

MyEye

Video Recorder 4

Grabación de vídeo inteligente de hasta 4 cámaras

ES - Instrucciones y advertencias para la instalación y el uso

Nice

1 - INTRODUCCION	3
1.1 - Generalidades	3
1.2 - Instrucciones de seguridad	3
1.3 - Aviso de privacidad	3
1.4 - Acerca de esta guía	3
2 - PELIGROS Y ADVERTENCIAS IMPORTANTES	4
2.1 - Seguridad eléctrica	4
2.2 - Medio ambiente	4
2.3 - Operación y mantenimiento diario	4
3 - INSTALACION	5
3.1 - Dimensiones	5
3.2 - Instalación del disco duro	5
3.3 - Conexión	6
4 - CONFIGURACION	7
4.1 - Puesta en servicio	7
4.2 - Inicialización del aparato	7
4.3 - Configuración de la red	8
4.4 - Añadir cámaras IP	9
4.4.1- Inicializar cámaras IP	9
4.4.2 - Añadir cámaras IP por resultados de búsqueda	10
4.4.3 - Añadir cámaras IP manualmente	11
4.5 - Configurar el horario de almacenamiento de la grabación de vídeo	11
4.6 - Inicio de sesión en la interfaz web	13
5 - RECOMEDACIONES SOBRE CIBERSEGURIDAD	13
6 - INFORMACION ADICIONAL	14

1 INTRODUCCION

1.1 - Generalidades

Esta Guía de inicio rápido (en adelante, la "Guía") describe las funciones, la instalación y el funcionamiento del dispositivo.

1.2 - Instrucciones de seguridad

En la guía, puede ver palabras de advertencia categorizadas de tipos específicos.

Señales de advertencia	Significado
Advertencia	Indica un riesgo potencial medio o bajo que puede provocar lesiones leves o moderadas si no se evita.
Advertencia	Indica un riesgo potencial que puede provocar daños materiales, pérdida de datos, menor rendimiento o resultados impredecibles si no se evita.
Anotación	Proporciona información adicional como texto destacado y complementario.

1.3 - Aviso de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar información personal de otras personas, como rostros, huellas dactilares, números de registro de automóviles, direcciones de correo electrónico, números de teléfono, datos de GPS, etc. Debe cumplir con las leyes y regulaciones de privacidad locales para proteger los derechos legítimos e intereses de otros mediante la implementación de medidas que incluyen, entre otras: proporcionar una identificación clara y visible para informar al interesado de la existencia del área de monitoreo y garantizar el contacto adecuado.

1.4 - Acerca de esta guía

- La guía es solo para referencia. En caso de discrepancia entre la Guía y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por operaciones que no estén de acuerdo con la Guía.
- La guía se actualizará de acuerdo con las últimas leyes y reglamentos de las regiones relacionadas. Para obtener más información, escanee el código QR o visite nuestro sitio web oficial. En caso de discrepancia entre la Guía del Usuario 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 último programa y documentación adicional.
- Es posible que todavía existan desviaciones en las especificaciones, descripciones de funciones y operaciones, o errores tipográficos. En caso de dudas o disputas, consulte nuestra aclaración final actual.
- Todas las marcas comerciales, marcas registradas y nombres de compañías en la Guía son propiedad de sus respectivos dueños.
- Visite nuestro sitio web y comuníquese con su proveedor o servicio al cliente si experimenta algún problema al usar el dispositivo.
- En caso de dudas o situaciones controvertidas, consulte nuestra explicación final actual.

2 PELIGROS Y ADVERTENCIAS IMPORTANTES

2.1 - Seguridad eléctrica

- Todas las instalaciones y operaciones descritas en este documento deben cumplir con las normas locales de seguridad eléctrica.
- Utilice una fuente de alimentación SELV (voltaje muy bajo de seguridad) y una fuente de alimentación con un voltaje nominal que cumpla con los requisitos de fuente de alimentación restringida IEC60950-1. Consulte las etiquetas de los dispositivos para conocer los requisitos de alimentación específicos.
- Antes de iniciar el dispositivo, asegúrese de que el dispositivo de suministro de energía esté operativo.
- Tenga cuidado de no pisar ni pellizcar el cable de alimentación, especialmente el enchufe, la toma de corriente y el conector que sobresalen del aparato.

2.2 - Medio ambiente

- No exponga el dispositivo a una luz intensa y concentrada, como la luz de una lámpara o la luz del sol; de lo contrario, puede causar un brillo excesivo o puntos brillantes en la imagen, que no son un defecto del dispositivo y pueden afectar la vida útil de su CMOS (Semiconductor de óxido metálico complementario).
- No coloque el dispositivo en un ambiente húmedo o polvoriento, en temperaturas muy altas o bajas, en lugares con fuerte radiación electromagnética o iluminación inestable.
- Mantenga el dispositivo alejado de líquidos para evitar daños a los componentes internos.
- Proteja el interior del dispositivo de la lluvia o la humedad para evitar incendios o rayos.
- Mantenga una buena ventilación para evitar la acumulación de calor.
- Transporte, use y almacene el dispositivo dentro del rango de temperatura y humedad permitido.
- No se permiten fuertes esfuerzos, vibraciones violentas o salpicaduras de agua durante el transporte, almacenamiento e instalación.
- Embale el dispositivo en un embalaje estándar de fábrica o material equivalente para el transporte.
- Instale el dispositivo en un lugar al que solo pueda acceder personal profesional con el conocimiento adecuado de las precauciones y advertencias de seguridad. Las personas no profesionales pueden sufrir lesiones accidentales si ingresan al área de ensamblaje mientras el equipo está funcionando normalmente.

