SONY

OPTICAL DISC ARCHIVE FILE MANAGER2

# ODS-FM2

Optical Disc Archive

INSTALLATION GUIDE English

1st Edition (Revised 2)

**NOTICE TO USERS**



## Trademarks

# Table of Contents

# Features

ODS-FM2 is a software application for archiving and retrieving using an Optical Disc Archive System. You use this software to manage not just cartridges inserted in the Optical Disc Archive System, but also cartridges in shelf management.
ODS-FM2 operations are performed using a web application. The application is accessed in a web browser from a client PC.

This Installation Guide describes the software installation procedure for both the configuration using a network connection to the ODS-L10 or ODS-L30M[1)] and the configuration where a drive unit is connected directly to a computer.

1) ODS-L60E and ODS-L100E units can also be connected.

## System Configurations

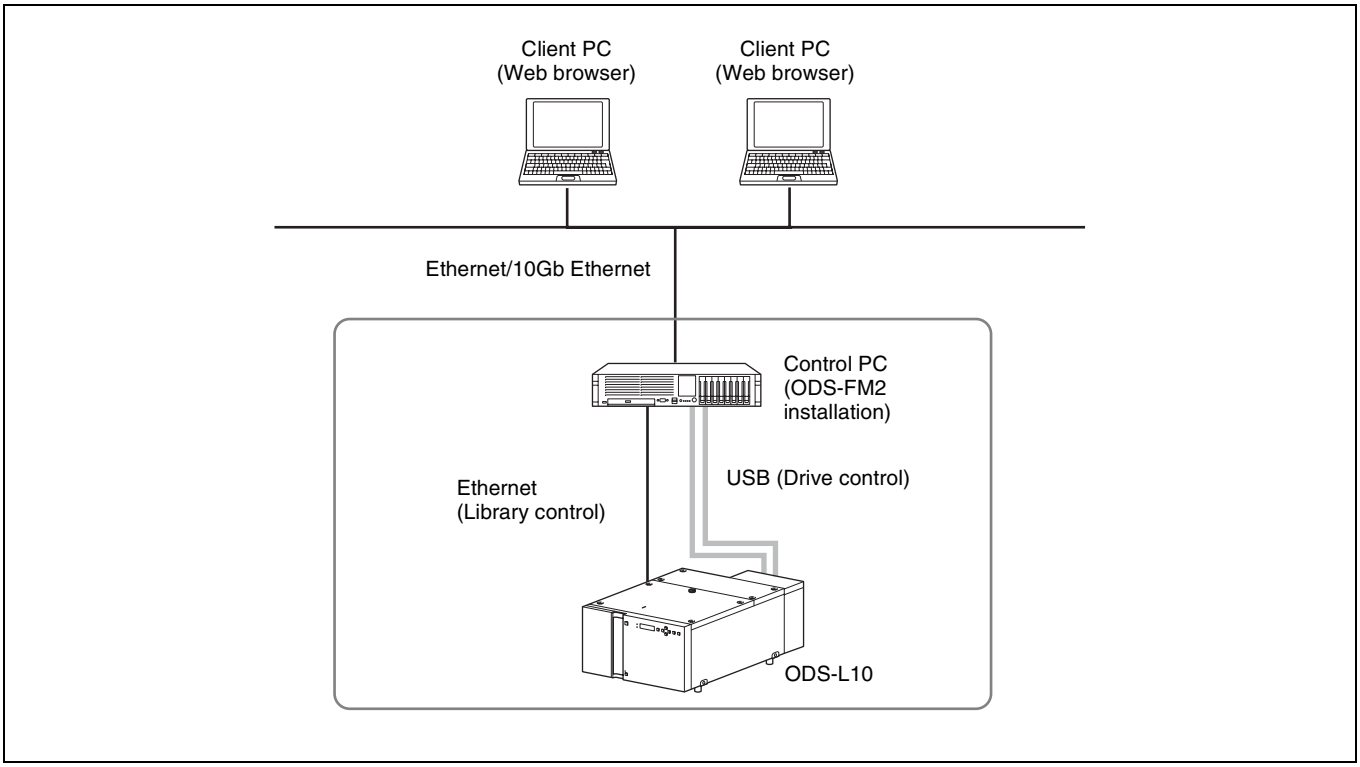
The basic system configurations for using ODS-FM2 are shown below.
The computer on which ODS-FM2 is installed is referred to as the “control PC.” The control PC connects to the Optical Disc Archive System in order to control the Optical Disc Archive System. You operate the ODS-FM2 by accessing the Control PC using a web browser on a client PC.

### Connection to ODS-L10

The control PC connects to both the network that the ODS-L10 is on and the network that the Client PCs and network storage are on. In addition, the control PC connects to each drive unit installed in the ODS-L10 using USB.

