Authorized Send

Version 6.4

Configuration Guide

11005-64-UD3-001

This page is intentionally left blank.

Contents

Preface 7

How to Use This Manual 7
Symbols Used in This Manual 7
Keys and Buttons Used in This Manual 8
Displays Used in This Manual 9
Abbreviations and Terms Used in This Manual 10
Hyperlinks 11
Legal Notices 12
Trademarks 12
Copyright 12
Disclaimers 12

Chapter 1 Introduction 13

1.1 Overview of Authorized Send 13
1.2 System Requirements 14
1.2.1 Operating Environment 14
1.2.2 Hardware Requirements 14
1.2.3 Server Requirements 15
1.2.4 Software Requirements 16
1.2.5 Home Directory Requirements 16
1.2.6 RightFax Requirements 17
1.2.7 Distributed File System Requirements 18
1.2.8 Communication Interfaces 19
1.2.9 Supported Authentication Protocols 20
1.2.10 MEAP Application Coexistence Support 20
1.3 Communication Environment 21
1.3.1 Communication Diagrams 27
1.3.1.1 Authentication Communication Diagrams 27
1.3.1.2 Address Book Communication Diagrams 30

Chapter 2 Configuring Authorized Send 31

2.1 Logging On to Authorized Send 32
2.2 Creating an Authentication Server 34
2.3 Editing an Authentication Server 59
2.3.1 Changing the Display Order of the Authentication Servers 62
2.4 Deleting an Authentication Server 65
2.5 Configuring the E-Mail Service Settings 67
2.5.1 Creating an Address Book Server 70
2.5.2 Editing an Address Book Server 97
2.5.3 Deleting an Address Book Server 99
2.6 Configuring the Scan to E-Mail Settings 101

2.7 Configuring the Scan to Folder Settings 108
2.7.1 Creating a Preset Share 115
2.7.2 Editing a Preset Share 120
2.7.3 Deleting a Preset Share 122
2.8 Configuring the Scan to Fax Settings 124
2.8.1 Creating a Fax Address Book 128
2.9 Configuring the Scan to I-Fax Settings 141
2.9.1 Creating an I-Fax Address Book 150
2.10 Configuring the Scan to RightFax Settings 164
2.10.1 Creating a Scan to RightFax Address Book 171
2.11 Configuring the Scan to Fax2Mail Settings 188
2.11.1 Creating a Fax2Mail Address Book 194
2.12 Configuring the Fax Forwarding Settings 211
2.12.1 Preparing Fax Forwarding with Advanced Box 211
2.12.1.1 Creating a New Advanced Box Folder 212
2.12.1.2 Configuring the Address Book Destination 217
2.12.1.3 Configuring the Forwarding and Network Settings 224
2.12.2 Preparing Fax Forwarding with FTP Server 231
2.12.2.1 FTP Print Settings 231
2.12.2.2 Configuring the Address Book Destination 234
2.12.2.3 Configuring the Forwarding Settings 241
2.12.3 Configuring the Authorized Send Servlet 245
2.12.3.1 Creating a Fax Forwarding Setting 245
2.12.3.2 Editing a Fax Forwarding Setting 253
2.12.3.3 Deleting a Fax Forwarding Setting 255
2.12.3.4 Configuring the General Settings 257
2.13 Configuring the Scan to FTP Settings 261
2.13.1 Creating an FTP Preset Server 267
2.13.2 Editing an FTP Preset Server 272
2.13.3 Deleting an FTP Preset Server 274
2.14 Configuring the Scan to SharePoint Settings 276
2.14.1 Creating a Preset SharePoint 282
2.14.2 Editing a Preset SharePoint 287
2.14.3 Deleting a Preset SharePoint 289
2.15 Configuring the Scan to Box Settings 291
2.15.1 Creating a Preset Box Path 298
2.15.2 Editing a Preset Box Path 303
2.15.3 Deleting a Preset Box Path 305
2.16 Configuring the Scan to Google Drive Settings 307
2.16.1 Creating a Preset Google Drive Path 314
2.16.2 Editing a Preset Google Drive Path 319
2.16.3 Deleting a Preset Google Drive File Path 321
2.17 Configuring the Scan to Multi-Destinations 323

2.18 Configuring the One-Touch Buttons Settings 328
2.18.1 Creating a Server Profile 334
2.18.2 Editing a Server Profile 344
2.18.3 Deleting a Server Profile 346
2.18.4 Creating a Shared Button Definition 348
2.18.5 Editing a Button Definition 380
2.18.6 Deleting a Button Definition 383
2.19 Configuring the Feature Controls 385
2.20 Configuring the Scan Settings 388
2.20.1 Creating a Scan Setting Profile 388
2.20.2 Editing a Scan Setting Profile 399
2.20.3 Deleting a Scan Setting Profile 401
2.20.4 Customizing Display of Paper Sizes 403
2.21 Configuring the File Name Template 407
2.21.1 Editing a File Name Template 413
2.21.2 Deleting a File Name Template 416
2.22 Configuring a Barcode Policy 419
2.23 Configuring the Metadata Index Settings 423
2.23.1 Creating a Metadata XML File Template 430
2.23.2 Editing a Metadata XML File Template 438
2.23.3 Deleting a Metadata XML File Template 440
2.24 Configuring the Options Settings 442
2.25 Configuring the Logs and Reports Settings 451
2.25.1 Configuring the Logging Settings 451
2.25.2 Configuring the Reporting Settings 458
2.26 Configuring the Configuration Management Settings 464
2.27 Configuring the Disclaimer 493
2.28 Viewing the Version Number 496
2.29 Changing the Login ID and Password 498
2.30 Logging Off Authorized Send 500
2.31 Using the Brand Configuration Tool (Optional) 501

Chapter 3 Configuring the MEAP Device 511

3.1 DNS Server Settings 511
3.2 Automatically Logging Off 515
3.3 Synchronizing the Device and Server Time 518
3.3.1 Automatic Time Synchronization 518
3.3.2 Adjusting the Device Time 523

Chapter 4 Appendix: Configuring Authorized Send with Trusted Login Managers 527

4.1 Universal Login Manager 527

This page is intentionally left blank.

Preface

Thank you for purchasing the Authorized Send V6.4 application. Please read this manual thoroughly before operating the product on your MEAP-enabled machine to familiarize yourself with its capabilities, and to make the most of its many functions. After reading this manual, store it in a safe place for future reference.

How to Use This Manual

This manual assumes that the reader has a good understanding of MEAP (Multifunctional Embedded Application Platform) and Canon imageRUNNER ADVANCE machines.

This manual does not provide instructions for using or installing the Authorized Send application. For instructions on using the Authorized Send application, see the *Authorized Send Version 6.4 User's Guide.* For instructions on installing the Authorized Send application, see the *Authorized Send Version 6.4 Installation Guide.*

Symbols Used in This Manual

The following symbols are used in this manual to explain procedures, restrictions, and instructions that should be observed for safety.

IMPORTANT	Indicates operational requirements and restrictions. Be sure to read these items carefully to operate the machine correctly, and avoid damaging the machine.
NOTE	Indicates a clarification of an operation, or contains additional explanations for a procedure. Reading these notes is highly recommended.

Keys and Buttons Used in This Manual

The following key and button names are a few examples of how keys and buttons to be pressed and clicked are represented in this manual:

Touch Panel Display Keys:	[Key Name]
Examples:	[Scan] [Cancel]
Control Panel Keys:	Key Icon (Key Name)
Examples:	⊙ (Start) (Stop)
Buttons on Computer Operations Screens:	[Button Name]
Examples:	[Scan to E-Mail] [Save]

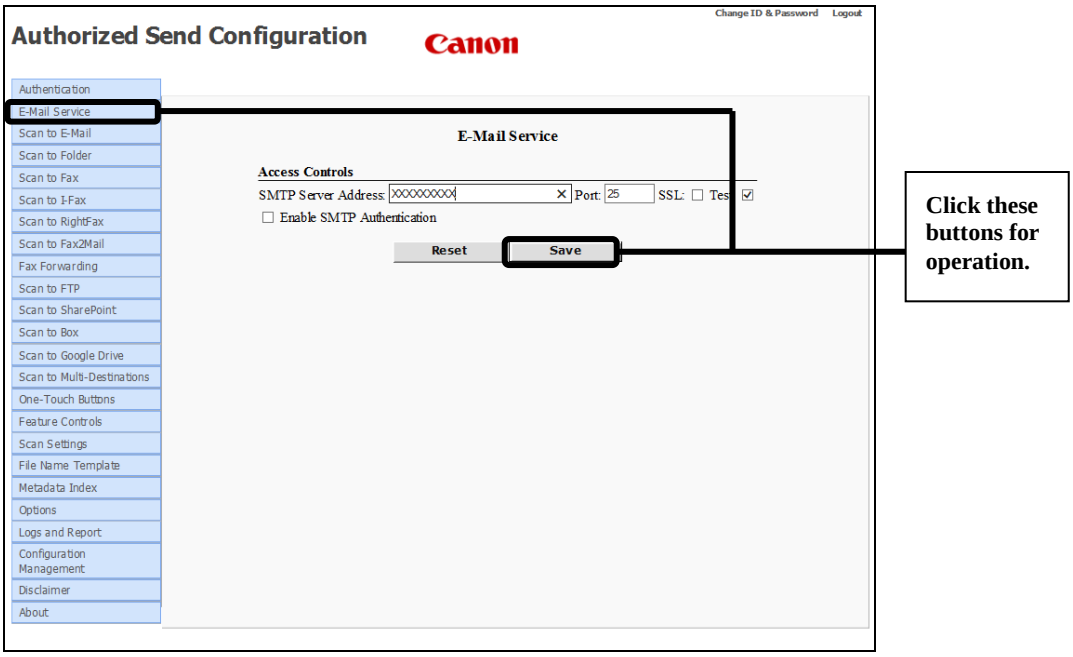
Displays Used in This Manual

Screen shots used in this manual are those taken when Authorized Send is being installed using MEAP SMS (Service Management Service), and when Authorized Send is running on the various imageRUNNER ADVANCE devices.

The keys/buttons you should select or click are marked with a circle, as shown below. When multiple keys/buttons can be selected on the screen, all keys/buttons are circled.

Example:

1. Click [E-Mail Service] ➞ [Save].



NOTE

Some operating systems and browsers may exhibit different displays and behaviors.

Abbreviations and Terms Used in This Manual

The following abbreviations are used in this manual.

Abbreviation	Definition
AD	Active Directory
AMS	Access Management System
DFS	Distributed File System
DN	Distinguished Name
DNS	Domain Name Service
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
FTPS	File Transfer Protocol over SSL
GIF	Graphics Interchange Format
HID	Human Interface Device
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
JPEG	Joint Photographic Experts Group
KDC	Key Distribution Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MEAP	Multifunctional Embedded Application Platform
MEAP device	Supported Canon imageRUNNER ADVANCE multifunctional machine that features embedded MEAP technology.
NTLM	NT LAN Manager
NTLMSSP	NT LAN Manager Security Support Provider
OCR	Optical Character Recognition
PDF	Portable Document Format
PNG	Portable Network Graphics
PPT	PowerPoint
Printable ASCII	These characters are from ‘ ’ (space) up to and including ‘~’ (tilde) on the ASCII table (the decimal values for the characters, x , are: 32 (space) ≤ x ≤ 126 (tilde)).
RGB	Red Green Blue
SCMS	Shared Credentials Management Service enables MEAP applications to register and view shared credentials.
S-FTP	SSH (Secure Shell) File Transfer Protocol
SMB	Server Message Block
SMS	Service Management Service
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer

Abbreviations and Terms Used in This Manual Table Continued

Abbreviation	Definition
String	A set of consecutive characters that the user is able to input into a text box. If input into a text box is required, a string that consists of all spaces is not valid.
TIFF	Tagged Image File Format
TLS	Transport Layer Security
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
XML	Extensible Markup Language
XPS	XML Paper Specification

Hyperlinks

When this manual is in its native PDF form, the blue underlined text represents a hyperlink to the corresponding sections of this manual or to external Web sites.

For example: See Chapter 1, “Introduction,” on p. 13.

Likewise, all entries in the Table of Contents are hyperlinks.

Legal Notices

Trademarks

Canon, the Canon logo, imageRUNNER ADVANCE, and MEAP are registered trademarks, and the MEAP logo is a trademark, of Canon Inc. in the United States and may also be a trademark or registered trademark in other countries.

Adobe and Adobe Acrobat are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, Windows Server, Office 365, and Internet Explorer are registered trademarks of Microsoft Corporation in the United States and are trademarks or registered trademarks of Microsoft Corporation in other countries.

Java and all Java-based trademarks and logos are the trademarks or registered trademarks of Oracle Corporation in the United States or other countries.

Google is a trademark of Google, Inc.

Other product and company names herein are, or may be, the trademarks of their respective owners.

Copyright

Copyright 2018 by Canon U.S.A., Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system without the prior written permission of Canon U.S.A., Inc.

Disclaimers

The information in this document is subject to change without notice.

CANON U.S.A., INC. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, EITHER EXPRESS OR IMPLIED, EXCEPT AS PROVIDED HEREIN, INCLUDING WITHOUT LIMITATION, THEREOF, WARRANTIES AS TO MARKETABILITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE OR NON-INFRINGEMENT. CANON U.S.A., INC. SHALL NOT BE LIABLE FOR ANY DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY NATURE, OR LOSSES OR EXPENSES RESULTING FROM THE USE OF THIS MATERIAL.

Chapter 1 Introduction

This chapter describes the overview of the Authorized Send application, the system requirements for installing, configuring, and operating the software and application, and the component functional requirements.

1.1 Overview of Authorized Send

Authorized Send is a customized MEAP application. It should be installed and operated on a Canon MEAP-enabled device, and provides authenticated scan to e-mail, scan to fax, and scan to folder functionalities. Authorized Send does not require the user to be authenticated to use the native functions of the machine, such as Copy, Print, and Scan, and does not interfere with any of these functions.

MEAP is a software platform embedded in a MEAP device that enables the development of custom applications, which run alongside native functions, such as Copy, Print, and Scan.

MEAP, developed by Canon, is based on Oracle's Java technology.

Authorized Send 6.4 is designed to perform the following new functions once configured from the Authorized Send Configuration servlet:

- Administrators can set the machine to display a disclaimer screen (which must be acknowledged to continue) before the user can log on to Authorized Send and after a user logs off of Authorized Send.
- A disclaimer message can be automatically appended to the body of all Scan to E-Mail jobs, including jobs started with the One-Touch Buttons.

IMPORTANT

- System Administrator knowledge of Microsoft Windows and Canon MEAP-enabled devices is necessary to install and configure the Authorized Send application.
- For instructions on using Authorized Send, see the *Authorized Send Version 6.4 User's Guide.*
- You can only encrypt a PDF document if the machine supports the Encrypted PDF mode. Contact the System Administrator for more information.

1.2 System Requirements

Authorized Send requires the proper installation and configuration of all items documented in this guide. Failure to correctly install or configure the software and application may affect its operation.

If Authorized Send is not working properly, the problem can likely be traced to an installation or configuration issue. Please consult the appropriate guides (including the *Authorized Send Version 6.4 Troubleshooting Guide*) before contacting Canon U.S.A.'s e-Support.

1.2.1 Operating Environment

To send an e-mail message, an Exchange Server is required.

1.2.2 Hardware Requirements

Authorized Send requires a Canon imageRUNNER ADVANCE device running the latest released firmware version, and the Canon imagePRESS C700 and C750 running the latest released firmware version. However, Canon devices that use a PRISMAsync controller are not supported.

The Scan to Fax function is not supported on these devices:

- imageRUNNER ADVANCE C2030/C2020
- imageRUNNER ADVANCE 500iF/400iF
- imageRUNNER ADVANCE C350iF/C250iF
- imageRUNNER ADVANCE C355iF/C255iF
- imageRUNNER ADVANCE C356iF II/C256iF II
- imageRUNNER ADVANCE 715iF II/715iFZ II/615iF II/615iFZ II/ 525iF II/525iFZ II

Optional Hardware Device

USB Keyboard: Model: Cherry G84 Vendor ID: 0x046A

IMPORTANT

- MEAP Settings and Use HTTP settings (from the Additional Functions or Settings/Registration screen) on the MEAP device must be enabled. (See the *Reference Guide* or the appropriate e-Manual that came with your machine.)
- Access to System Manager Settings (from the Additional Functions screen) or access to the Management mode (from the Settings/Registration screen) on the MEAP device is necessary.
- There must be network connectivity between the MEAP device, Active Directory servers, an e-mail server, and shared file servers.

1.2.3 Server Requirements

Authorized Send communicates with the following servers:

- Supported authentication servers:
  - Windows 2000 SP4/2003 SP2/2008 Standard SP2/2008 R2/2012/2012 R2 Active Directory
  - Lotus Domino Version 7
  - Novell NetWare 6.5 and eDirectory 8.7 SP2
  - Google
  - Office 365
- Supported address book servers:
  - Windows 2000 SP4/2003 SP2/2008 Standard SP2/2008 R2/2012/2012 R2 Active Directory
  - Lotus Domino Version 7
  - Novell NetWare 6.5 and eDirectory 8.7 SP2
- Supported name servers:
  - Windows 2000 SP4/2003 SP2/2008 Standard SP2/2008 R2/2012/2012 R2 DNS server
- Supported Scan to E-Mail servers:
  - Microsoft Exchange Server 2000/2003/2007/2010 SP1/2013
  - Gmail
  - Office 365
- Supported Scan to Network Share servers:
  - Local Share:
    Windows Vista SP1/XP SP2/2000 SP4/2003 SP2/2008 Standard SP2/2008 R2/2012/2012 R2/Advanced Box on imageRUNNER ADVANCE MEAP devices (NTLM V2)
  - Domain Share:
    Windows Vista SP1/XP SP2/2000 SP4/2003 SP2/2008 Standard SP2//2008 R2/2012/2012 R2
  - Windows DFS Share:
    Windows Vista SP1/XP SP2/2000 SP4/2003 SP2/2008 Standard SP2/2008 R2/2012/2012 R2
- Supported SharePoint servers:
  - 2007, 2010, 2013, and 2016
- The following I-Fax servers have been tested:
  - Relay Fax 6.7 by ALT-N Technologies
    (For the Scan to I-Fax function to work successfully with Relay Fax, each fax number used must have a corresponding e-mail address.)
- Supported FTP Servers
  - Red Hat Fedora Core 9 – VSFTP 2.0.6-4fc9 or later
  - Open SSH4.7 or later

1.2.4 Software Requirements

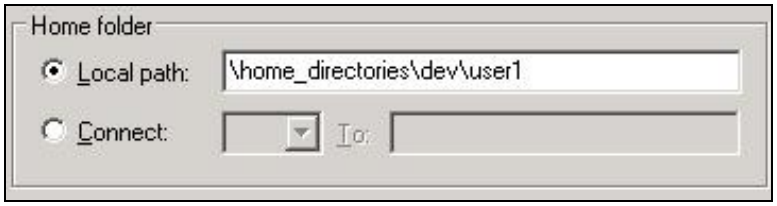
- Internet Explorer 6.0 or later, with JavaScript enabled, must be installed and configured prior to installing the Authorized Send application.
- KDC is necessary for Kerberos authentication.

1.2.5 Home Directory Requirements

If the System Administrator wants to configure the Retrieve Home Directory (Active Directory only) feature, the following three types of configurations are supported.

■ **Local Share**

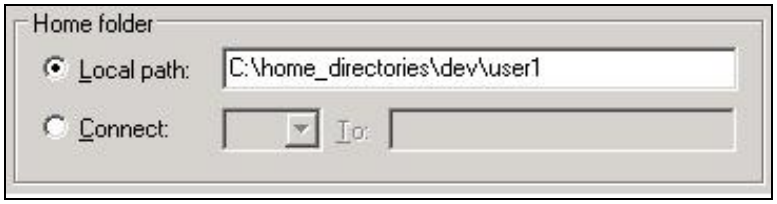
This configuration illustrates when the home directory exists on the authentication server as a local share. No text manipulation is required, and the value entered is used exactly as is.



Home Directory as a Local Share

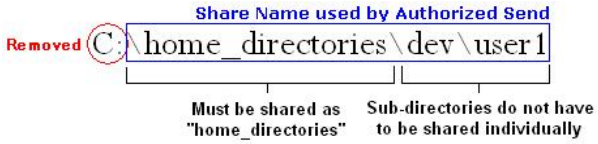
■ **Local Path**

This configuration illustrates when the home directory exists on the authentication server as a local folder.



Home Directory as a Local Path

When the home directory exists on the authentication server as a local folder, it is impossible for Authorized Send to use the text as it is. Therefore, some text manipulation is required. In this case, Authorized Send removes the leading drive letter (in this case, “C:”), and then the rest of the text is treated as a local share. In this example, “home_directories” must be a valid share name.



- **Mapped Share**

  This configuration illustrates when the home directory exists as a mapped share. In this example, “fileserver” is used as the host name of the file server, and “\home\dev\user1” is used as the share’s file path.

Home Directory as a Mapped Share

1.2.6 RightFax Requirements

The following versions of RightFax are supported:

- RightFax V16 EP2 SR2 (Enhancement Pack EP2 Service Release 2) and later
- RightFax V10.6 FP3 (Feature Pack 3) and later

1.2.7 Distributed File System Requirements

Authorized Send supports the following two DFS roots.

- **Standalone DFS root**
- **Domain-based DFS root**

  Successful domain-based DFS root support for Authorized Send requires that certain configuration settings be implemented and understood.

  1. Users can only access the domain-based DFS roots that belong to the domain against which they were authenticated.

  2. The authentication server created with Authorized Send's Configuration servlet must have the Domain Name configured to match the FQDN.

  IMPORTANT
  If the authentication server is configured with a NetBIOS domain name, access is granted to the application; however, you may not have access to any domain-based DFS roots.

  3. Browsing for domain-based DFS roots are not supported. A preset share or home directory must be configured, or be manually entered in the share location.

  IMPORTANT
  If you configure a preset share for a domain-based DFS root, the file server must be configured with the FQDN of the Domain (i.e., If the domain name is "MyCompany.com," then the file server must be configured with the FQDN "MyCompany.com." The FQDN is not case-sensitive.). This results in the domain-based DFS root's preset share on the file server matching the authentication server's domain name.

  4. The first successful DFS target is used; otherwise, the user cannot scan to the DFS root.

  IMPORTANT
  DFS share clustered file servers are supported.

1.2.8 Communication Interfaces

The table below shows the different communication interfaces, their specific port numbers, and descriptions used with Authorized Send.

Communication Interface	Port	Description
USB	—	Used to communicate with USB keyboards.
NTLM	Determined by AD server	Used for authentication.
Kerberos	TCP/UDP Port 88	Used for authentication.
LDAP	TCP Port 389	Used to retrieve e-mail addresses.
SMB	TCP Port 139/445	Used for the Scan to Folder function.
SMTP	TCP Port 25	Used to communicate with an e-mail server and the Scan to E-Mail function.
	TCP Port 465	Used for the Gmail server address.
	TCP Port 587	Used for the Office 365 server addresses.
HTTP	TCP Port 80/8000	Used to access the Authorized Send Configuration servlet and the administration Web page.
HTTPS	TCP Port 443/ 8443	Used to access the secure Configuration servlet and the secure administration Web page.
LDAP over SSL	TCP Port 636	Used to communicate with the LDAP server.
Syslog	UDP Port 514	Used to communicate with the syslog server.
FTP/FTPS	TCP Port 21	Used for the Scan to FTP function.
SFTP	TCP Port 22	Used for the Scan to S-FTP function.
IMAP	TCP Port 143	Used to send e-mail messages to the Sent folder on an Exchange Server.
DNS	TCP Port 53	Used to communicate with the Domain Name Server
SNMP	TCP Port 161	User to communicate using Simple Network Management Protocol.
Any TCP port set up by the user for the Scan to SharePoint's URL parameter.		
IMAP SSL	TCP Port 993	Used to send e-mail messages to the Sent folder on an Exchange Server.

1.2.9 Supported Authentication Protocols

Kerberos and NTLM are the supported protocols when communicating with a Microsoft Active Directory server.

SMTP over SSL (SMTPS) is the supported protocol when communicating with Google Gmail and Microsoft Office 365 servers.

Simple Binding is the supported protocol when communicating with Novell eDirectory and Lotus Domino.

Anonymous Binding is the protocol reserved for communication with any of the supported address book servers (when applicable).

IMPORTANT

If Simple is selected as the authentication method and Novell eDirectory is the targeted authentication server, set the following settings on the eDirectory server:

- Disable “Require TLS for Simple Binds with Password” for the LDAP Group.
- Disable “Require TLS for all operations” for the LDAP Server in the Connections section.
- In the Restrictions section, select [Use Low Cipher (56 or 64-bit)].

1.2.10 MEAP Application Coexistence Support

Authorized Send and the optional Barcode Feature Activation can coexist with other installed MEAP applications that have received verification by Canon U.S.A., Inc., provided that there are sufficient resources available on the MEAP device.

The following table shows the maximum values for MEAP resources that Authorized Send and Barcode Feature Activation could use in a MEAP device.

MEAP Device Resource Requirements	Maximum Resources	
	Authorized Send	Barcode Feature
File space usage	140,000 KB	100 KB
Memory usage	20,000 KB	30,000 KB
File descriptor usage	26	2
Socket usage	16	1
Thread usage	50	2

1.3 Communication Environment

Authorized Send must be installed on a MEAP-enabled device. There must be network connectivity between the MEAP device, DNS, authentication servers, address book servers, SMTP server, and shared file servers.

It is necessary to configure Authorized Send to communicate with the authentication servers and address book servers.

The following table lists the supported authentication servers and authentication methods.

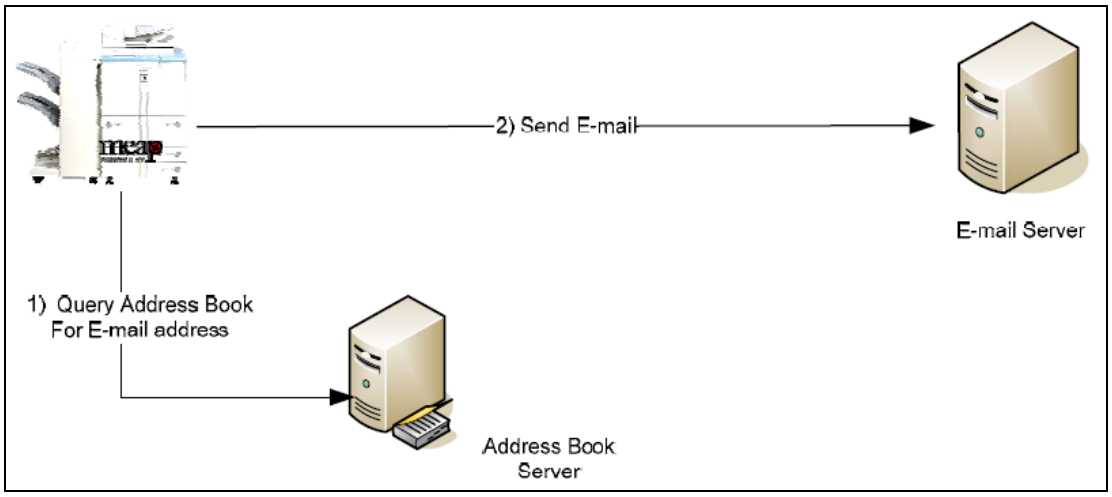
Supported Authentication Servers	Authentication Methods
Windows Active Directory	NTLM, Kerberos (with or without SSL)
Novell NetWare 6.5/eDirectory 8.7 SP2	Simple LDAP (with or without SSL)
Lotus Domino v7	Simple LDAP (with or without SSL)
smtp.gmail.com	SMTP over SSL (SMTPS)
smtp.office365.com	SMTP over SSL (SMTPS)

The following table lists the supported address book servers and binding methods.

Supported Address Book Servers	Binding Methods
Windows Active Directory	NTLM, Kerberos (with or without SSL)
Novell NetWare 6.5/eDirectory 8.7 SP2	Simple LDAP (with or without SSL)
Lotus Domino v7	Simple LDAP (with or without SSL)

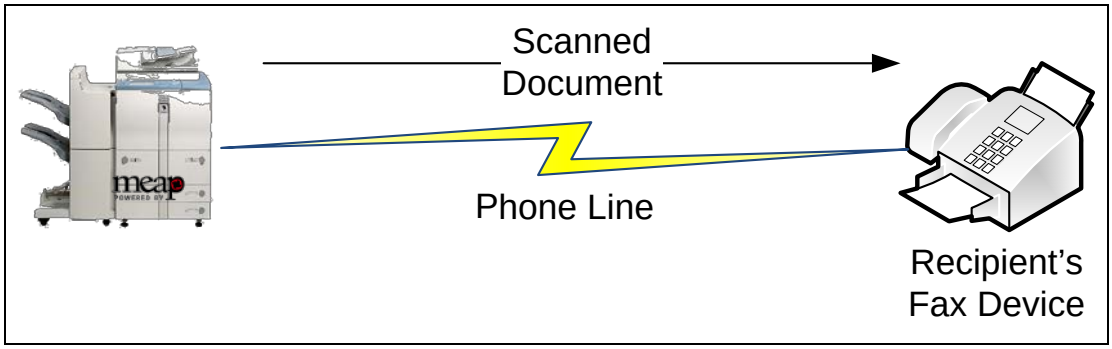
The following illustrations represent a flow of operations for the Scan to E-Mail, Scan to Fax, Scan to I-Fax, Scan to Folder, Scan to FTP, and Scan to SharePoint functions of the Authorized Send application.

Scan to E-Mail



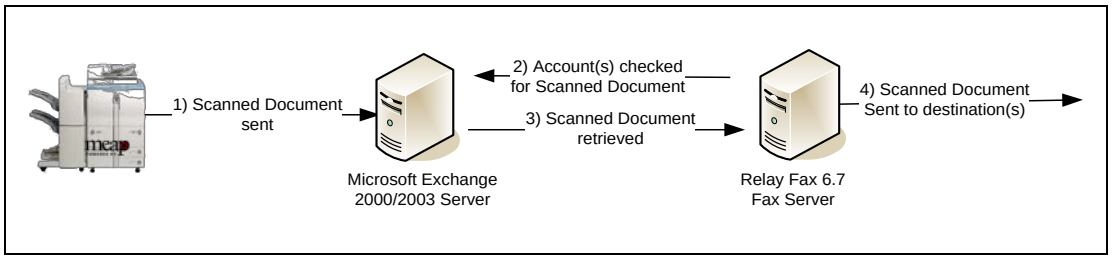
1. The user makes an address book query from the Scan to E-Mail function on the MEAP machine. The machine sends an LDAP query to the address book server to retrieve the desired list of e-mail addresses.
2. Once all e-mail addresses are verified and selected, the machine sends the e-mail message to the E-mail or SMTP server.

Scan to Fax



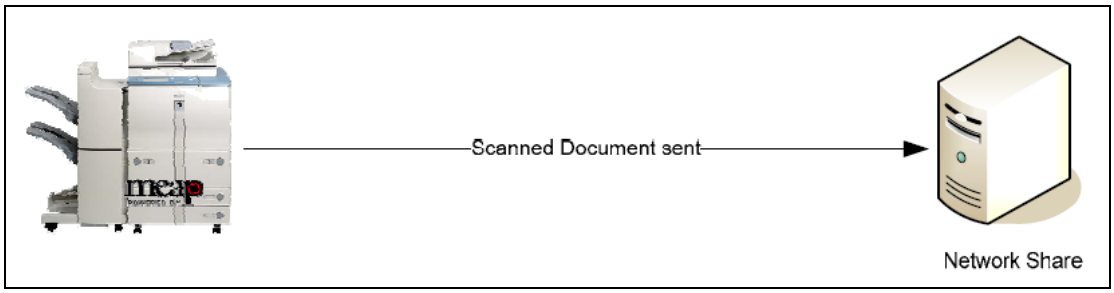
1. The user manually inputs the recipient's fax number or selects it from the address book.
2. The machine sends the scanned document to the recipient's fax device.

Scan to I-Fax



1. The user manually inputs the recipient's fax number or selects it from the address book.
2. The machine sends the scanned document to the SMTP server.
3. The SMTP server sends the scanned document to the fax server.
4. The fax server sends the scanned document to the destination.

Scan to Folder

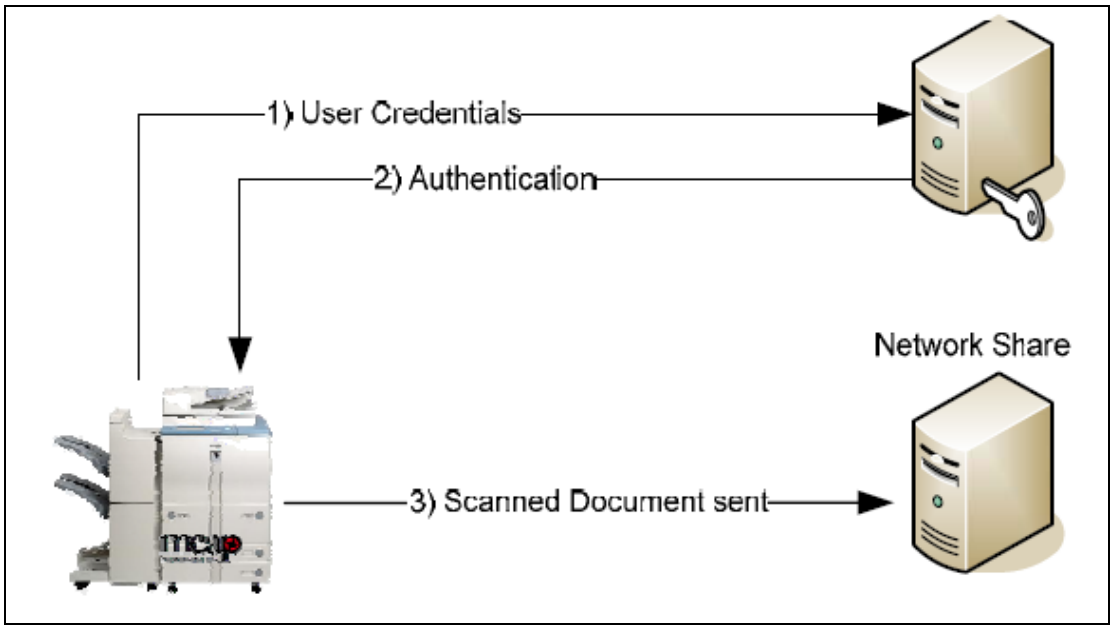


1. The user browses for the desired folder on the file server directly from the machine.
2. Once the directory is found and selected, the machine sends the file to the designated location on the file server.

NOTE

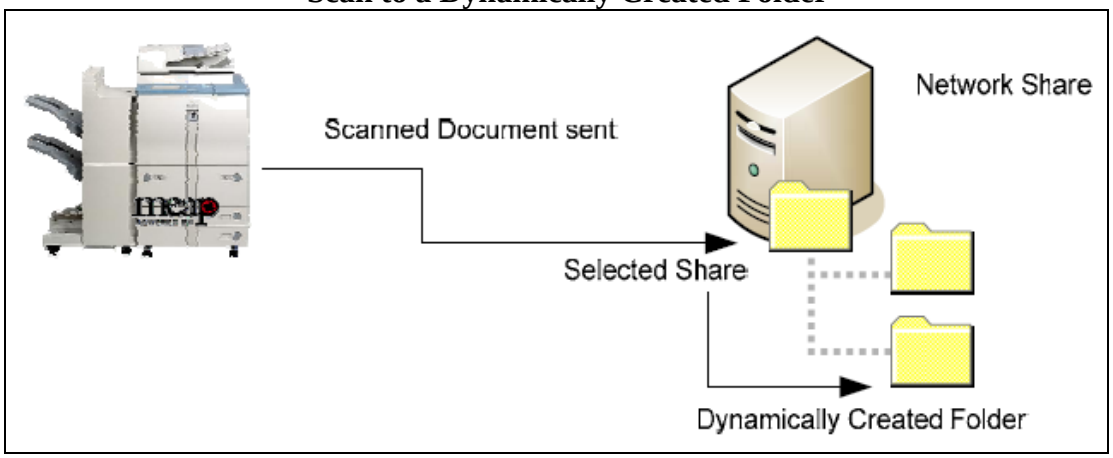
When a user accesses a network share, they are authenticated against that share using their credentials. If they do not have access rights to that share, they are prompted to enter a user name and password.

Scan to Folder with NTLM Authentication



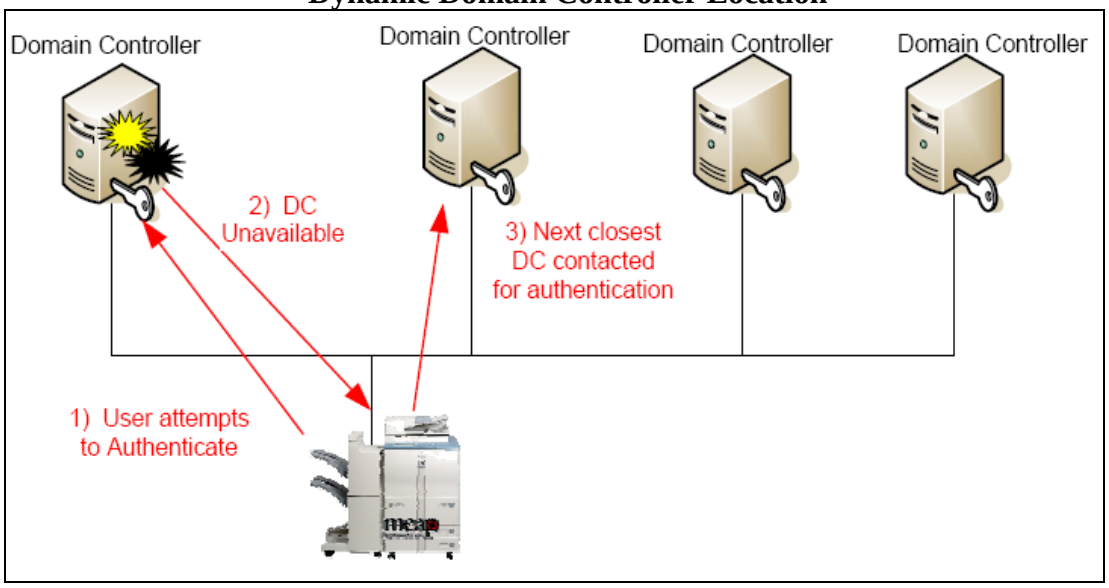
1. The user logs on to the machine using one of the authentication methods.
2. The user browses and enters their credentials to gain access to a network shared folder using NTLM as the authentication method.
3. Once access is granted, the scanned document is stored in the selected folder.

Scan to a Dynamically Created Folder



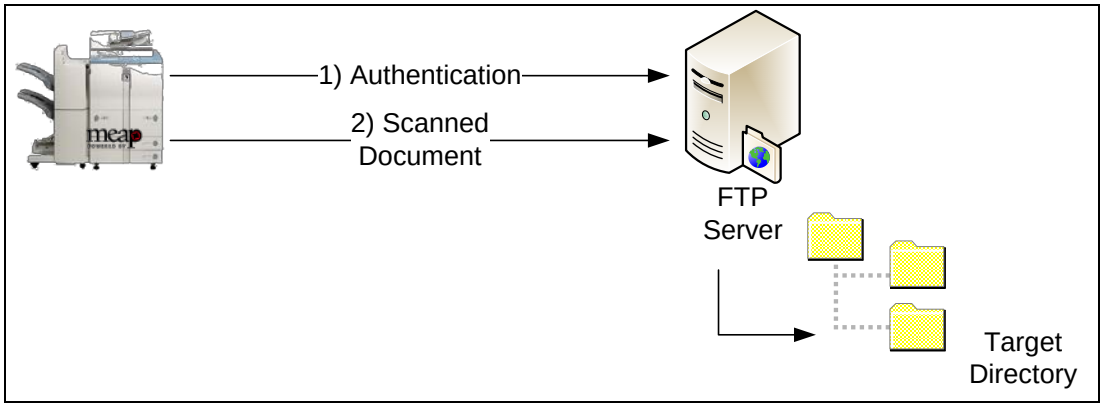
1. The authenticated user selects a folder, enters a document name, and scans the document.
2. The scanned document is automatically stored in a sub-folder (that was dynamically created) of the selected folder.

Dynamic Domain Controller Location



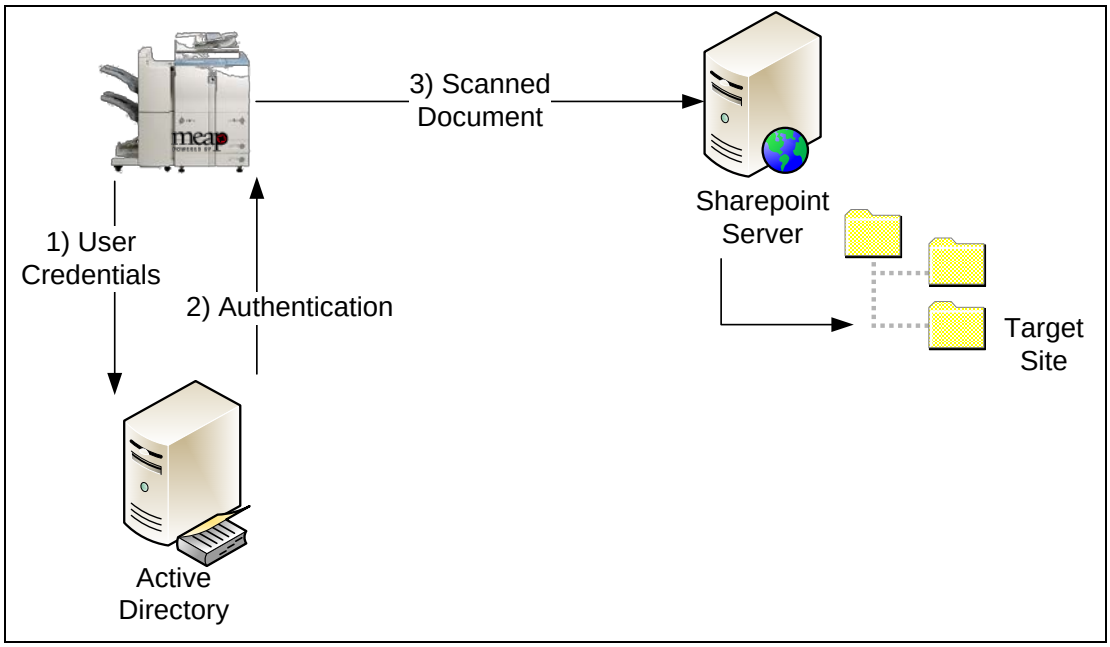
1. The user tries to log on to the machine using one of the authentication methods.
2. The system is unable to contact the authentication server previously cached.
3. The system locates the next closest available domain controller.
4. Authentication or address book lookup is performed by the new domain controller.
5. The new domain controller is cached.

Scan to FTP



1. The user tries to log on to the FTP server using FTP/S-FTP (not encrypted/encrypted) as one of the authentication methods.
2. The scanned document is stored in the selected folder on the FTP server.

Scan to SharePoint



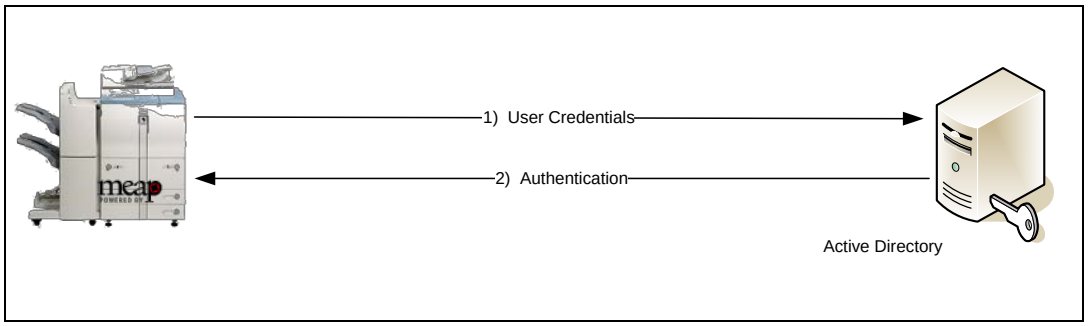
1. The user tries to log on to the SharePoint server.
2. The system authenticates the user via active directory.
3. The scanned document is stored in the selected folder on the SharePoint server.

1.3.1 Communication Diagrams

This section shows the flow of communication protocols based on the authentication method that you select. You can configure up to 10 authentication servers.

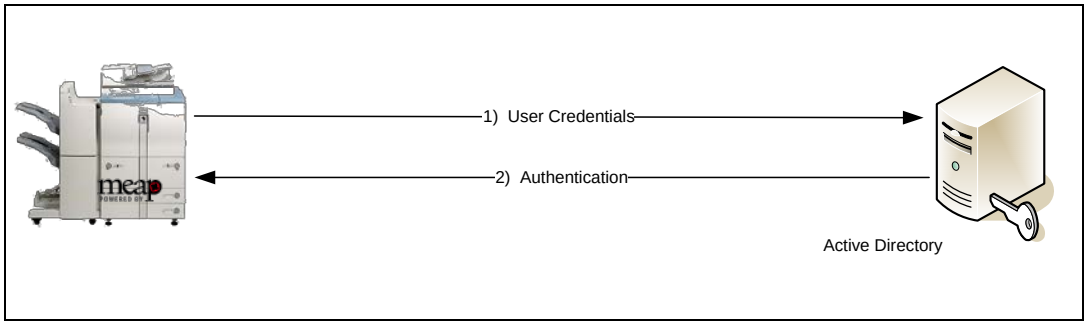
1.3.1.1 Authentication Communication Diagrams

Kerberos Authentication



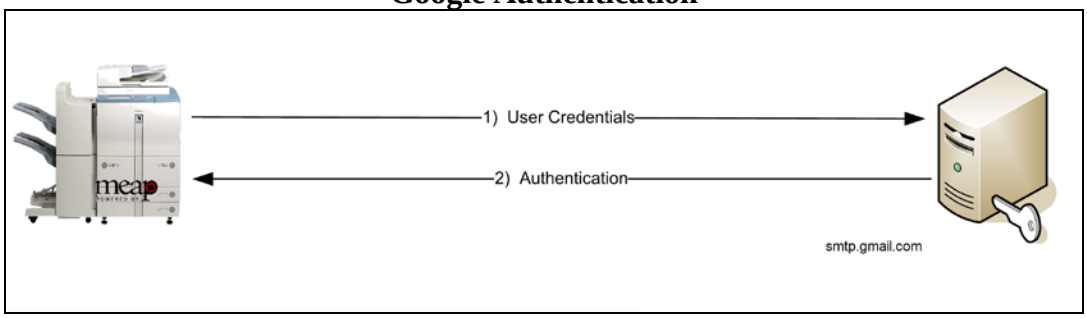
Communication Protocol LDAP/Kerberos

NTLM Authentication



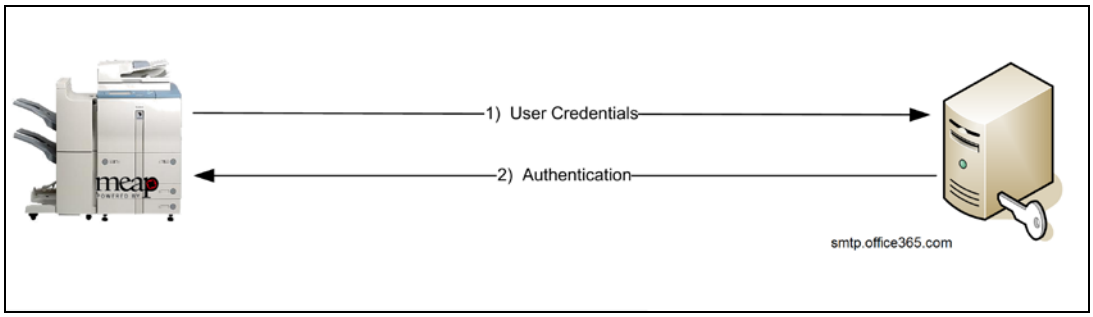
Communication Protocol LDAP/NTLM

Google Authentication



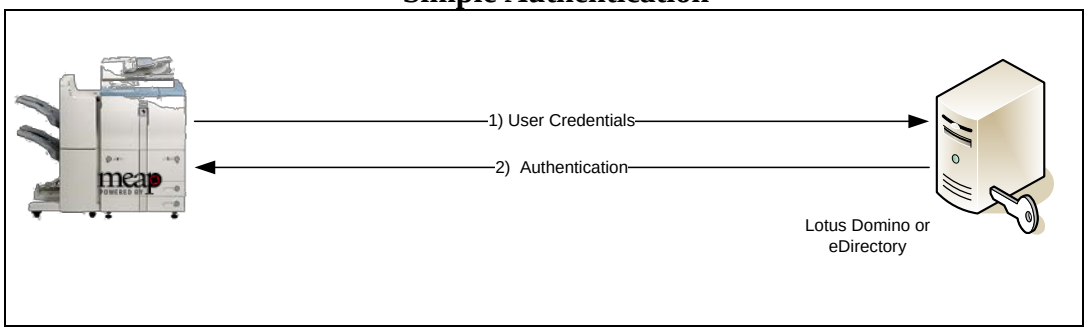
Communication Protocol SMTP over SSL (SMTPS)

Office 365 Authentication



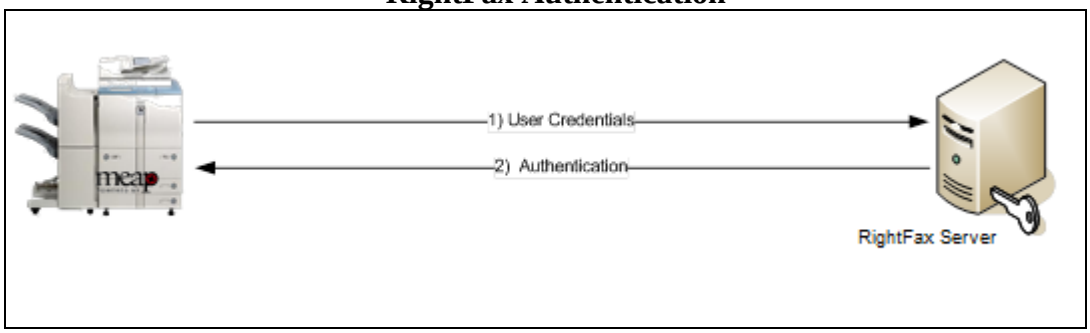
Communication Protocol SMTP over SSL (SMTPS)

Simple Authentication



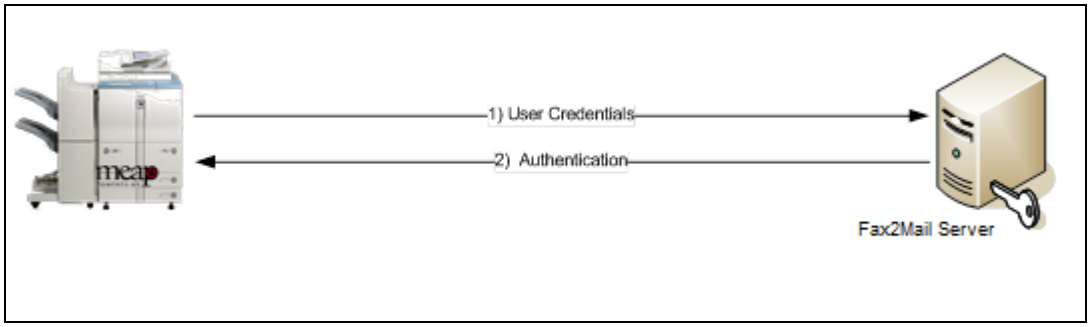
Communication Protocol LDAP/Simple

RightFax Authentication



Communication Protocol RightFax

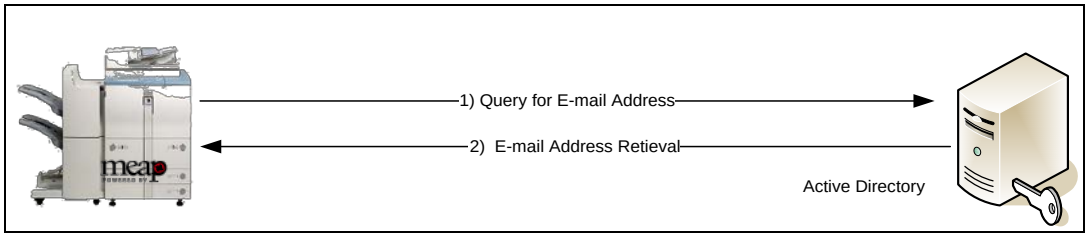
Fax2Mail Authentication



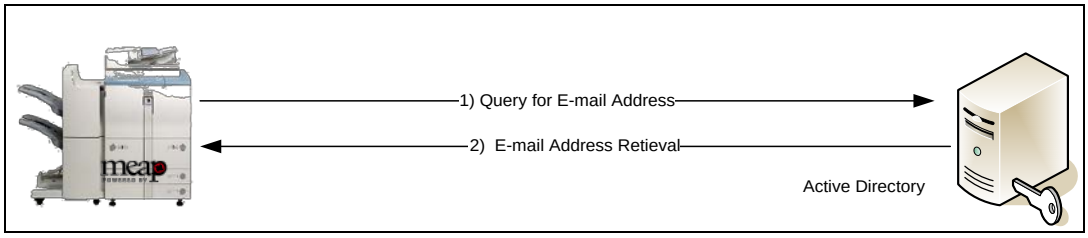
Communication Protocol Fax2Mail

1.3.1.2 Address Book Communication Diagrams

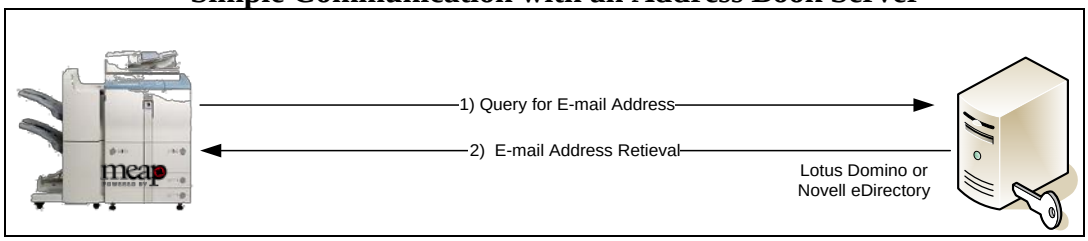
Kerberos Communication with an Address Book Server



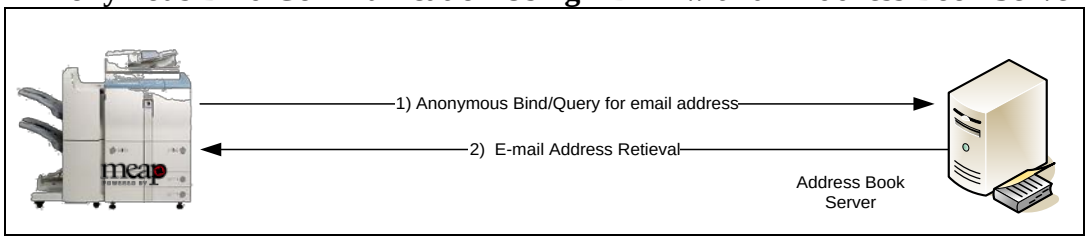
NTLM Communication with an Address Book Server



Simple Communication with an Address Book Server



Anonymous Bind Communication Using LDAP with an Address Book Server



Chapter 2 Configuring Authorized Send

This chapter describes how to configure Authorized Send from a Web browser and set up the authentication servers, address book servers, share names, and options for the Scan to E-Mail, Scan to Fax, and Scan to Folder functions. It also describes how to configure the application's interface appearance using the optional Brand Configuration Tool.

The Authorized Send Configuration page contains the following items for configuring Authorized Send:

Authentication:	Create up to 10 authentication servers.
E-Mail Service:	Configure an SMTP server, and up to 10 address book servers.
Scan to E-Mail:	Configure the Scan to E-Mail settings.
Scan to Fax:	Configure the Scan to Fax settings.
Scan to I-Fax:	Configure the Scan to I-Fax settings.
Scan to Folder:	Configure the Scan to Folder settings, and create preset folders for users to scan to.
Scan to RightFax	Configure the Scan to RightFax settings.
Scan to Fax2Mail	Configure the Scan to Fax2Mail settings.
Fax Forwarding	Configure the device to store incoming faxes, either via Advanced Box over SMB or an FTP server.
Scan to FTP:	Configure the Scan to FTP settings, and create preset FTP servers for users to scan to.
Scan to SharePoint:	Configure the Scan to SharePoint settings, and create preset SharePoint servers for users to scan to.
Scan to Box	Configure the Scan to Box settings.
Scan to Google Drive	Configure the Scan to Google Drive settings.
Scan to Multi-Destinations:	Configure the Scan to Multi-Destinations button settings.
One-Touch Buttons:	Configure the one-touch buttons with predefined parameters.
Feature Controls:	Configure the scan features.
Scan Settings:	Configure the default scan settings for each file type.
File Name Template:	Configure the syntax for the file name, and if users are expected to provide input for a flexible file name.
Barcode Policy:	If the Barcode package is installed, configure the Barcode policy.
Metadata Index:	Configure the type of data and format of the metadata file.
Options:	Configure the optional settings.
Logs and Report:	Configure the log settings, remote syslog servers, download and view the logs, and configure reporting.
Configuration Management:	Configures the distribution settings.
Disclaimer:	Configure the log on and log off disclaimer screen.
About:	Display the Authorized Send version information.

2.1 Logging On to Authorized Send

Follow the procedure below to log on to Authorized Send's Configuration servlet.

1. Open a browser window → enter the following URL:

   http://<device IP>:8000/AuthSendConfiguration
   https://<device IP>:8443/AuthSendConfiguration (if HTTPS is enabled on the MEAP device)
   (Replace <device IP> with the IP address of the MEAP device.)

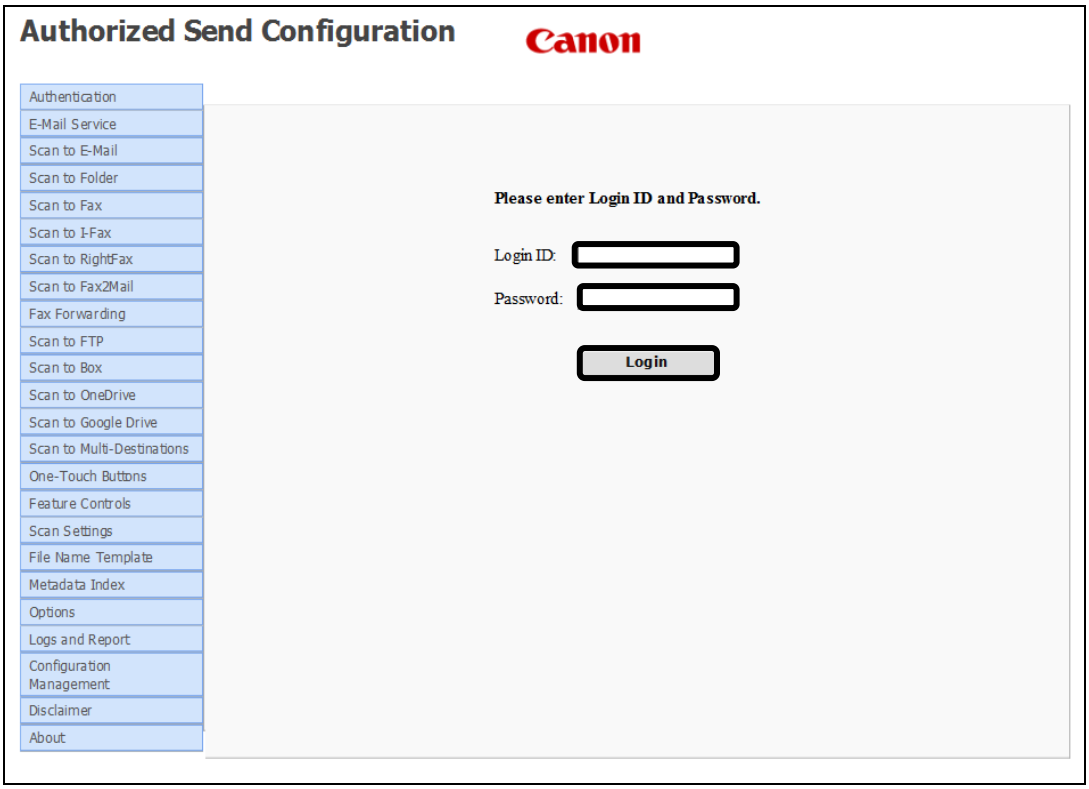
   The Please enter Login ID and Password screen is displayed.

IMPORTANT

- Enter **AuthSendConfiguration** exactly as shown, as it is case-sensitive.
- If Portal Service is installed, you can also access the Authorized Send Configuration screen by entering **http://<device IP>:8000** → click the Authorized Send Configuration link. (Replace <device IP> with the IP address of the MEAP device.)

2. Enter your user name in [Login ID] and your password in [Password] → click [Login].

   The default Login ID is ‘Administrator’, and the default password is ‘Admin’.



   The Authentication Servers screen is displayed.

IMPORTANT

- If you are using a license and it has expired, the message <The Authorized Send license has expired. Please contact your Canon dealer.> is displayed. You must update your license file, or you cannot access the Authorized Send Configuration servlet.
- If you install a new valid license without reinstalling Authorized Send, the device must be rebooted.

2.2 Creating an Authentication Server

You can create up to 10 domains for authentication.

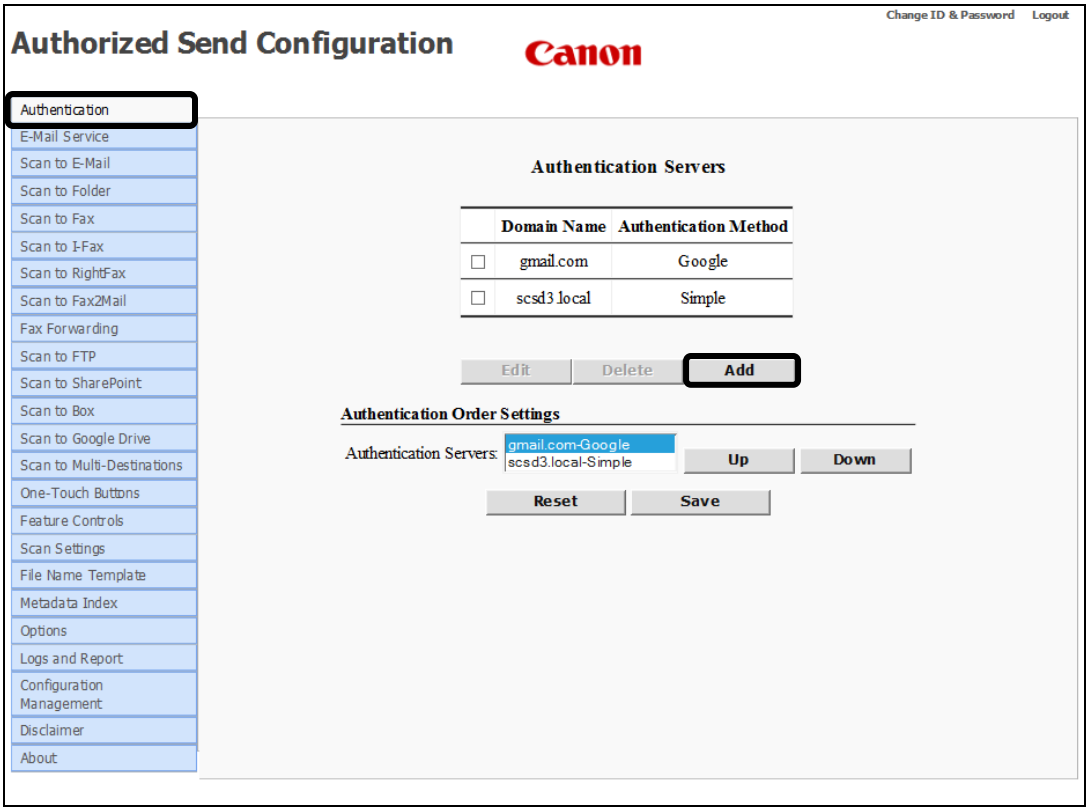
IMPORTANT

If you select the Kerberos protocol for the authentication method, make sure that the device clock setting is properly synchronized with the configured authentication server and address book server. For more information on synchronizing the device clock with the server clock, see "Synchronizing the Device and Server Time," on p. 518.

1. Log on to the Authorized Send Configuration servlet.

   For instructions on logging on to the Authorized Send Configuration servlet, see "Logging On to Authorized Send," on p. 32.

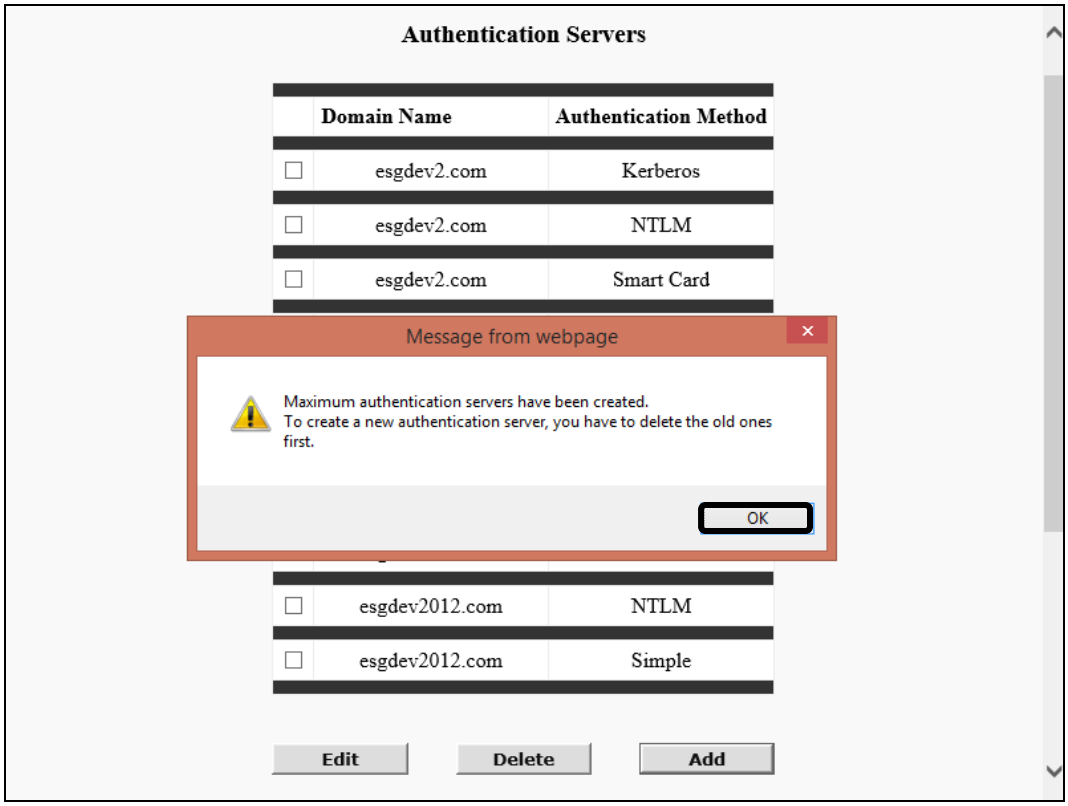
2. Click [Authentication] ➞ [Add].



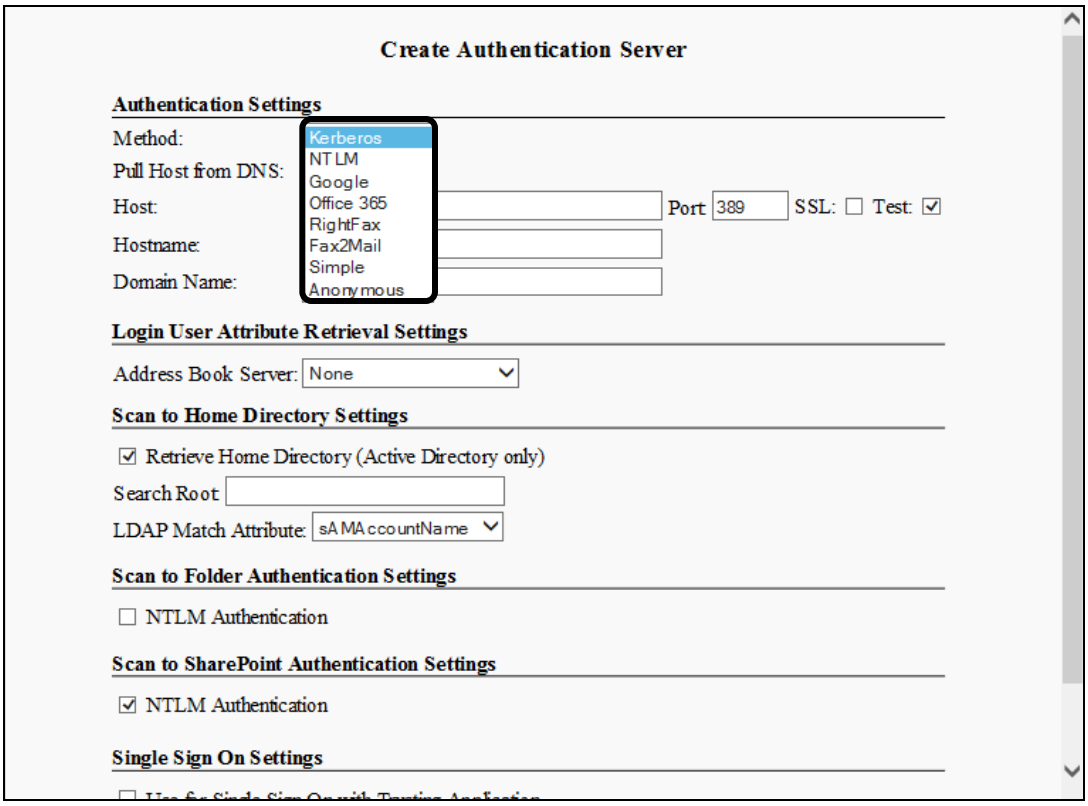
The Create Authentication Server screen is displayed.

NOTE

You can create a maximum of 10 authentication servers. If you attempt to create more than 10, a dialog box displays. Click [OK] and delete at least one existing server definition before you create another. See "Deleting an Authentication Server," on page 65 for information.



3. Click the Method drop-down list to select the authentication method.



Kerberos:	The machine communicates directly to Active Directory.
NTLM:	The machine communicates directly to Active Directory.
Google	The machine authenticates using Google's SMTP servers. This requires a valid Google account.
Office 365	The machine authenticates using Microsoft Office 365 SMTP servers. This requires a valid Office 365 account.
RightFax	The machine authenticates using the RightFax server defined in the authentication configuration.
Fax2Mail	The machine authenticates using the Fax2Mail server defined in the Authentication configuration.
Simple:	Necessary if you use Domino or eDirectory for authentication.

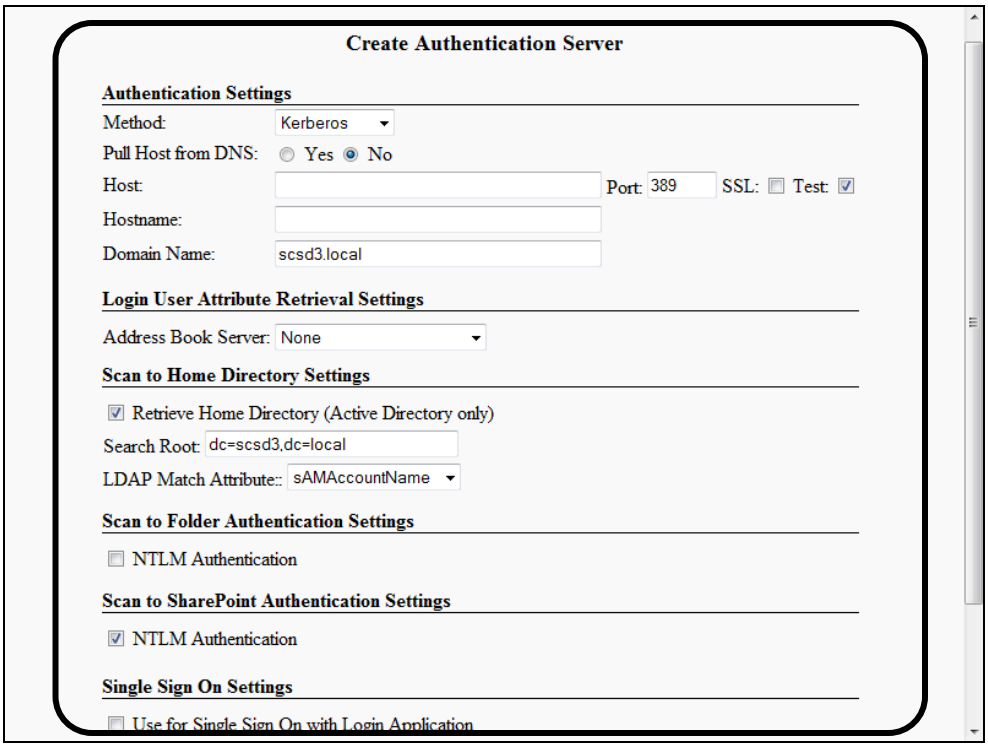
Anonymous: Configuring an anonymous authentication server enables you to use Authorized Send without logging on to the application.

IMPORTANT

- If an Anonymous authentication server is configured, the Authorized Send SIGN IN screen on the machine is always bypassed, and the user is logged on as an anonymous user.
- If an Anonymous server is created, other servers cannot be used.
- To disable Anonymous authentication, the Anonymous authentication server must be deleted. When Anonymous authentication is deleted, the default screen is the Authorized Send SIGN IN screen on the machine. For details about deleting an Anonymous authentication server, see "Deleting an Authentication Server," on p. 65.

4. Configure the settings for the selected authentication method.

   4.1 If you select [Kerberos] as the authentication method, configure the Authentication Settings, Login User E-Mail Address and Encryption Certificate Retrieval Settings, Scan to Home Directory Settings, Scan to Folder Authentication Settings, Scan to SharePoint Authentication Settings, and Single Sign On Settings.



Authentication Settings

Method:	Kerberos
Pull Host from DNS:	Select [Yes] to automatically pull the host information from the DNS after you click [Create]. Select [No] if you want to manually configure the host information. The default setting is 'No'. If you select the [Yes] radio button, the first "live" domain controller is used as the authentication server after you click [Create].
Pull Port from DNS:	This setting is only displayed when Pull Host from DNS is set to 'Yes'. Select this check box if you want the Port text box to be dynamically populated from the DNS.

Host:	This text box is displayed only if Pull Host from DNS is set to ‘No’. Enter the DNS name or IP address of the authentication server.
Port:	This text box is displayed only if Pull Host from DNS is set to ‘No’, and if the [Pull Port from DNS] check box is not selected. Enter the connecting port number of the authentication server. You can enter a maximum of five numbers. The default port number is ‘389’.
SSL:	This check box is displayed only if Pull Host from DNS is set to ‘No’, and if the [Pull Port from DNS] check box is not selected. Select this check box if you want the authentication server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.
Test:	This check box is displayed only if Pull Host from DNS is set to ‘No’. Select this check box if you want the connection to the authentication server to be verified before you save the settings. The [Test] check box is selected by default.
Hostname:	This text box is displayed only for Kerberos if Pull Host from DNS is set to ‘No’. Enter the host name of the authentication server.
Domain Name:	Enter the authentication server domain for this device. You can enter a string that consists of any character, and an unlimited number of characters. The default value is pulled from the device.

Login User E-Mail Address and Encryption Certificate Retrieval Settings

Address Book Server:	If you have already configured an address book server, select the address book server from which the user’s e-mail address can be retrieved from the drop-down list. The default setting is ‘None’.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user's home directory information from the authentication server. This creates a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only)] check box on the Create Address Book Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

Search Root:	Specify the search root for searching the user's home directory via LDAP. Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. [Search Root] only appears if the [Retrieve Home Directory (Active Directory only)] check box is selected. The default value for the Search Root text box is blank if the Domain Name text box is blank. If the Domain Name text box is populated, the Search Root text box is automatically populated based on the text entered in the Domain Name text box.
LDAP Match Attribute:	Select [sAMAccountName] or [userPrincipalName] from the drop-down list to determine which attribute to use for LDAP match. This enables you to search for the user's Home Directory. The default setting is 'sAMAccountName'.

Scan to Folder Authentication Settings

NTLM Authentication:	Select this check box to use NTLM as the authentication method for the Scan to Folder feature, regardless of the authentication method you selected for the authentication server.
NTLM domain name:	Enter the domain name to be used for NTLM authentication of a share for the Scan to Folder feature. The default value is the first part of the domain configured in the Domain Name text box.

IMPORTANT

If you select the Kerberos protocol for the authentication method, make sure that the device clock setting is properly synchronized with the configured authentication server and address book server. For more information on synchronizing the device clock with the server clock, see "Synchronizing the Device and Server Time," on p. 518.

Scan to SharePoint Authentication Settings

NTLM Authentication:	Select this check box to use NTLM as the authentication method for the Scan to SharePoint feature, regardless of the authentication method you selected for the authentication server. By default, this check box is selected.

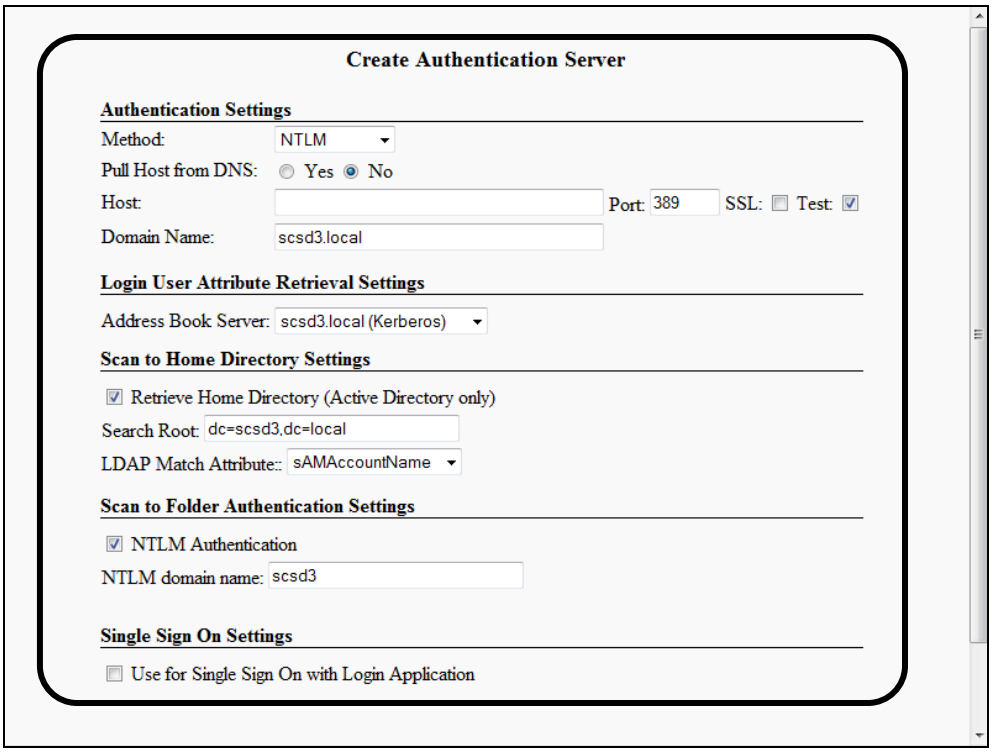
Single Sign On Settings

Use for Single Sign On with Login Application:	If this check box is selected, Authorized Send retrieves the domain of the user from a login application, or from any device that supports SCMS. If the domain matches the authentication server, Authorized Send attempts to authenticate to that authentication server with the user name and password retrieved from the login application or the device that supports SCMS. If the credentials are valid, the Authorized Send SIGN IN screen is bypassed. If the credentials are invalid, the Authorized Send SIGN IN screen is displayed and the user must attempt authentication manually. By default, this check box is not selected.

IMPORTANT

The compatible login applications for single sign on are AA-CAC, AA-PROX V2.1L, AA-PROX V2.1 or later, and Universal Login Manager (see Chapter 5 "Appendix: Configuring Authorized Send with Trusted Login Managers," for more information).

4.2 If you select [NTLM] as the authentication method, configure the Authentication Settings, Login User E-Mail Address and Encryption Certificate Retrieval Settings, Scan to Home Directory Settings, Scan to Folder Authentication Settings, and Single Sign On Settings.



Authentication Settings

Method: NTLM

Pull Host from DNS: Select [Yes] to automatically pull the host information from the DNS after you click [Create]. Select [No] if you want to manually configure the host information. The default setting is 'No'.

If you select the [Yes] radio button, the first "live" domain controller is used as the authentication server after you click [Create].

Pull Port from DNS: This setting is only displayed when you select the [Yes] radio button for [Pull Host from DNS]. Select this check box if you want the Port text box to be dynamically populated from the DNS.

Host:	This text box is displayed only if Pull Host from DNS is set to ‘No’. Enter the DNS name or IP address of the authentication server.
Port:	This text box is displayed only if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Enter the connecting port number of the authentication server. You can enter a maximum of five numbers. The default port number is ‘389’.
SSL:	This check box is displayed only if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Select this check box if you want the authentication server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.
Test:	This check box is displayed only if Pull Host from DNS is set to ‘No’. Select this check box if you want the connection to the authentication server to be verified before you save the settings. The [Test] check box is selected by default.
Domain Name:	Enter the authentication server domain for this device. You can enter a string that consists of any character, and an unlimited number of characters. The default value is pulled from the device.

Login User E-Mail Address and Encryption Certificate Retrieval Settings

Address Book Server:	If you have already configured an address book server, select the address book server from which the user’s e-mail address can be retrieved from the drop-down list. The default setting is ‘None’.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user's home directory information from the authentication server. This creates a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only)] check box on the Create Address Book Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

Search Root:	Specify the search root for searching the user's home directory via LDAP. Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. [Search Root] only appears if the [Retrieve Home Directory (Active Directory only)] check box is selected. The default value for the Search Root text box is blank if the Domain Name text box is blank. If the Domain Name text box is populated, the Search Root text box is automatically populated based on the text entered in the Domain Name text box.
LDAP Match Attribute:	Select [sAMAccountName] or [userPrincipalName] from the drop-down list to determine which attribute to use for LDAP match. This enables you to search for the user's Home Directory. The default setting is 'sAMAccountName'.

Scan to Folder Authentication Settings

NTLM Authentication:	Select this check box to use NTLM as the authentication method for the Scan to Folder feature, regardless of the authentication method you selected for the authentication server.
NTLM domain name:	Enter the domain name to be used for NTLM authentication of a share for the Scan to Folder feature. The default value is the first part of the domain configured in the Domain Name text box.

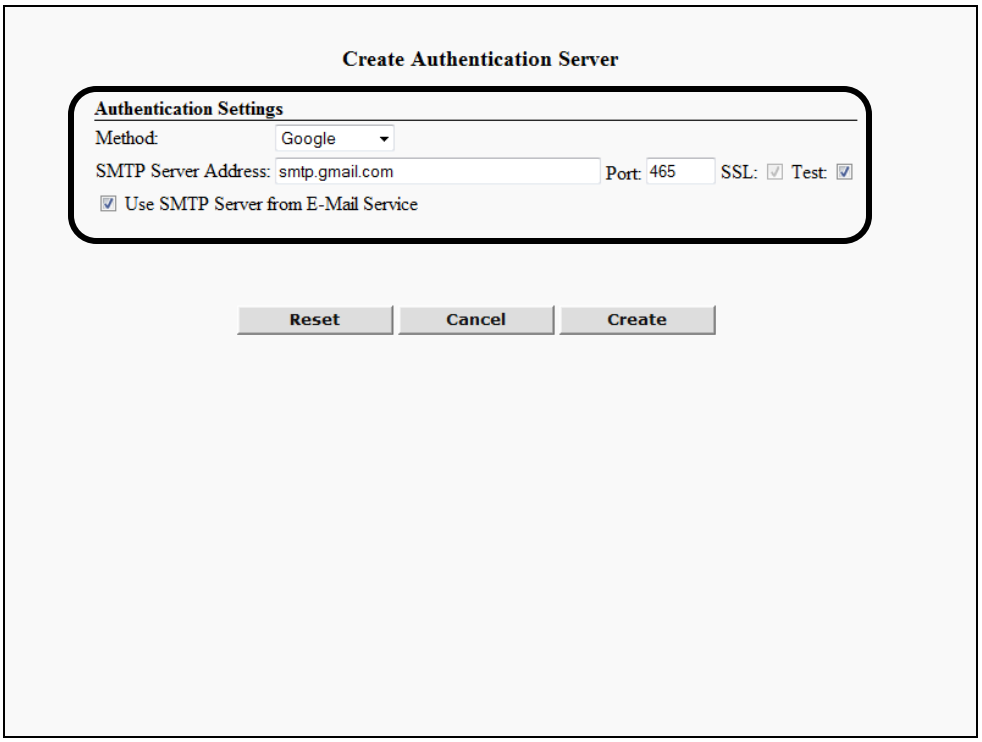
Single Sign On Settings

Use for Single Sign On with Login Application:	If this check box is selected, Authorized Send retrieves the domain of the user from a login application, or from any device that supports SCMS. If the domain matches the authentication server, Authorized Send attempts to authenticate to that authentication server with the user name and password retrieved from the login application or the device that supports SCMS. If the credentials are valid, the Authorized Send SIGN IN screen is bypassed. If the credentials are invalid, the Authorized Send SIGN IN screen is displayed and the user must attempt authentication manually. By default, this check box is not selected.

IMPORTANT

The compatible login applications for single sign on are AA-CAC, AA-PROX V2.1L, AA-PROX V2.1 or later, and Universal Login Manager (see Chapter 5 "Appendix: Configuring Authorized Send with Trusted Login Managers," for more information).

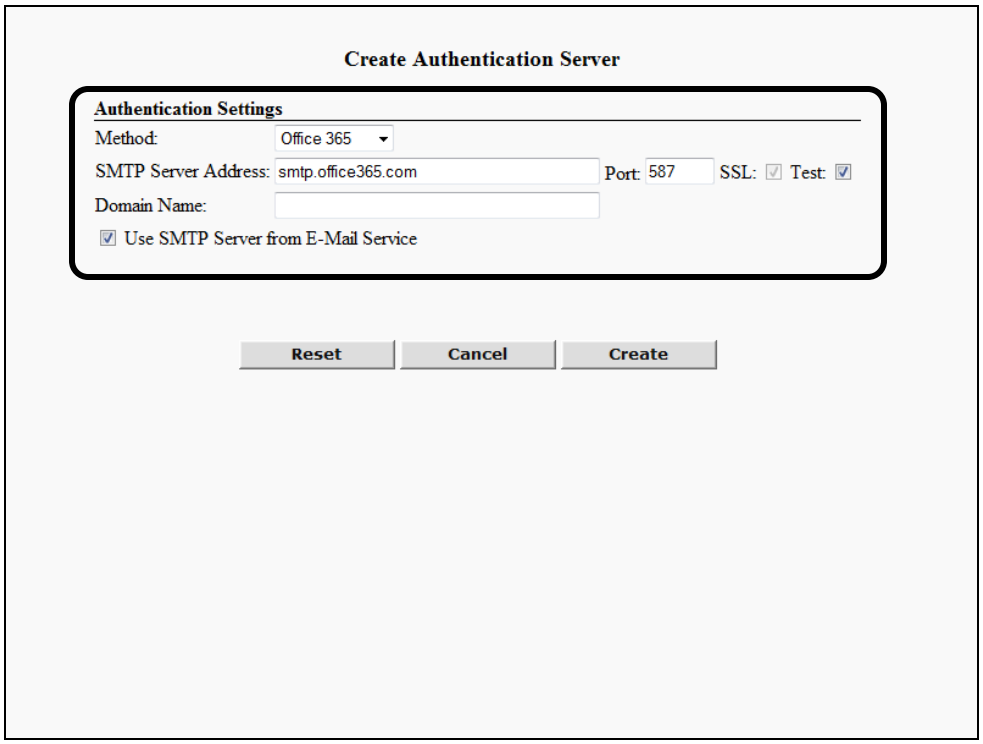
4.3 If you select [Google] as the authentication method, configure the Authentication Settings.



Authentication Settings

Method:	Google
SMTP Server Address:	Enter the IP address or the server name of the SMTP server. The default server address is ‘smtp.gmail.com’.
Port:	Enter the connecting port number of the authentication server. You can enter a maximum of five numbers. The default port number is ‘465’.
SSL:	SSL is required for authentication through Google. You cannot change this setting.
Test:	Select this check box if you want the connection to the authentication server to be verified before you save the settings. The [Test] check box is selected by default.
Use SMTP Server from E-mail Service:	Select this check box if you want to authenticate using the same SMTP server as defined in the <E-mail Service> configuration. The [Use SMTP…] check box is not selected by default.

4.4 If you select [Office 365] as the authentication method, configure the Authentication Settings.

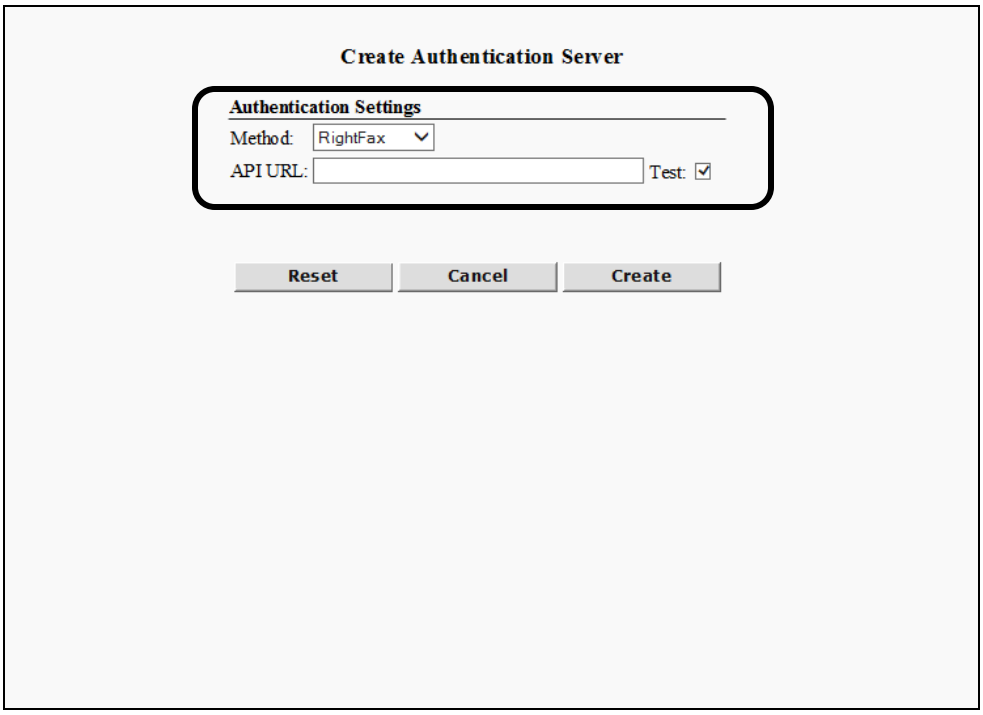


Authentication Settings

Method:	Office 365
SMTP Server Address:	Enter the IP address or the server name of the SMTP server. The default server address is 'smtp.office365.com'
Port:	Enter the connecting port number of the authentication server. You can enter a maximum of five numbers. The default port number is '587'.
SSL:	SSL is required for authentication through Office 365. You cannot change this setting.
Test:	Select this check box if you want the connection to the authentication server to be verified before you save the settings. The [Test] check box is selected by default.

Domain Name:	Enter the domain name of the Office 365 account as issued by Microsoft.
Use SMTP Server from E-mail Service:	Select this check box if you want to authenticate using the same SMTP server as defined in the <E-mail Service> configuration. The [Use SMTP…] check box is not selected by default.

4.5 If you select [RightFax] as the authentication method, configure the Authentication Settings.



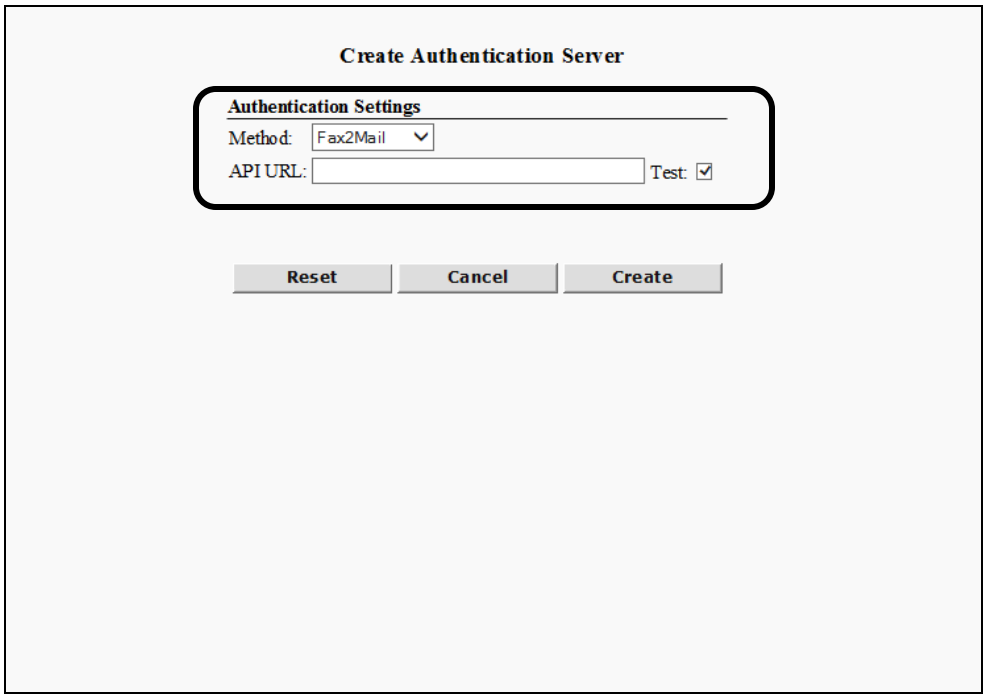
Authentication Settings

Method: RightFax

API URL: Enter the URL of the RightFax API. It should be the same as the RightFax API URL set in the RightFax configuration screen. It is blank by default.

Test: Select this check box to validate that the [API URL] setting is an active connection and is a valid RightFax server.

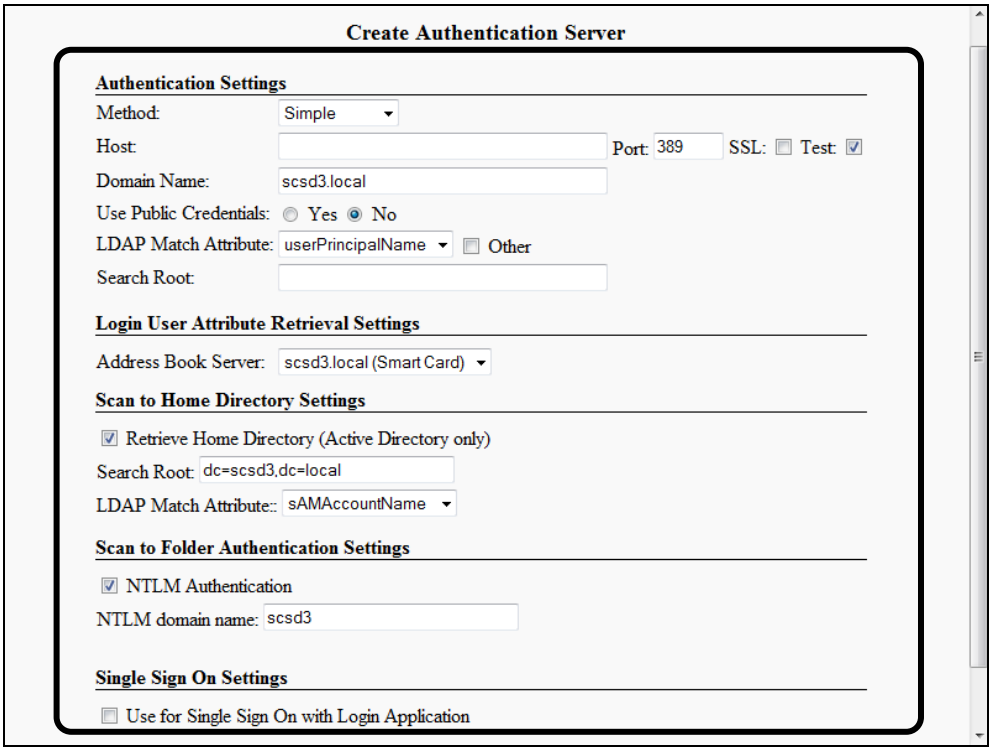
4.6 If you select [Fax2Mail] as the authentication method, configure the Authentication Settings.



Authentication Settings

Method:	Fax2Mail
API URL:	Enter the URL of the Fax2Mail API. It should be the same as the Fax2Mail API URL set in the Fax2Mail configuration screen. It is blank by default.
Test:	Select this check box to validate that the [API URL] setting is an active connection and is a valid Fax2Mail server.

4.7 If you select [Simple] as the authentication method, configure the Authentication Settings, Login User E-Mail Address and Encryption Certificate Retrieval Settings, Scan to Home Directory Settings, Scan to Folder Authentication Settings, and Single Sign On Settings.



Authentication Settings

Method: Simple

Host: Enter the DNS name or IP address of the authentication server.

Port: Enter the connecting port number of the authentication server. You can enter a maximum of five numbers. The default port number is '389'.

SSL: Select this check box if you want the authentication server to use SSL. If you select this check box, the host port number automatically changes to '636'.

Test: Select this check box if you want the connection to the authentication server to be verified before you save the settings. The [Test] check box is selected by default.

Domain Name:	Enter the authentication server domain for this device. You can enter a string that consists of any character, and an unlimited number of characters. The default value is pulled from the device.
Use Public Credentials:	Select [Yes] to configure the public credentials (Public DN and Public Password), or select [No] to use anonymous binding. The default setting is 'No'.
Public DN:	This text box is displayed only if Use Public Credentials is set to 'Yes'. If [Yes] is selected for Use Public Credentials, you must enter the user's login Distinguished Name to use when performing the first bind of the Simple Binding process.
Public Password:	This text box is displayed only if Use Public Credentials is set to 'Yes'. It is used as the password when performing the first bind of the Simple Binding process. It is an optional text box. You can enter a string that consists of any character, and an unlimited number of characters.
LDAP Match Attribute:	Select [uid], [sAMAccountName], or [userPrincipalName] from the drop-down list to determine which attribute to use for LDAP match. The default setting is 'uid'.
Other:	If you select this check box, the LDAP Match Attribute drop-down list becomes a text box, where you can enter the username's LDAP attribute to be matched with the username when performing the first bind of the Simple Binding process. You can enter a string that consists of any character, and an unlimited number of characters.
Search Root:	Specify the search root for searching the user's home directory via LDAP. *If the directory server is authenticating against eDirectory or Domino and the organization is, for example, Canon, then the search root is o=canon.*

Login User E-Mail Address and Encryption Certificate Retrieval Settings

Address Book Server:	If you have already configured an address book server, select the address book server from which the user's e-mail address can be retrieved from the drop-down list. The default setting is 'None'.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user's home directory information from the authentication server. This creates a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only)] check box on the Create Address Book Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

Search Root:	Specify the search root for searching the user's home directory via LDAP. Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. [Search Root] only appears if the [Retrieve Home Directory (Active Directory only)] check box is selected. The default value for the Search Root text box is blank if the Domain Name text box is blank. If the Domain Name text box is populated, the Search Root text box is automatically populated based on the text entered in the Domain Name text box.
LDAP Match Attribute:	Select [sAMAccountName] or [userPrincipalName] from the drop-down list to determine which attribute to use for LDAP match. This enables you to search for the user's Home Directory. The default setting is 'sAMAccountName'.

Scan to Folder Authentication Settings

NTLM Authentication:	Select this check box to use NTLM as the authentication method for the Scan to Folder feature, regardless of the authentication method you selected for the authentication server.
NTLM domain name:	Enter the domain name to be used for NTLM authentication of a share for the Scan to Folder feature. The default value is the first part of the domain configured in the Domain Name text box.

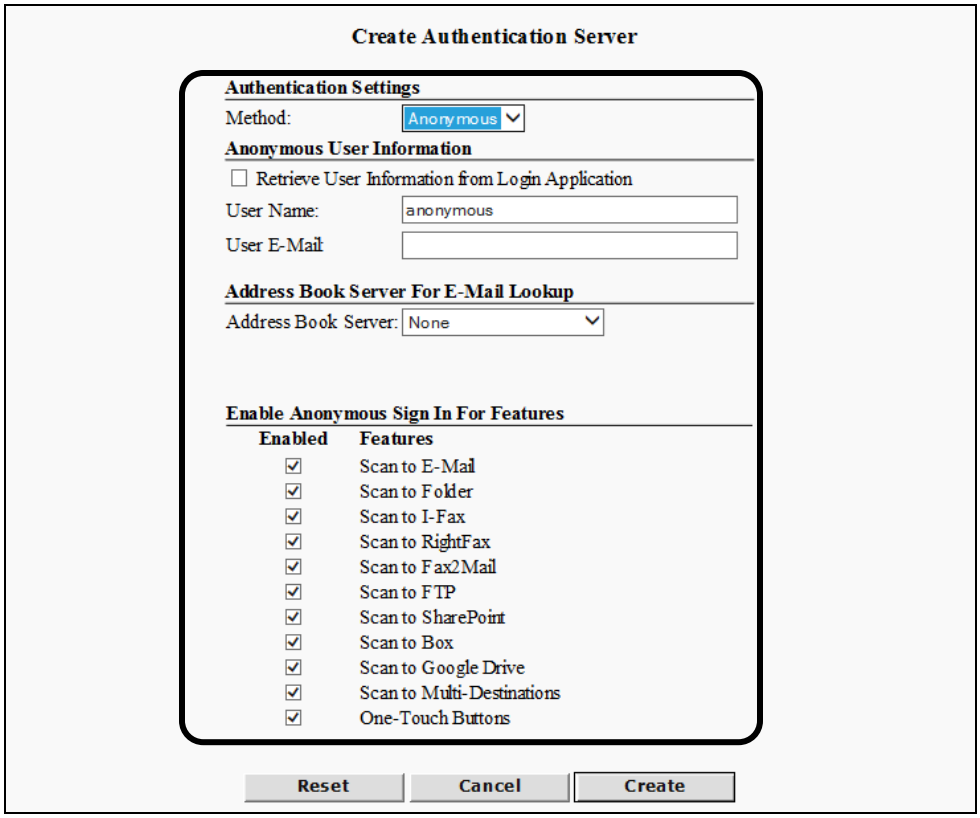
Single Sign on Settings

Use for Single Sign On with Login Application:	If this check box is selected, Authorized Send retrieves the domain of the user from a login application, or from any device that supports SCMS. If the domain matches the authentication server, Authorized Send attempts to authenticate to that authentication server with the user name and password retrieved from the login application or the device that supports SCMS. If the credentials are valid, the Authorized Send SIGN IN screen is bypassed. If the credentials are invalid, the Authorized Send SIGN IN screen is displayed and the user must attempt authentication manually. By default, this check box is not selected.

IMPORTANT

The compatible login applications for single sign on are AA-CAC, AA-PROX V2.1L, AA-PROX V2.1 or later, and Universal Login Manager (see Chapter 5 "Appendix: Configuring Authorized Send with Trusted Login Managers," for more information).

4.8 If you select [Anonymous] as the authentication method, configure the Anonymous User Information, Address Book Server for E-Mail Lookup, and Enable Anonymous Sign In For Features.



Authentication Settings

Method: Anonymous

Anonymous User Information

Retrieve User Information from Login Application: Select this check box to retrieve the user name and user e-mail from the login application when the user presses [Authorized Send] on the Main Menu screen of the machine. If this check box is selected, the User Name and User E-Mail text boxes are not displayed. By default, this check box is not selected.

NOTE
If no login application is enabled, the user name retrieved is the device default, and no user e-mail is retrieved since a default e-mail does not exist.

User Name:	This text box is displayed only if the [Retrieve User Information from Login Application] check box is not selected. Enter the user name for anonymous sending. You can enter a maximum of 40 characters. Validation cannot occur if this text box is blank. The default setting is ‘anonymous’.
User E-Mail:	This text box is displayed only if the [Retrieve User Information from Login Application] check box is not selected. This text box is used as the sender’s e-mail address for the Scan to Fax and Scan to E-Mail functions. Enter the anonymous user’s e-mail address. You can enter a maximum of 64 characters for the first (local) part, and a maximum of 255 characters for the domain part. This text box is optional.

Address Book Server for E-Mail Lookup

Address Book Server:	Select a configured address book server to use with the e-mail lookup feature of the Scan to E-Mail function. The default setting is ‘None’.

Enable Anonymous Sign In For Features

The check boxes in the <Enabled> column refer to the corresponding feature to the right of each check box. Select the check box next to the desired feature if you want to enable anonymous authentication sign in for that feature. If a check box is not selected and the user selects [Scan to E-Mail], for example, the Authorized Send SIGN IN screen with [Cancel] on the machine is displayed. All check boxes are selected by default.

IMPORTANT

- If an anonymous authentication server is configured, the Authorized Send SIGN IN screen on the machine is bypassed, and the user is logged on as an anonymous user. If at least one Authorized Send function is enabled, the Authorized Send MAIN screen on the machine is displayed. If only one Authorized Send function is enabled, only that function's screen is displayed.
- If the [User E-Mail] text box is blank, the Scan to Fax and Scan to E-Mail functions do not work on the machine.
- If only one function is enabled but, that function is inaccessible due to insufficient data, the Authorized Send MAIN screen on the machine is displayed with that function's button disabled and an error message.

NOTE

- Validation of the User Name and User E-Mail address occurs when [Create] is clicked. If validation fails, an error message is displayed.
- Only one anonymous authentication server can be configured.

5. Click [Create].

   If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

   To cancel creating the authentication server and return to the Authentication Servers screen, click [Cancel].

   A message is displayed informing you that the configuration has been saved, and the screen returns to the Authentication Servers screen.

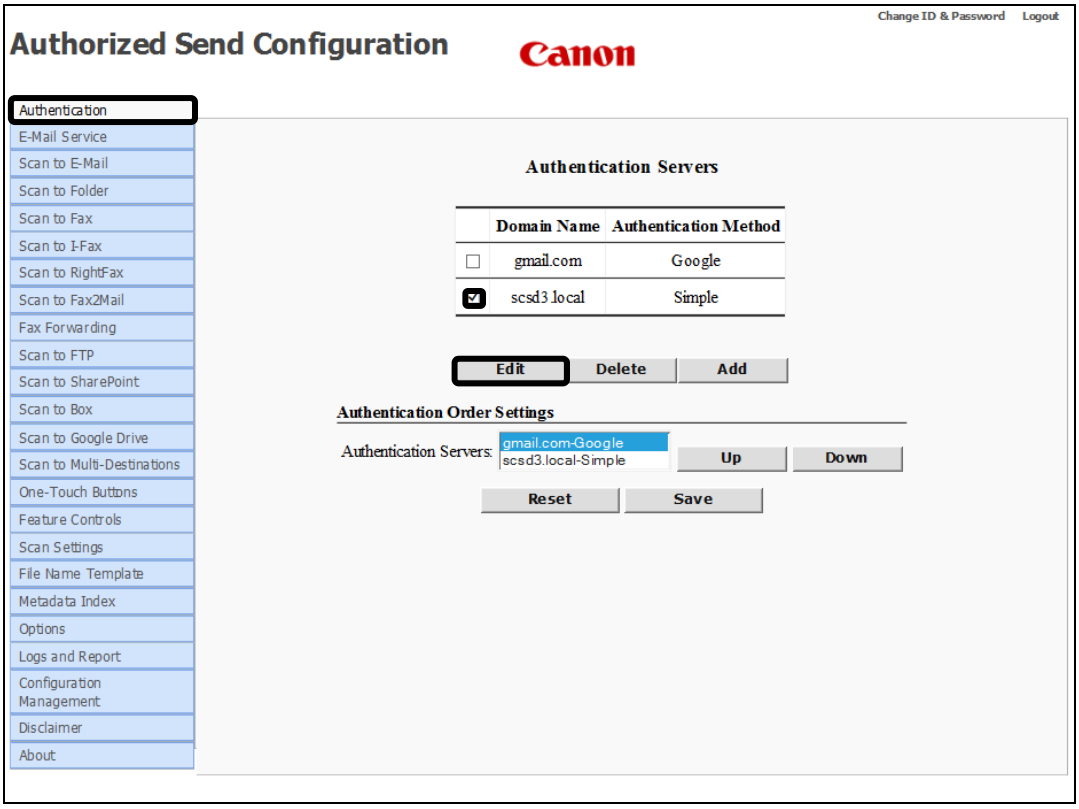
IMPORTANT

- Select the [Test] check box next to <Host> if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message is displayed. Enter the correct information → click [Save].

2.3 Editing an Authentication Server

You can edit a previously created authentication server from the Authorized Send Configuration screen.

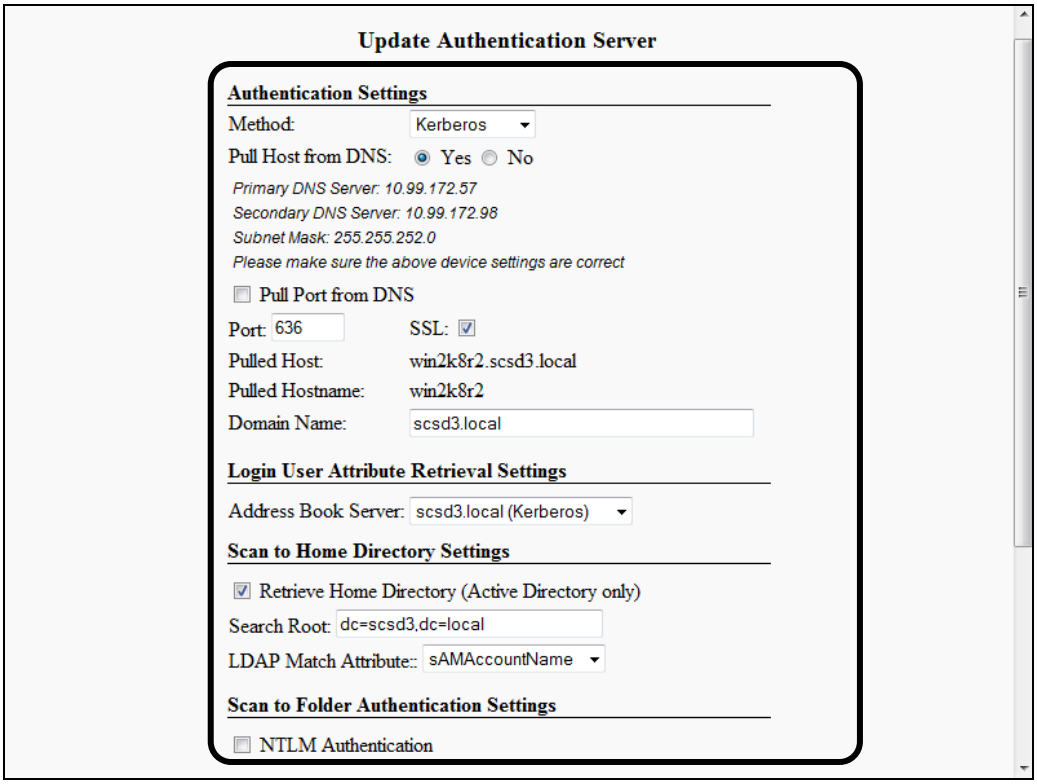
1. Click [Authentication] → select the check box next to the authentication server you want to edit → click [Edit].

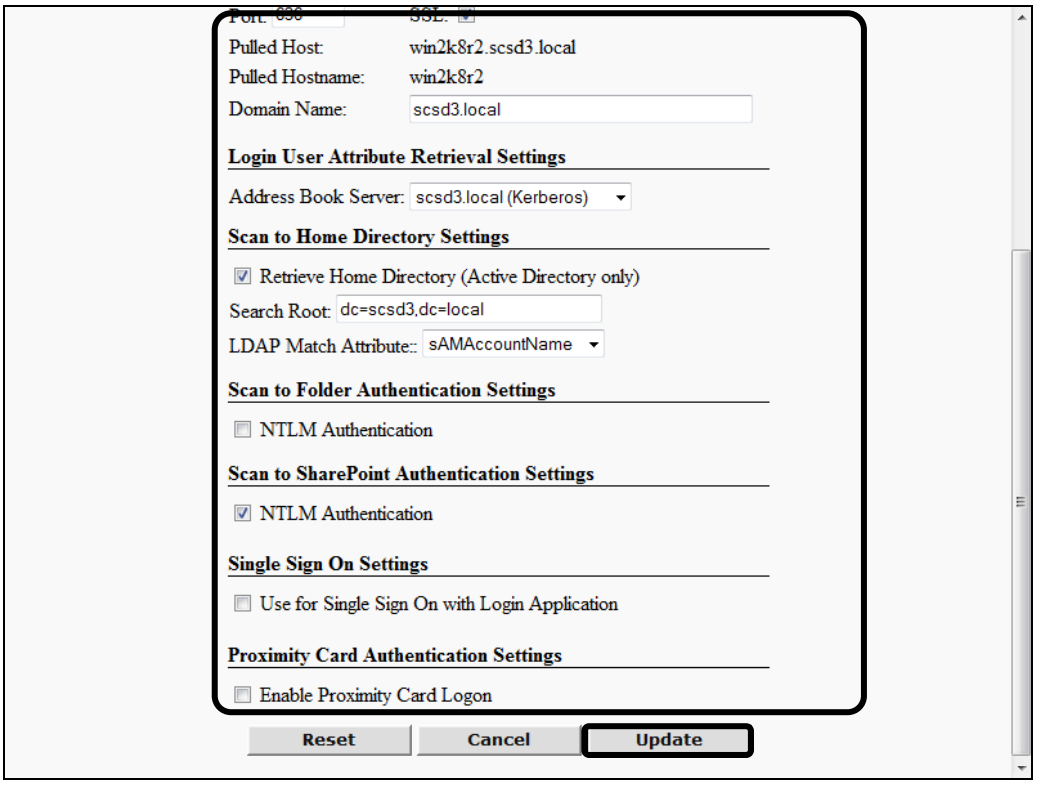


Note: you can only edit one authentication server definition at a time. If you select multiple definitions, the Edit button is greyed out.

The Update Authentication Server screen is displayed.

2. Edit the settings for the authentication server, as necessary → click [Update].





If ‘Kerberos’ or ‘NTLM’ is selected as the authentication method and Pull Host from DNS is set to ‘Yes’, the following two additional fields appear under <Authentication Settings> only on the Update Authentication Server screen:

Pulled Host:	The fully-qualified domain name of the machine is pulled from the DNS and automatically populates this field.
Pulled Hostname:	The host name of the authentication server is pulled from the DNS and automatically populates this field. This field appears only if the authentication method selected is ‘Kerberos’.

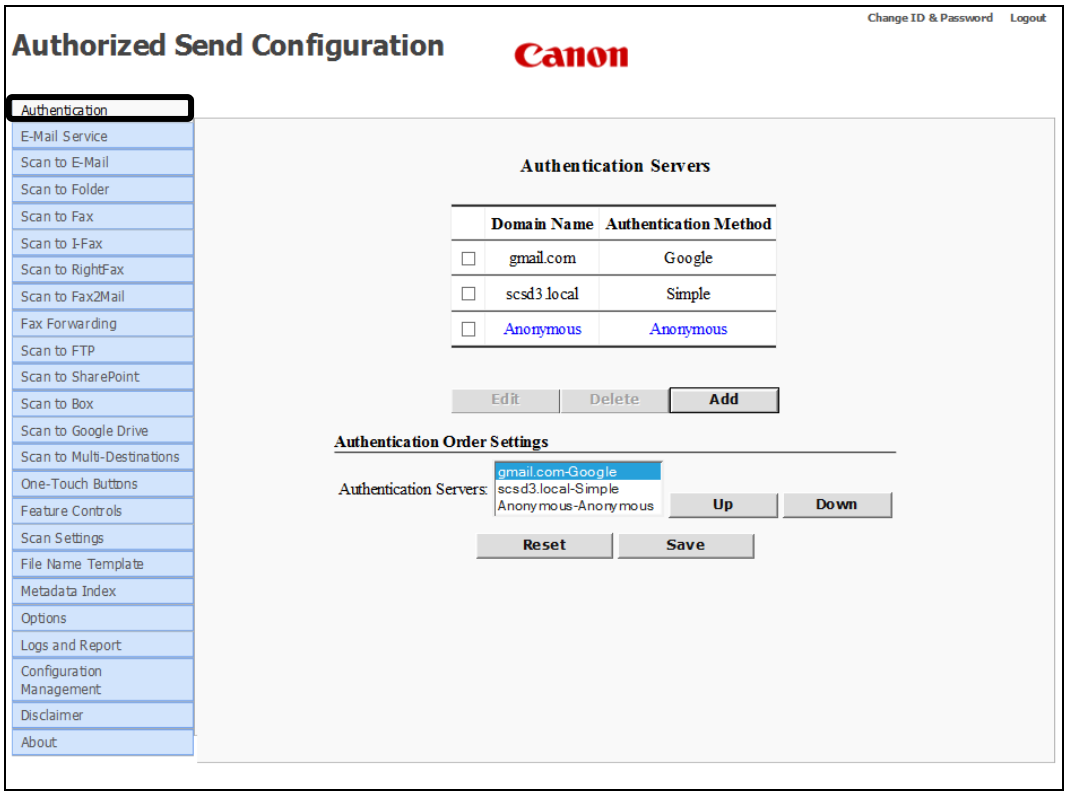
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the authentication server and return to the Authentication Servers screen, click [Cancel].

2.3.1 Changing the Display Order of the Authentication Servers

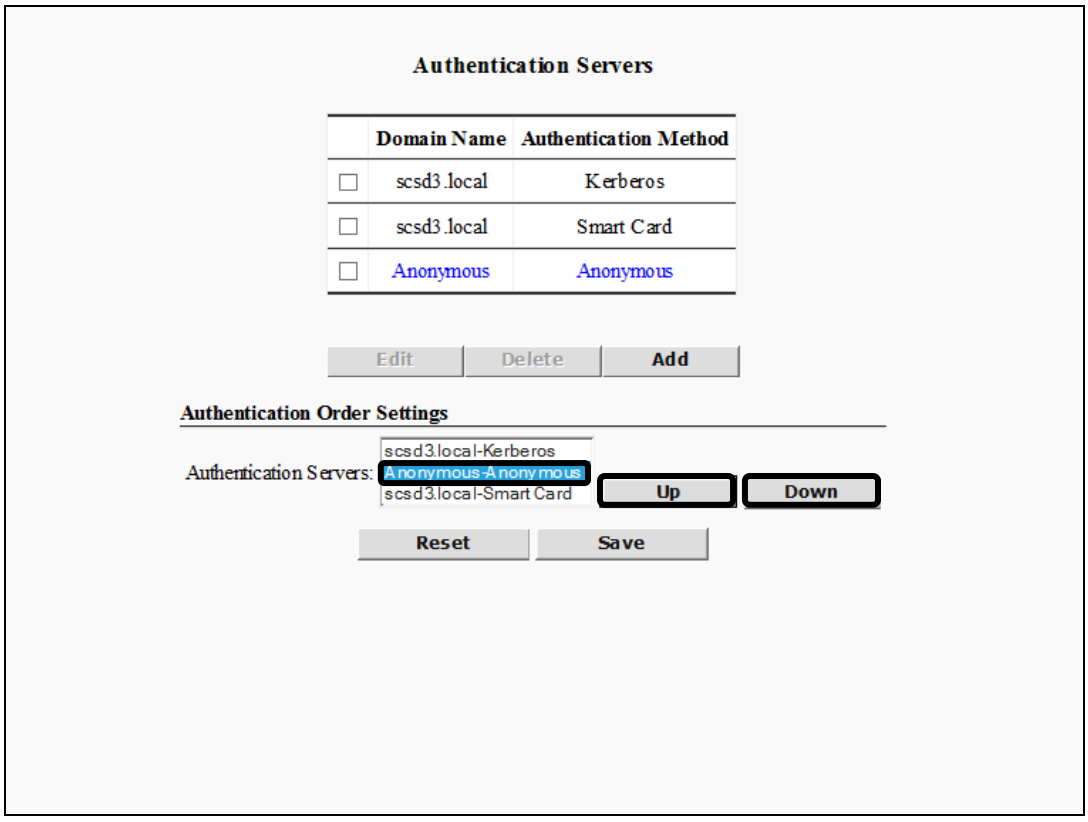
You can change the order in which the authentication servers are listed on the Authentication Servers screen.

1. Click [Authentication].

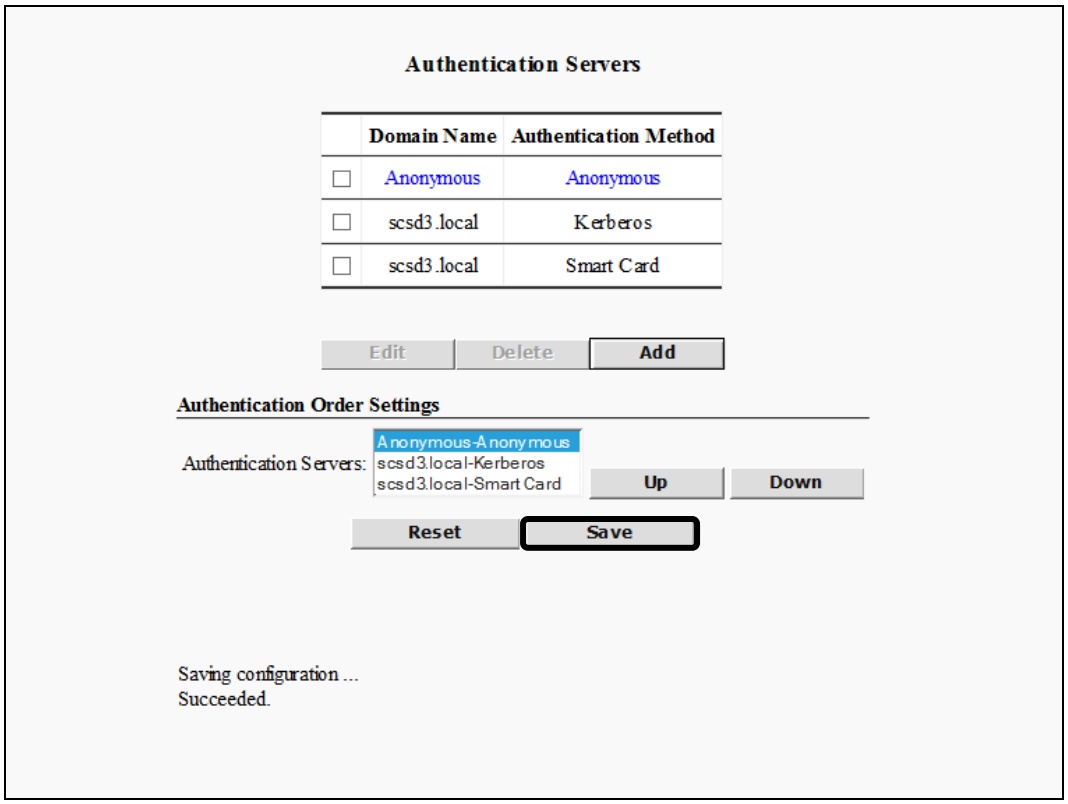


The Update Address Book Server screen is displayed.

2. In the [Authentication Servers] list box, select the authentication server you want to move in the list → click [Up] and [Down] to change its location in the list.



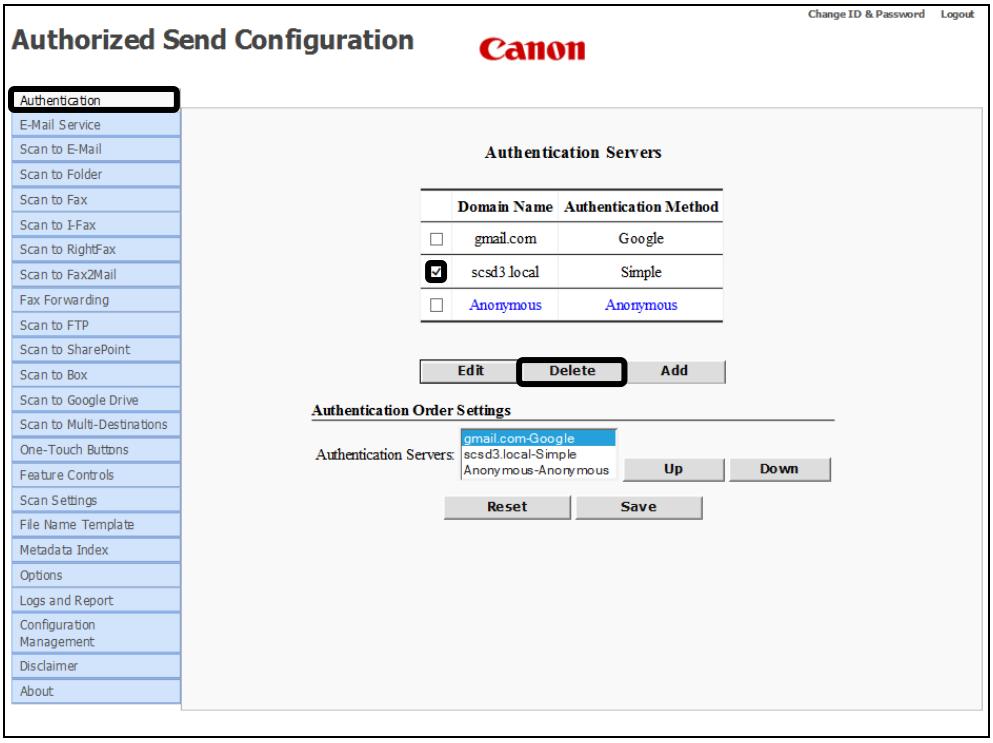
3. Click [Save] to save the changes.



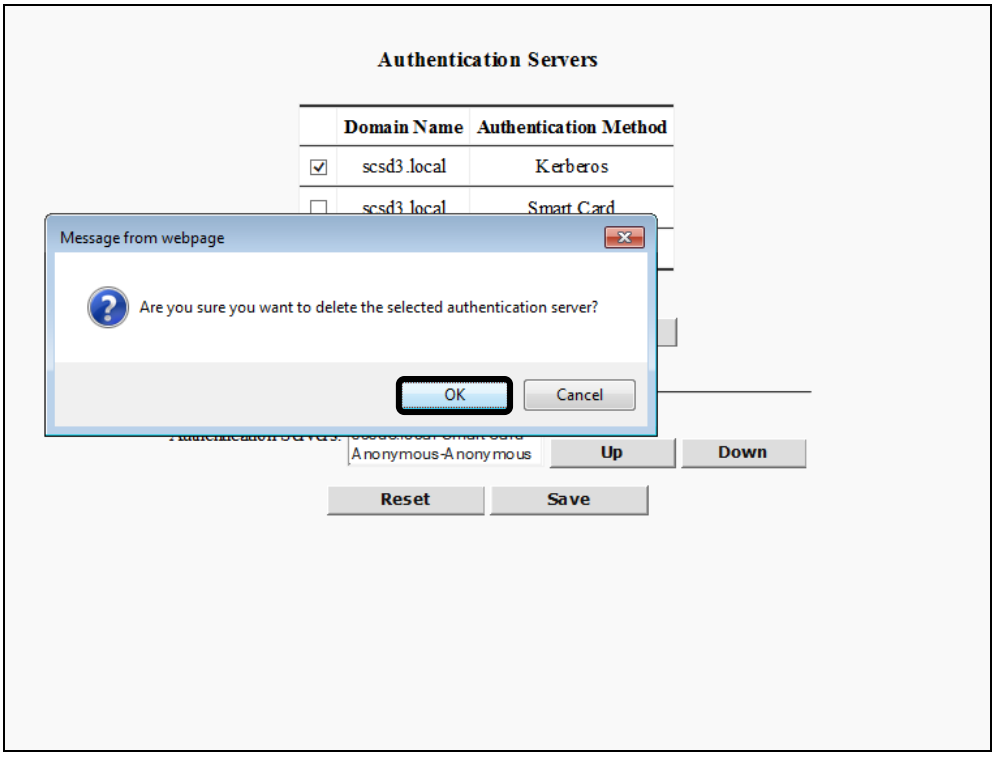
2.4 Deleting an Authentication Server

You can delete a previously created authentication server from the Authorized Send Configuration screen.

1. Click [Authentication] → select the check box next to the authentication server you want to delete → click [Delete].



2. Click [OK].



If you do not want to delete the authentication server, click [Cancel].