2.3 - Operación y mantenimiento diario

- No toque el elemento de disipación de calor del dispositivo para evitar quemaduras.
- Siga atentamente las instrucciones de la guía al desmontar el dispositivo; el desmontaje no profesional puede provocar fugas de agua o una calidad de imagen deficiente. Póngase en contacto con el servicio posventa para reemplazar el desecante si aparece condensación en la lente después de desempacar o si el desecante se vuelve verde (no todos los modelos están equipados con desecante).
- Se recomienda utilizar el dispositivo junto con un pararrayos para mejorar el efecto de protección contra rayos.
- Se recomienda conectar el orificio de puesta a tierra a tierra para aumentar la fiabilidad del dispositivo.
- No toque el sensor de imagen (CMOS) directamente. El polvo y la suciedad se pueden eliminar con un soplador o la lente se puede limpiar suavemente con un paño suave humedecido con alcohol.
- El exterior del dispositivo se puede limpiar con un paño suave y seco, que también se puede usar para eliminar las manchas difíciles cuando se humedece con un detergente suave. Para evitar posibles daños a la superficie de la carcasa de la máquina, lo que podría reducir el rendimiento, no utilice disolventes volátiles como alcohol, bencina, diluyentes o detergentes fuertes y abrasivos.
- La cubierta del domo es un componente óptico, no toque ni limpie la cubierta con las manos directamente durante el montaje o la operación. Para eliminar el polvo, la grasa o las huellas dactilares, limpie con un algodón dietílico sin aceite ligeramente humedecido o con un paño suave húmedo. También se puede utilizar un soplador para eliminar el polvo.

Advertencia

- Fortalecer la protección de su red, los datos del dispositivo y la información personal a través de medidas que incluyen, entre otras, usar una contraseña segura, modificar su contraseña regularmente, actualizar el software de su dispositivo a la última versión y configurar una computadora privada red. Para algunos dispositivos con versiones de software antiguas, la contraseña de ONVIF no se modificará automáticamente cuando se cambie la contraseña del sistema y deberá actualizar el software o actualizar manualmente la contraseña de ONVIF.
- Utilice componentes o accesorios estándar proporcionados por el fabricante y asegúrese de que ingenieros profesionales instalen y mantengan el dispositivo.
- La superficie del sensor de imagen no debe exponerse a la radiación del rayo láser en el entorno donde se utiliza el dispositivo de rayo láser.
- No encienda el dispositivo con dos o más fuentes de alimentación. A menos que se diga lo contrario. El incumplimiento de estas instrucciones puede dañar el dispositivo.

Precaución

Toda la instalación y operaciones aquí descritas deben ajustarse a las normas locales de seguridad eléctrica. El aparato no admite el montaje en pared con el panel frontal hacia abajo.

- Las siguientes figuras son sólo de referencia. El producto real prevalecerá.

3.1 - Dimensiones

Las siguientes figuras son sólo de referencia y prevalecerá el producto real.

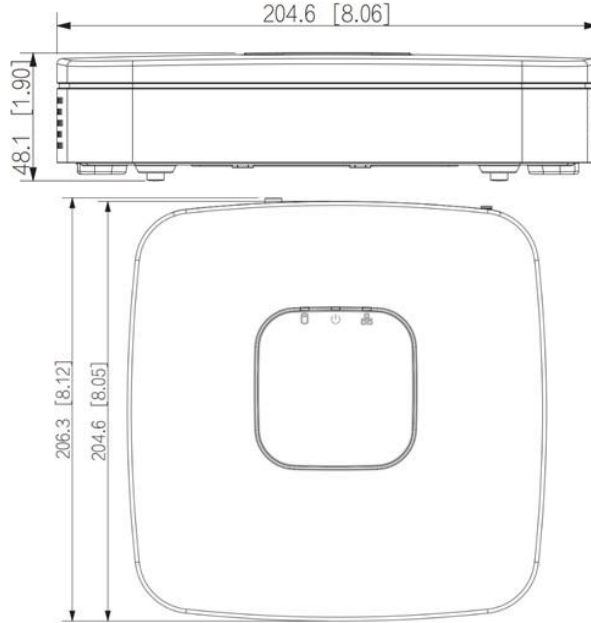


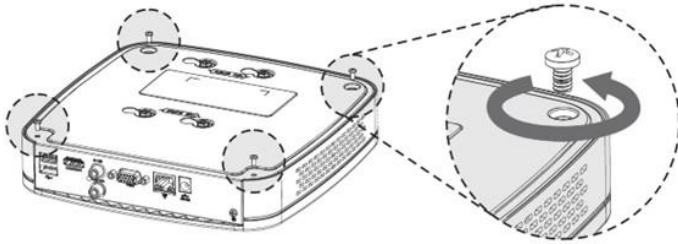
Figure 3-1 Dimensions (Unit: mm[inch])

3.2 - Instalación del disco duro

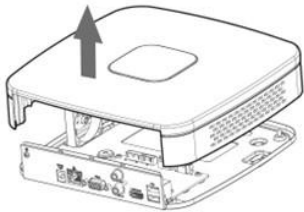
Apague el NVR y desenchufe el cable de alimentación antes de abrir la tapa para instalar el disco duro.

