Tiempo de reconocimiento facial y asistencia

Guía de inicio rápido

V1.0.0

Prefacio

General

Este manual presenta la instalación y las operaciones del reconocimiento facial de tiempo y asistencia (en lo sucesivo, "tiempo y asistencia"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Revisión histórica

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

Aviso de protección de privacidad

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

Sobre el Manual

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

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

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

Medidas de seguridad y advertencias importantes

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

Requisito de transporte

Transporte, use y almacene el Time & Attendance en condiciones de humedad y temperatura permitidas.

Requisito de almacenamiento

Guarde Time & Attendance en las condiciones de humedad y temperatura permitidas.

requerimientos de instalación

 **WARNING**

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

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

Requisitos de operación

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

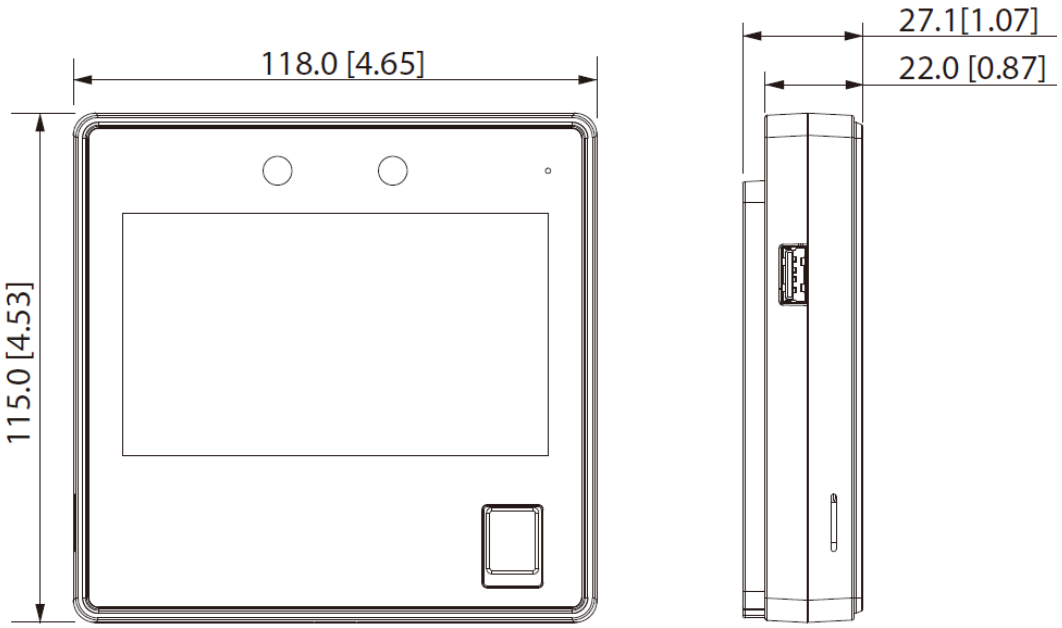
- No desenchufe el cable de alimentación del lateral del control de tiempo y asistencia mientras el adaptador está encendido.
- Opere Time & Attendance dentro del rango nominal de entrada y salida de energía.
- Utilice Time & Attendance en condiciones de humedad y temperatura permitidas.
- No deje caer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

Tabla de contenido

1 Estructura

La apariencia frontal puede diferir dependiendo de los diferentes modelos de Time & Attendance. Aquí tomamos el modelo de huella dactilar como ejemplo.

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



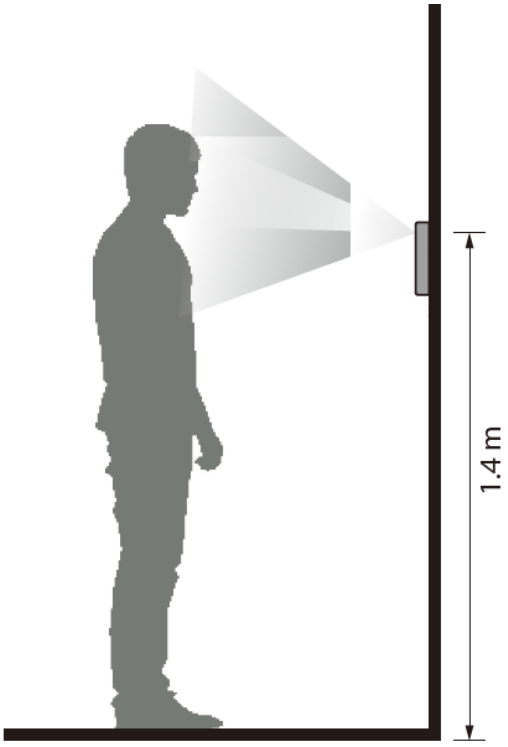
2 Conexión e Instalación

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 del Time & Attendance no debe ser inferior a 100 lux.
- Recomendamos instalar el interior, al menos a 3 metros de ventanas y puertas, y 2 metros de distancia 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

