

Estación de puerta digital (Serie VTO65)

Guía de inicio rápido



Prefacio

General

Este manual presenta las operaciones básicas de la estación de puerta digital (VTO). Para obtener más información, consulte el manual del usuario.

Modelo

VTO6521H, VTO6521H-D, VTO6531H, VTO6541H VTO6521F,

VTO6531F.

Instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con significado definido pueden aparecer en el manual.

Palabras de advertencia	Sentido
 PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría resultar en daños materiales, daños, pérdida de datos, menor rendimiento o resultado impredecible.
 Nota	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento	Febrero de 2020

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida causada por las operaciones que no cumplan con el manual. El manual se actualizará de acuerdo con las leyes y regulaciones más recientes de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más actualizado y la documentación complementaria. Todavía puede haber desviaciones en los datos técnicos, la descripción de funciones y operaciones, o errores en la impresión. Si hay alguna duda o disputa, nos reservamos el derecho a una explicación final. Actualice el software del lector o pruebe con otro software de lectura convencional si no puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.

- Visite nuestro sitio web, póngase en contacto con el proveedor o el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si existe alguna duda o controversia, nos reservamos el derecho a una explicación final.

Advertencias y medidas de seguridad importantes

La siguiente descripción es el método de aplicación correcto del dispositivo. Lea atentamente la guía antes de usarla para evitar peligros y pérdidas materiales. Cumpla estrictamente con la Guía durante la aplicación y consérvelos correctamente después de leerlos.

Requisito de funcionamiento

- No coloque ni instale el dispositivo en un área expuesta a la luz solar directa o cerca de un dispositivo generador de calor.
- No instale el dispositivo en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal, o instálelo en lugares estables, y evite que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo; no coloque sobre el dispositivo nada lleno de líquido para evitar que fluyan hacia el dispositivo.
- Instale el dispositivo en lugares bien ventilados; no bloquee su abertura de ventilación. Utilice el dispositivo solo dentro del rango nominal de entrada y salida.
- No desmonte el dispositivo de forma arbitraria.
- El dispositivo se utilizará con cables de red apantallados.

Requisitos de energía

- Utilice cables eléctricos (cables de alimentación) recomendados por esta área, que se utilizarán dentro de su especificación nominal.
- Utilice una fuente de alimentación que cumpla con los requisitos de SELV (voltaje de seguridad muy bajo) y suministre energía con un voltaje nominal que cumpla con la Fuente de energía limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del dispositivo.
- El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.
- No corte la fuente de alimentación durante la actualización del dispositivo. La fuente de alimentación se puede cortar solo después de que el dispositivo haya completado la actualización y se haya reiniciado.

Tabla de contenido

Prólogo	YO Advertencias y salvaguardias importantes	III 1 Estructura
.....	1
2 Conexión de cable		2
3 Instalación		3
4 Configuración web		6
4.1 Proceso de configuración		6
4.2 Inicialización de la interfaz web		6
4.3 Modificación de la dirección IP		8
4.4 Selección de servidores SIP		8
4.4.1 Videoportero (VTO) como servidor SIP		9
4.4.2 Plataforma (DSS Express / DSS Pro) como servidor SIP		12
5 Configuración de ingeniería		dieciséis
5.1 Entrar en la configuración de ingeniería		dieciséis
5.2 Configuración de la dirección IP		dieciséis
6 Registro de usuario		17
Apéndice 1 Notas sobre la grabación facial		18
Apéndice 2 Instrucción de registro de huellas dactilares		20
Apéndice 3 Recomendaciones de ciberseguridad		22

1 Estructura

La estación de puerta (VTO) tiene seis modelos. Los diferentes modelos tienen diferentes paneles frontales pero el mismo panel trasero.

Figura 1-1 Dimensiones (mm [pulgadas])