Durante la primera instalación, compruebe si el disco duro está instalado o no. Se recomienda utilizar un disco duro de nivel empresarial o de vigilancia. No se recomienda utilizar un disco duro de PC.

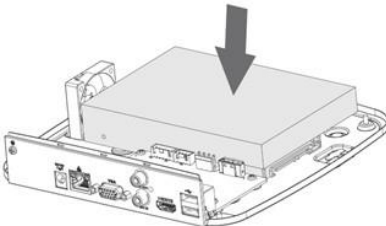
1. Dé la vuelta al dispositivo y retire los cuatro tornillos de fijación de la placa base.



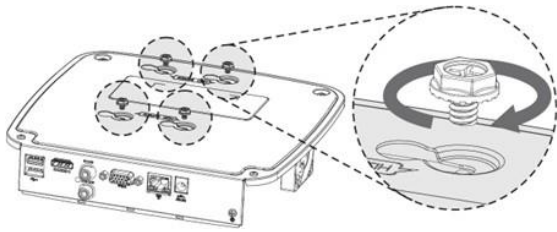
2. Retire la tapa siguiendo la dirección indicada por la siguiente flecha.



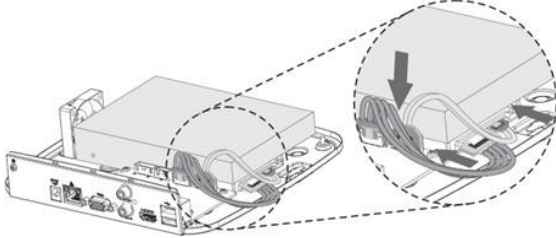
3. Haga coincidir los cuatro orificios de la parte inferior para colocar el disco duro.



4. Coloque el dispositivo boca abajo, haga coincidir los tornillos con los orificios del disco duro y fíjelos. El disco duro queda fijado a la placa base.



5. Conecte el cable de datos del HDD y el cable de alimentación al dispositivo.

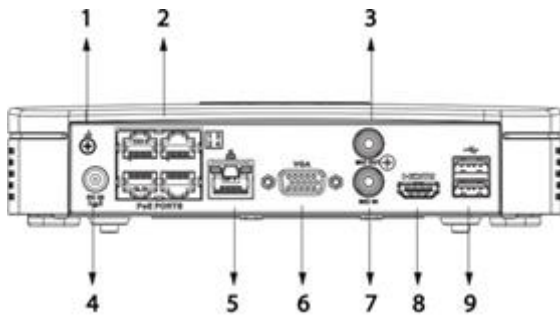


6. Vuelva a colocar la tapa y apriete los cuatro tornillos de la placa base para completar la instalación.



3.3 - Conexión

- Las siguientes figuras son sólo de referencia. El producto real prevalecerá.
- Por favor, compruebe cuidadosamente los iconos del panel trasero y consulte el producto real para obtener información detallada.
- Si el icono es (DC12V), introduzca 12 V CC. Si el icono es (DC48V), introduzca alimentación de 48 V CC.



- | | | | |
|---|-----------------------------|---|-------------------------|
| 1 | Toma de tierra | 2 | Puertos PoE |
| 3 | AUDIO OUT, conector RCA | 4 | Entrada de alimentación |
| 5 | Puerto de red | 6 | Puerto VGA |
| 7 | Entrada AUDIO, conector RCA | 8 | Puerto HDMI |
| 9 | Puertos USB | | |

4 CONFIGURACION

4.1 - Puesta en servicio

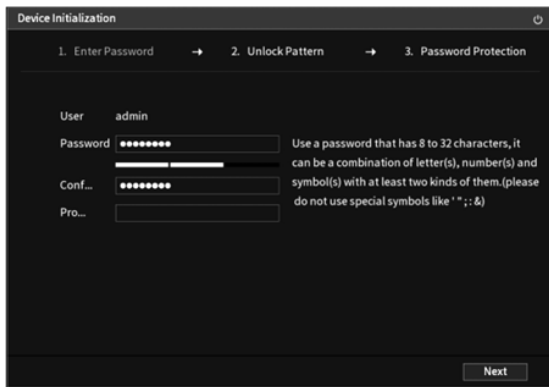
Antes de la puesta en servicio, asegúrese de que:

- La tensión nominal de entrada corresponde a los requisitos de alimentación del NVR (Grabador de Vídeo en Red).
- La conexión del cable de alimentación está lista.
- Para garantizar la seguridad de la unidad, conecte primero el NVR a la fuente de alimentación y después a la toma de corriente.
- Utilice siempre una corriente estable. Se recomienda utilizar un SAI como fuente de alimentación.
- Los aparatos de algunas series no disponen de botón de encendido/apagado. La unidad puede encenderse cuando la fuente de alimentación está conectada. Conecte la unidad a un monitor o televisor mediante un cable HDMI, enchúfela a una toma de corriente y, a continuación, pulse el botón de encendido para poner en marcha la unidad.

