

## Scan to E-mail White Paper

### NOTICE

THIS DOCUMENT SHALL NOT BE REPRODUCED IN WHOLE OR IN PART, FOR ANY PURPOSE OR IN ANY FASHION AND DISTRIBUTED WITHOUT THE PRIOR WRITTEN CONSENT OF RICOH CORPORATION. WHICH CONSENT RICOH CORPORATION MAY GRANT OR DENY IN ITS SOLE DISCRETION.

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 and for the benefit of such companies. Ricoh does not grant or intend to grant hereby any right to such trademarks or property to any third parties. No such use, or the use of any trade name, or web site is intended to convey endorsement or other affiliation with Ricoh products.

Although best efforts were made to prepare this document, Ricoh Corporation 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 performances, 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.

**Ricoh Americas Corporation  
May 2007**

---

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION.....</b>	<b>4</b>
1.2	Target Audience .....	4
<b>2</b>	<b>MODEL CROSS REFERENCE .....</b>	<b>5</b>
<b>3</b>	<b>SETTING/SPECS .....</b>	<b>7</b>
<b>4</b>	<b>SETTING UP SCAN TO E-MAIL VIA WEB IMAGE MONITOR .....</b>	<b>7</b>
4.1	Web Image Monitor Administrator Login Process.....	7
4.2	Network Settings via WIM.....	9
4.3	SMTP Authentication via WIM .....	10
4.4	POP before SMTP Configuration via WIM.....	11
4.5	LDAP Settings in WIM .....	11
4.6	Address Book Settings in WIM .....	13
4.7	Address Book Settings from the Operation Panel .....	15
<b>5</b>	<b>SETTING SENDER OPTIONS VIA THE MFP OPERATION PANEL.....</b>	<b>16</b>
5.1	Secure Devices.....	16
5.2	Non-Secure Devices.....	16
<b>6</b>	<b>SCAN TO E-MAIL OPERATION.....</b>	<b>17</b>
6.1	Additional Scan to E-mail Settings.....	17
6.2	Scanned Files Status .....	18
6.3	Additional MFP User Tool Options .....	18
<b>7</b>	<b>SCAN TO E-MAIL IN WINDOWS SERVER 2000 OR 2003.....</b>	<b>19</b>
7.1	Enabling SMTP Relay for Windows Server with MS Exchange .....	19
7.2	Device Relays through Exchange 5.5 on Windows 2000 Server .....	21
<b>8</b>	<b>SCAN TO E-MAIL FAILURE USING WINDOWS AUTHENTICATION .....</b>	<b>22</b>
8.1	Tracing the Authentication Error .....	22

8.2 Authentication Error Resolution .....23

**9 FILE SIZE LIMITS.....24**

9.1 Accessing the File Size Limits .....24

9.2 Setting File Size Limits on the MFP.....25

9.3 Decode Shell Extension.....27

**10 ARGOSOFT FOR E-MAIL RELAY .....28**

10.1 Creating ArGoSoft User Profiles .....29

10.2 ArGoSoft Setup in Web Image Monitor .....30

10.3 ArGoSoft Relay Monitor.....31

10.4 ArGoSoft Limitations.....31

**11 SUMMARY.....31**

# 1 Introduction

Ricoh Corporation developed Scan to E-mail to allow users the ease of sending scan files directly from the MFP to an entered destination.

The MFP can be configured to use Scan to E-mail via any of the three interfaces below.

- Op-Panel
- Web Image Monitor
- Smart Device Monitor

This can be used on mixed network environments.

- In addition to Windows, LINUX, UNIX and Mac OS can send/receive data to/from the FTP server.

## 1.2 Target Audience

The target audience for this White Paper is:

- IT Administrators.
- All end-users - The information contained in the document can be distributed to end-users as long as the restrictions outlined on the cover page are followed.
- The support and marketing staff of Ricoh Sales companies, including Ricoh family group companies and their subsidiaries.
- Technical support personnel (CEs) of dealers.

## 2 Model Cross Reference

The tables below covers all models referenced in this document.

Product Code	Ricoh Corp Model Name	Savin (USA) Model Name	Gestetner Model Name	Lanier Model Name
B051	Aficio 1224C	C2408	DSc224	LD024C
B052	Aficio 1232C	C3210	DSc232	LD032C
B064	Aficio 1060	2560	6002	LD060
B065	Aficio 1075	2575	7502	LD075
B070	Aficio 2090	4090	9002	LD090
B071	Aficio 2105	4105	10512	LD0105
B079	Aficio 2035	4035	3532	LD035
B082	Aficio 2045	4045	4532	LD045
B089	Aficio 2022	4022	Dsm622	LD122
B093	Aficio 2027	4027	Dsm627	LD127
B121	Aficio 2015	4015	DSM615	LD115
B122	Aficio 2018	4018	DSM618	LD118
B123	Aficio 2018D	4018D	DSM618d	LD118D
B129	Aficio 1515	3515	Dsm415	LD015
B130	Aficio 1515MF	3515MF	Dsm415pf	LD015spf
B132	Aficio 3260c	C6045	DSc460	LD160c
B135	Aficio 2035e	4035e	Dsm635	LD135
B138	Aficio 2045e	4045E	Dsm645	LD145
B140	Aficio 2060	4060	Dsm660	LD160
B141	Aficio 2075	4075	Dsm675	LD175
B142	Aficio 2060SP	4060sp	Dsm660sp	LD160 SP
B143	Aficio 2075SP	4075sp	Dsm675sp	LD175 SP
B147	Aficio 2232c	C3224	DSc332	LD232c
B149	Aficio 2238c	C3828	DSc338	LD238c
B156	Aficio 3224c	C2410	DSC424	LD124C
B163	Aficio 2051	4051	Dsm651	LD151
B168	Aficio 1515F	3515F	Dsm415f	LD015f
B169	Aficio 2013PS		Dsm415p	LD015sp
B178	Aficio 3235C	C3528	DSc435	LD335c
B180	Aficio 3245C	C4535	DSc445	LD345c
B182	Aficio 2035eSP	4035Esp	Dsm635sp	LD135
B183	Aficio 2045eSP	4045Esp	Dsm645sp	LD145
B188	Aficio 480W	4800WD	A080	LW411
B190	Aficio 2228c	C2820	DSc328	LD228c
B200	Aficio 5560	SDC555	CS555	LC155
B202	Aficio 3228C	C2824	DSC428	LD328c

<b>Product Code</b>	<b>Ricoh Corp Model Name</b>	<b>Savin (USA) Model Name</b>	<b>Gestetner Model Name</b>	<b>Lanier Model Name</b>
B205	Aficio 3025 SP/SPF/Spi/P	8025 SP/SPF/Spi/G	DSm725 SP/SPF/Spi/G	LD225/SP
B209	Aficio 3030 SP/SPF/Spi/P	8030 SP/SPF/Spi/G	DSm730 SP/SPF/Spi/G	LD230
B222	MP C3500	C3535	DSc535	LD435c
B224	MP C4500	C4540	DSc545	LD445c
B228	Aficio 2051SP	4051sp	DSm651sp	LD151 SP
B229	Aficio 615c	SGC 1506	GS 106	LD215cg
B230	Aficio MP C2500	C2525	DSc525	LD425c
B234	Aficio MP9000	8090	DSm790	LD190
B235	Aficio MP1100	8110	DSm7110	LD1110
B236	Aficio MP1350	8135	DSm7135	LD1135
B237	Aficio MP C3000	C3030	DSc530	LD430c
B245	Aficio MP 1500	-	DSm715	LD315
B246	Aficio MP 5500	8055	DSm755	LD255
B248	Aficio MP 6500	8065	DSm765	LD265
B249	Aficio MP 7500	8075	DSm775	LD275
B250	Aficio MP 5500 SP	8055 SP	DSm755 SP	LD255 SP
B252	Aficio MP 6500 SP	8065 SP	DSm765 SP	LD265 SP
B253	Aficio MP 7500 SP	8075 SP	DSm775 SP	LD275 SP
B259	Aficio 2016	8016	DSm616	LD116
B260	Aficio 2020	8020	DSm620	LD120
B261	Aficio 2020D	8020d	DSm620d	LD120d
B262 / B292	Aficio MP 161	816	DSm416	LD016
B264	Aficio 3035 SP/SPF/Spi/G	8035 SP/SPF/Spi/G	DSm735 SP/SPF/Spi/G	LD235
B265	Aficio 3045 SP/SPF/Spi/G	8045 SP/SPF/Spi/G	DSm745 SP/SPF/Spi/G	LD245
B276	Aficio MP 1600	9016	DSm716	LD316
B277	Aficio MP 2000	9021d	DSm721d	LD320
B284	Aficio MP 161F	816f	DSm416f	LD016f
B288	Aficio MP 161SPF	816mf	DSm416pf	LD016SPF
B291	Aficio MP 3500G	8035eg	DSm735eg	-
B295	Aficio 4500G	8045eg	DSm745eg	-
B296	Aficio MP 3500	8035e	DSm735e	LD335
B297	Aficio MP 4500	8045e	DSm 745e	LD345
D007	Aficio MP 2510	8025e	DSm725e	LD325
D008	Aficio MP 3010	8030e	DSm730e	LD330

### 3 Setting/Specs

- Email client such as MS Outlook 2000, Lotus Notes R5, or Outlook Express
- Email server such as Exchange, Lotus Notes

### 4 Setting up Scan to E-mail via Web Image Monitor

Many of the Scan to E-mail settings can be configured via Web Image Monitor (WIM). This section covers the steps used to configure the necessary settings. These settings can only be changed by an Administrator, and the process used to login as an Administrator is outlined in the following section.

