

Issued: March 18th, 2008



Technical Information:

Configuring Scan to SMB

(Case studies with user authentication)

Document Version 1.0

Global Technology Support Section

Service Support Department,

Marketing Center

MFP Business Group

Notice:

THIS DOCUMENT MAY NOT BE REPRODUCED OR DISTRIBUTED IN WHOLE OR IN PART, FOR ANY PURPOSE OR IN ANY FASHION WITHOUT THE PRIOR WRITTEN CONSENT OF RICOH COMPANY LIMITED. RICOH COMPANY LIMITED RETAINS THE SOLE DISCRETION TO GRANT OR DENY CONSENT TO ANY PERSON OR PARTY.

Copyright © 2008 by Ricoh Company Ltd.

All product names, domain names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

Although best efforts were made to prepare this document, Ricoh Company Limited makes no representation or warranties of any kind with regards to the completeness or accuracy of the contents and accepts no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this document.

Version history:

Version	Issue Date	Revised item
1.0	Mar. 18, 2008	1st release

Index

1. Introduction.....	3
2. Target readers	3
3. Target models	3
4. Important tips when configuring Scan to SMB.....	4
4-1 Access using the recipient's account.....	4
4-2 Other tips.....	5
5. Configuring Scan to SMB: Case studies with user authentication	6
5-1 Scanning to my folder	6
5-2 Adding personal destinations for one user	9
5-2-1 Adding from "Enter Destination / Manual Entry".....	9
5-2-2 Adding in the addressbook.....	11
5-3 Sharing a personal destination with other users.....	15
5-4 Creating a public destination	18
6. Using "Enter Destination (Manual Entry)" when Scanning	22
6-1 "Enter Destination" and the sender's SMB account.....	23
6-2 "Enter Destination" and the device default SMB account.....	24
7. Configuration notes	26
7-1 Access Privileges	26
7-2 Destination restriction settings	27

1. Introduction

This document will describe how to configure an MFP for Scan to SMB with user authentication (Basic/Windows/LDAP/Integration Server authentication).

This document contains some case studies of configuring the MFP for use with Scan to SMB and authentication (on the MFP side). Each case study starts with a scenario including the environment and MFP login privileges needed to complete the task. This is followed by the step-by-step procedure for completing the task.

The primary aim of this document is to provide sample procedures to our SEs. Each procedure can be modified to match specific environments used by customers. A procedure such as this which is designed specifically for a customer environment should make it easier for customers to configure existing entries or create new ones on their own. Note that in some cases the privileges of the operator (a user or the User Administrator) will affect the procedure for configuration. Differences in such cases will be explained.

Although this document focuses on Scan to SMB, it will not be difficult to modify the procedures for Scan to FTP or Scan to NCP.

Note for wording:

The term "addressbook entry" is used to refer to both users and destinations that have been entered in the addressbook. This distinction should become clear in the context of the document.

2. Target readers

This document is intended for the support staff of Ricoh family group companies and their subsidiaries. Readers should have basic knowledge of Scan to SMB and the authentication systems of MFP.

3. Target models

This document applies to 04A or later models.

Note: The descriptions and screen images will be based on 05A or later models. There are some differences between these and some earlier models:

1. The name of the button for manually entering the folder path and the access account:
04A, 05S: "Enter Destination"
05A or later: "Manual Entry"
2. The name of a related Extended Security setting and its default value:
04A: "Permit Adding of Destinations" is "Yes" by default
05S or later: "Restrict Adding of User Destinations" is "No" by default

4. Important tips when configuring Scan to SMB

There are some things to keep in mind before reading through these case studies.

4-1 Access using the recipient's account

When configuring destinations in the addressbook for Scan to SMB, there might be some misconceptions about the access account. GW MFPs have the following specification:

If a recipient is selected from the Scan to Folder destination list, the device will access the destination folder using the account that is configured for the recipient, regardless of whether user authentication is enabled/disabled.

When a user (userA) selects another user (userB) from the destination list, the sending user (userA) will access the recipient's (userB's) folder using user B's account. userA was used as an example in this case, but in fact, any user (including userB) who sends a scan to the userB destination folder will use userB's account to access userB's folder.

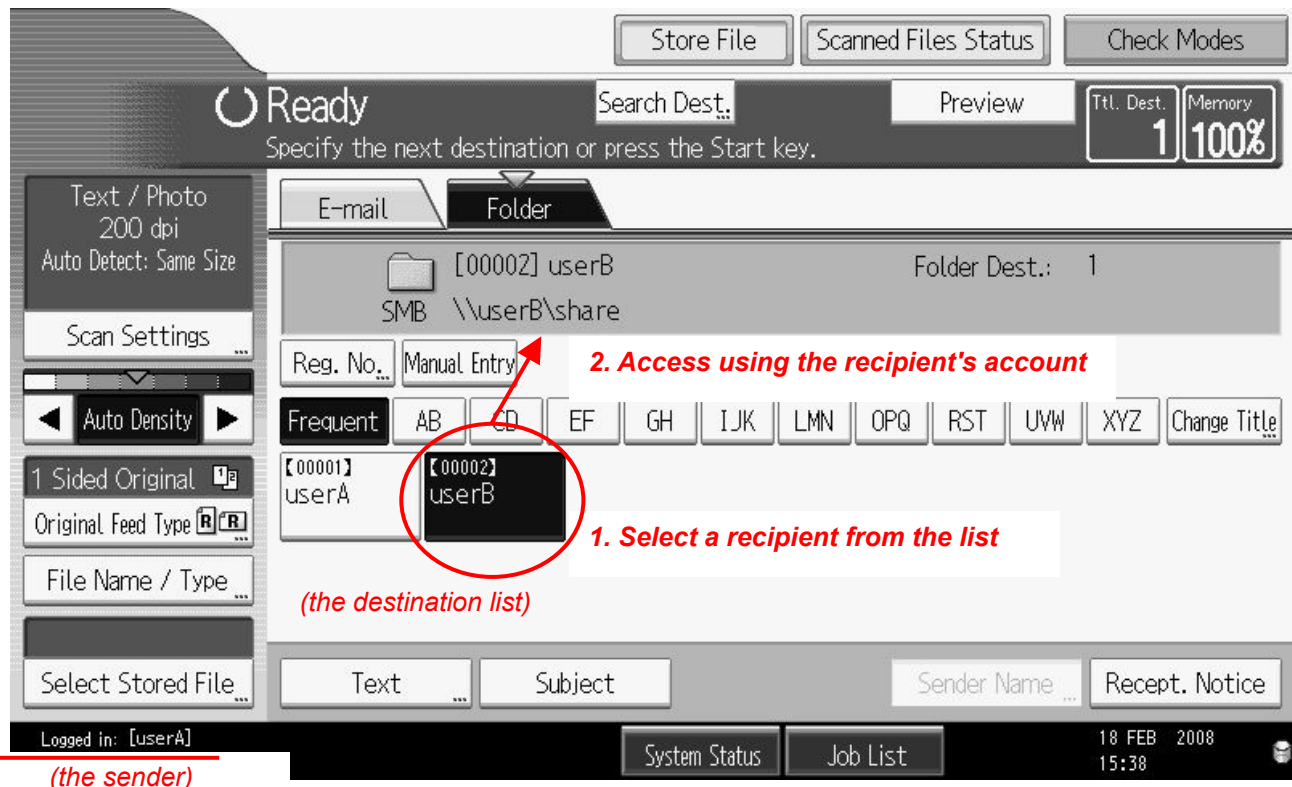


Figure 1

The account used to access a folder of a user is configured using the Folder Authentication setting in the addressbook (See **Figure 2**). This account will be used by whoever accesses this folder using Scan to SMB. A common misconception is that the account configured in Folder Authentication will be used by the user to access other user's destinations. This is not the case.

Authentication Information

■ Authentication Info at Login
Login User Name : usera
Login Password : Change

■ SMTP Authentication : Use Auth. Info at Login Specify Other Auth. Info below: Do not Specify
Login User Name :
Login Password : Change

■ Folder Authentication : Use Auth. Info at Login Specify Other Auth. Info below: Do not Specify
Login User Name : usera
Login Password : Change

The Folder Authentication account is used to access this user's folder.

Figure 2

In cases where multiple users share a destination folder, the result of this specification is that everyone uses the same account to access the folder. This might not meet the security policy of some users. For details, please see sections [5-3](#) and [5-4](#) for samples of the sharing.

If access accounts need to be individual (i.e. for access logging, or assigning file ownership to the sender), users need to manually enter the folder path and the access account (see Note in [Section 6](#)). It will be difficult to use the destination list for this purpose. It is not described in this document.

4-2 Other tips

Use of the account information also occurs when a user manually sends a scan using "Manual Entry" or "Enter Destination". This will be described in [Section 6](#).

Although this document does not explain all Scan to SMB settings, a couple of important points will be mentioned in [Section 7](#) as "Configuration Notes". These will include:

- Access privileges
- Restricting the ability of users to manually send a scan to a destination or creating an addressbook entry

5. Configuring Scan to SMB: Case studies with user authentication

5-1 Scanning to my folder

Case 1

A user who exists as an entry in the addressbook (userA) will be configured so that he can perform Scan to SMB by selecting himself in the destination list. The destination is an SMB folder in userA's PC, to which only userA has access. User authentication is enabled for the device and users will be required to login in order to scan. The userA destination will only appear in the destination list if userA is logged into the device.

Environment:

1. User authentication has already been configured for the device.
2. UserA already exists in the addressbook.
3. UserA has scanning privileges.

Can be configured by:

- the user himself (userA in this case)...Restriction settings (See [7-2](#)) must be disabled
- User Administrator

The point of this configuration:

UserA will be displayed in the destination list if (and only if) userA himself logs in to the MFP. Other users who log in to the device will not be able to see userA in the destination list. As long as User Authentication is enabled for the device, the Protection settings need not be configured because by default, no other users will have access to the destination.

Configuring the addressbook (in WIM/operation panel):

1. Login to the device as userA or the User Administrator.
2. Select userA in the addressbook and click Change.
3. Under Folder, select SMB as the Protocol setting and enter the path to the destination folder.



Folder	
■ Protocol	: SMB
■ Port No.	: 21
■ Connection Type	: NDS
■ Server Name	:
■ Path	: \userA\share

Figure 3

- Under Authentication Information > Folder Authentication, select either "Use Auth Info at Login" or "Specify Other Auth. Info". If "Specify Other Auth. Info" is selected, a user name and password will also have to be configured.

These are the settings as seen when logged in as userA:

The screenshot shows the 'Authentication Information' configuration page. It includes sections for 'Authentication Info at Login', 'SMTP Authentication', 'Folder Authentication', and 'LDAP Authentication'. Each section has a 'Login User Name' field and a 'Login Password' field with a 'Change' button. Radio buttons allow selecting 'Use Auth. Info at Login', 'Specify Other Auth. Info below', or 'Do not Specify'. The 'Folder Authentication' section is selected with 'Specify Other Auth. Info below' and has 'usera' in the 'Login User Name' field. The 'Available functions' section shows 'Scanner' selected.

Figure 4

These are the settings as seen when logged in as the User Administrator:

The screenshot shows the 'Authentication Information' configuration page. It includes sections for 'Authentication Info at Login', 'SMTP Authentication', 'Folder Authentication', and 'LDAP Authentication'. Each section has a 'Login User Name' field and a 'Login Password' field with a 'Change' button. Radio buttons allow selecting 'Use Auth. Info at Login', 'Specify Other Auth. Info below', or 'Do not Specify'. The 'Folder Authentication' section is selected with 'Specify Other Auth. Info below' and has 'usera' in the 'Login User Name' field. The 'Available functions' section shows 'Copier', 'Facsimile', 'Scanner', 'Document Server', and 'Printer' as checkboxes, with 'Scanner' checked.

Figure 5

- Under Protection, confirm that "Use Name as > Destination" is checked. No configuration is necessary for other Protection settings.

