



Grabador de vídeo en red

Guía de inicio rápido

ÍNDICE DE CONTENIDOS

Introducción	6
Cambiar el modo del dispositivo.....	7
Crear un clúster	7
Añada más NVR para aumentar la capacidad del clúster.....	11
Administrar el almacenamiento del clúster	12
Administrar HDD	12
Configurar el tipo de almacenamiento	13
Consultar el estado del clúster.....	15
Manejar las excepciones del clúster	16

Manual del usuario

COPYRIGHT ©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

TODOS LOS DERECHOS RESERVADOS.

Toda la información y cualquier parte obtenida de la misma, incluyendo entre otros la redacción, las imágenes y los gráficos, son propiedad de Hangzhou Hikvision Digital Technology Co., Ltd. o empresas subsidiarias (en adelante "Hikvision"). Este manual del usuario (en adelante "el Manual") no podrá ser reproducido, modificado o distribuido, parcialmente o en su totalidad, por ningún medio, sin el permiso previo por escrito de Hikvision. A menos que se estipule otra cosa, Hikvision no representa ni garantiza, de manera expresa o implícita, la información de este Manual.

Acerca de este Manual

Este Manual es aplicable al Grabador de Vídeo en Red (NVR, por sus siglas en inglés).

Este Manual incluye las instrucciones de manipulación y utilización del producto. Figuras, gráficos, imágenes y otra información que encontrará en lo sucesivo tienen únicamente con fines descriptivos y aclaratorios. La información incluida en el Manual está sujeta a cambios, sin aviso previo, debido a actualizaciones de software u otros motivos. Encuentre la última versión en la página web de la compañía (<http://overseas.hikvision.com/en/>).

Utilice este manual del usuario orientado por un profesional.

Reconocimiento de marcas comerciales

HIKVISION y otras marcas comerciales y logotipos de Hikvision son propiedad de Hikvision en diferentes jurisdicciones. Otras marcas comerciales y logotipos mencionados a continuación son propiedad de sus respectivos propietarios.

Avisos legales

HASTA DONDE LO PERMITA LA LEY VIGENTE, EL PRODUCTO DESCRITO, CON SU HARDWARE, SOFTWARE Y FIRMWARE, SE ENTREGA "TAL CUAL", CON TODOS SUS FALLOS Y ERRORES, Y HIKVISION NO OFRECE GARANTÍA, NI EXPRESA NI IMPLÍCITA, INCLUYENDO, ENTRE OTRAS, LA COMERCIABILIDAD, CALIDAD SATISFACTORIA, IDONEIDAD PARA UN PROPÓSITO PARTICULAR Y NO INFRACCIÓN DE LOS DERECHOS DE TERCERAS PARTES. EN NINGÚN CASO HIKVISION, SUS DIRECTORES, ADMINISTRADORES, EMPLEADOS O AGENTES, SE RESPONSABILIZARÁN ANTE USTED DE CUALQUIER DAÑO ESPECIAL, CONSECUCIONAL, INCIDENTAL O INDIRECTO, INCLUYENDO, ENTRE OTROS, LOS DAÑOS POR PÉRDIDAS DE BENEFICIOS DE NEGOCIOS, INTERRUPCIÓN DE NEGOCIOS O PÉRDIDAS DE DATOS O DOCUMENTACIÓN, EN RELACIÓN CON EL USO DE ESTE PRODUCTO, INCLUSO AUNQUE HIKVISION HAYA ADVERTIDO DE LA POSIBILIDAD DE TALES DAÑOS.

EN LO CONCERNIENTE A PRODUCTOS CON ACCESO A INTERNET, EL USO DEL PRODUCTO SE HARÁ COMPLETAMENTE BAJO SU PROPIO RIESGO Y RESPONSABILIDAD. HIKVISION NO ASUMIRÁ NINGUN A RESPONSABILIDAD POR FUNCIONAMIENTO ANORMAL, FILTRACIÓN DE PRIVACIDAD U OTROS DAÑOS QUE RESULTEN DE CIBERATAQUES, ATAQUES DE HACKER, INSPECCIÓN DE VIRUS U OTROS RIESGOS DE SEGURIDAD DE INTERNET; SIN EMBARGO, HIKVISION PROPORCIONARÁ APOYO TÉCNICO PUNTUAL SI ES SOLICITADO.

LAS LEYES CONCERNIENTES A VIGILANCIA VARÍAN SEGÚN LA JURISDICCIÓN. COMPRUEBE TODA LA LEGISLACIÓN PERTINENTE A SU JURISDICCIÓN ANTES DE USAR ESTE PRODUCTO PARA GARANTIZAR QUE SU UTILIZACIÓN CUMPLE CON LA LEY EN VIGOR. HIKVISION NO ASUME NINGUNA RESPONSABILIDAD EN EL CASO DE QUE ESTE PRODUCTO SE UTILICE PARA FINES ILEGALES.

