

**SONY®**

OPTICAL DISC ARCHIVE FILE MANAGER2

# **ODS-FM2**



Optical Disc Archive

INSTALLATION GUIDE Spanish

1st Edition (Revised 2)

## **Marcas comerciales**

- Microsoft, Windows, Internet Explorer y Microsoft Edge son marcas comerciales registradas de Microsoft Corporation en Estados Unidos y/o en otros países.
- Intel y Intel Core son marcas comerciales o marcas comerciales registradas de Intel Corporation en Estados Unidos y en otros países.
- Apple, macOS, OS X y Safari son marcas comerciales de Apple Inc., registradas en Estados Unidos y otros países.
- Chrome es una marca registrada de Google Inc.
- SmartDocs es una marca comercial de Teknowmics Co., Ltd.
- Los productos o nombres de sistemas que aparecen en este documento son marcas comerciales o marcas comerciales registradas de sus respectivos propietarios.

---

# Tabla de contenidos

<b>Características</b> .....	<b>4</b>
Configuraciones del sistema .....	4
<b>Entorno de funcionamiento</b> .....	<b>6</b>
Equipo de control .....	6
Equipo de cliente.....	6
Precauciones sobre redes.....	6
<b>Configuración</b> .....	<b>7</b>
Configuración del dispositivo con sistema de archivo en disco óptico .....	7
Configuración de ODS-FM2.....	8
Configuración del firewall .....	13
Configuración de comunicaciones HTTPS.....	14
<b>Visualización de la aplicación web</b> .....	<b>16</b>

# Características

ODS-FM2 es un software de aplicación para archivar y recuperar datos mediante un sistema de archivo en disco óptico. Este software se utiliza no solo para administrar cartuchos insertados en el sistema de archivo en disco óptico, sino también para administrar cartuchos en estanterías.

Las operaciones del ODS-FM2 se realizan mediante una aplicación web. Se accede a la aplicación a través de un navegador web desde un equipo de cliente.

La Guía de instalación describe el procedimiento de instalación del software para realizar la configuración a través de una conexión de red a la ODS-L10 o ODS-L30M<sup>1)</sup> y a través de una unidad de disco conectada directamente a un ordenador.

1) Las unidades ODS-L60E y ODS-L100E también se pueden conectar.

## Configuraciones del sistema

Las configuraciones básicas del sistema para utilizar ODS-FM2 se muestran a continuación.

El ordenador en el que está instalado ODS-FM2 se denomina "equipo de control". El equipo de control se

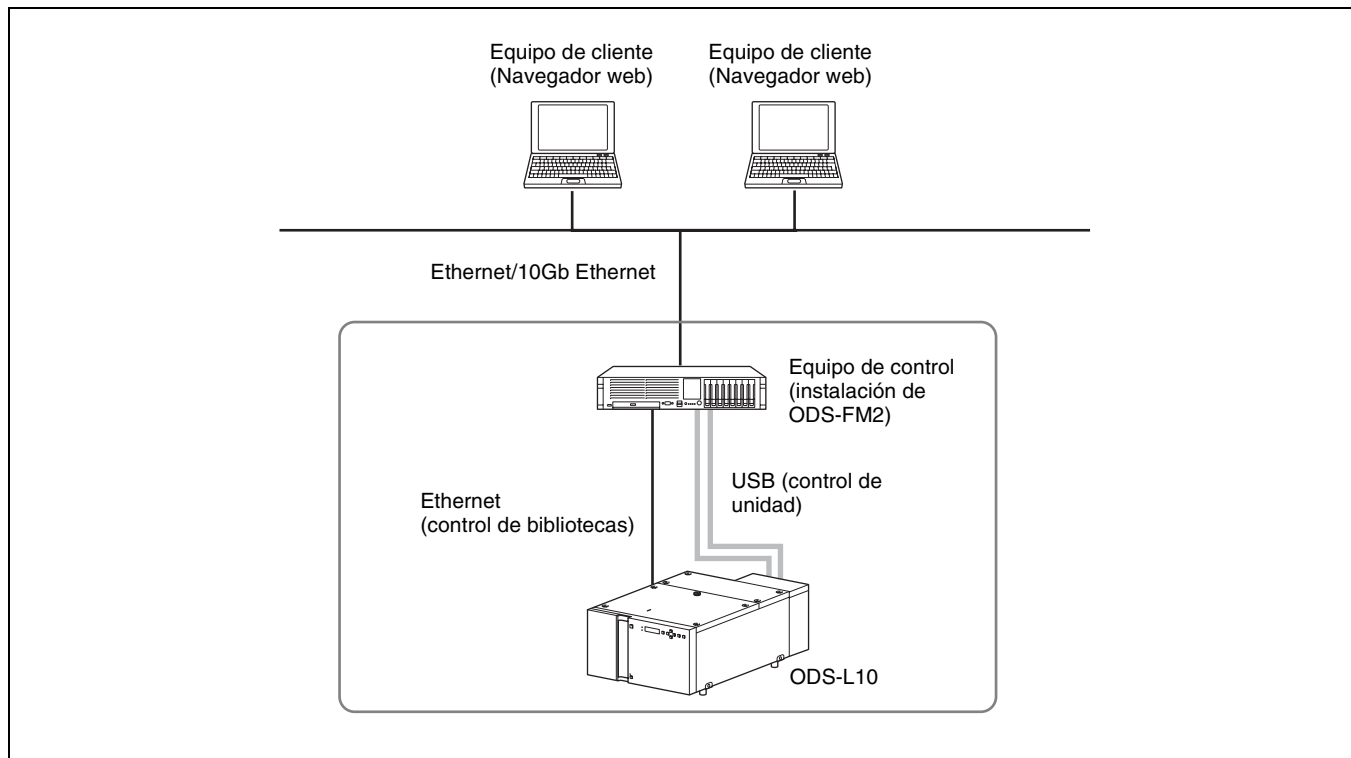
conecta al sistema de archivo en disco óptico para controlar dicho sistema. Puede utilizar la ODS-FM2 si accede al equipo de control mediante un navegador web en un equipo de cliente.

