Control de asistencia y tiempo mediante reconocimiento facial

Guía de inicio rápido

Versión 1.0.0

Prefacio

General

Este manual presenta la instalación y el funcionamiento del sistema de control de asistencia y horario con reconocimiento facial (en adelante, el "sistema de control de asistencia y horario"). Lea atentamente antes de utilizar el dispositivo y guarde el manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.0	Primer lanzamiento.	Junio de 2022

Aviso de protección de la privacidad

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

Acerca del manual

- El manual es solo de referencia. Pueden existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Pueden encontrarse ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Actualizaciones de productos

Es posible que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.

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

Medidas de seguridad y advertencias importantes

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

Requerimientos de transporte

Transportar, utilizar y almacenar el sistema de control horario en condiciones de temperatura y humedad permitidas.

Requisito de almacenamiento

Guarde el control de tiempo y asistencia en condiciones de temperatura y humedad permitidas.

Requisitos de instalación

- No conecte el adaptador de corriente al sistema de control de tiempo y asistencia mientras el adaptador esté encendido.
- Cumpla estrictamente con los códigos y estándares de seguridad eléctrica locales. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del sistema de control de asistencia.
- No conecte el sistema de control de asistencia a dos o más tipos de fuentes de alimentación para evitar dañarlo.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.

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

Requisitos de funcionamiento

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

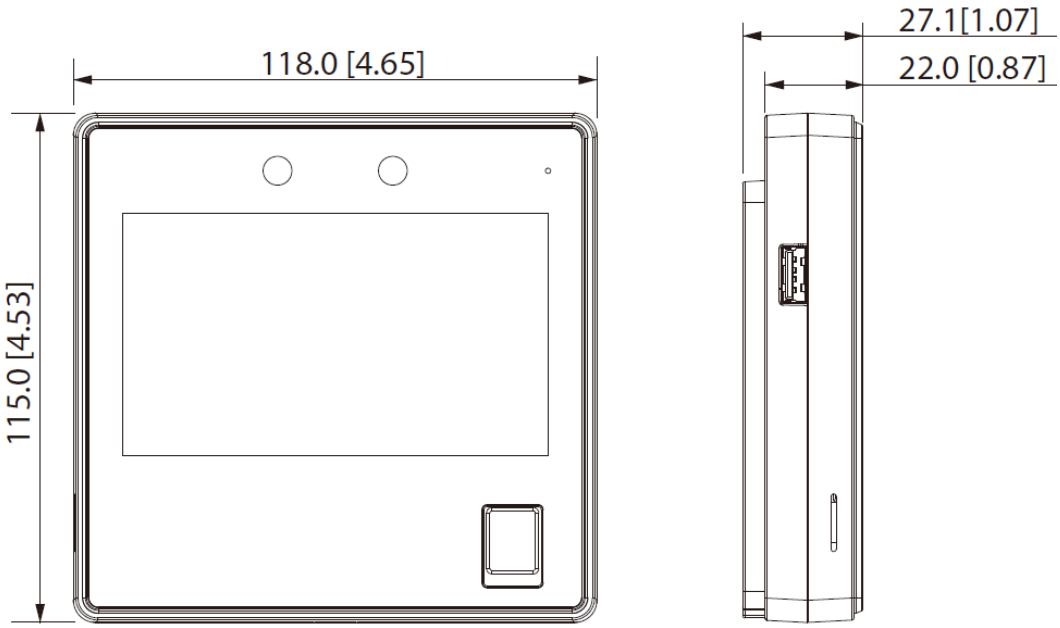
- No desconecte el cable de alimentación del costado del sistema de control de tiempo y asistencia mientras el adaptador esté encendido.
- Utilice el control de tiempo y asistencia dentro del rango nominal de entrada y salida de energía.
- Utilice el control de tiempo y asistencia en las condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquidos sobre el sistema de control de asistencia y asegúrese de que no haya ningún objeto lleno de líquido sobre el sistema para evitar que el líquido fluya hacia él.
- No desmonte el sistema de control de tiempo y asistencia sin instrucciones profesionales.

Tabla de contenido

1 Estructura

La apariencia frontal puede variar según los distintos modelos de control de asistencia. Aquí tomamos como ejemplo el modelo de huella dactilar.

Figura 1-1 Estructura (Unidad: mm [pulgadas])



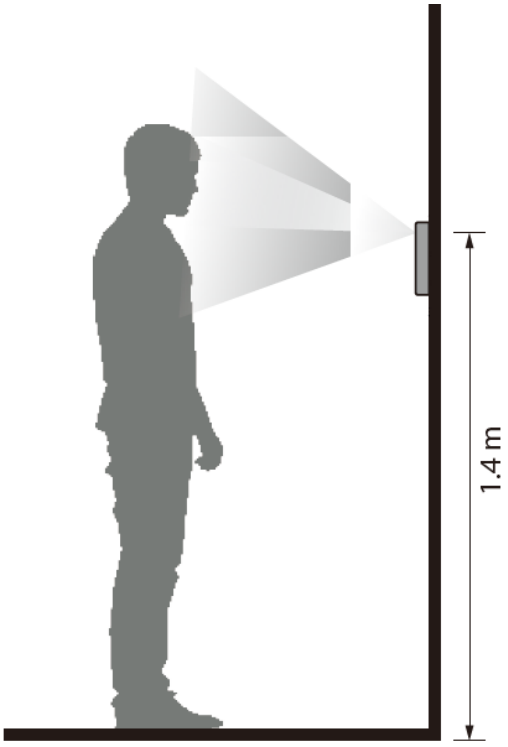
2 Conexión e instalación

2.1 Requisitos de instalación

- La altura de instalación es de 1,4 m (desde la lente hasta el suelo).
- La luz a 0,5 metros de distancia del control de horario y asistencia no debe ser inferior a 100 lux.
- Le recomendamos que lo instale en interiores, al menos a 3 metros de ventanas y puertas, y a 2 a metros de la fuente de luz.
- Evite la luz de fondo, la luz solar directa, la luz cercana y la luz oblicua.

