Tiempo y asistencia (independiente)

Guía de inicio rápido

V1.0.0

Tabla de contenido

Declaración y recomendaciones de ciberseguridad

Acciones obligatorias a tomar en materia de ciberseguridad

1. Cambie las contraseñas y use contraseñas seguras:

La razón número uno por la que los sistemas son "pirateados" se debe a que tienen contraseñas débiles o predeterminadas. Dahua recomienda cambiar las contraseñas predeterminadas de inmediato y elegir una contraseña segura siempre que sea posible. Una contraseña segura debe estar compuesta por al menos 8 caracteres y una combinación de caracteres especiales, números y letras mayúsculas y minúsculas.

2. Actualizar firmware

Como es un procedimiento estándar en la industria de la tecnología, recomendamos mantener actualizado el firmware de la cámara NVR, DVR y IP para garantizar que el sistema esté actualizado con los últimos parches y correcciones de seguridad.

Verifique la versión de firmware de sus dispositivos en ejecución. Si la fecha de lanzamiento del firmware tiene más de 18 meses, comuníquese con un distribuidor local autorizado de Dahua o con el soporte técnico de Dahua para conocer las actualizaciones disponibles.

Recomendaciones “agradables de tener” para mejorar la seguridad de su red

1. Cambie las contraseñas regularmente

Cambie regularmente las credenciales de sus dispositivos para ayudar a garantizar que solo los usuarios autorizados puedan acceder al sistema.

2. Cambiar los puertos HTTP y TCP predeterminados:

● Cambiar los puertos HTTP y TCP predeterminados para los sistemas Dahua. Estos son los dos puertos que se utilizan para comunicarse y ver videos de forma remota.

● Estos puertos se pueden cambiar a cualquier conjunto de números entre 1025 y 65535. Evitar los puertos predeterminados reduce el riesgo de que personas externas puedan adivinar qué puertos está utilizando.

3. Habilite HTTPS/SSL:

Configure un certificado SSL para habilitar HTTPS. Esto encriptará toda la comunicación entre sus dispositivos y la grabadora.

4. Habilitar filtro IP:

Habilitar su filtro IP evitará que todos, excepto aquellos con direcciones IP específicas, accedan al sistema.

5. Cambiar la contraseña de ONVIF:

En el firmware anterior de la cámara IP, la contraseña de ONVIF no cambia cuando cambia las credenciales del sistema. Deberá actualizar el firmware de la cámara a la última revisión o cambiar manualmente la contraseña de ONVIF.

6. Reenviar solo los puertos que necesita:

● Solo reenvíe los puertos HTTP y TCP que necesita usar. No reenvíe una gran variedad de números al dispositivo. No DMZ la dirección IP del dispositivo.

● No necesita reenviar ningún puerto para cámaras individuales si todas están conectadas a una grabadora en el sitio; solo se necesita el NVR.

7. Deshabilite el inicio de sesión automático en SmartPSS:

Aquellos que usan SmartPSS para ver su sistema y en una computadora que usan varias personas deben deshabilitar el inicio de sesión automático. Esto agrega una capa de seguridad para evitar que los usuarios sin las credenciales adecuadas accedan al sistema.

8. Utilice un nombre de usuario y una contraseña diferentes para SmartPSS:

En el caso de que su cuenta de redes sociales, banco, correo electrónico, etc. se vea comprometida, no querrá que alguien recopile esas contraseñas y las pruebe en su sistema de videovigilancia. El uso de un nombre de usuario y una contraseña diferentes para su sistema de seguridad hará que sea más difícil para alguien adivinar cómo ingresar a su sistema.

9. Funciones de límite de las cuentas de invitados:

Si su sistema está configurado para varios usuarios, asegúrese de que cada usuario solo tenga derechos sobre las características y funciones que necesita usar para realizar su trabajo.