#### 4.1 Web Image Monitor Administrator Login Process

In order to access, and change, the necessary settings, it is necessary to login to WIM as an Administrator. The Administrator login process is outlined below.

1. Enter the IP address in the address field using the following form: *http://printer host name or IP address* (e.g. <http://172.16.121.40>) and click on **Go** or press Enter. This opens the page shown in Figure 4.1 below.
2. In the upper right-hand corner, click **Login**, which opens a login page (Figure 2).

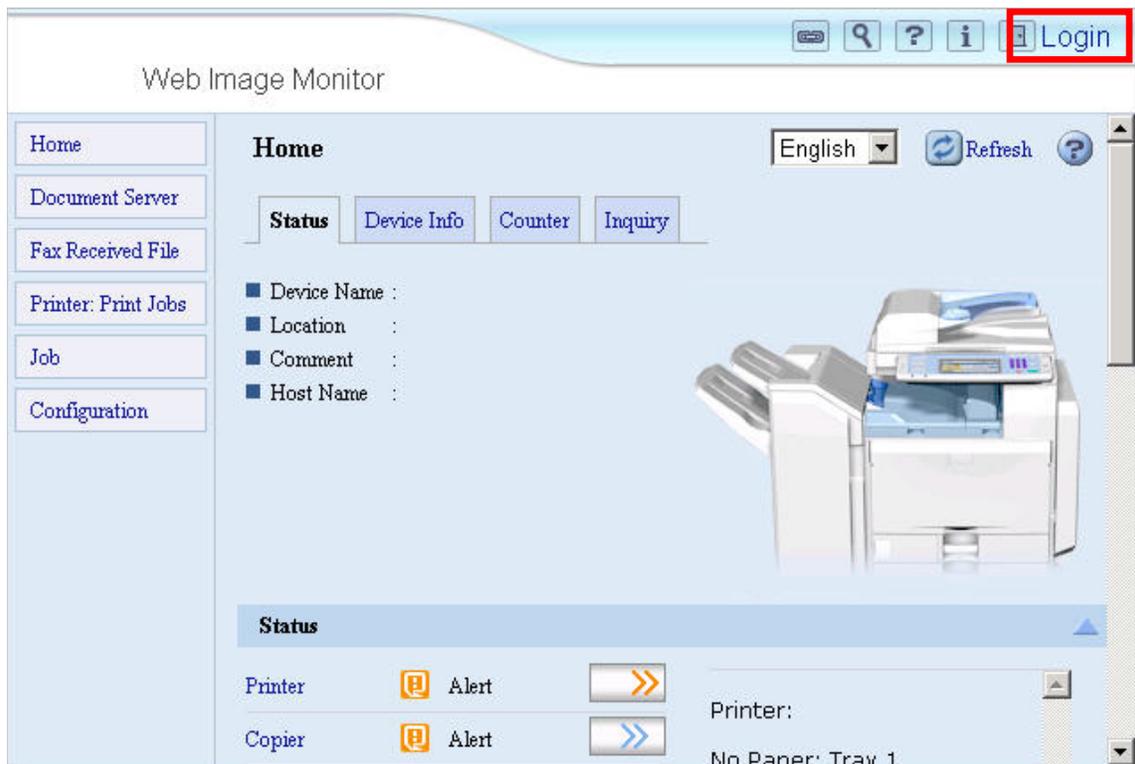


Figure 1: Web Image Monitor Main Screen

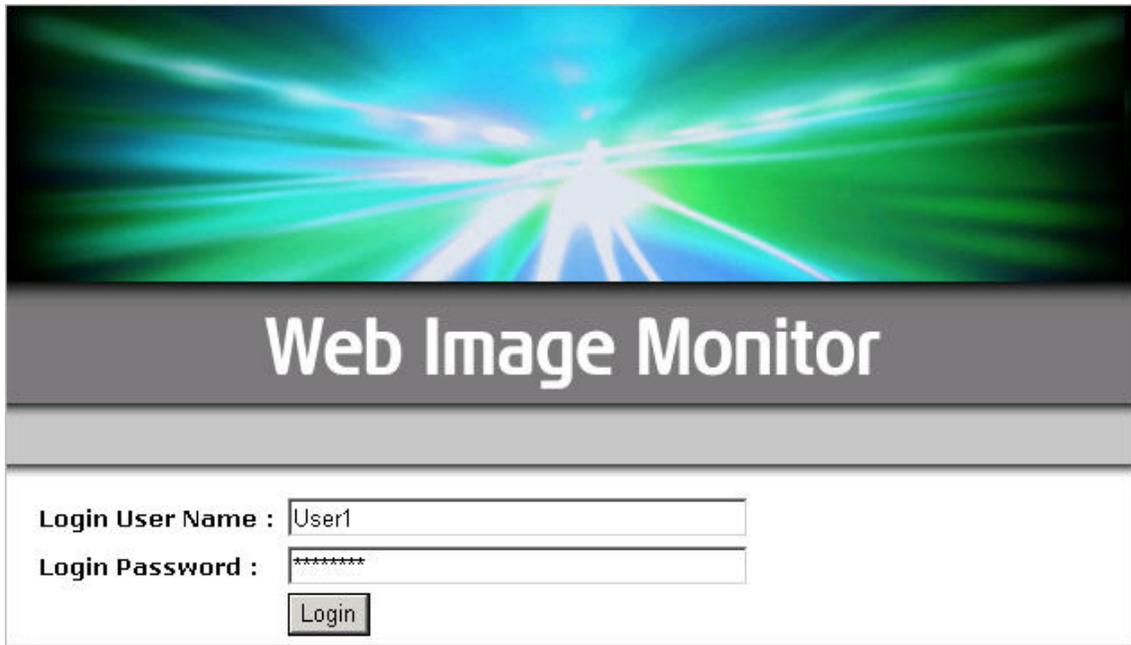


Figure 2: Web Image Monitor Login Page

1. Access to Administrator mode requires a password. Login to enter Administrator mode.
2. If the login was successful, the word **Administrator** in the upper right-hand corner. See Figure 3.
- 3.

**NOTE**

The login process may differ slightly depending on the machine in use.

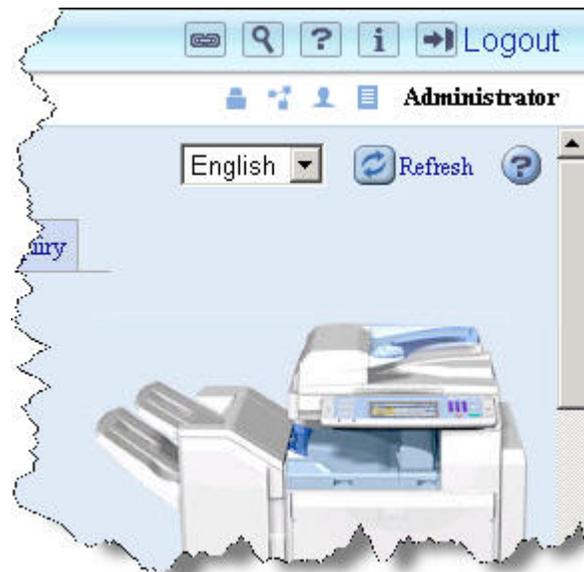


Figure 3: Administrator Main Screen

## 4.2 Network Settings via WIM

All of the necessary Network Settings can be configured via Web Image Monitor. This section covers how to access, and edit, the necessary settings.

1. Login to WIM as an Administrator (see section 4.1 – page 7 for more information).
2. From the left-hand toolbar, select **Configuration**.
3. Under the Network heading, click **IPv4**.
4. Enter Domain Name and WINS server, if applicable.
5. Enter Default Gateway and DNS servers.

**Ethernet**

- Host Name : RNPA90FE0
- DHCP :  Enable  Disable
- Domain Name :  Auto-Obtain (DHCP)  Specify
  - us.ricoh.ds
- IPv4 Address \* : 172.16.121.47 (172.16.121.47)
- Subnet Mask \* : 255.255.255.0 (255.255.255.0)
- DDNS :  Enable  Disable
- WINS :  Enable  Disable
- Primary WINS Server \* : 0.0.0.0 (0.0.0.0)
- Secondary WINS Server \* : 0.0.0.0 (0.0.0.0)
- Scope ID \* : 0

**Details**

- Default Gateway Address \* : 172.16.121.251 (172.16.121.251)
- DNS Server :  Auto-Obtain (DHCP)  Specify
  - Auto-Obtain (DHCP)
    - DNS Server1(DHCP) : 0.0.0.0
    - DNS Server2(DHCP) : 0.0.0.0
    - DNS Server3 : 172.16.4.51 The parameter sett
  - Specify
    - DNS Server1 : 172.16.4.51 The parameter sett
    - DNS Server2 : 172.16.3.51
    - DNS Server3 : 0.0.0.0
- LPR :  Enable  Disable
- RSH/RCP :  Enable  Disable
- DIPRINT :  Enable  Disable
- FTP :  Enable  Disable
- sftp :  Enable  Disable
- IPP :  Enable  Disable
- IPP Timeout : 900 seconds

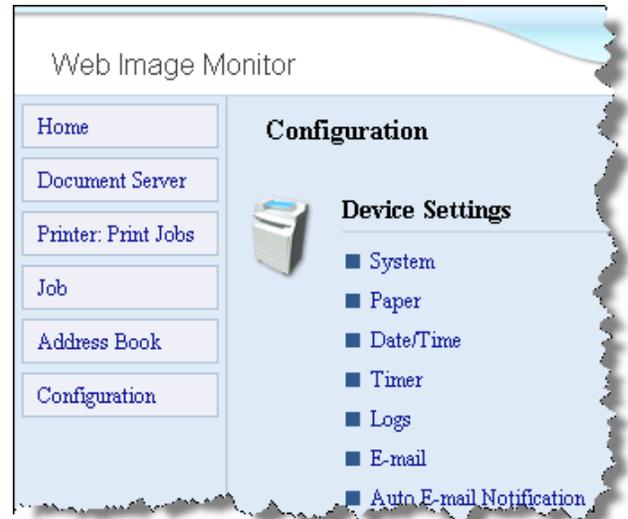
### 4.3 SMTP Authentication via WIM

After entering Administrator mode via the steps outlined in section 4.1 (page 7), the necessary SMTP Authentication settings can be entered from the E-mail settings page. Follow the steps below to access and configure the SMTP settings.

