



**AirZip® FileSECURE™ 4.0**  
**Secure Scanning**  
**With**  
**FileSECURE™ ScanSECURE™**

**Using Sharp's AR-M237/M277, AR-M355/M455 or  
AR-M550/M620/M700 Series Digital IMAGER™ MFPs**  
**Installation and Configuration Manual**

August 2005



(c) 2002-2005 AirZip, Inc. All rights reserved. AirZip, the AirZip logo, FileSECURE AutoSECURE, emailSECURE and ScanSECURE are either registered trademarks or trademarks of AirZip, Inc. in the USA and other countries.

Contact your Authorized AirZip Reseller to report problems and/or provide feedback.

Additional help resources or updates may be available by emailing [support@airzip.com](mailto:support@airzip.com)

AirZip Inc. reserves the right to make changes to this document and to the product described herein without notice. The software described in this manual is furnished under the terms and conditions of the AirZip Software License Agreement and may be used or copied only in accordance with the terms of the agreement.

For information about your legal rights concerning the use of the FileSECURE, please refer to the AirZip Software License agreement.

Outside In ® is a registered trademark of Stellant Chicago Inc. © 1992-2003 Stellant Chicago Inc. All Rights Reserved. Windows and Windows NT are registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Bzip2 and its associated library libbzip2 are Copyright (C) 1996-2000 Julian R Seward. All rights reserved.

JPEG2000 imaging software owned and copyrighted by Pegasus Imaging Corporation, Tampa, FL. All Rights Reserved.

Color Capture Driver are Copyright © 1995-2002 Black Ice, Inc. All Rights Reserved

Windows and Windows NT are registered trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Revision 4.0

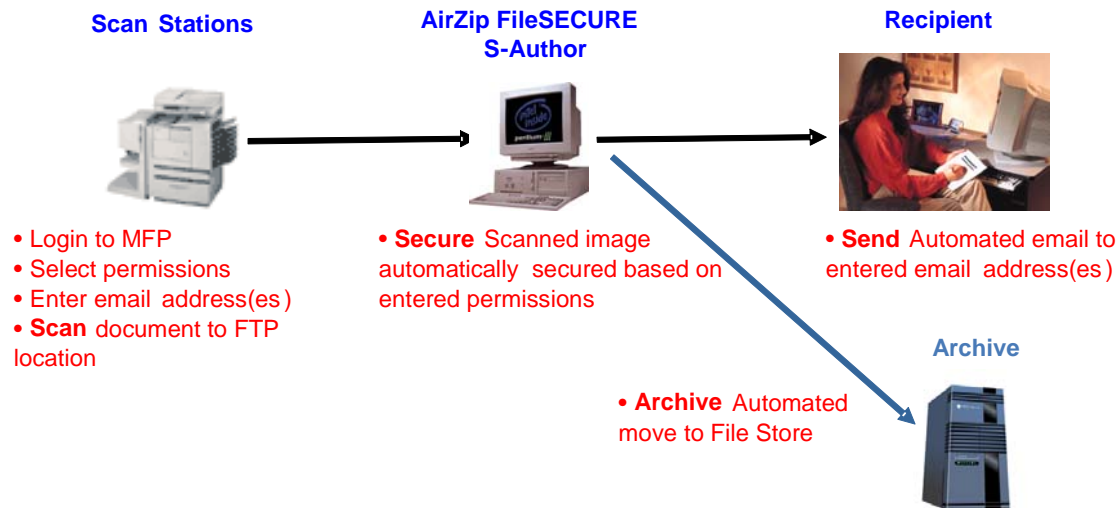
# Table of Contents

<b>1</b>	<b>Secure Scanning With FileSECURE</b> .....	<b>1</b>
<b>2</b>	<b>Secure Scanning Options</b> .....	<b>2</b>
2.1.1	<i>Multiple Destination Selection</i> .....	2
2.1.2	<i>Category Selection using Metadata</i> .....	2
2.1.3	<i>Folder Selection using Metadata</i> .....	2
2.1.4	<i>Email Recipient Selection using Metadata</i> .....	3
2.1.5	<i>Permissions Selection using Metadata</i> .....	3
2.1.6	<i>Sender Selection using Metadata</i> .....	3
<b>3</b>	<b>Secure Scanning Applications</b> .....	<b>4</b>
3.1	Secure Scanning to pre-configured email recipients.....	4
3.2	Secure Scanning to Archive with a user-selected security category.....	4
3.3	Secure Scanning to fixed recipient list with a user-selected security category .....	4
3.4	Secure Scanning to selected FileSECURE Users.....	5
3.5	Secure Scanning to arbitrary email recipients with user-selected Security Category or permissions.....	5
<b>4</b>	<b>Configuration</b> .....	<b>7</b>
4.1	Prerequisites .....	7
<b>5</b>	<b>Planning and Configuration</b> .....	<b>8</b>
5.1	Plan your Secure Scanning implementation.....	8
5.2	Gather necessary prerequisites.....	9
5.3	Metadata enable your Sharp Digital IMAGER .....	9
5.4	Configure your Secure Scanning PC.....	9
5.5	Configure the ScanSECURE operation for each Target Destination Folder and Subfolder. ....	10
5.6	Install Sharpdesk and the Network Scanning Tool from the Sharpdesk Software 3.1 CD on the ScanSECURE PC.....	13
5.7	Use the Network Scanning Tool to enable your ScanSECURE PC as a Scanner Destination	13
5.8	Configure the Sharp Digital IMAGER for the Metadata Delivery.....	17
5.9	Validate the operation from the Digital IMAGER .....	20
<b>6</b>	<b>ScanSECURE Processing – More Details</b> .....	<b>23</b>
6.1	Configuration Options .....	23
6.2	ScanSECURE Metadata Processing.....	23
6.3	ScanSECURE Errors.....	24
6.4	Sample Metadata.....	26
6.4.1	File Names .....	27

# 1 Secure Scanning With FileSECURE

Secure Scanning with AirZip FileSECURE is the capability to configure Sharp's AR-M237/M277, AR-M355/M455 or AR-M550/M620/M700 Series Digital IMAGERs and AirZip FileSECURE to automatically secure and distribute electronic documents as they are scanned.

Secure Scanning allows the Digital IMAGER operator to specify security permissions, archive folders, and even email addresses to which the document is to be sent, directly from the Digital IMAGER touchpad.



Secure Scanning with AirZip FileSECURE supports several different modes:

1. Secure Scanning to pre-configured email recipients
2. Secure Scanning to an Archive folder
3. Secure Scanning to a fixed email recipient list
4. Secure Scanning to selected FileSECURE Users
5. Secure Scanning to arbitrary email recipients where FileSECURE User accounts are automatically created.

Metadata entry is supported on Sharp's AR-M237/M277, AR-M355/M455 or AR-M550/M620/M700 series Digital IMAGER MFPs. This allows data describing the image file to be entered at the Digital IMAGER front panel and sent along with the image as an XML file to FTP destinations.

This manual describes:

1. Secure Scanning options,
2. Secure Scanning applications
3. how to configure a FileSECURE workstation to facilitate Secure Scanning
4. how to configure Sharp Digital IMAGER machines for Secure Scanning

Refer also to the following references:

- Sharp Metadata and NST Installation Guide for Sharp's AR-M237, AR-M277, AR-M355, AR-M455, AR-M550, AR-M620 and AR-M700 Digital IMAGER MFPs.

## 2 Secure Scanning Options

Sharp's AR-M237, AR-M277, AR-M355, AR-M455, AR-M550, AR-M620, and AR-M700 series Digital IMAGER's allows users to select alternative Destinations to which the Digital IMAGER transfers the scan documents and optionally enter data describing the image file at the Digital IMAGER front panel, which is sent along with the image as an XML file to FTP destinations. This data is referred to as Metadata. Secure Scanning with FileSECURE uses the Destination and Metadata to automatically secure and distribute the scanned version of document. .

FileSECURE provides the following capabilities for processing scanned documents and interpreting metadata generated by the Sharp Digital IMAGER:

1. Multiple Destination Selection
2. Category Selection using Metadata
3. Folder Selection using Metadata
4. Email Addresses Selection using Metadata
5. Permissions Selection using Metadata
6. Sender Selection using Metadata

### 2.1.1 Multiple Destination Selection

FileSECURE may be arranged to allow the Digital IMAGER operator to select multiple destinations for secure scanning, where each Destination has separate securing and distribution policies. FileSECURE ScanSECURE settings, operator entered Metadata, or the combination of both determines the Security Category applied, where the secured document is archived, and to whom the document is distributed.