4.2 - Inicialización del aparato

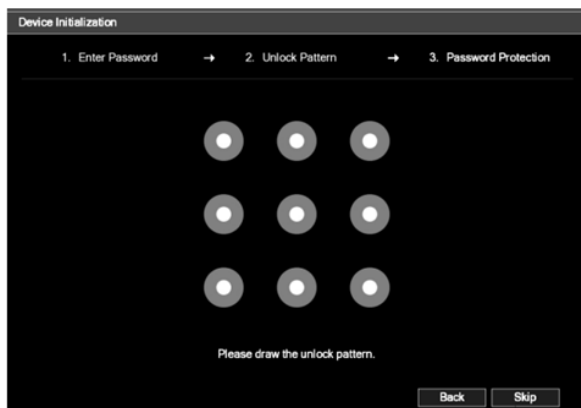
Durante la primera puesta en marcha, se debe configurar la información de la contraseña para el administrador (por defecto). Para garantizar la seguridad del aparato, la contraseña de acceso del administrador debe estar bien oculta y modificarse regularmente.

1. Encienda el aparato. Aparecerá la interfaz de inicialización del aparato. De la lista desplegable, seleccione la región, el idioma y el estándar de video según sea necesario.
2. Seleccione la zona horaria y configure la hora del sistema.
3. Lea el Acuerdo de Licencia de Software y seleccione "He leído y acepto todos los términos y condiciones".
4. Configure la información de la contraseña para el administrador. Para más detalles, consulte la siguiente tabla.



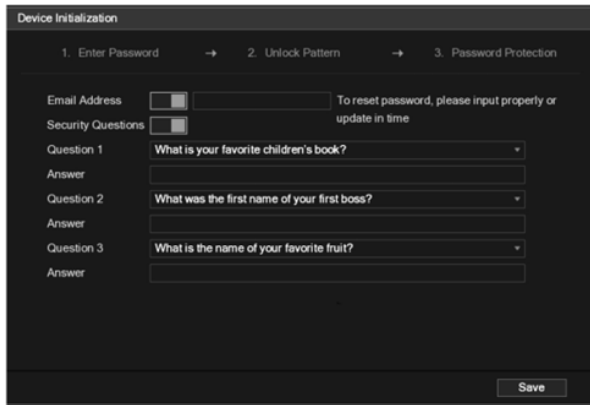
Paramount	Descripción
Usuario	El usuario por defecto es admin.
Contraseña	En el campo Contraseña, introduzca la contraseña de admin. La nueva contraseña puede contener entre 8 y 32 caracteres.
Confirmar contraseña	Los caracteres deben contener al menos dos tipos de números, letras y caracteres especiales (excluyendo "", "", ", ", ":" y "&").
Pregunta de apoyo	En el campo Pregunta, introduzca información que pueda recordarle su contraseña.

5. Utilice el ratón para dibujar un patrón de desbloqueo y, a continuación, vuelva a dibujarlo para confirmarlo.




- El patrón que desee configurar debe cruzar al menos cuatro puntos.
- Si no desea configurar el patrón de desbloqueo, haga clic en Omitir.
- Una vez configurado el patrón de desbloqueo, se utilizará como método de autenticación predeterminado. Si omite esta opción de configuración, introduzca la contraseña de inicio de sesión

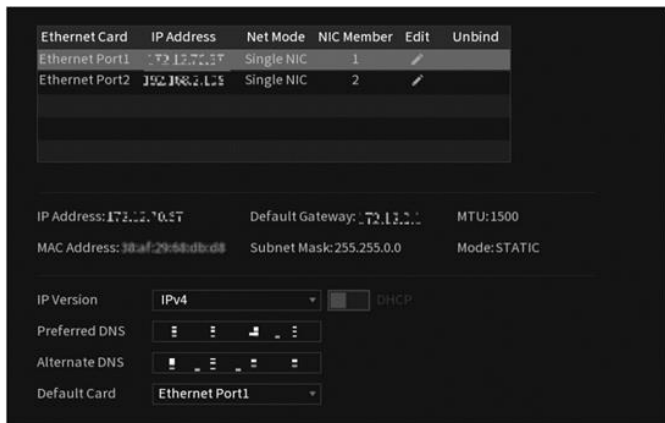
6. Aplique la dirección de correo electrónico reservada y las preguntas de seguridad al NVR.



- Active la casilla “Dirección de correo electrónico” e introduzca la dirección de correo electrónico.
 - Active la casilla “Habilitar preguntas de seguridad” e introduzca las respuestas a estas preguntas.
 - Una vez configurado, si olvida la contraseña del usuario administrador, puede restablecerla utilizando la dirección de correo electrónico reservada o las preguntas de seguridad.
 - Si no desea configurar los ajustes, desactive las funciones de dirección de correo electrónico y preguntas de seguridad en la interfaz.
7. Pulse OK para completar la inicialización.

