

Terminal de tiempo y asistencia

Guía de inicio rápido

V1.0.0

Advertencias y medidas de seguridad importantes

Este capítulo describe el contenido que cubre el manejo adecuado del acceso independiente, la prevención de peligros y la prevención de daños a la propiedad. Lea estos contenidos detenidamente antes de utilizar el acceso de forma independiente, cúmplalos al utilizarlos y guárdelos para futuras consultas.

Requisito de operación

- No coloque ni instale el acceso de forma independiente en un lugar expuesto a la luz solar o cerca de una fuente de calor.
- Mantenga el acceso independiente alejado de la humedad, el polvo o el hollín.
- Mantenga el acceso independiente instalado horizontalmente en el lugar estable para evitar que se caiga.
- No deje caer ni salpique líquido sobre el acceso independiente, y asegúrese de que no haya ningún objeto lleno de líquido en el acceso independiente para evitar que el líquido fluya hacia el acceso independiente.
- Instale el acceso independiente en un lugar bien ventilado y no bloquee la ventilación del acceso independiente.
- Opere el acceso de forma independiente dentro del rango nominal de entrada y salida de energía. No desmonte el acceso de forma independiente.
- Transporte, utilice y almacene el acceso de forma independiente en las condiciones de humedad y temperatura permitidas.

Seguridad ELECTRICA


- El uso inadecuado de la batería puede provocar un incendio, una explosión o una inflamación. Al reemplazar la batería, asegúrese de utilizar el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.
- Utilice el adaptador de corriente proporcionado con el acceso independiente; de lo contrario, podría provocar lesiones personales y daños al dispositivo.
- La fuente de alimentación debe cumplir con los requisitos de la norma de seguridad de voltaje muy bajo (SELV) y suministrar energía con un voltaje nominal que cumpla con el requisito de fuente de alimentación limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de suministro de energía está sujeto a la etiqueta del dispositivo.
- Conecte el dispositivo (estructura tipo I) a la toma de corriente con toma de tierra de protección.
- El acoplador del aparato es un dispositivo de desconexión. Cuando utilice el acoplador, mantenga el ángulo para facilitar la operación.

General

Esta Guía de inicio rápido (en lo sucesivo denominada "Guía") presenta la instalación y el funcionamiento básico de Time & Attendance (Independiente) (en lo sucesivo denominado "autónomo").

Las instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con significado definido pueden aparecer en la Guía.

Palabras de advertencia	Sentido
	Proporciona información adicional como énfasis y complemento del texto.

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como rostro, huellas dactilares, número de matrícula del automóvil, dirección de correo electrónico, número de teléfono, GPS, etc. 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 al sujeto de los datos la existencia de un área de vigilancia y proporcionar información relacionada. contacto.

Sobre la guía

- La guía es solo para referencia. Si hay inconsistencia entre la Guía y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida ocasionada por las operaciones que no cumplan con la Guía. La Guía se actualizará 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 hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y la Guía. Póngase en contacto con el servicio de atención al cliente para obtener el programa más actualizado y la documentación complementaria. Todavía puede haber desviaciones en los datos técnicos, la descripción de funciones y operaciones, o errores en la impresión. Si 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 la Guía (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en la Guía son propiedad de sus respectivos propietarios.
- Visite nuestro sitio web, comuníquese con el proveedor o con 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.

Tabla de contenido

Advertencias y salvaguardias importantes	II Prólogo
.....	III 1 Resumen
.....	1
1.1 Introducción	1
1.2 Características	1
1.3 Apariencia	1
1.4 Dimensiones	3
2 Instalación	4
2.1 Métodos de instalación	4
2.2 Conexión de cable	5
3 Operación	6
3.1 Aviso	6
3.2 Menú principal	6
3.3 Configurar parámetros de red	7
3.4 Agregar usuarios	8
3.4.1 Agregar uno por uno	8
3.4.2 Agregar lotes	9
3.5 Turno	10
3.5.1 Configuración de turno	10
3.5.2 Configuración de horario	11
3.5.3 Entrada tardía / salida anticipada permitida	12
3.6 Asistencia	13
3.6.1 Automático / Manual	13
3.6.2 Fijo	13
3.6.3 Forzado	13
3.7 Estadísticas de asistencia	14
Apéndice 1 Recomendaciones de ciberseguridad	15

1.1 Introducción

El tiempo y asistencia (independiente) se puede utilizar para verificar la asistencia. La verificación de asistencia se puede completar a través de tres métodos: huella digital, contraseña y tarjeta.