EN EL CASO DE QUE EXISTAN CONFLICTOS ENTRE LA INFORMACIÓN DE ESTE MANUAL CON LA LEY EN VIGOR, PREVALECERÁ ESTA ÚLTIMA.

Información normativa

Información de la FCC

Por favor, tenga en cuenta que cualquier cambio o modificación no aprobado expresamente por la parte responsable del cumplimiento podrá anular la autoridad del usuario para utilizar el equipo.

En conformidad con las normativas de la FCC: Este equipo ha sido probado y se ha verificado que cumple con los límites para los dispositivos digitales de Clase A indicados en la sección 15 de las normas de la FCC. Estos límites están diseñados para proporcionar una protección razonable contra las interferencias perjudiciales cuando el equipo se utiliza en un entorno comercial. Este equipo genera, usa y puede radiar energía de radiofrecuencia y, si no se instala y utiliza conforme a lo indicado en el manual de instrucciones, puede ocasionar interferencias perjudiciales a las comunicaciones por radio. El uso de este equipo en áreas residenciales puede ocasionar interferencias perjudiciales, en cuyo caso el coste de corregir dichas interferencias correrá a cargo del usuario.

Condiciones de la FCC

Este dispositivo cumple con la sección 15 de la normativa FCC. Su utilización está sujeta a las dos condiciones siguientes:

1. Este dispositivo no debe ocasionar interferencias perjudiciales.
2. Este dispositivo debe aceptar cualquier interferencia recibida, incluida aquella que pueda ocasionar un funcionamiento no deseado.

Declaración de conformidad de la UE



Este producto, y en su caso también los accesorios suministrados, tienen la marca "CE" y por tanto cumplen con las normas europeas armonizadas aplicables enumeradas en la Directiva de Compatibilidad Electromagnética 2014/30/UE, la Directiva de Baja Tensión 2014/35/UE y la directiva de Restricción del Uso de Sustancias Peligrosas 2011/65/UE.



2012/19/UE (directiva WEEE, Desechos de Equipos Eléctricos y Electromagnéticos): En la Unión Europea, los productos marcados con este símbolo no pueden ser arrojados al sistema de basura municipal sin recogida selectiva. Para un reciclaje adecuado, entregue este producto en el lugar de compra del equipo nuevo equivalente, o deshágase de él en el punto de recogida designado a tal efecto. Para más información vea la página web: www.recyclethis.info






2006/66/CE (directiva sobre baterías): Este producto lleva una batería que no puede arrojarse al sistema municipal de basuras sin recogida selectiva, dentro de la Unión Europea. Consulte la documentación del producto para ver la información específica de la batería. La batería lleva marcado este símbolo, que incluye unas letras indicando si contiene cadmio (Cd), plomo (Pb), o mercurio (Hg). Para un reciclaje adecuado, entregue la batería a su vendedor o llévela al punto de recogida de basuras designado a tal efecto. Para más información vea la página web: www.recyclethis.info

Cumplimiento industrial de la normativa canadiense sobre equipos causantes de interferencias (IECS, por sus siglas en inglés), ICES-003

Este dispositivo cumple con los requisitos de la normativa canadiense CAN ICES-3 (A)/NMB-3(A).

Convenciones de simbología

La definición de los símbolos que podrá encontrar en este documento es la siguiente.

Símbolo	Descripción
 NOTA	Proporciona información adicional para enfatizar o complementar puntos importantes del texto principal.
 ADVERTENCIA	Indica una situación potencialmente peligrosa, que de no ser evitada, podría ocasionar daños en el equipo, pérdida de datos, degradación del rendimiento o resultados inesperados.
 PELIGRO	Indica un peligro con alto nivel de riesgo, que de no ser evitado, ocasionará lesiones de gravedad o incluso la muerte.

Instrucciones de seguridad

- La correcta configuración de todas las contraseñas y del resto de parámetros de seguridad es responsabilidad del instalador y/o del usuario final.
- Para usar el producto debe cumplir estrictamente con la normativa de seguridad eléctrica de su país y región. Consulte las especificaciones técnicas para obtener información detallada.
- La tensión de entrada debe cumplir con las condiciones SELV (baja tensión de seguridad) y de fuente de alimentación de potencia limitada con 100 - 240 VCA, 48 VCC o 12 VCC, conforme a la normativa IEC60950-1. Consulte las especificaciones técnicas para obtener información detallada.
- No conecte varios dispositivos a un mismo adaptador eléctrico ya que la sobrecarga del adaptador puede ocasionar un sobrecalentamiento, siendo un riesgo de incendio.
- Asegúrese de que el enchufe esté bien conectado a la toma de corriente.
- Si hay presencia de humo, olores o ruidos procedentes del dispositivo, apague la alimentación inmediatamente y desenchufe el cable de alimentación. A continuación, contacte con el servicio técnico.