**Note**

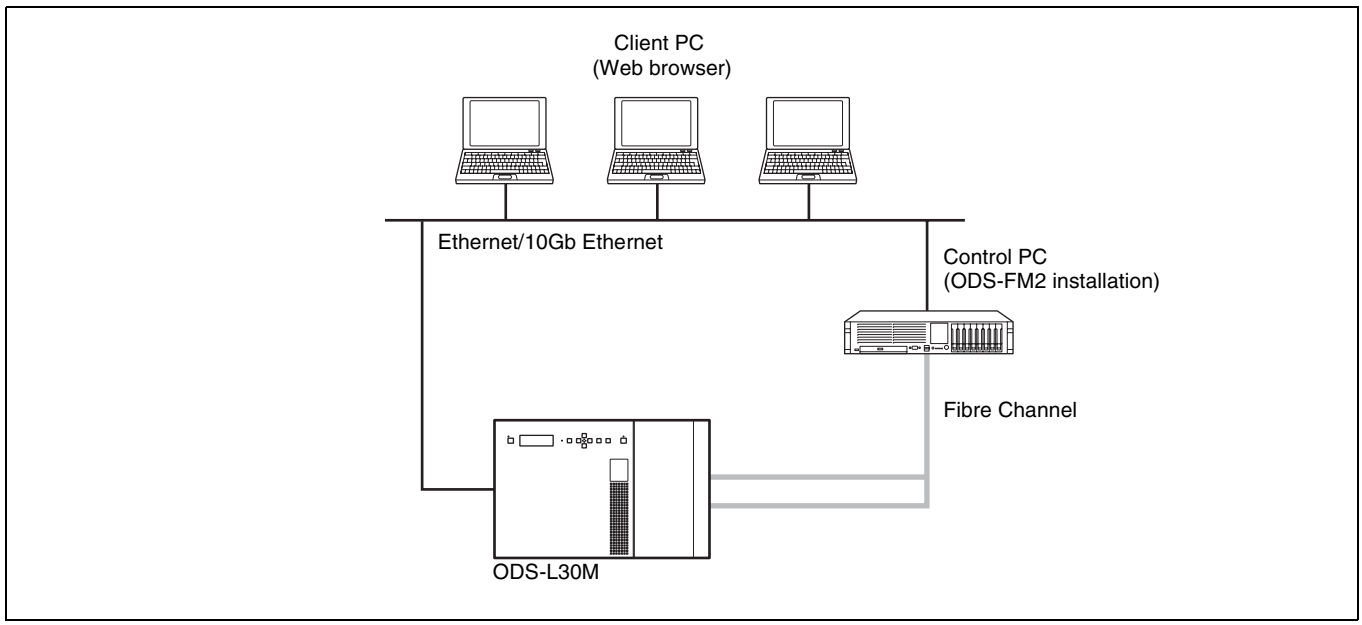
Virtual Tape mode is not available when connected to the ODS-L10.



## Connection to ODS-L30M

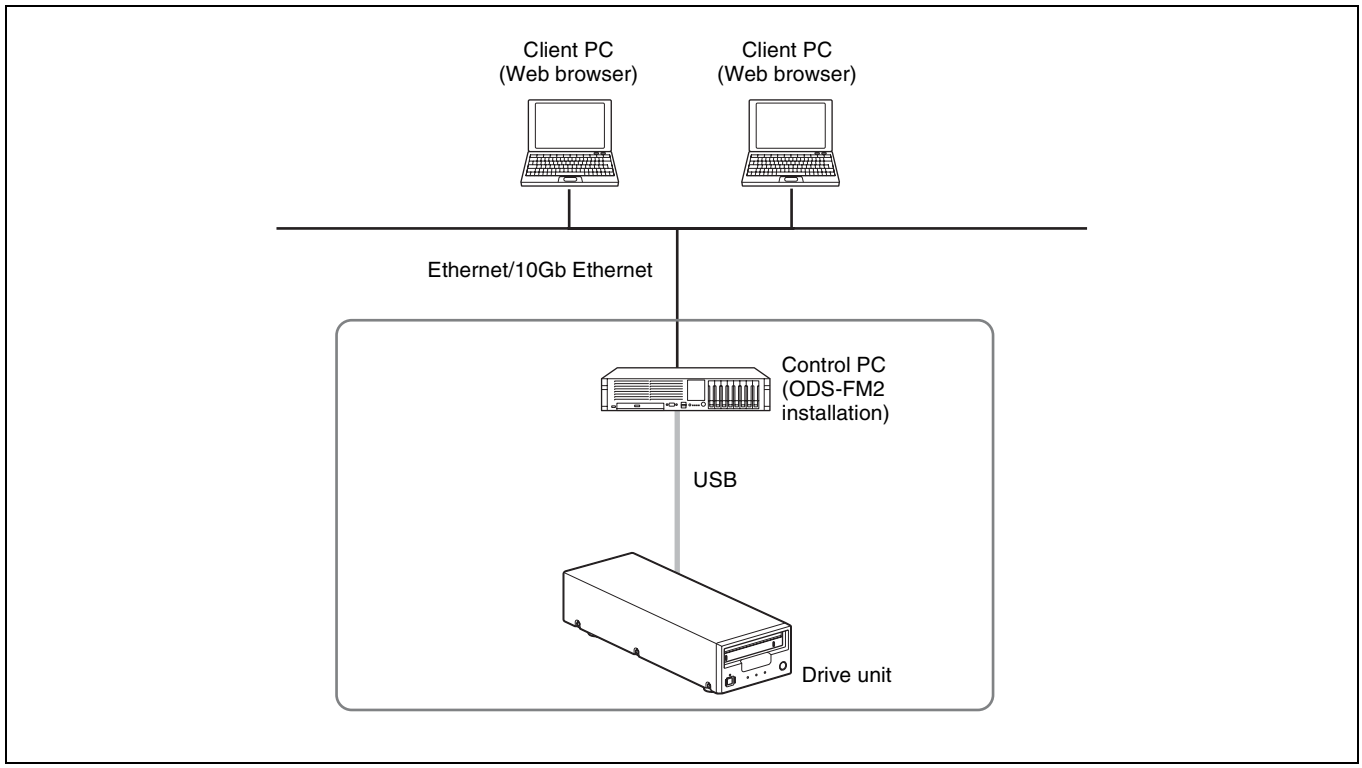
The drive unit installed in the ODS-L30M and control PC (server) connect using Fibre Channel.

The network, connecting the client PCs, connects to the control PC using Ethernet.




## Direct connection to drive unit

The control PC connects directly to each drive unit using USB. In addition, the control PC connects to the network that the client PCs and network storage are on.



# Operating Environment

The required operating environments for the control PC and client PCs is described below.

## Control PC

The required operating environment varies depending on the selected operating mode. The memory and HDD capacity requirements are values that do not include the space required for Optical Disc Archive Software.