1.2 Características

- La batería de reserva de alta capacidad funciona hasta 10 horas en el modo de espera. Puede conectarse a un dispositivo de control de acceso de terceros.
- Se puede registrar 1, 000 información de usuario (ID, nombre, huella digital, contraseña, número de tarjeta) en el tiempo y asistencia (independiente).
- Almacena hasta 100, 000 informes de registros de asistencia y 10, 000 registros de gestión. Todos los usuarios pueden consultar sus propios registros de asistencia.
- Solo los administradores pueden agregar nuevos usuarios, editar la información de los usuarios, consultar, importar o exportar registros de asistencia e informes de asistencia.
- Firmware de actualización de disco USB.
- Entrada de texto T9.
- 24 grupos de turno. 20 departamentos.

1.3 Apariencia

Figura 1-1 Apariencia



Tabla 1-1 Descripción de la clave

Icono	Descripción
0-9	Teclas numéricas para ingresar números y letras.


Icono	Descripción
ESC / F1	<ul style="list-style-type: none"> Presione la tecla para salir o ir al menú anterior. En la interfaz de espera, presione el botón para registrarse.
Λ / F2	<ul style="list-style-type: none"> En el modo de espera, presione la tecla, se mostrará BREAK OUT en la pantalla. Arriba (tecla de dirección; interruptor de tipo de asistencia).
v / F3	<ul style="list-style-type: none"> En el modo de espera, presione la tecla, BREAK IN se mostrará en la pantalla. Abajo (tecla de dirección; interruptor de tipo de asistencia). Entrar o
Aceptar / F4	<ul style="list-style-type: none"> confirmar. En la interfaz de espera, presione la tecla para pagar.
#	Eliminar tecla o tecla de método abreviado para revisar registros.
	<ul style="list-style-type: none"> Cuando el terminal está apagado / encendido, presione la tecla para encender / apagar el terminal (presione la tecla durante más de tres segundos para apagar el terminal). En el modo de espera, presione la tecla, y luego los administradores pueden ir al menú principal mediante huellas digitales, contraseñas o tarjetas. Cuando necesite ingresar texto, presione la tecla y luego podrá cambiar los tipos de ingreso de texto (números, letras y puntuación).