### 2.1.2 Category Selection using Metadata

The Security **Category** Selection allows Sharp Digital IMAGER operator to select the FileSECURE Security Category to be used when FileSECURE secures specific files, directly from the Digital IMAGER touch screen. FileSECURE Security Categories define specific permissions for users or groups of users for particular types of files. The FileSECURE System Manager configures Security Categories to make it easy for users to secure files in a manner that meets an organization's security policies. Examples of security Categories are Confidential, For Your Eyes Only, Health Records, Financial Records, etc.

The values for the Category selected at the Digital IMAGER must match exactly a FileSECURE Security Category that you have configured. If a Category matching that specified in the metadata does not exist, ScanSECURE will secure the file with a default Security Category and report the mismatch as an error.

### 2.1.3 Folder Selection using Metadata

The **Folder** Selection allows a Sharp Digital IMAGER user to select from a list of ScanSECURE processing options directly from the Digital IMAGER touch screen. The selection corresponds to a pre-configured ScanSECURE folder on the ScanSECURE Server. By simply selecting a Folder, the operator determines Security Category, Email processing options, and move file (archive) settings.

For example, an organization may have several different archive folders or email lists to which documents are routinely sent. The user simply selects from a list of folders which may be named *Financial Records*, *Medical Records*, *Loan Applications*, or other meaningful name relating to the typical types of documents being scanned. By making this simple selection, the user defines indirectly the Security Category for securing the file, email recipients to whom the file is to be sent, and possibly an archive folder to which the secured file is to be moved after securing and emailing. This is analogous to selecting from a set of preconfigured securing scripts. **Folder Selection may be used independently or in conjunction with Category Selection.**

The values for the Folder selected at the Digital IMAGER must match the exact name of a subfolder in the main ScanSECURE Folder where the Digital IMAGER sends the file and its metadata. Typically the subfolder will be configured for ScanSECURE. If a folder matching that specified in the metadata does not exist, ScanSECURE will secure the file with a default Security Category and report the mismatch as an error.

### **2.1.4 Email Recipient Selection using Metadata**


The **Email Recipient** selection capability enables Sharp Digital IMAGER user to select or enter email recipients to which the file once secured is to be sent. Secure Scanning may be configured to automatically configure a new FileSECURE Reader account to enable secured files to be sent to any potential email recipient.

### **2.1.5 Permissions Selection using Metadata**

If user-select Email recipients are provided in the metadata, the **Permissions** selection capability allows users of Sharp Digital IMAGERs to also select specific custom permissions to be assigned when the file is secured.

The Permissions selection allows the users to select one of the following permissions sets to be assigned to documents that they are emailing to specific users:

**View, View/Print, View/Print/Copy, View/Copy, View/Print/Copy/Control.**

 **Note:** If selected, these permissions override those contained in any user selected or default Security Category. The file will be secured with the user selected Security Category or the default Security Category specified in the Scan Secure Folder for the purposes of ‘categorizing’ the document but the actual permissions to be assigned for any specified recipients will be those specified in the **Permissions**).

### **2.1.6 Sender Selection using Metadata**

Emails containing secured files will normally be sent with the From address set to the email address corresponding the S-Author user account used to configure ScanSECURE. The **fromName** selection capability enables Sharp Digital IMAGER users to select an alternative FileSECURE User Account by its User ID from which emails containing secured files will be sent.

## 3 Secure Scanning Applications

Secure Scanning may be used in the following ways:

### 3.1 Secure Scanning to pre-configured email recipients

This is the simplest form of Secure Scanning. At the Sharp Digital IMAGER, the operator selects a Destination for the scanned image and scans the document. The Destination has a name such as *Financial Records*, *Insurance Application*, *Employee Record*, *Engineering Document*, or other meaningful name based on the types of documents typically scanned. Each Destination corresponds to a folder on a computer which has been configured with FileSECURE ScanSECURE. The document is scanned and sent as a file to the specified folder. ScanSECURE then

1. secures the file based on a pre-configured Security Category specified in the ScanSECURE settings,
2. optionally sends the secured file to fixed set of email recipients, or
3. optionally moves the secured file to a pre-selected folder on the same or different computer for archiving purposes.

This mode can be used with any Sharp Digital IMAGER capable of scanning files to an FTP Destination. It does not require metadata configuration.

### 3.2 Secure Scanning to Archive with a user-selected security category

At the Sharp Digital IMAGER, the operator selects Image Send, Data Entry and a Metadata Set, then selects:

1. a Category and/or
2. a Folder

The Digital IMAGER scans the file and its associated metadata to a folder monitored by FileSECURE. FileSECURE secures the file based on the metadata, then moves the file to a pre-selected archive folder on the same or different computer for archiving purposes.

If the user specifies a value for the **Folder**, FileSECURE moves the file and its associated Metadata file to the designated subfolder. This folder must be a subfolder of the folder that is used as the main FTP destination folder.

If the user does not specifies a value for the *Category*, FileSECURE secures the file based on a *default security Category*, optionally sends the secured file to a default set of email recipients, and/or optionally moves the secured file to a default archive folder. In other words, the processing is the same as for Basic Secure Scanning. The default security Category, default email recipients, and default archive folder are configured using FileSECURE ScanSECURE dialogs.

Options selected by the Users at the Digital IMAGER always override default settings.

### 3.3 Secure Scanning to fixed recipient list with a user-selected security category

At the Sharp Digital IMAGER, the user selects Image Send, Data Entry and a Metadata Set, then selects:

1. a target Folder
2. a security Category,

The document is scanned and sent to a folder where FileSECURE secures the file based on the selected options then sends the secured file to a fixed set of email recipients. The fixed list of recipients may vary depending on the user-selected Folder.

If the user selects a *Folder*, FileSECURE moves the file and its associated Metadata file to the designated folder before securing and processing the file.

If the user does not select a *Category*, FileSECURE secures the file based on a default security Category, optionally sends the secure file to a default set of email recipients, and/or moves the secured file to a default archive folder as noted above. The default security Category, default email recipients, and default archive folder are configured using FileSECURE ScanSECURE dialogs.

Options selected by the Users at the Digital IMAGER always override default options.

### 3.4 Secure Scanning to selected FileSECURE Users

From the Sharp Digital IMAGER, the user

1. selects Image Send, Data Entry and a Metadata Set then
2. selects a *Folder*, a *Category*, and/or custom *Permissions*. Then
3. selects email addresses for existing FileSECURE users from the Digital IMAGER Address Book.

The document is scanned and sent to a folder where FileSECURE

1. moves the document to another folder, or
2. secures the file based on the selected options,
3. sends the secured file to the user-selected email recipients, and then
4. optionally, moves the file to a pre-selected folder on the same or different computer for archiving purposes.

If the user selects a *Folder*, FileSECURE moves the file and its associated Metadata file to the designated folder before securing and processing the file.

If the user does not select a *Category*, custom *Permissions*, or Email addresses, FileSECURE secures the file based on a pre-selected default security category and optionally sends the secured file to a fixed set of email recipients or to a pre-selected default folder on the same or different computer for archiving purposes, as in the case of Basic Secure Scanning. The default security Category, default email recipients, and default archive folder are configured using FileSECURE ScanSECURE dialogs.

Options selected by the Users at the Digital IMAGER always override default options.

**Note:** In the above scenarios, it is quite possible to send secured files to persons who do not have the permissions to open them. ScanSECURE relies on proper configuration and does not check to ensure that recipients have necessary Permissions

### 3.5 Secure Scanning to arbitrary email recipients with user-selected Security Category or permissions

From the Sharp Digital IMAGER, the user

1. selects Image Send, Data Entry and a Metadata Set, then
2. selects a Folder, a Category, and/or custom Permissions, then
3. enters email addresses for a list of arbitrary users using the Digital IMAGER Local Address Book.

The document is scanned and sent to a folder where FileSECURE

1. moves the document to another folder, or
2. secures the file based on the selected options,
3. sends the secured file to the selected email recipients creating new FileSECURE Reader accounts as required with a expiration date configurable for the FileSECURE system, and then



4. optionally moves the file to a pre-selected folder on the same or different computer for archiving purposes.