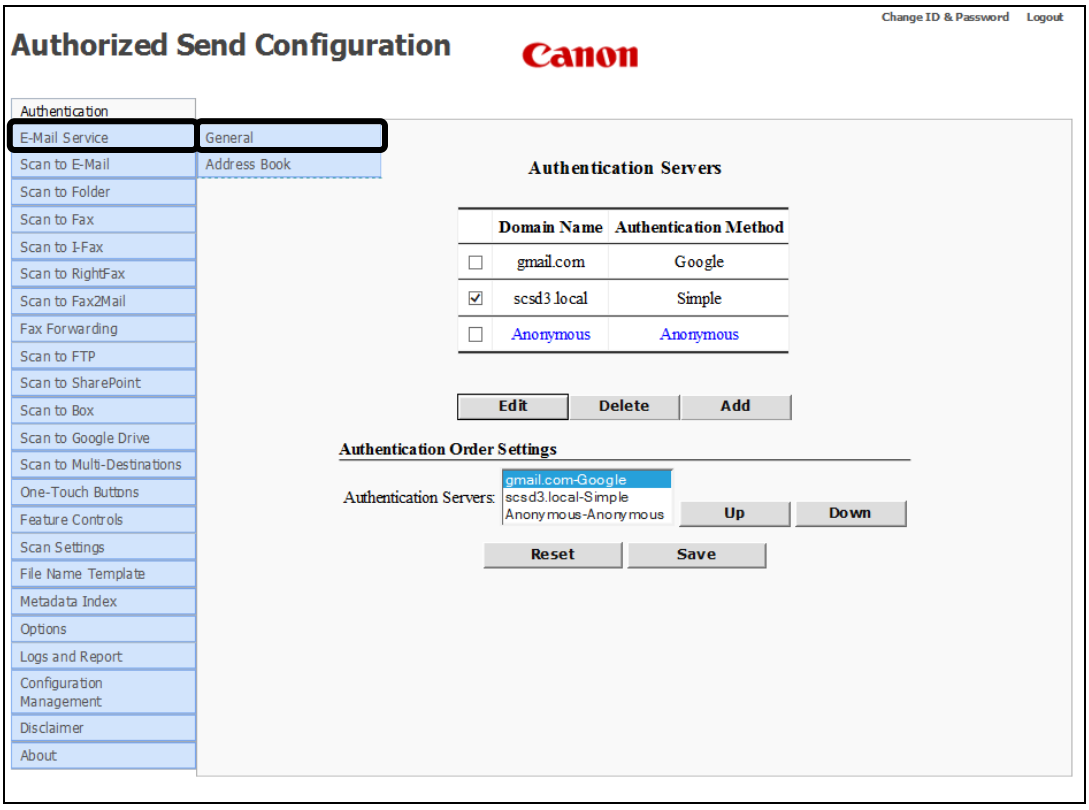
The authentication server is deleted from the list.

2.5 Configuring the E-Mail Service Settings

You can configure the settings for the SMTP server, which enables users to scan and send e-mail messages via an SMTP server, and create address book servers.

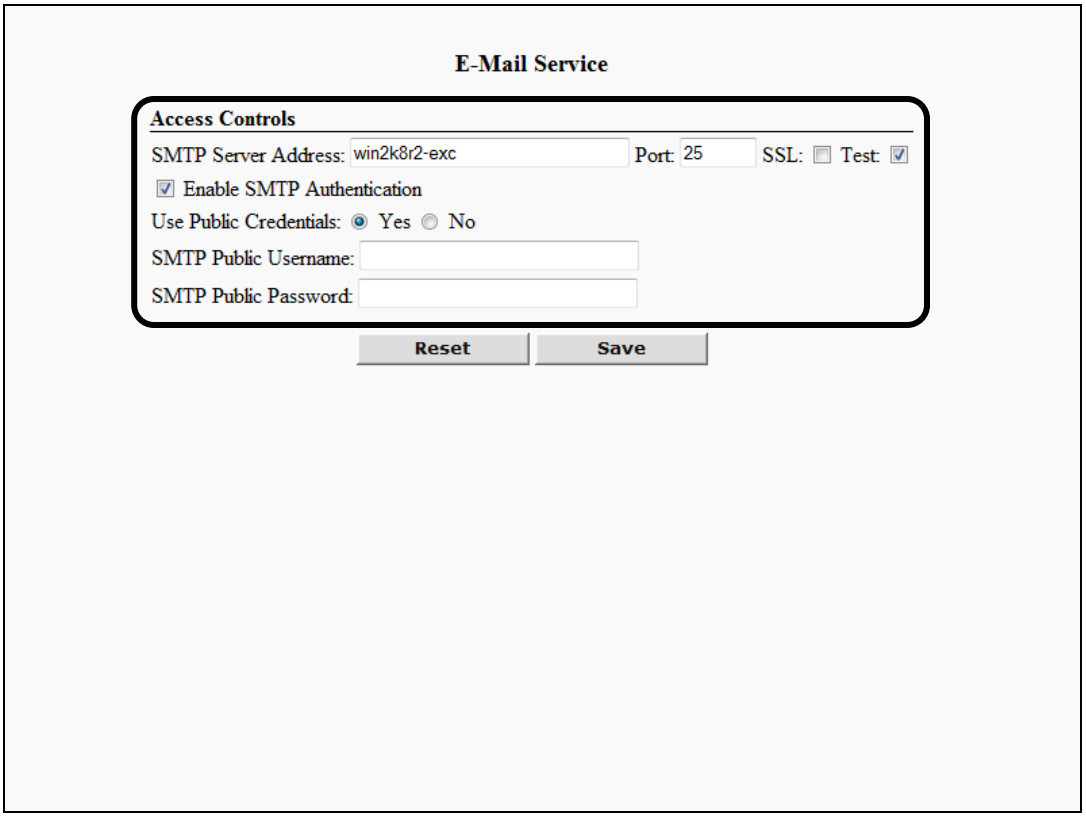
NOTE
The E-Mail Service Settings must be configured to use the Scan to E-Mail and Scan to I-Fax functions.

1. Click [E-Mail Service] → [General].



The E-Mail Service screen is displayed.

2. Configure the settings under <Access Controls>.



Access Controls

SMTP Server Address:	Enter the IP address or DNS name of the SMTP server. For Office 365, the IP address should be smtp.office365.com. For Gmail, the IP address should be smtp.gmail.com.
Port:	Enter the connecting port number of the SMTP server. You can enter a maximum of five numbers. The recommended port number value for the Office 365 server address is '587', and for the Gmail server address is '465' or '587'. The default port number is '25'.
SSL:	Select this check box if you want the authentication server to use SSL. If you select this check box, the connection to the SMTP server is performed over SSL.
Test:	Select this check box if you want the connection to the SMTP server to be verified before you save the settings. The [Test] check box is selected by default.

Enable SMTP Authentication:	Select this check box to have the user authenticated on the SMTP server when using the Scan to E-Mail or Scan to Fax function.

NOTE
It is recommended that this check box be selected if the SMTP server address points to an Office 365 or Gmail server address.

Use Public Credentials:	Select [Yes] to configure the SMTP public credentials (Public User Name, Public Password). If [Yes] is selected, enter the user's SMTP public name and password for SMTP authentication. If [No] is selected, the user's normal sign in credentials are used. The default setting is 'No'.
SMTP Public Username:	This text box is displayed only if the [Use Public Credentials] radio button is set to 'Yes.' If [Yes] is selected for Use Public Credentials, you must enter the user name for SMTP authentication.
SMTP Public Password:	This text box is displayed only if the [Use Public Credentials] radio button is set to 'Yes'. If [Yes] is selected for Use Public Credentials, you must enter the password for SMTP authentication.

3. Click [Save].

   If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

   A message is displayed informing you that the configuration has been saved.

IMPORTANT
- Select the [Test] check box if you want to test the validity of the IP address you entered before saving.
- If validation fails, an error message is displayed. Enter the correct information → click [Save].

NOTE
The [Test] check box is selected by default. If you do not want to test the validity of the address you entered, click the check box to clear the check mark.

2.5.1 Creating an Address Book Server

You can create up to 10 address book Servers.

When you create an address book server, you can either associate it with an authentication server, which has been previously created, or you can create a standalone address book server with no association to an authentication server.

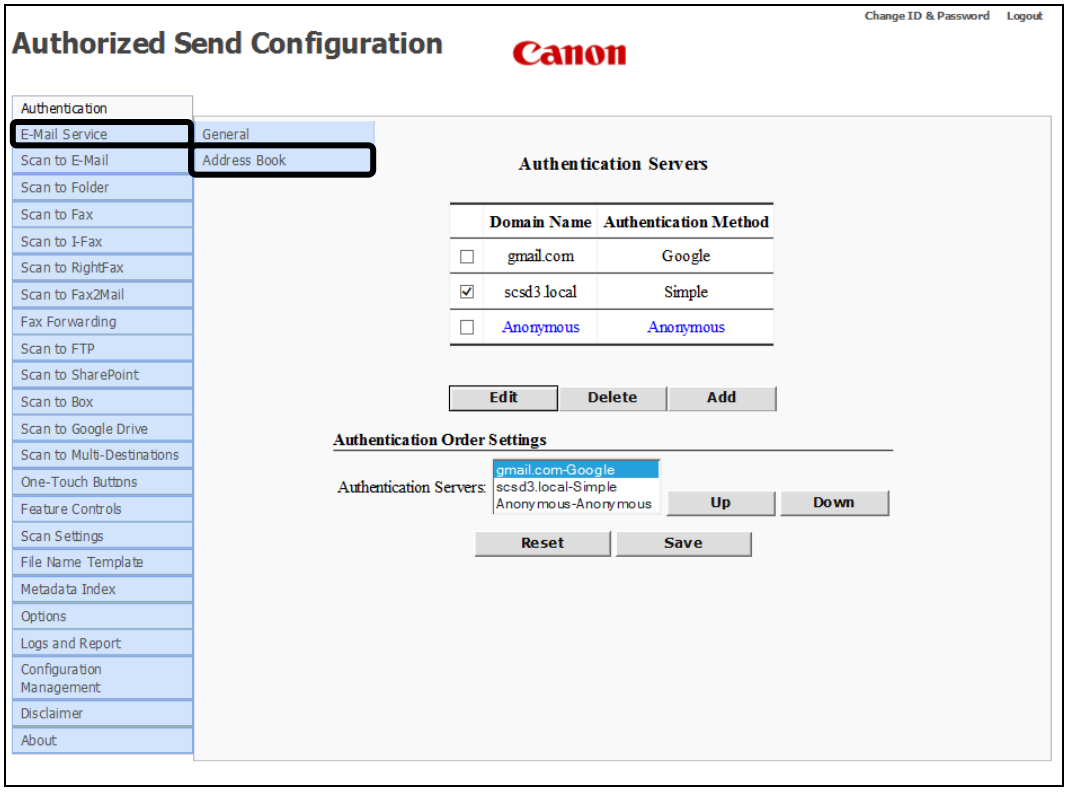
IMPORTANT

- You must configure an address book for an authentication server to retrieve an e-mail address for the user when authenticating against the authentication server.
- If you select the Kerberos protocol for the authentication method, make sure that the device clock setting is properly synchronized with the configured authentication server and address book server. For more information on synchronizing the device clock with the server clock, see "Synchronizing the Device and Server Time," on p. 518.

NOTE

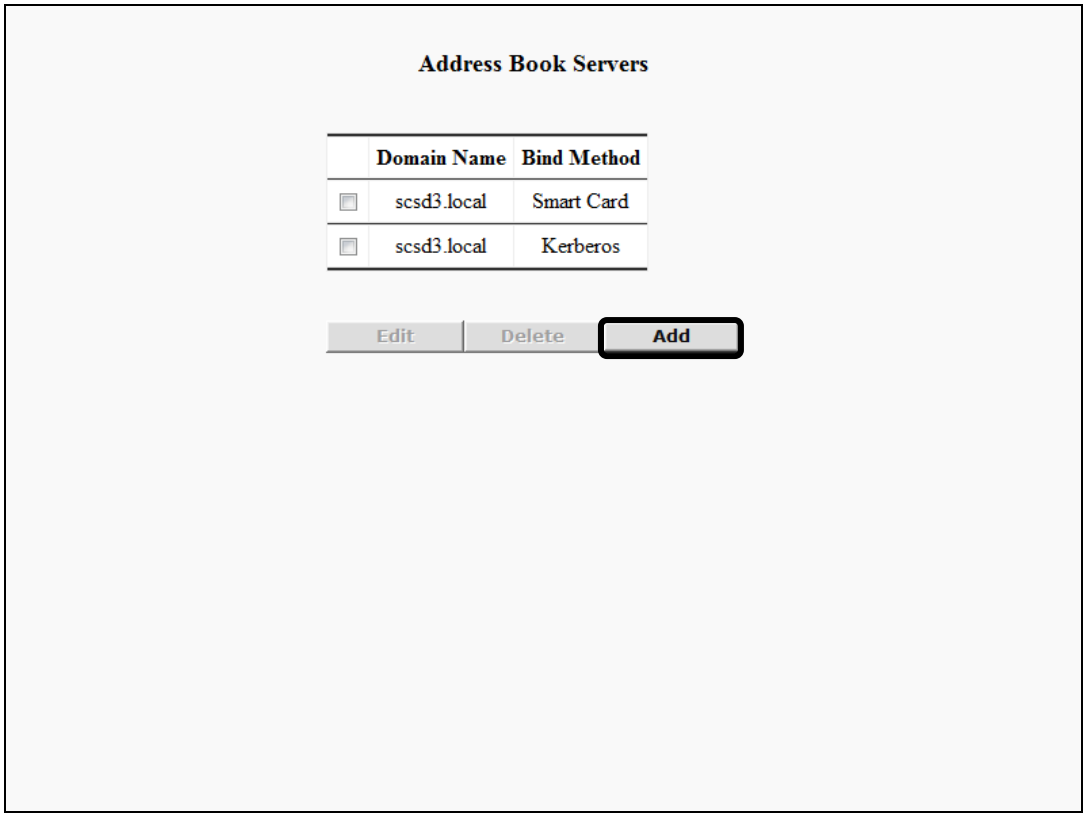
- To associate an address book with an authentication server, you must first create an authentication server for Authorized Send. For instructions on creating an authentication server, see "Creating an Authentication Server," on p. 34.
- This option may be initially set on this screen, as well as configured and edited on the Create Authentication Server screen.
- If you select [None] from the Authentication Server drop-down list when creating an address book server, the address book server is not associated with an authentication server, and does not interact with any other features of Authorized Send. Select [None] if you want to create an address book server that can be configured at a later time.

1. Click [E-Mail Service] ➞ [Address Book].



The Address Book Servers screen is displayed.

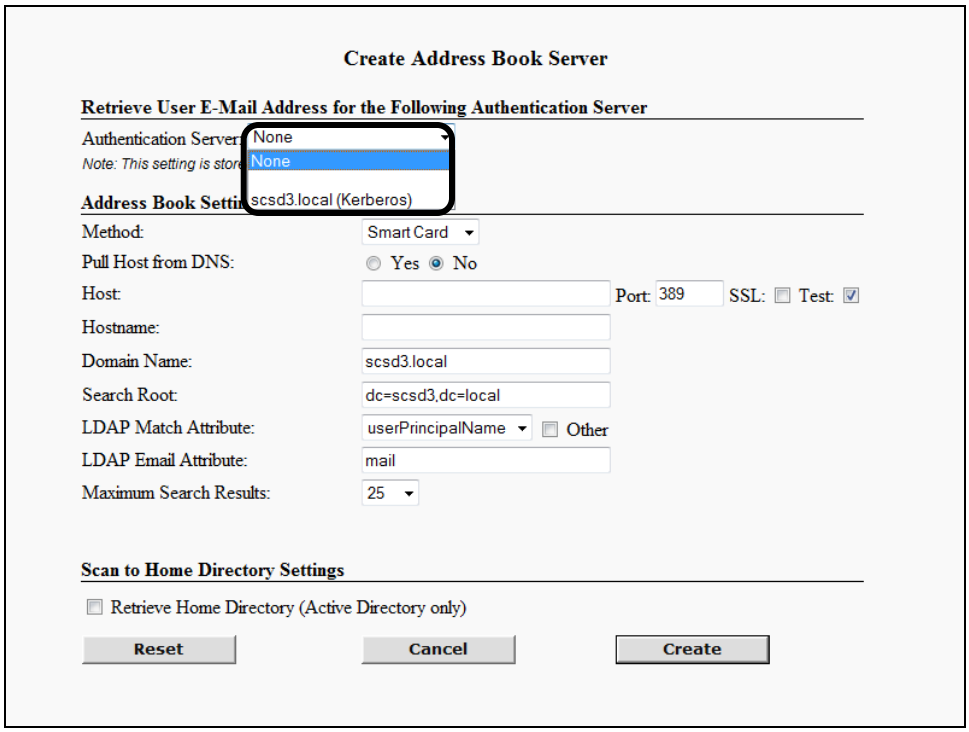
2. Click [Add].



The Create Address Book Server screen is displayed.

3. Specify whether you want to create an address book server with or without an association to an authentication server.

   3.1 If you want to create an address book server with an association to an authentication server, select [Kerberos], [NTLM], [Simple], or [Anonymous] from the Authentication Server drop-down list under <Retrieve User E-Mail Address for the Following Authentication Server>.



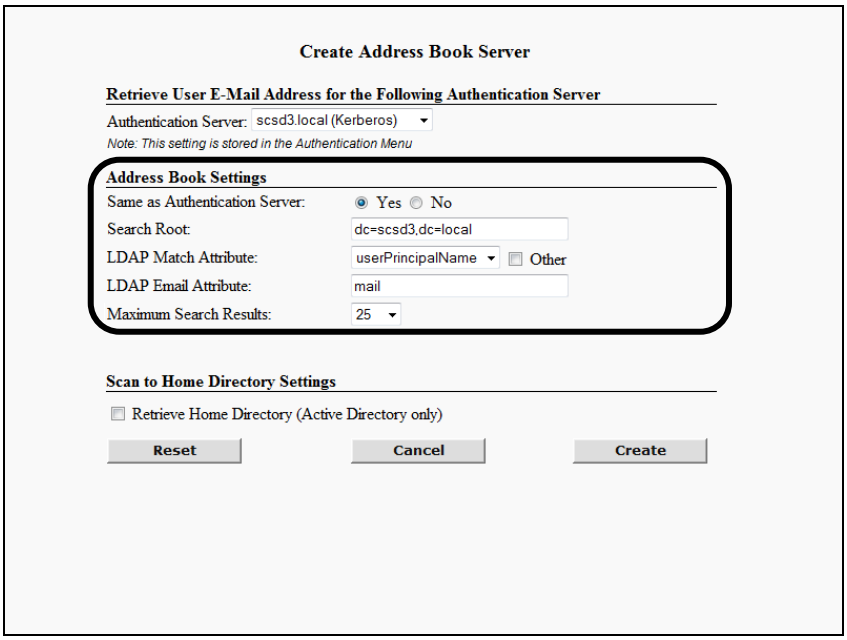
IMPORTANT

If you select [Kerberos], [NTLM], or [Simple] as the authentication server, [Same as Authentication Server] appears as an additional setting under <Address Book Settings>. Select [Yes] to create the address book with the same configuration settings as the selected authentication server. If you select [No], you must enter the configuration information for the authentication method.

NOTE

The items in the Authentication Server drop-down list correspond to previously registered authentication servers.

3.1.1 If you select a Kerberos or NTLM authentication server, configure the Address Book Settings and Scan to Home Directory Settings ➞ proceed to step 5.



Address Book Settings

Same as Authentication Server: Select [Yes] to create the address book with the same configuration settings as the selected authentication server. If you select [No], proceed to step 4 and enter the configuration information for the authentication method.

NOTE

Although step 4 shows a standalone address book server with no association to an authentication server, the configuration information is identical to if you were creating an address book server with an association to an authentication server (except for selecting [None] for the authentication server and not displaying [Same as Authentication Server]).

Search Root: Specify the search root for searching the user's home directory via LDAP.

Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts.

[Search Root] only appears if the [Retrieve Home Directory (Active Directory only)] check box is selected.

The default value for the Search Root text box is blank if the Domain Name text box is blank. If the Domain Name text box is populated, the Search Root text box is automatically populated based on the text entered in the Domain Name text box.

LDAP Match Attribute: Select [sAMAccountName], [userPrincipalName], or [uid] from the drop-down list to determine which attribute to use for LDAP match. The default setting is 'sAMAccountName'.

Other:	If you select this check box, the LDAP Match Attribute drop-down list becomes a text box, where you can enter the LDAP Match Attribute to be used for e-mail address retrieval. You can enter a string that consists of any character, and an unlimited number of characters. If the [Retrieve Home Directory (Active Directory only)] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval.
LDAP Email Attribute:	Enter the e-mail LDAP attribute to pull the user's e-mail address. An example for Active Directory is 'mail'.
Maximum Search Results:	Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the Authorized Send ADDRESS BOOK screen on the machine. The default setting is '25'.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user's home directory information from the address book server with the LDAP attribute of "Home Directory." This creates a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

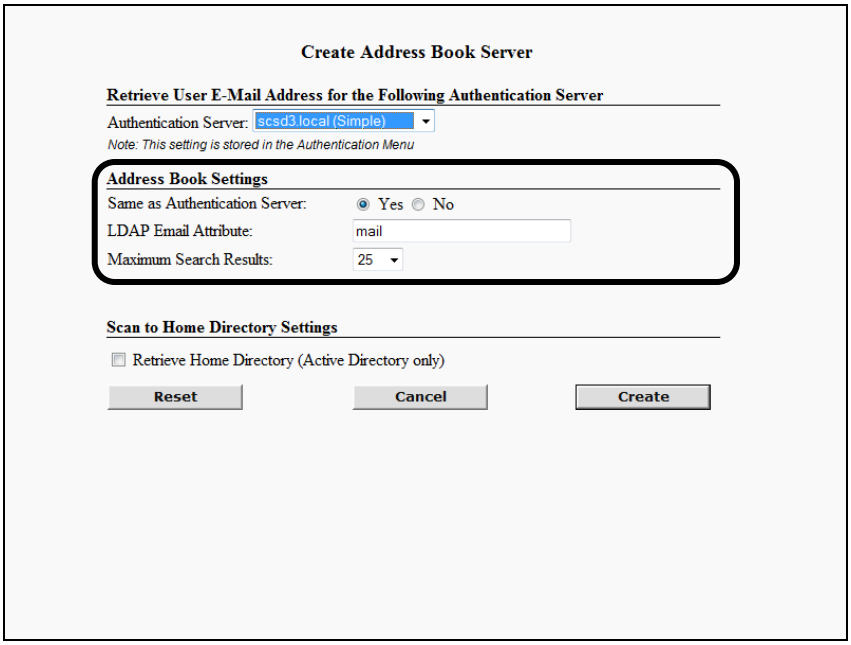
IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

IMPORTANT

If you select the Kerberos protocol for the authentication method, make sure that the device clock setting is properly synchronized with the configured authentication server and address book server. For more information on synchronizing the device clock with the server clock, see "Synchronizing the Device and Server Time," on p. 518.

3.1.2 If you select a Simple authentication server, configure the Address Book Settings and Scan to Home Directory Settings → proceed to step 5.



Address Book Settings

Same as Authentication Server: Select [Yes] to create the address book with the same configuration settings as the selected authentication server. If you select [No], proceed to step 4 and enter the configuration information for the authentication method.

NOTE

Although step 4 shows a standalone address book server with no association to an authentication server, the configuration information is identical to if you were creating an address book server with an association to an authentication server (except for selecting [None] for the authentication server and not displaying [Same as Authentication Server]).

LDAP Email Attribute:	Enter the e-mail LDAP attribute to pull the user's e-mail address. An example for Active Directory is 'mail'.
Maximum Search Results:	Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the Authorized Send ADDRESS BOOK screen on the machine. The default setting is '25'.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user's home directory information from the address book server with the LDAP attribute of "Home Directory." This creates a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

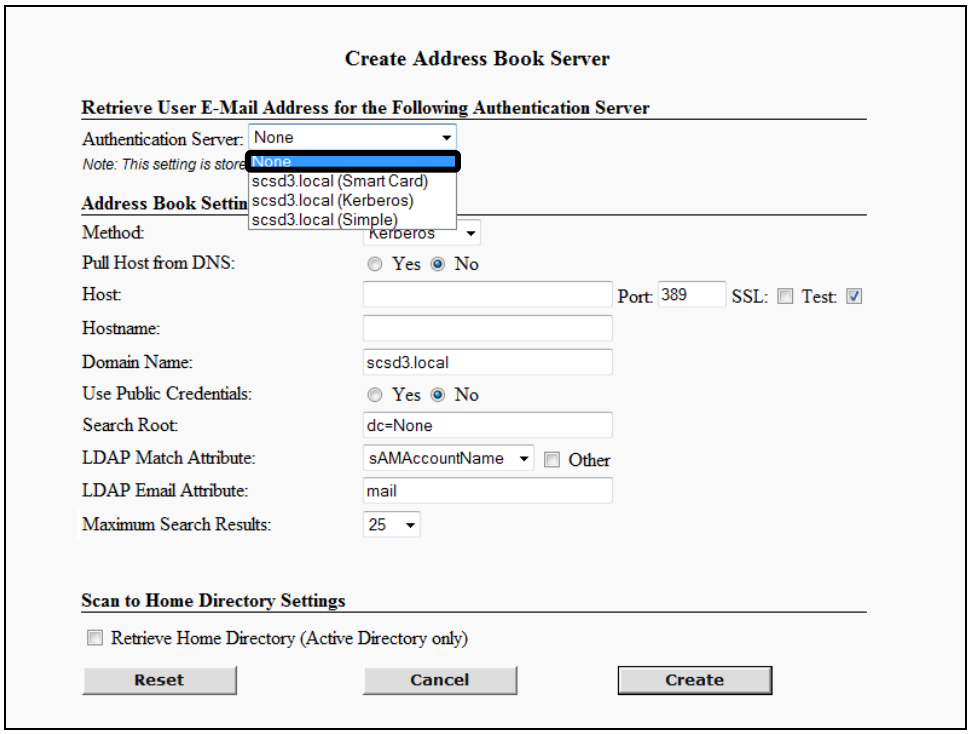
If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

3.1.3 If you select an Anonymous authentication server, proceed to step 4 and enter the configuration information for the authentication method.

NOTE

Although step 4 shows a standalone address book server with no association to an authentication server, the configuration information is identical to if you were creating an address book server with an association to an authentication server (except for selecting [None] for the authentication server and not displaying [Same as Authentication Server]).

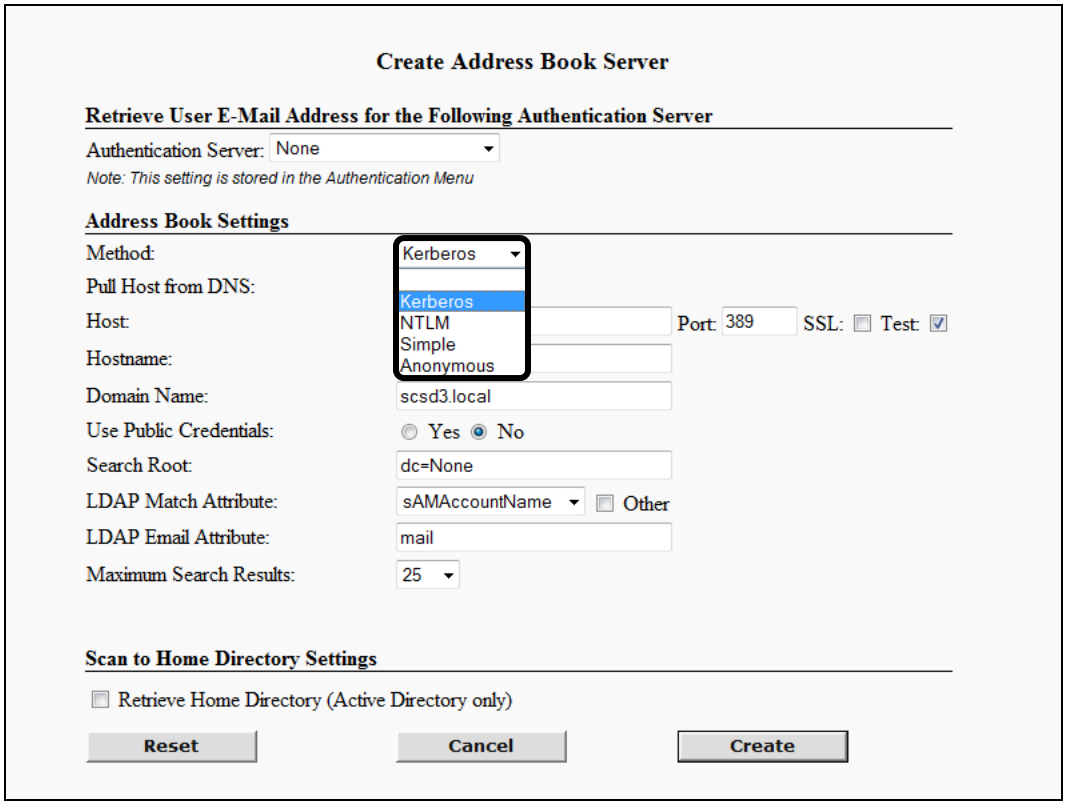
3.2 If you want to create a standalone address book server with no association to an authentication server, select [None] from the Authentication Server drop-down list under <Retrieve User E-Mail Address for the Following Authentication Server>.



NOTE

- The items in the Authentication Server drop-down list correspond to previously registered authentication servers.
- If you select [None] from the Authentication Server drop-down list, the address book server you create is not associated with an authentication server and does not interact with any other features of Authorized Send. Select [None] if you want to create an address book server that can be configured at a later time.

4. Select the authentication method from the Method drop-down list.



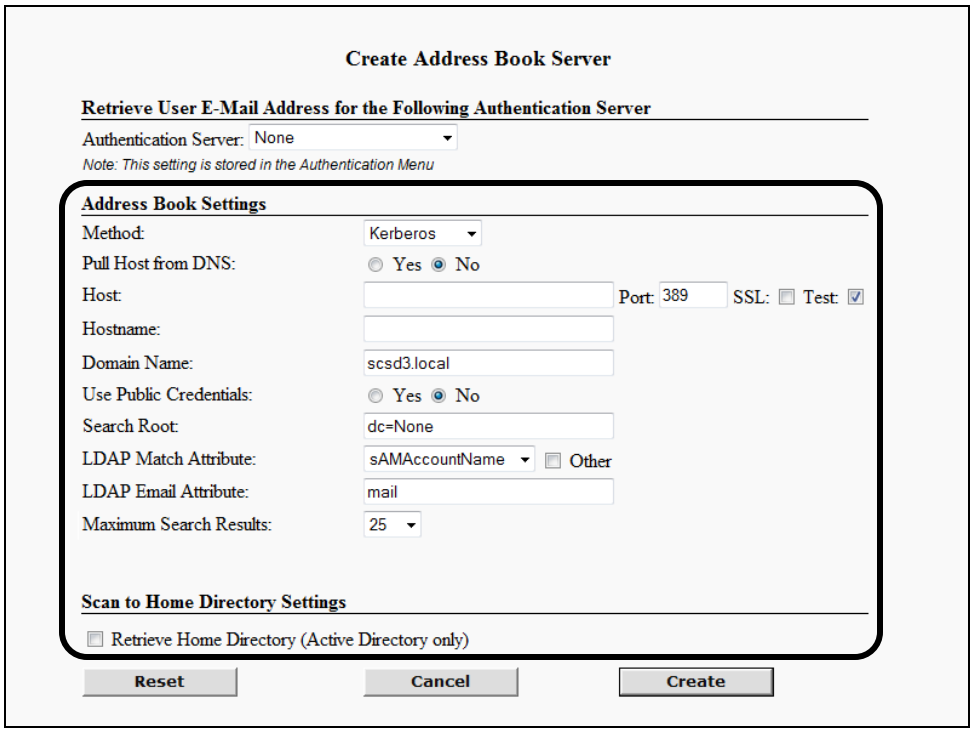
Kerberos: The machine communicates directly to Active Directory.

NTLM: The machine communicates directly to Active Directory.

Simple: Necessary, if you use Domino or eDirectory for authentication.

Anonymous: Authorized Send uses no user login credentials to search the address book for e-mail addresses.

4.1 If you select [Kerberos] as the authentication method, configure the Address Book Settings and Scan to Home Directory Settings.



Address Book Settings

Method: Kerberos

Pull Host from DNS: Select [Yes] to automatically pull the host information from the DNS after you click [Create]. Select [No] if you want to manually configure the host information. The default setting is 'No'.

If you select the [Yes] radio button, the first "live" domain controller is used as the address book server after you click [Create].

Pull Port from DNS: This setting is only displayed when Pull Host from DNS is set to 'Yes'. Select this check box if you want the Port text box to be dynamically populated from the DNS.

Host: This text box is displayed only if Pull Host from DNS is set to 'No'. Enter the DNS name or IP address of the address book server.

Port:	This text box is displayed only if Pull Host from DNS is set to ‘No’, and if the [Pull Port from DNS] check box is not selected. Enter the connecting port number of the address book server. You can enter a maximum of five numbers. The default port number is ‘389’.
SSL:	This check box is displayed only if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Select this check box if you want the address book server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.
Test:	This check box is displayed only if Pull Host from DNS is set to ‘No’. Select this check box if you want the connection to the address book server to be verified before you save the settings. The [Test] check box is selected by default.
Hostname:	This text box is displayed only if Pull Host from DNS is set to ‘No’. Enter the host name of the address book server.
Domain Name:	Enter the address book server domain for this device. The default value is pulled from the device.
Use Public Credentials:	Select [Yes] to use the public credentials (Public User Name and Public Password) configured by the System Administrator. Select [No] to use Anonymous binding. The default setting is ‘No’.
Public User Name:	This text box is displayed only if Use Public Credentials is set to ‘Yes’. If [Yes] is selected for Use Public Credentials, you must enter the user name for authentication against the address book server. You can enter a string that consists of any character, and an unlimited number of characters.
Public Password:	This text box is displayed only if Use Public Credentials is set to ‘Yes’. It is used as the password for authentication against the address book server. It is an optional text box. You can enter a string that consists of any character, and an unlimited number of characters.

Search Root:	Specify the search root for searching the user's home directory via LDAP. Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. The default value for the Search Root text box is blank if the Domain Name text box is blank. If the Domain Name text box is populated, the Search Root text box is automatically populated, based on the text entered in the Domain Name text box.
LDAP Match Attribute:	Select [sAMAccountName], [userPrincipalName], or [uid] from the drop-down list to determine which attribute to use for LDAP match. The default setting is 'sAMAccountName'.
Other:	If you select this check box, the LDAP Match Attribute drop-down list becomes a text box, where you can enter the LDAP Match Attribute to be used for e-mail address retrieval. You can enter a string that consists of any character, and an unlimited number of characters. If the [Retrieve Home Directory (Active Directory only)] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval.
LDAP Email Attribute:	Enter the e-mail LDAP attribute to pull the user's e-mail address. An example for Active Directory is 'mail'.
Maximum Search Results:	Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the Authorized Send ADDRESS BOOK screen on the machine. The default setting is '25'.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user's home directory information from the address book server with the LDAP attribute of "Home Directory." This creates a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

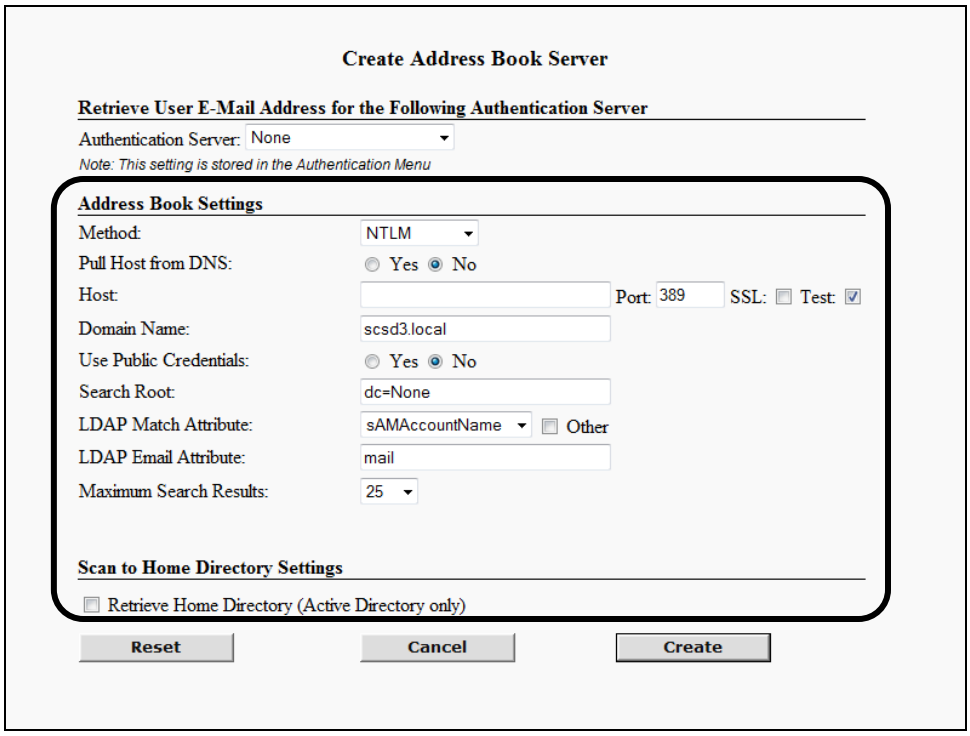
IMPORTANT

- If you select the Kerberos protocol for the authentication method, make sure that the device clock setting is properly synchronized with the configured authentication server and address book server. For more information on synchronizing the device clock with the server clock, see "Synchronizing the Device and Server Time," on p. 518.
- Select the [Test] check box if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message is displayed. Enter the correct information → click [Save].

NOTE

The [Test] check box is selected by default. If you do not want to test the validity of the addresses you entered, click the check box to clear the check mark.

4.2 If you select [NTLM] as the authentication method, configure the Address Book Settings and Scan to Home Directory Settings.



Address Book Settings

Method:	NTLM
Pull Host from DNS:	Select [Yes] to automatically pull the host information from the DNS after you click [Create]. Select [No] if you want to manually configure the host information. The default setting is 'No'. If you select the [Yes] radio button, the first "live" domain controller is used as the address book server after you click [Create].
Pull Port from DNS:	This setting is only displayed when Pull Host from DNS is set to 'Yes'. Select this check box if you want the Port text box to be dynamically populated from the DNS.
Pulled Host:	This field is only displayed when Pull Port from DNS is set to 'Yes'. The text displayed is the FQDN of the machine.
Pulled Hostname:	This field is only displayed when Pull Port from DNS is set to 'Yes'. The text displayed is a truncated version of the machine's name.
Host:	This text box is displayed only if Pull Host from DNS is set to 'No'. Enter the DNS name or IP address of the address book server.
Port:	This text box is displayed only if Pull Host from DNS is set to 'No' and if the [Pull Port from DNS] check box is not selected. Enter the connecting port number of the address book server. You can enter a maximum of five numbers. The default port number is '389'.
SSL:	This check box is displayed only if Pull Host from DNS is set to 'No' and if the [Pull Port from DNS] check box is not selected. Select this check box if you want the address book server to use SSL. If you select this check box, the host port number automatically changes to '636'.
Test:	This check box is displayed only if Pull Host from DNS is set to 'No'. Select this check box if you want the connection to the address book server to be verified before you save the settings. The [Test] check box is selected by default.

Domain Name:	Enter the address book server domain for this device. The default value is pulled from the device.
Use Public Credentials:	Select [Yes] to use the public credentials (Public User Name and Public Password) configured by the System Administrator. Select [No] to use Anonymous binding. The default setting is 'No'.
Public User Name:	This text box is displayed only if Use Public Credentials is set to 'Yes'. If [Yes] is selected for Use Public Credentials, you must enter the user name for authentication against the address book server. You can enter a string that consists of any character, and an unlimited number of characters.
Public Password:	This text box is displayed only if Use Public Credentials is set to 'Yes'. It is used as the password for authentication against the address book server. It is an optional text box. You can enter a string that consists of any character, and an unlimited number of characters.
Search Root:	Specify the search root for searching the user's home directory via LDAP. Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. The default value for the Search Root text box is blank if the Domain Name text box is blank. If the Domain Name text box is populated, the Search Root text box is automatically populated based on the text entered in the Domain Name text box.
LDAP Match Attribute:	Select [sAMAccountName], [userPrincipalName], or [uid] from the drop-down list to determine which attribute to use for LDAP match. The default setting is 'sAMAccountName'.

Other:	If you select this check box, the LDAP Match Attribute drop-down list becomes a text box, where you can enter the LDAP Match Attribute to be used for e-mail address retrieval. You can enter a string that consists of any character, and an unlimited number of characters. If the [Retrieve Home Directory (Active Directory only)] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval.
LDAP Email Attribute:	Enter the e-mail LDAP attribute to pull the user's e-mail address. An example for Active Directory is 'mail'.
Maximum Search Results:	Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the Authorized Send ADDRESS BOOK screen on the machine. The default setting is '25'.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user's home directory information from the address book server with the LDAP attribute of "Home Directory." This creates a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

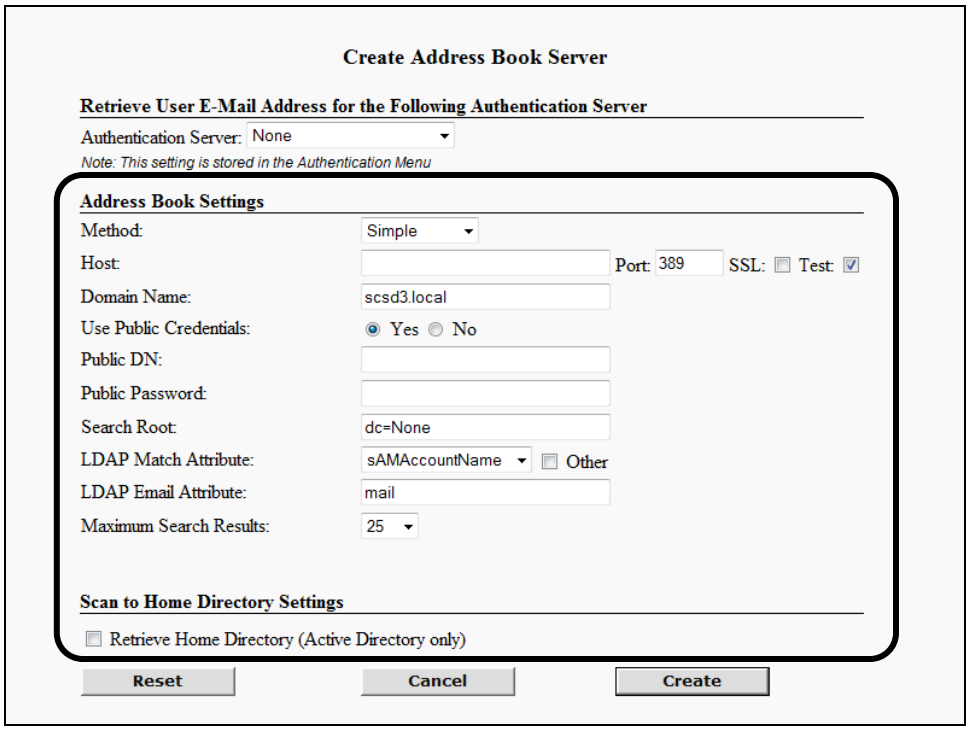
IMPORTANT

- Select the [Test] check box if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message is displayed. Enter the correct information → click [Save].

NOTE

The [Test] check box is selected by default. If you do not want to test the validity of the addresses you entered, click the check box to clear the check mark.

4.3 If you select [Simple] as the authentication method, configure the Address Book Settings and Scan to Home Directory Settings.



Address Book Settings

Method: Simple

Host: Enter the DNS name or IP address of the address book server.

Port: Enter the connecting port number of the address book server. You can enter a maximum of five numbers. The default port number is ‘389’.

SSL: Select this check box if you want the address book server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.

Test: Select this check box if you want the connection to the address book server to be verified before you save the settings. The [Test] check box is selected by default.

Domain Name: Enter the address book server domain for this device. The default value is pulled from the device.

Use Public Credentials:	Select [Yes] to configure the public credentials (Public DN and Public Password), or select [No] to use anonymous binding. The default setting is ‘No’.
Public DN:	This text box is displayed only if Use Public Credentials is set to ‘Yes’. If Use Public Credentials is set to ‘Yes’, you must enter the user’s login Distinguished Name to use when performing the first bind of the Simple Binding process.
Public Password:	This text box is displayed only if Use Public Credentials is set to ‘Yes’. It is used as the password for authentication against the address book server. It is an optional text box. You can enter a string that consists of any character, and an unlimited number of characters.
Search Root:	Specify the search root for searching the user’s home directory via LDAP. Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. The default value for the Search Root text box is blank if the Domain Name text box is blank. If the Domain Name text box is populated, the Search Root text box is automatically populated based on the text entered in the Domain Name text box.
LDAP Match Attribute:	Select [sAMAccountName], [userPrincipalName], or [uid] from the drop-down list to determine which attribute to use for LDAP match. The default setting is ‘sAMAccountName’.
Other:	If you select this check box, the LDAP Match Attribute drop-down list becomes a text box, where you can enter the LDAP Match Attribute to be used for e-mail address retrieval. You can enter a string that consists of any character, and an unlimited number of characters. If the [Retrieve Home Directory (Active Directory only)] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval.

LDAP Email Attribute:	Enter the e-mail LDAP attribute to pull the user's e-mail address. An example for eDirectory and Domino is 'mail'.
Maximum Search Results:	Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the Authorized Send ADDRESS BOOK screen on the machine. The default setting is '25'.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user's home directory information from the address book server with the LDAP attribute of "Home Directory." This creates a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

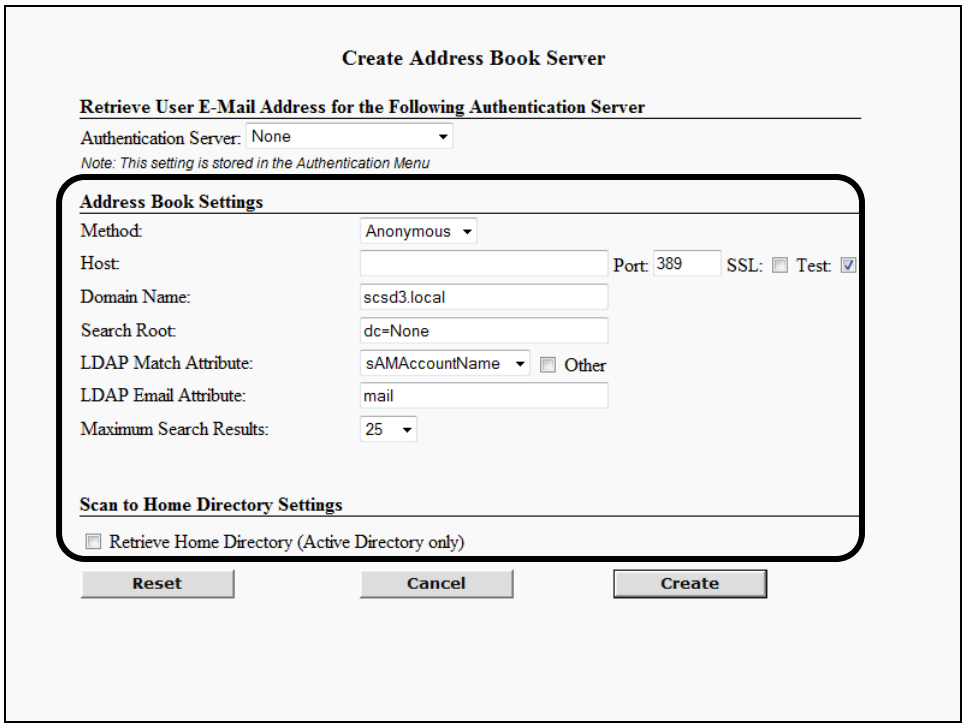
IMPORTANT

- Select the [Test] check box if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message is displayed. Enter the correct information → click [Save].

NOTE

The [Test] check box is selected by default. If you do not want to test the validity of the addresses you entered, click the check box to clear the check mark.

4.4 If you select [Anonymous] as the authentication method, configure the Address Book Settings and Scan to Home Directory Settings.



Address Book Settings

Method: Anonymous

Host: Enter the DNS name or IP address of the address book server.

Port: Enter the connecting port number of the address book server. You can enter a maximum of five numbers. The default port number is ‘389’.

SSL: Select this check box if you want the address book server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.

Test: Select this check box if you want the connection to the address book server to be verified before you save the settings. The [Test] check box is selected by default.

Domain Name: Enter the address book server domain for this device. The default value is pulled from the device.

Search Root:	Specify the search root for searching the user's home directory via LDAP. Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. The default value for the Search Root text box is blank if the Domain Name text box is blank. If the Domain Name text box is populated, the Search Root text box is automatically populated based on the text entered in the Domain Name text box.
LDAP Match Attribute:	Select [sAMAccountName], [userPrincipalName], or [uid] from the drop-down list to determine which attribute to use for LDAP match. The default setting is 'sAMAccountName'.
Other:	If you select this check box, the LDAP Match Attribute drop-down list becomes a text box, where you can enter the LDAP Match Attribute to be used for e-mail address retrieval. You can enter a string that consists of any character, and an unlimited number of characters. If the [Retrieve Home Directory (Active Directory only)] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval.
LDAP Email Attribute:	Enter the e-mail LDAP attribute to pull the user's e-mail address. An example for Active Directory, eDirectory, and Domino is 'mail'.
Maximum Search Results:	Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the Authorized Send ADDRESS BOOK screen on the machine. The default setting is '25'.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user's home directory information from the address book server with the LDAP attribute of "Home Directory." This creates a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

IMPORTANT

- Select the [Test] check box if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message is displayed. Enter the correct information → click [Save].

NOTE

The [Test] check box is selected by default. If you do not want to test the validity of the addresses you entered, click the check box to clear the check mark.

5. Click [Create].

   If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

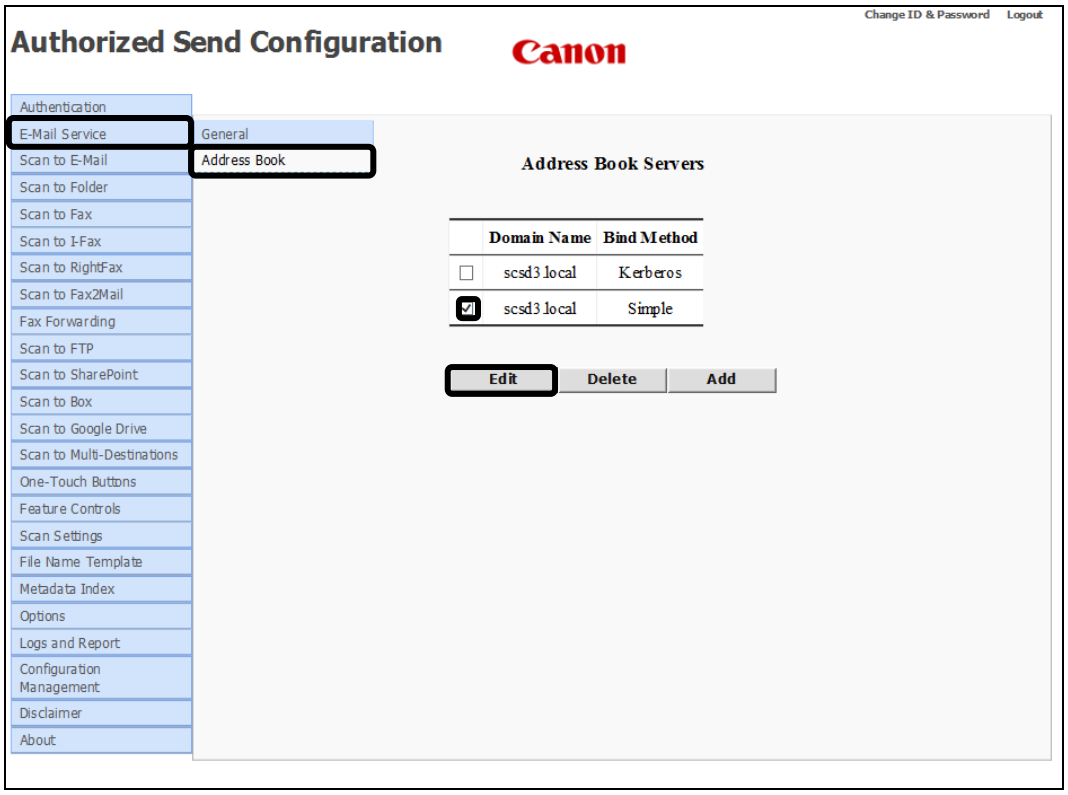
   To cancel creating the address book server and return to the Address Book Servers screen, click [Cancel].

   The address book server is created and added to the address book servers list on the Address Book Servers screen.

2.5.2 Editing an Address Book Server

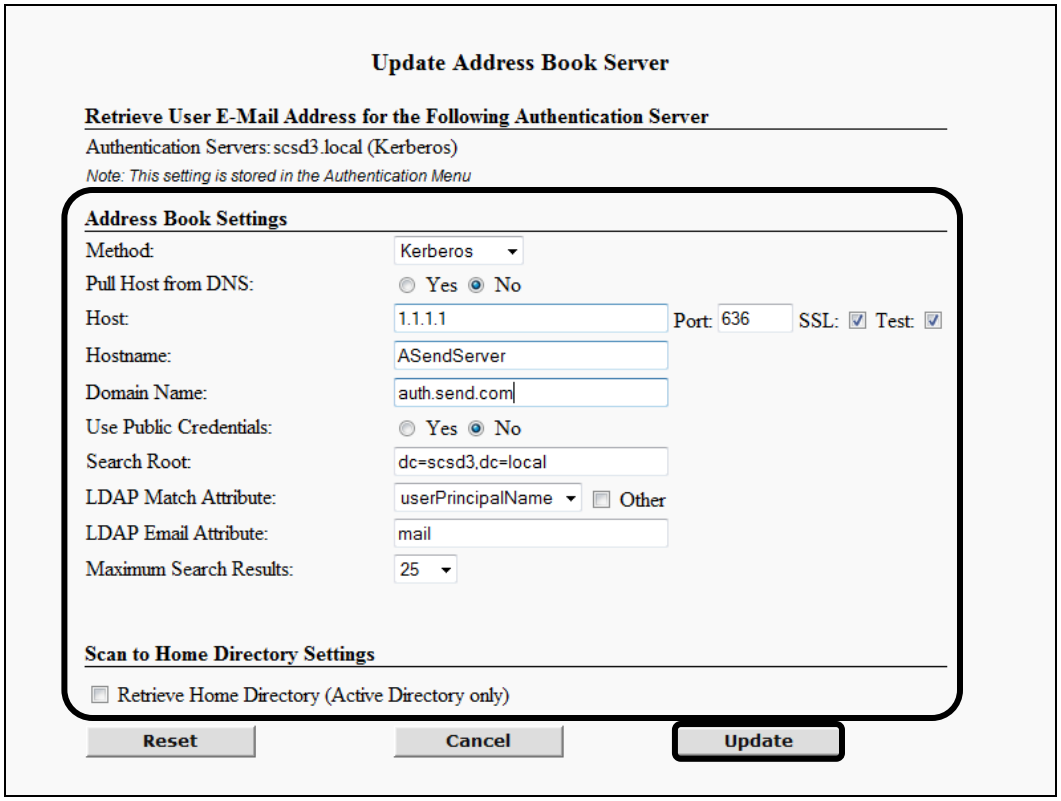
You can edit a previously created address book server from the Address Book Servers configuration screen.

1. Click [E-Mail Service] → [Address Book] → select the check box next to the address book server you want to edit → click [Edit].



The Update Address Book Server screen is displayed.

2. Edit the settings for the address book server as necessary → click [Update].



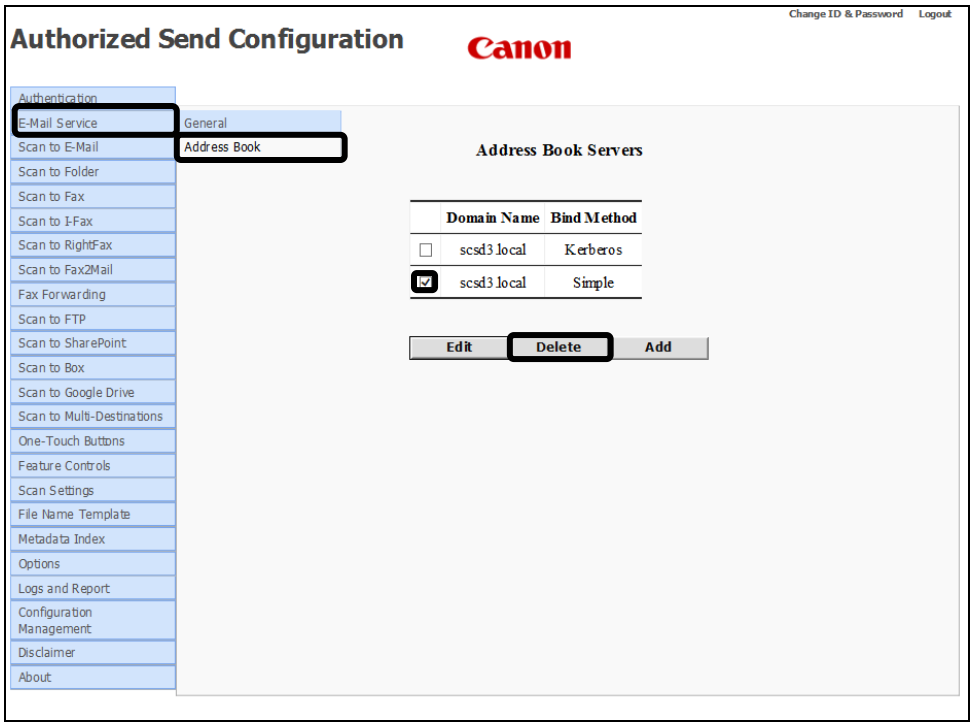
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the address book server and return to the Address Book Servers screen, click [Cancel].

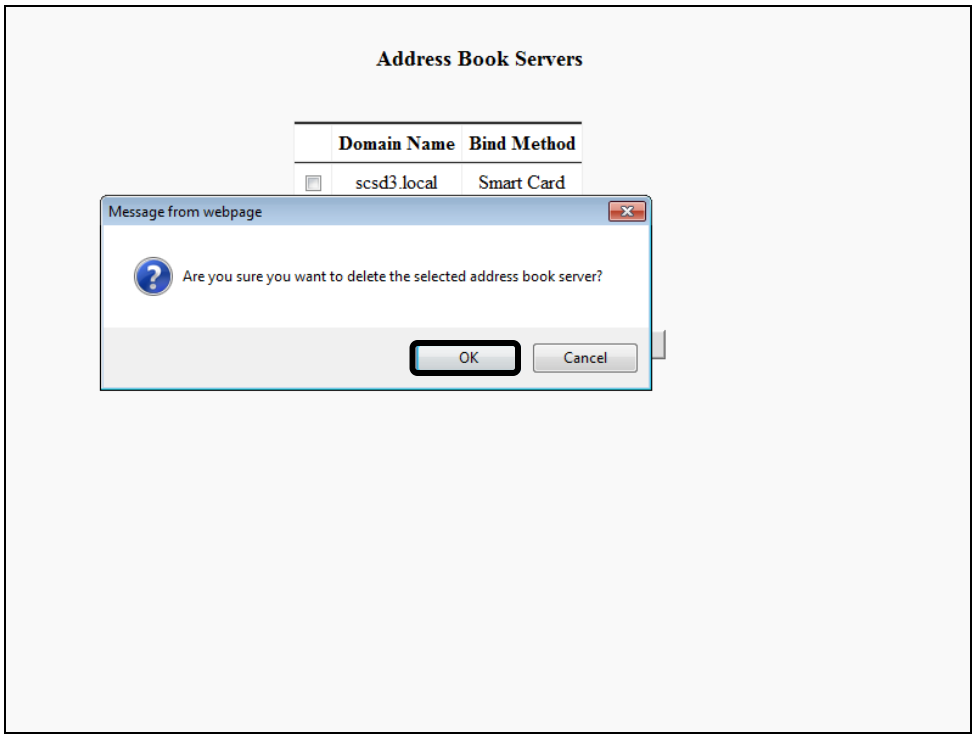
2.5.3 Deleting an Address Book Server

You can delete a previously created address book server from the Address Book Servers configuration screen.

1. Click [E-Mail Service] ➞ [Address Book] ➞ select the check box next to the address book server you want to delete ➞ click [Delete].



2. Click [OK].



If you do not want to delete the address book server, click [Cancel].

The address book server is deleted from the list.

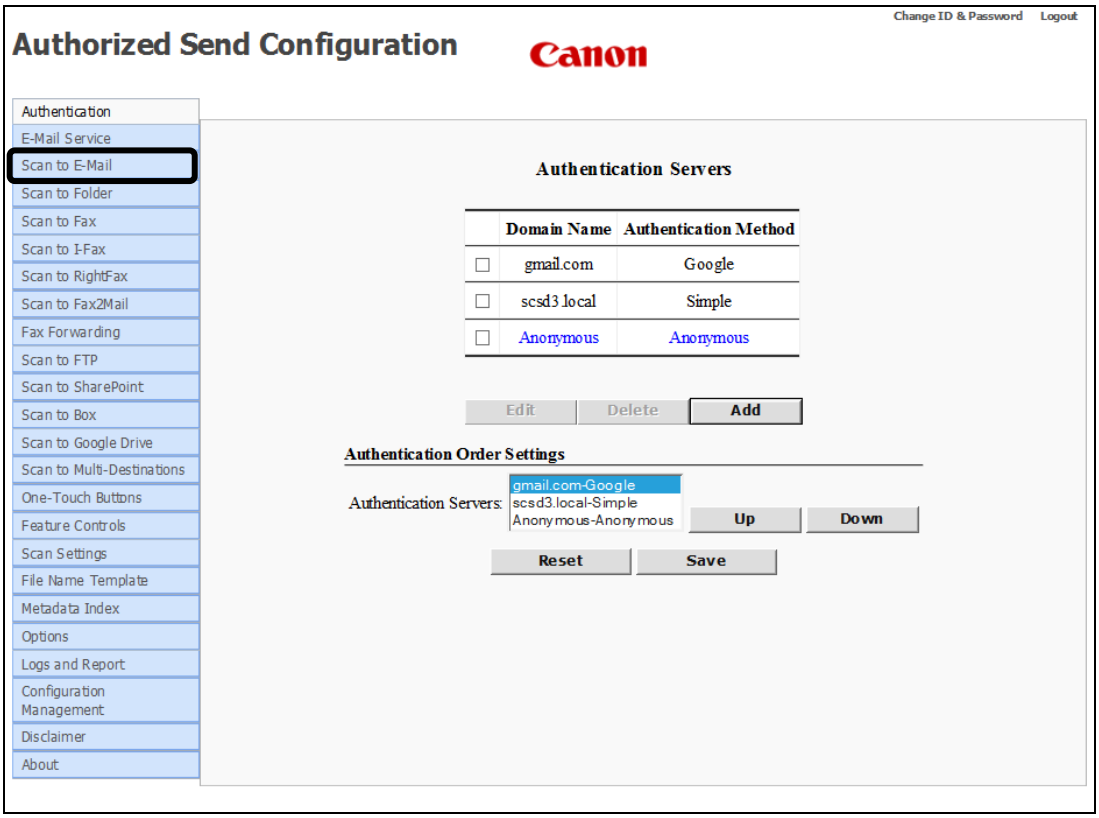
2.6 Configuring the Scan to E-Mail Settings

You can configure the Scan to E-Mail function, which enables users to scan and send documents via an SMTP server.

IMPORTANT

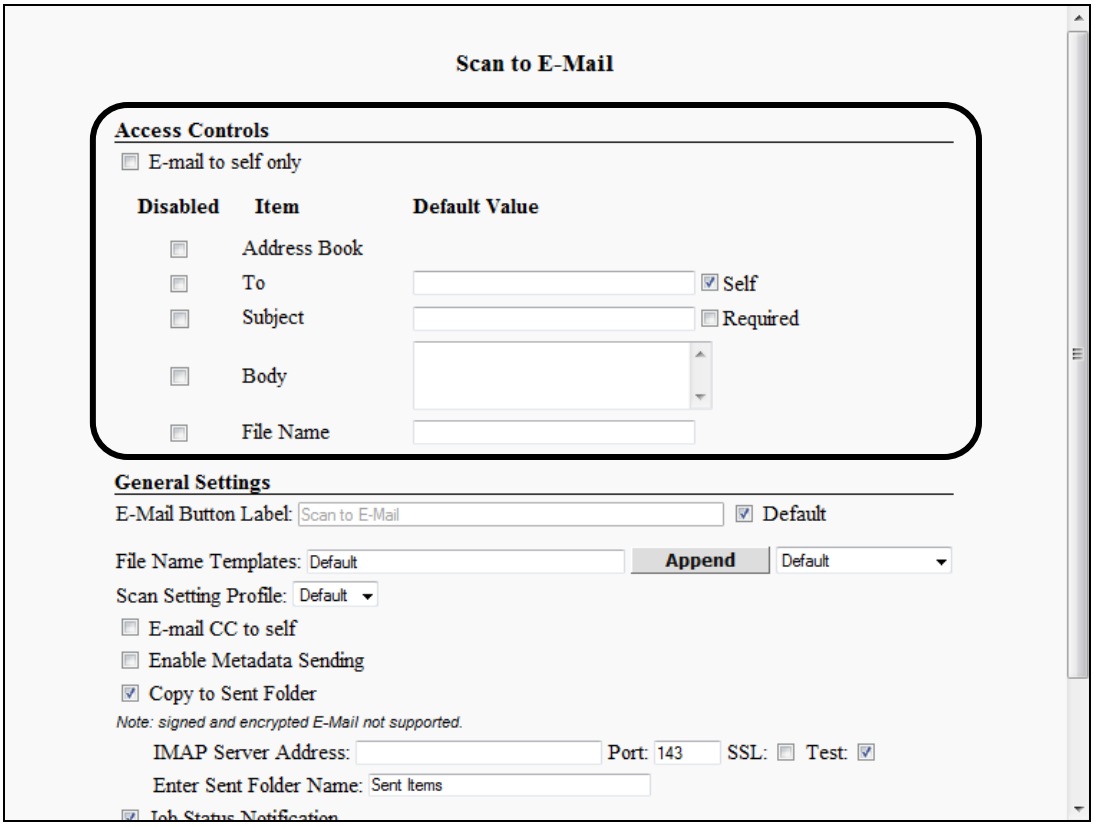
- If an AMS enabled login application is installed and running on the machine, [Scan to E-Mail] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the Scan to E-Mail function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [Scan to E-Mail].



The Scan to E-Mail screen is displayed.

2. Configure the settings under <Access Controls>.



Access Controls

E-mail to self only: Select this check box if you want to restrict users to only send e-mail messages to themselves, and to automatically disable the [Address Book] key and the [To] text box on the Authorized Send SCAN TO E-MAIL screen on the machine.

Disabled Column

Address Book: Select this check box if you want to restrict user access to the [Address Book] key on the Authorized Send SCAN TO E-MAIL screen on the machine. If you select this check box, the [Address Book] key is not displayed on the Authorized Send SCAN TO E-MAIL screen on the machine. The user can manually specify an e-mail address, but cannot select an address from the address book.

To: Select this check box if you want to prevent the user from manually entering an e-mail address. If you select this check box, the [To] text box on the Authorized Send SCAN TO E-MAIL screen on the machine is disabled and grayed out. The user can select an e-mail address from the address book, but cannot manually specify an address.

Self: This check box is displayed only when the [E-mail to self only] check box is not selected. When the [Self] check box is selected, the e-mail address of the user logged on to Authorized Send is displayed in the [To] text box on the Authorized Send SCAN TO E-MAIL screen on the machine. This check box is selected by default.

IMPORTANT

You must select the [Self] check box if you selected the [Address Book] and [To] check boxes at the same time, and the default value for the To text box is blank.

Subject: Select this check box to disable the [Subject] text box on the Authorized Send SCAN TO E-MAIL screen on the machine.

Required: Select this check box if you require the user to enter a subject for their e-mail messages.

Body: Select this check box to disable the [Body] text box on the Authorized Send SCAN TO E-MAIL screen on the machine.

File Name: Select this check box to disable the [File Name] text box on the Authorized Send SCAN TO E-MAIL screen on the machine.

Default Value Column

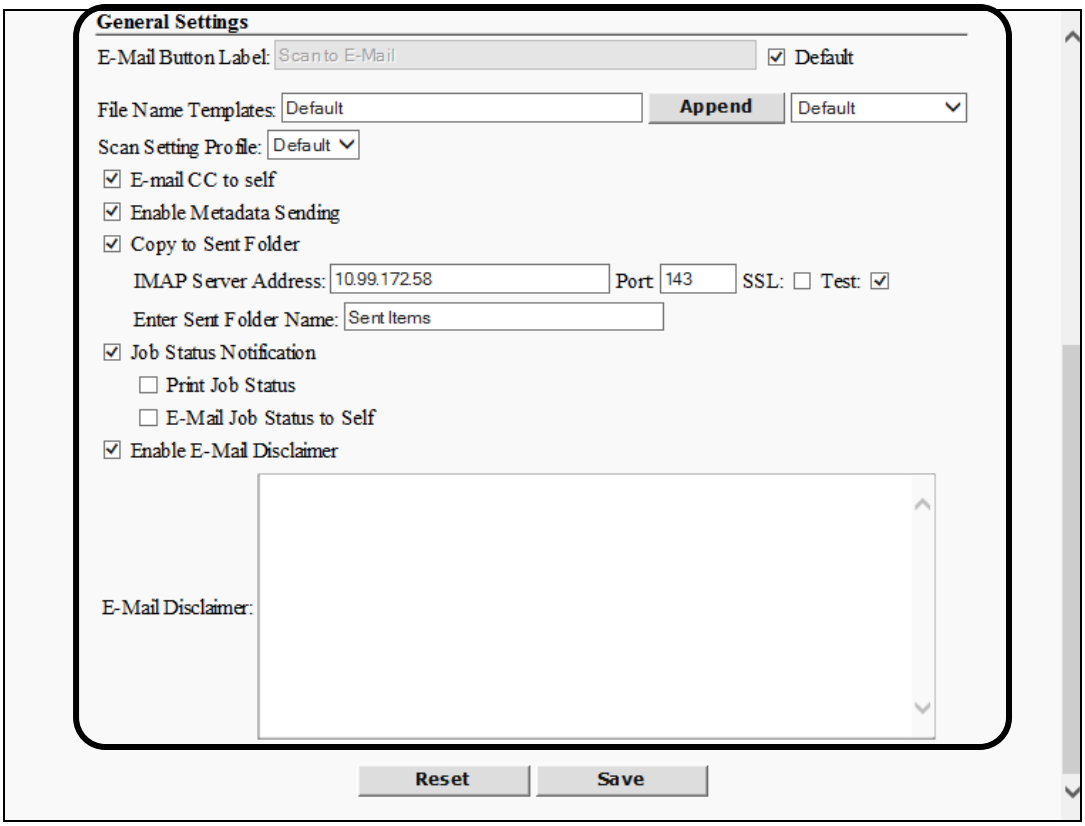
To: Enter the default e-mail address to be displayed in the [To] text box on the Authorized Send SCAN TO E-MAIL screen on the machine. This text box is required only if the [Address Book] and [To] check boxes are selected, and the [Self] check box is not selected. You can enter a string that consists of any character, and an unlimited number of characters.

Subject: Enter a default subject to be displayed in the [Subject] text box on the Authorized Send SCAN TO E-MAIL screen on the machine. This text box is required only if the [Subject] and [Required] check boxes are selected. You can enter a string that consists of any character, and a maximum number of 255 characters.

Body: Enter a default e-mail message to be displayed in the [Body] text box on the Authorized Send SCAN TO E-MAIL screen on the machine. This scrolling box is optional. You can enter a string that consists of any character, and a maximum number of 255 characters.

File Name: Enter the default file name to be displayed in the [File Name] text box on the Authorized Send SCAN TO E-MAIL screen on the machine. This text box is optional. You can enter a string that consists of any character, and a maximum number of 251 characters.

3. Configure the settings under <General Settings>.



General Settings

E-Mail Button Label: Enter the label for the [Scan to E-Mail] key that appears on the Authorized Send MAIN screen on the machine. It is a required text box that cannot be left blank. The number of any characters permitted is restricted by the width of the Scan to E-Mail icon.

Default: Select this check box if you want to use the default E-Mail Button Label setting ('Scan to E-Mail'). The E-Mail Button Label text box cannot be changed when the Default check box is selected.

File Name Templates: Enter one or more File Name Templates which the user can select when creating a scan job. The names in this list are created under the <File Name> tab. See "Configuring the File Name," on p. 407. The default value is 'Default'. Separate entries must be separated by commas. You can enter the File Name Templates manually or select the Templates from the Append drop-down list and click [Append].

Append:	Click [Append] to add a File Name Template (set in the Append drop-down list) to the string in the [File Name Templates] text box.
Append drop-down:	Select a pre-defined File Name Template that is added to the string in the [File Name Templates] text box after you click [Append].
E-mail CC to self:	Select this check box if you want a copy of each e-mail message sent via the Authorized Send SCAN TO E-MAIL screen on the machine to be sent to the currently logged on user's e-mail address. This check box is selected by default.
Enable Metadata Sending:	Select this check box if you want all scans sent using the Scan to E-Mail function to be accompanied by an XML file, which contains metadata as defined on the Metadata Index screen. This check box is not selected by default.
Copy to Sent Folder:	Select this check box if you want all e-mail messages sent from the Authorized Send SCAN TO E-MAIL screen on the machine to send a copy to the Exchange mail server's Sent folder. This check box is not selected by default.
IMAP Server Address:	This text box is displayed only if the [Copy to Sent Folder] check box is selected. Enter the IP address or DNS name of the IMAP server. The default value is pulled from the value entered in the [SMTP Server Address] text box on the E-Mail Service screen.
Port:	This text box is displayed only if the [Copy to Sent Folder] check box is selected. Enter the connecting port number of the IMAP server. You can enter a maximum of five numbers. The default port number is '143'.
SSL:	This check box is displayed only if the [Copy to Sent Folder] is selected. Select this check box if you want the connection to the IMAP server to be over the IMAPS protocol and port. If you select this check box, the port number automatically changes to '993'.
Test:	This check box is displayed only if the [Copy to Sent Folder] is selected. Select this check box if you want the connection to the IMAP server to be verified before you save the settings. The [Test] check box is selected by default.

Enter Sent Folder Name:	This text box is displayed only if the [Copy to Sent Folder] check box is selected. Enter the name of the destination folder on the target IMAP server where the scanned documents are sent by Authorized Send. The default setting is ‘Sent Items’.
Job Status Notification:	Select this check box if you want the logged on user of the Scan to E-Mail session to receive confirmation printout or email.
Print Job Status:	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to E-Mail session to receive a confirmation printout.
E-Mail Job Status to Self:	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to E-Mail session to receive a confirmation email.
Enable E-Mail Disclaimer:	Select this check box to append a disclaimer message to all Scan to E-Mail jobs. The disclaimer appears after the main body of text. This check box is unselected by default
E-Mail Disclaimer:	Enter the text to append to Scan to E-Mail jobs in the [E-Mail Disclaimer] text box. The text box must have at least one character and no more than 5,000 characters. The [E-Mail Disclaimer] text box appears only if the [Enable E-Mail Disclaimer] check box is enabled.

4. Click [Save].

NOTE
If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

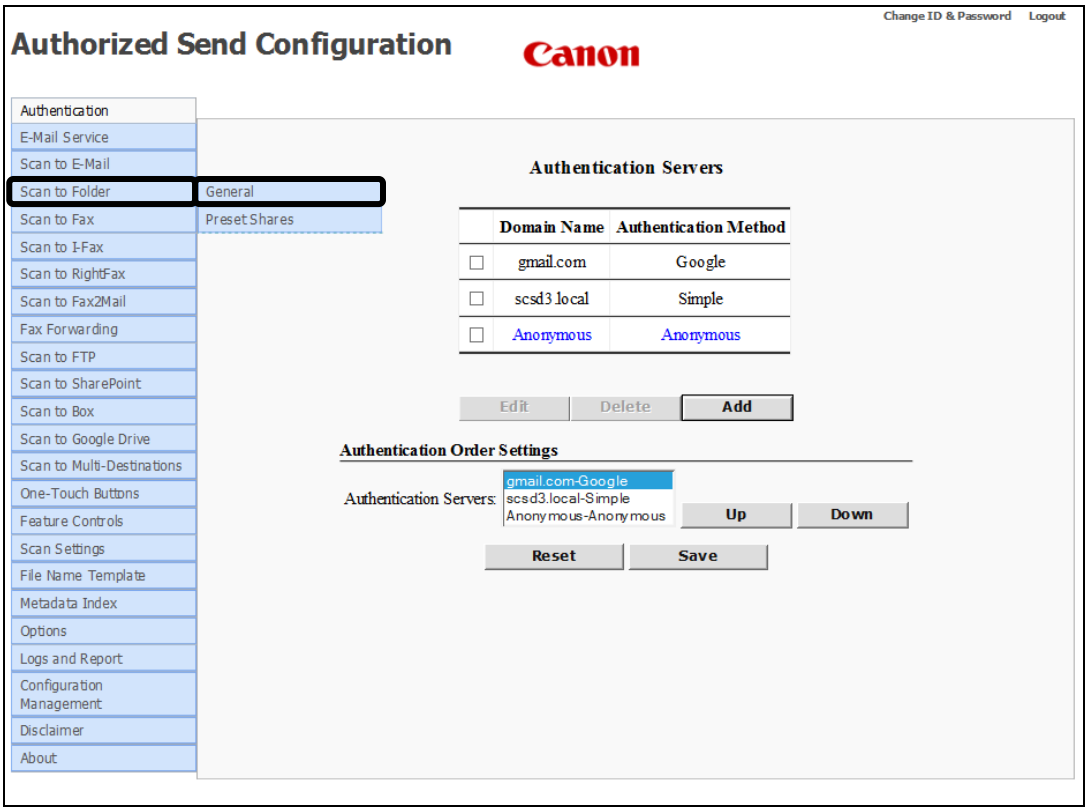
2.7 Configuring the Scan to Folder Settings

You can configure the Scan to Folder function, which enables users to scan and send documents to a specified folder or directory on the network, and create preset shares.

IMPORTANT

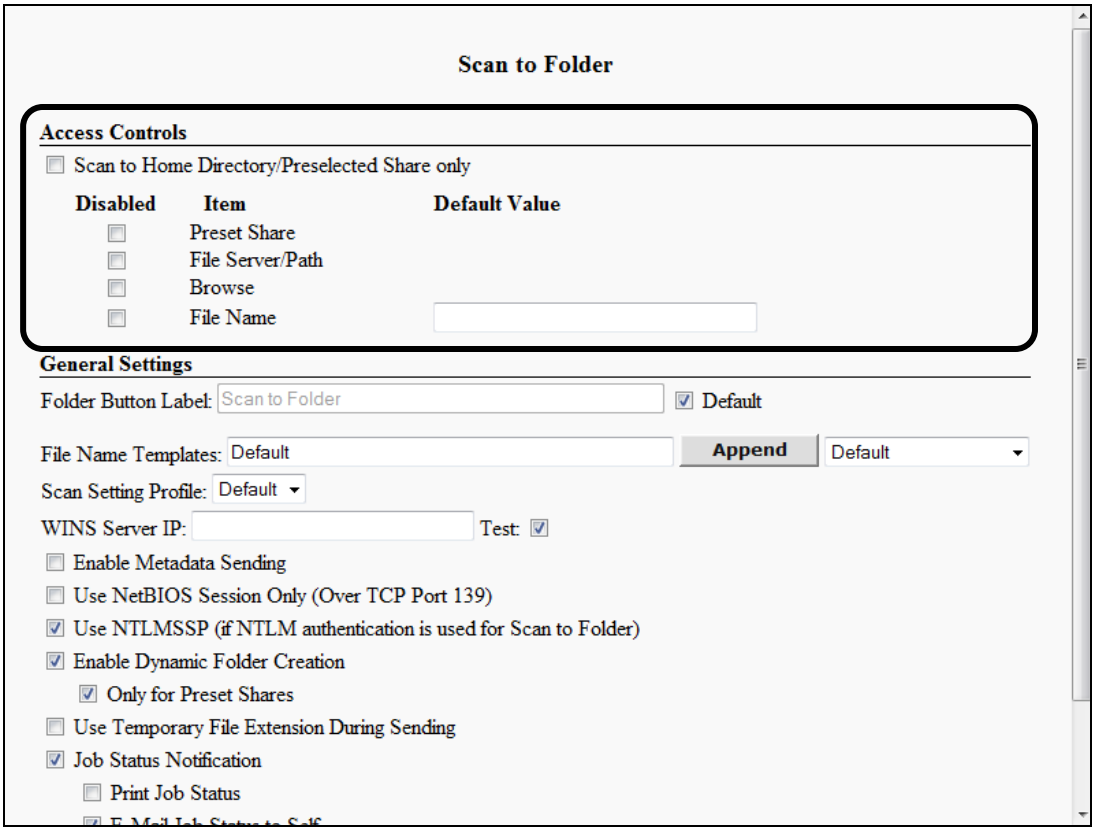
- If an AMS enabled login application is installed and running on the machine, [Scan to Folder] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the Scan to Folder function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [Scan to Folder] → [General].



The Scan to Folder screen is displayed.

2. Configure the settings under <Access Controls>.



Access Controls

Scan to Home Directory/Preselected Share only:	Select this check box if you want to automatically disable the [Preset Share], [File Server/Path], and [Browse] check boxes with one click.

Disabled Column

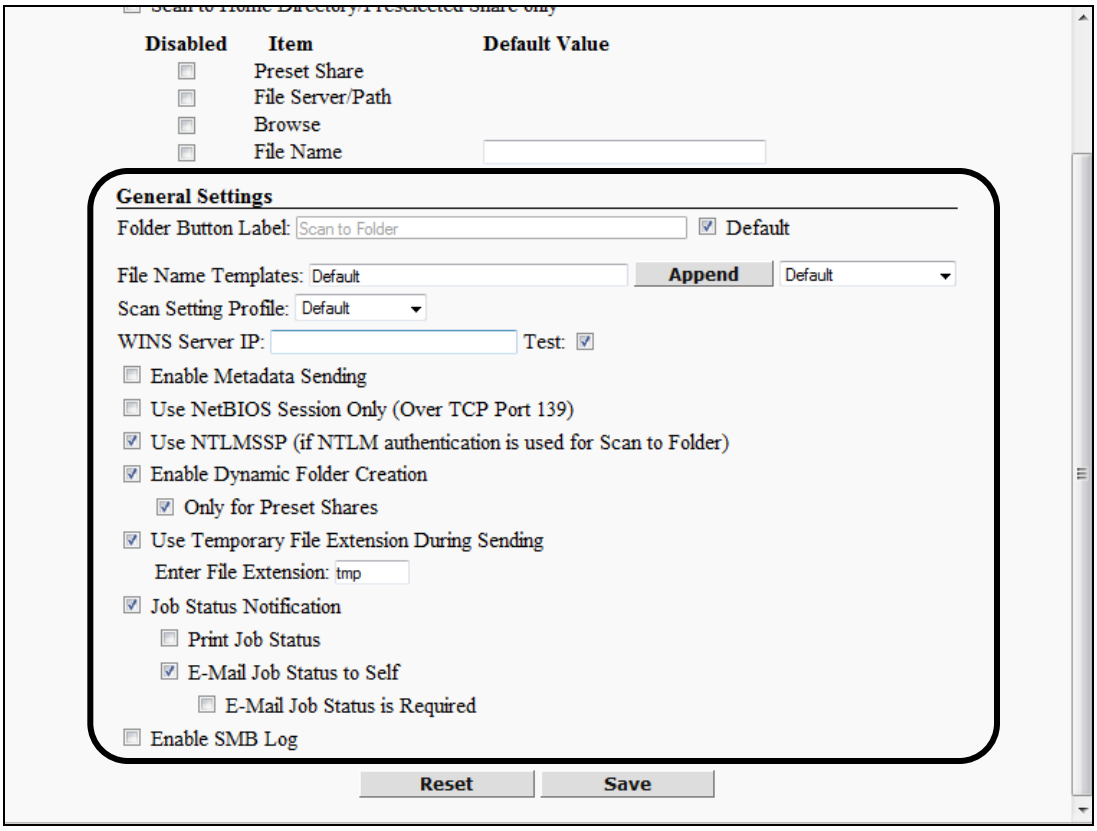
Preset Share:	Select this check box if you want to prevent the user from selecting a preset share from the Preset Share drop-down list on the Authorized Send SCAN TO FOLDER screen on the machine. If you select this check box, the Preset Share drop-down list is disabled and grayed out.
File Server/Path:	Select this check box if you want to disable and gray out the [File Server] and [File Path] text boxes on the Authorized Send SCAN TO FOLDER screen on the machine.

Browse:	Select this check box if you want to disable the [Browse] key on the Authorized Send SCAN TO FOLDER screen on the machine. If you select this check box, the [Browse] key does not appear on the Authorized Send SCAN TO FOLDER screen on the machine.
File Name:	Select this check box if you want to prevent the user from using the [File Name] text box on the Authorized Send SCAN TO FOLDER screen on the machine. If you select this check box, the [File Name] text box is disabled and grayed out.

Default Value Column

File Name:	Enter the default file name to be displayed in the [File Name] text box on the Authorized Send SCAN TO FOLDER screen on the machine. This text box is optional. You can enter a string that consists of any character, and a maximum of 251 characters.

3. Configure the settings under <General Settings>.



General Settings

Folder Button Label: Enter the label for the [Scan to Folder] key that appears on the Authorized Send MAIN screen on the machine. This is a required text box that cannot be left blank. The number of any characters permitted is restricted by the width of the Scan to Folder icon.

Default: Select this check box if you want to use the default Folder Button Label setting ('Scan to Folder'). The Folder Button Label text box cannot be changed when the Default check box is selected.

File Name Templates: Enter one or more File Name Templates which the user can select when creating a scan job. The names in this list are created under the <File Name> tab. See "Configuring the File Name," on p. 407. The default value is 'Default'. Separate entries must be separated by commas. You can enter the File Name Templates manually or select the Templates from the Append drop-down list and click [Append].

Append:	Click [Append] to add a File Name Template (set in the Append drop-down list) to the string in the [File Name Templates] text box.
Append drop-down:	Select a pre-defined File Name Template that is added to the string in the [File Name Templates] text box after you click [Append].
Scan Setting Profile:	Select a scan setting profile from the drop-down list. The default setting is ‘Default’, which corresponds to the default settings on the Scan Settings screen.
WINS Server IP:	Enter the IP address of the NetBIOS name server. This text box is optional. You can enter a string that consists of any character, and an unlimited number of characters.
Test:	Select this check box if you want the connection to the WINS server to be verified before you save the settings. The [Test] check box is selected by default.
Enable Metadata Sending:	Select this check box if you want all scans sent to use the Scan to Folder function and be accompanied by an XML file, which contains metadata as defined on the Metadata Index screen. This check box is not selected by default.
Use NetBIOS Session Only (Over TCP Port 139):	Select this check box if you want Authorized Send to only use port number 139 for Scan to Folder operations. By default, Authorized Send first tries to use port number 445. If this is unsuccessful, port number 139 is used.
Use NTLMSSP (if NTLM authentication is used for Scan to Folder:	Select this check box if you want Authorized Send to use NTLMSSP if NTLM authentication is used. This check box is selected by default.
Enable Dynamic Folder Creation:	Select this check box to automatically create any folders in the share path that may not exist when a user scans a document. If this check box is not selected and the user tries to scan to a folder that does not exist, an error message is displayed and the folder is not created.

Only for Preset Shares:	The [Only for Preset Shares] check box is displayed only if the [Enable Dynamic Folder Creation] check box is selected. Select this check box to enable dynamic folder creation for preset shares that were only created by a System Administrator. If a user enters a share path manually, that does not exist and is not a preset share, an error message is displayed, and the share is not dynamically created when a user scans a document. If this check box is not selected, a user can scan to any folder that does not exist, and the folder is automatically created. This check box is selected by default.
Use Temporary File Extension During Sending:	Select this check box to configure a temporary file extension that is used only during the sending process. Once sending is complete, the temporary file extension is automatically replaced with the appropriate extension of the file type that was sent (PDF, PDF(Compct), PDF(OCR), TIFF, TIFF(Single), JPEG, XPS, XPS(Compct), XPS(OCR), PPT, PPT(OCR), or WORD).
Enter File Extension:	The [Enter File Extension] text box is displayed only if the [Use Temporary File Extension During Sending] check box is selected. Enter the file extension to use while sending a document to a folder. You can enter a maximum of four alphanumeric characters. The default setting is 'tmp'. NOTE • You can only use alphanumeric characters. • Validation is performed after you click [Save] to make sure that: - The [Enter File Extension] text box is not empty. - The maximum number of four alphanumeric characters has not been exceeded. • If validation fails, an error message is displayed.
Job Status Notification:	Select this check box if you want the logged on user of the Scan to Folder session to receive confirmation printout or email.
Print Job Status:	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to Folder session to receive a confirmation printout.

E-Mail Job Status to Self:	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to Folder session to receive a confirmation email.
E-Mail Job Status is Required:	The [E-Mail Job Status is Required] check box is displayed only if the [Job Status Notification] and [E-Mail Job Status to Self] check boxes are selected. Select this check box if you want a confirmation e-mail message to be sent to the logged on user of the Scan to Folder session. If this check box is not selected, the [Email Confirmation] check box is displayed on the SCAN TO FOLDER screen on the machine, giving the user the option of receiving a confirmation e-mail message.
Enable SMB Log:	Select this check box if you want to include additional SMB-related debugging information in the job confirmation printout or email.

4. Click [Save].

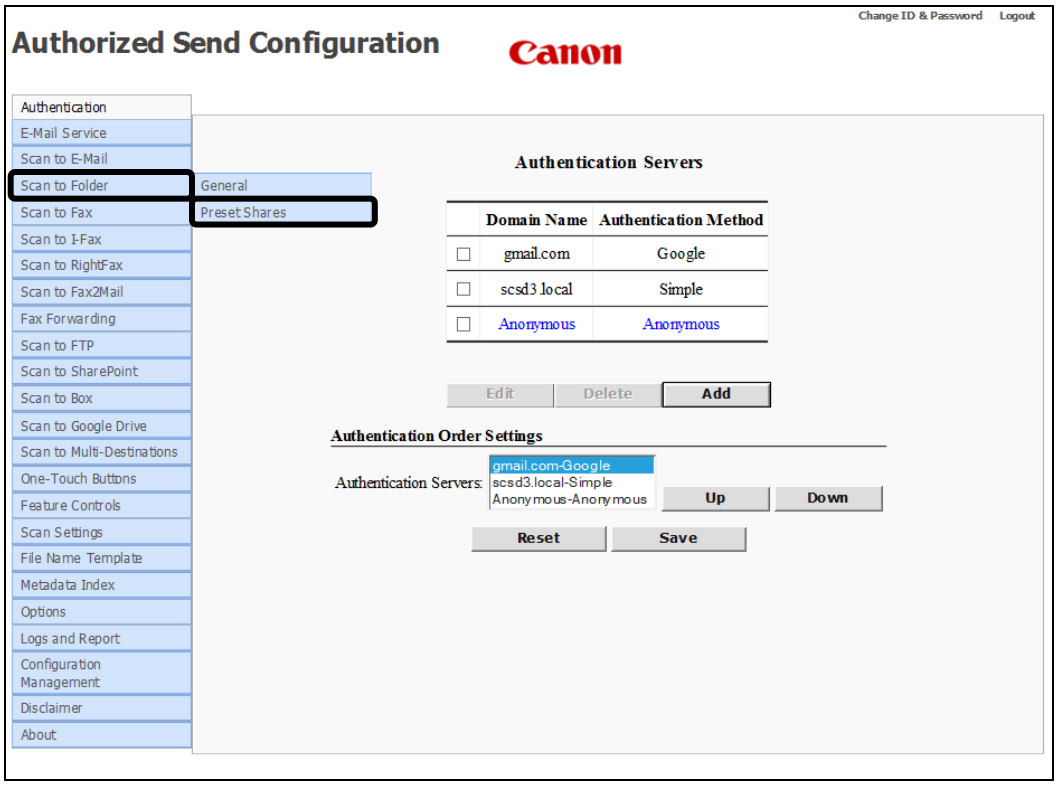
NOTE

If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.7.1 Creating a Preset Share

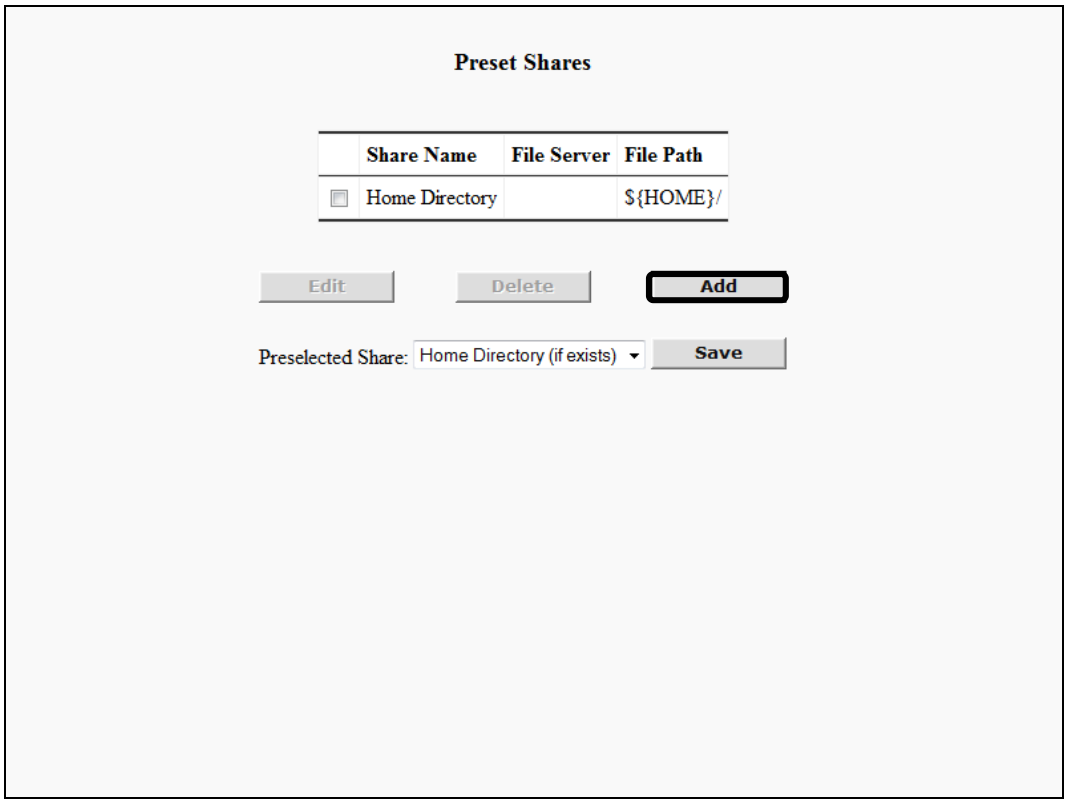
You can create any number of preset shares.

1. Click [Scan to Folder] → [Preset Shares].



The Preset Shares screen is displayed.

2. Click [Add].

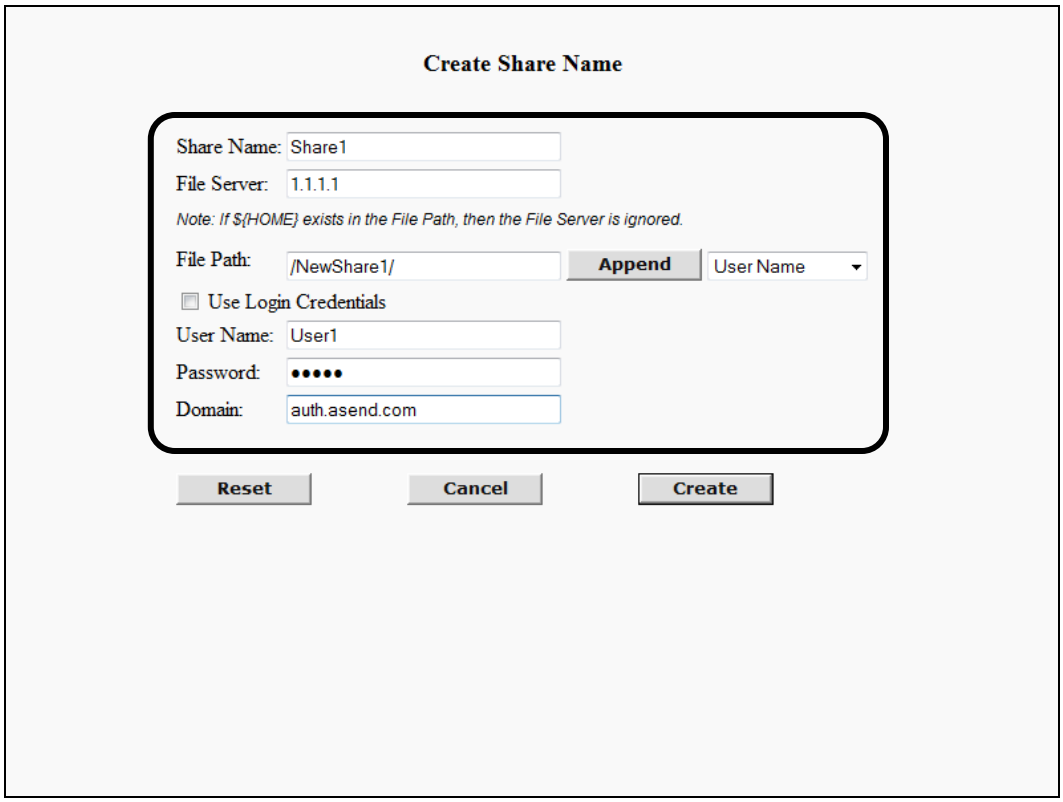


The Create Share Name screen is displayed.

NOTE

- The default setting for Share Name is ‘Home Directory’. This setting is automatically created by Authorized Send, and can be edited and deleted.
- ‘Home Directory’ appears automatically in the Preset Share drop-down list on the Authorized Send SCAN TO FOLDER screen on the machine, if the [Retrieve Home Directory (Active Directory only)] check box is selected on the Create/Update Authentication Server screen or Create/Update Address Book Server screen, and the home directory exists.

3. Configure the Share Name settings.



Create Share Name

Share Name:	Enter a name for the preset share. This name is added to the Preset Share drop-down list on the Authorized Send SCAN TO FOLDER screen on the machine The Share Name is case-sensitive. You can enter a string that consists of any character, and a maximum of 31 characters.
File Server:	Enter the DNS name or IP address to send scanned documents. You can enter a string that consists of any character, and an unlimited number of characters.
File Path:	Enter the path of the folder to send scanned documents. You can enter a string that consists of any character, and an unlimited number of characters.
Append:	Click [Append] to add a user's name or home directory variable (set in the Append drop-down list) to the string in the [File Path] text box.

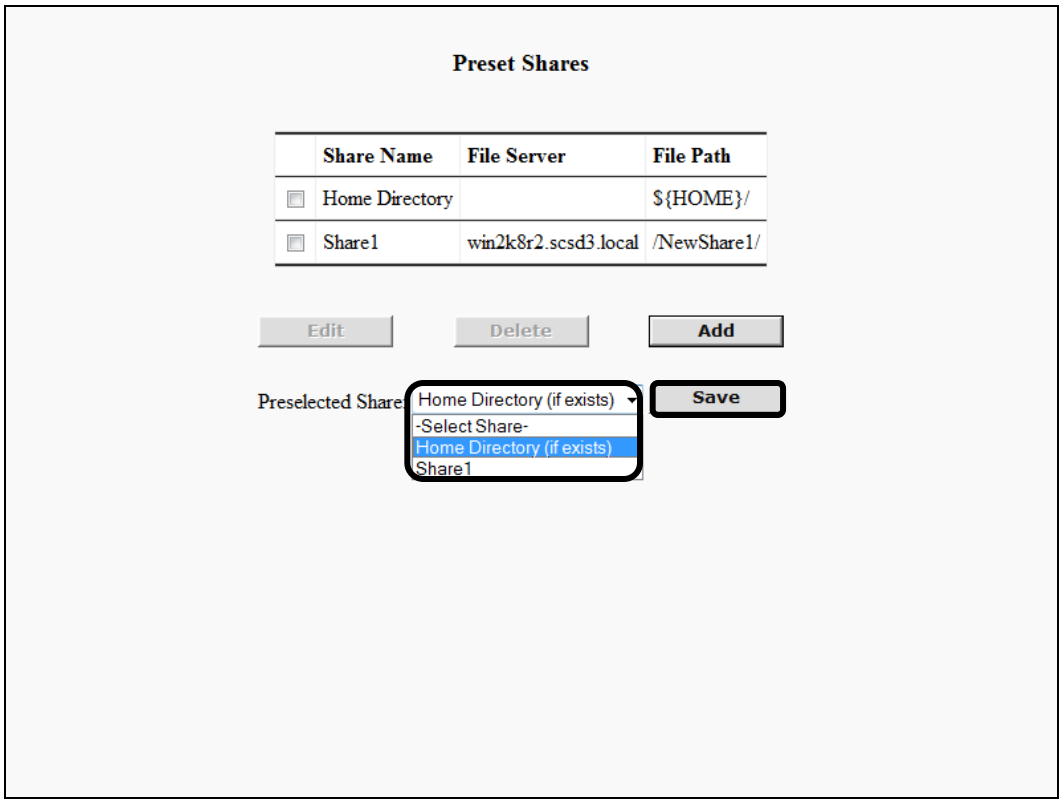
Append drop-down:	Select [User Name], [Home Directory], or [Index Field 1] through [Index Field 8] in conjunction with clicking [Append] to add the user's name or home directory variable to the string in the [File Path] text box.
Use Login Credential:	Select this check box to enable the User Name, Password, and Domain text boxes to be used to log on to the File server. This check box is selected by default. If you do not select the [Use Login Credential] check box, the File server uses the login credentials to start the scanning session.
User Name:	This text box is displayed only if the [Use Login Credential] check box is not selected. Enter the user name to be used to log on to the File server in the [User Name] text box. You can enter a string that consists of any character, and a maximum of 255 characters.
Password:	This text box is displayed only if the [Use Login Credential] check box is not selected. Enter the password to be used to log on to the File server in the [Password] text box. You can enter a string that consists of any character, and a maximum of 255 characters.
Domain:	This text box is displayed only if the [Use Login Credential] check box is not selected. Enter the domain to be used to log on to the File server in the [Domain] text box. You can enter a string that consists of any character, and a maximum of 255 characters.

4. Click [Create].

   If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

   To cancel creating the preset share and return to the Preset Shares configuration screen, click [Cancel].

5. If you want to specify a share name that automatically populates the value in the Preset Share drop-down list on the Authorized Send SCAN TO FOLDER screen on the machine, select a share name from the Preselected Share drop-down list → click [Save].



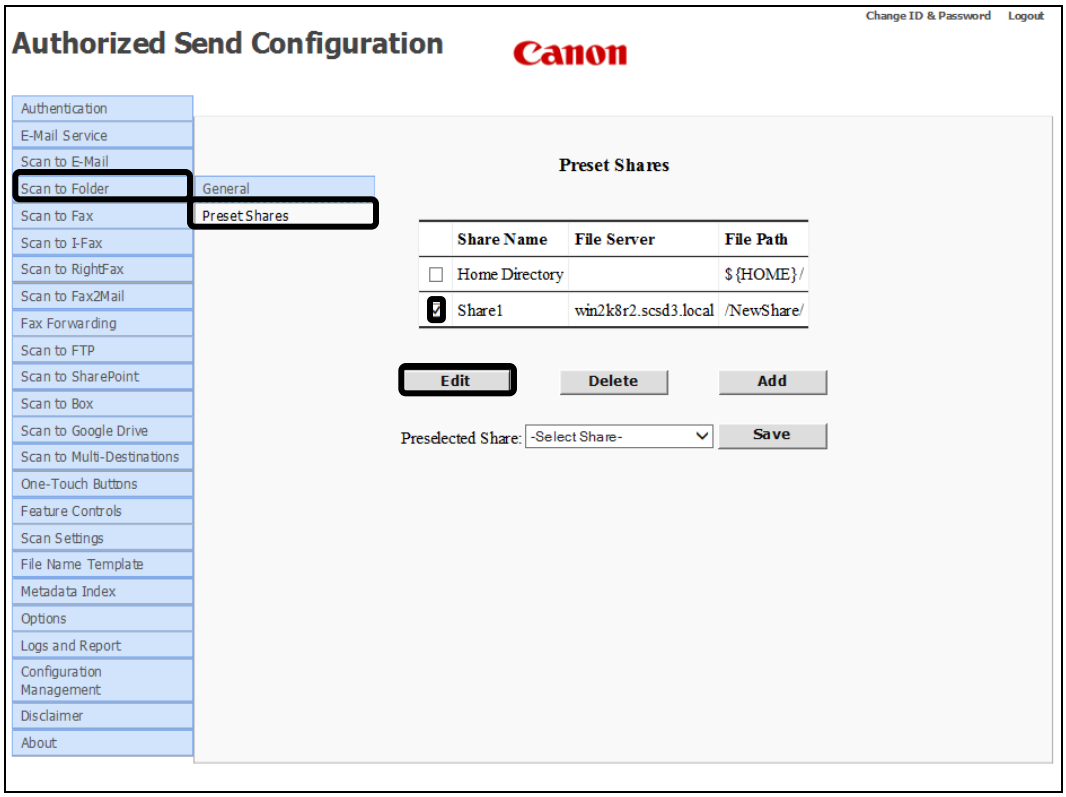
NOTE

- The default setting for Share Name is 'Home Directory'. This setting is automatically created by Authorized Send, and can only be deleted, not edited.
- 'Home Directory' appears automatically in the Preset Share drop-down list on the Authorized Send SCAN TO FOLDER screen on the machine, if the [Retrieve Home Directory (Active Directory only)] check box is selected on the Create/Update Authentication Server screen or Create/Update Address Book Server screen, and the home directory exists.
- If [Retrieve Home Directory (Active Directory only)] check box is not selected on the Create/Update Authentication Server screen or Create/Update Address Book Server screen, or if the user's home directory cannot be successfully retrieved, 'Select Share' is displayed in the Preset Share drop-down list on the Authorized Send SCAN TO FOLDER screen on the machine.

2.7.2 Editing a Preset Share

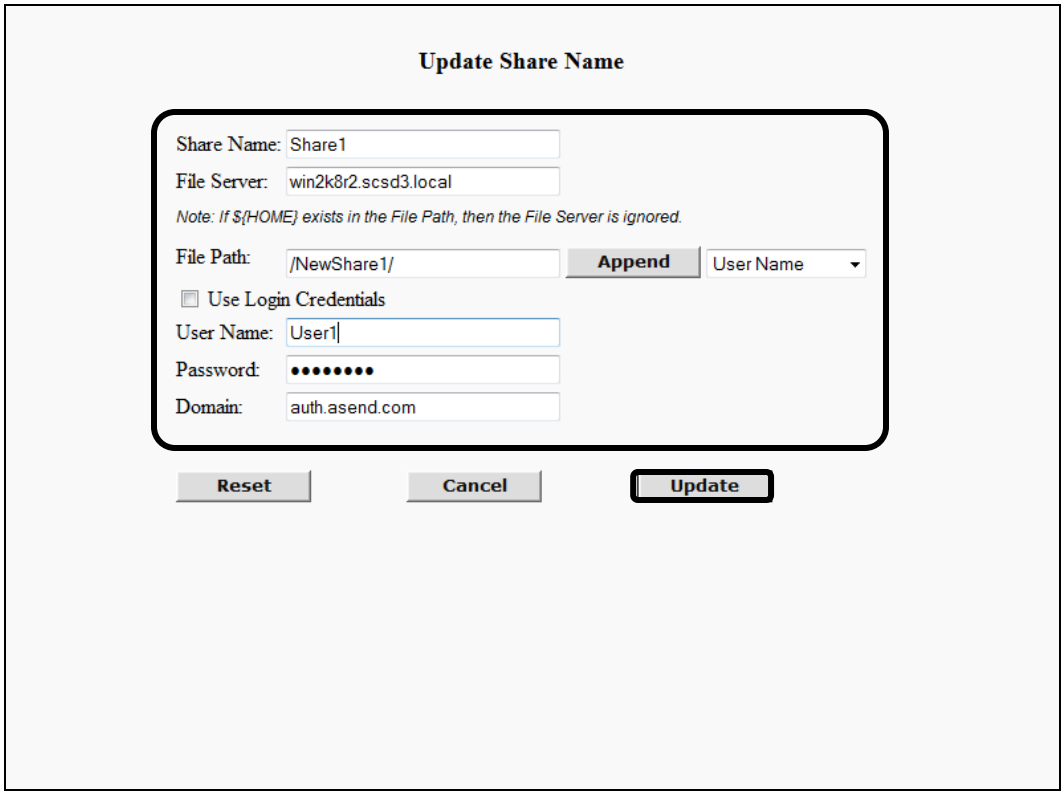
You can edit a previously created preset share from the Preset Shares configuration screen.

1. Click [Scan to Folder] → [Preset Shares] → select the check box next to the preset share you want to edit → click [Edit].



The Update Share Name screen is displayed.

2. Edit the settings for the preset share, as necessary → click [Update].



If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

NOTE

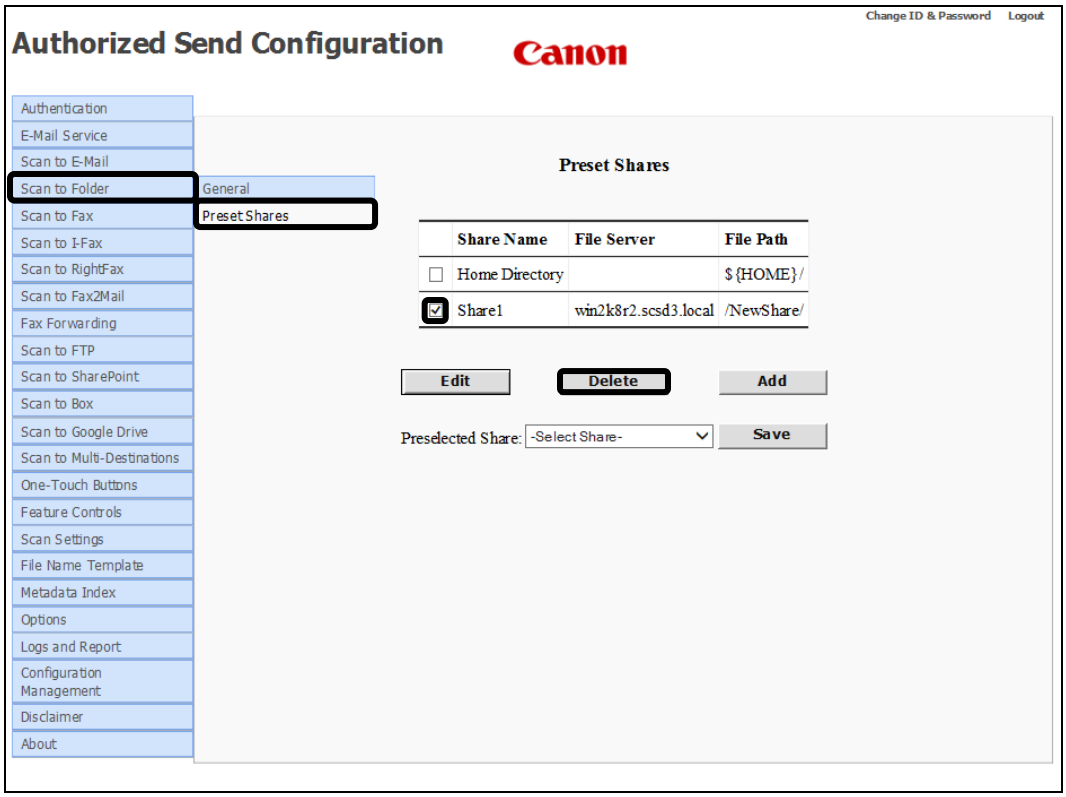
If you edit the default Home Directory share, you cannot change the share name from the default “Home Directory”.

To cancel editing the preset share and return to the Preset Shares configuration screen, click [Cancel].

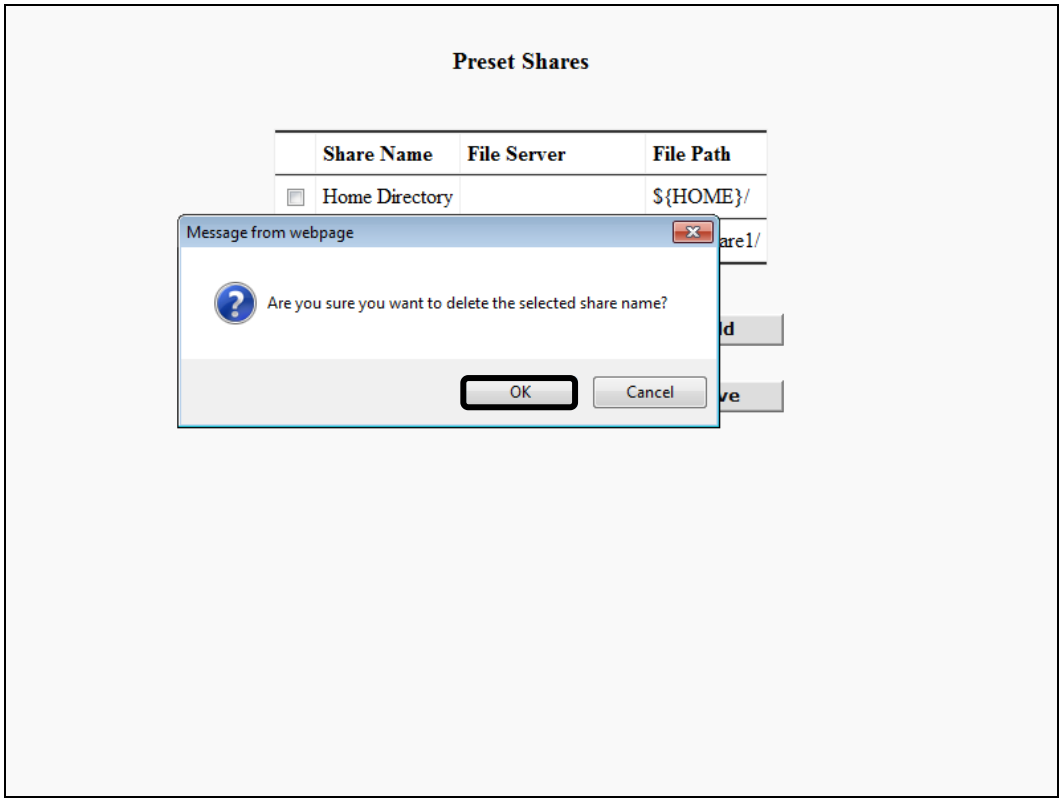
2.7.3 Deleting a Preset Share

You can delete a previously created preset share from the Preset Shares configuration screen.

1. Click [Scan to Folder] → [Preset Shares] → select the check box next to the preset share you want to delete → click [Delete].



2. Click [OK] on the confirmation dialog box.



If you do not want to delete the preset share, click [Cancel].

The preset share is deleted from the list.

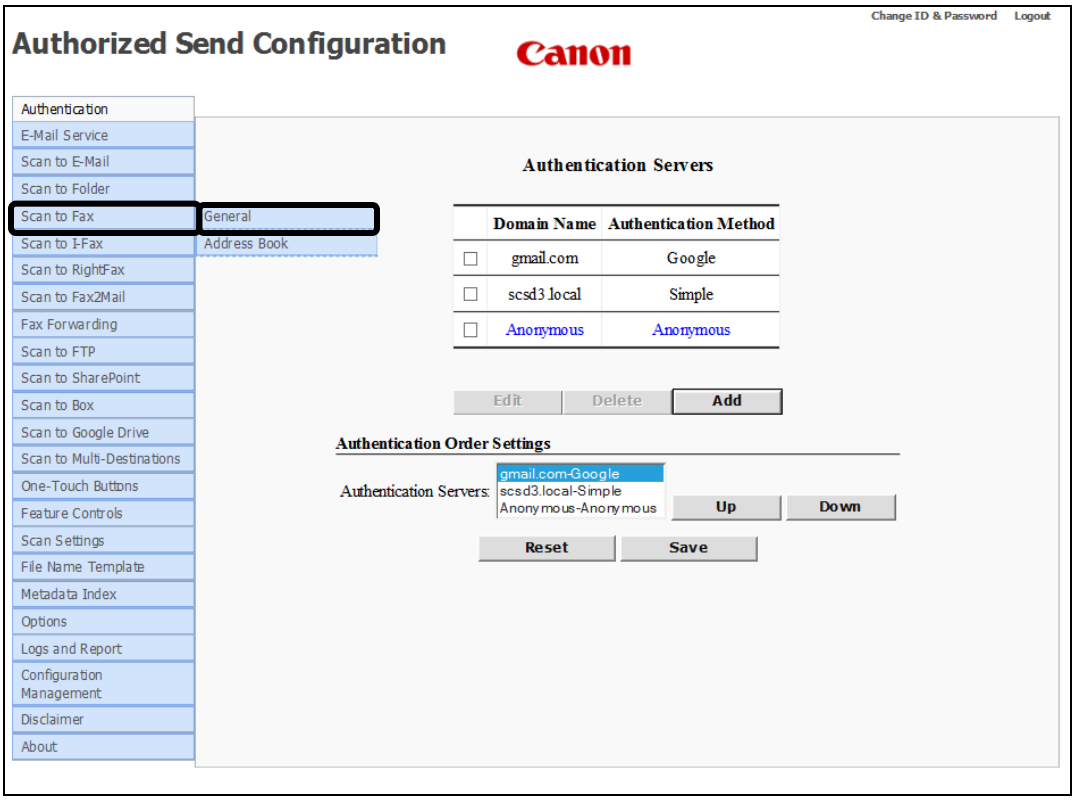
2.8 Configuring the Scan to Fax Settings

You can configure the Scan to Fax function, which enables users to scan and send documents to a fax machine, and create a fax address book.

IMPORTANT

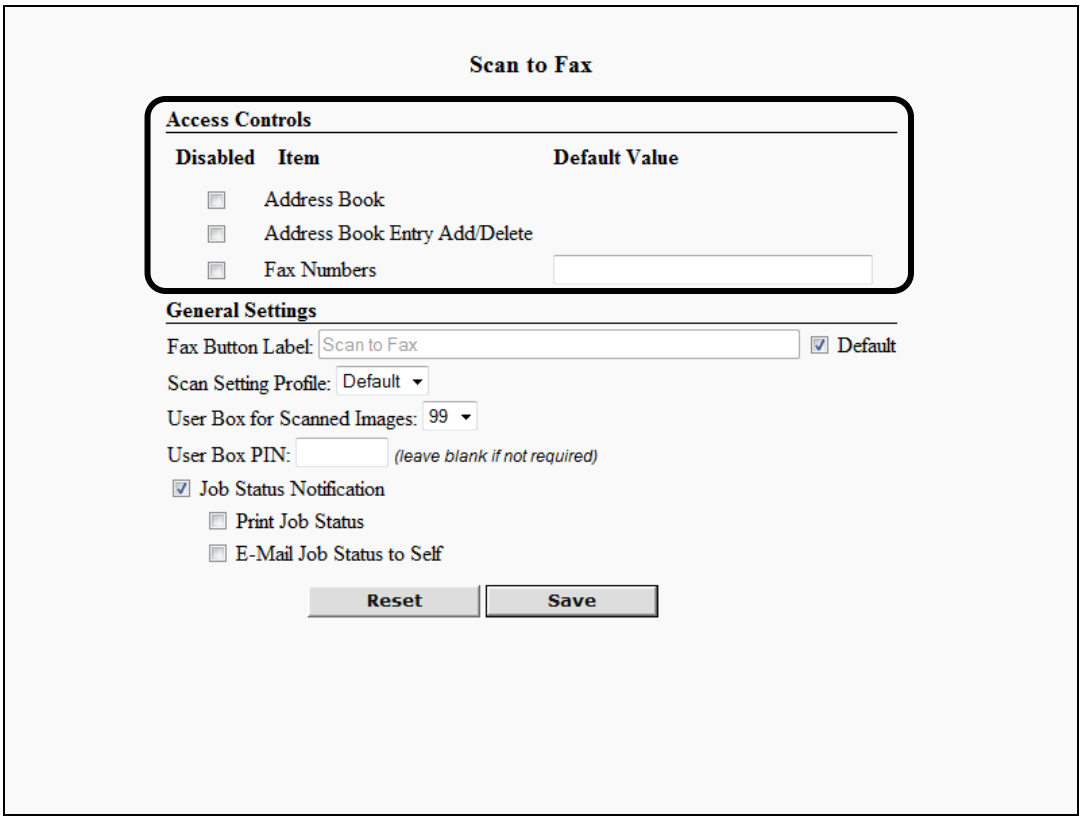
- If an AMS enabled login application is installed and running on the machine, [Scan to Fax] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the Scan to Fax function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.
- If the machine does not support faxing, the message <This device does not support fax.> is displayed instead of the Scan to Fax settings.

1. Click [Scan to Fax] ➞ [General].



The Scan to Fax screen is displayed.

2. Configure the settings under <Access Controls>.



Access Controls

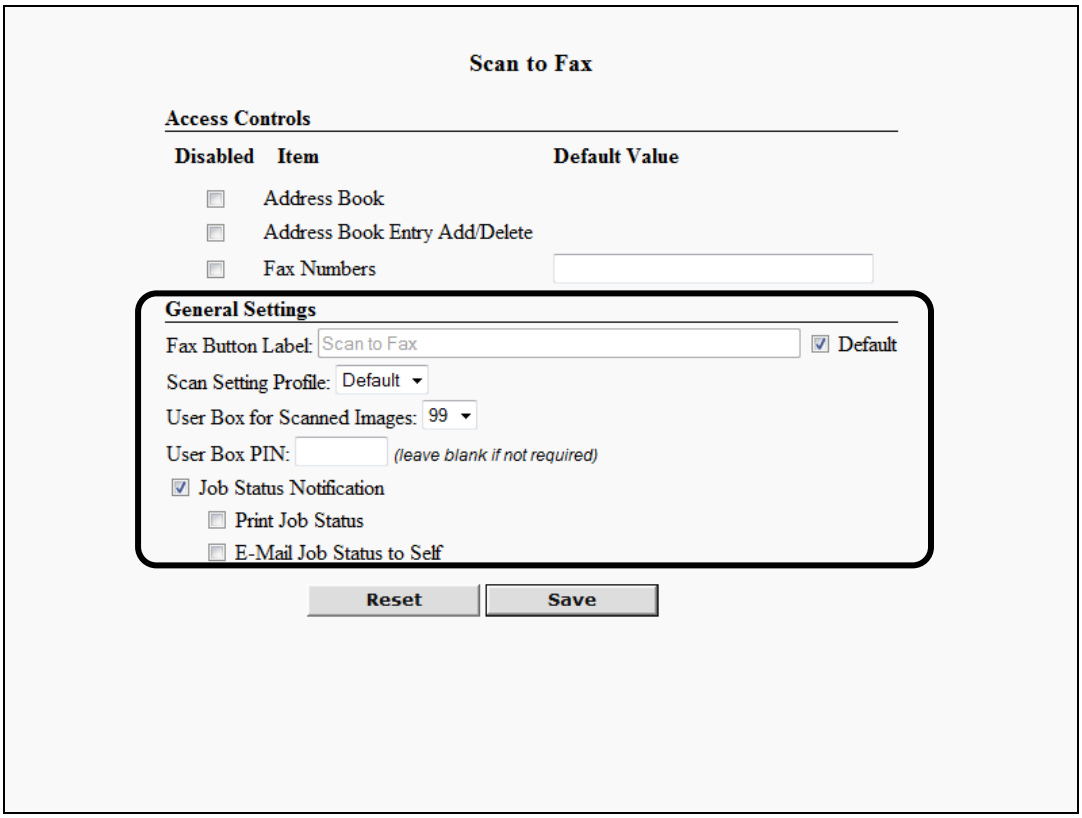
Disabled Item Column

Address Book:	Select this check box if you want to restrict user access to the [Address Book] key on the Authorized Send SCAN TO FAX screen on the machine. If you select this check box, the [Address Book] key is not displayed on the Authorized Send SCAN TO FAX screen on the machine. The user can manually specify a fax number, but cannot select a fax number from the address book.
Address Book Entry Add/Delete:	This check box is displayed only if the [Address Book] check box is not selected. Select this check box if you want to disable and hide the [Add] and [Delete] keys on the Authorized Send FAX ADDRESS BOOK screen on the machine.
Fax Numbers:	Select this check box if you want to disable the [Fax Numbers] text box on the Authorized Send SCAN TO FAX screen on the machine.

Default Value Column

Fax Numbers: Enter a default fax number to be displayed in the [Fax Number] text box on the Authorized Send SCAN TO FAX screen on the machine. The [Fax Numbers] text box is required only if both the [Address Book] and [Fax Numbers] check boxes are selected. You can enter a string that consists of only numbers separated by commas or semicolons. The maximum number of characters you can enter is 255. The default setting is blank.

3. Configure the settings under <General Settings>.



General Settings

Fax Button Label: Enter the label for the [Scan to Fax] key that appears on the Authorized Send MAIN screen on the machine. It is a required text box that cannot be left blank. The number of any characters permitted is restricted by the width of the Scan to Fax icon. The default setting is ‘Scan to Fax’.

Default:	Select this check box if you want to use the default Fax Button Label setting (‘Scan to Fax’). The Fax Button Label text box cannot be changed when the Default check box is selected.
Scan Setting Profile:	Select a scan setting profile from the drop-down list. The default setting is ‘Default’, which corresponds to the default settings on the Scan Settings screen.
User Box for Scanned Images:	Select from [0] to [99] from the drop-down list. The value selected is used by Authorized Send to save temporary data for each Authorized Send SCAN TO FAX session. The default setting is ‘99’.
User Box PIN:	Enter the value to be used by Authorized Send for access to the User Box, if it requires a PIN. The default setting for the [User Box PIN] text box is blank.
Job Status Notification:	Select this check box if you want the logged on user of the Scan to FTP session to receive confirmation printout or email.
Print Job Status:	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to FTP session to receive a confirmation printout.
E-Mail Job Status to Self:	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to FTP session to receive a confirmation email.

4. Click [Save].

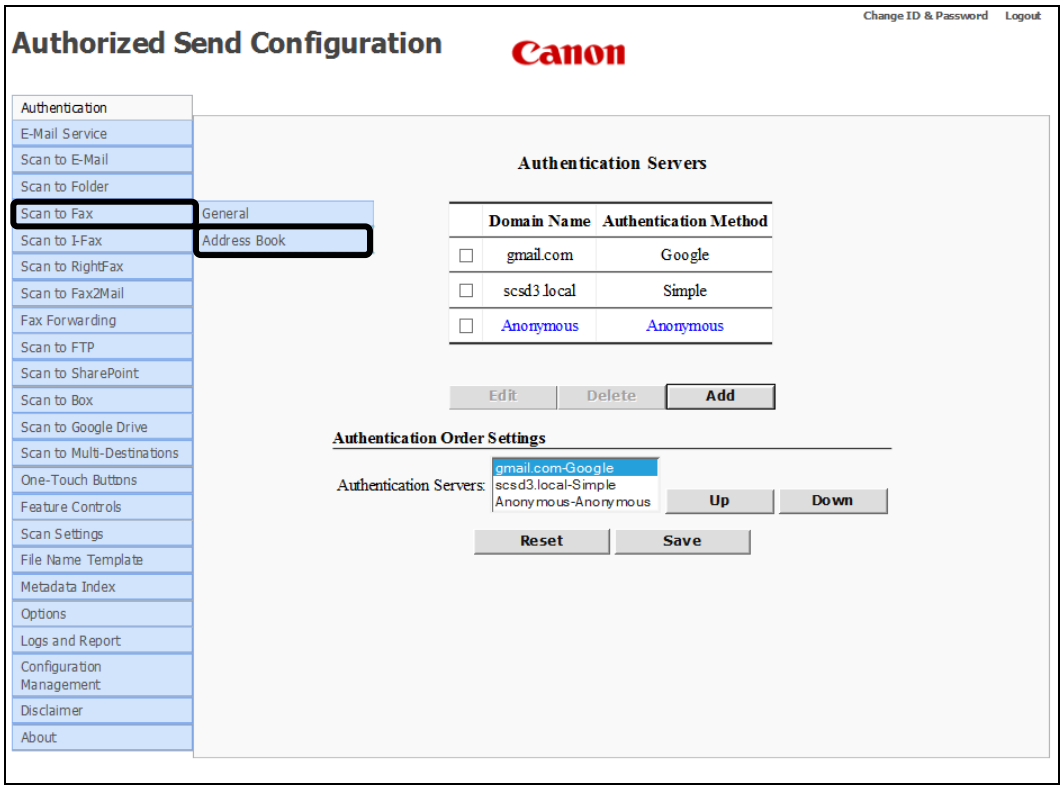
NOTE

- Validation is performed after you click [Save] to see if:
  - The [Address Book] and [Fax Numbers] check boxes are both selected, and the [Fax Numbers] text box is not empty.
  - The maximum number of acceptable characters in the [Fax Numbers] text box is 255.
  - The [Fax Numbers] text box default value contains only numbers, commas, or semicolons.
- If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.8.1 Creating a Fax Address Book

You can create a Fax Address Book to store your fax numbers.

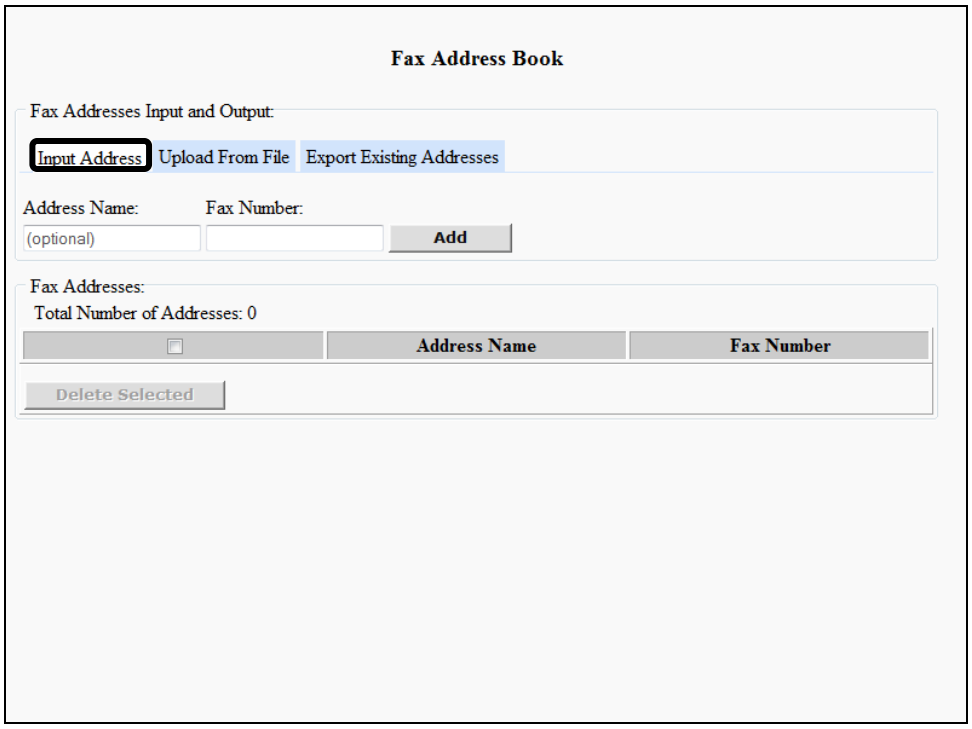
1. Click [Scan to Fax] → [Address Book].