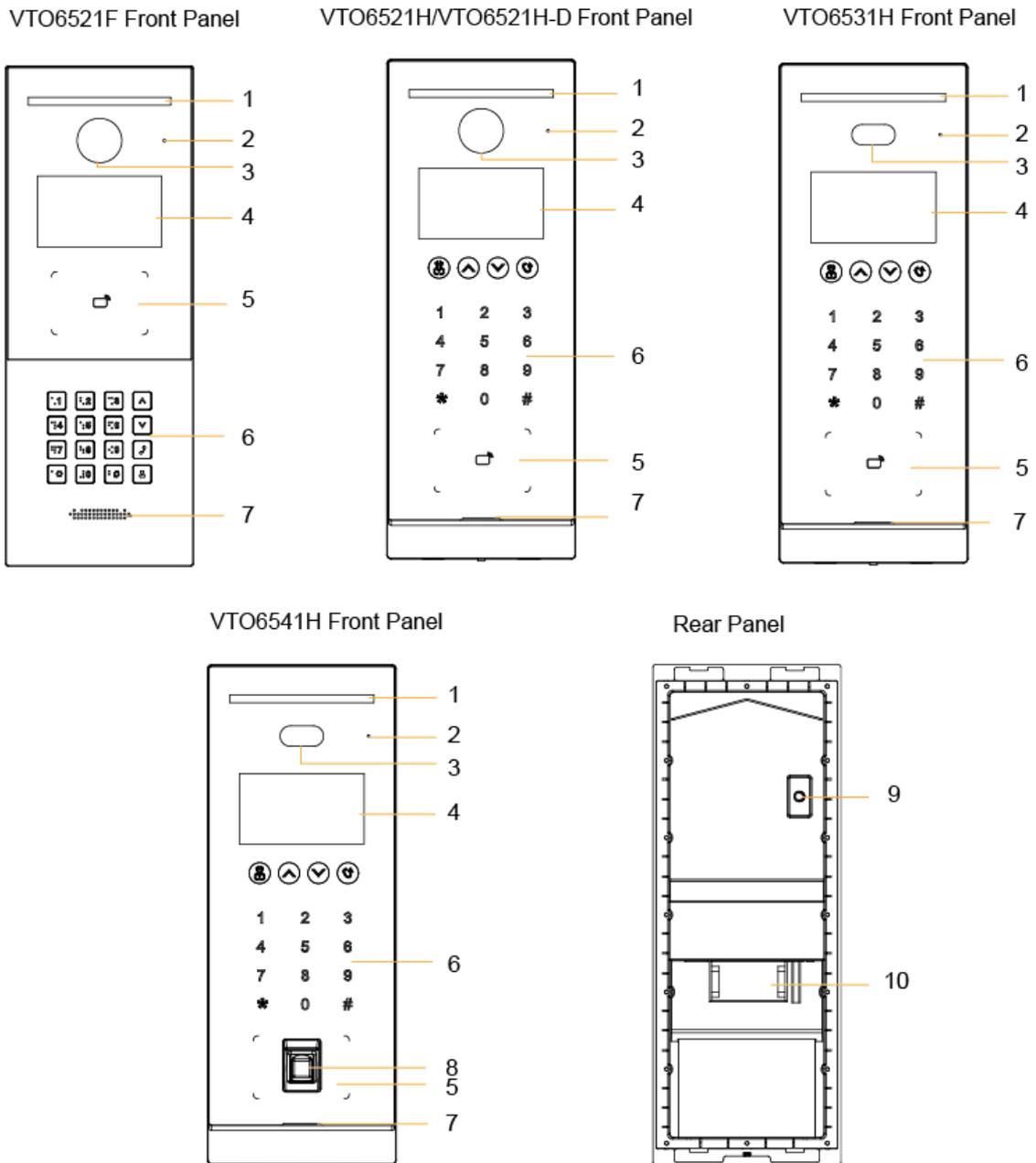
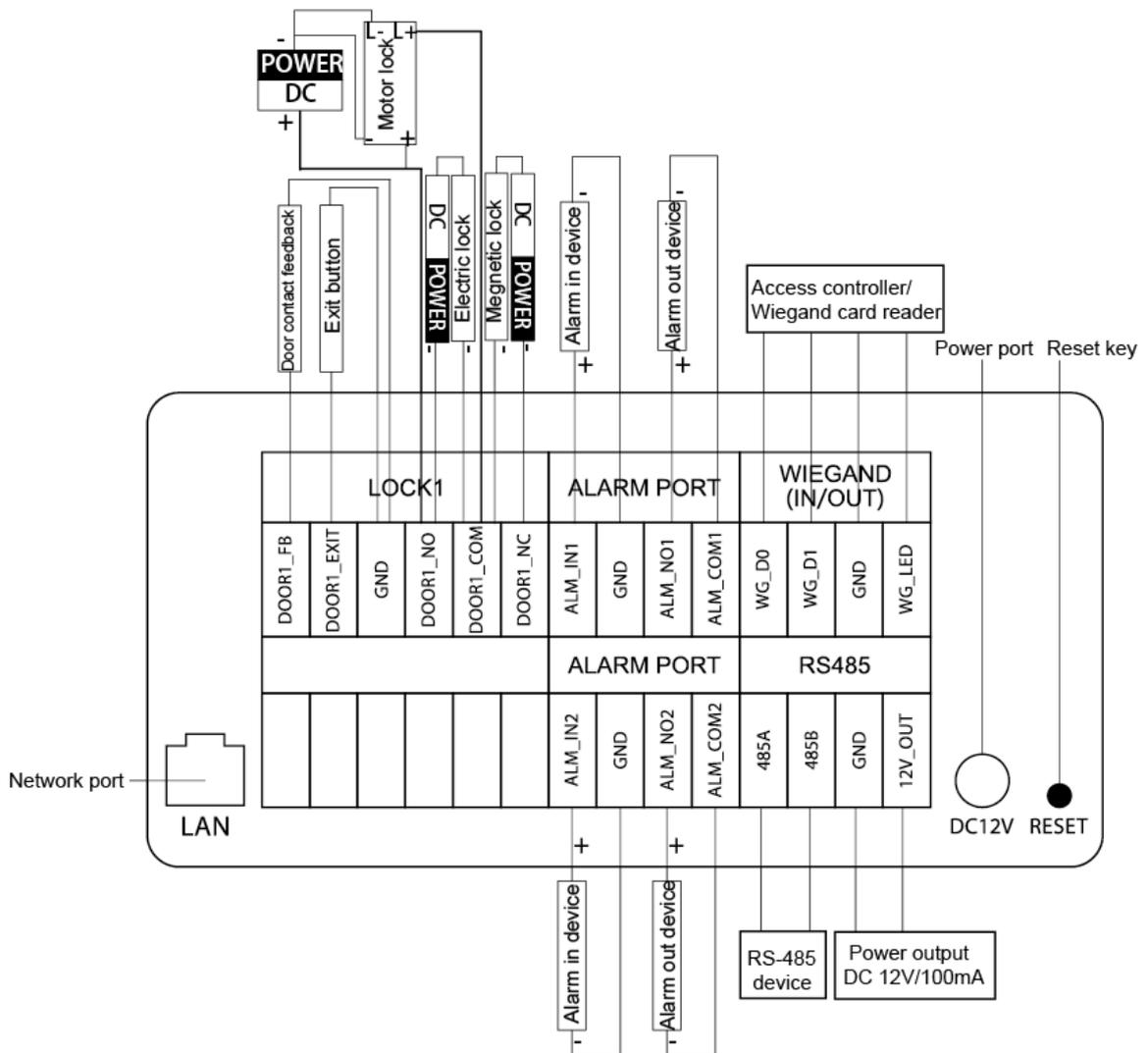


Tabla 1-1 Comp descripción onent

No.	Descripción	No.	Descripción
1	Iluminador blanco	6	Teclado
2	MIC	7	Altoparlante
3	Cámara	8	Sensor de huellas dactilares
4	Monitor	9	Botón de sabotaje
5	Área de deslizamiento de tarjetas	10	Puertos de función (conectados a cerraduras, controladores de acceso, dispositivos de entrada / salida de alarma)

2 Conexión de cable

Figura 2-1 Conexión de cables



3 Instalación



- No instale el videoportero digital en un ambiente con condensación, alta temperatura, luz solar directa y lugares manchados, polvorientos o químicamente corrosivos.
- La instalación y la prueba de ingeniería deben ser realizadas por profesionales. No desmonte ni repare arbitrariamente en caso de falla del dispositivo. Póngase en contacto con el servicio posventa.
- Prepare usted mismo destornilladores cruzados y guantes.
- La distancia recomendada entre la cámara y el suelo es de 1,4 a 1,6 m.