If the user selects a *Folder*, FileSECURE moves the file and its associated Metadata file to the designated folder before securing and processing the file.

If the user does not select a *Category*, custom *Permissions*, or Email address, FileSECURE secures the file based on a default security category and optionally sends the secured file to a default fixed set of email recipients or to a default folder on the same or different computer for archiving purposes. The default security Category, default email recipients, and default archive folder are configured using FileSECURE ScanSECURE dialogs.

Options selected by the Users at the Digital IMAGER always override default options.

## 4 Configuration

### 4.1 Prerequisites

To configure Secure Scanning with your Sharp Digital IMAGER, you require the following:

1. A Sharp AR-M237, AR-M277, AR-M355, AR-M455, AR-M550, AR-M620, and AR-M700 Digital IMAGER upgraded to the Dragon Firmware.
2. A Personal Computer to be used as the FileSECURE ScanSECURE Server
3. An email account from which to email
4. An S-Author Account on a FileSECURE Server
5. Sharpdesk Software 3.1 CD for installing the Network Scanning Tool (NST) Software (FTP software and scanned image processing software)
6. The FileSECURE Author Software which can be downloaded from [www.airzip.com/FileSECUREAuthor4.htm](http://www.airzip.com/FileSECUREAuthor4.htm)
7. One hour to complete and install the software

## 5 Planning and Configuration

To configure Secure Scanning with your Sharp Digital IMAGER, follow these steps:

1. Plan your Secure Scanning implementation.
2. Gather necessary prerequisites.
3. Upgrade your Sharp Digital IMAGER with the Dragon Firmware.
4. Configure your Secure Scanning PC.
5. Configure the ScanSECURE operation for each Target Destination Folder and Subfolder.
6. Install Sharpdesk and the Network Scanning Tool from the Sharpdesk Software 3.1 CD on the ScanSECURE PC.
7. Use the Network Scanning Tool to enable your ScanSECURE PC as a Scanner Destination.
8. Configure the Sharp Digital IMAGER for the Metadata Delivery.
9. Validate the operation from the Digital IMAGER.

The following sections provide guidelines for each of these steps.

### 5.1 Plan your Secure Scanning implementation

Your Secure Scanning deployment plan should identify the following:

1. The Secure Scanning Administrator. This should be a person who has access to the Personal Computer that will be used for securing and sending the documents and oversees scanning operations.
2. The types of documents that require securing - for example, human resource records, financial records, applications, legal documents, etc.
3. For each type of document, the email addresses where such documents should be sent
4. The permissions that will be provided to each recipients.
5. The content of the associated email message.
6. The Archive file where each type of file should be stored.

Attached is a form for creating the plan and below is an example plan:

#### Sample Secure Scanning Implementation Plan Example

Secure Scanning Administrator: John McCartney

Secure Scanning PC: John McCartney's PC

Documents to be secured	Distribution	Permissions	File Archive
Financial records (Purchase Orders, Invoices, Project billing reports, etc.)	Finance Records Processing Executive	View, Print View View	Financial Records on main file server
Loan applications (Application forms, bank statements, tax returns, etc.)	Loan Officer Loan Administration	View/Print View	Loan Applications on main file server

## 5.2 Gather necessary prerequisites

To configure Secure Scanning with your Sharp Digital IMAGER, you require the following:

1. A Sharp AR-M237, AR-M277, AR-M355, AR-M455, AR-M550, AR-M620, and AR-M700 Digital IMAGER upgraded to the Dragon Firmware.
2. A Personal Computer to be used as the FileSECURE ScanSECURE Server
3. An email account from which to email
4. An S-Author Account on a FileSECURE Server
5. Sharpdesk Software 3.1 CD for installing the Network Scanning Tool (NST) Software (FTP software and scanned image processing software)
6. The FileSECURE Author Software which can be downloaded from [www.airzip.com/FileSECUREAuthor4.htm](http://www.airzip.com/FileSECUREAuthor4.htm)
7. One hour to complete and install the software

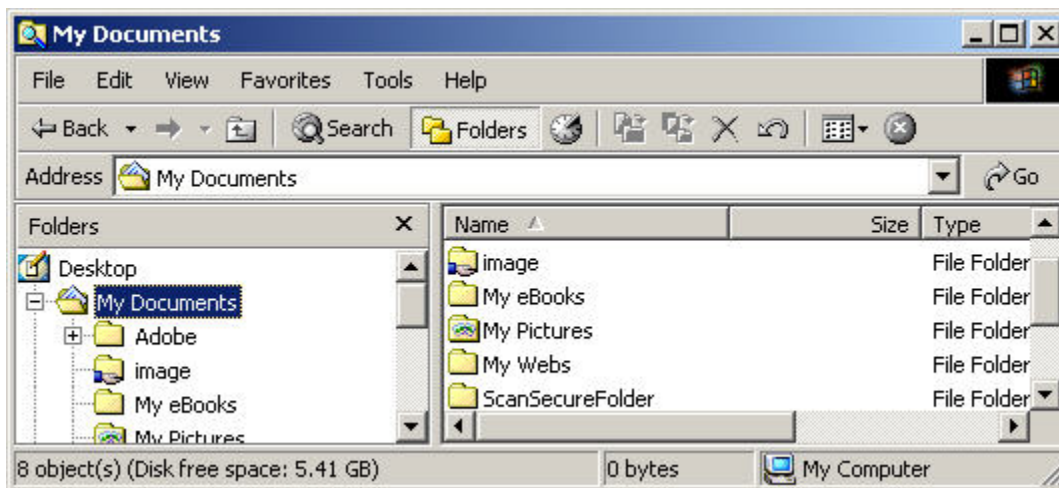
## 5.3 Metadata enable your Sharp Digital IMAGER

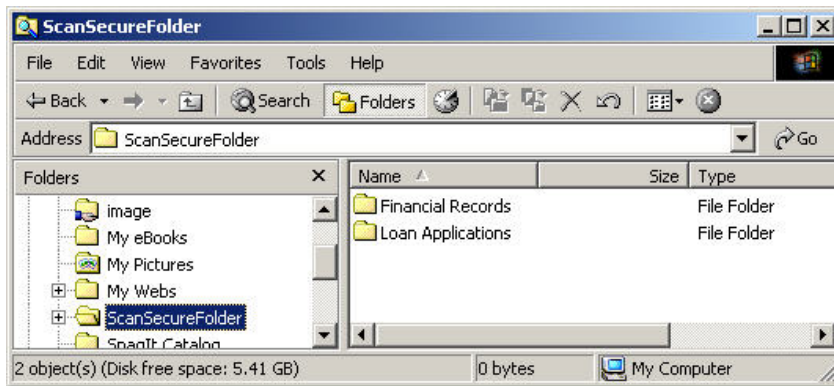
Simply order the "Application Integration Module" option for your Digital IMAGER through your Sharp distributor. Your Sharp distributor will provide the necessary activation code.

## 5.4 Configure your Secure Scanning PC

Follow these steps:

1. Configure the FileSECURE Server to support ScanSECURE and create an S-Author User Account on the FileSECURE Server for the Secure Scanning Administrator.
2. Install FileSECURE Author Software on the Secure Scanning PC. This software may be downloaded from [www.airzip.com/FileSECUREAuthor4.htm](http://www.airzip.com/FileSECUREAuthor4.htm)
3. Configure the S-Author User Account the Secure Scanning PC following the procedures in the online help for setting up this account
4. Use Windows Explorer to set up *Destination* folders and subfolders based on your Secure Scanning Plan.