4.3 - Configuración de la red

1. Seleccione Menú principal > Red > TCP/IP. Se muestra la interfaz TCP/IP. Haga clic en  para modificar la dirección IP de acuerdo con su dirección doméstica actual la configuración de su red doméstica (la dirección IP por defecto es 192.168.1.108)



Parámetro	Descripción
Versión IP	Puede seleccionar IPv4 o IPv6 en la lista Versión IP. Ambas versiones son compatibles para fines de acceso.
Dirección MAC	Muestra la dirección MAC del NVR.
DHCP	Habilita la función DHCP. La dirección IP, la máscara de subred y la puerta de enlace predeterminada no están disponibles para la configuración cuando la función DHCP está activada. <ul style="list-style-type: none"> • Si la función DHCP está en marcha, la información obtenida se mostrará en los campos Dirección IP, Máscara de subred y Puerta de enlace predeterminada. En caso contrario, todos los valores indicarán 0.0.0.0. • Si la conexión PPPoE se realiza correctamente, la dirección IP, la máscara de subred, la puerta de enlace predeterminada y DHCP no estarán disponibles para su configuración.
Dirección IP	Introduzca la dirección IP configure la máscara de subred y la puerta de enlace predeterminada adecuadas. NOTA La dirección IP y la puerta de enlace predeterminada deben estar en el mismo segmento de red.
Máscara de subred	
Puerta de enlace predeterminada	
DNS preferido	Introduzca la dirección IP del DNS.
DNS alternativo	Introduzca la dirección IP del DNS alternativo.
MTU	Introduzca el valor de la tarjeta de red. El valor oscila entre 1280 y 1500 bytes. El valor predeterminado es 1500. Los valores de MTU sugeridos son los siguientes. 1500: El valor más grande del paquete de información Ethernet. Este valor suele elegirse si no hay conexión PPPoE o VPN, y también es el valor por defecto de algunos routers, tarjetas de red y conmutadores. 1492: Valor optimizado para PPPoE. 1468: Valor optimizado para DHCP. 1450: Valor optimizado para VPN.
Test	Haga clic en Probar para comprobar que la dirección IP y la pasarela introducidas funcionan juntas.

4.4 - Añadir cámaras IP

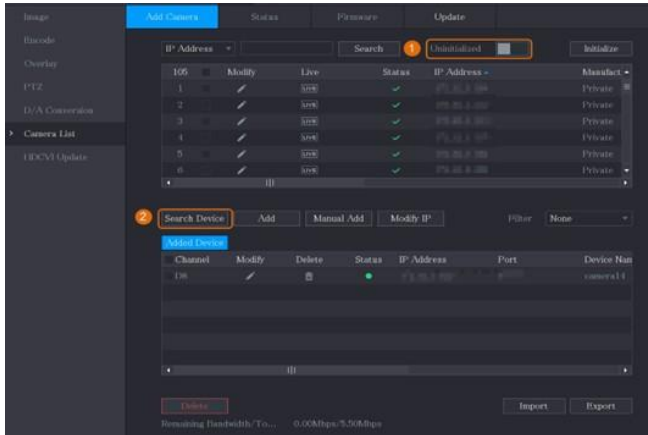
Se puede añadir una cámara IP basándose en los resultados de búsqueda o introduciendo manualmente la información de la dirección IP.

4.4.1 - Inicializar cámaras IP

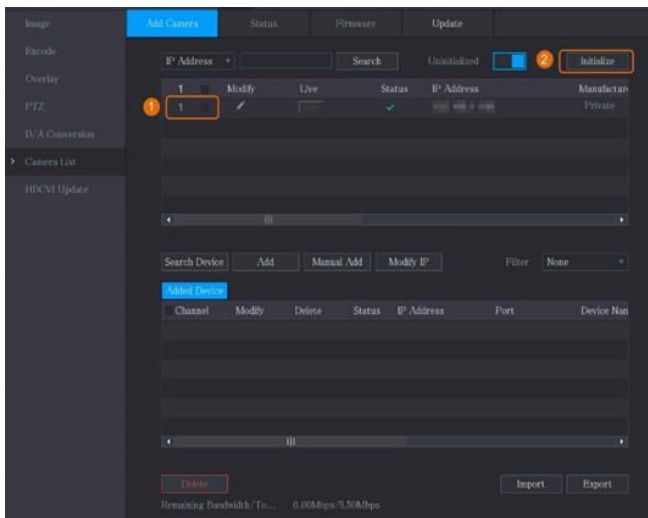
Este tema muestra cómo inicializar nuevas cámaras o cámaras después de un restablecimiento de fábrica.

- Cuando se conecta una cámara al NVR a través del puerto PoE integrado, el NVR inicializa automáticamente la cámara. La cámara acepta la contraseña del NVR y la dirección de correo electrónico de forma predeterminada.

1. Seleccione Menú principal > Cámara > Lista de cámaras > Añadir cámara.
2. Seleccione la casilla "Sin inicializar" y, a continuación, haga clic en Buscar dispositivo.



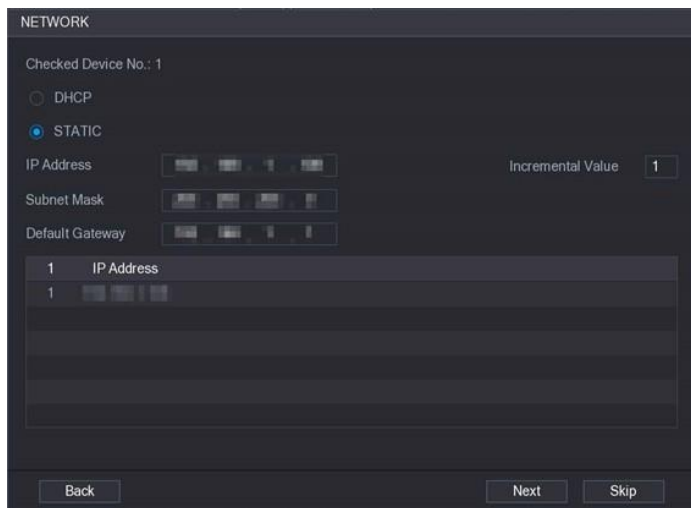
3. Seleccione la cámara que desea inicializar y, a continuación, haga clic en el botón Inicializar.