Figura 3-1 Altura de instalación

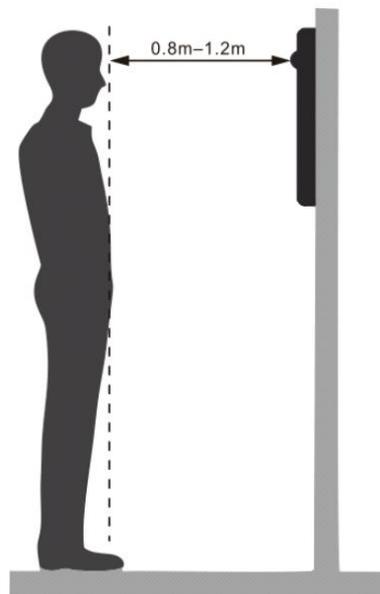


Figura 3-2 Instalación

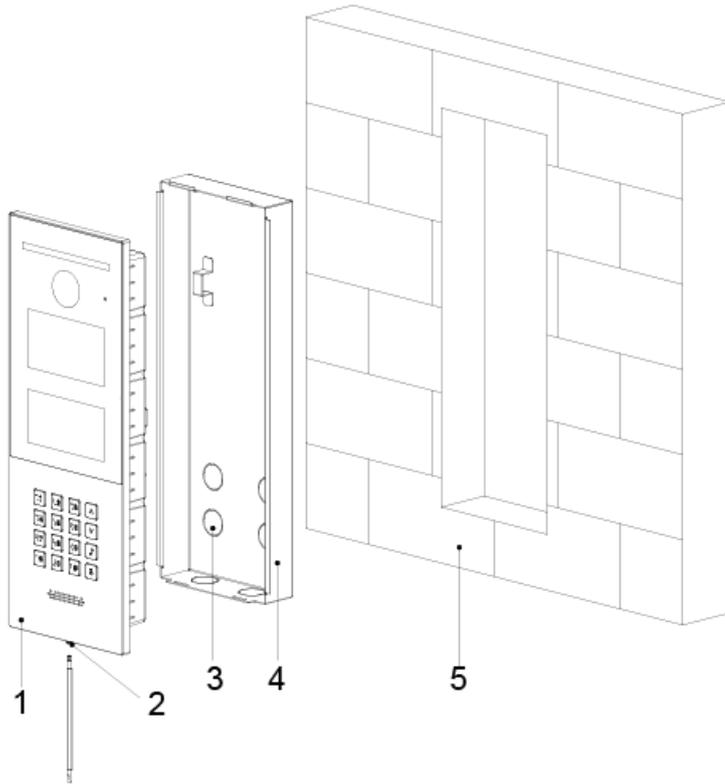


Tabla 3-1 Descripción de los componentes

No.	Descripción	No.	Descripción	No.	Descripción
1	Estación de puerta	3	Entrada de cable	5	pared
2	Tornillo	4	Placa de montaje	-	-

Procedimiento de instalación

Paso 1 Corte una abertura en la pared de acuerdo con las dimensiones de la placa de montaje.

Paso 2 Separe las tapas de los orificios según las posiciones de entrada de cables.

Paso 3 Coloque la placa de montaje en la abertura de la pared.

Paso 4 Fije la placa de montaje con cemento o sellador.

Paso 5 Conecte los cables. Consulte "Conexión de 2 cables".



Antes de conectar los cables, asegúrese de que la alimentación esté desconectada.

Paso 6 Coloque la estación de puerta en la placa de montaje y luego coloque el gancho en la parte posterior estación de puerta en la ranura de instalación de la placa de montaje.

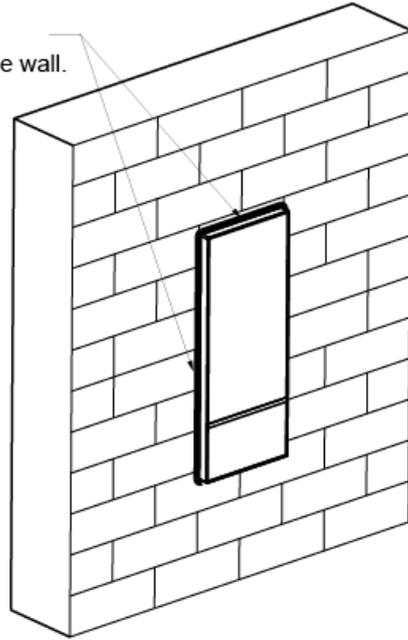
Paso 7 Apriete los tornillos en la parte inferior de la estación de puerta.

Paso 8 Aplique sellador de silicona a los espacios entre la estación de puerta y la placa de montaje.

La instalación está completa.

Figura 3-3 Aplicar sellador de silicona

Apply silicone sealant to gaps between the device and the wall.



4 Configuración web

Este capítulo presenta cómo inicializar, conectar y configurar parámetros para que las estaciones de puerta realicen funciones como la administración de dispositivos, llamadas y monitoreo. Para obtener más detalles, consulte el manual de usuario.

4.1 Proceso de configuración

Paso 1 Planifique la dirección IP y el número de cada videoportero y monitor interior.

Paso 2 Asegúrese de que no haya ningún cortocircuito o circuito abierto en los circuitos.

Paso 3 Configure la estación de puerta (VTO).

Además de inicializar la interfaz web y modificar la dirección IP, las configuraciones serán diferentes según los tipos de servidor SIP.

- 1) Cuando la estación de puerta que está operando funciona como servidor SIP, consulte "4.4.1 Estación de puerta (VTO) como servidor SIP".
- 2) Cuando la plataforma de gestión funciona como servidor SIP, consulte "4.4.2 Plataforma (DSS Express / DSS Pro) como servidor SIP".

Paso 4 Configure los monitores interiores (VTH). Consulte el manual del usuario de los monitores de interior (VTH) o el manual del usuario de la estación de puerta.

4.2 Inicialización de la interfaz web

Por primera vez, debe crear una contraseña para iniciar sesión en la interfaz web.

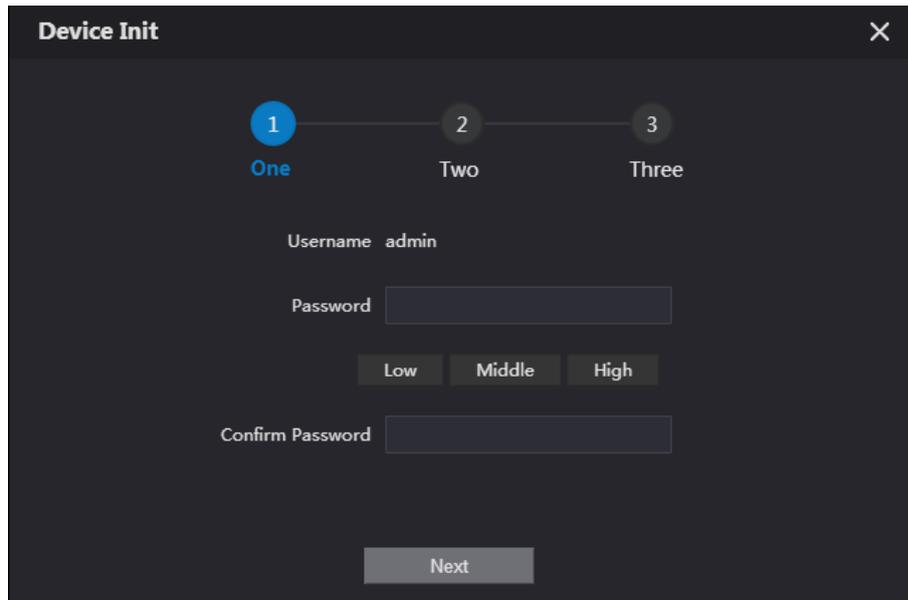


La dirección IP predeterminada de la estación de puerta es 192.168.1.108. Asegúrese de que la dirección IP de la PC esté en el mismo segmento de red que la del videoportero.

Paso 1 Conecte la estación de puerta a la fuente de alimentación y luego iníciela.

Paso 2 Abra el navegador en la PC, ingrese la dirección IP predeterminada del VTO en la dirección barra y luego presione Entrar.