Consejos preventivos y cautelares

Antes de conectar y utilizar su dispositivo, tenga en cuenta los consejos siguientes:

- Asegúrese de que la unidad esté instalada en un ambiente sin polvo y bien ventilado.
- La unidad ha sido diseñada solo para uso en interiores.
- Mantenga los líquidos alejados del dispositivo.
- Asegúrese de que las condiciones ambientales cumplen las especificaciones de fábrica.
- Compruebe que la unidad esté correctamente fijada a su soporte o estantería. Las sacudidas y golpes fuertes como consecuencia de alguna caída, pueden ocasionar daños graves en los componentes electrónicos sensibles de la unidad.
- Utilice el dispositivo con una fuente ininterrumpida de energía (UPS, por sus siglas en inglés) siempre que sea posible.
- Corte la alimentación de la unidad antes de conectar y desconectar accesorios y periféricos.
- Con este dispositivo debería utilizar un HDD recomendado de fábrica.
- El uso o sustitución inadecuados de la batería pueden ocasionar un riesgo de explosión. Cámbiela únicamente por otra del mismo tipo o equivalente. Deshágase de las baterías usadas conforme a las instrucciones proporcionadas por el fabricante de la batería.

Introducción

El clúster del NVR proporciona servicios de vigilancia al integrar varios NVR como servidores anfitriones en ejecución en un único clúster. Utiliza una única dirección IP para responder a los dispositivos externos. A través de esta dirección IP es posible configurar la mayoría de los servicios, cómo administración, configuración y funcionamiento.

Los NVR utilizados por el clúster deben cumplir con los requisitos siguientes:

- El clúster y los dispositivos NVR deben estar en la misma LAN.
- Todos los dispositivos NVR deben ser del mismo modelo y tener la misma versión de firmware.



NOTA

- Cada clúster es capaz de gestionar de 3 a 16 dispositivos NVR.
- Entradas de vídeo máx. del clúster = canales NVR de un NVR x (n-1), donde n es el número de NVR en el clúster. Por ejemplo, si tiene 3 NVR en un clúster y cada NVR tiene 128 canales de entrada de vídeo, las entradas de vídeo máx. del clúster = $128 \times (3-1) = 256$ canales.
- Una vez creado el clúster, la dirección IP del clúster será accesible transcurridos 15 s.

Cambiar el modo del dispositivo

Propósito:

Si desea añadir más NVR al clúster, deberá cambiar la opción **Device Mode** a **Cluster Mode** y añadir al menos 3 NVR al clúster. Cada clúster es capaz de gestionar de 3 a 16 NVR.

Paso 1: Abra el navegador web, escriba la dirección IP del NVR y pulse Intro.

Paso 2: Introduzca el nombre de usuario y la contraseña del NVR en la interfaz de inicio de sesión, y haga clic en **Login**.

Paso 3: Acceda a **Configuration >System >User Management**.

Paso 4: Configure la opción **Device Mode** como **Cluster Mode**.

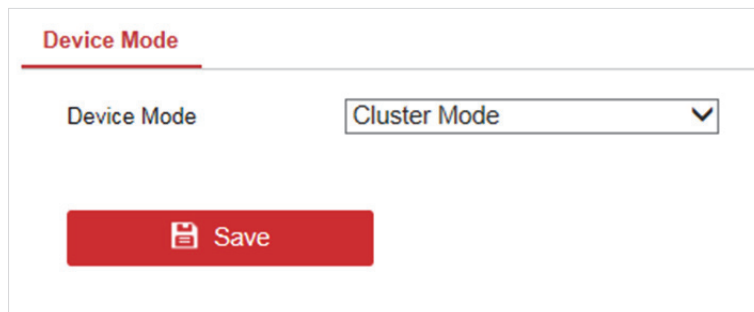


Figure 1 Cambiar el modo de trabajo

Paso 5: Haga clic sobre **Save** y espere a que el dispositivo se reinicie automáticamente.



NOTA

- Después de cambiar la opción **Device Mode** a **Cluster Mode**, algunas funciones quedarán inhabilitadas, como la administración de canales, administración de usuarios, entre otras. Los efectos de esta inhabilitación dependerán de la interfaz real.

Crear un clúster



NOTA


Es posible acceder a la administración y configuración de clústeres mediante el software del cliente de iVMS-4200.

Antes de empezar:

Compruebe que el software del cliente de iVMS-4200 correspondiente esté correctamente instalado.

El número de dispositivos NVR del clúster no puede ser inferior a 3. Asegúrese de cambiar la opción **Device Mode** a **Cluster Mode**.



Paso 1: Haga clic sobre  en el panel de control, o acceda a **Tool > Device Management > Device > Hikvision Device**.