Altura de instalación

Figura 2-1 Requisito de altura de instalación

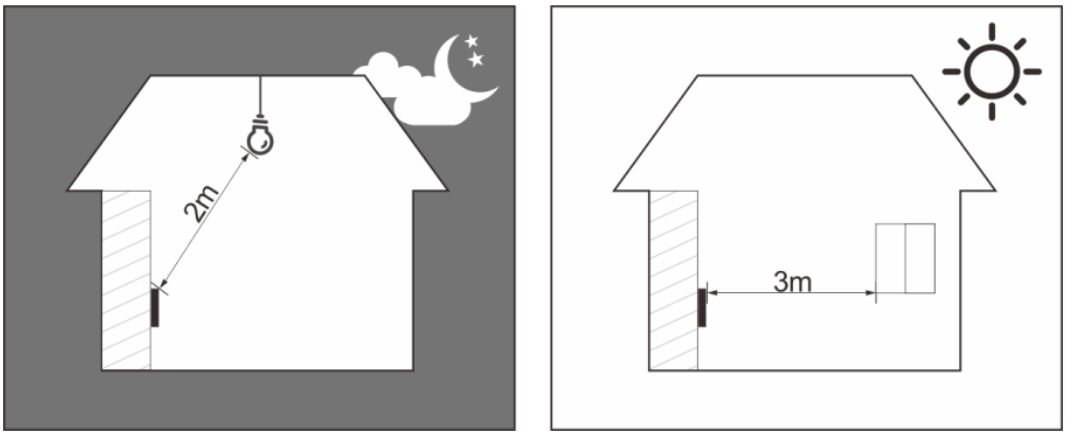


Requisitos de iluminación ambiental

Figura 2-2 Requisitos de iluminación ambiental

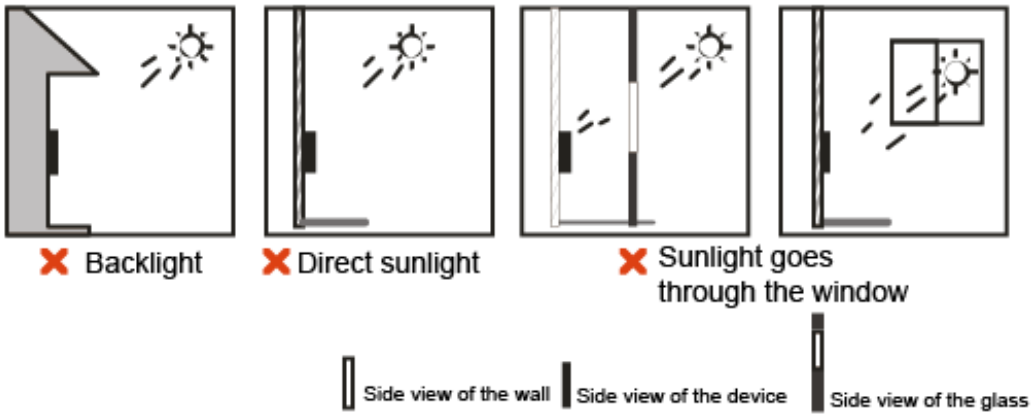
Ubicación de instalación recomendada

Figura 2-3 Ubicación de instalación recomendada



Ubicación de instalación no recomendada

Figura 2-4 Ubicación de instalación no recomendada



2.2 Proceso de instalación

Todos los sistemas de control de asistencia tienen el mismo método de instalación. En esta sección se toma como ejemplo el modelo de huella dactilar de control de asistencia.

2.2.1 Montaje en pared

Paso 1 Según la posición de los orificios en el soporte de instalación, taladre 3 orificios en la pared. Coloque pernos de expansión en los orificios.

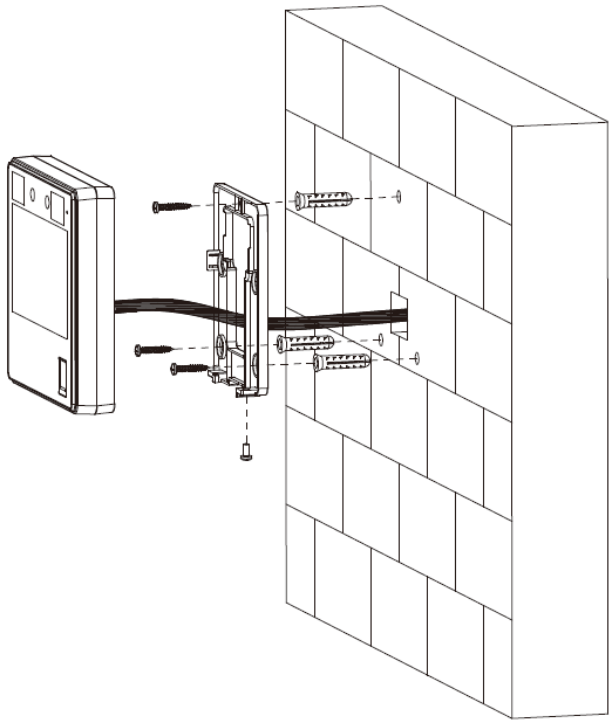
Paso 2 Utilice los 3 tornillos para fijar el soporte de instalación a la pared. Conecte

Paso 3 el sistema de control de asistencia.