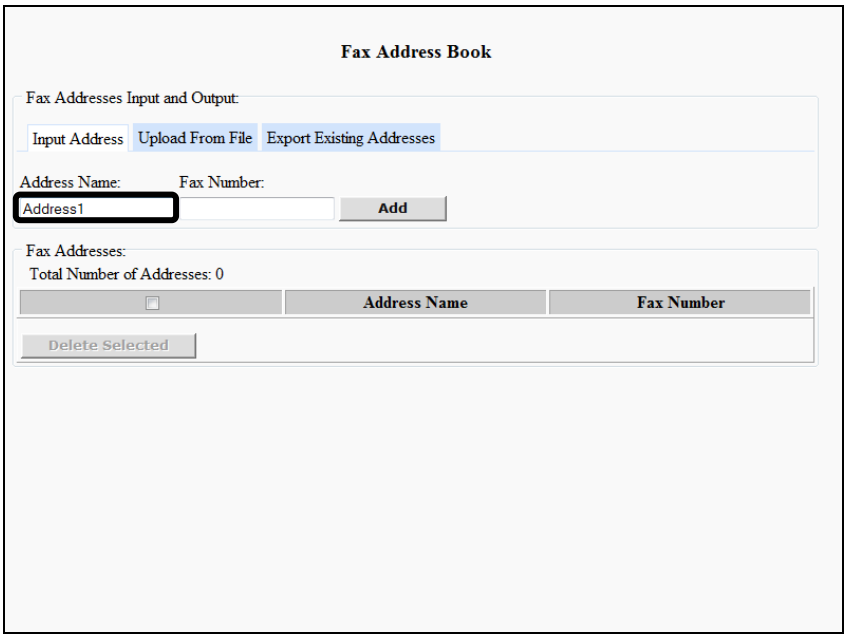
The Fax Address Book screen is displayed.

2. Input a fax address individually or upload it from a file. You can also export saved fax addresses to a text file.

    2.1 To input a fax address individually, click the [Input Address] tab.

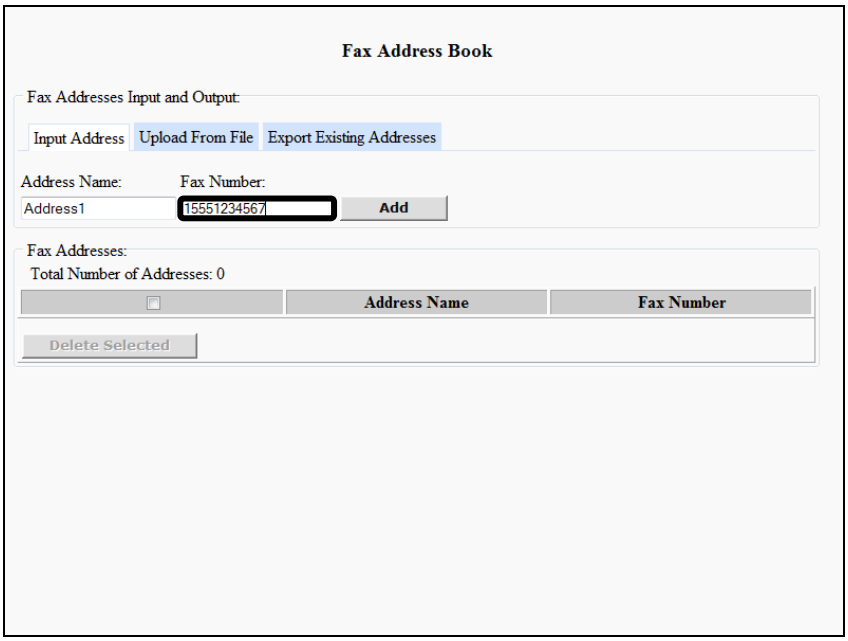


2.1.1 Enter an address name in the [Address Name] text box.



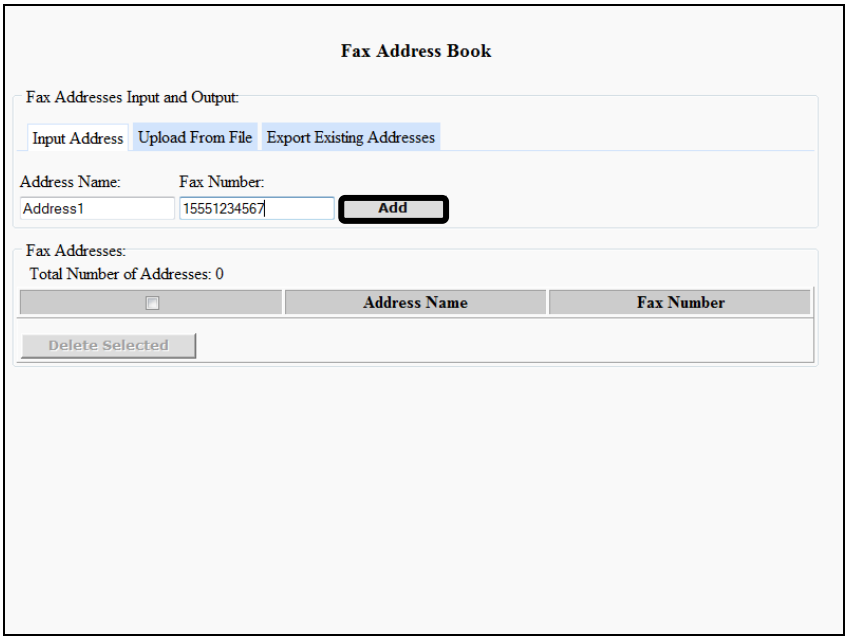
You can enter a string that consists of any character, and a maximum number of 32 characters.

2.1.2 Enter the fax number in the [Fax Number] text box.



You can enter an unlimited length of numbers only. No other characters are acceptable.

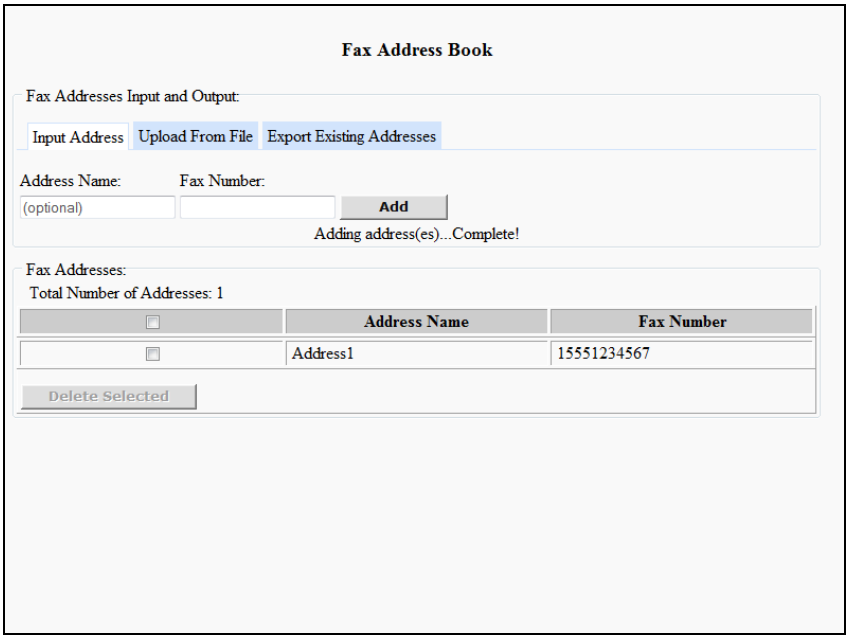
2.1.3 Click [Add] to start the validation process.



Validation is performed to see if:

- The [Fax Number] text box is not empty.
- The [Fax Number] text box contains only numbers.
- The fax number is not a duplicate of any number already entered in the Fax Address Book.
- The maximum number of fax addresses does not exceed 1000.

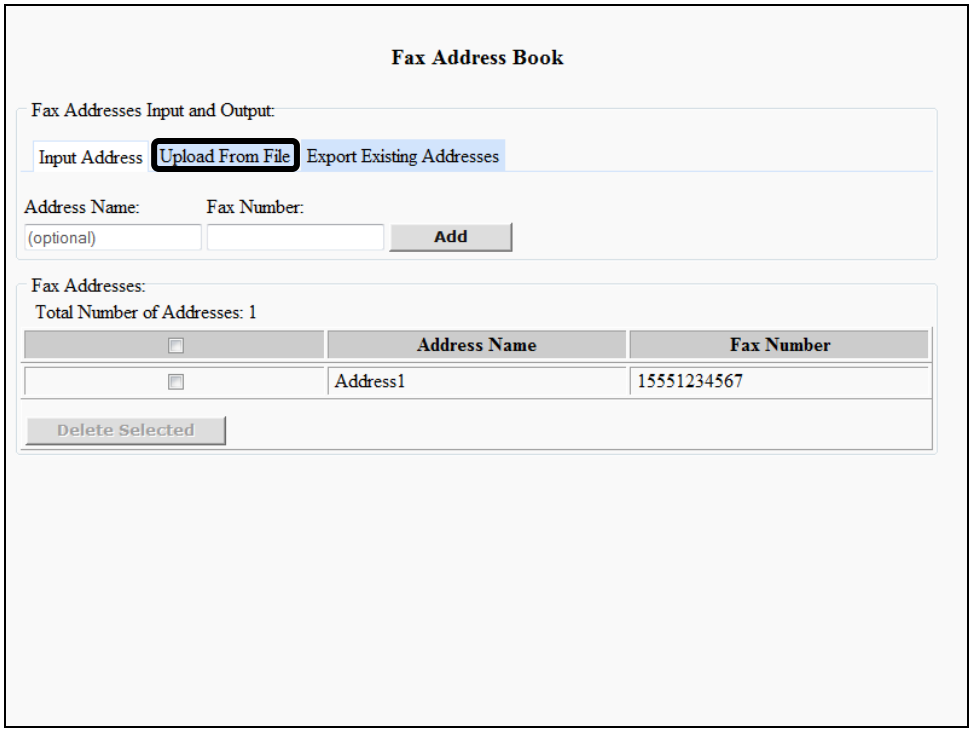
If the validation process is successful, the added fax address appears in the Fax Address table. If it fails, an error message is displayed in red.



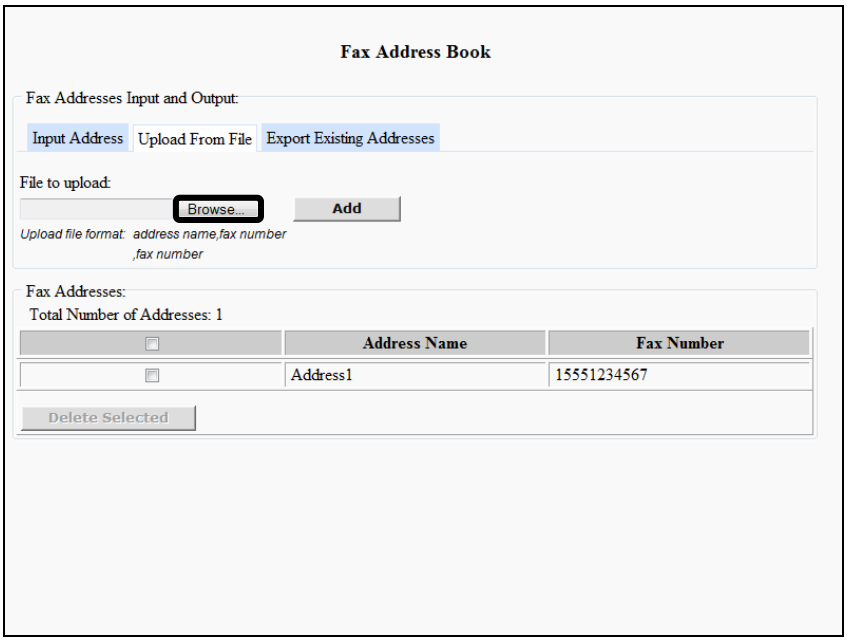
NOTE

<Total Number of Addresses:> displays the number of fax addresses that are in the Fax Addresses table. This number varies as fax addresses are added to, or deleted from, the Fax Addresses table.

2.2 To upload a fax address from a file, click the [Upload From File] tab.



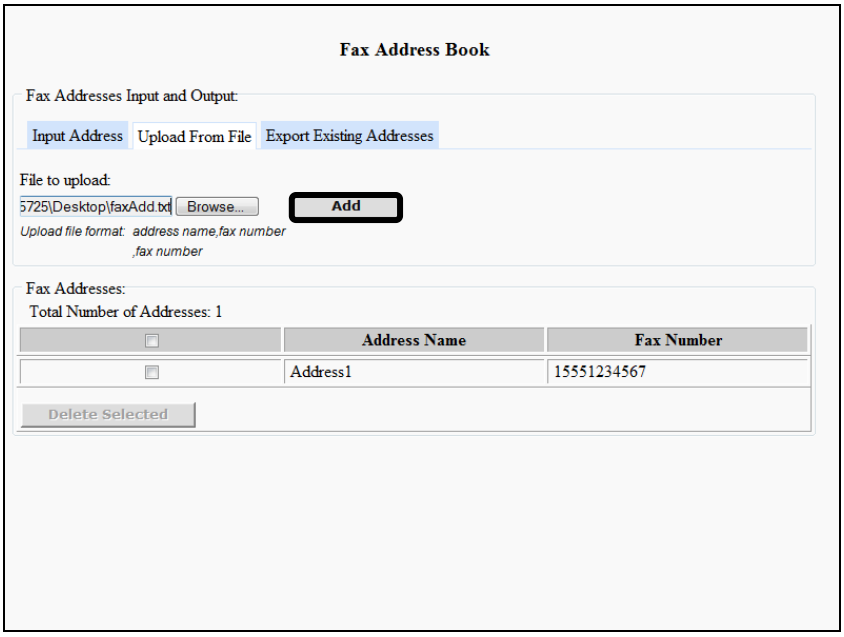
2.2.1 Click [Browse] →navigate to the drive or directory containing the file to upload → select the file → click [Open].



NOTE

The uploaded file extension must be ".txt" or ".csv," and is not case-sensitive.

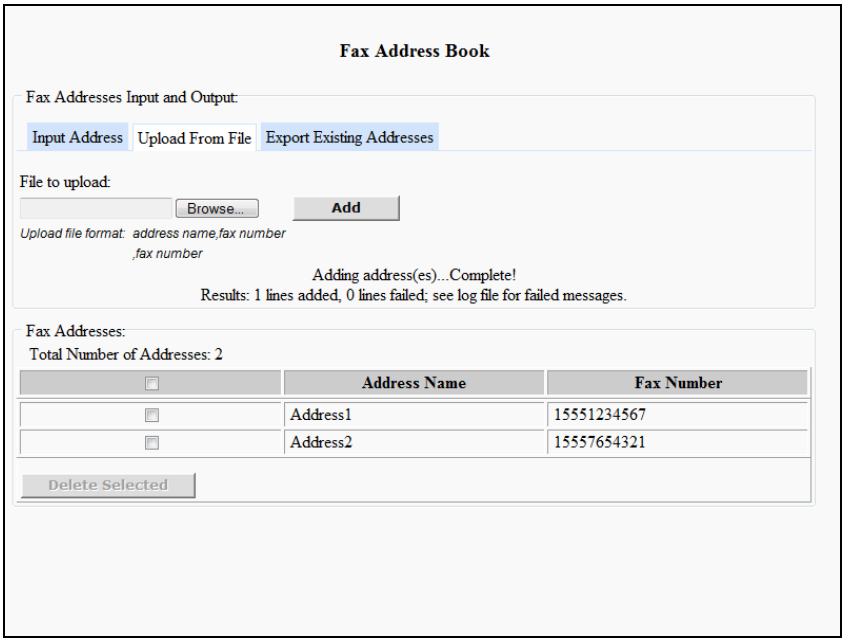
2.2.2 Click [Add] to start the validation process.



Validation is performed to see if:

- The uploaded file is a text file with the following format requirements:
  - Each fax address entry is on a separate line.
  - Each fax address entry contains an address name and fax number separated by a comma (“address_name,fax_number”).
  - Since the address name is optional, the format “,fax_number” is also acceptable.
- The address name, if used, does not exceed the maximum number of 32 characters. If the fax address name exceeds 32 characters, it is truncated.

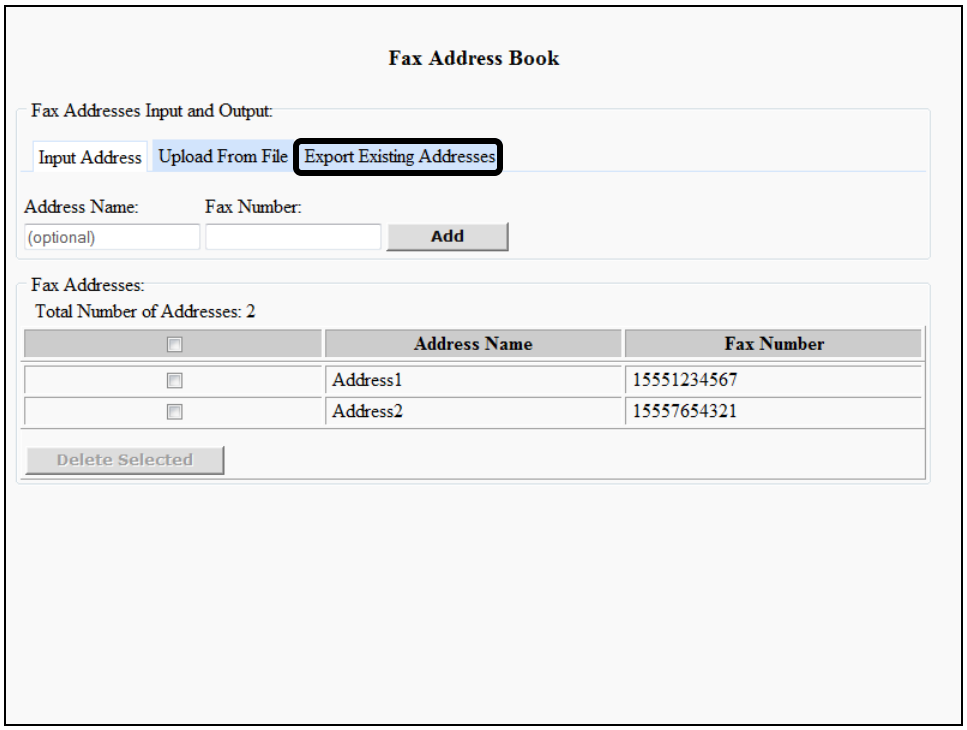
If the validation process is successful, the added fax address appears in the Fax Addresses table. If it fails, an error message is displayed in red.



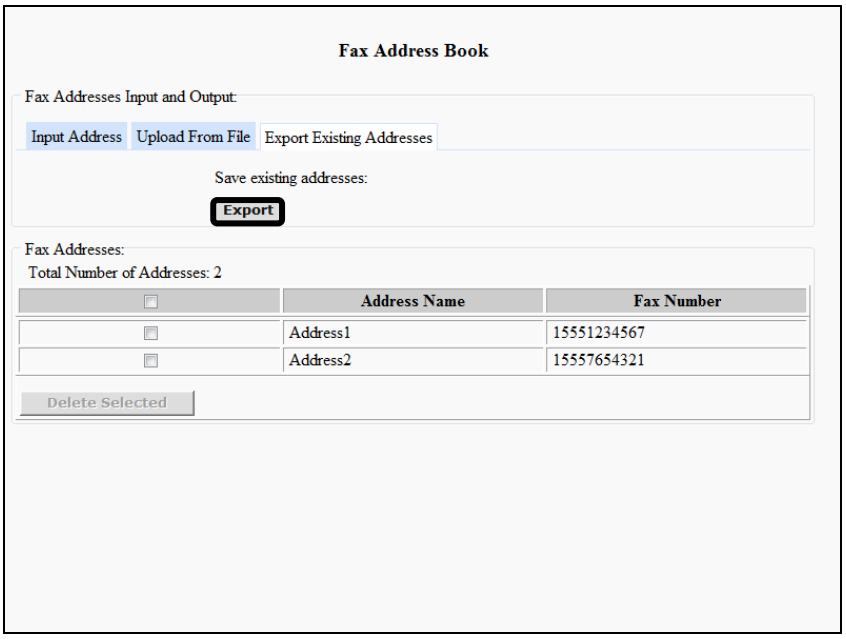
NOTE

- Any line entry in the uploaded file that is in an invalid format is reported as a failure with the line number. That line is skipped, and uploading continues with the next line.
- Any fax address in the uploaded file that has already been saved is ignored and reported as a duplicate. Only the number of duplicates found in the file is reported, not the exact line number.

2.3 To export the existing fax addresses to a text file, click the [Export Existing Addresses] tab.



2.3.1 Click [Export].



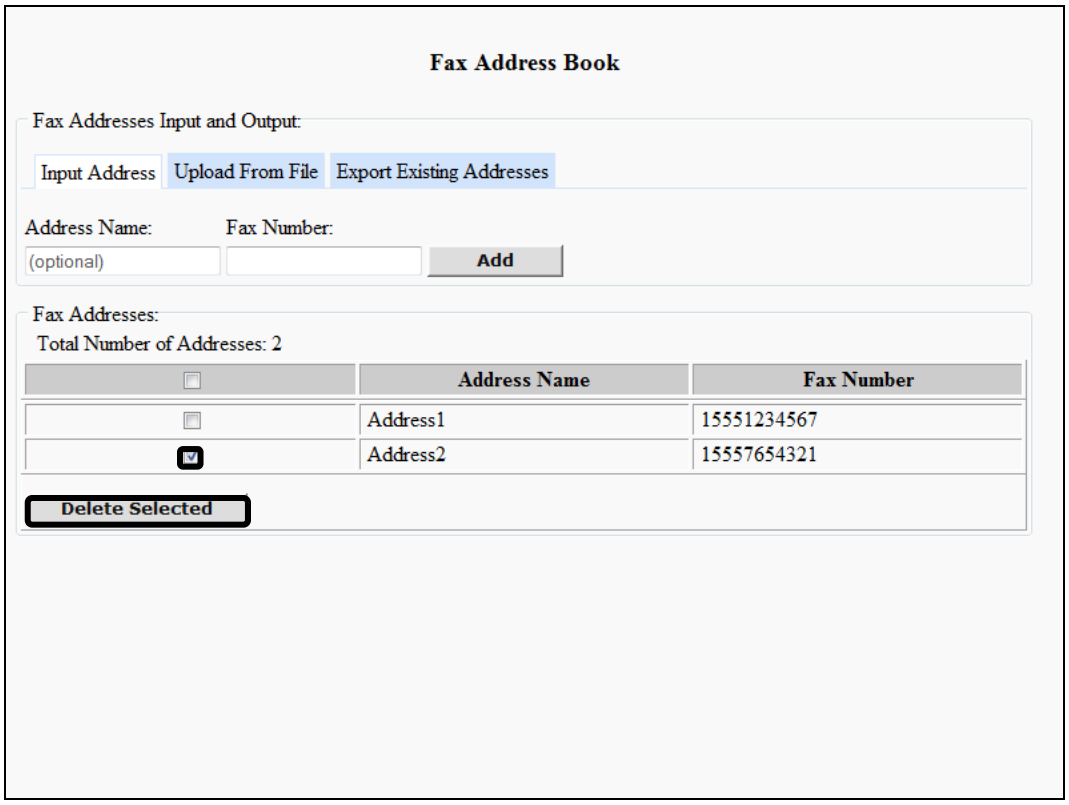
The existing fax addresses are exported to a text file.

The exported text file is formatted, as described below:

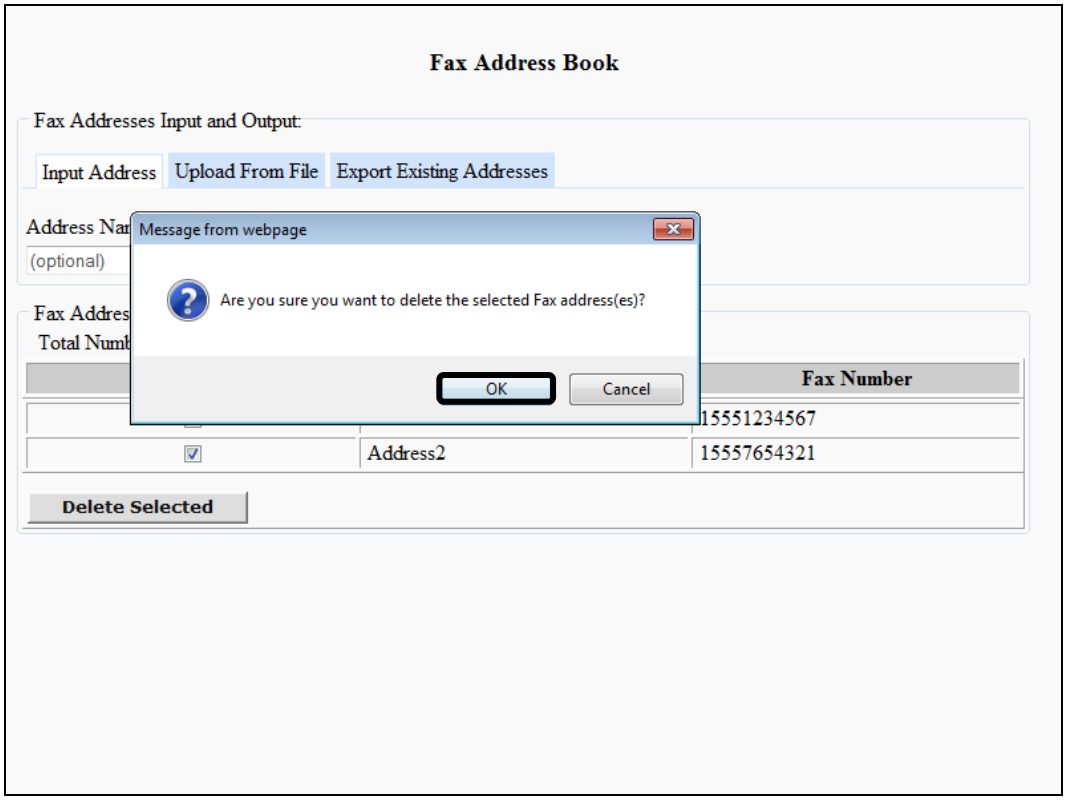
- Each fax address entry is on a separate line.
- Each fax address entry contains an address name and fax number separated by a comma (“address_name,fax_number”).
- Since the address name is optional, the format “,fax_number” is also acceptable.

2.3.2 Click [File] → [Save As] → navigate to the drive or directory where you want to save the file → click [Save].

3. To delete a fax address, click the check box next to the fax address you want to delete → click [Delete Selected].



4. Click [OK].



If you do not want to delete the fax address, click [Cancel].

The fax address is deleted from the list.

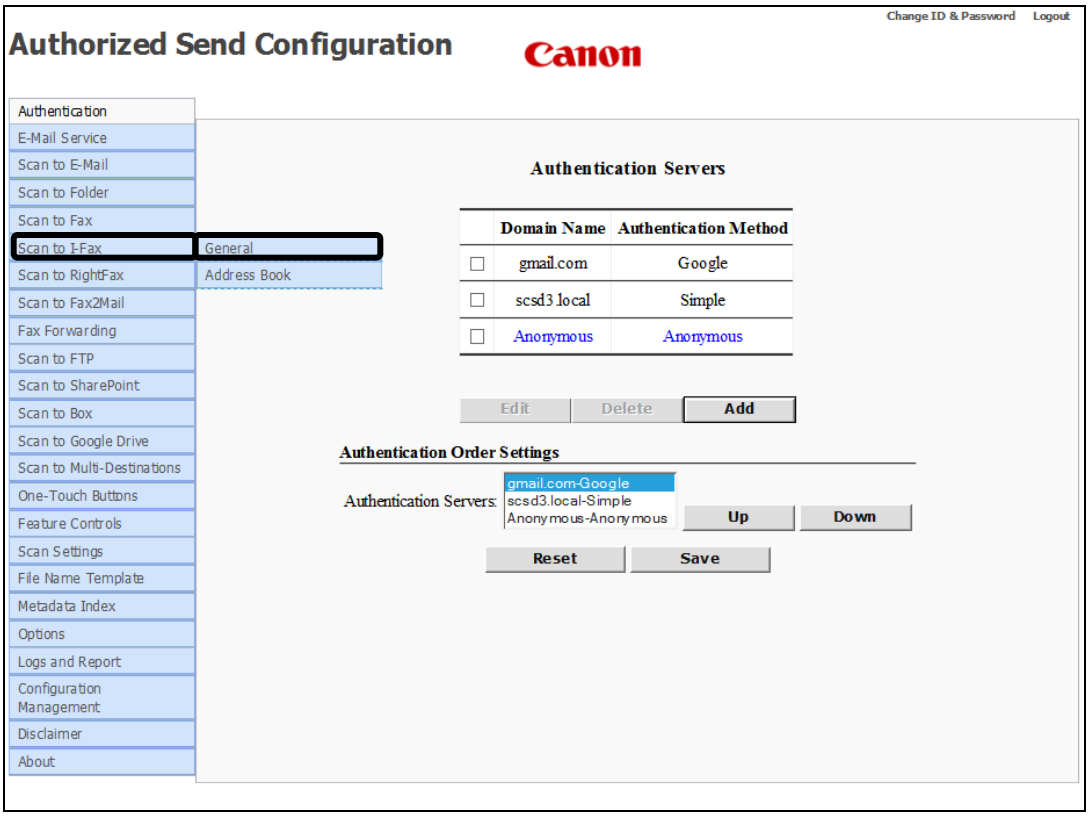
2.9 Configuring the Scan to I-Fax Settings

You can configure the Scan to I-Fax function, which enables users to scan and send documents via an SMTP server, and create an I-Fax address book.

IMPORTANT

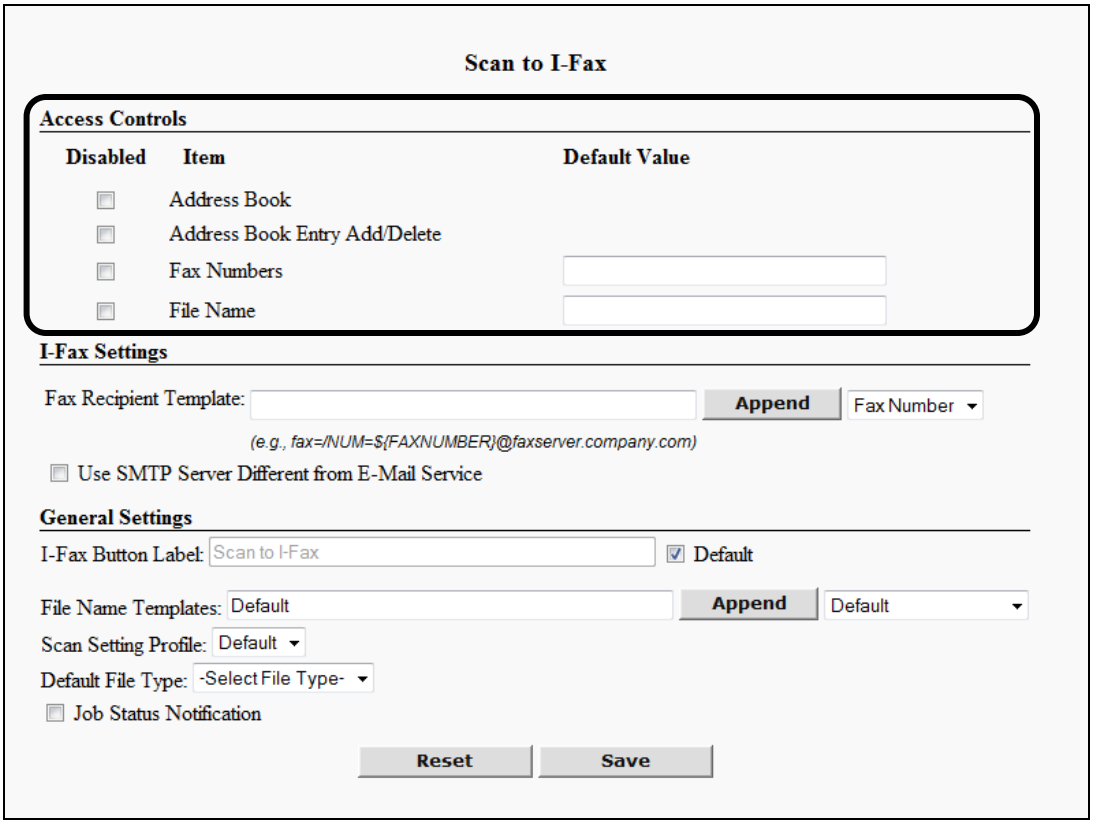
- If an AMS enabled login application is installed and running on the machine, [Scan to I-Fax] may be displayed but disabled on the machine, even if the Scan to I-Fax function is enabled in the Authorized Send Configuration servlet. This is based on the role of the user who logged on via the login application.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [Scan to I-Fax] → [General].



The Scan to I-Fax screen is displayed.

2. Configure the settings under <Access Controls>.



Access Controls

Disabled Item Column

Address Book: Select this check box if you want to restrict user access to the [Address Book] key on the Authorized Send SCAN TO I-FAX screen on the machine. If you select this check box, the [Address Book] key is not displayed on the Authorized Send SCAN TO I-FAX screen on the machine. The user can manually specify a fax number, but cannot select a fax number from the address book.

Address Book Entry Add/Delete: This check box is displayed only if the [Address Book] check box is not selected. Select this check box if you want to disable and hide the [Add] and [Delete] keys on the Authorized Send FAX ADDRESS BOOK screen on the machine.

Fax Numbers: Select this check box if you want to disable the [Fax Numbers] text box on the Authorized Send SCAN TO I-FAX screen on the machine.

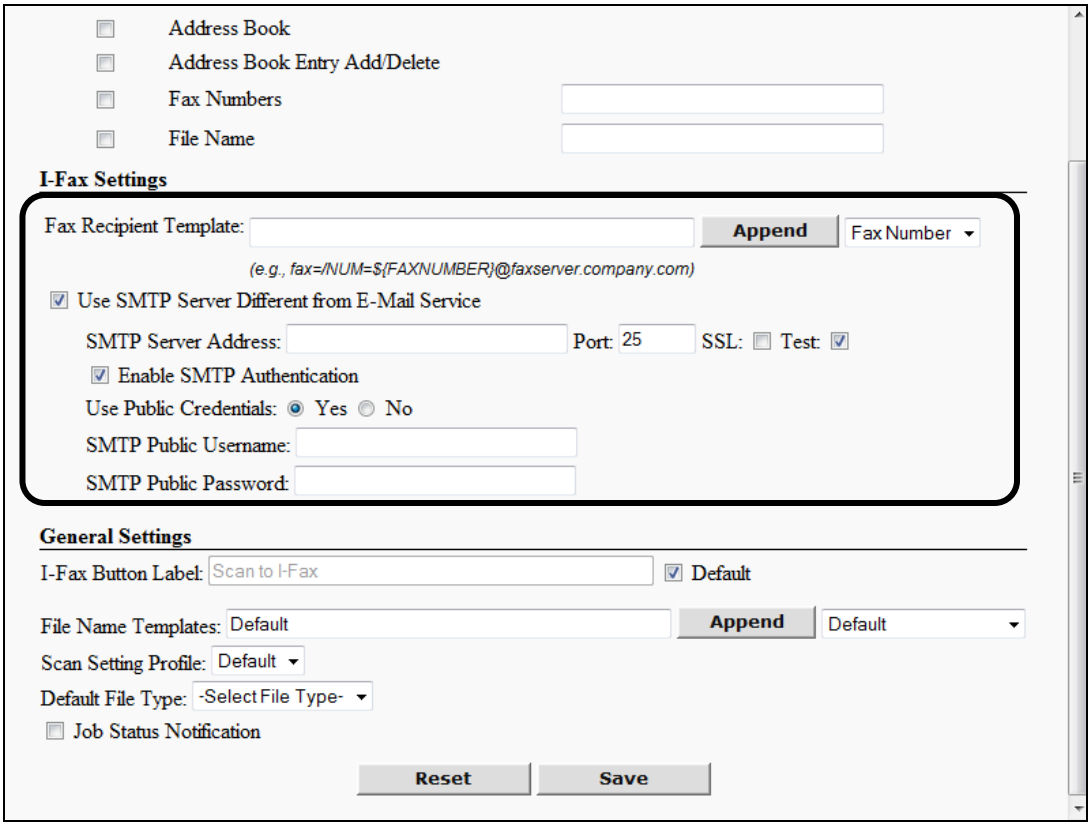
File Name: Select this check box to disable the [File Name] text box on the Authorized Send SCAN TO I-FAX screen on the machine.

Default Value Column

Fax Numbers: Enter a default fax number to be displayed in the [Fax Number] text box on the Authorized Send SCAN TO I-FAX screen on the machine. The [Fax Numbers] text box is a required field only if both the [Address Book] and [Fax Numbers] check boxes are selected. You can enter a string that consists of alphanumeric characters, periods (“.”), hyphens (“-“), spaces (“ “), and underscores (“_”), separated by commas or semicolons. You can enter a maximum of 255characters. The default setting is blank.

File Name: Enter the default file name to be displayed in the [File Name] text box on the Authorized Send SCAN TO I-FAX screen on the machine. This text box is optional. You can enter a string that consists of any character, and a maximum of 251 characters.

3. Configure the settings under <I-Fax Settings>.

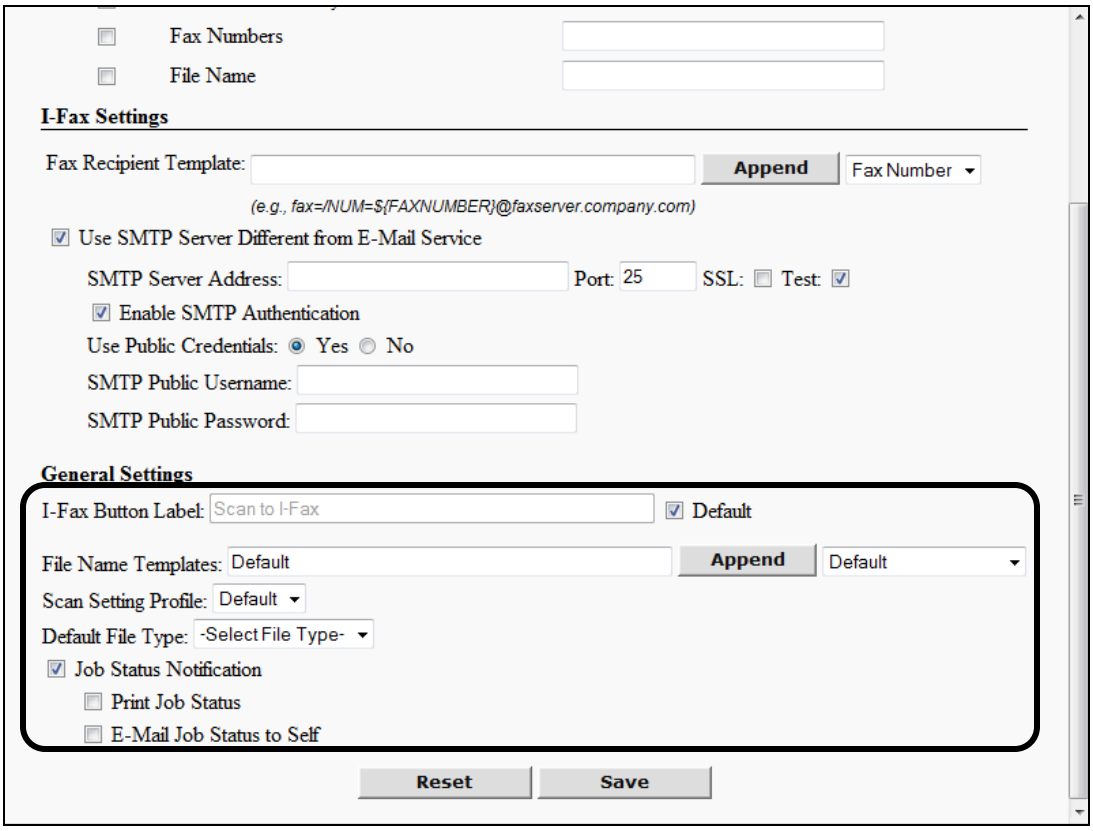


I-Fax Settings

Fax Recipient Template:	Enter a custom string (including the fax number entered by the user) to be used as the e-mail address when sending scanned documents to a fax server. This text box is required. You can enter a string that consists of any character, and an unlimited number of characters. For example, if you enter **${FAXNUMBER}@faxserver.company.com** as the string, and the fax number entered by the user (for example, '1234567') when sending from the Scan to I-Fax screen, Authorized Send sends an e-mail message to the SMTP server with "1234567@faxserver.company.com" in the "To:" text box. NOTE • The user does not see the template. The user only has to enter the fax numbers on the Authorized Send SCAN TO I-FAX screen on the machine. • If you upgrade Authorized Send from V3.*x* to V6.4, the fax template is automatically updated to the current format, which would include: '${FAXNUMBER}' as the prefix to what was configured in V3.*x*.
Append:	Click [Append] to add a dynamic variable (set in the Append drop-down list) to the string in the Fax Recipient Template. This is unnecessary if the string is entered manually in the [Fax Recipient Template] text box.
Append drop-down:	Select [Fax Number] in conjunction with clicking [Append] adds the fax number variable '${FAXNUMBER}' to the string in the [Fax Recipient Template] text box.
Use SMTP Server Different from E-Mail Service:	Select this check box to enable the SMTP Server Address text box, Port text box, Test check box, and Enable SMTP Authentication check box. The [Use SMTP Server Different from E-Mail Service] check box is not selected by default.
SMTP Server Address:	This text box is displayed only if the [Use SMTP Server Different from E-Mail Service] check box is selected. Enter the DNS name or IP address of the SMTP server. You can enter a string that consists of any character, and an unlimited number of characters.

Port:	This text box is displayed only if the [Use SMTP Server Different from E-Mail Service] check box is selected. Enter the connecting port number of the SMTP server. You can enter a maximum of five numbers. The default port number is ‘25’.
SSL:	Select this check box if you want the SMTP server to use SSL. If you select this check box, the SMTP server port number automatically changes to ‘636’.
Test:	This check box is displayed only if the [Use SMTP Server Different from E-Mail Service] check box is selected. Select this check box if you want the connection to the SMTP server to be verified before you save the settings. The [Test] check box is selected by default.
Enable SMTP Authentication:	This check box is displayed only if the [Use SMTP Server Different from E-Mail Service] check box is selected. Select the [Enable SMTP Authentication] check box to have the user authenticated on the SMTP server when using the Scan to E-Mail or Scan to Fax function. The [Enable SMTP Authentication] check box is not selected by default.
Use Public Credentials:	These radio buttons are displayed only if the [Enable SMTP Authentication] check box is selected. Select [Yes] to configure the SMTP public credentials (SMTP Public Username and SMTP Public Password). If [Yes] is selected, enter the user’s SMTP public name and password for SMTP authentication. The default setting is ‘No’.
SMTP Public Username:	This text box is displayed only if Use Public Credentials is set to ‘Yes’. Enter the user name for SMTP authentication. You can enter a string that consists of any character, and an unlimited number of characters.
SMTP Public Password:	This text box is displayed only if Use Public Credentials is set to ‘Yes’. Enter the password for SMTP authentication. You can enter a string that consists of any character, and an unlimited number of characters.

4. Configure the settings under <General Settings>.



General Settings

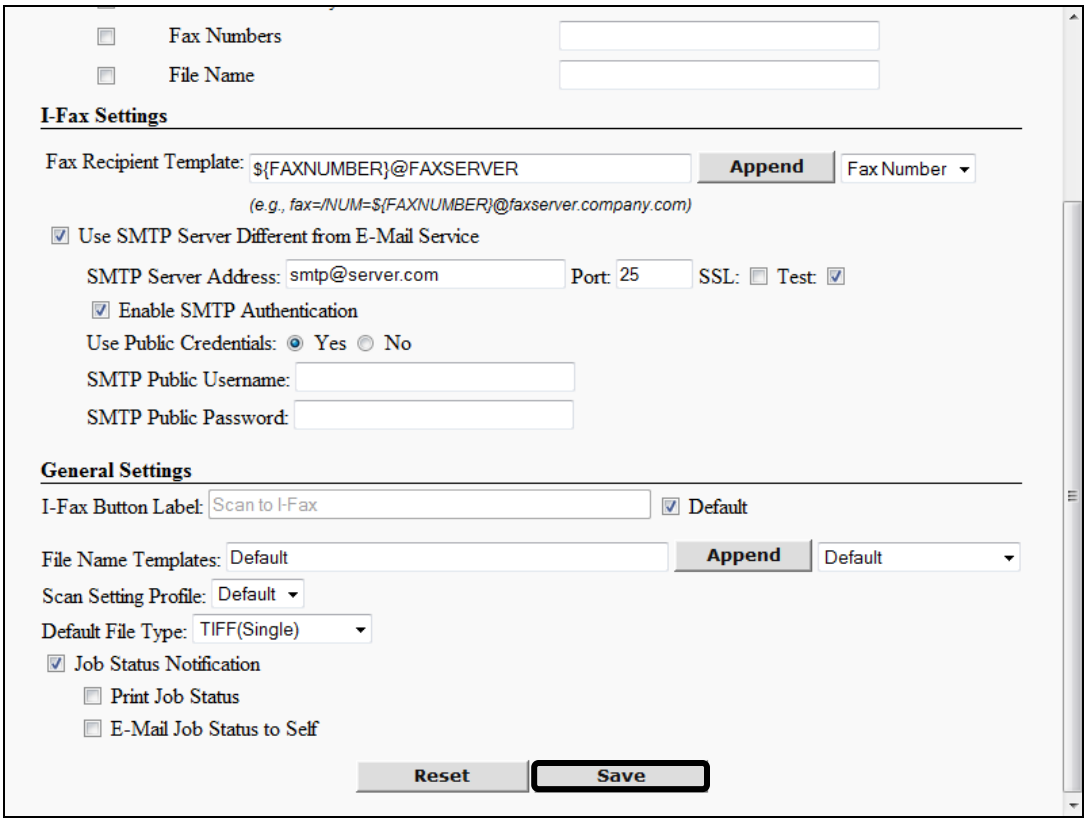
I-Fax Button Label: Enter the label for the [Scan to I-Fax] key that appears on the Authorized Send MAIN screen on the machine. It is a required text box that cannot be left blank. The number of any characters permitted is restricted by the width of the Scan to I-Fax icon.

Default: Select this check box if you want to use the default I-Fax Button Label setting ('Scan to I-Fax'). The I-Fax Button Label text box cannot be changed when the Default check box is selected.

File Name Templates: Enter one or more File Name Templates which the user can select when creating a scan job. The names in this list are created under the <File Name> tab. See "Configuring the File Name," on p. 407. The default value is 'Default'. Separate entries must be separated by commas. You can enter the File Name Templates manually or select the Templates from the Append drop-down list and click [Append].

Append:	Click [Append] to add a File Name Template (set in the Append drop-down list) to the string in the [File Name Templates] text box.
Append drop-down:	Select a pre-defined File Name Template that is added to the string in the [File Name Templates] text box after you click [Append].
Scan Setting Profile:	Select a scan setting profile from the drop-down list. The default setting is ‘Default’, which corresponds to the default settings on the Scan Settings screen.
Default File Type:	Select a default file type in which you want to send your I-Fax documents. The file types displayed in the drop-down list may vary, based on machine capabilities and installed options.
Job Status Notification:	Select this check box if you want the logged on user of the Scan to I-Fax session to receive confirmation printout or email.
Print Job Status:	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to I-Fax session to receive a confirmation printout.
E-Mail Job Status to Self:	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to I-Fax session to receive a confirmation email.

5. Click [Save].



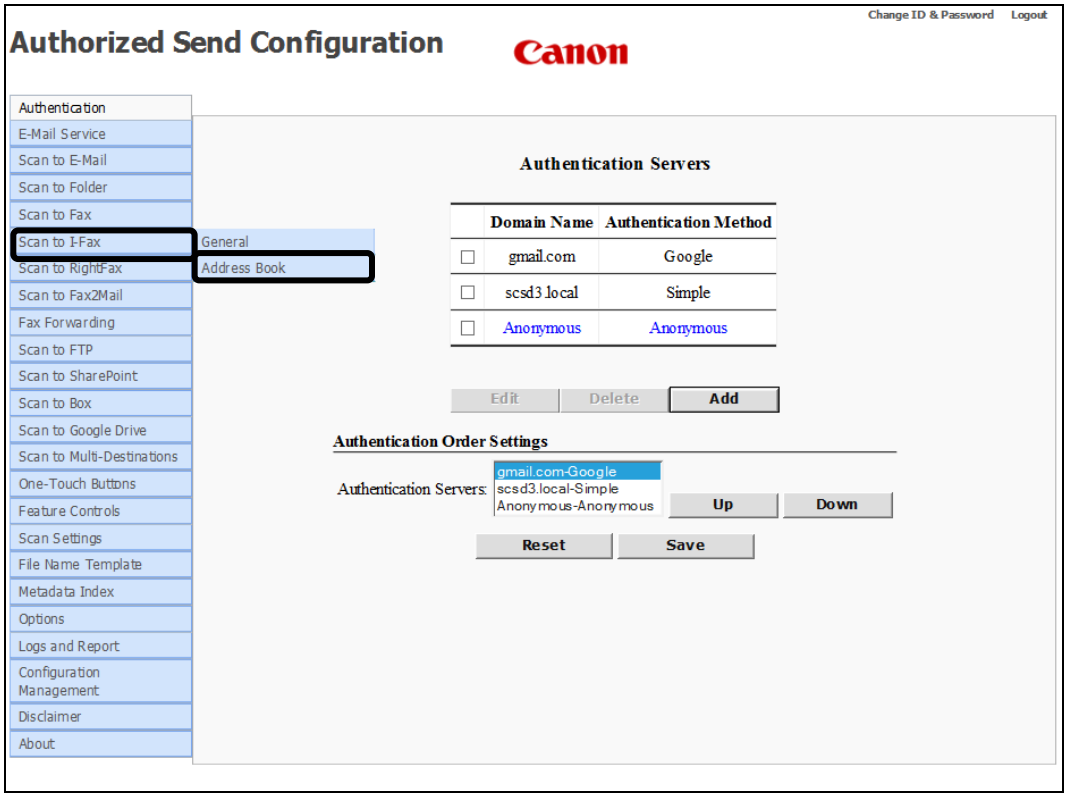
NOTE

- Validation is performed after you click [Save] to see if:
  - The [Address Book] and [Fax Numbers] check boxes are both selected, and the [Fax Numbers] text box is not empty.
  - The maximum number of acceptable characters in the [Fax Numbers] text box is 255.
  - The [Fax Numbers] text box default value contains only numbers, commas, or semicolons.
- If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.9.1 Creating an I-Fax Address Book

You can create an I-Fax Address Book to store your fax numbers.

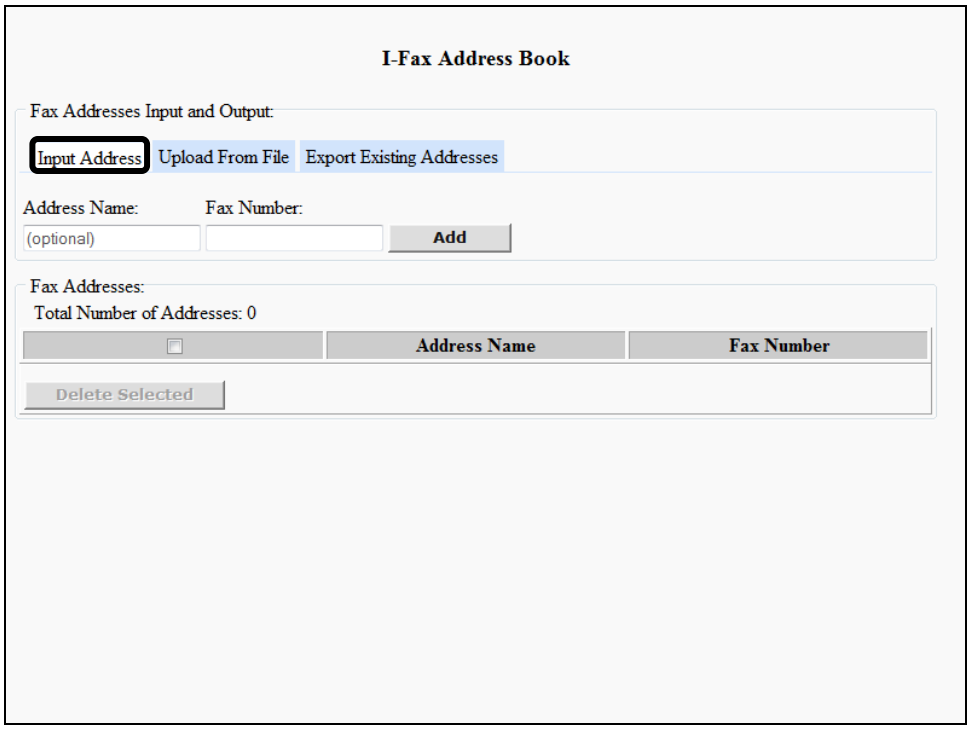
1. Click [Scan to I-Fax] → [Address Book].



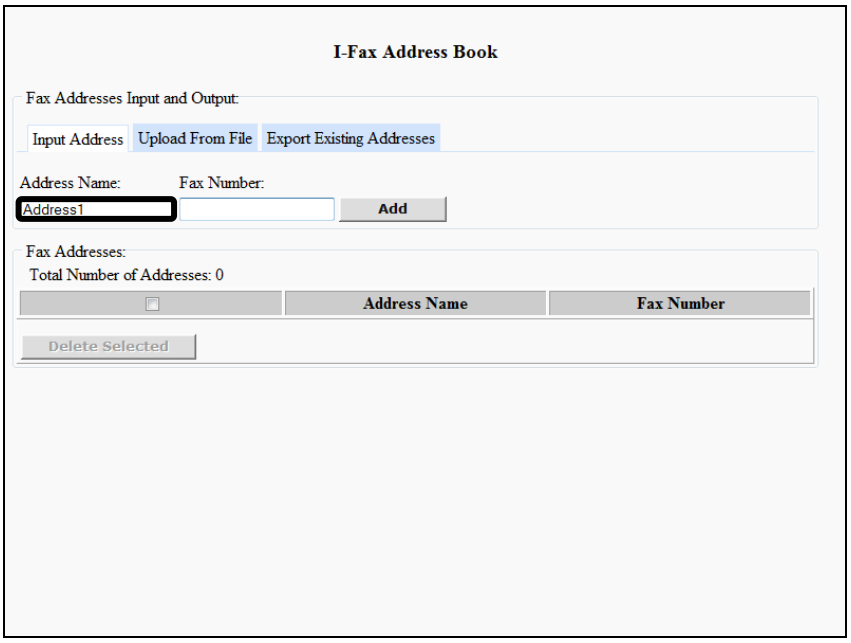
The I-Fax Address Book screen is displayed.

2. Input a fax address individually or upload it from a file. You can also export saved fax addresses to a text file.

   2.1 To input a fax address individually, click the [Input Address] tab.

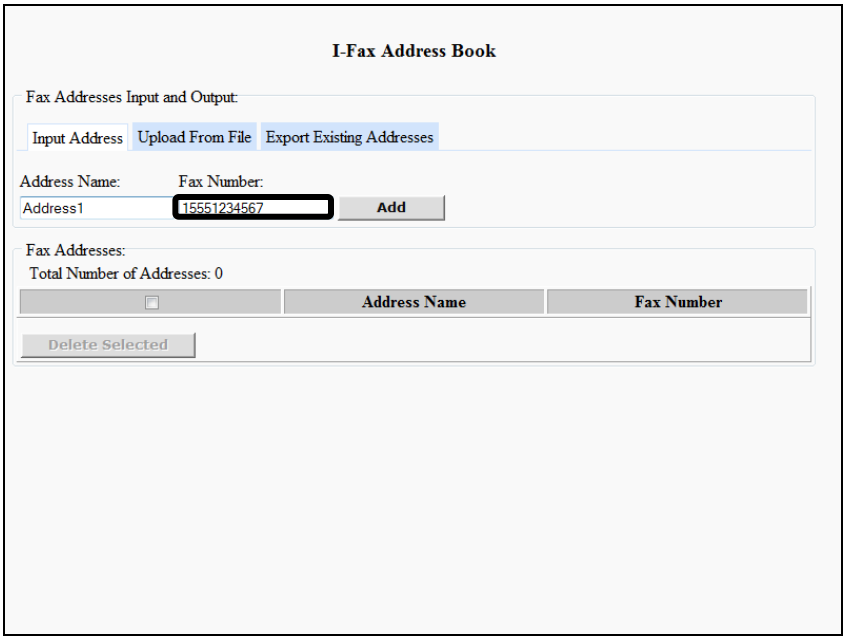


2.1.1 Enter an address name in the [Address Name] text box.



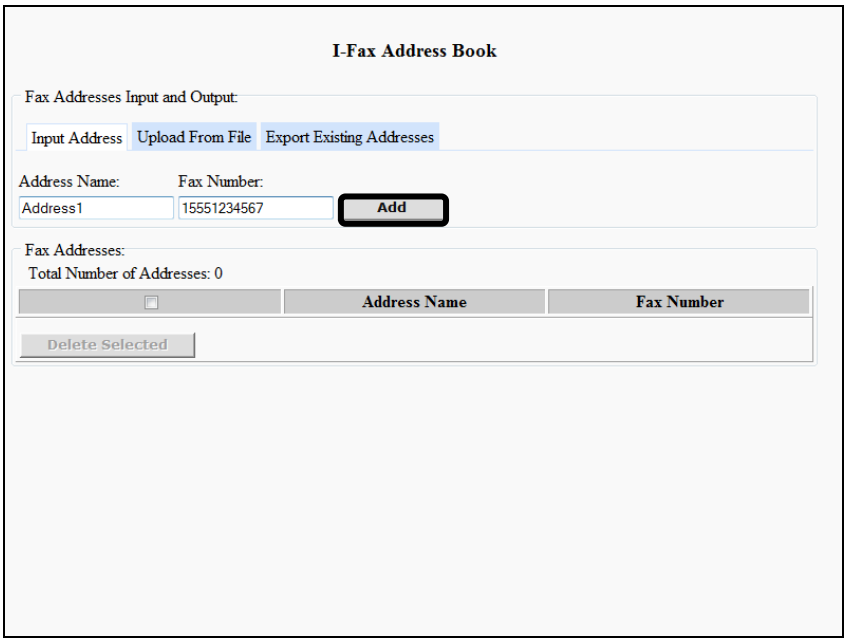
You can enter a maximum of 32 alphanumeric characters for the address name.

2.1.2 Enter the fax number in the [Fax Number] text box.



You can enter an unlimited length of alphanumeric characters, periods (“.”), hyphens (“-“), spaces (“ “), and underscores (“_”).

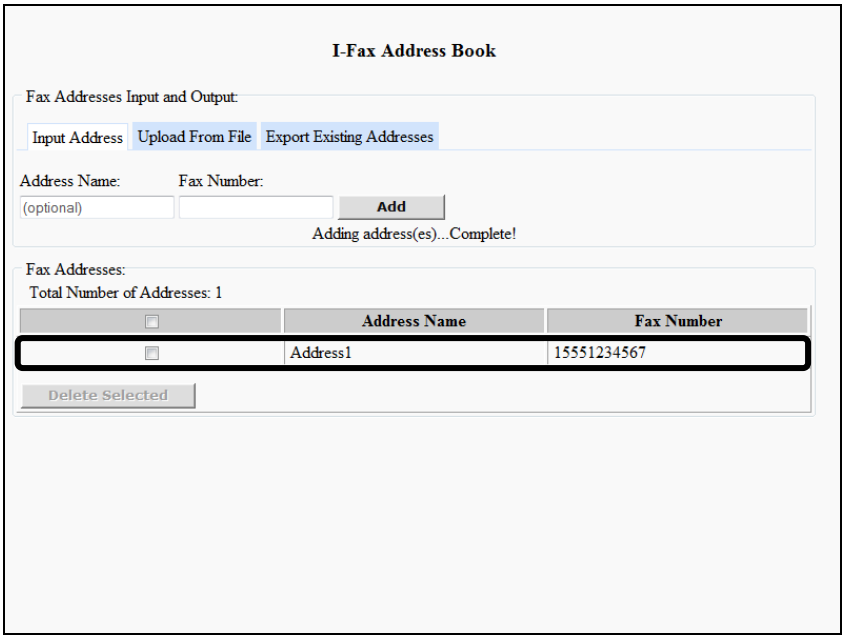
2.1.3 Click [Add] to start the validation process.



Validation is performed to see if:

- The [Fax Number] text box is not empty.
- The [Fax Number] text box contains only alphanumeric characters, periods (“.”), hyphens (“-“), spaces (“ “), and underscores (“_”).
- The fax number is not a duplicate of any number already entered in the Fax Address Book.
- The maximum number of fax addresses does not exceed 1000.

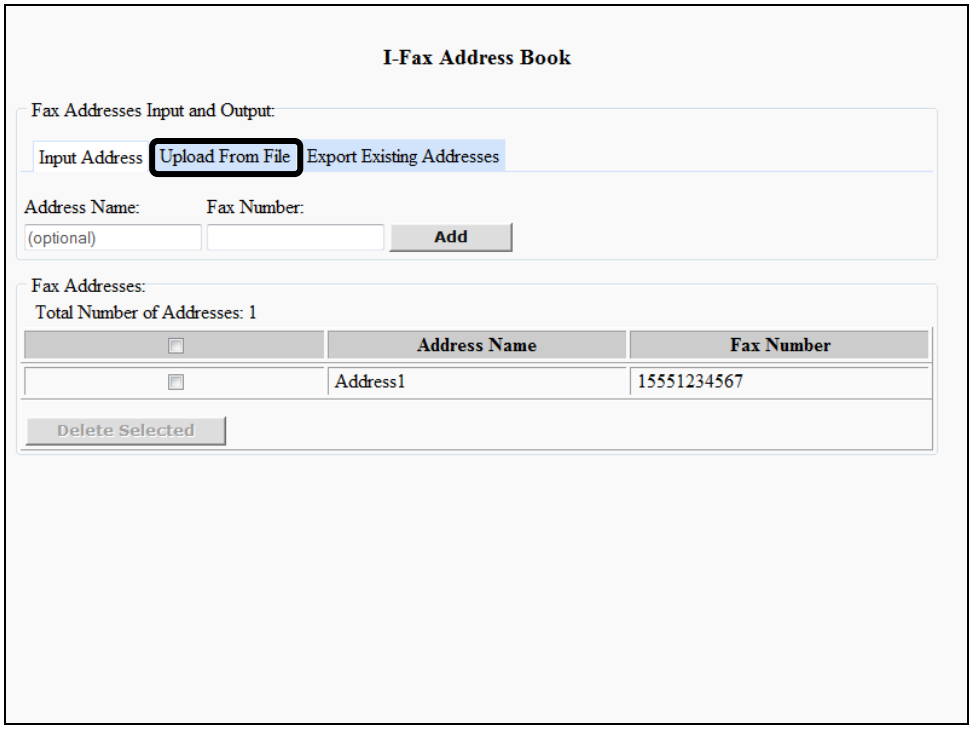
If the validation process is successful, the added fax address appears in the Fax Address table. If it fails, an error message is displayed in red.



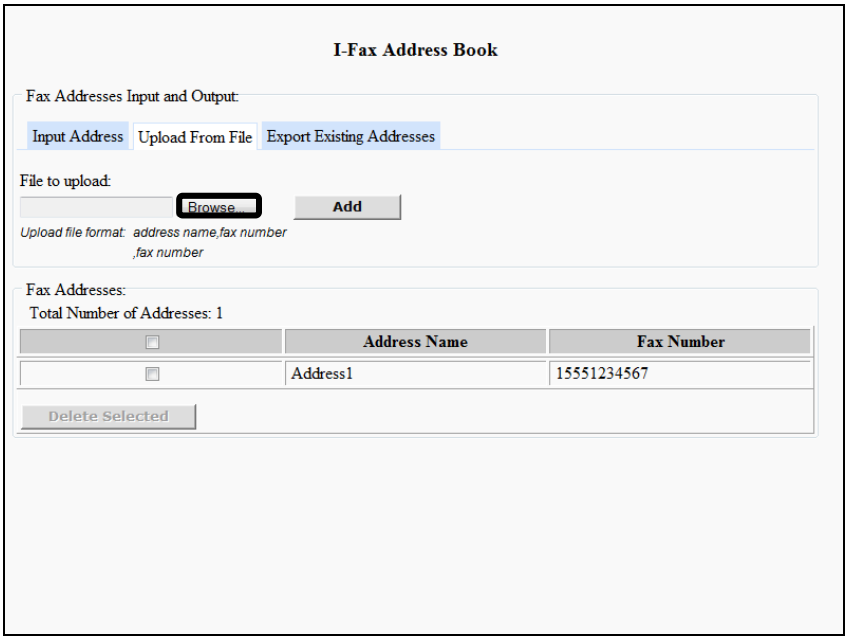
NOTE

<Total Number of Addresses:> displays the number of fax addresses that are in the Fax Addresses table. This number varies as fax addresses are added to, or deleted from, the Fax Addresses table.

2.2 To upload a fax address from a file, click the [Upload From File] tab.



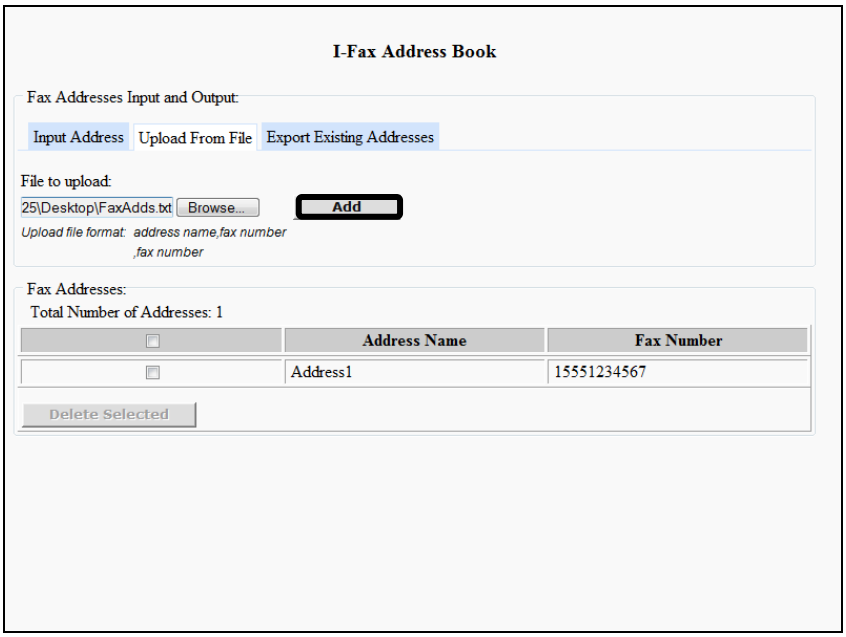
2.2.1 Click [Browse] →navigate to the drive or directory containing the file to upload → select the file → click [Open].



NOTE

The uploaded file extension must be ".txt" or ".csv," and is not case-sensitive.

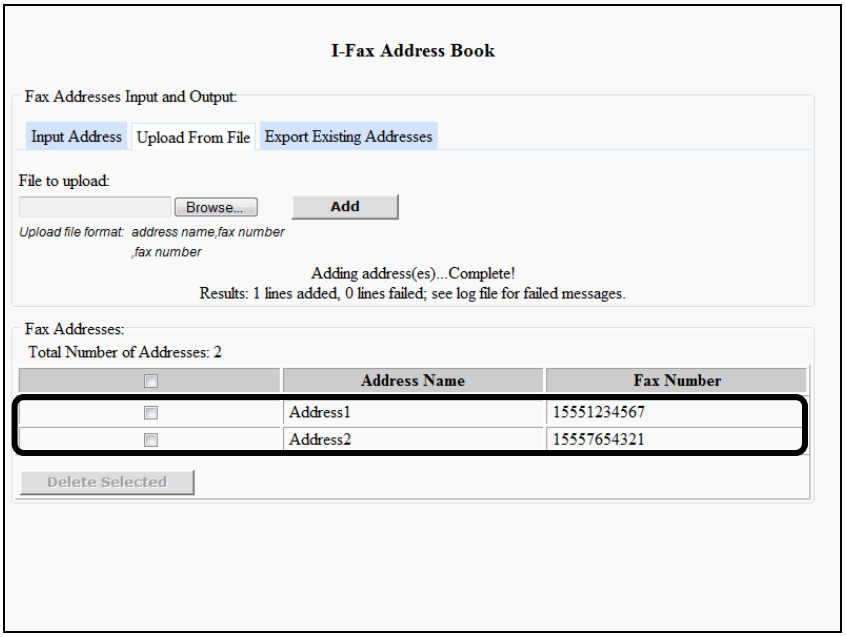
2.2.2 Click [Add] to start the validation process.



Validation is performed to see if:

- The uploaded file is a text file with the following format requirements:
  - Each fax address entry is on a separate line.
  - Each fax address entry contains an address name and fax number separated by a comma (“address_name,fax_number”).
  - Since the address name is optional, the format “,fax_number” is also acceptable.
- The address name, if used, does not exceed the maximum number of 32 characters. If the fax address name exceeds 32 characters, it is truncated.

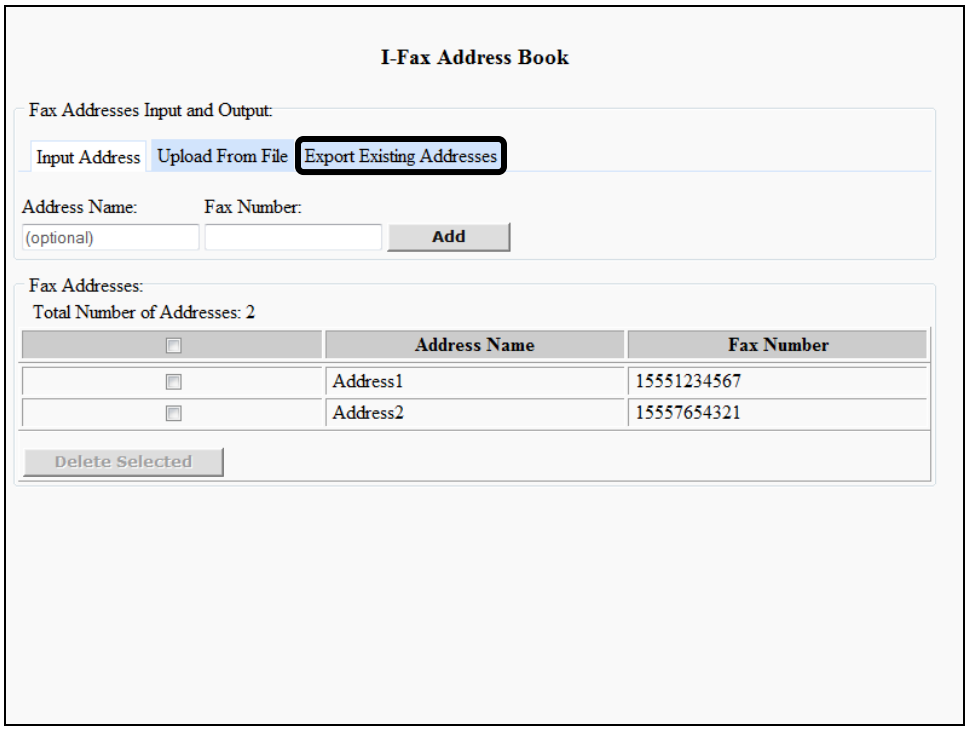
If the validation process is successful, the added fax address appears in the Fax Addresses table. If it fails, an error message is displayed in red.



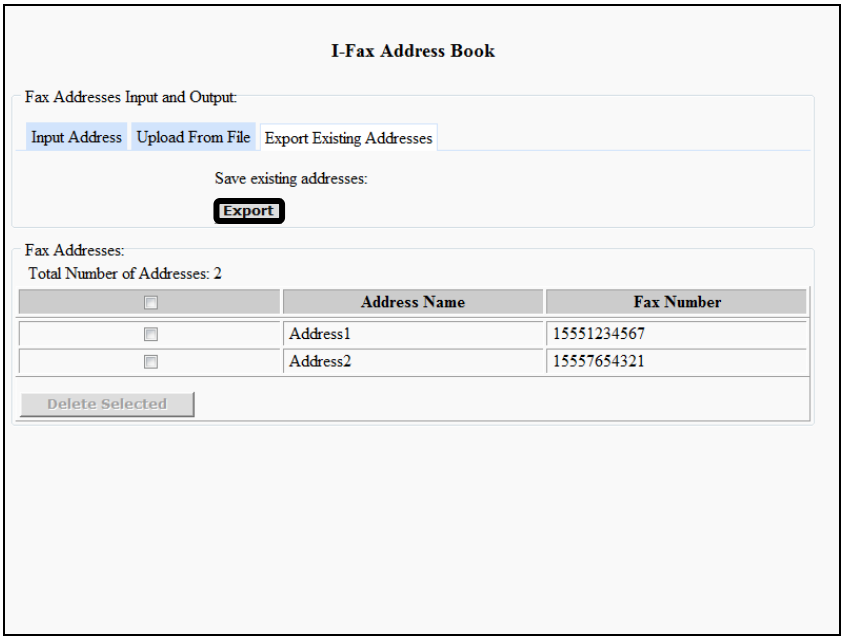
NOTE

- Any line entry in the uploaded file that is in an invalid format, is reported as a failure with the line number. That line is skipped, and uploading continues with the next line.
- Any fax address in the uploaded file that has already been saved is ignored, and reported as a duplicate. Only the number of duplicates found in the file is reported, not the exact line number.

2.3 To export the existing fax addresses to a text file, click the [Export Existing Addresses] tab.



2.3.1 Click [Export].



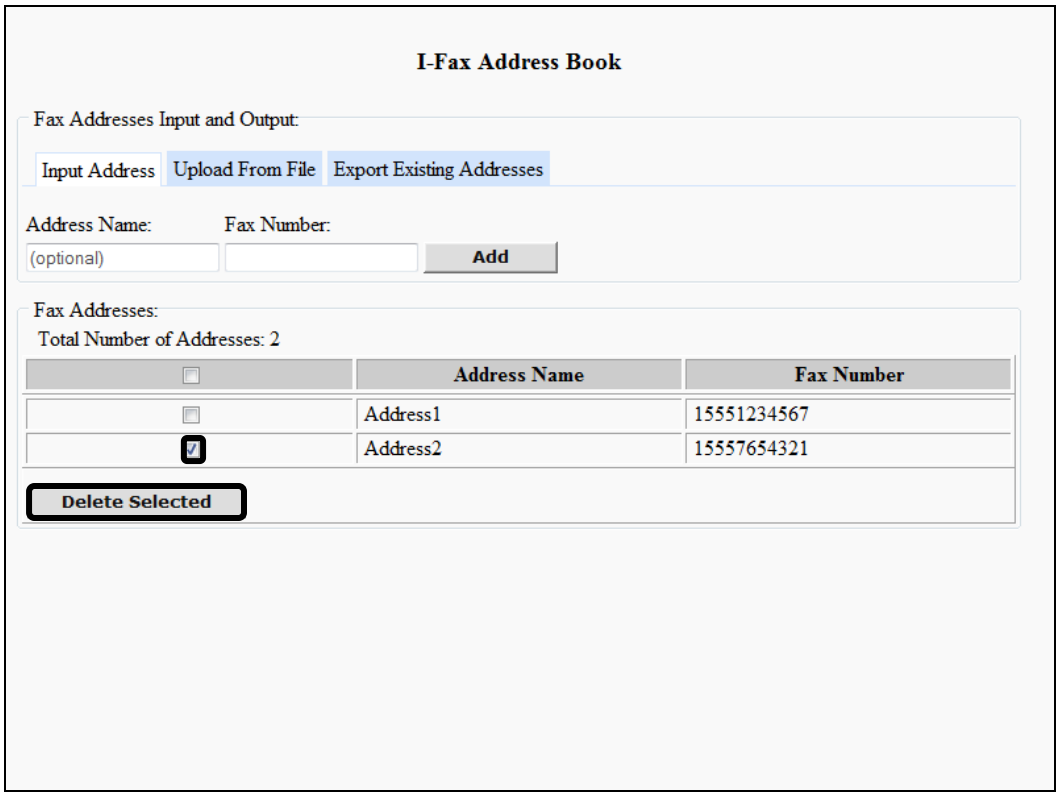
The existing fax addresses are exported to a text file.

The exported text file is formatted, as described below:

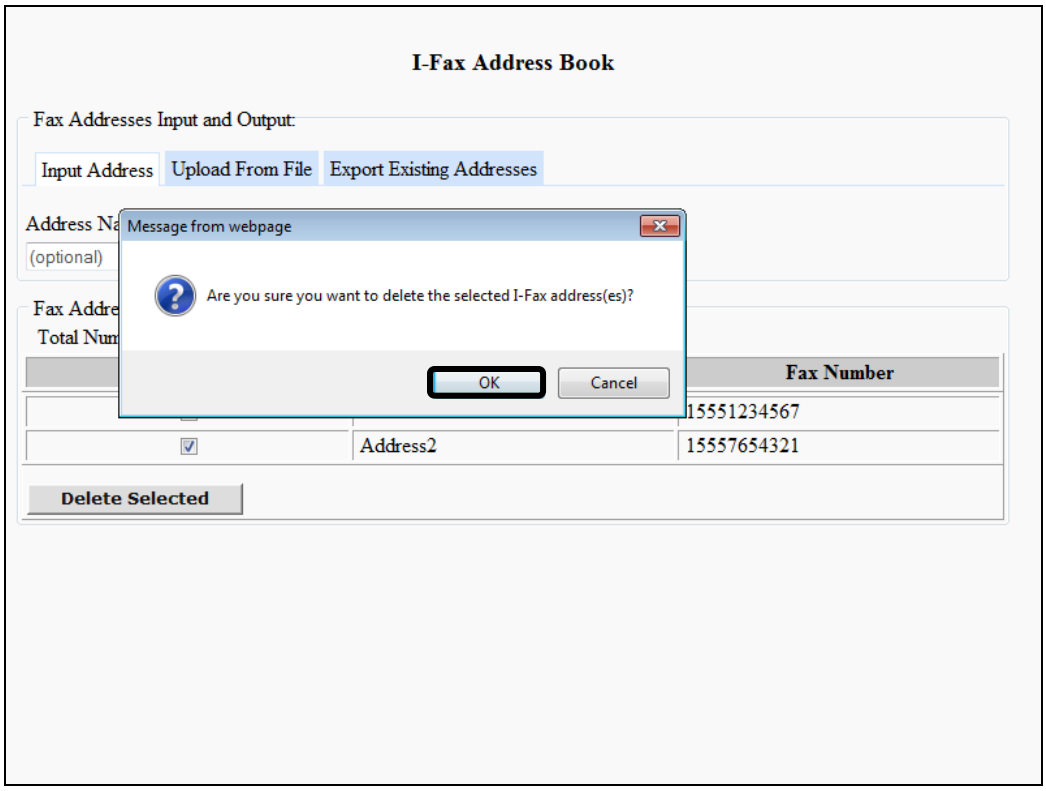
- Each fax address entry is on a separate line.
- Each fax address entry contains an address name and fax number, separated by a comma (“address_name,fax_number”).
- Since the address name is optional, the format “,fax_number” is also acceptable.

2.3.2 Click [File] ➞ [Save As] ➞ navigate to the drive or directory to where you want to save the file ➞ click [Save].

3. To delete a fax address, click the check box next to the fax address you want to delete → click [Delete Selected].



4. Click [OK].



If you do not want to delete the fax address, click [Cancel].

The fax address is deleted from the list.

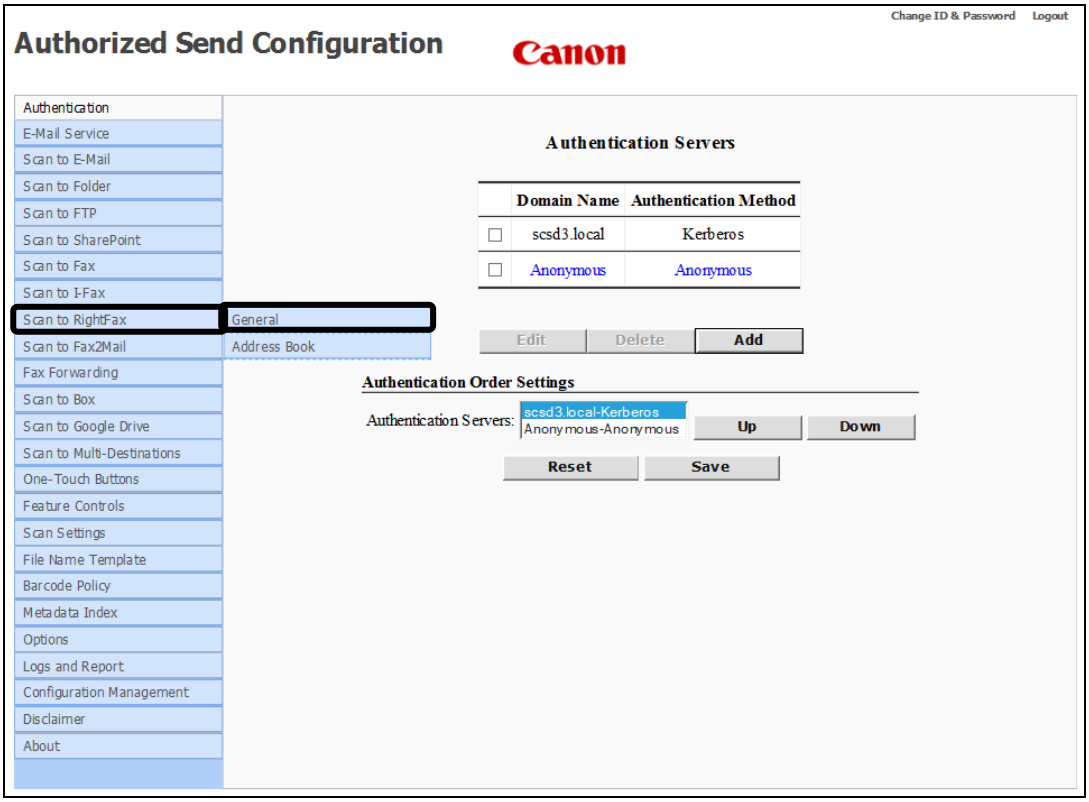
2.10 Configuring the Scan to RightFax Settings

You can configure the Scan to RightFax function, which enables users to scan and send documents to the RightFax service, which can integrate into email and document management applications.

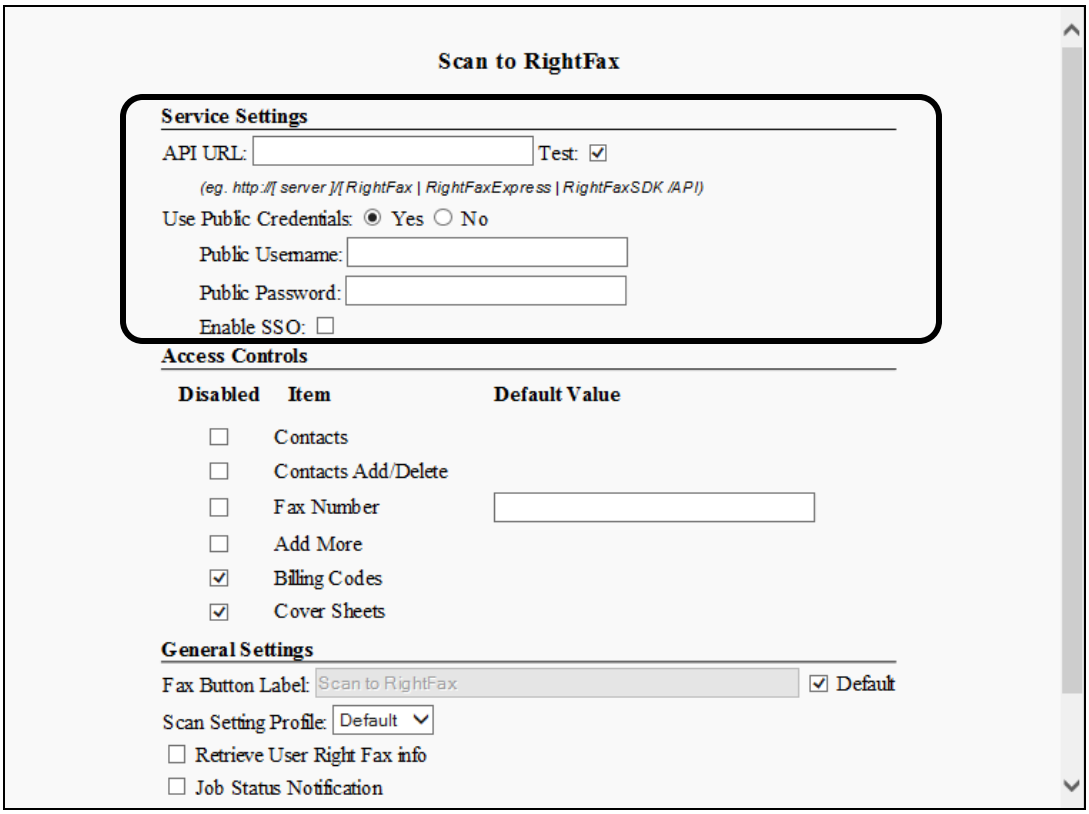
IMPORTANT

- The Scan to RightFax function is available only after the System Administrator has installed and started the “FaxServiceActivation.jar” service.
- If an AMS enabled login application is installed and running on the machine, [Scan to RightFax] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the Scan to RightFax function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [Scan to RightFax] → [General].



2. Configure the settings under <Service Settings>.

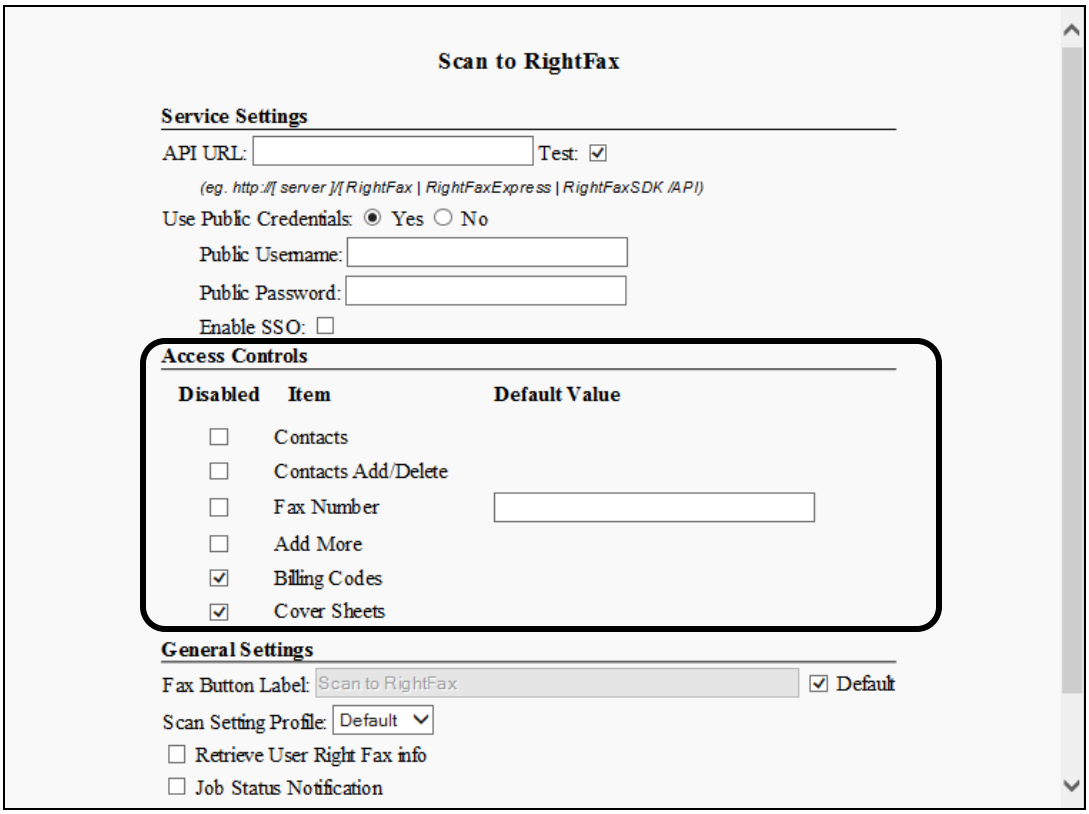


Service Settings

API URL:	Enter the URL of the RightFax API. It should be the same as the RightFax API URL set in the RightFax configuration screen. It is blank by default.
Test:	Select this check box to validate that the [API URL] setting is an active connection and is a valid RightFax server.
Use Public Credentials:	Select “Yes” to indicate that the Public Username, Public Password, and Enable SSO fields will be configured by the administrator. Select “No” to manually enter the public credentials data in the RightFax configuration screen The default selection is “No”.

Public Username:	Enter a valid user name to communicate with the RightFax server. This field should not be blank.
Public Password:	Enter a valid password (for the Public Username) to communicate with the RightFax server. This field should not be left blank.
Enable SSO:	Select this check box to enable Single Sign On for Authorized Send into the RightFax server. [Enable SSO] is not selected by default.

3. Configure the settings under <Access Controls>.



Access Controls

Disabled Item Column

Contacts:	Check this box to disable the [Contacts] button on the “Scan to RightFax” screen on the machine console. This check box is not selected by default.
Contacts Add/Delete:	Check this box to disable the [Add] and [Delete] buttons to appear in the “RightFax Contacts” screen on the machine console. This check box is not selected by default, and is only available when the [Contacts] check box above is selected.
Fax Number:	Check this box to disable display of a default fax number text box on the “Scan to RightFax” screen.
Add More:	Check this box to disable the [Add More] button on the “Scan to RightFax” screen on the machine console. This check box is not selected by default.

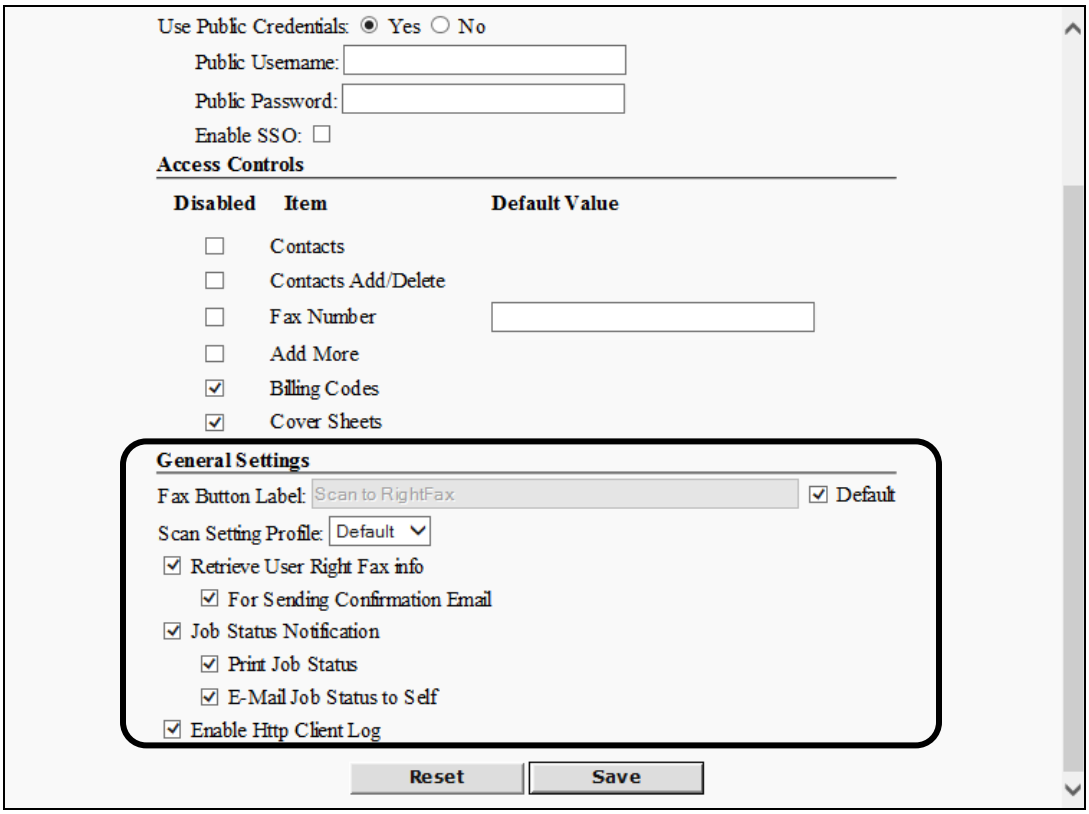
Billing Codes: Check this box to disable the [Billing Codes] button on the "Scan to RightFax" screen on the machine console. This check box is selected by default.

Cover Sheets: Check this box to disable the [Cover Sheets] button on the "Scan to RightFax" screen on the machine console. This check box is selected by default.

Default Value Column

Fax Number: If the [Fax Number] check box above is not selected, enter the number to appear in the [Default Fax Number]. This field can accept up to 25 numeric-only characters.

4. Configure the settings under <General Settings>.



General Settings

Fax Button Label:	If the [Default] check box is selected, enter a new name for the [Scan to RightFax] button on the machine console. By default, the [Default] check box is selected and the label is “Scan to RightFax”. This text field is active only when the [Default] check box is not selected.
Default:	Select this check box if you want to use the default button on the machine console (“Scan to RightFax”). This check box is selected by default.
Scan Setting Profile:	Select a scan profile from the pull-down list. The scan profiles are set using the Scan Setting Profile function.
Retrieve User Right Fax info:	Select this check box to display the [For Sending Confirmation Email] check box. If this check box is selected and the [For Sending…] check box is not selected when the RightFax configuration is saved, this check box reverts to unselected. This is unselected by default.

For Sending Confirmation Email:	This check box appears only when the [Retrieve User Right Fax info] check box is selected. Select this check box to send all confirmation emails to the email address associated with the current user's RightFax account. If a scan to RightFax destination is part of a scan to multi-destination or one-touch button configuration, the email is sent only if all destinations are to RightFax.
Job Status Notification:	Select this check box if you want the logged on user of the Scan to RightFax session to receive confirmation printout or email.
Print Job Status	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to RightFax session to receive a confirmation printout.
E-Mail Job Status to Self	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to RightFax session to receive a confirmation email.
Enable Http Client Log	Select this check box to enable more RightFax API and HTTP requests and responses to be recorded in the debugging log.

5. Click [Save].

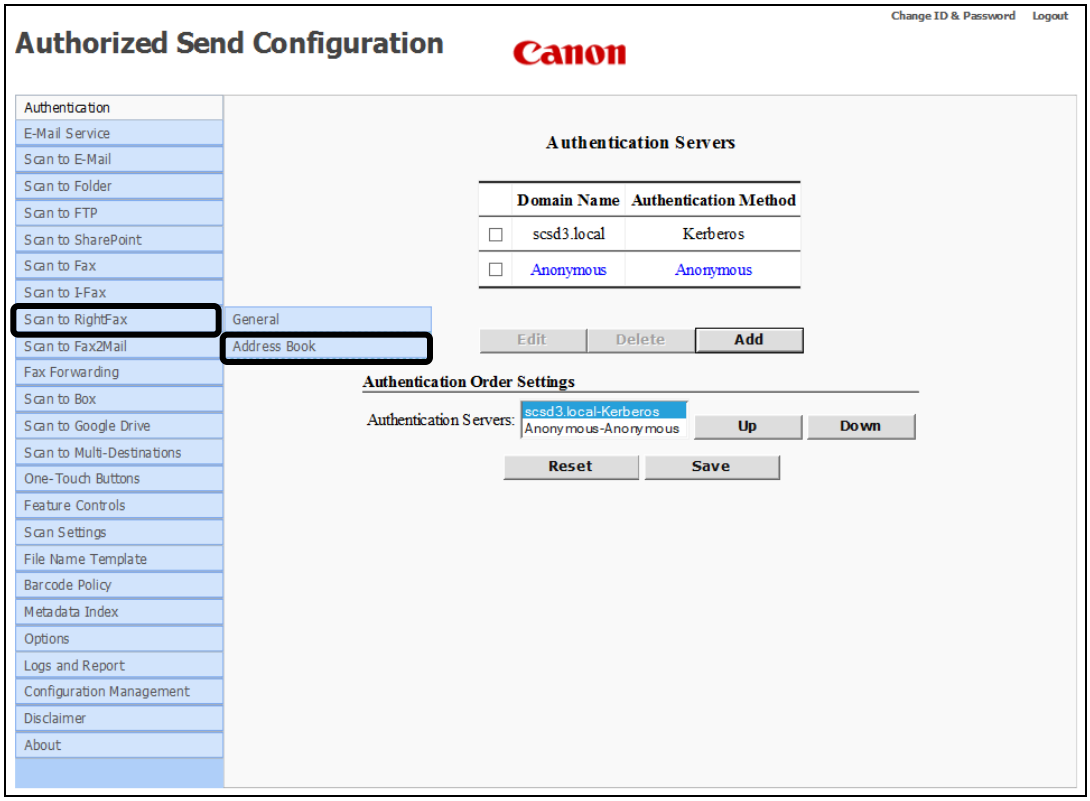
NOTE

If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.10.1 Creating a Scan to RightFax Address Book

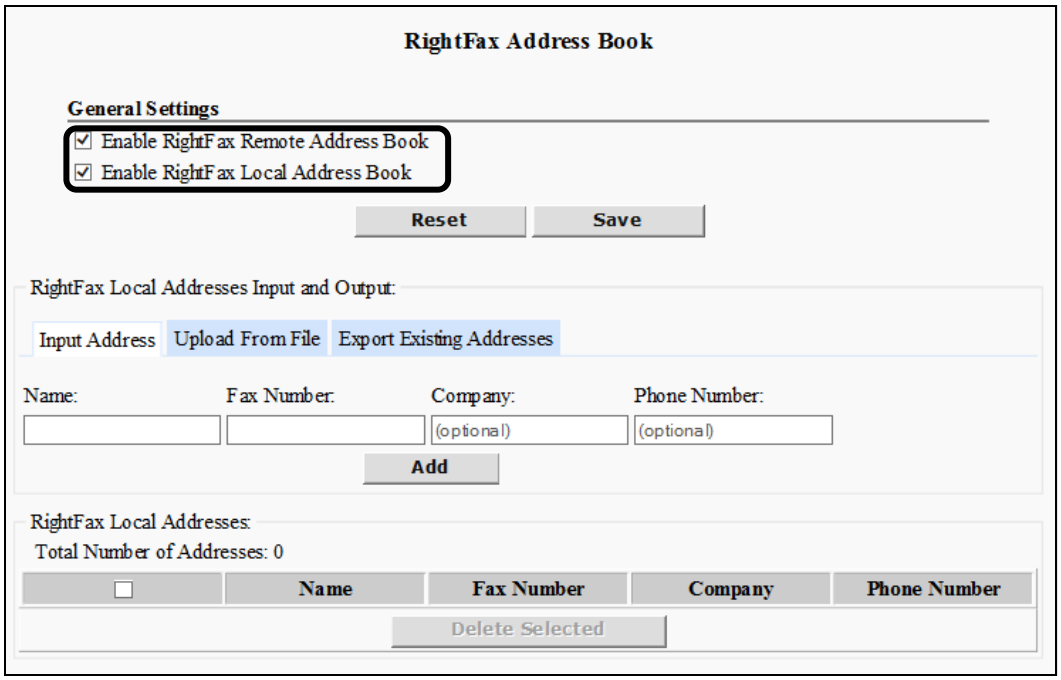
You can create a Scan to RightFax Address Book to store your fax numbers.

1. Click [Scan to RightFax] → [Address Book].



The RightFax Address Book screen is displayed.

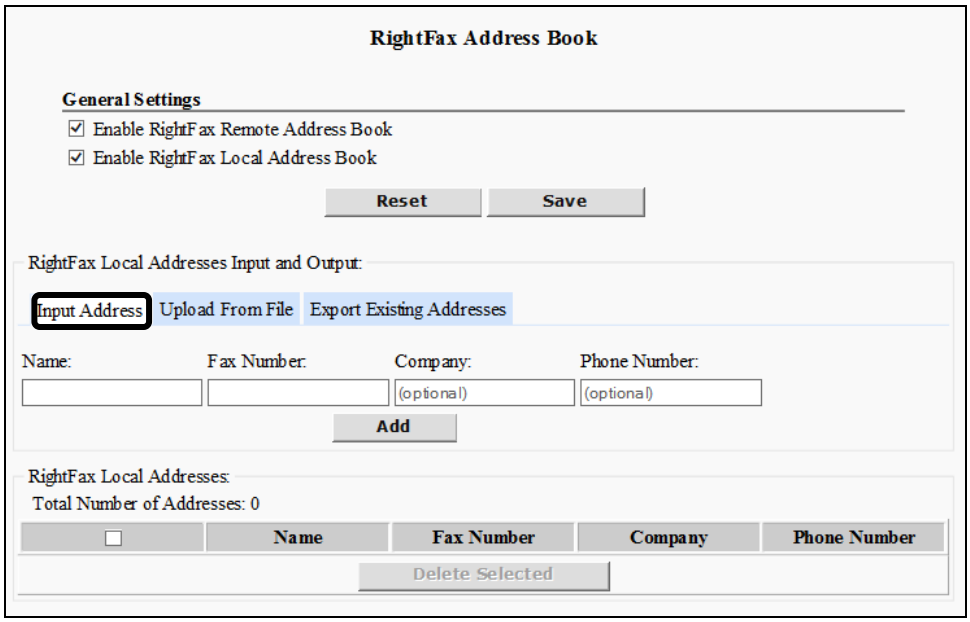
2. Select to which address books (RightFax remote and local) the end user has access.



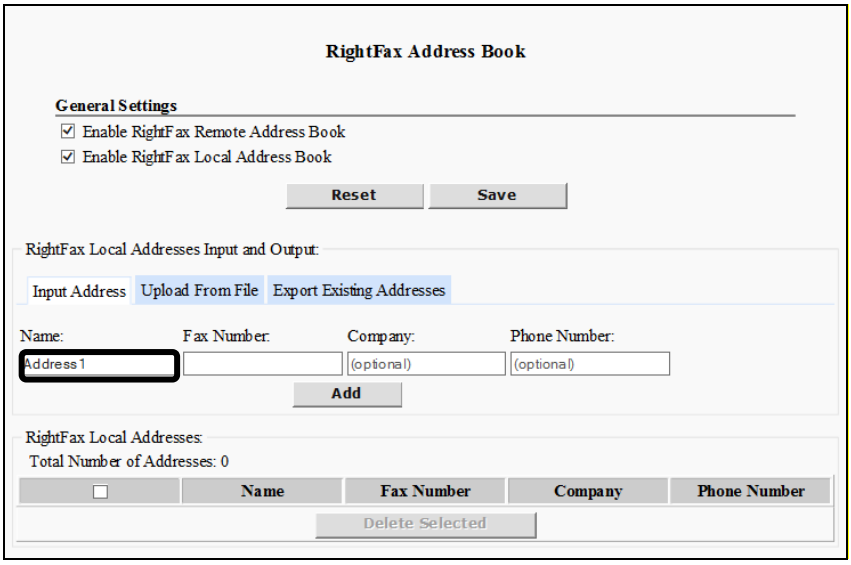
Enable RightFax Remote Address Book	Select this check box if you want the end user to be able to access address book entries stored on the remote RightFax server. If this is not selected, either only the local address book is available (if the local address book is enabled), or the [Contacts] button is not displayed (if the local address book is disabled). This check box is enabled by default.
Enable RightFax Local Address Book	Select this check box if you want the end user to be able to access address book entries stored in the local address book. If this is not selected, either only the Shared Contacts list is available (if the remote address book is enabled), or the [Contacts] button is not displayed (if the remote address book is disabled). This check box is enabled by default.

3. Input a fax address individually or upload it from a file. You can also export saved fax addresses to a text file.

   3.1 To input a fax address individually, click the [Input Address] tab.

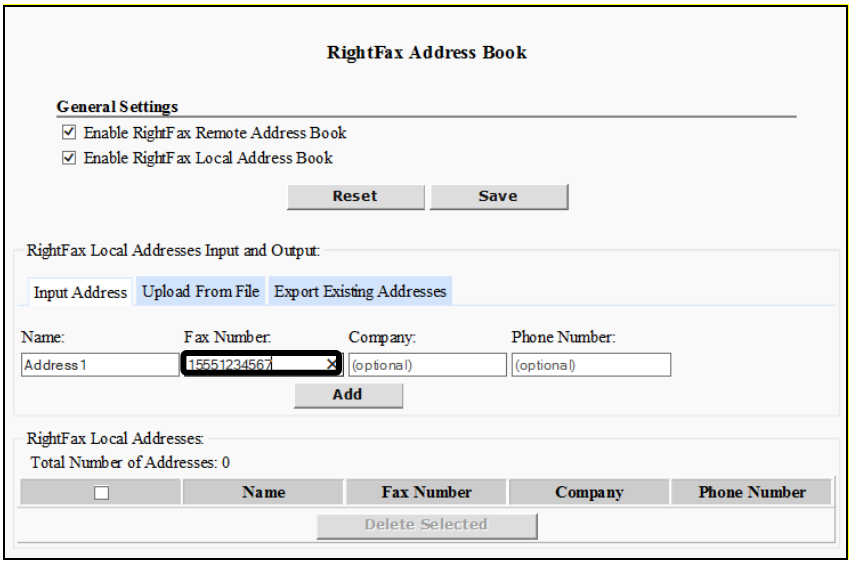


3.1.1 Enter an address name in the [Name] text box.



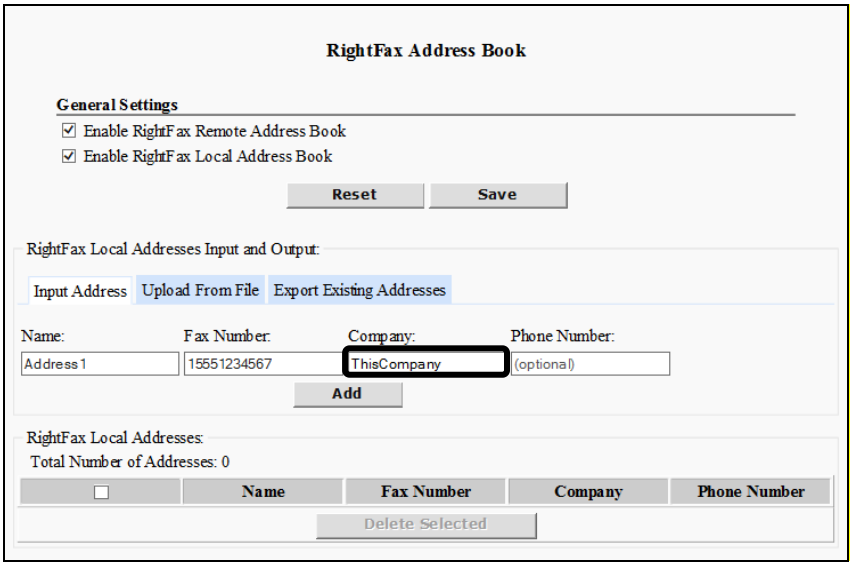
You can enter a maximum of 32 alphanumeric characters for the name.

3.1.2 Enter the fax number in the [Fax Number] text box.



You can enter a maximum of 25 numeric characters for the fax number. There must be a minimum of one character.

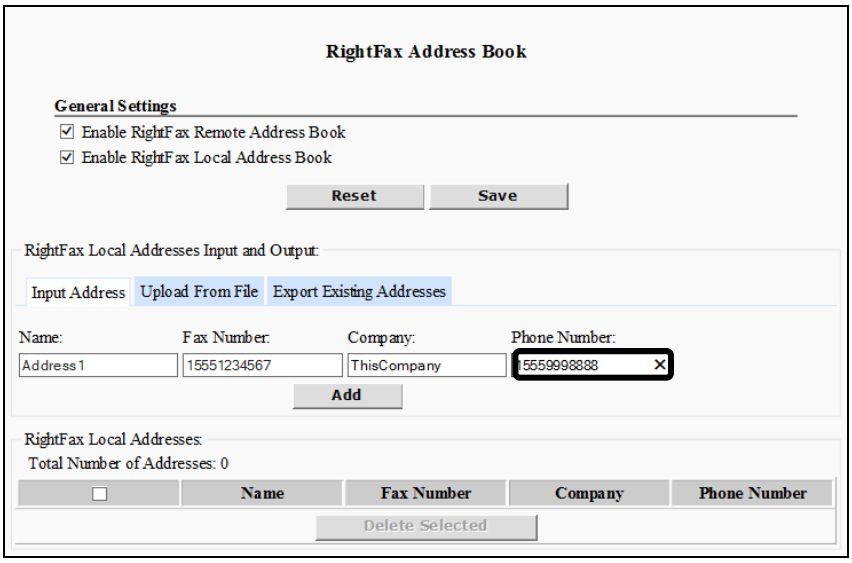
3.1.3 If desired, enter the company name in the [Company] text box.



The [Company] field is optional.

You can enter a maximum of 32 alphanumeric characters for the name.

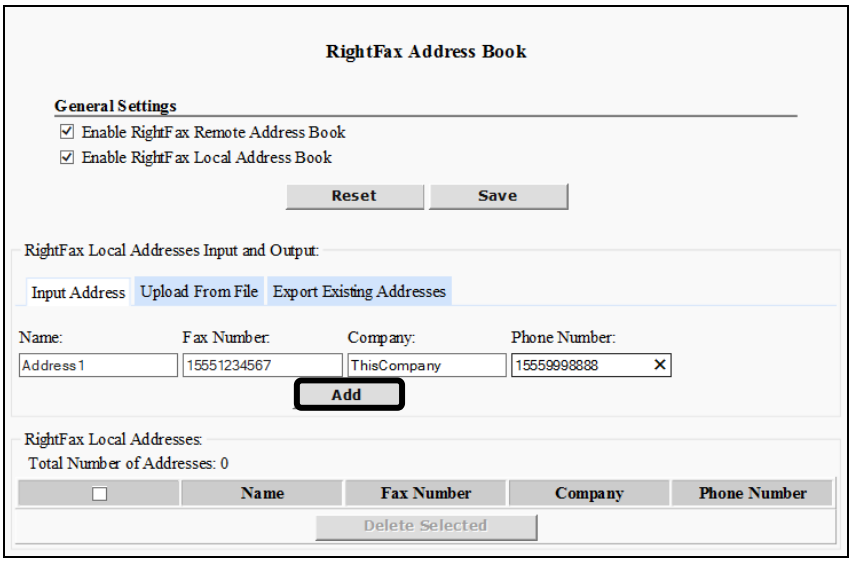
3.1.4 Enter the phone number in the [Phone Number] text box.



The [Phone Number] field is optional.

You can enter a maximum of 25 numeric characters for the phone number.

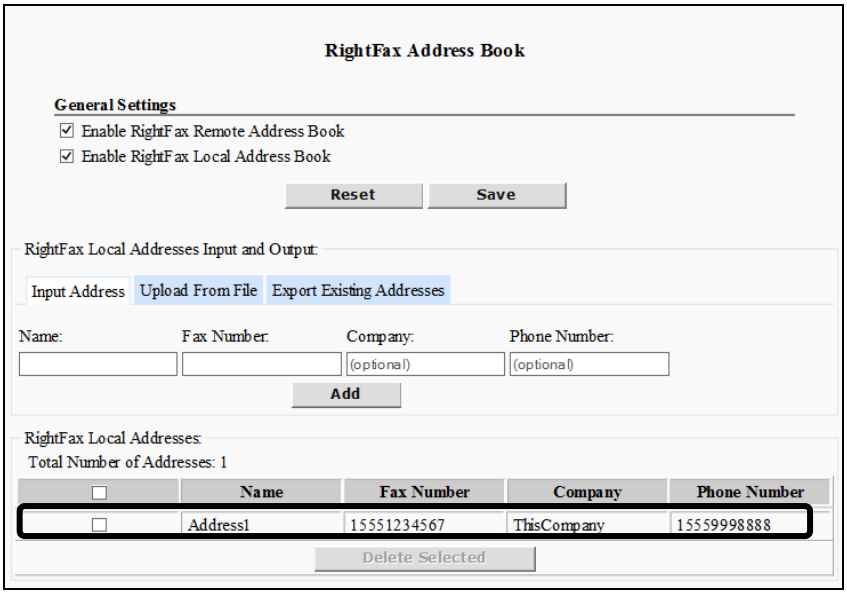
3.1.5 Click [Add] to start the validation process.



Validation is performed to see if:

- The [Name] text box is not empty.
- The [Fax Number] text box is not empty.
- The [Fax Number] text box contains only numeric characters.
- The fax number is not a duplicate of any number already entered in the RightFax Local Address Book.
- The maximum number of fax addresses does not exceed 1000.

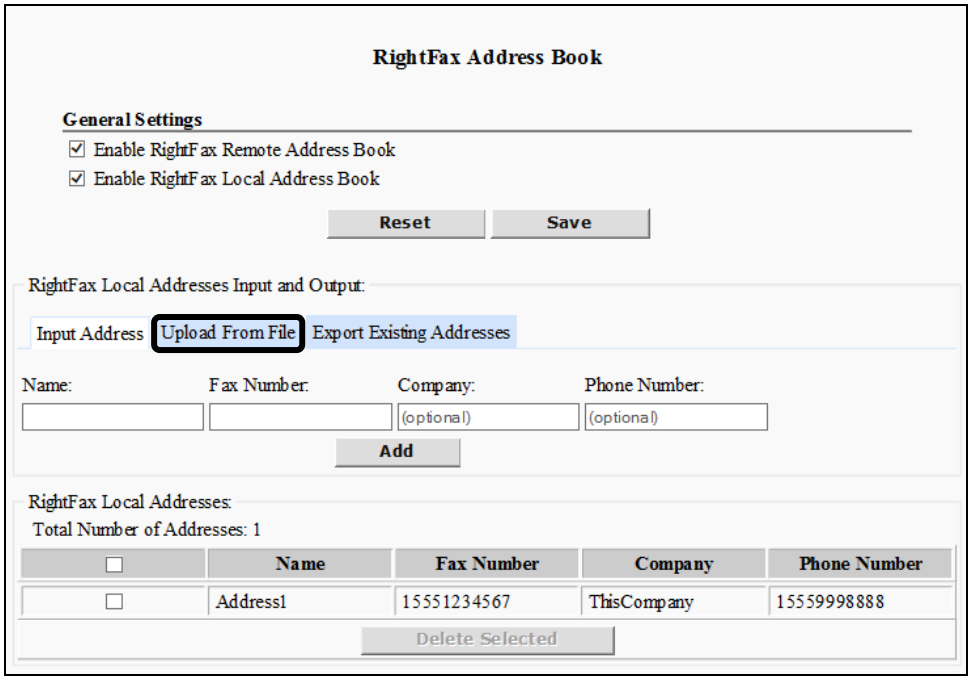
If the validation process is successful, the added fax address appears in the RightFax Local Addresses table. If it fails, an error message is displayed in red.



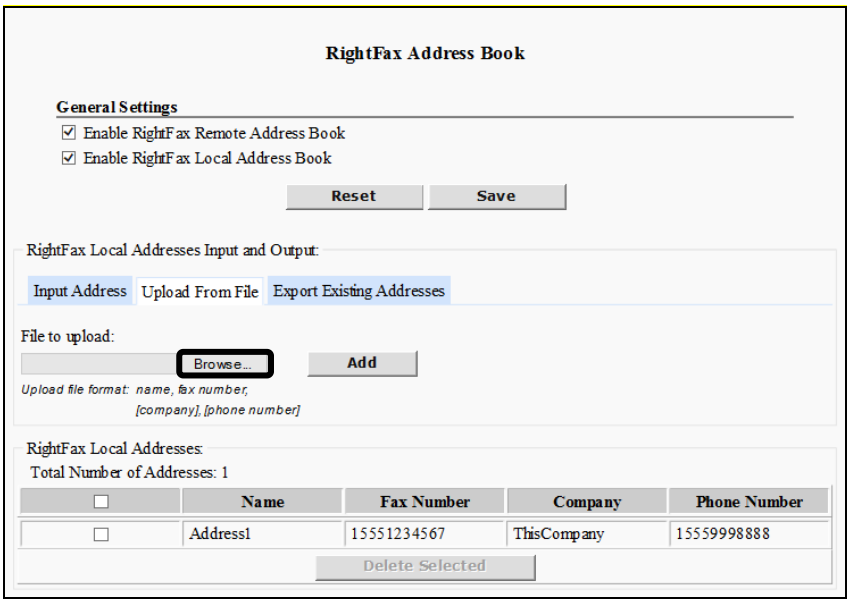
NOTE

<Total Number of Addresses:> displays the number of fax addresses that are in the RightFax Local Addresses table. This number varies as fax addresses are added to, or deleted from, the RightFax Local Addresses table.

3.2 To upload a fax address from a file, click the [Upload From File] tab.



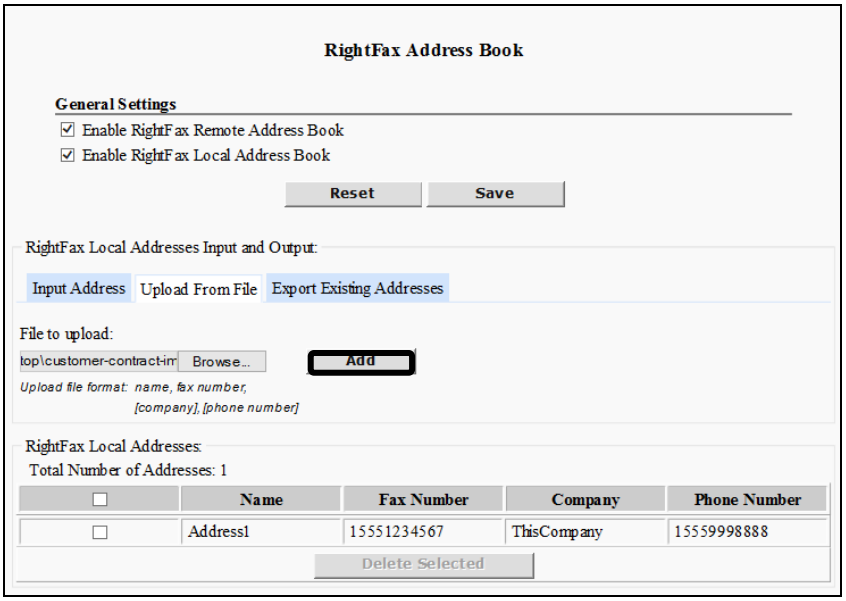
3.2.1 Click [Browse] →navigate to the drive or directory containing the file to upload → select the file → click [Open].



NOTE

The uploaded file extension must be ".txt" or ".csv," and is not case-sensitive.

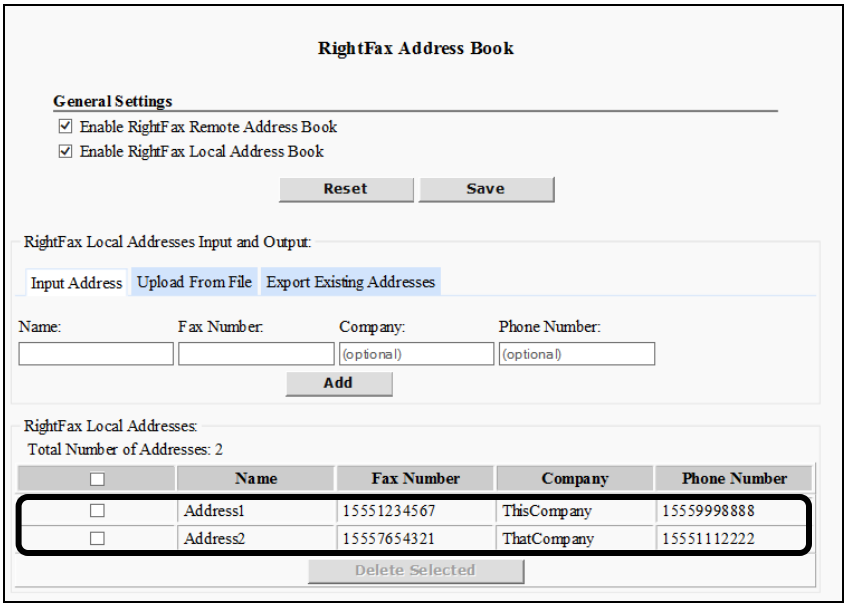
3.2.2 Click [Add] to start the validation process.



Validation is performed to see if:

- The uploaded file is a text/CSV file with the following format requirements:
  - Each fax address entry is on a separate line.
  - Each fax address entry contains at least an address name and fax number separated by a comma, with company name and phone number being optional fields. (“address_name,fax_number,company,phone_number”).
- The address name does not exceed the maximum number of 32 characters. If the fax address name exceeds 32 characters, it is truncated.

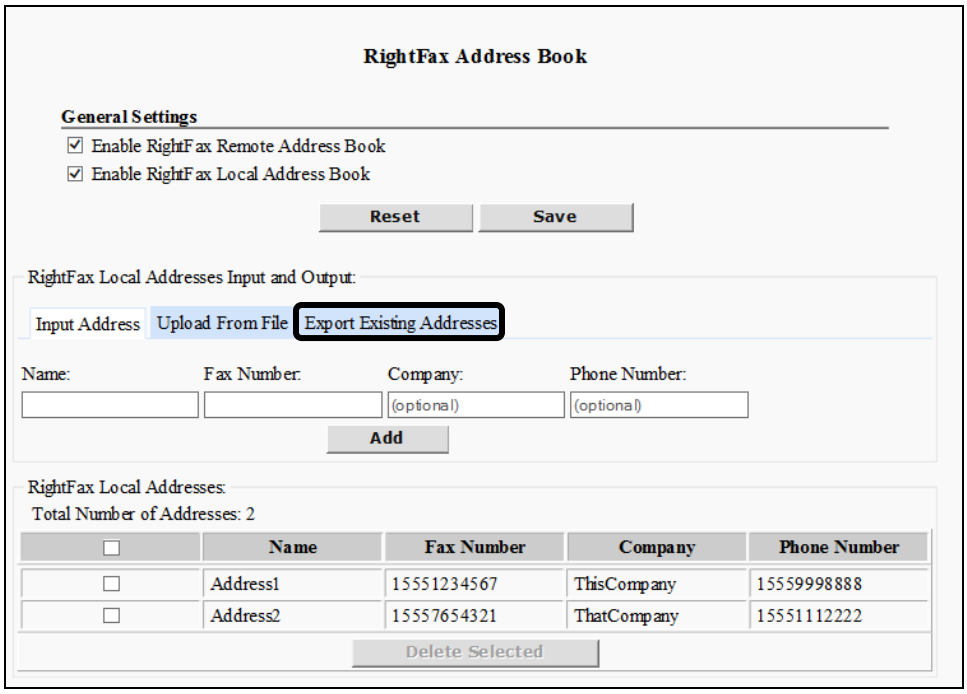
If the validation process is successful, the added fax address appears in the Fax Addresses table. If it fails, an error message is displayed in red.



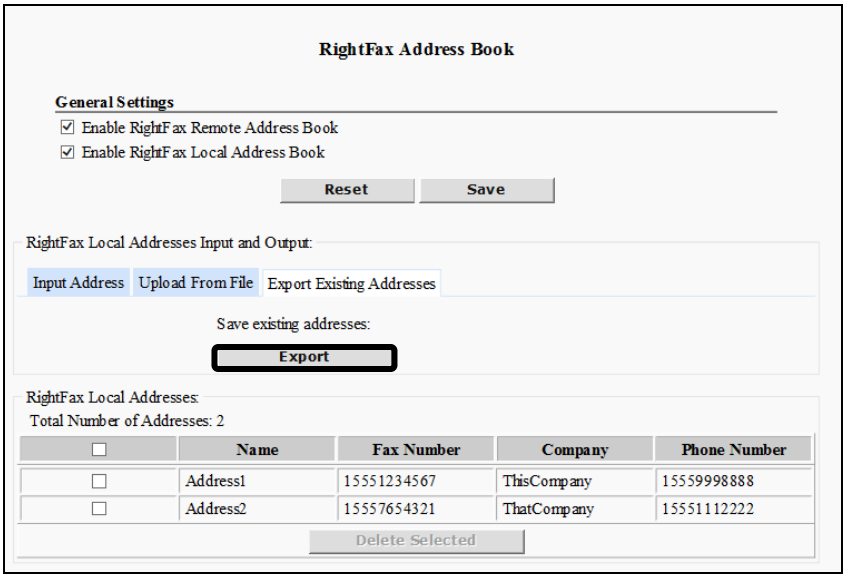
NOTE

- Any line entry in the uploaded file that is in an invalid format, is reported as a failure with the line number. That line is skipped, and uploading continues with the next line.
- Any fax address in the uploaded file that has already been saved is ignored, and reported as a duplicate. Only the number of duplicates found in the file is reported, not the exact line number.

3.3 To export the existing fax addresses to a text file, click the [Export Existing Addresses] tab.



3.3.1 Click [Export].



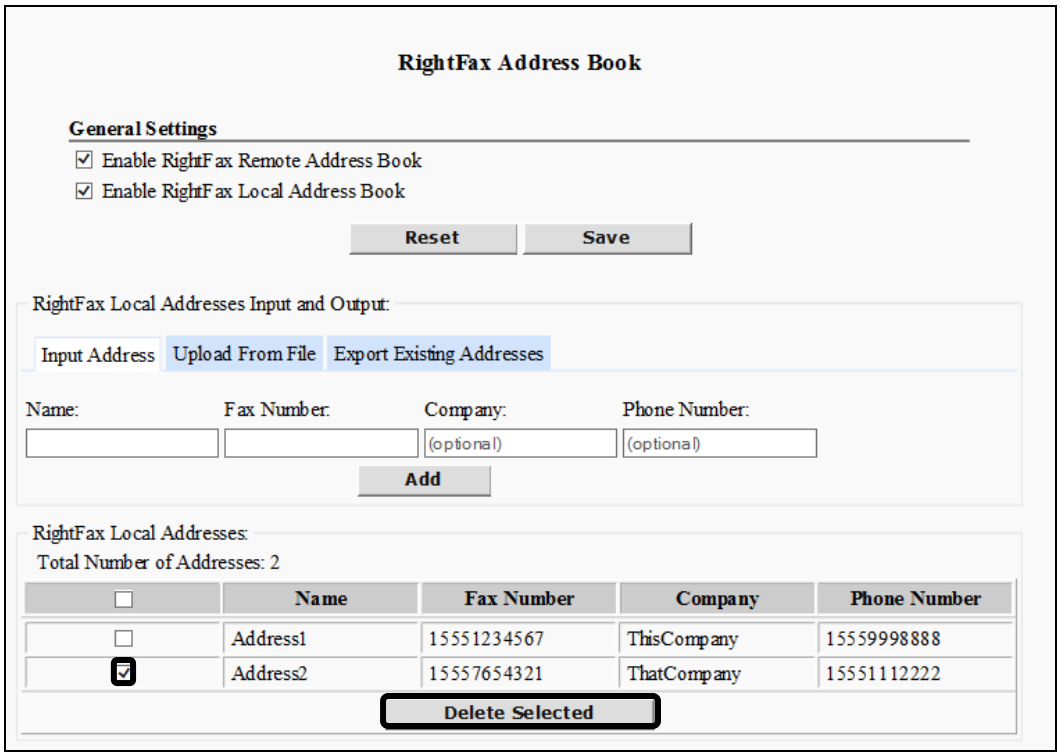
The existing fax addresses are exported to a text file.

The exported text file is formatted, as described below:

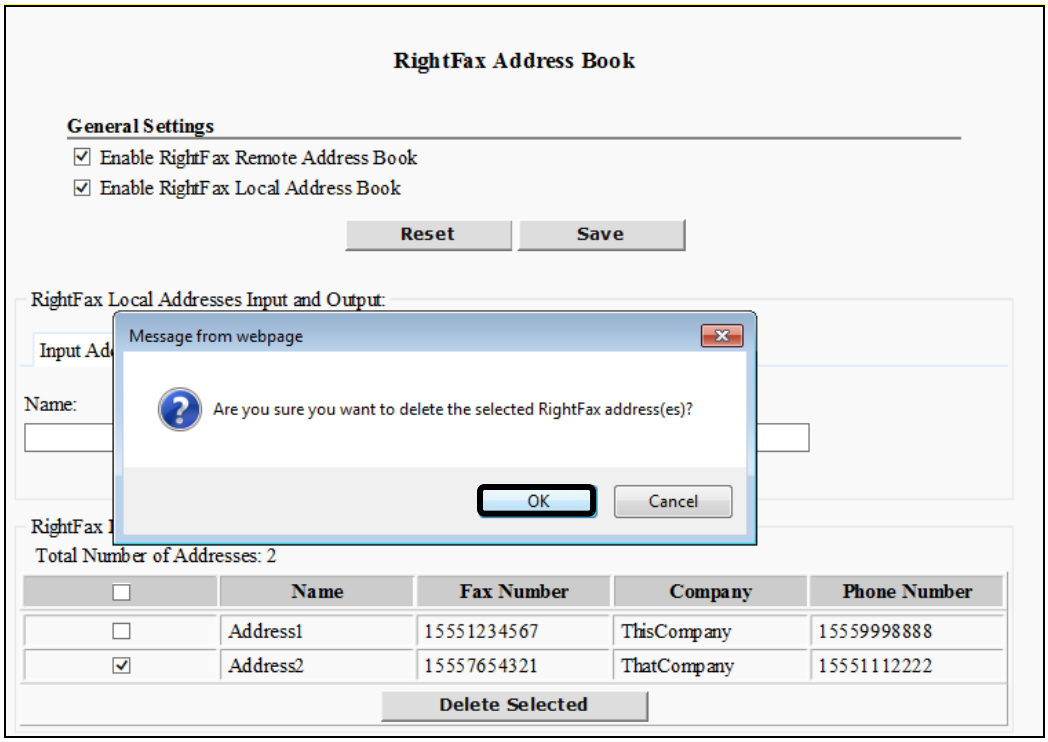
- Each fax address entry is on a separate line.
- Each fax address entry contains an address name and fax number, separated by a comma (“address_name,fax_number”). Optional fields are also separated by commas on the associated lines.