Figura 1-2 Panel trasero

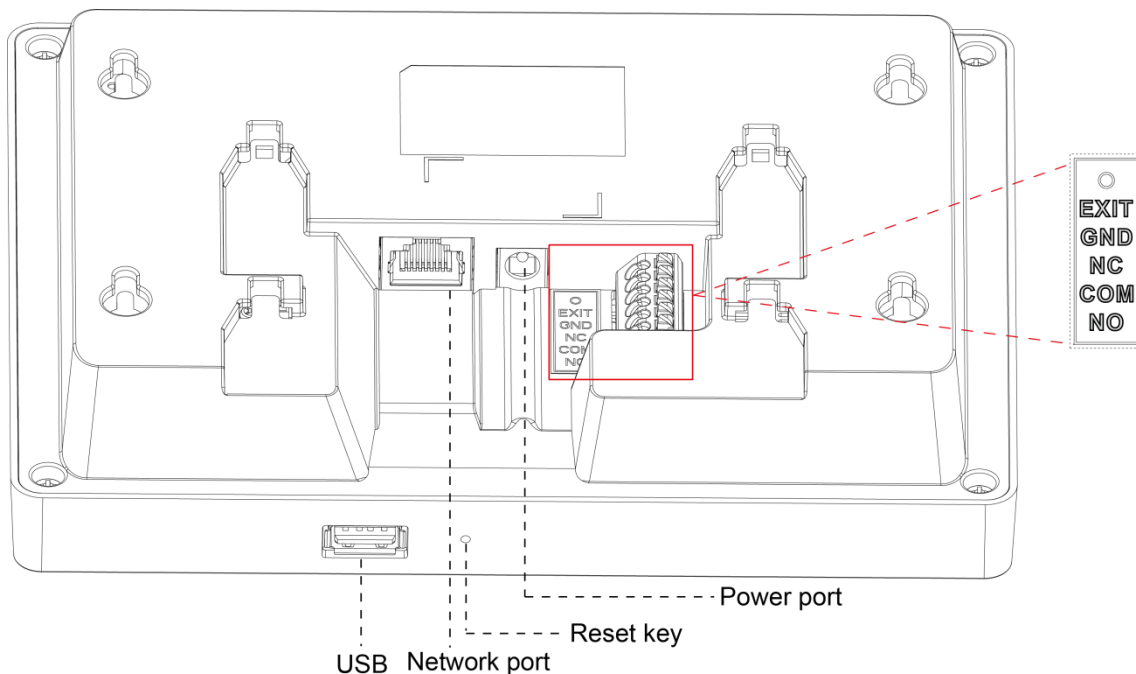


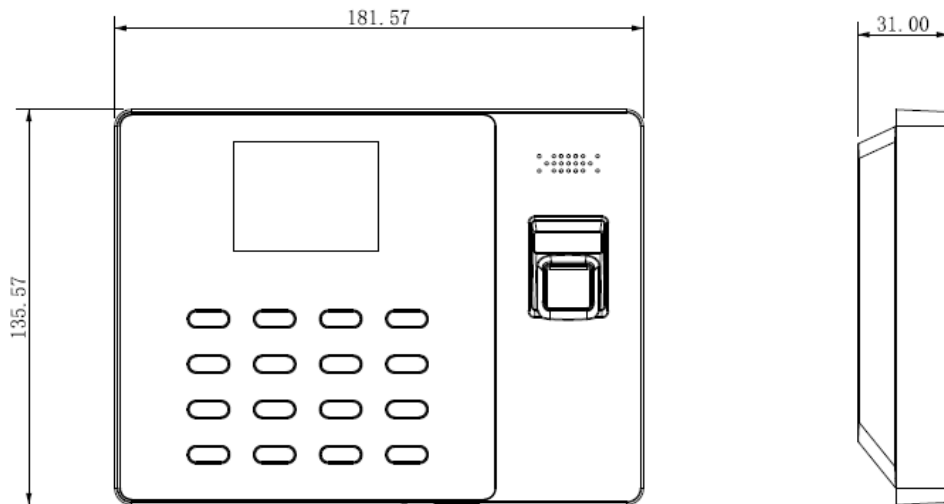
Tabla 1-2 Descripción del puerto

Puerto	Descripción
SALIDA	Conectado al botón de salida de la puerta.
GND	Conectado a la línea de tierra. Hace que el relé esté
CAROLINA DEL NORO	Normalmente cerrado.

Puerto	Descripción
COM	Puerto COM.
NO	Activa el relé normalmente.

1.4 Dimensiones

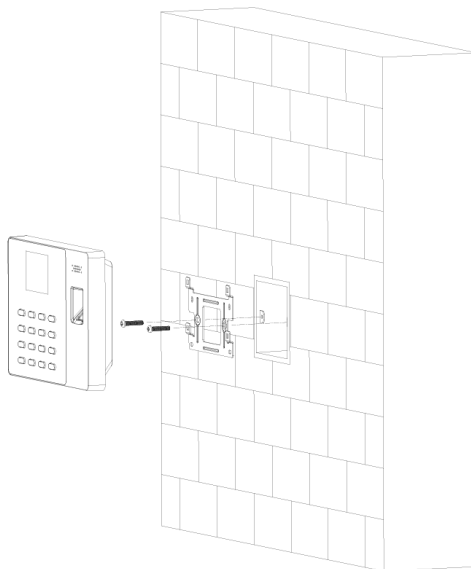
Figura 1-3 Dimensiones (mm)