Paso 4 Fije el tiempo y la asistencia en el soporte.

Paso 5 Atornille 1 tornillo de forma segura en la parte inferior del control de tiempo y asistencia.

Figura 2-5 Montaje en pared



2.2.2 86 Montaje en caja

Paso 1 Coloque una caja 86 en la pared a una altura adecuada. Fije el

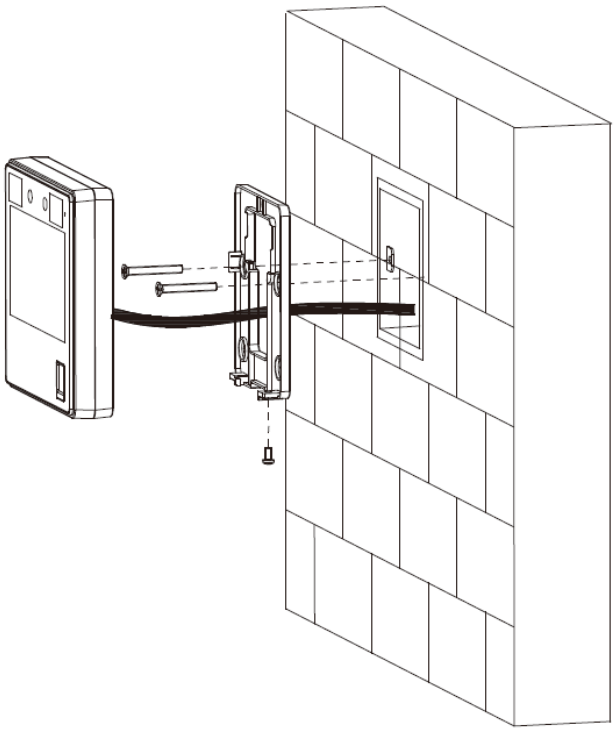
Paso 2 soporte de instalación a la caja 86 con 2 tornillos. Conecte el control

Paso 3 de asistencia y horario.

Paso 4 Fije el tiempo y la asistencia en el soporte.

Paso 5 Atornille 1 tornillo de forma segura en la parte inferior del control de tiempo y asistencia.

Figura 2-6 Montaje de caja 86

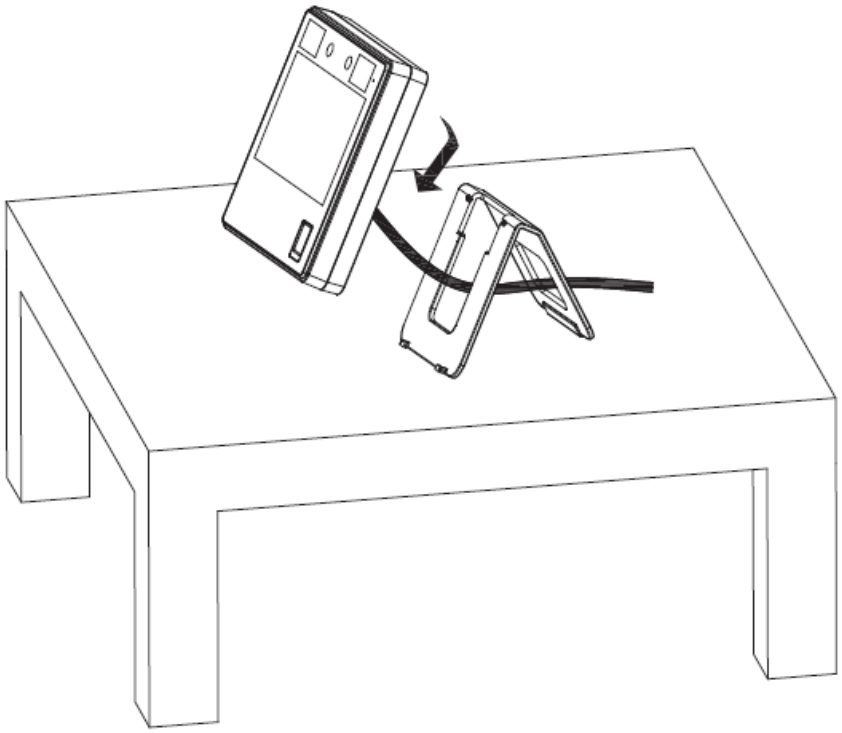


2.2.3 Montaje en mesa

Paso 1 Pase el cable a través de la abertura del soporte y luego conecte el cable al control de tiempo y asistencia.

Paso 2 Coloque el control de tiempo y asistencia en el soporte y deslícelo hacia abajo por el soporte.