1. On the left hand toolbar, click Configuration.
2. Under the Device Settings heading, select E-mail to access the e-mail settings.

#### NOTE

The navigation may vary slightly, based on the version of WIM in use.



3. On the E-mail settings screen, enter the Administrator's E-mail address.  
**NOTE:** Be sure and use a valid e-mail address. Never use *admin* or *administrator* as the e-mail address.
4. Under the SMTP heading, enter the SMTP IP address or name.

#### NOTES:

- If DNS is not working properly, using the server name may cause e-mail delivery failure.
  - Use the PING command to find the server's IP address (e.g. ping *ricoh.com* to find its IP address).
5. If required, enable SMTP Authentication by selecting On in the SMTP Authentication field.

6. Enter the SMTP Port number. The entry range is 1 to 65535 (default is 25).
7. If enabling SMTP Authentication, enter the necessary information (E-mail address, password – up to 63 alphanumeric characters, and User Name – up to 191 alphanumeric characters).
8. Click **OK** to save the settings and return to the MFP Configuration page (Some versions of WIM may have an Apply button).

## 4.4 POP before SMTP Configuration via WIM

POP before SMTP is an authorization method used by mail servers in which a user must prove they can receive e-mail before being allowed to send e-mail. POP before SMTP is generally transparent to the users that connect to the mail server, since most users receive/check e-mail before attempting to send e-mail. The goal is to prevent unauthorized users from sending e-mails through the server. Below is the process used to set up POP before SMTP.

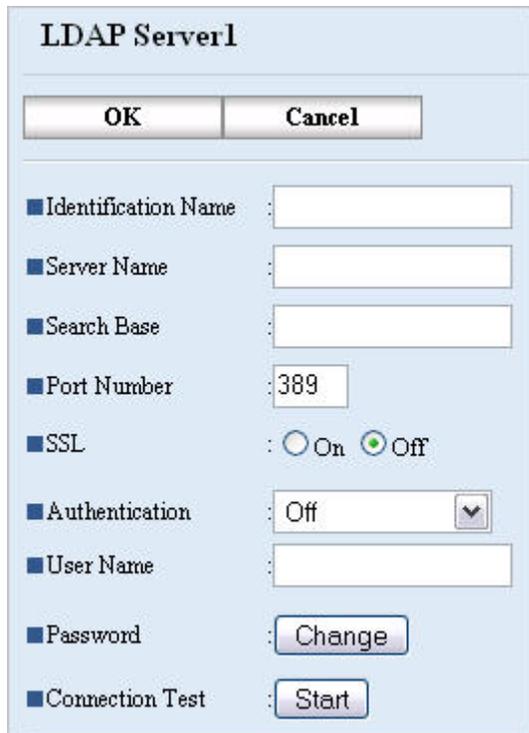
1. From the Administrator Configuration screen (page 8), select E-mail under the Device Settings heading.
2. Scroll down to POP before SMTP.
3. In the POP before SMTP field, select **ON** to enable the service.
4. Enter the necessary information in all other fields (E-mail, User Name, and password).
5. Click OK to save the settings and return to the MFP Configuration page.

## 4.5 LDAP Settings in WIM

Lightweight Directory Address Protocol (LDAP) is a protocol used to query and/or modify directory services running over TCP/IP.

1. Login to WIM as an Administrator (section 4.1 – page 7).
2. From the Configuration page, select LDAP Server (under Device Settings).
3. In the LDAP Search field, make sure **ON** is selected.
4. From the Program/Change/Delete menu, select LDAP Server 1, and click **Change**.

	LDAP Server	Identification Name
<input checked="" type="radio"/>	1	Not programmed
<input type="radio"/>	2	Not programmed
<input type="radio"/>	3	Not programmed
<input type="radio"/>	4	Not programmed
<input type="radio"/>	5	Not programmed



**LDAP Server1**

OK Cancel

■ Identification Name :

■ Server Name :

■ Search Base :

■ Port Number :

■ SSL :  On  Off

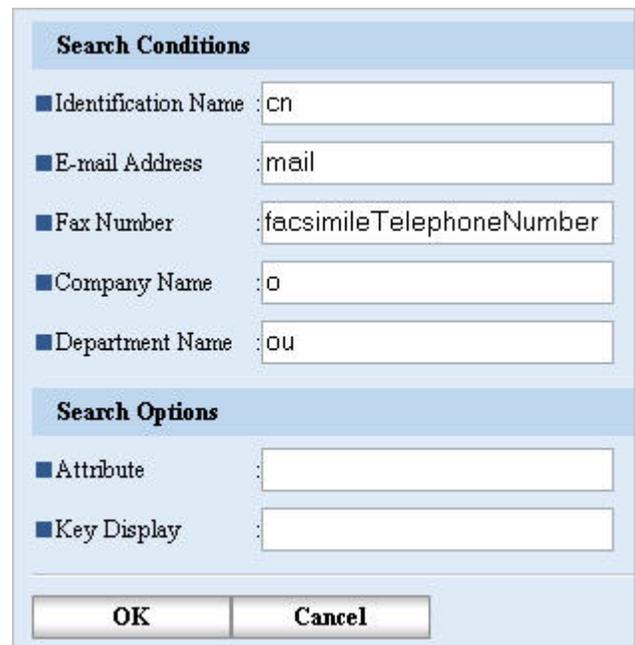
■ Authentication :  ▼

■ User Name :

■ Password :

■ Connection Test :

5. Enter the server information in the proper fields (name, search base, etc.).  
**NOTE:** To avoid potential DNS problems, enter the IP address as the server name.
6. To test the LDAP server connection, click Start next to the Connection Test field.
7. Under the Search Conditions heading, enter the desired search criteria (e.g. e-mail, department name).
8. Click **OK** to save the changes and return to the Configuration page.



**Search Conditions**

■ Identification Name :

■ E-mail Address :

■ Fax Number :

■ Company Name :

■ Department Name :

**Search Options**

■ Attribute :

■ Key Display :

OK Cancel

#### 4.5.1 Configuring LDAP on Non-Secure Devices at the MFP

To access the LDAP server settings on non-secure devices, follow this click path at the MFP operation panel: User Tools → System Settings → Key Operator Tools → Program/Change LDAP. From here all of the LDAP settings can be added and/or altered (e.g. server name, Port number, attribute, search base, etc.).

## 4.6 Address Book Settings in WIM

Using Web Image Monitor, user data can be added, deleted, and/or modified to ensure it is up to date. It also provides a faster, more efficient manner in which to update the address book than data entry from the MFP Operation Panel. This section outlines the steps to modify the MFP address book.

1. Login to Web Image Monitor as an Administrator (see section 4.1 – page 7).
2. From the left-hand toolbar, select **Address Book**.
3. The Address Book main screen will open. It displays the existing user list, including the Registration number, E-mail address, Name of each user (Figure 5.1).
4. From the Address Book main screen, click **Change** to edit an existing user or **Add User** to create a new user account.

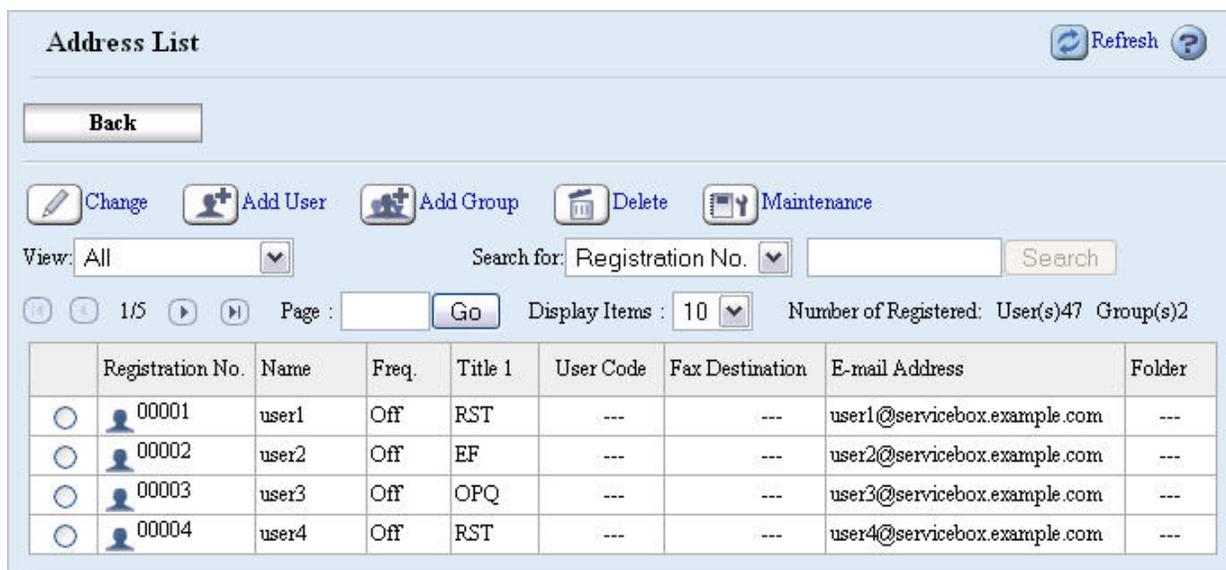
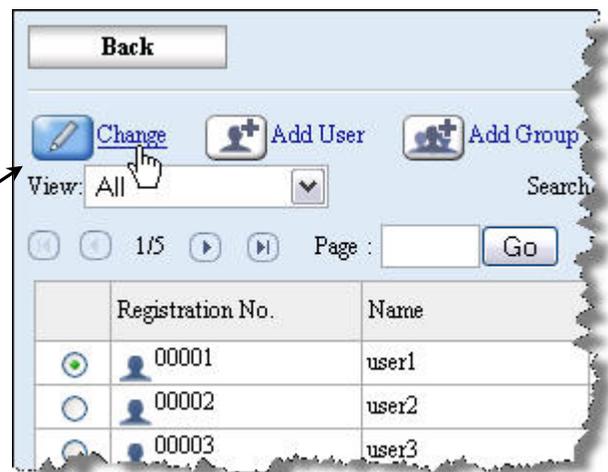


