SONY

OPTICAL DISC ARCHIVE FILE MANAGER2

ODS-FM2

Optical Disc Archive

INSTALLATION GUIDE French

1st Edition (Revised 6)

Marques commerciales

- Microsoft, Windows, Internet Explorer et Microsoft Edge sont des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.
- Intel et Intel Core sont des marques commerciales ou déposées de Intel Corporation aux États-Unis et dans d'autres pays.
- Apple, macOS, OS X et Safari sont des marques commerciales d'Apple Inc., déposée aux États-Unis et dans d'autres pays.
- Chrome est une marque déposée de Google Inc.
- SmartDocs est une marque commerciale de Teknowmics Co., Ltd.
- Les noms de produits et de marques qui figurent dans ce document sont des marques commerciales ou déposées de leurs propriétaires respectifs.

Table des matières

Fonctionnalités

ODS-FM2 est un logiciel d'archive et de récupération à l'aide d'un système d'archivage sur disque optique. Vous utilisez ce logiciel pour gérer non seulement les cartouches insérées dans le système d'archivage sur disque optique, mais également les cartouches dans l'étagère de gestion. Les opérations du ODS-FM2 sont effectuées en utilisant une application Web. L'application est accessible dans un navigateur Web depuis un PC client.

Ce Guide d'installation décrit la procédure d'installation du logiciel pour la configuration grâce à une connexion réseau au ODS-L10 ou ODS-L30M[1)] et la configuration où une unité de lecture est connectée directement à un ordinateur.

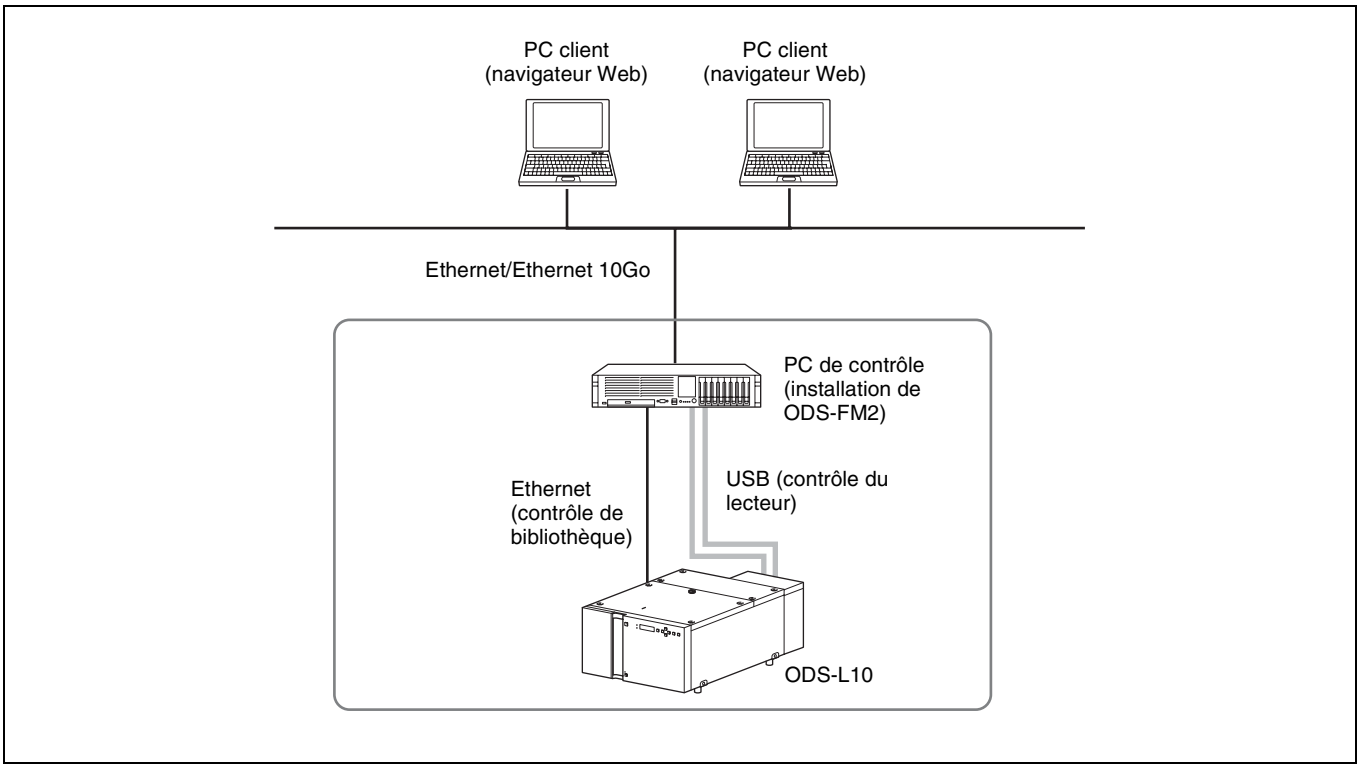
1) Les unités ODS-L60E et ODS-L100E peuvent également être connectées.

Configurations système

Les configurations système basiques pour utiliser le ODS-FM2 sont indiquées ci-dessous.
L'ordinateur sur lequel le ODS-FM2 est installé est appelé le « PC de contrôle ». Le PC de contrôle se connecte au système d'archivage sur disque optique afin de commander le système d'archivage sur disque optique. Vous utilisez le ODS-FM2 en accédant au PC de contrôle à l'aide d'un navigateur Web sur un PC client.