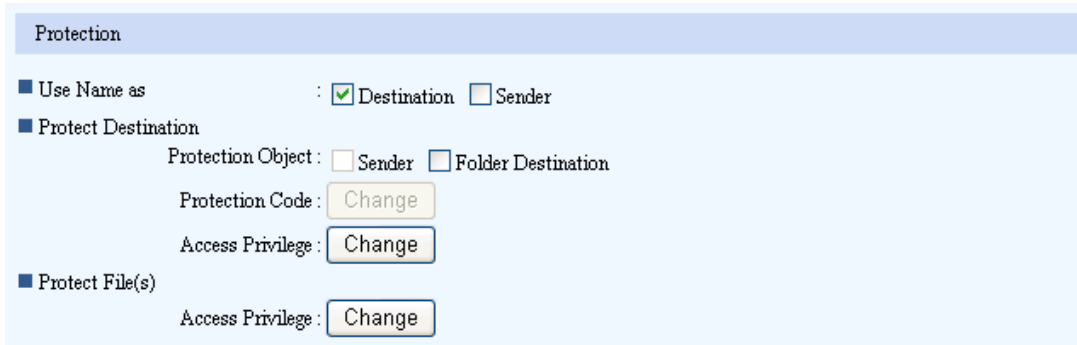


Figure 6

- Save the changes and exit.

Configuring the SMB folder:

Make sure that userA's Windows/SAMBA account has write privileges to the folder.

Scanning to SMB:

Login to the device as userA, select the destination and start scanning. When another user logs in, userA's destination will not be displayed in the destination list.

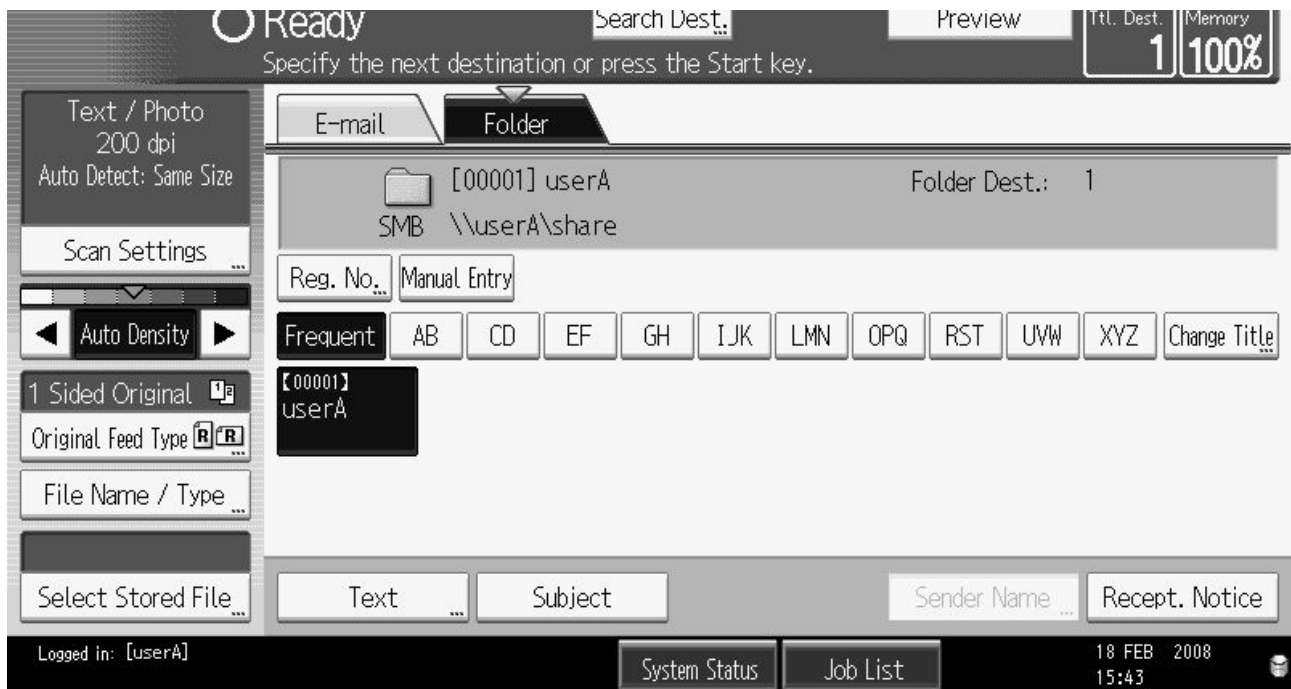


Figure 7

5-2 Adding personal destinations for one user

Case 2

If userA needs an additional destination other than the one configured in the userA addressbook entry, an additional destination-only entry can be created in the addressbook. A destination-only entry is not a user and has no login privileges. Its only purpose is as a destination. By default, the user who creates the destination-only entry will be the owner and therefore have the Full Control privilege over that entry in the addressbook.

Environment:

1. User authentication has already been configured for the device.
2. UserA already exists in the addressbook.
3. UserA has scanning privileges.

Can be configured by:

- the user himself (userA in this case)...Restriction settings (See [7-2](#)) must be disabled
- User Administrator

The point of this configuration:

There are two ways to create a destination-only addressbook entry for a user. An easy way is for the user himself to manually enter the destination path on the scanner interface and then add that path to the addressbook. The other way is to open the addressbook and simply create the destination-only entry.

Note: We have assumed that the destination folder on the file server is already accessible to userA.

5-2-1 Adding from "Enter Destination / Manual Entry"

Set up Scan to SMB and register the destination in the addressbook (operation panel only):

1. Login to the device as userA.
2. Press "Enter Destination" (05S or earlier) or "Manual Entry" (05A or later) and manually set up the folder path and login account.

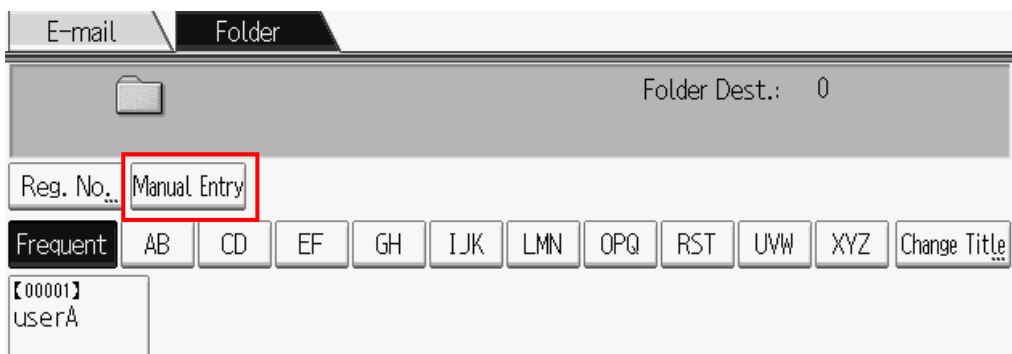


Figure 8

3. Press OK to go back to the scanner interface. (It will not be possible in some devices to manually register a destination after performing a Scan to SMB. Instead the destination must be registered before the scan is performed.)

4. Press "Prg. Dest".

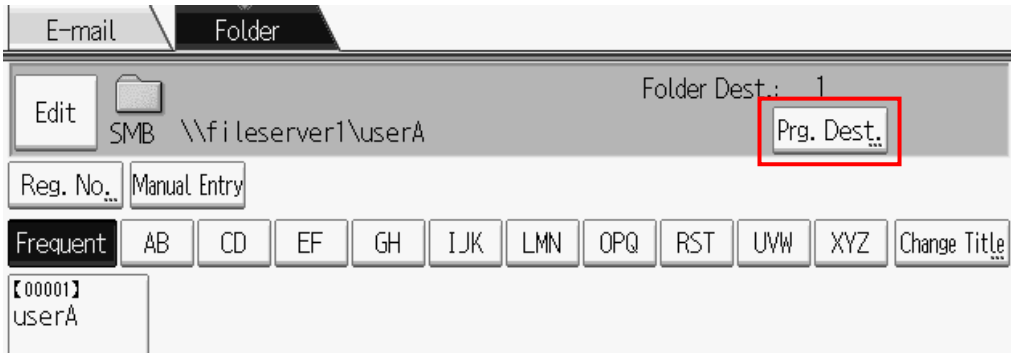


Figure 9

5. The "Folder" tab of the newly created addressbook entry will appear. Confirm that the path is correct, and then press the "Names" tab.

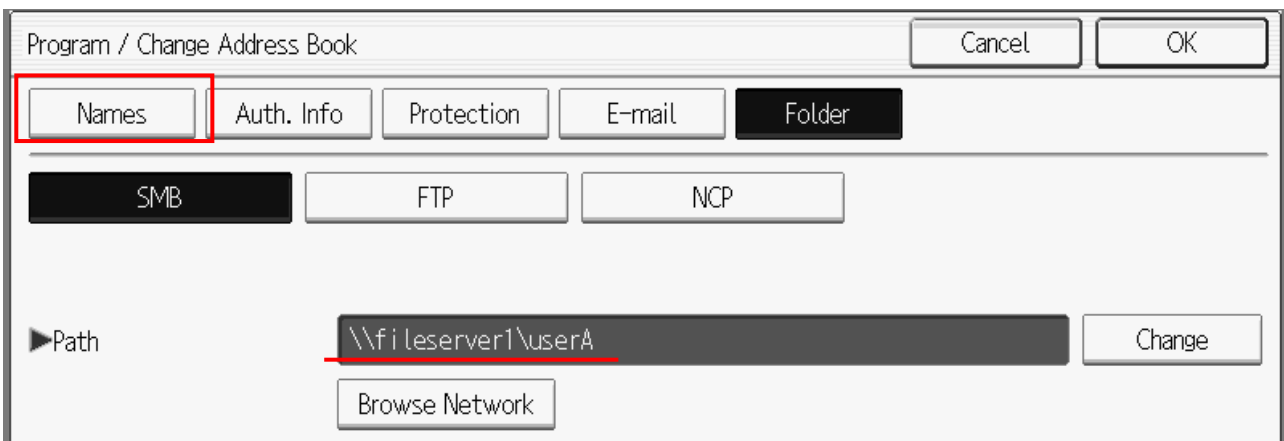


Figure 10

6. Under the "Names" tab, enter the name of the new entry, and press OK to register it.

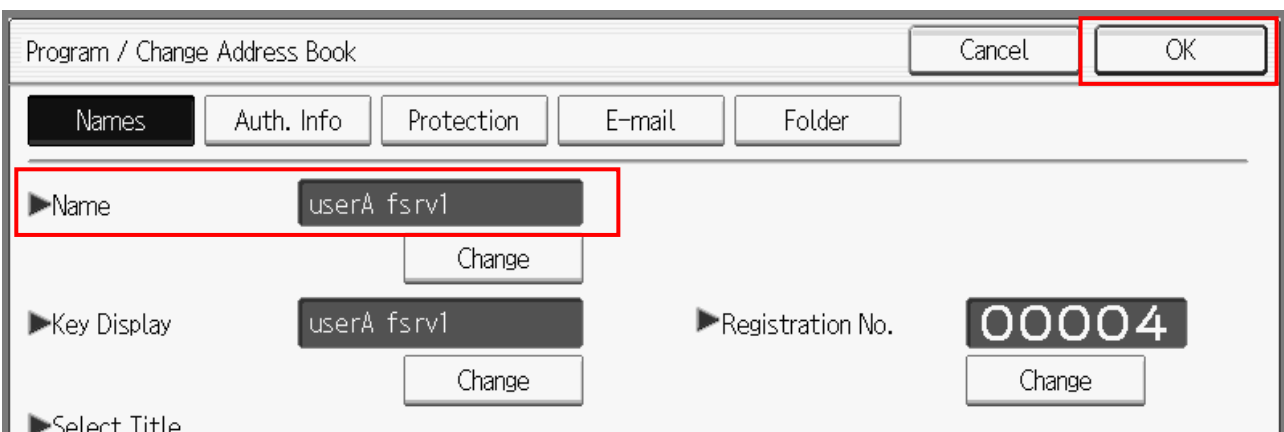


Figure 11

Note: Other tabs do not require configuration. They should be updated automatically.

