Acceso independiente

Manual del usuario

Versión 1.0.4

Prefacio

General

Este manual presenta la instalación y las operaciones básicas del Access Standalone (en adelante denominado "el Dispositivo").

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
 **PELIGRO**	Indica un alto riesgo 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, reducciones en el rendimiento o resultados impredecibles.
 **CONSEJOS**	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
 **NOTA**	Proporciona información adicional como complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.4	Se actualizó la gestión de usuarios.	Noviembre de 2023
Versión 1.0.3	Se actualizó el manual.	Enero de 2023
Versión 1.0.2	Se actualizó el manual.	Mayo de 2022
Versión 1.0.1	Se actualizaron las configuraciones del lector de tarjetas.	Octubre de 2021
Versión 1.0.0	Primer lanzamiento	Septiembre 2021

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, es posible que recopile datos personales de otras personas, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y normativas locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de las medidas de seguridad adecuadas.

medidas que incluyen, pero no se limitan a: Proporcionar una identificación clara y visible para informar a las personas de la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del manual

- El manual es solo de referencia. Pueden existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Pueden encontrarse ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de explicación final.
- Actualice el software de lectura o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de explicación final.

Medidas de seguridad y advertencias importantes

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

Requisitos de instalación

 **ADVERTENCIA**

- Conecte el dispositivo al adaptador antes de encenderlo.
- Cumpla estrictamente las normas de seguridad eléctrica locales y asegúrese de que el voltaje en el área sea estable y se ajuste a los requisitos de energía del dispositivo.
- No conecte el dispositivo a más de una fuente de alimentación, ya que podría dañarse.

- Observe todos los procedimientos de seguridad y use el equipo de protección requerido provisto 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 del estuche proporcionada por el fabricante del dispositivo.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en la norma 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 conexión a tierra de protección.

Requisitos de funcionamiento

- Asegúrese de que la fuente de alimentación del dispositivo funciona correctamente antes de usarlo. No
- desconecte el cable de alimentación del dispositivo mientras esté encendido. Utilice el dispositivo
- únicamente dentro del rango de potencia nominal.
- Utilice el dispositivo en las condiciones de humedad y temperatura permitidas.
- Evite que los líquidos salpiquen o goteen sobre el dispositivo. Asegúrese de que no haya objetos que contengan líquido sobre el dispositivo para evitar que los líquidos fluyan hacia él.
- No desmonte el dispositivo.

Tabla de contenido

1 Descripción general del producto

1.1 Introducción

El dispositivo, que cuenta con un potente procesador y un algoritmo de aprendizaje profundo, puede identificar huellas dactilares de forma instantánea y precisa. El dispositivo también permite desbloquear la puerta con tarjetas, contraseñas, huellas dactilares o combinaciones de las mismas. Para satisfacer diferentes necesidades, también funciona con un software de gestión para realizar más funciones.

La función de huella dactilar está disponible en modelos seleccionados.

1.2 Características

- Pantalla LCD.
- Panel de PC + ABS/acrílico apto para uso exterior.
- 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 alarmas, 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. Admite timbre.
- Funciona con SmartPSS AC yDSS Pro.

1.3 Dimensiones

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

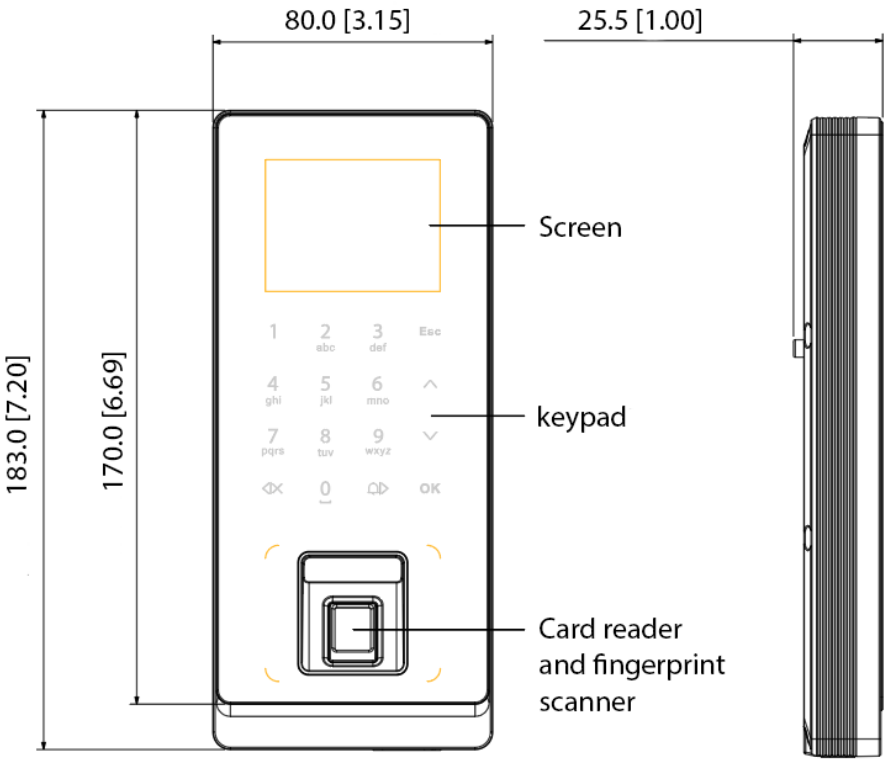
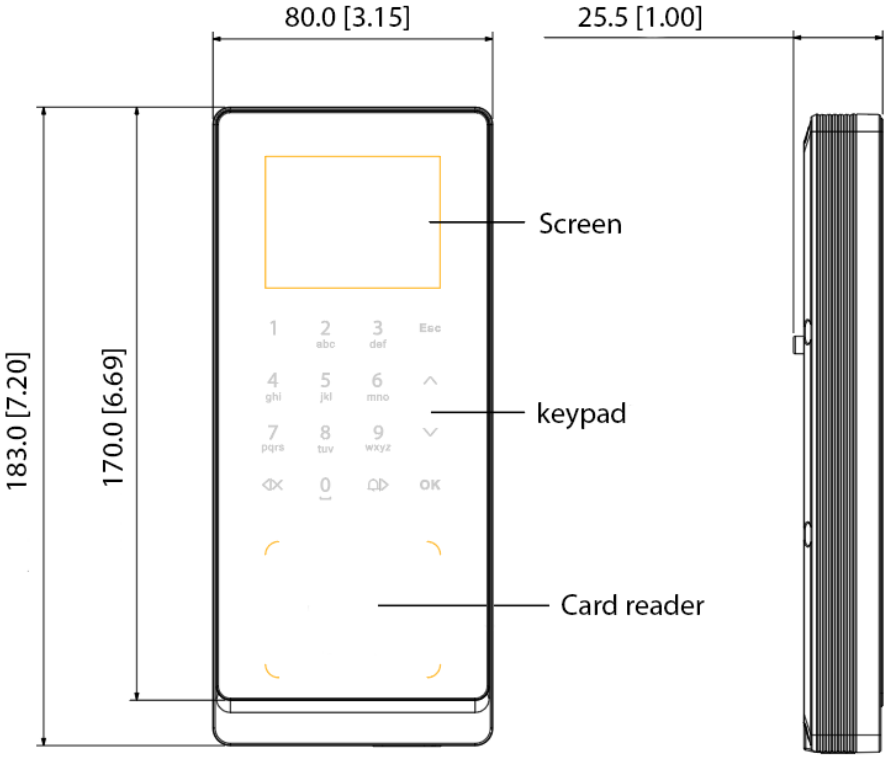


Figure 1-2 Dimensiones (2) (mm[pulgadas])

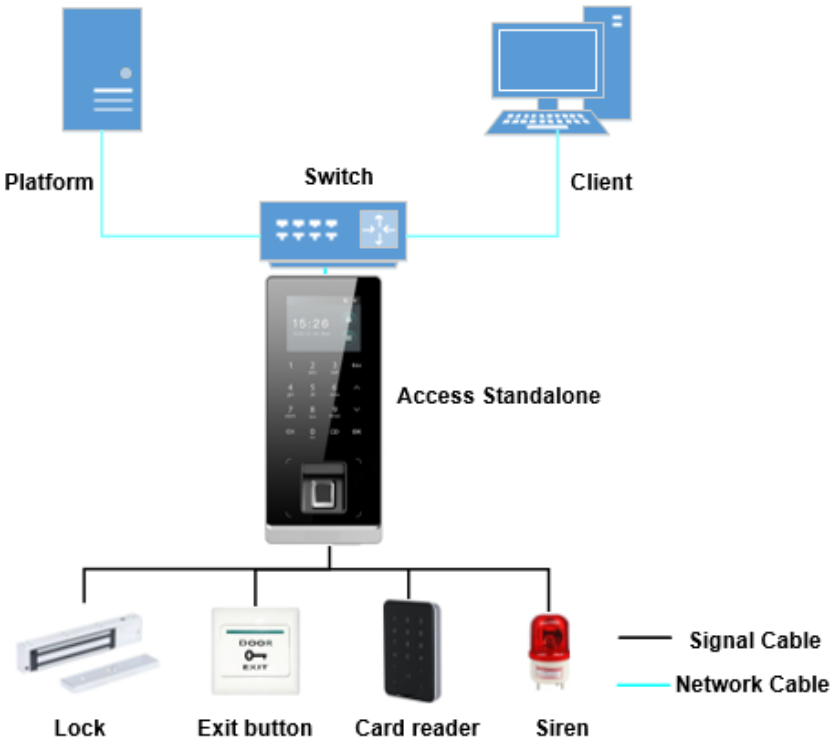


1.4 **Solicitud**

El dispositivo se puede utilizar en diversos escenarios, como edificios de oficinas, escuelas, parques industriales, complejos de apartamentos, fábricas, estadios públicos y centros comerciales. Este manual de usuario describe principalmente el dispositivo con la función de huella digital en el modo controlador.

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

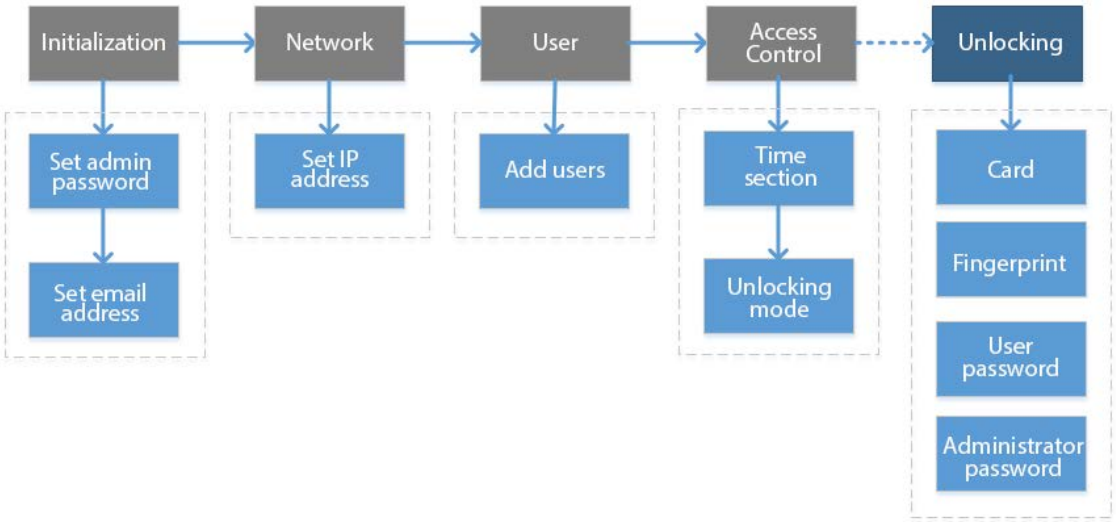
Figure 1-3 Diagrama de red



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

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

2.3 Inicialización

Para el primer uso o después de restaurar los valores predeterminados de fábrica, debe configurar una contraseña y asociar su dirección de correo electrónico a la cuenta de administrador. También debe configurar la zona horaria del dispositivo. Puede utilizar 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 sean espacios 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 las indicaciones sobre la fortaleza 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 durante 30 segundos.
- El dispositivo apaga la pantalla si permanece en la página de espera durante 30 segundos.
- La pantalla del manual del usuario es sólo para referencia.

Figure 2-3 Pantalla de espera

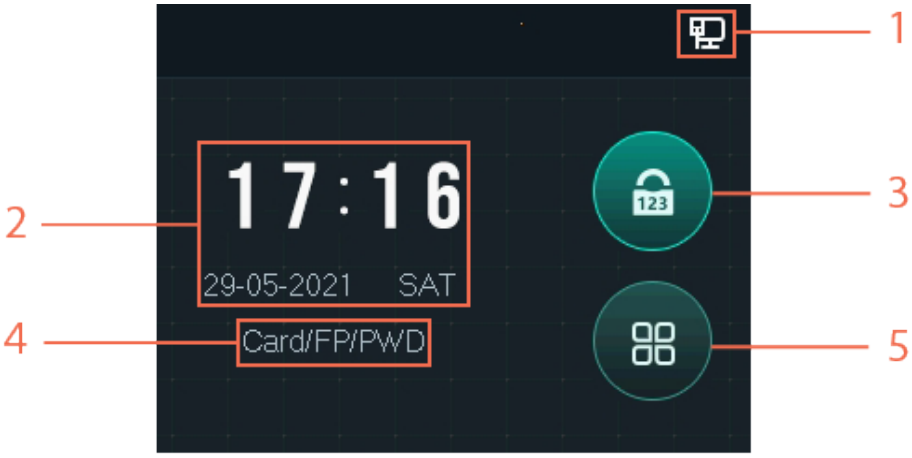


Tabla 2-2 Descripción de la página de espera

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

No.	Artículo	Descripción
3	Desbloquear el puerta con contraseña	Introduzca el ID de usuario y la contraseña, o la contraseña de administrador (para más detalles, consulte "2.6.4 Contraseña de administrador") para desbloquear la puerta.
4	Desbloqueo métodos	Muestra los métodos de desbloqueo que ha configurado.
5	Menú principal	Grifo para ingresar al menú principal. Solo administradores y usuarios con Los usuarios con permisos de administrador pueden iniciar sesión en el menú principal. Consulte "2.5 Iniciar 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 con diferentes permisos y cambiar el modo de desbloqueo.

Sólo el administrador y los usuarios admin pueden iniciar sesión en el menú principal.

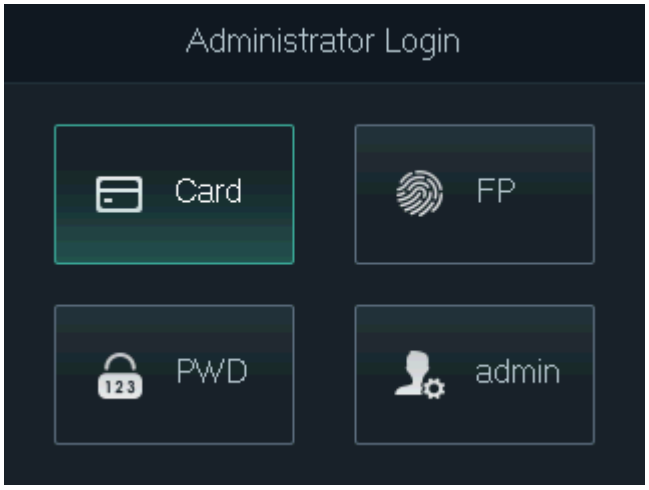
Step 1 En la pantalla de espera, toque .

Los métodos de verificación varían según el tipo de dispositivo.

Step 2 Inicie sesión en el menú principal.

- Inicie sesión como usuario con permisos 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



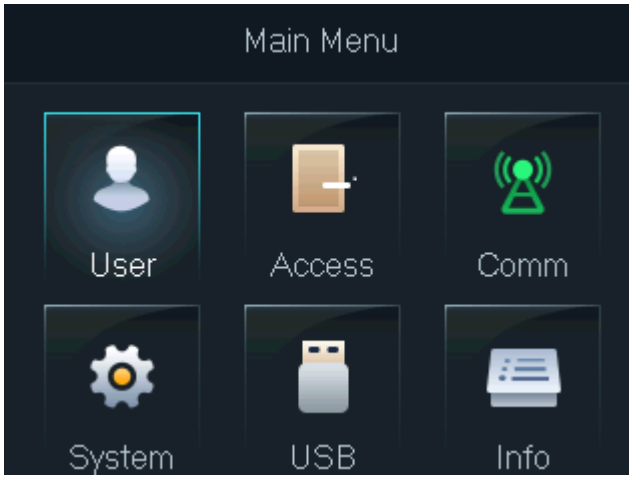
Step 3 En el menú principal, toque∧/∨para navegar por la página y luego toque**DE ACUERDO**para configurar parámetros del Dispositivo.

Utilice los accesos directos para configurar los 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 de acceso autónomo con identificación, si está conectado con un lector de tarjetas de identificación externo, La distancia entre el Access Standalone y el lector de tarjetas debe ser mayor a 10 cm. De lo contrario, El lector de tarjetas podría funcionar mal porque está demasiado cerca del Access Standalone.

2.6.2 Huella dactilar

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 Seleccionar**Personas con discapacidad**y luego toque**DE**

Step 3 **ACUERDO**. Introduzca el ID de usuario y la contraseña.

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

Step 4 Seleccionar**DE ACUERDO**y luego toque**DE ACUERDO**.

El sistema le 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 con solo ingresar la contraseña de administrador. Use 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 utilizar la contraseña de administrador para acceder a la puerta, debe habilitar la función. Consulte "2.7.3 "Configuración de contraseña de administrador".

Step 1 Seleccionar en la pantalla de espera.

Step 2 Seleccionar**Contraseña de administrador**y luego toque**DE**

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

Step 4 Seleccione**DE ACUERDO**y luego toque**DE ACUERDO**La puerta está abierta.

2.7 Gestión de usuarios

Puede agregar nuevos usuarios, ver la lista de usuarios o la lista de administradores en el**Usuario**pantalla.

2.7.1 Agregar nuevo usuario

Step 1 Seleccionar en la pantalla de espera y luego toque**DE ACUERDO**.

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

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

Figure 2-6 Agregar un nuevo usuario

Step 3 Configurar los parámetros.

Tabla 2-3 Descripción de los parámetros del usuario

Parámetro	Descripción
IDENTIFICACIÓN	Cada ID de usuario es único. Puede tener 18 caracteres, ya sean números, letras o una combinación de ambos.
Nombre	Ingrese el nombre (un máximo de 32 caracteres, incluidos números, símbolos y letras).
Huella dactilar	Cada usuario puede agregar hasta 3 huellas dactilares. Siga las instrucciones en pantalla y las indicaciones de voz para agregar huellas dactilares. Puede habilitar la función de alarma de coacción en cada huella dactilar. Una vez habilitada la función de alarma de coacción, se activará una alarma si la puerta se desbloquea con la huella dactilar de coacción.  - No recomendamos establecer la primera huella dactilar como huella dactilar de coacción. - Sólo algunos modelos admiten la función de huella digital.
Tarjeta	Puede registrar cinco tarjetas para cada usuario. En la página de registro de tarjetas, deslice su tarjeta por el lector de tarjetas y 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 puerta se desbloquea con la tarjeta de coacción.
Personas con discapacidad	Introduzca la contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos. La contraseña de coacción se suma en 1 al último dígito de la contraseña de desbloqueo. Por ejemplo, si la contraseña de usuario es 12345, la contraseña de coacción será 12346; si la contraseña de usuario es 789, la contraseña de coacción será 780. Se activará una alarma de coacción cuando se utilice una contraseña de coacción para desbloquear la puerta.
Permiso	Puede seleccionar un permiso de usuario para el nuevo usuario. ● Los usuarios normales solo tienen permiso para desbloquear la puerta. 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 durante los días festivos programados. El valor predeterminado es 255, lo que significa que no se ha configurado ningún plan de días festivos.
Fecha válida	Define un período durante el cual el usuario tiene control de acceso a la puerta.

Parámetro	Descripción
Tipo de usuario	• **General**:Los usuarios generales pueden desbloquear la puerta normalmente. • **Lista de bloqueo**:Cuando los usuarios de la lista de bloqueo desbloquean la puerta, el personal de servicio recibe una notificación. • **Invitado**:Los huéspedes pueden desbloquear la puerta dentro de un período definido o una cierta cantidad de veces. Una vez que expire el período definido o se agoten los tiempos de desbloqueo, no podrán desbloquear la puerta. • **Patrulla**Los usuarios en libertad condicional pueden tener un seguimiento de su asistencia, pero no tienen permisos de desbloqueo. • **personaje**: Cuando un usuario VIP desbloquea la puerta, el personal de servicio recibirá una notificación. El usuario VIP no está restringido por los modos de desbloqueo, como**Multi-tarjeta**y **Sección de tiempo**. • **Otros**:Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más. • **Usuario personalizado 1/2**:Lo mismo que**General**.

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

Step 5 **ACUERDO**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 de los usuarios.

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

Figure 2-7 Lista de usuarios

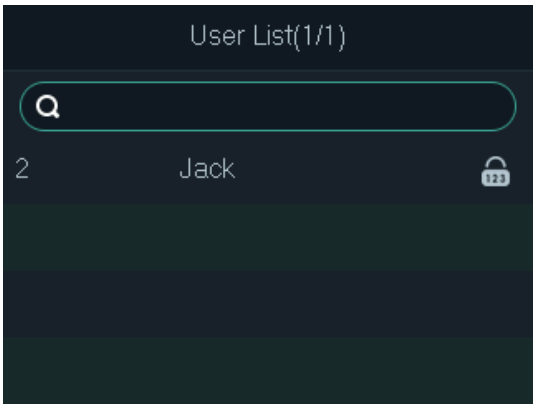
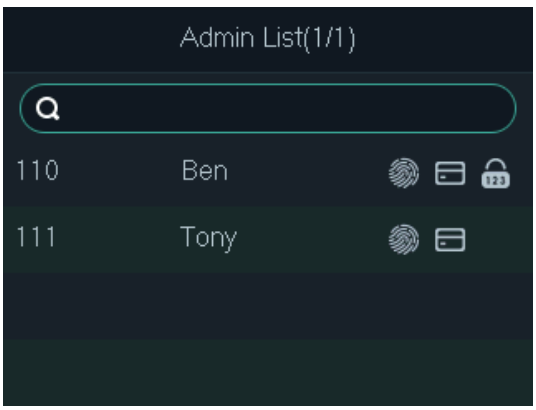


Figure 2-8 Lista de administradores



- Método de desbloqueo

- ◇ :Huella dactilar.
- ◇ : Tarjeta.
- ◇ : Contraseña.

Edición de información del usuario

Step 1 Seleccione el usuario y toque**DE**
Step 2 **ACUERDO**Editar la información del
Step 3 usuario. Pulsa**Esc**.
Step 4 Grifo**DE ACUERDO**para guardar los cambios.

Buscando usuarios

Step 1 Seleccionar y toque**DE ACUERDO**.
Step 2 Ingrese el ID del usuario, deslice una tarjeta o presione una huella digital para buscar al usuario.

Eliminar usuarios

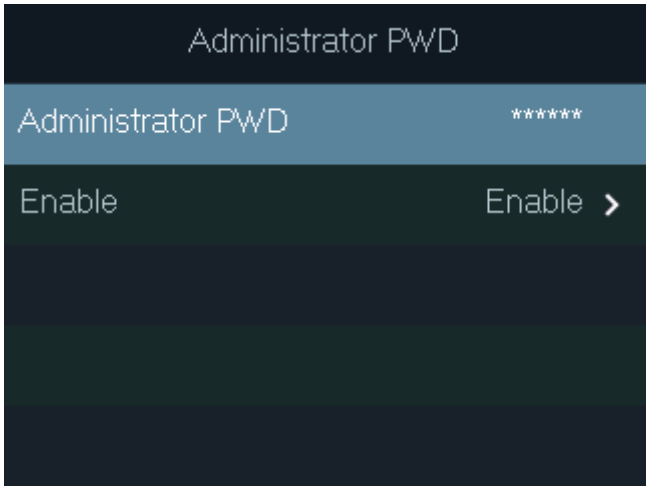
Seleccione el usuario, toque**DE ACUERDO**y luego seleccione para eliminar el usuario.

2.7.3 Configuración de la contraseña del administrador

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

Step 1 En el menú principal, seleccione**Usuario > Administrador PWD**Ingrese
Step 2 la contraseña de administrador y luego toque**DE ACUERDO**.

Figure 2-9 Contraseña de administrador

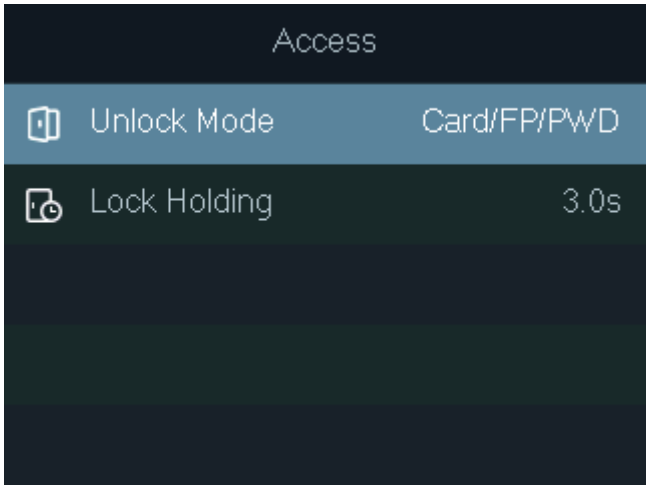


Step 3 Seleccionar**Permitir**y luego toque**DE ACUERDO**para habilitar la función.

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 según el tipo de dispositivo.

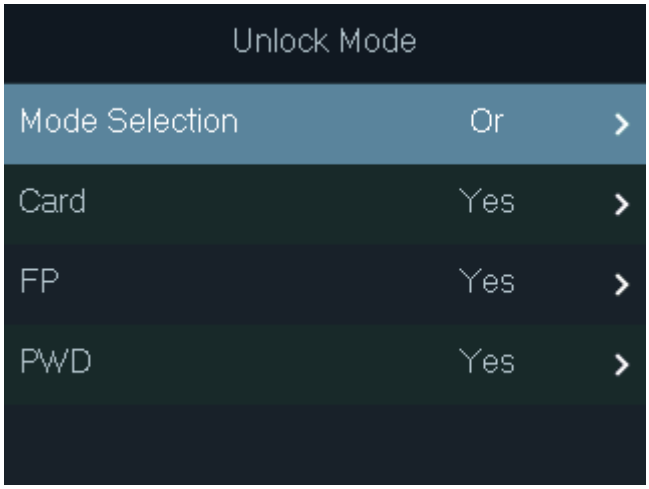
Utilice tarjeta, huella dactilar, contraseña o cualquiera de sus combinaciones para desbloquear la puerta.

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

Step 2 **DE ACUERDO**para configurar las combinaciones de desbloqueo.

- **Y**:Debes 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**DE ACUERDO**para guardar los cambios.

2.8.2 Configuración del tiempo de retención del bloqueo

La puerta permanecerá desbloqueada durante el período definido.

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

Step 2 Grifo**DE ACUERDO**y luego ingrese 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

Establezca la dirección IP del dispositivo para conectarlo a la red. Luego, puede iniciar sesión en el portal web para configurar el dispositivo y agregarlo a SmartPSS AC.

Step 1 En el menú principal, seleccione**Comm > Dirección IP**y luego toque**DE ACUERDO**.

Step 2 Seleccionar**Dirección IP**y toque**DE ACUERDO**Para configurar parámetros.

Figure 2-12 Configurar IP

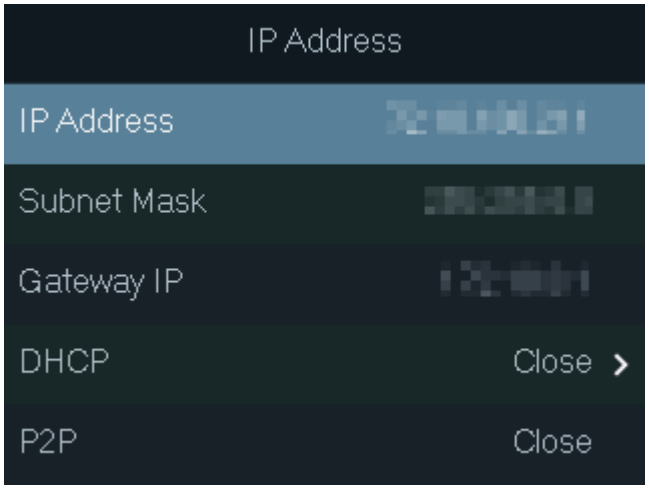


Tabla 2-4 Descripción de los parámetros de red

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

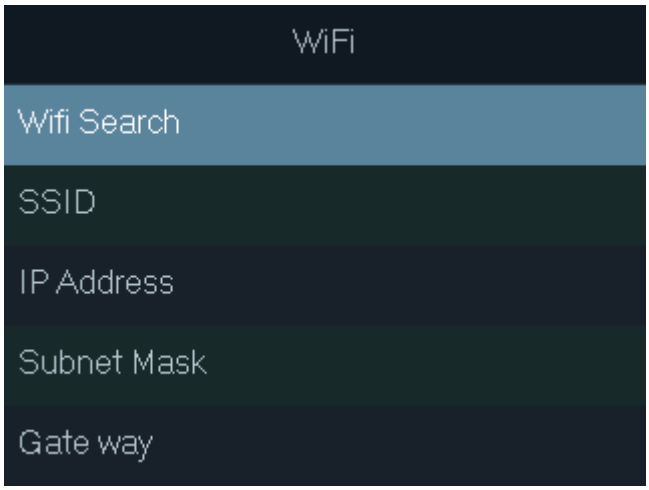
2.9.2 Configuración de Wi-Fi

Conecte el dispositivo a una red inalámbrica.

Sólo algunos modelos admiten Wi-Fi.

Step 1 En el menú principal, seleccione**Comm > Wi-Fi**y luego toque**DE ACUERDO**.

Figure 2-13 Wifi



Step 2 Seleccionar**Búsqueda de Wifi**y luego toque**DE ACUERDO**.

Step 3 Seleccionar**Wi-Fi**y luego toque**DE ACUERDO**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**DE ACUERDO**y luego 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**DE ACUERDO**.

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

Figure 2-14 Wiegand

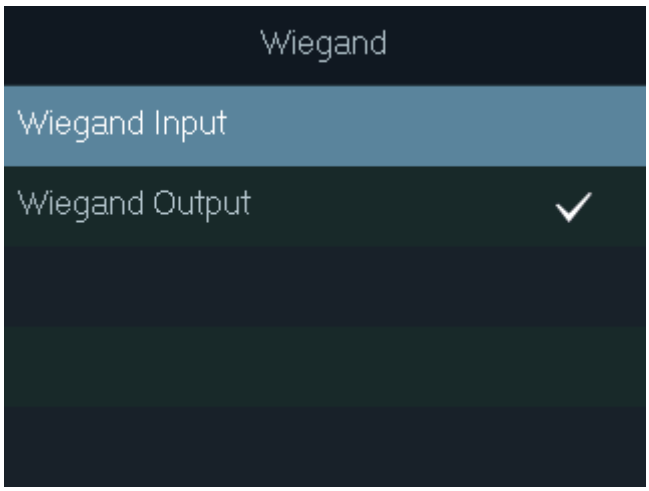


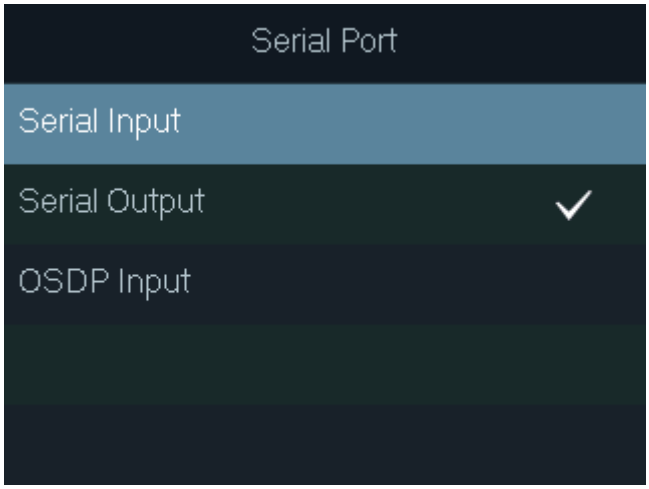
Tabla 2-5 Descripción de los parámetros Wiegand

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 el ID del usuario que pasa una tarjeta. ● **Tarjeta Nro.**:Emite el número de tarjeta que se utiliza.

2.9.4 Configuración del puerto serie

En el menú principal, seleccione**Comm > Puerto serial**y luego toque**DE ACUERDO**.

Figure 2-15 Configuración del puerto serie



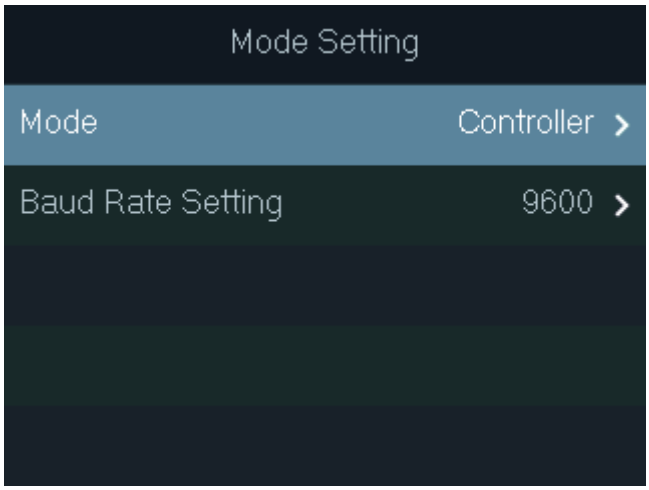
- Seleccionar**Entrada en serie**Cuando el dispositivo se conecta a un lector de tarjetas, el lector de tarjetas enviará el número de tarjeta al dispositivo o SmartPSS AC.
- Seleccionar**Salida en serie**Cuando el dispositivo funciona como lector de tarjetas, el dispositivo enviará el número de tarjeta al controlador y este controlará el acceso a la puerta.
  - ◇ **ID de usuario**:Emite el ID del usuario que pasa una tarjeta.
  - ◇ **Tarjeta Nro.**:Emite el número de tarjeta que se utiliza.
- Seleccionar**Entrada OSDP**Cuando el dispositivo se conecta a 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 controlador o lector de tarjetas. En el

menú principal, seleccione**Comm > 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 este último envía la información de la tarjeta al dispositivo o al 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 lector de tarjetas.
    - Para el modo de lector de tarjetas, consulte el método de cableado de un lector de tarjetas. Puede conectar El dispositivo se conecta a un controlador externo u otro acceso independiente a través del protocolo RS485. No es compatible con Wiegand.
    - Para el modo de 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 antimanipulación, DOOR1_COM y DOOR1_NC deben conectarse a los cables CASE y GND del controlador externo.

- Configuración de la velocidad en 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. Le recomendamos no modificar otras configuraciones en la web portal y en el dispositivo.
    - Para el modo controlador, debe configurar manualmente la misma velocidad en baudios que la externa. dispositivo.

2.10 Sistema

2.10.1 Tiempo

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

Step 1 En el menú principal, seleccione**Sistema > Tiempo**y luego toque**DE ACUERDO**

Step 2 Seleccione un parámetro y luego toque**DE ACUERDO**.

Figure 2-17 Ajustes de hora

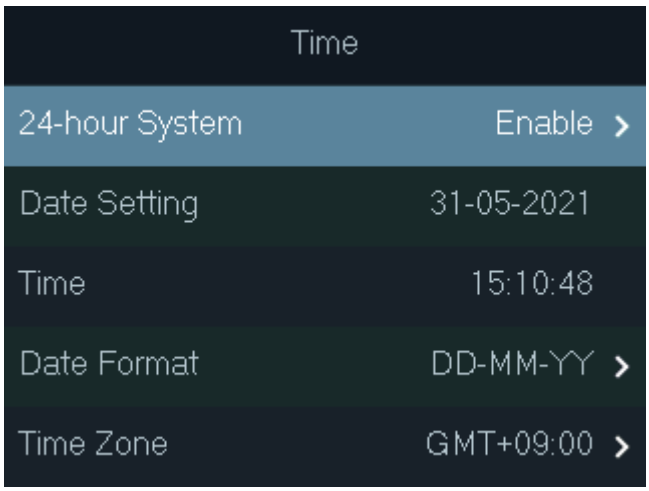


Tabla 2-6 Descripción de los parámetros de tiempo

Parámetro	Descripción
Sistema de 24 horas	Habilitar el formato de 24 horas.
Ajuste de fecha	Establecer la fecha.
Tiempo	Establezca la hora.
Formato de fecha	Seleccione un formato de fecha.
Huso horario	Seleccione una zona horaria.

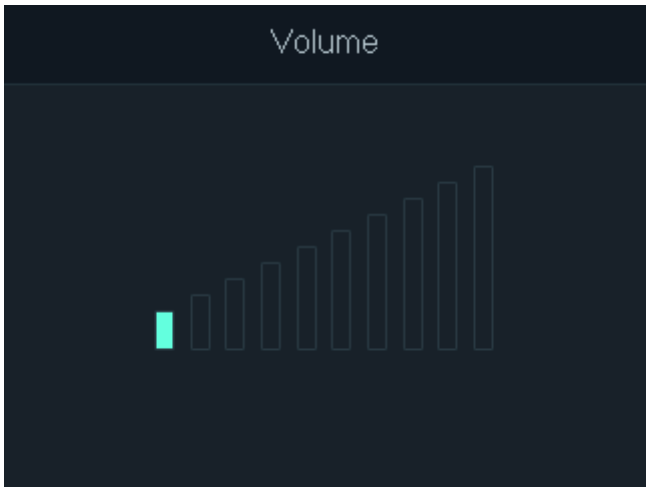
2.10.2 Volume

Ajuste el volumen del mensaje de voz.

Step 1 En el menú principal, seleccione**Sistema > Volumen**y luego toque**DE ACUERDO**

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

Figure 2-18 Ajustar el volumen



2.10.3 Restauración a la configuración predeterminada

⚠

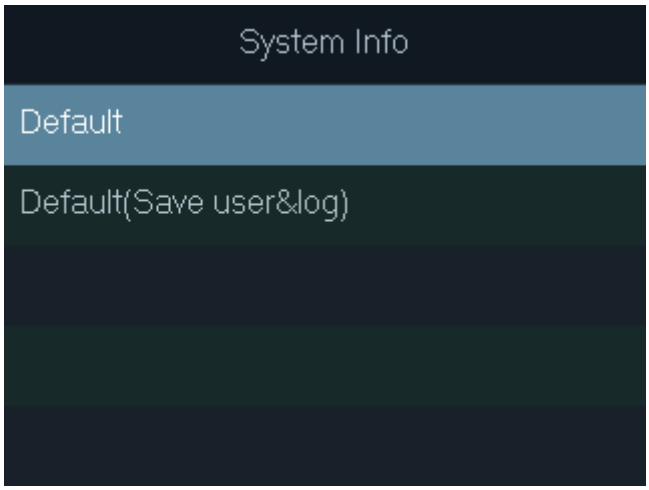
Se perderán los datos si restaura el dispositivo a los valores predeterminados de fábrica. Tenga en cuenta lo siguiente.

Step 1 En el menú principal, seleccione**Sistema > Restaurar fábrica**y luego toque**DE ACUERDO**Seleccione

Step 2 una opción y luego toque**DE ACUERDO**.

- **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 configuración predeterminada



2.10.4 Reinicio del dispositivo

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

2.11 Gestión USB

⚠

- Asegúrese de que haya una unidad flash USB insertada en el dispositivo antes de exportar 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 USB. Conducir primero.

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

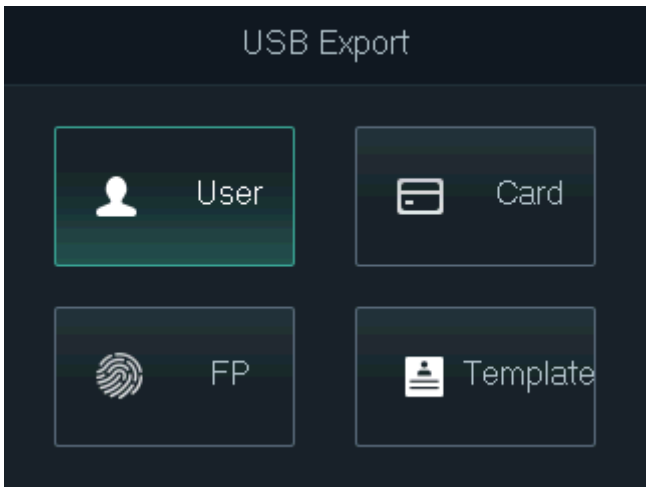
2.11.1 Exportación a USB

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

Step 1 En el menú principal, seleccione**USB > Exportación USB**y luego toque**DE ACUERDO**

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

Figure 2-20 Exportar datos a la unidad USB



Step 3 Grifo**DE ACUERDO**.

Los datos seleccionados se exportan a la unidad flash USB.

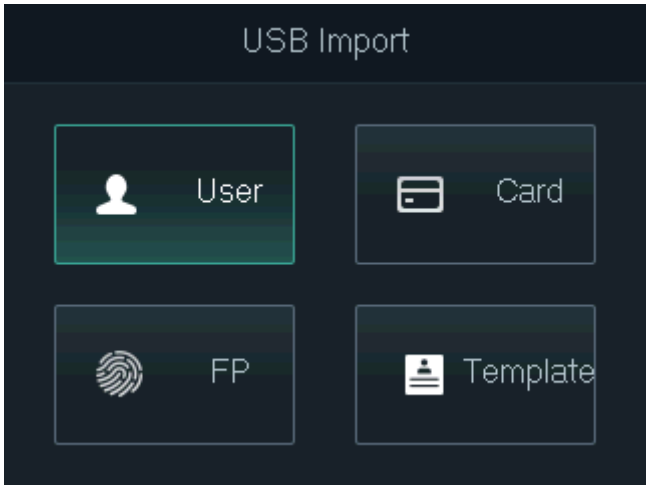
2.11.2 Importación desde USB

Puede importar datos desde USB al dispositivo.

Step 1 En el menú principal, seleccione**USB > Importación USB**y luego toque**DE ACUERDO**

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

Figure 2-21 Importar datos desde la unidad flash USB



Step 3 Grifo**DE ACUERDO**.

Los datos seleccionados se importan al dispositivo.

2.11.3 Actualización del sistema

Puede utilizar 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**DE ACUERDO**.

El dispositivo se reiniciará cuando se complete la actualización.

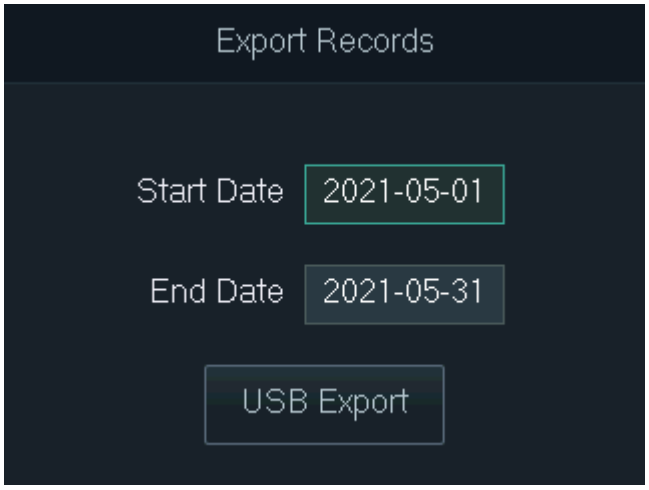
2.11.4 Exportación de registros de desbloqueo

Exportar registros de desbloqueo a una unidad flash USB.

