

**XEROX®**



# **Installation and Administration Guide**

---

Release 2.1

June 19, 2006

Xerox Corporation

Global Knowledge and Language Services

800 Phillips Road, Bldg. 0845-17S

Webster, New York 14580

USA

**Copyright © 2001–2006 by Xerox Corporation.** All rights reserved.

XEROX<sup>®</sup>, The Document Company<sup>®</sup>, the stylized X<sup>®</sup>, CentreWare<sup>®</sup>, Document Centre<sup>®</sup>, WorkCentre<sup>®</sup> Pro, DocuShare<sup>®</sup>, FlowPort<sup>®</sup>, PaperWare, SMARTsend, and FreeFlow are trademarks of or licensed to Xerox Corporation in the United States and other countries.

DataGlyph<sup>®</sup> is a trademark of Palo Alto Research Center, Inc.

Adobe and Acrobat are registered trademarks of Adobe Systems, Incorporated.

IBM, Lotus, Domino, and Domino.Doc are registered trademarks of IBM Corporation.

NetWare is a registered trademark of Novell, Inc.

Flash is a trademark of Macromedia, Inc.

Microsoft, Microsoft Windows, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Internet Explorer, Microsoft Office, Exchange 2000, SharePoint, and Internet Information Services (IIS) are registered trademarks of Microsoft Corporation.

Netscape Navigator is a registered trademark of Netscape Communications Corporation.

WordPerfect is a registered trademark of Corel Corporation.

WorkSite is a trademark of Interwoven, Inc.

Hummingbird DM is a trademark of Hummingbird, Ltd.

Documentum is a registered trademark of EMC Corporation.

LiveLink is a registered trademark of Open Text Corporation.

Xerox PDF Reader Powered by Foxit Software Company <http://www.foxitsoftware.com>

# Table of Contents

|  |            |
|--|------------|
| <b>Chapter 1 Welcome to SMARTsend</b>  | <b>1-1</b> |
| What is Included in This Release?  | 1-2        |
| What is New in This Release?   | 1-4        |
| SMARTsend Overview   | 1-5        |
| SMARTsend Documentation  | 1-6        |
| SMARTsend Installation and Administration Guide  | 1-6        |
| SMARTsend User Guide   | 1-6        |
| Help   | 1-6        |
| Quick Reference Cards  | 1-6        |
| Readme.txt   | 1-7        |
| Customer Support   | 1-8        |
| Telephone Support  | 1-8        |
| Internet Support   | 1-8        |
| <b>Chapter 2 Prepare for Installation</b>  | <b>2-1</b> |
| Advance Planning Considerations  | 2-2        |
| Security   | 2-2        |
| Scanning Device and Application Migration  | 2-3        |
| Network Configuration and Logistics  | 2-4        |
| SMARTsend Configuration Requirements   | 2-5        |
| SMARTsend Computer Configuration Requirements  | 2-7        |
| Verifying the SMARTsend Computer DNS Configuration   | 2-8        |
| Enable File and Printer Sharing  | 2-9        |
| Install and Configure IIS / FTP  | 2-10       |
| Enable ASP.NET   | 2-12       |
| Create Administrator, User, and Device Accounts  | 2-13       |
| Obtain and Install a Security Certificate  | 2-16       |
| Additional Requirements for Destinations   | 2-19       |
| Client and Browser Configuration   | 2-25       |
| Modifying Proxy Server Settings  | 2-25       |
| User Authentication Settings   | 2-26       |
| Language Settings  | 2-27       |
| Scanning Device Configuration  | 2-28       |
| Xerox Multifunction Device Requirements  | 2-28       |
| Internet Fax and E-mail Enabled Device Requirements  | 2-32       |
| Prepare Information for Installation   | 2-34       |
| Next Steps   | 2-35       |
| <b>Chapter 3 Install SMARTsend</b>   | <b>3-1</b> |
| Installer Overview   | 3-2        |
| Upgrade SMARTsend  | 3-3        |
| Upgrade Eligibility  | 3-4        |
| Install SMARTsend  | 3-5        |
| Installing and Configuring Optional Components   | 3-7        |
| Configuration Requirements for Optional Components   | 3-7        |
| Installation Instructions for Optional Components (Standard or Professional Edition feature) | 3-13       |
| Migrate SMARTsend to a Replacement Computer  | 3-15       |

|  |            |
|--|------------|
| Repair a SMARTsend Installation .....                                | 3-16       |
| Uninstall SMARTsend .....  | 3-17       |
| <b>Chapter 4 Site Configuration .....</b>                            | <b>4-1</b> |
| Accessing SMARTsend .....  | 4-2        |
| Administration Home Page .....                                       | 4-3        |
| Site Configuration .....   | 4-4        |
| Status Icons .....   | 4-4        |
| Review Security Settings .....                                       | 4-5        |
| General Site Security .....  | 4-5        |
| Device Scan Template Security .....                                  | 4-6        |
| Add/Update Xerox Devices .....                                       | 4-8        |
| Manage Xerox Devices .....   | 4-8        |
| Adding and Discovering Devices .....                                 | 4-9        |
| Using the Xerox Multifunction Device List .....                      | 4-11       |
| Device Configuration and Status Icons .....                          | 4-12       |
| Configuring a Device for use with SMARTsend .....                    | 4-13       |
| Deleting Devices .....   | 4-14       |
| Manage Device Accounts .....   | 4-15       |
| Configure Discovery Settings - Subnets .....                         | 4-17       |
| Configure Discovery Settings - SNMP Credentials .....                | 4-17       |
| Edit Device Configuration Defaults .....                             | 4-18       |
| Edit Xerox Device Properties .....                                   | 4-22       |
| Configure PaperWare Internet Fax Settings .....                      | 4-24       |
| Setup E-mail and Address Book .....                                  | 4-25       |
| SMTP Server Configuration .....                                      | 4-25       |
| LDAP Server Configuration .....                                      | 4-26       |
| Publish the My E-mail Workflow .....                                 | 4-27       |
| Schedule a Backup .....  | 4-28       |
| Configure Service Settings .....                                     | 4-29       |
| Configure Service Options .....                                      | 4-30       |
| Configuring a Service .....  | 4-32       |
| Service Setting Descriptions .....                                   | 4-32       |
| Additional Service Configuration Requirements and Restrictions ..... | 4-33       |
| Manage Application Account .....                                     | 4-34       |
| Changing the Application Account Password .....                      | 4-34       |
| General Settings .....   | 4-35       |
| Update Administrator Contact Information .....                       | 4-35       |
| Choose Error Handling Scheme .....                                   | 4-35       |
| Review Publication / Workflow Defaults .....                         | 4-36       |
| Document Type Properties .....                                       | 4-39       |
| Configure PaperWare Form Forwarding Settings .....                   | 4-40       |
| Next Steps .....   | 4-42       |
| Appendix A - Job Log Export Support .....                            | 4-43       |
| Appendix B - External Application Connection .....                   | 4-44       |
| <b>Chapter 5 Site Management .....</b>                               | <b>5-1</b> |
| Site Management Overview .....                                       | 5-2        |
| Manage Workflows and Publications .....                              | 5-3        |
| Sorting and Viewing Workflows .....                                  | 5-3        |
| Workflow/Publication Management Tasks .....                          | 5-3        |

|  |            |
|--|------------|
| Managing Xerox Devices .....   | 5-6        |
| View Xerox Devices .....   | 5-6        |
| Manage Device Accounts .....   | 5-6        |
| Configure Discovery Settings .....                                       | 5-6        |
| Device Configuration Defaults .....                                      | 5-6        |
| Backup Status .....  | 5-8        |
| <b>Chapter 6 Scan to Home .....</b>                                      | <b>6-1</b> |
| Scan to Home Overview .....  | 6-2        |
| Managing Scan to Home Templates .....                                    | 6-2        |
| Requirements .....   | 6-2        |
| Installing the SMARTsend Scan to Home Utility .....                      | 6-3        |
| Uninstalling the SMARTsend Scan to Home Utility .....                    | 6-4        |
| Getting Started with Scan to Home .....                                  | 6-5        |
| Advance Planning Considerations .....                                    | 6-5        |
| Adding Scan to Home Users From a Windows NT Domain .....                 | 6-6        |
| Adding Scan to Home Users from a Microsoft Active Directory Server ..... | 6-6        |
| Adding Scan to Home Users From an LDAP Directory Service .....           | 6-7        |
| Adding Scan to Home Users From the Local Computer .....                  | 6-8        |
| Scan to Home Utility .....   | 6-9        |
| Accessing the Scan to Home Utility .....                                 | 6-9        |
| Obtaining a List of Available Users .....                                | 6-9        |
| Choosing a Server .....  | 6-9        |
| Enter Source Information Dialog .....                                    | 6-10       |
| Active Directory or LDAP Mappings .....                                  | 6-11       |
| Showing Users .....  | 6-11       |
| Adding Users and Groups .....  | 6-12       |
| Status Bar .....   | 6-13       |
| Progress Bar .....   | 6-13       |
| User Menu Commands .....   | 6-13       |
| Tools Menu Commands .....  | 6-18       |
| File Menu Commands .....   | 6-19       |
| Exit Utility .....   | 6-19       |
| Editing User Properties .....  | 6-20       |
| SMARTsend Scan to Home Application Features .....                        | 6-21       |
| Importing Users into the SMARTsend Scan to Home User Database .....      | 6-21       |
| Managing the SMARTSend Scan to Home Users Database .....                 | 6-22       |
| Managing Master Filing Credentials .....                                 | 6-24       |
| Publishing Scan to Home Templates .....                                  | 6-25       |
| Publish Page .....   | 6-26       |
| Adding Scan to Home Publications to Additional Devices .....             | 6-27       |
| Viewing Scan to Home Publications .....                                  | 6-27       |
| Deleting Scan to Home Publications .....                                 | 6-27       |
| About Scan to Home Template Publishing Options .....                     | 6-27       |
| <b>Chapter 7 Problem Solving .....</b>                                   | <b>7-1</b> |
| Troubleshooting a Problem .....  | 7-2        |
| SMARTsend Confirmations and Error Logs .....                             | 7-3        |
| Common Issues .....  | 7-4        |
| Server Unavailable Errors .....  | 7-4        |
| 403 "Forbidden" Error .....  | 7-4        |

|  |                |
|--|----------------|
| SMARTsend does not recognize IIS FTP service .....                         | 7-4            |
| Unable to install MSDE during installation of SMARTsend .....              | 7-4            |
| Login Failure Message .....  | 7-5            |
| SMARTsend Inaccessibility within an Intranet .....                         | 7-5            |
| Windows 95/98/Me Client and Non-Microsoft Browser Access Problems .....    | 7-5            |
| Missing Icons on Document Destinations Page .....                          | 7-5            |
| Page Could Not be Displayed Error .....                                    | 7-5            |
| Pop-up Blocker Problems .....  | 7-5            |
| Device Communication and Configuration Issues .....                        | 7-6            |
| Template Refresh Failure at Devices .....                                  | 7-9            |
| SharePoint Portal Server 2001 Compatibility with Windows Server 2003 ..... | 7-10           |
| Frequently Asked Questions .....   | 7-14           |
| <b>Chapter 8 SMARTsend Utilities .....</b>                                 | <b>8-1</b>     |
| Requirements .....   | 8-2            |
| Template Importer .....  | 8-3            |
| File Format and Language Support .....                                     | 8-4            |
| Exceptions List .....  | 8-7            |
| Importing CentreWare Templates to SMARTsend Workflows .....                | 8-8            |
| Reconfiguring Devices for CentreWare Network Scanning Services .....       | 8-11           |
| Restore Tool .....   | 8-12           |
| Conditions for using the Restore Tool .....                                | 8-12           |
| Using the Restore Tool .....   | 8-12           |
| Exporting Job History .....  | 8-14           |
| <b>Chapter 9 SMARTsend Security .....</b>                                  | <b>9-1</b>     |
| Security Overview .....  | 9-2            |
| HTTPS/SSL Certificates .....   | 9-3            |
| Secure Password Entry .....  | 9-3            |
| Secure Web Site Configuration .....  | 9-3            |
| Site Security Policies .....   | 9-5            |
| General Site Security .....  | 9-5            |
| Device Scan Template Security .....  | 9-7            |
| PaperWare Forms .....  | 9-8            |
| Workflow Access Level Control .....  | 9-9            |
| Security Policy Interactions .....   | 9-10           |
| Scenarios .....  | 9-10           |
| SMARTsend Authentication .....   | 9-12           |
| Accessing SMARTsend .....  | 9-12           |
| SMARTsend Application Account .....  | 9-12           |
| Setting the Password for the Application Account .....                     | 9-12           |
| SMARTsend Device Accounts .....  | 9-13           |
| Credentials .....  | 9-14           |
| <b>Index .....</b>   | <b>INDEX-1</b> |

## Welcome to SMARTsend

This chapter describes the features and functions of the Xerox FreeFlow™ SMARTsend™ software and the support services available through both application documentation and Xerox customer support services.

### *What is in this chapter:*

- *What is Included in This Release?* ..... 1-2
- *What is New in This Release?* ..... 1-4
- *SMARTsend Overview* ..... 1-5
- *SMARTsend Documentation*..... 1-6
- *Customer Support*..... 1-8

# What is Included in This Release?

SMARTsend is available in Standard and Professional Editions.

## Features common to all versions

- Workflow creation features that define the conversion and transmission of paper-based documents from Xerox Multifunction Devices to the following destinations:
  - DocuShare server
  - E-Mail address
  - FTP location
  - Microsoft SharePoint Portal Server 2003
  - Network Folder
  - Remote Printer
  - External Application Connection
- Workflow publication and management features
- Backup and Restore Tools—to save SMARTsend workflows, credentials, user preferences, device configurations, and general settings.
- Template Importer—to import CentreWare Network Scanning Services templates into SMARTsend.
- Job History Exporter—to create a job history text file for analysis and reporting.

## Standard and Professional Edition features

In addition to the destinations common to all versions, support the conversion and transmission of paper-based documents to the following destinations:

- URL location
- Netware Folder
- Microsoft Exchange 2000 Web Folder
- Microsoft SharePoint Portal Server 2001
- Domino
- Domino.Doc

### **Optional components for Standard or Professional versions**

- Documentum version 5.2 destination support
- Hummingbird version 5.1.0.5 destination support
- Interwoven WorkSite version 8 destination support
- LiveLink version 9.5.0 destination support
- TRIM Context Server 6.0 destination support

### **Optional components for Professional version**

- TrueMatch—a patented Xerox technology that enables you to locate electronic documents by scanning portions of the original paper document.

## What is New in This Release?

- SMARTsend can now be installed on Windows XP computers.
- New file format and enhanced file compression options.
- Support for SNMPv3, HTTP, and HTTPS protocols for enhanced device configuration and security options.
- PaperWare forms forwarding, which enables you to configure SMARTsend computers to process PaperWare cover sheets that were created on other SMARTsend or Xerox Flowport computers.
- The Default scan template on Xerox devices can now be used with PaperWare cover sheets.
- Document Attribute (metadata) fields can now be masked and/or designated as required fields.
- SMARTsend can now be configured as a secure website.
- New optional components, such as Documentum, Interwoven WorkSite, Hummingbird, LiveLink destinations.
- Xerox TrueMatch support (optional), which enables you to create search workflows to locate documents on your network.
- Support for DocuShare 5.0.
- Dynamic Filing to a sub-folder.

## SMARTsend Overview

SMARTsend combines and enhances many of the powerful features of two Xerox products—FlowPort™ and CentreWare™ Network Scanning Services—to deliver one integrated software application. Built on the Microsoft .NET platform, SMARTsend software works with new and legacy Xerox advanced multifunction systems, as well as many types of Internet Fax devices from Xerox and other manufacturers.

Using SMARTsend, paper documents can be scanned in full color and converted into a variety of industry standard digital formats, including PDF, JFIF/JPEG, TIFF, and Multi-Page TIFF formats. SMARTsend can also convert scanned documents into editable files such as Excel, Word, PowerPoint or searchable PDF. The resulting files can then be edited, manipulated, saved and shared. SMARTsend also allows the user to add descriptive information (also known as metadata) that will accompany the scanned documents. These versatile features make it simple to categorize, search and retrieve scanned documents.

### Web-based application

SMARTsend is a web-based application that requires no additional client software. Users can easily create workflows that define the type of scanned document, the distribution locations and processes, and the methods and devices that can be used to submit SMARTsend scan jobs. The workflow is then published to make it available to users as device scan templates, or as PaperWare cover sheets (Professional Edition). These publications make it simple for anyone to scan a document and distribute the resulting electronic file(s) to a wide variety of destinations, including e-mail addresses, network folders, FTP folders, remote printers, external applications, Web URLs, Domino and Domino.doc repositories, Microsoft SharePoint Portal Server repositories, and Xerox DocuShare repositories. Additional destinations, such as advanced document management repositories, can be added as optional components.

### Ease of use

SMARTsend is designed for ease of use, versatility, and security. Wizards assist users with complex tasks, and descriptive instructions, status messages, and help system information accompany all SMARTsend screens. Users can set up e-mail and printed confirmation reports, and administrators can create job logs to track usage and obtain audit trails in support of legal and regulatory requirements. Where security is important, SMARTsend stands above the competition with support for the latest secure protocols and secure web site configuration options. In addition, the open and flexible .NET architecture permits easy integration with other programs and provides the flexibility to expand capabilities and features as Xerox makes future enhancements available.

# SMARTsend Documentation

Several forms of documentation are available with SMARTsend, including printable guides that are provided as Adobe Acrobat PDF format documents. The documentation components can be accessed from the links that are provided on the SMARTsend Home Pages, or from the links in the CD autorun program. SMARTsend administrators can also access the Readme file and the Installation and Administration Guide from the Start Menu on the SMARTsend computer.

The Adobe Acrobat Reader is required to view and print the guides. Obtain the reader from the Adobe Web site, [www.adobe.com](http://www.adobe.com).

## SMARTsend Installation and Administration Guide

The *SMARTsend Installation and Administration Guide* includes step-by-step instructions for installing and configuring the SMARTsend computer, clients, and supported scanning devices.

## SMARTsend User Guide

The *SMARTsend User Guide* introduces SMARTsend to new users. It includes overviews of all the main SMARTsend pages and features, as well as step-by-step instructions for key tasks users perform with SMARTsend.

## Help

SMARTsend contains extensive online Help that covers the use of the application beyond installation and initial configuration. Help links are included in the upper right corner of any SMARTsend page.

## Quick Reference Cards

SMARTsend documentation includes the following Quick Reference Cards:

- **Administrator Quick Reference**—Contains requirements, basic installation procedures, and site configuration information for SMARTsend administrators.
- **User Quick Reference**—Contains basic overview and getting started information for general SMARTsend users.

**NOTE:** The Administrator Quick Reference is not recommended for first-time installations of the product. Please use the Installation and Administration Guide for detailed planning and installation instructions.

## Readme.txt

Readme.txt provides product support information that was not available when the other documentation components were released for publication. This information is intended primarily for SMARTsend administrators, and it can be accessed by administrators using the following methods:

- After SMARTsend is installed:
  - On a Windows 2000 server, click **Start > Programs > Xerox > SMARTsend > View ReadMe.txt**;
  - OR -
  - On a Windows XP Professional computer or server running Windows Server 2003, click **Start > All Programs > Xerox > SMARTsend > View ReadMe.txt**.
- Insert the SMARTsend CD into your CD drive. Click the README File link from the CD Installer program.
- Click the View Readme file button during installation.

# Customer Support

You can contact Xerox for support either by telephone or Internet.

## Telephone Support

For additional assistance, contact Xerox by telephone to speak with a Customer Support Representative. Before you call, locate the SMARTsend Serial Number by clicking the About link in the upper right corner of any SMARTsend page. For future reference, be sure to record the Serial Number in the space provided below. The Serial Number is required to obtain technical support from Xerox.

| Xerox SMARTsend Serial Number: |
|--------------------------------|
|                                |

**NOTE:** SMARTsend permits the management of a limited number of devices. To identify the number of supported devices, click the About link on any SMARTsend page and locate the product serial number. The last set of digits appended to the serial number indicate the number of supported devices. By default, SMARTsend Standard and Professional Editions support the configuration of up to five devices and SMARTsend

The Xerox customer support telephone numbers are listed in the following table. If the telephone number for your country is not listed, please contact your local Xerox representative to obtain the number. If necessary, please record the telephone number in the space provided below.

| Xerox Customer Support Telephone Numbers: |                             |
|---|-----------------------------|
| <b>UNITED STATES</b>                      | 800-821-2797                |
| <b>UNITED STATES (TTY)</b>                | 800-855-2880                |
| <b>CANADA</b>                             | 800-939-3769 (800-93-XEROX) |
|   |                             |

## Internet Support

Additional tips and technical information are available from the Support & Drivers link on the Xerox Web site, [www.xerox.com](http://www.xerox.com). Locate or search for your product and access the product support resources. The documents in this section cover specific issues that may require special procedures or application notes regarding the operation and configuration of your Xerox product.

## Prepare for Installation

This chapter describes the hardware, software, network, and security issues that must be considered before the SMARTsend application is installed on a computer. These tasks and considerations are essential elements of a successful installation.

Please read this chapter thoroughly and perform all required configuration tasks before proceeding to Chapter 3, *Install SMARTsend*.

**TIP:** Print the Administrator Quick Reference card for use as a configuration checklist. The Administrator Quick Reference is available from the SMARTsend CD autorun program.

*What is in this chapter:*

- *Advance Planning Considerations* . . . . . 2-2
- *SMARTsend Configuration Requirements* . . . . . 2-5
- *Client and Browser Configuration* . . . . . 2-25
- *Scanning Device Configuration* . . . . . 2-28
- *Prepare Information for Installation* . . . . . 2-34
- *Next Steps* . . . . . 2-35

**NOTE:** If you are upgrading from a Trial Version or a previous version of SMARTsend, simply follow the upgrade procedures in Chapter 3, *Install SMARTsend*, to upgrade your software. The SMARTsend installation program will automatically upgrade a current Trial Version to the current licensed version. All workflows generated while using the Trial Version or a previous version will be accessible after the upgrade is completed. If you have a Trial Version of SMARTsend that has expired, you can upgrade to the retail version and retain all workflows. The retail version can be ordered through your Xerox sales representative, and installed as an upgrade to your existing Trial Version. See *Upgrade Eligibility* on page 3-4 for additional information.

## Advance Planning Considerations

This section contains information and issues that should be considered before you attempt to install and use the SMARTsend application. Please allow adequate lead time to address these issues.

### Security

A security certificate can be installed on the SMARTsend computer if secure password entry or secure data transfer is required within the SMARTsend operating environment. Security certificates are used to enable encryption of sensitive information. Security certificates can be obtained within the network by using software bundled with the network operating system or by using an open-source product. Externally, they can be obtained through the services of a third party for a fee. Which option to choose, if any, depends on factors such as these:

- Security policies and requirements that govern the use of network and physical resources within your organization must be reviewed in advance of your SMARTsend installation. Please consider how your security policies apply to SMARTsend and configure your computer, clients, and scanning devices accordingly. Refer to *Chapter 9, SMARTsend Security*, for additional security information.
- The latest Xerox multifunction devices, such as WorkCentre Pro 232/238/245/255/265/275 or newer devices, offer additional security capabilities such as authentication and more secure communication protocols such as SNMP v3 and HTTPs. These enhanced capabilities can further enhance end-to-end security when devices are configured for use with SMARTsend.
- SMARTsend makes the use of security certificates optional to accommodate installations where other security measures are employed or where security is not a concern. When a security certificate is installed on the SMARTsend computer, it will provide secure password entry when users access SMARTsend. Furthermore, if the *Require Secure Channel (SSL)* option and the security certificate are properly configured on the SMARTsend computer, all data transfer between SMARTsend users and devices will be encrypted. See *To configure the SMARTsend computer to require HTTPS/SSL*: on page 9-3 for additional information.
- If the use of SMARTsend will be limited to the local network or intranet, the most cost-effective approach may be to use the SelfSSL option, or set up a Certificate Authority in-house. A local Certificate Authority can be implemented by using Microsoft Certificate Services, which is included on each Microsoft operating system CD. The SelfSSL option is available in the Microsoft Internet Information Services (IIS) Resource Kit. Go to <http://www.microsoft.com/downloads> for additional information.
- If SMARTsend will be available on the Internet, using a third party for certificate services may be preferable. See *Obtain and Install a Security Certificate* on page 2-16 for more information.

**NOTE:** The process of obtaining a third party security certificate may take several days. If secure password entry is required within SMARTsend, you should plan and initiate this activity in advance of your SMARTsend installation to avoid the need to reconfigure the computer and SMARTsend at a later time.

## Scanning Device and Application Migration

***Skip this section if network scanning applications are not currently in use within your organization.***

If other scanning applications or services are being used at your site, you should consider the various impacts that a new SMARTsend installation will have on your existing scanning resources. Consider the following factors when determining your migration strategy:

- SMARTsend cannot be installed on the same computer as Xerox FlowPort.
- The SMARTsend computer cannot be a domain controller.
- SMARTsend can import templates that were created with CentreWare Network Scanning Services. See *Template Importer* on page 8-3 for additional information.
- Xerox Multifunction Devices cannot be configured for simultaneous use with both SMARTsend and CentreWare Network Scanning Services because each application must use the Default Repository. Therefore, each application must manage a different set of devices.
- During device configuration, SMARTsend overwrites the Default Repository and Template Pool scan settings of a Xerox Multifunction Device. If you have existing applications that use the Default Repository, reconfigure the device to use an Alternate Repository for those applications *before* configuring the device to use SMARTsend.

For example, to use a Xerox Multifunction Device with both FlowPort and SMARTsend, you must reconfigure the device to use an Alternate Repository for FlowPort *before* configuring the device with SMARTsend. Likewise, templates created using CentreWare Internet Services must also be modified if they currently utilize the Default Repository.

**TIP:** If any Xerox Multifunction Devices intended for use with SMARTsend are already configured for use with other scanning applications, then you should print and save a configuration sheet for those devices before you configure them for use with SMARTsend. The configuration sheet lists the current network scanning configuration, which may be useful in the future if the device needs to be reverted back to a previous configuration.

- If FlowPort and SMARTsend are configured in the same office environment on different computers, care must be taken to select the correct template at the device when using FlowPort or SMARTsend. Under these circumstances, the FlowPort computer should be assigned an alternate repository when configuring the Xerox Multifunction Device. Users must also ensure they select a SMARTsend template at the device when scanning. PaperWare (Professional Edition feature) users must select the SMARTsend PaperWare template.
- Beginning with Release 2.0, SMARTsend can process PaperWare forms (Professional Edition feature) that were created on other SMARTsend or Xerox Flowport computers. This option improves usability and extends the power of SMARTsend within the enterprise by effectively increasing the number of devices that can be used to initiate scan jobs from a single PaperWare cover sheet. See *Configure PaperWare Form Forwarding Settings* on page 4-40 for additional information.

## Network Configuration and Logistics

SMARTsend is a Web site designed to service multiple users simultaneously. The following factors may impact the ability to service SMARTsend users within your organization:

- Physical sites and network bandwidth, including such factors as the number and proximity of supported scanning devices, anticipated network traffic, availability of e-mail services for notifications, and workflow processing. Analyze these factors to determine the best location for the SMARTsend computer.
- Network configuration, security practices, and scanning device capabilities may limit the use of certain SMARTsend features. Some examples include:
  - If SMB is blocked on a router or is not available on a particular device, you will be limited to using FTP as the SMARTsend filing protocol.
  - If scanning devices are located on a different subnet, DNS must be properly configured and functional. See *Verifying the SMARTsend Computer DNS Configuration* on page 2-8 for more information.
  - If SNMP Broadcast is not enabled across routers, you will not be able to utilize the SMARTsend automated device discovery features.
  - If the SMARTsend workflow authentication features (private workflows, scan to my e-mail) will be used, the configured scanning devices must be in the same domain (or trusted domain) as the SMARTsend computer. The Xerox Multifunction devices must also support authentication, and authentication must be configured and enabled on each device.

Additional information concerning network and device configuration is provided throughout this guide. If problems are encountered after your installation, please refer to Chapter 7, *Problem Solving* for additional support information.

# SMARTsend Configuration Requirements

Computer configuration is the foundation for a successful SMARTsend installation. Please follow and confirm all the guidelines and requirements in this chapter before you install SMARTsend to ensure that the computer is properly configured to support SMARTsend. Detailed explanations and configuration details are provided in the sections following this checklist.

- ❑ For best performance, install SMARTsend on a dedicated computer with a minimum of a 1.0 GHz or faster CPU, at least 750 MB of free disk space, 512 MB RAM (1 GB or more is recommended), and a single network adapter (multiple adapters are not supported). The computer cannot be a domain controller.
- ❑ SMARTsend (Standard or Professional Editions) can be installed on the following platforms: Windows 2000 Server or Advanced Server (SP4 or later), Windows Server 2003 with all critical operating system software updates installed, or a Windows XP Professional computer (SP2 or later)..

**NOTE:** For large installations, multiple users, managing of many devices, a Windows 2000 or 2003 installation is recommended.

- ❑ SMARTsend may also be installed on any of the supported operating systems in conjunction with VMware (GSX Server version 3.2.0, Workstation 4.5) or Microsoft Virtual PC 2004/Virtual Server 2005.

**NOTE:** SMARTsend performance may degrade when it is run on a shared file/print server, or when using VMware or Microsoft Virtual PC/Virtual Server. Performance degradation is likely to be more significant when using SMARTsend Professional OCR features.

- ❑ TCP/IP must be enabled and functional.
- ❑ Confirm that the ports required for each supported protocol are not blocked by filtering at a switch, router, or firewall. See *TCP/IP Port Configuration* on page 2-29.
- ❑ If using DNS, it must be properly configured. If the PaperWare Form Forwarding options are used (Professional Edition), DNS must also be configured on all SMARTsend and FlowPort computers that will be receiving forwarded forms. See *Verifying the SMARTsend Computer DNS Configuration* on page 2-8 and *Configure PaperWare Form Forwarding Settings* on page 4-40.
- ❑ File and Printer Sharing must be enabled on the network adapter and port 139 must be available. See *Enable File and Printer Sharing* on page 2-9.
- ❑ Internet Information Services (IIS) 5.0, or higher, must be installed and configured with the Common Files, Internet Information Services Manager, and World Wide Web Service. If using FTP for filing, the FTP Server component must also be enabled. See *Install and Configure IIS / FTP* on page 2-10. Please note that IIS is part of the Windows operating system, and its components can be installed using the Windows Add/Remove Programs options.

**NOTE:** The SMARTsend installation program will install the .NET Framework if it is not present on the computer. However, IIS must be installed before the .NET Framework is installed on a Windows 2000 Server/Advanced Server, or on a Windows XP Professional computer. If the .NET Framework and IIS are currently installed on the computer and you are not certain if IIS was installed first, then these components should be uninstalled and reinstalled in the proper sequence.

- ❑ Confirm that the Default Web Site and the FTP server are running under IIS before using SMARTsend.
  - ❑ Confirm that the Windows Authentication Methods are properly configured in IIS before installing SMARTsend. Integrated Windows authentication is always required, and Basic Authentication is also needed when Windows 95/98/Me clients and non-Microsoft browsers are used with SMARTsend. See *Windows Authentication Methods Configuration* on page 2-11.
  - ❑ ASP.NET must be enabled (*Windows Server 2003 only*). See *Enable ASP.NET* on page 2-12.
- ❑ If SMARTsend is being installed on a Windows XP Professional computer, then Simple File Sharing must be disabled. Please consult the Microsoft web site, [www.microsoft.com](http://www.microsoft.com), for Simple File Sharing configuration instructions.
- ❑ SMARTsend administrator, user, and device accounts must be configured. See *Create Administrator, User, and Device Accounts* on page 2-13.
- ❑ If secure password entry is required, a security certificate must be installed (*Optional*). See *Obtain and Install a Security Certificate* on page 2-16.
- ❑ Additional configuration is required to manage the SMARTsend computer as a secure web site. See *Secure Web Site Configuration* on page 9-3.
- ❑ Additional configuration is required on the SMARTsend computer when using Domino.doc, SharePoint Portal Server 2001, SharePoint Portal Server 2003, Novell NetWare, Remote Printers, DocuShare, and other optional destinations. See *Additional Requirements for Destinations* on page 2-19.

## SMARTsend Computer Configuration Requirements

The following table summarizes the key configuration requirements and options that must be addressed for a successful install.

| SMARTsend Computer Configuration Requirements   | Windows 2000 Server/Advanced Server   | Windows Server 2003  | Windows XP Professional   |
|---|---|--|---|
| <b>Minimum Hardware:</b><br>1.0 GHz CPU, 750 MB free disk space, 512 MB RAM, single network adapter.                                  |    |    |    |
| SMARTsend computer can be used as a Domain Controller   |    |    |    |
| SMARTsend software can be installed with VMware (GSX Server version 3.2.0, Workstation 4.5) or MS Virtual PC 2004/Virtual Server 2005 |    |    |    |
| Enable TCP/IP support   |    |    |    |
| Confirm ports are available for each required protocol (FTP, SMB, HTTP, HTTPS)  |    |    |    |
| Install Internet Information Services 5.0+ with common files, IIS Manager, and World Wide Web Service.                                |   |   |   |
| Confirm that .NET Framework is installed <u>after</u> IIS is installed.   |  | Not Applicable   |  |
| Enable FTP Server   | Optional  | Optional   | Optional  |
| Enable Integrated Windows Authentication  |  |  |  |
| Enable ASP.NET  |  |  |  |
| Enable File and Printer Sharing   |  |  |  |
| Disable Simple File Sharing   | Not Applicable  | Not Applicable   |  |
| Create administrator and user accounts  |  |  |  |
| Install security certificate  | Optional  | Optional   | Optional  |
| Configure secure web site   | Optional  | Optional   | Optional  |
| Configure destinations...<br>(requirements vary)  |  |  |  |

Table 2-1: SMARTsend Computer Configuration Requirements Summary

## Verifying the SMARTsend Computer DNS Configuration

SMARTsend requires a valid DNS configuration to locate scanning devices or other computers when multiple subnets are involved. If the PaperWare Form Forwarding options are used (Professional Edition), DNS must also be configured on all SMARTsend and FlowPort computers that will be receiving forwarded forms. See *Configure PaperWare Form Forwarding Settings* on page 4-40 for additional information.

**NOTE:** Use of DNS is optional if SMARTsend and the scanning devices reside on a single subnet. If this is the case, you can use WINS or the device IP Address instead of DNS, and the following DNS verification procedures can be ignored. However, when DNS is used, DNS configuration issues must be resolved prior to installing and configuring SMARTsend.

### ► To verify the local DNS configuration:

- 1 Use *ipconfig* to verify that the IP addresses of the DNS servers are listed correctly and in the proper order.
  - a) Open the command prompt
  - b) Type *ipconfig /all*
  - c) Confirm that the DNS servers are listed properly
- 2 Use *nslookup* to verify SMARTsend computer and Xerox Multifunction Device network connectivity and name resolution.
  - a) Open the command prompt
  - b) Type *nslookup*
  - c) Enter the IP Address for the SMARTsend computer. The Host Name should be returned.
  - d) Next, enter the fully-qualified Host Name for the SMARTsend computer. The IP Address obtained from the previous step should be returned.
  - e) Repeat steps a-d using the IP Address and fully-qualified Host Name of the devices that you intend to configure for use with SMARTsend.

**NOTE:** If *nslookup* fails, there is a network connectivity issue that should be resolved before installing SMARTsend. If the IP address lookup succeeds and the DNS name lookup fails, check the DNS name resolution configuration. Likewise, if the Host Name lookup does not return the exact same result as the IP Address lookup, you should check the DNS name resolution configuration. Apply DNS name resolution changes as needed, then retest using *nslookup* to verify the DNS configuration.

## Enable File and Printer Sharing

The SMARTsend computer must be configured to enable File and Printer Sharing for Microsoft Networks and port 139 must be available. Use the following procedure to configure File and Printer Sharing on the SMARTsend computer.

**NOTE:** The following sample procedure is based on a Windows 2000 Server.

### ► To Configure File and Printer Sharing for Microsoft Networks:

- 1 On the SMARTsend computer, click **Start > Settings > Control Panel**.
- 2 Open the **Network Connections** option.
- 3 Right-click the appropriate network adapter and select **Properties**.
- 4 Select the option for **File and Printer Sharing for Microsoft Networks**. This option is enabled by default.
- 5 Click **OK** to save any changes.

## Install and Configure IIS / FTP

SMARTsend has several Microsoft Internet Information Services (IIS) installation and configuration dependencies. These dependencies must be addressed to ensure proper site configuration and reliable service for SMARTsend users. Please note that IIS is part of the Windows operating system, and its components can be installed using the Windows Add/Remove Programs options. Consult the Microsoft web site, [www.microsoft.com](http://www.microsoft.com), for additional IIS installation and configuration instructions.

**NOTE:** IIS must be installed before the .NET Framework is installed on a Windows XP Professional computer or Windows 2000 Server/Advanced Server. The SMARTsend installation program will install the .NET Framework if it is not present on the computer, but it cannot detect the order in which these applications were installed. If the .NET Framework and IIS are currently installed on the computer and you are not certain if IIS was installed first, then these components should be uninstalled and reinstalled in the proper sequence.

### General IIS Installation Requirements

Internet Information Services (IIS) 5.0, or higher, must be installed and configured with the following components or options enabled and running:

- Common Files**—Installs required IIS program files.
- Internet Information Services Manager**—Installs the IIS administrative interface into Microsoft Management Console.
- World Wide Web Service**—Uses the HTTP protocol to respond to Web client requests on a TCP/IP network.
- FTP Server (optional)**—Used to support FTP data transfer between the SMARTsend computer and configured scanning devices when the FTP filing protocol is selected. This component is not a part of the default IIS installation; it must be selected during the initial installation procedure or added to the installation afterwards.

**NOTE:** FTP support is required if the devices to be used with SMARTsend do not support SMB, HTTP, or HTTPS, or in cases where the use of these additional protocols is restricted on your network. In addition, if FTP is installed after SMARTsend is installed, please refer to the topic *SMARTsend does not recognize IIS FTP service* on page 7-4 for additional configuration instructions.

### FTP Service Directory Configuration

Devices that support FTP as a transfer protocol interpret FTP file path information according to UNIX conventions. The directory listing style of the Internet Information Services FTP Server must be configured to use UNIX style listings. (*NOTE: The following sample procedure is based on a Windows 2000 Server.*)

► *To change the FTP Home Directory style to UNIX and check read/write permissions:*

- 1 Open the Internet Information Services Manager (**Start > Programs > Administrative Tools > Internet Services Manager**) and expand IIS in the tree view.
- 2 Right-click **Default FTP Site** and select **Properties**.
- 3 Select the **Home Directory** tab and select **UNIX** as the Directory Listing Style.
- 4 Confirm that both **Read** and **Write** are checked.

- 5 Click **OK** on all screens.

## Windows Authentication Methods Configuration

SMARTsend requires proper configuration of the Internet Information Services (IIS) authentication options. These options should be configured and confirmed before the SMARTsend application is installed.

► *To configure Windows Authentication on the SMARTsend computer:*

- 1 If SMARTsend is installed on a Windows 2000 Server/Advanced Server:  
Click **Start > Settings > Control Panel > Administrative Tools > Internet Services Manager**.  
- OR -  
If SMARTsend is installed on a computer running Windows Server 2003 or Windows XP Professional:  
Click **Start > Control Panel > Administrative Tools > Internet Information Services**.
- 2 Expand IIS in the tree view.
- 3 Right-click **Default Web Site** and choose **Properties**.
- 4 Select the **Directory Security** tab.
- 5 Click **Edit** in the *Anonymous access and authentication control* section.
- 6 Select the **Integrated Windows Authentication** check box.
- 7 If Windows 95/98/Me clients or non-Microsoft browsers will be used with SMARTsend, then you should also select the **Basic Authentication** check box.
- 8 Click **OK** on all screens.