Figura 2-7 Montaje de mesa



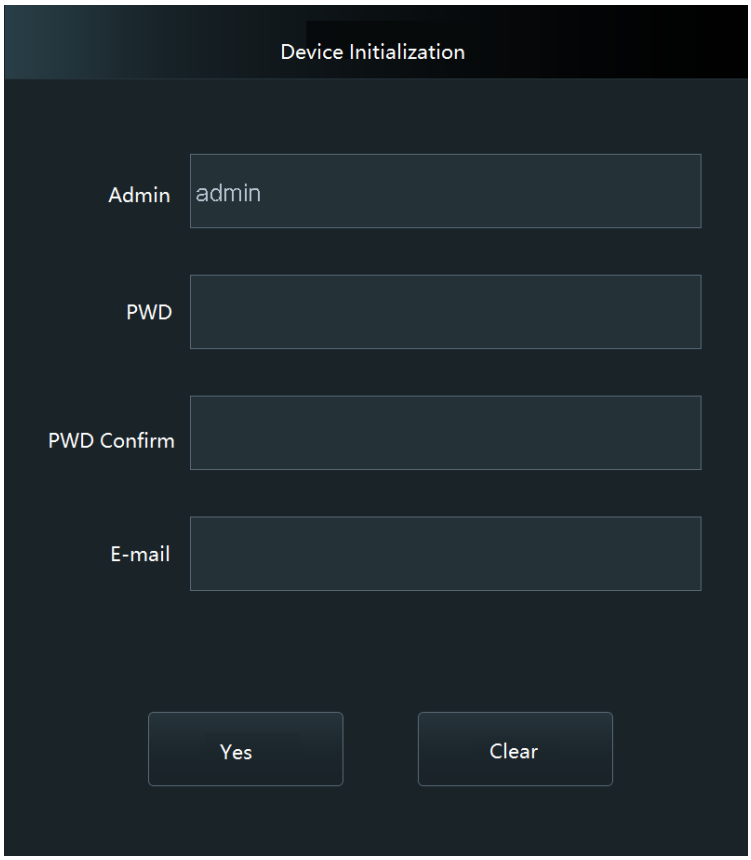
3 Configuraciones locales

Las operaciones locales pueden variar según los diferentes modelos.

3.1 Inicialización

Para el primer uso o después de restaurar los valores predeterminados de fábrica, debe seleccionar un idioma y luego establecer una contraseña y una dirección de correo electrónico para la cuenta de administrador. Después de eso, puede usar la cuenta de administrador para iniciar sesión en la pantalla del menú principal de Control de asistencia y horario y su página web.

Figura 3-1 Inicialización



- 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 sean espacios en blanco y contener al menos dos tipos de siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo las indicaciones sobre la fortaleza de la contraseña.

3.2 Agregar nuevos usuarios

Agregue nuevos usuarios ingresando información del usuario, como nombre, número de tarjeta, rostro y huella digital, y luego configure los permisos de usuario.

Paso 1 En el**Menú principal**pantalla, seleccionar**Usuario**>**Nuevo usuario**.

Paso 2 Configurar parámetros de usuario.

Figura 3-2 Nuevo usuario（1）

Figura 3-3 Nuevo usuario（2）

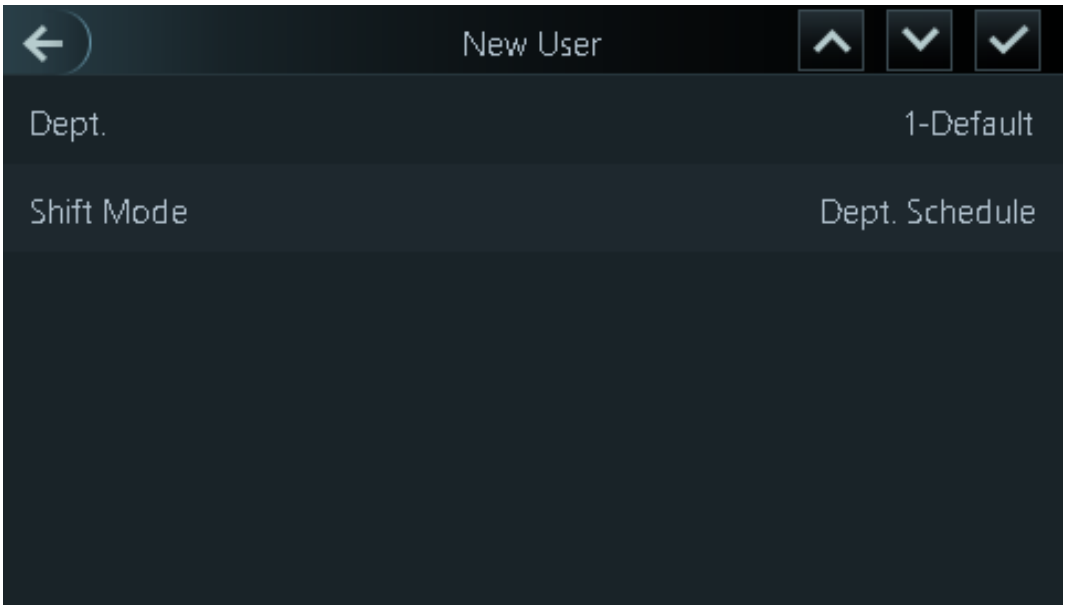


Tabla 3-1 Descripción del nuevo usuario

Parámetro	Descripción
ID de usuario	Introduzca el ID de usuario. El ID puede ser un número, una letra o una combinación de ambos, y la longitud máxima del ID de usuario es de 32 caracteres. Cada ID es único.
Nombre	Ingrese el nombre de usuario y la longitud máxima es de 32 caracteres, incluidos números, símbolos y letras.