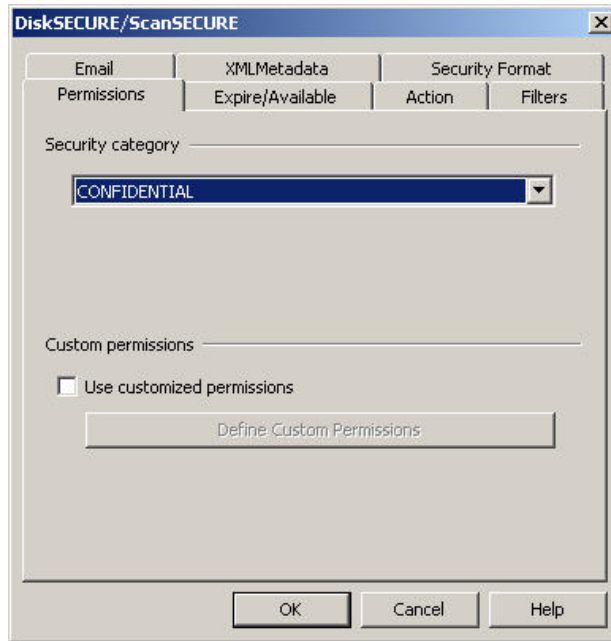


## 5.5 Configure the ScanSECURE operation for each Target Destination Folder and Subfolder.

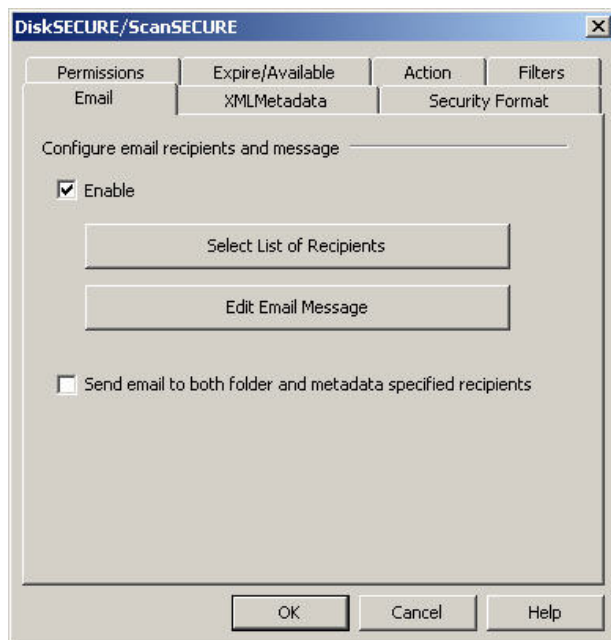
DiskSECURE, AutoSECURE, and ScanSECURE are closely-related FileSECURE features that allow you to secure files by merely moving them to specific folders on your computer. Secure Scanning requires an S-Author Account. An S-Author Account activates the ScanSECURE option.

To initially enable ScanSECURE

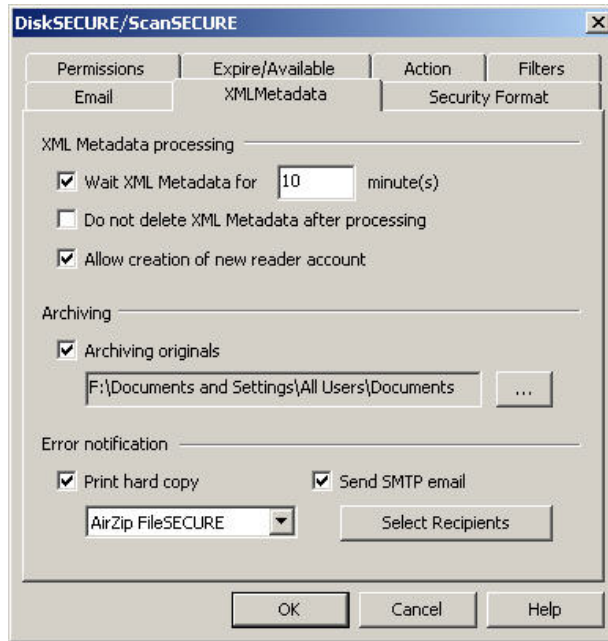
1. Open FileSECURE Author and log into the S-Author account that you wish to use with ScanSECURE. You may only use ScanSECURE with one FileSECURE Account and one Scanner.
2. Select the folder that you want to configure for ScanSECURE in either of the following ways:
  - a. Select Edit > DiskSECURE menu item. In the Folders panel on the Set DiskSECURE/ ScanSECURE dialog, click the Add folder button, then the browse button. Select a folder to add in Find Folder dialog and click OK.
  - b. Right-click a folder that you want to secure in the left pane of the FileSECURE Author window, then select Add to DiskSECURE from the popup menu.
  - c. Use the DiskSECURE/ ScanSECURE dialog (see below) to set default Permissions, Expire/Available date and times, Actions, Filters or other options for this DiskSECURE folder.



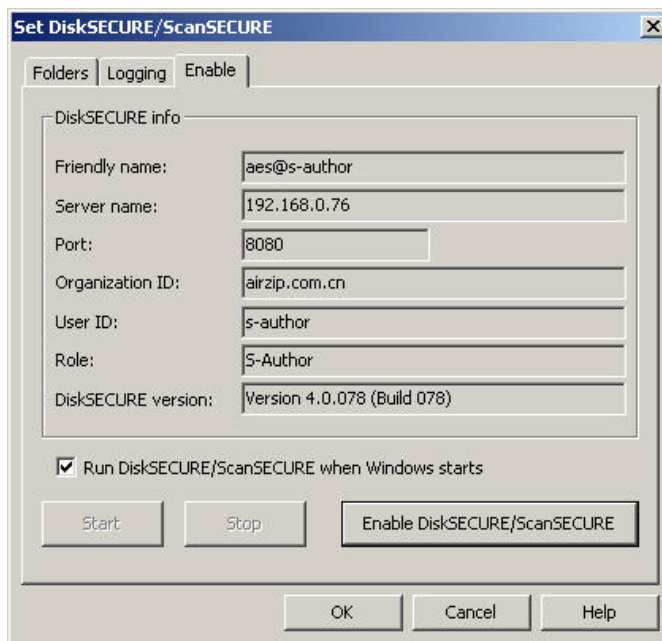
- d. Use the Email Options tab (see below) to set Emailing Options.



- e. Use the XMLMetadata tab (see below) to select ScanSECURE Metadata processing options for the selected folder.



3. Click **Apply** to accept changes. Click **Cancel** to not save the changes. Click **OK** to add the Folder and return to the Set DiskSECURE/ ScanSECURE dialog.
4. On the Set DiskSECURE/ ScanSECURE dialog, click the Enable tab (see below), then the Enable DiskSECURE button. When DiskSECURE is enabled, the DiskSECURE Tray Icon will appear in the system tray in the lower-right corner of the desktop.



5. Once DiskSECURE / ScanSECURE starts, click the Folder tab and proceed with adding other ScanSECURE folders.
6. Click **OK** to add the Folder. Click **Cancel** to not save the changes.

## 5.6 Install Sharpdesk and the Network Scanning Tool from the Sharpdesk Software 3.1 CD on the ScanSECURE PC

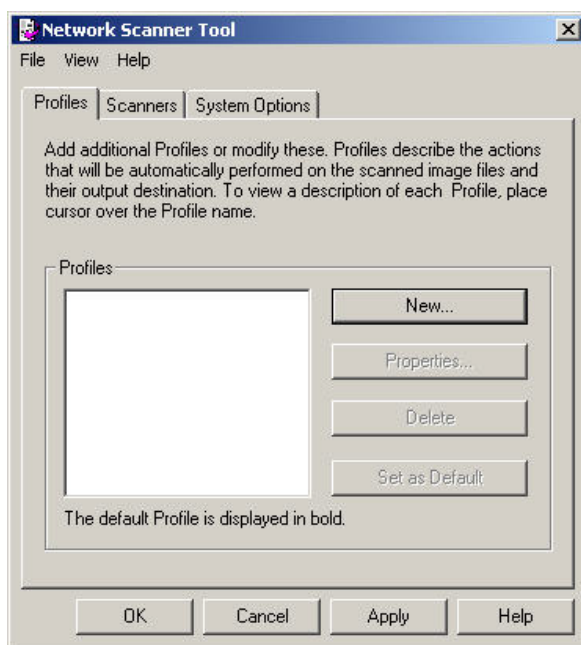
While any FTP based File Transfer software can be used to enable FTP site on your ScanSECURE PC, one of the easiest to set up is the Network Scanning Tool that comes with Sharpdesk Software. Contact Sharp to acquire this software.