## Enable ASP.NET

*Applicable to Windows Server 2003 installations only.*

When SMARTsend is installed to run under Windows Server 2003, ASP.NET must be enabled and properly configured on the server. Please consult the Microsoft web site, [www.microsoft.com](http://www.microsoft.com), for ASP.NET installation and configuration instructions.

**NOTE:** Additional ASP.NET configuration changes are required if the server has been upgraded to Windows Server 2003 from a previous installation of Windows 2000 Server or Advanced Server. When this is the case, the ASP.NET account must be granted execute permission to any files under wwwroot. To implement this change on your Windows 2003 server, open the **wwwroot Properties** dialog, then select the **Security** tab. Next, select the account for **Everyone**, then select the checkbox to **Allow Read & Execute**. Click **Apply** to save the changes, then click **OK** as needed to close the configuration dialogs.

## Create Administrator, User, and Device Accounts

SMARTsend administrators, users, and the Xerox Multifunction Devices used with SMARTsend must be authenticated with a valid Windows account in order to obtain access to the SMARTsend computer. The Windows system that hosts SMARTsend can either be a standalone system or a member of a domain, but it cannot be a domain controller.

Consider the following issues when determining your site-specific requirements for SMARTsend accounts:

- All members of the Administrator group on the SMARTsend computer have SMARTsend administrative privileges while all members of the Users group have SMARTsend user privileges. The computer administrator can use the Microsoft Management Console (MMC) Computer Management snap-in to create, view, or modify the accounts that provide access to the SMARTsend computer. See *Account Creation and Management* on page 2-14 for instructions.
- If you install the SMARTsend on a standalone computer, on a network that does not use a domain, or where users are outside of the domain (or its trusted domains), then you must create local accounts for the SMARTsend administrators and users.

**NOTE:** When SMARTsend is installed on a computer which is not a member of a domain, it is recommended that a full backup be made of the host computer after users have been created via MMC. In the event of a system crash, such as a hard drive failure, the computer should be restored from this full backup. This will ensure that user accounts in SMARTsend will continue to match those on the standalone computer.

- If you configure the SMARTsend computer as a member of a domain or trusted domain, then the domain security group (Domain Users) joins the computer's Users group by default. If you take no further action, all domain members will have access to the SMARTsend site in accordance with their existing domain privileges. The domain account provides authorized users with access to resources within the domain and any trusted domains. If needed, local accounts can also be added manually.
- When devices are configured within SMARTsend, local user Device Accounts are automatically created on the SMARTsend computer for each supported protocol. In most cases, no further configuration is required for Device Accounts. See *Manage Device Accounts* on page 4-15 for additional information.

## Account Creation and Management

The following procedures describe the use of Microsoft Management Console (MMC) for creating and managing SMARTsend administrator, user, and device accounts.

**NOTE:** The sample procedures in this section are based on a Windows 2000 Server. Individual steps and step names may vary slightly for Windows Server 2003 or Windows XP Professional.

### *Creating Local User or Administrator Accounts*

► *To create local user or administrator accounts:*

- 1 Open **Control Panel > Administrative Tools > Computer Management**.
- 2 Expand **Local Users and Groups**, then right-click the **Users** folder and select **New User**.
- 3 Enter the account information and choose the appropriate options.
- 4 Click **Create**.
- 5 Click **Close**.

### *Managing Local Access to SMARTsend*

► *To manage local access to SMARTsend:*

- 1 Open **Control Panel > Administrative Tools > Computer Management**.
- 2 Expand **Local Users and Groups**, then select the **Groups** folder.
- 3 Right-click **Users** or **Administrators** in the right panel, then select **Properties**.
- 4 Click **Add**, then select the user(s) or group(s) you want to have access to SMARTsend. Keep in mind that any User or Group added to the Administrators group will have administrative access to SMARTsend.
- 5 Click **OK** as needed to confirm the changes and close the dialogs.

**NOTE:** Membership in the Users or Administrators group is required to access the SMARTsend site. Only members of the Administrators group can be SMARTsend administrators.

### *Managing SMARTsend Access Within a Domain*

► *To manage SMARTsend access within a domain:*

- 1 Open **Control Panel > Administrative Tools > Computer Management**.
- 2 Expand **Local Users and Groups**, then select **Groups**.
- 3 Right-click **Users** in the right panel, then select **Properties**.
- 4 In the **Members** list, select the **Domain Users** group and then click **Remove**.
- 5 Add either single domain users or domain groups to the **Users** group as needed to provide access to the SMARTsend site.

- 6 Click **OK** as needed to confirm the changes and close the dialogs.

**NOTE:** Follow the same steps to limit Administrator access in the local Administrators group so that all members of the Domain Admins group do not have administrator access to the SMARTsend site.

### *Creating SMARTsend Device Accounts*

This is an optional procedure. See *Manage Device Accounts* on page 4-15 for additional information.



*To create SMARTsend device accounts:*

- 1 Follow the procedures for *Account Creation and Management* on page 2-14 to create a **Local User Account** for the Xerox Multifunction Devices that will be used with SMARTsend.

**NOTE:** Be sure to record and properly label the SMARTsend device account name and password when you create the account. You will be required to enter this information at a later time when you perform the site configuration tasks presented in *Add/Update Xerox Devices* on page 4-8.

- 2 Expand **Local Users and Groups**, then select the **Groups** folder.
- 3 Right-click **Users** in the right panel, then select **Properties**.
- 4 Inspect the **Member** list. If the SMARTsend Device Account is in the Users group, select the account and click **Remove**.
- 5 Click **OK**.
- 6 Right-click **Administrators** in the right panel, then select **Properties**.
- 7 Inspect the **Member** list. If the SMARTsend Device Account is in the Administrators group, select the account and click **Remove**. A device account should not have administrative privileges because it could pose a security risk.
- 8 Click **OK** as needed to confirm the changes and close the dialogs.

## Obtain and Install a Security Certificate

*Skip this section if secure password entry and communication is not required.*

A security certificate may be obtained by submitting a certificate request to a Certificate Authority (CA) and installing the returned certificate. This section assumes that Microsoft Certificate Services is installed on a computer within a network domain, with the role of Root CA. It includes the processes of creating the request file and submitting it to a certificate server. The examples and procedures in this section may vary with other configurations and certificate services. For detailed information on related SMARTsend security issues and secure configuration options, please refer to *HTTPS/SSL Certificates* on page 9-3.

**NOTE:** A SelfSSL option is available in the Microsoft Internet Information Services (IIS) Resource Kit. Go to <http://www.microsoft.com/downloads> for additional information.

The following information will be required as you obtain the certificate:

- **The "friendly" name of the new certificate.** This is a short, easily recognizable name like "Scanning Computer."
- **The bit length of the encryption key.** Longer keys are more secure; shorter keys have less impact on performance.
- **The "common name" of the site being secured.** This is either the fully qualified DNS name or NetBIOS name. Sites that appear on the Internet should use the fully qualified DNS name.
- **Location information.** This includes company, department, city, state, and country.

### Preparing a Certificate Request File

► **To prepare a certificate request file:**

The following instructions assume that you have already accessed the IIS management console on the computer where SMARTsend will be installed.

- 1 Right-click the IIS Default Web Site or IIS site where SMARTsend is or will be installed. Select **Properties**.
- 2 Select the **Directory Security** tab.
- 3 Click **Server Certificate**.
- 4 The Server Certificate Wizard window appears. Click **Next**.
- 5 Select **Create a new certificate**. Click **Next**.
- 6 Select **Prepare the request now, but send it later**. Click **Next**.
- 7 Enter the "friendly" name for the new certificate. Select the bit length if a different bit length is desired. Click **Next**.
- 8 Enter the organization name and unit. Click **Next**.
- 9 Enter the site's common name. Sites on the Internet should use their fully qualified DNS names; local (intranet) sites may use the computer's NetBIOS name. Click **Next**.

**NOTE:** SMARTsend will not be able to function properly under SSL if the Host Name on the certificate does not match the fully qualified computer name.

- 10 Enter the site's country, state or province, and city. Click **Next**.
- 11 Enter a file name for the certificate request. It will be a text (.txt) file. Click **Next**.

**NOTE:** Record the name and location of the certificate request file for later use.

- 12 The Request File Summary appears. Review the entries. Click **Back** to make corrections or **Next** to continue.
- 13 Click **Finish** to end the wizard. You have created but not submitted a certificate request file.

## Submitting a Certificate Request

► *To submit the file to the Certificate Authority (CA):*

- 1 Open your browser and enter the certificate server URL.
- 2 Select **Request a certificate**.
- 3 Select **Advanced request**.
- 4 Select **Submit a certificate request by using a base64-encoded CMC or PKCS #10 file or a renewal request by using a base64-encoded PKCS #7 file**.
- 5 Click the **Browse** link to find your certificate request file and open it. Click **Read** to load the file. The file contents should appear in the Saved Request field. Click **Submit**.

**NOTE:** Using the Browse link may not work if local security settings prohibit browser access to the disk on which the certificate request file resides. Alternatives to the Browse link include opening the request file in Notepad and performing a copy and paste to the Saved Request field, or making the CA server a trusted site in Internet Explorer.

- 6 The Certificate Issued page appears. If desired, you can change the Certificate Encoding (DER or Base 64) and the download options (download certificate or download certificate chain).
- 7 After choosing the certificate options, click the **Download Certificate** link. The File Download window appears and displays the name of your certificate (.cer) file. Click **Save** to save the file to a local folder. Be sure to note the location of this file for later use.

## Installing the Security Certificate

► *To install the security certificate:*

- 1 Return to the IIS Default Web Site, or the IIS site where SMARTsend will be installed, and then go to the **Properties** page in the IIS management console. Select the **Directory Security** tab.
- 2 Click **Server Certificate**.
- 3 The Web Server Certificate Wizard opens. Click **Next**.
- 4 The wizard detects the pending request and offers options to process or delete it. Select **Process the pending request and install the certificate**. Click **Next**.
- 5 Enter the location and name of the .cer file. Click **Next**.

- 6 Specify the SSL Port for this web site. Click **Next**.
- 7 The wizard presents a certificate summary based on the .cer file. Click **Next**.
- 8 A completion window displays. Click **Finish**.
- 9 Click **OK** to exit the Web Site Properties page.
- 10 Close the IIS management console window.

Your security certificate is installed. You may now use secure password entry with SMARTsend.

**NOTE:** See *Secure Web Site Configuration* on page 9-3 if you need to configure the SMARTsend computer for secure data transmission.

## Replacing a Security Certificate

The currently installed security certificate must be deleted before a security certificate can be replaced on the SMARTsend computer. Use the following instructions to delete a currently installed security certificate.

► *To replace a security certificate:*

- 1 Launch Microsoft Management Console on the SMARTsend computer.
- 2 Select **File > Add/Remove Snap-In**.
- 3 Select the **Standalone** tab on the Add/Remove Snap-in dialog.
- 4 Click **Add**.
- 5 Select **Certificates** on the Add Standalone Snap-in dialog.
- 6 Click **Add**.
- 7 Select **Computer** account at the Certificates snap-in dialog.
- 8 Click **Next >**.
- 9 Select **Local Computer** at the Select Computer dialog.
- 10 Click **Finish**.
- 11 Close the Add Standalone Snap-in dialog.

You should now be able to view and remove certificates.

## Additional Requirements for Destinations

*Skip this section if the destinations listed below are not required.*

Some SMARTsend destinations require the installation of a client or other software on the SMARTsend computer in order for the destination to function properly. These software requirements apply to the following scanning destinations:

- Domino.Doc destinations require the "Document Manager Desktop Enabler" (version 3.1 or later) to be installed on the SMARTsend computer. Access the home page on your Domino.doc server, then choose the Getting Started link. You can then choose the Download Document Manager Desktop Enabler link.
- If DocuShare or SharePoint Portal Server 2003 destinations will be accessed through an HTTP proxy server, then the SMARTsend computer registry must be customized. See *DocuShare and SharePoint Portal Server 2003 Access via HTTP Proxy Servers* on page 7-11.
- If SMARTsend is installed on a Windows 2000 Server/Advanced Server and it is supporting Microsoft SharePoint Portal Server 2001 destinations, then the SharePoint Portal Server 2001 client from the Microsoft web site must be installed on the SMARTsend computer. See *SharePoint Portal Server 2001 Compatibility with Windows Server 2003* on page 7-10.
- Novell NetWare folder destinations require the Novell Client for NetWare version 4.83 SP1 or later from either the Novell NetWare Client CD or the Novell Web site, [www.novell.com](http://www.novell.com).
- Optional destinations, such as Documentum, Hummingbird, and Interwoven, require the corresponding client software for each product to be installed on the SMARTsend computer. If you have purchased and installed any of these optional SMARTsend components (Standard or Professional Editions), please follow the client installation instructions provided with each product.
- LiveLink (Standard or Professional Editions) destinations require the purchase of the LiveLink SDK and the installation of four LiveLink SDK files. If you have purchased the LiveLink SDK, please review *LiveLink Configuration Requirements* on page 3-11 for additional information.
- Microsoft Office 2000, XP or 2003 must be installed and configured as an interactive user on the SMARTsend computer if Office documents (Word, Excel, PowerPoint, etc.) will be submitted to a Remote Printer destination. See *Configuring Microsoft Office as an Interactive User* on page 2-20 for additional information.
- Remote Printer destinations require the installation of a printer driver on the SMARTsend computer for each remote printer. See *Installing a Printer Driver for a Remote Printer Destination* on page 2-24 for additional information.

## Configuring Microsoft Office as an Interactive User

Use the following procedures to configure Microsoft Office as an interactive user to support distribution of Office documents to Remote Printer destinations. Please note that separate procedures are included for Windows 2000 Server and Windows Server 2003/XP Professional.

**NOTE:** The SMARTsend application must be installed prior to configuring Microsoft Office as the Interactive User.

### *Windows 2000 Server - Microsoft Office Interactive User Configuration Instructions*

To set up an Office Automation server under the interactive user account, follow these steps:

- 1 Log on to the computer as the Administrator and install (or reinstall) Office using a complete installation. For system robustness, it is recommended that you copy the contents of the Office CD-ROM to a local drive and install Office from this location.
- 2 Start the Office application that you intend to automate. This forces the application to register itself.
- 3 After the application is running, press **ALT+F11** to load the Microsoft Visual Basic for Applications (VBA) editor. This forces VBA to initialize itself.
- 4 Close the applications, including VBA.
- 5 Click **Start > Run**, and then type **DCOMCNFG**.
- 6 Select the application that you want to automate. The application names are listed below:  
Microsoft Excel 2000/2002/2003 - Microsoft Excel Application  
Microsoft Word 2000/2002/2003 - Microsoft Word Document  
Click **Properties** to open the property dialog box for each application.

**NOTE:** If you get a DCOM configuration warning to register clsid, go ahead and record it.

- 7 Click the **Security** tab. Verify that **Use Default Access Permissions** and **Use Default Launch Permissions** are selected.
- 8 Click the **Identity** tab and then select **The Interactive User**.
- 9 Click **OK** to close the property dialog box and return to the main applications list dialog box.
- 10 In the DCOM Configuration dialog box, click the **Default Security** tab.
- 11 Click **Edit Defaults** for access permissions. Verify that the following users are listed in the access permissions, or add the users if they are not listed:  
SYSTEM  
INTERACTIVE  
Everyone  
Administrators  
FF\_SMARTSEND\_USER  
IUSR\_<machinename>\*

IWAM\_<machinename>\*

\* These accounts only exist if Internet Information Server (IIS) is installed on the computer.

**NOTE:** You may have to click 'show users' to show some of the above accounts

- 12 Make sure that each user is allowed access and click **OK**.
- 13 Click **Edit Defaults** for launch permissions. Verify that the following users are listed in the launch permissions, or add the users if they are not listed:
  - SYSTEM
  - INTERACTIVE
  - Everyone
  - Administrators
  - FF\_SMARTSEND\_USER
  - IUSR\_<machinename>\*
  - IWAM\_<machinename>\*

\* These accounts exist only if IIS is installed on the computer.
- 14 Make sure that each user is allowed launch access, and then click **OK**.
- 15 Click **OK** to close DCOMCNFG.
- 16 Start REGEDIT and verify that the following keys and string values exist for the Office application that you want to automate:
  - Microsoft Excel 2000/2002/2003:**
    - Key: HKEY\_CLASSES\_ROOT\AppID\EXCEL.EXE
    - AppID: {00020812-0000-0000-C000-000000000046}
  - Microsoft Word 2000/2002/2003:**
    - Key: HKEY\_CLASSES\_ROOT\AppID\WINWORD.EXE
    - AppID: {00020906-0000-0000-C000-000000000046}

If these keys do not exist, you can create them by running the following .reg file on your system:

```
REGEDIT4
[HKEY_CLASSES_ROOT\AppID\WINWORD.EXE]
"AppID"="{00020906-0000-0000-C000-000000000046}"
[HKEY_CLASSES_ROOT\AppID\EXCEL.EXE]
"AppID"="{00020812-0000-0000-C000-000000000046}"
```
- 17 Restart the system. This is required.

*Windows Server 2003 and XP Professional - Microsoft Office Interactive User Configuration Instructions*

To set up an Office Automation server under the interactive user account, follow these steps:

- 1 Log on to the computer as the Administrator and install (or reinstall) Office using a complete installation. For system robustness, it is recommended that you copy the contents of the Office CD-ROM to a local drive and install Office from this location.
- 2 Start the Office application that you intend to automate. This forces the application to register itself.
- 3 After the application is running, press **ALT+F11** to load the Microsoft Visual Basic for Applications (VBA) editor. This forces VBA to initialize itself.
- 4 Close the applications, including VBA.
- 5 Go to **Administrative Tools > Component Services > Computers > My Computer > DCOM Config**. The application names are listed below:  
Microsoft Excel Application  
Microsoft Word Document  
Perform the following steps for each of the above applications:

**NOTE:** If you get a DCOM configuration warning to register clsid, go ahead and record it.

- 6 Right-click the Application and select **Properties**.
- 7 Click the **Identity** tab and then select **The Interactive User**.
- 8 Select the **Security** tab.
- 9 Select **Customize > Select Edit** for access permissions. Verify that the following users are listed in the access permissions, or add the users if they are not listed:  
SYSTEM  
INTERACTIVE  
Everyone  
Administrators  
FF\_SMARTSEND\_USER  
IUSR\_<machinename>\*  
IWAM\_<machinename>\*  
\* These accounts only exist if Internet Information Server (IIS) is installed on the computer.
- 10 Make sure that each user is allowed local access and click **OK**.
- 11 Select **Customize > Select Edit** for launch permissions. Verify that the following users are listed in the launch permissions, or add the users if they are not listed:  
SYSTEM  
INTERACTIVE  
Everyone  
Administrators

FF\_SMARTSEND\_USER

IUSR\_<machinename>\*

IWAM\_<machinename>\*

\* These accounts exist only if IIS is installed on the computer.

- 12 Make sure that each user is allowed local launch and activation access, and then click **OK**.
- 13 Click **OK** to close the Properties Page. Exit Component Services.
- 14 Start **REGEDIT** and verify that the following keys and string values exist for the Office application that you want to automate:

**Microsoft Excel 2000/2002/2003:**

Key: HKEY\_CLASSES\_ROOT\AppID\EXCEL.EXE

AppID: {00020812-0000-0000-C000-000000000046}

**Microsoft Word 2000/2002:**

Key: HKEY\_CLASSES\_ROOT\AppID\WINWORD.EXE

AppID: {00020906-0000-0000-C000-000000000046}

**Microsoft Word 2003:**

Key: HKEY\_CLASSES\_ROOT\AppID\WINWORD.EXE

AppID: {F04CCF7B-0D4A-43E3-816A-193163BCAA49}

If these keys do not exist, you can create them by running the following .reg file on your system:

```
REGEDIT4
```

```
[HKEY_CLASSES_ROOT\AppID\WINWORD.EXE]
```

```
"AppID"="{00020906-0000-0000-C000-000000000046}"
```

Note: The sample .reg file is for Word 2000 or Word 2002. If you are using Word 2003, change the AppID key to:

```
"AppID"="{F04CCF7B-0D4A-43E3-816A-193163BCAA49}"
```

```
[HKEY_CLASSES_ROOT\AppID\EXCEL.EXE]
```

```
"AppID"="{00020812-0000-0000-C000-000000000046}"
```

- 15 Restart the system. This is required.

## Installing a Printer Driver for a Remote Printer Destination

► *To install a printer driver for a Remote Printer destination:*

- 1 Make sure you are logged on to the SMARTsend computer as a user with administrative privileges. The network user account should be on the local network on which network printer is connected.
- 2 Open the Windows Add Printer wizard. Click **Next**.
- 3 Select **Local printer attached to this computer**, then click **Next**.
- 4 The Select a Printer Port dialog appears. Select the **Create a new port**, and then choose **Standard TCP/IP Port** as the port type. Click **Next**.
- 5 The Add Standard TCP/IP Printer Port Wizard appears. Click **Next**.
- 6 Enter the **Printer Name or IP address**. The Port Name will be filled in automatically (do not change this name). Click **Next**.
- 7 If necessary, select or enter Additional Port information, then click **Next**.
- 8 Click **Finish** to close the Add Standard TCP/IP Printer Port Wizard.
- 9 In the Add Printer Wizard, select a printer manufacturer and corresponding printer model from the list, or click **Have Disk...** to locate the driver you would like to install. Click **Next**.
- 10 Enter or confirm the Printer Name, and select a Default Printer option. Click **Next**.
- 11 In the Printer Sharing dialog, select **Share Name** and enter the name for the printer. Click **Next**.
- 12 Enter a location and comment, if needed. Click **Next**.
- 13 Print a test page, if needed. Click **Next**.
- 14 Click **Finish** to complete driver installation.

## Client and Browser Configuration

Confirm and test the following client and browser requirements prior to installing and using SMARTsend:

- ❑ Microsoft Internet Explorer version 5.5 or higher. (*Internet Explorer is recommended for best performance.*)
- ❑ Netscape version 7.2 or higher.
- ❑ Mozilla version 1.7 or higher.
- ❑ Mozilla FireFox version 1.0.6 or higher.
- ❑ If you are running SMARTsend on an intranet, the browser must be configured to include the SMARTsend computer in the proxy server exceptions list. See *Modifying Proxy Server Settings*.
- ❑ Popup blockers should be disabled or reconfigured to bypass or exclude SMARTsend. Popup blocking software will prevent certain SMARTsend screens from displaying.
- ❑ If using a multinational version of SMARTsend, the browser language setting must be configured to match the desired language. See *Language Settings* on page 2-27.
- ❑ Adobe Acrobat Reader version 4.0 or higher is required for viewing and printing PaperWare cover sheets (Professional Edition feature) and the SMARTsend documentation.

Additional information is provided in the following sections. The SMARTsend administrator should test and confirm these settings before propagating any configuration changes to each client workstation.

### Modifying Proxy Server Settings

When a proxy server is used to connect to the Internet, SMARTsend requires changing browser settings to prevent the proxy server from interfering with SMARTsend authentication. In general, this is done by setting the browser to bypass the proxy server when searching for any local IP address, by adding the SMARTsend computer IP address and fully qualified Host Name to an exception list, or by a combination of the two.

**NOTE:** Procedures and options vary with each browser type and version. For example, you may need to enter the specific IP Address AND the fully qualified Host Name of the SMARTsend computer to the proxy server exceptions list in some versions of Internet Explorer. Please consult the documentation provided with your browser for specific requirements and procedures.

#### ► To modify proxy server settings in Internet Explorer:

- 1 Select **Tools > Internet Options**.
  - 2 Select the **Connections** tab, then click **LAN Settings**.
  - 3 If **Use a proxy server** is selected, select **Bypass proxy server for local addresses**. If a proxy server is not being used, you do not need to continue with this procedure.
  - 4 Click **Advanced**.
  - 5 Enter the SMARTsend computer IP address and/or fully qualified Host Name in the Exceptions list.
  - 6 When finished, click **OK** on all screens.
- OR -
- 1 Select **Tools > Internet Options**.
  - 2 Select the **Security** tab, then click **Local Intranet**.
  - 3 Click **Sites**.

- 4 Click **Advanced** and add the SMARTsend computer IP address and/or fully qualified Host Name to the zone.
- 5 When finished, click **OK** on all screens.

► **To modify Proxy Server settings in Netscape and Mozilla:**

- 1 Open Netscape/Mozilla.
- 2 Access the Edit menu and select **Preferences**.
- 3 Select **Advanced > Proxies**.
- 4 Select **Manual Proxy Configuration** and enter the proxy server host name or IP address for each protocol supported. Enter the port number for each protocol in its Ports field.
- 5 Add the SMARTsend computer Host Name and/or IP address to the **No Proxy for** field. Separate multiple entries with commas.
- 6 Click **OK** to save all settings.

## User Authentication Settings

If the SMARTsend site authenticates users with their network account credentials, the site login process will not be encountered. Use the following procedure to make the SMARTsend site login mandatory. (*Example procedure is based on Windows XP Professional and Internet Explorer 6.0.*)

► **To require user authentication with Internet Explorer:**

- 1 From the Windows **Control Panel** or your browser **Tools** menu, select **Internet Options**.
- 2 Select the **Security** tab.
- 3 Select **Local Intranet**.
- 4 Click **Custom Level**.
- 5 Scroll to the Logon options for User Authentication and select **Prompt for user name and password**.
- 6 When finished, click **OK** on all screens.

**NOTE:** This login requirement, while configured in Internet Options, applies to Internet Explorer, Netscape, and Mozilla. Instructions may vary in different browsers and operating systems.

## Language Settings

**NOTE:** This information is only applicable for the multinational version of SMARTsend. If SMARTsend does not support the language that you selected, the application defaults to English.

### ► To set browser language support:

- 1 Confirm that the language in which SMARTsend should display appears in the following table.

| Language             | Language Specifier |
|----------------------|--------------------|
| Danish               | DA                 |
| Dutch                | NL                 |
| English              | EN                 |
| Finnish              | FI                 |
| French               | FR                 |
| German               | DE                 |
| Italian              | IT                 |
| Norwegian            | NO                 |
| Brazilian Portuguese | PT-BR              |
| Spanish              | ES                 |
| Swedish              | SV                 |

**Table 2-2: Supported Languages**

- 2 In Internet Explorer, select **Tools > Internet Options**. The Internet Options dialog box appears.
- 3 Select the General tab and click **Languages**. The Language Preference dialog box appears.
- 4 Languages and their specifiers appear in a scrolling window, with the specifier enclosed in square brackets. If you do not see your language listed, click **Add**. The Add Language screen appears. Select the language to add and click **OK**.
- 5 If the language you require is in the list, select the language and move it to the top of the list. Click **OK**.
- 6 When finished, click **OK** on all remaining screens.

# Scanning Device Configuration

SMARTsend provides several capabilities to discover and configure Xerox Multifunction Devices for use as SMARTsend scanning devices. For most configurations, SMARTsend can discover and configure devices with minimal administrator intervention. However, there are several configuration tasks which must be completed before using SMARTsend. These tasks may include configuring the network scanning options and filing protocols (FTP/SMB/HTTP/HTTPS) for the device, and configuring the account and credentials that the device requires to obtain access to the SMARTsend computer. In addition, if authentication is required for SMARTsend private workflows/Scan to My E-mail, then authentication must be supported, enabled, and configured on the device.

**NOTE:** Please consult the documentation provided with your Xerox device for additional information on configuring the device for network scanning.

## Xerox Multifunction Device Requirements

The following Xerox Multifunction Devices can be used with SMARTsend:

**NOTE:** An updated list of supported devices and device requirements is available from the Support & Drivers link on the Xerox web site at [www.xerox.com](http://www.xerox.com).

- ❑ Document Centre 265/255/240 (system software versions 18.6 or greater), 440/432/425/420 ST, 430/426 ST, 490/480/470/460 ST, or 555/545/535 ST
- ❑ WorkCentre Pro 65/75/90, 35/45/55, 32/40, 123/128, 165/175, C2128/C2636/C3545, 232/238/245/255/265/275
- ❑ Xerox 4110 Copier/Printer—subject to the following caveats:
  - Device discovery is not supported. The IP Address or Host Name must be entered manually.
  - Private templates are not supported because this device does not support network authentication.
  - Auto-refresh of templates is not supported. Users must select the Refresh button at the device user interface to update the template list.

The following configuration requirements apply to all Xerox Multifunction Devices that will be used with SMARTsend:

- ❑ TCP/IP must be enabled and properly configured.
- ❑ The Network Scanning Option must be enabled and properly configured.
- ❑ SMARTsend automatically creates several Windows accounts that are needed for device configuration. It also provides options to create and manage the device accounts manually. See *Create Administrator, User, and Device Accounts* on page 2-13 and *Manage Device Accounts* on page 4-15 for additional information.
- ❑ If authentication is required for private workflows/Scan to My E-mail, then authentication must be enabled and configured to authenticate users from the same domain or trusted domain as the SMARTsend computer. Please consult the documentation provided with your Xerox device for instructions on enabling and configuring authentication.
- ❑ During device configuration, SMARTsend overwrites the Default Repository and Template Pool scan settings of a Xerox Multifunction Device. If you have existing applications that use the Default Repository, reconfigure the applications and the device to use an Alternate Repository for those

applications *before* configuring the device to use SMARTsend. See *Scanning Device and Application Migration* on page 2-3 for additional information.

- ❑ A single Xerox Multifunction Device cannot use both CentreWare Network Scanning Services and SMARTsend. If existing CentreWare Network Scanning Services templates need to be utilized within SMARTsend, use the SMARTsend Template Importer to import the desired templates. See *Template Importer* on page 8-3.

**TIP:** If any Xerox Multifunction Devices intended for use with SMARTsend are already configured for use with other scanning applications, then you should print and save a configuration sheet for those devices before you configure them for use with SMARTsend. The configuration sheet lists the current network scanning configuration, which may be useful in the future if the device needs to be reverted back to a previous configuration.

## Data Transfer Protocols

SMARTsend can configure various scanning-related settings on Xerox Multifunction Devices, but it does not enable or change the data transfer protocol and option settings on the device or the SMARTsend computer. Check the following configuration settings prior to adding devices to SMARTsend:

- If FTP will be used for filing scan jobs, then the IIS FTP server must be installed and running. See *Install and Configure IIS / FTP* on page 2-10 for more information. This is the SMARTsend default.
- If SMB will be used for filing scan jobs, then SMB must be supported on the device. In addition, File and Printer Sharing for Microsoft Networks must be enabled on the Network Adapter on the SMARTsend computer. See *Enable File and Printer Sharing* on page 2-9 for instructions.
- If HTTP will be used for filing scan jobs, then HTTP must be supported and enabled on the device.
- If HTTPS will be used for filing scan jobs, then SSL/HTTPS must be supported and enabled on the device. In addition, the SMARTsend computer must have a security certificate installed.

**NOTE:** If you attempt to add a Xerox Multifunction Device to SMARTsend using a protocol that the device does not support, an alternate protocol will be used to configure the device. A status message will indicate which protocol SMARTsend is using for data transfer. See *Edit Device Configuration Defaults* on page 4-18 for additional information.

## TCP/IP Port Configuration

When configuring a device, SMARTsend uses the FTP, SMB, HTTP, and HTTPS ports that are defined on the SMARTsend computer. Following are the standard settings for each supported filing protocol:

| Protocol | TCP/IP Port |
|----------|-------------|
| FTP      | 21          |
| SMB      | 139         |
| HTTP     | 80          |
| HTTPS    | 443         |

**Table 2-3: Standard TCP/IP Ports**

Consider the following issues when configuring ports on your SMARTsend computer and Xerox devices:

- Confirm that the ports required for each supported protocol are not blocked by filtering at a switch, router, or firewall.
- Port (139) must be used for SMB filing.

- If non-standard ports are used on the SMARTsend computer, SMARTsend will configure the corresponding ports on the Xerox devices that will be used with SMARTsend.

**NOTE:** Some Xerox devices may not support non-standard ports. If this is the case for your device, reconfigure the SMARTsend computer to use a standard port and then reconfigure the device.

## Default Template Configuration

With the Professional Edition of SMARTsend, it is possible to use the Default scanning template on a Xerox Multifunction Device to process jobs that are scanned with a PaperWare cover sheet. This is a simple alternative to using the PaperWare template created by SMARTsend, but it is subject to the following configuration requirements and limitations:



**CAUTION:** Windows registry editing can pose serious risks if the changes are not implemented properly. Please perform a registry backup before proceeding. Consult the registry help system for registry backup instructions.

---

- The registry must be modified on the SMARTsend computer, as follows:
  - Click **Start > Run**, then type **regedit** and click **OK**.
  - Go to the following registry location:  
[HKEY\_LOCAL\_MACHINE\Software\Xerox\FreeFlowDDS\Settings\Install]
  - Right click on the Install folder to create a new "String Value." Name the new string value "ProcessDefaultTemplate," and set the value to True. (NOTE: the string value name is case sensitive.)
  - Close the registry.
  - If necessary, this change can be disabled by deleting the ProcessDefaultTemplate string value or setting the value to False.
- The device must be added to SMARTsend and properly configured for use with SMARTsend.
- The device Job Log must be enabled. For most devices, this setting can be accessed using CentreWare Internet Services (Properties > Services > Network Scanning > Default Template).
- The Default Filing Policy (for network scan templates) must be set to New Auto Generate or Rename New File. For most devices, this setting can be accessed using CentreWare Internet Services (Scan > Select Template > File Destinations > Edit > Filing Policy).
- The default template configuration settings can be confirmed or changed using CentreWare Internet Services, which can be accessed through a web browser. Simply enter the IP address of the Xerox Multifunction Device as the URL, then choose Properties > Services > Network Scanning > Default Template.
- The default glyph size that is printed on the PaperWare cover sheets requires a minimum scan resolution of 300 dpi. Therefore, the default resolution setting for the Default scanning template should be set to at least 300x300. For most devices, this setting can be accessed using CentreWare Internet Services (Properties>Services>Network Scanning> Default Template).

**TIP:** Be sure to inform SMARTsend users that the Default template can be used with PaperWare cover sheets. This option makes it simpler to scan because it eliminates the need to scroll through the list of templates on the device.

## Internet Fax and E-mail Enabled Device Requirements

The following Internet Fax and e-mail enabled devices can be used with SMARTsend Professional Edition via PaperWare cover sheets:

**NOTE:** An updated list of supported devices and device requirements is available from the Support & Drivers link on the Xerox web site at [www.xerox.com](http://www.xerox.com).

- ❑ E-mail enabled devices, including:
  - Xerox WorkCentre M20i
  - Xerox WorkCentre M118i
  - Xerox WorkCentre M24

**NOTE:** Due to the architecture of the e-mail feature on these devices, there may be certain scan file format restrictions associated with scanning from these devices. Please refer to *Caveats for E-mail Enabled Devices* on page 2-33 for additional information.

The same dedicated POP3 e-mail account that is created for the Internet Fax inbox on the incoming mail (POP3) server can be used for receiving e-mail from these devices. See *Configure PaperWare Internet Fax Settings* on page 4-24 for additional information.

- ❑ All Internet Fax devices that support RFC 2301 file format profiles S, F, or C, including:
  - Xerox WorkCentre Pro 685/785
  - Xerox WorkCentre Pro 416Si

The following configuration requirements apply to all Internet Fax devices:

- ❑ TCP/IP must be enabled and properly configured.
- ❑ A DNS Host Name, static IP address, or DHCP must be configured (*requirements vary by manufacturer*).
- ❑ Simple Mode Internet Fax must be available (Extended Mode is not supported by SMARTsend).
- ❑ A dedicated e-mail account must be created for the Internet Fax inbox, which is used by the SMARTsend computer.

Please consult the documentation provided by the Internet Fax device manufacturer for specific network configuration requirements.

## Caveats for E-mail Enabled Devices

Certain caveats apply when using PaperWare with the e-mail features provided by the following devices:

### *WorkCentre M20i*

- The file format must be set to TIFF because the PDF format emitted by the M20i is not compatible with SMARTsend.
- All scans must be sent in monochrome mode. In color mode, the M20i only generates single-page .jpg files that are not sufficient for PaperWare support.
- Since the M20i splits e-mails, SMARTsend will only process the first e-mail (since the PaperWare cover sheet is only in the first attachment). It is recommended that the maximum e-mail attachment size be set to 4 MB to minimize this occurrence.
- Printed confirmation sheets and the PaperWare "Refetch this form" feature do not work with the M20i since e-mail is used as the submission path.

### *WorkCentre M118i*

- Printed confirmation sheets and the PaperWare "Refetch this form" feature do not work with the M118i since e-mail is used as the submission path.
- The file format used may be PDF or MultiPage TIFF.

### *WorkCentre M24*

- The file format must be set to PDF. The M24 does not support multi-page TIFF for e-mail.
- Scans may be sent in color or monochrome.
- Printed confirmation sheets and the PaperWare "Refetch this form" feature do not work with the M118i since e-mail or Internet Fax is used as the submission path.

## Prepare Information for Installation

SMARTsend requires certain information for a successful installation and configuration. You can add or change most of the information from the SMARTsend Administration pages.

SMARTsend Administrator information

(Used to provide SMARTsend users with a point of contact for site administration and support. This information will appear on confirmation pages and other notifications.)

Telephone: \_\_\_\_\_

Name: \_\_\_\_\_

E-mail Address: \_\_\_\_\_

Mail (SMTP) server fully qualified DNS name or IP address

(Used for Scan to E-Mail, scan job confirmations, administrative event notifications, and configuration messages.)

DNS name or IP Address: \_\_\_\_\_

Application "Reply To" e-mail account address

(This Reply To information appears in the Reply to field of e-mail confirmation messages and error notifications. See *SMTP Server Configuration* on page 4-25 and *General Settings* on page 4-35 for more information.)

"Reply To" address: \_\_\_\_\_

LDAP server fully qualified DNS name or IP address

(Used for the integrated address book e-mail address lookup features.)

DNS name or IP Address: \_\_\_\_\_

Password for MSDE database access

(This password is required for configuration of the MSDE database that SMARTsend creates. It is only used by SMARTsend. Administrators and users do not need to use this password at any time other than the initial installation.)

Password: \_\_\_\_\_

Application path, if different from default (*path cannot be changed after installation*)

Path: \_\_\_\_\_

SMARTsend Device Account names and passwords—*Optional*

(SMARTsend creates device accounts for each protocol automatically. However, if you choose to create and manage these accounts manually, you should record this information in the space provided below. Device accounts are not required by the installer, but they will be required when Xerox Multifunction Devices are added during site configuration. See *Create Administrator, User, and Device Accounts* on page 2-13.)

FTP Account Name/Password: \_\_\_\_\_

SMB Account Name/Password: \_\_\_\_\_

HTTP Account Name/Password: \_\_\_\_\_

HTTPS Account Name/Password: \_\_\_\_\_

## Next Steps

You are ready to install SMARTsend software if you have completed all the required preparation tasks presented in this chapter. Please review and confirm the preparation requirements in this chapter, then proceed to Chapter 3 for the software installation instructions.

**NOTE:** If you are upgrading from a Trial Version or a previous version of SMARTsend, simply follow the upgrade procedures in Chapter 3, *Install SMARTsend*, to upgrade your software. The SMARTsend installation program will automatically upgrade a current Trial Version to the current licensed version. All workflows generated while using the Trial Version or a previous version will be accessible after the upgrade is completed. If you have a Trial Version of SMARTsend that has expired, you can upgrade to the retail version and retain all workflows. The retail version can be ordered through your Xerox sales representative, and installed as an upgrade to your existing Trial Version. See *Upgrade Eligibility* on page 3-4 for additional information.



## Install SMARTsend

This chapter describes the functions of the SMARTsend installer and describes the installation, startup, and removal of the application. Additional information and procedures for upgrading from the Trial Version or previous versions of SMARTsend are also provided.