### Conexión a ODS-L10

El equipo de control se conecta a la red en la que está la ODS-L10 y a la red donde están los equipos de cliente y el almacenamiento de red. Además, el equipo de control se conecta a cada unidad de disco instalada en la ODS-L10 a través de un USB.

#### Nota

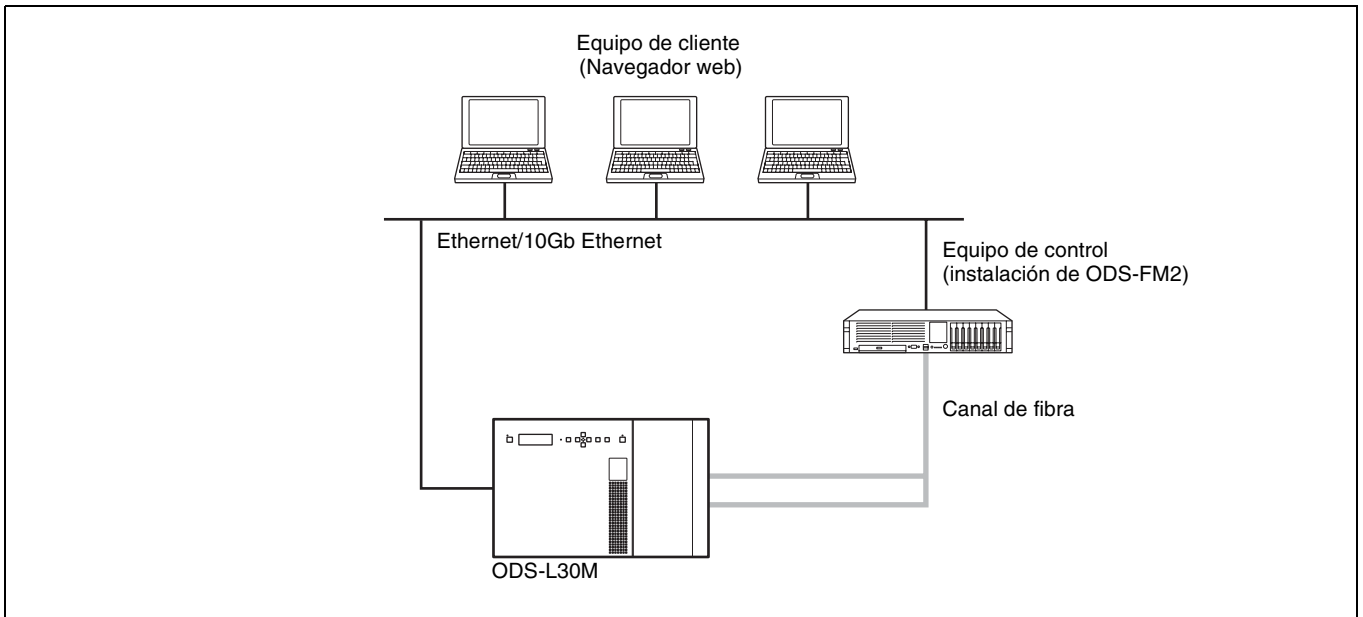
El modo Virtual Tape no está disponible cuando se conecta a la unidad ODS-L10.



## Conexión a ODS-L30M

La unidad de disco instalada en el ODS-L30M y el equipo de control (servidor) se conectan a través de un canal de fibra.

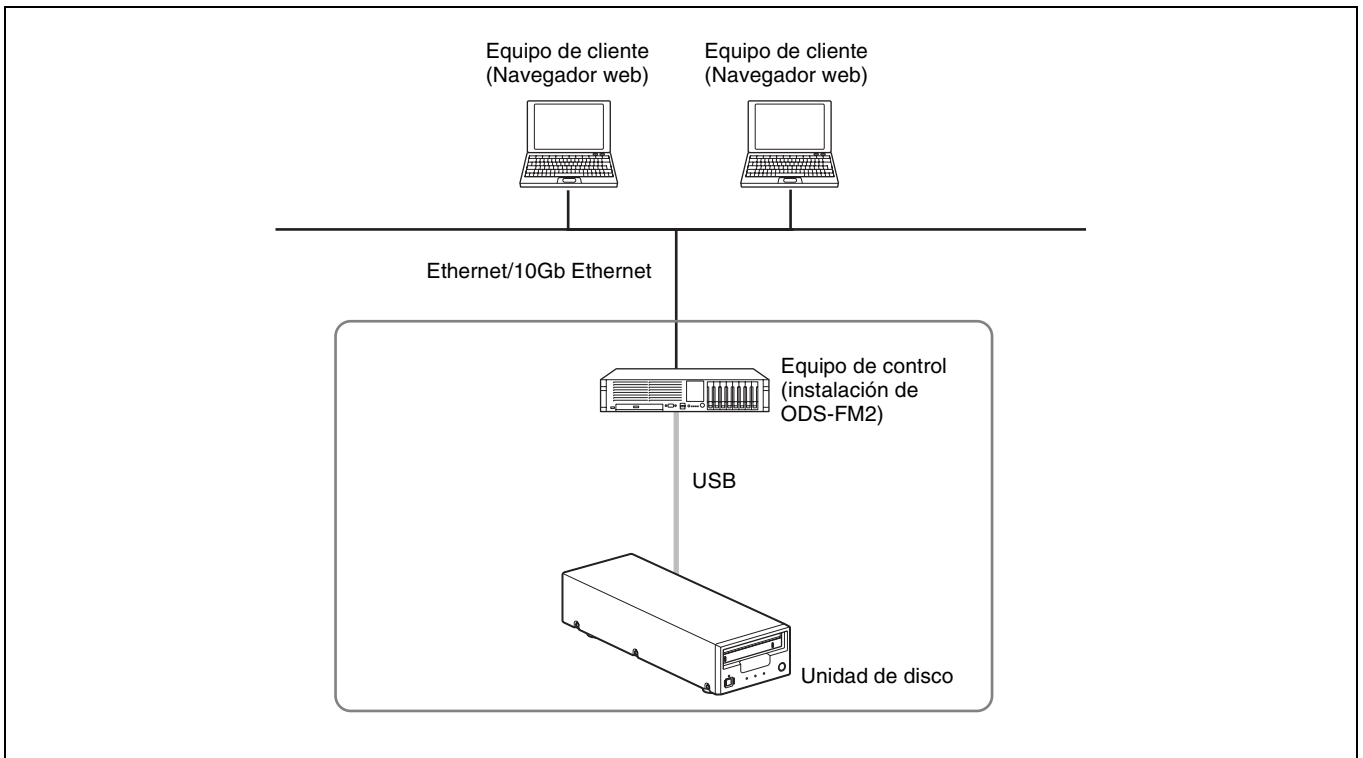
La red y los equipos de cliente de conexión se conectan al equipo de control mediante Ethernet.