4. Aplique la contraseña y la información de correo electrónico a la cámara IP
 - Seleccione "Usar la contraseña actual del dispositivo y la información de correo electrónico" para dejar las mismas credenciales para la cámara que en el NVR.
 - Desmarque la opción "Usar contraseña de dispositivo actual e información de correo electrónico" para definir credenciales diferentes para la cámara.
5. Configurar la dirección IP de la cámara
 - Seleccione DHCP si se ha implementado un servidor DHCP.
 - Seleccione Estática (preferido) e introduzca la dirección IP, la máscara de subred, la puerta de enlace predeterminada y el valor incremental.

Nota

- Establezca el valor incremental si desea cambiar las direcciones IP de varias cámaras simultáneamente. El NVR añadirá un valor incremental a la cuarta sección de la dirección IP después de asignar una dirección IP para estas cámaras

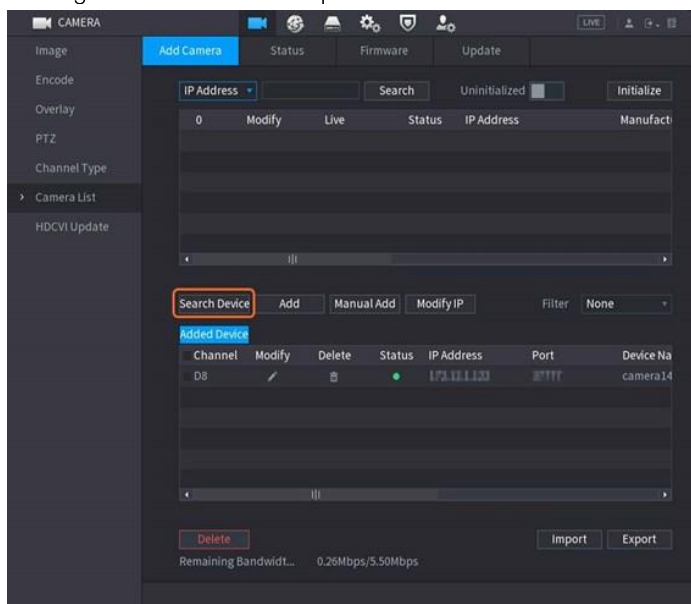


6. Pulse Siguiente. Espere 1-2 minutos a que finalice el procedimiento de inicialización.
7. Haga clic en Finalizar.

4.4.2 - Añadir cámaras IP por resultados de búsqueda

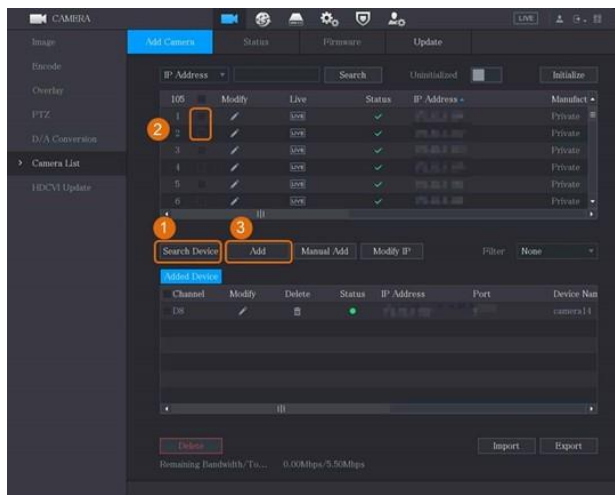
Asegúrese de que las cámaras que desea añadir ya se han inicializado y están conectadas a la red correcta.

1. Seleccione Menú principal > Cámara > Lista de cámaras > Añadir cámara.
2. Haga clic en Buscar un dispositivo.



3. Añadir cámaras IP:

- Añadir haciendo doble clic: Haga doble clic en la cámara de destino para añadirla a la lista de dispositivos añadidos.
- Añadir por casilla de verificación: Seleccione la casilla de verificación de la cámara de destino y, a continuación, haga clic en Añadir para añadirla a la lista de dispositivos añadidos
- Puede seleccionar más de una casilla de verificación y añadir cámaras por lotes.



- Si el estado de la cámara añadida es verde, significa que la cámara se ha añadido correctamente al NVR.

- Si el estado de la cámara añadida es rojo, esto indica un fallo de conexión entre la cámara y el NVR. Compruebe los parámetros de la cámara, como la contraseña, el protocolo y el número de canal, y vuelva a intentar añadir la cámara.

4.4.3 - Añadir cámaras IP manualmente

Se puede añadir una cámara IP a la vez mediante la información IP.

Asegúrese de que las cámaras que desea añadir ya han sido inicializadas y conectadas a la red correcta.

1. Seleccione Menú principal > Cámara > Lista de cámaras > Añadir cámara.
2. Haga clic en Añadir manualmente.
3. En el cuadro de diálogo Añadir manualmente, configure los parámetros.