**NOTE:** For new installations, please read and follow the preparation steps in Chapter 2, *Prepare for Installation*, before you attempt to install and configure SMARTsend.

### *What is in this chapter:*

- *Installer Overview* ..... 3-2
- *Upgrade SMARTsend* ..... 3-3
- *Install SMARTsend* ..... 3-5
- *Installing and Configuring Optional Components* ..... 3-7
- *Migrate SMARTsend to a Replacement Computer* ..... 3-15
- *Repair a SMARTsend Installation* ..... 3-16
- *Uninstall SMARTsend* ..... 3-17

# Installer Overview

The SMARTsend installation program performs the following tasks:

- Searches for a previous version of SMARTsend that is eligible to be upgraded. If a previous version can be upgraded, the installer will save the current customer configuration data (workflows, device configurations, templates, PaperWare forms (Professional Edition feature), etc.), install the software updates for the new version, and reconfigure the new version with the customer data from the previous version.

If a previous version of SMARTsend is not available for upgrade, the installer performs the standard installation tasks that are listed below.

- Searches for Internet Information Services (IIS) and cancels the installation if it is not present.
- Searches for the .NET Framework and MDAC (Microsoft Data Access Components) and installs them if necessary.

**NOTE:** IIS must be installed before the .NET Framework is installed on Windows XP Professional computer or a Windows 2000 Server/Advanced Server. The SMARTsend installation program will install the .NET Framework if it is not present on the computer, but it cannot detect the order in which these applications were installed. If the .NET Framework and IIS are currently installed on the computer and you are not certain if IIS was installed first, then these components should be uninstalled and reinstalled in the proper sequence.

- Installs the Microsoft SQL Server 2000 Desktop Engine (MSDE). A password is required.

**NOTE:** This password is for SMARTsend's internal use in database management. The application will not request this password.

- Installs SMARTsend software.
- Enters the following information into the SMARTsend database:
  - Administrator name
  - Administrator e-mail address
  - Administrator telephone number
  - SMTP server IP address or fully qualified DNS name
  - LDAP server IP address or fully qualified DNS name
  - SMARTsend 'Reply To' account

See *Prepare Information for Installation* on page 2-34 for additional information on these items.

# Upgrade SMARTsend

---



**CAUTION:** Xerox recommends backing up the current SMARTsend database before upgrading the application. See *Schedule a Backup* on page 4-28 for more information.

---

SMARTsend provides the capability to upgrade previous versions of the application to the latest version while maintaining important configuration data. The installer automatically migrates the following data to the new version:

- Number of device licenses purchased
- Backup data
- Device configurations
- Workflows
- PaperWare cover sheet publications (Professional Edition)
- Device scan template publications
- Custom document attribute profiles
- Destinations
- User and administrator preferences
- Credentials
- Service settings
- Job history data

**NOTE:** Template attribute settings that are set differently from a previous version of SMARTsend, are not updated automatically when an upgrade is performed. Template attributes can be updated by using the Restore Tool to restore a previous backup, or by using the Repair option on the Manage Xerox Devices page.

## Upgrade Eligibility

Some SMARTsend versions or upgrade combinations may not support automatic upgrades. The following guidelines apply to upgrades:

- Trial Versions can only be upgraded when the Trial Version release number matches the current version release number.
- Professional Versions (trial or full license) cannot be upgraded to the basic version of SMARTsend. A Professional Version can only be upgraded to another Professional Version.
- Basic Versions can be upgraded to the Professional Version.

**NOTE:** The SMARTsend Backup and Restore features provide an alternative method for migrating existing SMARTsend configuration data (including Trial versions of SMARTsend) to newer versions of SMARTsend. This method requires you to backup and uninstall the existing SMARTsend installation prior to installing a newer version. After completing these tasks, you can then use the Restore feature to migrate the backup data to the newly installed version of SMARTsend. See *Migrate SMARTsend to a Replacement Computer* on page 3-15 for more information.

### ► To upgrade an existing version of SMARTsend:

- 1 Log in to the SMARTsend computer as an administrator.
- 2 At the SMARTsend computer, insert the SMARTsend CD into the CD-ROM drive.
- 3 The CD should launch automatically. If it does not, click **Start > Run** and browse to the CD-ROM drive. Double-click the **Launch.exe** icon, which is located within the appropriate language folder.
- 4 Select the language in which the installer should run and click **OK**. The *Welcome to the FreeFlow SMARTsend Installer Program* window appears.
- 5 Click **SMARTsend Installation**.
- 6 There will be a delay while the installer checks the system for the presence of a previous version of SMARTsend that is eligible for an upgrade. After a successful check, the Installation Wizard screen appears. Click **Next**.
- 7 Read and accept the license agreement. Click **Next**.
- 8 Obtain the SMARTsend serial number from the product packaging and enter the serial number in the installer dialog. Click **Next**.
- 9 Click **Next** to proceed with the upgrade. The Ready to Install the Application window appears.
- 10 If necessary, click **Back** to revise installation options. When all settings are correct, click **Next** in the Ready to Install the Application window.
- 11 When the process has completed, click **Finish** to conclude the installation/upgrade.
- 12 Click **Yes** to reboot the computer immediately or **No** to reboot later. You must reboot the computer before using SMARTsend.

**NOTE:** Be sure to confirm that the required IIS and ASP.NET services are running after SMARTsend has been installed and the computer has rebooted. See *SMARTsend Configuration Requirements* on page 2-5 for more information.

# Install SMARTsend

**NOTE:** SMARTsend installation via Microsoft Windows Terminal Services (TS) or a Remote Desktop Connection is not supported. Installation should only be performed from the computer console. The computer must be connected and properly configured on your network when you install the application software. To ensure your system is configured correctly, you should copy the SMARTsend ISO image locally or run the SMARTsend install from the CD.

**NOTE:** If you attempt to install SMARTsend from a network share (for example, if you are running Microsoft Virtual Server and create a share on the host computer), you will receive a popup error with the heading 'SetDirAccess.exe - Common Runtime Language Debugging Services'. If you click OK, the installation will complete successfully. However, the SMARTsend directory tree may not have all the required directory permissions. If you have already installed and received this and other errors while running SMARTsend, please copy the ISO image locally or run the install again, and select the Repair option.

## ► To install SMARTsend:

- 1 Log in to the SMARTsend computer as an administrator.
- 2 At the SMARTsend computer, insert the SMARTsend CD into the CD-ROM drive.
- 3 The CD should launch automatically. If it does not, click **Start > Run** and browse to the CD-ROM drive. Double-click the **Launch.exe** icon, which is located within the appropriate language folder.
- 4 Select the language in which the installer should run and click **OK**. The *Welcome to the FreeFlow SMARTsend Installer Program* window appears.
- 5 Click **SMARTsend Installation**.
- 6 There will be a delay while the installer checks the system for the presence of several Microsoft components, including MDAC 2.8, IIS, and the Microsoft .NET Framework. If IIS is not present, the installation ends. If MDAC, the .NET Framework, or both are not present, or are earlier versions than required, the installer loads them. After a successful check, the Installation Wizard screen appears. Click **Next**.

**NOTE:** The popups that may appear while installing these applications, as well as MSDE, are generated by the Microsoft components. Follow any directions they display. You may have to reboot after installing one or more of these applications and restart the SMARTsend installation.

- 7 Read and accept the license agreement. Click **Next**.
- 8 Obtain the SMARTsend serial number from the product packaging and enter the serial number in the installer dialog. Click **Next**.
- 9 Enter the SMARTsend administrator's contact information. Click **Next**.

**NOTE:** See *Update Administrator Contact Information* on page 4-35 for more information about the administrator and 'Reply To' address configuration settings.

- 10 Enter the SMTP server fully-qualified DNS name and the 'Reply To' e-mail address that SMARTsend will use to send reports and status messages to administrators and users. Click **Next**.
- 11 If using an LDAP server for e-mail address lookup, enter that server's fully qualified DNS name or IP Address here. Click **Next**.

- 12 Choose the initial security setting for SMARTsend. A security certificate is required for secure password entry. After selecting a security option, click **Next**.
- 13 Enter and verify the MSDE password for SMARTsend database administration. Click **Next**.

**NOTE:** This password is for SMARTsend's internal use in database management. You must enter this password here and cannot update it within the application. The application will not request this password.

- 14 A default application path is defined by the installer. If necessary, use the Browse button to change the destination folder. You cannot change this folder after the installation has been performed.
- 15 Click **Next** to proceed with the installation. The Ready to Install the Application window appears.
- 16 If necessary, click **Back** to revise installation options. When all settings are correct, click **Next** in the Ready to Install the Application window. The installation will begin, but keep in mind that there may be several long delays while various components are being installed in the background.
- 17 When the installation process has completed, click **Finish** to conclude the installation.
- 18 Click **Yes** to reboot the computer immediately or **No** to reboot later. You must reboot the computer before using SMARTsend.

**NOTE:** Be sure to confirm that the required IIS and ASP.NET services are running after SMARTsend has been installed and the computer has rebooted. See *SMARTsend Configuration Requirements* on page 2-5 for more information.

- 19 Various site configuration tasks are required to prepare SMARTsend for use at your location. Follow the setup tasks in Chapter 4, *Site Configuration*, to complete the installation process. If you have optional components, you can install them after SMARTsend has been installed and the computer has been rebooted. See *Installing and Configuring Optional Components* on page 3-7 for additional information.

# Installing and Configuring Optional Components

Optional components, such as the Documentum, Hummingbird, Interwoven WorkSite, and LiveLink services, can be purchased from Xerox and installed with a licensed Standard or Professional Edition of SMARTsend. Some optional components, such as TrueMatch, can only be installed with the Professional Edition of SMARTsend. Please check the instructions that are provided with each optional component to confirm these requirements.

**NOTE:** A licensed version of SMARTsend must be properly installed before you can install any optional components.

## Configuration Requirements for Optional Components

Some SMARTsend optional components have additional configuration requirements that must be addressed before they can be used. The current requirements for the Documentum, Hummingbird, Interwoven WorkSite, LiveLink, and TrueMatch optional components are provided below.

**NOTE:** Some optional components require the installation and configuration of additional client software before the optional component is installed. Please review and fulfill these requirements before you install an optional component.

### Documentum Configuration Requirements

The following configuration requirements must be addressed to prepare the Documentum service for use with SMARTsend Standard or Professional Editions:

- 1 Documentum Content Server version 5.2 must be properly installed, configured, and functional.
- 2 The Documentum Desktop version 5.3 client must be installed on the SMARTsend computer before the Documentum option can be added to SMARTsend.
- 3 You may need to perform additional configuration steps to prepare the Documentum client for use.

**NOTE:** Please consult the install media and documentation provided with your Documentum product for client installation and configuration instructions.

- 4 Test the Documentum configuration from the SMARTsend computer by using the client to access an existing Documentum Docbase/Cabinet.
- 5 Follow the *Installation Instructions for Optional Components (Standard or Professional Edition feature)* on page 3-13 to install the Documentum optional component.
- 6 After the Documentum client and the optional component are both installed on the SMARTsend computer, you will need to make some configuration changes on the SMARTsend computer.

#### **For Windows XP Professional and Windows 2003 Server:**

- a) Edit file c:\windows\dmcl.ini
- b) Add Entry local\_path to [DMAPI\_CONFIGURATION]:
- c) [DMAPI\_CONFIGURATION]  
local\_path = C:\Documentum\dmcl

- d) For both Windows XP Professional and Windows 2003 installations, the Users group must be assigned Full Control access to the c:\Documentum folder (and children). Do this by:
- On the SMARTsend computer, browse to the c:\Documentum folder.
  - Right-click and select Properties.
  - At the Documentum Properties dialog, select the Security Tab.
  - Ensure that the Users group has been added and the Full Control access has been assigned.

**For Windows 2000 Server/Advanced Server:**

- a) Edit file c:\winnt\dmcl.ini
- b) Add Entry local\_path to [DMAPI\_CONFIGURATION]:
- c) [DMAPI\_CONFIGURATION]
- ```
local_path = C:\Documentum\dmcl
```
- d) Double check to make sure that the c:\documentum directory has "Everyone" set to have full control (This is the default when Documentum client is installed). Do this by:
- On the SMARTsend computer, browse to the c:\Documentum folder.
  - Right-click and select Properties.
  - At the Documentum Properties dialog, select the Security Tab.
  - Ensure that the Everyone group has Full Control access.

## Hummingbird Configuration Requirements

The following configuration requirements must be addressed to prepare the Hummingbird DM service for use with SMARTsend Standard or Professional Editions:

- 1 Hummingbird DM server version 5.1.0.5 must be properly installed, configured, and functional.
- 2 The Hummingbird DM version 5.1.0.5 client must be installed on the SMARTsend computer before the Hummingbird option can be added to SMARTsend. When installing the Hummingbird DM client on the SMARTsend computer, you must select the DM Internet Mode optional component. After installing the client, restart the computer if prompted to do so.
- 3 Once the client is installed on the SMARTsend computer, the DM WebTop Connection Mode must be set to Intranet, and the desired DM server must be specified using the DM Connection Wizard.

**NOTE:** Because of the limitation imposed by the Hummingbird client, SMARTsend will be able to use only one Hummingbird server at a time.

**NOTE:** Please consult the install media and documentation provided with your Hummingbird product for client installation and configuration instructions.

- 4 Test the Hummingbird configuration from the SMARTsend computer by using the client to access an existing Hummingbird Library/Folder.

**NOTE:** To enable the installation of the Hummingbird optional destination on a Windows 2000 Server/Advanced Server, you must grant the ASPNET account the 'Act as part of the operating system' privilege through the local security policy editor. To do this click Start > Programs > Administrative Tools > Local Security Policy. Expand Local Policies and double-click User Rights Assignment. Add the ASPNET account to the list of accounts that have rights to 'Act as part of the operating system.'

- 5 Follow the *Installation Instructions for Optional Components (Standard or Professional Edition feature)* on page 3-13 to install the Hummingbird service. After installing the Hummingbird service, continue with the next step (below) to configure the Hummingbird optional component.
- 6 Perform the following steps to configure the Hummingbird service:
  - a) Launch SMARTsend and log in as an administrator to access the Administration Home Page.
  - b) Click the **Configure Service Settings** link in the lower section of the Site Configuration panel.
  - c) Click on the **Hummingbird** link.

- d) Enter the **User Name, Password, and Domain Name** for a Windows user account that is configured on the Hummingbird server. The SMARTsend computer requires a valid user account to access the Hummingbird server.

**NOTE:** When the Hummingbird server and the SMARTsend computer are in different domains (without a trust relationship), and you are configuring the Hummingbird service, you must enter the User Name and Password for a Windows user account that exists both on the Hummingbird server and the SMARTsend computer. If the Hummingbird server and the SMARTsend computer are in the same domain or trusted domain, then a domain account User Name and Password may be entered.

**NOTE:** The Windows account used when configuring the Hummingbird service must be granted the 'Log on locally' privilege through the local security policy editor on the Hummingbird server. For example: to do this on a Windows 2000 Server/Advanced Server: click Start > Programs > Administrative Tools > Local Security Policy. Expand Local Policies and double-click User Rights Assignment. Add the Windows account being used to the list of accounts that have rights to 'Log on locally.'

- e) Click **Apply** to save any changes. See *Configure Service Settings* on page 4-29 for additional information.

## Interwoven WorkSite Configuration Requirements

The following configuration requirements must be addressed to prepare the Interwoven WorkSite service for use with SMARTsend Standard or Professional Editions:

- 1 Interwoven WorkSite server version 8.0 must be properly installed, configured, and functional.
- 2 The Interwoven WorkSite version 8.0 client must be installed on the SMARTsend computer before the Interwoven WorkSite option can be added to SMARTsend. After installing the client, restart the computer if prompted to do so.

**NOTE:** Please consult the install media and documentation provided with your Interwoven WorkSite product for client installation and configuration instructions.

- 3 Test the Interwoven configuration from the SMARTsend computer by using the client to access an existing Interwoven WorkSite server/database.
- 4 Follow the *Installation Instructions for Optional Components (Standard or Professional Edition feature)* on page 3-13 to install the Interwoven WorkSite optional component.

## LiveLink Configuration Requirements

The following configuration requirements must be addressed to prepare the LiveLink service for use with SMARTsend Standard or Professional Editions:

- 1 LiveLink version 9.5.0 must be properly installed, configured, and functional.
- 2 Install the Open Text LiveLink SDK version 9.5.0.1, and all of its prerequisites, on the SMARTsend computer before installing the LiveLink optional component. When asked if you would like to add the LAPI bin directory to your system path, click yes.
- 3 Install the proper Microsoft Visual J# .NET distribution for your version of the .NET Framework.
- 4 Follow the *Installation Instructions for Optional Components (Standard or Professional Edition feature)* on page 3-13 to install the LiveLink service.

## TrueMatch Configuration Requirements

The following configuration requirements must be addressed to prepare the TrueMatch service for use with SMARTsend (Professional Edition only):

- 1 Microsoft SharePoint Portal Server 2001 or 2003 must be properly installed, configured, and functional if it is an intended search destination.
- 2 Xerox DocuShare version 3.1 or 4.0 must be properly installed, configured, and functional if it is an intended search destination. The server must be configured to support searching.
- 3 Test the SharePoint and/or DocuShare configurations by performing a search within each repository, using the standard client or web tools provided with the repository. If you are unable to perform a search, please contact the system administrator who is responsible for the SharePoint and/or DocuShare server.
- 4 Perform the following steps to configure the TrueMatch service:
  - a) Launch SMARTsend Professional Edition and log in as an administrator to access the Administration Home Page.
  - b) Click the **Configure Service Settings** link in the lower section of the Site Configuration panel.
  - c) Click the **Edit** link for the TrueMatch service.
  - d) Edit the following default settings as needed:
    - **Maximum number of documents a user may select to locate**—sets the default limit for the number of documents that a search workflow will locate. The options are 1, 5, 10, 25 and 50.
    - **Maximum search timeout (in minute intervals)**—sets the default time limit for executing search workflows. The options are 5, 10, 15, and 20.
    - **Maximum retrieve file size (in Mb)**—sets the default file size limit for each retrieved document. The options are 2, 5, 10, 25, and 50 megabytes.
  - e) Click **Apply** to save any changes. See *Configure Service Settings* on page 4-29 for additional information. If TrueMatch will be used to search for and print the results of Microsoft Office documents (Word, Excel, PowerPoint), Microsoft Office 2000, XP or 2003 must be installed, and configured as an interactive user, on the SMARTsend computer. See *Configuring Microsoft Office as an Interactive User* on page 2-20 of the SMARTsend Installation and Administration Guide for additional information. If you are unable to print the TrueMatch results, after ensuring that Microsoft Office has been configured as an interactive user, uninstall and reinstall the Microsoft Office application.

**NOTE:** If SMARTsend is uninstalled and later reinstalled, you must reconfigure Microsoft Office as an interactive user.

The Xerox Walk-Up Printing Driver 2.0 is a required SMARTsend component, and is critical to the successful operation of TrueMatch search workflows. If not present on the SMARTsend computer, it will be installed with the installation of SMARTsend.

The Xerox Walk-Up Printing Driver 2.0 is not removed when SMARTsend is uninstalled. You can uninstall the Xerox Walk-up Print Driver using Add/Remove programs.

If the driver installation becomes corrupted - which can occur if the Xerox Walk-Up Printing Driver 2.0 printer object is deleted - the driver will need to be reinstalled. Please download the driver from the SMARTsend support page at [www.Xerox.com](http://www.Xerox.com), and reinstall it.

## Installation Instructions for Optional Components (Standard or Professional Edition feature)

**NOTE:** Some optional components require the installation and configuration of additional client software before the optional component is installed. Please review *Configuration Requirements for Optional Components* on page 3-7 before you perform the following installation procedure.

### ► To install SMARTsend Optional Destinations:

- 1 Log in to the SMARTsend computer as an administrator.
- 2 At the SMARTsend computer, insert the CD for the *FreeFlow™ SMARTsend™ Optional Destinations* into the CD-ROM drive.
- 3 Browse the CD-ROM drive using Windows Explorer. Open the folder for the destination you want to install.
- 4 Double-click the **Setup.exe** icon.
- 5 Select the language in which the installer should run and click **OK**.
- 6 Click **Next >** at the installer Welcome page.
- 7 Read and accept the license agreement. Click **Next**.
- 8 Click **Install** to begin the installation.
- 9 Click **Finish** on the confirmation screen. If prompted to restart the computer, click **Yes**.
- 10 See *Configuration Requirements for Optional Components* on page 3-7 for additional configuration requirements and instructions that pertain to each component.

For additional product support information, access the Readme files available on the *FreeFlow™ SMARTsend™ Optional Destinations* CD. The Readme files are located within the Readme folders for each optional destination. Readme files are provided for all supported languages, and can be identified by the two letter language abbreviation that is included in the file name. For example, the path and file name for the English Documentum Readme file is as follows:

`\\Documentum\\Readme\\Readme_en.txt`

- 11 Test each optional component in SMARTsend by creating a workflow for each newly-added destination. See Chapter 3, *Distribution Workflows* and Chapter 4, *Search Workflows* in the SMARTsend User Guide for additional information.

### ► To install SMARTsend TrueMatch:

- 1 Log in to the SMARTsend computer as an administrator.
- 2 At the SMARTsend computer, insert the *FreeFlow™ SMARTsend™ TrueMatch* CD into the CD-ROM drive.
- 3 Browse the CD-ROM drive using Windows Explorer.
- 4 Double-click the **setup.exe** icon to begin installation.
- 5 Select the language in which the installer should run and click **OK**.
- 6 Click **Next >** at the installer welcome page.
- 7 Read and accept the license agreement. Click **Next**.

- 8 Click **Install** to begin the installation.
- 9 Click **Finish** on the confirmation screen.
- 10 See *TrueMatch Configuration Requirements* on page 3-12 for additional configuration requirements and instructions.

For additional product support information, access the Readme file located in the Readme folder on the *FreeFlow™ SMARTsend™ TrueMatch* CD. Readme files are provided for all supported languages, and can be identified by the two letter language abbreviation that is included in the file name. For example, the English Readme file is named *Readme\_en.txt*.

- 11 Test the TrueMatch configuration within SMARTsend by creating a search workflow. See Chapter 4, *Search Workflows* in the SMARTsend User Guide for additional information.

## Migrate SMARTsend to a Replacement Computer

Existing SMARTsend configurations can be migrated to a replacement computer without recreating existing workflows, user preferences, device configurations, and general settings. This applies when migrating with the same version of SMARTsend, or when upgrading to a newer version of SMARTsend.

**NOTE:** Security Identifiers (SIDs) are required to identify SMARTsend users. Changing the domain of a computer will change the SIDs. Therefore, the replacement computer must be in a Windows NT/Active Directory domain where the domains of the current SMARTsend users are trusted.

### ► To migrate an existing SMARTsend configuration to a replacement computer:

- 1 On the current/original computer, launch SMARTsend using administrator credentials.
- 2 Open the Administration Home Page.
- 3 Locate the Backup Status pane and click the **Backup Now** button. SMARTsend creates a backup file in the following default location: `<drive>:\Inetpub\wwwroot\SMARTsend\Data\Backup\`. See *Backup Status* on page 5-8 for more information.
- 4 Copy the backup folder from the original computer to your desired location on the replacement computer.
- 5 Install SMARTsend on the replacement computer. Follow the instructions in the SMARTsend Installation and Administration Guide.
- 6 After a successful install, launch the Restore Tool on the replacement computer. See *Restore Tool* on page 8-12 for more information.
- 7 Choose the Backup Directory Path option, then browse to the location of the backup folder that you copied from the original computer.
- 8 After a successful restore, launch SMARTsend on the replacement computer.
- 9 Confirm that all workflows, user preferences, device configurations, and general settings have been restored.

**NOTE:** SMARTsend user credentials are not restored. Users will need to re-enter credentials for each supported service/destination type before they can execute workflows on the replacement computer. Refer users to the Manage My Credentials link on the User Home Page to update their credentials.

## Repair a SMARTsend Installation

*Skip this section if you are currently performing an installation.*

The SMARTsend installer provides an option to repair an existing SMARTsend installation. This feature reinstalls any missing or corrupt files, registry keys, and shortcuts used by SMARTsend. In addition, some registry settings for SMARTsend preferences may be reset to the default values. This repair option does not repair SMARTsend device configuration or device scan templates.

### ► To repair an existing SMARTsend installation:

- 1 Log in to the SMARTsend computer as an administrator.
- 2 Open the Windows **Control Panel** and select **Add/Remove Programs**.
- 3 Select **SMARTsend**, then select **Change**.
- 4 Select **Repair** on the Application Maintenance Page, then click **Next**.
- 5 Click **Next** on the Ready to Repair the Application page.
- 6 Follow the directions provided by the installer to complete the repair.

# Uninstall SMARTsend

*Skip this section if you are currently performing an installation or upgrade.*

The SMARTsend uninstall program removes the SMARTsend application and database files, including workflows, publications, device information, and user data (such as e-mail addresses and credentials). It does not remove Microsoft applications that were installed with the application, such as the .NET Framework, MDAC and MSDE. If any SMARTsend optional components (i.e. Documentum, Hummingbird, etc.) were installed on the SMARTsend computer, they will automatically be removed when SMARTsend is uninstalled.



**CAUTION:** Xerox recommends backing up the SMARTsend database before uninstalling the application. See *Schedule a Backup* on page 4-28 for more information.

---

## ► To uninstall SMARTsend:

- 1 If SMARTsend is installed on a Windows 2000 Server/Advanced Server:  
Click **Start > Settings > Control Panel > Add/Remove Programs**.  
- OR -  
If SMARTsend is installed on a computer running Windows Server 2003 or Windows XP Professional:  
Click **Start > Control Panel > Add or Remove Programs**.
- 2 Select **SMARTsend**.
- 3 Click **Change**. The Application Maintenance window appears.
- 4 Click **Remove**, then select **Next**. The Verify Database Delete window appears.
- 5 To continue uninstalling SMARTsend, check **OK to delete SMARTsend database permanently. I have performed a backup or do not need to restore my data**.
- 6 Click **Next** to begin uninstalling SMARTsend. Any optional SMARTsend components will also be uninstalled with the application.
- 7 Click **Finish** to exit the wizard.
- 8 Click **Yes** to reboot the computer immediately or **No** to reboot later. Rebooting the computer immediately is recommended. The computer must be rebooted before reinstalling SMARTsend.



## Site Configuration

This chapter describes the primary steps that the SMARTsend administrator performs to configure SMARTsend for use. These steps are based on the Site Configuration panel on the Administration Home Page. Please consult the SMARTsend User Guide for information pertaining to the User Home Page and any workflow creation and publishing features.

### *What is in this chapter:*

|                                                                    |      |
|--------------------------------------------------------------------|------|
| ■ <i>Accessing SMARTsend</i> . . . . .                             | 4-2  |
| ■ <i>Administration Home Page</i> . . . . .                        | 4-3  |
| ■ <i>Site Configuration</i> . . . . .                              | 4-4  |
| ■ <i>Review Security Settings</i> . . . . .                        | 4-5  |
| ■ <i>Add/Update Xerox Devices</i> . . . . .                        | 4-8  |
| ■ <i>Manage Xerox Devices</i> . . . . .                            | 4-8  |
| ■ <i>Adding and Discovering Devices</i> . . . . .                  | 4-9  |
| ■ <i>Configuring a Device for use with SMARTsend</i> . . . . .     | 4-13 |
| ■ <i>Configure Discovery Settings - Subnets</i> . . . . .          | 4-17 |
| ■ <i>Configure Discovery Settings - SNMP Credentials</i> . . . . . | 4-17 |
| ■ <i>Edit Device Configuration Defaults</i> . . . . .              | 4-18 |
| ■ <i>Manually Configure This Device</i> . . . . .                  | 4-22 |
| ■ <i>Configure PaperWare Internet Fax Settings</i> . . . . .       | 4-24 |
| ■ <i>Setup E-mail and Address Book</i> . . . . .                   | 4-25 |
| ■ <i>Publish the My E-mail Workflow</i> . . . . .                  | 4-27 |
| ■ <i>Schedule a Backup</i> . . . . .                               | 4-28 |
| ■ <i>Configure Service Settings</i> . . . . .                      | 4-29 |
| ■ <i>Manage Application Account</i> . . . . .                      | 4-34 |
| ■ <i>General Settings</i> . . . . .                                | 4-35 |
| ■ <i>Next Steps</i> . . . . .                                      | 4-42 |
| ■ <i>Appendix A - Job Log Export Support</i> . . . . .             | 4-43 |
| ■ <i>Appendix B - External Application Connection</i> . . . . .    | 4-44 |

## Accessing SMARTsend

SMARTsend can be accessed from any client browser that has access to the SMARTsend computer, or from the SMARTsend computer itself. When an administrator account is used to log in to the SMARTsend computer, the Administration Home Page appears. When a user account is used to log in to the SMARTsend computer, the User Home Page appears.

**NOTE:** Disable pop-up blockers before using SMARTsend.

### ► To access the Administration Home Page:

- 1 Log in to the SMARTsend computer as an Administrator, then click **Start > Programs (All Programs) > Xerox > SMARTsend > SMARTsend**.

- OR -

Launch your web browser from any computer and go to the SMARTsend home page located at *http://<computername or IP address>/SMARTsend*. Enter your SMARTsend administrative account credentials.

**NOTE:** See Chapter 7, *Problem Solving* for additional information if SMARTsend cannot be accessed from a client workstation.

- 2 The SMARTsend Welcome page displays by default. The Welcome page can be bypassed by selecting the option entitled **Do not show this screen next time I access SMARTsend**.
- 3 From the Welcome page, select **Click here to enter SMARTsend**.
- 4 The Administration Home Page appears. Keep in mind that some SMARTsend options and buttons that are located at the bottom of the pages may not be visible on all displays. Use the scroll bar on the right side of the window to scroll to the bottom of the pages as needed. If you change the settings on a page, you will need to click the **Apply** button at the bottom of the page in order to save the changes on certain pages.

**NOTE:** A SMARTsend administrator can choose to start SMARTsend from either the User Site Home Page or the Administration Home Page. Administrators who spend most of their time creating and editing workflows, for example, may prefer to start on the User Site Home Page. The My Home Page panel on the lower right section of the Administration Home Page enables you to choose the default startup page.

# Administration Home Page

The Administration Home Page is used by administrators to configure and manage the SMARTsend site. This page provides site configuration options and status information on the left side of the page, and site management links and information on the right side of the page.

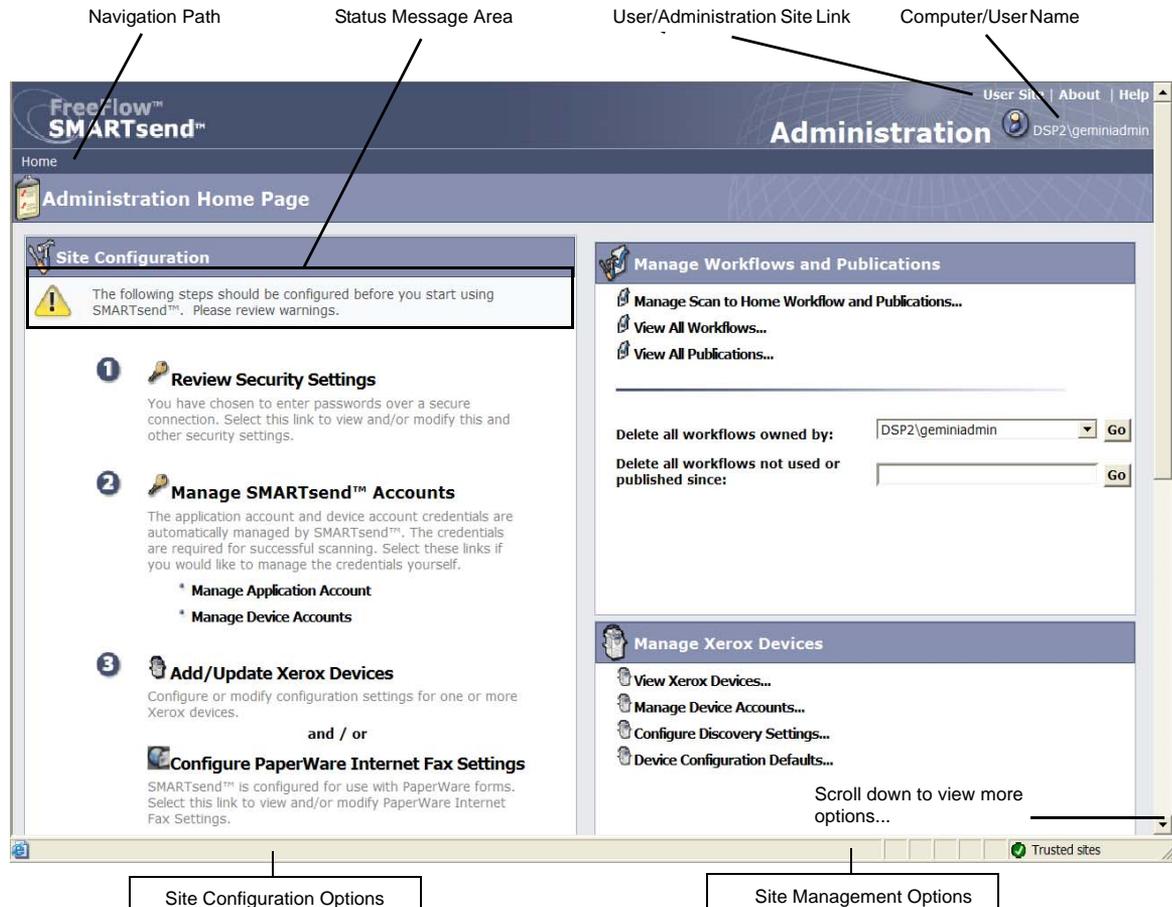


Figure 4-1: Administration Home Page (top section)

- **Navigation Path**—This area lists the current page and the pages that were used to access the current page. For example, *Home >> Manage Xerox Devices >> Add Devices* is displayed when viewing the Add/Update Xerox Devices page. Keep in mind that the text provides links to each page. Simply click on the links to access any of the SMARTsend pages in the path.
- **Status Message Area**—The messages displayed by SMARTsend will change based on the current operational status of the application.
- **User/Administrator Site Link**—This link is only available to SMARTsend administrators. It enables the administrator to switch back and forth from the Administration Home Page and the User Home Page.
- **Computer/User Name**—Displays the SMARTsend computer name and the account name for the user/administrator who is currently logged in.

# Site Configuration

The Site Configuration panel of the Administration Home Page lists the key tasks that are needed for proper site configuration. Some of the tasks are mandatory requirements, while others are optional or recommended configuration tasks that the administrator should perform to fully address all aspects of site configuration. The SMARTsend administrator should configure and test all critical site configuration settings to ensure that the site is fully operational for end users. Details for each Site Configuration option are provided in the following pages.

**NOTE:** Keep in mind that SMARTsend site configuration may fail if the prerequisite computer, client, and device configuration tasks have not been performed before using SMARTsend. If you have not done so already, please refer to Chapter 2, *Prepare for Installation*, to perform these critical configuration tasks.

## Status Icons

The Site Configuration area of the Administration Home Page displays various status messages and icons to help make you aware of configuration problems and to confirm that SMARTsend is properly configured for use. The following icons are used to indicate the current status of the key site configuration options:

**Table 4-1: Status Icons**

|                                                                                     |                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Indicates that a critical setting must be configured before SMARTsend can be used. Check the message area in the Site Configuration panel for diagnostic information.                                                          |
|  | Indicates that a specific site configuration setting may not be configured or functional. Keep in mind that SMARTsend can be used when these icons are present, but certain optional or recommended features may not function. |
|  | Indicates that all SMARTsend administrative options have been configured and the site is ready for use.                                                                                                                        |

When no critical warning icons appear in the Site Configuration panel, you can continue with additional site configuration tasks (optional), or proceed to the User Home Page and begin testing or using SMARTsend. See *Next Steps* on page 4-42 for more information.

**NOTE:** SMARTsend will not be operational until at least one Xerox Multifunction Device is configured, or the PaperWare (Professional Edition feature) capabilities are configured. See *Add/Update Xerox Devices* on page 4-8, or *Configure PaperWare Internet Fax Settings* on page 4-24 for more information.

## Review Security Settings

The Review Security Settings link enables you to configure security options for SMARTsend password entry, device authentication, and PaperWare forms (Professional Edition feature). Please refer to Chapter 9, *SMARTsend Security* for additional information.

### General Site Security

The General Site Security policies pertain to the secure entry of account and password information. The security policies selected here govern the transmission of this data between clients and the SMARTsend computer. The transmission of account and password data to workflow destinations is governed by additional factors, such as the transfer protocols that the destination supports. See Chapter 9, *SMARTsend Security* for additional information.

- **Enter passwords using a secure connection (*default setting*)**—Use this policy if you are using SSL for secure password entry. Xerox recommends this setting, because it provides for account name and password encryption as this information travels between clients and the SMARTsend computer. This option requires a security certificate, which should be obtained in advance. See Chapter 2, *Prepare for Installation* for more information about obtaining a security certificate.
- **Enter passwords over a non-secure connection**—Use this policy if you are using unsecured password entry. With this option, passwords are transmitted between clients and the SMARTsend computer in clear text format.

**NOTE:** If secure password entry is enabled, SMARTsend encrypts the account name and password on its way from the client to the SMARTsend computer. However, when this data is transferred to the device over SNMP, it is transferred as clear text.

## Device Scan Template Security

The Device Scan Template Security policies are used to configure the authentication settings for scan templates that have been published to Xerox Multifunction Devices. These authentication policies assume that SMARTsend is managing devices that support authentication, and that the devices have authentication enabled and properly configured to authenticate users from the same domain or trusted domain as the SMARTsend computer. These policies do not apply to PaperWare cover sheets (See *PaperWare Forms* on page 4-7).

### SMARTsend supports the following scan template security policies:

- **Require authentication at the device for all templates**—Use this policy to require all SMARTsend users to enter their credentials at the Xerox Multifunction Device when any public or private templates are used.
- **Require authentication at the device for private templates only (default setting)**—Use this policy to require workflow/template owners to enter their credentials at the Xerox Multifunction Device only when private templates are used. This setting permits public templates to be used without authentication.

**NOTE:** Devices that are capable of providing authentication are identified within SMARTsend by a lock on the device icons that appear on the Manage Xerox Devices page. Please keep in mind that this icon does not confirm that authentication is currently configured and operational on the device. Please consult the documentation provided with your Xerox Multifunction Device for instructions on enabling and configuring authentication.

Keep in mind that all users can select a private template at the device and attempt to scan a job. The job will initially appear to begin processing, but will eventually fail if the credentials entered at the device do not match the credentials of the private workflow on the SMARTsend computer. Job failures due to insufficient authentication will be reported on the Job Confirmation report (if enabled), but there will be no indication of job failure at the device user interface.

See *Security Policy Interactions* on page 9-10 of Chapter 9, *SMARTsend Security* for more information.

## PaperWare Forms

### Professional Edition Feature

The PaperWare Forms security policies are used to configure the authentication settings that apply to the use of PaperWare cover sheets. If the administrator has selected authentication, it is assumed that SMARTsend is managing devices that are configured to authenticate users from the same domain or trusted domain as the SMARTsend computer.

- **Allow authentication with PaperWare forms only (*default setting*)**—Use this policy if the login name and password information on the PaperWare form are sufficient for authentication, or if the device on which the form is used does not support authentication. This setting would allow anyone in possession of a PaperWare cover sheet to use it on Internet Fax devices or devices that do not support authentication, even if the originating workflow from which the cover sheet was published were a private or Scan to My E-mail workflow.
- **Require PaperWare form and login at the device for authentication**—Use this policy if users must supply login information both on the PaperWare cover sheet and at the device. When scanning devices support authentication, this setting restricts use of the PaperWare cover sheet derived from a public workflow to authorized device users, and to the workflow owner. If someone other than the private workflow owner scans a document when this policy is active, the job will initially appear to process at the device, but will eventually fail if the credentials entered at the device do not match the private workflow credentials on the SMARTsend computer. The failure will be reported on the Job Confirmation report (if enabled), but there will be no indication of job failure at the device user interface.