Paso 2: Haga clic en **Create Cluster**.

Paso 3: Introduzca los parámetros solicitados.

Paso 4: Haga clic en **Next**.

Cluster Name	Cluster_1
IP Address	10.65.159.211
Port	8001
HTTP Port No.	81
User Name	admin
Password
Verify

Figure 2 Configurar los parámetros del clúster

- **Cluster Name:** Elija el nombre que desee ponerle al clúster.
- **IP Address:** Introduzca la dirección IP del clúster. Asegúrese de que la dirección IP esté en la misma LAN que los NVR y que no entre en conflicto con otros dispositivos.
- **Port:** El núm. de puerto del clúster para el servicio externo.

- **HTTP Port No.:** El núm. de puerto HTTP del clúster para el servicio web externo
- **User Name:** El nombre de usuario predeterminado es admin.
- **Password:** Introduzca la contraseña para el clúster.



ADVERTENCIA

Se recomienda una contraseña segura – Le recomendamos encarecidamente que cree una contraseña segura de su propia elección (utilizando un mínimo de 8 caracteres, incluyendo al menos tres de las siguientes categorías: mayúsculas, minúsculas, números y caracteres especiales) para aumentar la seguridad de su producto. También le recomendamos que restablezca su contraseña con regularidad. Especialmente en los sistemas de alta seguridad, restablecer la contraseña una vez al mes o a la semana protegerá mejor su producto.

Paso 5: Añada los NVR al clúster. Puede añadir los dispositivos de las formas siguientes:

- **Añadir dispositivo manualmente**

- 1) Haga clic en **Add**.
- 2) Introduzca la información solicitada, incluyendo IP del dispositivo/nombre del dominio y contraseña.
- 3) Haga clic en **Add** para añadir el dispositivo.

Figura 3 Añadir dispositivos

- **Añadir dispositivos con conexión**

- 1) Seleccione los dispositivos desde **Online device**.
- 2) Haga clic en **Add to Client** para añadir un solo dispositivo, o en **Add all** para añadir todos los dispositivos.

- 3) Introduzca la información solicitada, incluyendo la contraseña del dispositivo.
- 4) Haga clic en **Add** para añadir el dispositivo.



NOTA

- Si hace clic en **Add all**, asegúrese de que todos los dispositivos en la lista tengan la misma contraseña.
- El número de puerto del clúster no puede estar en conflicto con otros dispositivos.

Paso 6: Haga clic en **Done** para terminar de añadir.

Una vez creado el clúster correctamente, este aparecerá en el área **Device for Management**.

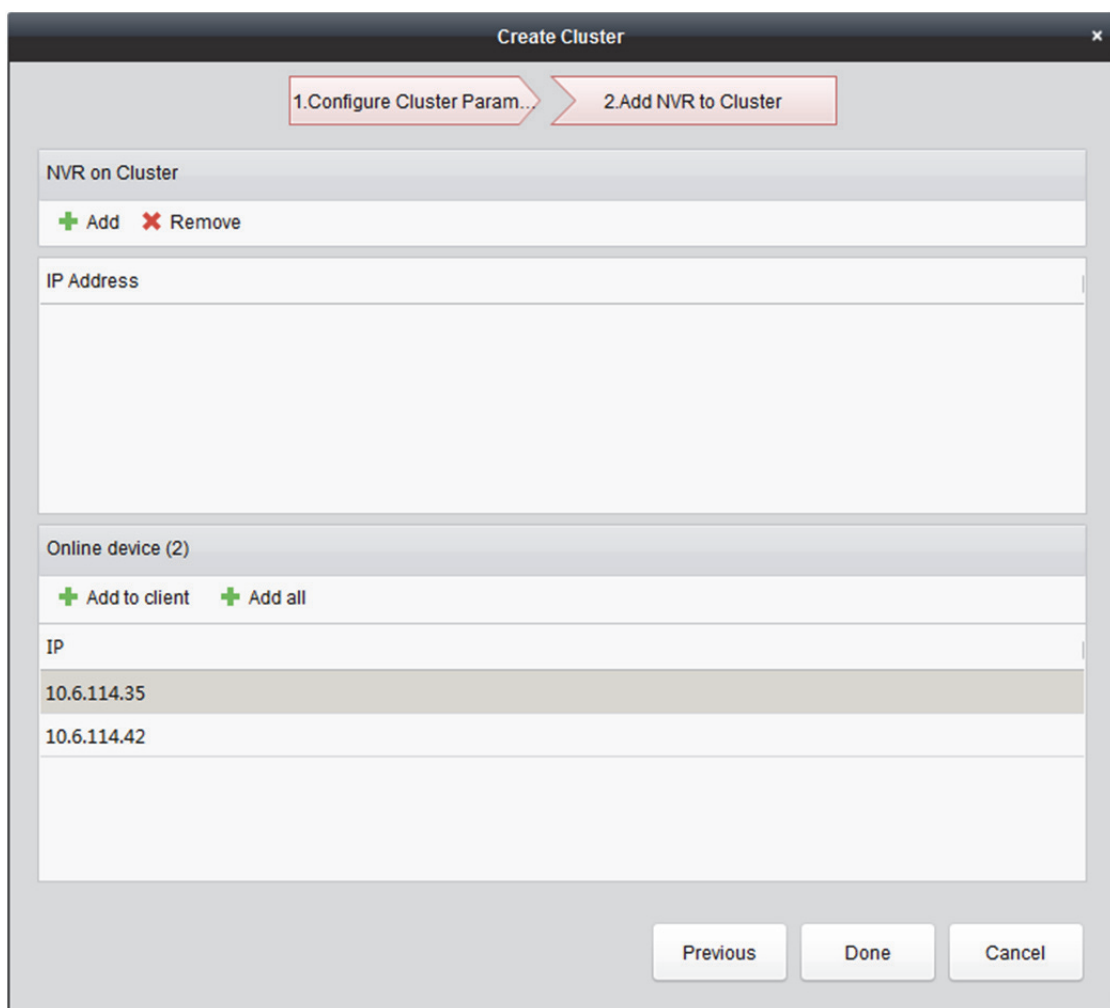


Figure 4 Añadir NVR al clúster


Añada más NVR para aumentar la capacidad del clúster.

Cada clúster permite de 3 a 16 NVR. Después de crear el clúster podrá añadir o eliminar NVR usando el software del cliente o el navegador web.

Antes de empezar:

A continuación tiene la información sobre cómo efectuar la configuración usando el cliente software. Si desea configurar el clúster usando el navegador web, acceda a la dirección IP del clúster: núm. de puerto HTTP, por ejemplo: 192.168.1.64:81.



Paso 1: Haga clic sobre  en el panel de control, o acceda a **Tool > Device Management > Device > Hikvision Device**.

Paso 2: Seleccione el clúster desde **Device for Management**.

Paso 3: Acceda a **Remote Configuration > Basic > System > Cluster Management**. En la lista de dispositivos podrá ver los NVR integrados en el clúster.

Device Management

Device List						Add	Delete
<input type="checkbox"/>	IP Address	Model	Running Status	CPU Usage	Memory Usage		
<input checked="" type="checkbox"/>	10.65.159.202	DS-96256NI-I16	Online	0	61		
<input type="checkbox"/>	10.65.159.203	DS-96256NI-I16	Online	0	60		
<input type="checkbox"/>	10.65.159.207	DS-96256NI-I16	Online	5	59		

Figura 5 Administración de dispositivos

Paso 4: Añada un NVR al clúster.

- 1) Haga clic en **Add**.
- 2) Introduzca los parámetros solicitados, incluyendo **IP Camera Address, Management Port, User Name, Password y Confirm**.
- 3) Haga clic en **OK**.

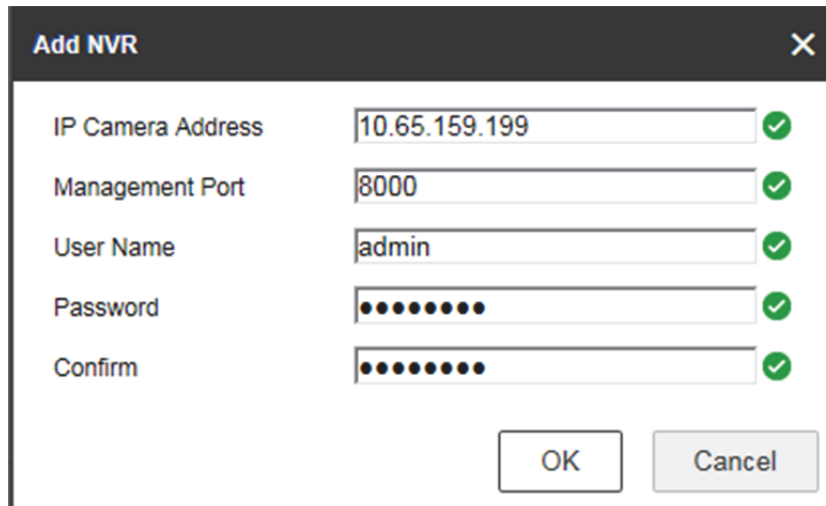


Figura 6 Añadir NVR

Podrá ver el dispositivo añadido correctamente en la **lista de dispositivos**.


Administrar el almacenamiento del clúster

Podrá administrar todos los HDD del clúster y establecer la cuota usando el software del cliente.

Administrar HDD

Podrá ver y formatear los HDD del clúster usando una única dirección IP.



Paso 1: Haga clic sobre  en el panel de control, o acceda a **Tool > Device Management > Device > Hikvision Device**.

Paso 2: Seleccione el clúster desde **Device for Management**.

Paso 3: Acceda a **Remote Configuration > Advanced > Storage > General**. Podrá ver la información del HDD en la opción **Configuring the HDD Parameters**, incluyendo la capacidad, el espacio libre, el estado, el tipo, etc.

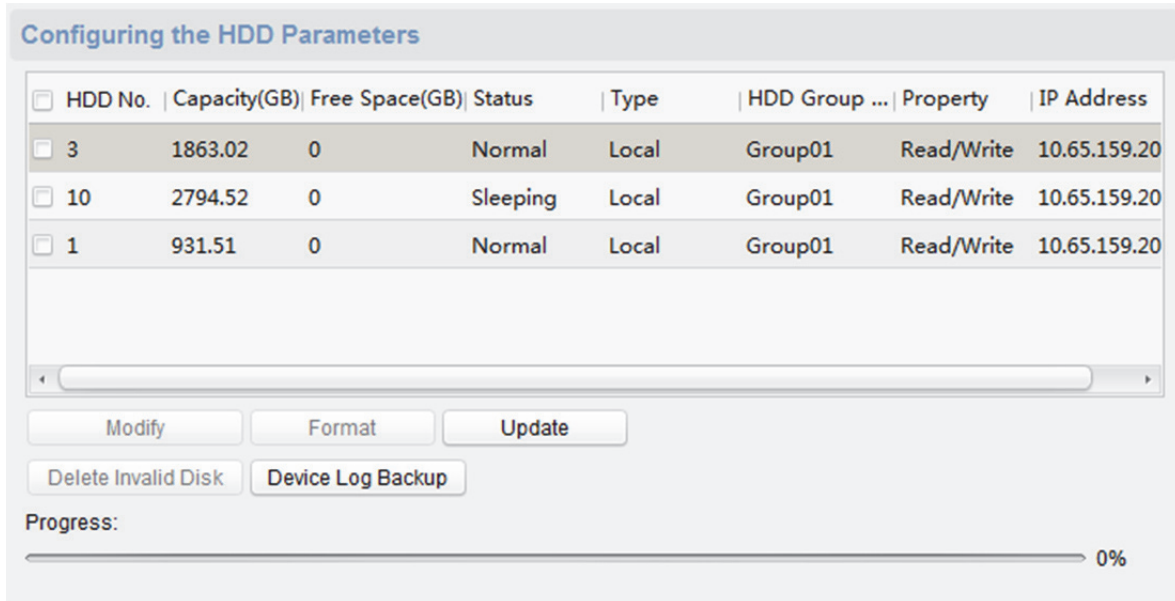


Figura 7 Configurar lo parámetros del HDD



NOTA

El valor predeterminado para todos los **números de grupos de HDD** es **Group01**.


Paso 4: **Opcional:** Formatear el HDD.

- 1) Marque la opción **HDD No.**
- 2) Haga clic en **Format**.
- 3) Haga clic en **OK**.

Configurar el tipo de almacenamiento

El modo de almacenamiento del HDD es **por cuota**. Es posible asignar la capacidad del HDD configurando la cuota como **Space** o **Time**.



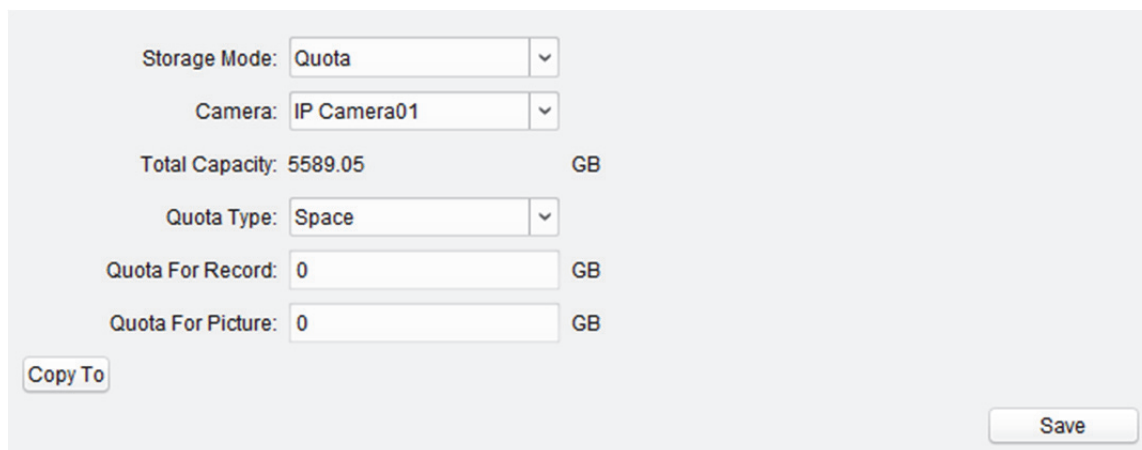
Paso 1: Haga clic sobre  en el panel de control, o acceda a **Tool > Device Management > Device > Hikvision Device**.