Parámetro	Description
Canal	En la lista desplegable Canal, seleccione el canal que desea que utilice el NVR para conectarse al dispositivo remoto.
Productor	Seleccione el fabricante del dispositivo remoto en la lista desplegable Fabricante.
Dirección IP	Introduzca la dirección IP de la cámara IP en el campo Dirección IP. <ul style="list-style-type: none"> • Cambie el valor por defecto (192.168.0.0) al que el sistema no puede conectarse.
Port RTSP	El valor por defecto es 554. Este valor puede cambiarse si es necesario.
Port HTTP	El valor por defecto es 80. Este valor puede cambiarse si es necesario. <ul style="list-style-type: none"> • Si introduce un valor diferente, por ejemplo 70, introduzca 70 después de la dirección IP al iniciar sesión en el NVR a través del navegador.
Port TCP	El valor por defecto es 37777, este valor se puede cambiar si es necesario.
Nombre de usuario	Introduzca el nombre de usuario del dispositivo remoto.
Contraseña	Introduzca la contraseña de usuario del dispositivo remoto.
CH remoto	Introduzca el número de canal del dispositivo remoto que desea añadir.
Estrategia del decodificador	En la lista Estrategia de decodificación, seleccione Predeterminada, En tiempo real o Fluida según sea necesario.
Tipo de protocolo	<ul style="list-style-type: none"> • Si la cámara IP se añade mediante protocolo privado, seleccione TCP. • Si la cámara IP se añade a través de ONVIF, seleccione Auto, TCP, UDP o MULTICAST. • Si la cámara IP se ha añadido a través de terceros, seleccione TCP o UDP.
Cifrado	Si la cámara IP se ha añadido a través del protocolo ONVIF, la selección de la casilla de verificación Cifrado proporcionará protección de cifrado para los datos transmitidos. HTTPS debe estar habilitado para que la cámara IP remota utilice esta función.

4.5 - Configurar el horario de almacenamiento de la grabación de vídeo

Por defecto, todas las cámaras graban vídeo continuamente durante 24 horas al día. Puede modificar la configuración si es necesario


1. Seleccione Menú principal > Memoria > Horario > Grabación



2. Configure los parámetros.

Parámetro	Descripción
Canal	Haga clic en la lista desplegable Canal Z y seleccione un canal para cambiar la configuración de grabación de vídeo.
Pregrabación	En el campo Pregrabar, establezca el tiempo de captura del vídeo adicional que aparece antes del evento para proporcionar contexto a la grabación. Rango de valores: 0 a 30 s.
Redundancia	<p>Permite a los usuarios configurar uno de los discos duros como disco duro redundante para guardar los archivos grabados en discos duros diferentes. En caso de fallo del disco duro, se puede encontrar una copia de seguridad de la grabación en el disco duro redundante.</p> <ul style="list-style-type: none"> • Seleccione Menú principal > ALMACENAMIENTO > Administrador de discos y, a continuación, configure el disco duro como disco duro redundante. • Seleccione Menú principal > ALMACENAMIENTO > Programar > Grabar y, a continuación, marque la casilla Redundancia. • Si el canal seleccionado no está grabando, la función de redundancia tendrá efecto en la siguiente grabación, esté o no marcada la casilla. • Si el canal seleccionado está grabando, se empaquetarán los archivos grabados actualmente y se iniciará la grabación de acuerdo con la nueva programación. • Esta función está disponible en determinados modelos. • El disco duro redundante sólo realiza copias de seguridad de los vídeos grabados, pero no de las instantáneas.
Tipo de evento	<p>Marque la casilla correspondiente al tipo de evento.</p> <p>General: La grabación general significa que el NVR graba todos los vídeos dentro de un intervalo de tiempo especificado. La grabación general aparece marcada en verde.</p> <p>Movimiento: La grabación de movimiento significa que el NVR sólo graba vídeo cuando se activa la detección de movimiento. Se representa con el color amarillo.</p> <p>Alarma: La grabación de alarma significa que el NVR graba vídeo cuando se activa una alarma. Se representa con el color rojo.</p> <p>M&A: La grabación M&A combina la grabación de movimiento y la grabación de alarma. El dispositivo graba vídeo cuando se detecta movimiento o se activa cualquier alarma. Se representa con el color naranja.</p> <p>Inteligente: La grabación inteligente significa que el NVR graba vídeo cuando se activa la detección inteligente. Se representa con el color azul.</p> <p>POS: La grabación POS significa que el NVR graba vídeo cuando se utiliza un dispositivo POS para realizar pagos. Se representa con el color morado.</p>
Periodo	Especifica el periodo durante el cual está activo el ajuste de grabación configurado. El sistema sólo activa la alarma durante el periodo definido.
Copiar a	Haga clic en Copiar para copiar la configuración a otros canales.

3. Establezca el horario dibujando o editando

- Dibujar: Mantenga pulsado el botón izquierdo del ratón y arrástrelo para dibujar un periodo.
- Edición: haga clic  para configurar el periodo y, a continuación, haga clic en Aceptar

4. Haga clic en Aplicar

- El horario de grabación configurado sólo puede tener efecto si la función de grabación automática está activada.

4.6 - Inicio de sesión en la interfaz web

1. Abra Internet Explorer, introduzca la dirección IP del dispositivo en la barra de direcciones y pulse Intro. Si aparece el asistente de configuración, siga las instrucciones para completar los ajustes.
2. Introduzca su nombre de usuario y contraseña en el cuadro de inicio de sesión y, a continuación, haga clic en Iniciar sesión.
3. Si es la primera vez que inicia sesión, haga clic en Haga clic aquí para descargar el complemento y, a continuación, instale el complemento siguiendo las instrucciones.
4. Aparecerá la interfaz principal.