Figura 4-1 Inicialización del dispositivo



Paso 3 Ingrese y confirme la contraseña, y luego haga clic en **Próximo**.

Se muestra la interfaz de configuración de correo electrónico.



La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo "":; &).

Paso 4 Seleccione el **Correo electrónico** casilla de verificación y luego ingrese su dirección de correo electrónico.



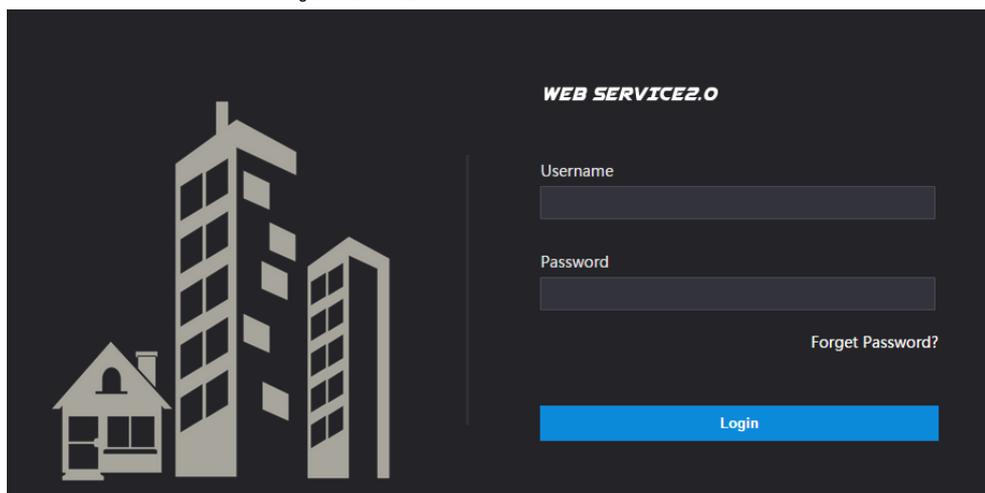
Esta dirección de correo electrónico se utiliza para restablecer la contraseña.

Paso 5 Haga clic en **Próximo**.

La inicialización tuvo éxito.

Paso 6 Haga clic en **OKAY**.

Figura 4-2 Interfaz de inicio de sesión



Paso 7 Ingrese el nombre de usuario y la contraseña, y luego haga clic en **Iniciar sesión** para iniciar sesión en la interfaz web.



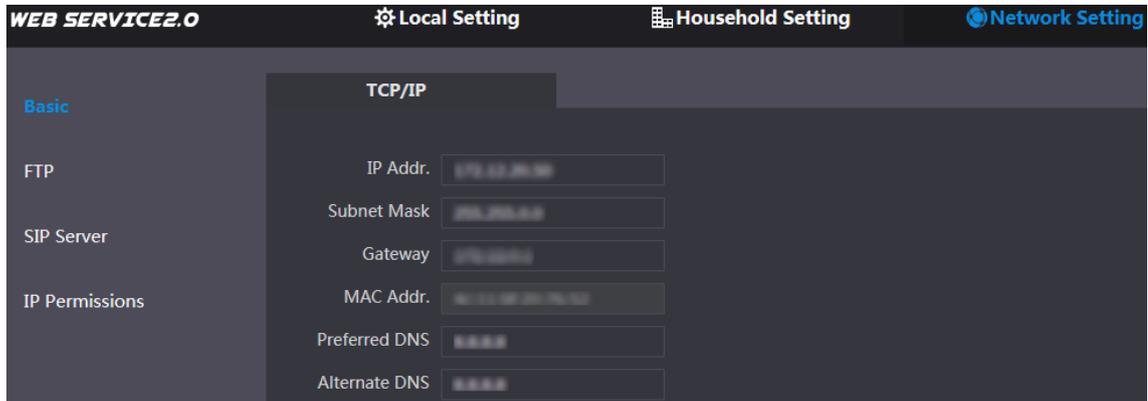
El nombre de usuario es admin por defecto; la contraseña es la que estableció en la Figura 4-1.

4.3 Modificación de la dirección IP

Para realizar la comunicación entre videoporteros, es necesario modificar la dirección IP del videoportero. Puede modificar la dirección IP en la estación de puerta o mediante la interfaz web. Aquí se demostrará cómo modificar la dirección IP a través de la interfaz web. Para modificar la dirección IP en la estación de puerta, consulte "5.2 Configuración de la dirección IP".

Paso 1 Seleccione **Configuración de red** > **Básico**.

Figura 4-3 Información de TCP / IP



Paso 2 Ingrese los parámetros de red que planeó y luego haga clic en **Salvar**.



Asegúrese de que la dirección IP de su PC y la estación de puerta estén en el mismo segmento de red.

El VTO se reiniciará.



- El DNS preferido y el DNS alternativo son 8.8.8.8 de forma predeterminada.
- Si la dirección IP de la PC está en el segmento de IP planificado, la interfaz irá a la interfaz de inicio de sesión automáticamente.
- Si la dirección IP de la PC no está en el segmento de IP planificado, la interfaz no irá a la interfaz de inicio de sesión. Debe establecer la dirección IP de la PC en el segmento de IP planificado.

4.4 Selección de servidores SIP

El Protocolo de inicio de sesión (SIP) se utiliza para señalar y controlar sesiones de comunicación multimedia en aplicaciones de llamadas de voz y video. Un servidor SIP es una aplicación que proporciona información o instrucciones a un agente de usuario.

- Cuando las estaciones de puerta (VTO) funcionan como servidor SIP, seleccione **VTO** desde el **Tipo de servidor** la lista desplegable. Se aplica a un escenario donde solo hay un edificio. Cuando la plataforma (Express / DSS) funciona como servidor SIP, seleccione **Express / DSS** desde el **Tipo de servidor** la lista desplegable. Se aplica a un escenario en el que hay varios edificios o varias unidades.

Paso 1 Inicie sesión en la página web.

Paso 2 En la página de inicio, seleccione **Configuración de red** > **Servidor SIP**.

Figura 4-4 servidor SIP

Paso 3 Seleccione un servidor SIP.

4.4.1 Videoportero (VTO) como servidor SIP

Paso 1 Seleccione el **Habilitar** casilla de verificación junto a **Servidor SIP**.

Paso 2 Seleccione **VTO** desde el **Tipo de servidor** la lista desplegable

Paso 3 Configure los parámetros (consulte la Tabla 4-3 para obtener más detalles).

Paso 4 Haga clic en **Salvar**.

La estación de puerta (VTO) se reiniciará automáticamente.

4.4.1.1 Configuración del número de videoportero (VTO) (1)

Cada estación de puerta (VTO) tiene un número único. Los números son normalmente los mismos que los números de los edificios.



