
Las configuraciones en la web se sincronizarán con el cliente de software si el dispositivo está añadido al cliente.

3.1.5.2 Registro de alarmas

Step 1 Inicie sesión en la página web.

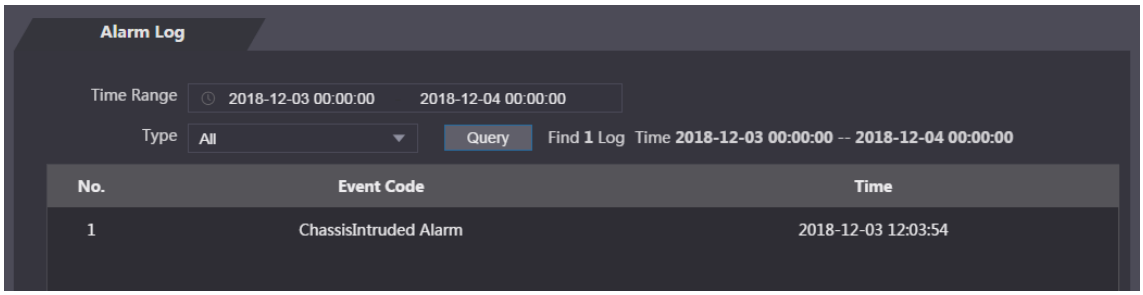
Step 2 Seleccione**Enlace de alarma**>**Registro de alarmas**.

Figure 3-12 Registro de alarmas



Step 3 Seleccione un intervalo de tiempo y un tipo de alarma y, a continuación, haga clic en**Consulta**.

Figure 3-13 Resultados de la consulta



3.1.6 Sección de tiempo

Configure secciones de tiempo y planes de vacaciones, y luego puede definir cuándo un usuario tiene los permisos para desbloquear puertas.

3.1.6.1 Configuración de la sección de tiempo

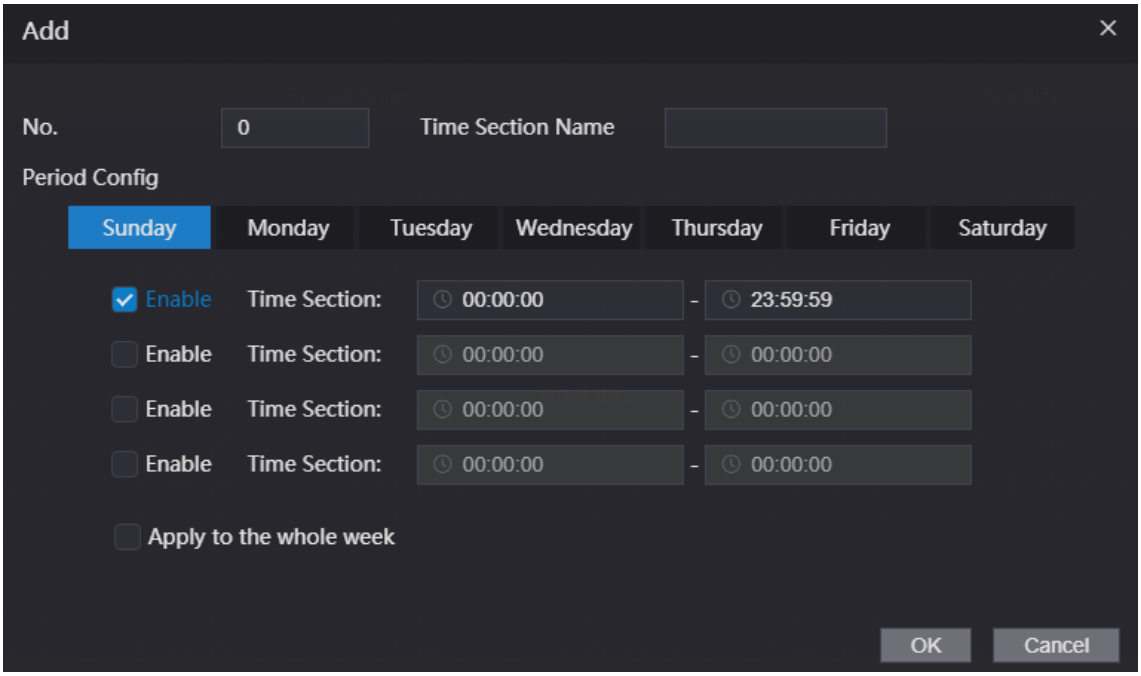
Puede configurar hasta 128 grupos (del No.0 al No.127) de la sección de tiempo. En cada grupo, debe configurar horarios de acceso a la puerta para una semana completa. Un usuario solo puede desbloquear la puerta durante el tiempo programado.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Sección de tiempo**>**Sección de tiempo**. Hacer

Step 3 clic**Agregar**.

Figure 3-14 Parámetros de la sección de tiempo



Step 4 Ingrese el número y el nombre de la sección de tiempo.

- **No.**: Introduzca un número de sección Va del 0 al 127.
- **Nombre de la sección de tiempo**: Ingrese un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (que contengan números, caracteres especiales y caracteres ingleses).

Step 5 Configure las secciones de tiempo para cada día.

Puede configurar hasta cuatro tramos de tiempo para un solo día.

Step 6 (Opcional) Haga clic en**Aplica para toda la semana**para copiar la configuración al resto de días. Hacer clic

Step 7 **OK**para guardar los cambios.

3.1.6.2 Configuración del grupo de vacaciones

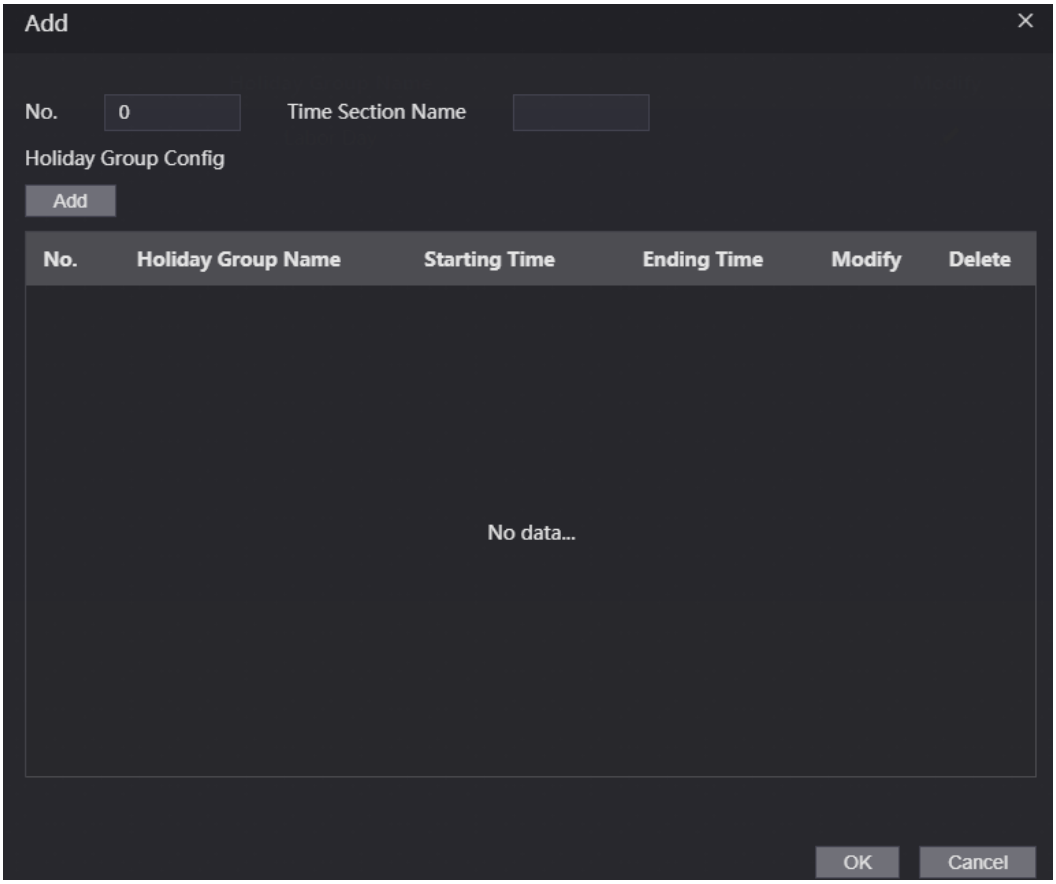
Establecer secciones de tiempo para diferentes grupos de vacaciones. Puede configurar hasta 128 grupos de días festivos (del No.0 al No.127). y hasta 16 tramos horarios para un mismo grupo vacacional. Los usuarios pueden desbloquear puertas en las secciones de tiempo definidas.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Sección de tiempo**>**Configuración de grupo de vacaciones**. Hacer

Step 3 clic**Agregar**.

Figure 3-15 Agregar un grupo de vacaciones



Step 4 Introduzca un número y un nombre para el grupo de vacaciones.

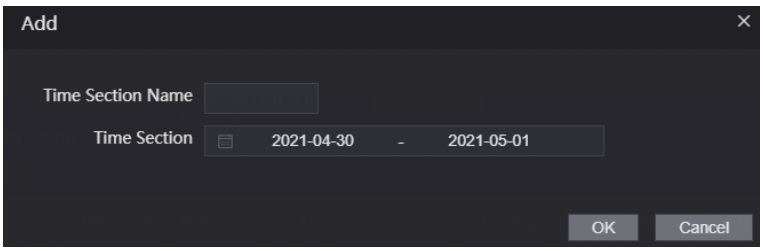
- **No.**: Introduzca un número de sección. Va de 0 a 127.
- **Nombre de la sección de tiempo**: Ingrese un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (que contengan números, caracteres especiales y caracteres ingleses).

Step 5 Hacer clic**Agregar**.

Step 6 Introduzca un nombre en el**Nombre de la sección de tiempo**seleccione la fecha de inicio y la fecha de finalización y, a continuación, haga clic en**OK**.

Puede agregar varios días festivos para un grupo de días festivos.

Figure 3-16 Añadir un día festivo



Step 7 Hacer clic**OK**.

3.1.6.3 Configuración del plan de vacaciones

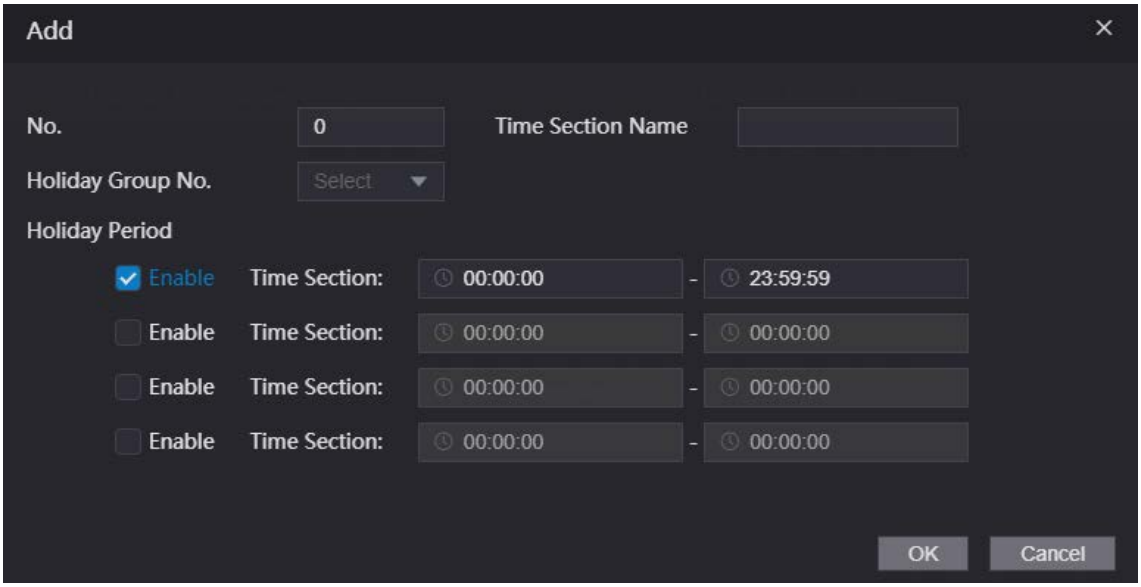
Asigne los grupos de vacaciones configurados al plan de vacaciones. Los usuarios solo pueden desbloquear la puerta en el tiempo definido en el plan de vacaciones.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Sección de tiempo**>**Configuración del plan de vacaciones**.

Step 3 Hacer clic**Agregar**.

Figure 3-17 Añadir un plan de vacaciones



Step 4 Introduzca un número y un nombre para el plan de vacaciones.

- **No.**: Introduzca un número de sección. Va de 0 a 127.
- **Nombre de la sección de tiempo**: Ingrese un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (que contengan números, caracteres especiales y caracteres ingleses).

Step 5 En el**Grupo de vacaciones No.**lista, seleccione el grupo de vacaciones que ha configurado.

Seleccione**255**si no desea seleccionar un grupo de vacaciones.

Step 6 En el**Periodo de festivos**área, configure las secciones de tiempo en el grupo de vacaciones. Puede configurar hasta cuatro tramos de tiempo.

Step 7 Hacer clic**OK**.

3.1.7 Capacidad de datos

Vea la capacidad de datos como usuarios, tarjetas y huellas dactilares que el dispositivo puede almacenar.

Step 1 Inicie sesión en la página web.

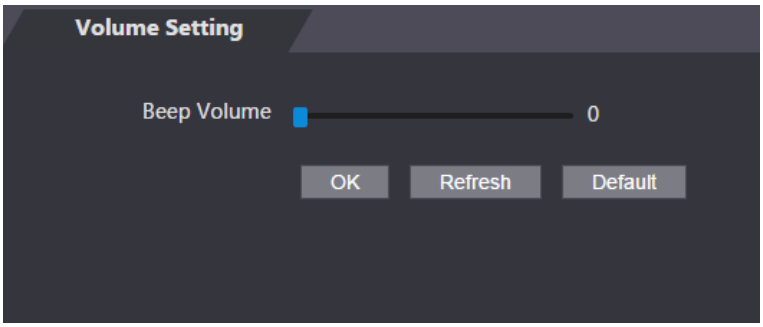
Step 2 Seleccione**Capacidad de datos**en la barra de navegación.