### File Manager mode

CPU Intel Core i5 3 GHz or higher
Memory 8 GB
HDD capacity 200 GB
(Additional capacity of 4 TB/drive is required if archiving files from the local HDD or retrieving files to the local HDD)
OS
- ODS-L10 or drive unit connection:
  Windows 10 64-bit
- ODS-L30M connection:
  Windows Server 2012
  Windows Server 2012 R2
  Windows Server 2016
  Windows Server 2019

Interface
- ODS-L10 connection:
  Ethernet × 2 ports (for PC client connection and ODS-L10 connection)
  USB ports (one for each drive)
- ODS-L30M connection:
  Ethernet × 1 port (for PC client connection and ODS-L30M connection)
  Fibre Channel HBA (Host Bus Adapter)
- Drive unit direct connection:
  Ethernet × 1 port (for PC client connection)
  USB ports (one for each drive)

### File Server mode

CPU Intel Core i5 3 GHz or higher
Memory 16 GB
HDD capacity 200 GB + 4 TB/drive
OS Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

Interface
- ODS-L10 connection:
  Ethernet × 2 ports (for PC client connection and ODS-L10 connection)
  USB ports (one for each drive)
- ODS-L30M connection:
  Ethernet × 1 port (for PC client connection and ODS-L30M connection)
  Fibre Channel HBA (Host Bus Adapter)
- Drive unit direct connection:
  Ethernet × 1 port (for PC client connection)
  USB ports (one for each drive)

### Virtual Tape mode

CPU Intel Core i5 3 GHz or higher
Memory 4 GB
HDD capacity N/A (space required for Optical Disc Archive Software only)
OS Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

Interface
- ODS-L30M connection:
  Ethernet × 1 port (for PC client connection and ODS-L30M connection)
  Fibre Channel HBA (Host Bus Adapter)
- Drive unit direct connection:
  Ethernet × 1 port (for PC client connection)
  USB ports (one for each drive)

**Note**

For details about the USB interface supported by each drive unit, refer to the operation manual for the drive unit.

## Client PC

Hardware Hardware supporting the following OS and web browser without problem.
OS Windows 7, Windows 8.1, Windows 10
macOS 10.13, 10.14, 10.15
Web browser Microsoft Internet Explorer 11, Microsoft Edge, Google Chrome, Safari 11/12/13

## Network Precautions

This application could be accessed by any unintended third party on the network, depending on a usage environment. Please connect to a secure network.

# Setting Up

This section describes the setup procedure for installing ODS-FM2 on the control PC in order to operate an Optical Disc Archive System using ODS-FM2.

**Notes**

- Update the ODS-L10/ODS-L30M firmware to the latest version.
- Update Optical Disc Archive Software and firmware of the drive units to the latest versions.

## Optical Disc Archive System Device Setup

### If control PC connects to ODS-L10

*For details about ODS-L10 operation, refer to the ODS-L10 Installation Manual and Operation Manual.*

**1** Install a drive unit in the ODS-L10.

Up to two ODS-D55U or ODS-D77U units can be installed in the ODS-L10. ODS-D280U/D380U and models that use Fibre Channel cannot be installed.

**2** Set the IP address of the ODS-L10.

*For details about the setting method, refer to the ODS-L10 Operation Manual.*

**3** Install Optical Disc Archive Software on the control PC (PC on which to install ODS-FM2).

**4** Install ODS-FM2 on the control PC.

Install the software by following the installer instructions.

**5** Connect the drive unit, installed in the ODS-L10, and the control PC using a USB cable.

If there are two drive units installed, connect both drive units with the control PC.

**6** Connect the network with the ODS-L10 to the network port on the control PC.

For details about network settings, refer to Windows documentation.

**7** Insert optical disc cartridges in the ODS-L10.

### If control PC connects to ODS-L30M

*For details about ODS-L30M operation, refer to the ODS-L30M Operation Manual.*

**1** Install the ODS-D77F/D280F/D380F Drive Unit in the ODS-L30M.

A combination of up to two ODS-D77F/D280F/D380F units can be installed in the ODS-L30M. If you want to install three or more units, consult your Sony representative.

**Note**

In configurations containing a mix of ODS-D77F, ODS-D280F, and ODS-D380F units, Virtual Tape mode cannot be used. To use Virtual Tape mode, choose a configuration containing units of a single model only.

**2** Set the IP address of the ODS-L30M.

*For details about the setting method, refer to the ODS-L30M Operation Manual.*

**3** Install Optical Disc Archive Software on the control PC.

**4** Install ODS-FM2 on the control PC.

Install the software by following the installer instructions.

**5** Connect the drive unit, installed in the ODS-L30M, to a Fibre Channel switch.

If there are two drive units installed, connect both drive units to the Fibre Channel switch.

**6** Connect the control PC to the Fibre Channel switch.

**7** Insert optical disc cartridges in the ODS-L30M.

### If control PC connects directly to drive unit

**1** Install Optical Disc Archive Software on the control PC.

**2** Install ODS-FM2 on the control PC.

Install the software by following the installer instructions.

**3** Connect the drive unit and the control PC using a USB cable.

**4** Insert optical disc cartridges in the drive unit.

# ODS-FM2 Setup

The ODS-FM2 configuration and activation is performed using the Library Software Configuration Tool.

**Note**

You must be connected to the Internet to activate the software. If the control PC is not connected to the Internet, prepare another PC that can connect to the Internet.

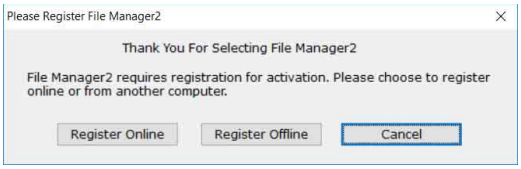
**1** On the control PC, select “Config Tool” from the Start menu or double-click C:\Program Files\Sony\ODAFileManager2\odafm\ConfigTool.exe to launch the Library Software Configuration Tool.