Figure 5.1: Address Book Main Screen

1. From the main address list, click on the radio button next to the name of the desired user.
2. Click the **Change** button to open the user edit screen.



3. For new users, a Registration number will be auto-populated.
4. Enter a Name and Key Display (what will appear on the MFP Op panel).  
**NOTE:** If no **Key Display** is entered, the user will not appear on the MFP operation panel.
5. From the drop down boxes, select the user's title(s).
6. If desired, select **On** in the Add to Freq. Radio button to have the user appear in the Frequent tab on the MFP.

7. Under the Authentication Information heading, specify the necessary information (User Code, SMTP, Folder, LDAP, etc). The **Specify Other Auth. below** radio must be selected to edit the Authentication information.

**NOTE**  
Authentication data (LDAP, SMTP) may have to be set in the SMTP or LDAP Authentication pages. Check with the customer for the settings in use.

**Protection**  
Protecting the Sender with a password provides added security by preventing others from sending e-mails with the user's name.  
**NOTES:**

- The Password must be numeric.
- Folder destination can also be protected with the same password.

## Additional Information

If the user has a folder setup for scanning enter that information here.

To add the user to a group, select Change and select the appropriate group.

**Folder**

■ Protocol : SMB ▾

■ Port No. : 21

■ Connection Type : NDS ▾

■ Server Name :

■ Path :

**Add to Group**

■ Details of Group :

### IMPORTANT

All FAX and E-mail information can also be added/edited from this page.

## 4.7 Address Book Settings from the Operation Panel

To enter/edit user information in the Address Book from the MFP operation panel, follow the steps below.

### 4.7.1 Operation Panel Navigation

**Secure Devices:** User Tools → System Settings → Administrator Tools

**Non-Secure Devices:** User Tools → System settings → Key Operator Tools → Address Book Management

### 4.7.2 Adding/Editing Address Book Information

Select **New Program** to add a user, or select an existing user to edit user settings. The same settings available via WIM are available at the operation panel (e.g. E-mail address, folder options, authentication options, etc.).

- User Codes
  - Maximum account number of User code is 500. Total (e-mail account and user code) account number is 2000.
- Group Management
  - If using Groups, add them in **Address Book: Program/Change/Delete Group** under Key Operator Tools
  - The group must be created before adding any users.

## 5 Setting Sender Options via the MFP Operation Panel

### 5.1 Secure Devices

By default a sender's name is required in order to use the Scan to E-mail function. The Key Operator's e-mail address can be used as the default sender by enabling Auto Specify Sender's Name.

Before enabling Auto Specify Sender's Name feature, check to ensure there is a Key Operator's E-mail address entered in the MFP. To check and/or enter one, follow this click path at the op panel: User Tools → Systems Settings → File Transfer → Administrator E-mail Address.

To enable Auto Specify Sender's Name, follow this click path: User Tools → System Settings → File Transfer → Auto Specify Sender's Name (Choose *On*).

### 5.2 Non-Secure Devices

Just as for secure devices, a sender's name is required in order to use the Scan to E-mail function. Any registered user email address shown in the operation panel can be used as a sender.

**NOTE**

To protect the senders name from being used by another person make sure to add a password for the user in the Address Book settings.

To use the key operator email address as the default sender (does not require a sender's name) first check to ensure there is an e-mail address for the Key Operator (and add an address if one does not exist).

To check/add a Key Operator E-mail address, follow this click path: User Tools → System Settings → Key Operator Tools → Key Operator Email Address.

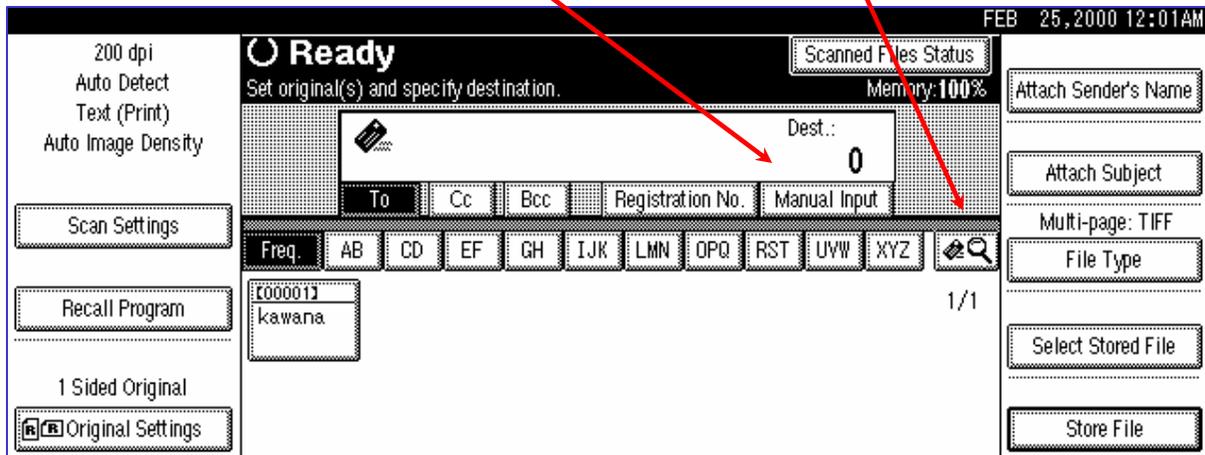
- Enter address

To enable Sender's Name Default, follow this click path: User Tools → Scanner Settings → File Transfer → Sender's Name Default (Choose *Yes*).

## 6 Scan to E-mail Operation

Now that all of the necessary settings are in place, the Scan to E-mail function should operate correctly. This section details the steps involved in using Scan to E-mail.

1. Set the document to scan in the MFP.
2. From the Scanner menu on the MFP operation panel, select the e-mail destination via Manual Input (keyed e-mail address) or Search (existing e-mail address).



3. Set any additional Scan criteria (configuration, subject.message) as needed.
4. Set Sender (unless using Auto Specify Sender's Name feature).
5. Press Start Key to complete the Scan to E-mail process.

### 6.1 Additional Scan to E-mail Settings

#### Destination Address: TO: CC: BCC

- The destination address can search from LDAP server

#### Sender Address

- When the mail cannot be delivered to the destination address, a mail notification will be sent to the senders address
- Sender address will be set in the "from" field of the email

#### Subject/Message

- The customer can attach the subject/message in the mail.

#### Notification setting

- When using this function, the client mailer software should support MDN (Message Disposition Notification:RFC2298) mode.

#### File Type settings

- The customer selects the file type using this function.

## 6.2 Scanned Files Status

To check on the status of the scanned document, press the Scanned Files Status button on the operation panel.



To keep a record of the status, users can print this list. It contains the following job information:

- Date/Time
- Destination
  - When multiple destinations were selected, the first selected destination is displayed.
- Sender
- File Name
- Status
  - Indicates whether delivery was successful or resulted in an error.

## 6.3 Additional MFP User Tool Options

Along with the options mentioned in previous sections, there are other e-mail options available from the User Tools menu of the MFP Operation Panel. When configuring the E-mail function, some of these options may be of use as well.

### User Tools: System Settings

- Interface setting
- File transfer setting
- Key Operator Tools

### User Tools: Scanner Settings

- Scan settings
- Destination List settings
- Send settings

### Programs

There are 10 different sets of scan settings available for use on the MFP. They are a combination of the settings below.

### Scan Type

- Text(Print)/Text(OCR)/Text Photo/Photo/Gray Scale – B&W MFPs
- Text(Full Color)/Photo(Full Color) – Color MFPs

### Resolution

- 100dpi/200dpi/300dpi/400dpi/600dpi

### Image Density

- Auto or select from a graduation of 7 steps.

### Scan Size

- Auto Detect/Selected Paper size/Custom Size

## 7 Scan to E-mail in Windows Server 2000 or 2003

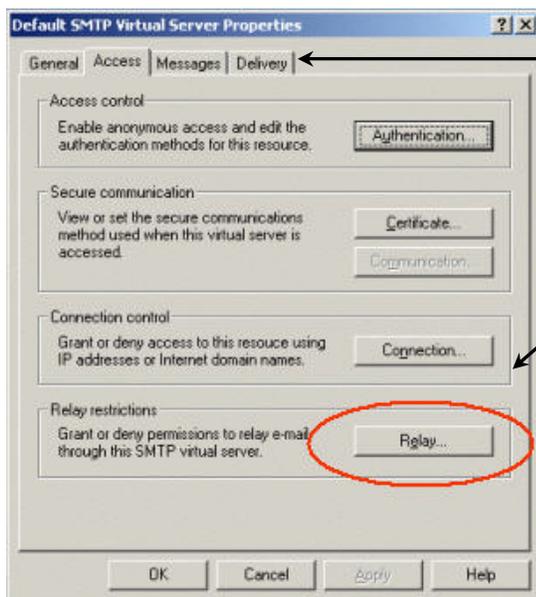
There is a common problem that occurs when installing an MFP or LAN-FAX for Scan to E-mail on a Windows server environment. Users state that they can send emails internally within their corporate email system, but they are unable to send emails from the MFP to outside email addresses.

The reason is that in a Windows 2000 and 2003 Sever environment, the network administrator has to allow SMTP relay for each device on their network that will be used for Scan to Email.

Follow the process below to set up the SMTP relay for the MFP, so Scan to E-mail will work for external e-mails.

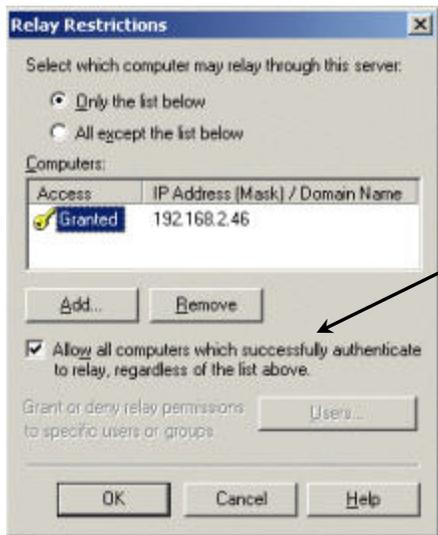
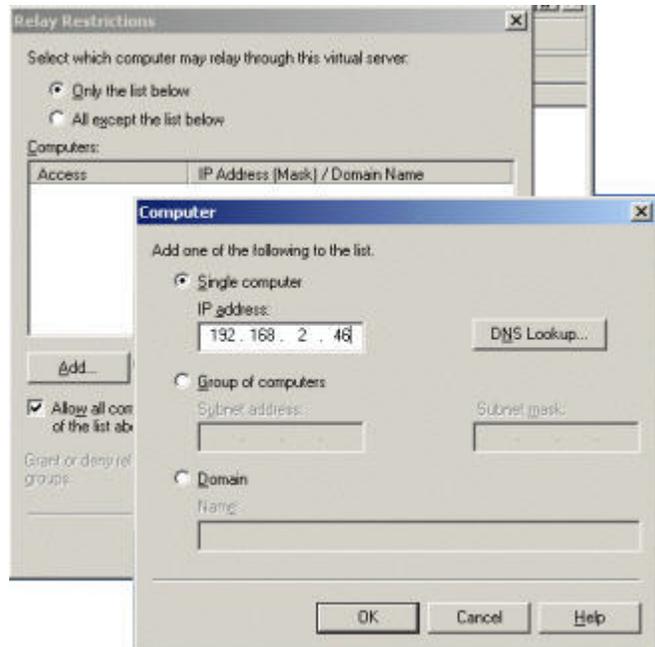
### 7.1 Enabling SMTP Relay for Windows Server with MS Exchange

1. From the Windows Start menu, select: Programs → Microsoft Exchange → System Manager.
2. When the System Manager opens, access the SMTP settings by following this click path: Servers → (*Server Name*) → Protocols → SMTP.
3. Right click on the default SMTP server, and select **Properties**.



4. From the Properties menu, select the **Access** tab.
5. Under the section labeled **Relay Restrictions**, click the **Relay** button.

6. From the Relay Restrictions pop-up, click the **Only the List below radio** button. This allows only the MFP(s) listed to access the SMTP relay.
7. Click **Add**.
8. On the Computer pop-up, enter MFP IP Address.
9. Click **OK** to close the pop-up and add the MFP to the SMTP relay access list.

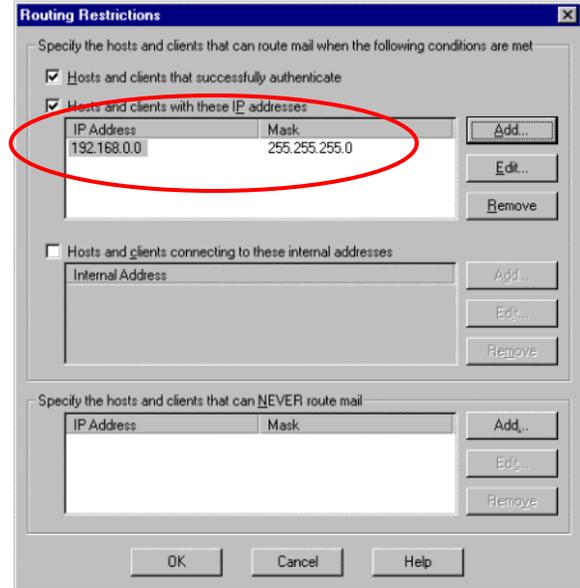
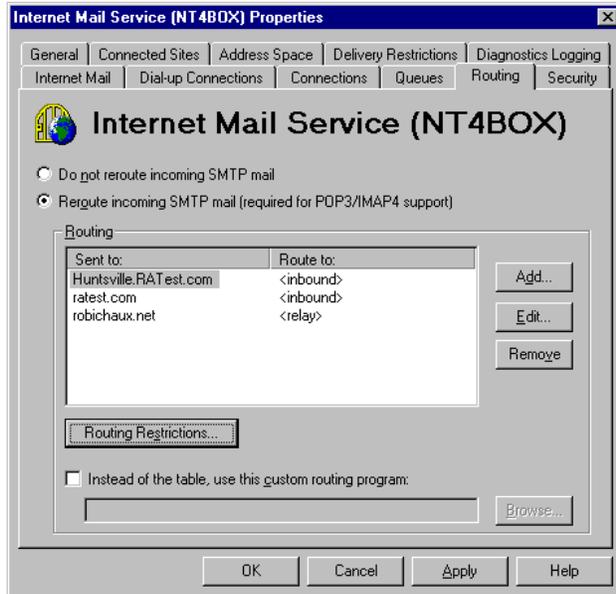


10. On the Relay Restrictions pop-up, be sure to check **Allow all computers that successfully authenticate to relay** before selecting **OK** to save the settings.

## 7.2 Device Relays through Exchange 5.5 on Windows 2000 Server

The steps below detail the process for adding the SMTP relay for the MFP in Exchange 5.5.

1. In the IMS Exchange Manger, select the **Reroute incoming SMTP mail** radio button to enable SMTP routing.
2. Click **Add** to enter the MFP address information.
3. Enter the IP address of the MFP and a Mask of 255.255.255.255, and click **OK** to save the information.



## 8 Scan to E-mail Failure using Windows Authentication

If Authentication fails, the MFP operation panel will display a message that reads: **Authentication with Destination has failed** (Figure 8.1). This means that the user does not have scanning rights on the MFP. This error also appears if the User is not Authenticating with the Windows server.

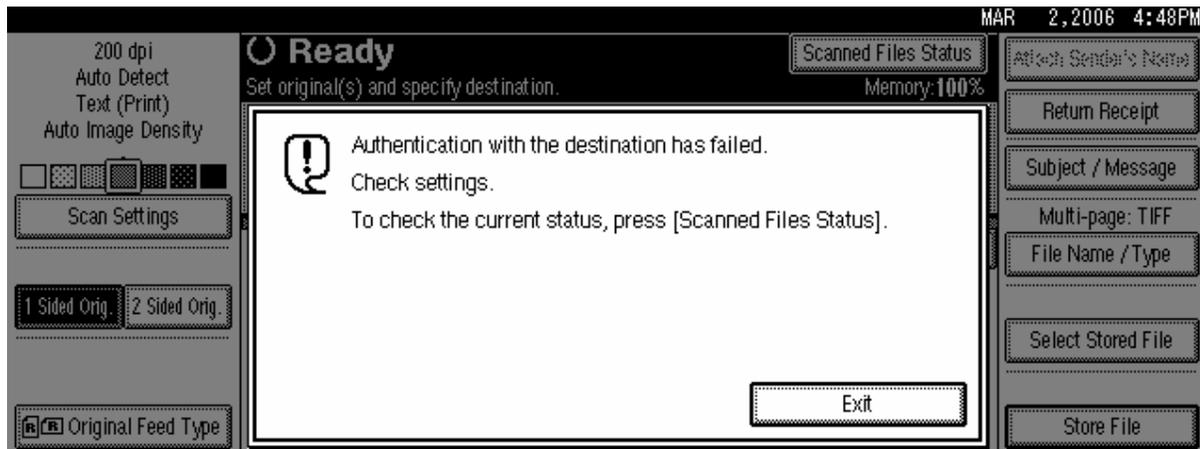


Figure 8.1: MFP Operation Panel

### 8.1 Tracing the Authentication Error

In order to fix the Authentication issue, it helps to use a Network Capture (e.g. Windshark) to trace the communication stream. The Network Capture process will show the exact Authentication failure point.

Time	Source	Destination	Protocol	Info
000338	192.168.1.104	192.168.1.103	TCP	65418 > smtp [ACK] Seq=1 Ack=1 Win=17520 Len=0 TSV=239!
000363	192.168.1.103	192.168.1.104	TCP	smtp > 65418 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MS
.644227	192.168.1.104	192.168.1.103	TCP	65418 > smtp [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
004605	192.168.1.103	192.168.1.104	SMTP	Response: 221 2.0.0 ricoh13.fsod.com Service closing tr
001455	192.168.1.104	192.168.1.103	SMTP	Message Body
029510	192.168.1.103	192.168.1.104	SMTP	Response: 250 2.6.0 <20060302145250EB.DCSML-S000130000

```

334 VxNTCm3nbw0G
c3RIMQ==
334 UGFzc3dvcmQ6
cGFzc3dvcmQ=
250 2.7.0 Authentication successful.
MAIL FROM:<stu1@fsod.com>
250 2.1.0 stu1@fsod.com...Sender OK
RCPT TO:<stu1@fsod.com>
250 2.1.5 stu1@fsod.com
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: "student1" <stu1@fsod.com>
Subject:
To: "student1" <stu1@fsod.com>
Date: Thu, 2 Mar 2006 14:52:50 -0500
Message-Id: <20060302145250EB.DCSML-S000130000.0000
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="DC_BOUND_PRE_<1141329170.00007493363e">

```

- From the Network Capture screen, right click SMTP Response to follow the initial SMTP TCP stream.
- In this case, User Authentication succeeds at the login screen, so it has failed someplace else.

Filter: (ip.addr eq 192.168.1.103 and ip.addr eq 192.168.1.104) a

Time	Source	Destination	Protocol	Info
588 0.000086	192.168.1.104	192.168.1.103	SMTP	Message Body
589 0.000245	192.168.1.104	192.168.1.103	SMTP	Message Body
590 0.000015	192.168.1.104	192.168.1.103	SMTP	Message Body
591 0.000235	192.168.1.103	192.168.1.104	TCP	[TCP Dup ACK 587#1] smtp > 65485 [ACK] Seq=610 Ack=7
592 0.002232	192.168.1.103	192.168.1.104	TCP	smtp > 65485 [ACK] Seq=610 Ack=77207 Win=17520 Len=0
593 0.000437	192.168.1.104	192.168.1.103	SMTP	Message Body
594 0.142033	192.168.1.103	192.168.1.104	SMTP	Response: 454 5.7.3 Client does not have permission
595 0.000715	192.168.1.104	192.168.1.103	TCP	65485 > smtp [ACK] Seq=78175 Ack=677 Win=17453 Len=0
596 0.000237	192.168.1.104	192.168.1.103	SMTP	Message Body
597 0.000005	192.168.1.104	192.168.1.103	TCP	65485 > smtp [FIN, ACK] Seq=78181 Ack=677 Win=17520

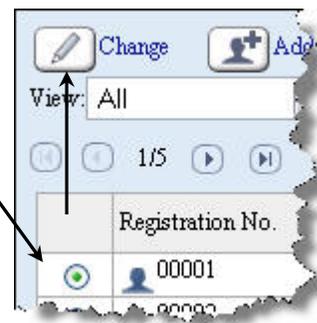
XpoAaJy0ANB4aQKg6FYANF6aAGi ccGkAoGxwADRemgBonLQAUDYrABovTQA0TloAKJsVAI2X  
 JgAaJy0A1M0KgMZLEwCNEY4NAJTNCoCywQHCOGkBoPHSBEDZrAAomxUAZbMCoGxWAJTNCocY  
 wQFNisAymYFQNmSAAiAAAiAAAiAAAiA  
 --DC\_BOUND\_PRE\_<1141321468.00007493363e>--  
 .  
 454 5.7.3 Client does not have permission to Send As this sender.  
 QUIT  
 221 2.0.0 ricoh13.tsod.com Service closing transmission channel

- Once the TCP stream opens, navigate to the end of the data transmission.
- At the end of the data, a note should appear stating: *Client does not have permission to Send As this sender.*

## 8.2 Authentication Error Resolution

The Authentication Error described in section 8.1 can be resolved via Web Image Monitor. To begin, login to WIM as an Administrator (for more information, see section 4.1 – page 7).

- After logging in as an Administrator, select **Address Book** from the left toolbar of WIM.
- From the Address Book main screen, click the radio button next to the User with Authentication problems and click **Change**.
- Under the Authentication Information heading, select **Specify Other Auth. Info below**.
- Enter a Login User Name.
- Next to the Login Password field, click **Change** to add, and confirm, the User's password.
- Click **OK** to save the changes.



**Authentication Information**

User Code :   
 SMTP Authentication :  Specify Other Auth. Info below:  Do not Specify  
 Login User Name :   
 Login Password :

## 9 File Size Limits

It is common for Exchange servers to have set size limits for files. If the e-mail sent from the MFP via Scan to E-mail exceeds this limit, an error screen similar to the one below (Figure 9.1) will appear on the MFP operation panel.

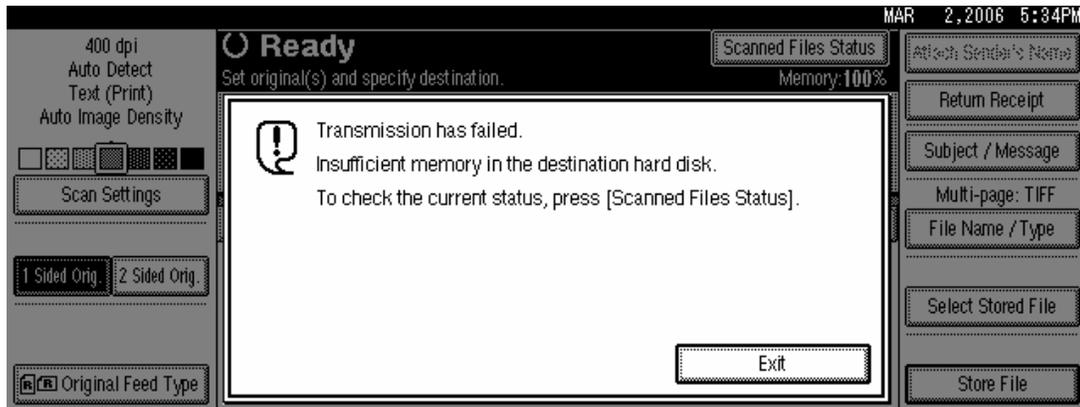
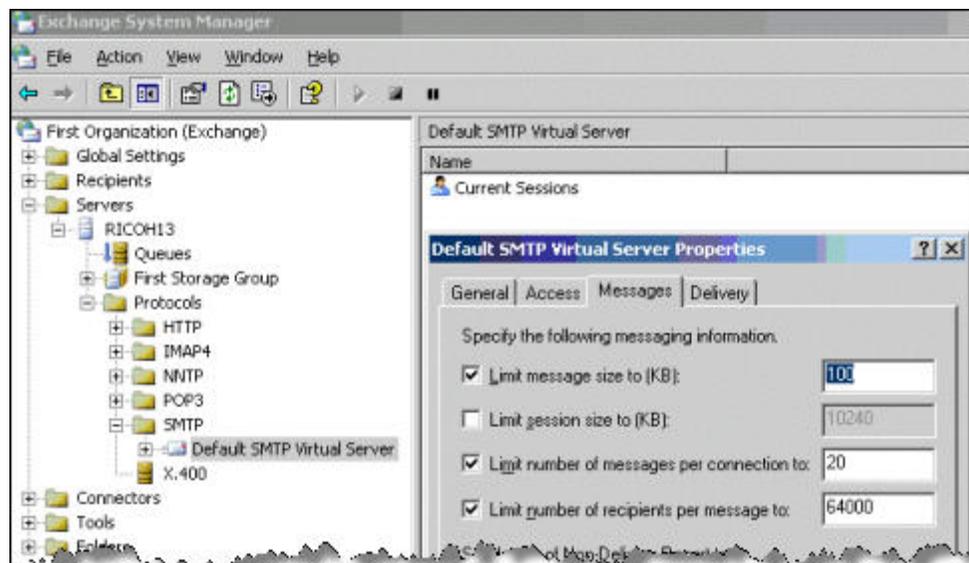


Figure 9.1: MFP Operation Panel Error

### 9.1 Accessing the File Size Limits

This section details the steps to follow when searching for the Exchange Server e-mail file size limits.

1. From the Windows Start menu, navigate to the Exchange System Manager via this path: Programs → Microsoft Exchange → System Manager.
2. From the left-hand navigation window of the System Manager, follow this click path: Servers → Mail Servers → SMTP → Default SMTP Virtual Server.



3. In the Server Properties pop-up, click on the **Messages** tab to view the Server file size limits (e.g. in the example above, the limit is 100KB).