- Puede cambiar el número de una estación de puerta (VTO) cuando no funciona como servidor SIP. Los números de la estación de puerta
- (VTO) pueden contener 5 números como máximo y no pueden ser iguales a ningún número de habitación.

Paso 1 Inicie sesión en la interfaz web.

Se muestra la página de inicio.

Paso 2 Seleccione **Configuración local**> **Básico**.

Figura 4-5 Propiedades del dispositivo

Paso 3 En el **VTO No.** cuadro de entrada, ingrese el número de estación de puerta (VTO) que planeó, y luego hacer clic **Confirmar** para guardar la configuración.

Tabla 4-1 Descripción de las propiedades del dispositivo

Parámetro	Descripción
Tipo de dispositivo	La estación de puerta se puede utilizar como estación de puerta de unidad y estación de cerca. Seleccione de acuerdo con los lugares donde se instalan las estaciones de puerta.
Número de llamada del centro	888888 de forma predeterminada. El valor predeterminado no se puede modificar.
VTO No.	El número de VTO solo se puede modificar cuando la estación de puerta que está operando no funciona como servidor SIP.
Llamada grupal	Una vez que haya habilitado la función de llamada de grupo, puede llamar al monitor interior principal (VTH) y sus extensiones al mismo tiempo.  Si el Llamada grupal La función está habilitada, la estación de puerta (VTO) se reiniciará automáticamente, y entonces esta función será válida.

4.4.1.2 Adición de monitores interiores (VTH)

Cuando la estación de puerta (VTO) que está operando funciona como servidor SIP, debe agregar todos los monitores interiores (VTH) a la estación de puerta (VTO); de lo contrario, las estaciones de puerta (VTO) no pueden comunicarse con los monitores interiores.



Cuando hay monitores interiores maestros (VTH) y extensiones, primero debe habilitar el **Llamada grupal** función en el **Básico** Interfaz, y luego agregue monitores interiores (VTH). Para habilitar el **Llamada grupal** función, consulte "4.4.1.1 Configuración del número de videoportero (VTO) (1)".

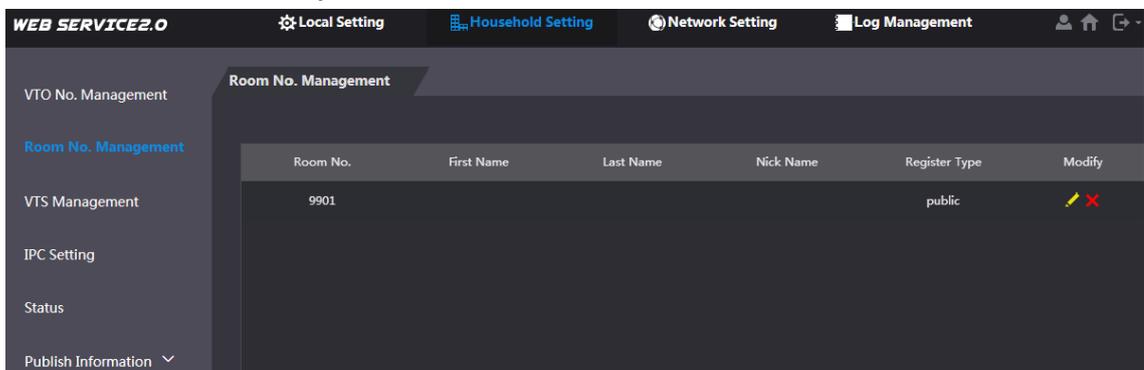
Agregar un monitor interior (VTH)



- Necesita agregar monitor interior (VTH) a la web del videoportero (VTO) solo cuando el videoportero (VTO) funciona como servidor SIP.
- Cuando haya monitor interior maestro (VTH) y extensiones, ambos se agregarán a la web del videoportero (VTO).

Paso 1 Seleccione **Configuración del hogar**> **Gestión de número de habitación**.

Figura 4-6 Gestión del número de habitación



Paso 2 Haga clic en **Añadir**.

Figura 4-7 Agregar

Paso 3 Configure los parámetros del monitor interior (VTH) consultando la Tabla 4-2.

Tabla 4-2 Descripciones de cómo agregar monitores de interior (VTH)

Parámetro	Descripción
Nombre de pila	Establezca el nombre de usuario y el apodo para cada monitor interior (VTH).
Apellido	
Nombre de Nick	
Habitación no.	<p>Configure el número de habitación en el monitor interior (VTH).</p>  <ul style="list-style-type: none"> El número corto del monitor de interior (VTH) consta de 1 a 5 números, que incluyen números y "#". Será el mismo que el número de habitación configurado en el monitor interior (VTH). Cuando hay monitores interiores maestros (VTH) y extensiones, para realizar la función de llamada de grupo, el número corto del monitor interior maestro (VTH) terminará con "# 0", y el número corto de la extensión VTH terminará con # 1, # 2 y # 3. Por ejemplo, si el número de VTH del monitor interior maestro es 101 # 0, los números de extensión serán 101 # 1, 101 # 2...
Registrarse	Mantenga el valor predeterminado para habilitar la señalización interactiva en el sistema SIP.
Contraseña	
Tipo de registro	

Paso 4 Haga clic en **Salvar** para completar la adición.

Repita estos pasos para agregar más monitores interiores.

Agregar monitores de interior (VTH) en lote

Paso 1 Seleccione **Configuración del hogar > Gestión de número de habitación**.

Figura 4-8 Agregar monitores interiores (VTH) en lote

Room No.	First Name	Last Name	Nick Name	Register Type	Modify
9901				public	

Unit Layer Amount: Room Amount in One Layer:
First Floor Number: Second Floor Number:

Add

Paso 2 Ingrese **Cantidad de capa de unidad, cantidad de habitación en una capa, número de primer piso, y**

Número del segundo piso.



- El rango de cantidad de capa unitaria es de 1 a 99, la cantidad de espacio en un rango de capa es de 1 a 99 y el rango de números del primer piso es de 1 a 9999.
- Los números de las habitaciones del segundo piso deben coincidir con los del primer piso. Por ejemplo, los números de habitación del primer piso son 100-199 y los números de habitación del segundo piso deben ser 200-299.

Paso 3 Haga clic en **Añadir** para completar la adición.

4.4.2 Plataforma (DSS Express / DSS Pro) como servidor SIP

Cuando una plataforma de gestión funciona como servidor SIP, debe registrar monitores interiores (VTH) y videoporteros (VTO) a través de la plataforma de gestión.

Paso 1 Seleccione **Configuración de red> Servidor SIP**.

Figura 4-9 servidor SIP

Paso 2 Seleccione **Express / DSS** desde el **Tipo de servidor** la lista desplegable.

Paso 3 Configure los parámetros de acuerdo con la Tabla 4-3.