3.3.2 Click [File] → [Save As] → navigate to the drive or directory to where you want to save the file → click [Save].

4. To delete a fax address, click the check box next to the fax address you want to delete → click [Delete Selected].



5. Click [OK].



If you do not want to delete the fax address, click [Cancel].

The fax address is deleted from the list.

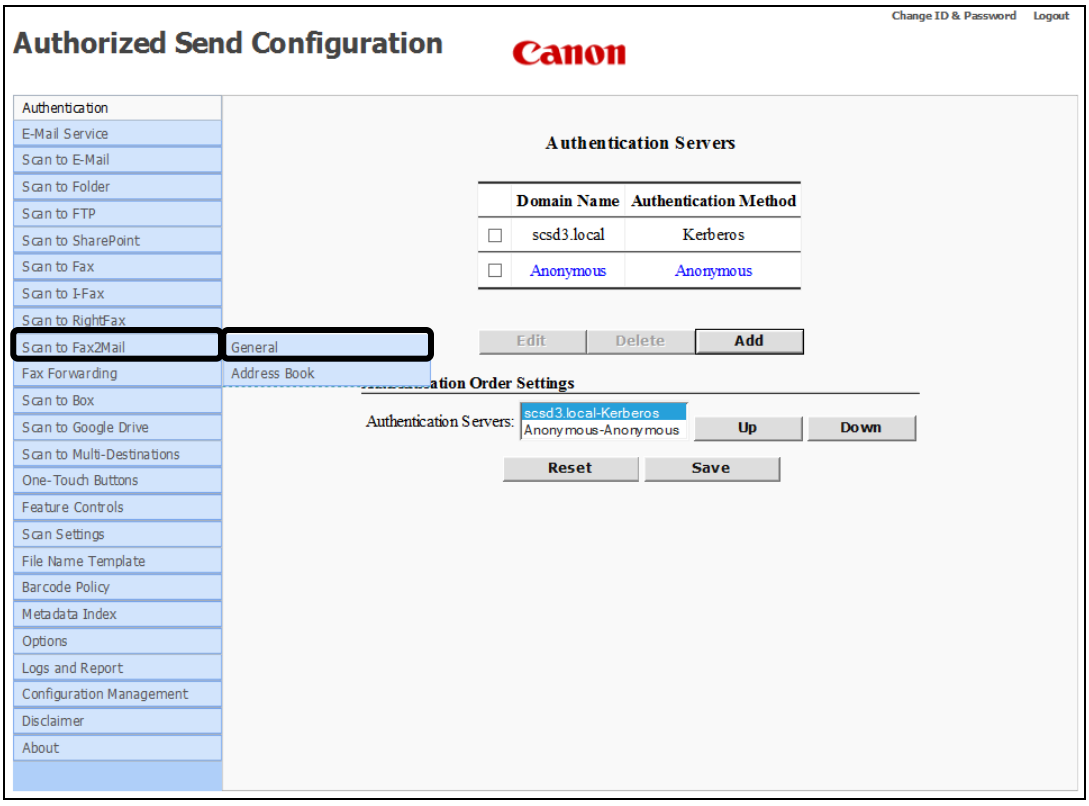
2.11 Configuring the Scan to Fax2Mail Settings

You can configure the Scan to Fax2Mail function, which enables users to scan and send documents to the Fax2Mail service.

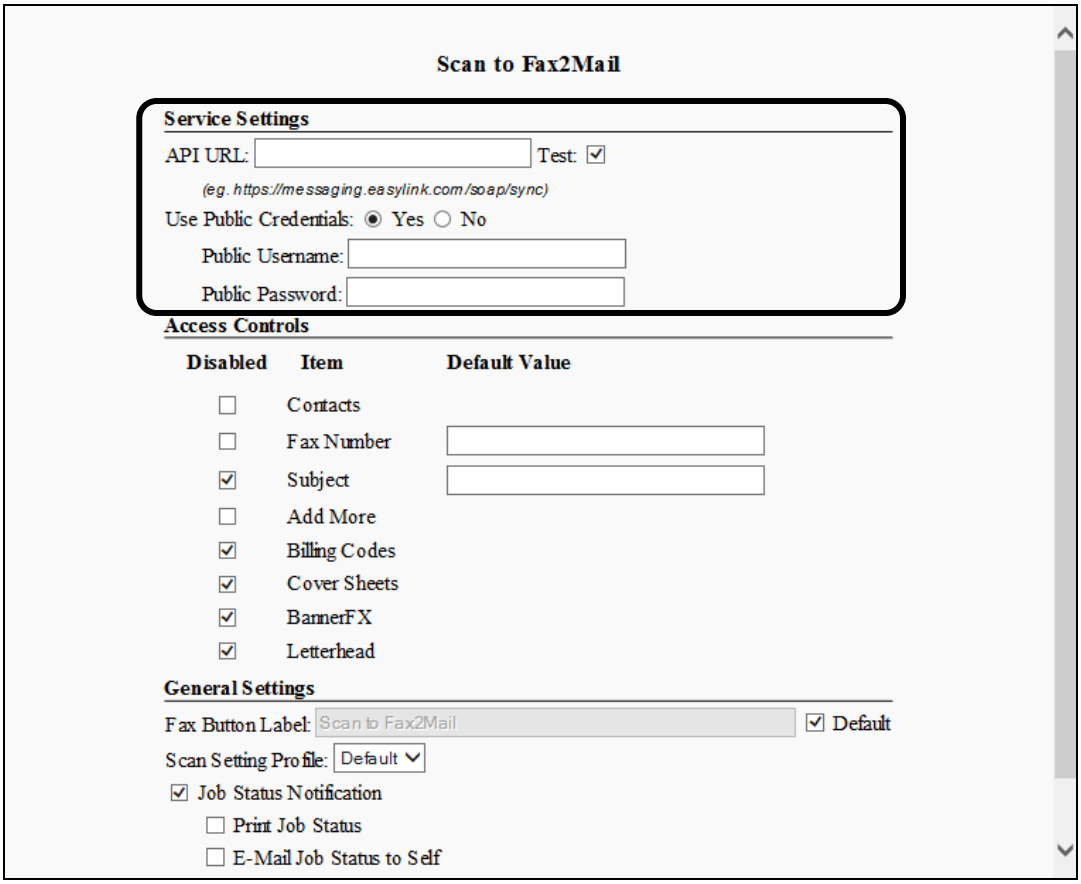
IMPORTANT

- The Scan to Fax2Mail function is available only after the System Administrator has installed and started the “FaxServiceActivation.jar” service.
- If an AMS enabled login application is installed and running on the machine, [Scan to Fax2Mail] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the Scan to Fax2Mail function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [Scan to Fax2Mail] →[General].



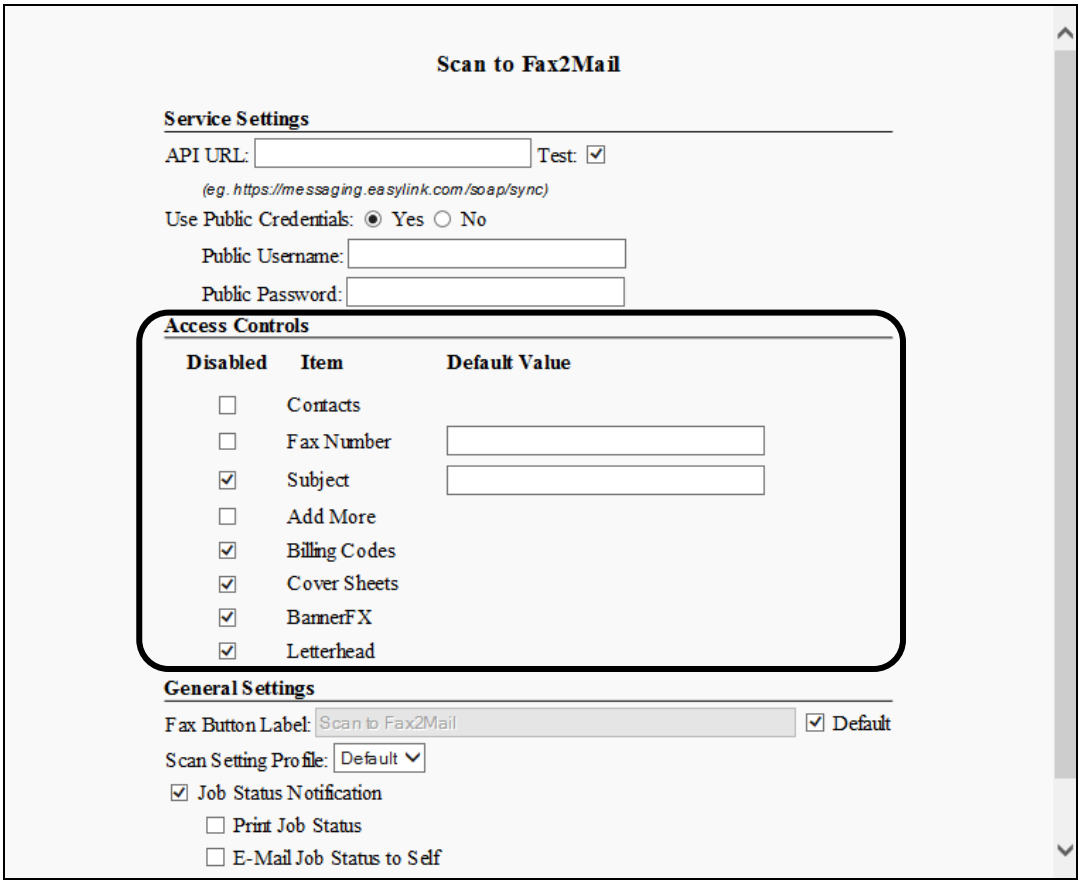
2. Configure the settings under <Service Settings>.



Service Settings

API URL:	Enter the URL of the Fax2Mail API. It should be the same as the Fax2Mail API URL set in the Fax2Mail configuration screen. It is blank by default.
Test:	Select this check box to validate that the [API URL] setting is an active connection and is a valid Fax2Mail server.
Use Public Credentials:	Select “Yes” to indicate that the Public Username and Public Password will be configured by the administrator. Select “No” to manually enter the public credentials data in the Fax2Mail configuration screen The default selection is “No”.
Public Username:	Enter a valid user name to communicate with the Fax2Mail server. This field should not be blank.
Public Password:	Enter a valid password (for the Public Username) to communicate with the Fax2Mail server. This field should not be left blank.

3. Configure the settings under <Access Controls>.



Access Controls

Disabled Item Column

Contacts: Check this box to disable the [Contacts] button on the “Scan to Fax2Mail” screen on the machine console. This check box is not selected by default.

Fax Number: Check this box to disable display of a default fax number text box on the “Scan to Fax2Mail” screen. This check box is not selected by default.

Subject: Check this box to disable display of the fax subject line. If the box is unchecked, enter an alphanumeric string up to 255 characters long in the [Subject] text box. The check box is selected and the text box is empty by default.

Add More: Check this box to disable the [Add More] button on the “Scan to Fax2Mail” screen on the machine console. This check box is not selected by default.

Billing Codes: Check this box to disable the [Billing Codes] button on the “Scan to Fax2Mail” screen on the machine console. This check box is selected by default.

Cover Sheets: Check this box to disable the [Cover Sheets] button on the “Scan to Fax2Mail” screen on the machine console. This check box is selected by default.

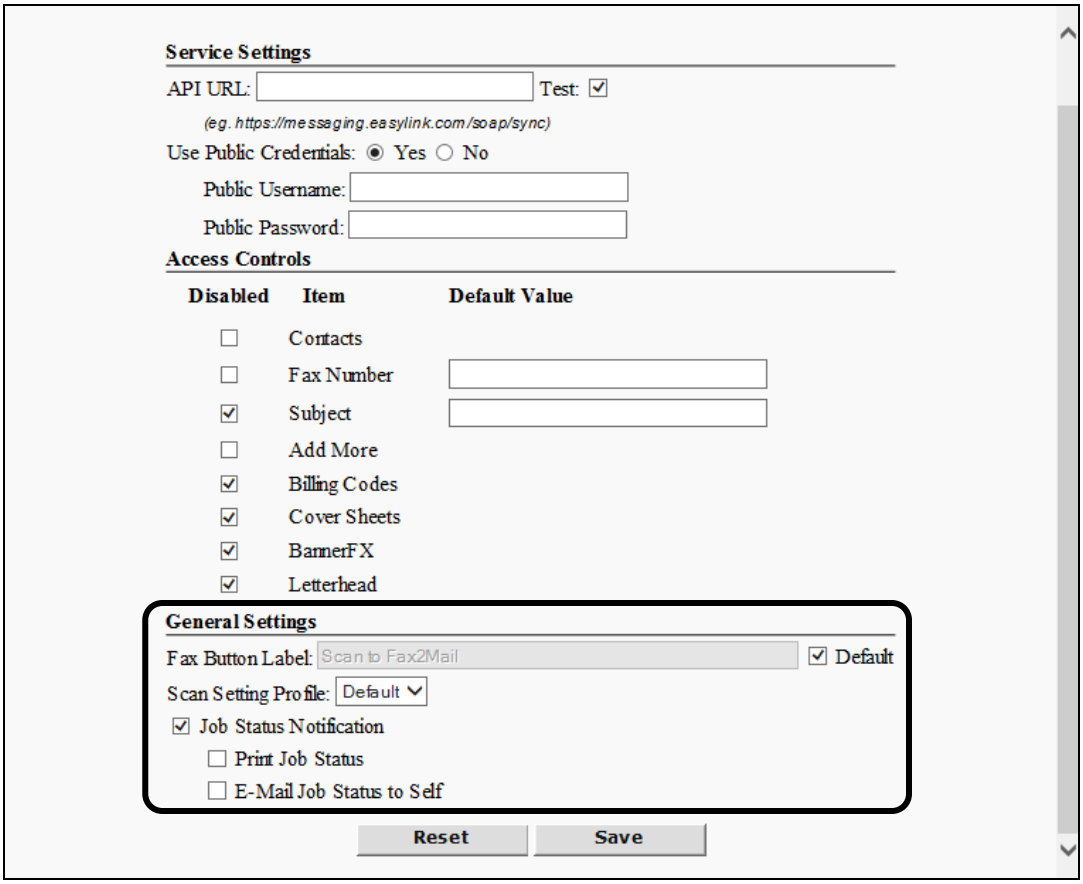
Banner FX: Check this box to disable the [Banner FX] button on the “Scan to Fax2Mail” screen on the machine console. This check box is selected by default.

Letterhead: Check this box to disable the [Letterhead] button on the “Scan to Fax2Mail” screen on the machine console. This check box is selected by default.

Default Value Column

Fax Number: If the [Fax Number] check box above is not selected, enter the number to appear in the [Default Fax Number]. This field can accept up to 25 numeric-only characters.

4. Configure the settings under <General Settings>.



General Settings

Fax Button Label:	If the [Default] check box is selected, enter a new name for the [Scan to Fax2Mail] button on the machine console. By default, the [Default] check box is selected and the label is “Scan to Fax2Mail”. This text field is active only when the [Default] check box is not selected.
Default:	Select this check box if you want to use the default button on the machine console (“Scan to Fax2Mail”). This check box is selected by default.
Scan Setting Profile:	Select a scan profile from the pull-down list. The scan profiles are set using the Scan Setting Profile function.

Job Status Notification:	Select this check box if you want the logged on user of the Scan to Fax2Mail session to receive confirmation printout or email.
Print Job Status	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to Fax2Mail session to receive a confirmation printout.
E-Mail Job Status to Self	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to Fax2Mail session to receive a confirmation email.

5. Click [Save].

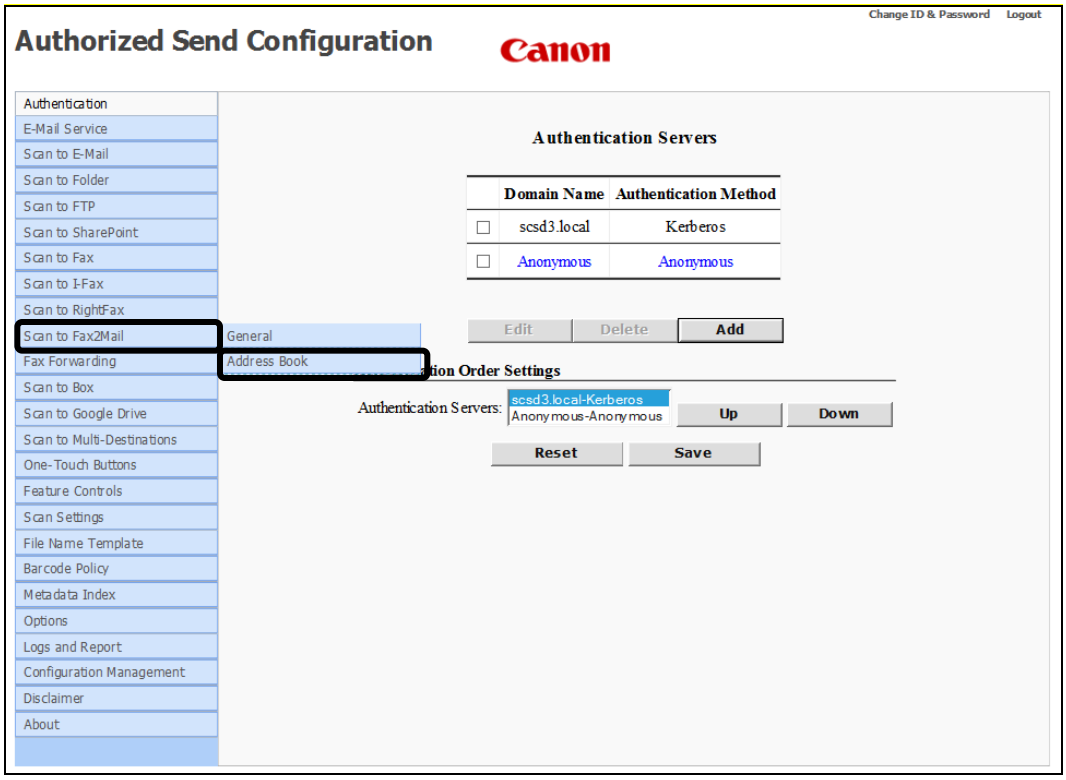
NOTE

If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.11.1 Creating a Fax2Mail Address Book

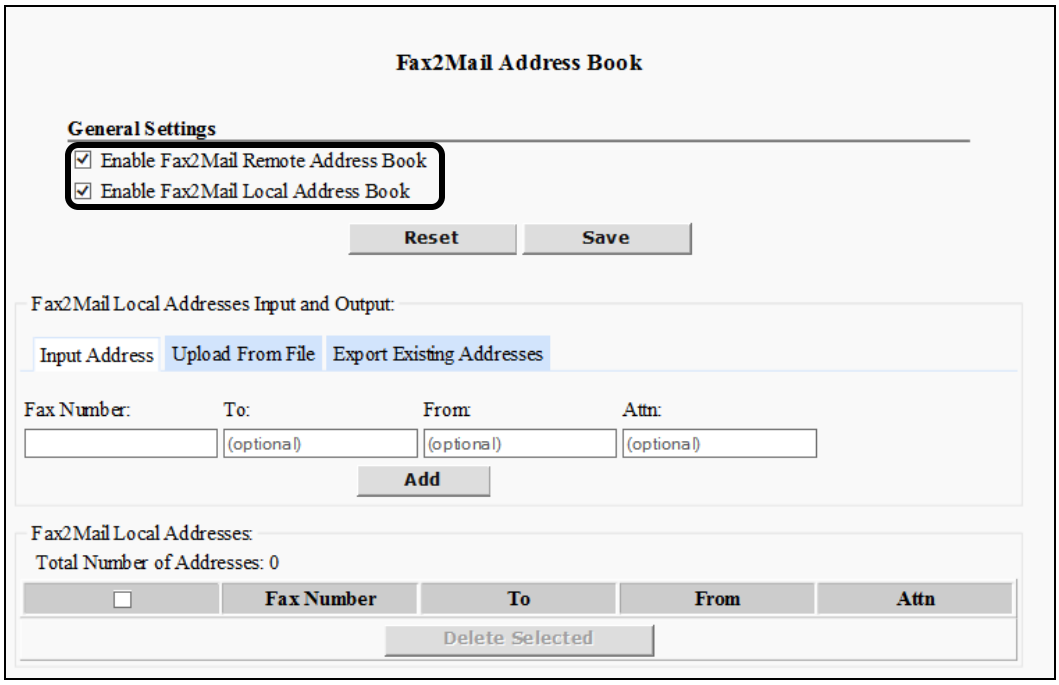
You can create a Fax2Mail Address Book to store your fax numbers.

1. Click [Scan to 2FaxMail] → [Address Book].



The Fax2Mail Address Book screen is displayed.

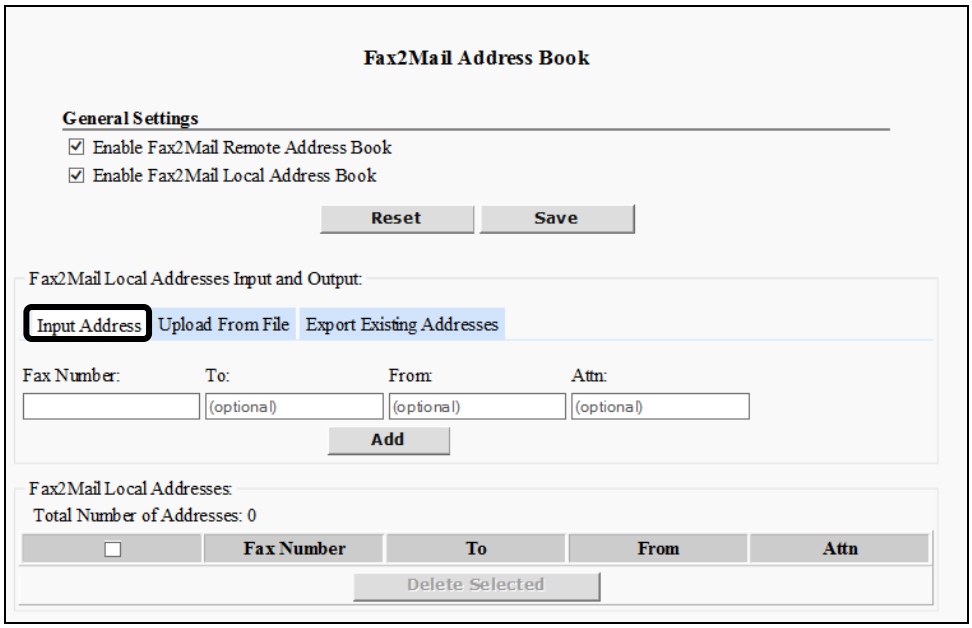
2. Select to which address books (Fax2Mail remote and local) the end user has access.



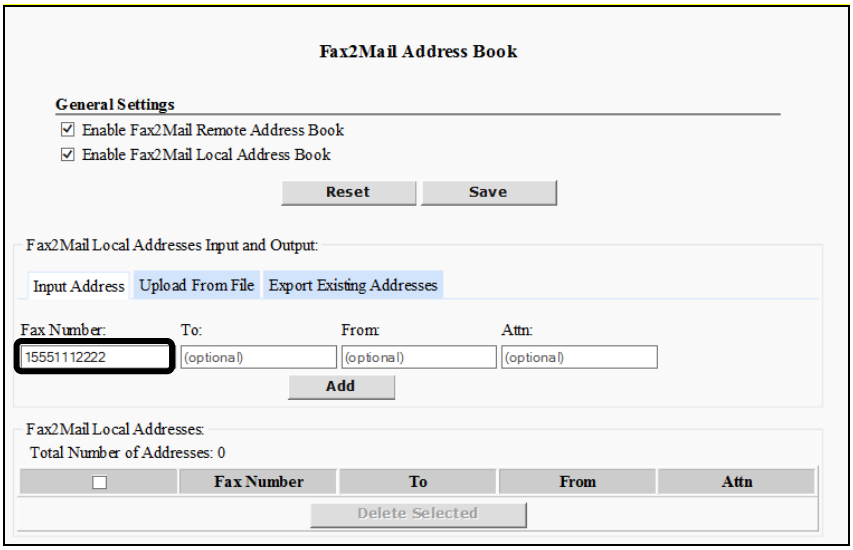
Enable Fax2Mail Remote Address Book	Select this check box if you want the end user to be able to access address book entries stored on the remote Fax2Mail server. If this is not selected, either the “local” option is the only contact level available (if the local address book is enabled), or the [Contacts] button is not displayed (if the local address book is disabled). This check box is enabled by default.
Enable Fax2Mail Local Address Book	Select this check box if you want the end user to be able to access address book entries stored in the local address book. If this is not selected, the “local” option is not available from the [Level] pull-down list. This check box is enabled by default.

3. Input a fax address individually or upload it from a file. You can also export saved fax addresses to a text file.

   3.1 To input a fax address individually, click the [Input Address] tab.

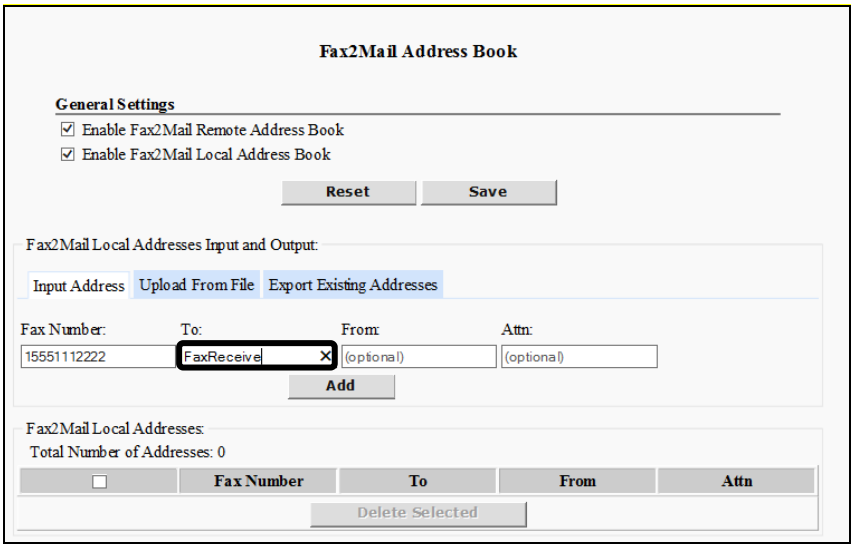


3.1.1 Enter a fax number in the [Fax Number] text box.



You can enter a maximum of 25 numeric characters for the fax number.

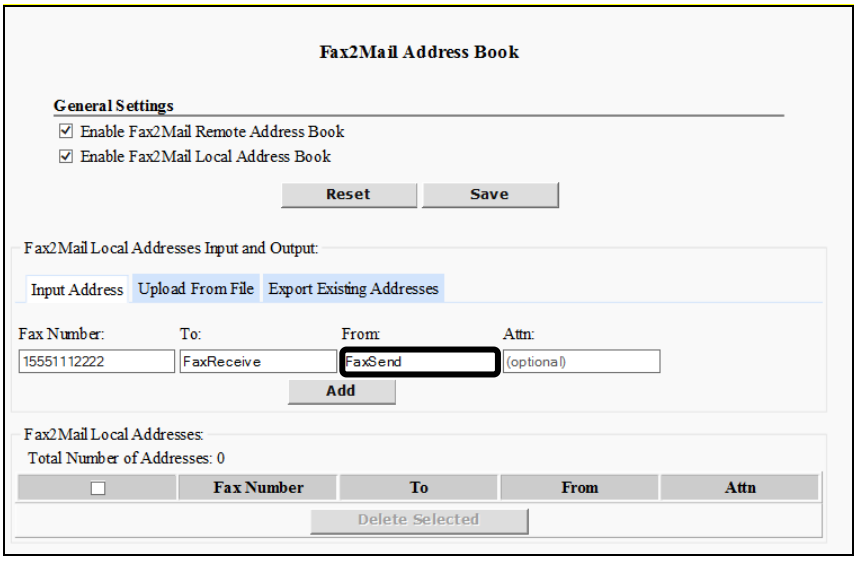
3.1.2 If desired, enter the fax receiver's name in the [To] text box.



The [To] field is optional.

You can enter a maximum of 32 characters of alphanumerics, periods (“.”), hyphens (“-“), spaces (“ “), and underscores (“_”).

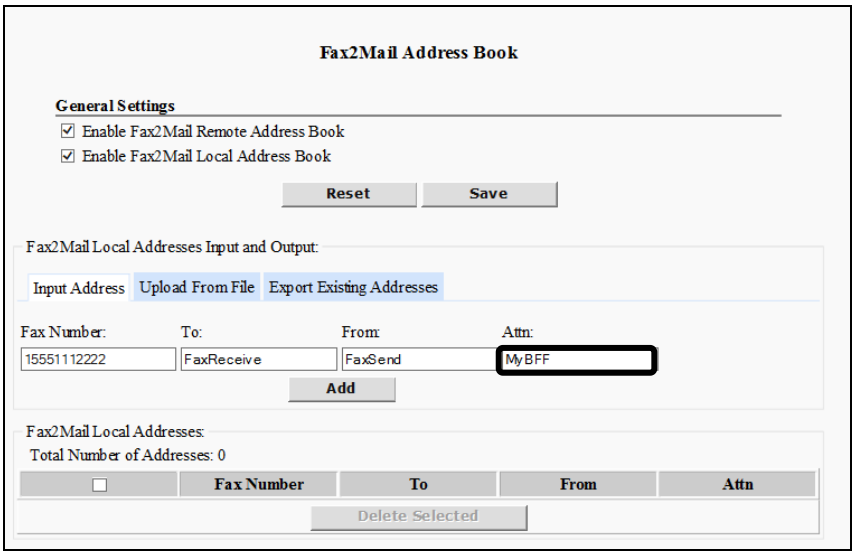
3.1.3 If desired, enter the fax sender's name in the [From] text box.



The [From] field is optional.

You can enter a maximum of 32 characters of alphanumerics, periods (“.”), hyphens (“-“), spaces (“ “), and underscores (“_”).

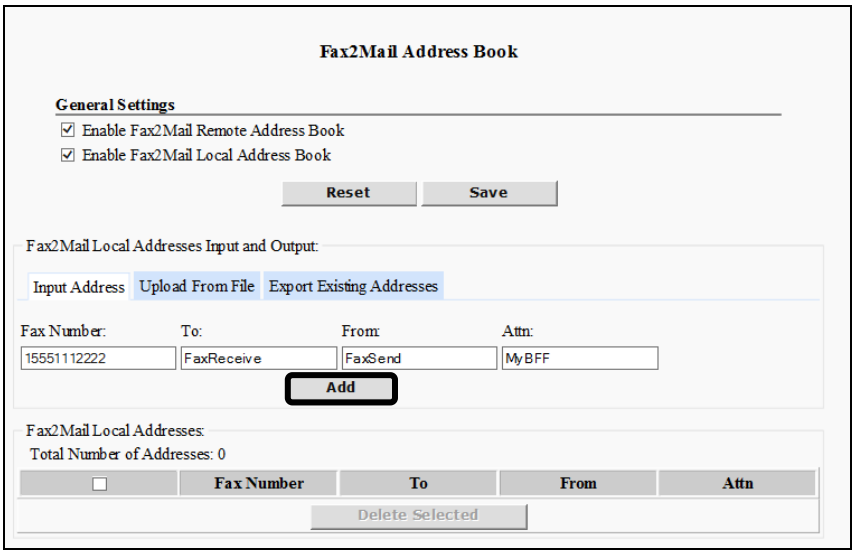
3.1.4 If desired, enter the name of the person at whom the fax attention is directed in the [Attn] text box.



The [Attn] field is optional.

You can enter a maximum of 32 characters of alphanumerics, periods (“.”), hyphens (“-“), spaces (“ “), and underscores (“_”).

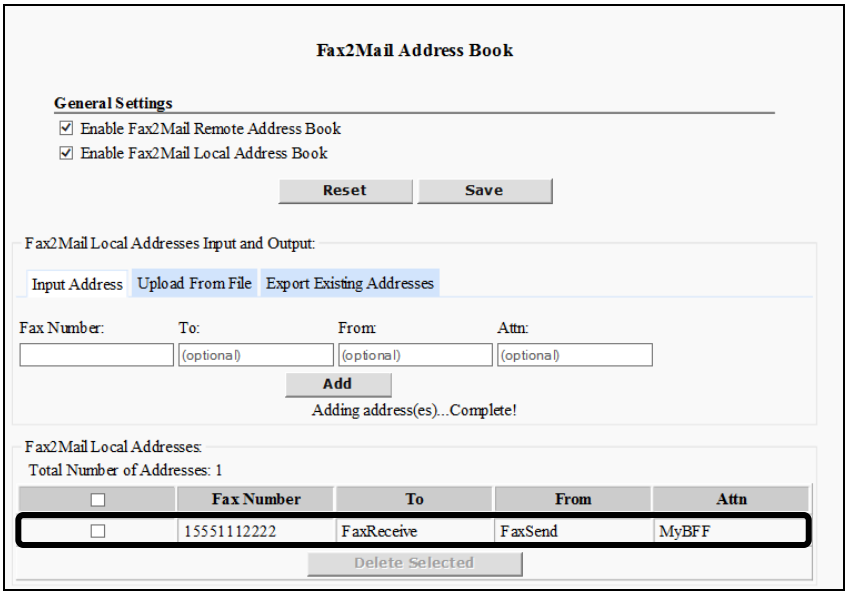
3.1.5 Click [Add] to start the validation process.



Validation is performed to see if:

- The [Fax Number] text box is not empty.
- The [Fax Number] text box contains only numeric characters, is a minimum of one character and a maximum of 25 characters.
- The fax number is not a duplicate of any number already entered in the Fax2Mail Local Address Book.
- The maximum number of fax addresses does not exceed 1000.

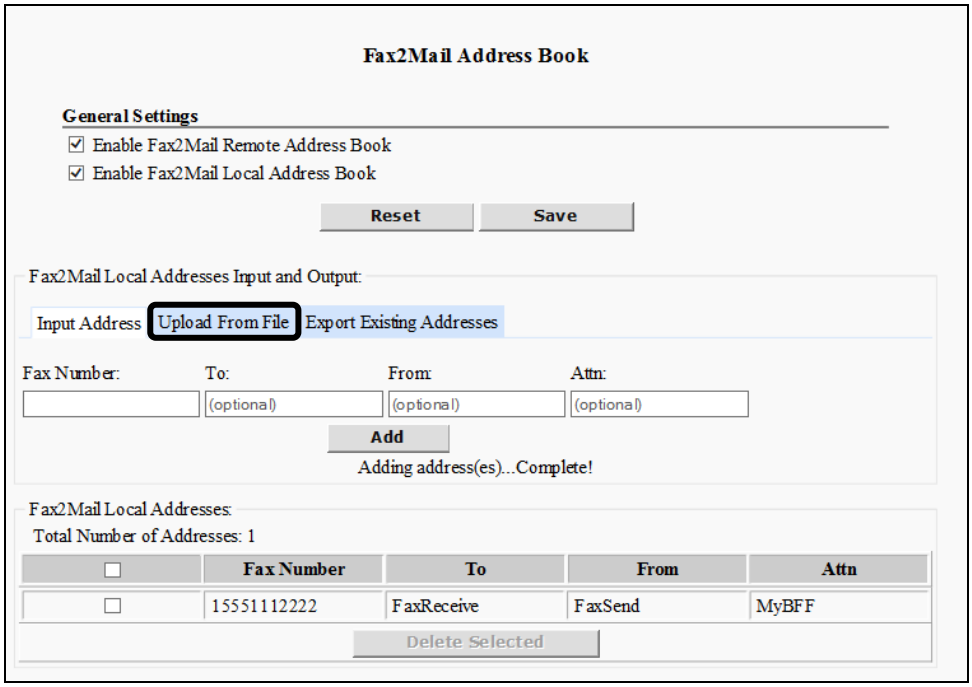
If the validation process is successful, the added fax address appears in the Fax2Mail Local Addresses table. If it fails, an error message is displayed in red.



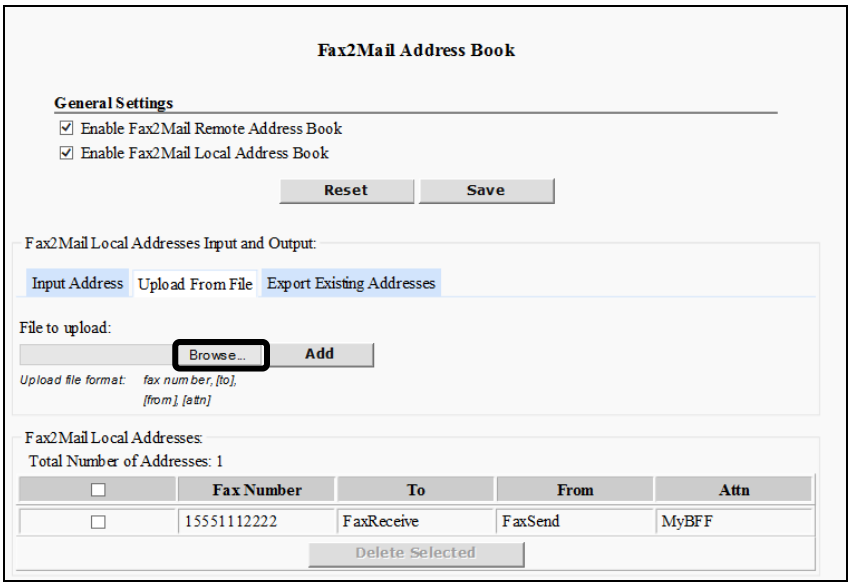
NOTE

<Total Number of Addresses:> displays the number of fax addresses that are in the Fax2Mail Local Addresses table. This number varies as fax addresses are added to, or deleted from, the Fax Addresses table.

3.2 To upload a fax address from a file, click the [Upload From File] tab.



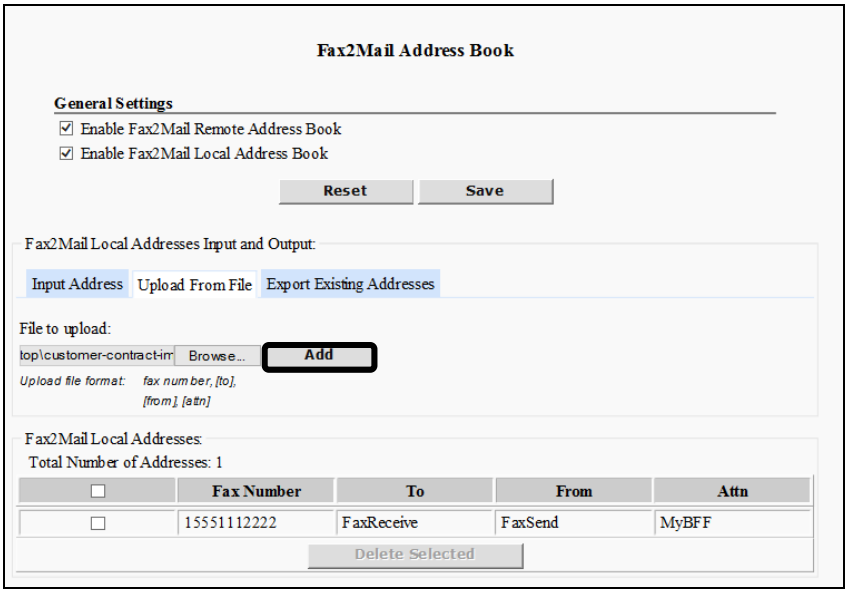
3.2.1 Click [Browse] →navigate to the drive or directory containing the file to upload → select the file → click [Open].



NOTE

The uploaded file extension must be ".txt" or ".csv," and is not case-sensitive.

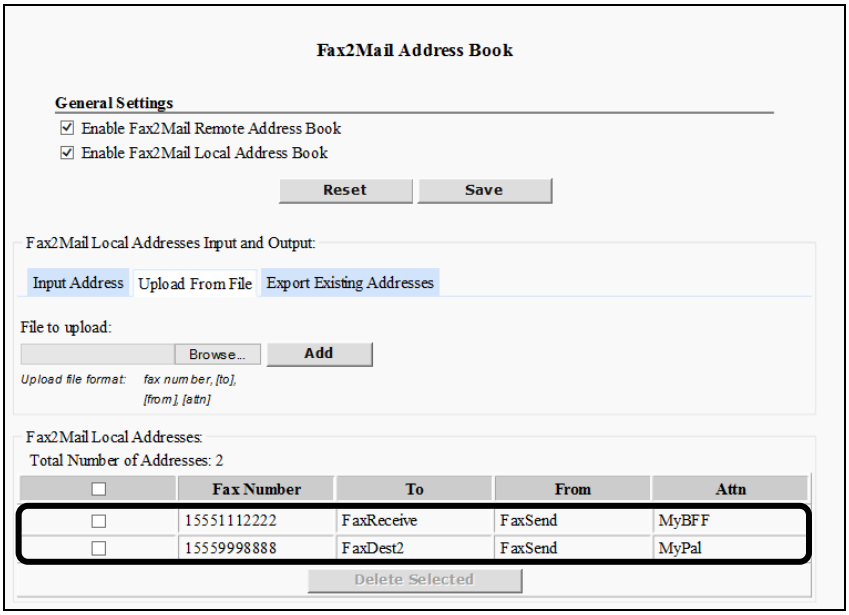
3.2.2 Click [Add] to start the validation process.



Validation is performed to see if:

- The uploaded file is a text/CSV file with the following format requirements:
  - Each fax address entry is on a separate line.
  - Each fax address entry contains at least a fax number, with optional fields being separated by a comma. (“fax_number,to,from,attention”).

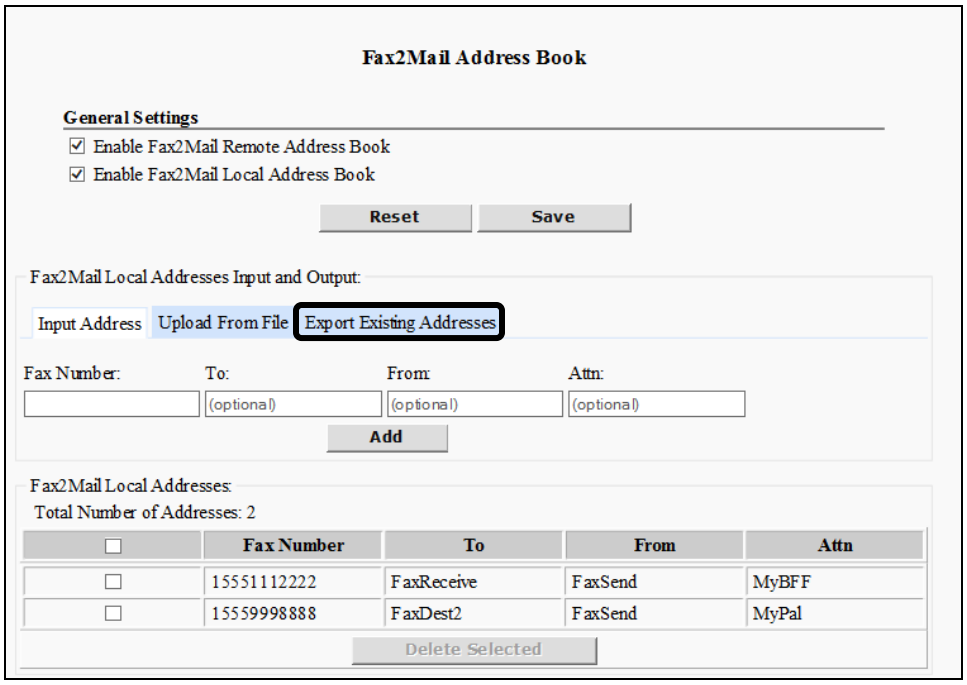
If the validation process is successful, the added fax address appears in the Fax2Mail Local Addresses table. If it fails, an error message is displayed in red.



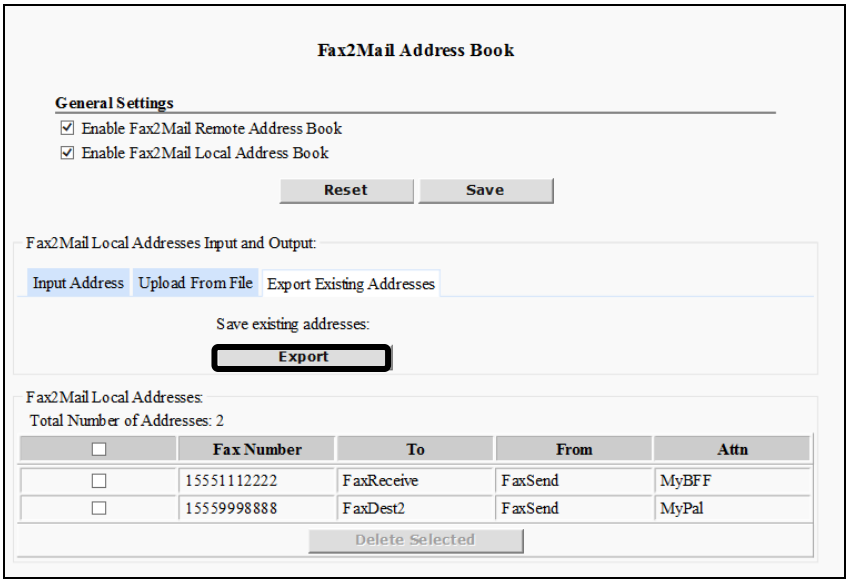
NOTE

- Any line entry in the uploaded file that is in an invalid format, is reported as a failure with the line number. That line is skipped, and uploading continues with the next line.
- Any fax address in the uploaded file that has already been saved is ignored, and reported as a duplicate. Only the number of duplicates found in the file is reported, not the exact line number.

3.3 To export the existing fax addresses to a text file, click the [Export Existing Addresses] tab.



3.3.1 Click [Export].



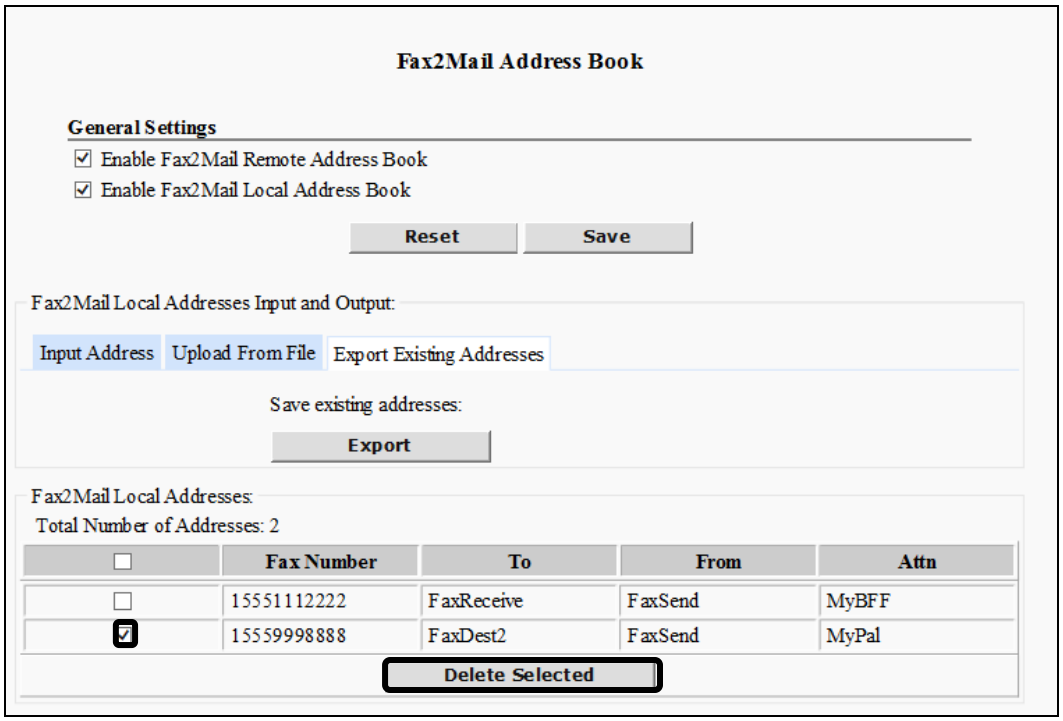
The existing fax addresses are exported to a text file.

The exported text file is formatted, as described below:

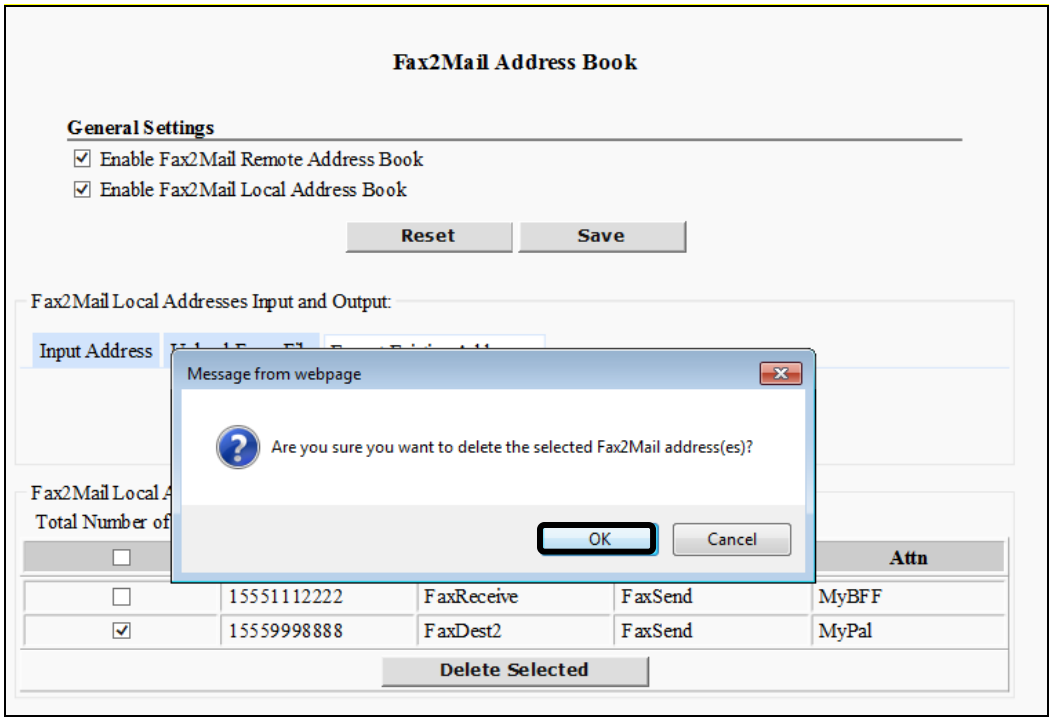
- Each fax address entry is on a separate line.
- Each fax address entry contains a fax number.
- Any other optional fields associated with the fax number are separated by a comma.

3.3.2 Click [File] → [Save As] → navigate to the drive or directory to where you want to save the file → click [Save].

4. To delete a fax address, click the check box next to the fax address you want to delete → click [Delete Selected].



5. Click [OK].



If you do not want to delete the fax address, click [Cancel].

The fax address is deleted from the list.

2.12 Configuring the Fax Forwarding Settings

The device first must be prepared by creating associations and changing settings using the device console or RUI (Remote User Interface). The procedures vary based on whether you are using Advanced Box or FTP to forward the faxes.

Once the device is prepared, log in to the Authorized Send servlet to finish configuration.

2.12.1 Preparing Fax Forwarding with Advanced Box

This section describes the procedures to prepare a device to use the Advanced Box for Fax Forwarding.

IMPORTANT

Not all devices which are compatible with Authorized Send Fax Forwarding have the Advanced Box feature. Refer to your device's documentation to verify Advance Box support. If your device does not support Advanced Box, you must use the FTP function for Fax Forwarding. See "Preparing Fax Forwarding with FTP Server," starting on page 231 for configuration information.

2.12.1.1 Creating a New Advanced Box Folder

You must create a new folder in the Advanced Box as a temporary storage location for incoming faxes.

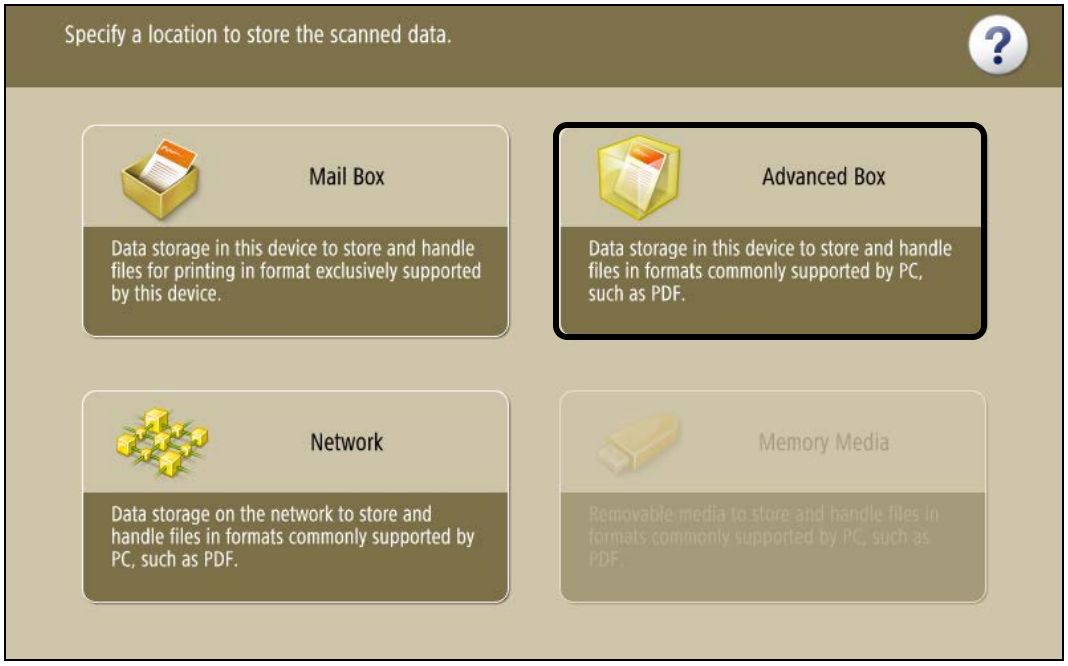
NOTE
You need Administrator-level permissions to configure the device's Advanced Box. Contact your System Administrator for credentials or assistance in configuring the Advanced Box for Fax Forwarding.

---

1. Walk up to the device and log in if necessary. Contact your System Administrator for log in procedures and any necessary credentials.

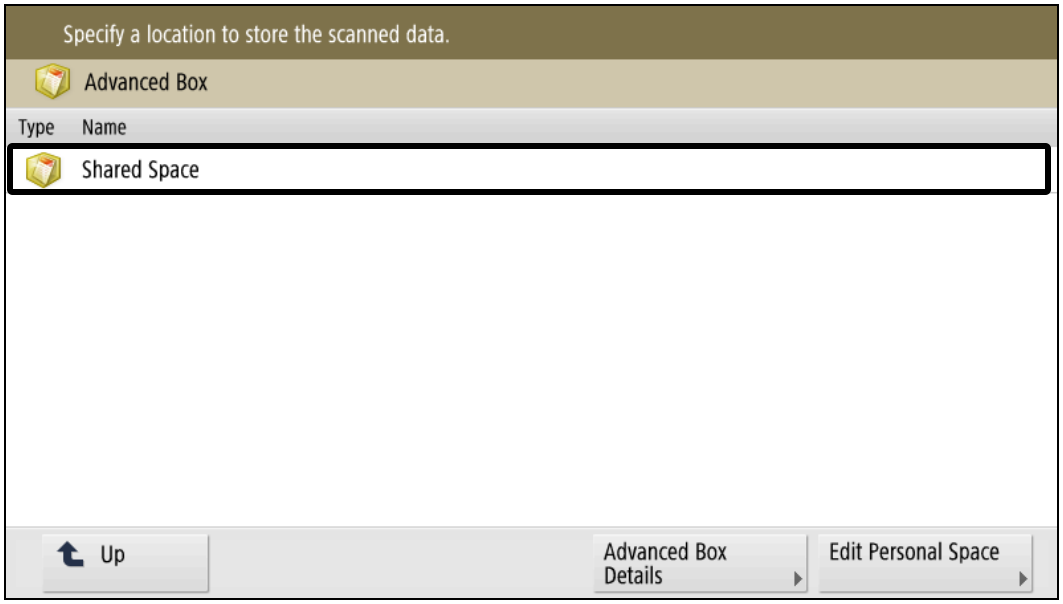
2. Press [Scan and Store] on the main menu.

3. Press [Advanced Box].

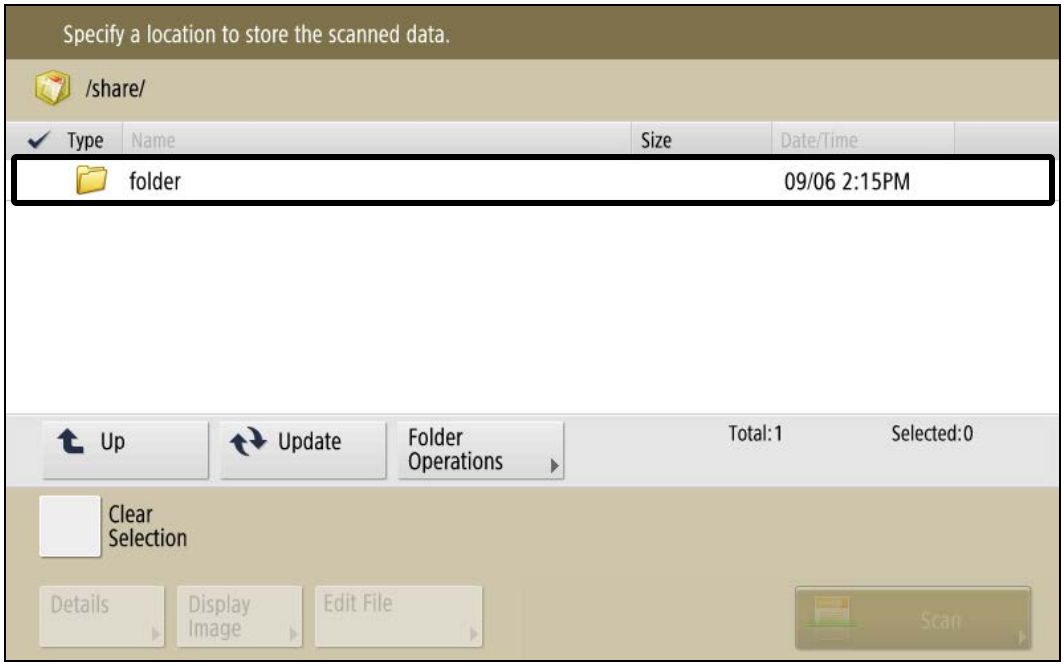


4. If the device requests credentials, enter the system administrator user name and password.

5. Press [Shared Space].

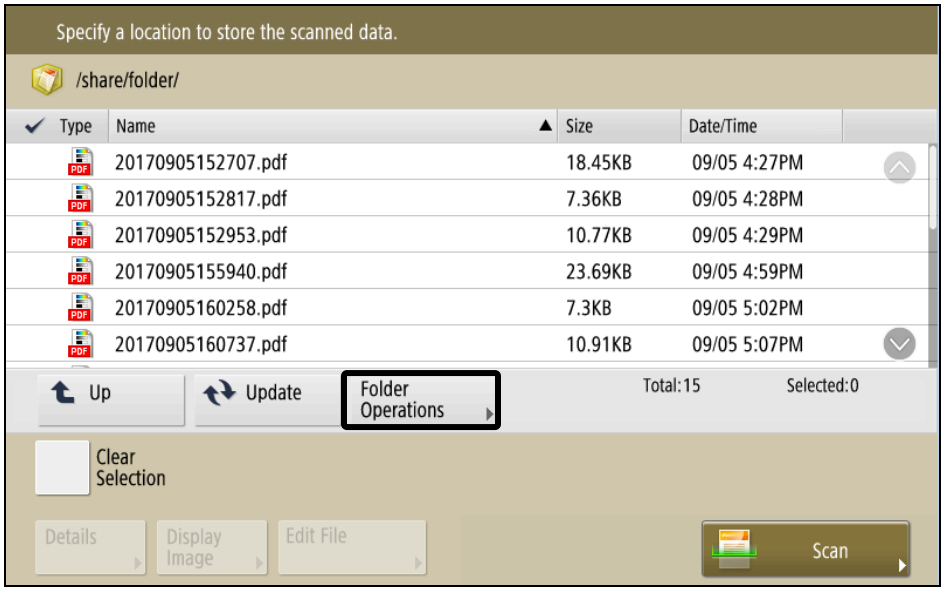


6. Press [Folder].

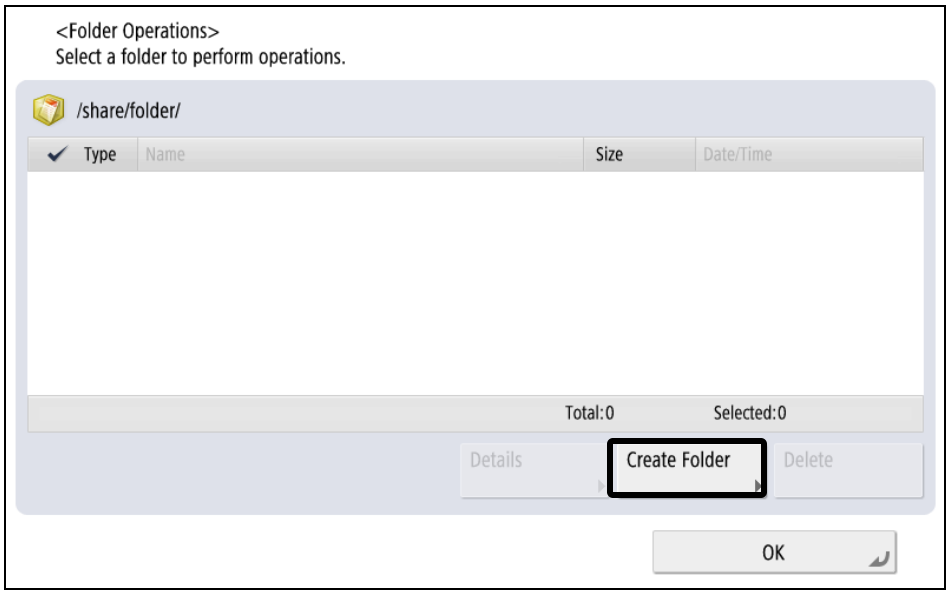


7. Create a new folder.

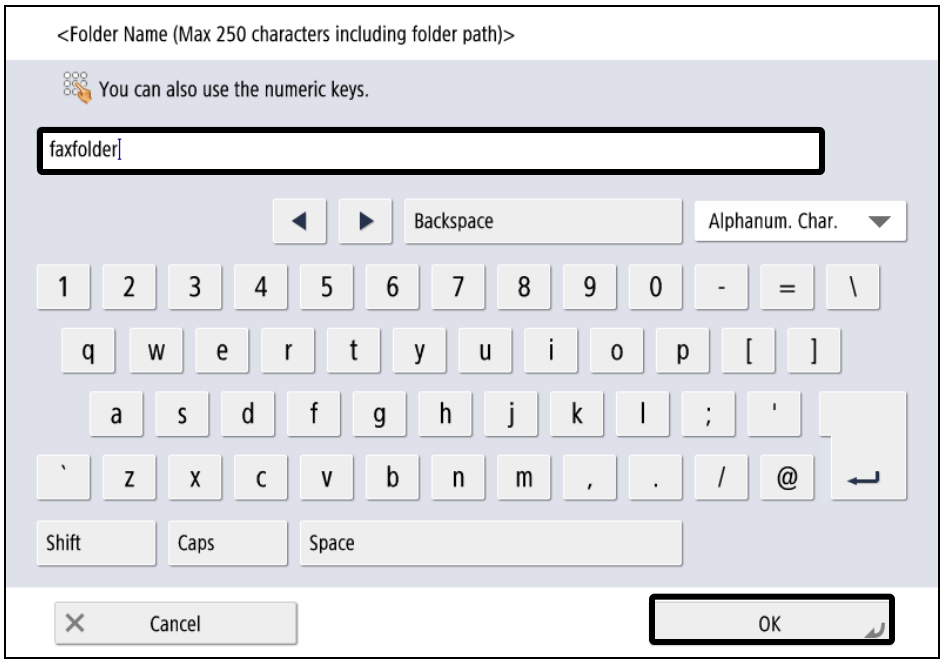
   7.1 Press [Folder Operations].



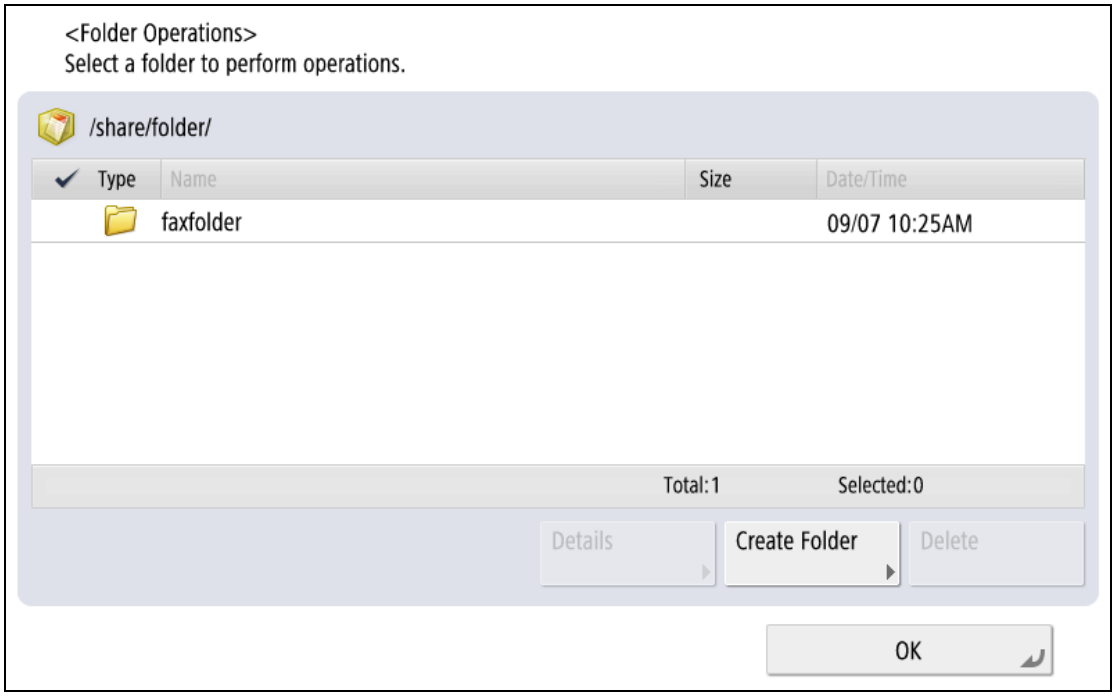
7.2 Press [Create Folder].



7.3 Enter a name for the new folder in the text box. → press [OK].



The Advanced Box folder is ready.



2.12.1.2 Configuring the Address Book Destination

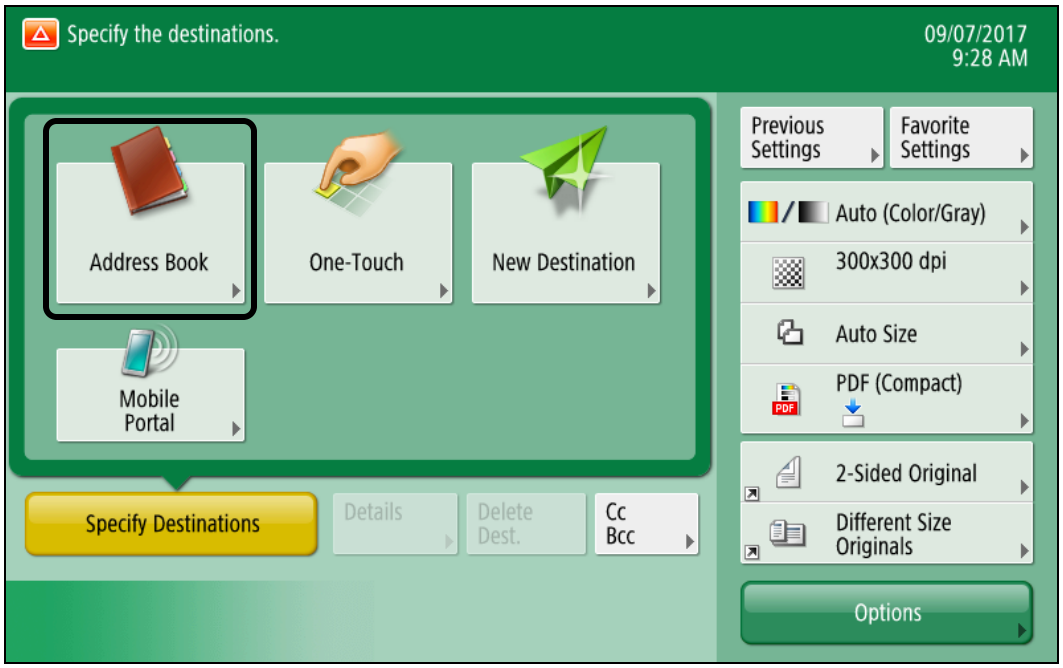
You must create a new destination in the Address Book to act as the destination for incoming faxes

---

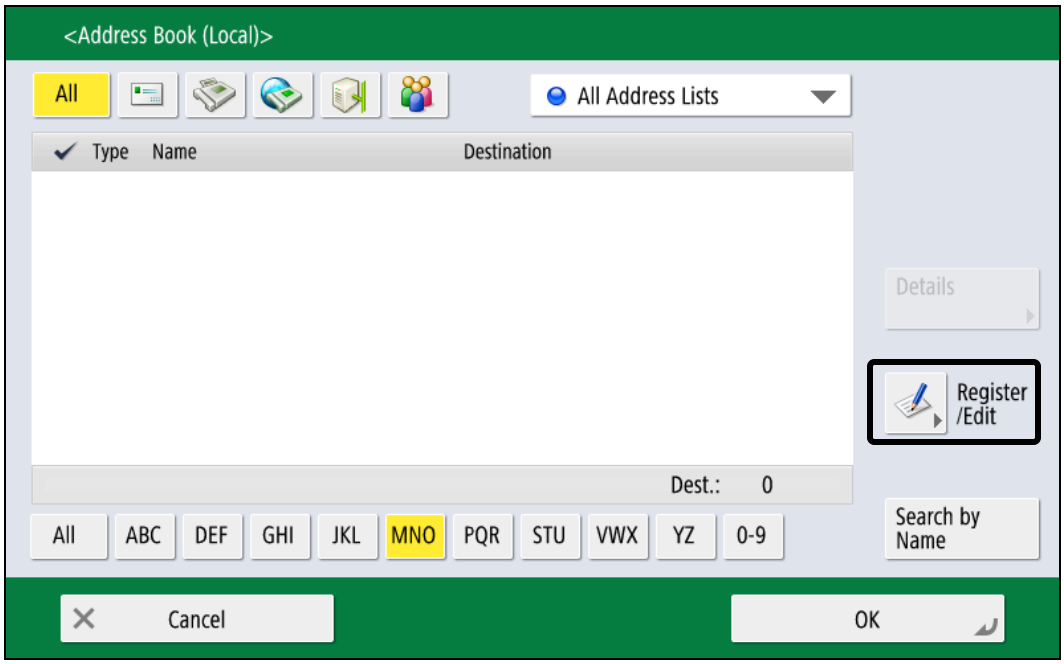
1. Walk up to the device and log in if necessary. Contact your System Administrator for log in procedures and any necessary credentials.

2. Press [Scan and Send] on the main menu.

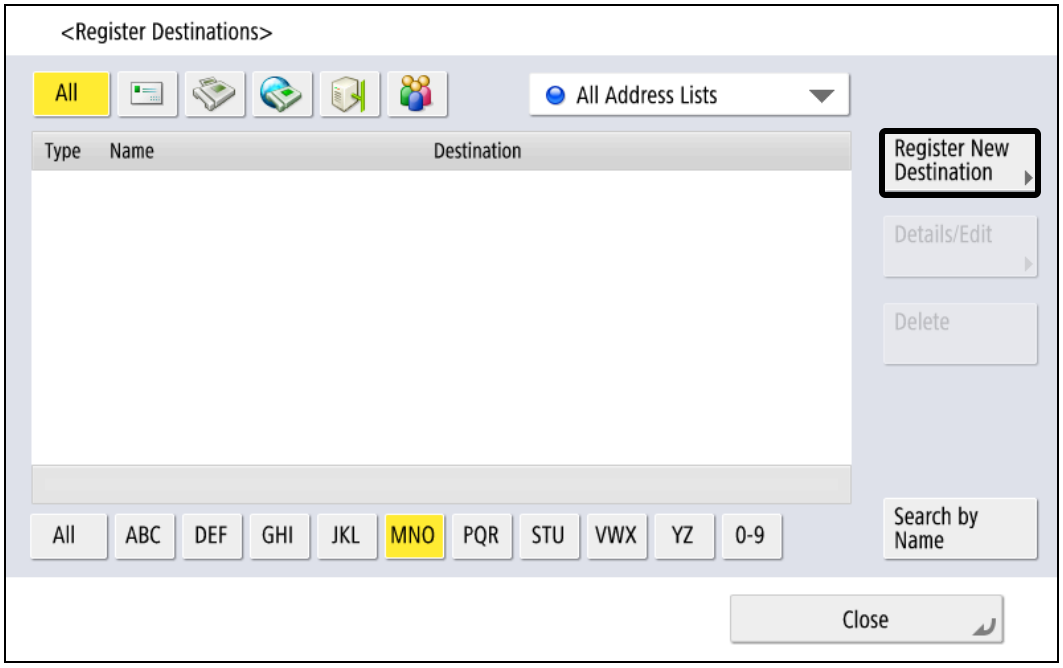
3. Press [Address Book].



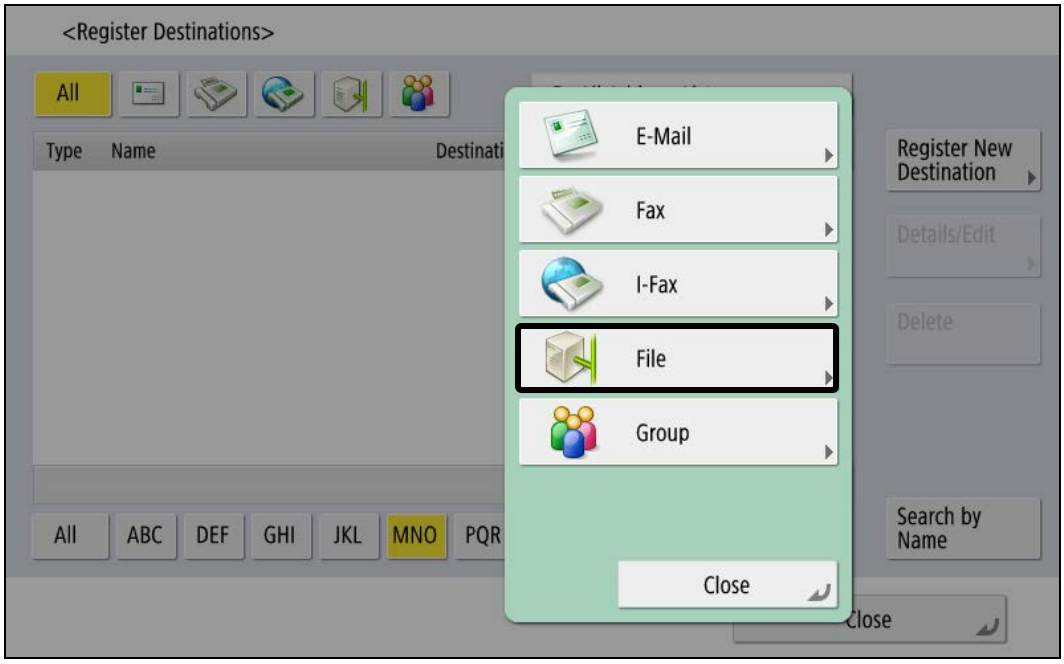
4. Press [Register/Edit].



5. Press [Register New Destination].

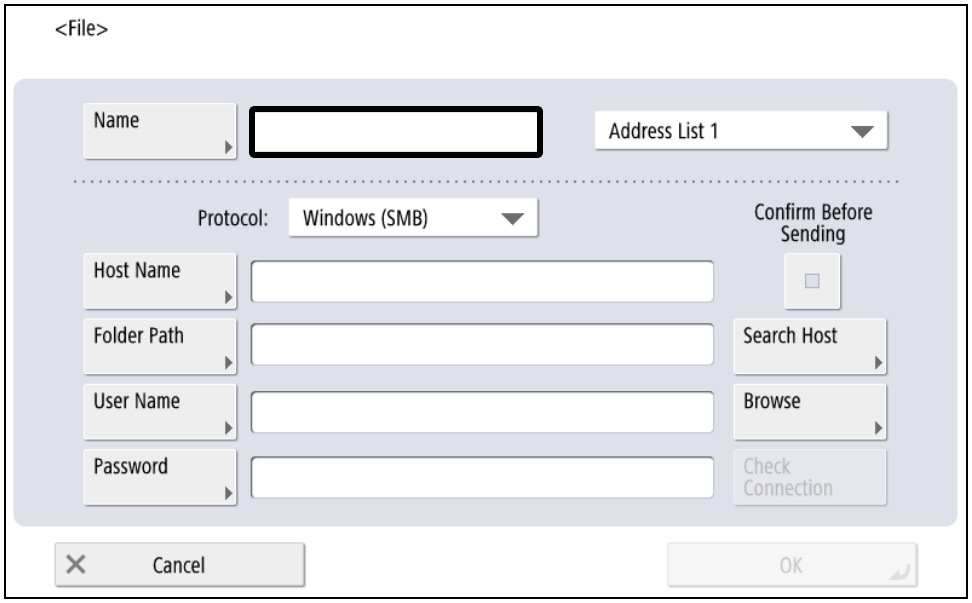


6. Press [File].

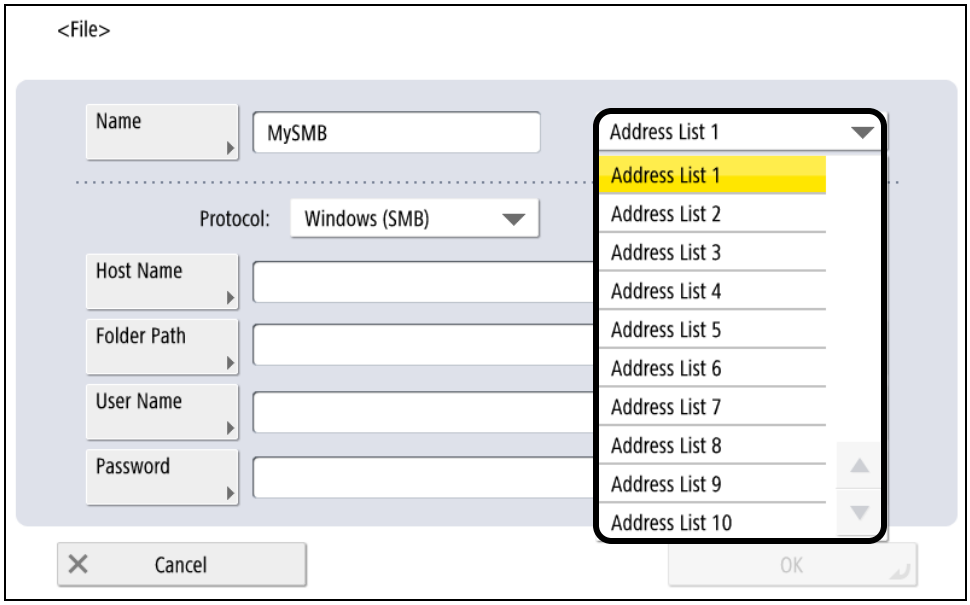


7. Create a new folder.

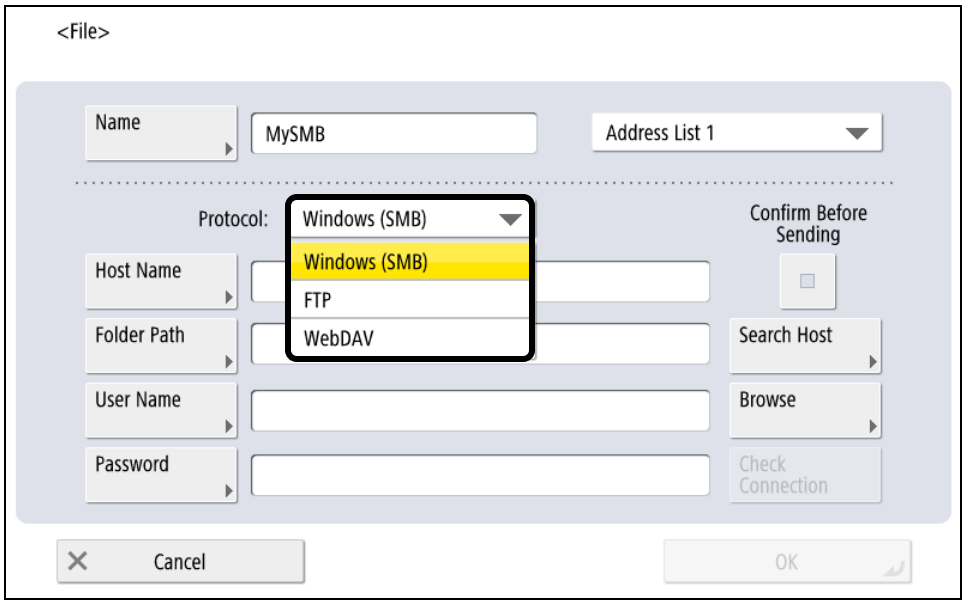
7.1 Enter a name for the destination.



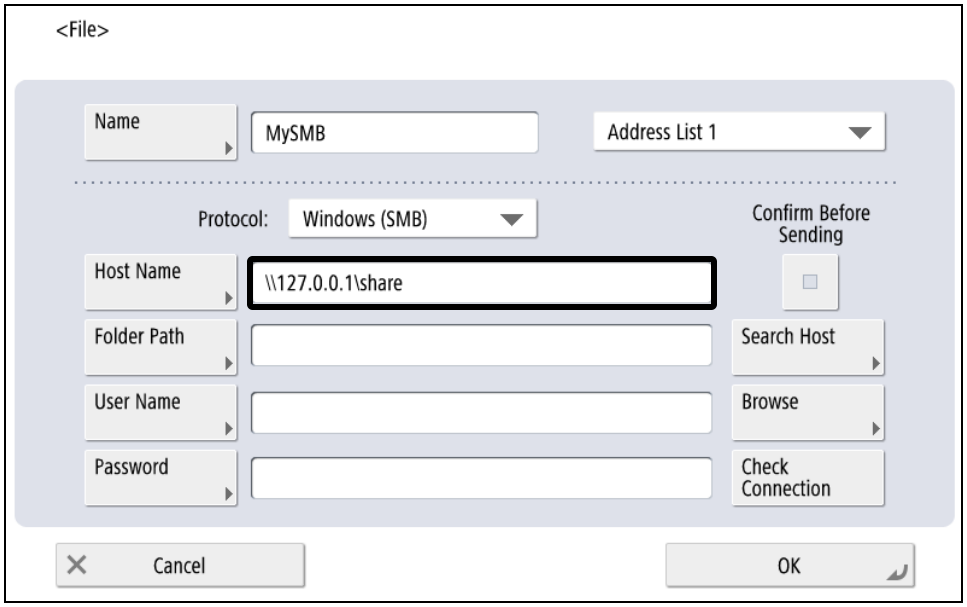
7.2 Press the Address List pull-down list and select the address list in which you want the destination to be set.



7.3 Select Windows (SMB) from the [Protocol] pull-down list.



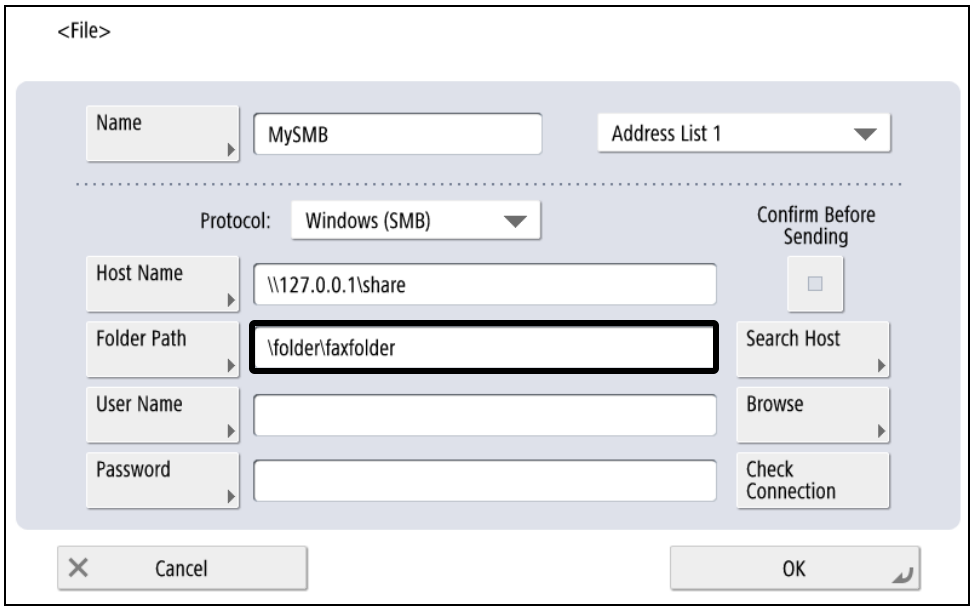
7.4 Enter “\\127.0.0.1\share” or “\\localhost\share” in the [Host Name] text box.



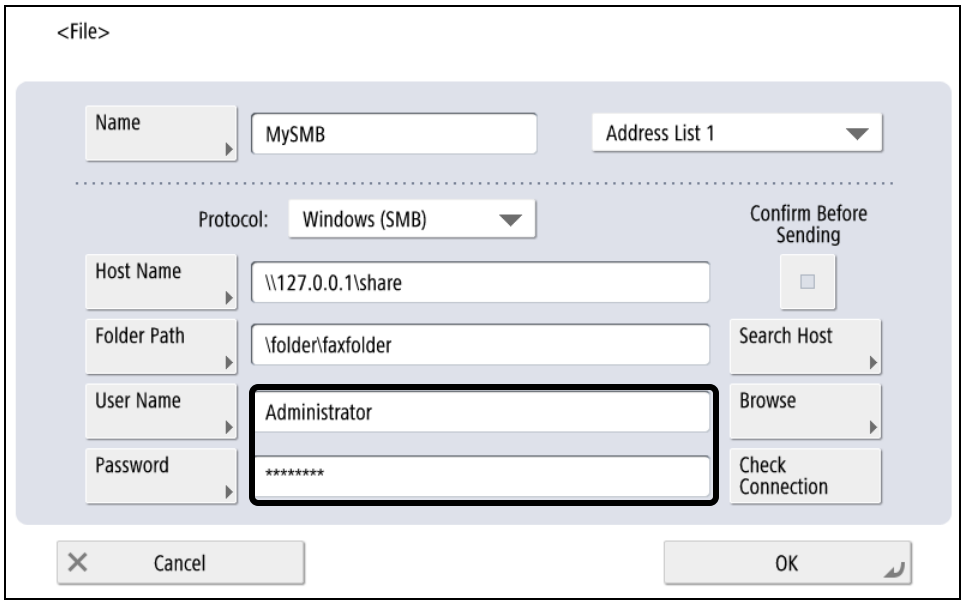
NOTE

Use \\127.0.0.1\share if your device has IPv6 and IPv4 enabled simultaneously

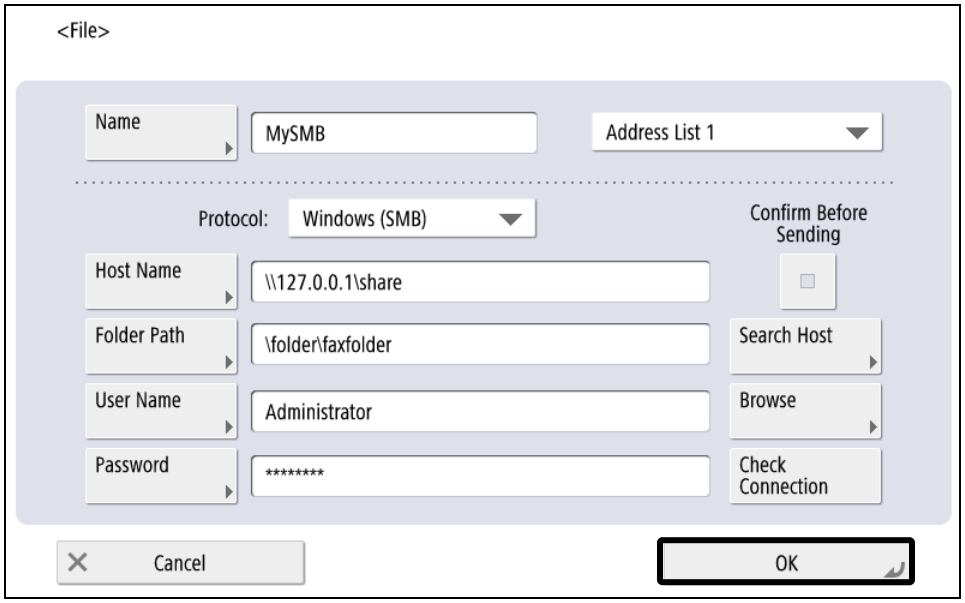
7.5 Enter the path of the folder you created in Advanced Box. For example, if you created \share\folder\fax, enter “\folder\fax”.



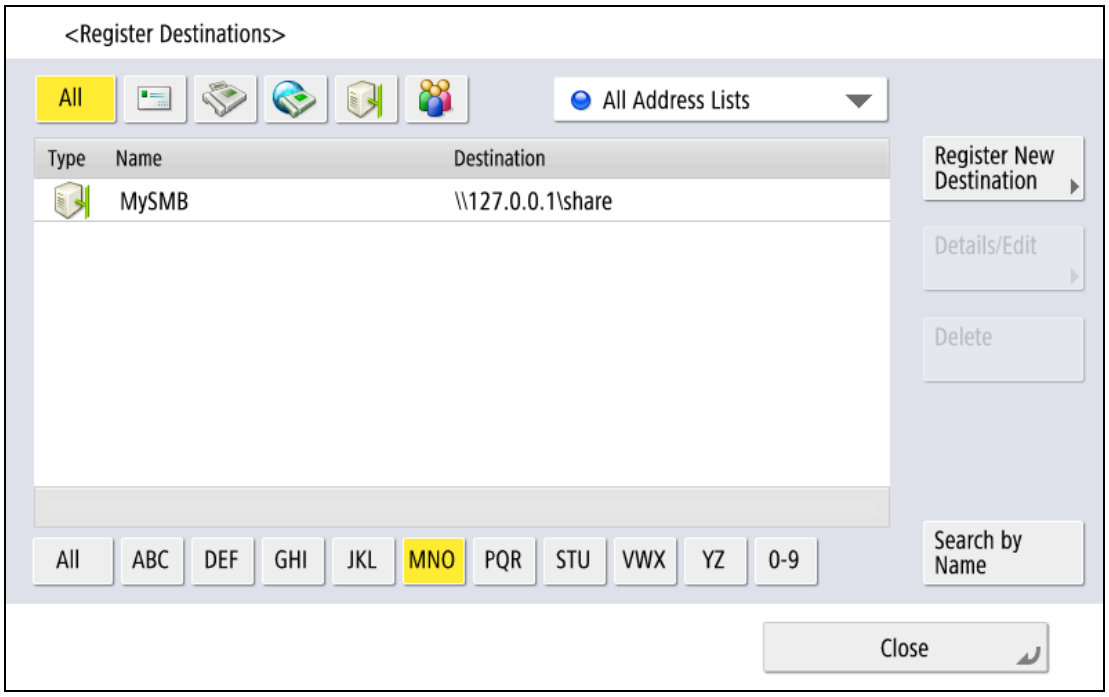
7.6 Enter the Advanced Box system administrator credentials in the [User Name] and [Password] text boxes.



7.7 Press [OK].



The Address Book destination is ready.

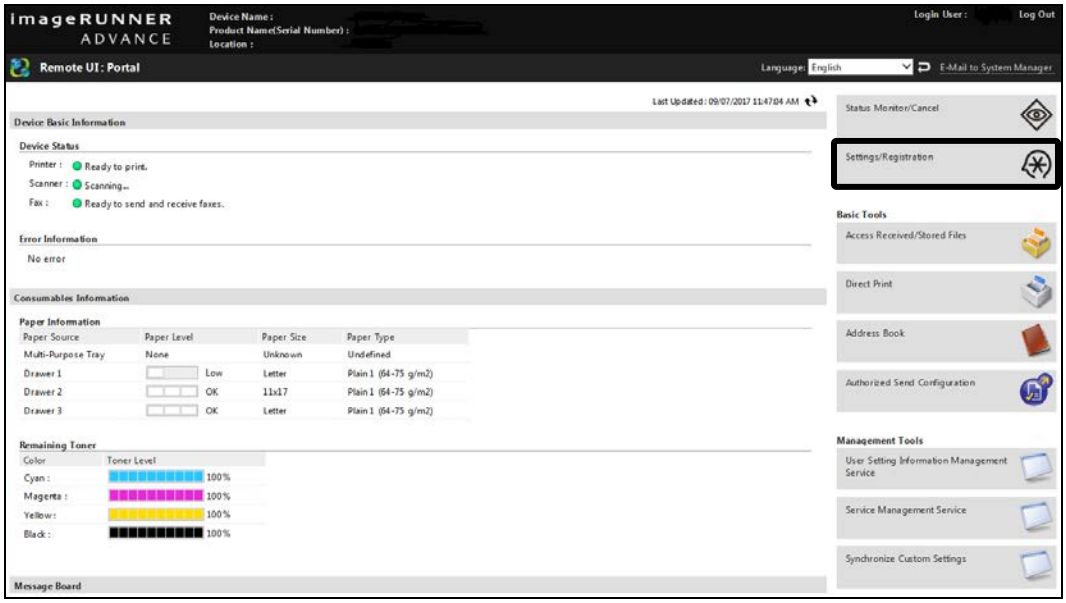


2.12.1.3 Configuring the Forwarding and Network Settings

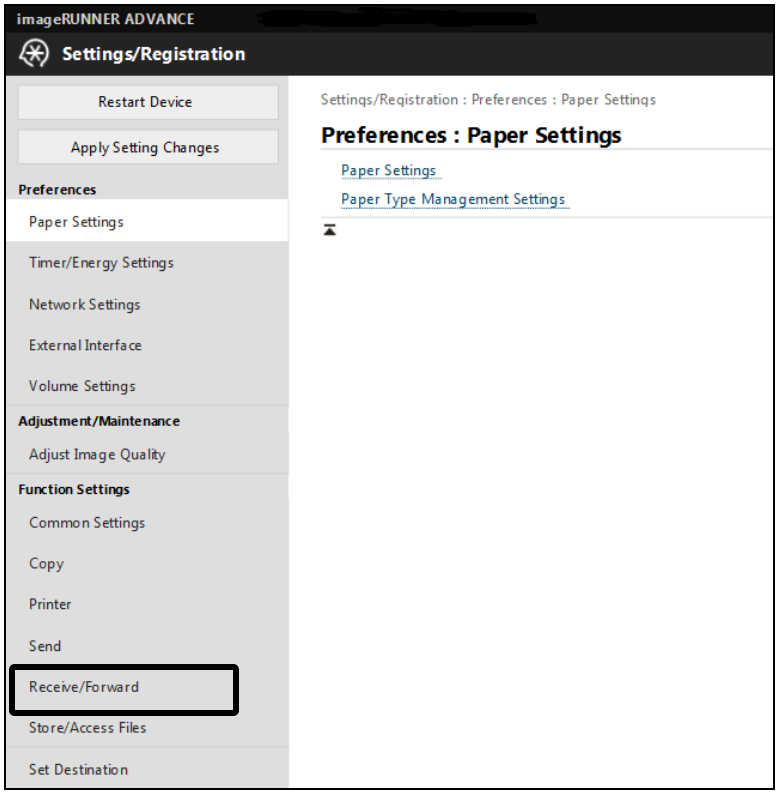
You must change the device's forwarding information and network settings to properly forward incoming faxes to the correct location(s).

1. Log in to the device's RUI (Remote User Interface). Contact your System Administrator for log in procedures and any necessary credentials.

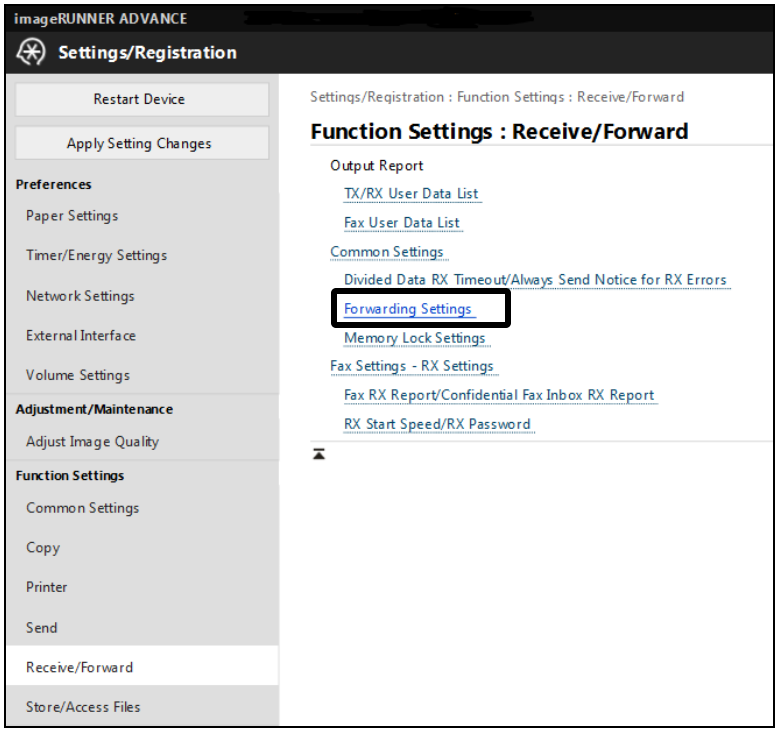
2. Click on [Settings/Registration].



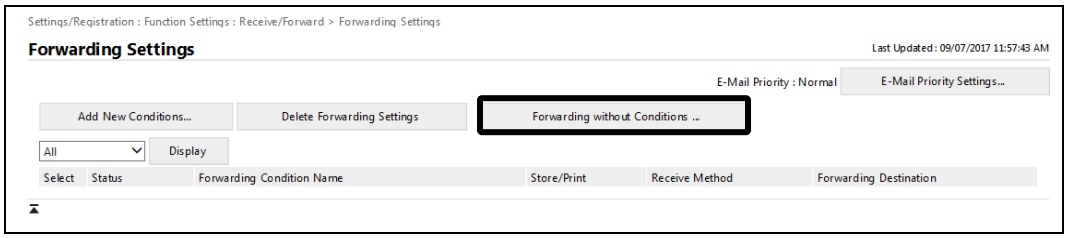
3. Under the Function Settings links, click on [Receive/Forward].



4. Click on [Forwarding Settings].

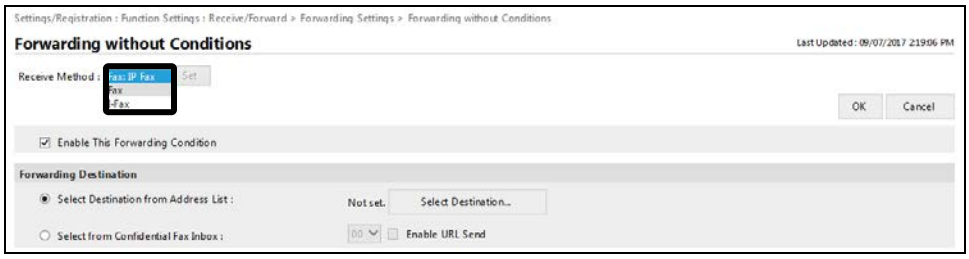


5. Click on [Forwarding without Conditions].

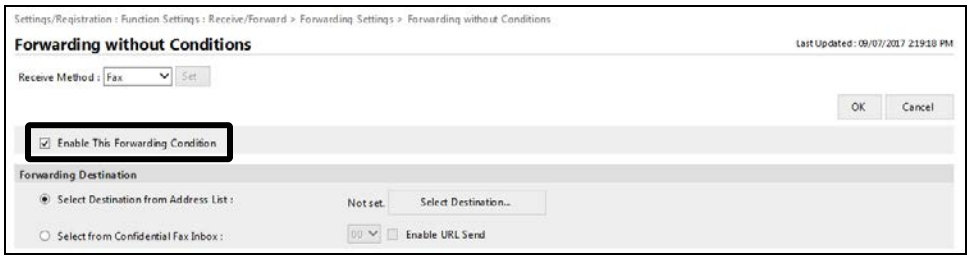


6. Create the forwarding association

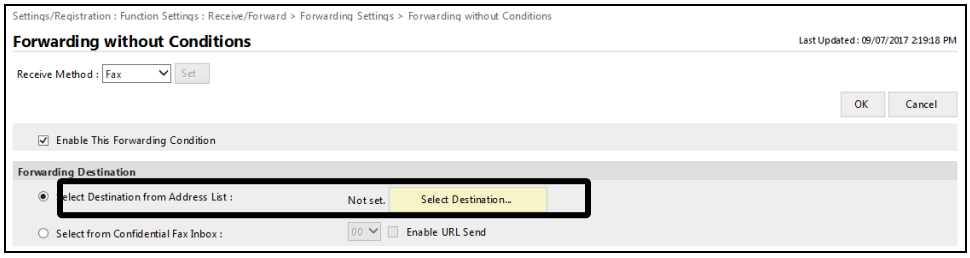
6.1 Select the incoming fax line from the [Receive Method] pull-down list → click [Set].



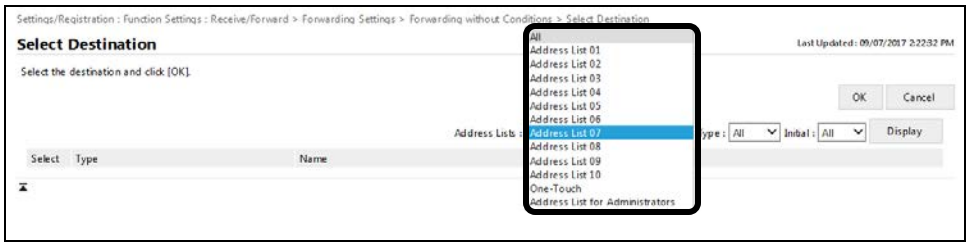
6.2 If it is not already selected, select the [Enable this Forwarding Condition] check box.



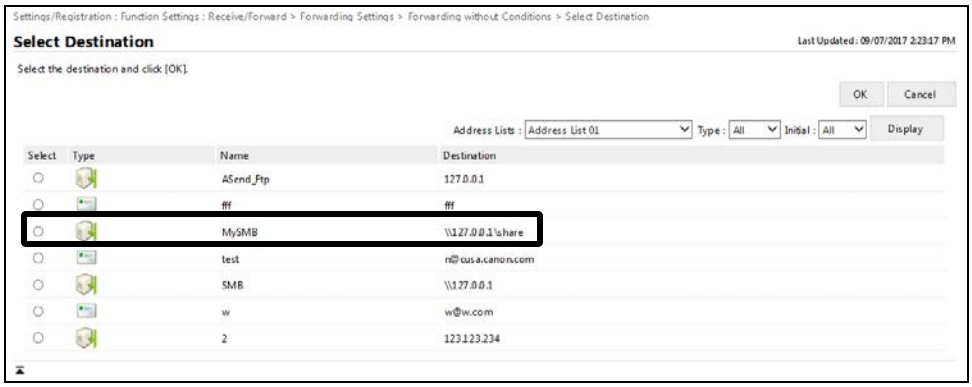
6.3 Select the [Select Destination from Address List] radio button → click on [Select Destination].



6.4 Select the address book to which you assigned the Fax Destination in Section 3.2.2. If you do not remember, select [All] → click [Display].



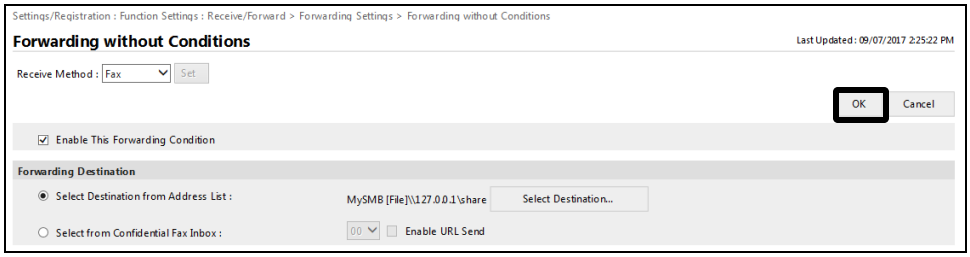
6.5 Select the radio button of the desired fax destination → click [OK].



NOTE

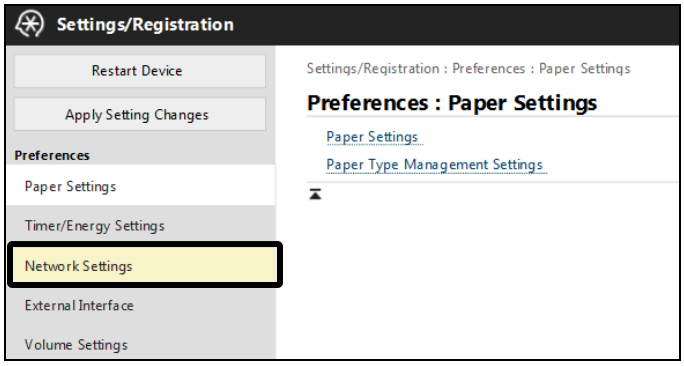
If the destination is from an Address Box other than the Administrator Address Box, a dialog box appears. Click [OK] to confirm the selected destination.

6.6 Click [OK] at the “Forwarding without Conditions” page.

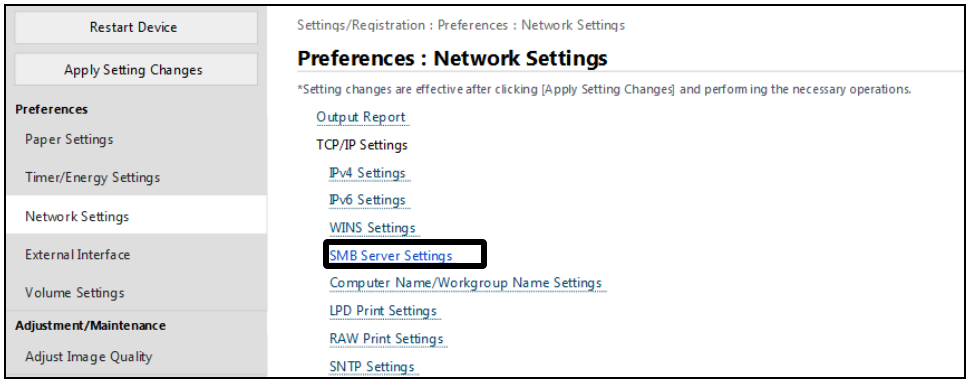


7. Update the network settings.

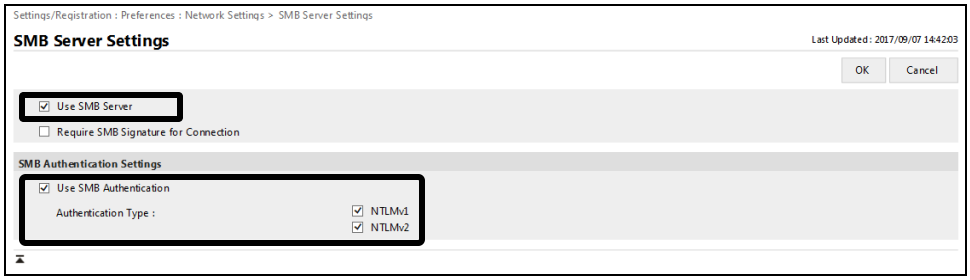
7.1 From the Settings/Registration screen, click [Network Settings].



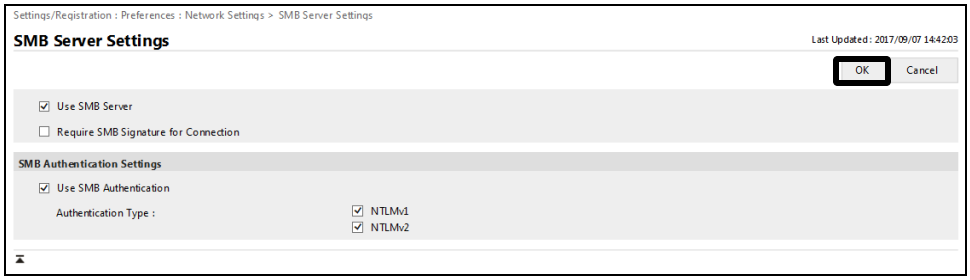
7.2 Click [SMB Server Settings].



7.3 Verify that the [Use SMB Server], [User SMB Authentication], and all [NTLMvX] check boxes are enabled. If any are not enabled, click them.

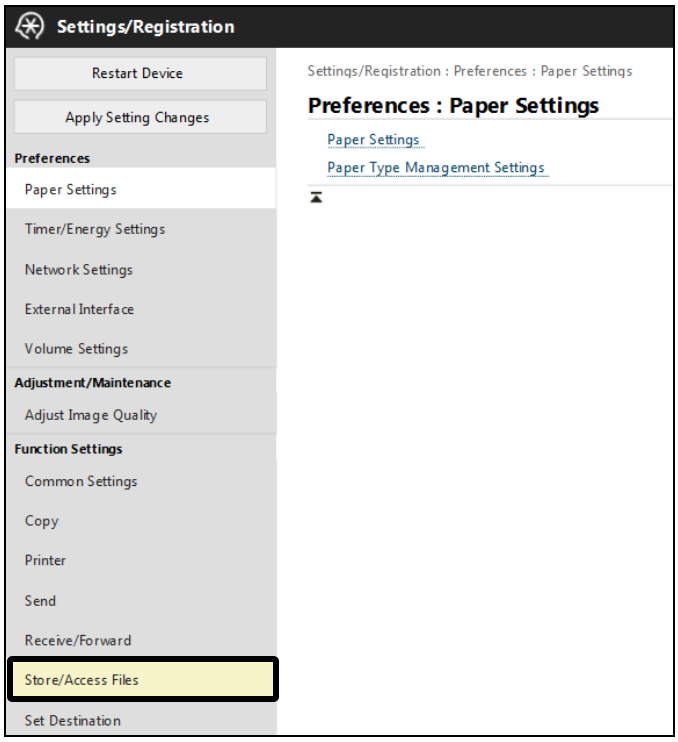


7.4 Click [OK].



8. Verify the Advance Box SMB settings.

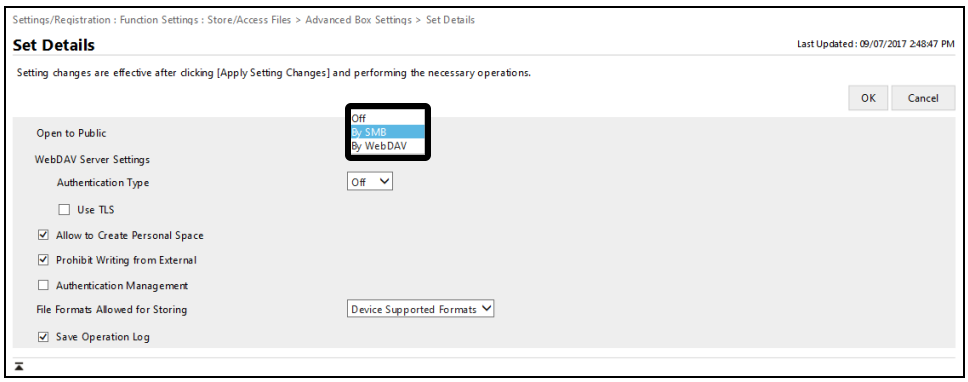
8.1 From the Settings/Registration screen, click [Store/Access Files].



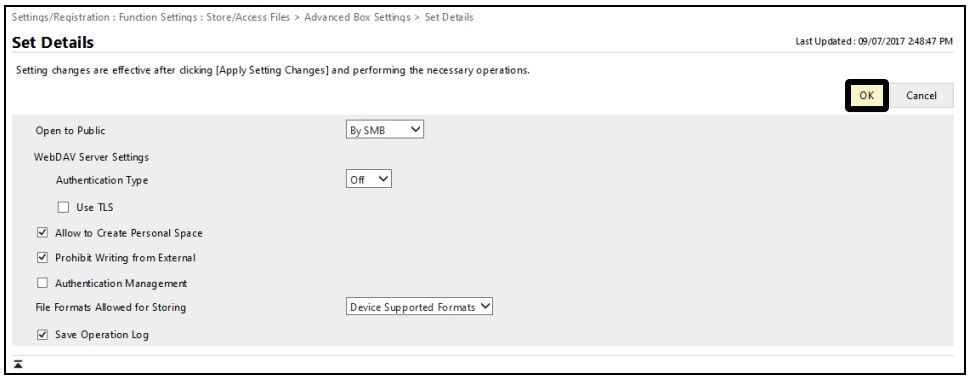
8.2 Click [Advanced Box Settings].

8.3 Click [Set Details].

8.4 Verify that the [Open to Public] pull-down list is set to [By SMB].



8.6 Click [OK].



IMPORTANT

Reboot the device after completing the above configuration procedures.

NOTE

Test the device setup by sending a fax to the device and checking the Advanced Box folder for the new incoming fax.

2.12.2 Preparing Fax Forwarding with FTP Server

This section describes the procedures to prepare a device to use the Authorized Send built-in FTP server for Fax Forwarding.

2.12.2.1 FTP Print Settings

FTP Printing and the Authorized Send FTP server both use port 21 by default. To use Fax Forwarding with the FTP server, you must either select a different port to use with the Authorized Send Fax Forwarding FTP server, or disable FTP printing.

See "Configuring the Authorized Send Servlet," starting on page 245 for instructions on specifying a different FTP port for Authorized Send. You must also change the FTP Send port in the device's Service Mode. Refer to your device's Service Manual for information on changing the FTP Send Port.

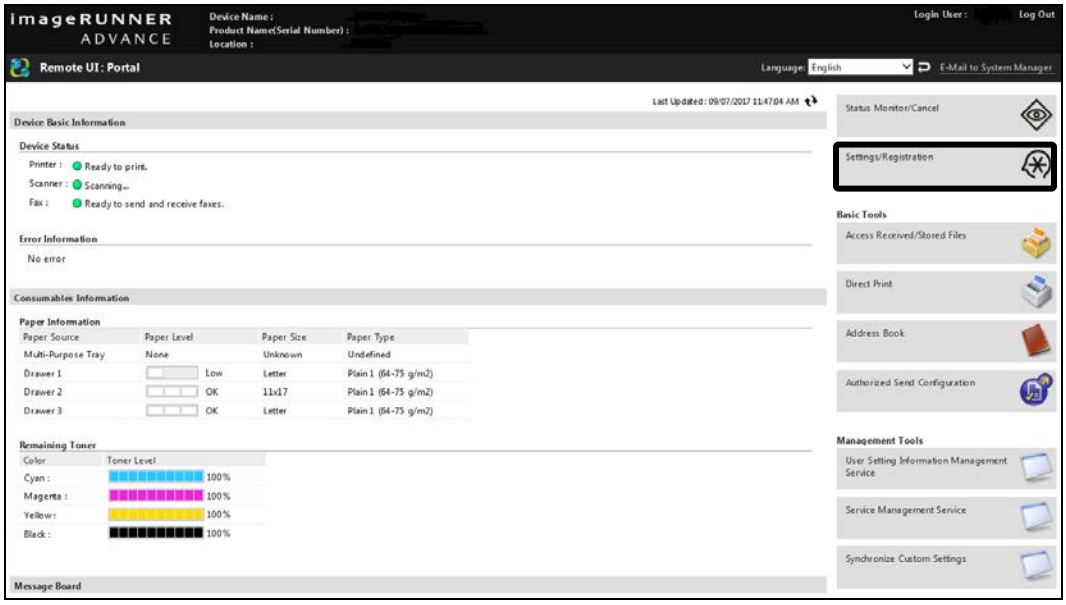
NOTE
You may need to contact your servicing dealer for assistance to access service mode and change the FTP Send Port. This is only necessary if you require FTP printing and Authorized Send Fax Forwarding using FTP to run simultaneously.

See below for disabling FTP printing.

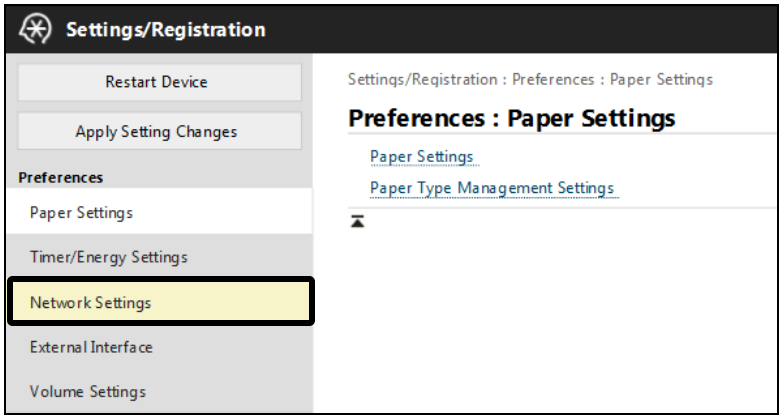
---

1. Log in to the device's RUI (Remote User Interface). Contact your System Administrator for log in procedures and any necessary credentials.

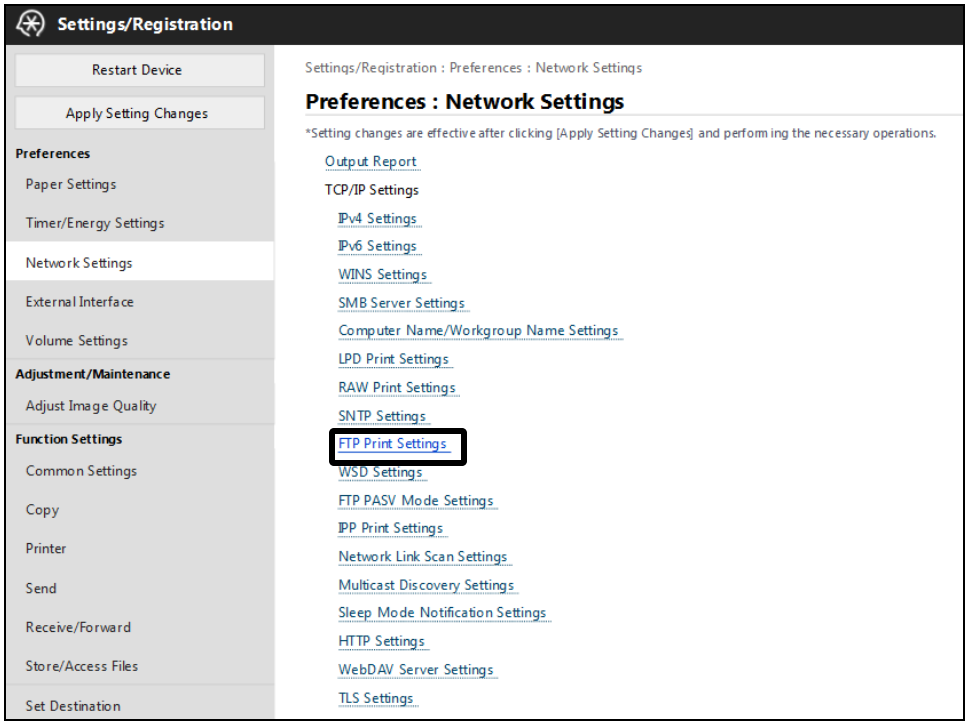
2. Click on [Settings/Registration].



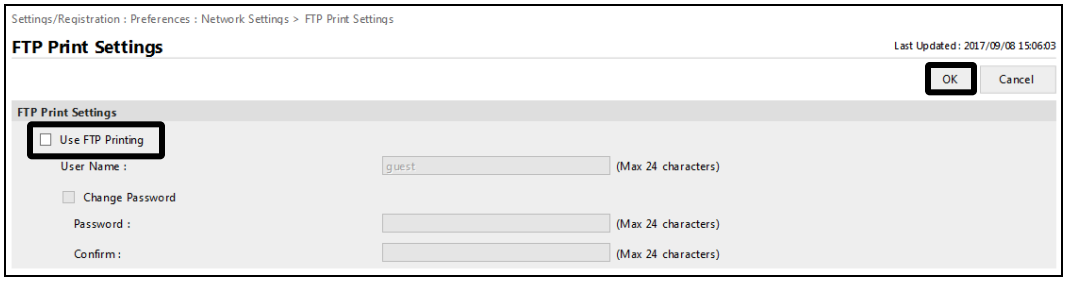
3. Under the Preferences link heading, click on [Network Settings].



4. In the TCP/IP Settings, click [FTP Print Settings].



5. Verify the [Use FTP Printing] check box is de-selected. If it is selected, click to de-select it →click [OK].



2.12.2.2 Configuring the Address Book Destination

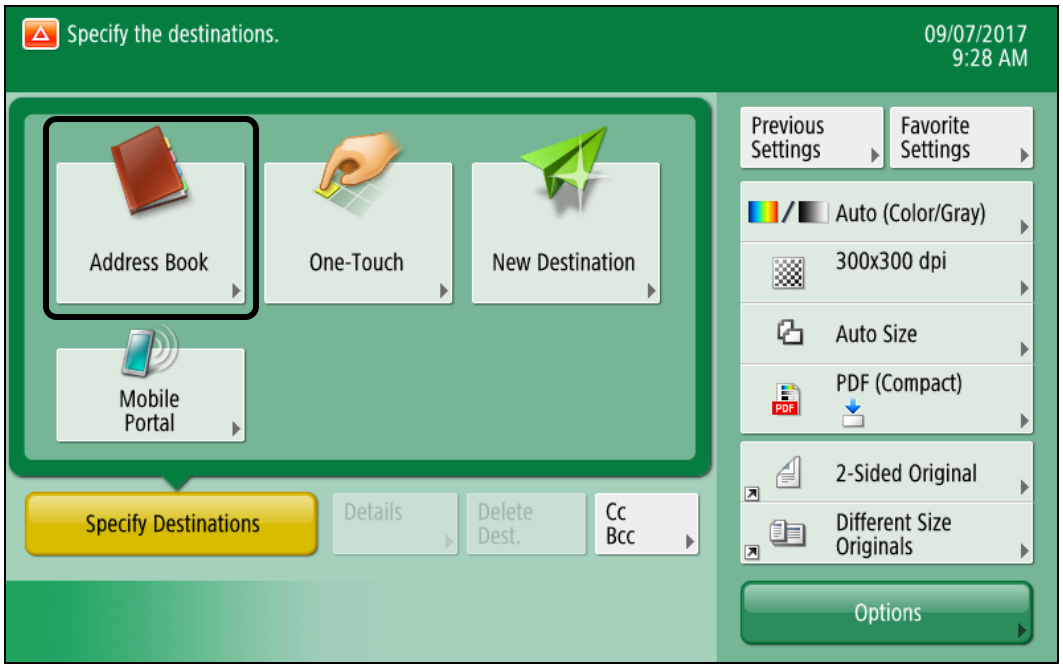
You must create a new destination in the Address Book to act as the destination for incoming faxes

---

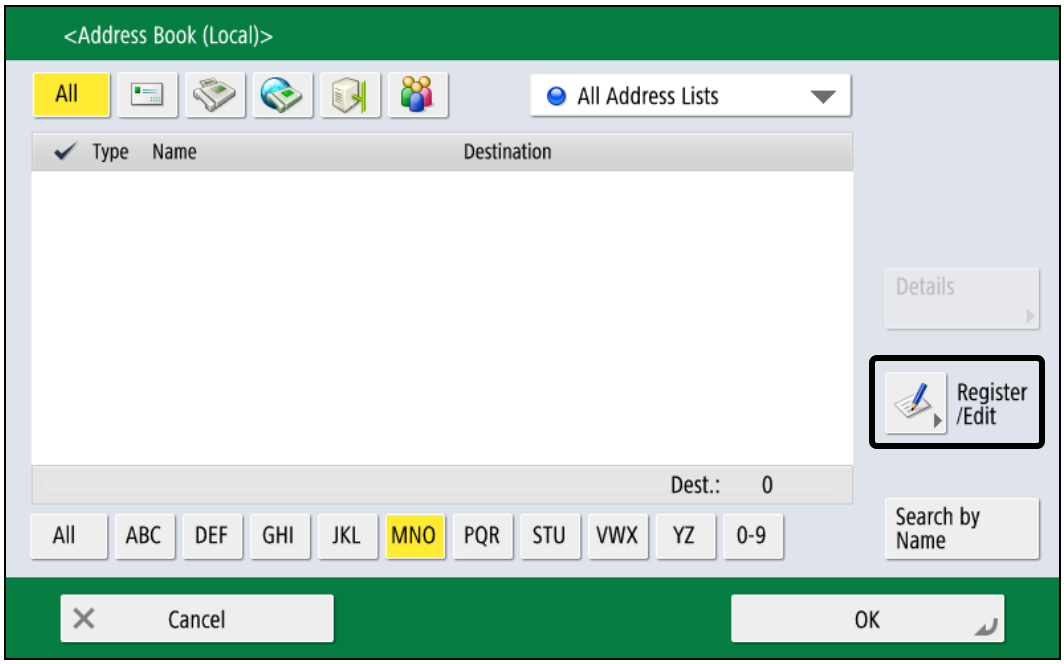
1. Walk up to the device and log in if necessary. Contact your System Administrator for log in procedures and any necessary credentials.

2. Press [Scan and Send] on the main menu.

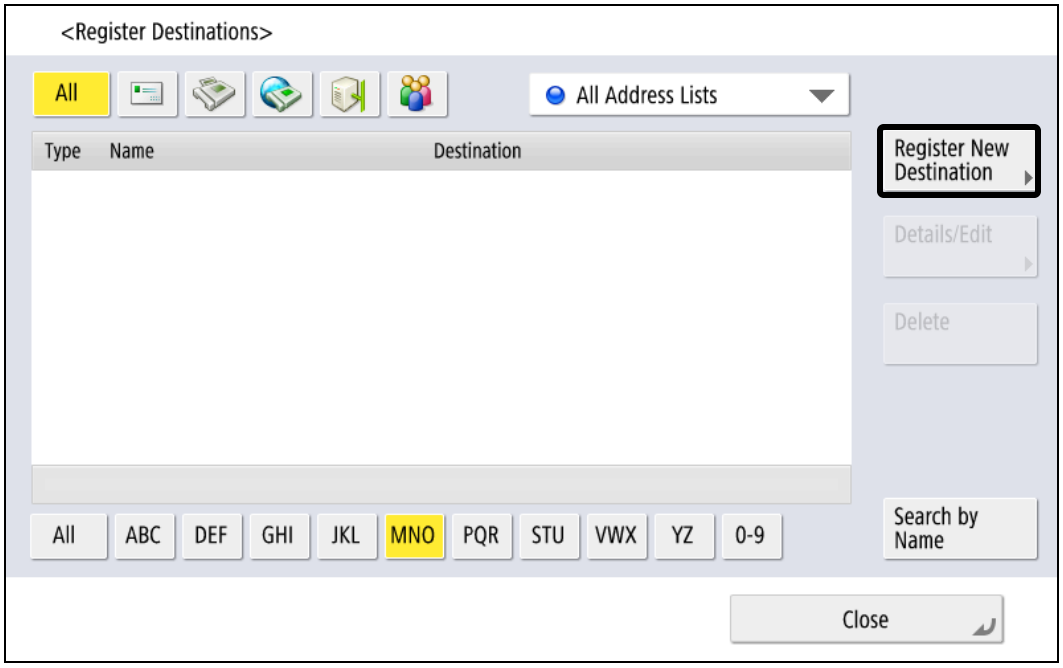
3. Press [Address Book].