Paso 2: Seleccione el clúster desde **Device for Management**.

Paso 3: Acceda a **Remote Configuration > Advanced > Storage > General**.

Paso 4: Seleccione la opción **Quotas Type** en la lista desplegable.

- **Time:** La cuota del HDD para grabar vídeos o capturar imágenes se establecerá por tiempo (en días).
- **Space:** La cuota del HDD para grabar vídeos o capturar imágenes se establecerá por tiempo (en GB).



The screenshot displays a configuration window for storage settings. It includes the following elements:

- Storage Mode:** A dropdown menu set to "Quota".
- Camera:** A dropdown menu set to "IP Camera01".
- Total Capacity:** A text field showing "5589.05" followed by "GB".
- Quota Type:** A dropdown menu set to "Space".
- Quota For Record:** A text field set to "0" followed by "GB".
- Quota For Picture:** A text field set to "0" followed by "GB".
- Buttons:** A "Copy To" button on the left and a "Save" button on the right.

Figura 8 Tipo de almacenamiento

Paso 5: **Opcional:** Haga clic en **Copy To** para copiar el valor de cuota del HDD actual a otros HDD.

Paso 6: Haga clic en **Save**.

Consultar el estado del clúster


Propósito:

Podrá ver el estado del clúster mediante el software del cliente. Esto incluye la dirección IP del clúster, el espacio libre del disco, el ancho de banda entrante restante y otra información del estado de los NVR integrados. También podrá ver el estado.

Antes de empezar:

Cerciórese que se añadió el clúster usando el software del cliente y que el clúster esté en línea.



Paso 1: Haga clic sobre  en el panel de control, o acceda a **Tool > Device Management > Device > Hikvision Device**.

Paso 2: Seleccione el clúster desde **Device for Management**.

Paso 3: Haga clic en **Device Status**.

Paso 4: Haga clic en **Cluster Status**. Podrá ver la dirección IP del clúster, el espacio libre del disco, el ancho de banda entrante restante y otra información del estado de los NVR integrados.

The screenshot shows a window titled "Device Status" with the following content:

- Device: Cluster_1
- Buttons: Cluste..., Camer..., Free Disk Space Size: 0 MB/57231
- Total Remaining Incoming Bandwidth: 2299Mbps
- Table with columns: Device Name, Device Type, Running Status, CPU Status, Memory Status, Remaining Inc...
- Buttons: Refresh, Cancel

Device Name	Device Type	Running Status	CPU Status	Memory Status	Remaining Inc...
10.65.159.202	DS-96256NI-I16	Online	3%	61%	768
10.65.159.203	DS-96256NI-I16	Online	0%	60%	768
10.65.159.207	DS-96256NI-I16	Online	8%	59%	763

Figura 9 Estado del clúster

Opcional: Haciendo clic en **Camera Status** podrá ver el estado de la cámara, incluyendo el nombre de la cámara, el estado de grabación, el estado de la señal, etc.