## Conexión directa a una unidad de disco

El equipo de control se conecta directamente a cada unidad de disco a través de un USB. Además, el equipo de control

se conecta a la red donde están los equipos de cliente y el almacenamiento de red.



---

# Entorno de funcionamiento

A continuación se describen los entornos de funcionamiento requeridos para el equipo de control y los equipos de cliente.

---

## Equipo de control

El entorno de funcionamiento requerido varía en función del modo de funcionamiento seleccionado. Los requisitos de memoria y disco duro son valores que no incluyen el espacio necesario para Optical Disc Archive Software.

### Modo File Manager

CPU Intel Core i5 de 3 GHz o superior  
Memoria 8 GB  
Capacidad del disco duro 200 GB  
(Se requiere una capacidad adicional de 4 TB por unidad para guardar archivos desde el disco duro local o para recuperar el disco duro local)

#### SO

- Conexión de la ODS-L10 o unidad de disco:  
Windows 10, 64 bits
- Conexión de la ODS-L30M:  
Windows Server 2012  
Windows Server 2012 R2  
Windows Server 2016  
Windows Server 2019

#### Interfaz

- Conexión de la ODS-L10:  
Ethernet × 2 puertos (para conectarse al equipo de cliente y a la ODS-L10)  
Puertos USB (uno para cada unidad)
- Conexión de la ODS-L30M:  
Ethernet × 1 puerto (para conectarse al equipo de cliente y a la ODS-L30M)  
Adaptador de bus de host (HBA) del canal de fibra
- Conexión directa de unidad de disco:  
Ethernet × 1 puerto (para conectarse al equipo de cliente)  
Puertos USB (uno para cada unidad)

### Modo File Server

CPU Intel Core i5 de 3 GHz o superior  
Memoria 16 GB  
Capacidad del disco duro 200 GB + 4 TB por unidad  
SO Windows Server 2012  
Windows Server 2012 R2  
Windows Server 2016  
Windows Server 2019

#### Interfaz

- Conexión de la ODS-L10:  
Ethernet × 2 puertos (para conectarse al equipo de cliente y a la ODS-L10)  
Puertos USB (uno para cada unidad)
- Conexión de la ODS-L30M:  
Ethernet × 1 puerto (para conectarse al equipo de cliente y a la ODS-L30M)  
Adaptador de bus de host (HBA) del canal de fibra
- Conexión directa de unidad de disco:  
Ethernet × 1 puerto (para conectarse al equipo de cliente)  
Puertos USB (uno para cada unidad)

### Modo Virtual Tape

CPU Intel Core i5 de 3 GHz o superior  
Memoria 4 GB  
Capacidad del disco duro N/D (espacio necesario solo para Optical Disc Archive Software)  
SO Windows Server 2012 R2  
Windows Server 2016  
Windows Server 2019

#### Interfaz

- Conexión de la ODS-L30M:  
Ethernet × 1 puerto (para conectarse al equipo de cliente y a la ODS-L30M)  
Adaptador de bus de host (HBA) del canal de fibra
- Conexión directa de unidad de disco:  
Ethernet × 1 puerto (para conectarse al equipo de cliente)  
Puertos USB (uno para cada unidad)

#### Nota

Para obtener más información sobre la interfaz USB compatible con cada unidad de disco, consulte el manual de funcionamiento de la unidad de disco.

---

## Equipo de cliente

Hardware Hardware compatible con los siguientes SO y navegadores web sin problemas.  
SO Windows 7, Windows 8.1, Windows 10  
macOS 10.13, 10.14, 10.15  
Navegador web Microsoft Internet Explorer 11, Microsoft Edge, Google Chrome, Safari 11/12/13

---

## Precauciones sobre redes

En función del entorno de uso, cualquier software de terceros no deseado podría acceder a esta aplicación a través de la red. Conéctese a una red segura.

# Configuración

En esta sección se describe el procedimiento de configuración para instalar ODS-FM2 en el equipo de control para utilizar un sistema de archivo de disco óptico mediante ODS-FM2.

## Notas

- Actualice el firmware ODS-L10/ODS-L30M a la versión más reciente.
- Actualice Optical Disc Archive Software y el firmware de las unidades de disco a las versiones más recientes.

## Configuración del dispositivo con sistema de archivo en disco óptico

### Si el equipo de control se conecta a la ODS-L10

Para obtener más información acerca del funcionamiento de la ODS-L10, consulte el Manual de instalación y el Manual de funcionamiento de ODS-L10.