## 5.7 Use the Network Scanning Tool to enable your ScanSECURE PC as a Scanner Destination

Follow these steps:

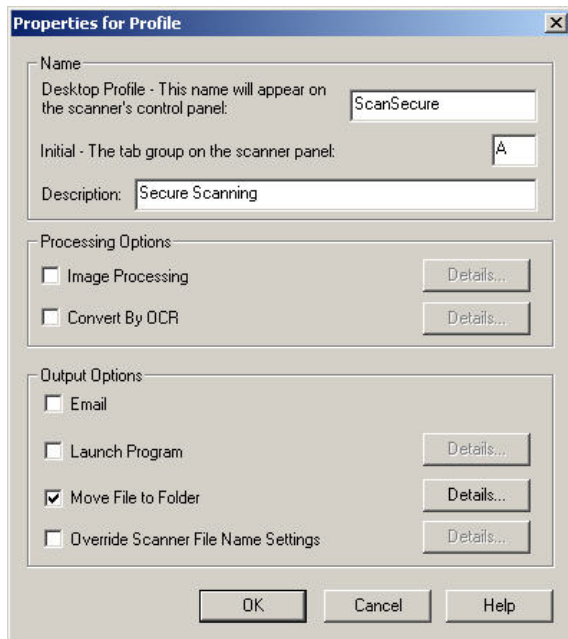
1. Open the Network Scanner Tool.

**Note:** Ensure that it connects with the Scanner properly and that FTP port is set to 21. This is essential. Using a port other than port 21 will NOT work!

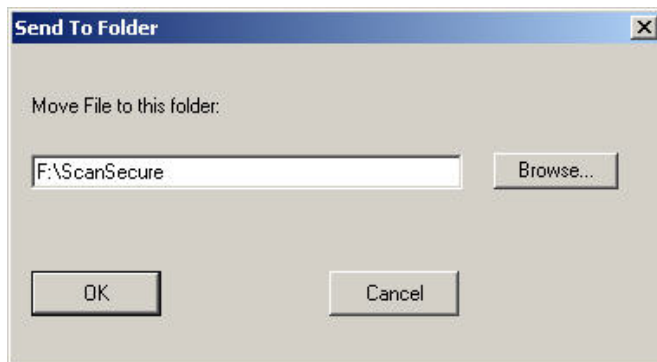


2. Click **New** to configure a New Destination on your ScanSECURE PC.
3. In the Properties for Profile window below, enter a name and description for the ScanSECURE Destination you want to make available for your application as shown by the example below.

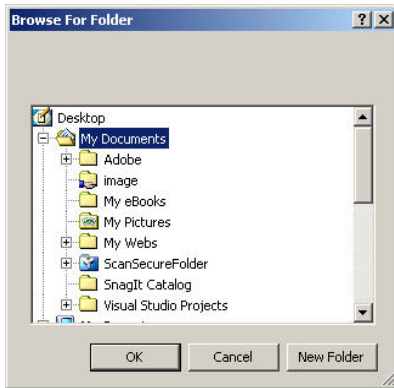




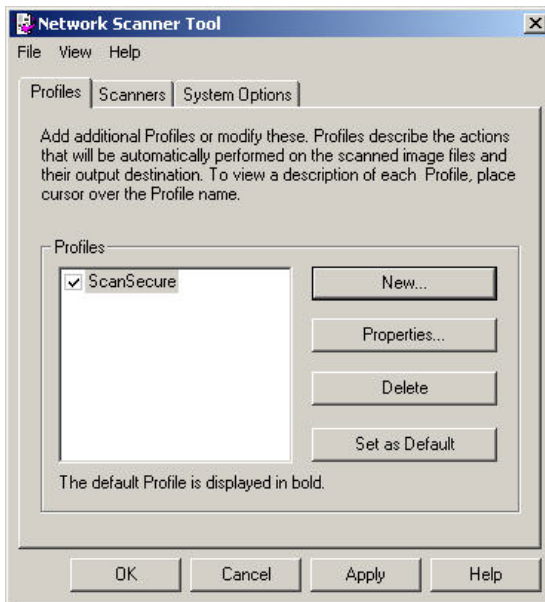
4. Check the **Move File to Folder** and click **Details**.
5. In the Send to Folder window below, click **Browse**.



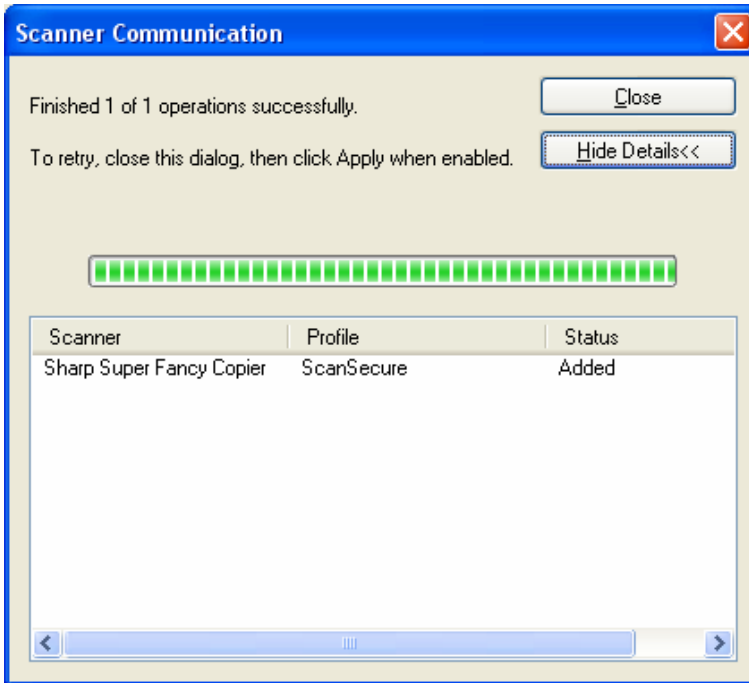
6. In the *Browse For Folder* dialog below, locate the Destination folder that you want to enable.



7. Click **OK** to return to the main Network Scanner Tool.

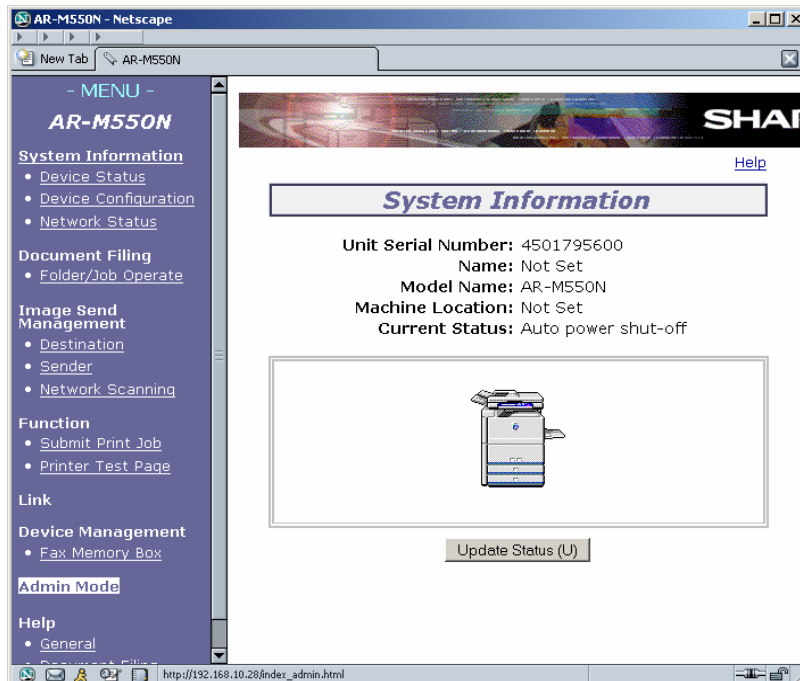


8. In the main Network Scanner Tool window, Click **Apply** to automatically enable a scanner configuration. The Scanner Communication Window below will confirm success.