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

Step 2 Seleccione la hora.

Figure 2-22 Exportar registros de desbloqueo



Step 3 Seleccionar**Exportación USB**y luego toque**DE ACUERDO**.

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

2.11.5 Exportación/importación de información del usuario

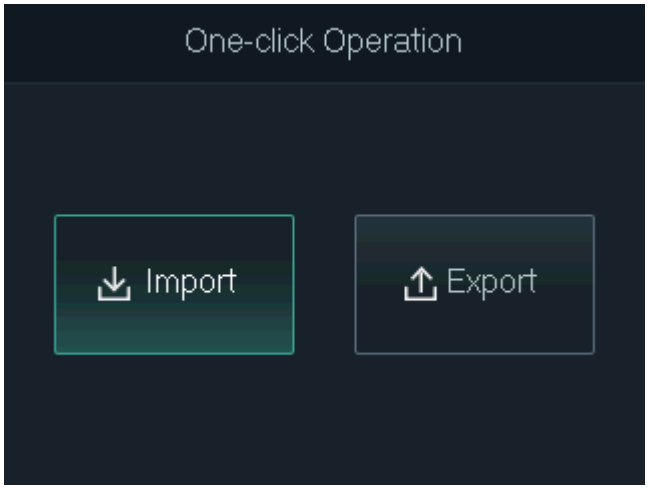
Puede utilizar la función de un clic para importar o exportar información del usuario, incluidas tarjetas y huellas dactilares.

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

- **Importar**:Importa información del usuario, incluidas tarjetas y huellas dactilares.
- **Exportar**:Exportar información del usuario, incluidas tarjetas y huellas dactilares.

Step 2 Seleccionar**Importar**o**Exportar**y luego toque**DE ACUERDO**.

Figure 2-23 Operación con un solo clic



2.12 Información del sistema

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

- **Capacidad de datos**:Muestra la cantidad 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 La Web en la computadora

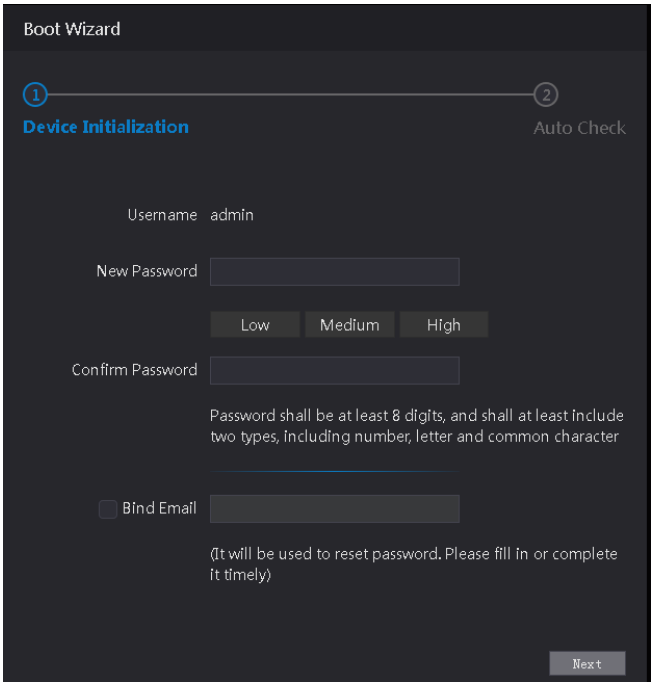
3.1.1 Inicialización

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

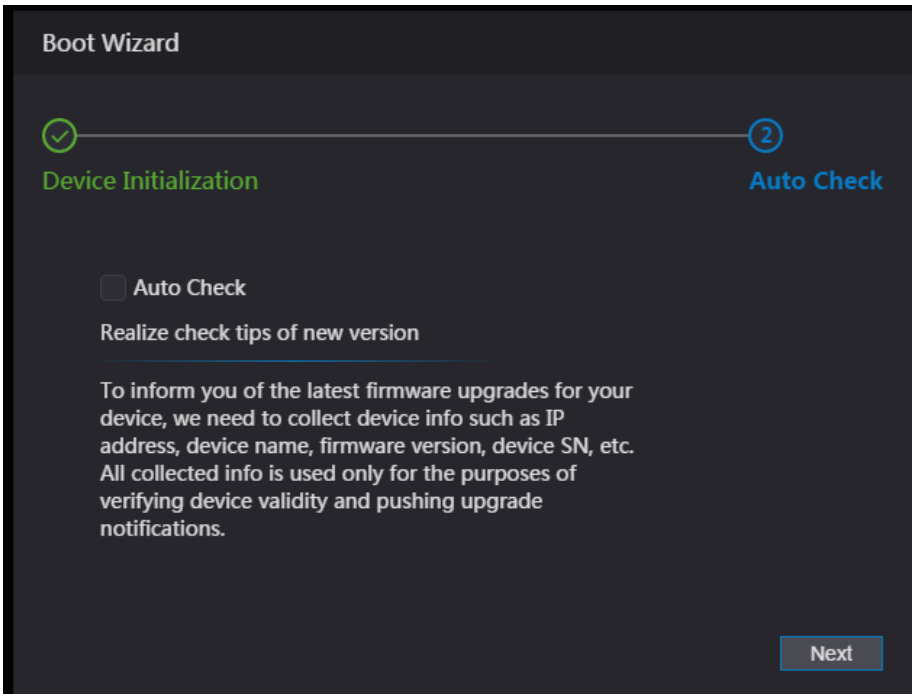


Step 2 Ingrese la nueva contraseña, confirme la contraseña, habilite**Vincular correo electrónico**, ingrese una dirección de correo electrónico y luego haga clic en**Próximo**.

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

Step 3 Hacer clic**Próximo**.

Figure 3-2 Comprobación automática

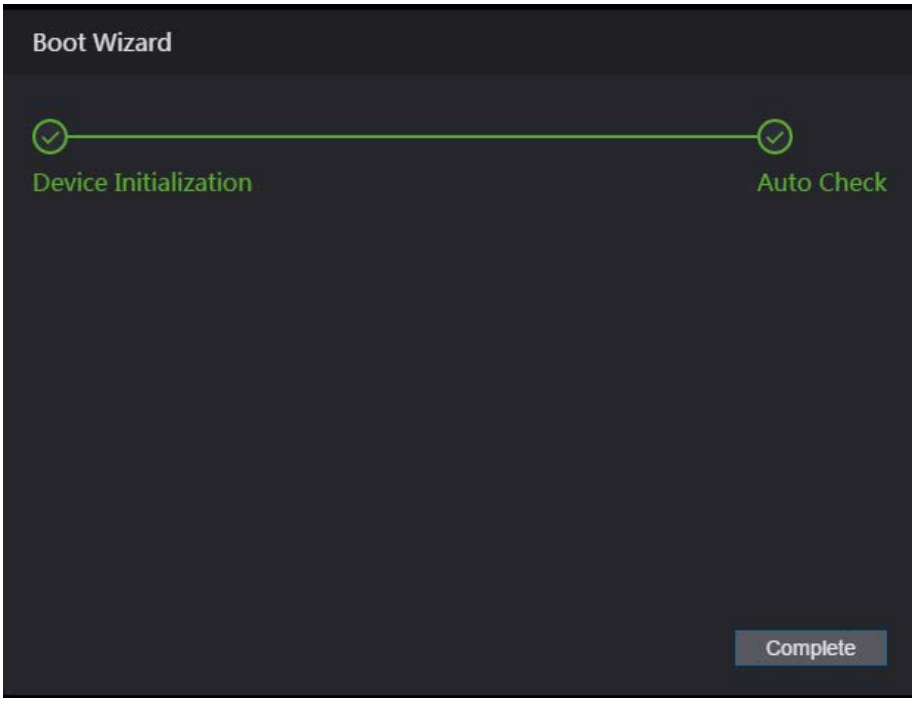


Step 4 (Opcional) Seleccionar**Comprobación automática**.

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

Step 5 Hacer clic**Próximo**.

Figure 3-3 Finalizar la inicialización



Step 6 Hacer clic**Completo**.

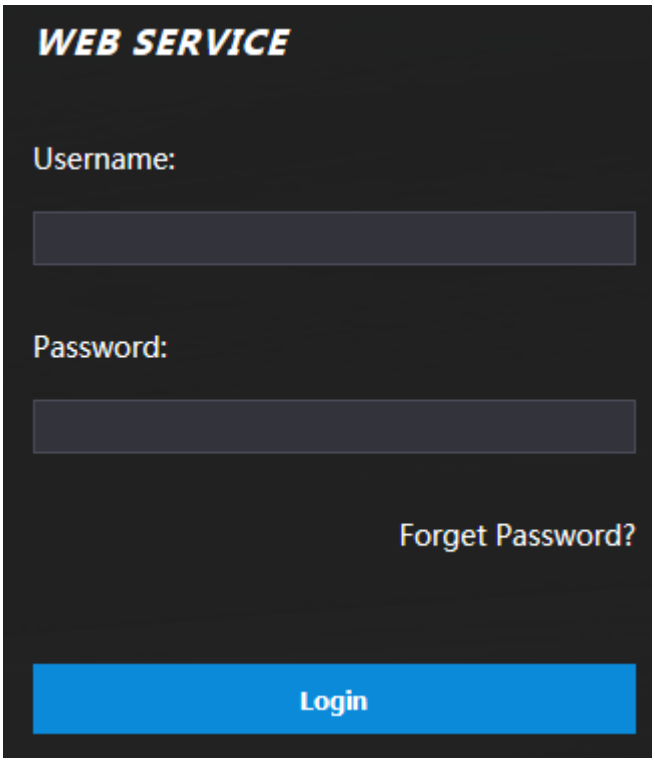
3.1.2 Iniciar sesión

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

Tecla Enter.

- 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 usted establece durante inicialización. Le recomendamos que cambie la contraseña de administrador periódicamente para aumentar la seguridad.
- Si olvidó la contraseña de administrador, haga clic en**¿Olvidaste tu contraseña?**para restablecerlo. Ver "3.3 Restablecer la contraseña ".

Step 3 Hacer clic**Acceso**.

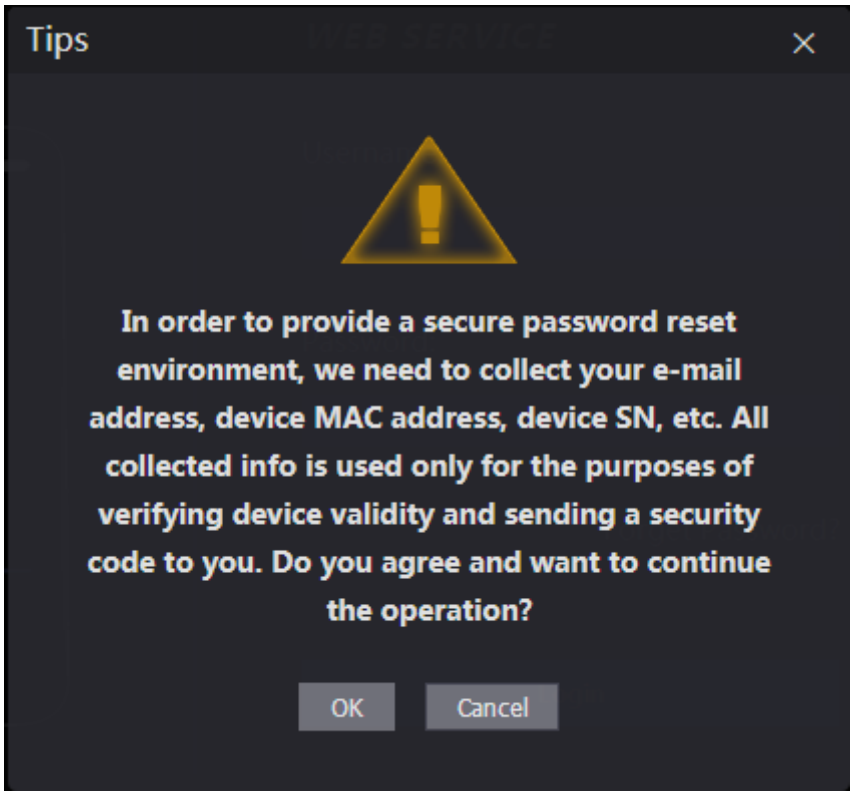
3.1.3 Restablecimiento de la contraseña

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.**DE ACUERDO**.

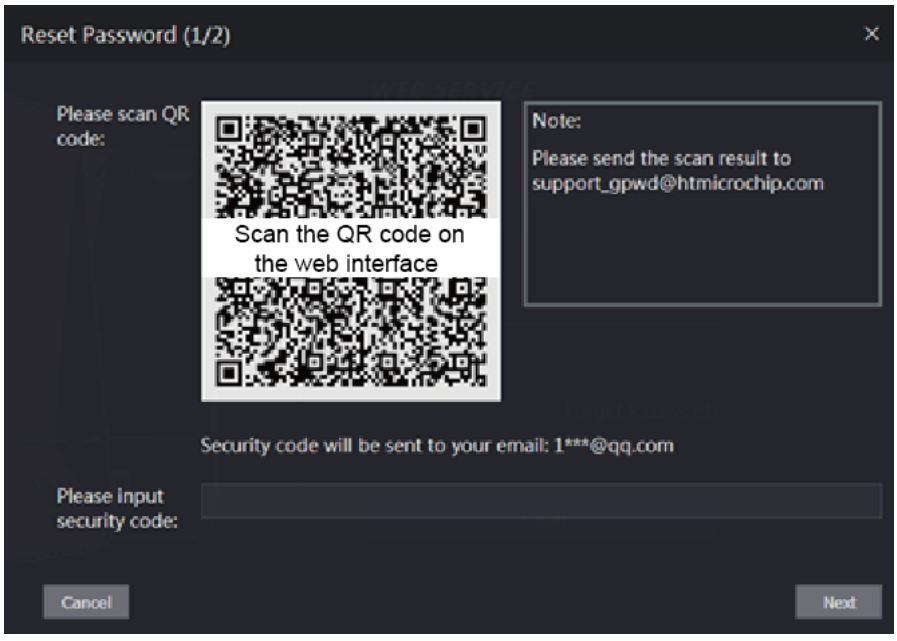
Figure 3-5 Mensaje de reinicio



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

- Se generarán un máximo de dos códigos de seguridad al escanear el mismo código QR. Si Los códigos de seguridad dejan de ser válidos, actualice el código QR y escanéelo nuevamente.
- 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 en un inválido. Si se ingresan códigos de seguridad incorrectos cinco veces consecutivas, el administrador Se congelará durante cinco minutos.

Figure 3-6 Restablecer contraseña



Step 4 Introduce el código de seguridad que has recibido. Haz

Step 5 clic**Próximo**.

Step 6 Restablecer y confirmar la nueva contraseña.

La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluidos ' " ; : &). Establezca una contraseña de alta seguridad siguiendo las indicaciones sobre la fortaleza de la contraseña.

Step 7 Hacer clic**DE ACUERDO**para completar el reinicio.

3.1.4 Configuración de parámetros de la puerta

Configurar los parámetros de control de acceso.

Step 1 Inicie sesión en la página web.

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

Figure 3-7 Figura 3-9 Parámetros de la puerta

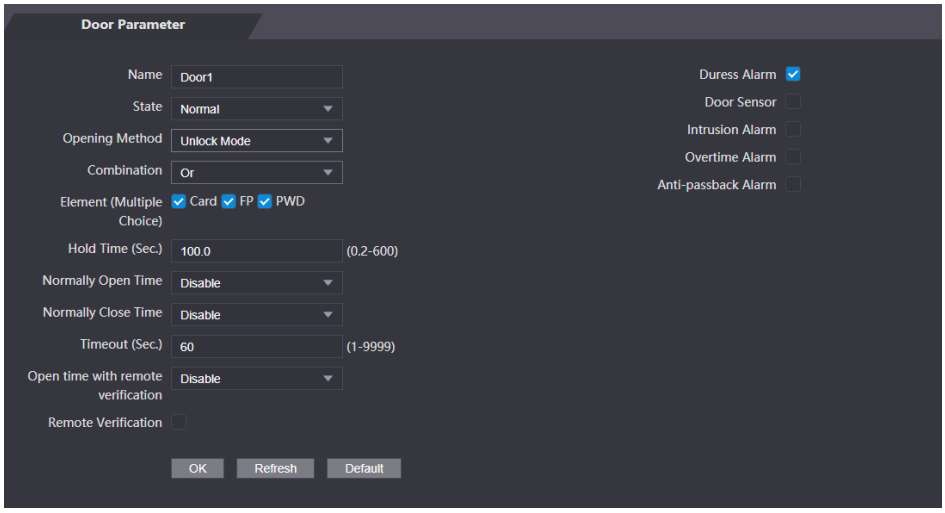


Tabla 3-1 Descripción de los parámetros de la puerta

Parámetro	Descripción
Nombre	Introduzca un nombre para la puerta que controla el dispositivo.
Estado	Seleccionar**CAROLINA DEL NORTE**para normalmente cerrado, o**NO**para apertura normal. Si se selecciona cualquiera de los dos, el método de apertura definido no será efectivo.
Apertura Método	● **Sección de tiempo:**Establecer diferentes métodos de desbloqueo para períodos definidos. **Multi-tarjeta** ● :El usuario puede desbloquear la puerta cuando varios usuarios y varios grupos de usuarios conceden acceso. ● **Modo de desbloqueo**:establecer combinaciones de desbloqueo.
Tiempo de retención (seg.)	Duración del desbloqueo. La puerta se volverá a bloquear después de transcurrido el tiempo establecido. Varía entre 0,2 y 600 segundos.
Normalmente abierto Tiempo	La puerta permanece abierta o cerrada durante el período definido.
Normalmente cerrado Tiempo	

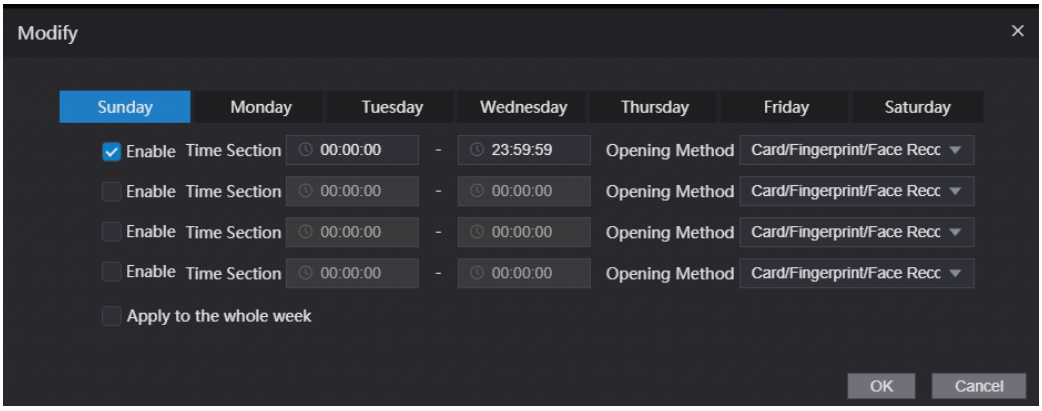
Parámetro	Descripción
Tiempo de espera (seg.)	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante un tiempo superior a este valor.
Remoto Verificación	Establezca el período de apertura de la puerta para verificación remota. Para obtener más información, consulte la sección "3.6.1 Configuración del tiempo". Cuando se autoriza la apertura de una puerta en el dispositivo, es necesario confirmarla en la plataforma antes de poder abrirla.
Alarma de coacción	Se activará una alarma cuando se utilice una tarjeta de coacción o una contraseña de coacción para desbloquear la puerta.
Sensor de puerta	Las alarmas de intrusión y de horas extras se pueden activar solo después**Sensor de puerta**está habilitado.
Alarma de intrusión	Cuando**Sensor de puerta**está habilitado, se activará una alarma de intrusión si la puerta se abre de forma anormal.
Alarma de horas extras	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante más tiempo del indicado.**Tiempo de espera (seg.)**, que varía de 1 a 9999 segundos.
Anti-passback Alarma	Si está habilitado, los usuarios deben verificar sus identidades tanto para entrar como para salir; de lo contrario, se activará una alarma. ● Si una persona entra con verificación y sale sin verificación, se activará una alarma cuando intente desbloquear nuevamente y se le negará el acceso al mismo tiempo. ● Si una persona entra sin verificación y sale con verificación, se activará una alarma cuando intente desbloquear nuevamente y se le negará el acceso al mismo tiempo.

Step 3 Configurar el método de desbloqueo.

- Sección de tiempo

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

Figure 3-8 Parámetro de sección de tiempo



2) Configure la hora y el método de apertura de una sección horaria. Puede configurar hasta cuatro secciones horarias para un solo día.

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

4) Haga clic**DE ACUERDO**.

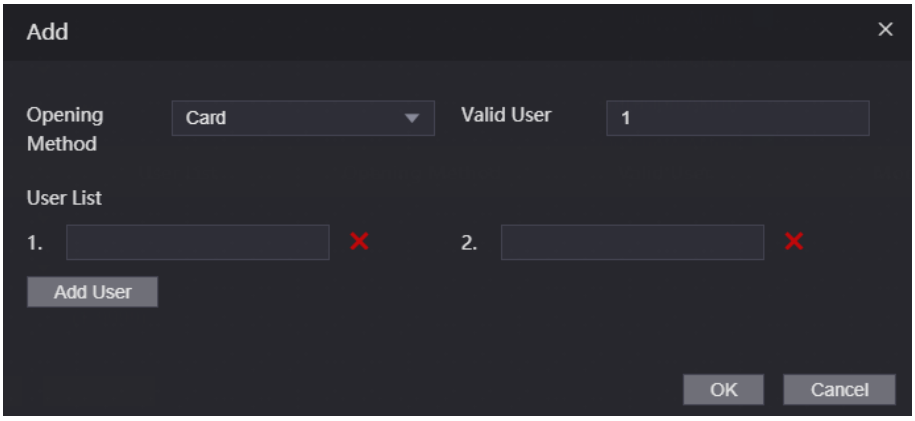
- Multi-tarjeta

1) En el**Método de apertura**lista, seleccionar**Multi-tarjeta**y luego haga clic en .

2) Haga clic**Agregar**.

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

Figure 3-9 Parámetros de múltiples tarjetas



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

- No se pueden agregar usuarios VIP, de patrulla y de lista de bloqueo.
- Todos los usuarios de los diferentes grupos deben verificar sus identidades en el orden del grupo. Desbloquea la puerta.

- Modo de desbloqueo

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

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

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

3) En el**Elemento**En la lista, seleccione el método de

Step 4 desbloqueo. Configure otros parámetros.

Step 5 Hacer clic**DE ACUERDO**.

3.1.5 Vinculación de alarmas

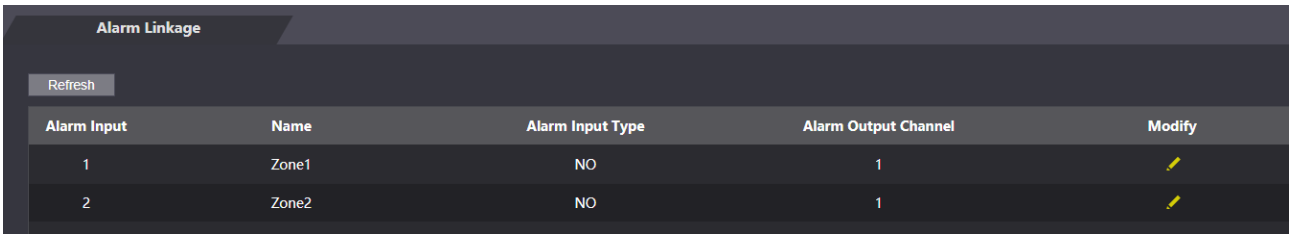
3.1.5.1 Configuración de la vinculación de alarmas

Se pueden conectar dispositivos de entrada de alarma al dispositivo y se pueden modificar los parámetros de vinculación de alarma.

Step 1 Inicie sesión en la página web.

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

Figure 3-10 Vinculación de alarma



Step 3 Hacer clic para configurar la vinculación de alarmas.

Figure 3-11 Modificar parámetros de vinculación

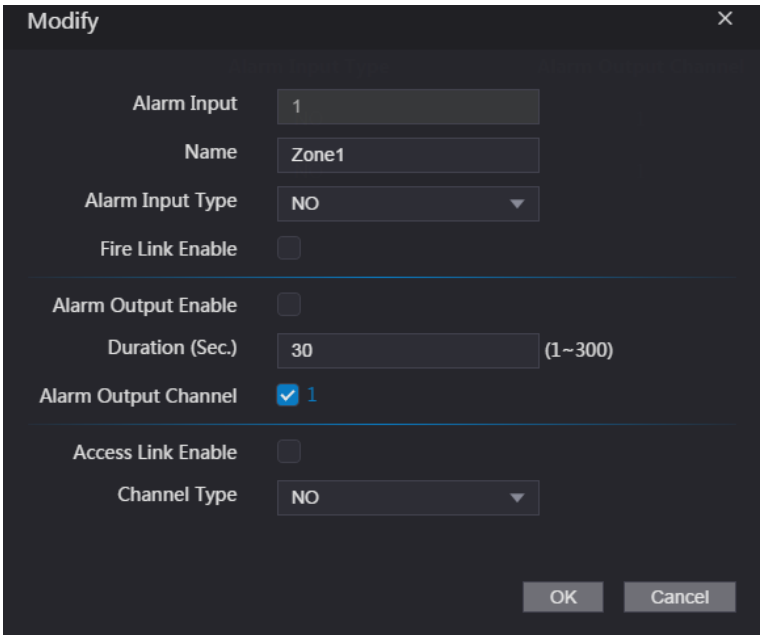


Tabla 3-2 Descripción de los parámetros de vinculación de alarmas

Parámetro	Descripción
Entrada de alarma	No puedes modificar el valor. Mantenlo 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 la conexión contra incendios está habilitada, el dispositivo generará alarmas contra incendios 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 están en NO de manera predeterminada.
Habilitar salida de alarma	Si la salida de alarma está habilitada, el relé puede generar mensajes de alarma.
Duración (seg.)	Duración de la alarma. Varía entre 1 s y 300 s.
Canal de salida de alarma	El dispositivo tiene un solo canal de salida. Seleccione el canal de salida según 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**DE ACUERDO**para guardar los cambios.

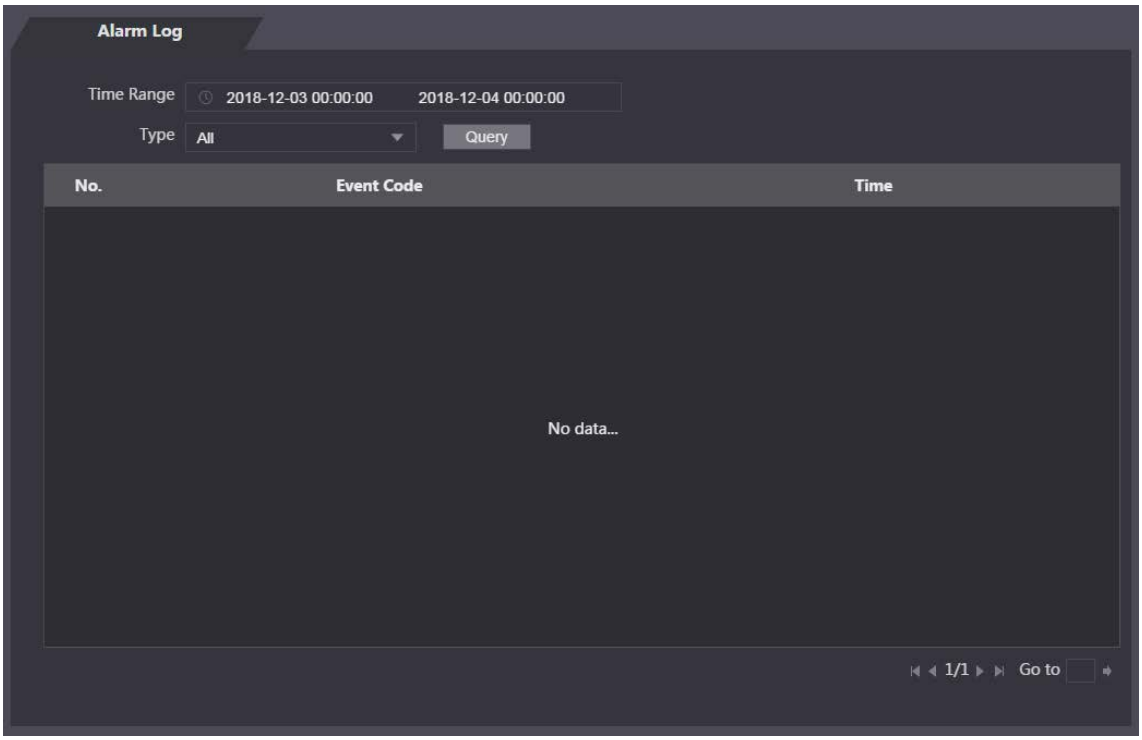
Las configuraciones en la web se sincronizarán con el cliente de software si el Dispositivo está añadido al cliente.

3.1.5.2 Registro de alarmas

Step 1 Inicie sesión en la página web.

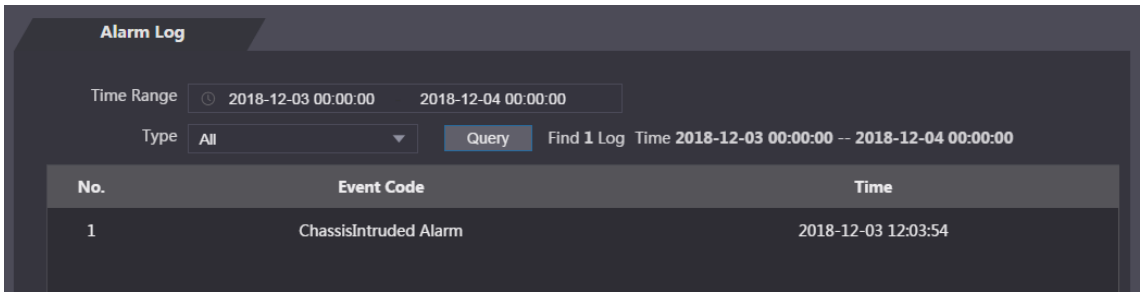
Step 2 Seleccionar**Enlace de alarma**>**Registro de alarmas**.

Figure 3-12 Registro de alarmas



Step 3 Seleccione un rango de tiempo y un tipo de alarma y luego 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 podrá definir cuándo un usuario tiene permisos para desbloquear puertas.

3.1.6.1 Sección de configuración de tiempo

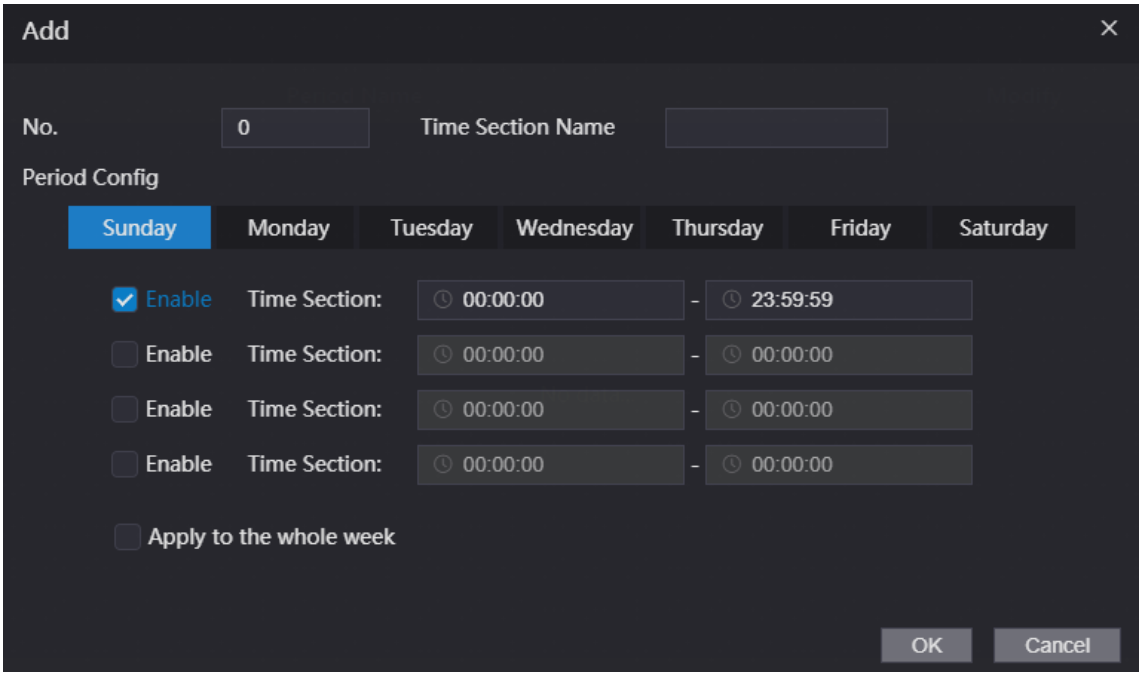
Puede configurar hasta 128 grupos (del n.º 0 al n.º 127) de secciones horarias. En cada grupo, debe configurar los horarios de acceso a las puertas para una semana completa. Un usuario solo puede desbloquear la puerta durante el horario programado.

Step 1 Inicie sesión en la página web.

Step 2 Seleccionar**Sección de tiempo**>**Sección de tiempo**Haga clic en

Step 3 **Agregar**.

Figure 3-14 Parámetros de la sección de tiempo



Step 4 Introduzca el número y el nombre para la sección de tiempo.

- **No.**:Ingrese un número de sección. Varía entre 0 y 127.
- **Nombre de la sección de tiempo**: Ingrese un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (que pueden incluir números, caracteres especiales y caracteres en inglés).

Step 5 Configurar secciones de tiempo para cada día.

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

Step 6 (Opcional) Haga clic en**Aplicar a toda la semana**Para copiar la configuración al resto de días, haga clic en**DE**

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

3.1.6.2 Configuración del grupo de vacaciones

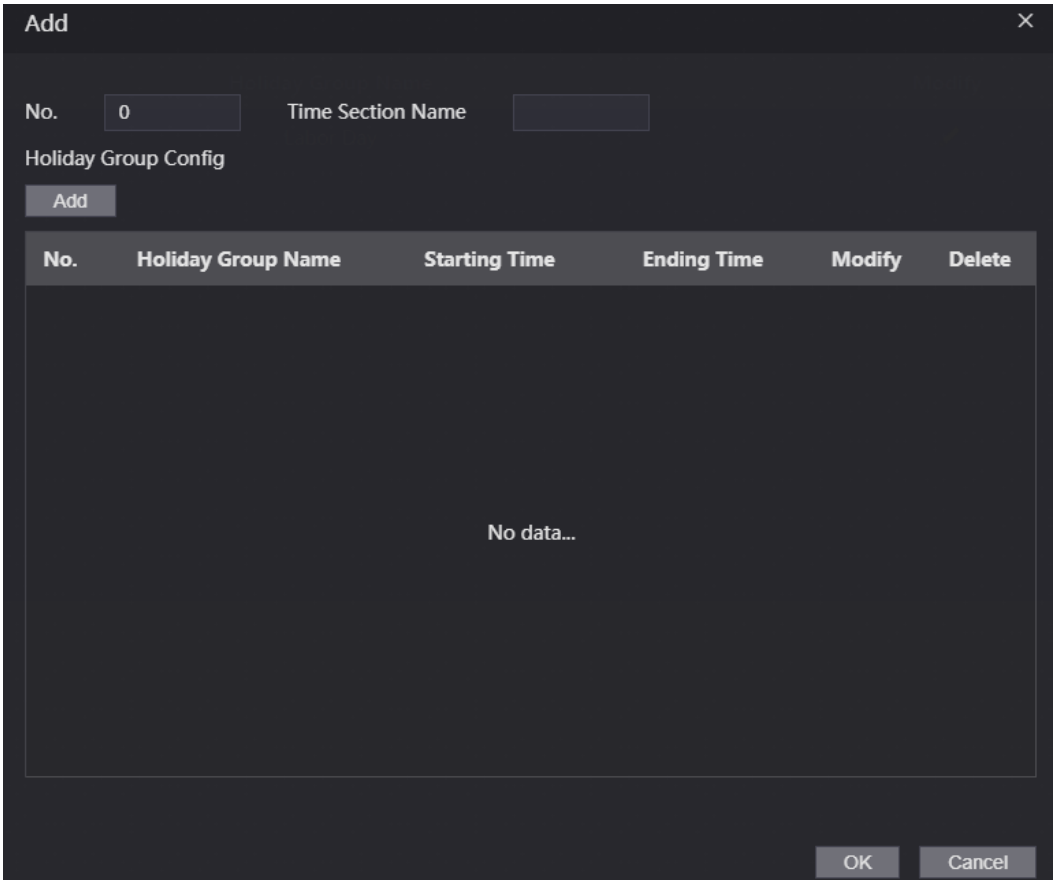
Establezca franjas horarias para diferentes grupos de vacaciones. Puede configurar hasta 128 grupos de vacaciones (desde el n.º 0 hasta el n.º 127) y hasta 16 franjas horarias para un solo grupo de vacaciones. Los usuarios pueden desbloquear puertas en las franjas horarias definidas.

Step 1 Inicie sesión en la página web.

Step 2 Seleccionar**Sección de tiempo**>**Configuración del grupo de vacaciones**Haga

Step 3 clic en**Agregar**.

Figure 3-15 Añadir un grupo de vacaciones



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

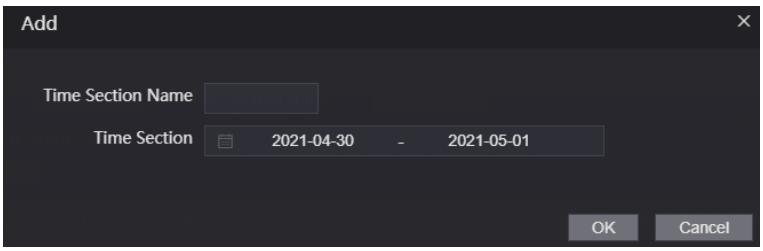
- **No.**:Ingrese un número de sección. Varía entre 0 y 127.
- **Nombre de la sección de tiempo**: Ingrese un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (que pueden incluir números, caracteres especiales y caracteres en inglés).

Step 5 Hacer clic**Agregar**.

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

Puede agregar varios días festivos para un grupo de vacaciones.

Figure 3-16 Añadir un día festivo



Step 7 Hacer clic**DE ACUERDO**.

3.1.6.3 Configuración del plan de vacaciones

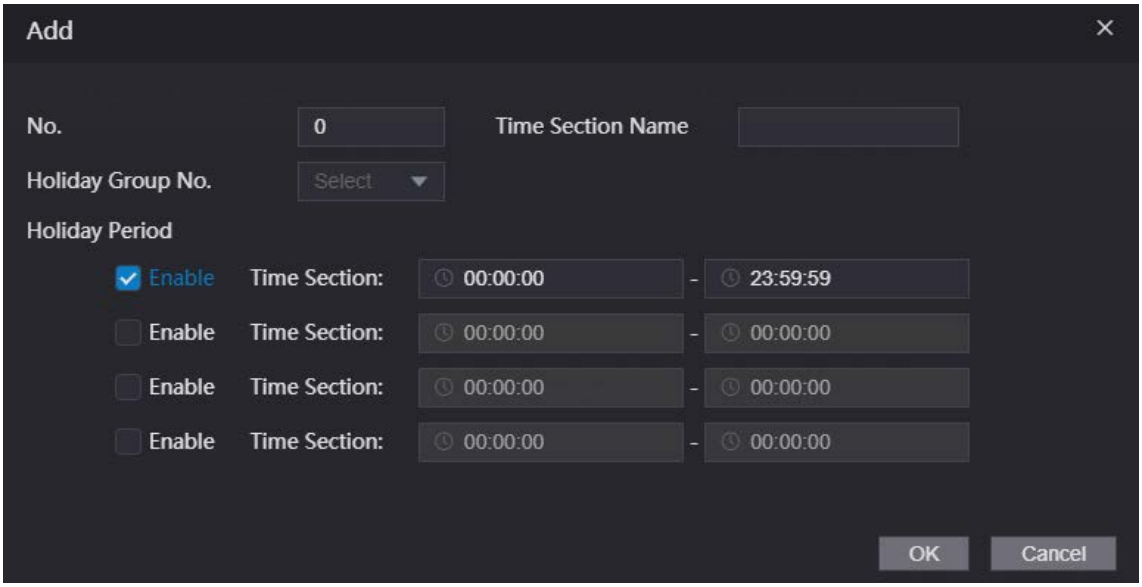
Asignar los grupos de vacaciones configurados al plan de vacaciones. Los usuarios solo pueden desbloquear la puerta en el horario definido en el plan de vacaciones.

Step 1 Inicie sesión en la página web.

Step 2 Seleccionar**Sección de tiempo**>**Configuración del plan de vacaciones**Haga clic

Step 3 en**Agregar**.

Figure 3-17 Añadir un plan de vacaciones



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

- **No.**:Ingrese un número de sección. Varía entre 0 y 127.
- **Nombre de la sección de tiempo**: Ingrese un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (que pueden incluir números, caracteres especiales y caracteres en inglés).

Step 5 En el**Grupo de vacaciones No.**Lista, seleccione el grupo de vacaciones que haya configurado.

Seleccionar**255**Si no desea seleccionar un grupo de vacaciones.

Step 6 En el**Periodo de vacaciones**Área, configure los tramos horarios en el grupo de vacaciones. Puede configurar hasta cuatro tramos horarios.

Step 7 Hacer clic**DE ACUERDO**.

3.1.7 Capacidad de datos

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

Step 1 Inicie sesión en la página web.

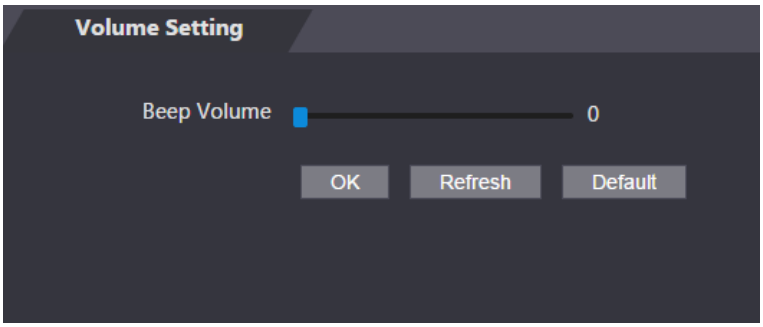
Step 2 Seleccionar**Capacidad de datos**en la barra de navegación.

3.1.8 Ajuste del volumen

Step 1 Inicie sesión en la página web.

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

Figure 3-18 Ajuste del volumen



Step 3 Hacer clic**DE ACUERDO**.