3.1.8 Configuración del volumen

Step 1 Inicie sesión en la página web.

Step 2 Hacer clic**Configuración de volumen**y ajuste el volumen.

Figure 3-18 Ajuste de volumen



Step 3 Hacer clic**OK**.

3.1.9 Configuración de red

3.1.9.1 Configuración de TCP/IP

Debe configurar la dirección IP y el servidor DNS para que el dispositivo pueda comunicarse con otros dispositivos.

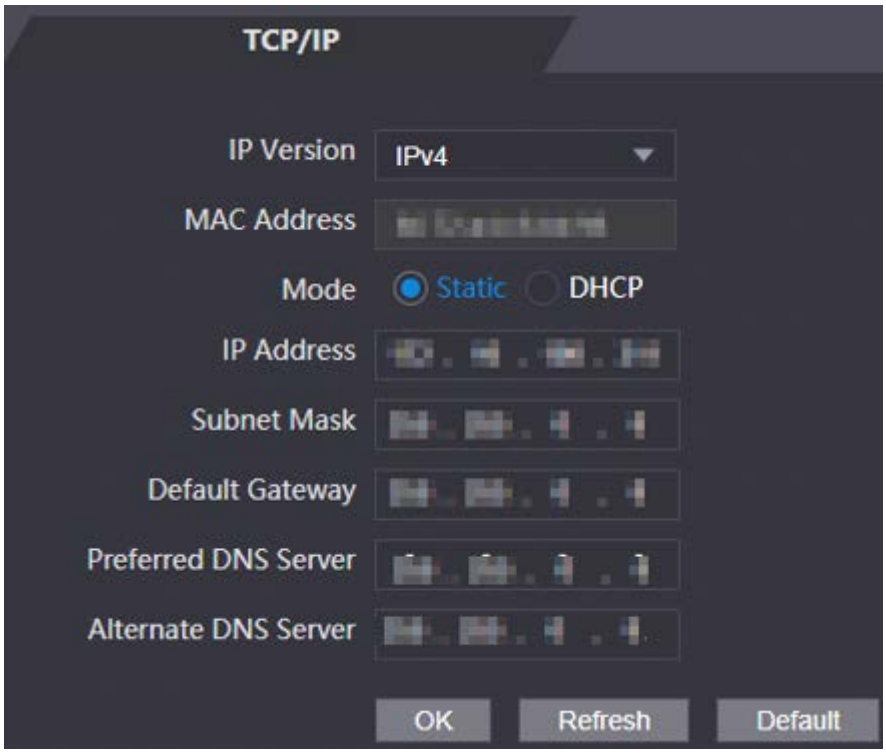
Requisito previo

Asegúrese de que el dispositivo esté conectado a la red.

Step 1 Inicie sesión en la página web. Seleccione

Step 2 **Configuración de red**>**TCP/IP**.

Figure 3-19 TCP/IP



Step 3 Configurar parámetros.

Tabla 3-3 Descripción de TCP/IP

Parámetro	Descripción
Versión IP	IPv4.
Dirección MAC	Dirección MAC del Dispositivo.
Modo	● **Estático**: establezca la dirección IP, la máscara de subred y la dirección de la puerta de enlace manualmente. ● **DHCP** - Después de habilitar DHCP, la dirección IP, la máscara de subred y la dirección de la puerta de enlace no se pueden configurar. - Si DHCP es efectivo, DHCP asignará automáticamente la dirección IP, la máscara de subred y la dirección de la puerta de enlace. - Si deshabilita DHCP, se mostrará la IP predeterminada.
Dirección IP Máscara de subred Puerta de enlace predeterminada	Ingrese la dirección IP y luego configure la máscara de subred y la dirección de la puerta de enlace. La dirección IP y la dirección de la puerta de enlace deben estar en el mismo segmento de red.
Privilegiado/ DNS alternativo Servidor	Configure la dirección IP del servidor DNS preferido.

Step 4 Hacer clic**OK**para completar el ajuste.

3.1.9.2 Configuración del puerto

Puede limitar el acceso al Dispositivo al mismo tiempo por web, software y teléfono, y configurar los números de puerto del Dispositivo.

Step 1 Inicie sesión en la página web. Seleccione

Step 2 **Configuración de red**>**Puerto**. Configure

Step 3 el número de puerto.

Excepto**Conexión máxima**, debe reiniciar el Dispositivo para que sus configuraciones sean efectivas.

Tabla 3-4 Descripción de los puertos

Parámetro	Descripción
máx. Conexión	Establezca el acceso máximo al dispositivo a través de clientes, como web, software y teléfono. Los clientes de la plataforma como SmartPSS AC no se cuentan.
Puerto TCP	El valor predeterminado es 37777.
Puerto HTTP	El valor predeterminado es 80. Si desea cambiar el número de puerto, agregue el número de puerto modificado después de la dirección cuando inicie sesión a través de un navegador web.
Puerto HTTPS	El valor predeterminado es 443.
Puerto RTSP	El valor predeterminado es 554.

Step 4 Hacer clic**OK**para completar el ajuste.

3.1.9.3 Registro

El Dispositivo informa su dirección al servidor designado para que los clientes puedan acceder.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Configuración de red**>**Registro automático**.

Step 3 Seleccione**Habilitar**e ingrese la IP del host, el puerto y la ID del subdispositivo.

Tabla 3-5 Descripción del registro automático

Parámetro	Descripción
IP del anfitrión	Dirección IP del servidor o nombre de dominio del servidor.
Puerto	Puerto del servidor utilizado para el registro automático.
ID de dispositivo secundario	ID del controlador de acceso asignado por el servidor.

Step 4 Hacer clic**OK**para completar el ajuste.

3.1.9.4 P2P

La computación o redes punto a punto es una arquitectura de aplicación distribuida que divide tareas o cargas de trabajo entre pares. Los usuarios pueden descargar la aplicación móvil escaneando el código QR y luego registrar una cuenta. Puede administrar varios dispositivos en la aplicación móvil. No se requiere el nombre de dominio dinámico, la asignación de puertos ni el servidor de tránsito.

Si desea utilizar P2P, debe conectar el Dispositivo a Internet; de lo contrario, esta función no puede trabaja correctamente.

Figure 3-20 P2P

Step 1 Inicie sesión en la página web. Seleccione

Step 2 **Configuración de red**>**P2P**. Seleccione**Habilitar**para

Step 3 habilitar la función P2P. Hacer clic**OK**.

Step 4

Escanee el código QR en su página web para obtener el número de serie del Dispositivo.

3.1.10 Configuración de la fecha

Puede configurar la zona horaria, la hora del sistema, DST (Horario de verano) o NTP (Protocolo de tiempo de red).

Step 1 Inicie sesión en la página web. Hacer

Step 2 clic**Configuración de la fecha**.

Figure 3-21 Ajuste de fecha

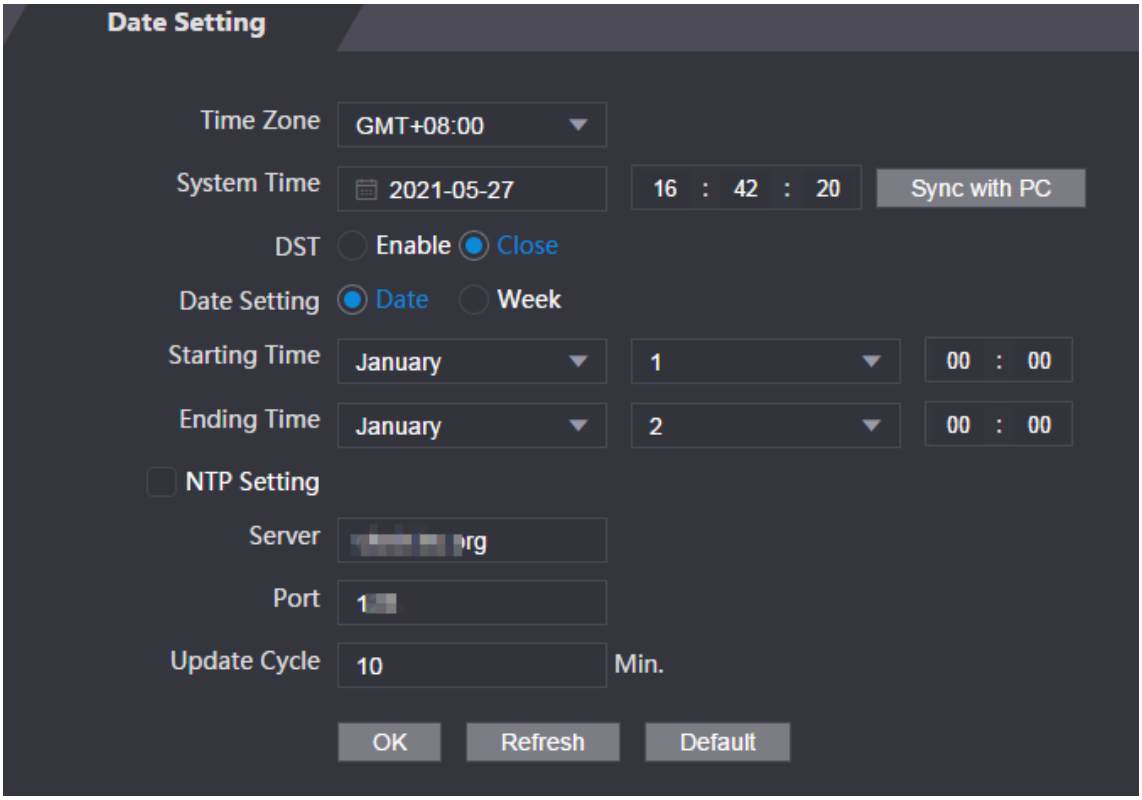


Tabla 3-6 Descripción de configuración de datos

Parámetro	Descripción
Zona horaria	Configura la zona horaria.
Hora del sistema	Configurar la hora del sistema. Hacer clic**Sincronizar con PC**y la hora del sistema cambia a la hora de la PC.
horario de verano	1. (Opcional) Habilite DST. 2. Selecciona**Fecha**o**Semana**en**Configuración de estado**. 3. Configure la hora de inicio y la hora de finalización.
Configuración NTP	1. Seleccione el**Configuración NTP**caja. 2. Configurar parámetros. ● **Servidor**: Introduzca el dominio de un servidor NTP y el dispositivo sincronizará automáticamente la hora con el servidor NTP. ● **Puerto**: Introduzca el puerto del servidor NTP. **Ciclo de actualización**: ● Ingrese el intervalo de sincronización de tiempo.

Step 3 Hacer clic**OK**.

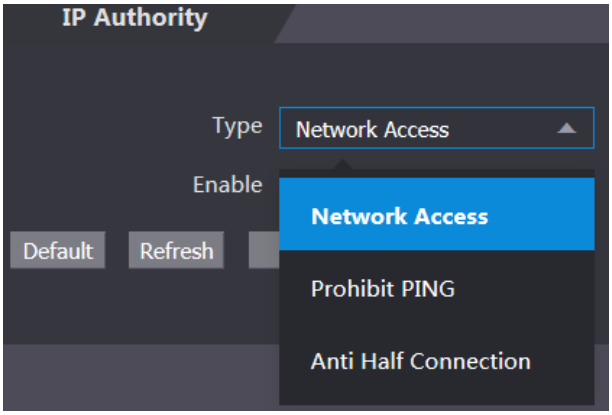
3.1.11 Gestión de la seguridad

3.1.11.1 Configuración de autoridad IP

Step 1 Inicie sesión en la página web.

Step 2 Hacer clic**Gestión de seguridad**>**Autoridad de PI**.

Figure 3-22 autoridad de PI



Step 3 Seleccione un modo de ciberseguridad en el**Escribe**lista.

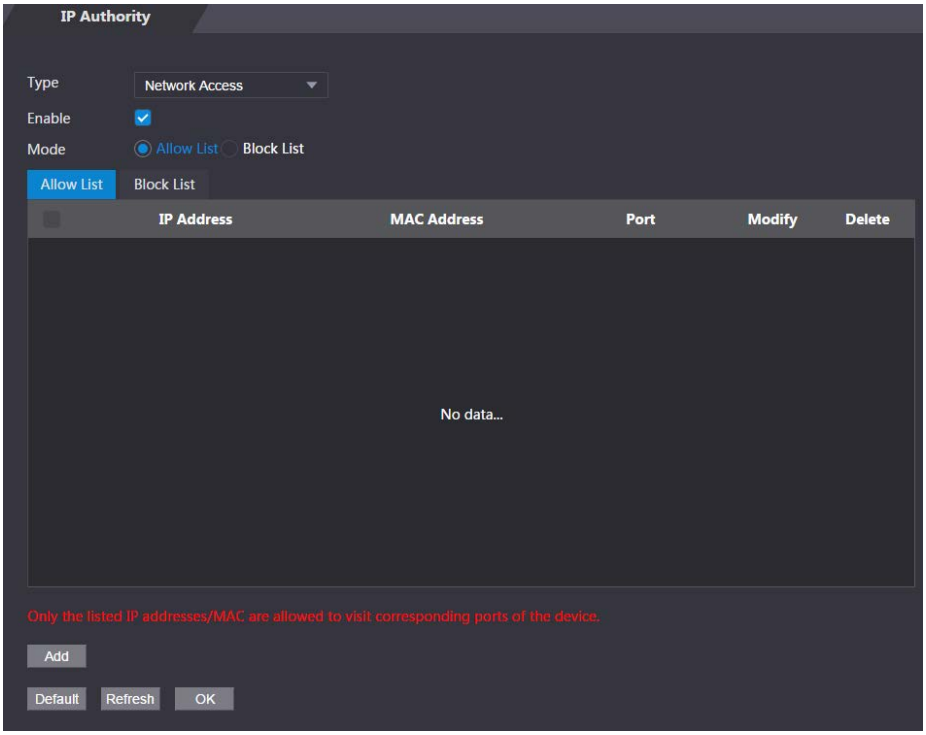
- **Acceso a la red**: Configure la lista de permitidos y la lista de bloqueados para controlar el acceso al dispositivo.
  - **Lista de permitidos**: una lista de direcciones IP/MAC de confianza que tienen acceso al dispositivo. **Lista**
  - **de bloqueos**: una lista de direcciones IP/MAC bloqueadas que no tienen acceso al dispositivo.
- **Prohibir PING**: Habilitar**PING prohibido**y el dispositivo no responderá a la solicitud de ping.
- **Media conexión anti**: Habilitar**Media conexión anti**función, y el dispositivo aún puede funcionar correctamente bajo el ataque de la mitad de la conexión.