2.1 Métodos de instalación

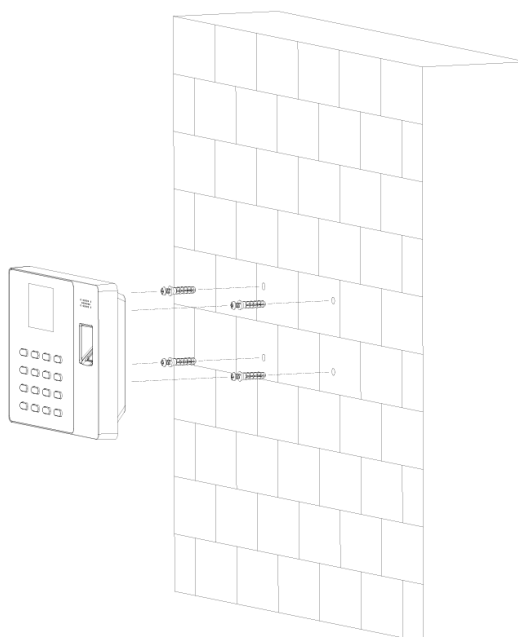
Instalado a través de caja eléctrica 86

Figura 2-1 Instalado a través de la caja eléctrica 86



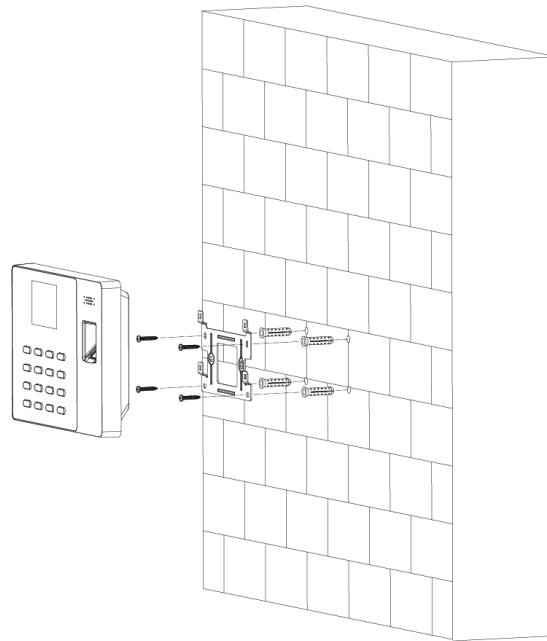
Instalado directamente en la pared

Figura 2-2 Instalado directamente en la pared



Instalado a través del soporte

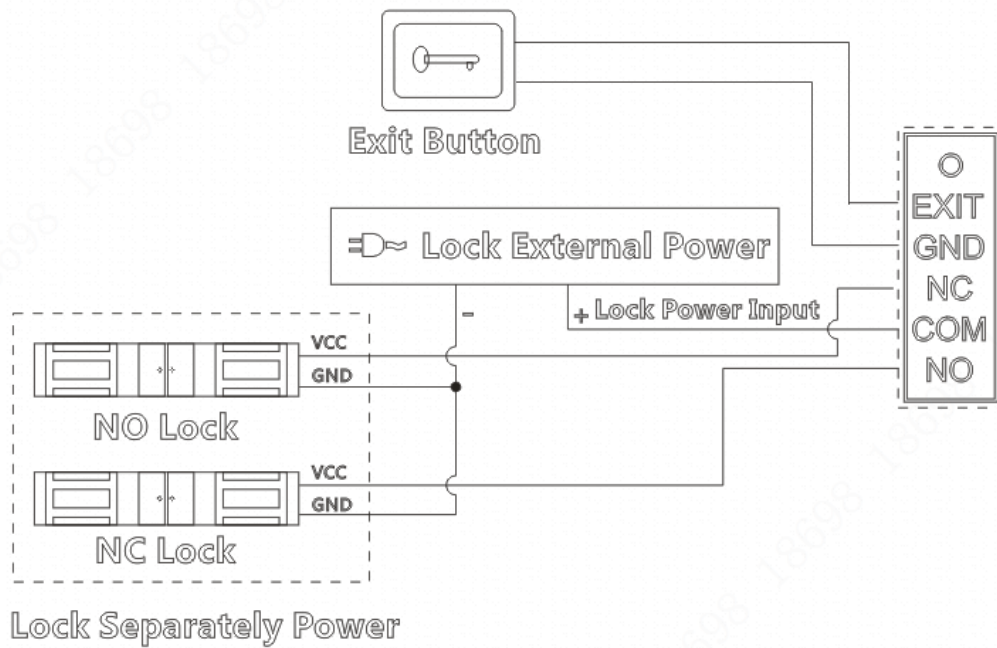
Figura 2-3 Instalado a través del soporte



2.2 Conexión de cable

El terminal se puede conectar al botón de salida para controlar la puerta. Vea la Figura 2-4.

Figura 2-4 Conexión de cables



3.1 Aviso


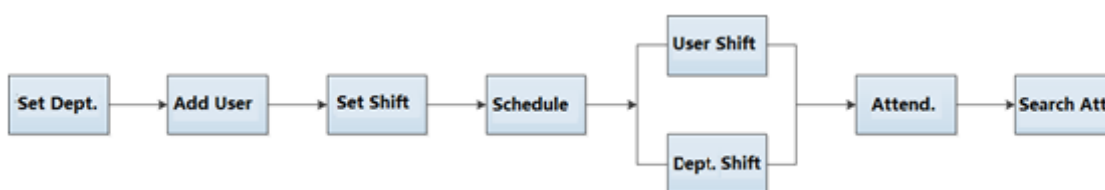
- Cuando el terminal está conectado a la fuente de alimentación, debe presionar  girar encendido.
- Antes de que se cree un administrador, cualquiera puede ingresar al menú principal y realizar la configuración del terminal. Por el bien de la seguridad de la información, primero debe crear administradores (seleccione **1 Usuario > Agregar nuevo usuario**, y luego seleccione una ID de usuario. Seleccione **Nivel de usuario**, presiona **Aceptar / F4** y entonces **^ / F2** o **v / F3** para seleccionar **Administrador**).
- Cuando necesite conectar el terminal a SmartPSS (la plataforma de administración), la ID predeterminada es "admin" y la contraseña predeterminada también es "admin".
- Las configuraciones sobre turnos, horarios y departamentos en la terminal son independientes de las de SmartPSS.
- Para el marco del sistema independiente, consulte la Figura 3-1.