Tabla 4-3 Descripción de los parámetros del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP del servidor SIP.
Puerto	<ul style="list-style-type: none"> Es 5060 por defecto cuando otras estaciones de puerta (VTO) en lugar del que está operando funcionan como servidor SIP. Es 5080 por defecto cuando la plataforma de gestión funciona como servidor SIP.
<u>Usuario Contraseña</u>	Utilice el valor predeterminado.
Dominio SIP	<ul style="list-style-type: none"> Será VDP cuando otras estaciones de puerta (VTO) en lugar de la que está operando funcionan como servidor SIP. Puede ser nulo o mantener el valor predeterminado cuando la plataforma funciona como servidor SIP.
Iniciar sesión Nombre de usuario / Contraseña	Nombre de usuario y contraseña para iniciar sesión en el servidor SIP.
IPAddr alternativo.	<p>Dirección IP del servidor alternativo (la estación de puerta (VTO) que está operando).</p>  <p>Si DSS Express o DSS Pro funciona como servidor SIP y el servidor alternativo está habilitado, cuando DSS Express o DSS Pro no pueden funcionar normalmente, el monitor de puerta (VTO) que está operando se utilizará como servidor SIP.</p>
Nombre de usuario alternativo	Nombre de usuario y contraseña para iniciar sesión en el servidor alternativo.
Contraseña alternativa	
IP de VTS alternativa Dirección	Dirección IP del VTS alternativo.
Servidor alternativo	Después de ingresar la dirección IP alternativa, el nombre de usuario, la contraseña y la dirección IP del VTS, debe seleccionar el Habilitar casilla de verificación para habilitar el servidor alternativo.

Paso 4 Haga clic en **Salvar**.

El VTO se reiniciará automáticamente.

4.4.2.1 Configuración del número de videoportero (VTO) (2)

Después de haber seleccionado el **Servidor alternativo** habilitar la casilla de verificación en la Figura 4-9, la estación de puerta (VTO) se reiniciará automáticamente.

Debe seleccionar el tipo de dispositivo, el número de edificio, el número de unidad y el número de VTO según sea necesario.

Paso 1 Inicie sesión en la interfaz web nuevamente.

Paso 2 Seleccione **Configuración local**> **Básico**.

Figura 4-10 Propiedades del dispositivo

The screenshot shows a 'Device Properties' configuration window. The fields are as follows:

- Device Type:** Unit Door Station (dropdown menu)
- Centre Call No.:** 888888
- Building No.:** 0 (with a checkbox to the right)
- Unit No.:** 0 (with a checkbox to the right)
- VTO No.:** 8001

Paso 3 Haga clic en **Confirmar**.

Tabla 4-4 Descripción de las propiedades del dispositivo

Parámetro	Descripción
Tipo de dispositivo	La estación de puerta se puede utilizar como estación de puerta de unidad y estación de cerca. Seleccione de acuerdo con los lugares donde se instalan las estaciones de puerta.
Número de llamada del centro	888888 de forma predeterminada. El valor predeterminado no se puede modificar.
Edificio número.	El rango del número de edificio es 0-99999. Hacer clic  junto al cuadro de entrada para habilitar la función de entrada del número de edificio y, a continuación, introduzca el número del edificio donde está instalado el portero automático.
Numero de unidad.	El rango de número de unidad es 0-9999. Hacer clic  detrás del cuadro de entrada para habilitar función de entrada del número de edificio y, a continuación, introduzca el número de unidad donde está instalado el portero.
VTO No.	El rango de números de VTO es 8001-8099. Ingrese el número de la estación de puerta (VTO) que está operando.  <ul style="list-style-type: none"> El número de VTO solo se puede modificar cuando la estación de puerta que está operando no funciona como servidor SIP. Si hay más de un videoportero (VTO) en una unidad, los números de los videoporteros (VTO) no pueden ser los mismos.

5 Configuración de ingeniería

5.1 Introducción de la configuración de ingeniería

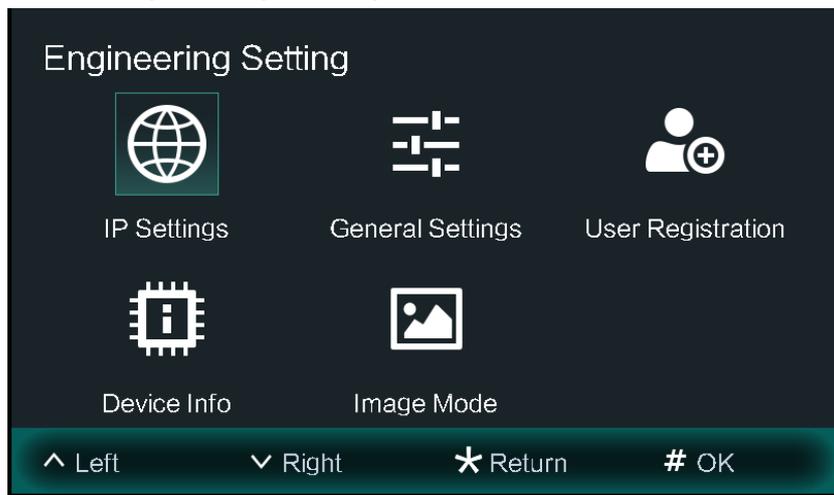


- La interfaz del proyecto es normalmente para administradores o ingenieros. Necesita establecer la contraseña del proyecto
- seleccionando **Configuración local**> **Control de acceso**> **Local** en la interfaz web.

Paso 1 Presione "*" contraseña del proyecto #" en el videoportero (VTO).

los **Configuración de ingeniería** se muestra la interfaz.

Figura 5-1 Configuración de ingeniería



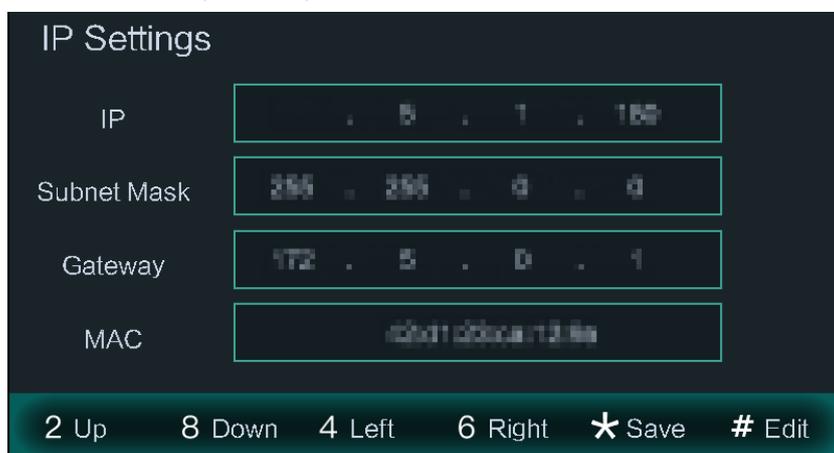
5.2 Configuración de la dirección IP

Debe planificar una dirección IP para la estación de puerta (VTO) para conectar la estación de puerta (VTO) a la red.

