Estación de puerta de villa (Versión 4.3)

Guía de inicio rápido

V1.0.0

Prefacio

General

Este manual presenta la estructura, el proceso de montaje y la configuración básica de la estación de puerta (en adelante, "VTO").

Las instrucciones de seguridad

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

Palabras de advertencia	Significado
 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 resultar en daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión
V1.0.0

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 ocasionada por las operaciones que no cumplan con el manual.

El manual se actualizaría de acuerdo con las últimas leyes y regulaciones de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si existe 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 reciente y la documentación complementaria.

Todavía puede haber desviaciones en los datos técnicos, las funciones y la descripción de las operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra 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 hay alguna duda o controversia, consulte nuestra explicación final.

Salvaguardias y advertencias importantes

La siguiente descripción es el método de aplicación correcto del dispositivo. Lea atentamente el manual antes de usarlo para evitar peligros y pérdidas materiales. Cumpla estrictamente con el manual durante la aplicación y consérvelo correctamente después de leerlo.

Requisito de funcionamiento

No coloque ni instale el dispositivo en un área expuesta a la luz solar directa o cerca de dispositivos generadores 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 los líquidos 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.

Transporte, use y almacene el dispositivo dentro del rango permitido de humedad y temperatura.

Requisitos de energía

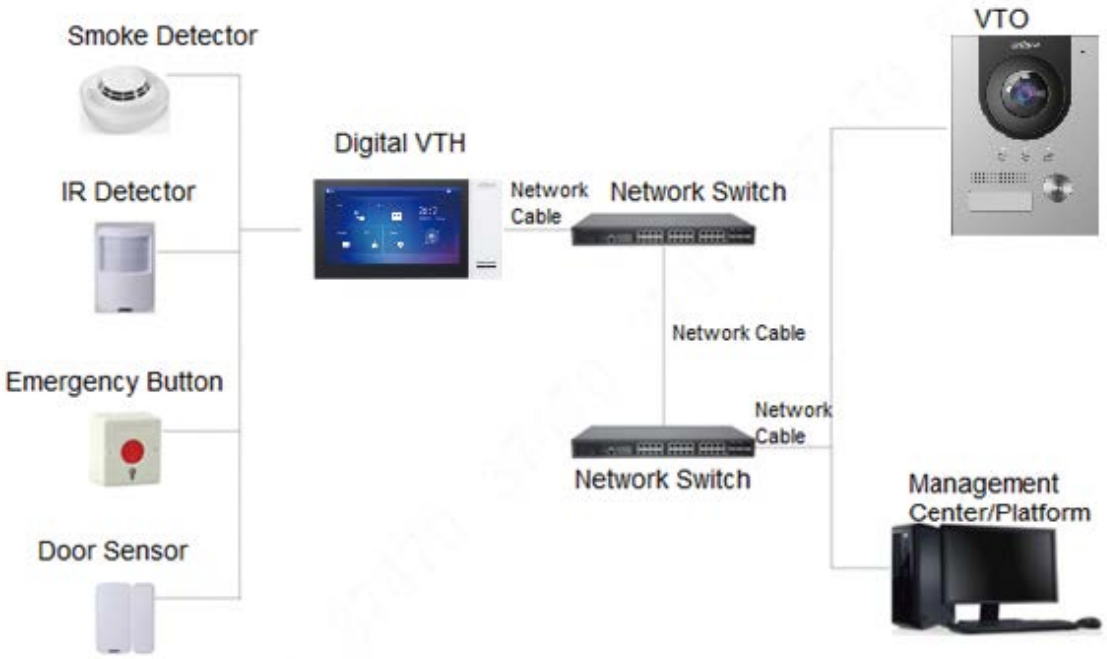
El producto utilizará cables eléctricos (cables de alimentación) requeridos por la región donde se utilizará el dispositivo.

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.

Tabla de contenido

1 Diagrama de red



2 Apariencia

2.1 VTO2101E-P

2.1.1 Panel frontal

Figure 2-1 VTO2101E-P

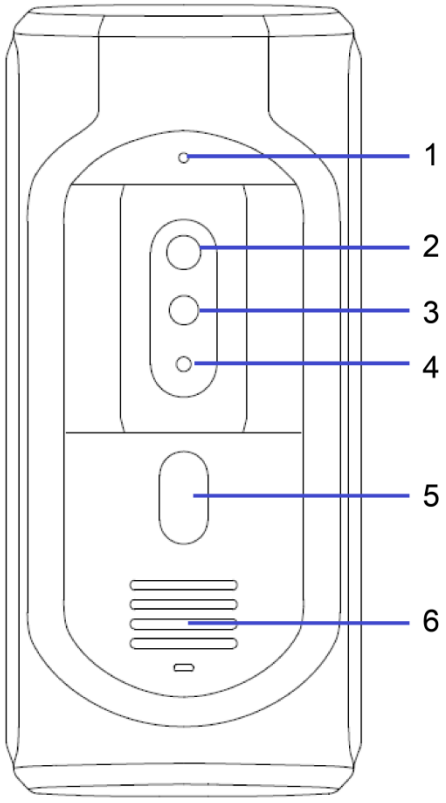


Tabla 2-1 Descripción del panel frontal

No.	Nombre	Descripción
1	MIC	Entradas de audio.
2	Cámara	Supervisa el área de la entrada.
3	Luz de iluminación infrarroja	Proporciona luz IR adicional para la cámara cuando está oscuro.
4	Sensor de luz	Detecta condiciones de iluminación ambiental.
5	Botón de llamada	Presione el botón para llamar a VTH o al centro de gestión.
6	Altavoz	Emite audio.

2.1.2 Panel trasero

Figure 2-2 VTO2101E-P

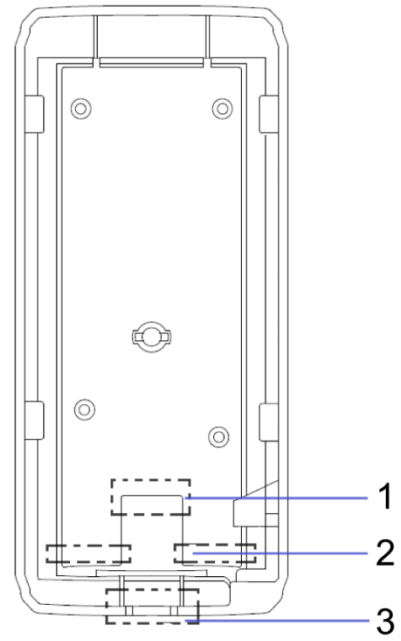


Tabla 2-2 Descripción del panel trasero

No.	Nombre	Descripción
1	Puerto de red	Conectado a la red con cables de red. Consulte la
2	Puertos RS-485	Figura 2-3 y la Tabla 2-3.
3	Bandeja de cables	Puede pasar cables a través de la bandeja de cables.

Figure 2-3 Conexión de cable

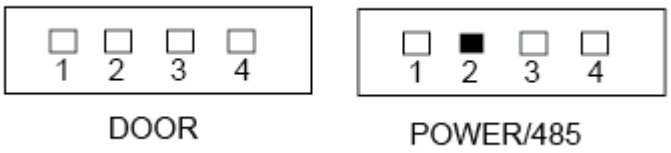


Tabla 2-3 Descripción del puerto

PUERTA		POTENCIA / 485	
No.	Nombre	No.	Nombre
1	NO	1	+ 12V
2	CAROLINA DEL NORTE	2	GND
3	COM	3	RS-485A
4	ALARMA EN	4	RS-485B

2.2 VTO3211D-P

2.2.1 Panel frontal

El número de botones del panel frontal varía según los modelos. VTO3211D-P2 tiene dos botones; VTO3211D-P4 tiene cuatro botones. Se tomará como ejemplo VTO3211D-P4.

Figure 2-4 VTO3211D-P

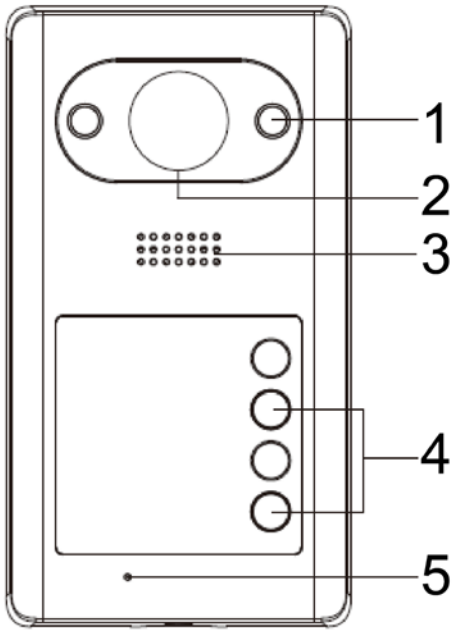


Tabla 2-4 Descripción del panel frontal

No.	Nombre	Descripción
1	Luz de iluminación IR	Proporciona luz IR adicional para la cámara cuando está oscuro.
2	Cámara	Supervisa el área de la entrada.
3	Altavoz	Emite audio.
4	Botón de llamada	Presione el botón para llamar a VTH o al centro de gestión. Entradas
5	MIC	de audio.

2.2.2 Panel trasero

Figure 2-5 VTO3211D-P

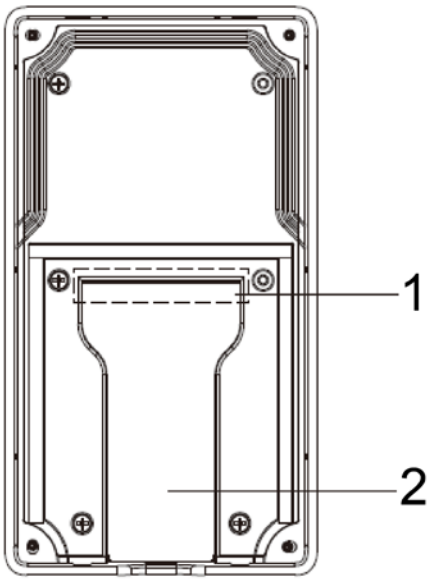


Tabla 2-5 Descripción del panel trasero

No.	Nombre	Descripción
1	Puertos de cable	Consulte la Figura 2-6 y la Tabla 2-6.
2	Bandeja de cables	Puede pasar el cable a través de la bandeja de cables.

Figure 2-6 Conexión de cable

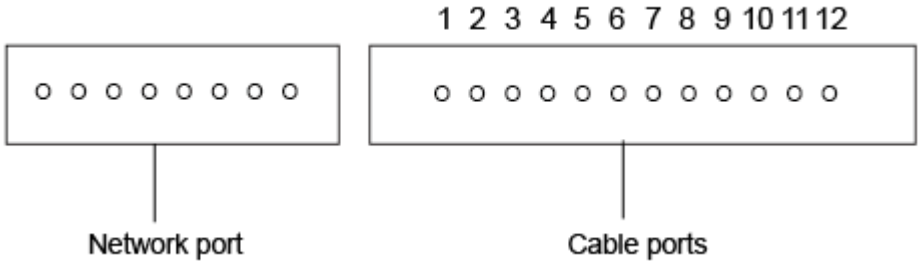


Tabla 2-6 Descripción del puerto de cable

No.	Nombre	No.	Nombre
1	ALM_COM	7	DOOR_FEED
2	ALM_NO	8	DOOR_NC
3	ALM_IN	9	DOOR_COM
4	RS485B	10	DOOR_NO
5	RS485A	11	GND
6	PUERTA ABIERTA	12	DC 12V

2.3 VTO2211G / VTO1201G

2.3.1 Panel frontal

Figure 2-7 Panel frontal de VTO2211G / VTO1201G

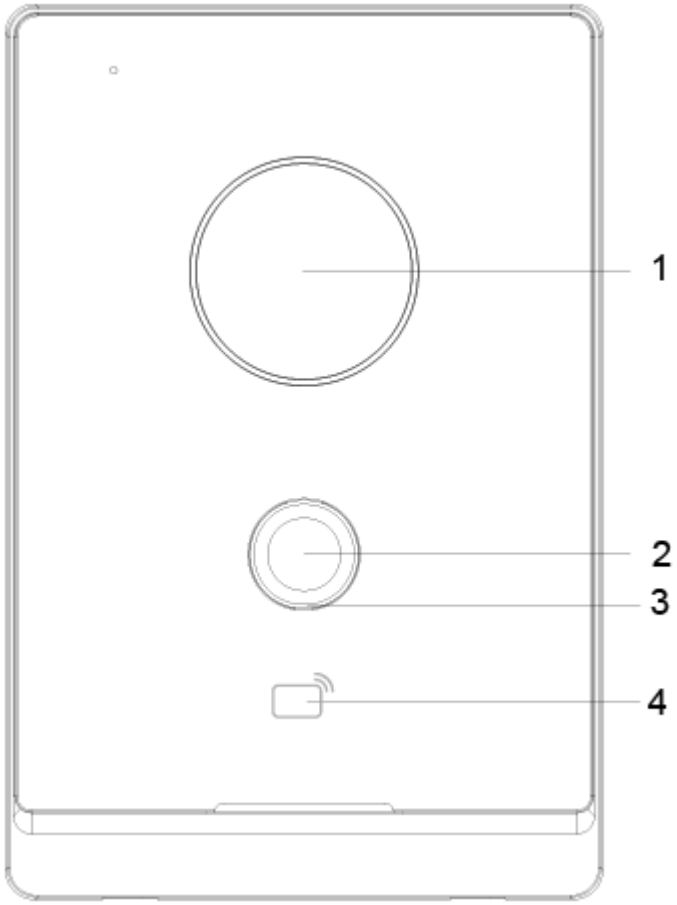


Tabla 2-7 Descripción del panel frontal

No.	Descripción
1	Cámara
2	Presione el botón para llamar a un monitor interior VTH o al centro de gestión.
3	Luz indicadora. ● Apagado: el dispositivo en modo de espera; ● Verde fijo: VTOhaciendo una llamada; Azul fijo: ● VTO durante una llamada; ● Verde amarillento: cuando desbloquea la puerta a través de VTH mientras VTO está haciendo una llamada. ● Rojo azulado: cuando desbloquea la puerta a través de VTH mientras está teniendo una llamada con el VTO; ● Luz verde de respiración: la red está desconectada.
4	Lector de tarjetas (solo para VTO2211G).

2.3.2 Panel trasero

Figure 2-8 Panel trasero de VTO2211G / VTO1201G

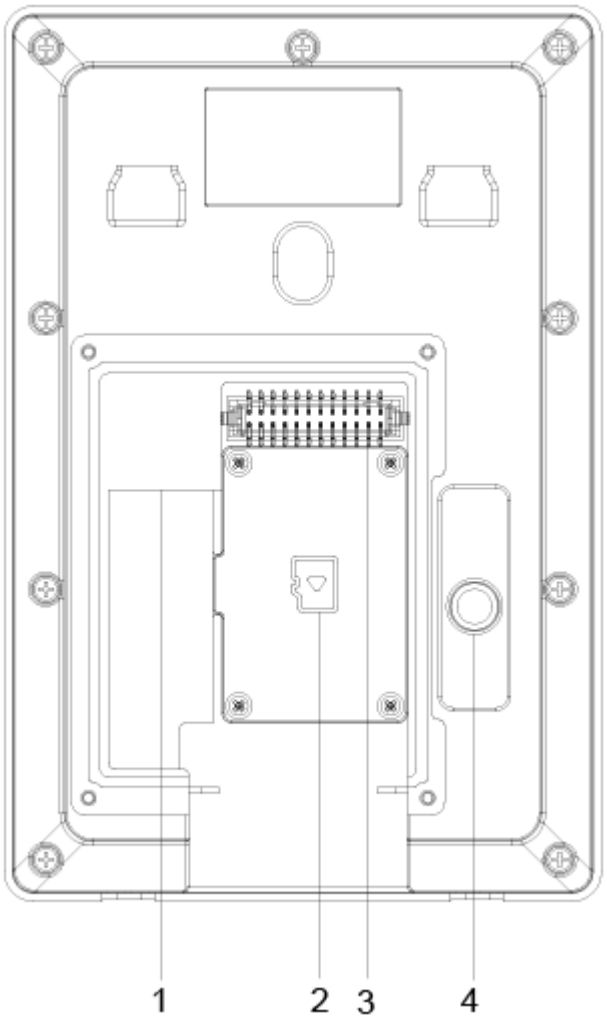


Tabla 2-8 Descripción del panel trasero

No.	Descripción	No.	Descripción
1	Puerto de red	3	Puertos
2	Tapa de la tarjeta SD	4	Botón de sabotaje

Figure 2-9 Conexión de cable VTO2211G

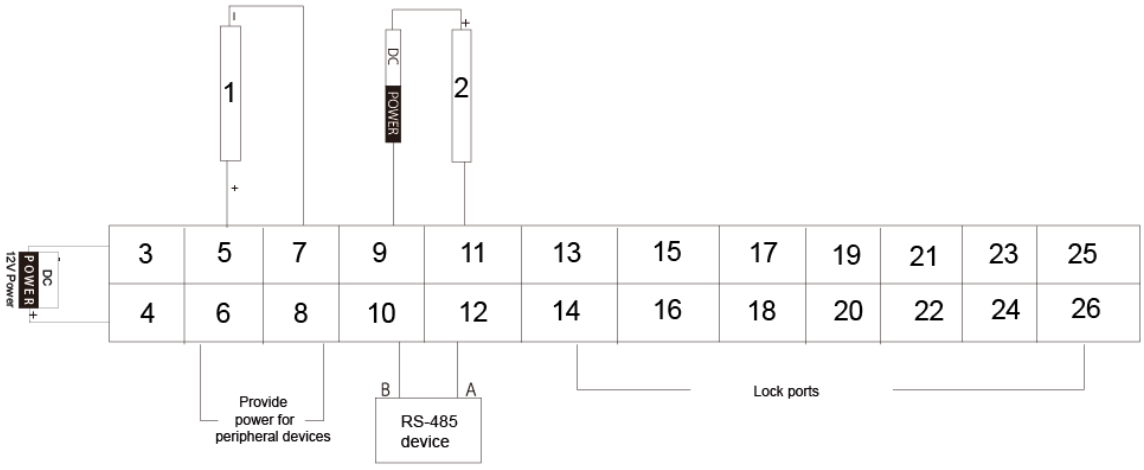


Tabla 2-9 Descripción del puerto

No.	Nombre	No.	Nombre
1	Dispositivo de entrada de alarma	14	DOOR1_NC
2	Dispositivo de salida de alarma	15	No disponible
3	DC EN-	dieciséis	DOOR1_COM
4	DC_IN +	17	No disponible
5	ALARM_IN	18	DOOR1_NO
6	+ 12V_OUT	19	No disponible
7	GND	20	GND
8	GND	21	No disponible
9	ALARM_NO	22	DOOR1_FB
10	RS485B	23	No disponible
11	ALARM_COM	24	GND
12	RS485A	25	No disponible
13	No disponible	26	DOOR1_PUSH

Figure 2-10 Conexión de cable VTO1201G

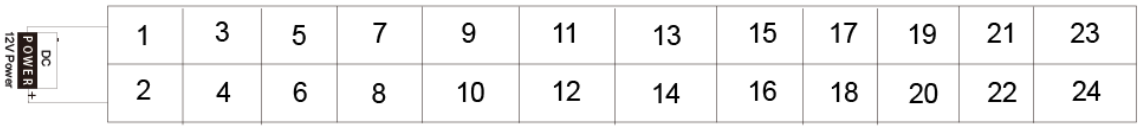


Tabla 2-10 Descripción del puerto

No.	Nombre
1	DC EN-
2	DC_IN +
3-24	Función reservada

Figure 2-11 Conexión de cables de bloqueo

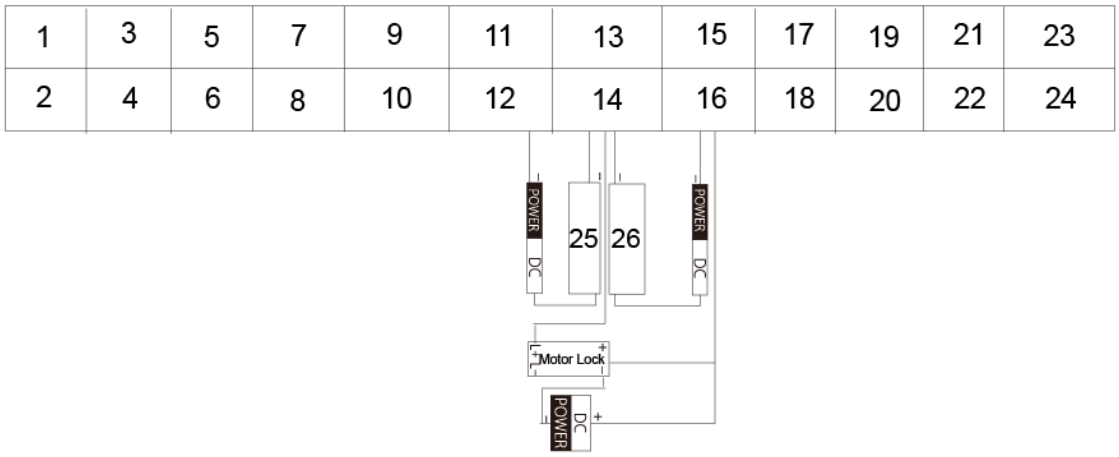


Tabla 2-11 Descripción del puerto

No.	Nombre	No.	Nombre
1	DC EN-	14	DOOR1_COM
2	DC_IN +	15	No disponible
3	ALARM_IN	dieciséis	DOOR1_NO
4	+ 12V_OUT	17	No disponible
5	GND	18	GND

No.	Nombre	No.	Nombre
6	GND	19	No disponible
7	ALARM_NO	20	DOOR1_FB
8	RS485B	21	No disponible
9	ALARM_COM	22	GND
10	RS485A	23	No disponible
11	No disponible	24	DOOR1_PUSH
12	DOOR1_NC	25	Cerradura magnética
13	No disponible	26	Cerradura electrica

3 Instalación

3.1 darse cuenta

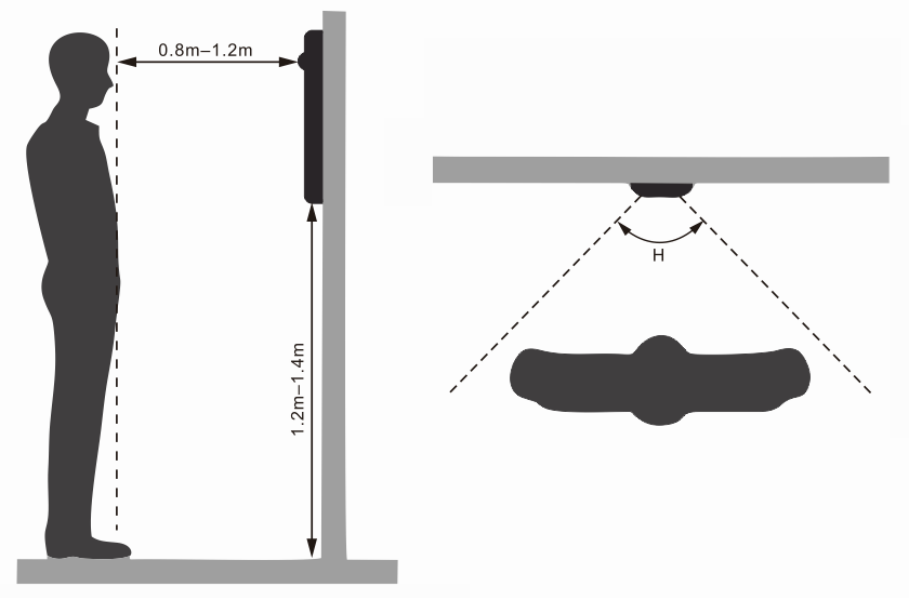
No instale el VTO en lugares con condensación, alta temperatura, grasa o polvo, corrosión química, luz solar directa o refugio cero.

La instalación y el ajuste deben ser realizados por profesionales y no desmonte el VTO.

3.2 Guia

Vea la Figura 3-1 la posición de instalación. El ángulo de visión horizontal del VTO varía con los diferentes modelos, mire hacia el centro del VTO tanto como sea posible.

Figure 3-1 Referencia de posición de instalación



4 Configuración

Este capítulo presenta cómo inicializar, conectar y realizar configuraciones primarias para VTO y VTH para realizar funciones básicas, incluida la administración de dispositivos, llamadas y monitoreo. Para obtener más información, consulte el manual del usuario.

4.1 Proceso de configuración

Antes de la configuración, verifique cada dispositivo y asegúrese de que no haya cortocircuito o circuito abierto.

Step 1 Planifique la dirección IP para cada dispositivo y también planifique el número de apartamento y el número de habitación que necesita.

Step 2 Configure los VTO. Consulte "4.3 Configuración de VTO".

1) Inicializar VTO. Consulte "4.3.1 Inicialización".

2) Configure los números de VTO. Consulte "4.3.2 Configuración de números VTO".

3) Configure los parámetros de la red VTO. Consulte "4.3.3 Configuración de parámetros de red".

4) Configure el servidor SIP. Consulte "4.3.4 Configuración del servidor SIP".

5) Configure el número de habitación de destino y la llamada de grupo. Consulte "4.3.5 Configuración de número de llamada y llamada de grupo".

6) Agregue VTO al servidor SIP. Consulte "4.3.6 Agregar VTO".

7) Agregue el número de habitación al servidor SIP. Consulte "4.3.7 Agregar RoomNumbers".

Step 3 Configure los VTH. Consulte el manual del usuario de VTH.

Step 4 Verifique la configuración. Consulte "4.4 Verificación de la configuración".

4.2 VDPConfig

Puede descargar "VDPConfig" y realizar la inicialización del dispositivo, la modificación de la dirección IP y la actualización del sistema para varios dispositivos al mismo tiempo. Para más detalles, consulte el manual de usuario correspondiente.

4.3 Configuración de VTO

Conecte el VTO a su PC con un cable de red y, para iniciar sesión por primera vez, debe crear una nueva contraseña para la interfaz web.

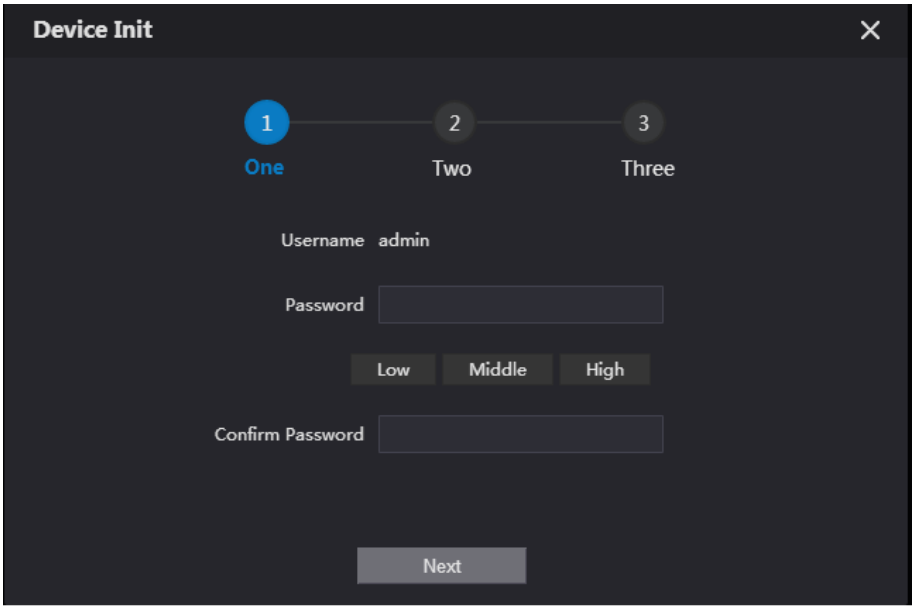
4.3.1 Inicialización

La dirección IP predeterminada de VTO es 192.168.1.110 y asegúrese de que la PC esté en el mismo segmento de red que el VTO.

Step 1 Conecte el VTO a la fuente de alimentación y luego enciéndalo.

Step 2 Abra el navegador de Internet en la PC, luego ingrese la dirección IP predeterminada del VTO en la barra de direcciones y luego presione Enter.

Figure 4-1 Inicialización del dispositivo



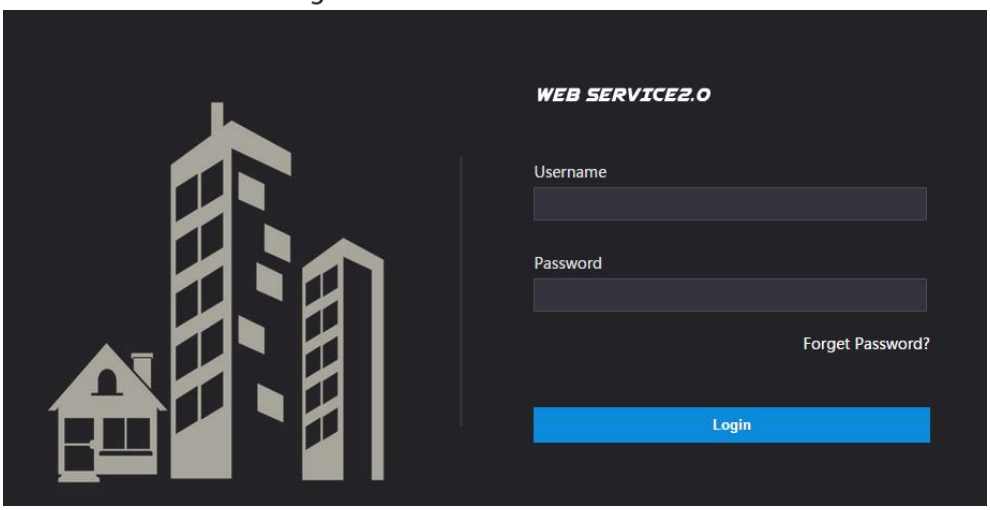
Step 3 Ingrese y confirme la contraseña, y luego haga clic en **Próximo.**

Step 4 Se muestra la interfaz de configuración de correo electrónico. Selecciona el**Correo electrónico** casilla de verificación y luego ingrese su dirección de correo electrónico. Esta dirección de correo electrónico se puede utilizar para restablecer la contraseña y se recomienda finalizar esta configuración.

Step 5 Hacer clic **Próximo.** La inicialización tuvo éxito. Hacer clic

Step 6 **está bien.**

Figure 4-2 Interfaz de inicio de sesión



4.3.2 Configuración de VTONumber

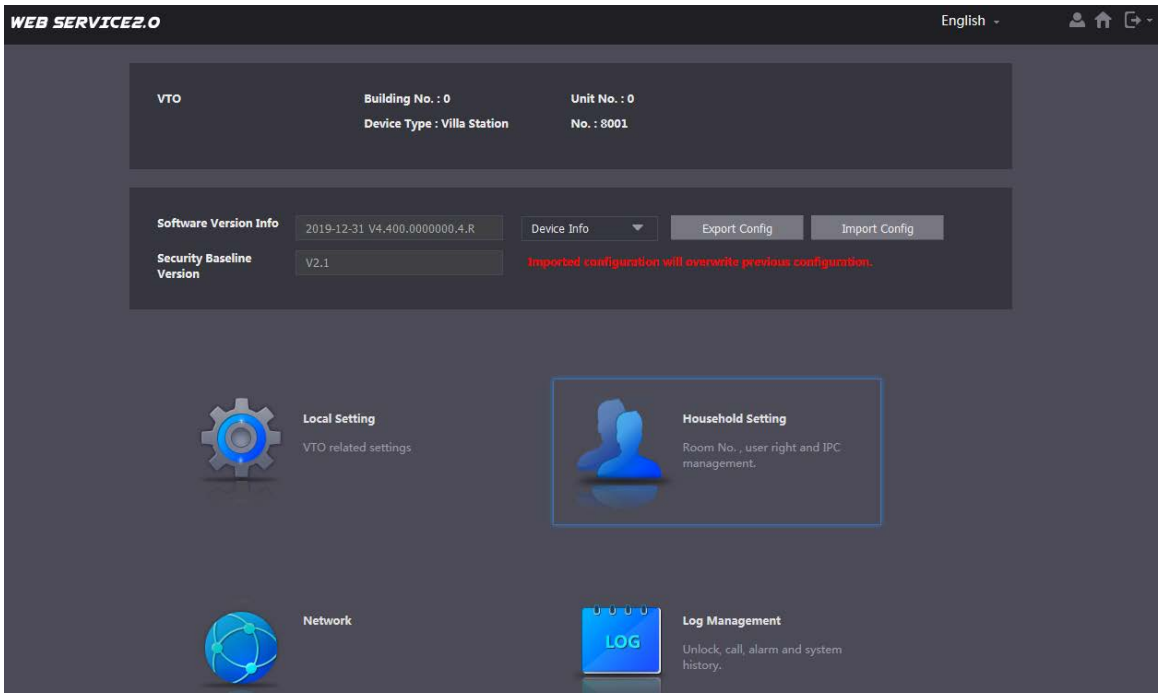
El número de VTO se puede utilizar para diferenciar cada VTO, y normalmente se configura según el número de apartamento o edificio.

Puede cambiar el número de un VTO cuando no está funcionando como servidor SIP.

El número VTO puede contener 5 números como máximo y no puede ser igual a ningún número de habitación.

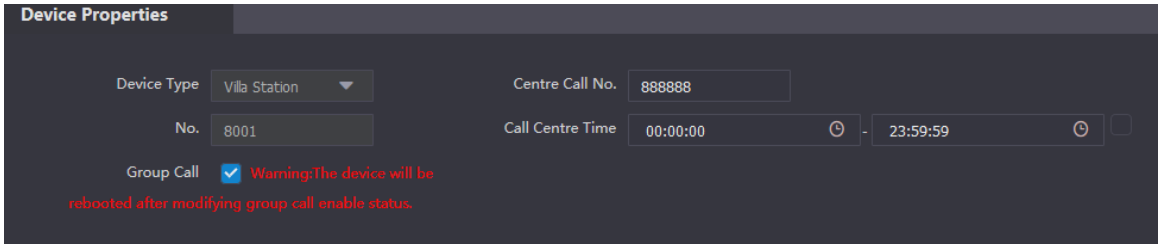
Step 1 Inicie sesión en la interfaz web del VTO y luego se muestra la interfaz principal.

Figure 4-3 Interfaz principal



Step 2 Seleccione Configuración local> Básico.

Figure 4-4 Propiedades del dispositivo

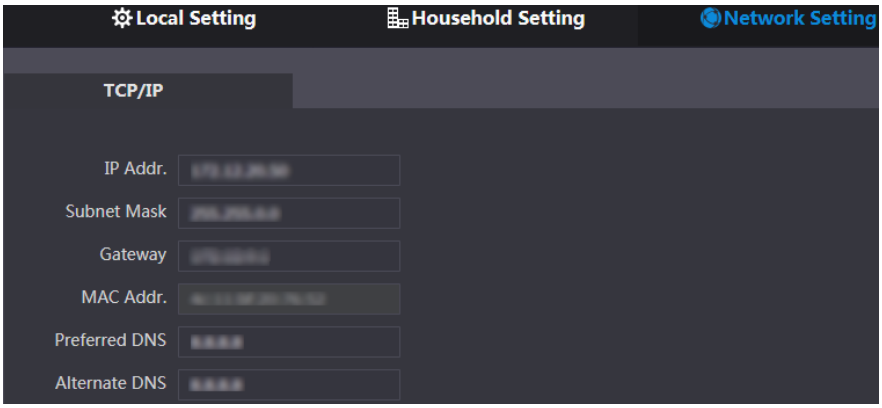


Step 3 En el **No.** cuadro de entrada, ingrese el número de VTO que planeó para el VTO que está operando, y luego haga clic en **Confirmar** ahorrar.

4.3.3 Configuración de parámetros de red

Step 1 Seleccione Configuración de red> Básico.

Figure 4-5 Información de TCP / IP



Step 2 Ingrese los parámetros de red que planeó y luego haga clic en **Ahorrar.**

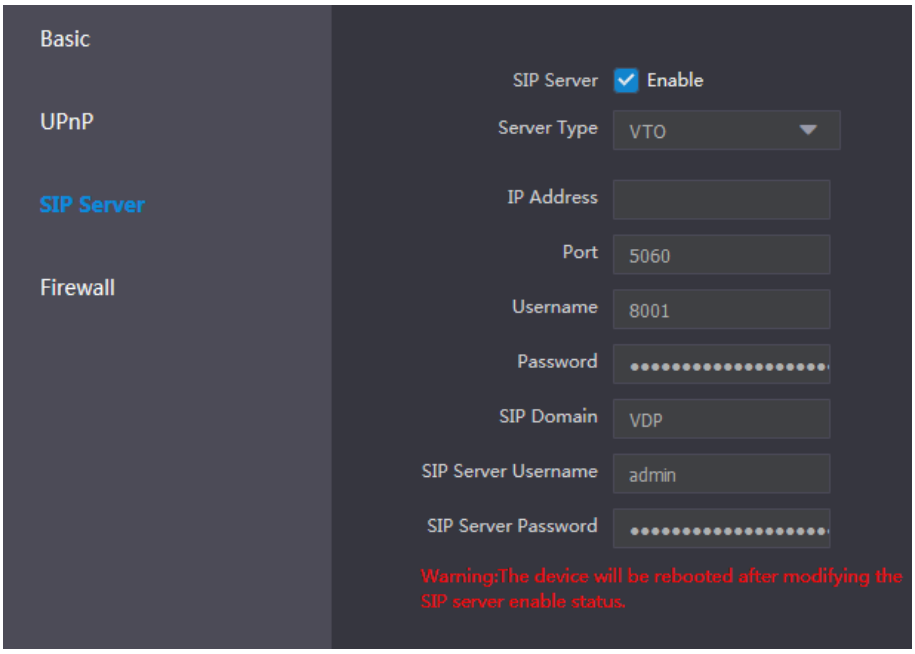
El VTO se reiniciará y deberá modificar la dirección IP de su PC al mismo segmento de red que el VTO para iniciar sesión nuevamente.

4.3.4 Configuración del servidor SIP

Se requiere el servidor SIP en la red para transmitir el protocolo de intercomunicación, y luego todos los VTO y VTH conectados al mismo servidor SIP pueden realizar videollamadas entre sí. Puede utilizar VTO u otros servidores como servidor SIP.

Step 1 Seleccione Configuración de red> Servidor SIP.

Figure 4-6 Servidor SIP



Step 2 Seleccione el tipo de servidor que necesita.

Si el VTO que está visitando funciona como servidor SIP Seleccione el **Permitir** casilla de verificación en **Servidor SIP,** y luego haga clic en **Ahorrar.**

El VTO se reiniciará y, después de reiniciar, podrá agregar VTO y dispositivos VTH al VTO que está operando. Consulte "4.3.6 QAdding VTO y 4.3.7 Add RoomNumber".

Si el VTO que está visitando no funciona como servidor SIP, no seleccione el **Permitir** casilla de verificación en **Servidor SIP,** de lo contrario, la conexión fallará. Si otro VTO funciona como servidor SIP

Seleccione **VTO** en el **Tipo de servidor** lista y, a continuación, configure los parámetros. Consulte la Tabla 4-1.

Tabla 4-1 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	La dirección IP del VTO que funciona como servidor SIP.
Puerto	5060
Nombre de usuario	Conserva el valor predeterminado.
Contraseña	
Dominio SIP	VDP
Nombre de usuario del servidor SIP	El nombre de usuario y la contraseña de la interfaz web del servidor SIP.
Contraseña del servidor SIP	

Si otros servidores funcionan como servidor SIP Seleccione **Express / DSS** en el **Tipo de servidor** lista, y luego consulte el manual correspondiente para la configuración detallada.

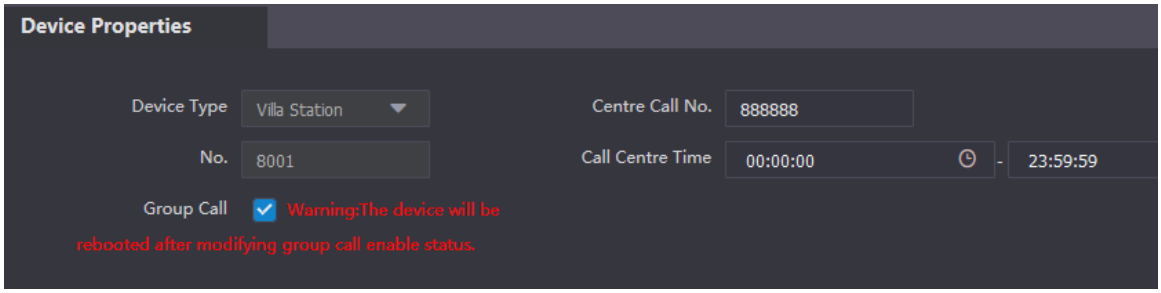
4.3.5 Configurar el número de llamada y la llamada de grupo

Debe configurar el número de llamada en cada VTO, y luego todos los VTO pueden llamar a la habitación definida cuando presiona el botón de llamada. En el servidor SIP, puede habilitar la función de llamada grupal y, al llamar a un VTH maestro, los VTH de extensión también recibirán la llamada.

Después de habilitar o deshabilitar la función de llamada de grupo, la estación de puerta se reiniciará.

Step 1 Seleccione Configuración local> Básico.

Figure 4-7 Propiedades del dispositivo



Step 2 En el **No.** cuadro de entrada, ingrese el número de habitación al que necesita llamar y luego haga clic en **Confirmar** ahorrar. Repita esta operación en cada interfaz de villa VTOweb.

Step 3 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración local> Básico.**

Step 4 Selecciona el **Llamada grupal** casilla de verificación y luego haga clic en **Confirmar.**

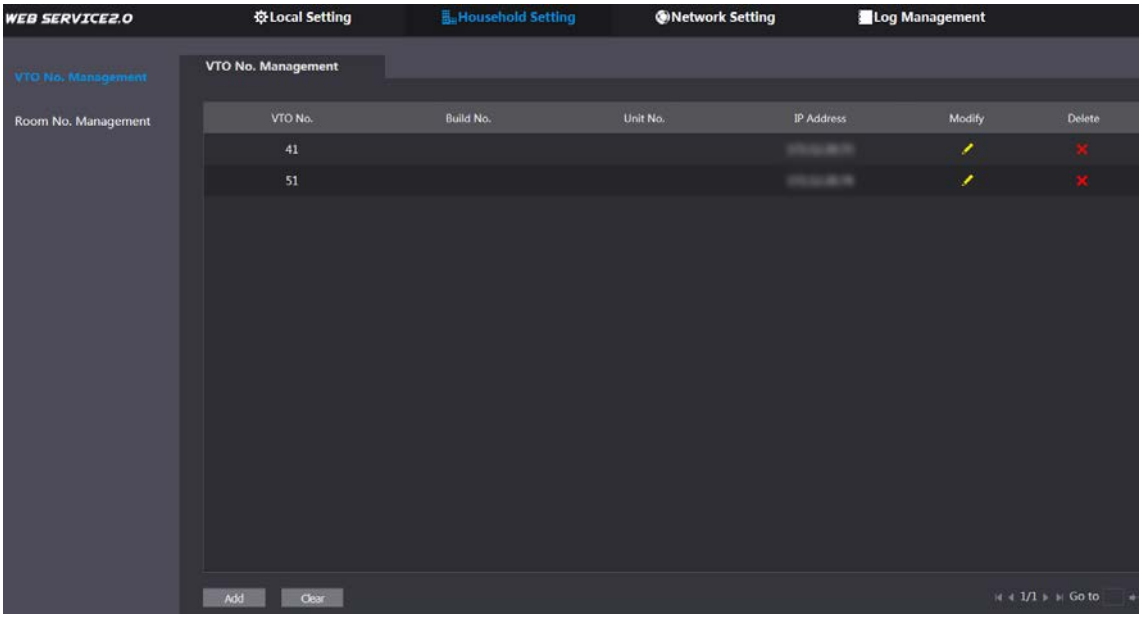
El VTO se reiniciará y, al llamar a un VTH maestro, la extensión VTH también recibirá la llamada.

4.3.6 Agregar VTO

Puede agregar VTO al servidor SIP y todos los VTO conectados al mismo servidor SIP pueden realizar videollamadas entre sí. Esta sección se aplica a la condición en la que un VTO funciona como servidor SIP, y si está utilizando otros servidores como servidor SIP, consulte el manual correspondiente para obtener la configuración detallada.

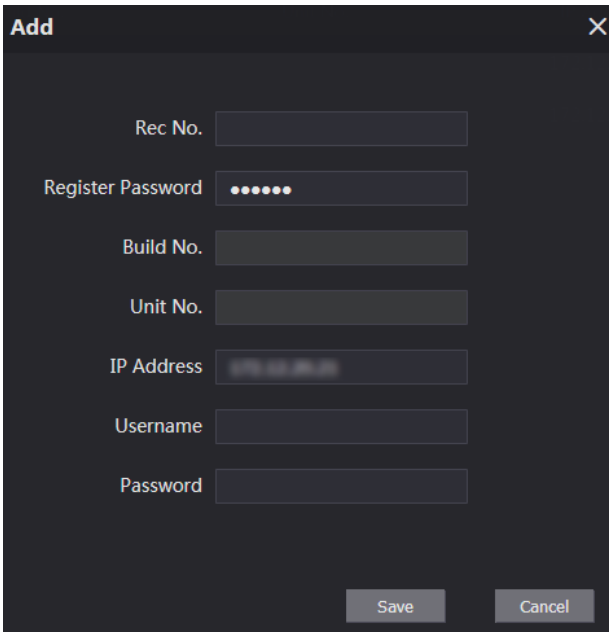
Step 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Entorno del hogar> Gestión del número de VTO.**

Figure 4-8 Gestión del número de VTO



Step 2 Hacer clic **Agregar.**

Figure 4-9 Agregar VTO



Step 3 Configure los parámetros y asegúrese de agregar también el servidor SIP.

Tabla 4-2 Agregar VTO

Parámetro	Descripción
Rec No.	El número de VTO que configuró para el VTO de destino. Consulte los detalles en "4.3.2 Configuración del número VTO".
Registrar contraseña	Mantener el valor predeterminado.
Construir No.	Disponible solo cuando otros servidores funcionan como servidor SIP.
Numero de unidad.	
Dirección IP	La dirección IP del VTO de destino.
Nombre de usuario	El nombre de usuario y la contraseña para la interfaz web del VTO de destino.
Contraseña	

Step 4 Hacer clic **Ahorrar.**

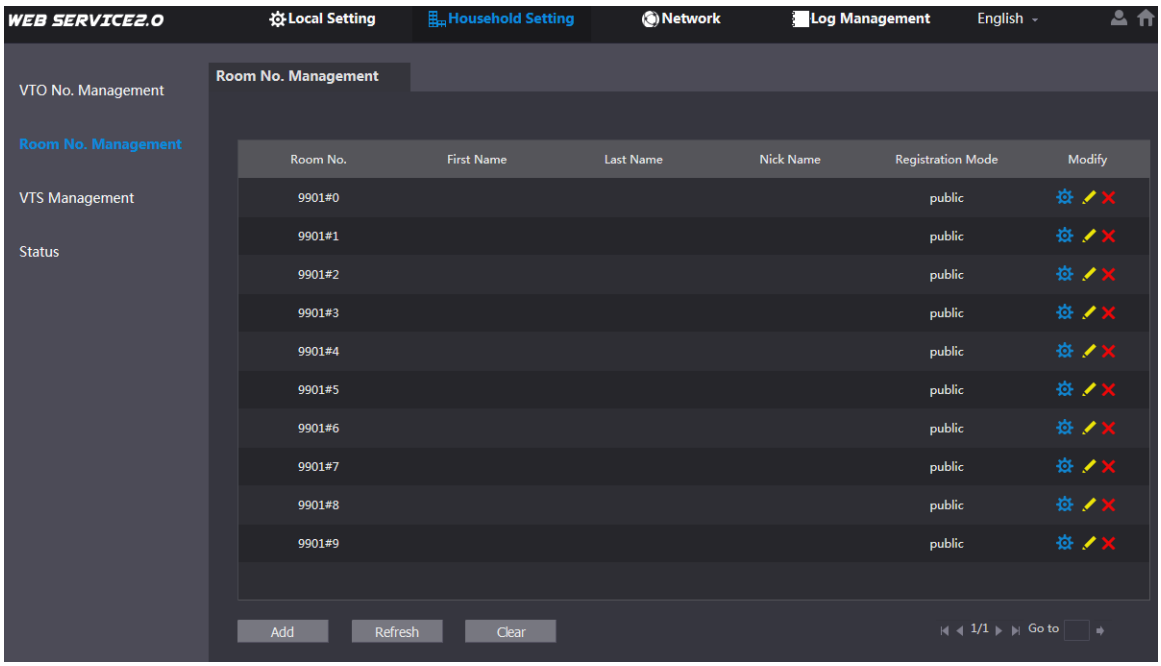
4.3.7 Agregar RoomNumber

Puede agregar el número de habitación planificado al servidor SIP y luego configurar el número de habitación en los VTH para conectarlos a la red. Esta sección se aplica a la condición en la que un VTO funciona como servidor SIP, y si usa otros servidores como servidor SIP, consulte el manual correspondiente para la configuración detallada.

El número de habitación puede contener 6 dígitos de números o letras o su combinación como máximo, y el número de habitación debe ser único.

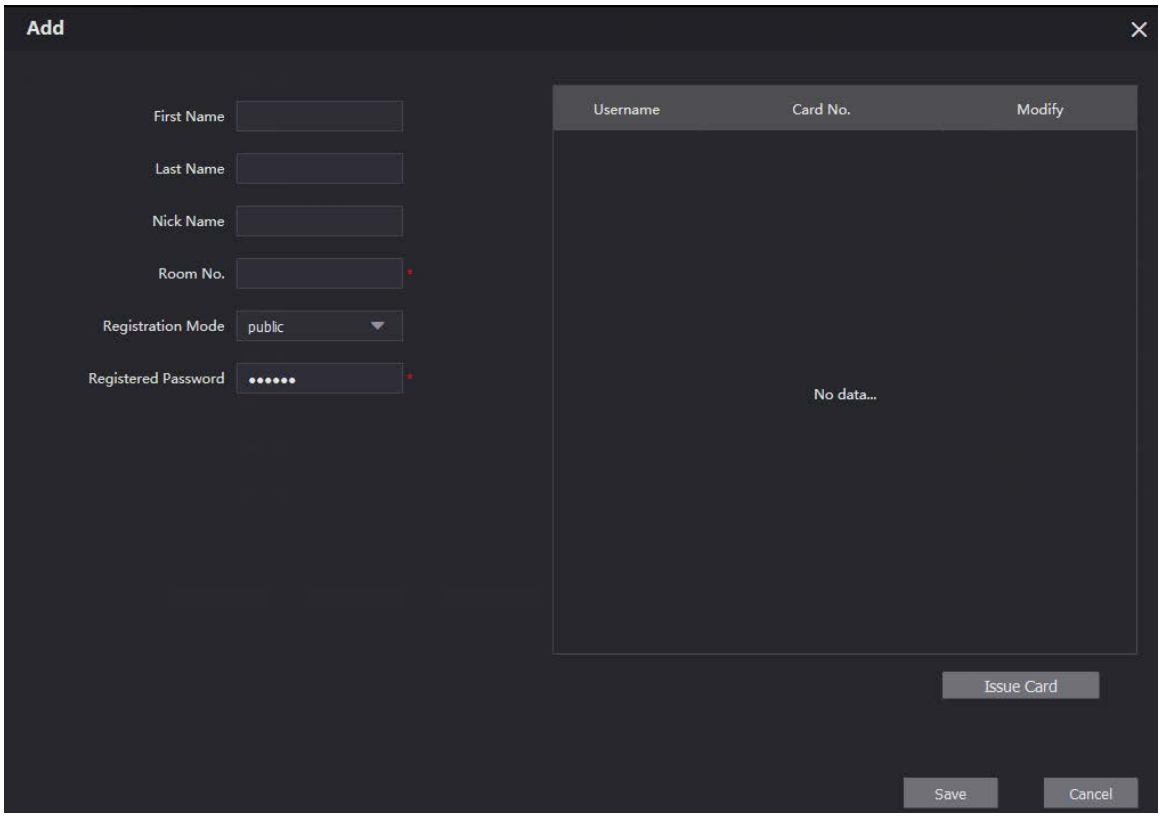
Step 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración del hogar> Gestión de número de habitación.**

Figure 4-10 Habitación no. Gestión



Step 2 Hacer clic **Agregar.**

Figure 4-11 Agregar número de habitación individual



Step 3 Configure la información de la habitación.

Tabla 4-3 Información de la habitación

Parámetro	Descripción
Primer nombre	Ingrese la información que necesita para diferenciar cada habitación.
Apellido	
Apodo	
Habitación no.	El número de habitación que planeaste.

Parámetro	Descripción
Primer nombre	Ingrese la información que necesita para diferenciar cada habitación.
Apellido	
Apodo	
	Si utiliza varios VTH, el número de habitación del VTH maestro debe ser "número de habitación # 0" y el número de habitación de la extensión VTH debe ser "roomnumber # 1", "roomnumber # 2", etc. Puede tener 9 VTH de extensión como máximo para un VTH maestro. Seleccione**público,** y
Modo de registro	**local** está reservado para uso futuro.
Contraseña registrada	Conserva el valor predeterminado.

Step 4 Hacer clic **Ahorrar.**

Se muestra el número de habitación agregado. Haga clic para para modificar la información de la habitación y haga clic en para eliminar una habitación.

4.4 Verificación de la configuración

4.4.1 Llamar a VTH desde VTO

Presione el botón de llamada en el VTO para iniciar una llamada con el VTH.

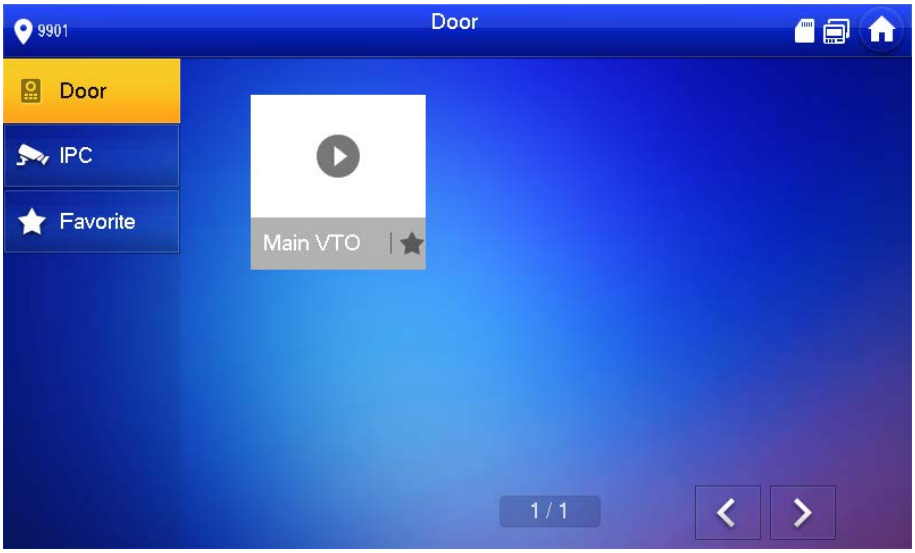
Figure 4-12 Pantalla de llamada

Grifo en el VTH para contestar la llamada.

4.4.2 Ver videos de monitoreo en el VTH

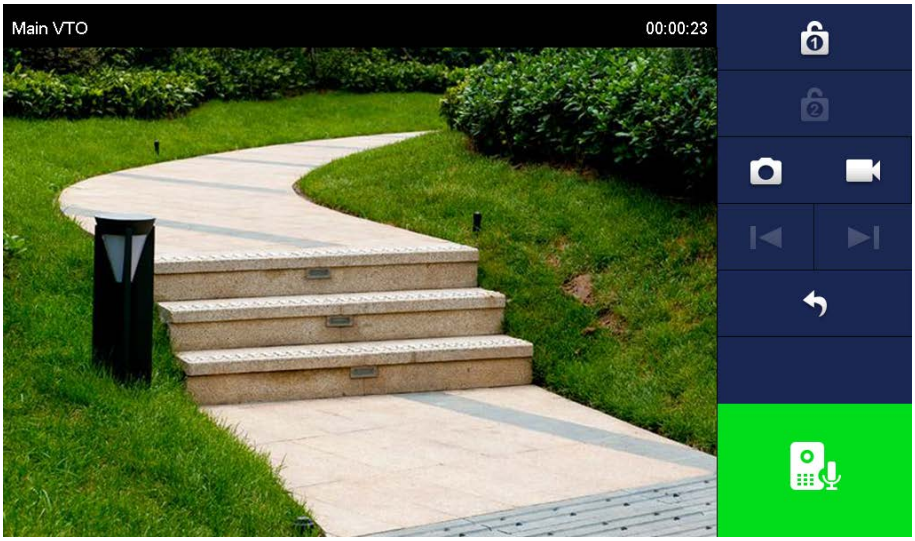
Step 1 En la interfaz principal del VTH, seleccione **Monitor> Puerta.**

Figure 4-13 Puerta



Step 2 Seleccione un VTO para ver videos de monitoreo.

Figure 4-14 Ver videos de monitoreo



5 Instalación de aplicaciones y adición de dispositivos

Escanee el siguiente código QR para descargar e instalar la aplicación.

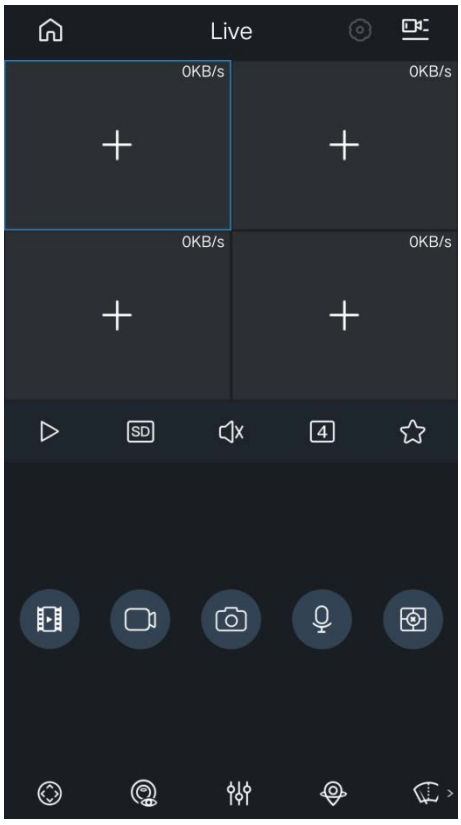
Antes de agregar el VTO al gDMSS Plus, debe modificar la dirección IP del VTO, asegúrese de que el VTO y el enrutador están conectados como a la misma red y conecte el VTO a la fuente.

Step 1 En su teléfono móvil, toque y luego siga las instrucciones en pantalla hasta que la región Se muestra la interfaz de selección.

Step 2 Seleccione una región.

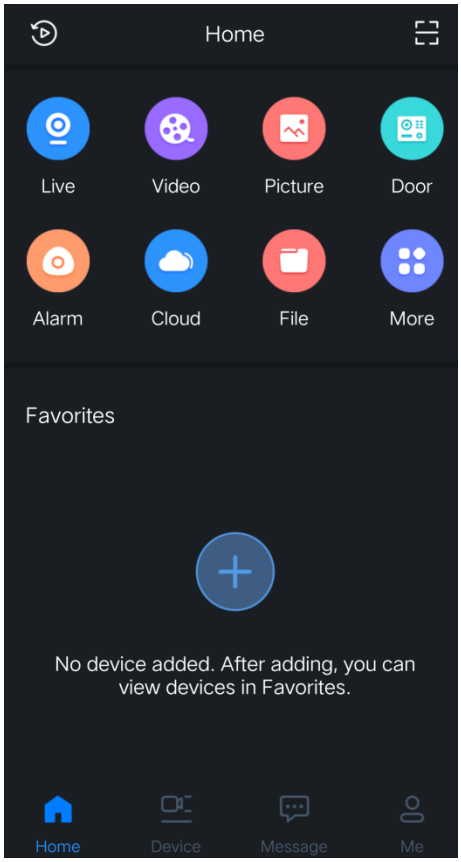
Step 3 Grifo **Hecho** en la esquina superior derecha de la interfaz.

Figure 5-1 Vivir



Step 4 Grifo en la esquina superior izquierda de la **Vivir** interfaz.

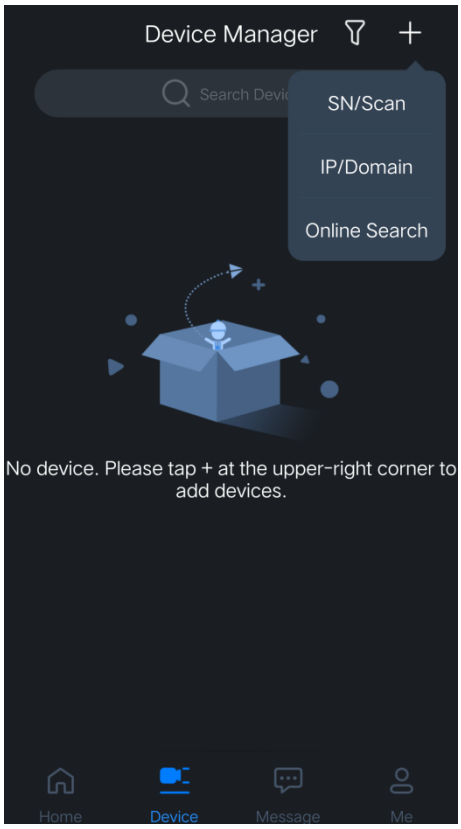
Figure 5-2 Casa



Step 5 Grifo  sobre el **Casa** interfaz.

Step 6 Grifo  en la esquina superior derecha de la **Administrador de dispositivos** interfaz.

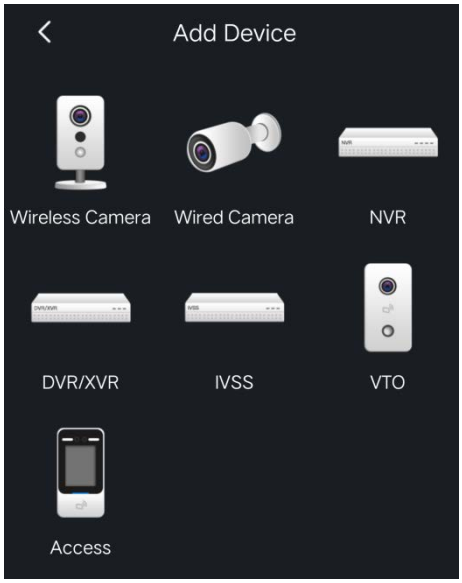
Figure 5-3 Administrador de dispositivos



5.1 Agregar a través de una red cableada

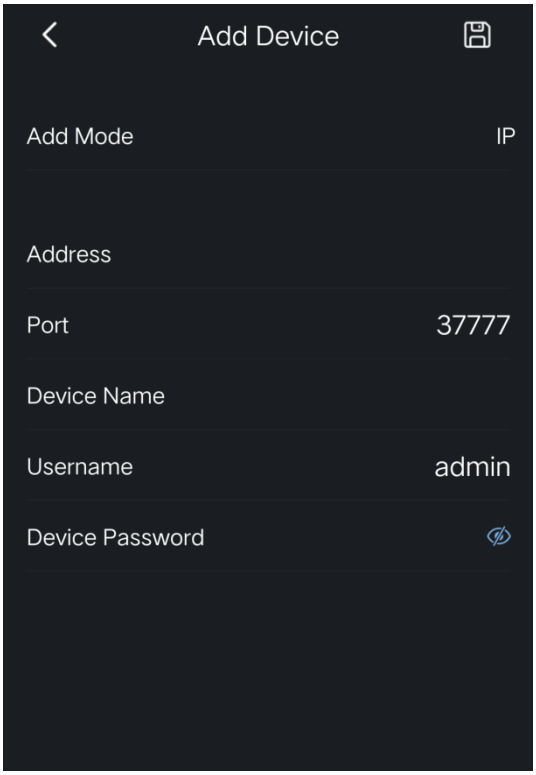
Step 1 Grifo **IP / dominio** en la Figura 5-3.

Figure 5-4 Añadir dispositivo



Step 2 Grifo **VTO** sobre el **Añadir dispositivo** interfaz.

Figure 5-5 Añadir dispositivo

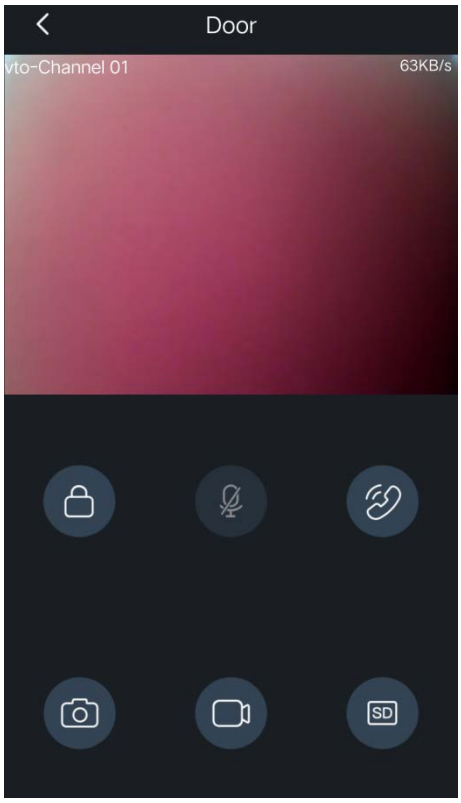


Step 3 Ingrese la dirección (dirección IP del VTO), el nombre del dispositivo y la contraseña del dispositivo.

Step 4 Grifo

Se agrega el VTO. Puede ver videos capturados por el VTO, llamar al VTO, desbloquear puertas cuando hay una llamada del VTO y más.

Figure 5-6 Puerta



5.2 Agregar a través de Soft Access Point (AP)

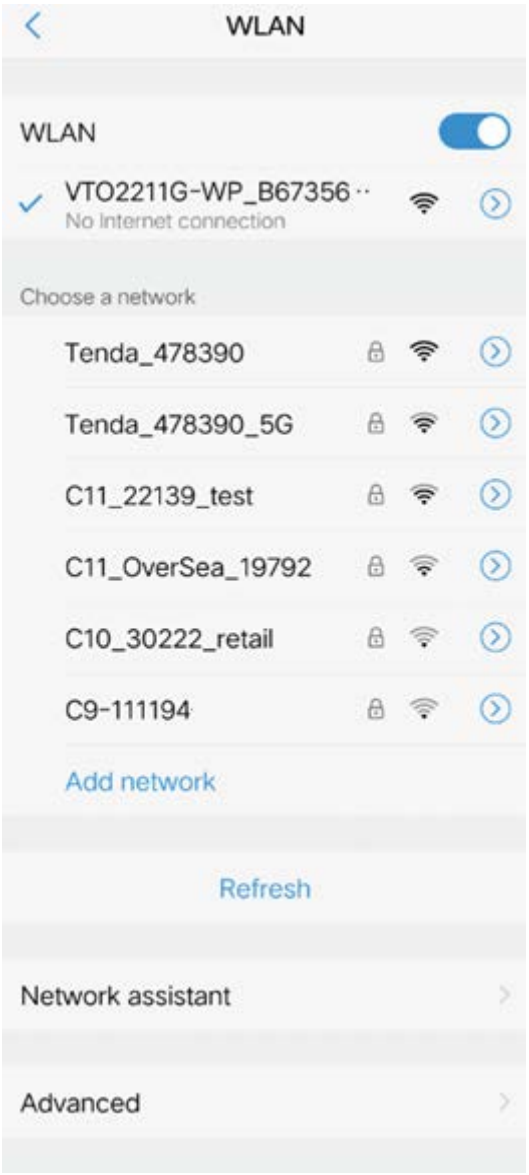
Step 1 Conecte la estación de puerta a la fuente de

Step 2 alimentación. Ve a la**WLAN** interfaz de su teléfono móvil.

Step 3 Mantenga presionado el botón de llamada en la estación de puerta durante más de 5 segundos hasta que

Step 4 escuche un pitido. Conecte su teléfono al**VTO2211G-WP_b67356 ..** la red.

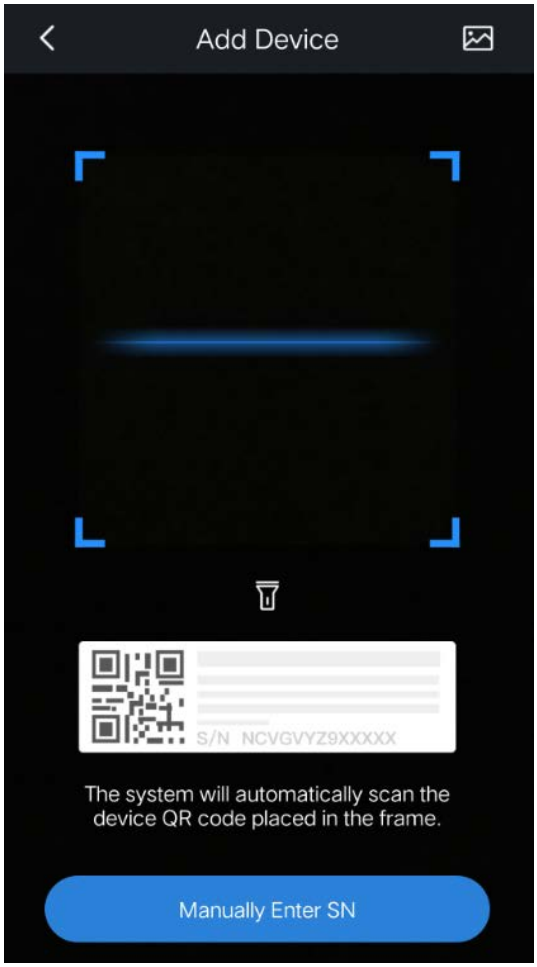
Figure 5-7 Teléfono móvilWLAN



Step 5 Grifo en la esquina superior derecha de la **Administrador de dispositivos** interfaz (consulte la Figura 5-3).

Step 6 Grifo **SN / Escaneo** en la Figura 5-3.