# Add/Update Xerox Devices

SMARTsend provides several features that enable you to identify and configure Xerox Multifunction Devices for use with SMARTsend. Available devices can be identified with an automated device discovery process, or with the manual entry of device IP addresses or Host Names. Click the Add/Update Xerox Devices link on the Administration Home Page to access these features.



**CAUTION:** During device configuration, SMARTsend overwrites the Default Repository and Template Pool scan settings of a Xerox Multifunction Device. If you have existing applications that use the Default Repository, reconfigure the device to use an Alternate Repository for those applications *before* configuring the device to use SMARTsend.

## Manage Xerox Devices

The Manage Xerox Devices page is the focal point for discovering, adding, and configuring Xerox devices for use with SMARTsend. This page is accessible from the Administration Home Page by clicking the Add/Update Xerox Devices link in the Site Configuration panel, or by clicking the View Xerox Devices link in the Manage Xerox Devices panel.

The screenshot shows the 'Manage Xerox Devices' page in the SMARTsend Administration interface. The page title is 'Manage Xerox Devices' and it includes a warning: 'Warning: Configuring a device will overwrite its current scan settings. Other applications that use the current template pool or default file repository scan settings will stop working.' Below the warning is an 'Add Devices' section with a text input field for 'Enter hostnames or IP addresses here' and buttons for 'Add To List' and 'Discover Now'. A table titled 'Xerox Multifunction Devices' displays a list of devices with columns for Status, Hostname or IP Address, Description, Location, and Error Message. The table contains 6 items. At the bottom of the page, there is a 'XEROX' logo and buttons for 'Configure', 'Test Configuration', 'Repair', and 'Delete'. The footer of the page includes 'Build: 2.0.20.0' and 'Copyright © 2001-2005 Xerox Corporation. All rights reserved.'

| Status                   | Hostname or IP Address       | Description             | Location             | Error Message |
|--------------------------|------------------------------|-------------------------|----------------------|---------------|
| <input type="checkbox"/> | redstar.na.xde3.xerox.org    | Configured on 8/15/2005 | 0855 - Lab4          |               |
| <input type="checkbox"/> | cowboys.na.xde3.xerox.org    | Discovered on 8/15/2005 | 855 Lab 4            |               |
| <input type="checkbox"/> | DSP-ORANGEMEN                | Discovered on 8/15/2005 | Building 855 Lab 4   |               |
| <input type="checkbox"/> | dsp-spode2.na.xde3.xerox.org | Discovered on 8/15/2005 | Building 888 - Lab 4 |               |
| <input type="checkbox"/> | muskscan.na.xde3.xerox.org   | Discovered on 8/15/2005 | Lab 4 Bldg 855       |               |
| <input type="checkbox"/> | spaceghost.na.xde3.xerox.org | Discovered on 8/15/2005 | Bldg 855 - lab 4     |               |

Figure 4-2: Manage Xerox Devices Page

## Adding and Discovering Devices

When SMARTsend is first installed, you must configure it for use by adding one or more devices. This can be accomplished by using the automated device discovery features provided by SMARTsend, or by manually entering the individual IP Addresses or Host Names of the devices you want to use with SMARTsend. Keep in mind that SMARTsend uses SNMP broadcast to discover Xerox Multifunction Devices that are capable of supporting network scanning, and the discovery process may take considerable time on large networks with many devices. Therefore, manual entry of IP Addresses or Host Names may be faster under some conditions.



**CAUTION:** SMARTsend discovery locates Xerox Multifunction Devices that are capable of supporting network scanning, but it does not confirm that each device is properly configured for network scanning. To avoid problems, please confirm that each device to be used with SMARTsend is properly configured before you add a device to SMARTsend. See *Device Communication and Configuration Issues* on page 7-6 for additional information.

### The following options enable you to discover and configure devices for use with SMARTsend:

- **Enter Host Names or IP Addresses** (*Add Devices panel*)—This feature provides a direct method of adding specific devices to the Xerox Multifunction Devices list. Simply enter the Host Names or IP addresses of the device and then click the Add To List button. To enter multiple devices, use a semicolon to separate each entry. This option may be preferable on larger networks where the automated discovery process can take a considerable amount of time.

**NOTE:** Devices that have been manually added to the Xerox Multifunction Devices list are never removed via automated cleanup. The user must explicitly delete the device in order to remove it from the list. See *Deleting Devices* on page 4-14 for more information.

- **Discover Now** (*Add Devices panel*)—This feature provides an automated method of locating Xerox Multifunction Devices that are capable of supporting network scanning. By default, SMARTsend searches only in the local subnet. Any devices found during this discovery will be displayed in the Xerox Multifunction Devices list.

**NOTE:** Automated discovery is only initiated via the Discover Now button. When the Discover Now button is clicked, devices that respond to the SNMP broadcast issued on the local subnet and any additional user subnets with the SNMP credentials entered on the Configure Discovery Settings - SNMP Credentials page are added or updated in the Xerox Multifunction Devices list. Any device that was previously discovered automatically and has not been discovered within the last 24 hours will be removed from the list.

**NOTE:** If SNMP Broadcast is not enabled across routers, you will not be able to utilize the SMARTsend Discover Now feature. See *Device Communication and Configuration Issues* on page 7-6 for more information.

- **Configure Discovery Settings > Subnets** (*Device Tasks panel*)—This feature enables you to add additional subnets to the SMARTsend broadcast discovery. See *Configure Discovery Settings - Subnets* on page 4-17 for more information.

**NOTE:** The subnet values displayed within SMARTsend are actually broadcast addresses. Do not use the Discover Now option if your network security policies do not permit SNMP broadcast discovery. In addition, if scanning devices are located on a different subnet, DNS must be properly configured and functional. See *Verifying the SMARTsend Computer DNS Configuration* on page 2-8 for more information.

- **Configure Discovery Settings > SNMP Credentials** (*Device Tasks panel*)—This feature enables you to add additional SNMP credentials to the SMARTsend broadcast discovery. See *Configure Discovery Settings - SNMP Credentials* on page 4-17 for more information.
- **Edit Device Configuration Defaults** (*Device Tasks panel*)—This feature enables you to configure the defaults that SMARTsend uses for device configuration. See *Edit Device Configuration Defaults* on page 4-18 for more information.

## Using the Xerox Multifunction Device List

The Manage Xerox Devices page provides options for sorting and viewing the list of Xerox Multifunction Devices.

### Sort

Click on the column headings to sort the list according to the data in the selected column.

### Display

The display feature sets the number of devices that will be displayed in the list at one time.

### Paging

When multiple pages of devices are available in the Xerox Multifunction Devices list, the page feature enables you to select the individual pages to be displayed.



You can use the navigation arrows ◀ ▶ to step forward or backward through each page in the list. You can also jump directly to the first or last page in the list by using the ◀◀ or ▶▶ arrows.

### Show/Hide Columns

The show/hide columns feature provides options for customizing the device configuration fields that are displayed on the Manage Xerox Devices page. These options are useful when devices are configured with different SNMP settings, or to simply provide more information to help you manage devices from a single page.

The show/hide columns link enables you to configure the following display options:

- IP Address
- SNMP Version
- SNMP v2c GET Community Name
- SNMP v2c SET Community Name
- SNMP v3 Username
- System Description
- Description
- Location
- Error Message
- Protocol

**NOTE:** If SNMP v3 is not enabled on the SMARTsend computer, the SNMP v3 Username option will not be available in this list.

When you open the show/hide columns dialog, you can select the fields that will be displayed on the Manage Xerox Devices page. Simply deselect any fields that you do not want to display. Click the OK button when you are finished configuring the fields.

## Device Configuration and Status Icons

A variety of icons are used on the Manage Xerox Devices page to indicate status and provide links to additional device configuration pages. The icons are described in the following table:

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p><b>Available Devices</b>—this icon appears next to Xerox devices that SMARTsend has discovered via SNMP Broadcast, as well as any devices that have been added to the list by typing the device Host Name or IP Address. These devices are ready to be configured for use with SMARTsend.</p>                                                                                                                                                                                                                                                                                                                                                          |
|    | <p><b>Configured Devices</b>—these icons appear next to Xerox devices that are currently configured to work with SMARTsend. When the icon includes a lock symbol, it indicates that the device supports authentication. When the icon includes the tools symbol, it indicates that the device was configured manually. Configuration and status information may be displayed in the list of Xerox Multifunction Devices, and each device can be reconfigured as needed. You can determine if a device is currently configured properly by selecting the check box for a device, then clicking the Test Configuration button located beneath the list.</p> |
|    | <p><b>Unavailable Devices</b>—this icon appears next to devices that have previously been configured for use with SMARTsend, but have become unavailable for use due to a device configuration problem. These devices will not function with SMARTsend unless their configuration is repaired or the device is manually reconfigured to work with SMARTsend. See <i>Device Communication and Configuration Issues</i> on page 7-6 for more information.</p>                                                                                                                                                                                               |
|   | <p><b>Device Properties</b>—click this icon to open the Edit Xerox Device Properties page, which enables you to view and edit the device configuration settings. See <i>Edit Xerox Device Properties</i> on page 4-22 for additional information.</p>                                                                                                                                                                                                                                                                                                                                                                                                     |
|  | <p><b>Configure</b>—click this icon when you have selected a Xerox device that you want to configure for use with SMARTsend. If the configuration fails, the status will be updated and troubleshooting information will be displayed in the Error Message column.</p>                                                                                                                                                                                                                                                                                                                                                                                    |
|  | <p><b>Test Configuration</b>—click this icon to determine if a Xerox device is properly configured for use with SMARTsend. The test will check the device configuration settings that are utilized by SMARTsend, and the test results for each device will be displayed in a separate window. See <i>Test Device Configuration</i> on page 7-7 for additional information.</p>                                                                                                                                                                                                                                                                            |
|  | <p><b>Repair</b>—click the Repair icon to correct configuration problems with a device that is no longer functioning properly with SMARTsend. SMARTsend will attempt to reconfigure the required settings, and will update the status accordingly. See <i>Repairing a Device Configuration</i> on page 5-7 for additional information.</p>                                                                                                                                                                                                                                                                                                                |
|  | <p><b>Delete</b>—click the Delete icon when you want to remove a Xerox device from the list on the Manage Xerox Devices page.</p> <p><b>NOTE:</b> When you delete a configured device, the published scan templates associated with the device will be deleted. Workflows associated with the publications will not be deleted.</p>                                                                                                                                                                                                                                                                                                                       |
|  | <p><b>Error Message/Troubleshooting Information</b>—when SMARTsend detects a device configuration issue, additional information will be displayed in the Error Message column. If more detailed diagnostic and troubleshooting information is available, you can click the icon to investigate the problem and take corrective action.</p>                                                                                                                                                                                                                                                                                                                |

Table 4-2: Device Configuration and Status Icons

## Configuring a Device for use with SMARTsend

After devices have been discovered and added to the Xerox Multifunction Devices list on the Manage Xerox Devices page, they can be selected and configured for use with SMARTsend. Simply click the checkboxes to select or deselect individual devices, then click the Configure button to configure the selected device(s).

**NOTE:** Some SMARTsend options and buttons located at the bottom of the page may not be visible on all displays. Use the scroll bar on the right side of the window to scroll to the bottom of the page.

### ► To configure a device for use with SMARTsend:

- 1 From the Administration Home Page, click the **Add/Update Xerox Devices** link within the Site Configuration panel on the left side of the page.
- 2 If needed, populate the Xerox Multifunction Devices list by clicking the **Discover Now** button, or by entering individual device Host Names or IP Addresses manually and clicking the **Add To List** button. See *Adding and Discovering Devices* on page 4-9 for more information.
- 3 Identify the device(s) you would like to configure for use with SMARTsend by selecting the check box to the left of each device Host Name or IP Address. If needed, click the **Device Properties** icon to configure the SNMP and Data Transfer Settings for the device. See *Configuring a Device for use with SMARTsend* on page 4-13 for more information.
- 4 Click the **Configure** button that is located below the Xerox Multifunction Devices list.

**NOTE:** If an error is encountered when using SMARTsend to configure a device, SMARTsend will attempt to rollback the device scan settings to the previous values. This rollback feature does not work if the device had been configured for NetWare scanning.

- 5 The Confirm Device Accounts dialog will be displayed if this is the first device being configured. It will also be displayed if the previous device accounts have been deleted from the computer. Click **OK** to create the specified accounts, or click **Cancel** if you prefer to create and manage your own device accounts. See *Create Administrator, User, and Device Accounts* on page 2-13 and *Manage Device Accounts* on page 4-15 for additional information.

**NOTE:** You may be prompted to enter your SMARTsend computer credentials when you add a device. You must use the same credentials you used to log into SMARTsend. If you supply different credentials, you may need to clear your browser cache before you can proceed.

- 6 SMARTsend will update the network scanning settings on the device to reflect the new computer, account, and default path. Once device configuration is complete, SMARTsend displays the Xerox Device Configuration status window, which reports the success or failure of the operation. The status window also confirms the transfer protocol and SNMP version that will be used for filing, and will provide additional diagnostic information if one or more devices could not be configured by SMARTsend. Click **OK** to return to the Manage Xerox Devices page.
- 7 Devices that have been successfully configured will display the Configured Devices icon  within the Xerox Multifunction devices list.

- 8 If a device configuration fails due to a temporary communication error, you may attempt to reconfigure the device again. See *Device Communication and Configuration Issues* on page 7-6 for more information.
- 9 If a device cannot be configured using the above procedures, a manual configuration may be required. See *Manually Configure This Device* on page 4-22 for more information.

## Deleting Devices

This option deletes any device that is selected on the Manage Xerox Devices page. When a device is deleted, any Device Scan Templates that have been published to the device are also deleted. Workflows are not affected by this operation.

### ▶ To delete a device from the Xerox Multifunction Devices list:

- 1 From the Administration Home Page, click the **View Xerox Devices** link.
- 2 Identify the device(s) you would like to delete by selecting the check box to the left of each device Host Name or IP Address.
- 3 Click the **Delete icon**  located in the column on the right to delete an individual device, or the **Delete** button that is located below the list if you need to delete several devices.
- 4 The Confirm Delete Device(s) dialog appears. Click **OK**.
- 5 The Delete Device(s) Status page appears. Click **OK** to return to the Manage Xerox Devices page. The deleted device(s) will be removed from the Xerox Multifunction Devices list.

**NOTE:** Keep in mind that the publications associated with a device will also be deleted, if the publications do not reside on any other device(s).

## Manage Device Accounts

The Manage Device Accounts page displays the Local User accounts that SMARTsend creates automatically for each data transfer protocol that is selected on the Edit Device Configuration Defaults page. These accounts enable Xerox devices to communicate with the SMARTsend computer. The following accounts are created by default:

- FF\_SMARTSEND\_FTP
- FF\_SMARTSEND\_SMB
- FF\_SMARTSEND\_HTTP
- FF\_SMARTSEND\_HTTPS

SMARTsend creates separate accounts for each protocol due to security reasons. For example, FTP uses clear text to transmit passwords and other data, which makes it less secure than the SMB and HTTPS protocols.

**NOTE:** Earlier versions of SMARTsend did not create device accounts automatically. With SMARTsend 2.0 and later, local user device accounts are automatically created on the SMARTsend computer for each supported protocol.

## Confirm Device Accounts

The Confirm Device Accounts dialog will be displayed before accounts are actually created on the SMARTsend computer. This dialog provides the opportunity to cancel the account creation process if you prefer to create the device accounts manually. See *Manage Your Own Device Accounts* below for additional information.

This dialog also appears during the process of configuring or repairing a device if the device accounts have been manually deleted from the SMARTsend computer. If this occurs, SMARTsend will recreate the accounts.

## Manage Your Own Device Accounts

The Manage your own device accounts option enables you to create or modify device accounts manually using Microsoft Management Console (MMC). This option may be preferred for security reasons or for compliance with other network administration policies.

You may choose to create new accounts using MMC, or re-use the SMARTsend device accounts if they have already been created. If you create or modify any device account with MMC, then you must change the SMARTsend device account settings on the Manage Device Account Credentials page to match the account credentials on the SMARTsend computer. You must then click **OK** or **Apply** to save the changes and reconfigure the devices with the new device account credentials.

**NOTE:** Devices that have been configured manually will continue to use the device account that was used during manual configuration. See *Manually Configure This Device* on page 4-22 for additional information.

## Consider the following recommendations if you choose to manage device accounts manually:

- Local User accounts are recommended for this purpose, and each account should be removed from the Users Group to provide additional security.

- Domain accounts may be used in many cases, but they may not be supported on some older Xerox devices.
- Administrator accounts should not be used for Device Accounts.
- If security issues are not a concern, you can use a single account for all protocols.
- A Username and Password are required for all accounts.
- If any device account is changed using Microsoft Management Console, the corresponding change must be made in SMARTsend on the Manage Device Account Credentials page.
- If any device account is changed within SMARTsend, the corresponding change must be made on the SMARTsend computer using Microsoft Management Console.

See *Create Administrator, User, and Device Accounts* on page 2-13 for more information.

## Configure Discovery Settings - Subnets

The Configure Discovery Settings - Subnets page enables you to add additional subnets to the SMARTsend broadcast discovery configuration.

### Adding a Subnet

- 1 From the Manage Xerox Devices page, click the **Configure Discovery Settings... > Subnets** link.
- 2 Enter a valid IP Address for the target subnet and the corresponding Subnet Mask.
- 3 Click **Add**. SMARTsend will calculate the corresponding Broadcast Address for the subnet and add it to the list of Subnet Broadcast Addresses.

The Subnet Broadcast Addresses in the list will be searched whenever the Discover Now feature is used.

### Deleting a Subnet

- 1 Click on the item in the Subnet Broadcast Addresses list.
- 2 Click **Remove**.

## Configure Discovery Settings - SNMP Credentials

The Configure Discovery Settings - SNMP Credentials page enables you to enter additional SNMP credentials that SMARTsend will use for device discovery when you click the Discover Now button. Additional SNMP credentials should be added if your Xerox devices have been configured with non-default SNMP credentials. The SNMP credentials in SMARTsend must match the SNMP credentials on the device(s) you want to discover with SMARTsend. When devices are discovered with these credentials, SMARTsend will automatically configure the device with the appropriate SNMP settings.

From the Manage Xerox Devices page, click the **Configure Discovery Settings... SNMP Credentials** link to configure the following SNMP settings:

**SNMP v2c**—enables you to enter additional GET community names. Enter each name in the GET Community Name field, then click the **Add** button. To delete an existing Community Name, simply select the box next to the name, then click the **Remove** button located beneath the list.

**SNMP v3**—enables you to enter additional SNMP v3 account credentials. Enter each Username in the Username field, along with the corresponding Authentication and Privacy passwords, and then click the **Add** button. To delete an existing account, simply select the box next to the account name, then click the **Remove** button located beneath the list.

**NOTE:** The SNMP v3 options are not displayed if SNMP v3 is not enabled within SMARTsend. From the Administration Home Page, click **Device Configuration Defaults...** under the Manage Xerox Devices section. See *Edit Device Configuration Defaults* on page 4-18 for additional information.

## Edit Device Configuration Defaults

The Device Configuration Defaults enable you to customize and prioritize the settings SMARTsend will use when configuring devices. To access this page, open the Manage Xerox Devices page and click the Edit Device Configuration Defaults... link in the left panel.

**NOTE:** Changing these settings will not affect devices that have already been configured.

If necessary, these settings can be changed for each individual device by editing the device properties. Device properties can be accessed from the Manage Xerox Devices page by clicking on the Device Properties icon .

## Data Transfer Protocols

The Data Transfer Protocol options define the protocols that can be used to transmit data between the SMARTsend computer and the Xerox Multifunction Devices. The supported protocols must be enabled within SMARTsend in order for them to be utilized when configuring devices.

**NOTE:** If you are allowing SMARTsend to manage the device accounts that will be used for filing, an account will be created on the SMARTsend computer for each selected protocol.

**TIP:** Confirm that the ports required for each supported protocol are not blocked by filtering at a switch, router, or firewall. See *TCP/IP Port Configuration* on page 2-29 for additional information.

### Enabled

The Enabled selection box lists the protocols that SMARTsend supports. Check the boxes to enable protocols that are supported by your Xerox Multifunction Devices and your application computer:

- **FTP**—Use for faster data transfer and compatibility with all devices. The FTP filing protocol is the default setting. Keep in mind that the IIS FTP service must be enabled and running on the SMARTsend computer if FTP filing is used. See *Install and Configure IIS / FTP* on page 2-10.
- **SMB**—Use for more secure data transfer. If SMB is selected when SMB is not supported (or configured) on the device, then an alternate protocol will be used, as defined by the Priority setting (see below).
- **HTTP**—Use for faster data transfer. This protocol may not be supported on older devices.
- **HTTPS**—Use for more secure data transfer. This protocol may not be supported on older devices.

**NOTE:** If a device does not support SMB or HTTP or HTTPS, you must add FTP support to IIS on the SMARTsend computer. If FTP support has been added to IIS after SMARTsend was installed, run Add/Remove Programs, select SMARTsend, click **Change**, and click **Repair** to update the application. See *Install and Configure IIS / FTP* on page 2-10 of Chapter 2, *Prepare for Installation*.

## Priority

The Priority setting enables you to define your data transfer protocol configuration preferences. SMARTsend will initially attempt to configure each device with the protocol at the top of the list. If the first protocol is not available, it will then attempt to use the second protocol in the list, and so on.

To define the Data Transfer Protocol priority, click on a protocol in the Priority list, and then click on the Move Up and Move Down buttons to arrange each protocol in the desired sequence. Items at the top of the list will have the highest (first) priority.

## Device Administrator Password

The Device Administrator Password is an optional security setting that affects device configuration. Each Xerox device is configured with an administrative password that is intended to control access to advanced device configuration settings. By default, SMARTsend does not require this password when it configures devices. If this extra level of security is desired, the default setting can be changed to require validation of the Device Administrator Password whenever devices are configured.

**Validate password upon device configuration**—when selected, SMARTsend will validate the Device Administrator Password whenever it attempts to configure a Xerox device.

**Default Admin Password / Confirm Admin Password**—when the validate password option is active, you must enter and confirm the Device Administrator Password in the corresponding fields. This is the password that is used for validation when a device is configured.

## SNMP Settings

The default SNMP Settings enable you to configure how SMARTsend communicates with Xerox Multifunction Devices during device discovery and configuration. Consider the following issues when adjusting the SNMP settings:

- SNMP v2c will be used for device discovery and configuration by default if SNMP v3 is not enabled.
- To use SNMP v3 for discovery and configuration, it must be enabled on the Edit Device Configuration Defaults page and the device administrator must configure each device to support SNMP v3.
- Devices that are manually added to the Xerox Multifunction Devices list (by entering a Host Name or IP address) will be configured using the default SNMP v2c Community Names or SNMP v3 Account Credentials (if supported).
- Devices that are automatically added to the Xerox Multifunction Devices list (using the Discover Now feature) will be configured using the SNMP credentials obtained from the device upon discovery.

### SNMP v2c Defaults

SNMP Community Names (GET/SET) are used when exchanging information with devices via SNMP v2c. The SNMP SET name is generally used to write or modify values on a device. The SNMP GET name is generally used to retrieve values from a device.

SMARTsend uses the SNMP Community Names for authentication during device discovery and configuration. Devices that are discovered by SMARTsend will use the GET name they were discovered with, and the default SET name for configuration. Devices that were added by manually entering their IP Addresses or Host Names will use both the default GET and SET names. If the devices to be used with SMARTsend have GET and SET names other than the default values of "public" and "private," you must enter the appropriate default names within SMARTsend, or modify the SNMP Community Names for each device on a case-by-case basis using the device properties page.

### Enable SNMP v3

Enabling SNMP v3 on the Edit Device Configuration Defaults page makes SNMP v3 the default protocol that SMARTsend will use for discovering and configuring devices. If SNMP v3 is not supported on a device, SMARTsend will revert to using SNMP v2c.

### SNMP v3 Defaults

SNMP v3 requires an account that provides the credentials needed to establish communication between the Xerox Multifunction Device and the SMARTsend application. The default account configuration options for SMARTsend can be configured on the Edit Device Configuration Defaults page.

### *Account Type*

This option enables you to select the default type of SNMP v3 account that SMARTsend will use. These settings must match the SNMP v3 account settings that are configured on the Xerox devices to be used with SMARTsend. The account configuration options will change based on the type of account you choose. The following options are available:

- **Xerox Client Account (default)**—provides the minimum device access required to support SMARTsend device configuration and network scanning services. Use of this setting with the default account Username and Password is recommended.
- **Custom Account**—provides a higher level of administrative security. The custom account settings must match the settings on the Xerox device, which can be configured using the device's Internet Services web pages to edit the SNMP v3 Administrator Account. Other custom accounts may also be configured on Xerox devices using third-party device management tools.

The following credentials must be configured when the SNMP v3 Custom Account setting is enabled:

- **Username**—enter the Username that matches the Username on your Xerox devices.
- **Authentication and Privacy Passwords**—enter the passwords that match the passwords on your Xerox devices.

## Edit Xerox Device Properties

Click on the Device Properties icon  to open the Edit Xerox Device Properties page. This icon provides access to the device properties that SMARTsend uses for communication, configuration, and data transfer. These settings include:

**Selected Device**—provides general information to help identify the device.

**Manual Configuration**—provides a means of manually configuring devices for use with SMARTsend. See *Manually Configure This Device* below for more information.

**Device Properties**—provides access to the SNMP and Data Transfer Settings. The settings displayed in these panels can be modified as needed. See *SNMP Settings* on page 4-20 for more information.

Click the **Configure** button at the bottom of the page to configure the selected device using the properties defined on this page. Click **Cancel** if you do not want to change these settings.

### Manually Configure This Device

SMARTsend provides the option to configure devices manually using the Internet Services web pages that are available on Xerox Multifunction Devices. This option can be used if the SMARTsend automatic configuration fails or is unavailable due to device limitations or SNMP constraints. See *Device Communication and Configuration Issues* on page 7-6 for additional information.

► *To manually configure a Xerox device:*

- 1 Click **Add/Update Xerox Devices** on the Administration Home Page.
- 2 If necessary, add the device to the Xerox Multifunction Devices list by using the Discover Now feature, or by typing the IP Address or Host Name and clicking the **Add to List** button.
- 3 Locate the Xerox device on the Manage Xerox Devices page, then click the corresponding Device Properties icon .
- 4 Click the **Manually configure this device** check box in the Manual Configuration panel of the Edit Xerox Device Properties page.
- 5 Adjust the SMARTsend **Data Transfer Settings**, **Device Capabilities**, and **Device Account** settings as needed. See *Configuring Device Properties* below for additional information.
- 6 Click the **Configure** button at the bottom of the Edit Xerox Device Properties page.
- 7 Click **OK** on the Manual Device Configuration Status page.
- 8 The Manual Device Configuration Instructions page will then display the scan settings that must be configured on the device. Click the **View Device Web Page** button to access the Internet Services web pages for the device.
- 9 From the device's Internet Services home page, select **Properties > Services > Network Scanning** to configure the Default Repository and **Properties > Services > Network Scanning > Advanced** to

configure the Template Pool settings on the device. These settings must match the SMARTsend settings that are displayed in the Manual Device Configuration Instructions page.

**NOTE:** For newer Xerox Multifunction Devices, SMARTsend requires that the Login Credentials Source (labeled Login Credentials Access to the Destination on the device's web embedded server's File Repository Setup page) be set to System. When manually configuring a newer Xerox Multifunction Device, please access the device's embedded web server and confirm that the value is set to System. If you are not manually configuring a new Xerox Multifunction Device, SMARTsend will take care of this setting.

- 10 Close the Internet Services web page, then click **OK** on the Manual Device Configuration Instructions page to complete the manual configuration process.

## Configuring Device Properties

When the **Manually configure this device** option is selected, the options on this page change to accommodate the requirements of the manual device configuration process. This process requires adjustment of the following Device Properties:

**Data Transfer Settings**—enables you to choose the protocol that will be used to transfer data between the device and the SMARTsend computer. The protocol settings on the device and the SMARTsend computer must be consistent and compatible. See *Data Transfer Protocols* on page 4-18 for more information.

**Device Capabilities (Limited/Full)**—enables you to choose the scanning capabilities of the Xerox device you are attempting to configure. Choose the option that corresponds with the scanning capabilities that your Xerox device provides, as listed in the following table:

| Scanning Attributes        | Limited       | Full          |
|----------------------------|---------------|---------------|
| Template Name Length Limit | 11 Characters | 20 Characters |
| Authentication Support     | Not Supported | Supported     |
| PDF Filing Support         | Not Supported | Supported     |

**Table 4-3: Device Capabilities Settings for Manual Configurations**

**NOTE:** Please consult the documentation provided with your Xerox system to determine if these scanning attributes are supported. If the Device Capabilities settings in SMARTsend do not match the capabilities of the device, SMARTsend will not be able to properly restrict or permit the publishing of workflows with the correct attributes.

**Assign SMARTsend Device Account**—enables you to define the network account that the device will use to communicate with the SMARTsend computer. When manually configuring one or more devices, you should create a separate device account on the SMARTsend computer and enter the Username here. See *Create Administrator, User, and Device Accounts* on page 2-13 for additional information. If the account password for the assigned SMARTsend account changes, you must return to this page and click the View Configuration Instructions button to update the account credentials for the device.

# Configure PaperWare Internet Fax Settings

## Professional Edition Feature

The Professional Edition of SMARTsend provide the ability to use PaperWare cover sheets with devices that support the Internet Fax protocol. PaperWare Internet Fax capabilities support a broader range of scanning devices, as well as many unique features that enhance the usability and versatility of SMARTsend.

To access the PaperWare Internet Fax Settings on the PaperWare Settings page, click the **Configure PaperWare Internet Fax Settings** link on the Administration Home Page.

**NOTE:** SMARTsend requires that a dedicated POP3 e-mail account be created for the Internet Fax inbox on the incoming mail (POP3) server.

### *Server Information*

Enter the fully qualified DNS names or IP Addresses of the Incoming Mail (POP3) and Outgoing Mail (SMTP) servers that will be used by SMARTsend for Internet Fax support. These servers can be identical to the SMTP server that SMARTsend uses for scanning to e-mail.

**Same as e-mail mail server (SMTP)**—If the same SMTP server will be used for Internet Fax outgoing mail and SMARTsend e-mail features, then select this option to avoid re-entering the outgoing mail server information.

**Polling Interval**—Enter the frequency at which the POP3 server will be polled for incoming mail. By default, the POP3 server will be polled once every 10 minutes.

### *POP3 Logon Information*

Enter the dedicated POP3 e-mail account user name and password that will be used by SMARTsend to log on and retrieve mail from the POP3 server.

## Setup E-mail and Address Book

The Setup E-mail and Address Book link on the Administration Home Page enables you to configure the SMARTsend SMTP and LDAP server configuration settings. These settings are required to enable SMARTsend features such as scan to e-mail and e-mail confirmation/notification messages, and the integrated address book features that enable users to enter part of a name in the SMARTsend fields that specify e-mail addresses as scanning destinations.

When you have finished entering SMTP and LDAP server information, click **Apply** to save your settings or click **Reset** to remove changes.

### SMTP Server Configuration

SMARTsend uses the SMTP (Simple Mail Transfer Protocol) server for outgoing e-mail only. SMARTsend features that require a configured SMTP Server include scan to e-mail destinations, scan job confirmations, administrative event notifications, and configuration test messages. These SMTP-based features may be considered optional, but they are recommended and will not function until a SMTP Server is properly configured within SMARTsend.

To configure these settings, enter the fully qualified DNS name or IP address of the SMTP server, port and authentication method (Username and Password) required by your SMTP server and click **Test**. If SMARTsend can contact the SMTP server and send a test message to the SMARTsend administrator, a status of **Succeeded** appears. If the test fails, you should confirm that the server information and the Reply To e-mail address was entered correctly. Also note that firewall or antivirus settings may block network traffic on port 25, which may be required for SMTP communication. If needed, modify the firewall or antivirus configurations to permit SMTP communication on port 25, then test the configuration again. If the test fails after confirming all these settings, check to see if the SMTP server is accessible and functioning properly with other applications to determine if the problem resides with the SMTP server.

**NOTE:** The Test button for the SMTP server uses the SMARTsend Administrator E-mail Address that is defined on the General Settings page (Administration Home Page >> General Settings >> Administrator Contact Information). The test will fail if a valid e-mail address is not provided in this field. See *Update Administrator Contact Information* on page 4-35 for more information.

### E-mail Signature Configuration

This feature enables you to edit the e-mail signature that SMARTsend places on all of its scan to e-mail messages. To restore the original signature, click **Restore to System Default**.

**NOTE:** Mail servers may impose file size limitations and limit the number of individual files that can be sent as attachments. SMARTsend Scan to E-Mail jobs that exceed these limitations will fail. The site administrator should notify users of the limitations that apply to SMARTsend Scan to E-Mail jobs.

## LDAP Server Configuration

LDAP (Lightweight Directory Access Protocol) is an optional configuration setting that is only applicable to the SMARTsend integrated address book lookup feature. When this feature is configured, SMARTsend uses LDAP to obtain and confirm e-mail address information when a user enters part of a name in the SMARTsend fields that specify e-mail addresses as scanning destinations.

To configure SMARTsend to use LDAP for e-mail address lookups, you need to enter the fully qualified DNS name or IP address of the LDAP server. To specify the use of SSL encryption when connecting to an LDAP server for address book lookup, select the SSL checkbox in the LDAP Server Configuration section of the page.

When the SSL checkbox is checked and a user name and password has been entered for the LDAP server, SMARTsend will use SSL encryption when connecting to the LDAP server.

### LDAP Authentication

If the LDAP server requires authentication (when it does not support anonymous directory access), then you will also need to enter credentials for the LDAP server. The credentials are the account Name and Password that the LDAP server requires for authentication.

After entering the LDAP server configuration information, click **Test** to verify the configuration. If SMARTsend can communicate with the LDAP server, a status of **Succeeded** appears. If the test fails, you should confirm that the LDAP server name and credentials you entered in SMARTsend match the actual server name and credentials that are configured on the LDAP server, then test the configuration again. If the test still fails, you should check your LDAP server to confirm that it is configured properly and is functioning with other applications that use LDAP.

### LDAP Property Mappings

SMARTsend provides the default LDAP Property Mapping for the E-mail Address (mail), Name (cn), and City (l) attributes. These default settings should match the defaults for most LDAP servers. If your LDAP server uses different mappings, you will need to change these SMARTsend mappings to match the mappings that are defined on your LDAP server. For further assistance, contact your LDAP server administrator.

## Publish the My E-mail Workflow

The My E-Mail workflow is used to automatically e-mail a scanned document to the submitter's e-mail account. The submitter is any SMARTsend user who logs into a Xerox Multifunction Device that supports authentication, or a SMARTsend user whose name appears on the PaperWare cover sheet (Professional Edition feature). The My E-mail Workflow is created automatically when SMARTsend is installed.

The My E-Mail workflow provides several unique advantages:

- It enables users to scan to their own e-mail accounts without creating a workflow.
- One workflow can be published as a single template to provide multiple users with scanning capabilities, rather than each user publishing their own unique scan to e-mail templates.

**NOTE:** This feature is only available for publication to Xerox Multifunction Devices that are configured to use authentication. If a device that is configured for authentication has not been added to SMARTsend, this option appears in small, gray, title-case characters and is unavailable.

From the Administration Home Page, select **Publish the My E-mail Workflow** to access the Publish Workflow to Xerox Multifunction Device page. You can then configure the Publication Settings, Document Attributes, and Scan Profile, and select the device(s) on which to publish the workflow. Consult chapters 3 and 4 of the SMARTsend User Guide for detailed information on creating and publishing workflows.

After the My E-mail workflow is published, the Publish the My E-mail Workflow link on the Administration Home Page changes to a View My E-mail Publication link. This link opens the Publication details for My E-mail page, which enables an administrator to publish the My E-mail workflow to additional devices. After the My E-mail workflow has been published, please inform SMARTsend users that they must log in to the SMARTsend site and enter their email address. The user's e-mail address will be used as the destination for the My E-mail workflow. If a user's e-mail address is not entered into SMARTsend, users will be unable to scan using this workflow..

**NOTE:** To modify the publication settings for the My E-mail workflow, you must delete the publication and then republish the My E-mail workflow with new settings.

## Schedule a Backup

The backup feature copies SMARTsend registry settings, workflows, device database, account database, publications, available services, file attributes, service account credentials, and administrative settings to a backup set that is catalogued by date and time. Program files and templates are not included, although templates are reconstructed from other data when running the Restore Tool, which is discussed in Chapter 7, *SMARTsend Utilities*.

**NOTE:** This process does not replace the routine of backing up the SMARTsend computer to an external storage device such as a tape drive. Its purpose is to record a snapshot of the SMARTsend installation while the database is not in use. The resulting backup set should be copied to an external storage device as part of the computer's regular backup routine.

### Backup Immediately

It is recommended that the SMARTsend database be backed up immediately before making major system changes or before uninstalling the application. Click **Start Backup** at any time to begin immediate SMARTsend database and registry entry backup. Backup will occur if SMARTsend is not currently in use.

### Schedule a Backup

Schedule backups on a frequent and regular basis. How often to back up the SMARTsend database depends on factors such as these:

- The frequency and volume of changes within SMARTsend, such as the addition of new devices, workflows, and publications.
- Available storage capacity (hard disk space) on the SMARTsend computer.

The Backup Interval setting permits you to choose among the following backup schedules:

- No Scheduled Backup (*not recommended*).
- **Once**. Performs one backup at the specified date and time.
- **Daily**. Performs a backup every 24 hours, starting at the designated date and time.
- **Weekly**. Performs a backup every seven days, starting at the designated date and time.

Use the built-in clock/calendar to assign a starting date and time for a scheduled backup. Choose a time when the SMARTsend computer is least likely to be in use to avoid performance degradation issues. When finished with configuring the SMARTsend database backup options, either save the new backup settings and implement the backup schedule by clicking **Apply**, or discard all changes by clicking **Reset**.

**NOTE:** If the computer is down during the scheduled backup time, the scheduled backup will be performed when the computer resumes operation. Periodically checking the Backup Status area of the Administration Home Page to confirm successful backups is recommended.

SMARTsend creates the following folder for backup storage:

```
<drive>:\Inetpub\wwwroot\SMARTsend\Data\Backup\
```

The backup filenames are based on the following naming convention:

```
FreeFlow SMARTsend_<year_month_day_hours_minutes_seconds>\<Backup_ID>.
```

The backup can be restored to the SMARTsend computer using the Restore Tool. See *Restore Tool* on page 8-12 of Chapter 8, *SMARTsend Utilities* for more information.

## Configure Service Settings

SMARTsend supports several different types of services that can be configured as scanning destinations. These services include network and FTP folders, remote printers, web and URL folders, and various document management repositories, such as DocuShare, SharePoint Portal Server, and Domino repositories. Most of these services appear as SMARTsend destinations, which are available to users when they create workflows. Other services, such as Optical Character Recognition (OCR), provide additional scanning options, such as the output file types that are available when defining workflows.

Following are the SMARTsend destinations that have specific version or configuration requirements:

- DocuShare version 3.1, 4.0 destinations
- Domino version 5.x, 6.0 destinations (Standard or Professional Edition feature)
- Domino.doc version 3.1 destinations (Standard or Professional Edition feature)
- NetWare 5.x, 6.x folder destinations (Standard or Professional Edition feature)
- Network Folders must be Microsoft/SMB folders.