Parámetro	Descripción
FP	Cada usuario puede registrar hasta 3 huellas dactilares. Siga las instrucciones en pantalla para registrar las huellas dactilares. Puede configurar la huella dactilar registrada como huella dactilar de coacción y se activará una alarma si la puerta se desbloquea con la huella dactilar de coacción. ● No recomendamos que configure la primera huella digital como huella dactilar de coacción. ● La función de huella dactilar solo está disponible para el modelo de huella dactilar del sistema de control de asistencia.
Rostro	Asegúrate de que tu rostro esté centrado en el marco de captura de imágenes y la imagen del rostro se capturará automáticamente. Puedes registrarte nuevamente si la imagen del rostro capturada no te satisface.
Tarjeta	Un usuario puede registrar hasta cinco tarjetas. Ingrese el número de su tarjeta o deslícela y luego el sistema de control de asistencia leerá la información de la tarjeta. Puede configurar la tarjeta registrada como tarjeta de coacción y luego se activará una alarma cuando se use una tarjeta de coacción para desbloquear la puerta. Sólo el modelo con deslizamiento de tarjeta admite esta función.
Personas con discapacidad	Introduzca la contraseña de usuario para desbloquear la puerta. La longitud máxima de la contraseña es de 8 dígitos.
Nivel de usuario	Establecer permisos de usuario para nuevos usuarios. ● **General**:Los usuarios sólo tienen permiso de acceso a la puerta. ● **Administración**:Los administradores pueden desbloquear la puerta y configurar la terminal de acceso.
Fecha válida	Define un período durante el cual se le concede al usuario acceso a un área segura.
Departamento	Configurar el departamento. Para obtener más información, consulte el manual del usuario de Control de asistencia y horario con reconocimiento facial.
Modo de cambio	Configure turnos según individuos o todo el departamento.

Paso 3 Grifo .

4 Iniciar sesión en la página web

En la página web también puedes configurar y actualizar el control de tiempo y asistencia.

Prerrequisitos

Asegúrese de que la computadora utilizada para iniciar sesión en la página web esté en la misma LAN que el control de tiempo y asistencia.

Las configuraciones de la página web varían según los modelos de Control de asistencia y horario. Solo algunos modelos Conexión de red de soporte de control de tiempo y asistencia.

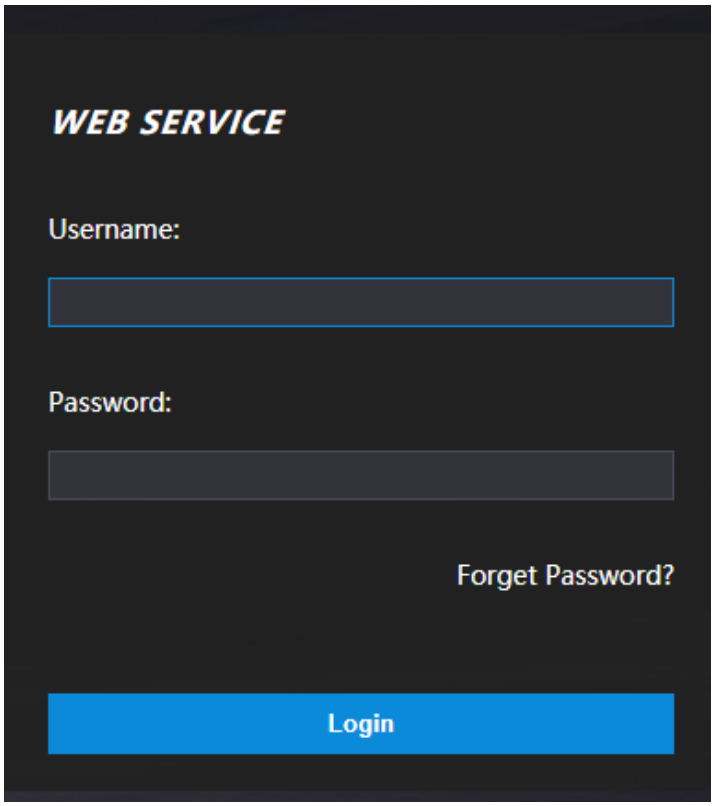
Procedimiento

Paso 1 Abra un navegador web, vaya a la dirección IP del control de tiempo y asistencia.

Puedes utilizar IE11, Firefox o Chrome.

Paso 2 Introduzca el nombre de usuario y la contraseña.

Figura 4-1 Inicialización



- El nombre de usuario predeterminado del administrador es admin, y la contraseña es la que usted configure. Durante la inicialización, le recomendamos que cambie la contraseña de administrador periódicamente. para aumentar la seguridad de la cuenta.
- Si olvida la contraseña de administrador, puede hacer clic**¿Olvidaste tu contraseña?**para restablecer la contraseña.

Paso 3 Hacer clic**Acceso**.