Paso 1 Seleccione **Configuración de IP** sobre el **Configuración de ingeniería** interfaz.

Paso 2 Introduzca la dirección IP, la máscara de subred y la puerta de enlace.

Figura 5-2 Configuración de IP



Paso 3 Presione * para completar la configuración.

6 Registro de usuario

Solo los usuarios cuya información, incluido el nombre de usuario, el número de personal, el número de habitación, la huella digital y el número de tarjeta, estén registrados pueden desbloquear las puertas.

Paso 1 Presione "*" contraseña del proyecto #" en el videoportero (VTO) para ir al **Configuración de ingeniería** interfaz.

Paso 2 Sobre el **Configuración de ingeniería** interfaz, seleccione **Registro de usuario**.

Paso 3 Seleccione **Añadir**.

Paso 4 Introduzca la ID de usuario y el número de

Paso 5 habitación. Pulse # para guardar la configuración.

Figura 6-1 Registro de usuario



Paso 6 Grabe imágenes de caras y emita tarjetas.

- Entrada de rostro: asegúrese de que su rostro esté en el medio del marco. Las imágenes de la cara del usuario se tomarán automáticamente. Si no está satisfecho, toque **Cancelar** para tomar una nueva imagen.
- (Solo para VTO 6541H) Huella digital: se pueden registrar como máximo tres huellas digitales de un usuario. Cada huella digital debe registrarse tres veces. Opere de acuerdo con el mensaje de voz. Tarjeta de emisión: puede emitir como máximo cinco tarjetas para cada usuario. Pase las tarjetas en la interfaz de emisión de tarjetas, los números de las tarjetas se reconocerán automáticamente.

- Emitir tarjetas a través de tarjetas autorizadas.



- Antes de emitir tarjetas, debe tener una tarjeta autorizada. Si no hay tarjetas autorizadas, debe emitir una tarjeta en la estación de puerta (VTO) mediante contraseña.

- En la interfaz web de la estación de puerta, seleccione **Configuración del hogar> Habitación No.**

Gestión>  y luego puede configurar una tarjeta como una tarjeta autorizada.

- Emitir tarjetas mediante contraseña.



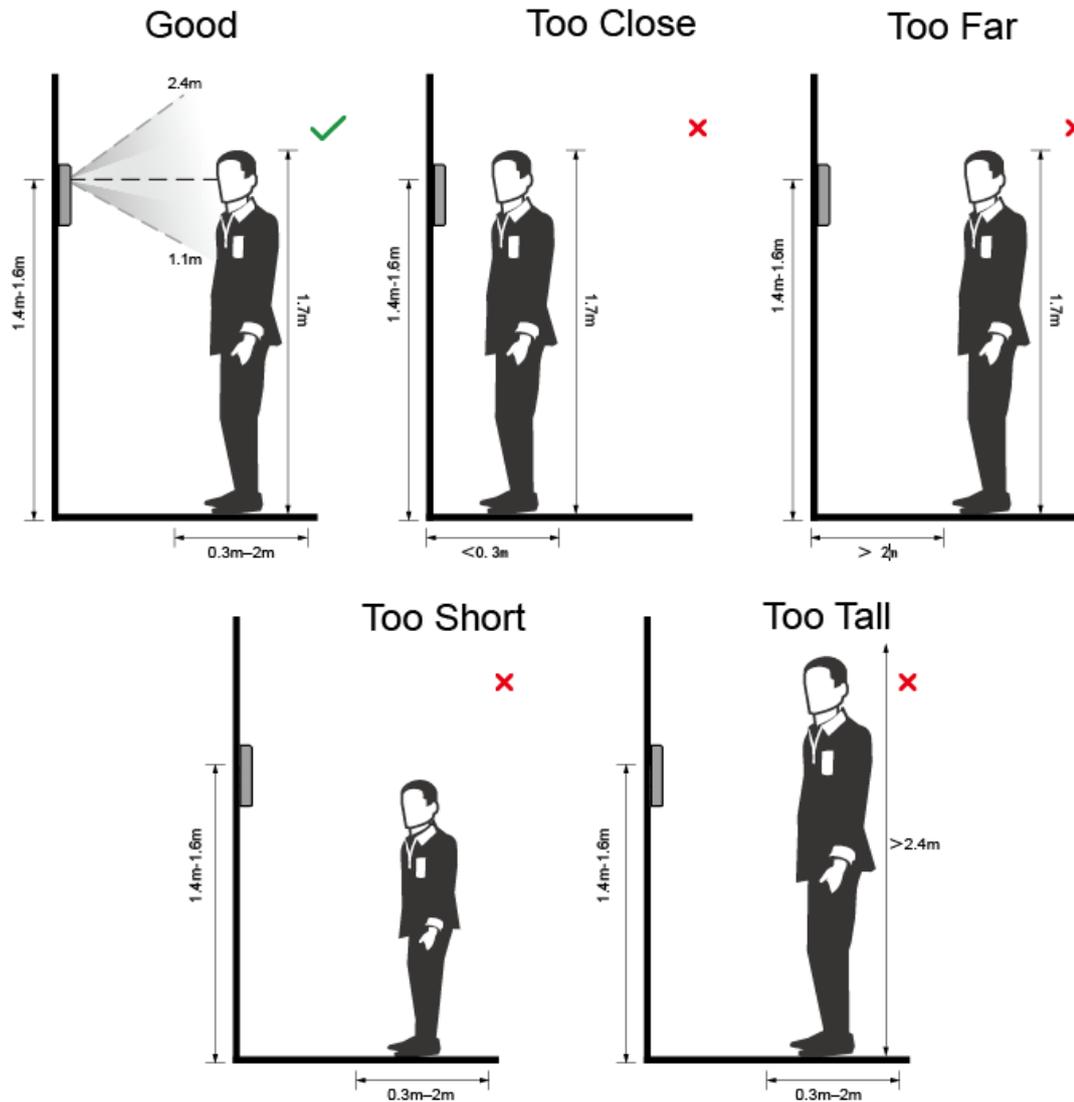
Tienes que entrar **Emitir contraseña de tarjeta** en la interfaz web de la estación de puerta (VTO) en **Configuración local> Control de acceso> Local.**

Apéndice 1 Notas sobre la grabación facial

Posición de la cara

Si su rostro no está en la posición adecuada, el efecto de reconocimiento facial podría verse afectado.