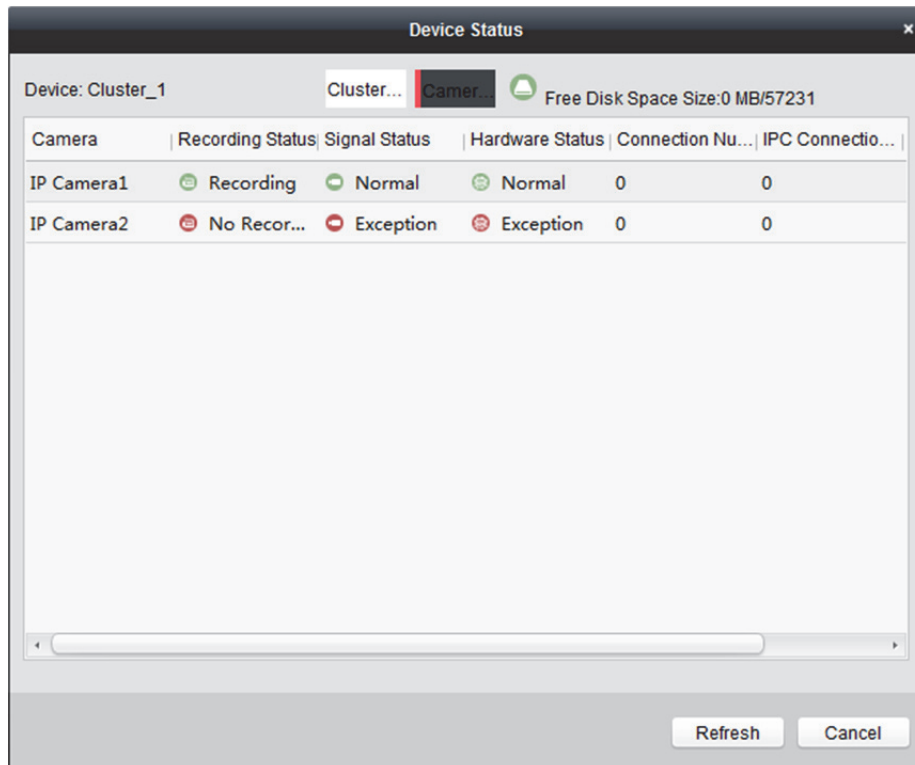


Figura 10 Estado de la cámara

Manejar las excepciones del clúster

El servidor anfitrión del clúster puede manejar los problemas de excepción en tiempo real. Los tipos de excepción del clúster incluyen almacenamiento del clúster lleno, desconexión del dispositivo, periodo de grabación insuficiente, fallo en la migración de la cámara IP, etc.

Paso 1: Abra el navegador web, escriba la dirección IP del clúster y pulse Intro.



NOTA

Use la dirección IP única del clúster y el número de puerto HTTP, por ejemplo: 192.168.1.64:8001.

Paso 2: Introduzca el nombre de usuario y la contraseña en la interfaz de inicio de sesión, y haga clic en **Login**.

Paso 3: Acceda a **Configuration > Event > Basic Event > Exception**.

Paso 4: Seleccione el tipo desde la lista desplegable **Exception Type**, por ejemplo, **Cluster storage is full** (almacenamiento del clúster está lleno).

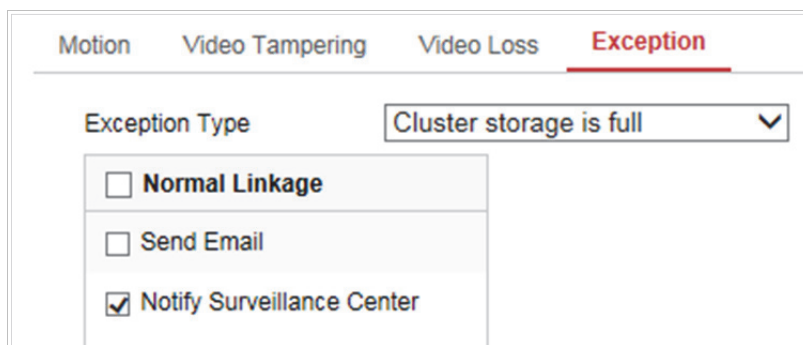


Figura 11 Excepción

Cluster storage is full: Cuando todos los HDD del clúster estén llenos, el servidor que esté trabajando como anfitrión informará de la excepción.

Device is offline: Cuando un NVR esté desconectado, el servidor que esté trabajando de anfitrión informará de la excepción.

Recording period is insufficient: Un periodo de grabación insuficiente puede ser ocasionado por diversos factores, como por ejemplo un cambio en la tasa de bits. Cuando la capacidad de almacenamiento de la cuota del HDD no es suficiente para las necesidades reales, el servidor que esté trabajando como anfitrión informará de la excepción e informará al usuario para que reconfigure la cuota. Mientras tanto, mostrará la capacidad del HDD y la capacidad de almacenamiento de cuota necesaria.

IPC migration failed: Cuando un NVR está desconectado, la carga de ese NVR será reasignada a otros NVR del clúster. Si hay un fallo en la migración de la cámara IP, el servidor que esté trabajando de anfitrión informará de la excepción.

Paso 5: Marque el tipo de vinculación normal, por ejemplo, **Send Email** y **Notify Surveillance Center**.




NOTA


- Si marca la opción de enviar correo electrónico, acceda a **Configuration > Network > Advanced Settings > Email** para configurar los parámetros del correo electrónico.
- Si marca la opción **Notify Surveillance Center**, asegúrese de tener habilitado el armado de alarma para el clúster mediante el software cliente de iVMS-4200 (**Tool > Device Arming Control**), de lo contrario no podrá enviar la señal de excepción.


Paso 6: Haga clic en **Save**.





www.rosarioseguridad.com.ar


 ventas@rosarioseguridad.com.ar

 +54 9 341 6708000

 +54 9 341 6799822


 [rosarioseguridadok](https://www.instagram.com/rosarioseguridadok)


 Rosario Seguridad

 Rosario Seguridad

Grupo Instaladores

 <https://www.facebook.com/groups/591852618012744/>

 +54 9 341 6591429

 +54 9 341 4577532

Avenida Presidente Perón 3998 - Rosario - Santa Fe - Argentina