Connexion au dispositif ODS-L10

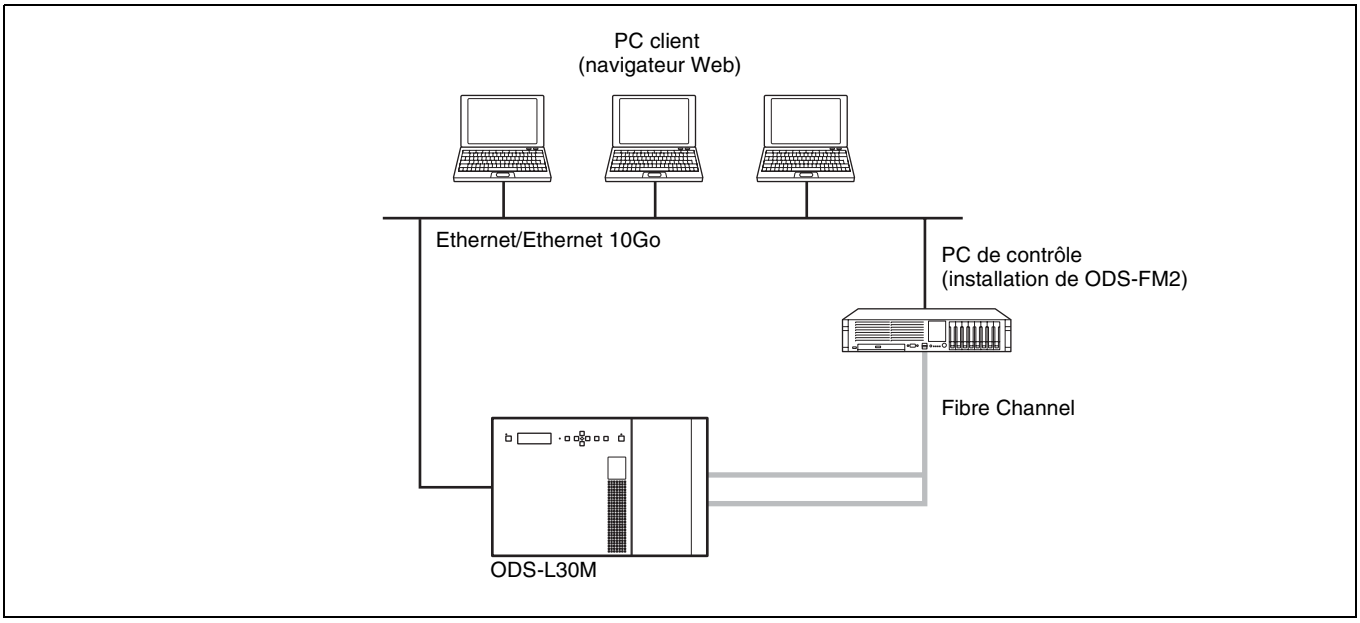
Le PC de contrôle se connecte au réseau sur lequel se trouve le ODS-L10 et au réseau sur lequel se trouvent les PC client et le stockage réseau. De plus, le PC de contrôle se connecte à chaque unité de lecture installée dans le ODS-L10 grâce à un port USB.



Connexion au dispositif ODS-L30M

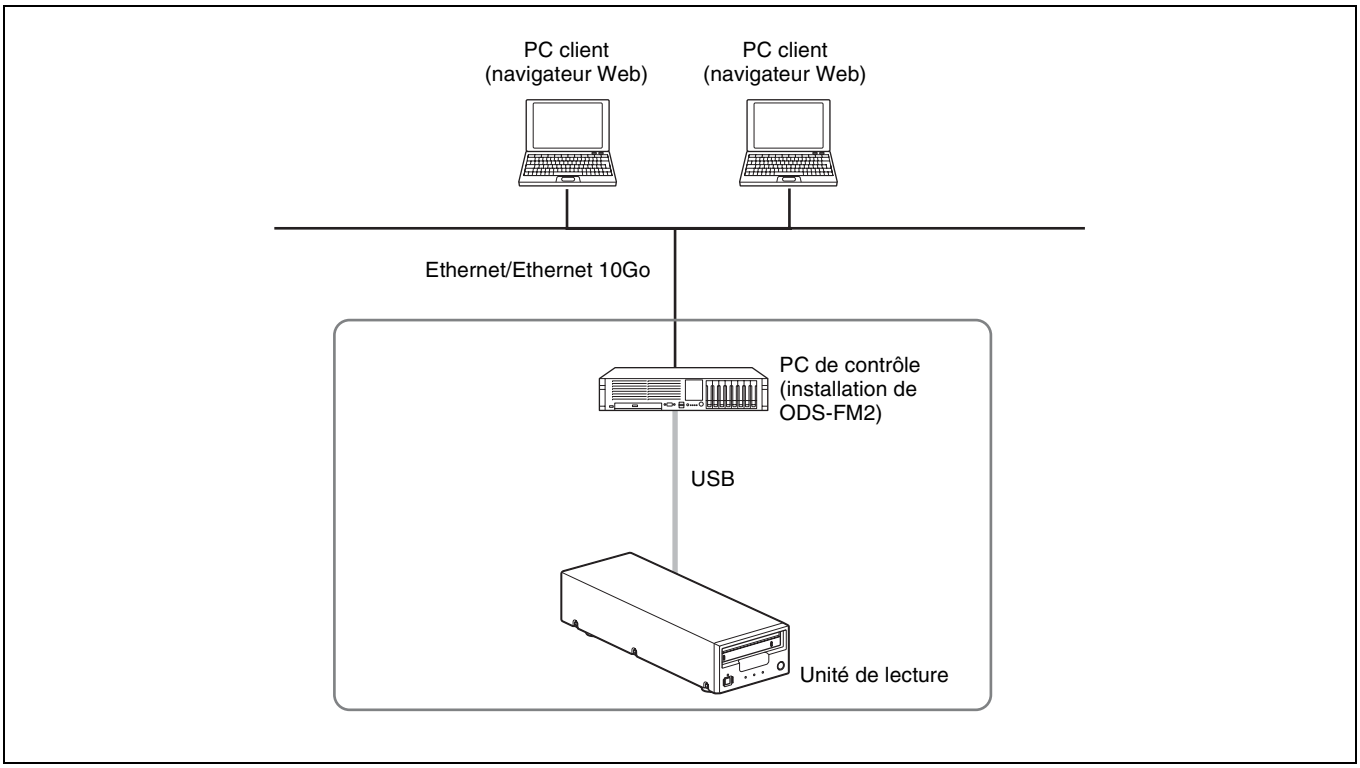
L'unité de lecture installée dans le dispositif ODS-L30M et le PC de contrôle se connectent à l'aide de Fibre Channel.