- 1 Instale la unidad de disco en la ODS-L10.  
Se pueden instalar hasta dos unidades ODS-D55U u ODS-D77U en la ODS-L10. La unidad ODS-D280U/D380U, así como otros modelos que usan canal de fibra, no se pueden instalar.
- 2 Establezca la dirección IP de ODS-L10.  
*Para obtener más información acerca del método de configuración, consulte el Manual de funcionamiento de ODS-L10.*
- 3 Instale Optical Disc Archive Software en el equipo de control (equipo en el que instalar ODS-FM2).
- 4 Instale ODS-FM2 en el equipo de control.  
Instale el software siguiendo las instrucciones del instalador.
- 5 Conéctese a la unidad de disco, instalada en ODS-L10, y el equipo de control mediante un cable USB.  
Si hay dos unidades de disco instaladas, conecte ambas unidades en el equipo de control.
- 6 Conéctese a la red con la ODS-L10 en el puerto de red de disco en el equipo de control.  
Para obtener más información acerca de la configuración de red, consulte la documentación de Windows.

- 7 Introduzca cartuchos de disco óptico en la unidad ODS-L10.

### Si el equipo de control se conecta a la ODS-L30M

Para obtener más información acerca del funcionamiento de la ODS-L30M, consulte el Manual de funcionamiento de la ODS-L30M.

- 1 Instale la unidad de disco ODS-D77F/D280F/D380F en la ODS-L30M.

Se puede instalar una combinación de hasta dos unidades ODS-D77F/D280F/D380F en la ODS-L30M. Si desea instalar tres unidades o más, consúltelo con su representante de Sony.

## Nota

En las configuraciones que contengan una mezcla de unidades ODS-D77F, ODS-D280F y ODS-D380F, el modo Virtual Tape no podrá utilizarse. Para usar el modo Virtual Tape, elija una configuración que contenga solo unidades de un único modelo.

- 2 Establezca la dirección IP de la ODS-L30M.  
*Para obtener más información acerca del método de configuración, consulte el Manual de funcionamiento de la ODS-L30M.*
- 3 Instale Optical Disc Archive Software en el equipo de control.
- 4 Instale ODS-FM2 en el equipo de control.  
Instale el software siguiendo las instrucciones del instalador.
- 5 Conecte la unidad de disco, instalada en la ODS-L30M, a un conmutador de canal de fibra.  
Si hay dos unidades de disco instaladas, conecte ambas unidades de disco al conmutador de canal de fibra.
- 6 Conecte el equipo de control al conmutador de canal de fibra.
- 7 Introduzca cartuchos de disco óptico en la unidad ODS-L30M.

### Si el equipo de control se conecta directamente a la unidad de disco

- 1 Instale Optical Disc Archive Software en el equipo de control.
- 2 Instale ODS-FM2 en el equipo de control.  
Instale el software siguiendo las instrucciones del instalador.

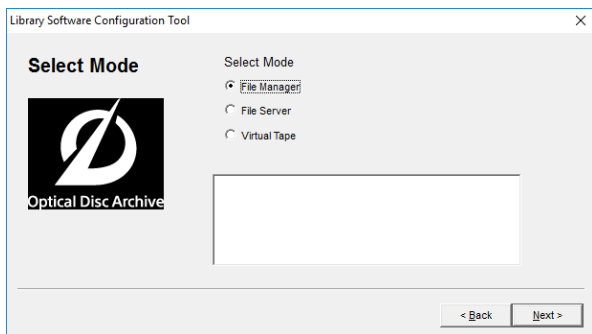




Si selecciona el modo File Manager, vaya a “Ajustes comunes a todos los modos” (página 12).

### Notas

- Si se selecciona [ODS-L10] en el paso 4, no podrá seleccionarse el modo Virtual Tape.
- Para seleccionar el modo Virtual Tape, salga de la aplicación que accede la Virtual Tape antes de hacer clic en [Next]. Al seleccionar el modo Virtual Tape y hacer clic en [Next], se mostrará un cuadro de diálogo de advertencia, independientemente de si la aplicación que accede a Virtual Tape ha terminado de cerrarse.

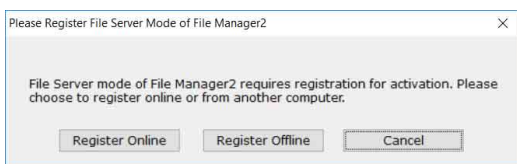


## Configuración del modo File Server

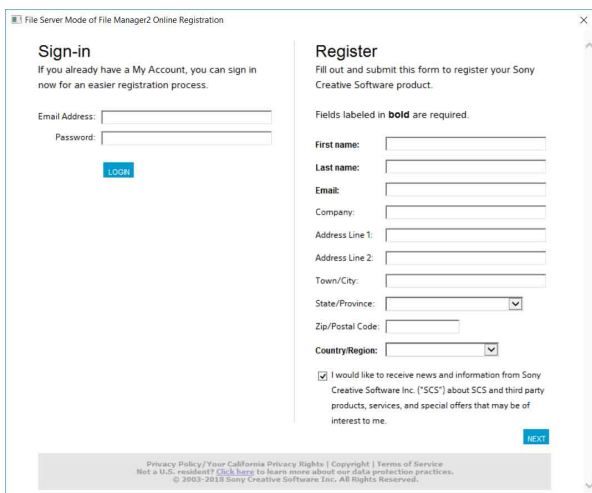
- 1 Active la licencia si aún no se ha activado la licencia del modo File Server.

### Si el equipo de control está conectado a Internet

- ① Haga clic en [Register Online].



- ② Introduzca los elementos necesarios y, a continuación, haga clic en [Next].

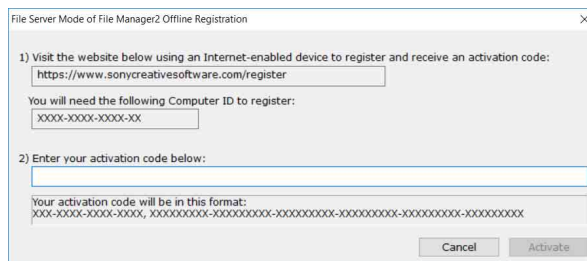


- ③ Introduzca el número de serie y, a continuación, haga clic en [Next].

Se activa la licencia del modo File Server.