Figura 3-1

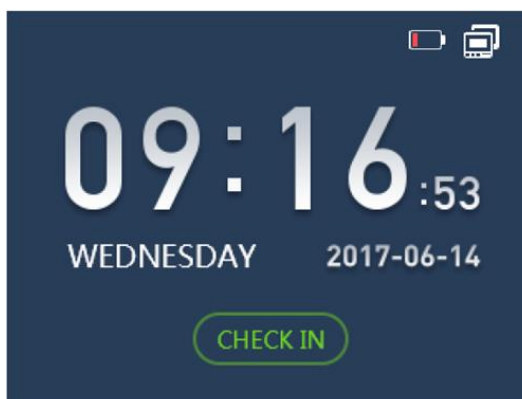


3.2 Menú principal




Modo de espera

Antes de ingresar a la página principal, se muestra la siguiente interfaz. Vea la Figura 3-2.

Figura 3-2 Interfaz de espera





- Antes de que se creen administradores, cualquiera puede ingresar al menú principal y realizar configuraciones. Una vez que se crean los administradores, solo los administradores pueden ingresar al menú principal.
-  indica que la red está desconectada.
-  indica que la red está conectada.
-  indica el nivel de la batería y la condición de conexión a la red. Cuando enciendes el terminal encendido por primera vez, el nivel de la batería es del 25% (puede durar aproximadamente una hora). A medida que pasa el tiempo, la vida útil de la batería se reduce.

Menú principal







presiona   , y luego se mostrará el menú principal. Vea la Figura 3-3.

Figura 3-3 Menú principal



- Una vez que haya creado administradores, debe presionar    primero, y luego tu puede ir al menú principal mediante los siguientes métodos:
 - Presione la punta de su dedo en el sensor de huellas digitales;
 - Ingrese el ID de usuario y la contraseña del administrador;
 - Pase su tarjeta por el lector de tarjetas.
- Puede seleccionar el icono mediante los dos métodos siguientes:
 - presiona **Λ / F2** o **V / F3**;
 - Presione las teclas numéricas.

3.3 Configurar parámetros de red

En el menú principal, seleccione **5 Característica> Comunicación**, y luego puede configurar la dirección IP, la máscara, la puerta de enlace, el MAC y el puerto. Vea la Figura 3-4.

Figura 3-4 Comunicación

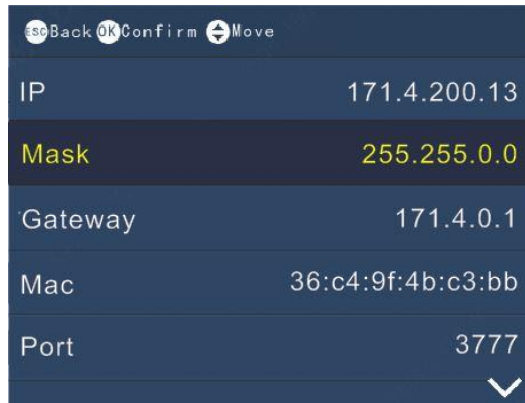


Tabla 3-1 Descripción de la interfaz de espera

Parámetro	Descripción
IP	Valor predeterminado 192.168.1.108, puede configurarlo según sus necesidades. Valor predeterminado
Máscara	255.255.255.0, puede configurarlo según sus necesidades. Valor predeterminado 192.168.1.1, puede
Puerta	configurarlo según sus necesidades.
MAC	Dirección MAC del terminal y no se puede modificar. Número de puerto, utilizado
Puerto	para iniciar sesión en el terminal en SmartPSS.

3.4 Agregar usuarios

Puede agregar usuarios uno por uno o puede agregar usuarios en lotes.

3.4.1 Agregar uno por uno

Paso 1 En el menú principal, seleccione **1 Usuario > Agregar nuevo usuario**. Vea la Figura 3-5 y la Figura 3-6.