3.1.11.1.2 Acceso a la red

Seleccione**Acceso a la red**en el**Escribe**lista.

Step 1 Selecciona el**Habilitar**caja.

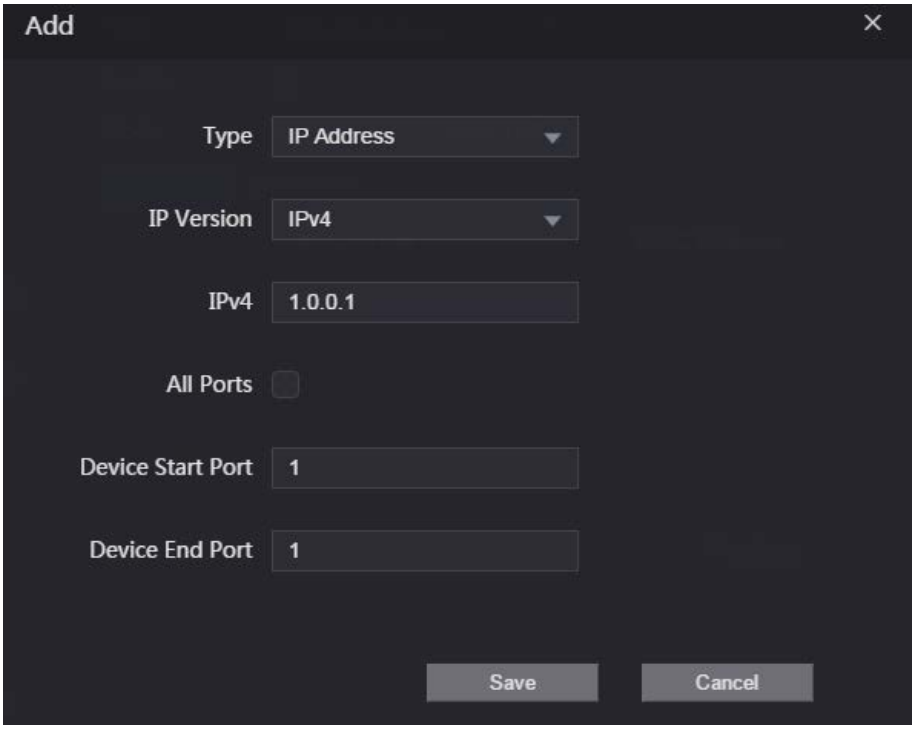
Figure 3-23 Acceso a la red



Step 2 Seleccione**Lista de permitidos**o**Lista de bloqueos**.

Step 3 Hacer clic**Agregar**.

Figure 3-24 Agregar IP



Step 4 Configurar parámetros.

Tabla 3-7 Descripción de la adición de parámetros IP

Parámetro	Descripción
Escribe	Seleccione el tipo de dirección en el**Escribe**lista.
Versión IP	IPv4 por defecto.
Todos los puertos	Seleccione**Todos los puertos**casilla de verificación y su configuración se aplicará a todos los puertos.

Parámetro	Descripción
Puerto de inicio del dispositivo	si borras**Todos los puertos**casilla de verificación, establezca el puerto de inicio del dispositivo y el puerto final del dispositivo.
Puerto final del dispositivo	

Step 5 Hacer clic**Salvar**, y el**Autoridad de PI**se muestra la ventana. Hacer

Step 6 clic**OK**.

Operaciones relacionadas

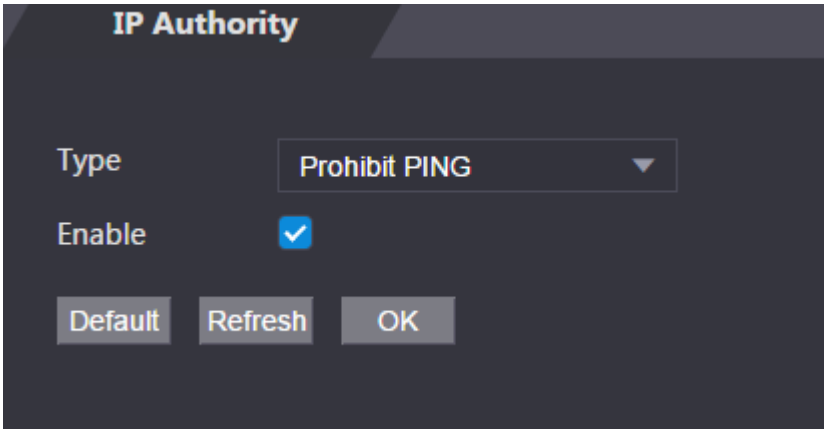
- Hacer clic  para editar la lista de permitidos o la lista de bloqueados.
- Hacer clic  para eliminar la lista de permitidos o la lista de bloqueados

3.1.11.1.3 Prohibir PING

Step 1 Seleccione**Prohibir PING**en el**Escribe**

Step 2 lista. Selecciona el**Habilitar**caja.

Figure 3-25 Prohibir PING



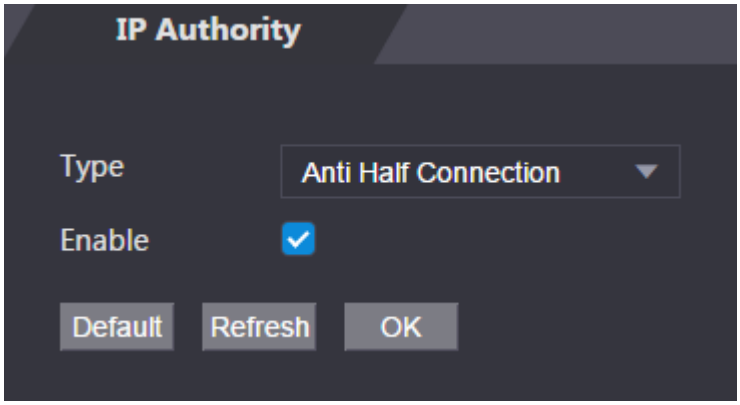
Step 3 Hacer clic**OK**.

3.1.11.1.4 Conexión Anti Half

Step 1 Selecciona el**Media conexión anti**en el**Escribe**lista.

Step 2 Selecciona el**Habilitar**caja.

Figure 3-26 Acceso a la red



Step 3 Hacer clic**OK**.

3.1.11.2 Configuración del sistema

3.1.11.2.1 Servicio del sistema

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Gestión de seguridad**>**Servicio del**

Step 3 **sistema**. Activa o desactiva los servicios del sistema.

Figure 3-27 servicio del sistema

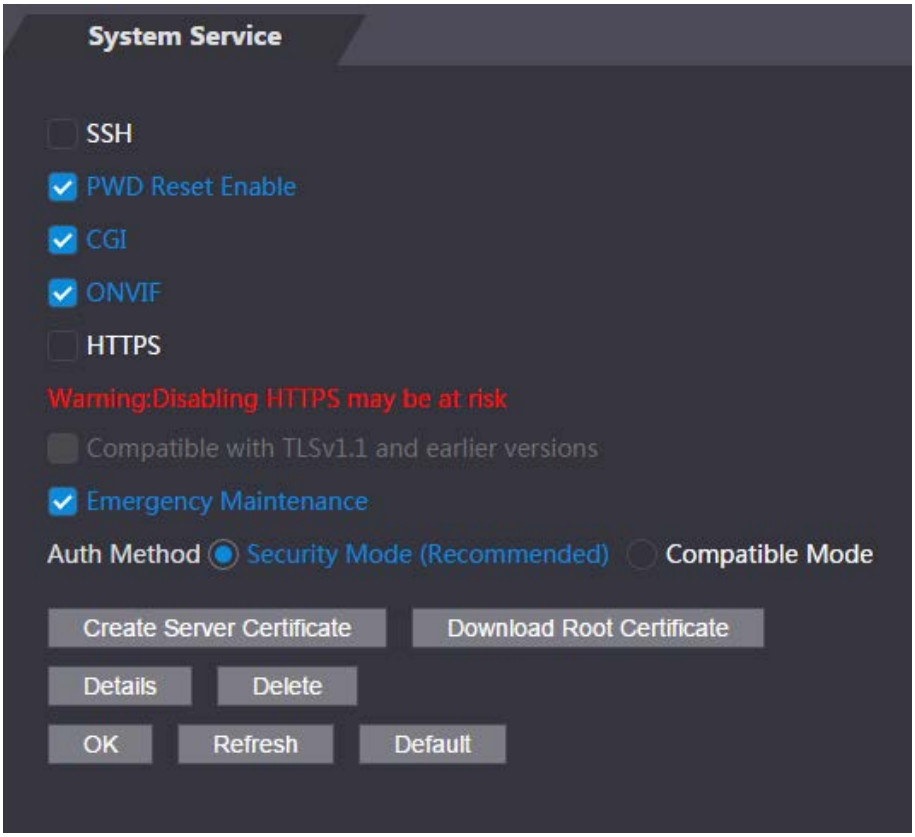


Tabla 3-8 Descripción del servicio del sistema

Parámetro	Descripción
SSH	Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura en una red no segura. Cuando SSH está habilitado, SSH proporciona un servicio criptográfico para la transmisión de datos.
Restablecimiento de PCD Habilitar	Si está habilitado, puede restablecer la contraseña. Esta función está habilitada por defecto.
CGI	Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas de manera similar a las aplicaciones de consola que se ejecutan en un servidor que genera dinámicamente páginas web.VR dne Cuando CGI está habilitado, se pueden usar comandos CGI. El CGI está habilitado de forma predeterminada.
ONVIF	Habilite otros dispositivos para extraer la transmisión de video del VTO a través del protocolo ONVIF.

Parámetro	Descripción
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, HTTPS se utilizará para acceder a los comandos CGI; de lo contrario, se utilizará HTTP. Cuando HTTPS está habilitado, el dispositivo se reiniciará automáticamente.
Compatible con TLSv1.1 y versiones anteriores	Habilite esta función si su navegador utiliza TLS V1.1 o versiones anteriores.
Emergencia Mantenimiento	Habilítelo para análisis de fallas y mantenimiento.
Método de autenticación	• **Modo de seguridad (recomendado)**: admite el inicio de sesión con autenticación Digest. • **Modo compatible**: Compatible con el método de inicio de sesión de dispositivos antiguos.

3.1.11.2.2 Crear certificado de servidor

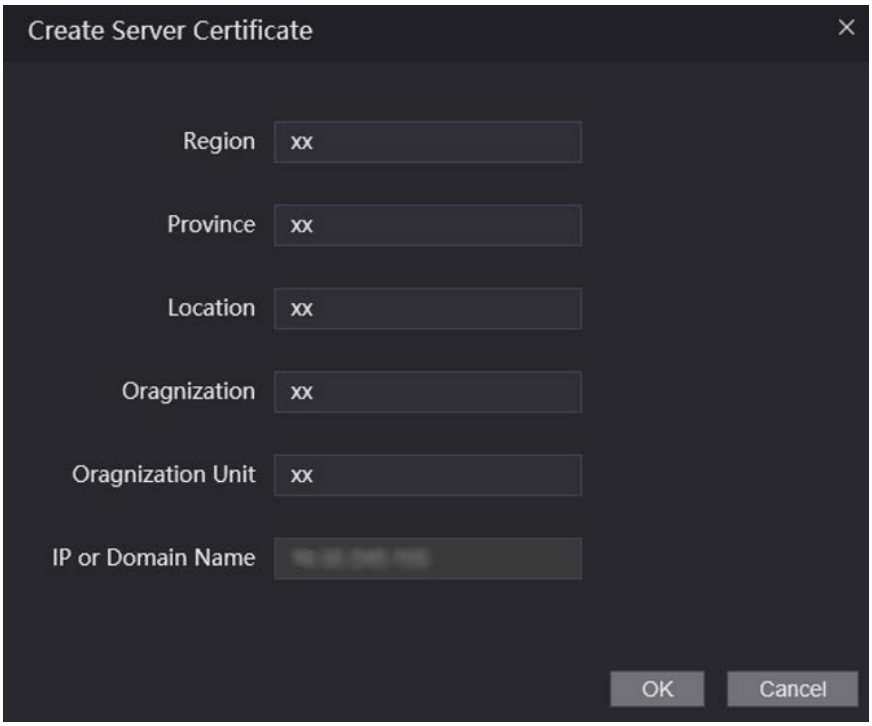
Configure el servidor HTTPS para mejorar la seguridad de su sitio web con el certificado del servidor.

- Si usa HTTPS por primera vez o se cambia la dirección IP del dispositivo, cree un servidor certificado e instalar un certificado raíz.
- Si cambia de PC para iniciar sesión en la web, debe descargar e instalar el certificado raíz nuevamente en la nueva PC o copiarlo a la nueva PC.

Step 1 Sobre el**Servicio del sistema**página, haga clic**Crear certificado de servidor**.

Step 2 Ingresa la información y haz clic**OK**y luego el dispositivo se reiniciará.