### Si el equipo de control no está conectado a Internet

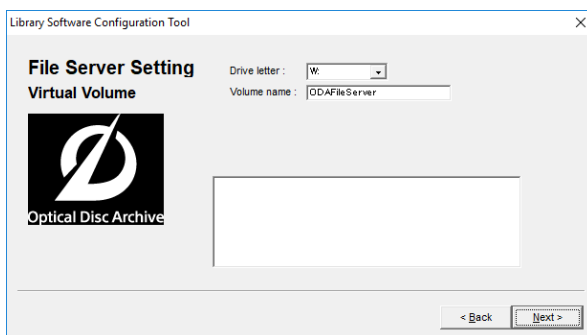
- ① Haga clic en [Register Offline].
- ② Introduzca la URL que se muestra en el cuadro de diálogo [Library Software Offline Registration] en un navegador web en otro equipo que esté conectado a Internet para mostrar la página web.



- ③ Introduzca y envíe el número de serie y la ID del ordenador (que se muestra en el cuadro de diálogo [Library Software Offline Registration]) en la página web para adquirir el código de activación.

- ④ Introduzca el código de activación en el cuadro de diálogo [Library Software Offline Registration] en el equipo de control y, a continuación, haga clic en [Activate].  
Se activa la licencia del modo File Server.

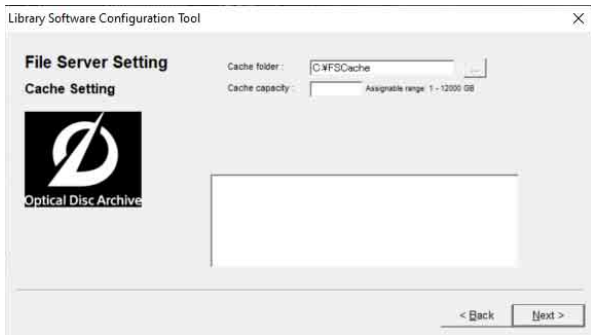
- 2 Seleccione la letra de la unidad del servidor de archivos en la pantalla File Server Setting y especifique la etiqueta de volumen.



- 3 Después de ajustar el volumen, haga clic en [Next].

- 4 Configure la carpeta y la capacidad de la caché para el servidor de archivos.

El servidor de archivos guardará temporalmente los archivos de escritura en la carpeta de caché.



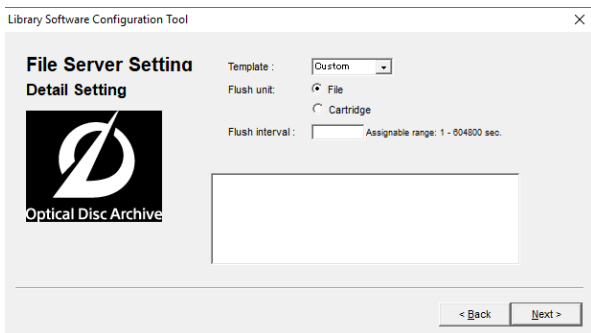
Cache folder: establezca la carpeta que se usará como carpeta de caché.

Cache capacity: establezca el tamaño máximo del almacenamiento de archivos en la caché.

### Nota

Se recomienda que prepare un disco o partición dedicado para la ruta de la carpeta de la caché de forma que ninguna otra aplicación utilice el volumen.

- 5 Después de establecer la carpeta y capacidad de caché, haga clic en [Next].
- 6 Establezca la configuración de detalles del servidor de archivos.



Template: seleccione la plantilla de configuración de la aplicación con el servidor de archivos. Para realizar la configuración manual, seleccione [Custom].

Flush unit: establece si el proceso de sincronización para la escritura de la caché al cartucho se produce en unidades de archivo o de cartucho.

- File: el tiempo desde que se actualizó por última vez un archivo antes de borrar la caché se administra para cada archivo. Cuando el valor alcanza el ajuste de [Flush interval], se registra un trabajo de archivado para sincronizar dicho archivo.
- Cartridge: el tiempo desde que se actualizó por última vez un archivo antes de borrar la caché se administra para cada cartucho. Cuando el valor alcanza el ajuste de [Flush interval], se registra un trabajo de archivado para sincronizar todos los archivos actualizados.

Flush interval: establece el tiempo desde que finaliza la escritura de un archivo en un volumen virtual o desde la última vez que se actualizó un archivo

hasta que el archivo en la caché se sincroniza con un cartucho.

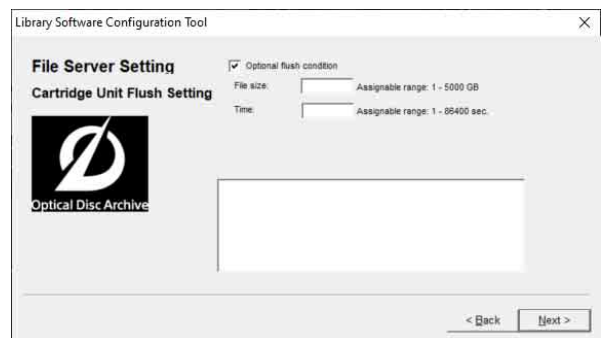
- 7 Después de establecer las propiedades de la caché, haga clic en [Next].

Si se selecciona [Cartridge] en [Flush unit], vaya al paso 8.

Si se selecciona [File] en [Flush unit] y [SmartDocs] en [Template], vaya al paso 10.

Si se selecciona [File] en [Flush unit] y [Custom] en [Template], vaya a “Ajustes comunes a todos los modos” (página 12).

- 8 Establezca las propiedades para cuando se borre por unidades de cartucho.



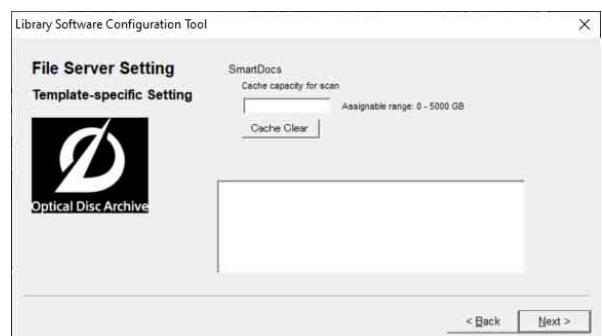
Optional flush condition: este ajuste solo es válido cuando se borran unidades de cartucho. Si está habilitado, además del registro normal de trabajo de archivado en [Flush interval], se puede realizar una sincronización más rápida según el tamaño total de los archivos que se van a actualizar. Cuando el tamaño total de los archivos que se van a sincronizar supera el ajuste de [File size] y los archivos no se han escrito o actualizado durante un tiempo determinado por [Time], se registra un trabajo de archivado para sincronizar los archivos.

- 9 Tras establecer las propiedades para cuando se borre por unidades de cartucho, haga clic en [Next].

Si se selecciona [SmartDocs] en [Template], vaya al paso 10.

Si se selecciona [Custom] en [Template], vaya a “Ajustes comunes a todos los modos” (página 12).

- 10 Especifique los ajustes específicos de la plantilla.





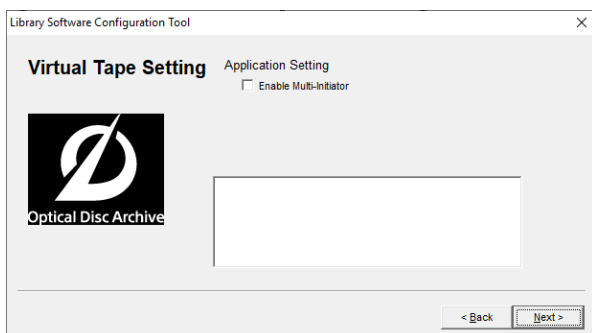
Enable CHAP: marque la casilla de verificación para permitir la autenticación de usuarios mediante CHAP.

Target CHAP Name: nombre de usuario utilizado para la autenticación. Introduzca una cadena de caracteres ASCII (sin caracteres de control) de entre 1 y 256 caracteres.

Target CHAP Secret: contraseña usada para la autenticación. Introduzca una cadena de caracteres ASCII (sin caracteres de control) de entre 12 y 16 caracteres.

**5** Después de configurar la aplicación y el protocolo CHAP, haga clic en [Next].

**6** Habilite o deshabilite el ajuste de iniciadores múltiples.



Si [Enable Multi-Initiator] está habilitado, se habilitan las conexiones de sincronización desde múltiples clientes. Si está deshabilitado, otros clientes no pueden conectarse si ya hay un cliente conectado.

**7** Después de establecer el ajuste de iniciador múltiple, haga clic en [Next].

A continuación, vaya a “Ajustes comunes a todos los modos”.

## Ajustes comunes a todos los modos

**1** Haga clic en [Next] en la pantalla Database Initialization.

La inicialización de la base de datos se realiza automáticamente. Si se selecciona “Direct Mode” u “ODS-L30M” en la pantalla Select System, vaya al paso **5**. Si se selecciona “ODS-L10”, vaya al siguiente paso.

**2** Introduzca la dirección de IP configurada en la ODS-L10 y la id, de inicio de sesión (el nombre de usuario) y contraseña para iniciar sesión en ODS-L10 y, a continuación, haga clic en [Next].

El equipo se conecta a la ODS-L10. Si la conexión se realiza correctamente, aparece la página Drive Setting.

**3** Si una unidad de disco se conecta al equipo de control pero no se instala en la ODS-L10, desconéctela del

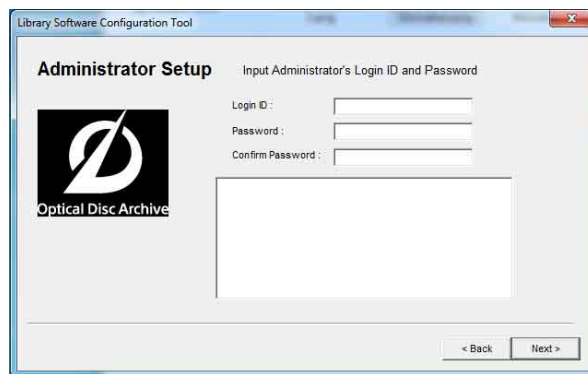
equipo de control para realizar una comprobación de la unidad.

**4** Haga clic en [Next].

La comprobación de la unidad se inicia. Si solo hay una unidad de disco instalada en la ODS-L10, aparecerá un mensaje de confirmación preguntándole si está ubicada en la ranura inferior o superior. Si está instalada en la ranura inferior, haga clic en [Yes]. Si está instalada en la ranura superior, haga clic en [No]. Cuando la comprobación de la unidad se complete, aparecerá la pantalla de Administrator Setup.

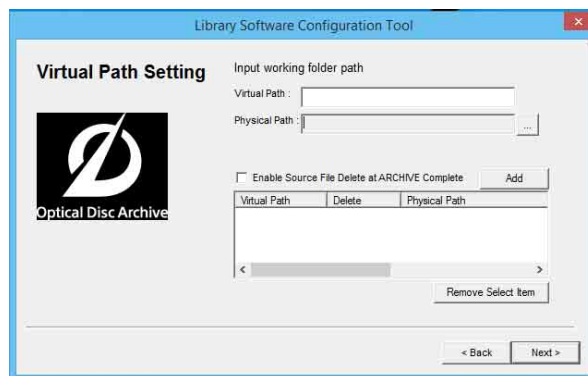
**5** Cree una cuenta para utilizarla cuando inicie sesión en ODS-FM2. Introduzca la id, de inicio de sesión y la contraseña y, a continuación, haga clic en [Next].

Al seleccionar el modo File Manager, establezca la carpeta raíz (ruta básica) en los pasos **6** y **7**. Cuando haya seleccionado el modo File Server o Virtual Tape, vaya al paso **8**.



**6** Especifique la carpeta de raíz (ruta de acceso base) que se visualizará en la pantalla Archivo de la unidad ODS-FM2.