10. UPnP:

● UPnP intentará automáticamente reenviar puertos en su enrutador o módem. Normalmente esto sería algo bueno. Sin embargo, si su sistema reenvía automáticamente los puertos y deja las credenciales predeterminadas, puede terminar con visitantes no deseados.

● Si reenvió manualmente los puertos HTTP y TCP en su enrutador/módem, esta función debe desactivarse independientemente. Se recomienda deshabilitar UPnP cuando la función no se usa en aplicaciones reales.

11. SNMP:

Deshabilite SNMP si no lo está utilizando. Si está utilizando SNMP, debe hacerlo solo temporalmente, solo con fines de seguimiento y prueba.

12. Multidifusión:

La multidifusión se utiliza para compartir transmisiones de video entre dos grabadoras. Actualmente no hay problemas conocidos relacionados con la multidifusión, pero si no está utilizando esta función, la desactivación puede mejorar la seguridad de su red.

13. Verifique el registro:

Si sospecha que alguien ha obtenido acceso no autorizado a su sistema, puede consultar el registro del sistema. El registro del sistema le mostrará qué direcciones IP se usaron para iniciar sesión en su sistema y a qué se accedió.

14. Bloquee físicamente el dispositivo:

Idealmente, desea evitar cualquier acceso físico no autorizado a su sistema. La mejor manera de lograr esto es instalar la grabadora en una caja de seguridad, un rack de servidor con llave o en una habitación que esté detrás de una cerradura y una llave.

15. Conecte las cámaras IP a los puertos PoE en la parte posterior de un NVR:

Las cámaras conectadas a los puertos PoE en la parte posterior de un NVR están aisladas del mundo exterior y no se puede acceder a ellas directamente.

16. Aislar NVR y red de cámaras IP

La red en la que reside su NVR y su cámara IP no debe ser la misma red que su red informática pública. Esto evitará que los visitantes o invitados no deseados obtengan acceso a la misma red que necesita el sistema de seguridad para funcionar correctamente.

Para obtener la información más reciente sobre Dahua, la declaración de seguridad cibernética y las recomendaciones, visitewww.dahuasecurity.com .

1 Descripción general del producto

1.1 Introducción

El tiempo de asistencia es un dispositivo de asistencia que firma mediante huella digital y contraseña. El dispositivo admite la configuración de asistencia de tiempo local, la exportación de estadísticas de asistencia de USB sin software y la gestión de asistencia de tiempo en el software de la plataforma. Tiene una apariencia simple y ordenada, adecuada para edificios comerciales, tiendas, fábricas, etc.

El dispositivo admite principalmente:

- Basado en TCP/IP
- Campana electrónica externa
- Dos roles de usuario: administrador y usuario normal
- Todos los usuarios pueden consultar sus registros de asistencia (presione #)
- Asistencia por huella digital o contraseña.
- Entrada de texto T9 del firmware de
- actualización del disco USB
- 16 teclas mecánicas y LCD de 2,4 pulgadas. Máximo
- de 2000 huellas dactilares y 1000 usuarios. Máximo
- de 100.000 registros de asistencia.
- 24 grupos de turno.
- 20 departamentos.

Advertencia:

Utilice un adaptador DC 5V 1A, y la temperatura de trabajo no puede exceder -5°C~+55°C.

2 Instalación del dispositivo

2.1 Lista de Verificación

No.	Nombre	Cantidad
1	Unidad	1
2	Adaptador de corriente	1
3	Línea eléctrica	1
4	Tornillo	- Bolsa de tornillos * 1 - Perno de expansión * 3
5	Guía de inicio rápido	1

Cuadro 2-1

2.2 Panel y Puerto

La apariencia del terminal de tiempo y asistencia se muestra en la Figura 2-1 y la Figura 2-2.