SMARTsend also offers optional components that can be installed separately. The following optional components are currently supported:

- TrueMatch (Professional Edition feature)
- Documentum version 5.2 (Standard or Professional Edition feature)
- Hummingbird version 5.1.0.5 (Standard or Professional Edition feature)
- Interwoven WorkSite version 8 (Standard or Professional Edition feature)
- LiveLink version 9.5.0 (Standard or Professional Edition feature)

SMARTsend administrators have the option to specify which services are available to users. For example, if your organization does not support Domino.doc repositories, you should disable the Domino.doc service in SMARTsend to avoid confusion and improve application performance. Disabling a service on the Configure Service Settings page results in the removal of the corresponding destination on the Workflow Explorer > Document Destinations page.

**NOTE:** Some SMARTsend workflow destinations require that a client or other software be installed on the SMARTsend computer. See *Additional Service Configuration Requirements and Restrictions* on page 4-33 for more information.

## Configure Service Options

The Configure Service Settings page enables you to configure the following services and certain service-related options:

| SMARTsend Services                                     | Description                                                                                                                                                                                                                                                                                                                                  | Configuration Options                                                                                                                                                                                             |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TrueMatch (Professional Edition feature)               | Create and manage search workflows that enable you to locate documents stored in DocuShare and SharePoint Portal Server repositories.<br><br>NOTE: This is an optional component. When using a TrueMatch search workflow to locate a matching or similar electronic version of a document, the documents must have been authored in English. | <ul style="list-style-type: none"> <li>■ Maximum number of documents a user may select to locate</li> <li>■ Maximum search timeout (in minute intervals)</li> <li>■ Maximum retrieve file size (in Mb)</li> </ul> |
| Documentum (Standard or Professional Edition feature)  | Scan to Documentum destinations<br><br>NOTE: This is an optional component that can be purchased from Xerox.                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> </ul>                                                                                                                                                |
| DocuShare                                              | Scan to DocuShare destinations                                                                                                                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> </ul>                                                                                                                                                |
| Domino (Standard or Professional Edition feature)      | Scan to Domino destinations                                                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> <li>■ Metadata Configuration XML</li> </ul>                                                                                                          |
| Domino.Doc (Standard or Professional Edition feature)  | Scan to Domino.Doc destinations                                                                                                                                                                                                                                                                                                              | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> </ul>                                                                                                                                                |
| External Application Connection                        | Scan to a third party application using the command line interface or a scripting language                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> </ul>                                                                                                                                                |
| FTP                                                    | Scan to FTP destinations                                                                                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> <li>■ Enable Document Attribute Field Support (Yes/No)</li> <li>■ Enable Job Log Export Support (Yes/No)</li> </ul>                                  |
| Hummingbird (Standard or Professional Edition feature) | Scan to Hummingbird destinations<br><br>NOTE: This is an optional component that can be purchased from Xerox.                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> <li>■ Username</li> <li>■ Password</li> <li>■ Domain Name</li> </ul>                                                                                 |
| Interwoven (Standard or Professional Edition feature)  | Scan to Interwoven destinations<br><br>NOTE: This is an optional component that can be purchased from Xerox.                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> </ul>                                                                                                                                                |

**Table 4-4: SMARTsend Service Configuration Options**

| SMARTsend Services                                                                 | Description                                                                                                                                                                 | Configuration Options                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft Exchange 2000 Web Folder (Standard or Professional Edition feature)      | Scan to Microsoft Exchange 2000 Web Folder destinations                                                                                                                     | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> </ul>                                                                                                                                                          |
| Microsoft SharePoint Portal Server 2001 (Standard or Professional Edition feature) | Scan to Microsoft SharePoint Portal Server 2001 destinations                                                                                                                | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> </ul>                                                                                                                                                          |
| Microsoft SharePoint Portal Server 2003                                            | Scan to Microsoft SharePoint Portal Server 2003 destinations                                                                                                                | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> </ul>                                                                                                                                                          |
| Netware Folder (Standard or Professional Edition feature)                          | Scan to Novell NetWare Folder destinations                                                                                                                                  | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> <li>■ Enable Document Attribute Field Support (Yes/No)</li> </ul>                                                                                              |
| Network Folder                                                                     | Scan to Network Folder destinations                                                                                                                                         | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> <li>■ Enable Document Attribute Field Support (Yes/No)</li> <li>■ Enable Job Log Export Support (Yes/No)</li> </ul>                                            |
| OCR (Professional Edition feature)                                                 | Configures the Optical Character Recognition (OCR) capabilities. Additional file types become available on the SMARTsend Document Name and Type page when OCR is enabled.   | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> <li>■ Default Source Document Language</li> <li>■ Default Output File Type</li> <li>■ Maximum number of OCR jobs that can be processed concurrently</li> </ul> |
| Remote Printer                                                                     | Scan to a Remote Printer - scans a document and prints it on the printer specified in the workflow.                                                                         | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> </ul>                                                                                                                                                          |
| Scan to URL Service (Standard or Professional Edition feature)                     | Enables users to forward scanned documents to a URL site using the http 'PUT' method. User credentials need to be provided for authentication prior to document forwarding. | <ul style="list-style-type: none"> <li>■ Enable/Disable</li> </ul>                                                                                                                                                          |

**Table 4-4: SMARTsend Service Configuration Options**

## Configuring a Service

### ► To configure a service:

- 1 Click **Configure Service Settings** on the Administration Home Page. The Configure Service Settings page appears.
- 2 All services are enabled by default. To change the status of a service, click its **Edit** link.
- 3 Check or uncheck the **Enabled** checkbox.
- 4 Some services display other options below the services list. Modify these options to suit the needs of your organization. See Table 4-4 and *Service Setting Descriptions* on page 4-32 for more information.
- 5 Click **Apply** to save the selections or **Cancel** to discard them.
- 6 When you have finished configuring the service settings, click the **Home** link in the upper left area of the page.

**NOTE:** The file format types "PDF, Text Searchable," and "Other" require the OCR service to be configured and enabled. When the OCR service is disabled, these file types will not be available on the SMARTsend Document Attributes page. If the OCR service is disabled, all previously created workflows that utilize these file formats will be deleted.

## Service Setting Descriptions

**Metadata Configuration XML**—This feature is intended for Domino systems integrators only.

**Enable Document Attribute Field Support**—This feature enables you to configure metadata support for certain services.

**Enable Job Log Export Support**—This feature is intended for use by advanced users and system integrators. When used with FTP and Network Folder destinations, it provides the capability to export and customize SMARTsend job logs. See *Appendix A - Job Log Export Support* on page 4-43 for additional information.

**Default Source Document Language**—The default preferred language when using Optical Character Recognition (OCR).

**Default Output File Type**—The default output file type when using OCR.

**Maximum number of OCR jobs that can be processed concurrently**—This setting establishes the limits for concurrent OCR job processing. Concurrent processing of multiple jobs can have a negative impact on site performance.

**User Name, Password, Domain Name**—Some services require a valid Windows user account to support authentication and communication between the SMARTsend computer and the destination computer. If these fields are presented for a service, they must be configured properly before the service will function.

## Additional Service Configuration Requirements and Restrictions

- Some SMARTsend services require the installation of a client or other software on the SMARTsend computer in order for the features to function properly. See *Additional Requirements for Destinations* on page 2-19 for more information.
- In order for SMARTsend to communicate properly with a Domino server, Domino Interop (DIIOP) must be running on the Domino server. To start DIIOP after the Domino server is already running, type “load DIIOP” from the Domino server command prompt. To start this task automatically, DIIOP will need to be added to the “Server Tasks” line in the notes.ini file on the Domino server and the Domino server must be restarted. The notes.ini file is found in the root of the Domino directory which by default is c:\lotus\domino. The line in notes.ini should look something like the following:  
“ServerTasks=Update,Replica,Router,AMgr,AdminP,CalConn,Sched,HTTP,LDAP,ddmTran,diiop”.  
The items that come before DIIOP may vary depending on the Domino server configuration.
- The Domino.doc server does not support certain document attribute (metadata) value entries via the device user interface. The server will not process entries that require the user to select from a drop-down list.
- Interwoven WorkSite destinations (*optional component for the Standard and Professional Editions*) do not support free-form text entry of document attributes (metadata). Metadata values for custom fields are restricted to the predefined set of values defined by the WorkSite administrator.
- The External Application Connection service is intended for advanced users and system integrators. A user must have system administrator privileges on the SMARTsend computer in order to create or edit workflows that utilize External Applications as destinations. See *Appendix B - External Application Connection* on page 4-44 for additional information.
- See Chapter 7, *Problem Solving* for more information on potential problems related to SMARTsend services.

## Manage Application Account

When SMARTsend is installed, the installer creates an Application Account as a local Windows account named *FF\_SMARTSEND\_USER*. The Application Account credentials are automatically managed on the SMARTsend computer, and under Local Users and Groups. The account name cannot be changed. See *SMARTsend Authentication* on page 9-12 for more information.

**NOTE:** You may be prompted to enter your SMARTsend computer credentials when you change the application account password. You must use the same credentials you used to log into SMARTsend. If you supply different credentials, you may need to clear your browser cache before you can proceed.

## Changing the Application Account Password

If necessary, the account password can be changed through SMARTsend using the following procedure.

**NOTE:** In order for SMARTsend to function properly, if the password for the *FF\_SMARTSEND\_USER* is changed by the Administrator, the new password must be created such that it complies with the effective security policy for the operating system being used.

### ► To change the Application Account password:

- 1 Choose **Manage Application Account** on the Administration Home Page. The **Manage Application Account Credentials** dialog appears.
- 2 Type the new password and password confirmation.
- 3 Click **OK** to save the changes.



---

**CAUTION:** Do not delete the Application Account or alter the account credentials using Microsoft Management Console (MMC). If the account is deleted, the computer must be rebooted to re-establish the Application Account. If the account credentials are modified using MMC, then the account credentials must also be changed within SMARTsend.

---

## General Settings

The General Settings links are located in the lower-left section of the Administration Home Page. These links provide access to the General Settings and Workflow Defaults pages.

### Update Administrator Contact Information

This link is used to enter and update the SMARTsend administrators's name, phone number, and e-mail address. This entry should identify the individual who is responsible for SMARTsend site administration and support. This information appears on Job Confirmation notices, error messages, and other communications between SMARTsend and its users.

The Reply To e-mail address is the e-mail address that will be listed on the job confirmation and notification messages that SMARTsend sends to users. If you prefer to use a valid e-mail address to which users can actually reply, enter the complete address in the 'Reply To' Address field.

**NOTE:** If the SMTP server being used requires a well-formed and/or valid address (*account name@domain/host name*), then you must enter a well-formed and/or valid address in the Reply To address field. See *SMTP Server Configuration* on page 4-25 for more information.

If you do not need to provide SMARTsend users with the ability to reply to SMARTsend confirmation and notification messages, you can use the default setting provided by SMARTsend. By default, SMARTsend appends the domain name of the SMTP server to the e-mail address that it generates. For example, at a company called "Mycompany," the reply address would be **SMARTsend@mycompany.com**.

### Choose Error Handling Scheme

SMARTsend logs system errors automatically. To notify the administrator of their occurrence via e-mail, select the option to **Log All System Errors and E-Mail Administrator**. The e-mail address specified for the Administrator Contact Information will be used for these notifications.

## Review Publication / Workflow Defaults

The Publication Defaults and Workflow Defaults establish the SMARTsend system defaults for every user that creates a workflow. Click these links to access the Workflow and Publication defaults page.

### Workflow Default Settings

#### Workflow Access

SMARTsend designates the creator of a workflow as its owner. Workflow owners have full ability to view, copy, modify, publish, use, and delete their workflows. The Workflow Access setting determines what privileges other SMARTsend users have to workflows that they did not create.

- Select Public to make new workflows accessible to all users by SMARTsend for viewing, copying, publication, and use.
- Select Private to limit workflow access to the workflow owners.
  - Private workflows are only available to their owners for viewing, copying, modifying, and publishing, and for use with devices that support authentication.
  - Private should only be selected as the default access level if the scanning devices that SMARTsend manages have authentication enabled and are members of the same domain or trusted domain as the SMARTsend computer. Private can also be selected when using PaperWare cover sheets (Professional Edition feature).

**NOTE:** In the case of private workflows, users with device access who are not the owners of a private workflow can still select a private template at the device and attempt to scan a job. The job will initially appear to begin processing, but will eventually fail once the device account information is compared with the private workflow account information on the SMARTsend computer. The failure will be reported on the Job Confirmation report (if enabled), but there will be no indication of job failure at the device user interface.

Only workflow owners can modify a workflow, regardless of its access privileges. Administrators can delete any workflow from the Manage Workflows page, regardless of its access privileges.

#### Job Confirmation

Select a default job status reporting option from among those listed in the following table:

| Option                                                                                   | Explanation                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No job confirmation                                                                      | SMARTsend does not report a job's status.                                                                                                                                                                                                                         |
| Workflow owner's e-mail                                                                  | SMARTsend reports the job's status to the workflow owner's e-mail address. Appropriate for Public or Private jobs.                                                                                                                                                |
| Workflow user's e-mail                                                                   | SMARTsend reports the job's status to the scan job submitter's e-mail address. Appropriate for Public jobs, but only using devices that support authentication.                                                                                                   |
| Printed confirmation<br>( <i>This option is not supported by Internet fax devices.</i> ) | SMARTsend confirms the job's status and certain details by printing a status report on the device that contains the published template. Please note that the confirmation report may contain private data. Use e-mail confirmation if data security is a concern. |

Table 4-5: SMARTsend Job Confirmation options

## Publication Defaults

### Scan Profile

The Scan Profile setting defines the basic characteristics of the paper document that will be scanned using SMARTsend. The Scan Profile is only applicable when scanning from a Xerox Multifunction Device. Select the default input document type from among those displayed in the following table:

|                                                 |
|-------------------------------------------------|
| 1-Sided Black/White Business Document (default) |
| 1-Sided Color Business Document                 |
| 2-Sided Black/White Business Document           |
| 2-Sided Color Business Document                 |
| Black/White Photo                               |
| Color Photo                                     |

**Table 4-6: SMARTsend Scan Profiles**

Choose a default setting that is likely to be the most frequently used format within your organization.

### Allow workflow publication to not expire

When this option is selected, the user will have the option to set the workflow publication expiration time to "Does Not Expire" when publishing a workflow. This setting may have implications for publication management. For example, when publications expire, they are automatically removed from the SMARTsend computer and the corresponding templates are removed from the devices on which they reside. If publications do not expire, there may be considerable management work required in the future if the number of publications becomes excessive. This would require the administrator to review and delete publications manually using the Manage Workflows page.

## Document Type

The Document Type setting enables the administrator to configure the default file type and format that is assigned to workflows. Select the default file type and format from the following options:

| Document Type                                       | Output File Formats                                                                                                                                                                            | Considerations                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PDF, Image Only                                     | PDF, Image Only<br>PDF, Image Only - Preserve Image from Scan Source                                                                                                                           | <ul style="list-style-type: none"> <li>■ Supported on all major platforms</li> <li>■ Can be filed to all SMARTsend repositories</li> <li>■ Many compression options</li> <li>■ Excellent balance of portability, compatibility, and compression options</li> <li>■ Some imaging tools may not support PDF</li> </ul>                                                          |
| PDF, Text Searchable (Professional Edition feature) | PDF with normal text<br>PDF with image substitutes<br>PDF with image on text<br>PDF with image on text - Preserve Page Orientation<br>PDF with image on text - Preserve Image from Scan Source | <ul style="list-style-type: none"> <li>■ All of the above, plus support for OCR</li> <li>■ Document can be searched for text</li> <li>■ Text can be copied from document</li> <li>■ Requires extra processing</li> <li>■ Information loss possible during processing</li> </ul>                                                                                               |
| JFIF                                                | JPEG                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>■ Each page stored as single document</li> <li>■ Widely supported image format</li> <li>■ Excellent for color images</li> <li>■ JPEG is the only supported compression</li> <li>■ May exhibit "ringing" artifacts in text documents</li> <li>■ Some repositories do not support single-page files</li> <li>■ No OCR support</li> </ul> |
| Single-page TIFF                                    | Single-page TIFF 6.0<br>Single-page TIFF 6.0 TTN2                                                                                                                                              | <ul style="list-style-type: none"> <li>■ Each page stored as single document</li> <li>■ Widely supported image format</li> <li>■ Moderate range of compression options</li> <li>■ Some repositories do not support this format</li> <li>■ No OCR support</li> </ul>                                                                                                           |
| Multi-page TIFF                                     | Multi-page TIFF 6.0<br>Multi-page TIFF 6.0 TTN2<br>Multi-page TIFF - Preserve Image from Scan Source                                                                                           | <ul style="list-style-type: none"> <li>■ Each page stored as single document</li> <li>■ Widely supported image format</li> <li>■ Moderate range of compression options</li> <li>■ Can be filed to all SMARTsend repositories</li> <li>■ No OCR support</li> </ul>                                                                                                             |

**Table 4-7: SMARTsend output file types and formats.**

| Document Type                                         | Output File Formats                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Considerations                                                                                                                                                                                                             |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Original Document Type                                | File format is determined at scan time. Some devices will enable you to choose a format at the device user interface, while other devices may be constrained to a specific format.                                                                                                                                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>■ Minimal information loss</li> <li>■ No OCR support</li> <li>■ File format determined at scan time and may vary by device</li> </ul>                                               |
| Other - OCR formats<br>(Professional Edition feature) | Microsoft Word 97, 2000, 2002, 2003 (*.doc)<br>Text, standard (*.txt)<br>Microsoft Excel 97, 2000, 2002, 2003 (.xls)<br>Microsoft PowerPoint 97 (*.rtf)<br>Microsoft Publisher 98 (*.rtf)<br>ASCII Text, formatted (*.txt)<br>ASCII Text, standard (*.txt)<br>ASCII Text, standardEx (*.txt)<br>Rich Text Format (*.rtf)<br>RTF Word 2000 (*.rtf)<br>RTF Word 6.0/95 (*.rtf)<br>RTF Word 97 (*.rtf)<br>Text, smart (*.txt)<br>Text, stripped (*.txt)<br>Text, plain (*.txt)<br>Text, comma delimited (*.csv)<br>Text, tab delimited (*.txt)<br>WordPad (*.rtf) | <ul style="list-style-type: none"> <li>■ Supports a variety of OCR/text-based formats</li> <li>■ Requires extra processing time</li> <li>■ Original image data is not preserved (may include embedded pictures)</li> </ul> |

**Table 4-7: SMARTsend output file types and formats.**

## Document Type Properties

SMARTsend supports a variety of document types, and many of them can be configured to optimize the default settings that influence file format selections, performance, and image quality. These default settings can be accessed by clicking the **Document Type > Properties** button on the Workflow Defaults page.

### Format

The file format selections vary with each document type. The supported output file types and formats are listed in Table 4-7. When you choose a format, the options available on the Document Type Properties page will change accordingly.

### Image and OCR Optimization Settings

Some document types, such as PDF, provide image optimization and compression settings that can be configured within SMARTsend. When OCR is utilized (Professional Edition feature), additional settings are provided to optimize OCR processing and quality. The default settings or these options can be configured by the SMARTsend system administrator, and they can also be adjusted by each SMARTsend user when workflows are published.

Please consult the SMARTsend User Guide, *Document Format and Properties* on page 3-28, for additional information.

## Configure PaperWare Form Forwarding Settings

### Professional Edition Feature

When properly configured, each SMARTsend computer can forward PaperWare cover sheets to the SMARTsend or FlowPort computer that was used to create the PaperWare cover sheet and the workflow from which it was published. Each SMARTsend computer can also be configured to receive and process PaperWare forms that have been forwarded to it by other SMARTsend computers and the scanning devices that they are configured to manage. These options provide unprecedented flexibility and ease of use by allowing end users to use their PaperWare cover sheets interchangeably with any supported Xerox Multifunction device or Internet Fax device.

SMARTsend provides several options that enable you to configure the way it processes PaperWare forms in environments that have more than one SMARTsend computer, as well as mixed environments where Xerox FlowPort servers are also in use. These features offer expanded interoperability and scalability, enabling SMARTsend to work with additional devices and computers in a seamless fashion.

### Forward PaperWare Forms

The SMARTsend computer must be configured to forward PaperWare forms to other computers. If a user scans a job with a PaperWare cover sheet that was created on another SMARTsend or FlowPort computer, the job will fail and an error message will be printed at the scanning device if the computer is not configured to forward PaperWare forms.

### Receive Forwarded PaperWare Forms

The SMARTsend computer must be configured to receive and process PaperWare forms that have been forwarded to it by other SMARTsend computers. A scan job will fail and an error message will be printed at the device where the scan originated if the originating computer is not configured to receive PaperWare forms from other computers.

### Enabling PaperWare Forms Forwarding and Receiving

► *To enable PaperWare forms forwarding and receiving:*

- 1 Open the SMARTsend Administration Home Page.
- 2 Scroll down to the General Settings section, then select the link to **Configure PaperWare Form Forwarding Settings**. The PaperWare Settings page appears.
- 3 Select the option to **Forward a PaperWare form to the computer on which it was published**. If applicable, select the option to **Process PaperWare forms forwarded from other computers**.

You will also need to select a Forwarding Protocol. See *Forwarding Protocol Used for Forms Published at this Computer* (below) for more information.

### Forwarding Protocol Used for Forms Published at this Computer

SMARTsend can use the HTTP or HTTPS protocols to forward PaperWare forms to other computers. HTTP is the default setting and provides faster job processing. HTTPS provides more security than HTTP, but it requires the installation of a security certificate on the SMARTsend computer. SMARTsend will not permit

the HTTPS protocol to be selected unless a security certificate is properly configured on the SMARTsend computer.

**NOTE:** If the protocol is changed after PaperWare forms have been published, existing PaperWare cover sheets will not be updated to use the new protocol. If this condition occurs, any outdated publications should be deleted and republished with the new settings. In addition, if the HTTPS protocol is being used and the security certificate is later deleted from the SMARTsend computer, the computer will not be able to forward the forms and the user will receive an error notification. A new security certificate will need to be installed in order to receive forwarded forms using HTTPS.

*Consider the following when using the PaperWare form forwarding options:*

- DNS must be properly configured on the sending and receiving computers. Forwarded jobs will fail and an error message will be displayed if the receiving computer is not addressable through DNS. See *Verifying the SMARTsend Computer DNS Configuration* on page 2-8 for additional information.
- HTTP forwarding will not work if the receiving computer is configured only for HTTPS. See *Secure Web Site Configuration* on page 9-3 for additional information.
- FlowPort forms created with version 2.2.1.88 or later are supported.
- Job logs and device information are not supported with FlowPort servers, so this information is only forwarded to SMARTsend computers. As a result, confirmation sheets cannot be printed at scan devices managed by a FlowPort servers.
- When a SMARTsend computer is used to forward a job to a FlowPort server, any image settings will be converted to binary TIFF color/grayscale settings. FlowPort does not support the PDF settings.
- If a SMARTsend computer is restored from a backup that was created from an earlier version of SMARTsend (before release 2.0), the PaperWare form forwarding settings will revert to the default settings.

## Next Steps

The following steps are recommended after the SMARTsend site has been configured:

- Click the **User Site** link in the upper right section of the Administration Home Page to create and publish workflows. Administrators are strongly advised to create, publish and test at least one public workflow for each supported destination. If private workflows, PaperWare cover sheets, or Optical Character Recognition (OCR) features are supported, then those options should be tested as well.
- Consult the SMARTsend User Guide to learn more about the User Home Page and using SMARTsend. Links to the documentation are on the right panels of both the User and Administration Home Pages.
- For information on managing and maintaining the site, proceed to Chapter 5, *Site Management*.

## Appendix A - Job Log Export Support

If enabled by the SMARTsend system administrator, the Job Log Export feature will allow a user to export the device job log to FTP and Network Folder destinations in order to support downstream applications that may have a use for it. See *Configure Service Settings* on page 4-29 for additional information on how to enable the Job Log Export feature.

This feature will also allow 3rd Party integrators to add custom service information to the template using valid Job Template Language (JTL). This information is appended to the device job log, which is then exported to the FTP or Network folder location along with the scanned images.

This feature is only available for the FTP and Network Folder destinations. Workflows defined with these two destinations and published as templates or as PaperWare cover sheets support job log export.

**NOTE:** Submitting jobs via Internet Fax is not supported for this feature.

### ► To add an FTP or Network Folder destination that supports Job Log Export:

- 1 Open a browser window and launch SMARTsend as either an Administrator or a User.
- 2 Navigate to the User Home Page. Click **Add a New Distribution Workflow** under the Workflows heading. The Destinations page will be displayed.
- 3 Locate the Network Folder heading. Click **add locations**. The Network Folder Properties window will be displayed.
- 4 Add a name for the destination.
- 5 Add the folder path, for example: \\myComputer\scans, where myComputer is the name of the machine on which the folder is located, and scans is the name of a network sharing folder.
- 6 Open Advanced Properties. Enter the custom JTL entries.

Example of Valid Entry:

```
[doc_object cobra_general]
{
string CobraXSTKey ="6076118D91C7199D85256D9500694DDC";
string DocumentCenterCategory ="B";
string CobraVER ="CIRX.V4.5(31)";
string DiagnoseKey ="2.01";
}end
```

NOTE: Further information on JTL usage can be obtained from the Xerox Business Partners program.

- 7 Click **OK**. If the data is unable to be appended, an error will be produced.
- 8 Continue defining the workflow.

## Appendix B - External Application Connection

The External Application Connection (EAC) destination is a mechanism enabled by SMARTsend to allow easy extensions of functionality. By using the EAC as a destination, you can have image files (or OCR'd files) delivered to an application to perform additional actions. SMARTsend will also pass along any document attribute information as part of the data sent to the application. The syntax to program an EAC is very simple, and can be compared to command line execution of an application or a batch/script file. You simply need to provide the patch to the executable (or script) and tell SMARTsend what parameters/arguments to pass along to the executable or script. See *Configure Service Settings* on page 4-29 for additional information on how to enable the External Application Connection.

► *To program an EAC workflow:*

- 1 Open a browser window and launch SMARTsend as an Administrator.
- 2 Navigate to the User Home Page. Click **Add a New Distribution Workflow** under the Workflows heading. The Destinations page will be displayed.
- 3 Locate the External Application heading. Click **add locations**. The External Application Connection Properties window will be displayed.
- 4 Select a Destination Name to identify the application, process, or filing location that the workflow will use to process scanned documents.
- 5 Enter command line parameters to invoke a third party application. These parameters may invoke a script or executable program, and can also define parameters that enable SMARTsend to export metadata. Following are several command line examples:

No Parameters:

myBatch.bat (This will simply execute the batch file. The batch file can perform any required actions independent of SMARTsend)

Static Parameters:

myBatch.bat deleteOldJobs (This will pass the static parameter "deleteOldJobs" to the batch file)

Document Location Parameters:

myBatch {DocumentUrl} (The location of the document will be passed as an argument)

myBatch.bat {DocumentUrls} (If multiple documents are generated, then a list of all the documents will be passed as arguments)

Metadata Parameters:

myBatch.bat {DocumentUrl} -title {Field1} -description {Field2} (The document location, and the 1st and 2nd Document Attributes parameters as programmed in the workflow will be passed along as parameters)

- 6 Select a Maximum Wait Time for External Application to Complete. This setting enables you to configure the amount of time that SMARTsend will wait for the external application to complete the tasks defined in the command line. When this time interval expires, SMARTsend will delete any documents that are temporarily stored on the computer.
- 7 If applicable, select Send URL link to document (no document attached). Select this option to send the URL for the document(s) to the External Application Connection. An error will be generated if you select this option and do not include a URL replacement tag in the command line.
- 8 Click **OK**.
- 9 Continue defining the workflow.

## Site Management

This chapter describes the key site management tasks that the SMARTsend administrator performs to optimize site performance, usability and reliability. The tasks covered in this chapter are based on the features that are available on the right side of the SMARTsend Administration Home Page.

Please consult Chapter 2 of the SMARTsend User Guide for information pertaining to the User Home Page and any features about workflow creation and publishing.

### *What is in this chapter:*

- *Site Management Overview* . . . . . 5-2
- *Manage Workflows and Publications*. . . . . 5-3
- *Managing Xerox Devices* . . . . . 5-6
- *Backup Status* . . . . . 5-8

## Site Management Overview

The right section of the Administration Home Page contains links for the Manage Workflows and Publications, Manage Xerox Devices, and site Backup features.

- **Manage Scan to Home Workflow and Publications**—opens the Import Scan to Home Users page.
- **View All Workflows**—opens the Manage Workflows page.
- **View All Publications**—opens the Manage Workflows page in the All Publications view.
- **Delete all workflows owned by**—provides a quick method of deleting all the workflows that have been created by a specific SMARTsend user.
- **Delete all workflows not used or published since**—provides a quick method of deleting multiple workflows that have been utilized within a specified period of time.
- **View Xerox Devices**—opens the Manage Xerox Devices page.
- **Manage Device Accounts**—opens the Manage Device Account Credentials page.
- **Configure Discovery Settings**—opens the Device Discovery Settings - Subnets page.
- **Device Configuration Defaults**—opens the Edit Device Configuration Defaults page.
- **Backup Status**—displays the last successful site backup, the next scheduled backup, and a button to perform an immediate backup.

These features are explained in greater details in the following pages.

# Manage Workflows and Publications

The View All Workflows and View All Publications links on the Administration Home Page open the Manage Workflows page. This page displays a list of all workflows/publications that are currently available on the site. The column headings in the list change based on the view that is selected in the Workflow Views panel. The various columns can include:

- **Workflow/Publication Name**—name assigned to the workflow/publication by the workflow owner.
- **Devices (All Publications By Device view)**—lists the IP Addresses of all Xerox Multifunction Devices that hold SMARTsend publications (Device scan templates).
- **Workflow Owner**—name of the individual who created the workflow.
- **Publication Type**—Device Scan Template, PaperWare Cover Sheet, PaperWare Template.
- **Expiration Time (Publication view)**—date and time the publication is scheduled to expire.
- **Total Publications**—the total number of templates and/or PaperWare cover sheets that have been created from the workflow.
- **Last Used**—date on which any publication generated from the workflow was last used to scan.
- **Last Modified On**—date on which the workflow was last modified.

## Sorting and Viewing Workflows

The Manage Workflows page provides options for sorting the list of workflows. Simply click on the column headings in the list to sort the list according to the data in the selected column.

The display and page features can also be used to select the information to be displayed on the page. Display sets the number of workflows that will be displayed on the page at one time. When multiple pages of workflows are available, the page feature enables you to select the individual pages to be displayed.



Navigation arrows provide an additional method of navigating through lists that contain multiple pages.

## Workflow/Publication Management Tasks

The upper-left panel of the Manage Workflows page contains links for workflow and publication management tasks. These tasks change based on the Workflow View that is selected.

### Delete This Workflow

Individual workflows are deleted with the Delete This Workflow option. All publications generated from the workflow will also be deleted and will no longer be available for scanning. Administrators may want to delete workflows that have not been used for a significant period of time. See *Deleting all workflows not used or published since* on page 5-5 for instructions.

**NOTE:** Exercise caution when deleting workflows. When a workflow is deleted, its corresponding publications (device scan templates) are deleted, and any PaperWare cover sheets (*Professional Edition feature*) become invalid.

► *To delete this workflow:*

- 1 Select a workflow on the Manage Workflows page.

- 2 Click the **Delete this workflow** link.
- 3 Click **OK** in the confirmation dialog.

## Delete This Workflow's Publications

All publications associated with a specific workflow can be deleted without affecting the original workflow. Once deleted, the publications are no longer available. This feature is useful when the original workflow is still valid, but the publications based on the workflow have become too numerous to manage. For example, when the limit of 255 templates on a Xerox device has been reached, or when there are many publications that have not been used for a considerable period of time.

### ► To delete a workflow's publications:

- 1 On the Manage Workflows page, click **Show All** to make sure you are in the Workflows view.
- 2 Select a workflow in the list.
- 3 Click the **Delete this workflow's publications** link.
- 4 Click **OK** in the confirmation dialog.

### ► To delete individual publications:

- 1 On the Manage Workflows page, click **All Publications** to make sure you are in the Publications view.
- 2 Select a publication in the list.
- 3 Click the **Delete this publication** link.
- 4 Click **OK** in the confirmation dialog. The specified publication is deleted, but the original workflow and all other publications are retained.

## Workflow Views

The Workflow Views options enable you to view different listings of workflows and publications. Administrators can view the list of public and private workflows, but cannot view the content of any workflow from the Manage Workflows page.

- **Show All**—provides a list of all the workflows on the SMARTsend computer.
- **All Publications**—provides a list of all publications on the SMARTsend computer, including PaperWare cover sheets, PaperWare Templates, and Device Scan Templates.
- **All Publications by Device**—provides a list of all the publications per configured device on the SMARTsend computer. The list will display the device name first in the left column and then show its associated publications and workflows. This view enables you to delete selected publications on individual devices, which is useful for managing templates on devices that have a limit of 255 templates.
- **All PaperWare Publications** (*Professional Edition feature*)—provides a list of all the available PaperWare cover sheets.

**NOTE:** The column headings on the Manage Workflows page change based on the view that is selected in the Workflow Views panel.

## Workflow Details

The Workflow Details panel on the Manage Workflows page provides detailed information for the workflow that is currently selected in the list. Workflow details can include:

- **Name**—name assigned to workflow by the owner.
- **Description**—text description entered by workflow owner.
- **Owner**—workflow owner account name.
- **Access**—public/private.
- **Last Used**—date/time on which any publication generated from the workflow was last used to scan.
- **Last Modified On**—date/time on which the workflow was last modified.
- **Device Publications**— # of Device Scan Templates published from the workflow.
- **PaperWare Publications**— # of PaperWare cover sheets published from the workflow.
- **Workflow Type**—type of workflow, such as distribution, search, or scan to home workflows.

**NOTE:** Workflow Details are only available when the Show All view is selected.

## Deleting all workflows owned by

The Delete all workflows owned by option enables you to delete every workflow that has been created by a specific SMARTsend user. This feature is useful if an individual has left your organization or is no longer authorized to use the SMARTsend site. Each user who currently has a SMARTsend account can be selected from a list.

► *To delete all workflows for a specific user:*

- 1 Open the **Delete all workflows owned by** list and select a user/account name.
- 2 Click **Go**.
- 3 Click **OK** in the confirmation dialog.

## Deleting all workflows not used or published since

This option enables you to delete all the workflows that have not been used since a specific date. For example, you can enter June 1, 2004 (or 6/1/04) in this field to delete all the workflows that have not been utilized between June 1, 2004 and the current date.

► *To delete all workflows not used or published since:*

- 1 Enter a date in the **Delete all workflows not used or published since** list. Use the format mm/dd/yy, or month, day, year.
- 2 Click **Go**.
- 3 Click **OK** in the confirmation dialog.

## Managing Xerox Devices

The Manage Xerox Devices panel on the Administration Home Page provides access to the SMARTsend device management pages and features. These links include:

- View Xerox Devices...
- Manage Device Accounts...
- Configure Discovery Settings...
- Device Configuration Defaults...

The View Xerox Devices link opens the Manage Xerox Devices page. This page lists the devices that are configured for use with SMARTsend, and provides access to features that enable administrators to discover and configure Xerox Multifunction Devices. Each device must be configured by SMARTsend before it can be used for scanning documents. General device management tasks may include adding, updating or deleting devices, and repairing SMARTsend device configurations.

### View Xerox Devices

Select the View Xerox Devices link from the Administration Home Page to access the Manage Xerox Devices page. This page includes a list of devices that are currently configured for use with SMARTsend, and provides access to features that enable administrators to discover and configure Xerox Multifunction Devices. Each device must be configured by SMARTsend before it can be used for scanning documents. General device management tasks may include adding, updating or deleting devices, and repairing SMARTsend device configurations. See *Add/Update Xerox Devices* on page 4-8 for additional information.

### Manage Device Accounts

The Manage Device Accounts page enables you to view and configure the Local User accounts that enable Xerox devices to communicate with the SMARTsend computer. See *Manage Device Accounts* on page 4-15 for additional information.

### Configure Discovery Settings

The Configure Discovery Settings options enable you to add additional subnets to the SMARTsend broadcast discovery configuration. In addition, you can access pages that enable you to configure the SNMP credentials that are required for discovery. See *Configure Discovery Settings - Subnets* on page 4-17 for additional information.

### Device Configuration Defaults

The Edit Device Configuration Defaults page enables you to view and configure the settings SMARTsend will use when configuring devices. See *Edit Device Configuration Defaults* on page 4-18 for additional information.

## Repairing a Device Configuration

The Repair feature attempts to restore the SMARTsend device configuration settings without requiring you to re-enter the information that is needed when configuring a device. This feature is used when a configured Xerox Multifunction Device is not functioning with SMARTsend. For example, you can use this option if settings were inadvertently deleted or overwritten on the device by another tool. Try this option first before attempting to reinstall a device that has stopped working with SMARTsend.

Keep in mind that a repair could fail if a device is turned off or is in the process of rebooting. The repair will also fail if the SNMP settings on the device do not match the SMARTsend settings. If any of these factors were present during the repair, you should resolve the issues and run the repair again.

► *To repair a device configuration:*

- 1 Click the **View Xerox Devices...** link on the Administration home page.
- 2 Select one or more devices from the Xerox Multifunction Devices list on the Manage Xerox Devices page. Click the check box to the left of the device name to make your selection(s).
- 3 Click the **Repair** button located beneath the list, or the Repair icon  in the column on the right side of the page. If the repair is successful, the status of the device will be updated accordingly.
- 4 If the repair was unsuccessful, review the error message and problem solving information displayed in the list. See *Device Communication and Configuration Issues* on page 7-6 for additional information.

## Backup Status

This area of the Administration home page displays status messages pertaining to the SMARTsend site database and registry setting backup process. The date and time of the Last Backup and the Next (scheduled) Backup are listed. You can also perform an immediate backup at any time by clicking **Backup Now**.

The Backup Status indicators work in conjunction with the Schedule a Backup feature that is provided in the Site Configuration area of the Administration Home Page. See *Schedule a Backup* on page 4-28 for additional information.

## Scan to Home

The SMARTsend Scan to Home feature enables you to scan and deliver documents to a defined user's home scan destination. This destination can be a network folder, an FTP site or an e-mail address.

Managing templates for users involves the creation of a list of users and corresponding home locations and the publication of device scan templates. SMARTsend supplies both a client-based administrative tool, called the Scan to Home Utility, and Scan to Home application features to facilitate the creation of user lists and publication of Scan to Home user templates.

The SMARTsend Scan to Home Utility is a standalone windows client application that assists system administrators in selecting users, providing mappings to directory services and generating an output file that can be imported into the SMARTsend application.

This chapter describes the operation of the Scan to Home Utility and the SMARTsend application Scan to Home features.

### *What is in this chapter:*

- *Scan to Home Overview* ..... 6-2
- *Getting Started with Scan to Home* ..... 6-5
- *Scan to Home Utility* ..... 6-9
- *Adding Users and Groups* ..... 6-12

## Scan to Home Overview

The SMARTsend Scan to Home feature enables you to scan and deliver documents to a defined user's home scan destination. This destination can be a network folder, an FTP site or an e-mail address.

An intuitive and flexible Scan to Home Utility allows you to generate mappings of users to home scan destinations using Microsoft Active Directory, LDAP, NT Domains, or manual entry.

The SMARTsend application enables you to publish device scan templates for individual users and/or groups to a device configured for use with SMARTsend.

Once a list of users and directory service mappings has been generated and saved as a CSV file, the export procedure is complete. You then use the Scan to Home features of the SMARTsend application to import the information from the CSV file to the SMARTsend database, provide filing credentials and publish Scan to Home device scan templates to devices that have been configured for use with SMARTsend. The same CSV file can be used at multiple SMARTsend computers, enabling greater efficiency in deployment.

With user authentication at the Xerox Multifunction Device or document attribute field (metadata) authentication enabled, a single scan template can direct jobs to a user's home scan destination. If desired, individual templates per user can also be generated for one touch access.

## Managing Scan to Home Templates

The following steps can be followed to quickly enable users to scan to their home destination using SMARTsend.

### ► To manage Scan to Home templates:

- 1 Install the SMARTsend Scan to Home Utility from the SMARTsend CD.
- 2 Use the Scan to Home Utility to create a list of users, directory service mappings and corresponding user properties.
- 3 Optionally, use the Scan to Home Utility to create user home scan destinations and manage access rights.
- 4 Export the list of users and properties to a CSV file.
- 5 Launch the SMARTsend application as an Administrator.
- 6 Use the SMARTsend application Scan to Home features to import users and user properties from the CSV file to the SMARTsend database.
- 7 Set the Scan to Home publication options.
- 8 Publish the Scan to Home template(s) to devices configured for use with SMARTsend.
- 9 Inform SMARTsend users that they can begin scanning using SMARTsend.

## Requirements

The SMARTsend Scan to Home Utility is a client based Windows utility available for install from the SMARTsend installation CD. It can be installed on the SMARTsend computer or a networked, client computer.

### System Requirements:

- Windows XP Professional or Windows 2000/ 2003 Server operating systems.
- Administrative privileges on the computer where the utility is being installed.

- Installation of the Microsoft .NET Framework version 1.1 or newer on the computer where the utility is being installed. Go to <http://www.microsoft.com/downloads> to obtain the Microsoft .NET Framework.

**NOTE:** if the Scan to Home Utility is being installed on the same computer as the SMARTsend application, SMARTsend will install the .NET Framework.

## Installing the SMARTsend Scan to Home Utility

The Scan to Home Utility is installed on the SMARTsend server or client computers connected to the same network as the SMARTsend server.

### To install the Scan to Home Utility:

- 1 Log in to the computer, where the utility will be installed, as an Administrator.
- 2 Insert the SMARTsend CD into the CD-ROM drive.
- 3 If the CD launches automatically, exit the SMARTsend application.
- 4 Click **Start** > **Run** and browse to the CD-ROM drive.
- 5 Open the \\Tools\ScanToHome folder.
- 6 Double-click the file Setup.exe. Click **OK**.
- 7 Select the language and click **OK**.
- 8 Click **Next** on the installer welcome page.
- 9 Read and accept the license agreement. Click **Next**.
- 10 Confirm the installation directory, then click **Next** to initiate the installation process.
- 11 Click **Install** to begin installation.
- 12 When the installation process is complete, click **Finish**.

## Uninstalling the SMARTsend Scan to Home Utility

The Scan to Home Utility uninstall program removes the Scan to Home Utility application and application files. It does not remove CSV files that were created using the utility.

### To uninstall the SMARTsend Scan to Home Utility:

- 1 Open Control Panel.
  - a) On a Windows 2000 Server/Advanced Server, from the Start menu select **Settings > Control Panel**.
  - b) On a computer running Windows Server 2003 or Windows XP Professional, from the Start menu select **Control Panel**.
- 2 In Control Panel, click **Add or Remove Programs**.
- 3 Select **SMARTsend Scan to Home Utility**.
- 4 Click **Change\Remove**, then click **OK** to confirm removal of the SMARTsend Scan to Home Utility.
- 5 Click **Finish**.

# Getting Started with Scan to Home

## Advance Planning Considerations

Before you begin adding users, you need to decide (based on your current Microsoft Windows user setup), where you will obtain your user information and the information that is required for each user source.

Possible user sources are:

### NT Domain, LDAP or Microsoft Active Directory Service

Required Information:

- Server name or Domain of the NT domain controller, LDAP server or Active Directory domain.
- Username and Password to use when accessing the NT domain controller, LDAP server or Active Directory domain.

**NOTE:** Note: If anonymous access is enabled, this can be skipped.

List of which users will be managed and corresponding user properties:

- Domain
- Locations of Home Scan Destinations: FTP Server, Network Folder or E-mail
- Location and existence of Home Scan Destinations
- Master Filing Credentials

### Local Computer

List of which users will be managed and corresponding user properties:

- Domain
- Locations of Home Scan Destinations: FTP Server, Network Folder or E-mail
- Location and existence of Home Scan Destinations
- Master Filing Credentials

## Adding Scan to Home Users From a Windows NT Domain

### ► To add Scan to Home users from a Windows NT Domain:

- 1 Open the Scan to Home Utility:
  - a) On Windows 2000, click **Start > Programs > Xerox > SMARTsend > Scan to Home Utility**.
  - b) On Windows XP or Windows Server 2003, click **Start > All Programs > Xerox > SMARTsend > Scan to Home Utility**.
- 2 Navigate to the Available Users panel and select **Retrieve User List From the NT Domain**.
- 3 Click **Choose Server**. The Enter Source Information dialog opens. Type the necessary information to direct the utility to the NT Domain controller with the user information.
  - a) Enter the Server name or Domain of the NT domain controller.
  - b) Type the Username and Password for access to the NT Domain server or select anonymous access.

**NOTE:** The username and password information will not be saved. It will only be used when accessing the list of available users.

- c) Click **Get Users** to retrieve the list of available users from the NT Domain server. The Available Users panel will be populated with these data.
- 4 Select the users to be managed.
- 5 Click **Add**. The selected users are moved from the Available Users list to the Selected Users list.
- 6 From the **File** menu, select **Save** to export the list of users and mapping to a CSV file.
- 7 Type a name for the CSV file and click **Save**. The CSV file is now ready to be imported to the SMARTsend application to create Scan to Home templates.
- 8 Click **Exit** to close the application.

## Adding Scan to Home Users from a Microsoft Active Directory Server

Please refer to *Adding Scan to Home Users From an LDAP Directory Service* on page 6-7.

## Adding Scan to Home Users From an LDAP Directory Service

The process for adding users from a Microsoft Active Directory server is nearly identical to this procedure, so if you are working with an Active Directory server, please refer to these steps for guidance.

### ► To add Scan to Home users from an LDAP directory service:

- 1 Open the Scan to Home Utility:
  - a) On Windows 2000, click **Start > Programs > Xerox > SMARTsend > Scan to Home Utility**.
  - b) On Windows XP or Windows Server 2003, click **Start > All Programs > Xerox > SMARTsend > Scan to Home Utility**.
- 2 Navigate to the Available Users panel and select **Retrieve User List From the LDAP directory service**.
- 3 Click **Choose Server**. The Enter Source Information dialog opens. Type the necessary information to direct the utility to the LDAP server with the user information.
  - a) Type the Server name or Domain of the LDAP server.
  - b) Type the Username and Password for access to the LDAP server. Alternatively, click Use anonymous access if it is supported by the LDAP server.

**NOTE:** The username and password information will not be saved. It will only be used when accessing the list of available users.

- c) To narrow the search, type a Search Context and Filter (optional).
  - d) Click the **Mappings** button to map the user Login Name, E-mail Address and Home Location to values that are retrieved from the LDAP server.
  - e) Click **OK**.
  - f) Click **Get Users** to retrieve the list of available users from the LDAP server. The Available Users panel will be populated with these data.
- 4 Select the users to be managed.
- 5 Click **Add**. The selected users are moved from the Available Users list to the Selected Users list.
- 6 From the **File** menu, select **Save** to export the list of users and mapping to a CSV file.
- 7 Type a name for the CSV file and click **Save**. The CSV file is now ready to be imported to the SMARTsend application to create Scan to Home templates.
- 8 Click **Exit** to close the application.

## Adding Scan to Home Users From the Local Computer

### ► To add Scan to Home users from the Local Computer:

- 1 Open the Scan to Home Utility:
  - a) On Windows 2000, click **Start > Programs > Xerox > SMARTsend > Scan to Home Utility**.
  - b) On Windows XP or Windows Server 2003, click **Start > All Programs > Xerox > SMARTsend > Scan to Home Utility**.
- 2 Navigate to the Available Users panel and select **Local Computer**.
- 3 Click **Show Users** to retrieve the list of available users from the local computer. The Available Users panel will be populated with these data.
- 4 Select the users to be managed.
- 5 Click **Add**. The selected users are moved from the Available Users list to the Selected Users list.
- 6 From the **File** menu, select **Save** to export the list of users and mapping to a CSV file.
- 7 Type a name for the CSV file and click **Save**. The CSV file is now ready to be imported to the SMARTsend application to create Scan to Home templates.
- 8 Click **Exit** to close the application.

# Scan to Home Utility

## Accessing the Scan to Home Utility

The left side of the screen contains options and information on available users. The right side of the screen contains a list selected users.

### ► To access the Scan to Home Utility:

- 1 Open the Scan to Home Utility:
  - a) On Windows 2000, click **Start > Programs > Xerox > SMARTsend > Scan to Home Utility**.
  - b) On Windows XP or Windows Server 2003, click **Start > All Programs > Xerox > SMARTsend > Scan to Home Utility**.
- 2 The SMARTsend Scan to Home Utility main window appears.

## Obtaining a List of Available Users

Located on the left side of the main window, the list of **Available Users** is used to populate the list of **Selected Users**. The list of **Available Users** is populated from the following sources:

- Microsoft Active Directory Service
- LDAP Server
- Windows NT Domain
- Local Computer

## Choosing a Server

The **Choose Server** button opens the **Enter Source Information** dialog where you can enter the information for the directory service you wish to use when retrieving users. The **Choose Server** button will be enabled if the Active Directory, LDAP or NT Domain source has been selected.

## Enter Source Information Dialog

The **Enter Source Information** dialog will open when you select Active Directory, LDAP or NT Domain as the source of available users and then click the **Choose Server** button.

The **Server** or **Domain**, **Username** and **Password** fields are required fields. The **Search Context**, **Filter** and **Port** fields can be used to narrow a search.

### LDAP Server Source Information

This table lists the fields available in the Enter Source Information dialog when an LDAP Server is selected as the source for available users.

| Field Name     | Description                                                                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server         | Server name of the LDAP server.                                                                                                                                           |
| Username       | If the LDAP server does not support anonymous access, enter the Username to use when accessing the LDAP server.<br>Note: Username will not be stored in the CSV file.     |
| Password       | If the LDAP server service does not support anonymous access, enter the Password to use when accessing LDAP server.<br>Note: Password will not be stored in the CSV file. |
| Search Context | Relative context of the directory tree where the user search will occur (e.g. cn=users).                                                                                  |
| Filter         | Expression to limit search results (e.g. user would limit search results to items which contain "user")                                                                   |
| Port           | Port to use when accessing the LDAP server.<br>Default = 389. Change default if value for your LDAP server is different.                                                  |

**Table 6-1: LDAP Source Information**

### Microsoft Active Directory Source Information

This table lists the fields available in the Enter Source Information dialog when Microsoft Active Directory Server is selected as the source for available users.

| Field Name       | Description                                                                                                                                                                                                                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server or Domain | Server or Domain name of the Windows 2000 server that is configured with the Active Directory service.<br>We recommend that you enter the domain name. Using a domain name will allow the use of any domain controller that is available. |
| Username         | If the Active Directory service does not support anonymous access, enter the Username to use when accessing the server configured with Microsoft Active Directory service.<br>Note: Username will not be stored in the CSV file.          |
| Password         | If the Active Directory service does not support anonymous access, enter the Password to use when accessing server configured with Microsoft Active Directory service.<br>Note: Password will not be stored in the CSV file.              |
| Search Context   | Relative context of the directory tree where the user search will occur (e.g. cn=users).                                                                                                                                                  |
| Filter           | Expression to limit search results (e.g. user would limit search results to items which contain "user").                                                                                                                                  |
| Port             | N/A                                                                                                                                                                                                                                       |

**Table 6-2: Microsoft Active Directory Source Information**

## Windows NT Domain Source Information

| Field Name       | Description                                                                                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server or Domain | Server or Domain name of the Windows NT domain controller.<br>We recommend that you enter the domain name. Using a domain name will allow the use of any domain controller that is available.           |
| Username         | If the Windows NT domain controller does not support anonymous access, enter the Username to use when accessing the Windows NT domain controller.<br>Note: Username will not be stored in the CSV file. |
| Password         | If the Windows NT domain controller does not support anonymous access, enter the Password to use when accessing the Windows NT domain controller.<br>Note: Password will not be stored in the CSV file. |

**Table 6-3: Windows NT Domain Source Information**

## Active Directory or LDAP Mappings

The Mappings button will be available, from the Enter Source Information dialog, if you have selected either Active Directory or LDAP as the source of available users. The **Mappings** button will open either the Active Directory Mappings or LDAP Mappings dialog.

**NOTE:** Note: The mapping information that is entered at this dialog will be saved and displayed each subsequent time that this dialog is accessed.

These mappings define how the information from either the Active Directory or LDAP services will be mapped to the properties Login Name, E-mail Address, and Home Location.

| Field Name     | Description                                                                                                                                                                                                                                                                                                                                       |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Login Name     | Enter the Active Directory or LDAP server field that will be used when retrieving information for the Username user property.                                                                                                                                                                                                                     |
| E-mail Address | Enter the Active Directory or LDAP server field that will be used when retrieving information for the E-mail user property.<br>This is an optional field. If it is not available, and you would like to use it to define a user's scan destination, it can be entered manually using the Properties button on the Selected Users panel.           |
| Home Location  | Enter the Active Directory or LDAP server field that will be used when retrieving information for the Scan Destination user property.<br>This is an optional field. If it is not available, and you would like to use it to define a user's scan destination, it can be entered manually using the Properties button on the Selected Users panel. |

**Table 6-4: Active Directory or LDAP Mappings**

## Showing Users

The **Show Users** button retrieves a list of available users from the local computer. The **Show Users** button will only be enabled if the Local Computer source has been selected.

## Adding Users and Groups

After populating the list of users from the available sources, click the checkbox next to the desired users and/or groups listed in the Available Users list and click the Add button. These users will now appear in the Selected Users list located on the right side of the main window. The **Add** button will be enabled if at least one user and/or group are selected from the Available Users list.

**NOTE:** Note: When you select to add a group to the list of Selected Users, by default, an individual entry will be added for each member of the group. An entry for the group will be added only if Add an entry for Groups in addition to their users has been selected from the Tools > Options utility menu.

## Selected Users List

Located on the right side of the main window, the Selected Users List is populated with a list of users and user properties to be exported to a CSV file. The list of Selected Users is generated from the list of Available Users.

Available columns may be resized if additional viewing space is needed. Columns may also be added or removed from the current view by right-clicking in the Selected Users panel and selecting the desired columns.

| Field Name                    | Description                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username                      | Non-editable field.<br>Consists of a user's Domain\ Network ID.<br>Maps to Domain, Network ID when imported to the SMARTsend database. See <i>Managing the SMARTSend Scan to Home Users Database</i> on page 6-22 for more information.                                                                                                                                    |
| Destination Type              | Defines whether the user's home scan destination is an FTP server, Network Folder or E-mail address.                                                                                                                                                                                                                                                                       |
| Scan Output Type              | Defines the format of the file that will be distributed to the Scan Destination.                                                                                                                                                                                                                                                                                           |
| Confirmation Type             | Defines the type of confirmation that the user will receive when the scan job has completed.                                                                                                                                                                                                                                                                               |
| Scan Destination              | Defines the location where SMARTsend documents will be filed for Scan to Home users.                                                                                                                                                                                                                                                                                       |
| Template Name                 | Not a required field.<br>Will be defaulted to the User ID.<br>Can be edited on a per user basis.<br>Will be used as the template name on the Xerox Multifunction Device when the Scan to Home workflow is published as individual templates for selected users. See Publish Template(s) on page TBD for additional information.                                            |
| User ID                       | Editable on a per user basis.<br>Default = Network ID portion of Username                                                                                                                                                                                                                                                                                                  |
| Source Document Language Code | The code that defines the language of the source documents.<br>Will only be used for OCR operation with the SMARTsend Professional Edition.<br>Will define the language dictionary that will be used when performing OCR on the document.<br>The two letter language code will be displayed.<br>Select User Properties to view the corresponding source document language. |

**Table 6-5: Fields in the Selected Users List**

## Removing Users

To remove one or more users and/or groups from the list of Selected Users, select the users and/or groups and click **Remove**.

To select multiple users, press and hold the CTRL key while clicking on each user.

The **Remove** button is only enabled if at least one user from the Selected Users list has been selected.

## User Properties

To view the user properties of users in the Selected Users list, select the users and/or groups and click **Properties**. The User Properties dialog will be displayed. The **Properties** button is only enabled if at least one user from the Selected Users list has been selected.

**NOTE:** Note: If more than one user or group is selected, only the user properties that are the same for all users will be populated on the User Properties dialog. All other values will be left blank.

See *User Defaults* on page 6-14 for a description of user properties.

## Status Bar

Provides status information to the system administrator when an operation has been performed. Provides additional guidance during the user selection process.

## Progress Bar

Activates when an operation is being performed. The **Stop** button allows you to terminate an operation being tracked by the progress bar.

## User Menu Commands

### Clear Selected Users List

This option clears the list of Selected Users. To clear the list, select **Clear Selected Users List** from the **User** menu. You will be prompted to save your changes prior to clearing the Selected Users List.

### Hide Selected Users and Groups from the Available List

By default, users and groups who are added to the Selected Users list will be removed from the Available Users list.

To disable the feature and keep users and groups from being removed from the Available Users list, select **Hide selected users from the Available Users list** from the **User** menu.

**TIP:** Having this option selected helps avoid the potential of selecting duplicate users.

## User Defaults

This option allows you to define the user properties used for all users added to the Selected Users list. To change the default user properties, select **User Defaults** from the **User** menu.

| Field Name               | Description                                                                                                                                  | Possible Values                                                                                                                                                          |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Destination Type         | Defines the type of destination that will be filed to.                                                                                       | <ul style="list-style-type: none"><li>■ Network Folder (default)</li><li>■ FTP</li><li>■ E-mail</li></ul>                                                                |
| Scan Output Type         | Defines the format of the file that will be distributed to the Scan Destination.                                                             | <ul style="list-style-type: none"><li>■ PDF, Text Searchable (*.pdf)<sup>1</sup></li><li>■ PDF, Image Only (*.pdf) (default)</li><li>■ Multi-Page Tiff (*.tif)</li></ul> |
| Source Document Language | Defines the language of the source document. Will also define the language dictionary that will be used when performing OCR on the document. | <ul style="list-style-type: none"><li>■ Same as the OCR languages defined in the SMARTsend application.</li><li>■ Default: English</li></ul>                             |
| Confirmation Type        | Defines the type of confirmation that the Scan to Home user will receive when the scan job has completed.                                    | <ul style="list-style-type: none"><li>■ No confirmation</li><li>■ Printed (default)</li></ul>                                                                            |

**Table 6-6: User Default Properties**

| Field Name       | Description                                                                           | Possible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scan Destination | Defines the home scan destination where output documents will be stored for the user. | <ul style="list-style-type: none"> <li>■ Default:<br/>\\thiscomputername\SS_Scans\%Username%</li> <li>■ Variable Options: Allows you to place variable data in the Scan Destination property. <ul style="list-style-type: none"> <li>■ Username: For each user, the Network ID portion of the Username field will be inserted in place of the %Username% variable. (e.g. If the Scan Destination has been defined as \\thiscomputername\SS_Scans\%Username%, a Username of XRXNA\UserA will resolve to a Scan Destination of \\thiscomputername\SS_Scans\UserA.)</li> <li>■ Domain: For each user, the Domain portion of the Username field will be inserted in place of the %Domain% variable.(e.g. If the Scan Destination has been defined as \\thiscomputername\SS_Scans\%Domain%\_%Username%, a Username of XRXNA\UserA will resolve to a Scan Destination of \\thiscomputername\SS_Scans\XRXNA_UserA.</li> <li>■ E-mail: For each user, the following will be inserted in place of the %E-mail% variable: <ul style="list-style-type: none"> <li>■ Active Directory/ LDAP User Sources: Mappings entered for the E-mail field on the Mappings dialog.</li> <li>■ NT Domain/ Local Computer User Sources: Value will be unavailable by default.</li> <li>■ Home Location: For each user, the following will be inserted in place of the %Home Location% variable: <ul style="list-style-type: none"> <li>■ Active Directory/ LDAP User Sources: Mappings entered for the Home Location field on the Mappings dialog.</li> <li>■ NT Domain/ Local Computer User Sources: Value will be unavailable by default.</li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>Note: If a value for E-mail or Home Location is not available, and you would like to use it to define a user's Scan Destination, select each individual user and click the Properties button. Modify the Scan Destination field to include the information.</p> |

**Table 6-6: User Default Properties**

| Field Name              | Description                                                                                                                                                      | Possible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Template Name At Device | Defines the name of the device scan template that will be published when using the SMARTsend application to publish individual templates for Scan to Home users. | <ul style="list-style-type: none"> <li>■ Default: %Username% (Network ID portion of Username field will be used).</li> <li>■ Editable on a per user basis. Using the Properties button on the Selected Users panel.</li> <li>■ Variable Options: Allows you to place variable data in the Template Name property. <ul style="list-style-type: none"> <li>■ Username: For each user, the Network ID portion of the Username field will be inserted in place of the %Username% variable. (e.g. A Username of XRXNA\UserA will resolve to a Template Name of UserA.)</li> <li>■ Domain: For each user, the Domain portion of the Username field will be inserted in place of the %Domain% variable.(e.g. If the Template Name has been defined as %Domain%_Username%, a Username of XRXNA\UserA will resolve to a Template Name of XRXNA_UserA.</li> </ul> </li> </ul> |

**Table 6-6: User Default Properties**

| Field Name                    | Description                                                                                                                                                                                                                                                                  | Possible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Document Attribute Identifier | Populates the User ID field. When the SMARTsend application is used to publish a single template for Scan to Home users and users will be identified by a document attribute field, the value entered for User ID will be compared to that entered by the user at scan time. | <ul style="list-style-type: none"> <li>■ Default: %Username% (Network ID portion of Username field will be used).</li> <li>■ Editable on a per user basis. Using the Properties button on the Selected Users panel.</li> <li>■ Variable Options: Allows you to place variable data in the Document Attribute Identifier property. <ul style="list-style-type: none"> <li>■ Username: For each user, the Network ID portion of the Username field will be inserted in place of the %Username% variable. (e.g. A Username of XRXNA\UserA will resolve to a Document Attribute Identifier of UserA.).</li> <li>■ Domain: For each user, the Domain portion of the Username field will be inserted in place of the %Domain% variable.(e.g. If the Document Attribute Identifier has been defined as %Domain%_%Username%, a Username of XRXNA\UserA will resolve to a Document Attribute Identifier of XRXNA_UserA.</li> <li>■ E-mail: For each user, the following will be inserted in place of the %E-mail% variable: <ul style="list-style-type: none"> <li>■ Active Directory/ LDAP User Sources: Mappings entered for the E-mail field on the Mappings dialog.</li> <li>■ NT Domain/ Local Computer User Sources: Value will be unavailable by default.</li> </ul> </li> </ul> </li> </ul> <p>Note: If a value for E-mail is not available, and you would like to use it to define the Document Attribute Identifier, select each individual user and click the Properties button. Modify the Document Attribute Identifier field to include the information.</p> |

**Table 6-6: User Default Properties**

<sup>1</sup> **Requires** either the SMARTsend Professional Edition to perform OCR on the source documents. If selected, the Scan Output Type will revert to PDF, Image Only (\*.pdf) on import to SMARTsend if either the Professional Edition is not used.

**NOTE:** Note: Any changes to default settings are saved and will be available the next time you access User Defaults.

## Tools Menu Commands

### Create User Folders

This option creates home scan destinations for users in the Selected Users list when the Destination Type is either an FTP server or a network folder.

To open the Create User Folders dialog, select **Create User Folders** from the **Tools** menu.

#### Create folders for selected users:

Select this option if you would like to have folders created for users that are added to the Selected Users list. If selected, folders will be created according to what is specified in the Scan Destination user property.

#### Set permissions for selected users:

Define the permissions that will be assigned to user FTP server and network folders.

|                                        |                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Set user permissions:</b>           | If selected, full-control permissions to the folders will be given to the user who has specified the folder as their Scan Destination. Users will be identified by the Username property.                                                                                                                        |
| <b>Set filing account permissions:</b> | Allows you to define the account name that will be used by SMARTsend when filing to the user folders. If selected, full-control permissions for this account will be applied to the user folders. These accounts should be domain accounts or local accounts on the computer where the user folders are located. |

#### Use current account credentials:

When accessing the computer where the accounts are to be created or permissions are to be set, the credentials retrieved from the computer where the Scan to Home Utility is installed will be used.

#### Use the credentials below:

This option allows you to specify a username and password to use when accessing the computer where the accounts are to be created or permissions are to be set. These credentials are used for accessing the computer and will not be stored.

## Options

This feature allows you to define settings that will be used when adding users to the Selected Users list.

To open the Options dialog, select **Options** from the **Tools** menu.

### Add an entry for Groups in addition to their users:

Select this option when adding a Windows Group to the list of Selected Users if you would like to create both an entry for the group and entries for each user in the group.

If this option is not selected, you will be prompted to make this decision each time a group is added to the list of Selected Users.

### Remove group members when removing a group:

Select this option if you want group member removed from the list of Selected Users when the group is removed.

### When adding a duplicate user:

When a duplicate user is added to the list of Selected Users, you can select from the following options:

- **Always overwrite existing users**
- **Prompt before overwriting**
- **Never overwrite existing user**

## File Menu Commands

### Open an Existing .CSV File

To open an existing CSV file, select **Open** from the **File** menu.

### Exporting a CSV File

The list of selected users must be exported to a CSV (Comma Separated Values) file to be imported into SMARTsend.

*To export a CSV file:*

- 1 Select **Save** from the **File** menu.
- 2 Type a name for the CSV file.
- 3 Choose a location for the file.
- 4 Click **Save**.

The file is now ready to be imported into the SMARTsend application.

## Exit Utility

To exit the utility, click the **Exit** button. If changes have not been saved, you will be prompted to save.

## Editing User Properties

### Modifying Single Users

- *To modify the properties of a single user:*
- 1 Select the user you wish to modify.
  - 2 Click **Properties**. The User Properties dialog opens.
  - 3 Make the necessary changes.
  - 4 If you would like to apply the changes to all future new users, select **Apply to new selected users from now on**.
  - 5 Click **OK**.

### Modifying Multiple Users

- *To modify the properties of multiple users:*
- 1 Press and hold the CTRL key.
  - 2 Select the users you wish to modify.
  - 3 Click **Properties**. The User Properties dialog opens.
  - 4 Make the necessary changes.
  - 5 If you would like to apply the changes to all future new users, select **Apply to new selected users from now on**.

**NOTE:** The utility will only pre-fill those user properties that are identical for all selected users. All other properties will be left blank when the User Properties dialog opens.

- 6 Click **OK**.

## SMARTsend Scan to Home Application Features

After the list of selected users has been exported to a CSV file using the Scan to Home Utility, you are ready to use the Scan to Home features of the SMARTsend application to import users and publish device scan templates. SMARTsend users can publish to their home scan destinations using these device scan templates.

**NOTE:** If you have not yet used the Scan to Home Utility to create and export a list of selected users, please see *Managing Scan to Home Templates* on page 6-2.

### Importing Users into the SMARTsend Scan to Home User Database

The Import Users page allows you to import the contents of a CSV file into the SMARTsend database. This creates a list of users, and their corresponding Scan to Home properties, in the SMARTsend database. A CSV file is created using the Scan to Home Utility. See *Managing Scan to Home Templates* on page 6-2.

#### To import users into the SMARTsend Scan to Home user database

- 1 Launch SMARTsend as an Administrator.
- 2 On the Administration Home Page, locate the Manage Workflows and Publications pane and click the **Manage Scan to Home Workflow and Publications** link.
- 3 Click **Browse** to locate the file to import.
- 4 Click **Open** to display the contents of the CSV file. The contents of the selected CSV file will be shown and the Import Options will be enabled.

**NOTE:** If any problems are encountered with the CSV file, warnings and errors will be displayed when the file is opened. The Import Options will be unavailable if errors are found in the CSV file.

- 5 Review and confirm the contents of the CSV file prior to importing it into the SMARTsend database.
- 6 Select Import Options:
  - **Append the users above to the users in the database (default)** - Merges the list of users in the CSV file being imported to the list of existing Scan to Home users in the SMARTsend database. New users will be added and existing users will be replaced if duplicates exist.

**NOTE:** If a user in the CSV file being imported is already in the SMARTsend database, the existing Scan to Home user properties in the database will be overwritten.

- **Replace the users in the database with the users above** - The entire list of Scan to Home users in the SMARTsend database will be replaced with the list of users in the CSV file being imported. All prior users will be removed.
- 7 Click the **Import** button. If successful, the contents of the CSV file will be imported into the SMARTsend database and cleared from the Import Users page. If unsuccessful, an error will be displayed at the top of the page.
  - 8 If desired, import additional CSV files into the SMARTsend database.

## Managing the SMARTsend Scan to Home Users Database

The Manage Users page allows you to view and edit the list of Scan to Home users that have been imported from CSV files to the SMARTsend database. From this page, you can:

- Add individual users to the SMARTsend Scan to Home users database
- Edit the properties of individual users
- Delete users from the database
- Export your changes as a CSV file

See *Selected Users List* on page 6-12 for a detailed description of the information that is displayed on the Manage Users page.

### Accessing the Manage Users Page

*To access the Manage Users page:*

- 1 Launch SMARTsend as an Administrator.
- 2 On the Administration Home Page, locate the Manage Workflows and Publications pane and click the **Manage Scan to Home Workflow and Publications** link.
- 3 From the Scan to Home Tasks panel, click **Manage Users**.
- 4 The list of Scan to Home users in the SMARTsend database is displayed.

### Editing Users in the Database

*To edit the contents of the SMARTsend Scan to Home users database:*

- 1 On the Manage Users page, scroll right. At the end of each user's row is a link labeled **Edit**.
- 2 Click **Edit** for the user you wish to modify. The properties for the user become editable.
- 3 Make the desired changes.
- 4 Click **Apply** to save your changes or click **Cancel** to discard changes.

### Deleting Users from the Database

*To delete users from the SMARTsend Scan to Home users database:*

- 1 At the Manage Users page, select the checkbox for the user(s) you wish to delete.
- 2 Click **Delete**.
- 3 Click **OK** to confirm the selection.

### Adding Individual Users to the Database

*To add an individual user to the SMARTsend Scan to Home users database:*

- 1 On the Manage Users page, scroll down to the row labeled **New User**.
- 2 Scroll right to the end of the row. At the end of each user's row is a link labeled **Edit**.
- 3 Click **Edit**. The properties for the user become editable.
- 4 Type the user information in the available data fields.

- 5 Click **Apply** to save your changes or click **Cancel** to discard changes.
- 6 Repeat this procedure for each individual user you wish to add.

## Exporting Your Database Changes

Your modifications to the SMARTsend Scan to Home users database can be exported to a CSV file.

*To export your database changes:*

- 1 At the Manage Users page, click the **Export** button to export all Scan to Home users to a CSV file.
- 2 Choose one of the following:
  - a) Click **Open** to open and then save the CSV file.
  - b) Click **Save** to save the file to a new or existing CSV file.

**TIP:** If you are using both the Scan to Home Utility and the SMARTsend application to edit the contents of CSV files, you may want to export the contents of the SMARTsend database to a CSV file in order to maintain a current file to be used with the client tool.

## Managing Master Filing Credentials

In order to acquire access for filing to all FTP and Network Folder scan destinations, SMARTsend requires that master credentials be entered before templates are published for Scan to Home users.

### To manage the Master Filing Credentials:

- 1 Launch SMARTsend as an Administrator.
- 2 On the Administration Home Page, locate the Manage Workflows and Publications pane and click the **Manage Scan to Home Workflow and Publications** link.
- 3 From the Scan to Home Tasks panel, click on **Master Filing Credentials**.
- 4 On the Master Filing Credentials page, type and confirm the username and password for the master filing credentials to be used for filing to Network Folder scan destinations.
- 5 Click **Save Credentials** to store the master filing account credentials.
- 6 Type and confirm the username and password for the master filing credentials to be used for filing to FTP scan destinations.
- 7 Click **Save Credentials** to store the master filing account credentials.

**NOTE:** If available, SMARTsend will pre-populate the master filing account usernames from the imported CSV file. If you are importing users from multiple CSV files, make sure that the scan destinations can be accessed using the same master filing credentials. If the master filing account usernames are changed in the SMARTsend application, this information will not be updated in the CSV file. Passwords are not stored in the CSV file.

## Publishing Scan to Home Templates

Before users can be given access to Scan to Home device scan templates, you must select publication and document naming options, select document attribute fields and publish the Scan to Home templates to selected devices that have been configured for use with SMARTsend.

**NOTE:** You will be unable to publish Scan to Home device scan templates if credentials have not been entered at the Master Filing Credentials page.

### To publish SMARTsend Scan to Home templates:

- 1 Launch SMARTsend as an Administrator.
- 2 On the Administration Home Page, locate the Manage Workflows and Publications pane and click the **Manage Scan to Home Workflow and Publications** link.
- 3 From the Scan to Home Tasks panel, click **Publish Template(s)**.
- 4 Select a Publication Option.
  - *A Single Template That Users Share* on page 6-27. Choose an authentication option:
    - *Users will be Identified by Device Authentication* on page 6-27
    - *Users will be Identified by a Document Attribute Field* on page 6-28
  - *Individual Templates for the Users and Groups Selected Below (Default)* on page 6-28
- 5 Select a *Document Name* option.

See "Document Name" in the *SMARTsend User Guide* for additional information.
- 6 Select a *Document Attribute Profile*.

See "Document Attribute Profiles" in the *SMARTsend User Guide* for additional information.
- 7 Click **Publish to a Multifunction Device**. The Publish Workflow to Xerox Multifunction Device page is displayed.

## Publish Page

### Publishing a Common Template That Users Share

When this option has been selected:

- 1 Specify a unique publication name. The default publication name is `_MyHome`.

**NOTE:** When modifying the publication name keep in mind that, at the device local user interface, device scan templates that have an underscore as the first character of the name will be placed ahead of templates that have an alphanumeric character as the first character.

- 2 Select an expiration time.
- 3 Select the devices to which the template will be published.
- 4 Enter document attribute values. If the values are to be specified at the device, select **Editable at the device**.
- 5 Select a **Scan Profile**. Click **Properties** to adjust the scan settings as needed.
- 6 Click **OK**.
- 7 The template will be published. Click **Return to Home Page** at the bottom of the page to return to the User Home Page.

See Chapter 5, Publishing Workflows in the SMARTsend User Guide for additional information.

### Publishing Individual Templates for the Users and Groups Selected Below

When this option has been selected:

- 1 Select an expiration time.
- 2 Select the devices to which the template will be published.
- 3 Enter document attribute values. If the values are to be specified at the device, select **Editable at the device**.
- 4 Select a **Scan Profile**. Click **Properties** to adjust the scan settings as needed.
- 5 Click **OK**.
- 6 The template will be published. Click **Return to Home Page** at the bottom of the page to return to the User Home Page.

See Chapter 5, Publishing Workflows in the SMARTsend User Guide for additional information.

**NOTE:** When using this option, you will not be prompted to enter a publication name. Individual values stored in the SMARTsend database for the Template Name property will be used as the publication name for the device scan templates. It is important that each Template Name be unique. Templates will only be published for users that have a unique Template Name.

## Adding Scan to Home Publications to Additional Devices

In order to publish Scan to Home device scan templates to additional devices, follow the same procedure for publishing templates and reselect all of the devices where you would like to publish the templates.

## Viewing Scan to Home Publications

**To view Scan to Home device scan template publications from the User Home Page:**

- 1 Launch SMARTsend as an Administrator.
- 2 On the User Home Page, locate the Workflows pane and click the **View All Workflows** link. The Workflow Explorer page will be displayed.
- 3 Select the Scan to Home workflow.
- 4 From the Workflow Tasks panel, click **View Publications**.

**To view Scan to Home device scan template publications from the Administration Home Page:**

- 1 Launch SMARTsend as an Administrator.
- 2 On the Administration Home Page, locate the Manage Workflows and Publications pane and click the **View All Workflows** link. The Manage Workflows page will be displayed.
- 3 Select the Scan to Home workflow.
- 4 From the Workflow Views panel, click the desired view publication option.

## Deleting Scan to Home Publications

**To delete Scan to Home device scan template publications:**

- 1 Launch SMARTsend as an Administrator.
- 2 On the Administration Home Page, locate the Manage Workflows and Publications pane and click the **View All Publications** link. The Manage Workflows page will be displayed.
- 3 Select the Scan to Home publication you would like to delete.

## About Scan to Home Template Publishing Options

This section explains some of the options on the Scan to Home Template Publishing Options.

### A Single Template That Users Share

If this option is selected, a single device scan template, with default name `_MyHome`, will be published. When the `_MyHome` template is selected at the scanning device, the template will file to the authenticated users Scan Destination defined in the SMARTsend database.

### Users will be Identified by Device Authentication

Requires that the scanning device(s), where the Scan to Home device scan template is published, also support authentication, and that authentication be configured and enabled on each device. Values provided to SMARTsend in the device job log will be compared to the Domain and Network ID properties stored in the SMARTsend database and will be used to identify a Scan to Home user's Scan Destination.

The scanning device must be configured to require the device job log contain both the Domain and User Name that a user enters to authenticate. Please consult your device system administrator for additional information.

### Users will be Identified by a Document Attribute Field

Requires the system administrator to enter a prompt name in the Document Attribute Field Name field. When the Scan to Home workflow is published as a device scan template, a required document attribute field, with this prompt name, will be included in the template. The default prompt name will be Username. At scan time, values entered by users for this field will be compared to the User ID property stored in the SMARTsend database and will be used to identify a Scan to Home user's Scan Destination.

This document attribute field will be editable at the device and will reduce the number of fields that can be designated as editable at the device from six to five. Also, please ensure that the prompt name that you enter does not conflict with the field names of the document attribute fields in the Document Attribute Profile that you will select.

### Individual Templates for the Users and Groups Selected Below (Default)

If this option is selected, a uniquely named device scan template will be published for each selected user. Values stored in the SMARTsend database for the Template Name property will be used for naming of the device scan template(s). With this option, template users will not need to authenticate at scan time. The device scan template will file to the Scan Destination value stored in the SMARTsend database for users of the template. Click **Hide users with Scan to Home publications** to show only the users that do not have Scan to Home device scan templates published.

This option requires that all Template Name property values in the SMARTsend database be unique. If the Template Name property values are not unique, a validation error will be produced and you will be unable to publish templates using this option. Use the Manage Users page to review and edit Template Name property values.

### Document Attribute Profile

Sets of document attribute fields configured for reuse. Each field in the profile is associated or mapped to a corresponding field for one or more destinations. By default, the **No Document Profile** option will be selected.

A document attribute profile may include default or custom attribute properties and mappings that are common to a specific workflow. Custom profiles must be created prior to publishing Scan to Home device scan templates. When you select a document attribute profile, a static view of the fields that are associated with the profile will be shown.

### Document Name

The Document Name options define the output file name of the file to be generated and filed to the Scan Destination. Identification information is applied after the document is scanned. Determine the constraints (such as the characters allowed and the file overwrite policy) of your filing destinations before naming the output document.

## Problem Solving

Application, device, and network errors can occur in a variety of situations. This chapter includes some of the common issues and Frequently Asked Questions that pertain to SMARTsend, Xerox Multifunction Devices, and related networking issues.

*What's in this chapter:*

- *Troubleshooting a Problem* ..... 7-2
- *SMARTsend Confirmations and Error Logs*..... 7-3
- *Common Issues*..... 7-4
- *Frequently Asked Questions*..... 7-14

## Troubleshooting a Problem

When a problem persists, document the error messages and gather information to define the problem. The following problem-solving procedures are recommended:

- Accurately define the problem. When, where, and how does the problem occur?
- Reproduce the problem. Can the problem be reproduced consistently or is it an intermittent problem?
- Ask other users if they have encountered the problem, and keep a log to track problem occurrences.
- Examine the data for trends and the common attributes that may be related to the problem. For example, does the problem occur only with a specific multifunction device or on a specific workstation or network configuration?
- Review the product documentation, including the README files and problem solving topics, to see if any similar problems are documented.

If a cause and solution to the problem cannot be identified, call Xerox Customer Support to report the error information. Provide the support representative with the documentation that you have gathered to define the problem. Be sure to have your product Serial Number available at the time you place the call. See *Customer Support* on page 1-8 for additional information.

# SMARTsend Confirmations and Error Logs

SMARTsend supplies the following information to aid the troubleshooting process:

- **Job Confirmation Page.** If an option to report job outcome has been selected, a job confirmation page is either printed or e-mailed according to the Job Confirmation setting in the Workflow Settings page. Keep in mind that printed confirmation can be issued to a device only if the device provides its IP address in the job log. Some older Xerox devices, such as the Document Centre 420/425/432/440 series, do not provide this information. The Document Centre 545/555 series will provide its IP address in the job log if the Confirmation Report is enabled on the device. If a device does not support these requirements, choose e-mail confirmation as an alternative.

**NOTE:** The default for this option is OFF. If you edit an existing workflow and turn this feature on, you will need to re-publish the Device Scan Templates or PaperWare cover sheets (Professional Edition feature) in order for the confirmation to work.

Should troubleshooting be necessary, use the information from this page to trace a job's path from scanning device to destination. The following job data are reported:

- **Job Status.** SUCCEEDED or FAILED
- **Job Status Details.** An explanation for jobs with a status of FAILED.
- **Job Information.** Reports the job date and time, SMARTsend computer name, and job submitter (user).
- **Workflow Information.** Reports the workflow name, description, publication name, publication date and time, and publication creator (owner).
- **Document Scanner Service.** Reports status of the actual scanning procedure.
- **Destination Name.** Reports disposition of job at final destination, such as at a DocuShare site, FTP site, or remote printer.
- **Notes.** Additional comments on Job Status related to E-mail and Remote Printer destinations.
- **Administrator contact information.** Prints the name, e-mail address, and telephone number of the SMARTsend administrator as entered in the Administration General Settings page.
- **System Error Logs.** SMARTsend maintains a SMARTsendLog that reports a variety of system events such as device configuration, the starting and stopping of SMARTsend services and unsuccessful database backup attempts. Access it through Windows Event Viewer.

Events such as the starting and stopping of SMARTsend services are reported to the standard Windows event logs as appropriate. The Windows logs also contain entries concerning the Microsoft applications with which SMARTsend works, such as the .NET Framework, MSDE, and MDAC.

## Common Issues

### Server Unavailable Errors

Both the Microsoft .NET Framework and Internet Information Services (IIS) are installed on my Windows 2000 server, but when I start SMARTsend, I receive a "Server unavailable" error message.

IIS must be installed before the .NET Framework on a Windows 2000 server. Please consult the Microsoft Web site, [www.microsoft.com](http://www.microsoft.com), for IIS installation and configuration instructions.

▶ **To remedy, perform the following procedure:**

- 1 Uninstall SMARTsend, IIS, and the .NET Framework.
- 2 Reboot.
- 3 Reinstall IIS.
- 4 Reinstall SMARTsend (the SMARTsend installer loads the .NET Framework.).
- 5 After rebooting, SMARTsend should work properly.

### 403 "Forbidden" Error

I installed SMARTsend on a Windows Server 2003 host. When I start the application I receive a "403 Forbidden" error.

SMARTsend requires that ASP.NET be installed on a host running Windows Server 2003. ASP.NET is not installed on Windows Server 2003 by default. Please consult the Microsoft Web site, [www.microsoft.com](http://www.microsoft.com), for ASP.NET installation and configuration instructions.

### SMARTsend does not recognize IIS FTP service

If the IIS FTP service was installed after SMARTsend was installed, SMARTsend will not recognize the FTP service. Perform the following procedure to remedy this situation.

▶ **To add support for the FTP protocol to SMARTsend:**

- 1 Access Add/Remove Programs on a SMARTsend computer running Windows 2000 Server, or Add or Remove Programs on a SMARTsend computer running Windows Server 2003 or Windows XP Professional.
- 2 Select SMARTsend
- 3 Click **Change**.
- 4 Click **Repair**.
- 5 Complete the procedure.

### Unable to install MSDE during installation of SMARTsend

The SMARTsend installer may be unable to install MSDE if multiple security certificates have previously been installed on the SMARTsend computer. All previously installed certificates must be properly removed from the SMARTsend computer prior to installation. See *Replacing a Security Certificate* on page 2-18 for more information.

## Login Failure Message

When I try to scan with a published workflow (a Device Scan Template or PaperWare Cover Sheet), I get the following login failure message:

*A login failure occurred. Please contact the workflow owner to check for valid credentials for this destination.*

This message indicates that the template or cover sheet you are attempting to use has invalid or missing credentials. Published workflows require valid credentials to gain access to each destination. If the credentials change for any scanning destination, then the workflow owner must make the corresponding change to their SMARTsend credentials. Use the Manage My Credentials link on the SMARTsend User Home Page to update credentials.

## SMARTsend Inaccessibility within an Intranet

The behavior of the proxy server settings within newer versions of Internet Explorer and other browsers may vary among different software releases. If you are running SMARTsend on an intranet, the SMARTsend computer must be in the proxy server exceptions list. See *Client and Browser Configuration* on page 2-25 for more information.

**NOTE:** Each user may need to enter the specific IP Address AND the fully qualified Host Name for the SMARTsend computer.

## Windows 95/98/Me Client and Non-Microsoft Browser Access Problems

The IIS Basic Authentication setting must be enabled on the SMARTsend computer when the following client configurations exist:

- Any supported non-Microsoft browser is used to access SMARTsend.
- Any supported browser is used to access SMARTsend from a Windows 95/98/Me computer.

With these configurations, users will not be able to access SMARTsend if the IIS Basic Authentication option is disabled on the SMARTsend computer. See *Windows Authentication Methods Configuration* on page 2-11 for more information.

## Missing Icons on Document Destinations Page

In some cases, inconsistent DNS configurations may prevent the icons on the Document Destinations page from displaying. To resolve this issue, verify that the client computer has the same DNS configuration as the SMARTsend computer and correct any inconsistencies.

## Page Could Not be Displayed Error

After a server upgrade from Windows 2000 Server or Advanced Server to Windows Server 2003, users may experience a Page Could Not be Displayed error when accessing the site. If this situation occurs, check to confirm that the IIS default web site is running. See *Install and Configure IIS / FTP* on page 2-10 and *Enable ASP.NET* on page 2-12 for more information.

## Pop-up Blocker Problems

Pop-up blockers may interfere with some SMARTsend windows. Pop-up blockers should be disabled for the SMARTsend URL.

## Device Communication and Configuration Issues

There are a variety of configuration issues that can interfere with communication between SMARTsend and Xerox Multifunction Devices. In some cases, SMARTsend can repair certain configuration problems. If the problem cannot be repaired, SMARTsend will provide error messages and troubleshooting information to help you resolve these issues.

The first course of action to resolve device communication and configuration issues is to use the SMARTsend device Repair feature.

### ► To repair a device configuration:

- 1 From the Administration Home Page, click **View Xerox Devices**.
- 2 Select the device from the list.
- 3 Click **Repair**. If the problem can be fixed automatically, the status icon will change to signify that the device is properly configured. If SMARTsend detects a configuration problem that it cannot repair, additional information will be displayed in the Error Message column.

If the Repair does not resolve the problem, use the Test Configuration feature to perform a more comprehensive configuration test and obtain more detailed status and troubleshooting information.

### ► To test a device configuration:

- 1 From the Administration Home Page, click **View Xerox Devices**.
- 2 Select the device from the list.
- 3 Click **Test Configuration**. SMARTsend will display a Test Device Configuration page containing a test summary and individual status indicators for each test category. Review the information, then click **OK** to return to the Manage Xerox Device page. See *Test Device Configuration* on page 7-7 for additional information.
- 4 If the test failed, an Error Message will be displayed on the Manage Xerox Devices page. Follow the troubleshooting instructions provided in the Error Message column.

**NOTE:** If an error is detected, click the  icon in the Error Message column to display additional diagnostic and troubleshooting information.

## Test Device Configuration

The Test Device Configuration page depicts the test results that are obtained when the Test Configuration feature is performed on one or more Xerox devices. The following information is provided:

**Test Summary**—This column summarizes the test results for a given device. When a device fails any test, it will be shown as unavailable and an error message will be displayed in the Error Message column on the Manage Xerox Devices page. You can click the  icon in the Error Message column to display additional diagnostic and troubleshooting information.

**Device Account Test**—This test validates the credentials for the device account. This test will fail if the device account password has expired or if the device account was deleted.

**Default Repository Access Test**—This test verifies that the default repository on the device is accessible by the device account. This test will fail if the device account does not have access to the default repository directory or the SMARTsend computer.

**Protocol Test**—This test verifies that the data transfer protocol configured on the device is still supported by the SMARTsend computer. This test will fail if the data transfer protocol is invalid or was removed from the SMARTsend computer.

**Port Test**—This test verifies that the data transfer protocol port on the SMARTsend computer matches the port configured on the device. This test will fail if the data transfer protocol port was updated on the SMARTsend computer, and the device was not reconfigured.

**Device Settings Test**—This test verifies that the network scanning settings on the device match the SMARTsend system settings. This test will fail if the device was configured for network scanning by another application or configuration method.

**Template Pool Access Test**—This test verifies that the template pool is accessible by the device account and contains all template publications for this device. This test will fail if the device account does not have access to the template pool directory or the SMARTsend computer, or if one or more templates were deleted from the SMARTsend computer file system.

**If you are unable to resolve the problem using the Repair and Test Configuration options, check the following items:**

- The Xerox Multifunction Device must be online and not in the process of rebooting.
- The Xerox Multifunction Device must be properly configured to support network scanning.
- TCP/IP must be enabled on the device.
- SNMP must be enabled on the device and the SNMP settings must match the SNMP settings configured within SMARTsend.
- SNMP communication must be enabled on your network, and SNMP broadcast must be enabled to support SMARTsend device discovery (Discover Now option).
- If using DNS, verify that the computer is correctly configured in DNS. See *Verifying the SMARTsend Computer DNS Configuration* on page 2-8 for more information.
- If the SMARTsend computer is configured in DNS, the Xerox Multifunction Devices used with SMARTsend must be configured for DNS. The device DNS settings should be configured manually via the device user interface, or via the embedded web server (CentreWare Internet Services) before you attempt to add the device to SMARTsend.
- If the SMARTsend computer address or fully qualified Host Name changes, the site administrator must repair or reconfigure all devices that have been configured to work with that computer.
- If the update template list feature at the Xerox Multifunction Device generates errors or a partial template list, perform the following actions:
  - Follow the device Repair and Test Configuration procedures if you have not done so. See *Device Communication and Configuration Issues* on page 7-6 for additional information.
  - See *Template Refresh Failure at Devices* on page 7-9 for additional information.
- SMARTsend does not automatically support device account names that have been modified at the device user interface or the embedded web server (CentreWare Internet Services). These configuration changes should be made via the SMARTsend Manage Device Account Credentials page.
- If SMARTsend is being installed on a Windows XP Professional computer, then Simple File Sharing must be turned off. Please consult the Microsoft web site, [www.microsoft.com](http://www.microsoft.com), for Simple File Sharing configuration instructions.
- If SMB filing is required, then File and Printer Sharing must be turned on. See *Enable File and Printer Sharing* on page 2-9 for additional information.
- Confirm that the ports required for each supported protocol (FTP, SMB, HTTP, HTTPS) are not blocked by filtering at a switch, router, or firewall. See *TCP/IP Port Configuration* on page 2-29 for additional information.
- If these actions do not resolve the problem, reboot the device and check these items again. If the problem persists, contact Xerox customer support for assistance.

**NOTE:** SMARTsend supports the management of a limited number of Xerox Multifunction Devices. Open the SMARTsend About box to check the number of devices that are available. The last digits appended to the Serial Number indicate the number of devices that can be supported with your current installation. By default, SMARTsend Standard and Professional Editions support the configuration of up to five devices. License pack upgrades allowing the management of more devices may be purchased.

## Template Refresh Failure at Devices

There are several potential causes of template refresh failures on Xerox Multifunction Devices. The general issue is that the device, regardless of selected transfer protocol (SMB, FTP, HTTP, HTTPS), either cannot access the templates from the computer or cannot log in to that location. In some cases, the device configuration could also be overwritten by another application.

Use the SMARTsend device Repair and Test Configuration features to resolve template problems. See *Device Communication and Configuration Issues* on page 7-6 for additional information.

### If the template refresh problem is not resolved after checking all the device communication and configuration issues, try the following measures:

- Confirm that the device is pointed to the correct SMARTsend computer. This can be verified using the device embedded web server (CentreWare Internet Services).
- Confirm that the accounts for template pool and repository credentials contain the correct password.
- Confirm that the SMARTsend device account password is synchronized with the account password on the device.
- Confirm that the SMARTsend device account has local logon privileges on the SMARTsend computer.
- Confirm that the SMARTsend device accounts have network access to the SMARTsend computer. This can be done by checking the Local Security Policy on the computer to ensure that the Users group has local access.
- Confirm that the device Template Pool Setup is configured properly and is using the correct protocol. Also, confirm that the IP Address or Host Name for the template pool setup and file repository setup points to the SMARTsend computer IP Address.

**NOTE:** Use the CentreWare Internet Services remote user interface to confirm these settings.

### Try the following approaches if your transfer protocol is FTP:

- Confirm that FTP is installed and running under IIS on the SMARTsend computer.
- If FTP was installed after SMARTsend was installed, follow the instructions provided under *SMARTsend does not recognize IIS FTP service* on page 7-4.
- Use the Windows command prompt to start a FTP session and try logging in to FTP using the same account name and password used to set up the device. For example

```
> FTP localhost (or IP Address)
```

```
> username
```

```
> password
```

If login fails, it is most likely that the account name and password used are not valid.

**NOTE:** It is best to use a client on the same segment of the network as the device that you are troubleshooting.

### Try the following approach if your transfer protocol is SMB:

- Verify the account name and password by accessing the SMB share from another client.

## SharePoint Portal Server 2001 Compatibility with Windows Server 2003

The SharePoint Portal Server 2001 client cannot be installed with the Windows Server 2003 operating system. If SMARTsend is installed on a Windows Server 2003 server and a SharePoint Portal Server 2001 destination is required, the following procedure must be used.

### ► To configure a SharePoint Portal Server 2001 destination on Windows Server 2003:

- 1 From the SMARTsend User Site, click **Manage My Credentials**.
- 2 Under the Credentials Tasks, click **Add new credential**.
- 3 For the Account Type, select **Microsoft SharePoint Portal Server 2003**.
- 4 Complete the remaining fields in the Account Settings dialog by entering the SharePoint Portal Server 2001 parameters instead of the SharePoint Portal Server 2003 parameters.
- 5 Click **OK** to create the SharePoint Portal Server 2001 credential.

**NOTE:** This procedure enables users to create a SharePoint Portal Server 2001 destination using the SMARTsend Microsoft SharePoint Portal Server 2003 destination service. Under these circumstances, it would be best to disable the SMARTsend Microsoft SharePoint Portal Server 2001 service to avoid end user confusion. To do so, select Configure Service Settings on Administration Home Page, then Edit and uncheck (disable) the SharePoint Portal Server 2001 service.

## SharePoint 2001 / Windows 2000 SP4 Incompatibility

When SMARTsend is installed on a Windows 2000 or Windows 2000 Advanced Server with Windows 2000 SP4 installed, users may experience an inoperable Expand (+) button on the SharePoint Portal Server 2001 destination page.

### ► To resolve the browse button operability issue:

- 1 Install SharePoint Portal Server 2001 SP3 on the SharePoint server.
- 2 Enable "Directory Browsing" in Microsoft Internet Information Services (IIS) on the SMARTsend computer.

Please consult the Microsoft Web site, [www.microsoft.com](http://www.microsoft.com), for IIS installation and configuration instructions.

## "Validation Failed" Error with Domino.doc Destinations

Several SMARTsend scanning destinations require the installation of a client or additional software on the SMARTsend computer. In the case of Domino.doc destinations, a user will receive a "validation failed" error message if the Domino.doc client is not installed on the SMARTsend computer. See *Additional Requirements for Destinations* on page 2-19 for more information.

## Domino Server Error Messages

Storage of large documents may fail on some Domino servers. The server may generate error messages such as *Invalid POST Request Exception*, *Error Uploading Files*, or *Internal Server Error*. To resolve this error, go to the Internet Protocols - Domino Web Engine tab and set the Maximum POST data setting to a value that will handle the anticipated maximum file size.

## DocuShare and SharePoint Portal Server 2003 Access via HTTP Proxy Servers

The SMARTsend computer registry must be customized if a DocuShare or SharePoint Portal Server 2003 destination needs to be accessed through an HTTP proxy server. The customization procedures are documented below.



**CAUTION:** Windows registry editing can pose serious risks if the changes are not implemented properly. Please perform a registry backup before proceeding.

► *To enable SMARTsend proxy server support for DocuShare or SharePoint Portal Server 2003:*

- 1 Log in to the SMARTsend computer as an administrator.
- 2 Click **Start > Run**.
- 3 In the Run dialog, type **REGEDIT**. Click **OK**.
- 4 Open the following registry location:  
[HKEY\_LOCAL\_MACHINE\Software\Xerox\FreeFlowDDS\Settings\Install]
- 5 Right-click on or within the Install folder and select **New > String Value** to create registry entries for each of the following items:
  - a) ProxyEnable (string value = 1)
  - b) ProxyServer (string value = <protocol>=<server>:<port>)  
Use the following syntax if a different proxy server is used for each protocol:  
<protocol 1>=<server>:<port>;<protocol 2>=<server>:<port>  
Example: http=www.wb.mycompany.com:8080;https=www.wb.mycompany.com:8000  
- OR -  
Use the following syntax if the same proxy server is used for each protocol:  
<server>:<port>  
Example: www.wb.mycompany.com:8080
  - c) ProxyOverride (string value = *addresses accessible without a proxy server*)  
Example: 13.\*.\*.\*;xww\*.world.xerox.com

**NOTE:** ProxyOverride values may be copied directly from the Internet Explorer proxy server configuration. From Internet Explorer, choose **Tools > Internet Options > Connections > LAN Settings > Advanced > Exceptions**.

- 6 Close the registry to save the changes.
- 7 Confirm DocuShare or SharePoint Portal Server 2003 access from the SMARTsend computer by using a browser to access a valid DocuShare or SharePoint Portal Server 2003 collection. Once access has been confirmed, SMARTsend may be used to file to the DocuShare or SharePoint Portal Server 2003 destination.

## Install/Uninstall and Add Device Errors Related to DCOM Default Access Permissions

The following error conditions may occur if the DCOM Default Access Permissions have been altered on Windows 2000-based SMARTsend computers:

- .NET Framework version 1.1 error displayed during the SMARTsend installation, but the .NET Framework version 1.1 was installed properly.
- Add/Remove Programs window cannot be moved, resized, or closed after a failed uninstall.
- Fatal errors during installation message displayed 15-20 minutes after attempted install
- Add Xerox Devices operation fails because of an access denied error condition.

### ► *To correct DCOM Access Permissions (in Windows 2000):*

- 1 Click **Start > Run**.
- 2 Type *dcomcnfg* and press **Enter**. The Distributed COM Configuration Properties dialog box appears.
- 3 Click the Default Security tab.
- 4 Click **Edit Default** in the Default Access Permissions section. The Registry Value Permissions dialog box appears.
- 5 If both of the following conditions apply, click **OK** twice to exit.
  - The Name field includes the SYSTEM and INTERACTIVE accounts.
  - Type of Access for both accounts is Allow Access.Otherwise, proceed to Step 6.
- 6 Click **Add**. The **Add Users and Groups dialog box appears**.
- 7 Confirm that the local computer name is listed under List Names From.
- 8 Confirm that Type of Access is set to Allow Access.
- 9 Select the INTERACTIVE account if it was missing and click **Add**.
- 10 Select the SYSTEM account if it was missing and click **Add**.
- 11 Click **OK** on the next three screens to exit Distributed COM Configuration.
- 12 Log off and log on to the computer to implement your changes.

Refer to Microsoft Knowledge Base article #[274696](#) for additional support information. The article is available at <http://www.microsoft.com>.

## .NET Framework 1.1 Uninstall Issues

The .NET Framework uninstaller for Windows 2000 does not uninstall the 1.1 Framework completely, causing the SMARTsend installer to malfunction. You need to manually delete certain registry entries to resolve this problem.



**CAUTION:** Windows registry editing can pose serious risks if the changes are not implemented properly. Please perform a registry backup before proceeding.

---

► *To delete .NET Framework registry entries:*

- 1) Click **Start > Run**.
- 2) In the Open box, type **regedit**, and then click **OK** to start Registry Editor.
- 3) In the Registry Editor, delete the following registry entry:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\.NETFramework\policy\v1.1

**NOTE:** Delete the .NET Framework folder from the top of the registry (not the v1.1 folder only).

## Windows 2000 Advanced Server SP4 Device Management Issues

Updating a Windows 2000 Advanced Server to SP4 causes issues with SMARTsend device management (discovery and configuration). The problem(s) are associated with known Microsoft issues where the process that runs ASP.Net is not granted appropriate permissions. These issues and the workarounds are documented in Microsoft Knowledge Base Articles [824308](#), and [827559](#). These articles are available at <http://www.microsoft.com>.

## Frequently Asked Questions

### How does an administrator control access to SMARTsend?

SMARTsend uses Windows and relies on standard Windows accounts to manage access to the SMARTsend site. See *Create Administrator, User, and Device Accounts* on page 2-13 for more information.

### How do I configure SMARTsend to use a Sun Java System Directory LDAP Server for Integrated Address Book Lookup?

The following string entry should be added to the Registry before configuring the SMARTsend LDAP settings:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Xerox\FreeFlowDDS\Settings\Install] LdapObjectFilter = (objectClass=person)
```

**NOTE:** This value is not required for other types of LDAP servers and may cause them to fail to return user records. Also, depending on server setup, a different filter string may be required.

To configure the SMARTsend LDAP settings, click on Setup E-mail and Address Book from the Administration Home Page:

- 1 At the E-mail and Address Book Setup page, enter a valid LDAP host name (e.g. v-sundir).
- 2 Enter colon port number after the host name (e.g. v-sundir:389).
- 3 Enter a forward slash and base (e.g. v-sundir:389/o=Test\_Domain)
- 4 Enter valid LDAP property mappings.
- 5 Select Apply button and then select Test to verify success.

**NOTE:** Short host names may or may not work so please use the full host name (e.g. v-sundir.domain.com).

### Can I install SMARTsend on a domain controller?

No. SMARTsend cannot operate on a domain controller. SMARTsend should reside on its own application computer within a Windows 2000 Server/Advanced Server or Windows Server 2003 domain.

### Can I install SMARTsend on a computer running Xerox FlowPort?

No. SMARTsend cannot operate on a computer that runs Xerox FlowPort.

### Can I install SMARTsend on a computer running CentreWare Network Scanning Services?

No. SMARTsend should not be installed on a computer that runs Xerox CentreWare Network Scanning Services.

### **During installation, I get a question from Microsoft SQL Server Desktop Engine asking me to reboot the server. However, the SMARTsend installation continues whether I click Yes or No. Why?**

The question box is part of the Microsoft MSDE installer. It appears on the computer when installing MSDE for the first time. Systems where MSDE has been installed prior to the SMARTsend installation will not see it.

If you see this question, you must click **Yes** or **No** to continue with the SMARTsend installation. However, no reboot will occur even if you click **Yes**. The SMARTsend installer will finish installing the application and display its own reboot window. Clicking **Yes** at that point reboots the computer.

### **Does the Template Importer import FlowPort PaperWare templates to SMARTsend workflows?**

The Template Importer does not import FlowPort PaperWare templates to SMARTsend workflows. It only imports CentreWare Network Scanning Services templates into workflows.

### **How can I learn the SMARTsend workflow names of imported CentreWare Network Scanning Services templates?**

You can learn the workflow names of imported CentreWare Network Scanning Services templates by starting SMARTsend and accessing the Workflow Explorer. Imported templates become SMARTsend workflows, and they retain their CentreWare Network Scanning Services filenames, less the .xst extension.

### **Why aren't my CentreWare Network Scanning Services templates available after running the Template Importer?**

The Template Importer creates new SMARTsend workflows that are based on the imported templates. The resulting workflows must then be published to a Xerox Multifunction Device as a Device Scan Template.

### **The account under which I administer SMARTsend lacks administrative privileges on a CentreWare Network Scanning Services server. Can I use the Template Importer to import templates from that server?**

You can use the Template Importer to import CentreWare Network Scanning Services templates from any CentreWare Network Scanning Services server for which you know an administrative account name and password, which can differ from the administrative account name and password used with SMARTsend.

### **If I publish a workflow to a PaperWare Cover Sheet, and send it to print on A4 paper, it does not print. Why?**

An A4 PaperWare Cover Sheet will not print if the printer driver's default Paper Source option is set to Auto Select. Set Paper Source to a tray that contains A4 paper and try printing again. Also, bear in mind that various settings in the printer driver, such as image quality adjustments, can impact your ability to print and use PaperWare cover sheets successfully.

### **When running on a Windows XP computer, SMARTsend is unable to display all destinations on the Document Destinations page. Why?**

IIS on Windows XP is configured out of the box for a maximum of 10 HTTP connections. If installing SMARTsend on a Windows XP computer and running OCR jobs or jobs with a large page count, the number of HTTP connections may be exceeded. This may cause SMARTsend to be unable to show all destinations on the Document Destinations page. The number of HTTP connections can be increased to 40 (but not higher). To do this, find the adsutil.vbs script on the SMARTsend computer (should be in c:\inetpub\AdminScripts or similar) and run the following command:

```
adsutil set w3svc/MaxConnections 40.
```

### **When running on a Windows Server 2003 computer with Service Pack 1, SMARTsend is unable to display all services on the Configure Service Settings page and the corresponding destinations on the Document Destinations page. Why?**

When SMARTsend is installed on a Windows Server 2003 computer with Service Pack 1 installed and the computer is configured as a standalone computer (not in a domain), DNS is not always handled fully by the network infrastructure. That is, the DHCP server does not completely register the hostname. As a result, services may not be listed on the Configure Service Settings page and the corresponding destinations will not be available on the Destinations page. To fix this, specify a primary DNS suffix when configuring the computer name. This can be done with the following steps:

- 1 At the SMARTsend computer, right click on My Computer and select Properties.
- 2 Click on the Computer Name tab.
- 3 Click on the Change button.
- 4 Specify a Primary DNS suffix when configuring the computer name.
- 5 Click OK. Exit out.
- 6 Reboot the computer.

**NOTE:** The fix may not occur immediately. Give the DNS server time to replicate the information.

### **My organization's network does not use a domain. How would we log in to SMARTsend?**

In this situation, all SMARTsend users must have local accounts on the SMARTsend computer. Users would log in to the SMARTsend application using the username and password for their local account.

### **Users are unable to print Microsoft Office Documents to a Remote Printer destination. Why?**

If you are unable to print Office documents to a Remote Printer destination, please ensure that Microsoft Office has been configured as an interactive user. If this fails to remedy the problem, uninstall and reinstall the Microsoft Office application.

If SMARTsend is uninstalled and later reinstalled, and you will be submitting Office documents to a Remote Printer destination, you must reconfigure Microsoft Office as an interactive user.

See *Configuring Microsoft Office as an Interactive User* on page 2-20 of the SMARTsend Installation and Administration Guide for additional information.

### **Will SMARTsend work in an Active Directory environment?**

Yes. SMARTsend does function within an Active Directory environment. On Windows 2000 and Windows 2003 domain controller servers, Active Directory is used to create domains. SMARTsend computers may be members of these domains and users of SMARTsend may be domain users.

### **Does SMARTsend require Active Directory?**

No. SMARTsend does not require Active Directory to function. SMARTsend can be installed on a Windows 2000 Server/Advanced Server, a Windows XP Professional computer, or a Windows 2003 Server that is configured as a stand-alone server.

SMARTsend does support the lookup of e-mail addresses via LDAP for building workflows. The LDAP lookup is not specific to Active Directory. This lookup is done only at workflow creation time when a user

types in a partial name and clicks "check names" during the process of creating an e-mail destination. If LDAP lookup is not available, e-mail addresses can still be typed by hand.

### **Does SMARTsend provide a means to enter a user name and password for querying Active Directory?**

No, but it is not necessary. When using SMARTsend to create workflows, the user is authenticated to the SMARTsend computer. That user's network identity is used to perform any LDAP queries that may be required for selecting e-mail addresses from the address book. If the user identity has rights to the address book, the query will succeed. If the user does not have rights to the address book, they can manually enter e-mail addresses.

SMARTsend complies with the access rights defined by the LDAP system administrator. If the user does not have rights to the address book, rights will not be granted via SMARTsend.

### **If I publish a workflow, defined with a Job Confirmation Method of Printed, to a Xerox Multifunction Device that has Job Based Accounting enabled, I do not receive a printed job confirmation at the device. Why?**

The Job Based Accounting feature enabled in SMARTsend will allow a user to publish a workflow, defined with a Job Confirmation Method of Printed, to a Xerox Multifunction Device that has Job Based Accounting enabled. When a user executes a scan job using the published workflow, a printed confirmation showing the success status of the scan job will be received.

When this feature is not enabled in SMARTsend, a user may still publish and use the workflow. However, a printed confirmation will not be received at the device. This will be the case whether the job is successful or not.

To enable Job Based Accounting support on the SMARTsend computer, perform the following steps:

- 1 Click on Start > Run and type regedit and hit Enter.
- 2 Go to the following registry location:  
[HKEY\_LOCAL\_MACHINE\Software\Xerox\FreeFlowDDS\Settings\Install]
- 3 Right click on the Install folder to create a new "String Value".
- 4 Name the new string value "JBAEnabled" and set the value to 1.
- 5 Right click on the Install folder to create a new "String Value".
- 6 Name the new string value "JBAUserID" and set the value to be the associated user id to use with Job Based Accounting.
- 7 Right click on the Install folder to create a new "String Value".
- 8 Name the new string value "JBAAccountID" and set the value to be the associated account id to use with Job Based Accounting.
- 9 Close the registry.

### **Does SMARTsend require anonymous access to the address book?**

SMARTsend does not require anonymous access to the address book. If the LDAP server being used does not support anonymous directory access, go to the Administration Home Page and click on the Setup E-mail and Address Book link to enter credentials that can be used when accessing the LDAP server.



## SMARTsend Utilities

SMARTsend supplies several administrative utilities. The Template Importer imports CentreWare Network Scanning Services templates into SMARTsend workflows. The Restore Tool is a wizard that performs an in-place restoration of a database backup, while the Job History Exporter makes SMARTsend job data available for use by other applications.

This chapter describes the operation of these utilities.

### *What is in this chapter:*

- *Requirements* ..... 8-2
- *Template Importer* ..... 8-3
- *Restore Tool* ..... 8-12
- *Exporting Job History* ..... 8-14

## Requirements

The Template Importer, Restore Tool and Job History Exporter are a part of the standard SMARTsend installation. Operational requirements are as follows:

- Administrative privileges on the SMARTsend computer.
- Access to the SMARTsend computer Desktop.
- To use the Template Importer, the following additional requirements apply:
- CentreWare Network Scanning Services template pool, version 3.x or later.
- Templates that reside in the CentreWare Network Scanning Services folder designated as the template pool location.
- If you have templates that scan to OCR and meet the supported file format and language recognition requirements. See *File Format and Language Support* on page 8-4.
- SMARTsend Professional Edition, if importing templates that support OCR.

## Template Importer

The SMARTsend Template Importer imports CentreWare Network Scanning Services templates into SMARTsend workflows. This tool assists system administrators who are migrating from CentreWare Network Scanning Services to SMARTsend and wish to use their existing CentreWare scanning templates with SMARTsend. The source templates remain in their original locations to allow users to retain access to their current services during the transition to SMARTsend.

### The Template Importer will:

- Assist with the upgrade from CentreWare Network Scanning Services 3.x, 4.x and 5.x to SMARTsend.
- Facilitate the conversion of existing CentreWare templates to SMARTsend workflows that perform the same functions as the templates imported from a selected CentreWare Network Scanning Services Scan Server.

Once the import procedure is complete, the system administrator uses the device management features of SMARTsend to migrate Xerox Multifunction Devices from the CentreWare Network Scanning Services server to the SMARTsend computer. Users can then publish the imported templates (workflows) to the Xerox Multifunction devices as device scan templates. If you are using the SMARTsend Professional Edition, users also have the option to publish imported templates as PaperWare cover sheets.

See *Scanning Device and Application Migration* on page 2-3 for additional information and migration considerations. Refer to Chapter 4 of the SMARTsend User Guide for information on publishing workflows.

**NOTE:** See *Exceptions List* on page 8-7 for the kinds of templates and template data that are not imported.

## File Format and Language Support

In the Professional Edition of SMARTsend, the Template Importer imports CentreWare Network Scanning Services templates that support scanning to OCR. The following tables supply information on the CentreWare Network Scanning Services file formats and languages that the Template Importer supports:

### Supported OCR file formats

This table lists the OCR file formats that the Template Importer supports in the Professional Edition of SMARTsend. .

|                         |                                   |
|-------------------------|-----------------------------------|
| ■ ASCII_STD             | ■ PDF_NORMAL_HIGHLY_SUSPECT_WORDS |
| ■ ASCII_STD_DOS         | ■ PDF_NORMAL_NO_WORD_IMAGES       |
| ■ ASCII_STRIPPED        | ■ PDF_NORMAL_SUSPECT_WORD_IMAGES  |
| ■ ASCII_STRIPPED_DOS    | ■ POWERPOINT_97                   |
| ■ EXCEL_OFFICE_97       | ■ PUBLISHER_98                    |
| ■ HTML                  | ■ RTF                             |
| ■ HTML 3.0              | ■ RTF_WORD_6_0                    |
| ■ HTML 4.0              | ■ RTF_WORD_97                     |
| ■ HTML_HOTMETAL         | ■ RTF_WORD_2000                   |
| ■ HTML_NETSCAPE         | ■ UNICODE                         |
| ■ HTML_TABLE            | ■ UNICODE_LB                      |
| ■ HTML_WYSIWYG          | ■ UNICODE_CSV                     |
| ■ PDF                   | ■ WORD_6_0                        |
| ■ PDF_IMAGE_ONLY        | ■ WORD_PERFECT_8_9_0              |
| ■ PDF_IMAGE_SUBSTITUTES | ■ WORD_7_0                        |
| ■ PDF_IMAGE_TEXT        | ■ WORD_OFFICE_97                  |

**Table 8-1: Supported OCR file formats**

## Supported OCR Recognition types

Templates for scanning to OCR include a field called OCR Recognition that specifies the language the OCR software uses to "read" graphic characters during their conversion to text.

The following table lists the languages that the Template Importer supports. If the value of the OCR Recognition field in the CentreWare Network Scanning Services template matches a language in the table, the Template Importer imports that template, assuming that none of the exceptions described in the *Exceptions List* on page 8-7 apply.

|                     |                          |                   |
|---------------------|--------------------------|-------------------|
| ■ AFRIKAANS         | ■ IDO                    | ■ PROVENÇAL       |
| ■ ALBANIAN          | ■ INDONESIAN             | ■ QUECHUA         |
| ■ AYMARA            | ■ INTERLINGUA            | ■ RHAETIC         |
| ■ BASQUE            | ■ ITALIAN                | ■ ROMANIAN        |
| ■ BEMBA             | ■ KABARDIAN              | ■ ROMANY          |
| ■ BLACKFOOT         | ■ KASUB                  | ■ RUANDA          |
| ■ BRETON            | ■ KAWA                   | ■ RUNDI           |
| ■ BUGOTU            | ■ KIKUYU                 | ■ RUSSIAN         |
| ■ BULGARIAN         | ■ KONGO                  | ■ SAMOAN          |
| ■ BYELORUSSIAN      | ■ KPILLE                 | ■ SARDINIAN       |
| ■ CATALAN           | ■ KURDISH                | ■ SERBIAN         |
| ■ CHAMORRO          | ■ LAPPISH                | ■ SHONA           |
| ■ CHECHEN           | ■ LATIN                  | ■ SIOUX           |
| ■ CORSICAN          | ■ LATVIAN                | ■ SLOVAK          |
| ■ CROATIAN          | ■ LITHUANIAN             | ■ SLOVENIAN       |
| ■ CROW              | ■ LUBA                   | ■ SOMALI          |
| ■ CZECH             | ■ LUXEMBOURGIAN          | ■ SORBIAN         |
| ■ DANISH            | ■ MACEDONIAN             | ■ SOTHO           |
| ■ DUTCH             | ■ MALAGASY               | ■ SPANISH         |
| ■ ENGLISH           | ■ MALAY                  | ■ SUNDANESE       |
| ■ ESKIMO            | ■ MALINKE                | ■ SWAHILI         |
| ■ ESPERANTO         | ■ MALTESE                | ■ SWAZI           |
| ■ ESTONIAN          | ■ MAORI                  | ■ SWEDISH         |
| ■ FAROESE           | ■ MAYAN                  | ■ TAGALOG         |
| ■ FIJIAN            | ■ MIAO                   | ■ TAHITIAN        |
| ■ FINNISH           | ■ MINANKABAW             | ■ TINPO           |
| ■ FRENCH            | ■ MOHAWK                 | ■ TONGAN          |
| ■ FRISIAN           | ■ MOLDAVIAN              | ■ TSWANA (CHUANA) |
| ■ FRIULIAN          | ■ NAHUATL                | ■ TUN             |
| ■ GAELIC (IRISH)    | ■ NORWEGIAN              | ■ TURKISH         |
| ■ GAELIC (SCOTTISH) | ■ NYANIA                 | ■ UKRAINIAN       |
| ■ GANDA (LUGANDA)   | ■ OCCIDENTAL             | ■ VISAYAN         |
| ■ GERMAN            | ■ OJIBWAY                | ■ WELSH           |
| ■ GUARANI           | ■ PAPIAMENTO             | ■ WOLOF           |
| ■ GREEK             | ■ PIGINENGLISH           | ■ XHOSA           |
| ■ HANI              | ■ POLISH                 | ■ ZAPOTEC         |
| ■ HAWAIIAN          | ■ PORTUGUESE (BRAZILIAN) | ■ ZULU            |
| ■ HUNGARIAN         | ■ PORTUGUESE (EUROPEAN)  |                   |
| ■ ICELANDIC         |                          |                   |

**Table 8-2: The Template Importer can import templates whose OCR Recognition fields are set to any of these languages.**

## Exceptions List

The following list contains the types of CentreWare Network Scanning Services templates, or elements of these templates, that the Template Importer does not import:

- Templates created in CentreWare Network Scanning Services versions 2.x or earlier. Templates must be version 3.x or later.
- NetWare 3.x repositories. SMARTsend does not support scanning to NetWare 3.x repositories.
- **CentreWare Network Scanning Services document attribute fields listed in the supported templates.** SMARTsend maps document attribute fields (metadata) to workflow destinations. Mapping information is not available in CentreWare Network Scanning Services templates. Please refer to the SMARTsend User Guide for information on document attribute mapping.
- **Scan to Microsoft Exchange Public Folders.** SMARTsend uses Microsoft Exchange 2000 Web Folders as a destination, which is incompatible with Exchange Public Folders and destinations.
- **Custom or third party templates.**
- Scan to DigiPath templates.
- Group templates. SMARTsend has no equivalent concept.
- **Print Local Copy feature.** The Template Importer does not import the portions of a CentreWare Network Scanning Services template that concern printing a copy of the scanned document on the printer from which it was scanned.
- **Templates that scan to a Fax Service.**
- Default template. The default template for a Xerox Multifunction Device is re-created when SMARTsend configures the device.
- **Templates that contain OCR file formats and/or recognition languages that are not supported by the SMARTsend OCR service.** Table 8-1 on page 8-4 and Table 8-2 on page 8-6 include lists of supported OCR file formats and recognition languages. Templates that OCR to other file formats and specify other recognition languages are not imported.

**NOTE:** SMARTsend imports templates that scan to user folders or to repositories on the CentreWare Network Scanning Services server. However, if a system administrator uninstalls a Xerox Multifunction Device and deletes the corresponding CentreWare Network Scanning Services server, the users will need to modify the SMARTsend workflows to include a valid destination. SMARTsend will not manage user folders. The system administrator must add and remove user folders from the CentreWare Network Scanning Services scan server.

## Importing CentreWare Templates to SMARTsend Workflows

The SMARTsend Template Importer imports CentreWare Network Scanning Services templates into SMARTsend workflows.

### ► To import CentreWare Network Scanning Services templates to SMARTsend workflows:

- 1 SMARTsend must be installed and configured on the application computer. See Chapters 1-3 of this guide for complete instructions.
- 2 Open the Template Importer. If running Windows 2000:  
Click **Start > Programs > Xerox > SMARTsend > Template Importer**.  
- OR -  
If running Windows Server 2003 or Windows XP Professional:  
Click **Start > All Programs > Xerox > SMARTsend > Template Importer**.
- 3 The SMARTsend Template Importer window appears. Click **Browse for Templates**.
- 4 Each scan server that CentreWare Network Scanning Services manages has its own Cw\_scan.ini file in the root folder that was created when CentreWare Network Scanning Services was installed. Locate and select the appropriate Cw\_scan.ini file. Click **Open**. If you cannot browse to your CentreWare scan server location, you may need to map a network drive to the CentreWare scan server before performing this step.

**NOTE:** If the cw\_scan.ini files are on another server to which you do not have administrative privileges, you will be prompted to log in under an account that has administrator privileges.

- 5 The Template Importer displays the number of templates (.xst files) in the CentreWare Network Scanning Services template pool folder. Click **Import Templates**. The Template Importer processes the .xst files and displays the results in the Import Status panel. Files imported into workflows appear first. Files not imported appear below them in a separate list. A status message will indicate when the template pool import is complete.
- 6 Click **Save Results** to generate a report. The report consists of a comma-delimited text file, readable by applications such as Windows word processors and Microsoft Excel, that contains the following information:

| Field Name                   | Description                                                            |
|------------------------------|------------------------------------------------------------------------|
| Template Pool Location       | Path to CentreWare Network Scanning Services template pool             |
| CentreWare Template Name     | Name (with extension) of CentreWare Network Scanning Services template |
| SMARTsend (TM) Workflow Name | Name of SMARTsend workflow                                             |
| Conversion Status            | Value of either Success or Failed                                      |
| Description of Failure       | Explanation for Failed status                                          |

**Table 8-3: Template Importer report fields**

- 7 Click **Exit** to close the Template Importer.

**NOTE:** When you import CentreWare Network Scanning Services templates into SMARTsend, the templates are not deleted or removed from the CentreWare scan server. Likewise, any Xerox Multifunction Devices that were used with CentreWare Network Scanning Services will continue to point to the CentreWare scan server until they are reconfigured by SMARTsend. The CentreWare scan server will remain intact after the device(s) are reconfigured with SMARTsend.

- 8 Launch SMARTsend in your web browser (*http://<computername or IP address>/SMARTsend*). If you logged in as a SMARTsend Administrator, click the User Site link in the upper right corner of the Administration Home Page.
- 9 At the User Home Page, select View All Workflows. The imported templates appear as new workflows bearing the original template filenames, without the .xst extensions. The workflows are owned by the administrator who performed the conversion and they are classified as Public.

**NOTE:** If a duplicate workflow name exists on the SMARTsend computer, the new workflow is renamed to avoid overwrites. The first duplicate has "\_1" appended to its name, the second duplicate has "\_2" appended, etc.

- 10 Workflows can be published to a configured Xerox Multifunction Device or as a PaperWare cover sheet.

When the CentreWare Network Scanning Services templates are imported to SMARTsend workflows, the user account used to import the templates designates the owner of the newly created workflows. To use the imported workflows, the SMARTsend Administrator must log in using the same user account that was used when the templates were imported.

**TIP:** To verify that you have logged in as the workflow owner, locate the current SMARTsend user name in the top right corner of any SMARTsend page. Click on the workflow for which you want the owner information, then view the Details pane on the left side of the Workflow Explorer page. The Details pane lists the Owner of the workflow. The current SMARTsend user and workflow owner must be the same in order to use the imported template/workflow.

- 11 As the workflow owner, the administrator must enter the credentials for each of the locations in the newly created workflows. This can be done using two methods:
  - a) Use the 'Add a New Credential' link from the user home page.- OR -
  - b) SMARTsend will prompt the Administrator for credentials when publishing a newly created/imported workflow.
- 12 Alternatively, users can manage their own credentials by becoming the owner of the newly created workflow. Use the following procedure after the administrator imports the CentreWare templates to SMARTsend workflows:
  - c) Login to the SMARTsend computer and go to the User Home Page.
  - d) Click the **View All Workflows...** link.
  - e) Select the workflow that you want to own.

- f) Click the **Edit this workflow...** link.
- g) Rename the workflow.
- h) Click **Save As**.

The user is now the workflow owner and can enter credentials for the workflow using either of the following procedures:

- a) Select the 'Add a New Credential' link from the user home page.
- OR -
- b) SMARTsend will prompt the User for credentials when publishing a newly created/imported workflow.

Consult chapters 3 and 4 of the SMARTsend User Guide for information on modifying and publishing workflows.

## Reconfiguring Devices for CentreWare Network Scanning Services

If you need to reconfigure a Xerox Multifunction Device to use CentreWare Network Scanning Services after you have configured the device with SMARTsend, use the following procedure to point the device back to the CentreWare scan server.

### ► To reconfigure a Xerox device for CentreWare Network Scanning Services:

- 1 Launch the CentreWare Add Network Scanner wizard from a workstation while logged on as a user with administrator permissions. (Example: **Start > Programs > Xerox > CentreWare > Add Network Scanner**)
- 2 Select **Enable a new Xerox system scanner for network scanning and associate it with a scan server**. Click **Next**.
- 3 Select a method to detect the Xerox Multifunction Device you are configuring and click **Next**.
- 4 If prompted, enter the password for the device and click **OK**.
- 5 Select the server operating system and browse to the directory of the existing scan server. Click **Next**.
- 6 Enter the Xerox system login name and password and click **Next**.
- 7 Click **Next**, and then **Finish**.

**NOTE:** The Xerox device uses the templates at the CentreWare scan server. There is no way to migrate workflows created or edited in SMARTsend back to the CentreWare scan template folder.

Consult the *CentreWare Network Scanning Services Installation Guide* for additional instructions.

## Restore Tool

The SMARTsend Restore Tool works in conjunction with the SMARTsend Backup features. The backup feature copies SMARTsend registry settings, workflows, device database, account database, publications, available services, file attributes, service account credentials, and administrative settings to a backup set that is catalogued by date and time. Program files and templates are not included, although templates are reconstructed from other data when running the Restore Tool.

SMARTsend creates the following folder for backup storage:

```
<drive>:\Inetpub\wwwroot\SMARTsend\Data\Backup\
```

The backup filenames are based on the following naming convention:

```
FreeFlow SMARTsend_<year_month_day_hours_minutes_seconds>\<Backup_ID>.
```

**NOTE:** This process does not replace the routine of backing up the SMARTsend computer to an external storage device such as a tape drive. Its purpose is to record a snapshot of the SMARTsend installation while the database is not in use. The resulting backup set should be copied to an external storage device as part of the computer's regular backup routine.

## Conditions for using the Restore Tool

The Restore Tool must operate under the following conditions:

- The computer must reside in the same domain that it did when the backup occurred.
- There must be enough hard disk capacity to accommodate both the backup set files and the resultant SMARTsend database and Windows registry entries.
- The SMARTsend backup operation does not include local user accounts. If the computer is either being rebuilt or replaced, the original user account information, especially the original SIDs, must be recovered with a standard backup or disaster recovery product for local users to retain their SMARTsend access privileges.
- The Restore Tool stops SMARTsend and IIS services before restoring the database, and restarts them after restoration completes. SMARTsend does not accept new jobs until the services are restarted.

## Using the Restore Tool

### ► To use the Restore Tool:

- 1 If your backup has been moved, return it to its original location. Backup folders reside in `<drive>:\Inetpub\wwwroot\SMARTsend\Data\Backup\`  
`FreeFlow SMARTsend_<year_month_day_hours_minutes_seconds>\<Backup_ID>.`
- 2 If running Windows 2000:  
Click **Start > Programs > Xerox > SMARTsend > Restore Tool.**  
- OR -  
If running Windows Server 2003 or Windows XP Professional:  
Click **Start > All Programs > Xerox > SMARTsend > Restore Tool.**
- 3 The Restore Tool Wizard Welcome screen appears. Click **Next.**
- 4 A list of backup sets, called Restore Points, appears. Select the date and time that corresponds with your backup.

- OR -

If you do not see the desired backup set in the list, click **Backup Directory Path** and browse to the location of the backup set.

After selecting a backup set, click **Next**.

- 5 A window that displays the selected backup path and a warning message about the acceptance of incoming jobs appears. To stop the acceptance of incoming jobs and continue with the restore, click **Next**.
- 6 A caution window that announces the stoppage of IIS services appears. Click **Next**.

**NOTE:** At this point, SMARTsend communicates the number of jobs that are currently processing. Clicking **Next** cancels these jobs.

- 7 Click **Start** to begin the restore.
- 8 A status window reports the outcome. Click **Finish** to exit the wizard. IIS and SMARTsend services restart.

**NOTE:** When using the SMARTsend Restore Tool to perform a restore of a SMARTsend backup with a large number of configured devices, the Restore Tool may go into an unresponsive state. This is normal behavior and the restore process may take a long time to complete.

## Exporting Job History

The Job History Exporter converts the SMARTsend job log into a comma-delimited text file for use by analytical and reporting applications. It also provides a method of retaining job history information beyond the 90 day limit that SMARTsend imposes. Job records remain in SMARTsend after running this utility.

**NOTE:** SMARTsend checks the job history database once a day and deletes job information that is older than 90 days. If you need to retain job history data for a longer time interval, you should run the Job History Exporter at least every 90 days to save the data before it is automatically deleted by SMARTsend.

### ► To export the job history log:

- 1 If running Windows 2000:  
Click **Start > Programs > Xerox > SMARTsend > Job History Exporter**.  
- OR -  
If running Windows Server 2003 or Windows XP Professional:  
Click **Start > All Programs > Xerox > SMARTsend > Job History Exporter**.
- 2 Enter a file name, including the .txt or .csv extension. The extension choice depends on the application in which this data is used.
- 3 Click **Export Data**. The Job History Exporter sets up the history file. The default path is `<drive>:\>Documents and Settings\<account_name>\<job_history_filename>`.
- 4 A results window appears. Click **OK**.
- 5 Click **Exit**.

The job history records consist of the following fields:

| Field Name       | Description                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------|
| Task_Name        | SMARTsend workflow name                                                                                            |
| Owner            | Workflow owner                                                                                                     |
| Submitter        | Workflow user                                                                                                      |
| Activation_Name  | Publication name                                                                                                   |
| Activation_Owner | Publication owner                                                                                                  |
| Start_Time       | Date and time job was submitted to SMARTsend                                                                       |
| Page Count       | The number of physical pages scanned                                                                               |
| Input_Format     | Format of the scanned document at the scanning device                                                              |
| Output_Format    | Format of the scanned document at the job's completion, such as after conversion into a readable format using OCR. |
| Status           | <b>Succeeded</b> or <b>Failed</b>                                                                                  |
| Error_Message    | Explanation for jobs whose Status is <b>Failed</b>                                                                 |
| Access           | Workflow access level (public/private)                                                                             |

**Table 8-4: Job History Exporter report fields**

## SMARTsend Security

This chapter summarizes the concepts and tools underlying the security capabilities of SMARTsend. These capabilities leverage the Microsoft Windows security model, the authentication capabilities of scanning devices, and the security provisions of workflow destinations. SMARTsend must accommodate the variations in security features within these components, as well as the capabilities of Internet Fax devices, to provide network scanning capabilities to its users.

### *What is in this chapter:*

|                                                  |      |
|--------------------------------------------------|------|
| ■ <i>Security Overview</i> . . . . .             | 9-2  |
| ■ <i>HTTPS/SSL Certificates</i> . . . . .        | 9-3  |
| ■ <i>Site Security Policies</i> . . . . .        | 9-5  |
| ■ <i>Workflow Access Level Control</i> . . . . . | 9-9  |
| ■ <i>Security Policy Interactions</i> . . . . .  | 9-10 |
| ■ <i>SMARTsend Authentication</i> . . . . .      | 9-12 |
| ■ <i>Credentials</i> . . . . .                   | 9-14 |

## Security Overview

There are several security-related issues to consider when installing, configuring, and using SMARTsend. The key elements of site security include:

- HTTPS/SSL Certificates
- Site Security Policies
- Security Policy Interactions
- SMARTsend Authentication

The configuration of these elements dictates how SMARTsend protects data transmission on the SMARTsend computer, restricts unauthorized access to distribution destinations, and maintains user privacy. These security elements should be reviewed and applied, as needed, to meet the specific security requirements of each organization or workgroup.

## HTTPS/SSL Certificates

SMARTsend provides options to configure the web site for secure password entry and secure data transmission. These options are based on the HTTPS and SSL (Secure Socket Layer) protocols provided by the Windows operating system.

HTTPS/SSL provides the following:

- Confidentiality—Encrypted information is exchanged between clients and servers over a secure connection.
- Integrity—The integrity of message content exchanged between client and server is verified.

HTTPS requires the usage of Secure Server Certificates (SSL certificates). For instructions on how to obtain and install an SSL certificate for the SMARTsend computer, refer to *Obtain and Install a Security Certificate* on page 2-16 of Chapter 2, *Prepare for Installation*.

SMARTsend makes the use of security certificates optional to accommodate installations where other security measures are employed or where security is not a concern. When a security certificate is installed on the SMARTsend computer, it will provide secure password entry when users access SMARTsend. Furthermore, if the *Require Secure Channel (SSL)* option and the security certificate are properly configured on the SMARTsend computer, all data transfer between SMARTsend users and devices will be encrypted.

For more information, visit Microsoft on the web at:

<http://www.microsoft.com/technet/security/topics/identity/default.mspx>

### Secure Password Entry

When the secure password entry option is configured in SMARTsend, the HTTPS transmission protocol is used to transmit user credentials and passwords securely across the network. When this option is not selected, passwords are sent in clear text across the network and are vulnerable to security issues. See *General Site Security* on page 9-5 for additional information.

### Secure Web Site Configuration

The SMARTsend computer can also be configured to require the use of SSL for all communication and data transfer. This involves manual configuration of the IIS (Internet Information Services) Directory Security properties using Microsoft Management Console. This is performed on the computer after SMARTsend and an SSL Certificate have been installed.

**NOTE:** Certificates establish identity and trusts for the secure exchange of information. Certificate authorities can issue certificates to users, devices and services. SMARTsend will not be able to function properly under SSL if the Host Name on the certificate does not match the fully qualified computer name, or if the certificate has expired.

### Configuring the SMARTsend Computer to Require HTTPS/SSL

► *To configure the SMARTsend computer to require HTTPS/SSL:*

- 1 Log in to the SMARTsend computer as an administrator.
- 2 Open the Internet Information Services Manager (**Start > Programs > Administrative Tools > Internet Services Manager**) and expand IIS in the tree view.
- 3 Right-click the **SMARTsend** web site and select **Properties**.
- 4 Select the **Directory Security** tab and select the **Edit...** button in the Secure Communications section.

- 5 Select the option for **Require secure channel (SSL)**.
- 6 Click **OK to exit all screens**.
- 7 Close the IIS management console window.
- 8 Restart the *FreeFlow SMARTsend Coordinator* service or reboot the computer to activate the changes.

# Site Security Policies

SMARTSend has site security policies that govern secure connection usage, scan time security, PaperWare form security, and workflow access. Each of these policies and their respective interactions will be described in detail in the following sections.

## General Site Security

Click the Review Security Settings link on the *Administration Home Page* to access the General Site Security policy. It is under the Security heading on the General Settings page.

The General Site Security Policy controls whether or not secure connections will be used when entering passwords from the SMARTsend web application. There are two SMARTsend options for General Site Security Policy:

- Enter passwords using a secure connection
- Enter passwords over a non-secure connection

The default and recommended setting is Enter passwords using a secure connection.

### Enter Passwords Using a Secure Connection

The secure password entry policy requires installation of a Secure Server Certificate on the SMARTsend computer. This is the recommended configuration. If a certificate is not available, you must install one on the SMARTsend computer when this option is selected. For instructions on how to obtain and install an SSL certificate for the SMARTsend computer, see *Obtain and Install a Security Certificate* on page 2-16.

This setting ensures privacy by using HTTPS to transfer data from any application pages that prompt for user passwords.

### Enter Passwords Over a Non-secure Connection

This policy is not recommended because passwords will be transmitted in clear text over your network. This leaves passwords vulnerable to a network sniffer. A server certificate is not required with this configuration.

## Troubleshooting

- If the Enter passwords using a secure connection policy is selected and a security certificate is not installed on the SMARTsend computer, the user will receive a 'Page Not Found' error whenever a page that requires password entry is launched. When this situation occurs, the administrator will receive a warning on the administration home page to indicate that a certificate is required but missing. To correct the problem, a certificate must be installed on the SMARTsend computer or the Enter passwords over a non-secure connection policy should be selected. It is recommended that the certificate be installed in this situation. Until the situation is rectified, device configuration will fail, managing the SMARTsend application account will fail, users will be unable to create workflows with destinations that require credentials and users will be unable to manage existing credentials.
- If the Enter passwords using a secure connection policy is chosen and the security certificate has expired, users will receive a warning each time a page that requires password entry is launched. They must choose to ignore the warning or the password entry pages will not launch. In this scenario, it is recommended that the administrator update the security certificate on the SMARTsend computer.
- In some cases, when the Enter passwords using a secure connection policy is chosen, users will be prompted to re-enter their SMARTsend computer credentials before an HTTPS page (used for password entry) is launched. When this scenario arises, users must enter the same credentials that they used to log in to SMARTsend. Otherwise, the HTTPS pages will not launch. If the user mistakenly enters different user credentials, they may need to clear their browser cache before attempting to launch the HTTPS page again.

## Device Scan Template Security

This policy determines whether user-specific authentication is required to submit a scan job. There are two SMARTsend options for the Device Scan Template Security Policy, Require authentication at the device for all templates, and Require authentication at the device for private templates only.

### Require Authentication at the Device For All Templates

When Require authentication at the device for all templates is selected, all device scan templates will require authentication before scanning can occur. This is the highest device scan template security setting. This option limits the user to Xerox Multifunction Devices that support authentication. Note that if a user attempts to scan over Internet Fax, scanning may not work. Please refer to the Security Policy Interactions section below for details.

### Require Authentication at the Device For Private Templates Only

The Require authentication at the device for private templates only option is the default. When this option is selected, only private workflows will require authentication at the device before a scan job is executed by SMARTsend.

For user authentication at a Xerox Multifunction Device to occur, the device must support authentication features and be configured to use them. The device must be configured to authenticate against the same Windows domain or trusted domain as the SMARTsend computer. When authentication is enabled and properly configured, users will be required to enter a domain user name and password at the device before processing a workflow publication.

To determine if your devices support authentication, consult the documentation associated with your Xerox Multifunction Devices.

## PaperWare Forms

### Professional Edition feature

A cover sheet is a type of PaperWare form. This policy determines whether a PaperWare cover sheet is considered a valid form of user authentication. There are two options for the PaperWare Form Security Policy, Allow authentication with PaperWare forms only, and Require PaperWare form and login at the device for authentication.

#### Allow authentication with PaperWare forms only

This is the default PaperWare Form Security Policy. Each PaperWare cover sheet has an owner specified in the top left corner of the cover sheet header. The owner is the SMARTsend user who created the PaperWare cover sheet by publishing the workflow. Using this option, the cover sheet owner's credentials will be used to authenticate the scan job submitter. With this policy set, private workflows can be published as PaperWare cover sheets and the owner specified in the cover sheet will be used to authenticate the scan job submitter. This allows for the use of private templates in environments that do not have Xerox Multifunction Devices with authentication enabled.

Note that if a user scans from a Xerox Multifunction Device that has authentication enabled, they will still be prompted to authenticate at the device. The credentials entered at the device will be used in place of the credentials on the cover sheet.

#### Require PaperWare form and login at the device for authentication

This policy option does not allow the owner specified on the PaperWare cover sheet to be used to authenticate the scan job submitter. This is the highest PaperWare Form Security Policy setting. If this policy option is selected, private workflows published as PaperWare cover sheets will require authentication at a Xerox Multifunction Device in order to identify the scan job submitter. Cover sheets created from private workflows will not work when scanning over Internet Fax, because the user will not be given the opportunity to authenticate. Refer to the Security Policy Interactions section below for details.

## Workflow Access Level Control

Workflows have two possible access levels, public and private. Public workflows are accessible by all users on the SMARTsend computer using the *View All Workflows* link on the user home page. Each user may edit or publish any public workflow on the SMARTsend computer. The workflow owner is the individual who created the workflow. Only the workflow owner may overwrite a public workflow. All other users may edit a public workflow, but will be required to save their changes as a new workflow.

Private workflows are accessible only by the owner of the workflow. They may only be viewed, published, and scanned by the workflow owner. For this reason, private workflows should only be published to Xerox Multifunction Devices that support authentication. They may also be published as PaperWare cover sheets and used on all devices depending on the *Device Scan Template Security* and *PaperWare Forms Security* Policy setting. Private workflows are recommended for when the user wants to control who can scan to their destinations. If someone other than the workflow owner attempts to scan using a private workflow, the job will fail.

The default workflow access may be set from the Review Workflow Defaults link on the *Administration Home Page*.

## Security Policy Interactions

Please set up your security policies based on the goals presented in the table below. The interactions between the policies are detailed in the table as well in the scenarios that follow. Each scenario contains recommendations for policy setup.

|   | Goal                                                                                                         | Template Security Policy                                          | PaperWare Forms Policy**                                          | Notes                                                                                                           |
|---|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| 1 | I only want users to have to login when absolutely necessary.                                                | Require authentication at the device for private templates only.* | Allow authentication with PaperWare forms only.                   |                                                                                                                 |
| 2 | I want to use non-Xerox equipment or Xerox Multifunction Devices that do not support network authentication. | Require authentication at the device for private templates only.  | Allow authentication with PaperWare forms only                    | Private workflows can only be published as PaperWare forms.                                                     |
| 3 | I want users to have to login at a Xerox Multifunction device to execute all private workflows.              | Require authentication at the device for private templates only.  | Require PaperWare form and login at the device for authentication | Private workflows only available from Xerox Devices that support network authentication.                        |
| 4 | I want users to have to login at a Xerox Multifunction device to execute all workflows                       | Require authentication at the device for all templates.           | Require PaperWare form and login at the device for authentication | All workflows unavailable from non-Xerox equipment or Xerox devices that do not support network authentication. |

**Table 9-1: Security Goals and Policies**

\* If a device has authentication enabled, it will require authentication regardless of the SMARTsend security policy.

\*\*Professional Edition feature.

## Scenarios

### Small Office

This configuration is appropriate for a small office environment where all network resources are located at the same physical location and the same logical TCP/IP subnet. The local network is assumed to be trusted or the sensitivity of the documents being scanned is low. There are a small number of trusted users in this scenario, so there is no need to create private workflows.

See item 2 in *Security Policy Interactions* on page 9-10.

#### Recommendations:

**General Site Security:** Using HTTPS to protect password entry is not required in this environment. Set the policy to 'Enter passwords over a non-secure connection' to avoid the overhead associated with certificate management.

**Device Scan Template Security:** Network authentication is not necessary or available in this scenario. Set the policy to 'Require authentication at the device for private templates only.'

**PaperWare Forms (Professional Edition feature):** A small office will often contain Internet Fax devices in addition to or instead of a Xerox Multifunction Device. Set the policy to 'Allow authentication with PaperWare forms only' to allow the use of Internet Fax devices.

## Secure Private Workflows

This configuration is appropriate for a medium sized office environment that is part of a corporate intranet. In this scenario, some public workflows are available scanning tasks that can be scanned either via PaperWare forms or from a Xerox Multifunction Device without network authentication. However, there is also a need to define a set of private workflows with stronger security requirements. These private workflows should only be scanned from a Xerox Multifunction Device that supports network authentication.

See item 3 in *Security Policy Interactions* on page 9-10.

### Recommendations:

**General Site Security:** HTTPS for protecting password entry is required in this environment. Set the policy to 'Enter passwords using a secure connection (recommended, requires a security certificate)' to ensure that HTTPS is used.

**Device Scan Template Security:** Set the policy to 'Require authentication at the device for private templates only' to only require network authentication for private workflows.

**PaperWare Forms:** Possession of the PaperWare form is not a strict enough authentication requirement in this scenario. Set the policy to 'Require PaperWare form and login at the device for authentication' to require that all users must successfully authenticate at a Xerox Multifunction Device to execute private workflows.

## Secure Workgroup

This configuration is appropriate for a medium sized office environment that is part of a corporate intranet. All network resources are members of a Windows domain are configured to require domain credentials for access. Network policies require strict auditing of network access, so Xerox Multifunction Devices configured for network authentication are used exclusively for scanning.

See item 4 in *Security Policy Interactions* on page 9-10.

### Recommendations:

**General Site Security:** HTTPS for protecting password entry is required in this environment. Set the policy to 'Enter passwords using a secure connection (recommended, requires a security certificate)' to ensure that HTTPS is used.

**Device Scan Template Security:** Set the policy to 'Require authentication at the device for all templates' to ensure that all users must successfully authenticate at a Xerox Multifunction Device to scan. This setting will also ensure that the submitter is always tracked in the job history log for auditing purposes.

**PaperWare Forms:** Possession of the PaperWare form is not a strict enough authentication requirement in this scenario. Set the policy to 'Require PaperWare form and login at the device for authentication' to require that all users must successfully authenticate at a Xerox Multifunction Device to scan.

# SMARTsend Authentication

SMARTsend uses various authentication mechanisms to allow access to the application and to ensure that information and options are only available to the appropriate individuals.

## Accessing SMARTsend

SMARTsend administrators and users are required to be authenticated with a valid Windows account to obtain access to the SMARTsend web application. Users must use their SMARTsend computer credentials to access the SMARTsend web site. Administration and user roles on the SMARTsend computer dictate roles on the SMARTsend web site. Access to the SMARTsend administration site will only be granted to accounts with administrative privileges on the SMARTsend computer.

If the SMARTsend computer is a member of a Windows domain, then Windows will automatically grant access to the SMARTsend web site to users who are members of the same domain. If the SMARTsend computer is not a domain member, accounts can be added individually using the Windows account creation tools in the Microsoft Management Console. Similarly, administrative rights can be granted using the same tools.

## SMARTsend Application Account

The SMARTsend application performs server side processing when users scan with a published SMARTsend workflow. This processing will execute under a special low privilege identity called the SMARTsend Application Account. The Application Account will be automatically created when SMARTsend is installed and will result in a local Windows user account named FF\_SMARTSEND\_USER. The password for the Application Account is also automatically generated with a 16 character randomly generated password that exceeds the default complexity requirements in all versions of Microsoft Windows. The name of the Application Account cannot be changed.

## Setting the Password for the Application Account

If your organization has extremely strict password requirements and the automatically generated password does not meet them or your organization policy requires that Administrators specify the passwords for all system accounts, the password for the FF\_SMARTSEND\_USER account can be manually changed.

**NOTE:** In order for SMARTsend to function properly, if the password for the FF\_SMARTSEND\_USER is changed by the Administrator, the new password must be created such that it complies with the effective security policy for the operating system being used.

### To set the password for the Application Account:



**CAUTION:** Do not delete the SMARTsend Application Account (FF\_SMARTSEND\_USER) from the Microsoft Management Console (MMC). If the account is deleted, the computer must be rebooted to re-establish the SMARTsend Application Account. All credentials on the SMARTsend web site will become invalid when the SMARTsend Application Account is deleted. Each user must go to Manage My Credentials from the user home page and re-enter all of their passwords. All jobs will fail until the computer has been restarted and the credentials have been re-entered.

- 1 Go to the Microsoft Management Console on the SMARTsend computer and update the password for the FF\_SMARTSEND\_USER account.

- 2 From the Administration Home Page, choose Manage Application Account.
- 3 Type the new password in the Manage Application Account Credentials dialog. It must match the one you entered in step 1.

**NOTE:** If the credentials for FF\_SMARTSEND\_USER are modified at the MMC, then the administrator must also update them at the SMARTsend computer using the Manage Application Account link on the Administration Home Page. All scan jobs will fail until this resynchronization occurs.

## SMARTsend Device Accounts

Xerox Multifunction Devices require a valid Windows account on the SMARTsend computer for authentication. The account enables each device to communicate with the SMARTsend computer, as needed, to exchange template information and other configuration data. See *Manage Device Accounts* on page 4-15 for additional information.



**CAUTION:** The SMARTsend device account should be a separate user account that is used exclusively for the Xerox Multifunction Devices that will be used with SMARTsend. Due to security issues, this account should not be a member of any group, and it should not be an administrator account. The Secure Password Entry features within SMARTsend encrypt password transmissions between clients and the SMARTsend computer. However, SMARTsend device account credentials may be transmitted between the SMARTsend computer and the devices using SNMP and clear text.

---

## Credentials

Credentials provide proof of identification which is used to acquire access to an application or service. For example, user name and password are often used for proof of identification. SMARTsend credentials are required for browsing and scanning to all supported destinations or search locations:

Users will be prompted to enter credentials at workflow creation time and workflow publication time if they are needed. The workflow owner's credentials are always used for filing to destinations. If a credential is removed from SMARTsend or becomes invalid because it is out of sync with the user name and password at the destination, scan job submission will fail. SMARTsend will attempt to detect this from the web site and prompt users accordingly. When credentials are missing or invalid, the workflow owner must update or re-enter them from the My Credentials link in the user home page.

The My Credentials panel on the User Home Page provides links for adding and managing individual user credentials.

- Add a New Credential is used to quickly create a new credential.
- Manage My Credentials is used to add, edit, or delete credentials.

**NOTE:** If user credentials change or expire within any account, the workflow owner will need to update the corresponding SMARTsend credentials using the Manage My Credentials option.

**Symbols**

\_MyHome 6-27

**A**

Access the Administration Home Page 4-2

Accessing SMARTsend 4-2

Accounts 9-12

Active Directory 6-11

Add/Update Xerox devices 4-8, 5-7

Adding and Discovering Devices 4-9

Adobe Acrobat Reader 2-25

ASP.NET 2-12

Authentication

    Access 9-12

    device 4-34

    Scenarios 9-10

authentication 6-2

Available Users list 6-6, 6-12

Available Users panel 6-6

**B**

Backup

    immediate 4-28

    scheduled 4-28

Backup Status 5-8

Browser configuration 2-25

**C**

Client configuration 2-25

Common Issues 7-4

Configuration

    E-mail Signature 4-25

    LDAP Server 4-26

    SMTP Server 4-25

Configuration Requirements for Optional Components 3-7

Configure Discovery Settings 4-10

Configure Discovery Settings - Subnets 4-17

Configure PaperWare Form Forwarding Settings 4-40

Configure the SMARTsend Computer 2-5

Configuring Device Properties 4-23

Configuring Xerox devices 4-8

Create User Folders 6-18

CSV file 6-2

Customer Support 1-8

**D**

Data Transfer Protocol 4-18

Data Transfer Protocols 2-29

Default Template Configuration 2-31

Delete all workflows not used or published since 5-5

Delete all workflows owned by 5-5

Deleting Devices 4-14

Destination Support

    Versions 4-29

Device

    Manage Accounts 5-6

Device Configuration

    Default Repository Settings 2-3

device job log 6-27

device scan template 6-27

Device Scan Template Security 9-7

Device Tasks 5-6

directory service mappings 6-2

Discover Now 4-9

document attribute field 6-2

document attribute profile 6-28

Document attributes

    configuring 4-38

Document Name 6-28

Document Type Properties 4-39

Documentation 1-6, 1-8

    Help 1-6

    Quick Reference cards 1-6

    readme.txt 1-7

    SMARTsend Installation and Administration Guide 1-6

Documentum Configuration Requirements 3-7

DocuShare access via http proxy servers 7-11

**E**

e-mail address 6-2

E-mail Signature Configuration 4-25

Enable ASP.NET 2-12

Enable Job Log Export Support 4-32

Enter Source Information dialog 6-6 to 6-7

Error handling

    configuring 4-35

Exceptions list

    Template Importer 8-7

**F**

FAQs 7-14

File formats supported

    Template Importer 8-4

Forwarding Protocol 4-40

Frequently Asked Questions 7-14

- FTP 4-18, 6-24
  - configuring in IIS 2-10
- FTP site 6-2
- G**
- General Site Security 4-5, 9-5
- Get Users 6-7
- H**
- Hide selected users from the Available Users list 6-13
- home scan destination 6-2
- HTTP 4-18
- HTTP/SSL Certificates 9-3
- HTTPS 4-18
- Hummingbird Configuration Requirements 3-9
- I**
- Import Users 6-21
- Installation and Administration Guide 1-6
- Installation Considerations 2-4
- Installation Procedures 3-5
- Installer Overview 3-2
- Installer Tasks 3-2
- Installing and Configuring Optional Components 3-7
- Internet Explorer 2-25
- Internet Information Services (IIS) 2-10
- Internet Information Services (IIS) requirements 2-5
- Internet Support 1-8
- Interwoven WorkSite Configuration Requirements 3-11
- J**
- Job Confirmation Page 7-3
- L**
- Language support
  - Template Importer 8-4
- LDAP Authentication 4-26
- LDAP directory service 6-7
- LDAP Mappings 6-11
- LDAP Property Mappings 4-26
- LDAP Server 4-26, 6-10
- LDAP Server Configuration 4-26
- list of users 6-2
- LiveLink Configuration Requirements 3-11
- M**
- Manage Device Accounts 5-6
- Manage Users 6-22, 6-28
- Manage Workflows 6-27
- Manage Workflows and Publications 5-3
- Managing Xerox Devices 5-6
- Manually Configure This Device 4-22
- Mappings button 6-7, 6-11
- Master Filing Credentials 6-24
- metadata 6-2
- Microsoft Active Directory 6-10
- Microsoft Active Directory Server 6-6
- Microsoft Active Directory server 6-7
- Migrating SMARTsend to a Replacement Computer 3-15
- Mozilla 2-25
- My E-Mail workflow publishing 4-27
- N**
- Netscape 2-25
- Network Configuration and Logistics 2-4
- Network Folder 6-24
- network folder 6-2
- No Document Profile 6-28
- O**
- OCR 6-17
- P**
- PaperWare Forms Security 9-8
- PaperWare Internet Fax Settings 4-24
- Popup blocking software 2-25
- Product Overview 1-5
- Proxy Server Settings 2-25
- Proxy server support for DocuShare 7-11
- Publication defaults
  - configuring 4-37
- Publish My E-mail Workflow 4-27
- Q**
- Quick Reference cards 1-6
- R**
- Readme.txt 1-7
- Repair a SMARTsend Installation 3-16
- Repair This Device Configuration 5-7
- Replacement Computer - Migration Instructions 3-15
- Requirements
  - SMARTsend utilities 8-2
  - Template Importer 8-4
- Review Security Settings 4-5

## **S**

- Scan Output Type 6-17
  - Scan to Home 6-1
  - Scan to Home Application 6-21
  - Scan to Home Utility 6-2, 6-6 to 6-8
    - installation 6-3
    - uninstalling 6-4
  - Secure Password Entry 9-3
  - Secure Web Site Configuration 9-3
  - Security
    - device authentication 4-34
    - device scan template 4-6
    - Device Scan Templates 9-7
    - PaperWare Forms 9-8
    - PaperWare forms 4-7
  - Security Overview 9-2
  - Security Policy Interactions 9-10
  - Selected Users List 6-12
    - Clearing 6-13
  - Selected Users list 6-6, 6-12 to 6-13, 6-18
  - Serial Number 1-8
  - Services
    - configuring 4-29
  - Settings, General 4-35
  - Show Users 6-8
  - Show Users button 6-11
  - Site Configuration 4-1
  - Site Management 5-1
  - Site Management Overview 5-2
  - Site Security - general 4-5
  - Site Security Policies 9-5
  - SMARTsend
    - accessing 4-2
    - common issues 7-4
    - Frequently Asked Questions 7-14
    - uninstalling 3-17
  - SMARTsend Authentication 9-12
  - SMARTsend Configuration 4-26
    - Add/Update Xerox devices 4-8
    - administrator contact information 4-35
    - backup 4-28
    - device scan template security 4-6
    - document type 4-38
    - error handling 4-35
    - immediate backup 4-28
    - My E-mail workflow 4-27
    - PaperWare forms security 4-7
    - PaperWare Internet Fax 4-24
    - publication defaults 4-37
    - scheduled backup 4-28
    - service settings 4-29
    - SMTP server 4-25
    - workflow defaults 4-36
  - SMARTsend Configuration Requirements 2-5
  - SMARTsend Documentation 1-6
    - Help 1-6
    - Installation and Administration Guide 1-6
    - Quick Reference cards 1-6
    - readme.txt 1-7
  - SMARTsend features 1-2
  - SMARTsend Installation and Administration Guide 1-6
  - SMARTsend Overview 1-5
  - SMARTsend proxy server support for DocuShare 7-11
  - SMARTsend Security 9-1
  - SMARTsend Serial Number 1-8
  - SMARTsend User Guide 1-6
  - SMARTsend Utilities
    - requirements 8-2
  - SMB 4-18
  - SMTP Server Configuration 4-25
  - SNMP Community Names 4-20
  - SNMP v2c Defaults 4-20
  - SNMP v3 Defaults 4-20
  - Sorting and Viewing Workflows 5-3
  - Subnets 4-10
  - System Error Logs 7-3
- ## **T**
- TCP/IP Port Configuration 2-29
  - Telephone Support 1-8
  - Template Importer
    - exceptions list 8-7
    - file format and language support 8-4
    - requirements 8-4
    - using 8-8
  - Template Name 6-28
  - Template Pool Settings 2-3
  - To upgrade and existing version of SMARTsend 3-4
  - Troubleshooting 7-2
  - TrueMatch Configuration Requirements 3-12
- ## **U**
- Uninstalling SMARTsend 3-17

Upgrade Eligibility 3-4  
Upgrade SMARTsend 3-3  
Upgrading SMARTsend 3-4  
User Authentication Settings 2-26  
User Properties dialog 6-13

## **V**

Versions Eligible for Upgrade 3-4  
View All Publications 6-27  
View All Workflows 6-27  
View Publications 6-27  
View Xerox Devices 5-6

## **W**

What's Included in This Release 1-2  
Windows Authentication Methods Configuration 2-11  
Windows NT Domain 6-6  
Windows NT Domain Source 6-11  
Workflow Access Level Control 9-9  
Workflow defaults  
    configuring 4-36  
Workflow Details 5-5  
Workflow Views 5-4  
Workflow/Publication Management Tasks  
    5-3

## **X**

Xerox Customer Support 1-8  
Xerox Internet Support 1-8  
Xerox Telephone Support 1-8