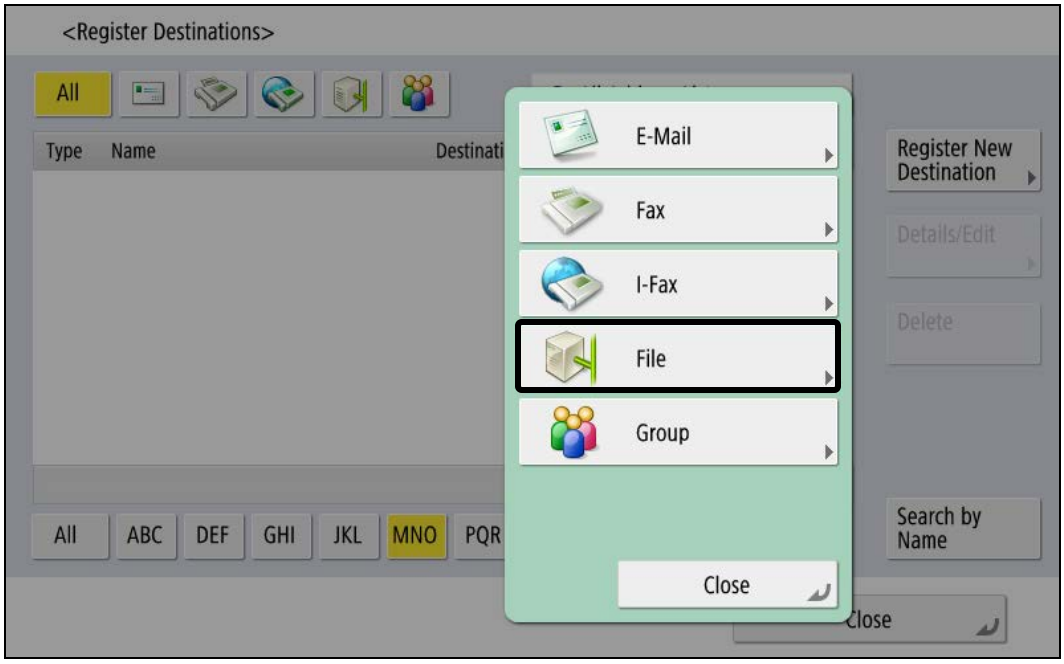
4. Press [Register/Edit].



5. Press [Register New Destination].

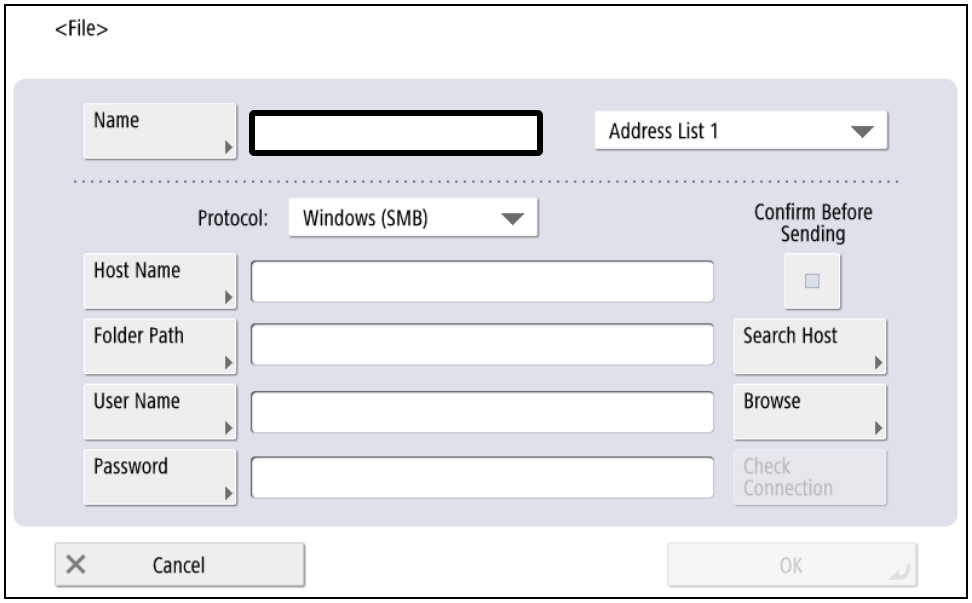


6. Press [File].

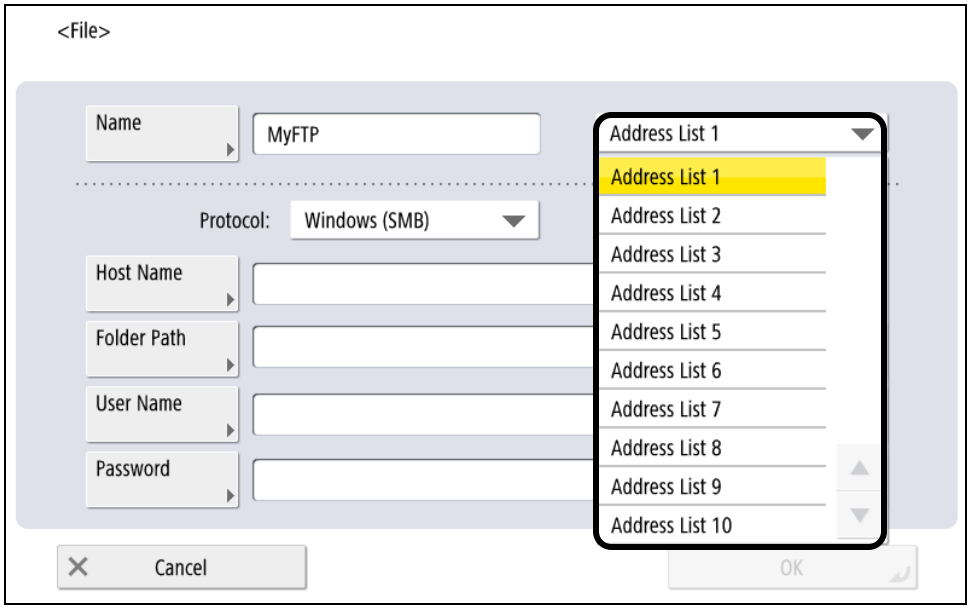


7. Create a new folder.

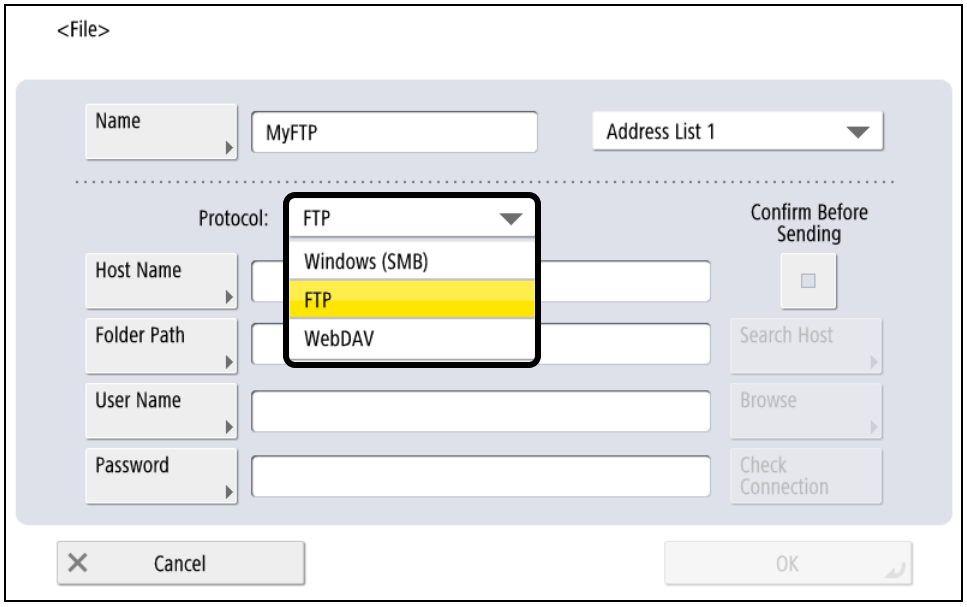
7.1 Enter a name for the destination.



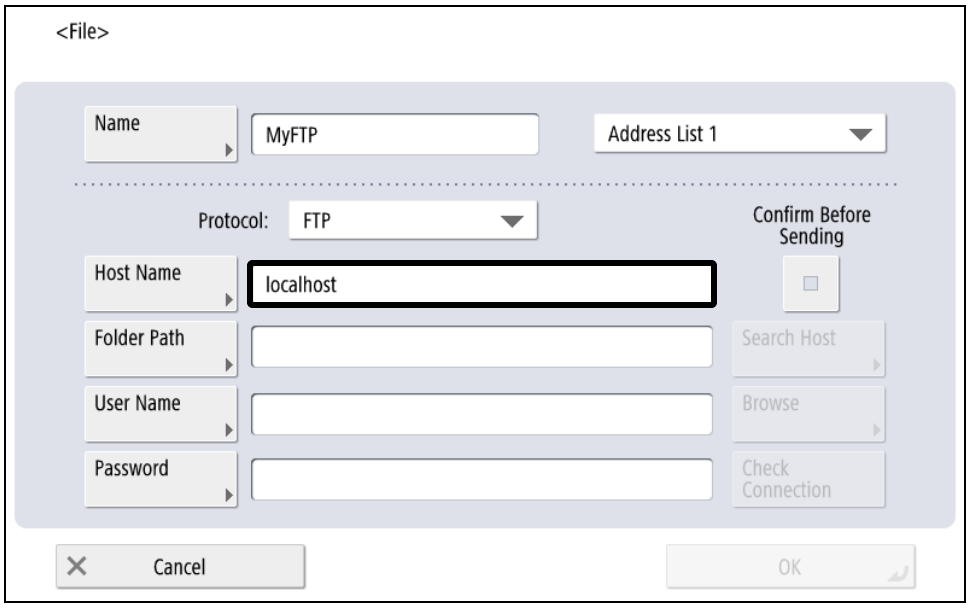
7.2 Press the Address List pull-down list and select the address list in which you want the destination to be set.



7.3 Select FTP from the [Protocol] pull-down list.

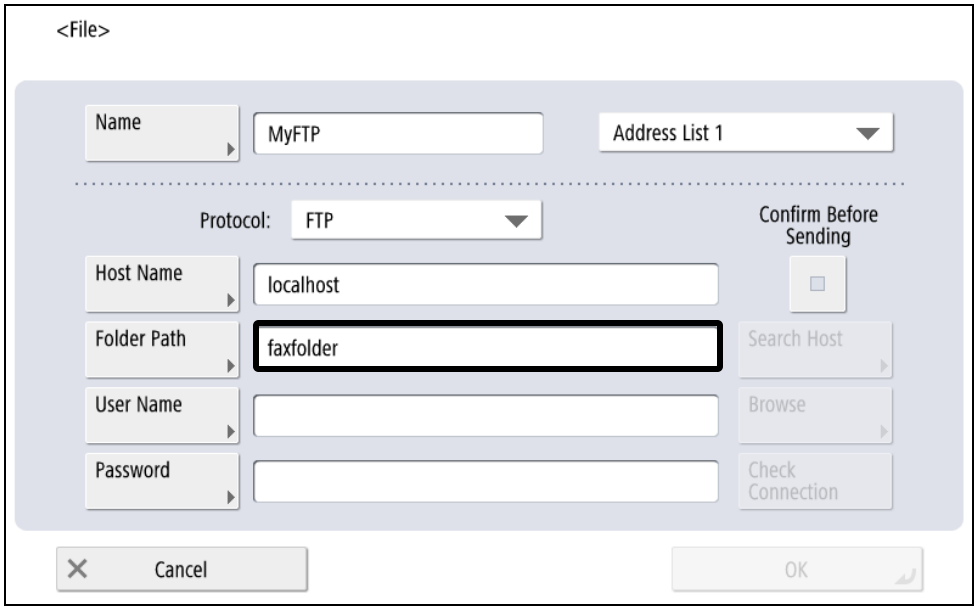


7.4 Enter “127.0.0.1” or “localhost” in the [Host Name] text box.

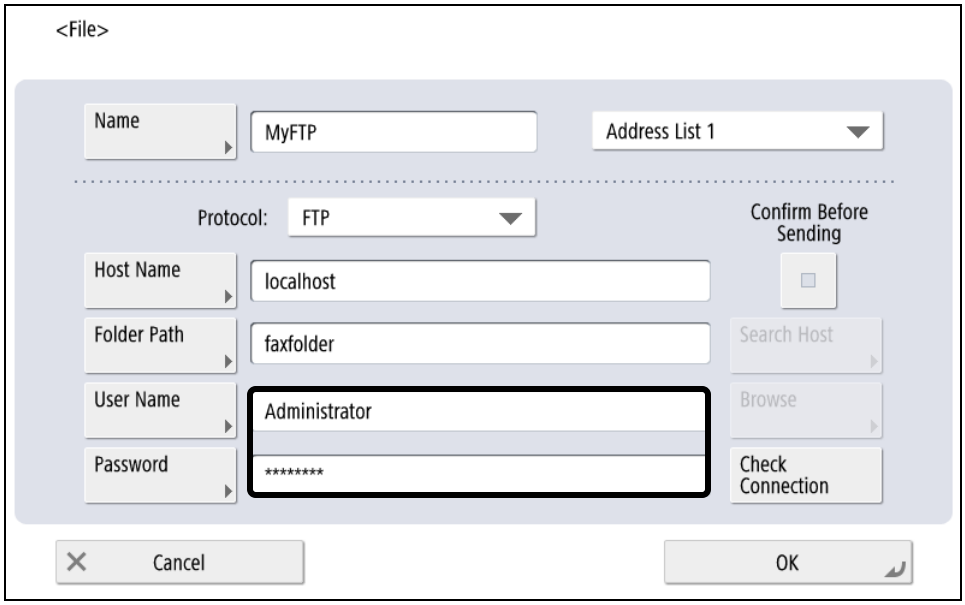


NOTE
Use 127.0.0.1 if your device has IPv6 and IPv4 enabled simultaneously

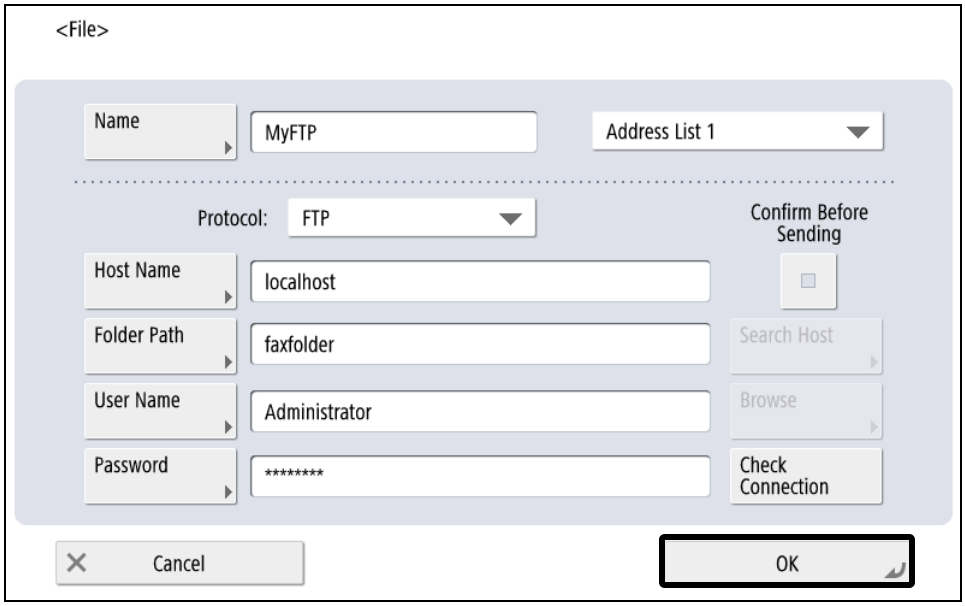
7.5 Enter a desired folder name.



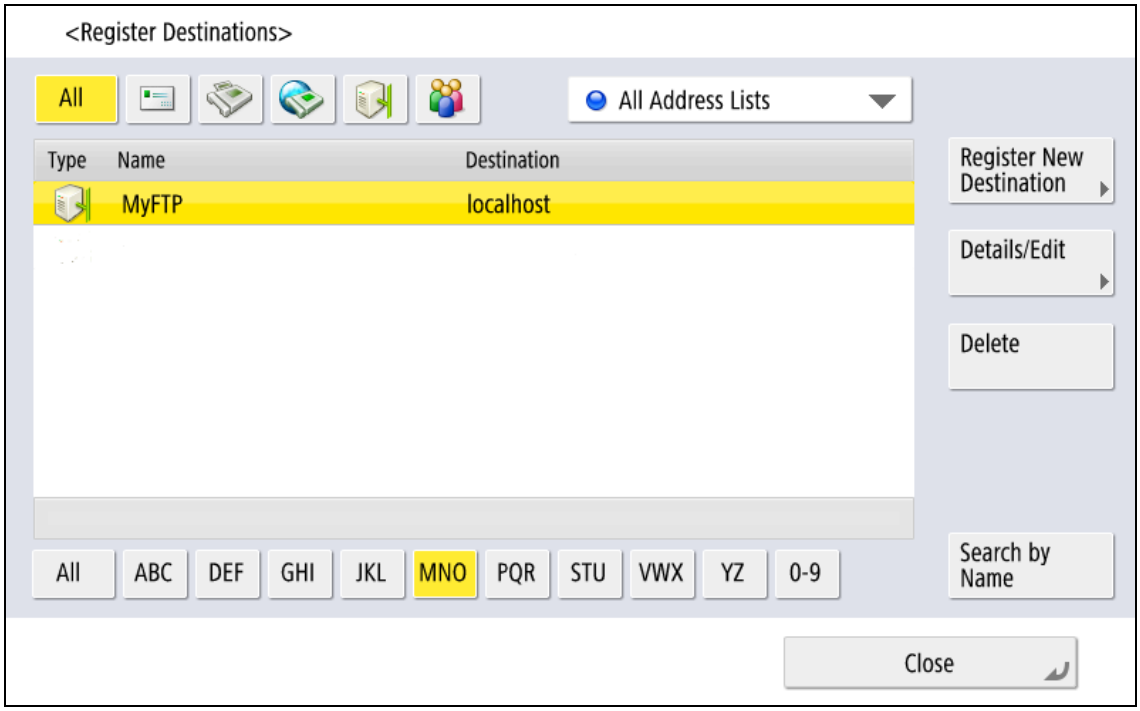
7.6 Set the FTP credentials in the [User Name] and [Password] text boxes.



7.7 Press [OK].



The Address Book destination is ready.

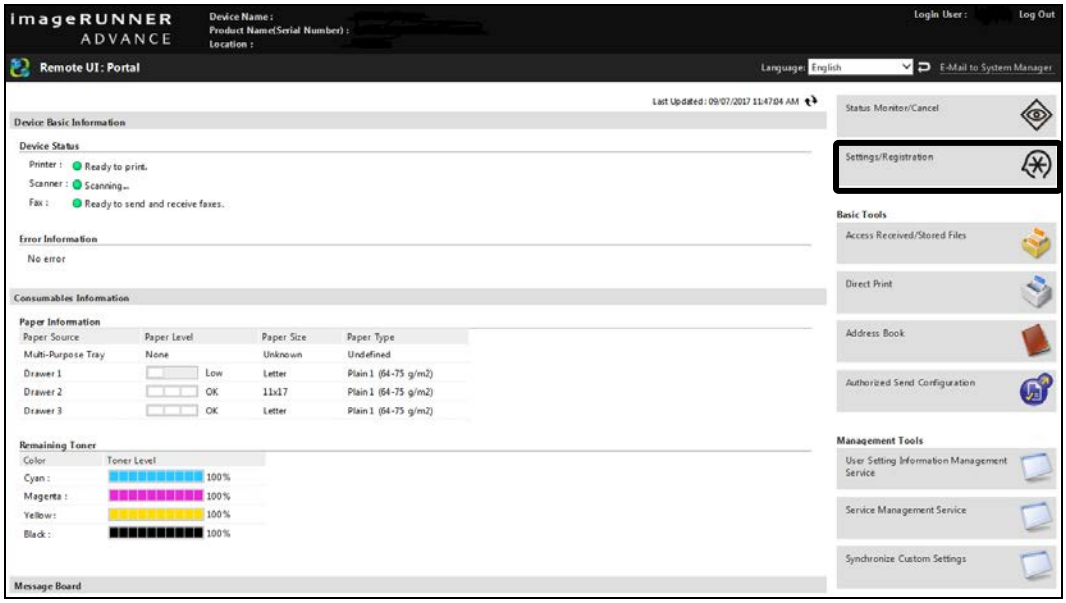


2.12.2.3 Configuring the Forwarding Settings

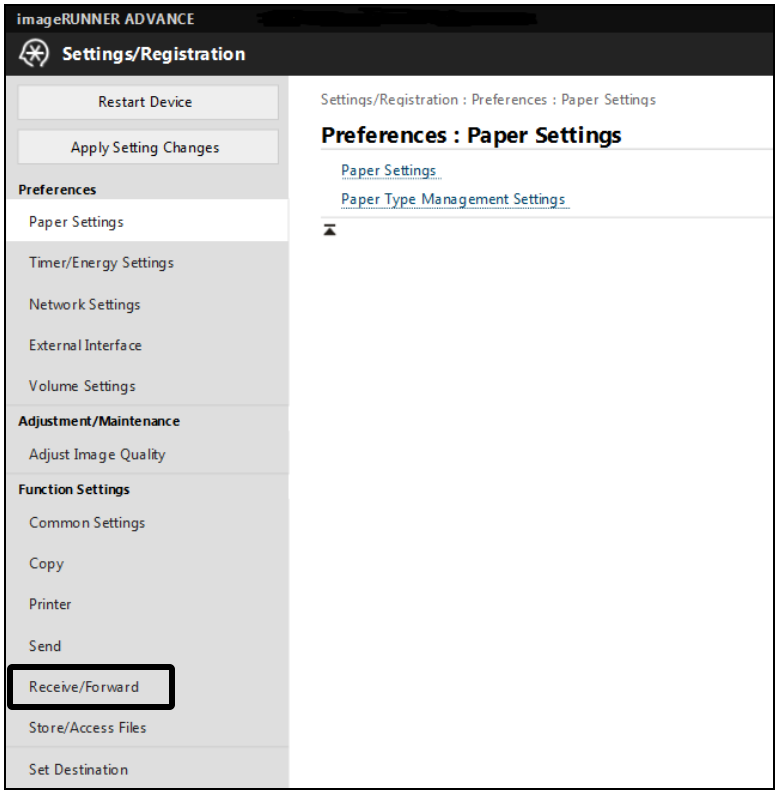
You must change the device's forwarding information to properly forward incoming faxes to the correct location(s).

1. Log in to the device's RUI (Remote User Interface). Contact your System Administrator for log in procedures and any necessary credentials.

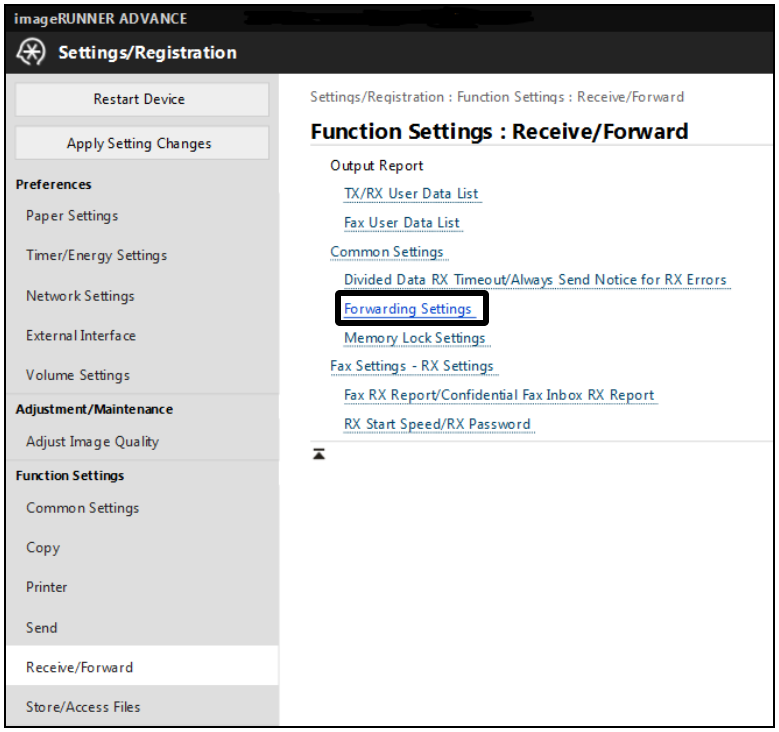
2. Click on [Settings/Registration].



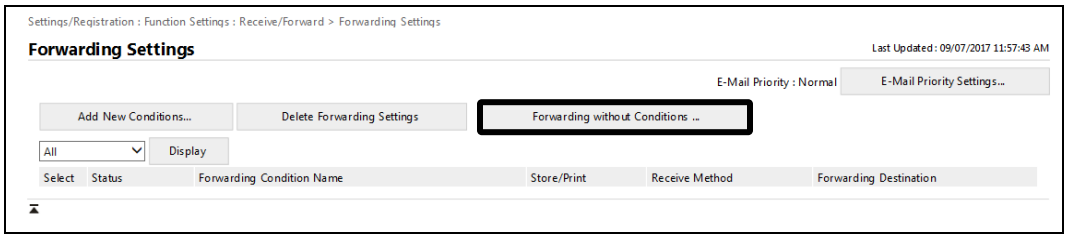
3. Under the Function Settings links, click on [Receive/Forward].



4. Click on [Forwarding Settings].

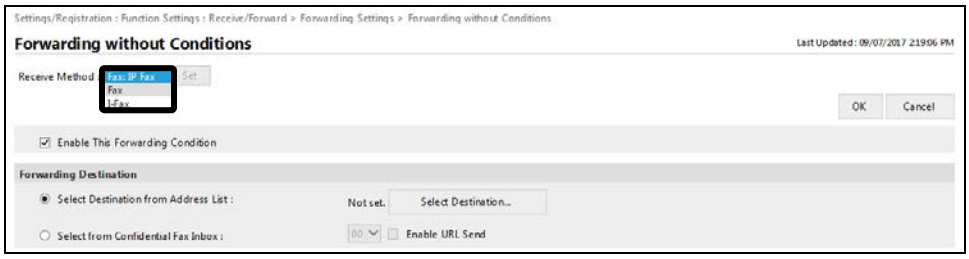


5. Click on [Forward without Conditions].

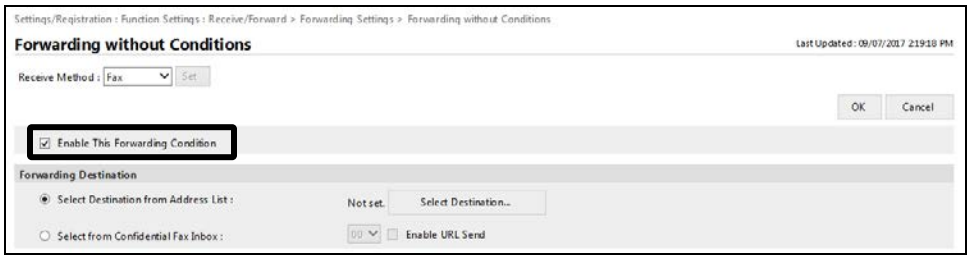


6. Create the forwarding association

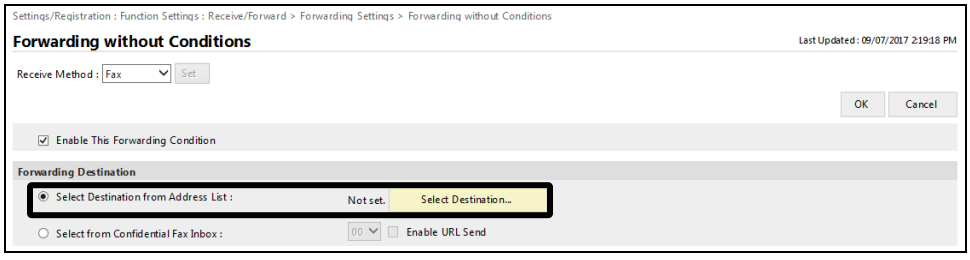
6.1 Select the incoming fax line from the [Receive Method] pull-down list → click [Set].



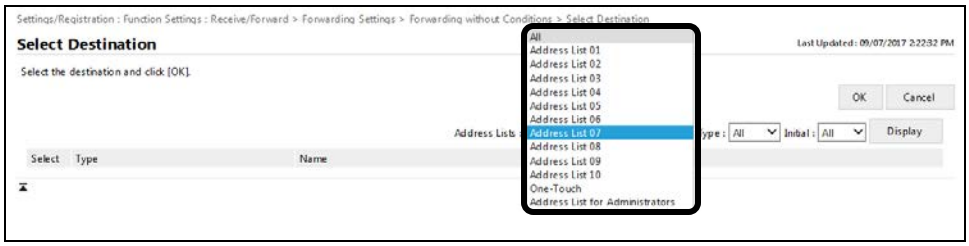
6.2 If it is not already selected, select the [Enable this Forwarding Condition] check box.



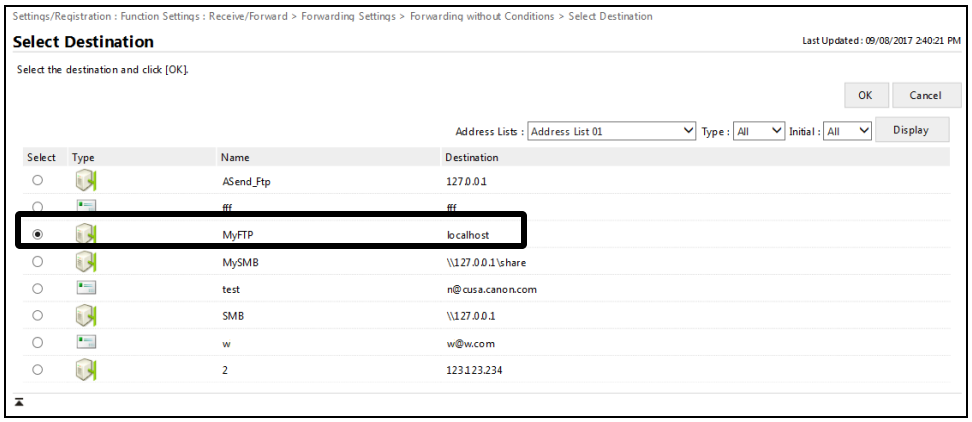
6.3 Select the [Select Destination from Address List] radio button → click on [Select Destination].



6.4 Select the address book to which you assigned the Fax Destination in Section 3.3.2. If you do not remember, select [All] → click [Display].



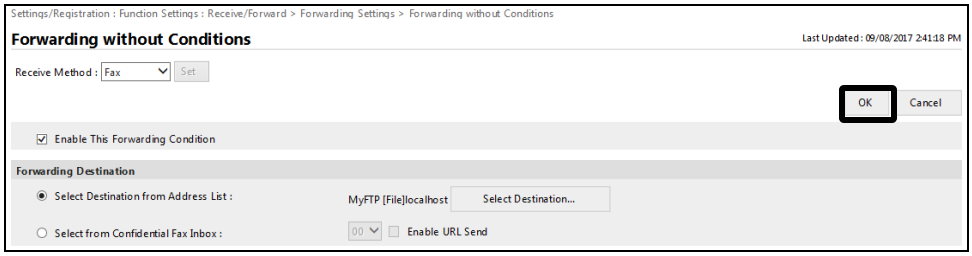
6.5 Select the radio button of the desired fax destination → click [OK].



NOTE

If the destination is from an Address Box other than the Administrator Address Box, a dialog box appears. Click [OK] to confirm the selected destination.

6.6 Click [OK] at the “Forwarding without Conditions” page.



IMPORTANT

Reboot the device after completing the above configuration procedures.

2.12.3 Configuring the Authorized Send Servlet

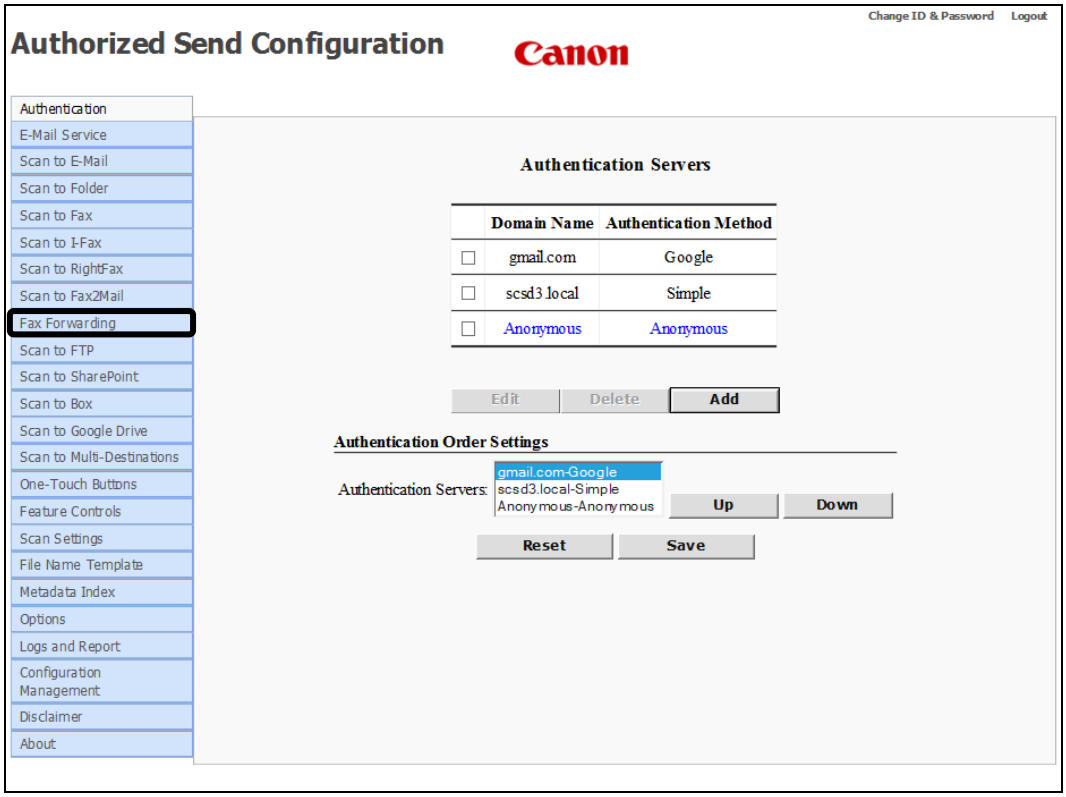
This section describes the procedures to configure the Authorized Send servlet for Fax Forwarding.

2.12.3.1 Creating a Fax Forwarding Setting

You can create up to 10 Fax Forwarding Settings.

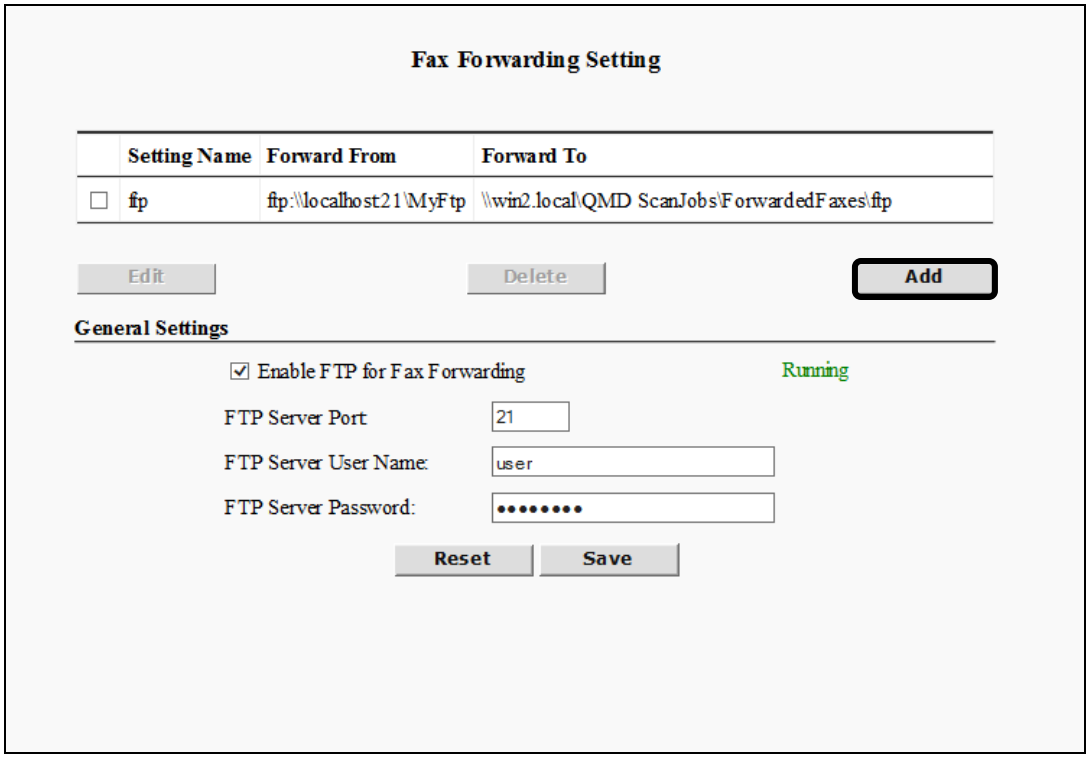
---

1. Log in to the Authorized Send configuration servlet.
2. Click [E-Mail Service] →[Address Book].



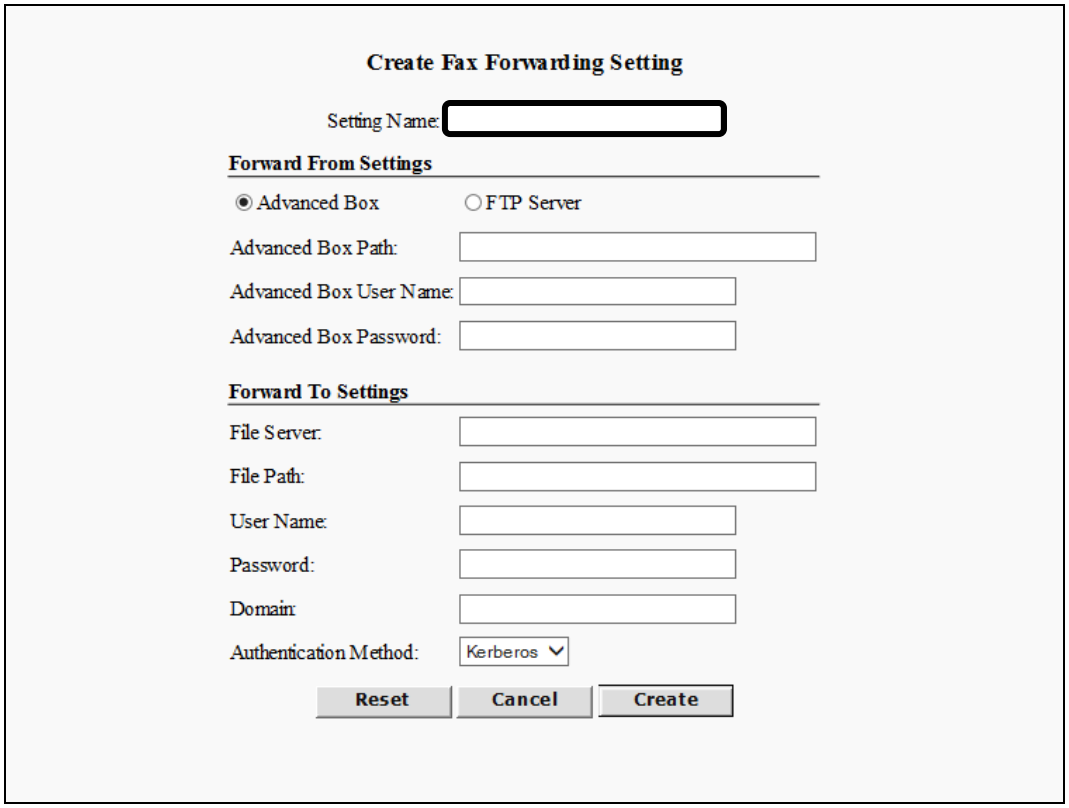
The Fax Forwarding Setting screen is displayed.

3. Click [Add].



The Create Fax Forwarding Setting screen is displayed.

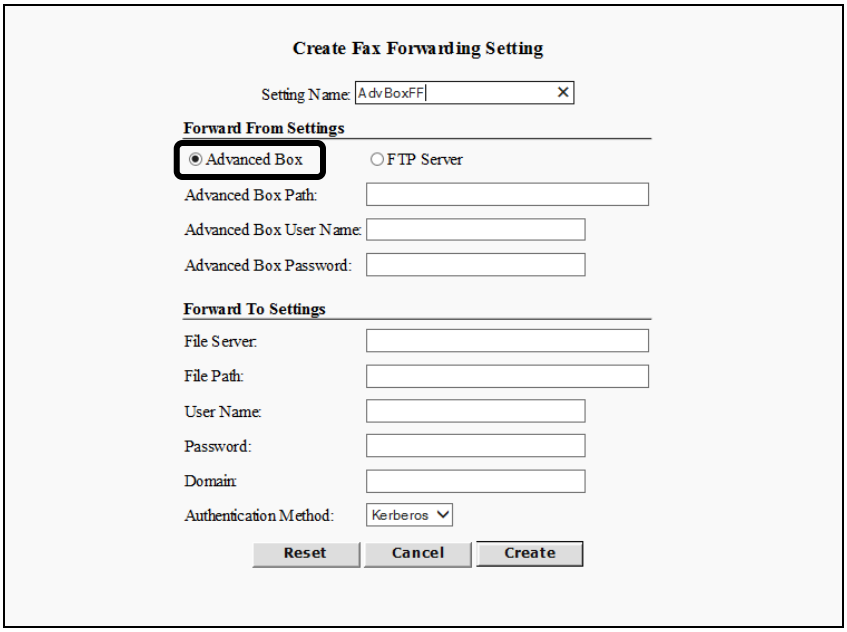
4. Enter the desired setting name in the [Setting Name] text box.



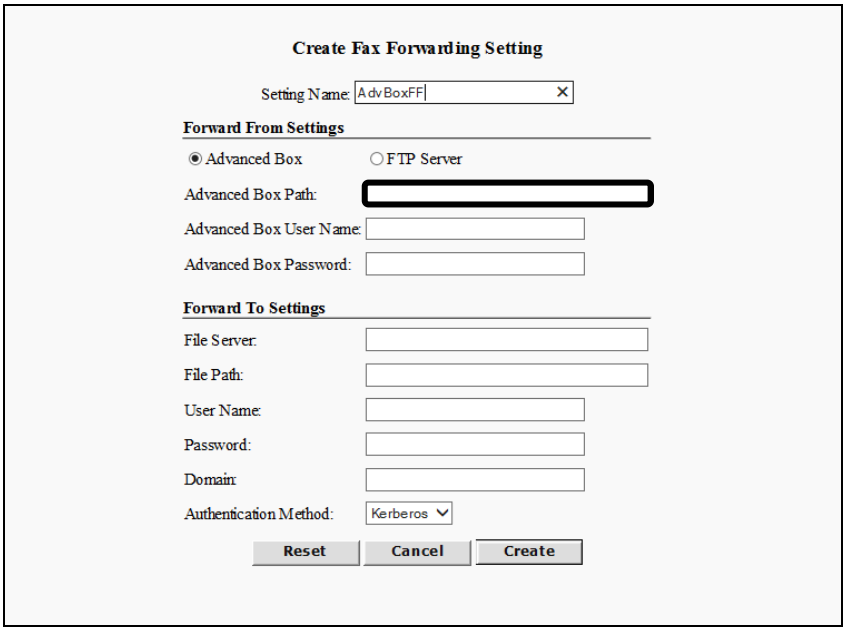
5. Specify whether you will forward faxes using the Advanced Box or FTP.

5.1 If you want to forward faxes using the Advanced Box, set the appropriate values in the <Forward From Settings>.

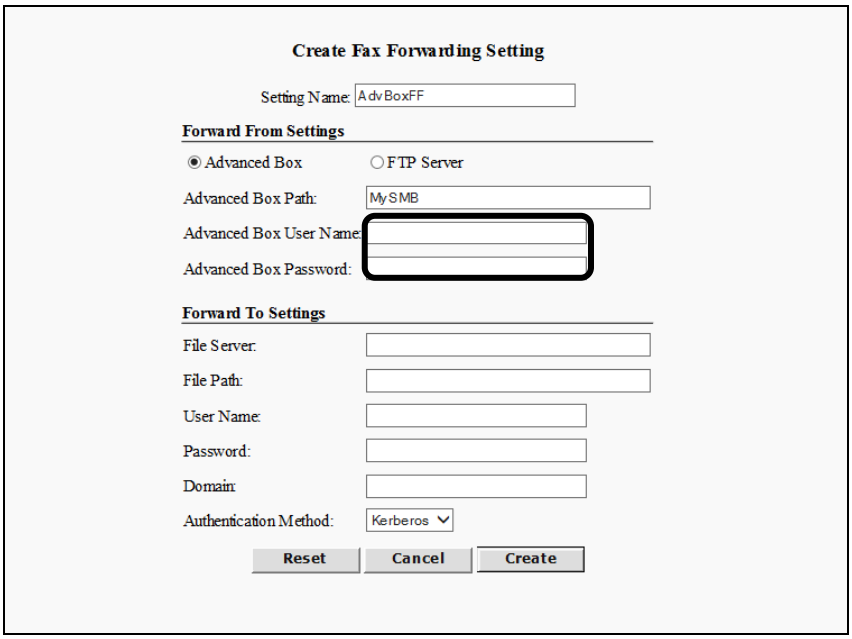
5.1.1 Select the [Advanced Box] radio button.



5.1.2 Enter the Advanced Box path in the [Advanced Box Path] text box.

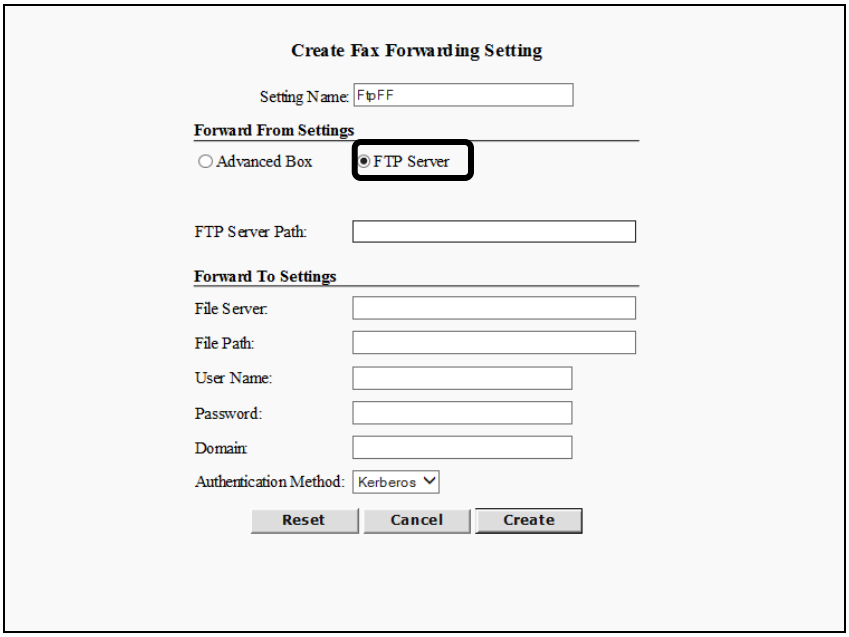


5.1.3 Enter the Advanced Box credentials in the [Advanced Box User Name] and [Advanced Box Password] text boxes.

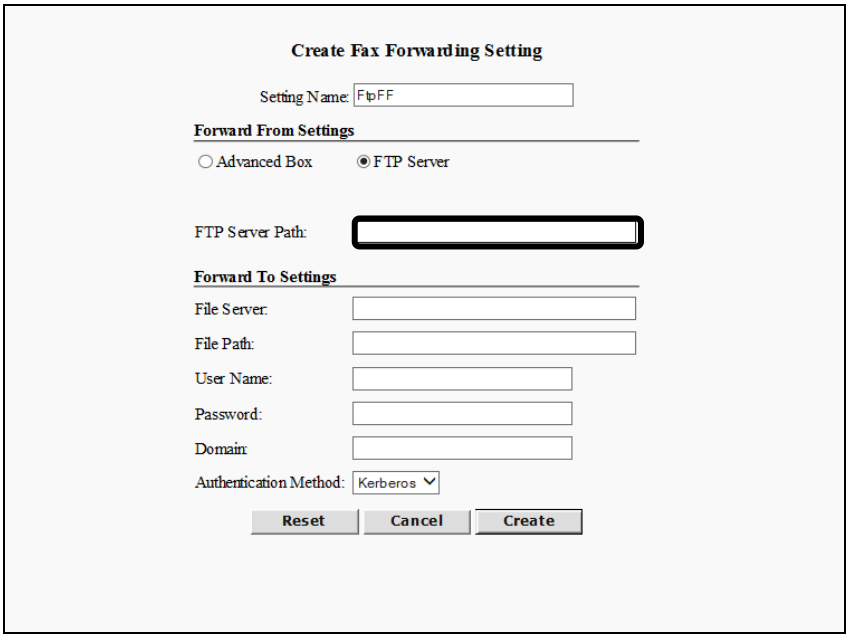


5.2 If you want to forward faxes using FTP, set the appropriate values in the <Forward From Settings>.

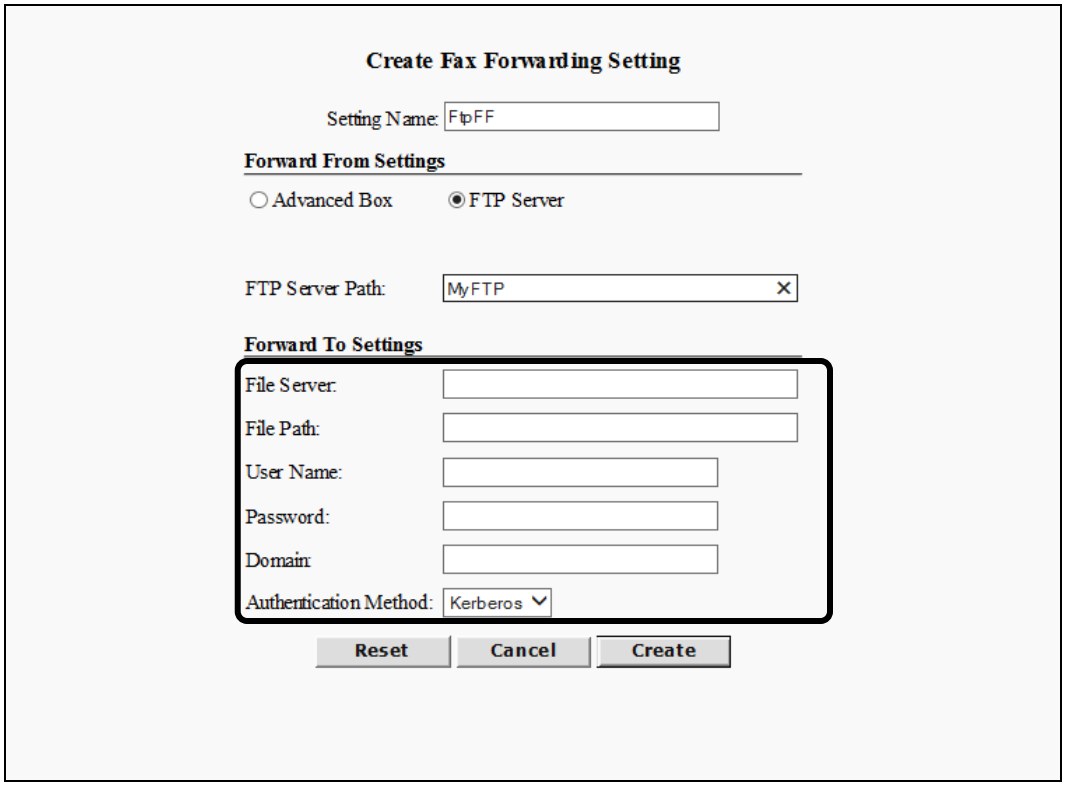
5.2.1 Select the [Advanced Box] radio button.



5.2.2 Enter the FTP server path in the [FTP Server Path] text box.



6. Configure the <Forward To Settings>.

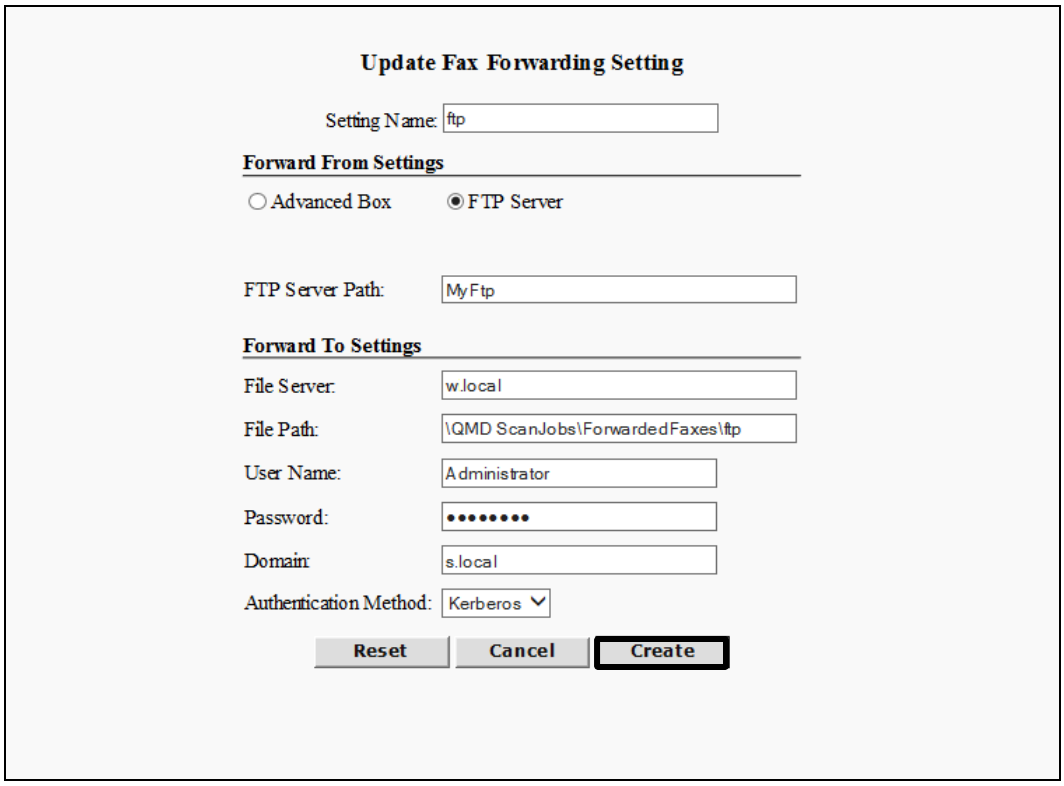


Forward To Settings

File Server:	The destination file server for the forwarded fax. This is a required field and can consist of any valid file server name.
File Path:	The destination path on the file server for the forwarded fax. This is a required field and can consist of any valid path name on the destination file server. This field must be unique from any other defined FTP Fax Forwarding Settings.
User Name:	The destination file server user name. This is a required field and may not be longer than 255 characters.
Password:	The destination file server password. This is a required field and must be the valid password for the [User Name] entered.

Domain:	The destination file server domain name. This is a required field and may not be longer than 255 characters
Authentication Method:	The type of authentication method to use for credential verification on the destination file server. Only [Kerberos] and [NTLM] are available in the pull-down list. [Kerberos] is the default.

7. Click [Create].



If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

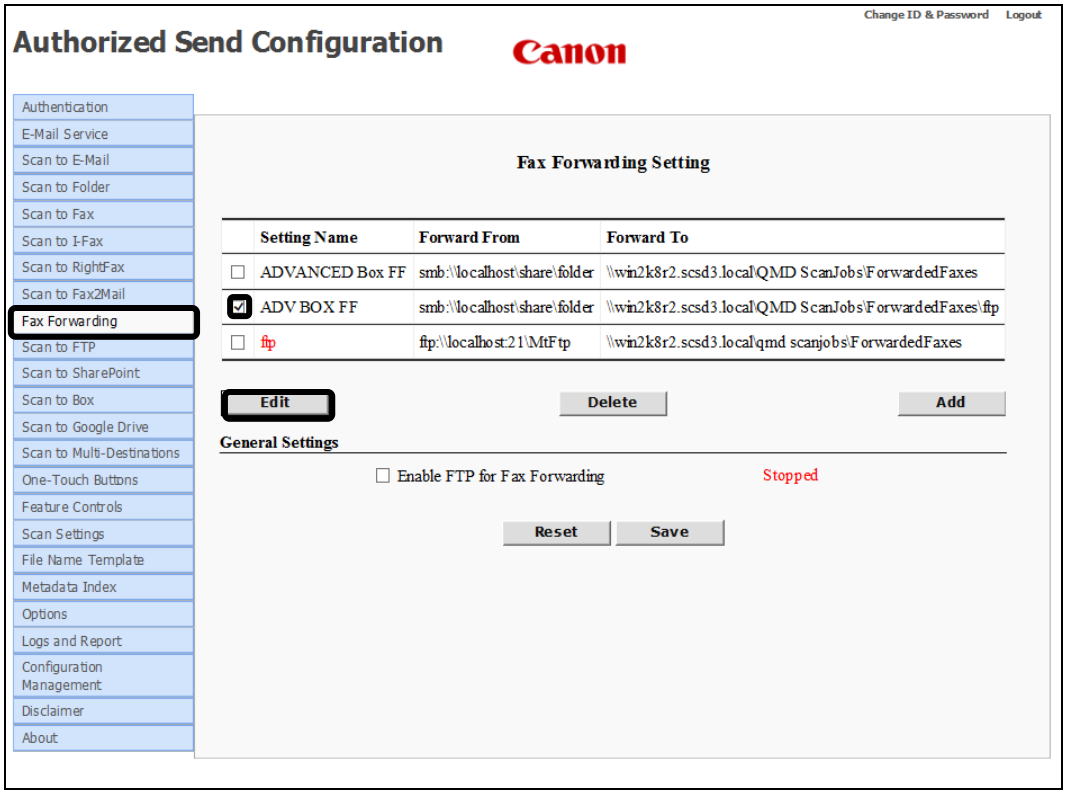
To cancel creating the address book server and return to the Fax Forwarding Settings screen, click [Cancel].

The fax forwarding setting is created and added to the fax forwarding settings list on the For Forwarding Settings screen.

2.12.3.2 Editing a Fax Forwarding Setting

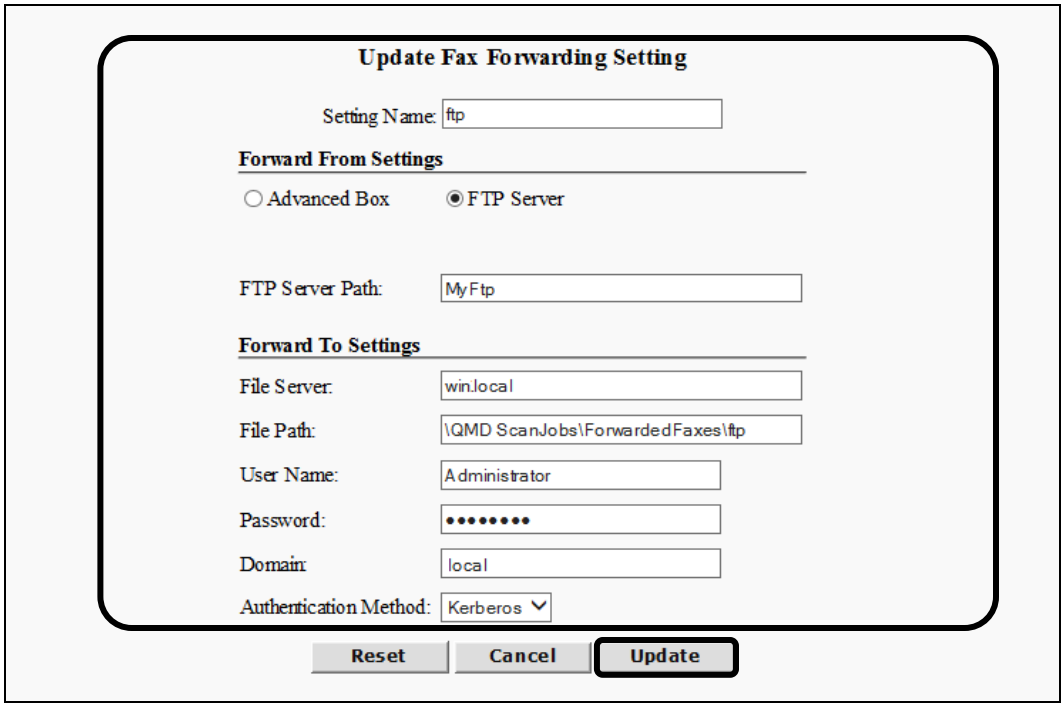
You can edit a previously created Fax Forwarding Setting from the Fax Forwarding configuration screen.

1. Click [Fax Forwarding] → select the check box next to the Fax Forwarding Setting you want to edit → click [Edit].



The Update Fax Forwarding Setting screen is displayed.

2. Edit the settings for the address book server as necessary → click [Update].



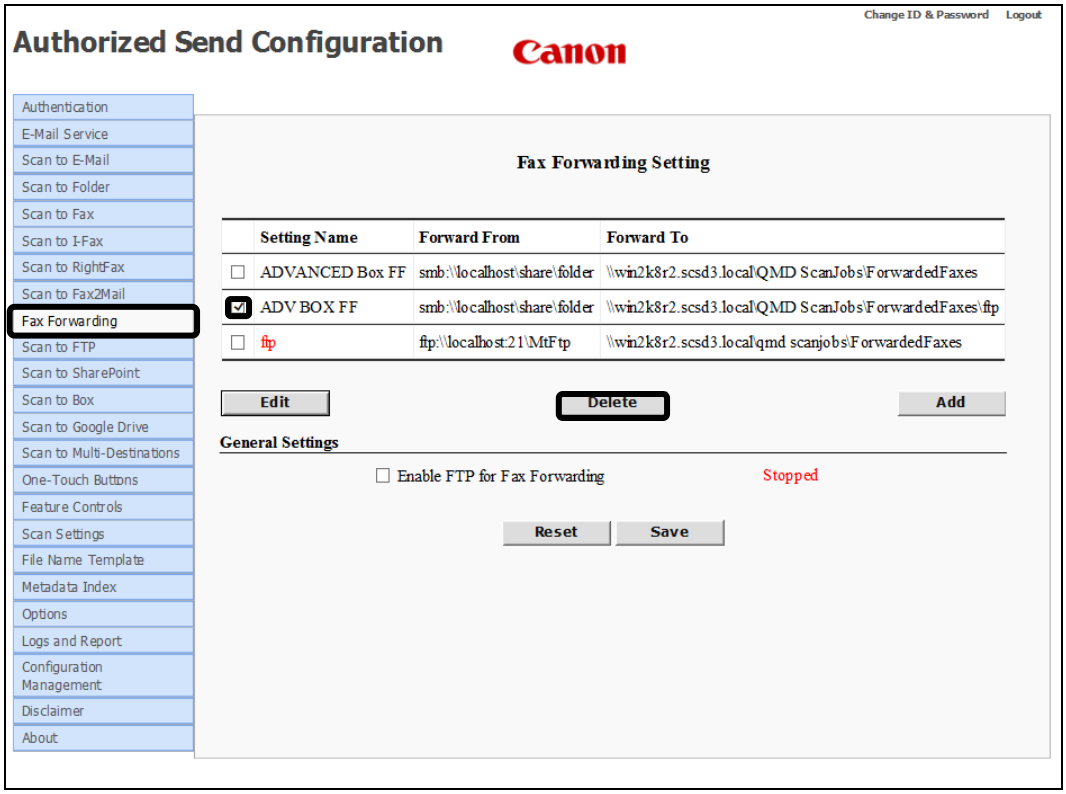
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the address book server and return to the Fax Forwarding Setting screen, click [Cancel].

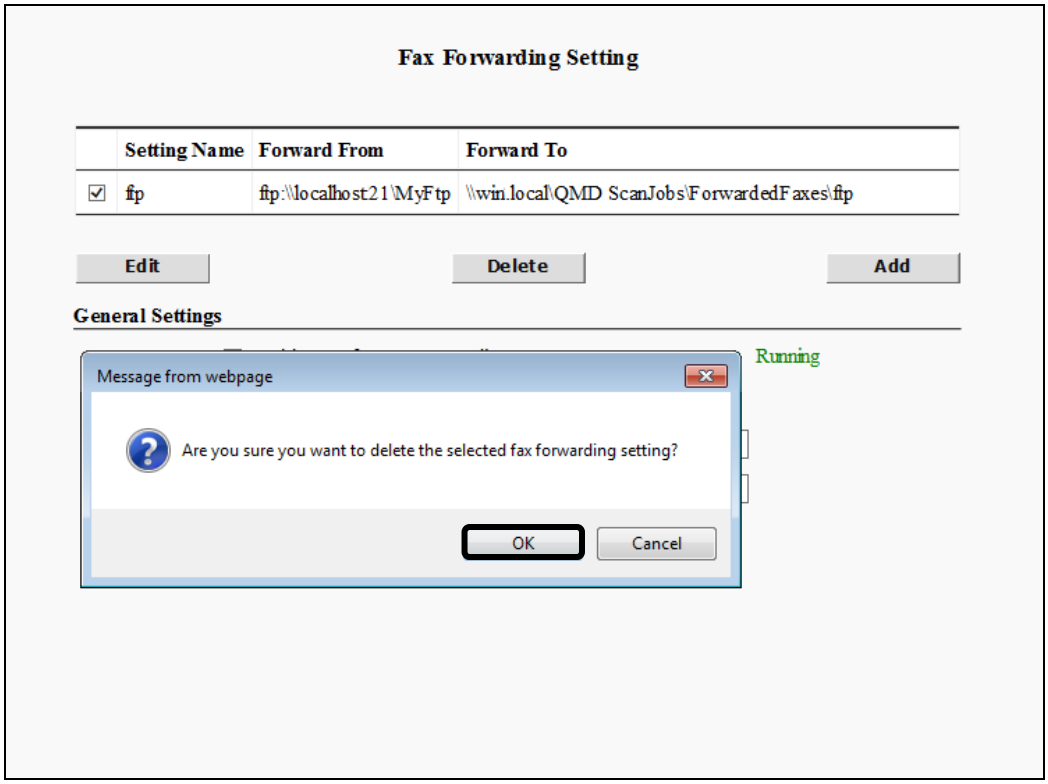
2.12.3.3 Deleting a Fax Forwarding Setting

You can delete a previously created Fax Forwarding setting from the fax forwarding configuration screen.

1. Click [Fax Forwarding] → select the check box next to the Fax Forwarding Setting you want to delete → click [Delete].



2. Click [OK].



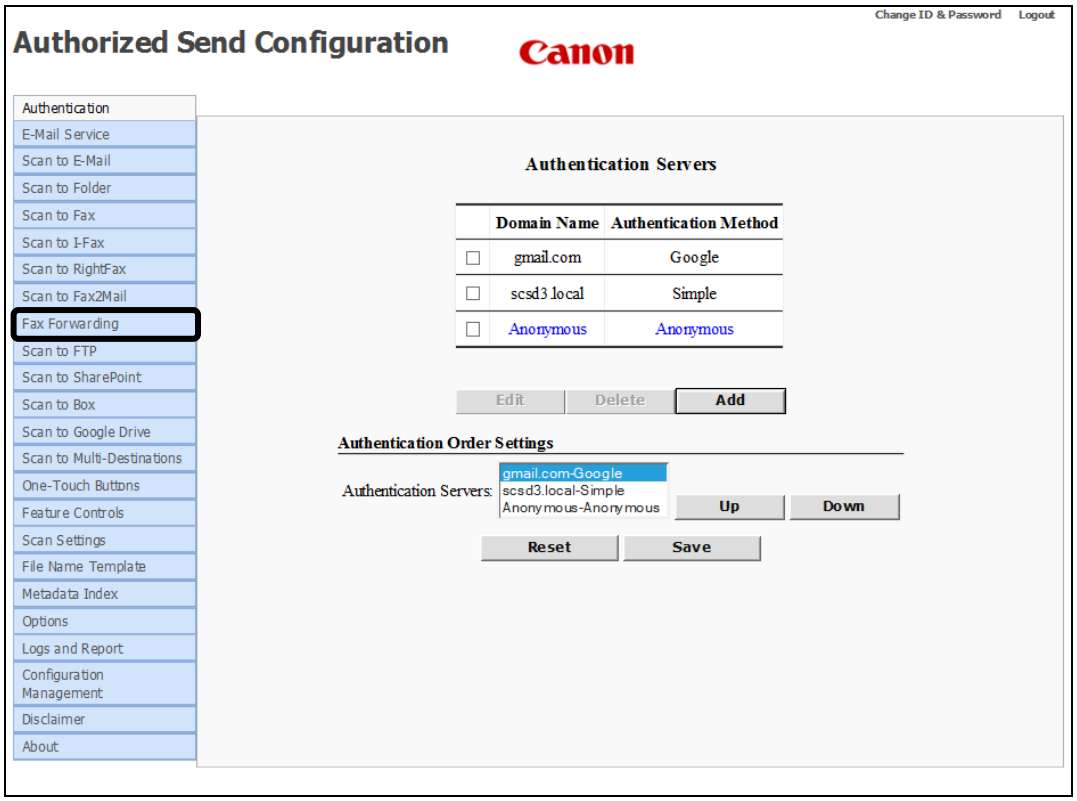
If you do not want to delete the Fax Forwarding Setting, click [Cancel].

The Fax Forwarding Setting is deleted from the list.

2.12.3.4 Configuring the General Settings

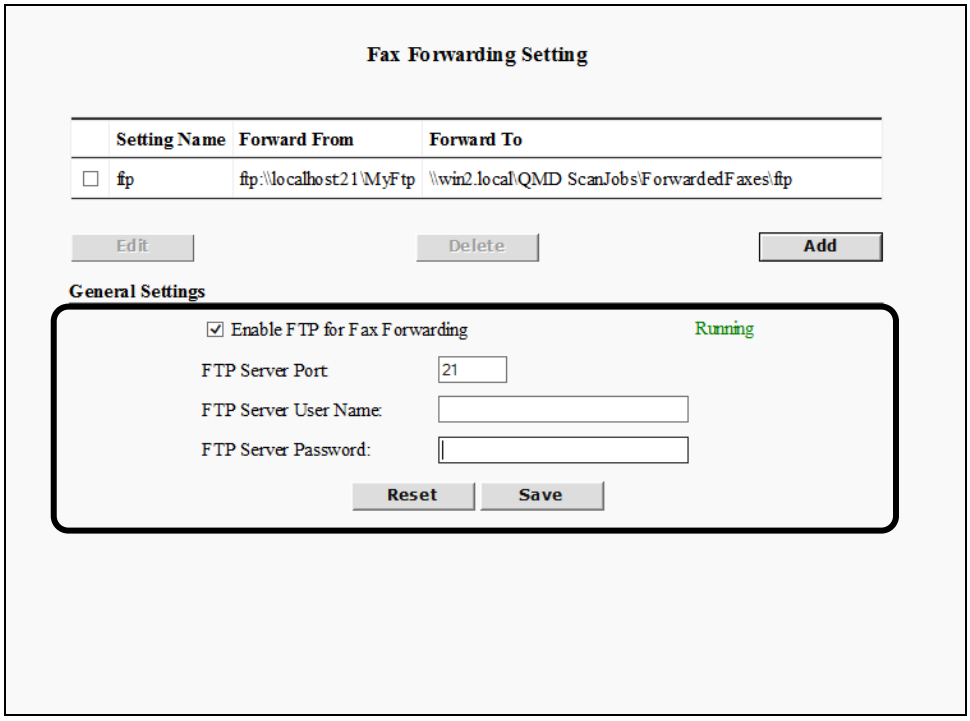
You can configure general Fax Forwarding settings from the Fax Forwarding Settings configuration screen.

1. Click [Fax Forwarding].



2. Specify the General Settings based on whether or not you will be using FTP forwarding or Advanced Box forwarding.

   2.1 If you will be using FTP forwarding, select the [Enable FTP for Fax Forwarding] check box and set the appropriate values in the <General Settings>.



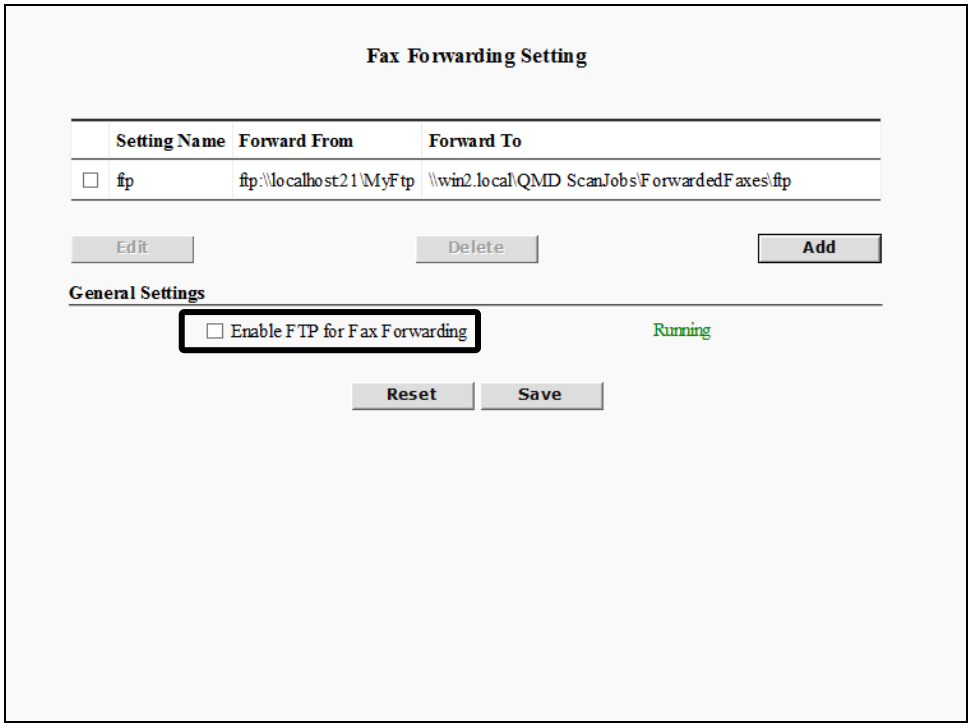
FTP Server Port: Set the FTP server port. The value must be numeric between 1 and 65535. The default is 21.

If FTP printing is enabled on the device, you must set this port to something other than the default, and to the same value as the FTP send port configured in service mode.

FTP Server User Name: Create the Authorized Send FTP Server user name. There is a maximum length of 255 characters.

FTP Server Password: Create the Authorized Send FTP Server password.

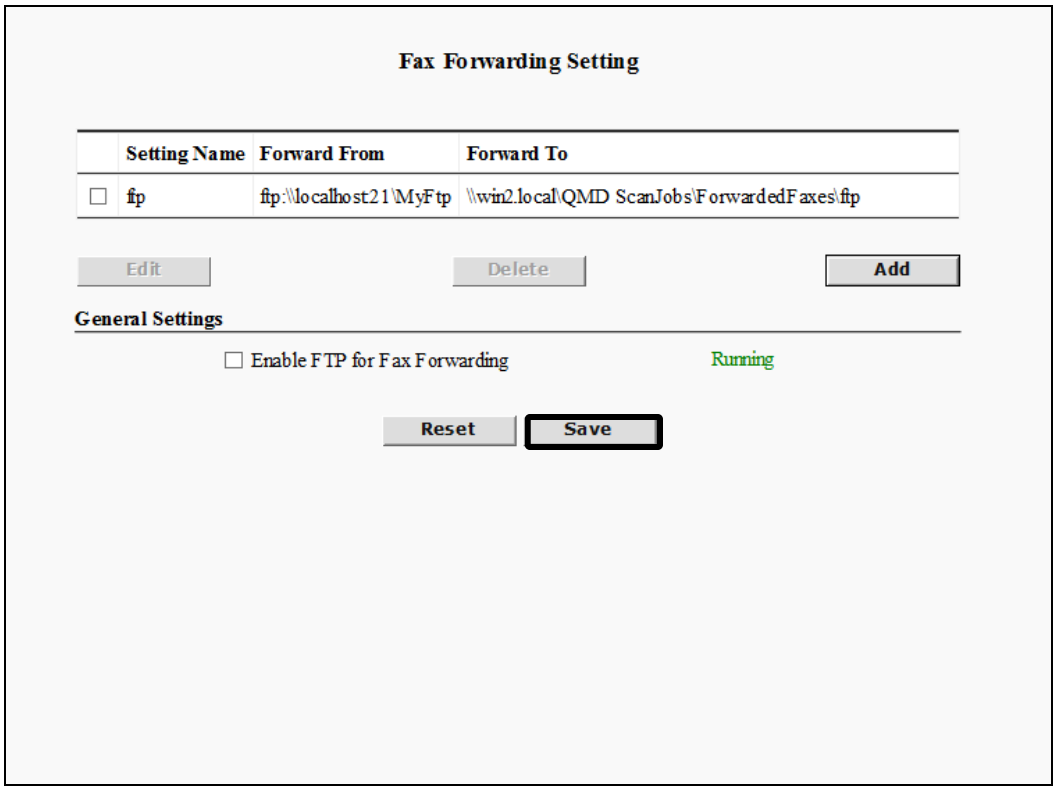
2.2 If you will be using Advanced Box forwarding, de-select the [Enable FTP for Fax Forwarding] check box. No other fields display in the <General Settings> section.



NOTE

If you use FTP forwarding, you must enable the [Enable FTP for Fax Forwarding] check box. Do not disable this check box unless you will be using Advanced Box exclusively. Running the FTP server when using Advanced Box for Fax Forwarding has no effect.

3. Click [Save].



If you disabled the FTP server, the server status should indicate it has stopped. If you enabled the FTP server, the server status should indicate it is running.

If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

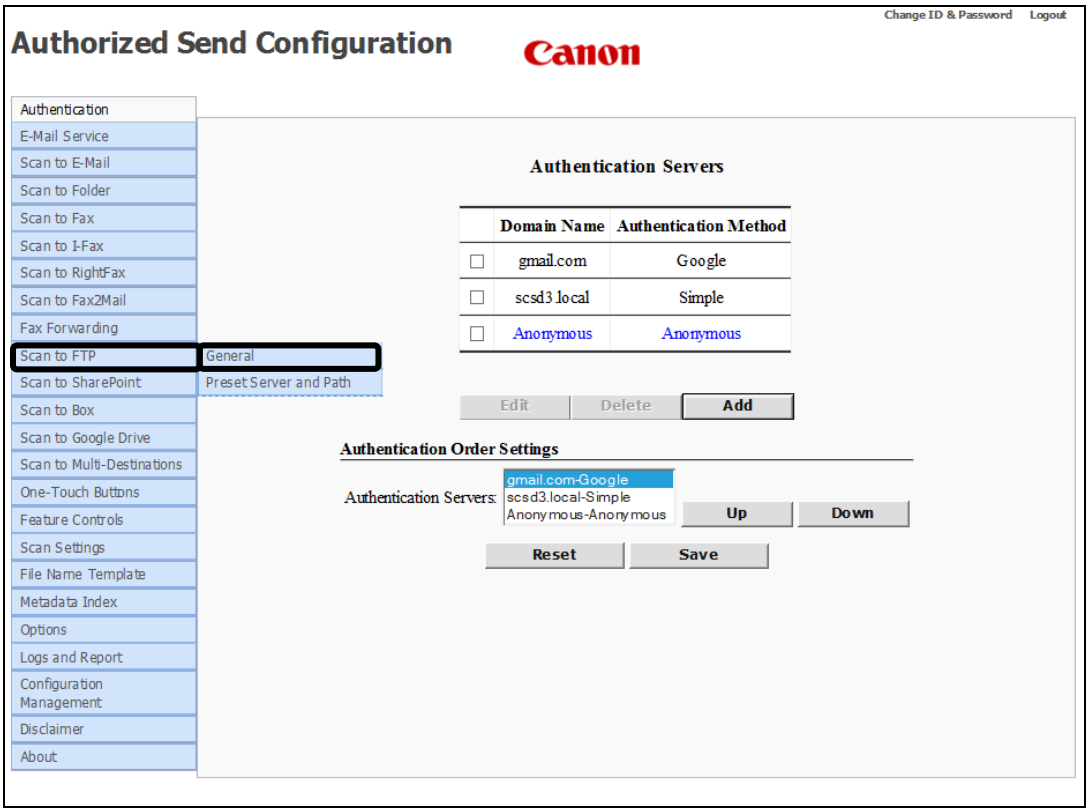
2.13 Configuring the Scan to FTP Settings

You can configure the Scan to FTP function, which enables users to scan and send documents via an FTP server, and create FTP preset servers.

IMPORTANT

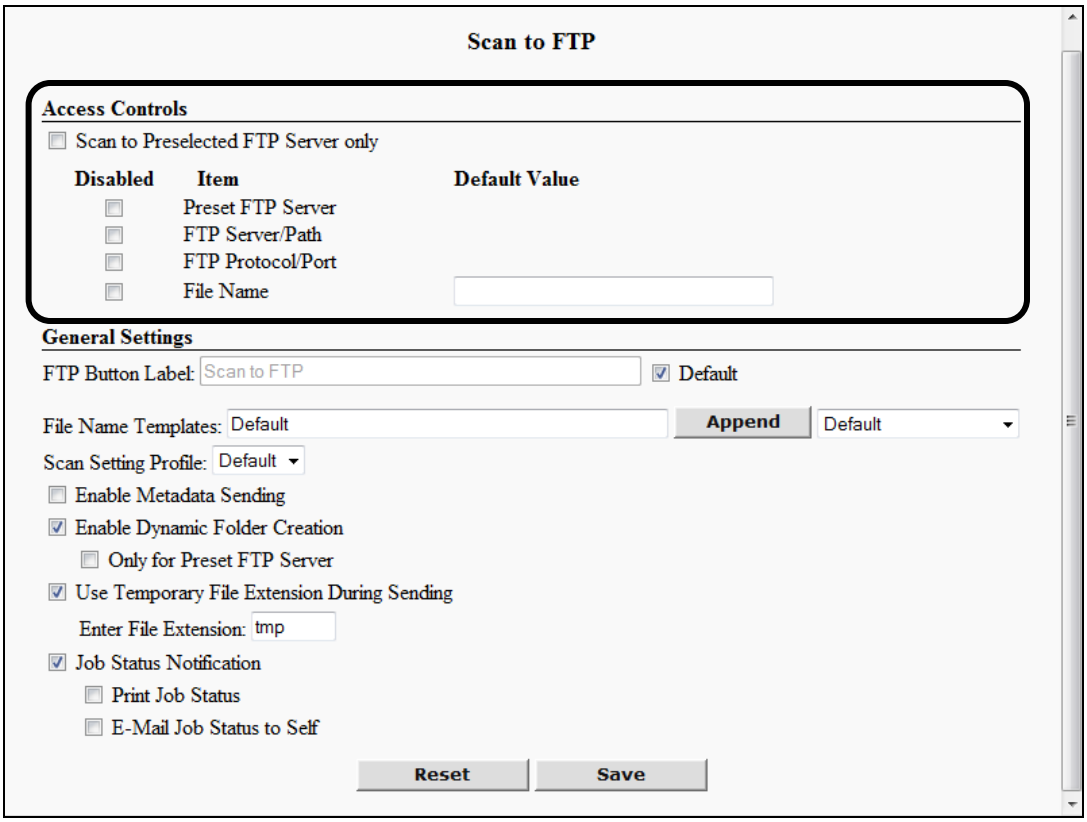
- If an AMS enabled login application is installed and running on the machine, [Scan to FTP] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the Scan to FTP function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [Scan to FTP] → [General].



The Scan to FTP screen is displayed.

2. Configure the settings under <Access Controls>.



Access Controls

Scan to Preselected FTP Server only:	Select this check box if you want to automatically disable the Preset FTP Server, FTP Server/Path, and FTP Protocol/Port check boxes with one click.

Disabled Item Column

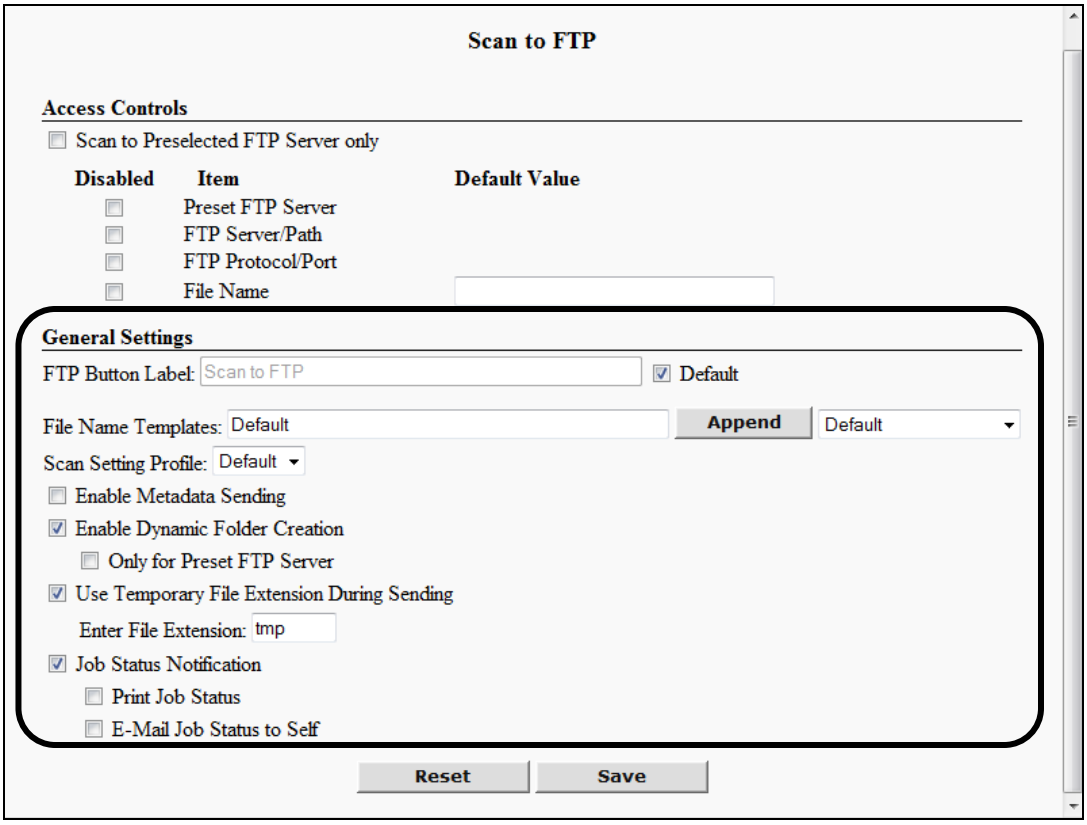
Preset FTP Server:	Select this check box if you want to prevent the user from selecting a preset share from the Preset Servers drop-down list on the Authorized Send SCAN TO FTP screen on the machine. If you select this check box, the Preset Servers drop-down list is disabled and grayed out.
FTP Server/Path:	Select this check box if you want to disable and gray out the FTP Server and Folder Path text boxes on the Authorized Send SCAN TO FTP screen on the machine.
FTP Protocol/Port:	Select this check box if you want to disable and gray out the Port text box and By drop-down list on the Authorized Send SCAN TO FTP screen on the machine.

File Name: Select this check box if you want to prevent the user from using the File Name text box on the Authorized Send SCAN TO FTP screen on the machine. If you select this check box, the File Name text box is disabled and grayed out.

Default Value Column

File Name: Enter the default file name to be displayed in the [File Name] text box on the Authorized Send SCAN TO FTP screen on the machine. This text box is optional. You can enter a string that consists of any character, and a maximum of 251 characters.

3. Configure the settings under <General Settings>.



General Settings

FTP Button Label: Enter the label for the [Scan to FTP] key that appears on the Authorized Send MAIN screen on the machine. It is a required text box that cannot be left blank. The number of any characters permitted is restricted by the width of the Scan to FTP icon.

Default: Select this check box if you want to use the default FTP Button Label setting ('Scan to FTP'). The FTP Button Label text box cannot be changed when the Default check box is selected.

File Name Templates: Enter one or more File Name Templates which the user can select when creating a scan job. The names in this list are created under the <File Name> tab. See "Configuring the File Name," on p. 407. The default value is 'Default'. Separate entries must be separated by commas. You can enter the File Name Templates manually or select the Templates from the Append drop-down list and click [Append].

Append:	Click [Append] to add a File Name Template (set in the Append drop-down list) to the string in the [File Name Templates] text box.
Append drop-down:	Select a pre-defined File Name Template that is added to the string in the [File Name Templates] text box after you click [Append].
Enable Metadata Sending:	Select this check box if you want all scans sent via the Scan to FTP function to be accompanied by an XML file, which contains metadata as defined on the Metadata Index screen. This check box is not selected by default.
Enable Dynamic Folder Creation:	Select this check box to automatically create any folders in the share path that may not exist when a user scans a document. If this check box is not selected and the user tries to scan to a folder that does not exist, an error message is displayed, and the folder is not created. This check box is selected by default.
Only for Preset FTP Server:	The [Only for Preset Shares] check box is displayed only if the [Enable Dynamic Folder Creation] check box is selected. Select this check box to enable a user to scan to a non-pre-existing folder only if the target FTP server is a preset FTP server. In this case, the folder is dynamically created. If a user enters a folder path that does not exist and the target FTP server is not a preset FTP server, an error message is displayed and the share is not created. If this check box is not selected, a user can scan to any folder on the target FTP server that does not exist, and the folder is automatically created. This check box is selected by default.
Use Temporary File Extension During Sending:	Select this check box to configure a temporary file extension that is used only during the sending process. Once sending is complete, the temporary file extension is automatically replaced with the appropriate extension of the file type that was sent (PDF, PDF(Compct), PDF(OCR), TIFF, TIFF(Single), JPEG, XPS, XPS(Compct), XPS(OCR), PPT, PPT(OCR), or WORD).

Enter File Extension:	The [Enter File Extension] text box is displayed only if the [Use Temporary File Extension During Sending] check box is selected. Enter the file extension to use when you send a document to a folder. You can enter a maximum of four alphanumeric characters. The default setting is ‘tmp’.

NOTE

- Only alphanumeric characters can be used.
- Validation is performed after you click [Save] to make sure that:
  - The [Enter File Extension] text box is not empty.
  - The maximum of four alphanumeric characters has not been exceeded.
- If validation fails, an error message is displayed.

Job Status Notification:	Select this check box if you want the logged on user of the Scan to FTP session to receive confirmation printout or email.
Print Job Status:	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to FTP session to receive a confirmation printout.
E-Mail Job Status to Self:	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to FTP session to receive a confirmation email.

4. Click [Save].

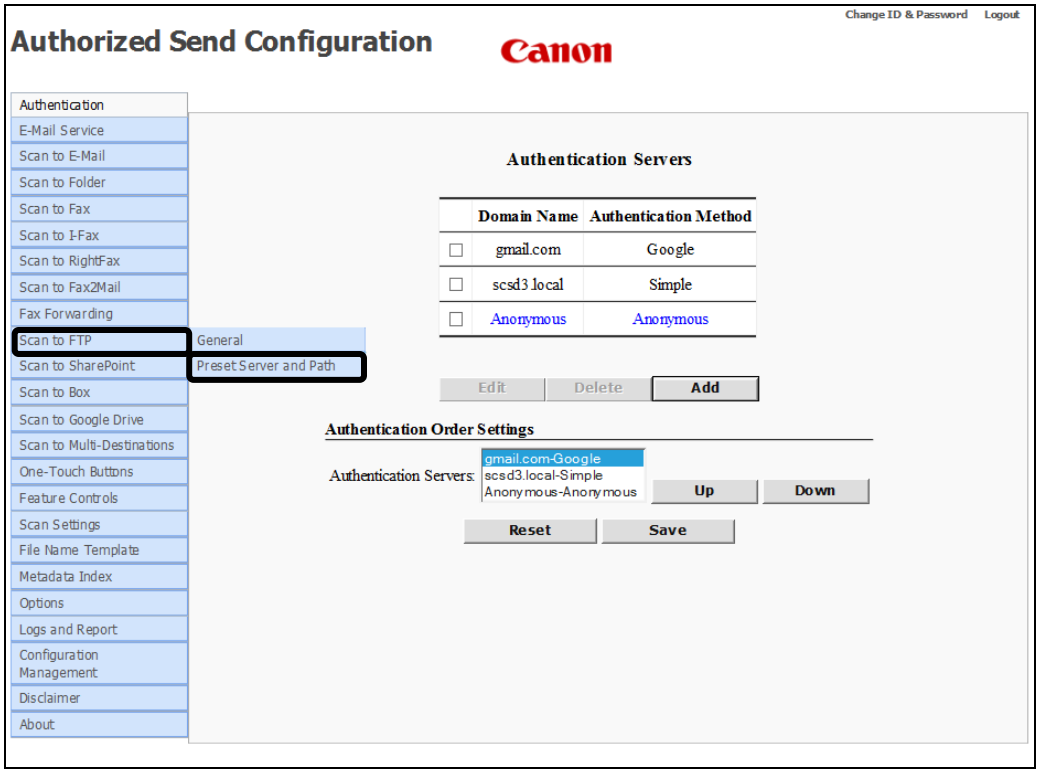
NOTE

If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.13.1 Creating an FTP Preset Server

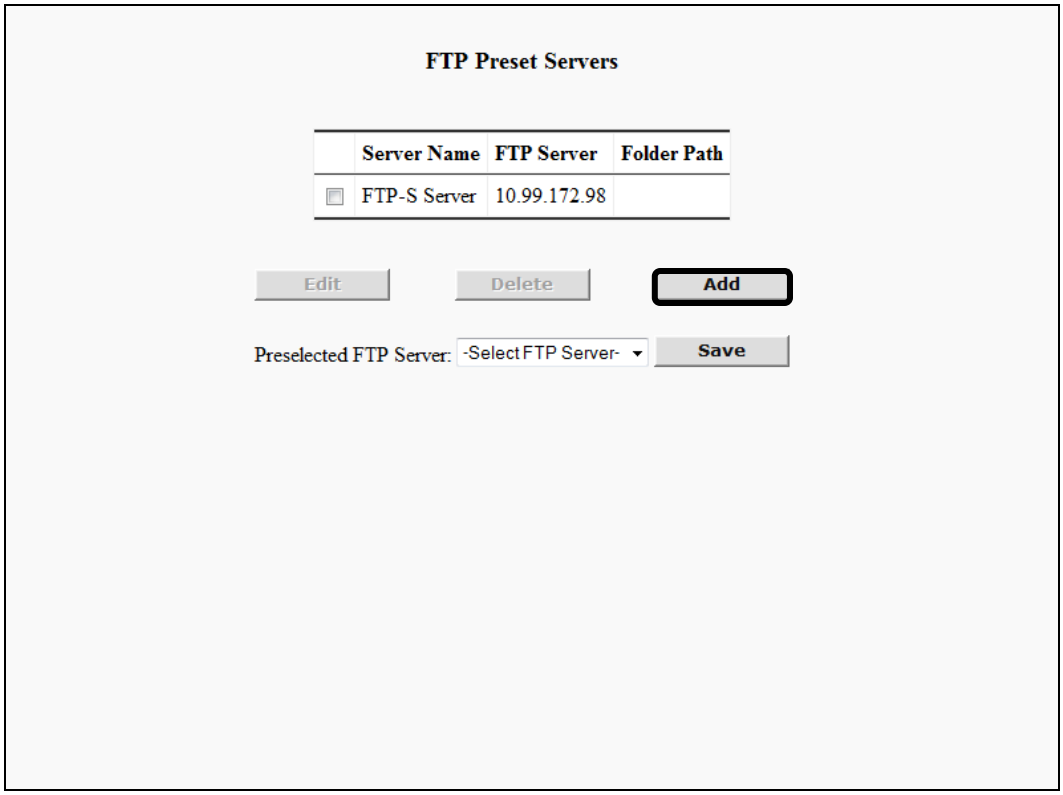
You can create any number of FTP preset servers.

1. Click [Scan to FTP] → [Preset Server and Path].



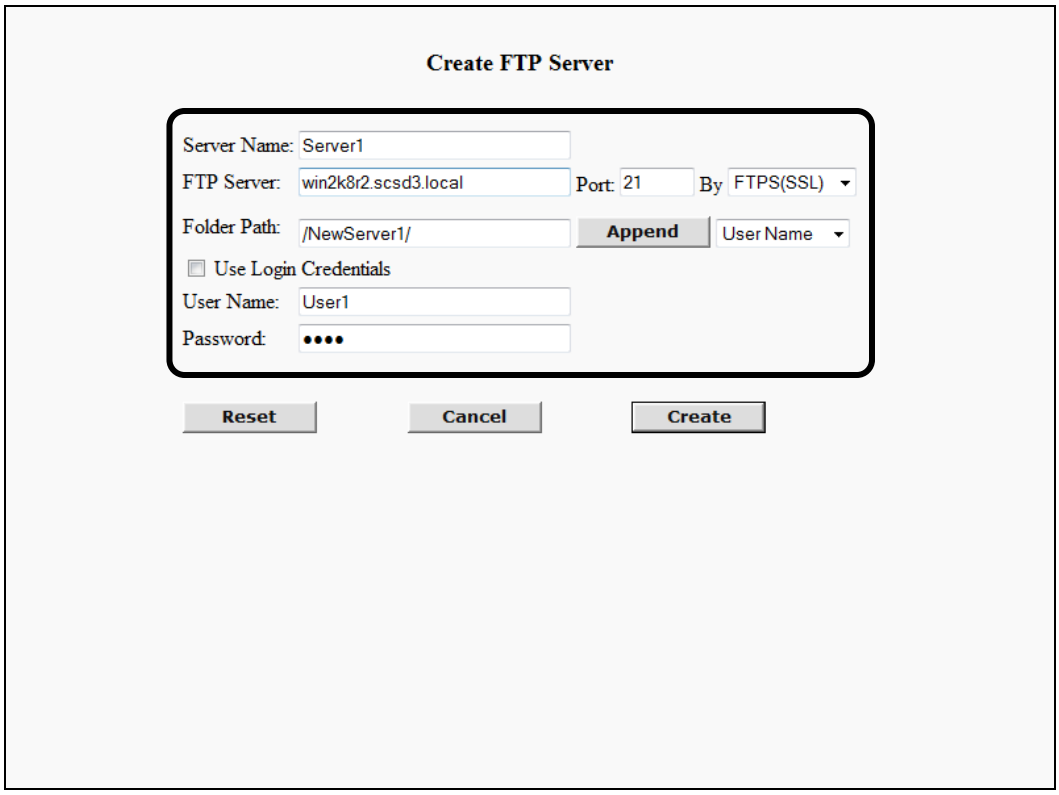
The FTP Preset Servers screen is displayed.

2. Click [Add].



The Create FTP Server screen is displayed.

3. Configure the FTP Server settings.



Server Name:	Enter a name for the server. This name is added to the Preset Server drop-down list on the Authorized Send SCAN TO FTP screen on the machine. The Server Name is case-sensitive. You can enter a string that consists of any character, and a maximum of 31 characters.
FTP Server:	Enter the DNS name or IP address to send scanned documents. You can enter a string that consists of any character, and an unlimited number of characters.
Port:	Enter the connecting port number of the FTP server. You can enter a maximum of five numbers, ranging only from 0 to 65535. The default port number is ‘21’.
by:	From is drop-down list, select [FTP], [SFTP(SSH)], or [FTPS(SSL)] as the protocol to use. If you select [FTP] or [FTPS(SSL)], the port number automatically changes to ‘21’. If you select [SFTP(SSH)], the port number automatically changes to ‘22’. The default setting is ‘FTP’.

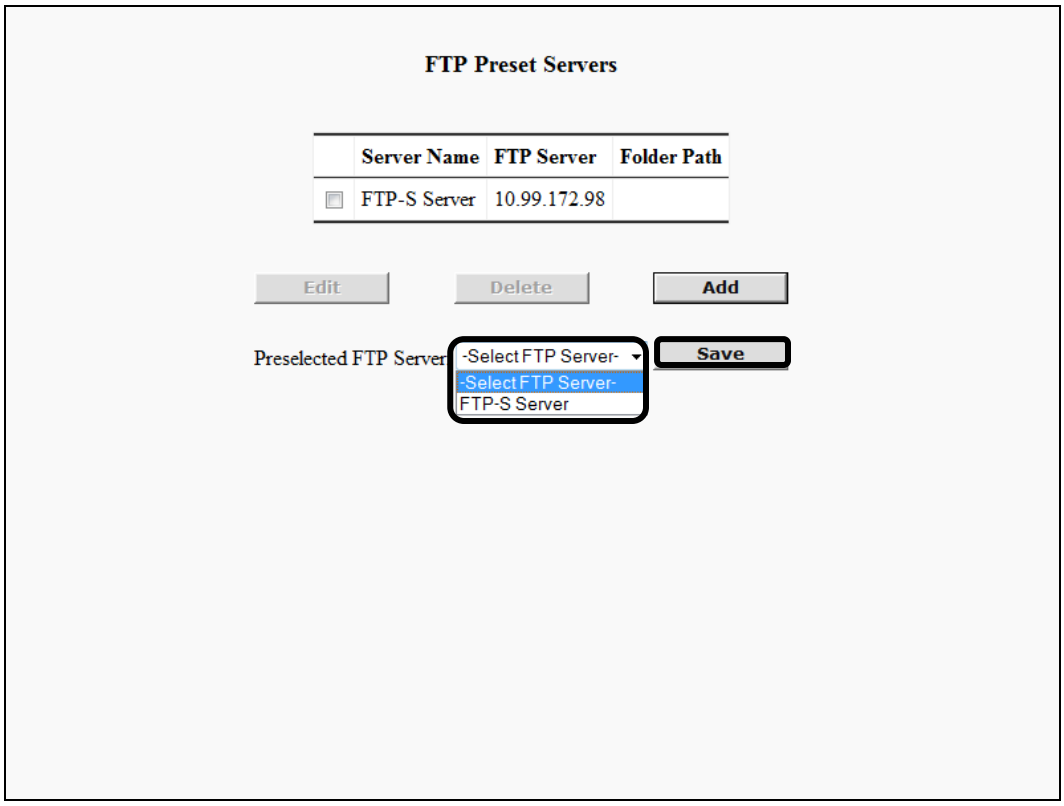
Folder Path:	Enter the path of the folder to send scanned documents. You can enter a string that consists of any character, and an unlimited number of characters.
Append:	Click [Append] to add a dynamic variable (set in the Append drop-down list) to the string in the [Folder Path] text box.
Append drop-down:	Select a dynamic variable that is added to the string in the [Folder Path] text box after you click [Append]. The default value is 'User Name'.
Use Login Credential:	Select this check box to disable and hide the [User Name] and [Password] text boxes. If you do not select the [Use Login Credential] check box, the FTP server uses the login credentials that were used to start the scanning session.
User Name:	This text box is displayed only if the [Use Login Credential] check box is not selected. Enter the user name to use to log on to the FTP server in the [User Name] text box. You can enter a string that consists of any character, and a maximum of 255 characters.
Password:	This text box is displayed only if the [Use Login Credential] check box is not selected. Enter the password to use to log on to the FTP server in the [Password] text box. You can enter a string that consists of any character, and a maximum of 255 characters.

4. Click [Create].

   If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

   To cancel creating the preset share and return to the FTP Preset Servers configuration screen, click [Cancel].

5. If you want to specify a server name that automatically populates the value in the Preset Server drop-down list on the Authorized Send SCAN TO FTP screen on the machine, select a server name from the Preselected FTP Server drop-down list → click [Save].



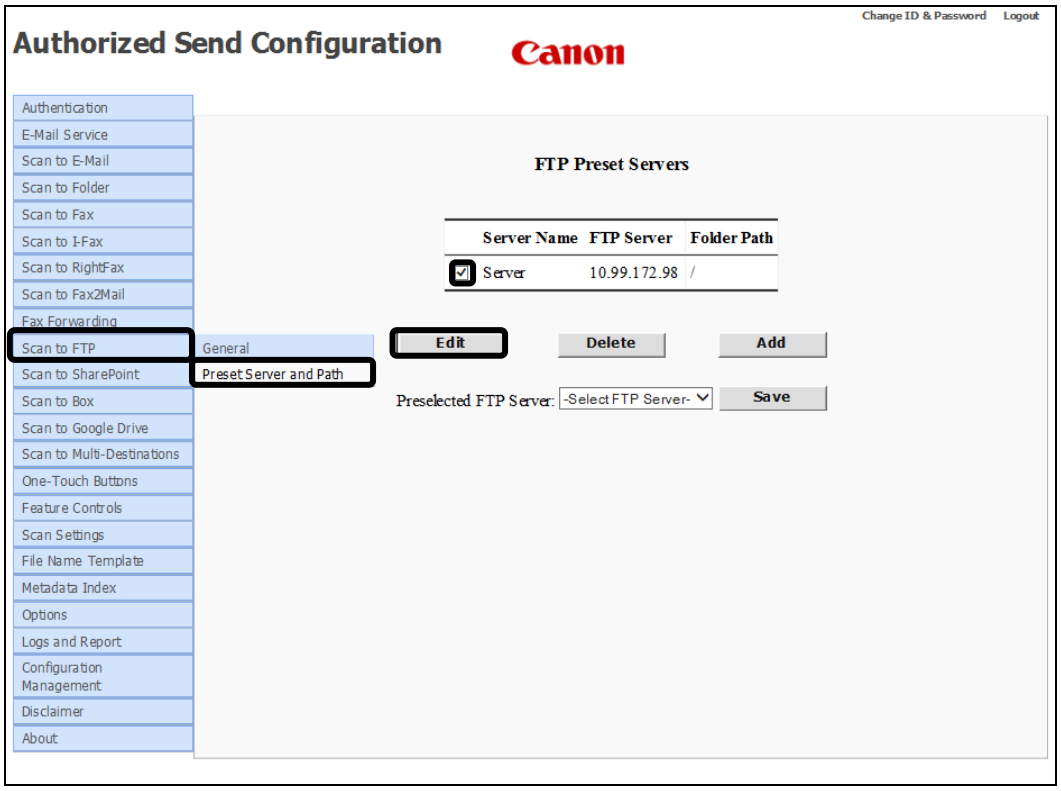
NOTE

- The default setting is 'Select FTP Server'
- 'Select FTP Server' appears automatically in the Preset Server drop-down list on the Authorized Send SCAN TO FTP screen on the machine.
- If the preselected FTP server you selected is deleted, 'Select FTP Server' is displayed in the Preset Server drop-down list on the Authorized Send SCAN TO FTP screen on the machine.

2.13.2 Editing an FTP Preset Server

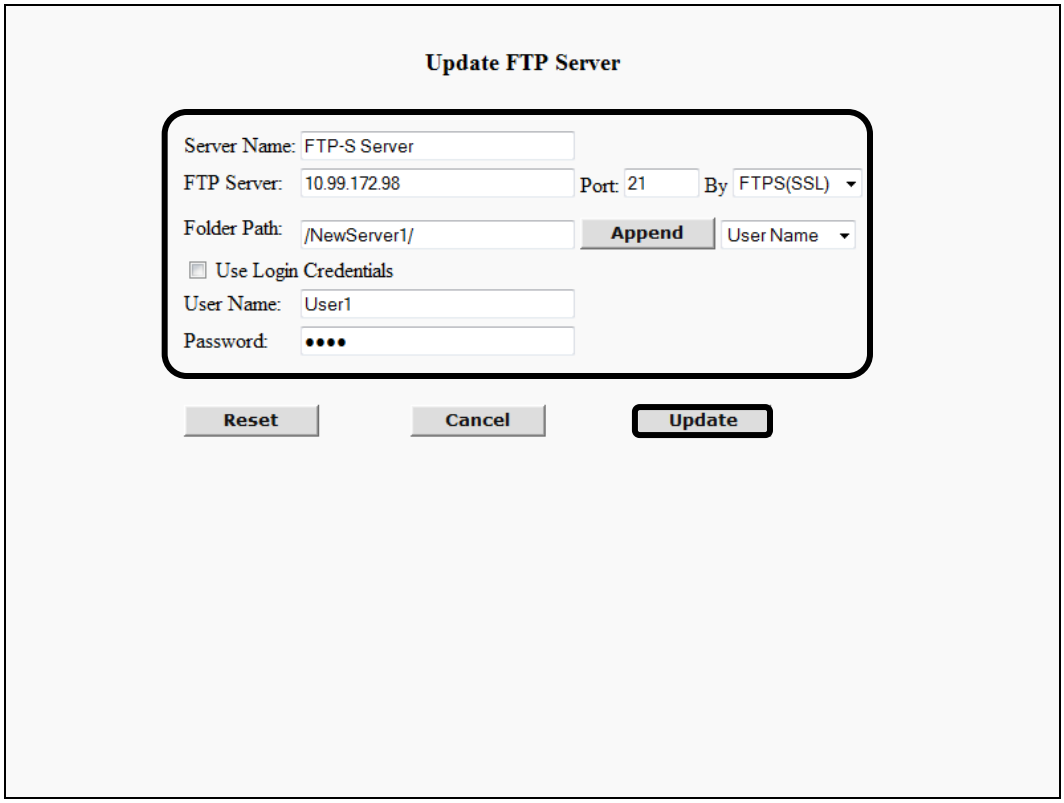
You can edit a previously created FTP preset server from the FTP Preset Servers configuration screen.

1. Click [Scan to FTP] → [Preset Server and Path] → select the check box next to the FTP preset server you want to edit → click [Edit].



The Update FTP Server screen is displayed.

2. Edit the settings for the FTP preset server, as necessary → click [Update].



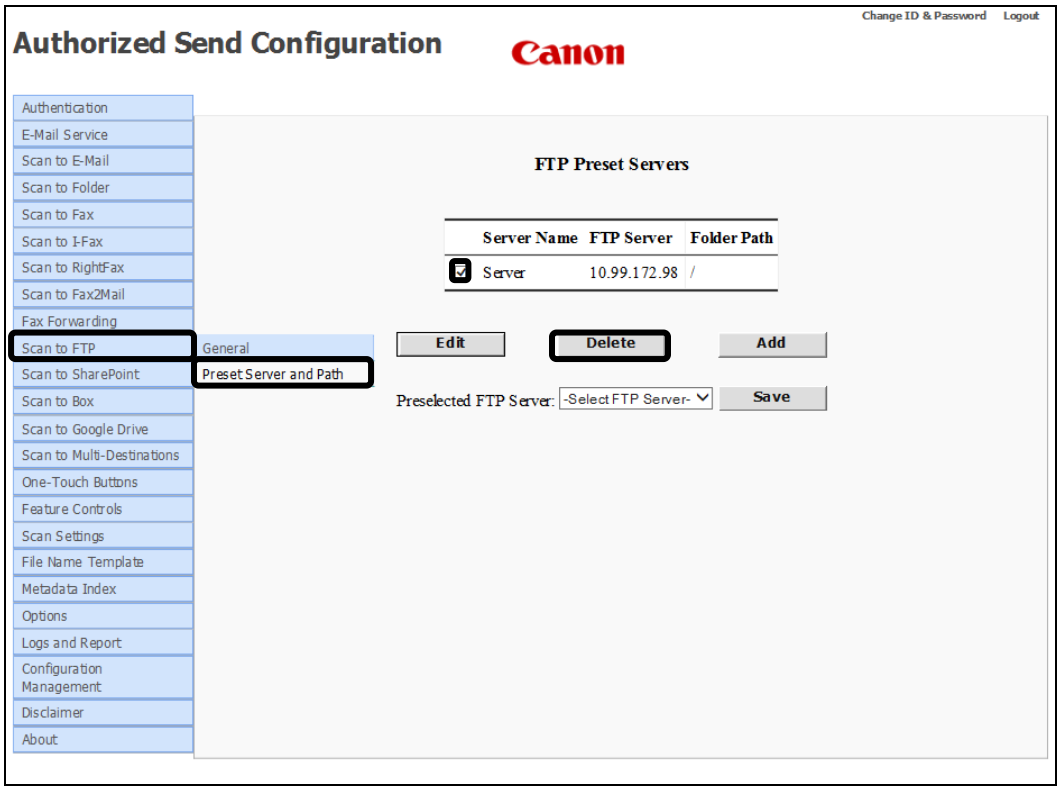
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the FTP preset server and return to the FTP Preset Servers configuration screen, click [Cancel].

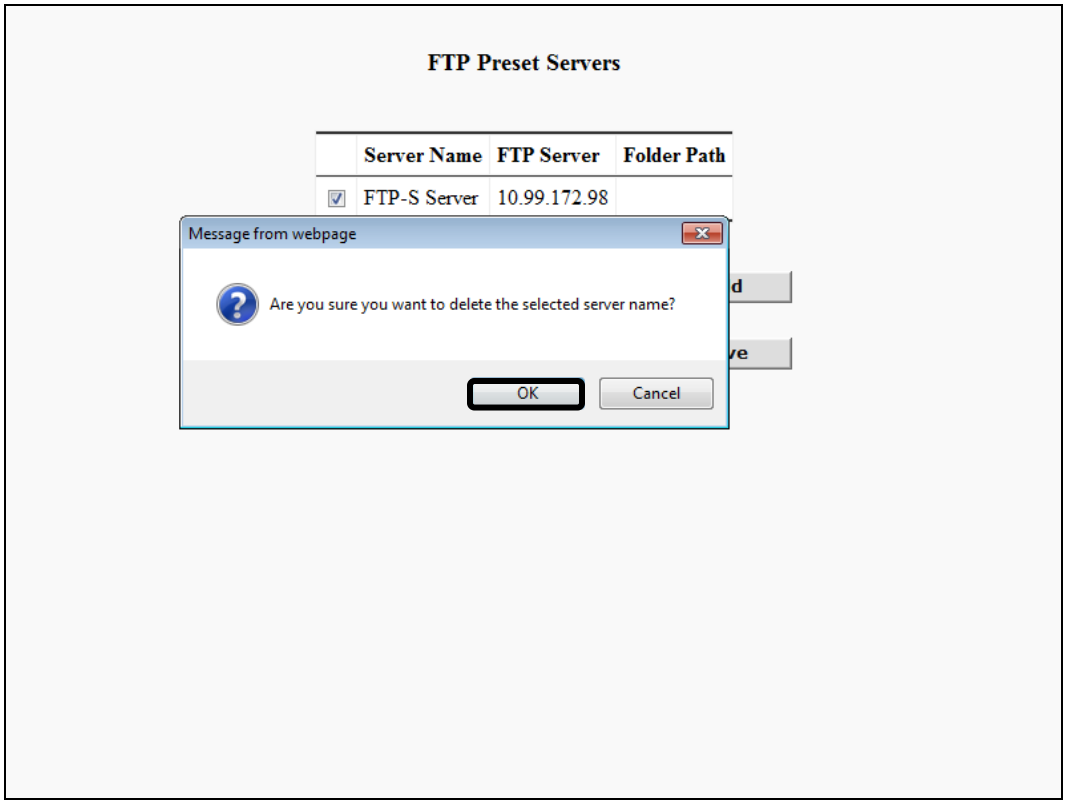
2.13.3 Deleting an FTP Preset Server

You can delete a previously created FTP preset server from the FTP Preset Servers configuration screen.

1. Click [Scan to FTP] ➞ [Preset Server and Path] ➞ select the check box next to the FTP preset server you want to delete ➞ click [Delete].



2. Click [OK] on the confirmation dialog box.



If you do not want to delete the FTP preset server, click [Cancel].

The FTP preset server is deleted from the list.

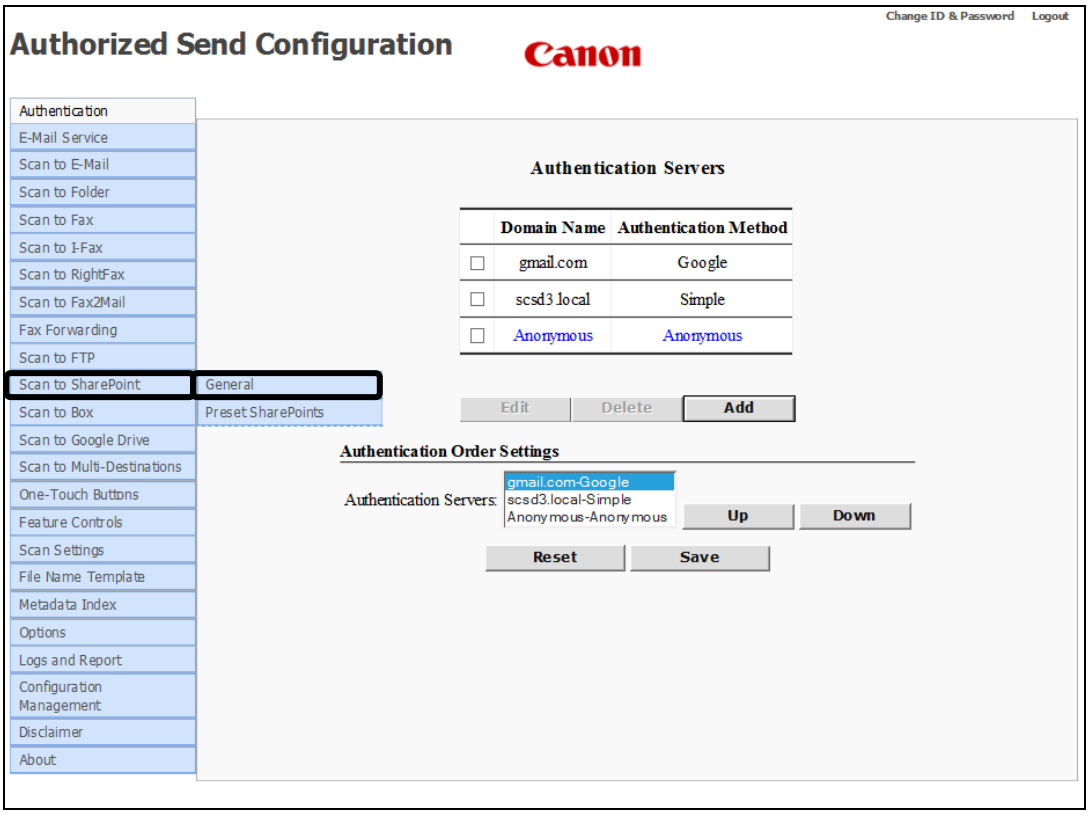
2.14 Configuring the Scan to SharePoint Settings

You can configure the Scan to SharePoint function, which enables users to scan and send documents via a SharePoint server, and create preset SharePoint servers.

IMPORTANT

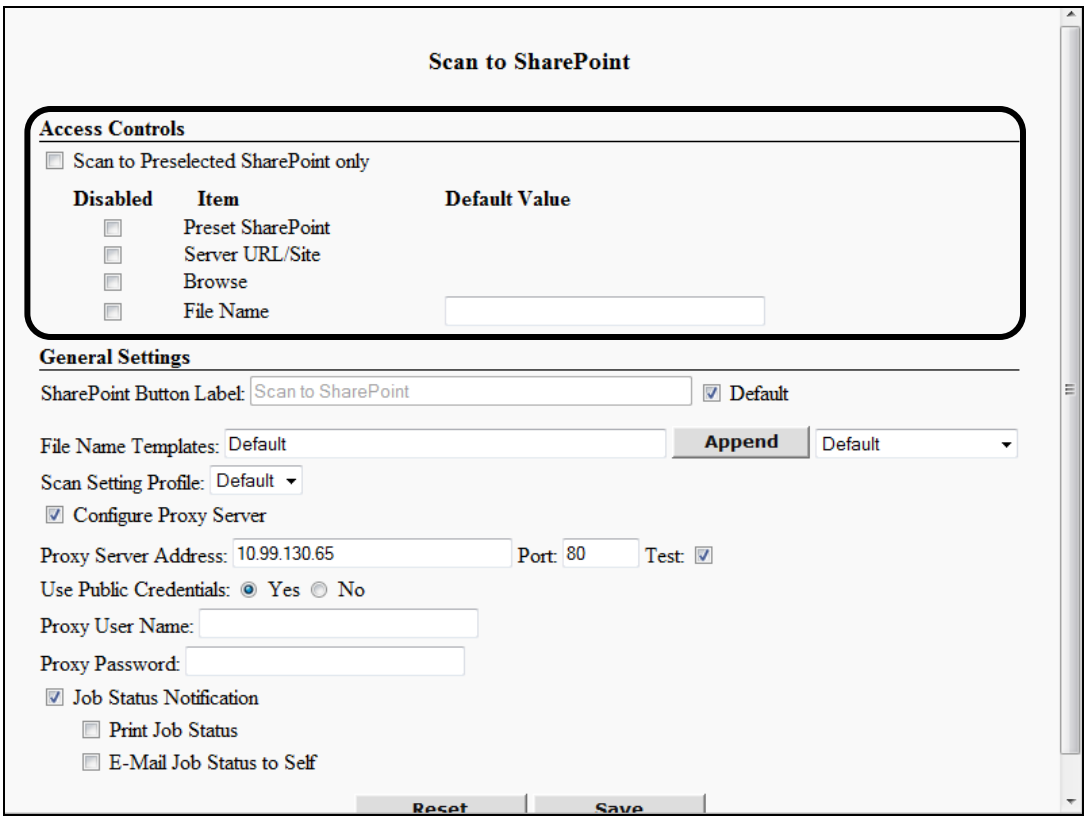
- If an AMS enabled login application is installed and running on the machine, [Scan to SharePoint] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the Scan to SharePoint function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [Scan to SharePoint] → [General].



The Scan to SharePoint screen is displayed.

2. Configure the settings under <Access Controls>.



Access Controls

Scan to Preselected SharePoint only:	Select this check box if you want to automatically disable the [Preset SharePoint] and [Browse] check boxes with one click.

Disabled Item Column

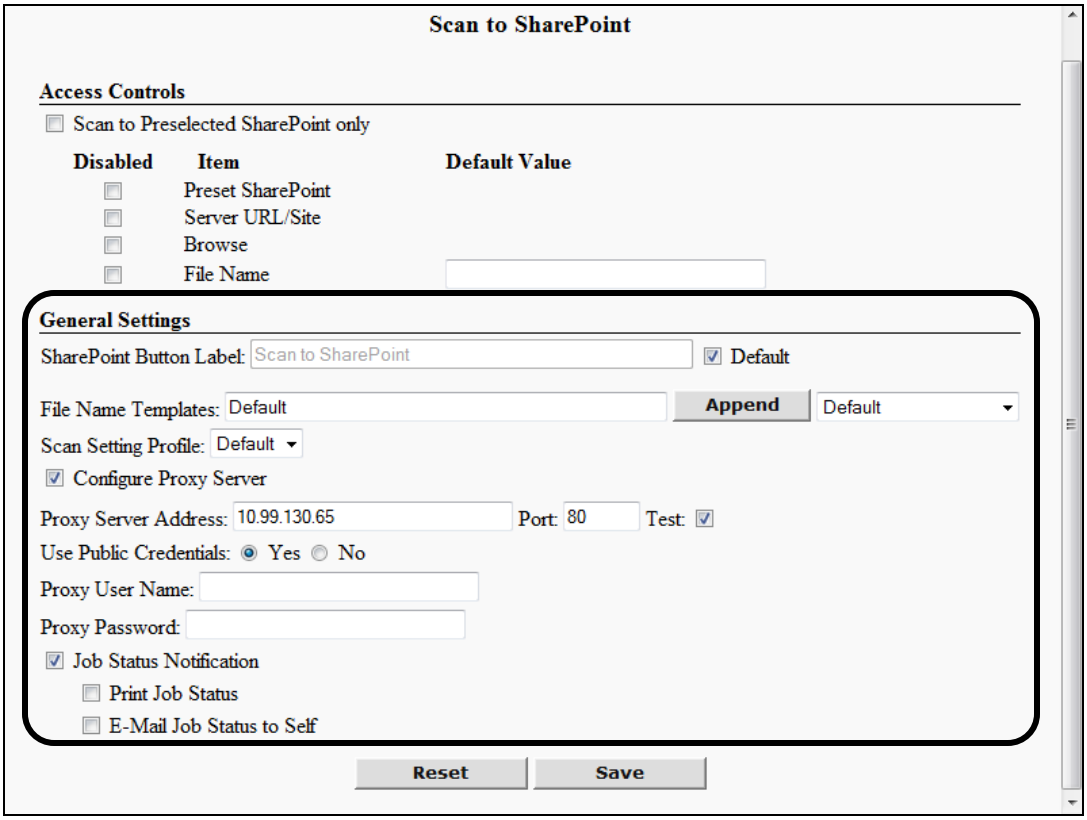
Preset SharePoint:	The [Preset SharePoint] check box is displayed only if the [Scan to Preselected SharePoint only] check box is not selected. Select this check box if you want to prevent the user from selecting a preset URL from the Preset URL drop-down list on the Authorized Send SCAN TO SHAREPOINT screen on the machine. If you select this check box, the Preset URL drop-down list is disabled and grayed out.
Server URL/Site:	Select this check box if you want to disable and gray out the Server URL text box on the Authorized Send SCAN TO SHAREPOINT screen on the machine.

Browse:	The [Browse] check box is displayed only if the [Scan to Preselected SharePoint only] check box is not selected. Select this check box if you want to disable and hide the [Browse] key on the Authorized Send SCAN TO SHAREPOINT screen on the machine.
File Name:	Select this check box if you want to prevent the user from using the [File Name] text box on the Authorized Send SCAN TO SHAREPOINT screen on the machine. If you select this check box, the [File Name] text box is disabled and grayed out.

Default Value Column

File Name:	Enter the default file name to be displayed in the [File Name] text box on the Authorized Send SCAN TO SHAREPOINT screen on the machine. This text box is optional. You can enter a string that consists of any character, and a maximum of 251 characters.

3. Configure the settings under <General Settings>.



General Settings

SharePoint Button Label:	Enter the label for the [Scan to SharePoint] key that appears on the Authorized Send MAIN screen on the machine. It is a required text box that cannot be left blank. The number of any characters permitted is restricted by the width of the Scan to SharePoint icon.
Default	Select this check box if you want to use the default SharePoint Button Label setting (‘Scan to SharePoint’). The SharePoint Button Label text box cannot be changed when the Default check box is selected.
File Name Templates:	Enter one or more File Name Templates which the user can select when creating a scan job. The names in this list are created under the <File Name> tab. See “Configuring the File Name,” on p. 407. The default value is ‘Default’. Separate entries must be separated by commas. You can enter the File Name Templates manually or select the Templates from the Append drop-down list and click [Append].

Append:	Click [Append] to add a File Name Template (set in the Append drop-down list) to the string in the [File Name Templates] text box.
Append drop-down:	Select a pre-defined File Name Template that is added to the string in the [File Name Templates] text box after you click [Append].
Scan Setting Profile:	Select a scan setting profile from the drop-down list. The default setting is ‘Default’, which corresponds to the default settings on the Scan Settings screen.
Configure Proxy Server:	Select this check box if you want to enable the [Proxy Server], [Port], and [Text] text boxes, and the [Use Public Credentials] radio buttons. The [Configure Proxy Server] check box is not selected by default.
Proxy Server Address:	This text box is displayed only if the [Configure Proxy Server] check box is selected. Enter the DNS name of the IP address of the proxy server to be used to connect to any SharePoint server. You can enter a string that consists of any character, and an unlimited number of characters.
Port:	This text box is displayed only if the [Configure Proxy Server] check box is selected. Enter the connecting port number of the proxy server. You can enter a maximum of five numbers, ranging only from 0 to 65535. The default port number is ‘80’.
Test:	This check box is displayed only if the [Configure Proxy Server] check box is selected. Select this check box if you want to test the connection to the proxy server before you save the settings. The [Text] check box is selected by default.
Use Public Credentials:	These radio buttons are displayed only if the [Configure Proxy Server] check box is selected. Select [Yes] to configure the public credentials (Proxy User Name and Proxy Password) for proxy server authentication. If you select [No], the user’s sign-in credentials are used for proxy server authentication. The default setting is ‘No’.

Proxy User Name:	This text box is displayed only if the [Use Public Credentials] radio button is set to 'Yes'. If you select [Yes] for Use Public Credentials, you must enter the user name for proxy server authentication. You can enter a string that consists of any character, and an unlimited number of characters.
Proxy Password:	This text box is displayed only if the [Use Public Credentials] radio button is set to 'Yes'. If you select [Yes] for Use Public Credentials, you must enter the password for proxy server authentication. You can enter a string that consists of any character, and an unlimited number of characters.
Job Status Notification:	Select this check box if you want the logged on user of the Scan to SharePoint session to receive confirmation printout or email.
Print Job Status:	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to SharePoint session to receive a confirmation printout.
E-Mail Job Status to Self:	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to SharePoint session to receive a confirmation email.

4. Click [Save].

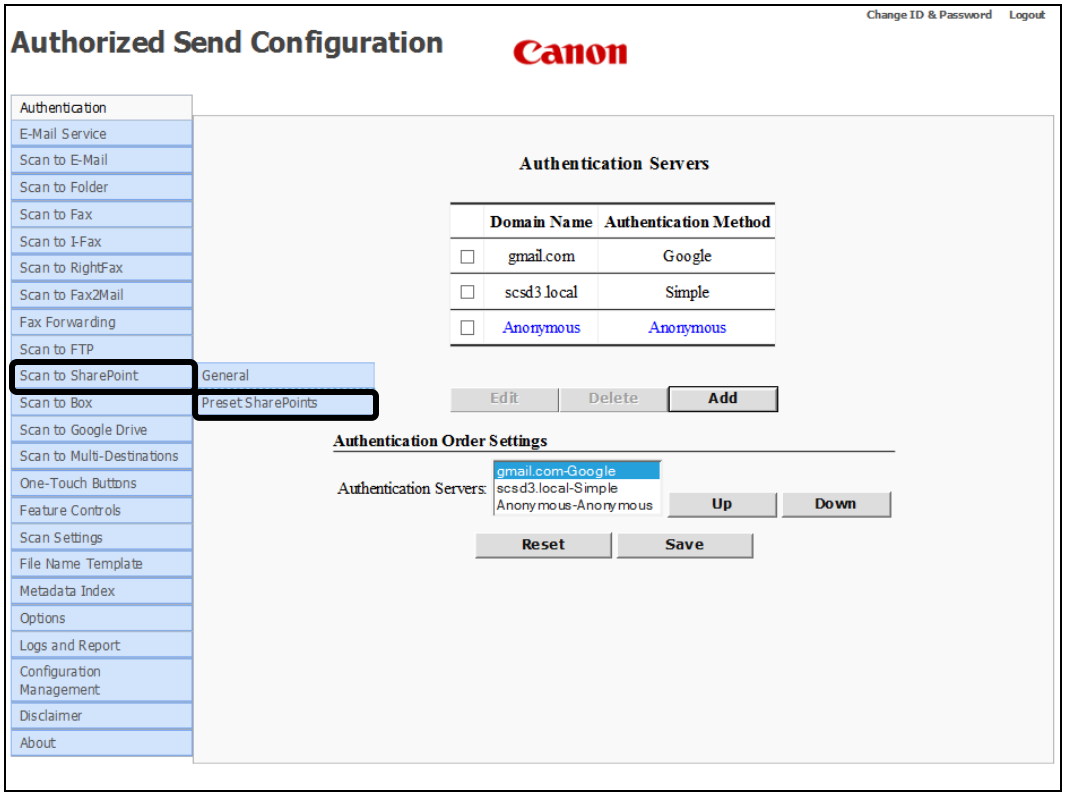
NOTE

If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.14.1 Creating a Preset SharePoint

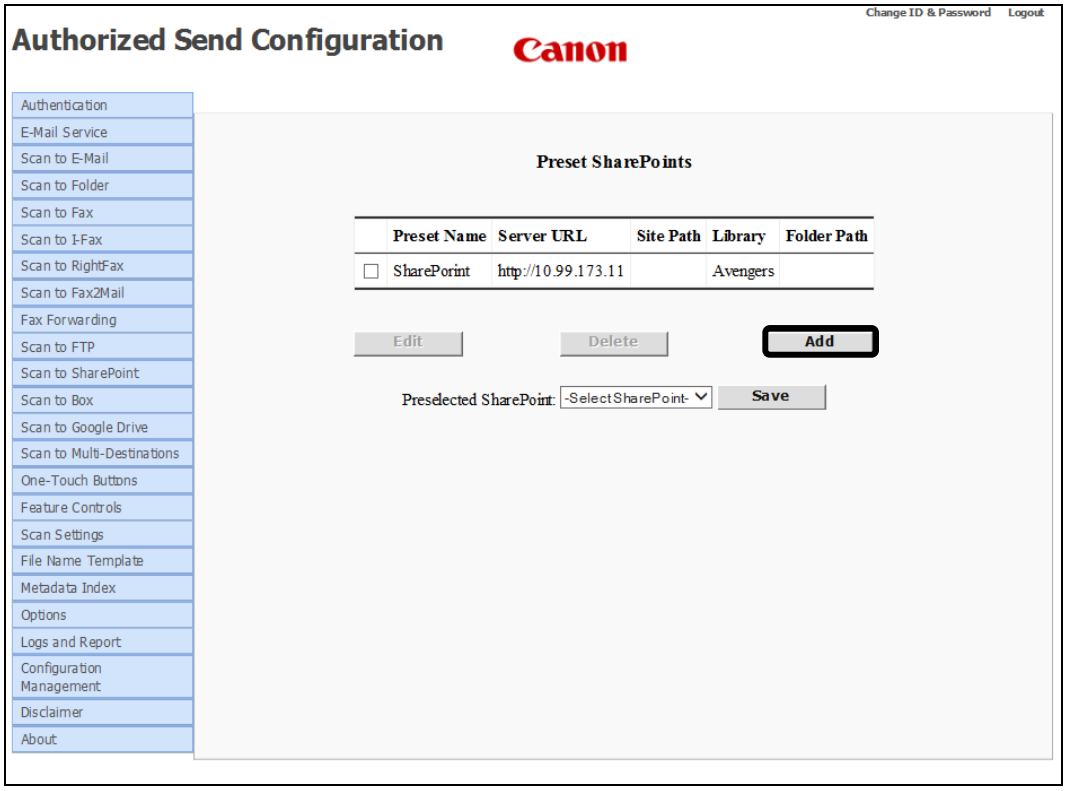
You can create any number of preset SharePoints.

1. Click [Scan to SharePoint] → [Preset SharePoints].



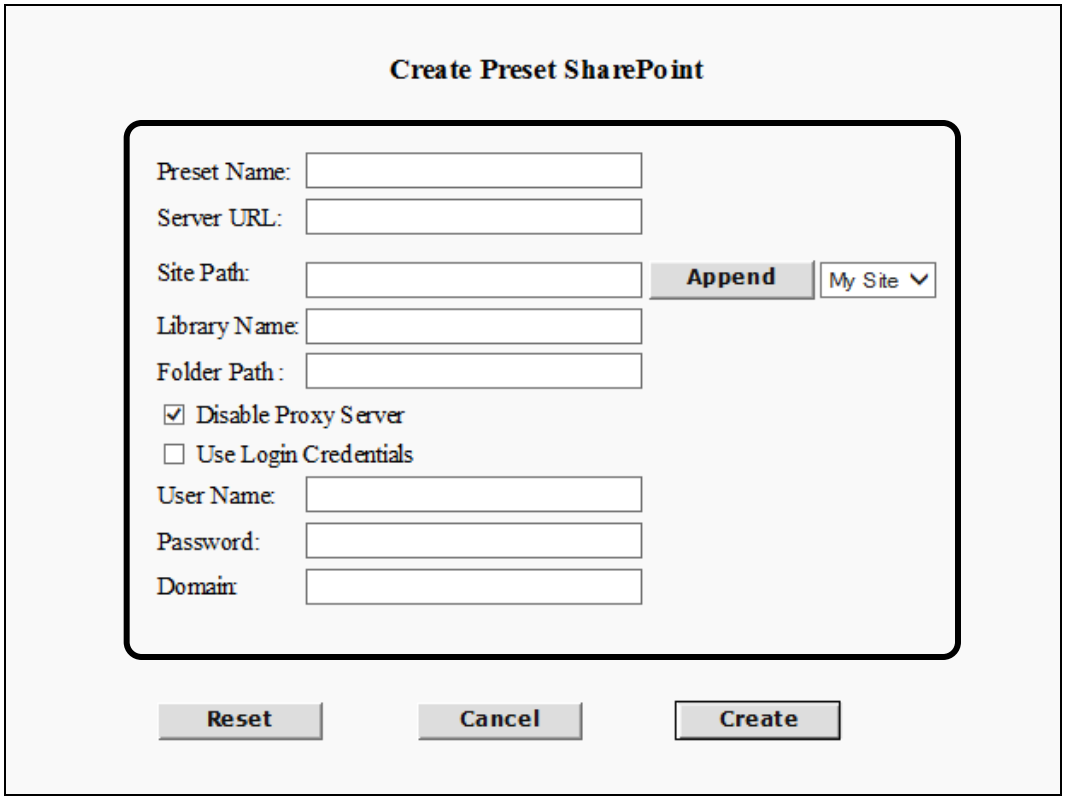
The Preset SharePoints screen is displayed.

2. Click [Add].



The Create Preset SharePoint screen is displayed.

3. Configure the Create Preset SharePoint settings.



Preset Name: Enter a name for the server. This name is added to the Preset URL drop-down list on the Authorized Send SCAN TO SHAREPOINT screen on the machine. The Preset Name is case-sensitive. You can enter a string that consists of any character, and a maximum of 31 characters.

Server URL: Enter the URL address to send scanned documents. You can enter a string that consists of any character, and an unlimited number of characters.

Site Path: Enter the path to where you want to send scanned documents. This is an optional text box. You can enter a string that consists of any character, and an unlimited number of characters.

Append: Click [Append] to add a dynamic variable (set in the Append drop-down list) to the string in the [Site Path] text box.

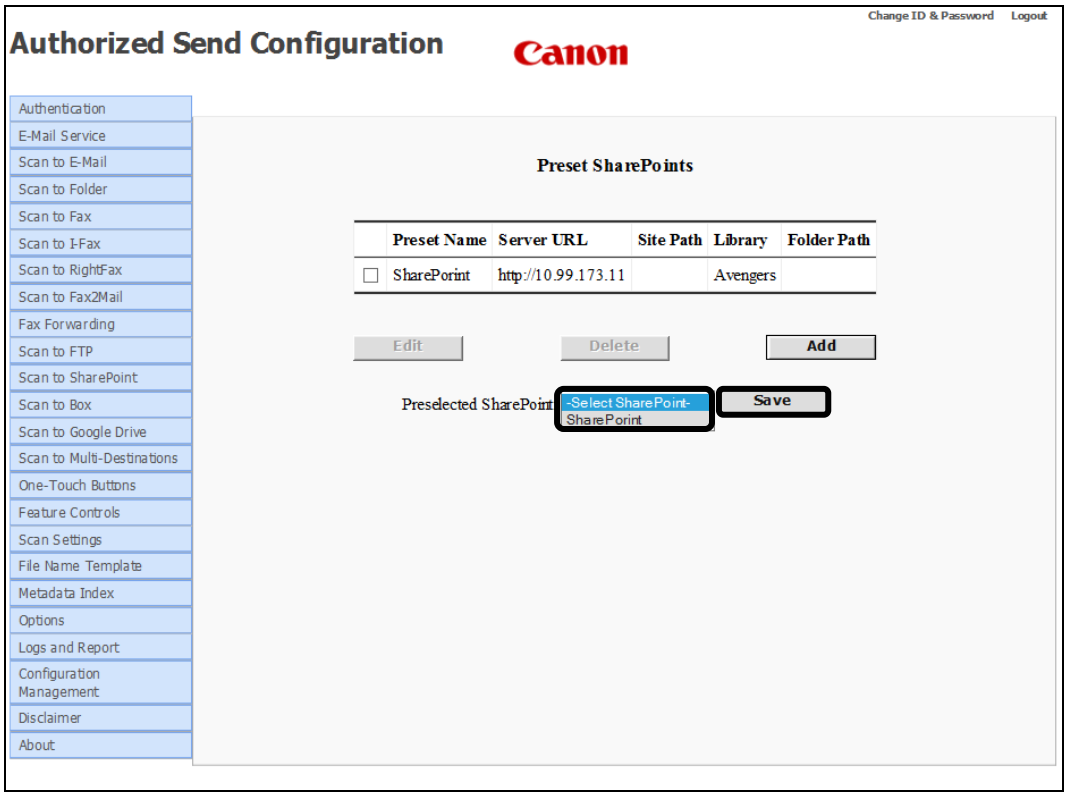
Append drop-down:	Select a dynamic variable that is added to the string in the [Site Path] text box after you click [Append]. The default value is ‘My Site’.
Library Name:	Enter the name of the library to where you want to send scanned documents. You can enter a string that consists of any character, and an unlimited number of characters.
Folder Path:	Enter the path of the folder under the library to where you want to send scanned documents. This is an optional text box. You can enter a string that consists of any character, and an unlimited number of characters.
Disable Proxy Server:	Select this check box to ignore using any proxy server set on the Scan to SharePoint configuration screen. The default is unchecked.
Use Login Credential:	Select this check box to disable and hide the [User Name]and [Password] text boxes. If you do not select the [Use Login Credential] check box, the SharePoint server uses the login credentials that were used to start the scanning session.
User Name: Password: Domain:	These text boxes are displayed only if the [Use Login Credential] check box is not selected. Enter the user name, password, and domain to use to log on to the SharePoint server in the [User Name], [Password], and [Domain] text boxes. You can enter a string that consists of any character, and a maximum of 255 characters per text box.

4. Click [Create].

   If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

   To cancel creating the preset SharePoint and return to the Preset SharePoints configuration screen, click [Cancel].

5. If you want to specify a SharePoint name that automatically populates the value in the Preset URL drop-down list on the Authorized Send SCAN TO SHAREPOINT screen on the machine, select a SharePoint name from the Preselected SharePoint drop-down list → click [Save].



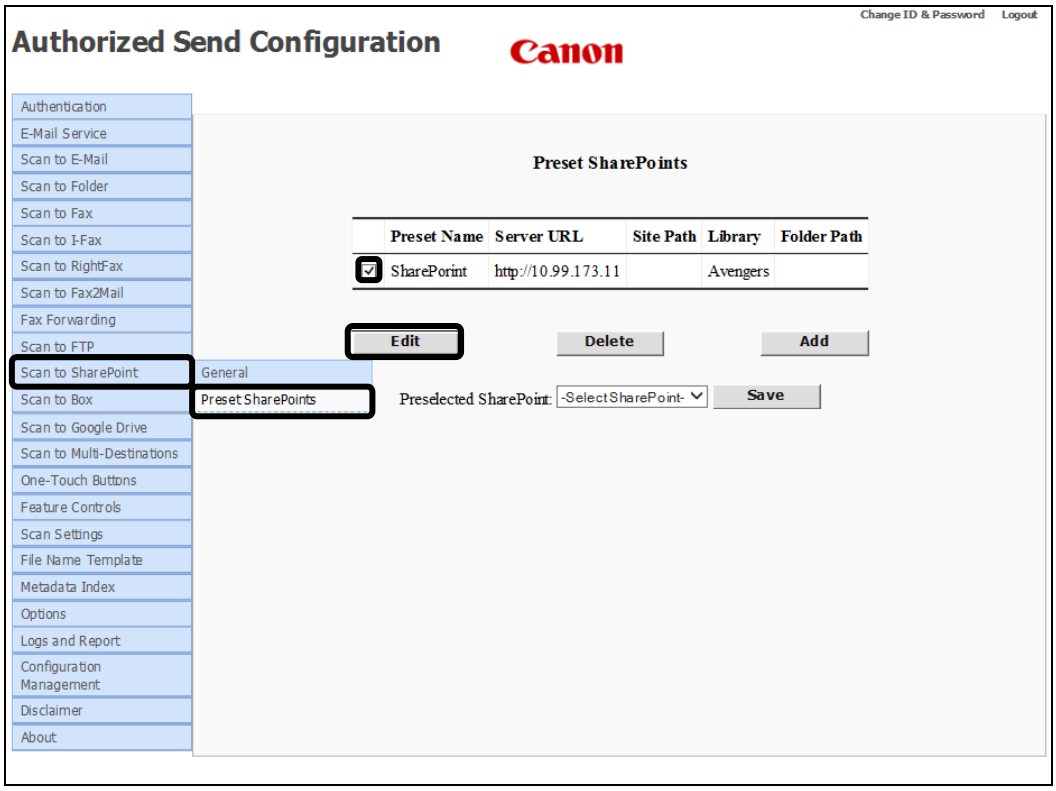
NOTE

- The default setting is 'Select SharePoint'.
- [Select SharePoint] appears automatically in the Preset URL drop-down list on the Authorized Send SCAN TO SHAREPOINT screen on the machine.
- If the preselected SharePoint you selected is deleted, [Select SharePoint] is displayed in the Preset URL drop-down list on the Authorized Send SCAN TO SHAREPOINT screen on the machine.

2.14.2 Editing a Preset SharePoint

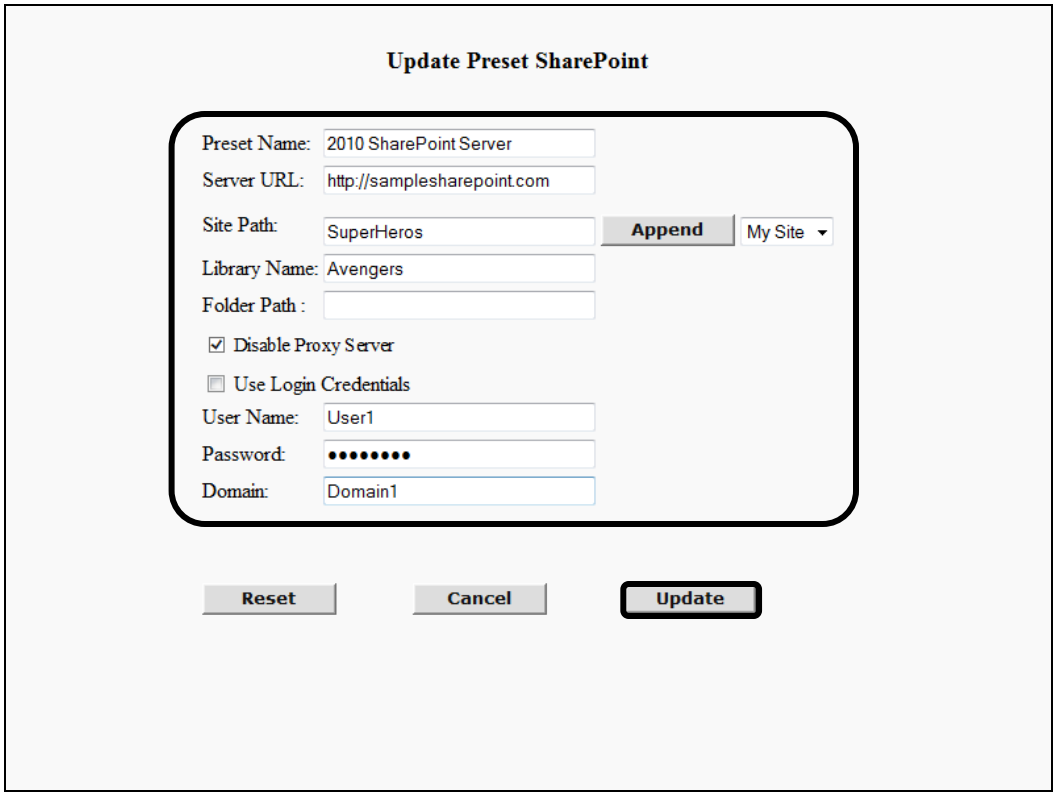
You can edit a previously created preset SharePoint from the Preset SharePoints configuration screen.

1. Click [Scan to SharePoint] → [Preset SharePoints] → select the check box next to the preset SharePoint you want to edit → click [Edit].



The Update Preset SharePoint screen is displayed.

2. Edit the settings for the preset SharePoint, as necessary → click [Update].



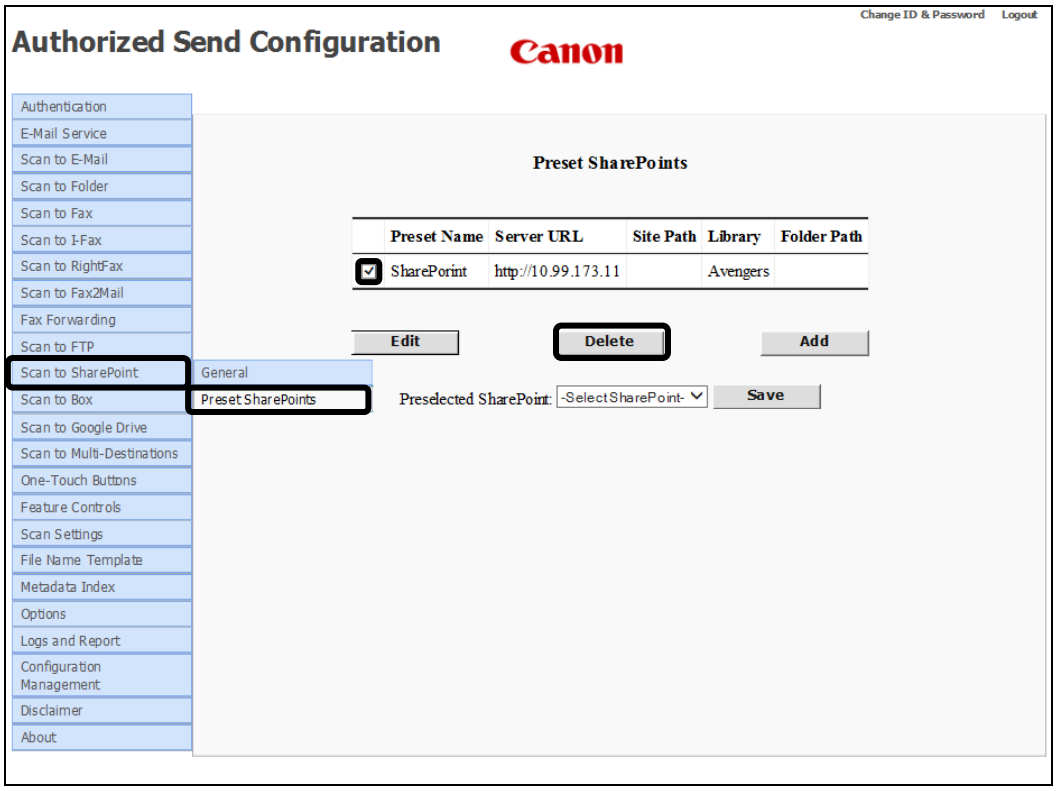
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the preset SharePoint and return to the Preset SharePoints configuration screen, click [Cancel].

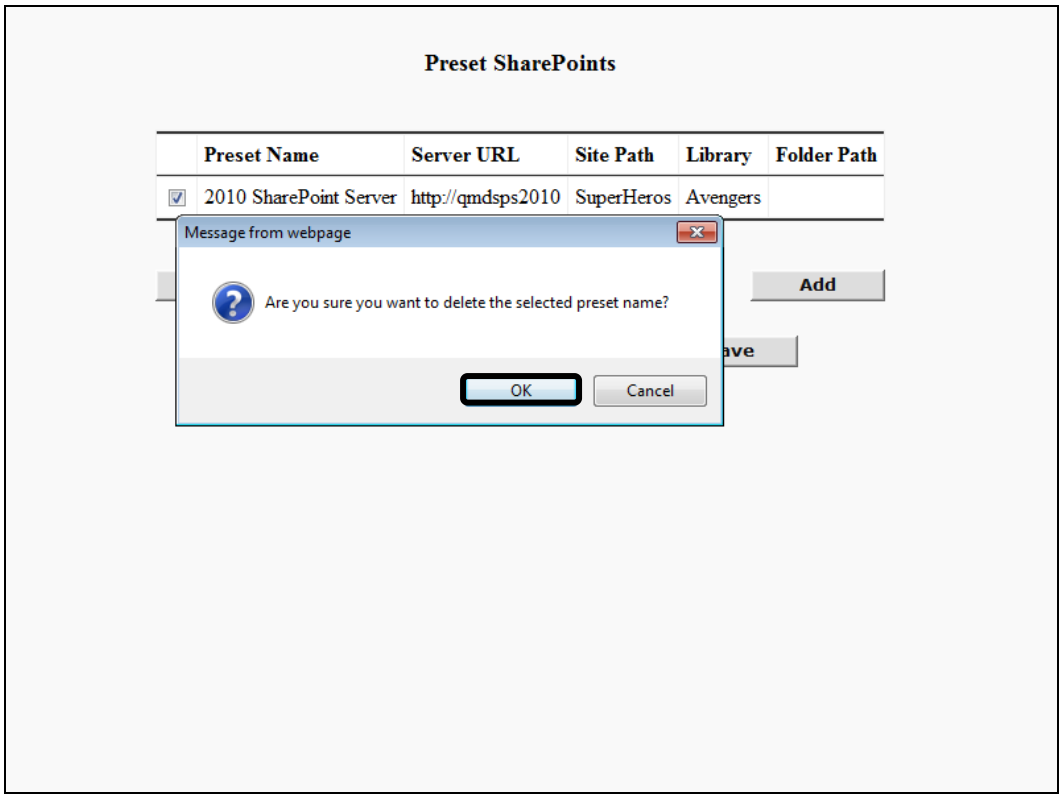
2.14.3 Deleting a Preset SharePoint

You can delete a previously created preset SharePoint from the Preset SharePoints configuration screen.

1. Click [Scan to SharePoint] → [Preset SharePoints] → select the check box next to the preset SharePoint you want to delete → click [Delete].



2. Click [OK] on the confirmation dialog box.



If you do not want to delete the preset SharePoint, click [Cancel].

The preset SharePoint is deleted from the list.

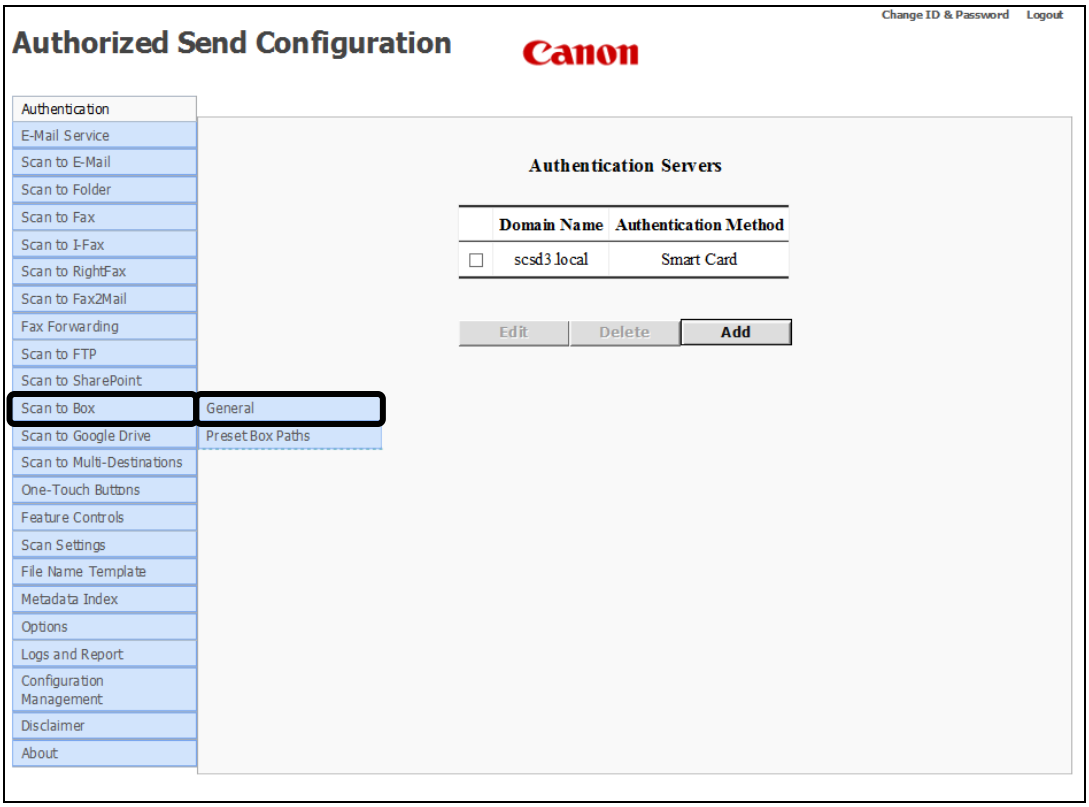
2.15 Configuring the Scan to Box Settings

You can configure the Scan to Box function, which enables users to scan and send documents via a Box account, and create preset Box destinations.

IMPORTANT

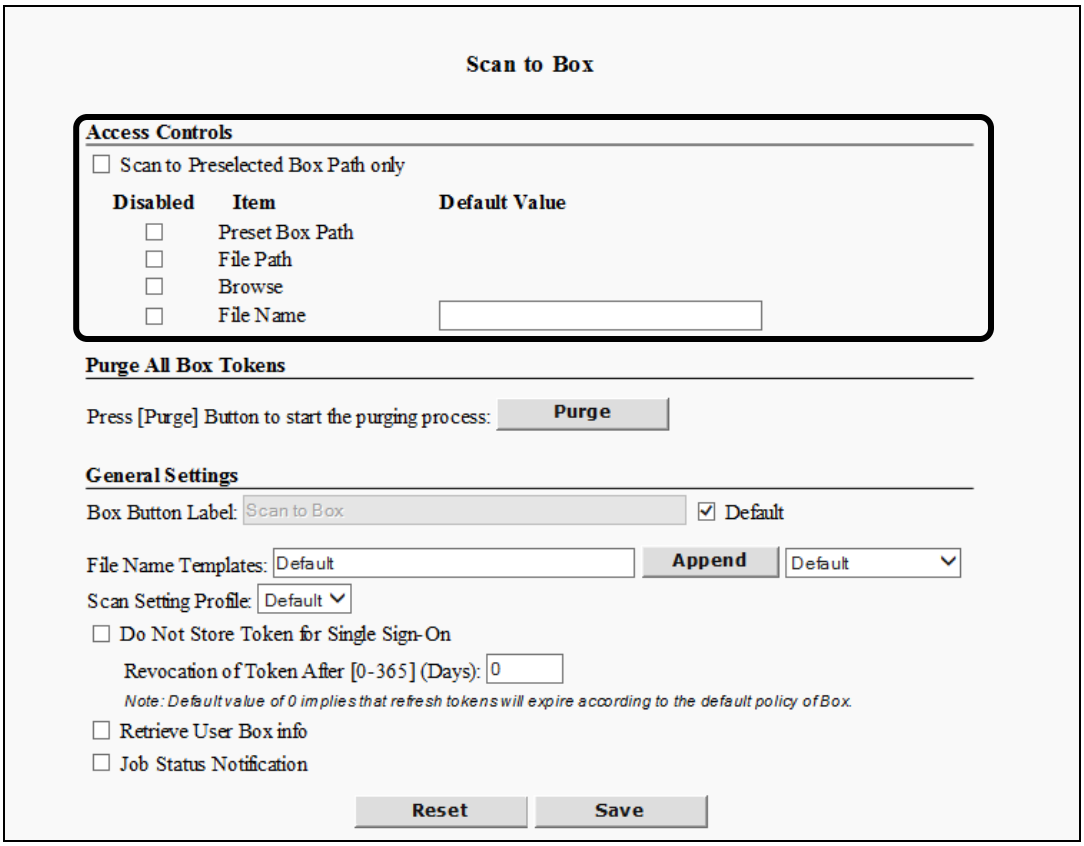
- If an AMS enabled login application is installed and running on the machine, [Scan to Box] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the Scan to Box function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [Scan to Box] →[General].



The Scan to Box screen is displayed.

2. Configure the settings under <Access Controls>.



Access Controls

Scan to Preselected Box Path only:	Check this box to force all users to scan to a pre-set Box path only. If this is unchecked, the [Preset Box Path], [File Path], and [Browse] check boxes appear. This is unchecked by default.

Disabled Item Column

Preset Box Path:	Check this box to remove the “Preset Box Path” selection from the Scan to Box pull-down list. This is unchecked by default.
File Path:	Check this box to remove the [Box Path] text field from the Scan to Box screen on the machine console. This is unchecked by default.

Browse: Check this box to remove the [Browse] button from the Scan to Box screen on the machine console. This is unchecked by default.

File Name: Check this box to disable the [File Name] text field on the Scan to Box screen on the machine console. This is unchecked by default.

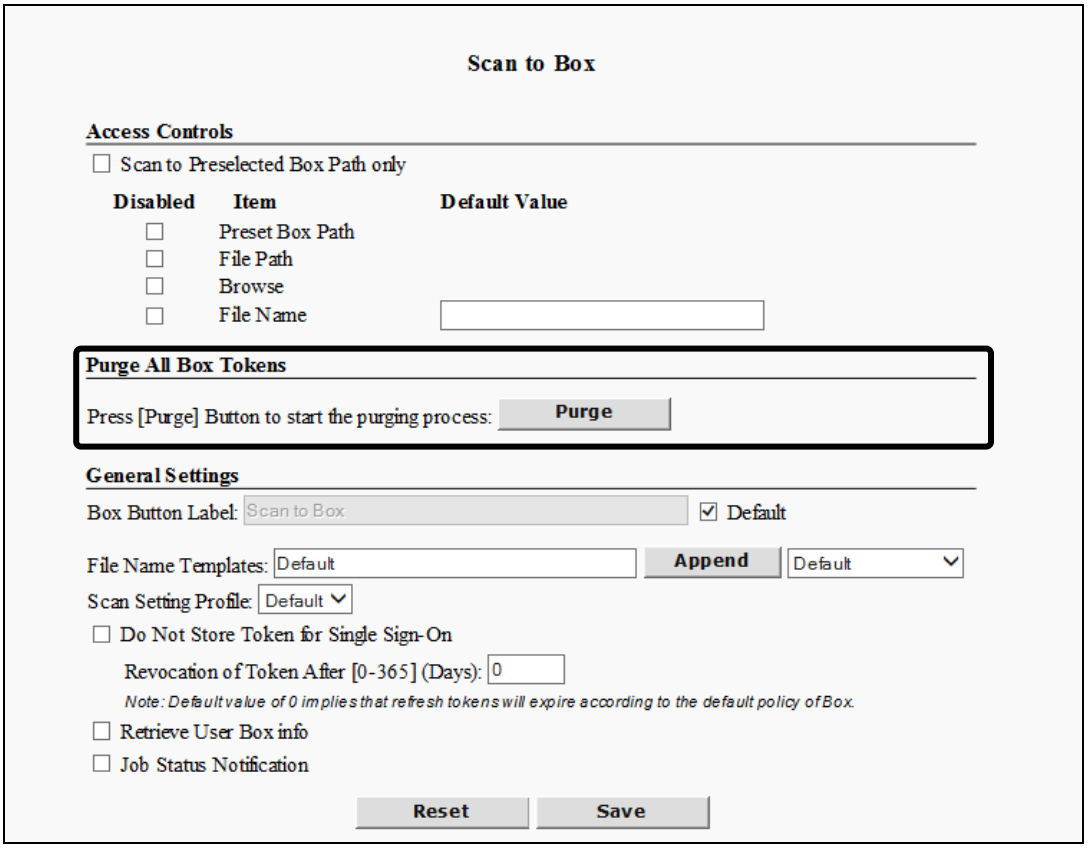
Default Value Column

File Name: Enter the name of a default file name which appears in the [File Name] text box on the Scan to Box screen. The field has a maximum length of 251 characters, which must be alphanumeric, or one of the following characters:

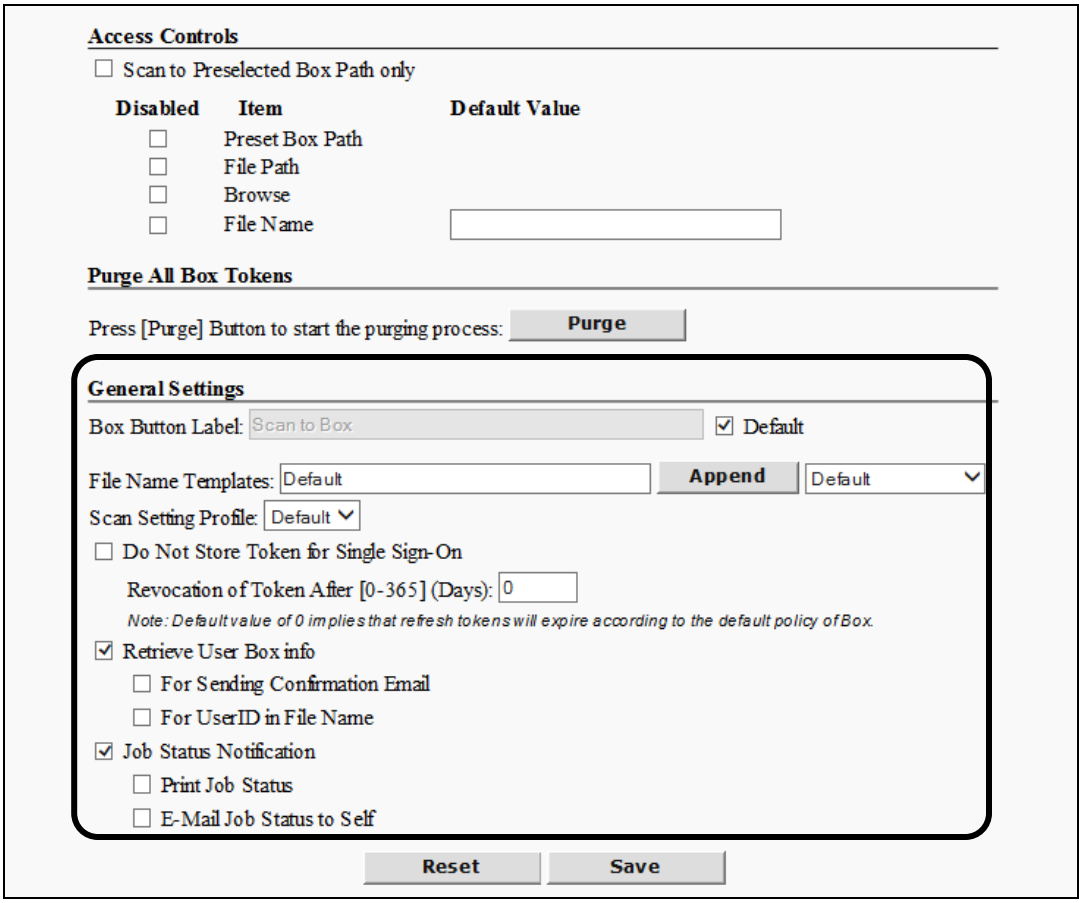
" " (space)
"`" (accent)
"-" (hyphen)
"=" (equal)
"!" (exclamation mark)
"@" (at)
"$" (dollar sign)
"^" (carat)
"(" (left parenthesis)
")" (right parenthesis)
"_" (underscore)
"+" (plus)
"." (period)

If Advanced File Name is enabled, the File Name has any customized fields appended.

3. If you need to clear any outdated or obsolete Box access tokens, press [Purge] to remove them. A new Box access token is generated the next time Authorized Send makes a call to the Box API.



4. Configure the settings under <General Settings>.



General Settings

Box Button Label:	If the [Default] check box is selected, enter a new name for the [Scan to Box] button on the machine console. By default, the [Default] check box is selected and the label is “Scan to Box”. This text field is active only when the [Default] check box is not selected.
Default:	Select this check box if you want to use the default button on the machine console (“Scan to Box”). This check box is selected by default.
File Name Templates:	Enter one or more File Name Templates which the user can select when creating a scan job. The names in this list are created under the <File Name> tab. See “Configuring the File Name,” on p. 407. The default value is ‘Default’. Separate entries must be separated by commas. You can enter the File Name Templates manually or select the Templates from the Append drop-down list and click [Append].

Append:	Click [Append] to add a File Name Template (set in the Append drop-down list) to the string in the [File Name Templates] text box.
Append drop-down:	Select a pre-defined File Name Template that is added to the string in the [File Name Templates] text box after you click [Append].
Scan Setting Profile:	Select a scan profile from the pull-down list. The scan profiles are set using the Scan Setting Profile function.
Do Not Store Token to Stay Logged In:	Select this check box if you want users to have to log in to their Box account every time they use Authorized Send. If this is not selected, the user credentials are saved between sessions. This is unchecked by default.
Revocation of Token after [0-365] Days	If you do not select the [Do Not Store Token...] check box, enter the number of days after which the authorization token should expire. The value must be a number from zero (0) to 365. If the revocation period is set to 0, tokens expire according to Box policy. The default value is 0.
Retrieve User Box info:	Select this check box to enable Authorized Send to use information from the user's Box account.
For Sending Confirmation Email	The [For Sending Confirmation Email] check box is displayed only when the [Retrieve User Box info] check box is selected. Select this check box to send confirmation emails to the address associated with the user's Box account. When scanning to multiple destinations or using the one-touch buttons, this check box only has an effect if all destinations are Box locations.
For User ID in File Name	The [For Sending Confirmation Email] check box is displayed only when the [Retrieve User Box info] check box is selected. Select this check box to use the user's Box account ID instead of the ${UID} placeholder in file name appendixes.
Job Status Notification:	Select this check box if you want the logged on user of the Scan to Box session to receive confirmation printout or email.

Print Job Status	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to Box session to receive a confirmation printout.
E-Mail Job Status to Self	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to Box session to receive a confirmation email.

5. Click [Save].

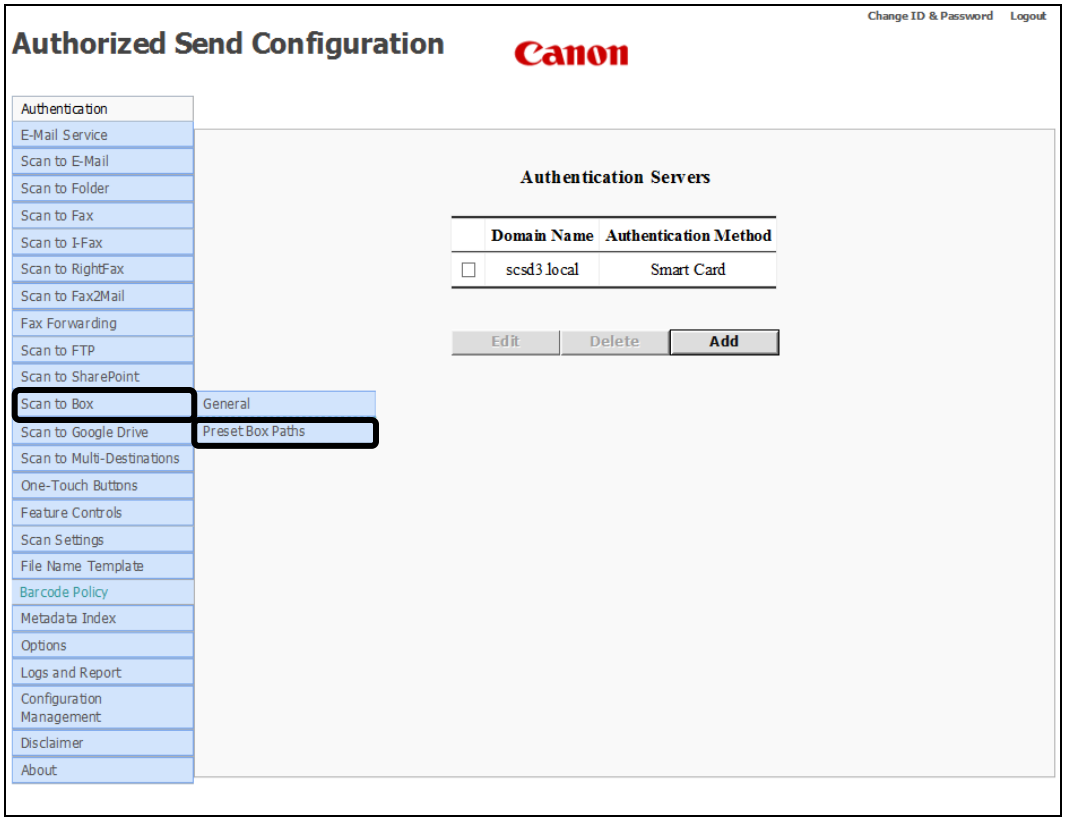
NOTE

If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.15.1 Creating a Preset Box Path

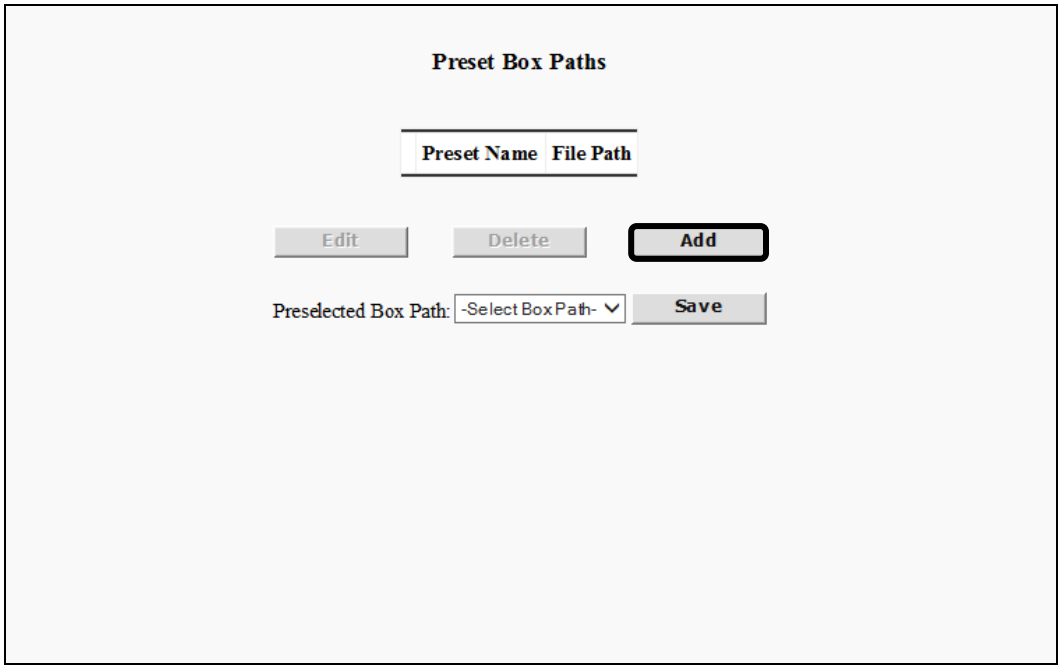
You can create any number of preset box paths.

1. Click [Scan to Box] → [Preset Box Paths].



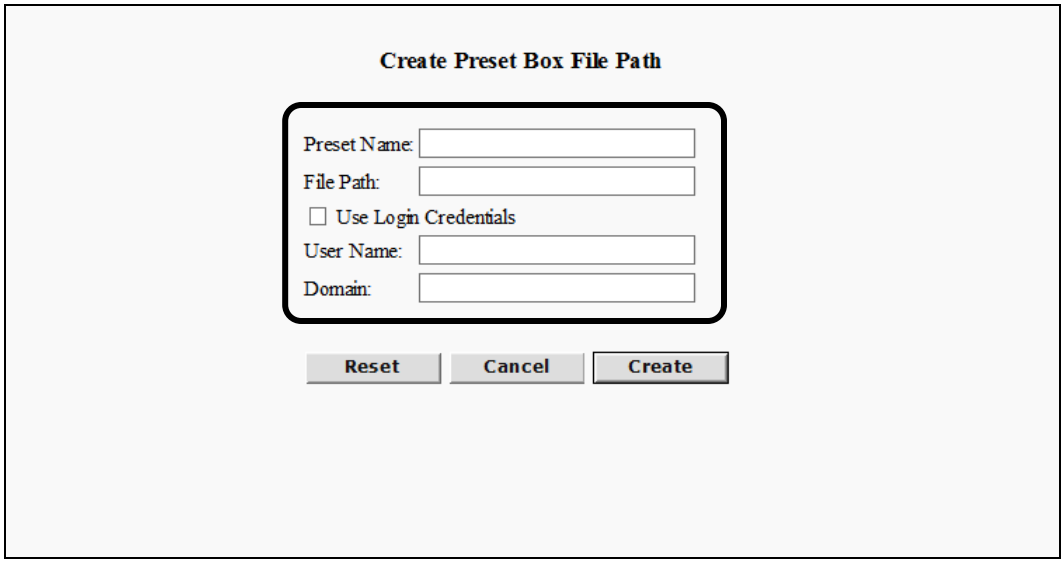
The Preset Box Paths screen is displayed.

2. Click [Add].



The Create Preset Box File Path screen displays.

3. Configure the Preset Box File Path Settings.



Preset Name: Enter the name of the preset Box path to create. You may enter a maximum of 31 characters, and it may not be a duplicate of any other preset path name. This field is required and is blank by default.

File Path: Enter the Box file path. The file path must be a valid file path in the destination Box account.

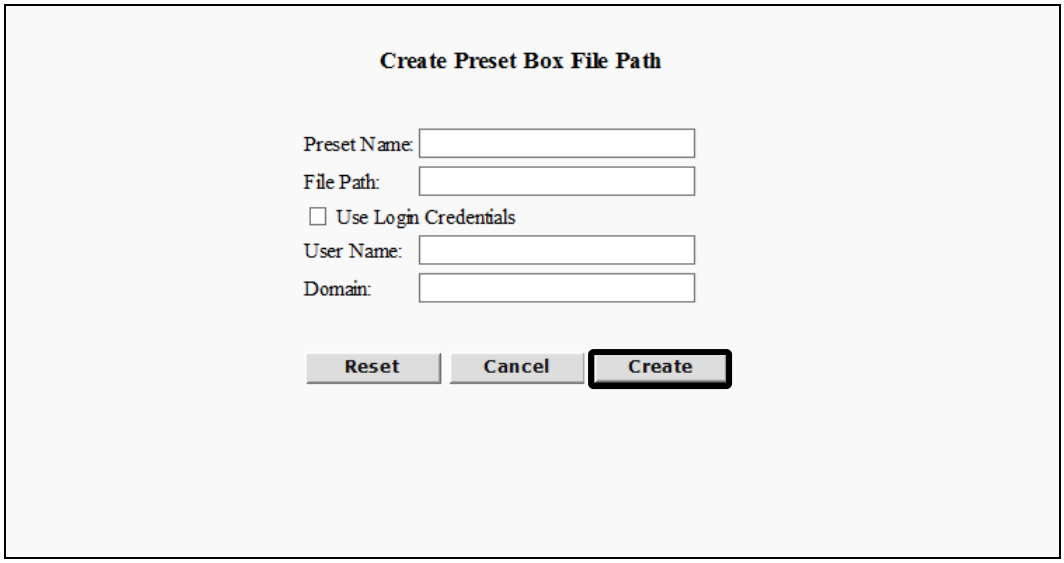
Use Login Credentials: Select this check box to use the same credentials as were used to start the Authorized Send scan session. If you unselect this check box, a different set of valid credentials must be supplied. This is checked by default.

User Name: The [User Name] text box is displayed only when the [Use Login Credentials] check box is unselected. Enter a valid user name which will be used to authenticate against Authorized Send. The name has a maximum of 255 characters.

Domain: The [Domain] text box is displayed only when the [Use Login Credentials] check box is unselected. Enter a valid account domain which will be used to authenticate against Authorized Send. The domain has a maximum of 255 characters.

NOTE
If the user and domain name specified above do not already have a valid Box token on the device, the user is redirected to Box login to create one.

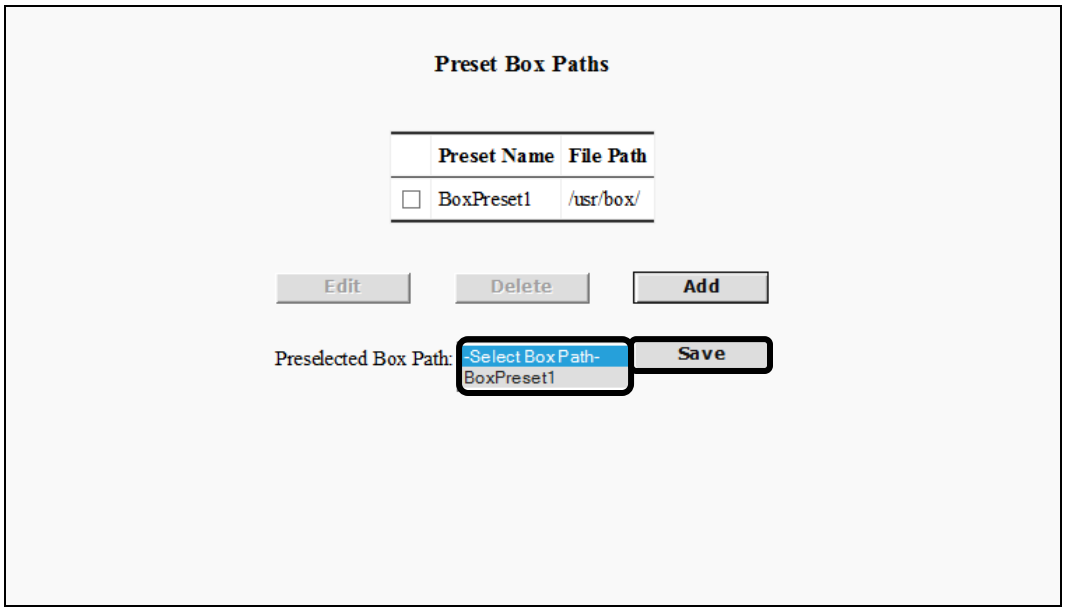
4. Click [Create].



If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

To cancel creating the preset share and return to the Preset Box Paths configuration screen, click [Cancel].

5. If you want to specify a server name that automatically populates the value in the Preselected Box Path drop-down list on the Authorized Send SCAN TO BOX screen on the machine, select a server name from the Preselected Box Path drop-down list → click [Save].



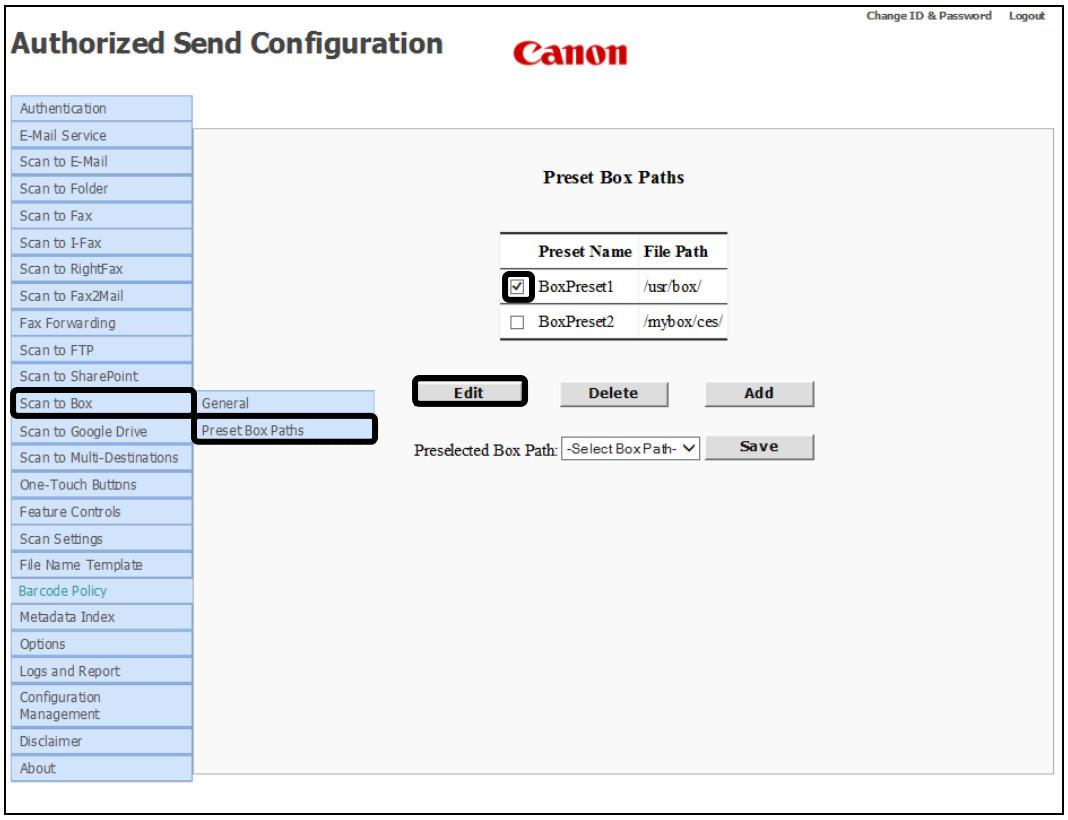
NOTE

- The default setting is ‘Select Box Path’
- ‘Select Box Path’ appears automatically in the Preset Server drop-down list on the Authorized Send SCAN TO BOX screen on the machine.
- If the preselected Box path you selected is deleted, ‘Select Box Path’ is displayed in the Preset Box Path drop-down list on the Authorized Send SCAN TO BOX screen on the machine.

2.15.2 Editing a Preset Box Path

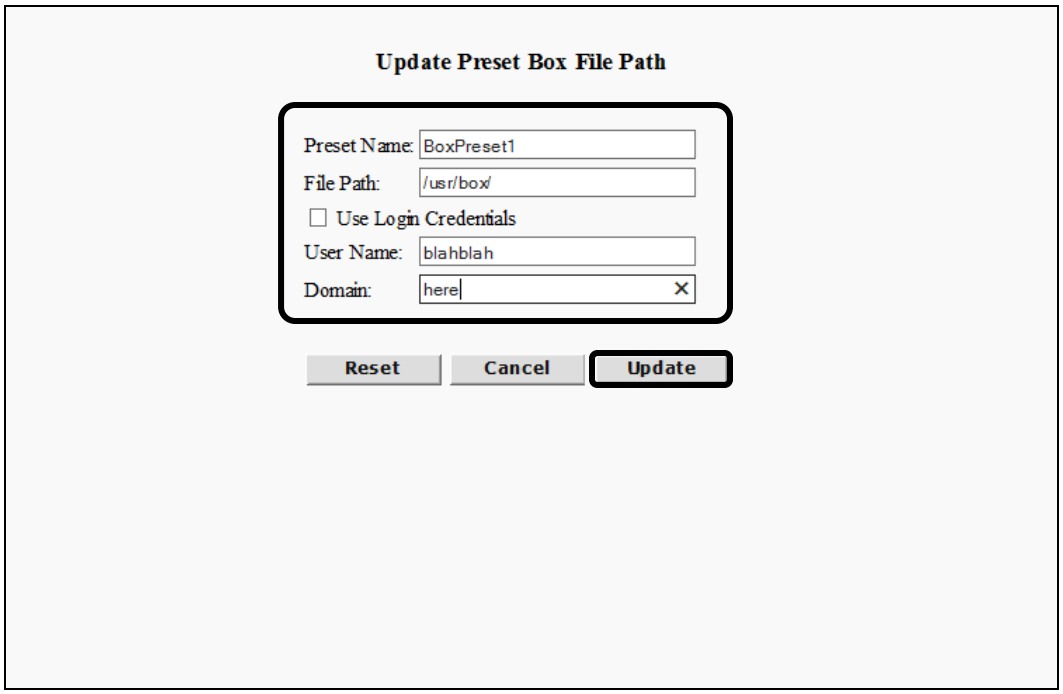
You can edit a previously created preset Box path from the Preset Box Paths configuration screen.

1. Click [Scan to Box] →[Preset Box Paths] →select the check box next to the preset Box path you want to edit →click [Edit].



The Update Preset Box File Path screen displays.

2. Edit the settings for the preset Box path, as necessary →click [Update].



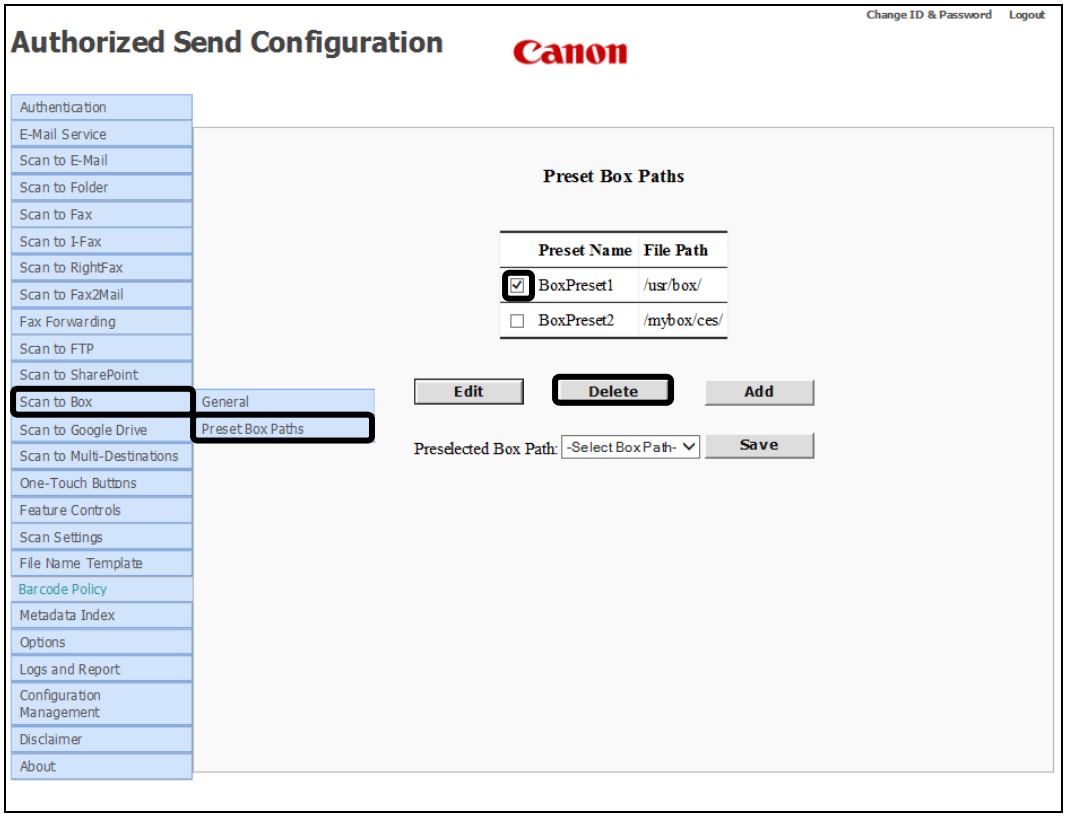
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the preset SharePoint and return to the Preset Box Paths configuration screen, click [Cancel].

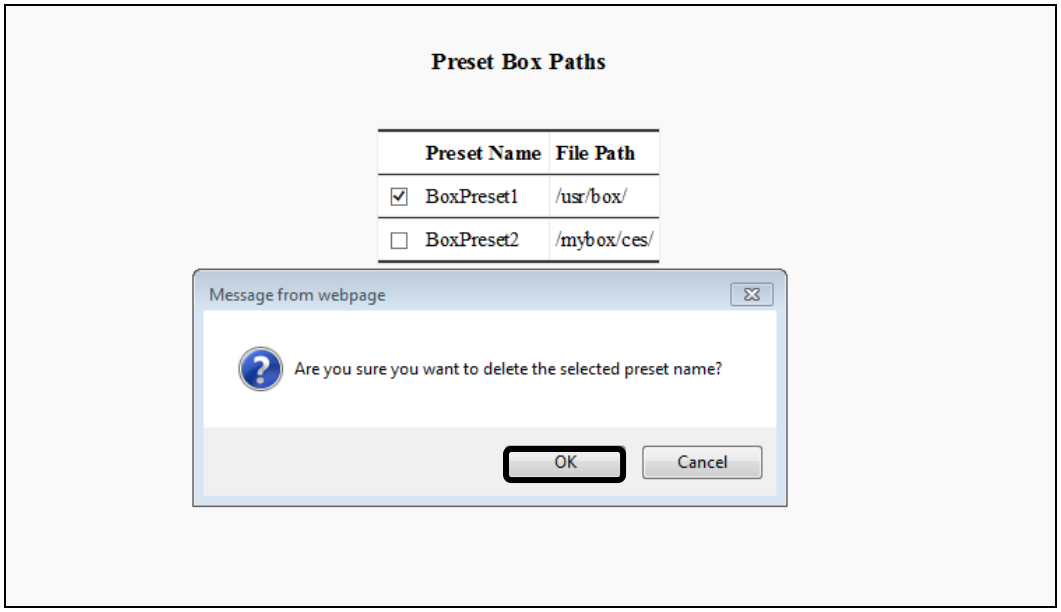
2.15.3 Deleting a Preset Box Path

You can delete a previously created preset Box path from the Preset Box Paths configuration screen.

1. Click [Scan to Box] →[Preset Box Paths] →select the check box next to the preset Box path you want to delete →click [Delete].



2. Click [OK] on the confirmation dialog box.



If you do not want to delete the preset Box path, click [Cancel].

The preset Box path is deleted from the list.

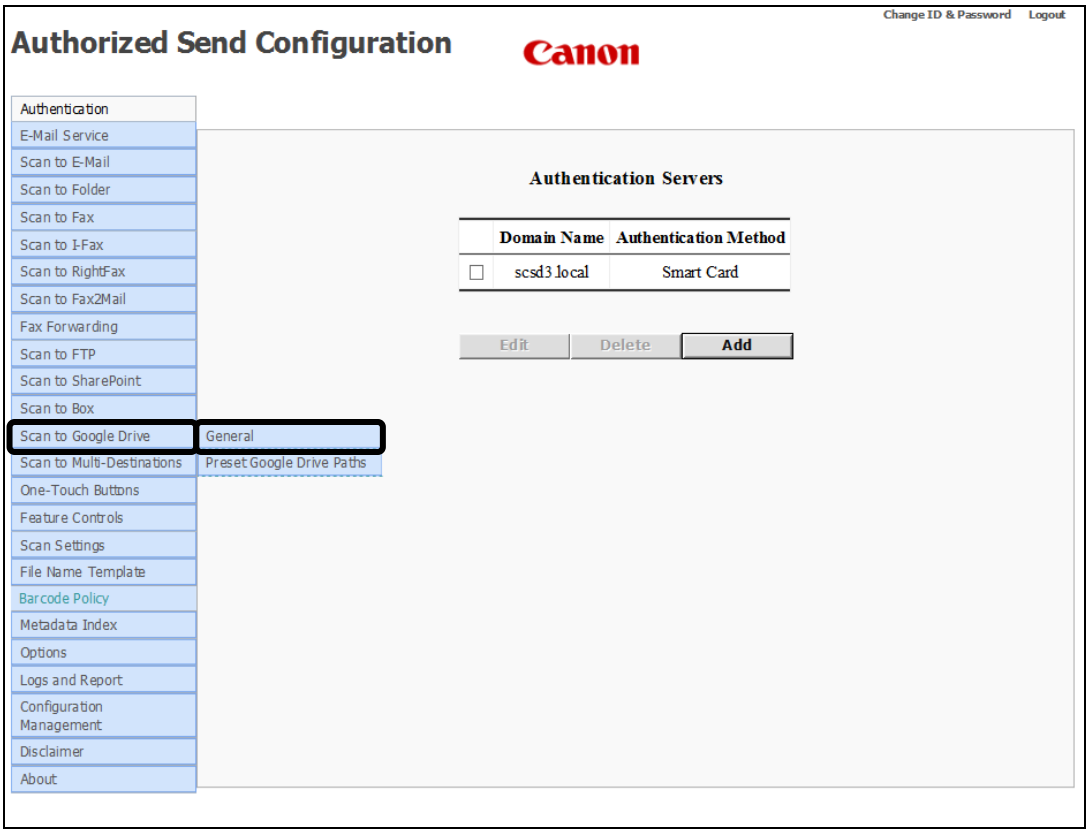
2.16 Configuring the Scan to Google Drive Settings

You can configure the Scan to Google Drive function, which enables users to scan and send documents via a Google Drive account, and create preset Google Drive destinations.

IMPORTANT

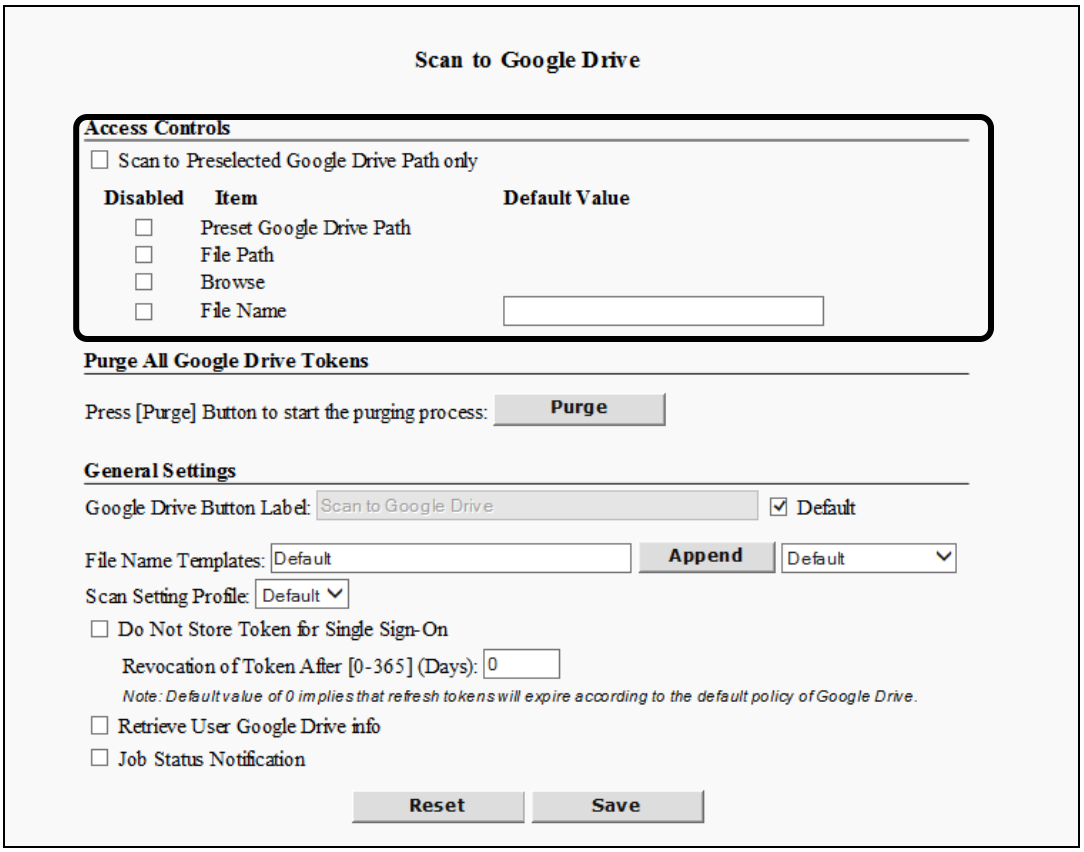
- If an AMS enabled login application is installed and running on the machine, [Scan to Google Drive] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the Scan to Google Drive function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [Scan to Google Drive] →[General].



The Scan to Google Drive screen displays.

2. Configure the settings under <Access Controls>.



Access Controls

Scan to Preselected Google Drive Path only:	Check this box to force all users to scan to a pre-set Google Drive path only. If this is unchecked, the [Preset Google Drive Path], [File Path], and [Browse] check boxes appear. This is unchecked by default.

Disabled Item Column

Preset Google Drive Path:	Check this box to remove the “Preset Google Drive Path” selection from the Scan to Google Drive pull-down list. This is unchecked by default.
File Path:	Check this box to remove the [Google Drive Path] text field from the Scan to Google Drive screen on the machine console. This is unchecked by default.

Browse: Check this box to remove the [Browse] button from the Scan to Google Drive screen on the machine console. This is unchecked by default.

File Name: Check this box to disable the [File Name] text field on the Scan to Google Drive screen on the machine console. This is unchecked by default.

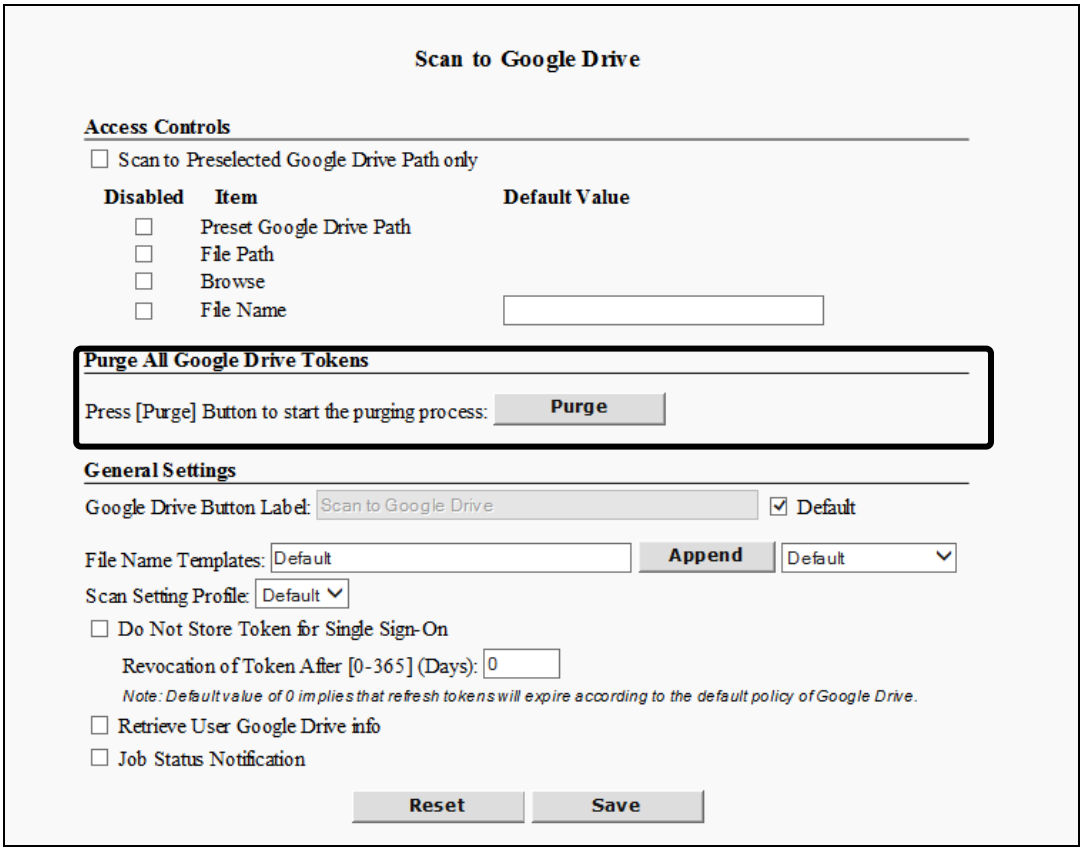
Default Value Column

File Name: Enter the name of a default file name which appears in the [File Name] text box on the Scan to Google Drive screen. The field has a maximum length of 251 characters, which must be alphanumeric, or one of the following characters:

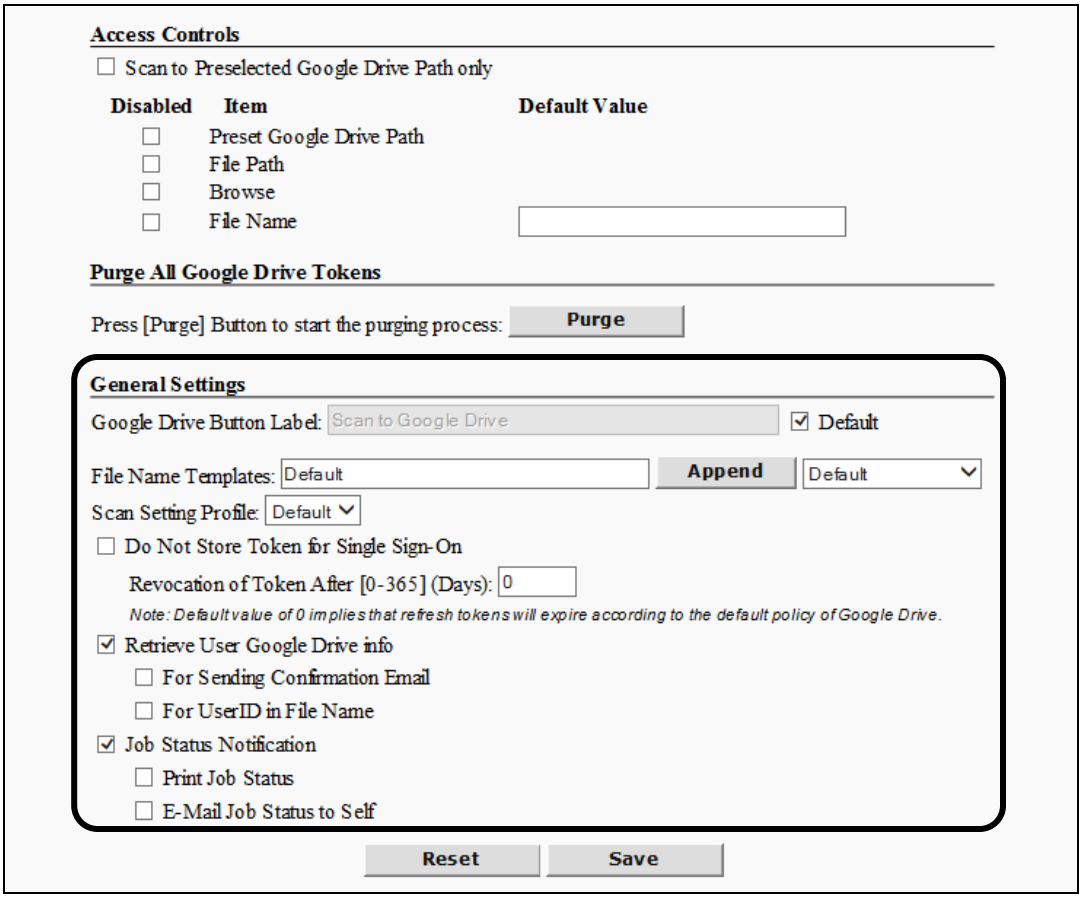
" " (space)
"`" (accent)
"-" (hyphen)
"=" (equal)
"!" (exclamation mark)
"@" (at)
"$" (dollar sign)
"^" (carat)
"(" (left parenthesis)
")" (right parenthesis)
"_" (underscore)
"+" (plus)
"." (period)

If Advanced File Name is enabled, the File Name has any customized fields appended.

3. If you need to clear any outdated or obsolete Google Drive access tokens, press [Purge] to remove them. A new Google Drive access token is generated the next time Authorized Send makes a call to the Google Drive API.



4. Configure the settings under <General Settings>.



General Settings

Google Drive Button Label:	If the [Default] check box is selected, enter a new name for the [Scan to Google Drive] button on the machine console. By default, the [Default] check box is selected and the label is “Scan to Google Drive”. This text field is active only when the [Default] check box is not selected.
Default:	Select this check box if you want to use the default button on the machine console (“Scan to Google Drive”). This check box is selected by default.
File Name Templates:	Enter one or more File Name Templates which the user can select when creating a scan job. The names in this list are created under the <File Name> tab. See “Configuring the File Name,” on p. 407. The default value is ‘Default’. Separate entries must be separated by commas. You can enter the File Name Templates manually or select the Templates from the Append drop-down list and click [Append].

Append:	Click [Append] to add a File Name Template (set in the Append drop-down list) to the string in the [File Name Templates] text box.
Append drop-down:	Select a pre-defined File Name Template that is added to the string in the [File Name Templates] text box after you click [Append].
Scan Setting Profile:	Select a scan profile from the pull-down list. The scan profiles are set using the Scan Setting Profile function.
Do Not Store Token to Stay Logged In:	Select this check box if you want users to have to log in to their Google Drive account every time they use Authorized Send. If this is not selected, the user credentials are saved between sessions. This is unchecked by default.
Revocation of Token after [0-365] Days	If you do not select the [Do Not Store Token...] check box, enter the number of days after which the authorization token should expire. The value must be a number from zero (0) to 365. If the revocation period is set to 0, tokens expire according to Google Drive policy. The default value is 0.
Retrieve User Google Drive info:	Select this check box to enable Authorized Send to use information from the user's Google Drive account.
For Sending Confirmation Email	The [For Sending Confirmation Email] check box is displayed only when the [Retrieve User Google Drive info] check box is selected. Select this check box to send confirmation emails to the address associated with the user's Google Drive account. When scanning to multiple destinations or using the one-touch buttons, this check box only has an effect if all destinations are Google Drive locations.
For User ID in File Name	The [For Sending Confirmation Email] check box is displayed only when the [Retrieve User Google Drive info] check box is selected. Select this check box to use the user's Google Drive account ID instead of the ${UID} placeholder in file name appendixes.

Job Status Notification:	Select this check box if you want the logged on user of the Scan to Google Drive session to receive confirmation printout or email.
Print Job Status	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to Google Drive session to receive a confirmation printout.
E-Mail Job Status to Self	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to Google Drive session to receive a confirmation email.

5. Click [Save].

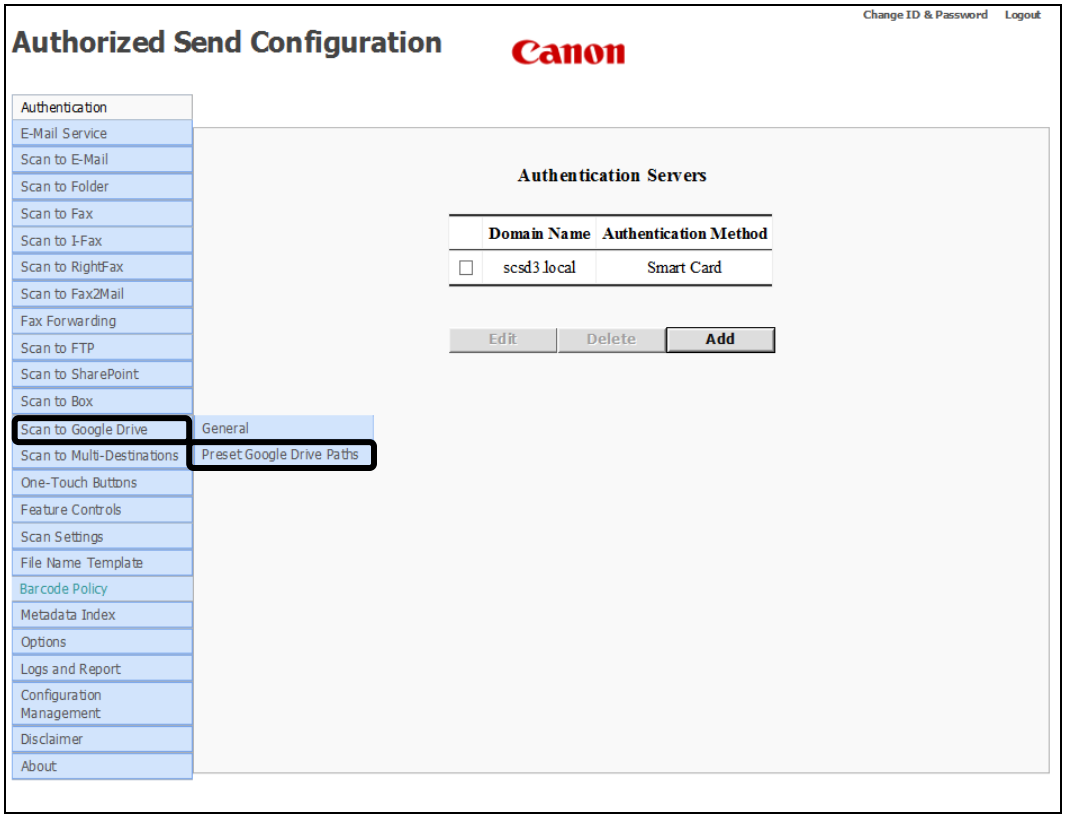
NOTE

If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.16.1 Creating a Preset Google Drive Path

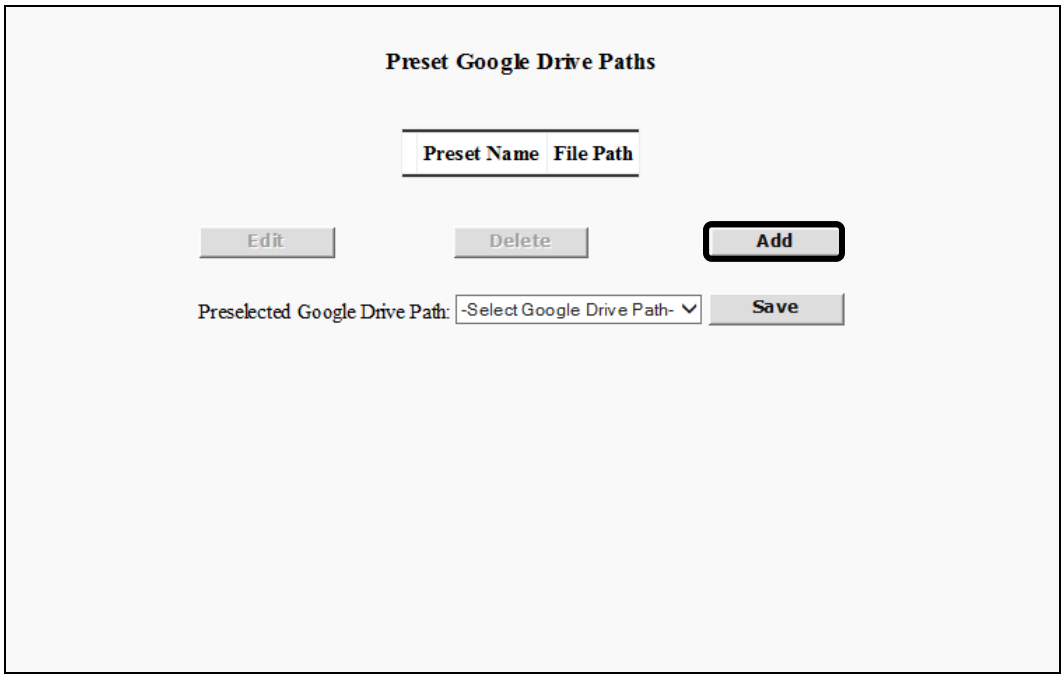
You can create any number of preset Google Drive paths.

1. Click [Scan to Google Drive] → [Preset Google Drive Paths].



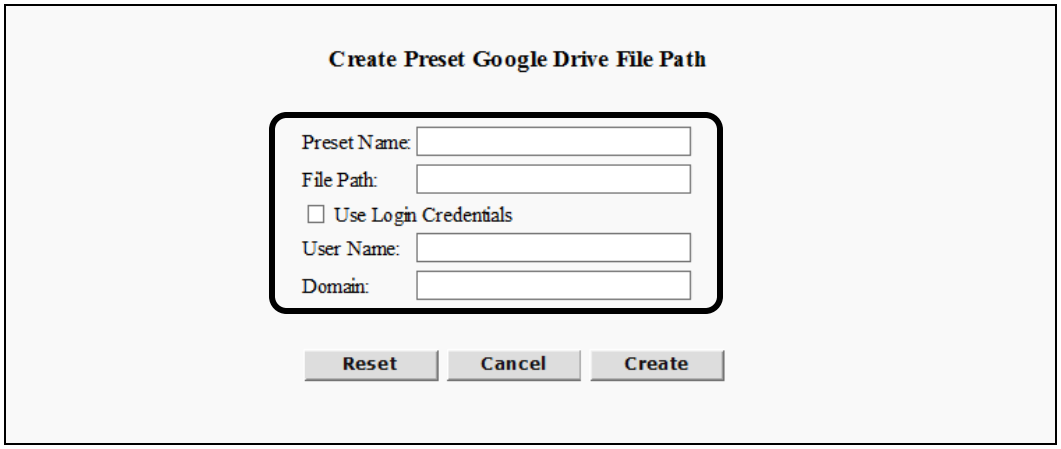
The Preset Google Drive Paths screen displays.

2. Click [Add].



The Create Preset Google Drive File Path screen displays.

3. Configure the Preset Google Drive File Path Settings.



Preset Name: Enter the name of the preset Google Drive path to create. You may enter a maximum of 31 characters, and it may not be a duplicate of any other preset path name. This field is required and is blank by default.

File Path: Enter the Google Drive file path. The file path must be a valid file path in the destination Google Drive account.

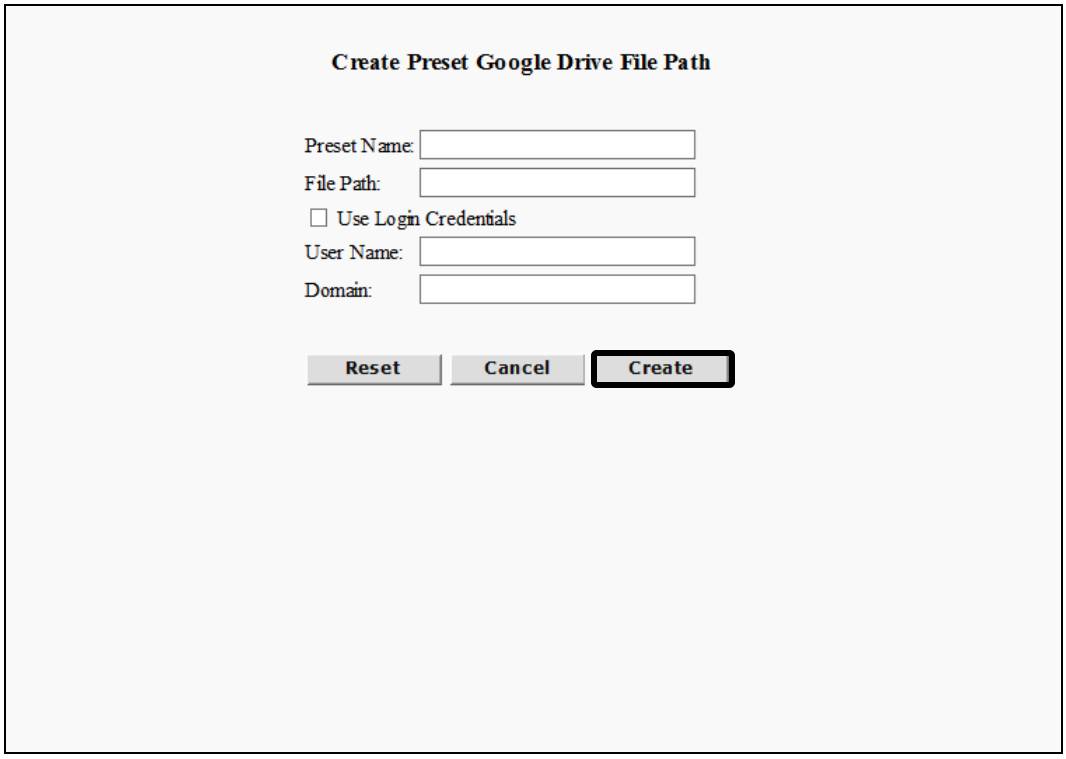
Use Login Credentials: Select this check box to use the same credentials as were used to start the Authorized Send scan session. If you unselect this check box, a different set of valid credentials must be supplied. This is checked by default.

User Name: The [User Name] text box is displayed only when the [Use Login Credentials] check box is unselected. Enter a valid user name which will be used to authenticate against Authorized Send. The name has a maximum of 255 characters.

Domain: The [Domain] text box is displayed only when the [Use Login Credentials] check box is unselected. Enter a valid account domain which will be used to authenticate against Authorized Send. The domain has a maximum of 255 characters.

NOTE
If the user and domain name specified above do not already have a valid Box token on the device, the user is redirected to Box login to create one.

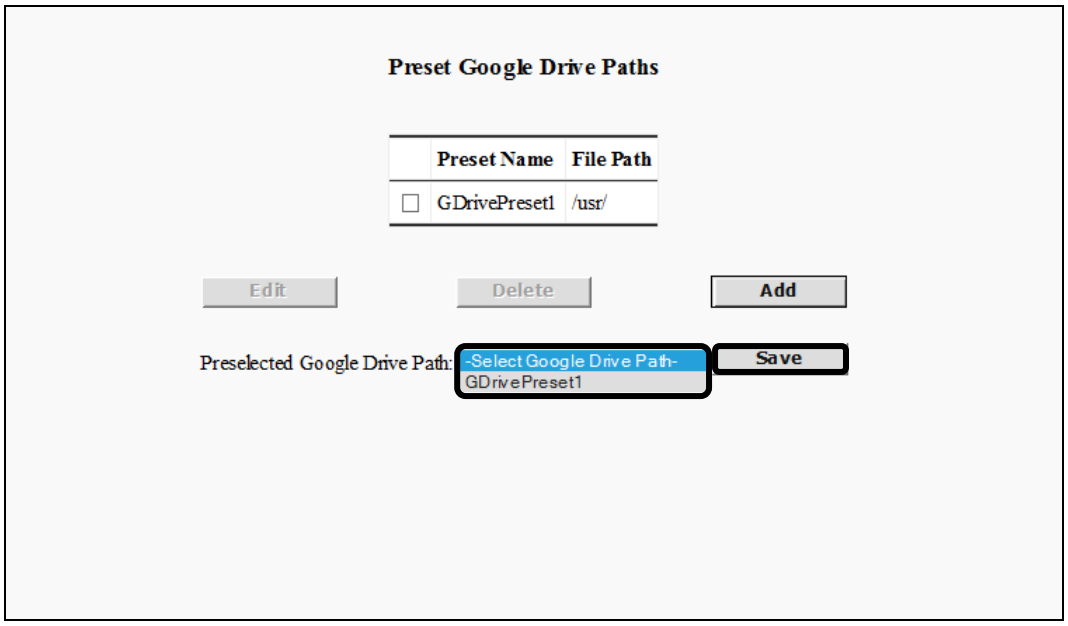
4. Click [Create].



If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

To cancel creating the preset share and return to the Preset Google Drive Paths configuration screen, click [Cancel].

5. If you want to specify a server name that automatically populates the value in the Preselected Google Drive Path drop-down list on the Authorized Send SCAN TO GOOGLE DRIVE screen on the machine, select a server name from the Preselected Google Drive Path drop-down list → click [Save].



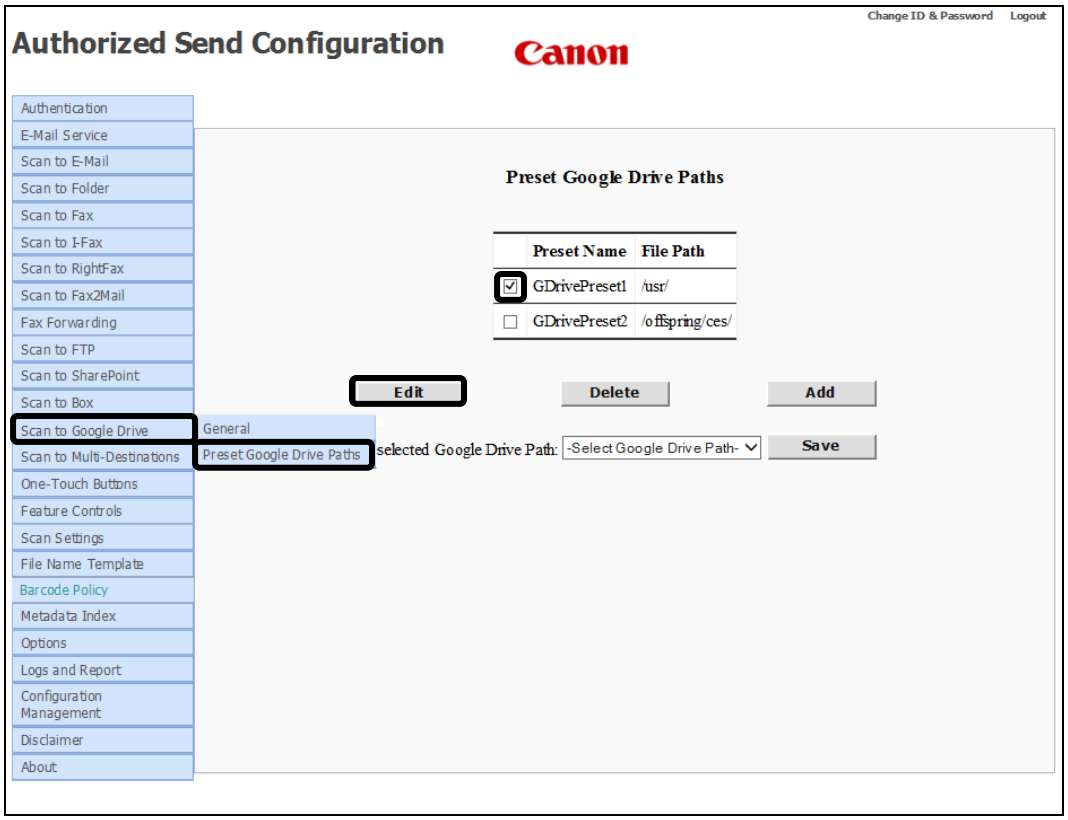
NOTE

- The default setting is ‘Select Google Drive Path’
- ‘Select Google Drive Path’ appears automatically in the Preset Server drop-down list on the Authorized Send SCAN TO GOOGLE DRIVE screen on the machine.
- If the preselected Google Drive path you selected is deleted, ‘Select Google Drive Path’ is displayed in the Preset Google Drive Path drop-down list on the Authorized Send SCAN TO GOOGLE DRIVE screen on the machine.

2.16.2 Editing a Preset Google Drive Path

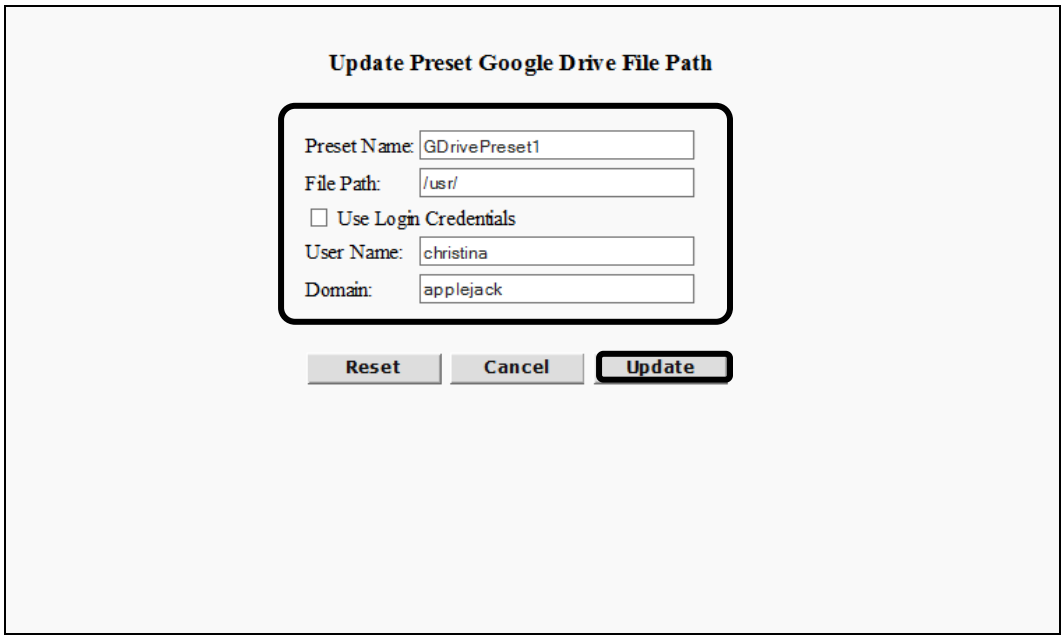
You can edit a previously created preset Google Drive path from the Preset Google Drive Paths configuration screen.

1. Click [Scan to Google Drive] →[Preset Google Drive Paths] →select the check box next to the preset Google Drive path you want to edit →click [Edit].



The Update Preset Google Drive File Path screen displays.

2. Edit the settings for the preset Google Drive file path, as necessary →click [Update].



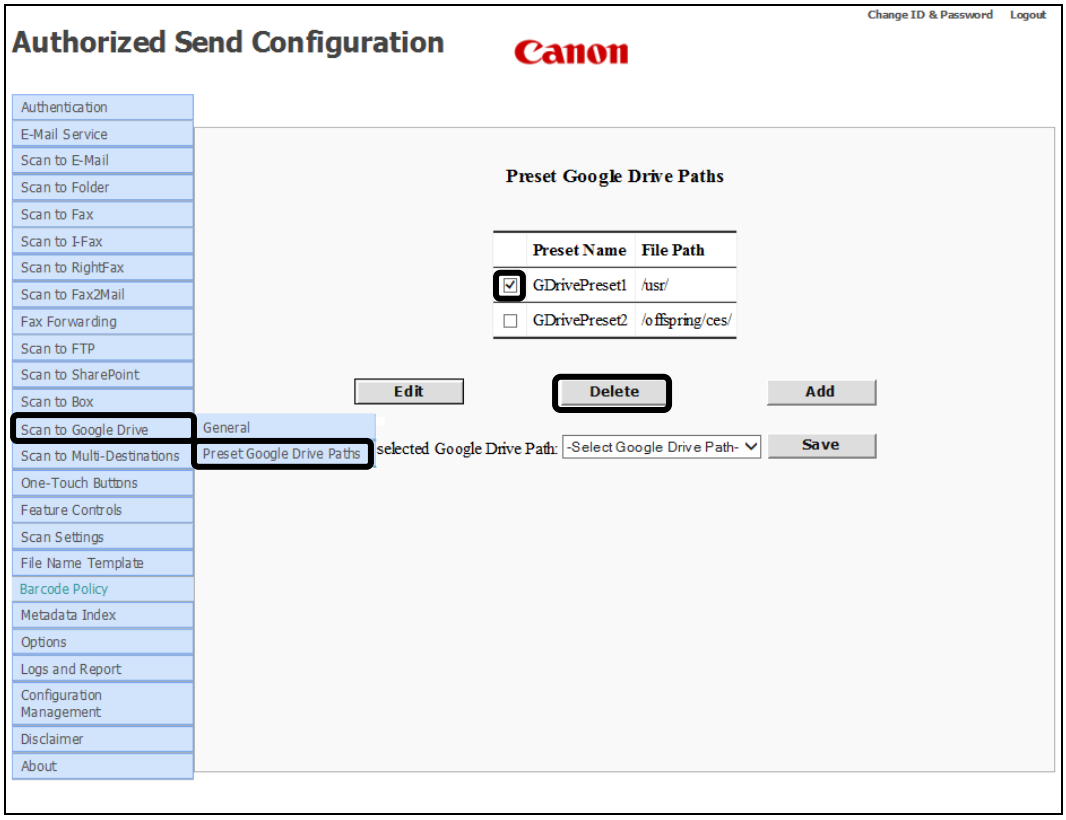
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the preset Google Drive file path and return to the Preset Google Drive Paths configuration screen, click [Cancel].

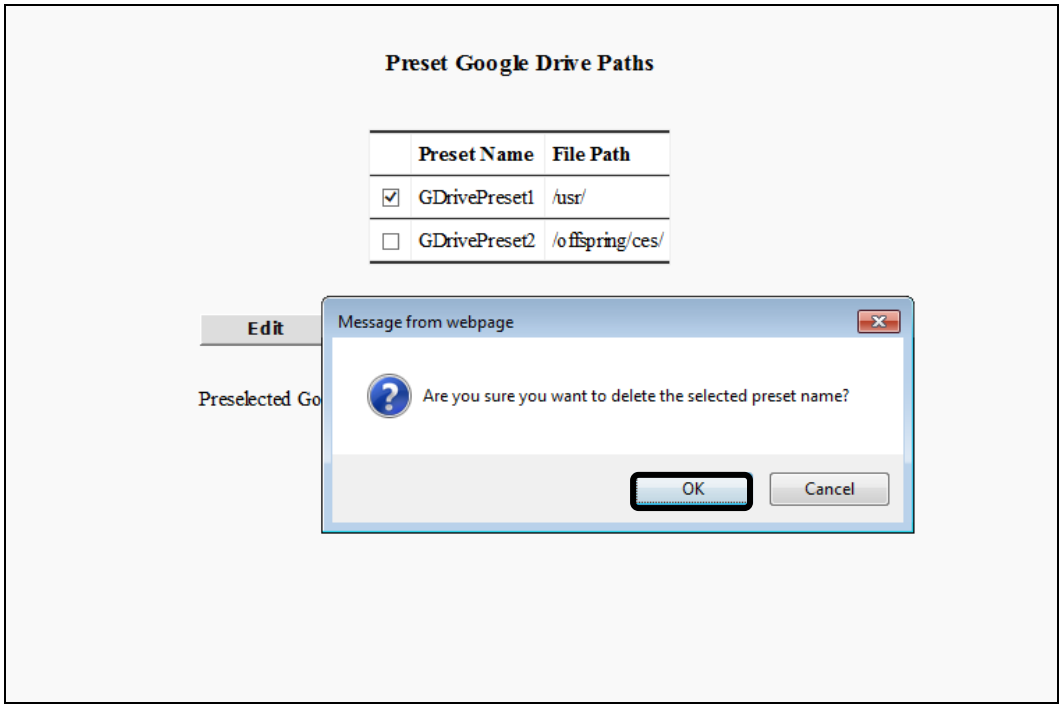
2.16.3 Deleting a Preset Google Drive File Path

You can delete a previously created preset Google Drive path from the Preset Google Drive Paths configuration screen.

1. Click [Scan to Google Drive] →[Preset Google Drive Paths] →select the check box next to the preset Google Drive path you want to delete →click [Delete].



2. Click [OK] on the confirmation dialog box.



If you do not want to delete the preset Google Drive path, click [Cancel].

The preset Google Drive path is deleted from the list.

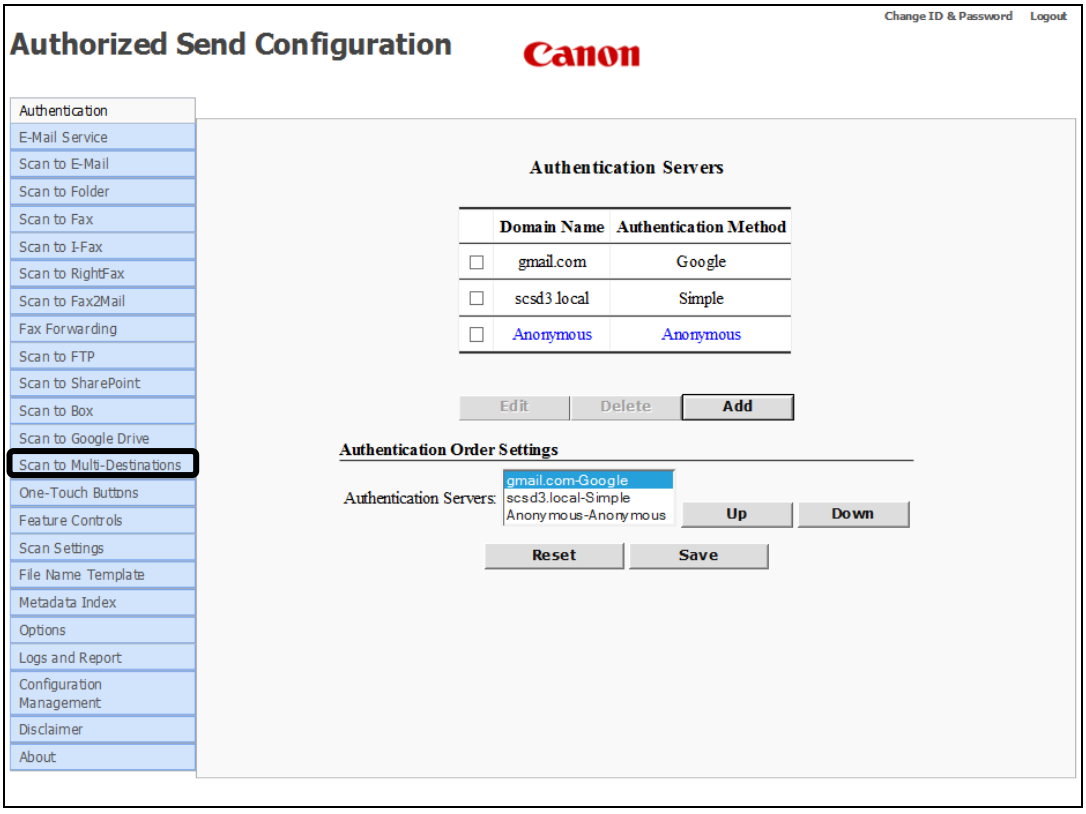
2.17 Configuring the Scan to Multi-Destinations

You can configure the Scan to Multi-Destinations function, which enables users to scan and send documents via Scan to E-Mail, Scan to Fax, Scan to I-Fax, Scan to Folder, Scan to FTP, Scan to SharePoint, Scan to Box, and Scan to Google Drive at the press of the [Scan to Multi-Destinations] key. A maximum of 10 destinations can be selected by the user.

IMPORTANT

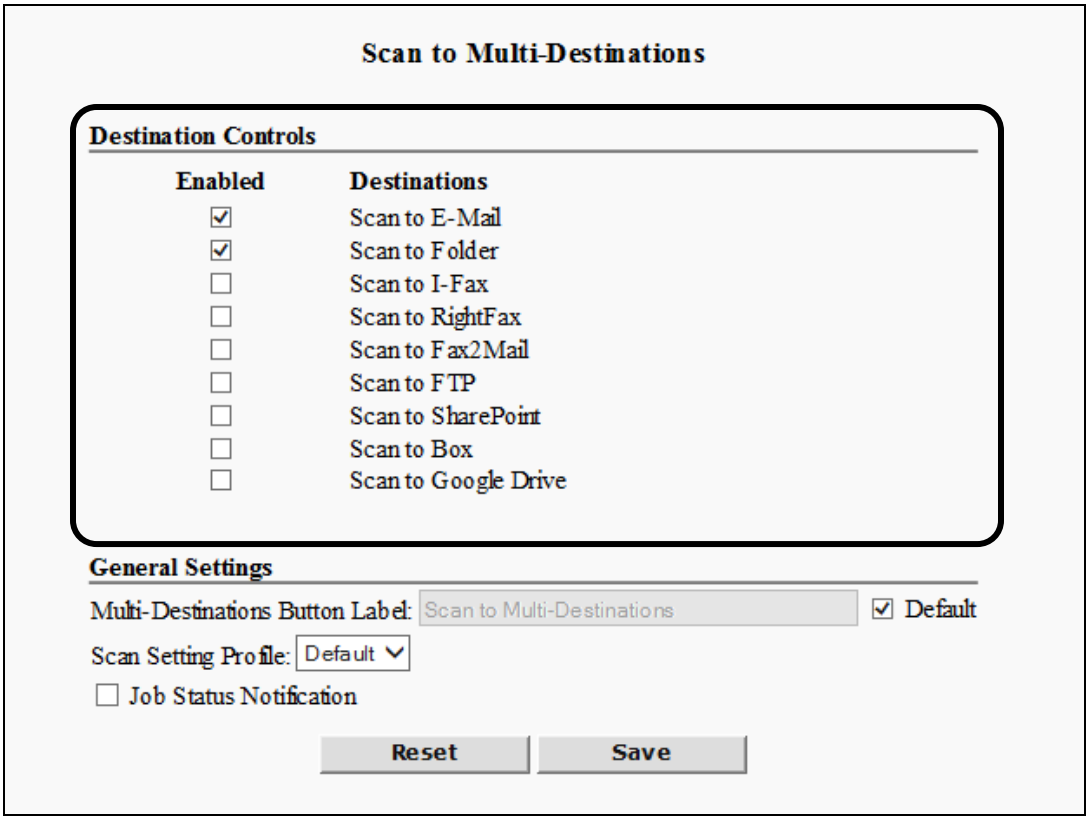
- If an AMS enabled login application is installed and running on the machine, [Scan to Multi-Destinations] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the Scan to Multi-Destinations function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [Scan to Multi-Destinations].



The Scan to Multi-Destinations screen is displayed.

2. Configure the settings under <Destination Controls>.



Destination Controls

Enabled Column

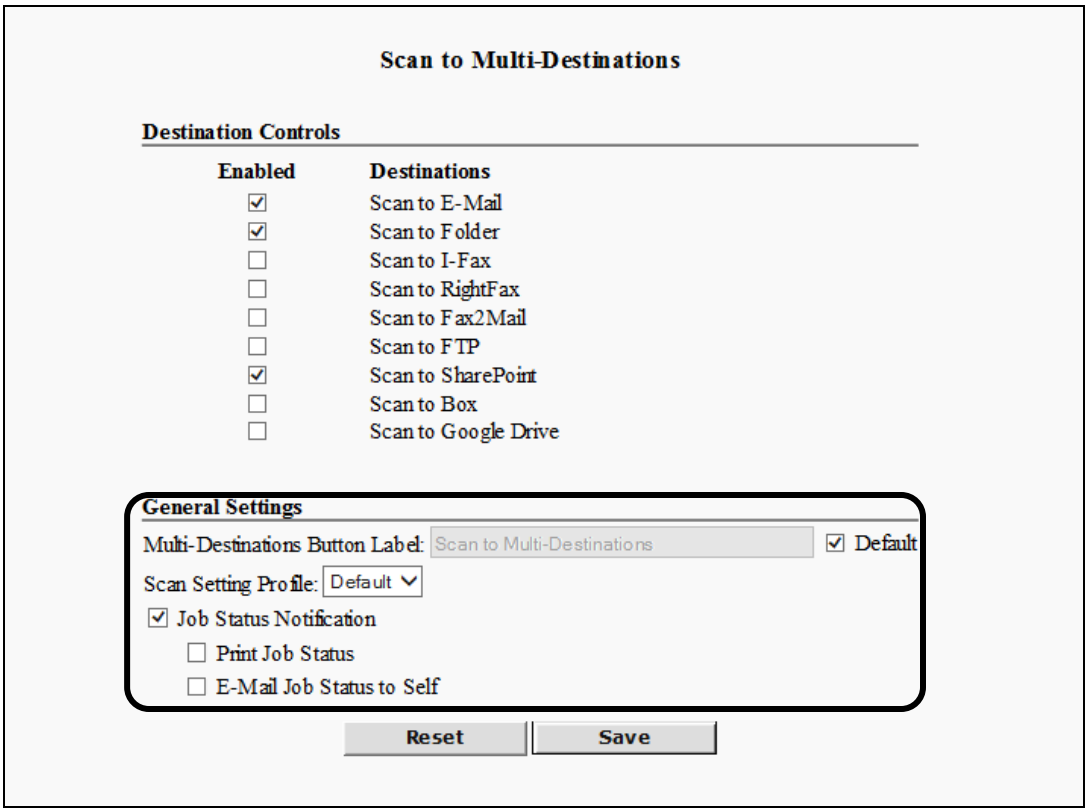
Scan to E-mail:
Scan to Folder:
Scan to Fax:
Scan to RightFax
Scan to Fax2Mail:
Scan to I-Fax:
Scan to FTP:
Scan to SharePoint:
Scan to Box:
Scan to Google Drive:

Select each check box if you want the corresponding function to appear in the New Destinations drop-down list on the Authorized Send SCAN TO MULTI-DESTINATIONS screen on the machine. The [Scan to E-mail] and [Scan to Folder] check boxes are selected by default.

NOTE

- The listed Destination Controls will vary, depending on machine configuration and capabilities.
- If you select the [Scan to E-Mail], [Scan to Folder], [Scan to Fax], [Scan to I-Fax], [Scan to FTP], and [Scan to SharePoint] check boxes in the [Feature Controls] tab, which enables these functions, the settings used when [Scan to Multi-Destinations] is pressed on the MAIN screen on the machine, are those configured within each function.
- These settings are also reflected in the available destinations for Personal Buttons. See the *Authorized Send Version 6.4 User's Guide* for more information.
- If the function check boxes are not selected in the [Feature Controls] tab, the settings used when [Scan to Multi-Destinations] is pressed on the MAIN screen on the machine, are the default values of the individual functions.

3. Configure the settings under <General Settings>.



General Settings

Multi-Destinations Button Label:	Enter the label for the [Scan to Multi-Destinations] key that appears on the Authorized Send MAIN screen on the machine. It is a required text box that cannot be left blank. The number of any characters permitted is restricted by the width of the Scan to Multi-Destinations icon.
Scan Setting Profile:	Select a scan setting profile from the drop-down list. The default setting is 'Default', which corresponds to the default settings on the Scan Settings screen.
Default:	Select this check box if you want to use the default Multi-Destinations Button Label setting ('Scan to Multi-Destinations'). The Multi-Destinations Button Label text box cannot be changed when the Default check box is selected.
Job Status Notification:	Select this check box if you want the logged on user of the Scan to Multi-Destinations session to receive confirmation printout or email.

Print Job Status:	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to Multi-Destinations session to receive a confirmation printout.
E-Mail Job Status to Self:	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the Scan to Multi-Destinations session to receive a confirmation email.

4. Click [Save].

NOTE
If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

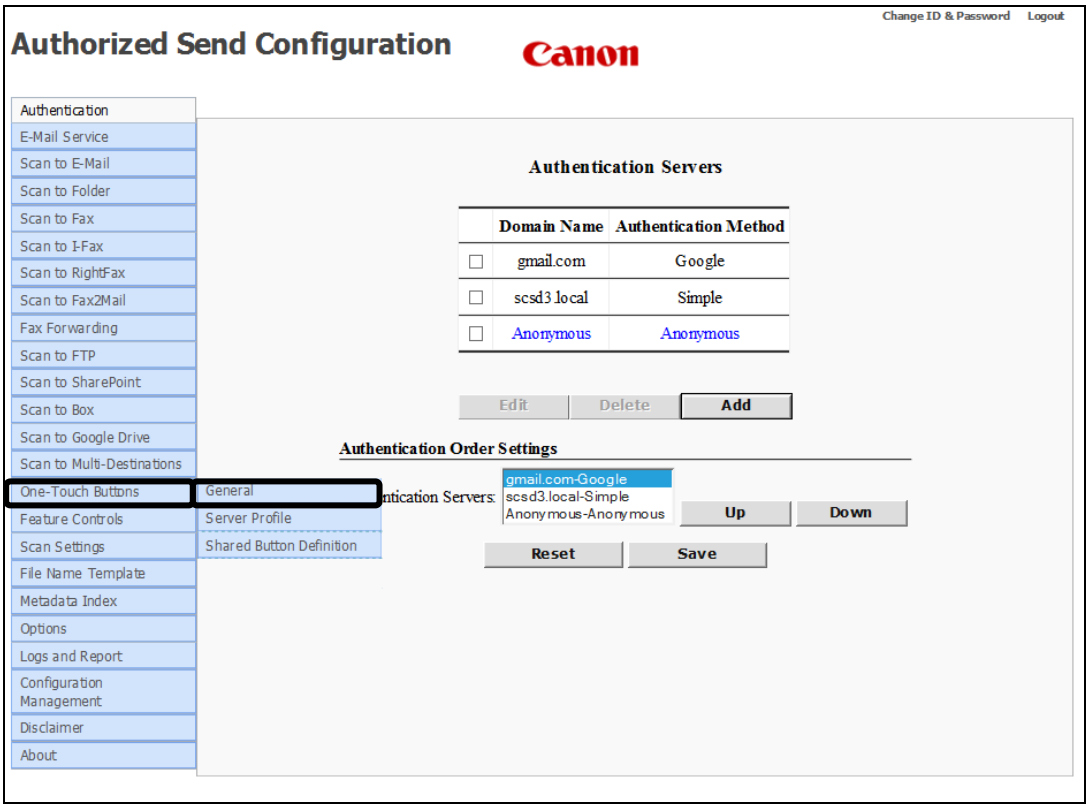
2.18 Configuring the One-Touch Buttons Settings

You can configure the One-Touch Buttons function, which enables users to scan and send documents using predetermined servers, destinations, and scan settings.

IMPORTANT

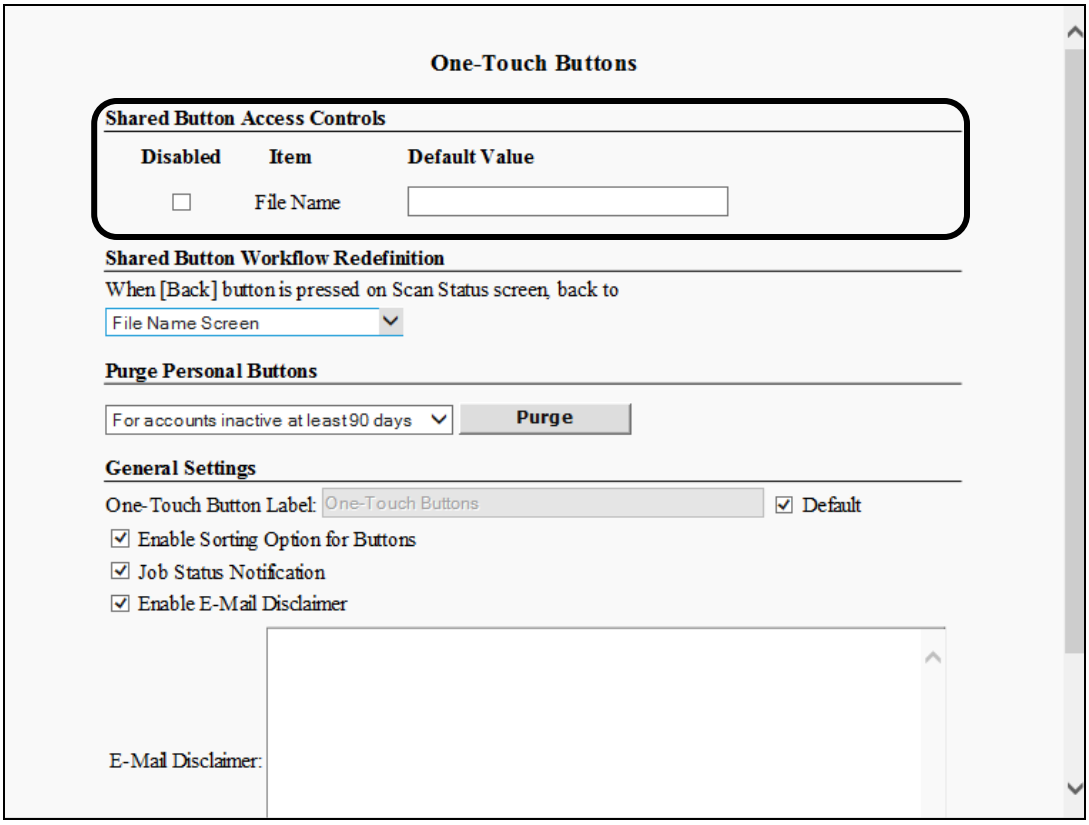
- If an AMS enabled login application is installed and running on the machine, [One-Touch Buttons] may be displayed but disabled on the machine, based on the role of the user that logged on to the login application, even if the One-Touch Buttons function is enabled in the Authorized Send Configuration servlet.
- If an AMS enabled login application is installed and running on the machine, and the login application specifies that scanning is disabled, the functions that were enabled in the Authorized Send Configuration servlet are all disabled on the machine, and an error message is displayed.

1. Click [One-Touch Buttons] → [General].



The One-Touch Buttons screen is displayed.

2. Configure the settings under <Shared Button Access Controls>.



Shared Button Access Controls

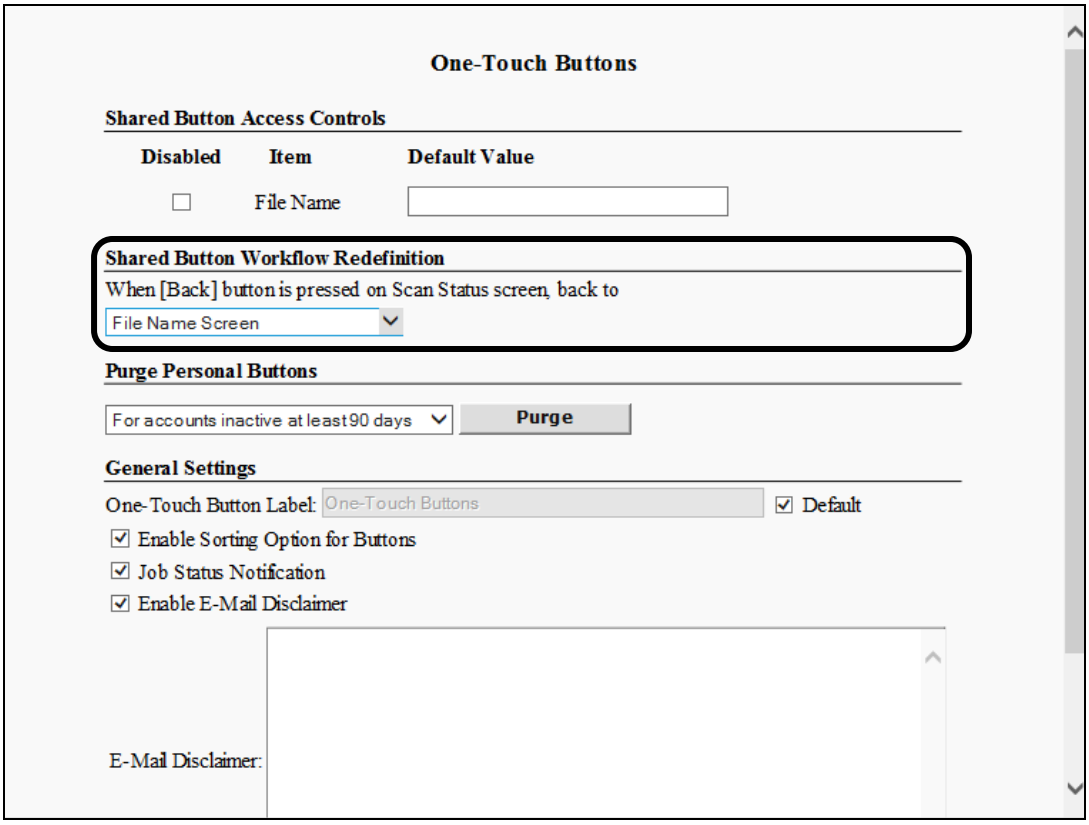
Disabled Item Column

File Name: Select this check box if you want to prevent the user from using the [File Name] text box on the Authorized Send FILE NAME screen on the machine. If you select this check box, the [File Name] text box is disabled and grayed out.

Default Value Column

File Name: Enter the default file name to be displayed in the [File Name] text box on the Authorized Send FILE NAME screen on the machine. This text box is optional. You can enter a string that consists of any character, and a maximum of 251 characters.

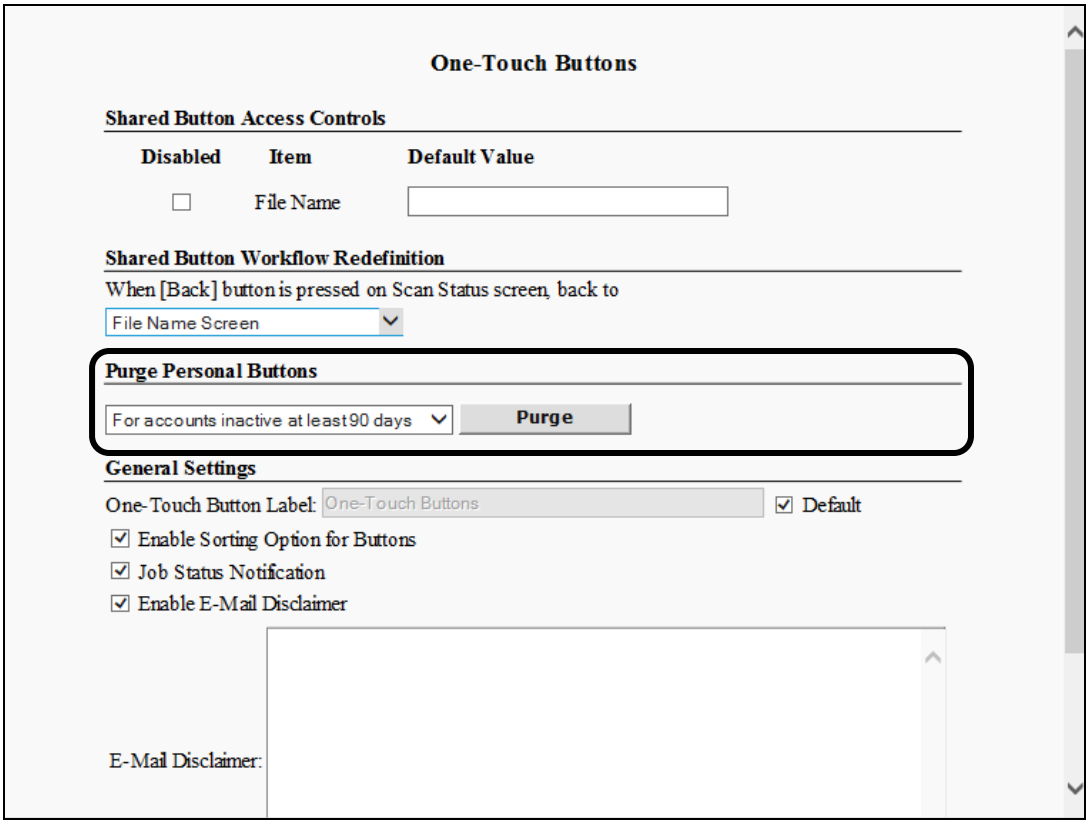
3. Configure the settings under <Shared Button Workflow Redefinition>.



Shared Button Workflow Redefinition

'When [Back] button is pressed' drop-down list:	Select the behavior of the [Back] button on the scan status screen.

4. Configure the settings under <Purge Personal Buttons>.

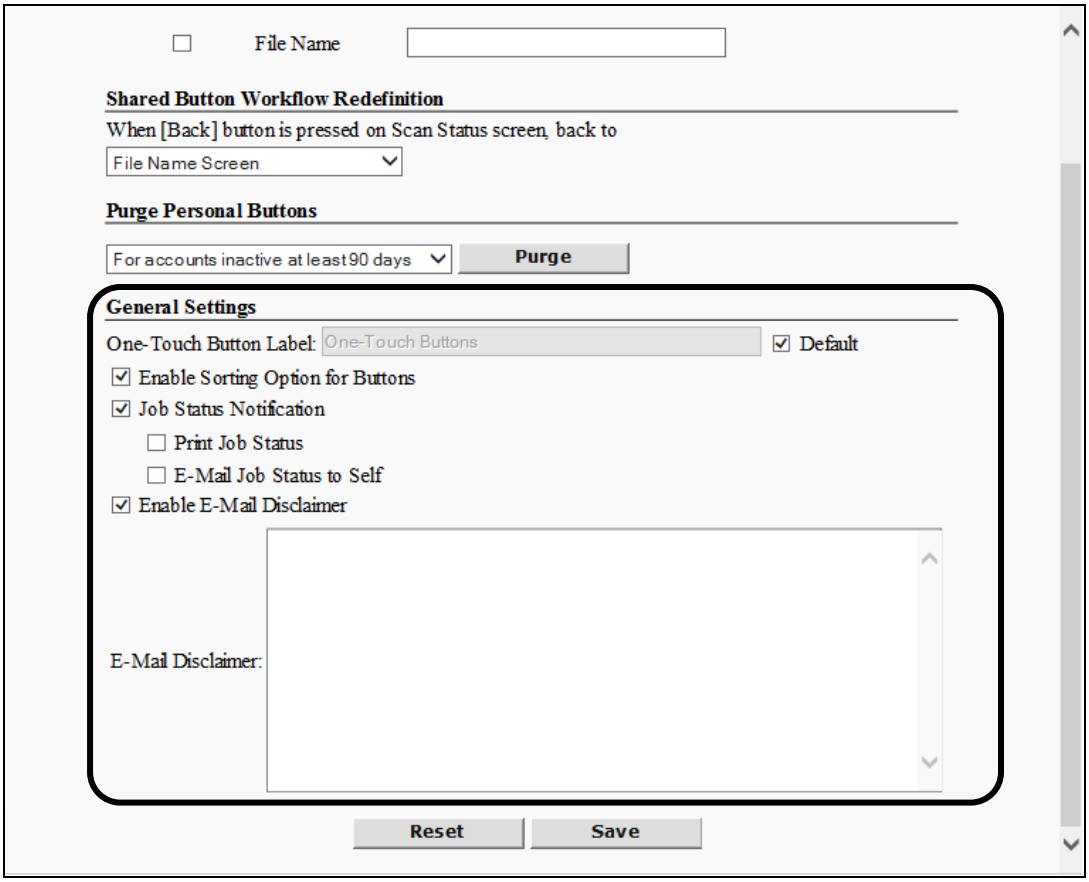


Purge Personal Buttons

Purge drop-down list: Select the user account inactivity threshold where personal buttons will be purged. If a user has not logged in since the set threshold and you click [Purge], all of that user's personal buttons are deleted.

Purge: Click [Purge] to immediate perform the personal button purge operation selected in the corresponding drop-down list.

5. Configure the settings under <General Settings>.



General Settings

One-Touch Button Label:	Enter the label for the [One-Touch Buttons] key that appears on the Authorized Send MAIN screen on the machine. It is a required text box that cannot be left blank. The number of any characters permitted is restricted by the width of the One-Touch Buttons icon.
Default:	Select this check box if you want to use the default One-Touch Button Label setting (‘One-Touch Buttons’). The One-Touch Button Label text box cannot be changed when the Default check box is selected.
Enable Sorting Option for Buttons:	Select this check box if you want to give the user the option to sort the one-touch buttons. If this check box is selected, the [Sort One-Touch Buttons] check box appears on the Authorized Send ONE-TOUCH BUTTONS screen on the machine. The [Enable Sorting Option for Buttons] check box is selected by default.

Job Status Notification:	Select this check box if you want the logged on user of the One-Touch Buttons session to receive confirmation printout or email.
Print Job Status:	The [Print Job Status] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the One-Touch Buttons session to receive a confirmation printout.
E-Mail Job Status to Self:	The [E-Mail Job Status to Self] check box is displayed only when the [Job Status Notification] check box is selected. Select this check box if you want the logged on user of the One-Touch Buttons session to receive a confirmation email.
Enable E-Mail Disclaimer:	Select this check box to append a disclaimer message to all Scan to E-Mail jobs started by a One-Touch Button. The disclaimer appears after the main body of text. This check box is unselected by default
E-Mail Disclaimer:	Enter the text to append to Scan to E-Mail jobs started by a One-Touch Button in the [E-Mail Disclaimer] text box. The text box must have at least one character and no more than 5,000 characters. The [E-Mail Disclaimer] text box appears only if the [Enable E-Mail Disclaimer] check box is enabled.

6. Click [Save].

NOTE

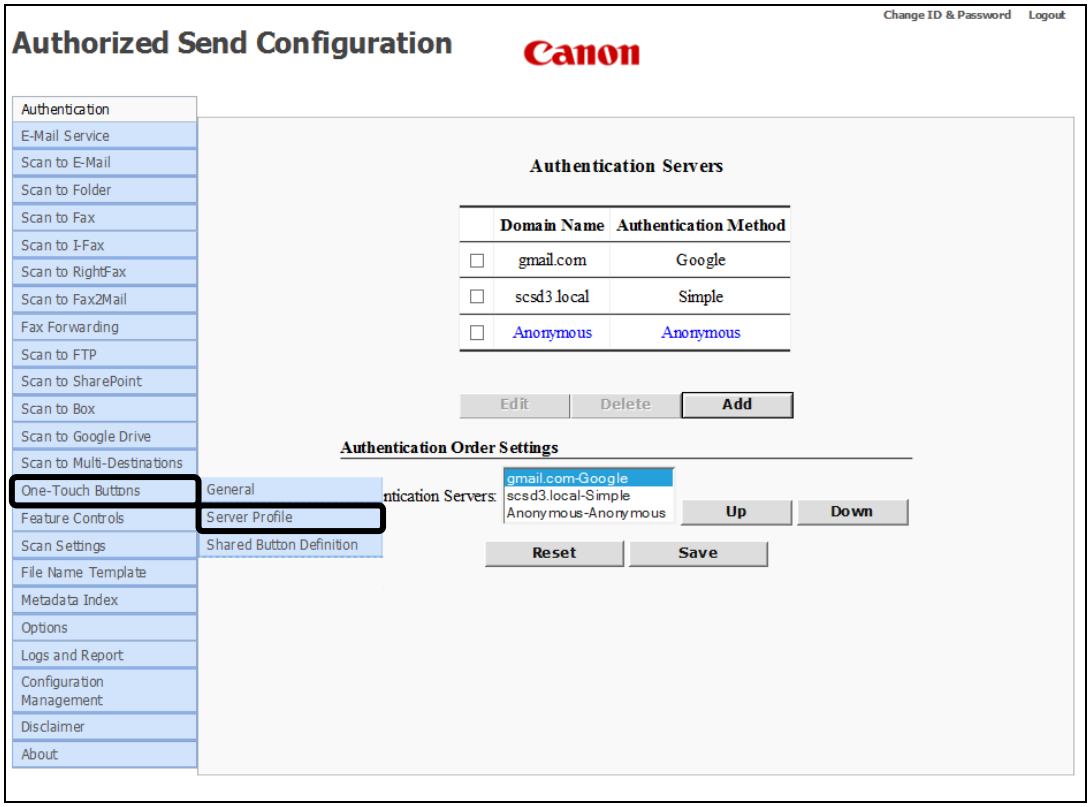
If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.18.1 Creating a Server Profile

You can create a server profile to be used as a destination by any one-touch button.

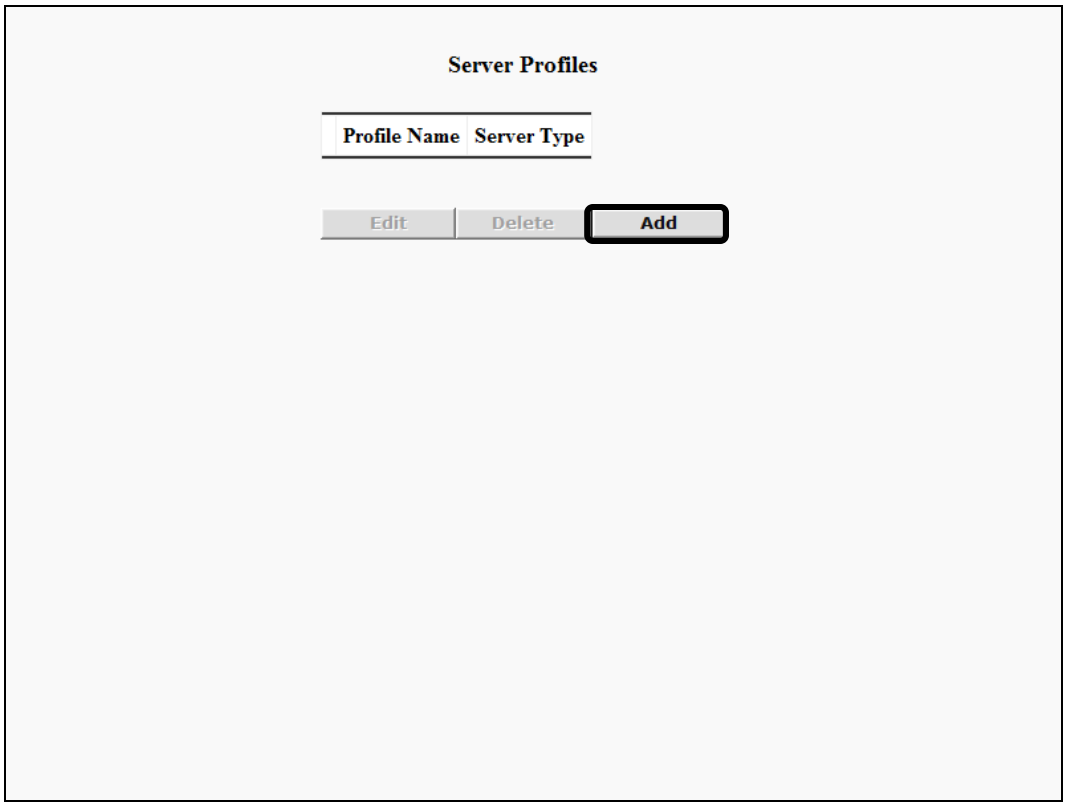
You can create up to 10 Server Profiles.

1. Click [One-Touch Buttons] → [Server Profile].



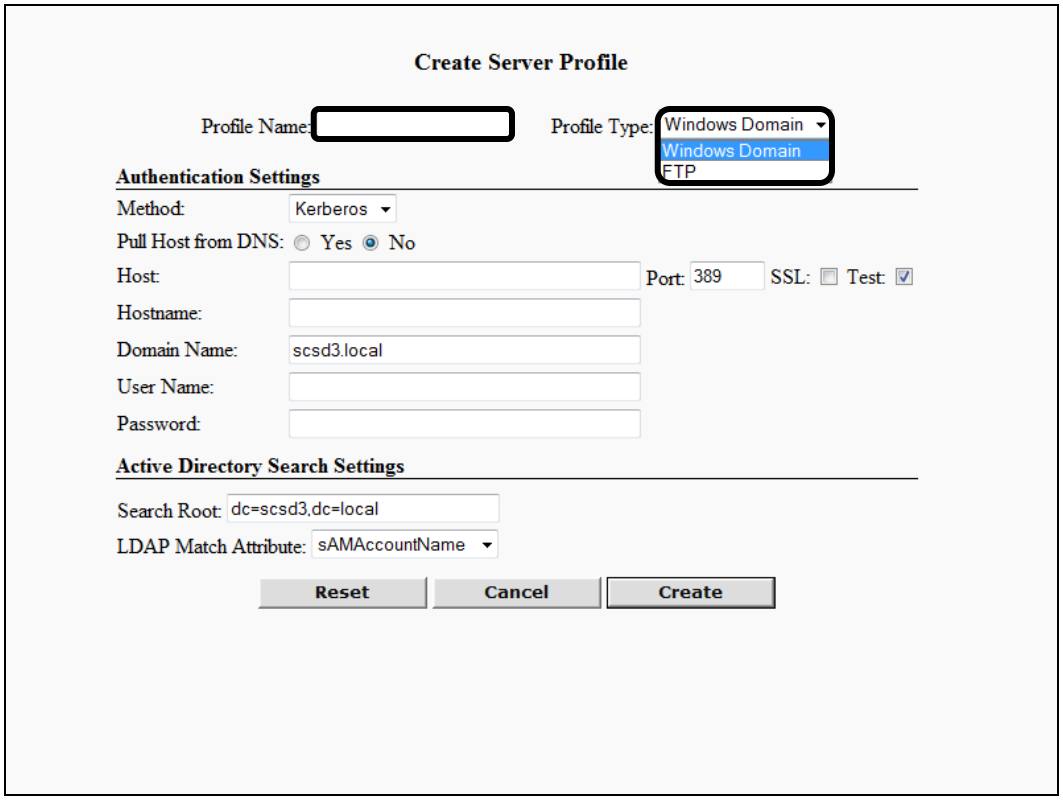
The Server Profiles screen is displayed.

2. Click [Add].



The Create Server Profile screen is displayed.

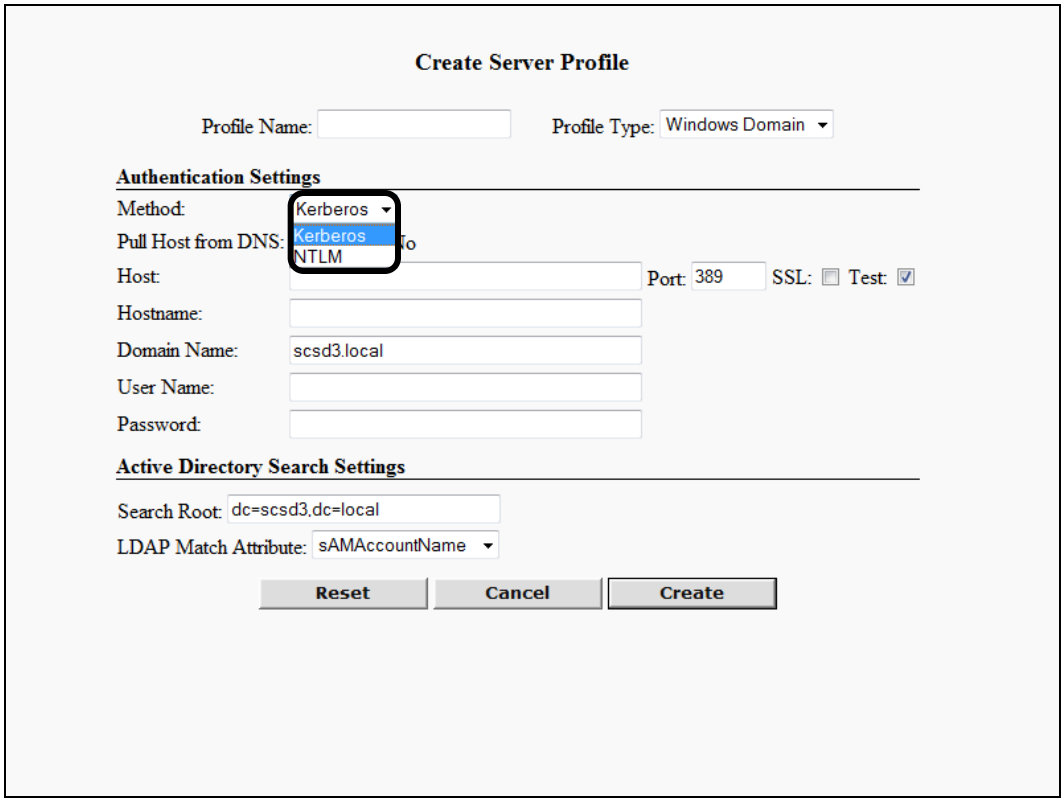
3. Configure the [Profile Name] text box and Profile Type drop-down list.



Profile Name: Enter a name for the server profile. This name is added to the Profile Name list on the Server Profiles screen. It is a required text box that cannot be left blank. The Profile Name is case-sensitive. You can enter a string that consists of any character, and a maximum of 20 characters.

Profile Type: Select [Windows Domain] or [FTP] from the drop-down list as the type of host server Authorized Send is connected to for user authentication. The default setting is 'Windows Domain'.

4. Click the Method drop-down list to select the authentication method.

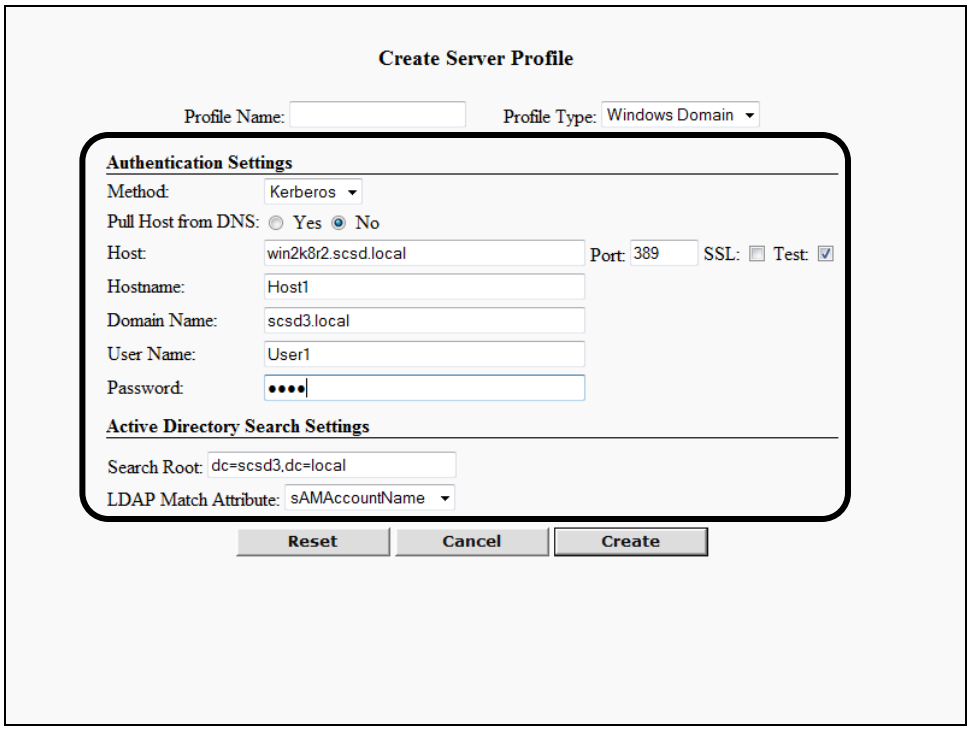


Kerberos: The machine communicates directly to Active Directory.

NTLM: The machine communicates directly to Active Directory.

5. Configure the settings for the selected authentication method.

5.1 If you select [Kerberos] as the authentication method, configure the Authentication Settings and Active Directory Search Settings.



Authentication Settings

Method: Kerberos

Pull Host from DNS: Select [Yes] to automatically pull the host information from the DNS after you click [Create]. Select [No] if you want to manually configure the host information. The default setting is 'No'.

If you select the [Yes] radio button, the first "live" domain controller is used as the authentication server after you click [Create].

Host: This text box is displayed only if Pull Host from DNS is set to 'No'. Enter the DNS name or IP address of the authentication server. You can enter a string that consists of any character, and an unlimited number of characters.

Port: Enter the connecting port number of the authentication server. You can enter a maximum of five numbers. The default port number is '389'.

SSL: Select this check box if you want the authentication server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.

Test: This check box is displayed only if Pull Host from DNS is set to ‘No’. Select this check box if you want the connection to the authentication server to be verified before you save the settings. The [Test] check box is selected by default.

Hostname: This text box is displayed only for Kerberos, and if Pull Host from DNS is set to ‘No’. Enter the host name of the authentication server. This is a required text box that cannot be left blank. You can enter a string that consists of any character, and an unlimited number of characters.

Domain Name: Enter the authentication server domain for this device. You can enter a string that consists of any character, and an unlimited number of characters. The default value is pulled from the device.

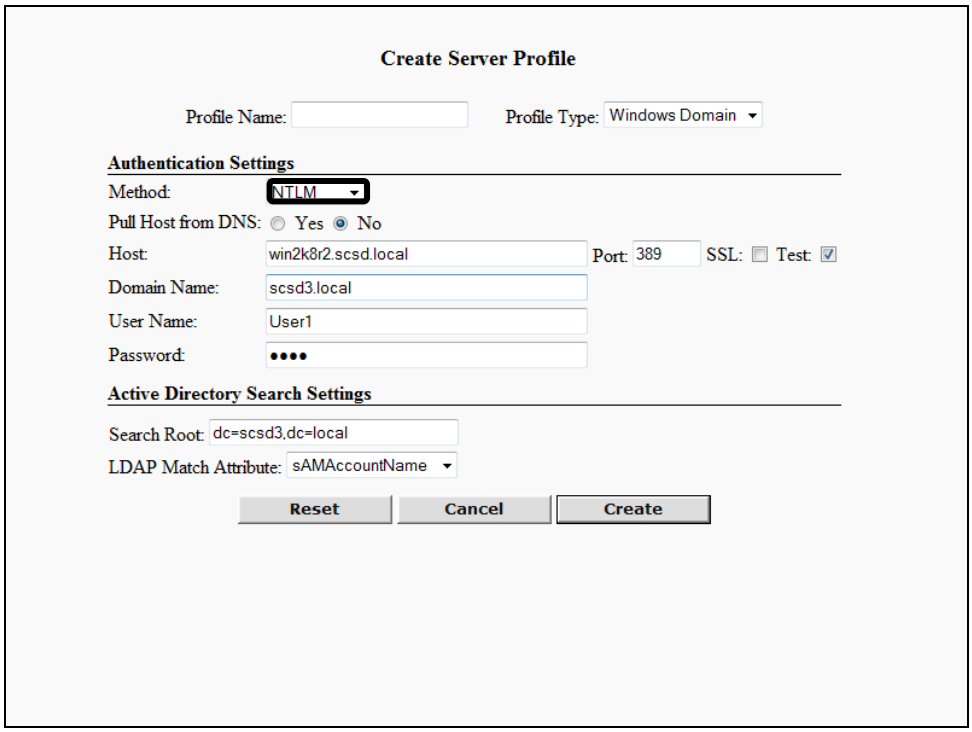
User Name: Enter the user name to use when you sign in on the Authorized Send SIGN IN screen on the machine. This user name is used when the user’s own credentials cannot access the scan’s target destination. You can enter a string that consists of any character, and an unlimited number of characters.

Password: Enter the password to use when you sign in on the Authorized Send SIGN IN screen on the machine. This password is used when the user’s own credentials cannot access the scan’s target destination. You can enter a string that consists of any character, and an unlimited number of characters.

Active Directory Search Settings

Search Root:	Specify the search root for searching the user's home directory via LDAP. Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. It is a required text box that cannot be left blank. You can enter a string that consists of any character, and an unlimited number of characters. The default value for the [Search Root] text box is blank if the [Domain Name] text box is blank. If the [Domain Name] text box is populated, the [Search Root] text box is automatically populated based on the text entered in the [Domain Name] text box.
LDAP Match Attribute:	Select [sAMAccountName] or [userPrincipalName] from the drop-down list to determine which attribute to use for LDAP match. This enables you to search for the user's Home Directory. The default setting is 'sAMAccountName'.

5.2 If you select [NTLM] as the authentication method, configure the Authentication Settings and Active Directory Search Settings.



Authentication Settings

Method: NTLM

Pull Host from DNS: Select [Yes] to automatically pull the host information from the DNS after you click [Create]. Select [No] if you want to manually configure the host information. The default setting is 'No'.

If you select the [Yes] radio button, the first "live" domain controller is used as the authentication server after you click [Create].

Host: This text box is displayed only if Pull Host from DNS is set to 'No'. Enter the DNS name or IP address of the authentication server. You can enter a string that consists of any character, and an unlimited number of characters.

Port: Enter the connecting port number of the authentication server. You can enter a maximum of five numbers. The default port number is '389'.

SSL: Select this check box if you want the authentication server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.

Test: This check box is displayed only if Pull Host from DNS is set to ‘No’. Select this check box if you want the connection to the authentication server to be verified before you save the settings. The [Test] check box is selected by default.

Domain Name: Enter the authentication server domain for this device. You can enter a string that consists of any character, and an unlimited number of characters. The default value is pulled from the device.

User Name: Enter the user name to use to sign in on the Authorized Send SIGN IN screen on the machine. This user name is used when the user’s own credentials cannot access the scan’s target destination. You can enter a string that consists of any character, and an unlimited number of characters.

Password: Enter the password to use when you sign in on the Authorized Send SIGN IN screen on the machine. This password is used when the user’s own credentials cannot access the scan’s target destination. You can enter a string that consists of any character, and an unlimited number of characters.

Active Directory Search Settings

Search Root: Specify the search root for searching the user’s home directory via LDAP.

Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts.

It is a required text box that cannot be left blank. You can enter a string that consists of any character, and an unlimited number of characters. The default value for the [Search Root] text box is blank if the [Domain Name] text box is blank. If the [Domain Name] text box is populated, the [Search Root] text box is automatically populated based on the text entered in the [Domain Name] text box.

LDAP Match Attribute:	Select [sAMAccountName] or [userPrincipalName] from the drop-down list to determine which attribute to use for LDAP match. This enables you to search for the user's Home Directory. The default setting is 'sAMAccountName'.

6. Click [Create].

   If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

   To cancel creating the server profile and return to the Server Profiles screen, click [Cancel].

   A message is displayed informing you that the configuration has been saved, and the screen returns to the Server Profiles screen.

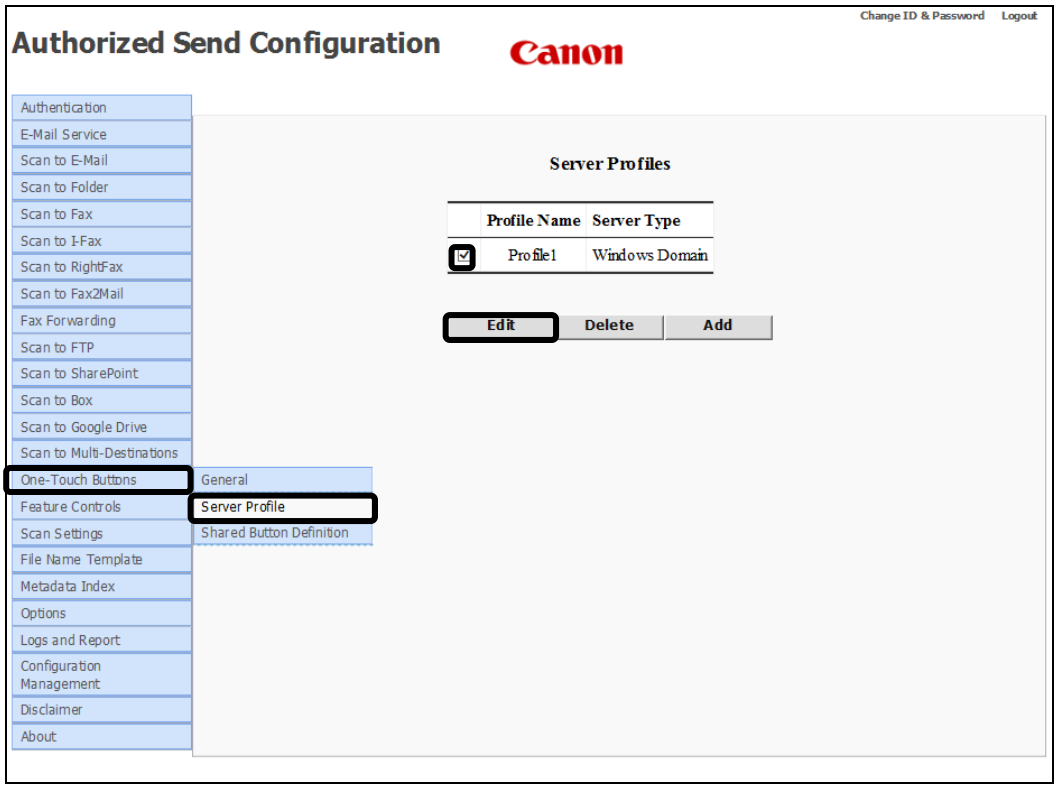
IMPORTANT

- Select the [Test] check box next to <Host> if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message is displayed. Enter the correct information → click [Save].

2.18.2 Editing a Server Profile

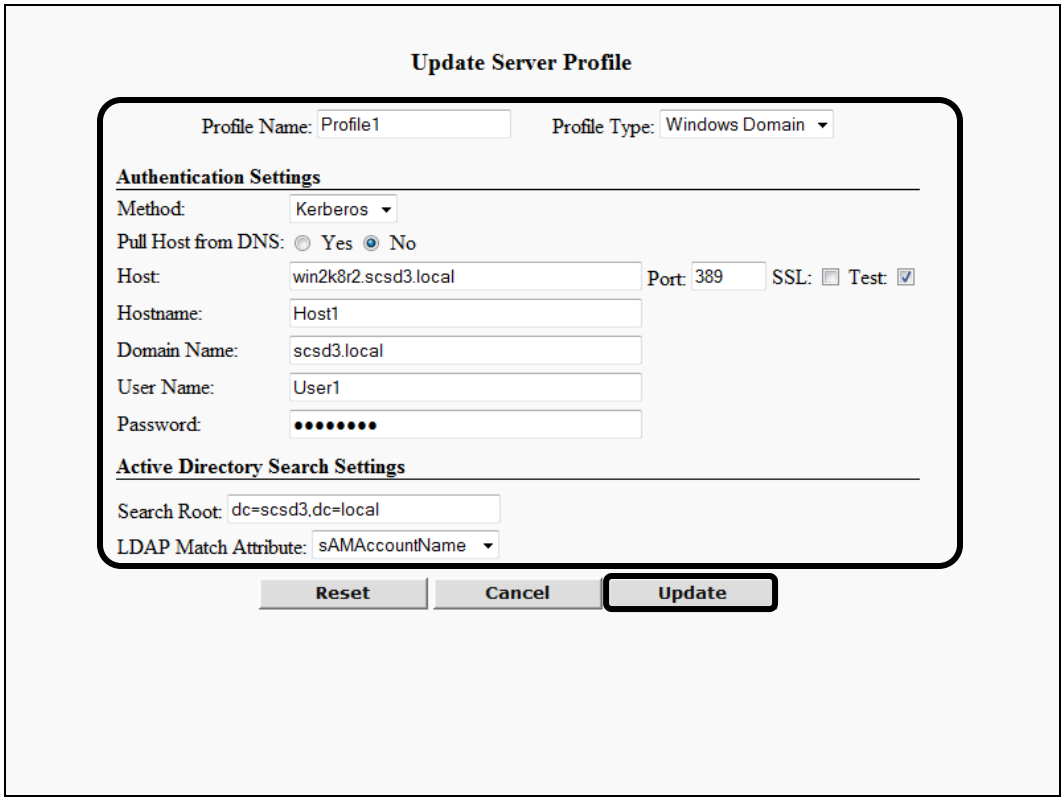
You can edit a previously created server profile name from the Server Profiles configuration screen.

1. Click [One-Touch Buttons] → [Server Profile] → select the check box next to the server profile name you want to edit → click [Edit].



The Update Server Profile screen is displayed.

2. Edit the settings for the server profile, as necessary → click [Update].



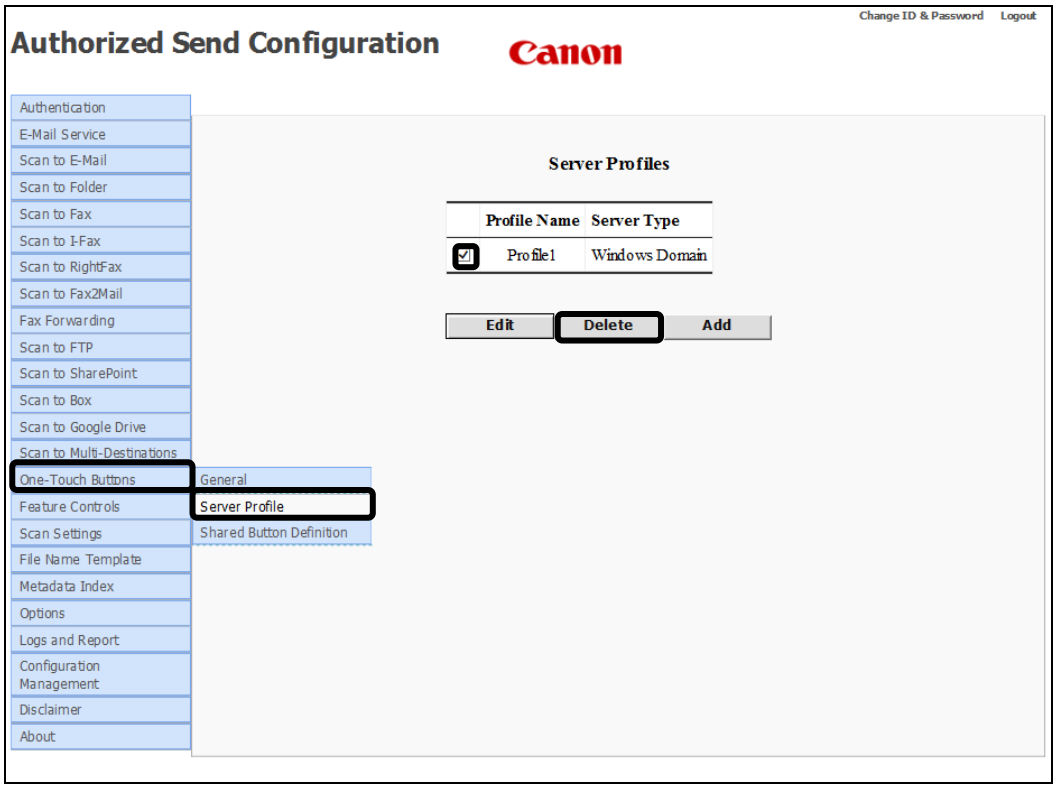
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the server profile name and return to the Server Profiles configuration screen, click [Cancel].

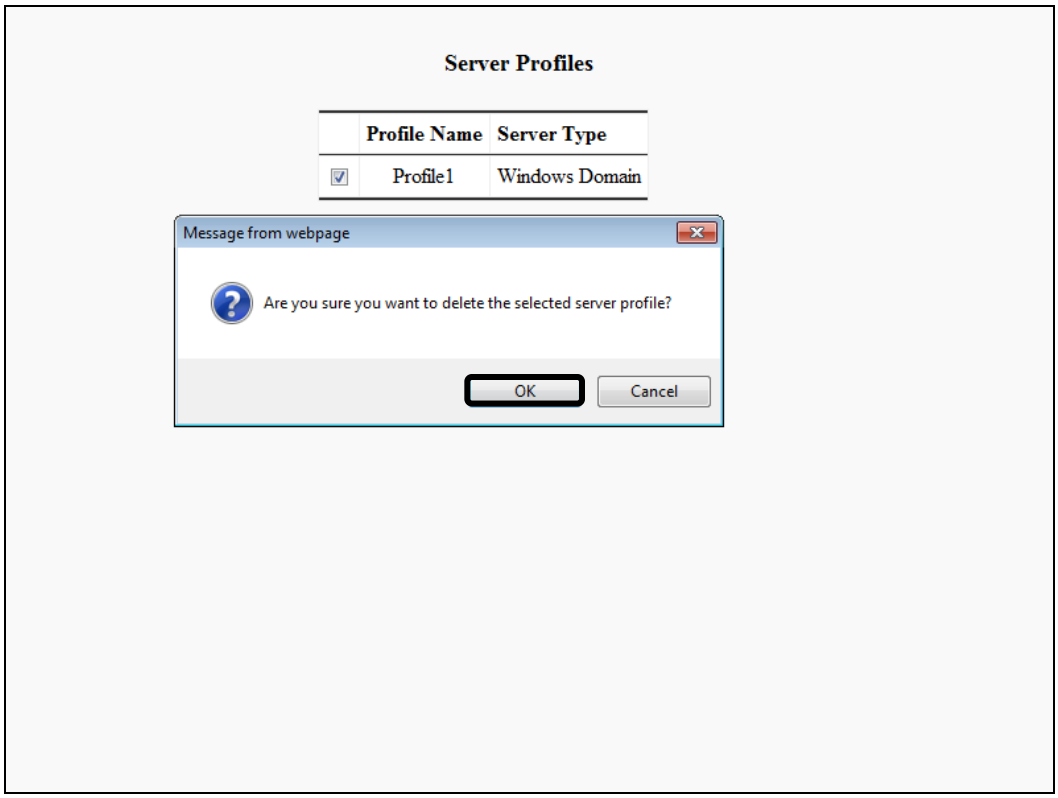
2.18.3 Deleting a Server Profile

You can delete a previously created server profile name from the Server Profiles configuration screen.

1. Click [One-Touch Buttons] ➞ [Server Profile] ➞ select the check box next to the server profile name you want to delete ➞ click [Delete].



2. Click [OK] on the confirmation dialog box.



If you do not want to delete the server profile name, click [Cancel].

The server profile name is deleted from the list.

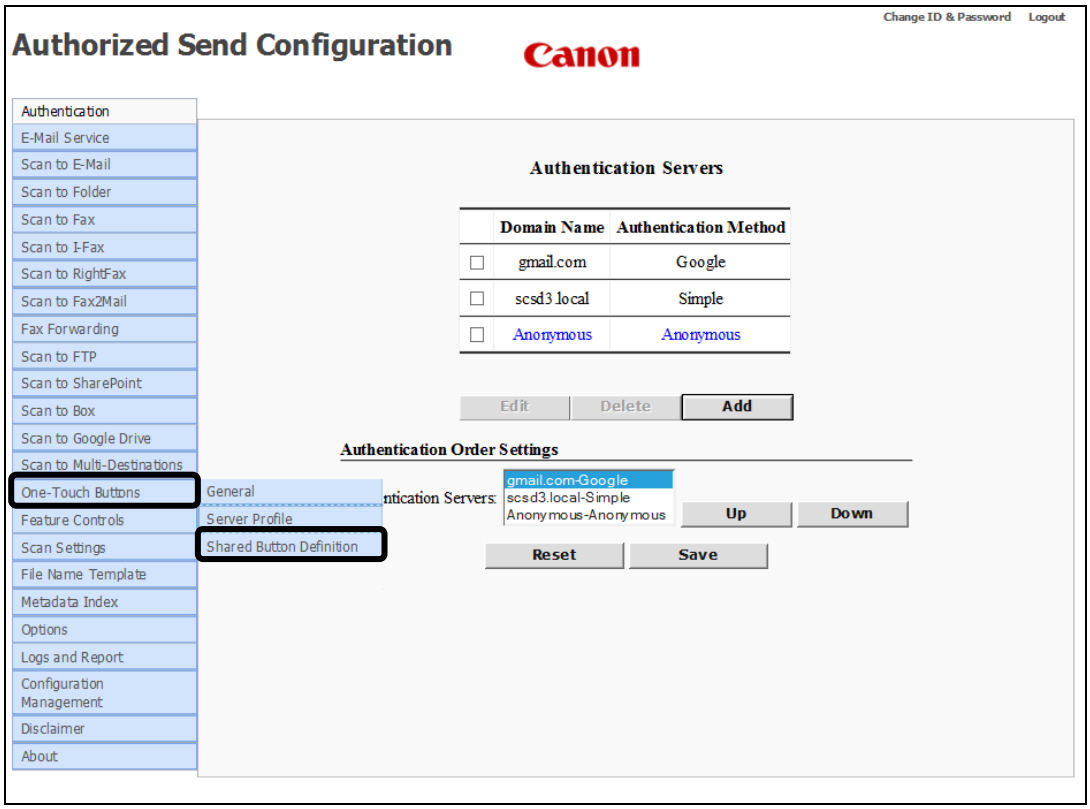
2.18.4 Creating a Shared Button Definition

You can create a shared button definition that defines a button's name, destination settings, server that is used, scan settings profile, and metadata settings. Shared buttons are available to all users.

You can create up to 12 shared button definitions.

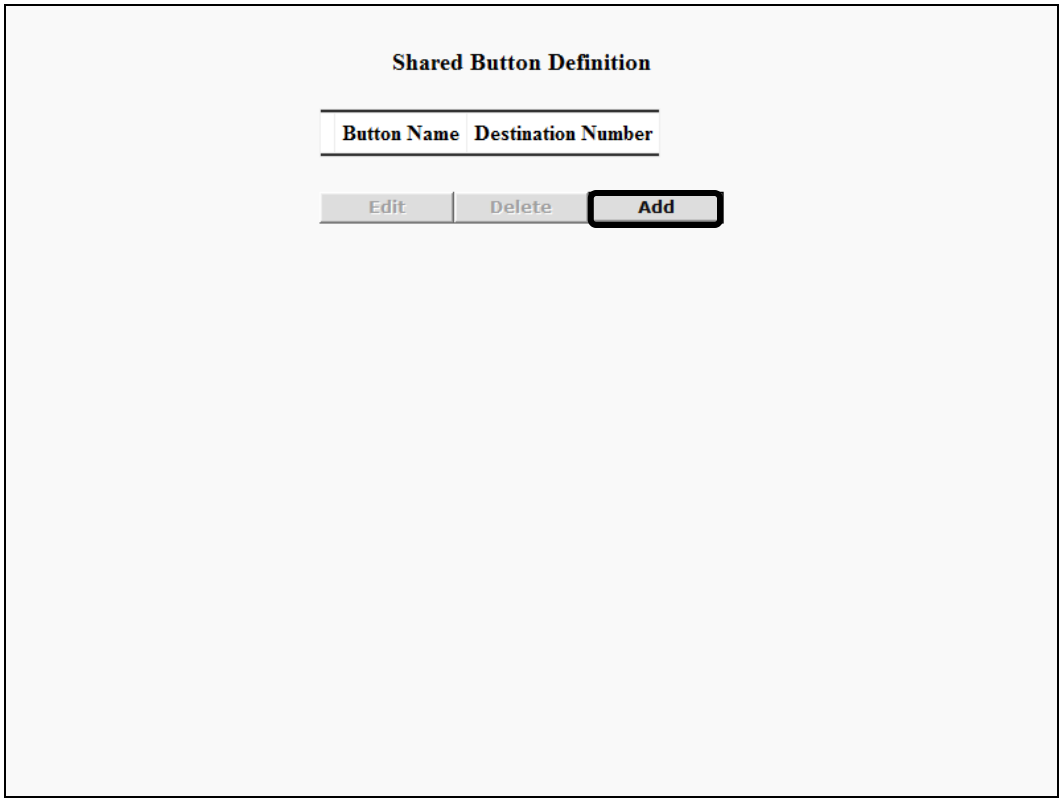
---

1. Click [One-Touch Buttons] → [Shared Button Definition].



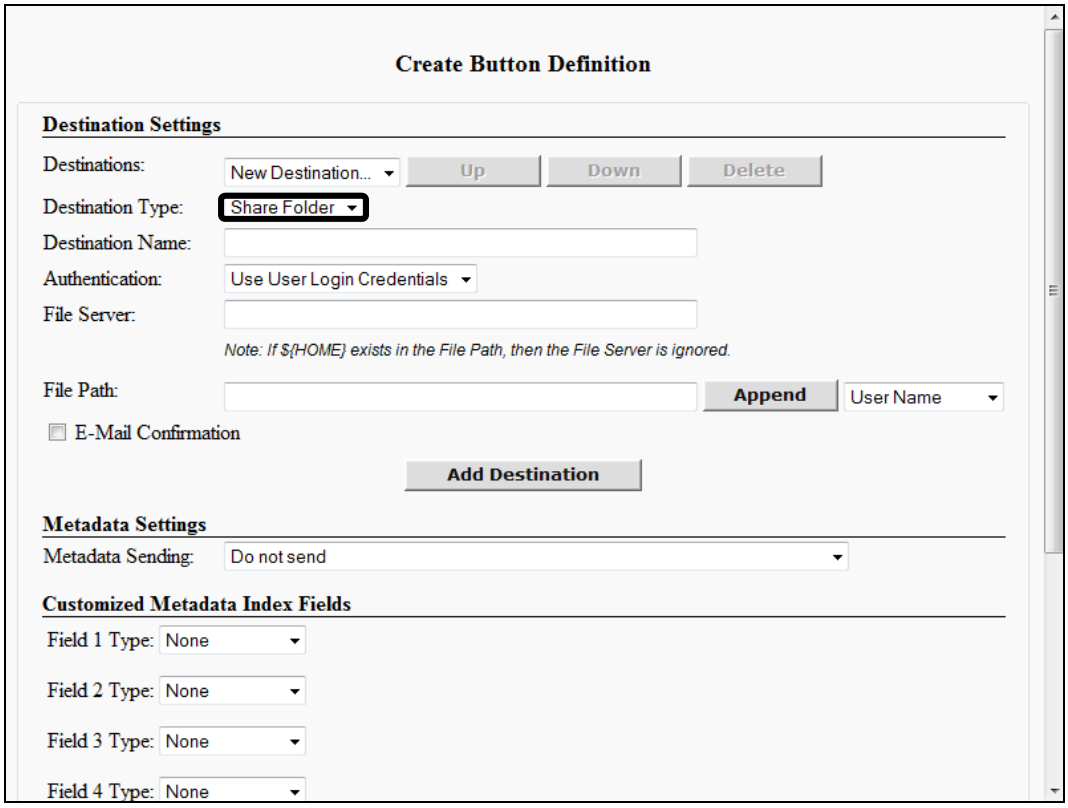
The Button Definition screen is displayed.

2. Click [Add].



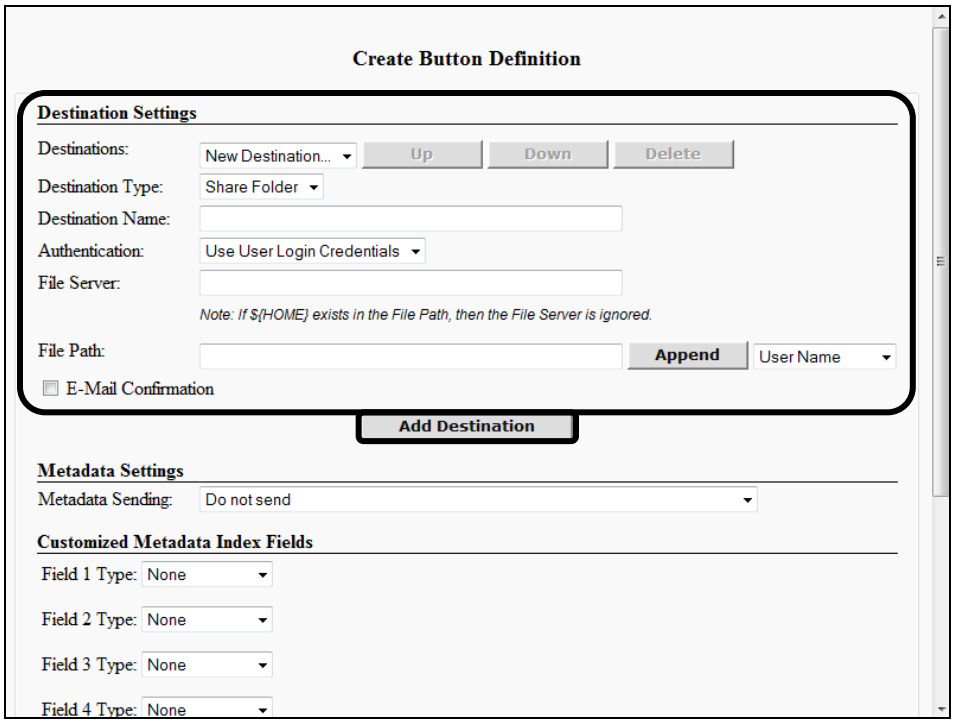
The Create Button Definition screen is displayed.

3. Select [Share Folder], [FTP Server], [SharePoint], [E-Mail], [I-FAX], [FAX], [RightFax], [Fax2Mail], [Box], or [Google Drive] from the Destination Type drop-down list to select the destination type.



4. Configure the settings for the selected destination type.

    4.1 If you select [Share Folder] as the destination type, configure the Destination Settings → click [Add Destination].



Destination Settings

Destination Type: Share Folder

Destination Name: Enter a destination name to be added to the Destinations list box. This text box is required. You can enter a string that consists of any character, and a maximum of 40 characters.

Authentication: Select [Use User Login Credentials], [User Server Profile], or [Use Local Credentials] from the drop-down list to authenticate to the folder. The default setting is 'Use User Login Credentials'.

File Server: Enter the DNS name or IP address to where you want to send scanned documents. This text box is required. You can enter a string that consists of any character, and an unlimited number of characters.

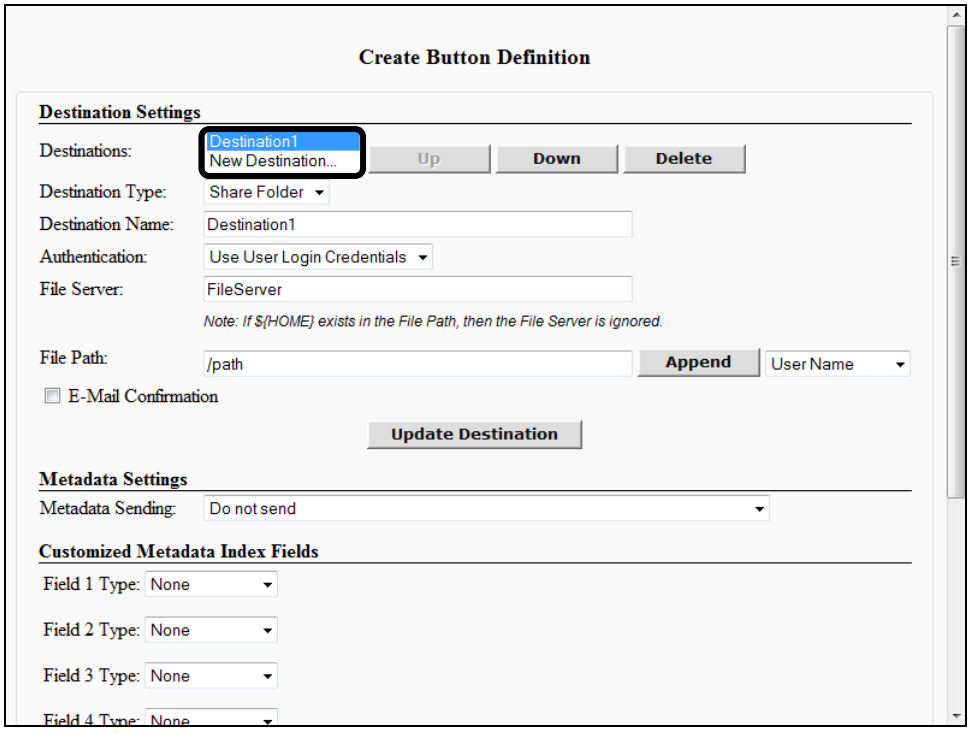
File Path: Enter the path of the folder to where you want to send scanned documents. This text box is required. You can enter a string that consists of any character, and an unlimited number of characters.

Append: Click [Append] to add a dynamic variable (set in the Append drop-down list) to the string in the [File Path] text box.

Append drop-down: Select a dynamic variable that is added to the string in the [File Path] text box after you click [Append]. The default value is 'User Name'.

E-Mail Confirmation: Select this check box if you want Authorized Send to e-mail a confirmation message to the user at the completion of a Scan to Folder job. An e-mail is sent regardless of success or failure of the job.

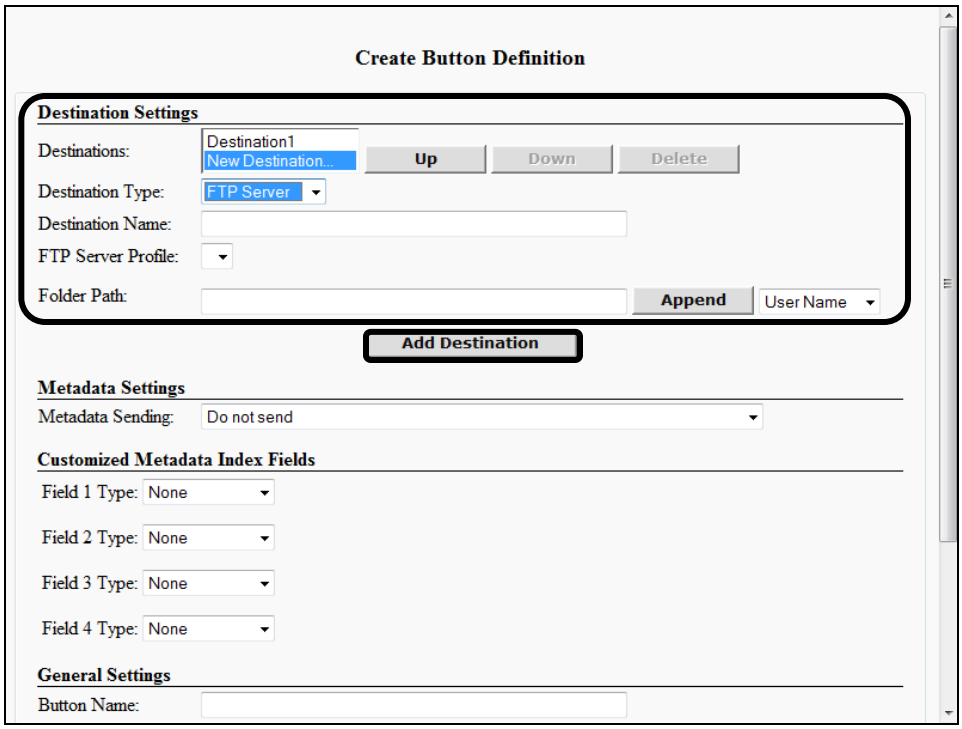
The destination is added to the Destinations list box.



If you want to move a destination's location up or down in the list, select the destination → click [Up] or [Down].

If you want to delete a destination, select the destination → click [Delete].

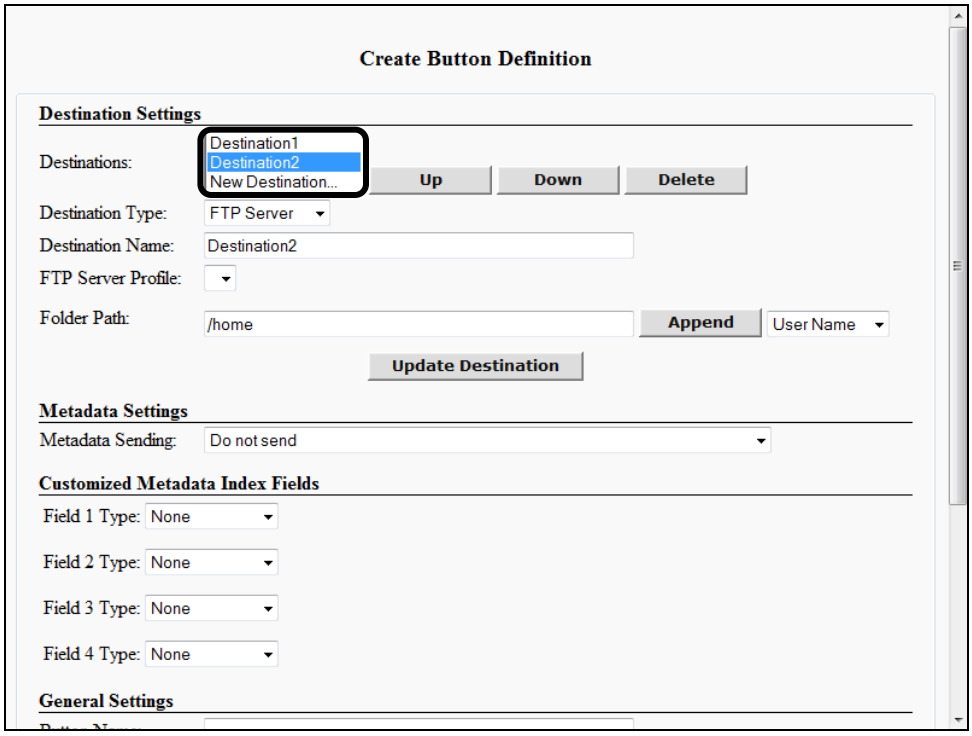
4.2 If you select [FTP Server] as the destination type, configure the Destination Settings → click [Add Destination].



Destination Settings

Destination Type:	FTP Server
Destination Name:	Enter a destination name that is added to the Destinations list box. This text box is required. You can enter a string that consists of any character, and a maximum of 40 characters.
FTP Server Profile:	Select an FTP server profile from the drop-down list.
Folder Path:	Enter the path of the folder to where you want to send scanned documents. You can enter a string that consists of any character, and a maximum of 255 characters.
Append:	Click [Append] to add a dynamic variable (set in the Append drop-down list) to the string in the [Folder Path] text box.
Append drop-down:	Select a dynamic variable that is added to the string in the [Folder Path] text box after you click [Append]. The default value is ‘User Name’.

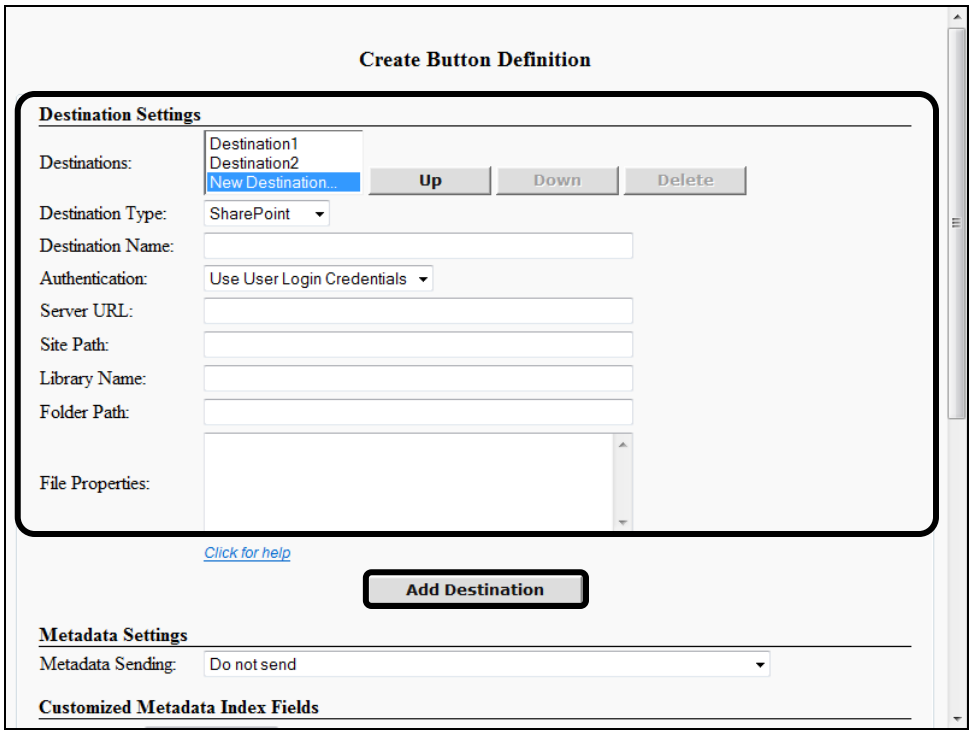
The destination is added to the Destinations list box.



If you want to move a destination's location up or down in the list, select the destination → click [Up] or [Down].

If you want to delete a destination, select the destination → click [Delete].

4.3 If you select [SharePoint] as the destination type, configure the Destination Settings → click [Add Destination].



Destination Settings

Destination Type: SharePoint

Destination Name: Enter a destination name that is added to the Destinations list box. This text box is required. You can enter a string that consists of any character, and a maximum of 40 characters.

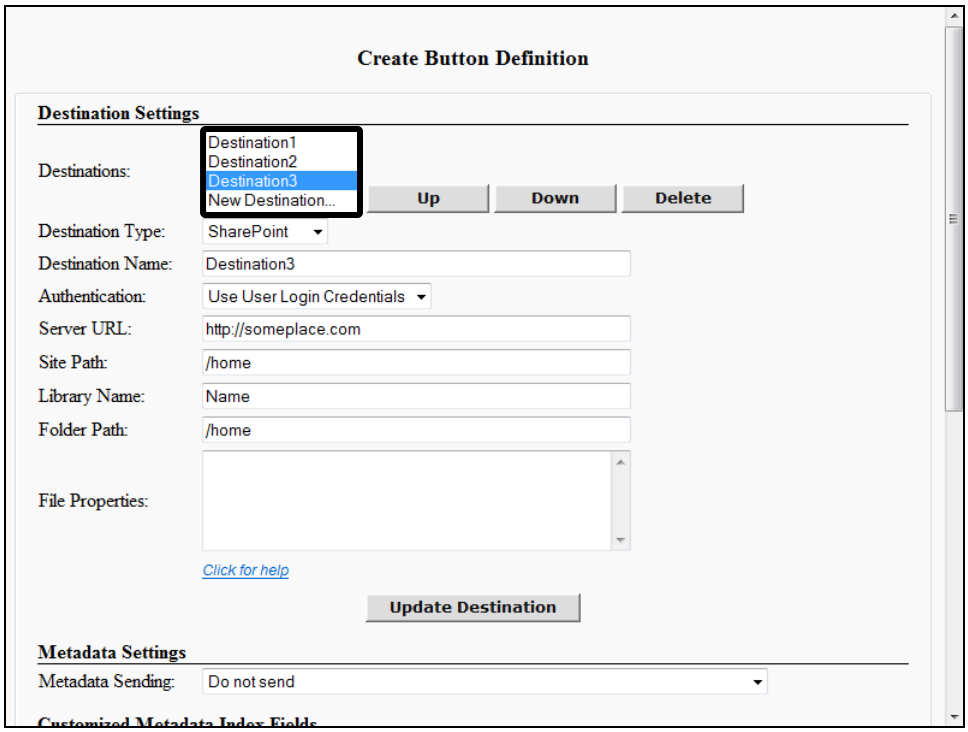
Authentication: Select [Use User Login Credentials], [User Server Profile], or [Use Local Credentials] from the drop-down list to authenticate to the SharePoint server. The default setting is 'Use User Login Credentials'.

Server URL: Enter the URL address to where you want to send scanned documents. You can enter a string that consists of any character, and an unlimited number of characters.

Site Path: Enter the path to the site where you want to send scanned documents. This is an optional text box. You can enter a string that consists of any character, and an unlimited number of characters.

Library Name:	Enter the name of the library where you want to send scanned documents. You can enter a string that consists of any character, and an unlimited number of characters.
Folder Path:	Enter the path of the folder under the library to where you want to send scanned. This is an optional text box. You can enter a string that consists of any character, and an unlimited number of characters.
File Properties:	Enter the property values needed to upload to a SharePoint library location. Each line should contain only one property name and its value in the format of 'propertyName=propertyValue'. You can enter up to 15 lines, and each line can contain any characters.
Click for help:	Click this hyperlink to open a browser window, which shows examples of the proper way to enter the property values for the [File Properties] text box.

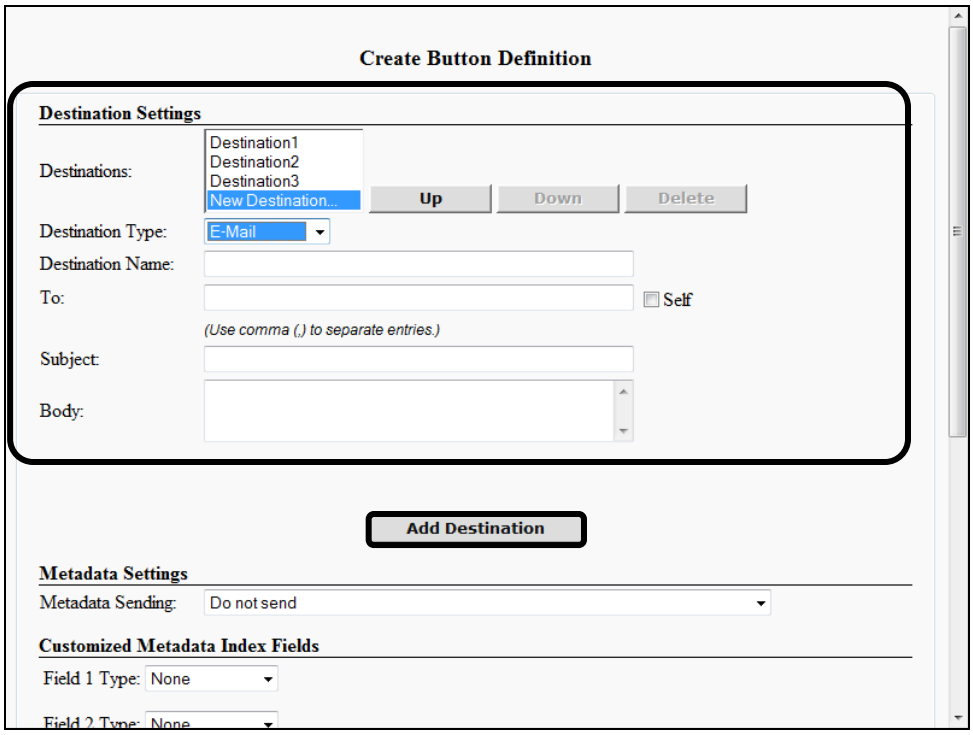
The destination is added to the Destinations list box.



If you want to move a destination's location up or down in the list, select the destination → click [Up] or [Down].

If you want to delete a destination, select the destination → click [Delete].

4.4 If you select [E-Mail] as the destination type, configure the Destination Settings → click [Add Destination].



Destination Settings

Destination Type: E-Mail

Destination Name: Enter a destination name that is added to the Destinations list box. This text box is required. You can enter a string that consists of any character, and a maximum of 40 characters.

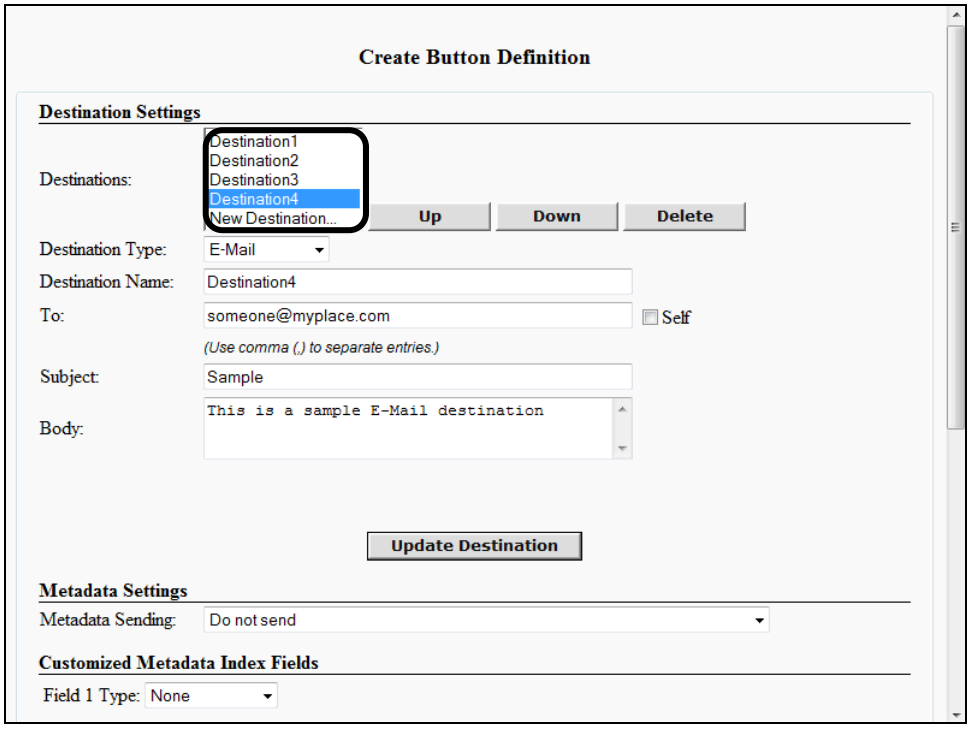
To: Enter an e-mail address. You can enter a string that consists of any character, and a maximum of 255 characters.

Self: Select this check box to display the e-mail address of the user logged on to Authorized Send in the [To] text box.

Subject: Enter a subject. You can enter a string that consists of any character, and a maximum of 255 characters.

Body: Enter an e-mail message. You can enter a string that consists of any character, and a maximum of 255 characters

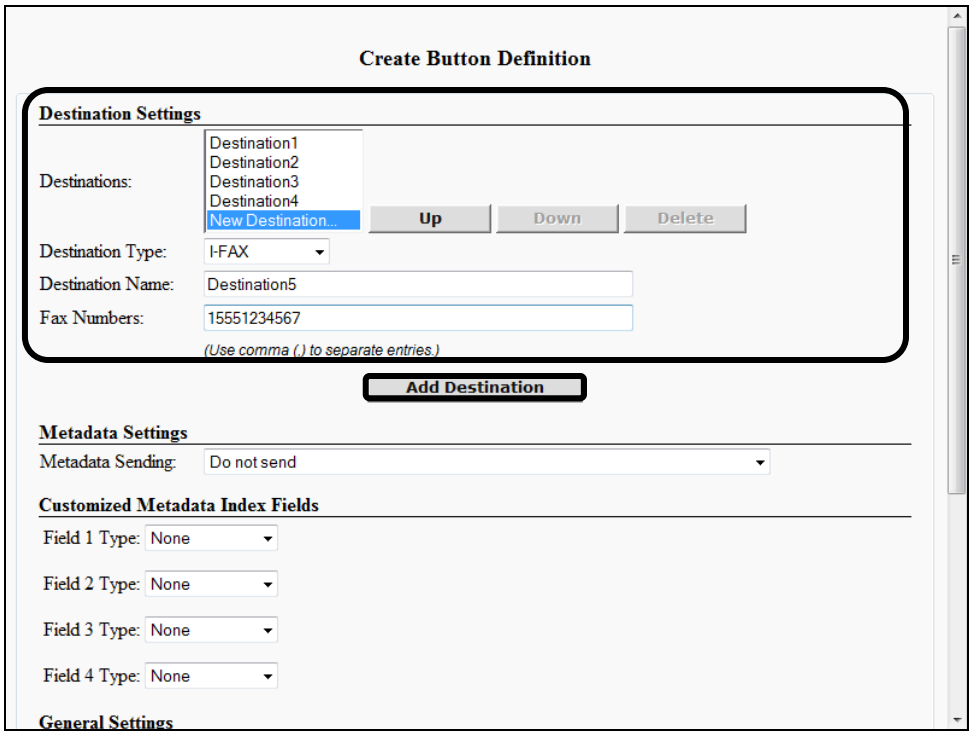
The destination is added to the Destinations list box.



If you want to move a destination's location up or down in the list, select the destination → click [Up] or [Down].

If you want to delete a destination, select the destination → click [Delete].

4.5 If you select [I-FAX] as the destination type, configure the Destination Settings → click [Add Destination].



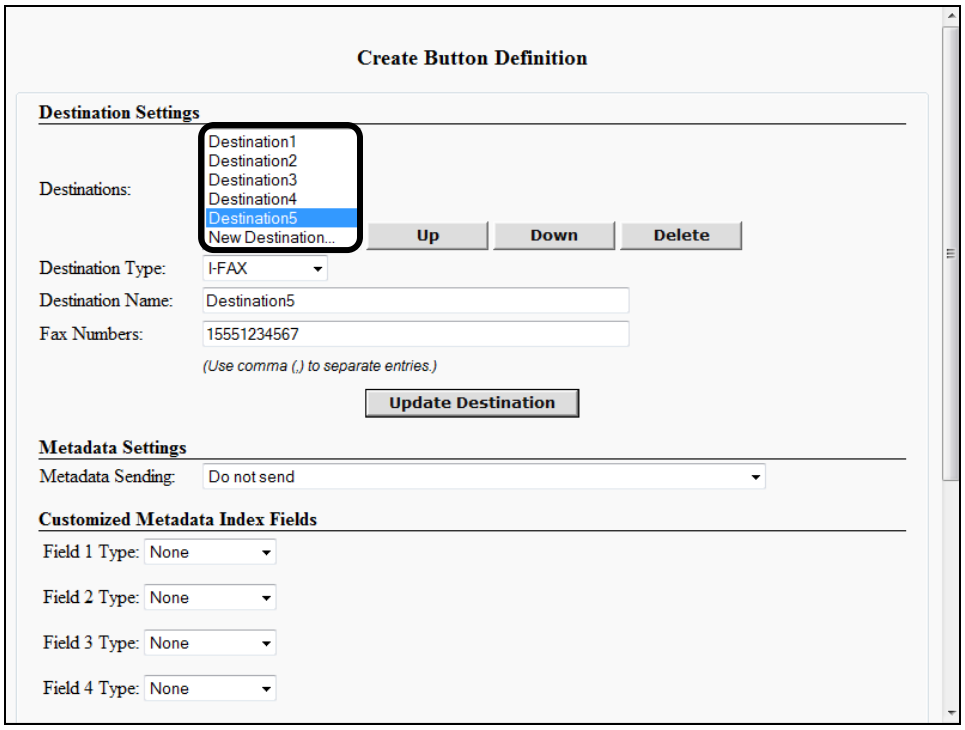
Destination Settings

Destination Type: I-FAX

Destination Name: Enter a destination name that is added to the Destinations list box. This text box is required. You can enter a string that consists of any character, and a maximum of 40 characters.

Fax Numbers: Enter a fax number, or fax numbers separated by commas or semicolons. You can enter a string of alphanumeric characters, periods (“.”), hyphens (“-“), spaces (‘ “), and underscores (“_”), separated by commas or semicolons, and a maximum of 255 characters.

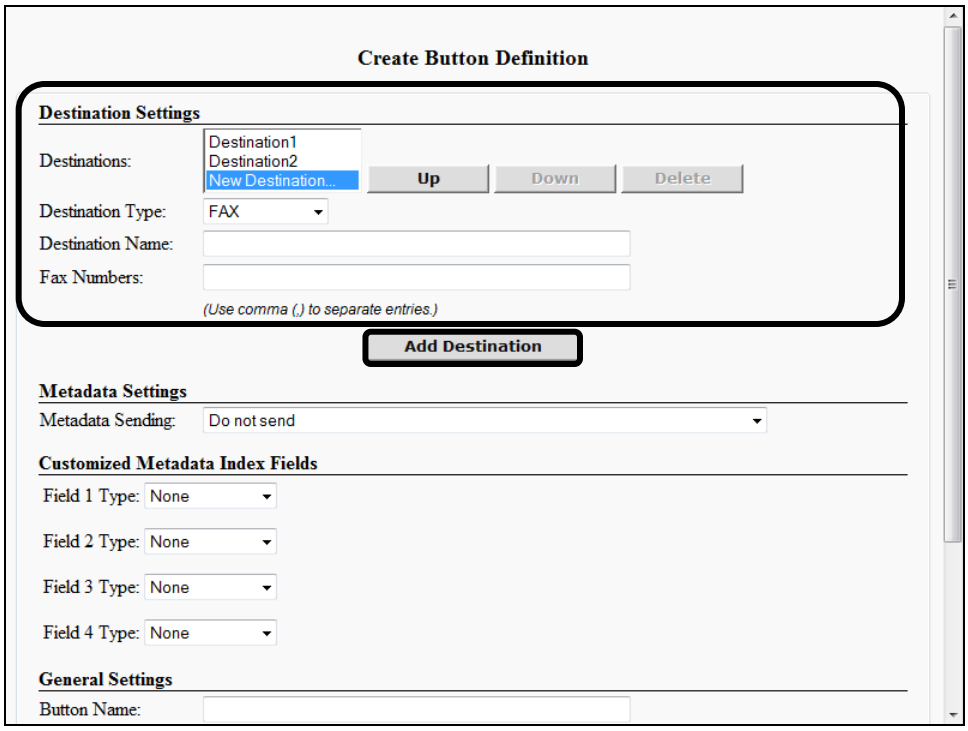
The destination is added to the Destinations list box.



If you want to move a destination's location up or down in the list, select the destination → click [Up] or [Down].

If you want to delete a destination, select the destination → click [Delete].

4.6 If you select [FAX] as the destination type, configure the Destination Settings → click [Add Destination].



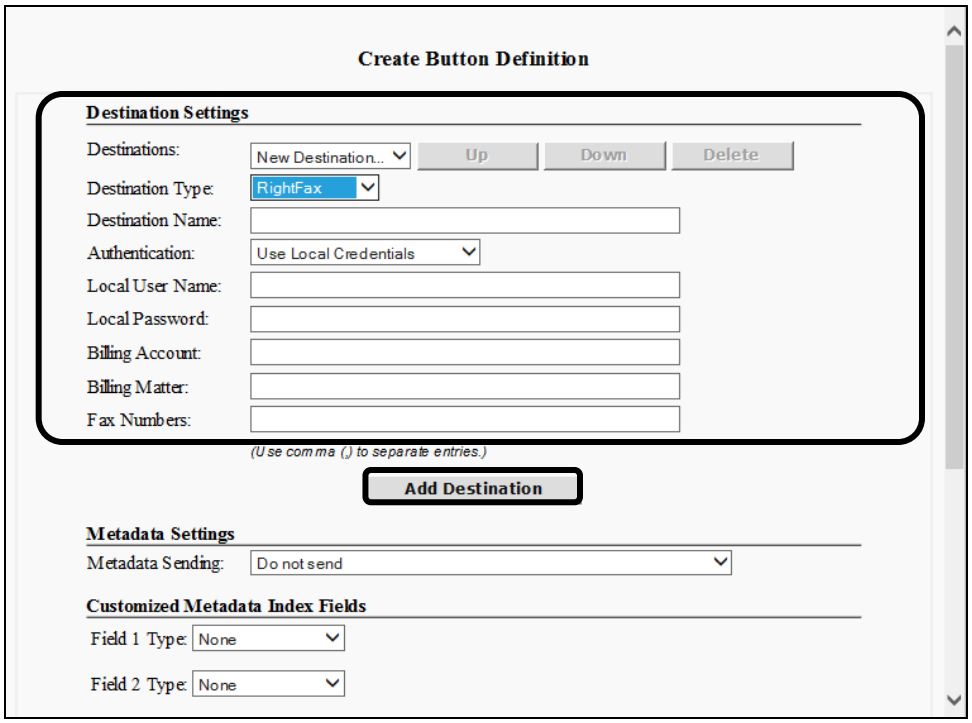
Destination Settings

Destination Type: FAX

Destination Name: Enter a destination name that is added to the Destinations list box. This text box is required. You can enter a string that consists of any character, and a maximum of 40 characters.

Fax Numbers: Enter a fax number, or fax numbers separated by commas. You can enter a string of only numbers separated by commas, and a maximum of 255 characters.

4.7 If you select [RightFax] as the destination type, configure the Destination Settings → click [Add Destination].



Destination Settings

Destination Type: RightFax

Destination Name: Enter a destination name that is added to the Destinations list box. This text box is required. You can enter a string that consists of any character, and a maximum of 40 characters.

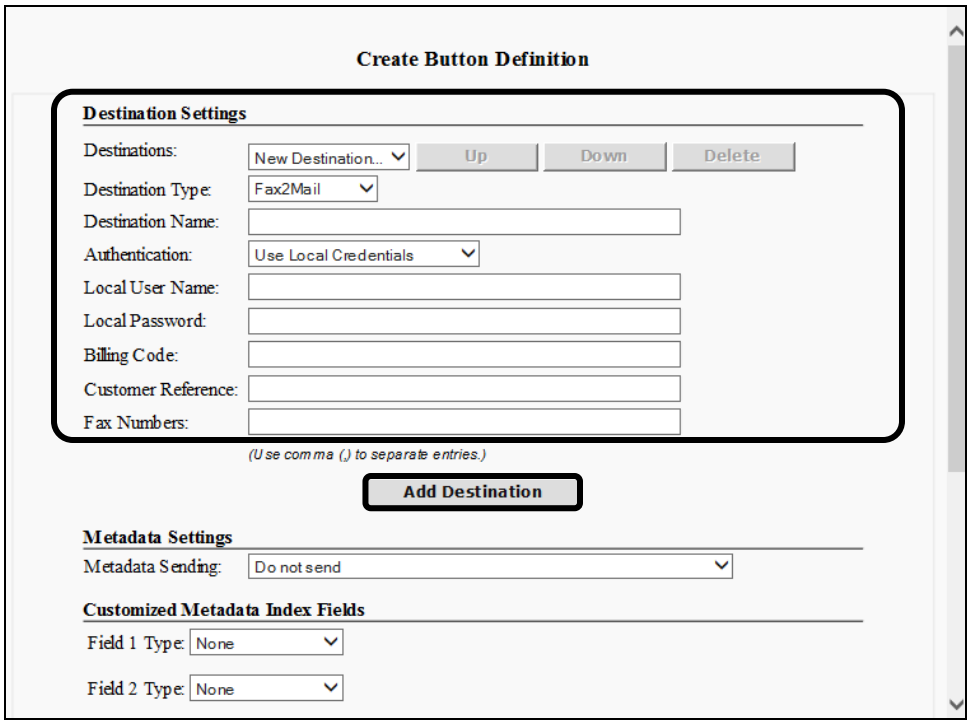
Authentication: Select either [Use User Login Credentials] or [Use Local Credentials]. If authentication is set to [Use User Login Credentials], Authorized Send uses the user's current credentials to log in to the RightFax server. If the credentials are invalid, the send fails. If authentication is set to [Use Local Credentials], the user is prompted to enter a user name and password before sending.

Local User Name: This text box appears only when [Authentication] is set to [Use Local Credentials].

Local Password: This text box appears only when [Authentication] is set to [Use Local Credentials].

Billing Account:	The RightFax administrator can identify faxes based on certain criteria. Enter the RightFax billing account number if it is known. This field is optional.
Billing Matter:	The RightFax administrator can identify faxes based on certain criteria. Enter the RightFax billing matter if it is known. This field is optional.
Fax Numbers:	Enter a fax number, or fax numbers separated by commas. You can enter a string of only numbers separated by commas, and a maximum of 255 characters.

4.8 If you select [Fax2Mail] as the destination type, configure the Destination Settings → click [Add Destination].



Destination Settings

Destination Type: Fax2Mail

Destination Name: Enter a destination name that is added to the Destinations list box. This text box is required. You can enter a string that consists of any character, and a maximum of 40 characters.

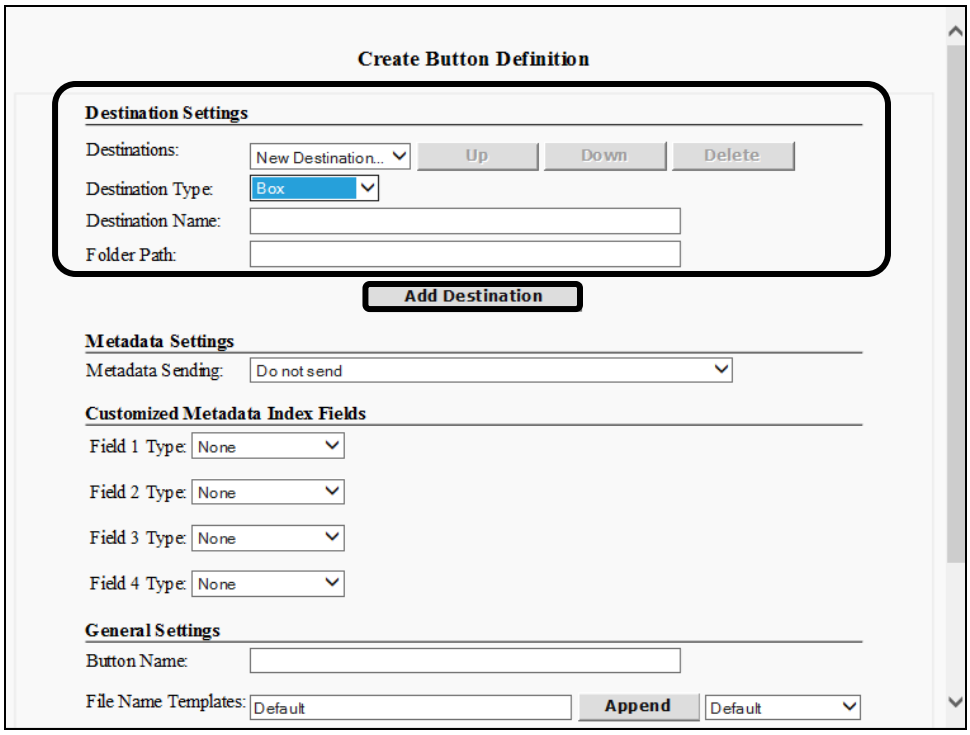
Authentication: Select either [Use User Login Credentials] or [Use Local Credentials]. If authentication is set to [Use User Login Credentials], Authorized Send uses the user's current credentials to log in to the RightFax server. If the credentials are invalid, the send fails. If authentication is set to [Use Local Credentials], the user is prompted to enter a user name and password before sending.

Local User Name: This text box appears only when [Authentication] is set to [Use Local Credentials].

Local Password: This text box appears only when [Authentication] is set to [Use Local Credentials].

Billing Code:	Fax2Mail can identify faxes by a customer-assigned billing code. Enter the Fax2Mail billing code number if it is known. The Billing Code can be up to 20 characters long. This field is optional.
Customer Reference:	Fax2Mail can identify faxes by a customer-defined identifier. Enter the Fax2Mail customer reference if it is known. This field is optional.
Fax Numbers:	Enter a fax number, or fax numbers separated by commas. You can enter a string of only numbers separated by commas, and a maximum of 255 characters.

4.9 If you select [Box] or [Google Drive] as the destination type, configure the Destination Settings → click [Add Destination].



Destination Settings

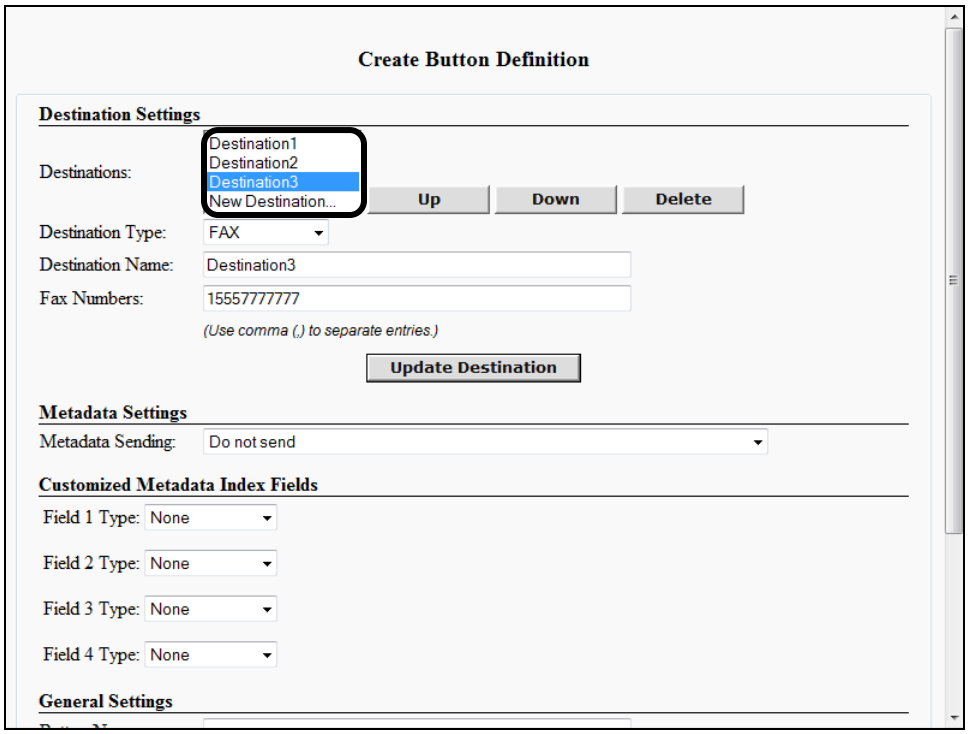
Destination Type: Box or Google Drive

Destination Name: Enter a destination name that is added to the Destinations list box. This text box is required. You can enter a string that consists of any character, and a maximum of 40 characters.

Folder Path: Enter a folder path as the destination of the send job.

NOTE
Authorized Send uses the current user's credentials to log in to the destination cloud service. If the current user does not have a valid cloud service token on the device, the send fails.

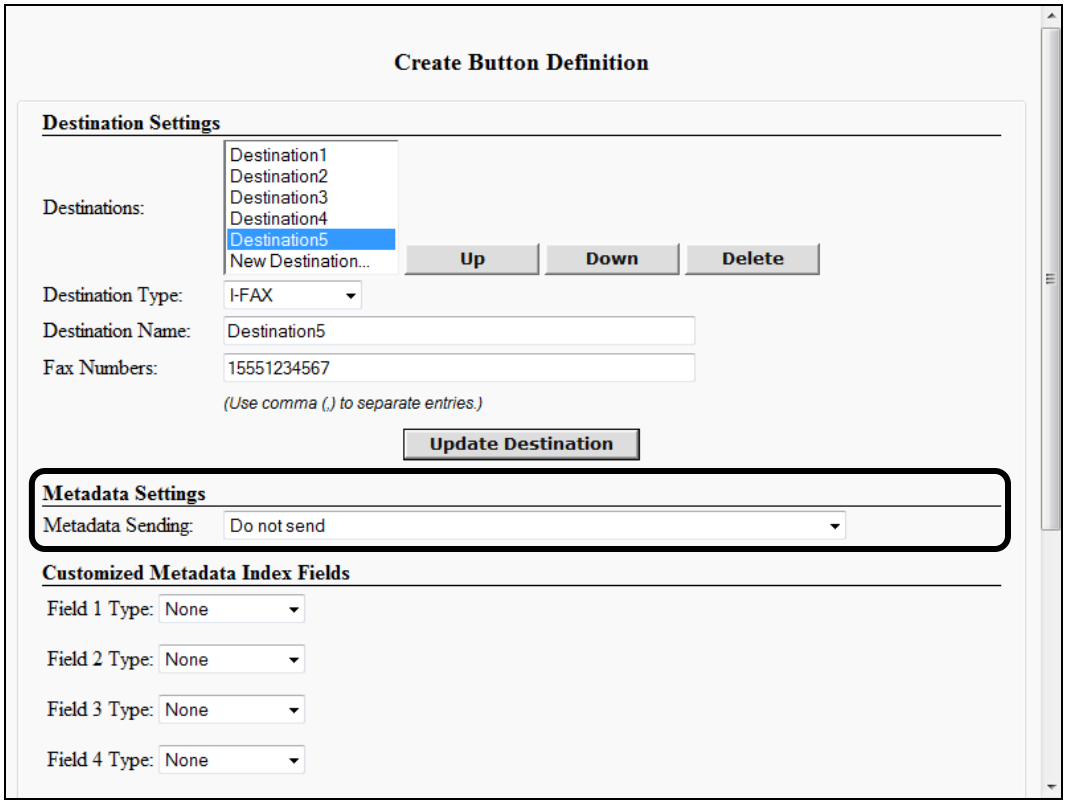
The destination is added to the Destinations list box.



If you want to move a destination's location up or down in the list, select the destination ➞ click [Up] or [Down].

If you want to delete a destination, select the destination ➞ click [Delete].

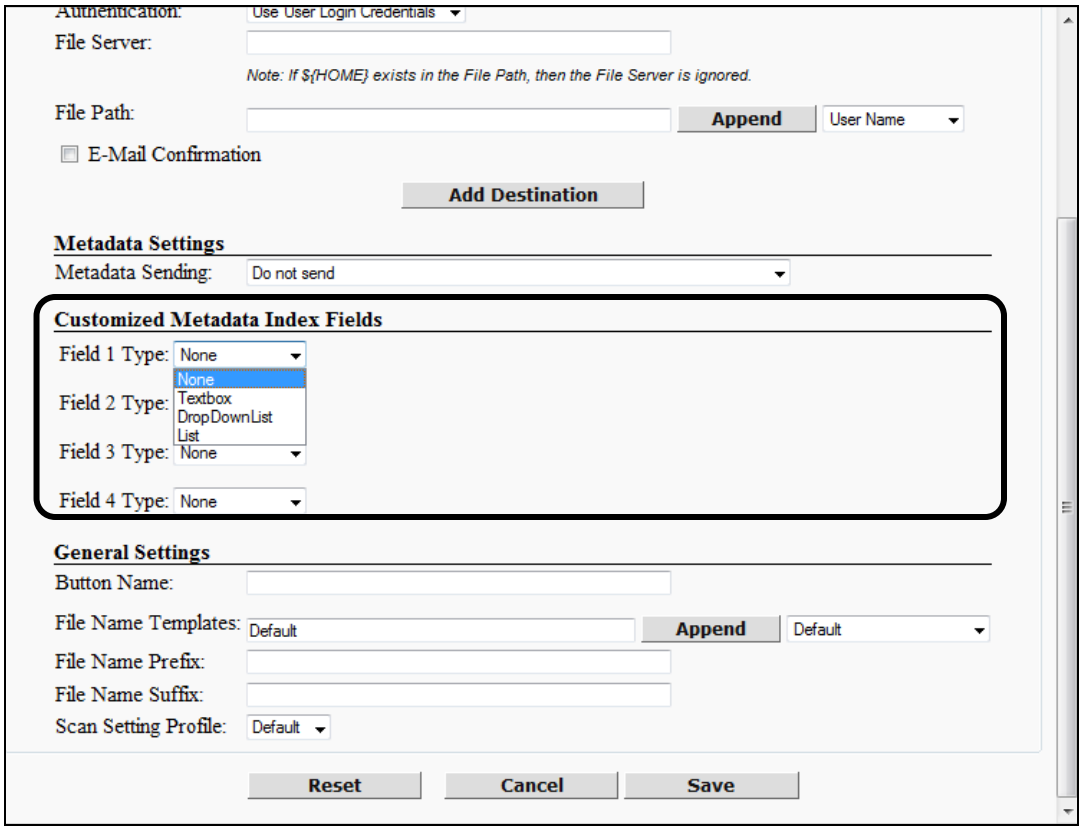
5. Configure the settings under <Metadata Settings>.



Metadata Settings

Metadata Sending: Select [Do not send], [Send default (if enabled) – standard and customized index], [Send default (if enabled) – standard only and the following customized index], or [Send the following customized index only] from the drop-down list. The default setting is 'Do not send'.

6. Configure the settings under <Customized Metadata Index Fields>.



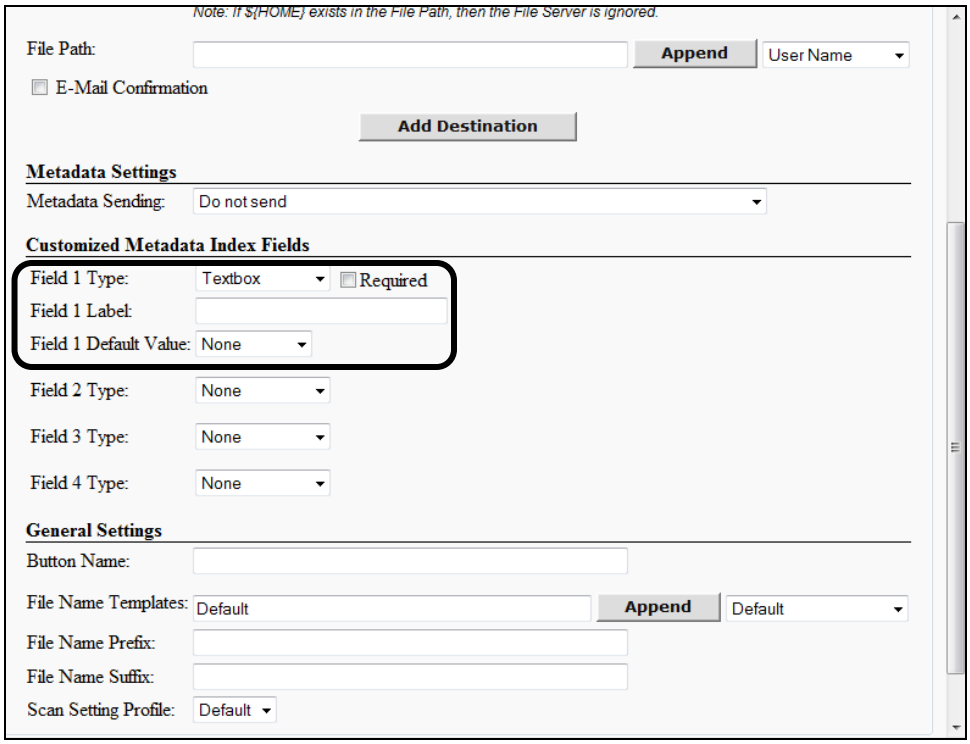
Customized Metadata Index Fields

You can customize up to four (4) metadata index fields. For each custom index field you want to define:

NOTE

Index Fields defined here will override those defined in the Metadata Index configuration screen. For example, define Field 1 in the Metadata Index configuration screen as a text box for a user name. Define Field 1 in this screen as a drop-down list for a directory path. Any File Name templates you use in a One-Touch Button definition which uses ${FIELD1} will use the directory path drop-down list and not the user name text box. To use the system-wide Metadata Index definitions, leave these fields undefined (set [Type] to [None]).

6.1 If you select [Textbox] as the field type, configure the metadata index fields.



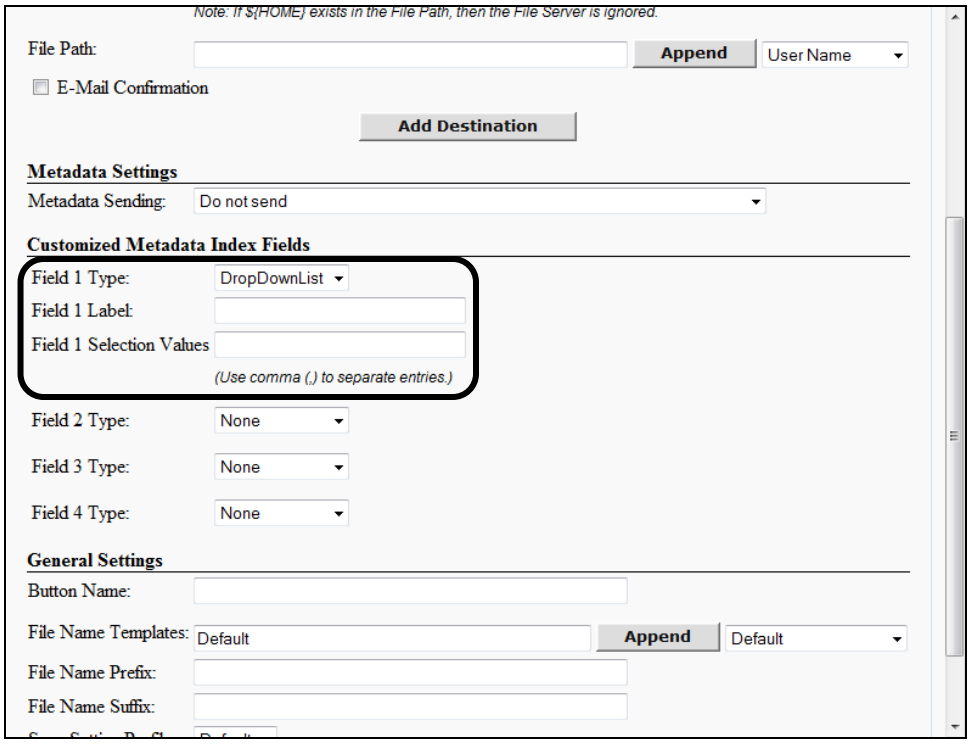
Field Type: [Textbox]

Required: If this check box is selected, the user is required to input some text. If this check box is not selected, the user can input text or no text. This check box is not selected by default.

Field Label: Enter the label for this field that appears on the Authorized Send CUSTOMIZED INDEX screen on the machine. You can enter a string that consists of any character, and a maximum of 60 characters. An asterisk appears before the label name on the device screen if the [Required if Included in File Name] check box is selected.

Field Default Value:	Select the default value for the field. If you select [None], no value appears in the field on the Authorized Send CUSTOMIZED INDEX screen. If you select [User Name], the current Authorized Send user name appears in the field.
Value Changeable By End User:	This check box appears only if the [Field Default Value] is set to [User Name]. Select this check box if you want the user to be able to change the field from the user's name to something else. This is not selected by default.

6.2 If you select [DropDownList] as the field type, configure the metadata index fields.



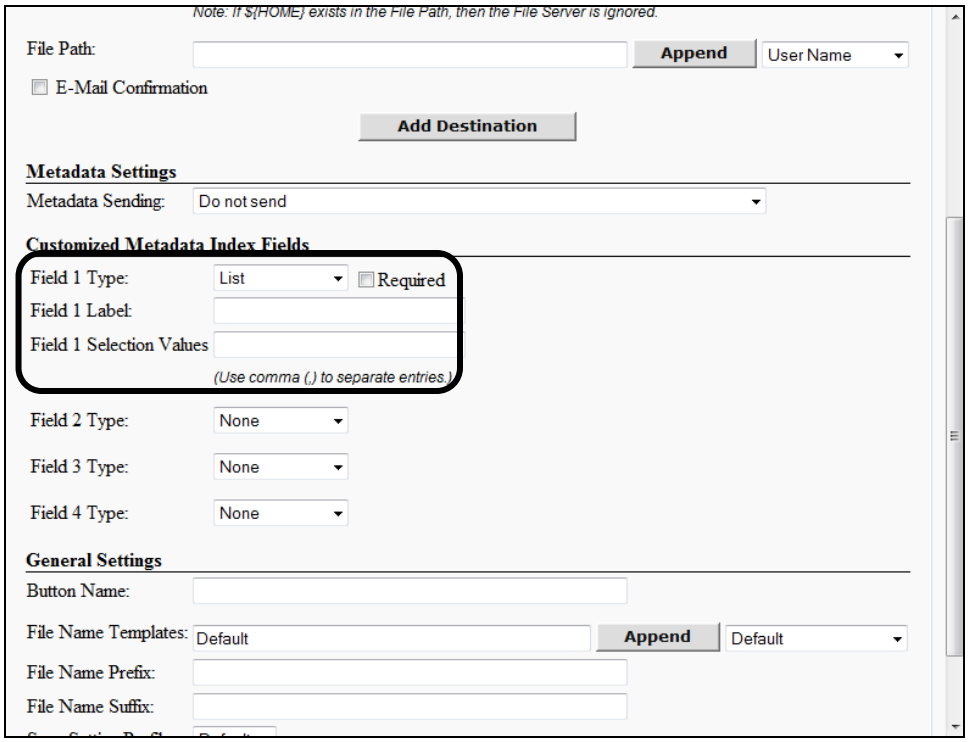
Field Type: [DropDownList]

In a drop-down list, the user can only select one value from the options list. If you want to allow users to select multiple values, use [List] instead.

Field Label: Enter the label for this field that appears on the Authorized Send CUSTOMIZED INDEX screen on the machine. You can enter a string that consists of any character, and a maximum of 60 characters.

Field Selection Values:	Enter the values you want the user to select on Authorized Send CUSTOMIZED INDEX screen on the machine, separated by commas. For each value, you can enter a string that consists of any alphanumeric character, and the following symbols: space ‘ ’, accent ‘‘’, hyphen ‘-’, equal ‘=’, exclamation point ‘!’, at symbol ‘@’, dollar sign ‘$’, carat ‘^’, left parentheses(’, right parentheses)’, underscore ‘_’, plus sign ‘+’, and period ‘.’. A comma ‘,’ can only be used as a delimiter in this text box. Each individual value cannot exceed a maximum of 251 characters. The maximum number of selectable values cannot exceed 20.

6.3 If you select [List] as the field type, configure the metadata index fields.



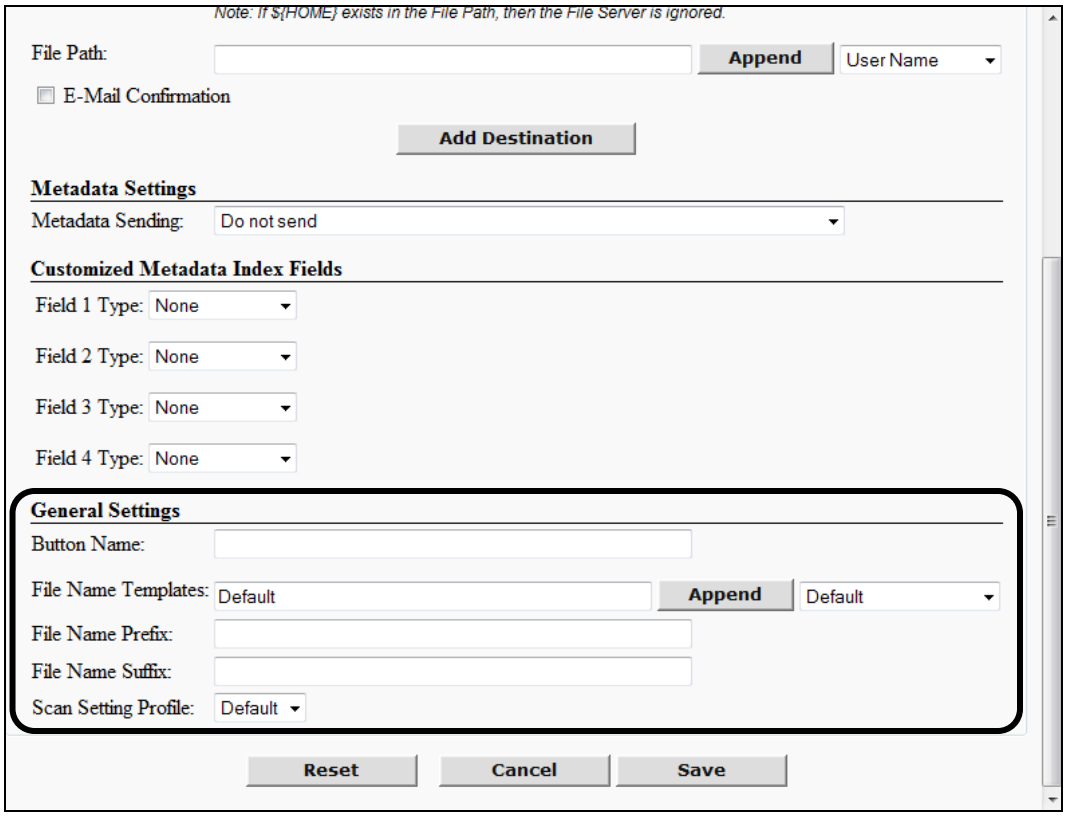
Field Type: [List]

In a list, the user can select one or more values from the options list. If you want to limit users to selecting only one value, use [DropDownList] instead.

Required: If this check box is selected, the user is required to input at least one list element, with multiple elements separated by a comma. If this check box is not selected, the user can input no elements. This check box is not selected by default.

Field Label:	Enter the label for this field that appears on the Authorized Send CUSTOMIZED INDEX screen on the machine. You can enter a string that consists of any character, and a maximum of 60 characters.
Field Selection Values:	Enter the values you want the user to select on Authorized Send CUSTOMIZED INDEX screen on the machine, separated by commas. For each value, you can enter a string that consists of any alphanumeric character, and the following symbols: space ‘ ’, accent ‘‘’, hyphen ‘-’, equal ‘=’, exclamation point ‘!’, at symbol ‘@’, dollar sign ‘$’, carat ‘^’, left parentheses(’, right parentheses)’, underscore ‘_’, plus sign ‘+’, and period ‘.’. A comma ‘,’ can only be used as a delimiter in this text box. Each individual value cannot exceed a maximum of 251 characters. The maximum number of selectable values cannot exceed 20.

7. Configure the settings under <General Settings>.



General Settings

Button Name: Enter a label for the button that appears on the Authorized Send ONE-TOUCH BUTTONS screen on the machine. It is a required text box that cannot be left blank. You can enter a string that consists of any character. The number of any characters permitted is restricted by the width of the icon on the device's display.

File Name Templates: Enter one or more File Name Templates which the user can select when creating a scan job. The names in this list are created under the <File Name> tab. See "Configuring the File Name," on p. 407. The default value is 'Default'. Separate entries must be separated by commas. You can enter the File Name Templates manually or select the Templates from the Append drop-down list and click [Append].

Append: Click [Append] to add a File Name Template (set in the Append drop-down list) to the string in the [File Name Templates] text box.

Append drop-down:	Select a pre-defined File Name Template that is added to the string in the [File Name Templates] text box after you click [Append].
File Name Prefix:	Enter a prefix that is used for the names of all files generated by this button. You can enter a string that consists of any character, and a maximum of 50 characters.
File Name Suffix:	Enter a suffix that is used for the names of all files generated by this button. You can enter a string that consists of any character, and a maximum of 50 characters
Scan Setting Profile:	Select a scan setting profile from the drop-down list. The default setting is ‘Default’, which corresponds to the default settings on the Scan Settings screen.

8. Click [Save].

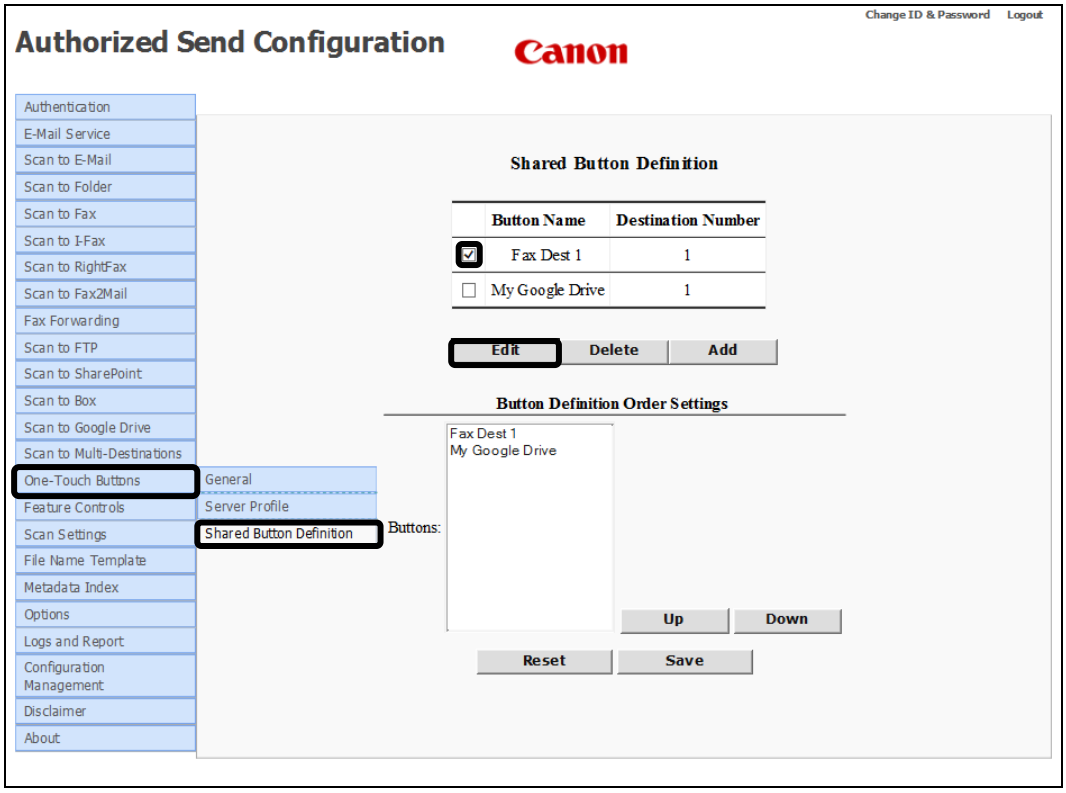
   If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

   To cancel creating the preset share and return to the Button Definition configuration screen, click [Cancel].

2.18.5 Editing a Button Definition

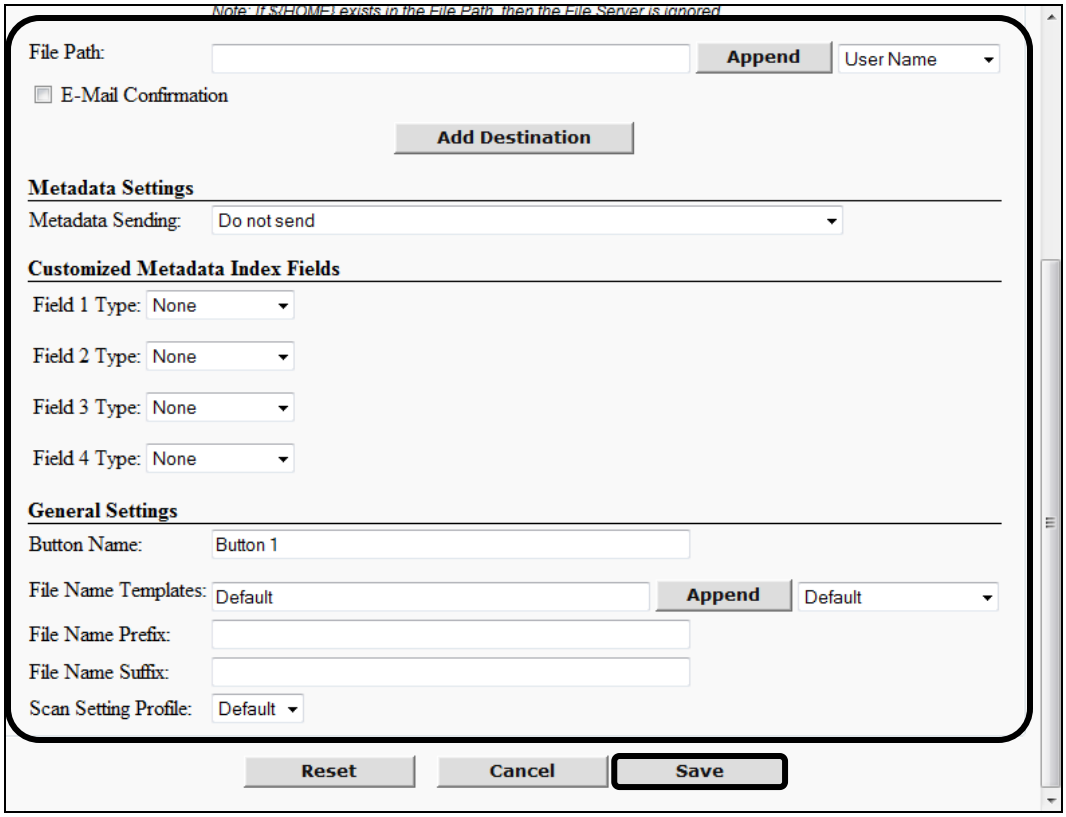
You can edit a previously created button definition from the Button Definition configuration screen.

1. Click [One-Touch Buttons] → [Shared Button Definition] → select the check box next to the button definition name you want to edit → click [Edit].



The Update Button Definition screen is displayed.

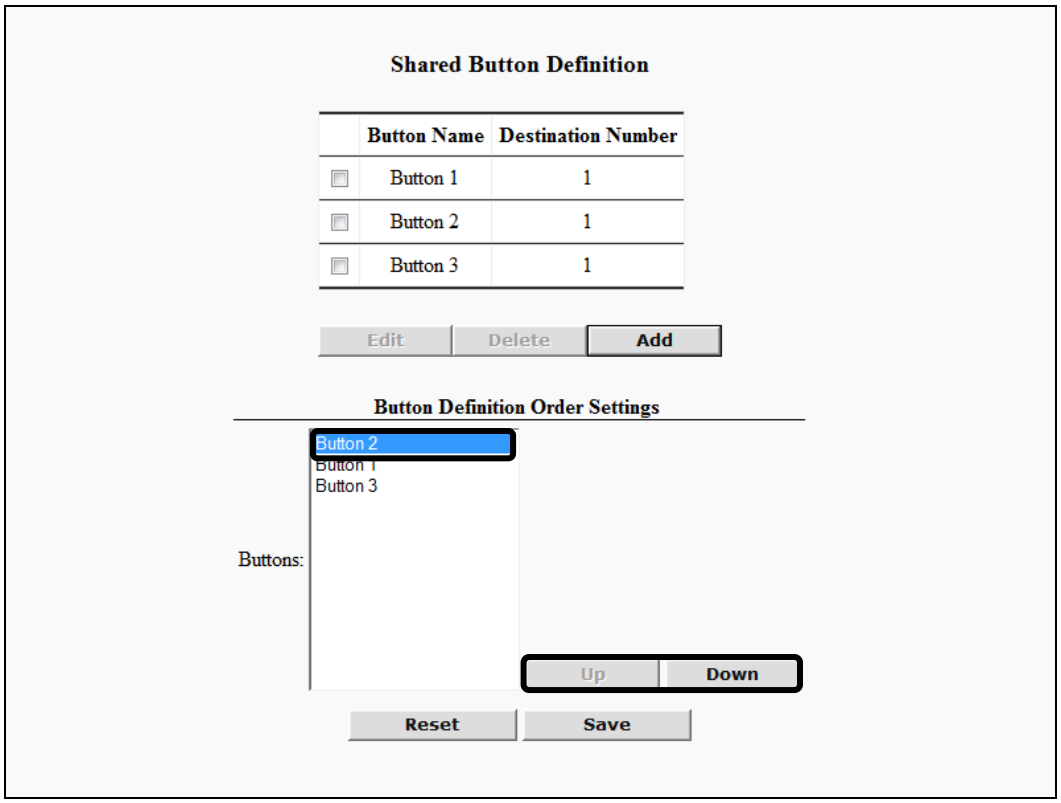
2. Edit the settings for the button definition, as necessary → click [Save].



If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the server profile name and return to the Button Definition configuration screen, click [Cancel].

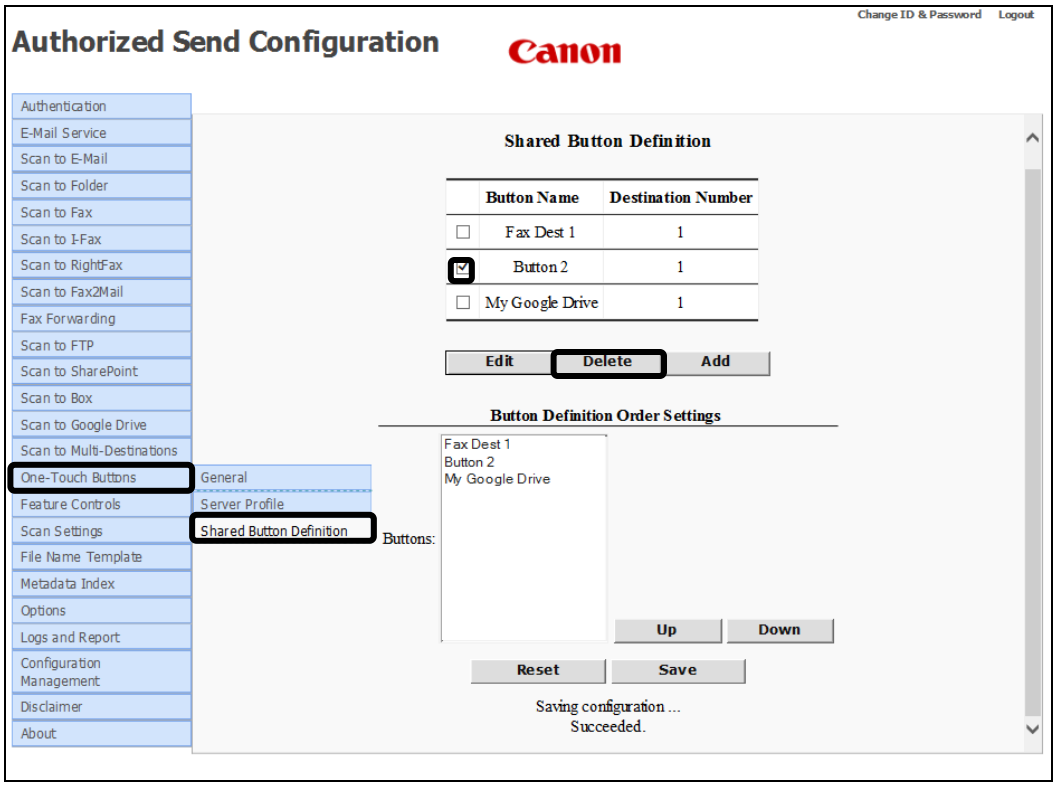
3. If you want to change the order in which the buttons appear on the ONE-TOUCH BUTTONS screen, select the button that you want to move under <Button Definition Order Settings> → click [Up] or [Down] until the button appears where you want it in the list.



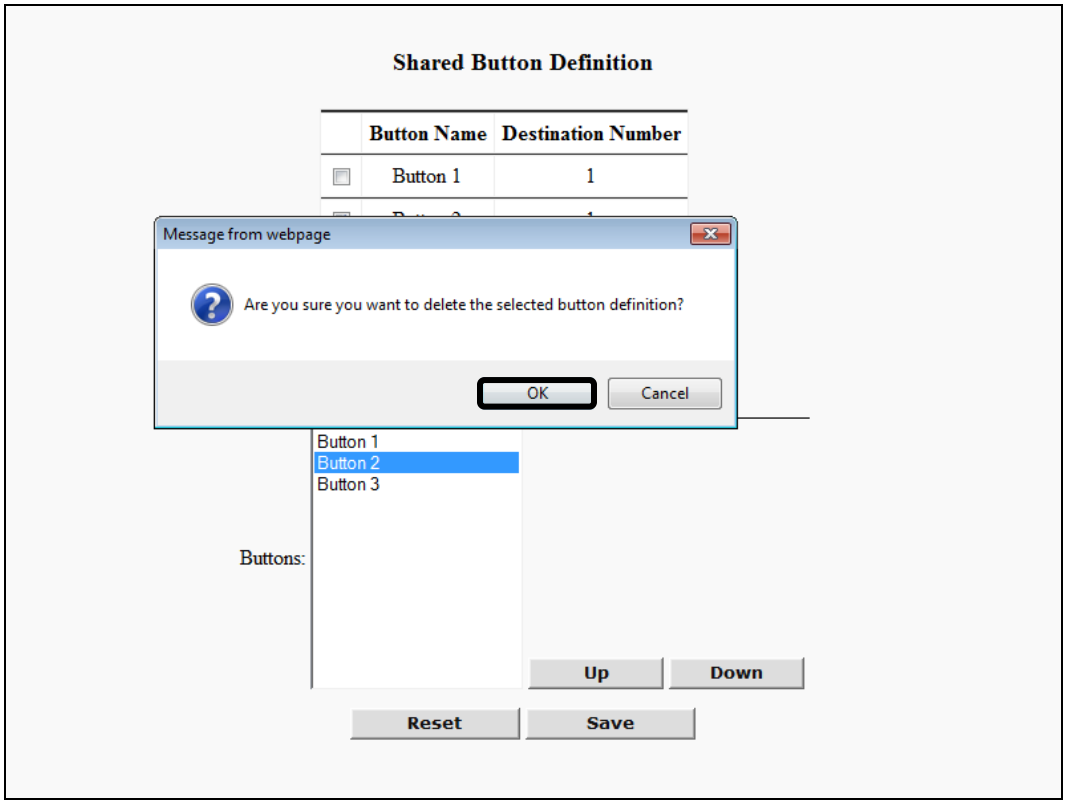
2.18.6 Deleting a Button Definition

You can delete a previously created button definition name from the Button Definition configuration screen.

1. Click [One-Touch Buttons] → [Shared Button Definition] → select the check box next to the button definition name you want to delete → click [Delete].



2. Click [OK] on the confirmation dialog box.



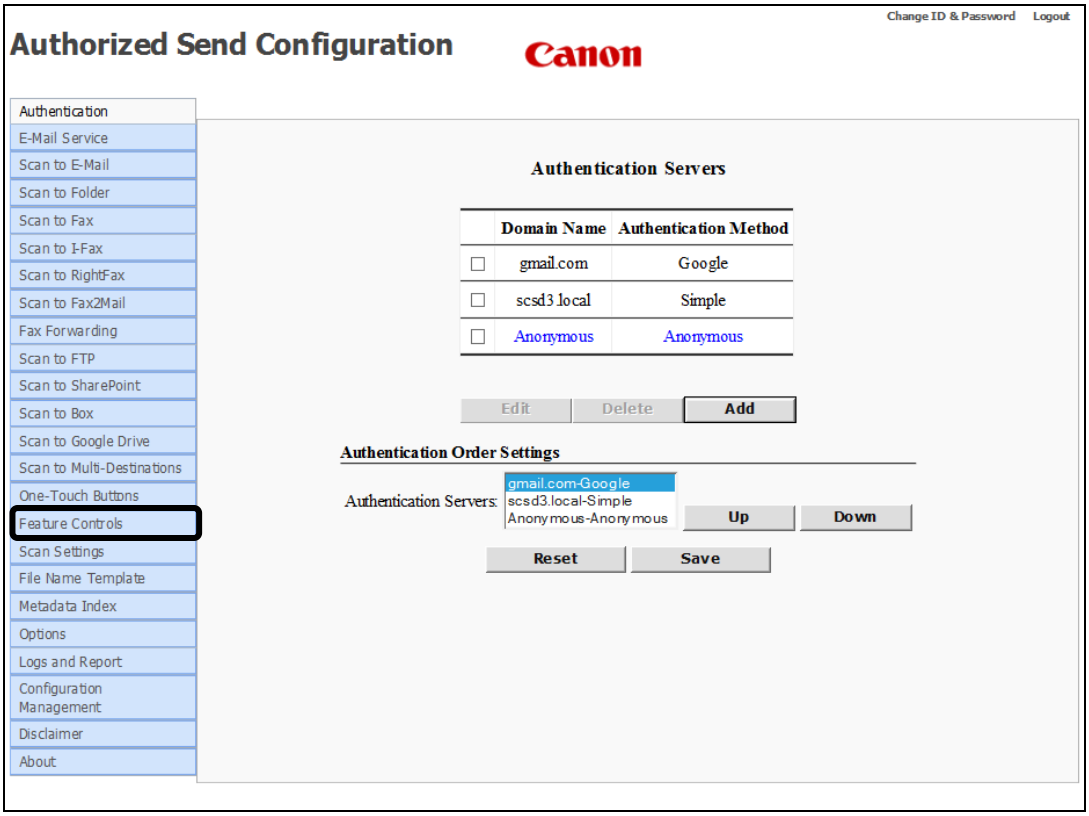
If you do not want to delete the button definition name, click [Cancel].

The button definition name is deleted from the list.

2.19 Configuring the Feature Controls

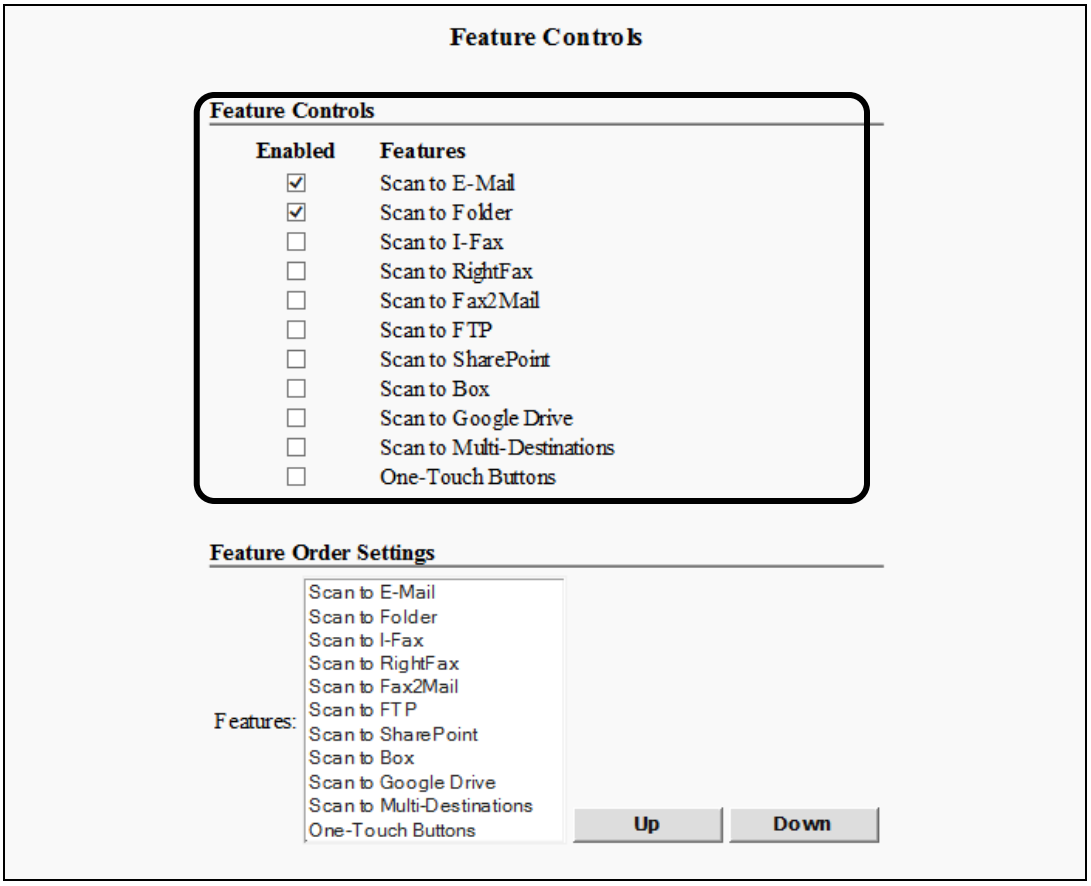
You can configure the Feature Controls function, which enables or disables all of the different scanning functions and sets their order of appearance for the user.

1. Click [Feature Controls].



The Feature Controls screen is displayed.

2. Configure the settings under <Feature Controls>.



Feature Controls

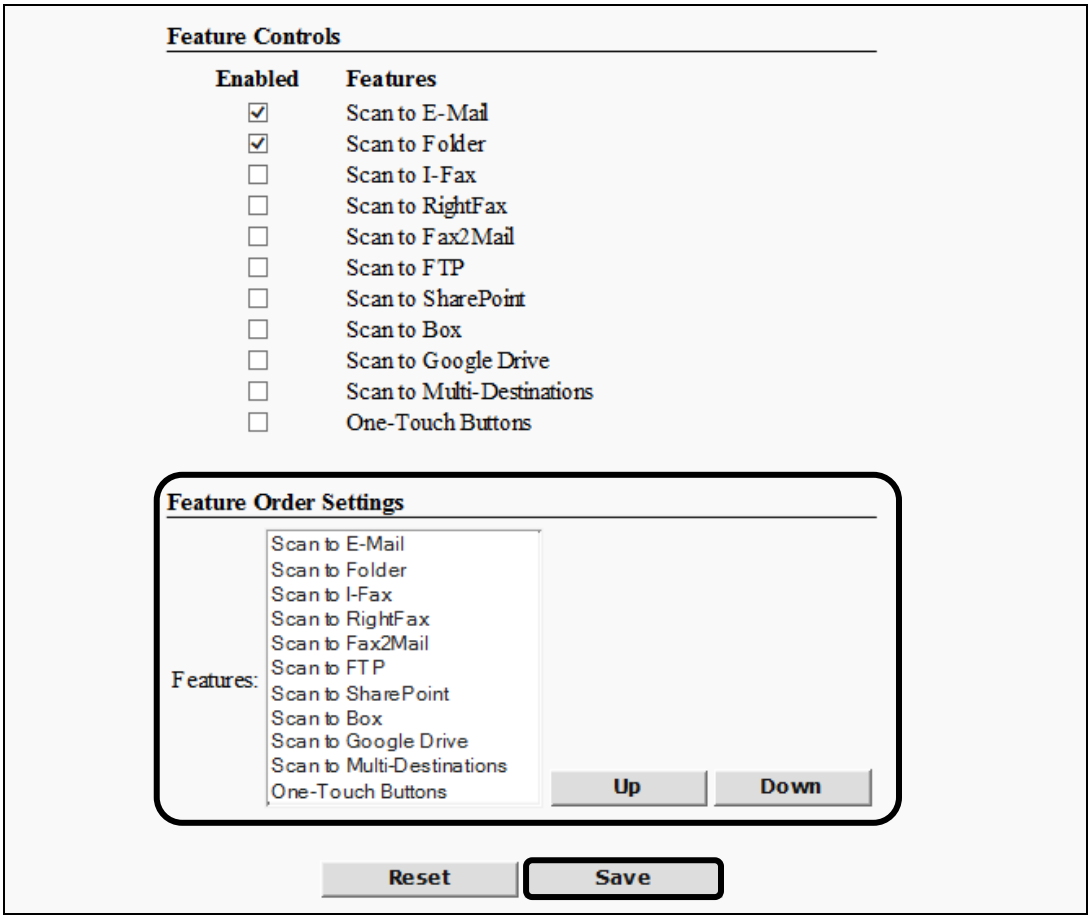
Enabled Column

Select the [Scan to E-Mail], [Scan to Folder], [Scan to I-Fax], [Scan to RightFax], [Scan to Fax2Mail], [Scan to FTP], [Scan to SharePoint], [Scan to Box], [Scan to Google Drive], [Scan to Multi-Destinations], or [One-Touch Buttons] check box if you want the individual functions to appear on the Authorized Send MAIN screen on the machine.