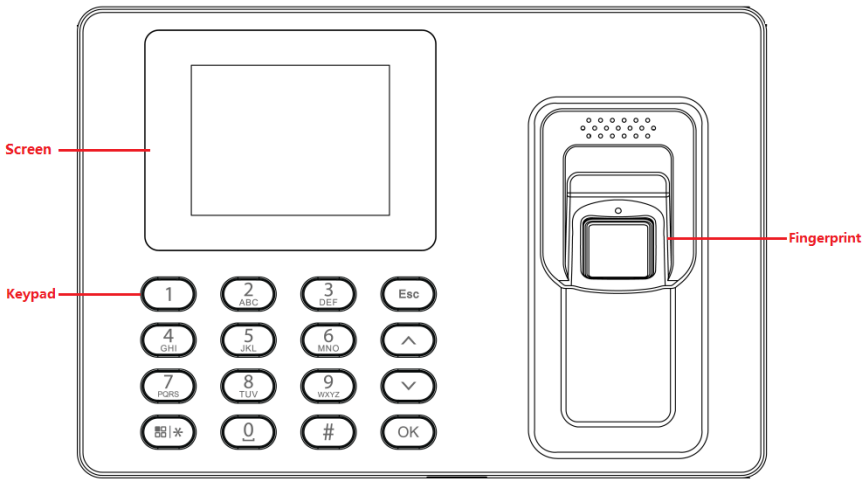


Figura 2-1

Icono	Nota
0～9	Tecla numérica para la entrada de números y letras
Esc	Atrás o salir
^	Arriba (interruptor de eventos de asistencia)
v	Abajo (interruptor de eventos de asistencia)
OK	Ingresa o confirma
#	Retroceso
	Ingrese al menú principal o cambie la entrada

Gráfico 2-2

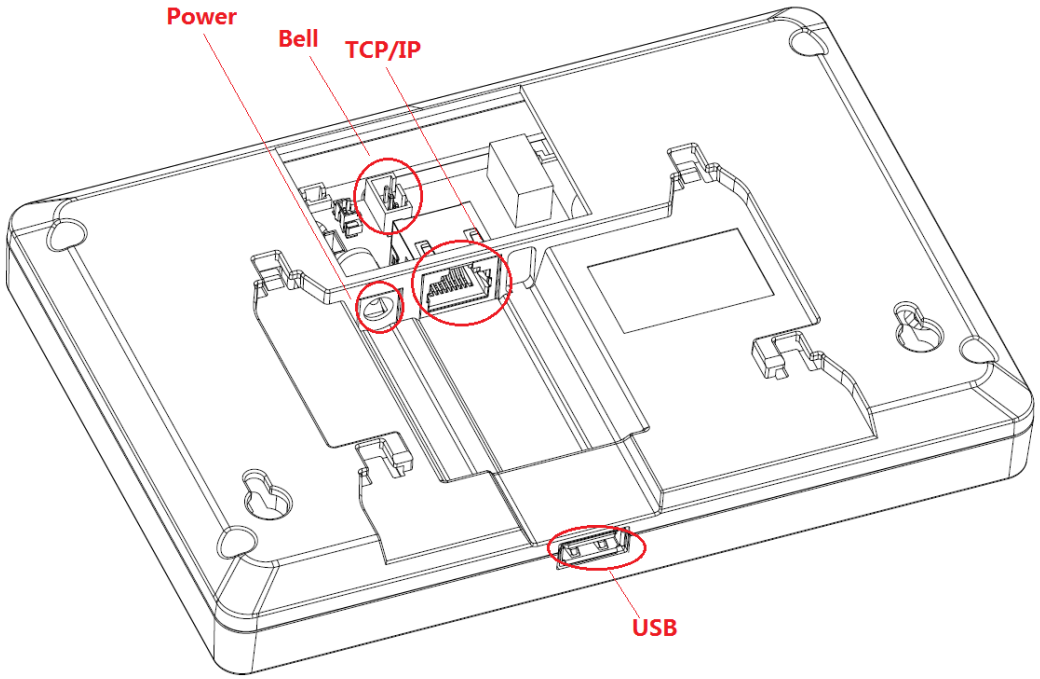


Figura 2-2

Pasos de conexión de campana:

Paso 1: Retire 4 tornillos con un destornillador y luego desmonte el dispositivo. Paso 2: conecte los 3 pines para la campana electrónica

Paso 3: cubre el panel trasero y monta el dispositivo

2.3 Dimensiones

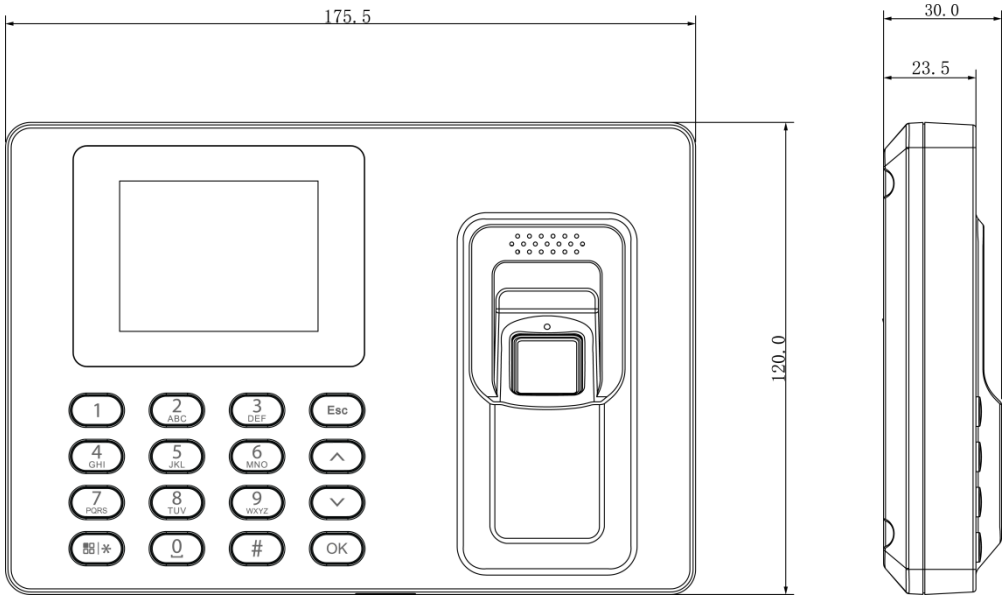


Figura 2-3

2.4 Instalación

La instalación de tiempo de asistencia se muestra en la Figura 2-4.

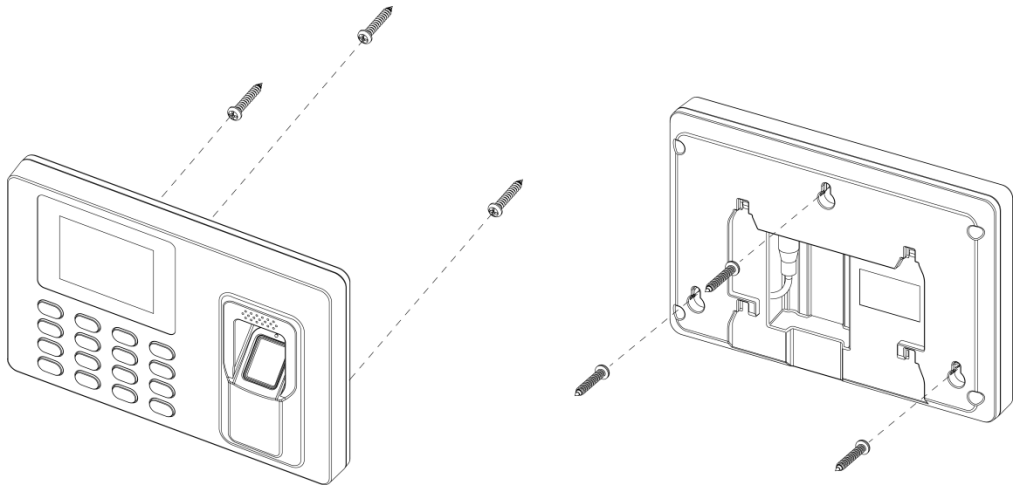


Figura 2-4

Pasos de instalación:

Paso 1. Pegue el mapa de instalación en la superficie que va a instalar y excave un agujero de acuerdo con la posición del agujero en el mapa. Inserte el perno de expansión en el orificio de instalación. Paso 2. Fije el tornillo en la pared de acuerdo con el mapa, deje un espacio de 2 mm ~ 2,5 mm entre tornillo y pared.

Paso 3. Enchufe el enchufe de alimentación, coloque el cable en orden en sus áreas

Paso 4. correspondientes. Cuelgue el dispositivo en el tornillo.

3 Marco del sistema

3.1 Aviso

- Para la función de administrador: cuando el dispositivo no tiene funciones de administrador, todos pueden ingresar al menú del sistema. Cuando hay uno o más roles de administrador en el sistema, el menú se bloqueará y solo el administrador puede ingresar al menú con huella digital o contraseña. Por lo tanto, asegúrese de que haya 1 o varios usuarios administradores en el dispositivo.

  Usuario - Agregar Nuevo Usuario-Nivel de Usuario -Administrador, este usuario es usuario administrador.

- Para la regla de tiempo de asistencia: el departamento de programación de turnos en el equipo es independiente, es para el modo independiente, no tiene ninguna conexión con el modo de plataforma, las reglas de asistencia y otras configuraciones de la plataforma de software, y no realiza un procesamiento síncrono.

- Para el modo de plataforma, el nombre de usuario es admin, la contraseña predeterminada también es admin

- Para el modo independiente, el marco del sistema se muestra en la Figura 3-1.

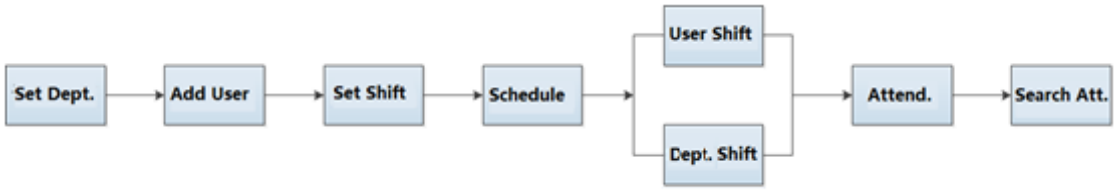


Figura 3-1

3.2 Menú principal

Hacer clic  , el sistema muestra el menú principal, consulte la Figura 3-2.

Nota:

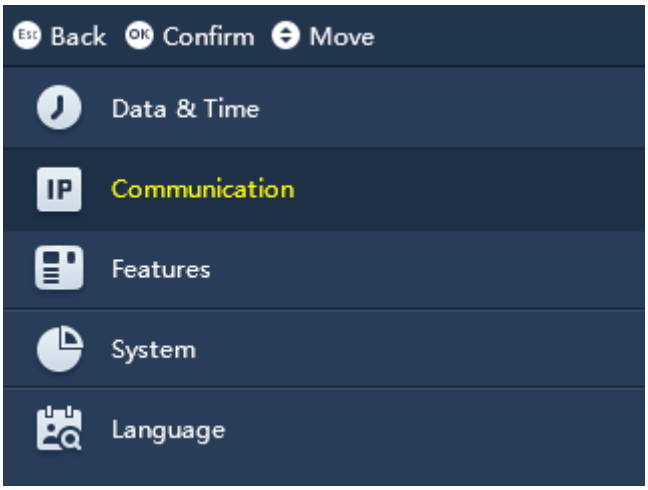
Si ha agregado un usuario administrador, puede ingresar la ID y la contraseña del usuario administrador o la huella digital para iniciar sesión.