Figure 3-28 Crear certificado de servidor

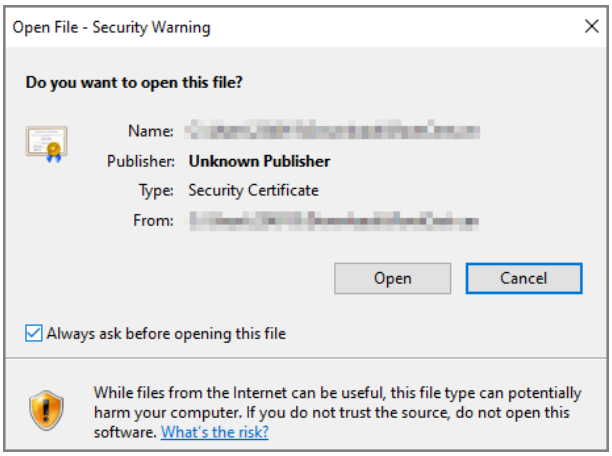


3.1.11.2.3 Descarga del certificado raíz

Step 1 Sobre el**Servicio del sistema**página, haga clic**Descargar certificado raíz**. Haga

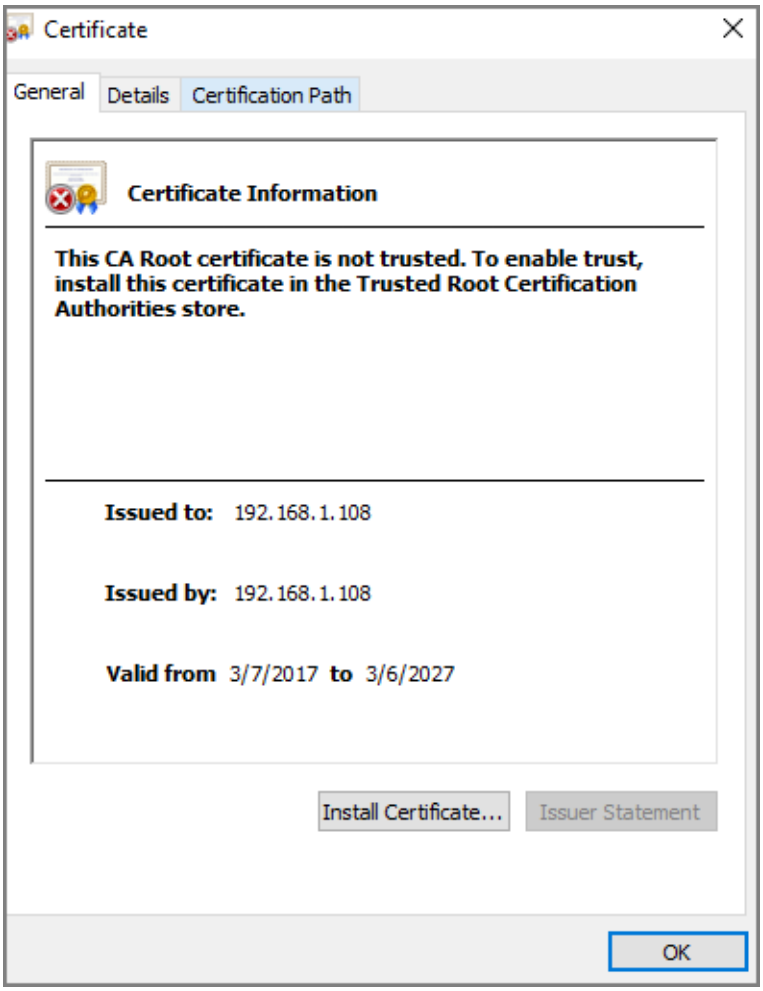
Step 2 doble clic en el archivo que ha descargado y luego haga clic en**Abierto**.

Figure 3-29 Descarga de archivos



Step 3 Hacer clic**Instalar certificado**.

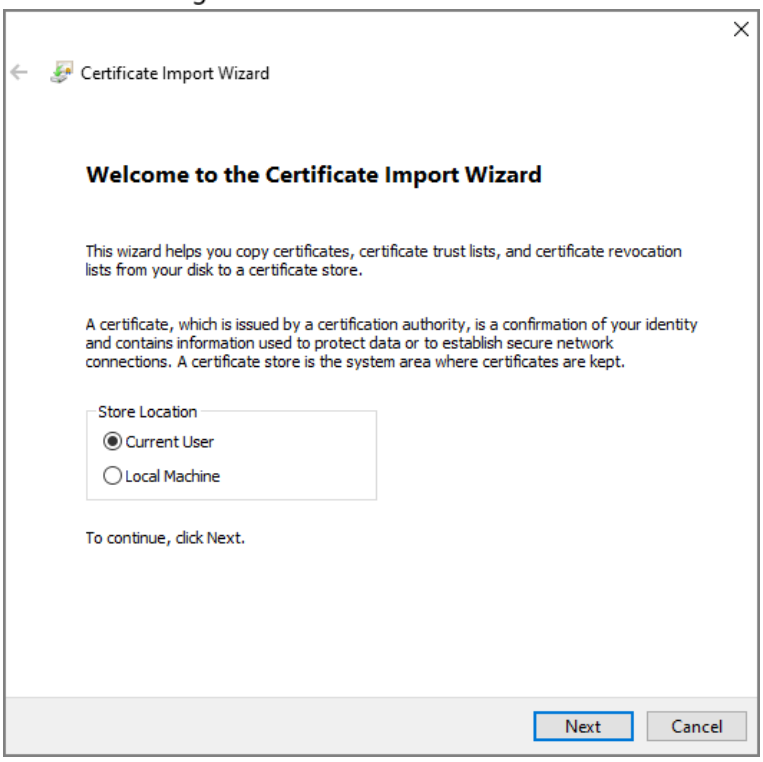
Figure 3-30 Información certificada



Step 4 Seleccione**Usuario actual**o**Máquina local**y luego haga clic en**Próximo**.

- **Usuario actual**: Se aplica al usuario que ha iniciado sesión en la PC. **Máquina**
- **local**: Se aplica a todos los usuarios que han iniciado sesión en la PC

Figure 3-31 Ubicación de la tienda

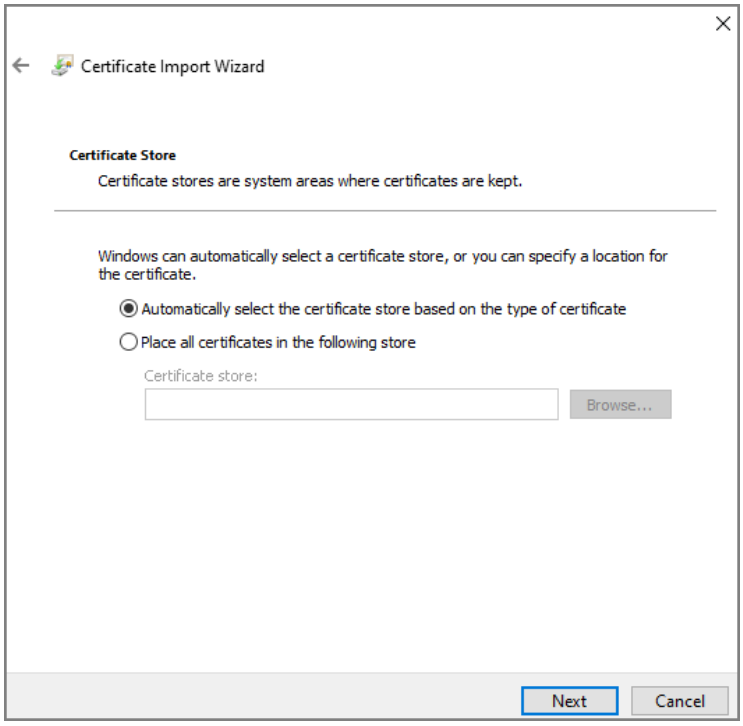


Step 5 Seleccione la ubicación de almacenamiento adecuada.

1) Seleccionar**Coloque todos los certificados en la siguiente tienda**.

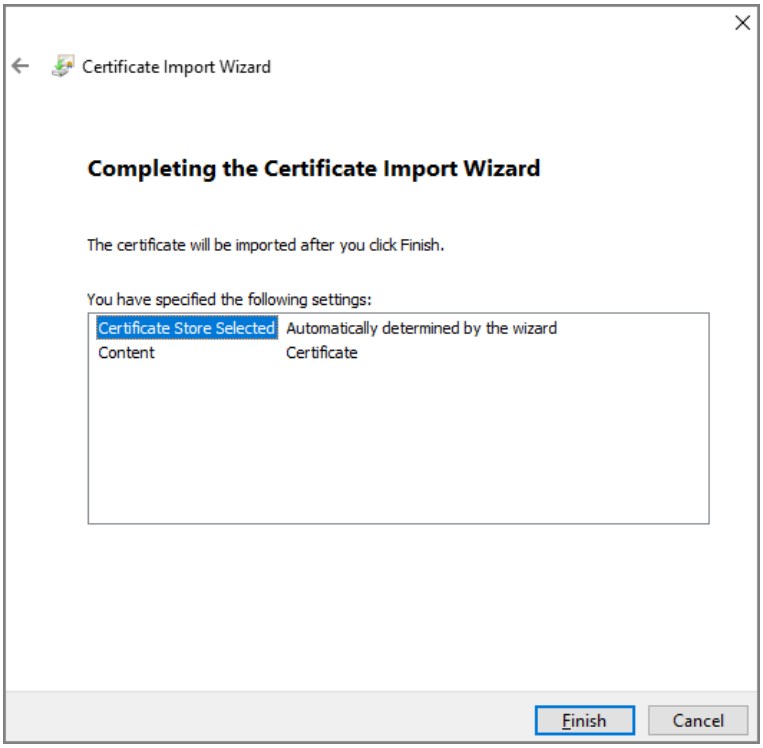
2) Haga clic**Navegar**para importar el certificado al**Autoridades de certificación raíz de confianza** almacenar y luego haga clic en**Próximo**.

Figure 3-32 Almacén de certificados



Step 6 Hacer clic**Finalizar**.

Figure 3-33 Almacén de certificados seleccionado



3.1.12 Gestión de usuarios

Puede agregar y eliminar usuarios, cambiar las contraseñas de los usuarios y vincular su dirección de correo electrónico para restablecer la contraseña cuando la olvide.

Usuario se refiere al usuario que inicia sesión en la página web.

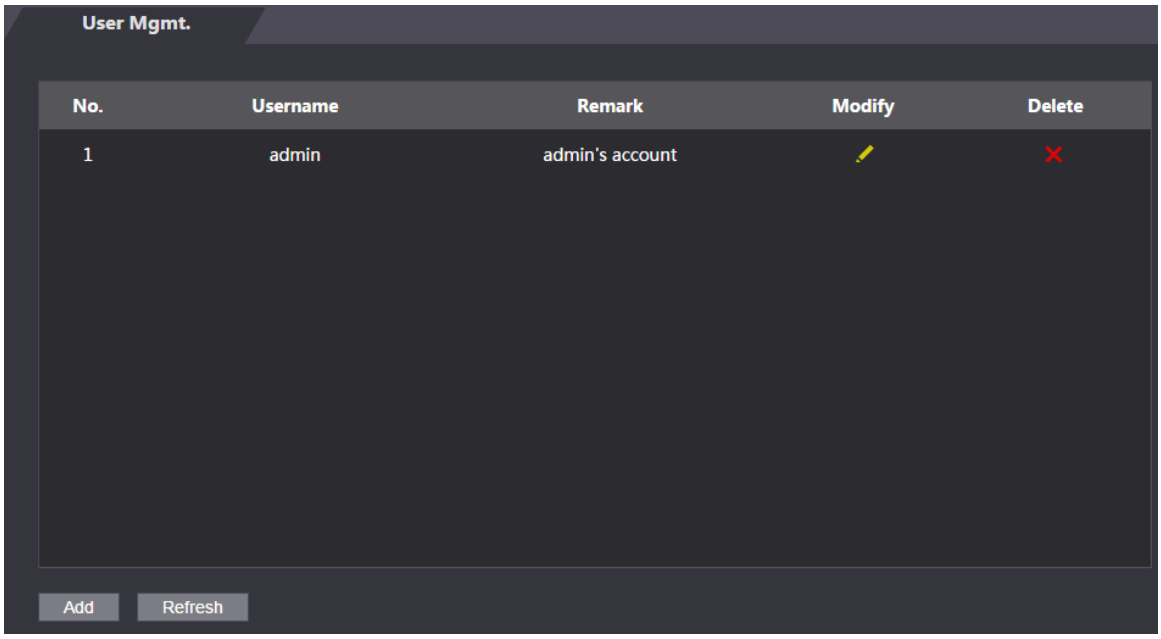
3.1.12.1 Usuario

3.1.12.1.1 Adición de usuarios

Step 1 Inicie sesión en la página web. Seleccione**Gestión de usuarios**>**Gestión de usuarios**.

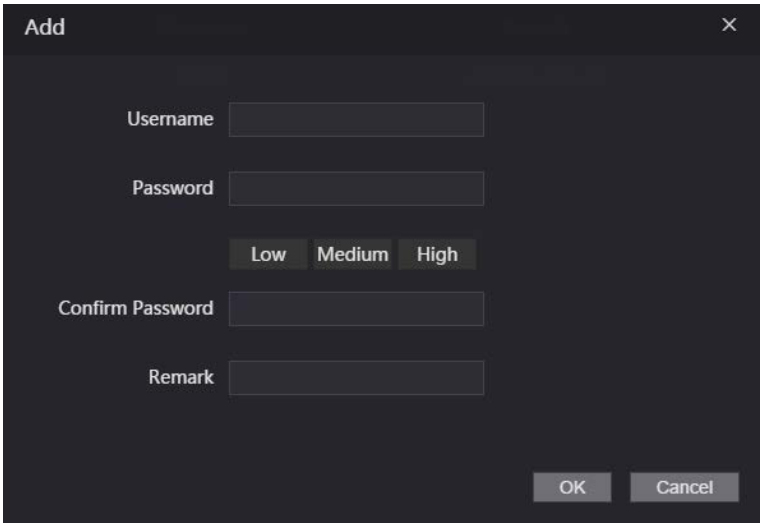
Step 2

Figure 3-34 Gestión de usuarios



Step 3 Hacer clic**Agregar**.