Le réseau, qui connecte les PC client, se connecte au PC de contrôle à l'aide d'Ethernet.



Connexion directe à l'unité de lecture

Le PC de contrôle se connecte directement à chaque unité de lecture grâce à un port USB. De plus, le PC de contrôle se connecte au réseau sur lequel se trouvent les PC client et le stockage réseau.



Environnement d’exploitation

Les environnements de fonctionnement requis pour le PC de contrôle et les PC client sont décrits ci-dessous.

PC de contrôle

L’environnement de fonctionnement requis varie en fonction du mode de fonctionnement sélectionné. Les exigences de capacité de la mémoire et du disque dur sont des valeurs qui n’incluent pas l’espace requis pour Optical Disc Archive Software.

Mode File Manager

Unité centrale Intel Core i5 3 GHz ou supérieur
Mémoire 8 Go
Capacité du disque dur
200 Go + (capacité maximale des cartouches prises en charge × nombre de lecteurs)*
* Exemple : si vous utilisez un lecteur qui prend en charge les cartouches de 3e génération, 5,5 To × 1 lecteur = 5,5 To
SE
- Connexion au dispositif ODS-L10 ou unité de lecture :
  Windows 10 64 bits
  Windows 11 64 bits
- Connexion au dispositif ODS-L30M :
  Windows Server 2016
  Windows Server 2019
  Windows Server 2022

Interface
- Connexion au dispositif ODS-L10 :
  Ethernet × 2 ports (pour connexion PC client et connexion ODS-L10)
  Ports USB (un pour chaque lecteur)
- Connexion au dispositif ODS-L30M :
  Ethernet × 1 port (pour connexion PC client et connexion ODS-L30M)
  Fibre Channel HBA (Host Bus Adapter - Contrôleur hôte de bus)
- Connexion directe à l’unité de lecture :
  Ethernet × 1 port (pour connexion PC client)
  Ports USB (un pour chaque lecteur)

Mode File Server

Unité centrale Intel Core i5 3 GHz ou supérieur
Mémoire 16 Go
Capacité du disque dur
200 Go + 4 To/lecteur
SE Windows Server 2016
Windows Server 2019
Windows Server 2022

Interface
- Connexion au dispositif ODS-L10 :
  Ethernet × 2 ports (pour connexion PC client et connexion ODS-L10)
  Ports USB (un pour chaque lecteur)
- Connexion au dispositif ODS-L30M :
  Ethernet × 1 port (pour connexion PC client et connexion ODS-L30M)
  Fibre Channel HBA (Host Bus Adapter - Contrôleur hôte de bus)
- Connexion directe à l’unité de lecture :
  Ethernet × 1 port (pour connexion PC client)
  Ports USB (un pour chaque lecteur)

Remarque

Pour plus de détails sur l’interface USB prise en charge par chaque unité de lecture, reportez-vous au manuel d’utilisation de l’unité de lecture.

PC client

Matériel Matériel prenant en charge le SE et le navigateur Web suivants sans problème.
SE Windows 10, Windows 11
macOS 11.7, 12.6, 13.5
Navigateur Web Microsoft Internet Explorer 11, Microsoft Edge, Google Chrome, Safari 14/15/16

Précautions de réseau

Cette application peut être accessible par un tiers non prévu sur le réseau en fonction de l’environnement d’utilisation. Connectez-vous à un réseau sécurisé.

Configuration

Cette section décrit la procédure de configuration pour installer ODS-FM2 sur le PC de contrôle afin de faire fonctionner le système d'archivage sur disque optique à l'aide de ODS-FM2.

Remarques

- Mettez à jour ODS-FM2 sur la version la plus récente.
- Mettez à jour le micrologiciel ODS-L10/ODS-L30M sur la version la plus récente.
- Mettez à jour Optical Disc Archive Software et le micrologiciel des unités de lecture sur la version la plus récente.

Configuration du dispositif du système d'archivage sur disque optique

Si le PC de contrôle se connecte au dispositif ODS-L10

Pour plus de détails sur le fonctionnement de ODS-L10, consultez le Manuel d'installation et le Manuel d'utilisation de ODS-L10.

1 Installez l'unité de lecture dans le ODS-L10.

Vous pouvez installer maximum deux unités ODS-D55U ou ODS-D77U dans le ODS-L10. ODS-D280U/D380U et les modèles qui utilisent Fibre Channel ne peuvent pas être installés.

2 Définissez l'adresse IP de ODS-L10.

Pour plus de détails sur la méthode de configuration, consultez le Manuel d'utilisation de ODS-L10.

3 Installez Optical Disc Archive Software sur le PC de contrôle (PC sur lequel installer ODS-FM2).

4 Installez ODS-FM2 sur le PC de contrôle.

Installez le logiciel en suivant les instructions du programme d'installation.

5 Connectez l'unité de lecture, installé dans le ODS-L10, et le PC de contrôle à l'aide d'un câble USB.

Si deux unités de lecture sont installées, connectez les deux lecteurs avec le PC de contrôle.

6 Connectez le réseau contenant le ODS-L10 au port réseau sur le PC de contrôle.

Pour plus de détails sur les réglages réseau, consultez la documentation Windows.

7 Insérez les cartouches de disque optique dans le dispositif ODS-L10.

Si le PC de contrôle se connecte au dispositif ODS-L30M

Pour plus de détails sur le fonctionnement du dispositif ODS-L30M, consultez le Manuel d'utilisation du dispositif ODS-L30M.

1 Installez l'unité de lecture ODS-D77F/D280F/D380F dans le dispositif ODS-L30M.

Une combinaison de deux unités ODS-D77F/D280F/D380F peut être installée dans le ODS-L30M. Si vous souhaitez installer trois unités ou plus, contactez votre service après-vente Sony.

2 Définissez l'adresse IP du dispositif ODS-L30M.

Pour plus de détails sur la méthode de configuration, consultez le Manuel d'utilisation du dispositif ODS-L30M.

3 Installez Optical Disc Archive Software sur le PC de contrôle.

4 Installez ODS-FM2 sur le PC de contrôle.

Installez le logiciel en suivant les instructions du programme d'installation.

5 Connectez l'unité de lecture, installée dans le dispositif ODS-L30M, à un interrupteur Fibre Channel.

Si deux unités de lecture sont installées, connectez les deux unités de lecture à l'interrupteur Fibre Channel.

6 Connectez le PC de contrôle à l'interrupteur Fibre Channel.

7 Insérez les cartouches de disque optique dans le dispositif ODS-L30M.

Si le PC de contrôle se connecte directement à l'unité de lecture

1 Installez Optical Disc Archive Software sur le PC de contrôle.

2 Installez ODS-FM2 sur le PC de contrôle.

Installez le logiciel en suivant les instructions du programme d'installation.

3 Connectez l'unité de lecture et le PC de contrôle à l'aide d'un câble USB.

4 Insérez des cartouches de disque optique dans l'unité de lecture.

Installation ODS-FM2

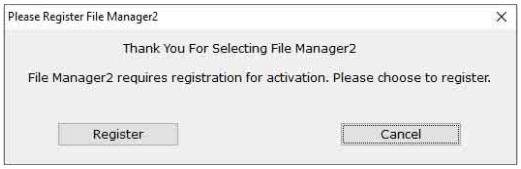
La configuration et l'activation de ODS-FM2 est effectuée grâce au Library Software Configuration Tool.

1 Sur le PC de contrôle, sélectionnez « Config Tool » dans le menu Démarrer ou double-cliquez sur C:\Program Files\Sony\ODAFileManager2\odafm\ConfigTool.exe pour lancer le Library Software Configuration Tool.

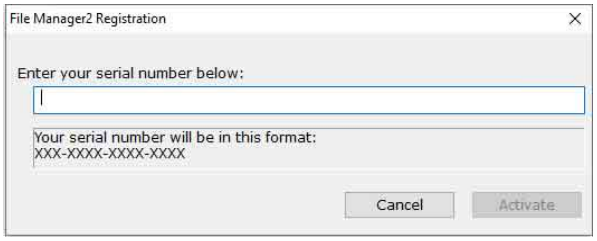
Démarrez le Library Software Configuration Tool depuis un compte qui dispose des privilèges administrateur.

2 Enregistrez la licence si la licence d'ODS-FM2 n'a pas encore été enregistrée.

① Cliquez sur le bouton [Register].

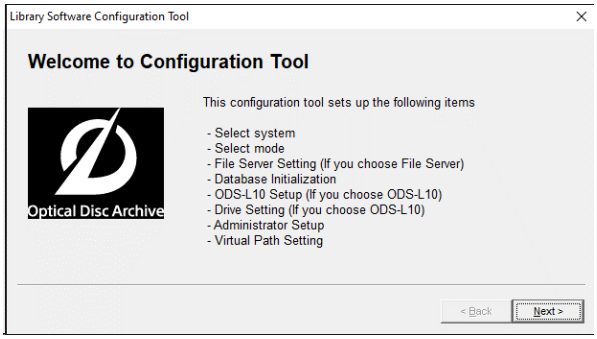


② Saisissez le numéro de série, puis cliquez sur le bouton [Activate].



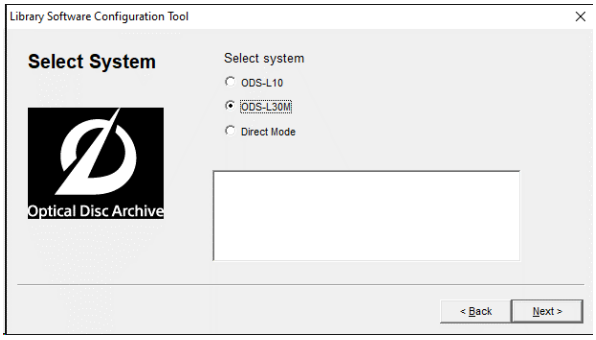
La licence est activée et le Library Software Configuration Tool se lance.

3 Cliquez sur [Next].



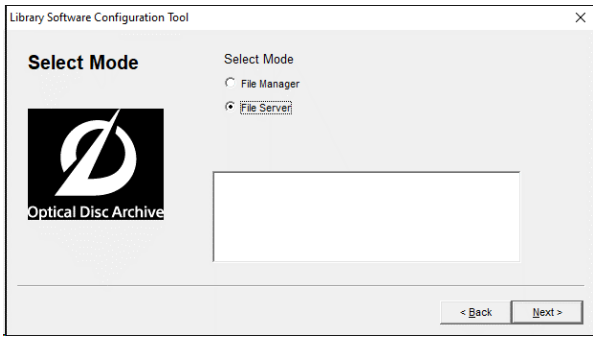
4 Sélectionnez le système à connecter sur l'écran Select System.

Sélectionnez « Direct Mode » si vous vous connectez directement à l'unité de lecture.



5 Sélectionnez le mode à utiliser sur l'écran Select Mode, puis cliquez sur [Next].

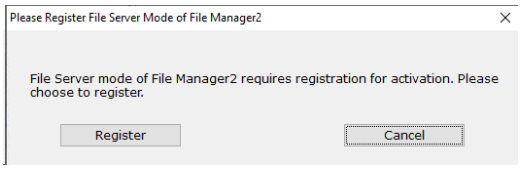
Lorsque le mode File Server est sélectionné, passez à *« Paramètres du mode File Server » (page 8)*.
Lorsque le mode File Manager est sélectionné, passez à *« Paramètres communs à tous les modes » (page 10)*.



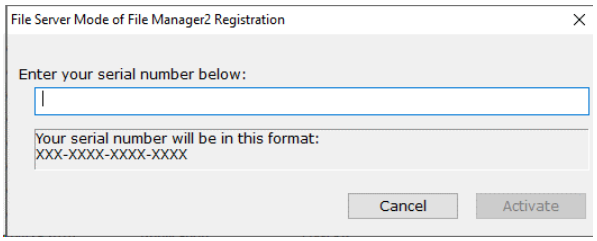
Paramètres du mode File Server

1 Enregistrez la licence du mode File Server si la licence n'a pas encore été enregistrée.

① Cliquez sur le bouton [Register].

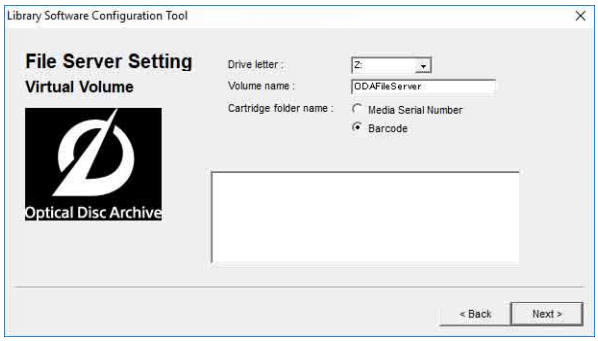


② Saisissez le numéro de série, puis cliquez sur le bouton [Activate].



La licence du mode File Server est activée.

2 Réglez le volume pour le serveur de fichiers sur l'écran File Server Setting.

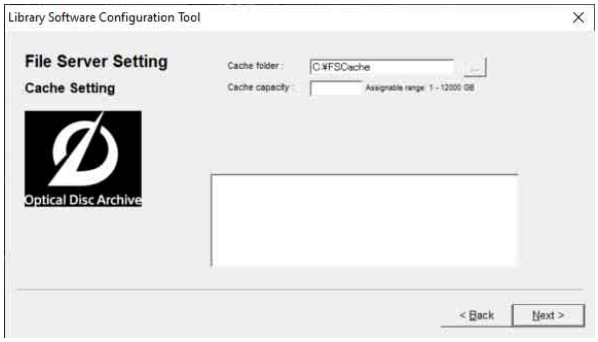


Drive letter : sélectionnez la lettre du lecteur pour le serveur de fichiers.
Volume name : spécifiez l'étiquette de volume.
Cartridge folder name : sélectionnez la méthode de dénomination du dossier de la cartouche.

3 Après avoir réglé le volume, cliquez sur [Next].

4 Définissez le dossier de cache et la capacité du cache pour le serveur de fichiers.

Le serveur de fichiers enregistre temporairement les fichiers d'écriture dans le dossier cache.



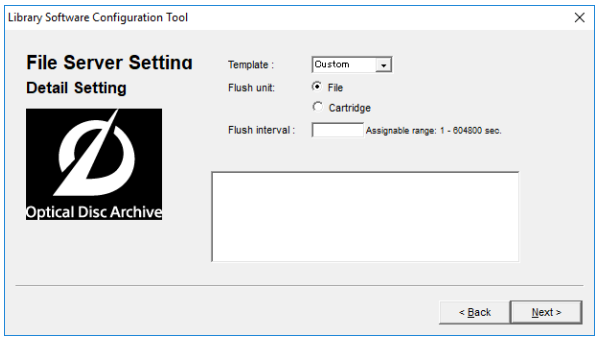
Cache folder : définit le dossier utilisé comme dossier cache.
Cache capacity : définit la taille maximale du stockage des fichiers du cache.

Remarque

Il est recommandé de préparer un disque ou une partition dédiée pour le chemin d'accès au dossier de cache de sorte que le volume ne soit pas utilisé par d'autres applications.

5 Après avoir défini le chemin d'accès au dossier de cache et la capacité cache, cliquez sur [Next].

6 Définissez les réglages de détail pour le serveur de fichiers.



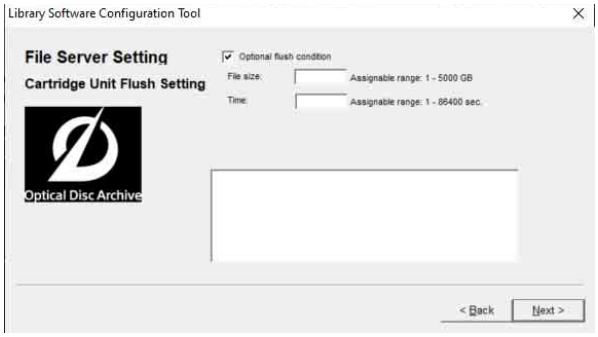
Template : sélectionne le modèle de configuration pour l'application accédant au serveur de fichiers. Pour configurer manuellement, sélectionnez [Custom].
Flush unit : définit si le processus de synchronisation pour l'écriture du cache vers la cartouche s'effectue par unités de fichier ou par unités de cartouche.
- File : le temps écoulé depuis la dernière mise à jour d'un fichier avant la vidange du cache est géré pour chaque fichier. Lorsque cette valeur atteint le réglage [Flush interval], une tâche d'archivage est enregistrée afin de synchroniser ce fichier.
- Cartridge : le temps écoulé depuis la dernière mise à jour d'un fichier avant la vidange du cache est géré pour chaque cartouche. Lorsque cette valeur atteint le réglage [Flush interval], une tâche d'archivage est enregistrée afin de synchroniser tous les fichiers mis à jour.

Flush interval : définit le temps entre la fin de l'écriture d'un fichier vers un volume virtuel ou entre la dernière mise à jour du fichier et la synchronisation du fichier en cache avec une cartouche.

7 Après avoir réglé les propriétés du cache, cliquez sur [Next].

Si [Cartridge] est sélectionné dans [Flush unit], passez à l'étape **8**.
Si [File] est sélectionné dans [Flush unit] et [SmartDocs] est sélectionné dans [Template], passez à l'étape **10**.
Si [File] est sélectionné dans [Flush unit] et [Custom] est sélectionné dans [Template], passez à l'étape *« Paramètres communs à tous les modes » (page 10)*.

8 Définissez les propriétés pour la vidange par unités de cartouche.

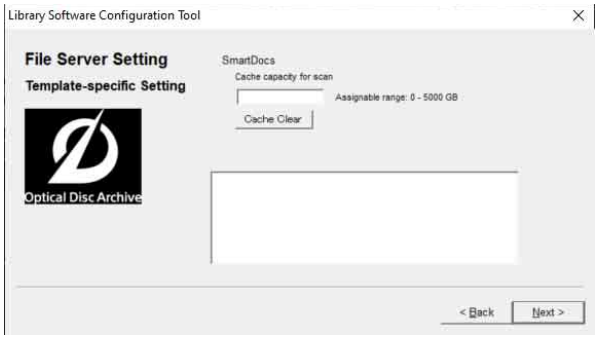


Optional flush condition : ce réglage n'est valable que pour la vidange par unités de cartouche. Lorsque cette option est activée, en plus de l'enregistrement normal des tâches d'archivage basé sur [Flush interval], une synchronisation plus rapide peut être effectuée en fonction de la taille totale des fichiers à mettre à jour.
Lorsque la taille totale des fichiers à synchroniser dépasse le réglage [File size] et que les fichiers n'ont pas été écrits ou mis à jour pendant une durée donnée par [Time], une tâche d'archivage est enregistrée pour synchroniser les fichiers.

9 Après avoir défini les propriétés pour la vidange par unités de cartouche, cliquez sur [Next].

Si [SmartDocs] est sélectionné dans [Template], passez à l'étape **10**.
Si [Custom] est sélectionné dans [Template], passez à *« Paramètres communs à tous les modes » (page 10)*.

10 Spécifiez les réglages spécifiques au modèle.



Cache capacity for scan : définit la capacité du cache utilisé par la fonction de numérisation SmartDocs. Une capacité indépendante du réglage [Cache capacity] à l'étape **4** est réservée sur le même volume.
Bouton [Cache Clear] : supprime les fichiers de la capacité du cache pour la numérisation, effaçant ainsi l'espace utilisé.

11 Après avoir défini les réglages spécifiques au modèle, cliquez sur [Next].

Ensuite, passez à *« Paramètres communs à tous les modes » (page 10)*.

Paramètres communs à tous les modes

1 Cliquez sur [Next] sur l'écran Database Initialization.

L'initialisation de la base de données est effectuée automatiquement. Si « Direct Mode » ou « ODS-L30M » est sélectionné sur l'écran Select System, passez à l'étape **5**. Si « ODS-L10 » est sélectionné, passez à l'étape suivante.

2 Saisissez l'adresse IP configurée sur le ODS-L10 et l'ID de connexion (nom d'utilisateur)/mot de passe pour vous connecter à ODS-L10, puis cliquez sur [Next].

Le PC se connecte à ODS-L10.
La page Drive Setting apparaît si la connexion est réussie.

3 Si une unité de lecture est connecté au PC de contrôle mais n'est pas installé sur le ODS-L10, déconnectez-le du PC de contrôle afin d'effectuer une vérification du lecteur.

4 Cliquez sur [Next].

La vérification du lecteur commence.
Si un seul unité de lecture est installé sur le ODS-L10, un message de confirmation apparaît vous demandant s'il se trouve dans le logement du haut ou du bas. S'il est installé dans le logement du bas, cliquez sur [Yes]. S'il est installé dans le logement du haut, cliquez sur [No]. L'écran Administrator Setup apparaît lorsque la vérification du lecteur est terminée.

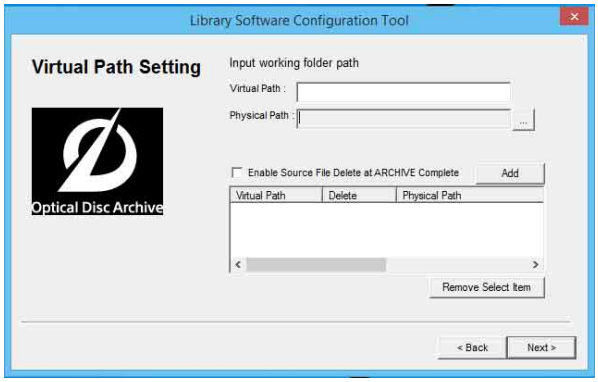
5 Créez un compte à utiliser lors de la connexion à ODS-FM2. Saisissez l'ID de connexion et le mot de passe, puis cliquez sur [Next].

Lorsque le mode File Manager est sélectionné, réglez le dossier racine (chemin d'accès de base) lors des étapes **6** et **7**. Lorsque le mode File Server est sélectionné, passez à l'étape **8**.

6 Indiquez le dossier racine (chemin d'accès de base) à afficher sur l'écran Archive du ODS-FM2.

Seuls les fichiers/dossiers sous le chemin d'accès de base indiqué sont affichés sur l'écran Archive. Restreindre les dossiers qui sont affichés empêche les

fichiers système d'être modifiés par erreur. Plusieurs chemins d'accès de base peuvent être spécifiés.



Virtual Path : saisissez le nom pour le chemin d'accès de base à afficher sur l'écran Archive.

Physical Path : indiquez le chemin physique pour le chemin d'accès de base à afficher. Vous pouvez également spécifier un chemin d'accès réseau.

Enable Source File Delete at ARCHIVE Complete : choisissez de supprimer automatiquement le fichier après l'archivage ou non. Si vous ne le sélectionnez pas, le fichier archivé reste et doit être effacé manuellement lorsque vous n'en avez plus l'utilité.

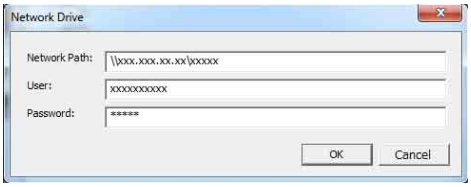
Bouton Add : ajoute le chemin d'accès de base avec les réglages spécifiés. Le chemin d'accès de base spécifié est ajouté à la liste inférieure.

Pour attribuer un chemin d'accès réseau

① Cliquez sur le bouton […] pour l'élément [Physical Path].

② Cliquez sur le bouton [Add Network Drive] dans la boîte de dialogue [Reference].

③ Saisissez le chemin d'accès réseau au format UNC (\\nom_serveur ou adresse_IP\nom_partage\nom_dossier) dans [Network Path] de la boîte de dialogue [Network Drive].
Configurez les réglages comme décrit dans *« Réglage des informations d'identification d'utilisateur de connexion pour le chemin d'accès réseau » (page 14)* au préalable.



④ Si nécessaire, saisissez un nom d'utilisateur et un mot de passe, [User] et [Password], respectivement.

⑤ Cliquez sur le bouton [OK].
Le chemin d'accès réseau ajouté est affiché dans la boîte de dialogue [Reference].

⑥ Sélectionnez le chemin d'accès réseau et cliquez sur le bouton [Select].
La boîte de dialogue [Reference] se ferme, et le chemin d'accès réseau apparaît dans l'élément [Physical Path] sur la page Virtual Path Setting.

⑦ Spécifiez [Virtual Path] et cliquez sur le bouton [Add].

7 Après avoir défini le(s) chemin(s) d'accès de base, cliquez sur [Next].

8 Cliquez sur [Finish] lorsque la configuration est terminée et que la boîte de dialogue apparaît.

9 Connectez le réseau sur lequel se trouvent les PC client à un port réseau sur le PC de contrôle.

Si vous utilisez une connexion réseau au ODS-L10, connectez les PC client à un autre réseau que le ODS-L10.
Le système d'archivage sur disque optique peut maintenant être utilisé grâce à l'application Web depuis un PC client.

Remarques

- Si le logiciel antivirus ou le logiciel de sécurité est installé sur le PC de contrôle, l'accès d'entrée par le port 8080 depuis un PC client risque d'être bloqué. Dans ce cas, configurez votre logiciel de sécurité pour permettre l'accès d'entrée par le port 8080. Pour plus de détails sur la configuration, consultez le mode d'emploi de votre logiciel de sécurité.
- **Si la configuration du matériel du dispositif est modifiée ou si la connexion de l'unité de lecture est modifiée, ODS-FM2 ne fonctionnera plus correctement. Si cela se produit, reconfigurez les réglages du logiciel ODS-FM2 à l'aide de Library Software Configuration Tool.**
- Si les réglages de configuration du dispositif ODS-L10 ou ODS-L30M sont modifiés dans le menu Setup de la page Web ou sur l'écran du panneau avant de l'unité, reconfigurez le logiciel ODS-FM2 à l'aide de Library Software Configuration Tool.
- Optical Disc Archive Filer ne peut pas être démarré lorsque vous utilisez ODS-FM2. Pour utiliser Optical Disc Archive Filer, mettez d'abord fin au service ODS-FM2 puis démarrez Optical Disc Archive Filer. (Optical Disc Archive Filer est compris dans Optical Disc Archive Software.)

Paramètres du pare-feu

Les paramètres du pare-feu suivants sont recommandés pour bloquer les connexions à MariaDB depuis une source externe.

1 Sélectionnez [Panneau de configuration] > [Système et sécurité] > [Pare-feu Windows] > [Paramètres avancés] > [Règles de trafic entrant] > [Nouvelle règle…].

2 Configurez les éléments suivants dans l'Assistant Nouvelle règle de trafic entrant.

- Type de règle : sélectionnez [Port].
- Protocole et ports : sélectionnez [TCP] et [Ports locaux spécifiques] (saisissez le port « 3306 »).
- Action : sélectionnez [Bloquer la connexion].
- Profil : sélectionnez tout.
- Nom : saisissez le nom « MariaDBPort ».

3 Cliquez sur [Terminer].

4 Sélectionnez à nouveau [Nouvelle règle...] pour afficher l'Assistant Nouvelle règle de trafic entrant, et configurez les éléments suivants.

- Type de règle : sélectionnez [Port].
- Protocole et ports : sélectionnez [UDP] et [Ports locaux spécifiques] (saisissez le port « 3306 »).
- Action : sélectionnez [Bloquer la connexion].
- Profil : sélectionnez tout.
- Nom : saisissez le nom « MariaDBPort ».

5 Cliquez sur [Terminer].

Paramètres des communications HTTPS

Les communications peuvent être cryptées en réglant la communication HTTPS.

Génération d'un fichier de magasin de clés

1 Lancez [Invite de commandes].

2 Saisissez la commande suivante.

cd C:\Program Files\Zulu\zulu-8-jre\bin
keytool -genkey -alias tomcat -keyalg RSA -keysize 2048 -keystore <*nom de fichier du magasin de clés*>

Exemple de nom de fichier de magasin de clés :
filemanager2.keystore

3 Saisissez un mot de passe lorsque vous êtes invité à régler un mot de passe de magasin de clés.

Enter keystore password : ********
(mot de passe non affiché)

4 Saisissez à nouveau le même mot de passe lorsque vous y êtes invité.

Re-enter new password : ********
(mot de passe non affiché)

5 Saisissez les informations relatives à la demande de signature de certificat (CSR).

Exemple de saisie :

```
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 Corporation
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 Vérifiez le contenu affiché des informations saisies, puis saisissez « yes ».

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

7 Appuyez sur la touche Retour (Entrée) sans rien saisir lorsque l'invite suivante s'affiche.

Enter key password for (RETURN if same as keystore password) :
Un fichier de magasin de clés avec le nom spécifié à l'étape **2** est généré.

Génération d'un CSR

1 Lancez [Invite de commandes].

2 Saisissez la commande suivante.

cd C:\Program Files\Zulu\zulu-8-jre\bin
keytool -certreq -sigalg SHA1withRSA -alias tomcat -file <*nom de fichier CSR*> -keystore <*nom de fichier du magasin de clés*>

Exemple du nom de fichier CSR :
filemanager2.csr

3 Saisissez le mot de passe spécifié lors de la génération du fichier de magasin de clés lorsque vous y êtes invité.

Enter keystore password : ********
Un fichier CSR avec le nom spécifié à l'étape **2** est généré.

Émission d'un certificat de serveur

Passez le CSR généré à une autorité de certification pour qu'un certificat de serveur signé soit émis.

Génération d'un certificat de serveur utilisé par les applications

1 Placez le certificat de serveur signé et le certificat intermédiaire dans un répertoire arbitraire.

2 Lancez [Invite de commandes].

3 Fusionnez le certificat de serveur signé et le certificat intermédiaire dans un répertoire arbitraire.

copy <*nom de fichier du certificat de serveur signé*> + <*nom de fichier du certificat intermédiaire*> <*nom de fichier du certificat de serveur utilisé par les applications*>

Exemple de nom de fichier de certificat de serveur utilisé par les applications :
filemanager2.cer

Installation d'un certificat

1 Saisissez la commande suivante.

keytool -import -alias tomcat -keystore <*nom de fichier du magasin de clés*> -file <*nom de fichier généré à la section précédente étape **3***>

2 Saisissez le mot de passe spécifié lors de la génération du fichier de magasin de clés lorsque vous y êtes invité.

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

3 Saisissez « yes » si l'invite suivante s'affiche.

```
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
```

Les astérisques indiquent l'affichage des informations enregistrées.

Activation HTTPS

1 Arrêtez le service Tomcat.

① Dans le menu [Démarrer], cliquez sur [Outils d'administration Windows] > [Services].

② Recherchez et cliquez sur le service « Apache Tomcat » dans la liste des services.

③ Cliquez sur [Arrêter un service] sur le côté gauche de la liste des services.

2 Éditez le fichier de configuration Tomcat (server.xml).

① Ouvrez C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\server.xml.

② Saisissez le nom de domaine réel à la ligne 104.

Avant l'édition

```
<Engine name="Catalina" defaultHost="localhost">
```

Après l'édition

```
<Engine name="Catalina" defaultHost="<nom de domaine>">
```

③ Saisissez le nom de domaine réel à la ligne 124.

Avant l'édition

```
<Host name="localhost" appBase="webapps"
    unpackWARs="true" autoDeploy="true">
```

Après l'édition

```
<Host name="<nom de domaine>" appBase="webapps"
    unpackWARs="true" autoDeploy="true">
```

④ Annulez le commentaire du bloc à la ligne 85.

⑤ Copiez le contenu ci-dessous dans « Après l'édition ».

⑥ Saisissez le chemin d'accès complet du fichier de magasin de clés réel dans <*nom de fichier du magasin de clés*> et saisissez le mot de passe spécifié lors de la génération du fichier de magasin de clés dans <*mot de passe du magasin de clés*>.

Avant l'édition

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

Après l'édition

```
<Connector port="8443"
    protocol="org.apache.coyote.http11.Http11Protocol"
    SSLEnabled="true"
    maxThreads="150"
    scheme="https"
    secure="true"
    keystoreFile="<nom de fichier du magasin de clés>"
    keystorePass="<mot de passe du magasin de clés>"
    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"
/>
```

Pour empêcher les communications HTTP, annulez le commentaire du bloc à la ligne 70 comme suit.

Avant l'édition

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

Après l'édition

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

3 Démarrez le service Tomcat.

① Dans le menu [Démarrer], cliquez sur [Outils d'administration Windows] > [Services].

② Recherchez et cliquez sur le service « Apache Tomcat » dans la liste des services.

③ Cliquez sur [Démarrer un service] sur le côté gauche de la liste des services.

4 Exécutez Config Tool.

5 Vérifiez la communication HTTPS.

Lancez un navigateur Web et accédez à « https://<*nom de domaine*>:8443 » et vérifiez que l'écran de connexion s'affiche.

Configuration de l'auto-récupération du service DB

1 Saisissez « Services » dans le champ de recherche de la barre des tâches, puis sélectionnez [Services].

2 Sélectionnez et double-cliquez sur « MariaDB » dans la liste.

3 Cliquez sur l'onglet [Récupération] dans la boîte de dialogue [Propriétés de MariaDB].

4 Sélectionnez [Redémarrer le service] dans les menus déroulants [Première défaillance], [Deuxième défaillance] et [Défaillances suivantes].

5 Réglez [Réinitialiser le compteur de défaillances après] sur jour 1 et [Redémarrer le service après] sur 1 minute.

6 Cliquez sur le bouton [Appliquer] pour fermer la boîte de dialogue.

Réglage des informations d'identification d'utilisateur de connexion pour le chemin d'accès réseau

1 Saisissez « Gestionnaire d'identification » dans la zone de recherche de la barre des tâches, puis sélectionnez [Gestionnaire d'identification Panneau de configuration].

2 Sélectionnez [Informations d'identification Windows], et cliquez sur [Ajouter des informations d'identification Windows].

3 Saisissez le chemin d'accès réseau à enregistrer dans le chemin de base, ainsi que le nom d'utilisateur et le mot de passe.

4 Cliquez sur le bouton [OK] pour fermer la boîte de dialogue.

Affichage de l’application Web

Si la communication HTTPS n’est pas configurée

Affichez un navigateur Web sur un PC client, puis saisissez « http:///(adresse IP du PC de contrôle):8080/ » dans la barre d’adresses. L’écran de connexion apparaît lorsque le navigateur Web se connecte au PC de contrôle. Saisissez le nom d’utilisateur et mot de passe configurés dans le Library Software Configuration Tool pour vous connecter.

Si la communication HTTPS est configurée

Ouvrez une fenêtre de navigateur Web sur un PC client, puis saisissez « http://<*nom de domaine*>:8443/ » dans la barre d’adresses.
L’écran de connexion apparaît lorsque le navigateur Web se connecte au PC de contrôle. Saisissez le nom d’utilisateur et mot de passe configurés dans le Library Software Configuration Tool pour vous connecter.

ODS-FM2(WW)
5-000-612-**37** (1)

Sony Corporation