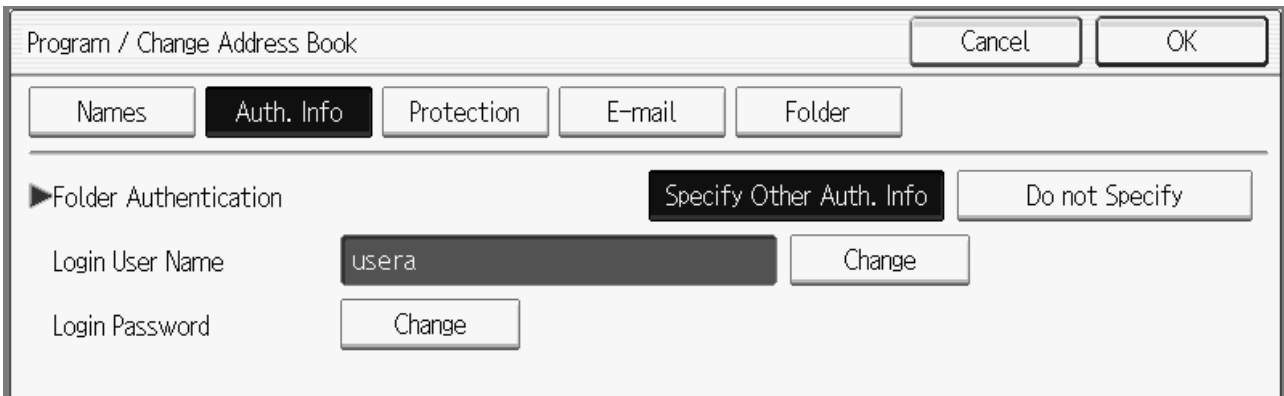


Figure 12

Scan to SMB using the new entry:

If the user returns to the Scanner interface on the operation panel, the new entry should be displayed in the destination list. Only the user who created this destination (userA) will be able to see it in the destination list.

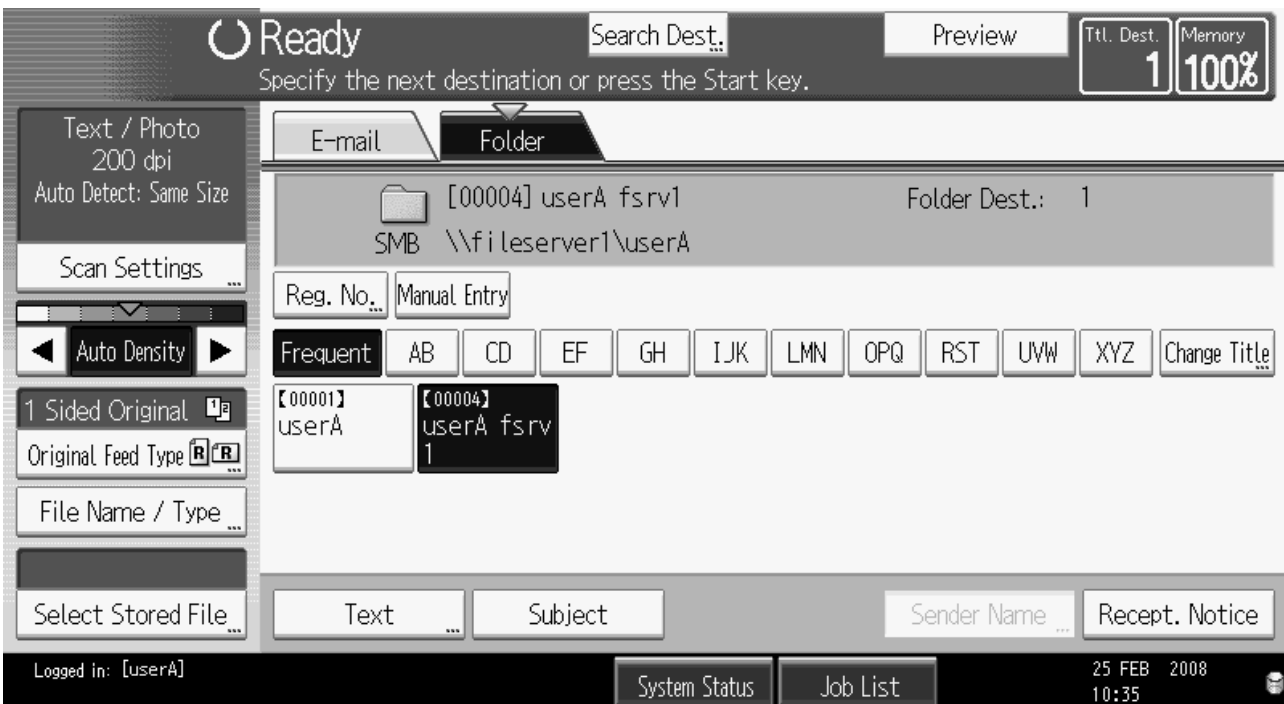


Figure 13

5-2-2 Adding in the addressbook

Open the addressbook and create the destination (WIM/operation panel):

1. Login to the device as userA or the User Administrator
2. Click Add in the addressbook to create a new entry.

3. Enter the name for the entry.

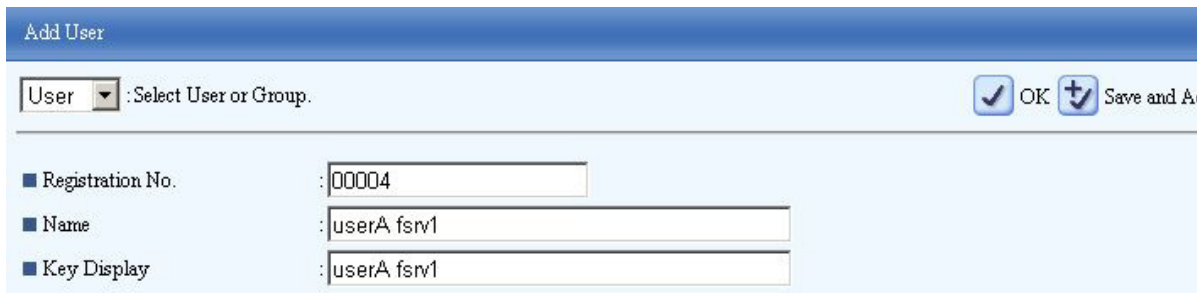


Figure 14

4. Under Folder, select SMB as the Protocol setting and enter the path to the destination folder.

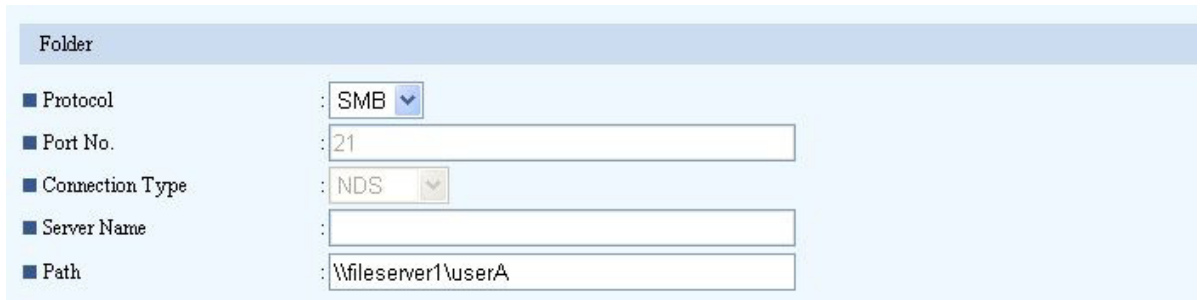


Figure 15

5. Under Authentication Information > Folder Authentication, select "Specify Other Auth. Info" and enter userA's username/password. (In fact any account with write privileges to the folder can be configured here)

Important: Do not use "Use Auth Info at Login". (No device login account will be given to this entry)

These are the settings as seen when logged in as userA.

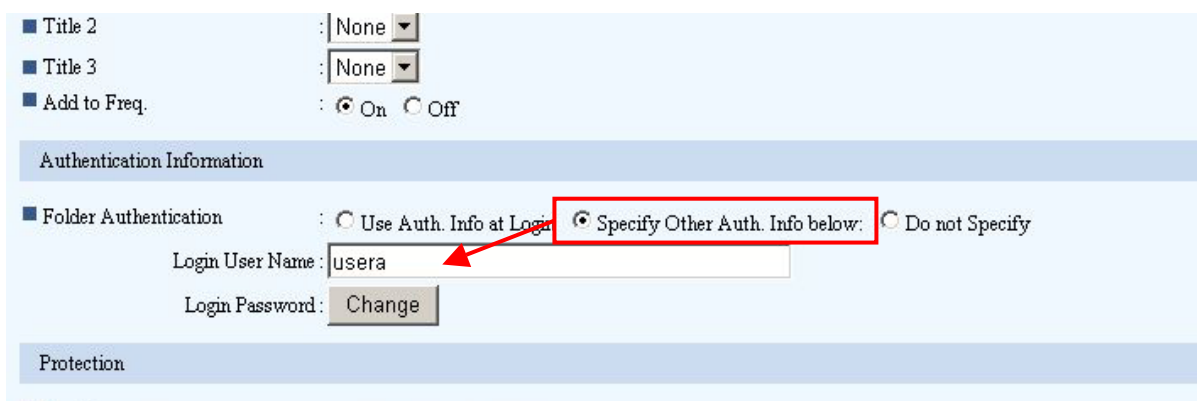


Figure 16

These are the settings as seen when logged in as the User Administrator.

Figure 17

- Under Protection, confirm that "Use Name as > Destination" is checked. The correct configuration for Protect Destination > Access Privilege, depends on who created the entry.

If a user created the entry, there is no need to configure the access privileges. The creator will automatically be given the Full Control privilege. (See 6-1 for a description of access privileges)

If the User Administrator created the entry, click Change and grant the desired privileges to userA's device login account. The privileges given will depend on what userA needs to do and the customer's security policy. (See 6-1 for a description of access privileges)

Public

Use Name as: Destination Sender

Protect Destination: Protection Object: Sender Folder Destination

Protection Code: Change

Access Privilege: Change

Protect File(s): Access Privilege: Change

User/Group

Click User(s) or Group(s) to give the privilege(s).

Navigation: 1/1 Page: [] Go Number of Registered: User(s)3 Group(s)0

Registration No.	Name	Read-only	Edit	Edit/Delete	Full Control
00001	userA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00002	userB	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00003	userC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 18

7. Save the changes and exit.

Scanning to SMB:

Login to the device as userA, select the destination and start scanning. When another user logs in, the newly configured destination will not be displayed in the destination list.

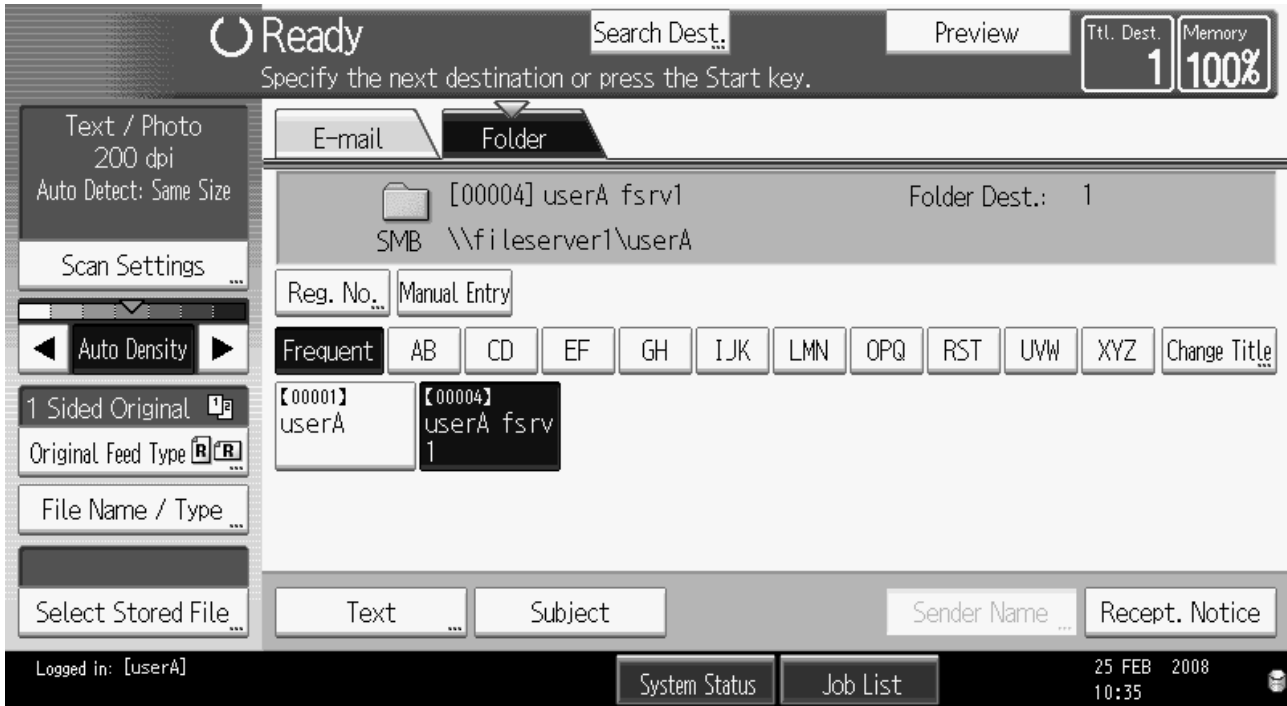


Figure 19

5-3 Sharing a personal destination with other users

Case 3

UserA's personal destination is to be shared with userB and userC. UserA will keep the Full Control privilege as the owner of the destination.