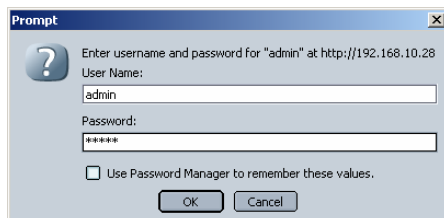


## 5.8 Configure the Sharp Digital IMAGER for the Metadata Delivery

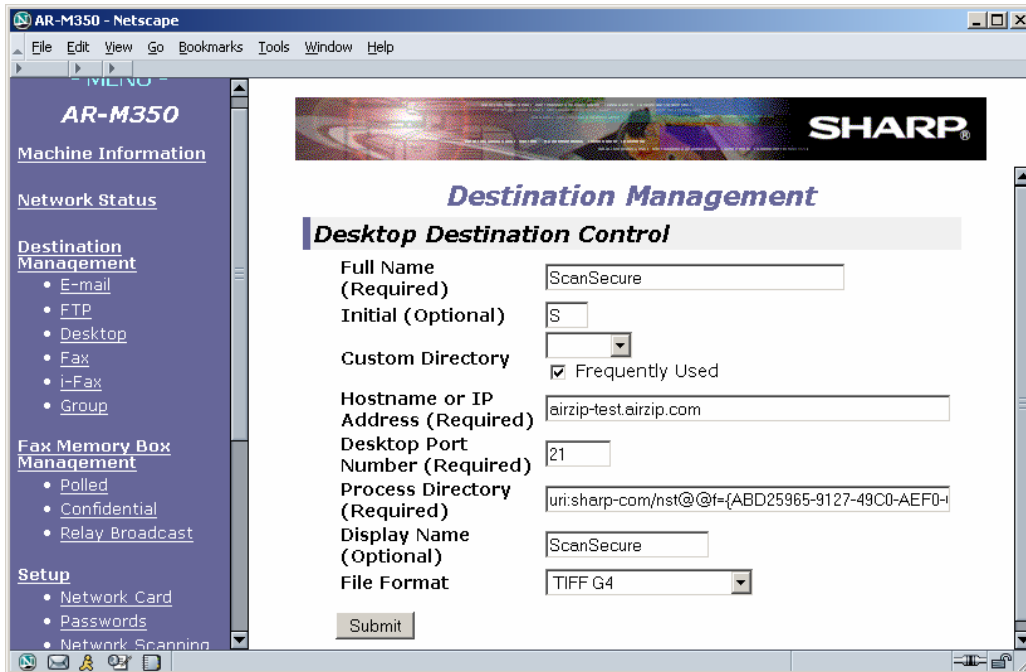
1. Connect to the Digital IMAGER using your browser and select the Admin mode:



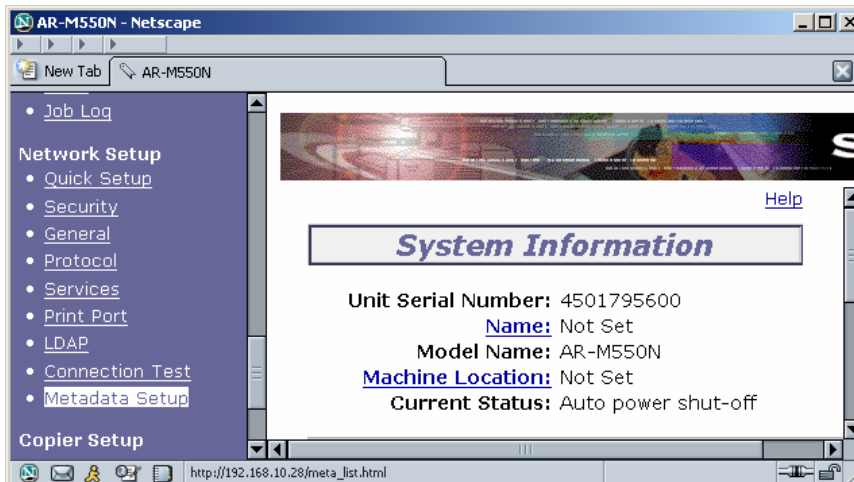
2. Authenticate with the copier:



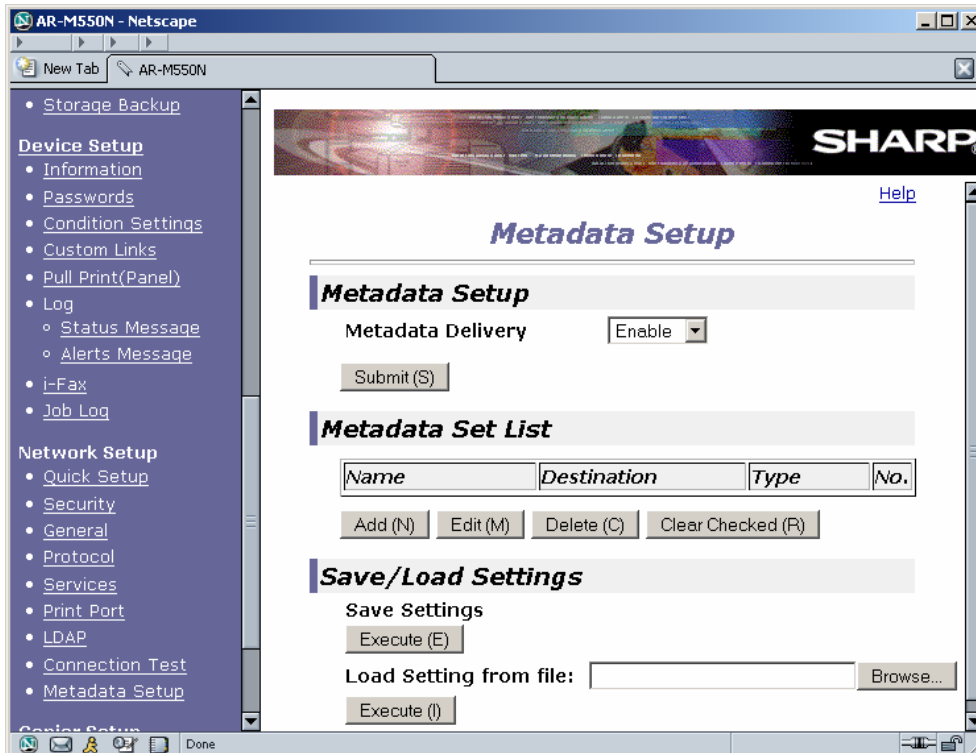
3. Select Destination Management, locate the ScanSECURE Destination that you have just configured and click **Edit**.
4. In Desktop Destination Control display below, specified Tiff G3 or G4 as the File Format.



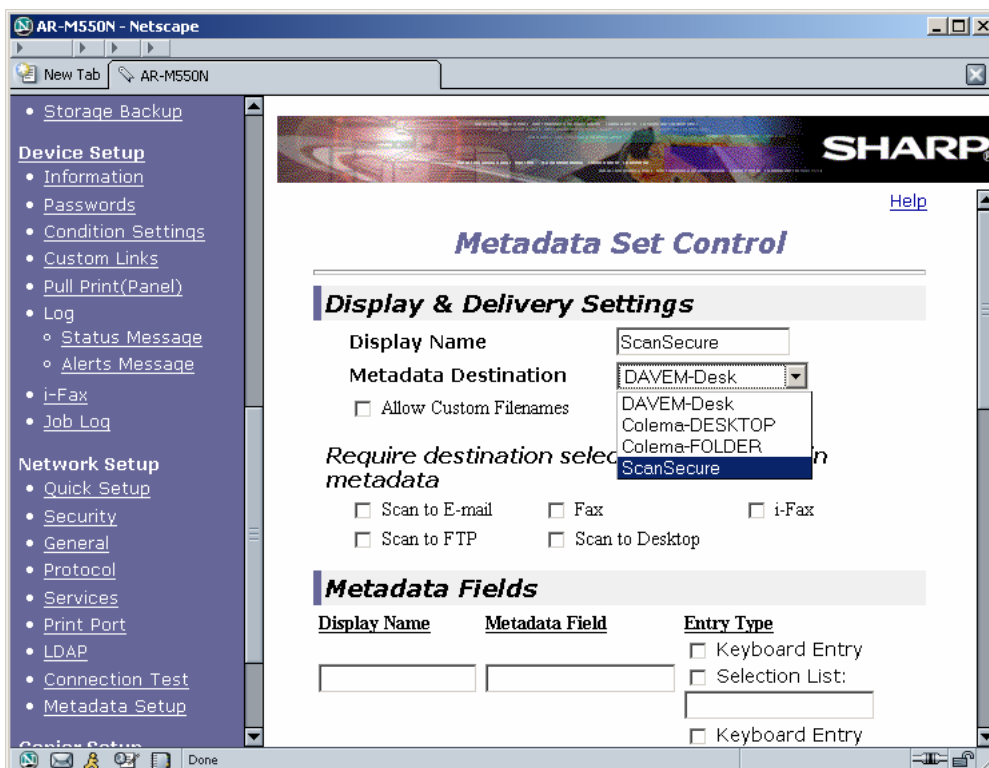
5. Next select **Metadata Setup**.