Figure 3-35 Agregar usuario



Step 4 Ingrese el nombre de usuario, la contraseña, confirme la contraseña y comente.

Step 5 Hacer clic**OK**.

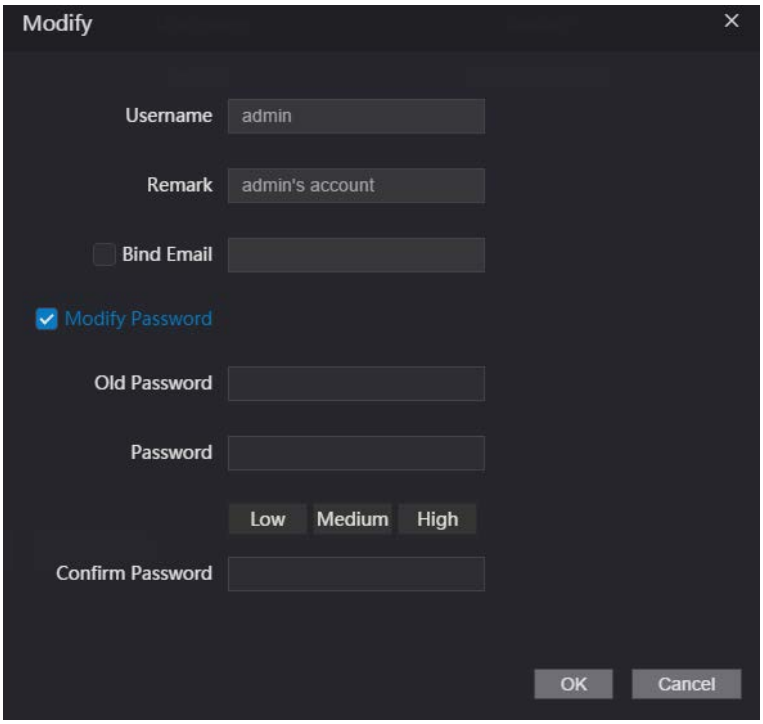
3.1.12.1.2 Cambio de contraseña

Step 1 Inicie sesión en la página web. Seleccione**Gestión**

Step 2 **de usuarios**>**Gestión de usuarios**. Haga clic en .

Step 3 

Figure 3-36 Modificar la información del usuario



Step 4 Selecciona el**Vincular correo electrónico**e ingrese la dirección de correo electrónico.

Step 5 Selecciona el**Modificar la contraseña**casilla de verificación, y luego ingrese la contraseña anterior, la contraseña nueva y confirme la contraseña.

Step 6 Hacer clic**OK**.

3.1.12.2 Usuario ONVIF

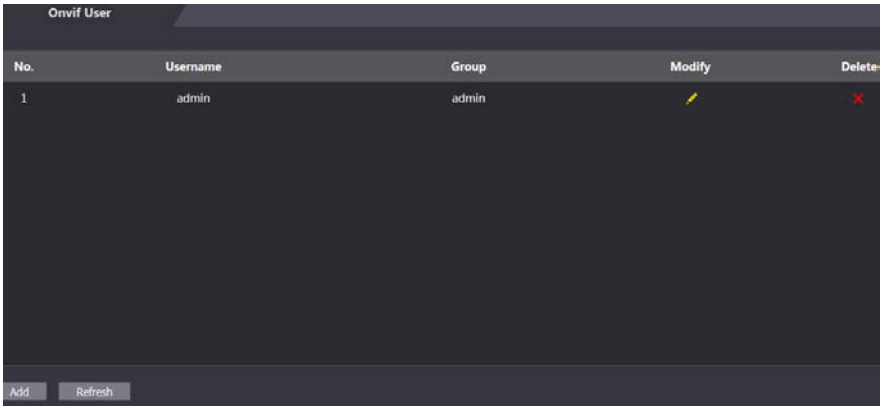
Open Network Video Interface Forum (ONVIF), un foro global y abierto de la industria establecido para el desarrollo de un estándar abierto global para la interfaz de productos físicos de seguridad basados en IP. Cree usuarios ONVIF y verifique sus identidades a través del protocolo ONVIF.

3.1.12.2.1 Agregar usuario ONVIF

Step 1 Inicie sesión en la página web. Seleccione

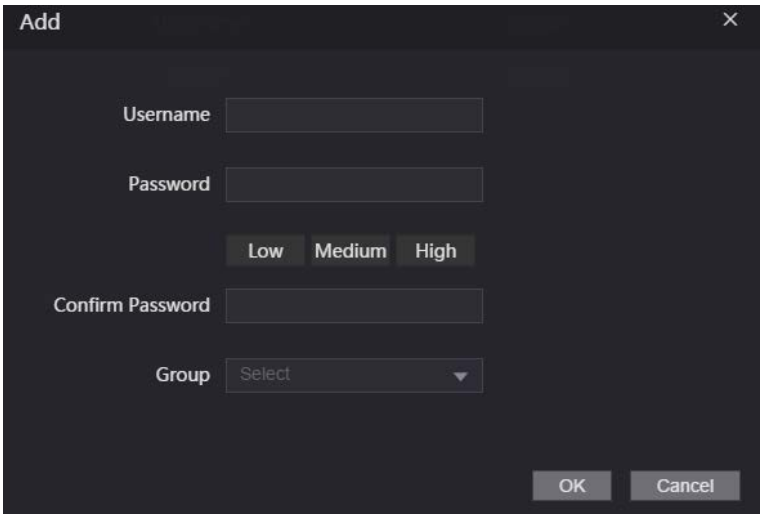
Step 2 **Gestión de usuarios**>**Usuario Onvif**.

Figure 3-37 Usuario de Onvif



Step 3 Hacer clic**Agregar**.

Figure 3-38 Añadir usuario ONVIF



Step 4 Ingrese el nombre de usuario, la contraseña y confirme la contraseña.

Step 5 Seleccione el grupo.

Step 6 Hacer clic**OK**.

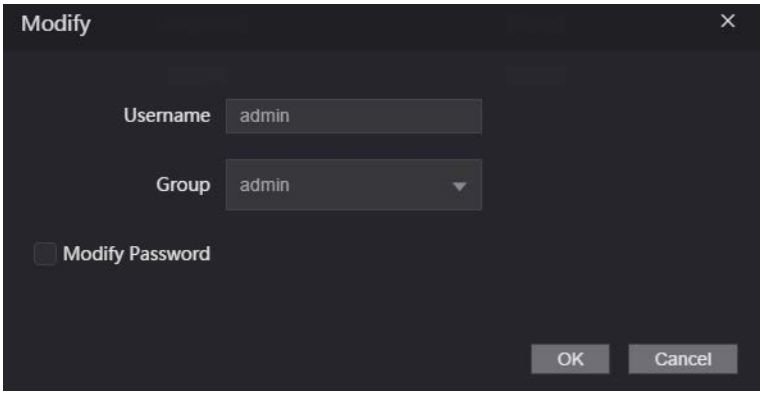
3.1.12.2.2 Cambio de contraseña

Step 1 Inicie sesión en la página web. Seleccione**Gestión**

Step 2 **de usuarios**>**Usuario Onvif**. Haga clic en .

Step 3 

Figure 3-39 Cambiar la contraseña (usuario ONVIF)



Step 4 Selecciona el**Modificar la contraseña**casilla de verificación, y luego ingrese la contraseña anterior, la contraseña nueva y confirme la contraseña.

Step 5 Hacer clic**OK**.

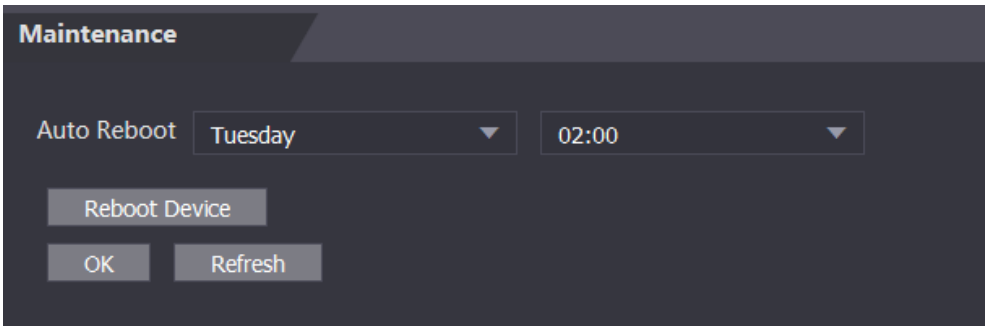
3.1.13 Mantenimiento

Puede reiniciar regularmente el dispositivo durante el tiempo de inactividad para mejorar su rendimiento.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Mantenimiento**.

Figure 3-40 Mantenimiento



Step 3 Establezca la hora y luego haga clic en**OK**.

El dispositivo se reiniciará a la hora definida.

Está**Nunca**por defecto.

Step 4 (Opcional) Haga clic en**Reiniciar dispositivo**y el dispositivo se reiniciará inmediatamente.

3.1.14 Gestión de la configuración

Cuando más de un dispositivo necesita las mismas configuraciones, puede configurar sus parámetros importando o exportando archivos de configuración.

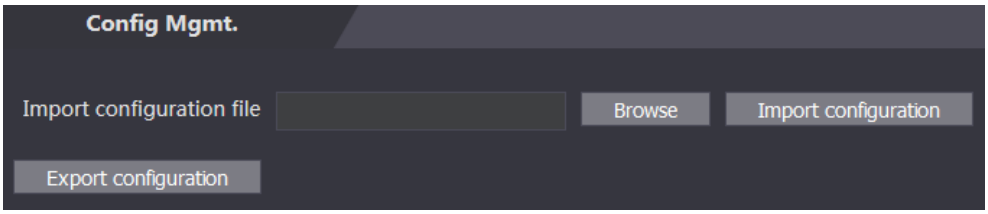
3.1.14.1 Exportación del archivo de configuración

Puede exportar el archivo de configuración del dispositivo para realizar una copia de seguridad.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Gestión de configuración**>**Gestión de configuración**.

Figure 3-41 Gestión de la configuración



Step 3 Hacer clic**Exportar configuración**para guardar el archivo de configuración localmente.

La información de IP del dispositivo no se exportará.

3.1.14.2 Importación del archivo de configuración

Puede exportar el archivo de configuración del dispositivo a otro con el mismo modelo de dispositivo.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Gestión de configuración**>**Gestión de configuración**.

Step 3 Hacer clic**Navegar**para seleccionar el archivo de configuración y luego haga clic en**Importar configuración**. El dispositivo se reiniciará después de importar el archivo de configuración.

3.1.14.3 Funciones de configuración

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Gestión de configuración**>**Gestión de configuración**. En

Step 3 el**Características**área, establezca las características.

Figure 3-42 Características

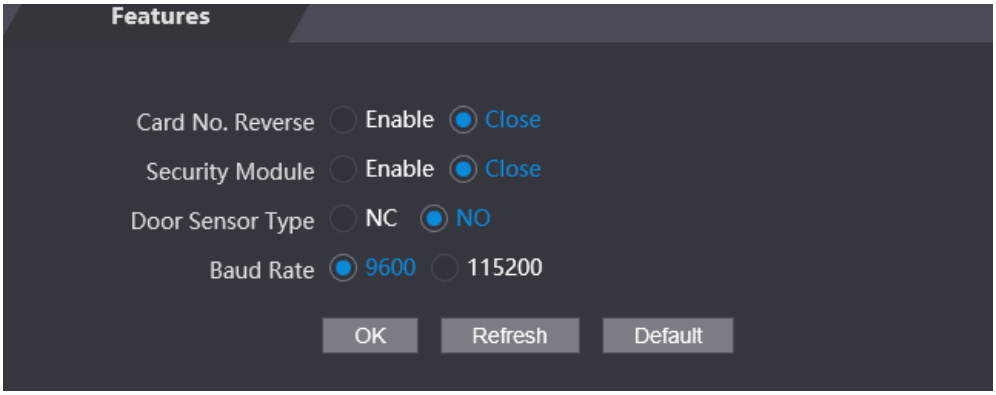


Tabla 3-9 Descripción de características

Parámetro	Descripción
Número de tarjeta Reverso	Habilitar**Número de tarjeta Reverso**función, si configura la salida Wiegand y conecta un dispositivo externo, pero el orden del número de tarjeta recibido no coincide con el del número real.
Módulo de seguridad	Si**Módulo de seguridad**está habilitado, el botón de salida de la puerta, el bloqueo y el enlace de incendio no son válidos.
Tipo de sensor de puerta	Establecer tipo de sensor de puerta: ● **CAROLINA DEL NORTE**: Normalmente ● cerrado. **NO**: Normalmente abierto.
Tasa de baudios	Seleccione la tasa de baudios según el dispositivo externo.

Step 4 Hacer clic**OK**.

3.1.14.4 Configuración de la huella digital

Puede configurar el nivel de identidad de la huella digital para ajustar la tasa de precisión del reconocimiento.

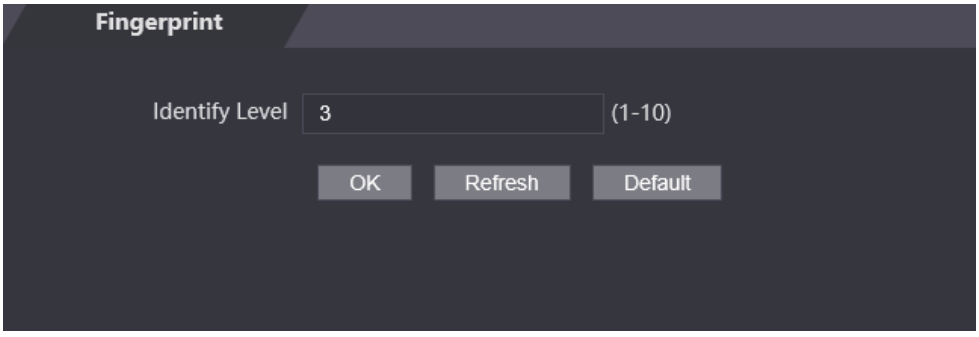
Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Gestión de configuración**>**Gestión de configuración**.

