

# iR Security Kit-A2 Installation Procedure

## Procédure d'installation du Kit de Sécurité-A2 pour iR

## Installationsverfahren für den iR Security Kit-A2

## Procedura di installazione di iR Security Kit-A2

Take the following steps when this security kit is installed to the host machine.

ENGLISH

Procéder aux étapes suivantes lorsque ce kit de sécurité est installé sur la machine hôte.

FRANÇAIS

Für die Installation der Sicherheitsausrüstung in dem Hostgerät ist wie folgt vorzugehen.

DEUTSCH

Per installare il kit di sicurezza nella macchina host, procedere come descritto di seguito.

ITALIANO



# 1.1 Points to Note About Installation

---

## 1.1.1 Points to Note at Time of Installation

0007-7622

---

### **Caution**

#### 1. Required Accessories

To install the product, you will need the following separately available accessories:

Expansion Bus-B1, USB Application Interface Board-D1 (except US), iR 256MB Expansion RAM-B1 (except US). Be sure that these accessories have been properly installed before starting the work; otherwise, there will be a message to indicate the absence of resources when you attempt to register a license key. The special option may be needed with the copier product used.

#### 2. Time Needed for HDD Initialization

- When the machine restarts for the first time after a license key has been registered, it may take more than 30 min to complete a restart run. It may take even longer if you have changed service mode settings to select 'write random data 3 times'.

The user data will be deleted from the hard disk for the following:

- when the security function is enabled by registering the product's license key
- when a data encryption key is re-generated
- when the product's license key is invalidated to stop using the security function

Before attempting any of the foregoing, be sure to inform the user's device supervisor that the items of data shown in the following table will be lost and it is important to make a backup of data as necessary. Making a backup, however, is not the work of the service person, as it inherently involves security issues. The instructions herein are for reference purposes only.

T-1-1

<b>Data Erased</b>	<b>Able to Be Backed Up</b>
Information registered in the Address Book	Yes
Settings made from the Additional Functions screen	Yes*1
Forwarding Settings	Yes

<b>Data Erased</b>	<b>Able to Be Backed Up</b>
MEAP applications	Yes
License files for MEAP applications	Yes
Registered SDL (Simple Device Login) user authentication information	Yes
Data saved using MEAP applications	Yes*2
MEAP SMS (Service Management Service) password (the password will return to its default password if it was changed)	No
Mode Memory settings registered in the Copy and Mail Box functions	No
Data stored in inboxes	No
Scan modes registered in the Send Function	No
Unsent documents (documents waiting to be sent with the Delayed Send mode)	No
Image forms stored in the Form Composition mode	No
Job logs	No

\*1 Can only be backed up using the Remote UI or Device Information Delivery Settings mode.

\*2 Depending on the MEAP application.

Items of data that can be backed up

#### T-1-2

<b>The data can be backed up</b>	<b>Reference</b>
Address Book Settings	See the Remote UI Guide.
Additional Functions Settings	
Forwarding Settings	
Information on exporting data	
License files for MEAP applications	See the MEAP SMS Administrator's Guide.
Information on downloading license files	

The data can be backed up	Reference
User authentication information registered with SDL	See the MEAP SMS Administrator's Guide.
Information on exporting user authentication information	
Information which can be delivered using the Device Information Delivery Settings mode	Can only be backed up if you have another imageRUNNER machine that is equipped with the Device Information Delivery Settings mode. It is not necessary to back up this information if you want to use it. For more information on the Device Information Delivery settings mode, see the Reference Guide.
Data saved by MEAP applications	Depending on the MEAP application. For information, see the documentation included with the application.

#### 4. Work After Installing the Kit

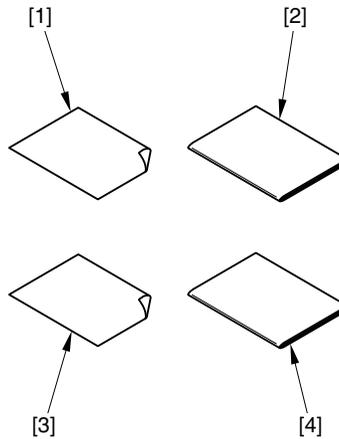
- If you disable functions of the Security Kit, passwords set for User Inboxes, Confidential Fax Inboxes, and the Memory RX Inbox are erased. Set these passwords again.
- If you have logged in to the machine using a login service, such as SDL (Simple Device Login) or SSO (Single Sign-On) before disabling functions of the Security Kit, you must select the login service again in SMS (Service Management Service) after restarting the machine. For information on changing the login service, see the MEAP SMS Administrator's Guide.

## 1.2 Checking components

---

### 1.2.1 Checking Items in the Package

0008-2781



F-1-1

[1] License Access Number Certificate Sheet	1pc.
[2] Reference Guide	1pc.
[3] Caution sheet for Users	1pc.
[4] License Registration Booklet	1pc.

## 1.3 Installation procedure

---

### 1.3.1 Backing Up

#### Data

(reference only) 0008-3214

**Memo: Points to note when the security kit and its iR machine are installed at a time.**

Install the security kit first if the security kit and its iR machine are installed at a time. Backup work is unnecessary in this case. If the security kit is installed in a machine that is already set up, backup work is required.

Overview of backup procedures for each data is as follows.

**Backup using the import/export function of Remote UI**

**Procedure for backing up address book information**

(1) Access the following URL, and access Remote UI.

[http:// \[Device IP Address\] /](http:// [Device IP Address] /)

(2) Click Add. Func., and select import/export from the menu displayed. A dialog box is displayed at this time if a system administrator ID and a password are set up. Enter a system administrator ID in the user name field, and a password in the password field. Click OK.

(3) Click Address Book and click Export.

(4) Select Address Book and file format, and click Start Export.

(5) Specify a storage location of the files according to the screens. Name files to easily identify a file and its page of address book.

**Memo:**

All information in address book is included once Forwarding settings are exported.

Backup of Address Book is unnecessary if there is no need to backup pages individually.

**Procedure for exporting Forwarding settings**

(1) Access the following URL, and access Remote UI.

[http:// \[Device IP Address\] /](http:// [Device IP Address] /)

(2) Click Add. Func., and select import/export from the menu displayed. A dialog box is displayed at this time if a system administrator ID and a password are set up. Enter a system administrator ID in the user name field, and a password in the password field. Click OK.

(3) Click Forwarding settings.

(4) Click Export, and click Start Export.

(5) Specify a storage location of files according to the screens.

**Procedure for exporting Additional Functions**

(1) Access the following URL, and access Remote UI.

http:// [Device IP Address] /

- (2) Click Add. Func., and select Import/Export from the menu displayed. A dialog box is displayed at this time if a system administrator ID and a password are set up. Enter a system administrator ID in the user name field, and a password in the password field. Click OK.
- (3) Click Additional Functions and Click Export.
- (4) Select Address Book, and click Start Export.
- (5) Specify a storage location of files according to the screens.

### **Backup using the device information delivery function**

If same iR machines connected on the network are installed more than two and they have the device information delivery function, it is possible to register one machine as a master and deliver same information to the other machines to synchronize settings.

Refer to [Device Information Delivery] in the Reference Guide.

- (1) Make settings of a master machine (i.e., transmission side). Register destinations of device information to the master machine. Select Additional Functions>System Settings>Device Information Delivery Settings>Register Destinations.
- (2) Register destinations manually/ automatically. In the case of auto-search, select destinations from search results, and

press OK.

- (3) Check settings status of destinations to see if the master machine can send device information to slave machines.
- (4) Make manual delivery settings. Make the settings when slave machines are not used on the network/Local UI.
- (5) Select Additional Functions>System Settings>Device Information Delivery Settings>Transmitting and Settings>Manual Delivery. Set target information for delivery to ON from Add. function settings value, Dept. ID, and Address Book, and press Next.

If address book is selected, forwarding settings and favorites button settings are also delivered.

- (6) Select destinations, and press Manual delivery start. Device information will be delivered to the specified slave machines. Check delivery results after delivery.

### **Backup of MEAP applications**

If any of MEAP applications is already installed, data and a license stored in the MEAP application is deleted. However, you don't need to consider it if MEAP applications are not installed.

If a MEAP application has the backup function, be sure to backup data specific to the MEAP application using the function. For licenses, it is necessary to stop all applications from SMS (Service Management Service), disable the licenses, and download the disable license files.

**Note: MEAP backup function using SST**

Concerning data backed up with MEAPback of SST before starting the security kit, it must not be re-written to the iR machine after the security kit starts to run. Also, if data backed up after the security kit starts to run is re-written to an iR machine that the security kit is yet to run, it does not work properly. It is absolutely necessary to match operating conditions of the security kit before and after backup work. For that reason, backup is impossible with the MEAP backup function while installing the security kit.

The following procedures are for stopping MEAP applications, disable licenses, and downloading license files. Refer to the MEAP SMS Administrator Guide for details.

**Stopping/Disabling MEAP applications, Downloading license files, Uninstalling MEAP application.**

(1) Select the following URL to access SMS.  
`http://[Device IP Address]:8000/sms`  
If user changed a SMS password from a default, ask the user to login or ask the user to change the password after the security kit starts to run. The default password is [MeapSmsLogin].

**Note:**

SMS password will be initialized after the security kit starts to run.

Therefore, be sure to ask user to change a password.

(2) Select the radio button of an application to be stopped from the Application list page, and click stop.

(3) Click name of application that a license is Installed, and access the Application License Information page.

(4) Click License Management, and click Disable. Click OK on the Disable license file confirmation screen.

(5) Click download from Download/Delete Disabled License File.

Specify a storage location of a file according to indications on the screens. At this time, name the file to easily identify an application and its disable license file. Click deletion after the disable license file is downloaded to PC. Click OK on the Delete disabled license file confirmation screen.

(6) Go back to the application list page, and select the radio button of an application to be uninstalled. Then, click uninstall. Click OK on the uninstallation confirmation screen. Repeat the steps (1) to (6) if there are multiple applications.

(7) After the security kit starts to run, re-install applications using application files (jar file) of applications and the backed up disable license files (.lic file).

### **User authentication information registered in SDL (Simple Device Login)**

When user changed a login application of MEAP to SDL, backup of user authentication information is necessary according to the following procedure.

- (1) Access the following URL.  
`http:// [Device IP Address]:8000/sdl/`
- (2) Login using user name and a password registered in SDL as an administrator.  
Defaults are as follows:  
User name: Administrator  
Password: password
- (3) Click user management.
- (4) Place a checkmark to Select All, and click Export.
- (5) Click start without changing File Format and Encoding from defaults.
- (6) Specify a storage location of file, and click save.

#### **Note: Data that backup is impossible**

Data stored in the boxes, yet-to-be-transmitted documents, overlaid-image data are deleted since backup is impossible. Ask user how to handle data that backup is impossible, and take appropriate actions such as printing out the data if necessary.

Refer to Points to Note on Installation for details of data that backup is impossible.

### **1.3.2 Obtaining and Registering the license key**

0008-3227

After completion of data backup, then move to next step: obtain a license key through LMS and register it. Basically users are supposed to operate obtaining their license keys by themselves following the License Registration booklet Guide, which offers the detailed procedures. The outline of the procedures is described below just for reference.

#### **Memo: What is LMS?**

The LMS (License Management System) is new license server system, which has been offered by Canon Inc. to be used as a mean of validating the iR software options. The purposes of the system are to centrally manage the options in the forms of license and to keep the options from being copied. Instead of conventional methods, such as a dongle or PC, in this new system, the license keys are used in order to validate the options. Basically users are supposed to do the operation, however, the situation will be various in countries or regions. When purchasing an option, a license access number certificate sheet is packaged with the option. The access number is used to obtain a license key, which is specific to the number. Users can access to the Web server, the LMS itself, with the number, and obtain the license key. With the license key is registered to

the iR device, the function of the option is validated finally.

When users input both the number on the license access number certificate sheet and the device serial No. of the iR itself to the LMS, a license key composed of 24-digit number, which is specific to each option, is generated. The key includes the information of the device serial No., therefore, users cannot use the key to other devices. Additionally, when once the option information is validated, it will not be invalidated even if parts are replaced for repairs since the information is backed up and stored in the device.

**Procedures to obtain and register the license key**

(1) Access to the LMS clicking the URL below, and obtain a license key following instructions displayed on the screen step by step.

The URL of the LMS  
<http://www.canon.com/lms/ir/>

**Memo:**

When users obtain a license key, both the 24-digit number on the License Access Number Certificate Sheet and the serial No. (e.g.: ABC01234) of the device to be installed are required. The device serial No. is displayed in the "Serial Number" when the counter key of the iR is pressed.

(2) Write down the 24-digit number displayed on the Web in the space provided on the license access number certificate sheet.

**Memo:**

Make sure to transcribe correctly. Give an appropriate explanation to users so that they will keep License Access Number Certificate Sheet surely.

(3) Press the Additional function>System settings>License Registration, then input the license key in the designated space, and press Start key so that the license key is registered and the function of the option is validated.

If the function fails to be validated, an error message will be displayed. Refer to the followings what action to be required.

"There are not enough required features for install."

→Check if the USB Application Interface Board-D1 is recognized correctly and also check if the RAM capacity is 512MB. The special option may be needed with the copier product used.

"The value for the license key is incorrect. Check the license key."

→Check if the license key issued to another device is used.

→Check if the license key is input wrongly.

→Check if the license key is correct.

"This function has already enabled."

→Check if the security function has already been enabled.

(4) Press the power switch on the control panel for 3 seconds or more. Following the instructions displayed on the shutdown sequence step by step with operations to select appropriate items on the touch panel so that the main switch can be ready for turning off. Turn the main power off, and after 10 seconds, turn it on again.

(5) The registered license will be validated when the power supply of the device itself is turned on once again.

At the first reboot after the license key registration, in some cases, it might take 30 min. or more in order to initialize the data in HDD. If the data erasing method of HDD of the device is set to "Overwrite random data 3 times", it might take longer than the cases above. Make sure not to turn off the power supply when the message, "Remaining data that is not needed is being erased. Do not turn off the main power.", is displayed.

(6) When the device starts normally, press counter key and then press the Device Configuration to check if the security kit is displayed in the space of options. Then, set the Service mode at user's request.

### 1.3.3 Setting the

#### Service mode

0008-2981

When this kit is installed, the Service mode needs changing in response to the user's request.

#### **1. Changing the setting of "Complete erasing of HDD"**

Change the setting of complete erasing of HDD at user's request.

- Service mode level 2

COPIER>OPTION>USER>HDCR-DSP

Set value

1: Overwrite NULL data one time

2: Overwrite Random data one time

3: Overwrite Random data three times

Default value: 1

#### **Note:**

As the value is set higher, the security level becomes higher while the performance level becomes lower.

#### **2. Switching the key of "Job Log Display ON/OFF" between display and not display**

Switch the key of "Job Log Display ON/OFF" between display and not display.

- Service mode level 2

COPIER>OPTION>USER>LGSW-DSP

Set value

0: Not display the key

1: Display the key

Default value: 0

**Note:**

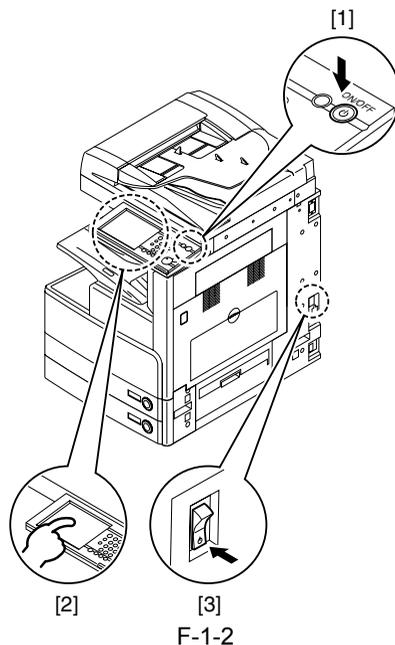
When this key is set to "1", the device will always respond "0" to the demands of job history reference from the remote applications. Therefore, software, such as NetSpot Accountant, which manages the device using the job history, cannot be used.

**3. OFF/ON of connection devices**

Re-start procedure may change with connection apparatus used.

When the setting of the Service mode is changed, need to turn off/ on the power of connection devices.

- 1) Press the power switch on the control unit for 3 seconds or more.
- 2) Following the instructions displayed on the shutdown sequence step by step with operations to select appropriate items on the touch panel so that the main switch can be ready for turning off.
- 3) Turn the main power off.



- 4) Turn the main power on.

**Memo:**

If the target data to be erased completely remain in the HDD at the time of turning off the main power, the erasing operation will be carried out at the start-up.

# Procédure d'installation du Kit de Sécurité-A2 pour iR

Procéder aux étapes suivantes lorsque ce kit de sécurité est installé sur la machine hôte.

## 1.1 Points caractéristiques de l'installation

---

### 1.1.1 Points caractéristiques de l'installation

0007-7622

---

#### **Attention**

1. Les options suivantes sont requises pour l'installation du kit de sécurité : Kit d'extension B1 du Bus PCI, carte I/F USB-D1 et extension RAM imprimante 256 Mo-B1 (sauf sur modèle 120V)

Assurez-vous auparavant que ces options soient installées. Si elles ne sont pas installées, la clé de licence ne pourra être enregistré et le message "Il manque des options requises pour l'installation" apparaîtra.

2. Les données de l'utilisateur sont effacées dans les cas suivants.

- Lors de l'enregistrement d'une clé de licence du kit de sécurité pour activer les fonctions de sécurité.
- Lors d'une nouvelle création de clé d'encryptage des données.
- Lors de l'annulation d'une licence du kit de sécurité pour arrêter la sécurité.

Informez la personne chargée de l'administration de l'appareil que les données ci-dessous sont toutes effacées si l'une des actions ci-dessus est effectuée et qu'il est par conséquent nécessaire d'effectuer une sauvegarde des données. Pour des raisons de sécurité, une personne quelconque du service ne doit pas sauvegarder les données de l'utilisateur. Pour référence, la procédure de sauvegarde est indiquée dans ce manuel.

Données à effacer

- Données stockées dans les boîtes de courrier
- Informations contenues dans le carnet d'adresses
- Paramètres de numérisation mémorisés pour la fonction de transmission
- Mode de mémoire enregistré pour les fonctions copie / boîte

- Applications MEAP et fichiers de licence
- Données stockées pour chaque application MEAP
- Mot de passe du Service Management Service (SMS) MEAP  
(Si l'utilisateur change le mot de passe, celui-ci se réinitialise aux paramètres d'usine)
- Informations d'authentification de l'utilisateur enregistré en SDL (Simple Device Login)
- Documents en attente de transmission (par exemple les documents à transmission programmée/en réserve de transmission)
- Historique des tâches
- Paramètres définis en mode utilisateur
- Paramètres d'expédition mémorisés

L'utilisateur doit sauvegarder les données suivantes:

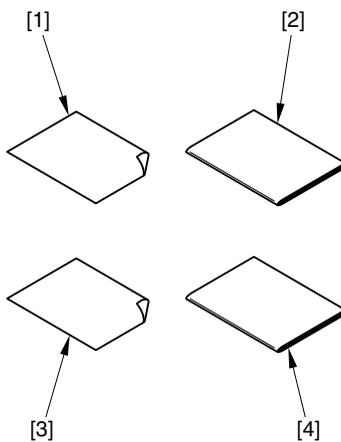
- Carnet d'adresses, paramètres des fonctions supplémentaires, paramètres d'expédition  
(Voir le [Guide Remote UI] pour l'exportation des données.)
- Fichiers de licences des applications MEAP  
(Voir le [Guide administrateur MEAP SMS] pour le téléchargement des fichiers de licence.)
- Informations d'authentification de l'utilisateur enregistré en SDL  
(Voir le [Guide administrateur MEAP SMS] pour l'exportation des informations d'authentification.)
- Données enregistrées pouvant être transmises en utilisant la fonction de transmission d'informations  
(Sauvegarde possible uniquement si une autre machine iR possède la fonction de transmission d'informations. La sauvegarde n'est pas nécessaire si les données de l'utilisateur sont mémorisées dans la machine iR. Voir le [Guide de référence] pour les fonctions de transmission d'information.)
- Données stockées dans les applications MEAP  
(Les données stockées doivent être sauvegardées selon les applications MEAP. Pour plus de détails, vérifier le manuel d'instructions de chaque application.)
- Les mots de passe pour les boîtes utilisateur, fax et système sont effacés une fois qu'une clé de licence est enregistrée. Toutefois, assurez-vous d'enregistrer à nouveau ces mots de passe.
- Avant d'enregistrer une clé de licence, il est nécessaire de sélectionner à nouveau le service de login après un redémarrage si l'utilisateur a paramétré l'authentification en SDL (Simple Device Login) ou en SSO (Single Sign-On).
- Le premier redémarrage après l'enregistrement d'une clé de licence peut prendre plus de 30 minutes. Il peut prendre beaucoup plus de temps si l'utilisateur a modifié les paramètres des services pour effacer des données du disque dur par "triple remplacement des données aléatoires".

## 1.2 Vérifier les articles fournis

---

### 1.2.1 Vérifier les articles fournis

0008-2781



F-1-1

[1] Certificat de numéro d'accès à la licence	1
[2] Guide de référence	1
[3] Feuillet d'avertissement pour les utilisateurs	1
[4] Livret d'enregistrement de la licence	1
[5] Procédure d'installation	1

## 1.3 Procédure d'installation

---

### 1.3.1 Sauvegarde des données

0008-3214

**Note: Points caractéristiques à observer lorsque le kit de sécurité et ses machines iR sont installés en même temps.**

Installer d'abord le kit de sécurité si le kit de sécurité et ses machines iR sont installés en même temps. La sauvegarde n'est pas nécessaire dans ce cas. Si le kit de sécurité est installé sur une machine déjà configurée, la sauvegarde est nécessaire.

La vue d'ensemble des procédures de sauvegarde pour chaque type de données est indiquée ci-dessous.

**Sauvegarder en utilisant la fonction import/export de la Remote UI**

**Procédure de sauvegarde des informations du carnet d'adresses**

(1) Accéder à la Remote UI en allant à l'adresse suivante.

http:// [Adresse IP de l'appareil] /

(2) Cliquer sur Add. Func. (Ajouter Fonction) et sélectionner Import/Export sur le menu affiché. Une boîte de dialogue s'affiche alors si une identité d'administrateur système et un mot de passe sont définis. Entrer l'identité de l'administrateur système dans le champ

réservé au nom d'utilisateur et un mot de passe dans le champ correspondant.

Cliquer sur OK.

(3) Cliquer sur le carnet d'adresses.

(4) Sélectionner le carnet d'adresses et le format de fichiers puis cliquer sur "Start Export" (démarrer l'exportation).

(5) Spécifier une destination de stockage pour les fichiers selon les écrans. Nommer les fichiers de manière à identifier facilement le fichier et la page du carnet d'adresses correspondante.

**Note:**

Toutes les informations contenues dans le carnet d'adresses sont incluses une fois que l'exportation des paramètres d'expédition a été effectuée.

La sauvegarde du carnet d'adresses est inutile si la sauvegarde des pages individuelles n'est pas nécessaire.

**Procédure d'exportation des paramètres d'expédition**

(1) Accéder à la Remote UI en allant à l'adresse suivante.

http:// [Adresse IP de l'appareil] /

(2) Cliquer sur Add. Func. (Ajouter Fonction) et sélectionner Import/Export sur le menu affiché. Une boîte de dialogue s'affiche alors si une identité d'administrateur système et un mot de passe sont définis. Entrer l'identité de l'administrateur système dans le champ réservé au nom d'utilisateur et un mot de passe dans le champ correspondant.

Cliquer sur OK.

(3) Cliquer sur "Forwarding settings" (paramètres d'expédition).

(4) Cliquer sur "Export" puis cliquer sur "Start Export" (démarrer l'exportation).

(5) Spécifier une destination de stockage pour les fichiers selon les écrans.

### **Procédure d'exportation des fonctions supplémentaires**

(1) Accéder à la Remote UI en allant à l'adresse suivante.

[http:// \[Adresse IP de l'appareil\] /](http:// [Adresse IP de l'appareil] /)

(2) Cliquer sur Add. Func. (Ajouter Fonction) et sélectionner Import/Export sur le menu affiché. Une boîte de dialogue s'affiche alors si une identité

d'administrateur système et un mot de passe sont définis. Entrer l'identité de l'administrateur système dans le champ réservé au nom d'utilisateur et un mot de passe dans le champ correspondant.

Cliquer sur OK.

(3) Cliquer sur "Additional Functions" (fonctions supplémentaires).

(4) Cliquer sur "Export" puis cliquer sur "Start Export" (démarrer l'exportation).

(5) Spécifier une destination de stockage pour les fichiers selon les écrans.

### **Sauvegarde en utilisant la fonction de transmission d'informations**

Si plus de deux machines iR raccordées au réseau sont installées et si elles possèdent la fonction de transmission d'informations, il est possible d'enregistrer une machine

comme maître et de fournir les mêmes informations aux autres machines pour synchroniser les paramètres.

Voir [Système de transmission d'informations] dans le guide de référence.

(1) Paramétrer la machine maître (par exemple le côté de sortie). Enregistrer les destinations du système d'information vers la machine maître. Sélectionner Additional Functions (Fonctions supplémentaires) >System Settings (Paramètres système)>Device Information Delivery Settings (Paramètres du système de transmission d'informations)>Register Destinations (Enregistrer les destinations).

(2) Enregistrer les destinations manuellement/automatiquement. Dans le cas d'une recherche automatique, sélectionner les destinations pour chaque résultat puis appuyer sur OK.

(3) Vérifier les paramètres de statut des destinations pour voir si la machine maître peut envoyer le système d'information au machines esclaves.

(4) Régler les paramètres une transmission manuelle. Régler les paramètres pour les machines esclaves utilisées hors du réseau/UI local.

(5) Sélectionner Additional Functions (Fonctions supplémentaires)>System Settings (Paramètres système)>Device Information Delivery Settings (Paramètres du système de transmission d'informations)>Manual Delivery Settings (Paramètres de transmission manuelle).

Paramétrer les informations cibles à remettre sur ON en sélectionnant "Add. Function settings" (ajout de paramètre de fonction), "Dept. ID" (Identité Dep.) et carnet d'adresses puis appuyez sur "Next" (suivant).

Si le carnet d'adresses est sélectionné, les paramètres d'expédition et ceux des touches favoris sont également transmis.

(6) Sélectionner les destinations puis appuyer sur "Manual delivery start" (Démarrage transmission manuelle). Les informations de l'appareil seront transmises aux machines esclaves spécifiées. À la fin de la transmission, en vérifier les résultats.

### **Sauvegarde des applications MEAP**

Si une des applications MEAP est déjà installée, les données et la licence enregistrée dans l'application MEAP seront effacées. La sauvegarde est toutefois inutile si aucune application MEAP n'est installée.

Si une application MEAP possède la fonction de sauvegarde, s'assurer de sauvegarder les données spécifiques à l'application MEAP en utilisant cette fonction. Pour les licences, il est nécessaire d'arrêter toutes les applications du SMS (Service Management Service), d'annuler les licences et de télécharger les fichiers de licence désactivés.

### **Note: Fonction de sauvegarde MEAP en utilisant SST**

Les données sauvegardées avec MEAPback du SST avant le démarrage du kit de sécurité ne doivent pas être réinscrites sur la machine iR une fois que le kit de sécurité est en marche. De même, si les données sauvegardées après le démarrage du kit de sécurité sont réinscrites sur une machine iR dont le kit de sécurité n'est pas encore actif, celui-ci ne fonctionnera pas correctement. Il est absolument nécessaire de faire correspondre les conditions de fonctionnement du kit de sécurité avant et après l'opération de sauvegarde. Pour cette raison, la sauvegarde est impossible avec la fonction de sauvegarde MEAP lors de l'installation du kit de sécurité.

Les procédures suivantes indiquent comment arrêter les applications MEAP, désactiver les licences et télécharger les fichiers de licence. Voir le Guide de l'administrateur MEAP SMS pour plus de détails.

### **Arrêt/Désactivation des applications MEAP, Téléchargement de fichiers de licence, Désinstallation des applications MEAP.**

(1) Accéder au SMS en allant à l'adresse suivante.

[http://\[Device IP Address\]:8000/sms](http://[Device IP Address]:8000/sms)

Si l'utilisateur a modifié un mot de passe SMS par rapport à celui d'origine, demander à l'utilisateur de se connecter ou de changer le mot de passe après le

démarrage du kit de sécurité. Le mot de passe par défaut est [MeapSmsLogin].

**Note:**

Le mot de passe SMS sera initialisé après le démarrage du kit de sécurité.

S'assurer toutefois de demander à l'utilisateur la modification du mot de passe.

(2) Sélectionner la case d'option de l'application à arrêter à partir de la page listant les applications, puis cliquer sur "Stop".

(3) Cliquer sur le nom de l'application dont la licence est déjà installée et accéder à la page d'information application/licence.

(4) Cliquer sur "License management" (gestion de licence) puis cliquer sur "Disable" (désactiver). Cliquer sur OK sur l'écran de confirmation du fichier de désactivation de licence.

(5) Cliquer sur télécharger à partir de "télécharger/supprimer les fichiers de licence invalides". Spécifier une destination de stockage pour le fichier selon les écrans. À ce point, nommer le fichier de manière à identifier facilement l'application et son fichier de désactivation de licence.

Cliquer sur "Deletion" (supprimer) une fois que le fichier de désactivation de licence est téléchargé sur PC. Cliquer sur OK sur l'écran de confirmation de suppression du fichier de désactivation de licence.

(6) Retourner à la page listant les applications et sélectionner la case d'option d'une autre application à désinstaller.

Ensuite, cliquer sur "Uninstall" (désinstaller). Cliquer OK sur l'écran de confirmation de désinstallation. Répéter les étapes (1) à (6) pour les autres applications.

(7) Après le démarrage du kit de démarrage, réinstaller les application en utilisant les fichiers d'inscription (fichiers .jar) des applications et le fichier de sauvegarde des licences désactivées (fichiers .lic).

**Informations d'authentification de l'utilisateur enregistré en SDL (Simple Device Login)**

Lorsque l'utilisateur a modifié la connexion d'une application MEAP en SDL, il est nécessaire d'effectuer la sauvegarde des informations d'authentification de l'utilisateur selon les étapes suivantes.

(1) Aller à l'adresse suivante  
[http:// \[Device IP Address\]:8000/sdl/](http://[Device IP Address]:8000/sdl/)

(2) Se connecter en utilisant le nom et le mot de passe enregistrés comme administrateur en SDL.

Les informations par défaut sont:

Nom d'utilisateur: Administrator

Mot de passe: password

(3) Cliquer sur "User management" (gestion d'utilisateur).

(4) Cocher tous les choix et cliquer sur "Export".

(5) Cliquer sur "Start" sans changer le format du fichier et le code du texte par défaut.

(6) Spécifier la destination de stockage du fichier puis cliquer sur "Save" (sauvegarder).

**Note: Données dont la sauvegarde est impossible**

La sauvegarde des données stockées dans les boîtes "documents en attente de transmission" et "données de recouvrement d'image" est impossible.

Demander à l'utilisateur comment traiter les données dont la sauvegarde est impossible, puis prendre les mesures appropriées telles que l'impression des données si nécessaire.

Voir les Points caractéristiques de l'installation pour plus de détails sur les données dont la sauvegarde est impossible.

### 1.3.2 Obtention et enregistrement de la clé de licence 0008-3227

Après l'achèvement de la sauvegarde des données, procéder à l'étape suivante : Obtenir une clé de licence avec le LMS et l'enregistrer. Les utilisateurs sont sensés obtenir les clés de licence par eux-mêmes en suivant les informations du Guide d'enregistrement des licence qui indique les procédures détaillées. L'ébauche des procédures est décrite ci-dessous pour information.

**Note: Qu'est ce que le LMS?**

Le LMS (License Management System) est le nouveau système de serveur de licence qui été proposé par Canon comme moyen de validation des options de logiciels iR. Les buts de ce système sont principalement la gestion des options dans les formulaires de licence et la protection des licences contre la copie. À la place de méthodes conventionnelles, telles que les dongle ou PC, dans ce nouveau système les clés de licence sont utilisées pour valider les options. Les utilisateurs sont sensés effectuer les opérations, cependant, la situation sera différente selon les pays ou les régions. Lors de l'achat d'une option, un certificat de numéro d'accès à la licence est inclus avec l'option. Le numéro d'accès est utilisé pour obtenir une clé de licence spécifique à ce numéro. Les utilisateurs peuvent accéder au serveur Internet, le

LMS même, avec le numéro et obtenir la clé de licence. Lorsque la clé de licence est enregistrée sur l'appareil iR, la fonction de l'option est enfin validée.

Lorsque l'utilisateur entre le numéro du certificat d'accès à la licence et le numéro de série de l'appareil iR sur le LMS, une clé de licence, composée de 24 chiffres et spécifique à chaque option, est créée. La clé inclut les informations du numéro de série de l'appareil, ainsi les utilisateurs ne peuvent utiliser la clé pour d'autres appareils. De plus, lorsque les informations de l'option sont validées, elles ne seront pas invalidées même si des pièces sont remplacées pour réparations, tant que l'information sera sauvegardée et stockée dans l'appareil.

### **Procédures pour obtenir et enregistrer la clé de licence**

(1) Accéder au LMS en cliquant sur l'adresse ci-dessous et obtenir une clé de licence en suivant les instructions affichées à l'écran pas à pas.

Adresse du LMS

<http://www.canon.com/lms/ir/>

#### **Note:**

Lorsque l'utilisateur obtient une clé de licence, le numéro à 24 chiffres sur la carte d'accès à la licence et le numéro de série (par ex. : ABC01234) de l'appareil à installer, sont requis. Le numéro de série de l'appareil est affiché dans le champ

"Serial No." lorsque la touche "Counter" de l'iR est enfoncée.

(2) Noter le numéro à 24 chiffres affiché sur le site Internet, dans l'espace prévu sur le certificat de numéro d'accès à la licence.

#### **Note:**

S'assurer de le noter correctement. Donner une explication adéquate aux utilisateurs afin qu'ils conservent en lieu sûr les cartes de numéro d'accès à la licence.

(3) Appuyer sur Additional function (Fonctions supplémentaires)>System settings (Paramètres système)>License Registration (Enregistrement de licence), puis entrer la clé de licence dans l'espace prévu. Appuyer sur "Start" afin que la clé de licence soit enregistrée et que la fonction de l'option soit validée.

Si la validation de la fonction échoue, un message d'erreur apparaîtra. Voir ci-dessous l'action requise.

"Il manque des options requises pour l'installation."

→ Vérifier que la carte I/F USB-D1 soit correctement reconnue et que la capacité de mémoire soit de 512 Mo.

"La valeur de la clé de licence est incorrecte. Vérifier la clé de licence."

→Vérifier que la clé de licence ne soit pas utilisée pour un autre appareil.

→Vérifier que la clé de licence soit entrée correctement.

→Vérifier que la clé de licence soit correcte.

"Cette fonction a déjà été activée."

→Vérifier que la fonction de sécurité n'ait pas été encore activée.

(4) Appuyer sur l'interrupteur d'alimentation sur le panneau de contrôle pendant au moins 3 secondes. Suivre les instructions affichées sur la séquence d'arrêt pas à pas, sélectionnant les éléments appropriés sur le panneau de contrôle afin de préparer l'interrupteur principal à l'arrêt. Éteindre l'appareil puis le rallumer après 10 secondes.

(5) La licence enregistrée sera validée lorsque l'appareil sera à nouveau allumé. Au premier redémarrage suivant l'enregistrement de la clé de licence, dans certains cas, l'initialisation des données du disque dur peut prendre 30 minutes voire plus. Si la méthode d'effacement des données du disque dur est "triple remplacement des données aléatoires", cela peut prendre plus de temps que le cas ci-dessus. S'assurer de ne pas éteindre l'appareil lorsque s'affiche le message " Il reste des données qui ne doivent pas être effacées. Ne pas éteindre l'appareil " .

(6) Lorsque l'appareil démarre normalement, appuyer sur la touche "counter" (compteur) puis vérifier la présence du kit de sécurité dans les options de configuration de l'appareil. Ensuite, configurer le mode service selon les besoins de l'utilisateur.

### 1.3.3 Paramétrer le mode service 0008-2981

Lorsque le kit est installé, le mode service nécessite des modifications pour répondre aux besoins de l'utilisateur.

#### 1. Modifier les paramètres de l'

##### "Effacement complet du disque dur"

Modifier les paramètres de l'effacement complet du disque dur selon les besoins de l'utilisateur.

- Mode service niveau 2

COPIER>OPTION>USER>HDCR-DSP

Choisir la valeur

- 1: Simple remplacement des données NULL
- 2: Simple remplacement des données aléatoires
- 3: Triple remplacement des données aléatoires

Valeur par défaut: 1

#### **Note:**

Plus la valeur est élevée, plus le niveau de sécurité devient élevé au détriment du niveau de performances.

#### 2. Sélection de l'affichage ou non de la touche "Afficher/Cacher l'historique des tâches"

Sélectionner l'affichage ou non de la touche "Afficher/Cacher l'historique des tâches"

- Mode service niveau 2

COPIER>OPTION>USER>LGSW-DSP

Choisir la valeur

0: Ne pas afficher la touche

1: Afficher la touche

Valeur par défaut : 0

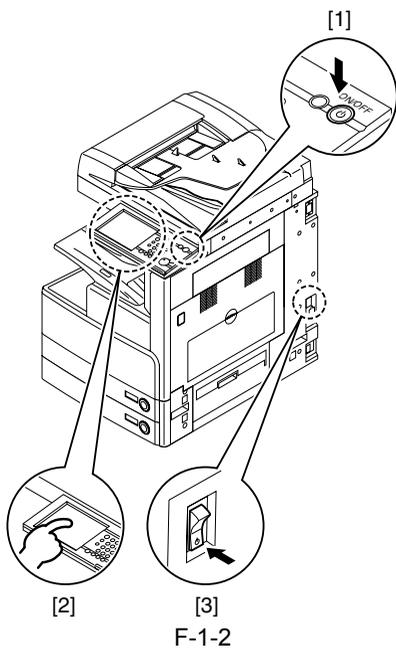
#### **Note:**

Lorsque cette touche est définie sur "1", l'appareil répondra toujours "0" aux demandes de références sur l'historique des tâches provenant d'applications distantes. Ainsi ne peuvent être utilisés les logiciels tel que NetSpot Accountant, qui gère l'appareil en utilisant l'historique des tâches.

#### 3. Marche/Arrêt des systèmes de connexion

Lorsque le paramétrage du mode service est modifié, il est nécessaire d'arrêter puis rallumer les systèmes de connexion.

- 1) Appuyer sur l'interrupteur d'alimentation du panneau de contrôle pendant au moins 3 secondes.
- 2) Suivre les instructions affichées sur la séquence d'arrêt pas à pas, sélectionnant les éléments appropriés sur le panneau de contrôle afin de préparer l'interrupteur principal à l'arrêt.
- 3) Éteindre la machine avec l'interrupteur principal.



4) Rallumer la machine avec l'interrupteur principal.

**Note:**

Si les données qui doivent être effacées complètement restent sur le disque dur au moment de la coupure de l'interrupteur principal, les opérations d'effacement seront exécutées au redémarrage.

# Installationsverfahren für den iR Security Kit-A2

Für die Installation der Sicherheitsausrüstung in dem Hostgerät ist wie folgt vorzugehen.

## 1.1 Bei der Installation zu beachtende Punkte

---

### 1.1.1 Bei der Installation zu beachtende Punkte

0007-7622

---

#### **Vorsicht!**

1. Folgende Optionen sind für die Installation der Sicherheitsausrüstung erforderlich: PCI Bus Expansion Kit-B1, USB Application Interface Board-D1, und iR256MB Expansion RAM-B1 (ausgenommen Modell 120V)

Stellen Sie zuvor sicher, über diese Komponenten zu verfügen. Wenn dem nicht so ist, kann die Registrierung des Lizenzcodes nicht anwendungsbezogen werden und folgende Anzeige erscheint, "Die verfügbaren Optionen sind für ein Fortschreiten der Installation unzureichend".

2. Benutzerdaten auf der Festplatte werden in den nachstehenden Fällen gelöscht.

- Wenn ein Lizenzcode der Sicherheitsausrüstung für die Befähigung der Sicherheitsfunktionen registriert wird.
- Bei der Wiederherstellung eines Datencodierungsschlüssels.
- Wenn ein Lizenzcode der Sicherheitsausrüstung ungültig gemacht wird, um die Sicherheitsoperationen zu stoppen.

Informieren sie den Verwalter der Benutzervorrichtungen darüber, dass alle unten aufgeführten Daten gelöscht werden, wenn eine der folgenden Tätigkeiten ausgeführt wird und veranlassen sie den Benutzer zur Erstellung einer Sicherheitskopie der notwendigen Daten. Unter dem Aspekt der Sicherheit sollte es den Wartungsbediensteten nicht gestattet sein, eine Sicherheitskopie von den Benutzerdaten anzulegen.

Für weitere Informationen ist auf das in diesem Handbuch beschriebene Verfahren für die Anlegung von Sicherheitskopien Bezug zu nehmen.

Daten, die gelöscht werden

- In Mailboxen gespeicherte Daten
- Informationen über die im Adressbuch eingetragene Adressen
- Unter Anwendung der Übertragungsfunktion gespeicherte Scannereinstellungen
- Unter Anwendung der Kopiefunktion/Box gespeicherter Speichermodus
- MEAP Applikationen und Lizenzdatei
- Mit MEAP Applikationen gespeicherte Daten
- Passwort für das Service Management Service (SMS) MEAP  
(wenn der Benutzer das Passwort geändert hat, so wird dieses bei den Werkeinstellungen wiederhergestellt.)
- In SDL (Simple Device Login) gespeicherte Informationen für die Benutzerbeglaubigung
- Yet-to-be- zu übertragene Dokumente (z.B. Dokumente der Timerübertragung/für die Übertragung dediziert)
- Job history Information
- In der Benutzermodalität durchgeführte Einstellungen
- Eingestellte Weiterleitungseinstellungen

Benutzer sollten von den folgenden Daten eine Sicherheitskopie anlegen:

- Adressbuch, zusätzliche Funktionseinstellungen, Weiterleitungseinstellungen  
(beziehen Sie sich auf den [Remote UI Guide] für weitere Informationen über den Datenexport.)
- Lizenzdatei der MEAP Applikationen  
(beziehen Sie sich auf den [MEAP SMS Administrator Guide] für weitere Informationen über das Herunterladen der Lizenzdatei.)
- In SDL gespeicherte Informationen für die Benutzerbeglaubigung  
(beziehen Sie sich auf den [MEAP SMS Administrator Guide] für weitere Informationen über den Export der Beglaubigungsinformation.)
- Gespeicherte Daten, die unter Benutzung der Funktion von der Informationszustellung des Geräts übertragen werden können  
(die Erstellung einer Sicherheitskopie ist nur dann möglich, wenn eine andere iR Vorrichtung vorhanden ist, die über die Funktion der Informationszustellung des Geräts verfügt. Die Erstellung einer Sicherheitskopie ist nur dann möglich, wenn eine andere iR Vorrichtung vorhanden ist, die über die Funktion der Informationszustellung des Geräts verfügt. Die Erstellung einer Sicherheitskopie ist stattdessen nicht nötig, wenn der Benutzer in iR Geräten gespeicherte Daten benutzt. Beziehen Sie sich auf das [Referenzhandbuch] für weitere Informationen über die Funktion der Informationszustellung.)

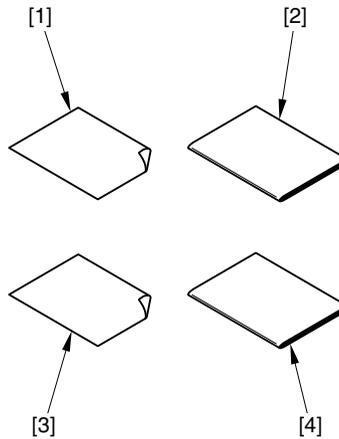
- In MEAP Applikationen gespeicherte Daten  
(je nach der angewandten MEAP Applikation kann von gespeicherten Daten eine Sicherheitskopie angelegt werden. Für weitere Einzelheiten ist das Anleitungshandbuch jeder Applikation einzusehen.)
  - Passworte der Benutzerbox, der Faxbox und der Systembox werden nur einmal gelöscht, wenn der Lizenzcode eingestellt wird. Daher muss die nochmalige Eintragung dieser Passworte sichergestellt sein.
  - Vor der Eintragung eines Lizenzcodes muss der Loginservice nach einem Neustart erneut gewählt werden, wenn der Benutzer eine Eintragung für die Benutzerbeglaubigung in SDL (Simple Device Login) oder SSO (Single Sign-On) gewählt hat
  - Nach der Eintragung eines Lizenzcodes kann diese Operation mehr als 30 Minuten für den Neustart beanspruchen.
- Es kann allerdings länger dauern, wenn der Benutzer die Modalitätseinstellungen des Service aufgrund der auf der Festplatte vorhandenen Datenlöschung durch eine "3-malige Überschreibung der Randomdaten" geändert hat.
-

## 1.2 Artikel in der Verpackung kontrollieren

---

### 1.2.1 Artikel in der Verpackung kontrollieren

0008-2781



F-1-1

[1] Bescheinigung der Lizenzzugriffsnummer	1 St.
[2] Referenzanleitung	1 St.
[3] Unterlagen mit Warnhinweisen für die Benutzer	1 St.
[4] Broschüre der Lizenzeintragung	1 St.
[5] Installationsverfahren	1 St.

## 1.3 Installationsverfahren

### 1.3.1 Sicherheitskopie

der Daten erstellen 0008-3214

**Merkzettel: bei der gleichzeitigen Installation der Sicherheitsausrüstung und des entsprechenden iR Geräts zu beachtende Punkte.**

Bei einer gleichzeitigen Installation der Sicherheitsausrüstung und des iR Geräts muss zuerst die Sicherheitsausrüstung installiert werden. Die Erstellung einer Sicherheitskopie ist in diesem Fall nicht nötig. Wenn die Sicherheitsausrüstung in einem schon konfigurierten Gerät installiert wird, ist stattdessen das Anlegen einer Sicherheitskopie erforderlich.

Nachstehend wird ein Überblick über die Verfahren für die Erstellung einer Sicherheitskopie der Daten beschrieben.

**Anlegung einer Sicherheitskopie unter Anwendung der Import/Export Funktion des Remote UI**

**Verfahren für die Anlegung einer Sicherheitskopie der Adressbuchinformationen**

(1) Zugriff auf das folgende URL, dann Zugriff auf das Remote UI.  
http:// [IP Adresse des Geräts] /

(2) Klicken Sie Add. Func. (Hinzufügung einer Funktion) und wählen Sie Import/Export vom angezeigten Menü. Wenn ein ID System Administrator und ein Passwort konfiguriert worden sind, wird ein Dialogfenster angezeigt. Geben Sie den ID System Administrator in das Feld des User Names (Benutzernamen) und ein Passwort in das Passwortfeld ein. OK klicken.

(3) Adressbuch auswählen.

(4) Adressbuch und Dateiformat wählen, Start Export klicken.

(5) Geben Sie den Speicherplatz der Dateien nach den auf den Bildschirm angezeigten Anweisungen ein. Benennen Sie die Dateien, um eine Datei und ihre Adressbuchseite leicht identifizieren zu können.

**Merkzettel:**

Alle im Adressbuch enthaltenen Informationen werden in dem Augenblick eingeschlossen, in dem die Weiterleitungseinstellungen exportiert werden.

Das Anlegen einer Sicherheitskopie von dem Adressbuch ist nicht nötig, wenn keine Sicherheitskopie von einzelnen Seiten benötigt wird.

**Verfahren für die Ausführung der Weiterleitungseinstellungen**

(1) Zugriff auf das folgende URL, dann Zugriff auf das Remote UI.  
http:// [IP Adresse des Geräts] /

- (2) Klicken Sie Add. Func. (Hinzufügung einer Funktion) und wählen Sie Import/Export vom angezeigten Menü. Wenn ein ID System Administrator und ein Passwort konfiguriert worden sind, wird ein Dialogfenster angezeigt. Geben Sie den ID System Administrator in das Feld des User Names (Benutzernamen) und ein Passwort in das Passwortfeld ein. OK klicken.
- (3) Forwarding Settings wählen (Weiterleitungseinstellungen).
- (4) Export und Start Export klicken.
- (5) Geben Sie den Speicherplatz der Dateien nach den auf den Bildschirmen angezeigten Anweisungen ein

### **Verfahren für den Export der Additional Functions**

- (1) Zugriff auf das folgenden URL und das Remote UI.  
http:// [IP Adresse des Geräts] /
- (2) Klicken Sie Add. Func. (Hinzufügung einer Funktion) und wählen Sie Import/Export vom angezeigten Menü. Wenn ein ID System Administrator und ein Passwort konfiguriert worden sind, wird ein Dialogfenster angezeigt. Geben Sie den ID System Administrator in das Feld des User Names (Benutzernamen) und ein Passwort in das Passwortfeld ein. OK klicken.
- (3) Additional Functions klicken.
- (4) Export und Start Export klicken.
- (5) Geben Sie den Speicherplatz der Dateien nach den auf den Bildschirmen angezeigten Anweisungen ein.

### **Anlegung einer Sicherheitskopie durch die Funktion der**

#### **Informationszustellung**

Wenn mehr als zwei gleiche iR Vorrichtungen auf einem Netz zusammenschlossen sind und wenn diese die Funktion der Informationszustellung besitzen, kann eine Vorrichtung als Master eingestellt werden und für eine Synchronisierung der Einstellungen die gleichen Informationen zu den anderen Vorrichtungen senden. Nehmen Sie auf das Kapitel [Zustellung der Informationen der Vorrichtung] in dem Referenzhandbuch Bezug.

- (1) Führen Sie die Einstellungen der Mastervorrichtung aus (z.B. Übertragungseinstellungen). Wählen Sie Additional Functions>System Settings>Device Information Delivery Settings>Register Destinations.
- (2) Stellen Sie die Destinationen manuell/automatisch ein. Bei einer automatischen Suche sind die Destinationen von den Ergebnissen der Suche zu wählen. OK klicken.
- (3) Überprüfen Sie den Status der Destinationseinstellungen um festzustellen, ob das Mastergerät zur Weiterleitung der Informationen der Vorrichtung zu den Slavemaschinen fähig ist.

(4) Führen Sie die Einstellungen der manuellen Weiterleitung aus. Wenden Sie diese Einstellungen an, wenn die Slavemaschinen in dem Netz/lokaler UI nicht benutzt werden.

(5) Wählen Sie Additional Functions>System Settings>Device Information Delivery Settings>Manual Delivery Settings. Stellen Sie die Destinationsinformationen für die Zustellung auf ON, wählen Sie Add. function settings, Dept. ID, und vom Adressbuch, dann Next drücken.

Wenn das Adressbuch ausgewählt ist, werden auch die Weiterleitungseinstellungen und die von der Vorzugstaste zugestellt.

(6) Destinationen wählen und Manual Delivery Start drücken. Die Informationen der Vorrichtung werden den genau angegebenen Slavemaschinen zugestellt. Überprüfen Sie nach der erfolgten Weiterleitung die Ergebnisse der Zustellung.

### **Erstellung einer Sicherheitskopie von den MEAP Applikationen**

Wenn schon eine MEAP Applikation installiert worden ist, werden die in der MEAP Applikation gespeicherten Daten und die Lizenz gelöscht. Dies bildet wie auch immer kein Grund zur Besorgnis, wenn die MEAP Applikationen nicht installiert worden sind. Wenn eine MEAP

Applikation eine Sicherheitskopiefunktion besitzt, muss sichergestellt werden, dass die Erstellung einer Sicherheitskopie dieser genau angegebenen Daten der MEAP Applikation unter Benutzung dieser Funktion durchgeführt wird.

Hinsichtlich der Lizenzen müssen alle Applikationen vom SMS (Service Management Service) gestoppt werden, alle Lizenzen sind zu deaktivieren und ein Download der deaktivierten Lizenzdateien ist durchzuführen.

### **Hinweis: MEAP Funktion für die Erstellung einer Sicherheitskopie durch SST**

Mit Bezug auf die Daten, die durch MEAPback vom SST vor dem Start der Sicherheitsausrüstung eine Sicherheitskopie erstellt worden ist, müssen diese in der iR Vorrichtung nach dem Start der Sicherheitsausrüstung nicht erneut geschrieben werden. Wenn außerdem die Daten, von denen eine Sicherheitskopie nach dem Start der Sicherheitsausrüstung erstellt worden ist, erneut in einer iR Vorrichtung geschrieben werden, in der die Sicherheitsausrüstung noch nicht gestartet worden ist, wird diese nicht korrekt funktionieren. Es ist daher unerlässlich, dass die Betriebsbedingungen der Sicherheitsausrüstung vor und nach den Operationen für die Erstellung einer Sicherheitskopie übereinstimmen. Aus diesem Grund ist es unmöglich, durch die

MEAP Funktion für die Sicherheitskopie eine solche zu erstellen, während die Sicherheitsausrüstung installiert wird.

Benutzen Sie die folgenden Verfahren, um die MEAP Applikationen zu stoppen, Lizenzen zu deaktivieren und ein Download der Lizenzdateien durchzuführen. Für weitere Einzelheiten dazu ist die Anleitung des Administrator SMS MEAP einzusehen.

**Stop/Deaktivierung der MEAP Applikationen, Durchführung Download Lizenzdateien, Installationslöschung MEAP Applikationen.**

(1) Folgenden URL für einen SMS Zugriff wählen.

[http://\[IP Adresse des Geräts\]:8000/sms](http://[IP Adresse des Geräts]:8000/sms)

Falls der Benutzer seit dem voreingestellten Passwort ein SMS Passwort geändert hat, muss der Benutzer das Login durchführen oder das Passwort nach der Durchführung der Sicherheitsausrüstung verändern. Das voreingestellte Passwort ist [MeapSmsLogin].

**Hinweis:**

Das SMS Passwort wird nach der Durchführung der Sicherheitsausrüstung initialisiert.

Daher muss sichergestellt sein, dass der Benutzer gebeten worden ist, das Passwort zu ändern.

(2) Im Fenster mit den Applikationsverzeichnis ist die Taste für die zu stoppende Applikationsoption auszuwählen, danach ist auf Stop zu klicken.

(3) Den Applikationsnamen wählen, für den schon eine Lizenz installiert worden ist und auf die Informationsseite über die Applikation/Lizenz zugreifen.

(4) License Management klicken und dann Disable. OK auf dem Bestätigungsbildschirm der Deaktivierung für die Lizenzdatei klicken.

(5) Download im Fenster von Download/ Löschen der ungültigen Lizenzdatei klicken. Es muss eine Datei, in der der File gespeichert werden soll, nach den Angaben auf dem Bildschirm genau angegeben werden. Nun ist die Datei zu benennen, so dass die Applikation und die entsprechende Lizenzdatei leicht zu identifizieren sind.

Deletion (Löschen) klicken, nachdem das Download des Deaktivierungsfiles der Lizenz im PC durchgeführt worden ist. OK auf dem Bestätigungsbildschirm für die Löschung der Deaktivierungsdatei der Lizenz klicken.

(6) Zu dem Fenster mit dem Applikationsverzeichnis zurückkehren und die Taste für die Applikationsoption wählen, die zu löschen ist. Danach die Taste Uninstall drücken. OK auf dem Bildschirm für die Löschung der Installation drücken. Falls verschiedene Applikationen vorgesehen sind, müssen

die Punkte von (1) bis (6) wiederholt werden.

(7) Nach dem Start der Sicherheitsausrüstung müssen die gewünschten Applikationen wieder installiert werden. Dazu sind die Applikationsfiles (jar file) der betroffenen Applikationen zu benutzen, sowie die Deaktivierungsdatei der Lizenzen, von denen eine Sicherheitskopie erstellt worden ist (lic file).

### **In SDL (Simple Device Login) eingegebene Informationen für die Benutzerbefugnis**

Wenn der Benutzer die Loginapplikation von MEAP nach SDL ändert, muss von den Informationen der Benutzerbeglaubigung eine Sicherheitskopie erstellt werden. Dazu ist das folgende Verfahren zu befolgen.

(1) Zugriff auf folgendes URL.

[http:// \[IP Adresse des Geräts\]:8000/sdl/](http://[IP Adresse des Geräts]:8000/sdl/)

(2) Durchführung des Login durch die Eingabe des in SDL als Administrator registrierten Benutzernamens und Passwort.

Voreingestellte Eingaben wie folgt:

NBenutzername: Administrator

Passwort: password

(3) User Management klicken

(4) Alle möglichen Wahlen kennzeichnen und Export klicken.

(5) Start klicken, wobei das Dateiformat und der Code des voreingestellten Textes unverändert zu belassen sind.

(6) Eine Datei angeben, in der der File zu speichern ist, dann Save klicken.

### **Hinweis: Daten für die eine Erstellung von einer Sicherheitskopie unmöglich ist**

In Boxen gespeicherte Daten, noch nicht weitergeleitete Dokumente, übereinander gelagerte Bilddaten werden gelöscht, da die Erstellung einer Sicherheitskopie nicht möglich ist. Fragen Sie den Benutzer, wie solche Daten verwaltet werden sollen und handeln Sie demzufolge, z.B. indem die nötigen Daten ausgedruckt werden.

Nehmen Sie Bezug auf den Abschnitt "Bei der Installation zu beachtende Punkte" für weitere Einzelheiten über Daten, für die keine Sicherheitskopie erstellt werden kann.

## 1.3.2 Erhalt und

### Registrierung des

### Lizenzcodes 0008-3227

Nach der Erstellung einer Sicherheitskopie für die Daten ist die folgende Phase durchzuführen: der Erhalt eines Lizenzcodes durch LMS und seine Registrierung. Im Allgemeinen wird angenommen, dass die Benutzer bei ihrer Tätigkeit automatisch ihre Lizenzcodes erhalten, indem die Leitlinien der Broschüre für die Lizenzeintragung befolgt werden, welche alle notwendigen Prozeduren detailliert angeben. Nachstehend ein Überblick über diese Verfahren.

#### **Merkzettel: Was ist LMS?**

LMS (License Management System) ist ein neues Serversystem für Lizenzen, das von Canon INC. als ein Beglaubigungssystem der Softwareoptionen iR angeboten wird. Ziele des Systems sind: die Optionen zentral unter Lizenzform zu verwalten und zu verhindern, dass die Optionen kopiert werden. In diesem neuen System werden Lizenzcodes benutzt, um die Optionen zu bestätigen, anstatt herkömmliche Methoden wie natürliche Schutzvorrichtungen oder PC. Im Wesentlichen wird angenommen, dass die Benutzer diese Operation ausführen, dennoch könnte die Lage je nach Region oder Land variieren. Bei dem Kauf einer

Option wird dieser auch eine Bescheinigung des Codes für den Lizenzzugriff beigelegt. Der Zugriffscode wird benutzt, um einen Lizenzcode zu erhalten, der für diesen Code spezifisch ist. Mit diesem Code haben die Benutzer einen Zugriff auf den WEB Server, auf das LMS selbst und sie können den Lizenzcode erhalten. Mit dem Lizenzcode wird die Registrierung an der iR Vorrichtung durchgeführt und zum Schluss wird die Funktion der Option bestätigt.

Wenn die Benutzer sowohl den auf der Codebescheinigung für den Lizenzzugriff angegebenen Code eingeben, als auch die serielle Nummer der iR Vorrichtung in LMS, wird ein Lizenzcode erzeugt, der aus 24 Ziffern besteht und für jede Option spezifisch ist. Der Schlüssel enthält Informationen bezüglich der seriellen Nummer der entsprechenden Vorrichtung, folglich können die Benutzer den Schlüssel in anderen Vorrichtungen nicht benutzen. Außerdem werden in dem Moment, in dem die Optionsinformationen beglaubigt werden, diese selbst bei einem eventuellen Ersatz einiger Teile für die Reparatur nicht für ungültig erklärt, da die Informationen in einer Sicherheitskopie und in der Vorrichtung gespeichert sind.

### **Prozedur für den Erhalt und die Registrierung des Lizenzcodes**

(1) Zugriff auf LMS durch ein Klicken auf das untere URL und Erhalt eines Lizenzcodes durch die schrittweise Befolgung der auf dem Bildschirm angezeigten Anleitungen.

URL vom LMS

<http://www.canon.com/lms/ir/>

#### **Merkzettel:**

Wenn der Benutzer einen Lizenzcode erhält, werden sowohl der 24-stellige Code auf der Codebescheinigung des Lizenzzugriffs, als auch die serielle Nummer (Beispiel ABC1234) der zu installierenden Vorrichtung gefordert. Die serielle Nummer der Vorrichtung wird in dem Feld "Serial No." angezeigt wenn die Counter Taste des iR gedrückt wird.

(2) Notieren Sie den 24-stelligen, im Web angezeigten Code in dem dazu vorgesehenen Feld der Codebescheinigung für den Lizenzzugriff.

#### **Merkzettel**

Achten Sie darauf, diesen korrekt zu übertragen. Geben Sie den Benutzern eine angemessene Erklärung, damit sie den Code für den Lizenzzugriff sicher aufbewahren.

(3) Drücken Sie Additional function>System settings>License Registration, geben Sie dann den Lizenzcode in den dazu vorgesehenen Raum ein und drücken Sie die Starttaste, so dass der Lizenzcode registriert und die Funktion der Option beglaubigt wird. Falls Probleme bei der Beglaubigung der Funktion auftauchen sollten, wird eine Fehlermeldung angezeigt. Danach werden einige Angaben über die angeforderten Optionen wiedergegeben.

"Fortsetzung der Installation unmöglich. Vorhandene Eigenschaften unzureichend."  
→ Kontrollieren Sie, ob die Schnittstellenkarte USB Application Interface Board-D1 korrekt anerkannt worden ist und überprüfen Sie, dass die Speicherkapazität RAM 512MB entspricht.

"Falscher Wert des Lizenzcodes. Lizenzcode überprüfen."  
→Kontrollieren, ob irrtümlich der Lizenzcode für eine andere Vorrichtung benutzt worden ist.  
→Kontrollieren Sie, dass der Lizenzcode korrekt eingegeben worden ist.  
→Kontrollieren Sie, dass der Lizenzcode korrekt ist.

"Funktion schon befähigt."  
→Kontrollieren Sie, ob die Sicherheitsfunktion schon befähigt worden ist.

(4) Halten Sie den Schalter zum Einschalten der Kontrolltafel länger als 3 Sekunden gedrückt. Befolgen Sie Schritt für Schritt die Anweisungen, die in der Schließfolge angezeigt werden, wobei die passenden Punkte der Kontrolltafel gewählt werden, so dass das Ausschalten des Schalters vorbereitet werden kann. Hauptschalter ausschalten und nach 10 Sekunden wieder einschalten.

(5) Die registrierte Lizenz wird beim neuen Einschalten der Vorrichtung beglaubigt. Der erste Start nach der Registrierung des Lizenzcodes könnte in einigen Fällen 30 Minuten und mehr für die Initialisierung der Daten im HDD dauern. Falls die Methode der Datenlöschung des HDD der Vorrichtung auf "3-maliges Überschreiben der Randomdaten" eingestellt ist, könnte die erforderliche Zeit länger sein, als in den zuvor beschriebenen Fällen. Versichern Sie sich, die Vorrichtung nicht auszuschalten, wenn die Meldung erscheint: "Entfernung der verbleibenden Daten nicht erforderlich. Vorrichtung nicht ausschalten".

(6) Bei dem normalen Start der Vorrichtung ist die Counter Taste zu drücken und folglich die Konfiguration der Vorrichtung anzuzeigen, um zu kontrollieren, dass die Sicherheitsausrüstung in dem Optionsraum angezeigt wird. Danach ist die Servicemodalität auf Anfrage des Benutzers einzustellen.

### 1.3.3 Einstellung der Servicemodalität 0008-2981

Bei der Einstellung dieser Ausrüstung muss die Servicemodalität als Antwort auf die Anfrage des Benutzers geändert werden.

#### **1. Die Einstellung "Komplette Löschung des HDD" gestattet die Änderung der kompletten Löscheinrichtung des HDD auf Anfrage des Benutzers.**

- Servicemodalität Stufe 2

COPIER>OPTION>USER>HDCR-DSP

Wert eingeben:

1: NULL Daten einmal überschreiben

2: Random Daten einmal überschreiben

3: Random Daten dreimal überschreiben

Voreingestellter Wert: 1

#### **Hinweis:**

Da der eingegebene Wert höher ist, wird auch das Sicherheitsniveau größer, während sich das Leistungsniveau verringert.

#### **2. Benutzung des Schalters "Job history display ON/OFF"**

Benutzen Sie den Schalter "Job history display ON/OFF".

- Servicemodalität Stufe 2

COPIER>OPTION>USER>LGSW-DSP

Wert eingeben

0: Schlüssel nicht anzeigen

1: Schlüssel anzeigen

Voreingestellter Wert: 0

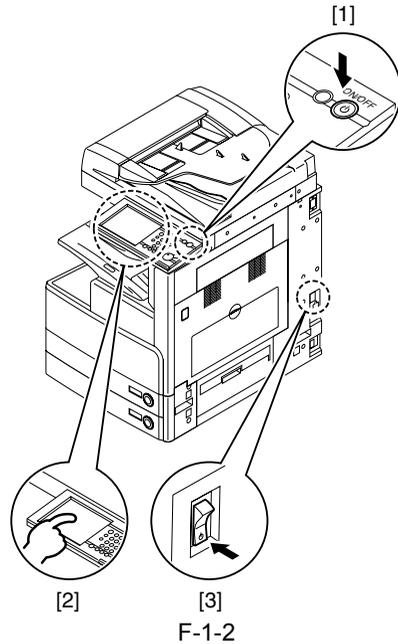
**Hinweis:**

Wenn dieser Schlüssel auf "1" gestellt ist, wird die Vorrichtung auf die Anfragen der aktiven Chronologie seitens der rechnerfernen Applikationen immer mit "0" antworten. Folglich ist eine Benutzung des Softwares als ein NetSpot Accountant, der die Vorrichtung unter Benutzung der aktiven Chronologie verwaltet, nicht möglich.

**3. OFF/ON der Verbindungsvorrichtungen**

Wenn die Einstellung der Servicemodalität verändert wird, müssen die Verbindungsvorrichtungen ein-/ausgeschaltet werden.

- 1) Den Schalter zum Einschalten der Kontrolleinheit länger als 3 Sekunden gedrückt halten.
- 2) Befolgen Sie die in der Schließfolge angezeigten Anweisungen Schritt für Schritt, wobei der passende Punkt der Kontrolltafel gewählt wird, so dass das Ausschalten des Schalters vorbereitet wird.
- 3) Vorrichtung durch den Hauptschalter ausschalten.



- 4) Vorrichtung durch den Hauptschalter einschalten.

**Merkzettel:**

Verbleiben die zu löschenden Destinationsdaten im Augenblick des Ausschaltens durch den Hauptschalter komplett im HDD enthalten, wird der Vorgang des Löschens bei der Neustartphase beendet.

# Procedura di installazione di iR Security Kit-A2

Per installare il kit di sicurezza nella macchina host, procedere come descritto di seguito.

## 1.1 Concetti importanti sull'installazione

---

### 1.1.1 Concetti importanti sull'installazione

0007-7622

---

#### **Attenzione!**

1. Per installare il kit di sicurezza, sono necessari i seguenti requisiti: Kit di espansione PCI Bus B1, scheda interfaccia USB D1, ed espansione memoria iR 256MB-B1 (a eccezione del modello 120V).

Prima di procedere, assicurarsi di disporre di questi componenti. In caso negativo, sarà impossibile finalizzare la registrazione del codice di licenza e verrà visualizzato il messaggio: "Non sono disponibili i requisiti sufficienti per procedere con l'installazione".

2. I dati utente presenti sull'hard disk vengono cancellati nei seguenti casi.

- Quando viene registrato un codice di licenza del kit di sicurezza, per abilitare le funzioni di sicurezza.
- Quando viene rigenerato un codice di codifica dei dati.
- Quando viene invalidato un codice di licenza del kit di sicurezza, per arrestare l'operazione di sicurezza.

Informare l'amministratore del dispositivo dell'utente che, nel caso in cui venga effettuata una delle seguenti operazioni, i dati mostrati di seguito verranno tutti cancellati, e invitare l'utente ad eseguire un backup dei dati necessari. In termini di sicurezza, non dovrebbe essere consentito ad alcun personale di servizio di effettuare il backup dei dati utente. Per ulteriori informazioni in merito, fare riferimento alla procedura di backup descritta nel presente manuale.

Dati che saranno rimossi:

- Dati memorizzati nelle caselle di posta.
- Informazioni sugli indirizzi registrati nella Rubrica.
- Impostazioni di scansione registrate utilizzando la funzione di trasmissione.
- Memoria modalità registrata, utilizzando la funzione di copia funzione/casella.
- Applicazioni MEAP e file di licenza.

- Dati memorizzati utilizzando un'applicazione MEAP.
  - Password del Service Management Service (SMS) di MEAP.
- Se l'utente ha modificato la password, questa viene ripristinata alle impostazioni di fabbrica.
- Informazioni di autenticazione utente registrate in SDL (Simple Device Login).
  - Documenti da trasmettere (per esempio, documenti di trasmissione timer/dedicati alla trasmissione).
  - Informazioni di cronologia attività.
  - Impostazioni effettuate in modalità utente.
  - Impostazioni di inoltro registrate.

È necessario che l'utente esegua il backup dei seguenti dati:

- Rubrica, impostazioni di funzioni aggiuntive, impostazioni di inoltro- Lizenzdatei der MEAP Applikationen (fare riferimento alla [Guida IU remota] per ulteriori informazioni sull'esportazione dei dati).
- File di licenza delle applicazioni MEAP (fare riferimento alla [Guida dell'amministratore SMS MEAP] per ulteriori informazioni sul download dei file di licenza).
- Informazioni di autenticazione utente registrate in SDL (fare riferimento alla [Guida dell'amministratore SMS MEAP] per ulteriori informazioni sull'esportazione delle informazioni di autenticazione).
- Dati registrati, che possono essere trasmessi utilizzando la funzione di consegna informazioni del dispositivo (è possibile effettuare un backup solo quando esiste un'altra macchina iR che dispone della funzione di consegna informazioni del dispositivo. Al contrario, il backup non è necessario se l'utente si serve dei dati registrati nella macchina iR. Fare riferimento alla [Guida di riferimento] per ulteriori informazioni sulla funzione di consegna informazioni).
- Dati memorizzati nelle applicazioni MEAP (è possibile eseguire un backup dei dati memorizzati a seconda dell'applicazione MEAP impiegata. Per ulteriori dettagli in merito, vedere il Manuale d'istruzioni di ciascuna applicazione).
- Le password per casella utente, casella fax e casella di sistema vengono cancellate una sola volta, quando viene registrato il codice di licenza. Di conseguenza, assicurarsi di registrare nuovamente tali password.
- Prima di registrare un codice di licenza, è necessario selezionare nuovamente il servizio di login dopo un riavvio, se l'utente ha scelto di effettuare l'autenticazione utente in SDL (Simple Device Login) o SSO (Single Sign-On).
- Questa operazione potrebbe richiedere un riavvio di oltre 30 minuti, dopo la registrazione di un codice di licenza.

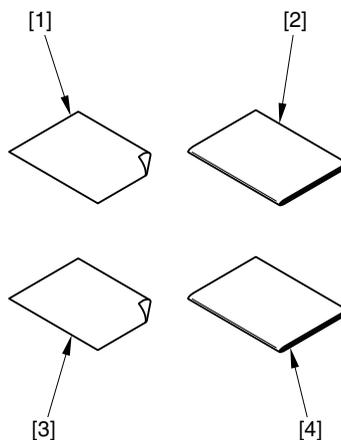
Tuttavia, potrebbe richiedere molto più tempo, se l'utente ha modificato le impostazioni di modalità del servizio, a causa della cancellazione dei dati presenti sull'hard disk, tramite "sovrascrittura dei dati random per tre volte".

## 1.2 Verifica del contenuto della confezione

---

### 1.2.1 Verifica del contenuto della confezione

0008-2781



F-1-1

- |   |       |
|---|-------|
| [1] Certificato del numero di accesso licenza.                  | 1 pz. |
| [2] Guida di riferimento.                                       | 1 pz. |
| [3] Documenti con le indicazioni di precauzione per gli utenti. | 1 pz. |
| [4] Libretto di registrazione licenza.                          | 1 pz. |
| [5] Procedura d'installazione.                                  | 1 pz. |

## 1.3 Procedura d'installazione

---

### 1.3.1 Eseguire il backup dei dati 0008-3214

**Promemoria: Concetti importanti da osservare, nell'installazione contemporanea del kit di sicurezza e della macchina iR corrispondente.**

Nel caso dell'installazione contemporanea del kit di sicurezza e della macchina iR corrispondente, installare innanzitutto il kit di sicurezza. In questo caso, non è necessario eseguire alcun backup. Al contrario, se il kit di sicurezza viene installato in una macchina già configurata, è necessario eseguire il backup.

Di seguito, viene descritta una panoramica delle procedure di backup dei dati.

**Backup tramite la funzione di importazione/esportazione dell'IU remota**

**Procedura per l'esecuzione del backup delle informazioni contenute nella Rubrica**

(1) Accedere al seguente URL, quindi accedere all'IU remota.

[http:// \[indirizzo IP del dispositivo\] /](http:// [indirizzo IP del dispositivo] /)

(2) Fare clic su Add. Func. (Aggiungi funzione) e selezionare Import/Export (Importa/Esporta) dal menu che comparirà. A questo punto, se sono stati configurati un ID dell'amministratore di sistema e una password, viene visualizzata una finestra di dialogo. Digitare l'ID dell'amministratore di sistema nel campo User Name (Nome Utente) e una password nel campo Password. Fare clic su OK.

(3) Selezionare la Rubrica.

(4) Scegliere una Rubrica e un formato di file, quindi fare clic su Start Export (Avvia Esportazione).

(5) Specificare una cartella in cui memorizzare i file, seguendo le indicazioni riportate nelle schermate che compariranno. Assegnare un nome ai file, in modo da identificare facilmente i file e le pagine corrispondenti della Rubrica.

**Promemoria:**

Tutte le informazioni presenti nella Rubrica vengono incluse nel momento in cui vengono esportate le impostazioni di inoltro.

Il backup della Rubrica non è necessario se non si desidera effettuare il backup singolo di ciascuna pagina.

**Procedura per l'esportazione delle impostazioni di inoltro**

(1) Accedere al seguente URL, quindi accedere all'IU remota.

[http:// \[indirizzo IP del dispositivo\] /](http:// [indirizzo IP del dispositivo] /)

- (2) Fare clic su Add. Func. (Aggiungi funzione) e selezionare Import/Export (Importa/Esporta) dal menu che comparirà. A questo punto, se sono stati configurati un ID dell'amministratore di sistema e una password, viene visualizzata una finestra di dialogo. Digitare l'ID dell'amministratore di sistema nel campo User Name (Nome Utente) e una password nel campo Password. Fare clic su OK.
- (3) Fare clic su Forwarding Settings (Impostazioni di Inoltro).
- (4) Fare clic su Export (Esporta) e quindi su Start Export (Avvia Esportazione).
- (5) Specificare una cartella in cui memorizzare i file, secondo le schermate che compariranno.

### **Procedura per l'esportazione delle funzioni aggiuntive**

- (1) Accedere al seguente URL, quindi accedere all'IU remota.  
[http:// \[indirizzo IP del dispositivo\] /](http:// [indirizzo IP del dispositivo] /)
- (2) Fare clic su Add. Func. (Aggiungi funzione) e selezionare Import/Export (Importa/Esporta) dal menu che comparirà. A questo punto, se sono stati configurati un ID dell'amministratore di sistema e una password, viene visualizzata una finestra di dialogo. Digitare l'ID dell'amministratore di sistema nel campo User Name (Nome Utente) e una password nel campo Password. Fare clic su OK.
- (3) Fare clic su Additional Functions (Funzioni Aggiuntive).
- (4) Fare clic su Export (Esporta) e quindi

- su Start Export (Avvia Esportazione).
- (5) Specificare una cartella in cui memorizzare i file, secondo le schermate che compariranno.

### **Backup tramite la funzione di consegna informazioni**

Se sono installate più di due macchine iR uguali connesse in rete e se queste possiedono la funzione di consegna informazioni, è possibile registrare una macchina come master e consegnare le stesse informazioni alle altre macchine, per sincronizzare le impostazioni. Fare riferimento al capitolo [Consegna delle informazioni del dispositivo] nella Guida di riferimento.

- (1) Impostare la macchina master (per esempio, impostazioni di trasmissione). Registrare le destinazioni delle informazioni del dispositivo nella macchina master. Selezionare Additional Functions (Funzioni Aggiuntive) > System Settings (Impostazioni di Sistema) > Device Information Delivery Settings (Impostazioni di Consegna Informazioni del Dispositivo) > Register Destinations (Registra Destinazioni).
- (2) Registrare le destinazioni manualmente/automaticamente. Nel caso di una ricerca automatica, selezionare le destinazioni dai risultati della ricerca e premere OK.
- (3) Verificare lo stato delle impostazioni delle destinazioni, per riscontrare se la

macchina master è in grado di inviare le informazioni del dispositivo alle macchine slave.

(4) Effettuare le impostazioni di consegna manuali. Applicare tali impostazioni quando le macchine slave non sono un uso nella rete/IU locale.

(5) Selezionare Additional Functions (Funzioni Aggiuntive) > System Settings (Impostazioni di Sistema) > Device Information Delivery Settings (Impostazioni di Consegna Informazioni del Dispositivo) > Manual Delivery Settings (Impostazioni di Consegna Manuali). Impostare le informazioni di destinazione per la consegna a ON, selezionando Add. Function Settings (Aggiungi Impostazioni di Funzione), Dept. ID (ID Dept.) e dalla Rubrica, quindi premere Next (Avanti).

Se è selezionata la Rubrica, verranno consegnate anche le impostazioni di inoltro e del pulsante Preferiti.

(6) Selezionare le destinazioni e premere Manual Delivery Start (Avvia Consegna Manuale). Le informazioni del dispositivo verranno consegnate alle macchine slave specificate. Verificare i risultati di consegna dopo l'avvenuta consegna.

### **Backup di applicazioni MEAP**

Se è già stata installata un'applicazione MEAP, i dati e la licenza memorizzati nell'applicazione MEAP vengono cancellati. Tuttavia, questo non costituisce alcuna preoccupazione se le applicazioni MEAP non sono state installate.

Se un'applicazione MEAP possiede una funzione di backup, assicurarsi di effettuare il backup dei dati specifici di tale applicazione MEAP utilizzando questa funzione. Per quanto riguarda le licenze, è necessario arrestare tutte le applicazioni da SMS (Service Management Service), disattivare tutte le licenze ed effettuare il download dei file di licenza disattivati.

### **Nota: Funzione MEAP di backup tramite SST**

Per quanto riguarda i dati di cui è stato effettuato il backup tramite MEAPback di SST prima di avviare il kit di sicurezza, questi non devono essere riscritti nella macchina iR dopo l'avvio del kit di sicurezza. Inoltre, se i dati di cui è stato eseguito il backup dopo l'avvio del kit di sicurezza vengono riscritti in una macchina iR dove il kit di sicurezza non è ancora stato avviato, questa non funzionerà in modo corretto. È assolutamente necessario che le condizioni operative del kit di sicurezza corrispondano, prima e dopo le operazioni di backup. Per tale motivo, è impossibile effettuare il backup tramite la funzione MEAP di backup, mentre si installa il kit di sicurezza. Utilizzare le seguenti procedure per arrestare applicazioni MEAP, disattivare licenze ed effettuare il download dei file di licenza. Fare riferimento alla Guida dell'Amministratore SMS MEAP per ulteriori dettagli in merito.

**Arrestare/Disattivare applicazioni MEAP, effettuare il download dei file di licenza, disinstallare applicazioni MEAP.**

(1) Selezionare il seguente URL, per accedere all'SMS.

http://[indirizzo IP del dispositivo]:8000/sms

Se l'utente ha modificato una password SMS a partire da quella predefinita, chiedere all'utente di effettuare il login o di modificare la password dopo l'esecuzione del kit di sicurezza. La password predefinita è [MeapSmsLogin].

**Nota:**

La password SMS verrà inizializzata dopo l'esecuzione del kit di sicurezza.

Di conseguenza, assicurarsi di chiedere all'utente di cambiare la password.