Solo los archivos y carpetas en la ruta de acceso base especificada se mostrarán en la pantalla Archivo. Si se restringen las carpetas que se muestran se evitará que los archivos del sistema se modifiquen por error. Pueden especificarse varias rutas de acceso base.



Virtual Path: especifique un nombre para la ruta de acceso base que se visualizará en la pantalla Archivo.

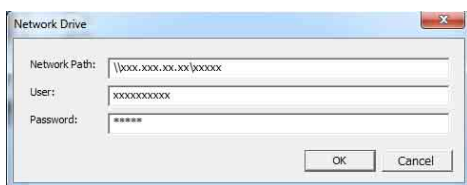
Physical Path: especifique la ruta física para que se visualice la ruta de acceso base. También puede especificar una unidad de red.

Enable Source File Delete at ARCHIVE Complete: seleccione si eliminar automáticamente el archivo una vez archivado. Si no se selecciona, el archivo se mantiene una vez archivado y deberá borrarse manualmente cuando ya no se necesite.

Botón Add: Añade la ruta de acceso de base con la configuración especificada. La ruta de acceso de base especificada se añade a la lista inferior.

### Para asignar una unidad de red

- 1 Haga clic en el botón [...] en el elemento [Physical Path].
- 2 Haga clic en el botón [Network Drive] en el cuadro de diálogo [Reference].
- 3 Introduzca la ruta de la unidad de red en formato UNC (\\nombre\_servidor o dirección\_IP\ nombre\_carpeta) en [Network Path] en el cuadro de diálogo [Network Drive].



- 4 Si es necesario, introduzca un nombre de usuario y contraseña en [User] y [Password] respectivamente.
  - 5 Haga clic en el botón [OK]. La unidad de red añadida aparece en el cuadro de diálogo [Reference].
  - 6 Seleccione la unidad de red y haga clic en el botón [Select]. El cuadro de diálogo [Reference] se cierra y la ruta de la unidad de red seleccionada aparece en el elemento [Physical Path] en la página Virtual Path Setting.
  - 7 Especifique la [Virtual Path] y haga clic en el botón [Add].
- 7** Después de ajustar la(s) ruta(s) de acceso de base, haga clic en [Next].
- 8** Cuando aparezca el cuadro de diálogo, haga clic en [Finish].
- 9** Conecte la red donde están los equipos de cliente a un puerto de red en el equipo de control.

Si está utilizando una conexión de red a la ODS-L10, conecte los equipos de cliente a una red que no sea la de ODS-L10.

El sistema de archivo en disco óptico puede utilizarse ahora mediante la aplicación web desde un equipo de cliente.

### Notas

- Si tiene instalado un software antivirus o un software de seguridad en el equipo de control, es posible que el acceso de entrada al puerto 8080 de un equipo de cliente se bloquee. En este caso, configure su software de seguridad para que permita el acceso de entrada al puerto 8080. Para obtener más información acerca de la configuración, consulte el manual de instrucciones de su software de seguridad.
- Si se modifica la configuración del hardware o la conexión de la unidad de disco, ODS-FM2 no funcionará correctamente. Si esto ocurre, vuelva a configurar los ajustes de la ODS-FM2 mediante Library Software Configuration Tool.
- Si se modifica la configuración del ODS-L10 u ODS-L30M en el menú Setup de la página web o en la pantalla del panel frontal de la unidad, vuelva a configurar ODS-FM2 mediante Library Software Configuration Tool.
- Optical Disc Archive Filer no se puede iniciar cuando se utiliza ODS-FM2. Para utilizar Optical Disc Archive Filer, finalice primero el servicio ODS-FM2 y, a continuación, inicie Optical Disc Archive Filer. (Optical Disc Archive Filer se incluye con Optical Disc Archive Software).

## Configuración del firewall

Se recomiendan los siguientes ajustes de firewall para bloquear las conexiones a MariaDB desde una fuente externa.

- 1 Seleccione [Panel de control] > [Sistema y seguridad] > [Firewall de Windows] > [Configuración avanzada] > [Reglas de entrada] > [Nueva regla...].
- 2 Configure las siguientes opciones en el Asistente para nueva regla de entrada.
  - Tipo de regla: seleccione [Puerto].
  - Protocolo y puertos: seleccione [TCP] y [Puertos locales específicos] (introduzca el puerto “3306”).
  - Acción: seleccione [Bloquear la conexión].
  - Perfil: seleccione todo.
  - Nombre: introduzca el nombre “MariaDBPort”.
- 3 Haga clic en [Finalizar].
- 4 Vuelva a seleccionar [Nueva regla...] para visualizar el Asistente para nueva regla de entrada y configure las siguientes opciones.
  - Tipo de regla: seleccione [Puerto].
  - Protocolo y puertos: seleccione [UDP] y [Puertos locales específicos] (introduzca el puerto “3306”).
  - Acción: seleccione [Bloquear la conexión].
  - Perfil: seleccione todo.
  - Nombre: introduzca el nombre “MariaDBPort”.
- 5 Haga clic en [Finalizar].

## Configuración de comunicaciones HTTPS

Es posible cifrar las comunicaciones estableciendo una comunicación HTTPS.