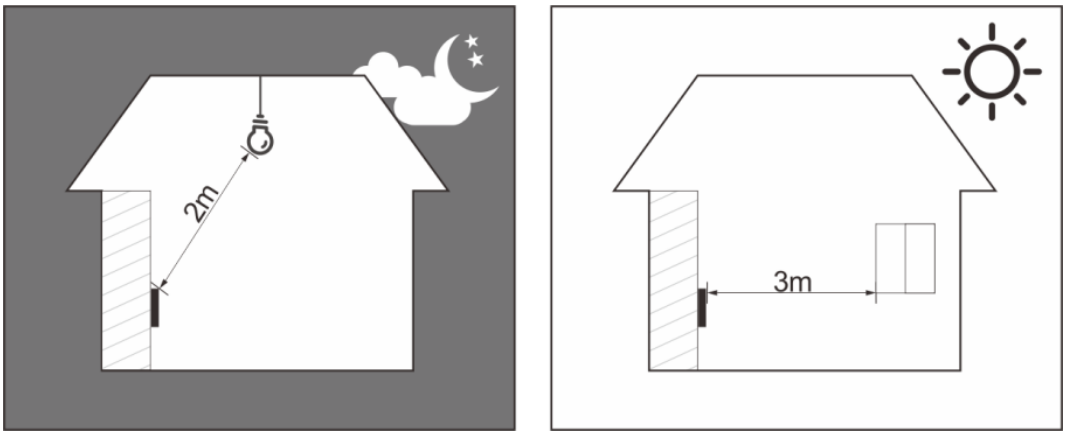


Requisitos de iluminación ambiental

Figura 2-2 Requisitos de iluminación ambiental

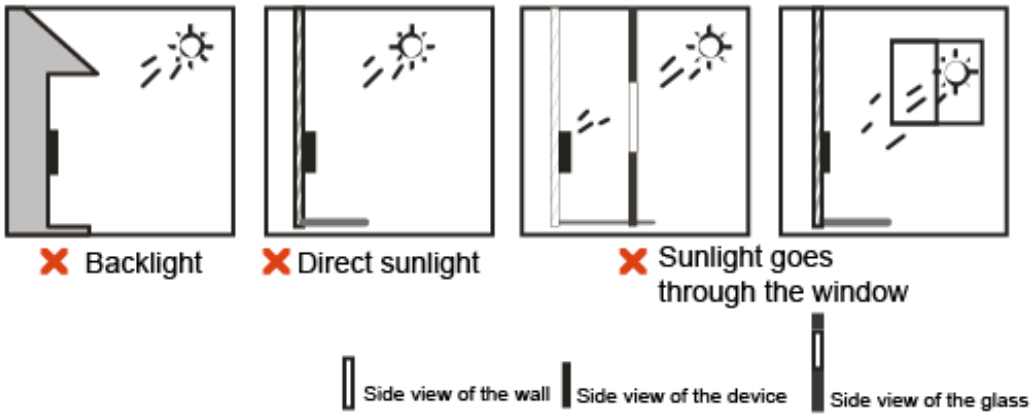
Ubicación de instalación recomendada

Figura 2-3 Ubicación de instalación recomendada



Ubicación de instalación no recomendada

Figura 2-4 Lugar de instalación no recomendado



2.2 Proceso de instalación

Todo el tiempo y asistencia tiene el mismo método de instalación. Esta sección toma como ejemplo el modelo de huella digital de tiempo y asistencia.

2.2.1 Montaje en pared

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

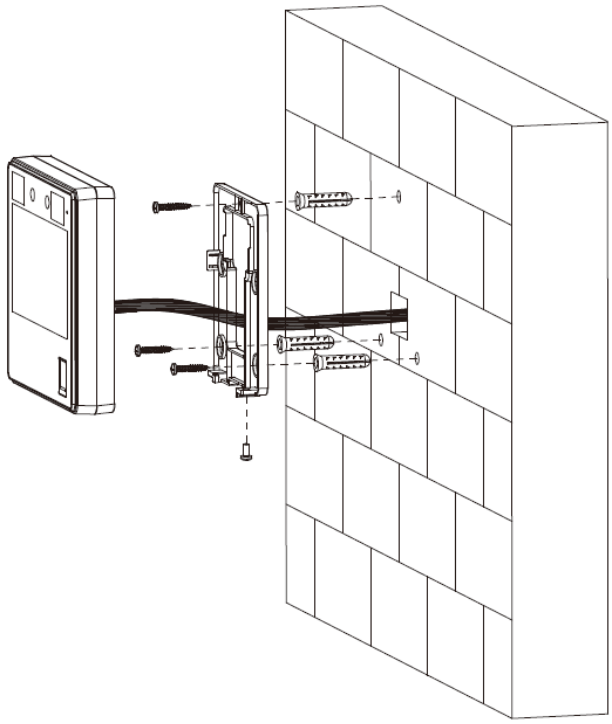
Paso 2 Utilice los 3 tornillos para fijar el soporte de instalación a la pared.