Environment:

1. User authentication has already been configured in the device.
2. All three users already exist in the addressbook.
3. All three users are approved for Scanning.
4. UserA's personal destination has already been configured.

Can be configured by:

- the user himself (userA in this case)...Restriction settings (See [7-2](#)) must be disabled
- User Administrator

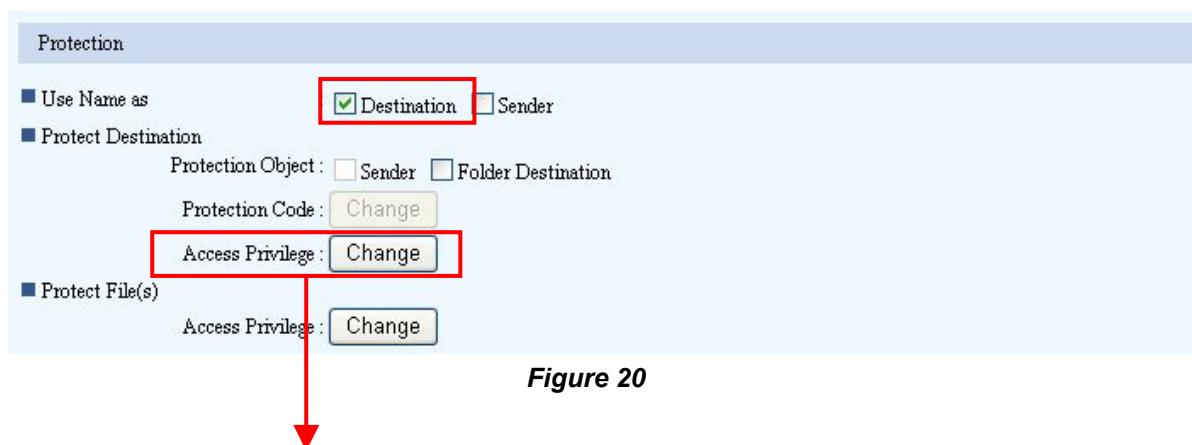
The point of this configuration:

Regardless of the number of users who have access to a destination, all users will access the destination using the same account (the one configured in the added addressbook entry). The security of this situation might concern security conscious customers. This will be discussed in greater detail at the end of this section.

Configuring the destination in the addressbook (WIM/operation panel):

The following procedure is the same for both a user and the User Administrator.

1. Login to the device as userA or the User Administrator.
2. Select the addressbook entry that will be the shared destination, and click Change.
3. In the Protection settings, confirm that "Use Name as > Destination" is checked.
4. Then click Protect Destination > Access Privilege > Change.



- Assign the Read-only permission for this addressbook entry to userB and userC.

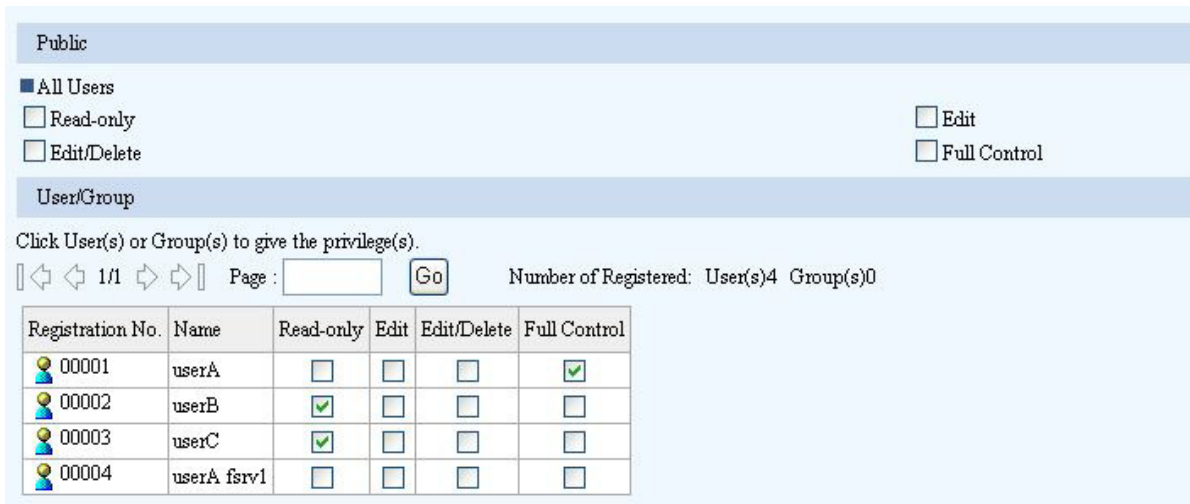


Figure 21

- Save the changes and exit.

Configuring the SMB folder:

Make sure that userA's Windows/SAMBA account has write privileges to the folder. If userB and userC need to retrieve their files, then they should also be assigned permissions on the file server (at least read-only if they are to retrieve their files).

Scanning to SMB:

When any of userA, userB, or userC login to the device, they will see the destination.

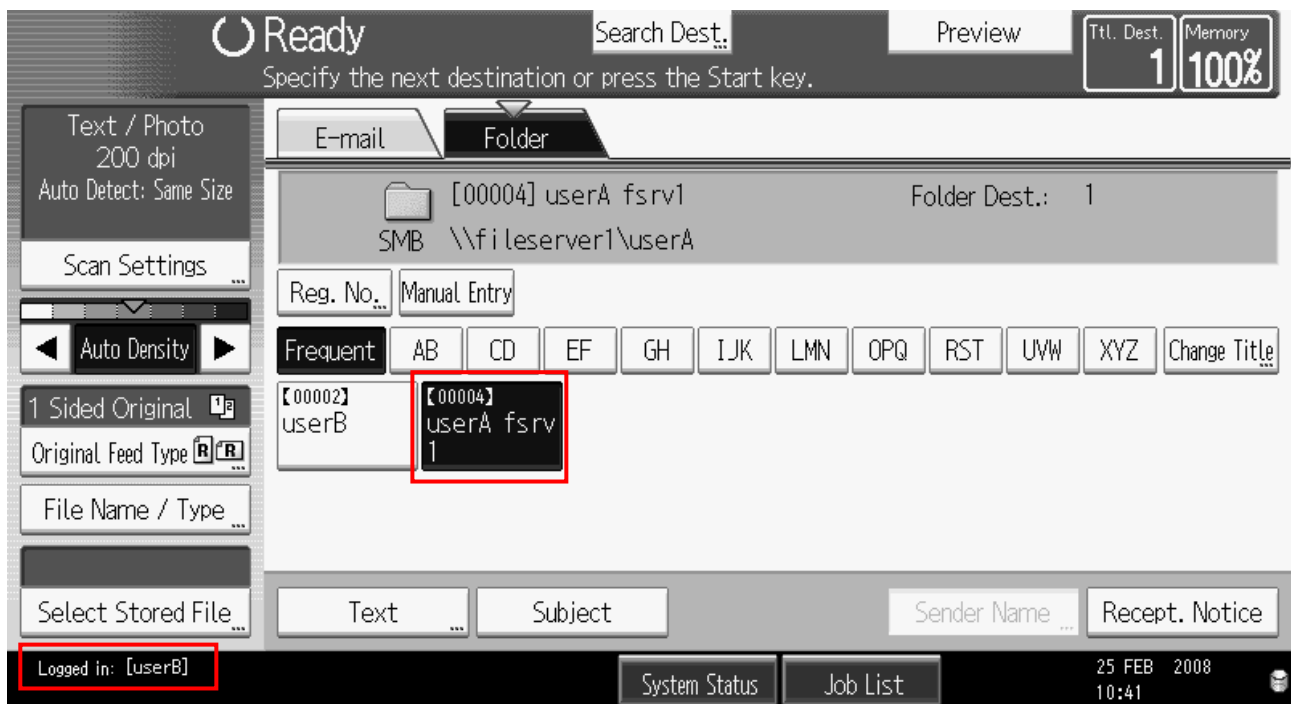


Figure 22

Note: The access account issue in sharing the destination (appeared in this case study)

If a destination is shared among several MFP users, Scan to SMB is performed using the same account (userA's account in this example). The owner of the files will always be userA regardless of who performed the Scan to SMB. No information about the sender (the user logged into the MFP) will be logged on the server side. However, the MFP will log the senders in Scanned File Status.

1. A user logs in to the device.

2. "UserA fsrv1" is selected from the destination list.

3. UserA's account is used to access the destination.

4. UserA will be the owner of all files.

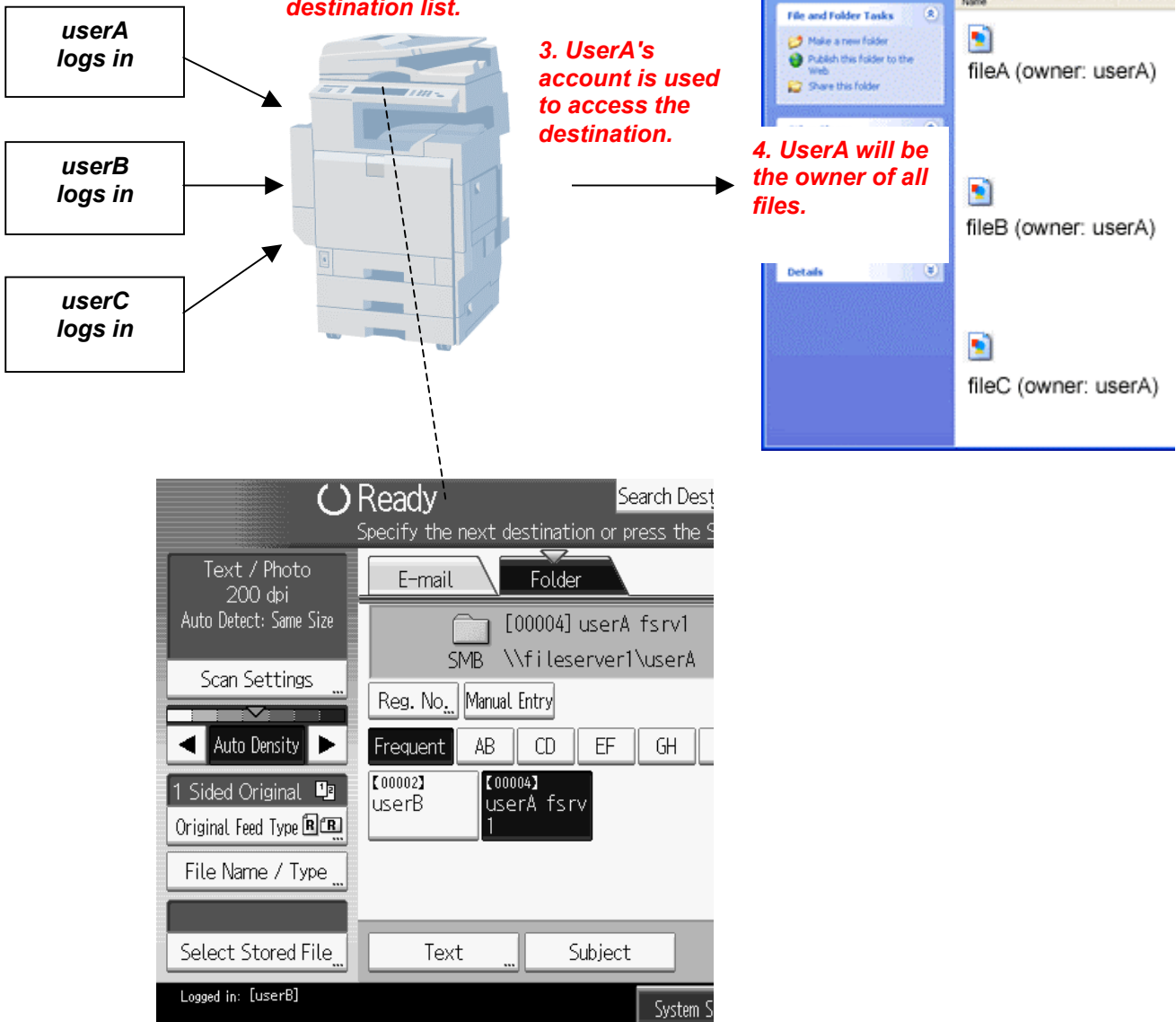


Figure 23

5-4 Creating a public destination

Case 4

A new addressbook entry is used as a "Public" destination by all the addressbook users who are approved for Scanning. The entry will appear in the destination lists of all the users who exist now, as well as of the users who will be added in the future.

Environment:

1. User authentication has already been configured in the device.
2. Users are approved for Scanning

Can be configured by:

- A user (userA in this case)...Restriction settings (See [7-2](#)) must be disabled
- User Administrator

The point of this configuration:

Using the "Public" setting in Protect Destination > Access Privilege, all the users who are approved for scanning will automatically have access to the destination. There will be no need to configure Access Privilege settings for each existing or added user. Note that if a user creates a public destination entry, the user will be the owner of the entry and have the Full Control privilege over that entry in the addressbook.

Regardless of the number of users who have access to a destination, all users will access the destination using the same account (the one configured for the created addressbook entry). The security of this situation might concern security conscious customers. This will be discussed in greater detail at the end of this section.

Creating and configuring the addressbook entry:

1. Login to the device as a user or the User Administrator
2. Click Add in the addressbook to create a new entry.
3. Enter a name for the entry.

Add User

User : Select User or Group. OK Save and...

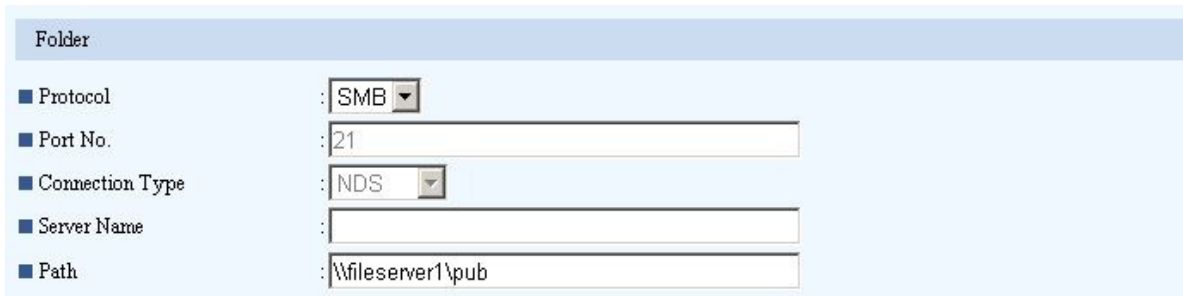
■ Registration No. : 00008

■ Name : public

■ Key Display : public

Figure 24

- Under Folder, select SMB as the Protocol setting and enter the path to the destination folder.

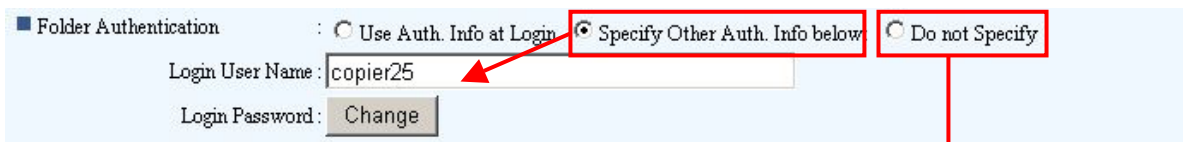


Folder	
■ Protocol	: SMB
■ Port No.	: 21
■ Connection Type	: NDS
■ Server Name	:
■ Path	: \\fileserv1\pub

Figure 25

- Under Authentication Information > Folder Authentication, select "Specify Other Auth. Info" or "Do not Specify".

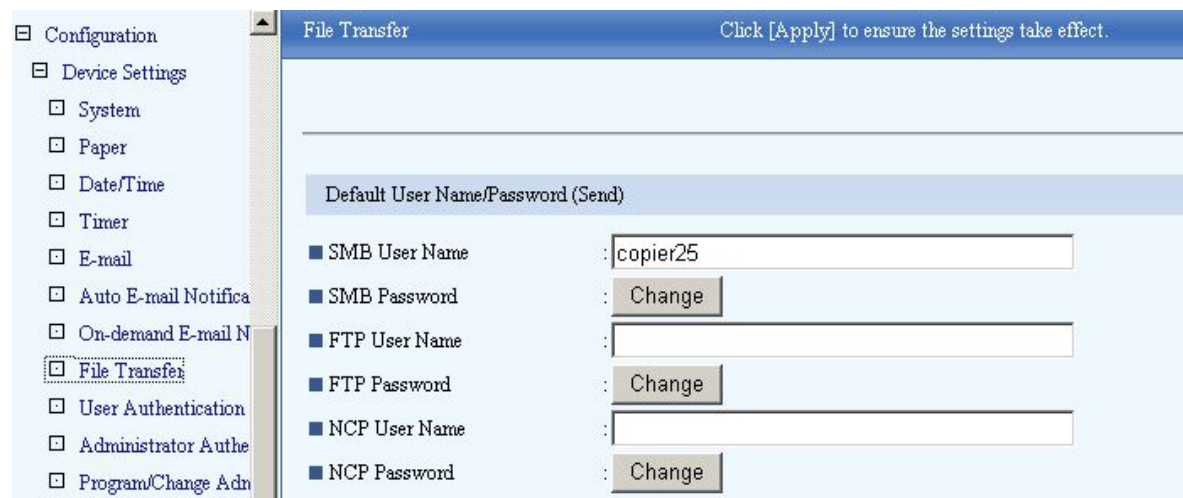
Important: Do not use "Use Auth Info at Login". (No device login account will be given to this entry)



■ Folder Authentication	: <input type="radio"/> Use Auth. Info at Login	<input checked="" type="radio"/> Specify Other Auth. Info below	<input type="radio"/> Do not Specify
Login User Name:	: copier25		
Login Password:	: Change		

Figure 26

If "Do not Specify" is selected, the default device Scan to SMB account will be used to access the SMB folder.



File Transfer		Click [Apply] to ensure the settings take effect.
Default User Name/Password (Send)		
■ SMB User Name	:	copier25
■ SMB Password	:	Change
■ FTP User Name	:	
■ FTP Password	:	Change
■ NCP User Name	:	
■ NCP Password	:	Change

Figure 27

Note: Either an existing addressbook user's account or a new account can be assigned to this entry in the addressbook. If a new account is used, it will be necessary to configure the destination folder to grant write privileges to the account.

- Under Protection, confirm that "Use Name as > Destination" is checked. Then click Protect Destination > Access Privilege > Change and assign the Read-only permission for the addressbook entry to All Users under Public.

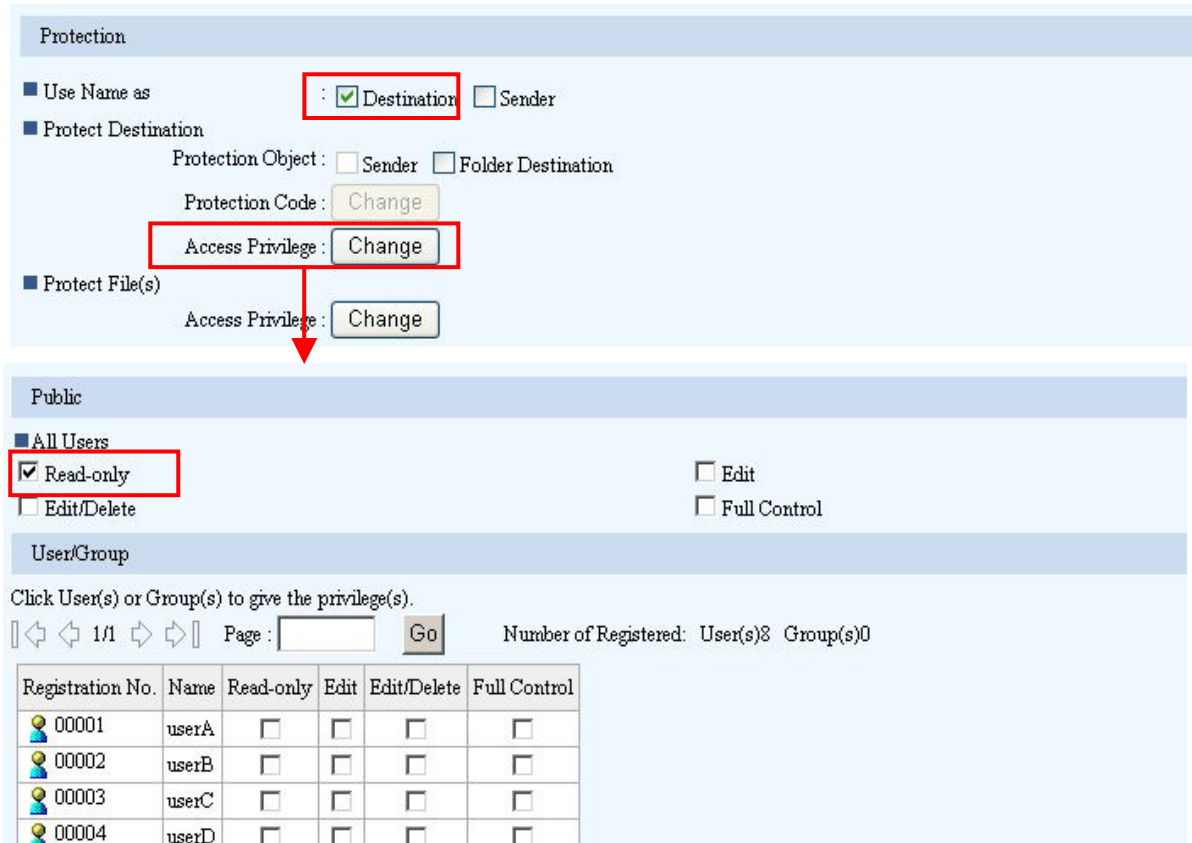


Figure 28

7. Save the changes and exit.

Scanning to SMB:

All users given the Read-only permission will be able to see the destination when they login.

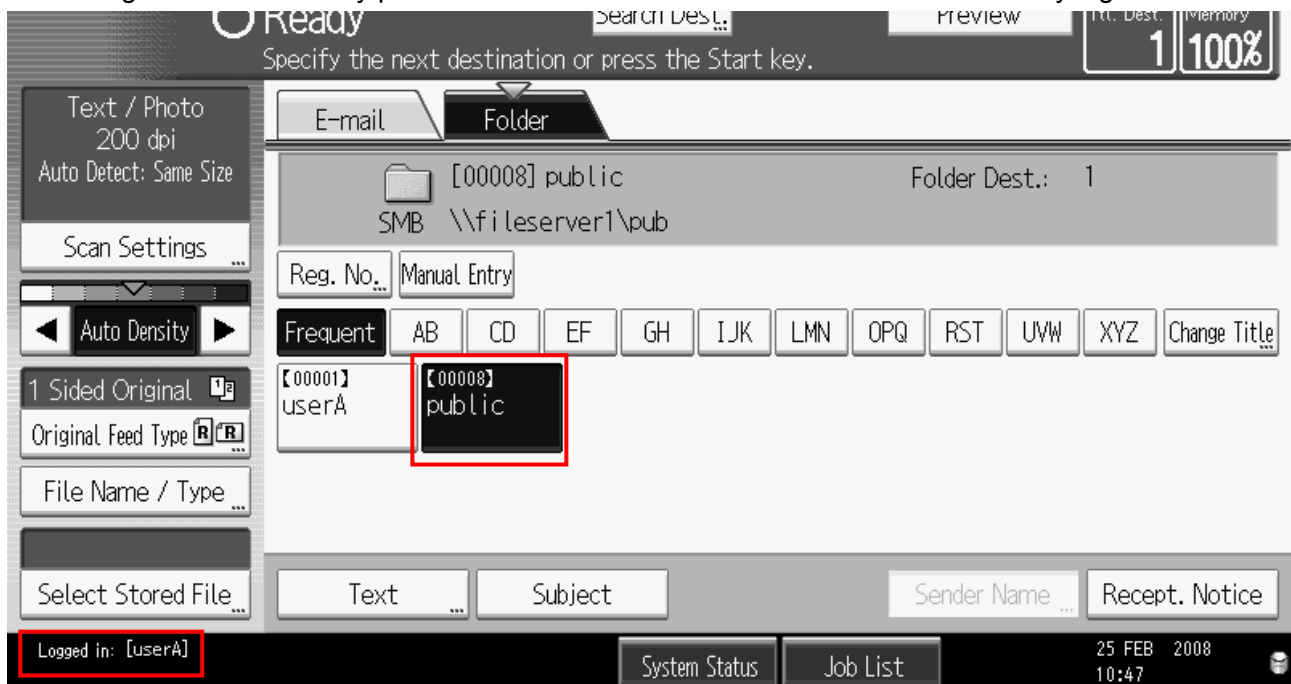


Figure 29

Note: The access account issue in sharing the destination (appeared in this case study)

If a destination is shared among several MFP users, Scan to SMB is performed using the same account (the account configured by the User Admin in this example). The owner of the files will always be the configured account regardless of who performed the Scan to SMB. No information about the sender (the user logged into the MFP) will be logged on the server side. However, the MFP will log the senders in Scanned File Status.

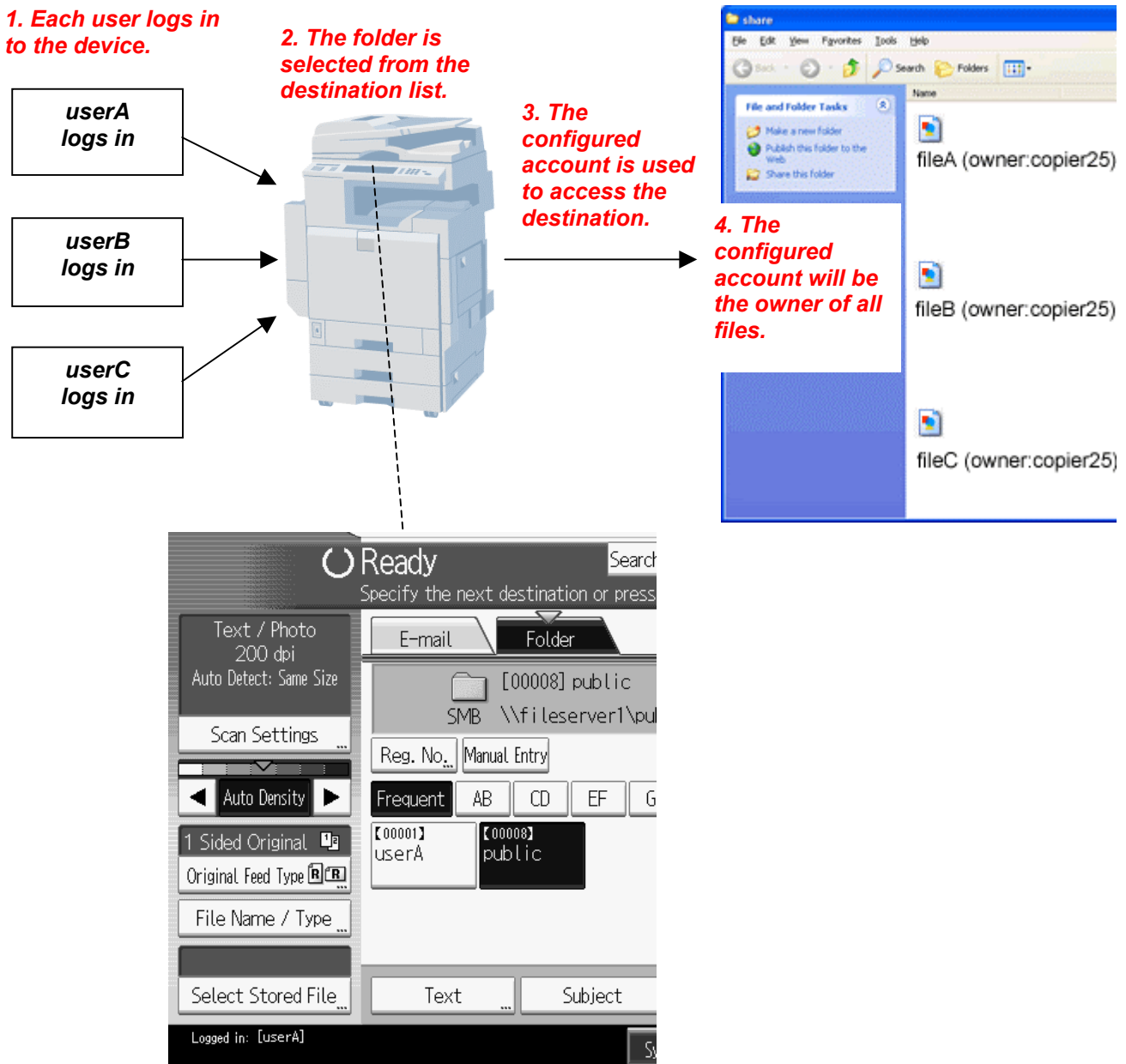


Figure 30

6. Using "Enter Destination (Manual Entry)" when Scanning

It is possible to send a Scan to SMB to a destination that has not been configured in the address book. This is done by using "Enter Destination" from the Scanner interface. In such a case, an SMB login account might be pre-configured automatically in the Enter Destination screen. This section explains the source of this pre-configured account.

The "Enter Destination" button in 05S or earlier models.

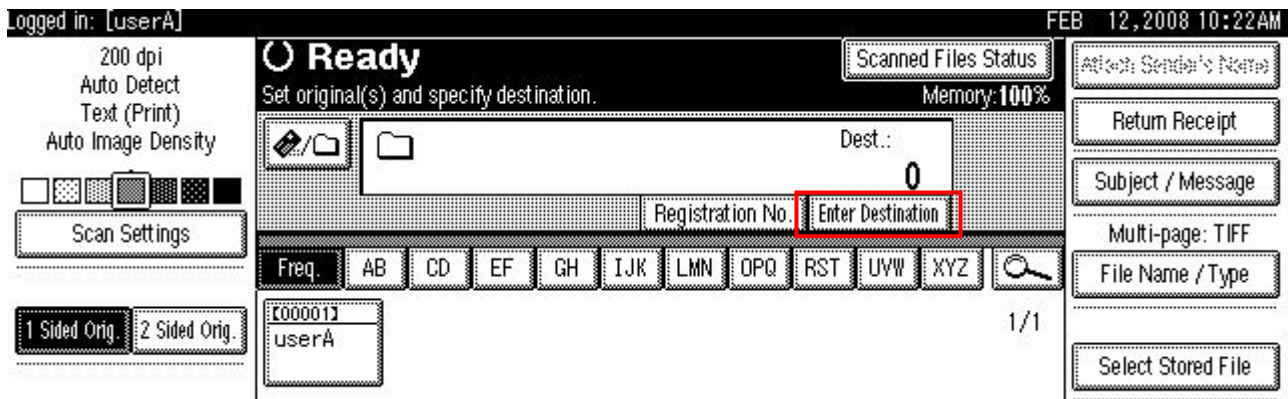


Figure 31

The "Manual Entry" in 05A or later models.

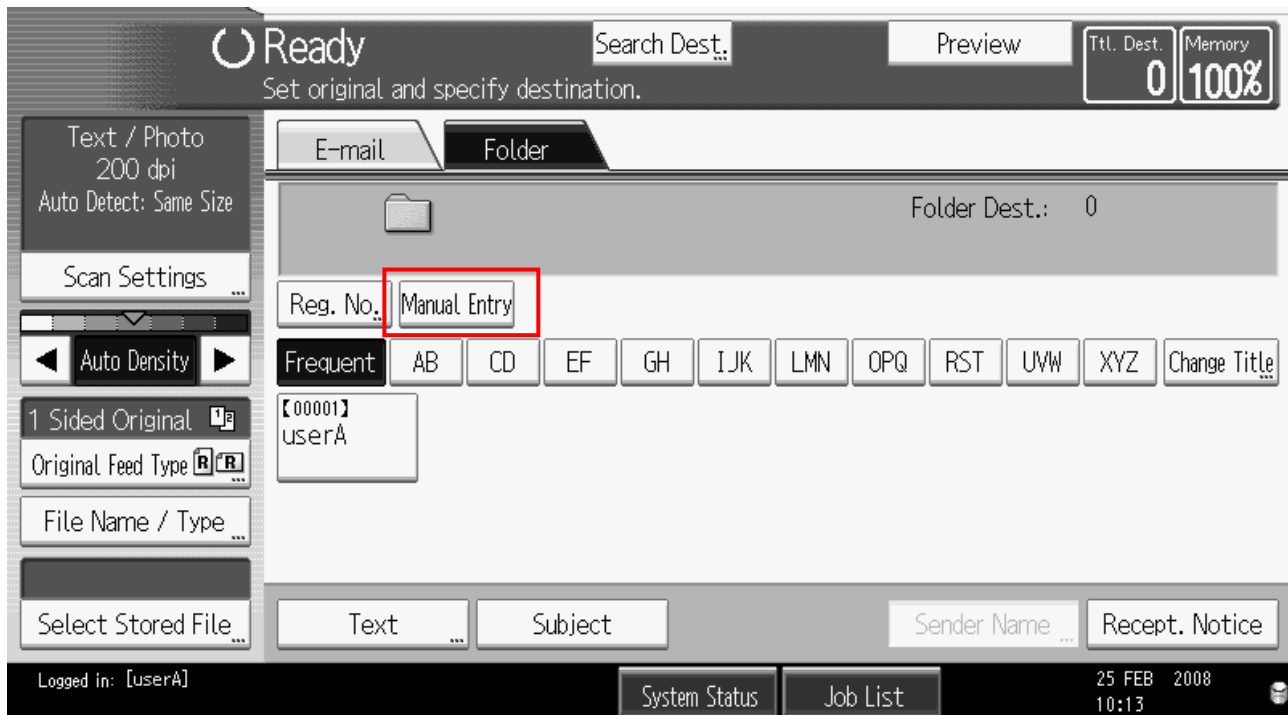


Figure 32

Note: A user's use of "Enter Destination / Manual Entry" can be restricted by Extended Security settings. See [7-2](#) for details.

6-1 "Enter Destination" and the sender's SMB account

If user authentication (Basic/Windows/LDAP/Integration Server) is enabled on the device, the account that is configured for the sender will appear in the screen as the default value. However, the Path, User Name, or Password can all be changed by clicking the Manual Entry button (or the Browse button to find a path).

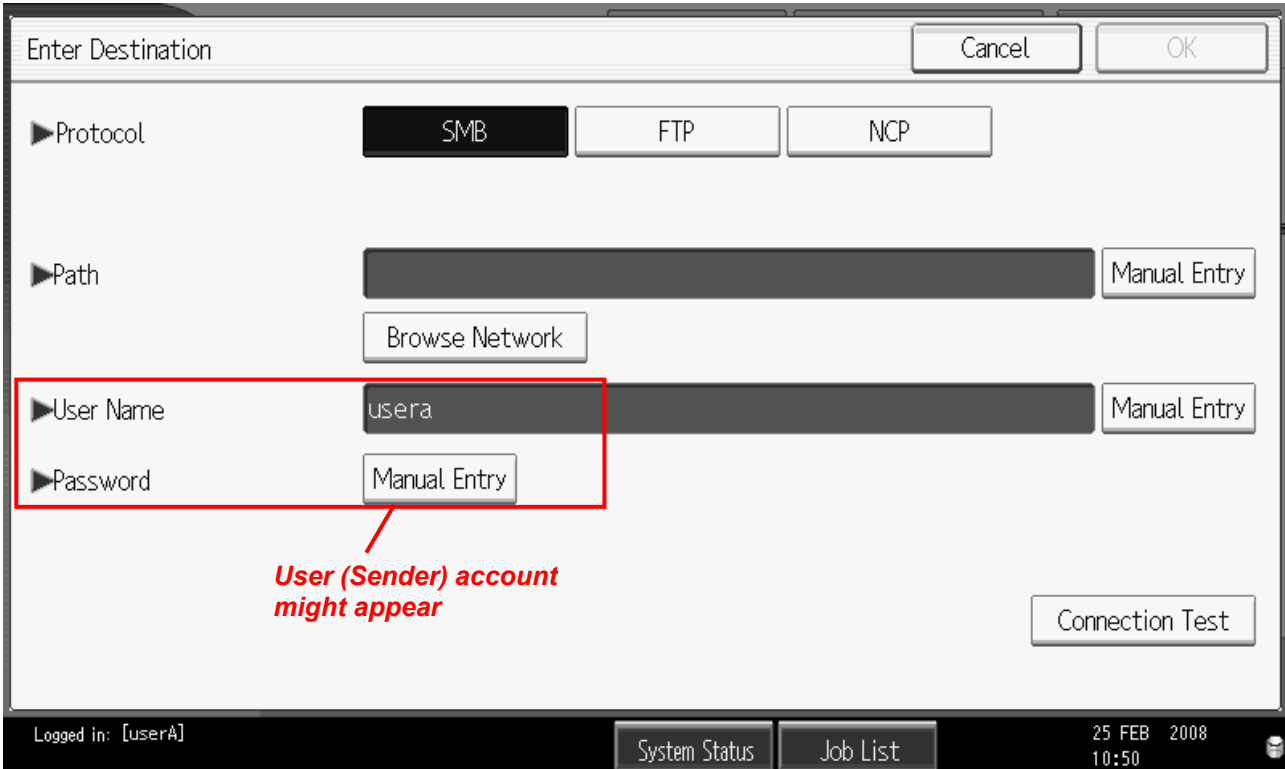


Figure 33

The name that appears for the User Name depends on whether "Use Auth. Info at Login" or "Specify Other Auth. Info" is selected in Folder Authentication. If "Use Auth. Info..." is selected, the account configured in "Authentication Info. at Login" will appear. If "Specify Other..." is selected, the account configured in "Folder Authentication" will appear.