3.1.9 Configuración de la 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.

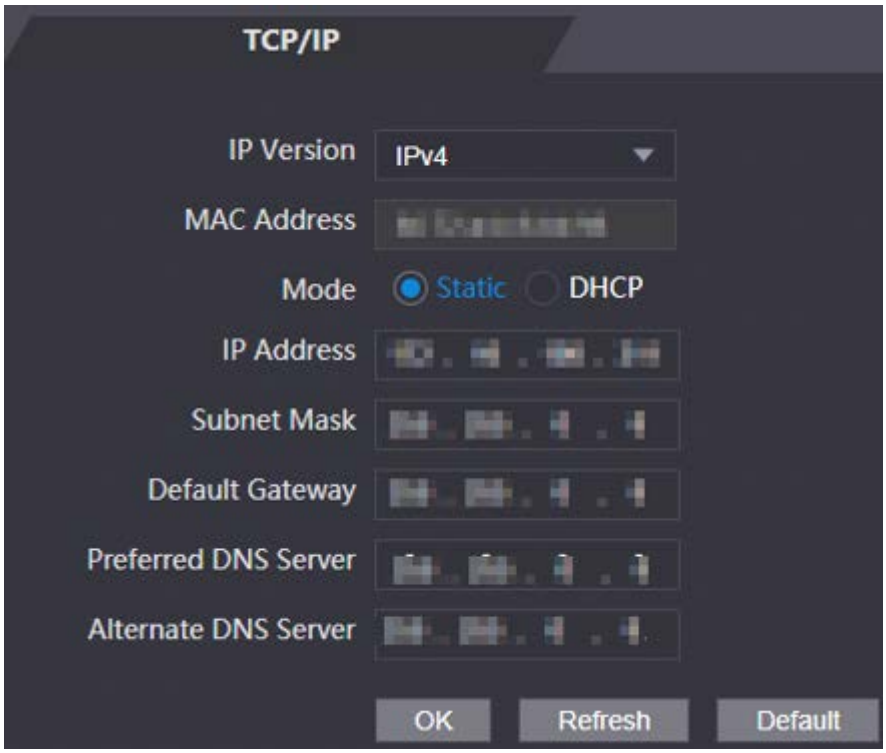
Requisito previo

Asegúrese de que el dispositivo esté conectado a la red.

Step 1 Inicie sesión en la página web. Seleccione

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

Figure 3-19 Protocolo TCP/IP



Step 3 Configurar parámetros.

Tabla 3-3 Descripción de TCP/IP

Parámetro	Descripción
Versión IP	Protocolo de Internet (IPv4)
Dirección MAC	Dirección MAC del dispositivo.
Modo	● **Estático**:Configure la dirección IP, la máscara de subred y la dirección de puerta de enlace ● manualmente. **DHCP** - Una vez habilitado DHCP, no se pueden configurar la dirección IP, la máscara de subred ni la dirección de puerta de enlace. - Si DHCP es efectivo, la dirección IP, la máscara de subred y la dirección de puerta de enlace serán asignadas por DHCP automáticamente. - 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 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	Establezca la dirección IP del servidor DNS preferido.

Step 4 Hacer clic**DE ACUERDO**para completar la configuración.

3.1.9.2 Configuración del puerto

Puede limitar el acceso al Dispositivo al mismo tiempo mediante la web, el software y el 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
Máximo Conexión	Establezca el acceso máximo al dispositivo a través de clientes, como web, software y teléfono. Los clientes de 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**DE ACUERDO**para completar la configuración.

3.1.9.3 Registrarse

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

Step 1 Inicie sesión en la página web.

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

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

Tabla 3-5 Descripción del registro automático

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

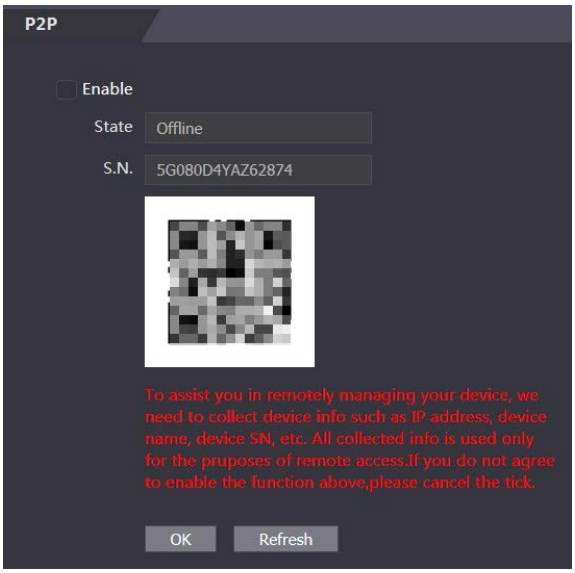
Step 4 Hacer clic**DE ACUERDO**para completar la configuración.

3.1.9.4 P2P

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

Si desea utilizar P2P, debe conectar el Dispositivo a Internet; de lo contrario, esta función no podrá trabajar correctamente

Figure 3-20 P2P



Step 1 Inicie sesión en la página web. Seleccione**Configuración de**

Step 2 **red**>**P2P**. Seleccionar**Permitir**Para habilitar la función P2P,

Step 3 haga clic en**DE ACUERDO**.

Step 4

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

3.1.10 Fecha de configuración

Puede configurar la zona horaria, la hora del sistema, el horario de verano (DST) o el protocolo NTP (protocolo de tiempo de red).

Step 1 Inicie sesión en la página web.

Step 2 Haga clic en**Ajuste de fecha**.

Figure 3-21 Ajuste de fecha

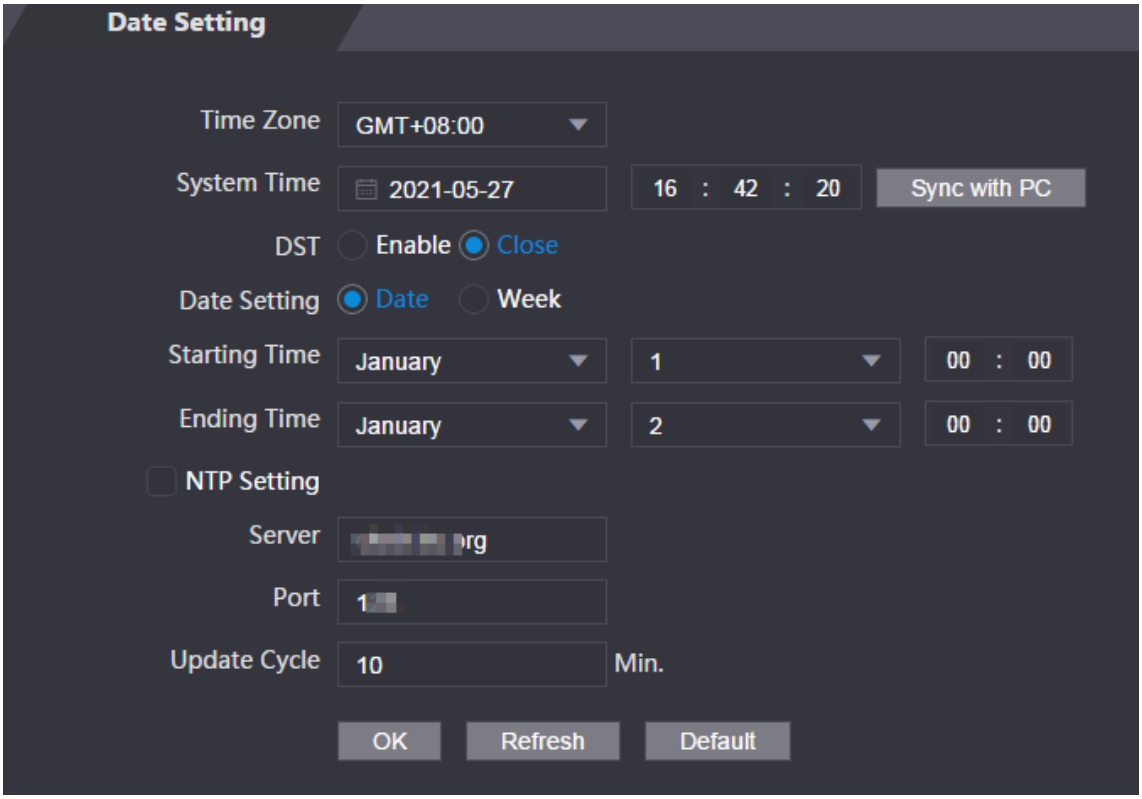


Tabla 3-6 Descripción de la configuración de datos

Parámetro	Descripción
Huso horario	Configurar 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 el horario de verano. 2. Seleccionar**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**:Ingrese 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**: ● Introduzca el intervalo de sincronización horaria.

Step 3 Hacer clic**DE ACUERDO**.

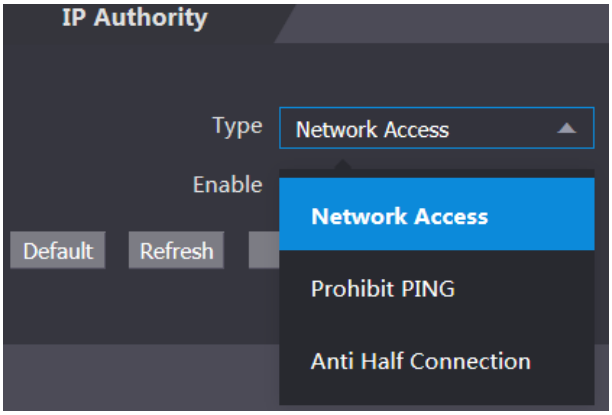
3.1.11 Gestión de la seguridad

3.1.11.1 Configuración de la autoridad IP

Step 1 Inicie sesión en la página web.

Step 2 Hacer clic**Gestión de seguridad.**>**Autoridad de propiedad intelectual**.

Figure 3-22 Autoridad de propiedad intelectual



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

- **Acceso a la red**:Establezca la lista de permitidos y la lista de bloqueados para controlar el acceso al dispositivo.
  - **Lista de permitidos**:una lista de direcciones IP/MAC confiables que tienen acceso al dispositivo. **Lista de**
  - **bloqueo**:una lista de direcciones IP/MAC bloqueadas que no tienen acceso al dispositivo.
- **Prohibir PING**: Permitir**PING prohibido**función y el dispositivo no responderá a la solicitud Ping.
- **Anti-Media Conexión**: Permitir**Anti-Media Conexión**función, y el dispositivo aún puede funcionar correctamente bajo un ataque de media conexión.

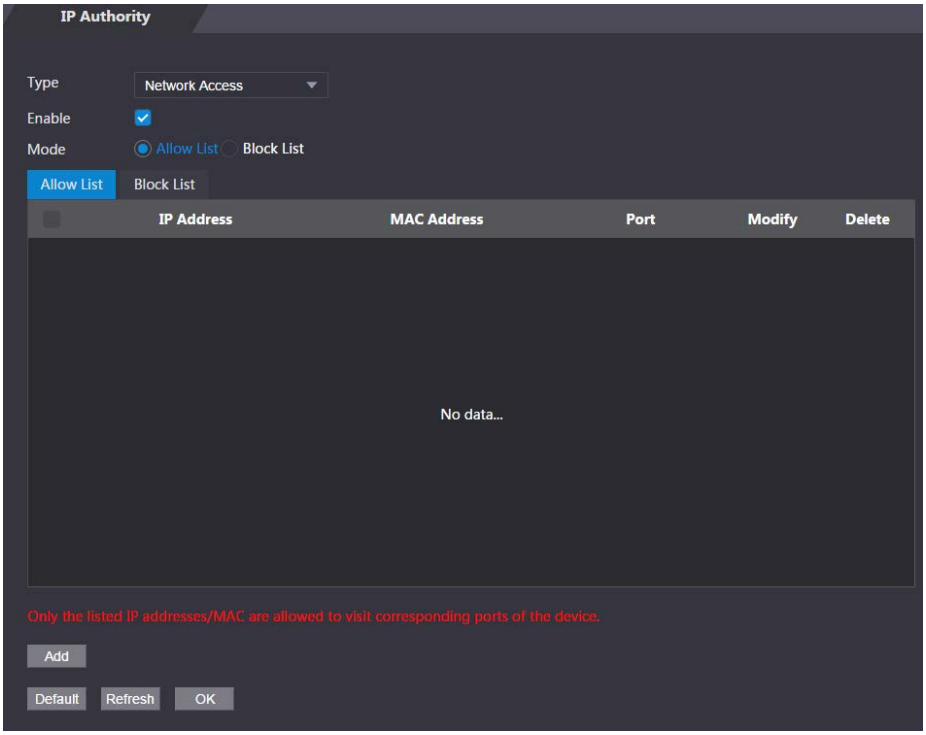
3.1.11.1.2 Acceso a la red

Seleccionar**Acceso a la red**en el**Tipo**lista.

Procedimiento

Step 1 Seleccione el**Permitir**caja.

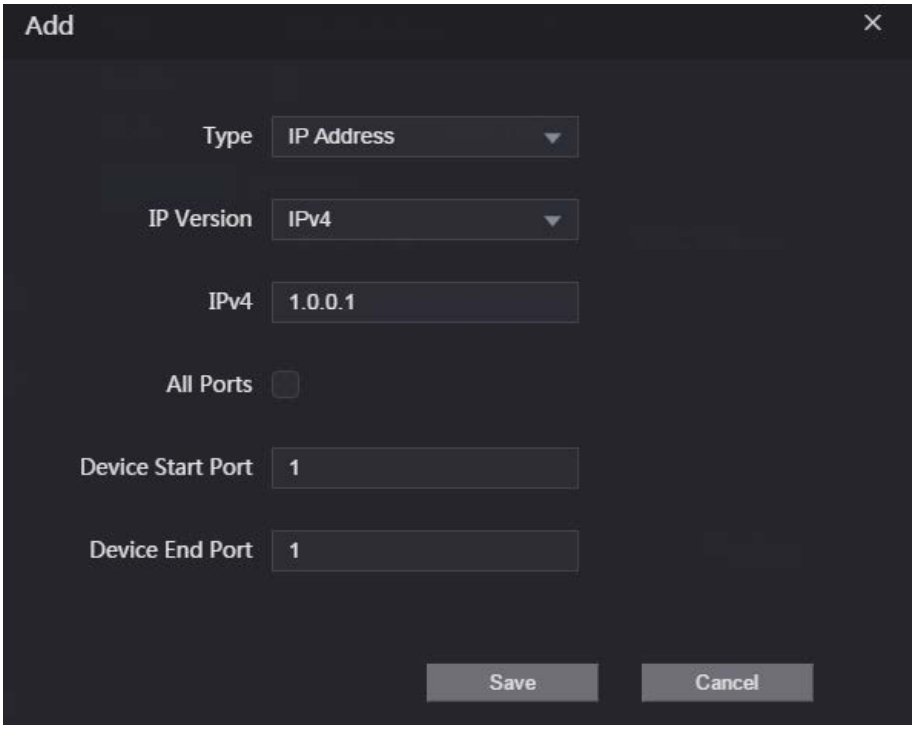
Figure 3-23 Acceso a la red



Step 2 Seleccionar**Lista de permitidos**o**Lista de bloqueos**Haga

Step 3 clic en**Agregar**.

Figure 3-24 Agregar IP



Step 4 Configurar parámetros.

Tabla 3-7 Descripción de cómo agregar parámetros de IP

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

Parámetro	Descripción
Puerto de inicio del dispositivo	Si lo aclarasTodos los puertosCasilla de verificación, establece el puerto de inicio del dispositivo y el puerto final del dispositivo.
Puerto final del dispositivo	

Step 5 Hacer clicAhorrar, y elAutoridad de propiedad intelectualSe muestra la ventana. Haga clic enDE

Step 6 ACUERDO.

Operaciones relacionadas

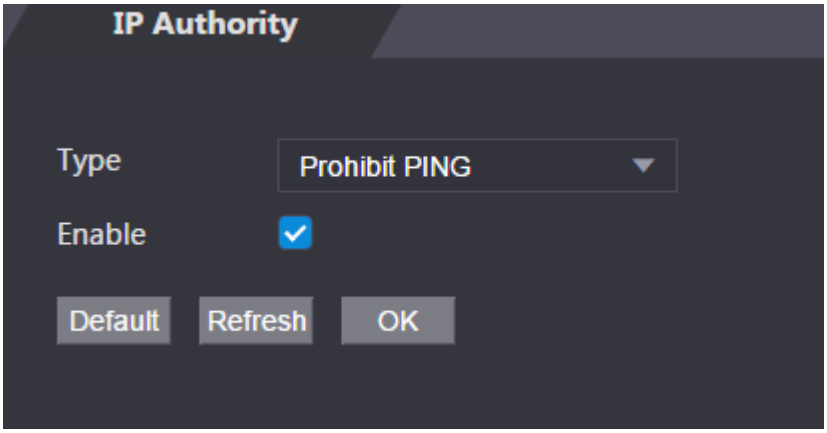
- Hacer clic  para editar la lista de permitidos o la lista de bloqueados.
- Hacer clic  para eliminar la lista blanca o la lista negra

3.1.11.1.3 Prohibir PING

Step 1 SeleccionarProhibir PINGen elTipolista.

Step 2 Seleccione laPermitircaja.

Figure 3-25 Prohibir PING



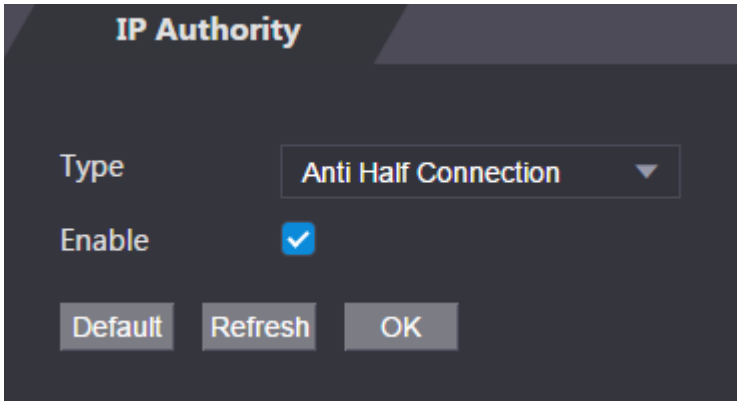
Step 3 Hacer clicDE ACUERDO.

3.1.11.1.4 Conexión anti-media

Step 1 Seleccione elAnti-Media Conexiónen elTipolista.

Step 2 Seleccione laPermitircaja.

Figure 3-26 Acceso a la red



Step 3 Hacer clicDE ACUERDO.

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 Seleccionar**Gestión de seguridad.**>**Servicio del sistema**

Step 3 . Habilitar o deshabilitar los servicios del sistema.

Figure 3-27 Servicio del sistema

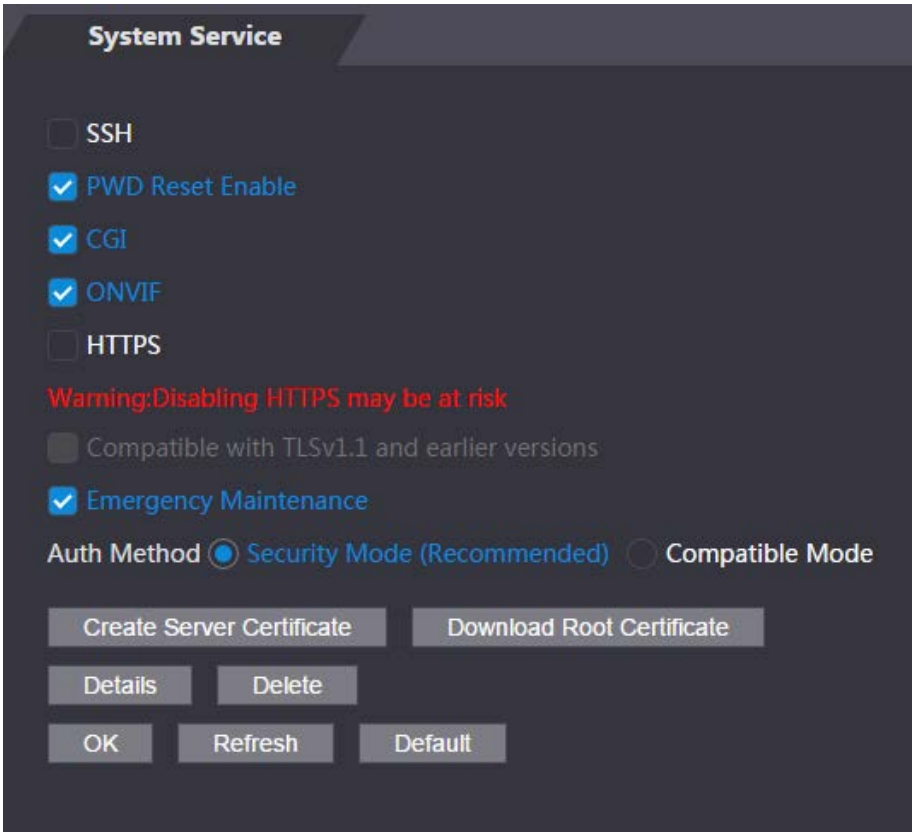


Tabla 3-8 Descripción del servicio del sistema

Parámetro	Descripción
SSH	Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura a través de una red no segura. Cuando SSH está habilitado, SSH proporciona un servicio criptográfico para la transmisión de datos.
Restablecimiento de contraseña Permitir	Si está habilitada, puede restablecer la contraseña. Esta función está habilitada de manera predeterminada.
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 páginas web dinámicamente.VR dne Cuando CGI está habilitado, se pueden usar comandos CGI. CGI está habilitado de manera predeterminada.
ONVIF	Permitir que otros dispositivos extraigan la transmisión de video del VTO a través del protocolo ONVIF.

Parámetro	Descripción
HTTPS	El Protocolo seguro de transferencia de hipertexto (HTTPS) es un protocolo para la comunicación segura a través de una red de computadoras. Cuando HTTPS está habilitado, se utilizará HTTPS 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 Creación de un certificado de servidor

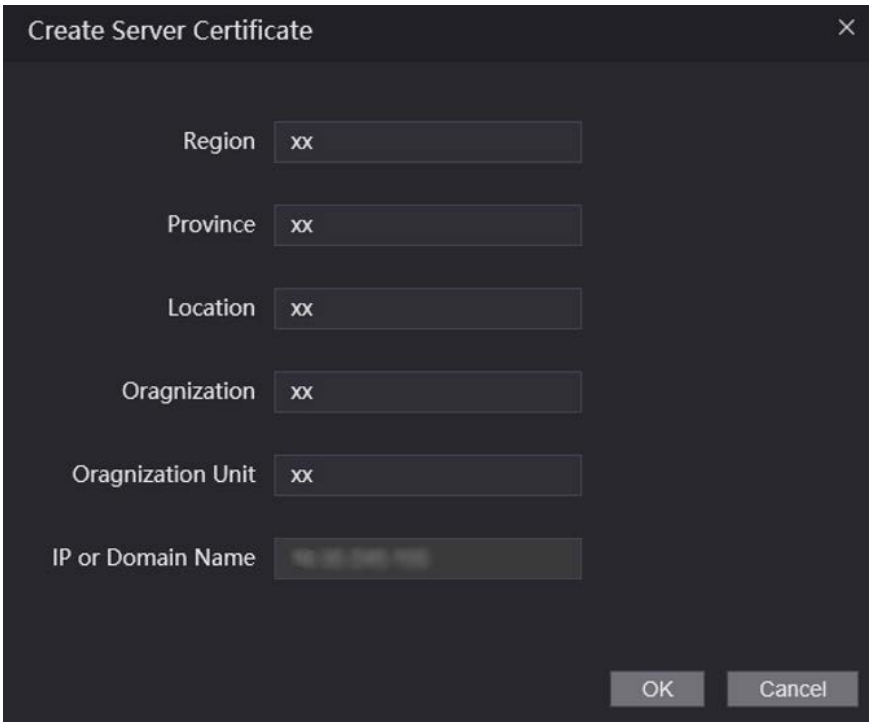
Configure el servidor HTTPS para mejorar la seguridad de su sitio web con el certificado de servidor.