Figura 3-5 Agregar nuevo usuario (1)

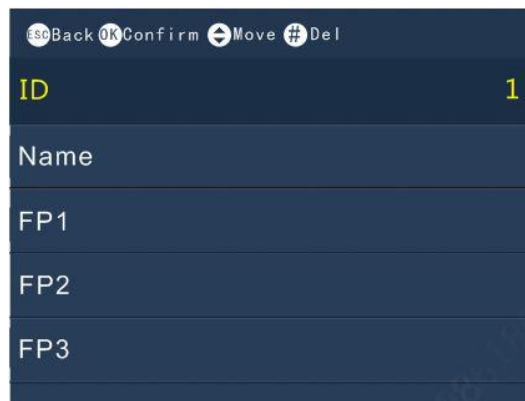
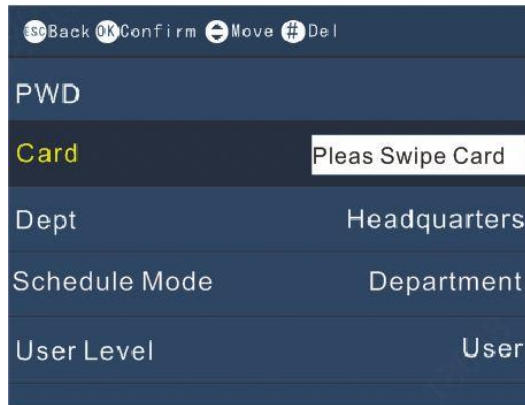


Figura 3-6 Agregar nuevo usuario (2)



Paso 2 Realice las siguientes operaciones:

- 1) Ingrese el ID de usuario y el nombre;
- 2) Registrar las huellas dactilares del usuario;
- 3) Permitir que los usuarios establezcan una contraseña;
- 4) Registrar una tarjeta para el nuevo usuario;
- 5) Seleccione un departamento;
- 6) Seleccione un modo de programación;
- 7) Seleccione un nivel de usuario. Se

agrega un nuevo usuario.



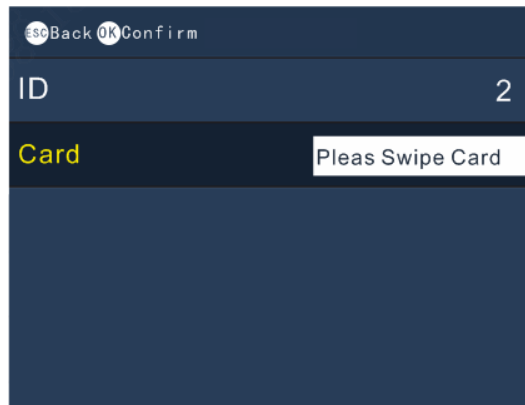
- La longitud máxima de la ID de usuario es de 8 dígitos (el rango de longitud de la ID de usuario puede ser 1-99999999).
- La longitud máxima del nombre de usuario es de 16 letras.
- Las contraseñas pueden ser números de 1 a 8 dígitos (el cero por sí solo no se puede establecer como contraseña y no puede ser el primer número de una contraseña).
- Se pueden registrar como máximo tres huellas dactilares para un usuario.

3.4.2 Agregar lotes

Agregar usuarios deslizando tarjetas

Seleccione **1 usuario > Agregar tarjetas en lote**. Pase las tarjetas por el lector de tarjetas y, a continuación, se guardará automáticamente la identificación de usuario y el número de tarjeta. Necesita editar nombres de usuario, agregar huellas digitales y contraseñas por separado. Vea la Figura 3-7.

Figura 3-7 Deslizar tarjetas para agregar usuarios



Agregar usuarios a través de USB

Puede exportar la información del usuario (incluyendo ID de usuario, nombre de usuario, contraseña, número de tarjeta, departamento, nivel de usuario y modo de programación) de un terminal a otro terminal. La información exportada se almacenará en un gráfico de Excel. Puede editar información en el gráfico. Cuando se importa a otros terminales, la información de usuario con la misma ID de usuario se sobrescribirá.

Paso 1 En el menú principal, seleccione **4 USB> Importar información de usuario**.

El aviso **La nueva información cubrirá la anterior** será mostrado.

Paso 2 Presione **Confirmar-Aceptar**.

Y luego se importará la información del usuario.



Cuando el espacio de almacenamiento del USB es inferior a 1 M, los archivos se pueden exportar pero pueden estar dañados.

3.5 Turno

Puede establecer períodos de turno. Hay 24 turnos en total.

3.5.1 Configuración de turno

En el menú principal, seleccione **3 Mayús> Configuración de turno> Mayús**. Puede configurar 24 turnos como máximo. Vea la Figura 3-8.