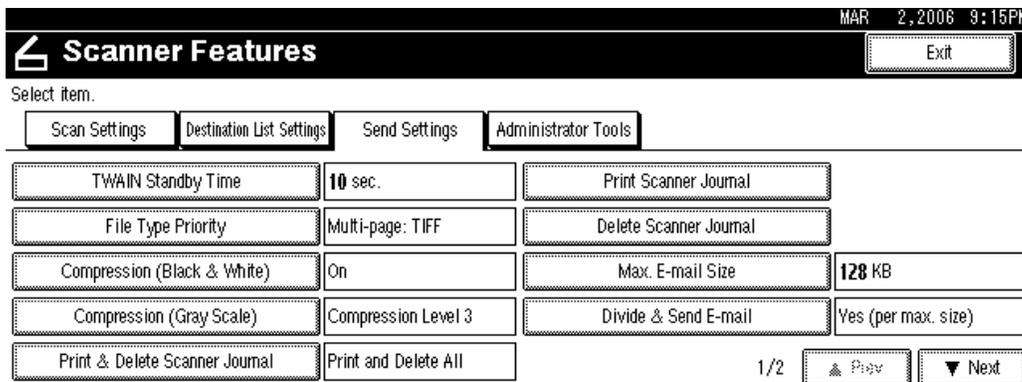
## 9.2 Setting File Size Limits on the MFP

In addition to server size limits, the file size limits when using the Scan to E-mail functions can be set at the MFP. This section details how to access, and alter, the MFP file size limits.

1. To access the size limit settings from the MFP operation panel, select: User Tools → Scanner Features → Send Settings.
2. From this tab the maximum E-mail size can be changed (Max. E-mail Size), and Divide & Send E-mail can be enabled.

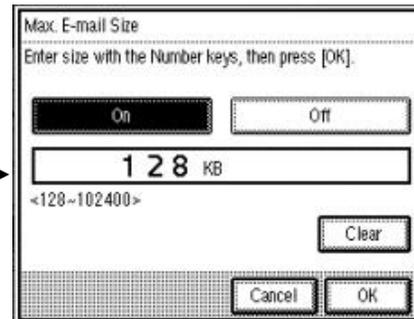
### DEFINITION

Divide & Send E-mail will break up any e-mail that exceeds file limits into smaller sections and e-mail the sections. These sections are then automatically recombined at the destination.



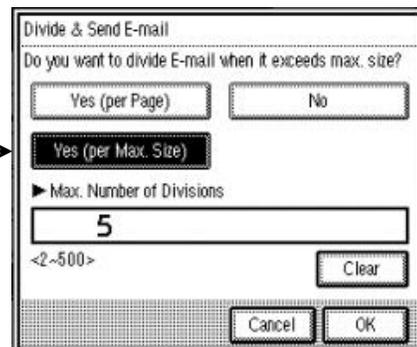
#### Max E-mail Size

Set Max E-Mail Size just under the max file limit set on the Exchange server



#### Divide & Send E-mail

Select **Yes (per Max. Size)** and the number of divisions required to send documents that are scanned to email.





### 9.3 Decode Shell Extension

Install the Decode Shell Extension from the Funduc website at: <http://www.funduc.com/otsoft.htm#decodeshellextension>. After completing the install, the computer will have to be rebooted to use the program. Follow the steps below to use Decode Shell Extension to re-create an e-mail sent via the Divide & Send method.

1. Open the multipart emails, and save the entire message(s) as a text (.txt) file.
  1. In Lotus Notes: Use the File → Export command.
  2. Other e-mail Clients (e.g. Outlook): Use File → Save command.
2. Once saved, all of the e-mail text files must be combined into one file.
3. Use the File/Select All command and then copy and paste the messages in order.
4. Right click the file created and select **Decode** (Figure 9.2).
5. Decode Shell Extension will create a PDF file of the complete attachment (Figure 9.3).

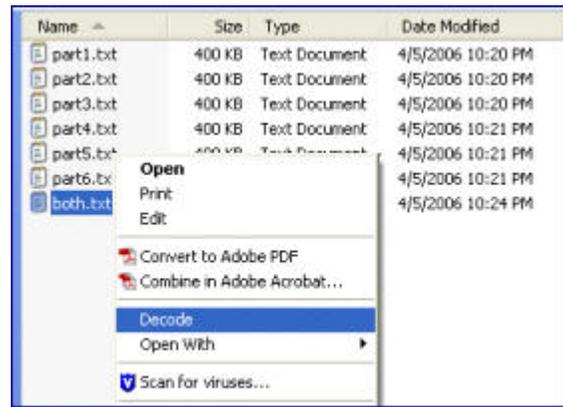


Figure 9.2: Decode File Selection

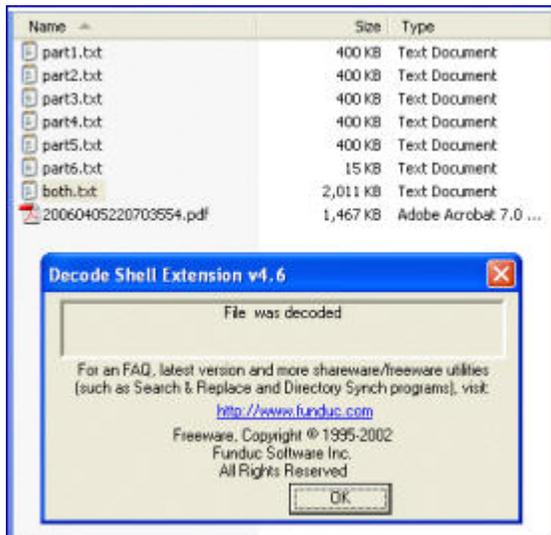
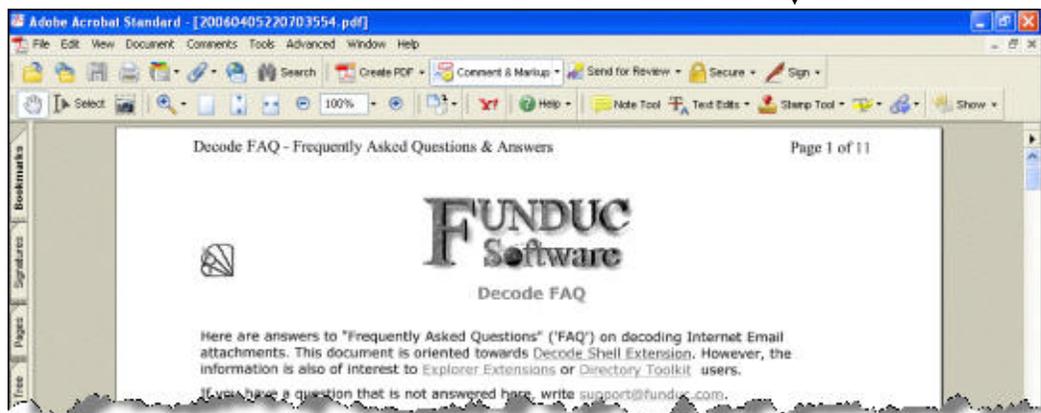


Figure 9.3: PDF File Creation

6. Once the pdf has been created, the pop-up shown in Figure 9.3 (at left) will appear, confirming the file decode.
7. Click OK to close the pop-up.
8. Open the pdf to ensure the scanned document is accurate and complete.



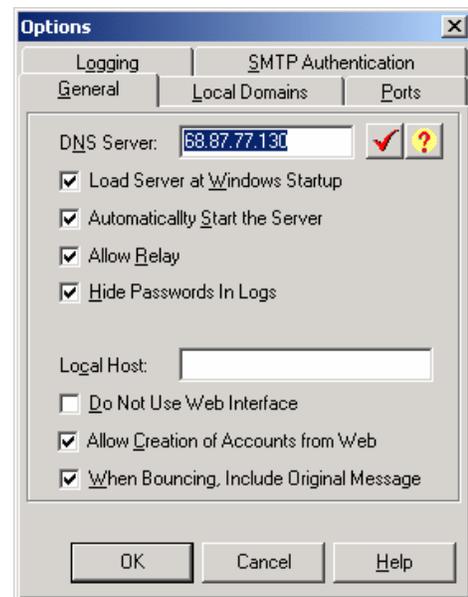
## 10 ArGoSoft for E-mail Relay

When using an Internet Service Provider outside the corporate firewall to relay email, it may be necessary to the ISP customer support staff to allow the MFP connection. In some cases, ArGoSoft, installed on a computer that is always powered on, can be used to relay emails through the ISP's DNS server.

ArGoSoft is a free application, available for download at the URL below:  
<http://argosoft.com/RootPages/Download.aspx>.

After downloading, and installing, the application, use the process below to use ArGoSoft.

1. Once installed, start the ArGoSoft server, right click on the icon in your startup area and select Options.
2. From the General tab, click the check mark “✓” button to view available DNS servers.
3. In the example at right, the DNS server is one of Comcast's servers.
4. On the pop-up that opens, select **Yes** to confirm the use of this DNS server.