Apéndice 1 Puntos importantes de la toma de huellas dactilares

Instrucciones de registro

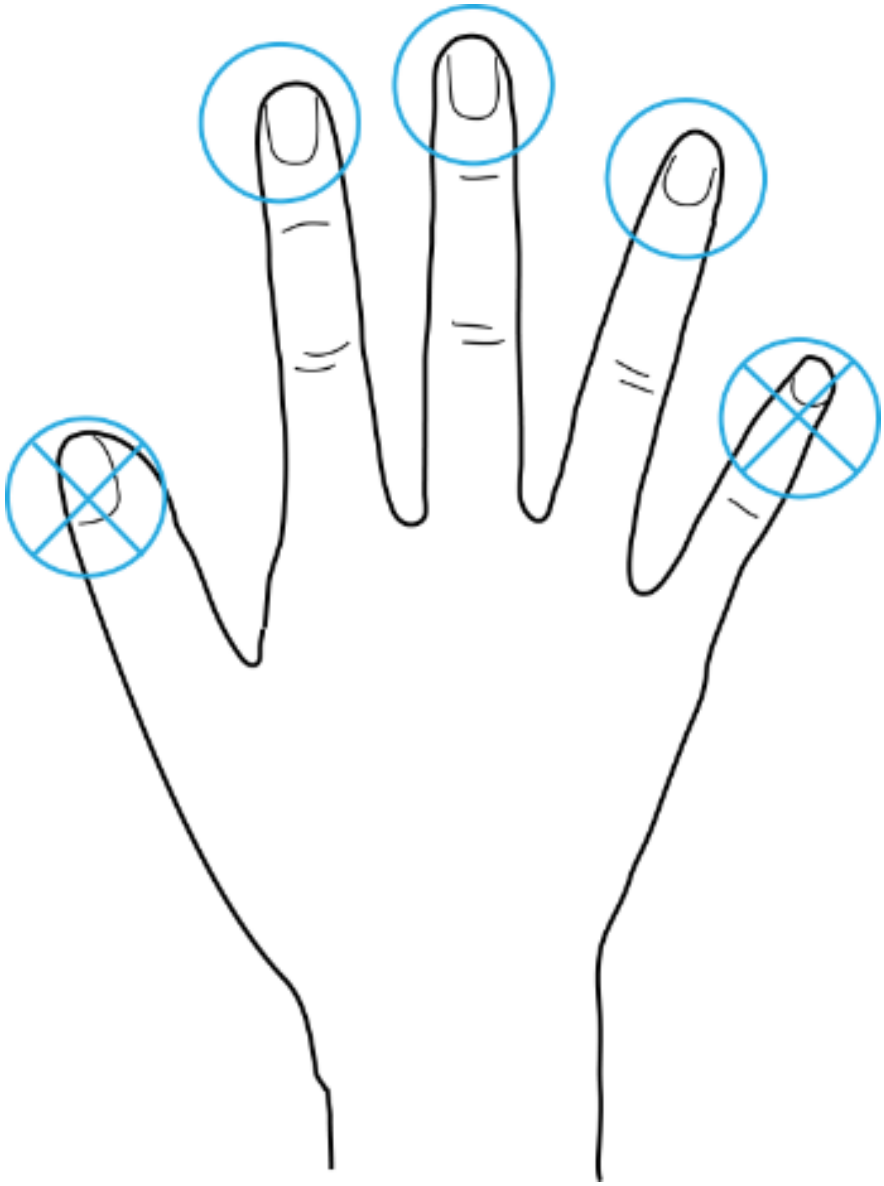
Al registrar la huella dactilar, preste atención a los siguientes puntos:

- Asegúrese de que sus dedos y la superficie del escáner estén limpios y secos.
- Presione 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.

Se recomiendan los dedos

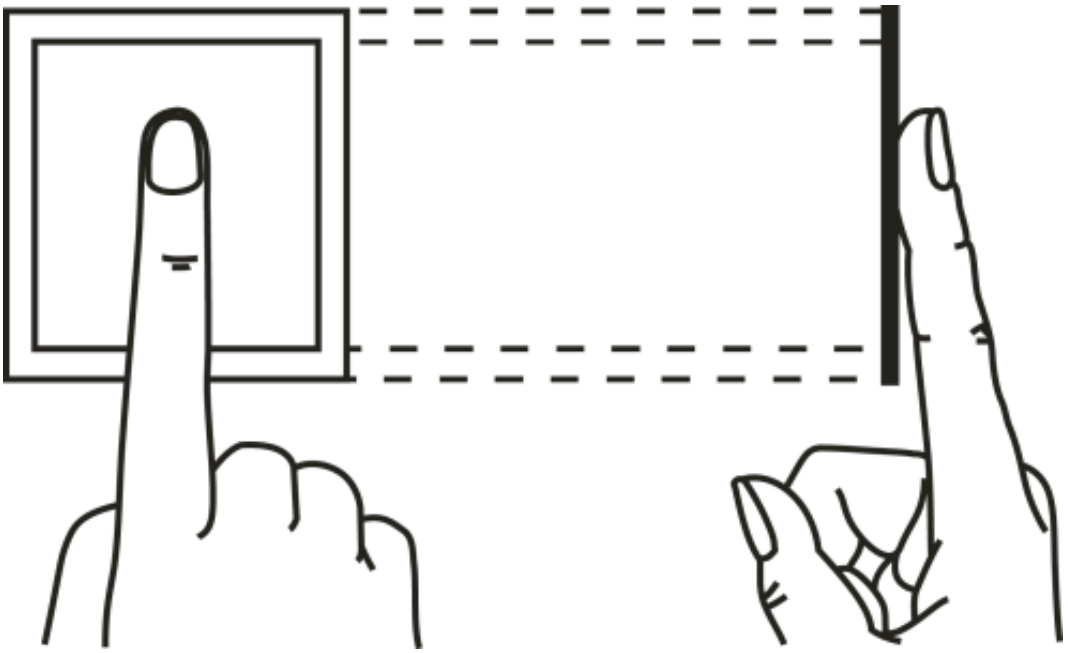
Se recomiendan los dedos índice, medio y anular. Los pulgares y meñiques no se pueden colocar fácilmente en el centro de la grabación.