Paso 3 Conecte el tiempo y la asistencia.

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

Paso 5 Atornille 1 tornillo firmemente en la parte inferior del Time & Attendance.

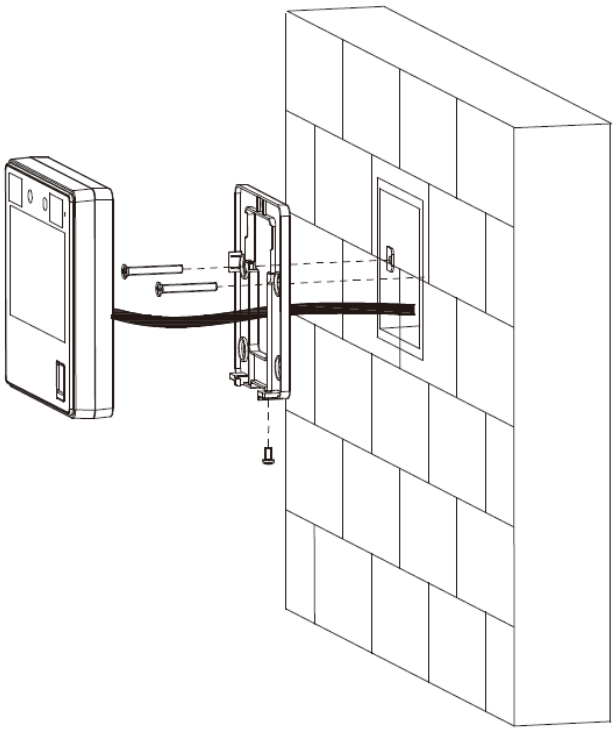
Figura 2-5 Montaje en pared



2.2.2 Montaje en caja 86

Paso 1 Coloque una caja de 86 en la pared a una altura adecuada. Fije el
Paso 2 soporte de instalación a la caja 86 con 2 tornillos. Conecte el
Paso 3 tiempo y la asistencia.
Paso 4 Fije el tiempo y la asistencia en el soporte.
Paso 5 Atornille 1 tornillo firmemente en la parte inferior del Time & Attendance.

Figura 2-6 Montaje en caja 86

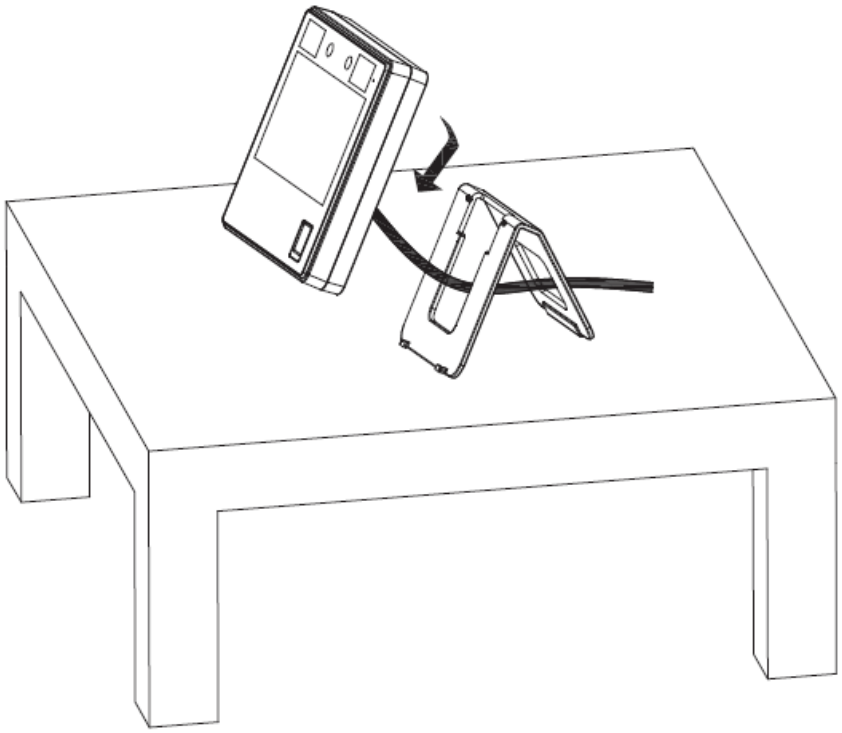


2.2.3 Montaje en mesa

Paso 1 Pase el cable a través de la abertura del soporte y luego conecte el cable a Time & Attendance.

Paso 2 Encaje el Time & Attendance en el soporte y deslícelo hacia abajo.