Figura 3-8 Configuración de cambio

Shift NO	DutyT1	DutyT2	Overtime Session
1	08 : 30 - 12 : 00		
2		DutyT2	
3		13 : 30 - 17 : 00	
4			Overtime Session
5			20 : 00 - 21 : 00
6			

Tabla 3-2 Descripción de la configuración de cambio

Deber	Descripción
Deber T1	Puede establecer la duración del tiempo de servicio en cada turno. Por ejemplo, de 08:30 a 12:00.
Servicio T2	Puede establecer la duración del tiempo de servicio en cada turno. Por ejemplo 13: 30-17: 00.
Tiempo extraordinario Sesión	Puede establecer la duración de las horas extraordinarias. Por ejemplo, de 20:00 a 21:00.



- Hay dos períodos en los que es posible que deba iniciar y cerrar sesión, porque hay un intervalo entre Duty T1 y Duty T2.
- Si inició sesión más de una vez, el sistema toma como efectivo los primeros registros de inicio de sesión; si se desconectó por más de una vez, el sistema solo toma como efectivos los últimos registros de cierre de sesión.
- En la sesión de horas extra, no hay una configuración de tiempo de salida tardía / temprana.

Turno de importación / exportación

Una vez que haya realizado los ajustes de cambio en un terminal, puede exportar los ajustes a través de unidades flash y luego importarlos a otros terminales, por lo que no es necesario realizar ajustes repetidamente.

3.5.2 Configuración de horario

En el menú principal, seleccione **3 Mayús> Configuración de programación**, y luego puede establecer un horario en cada mes (solo el mes actual y el mes siguiente) para los usuarios y establecer horarios en cada semana para los departamentos.

Horario de usuario

Paso 1 En el menú principal, seleccione **Mayús> Configuración de programación> Programación de usuario**.

Paso 2 Presione **Aceptar / F4**.

Paso 3 Introduzca la ID de usuario.

El nombre de usuario y el nombre del departamento se mostrarán automáticamente.

Paso 4 Presione **Aceptar / F4**.

Vea la Figura 3-9.

Figura 3-9 Programación del usuario

User:1 2017/6 schedules						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1 1	2 1	3
4	5 1	6 1	7 1	8 1	9 1	10
11	12 1	13 1	14 1	15 1	16 1	17
18	19 1	20 1	21 1	22 1	23 1	24
25	26 1	27 1	28 1	29 1	30 1	



- Los números en el centro de cada casilla son números de turno. Hay 24 turnos en total. Los números en la esquina superior izquierda de cada cuadro son días.
- Nulo y 0 significa fuera de servicio. 25
- significa viaje de negocios. 26 significa irse.

Horario del Departamento

Paso 1 En el menú principal, seleccione **Mayús> Configuración de programación> Departamento**.

Paso 2 Seleccione un departamento.

Paso 3 Presione **Aceptar / F4**.

Vea la Figura 3-10.

Figura 3-10 Programación del departamento

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	1	1	1	1	

Calendario de importación / exportación



- Antes de exportar o importar programas, asegúrese de que el USB esté insertado. Durante la exportación o la importación, no retire el USB ni utilice el terminal, de lo contrario, la exportación o la importación fallarán y se producirá un mal funcionamiento del sistema.
- Una vez que haya realizado los ajustes de programación en un terminal, puede exportar los ajustes a través de unidades flash y luego importarlos a otros terminales, por lo que no es necesario realizar ajustes repetidamente.

3.5.3 Entrada tardía / salida anticipada permitida

La entrada tardía permitida se utiliza para establecer horarios de trabajo flexibles. Por ejemplo, la hora de inicio de trabajo permitida es a las 8:30 y la hora de retraso es de 5 minutos, entonces si un usuario verifica su asistencia antes de las 8:35, no se considera que llegue tarde.

La salida anticipada permitida también se usa para establecer horarios de trabajo flexibles. Por ejemplo, el tiempo de trabajo final permitido es a las 17:30 y el tiempo de salida anticipada es de 5 minutos, entonces si un usuario verifica su asistencia después de las 17:25, no se considera que se haya ido temprano.



- Durante el período de Duty 1 y Duty 2, solo tiene una oportunidad de verificar su asistencia tarde y una oportunidad de irse temprano.
- Si llega tarde o se va temprano dentro del período de tiempo permitido, las horas extra se seguirán contando.

3.6 Asistencia

Hay tres modos de verificación de asistencia: automático / manual. Fijo y Forzado; y tres métodos de verificación de asistencia: huella digital, contraseña y tarjeta.