(2) All'interno della finestra contenente l'elenco di applicazioni, selezionare il pulsante di opzione dell'applicazione che si desidera arrestare, quindi fare clic su Stop.

(3) Fare clic sul nome dell'applicazione per cui è già stata installata una licenza e accedere alla pagina di informazioni sull'applicazione/licenza.

(4) Fare clic su License Management (Gestione Licenze) e quindi su Disable (Disattiva). Fare clic su OK nella schermata di conferma della disattivazione del file di licenza.

(5) Fare clic su Download nella finestra di download/cancellazione file di licenza non

valido. Specificare una cartella in cui memorizzare il file, secondo le indicazioni delle schermate che compariranno. A questo punto, assegnare un nome al file, in modo da identificare facilmente l'applicazione e il file di licenza corrispondente.

Fare clic su Deletion (Cancella), dopo aver effettuato il download del file di disattivazione della licenza nel PC. Fare clic su OK, nella schermata di conferma della cancellazione del file di disattivazione della licenza.

(6) Tornare alla finestra contenente l'elenco di applicazioni e selezionare il pulsante di opzione dell'applicazione che si desidera disinstallare. Quindi, fare clic su Uninstall (Disinstalla). Fare clic su OK, nella schermata di conferma della disinstallazione. Se sono presenti diverse applicazioni, ripetere i passaggi da (1) a (6).

(7) Dopo l'avvio del kit di sicurezza, reinstallare le applicazioni desiderate, utilizzando i file di applicazione (jar file) delle applicazioni in questione, nonché i file di disattivazione licenze di cui è stato effettuato il backup (file con estensione .lic).

**Informazioni di autenticazione utente registrate in SDL (Simple Device Login)**

Quando l'utente cambia l'applicazione di login da MEAP a SDL, è necessario effettuare il backup delle informazioni di autenticazione utente, attenendosi alla seguente procedura.

- (1) Accedere al seguente URL.  
http:// [indirizzo IP del dispositivo]:8000/  
sdl/
- (2) Effettuare il login inserendo nome utente e password registrati in SDL, in qualità di amministratore.  
Le impostazioni predefinite sono le seguenti:  
Nome utente: Administrator  
Password: password
- (3) Fare clic su User Management (Gestione Utenti).
- (4) Contrassegnare tutte le scelte possibili e fare clic su Export (Esporta).
- (5) Fare clic su Start (Avvia), lasciando invariati il formato di file e il codice di testo predefiniti.
- (6) Specificare una cartella in cui memorizzare il file, quindi fare clic su Save (Salva).

**Nota: Dati per cui è impossibile eseguire il backup**

I dati memorizzati in caselle, documenti non ancora trasmessi, dati immagine sovrapposti, vengono cancellati, dal momento che non è possibile eseguirne il backup. Chiedere all'utente come gestire i dati di cui è impossibile eseguire il backup e agire di conseguenza, per esempio, stampando i dati necessari.  
Fare riferimento alla sezione Concetti importanti sull'installazione, per ulteriori dettagli sui dati di cui è impossibile eseguire il backup.

### 1.3.2 Ottenere e registrare la chiave di licenza 0008-3227

Al termine del backup dei dati, procedere alla fase successiva: ottenere una chiave di licenza tramite LMS e registrarla. In genere, si suppone che gli utenti operino ottenendo autonomamente le proprie chiavi di licenza, seguendo le linee guida indicate nel Libretto di registrazione licenza, che illustra in dettaglio tutte le procedure necessarie. Di seguito, viene descritta una panoramica delle procedure, come riferimento.

**Promemoria: Che cos'è LMS?**

LMS (License Management System, sistema di gestione licenze) è un nuovo sistema server di licenze, offerto da Canon Inc. per l'impiego come mezzo di convalida delle opzioni software iR. Gli scopi del sistema sono: gestire centralmente le opzioni sotto forma di licenza ed evitare che le opzioni vengano copiate. In questo nuovo sistema, vengono usate le chiavi di licenza per convalidare le opzioni, anziché i metodi convenzionali, come protezioni fisiche o PC.  
Fondamentalmente, si suppone che siano gli utenti ad eseguire questa operazione, tuttavia, la situazione potrebbe variare a seconda delle regioni o dei paesi. Quando si acquista un'opzione, con l'opzione viene allegato anche un certificato del codice di accesso licenza. Il codice di accesso viene

utilizzato per ottenere una chiave di licenza, specifica per tale codice. Con tale codice, gli utenti possono accedere al server Web, a LMS stesso, e ottenere la chiave di licenza. Con la chiave di licenza, si effettua la registrazione al dispositivo iR, e infine viene convalidata la funzione dell'opzione.

Quando gli utenti inseriscono sia il codice riportato sul certificato del codice di accesso licenza che il numero seriale del dispositivo iR stesso in LMS, viene generata una chiave di licenza composta da 24 cifre, specifica per ciascuna opzione. La chiave include le informazioni relative al numero seriale del dispositivo corrispondente, di conseguenza, gli utenti non possono usare la chiave in altri dispositivi. Inoltre, nel momento in cui vengono convalidate le informazioni di opzione, queste non verranno invalidate anche se ne fossero sostituite alcune parti per la riparazione, dal momento che le informazioni sono salvate in un backup e memorizzate nel dispositivo.

### **Procedure per ottenere e registrare la chiave di licenza**

(1) Accedere a LMS facendo clic sull'URL sottostante e ottenere una chiave di licenza seguendo le istruzioni visualizzate nelle schermate passo per passo.

URL di LMS:

<http://www.canon.com/lms/ir/>

### **Promemoria:**

Quando l'utente ottiene una chiave di licenza, vengono richiesti sia il codice a 24 cifre riportato sul certificato del codice di accesso licenza che il numero seriale (per esempio, ABC01234) del dispositivo da installare. Il numero seriale del dispositivo viene visualizzato nel campo "Serial No." (N° Seriale), quando viene premuto il tasto Counter (Contatore) dell'iR.

(2) Annotarsi il codice a 24 cifre visualizzato nel Web, nello spazio apposito del certificato del codice di accesso licenza.

### **Promemoria:**

Assicurarsi di trascriverlo correttamente. Fornire una spiegazione adeguata agli utenti, in modo che conservino al sicuro il codice di accesso licenza.

(3) Premere Additional Functions (Funzioni Aggiuntive) > System Settings (Impostazioni di Sistema) > License Registration (Registrazione Licenza), quindi inserire la chiave di licenza nello spazio designato e premere il pulsante Start (Avvia), in modo da registrare la chiave di licenza e da convalidare la funzione dell'opzione.

Se si riscontrano problemi nella convalida della funzione, viene visualizzato un messaggio di errore. Di seguito, sono riportate alcune indicazioni sulle operazioni richieste.

"Impossibile procedere con l'installazione. Non sono presenti i requisiti sufficienti".

→ Verificare se la scheda interfaccia USB D1 sia stata riconosciuta correttamente e controllare che la capacità di memoria RAM corrisponda a 512 MB.

"Il valore della chiave di licenza è errato. Verificare la chiave di licenza".

→ Verificare di non aver erroneamente utilizzato la chiave di licenza emessa per un altro dispositivo.

→ Verificare di aver digitato correttamente la chiave di licenza.

→ Verificare che la chiave di licenza sia corretta.

"Funzione già attivata".

→ Verificare che la funzione di sicurezza non sia già stata attivata.

(4) Tenere premuto per più di 3 secondi l'interruttore di accensione del pannello di controllo. Seguire le istruzioni visualizzate nella sequenza di chiusura passo per passo, selezionando le voci adeguate del pannello di controllo, in modo da preparare lo spegnimento dell'interruttore. Spegnerlo l'interruttore generale e, dopo 10 secondi, riaccenderlo di nuovo.

(5) La licenza registrata viene convalidata alla nuova accensione del dispositivo.

Il primo riavvio dopo la registrazione della chiave di licenza potrebbe, in alcuni casi, richiedere 30 minuti e oltre per

l'inizializzazione dei dati nell'HDD. Se il metodo di cancellazione dati dell'HDD del dispositivo è impostato a "Sovrascrivere per 3 volte i dati random", potrebbe richiedere più tempo dei casi precedentemente descritti. Assicurarsi di non spegnere il dispositivo quando compare il messaggio: "Rimozione dei dati rimanenti non necessaria. Non spegnere il dispositivo".

(6) Quando il dispositivo viene avviato normalmente, premere il tasto Counter (Contatore) e quindi visualizzare la configurazione del dispositivo per controllare che il kit di sicurezza sia visualizzato nello spazio delle opzioni. Quindi, impostare la modalità Service su richiesta dell'utente.

### 1.3.3 Impostazione

#### della modalità

#### Service

0008-2981

Al momento dell'installazione di questo kit, è necessario modificare la modalità Service in risposta alla richiesta dell'utente.

#### **1. L'impostazione "Cancellazione completa dell'HDD"**

Consente di cambiare l'impostazione di cancellazione completa dell'HDD su richiesta dell'utente.

- Modalità Service livello 2

COPIER>OPTION>USER>HDCR-DSP

Impostare valore

1: Sovrascrivere i dati NULL una volta

2: Sovrascrivere i dati Random una volta

3: Sovrascrivere i dati Random tre volte

Valore predefinito: 1

#### **Nota:**

Poiché il valore impostato è maggiore, il livello di sicurezza diventa maggiore, mentre il livello di prestazioni si riduce.

#### **2. Impiego dell'interruttore "Visualizza cronologia attività ON/OFF".**

Utilizzare l'interruttore "Visualizza cronologia attività ON/OFF".

-Modalità Service livello 2

COPIER>OPTION>USER>LGSW-DSP

Impostare valore

0: Non visualizzare la chiave

1: Visualizzare la chiave

Valore predefinito: 0

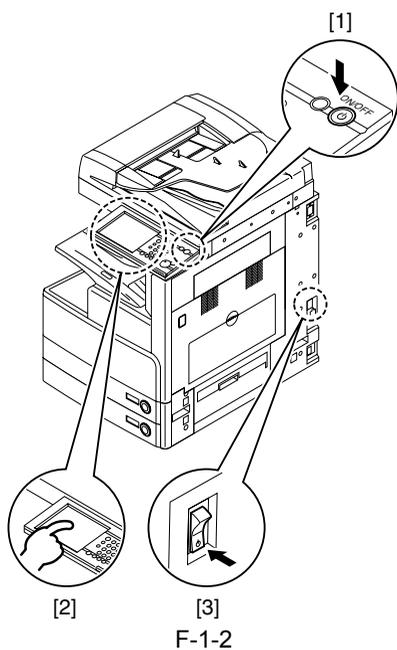
#### **Nota:**

Quando questa chiave è impostata a "1", il dispositivo risponderà sempre "0" alle richieste della cronologia attività da parte di applicazioni remote. Di conseguenza, non è possibile utilizzare software come NetSpot Accountant, che gestisce il dispositivo utilizzando la cronologia attività.

#### **3. SPEGNIMENTO/ACCENSIONE dei dispositivi di connessione**

Quando viene modificata l'impostazione della modalità Service, è necessario spegnere/accendere i dispositivi di connessione.

- 1) Tenere premuto per più di 3 secondi l'interruttore di accensione dell'unità di controllo.
- 2) Seguire le istruzioni visualizzate nella sequenza di chiusura passo per passo, selezionando le voci adeguate del pannello di controllo, in modo da preparare lo spegnimento dell'interruttore.
- 3) Spegnere il dispositivo tramite l'interruttore principale.



F-1-2

4) Accendere il dispositivo tramite l'interruttore principale.

**Promemoria:**

Se i dati di destinazione da cancellare completamente rimangono nell'HDD al momento dallo spegnimento tramite l'interruttore principale, l'operazione di cancellazione verrà portata a termine in fase di riavvio.