5 RECOMENDACIONES SOBRE CIBERSEGURIDAD

Medidas obligatorias de ciberseguridad

A. Cambio de contraseñas y uso de contraseñas seguras:

La principal razón de los sistemas "hackeados" es tener contraseñas débiles o por defecto. Se recomienda cambiar inmediatamente las contraseñas por defecto y elegir contraseñas seguras siempre que sea posible. Una contraseña segura debe constar de al menos 8 caracteres y una combinación de caracteres especiales, números y letras mayúsculas y minúsculas.

B. Actualización del firmware

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

"Nice to have" recomendaciones para mejorar la seguridad de su red

A. Cambie las contraseñas con regularidad

Cambie regularmente las credenciales de sus dispositivos para asegurarse de que sólo los usuarios autorizados tienen acceso al sistema.

B. Cambie los puertos HTTP y TCP por defecto:

- Cambie los puertos HTTP y TCP por defecto de sus sistemas. Estos son los dos puertos utilizados para la comunicación y la visualización remota de las secuencias de vídeo.
- Estos puertos se pueden cambiar a cualquier conjunto de números en el rango 1025-65535. Evitar los puertos por defecto reduce el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

C. Transmisión cifrada de audio y vídeo

Si el contenido de sus datos de audio y vídeo es muy importante o sensible, le recomendamos que utilice la función de transmisión cifrada para reducir el riesgo de que le roben los datos de audio y vídeo durante la transmisión.

Recuerde: la transmisión encriptada supondrá cierta pérdida de rendimiento en la transmisión.

D. Activar filtro IP:

Habilitar el filtro IP impedirá que cualquier persona acceda al sistema excepto aquellos con direcciones IP específicas.

E. Cambiar contraseña ONVIF:

Para firmware de cámara IP más antiguos, la contraseña ONVIF no cambia cuando se cambian las credenciales del sistema. Deberá actualizar el firmware de la cámara a la última versión o cambiar manualmente la contraseña ONVIF.

F. Habilitar bloqueo de cuenta

La función de bloqueo de cuenta está activada por defecto y recomendamos dejarla activada para garantizar la seguridad de la cuenta. Si un atacante intenta iniciar sesión utilizando una contraseña incorrecta varias veces, la cuenta correspondiente y la dirección IP de origen se bloquearán.

G. Reenvíe sólo los puertos necesarios:

- Reenvíe sólo los puertos HTTP y TCP que necesite. No reenvíe una amplia gama de números al dispositivo. No DMZ la dirección IP del dispositivo.
- No necesita reenviar ningún puerto para cámaras individuales si todas están conectadas al DVR in situ; sólo necesita el NVR.

H. Restrinja la funcionalidad de cuenta de invitado:

Si el sistema está configurado para varios usuarios, asegúrese de que cada usuario sólo tiene acceso a las funciones que necesita para realizar su trabajo.

I. Desactive los servicios innecesarios y seleccione modos seguros

Si no es necesario, es aconsejable desactivar ciertos servicios como SNMP, SMTP, UPnP, etc. para reducir riesgos.

Si es necesario, se recomienda utilizar modos seguros, incluidos, entre otros, los siguientes servicios:

- SNMP: Seleccione SNMP v3 y configure contraseñas de cifrado y autenticación seguras.
- SMTP: Seleccione TLS para acceder al servidor de buzones.
- FTP: Seleccione SFTP y configure contraseñas seguras.
- AP hotspot: Seleccione el modo de cifrado WPA2-PSK y establezca contraseñas seguras.

J. Auditoría segura

Comprobación de usuarios en línea: le recomendamos que compruebe regularmente los usuarios en línea para ver si el NVR ha iniciado sesión sin autorización.

Comprobación de los registros del dispositivo: Revisando los registros, puede averiguar las direcciones IP que se han utilizado para iniciar sesión en los dispositivos y sus operaciones clave.

K. Registro de red

Debido a la limitada capacidad de memoria del dispositivo, el registro almacenado es limitado. Si es necesario almacenar el registro durante un largo periodo de tiempo, se recomienda activar la función de registro de red para garantizar que los registros críticos se sincronizan con el servidor de registro de red con fines de seguimiento.

L. Bloquear físicamente el dispositivo:

Lo ideal es impedir el acceso físico no autorizado al sistema. La mejor manera de conseguirlo es instalar el registrador en una caja cerrada con llave, en un armario de servidor con cerradura o en una habitación detrás de una puerta cerrada con llave.

M. Conexión de cámaras IP a los puertos PoE de la parte posterior de la unidad NVR:

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

N. Creación de un entorno de red seguro

Para garantizar mejor la seguridad de sus equipos y reducir las posibles amenazas cibernéticas, le recomendamos:

- Desactivar la función de mapeo de puertos del router para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe estar dividida y aislada en función de las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, redes GAP y otras tecnologías para particionar la red y lograr el aislamiento de la misma.
- Establezca un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.

O. Se recomienda habilitar un cortafuegos o una función de lista de bloqueo y permiso para reducir el riesgo de ataque al dispositivo.

6 INFORMACION ADICIONAL

Para más información y para descargar el software necesario, visite la siguiente página web:





Nice SpA
Oderzo TV Italia
info@niceforyou.com

www.niceforyou.com