Acceso independiente

Manual de usuario

V1.0.0

Prefacio

General

Este manual presenta las funciones y operaciones de Access Standalone. Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	noviembre 2022

Aviso de protección de privacidad

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

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Por favor

póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.

- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si se produce algún problema durante el uso del dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado de Access Standalone, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar Access Standalone y cumpla con las pautas cuando lo use.

Requisito de transporte

Transporte, use y almacene Access Standalone en condiciones de humedad y temperatura permitidas.

Requisito de almacenamiento

Guarde Access Standalone en las condiciones de humedad y temperatura permitidas.

requerimientos de instalación

 **WARNING**

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

- El personal que trabaje en alturas debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque Access Standalone en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga Access Standalone alejado de la humedad, el polvo y el hollín.
- Instale Access Standalone en una superficie estable para evitar que se caiga.
- Instale Access Standalone en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o una fuente de alimentación de gabinete proporcionada por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumpla con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de suministro de energía están sujetos a la etiqueta Access Standalone.
- Access Standalone es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del Access Standalone esté conectada a una toma de corriente con conexión a tierra de protección.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de usar.

- No desenchufe el cable de alimentación del lateral de Access Standalone mientras el adaptador está encendido.
- Opere Access Standalone dentro del rango nominal de entrada y salida de energía.
- Utilice Access Standalone en condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquido sobre Access Standalone y asegúrese de que no haya ningún objeto lleno de líquido sobre Access Standalone para evitar que el líquido fluya hacia él.
- No desmonte el Access Standalone sin instrucción profesional.

Tabla de contenido

1 Descripción general del producto

1.1 Introducción

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

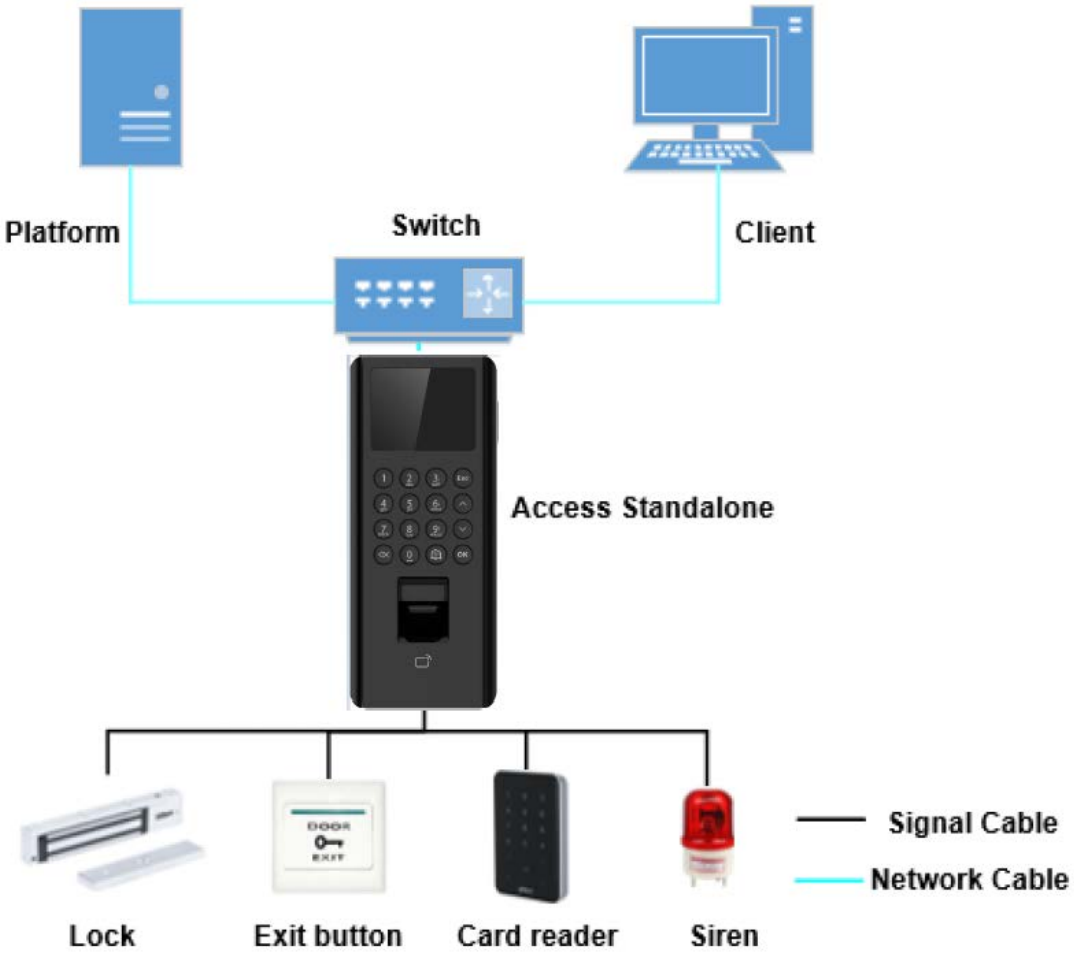
La función de huella digital está disponible en modelos selectos.

1.2 Aplicación

El es aplicable a una variedad de escenarios, como edificios de oficinas, escuelas, parques industriales, complejos de apartamentos, fábricas, estadios públicos y centros de negocios.

El siguiente diagrama es solo de referencia y puede diferir del producto real.

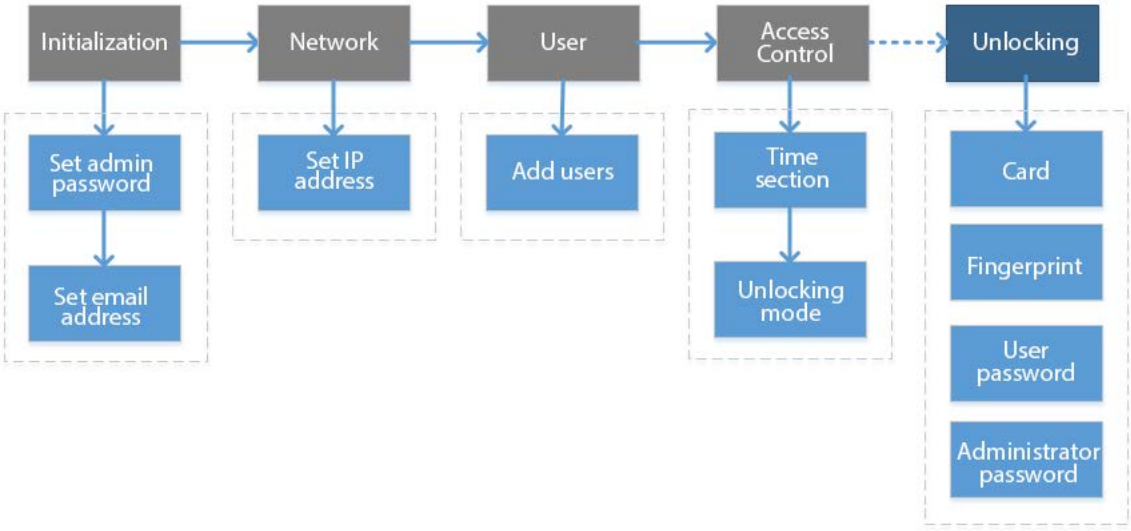
Figura 1-1 Diagrama de red



2 Configuración local

2.1 Proceso de configuración

Figura 2-1 Flujo de trabajo de configuración



2.2 Funciones del teclado

Tabla 2-1 Descripción del teclado

teclado	Descripción
número o carta	Introduzca información o seleccione menús.
∧	Utilice las teclas de flecha para navegar por los menús.
∨	
Esc	Cancele la selección o vuelva a la pantalla anterior.
DE ACUERDO	Ir a la pantalla seleccionada o confirmar los cambios.
	Ir a la pantalla del menú principal.
	Retroceso.
	Toque el timbre, pase a la página siguiente o cambie el método de entrada. El timbre puede funcionar solo cuando Access Standalone está en la pantalla de espera.

2.3 Pantalla de espera

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

- Access Standalone vuelve a la pantalla de espera si no se realiza ninguna operación en 30 segundos.
- Access Standalone apaga la pantalla si permanece en la pantalla de espera durante 30 segundos.
- La siguiente pantalla es solo de referencia y puede diferir del producto real.

Figura 2-2 Pantalla de espera

Tabla 2-2 Descripción de la pantalla de espera

No.	Artículo	Descripción
1	Estado	Muestra el estado de Wi-Fi, la red cableada (si existe) y la unidad USB.
2	Fecha & Tiempo	Hora y fecha.
3	Desbloquear el puerta con contraseña	Ingrese la ID de usuario y la contraseña, o ingrese la contraseña del administrador para desbloquear la puerta.
4	Desbloqueo métodos	Muestra los métodos de desbloqueo disponibles en Access Standalone.
5	Principal menú	Grifo para entrar en el menú principal. Solo cuenta de administrador y usuarios con la permiso de administrador puede acceder a la pantalla del menú principal. Para obtener más información, consulte "2.5 Inicio de sesión".

2.4 Inicialización

Para el uso por primera vez o después de restaurar los valores predeterminados de fábrica, debe configurar la contraseña y la dirección de correo electrónico para la cuenta de administrador. Puede usar la cuenta de administrador para iniciar sesión en el menú principal de Access Standalone y su página web.

Figura 2-3 Inicialización

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

2.5 Iniciar sesión

Inicie sesión en el menú principal para configurar Access Standalone. Solo la cuenta de administrador y la cuenta de administrador pueden ingresar al menú principal de Access Standalone. Para el uso por primera vez, use la cuenta de administrador para ingresar a la pantalla del menú principal y luego puede crear las otras cuentas de administrador.

Información de contexto

- Cuenta de administrador: puede iniciar sesión en la pantalla del menú principal de Access Standalone, pero no tiene permiso de acceso a la puerta.
- Cuenta de administrador: puede iniciar sesión en el menú principal de Access Standalone y tiene permisos de acceso a la puerta.

Procedimiento

Paso 1 En la pantalla de espera, toque∧y∨para seleccionar y luego toque**DE ACUERDO**.

Paso 2 Seleccione un método de verificación para ingresar al menú principal.

Los métodos de verificación pueden diferir según los modelos de Access Standalone.

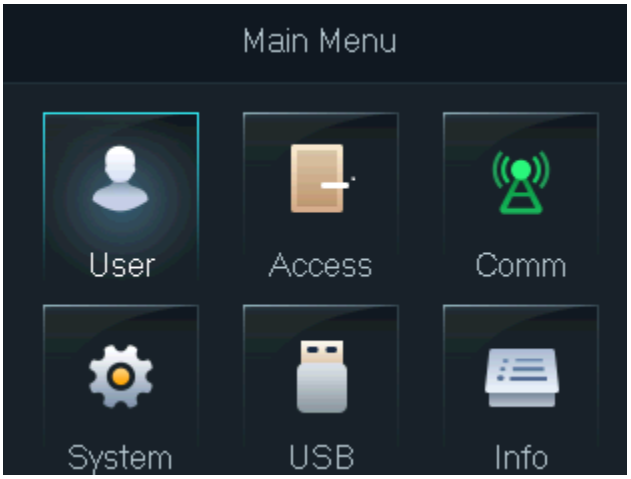
- Tarjeta: ingrese al menú principal deslizando la tarjeta.
- FP: Ingresa al menú principal a través de la huella digital.
- PWD: Introduzca el ID de usuario y la contraseña de la cuenta de administrador.
- Admin: ingrese la contraseña de administrador para ingresar al menú principal.

Paso 3 En el menú principal, toque∧o∨para navegar por los menús y luego toque**DE ACUERDO**para configurar el parámetros

Use los accesos directos para seleccionar los menús 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.

Figura 2-4 Menú principal



2.6 Red de comunicación

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

2.6.1 Configuración de IP

Establezca la dirección IP para Access Standalone para conectarlo a la red. Después de eso, puede iniciar sesión en la página web y en la plataforma de administración para administrar Access Standalone.

Procedimiento

Paso 1 En el menú principal, seleccione**Dirección IP de comunicación**y luego toque**DE**

Paso 2 **ACUERDO**. Seleccionar**Dirección IP**y toca**DE ACUERDO**para configurar parámetros.

Figura 2-5 Configurar IP

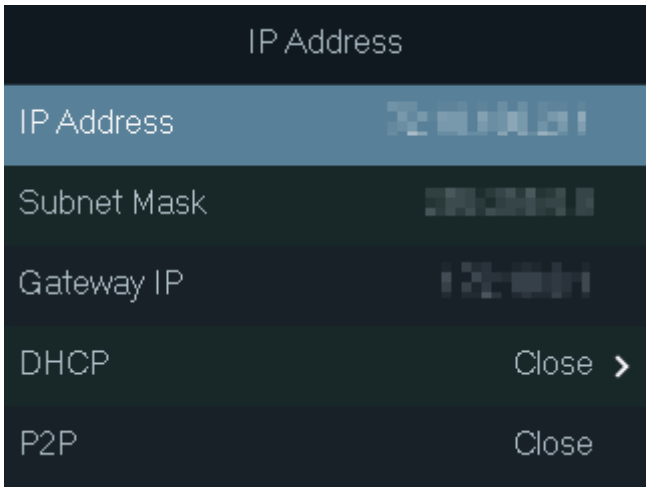


Tabla 2-3 Descripción de los parámetros de red

Parámetro	Descripción
Dirección IP/Subred Máscara/IP de puerta de enlace	La dirección IP, la máscara de subred y la dirección IP de la puerta de enlace deben estar en el mismo segmento de red.
DHCP	Significa Protocolo de configuración dinámica de host. Cuando DHCP está activado, Access Standalone se asignará automáticamente con la dirección IP, la máscara de subred y la puerta de enlace.
P2P	La tecnología P2P (peer-to-peer) permite a los usuarios administrar dispositivos sin solicitar DDNS, configurar el mapeo de puertos o implementar un servidor de tránsito.

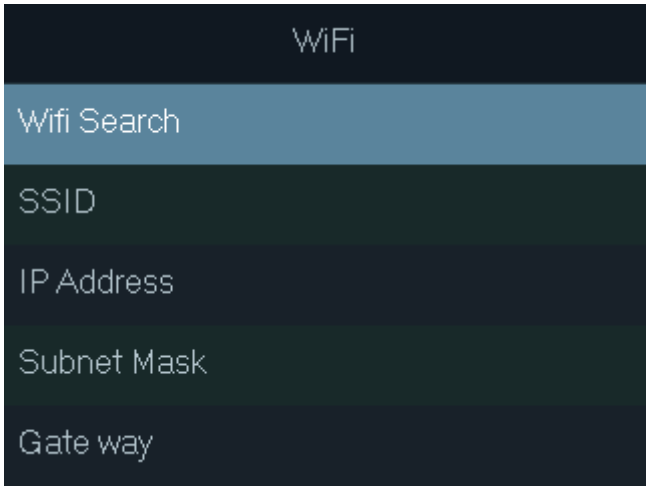
2.6.2 Configuración de WiFi

Conecte Access Standalone a una red inalámbrica. Wi-Fi solo está disponible en modelos seleccionados.

Procedimiento

Paso 1 En el menú principal, seleccione**CommWi-Fi**y luego toque**DE ACUERDO**.

Figura 2-6 Wifi



Paso 2 Seleccionar**Wifi**>**Buscar**y luego toque**DE ACUERDO**.

Paso 3 Seleccionar**Wifi**y luego toque**DE ACUERDO**para habilitar la función Wi-Fi.

Access Standalone buscará y mostrará todas las redes inalámbricas disponibles.

Grifo  O  para ir a la página anterior o siguiente.

Etapa 4 Seleccione una red inalámbrica, toque**DE ACUERDO**e ingrese la contraseña.

2.6.3 Configuración de Wiegand

Configure la entrada o salida Wiegand para conectar un lector de tarjetas o Access Standalone. En el menú principal, seleccione**comunicación**>**Wiegand**y luego toque**DE ACUERDO**.

- Seleccionar**Entrada Wiegand**cuando conecta un lector de tarjetas externo al Access Standalone.
- Seleccionar**Salida Wiegand**cuando Access Standalone funciona como un lector de tarjetas y necesita conectarlo a un controlador u otro terminal de acceso.

Tabla 2-4 Descripción de los parámetros de Wiegand

Parámetro	Descripción
Tipo de salida	Seleccione un formato Wiegand para leer números de tarjeta o números de identificación. ● **Wiegand26**: Lee 3 bytes o 6 dígitos. ● **Wiegand34**: Lee 4 bytes u 8 dígitos. ● **Wiegand66**: Lee 8 bytes o 16 dígitos.
Ancho de pulso	Ingrese el ancho de pulso y el intervalo de pulso de la salida Wiegand.
Intervalo de pulso	
Tipo de datos de salida	Seleccione el tipo de datos de salida. ● **ID de usuario**: genera datos basados en el ID de usuario. ● **número de tarjeta**: genera datos basados en el primer número de tarjeta del usuario y el formato de datos es hexadecimal o decimal.

2.6.4 Configuración del puerto serie

En el menú principal, seleccione**Puerto serie de comunicaciones**y luego toque**DE ACUERDO**.

- Seleccionar**Entrada en serie**cuando Access Standalone se conecta a un lector de tarjetas.
- Seleccionar**Salida en serie**cuando Access Standalone funciona como un lector de tarjetas, y Access Standalone enviará datos a Access Standalone para controlar el acceso a la puerta.
  - ◇ **ID de usuario**: genera datos basados en el ID del usuario.
  - ◇ **número de tarjeta**: Emite datos basados en el número de tarjeta cuando los usuarios deslizan la tarjeta para desbloquear la puerta.
- Seleccionar**Entrada OSDP**cuando Access Standalone está conectado a un lector de tarjetas basado en el protocolo OSDP.

2.6.5 Modos de configuración

Establezca Access Standalone en modo lector de tarjetas o modo controlador.

Procedimiento

Paso 1 En el menú principal, seleccione**comunicación**>**Configuración de modo**y luego toque**DE ACUERDO**.

Paso 2 Seleccione el modo.

- Seleccionar**Controlador**cuando se conecta a un lector de tarjetas.
- Seleccionar**Lector de tarjetas**cuando Access Standalone funciona como un lector de tarjetas y necesita conectarlo a un controlador u otro terminal de acceso. En este modo, RS-485 no es compatible.

En el**Lector de tarjetas**modo, no puede establecer la entrada en serie. PUERTA_COM y PUERTA_NC conéctese a la CAJA y GND del Access Standalone externo para la alarma antimanipulación.

Paso 3 Seleccionar**Configuración de la tasa de baudios**para establecer la velocidad en baudios.

- En el**Lector de tarjetas**modo, la velocidad en baudios se ajusta automáticamente de acuerdo con el acceso independiente.
- En el**Controlador**modo, puede establecer la velocidad en baudios. El baudio del Access Standalone debe ser el mismo que el del dispositivo externo para una comunicación exitosa.

2.7 Gestión de usuarios

Puede agregar nuevos usuarios, ver la lista de usuarios/administradores y editar la información del usuario.

2.7.1 Agregar nuevo usuario

Procedimiento

Paso 1 Grifo∧o∨para seleccionar en la pantalla de espera y luego toque**DE ACUERDO**.

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

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

Figura 2-7 Agregar un nuevo usuario

Paso 3 Configure los parámetros.

Tabla 2-5 Descripción de los parámetros de usuario

Parámetro	Descripción
IDENTIFICACIÓN	Cada ID de usuario es único. Puede ser de 18 caracteres de números, letras o su combinación.
Nombre	Introduzca el nombre (un máximo de 32 caracteres, incluidos números, símbolos y letras).

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

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

Paso 5 **ACUERDO**para guardar los cambios.

2.7.2 Visualización de la información del usuario

Puede ver y buscar todos los usuarios generales y usuarios administradores, y editar la información del usuario. En el menú principal, seleccione**Usuario**>**Lista de usuarios/Lista de administradores**, se muestran todos los usuarios agregados.

Figura 2-8 Lista de usuarios

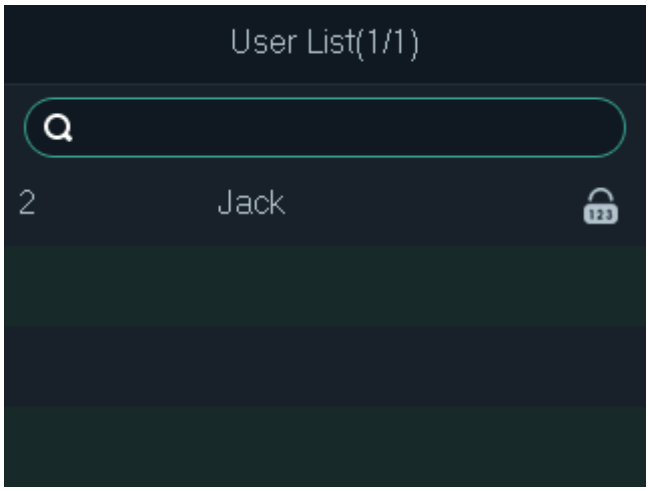
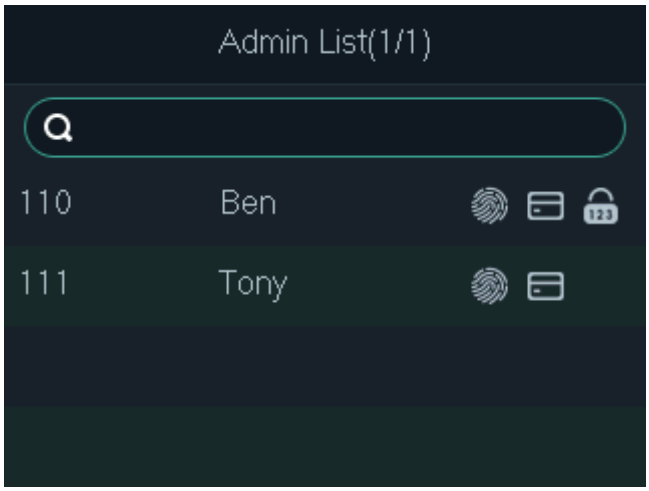


Figura 2-9 Lista de administradores



- : Huella dactilar
- : Tarjeta
- : Contraseña

Editar información de usuario

1. Seleccione el usuario y luego toque**DE ACUERDO**。

2. Edite la información del usuario.

3. Toque**Esc**y luego toque**DE ACUERDO**para guardar los cambios.

Buscar usuarios

1. Seleccione y luego toque**DE ACUERDO**.

2. Ingrese la ID del usuario, deslice la tarjeta o coloque el dedo en el escáner de huellas dactilares para buscar al usuario.

Eliminar usuarios

1. Seleccione el usuario y luego toque**DE ACUERDO**.

2. Seleccione para eliminar el usuario.

2.7.3 Configuración de la contraseña de administrador

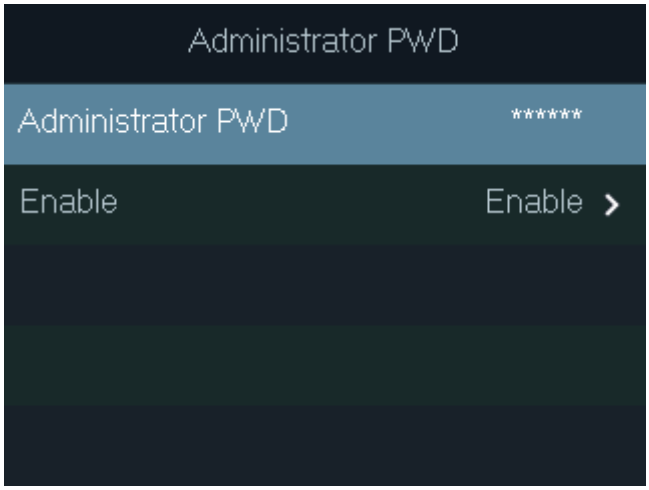
Puede desbloquear la puerta ingresando solo la contraseña de administrador. La contraseña de administrador no está limitada por los tipos de usuario. Solo se permite una contraseña de administrador para el dispositivo, pero puede configurar 100 contraseñas de administrador a través de la plataforma.

Procedimiento

Paso 1 En el menú principal, seleccione**Usuario**>**PCD del administrador**

Paso 2 Ingrese la contraseña del administrador y luego toque**DE ACUERDO**.

Figura 2-10 Contraseña de administrador

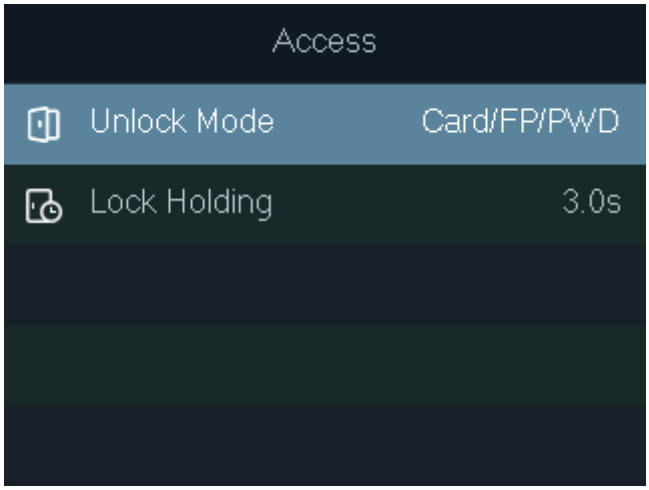


Paso 3 Seleccionar**Permitir**y luego toque**DE ACUERDO**para habilitar la función.

2.8 Gestión de control de acceso

Configure el modo de desbloqueo y la duración del desbloqueo.

Figura 2-11 Gestión de control de acceso



2.8.1 Configuración de los modos de desbloqueo

Configura las combinaciones de desbloqueo. Use tarjeta, huella digital, contraseña o sus combinaciones para desbloquear la puerta. Los métodos de desbloqueo pueden diferir según los modelos de Access Standalone.

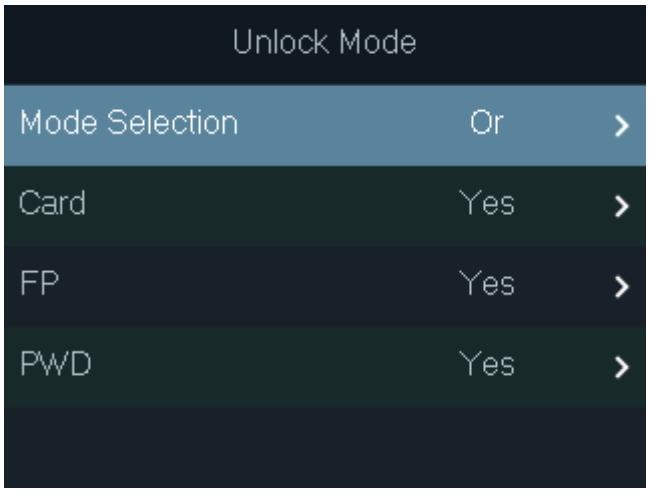
Procedimiento

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

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

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

Figura 2-12 Elemento (opción múltiple)



Paso 3 Grifo**Esc**.

Etapa 4 Grifo**DE ACUERDO**para guardar los cambios.

2.8.2 Configuración del tiempo de espera de bloqueo

La puerta permanecerá desbloqueada durante el tiempo definido para el paso de personas.

Procedimiento

Paso 1 En el menú principal, seleccione**Acceso**>**bloqueo de retención**. Grifo**DE**

Paso 2 **ACUERDO**y, a continuación, introduzca la hora.

Grifo para cambiar el método de entrada.

2.9 Desbloqueo de la puerta

2.9.1 Desbloqueo por Tarjetas

Pase su tarjeta para desbloquear la puerta.

2.9.2 Desbloqueo por Huella Dactilar

Coloque su dedo en el escáner de huellas dactilares para desbloquear la puerta.

2.9.3 Desbloqueo por contraseña de usuario

Introduzca el ID de usuario y la contraseña para desbloquear la puerta. El procedimiento de desbloqueo puede diferir según la serie de Access Standalone.

Serie ASI22XXH

1. En la pantalla de espera, toque∧y∨para seleccionar y luego toque**DE ACUERDO**.
2. Seleccione**PCD**y luego toque**DE ACUERDO**.
3. Ingrese la ID de usuario y luego toque**DE ACUERDO**.

   Puede tocar pa cambiar el método de entrada.
4. Seleccione**PCD**, ingrese la contraseña y luego toque**DE ACUERDO**.
5. Seleccione**DE ACUERDO**y luego toque**DE ACUERDO**.

Serie ASI22XXJ

1. En la pantalla de espera, toque∧y∨para seleccionar y luego toque**DE ACUERDO**.
2. Seleccione**PCD**y luego toque**DE ACUERDO**.
3. Ingrese la ID de usuario y luego toque**DE ACUERDO**.
   - Puedes tocar para cambiar el método de
   - Puedes tocar entrada. borrar.
4. Ingrese la contraseña y luego toque**DE ACUERDO**.
5. Toque**DE ACUERDO**

2.9.4 Desbloqueo por contraseña de administrador

Información de contexto

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

Para usar la contraseña de administrador para el acceso a la puerta, debe activar la función. Para más detalles, consulte "2.7.3 Configuración de la contraseña de administrador".

Procedimiento

Paso 1 Seleccionar en la pantalla de espera.

Paso 2 Seleccionar**PCD del administrador**y luego toque**DE ACUERDO**.

Paso 3 Introduzca la contraseña de administrador. Seleccionar**DE ACUERDO**y luego toque**DE ACUERDO**.

Etapa 4 La puerta está desbloqueada.

2.10 Configuración del sistema

2.10.1 Configuración de la hora

Configure la hora de Access Standalone, como la fecha, la hora y el formato de fecha.

Procedimiento

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

Paso 2 Seleccione un parámetro y luego toque**DE ACUERDO**para editarlo.

Figura 2-13 Configuración de tiempo

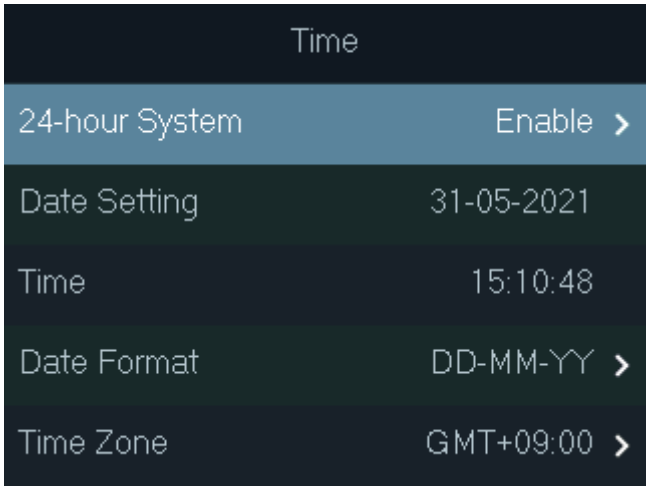


Tabla 2-6 Descripción de los parámetros de tiempo

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

2.10.2 Configuración del volumen

Ajuste el volumen del mensaje de voz.

Procedimiento

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

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

2.10.3 Restauración de valores predeterminados de fábrica

Procedimiento

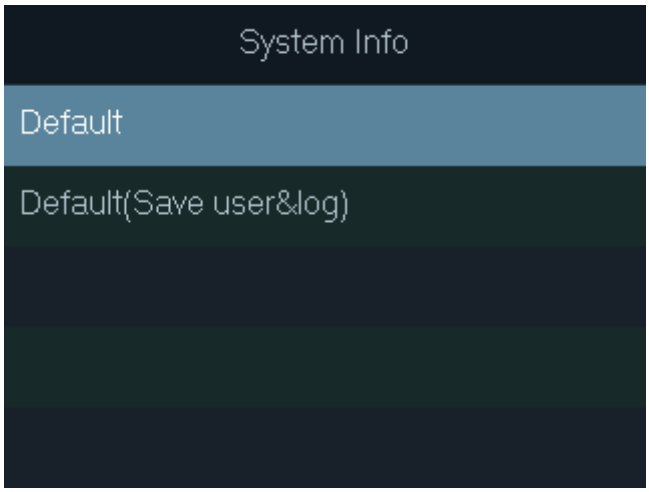
Paso 1 En el menú principal, seleccione**Sistema**>**Restaurar Fábrica**y luego toque**DE ACUERDO**. Seleccione

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

Restaurar los valores predeterminados de fábrica podría provocar la pérdida de datos. Por favor tenga en cuenta.

- **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.

Figura 2-14 Restaurar a la 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 antes de exportar la información del usuario o actualizarla. sistema. Para evitar fallas, no extraiga la unidad flash USB ni realice ninguna operación durante el proceso.
- Si desea importar datos de uno a otro, debe exportar los datos a una unidad flash USB primero.

Puede usar una unidad flash USB para actualizar Access Standalone y exportar o importar información de usuario.

2.11.1 Exportando a USB

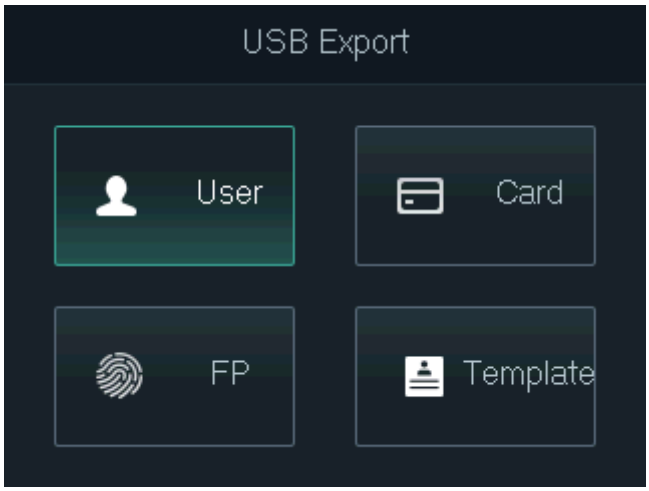
Exporte datos del dispositivo a una unidad flash USB. Los datos exportados están encriptados y no se pueden editar.

Procedimiento

Paso 1 En el menú principal, seleccione**USB**Exportación USBy luego toque**DE ACUERDO**

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

Figura 2-15 Exportar datos a la unidad USB



Paso 3 Grifo**DE ACUERDO**.

Los datos seleccionados se exportan a la unidad flash USB.

2.11.2 Importación desde USB

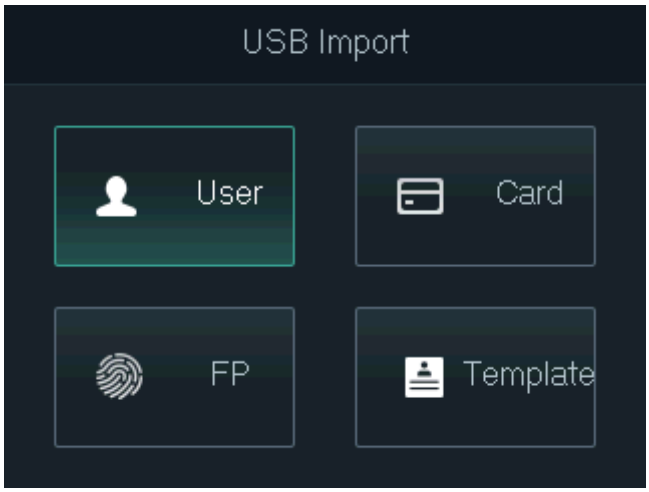
Puede importar datos desde USB al dispositivo.

Procedimiento

Paso 1 En el menú principal, seleccione**Importación USBUSB**y luego toque**DE ACUERDO**.

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

Figura 2-16 Importar datos desde la unidad flash USB



Paso 3 Grifo**DE ACUERDO**.

Los datos seleccionados se importan al dispositivo.

2.11.3 Sistema de actualización

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

Procedimiento

Paso 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.

Paso 2 En el menú principal, seleccione**Actualización de USBUSB**. Grifo**DE**

Paso 3 **ACUERDO**.

El dispositivo se reiniciará cuando se complete la actualización.

2.11.4 Exportación de registros de desbloqueo

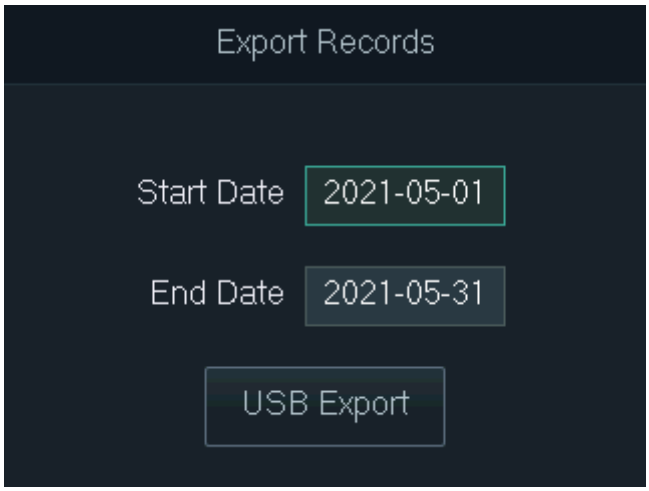
Exporte registros de desbloqueo a una unidad flash USB.

Procedimiento

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

Paso 2 Selecciona la hora.

Figura 2-17 Exportar registros de desbloqueo



Paso 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 de usuario

Puede importar o exportar información de usuario, incluidas tarjetas y huellas dactilares.

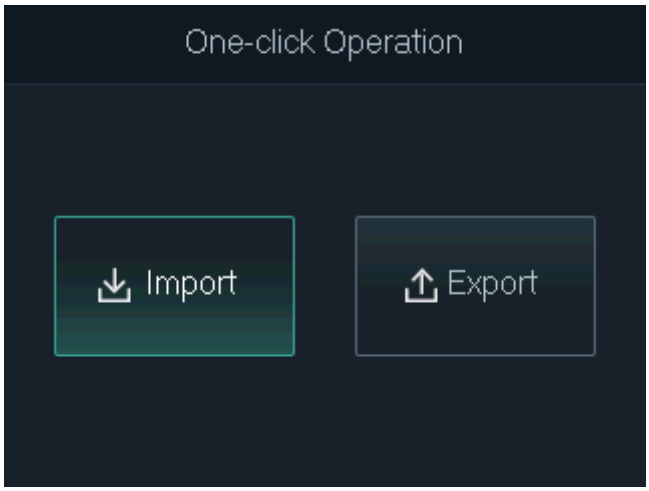
Procedimiento

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

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

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

Figura 2-18 Importar/exportar información de usuario



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

3 Configuraciones Web

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

3.1 Web en la computadora

3.1.1 Inicialización

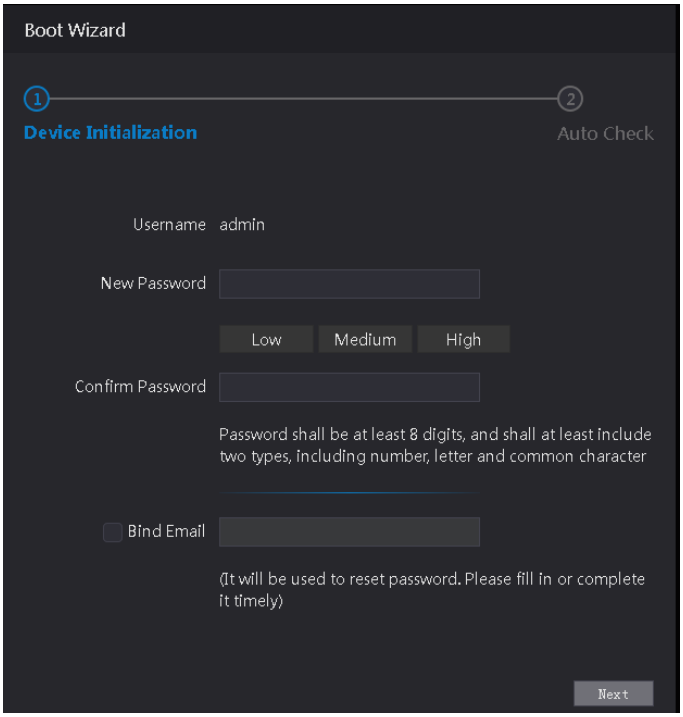
Debe establecer una contraseña y vincular una dirección de correo electrónico antes de iniciar sesión en la web por primera vez.

Procedimiento

Paso 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.

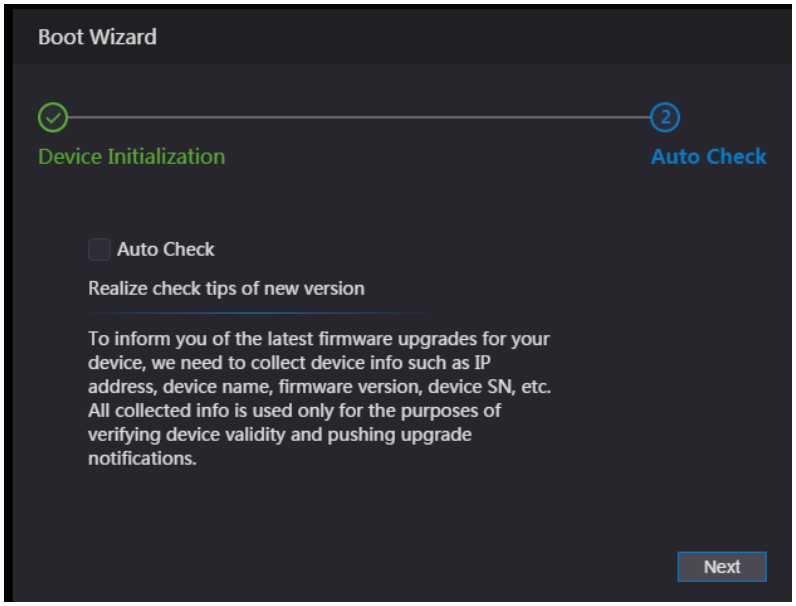
Figura 3-1 Inicialización



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

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

Figura 3-2 Comprobación automática



Paso 3 Hacer clic**Próximo**.

Etapa 4 (Opcional) Seleccione**Verificación automática**.

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

Paso 5 Hacer clic**Próximo**.

Paso 6 Hacer clic**Completo**.

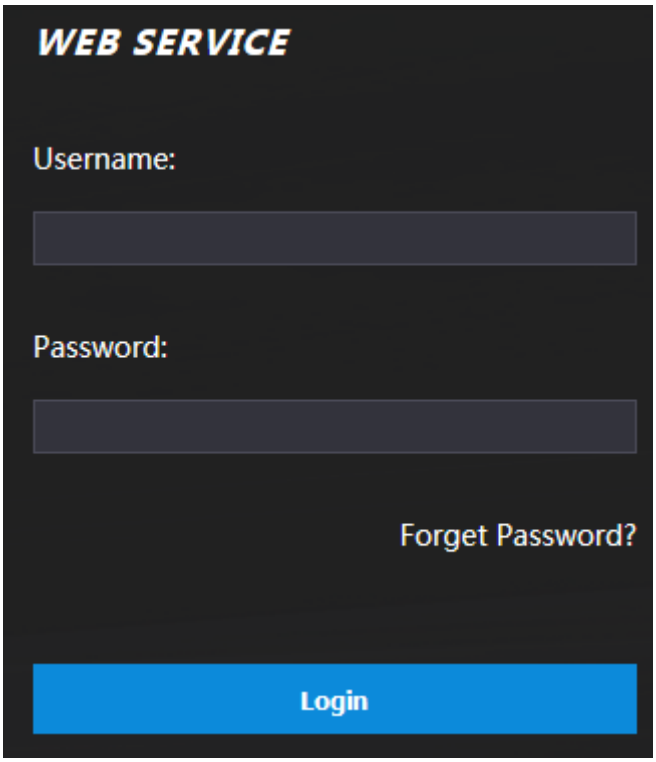
3.1.2 Iniciar sesión

Procedimiento

Paso 1 Vaya a la dirección IP (192.168.1.108 por defecto) de Access Standalone en el navegador y presione la tecla Enter.

Asegúrese de que la computadora esté en la misma LAN que Access Standalone.

Figura 3-3 Inicio de sesión



Paso 2 Introduzca el nombre de usuario y la contraseña.

- El nombre de administrador predeterminado es admin, y la contraseña es la que estableció durante inicialización Le recomendamos que cambie la contraseña de administrador regularmente para aumentar la seguridad.
- Si olvidó la contraseña de administrador, haga clic en**¿Contraseña olvidada?**para restablecerlo. Para detalles, consulte "3.1.3 Restablecimiento de la contraseña".

Paso 3 Hacer clic**Acceso**.

3.1.3 Restablecimiento de la contraseña

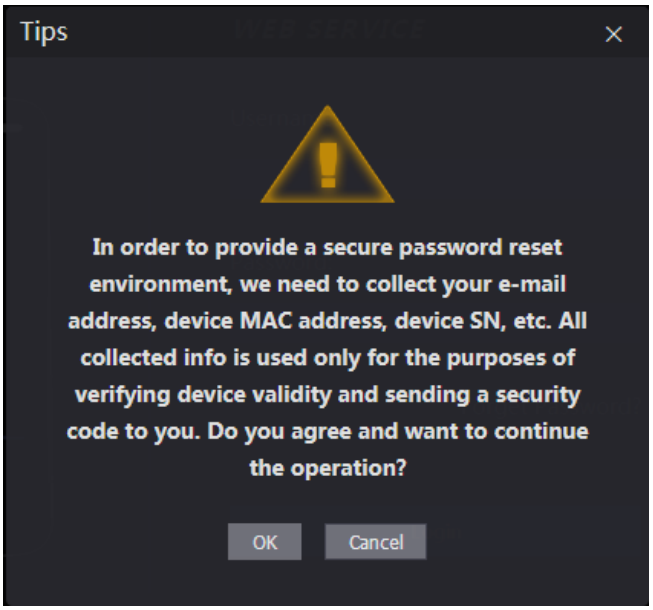
Al restablecer la contraseña de la cuenta de administrador, se requiere su dirección de correo electrónico.

Procedimiento

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

Paso 2 **contraseña**. Lea atentamente el mensaje y haga clic en**DE ACUERDO**.

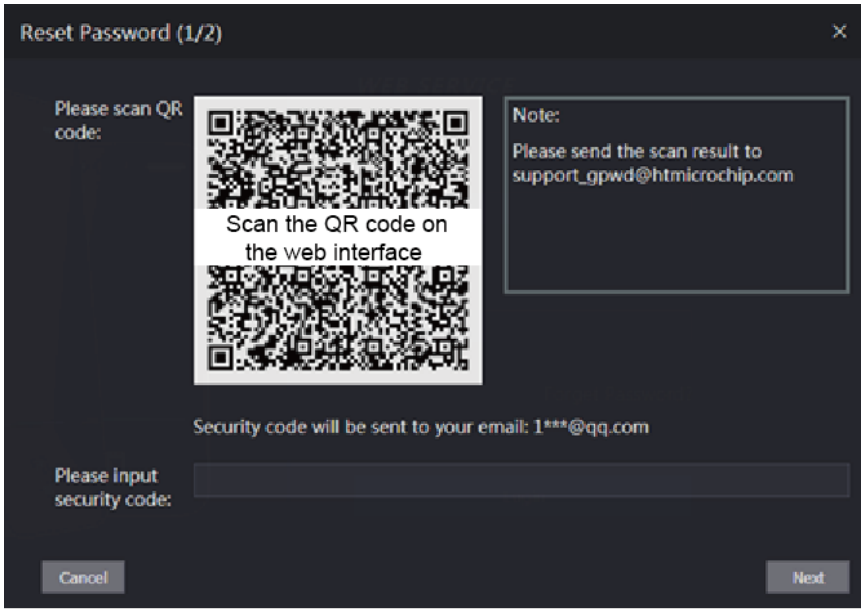
Figura 3-4 Indicación de reinicio



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

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

Figura 3-5 Restablecer contraseña



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

Paso 5 clic**Próximo**.

Paso 6 Restablece y confirma la nueva contraseña.

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

Paso 7 Hacer clic**DE ACUERDO**para completar el restablecimiento.

3.1.4 Configuración de parámetros de puerta

Configure los parámetros de control de acceso.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Parámetro de la puerta**.

Figura 3-6 Parámetro de puerta

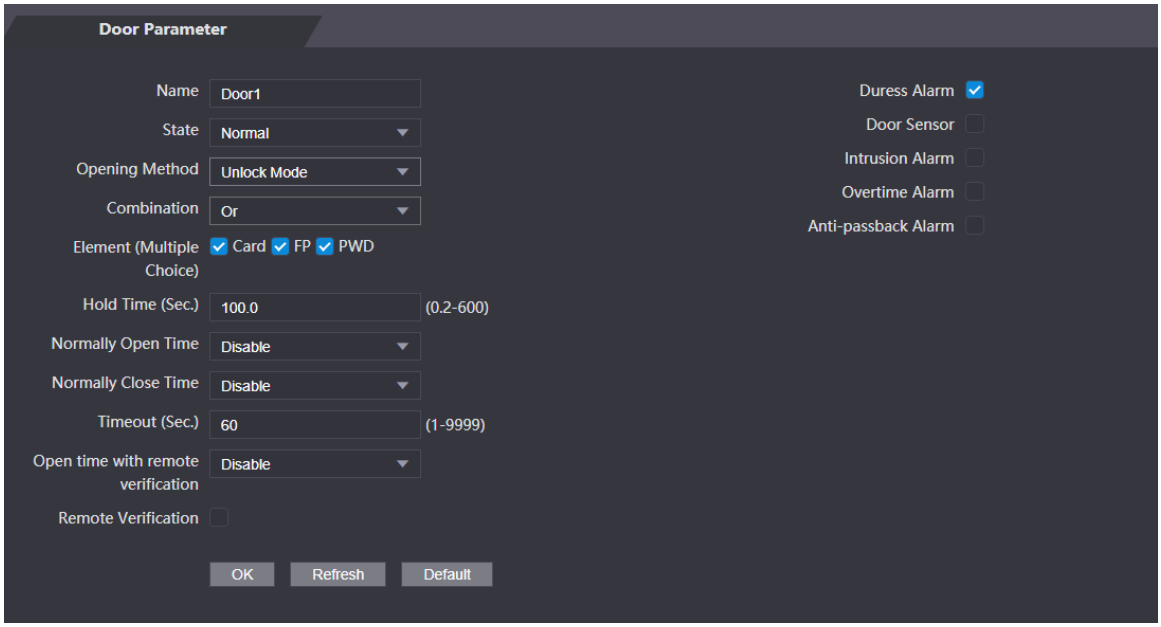


Tabla 3-1 Descripción de los parámetros de la puerta

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

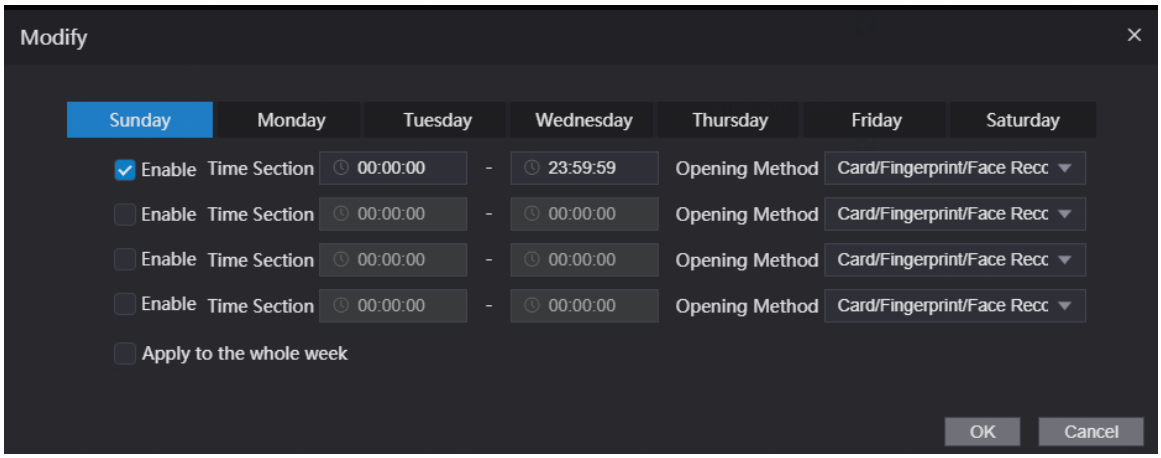
Parámetro	Descripción
Hora normalmente cerrada	
Tiempo de espera (seg.)	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante más tiempo que este valor.
Verificación remota	Configure el período de apertura de la puerta de verificación remota. Para más detalles, consulte "3.1.6.1 Configuración de las secciones de tiempo". Cuando se autoriza la apertura de una puerta en el dispositivo, debe confirmarse en la plataforma antes de que se pueda abrir.
alarma de coacción	Se activará una alarma cuando se use una tarjeta de coacción o una contraseña de coacción para abrir la puerta.
sensor de puerta	Las alarmas de intrusión y horas extras pueden activarse solo después de **sensor de puerta**está habilitado.
Alarma de intrusión	Cuando**sensor de puerta**está habilitado, se activará una alarma de intrusión si la puerta se abre de manera anormal.
Alarma de horas extras	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante más tiempo que el**Tiempo de espera (seg)**, que va de 1 a 9999 segundos.
Alarma anti-retorno	Si está habilitado, los usuarios deben verificar las identidades tanto para la entrada como para la salida; de lo contrario, se activará una alarma. ● Si una persona ingresa con verificación y sale sin verificación, se activará una alarma cuando intente desbloquear nuevamente y se negará el acceso al mismo tiempo. ● Si una persona ingresa sin verificación y sale con verificación, se activará una alarma cuando intente desbloquear nuevamente y se negará el acceso al mismo tiempo.

Paso 3 Configure el método de desbloqueo.

● Sección de tiempo

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

Figura 3-7 Parámetro de la sección de tiempo



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

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

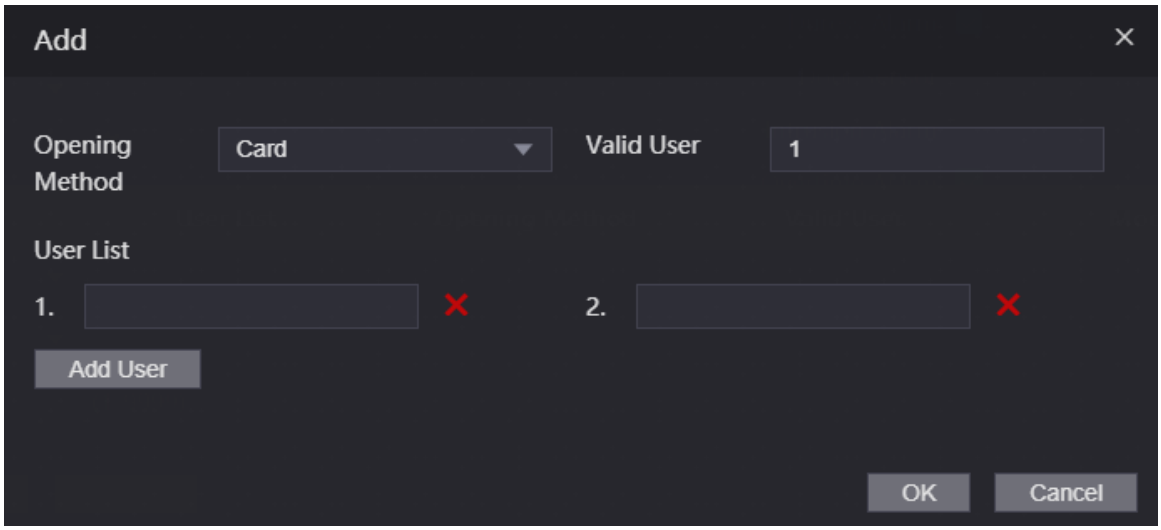
4) Haga clic**DE ACUERDO**.

- multitarjeta

1) Haga clic**Agregar**.

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

Figura 3-8 Parámetro multitarjeta



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

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

- Modo de desbloqueo

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

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

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

Etapa 4 Configurar otros parámetros.

Paso 5 Hacer clic**DE ACUERDO**.

3.1.5 Enlace de alarma

3.1.5.1 Configuración de enlaces de alarma

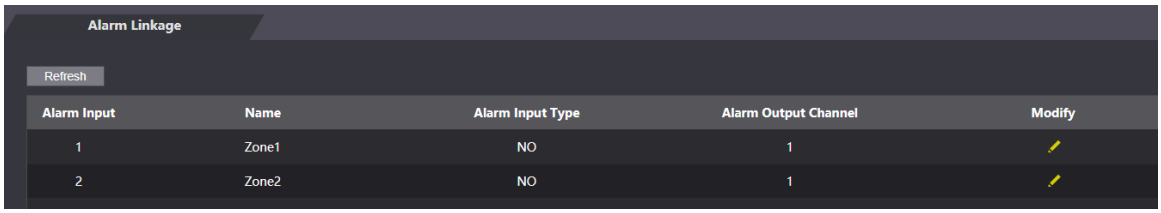
Los dispositivos de entrada de alarma se pueden conectar al dispositivo y se pueden modificar los parámetros de enlace de alarma.

Procedimiento

Paso 1 Inicie sesión en la página web.

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

Figura 3-9 Enlace de alarma



Paso 3 Hacer clic para configurar el enlace de alarma.

Figura 3-10 Modificar parámetros de vinculación

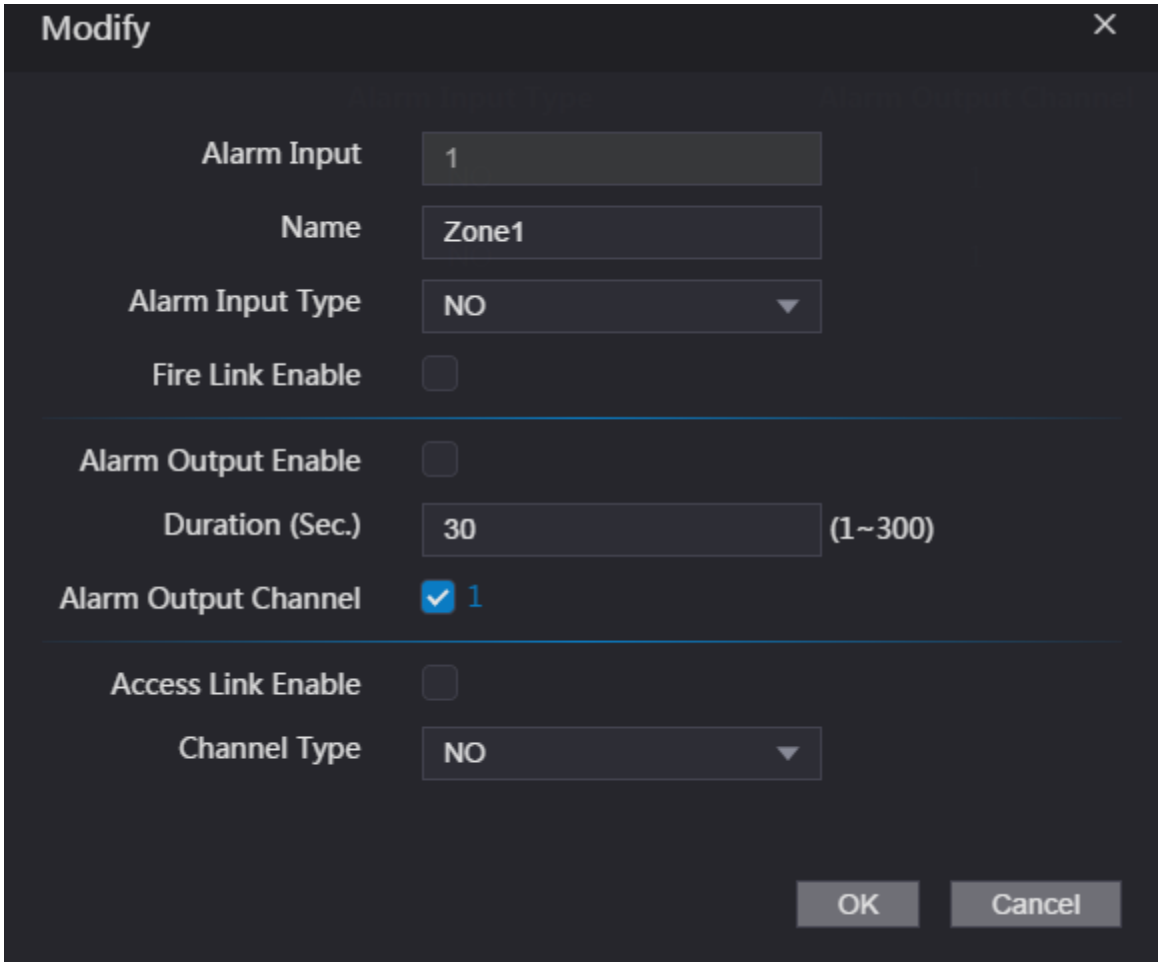


Tabla 3-2 Descripción de los parámetros de vinculación de alarmas

Parámetro	Descripción
Entrada de alarma	No puede modificar el valor. Manténgalo predeterminado.
Nombre	Introduzca un nombre de zona.
Tipo de entrada de alarma	Seleccione el tipo según el dispositivo de alarma. ● **NO**: El circuito del dispositivo de alarma normalmente está abierto y se cierra cuando se activa una alarma. ● **CAROLINA DEL NORTE**: El circuito del dispositivo de alarma normalmente está cerrado y se abre cuando se activa una alarma.

Parámetro	Descripción
Habilitar enlace de fuego	Si el enlace de incendio está habilitado, el dispositivo generará alarmas de incendio cuando se active. Los mensajes de alarma se muestran en el registro de alarmas. Si el enlace de incendio está habilitado, la salida de alarma y el enlace de acceso son NO por defecto.
Habilitar salida de alarma	Si la salida de alarma está habilitada, el relé puede generar mensajes de alarma.
Duración (seg.)	Duración de la alarma. Va desde 1 s hasta 300 s.
Canal de salida de alarma	El dispositivo tiene un solo canal de salida. Seleccione el canal de salida de acuerdo con su dispositivo de alarma.
Habilitar enlace de acceso	Si el enlace de acceso está habilitado, el dispositivo estará normalmente encendido o normalmente cerrado cuando haya señales de alarma de entrada.
Tipo de canal	Hay dos opciones: NO y NC.

Etapa 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 Visualización de registros de alarma

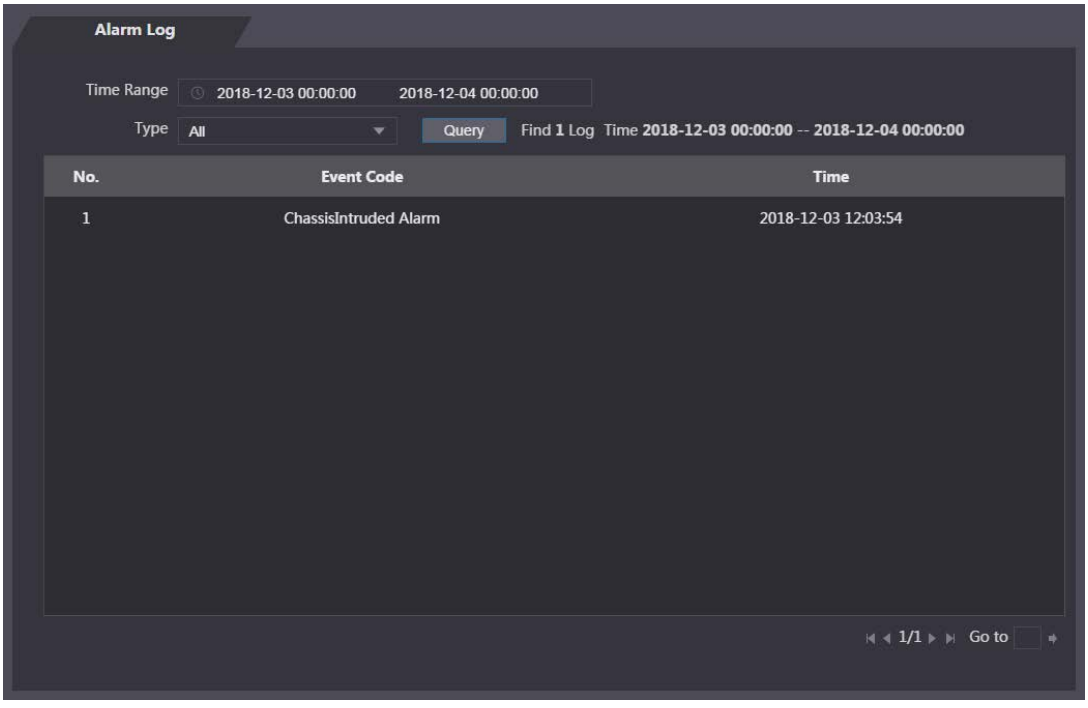
Procedimiento

Paso 1 Inicie sesión en la página web.

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

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

Figura 3-11 Resultados de la consulta



3.1.6 Secciones de tiempo

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

3.1.6.1 Configuración de las secciones de tiempo

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

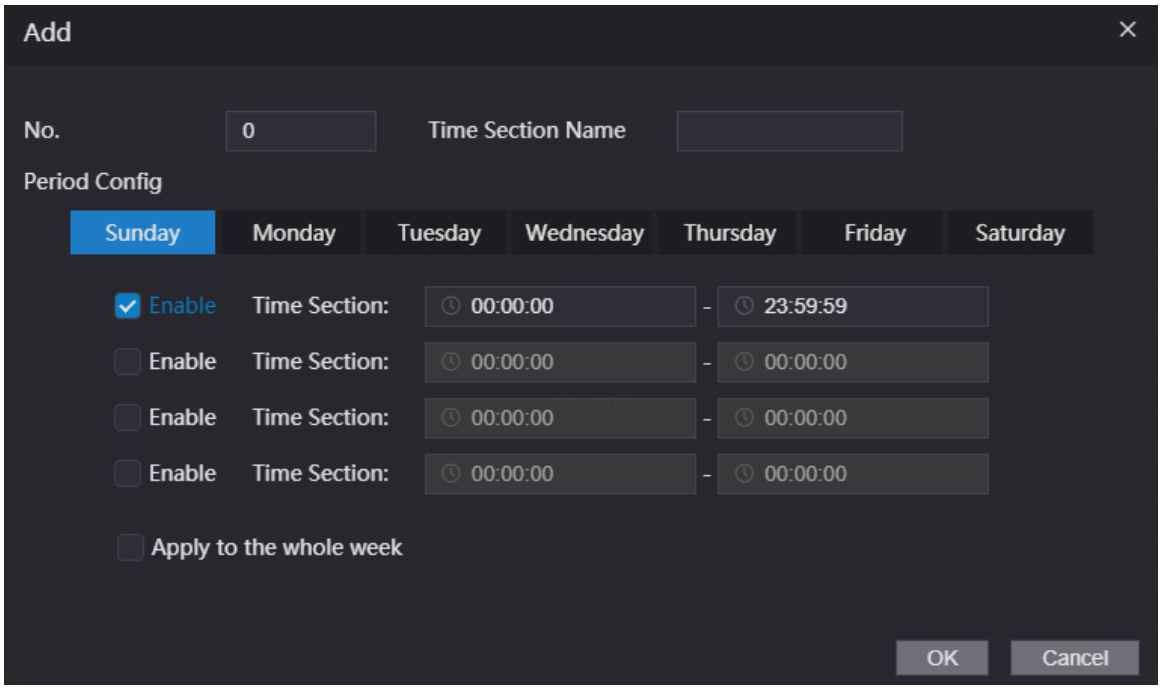
Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Sección de tiempo**>**Sección de tiempo**.

Paso 3 Hacer clic**Agregar**.

Figura 3-12 Parámetros de la sección de tiempo



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

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

Paso 5 Configure las secciones de tiempo para cada día.

Paso 6 Puede configurar hasta cuatro tramos de tiempo para un solo día.

Paso 7 (Opcional) Haga clic en**Aplica para toda la semana**para copiar la configuración al resto de días. Hacer clic**DE**

Paso 8 **ACUERDO**para guardar los cambios.

3.1.6.2 Configuración de grupos de vacaciones

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

en los tramos de tiempo definidos.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Sección de tiempo**>**Grupo de vacaciones**>**Configuración**.

Paso 3 Hacer clic**Agregar**.

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

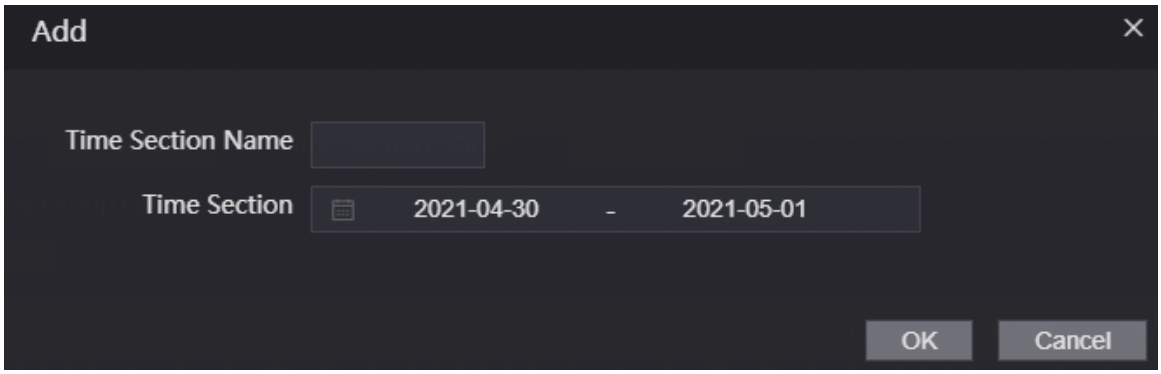
- **No.**: Introduzca un número de sección. Va de 0 a 127.
- **Nombre de la sección de tiempo**: Ingrese un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (que contengan números, caracteres especiales y caracteres ingleses).

Paso 5 Hacer clic**Agregar**.

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

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

Figura 3-13 Agregar un feriado



Paso 7 Hacer clic**DE ACUERDO**.

3.1.6.3 Configuración de planes de vacaciones

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

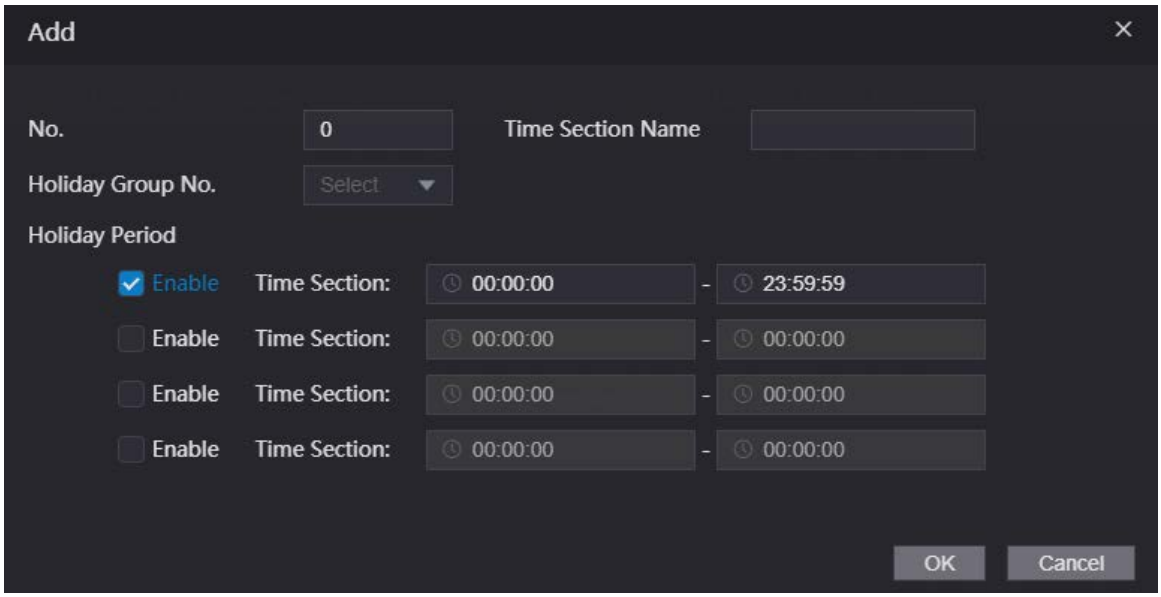
Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Sección de tiempo**>**Plan de vacaciones**>**Configuración**. Hacer clic

Paso 3 **Agregar**.

Figura 3-14 Agregar un plan de vacaciones



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

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

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

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

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

Paso 7 Hacer clic**DE ACUERDO**.

3.1.7 Capacidad de datos

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

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Capacidad de datos**.

3.1.8 Configuración del volumen

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Hacer clic**Configuración de volumen**y ajuste el volumen. Hacer clic**DE**

Paso 3 **ACUERDO**.

3.1.9 Configuración de red

3.1.9.1 Configuración de TCP/IP

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

requisitos previos

Asegúrese de que el dispositivo esté conectado a la red.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccionar

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

3.1.9.2 Configuración del puerto

Puede limitar el acceso a Access Standalone al mismo tiempo a través de la página web, el cliente de escritorio y más.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccionar

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

Paso 3 el número de puerto.

Excepto**Conexión máxima**y**Puerto RTSP**, debe reiniciar Access Standalone para hacer efectivas las configuraciones después de cambiar otros parámetros.

Tabla 3-3 Descripción de los puertos

Parámetro	Descripción
Conexión máxima	Puede establecer la cantidad máxima de clientes (como la página web, el cliente de escritorio) que pueden acceder a Access Standalone al mismo tiempo.
Puerto TCP	El valor predeterminado es 37777.
Puerto HTTP	El valor predeterminado es 80. Si desea cambiar el número de puerto, agregue el nuevo número de puerto después de la dirección IP cuando inicie sesión en la página web.
Puerto HTTPS	El valor predeterminado es 443.
Puerto RTSP	El valor predeterminado es 554.

Etapa 4 Hacer clic**DE ACUERDO**para completar el ajuste.

3.1.9.3 Configuración del registro automático

Access Standalone informa su dirección al servidor designado para que pueda acceder a Access Standalone a través de la plataforma de administración.

Procedimiento

Paso 1 Inicie sesión en la página web.

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

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

Tabla 3-4 Descripción del registro automático

Parámetro	Descripción
IP del anfitrión	La dirección IP o el nombre de dominio del servidor.
Puerto	El puerto del servidor utilizado para el registro automático.
ID de subdispositivo	Introduzca el ID del subdispositivo (definido por el usuario). Cuando agrega Access Standalone a la plataforma de administración, el ID del subdispositivo en la plataforma de administración debe cumplir con el ID de subdispositivo definido en Access Standalone.

Etapa 4 Hacer clic**DE ACUERDO**.

3.1.9.4 Configuración de P2P

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

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Configuración de red**>**P2P**.

Figura 3-15 P2P

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

Paso 3 Seleccionar**Permitir**para habilitar la función P2P. Hacer clic**DE**

Etapa 4 **ACUERDO**.

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

3.1.10 Configuración de la fecha

Procedimiento

Paso 1 Inicie sesión en la página web. Hacer

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

Figura 3-16 Configuración de la fecha

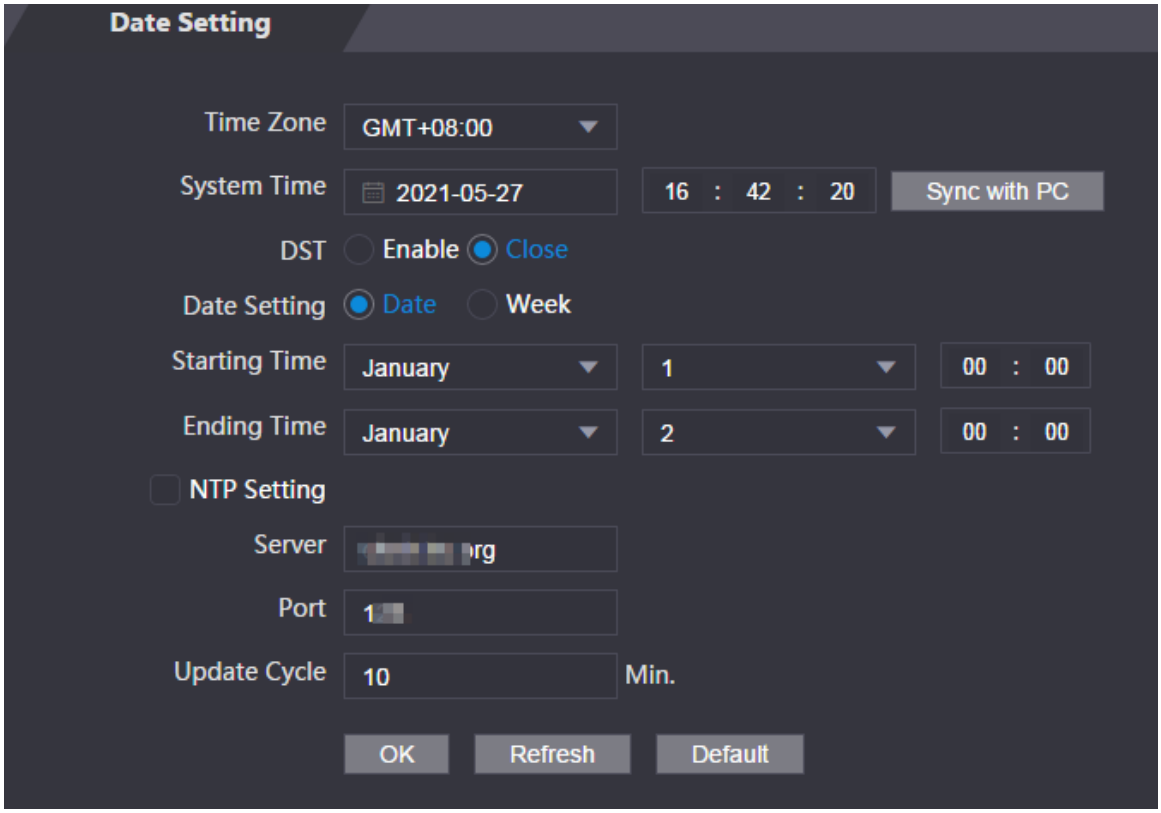


Tabla 3-5 Descripción de configuración de datos

Parámetro	Descripción
Zona horaria	Configura la zona horaria.
Hora del sistema	Configurar la hora del sistema. Hacer clic**Sincronizar con PC**y la hora del sistema cambia a la hora de la PC.
horario de verano	1. (Opcional) Habilite DST. 2. Seleccione**Fecha**o**Semana**en**Configuración de estado**. 3. Configure la hora de inicio y la hora de finalización.

Parámetro	Descripción
Configuración NTP	1. Seleccione el**Configuración NTP**caja. 2. Configurar parámetros. ● **Servidor**: Introduzca el dominio de un servidor NTP y el dispositivo sincronizará automáticamente la hora con el servidor NTP. ● **Puerto**: Introduzca el puerto del servidor NTP. ● **Ciclo de actualización**: Ingrese el intervalo de sincronización de tiempo.

Paso 3 Hacer clic**DE ACUERDO**.

3.1.11 Gestión de la seguridad

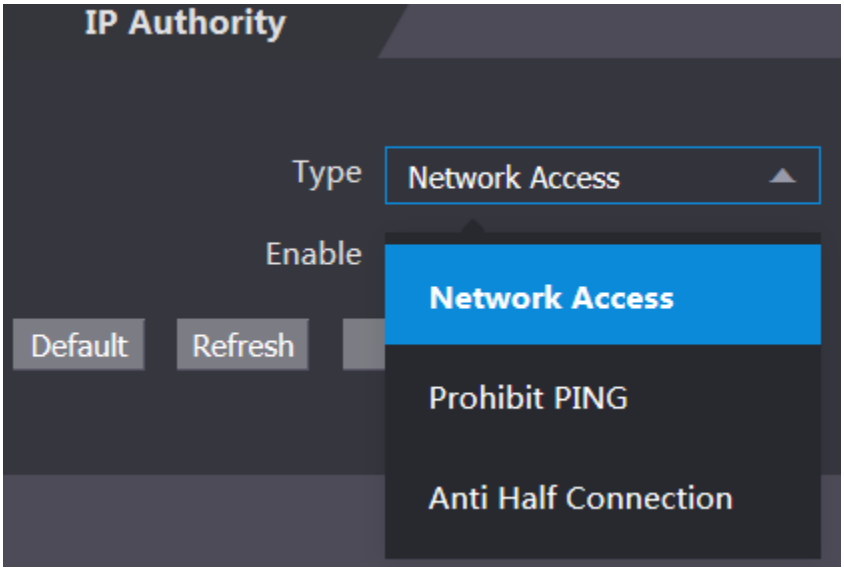
3.1.11.1 Configuración de autoridad IP

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Hacer clic**Autoridad de IP de gestión de seguridad**.

Figura 3-17 Autoridad IP



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

- **Acceso a la red**: Configure la lista de permitidos y la lista de bloqueados para controlar el acceso al dispositivo.
- **Prohibir PING**: Permitir**PING prohibido**y el dispositivo no responderá a la solicitud de ping.
- **Media conexión anti**: Permitir**Media conexión anti**función, y el dispositivo aún puede funcionar correctamente bajo el ataque de la mitad de la conexión.

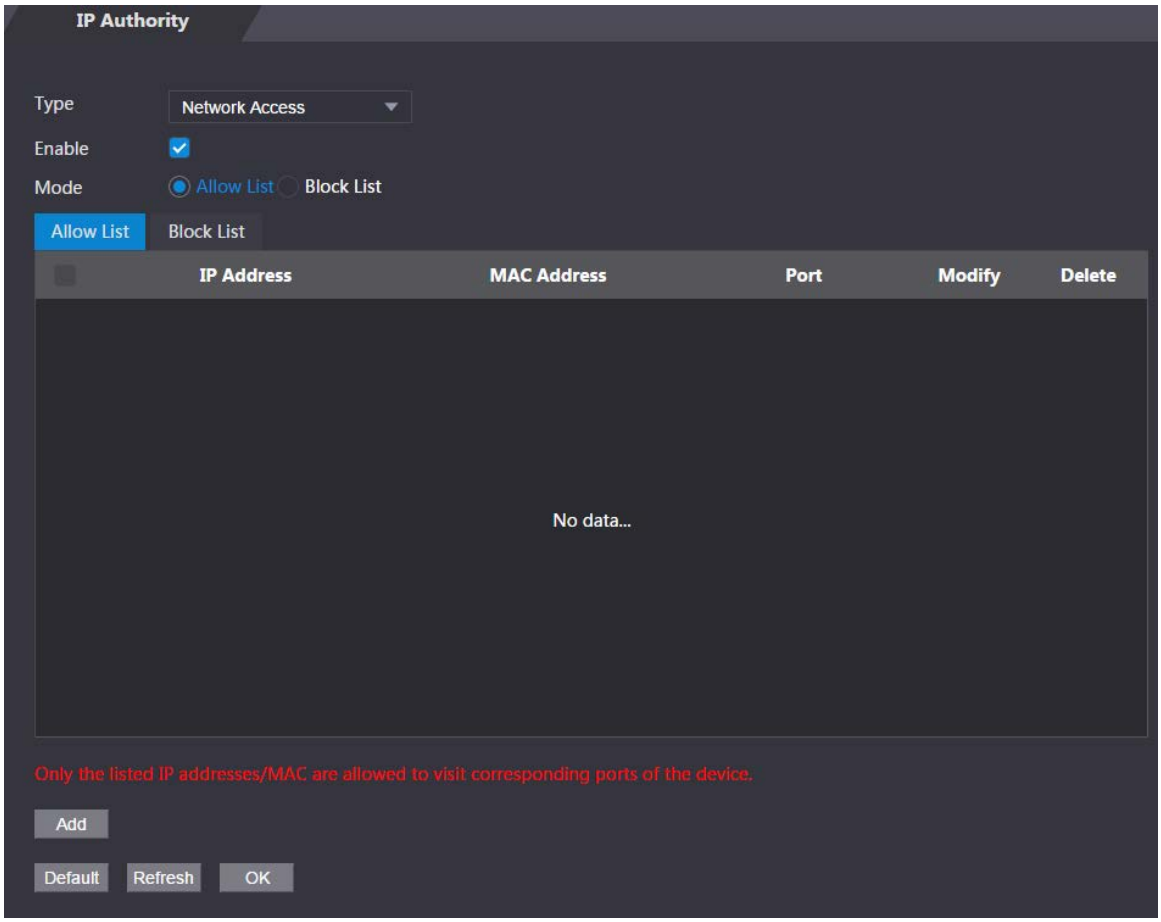
3.1.11.1.1 Acceso a la red

Procedimiento

Paso 1 Seleccionar**Acceso a la red**en el**Tipo**lista.

Paso 2 Selecciona el**Permitir**caja.

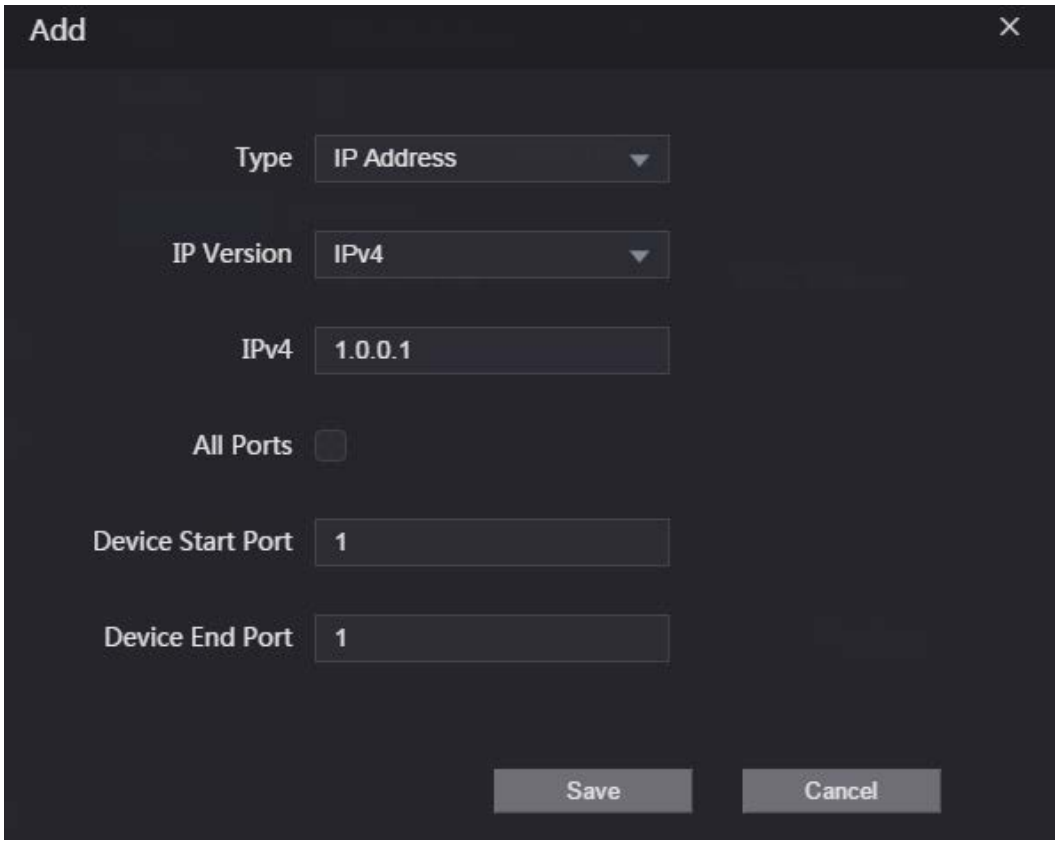
Figura 3-18 Acceso a la red



Paso 3 Seleccionar**Lista de permitidos**o**Lista de bloqueos**.

Etapa 4 Hacer clic**Agregar**.

Figura 3-19 Agregar IP



Paso 5 Configurar parámetros.

Tabla 3-6 Descripción de la adición de parámetros 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.
Puerto de inicio del dispositivo	si borras**Todos los puertos**casilla de verificación, establezca el puerto de inicio del dispositivo y el puerto final del dispositivo.
Puerto final del dispositivo	

Paso 6 Hacer clic**Ahorrar**, y el**Autoridad de PI**se muestra la ventana. Hacer clic**DE**

Paso 7 **ACUERDO**.

Operaciones relacionadas

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

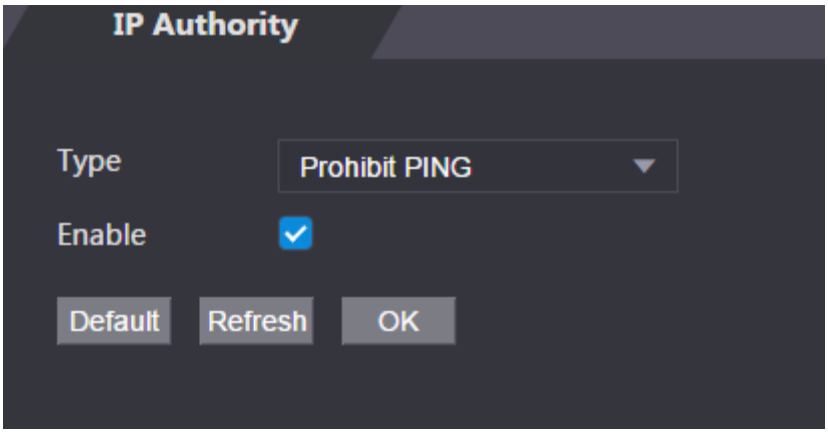
3.1.11.1.2 Prohibir PING

Procedimiento

Paso 1 Seleccionar**Prohibir PING**en el**Tipo**lista.

Paso 2 Selecciona el**Permitir**caja.

Figura 3-20 Prohibir PING



Paso 3 Hacer clic**DE ACUERDO**.

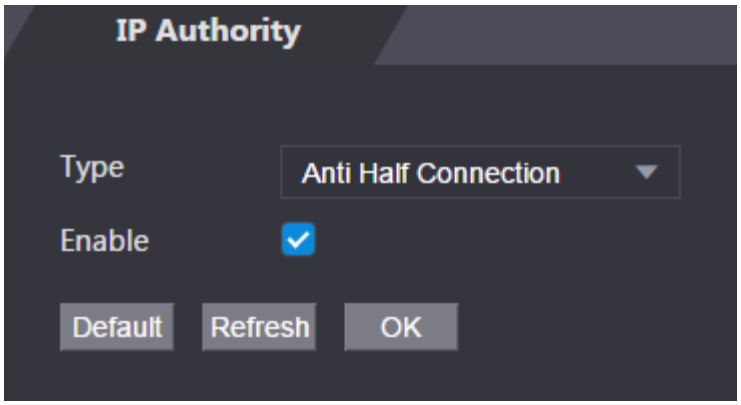
3.1.11.1.3 Conexión Anti Half

Procedimiento

Paso 1 Selecciona el**Media conexión anti**en el**Tipo**lista.

Paso 2 Selecciona el**Permitir**caja.

Figura 3-21 Acceso a la red



Paso 3 Hacer clic**DE ACUERDO**.

3.1.11.2 Configuración del sistema

3.1.11.2.1 Servicio del sistema

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Gestión de seguridad**>**Servicio del**

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

Figura 3-22 Servicio del sistema

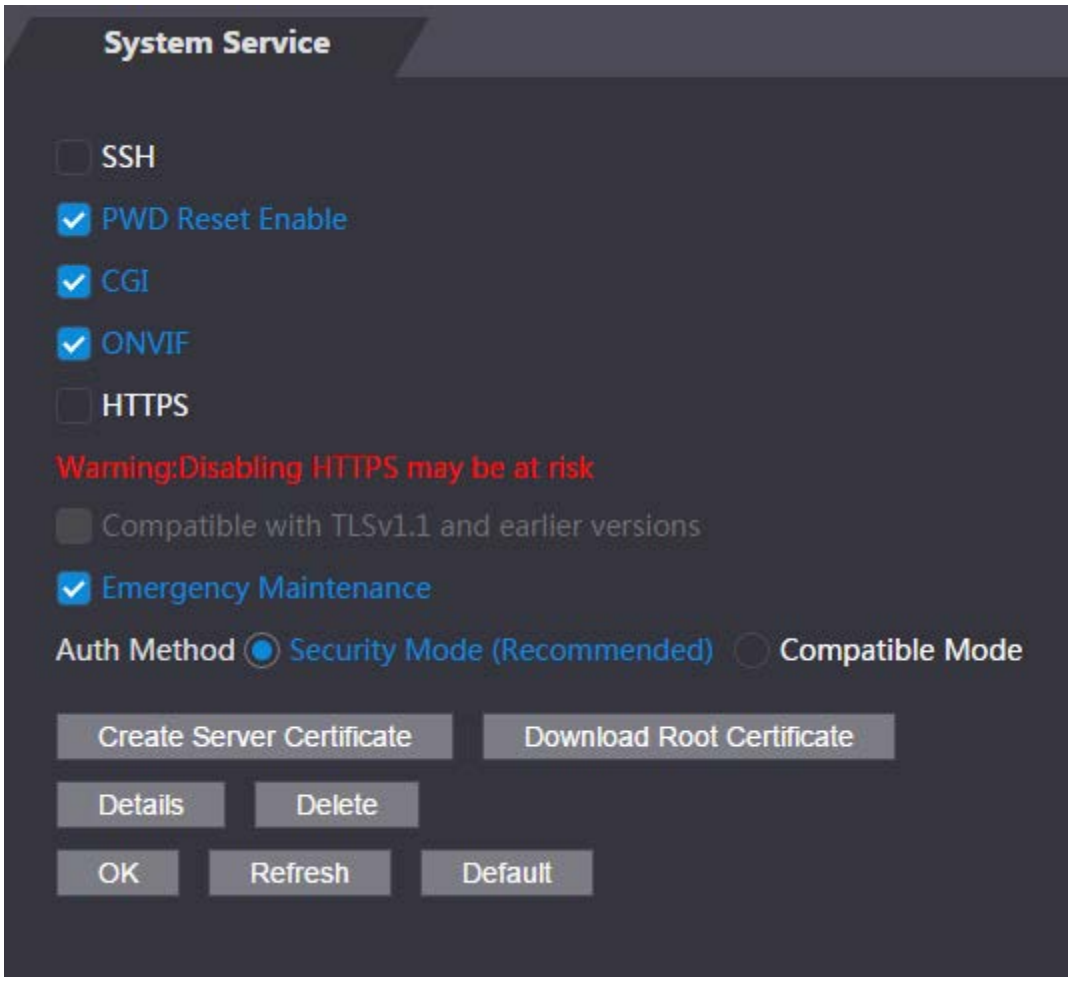


Tabla 3-7 Descripción del servicio del sistema

Parámetro	Descripción
SSH	Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura en una red no segura. Cuando SSH está habilitado, SSH proporciona un servicio criptográfico para la transmisión de datos.
Habilitar restablecimiento de PWD	Si está habilitado, puede restablecer la contraseña. Esta función está habilitada por defecto.
CGI	Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas de manera similar a las aplicaciones de consola que se ejecutan en un servidor que genera páginas web dinámicamente. Cuando CGI está habilitado, se pueden usar comandos CGI. El CGI está habilitado de forma predeterminada.
ONVIF	Habilite otros dispositivos para extraer la transmisión de video del VTO a través del protocolo ONVIF.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, HTTPS se utilizará para acceder a los comandos CGI; de lo contrario, se utilizará HTTP.
Compatible con TLSv1.1 y versiones anteriores	Habilite esta función si su navegador utiliza TLS V1.1 o versiones anteriores.
Mantenimiento de emergencia	Habilítelo para análisis de fallas y mantenimiento.
Método de autenticación	● **Modo de seguridad (recomendado)**: admite el inicio de sesión con autenticación Digest. ● **Modo compatible**: Compatible con el método de inicio de sesión de dispositivos antiguos.

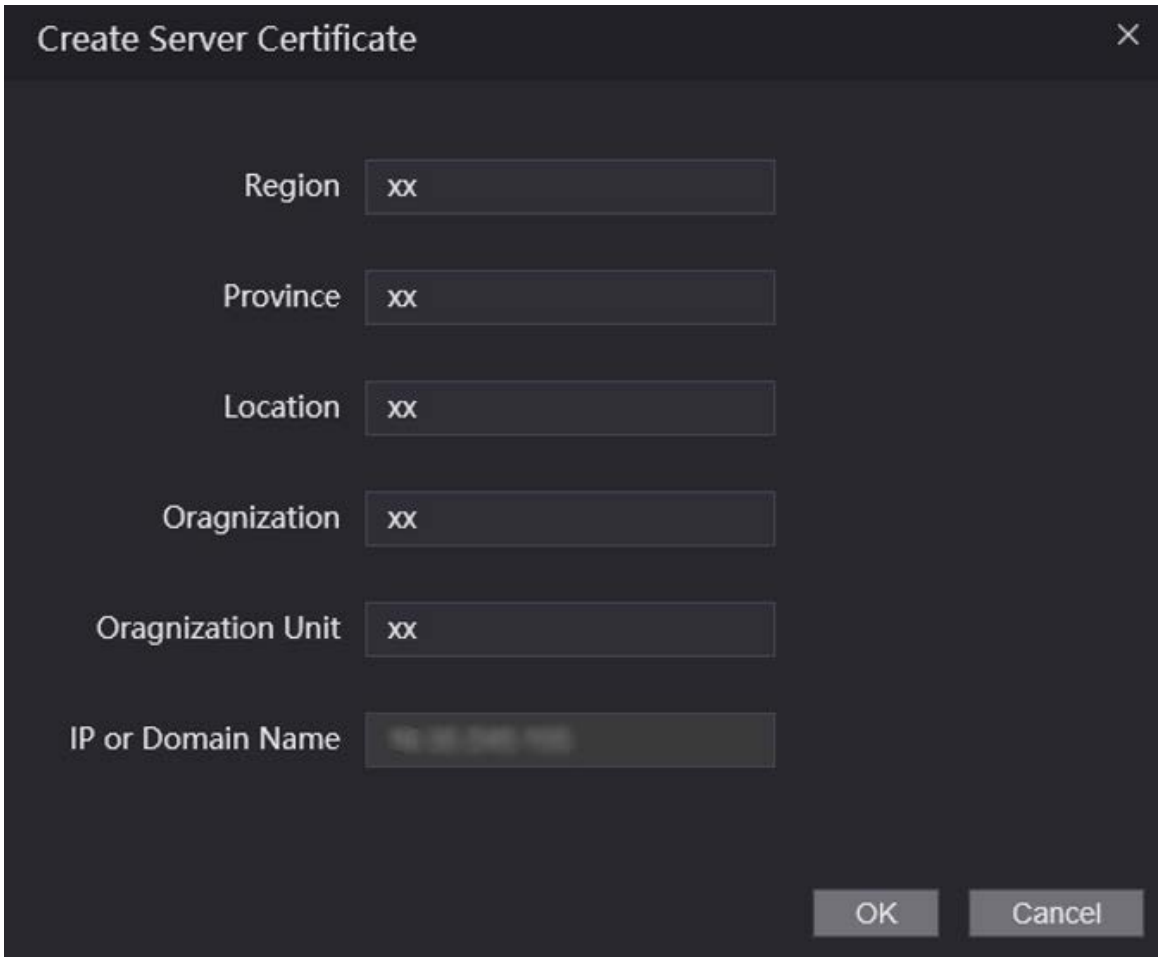
3.1.11.2.2 Crear certificado de servidor

Procedimiento

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

Paso 2 Ingresa la información y haz clic**DE ACUERDO**y luego el dispositivo se reiniciará.

Figura 3-23 Crear certificado de servidor



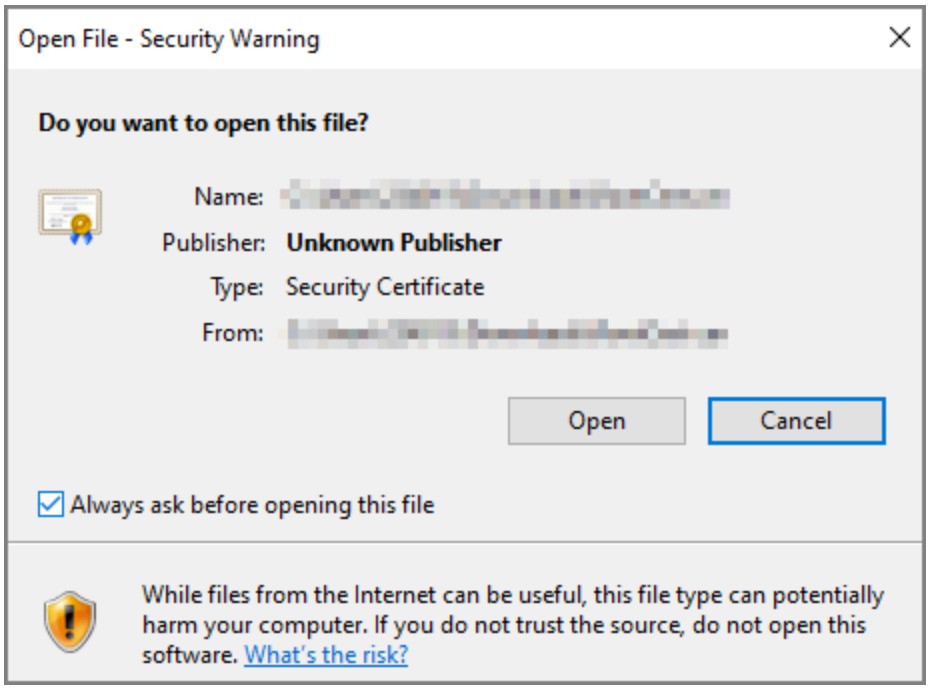
3.1.11.2.3 Descarga del certificado raíz

Procedimiento

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

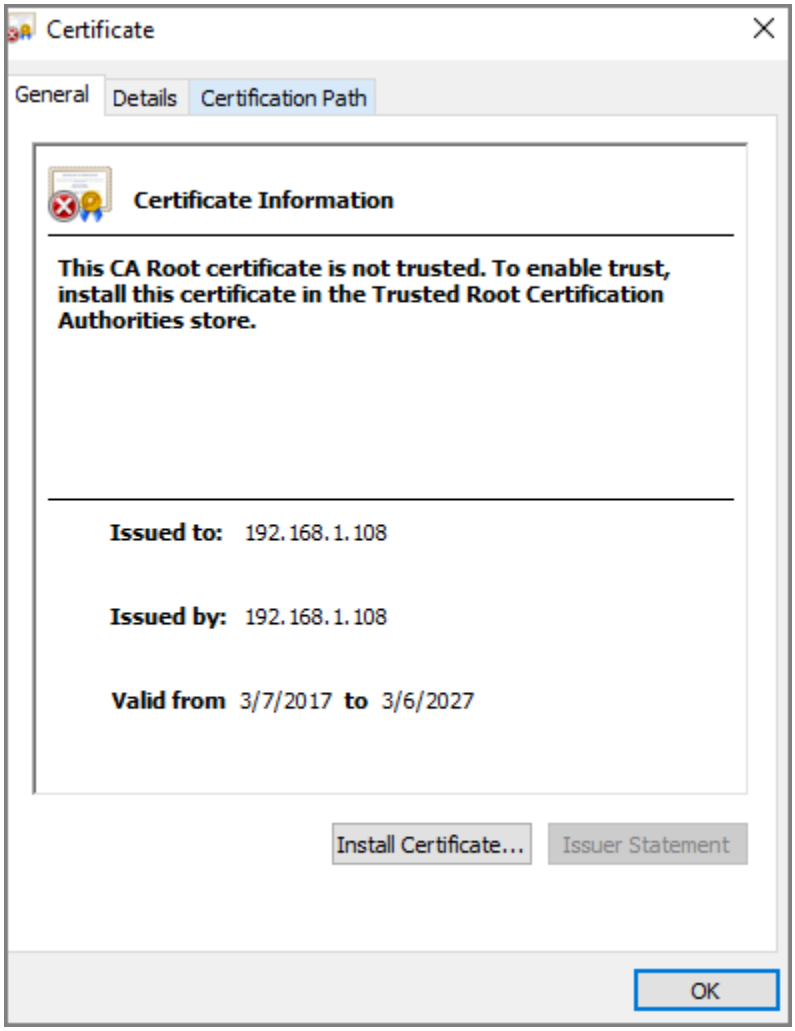
Paso 2 doble clic en el archivo que ha descargado y luego haga clic en**Abierto**.

Figura 3-24 Descarga de archivos



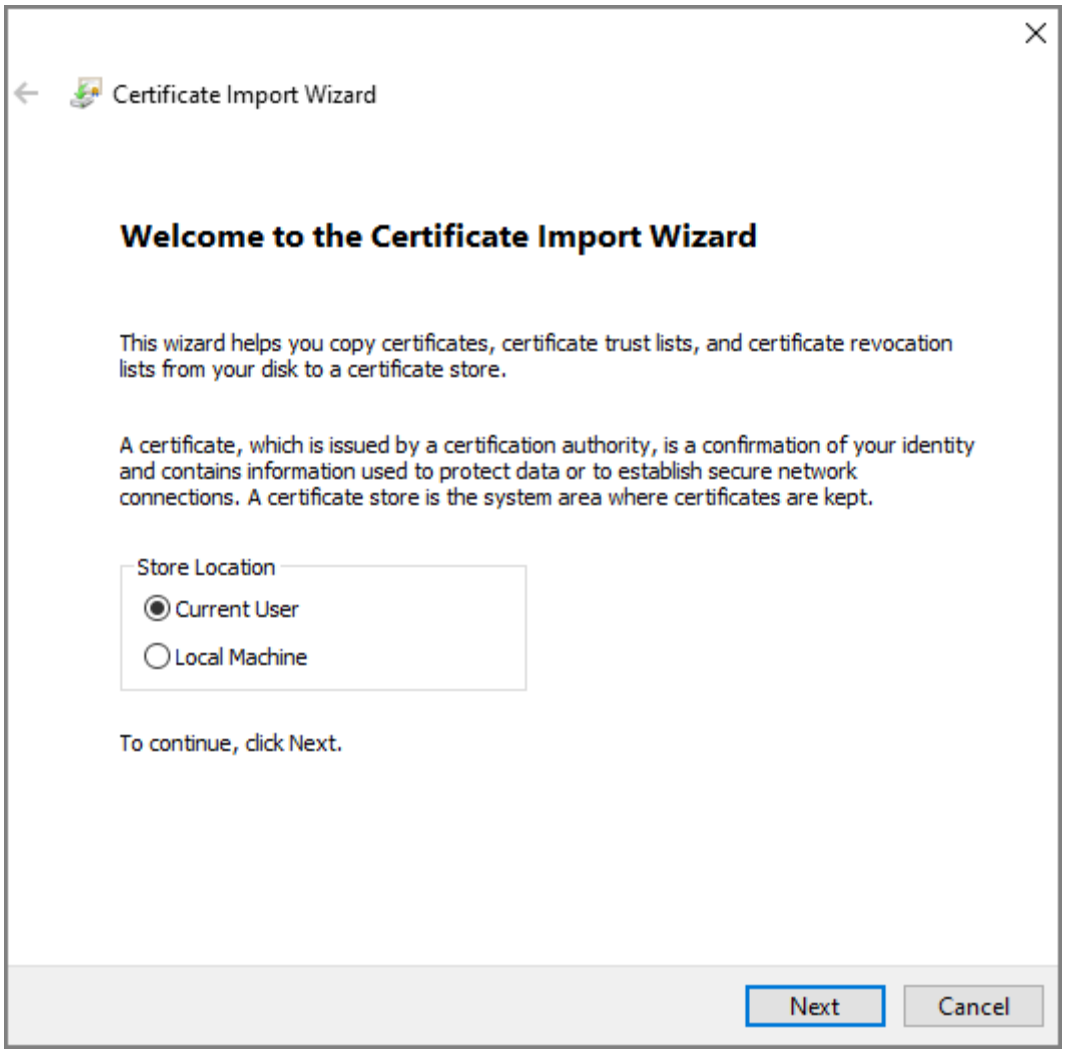
Paso 3 Hacer clic**Instalar certificado**.

Figura 3-25 Información del certificado



Etapa 4 Seleccionar**Usuario actual**o**Máquina local**y luego haga clic en**Próximo**.

Figura 3-26 Ubicación de la tienda

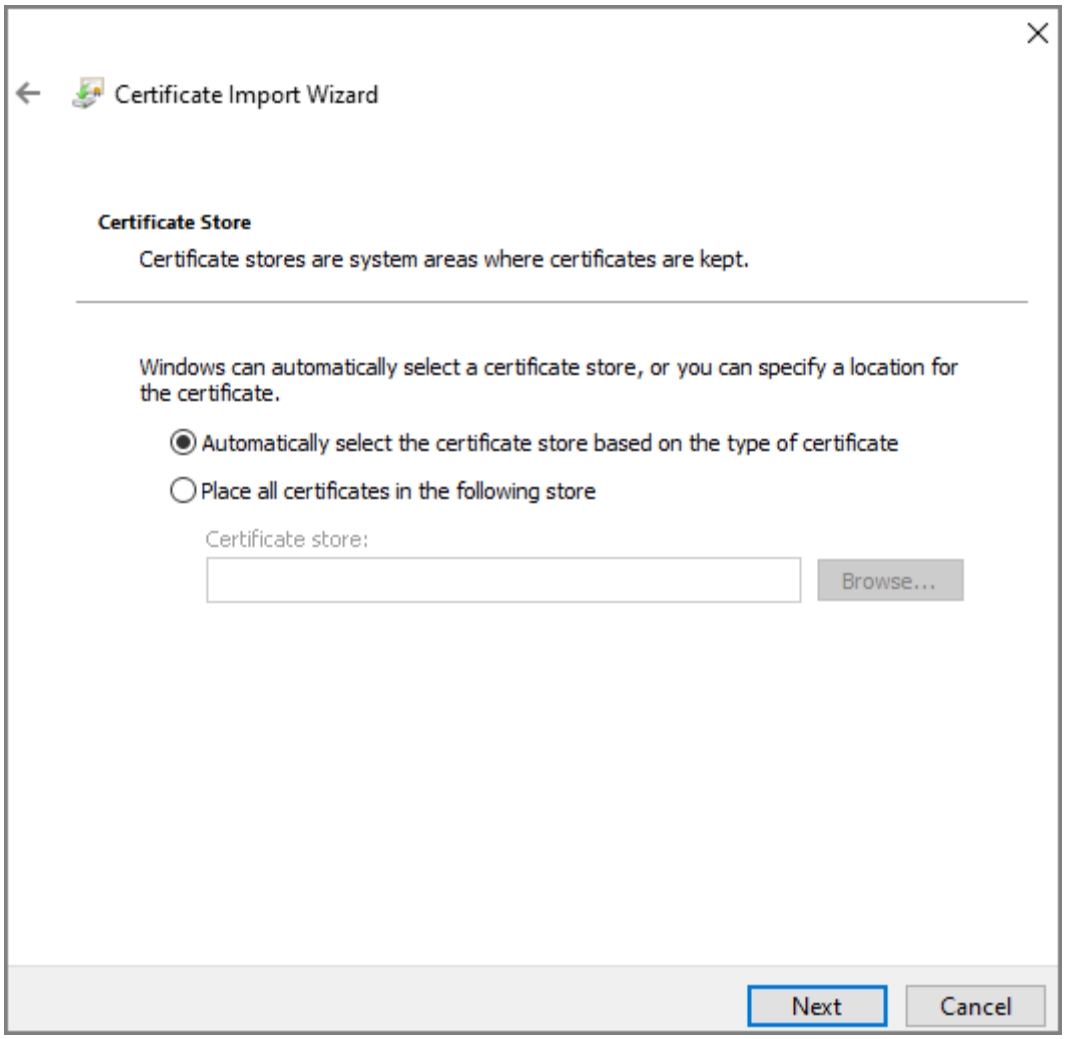


- **Usuario actual**: Se aplica al usuario que ha iniciado sesión en la PC.
- **Máquina local**: Se aplica a todos los usuarios que han iniciado sesión en la PC.

Paso 5 Seleccione la ubicación de almacenamiento adecuada.

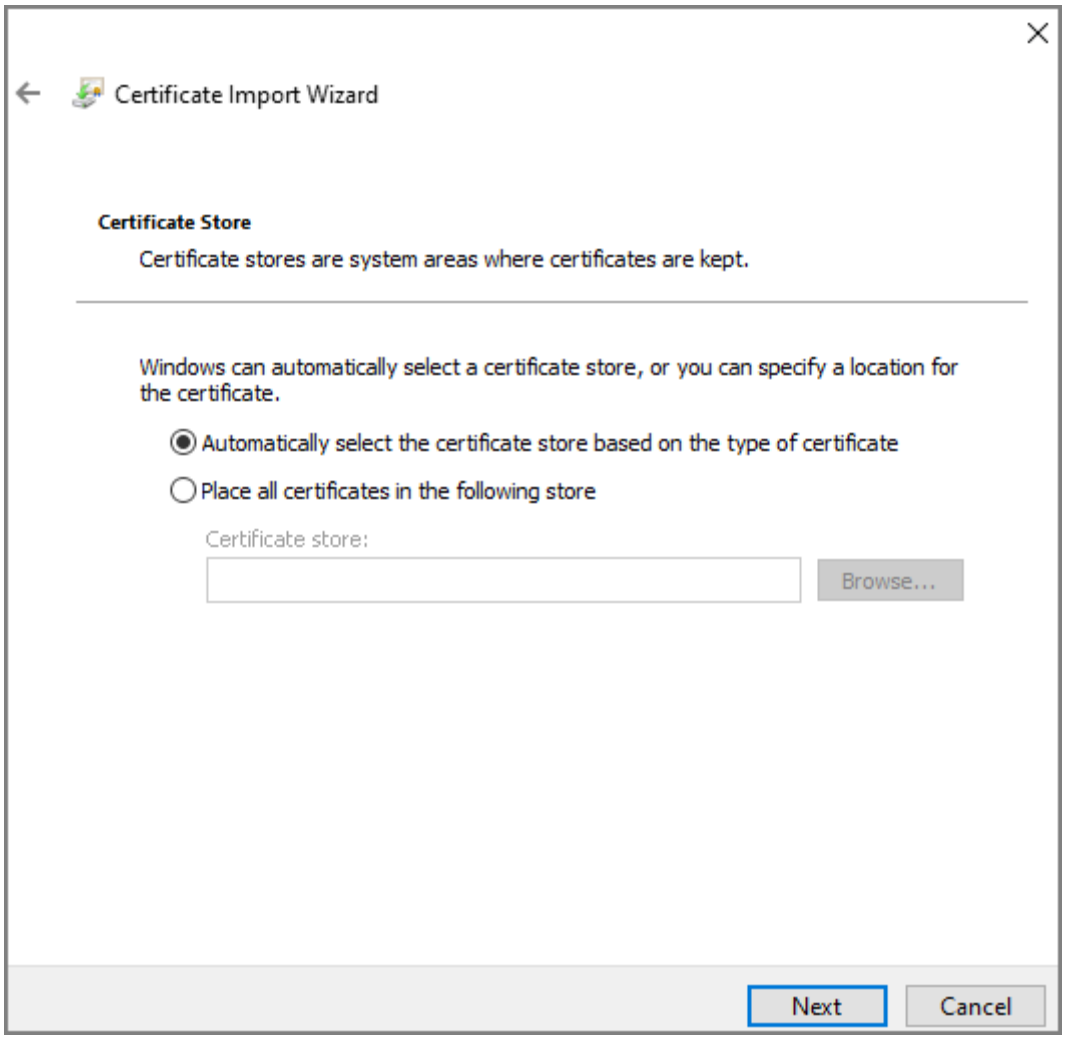
1) Seleccionar**Coloque todos los certificados en la siguiente tienda**.

Figura 3-27 Almacén de certificados



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

Figura 3-28 Almacén de certificados



Paso 6 Hacer clic**Finalizar**.

3.1.12 Gestión de usuarios

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

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

3.1.12.1 Adición de usuarios

Puede agregar nuevos usuarios y luego pueden iniciar sesión en la página web de Access Standalone.

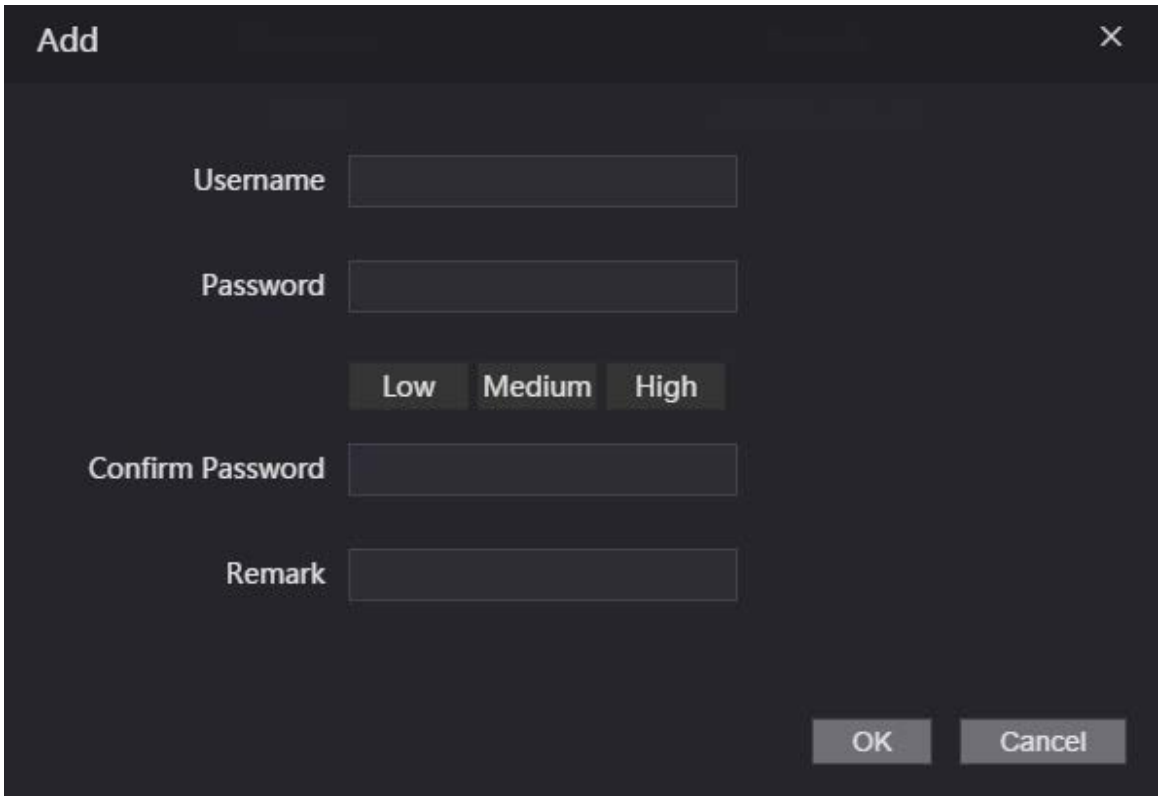
Procedimiento

Paso 1 Inicie sesión en la página web. Seleccionar**Gestión de**

Paso 2 **usuarios**>**Gestión de usuarios**. Hacer clic**Agregar**.

Paso 3

Figura 3-29 Agregar usuario



Etapa 4 Ingrese el nombre de usuario, la contraseña, confirme la contraseña y comente. Hacer clic**DE**

Paso 5 **ACUERDO**.

3.1.12.2 Adición de usuarios ONVIF

Información de contexto

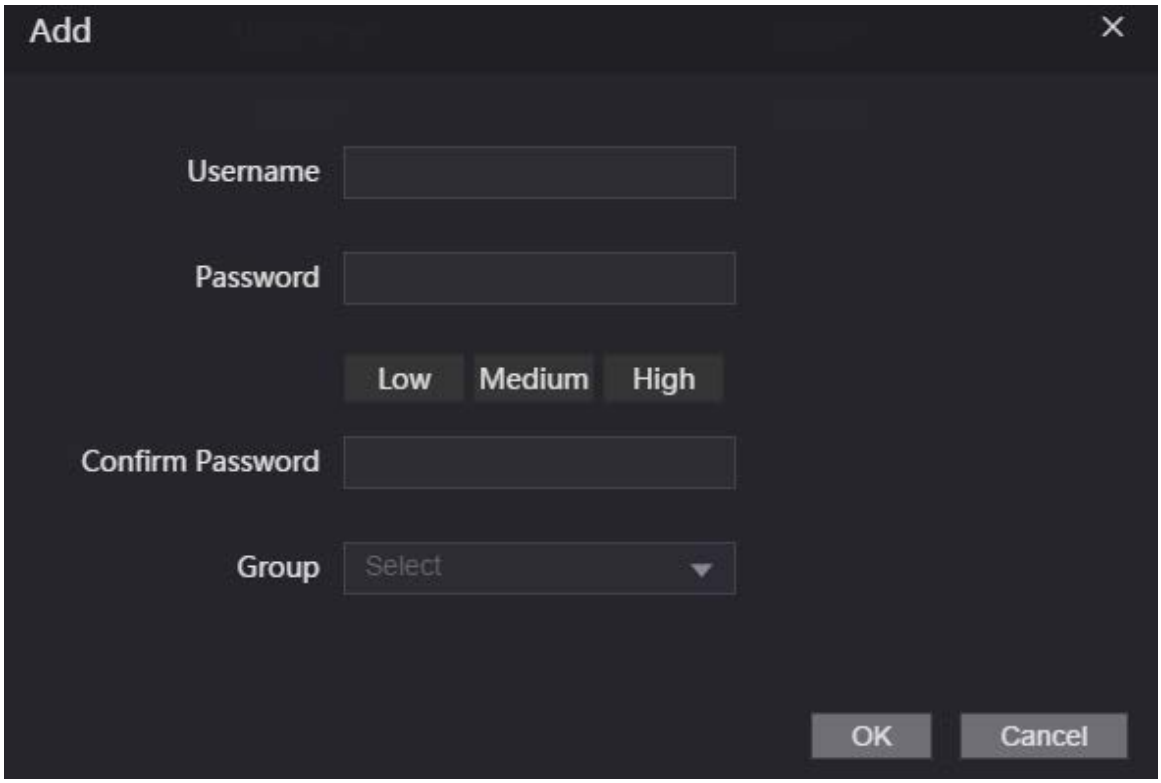
Open Network Video Interface Forum (ONVIF), un foro global y abierto de la industria establecido para el desarrollo de un estándar abierto global para la interfaz de productos de seguridad físicos basados en IP, que permite la compatibilidad de diferentes fabricantes. Los usuarios de ONVIF tienen sus identidades verificadas a través del protocolo ONVIF. El usuario predeterminado de ONVIF es admin.

Procedimiento

Paso 1 En la página de inicio, seleccione**Gestión de usuarios**>**Usuario Onvif**.

Paso 2 Hacer clic**Agregar**y luego configure los parámetros.

Figura 3-30 Agregar usuario ONVIF



Paso 3 Hacer clic**DE ACUERDO**.

3.1.13 Mantenimiento

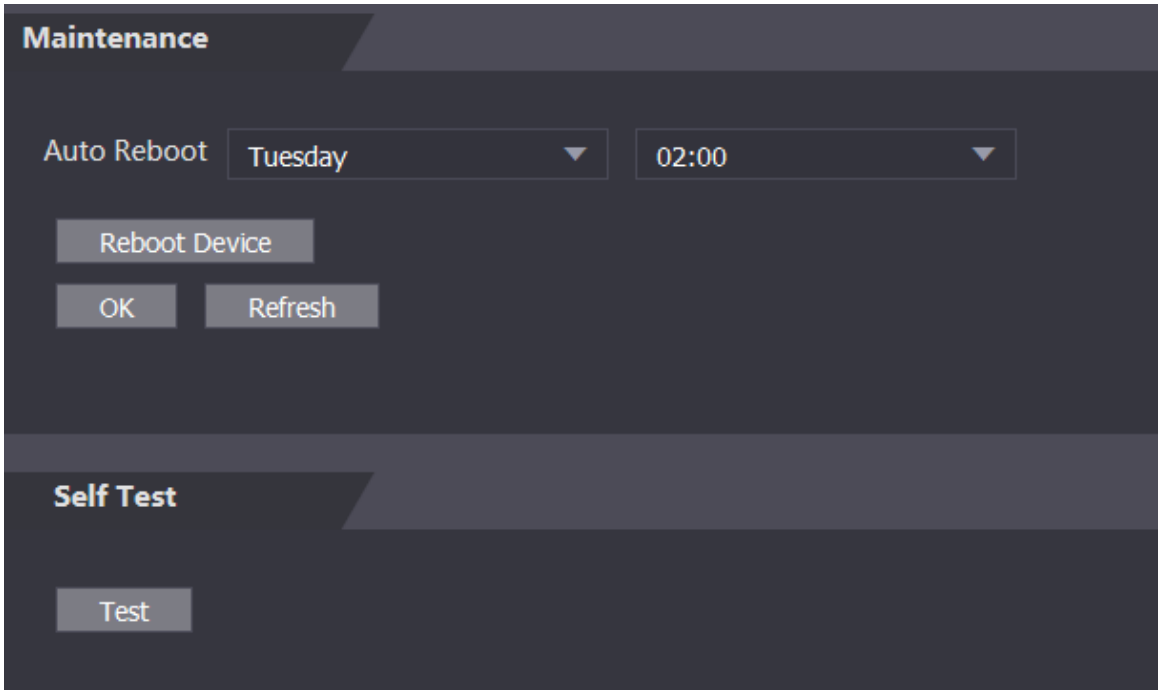
Puede reiniciar regularmente el dispositivo durante el tiempo de inactividad para mejorar su rendimiento.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Mantenimiento**.

Figura 3-31 Mantenimiento



Paso 3 Establezca la hora y luego haga clic en**DE ACUERDO**.

El dispositivo se reiniciará a la hora definida.

Es**Nunca**por defecto.

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

3.1.14 Gestión de la configuración

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

3.1.14.1 Exportación del archivo de configuración

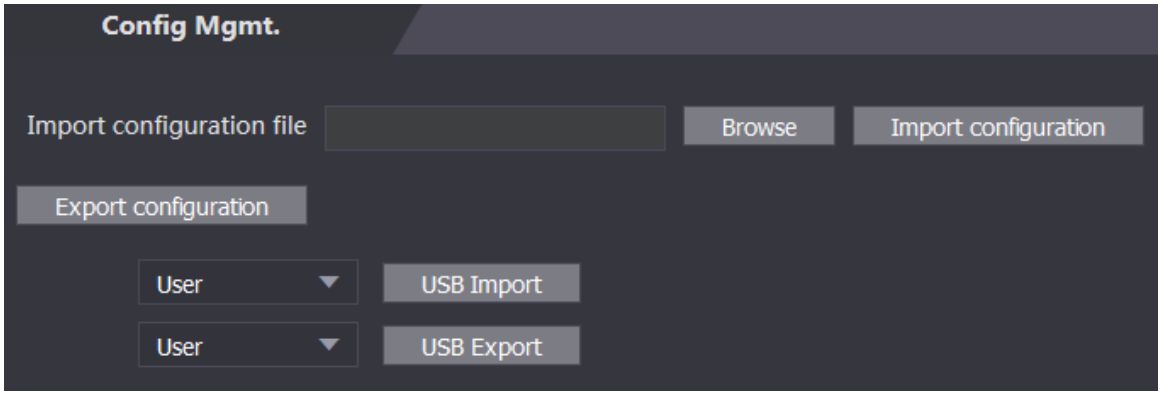
Puede exportar el archivo de configuración del dispositivo para realizar una copia de seguridad.

Procedimiento

Paso 1 Inicie sesión en la página web.

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

Figura 3-32 Gestión de la configuración



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

La información de IP del dispositivo no se exportará.

3.1.14.2 Importación del archivo de configuración

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

Procedimiento

Paso 1 Inicie sesión en la página web.

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

Paso 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

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Gestión de configuración**>**Gestión de configuración**. En

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

Figura 3-33 Características

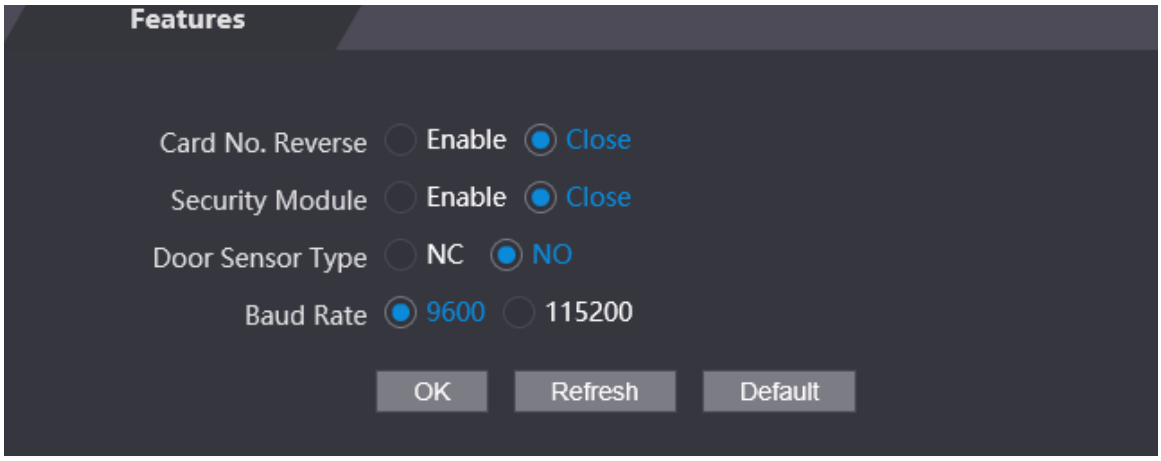


Tabla 3-9 Descripción de características

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

Etapa 4 Hacer clic**DE ACUERDO**.

3.1.14.4 Configuración de la huella digital

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

Procedimiento

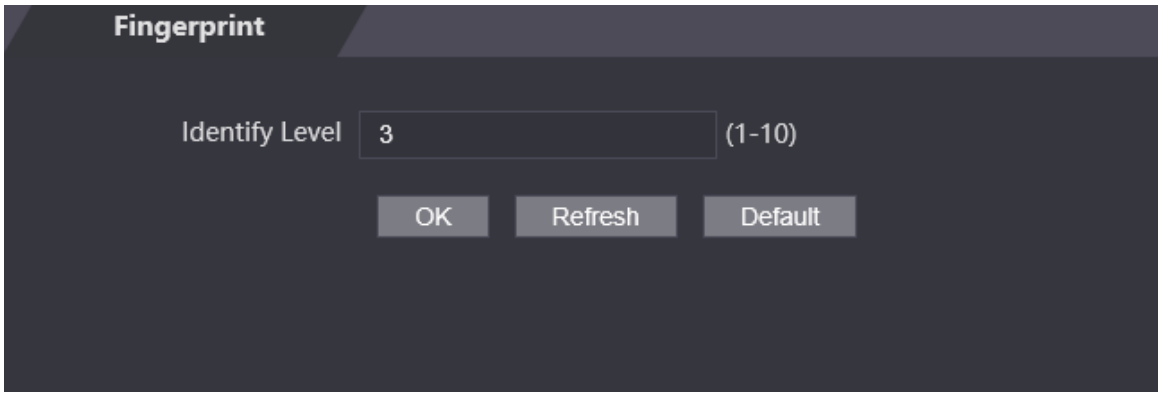
Paso 1 Inicie sesión en la página web.

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

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

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

Figura 3-34 Nivel de identidad de la huella digital



Etapa 4 Hacer clic**DE ACUERDO**.

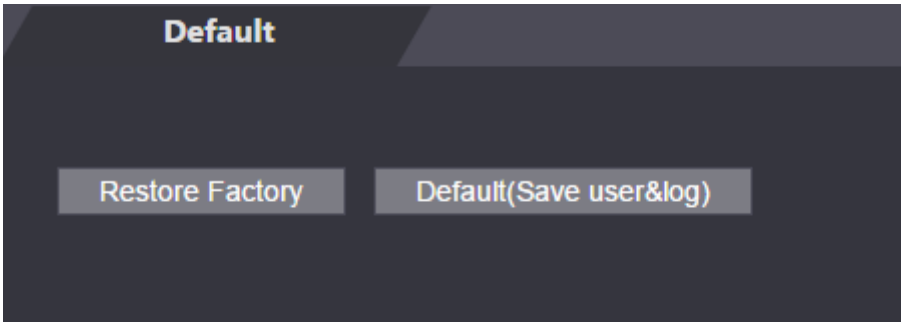
3.1.14.5 Restablecimiento de valores predeterminados de fábrica

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccionar

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

Figura 3-35 Predeterminado



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

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

3.1.14.6 Configuración de las funciones del puerto

Algunos cables se pueden utilizar para diferentes propósitos. Utilice cables según sus necesidades. Para obtener más información, consulte la Guía de inicio rápido de Access Standalone.

Procedimiento

Paso 1 En la página web de Access Standalone, seleccione**Gestión de configuración**>**Configuración de interfaz**.

Figura 3-36 Configurar funciones de puerto (ASI2221J/ASI2212J-D)

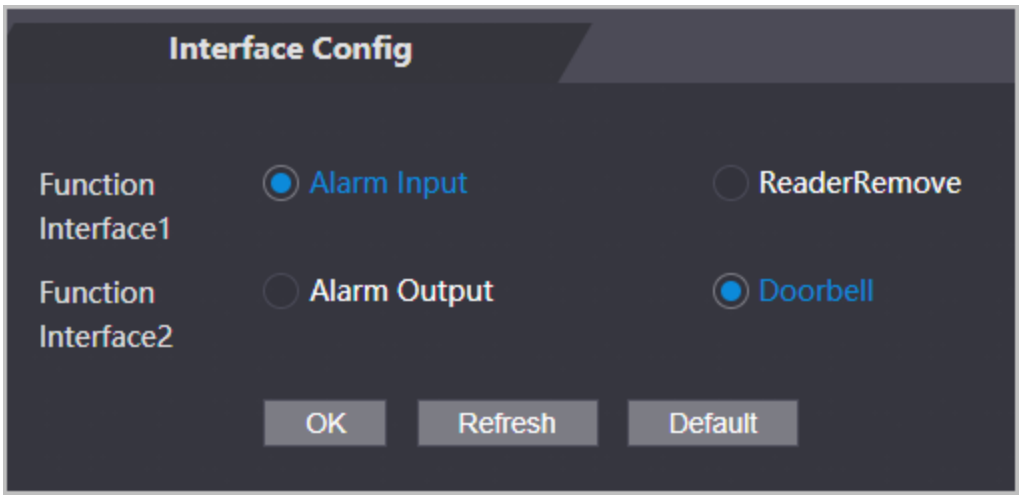
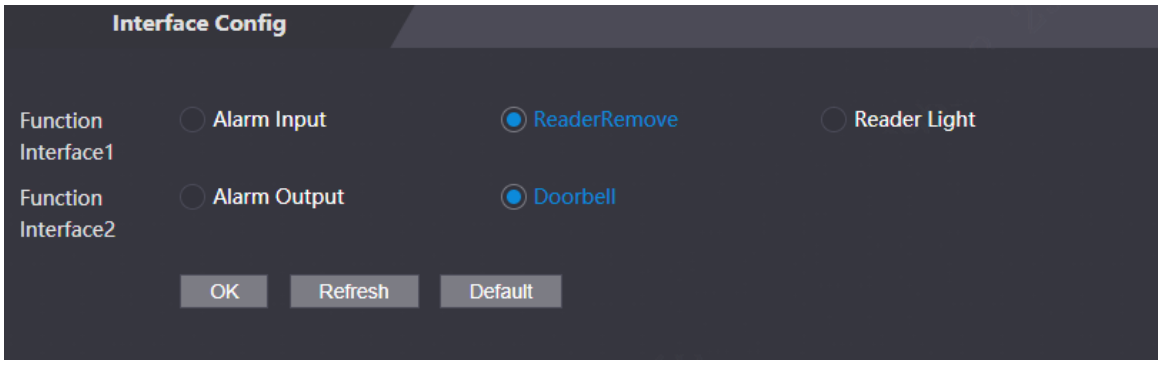


Figura 3-37 Configurar funciones de puerto (ASI2212J-DPW/ ASI2212J-PW)



Paso 2 Seleccione la función del puerto.

Tabla 3-10 Descripciones de las funciones de los puertos

Modelo	Alambrado	Descripción
ASI2221J/ASI2212JD	Alarma entrada/alarma producción	1. Conecta el dispositivo de entrada de alarma a WG_LED/ALM_IN/CASE y GND. 2. Conecta el dispositivo de salida de alarma a ALM_COM/BELL+ y ALM_NO/BELL-. 3. Seleccione**Entrada de alarma**de**Interfaz de funciones1**y luego seleccione**Salida de alarma**de**Interfaz de funciones2**.
	Lector anti-manipulación alarma	1. Conecte el cable CASE del lector de tarjetas a WG_LED/ALM_IN/CASE. 2. Seleccione**Lector****Eliminar**de**Interfaz de funciones1**y, a continuación, seleccione cualquier opción de**Interfaz de funciones2**.
	Lector LED	1. Conecte el cable LED del lector de tarjetas a WG_LED/ALM_IN/CASE. 2. Seleccione**Luz del lector**de**Interfaz de funciones1**y, a continuación, seleccione cualquier opción de**Interfaz de funciones2**.
	Timbre de la puerta	1. Conecte el timbre a ALM_COM/BELL+ y ALM_NO/BELL+. 2. Seleccione cualquier opción de**Interfaz de funciones1**y luego seleccione**Timbre de la puerta**de**Interfaz de funciones2**.

Modelo	Alambrado	Descripción
ASI2212J-DPW/ ASI2212J-PW	Alarma entrada/alarma producción	1. Conecta el dispositivo de entrada de alarma a ALARM1/CASE. 2. Conecta el dispositivo de salida de alarma a ALMRM1_COM/BELL+ y ALMRM1_NO/BELL-. 3. Seleccione**Entrada de alarma**de**Interfaz de funciones1**y luego seleccione**Salida de alarma**de**Interfaz de funciones2**.
	Lector anti-manipulación alarma	1. Conecte el cable CASE del lector de tarjetas a ALARM1/CASE. 2. Seleccione**LectorEliminar**de**Interfaz de funciones1**y, a continuación, seleccione cualquier opción de**Interfaz de funciones2**.
	Timbre de la puerta	1. Conecte el timbre a ALARM1_COM/BELL+ y ALARM1_NO/BELL+. 2. Seleccione cualquier opción de**Interfaz de funciones1**y luego seleccione**Timbre de la puerta**de**Interfaz de funciones2**.

3.1.15 Actualización del Sistema

- Utilice el archivo de actualización correcto. Asegúrese de obtener el archivo de actualización correcto del soporte técnico.
- No desconecte la fuente de alimentación ni la red, ni reinicie ni apague Access Standalone. durante la actualización.

3.1.15.1 Actualización de archivos

Procedimiento

Paso 1 En la página de inicio, seleccione**Mejora**.

Paso 2 En el**Actualización de archivo**área, haga clic**Navegar**y, a continuación, cargue el archivo de actualización.

El archivo de actualización debe ser un archivo .bin.

Paso 3 Hacer clic**Actualizar**.

Access Standalone se reiniciará después de que se complete la actualización.