Figura 3-2

Prensa o para seleccionar, haga clic o haga clic directamente en la tecla numérica para ingresar cada función.

3.3 Establecer dirección IP

La configuración de comunicación incluye la dirección IP, la máscara y la puerta de enlace



3.4 Establecer departamento

El sistema ya tiene 16 departamentos, y puede nombrar estos departamentos. Después de nombrar el departamento, el nuevo nombre se mostrará en el parámetro Departamento creado por el nuevo usuario. En su lugar, no se mostrará el departamento sin nombre.

Seleccione Administración de usuarios>Editar y eliminar departamento, haga clic en OK. Aquí puedes enlazar ID de departamento a nombre de departamento, vea la Figura 3-3.

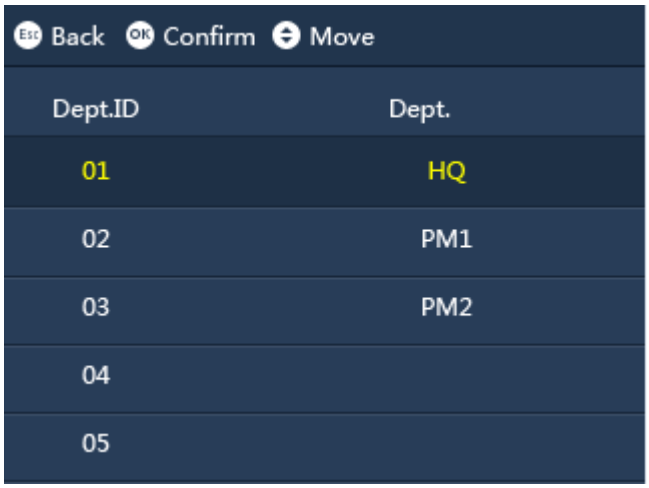


Figura 3-3

3.5 Agregar usuario

Puede agregar un nuevo usuario, así como registrar la información del nuevo usuario, incluida la identificación, el nombre, la huella digital, la contraseña, etc. Un usuario puede registrarse para asistir con la huella digital y la contraseña. El sistema admite hasta 1000 usuarios y 5 usuarios administradores. Por favor, no olvide configurar el usuario administrador. Una vez que el dispositivo sea administrador, el menú se bloqueará y solo los administradores tendrán acceso privilegiado al menú.

Seleccione Usuario>Agregar nuevo usuario, haga clic en OK. Ver

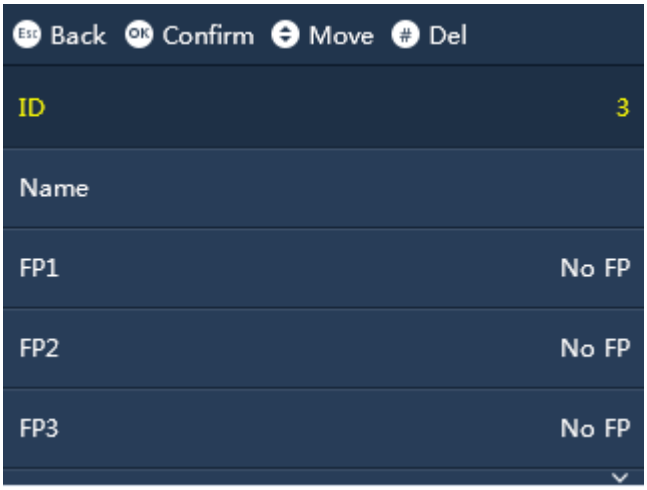


Figura 3-4

Figura 3-5

Nota:

- ID de usuario máximo es de 8 dígitos. El nombre de
- usuario tiene un máximo de 16 dígitos.
- La contraseña de entrada puede ser de 1 a 8 dígitos de número.

3.6 Cambio

El sistema admite 24 turnos. Cada turno puede establecer dos períodos y un turno de horas extras.