- Si utiliza 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 nuevamente el certificado raíz en la nueva PC o copiarlo a la nueva PC.

Step 1 En el**Servicio del sistema**página, haga clic**Crear certificado de servidor**Ingrese la

Step 2 información y haga clic**DE ACUERDO**y luego el dispositivo se reiniciará.

Figure 3-28 Crear certificado de servidor

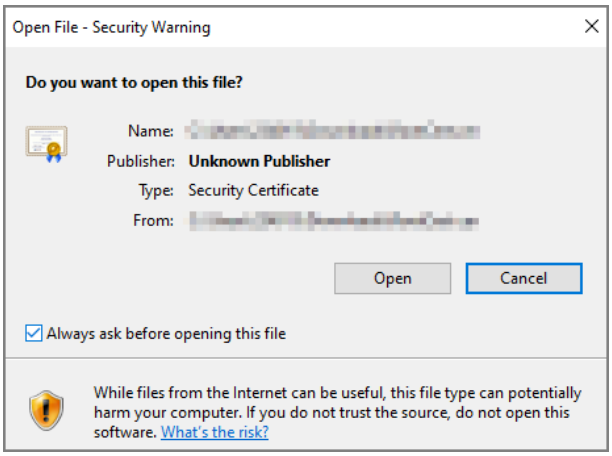


3.1.11.2.3 Descarga del certificado raíz

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

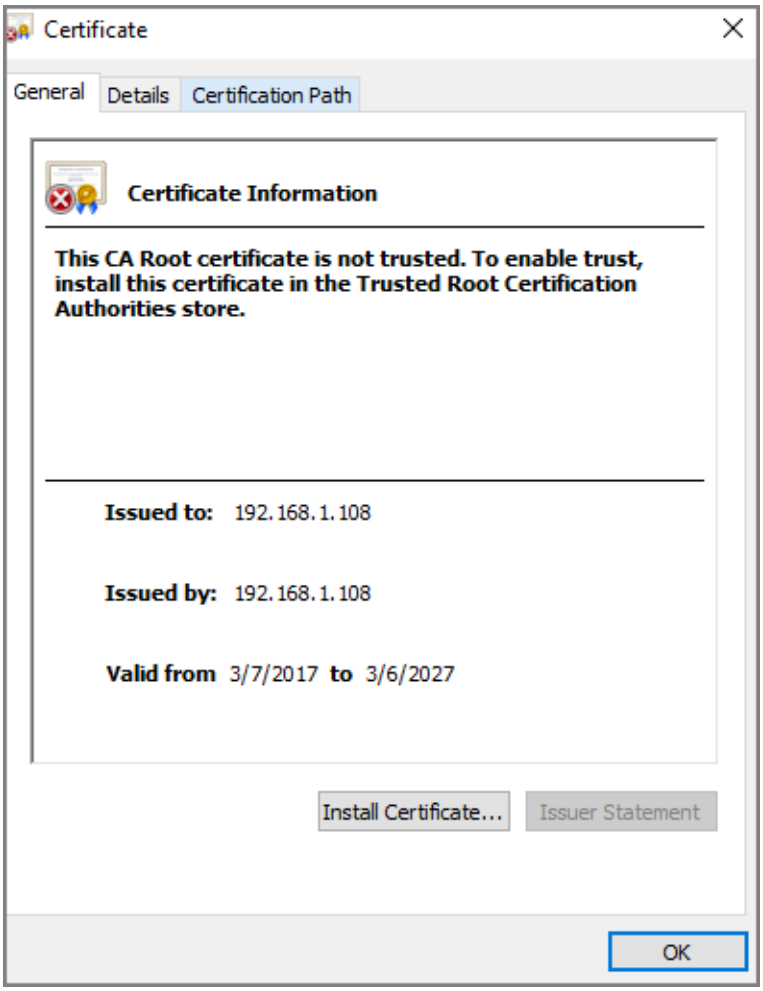
Step 2 doble clic en el archivo que ha descargado y luego haga clic en**Abierto**.

Figure 3-29 Descarga de archivos



Step 3 Hacer clic**Instalar certificado**.

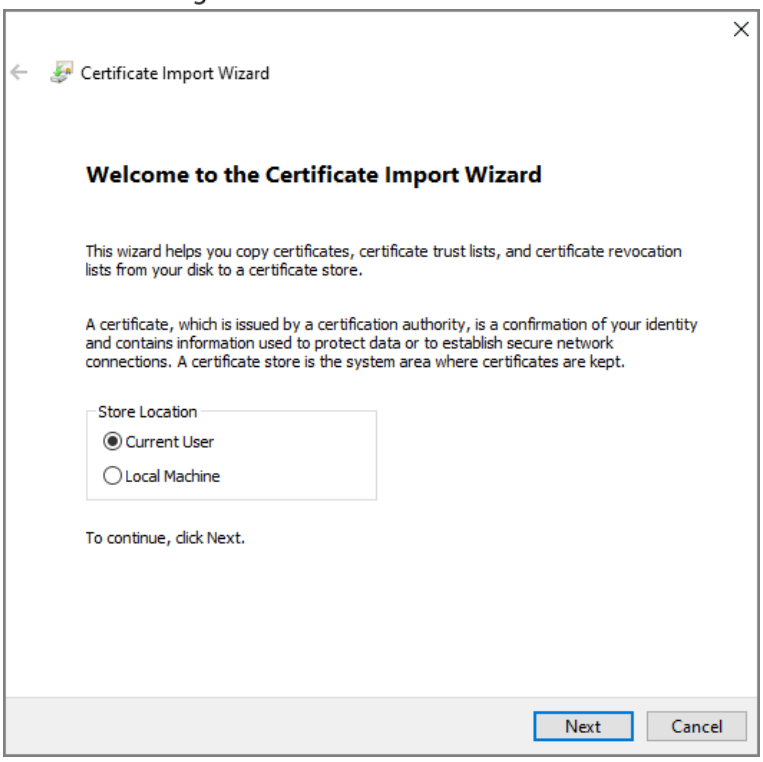
Figure 3-30 Información del certificado



Step 4 Seleccionar**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

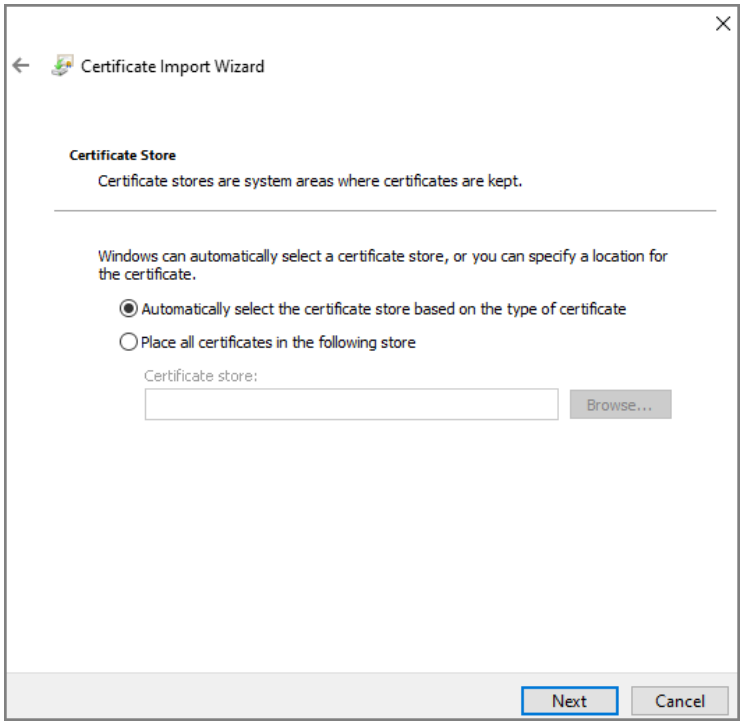


Step 5 Seleccione la ubicación de almacenamiento adecuada.

1) Seleccionar**Coloque todos los certificados en el siguiente almacén**.

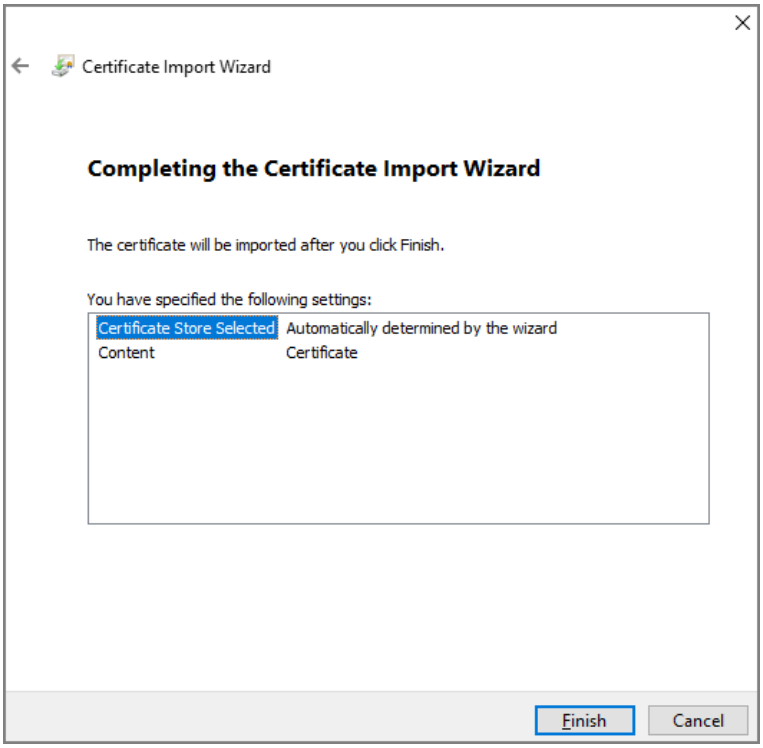
2) Haga clic**Navegar**para importar el certificado a la**Autoridades de certificación raíz de confianza** tienda y luego haga clic en**Próximo**.

Figure 3-32 Almacén de certificados



Step 6 Hacer clic**Finalizar**.

Figure 3-33 Tienda de certificados seleccionada



3.1.12 Gestión de usuarios

Puede agregar y eliminar usuarios, cambiar sus contraseñas 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.

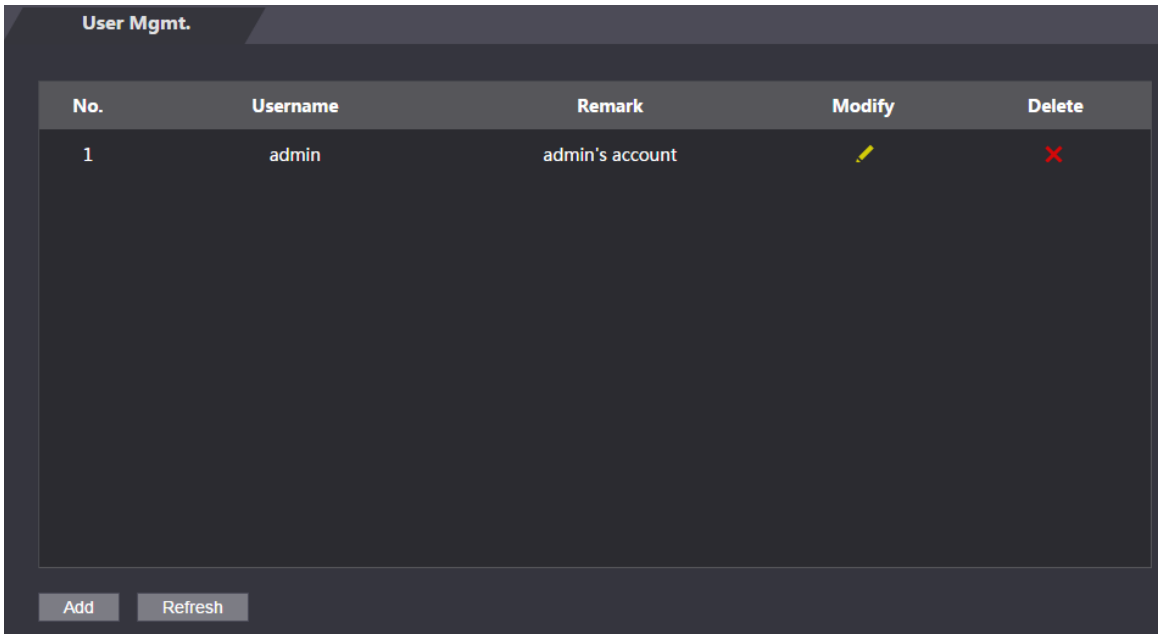
3.1.12.1 Usuario

3.1.12.1.1 Agregar usuarios

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

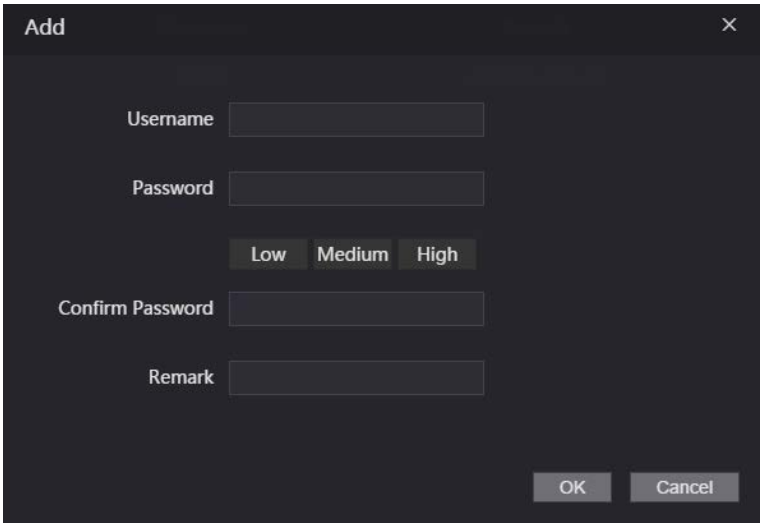
Step 2 **de usuarios.**>**Gestión de usuarios**.

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 haga clic en el comentario.

Step 5 **DE ACUERDO**.

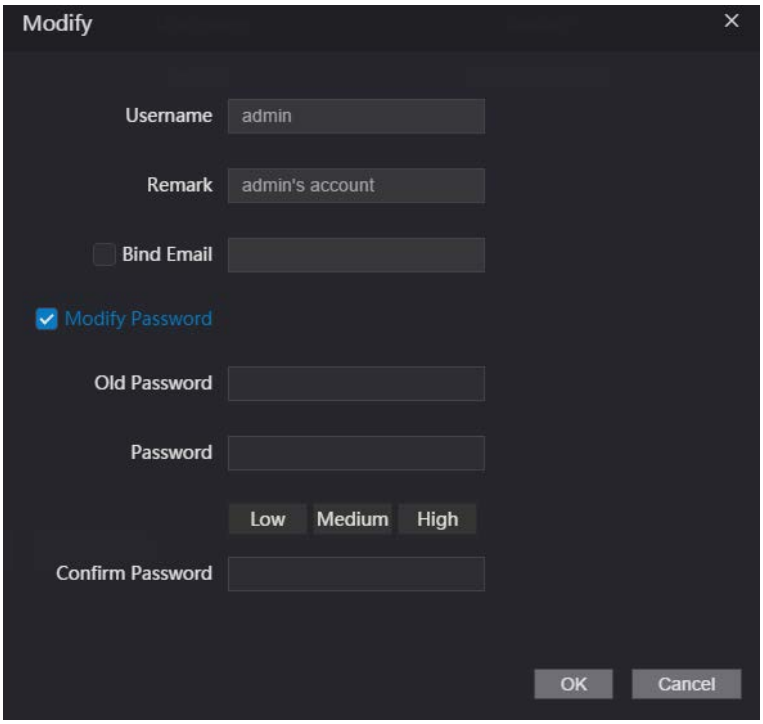
3.1.12.1.2 Cambio de contraseña

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 información del usuario



Step 4 Seleccione el**Vincular correo electrónico**casilla de verificación e introduzca la dirección de correo electrónico.

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

Step 6 Hacer clic**DE ACUERDO**.

3.1.12.2 Usuario ONVIF

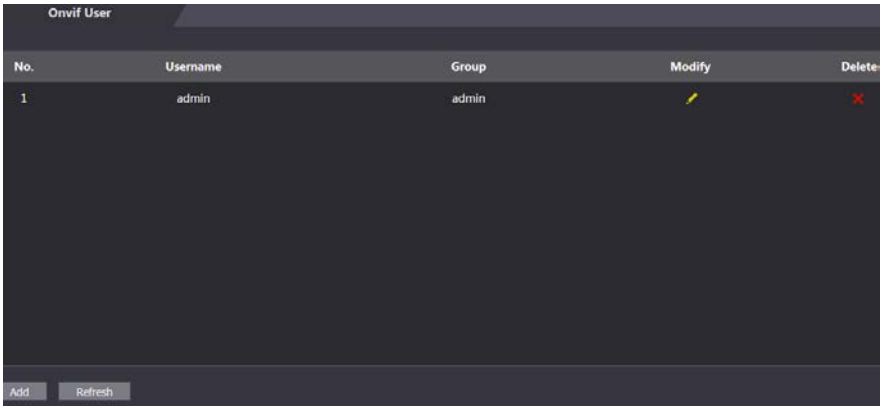
Open Network Video Interface Forum (ONVIF), un foro industrial abierto y global creado para desarrollar un estándar abierto global para la interfaz de productos de seguridad basados en IP físicos. Cree usuarios ONVIF y verifique sus identidades a través del protocolo ONVIF.

3.1.12.2.1 Agregar usuario ONVIF

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

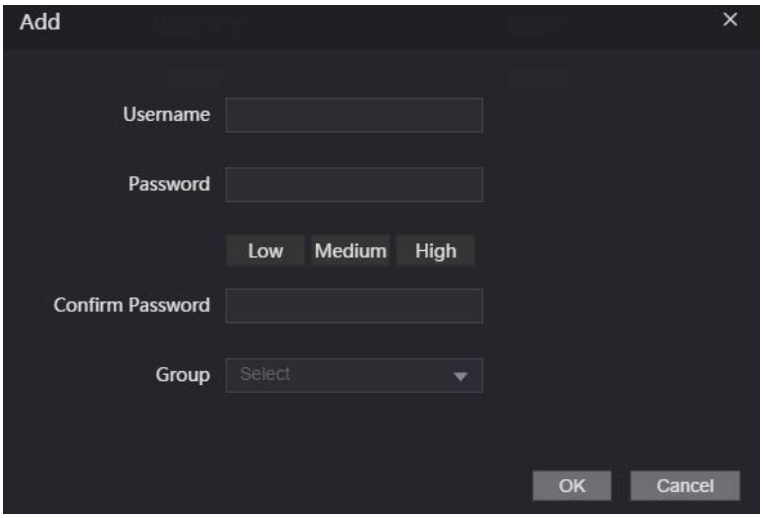
Step 2 **de usuarios.**>**Usuario de Onvif**.

Figure 3-37 Usuario de Onvif



Step 3 Hacer clic**Agregar**.

Figure 3-38 Agregar usuario ONVIF



Step 4 Introduce el nombre de usuario, la contraseña y confirma la contraseña.

Step 5 Selecciona el grupo.

Step 6 Hacer clic**DE ACUERDO**.

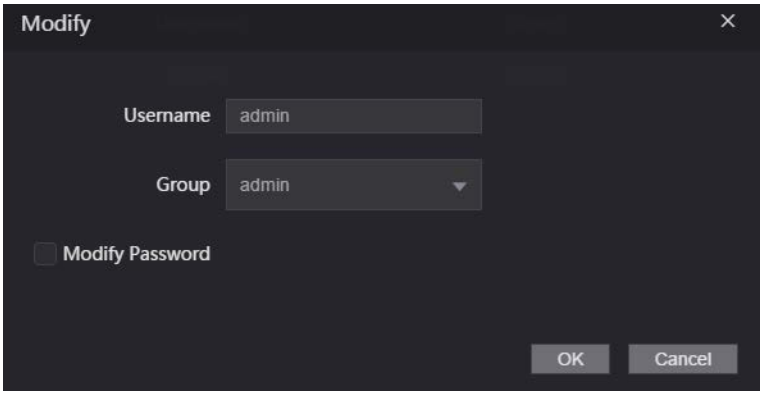
3.1.12.2.2 Cambio de contraseña

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

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

Step 3 

Figure 3-39 Cambiar la contraseña (usuario ONVIF)



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

Step 5 Hacer clic**DE ACUERDO**.