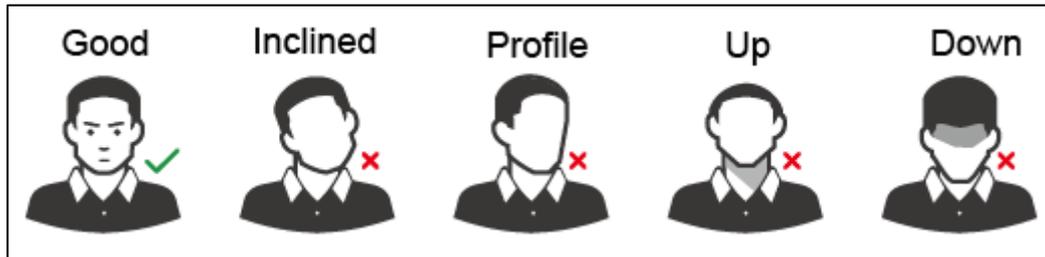
Apéndice Figura 1-1 Posición adecuada de la cara



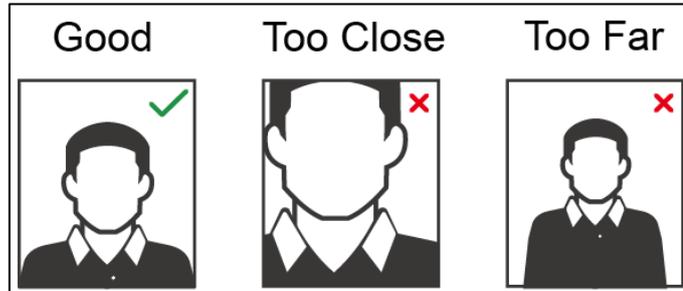
Requisitos de caras

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

Apéndice Figura 1-2 Posición de la cabeza



Apéndice Figura 1-3 Distancia entre caras



Al importar imágenes faciales a través de la plataforma de administración, asegúrese de que los píxeles de la imagen sean superiores a 500 × 500; el tamaño de la imagen es inferior a 100 KB; el formato de imagen es JPG; el color de fondo de la imagen es color puro (el blanco es el mejor); y el nombre de la imagen y la identificación de la persona son iguales.

Apéndice 2 Instrucción de registro de huellas dactilares

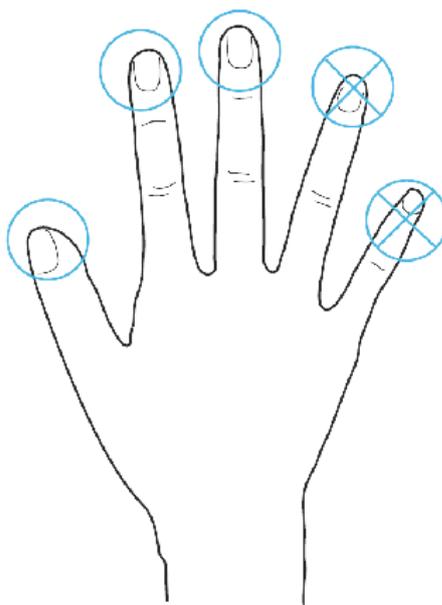
darse cuenta

- Asegúrese de que sus dedos estén limpios y secos antes de registrar sus huellas digitales.
- Presione con el dedo el área de grabación de huellas digitales y haga que su huella digital esté centrada en el área de grabación.
- No coloque el sensor de huellas dactilares en lugares con mucha luz, alta temperatura y mucha humedad.
- Para aquellos cuyas huellas dactilares están gastadas o no están claras, pruebe otros métodos de desbloqueo.

Dedos recomendados

Se recomiendan los dedos pulgar, índice y medio porque otros dedos no se pueden colocar fácilmente en el centro de grabación.

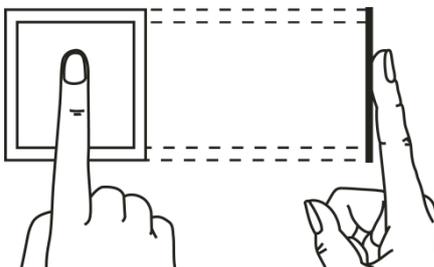
Apéndice Figura 2-1 Dedos recomendados



Método de presión con los dedos

- Método correcto

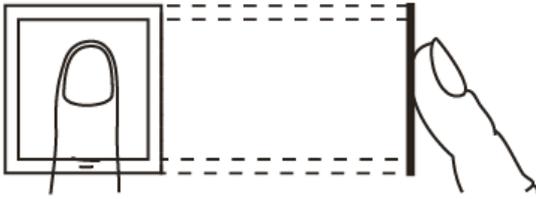
Apéndice Figura 2-2 Presión correcta con los dedos



- Método incorrecto

Apéndice Figura 2-3 Pulsación incorrecta del dedo

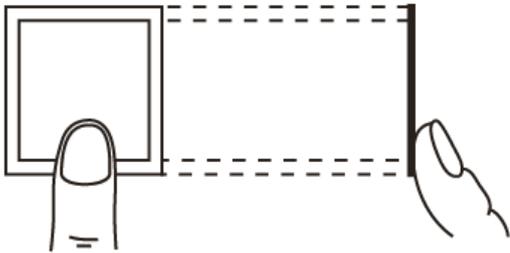
Fingertip perpendicular to the record area



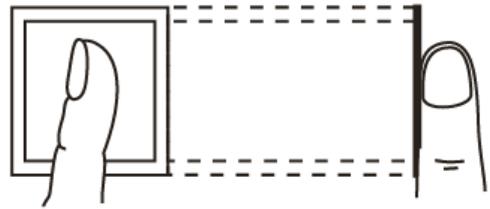
Fingertip not at the center of the record area



Fingertip not at the center of the record area



Fingertip inclination



Apéndice 3 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 muestran algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias que deben tomarse para la seguridad de la red de equipos básicos:

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 personajes; 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 cliente a tiempo

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

Recomendaciones "Es bueno tener" para mejorar la seguridad de la red de su equipo:

1. Protección física

Le sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala de computadoras especial y gabinete, e implemente permisos de control de acceso bien hechos y administración de claves para evitar que el personal no autorizado lleve a cabo contactos físicos como daños en el hardware, conexión no autorizada de equipos extraíbles (como un disco flash USB , puerto serie), etc.

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de ser adivinado o descifrado.

3. Establecer y actualizar contraseñas Restablecer información a tiempo

El equipo 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 sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan 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 con la contraseña incorrecta varias veces, 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 en cualquier conjunto de números

entre 1024 ~ 65535, lo que reduce el riesgo de que personas externas 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. Habilitar lista blanca

Le sugerimos que habilite la función de lista blanca para evitar que todos, excepto aquellos con direcciones IP específicas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo adjunto a la lista blanca.

8. Enlace de dirección MAC

Le recomendamos que vincule la dirección IP y MAC de la puerta de enlace al equipo, reduciendo así el riesgo de suplantación de ARP.

9. Asignar cuentas y privilegios de forma razonable

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

10. Deshabilite los servicios innecesarios y elija modos seguros

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

11. Transmisión encriptada de audio y video

Si su contenido de datos de audio y video es muy importante o sensible, 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 provocará cierta pérdida en la eficiencia de transmisión.

12. Auditoría segura

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

13. Registro de red

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

14. Construya un entorno de red seguro

Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, recomendamos:

- Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la 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, red GAP y otras tecnologías para particionar la red.

para 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.