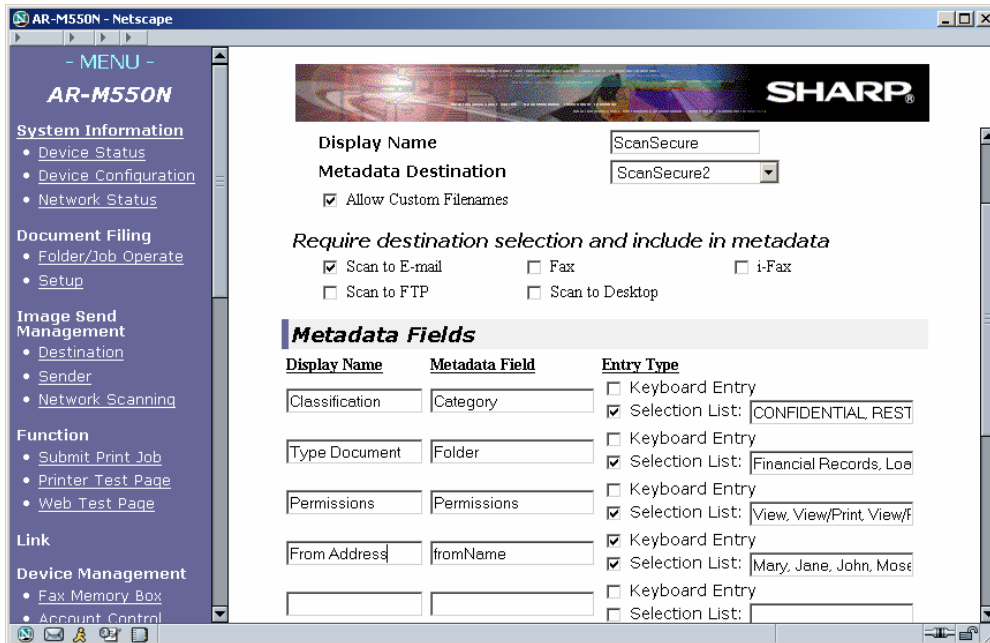
6. Enable Metadata Delivery by selecting Enable and clicking **Submit**.



7. Under Metadata Set List, click **Add**.
8. In the Metadata Set Control window, specify a Display Name and corresponding Destination location using the pull down list.



- Enter the Display Names, Metadata Fields, and Entry Type that support your application. . It is far less error prone to provide a Selection List than allow Keyboard entry. Click Scan to E-mail to require users to enter an email recipients



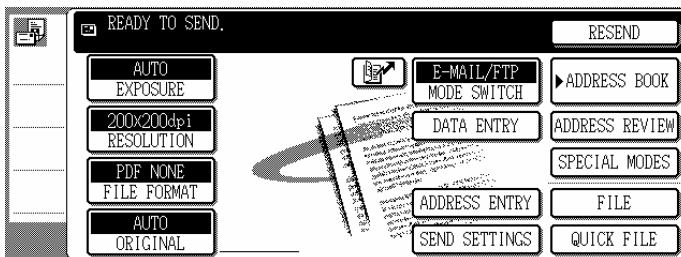
## 5.9 Validate the operation from the Digital IMAGER

Once configured, following these steps to ensure that the scanned file and metadata are being properly delivered and secured:

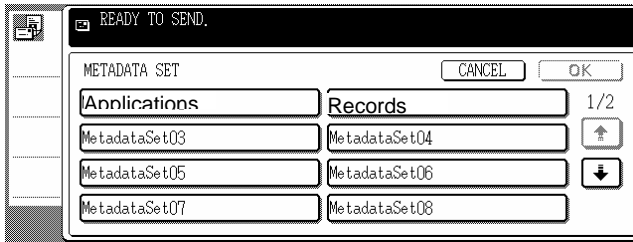
- Place a document to be scanned in the scanner tray.
- Press Image Send.



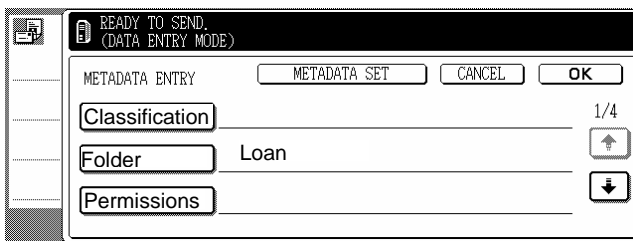
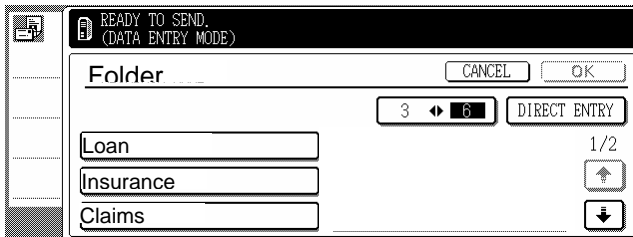
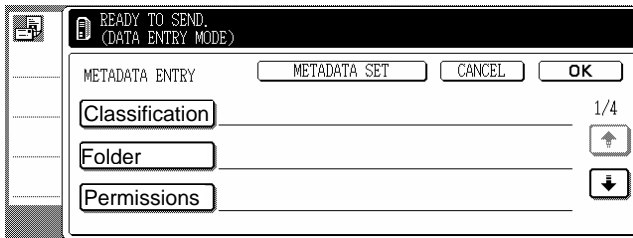
- Select Data Entry on the touch panel.



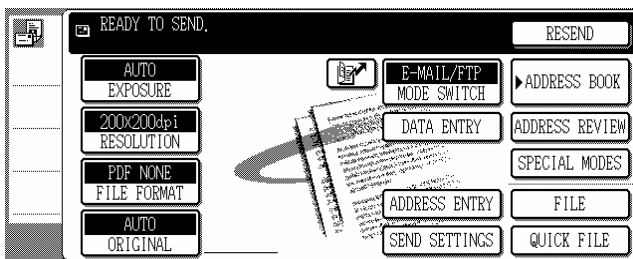
- Select the Metadata Set that you have configured.



5. Answer the Metadata questions to determine how ScanSECURE will process the file as shown below.



6. When complete, press OK.
7. If your application requires the entry of email recipients, when returned to the main window, select Local Address Book



8. Use the Address Book below to select or enter Email recipients.





## 6 ScanSECURE Processing – More Details

FileSECURE ScanSECURE is configured for a particular file folder on a particular Windows personal computer or Server. When configured for Metadata processing, ScanSECURE processes new files and optionally associated XML Metadata files when deposited by a Sharp Digital IMAGER in a local folder.

### 6.1 Configuration Options

ScanSECURE allows multiple folders (also known as directories) to be configured, each with different ScanSECURE settings. The following ScanSECURE Metadata processing options are provided.

- **Wait for XML Metadata for select number of minutes.**

If checked, FileSECURE will secure the file based on the contents of the metadata if a metadata file arrives within the selected number of minutes. If the XML Metadata is not received within this interval, FileSECURE will secure and distribute new files according to the Permissions, Expire/Available, Actions, Filters, and Email settings for this folder.

- **Enable Emailing.**

If Emailing is enabled on the Email tab, ScanSECURE emails secured files only to the recipients defined in metadata. If the metadata does not include email recipients, ScanSECURE will secure files and send them via email to the Select(ed) List of Recipients defined on the Email tab.

If Emailing is NOT enabled on the Email tab, ScanSECURE sends secured files only to those recipients defined in metadata.

The content of the email message can be modified using the Edit Email Message function on the Email tab.

- **Allow Creation of New Reader Accounts.**

If this option is enabled, FileSECURE creates new Reader Accounts based on the recipient address(es) in the XML metadata file. New Reader accounts that ScanSECURE creates will expire after the number of days configured by the FileSECURE System Manager for the Organization's Reader Expiration.

If **Allow Creation of New Reader Accounts** is ENABLED and the S-Author Account being used is allowed to add new Readers, FileSECURE will automatically create a new temporary Reader account for each user where the user does not already have a valid or expired account. Where a Reader account with the same email address has expired, FileSECURE will automatically extend the Reader account (rather than create a new one). FileSECURE will ONLY extend Reader Accounts. FileSECURE will NOT extend Author and Manager Accounts

If **Allow Creation of New Reader Accounts** is ENABLED but the S-Author Account does NOT allowed to add new Readers, FileSECURE will email the newly-secured documents only to existing and enabled FileSECURE users (based again on a match between the XML-specified recipient email address(es) and the email addresses of existing users).