Seleccione Turno>Configuración de turno>Turno, haga clic en OK.

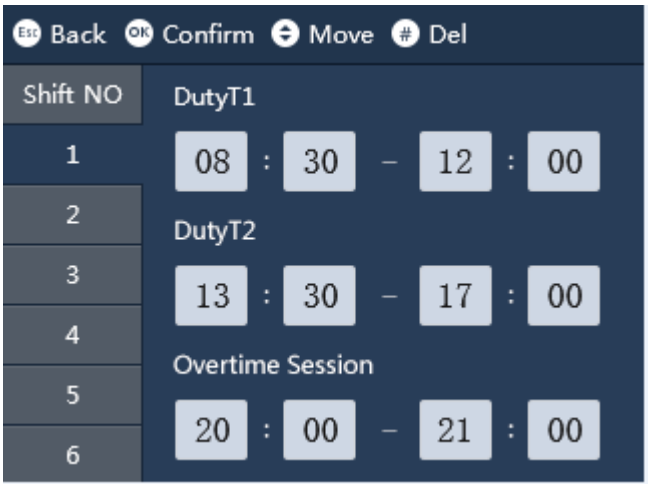


Figura 3-6

Parámetro	Descripción
Servicio T1, Servicio T2	Establecer el período de asistencia, ya que debe cumplirse el período entre el inicio y la salida este período para ser asistencia normal. De lo contrario es asistencia anormal. El sistema admite dos periodos. Si establece dos períodos, el período 1 y 2 deben ser de asistencia normal, por lo que el usuario será de asistencia normal.
Sesión de tiempo extra	Establezca una sesión de trabajo de horas extras, ya que el inicio y la salida dentro de este período serán horas extra de trabajo.

Gráfico 3-1

3.7 Calendario

El sistema admite el horario del usuario y el horario del departamento. Puede configurar según su necesidad.

3.7.1 Horario de usuario

Puede configurar el calendario del mes actual y del próximo mes para un usuario.

Paso 1. Seleccione Turno>Configuración de horario>Horario de usuario, haga clic en OK.

Paso 2. Ingrese el número de usuario, para mostrar automáticamente el nombre y el departamento, haga clic en OK, ver Figura 3-7.

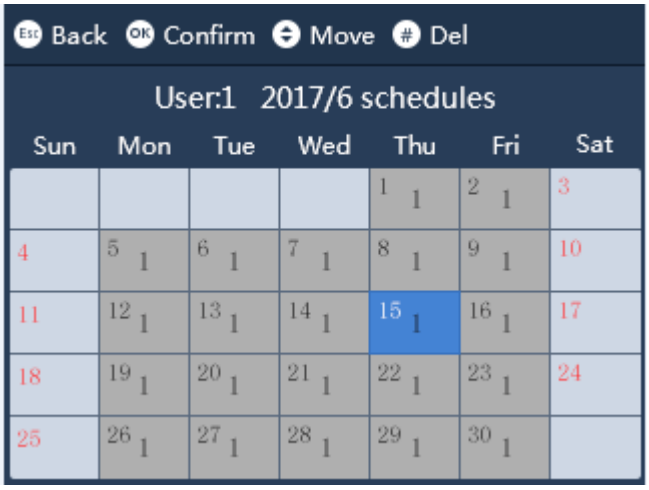


Figura 3-7

- 1-24 significa cambio en la
- configuración. Null y 0 están fuera de
- servicio. 25 significa viaje de
- negocios. 26 significa salir.

3.7.2 Horario del departamento

Seleccione Departamento, configure el método de turno de ciclo para el departamento correspondiente.

Paso 1. Seleccione Turno>Configuración de horario>Horario de departamento, haga clic en OK.

Paso 2. Haga clic en conjunto de departamentos, haga clic en OK, consulte la Figura 3-8.