Step 3 En el**Huella dactilar**área, establezca el nivel de identidad.

El nivel de identidad más alto significa una precisión de reconocimiento más alta y un umbral de reconocimiento más alto.

Figure 3-43 Nivel de identidad de huellas dactilares



Step 4 Hacer clic**OK**.

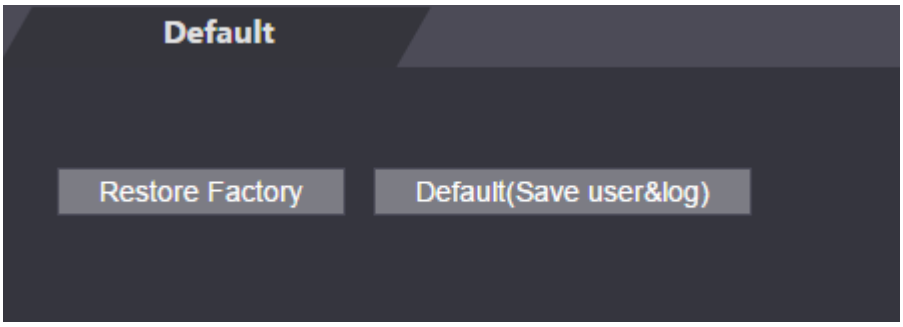
3.1.14.5 Restablecimiento de valores predeterminados de fábrica

Restaurar el dispositivo a las configuraciones predeterminadas provocará la pérdida de datos. Por favor tenga en cuenta.

Step 1 Inicie sesión en la página web. Seleccione

Step 2 **Gestión de configuración**>**Por defecto**.

Figure 3-44 Por defecto



Step 3 Restaure los valores predeterminados de fábrica si es necesario.

- **Restaurar fábrica:**Restablece las configuraciones del Dispositivo y elimina todos los datos.
- **Restaurar fábrica (Guardar usuario y registro)**: restablece las configuraciones del dispositivo y elimina todos los datos excepto la información del usuario y los registros.

3.1.15 Sistema de actualización

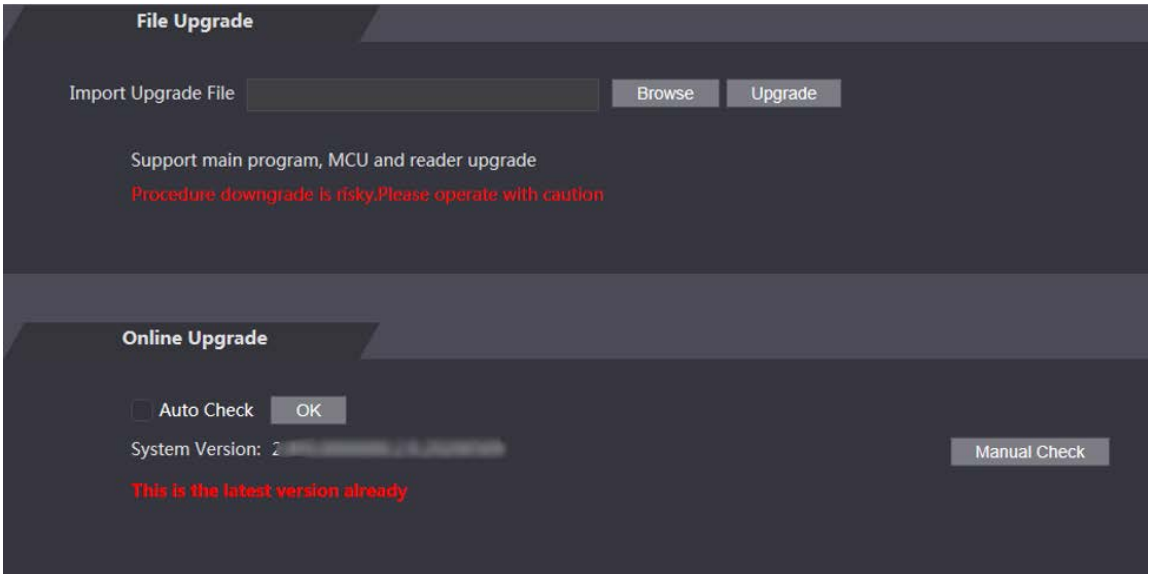
- Exporte el archivo de configuración para hacer una copia de seguridad antes de actualizar y luego importe el archivo después de la actualización completa
- Utilice el archivo de actualización correcto. Asegúrese de obtener el archivo de actualización correcto del soporte técnico.

No desconecte la alimentación o la red, ni reinicie ni apague el dispositivo durante la actualización.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Potenciar**.

Figure 3-45 Potenciar



Step 3 Seleccione el método de actualización.

- Actualización de archivo

1) Haga clic**Navegar**y luego cargue el archivo de actualización. El archivo de actualización debe ser un archivo .bin.

2) Haga clic**Potenciar**.

El dispositivo se reiniciará después de que se complete la actualización.

- Actualización en línea

1) Seleccione el**Verificación automática**casilla de verificación y, a continuación, haga clic en**OK**. El sistema busca una nueva versión automáticamente.

Necesitamos recopilar datos como el nombre del dispositivo, la versión del firmware y el número de serie del dispositivo. número para proceder a la verificación automática. La información recopilada solo se utiliza para verificar la legalidad de las cámaras y notificación de actualización.

2) Si hay alguna nueva versión disponible, haga clic en**Potenciar**. El dispositivo se reiniciará después de que se complete la actualización.

Hacer clic**Comprobación manual**para buscar una nueva versión manualmente.

3.1.16 Información de la versión

Vea información que incluye la dirección MAC, el número de serie, la versión de MCU, la versión web, la versión de referencia de seguridad, la versión del sistema y la versión de firmware.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Información de la versión**para ver la información de la versión.

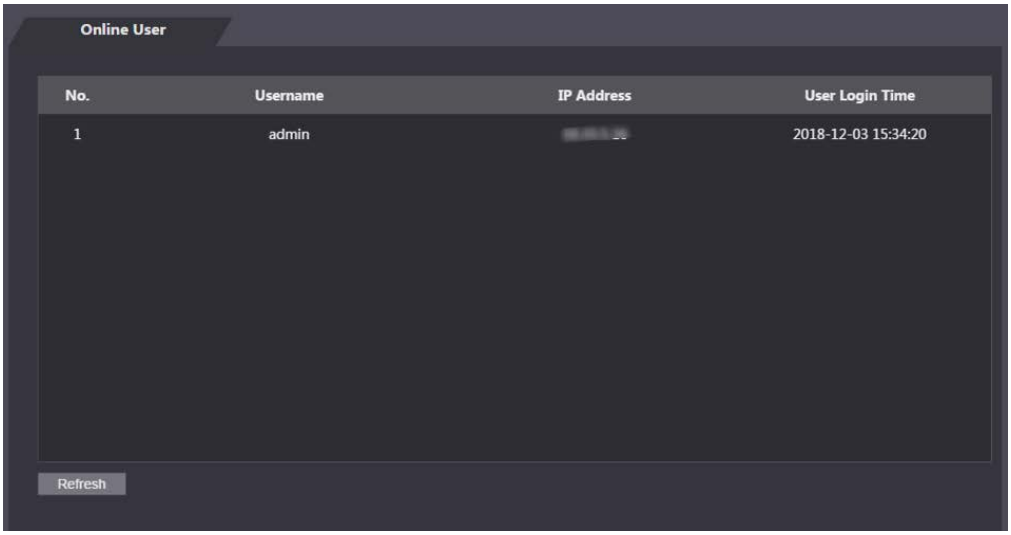
3.1.17 Visualización del usuario en línea

Puede ver los usuarios en línea que inician sesión en la web, incluido su nombre de usuario, dirección IP y hora de inicio de sesión.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Usuario en línea**.

Figure 3-46 Usuario en línea



3.1.18 Visualización de registros del sistema

Vea y haga una copia de seguridad de los registros del sistema, los registros de administración y los registros de desbloqueo.

3.1.18.1 Registros del sistema

Ver y buscar registros del sistema.

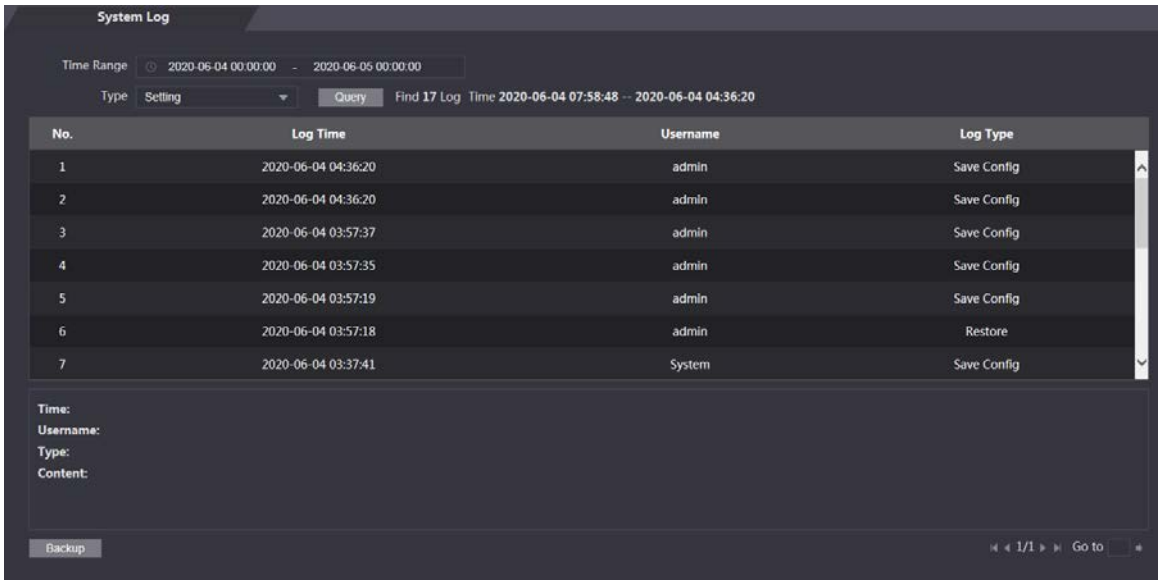
Step 1 Inicie sesión en la página web. Seleccione**Registro**

Step 2 **del sistema**>**Registro del sistema**.

Step 3 Seleccione el intervalo de tiempo y el tipo de registro y, a continuación, haga clic en**Consulta**.

Hacer clic**Respaldo**para descargar los resultados.

Figure 3-47 Buscar registros



3.1.18.2 Registros de administración

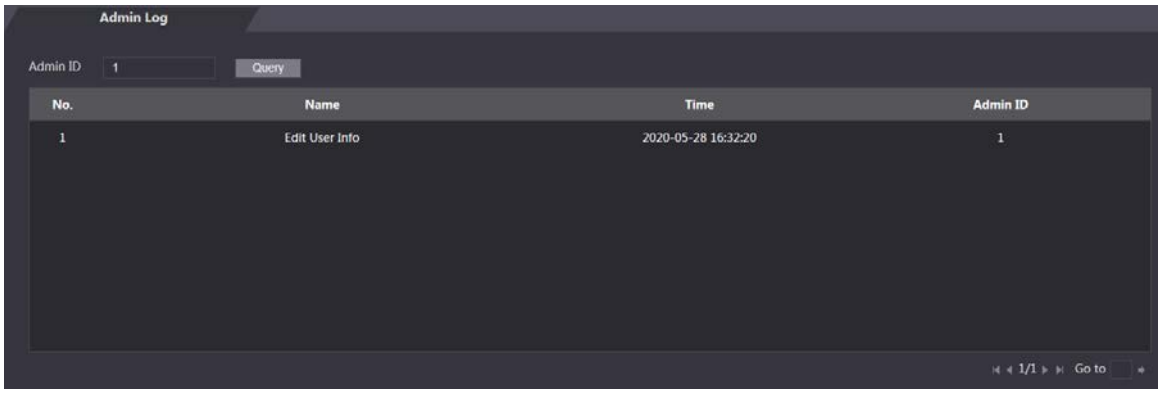
Busque registros de administrador mediante el ID de administrador.

Step 1 Inicie sesión en la página web. Seleccione**Registro del sistema**>**Registro de**

Step 2 **administración**. Ingrese la identificación del administrador y luego haga clic

Step 3 en**Consulta**.

Figure 3-48 Registro de administración



3.1.18.3 Desbloquear registros

Busque y exporte registros de desbloqueo.

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Registro del sistema**>**Registros de búsqueda**.

Step 3 Seleccione el intervalo de tiempo y el tipo de registro y, a continuación, haga clic en**Consulta**.

Step 4 Hacer clic**Exportar datos**para descargar los resultados.

3.1.19 Cerrar sesión

Hacer clic  en la esquina superior izquierda y luego haga clic en**OK**para salir de la página web.

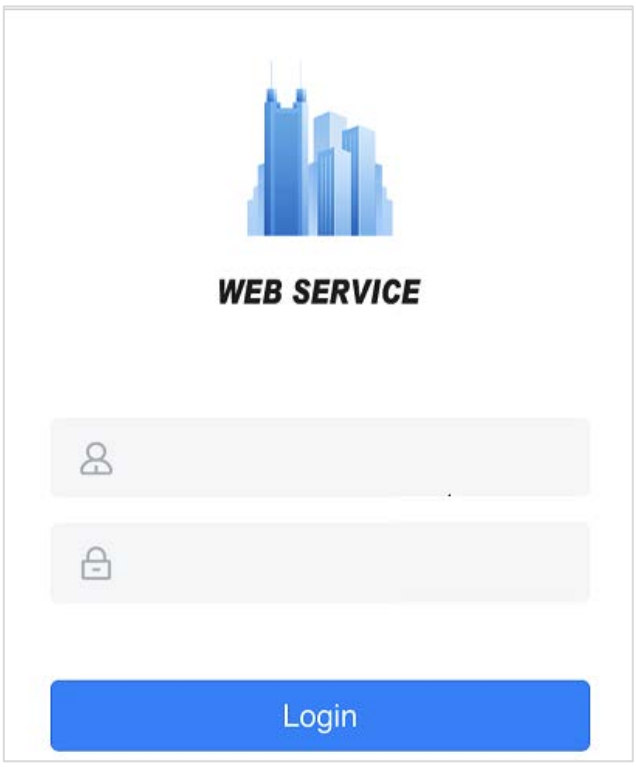
3.2 Internet en el teléfono

Asegúrese de que el dispositivo esté en la misma LAN que su teléfono. Conecte el dispositivo al punto de acceso de su teléfono o conecte el dispositivo y su teléfono al mismo enrutador.

Solo se pueden configurar ciertos parámetros en el portal web si inicia sesión en un teléfono.

Step 1 Vaya a la dirección IP (192.168.1.108 por defecto) del Dispositivo en el navegador.

Figure 3-49 Acceso



Step 2 Introduzca el nombre de usuario y la contraseña.

El nombre de administrador predeterminado es admin, y la contraseña es la que estableció durante inicialización Le recomendamos que cambie la contraseña de administrador regularmente para aumentar seguridad.

Step 3 Hacer clic**Acceso**.

4 Configuración de CA de SmartPSS

Este capítulo presenta cómo administrar y configurar el dispositivo mediante el uso de SmartPSS AC. Para obtener más información, consulte el manual del usuario de SmartPSS AC.

Utilice Smart PSS AC como ejemplo para las configuraciones. Las ventanas en el manual del usuario son solo para referencia, y puede diferir del producto real.

4.1 Iniciando sesión

Step 1 Instale SmartPSS AC.

Step 2 Haga doble clic en y luego siga las indicaciones para completar la inicialización e iniciar sesión.

4.2 Adición de dispositivos

Debe agregar el dispositivo a SmartPSS AC. Puede en lote o individualmente.

4.2.1 Agregando individualmente

Step 1 Inicie sesión en SmartPSS AC. Hacer

Step 2 clic**Administrador de dispositivos**.

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

Step 4 página. Ingrese la información requerida.

Figure 4-1 Ingrese la información del dispositivo

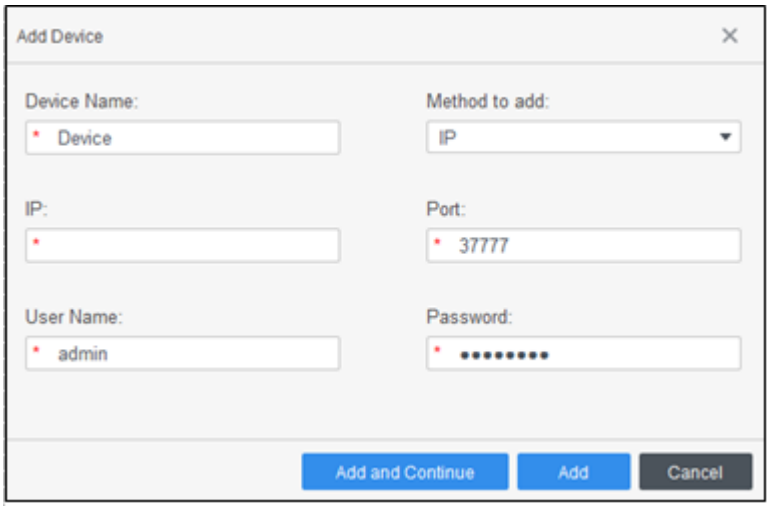


Tabla 4-1 Descripción de los parámetros del dispositivo

Parámetro	Descripción
Nombre del dispositivo	Introduzca un nombre del dispositivo. Recomendamos nombrar el dispositivo de acuerdo con su área de instalación.
Método para agregar	Seleccione**IP**para agregar un dispositivo a través de la dirección IP.
IP	Introduzca la dirección IP del dispositivo.
Puerto	El número de puerto es 37777 por defecto.
Nombre de usuario, Clave	Introduzca el nombre de usuario y la contraseña del dispositivo.

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

El dispositivo inicia sesión automáticamente después de ser agregado.**En línea**se muestra después de un inicio de sesión exitoso.

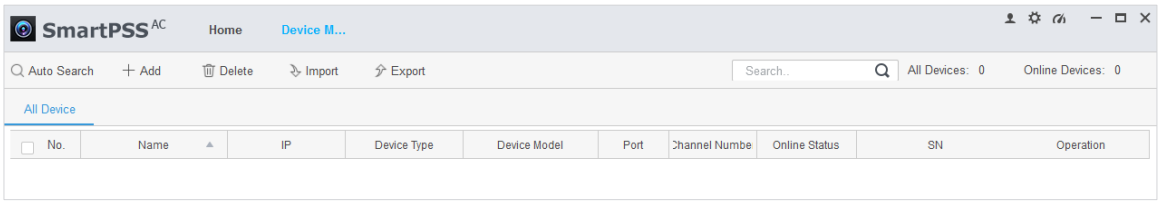
4.2.2 Agregar en lote

Recomendamos la función de búsqueda automática cuando agrega dispositivos en lote. Los dispositivos que agregue deben estar en el mismo segmento de red.

Step 1 Inicie sesión en SmartPSS AC. Hacer

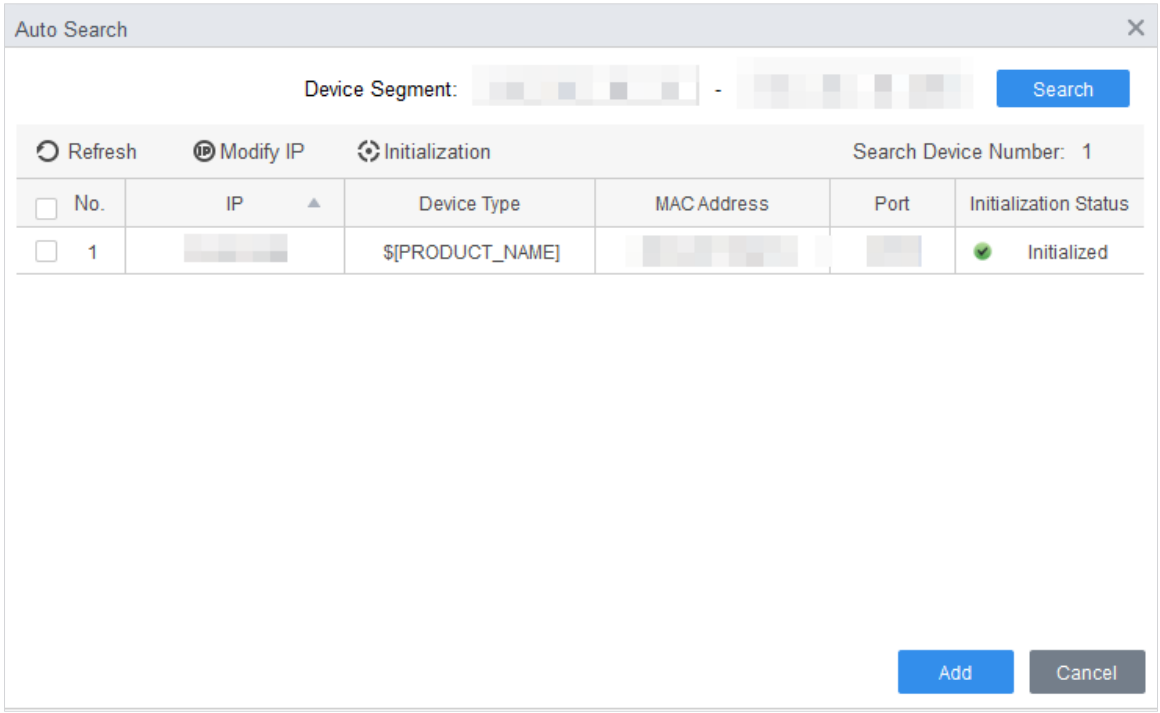
Step 2 clic**Administrador de dispositivos**.

Figure 4-2 Dispositivos



Step 3 Hacer clic**Auto búsqueda**.

Figure 4-3 Auto búsqueda



Step 4 Ingrese el segmento de red y luego haga clic en**Búsqueda**. Se mostrará una lista de dispositivos.

- Hacer clic**Búsqueda**para actualizar la lista de dispositivos.
- Seleccione un dispositivo y luego haga clic en**Modificar IP**para modificar su dirección IP. Para más detalles, consulte el manual de usuario de SmartPSS AC.

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

Step 6 Introduzca el nombre de usuario y la contraseña del dispositivo.

Puede ver los dispositivos agregados en la**Dispositivos**página.

- El dispositivo inicia sesión automáticamente después de ser agregado.**En línea**se muestra después de éxito acceso.

Operación relacionada

- : edite la información del dispositivo, incluido el nombre del dispositivo, la dirección IP, el número de puerto, el nombre de usuario y clave.
  También puede hacer doble clic en el dispositivo para editar su información.
- : Configure el dispositivo. Puede configurar la hora, actualizar el dispositivo, reiniciar el dispositivo y extraer información del usuario o registros de asistencia del dispositivo.
- y : Iniciar y cerrar sesión en el dispositivo.
- : elimina el dispositivo.

4.3 Gestión de usuarios

Agregue usuarios, emita tarjetas para ellos y configure sus permisos de acceso.

4.3.1 Configuración del tipo de tarjeta

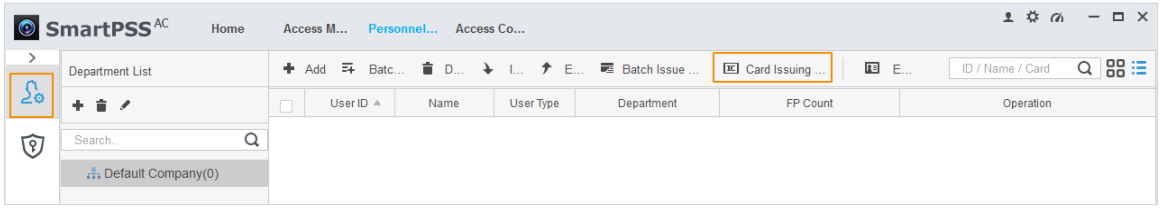
Antes de emitir la tarjeta, establezca primero el tipo de tarjeta. Por ejemplo, si la tarjeta emitida es una tarjeta de identificación, establezca el tipo en Tarjeta de identificación.

Los tipos de tarjetas deben ser los mismos que los tipos de emisores de tarjetas; de lo contrario, los números de tarjeta no se pueden leer.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Gerente de Personal**.

Figure 4-4 gerente de personal

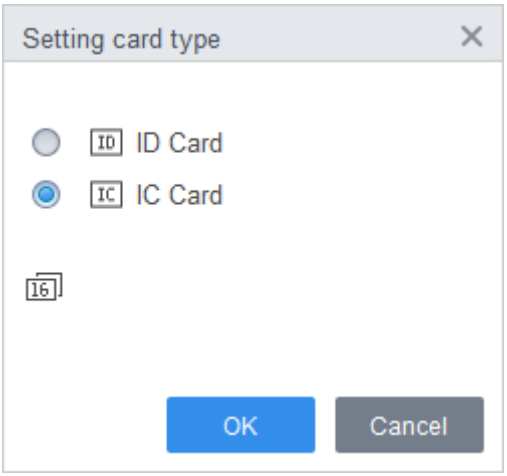


Step 3 Hacer clic y luego haga clic en .

Step 4 Sobre el**Configuración del tipo de tarjeta**ventana, seleccione un tipo de tarjeta.

Step 5 Hacer clic para seleccionar el método de visualización del número de tarjeta en decimal o en hexadecimal.

Figure 4-5 Configuración del tipo de tarjeta



Step 6 Hacer clic**OK**.

4.3.2 Agregar usuario

4.3.2.1 Adición individual

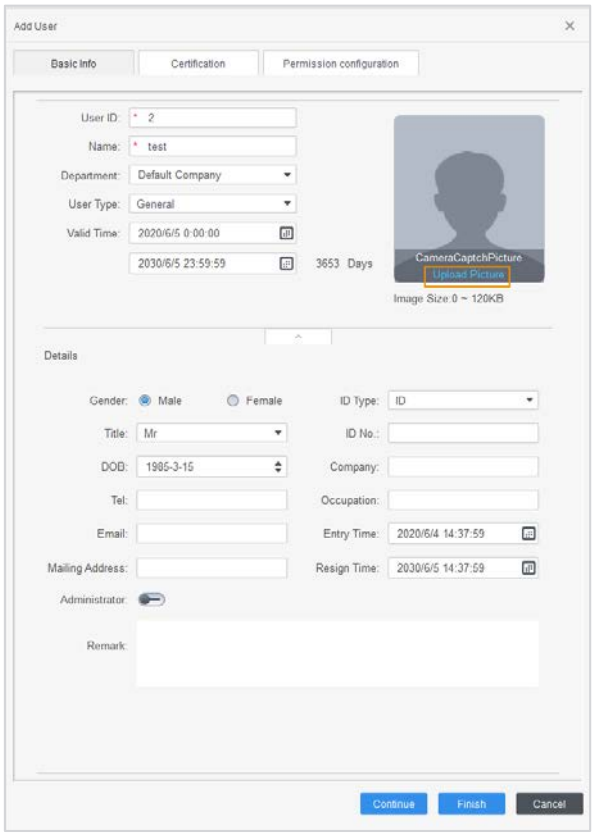
Puede agregar usuarios uno por uno manualmente.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Gerente de Personal**>**Usuario**>**Agregar**.

Step 3 Haga clic en el**Información básica**pestaña, e ingrese la información básica del usuario.

Figure 4-6 Agregar información básica



Step 4 Haga clic en el**Certificación**pestaña para agregar información de certificación del usuario.

- Configurar contraseña.

  La contraseña debe constar de 6 a 8 dígitos.

- Configurar tarjeta.

  El número de tarjeta puede leerse automáticamente o introducirse manualmente. Para leer la tarjeta número automáticamente, seleccione un lector de tarjetas y luego coloque la tarjeta en el lector de tarjetas.

1) Haga clic en , establezca**Lector de tarjetas**para**Dispositivo**y luego seleccione el dispositivo que agrega desde**Dispositivo**.

2) Haga clic**Agregar**, deslice una tarjeta en el dispositivo y luego se mostrará el número de tarjeta.

3) Haga clic**OK**.

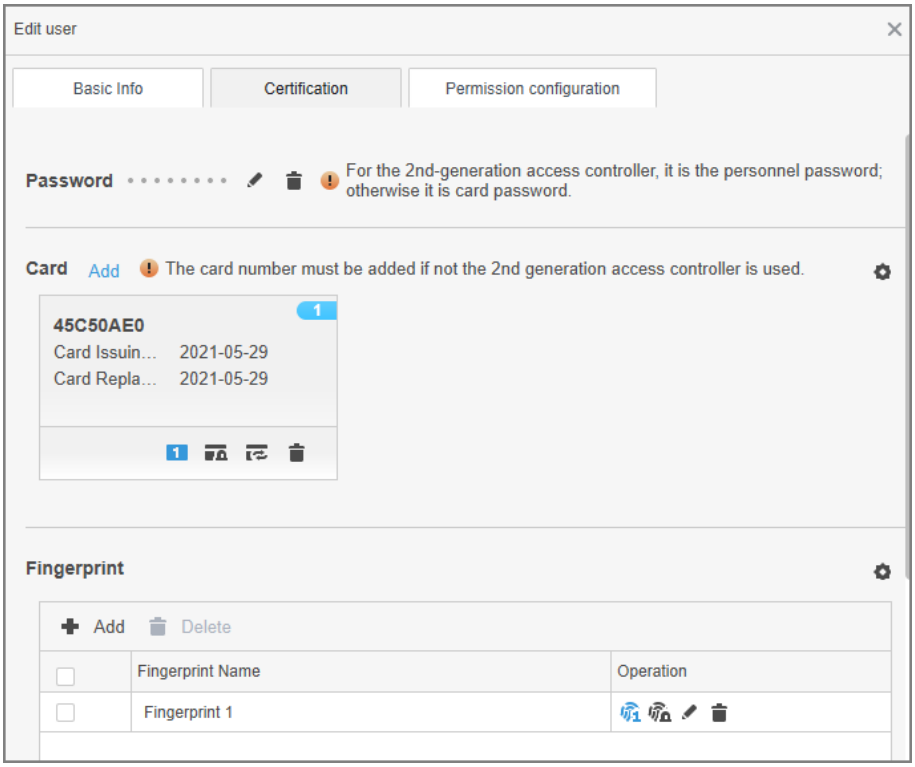
4) (Opcional) Después de agregar una tarjeta, puede configurar la tarjeta como tarjeta principal o tarjeta de coacción, reemplazar la tarjeta por una nueva o eliminar la tarjeta.

- Configurar huella dactilar.

1) Haga clic en , establezca**Recolector de huellas dactilares**para**Dispositivo**.

2) Haga clic**Agregar**y presione su dedo en el escáner tres veces seguidas.

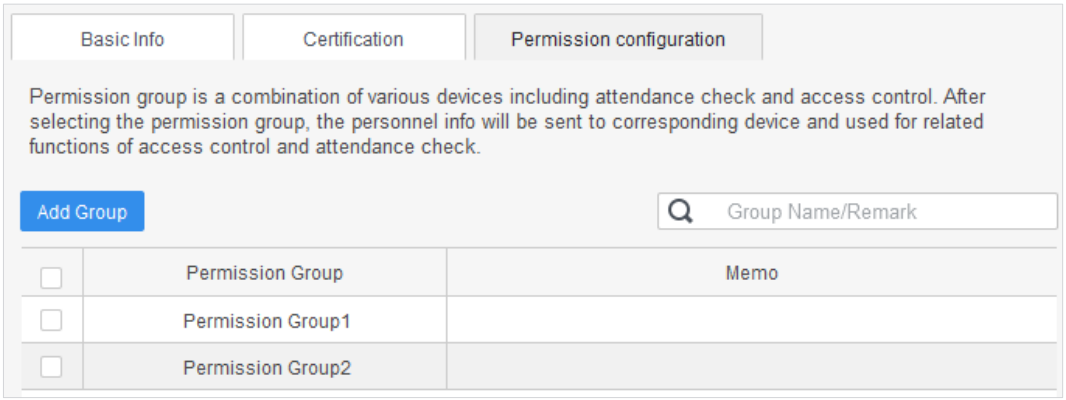
Figure 4-7 Agregar contraseña, tarjeta y huella digital



Step 5 Configurar permisos para el usuario.

Para obtener más información, consulte "4.4 Asignación de permisos".

Figure 4-8 Configuración de permisos



Step 6 Hacer clic**Finalizar**.

4.3.2.2 Agregar en lote

Puede agregar usuarios en lotes.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Gerente de Personal**>**Usuario**>**Agregar lote**.

Step 3 Seleccione**Dispositivo**desde**Dispositivo**y luego seleccione el dispositivo que agrega.

Step 4 Configure los siguientes parámetros.

- **Nº de inicio**: El ID de usuario comienza con el número que definió. **Cantidad**
- : El número de usuarios que desea agregar. **Departamento**: Seleccione el
- departamento al que pertenece el usuario.

- **Tiempo efectivo**y**Tiempo expirado**: Los usuarios pueden desbloquear la puerta dentro del período definido.

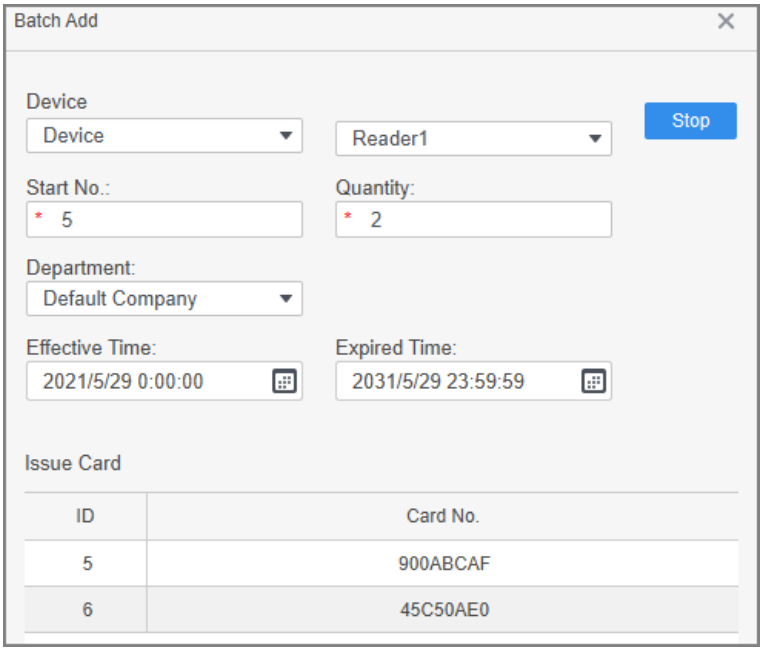
Step 5 Hacer clic**Asunto**.

El número de tarjeta se leerá automáticamente. Hacer clic

Step 6 **Detener**cuando termine de emitir tarjetas. Hacer clic**OK**.

Step 7

Figure 4-9 Agregar usuarios en lotes



Step 8 En la lista de usuarios, haga clic en para editar la información de los usuarios añadidos.

4.4 Asignación de permisos

Agregue dispositivos a un grupo de permisos y luego los usuarios del grupo podrán desbloquear las puertas correspondientes.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Gerente de Personal**>**Configuración de permisos**.

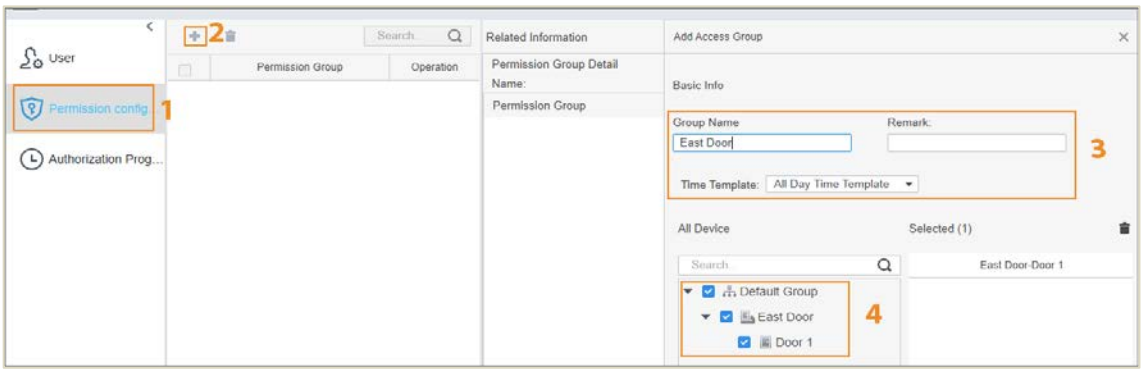
Step 3 Haga clic en .

Step 4 Ingrese el nombre del grupo, comentarios (opcional) y seleccione una plantilla de tiempo.

Step 5 Seleccione los dispositivos.

Step 6 Hacer clic**OK**.

Figure 4-10 Crear un grupo de permisos



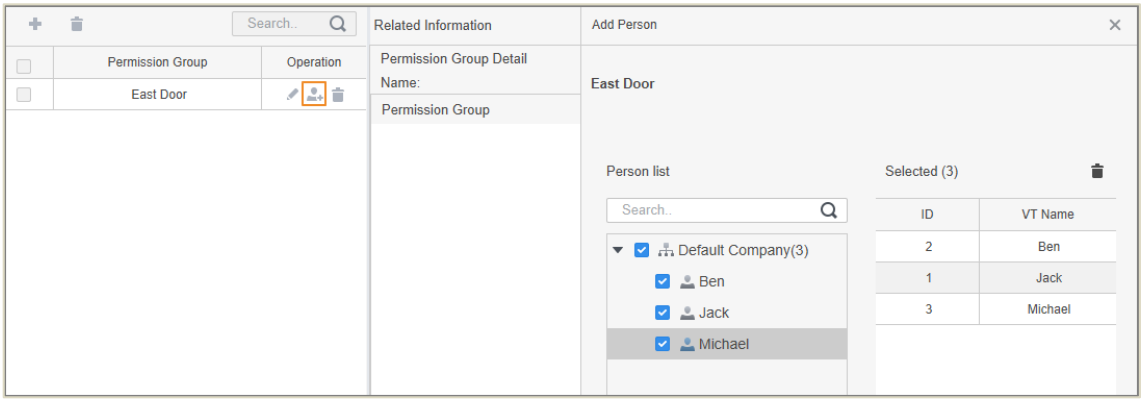
Step 7 Hacer clic del grupo de permisos que agregó.

Step 8 Seleccione los usuarios que desea agregar al grupo de permisos. Hacer

Step 9 clic**OK**.

Los usuarios del grupo de permisos pueden deslizar sus tarjetas o usar otros métodos de desbloqueo para desbloquear la puerta.

Figure 4-11 Agregar usuarios a un grupo de permisos



Appendix 1 Instrucciones de registro de huellas dactilares

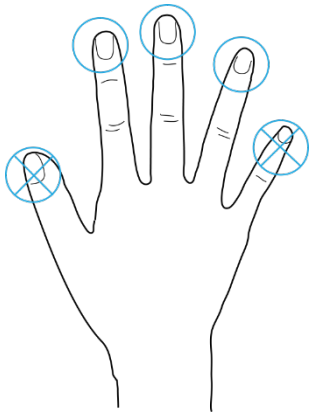
Cuando registre la huella digital, preste atención a los siguientes puntos:

- 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.

Dedos recomendados

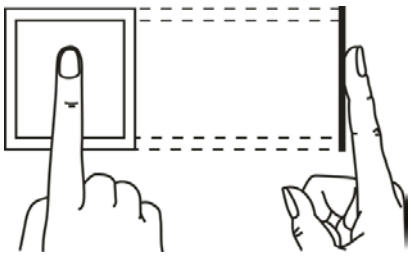
Se recomiendan los dedos índice, medio y anular. Los pulgares y los meñiques no se pueden colocar fácilmente en el centro de grabación.

Apéndice Figura 1-1 Dedos recomendados

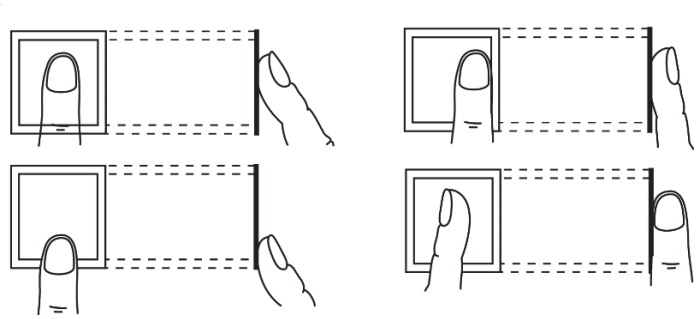


Cómo presionar su huella digital en el escáner

Apéndice Figura 1-2 Colocación correcta



Apéndice Figura 1-3 Colocación incorrecta



Appendix 2 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: 2. 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.

3. Cambie las contraseñas regularmente

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

4. 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.

5. 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.

6. 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.

7. Habilitar HTTPS

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

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.