- **Archive Originals to a selected folder**

Both the original scanned document and its associated metadata file are archived.

- **Send ScanSECURE error messages to a printer**
- **Send error messages via SMTP email to specific users**

### 6.2 ScanSECURE Metadata Processing

If **Wait for XML Metadata** is enabled, ScanSECURE perform the following functions:

ScanSECURE will move the newly arrived scanned documents and its associated metadata file to the subfolder for processing, if three conditions are met:

1. a **Folder** value is specified in the XML,
2. the value is different from the current folder name, and
3. the value is identical to the name of the subfolder located in the current subfolder.

If a **Folder** value is not specified, the value is the same as the current folder, or the value does not match the name of a subfolder, ScanSECURE processes the file based on the settings of the current folder.

ScanSECURE will secure a file with the Security Category provided in the metadata file rather than the *default Security Category* configured for the current folder, if two conditions are met:

1. a **Category** value is specified in the XML, and
2. the value matches a Security Category configured for the current FileSECURE Organization.

If a **Category** value is not specified or its value does not match the name of a currently configured Security Category, ScanSECURE will secure the file using the *default Security Category* set up for the current ScanSECURE Folder.

ScanSECURE will email secured files to metadata-specified **email recipients** in addition to those defined using the Email tab if conditions are met:

1. the metadata-specified **email recipients** have active FileSECURE Accounts, and
2. **EmailSecure (SMTP Email)** is activated for the current FileSECURE Organization,

If both **Permissions** AND **email recipients** are included in the metadata, ScanSECURE will add the designated *permissions* for each metadata-specified Email recipient as custom permissions in addition to assigning the Security Category permissions as described above, if the value of **Permissions** specified in the XML is a valid value.

ScanSECURE will email secured files from an email address where the metadata specified “**fromName**” value matches the UserID of an active (not expired or disabled) FileSECURE Author account. Otherwise, ScanSECURE will mail secured files from the email address associated with the S-Author User Account.

ScanSECURE will create new FileSECURE Reader account or reactive an expired FileSECURE Reader account for each metadata-specified Email recipient who does not have a currently active FileSECURE Account, if three conditions are met:

1. **Allow Creation of New Reader Accounts** is enabled, and
2. **EmailSecure (SMTP Email)** is activated for the current FileSECURE Organization,

ScanSECURE shreds (or deletes) the original file or moves the original file (and the associated XML Metadata file) to another directory based upon the defaults set up for current ScanSECURE Folder.

### 6.3 ScanSECURE Errors

Configuration settings or other conditions may prevent error free operation.

**The following errors may be reported when configuring ScanSECURE:**

Error	Corrective Action
DiskSECURE/ ScanSECURE is in use by another account.	Log in using that account to change settings.
This folder is a global configuration folder and cannot be used with DiskSECURE / ScanSECURE.	Configure an alternative folder as this type of folder can never be used with DiskSECURE / ScanSECURE)
This folder is an UNC folder and cannot be used with DiskSECURE / ScanSECURE.	Configure an alternative folder or change the folder's property.
This folder is shared and cannot be used with	Configure an alternative folder or change the

DiskSECURE.	folder's property. (Only reported when using DiskSECURE)
This folder is invalid.	Configure an alternative folder.
The log file location that you have specified is in a DiskSECURE /ScanSECURE folder.	Select a location other than a DiskSECURE / ScanSECURE folder for the log file.

#### Error conditions that may occurring when starting ScanSECURE.

Error	Corrective Action
Failed to logon to the FileSECURE server.	Verify your network configuration using the Account Test function.
Do not have proper permissions.	Verify that the account configured for ScanSECURE is configured as an S-Author account.
Folder path is invalid	Verify the folder path.
Can not find configuration file.	Disable and re-enable DiskSECURE/ScanSECURE for the targeted folders.
Configuration file is invalid.	Disable and re-enable DiskSECURE/ScanSECURE for the targeted folders.
There are no DiskSECURE/ScanSECURE folders configured or selected.	Configure at least one folder for use with DiskSECURE / ScanSECURE and restart.

#### The following error conditions may occur during execution

Error	Corrective Action
Secure file failed.	Verify that your network connection and FileSECURE Server are available. Also verify that there is adequate disk space available for securing files. Verify that this file is available and not opened by other applications. Verify all DiskSECURE/ScanSECURE settings. FileSECURE will retry the process at intervals until it is successful.
Archive file failed.	Verify the availability of the Archive folder location. Verify this file is available and not opened by other applications.
Shred file failed.	Verify that the file is not write-protected. Verify this file is available and not opened by other applications. Verify DiskSECURE/ScanSECURE settings as above.
Mail file failed.	Verify EmailSecure SMTP settings are correct and that you email server is functioning.
No or unreadable metadata found after N minutes where XML is enabled.	Verify the network connections between the scanner and the FileSECURE Server. Verify

	scanner setting to ensure that this folder is configured for Metadata transmission only.
Invalid Folder – A subfolder with that name does not exist at the same level as the current folder.	Verify that the Folder values selectable from the Scanner correspond exactly to Subfolders configured in the main ScanSECURE Destination folder.
Invalid Category – Category does not exist	Verify that Category values selectable from the Scanner are valid FileSECURE Categories for the Organization being used.
Invalid Permission	Verify that Permissions values selectable from the Scanner are one of the following: <b>ViewOnly, View/Print, View/Print/Copy, or View/Print/Copy/Control.</b>
Invalid fromName – UserID of FileSECURE user same with the fromName does not exist	Verify that fromname values selectable from the Scanner correspond to valid UserIds of FileSECURE Author Accounts.
Invalid file(s) – file(s) list(s) in XML do(es) not exist	Verify the network connections between the scanner and the FileSECURE Server.

## 6.4 Sample Metadata

The following example shows the metadata that is generated when the user selects both a Folder and a Category in the Metadata Delivery Mode:

```
- <?xml version="1.0" encoding="UTF-8" ?>
<metadata xmlns="http://www.sharp-world.com/sharp-mfp-metadata/datatypes"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.sharp-
  world.com/sharp-mfp-metadata/datatypes/datatypes.xsd">
  <metadataSetName>ScanSECURE</metadataSetName>
  <deviceId sendType="ip">192.168.10.29</deviceId>
  <appUserPasswordOn>false</appUserPasswordOn>
  <destinations>
  <address>
  <to sendType="mailto">filesecure_user1@airzip.com</to>
  <name> filesecure_user </name>
  </address>
  </destinations>
  <fromName> filesecure_userID2</fromName>
  <files>
  <file format="tiff-fx" encoding="none" encryption="none" compression="none">
  <fileName>AR-M550N_20040929_021943_49e893457570_001.tif</fileName>
  <fileLocation />
  </file>
  </files>
```

```

<deviceName />
<deviceModel>AR-M550N</deviceModel>
<dateTime>2004-09-29T02:19:43</dateTime>
<imageResolution units="dpi" x="300" y="300" />
<pageSize units="pixel" x="2544" y="3295">letter</pageSize>
<imageMode>text</imageMode>
<userMetadataSet>
<user_metadata>
<prompt>Classification</prompt>
<tag>Category</tag>
<value>CONFIDENTIAL</value>
  </user_metadata>
<user_metadata>
<prompt>Type Document</prompt>
<tag>Folder</tag>
<value>Financial Records</value>
  </user_metadata>
</userMetadataSet>
</metadata>

```

### 6.4.1 File Names

The names of the files transferred to the FTP site are a combination of machine name, time, and date. The scanned image will have an extension of TIF or PDF depending on the Default File Format specified in the Fax Server Setup. The XML file will have the extension xml. See examples below:

AR-M350\_20040415\_103321\_447aa1654330\_001.tif

AR-M350\_20040415\_103321\_447aa1654330.xml

AR-M350\_20040415\_105022\_447ab2664330\_001.tif

AR-M350\_20040415\_105022\_447ab2664330.xml

## Attachment

### Secure Scanning Planning Template

Secure Scanning Planning Form

Secure Scanning Administrator:

ScanSECURE PC Location:

<b>Documents to be secured</b>	<b>Distribution</b>	<b>Permissions</b>	<b>File Archive</b>

Scan Secure Email Template Text

Subject:

Body: