Acceso independiente

Guía de inicio rápido

V1.0.0

Prefacio

General

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

Las instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	septiembre 2021

Aviso de protección de privacidad

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

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas.

Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre la versión electrónica y la versión en papel.

- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el controlador de acceso.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

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

Requisitos operativos

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

requerimientos de instalación

 **ADVERTENCIA**

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

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

Tabla de contenido

1 Estructura

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

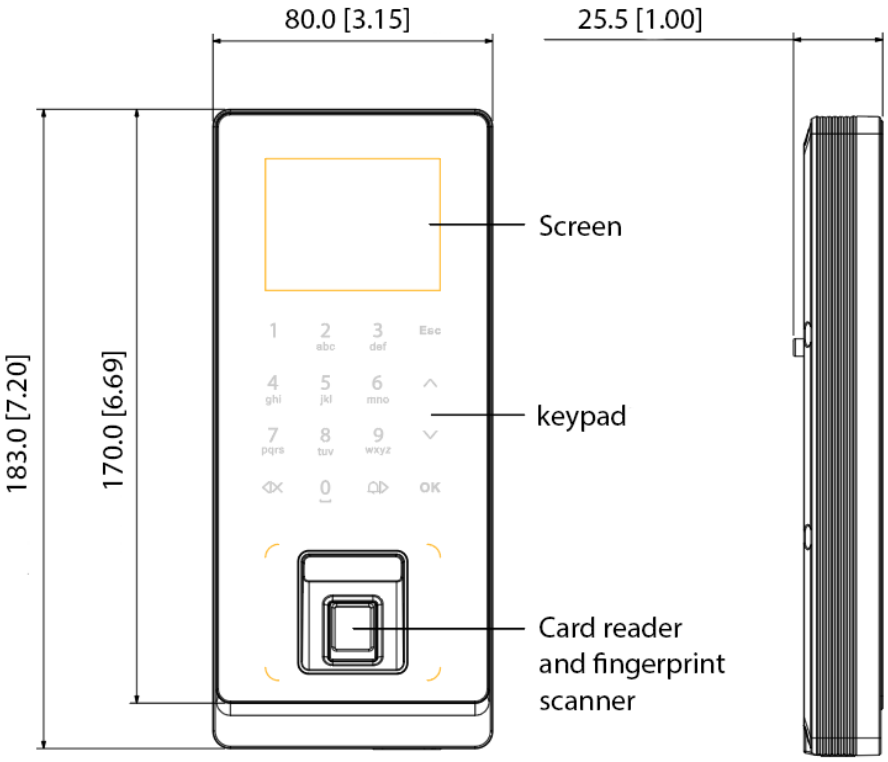
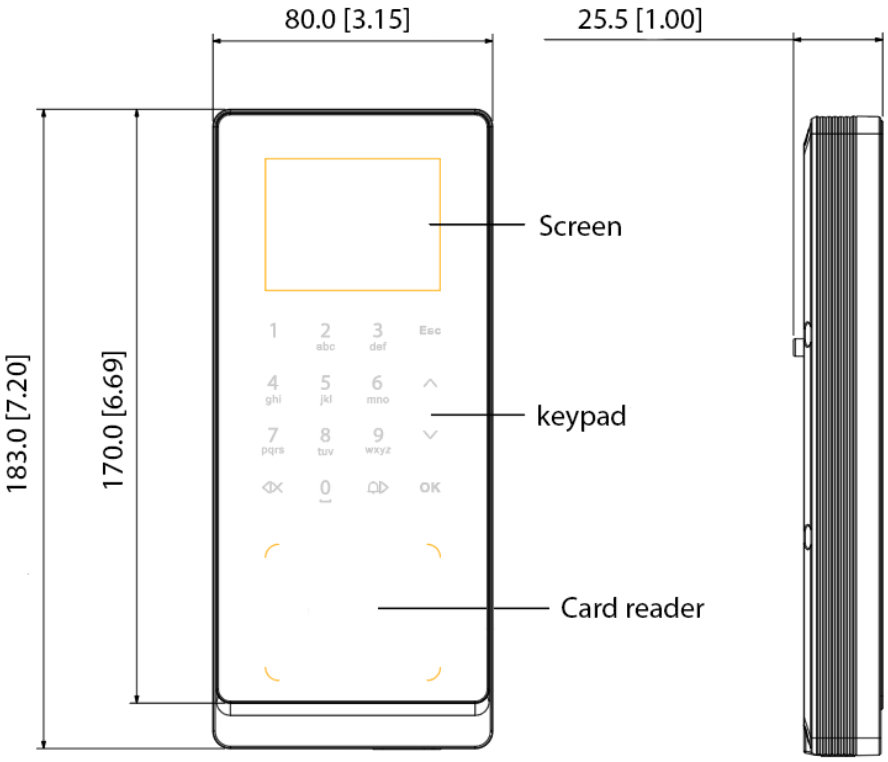


Figure 1-2 Dimensiones (2) (mm [pulgadas])



2 Cableado e Instalación

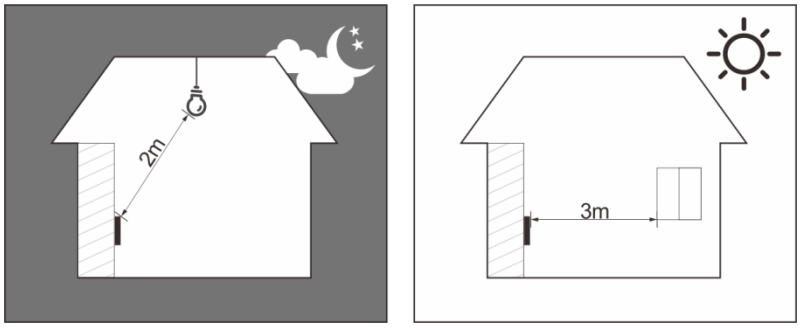
2.1 Requisitos ambientales

- La iluminación a 0,5 m del dispositivo no debe ser inferior a 100 lx.

Figure 2-1 Entorno de instalación

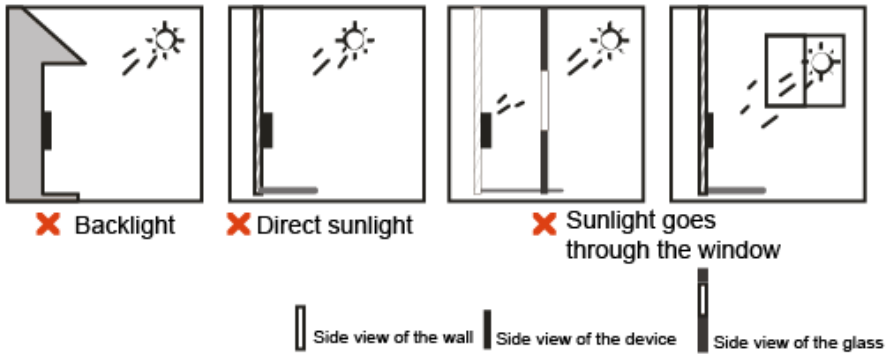
- Recomendamos instalar el dispositivo en interiores, a 3 m de las ventanas o puertas y a 2 m de cualquier fuente de luz.

Figure 2-2 Posición de instalación



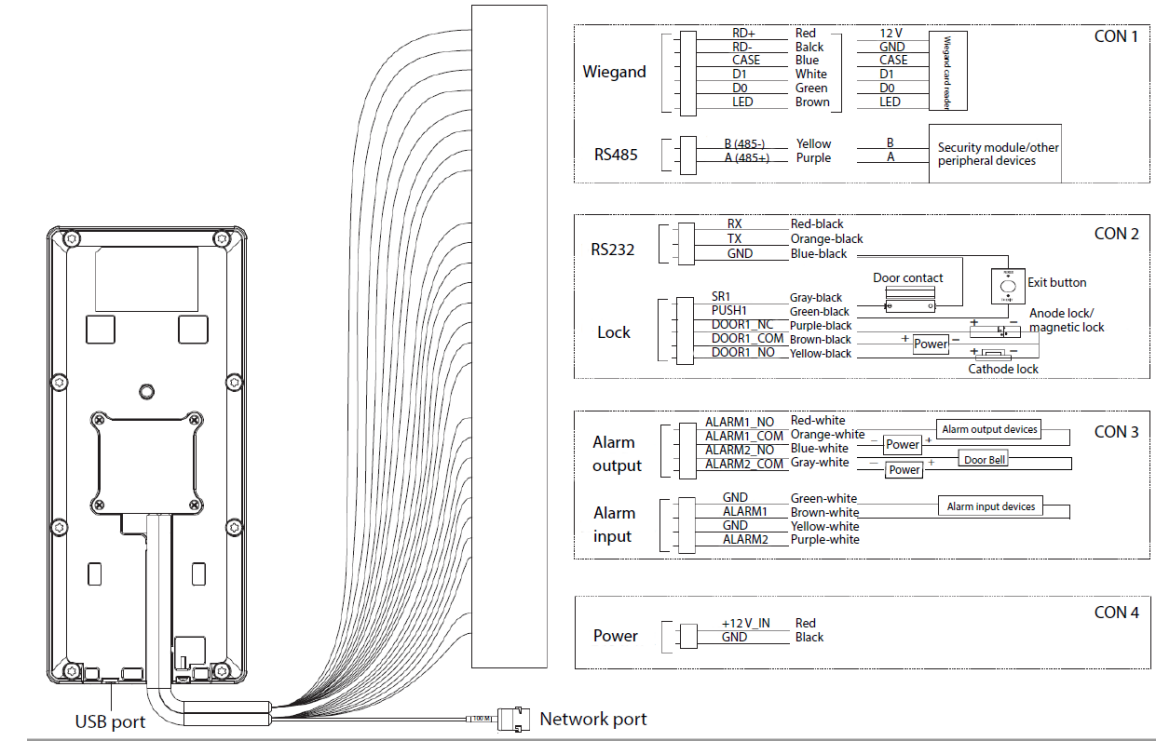
- No exponga el dispositivo a la luz de fondo, a la luz solar ni lo coloque cerca de ninguna luz.

Figure 2-3 Lugares no recomendados



2.2 Alambrado

Figure 2-4 Descripción del cableado



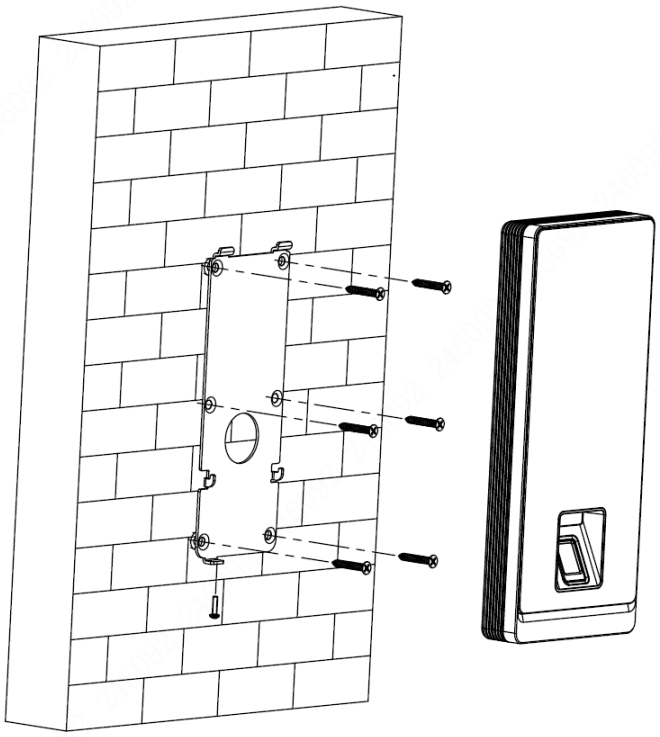
- En el portal web, seleccione**Gestión de configuración**>**Características**para comprobar si**Módulo de seguridad**está habilitado.

  Si está habilitado, debe comprar un módulo de seguridad compatible y requiere una fuente de alimentación separada suministro.
- Cuando el módulo de seguridad está habilitado, el botón de salida de la puerta, el bloqueo y el enlace de disparo no serán válidos.

2.3 Instalación

Esta sección utiliza un dispositivo con la función de huella digital como ejemplo. Le recomendamos que instale el dispositivo a 1,2 m–1,6 m por encima del suelo (desde el centro de la lente hasta el suelo).

Figure 2-5 Instale el dispositivo en la pared.



Step 1 Marque los agujeros en la pared de acuerdo con el soporte. Taladre seis orificios para tornillos y una salida de cable en la pared. Coloque pernos de expansión en los agujeros.

Step 2 Use tornillos para fijar el soporte a la pared. Conecte

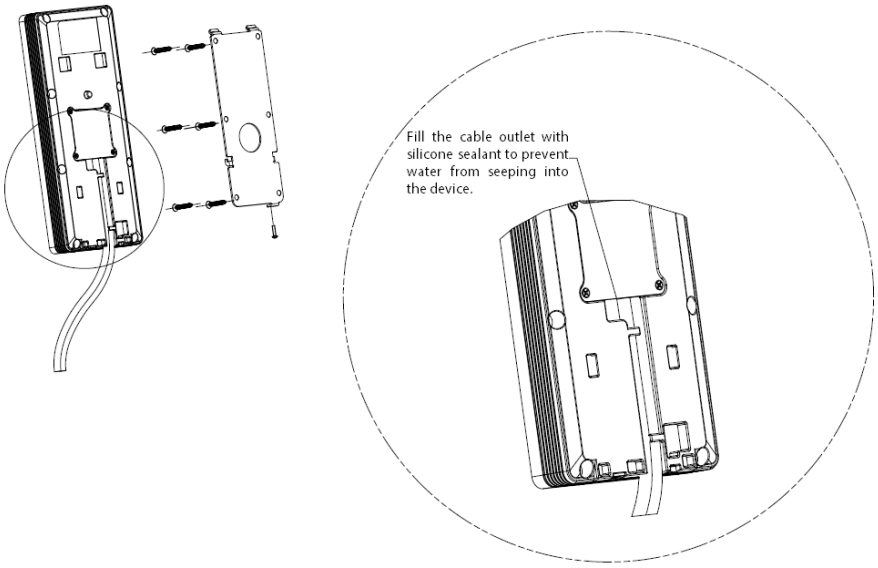
Step 3 el dispositivo. Consulte "2.2 Cableado".

Step 4 Coloque el dispositivo en los ganchos del soporte. Apriete el

Step 5 tornillo en la parte inferior del dispositivo. (Opcional) Aplique

Step 6 sellador de silicona a la salida del cable.

Figure 2-6 Aplicar sellador de silicona



3 configuraciones locales

3.1 Inicialización

Para el uso por primera vez o después de restaurar los valores predeterminados de fábrica, debe establecer una contraseña y vincular su dirección de correo electrónico para la cuenta de administrador. También debe configurar la zona horaria del dispositivo. Puede usar la cuenta de administrador para iniciar sesión en el menú principal del dispositivo, configurar el dispositivo e iniciar sesión en la interfaz web y SmartPSS AC.

Figure 3-1 Inicializar el dispositivo

- Si olvida la contraseña de administrador, envíe una solicitud de restablecimiento a su dirección de correo electrónico vinculada.
- 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.

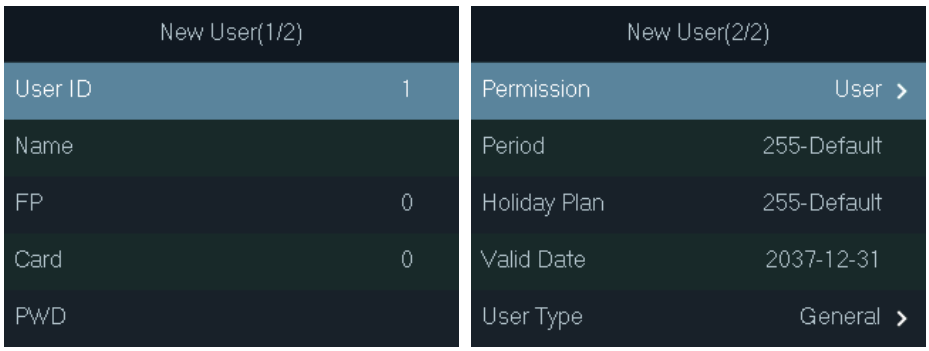
3.2 Adición de usuarios

Step 1 En la interfaz de espera, los botones de flecha para seleccionar y luego toque**OK**.

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

Las interfaces en este manual son solo para referencia y pueden diferir del producto real.

Figure 3-2 Agregar un nuevo usuario



Step 3 Configure los parámetros.

Tabla 3-1 Descripción de los parámetros de usuario

Parámetro	Descripción
IDENTIFICACIÓN.	Cada ID de usuario es único. Pueden ser 18 caracteres de números, letras o su combinación.
Nombre	Puede ingresar nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
Huella dactilar	Cada usuario puede agregar hasta 3 huellas dactilares. Siga las indicaciones en pantalla y las indicaciones de voz para agregar huellas dactilares. Puede habilitar la función de huella digital bajo coacción debajo de cada huella digital. Después de habilitar la función de alarma de coacción, se activará una alarma si la puerta se desbloquea con la huella dactilar de coacción. - No recomendamos configurar la primera huella digital como huella digital de coacción. - Solo ciertos modelos admiten la función de huella digital.
Tarjeta	Puede registrar cinco tarjetas para cada usuario. En la interfaz de registro de la tarjeta, deslice su tarjeta y luego el dispositivo leerá la información de la tarjeta. Puede habilitar la función de tarjeta de coacción en la interfaz de registro de 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 solo tienen permiso de desbloqueo de puertas. ● Los administradores pueden configurar el dispositivo y desbloquear la puerta.
Período	Un usuario solo puede desbloquear la puerta dentro del período definido. El valor predeterminado es 255, lo que significa que el usuario puede desbloquear la puerta en cualquier momento.
Fiesta Plan	Un usuario solo puede desbloquear la puerta dentro del período definido. El valor predeterminado es 255, lo que significa que el usuario puede desbloquear la puerta en cualquier momento.
Fecha válida	Defina un período durante el cual el usuario tiene control de acceso a la puerta.
Tipo de usuario	● **General**: Los usuarios generales pueden desbloquear la puerta normalmente. ● **Lista de bloqueos**: cuando los usuarios de la lista de bloqueo desbloquean la puerta, el personal de servicio recibe una notificación. ● **Huésped**: Los invitados pueden desbloquear la puerta dentro de un período definido o por una cierta cantidad 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 usuario VIP desbloquea la puerta, el personal de servicio recibe una notificación. El usuario VIP no está restringido por modos de desbloqueo, como **multitarjeta** y**Sección de tiempo**. ● **Otros**: Cuando desbloqueen la puerta, la puerta permanecerá desbloqueada durante 5 segundos más. ● **Usuario personalizado 1/2**: Igual que**General**.

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

Step 5 **OK**para guardar la configuración.

4 Configuraciones Web

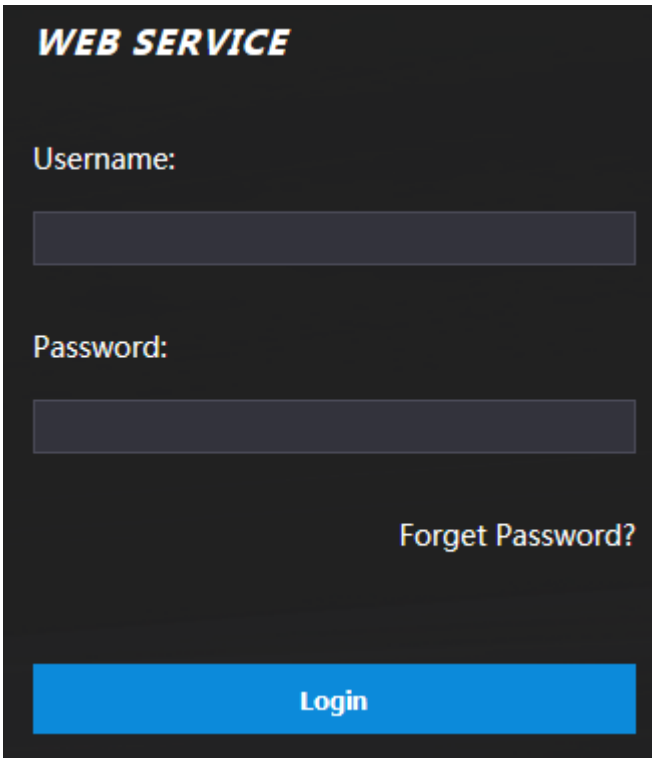
En la interfaz web, puede configurar y actualizar el dispositivo. Para obtener más información, consulte "Acceder al Manual del usuario independiente". Aquí sólo se describe la operación de inicio de sesión en la web.

4.1 Iniciar sesión en la computadora

Step 1 Vaya a la dirección IP (192.168.1.108 por defecto) del dispositivo en un navegador y presione la tecla Enter.

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

Figure 4-1 Acceso



Step 2 Introduzca el nombre de usuario y la contraseña.

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

Step 3 Hacer clic**Acceso**.

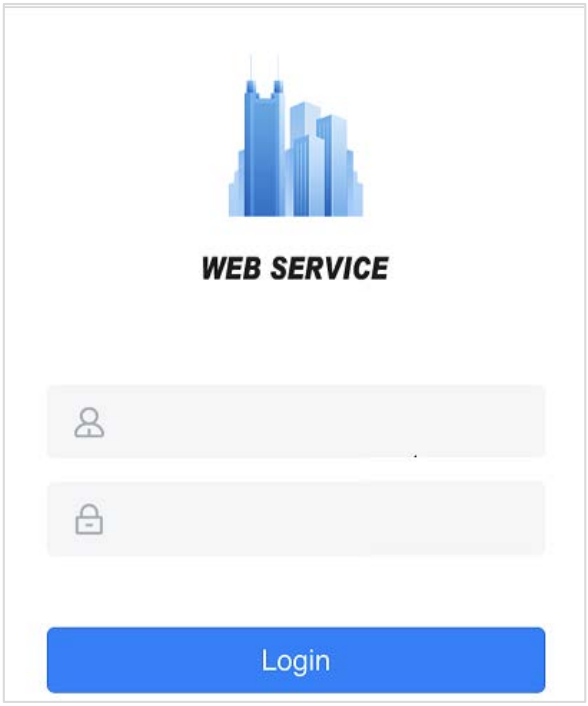
4.2 Iniciar sesión en el teléfono

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

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

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

Figure 4-2 Acceso



Step 2 Introduzca el nombre de usuario y la contraseña.

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

Step 3 Hacer clic**Acceso**.

Appendix 1 Instrucciones de registro de huellas dactilares

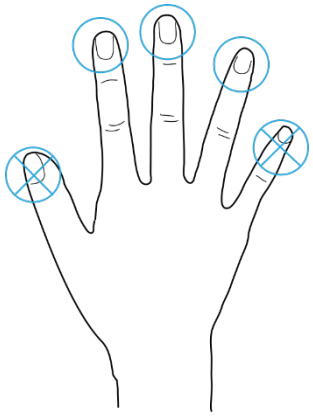
Antes de registrar sus huellas dactilares, preste atención a lo siguiente:

- Asegúrese de que sus dedos 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

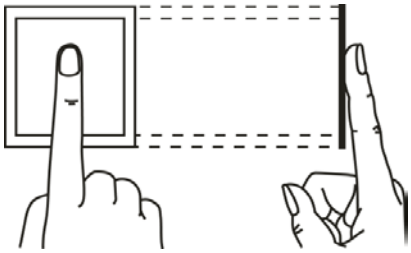
Se recomiendan los dedos índice, medio y anular. Los pulgares y los meñiques no se pueden colocar fácilmente en el centro de grabación.

Apéndice Figura 1-1 Dedos recomendados

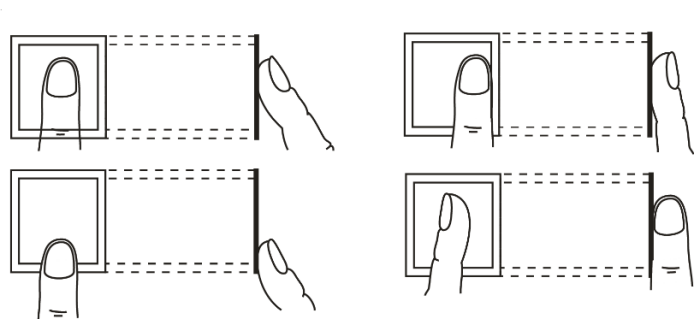


Cómo presionar su huella digital en el escáner

Apéndice Figura 1-2 Correcto



Apéndice Figura 1-3 Incorrecto



Appendix 2 Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación se presentan algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

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

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

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

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

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

2. Cambie las contraseñas regularmente

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

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

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

Le recomendamos vincular la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de suplantación de identidad ARP.

8. Asigne cuentas y privilegios de manera razonable

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

9. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

10. Transmisión encriptada de audio y video

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

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

11. Auditoría segura

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

12. Registro de red

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

13. Construya un entorno de red seguro

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

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