Start the Library Software Configuration Tool from an account that has administrator privileges.

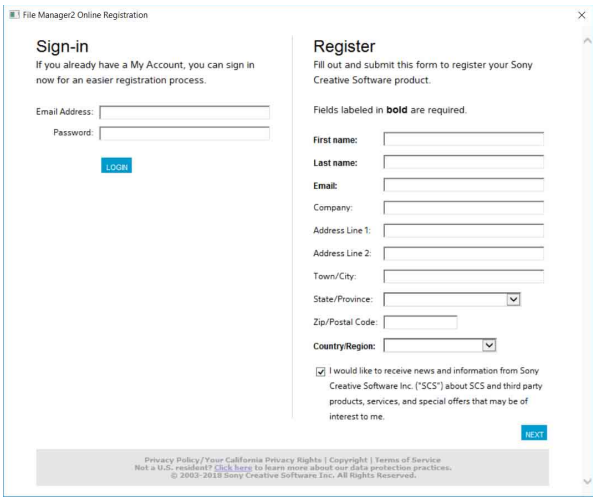
**2** Activate the license if the ODS-FM2 license has not been activated yet.

### If the control PC is connected to the Internet

① Click [Register Online].




② Enter the required items, then click [Next].

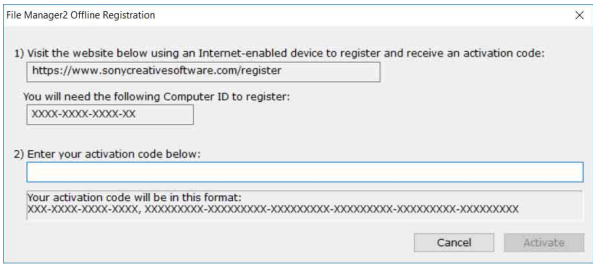



③ Enter the serial number, then click [Next].
The software is activated and the Library Software Configuration Tool starts.

### If the control PC is not connected to the Internet

① Click [Register Offline].

② Enter the URL displayed in the [Library Software Offline Registration] dialog in a web browser on another PC that is connected to the Internet to display the web page.



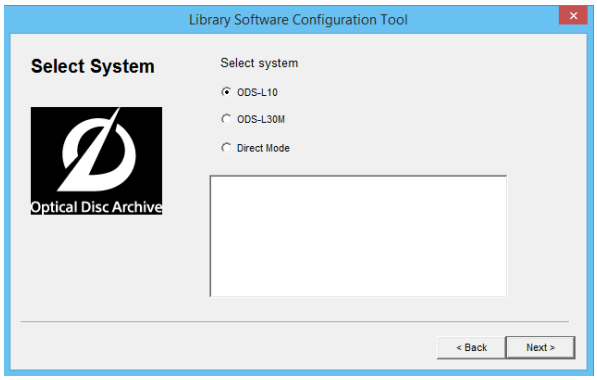

③ Enter and submit the serial number and computer ID (displayed in the [Library Software Offline Registration] dialog) in the web page to acquire the activation code.

④ Enter the activation code into the [Library Software Offline Registration] dialog on the control PC, then click [Activate].
The software is activated and the Library Software Configuration Tool starts.

**3** Click [Next].

**4** Select the system to connect on the Select System screen.

Select “Direct Mode” if connecting directly to the drive unit.

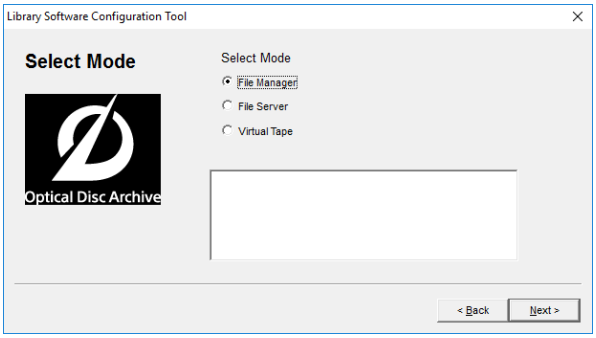



**5** Select the mode to use on the Select Mode screen, then click [Next].

When File Server mode is selected, proceed to *“File Server mode settings” (page 9)*.
When Virtual Tape mode is selected, proceed to *“Virtual Tape mode settings” (page 11)*.
When File Manager mode is selected, proceed to *“Settings common to all modes” (page 12)*.

**Notes**

- If [ODS-L10] is selected in step **4**, Virtual Tape mode cannot be selected.
- To select Virtual Tape mode, exit the application that is accessing the virtual tape before clicking [Next]. Selecting Virtual Tape mode and clicking [Next] will display a warning dialog, regardless of whether the application that is accessing the virtual tape has finished exiting.

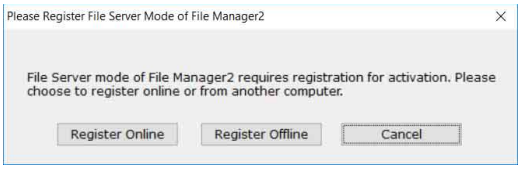



## File Server mode settings

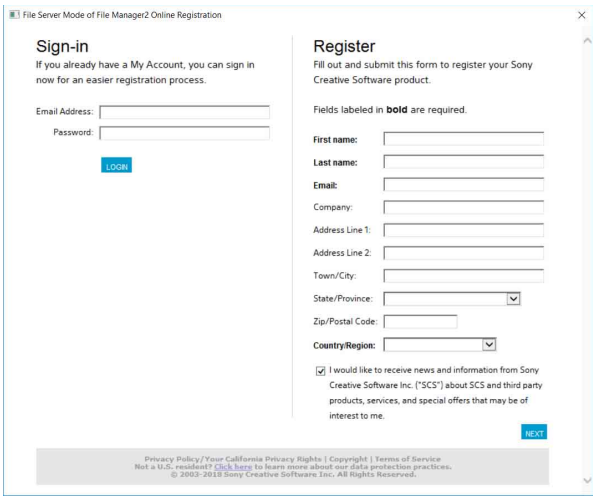
**1** Activate the license if the File Server mode license has not been activated yet.