Figure 5-8 Escanea el código QR

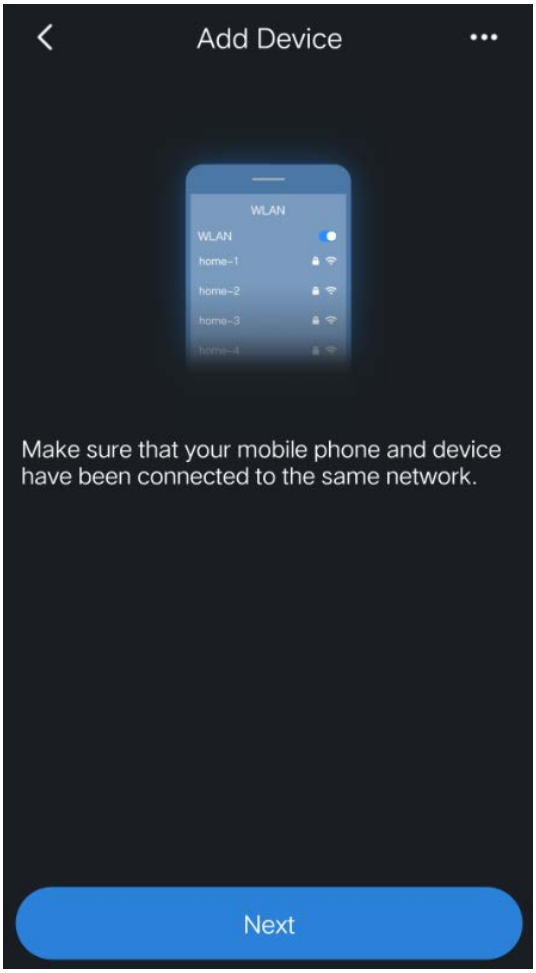


Step 7 Escanee el código QR en la cubierta trasera del videoportero.

El código QR también se puede encontrar en **Red> Básico> P2P** en la interfaz web, toque

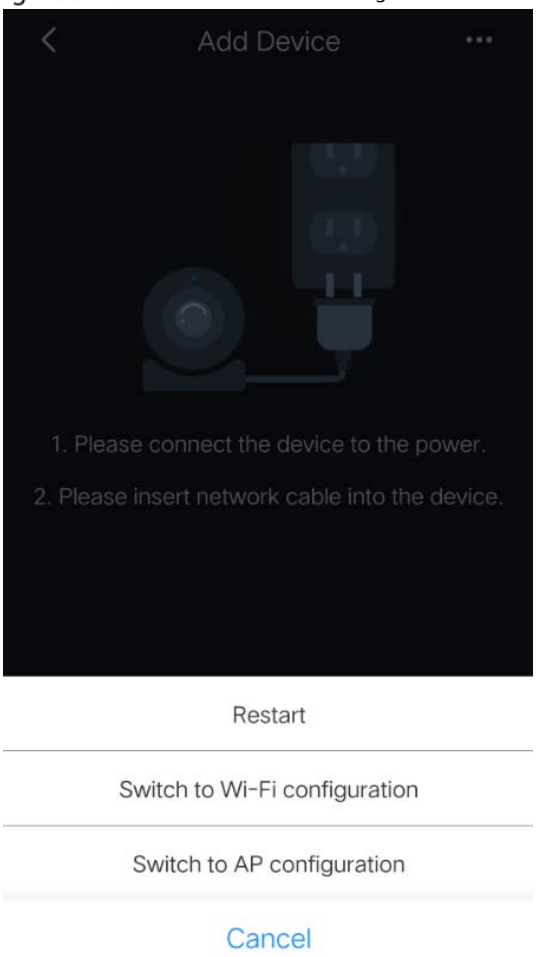
Step 8 **Próximo.**

Figure 5-9 Añadir dispositivo



Step 9 Grifo ••• en la esquina superior derecha.

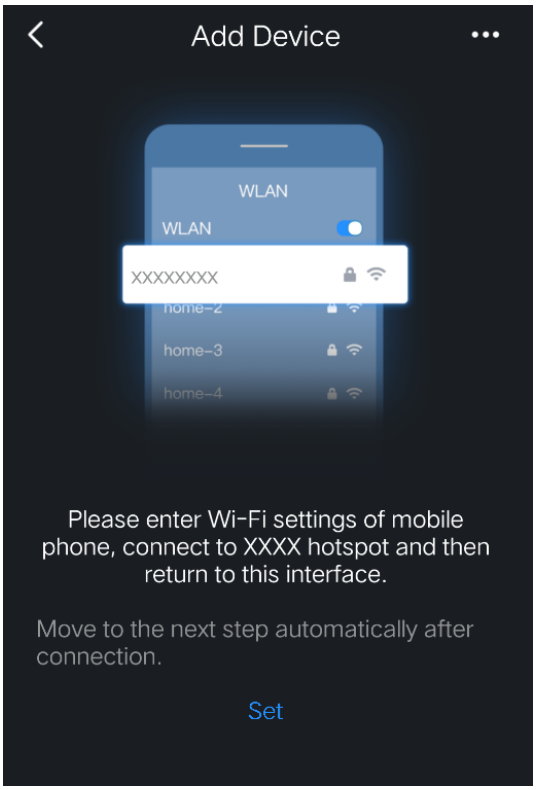
Figure 5-10 Seleccione el modo de configuración de red



Step 10 Seleccione **Cambie a Configuración AP.**

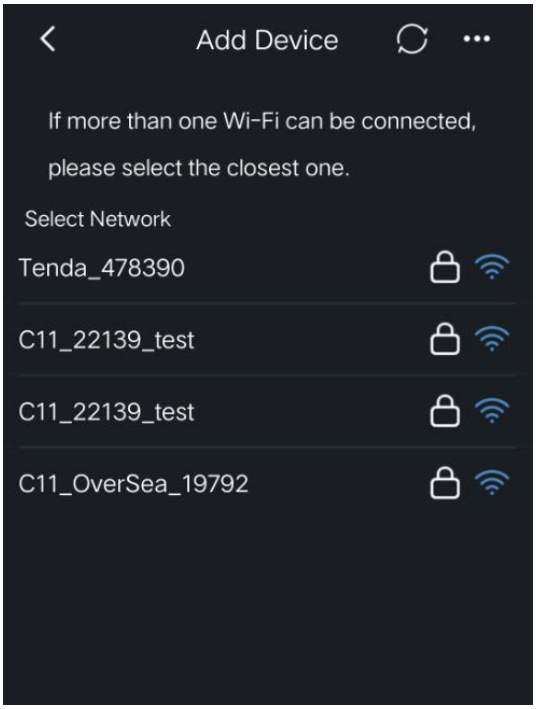
Step 11 Grifo **Próximo.**

Figure 5-11 Establecer red telefónica



Step 12 Grifo **Colocar.**

Figure 5-12 Seleccione aWi-Fi



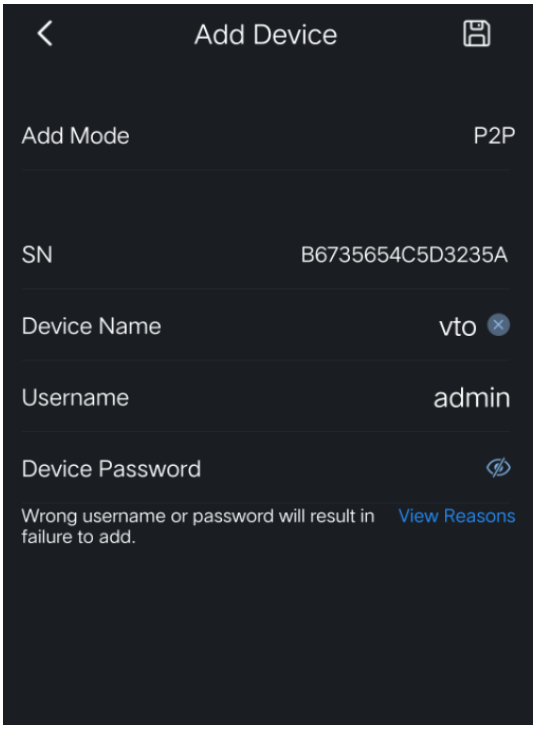
Step 13 Toque un nombre de Wi-Fi.

Figure 5-13 Ingrese la contraseña de Wi-Fi

Step 14 Ingrese la contraseña de Wi-Fi. Grifo

Step 15 **Próximo.**

Figure 5-14 Añadir dispositivo



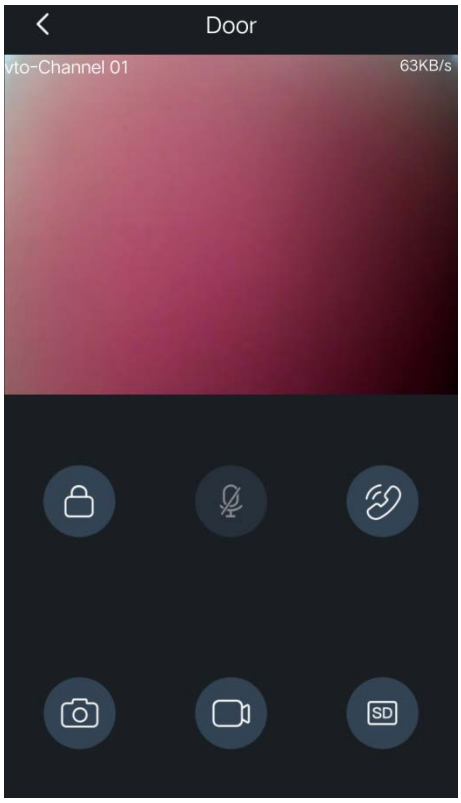
Step 16 Ingrese el nombre del dispositivo y la contraseña del dispositivo (contraseña de inicio de sesión web de la estación de puerta).

Step 17 Grifo

Se agrega el VTO. Puede ver videos capturados por el VTO, llamar al VTO, desbloquear puertas cuando hay una llamada del VTO y más.

Después de agregar estaciones de puerta a la aplicación, debe suscribirse a los mensajes y luego se pueden enviar notificaciones automáticas a su teléfono.

Figure 5-15 Puerta



Appendix 1 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 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 personajes; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;

No incluya 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 inTime

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 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 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 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 dispositivos 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 la información de restablecimiento de contraseñas

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 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. Habilite el 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, reduciendo el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6. Habilite 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 que vincule la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de suplantación de ARP.

8. 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.

9. Desactive los servicios innecesarios y elija los 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 de correo.

FTP: elija SFTP y configure contraseñas seguras.

Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10. 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 cifrada provocará una pérdida en la eficiencia de la transmisión.

11. 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.

Verificar el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

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 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.

13. Construya un entorno de red seguro

Para garantizar mejor la seguridad del dispositivo 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 la 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 utilizar VLAN, red GAP 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 permitidos para acceder al dispositivo.