Apéndice Figura 1-1 Dedos recomendados

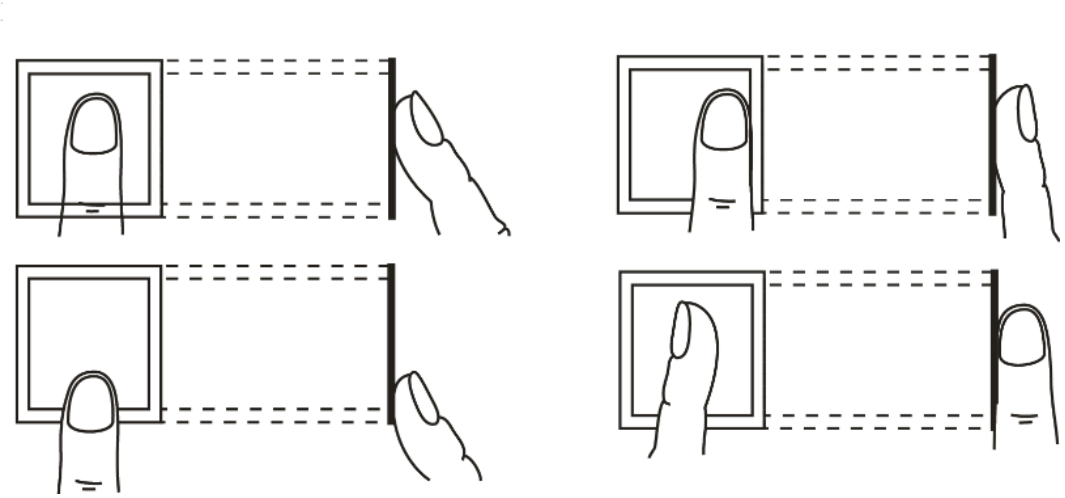


Cómo presionar su huella digital en el escáner

Apéndice Figura 1-2 Colocación correcta



Apéndice Figura 1-3 Colocación incorrecta



Apéndice 2 Puntos importantes del rostro

Registro

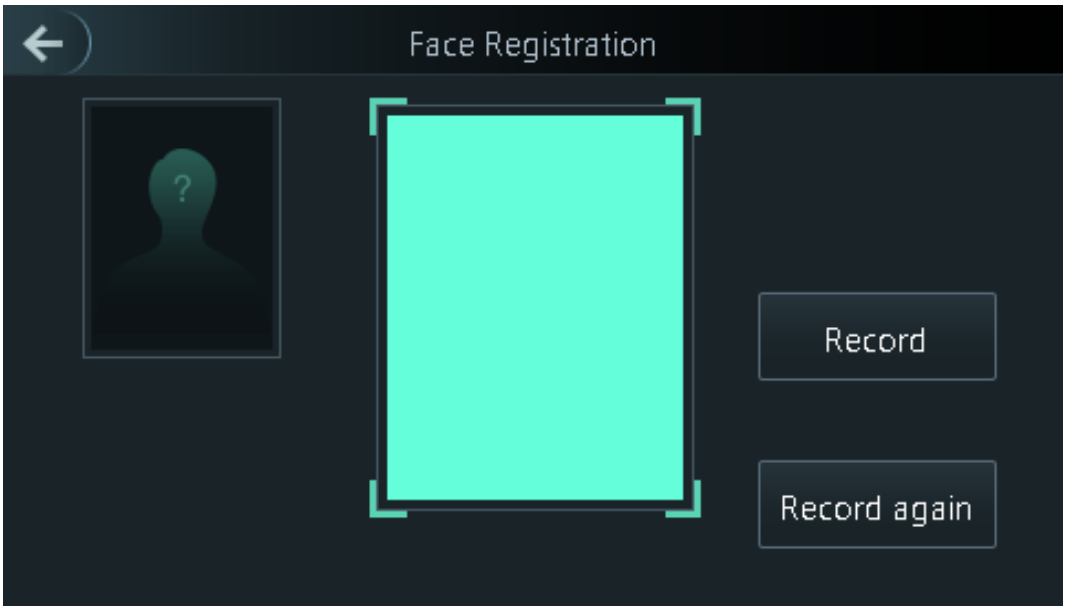
Antes de la inscripción

- Las gafas, los sombreros y las barbas pueden influir en el rendimiento del reconocimiento facial.
- No te cubras las cejas cuando uses sombrero.
- No cambie mucho el estilo de su barba si utiliza el control de tiempo y asistencia; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el control de tiempo y asistencia al menos a 2 metros de distancia de fuentes de luz y al menos a 3 metros de ventanas o puertas; de lo contrario, la luz de fondo y la luz solar directa podrían influir en el rendimiento de reconocimiento facial del control de tiempo y asistencia.

Durante el registro

- Puedes registrar rostros a través del dispositivo o a través de la plataforma. Para el registro a través de la plataforma, consulta el manual de usuario de la plataforma.
- Centra tu cabeza en el marco de captura de fotos. La imagen de tu rostro se capturará automáticamente.