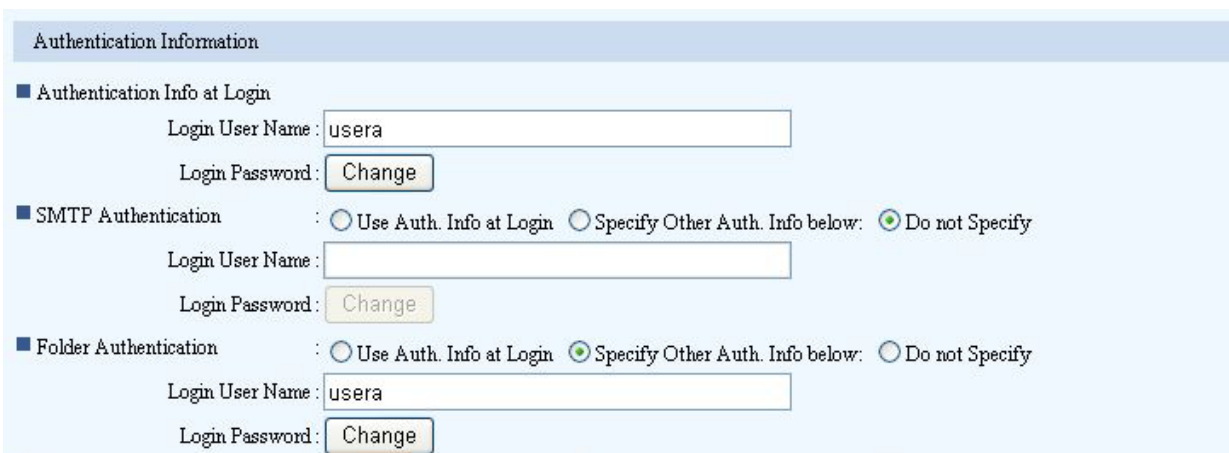


Figure 34

6-2 "Enter Destination" and the device default SMB account

If Scan to SMB is performed using a blank username and password, the device default SMB account (Device Settings > File Transfer > SMB User Name/Password) will be used automatically. This will seem transparent to the user.

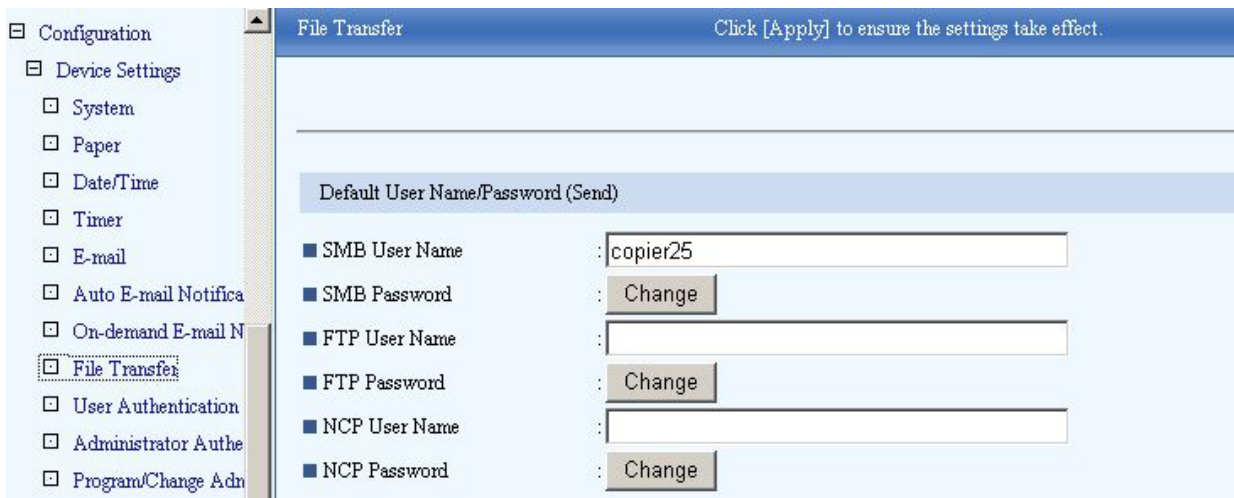
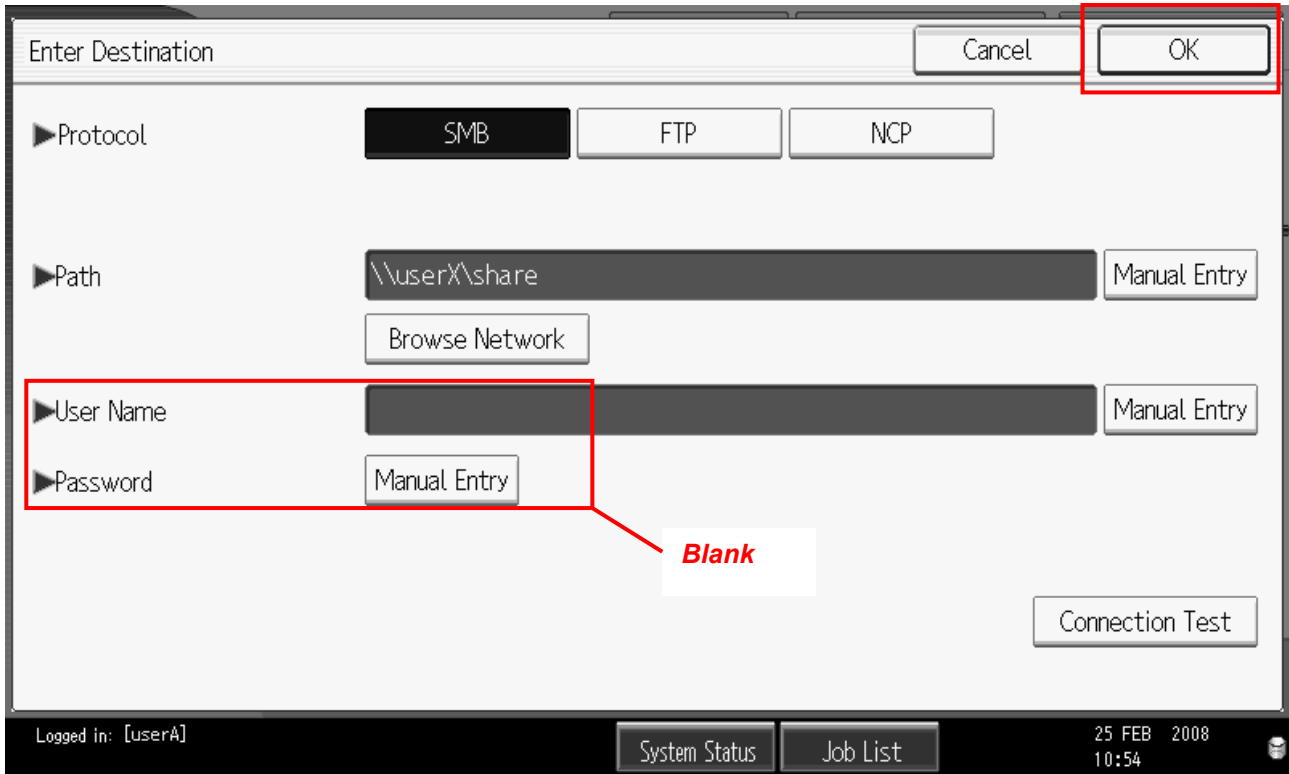


Figure 35

The access account when using "Enter Destination / Manual Entry"

Using "Enter Destination / Manual Entry", the manually entered individual access accounts are used to access the destination folder. The owner of the files will be the senders of them.

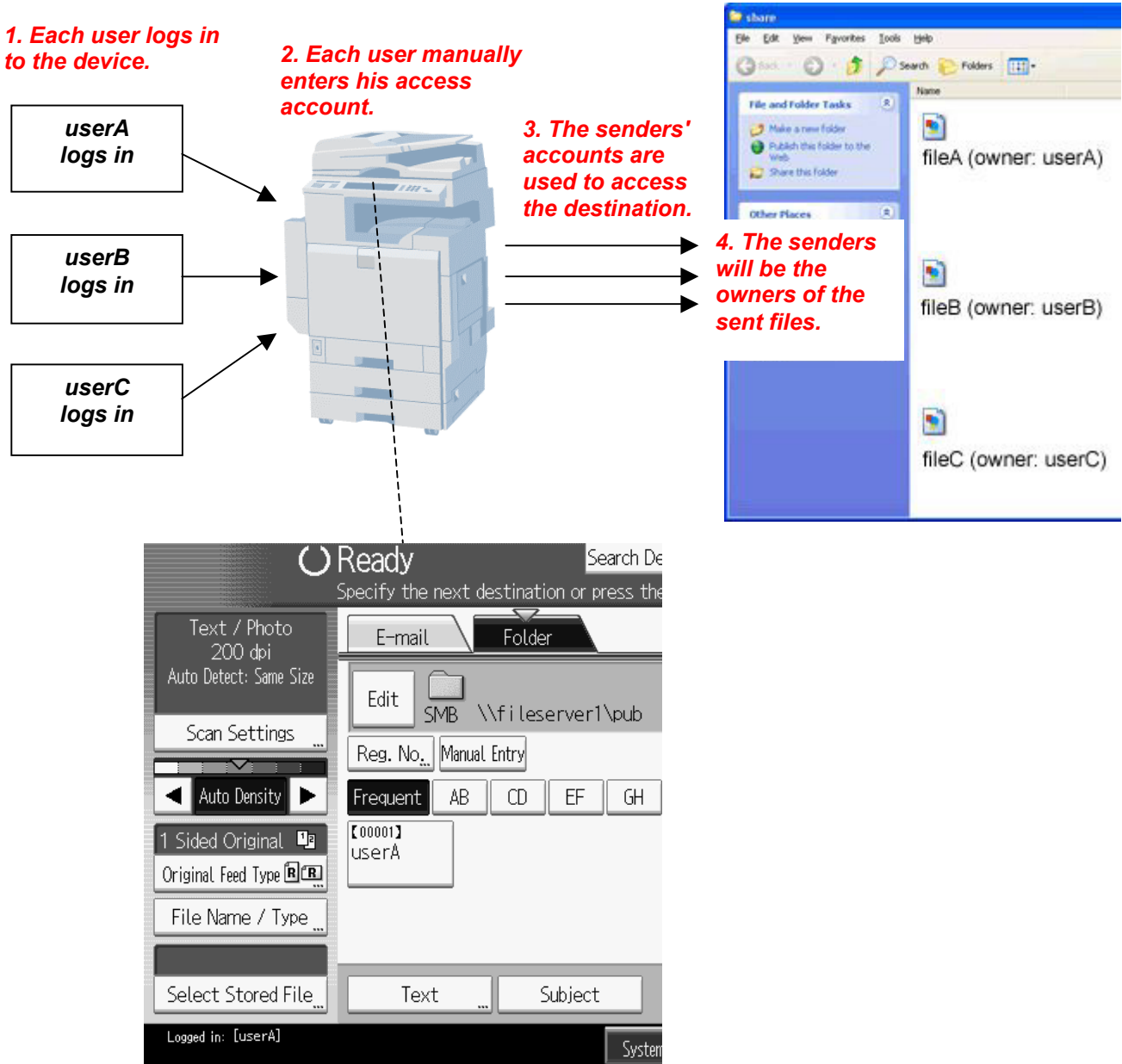


Figure 36

7. Configuration notes

7-1 Access Privileges

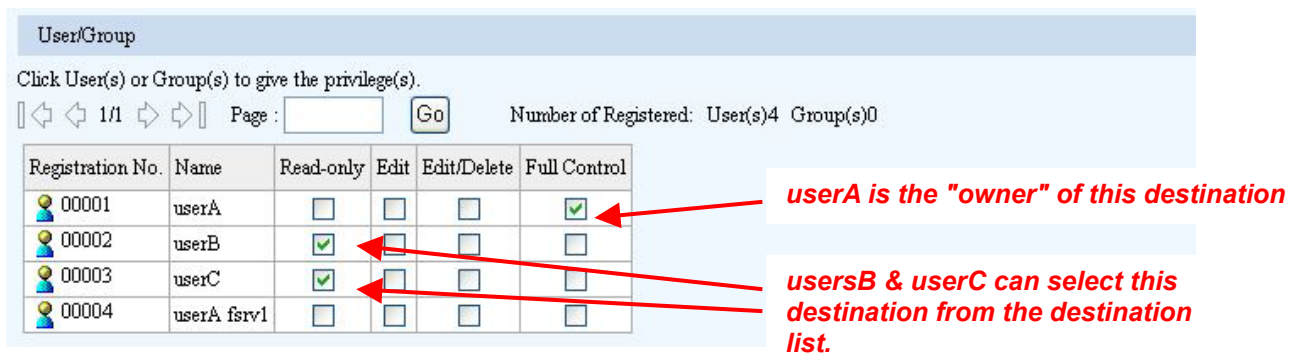
The most important thing to understand about addressbook permissions is that they have nothing to do with folder permissions. The permissions configured in the addressbook simply allow users different levels of access to addressbook entries.