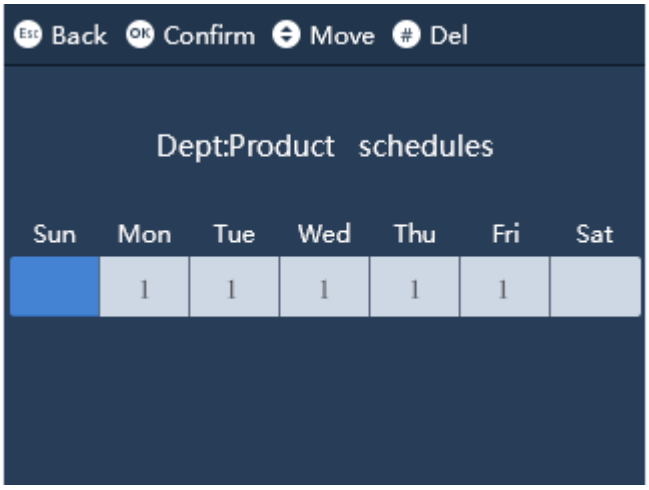


Figura 3-8

- 1-24 significa cambio en la
- configuración. Null y 0 están fuera de
- servicio. 25 significa viaje de
- negocios. 26 significa salir.

3.8 Asistencia

En la interfaz de espera, puede registrarse para asistir mediante huella digital o contraseña.

-Asistencia de huellas dactilares

En el área de huellas dactilares, presione su dedo sobre él.

-Asistencia con contraseña

Haga clic en la tecla numérica, para ingresar la ID de usuario, haga clic en OK e ingrese la contraseña. Hacer clic OK otra vez completar.

3.9 Estadísticas de Asistencia

Advertencia

Antes de exportar el registro de asistencia, asegúrese de insertar un disco USB. Durante la exportación, no expulse el disco USB ni opere el sistema, de lo contrario, la exportación fallará y provocará un mal funcionamiento del sistema.

Puede buscar y exportar registro de asistencia, mientras que el sistema almacena hasta 100.000 registros.

Después de ingresar al menú principal, haga clic en  o  para seleccionar Estadísticas ATT, haga clic en  .

O puede hacer clic directamente en la tecla "2", consulte la Figura 3-9.

Cuando seleccione Exportar registro ATT mensual o Exportar informe ATT mensual, haga clic en  para exportar el registro.

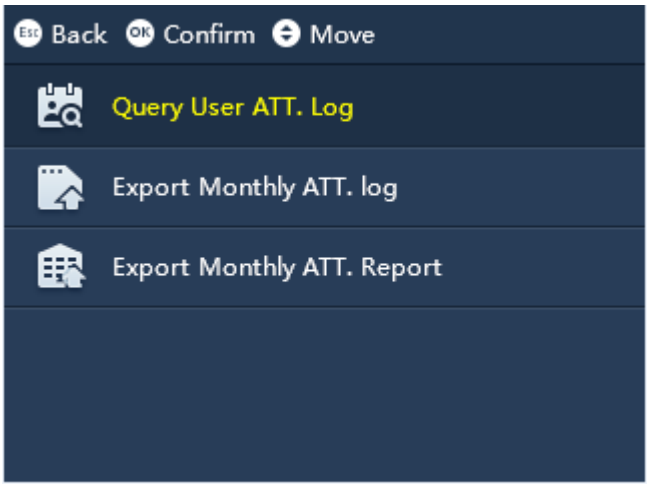


Figura 3-9

Nota:

- **Este manual es solo para referencia. Se puede encontrar una ligera diferencia en la interfaz de usuario.**
- **Todos los diseños y el software aquí están sujetos a cambios sin previo aviso por escrito.**
- **Todas las marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos dueños.**
- **Si hay alguna duda o controversia, consulte la explicación final de nosotros.**

- **Visite nuestro sitio web o comuníquese con un ingeniero de servicio local del usuario para obtener más información.**