3.6.1 Automático / Manual

En **Manual de auto** modo, hay tres métodos:

- Puede verificar su asistencia directamente presionando el dedo en el sensor de huellas digitales, ingresando su ID de usuario y contraseña, o deslizando su tarjeta;



Necesita hacer ajustes de turno por adelantado en **3 Mayús> Configuración de turno> Mayús**. Consulte "3.5.1 Configuración de turno".

- Puede seleccionar un evento de asistencia presionando **Esc / F1**, **Λ / F2**, **V / F3**, y **Aceptar / F4**, y luego verifique la asistencia de huellas dactilares, contraseña o tarjeta;
- Puede registrar su asistencia sin configurar los turnos y sin seleccionar eventos de asistencia.

3.6.2 Fijo

En el modo fijo, puede seleccionar un evento de asistencia fija para una terminal, y luego los usuarios pueden iniciar sesión en una terminal y cerrar sesión en otra terminal.

Paso 1 En la interfaz de espera, seleccione **5 Función> Funciones> Att. Modo de evento**.

Paso 2 Presione **Aceptar / F4**.

Aparece el cuadro de texto blanco. prensa **Λ / F2** o **V / F3** para

Paso 3 seleccionar Fijo. prensa **Aceptar / F4**.

Paso 4

Paso 5 prensa **V / F3**.

Paso 6 prensa **Aceptar / F4**.

Aparece el cuadro de texto blanco. prensa **Λ / F2** o **V / F3** para seleccionar entre Check in, Break out, Break in, Check out,

Paso 7 OT-In y OT-Out.

3.6.3 Forzado

En el modo Forzado, debe seleccionar su tipo de asistencia (1.Registrarse; 2.Break out; 3.Break in; 4.Check out; 5.OT-In; 6.OT-Out) después de presionar el dedo punta en el sensor de huellas digitales, ingrese su ID de usuario y contraseña, o deslice su tarjeta.

Paso 1 En la interfaz de espera, seleccione **5 Función> Funciones> Att. Modo de evento**.

Paso 2 Presione **Aceptar / F4**.

Aparece el cuadro de texto blanco.

Paso 3 Presione **Λ / F2** o **v / F3** para seleccionar Forzado.

Paso 4 Presione **Aceptar / F4**.



prensa **Λ / F2** o **v / F3** continuamente, **ESCAPE, CHECK IN, OT-OUT, OT-IN, VERIFICACIÓN, INGRESO** se mostrará a su vez. Hay teclas de acceso directo para el check-in, check-out, robo y fuga.

- **Esc / F1**: prensa **Esc / F1, REGISTRO** aparecerá en la pantalla y luego podrá registrarse mediante huella digital, contraseña o tarjeta.
- **Λ / F2**: prensa **Λ / F2, ESCAPAR** se mostrará en la pantalla, y luego podrá realizar una asistencia cuando necesite salir durante el horario de trabajo mediante huella digital, contraseña o tarjeta.
- **v / F3**: prensa **v / F3, INGRESO** aparecerá en la pantalla, y luego podrás realizar una asistencia cuando regreses a la empresa durante el horario de trabajo mediante huella digital, contraseña o tarjeta.
- **Aceptar / F4**: prensa **OK / F4, COMPROBAR** se mostrará en la pantalla, y luego podrá realizar el pago mediante huella digital, contraseña o tarjeta.
- **OT-IN**: puede hacer un registro de asistencia antes de tener que trabajar horas extras.
- **OT-OUT**: Puede hacer un registro de asistencia después de haber trabajado horas extra.

3.7 Estadísticas de asistencia



Antes de exportar el registro de asistencia, asegúrese de que el USB esté insertado. Durante la exportación, no retire el USB ni utilice la unidad independiente, de lo contrario, la exportación fallará y se producirá un mal funcionamiento del sistema.

Puede consultar y exportar el registro de asistencia.

En el menú principal, seleccione **2 Datos > Exportar ATT mensual. log / Exportar ATT mensual. Reporte**, prensa **Aceptar / F4**, seleccione un mes y luego presione **Aceptar / F4** para exportar registros e informes.

Apéndice 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 de Dahua sobre cómo crear un sistema de seguridad más seguro.

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

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software cliente a tiempo

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

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

1. Protección física

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

2. Cambie las contraseñas con regularidad

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

3. Establecer y actualizar contraseñas Restablecer información a tiempo

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Habilitar lista blanca

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

8. Enlace de dirección MAC

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

9. Asignar cuentas y privilegios de forma razonable

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

10. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

11. Transmisión encriptada de audio y video

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

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

12. Auditoría segura

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

13. Registro de red

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

14. Construya un entorno de red seguro

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

- Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde una red externa.

- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere 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.