Figura 2-7 Montaje en mesa



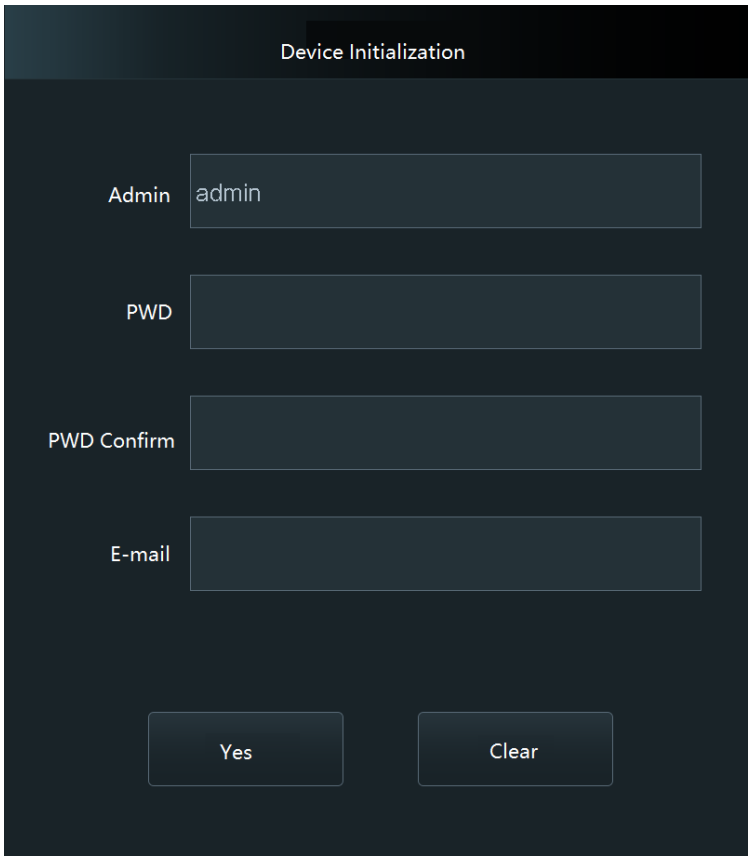
3 configuraciones locales

Las operaciones locales pueden diferir según los diferentes modelos.

3.1 Inicialización

Para el uso por primera vez 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 Time & Attendance 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 estén en blanco y contener al menos dos tipos de siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo el indicador de seguridad de la contraseña.

3.2 Adición de nuevos usuarios

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

Paso 1 Sobre el**Menú principal**pantalla, seleccione**Usuario**>**Nuevo Usuario**.

Paso 2 Configurar parámetros de usuario.

Figura 3-2 Nuevo usuario(1)

Figura 3-3 Nuevo usuario(2)

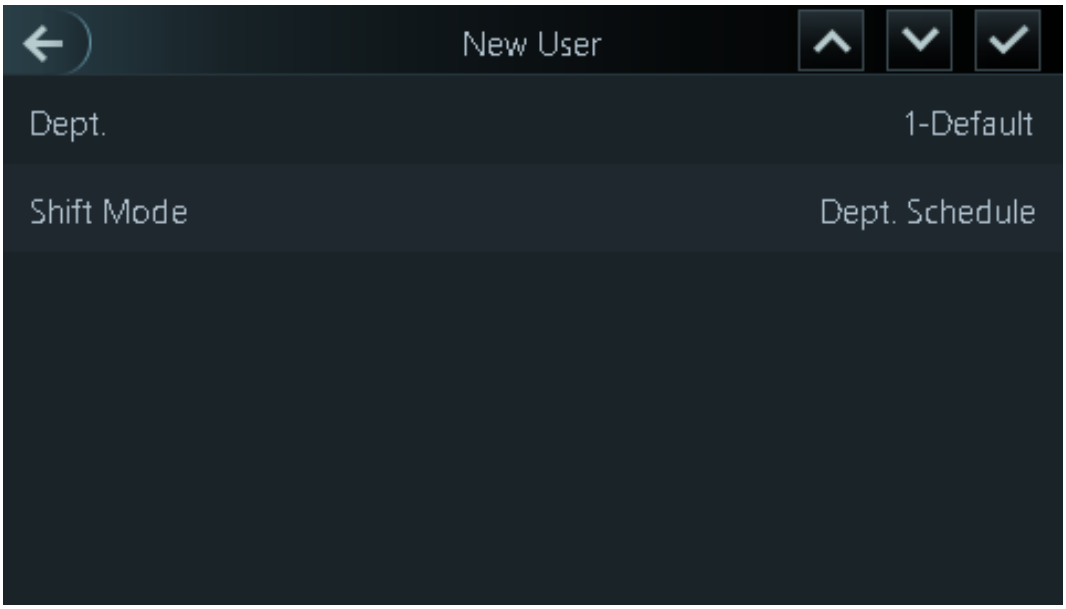


Tabla 3-1 Nueva descripción de usuario

Parámetro	Descripción
ID de usuario	Ingrese la identificación del usuario. El ID puede ser números, letras y sus combinaciones, y la longitud máxima del ID de usuario es de 32 caracteres. Cada identificación es única.
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 digital registrada como huella digital de coacción, y se activará una alarma si la puerta se abre con la huella digital de coacción. ● No recomendamos que configure la primera huella digital como la huella digital de coacción. ● La función de huellas dactilares solo está disponible para el modelo de huellas dactilares de Time Attendance.
Cara	Asegúrese de que su cara esté centrada en el cuadro de captura de imágenes y la imagen de la cara se capturará automáticamente. Puede registrarse nuevamente si encuentra que la imagen de la cara capturada no es satisfactoria.
Tarjeta	Un usuario puede registrar hasta cinco tarjetas. Ingrese su número de tarjeta o deslice su tarjeta, y luego la información de la tarjeta será leída por Time Attendance. 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. Solo el modelo de deslizamiento de tarjeta admite esta función.
PCD	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 solo tienen permiso de acceso a la puerta. ● **Administración**: Los administradores pueden desbloquear la puerta y configurar la Terminal de acceso.
Fecha válida	Defina un período durante el cual se otorga al usuario acceso a un área segura.
departamento	Configurar el departamento. Para obtener más información, consulte el manual de usuario de Face Recognition Time & Attendance.
Modo de cambio	Configure los turnos en función de las personas o de todo el departamento.

Paso 3 Tocar .

4 Iniciar sesión en la página web

En la página web, también puede configurar y actualizar el tiempo y la asistencia.

requisitos previos

Asegúrese de que la computadora utilizada para iniciar sesión en la página web esté en la misma LAN que Time & Attendance.

Las configuraciones de la página web difieren según los modelos de Time & Attendance. Solo ciertos modelos de conexión de red de soporte de tiempo y asistencia.

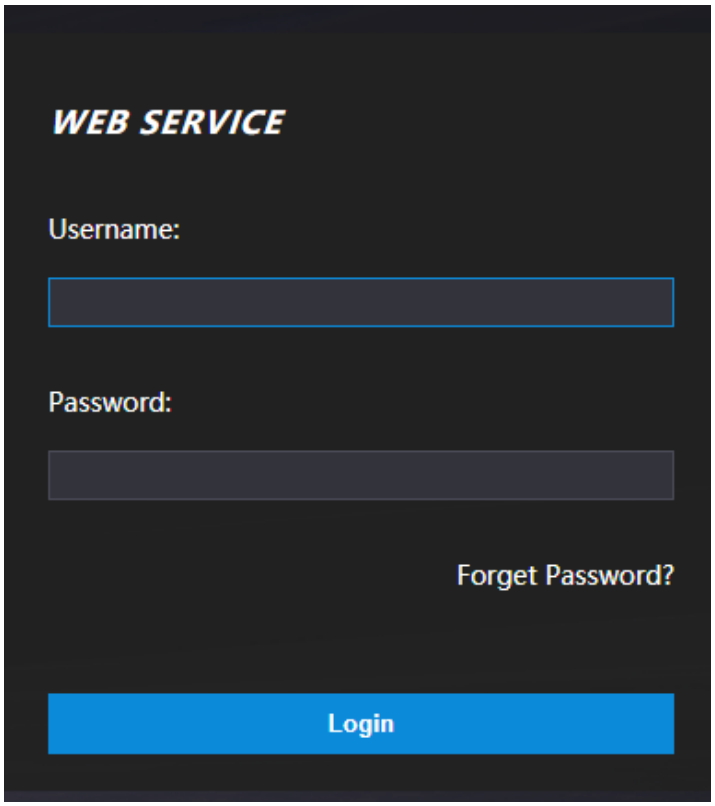
Procedimiento

Paso 1 Abra un navegador web, vaya a la dirección IP de Time & Attendance.

Puede usar 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 establece durante la inicialización. Le recomendamos que cambie la contraseña de administrador con regularidad. para aumentar la seguridad de la cuenta.
- Si olvida la contraseña de administrador, puede hacer clic en**¿Contraseña olvidada?**para restablecer la contraseña.

Paso 3 Hacer clic**Acceso**.

Apéndice 1 Puntos importantes de la huella digital

Instrucciones de registro

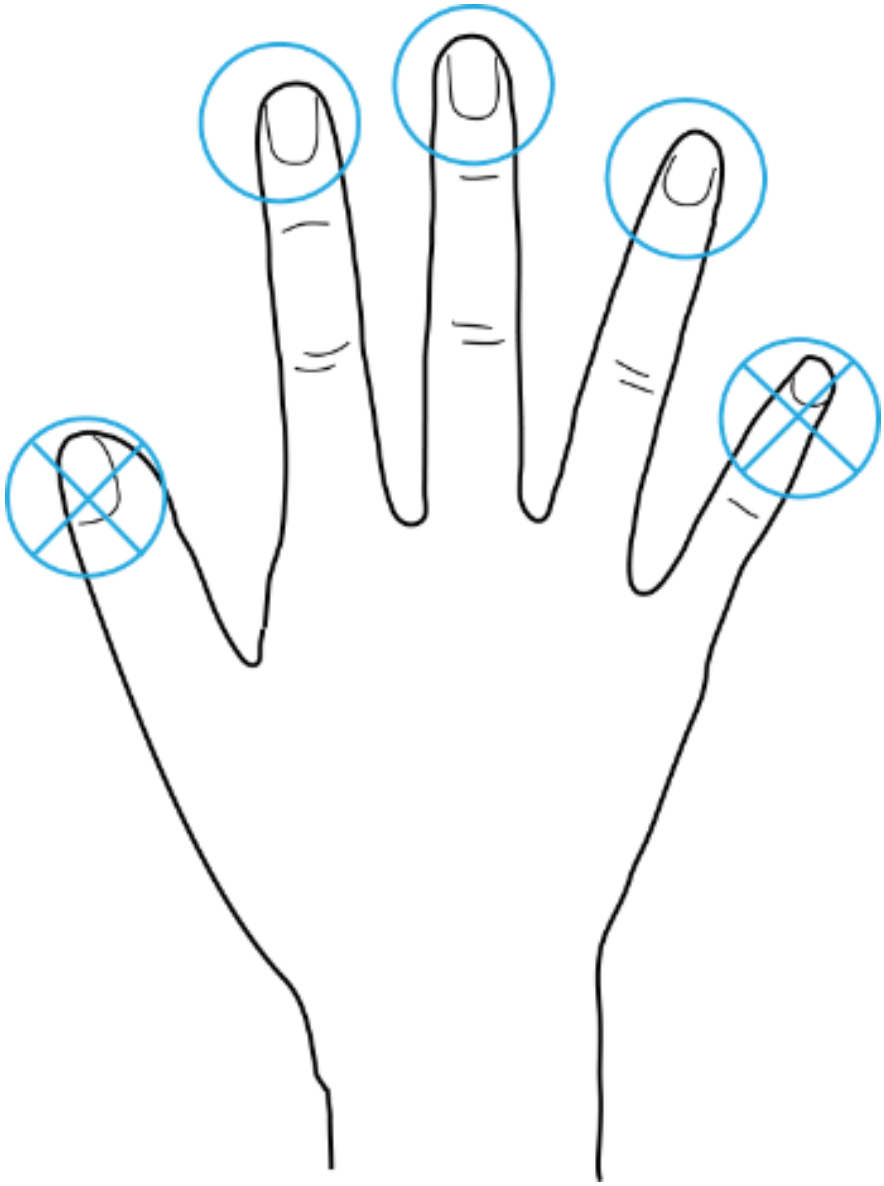
Cuando registre la huella digital, preste atención a los siguientes puntos:

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

Dedos recomendados

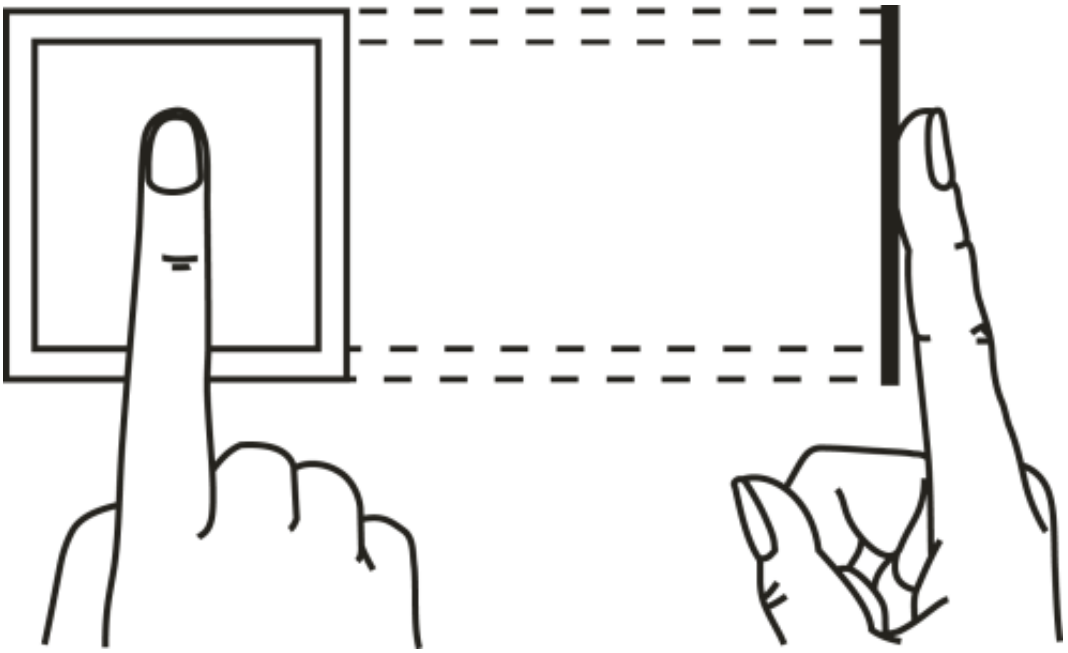
Se recomiendan los dedos índice, medio y anular. Los pulgares y los meñiques no se pueden colocar fácilmente en el centro de grabación.

Apéndice Figura 1-1 Dedos recomendados

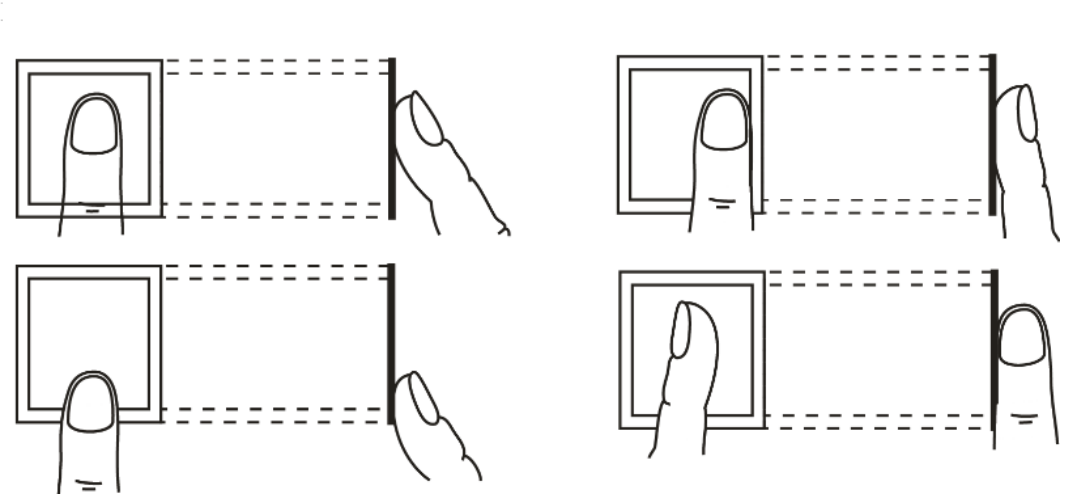


Cómo presionar su huella digital en el escáner

Apéndice Figura 1-2 Colocación correcta



Apéndice Figura 1-3 Colocación incorrecta



Apéndice 2 Puntos importantes de la cara

Registro

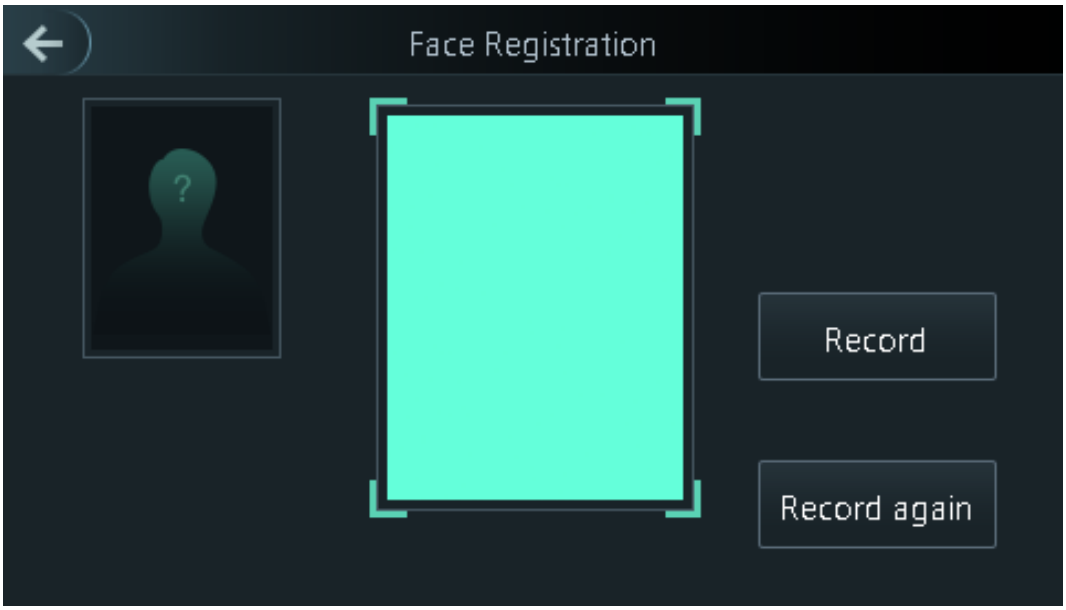
Antes del registro

- Las gafas, los sombreros y la barba pueden influir en el rendimiento del reconocimiento facial.
- No cubra sus cejas cuando use sombreros.
- No cambie mucho su estilo de barba si usa el Tiempo y asistencia; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga Time & Attendance al menos a 2 metros de distancia de la fuente 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 del reconocimiento facial de Time & Attendance.

Durante el registro

- Puedes registrar rostros a través del dispositivo o a través de la plataforma. Para el registro a través de la plataforma, consulte el manual de usuario de la plataforma.
- Haga que su cabeza se centre en el marco de captura de fotos. La imagen de la cara se capturará automáticamente.

Apéndice Figura 2-1 Registro de rostros

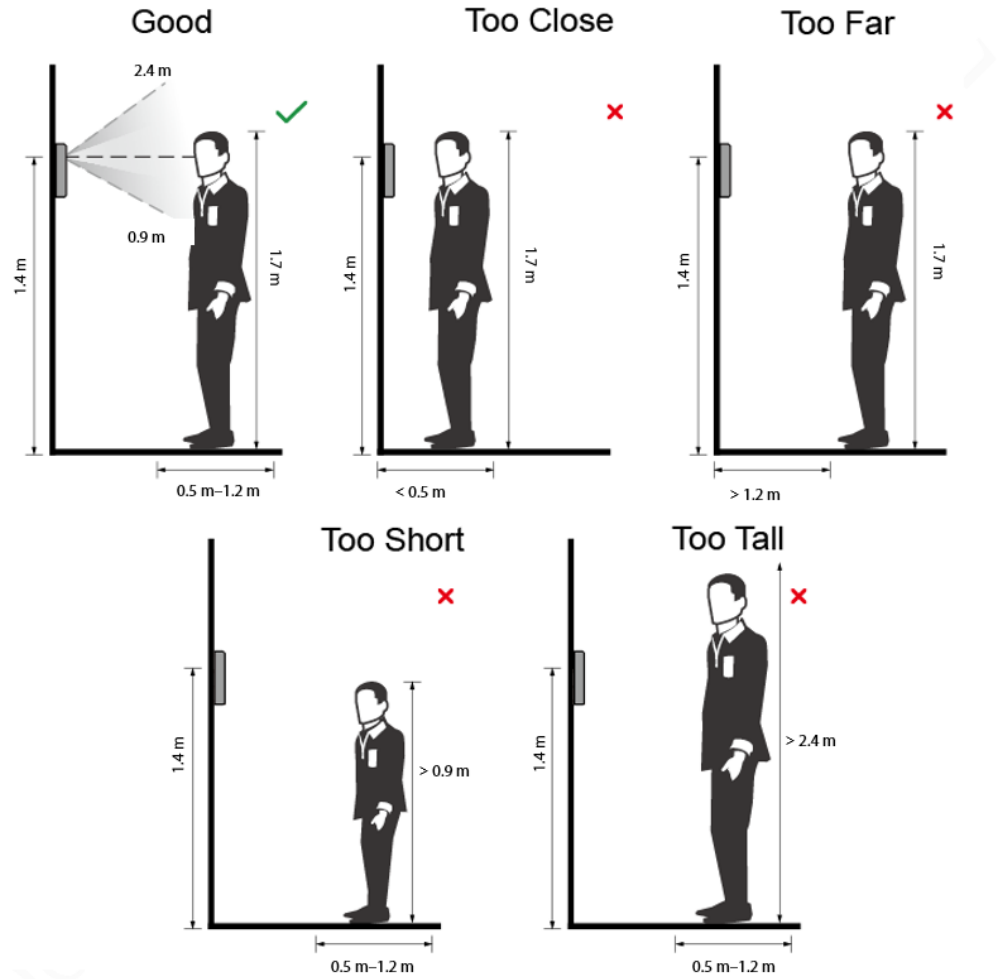


- No sacuda la cabeza o el cuerpo, de lo contrario, el registro podría fallar.
- Evite que aparezcan dos rostros en el cuadro de captura al mismo tiempo.

Posición de la cara

Si su rostro 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 que la frente no esté cubierta por pelo.
- No use anteojos, sombreros, barbas pobladas u otros adornos faciales que influyan en la grabación de imágenes faciales.
- Con los ojos abiertos, sin expresiones faciales, y coloca tu rostro hacia el centro de la cámara.
- Cuando grabe su rostro o durante el reconocimiento facial, no mantenga su rostro demasiado cerca o 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 el ID de la persona son los mismos.
- Asegúrese de que la cara ocupe más de 1/3 pero no más de 2/3 del área total de la imagen, y la relación de aspecto no supera 1:2.

Apéndice 3 Recomendaciones sobre ciberseguridad

Acciones obligatorias a realizar 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 caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No contenga el nombre de la cuenta o el nombre de la cuenta en orden inverso.
- No utilice caracteres continuos, como 123, abc, etc.
- No utilice caracteres superpuestos, como 111, aaa, etc.

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

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su 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 "autoverificación de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su 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 un gabinete y una sala de computadoras especiales, e implemente una administración de claves y permisos de control de acceso bien hechos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conexión no autorizada de equipos extraíbles (como un disco flash USB, puerto), etc

2.**Cambie las contraseñas regularmente**

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

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

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

4.**Habilitar bloqueo de cuenta**

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

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

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

6.**Habilitar HTTPS**

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

7.**Enlace de dirección MAC**

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

reduciendo el riesgo de falsificación de ARP.

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

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

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

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

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

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

10**Transmisión encriptada de audio y video**

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

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

11**Auditoría segura**

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

12**Registro de red**

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

13**Construir un entorno de red seguro**

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