### Generación de un archivo de Keystore

**1** Ejecute [Símbolo del sistema].

**2** Introduzca el siguiente comando.

```
cd C:\Program Files\Zulu\zulu-8-jre\bin
keytool -genkey -alias tomcat -keyalg RSA -keysize
2048 -keystore <nombrearchivo_keystore>
```

**Ejemplo de nombre de archivo de Keystore:**  
filemanager2.keystore

**3** Introduzca una contraseña cuando se le solicite establecer una contraseña de Keystore.

Enter keystore password: \*\*\*\*\*  
(La contraseña no se muestra)

**4** Vuelva a introducir la misma contraseña cuando se le solicite.

Re-enter new password: \*\*\*\*\*  
(La contraseña no se muestra)

**5** Introduzca la información de la solicitud de firma de certificado (CSR).

Ejemplo:

```
What is your first and last name?
[Unknown]: www.sony.jp
What is the name of your organizational unit?
[Unknown]: File Manager2
What is the name of your organization?
[Unknown]: Sony Imaging Products & Solutions Inc.
What is the name of your City or Locality?
[Unknown]: Minato-ku
What is the name of your State or Province?
[Unknown]: Tokyo
What is the two-letter country code for this unit?
[Unknown]: JP
```

**6** Compruebe el contenido mostrado de la información introducida y, a continuación, escriba “yes”.

```
Is CN=www.sony.jp, OU=File Manager2, O=Sony Imaging
Products & Solutions Inc., L=Minato-ku, ST=Tokyo, C=JP correct?
[no]: yes
```

**7** Pulse la tecla Return (Enter) sin escribir nada cuando aparezca el siguiente mensaje.

Enter key password for (RETURN if same as keystore password):  
Se genera un archivo de Keystore con el nombre especificado en el paso **2**.

### Generación de un CSR

**1** Ejecute [Símbolo del sistema].

**2** Introduzca el siguiente comando.

```
cd C:\Program Files\Zulu\zulu-8-jre\bin
keytool -certreq -sigalg SHA1withRSA -alias tomcat
-file <nombrearchivo_CSR> -keystore
<nombrearchivo_keystore>
```

**Ejemplo de nombre de archivo CSR:**  
filemanager2.csr

**3** Cuando se le solicite, introduzca la contraseña especificada al generar el archivo de Keystore.

Enter keystore password: \*\*\*\*\*  
Se genera un archivo CSR con el nombre especificado en el paso **2**.

### Emisión de un certificado de servidor

Haga llegar el CSR generado a una autoridad de certificación para que emita un certificado de servidor firmado.

### Generación de un certificado de servidor usado por aplicaciones

**1** Coloque el certificado de servidor firmado y el certificado intermedio en un directorio arbitrario.

**2** Ejecute [Símbolo del sistema].

**3** Combine el certificado de servidor firmado y el certificado intermedio en un solo archivo.

```
copy <nombrearchivo_certificado_firmado> +
<nombrearchivo_certificado_intermedio>
<nombrearchivo_certificado_servidor_utilizado_por
_aplicaciones>
```

**Ejemplo de nombre de archivo de certificado de servidor usado por aplicaciones:**  
filemanager2.cer

### Instalación de un certificado

**1** Introduzca el siguiente comando.

```
keytool -import -alias tomcat -keystore
<nombrearchivo_keystore> -file
<nombrearchivo_generado_en_paso3_de_sección
anterior>
```

**2** Cuando se le solicite, introduzca la contraseña especificada al generar el archivo de Keystore.

Enter keystore password: \*\*\*\*\*



### 3 Escriba “yes” si aparece el siguiente mensaje.

```
Top-level certificate in reply:
Owner: CN=*****, O=*****, C=**
Issuer: OU=*****, O=*****, C=**
Serial number: ****
Valid from: **** until: ****
Certificate fingerprints:
MD5: ****
... is not trusted. Install reply anyway? [no]: yes
```

Los asteriscos indican la visualización de información registrada.

## Habilitar HTTPS

### 1 Detenga el servicio de Tomcat.

- ① En el menú [Inicio], haga clic en [Herramientas administrativas de Windows] > [Servicios].
- ② Busque el servicio “Apache Tomcat” en la lista de servicios y haga clic en él.
- ③ Haga clic en [Detener el servicio] a la izquierda de la lista de servicios.

### 2 Edite el archivo de configuración de Tomcat (server.xml).

- ① Abra C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\server.xml y quite la marca de comentario del bloque en la línea 85.
- ② Copie el contenido que se muestra a continuación en “Después de editar”.
- ③ Introduzca la ruta completa del archivo de Keystore actual en `<nombrearchivo_keystore>` e introduzca la contraseña especificada al generar el archivo de Keystore en `<contraseña_keystore>`.

#### Antes de editar

```
<!--
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
-->
```

#### Después de editar

```
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11Protocol"
SSLEnabled="true"
maxThreads="150"
scheme="https"
secure="true"
keystoreFile="<nombrearchivo_keystore>"
keystorePass="<contraseña_keystore>"
clientAuth="false"
sslProtocol="TLSv1.2"
sslEnabledProtocols="TLSv1.1,TLSv1.2"
ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA384,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA"
/>
```

Para evitar las comunicaciones HTTP, comente el bloque en la línea 70 de la siguiente manera:

#### Antes de editar

```
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443"
useBodyEncodingForURI="true" />
```

#### Después de editar

```
<!--
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443"
useBodyEncodingForURI="true" />
-->
```

### 3 Inicie el servicio de Tomcat.

- ① En el menú [Inicio], haga clic en [Herramientas administrativas de Windows] > [Servicios].
- ② Busque el servicio “Apache Tomcat” en la lista de servicios y haga clic en él.
- ③ Haga clic en [Iniciar el servicio] a la izquierda de la lista de servicios.

### 4 Ejecute Config Tool.

## 5 Compruebe la comunicación HTTPS.

Ejecute un navegador web, acceda a “https://<nombre\_dominio>:8443” y compruebe que se muestra la pantalla de inicio de sesión.

---

# Visualización de la aplicación web

### **Si no se configura la comunicación HTTPS**

Visualice un navegador web en un equipo de cliente e introduzca “http://(dirección IP del equipo de control):8080/” en la barra de direcciones. Aparecerá la pantalla de inicio de sesión cuando el navegador web se conecte al equipo de control. Introduzca el nombre de usuario y la contraseña configurados en Library Software Configuration Tool para iniciar sesión.

### **Si se configura la comunicación HTTPS**

Abra una ventana del navegador web en el equipo de cliente e introduzca “http://<nombre\_dominio>:8443/” en la barra de direcciones.

Aparecerá la pantalla de inicio de sesión cuando el navegador web se conecte al equipo de control. Introduzca el nombre de usuario y la contraseña configurados en Library Software Configuration Tool para iniciar sesión.



