

Módulo de PC de operaciones

Manual de usuario



Prefacio

General

Este manual presenta la instalación, funciones y operaciones del dispositivo (en adelante, "el Dispositivo"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	enero 2024

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como su rostro, audio, 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 proporcionar la información de contacto requerida.

Acerca del Manual

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.

- No somos responsables de las pérdidas incurridas 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 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 sólo para referencia. Es posible que se encuentren 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. Las actualizaciones de productos pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Pueden existir 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 otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con 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 dar una explicación final.

Salvaguardias y advertencias importantes

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

Requisitos de transporte



Transporte el equipo dentro del rango de humedad permitido ($\leq 95\%$ RH) y temperatura (-10°C a $+50^{\circ}\text{C}$).

Requisitos de almacenamiento



Guarde el equipo dentro del rango de humedad permitido ($\leq 95\%$ RH) y temperatura (-10°C a $+50^{\circ}\text{C}$).

Requerimientos de instalación



ADVERTENCIA

- Para evitar descargas eléctricas al cuerpo humano o daños al producto, apague la fuente de alimentación de CA antes de conectar dispositivos (no plug and play) cada vez.
- Evite utilizar este producto en ambientes con temperaturas altas o bajas (temperatura de funcionamiento: -10 a 50 grados centígrados; humedad: 10% a 95% ; temperatura de almacenamiento: -20 a 70 grados Celsius). No someta el producto a fuertes impactos o vibraciones, ya que puede provocar un mal funcionamiento o daños en el equipo.
- Al mover el producto, asegúrese de desconectar la fuente de alimentación de CA.



No instale el dispositivo en un lugar húmedo.

Requisitos de mantenimiento



ADVERTENCIA

- No utilice un paño húmedo para limpiar su computadora para evitar que el líquido gotee dentro de la computadora y provoque quemaduras.
- Para evitar daños innecesarios al producto causados por encendidos y apagados frecuentes, espere al menos 30 segundos antes de encender la máquina.



No desmonte el equipo al azar. Debe estar presente personal profesional para el mantenimiento y la instalación.

Tabla de contenido

Prefacio..... I **Medidas de seguridad y advertencias importantes..... III** **1**

Resumir 1

2 Introducción del producto 2

 2.1 Configuración del producto 2

 2.2 Interfaz E/S..... 3

Appendix 1 Recomendaciones de ciberseguridad 4

1 resumir

Gracias por elegir nuestros productos.

Antes de utilizar su producto, asegúrese de que su embalaje esté completo, si ha sufrido daños o encuentra algún faltante, comuníquese con su agencia lo antes posible.

- OPS × 1
- Manual del producto × 1
- Tornillo ATN × 2
- Antena Wi-Fi × 2

2 Introducción del producto

2.1 Configuración del producto

UPC	- Procesador móvil Intel® Tiger Lake
Gráficos	- Gráficos Intel® Iris® Xe
Almacenamiento	- 1 x tamaño M.2 2280 para SSD NVMe/SATA - 1 interfaz SATA de 2,5"
Memoria	- 2 x SO-DIMM DDR4 3200 MHz, máx. 32 GB
Audio	- Circuito integrado de audio Realtek ALC897 HD
Interfaz E/S frontal	- 1 HDMI1.4 - 2 x USB3.1, 1 x USB2.0, 1 x Tipo-C (USB3.1) - 1 conector RJ45 - 1 conector dos en uno de salida de línea y entrada de micrófono - 2 x Wi-Fi/BT ANT - 1 botón de encendido - 1 botón de reinicio
Interfaz IO trasera	- 1 x 80 pines: 1 x salida HDMI 2.0, 1 x USB3.0, 2 x USB2.0, TTL - 1 conector de entrada CC de 2,5/5,5
Inalámbrico	- 1 módulo WIFI/BT M.2 2230
Red	-Realtek Gigabit Ethernet
Perro guardián	- Apoyo
Entrada de alimentación	- ENTRADA DE 12-19 VCC
Ambiental requisito	- Temperatura de trabajo/temperatura de almacenamiento: -5 ~ 45°C/-20 ~ 70°C - Humedad de trabajo/no trabajo: 10% ~ 90% sin condensación / 5% ~ 95% sin condensación
SO	- Compatible con Windows10/Windows11/Linux
Dimensiones	- 119x180x30mm

2.2 Interfaz E/S

Interfaz E/S frontal



Interfaz IO trasera



- WIFI-1/2: Antena WIFI/BT
- BOTÓN DE ENCENDIDO: Botón del interruptor de encendido
- Conector LINE_OUT&MIC-IN dos en uno: interfaz de salida de audio con micrófono
- LED: indicador de disco duro (superior), indicador de alimentación (inferior)
- TYPE_C: puerto TYPE_C
- REINICIAR: Botón de reinicio
- Cerradura: Orificio antirrobo
- HDMI: interfaz de pantalla multimedia de alta definición
- USB3.1: puerto USB3.1
- LAN: interfaz de red RJ-45
- USB2.0: puerto USB2.0
- JAE 80PIN: puerto de extensión de 80 pines
- DC IN: interfaz de alimentación de CC

Appendix 1 Recomendaciones de ciberseguridad

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres.
- Incluya al menos dos tipos de personajes; Los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No incluya el nombre de la cuenta 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 cliente a tiempo

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

Recomendaciones "es bueno tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

Le sugerimos que realice protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales, e implemente permisos de control de acceso y administración de claves bien hechos para evitar que personal no autorizado lleve a cabo contactos físicos, como daños en el hardware, conexión no autorizada de un dispositivo extraíble (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 que las adivinen o las descifren.

3. Establecer y actualizar contraseñas Restablecer información oportuna

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

4. Habilite el bloqueo de cuenta

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

5. Cambie HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie 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. Habilite HTTPS

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

7. Vinculación de direcciones MAC

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

el riesgo de suplantación de ARP.

8. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable 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 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 cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión cifrada de audio y vídeo

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión cifrada 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 la transmisión.

11. Auditoría segura

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

12. Registro de red

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante un período prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

13. Construya un entorno de red seguro

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe dividirse y aislarse según las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts permitidos para acceder al dispositivo.