3.1.15.2 Actualización en línea

Procedimiento

Paso 1 En la página de inicio, seleccione**Mejora**.

Paso 2 En el**Actualización en línea**área, seleccione un método de actualización.

- Seleccionar**Verificación automática**, Access Standalone comprobará automáticamente si su última versión está disponible.
- Seleccionar**Comprobación manual**y puede verificar inmediatamente si la última versión está disponible.

Paso 3 Actualice Access Standalone cuando esté disponible la última versión.

3.1.16 Información de la versión

Ver información, incluida la dirección MAC, el número de serie y más.

Procedimiento

Paso 1 Inicie sesión en la página web.

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

3.1.17 Visualización de usuarios en línea

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

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Usuario en línea**.

3.1.18 Visualización de registros del sistema

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

3.1.18.1 Registros del sistema

Ver y buscar registros del sistema.

Procedimiento

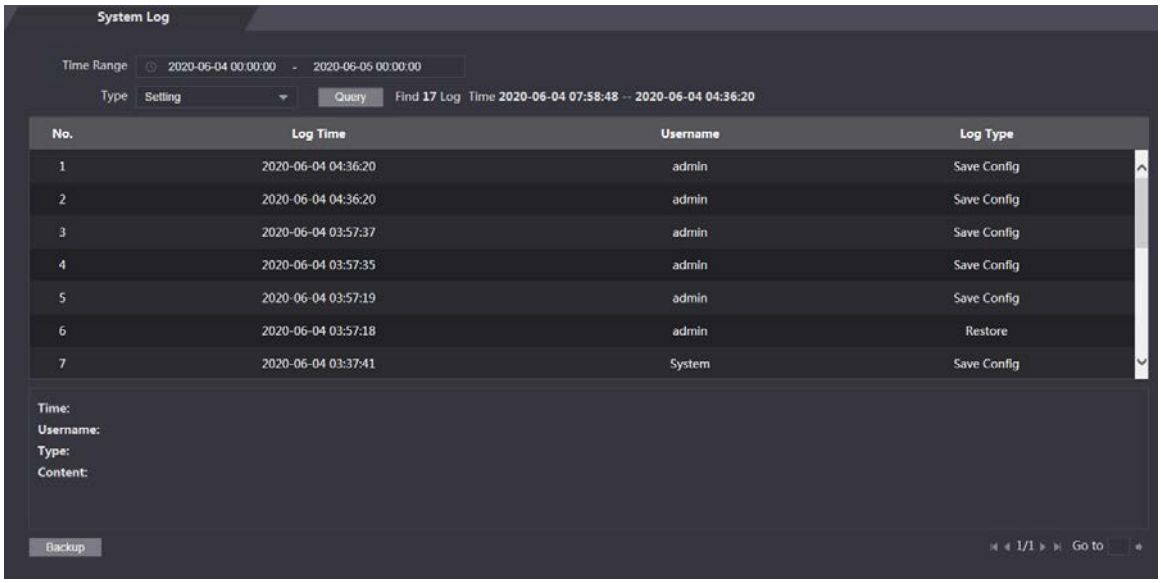
Paso 1 Inicie sesión en la página web. Seleccionar**Registro**

Paso 2 **del sistema**>**Registro del sistema**.

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

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

Figura 3-38 Búsqueda de registros



3.1.18.2 Registros de administración

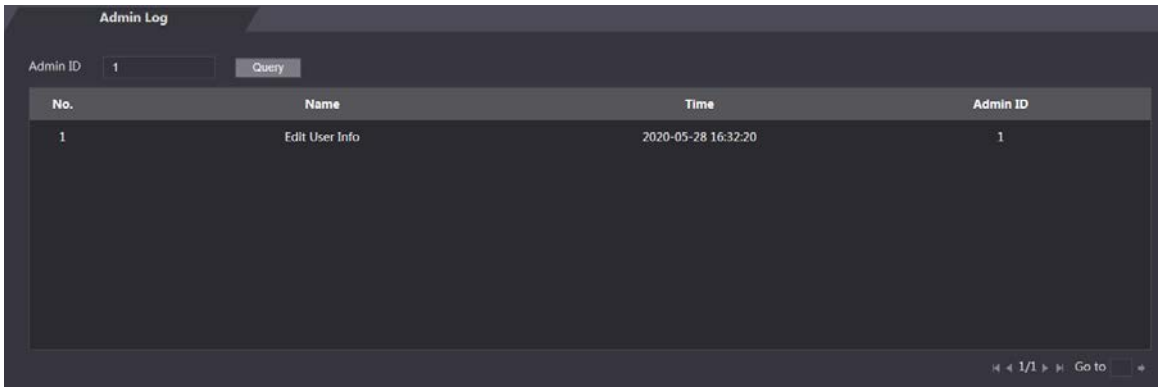
Procedimiento

Paso 1 Inicie sesión en la página web. Seleccionar**Registro del sistema**>**Registro de**

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

Paso 3 en**Consulta**.

Figura 3-39 Registro de administrador



3.1.18.3 Desbloquear registros

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Registro del sistema**>**Registros de búsqueda**.

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

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

3.1.19 Cerrar sesión

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

3.2 Web en el teléfono

Información de contexto

Asegúrese de que Access Standalone esté en la misma LAN que su teléfono. Conecte Access Standalone al punto de acceso de su teléfono o conéctelo y su teléfono al mismo enrutador.

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

Procedimiento

Paso 1 Vaya a la dirección IP (192.168.1.108 por defecto) de Access Standalone en el navegador. Introduzca el

Paso 2 nombre de usuario y la contraseña.

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

Paso 3 Hacer clic**Acceso**.

4 Configuración inteligente de PSS Lite

Esta sección presenta cómo administrar y configurar Access Standalone a través de Smart PSS Lite. También puede configurar reglas de tiempo de asistencia en la plataforma, como turnos, modos, horarios y más. Para obtener más información, consulte el manual del usuario de Smart PSS Lite.

4.1 Instalación e inicio de sesión

Instale e inicie sesión en Smart PSS Lite. Para obtener más información, consulte el manual de usuario de Smart PSS Lite.

Procedimiento

Paso 1 Obtenga el paquete de software de Smart PSS Lite del soporte técnico y luego instale y ejecute el software de acuerdo con las instrucciones.

Paso 2 Inicialice Smart PSS Lite cuando inicie sesión por primera vez, incluida la configuración de contraseña y preguntas de seguridad.

Configure la contraseña para el primer uso y luego configure las preguntas de seguridad para restablecer su contraseña cuando la olvidó.

Paso 3 Ingrese su nombre de usuario y contraseña para iniciar sesión en Smart PSS Lite.

4.2 Adición de dispositivos

Debe agregar Access Standalone a Smart PSS Lite. Puede agregarlos en lotes o individualmente.

4.2.1 Agregando individualmente

Puede agregar Access Standalone individualmente ingresando sus direcciones IP o nombres de dominio.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Administrador de dispositivos**y haga clic

Paso 3 **Agregar**. Ingrese la información del dispositivo.

Figura 4-1 Información del dispositivo

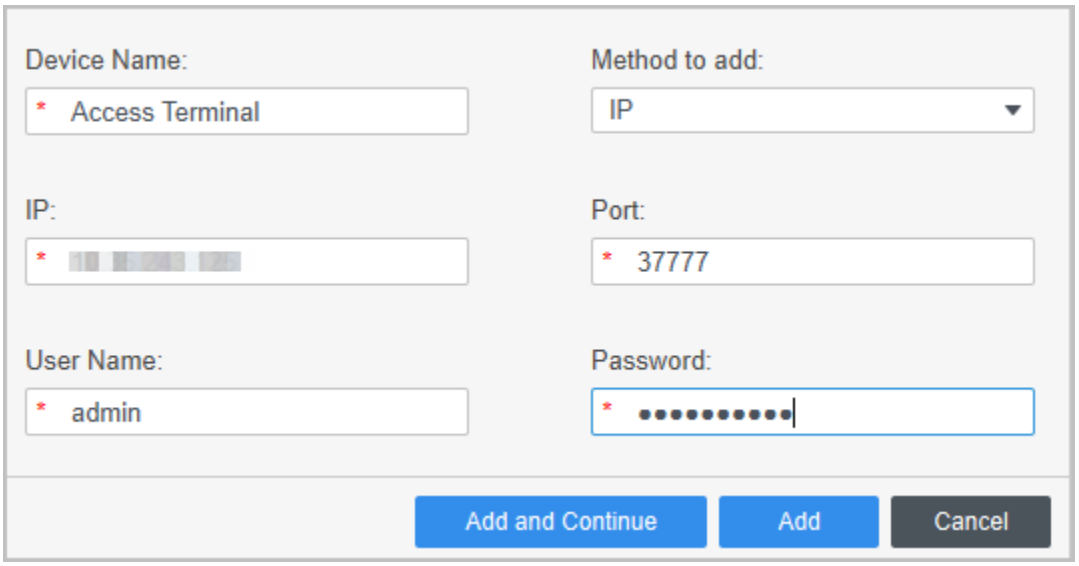


Tabla 4-1 Parámetros del dispositivo Descripción

Parámetro	Descripción
Nombre del dispositivo	Introduzca un nombre para Access Standalone. Le recomendamos que le ponga el nombre de su área de instalación.
Método para agregar	Seleccionar**IP**para agregar el Terminal de Acceso ingresando su Dirección IP.
IP	Ingrese la dirección IP del Access Standalone.
Puerto	El número de puerto es 37777 por defecto.
Usuario Contraseña	Ingrese el nombre de usuario y la contraseña de la Terminal de Acceso.

Etapa 4 Hacer clic**Agregar**.

Las pantallas de Access Standalone añadidas en la**Dispositivos**página. Puedes hacer clic**Agregar y continuar**para agregar más accesos independientes.

4.2.2 Adición de lotes

Le recomendamos que utilice la función de búsqueda automática cuando agregue acceso independiente en lotes. Asegúrese de que los Access Standalones que agregue deben estar en el mismo segmento de red.

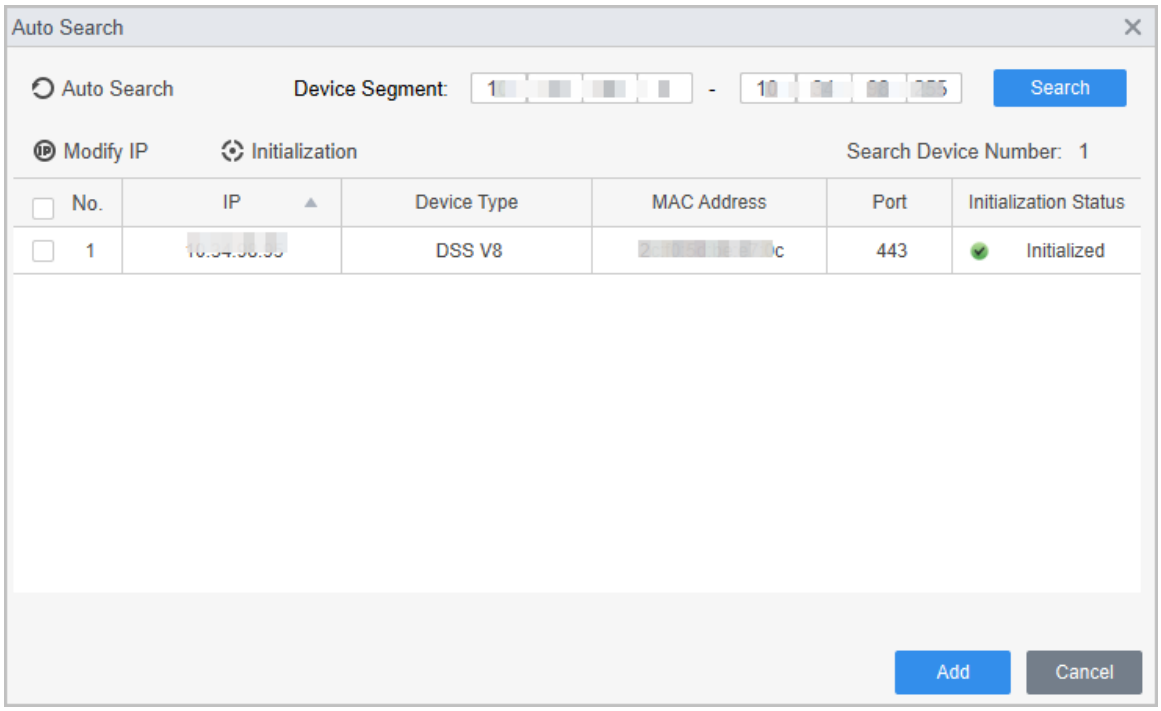
Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Administrador de dispositivos**y buscar dispositivos.

- Hacer clic**Auto búsqueda**, para buscar dispositivos en la misma LAN.
- Ingrese el rango del segmento de red y luego haga clic en**Buscar**.

Figura 4-2 Búsqueda automática



Se mostrará una lista de dispositivos.

Seleccione un dispositivo y luego haga clic en**Modificar IP**para modificar su dirección IP.

Paso 3 Seleccione el Access Standalone que desea agregar a Smart PSS Lite y luego haga clic en**Agregar**.

Etapa 4 Introduzca el nombre de usuario y la contraseña de Access Standalone.

Puede ver el Access Standalone agregado en el**Dispositivos**página.

Access Standalone inicia sesión automáticamente en Smart PSS Lite después de agregarlo.**En línea**es se muestra después de un inicio de sesión exitoso.

4.3 Gestión de usuarios

Agregue usuarios, asígneles tarjetas y configure sus permisos de acceso.

4.3.1 Configuración del tipo de tarjeta

Establezca el tipo de tarjeta antes de asignar tarjetas a los usuarios. Por ejemplo, si la tarjeta asignada es una tarjeta de identificación, establezca el tipo de tarjeta en Tarjeta de identificación.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Solución de acceso**>**Gerente de Personal**>**Usuario**. Sobre el

Paso 3 **Tipo de emisión de tarjeta**y luego seleccione un tipo de tarjeta.

Asegúrese de que el tipo de tarjeta sea el mismo que la tarjeta realmente asignada; de lo contrario, la tarjeta No se puede leer el número.

Etapa 4 Hacer clic**DE ACUERDO**.

4.3.2 Adición de usuarios

4.3.2.1 Adición individual

Puede agregar usuarios individualmente.

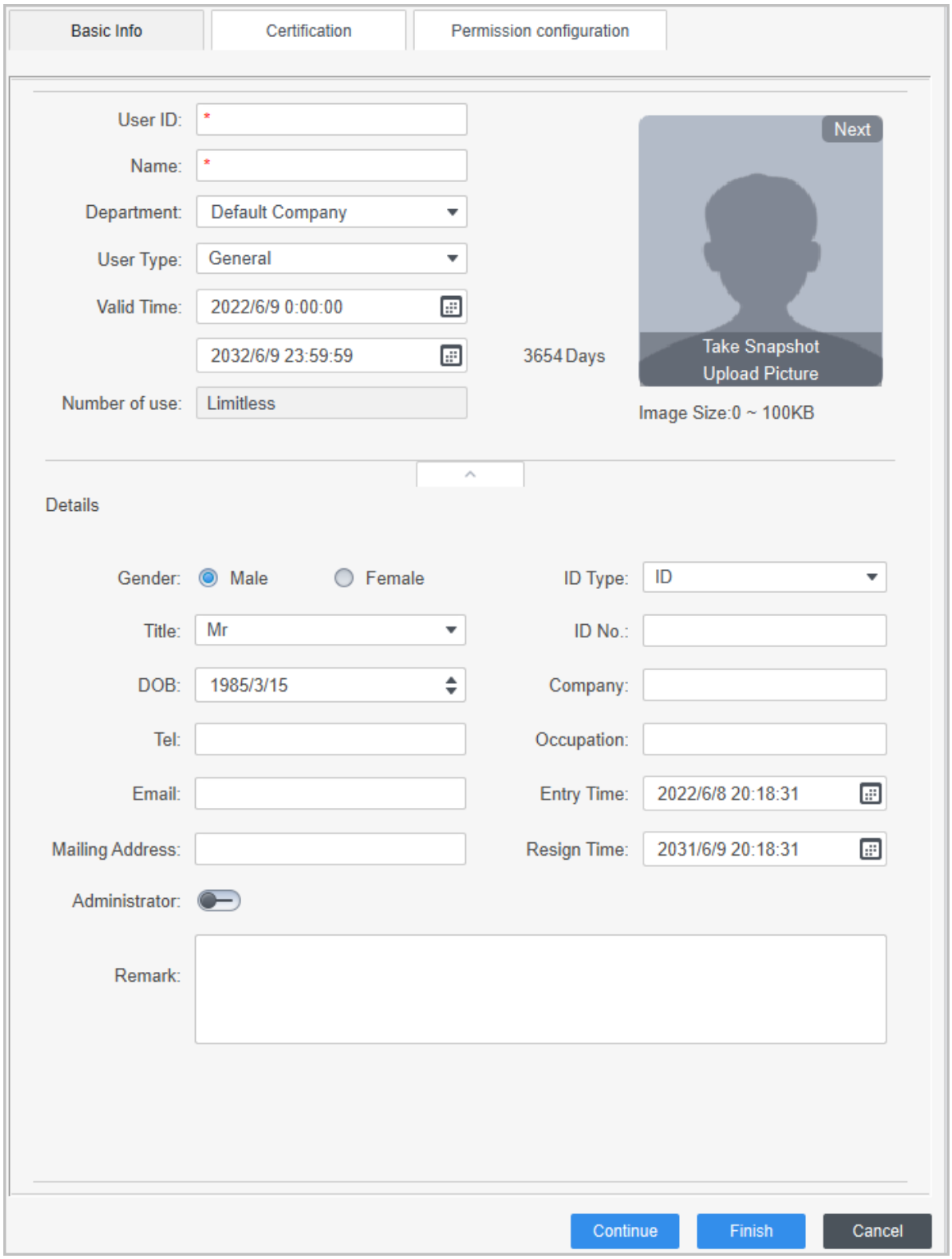
Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Solución de acceso**>**Gerente de Personal**>**Usuario**>**Agregar**.

Paso 3 Hacer clic**Información básica**pestaña e ingrese la información básica del usuario, y luego importe la imagen de la cara.

Figura 4-3 Agregar información básica



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

- Configurar contraseña: la contraseña debe constar de 6 a 8 dígitos.
- Configurar tarjeta: El número de tarjeta puede leerse automáticamente o introducirse manualmente. Para leer el número de tarjeta automáticamente, seleccione un lector de tarjetas y luego coloque la tarjeta en el lector de tarjetas.

  1. En el**Tarjeta**área, haga clic y seleccione**Emisor de la tarjeta**y luego haga clic en**DE ACUERDO**.
  2. Haga clic en**Agregar**, deslice una tarjeta en el lector de tarjetas.

     Se muestra el número de tarjeta.

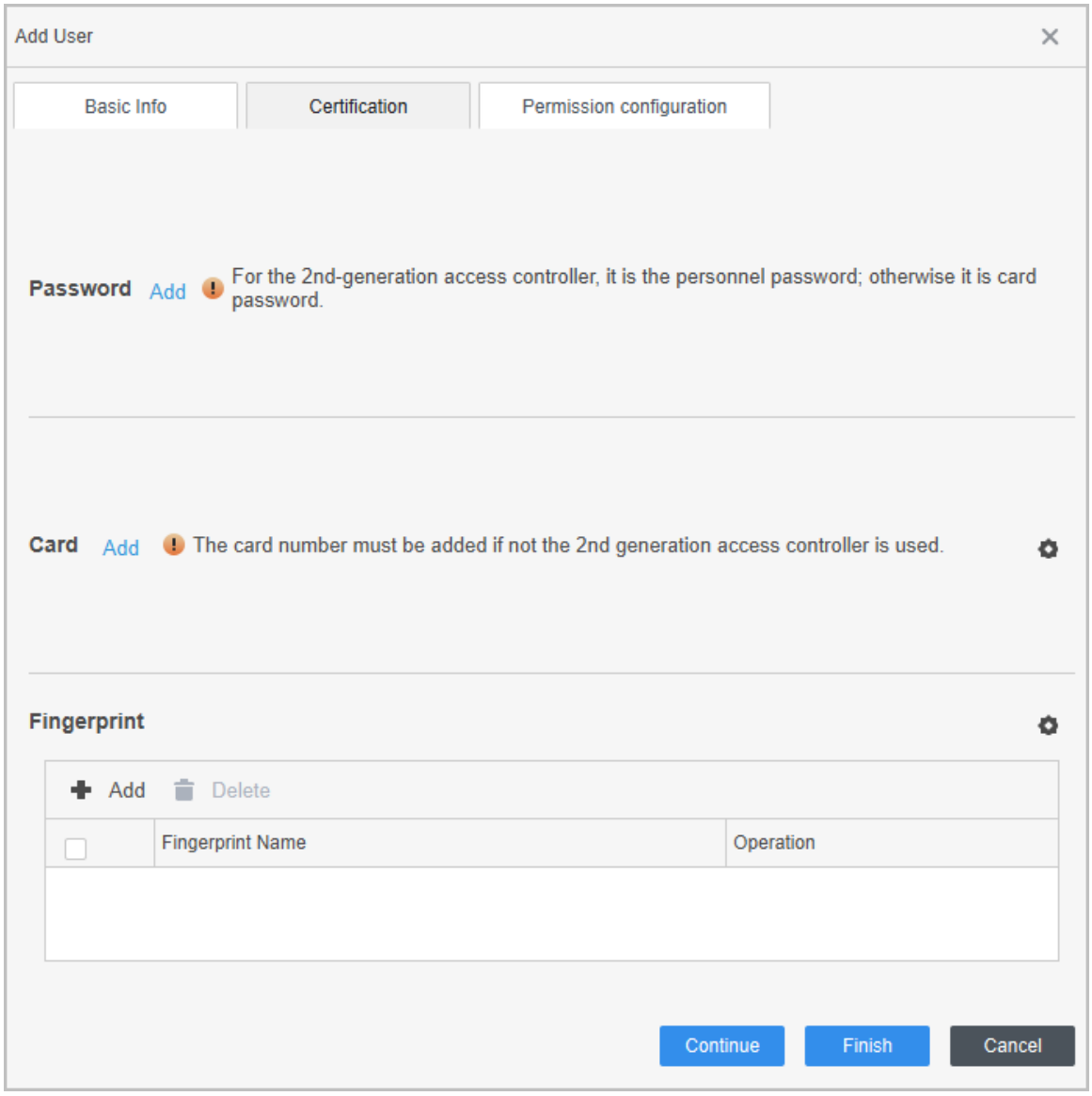
3. Haga clic en**DE ACUERDO**.

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

- Configurar huella dactilar.

1. En el**Huella dactilar**área, haga clic y seleccione**Escáner de huellas dactilares**y luego haga clic en **DE ACUERDO**.
2. Haga clic en**Agregar huella digital**, presione el dedo sobre el escáner tres veces seguidas.

Figura 4-4 Agregar contraseña, tarjeta y huella digital



Paso 5 Configurar permisos para el usuario. Para obtener más información, consulte "4.3.3 Asignación de permisos de acceso".

Paso 6 Hacer clic**Finalizar**.

4.3.2.2 Adición de lotes

Puede agregar usuarios en lotes.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

Paso 3 Seleccionar**Emisor de la tarjeta**desde el**Dispositivo**list, y luego configure los parámetros.