Read-only: MFP users with this permission can see the destination in the MFP's destination list.

Edit: MFP users with this permission can reconfigure the destination.

Edit/Delete: In addition to editing, MFP users with this permission can also delete the entry.

Full Control: MFP users with this permission can change the permissions of other MFP users. The owner of the destination entry will be given this permission by default.



The screenshot shows a table with columns: Registration No., Name, Read-only, Edit, Edit/Delete, and Full Control. There are four rows of users. Red arrows point from text annotations to specific cells in the table.

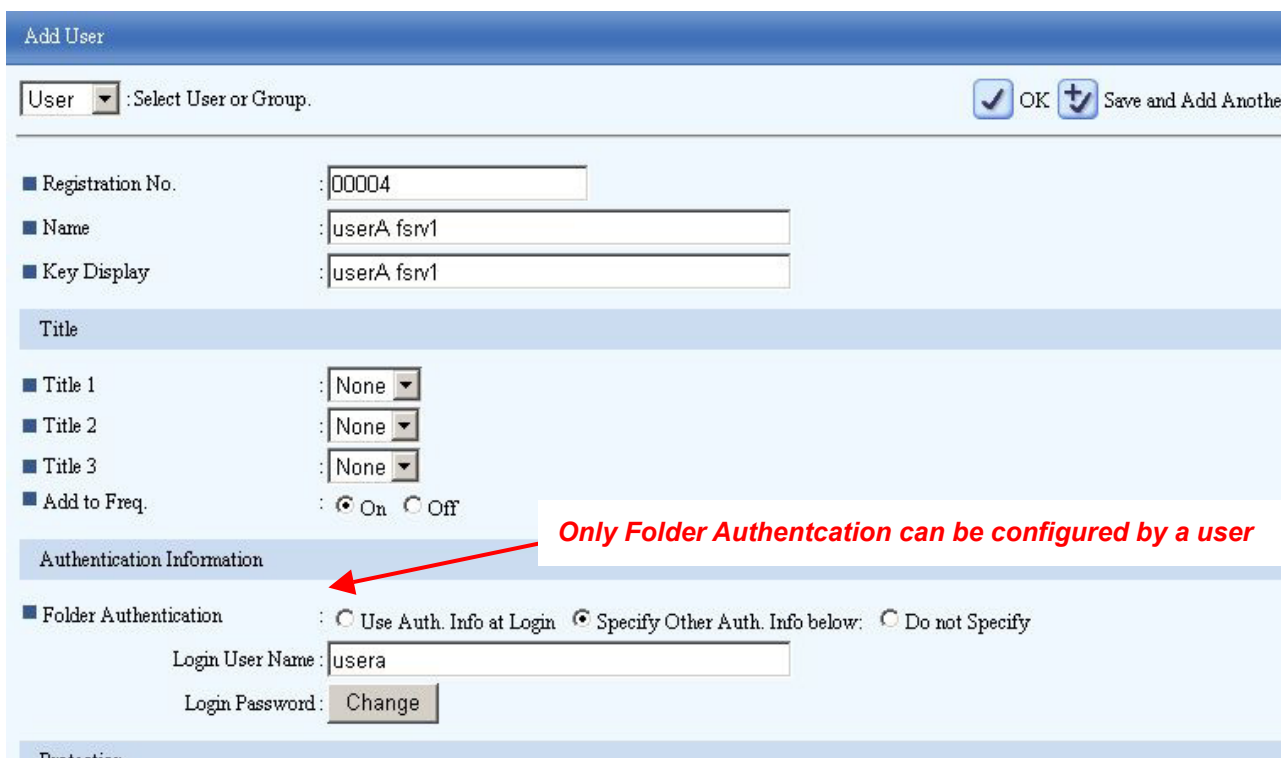
Registration No.	Name	Read-only	Edit	Edit/Delete	Full Control
00001	userA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
00002	userB	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00003	userC	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00004	userA fsrv1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

userA is the "owner" of this destination

usersB & userC can select this destination from the destination list.

Figure 37

Note: As mentioned in section 5-2, when a destination-only account is created, the "Use Auth. Info at Login" setting should never be selected. Because this account is only used as a destination, it will never login to the device and will therefore have no "Auth. Info".



The screenshot shows the 'Add User' configuration form. The 'Folder Authentication' section is highlighted with a red arrow pointing to the 'Specify Other Auth. Info below' radio button.

Only Folder Authentication can be configured by a user

Figure 38

7-2 Destination restriction settings

Users can be prevented from manually entering a destination or creating/editing a destination in the addressbook. This is done using Extended Security (operation panel only) and can only be performed by the User Administrator.

System Settings > Administrator Tools > Extended Security.

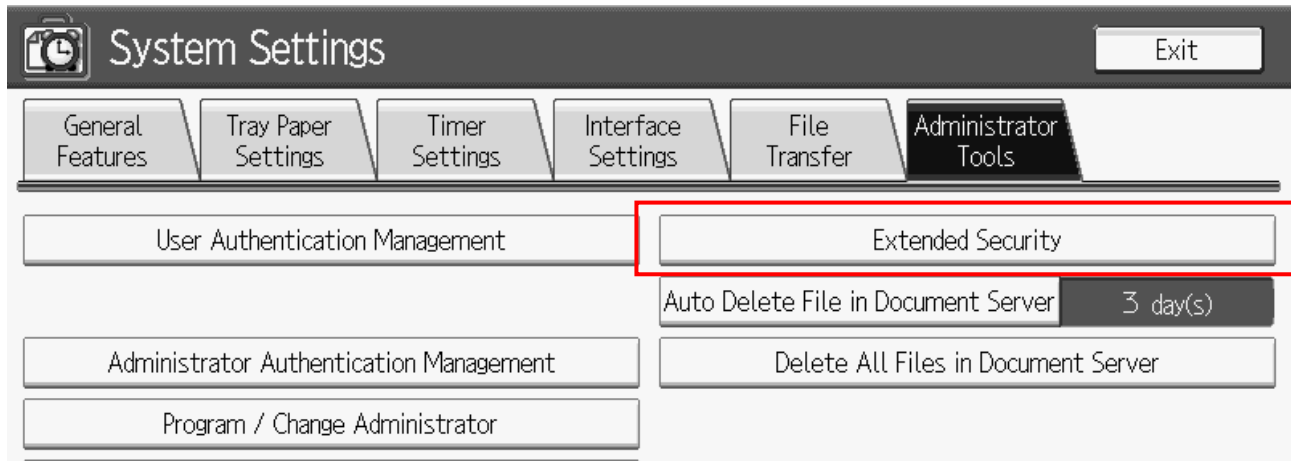


Figure 39

The restriction settings can be configured only by User Administrator.

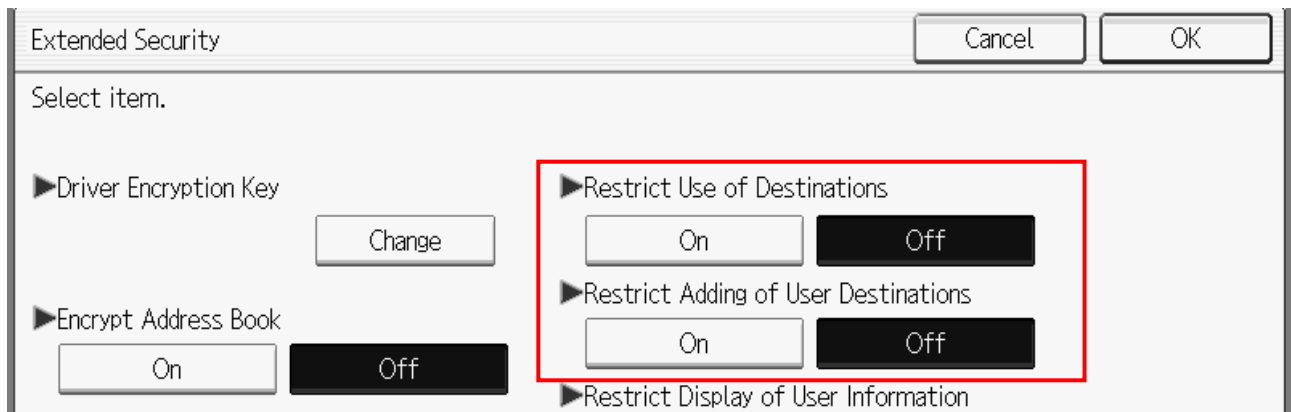


Figure 40

Restrict Use of Destinations:

This setting is "Off" by default. Turning it "On", removes the "Enter Destination" button from the Scan to Folder interface on the MFP operation panel. This prevents users from manually entering Scan to SMB paths.

Note: Turning this setting "On" also removes the "Manual Input" button from the Scan to Email interface and will prevent users from manually entering Scan to Email destinations.

Restrict Adding of User Destinations:

This setting is "Off" by default. Turning it "On", removes the "Prog Dest." button. This prevents users from adding new addressbook entries from the Scanner interface. Users will also be prevented from adding or editing destinations using the addressbook interface.

Note: This will also prevent users from adding new addressbook entries in Scan to Email.

The default screen after using "Enter Destination" in Scan to SMB:



Figure 41

"Restrict Use of Destinations" enabled:



Figure 42

"Restrict Adding of User Destinations" enabled:



Figure 43

Note:

Enabling either of these settings prevents users from accessing the addressbook as a whole. As a result, not only entries for personal destinations but also entries for device login accounts become inaccessible for users. Users will not be able to edit their own authentication information, folder paths or email addresses anymore. If the Basic Authentication is used, users will not be able to edit their own passwords either.

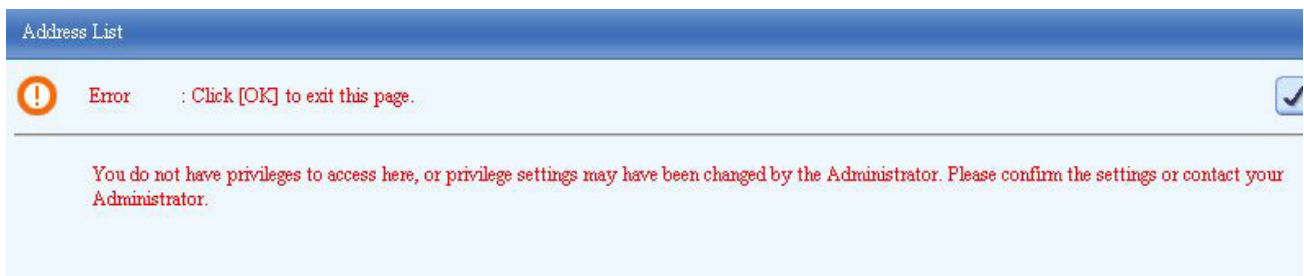


Figure 44