Apéndice Figura 2-1 Registro de rostros

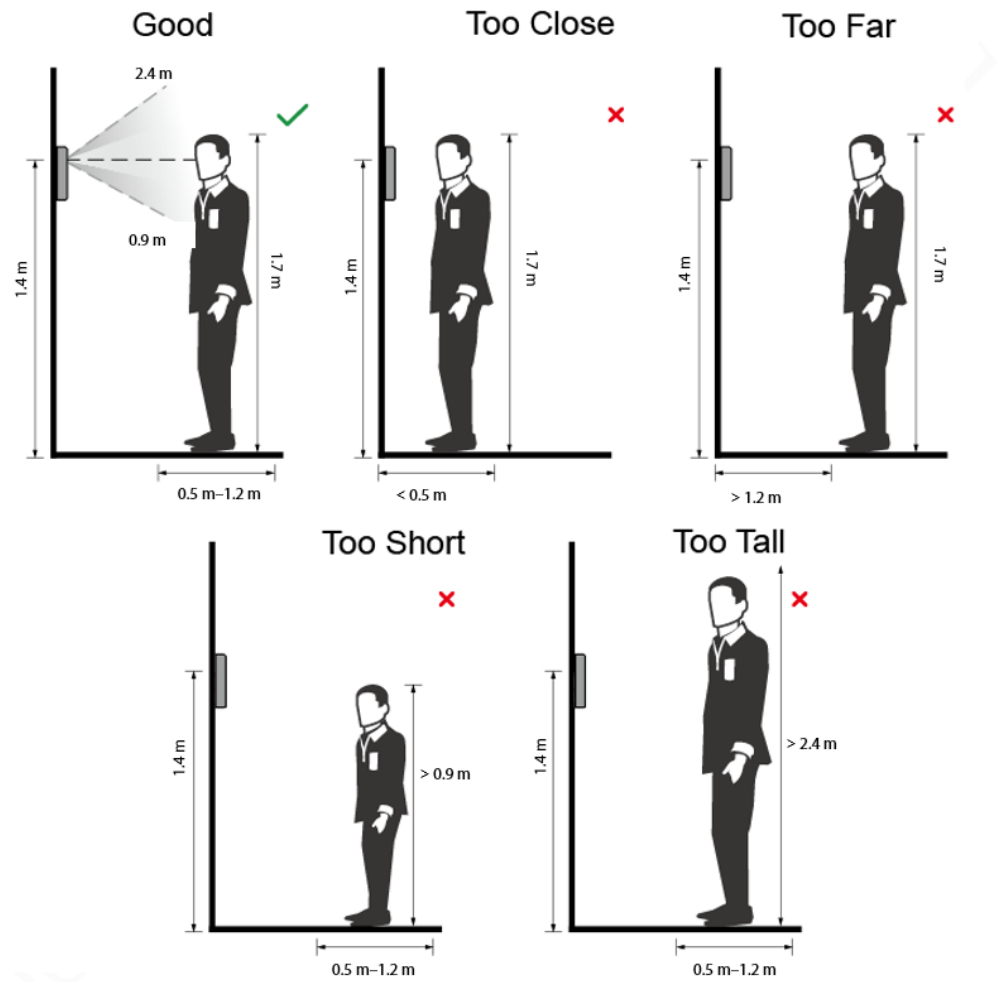


- No mueva la cabeza ni el cuerpo, de lo contrario el registro podría fallar.
- Evite que aparezcan dos caras en el cuadro de captura al mismo tiempo.

Posición de la cara

Si su cara no está en la posición adecuada, la precisión del reconocimiento facial podría verse afectada.

Apéndice Figura 2-2 Posición adecuada de la cara



Requisitos de las caras

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

Apéndice Figura 2-3 Posición de la cabeza

Apéndice Figura 2-4 Distancia entre caras

- Al importar imágenes de rostros a través de la plataforma de administración, asegúrese de que la imagen La resolución está dentro del rango de 150 × 300 píxeles a 600 × 1200 píxeles; los píxeles de la imagen son más de 500 × 500 píxeles; el tamaño de la imagen es inferior a 100 KB y el nombre de la imagen y la identificación de la persona son los mismos.
- Asegúrese de que el rostro ocupe más de 1/3 pero no más de 2/3 del área total de la imagen. y la relación de aspecto no exceda de 1:2.

Apéndice 3 Recomendaciones de ciberseguridad

Acciones obligatorias a tomar para la seguridad básica de la red de equipos:

1.**Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su 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 esté conectado a la red pública, se recomienda habilitar la función de "comprobación automática de actualizaciones" para obtener información oportuna sobre las actualizaciones de firmware publicadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "deseables de tener" para mejorar la seguridad de la red de sus equipos:

1.**Protección física**

Le sugerimos que realice una protección física de los equipos, especialmente de los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala de computadoras y un gabinete especiales, e implemente un control de acceso y una gestión de claves adecuados para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conectar sin autorización equipos extraíbles (como memorias USB, puertos seriales), etc.

2.**Cambie las contraseñas periódicamente**

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

3.**Establecer y actualizar contraseñas Restablecer información oportunamente**

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

4.**Habilitar bloqueo de cuenta**

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

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

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

6.**Habilitar HTTPS**

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

7.**Vinculación de dirección MAC**

Le recomendamos vincular la dirección IP y MAC del gateway al equipo, de esta manera

reduciendo el riesgo de suplantación de ARP.

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

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

9.**Desactivar servicios innecesarios y elegir modos seguros**

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

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

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

10.**Transmisión de audio y vídeo encriptados**

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

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

11.**Auditoría segura**

- Comprobar usuarios en línea: le sugerimos que compruebe periódicamente los usuarios en línea para ver si el dispositivo ha iniciado sesión sin autorización.
- Consultar log de equipos: Al consultar los logs podrás conocer las direcciones IP que se utilizaron para iniciar sesión en tus dispositivos y sus operaciones claves.

12.**Registro de red**

Debido a la capacidad de almacenamiento limitada del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante un período prolongado, se recomienda que habilite la función de registro de red para garantizar que los registros críticos se sincronicen con el servidor de registro de red para realizar el seguimiento.

13.**Construir un entorno de red seguro**

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

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