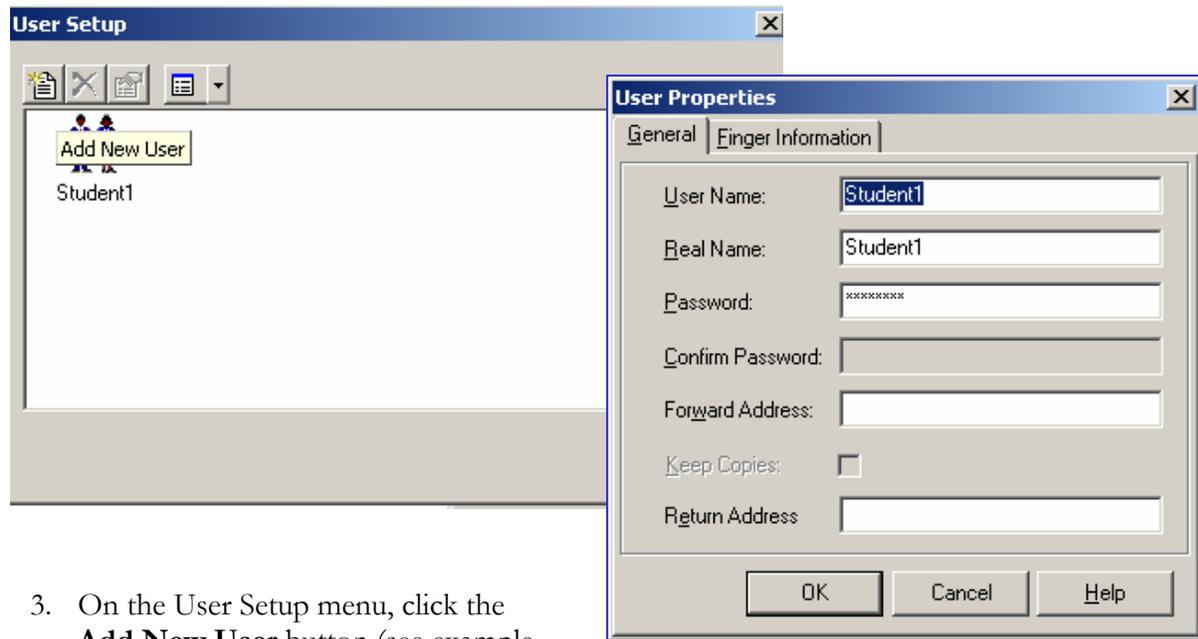
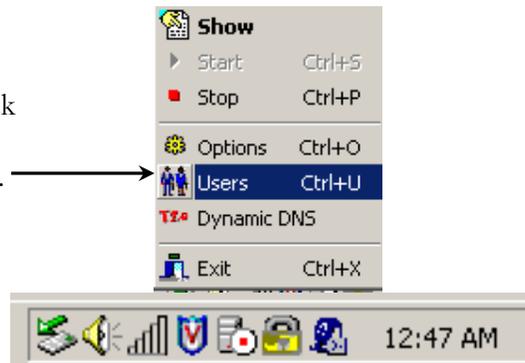
5. On the Options menu, select the **Local Domains** tab.
6. Input the Domain name (*ricoh in the example at right*), and click **Add**.
7. Click **OK** to save the changes and close the Options menu.



## 10.1 Creating ArGoSoft User Profiles

This section details the creation of User Profiles in the ArGoSoft application.

1. On the Windows System Tray, right-click on the ArGoSoft icon.
2. From the right-click menu, select **Users**.

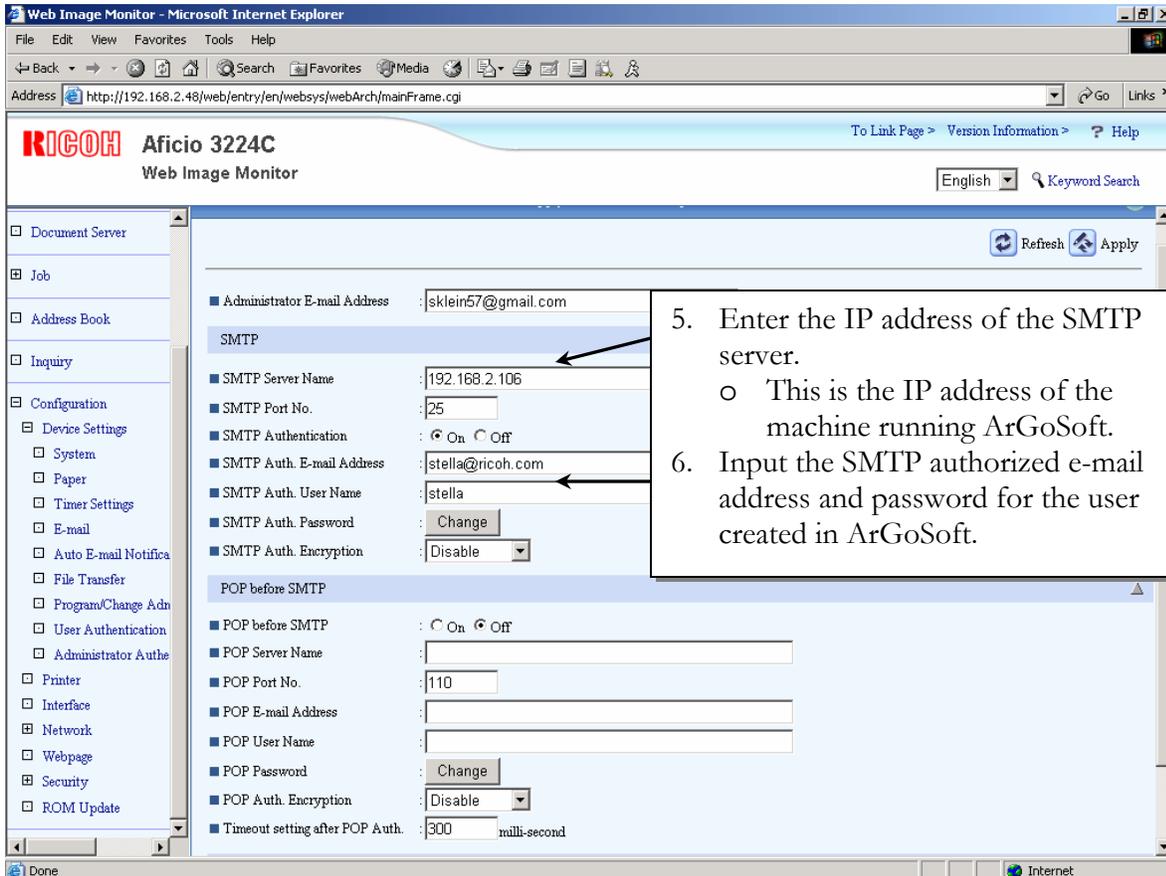


3. On the User Setup menu, click the **Add New User** button (see example above).
4. In the User Properties pop-up, enter the User Name and Password.
5. Click **OK** to add the user and save the settings.

## 10.2 ArGoSoft Setup in Web Image Monitor

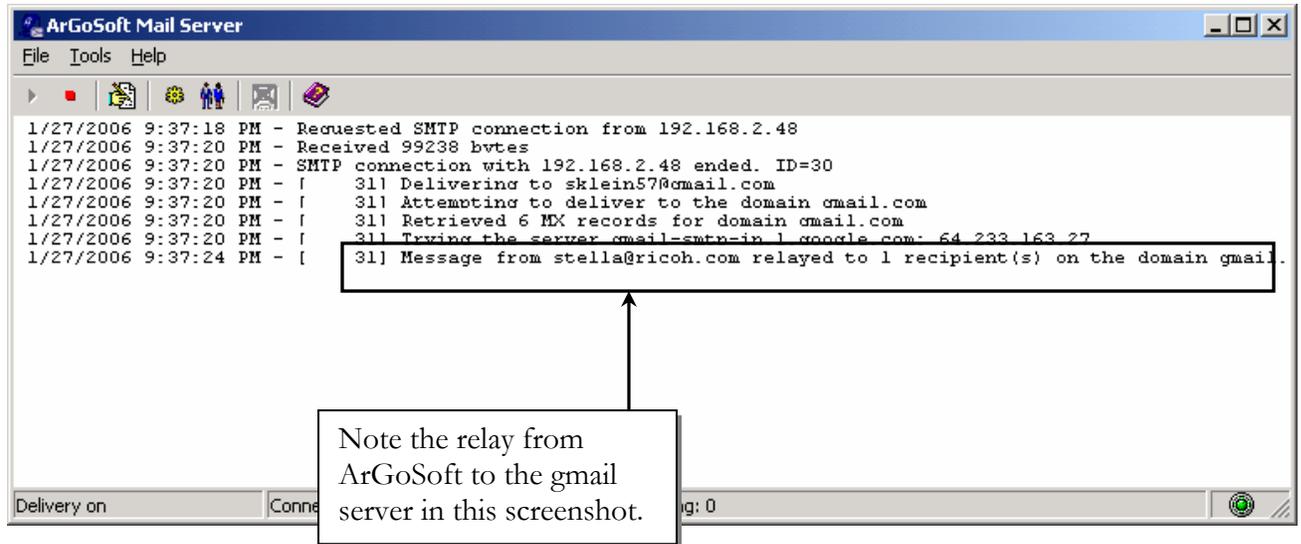
In order to finalize the ArGoSoft setup, the computer settings must be added via WIM.

1. Start by accessing the MFP's WIM page by entering the IP address into a web browser.
2. Following that, login as an administrator (for more information, see Section 4.1 – page 7).
3. From the left-hand toolbar, select **Configuration**.
4. On the Configuration page, click **E-mail**.



## 10.3 ArGoSoft Relay Monitor

Once all of the settings have been entered, the ArGoSoft application can monitor all of the mail communications. In the Windows System Tray, right-click the ArGoSoft icon and select **Show** to view the communication data.



## 10.4 ArGoSoft Limitations

There are some limitations when using the ArGoSoft application, which may impair, or prevent, its use.

- Many servers do not allow relays using this method.
  - If that is the case, some email addresses will not be accessible.
  - A failure to send entry will be in the ArGoSoft log.
  - For most environments, upgrading to ArGoSoft Pro (\$130.00) solves this problem.
- It is always best for the customer to contact their internet provider to setup email service for the MFP.

## 11 Summary

The material covered in this White Paper should help answer many questions concerning Scan to E-mail, such as the MFP setup process, server configuration, and additional tools to aid in the setup and use of Scan to E-mail.

This White Paper contains all of the setup information needed to enable, and use, the Scan to E-mail function. It applies only to the machines listed in the Model Cross reference (page 5).