### If the control PC is connected to the Internet

① Click [Register Online].




② Enter the required items, then click [Next].

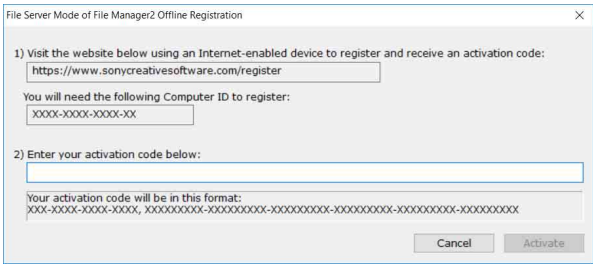



③ Enter the serial number, then click [Next].
The File Server mode license is activated.

### If the control PC is not connected to the Internet

① Click [Register Offline].

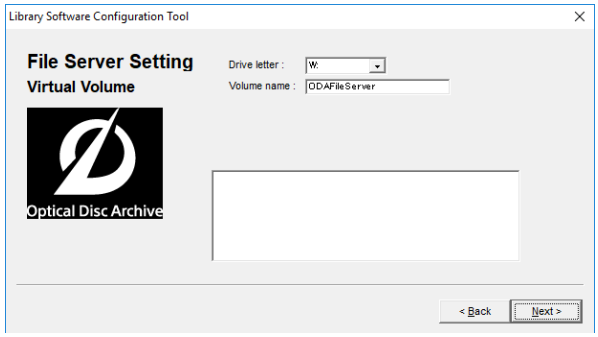
② Enter the URL displayed in the [Library Software Offline Registration] dialog in a web browser on another PC that is connected to the Internet to display the web page.




③ Enter and submit the serial number and computer ID (displayed in the [Library Software Offline Registration] dialog) in the web page to acquire the activation code.

④ Enter the activation code into the [Library Software Offline Registration] dialog on the control PC, then click [Activate].
The File Server mode license is activated.

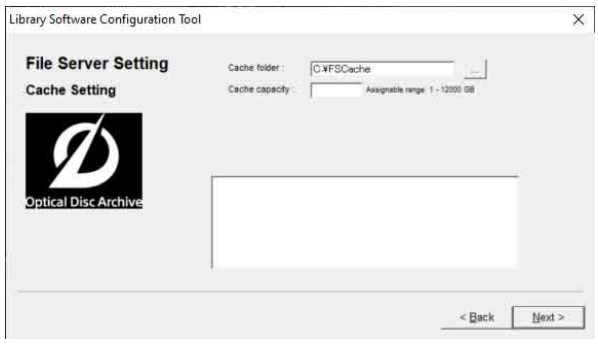
**2** Select the drive letter for the file server on the File Server Setting screen, and specify the volume label.




**3** After setting the volume, click [Next].

**4** Set the cache folder and cache capacity for the file server.

The file server will temporarily save write files in the cache folder.



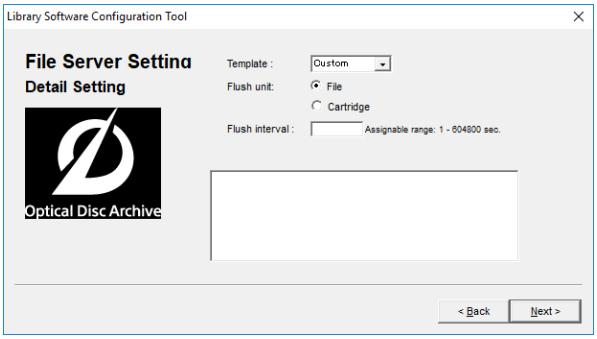
Cache folder: Set the folder used as the cache folder.
Cache capacity: Set the maximum size of the cache file storage.

**Note**

It is recommended that you prepare a dedicated disk or partition for the cache folder path so that the volume is not used by other applications.

**5** After setting the cache folder and cache capacity, click [Next].

**6** Set the detail settings for the file server.



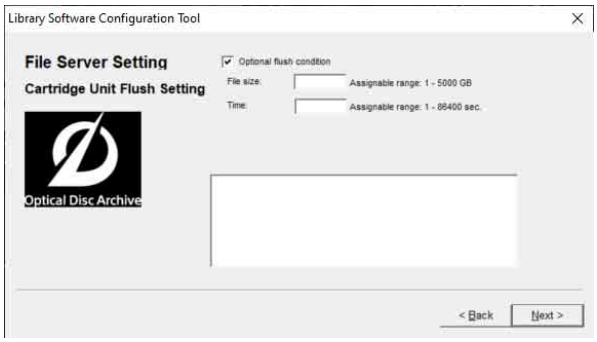

Template: Select the configuration template for the application that accesses the file server. To configure manually, select [Custom].
Flush unit: Sets whether the sync process for writing from the cache to cartridge occurs in file units or cartridge units.
- File: The time since a file was last updated before flushing the cache is managed for each file. When that value reaches the [Flush interval] setting, an archive job is registered in order to synchronize that file.
- Cartridge: The time since a file was last updated before flushing the cache is managed for each cartridge. When that value reaches the [Flush interval] setting, an archive job is registered in order to synchronize all the updated files.

Flush interval: Sets the time from when writing a file to a virtual volume ends or from when the file is last updated until the file in cache is synchronized with a cartridge.

**7** After setting the cache properties, click [Next].

If [Cartridge] is selected in [Flush unit], proceed to step **8**.
If [File] is selected in [Flush unit] and [SmartDocs] is selected in [Template], proceed to step **10**.
If [File] is selected in [Flush unit] and [Custom] is selected in [Template], proceed to *"Settings common to all modes" (page 12)*.

**8** Set the properties for when flushing by cartridge units.

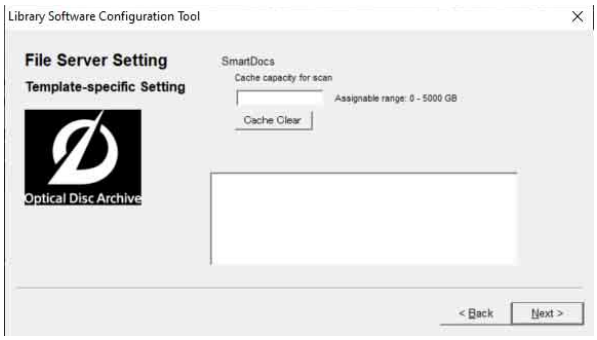



Optional flush condition: This setting is valid only when flushing by cartridge units. When enabled, in addition to the normal archive job registration based on the [Flush interval], faster synchronization can be performed according to the total size of files to be updated.
When both the total size of files to be synchronized exceeds the [File size] setting and the files have not been written or updated for a duration given by [Time], an archive job is registered to synchronize the files.

**9** After setting the properties for when flushing by cartridge units, click [Next].

If [SmartDocs] is selected in [Template], proceed to step **10**.
If [Custom] is selected in [Template], proceed to *"Settings common to all modes" (page 12)*.

**10** Specify the template-specific settings.




Cache capacity for scan: Sets the cache capacity used by the SmartDocs scan function. A capacity independent of the [Cache capacity] setting in step **4** is reserved on the same volume.
[Cache Clear] button: Deletes the files from within the cache capacity for scanning, clearing the used space.

**11** After setting the template-specific settings, click [Next].

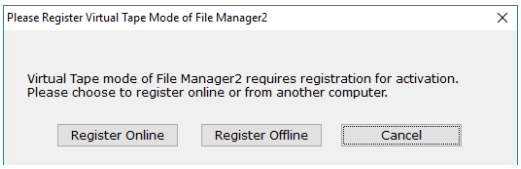
Next, proceed to *"Settings common to all modes" (page 12)*.

## Virtual Tape mode settings

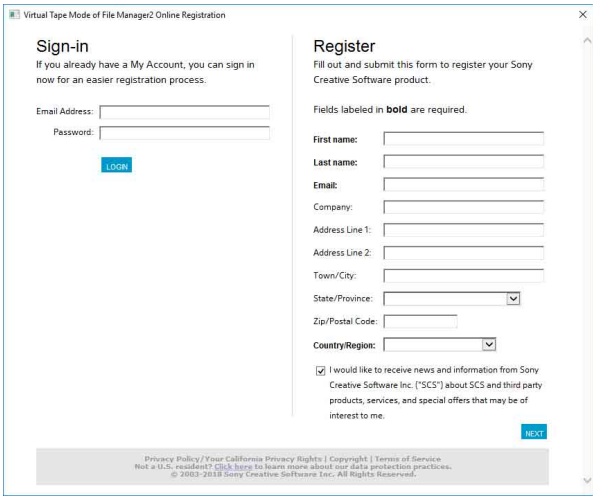
**1** Activate the license if the Virtual Tape mode license has not been activated yet.

### If the control PC is connected to the Internet

① Click [Register Online].




② Enter the required items, then click [Next].

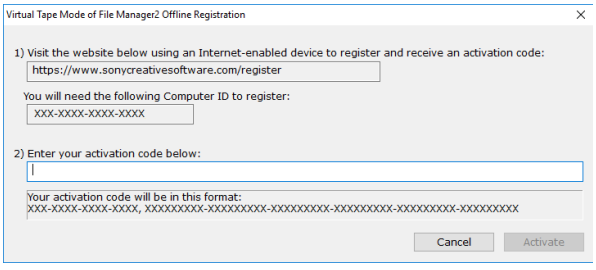



③ Enter the serial number, then click [Next].
The Virtual Tape mode license is activated.

### If the control PC is not connected to the Internet

① Click [Register Offline].

② Enter the URL displayed in the [Library Software Offline Registration] dialog in a web browser on another PC that is connected to the Internet to display the web page.



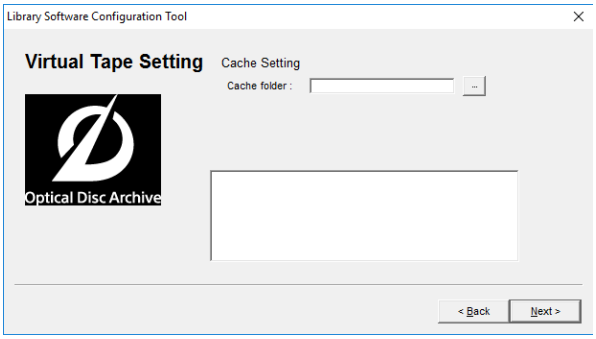

③ Enter and submit the serial number and computer ID (displayed in the [Library Software Offline Registration] dialog) in the web page to acquire the activation code.

④ Enter the activation code into the [Library Software Offline Registration] dialog on the control PC, then click [Activate].
The Virtual Tape mode license is activated.

**2** Specify the path of the cache folder on the Virtual Tape Setting screen.

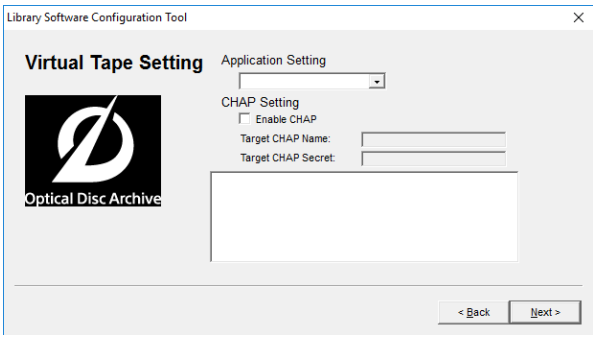
**Note**

It is recommended that you prepare a dedicated disk or partition for the cache folder path so that the volume is not used by other applications.




**3** After setting the path of the cache folder, click [Next].

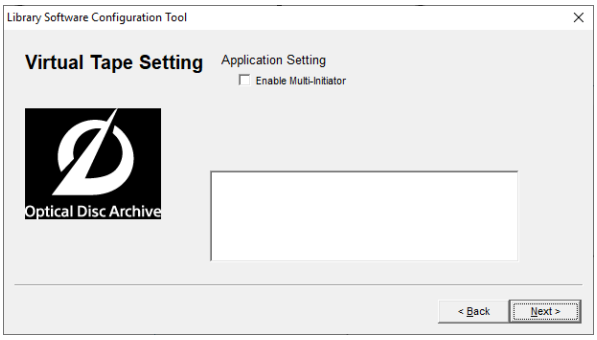
**4** Configure the application to be used and CHAP (Challenge-Handshake Authentication Protocol).




Application Setting: Select the application that uses the virtual tape from the drop-down list.
Enable CHAP: Place a check mark in the checkbox to enable user authentication using CHAP.
Target CHAP Name: User name used for authentication. Enter an ASCII character string (excluding control characters) of 1 to 256 characters.
Target CHAP Secret: Password used to authentication. Enter an ASCII character string (excluding control characters) of 12 to 16 characters.

**5** After configuring the application and CHAP, click [Next].

**6** Enable or disable the multi-initiator setting.




When [Enable Multi-Initiator] is enabled, sync connections from multiple clients are enabled. When disabled, other clients cannot be connected if there is already a client connected.

**7** After setting the multi-initiator setting, click [Next].

Next, proceed to *"Settings common to all modes"*.

## Settings common to all modes

**1** Click [Next] on the Database Initialization screen.

Database initialization is automatically performed. If "Direct Mode" or "ODS-L30M" is selected on the Select System screen, proceed to step **5**. If "ODS-L10" is selected, proceed to the next step.

**2** Enter the IP address configured on the ODS-L10 and the login ID (user name)/password for logging in to the ODS-L10, then click [Next].

The PC connects to the ODS-L10.
The Drive Setting page appears if the connection is successful.

**3** If a drive unit is connected to the control PC but is not installed in the ODS-L10, disconnect it from the control PC in order to do a drive check.

**4** Click [Next].

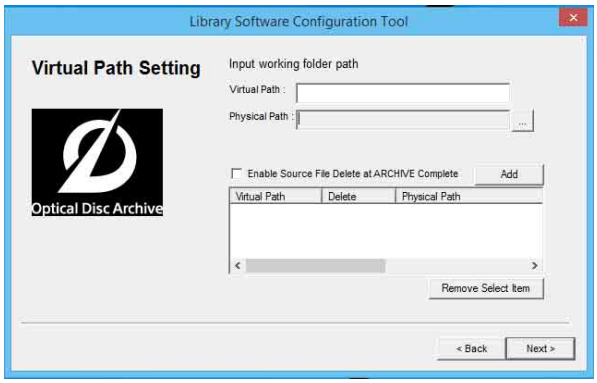
The drive check starts.
If there is only one drive unit installed in the ODS-L10, a confirmation message appears asking whether it is located in the top or bottom slot. If installed in the bottom slot, click [Yes]. If installed in the top slot, click [No]. The Administrator Setup screen appears when the drive check is finished.

**5** Create an account to use when logging in to the ODS-FM2. Enter the login ID and password, then click [Next].

When File Manager mode is selected, set the root folder (base path) in steps **6** and **7**. When File Server mode or Virtual Tape mode is selected, proceed to step **8**.


**6** Specify the root folder (base path) to be displayed on the ODS-FM2 Archive screen.

Only the files/folders under the specified base path are displayed on the Archive screen. Restricting the folders that are displayed prevents system files being changed in error. Multiple base paths can be specified.



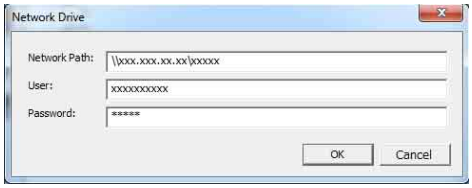

Virtual Path: Enter a name for the base path to be displayed on the Archive screen.
Physical Path: Specify the physical path for the base path to be displayed. You can also specify a network drive.
Enable Source File Delete at ARCHIVE Complete: Select whether to automatically delete the file after archiving. If not selected, the archived file remains and must be deleted manually when no longer needed.
Add button: Adds the base path with the specified settings. The specified base path is added to the lower list.

### To assign a network drive

① Click the […] button for the [Physical Path] item.

② Click the [Network Drive] button in the [Reference] dialog.

③ Enter the path of the network drive in UNC format (\\server_name or IP_address\folder_name) in [Network Path] in the [Network Drive] dialog.



④ If required, enter a user name and password in [User] and [Password], respectively.

⑤ Click the [OK] button.
The added network drive appears in the [Reference] dialog.

⑥ Select the network drive and click the [Select] button.
The [Reference] dialog closes, and the path of the selected network drive appears in the [Physical Path] item on the Virtual Path Setting page.

⑦ Specify [Virtual Path] and click the [Add] button.

**7** After setting the base path(s), click [Next].

**8** Click [Finish] when the configuration is finished dialog box appears.

**9** Connect the network that the client PCs are on to a network port on the control PC.

If using a network connection to the ODS-L10, connect the client PCs to a different network than the ODS-L10.
The Optical Disc Archive System can now be operated using the web application from a client PC.

**Notes**

- If anti-virus software or security software is installed on the control PC, inbound access on port 8080 from a client PC may be blocked. In this case, configure your security software to allow inbound access on port 8080. For details about configuration, refer to the operating instructions for your security software.
- If the hardware configuration is changed or the drive unit connection is changed, ODS-FM2 will no longer work correctly. If this occurs, reconfigure the ODS-FM2 settings using the Library Software Configuration Tool.
- If ODS-L10 or ODS-L30M configuration settings are changed in the Setup menu of the web page or on the display on the front panel of the unit, reconfigure ODS-FM2 using the Library Software Configuration Tool.
- Optical Disc Archive Filer cannot be started when using ODS-FM2. To use Optical Disc Archive Filer, first terminate the ODS-FM2 service and then start Optical Disc Archive Filer. (Optical Disc Archive Filer is included with Optical Disc Archive Software.)

## Firewall Settings

The following firewall settings are recommended in order to block connections to MariaDB from an external source.

**1** Select [Control Panel] > [System and Security] > [Windows Firewall] > [Advanced settings] > [Inbound Rules] > [New Rule…].

**2** Configure the following in the New Inbound Rule Wizard.

- Rule Type: Select [Port].
- Protocol and Ports: Select [TCP] and [Specific local ports] (enter port “3306”).
- Action: Select [Block the connection].
- Profile: Select all.
- Name: Enter “MariaDBPort” name.

**3** Click [Finish].

**4** Select [New Rule…] again to display the New Inbound Rule Wizard, and configure the following.

- Rule Type: Select [Port].
- Protocol and Ports: Select [UDP] and [Specific local ports] (enter port “3306”).
- Action: Select [Block the connection].
- Profile: Select all.
- Name: Enter “MariaDBPort” name.

**5** Click [Finish].

## HTTPS Communications Settings

Communications can be encrypted by setting HTTPS communication.

### Generating a keystore file

**1** Launch [Command Prompt].

**2** Enter the following command.

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

**Example keystore file name:**
filemanager2.keystore

**3** Enter a password when prompted to set a keystore password.

Enter keystore password: ********
(Password is not displayed)

**4** Enter the same password again when prompted to do so.

Re-enter new password: ********
(Password is not displayed)

**5** Enter information for the certificate signing request (CSR).

Input example:

```
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** Check the displayed contents of the entered information, and then enter “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** Press the Return (Enter) key without entering anything when the following prompt appears.

Enter key password for (RETURN if same as keystore password):
A keystore file with the name specified in step **2** is generated.

## Generating a CSR

**1** Launch [Command Prompt].

**2** Enter the following command.

cd C:\Program Files\Zulu\zulu-8-jre\bin
keytool -certreq -sigalg SHA1withRSA -alias tomcat -file <*CSR_filename*> -keystore <*keystore_filename*>

**Example CSR file name:**
filemanager2.csr

**3** Enter the password specified when generating the keystore file when prompted.

Enter keystore password: ********
A CSR file with the name specified in step **2** is generated.

## Issuing a server certificate

Pass the generated CSR to a certificate authority to have a signed server certificate issued.

## Generating a server certificate used by applications

**1** Place the signed server certificate and intermediate certificate in an arbitrary directory.

**2** Launch [Command Prompt].

**3** Merge the signed server certificate and intermediate certificate into a single file.

copy <*signed_server_certificate_filename*> + <*Intermediate_certificate_filename*> <*server_certificate_filename_used_by_applications*>

**Example server certificate file name used by applications:**
filemanager2.cer

## Installing a certificate

**1** Enter the following command.

keytool -import -alias tomcat -keystore <*keystore_filename*> -file <*filename_generated_in_step**3**_previous section*>

**2** Enter the password specified when generating the keystore file when prompted.

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

**3** Enter “yes” if the following prompt appears.

```
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
```

Asterisks indicate the display of registered information.

## Enabling HTTPS

**1** Stop the Tomcat service.

① From the [Start] menu, click [Windows Administrative Tools] > [Services].

② Search for and click the “Apache Tomcat” service in the list of services.

③ Click [Stop the service] on the left side of the list of services.

**2** Edit the Tomcat configuration file (server.xml).

① Open C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\server.xml, and uncomment the block at line 85.

② Copy the content shown below in “After editing.”

③ Enter the full path of the actual keystore file in <*keystore_filename*>, and enter the password specified when generating the keystore file in <*keystore_password*>.

**Before editing**

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

### After editing

```
<Connector port="8443"
    protocol="org.apache.coyote.http11.Http11Protocol"
    SSLEnabled="true"
    maxThreads="150"
    scheme="https"
    secure="true"
    keystoreFile="<keystore_filename>"
    keystorePass="<keystore_password>"
    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_256_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"
/>
```

To prevent HTTP communications, comment out the block at line 70 as follows.

### Before editing

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

### After editing

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

**3** Start the Tomcat service.

① From the [Start] menu, click [Windows Administrative Tools] > [Services].

② Search for and click the “Apache Tomcat” service in the list of services.

③ Click [Start the service] on the left side of the list of services.

**4** Run the Config Tool.

**5** Check the HTTPS communication.

Launch a web browser and access “https://<*domain_name*>:8443” and check that the login screen is displayed.

# Displaying the Web Application

### If HTTPS communication is not configured

Display a web browser on the client PC, and enter "http://(control PC IP address):8080/" into the address bar. The login screen appears when the web browser connects to the control PC. Enter the username and password configured in the Library Software Configuration Tool to log in.

### If HTTPS communication is configured

Open a web browser window on the client PC, and enter "http://<*domain_name*>:8443/" into the address bar. The login screen appears when the web browser connects to the control PC. Enter the user name and password configured in the Library Software Configuration Tool to log in.

ODS-FM2(WW)
5-000-612-**13** (1)

Sony Imaging Products & Solutions Inc.

http://www.sony.net/