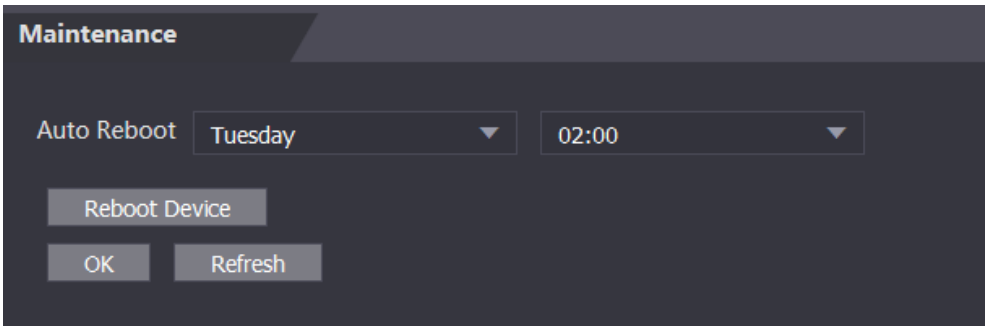
3.1.13 Mantenimiento

Puede reiniciar periódicamente 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**DE ACUERDO**.

El dispositivo se reiniciará a la hora definida.

Es**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 parámetros para ellos importando o exportando archivos de configuración.

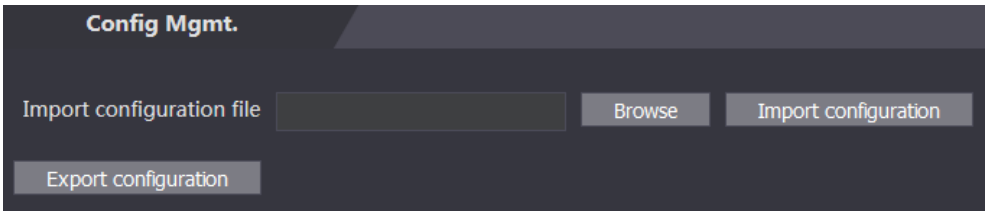
3.1.14.1 Exportación de archivo de configuración

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

Step 1 Inicie sesión en la página web.

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

Figure 3-41 Gestión de configuración



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

La información IP del dispositivo no se exportará.

3.1.14.2 Importación de 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 Seleccionar**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 Seleccionar**Gestión de configuración**>**Gestión de configuración**. En

Step 3 el**Características**Área, establecer las características.

Figure 3-42 Características

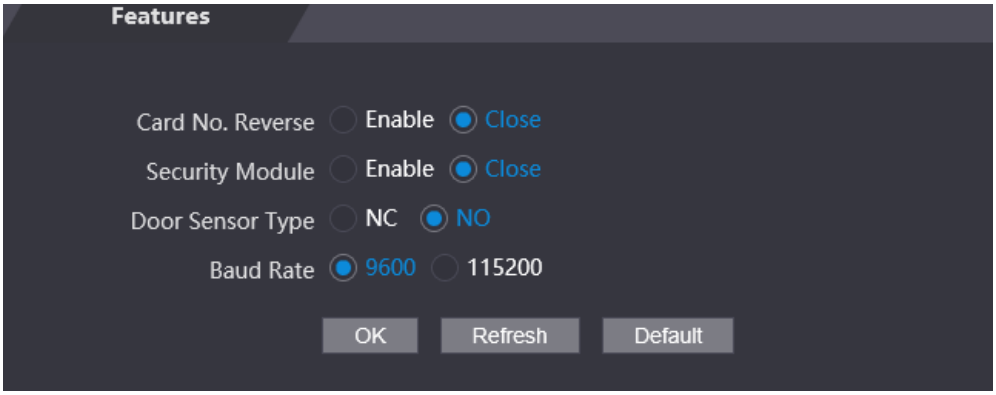


Tabla 3-9 Descripción de características

Parámetro	Descripción
Tarjeta N° Reverso	Permitir**Tarjeta N° Reverso**función, si configura la salida Wiegand y conecta un dispositivo externo, pero el orden del número de tarjeta recibido es inconsistente con el del número real.
Módulo de seguridad	Si**Módulo de seguridad**está habilitado, el botón de salida de la puerta, la cerradura y el enlace contra incendios no son válidos.
Tipo de sensor de puerta	Establecer el tipo de sensor de puerta: ● **CAROLINA DEL NORTE**:Normalmente ● cerrado. **NO**:Normalmente abierto.
Tasa de Baud	Seleccione la velocidad en baudios según el dispositivo externo.

Step 4 Hacer clic**DE ACUERDO**.

3.1.14.4 Configuración de huella digital

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

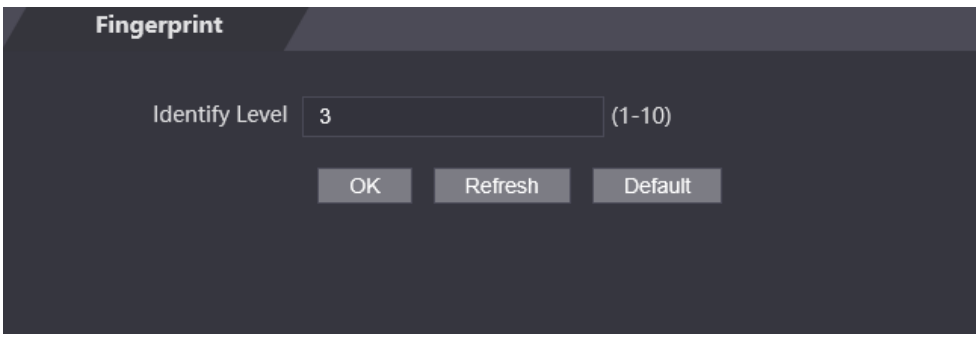
Step 1 Inicie sesión en la página web.

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

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

Un nivel de identidad más alto significa una mayor precisión de reconocimiento y un umbral de reconocimiento más alto.

Figure 3-43 Nivel de identidad de la huella dactilar



Step 4 Hacer clic**DE ACUERDO**.

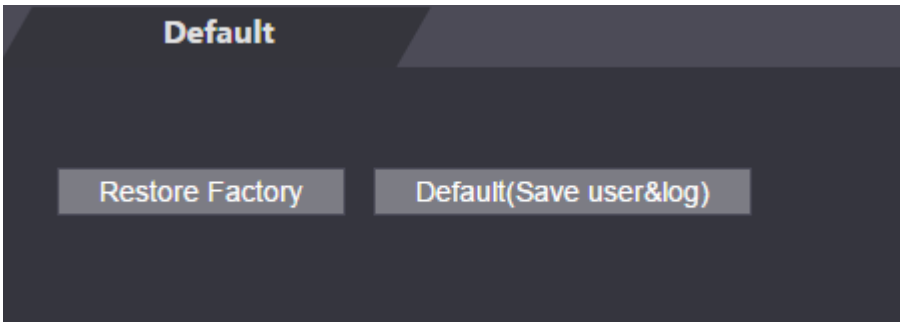
3.1.14.5 Restauración de valores predeterminados de fábrica

Si se restaura el dispositivo a la configuración predeterminada, se perderán los datos. Tenga en cuenta lo siguiente.

Step 1 Inicie sesión en la página web. Seleccione

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

Figure 3-44 Por defecto



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

- **Restaurar fábrica:**Restablece las configuraciones del dispositivo y borra 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 Actualización del sistema

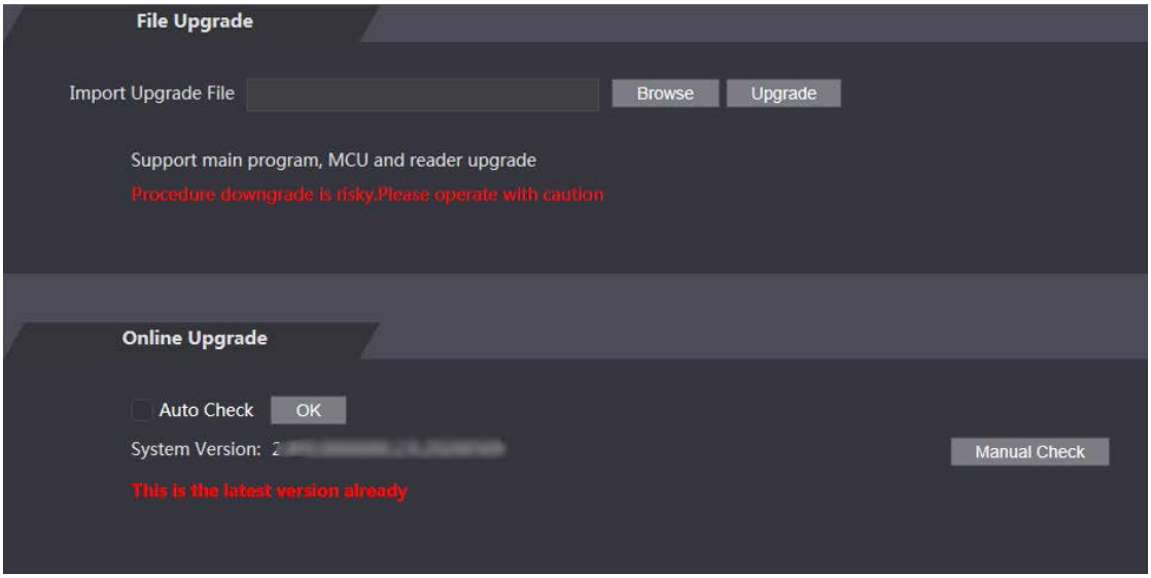
- Exporte el archivo de configuración para realizar una copia de seguridad antes de actualizar y luego importe el archivo después de la actualización Completa.
- Utilice el archivo de actualización correcto. Asegúrese de obtener el archivo de actualización correcto del soporte técnico.

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

Step 1 Inicie sesión en la página web.

Step 2 Seleccione**Mejora**.

Figure 3-45 Mejora



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**Mejora**.

El dispositivo se reiniciará una vez que se complete la actualización.

- Actualización en línea

1) Seleccione el**Comprobación automática**casilla de verificación y luego haga clic en**DE**

ACUERDOEl sistema busca automáticamente nuevas versiones.

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 actualizaciones.

2) Si hay alguna nueva versión disponible, haga clic en**Mejora**. El

dispositivo se reiniciará una vez completada la actualización.

Hacer clic**Comprobación manual**para comprobar manualmente si hay una nueva versión.

3.1.16 Información de la versión

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

Step 1 Inicie sesión en la página web.

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

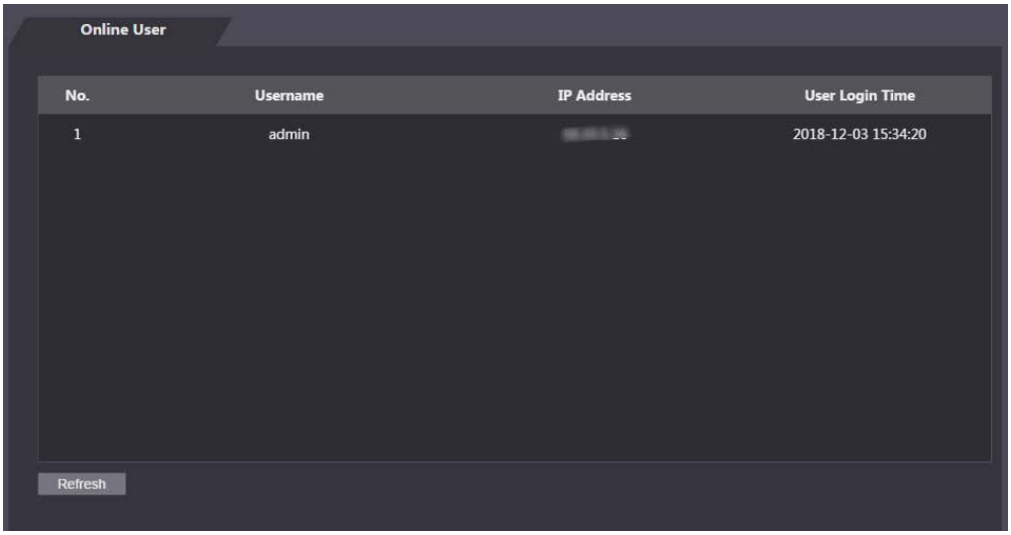
3.1.17 Visualización de usuarios en línea

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

Ver y realizar copias de seguridad de los registros del sistema, registros de administración y registros de desbloqueo.

3.1.18.1 Registros del sistema

Ver y buscar registros del sistema.

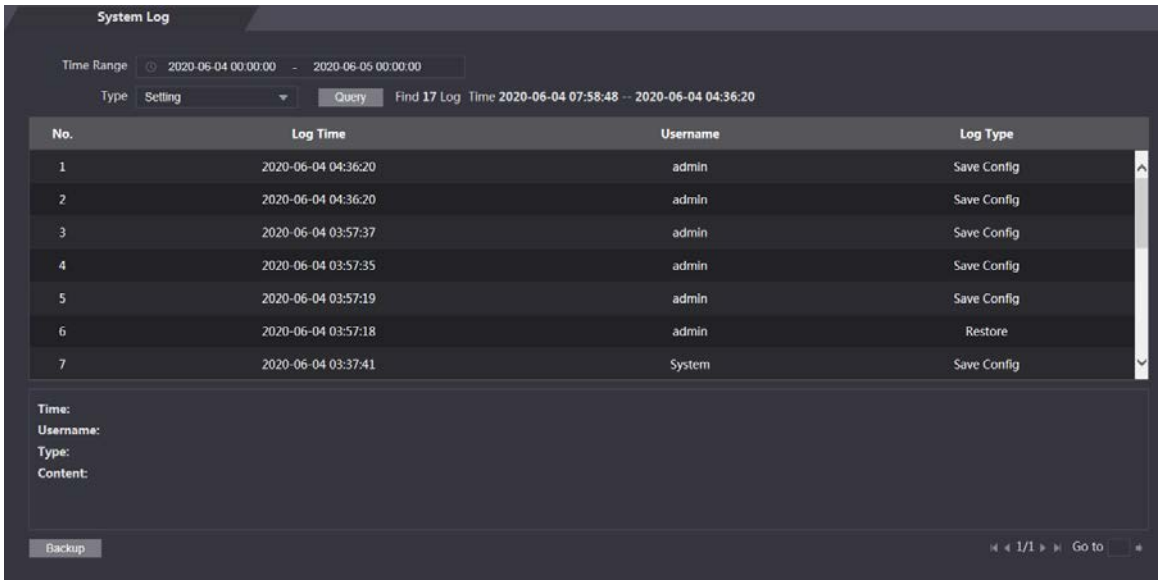
Step 1 Inicie sesión en la página web. Seleccione**Registro**

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

Step 3 Seleccione el rango de tiempo y el tipo de registro y luego haga clic en**Consulta**.

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

Figure 3-47 Buscar registros



3.1.18.2 Registros de administración

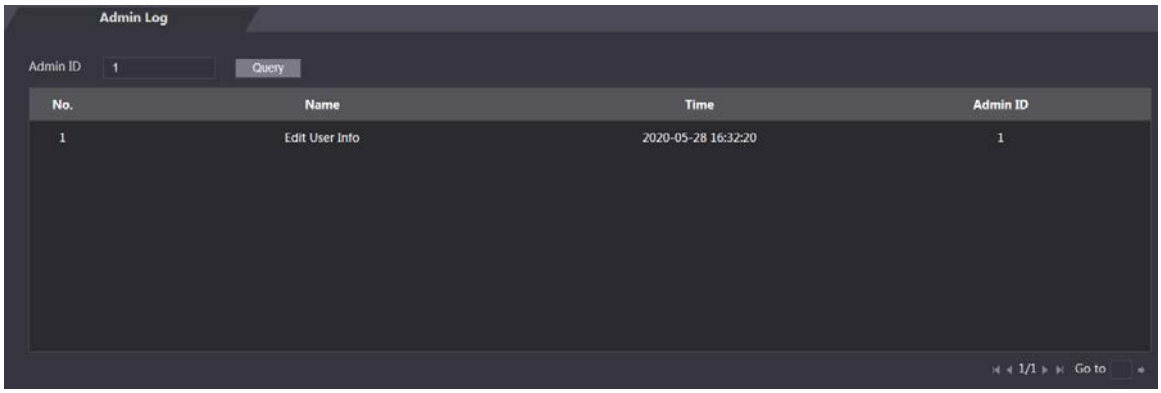
Busque registros de administración utilizando el ID de administrador.

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

Step 2 **Registro de administración**Ingrese el ID de administrador y luego

Step 3 haga clic 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 Seleccionar**Registro del sistema**>**Buscar registros**.

Step 3 Seleccione el rango de tiempo y el tipo de registro y luego haga clic en**Consulta**Haga

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

3.1.19 Cerrar sesión

Hacer clic  en la esquina superior izquierda y luego haga clic en**DE ACUERDO**para cerrar sesión en la página web.

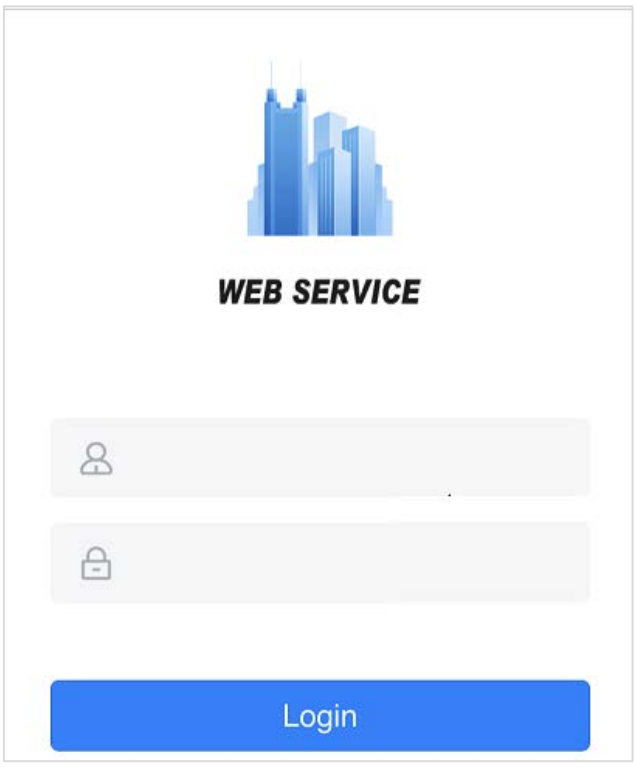
3.2 Web en el teléfono

Asegúrate de que el dispositivo esté en la misma red LAN que tu teléfono. Conecta el dispositivo al punto de acceso de tu teléfono o conecta el dispositivo y tu 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 usted establece durante inicialización. Le recomendamos que cambie la contraseña de administrador periódicamente para aumentar seguridad.

Step 3 Hacer clic**Acceso**.

4 Configuración de CA SmartPSS

En este capítulo se presenta cómo administrar y configurar el dispositivo mediante 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 del manual del usuario son solo para fines ilustrativos. referencia y puede diferir del producto real.

4.1 Iniciar sesión

Step 1 Instalar SmartPSS AC.

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

4.2 Agregar dispositivos

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

4.2.1 Agregar individualmente

Step 1 Inicie sesión en SmartPSS AC. Haga clic

Step 2 en**Administrador de dispositivos**.

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

Step 4 página. Ingrese la información requerida.

Figure 4-1 Introducir información del dispositivo

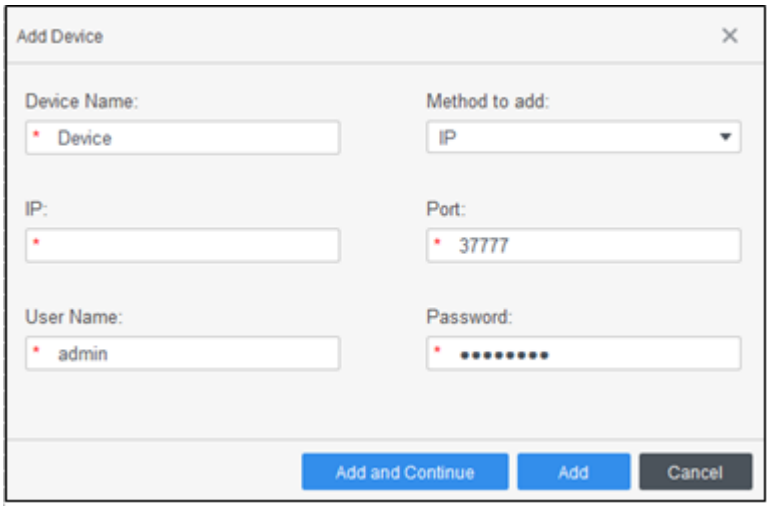


Tabla 4-1 Descripción de los parámetros del dispositivo

Parámetro	Descripción
Nombre del dispositivo	Introduzca un nombre para el dispositivo. Recomendamos nombrar el dispositivo según su zona de instalación.
Método para agregar	Seleccionar**Propiedad intelectual**para agregar dispositivo a través de la dirección IP.
Propiedad intelectual	Introduzca la dirección IP del dispositivo.
Puerto	El número de puerto es 37777 por defecto.
Nombre de usuario, Contraseña	Introduzca el nombre de usuario y la contraseña del dispositivo.

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

El dispositivo inicia sesión automáticamente después de agregarse.**En línea**Se muestra después de iniciar sesión correctamente.

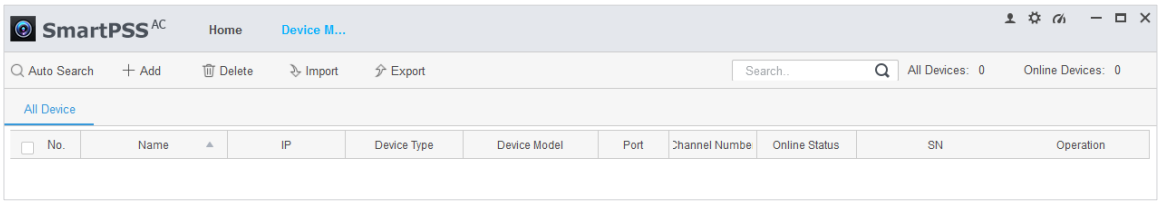
4.2.2 Adición por lotes

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

Step 1 Inicie sesión en SmartPSS AC. Haga clic

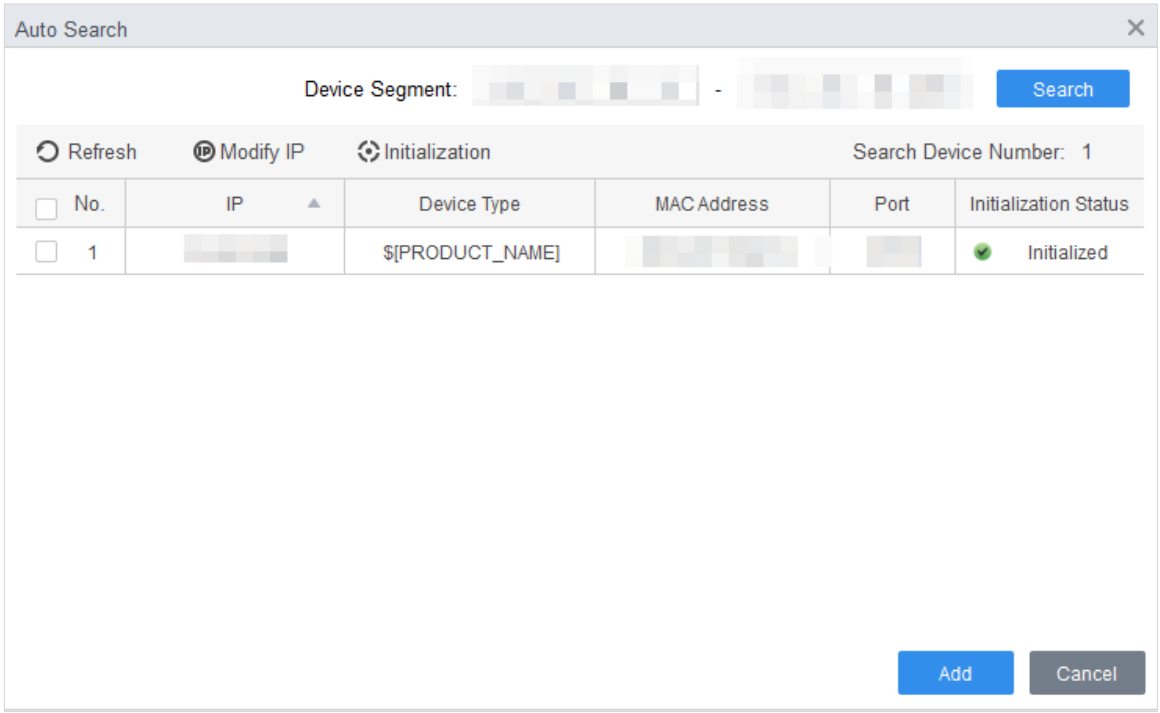
Step 2 en**Administrador de dispositivos**.

Figure 4-2 Dispositivos



Step 3 Hacer clic**Búsqueda automática**.

Figure 4-3 Búsqueda automática



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

- Hacer clic**Buscar**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 la manual de usuario de SmartPSS AC.

Step 5 Seleccione los dispositivos que desea agregar al 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 el**Dispositivos**página.

- El dispositivo inicia sesión automáticamente después de agregarse.**En línea**se muestra después de tener 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 contraseña.

  También puede hacer doble clic en el dispositivo para editar su información.
- :Configure el dispositivo. Puede configurar la hora, actualizar el dispositivo, reiniciarlo y Extraer información del usuario o registros de asistencia del dispositivo.
- y : Iniciar y cerrar sesión en el dispositivo.
- :Eliminar 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

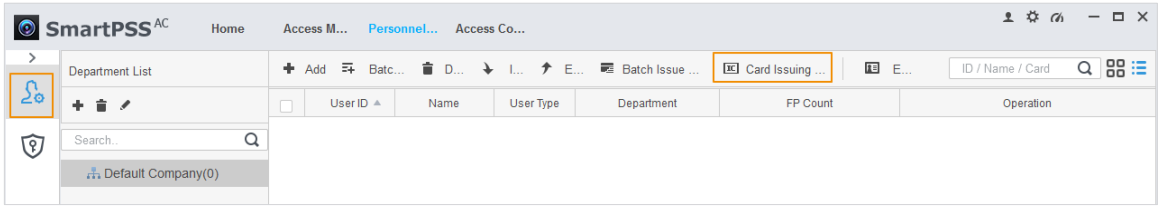
Antes de emitir una tarjeta, configure primero el tipo de tarjeta. Por ejemplo, si la tarjeta emitida es una tarjeta de identificación, configure el tipo como tarjeta de identificación.

Los tipos de tarjetas deben ser los mismos que los del emisor de la tarjeta; de lo contrario, no se podrán leer los números de tarjeta.

Step 1 Inicie sesión en SmartPSS AC. Haga

Step 2 clic en**Gerente de personal**.

Figure 4-4 Gerente de personal

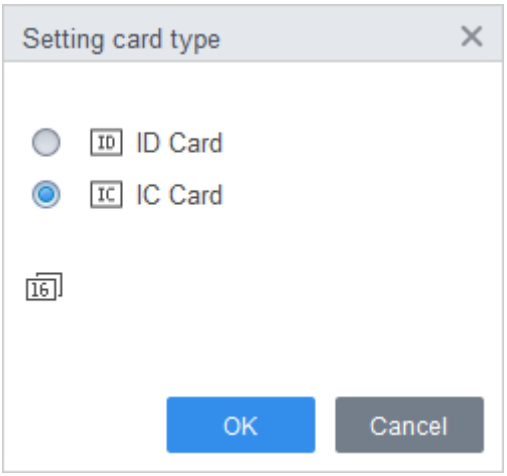


Step 3 Hacer clic y luego haga clic en .

Step 4 En el**Tipo de tarjeta de configuración**ventana, seleccione un tipo de tarjeta.

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

Figure 4-5 Tipo de tarjeta de configuración



Step 6 Hacer clic**DE ACUERDO**.

4.3.2 Agregar usuario

4.3.2.1 Agregar individualmente

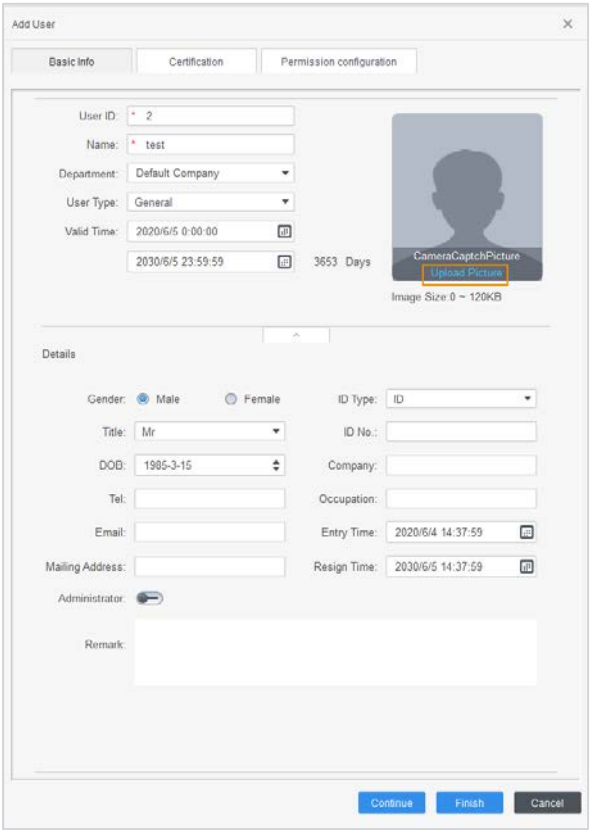
Puede agregar usuarios uno por uno manualmente.

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 Añadir información básica



Step 4 Haga clic en el**Proceso de dar un título**Pestaña para agregar información de certificación del usuario.

- Configurar contraseña.

  La contraseña debe tener entre 6 y 8 dígitos.

- Configurar tarjeta.

  El número de tarjeta se puede leer automáticamente o ingresar 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 , configure**Lector de tarjetas**a**Dispositivo**y luego seleccione el dispositivo que desea agregar desde**Dispositivo**.

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

3) Haga clic**DE ACUERDO**.

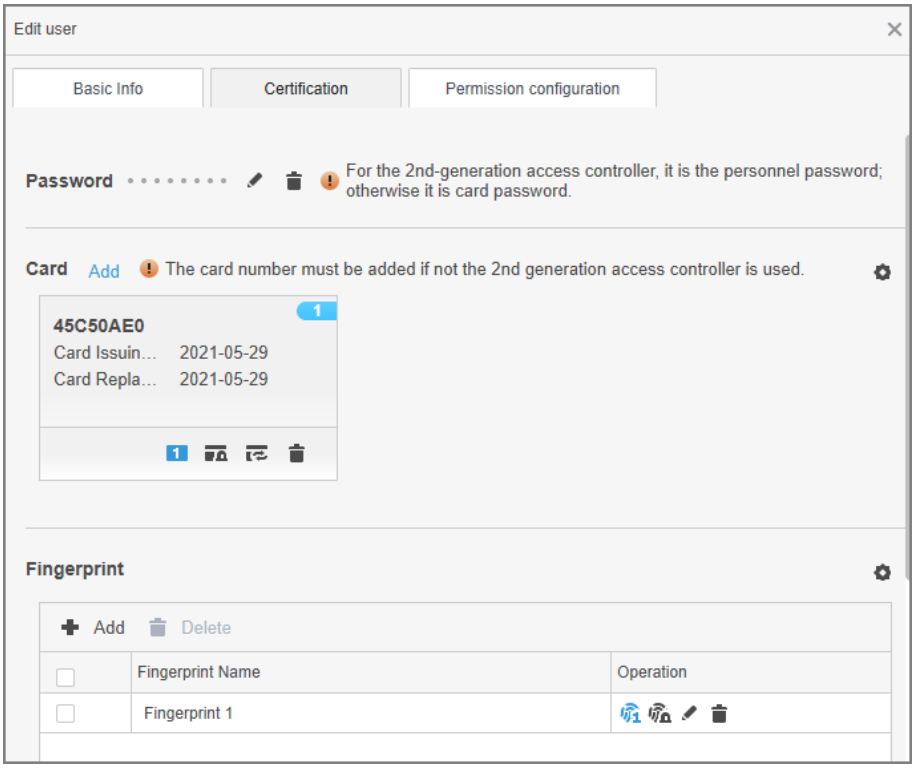
4) (Opcional) Después de agregar una tarjeta, puede configurarla como tarjeta principal o tarjeta de coacción, o reemplazarla por una nueva, o eliminarla.

- Configurar huella digital.

1) Haga clic en , configure**Recolector de huellas dactilares**a**Dispositivo**.

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

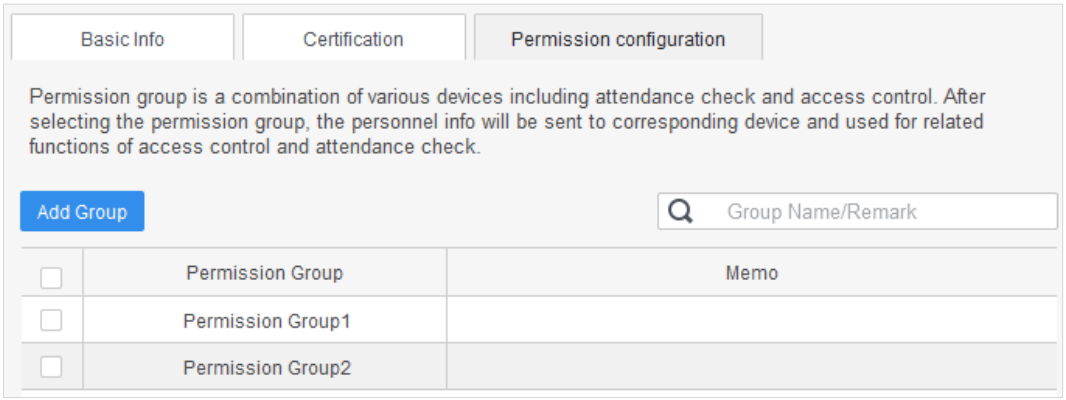
Figure 4-7 Agregar contraseña, tarjeta y huella digital



Step 5 Configurar permisos para el usuario.

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

Figure 4-8 Configuración de permisos



Step 6 Hacer clic**Finalizar**.

4.3.2.2 Adición por lotes

Puede agregar usuarios en lotes.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Gerente de personal**>**Usuario**>**Agregar por lotes**.

Step 3 Seleccionar**Dispositivo**de**Dispositivo**y, a continuación, seleccione el dispositivo que desea

Step 4 agregar. Configure los siguientes parámetros.

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

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

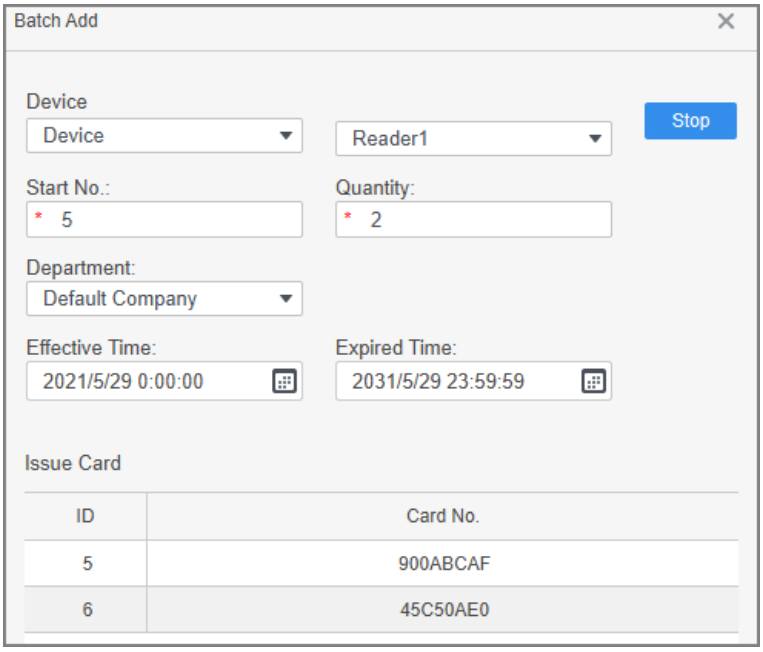
Step 5 Hacer clic**Asunto**.

El número de tarjeta se leerá automáticamente. Haga clic

Step 6 **Detener**Cuando termine de emitir tarjetas, haga clic en**DE**

Step 7 **ACUERDO**.

Figure 4-9 Agregar usuarios en lotes



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

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**Haga

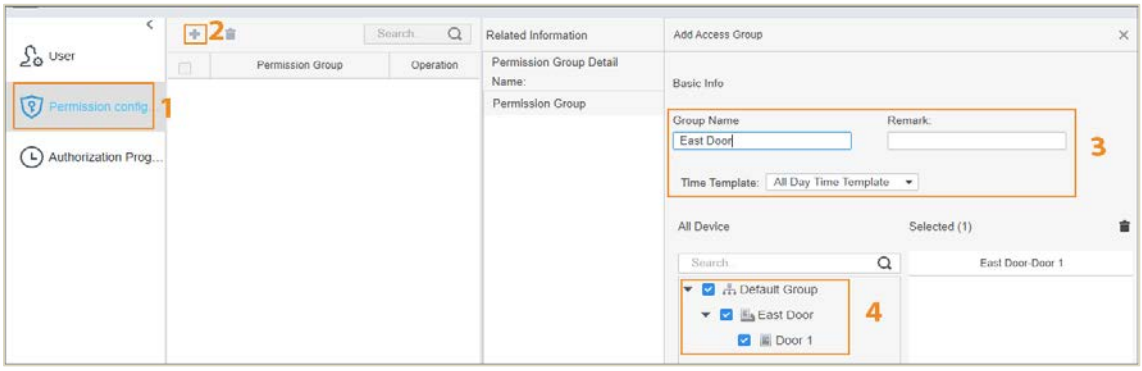
Step 3 clic en .

Step 4 Introduzca el nombre del grupo, las observaciones (opcionales) y seleccione una plantilla de tiempo.

Step 5 Seleccione los dispositivos.

Step 6 Hacer clic**DE ACUERDO**.

Figure 4-10 Crear un grupo de permisos



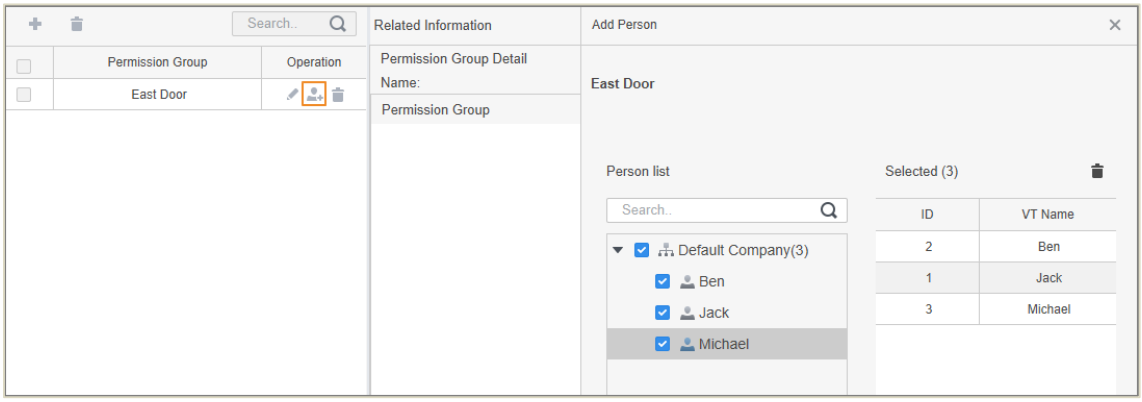
Step 7 Hacer clic del grupo de permisos que agregó.

Step 8 Seleccione los usuarios que desea agregar al grupo de permisos. Haga clic en**DE**

Step 9 **ACUERDO**.

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

Figure 4-11 Agregar usuarios a un grupo de permisos



Appendix 1 Instrucciones para el registro de huellas dactilares

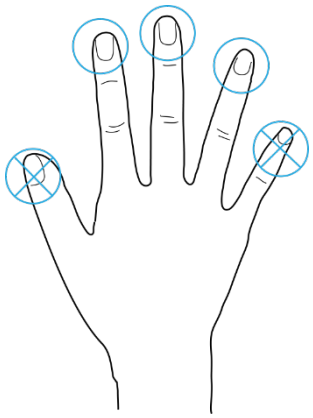
Al registrar la huella dactilar, preste atención a los siguientes puntos:

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

Se recomiendan los dedos

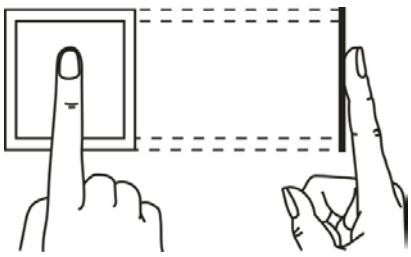
Se recomiendan los dedos índice, medio y anular. Los pulgares y meñiques no se pueden colocar fácilmente en el centro de la grabación.

Apéndice Figura 1-1 Dedos recomendados

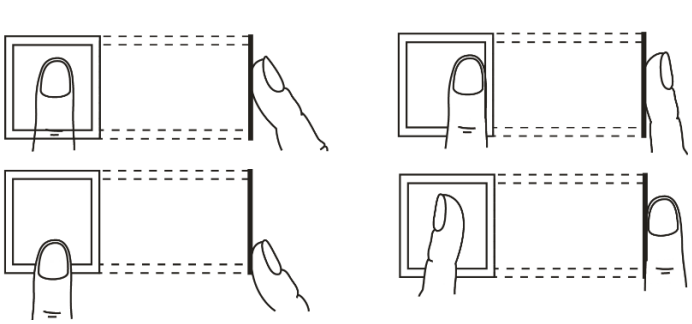


Cómo presionar su huella digital en el escáner

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. Utilice 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 incluya el nombre de la cuenta ni el nombre de la cuenta en orden inverso.
- No utilice caracteres continuos, como 123, abc, etc.
- No utilice caracteres 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 esté conectado a la red pública, se recomienda habilitar la función de "comprobación automática de actualizaciones" para obtener información oportuna sobre las actualizaciones de firmware publicadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "deseables de tener" para mejorar la seguridad de la red de su dispositivo: 2. Protección física

Le sugerimos que proteja físicamente el dispositivo, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales e implemente un control de acceso y una gestión de claves bien hechos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conectar sin autorización dispositivos extraíbles (como un disco flash USB, un puerto serial), etc.

3. Cambie las contraseñas periódicamente

Le sugerimos que cambie sus contraseñas periódicamente para reducir el riesgo de que sean adivinadas o descifradas.

4. Establezca y actualice la información de restablecimiento de contraseñas de manera oportuna

El dispositivo admite la función de restablecimiento de contraseña. Configure a tiempo la información relacionada con el restablecimiento de contraseña, incluido el buzón de correo del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección de contraseña, se recomienda no utilizar aquellas que se puedan adivinar fácilmente.

5. Habilitar bloqueo de cuenta

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

6. Cambiar el 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 externas puedan adivinar qué puertos está utilizando.

7. Habilitar HTTPS

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

8. Vinculación de direcciones MAC

Le recomendamos vincular la dirección IP y MAC del gateway al dispositivo, reduciendo así

el riesgo de suplantación de ARP.

9. Asignar cuentas y privilegios de manera razonable

Según los requisitos comerciales y de gestión, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

10. Desactivar servicios innecesarios y elegir modos seguros

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir 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 autenticación seguras.
- SMTP: Elija TLS para acceder al servidor de buzón. FTP:
- Elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

11. Transmisión de audio y vídeo encriptados

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 que los datos de audio y video sean robados durante la transmisión.

Recordatorio: la transmisión cifrada provocará cierta pérdida en la eficiencia de transmisión.

12. Auditoría segura

- Comprobar usuarios en línea: le sugerimos que compruebe periódicamente los usuarios en línea para ver si el dispositivo ha iniciado sesión sin autorización.
- Comprobar el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se utilizaron 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 un período prolongado, se recomienda que habilite la función de registro de red para garantizar que los registros críticos se sincronicen con el servidor de registro de red para realizar el seguimiento.

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 la red externa.
- La red debe estar dividida y aislada de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se recomienda utilizar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establecer 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 a los que se les permite acceder al dispositivo.