Figura 4-5 Agregar usuarios en lotes

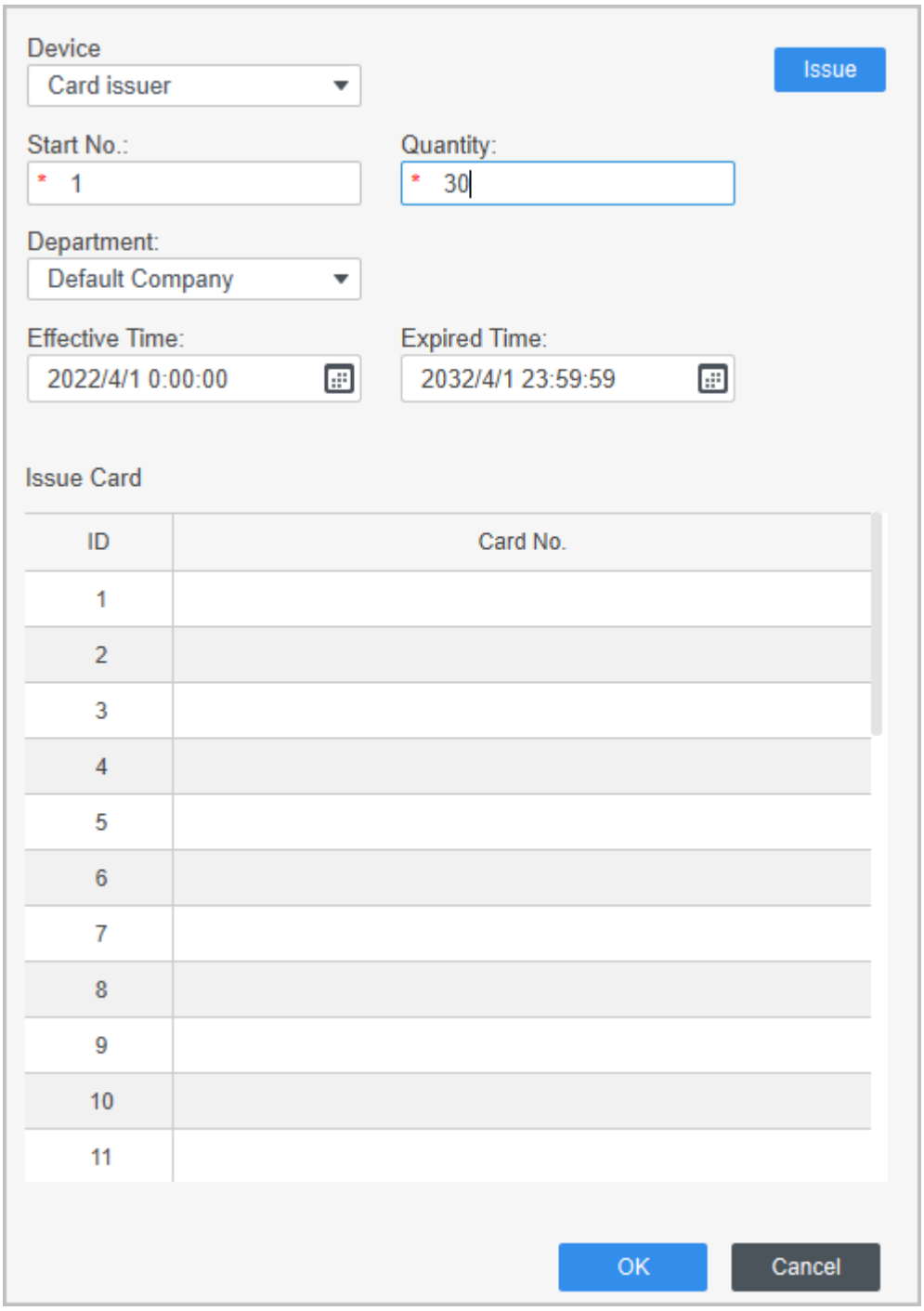


Tabla 4-2 Parámetros de agregar usuarios en lotes

Parámetro	Descripción
Nº de inicio	El ID de usuario comienza con el número que definió.
Cantidad	El número de usuarios que desea agregar.
Departamento	Seleccione el departamento al que pertenece el usuario.
Tiempo Efectivo/Tiempo Vencido	Los usuarios pueden desbloquear la puerta dentro del período definido.

Etapa 4 Hacer clic**Asunto**.

El número de tarjeta se leerá automáticamente. Hacer clic**DE**

Paso 5 **ACUERDO**.

Paso 6 Sobre el**Usuario**página, haga clic para completar la información del usuario.

4.3.3 Asignación de permiso de acceso

Cree un grupo de permisos que sea una colección de permisos de acceso a puertas y luego asocie usuarios con el grupo para que los usuarios puedan desbloquear las puertas correspondientes.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Solución de acceso**>**Gerente de Personal**>**Configuración de permisos**. Haga clic

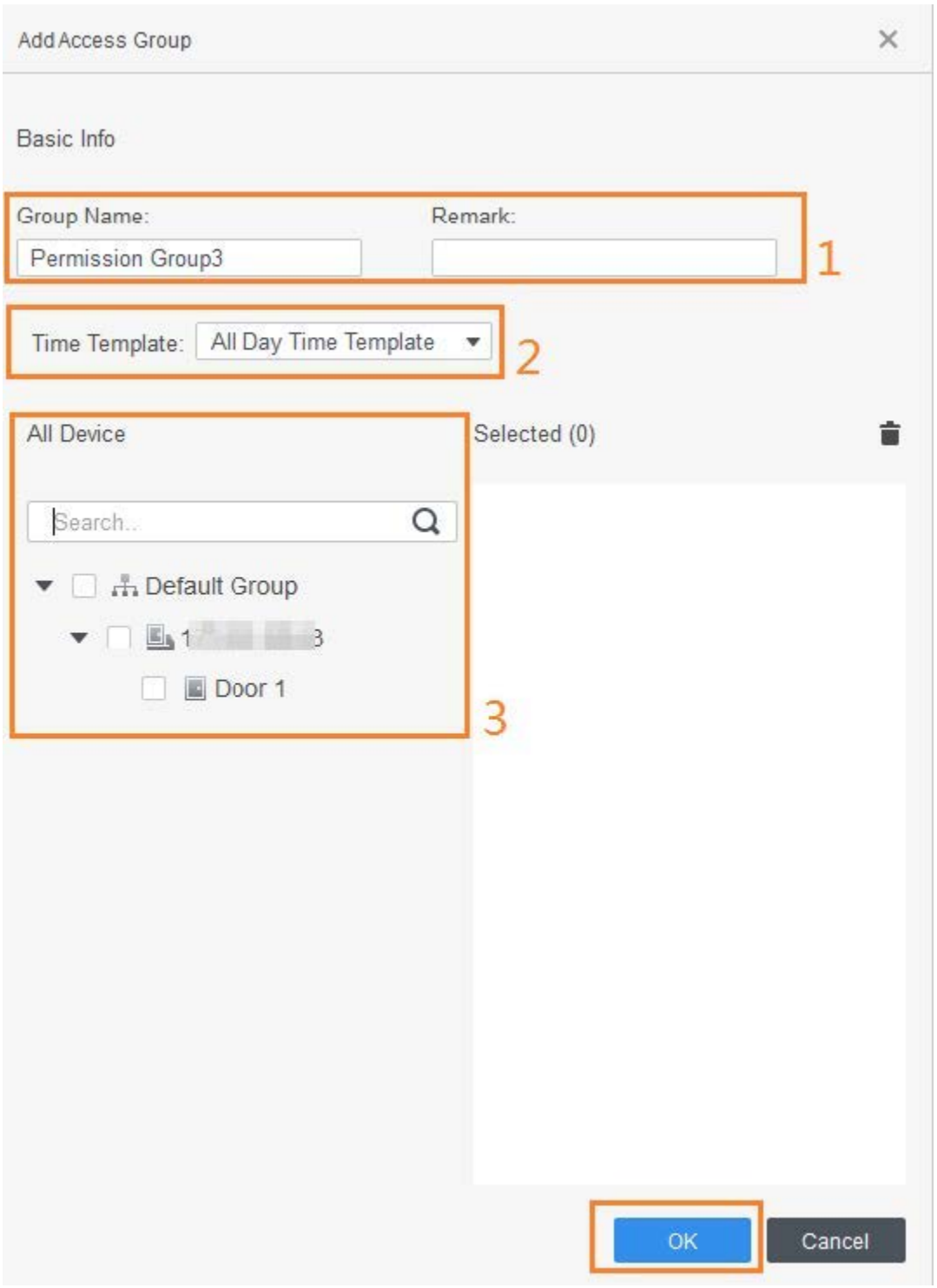
Paso 3 en .

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

Paso 5 Seleccione el dispositivo de control de acceso.

Paso 6 Hacer clic**DE ACUERDO**.

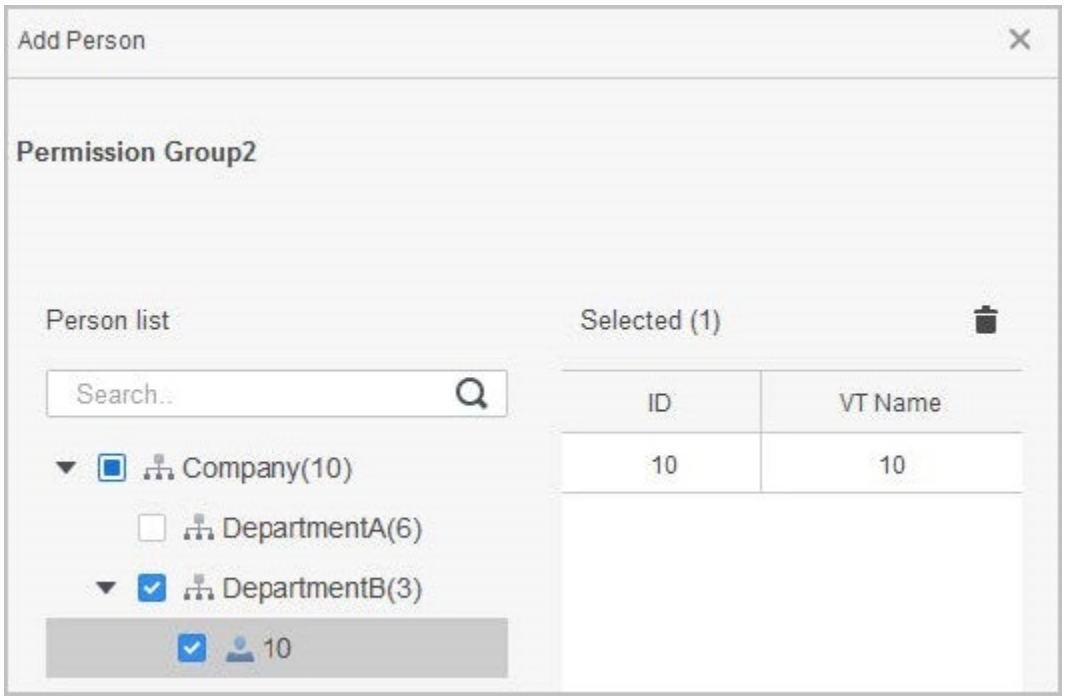
Figura 4-6 Crear un grupo de permisos



Paso 7 Hacer clic del grupo de permisos que agregó.

Paso 8 Seleccione usuarios para asociarlos con el grupo de permisos.

Figura 4-7 Agregar usuarios a un grupo de permisos



Paso 9 Hacer clic**DE ACUERDO**.

Los usuarios del grupo de permisos pueden desbloquear la puerta después de una verificación de identidad válida.

4.4 Gestión de acceso

4.4.1 Apertura y cierre de puertas a distancia

Puede monitorear y controlar la puerta de forma remota a través de Smart PSS Lite. Por ejemplo, puede abrir o cerrar la puerta de forma remota.

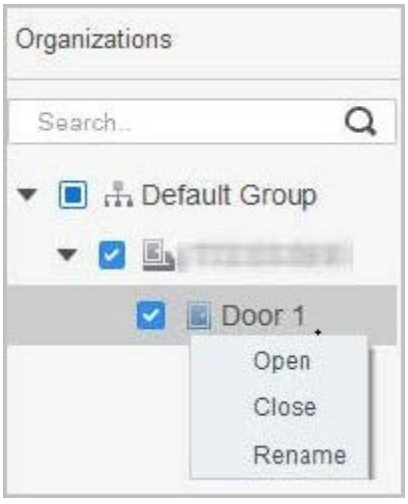
Procedimiento

Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

Paso 2 Controlar remotamente la puerta.

- Seleccione la puerta, haga clic derecho y seleccione**Abierto**o**Cerca**.

Figura 4-8 Puerta abierta



- Haga clic en o para abrir o cerrar la puerta.

Operaciones relacionadas

- Filtrado de eventos: Seleccione el tipo de evento en el**Información del evento**y la lista de eventos muestra el tipo de evento seleccionado, como eventos de alarma y eventos anormales.
- Bloqueo de actualización de eventos: haga clic para bloquear la lista de eventos, y luego la lista de eventos dejará de actualizarse. Haga clic para desbloquear.
- Eliminación de eventos: Haga clic para borrar todos los eventos en la lista de eventos.

4.4.2 Configuración de Siempre abierto y Siempre cerrado

Después de configurar siempre abierta o siempre cerrada, la puerta permanece abierta o cerrada todo el tiempo.

Procedimiento

Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

Paso 2 Hacer clic**Siempre abierto**o**Siempre Cerrar**para abrir o cerrar la puerta.

Figura 4-9 Siempre abierto o cerrado

La puerta permanecerá abierta o cerrada todo el tiempo. Puedes hacer clic**Normal**para restaurar el control de acceso al estado normal, y luego la puerta se abrirá o cerrará según los métodos de verificación configurados.

4.4.3 Supervisión del estado de la puerta

Procedimiento

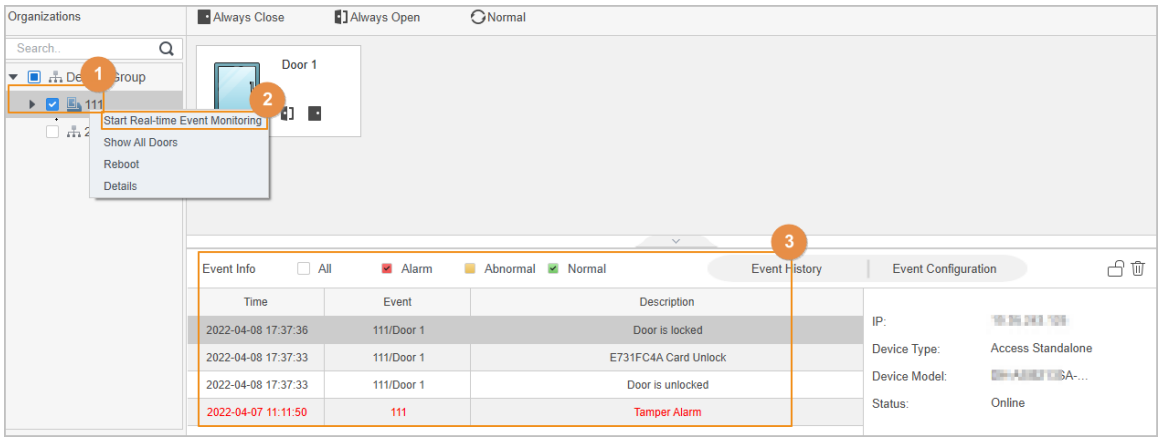
Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

Paso 2 Seleccione Access Standalone en el árbol de dispositivos, haga clic derecho y luego seleccione**Iniciar monitoreo de eventos en tiempo real**.

Los eventos de control de acceso en tiempo real se mostrarán en la lista de eventos.

Hacer clic**Detener supervisión**, los eventos de control de acceso en tiempo real no se mostrarán.

Figura 4-10 Supervisar el estado de la puerta



Operaciones relacionadas

- Mostrar todas las puertas: muestra todas las puertas controladas por Access Standalone.
- Reiniciar: reinicie Access Standalone.
- Detalles: vea los detalles del dispositivo, como la dirección IP, el modelo y el estado.

Apéndice 1 Puntos importantes de la huella digital

Instrucciones de registro

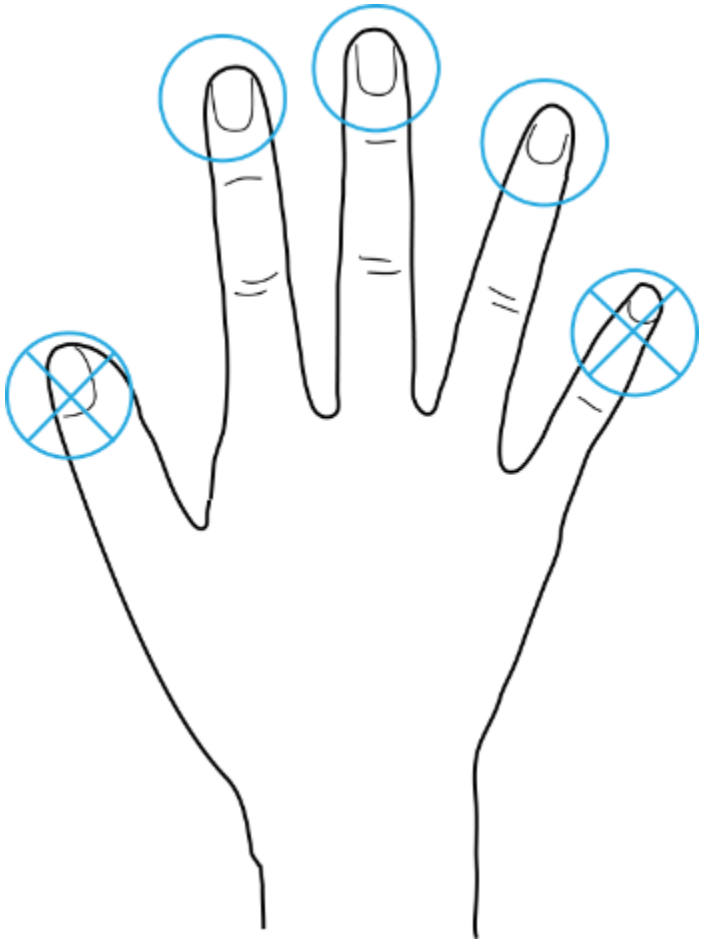
Cuando registre la huella digital, preste atención a los siguientes puntos:

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

Dedos recomendados

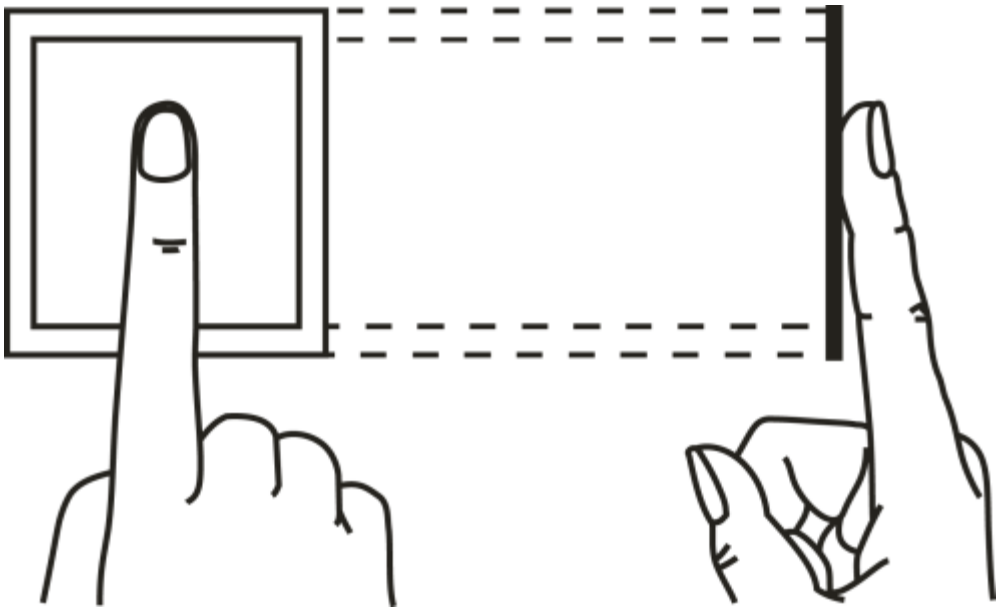
Se recomiendan los dedos índice, medio y anular. Los pulgares y los meñiques no se pueden colocar fácilmente en el centro de grabación.

Apéndice Figura 1-1 Dedos recomendados

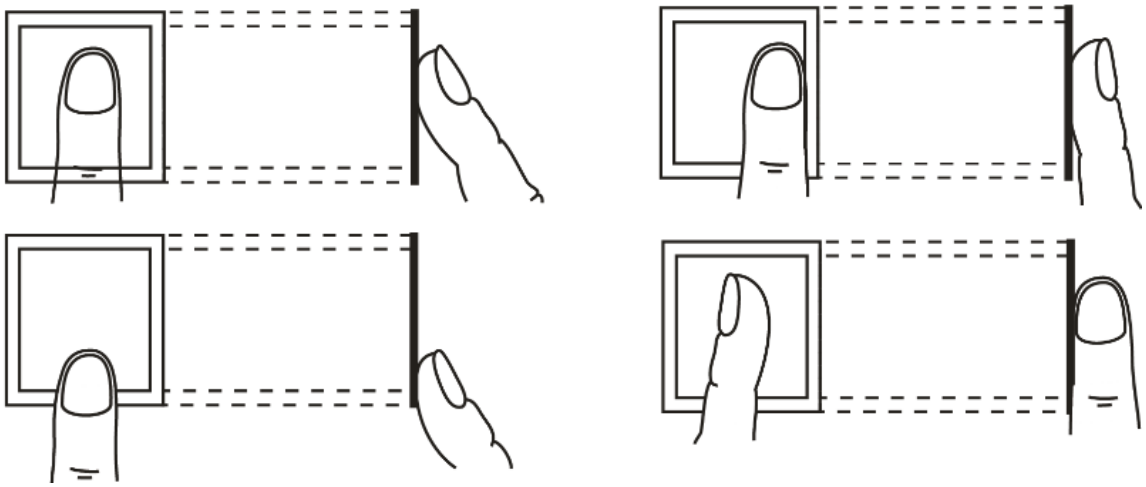


Cómo presionar su huella digital en el escáner

Apéndice Figura 1-2 Colocación correcta



Apéndice Figura 1-3 Colocación incorrecta



Apéndice 2 Recomendaciones sobre 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 contenga el nombre de la cuenta o el nombre de la cuenta en orden inverso.
- No utilice caracteres continuos, como 123, abc, etc.
- No utilice caracteres superpuestos, como 111, aaa, etc.

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

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

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su dispositivo:

1.**Protección Física**

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

2.**Cambie las contraseñas regularmente**

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

3.**Establecer y actualizar contraseñas Restablecer información a tiempo**

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

4.**Habilitar bloqueo de cuenta**

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

5.**Cambiar HTTP predeterminado y otros puertos de servicio**

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

6.**Habilitar HTTPS**

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

7.**Enlace de dirección MAC**

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

el riesgo de suplantación de ARP.

8.**Asigne cuentas y privilegios de manera razonable**

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

9.**Deshabilite los servicios innecesarios y elija modos seguros**

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

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

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

10**Transmisión encriptada de audio y video**

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

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

11**Auditoría segura**

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

12**Registro de red**

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

13**Construir un entorno de red seguro**

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

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