NOTE

- The [Scan to E-Mail] and [Scan to Folder] check boxes are selected by default.
- If the device does not support analog fax phone lines, the [Scan to Fax] check box is not displayed.

3. Configure the settings under <Feature Order Settings> ➞ click [Save].



Feature Order Settings

To rearrange the order of how functions appear in Feature Controls and on the Authorized Send MAIN screen on the machine, select a function from the Feature Order Settings scroll box ➞ click [Up] or [Down] to move the function's location in the list up or down. Each click you make moves the selected function up or down in the list one line at a time.

The default order of the functions that appear on the Authorized Send MAIN screen on the machine are Scan to E-Mail, Scan to Folder, Scan to I-Fax, Scan to RightFax, Scan to Fax2Mail, Scan to FTP, Scan to SharePoint, Scan to Box, Scan to Google Drive, Scan to Multi-Destinations, and One-Touch Buttons.

NOTE
If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.20 Configuring the Scan Settings

You can configure the Scan Settings function, which sets the default scan settings for each file type.

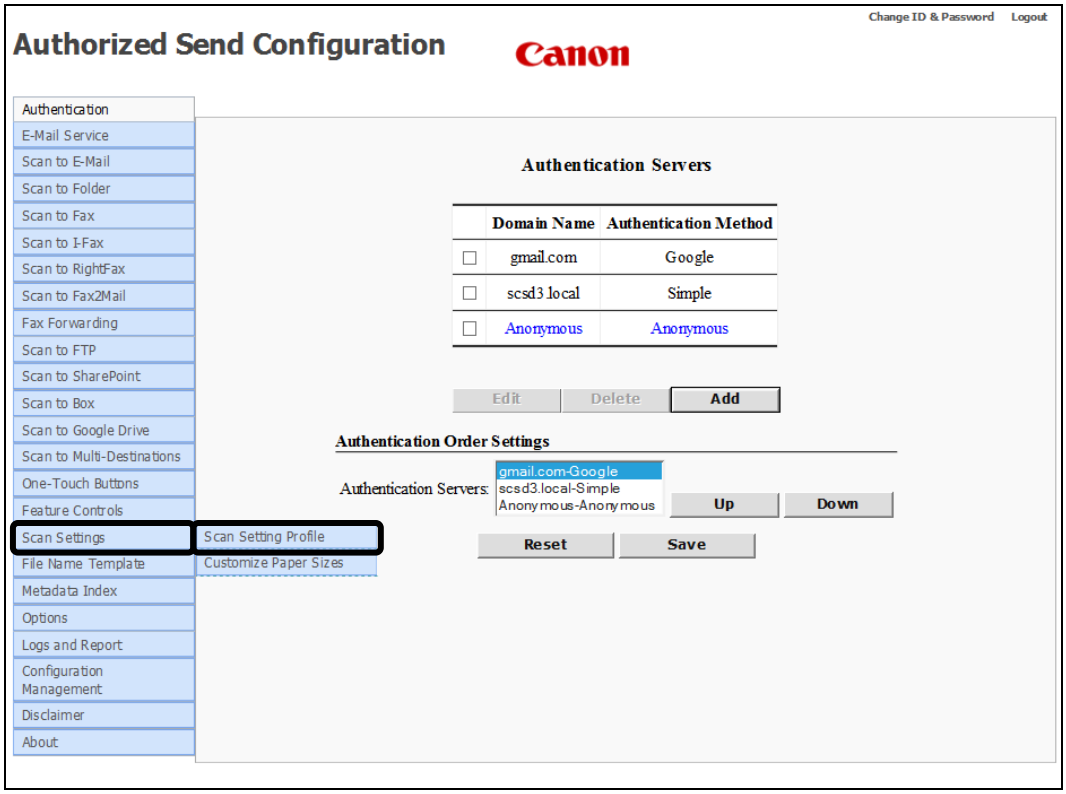
IMPORTANT

If an AMS enabled login application is installed and running on the machine, and the login application specifies that color scanning is disabled, the Color Mode drop-down list is forced to 'Black', scanning is done only in black-and-white, and [PDF(Compct)] and [JPEG] are grayed out.

2.20.1 Creating a Scan Setting Profile

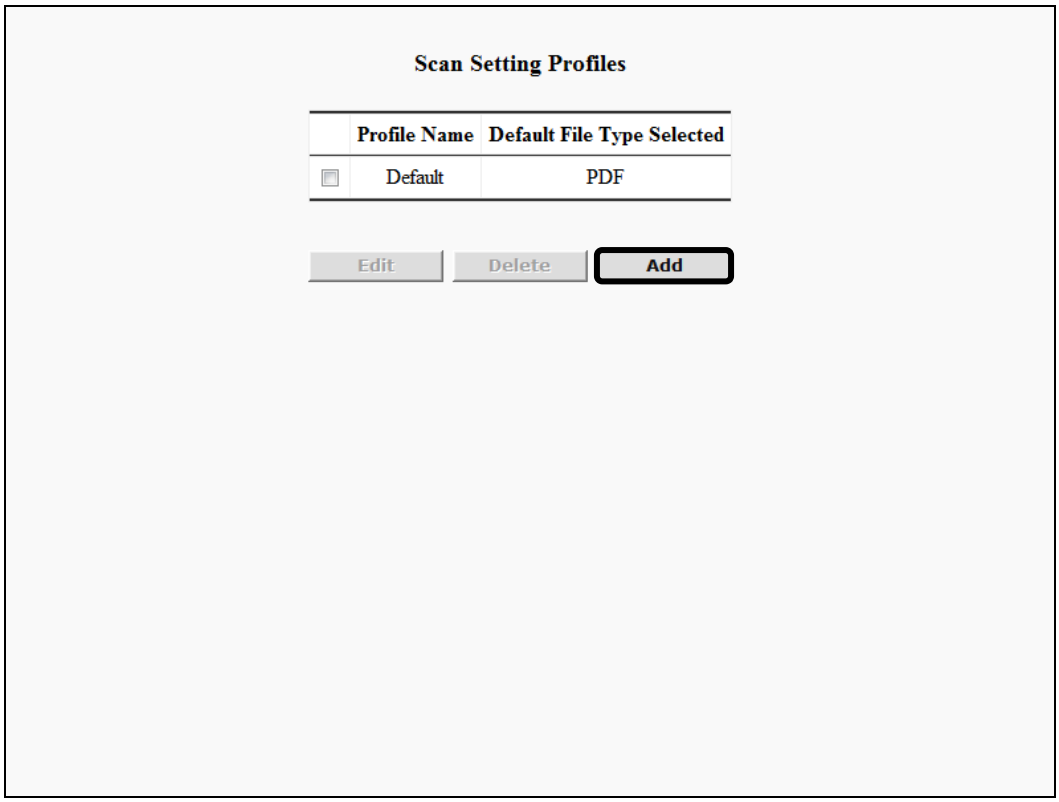
You can create different Scan Setting Profiles to use during scanning.

1. Click [Scan Settings] → click [Scan Setting Profile].

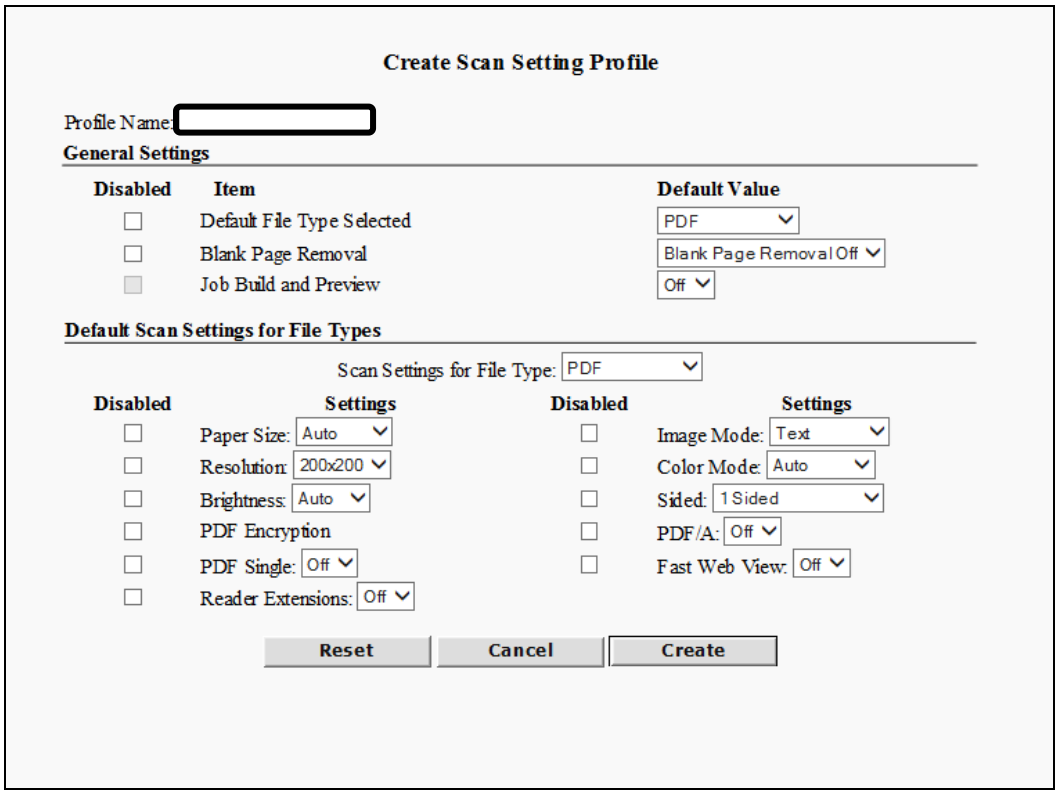


The Scan Setting Profile screen is displayed.

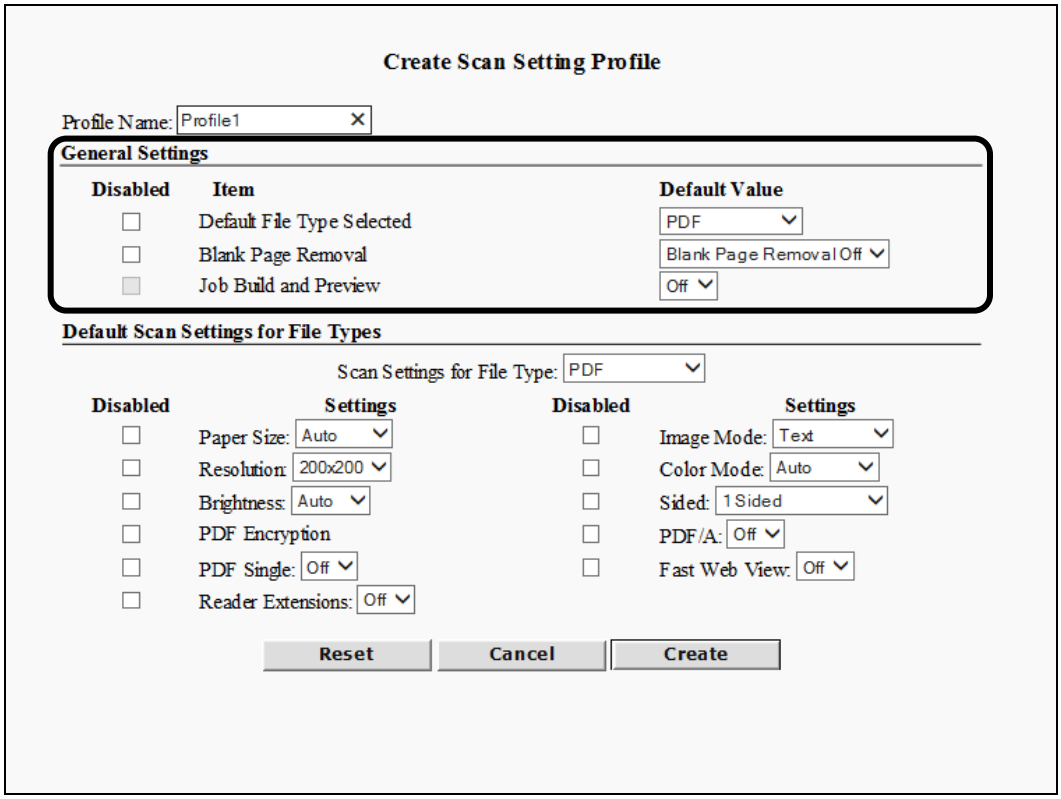
2. Click [Add] to create a new profile.



3. Enter a profile name in the [Profile Name] text box.



4. Configure the settings under <General Settings>.



General Settings

Disabled Column
Default File Type Selected:
Blank Page Removal:
Job Build and:
Preview:

By default, each check box in this column is not selected. Select the check boxes next to the desired settings that you want to disable and gray out on the Authorized Send SCAN SETTINGS screen on the machine. The check box for [Job Build and Preview] cannot currently be selected.

Default File Type Selected:

If you want to change the default file type, select a file type from the drop-down list. The default setting is 'PDF'.

NOTE
The entire drop-down list may include [PDF], [PDF(Compct)], [PDF(OCR)], [TIFF], [TIFF(Single)], [JPEG], [XPS], [XPS(Compct)], [XPS(OCR)], [PPT], [PPT(OCR)], or [WORD], depending on if the file type is supported and installed on your machine.

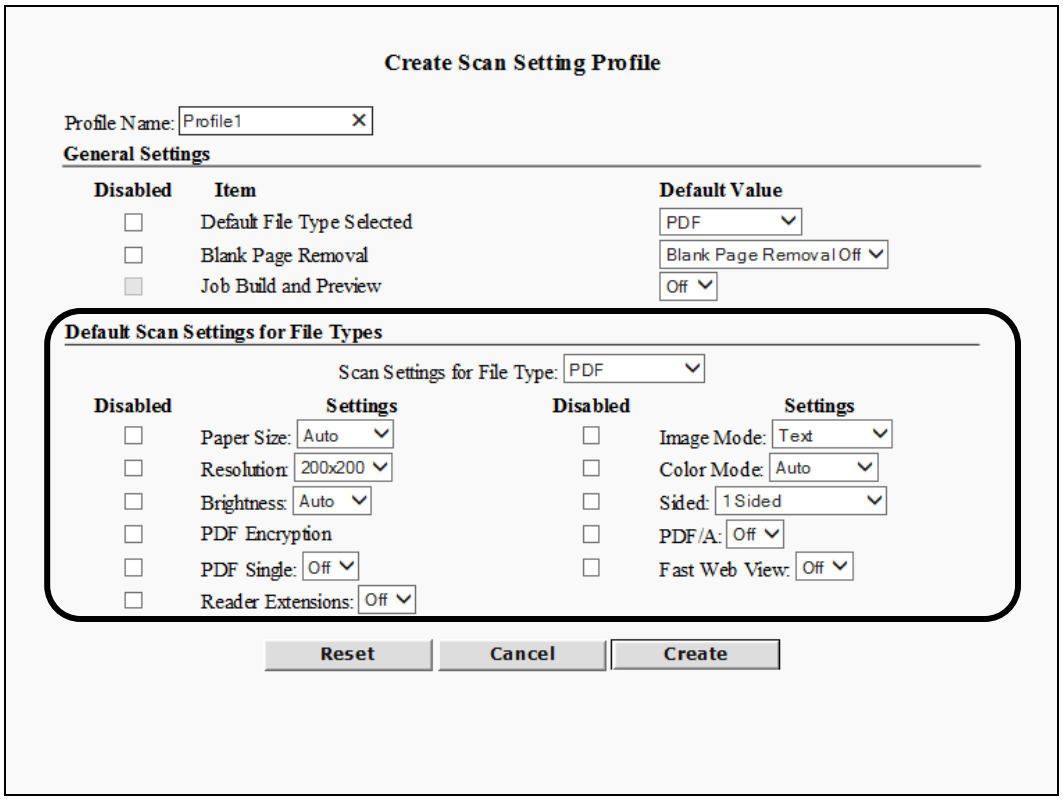
Blank Page Removal: Select the sensitivity of the Blank Page Removal function using the drop-down list. [Blank Page Removal 1] will identify the least number of blank pages. [Blank Page Removal 4] will identify the largest number of blank pages. The default setting is ‘Blank Page Removal Off’.

NOTE

Blank Page Removal is not supported on the imageRUNNER ADVANCE 4000 Series and 8200 Series. Blank Page Removal is not supported on the imageRUNNER ADVANCE 3500 Series when the color mode is set to B&W (black-and-white), the paper size is Auto, Mixed, 11” x 17”, or A3, and the resolution is 600 x 600 dpi. The Blank Page removal feature is disabled for the user when these conditions are met.

Job Build and Preview: Select [On] or [Off] to set the default state of the [Job Build and Preview] button on the machine console. The default setting is ‘Off’.

5. Configure the settings under <Default Scan Settings for File Types>.



Default Scan Settings for File Types

Scan Settings for File Type:	Select [PDF], [PDF(Compct)], [PDF(OCR)], [TIFF], [TIFF(Single)], [JPEG], [XPS], [XPS(Compct)], [XPS(OCR)], [PPT], [PPT(OCR)], or [WORD] from the drop-down list, depending on if the file type is supported and installed on your machine. The file type selected in conjunction with the specific scan settings that you select and save, are displayed as the new default settings for that file type on the Authorized Send SCAN SETTINGS screen on the machine. The default setting is ‘PDF’.

Disabled Column
Paper Size:
Resolution:
Brightness:
PDF Encryption:
Fast Web View:
Reader Extensions:
Image Mode:
Color Mode:
Sided:
PDF/A:
PDF Single:

By default, each check box in this column is not selected, unless a particular default scan setting, based on the file type you select from the Scan Settings for File Type drop-down list, requires it to be disabled and grayed out. Select the check boxes next to the desired settings that you want to disable and gray out on the Authorized Send SCAN SETTINGS screen on the machine.

NOTE

- The [PDF Encryption], [Fast Web View], and [Reader Extensions] check boxes only appear on machines that support these features.
- PDF/A is a file format for the long-term archiving of electronic documents.
- PDF/A and Reader Extensions cannot be enabled simultaneously.

Settings Column

By default, some settings are automatically selected and grayed out, based on the file type you select from the Scan Settings for File Type drop-down list.

Paper Size:

Select [Auto], [Letter], [Letter-R], [Legal], [11x17], or [Mixed] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default setting is ‘Auto’.

NOTE

- Select [Auto] if you want to scan a letter-size document in a landscape orientation.
- If [Auto] is selected, scanning originals with different sizes or with different orientations may produce unexpected results.
- Select [Letter] if you want to scan in a portrait orientation.
- If you select [Letter] for scanning in a landscape orientation, the scanned image is truncated.
- Select [Mixed] to scan a batch of mixed-size originals.
- The Paper Size drop-down list is populated with only ‘Letter-R’ and ‘Legal’ for the imageRUNNER ADVANCE 500iF and 400iF, and imageRUNNER ADVANCE C350iF/C250iF devices.

Resolution: Select [200x200], [300x300], or [600x600] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default setting depends on the file type that you selected.

NOTE

- If your machine does not support a particular resolution, that resolution is not displayed.
- The Resolution drop-down list is populated with only '200x200 dpi' and '300x300 dpi' for the imageRUNNER ADVANCE 500iF and 400iF, and imageRUNNER ADVANCE C350iF/C250iF devices if [Auto] or [Full Color] is selected from the Color Mode drop-down list.

Brightness: Select [Auto], [10%], [20%], [30%], [40%], [50%], [60%], [70%], [80%], [90%], or [100%] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default setting is 'Auto'.

Image Mode: Select [Text], [Text/Photo], or [Photo] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default setting is 'Text'.

Color Mode: Select [Auto], [Full Color], or [Black] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default setting depends on the file type that you selected.

NOTE

- If your machine's scanner is black-and-white only, [Black] is automatically selected and the Color Mode drop-down list is disabled and grayed out.
- The Color Mode selections that are available depend on the file type that you selected from the File Type drop-down list.
  - PDF: [Auto], [Full Color], and [Black]
  - PDF(Compct): Only [Full Color]
  - PDF(OCR): [Auto], [Full Color], and [Black]
  - TIFF: Only [Black]
  - TIFF(Single): Only [Black]
  - JPEG: Only [Full Color]
  - XPS: [Auto], [Full Color], and [Black]
  - XPS(Compct): Only [Full Color]
  - XPS(OCR): [Auto], [Full Color], and [Black]
  - PPT: Only [Full Color]
  - PPT(OCR): Only [Full Color]
  - WORD: Only [Full Color]
- The Color Mode drop-down list is populated with only 'Black' for the imageRUNNER ADVANCE 500iF and 400iF, and imageRUNNER ADVANCE C350iF/C250iF devices if [600x600 dpi] is selected from the Resolution drop-down list.

Sided: Select [1 Sided], [2 Sided Booklet], or [2 Sided Calendar] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default setting is '1 Sided'.

PDF Single: Select [On] or [Off] from the drop-down list to set the default state of the PDF Single check box in the Scan Settings screen.

NOTE

The table below displays the default scan settings for each file type that automatically appears on the Authorized Send SCAN SETTINGS screen on the machine, unless they are changed and saved by the System Administrator.

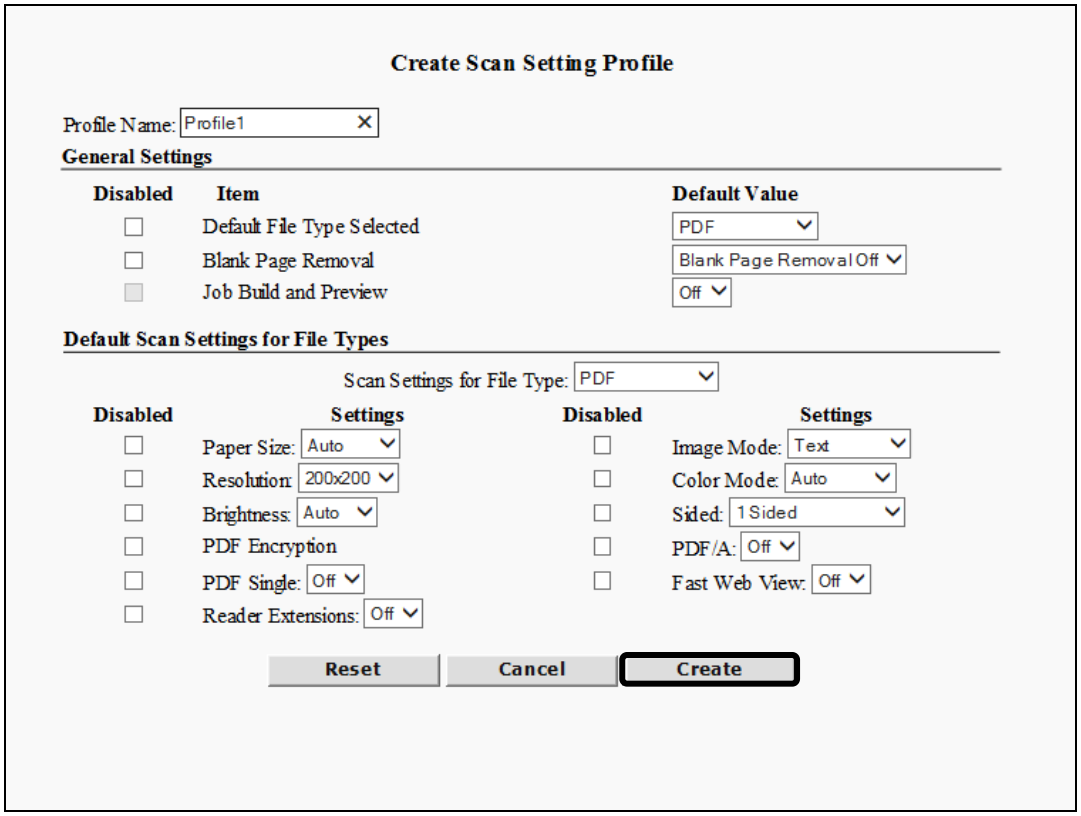
File Type	Paper Size	Res.	Bright	PDF Encrypt.	Img. Mode	Color Mode	Sided	PDF/A
PDF	Auto*1	200x200	Auto	Available	Text	Auto	1 Sided	Available
PDF (Compct)	Auto*1	300x300*2	Auto	Available	Text	Full Color*3	1 Sided	Available
PDF (OCR)	Auto*1	200x200	Auto	Available	Text	Auto	1 Sided	Not Available
TIFF	Auto*1	200x200	Auto	Not Available	Text	Black*3	1 Sided	Not Available
TIFF (Single)	Auto*1	200x200	Auto	Not Available	Text	Black*3	1 Sided	Not Available
JPEG	Auto*1	200x200	Auto	Not Available	Text	Full Color*3	1 Sided	Not Available
XPS	Auto*1	200x200	Auto	Not Available	Text	Auto*3	1-Sided	Not Available
XPS (Compct)	Auto*1	300x300*2	Auto	Not Available	Text	Auto*3	1-Sided	Not Available
XPS (OCR)	Auto*1	300x300	Auto	Not Available	Text	Full Color*3	1-Sided	Not Available
PPT	Auto*1	300x300	Auto	Not Available	Text	Full Color*3	1-Sided	Not Available
PPT (OCR)	Auto*1	300x300	Auto	Not Available	Text	Full Color*3	1-Sided	Not Available
WORD	Auto*1	300x300*2	Auto	Not Available	Text	Full Color*3	1-Sided	Not Available

*1 The imageRUNNER ADVANCE 400iF and 500iF, and imageRUNNER ADVANCE C350iF/C250iF devices default paper size is 'Letter-R'.

*2 The Resolution Mode drop-down list is disabled.

*3 The Color Mode drop-down list is disabled.

6. Click [Create].



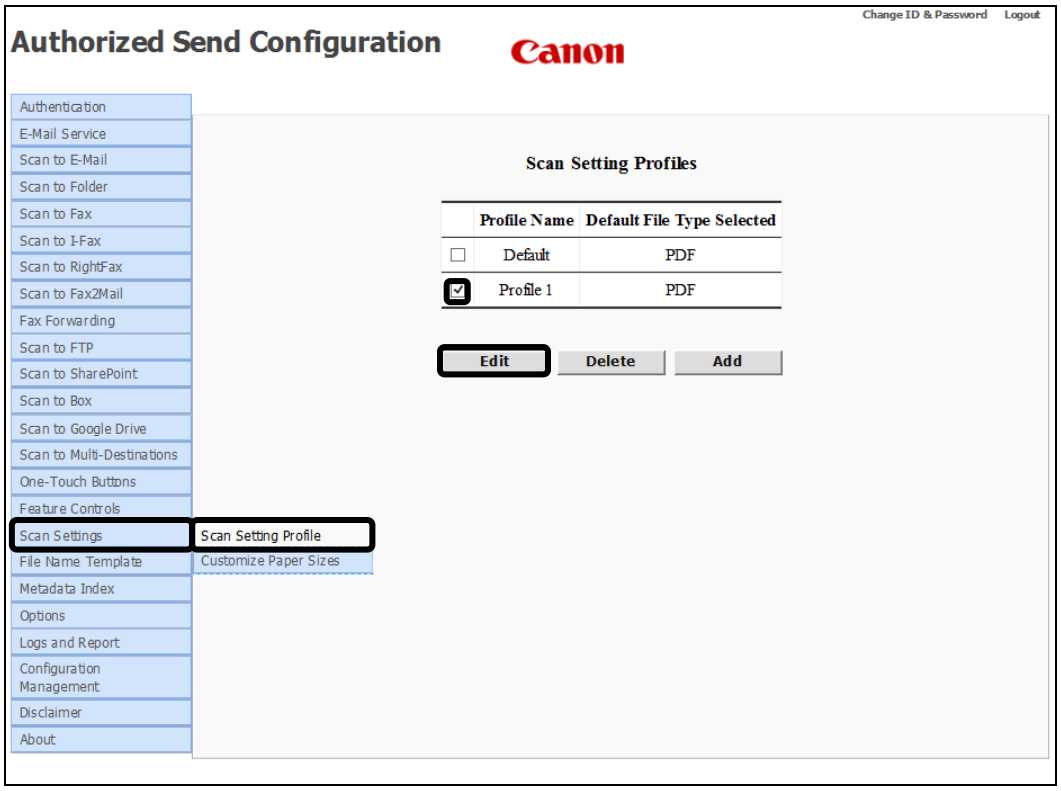
If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

To cancel creating a profile and return to the Scan Setting Profile screen, click [Cancel].

2.20.2 Editing a Scan Setting Profile

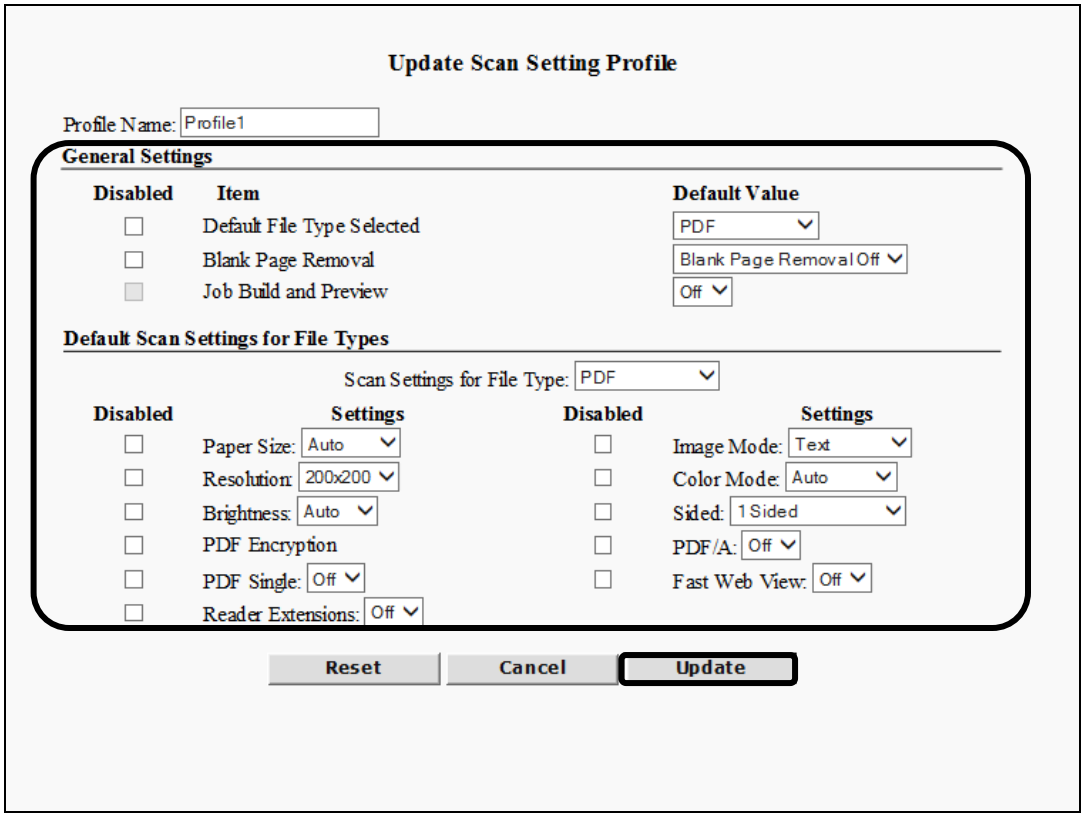
You can edit a previously-created scan profile from the Scan Setting Profile configuration screen.

1. Click [Scan Settings] → [Scan Setting Profile] → select the check box next to the profile you want to edit → click [Edit].



The Update Scan Setting Profile screen is displayed.

2. Edit the settings for the scan profile, as necessary → click [Update].



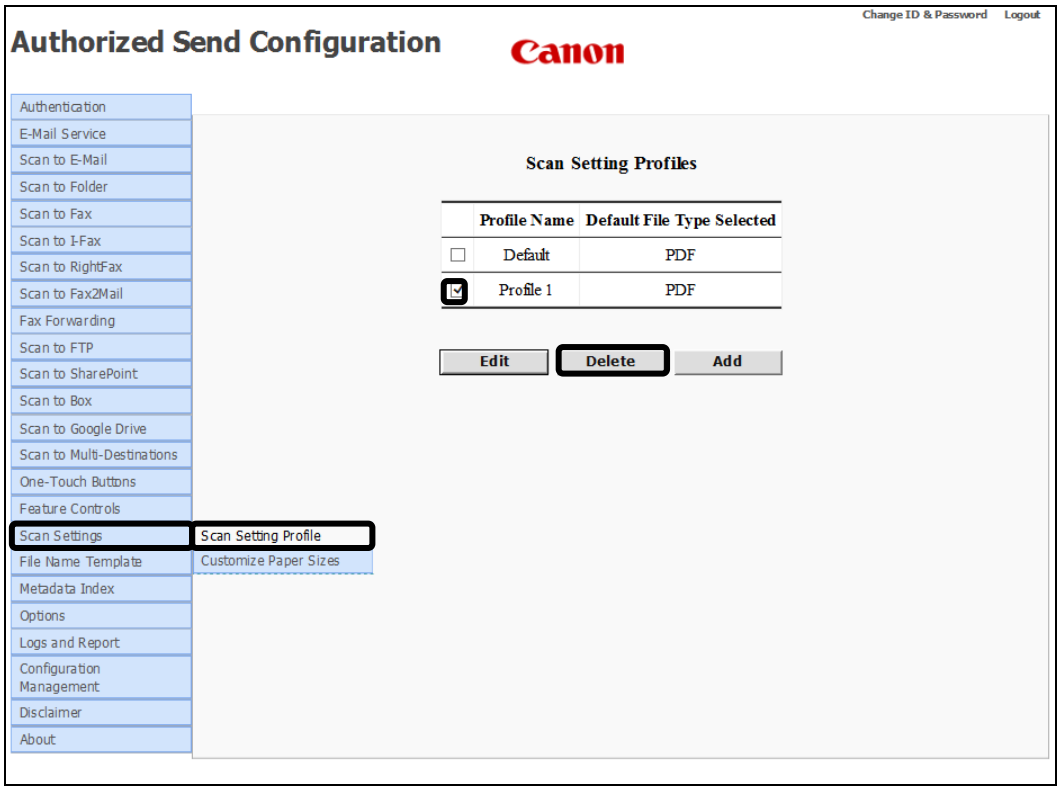
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the scan profile and return to the Scan Setting Profile screen, click [Cancel].

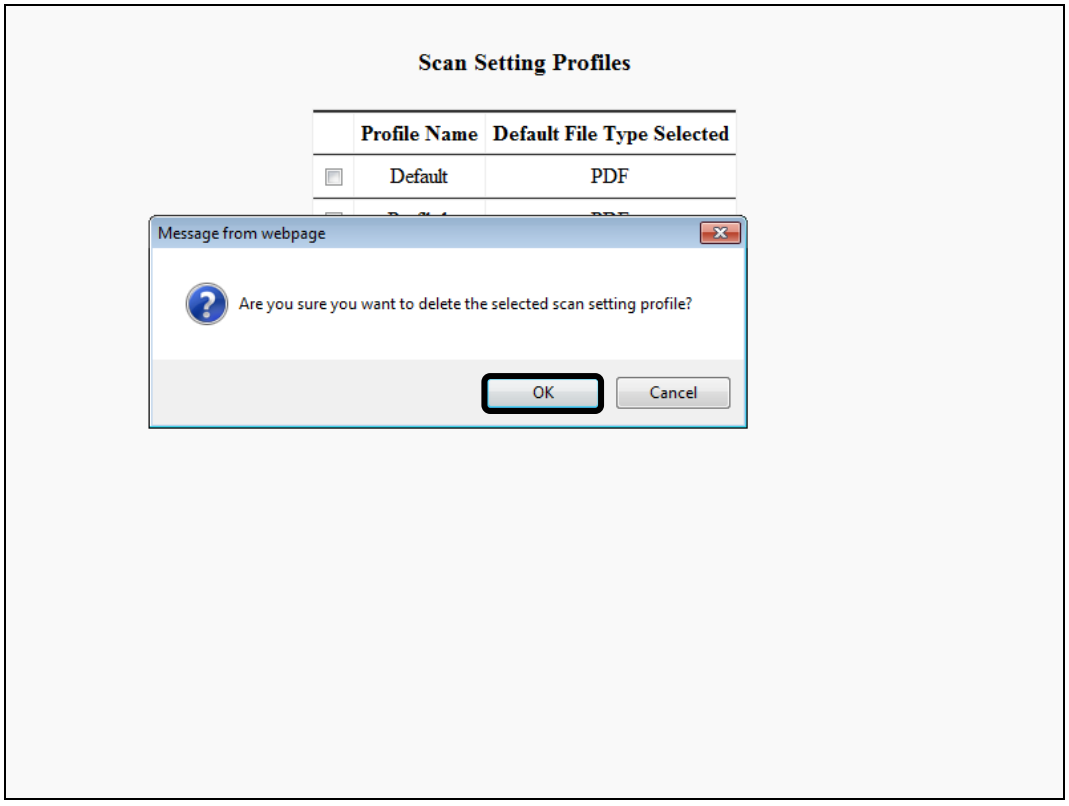
2.20.3 Deleting a Scan Setting Profile

You can delete a previously-created scan profile from the Scan Setting Profile configuration screen.

1. Click [Scan Settings] ➞ [Scan Setting Profile] ➞ select the check box next to the scan profile you want to delete ➞ click [Delete].



2. Click [OK] on the confirmation dialog box.



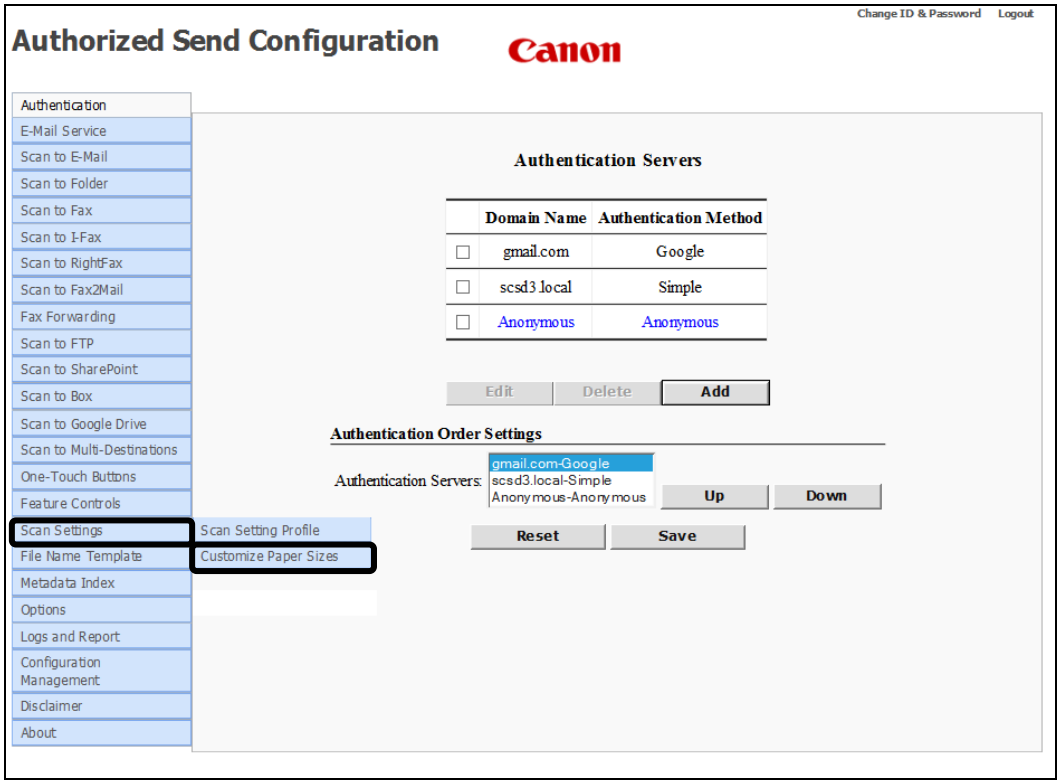
If you do not want to delete the scan profile, click [Cancel].

The scan profile is deleted from the list.

2.20.4 Customizing Display of Paper Sizes

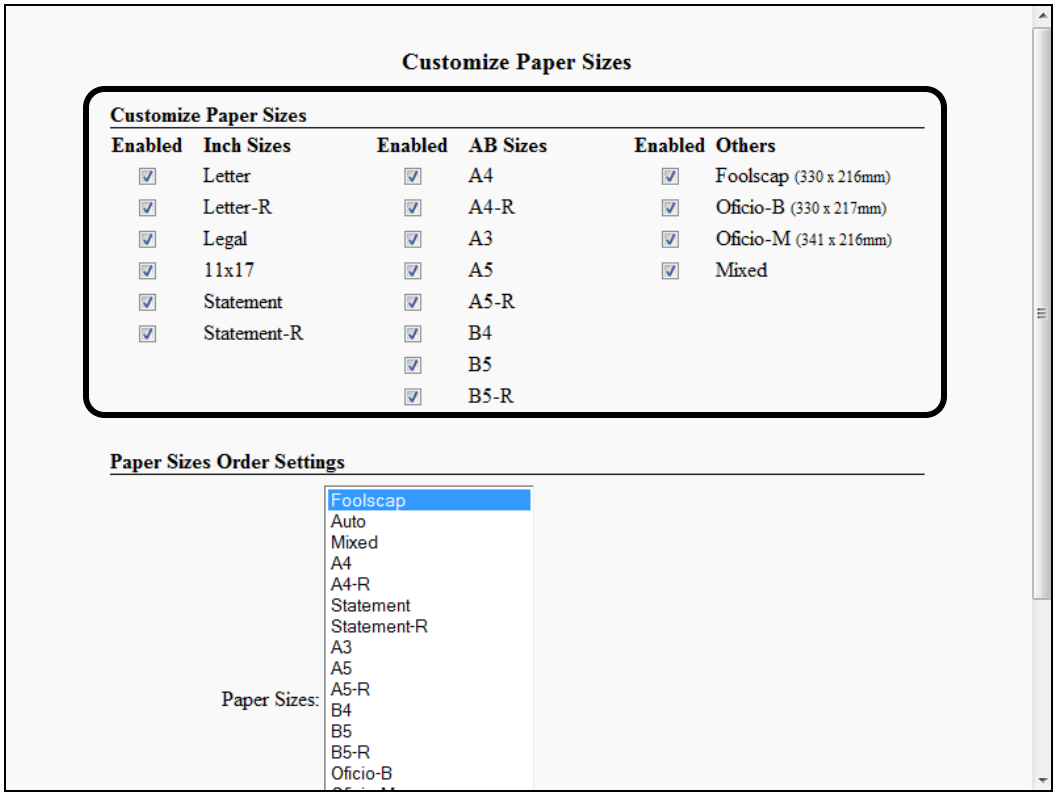
You can set which paper sizes appear in the Authorized Send Scan Settings screen.

1. Click [Scan Settings] → [Customize Paper Sizes].



The Customize Paper Sizes screen appears

2. Configure the settings under <Customize Paper Sizes>.



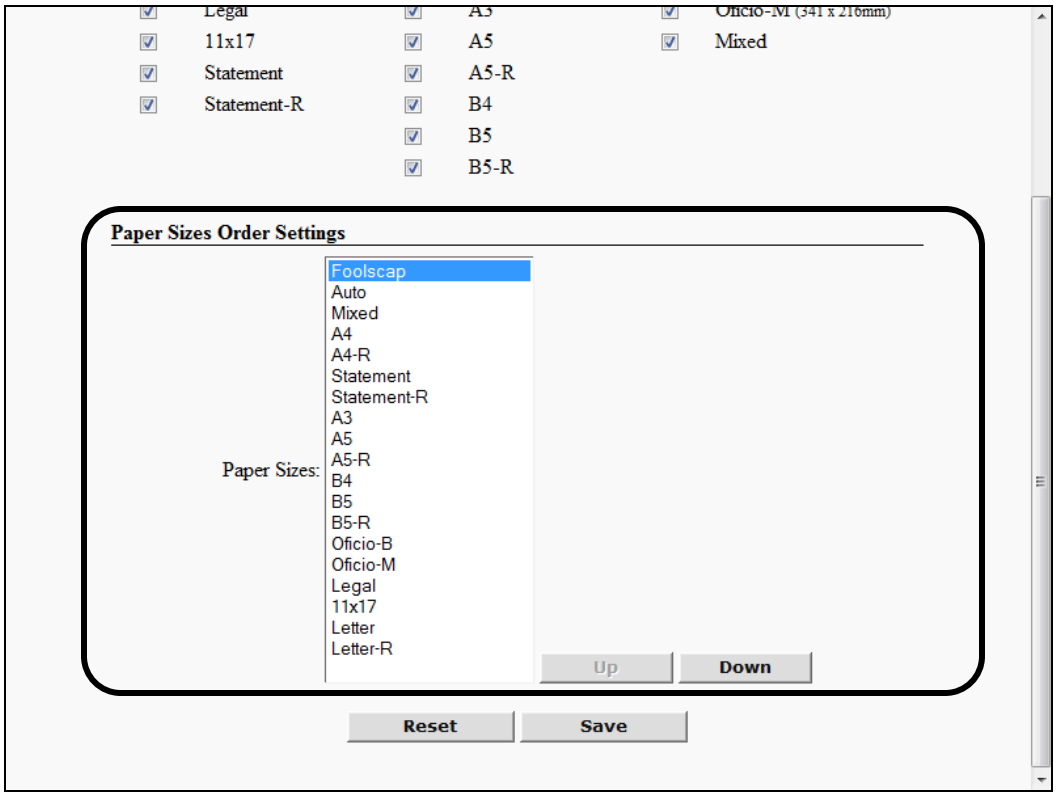
Customize Paper Sizes

Enabled Column — Select the check box next to the paper sizes you want to enable in the Authorized Send scan setting screen. The paper sizes listed are limited to the sizes that the machine can support.

IMPORTANT

Your machine requires extra configuration in order to use special paper sizes (e.g., Foolscap, Oficio, etc.). Contact your Authorized Send dealer to have your machine properly configured.

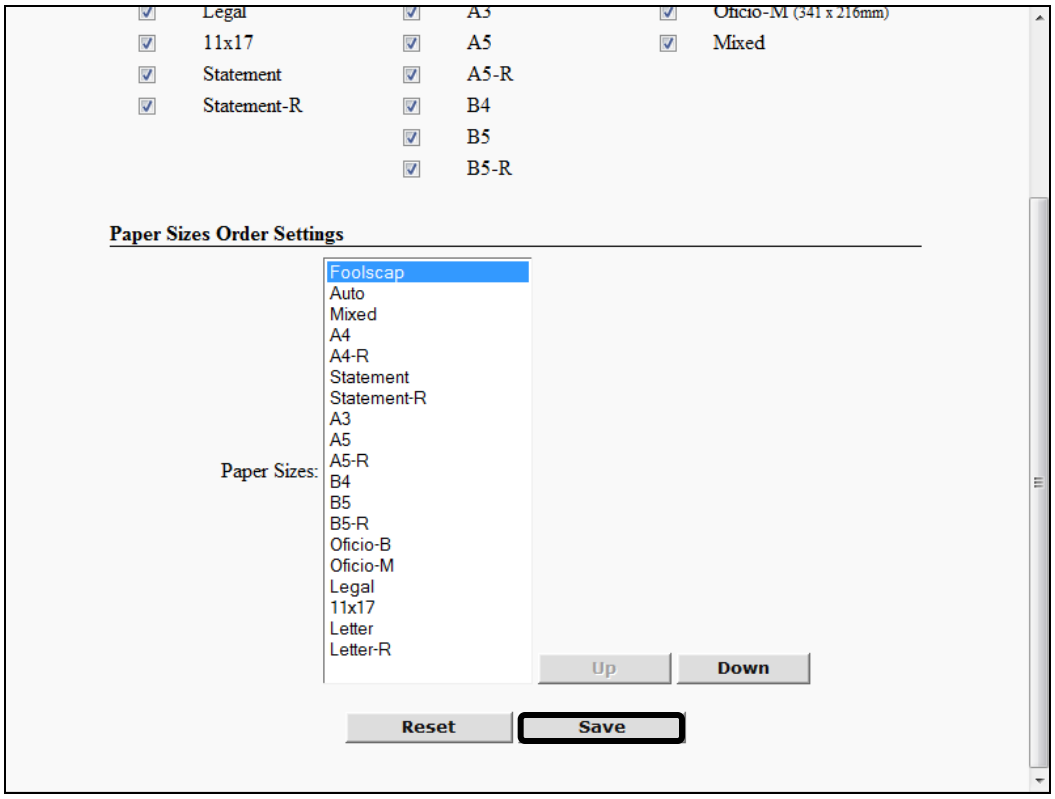
3. Configure the order in which the enabled paper sizes appear under <Paper Sizes Order Settings>.



Paper Sizes Order Settings

Click on the paper size you want to move, and click [Up] or [Down] to move it up or down in the list.

4. Click [Save].



If you made a mistake or want to start over using the original settings, click [Reset].

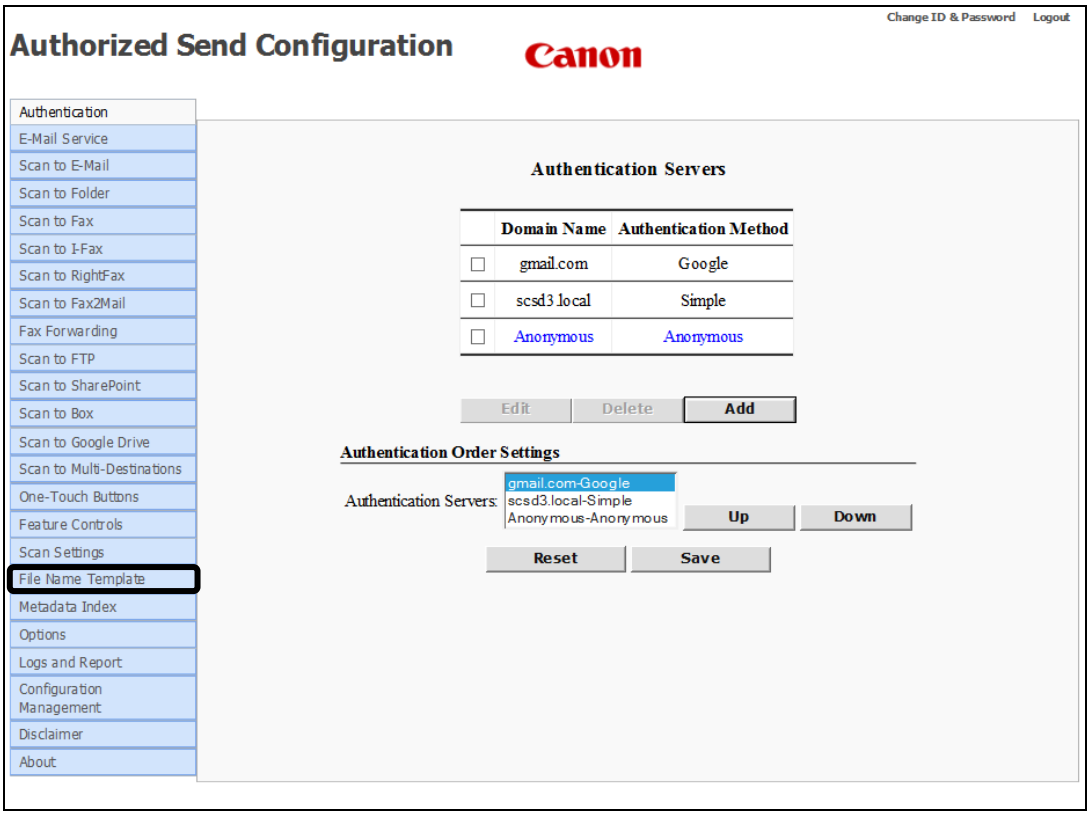
2.21 Configuring the File Name Template

You can configure the File Name Template function, which defines the syntax for file names and how users are expected to provide input for flexible file names. These file names are stored in templates, and the templates can be used in in the functions: Scan to E-mail, Scan to I-fax, Scan to Folder, Scan to FTP, Scan to SharePoint, and One-Touch Buttons.

You can create up to 10 send file name templates.

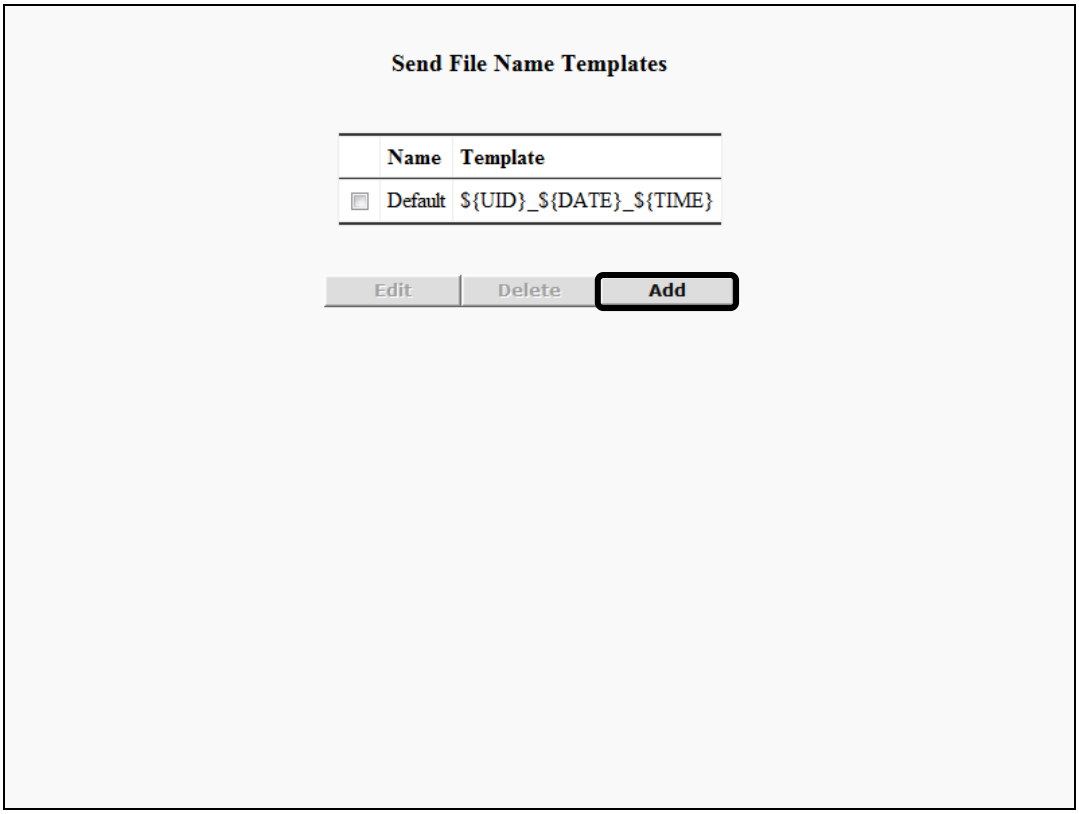
---

1. Click [File Name Template].



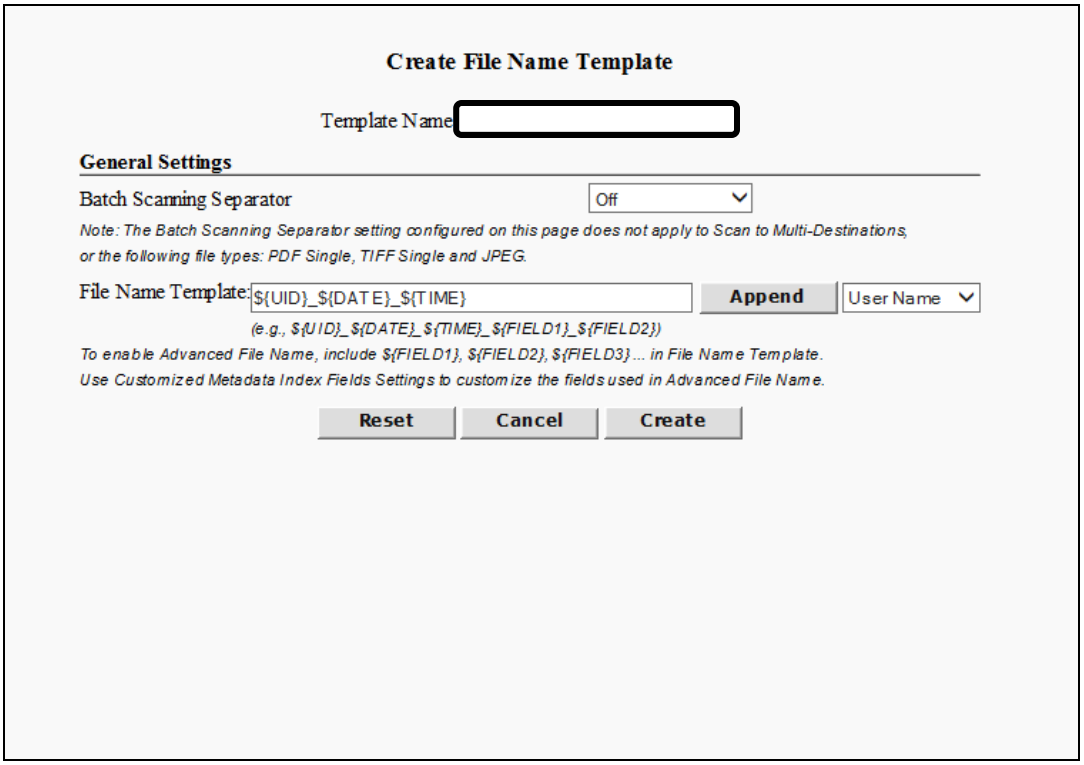
The Send File Name Templates screen is displayed.

2. Click [Add].



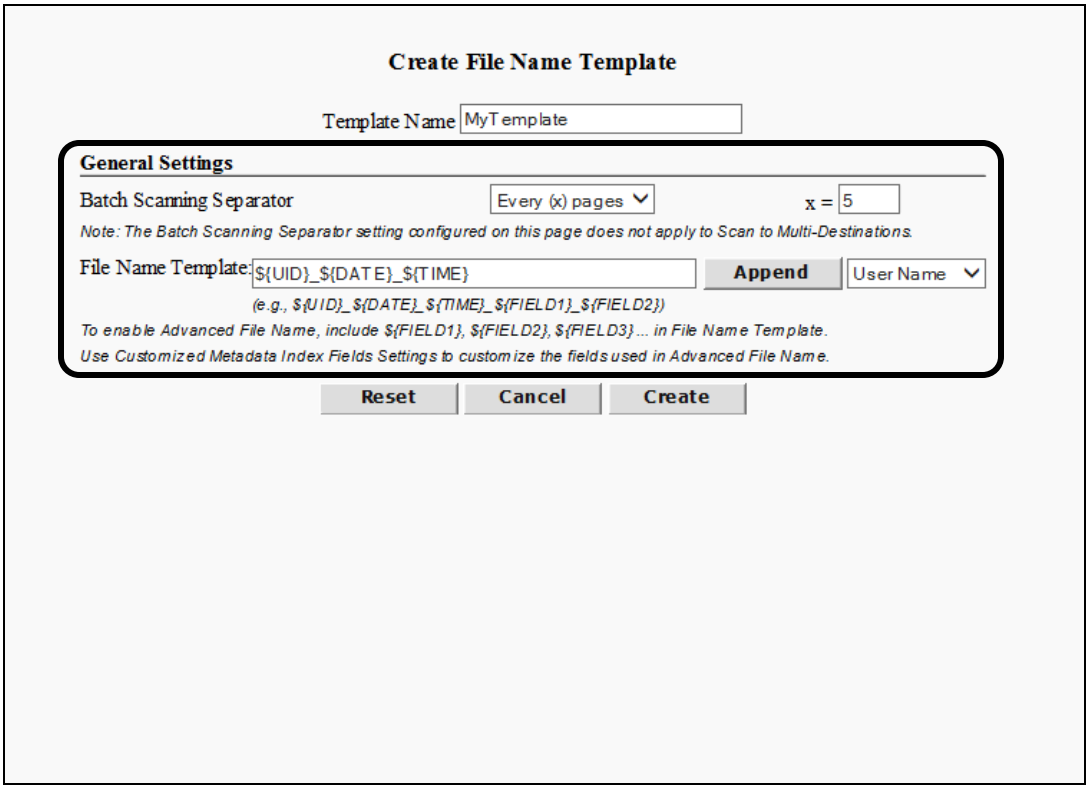
The Create File Name Template screen is displayed.

3. Enter a name for the template you want to create in the [Template Name] text box.



Template Name: Enter a name for the template you want to create in this text box. This name is added to the selection list on the Send File Name Templates screen. This text box is required. You can enter a string that consists of any character, and a maximum of 31 characters. The template name is case-sensitive and must be unique.

4. Configure the settings under <General Settings>.



General Settings

Batch Scanning Separator:

Scan jobs can be separated into individual batches. Select the desire batch limit from the [Batch Scanning Separator] pull-down list.

Off – A scan job is sent in its entirety in one pass. This is the default.

Every (x) Pages – The maximum size of any individual batch is defined by (x). This option causes the [X=] text field to appear.

Blank Page – The delineation between batches is a blank page. The device must support blank page detection for this option to function.

Barcode – The delineation between batches is a page with a barcode. The device must support barcode detection and have the Authorized Send Barcode package installed.

X=	This field only displays when [Batch Scanning Separator] is set to “Every (x) Pages”. Enter the maximum number of pages which can be part of a batch. The value must be a whole number between 1 and 999 (inclusive). The default value is 5.
File Name Template:	Enter the custom string to be used as part of the file name when sending a scanned document. Click [Append] to configure where you want the different variables, which you select from the Append drop-down list, to appear in the file name string. You can enter a string that consists of any character, and an unlimited number of characters. The default setting is ‘${UID}_${DATE}_${TIME}’. *For example, if you enter **${UID}_${DATE}** as the string, the document is sent using the string as the file name, where ${UID} is substituted by the user name used in the scan session, and ${DATE} is substituted by the scan date.*
Append:	Click [Append] to add the value set in the Append drop-down list to the string in the [File Name Template] text box.
Append drop-down:	Select [User Name], [Date], [Time], [Device IP], or [Index Field 1] through [Index Field 8]. If you click [Append] along with selecting an item from the Append drop-down list, the selected value is appended as a variable name to the string in the [File Name Templates] text box. You can select more than one value to append to the file name string. See the configuration of customized index fields in Section 2.17 for an explanation of [Index Field 1] through [Index Field 8]. NOTE If the Barcode package is installed, the [Barcode] selection is available in the Append drop-down. The ${BARCODE} variable will be replaced by the barcode found (if any) during the scan. See “Configuring a Barcode Policy,” on page 419.

NOTE

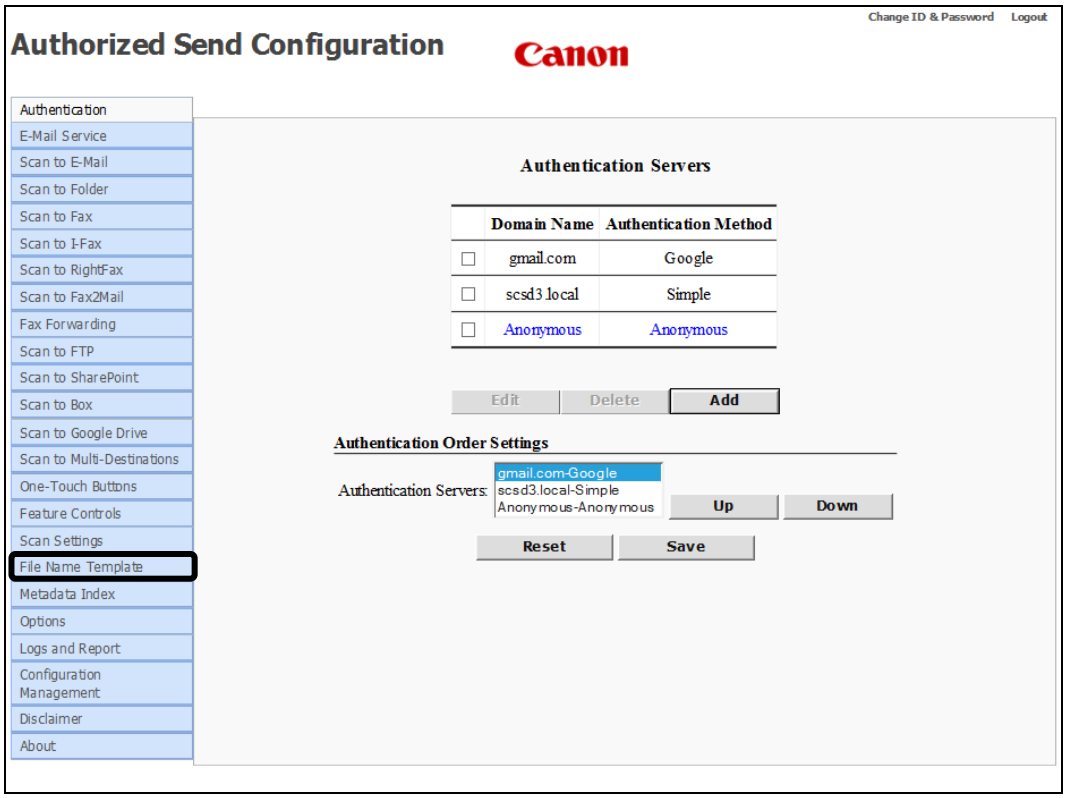
If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

Click [Cancel] to stop creating a new file name template and return to the Send File Name Templates screen.

2.21.1 Editing a File Name Template

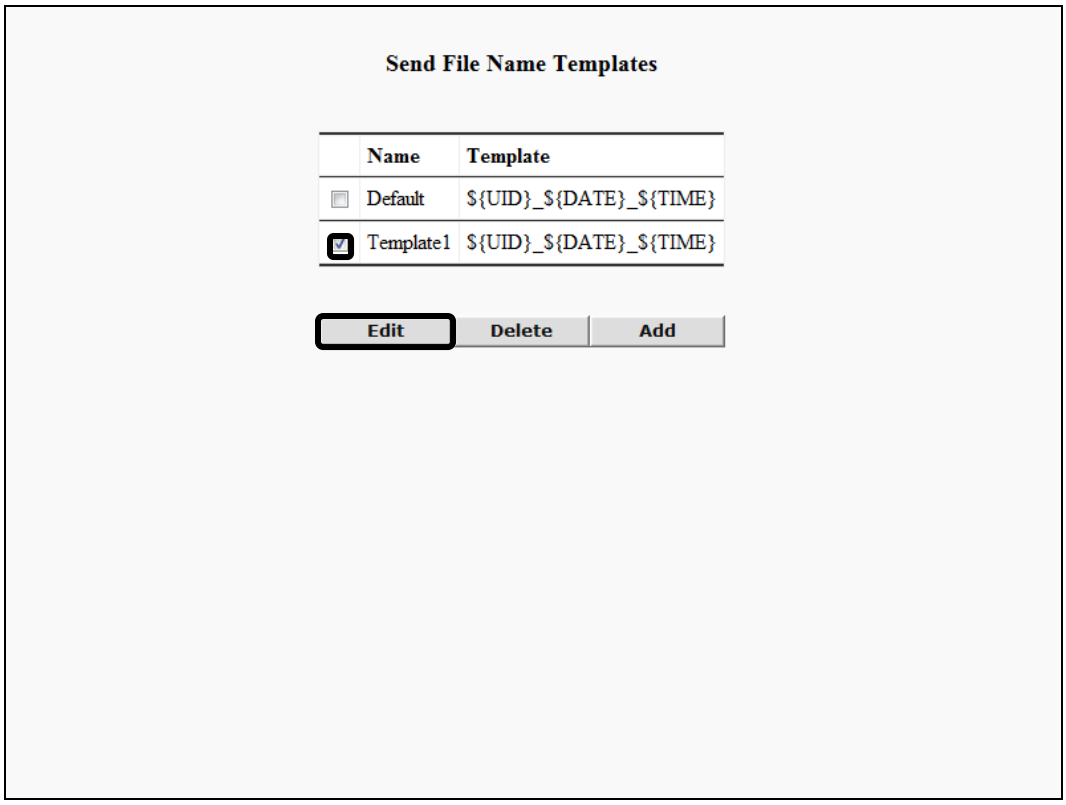
You can edit a previously created file name template from the Send File Name Templates configuration screen.

1. Click [File Name Template]



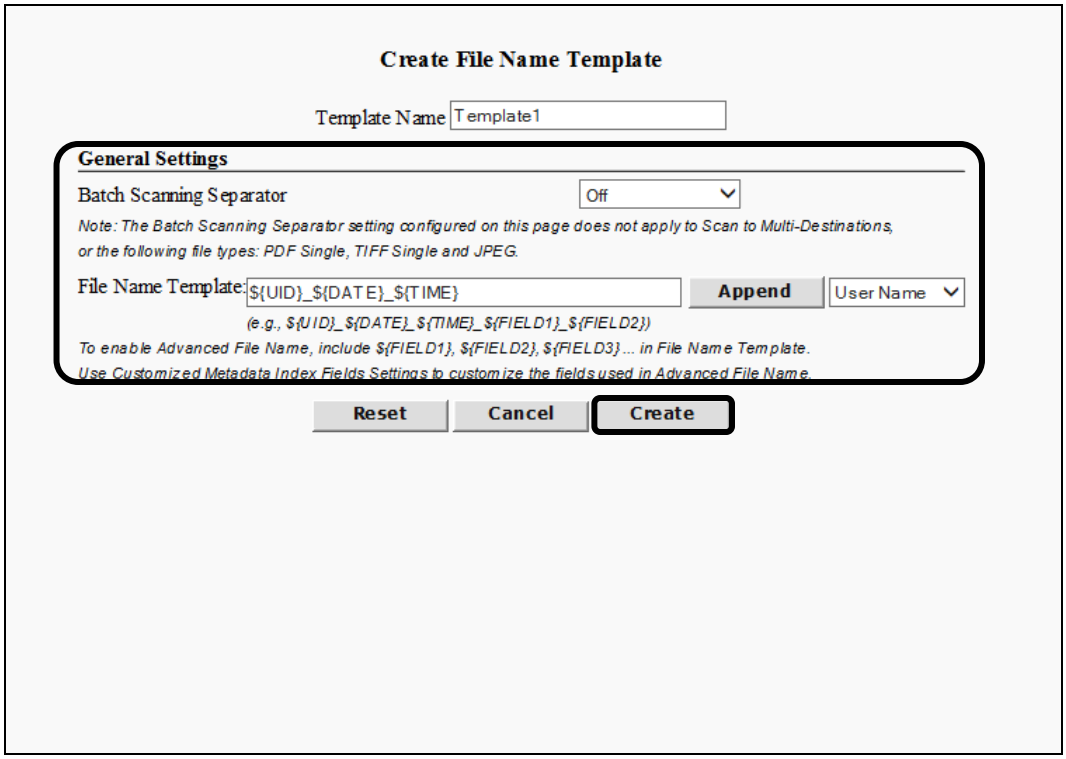
The Send File Name Templates screen appears.

2. Select the check box next to the file name template you want to edit → click [Edit].



The Update File Name Template screen is displayed.

3. Edit the settings for the file name template, as necessary → click [Update].



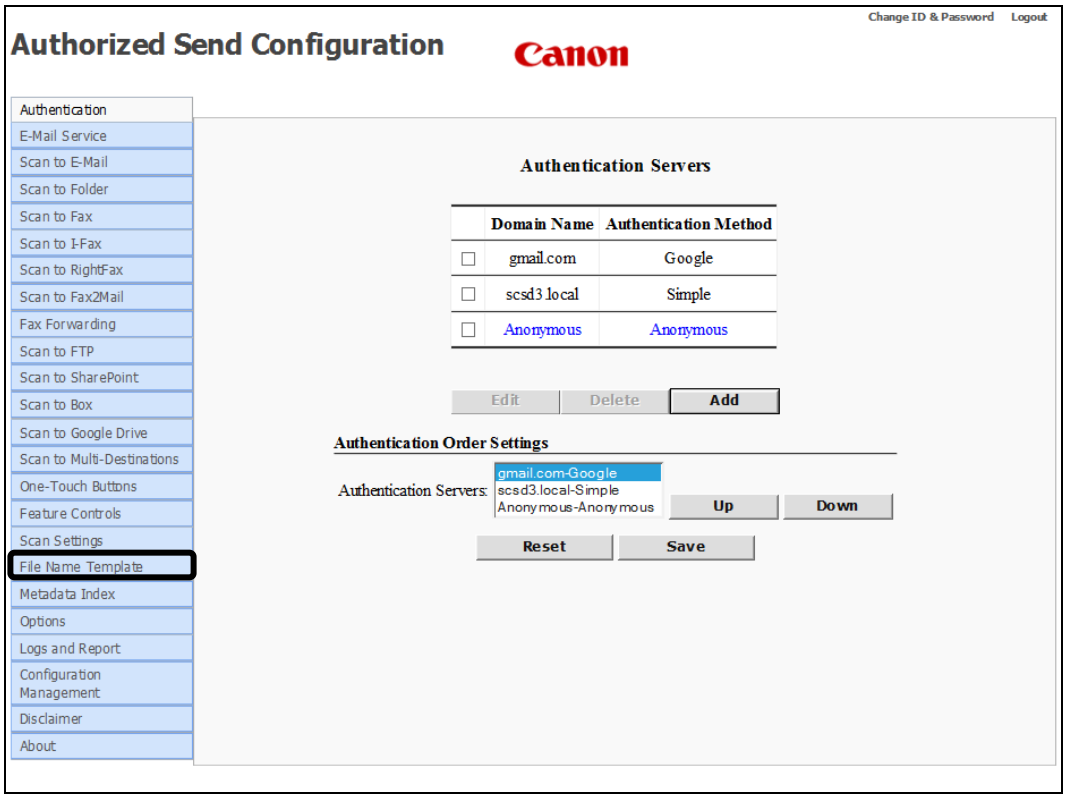
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the file name template and return to the Send File Name Templates configuration screen, click [Cancel].

2.21.2 Deleting a File Name Template

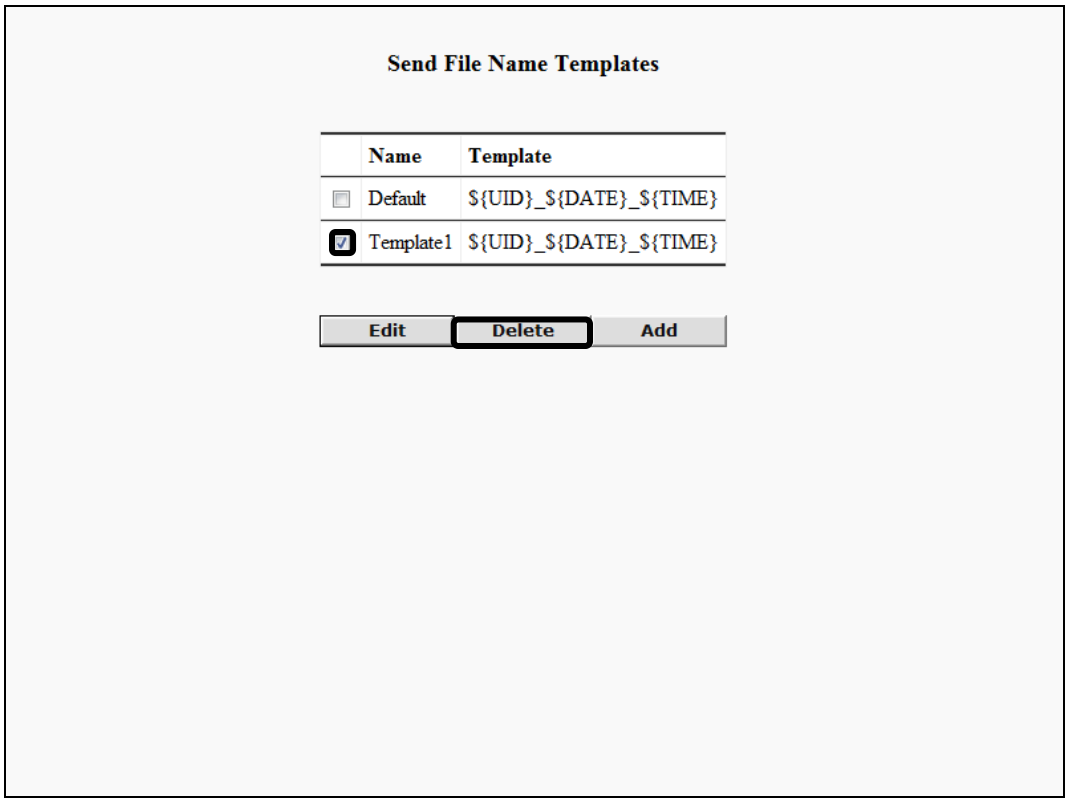
You can delete a previously created file name template from the Send File Name Templates configuration screen.

1. Click [File Name Template]

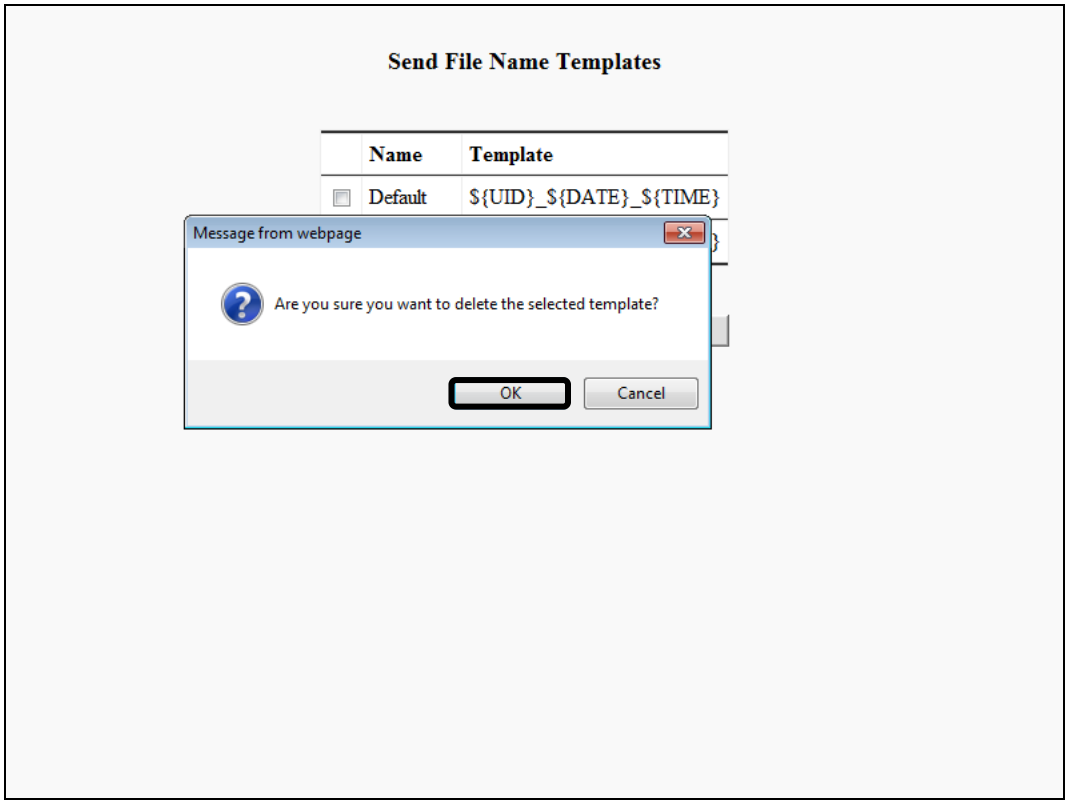


The Send File Name Templates screen appears.

2. Select the check box next to the file name template you want to delete → click [Delete].



3. Click [OK] on the confirmation dialog box.



If you do not want to delete the file name template, click [Cancel].

The file name template is deleted from the list.

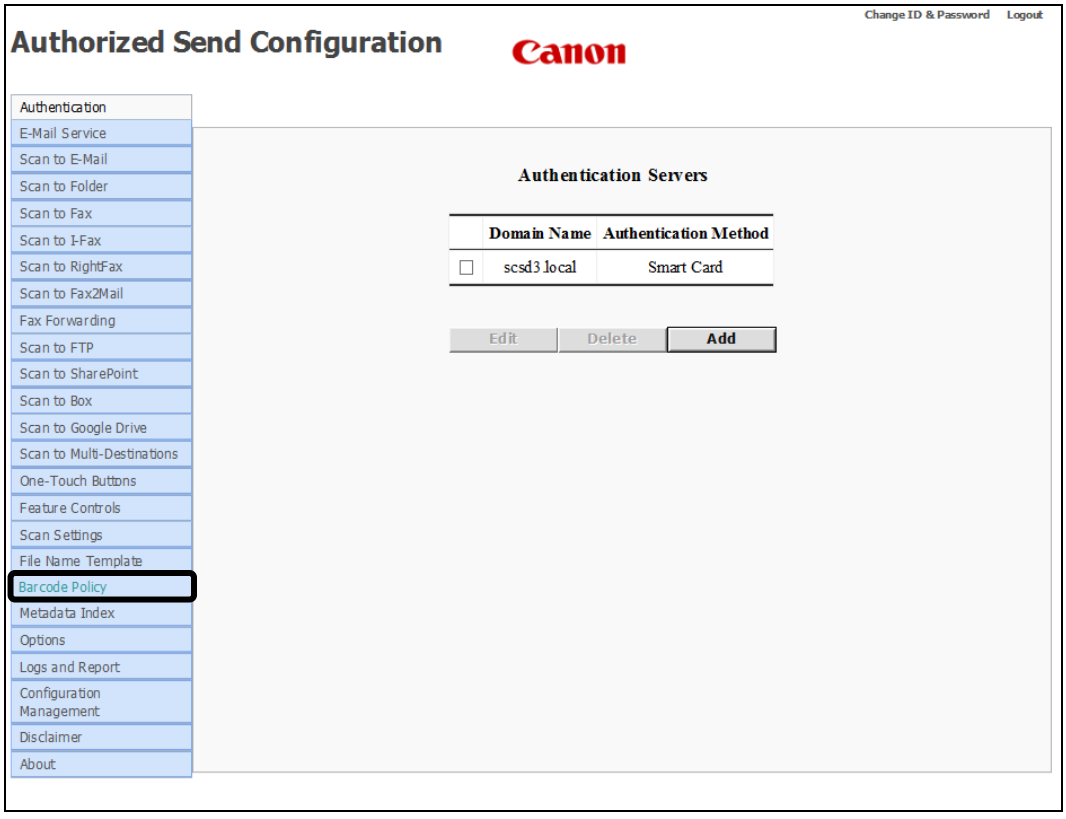
2.22 Configuring a Barcode Policy

NOTE

The Barcode feature requires installation of the Barcode Feature Activation package. See the *Authorized Send Version 6.4 Installation Guide* for information. If the Barcode Feature Activation package is not installed, the [Barcode Policy] menu option does not appear.

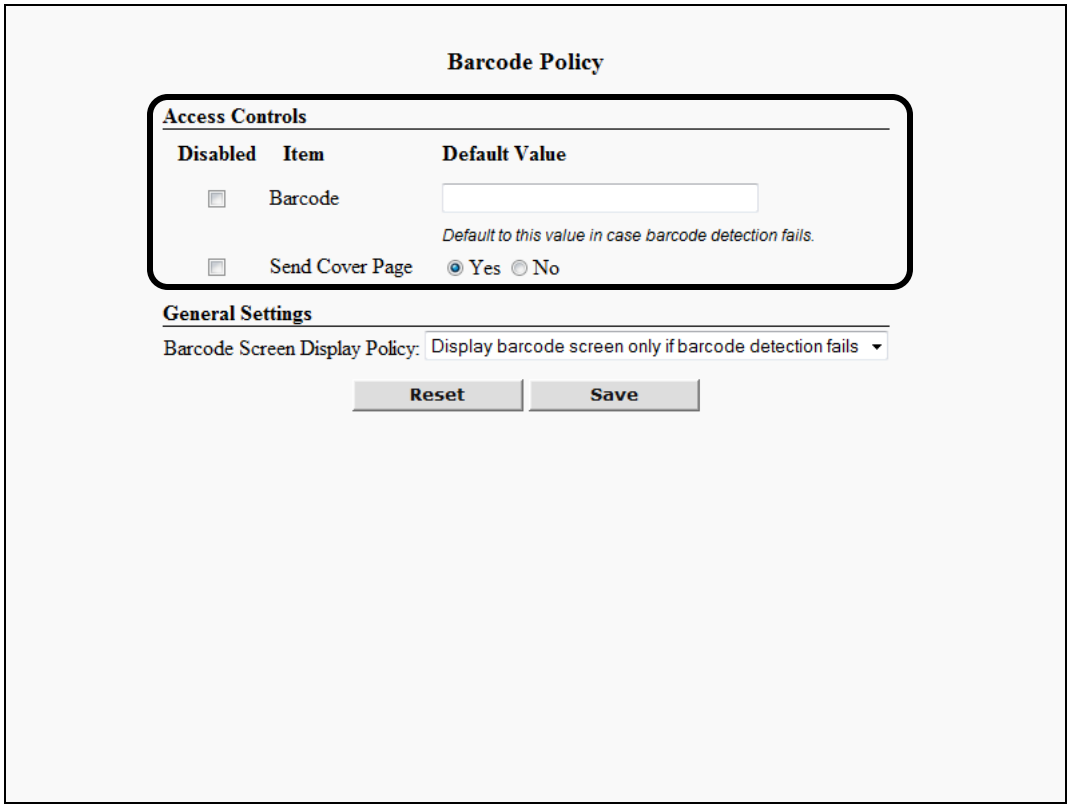
The optional barcode software allows Authorized Send to read barcode cover sheets and use the barcode as metadata.

1. Click [Barcode Policy].



The Barcode Policy screen appears.

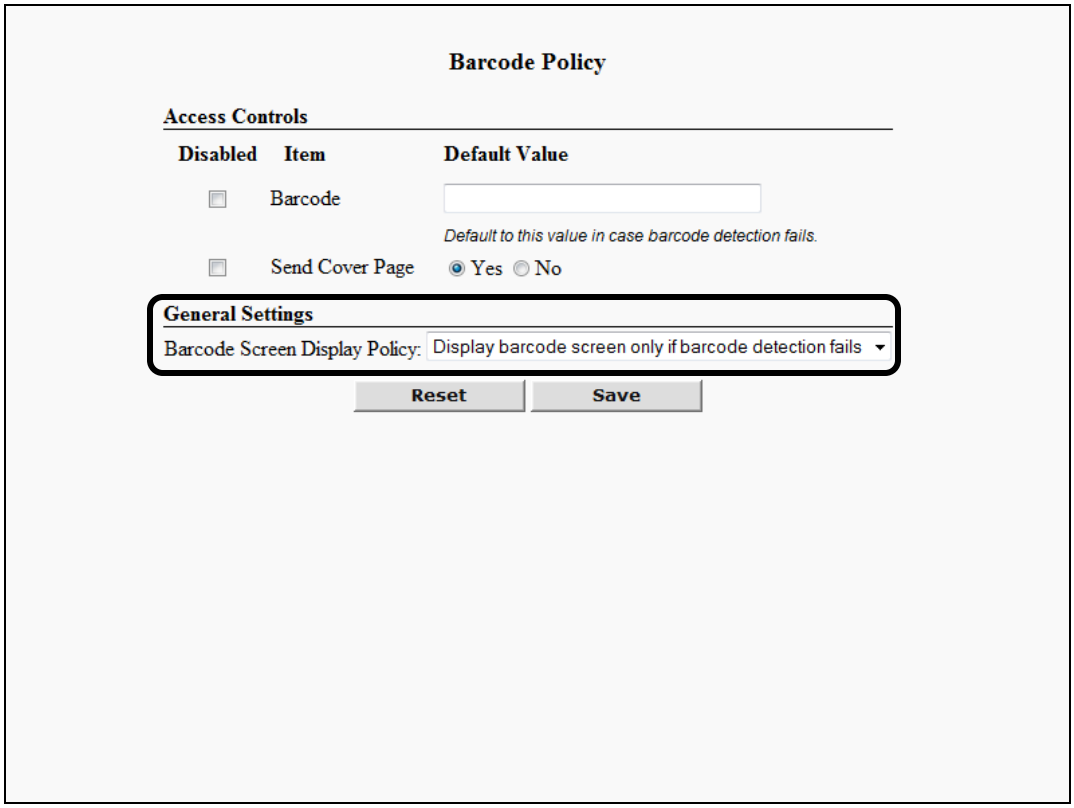
2. Configure the settings under <Access Controls>.



Access Controls

Disabled Column Barcode: Send Cover Page:	By default, each check box in this column is not selected. Select the check boxes next to the desired settings that you want to disable and gray out on the Authorized Send Barcode screen on the machine
Barcode:	Enter the default value you want to appear in the [Barcode] text box on the Authorized Send Barcode screen.
Send Cover Page:	Set the default value of the [Send Cover Page] check box on the Authorized Send Barcode screen.

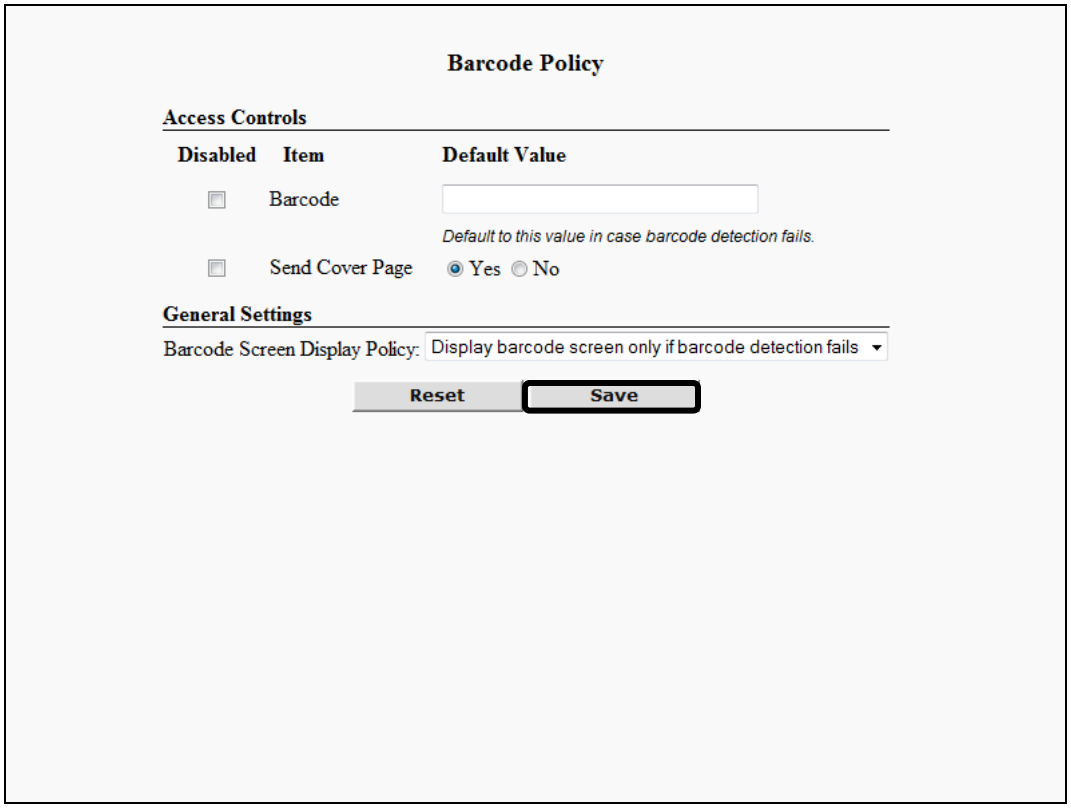
3. Configure the settings under <General Settings>.



General Settings

Barcode Screen Display Policy:	Use the pull down list to select the desired behavior when scanning using barcodes. Select [Do not display barcode screen] to prevent Authorized Send from bringing up the Barcode screen, even if no barcode is detected on the cover page. Select [Display barcode screen only if barcode detection fails] to have Authorized Send bypass the barcode screen if it detects a barcode on the cover page. Select [Display barcode screen always] to have Authorized Send always display the barcode screen, even if it successfully reads a barcode from the cover page.

4. Click [Save].

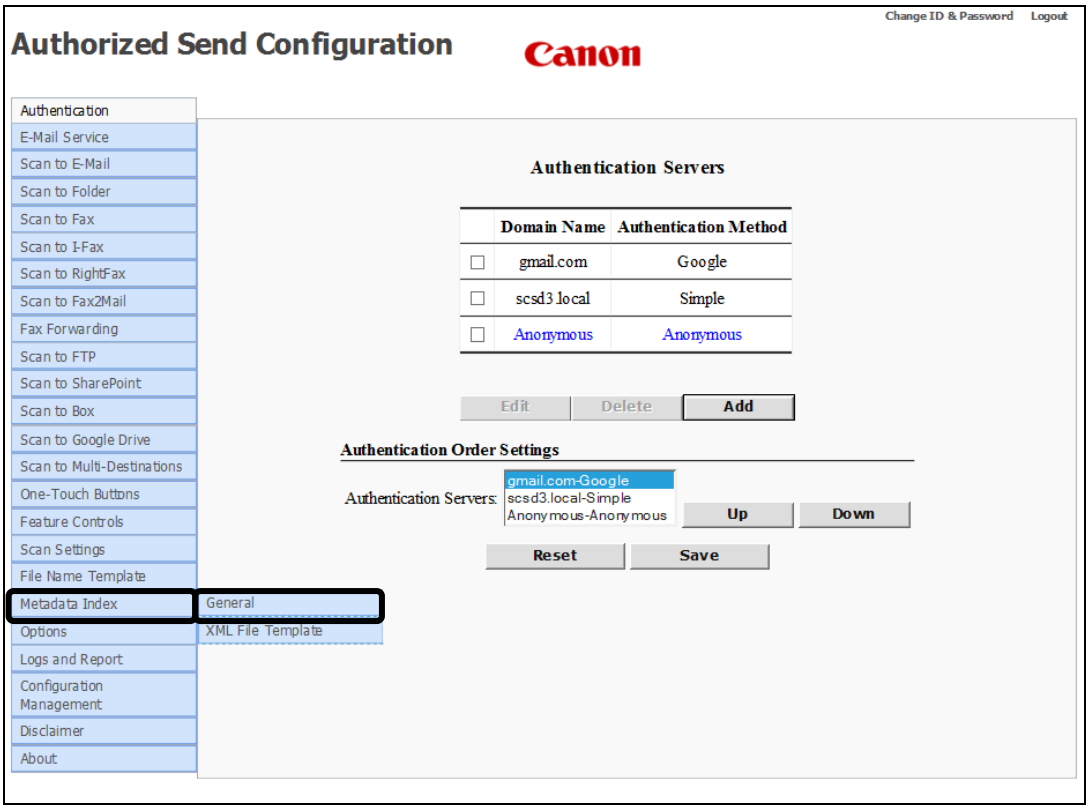


If you made a mistake or want to return to the previous values, click [Reset].

2.23 Configuring the Metadata Index Settings

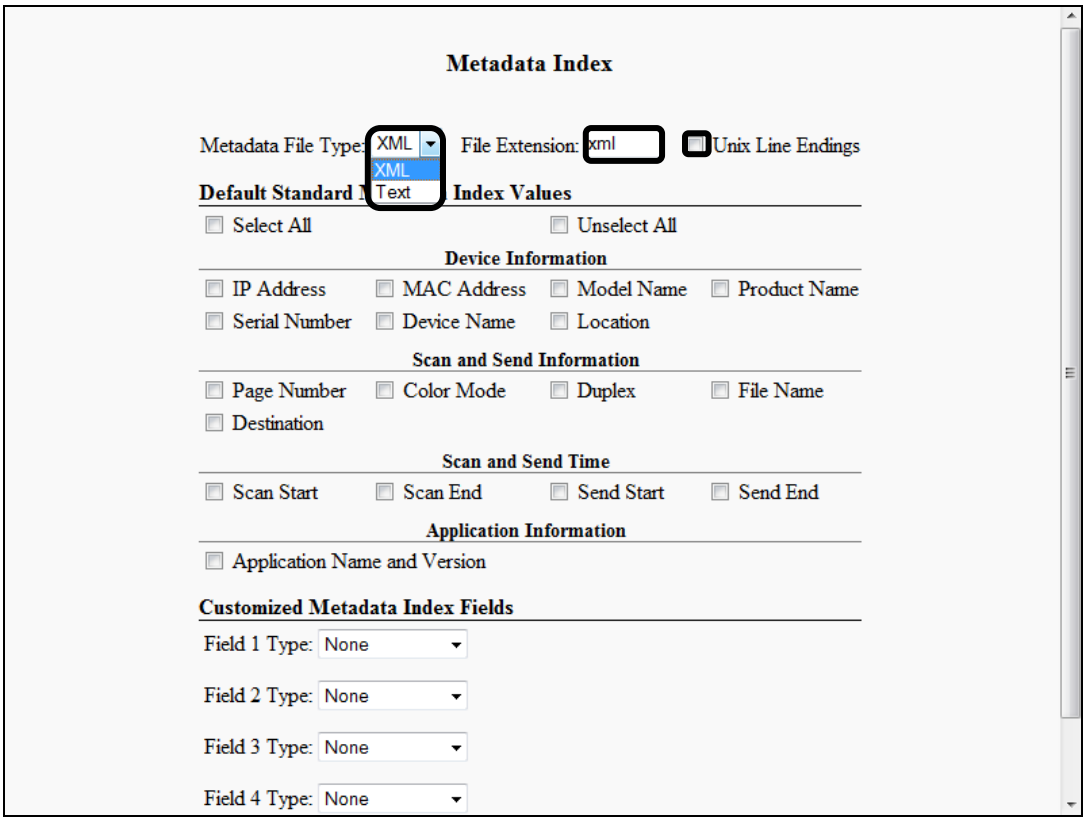
You can configure the Metadata Index function, which is used for the metadata file format and contents.

1. Click [Metadata Index] → [General].



The Metadata Index screen is displayed.

2. Configure the Metadata File Type drop-down list, [File Extension] text box, and [Unix Line Endings] check box.



Metadata File Type: Select [XML] or [Text] from the drop-down list as the file type for the output metadata. The default setting is 'XML'.

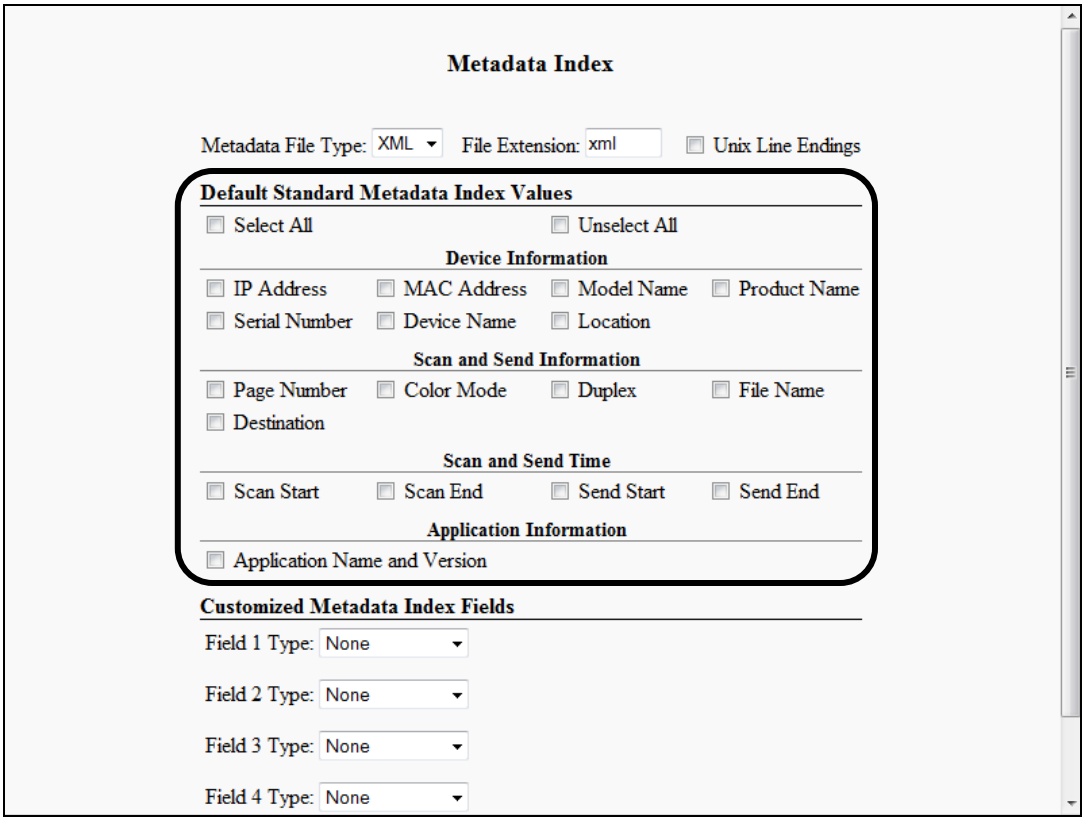
File Extension: Enter the file extension to use for the created metadata file. You can enter a maximum of 10 alphanumeric characters. The default setting is 'xml', if the selected Metadata File Type is [XML], and 'txt' if the selected Metadata File Type is [Text].

NOTE

- Only alphanumeric characters can be used.
- Validation is performed after you click [Save] to make sure that:
  - The [File Extension] text box is not empty.
  - Up to 10 alphanumeric characters has not been exceeded.
- If validation fails, an error message is displayed.

Unix Line Endings: Select this check box if you want the output of the metadata file to be compatible with Unix machines. This check box is not selected by default.

3. Configure the settings under <Default Standard Metadata Index Values>.



Select the [Select All] check box to select all check boxes in the Default Standard Metadata Index Values section. Select the [Unselect All] to reset all check boxes in the Default Standard Metadata Index Values section.

Device Information

Select the [IP Address], [MAC Address], [Model Name], [Product Name], [Serial Number], [Device Name], and [Location] check boxes to include these data items in the metadata file.

Scan and Send Information

Select the [Page Number] (number of pages that make up the document you scanned and sent), [Color Mode], [Duplex], [File Name] and [Destination] check boxes to include these data items in the metadata file.

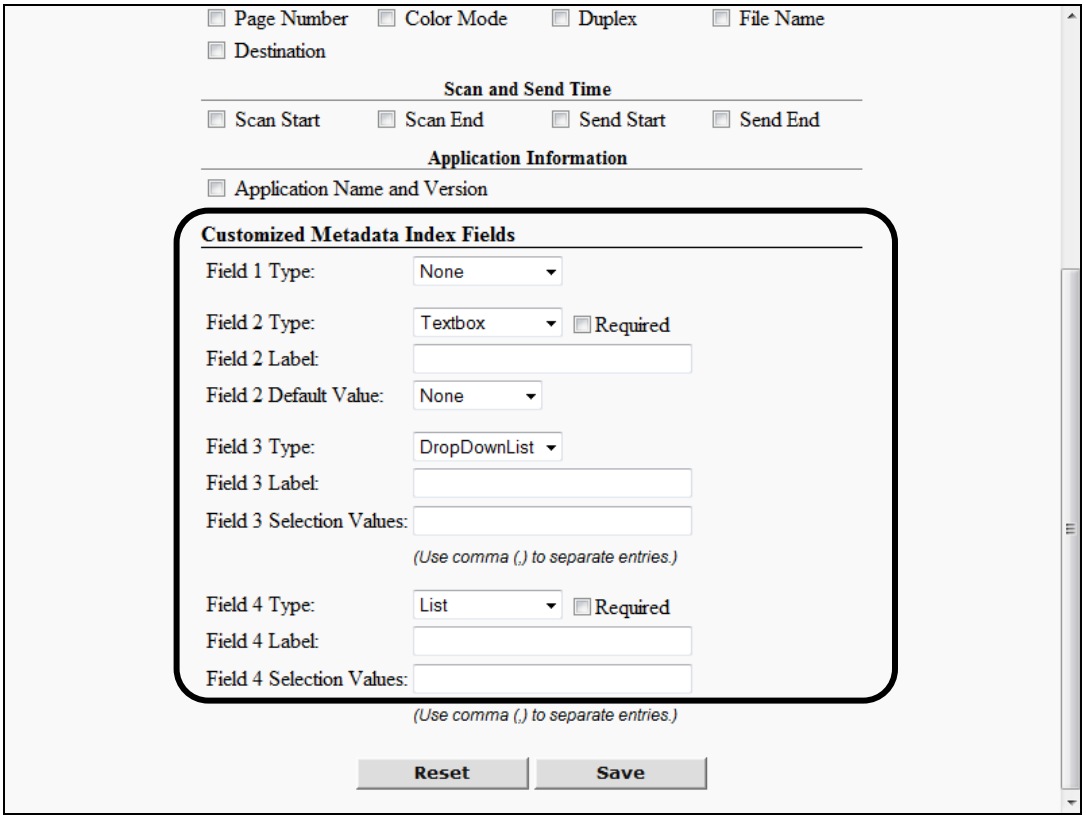
Scan and Send Time

Select the [Scan Start], [Scan End], [Send Start], and [Send End] check boxes to include these data items in the metadata file.

Application Information

Application Name and Version:	Select this check box to include the application name and version data in the metadata file.

4. Configure the settings under <Customized Metadata Index Fields>.



You can customize up to eight metadata index fields to use as part of a file name template. The templates can be used for the following functions: Scan to E-Mail, Scan to I-fax, Scan to Folder, Scan to FTP, Scan to SharePoint, Scan to Multi-Destinations, and One-Touch Buttons.

NOTE

One-Touch Buttons can have their own localized metadata index fields which override those set here. For more information, see "Creating a Button Definition," on page 348.

By default, the initial number of metadata index fields that you can configure is four. How you configure the metadata index fields in the Authorized Send Configuration servlet, determines what data the user can enter or select for the metadata file on the Authorized Send CUSTOMIZED INDEX screen on the machine. Index Fields 1, 2, 3, and 4 are standard. However, if you select and save Index Field 4, an additional Index Field 5 is displayed. Selecting and saving Index Field 5 produces an additional Index Field 6, and so on. You can select a maximum of eight metadata index fields.

Select [None], [Textbox], [Masked Textbox] [DropDownList], or [List] for the standard Field Type drop-down lists 1 through 4 (and the additional Index Fields 5 through 8, if necessary). The default setting for all eight Field types is 'None', which hides the Authorized Send CUSTOMIZED INDEX screen on the machine, and prevents the user from inputting any metadata.

The examples below show the functionality for the standard four field types in the order they appear in the Field *x* Type drop-down list, where *x* can be numbers 1 to 4; however, the four field types can be made to appear in any order.

Field 1 Type:	If you select [None] from the drop-down list, this field is hidden on the Authorized Send CUSTOMIZED INDEX screen on the machine.
Field 2 Type:	If you select [Textbox] from the drop-down list, a text box appears on the Authorized Send CUSTOMIZED INDEX screen on the machine.
Required:	If you select this check box, the user must enter data in the text box on the Authorized Send CUSTOMIZED INDEX screen on the machine.
Field 2 Label:	Enter a label for the text box that appears on the Authorized Send CUSTOMIZED INDEX screen on the machine. You can enter a string that consists of any character, and a maximum of 30 characters. If the [Required] check box is selected, an asterisk (*) appears before the label's name on the Authorized Send CUSTOMIZED INDEX screen on the machine, indicating that this is a required field.
Field 3 Type:	If you select [DropDownList] from the drop-down list, a drop-down list appears on the Authorized Send CUSTOMIZED INDEX screen on the machine.

Field 3 Label:	Enter a label for the drop-down list that appears on the Authorized Send CUSTOMIZED INDEX screen on the machine. You can enter a string that consists of any character, and a maximum of 30 characters. The default value is the first value that appears in the drop-down list.
Field 3 Selection Values:	Enter the values in this text box separated by commas, which you want available for the user to select on the Authorized Send CUSTOMIZED INDEX screen on the machine. For each value, you can enter a string that consists of any character, except for a comma ‘,’, which is used as a delimiter. Each individual selection value cannot exceed a maximum of 255 characters. The maximum number of selectable values cannot exceed 20.
Field 4 Type:	If you select [List] from the drop-down list, a list box appears on the Authorized Send CUSTOMIZED INDEX screen on the machine.
Required:	If you select this check box, the user must select a value in the list box on the Authorized Send CUSTOMIZED INDEX screen on the machine.
Field 4 Label:	Enter a label for the list box that appears on the Authorized Send CUSTOMIZED INDEX screen on the machine. You can enter a string that consists of any character, and a maximum of 30 characters. If the [Required] check box is selected, an asterisk (*) appears before the label’s name on the Authorized Send CUSTOMIZED INDEX screen on the machine, indicating that this is a required field.
Field 4 Selection Values:	Enter the values in this text box, separated by commas, which you want available for the user to select on the Authorized Send CUSTOMIZED INDEX screen on the machine. For each value, you can enter a string that consists of any character, except for a comma ‘,’, which is used a delimiter. Each individual selection value cannot exceed a maximum of 255 characters. The maximum number of selectable values cannot exceed 20.

5. Click [Save].

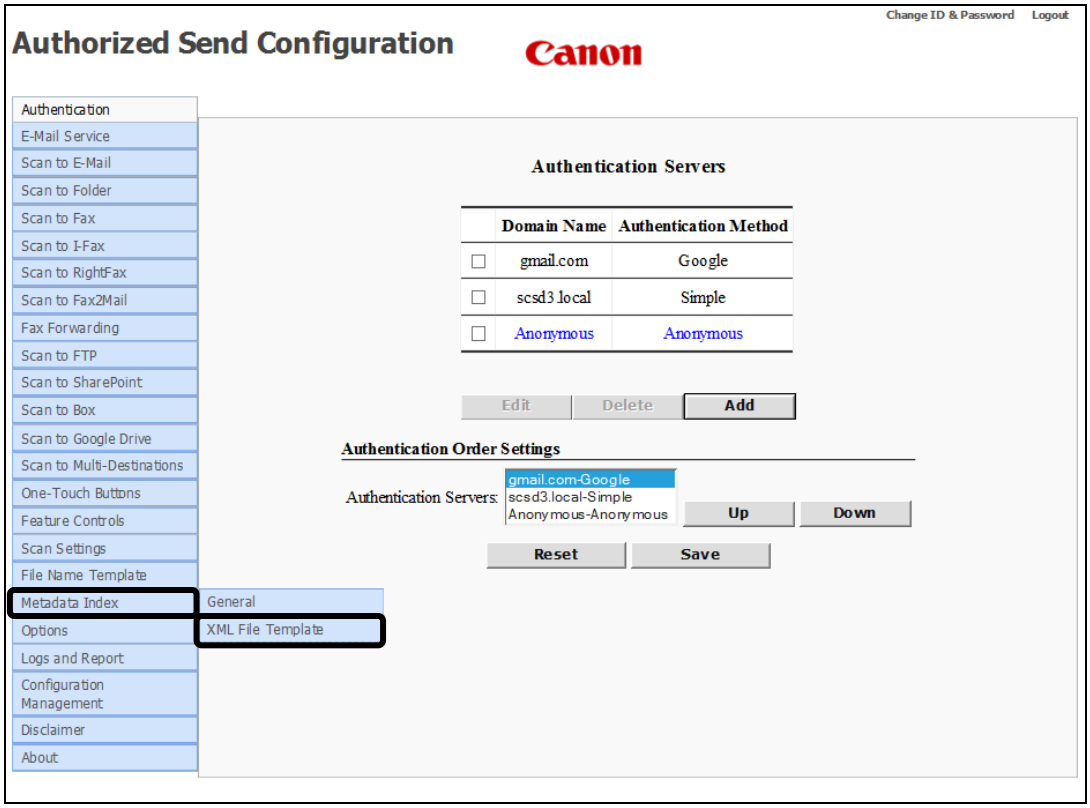
NOTE

If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.23.1 Creating a Metadata XML File Template

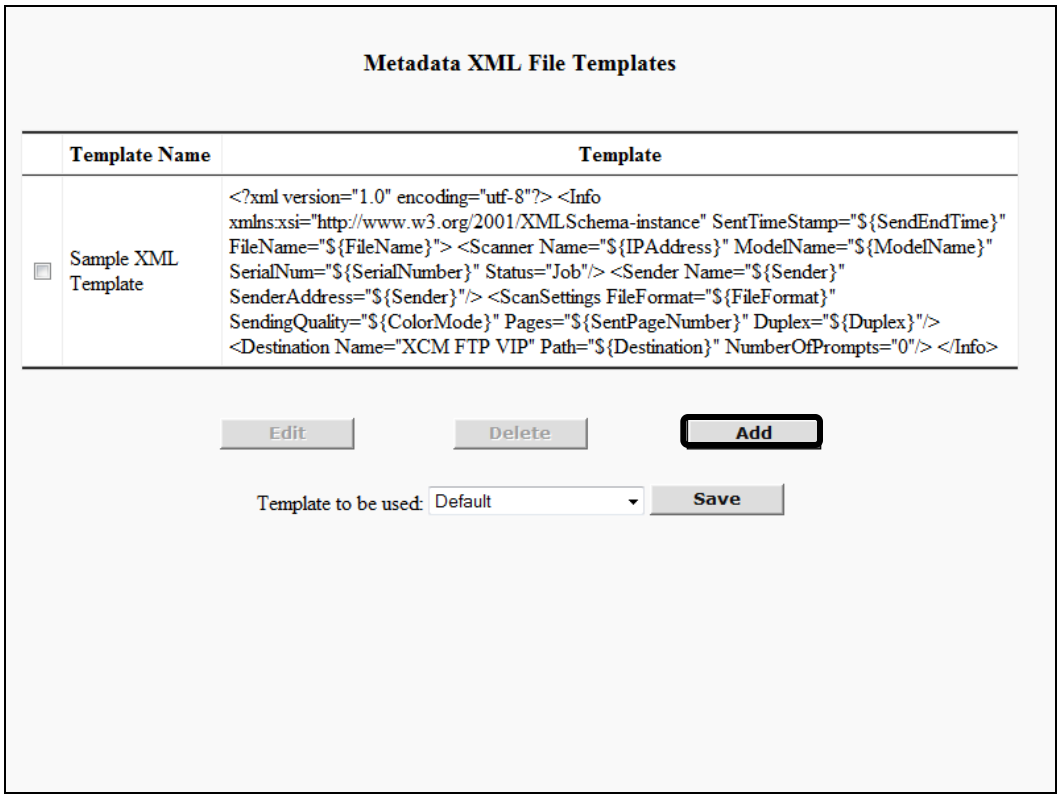
You can create a metadata XML file template.

1. Click [Metadata Index] → [XML File Template].



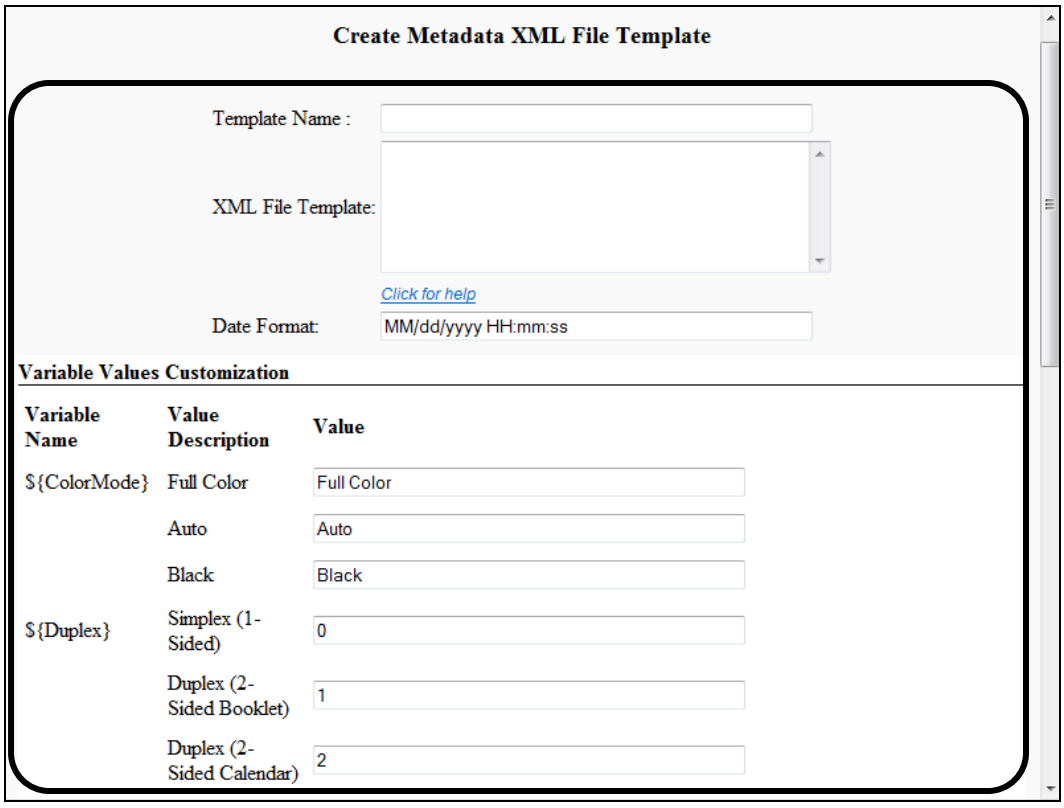
The Metadata XML File Templates screen is displayed.

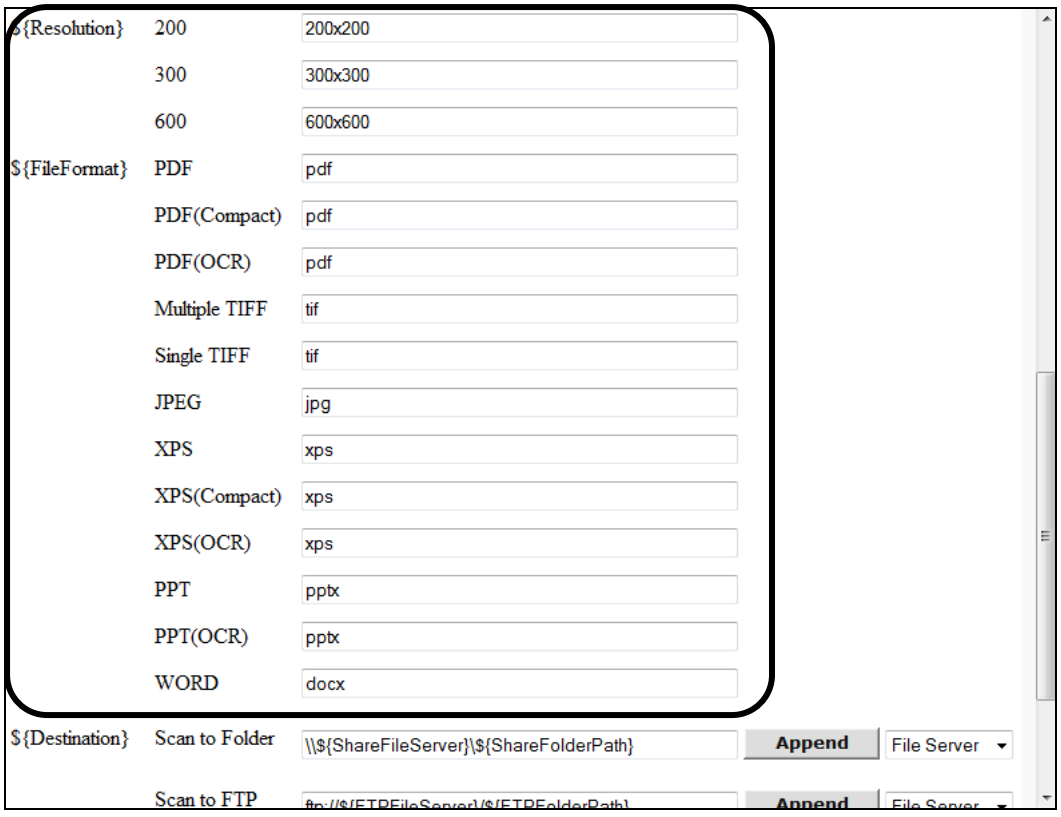
2. Click [Add].

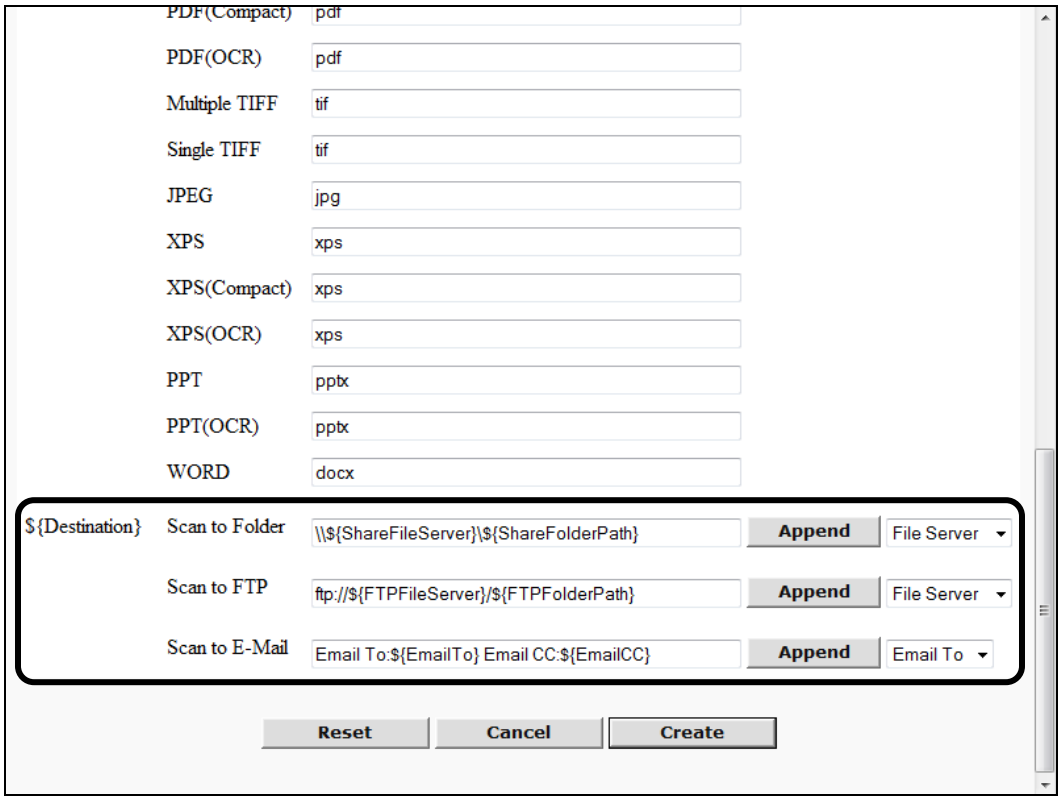


The Create Metadata XML File Template screen is displayed.

3. Configure the Create Metadata XML Template settings.







Template Name: Enter a name for your XML template file in this text box. You can enter a string that consists of any character, and a maximum of 31 characters. This is a required text box that cannot be left blank.

XML File Template: This text box holds your customized XML file template. Select the [Click for help] hyperlink to display the Metadata XML Template Help screen ➞ copy the text under <Sample Metadata XML File Template> ➞ paste it into the [XML File Template] text box ➞ modify the contents, as needed to make your customized XML file template. You can enter a string that consists of any character, and an unlimited number of strings. This is a required text box that cannot be left blank.

Date Format: Enter the value in which you want your customized XML metadata file template to use for the Date Format for the start and end times of scanning and sending documents. You can enter a string that consists of any character, and a maximum of 19 characters. This is a required text box that cannot be left blank. The default format is 'MM/dd/yyyy HH:mm:ss'.

Variable Values Customization

Variable Name: ${ColorMode}

Full Color: Enter the value that you want your customized XML metadata file template to use for Full Color. You can enter a string that consists of any character, and a maximum of 19 characters. This is a required text box that cannot be left blank. The default setting is 'Full Color'.

Auto: Enter the value that you want your customized XML metadata file template to use for Auto. You can enter a string that consists of any character, and a maximum of 19 characters. This is a required text box that cannot be left blank. The default setting is 'Auto'.

Black: Enter the value that you want your customized XML metadata file template to use for Black. You can enter a string that consists of any character, and a maximum of 15 characters. This is a required text box that cannot be left blank. The default setting is 'Black'.

${Duplex}

Simplex (1-Sided): Enter the value that you want your customized XML metadata file template to use for Simplex (1-Sided). You can enter a string that consists of any character, and a maximum of 15 characters. This is a required text box that cannot be left blank. The default setting is ‘0’.

Duplex (2-Sided): Enter the value that you want your customized XML metadata file template to use for Duplex (2-Sided). You can enter a string that consists of any character, and a maximum of 15 characters. This is a required text box that cannot be left blank. The default setting is ‘1’.

${Resolution}

200: Enter the value you want your customized XML metadata file template to use for 200 dpi resolution. You can enter a string that consists of any character, and a maximum of 15 characters. This is a required text box that cannot be left blank. The default setting is ‘200x200’.

300: Enter the value you want your customized XML metadata file template to use for 300 dpi resolution. You can enter a string that consists of any character, and a maximum of 15 characters. This is a required text box that cannot be left blank. The default setting is ‘300x300’.

600: Enter the value you want your customized XML metadata file template to use for 600 dpi resolution. You can enter a string that consists of any character, and a maximum of 15 characters. This is a required text box that cannot be left blank. The default setting is ‘600x600’.

${FileFormat}

Enter the extension you want your customized XML metadata file template to use for each file format. The file formats displayed are only available if your machine supports them. You can enter a string that consists of any character, and a maximum of 15 characters. These are required text boxes that cannot be left blank.

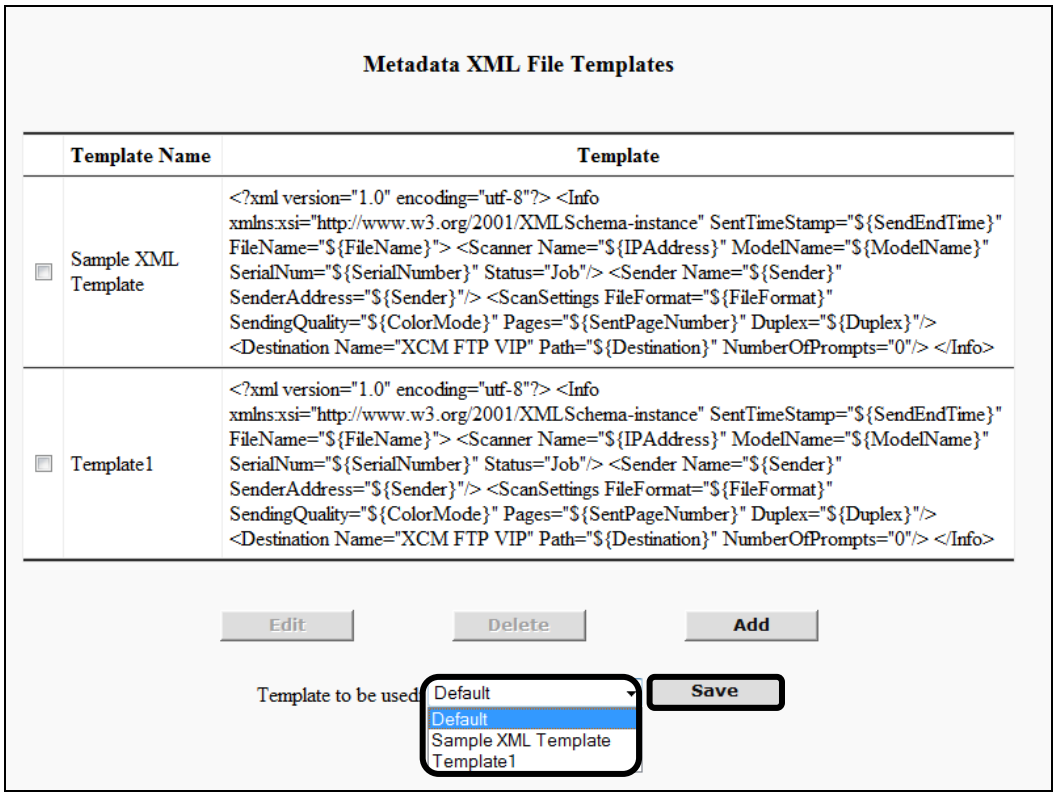
${Destination}

Scan to Folder:	Enter the destination that you want your customized XML metadata file template to use for Scan to Folder. You can enter a string that consists of any character. This is a required text box that cannot be left blank. The default setting is '\\${ShareFileServer}\${ShareFolderPath}'.
Append:	Click [Append] to add the value set in the Append drop-down list to the string in the [Scan to Folder] text box.
Append drop-down:	Select [File Server] or [Folder Path] from this drop-down list. If you click [Append] along with selecting an item from the Append drop-down list, the selected value is appended as a variable name to the string in the [Scan to Folder] text box.
Scan to FTP:	Enter the destination you want your customized XML metadata file template to use for Scan to FTP. You can enter a string that consists of any character. This is a required text box that cannot be left blank. The default setting is 'ftp://${FTPFileServer}/${FTPFolderPath}'.
Append:	Click [Append] to add the value set in the Append drop-down list to the string in the [Scan to FTP] text box.
Append drop-down:	Select [File Server] or [Folder Path] from this drop-down list. If you click [Append] along with selecting an item from the Append drop-down list, the selected value is appended as a variable name to the string in the [Scan to FTP] text box.
Scan to E-Mail:	Enter the destination you want your customized XML metadata file template to use for Scan to E-Mail. You can enter a string that consists of any character. This is a required text box that cannot be left blank. The default setting is '${EmailTo} Email CC:${EmailCC}'.
Append:	Click [Append] to add the value set in the Append drop-down list to the string in the [Scan to E-Mail] text box.
Append drop-down:	Select [Email To] or [Email CC] from this drop-down list. If you click [Append] along with selecting an item from the Append drop-down list, the selected value is appended as a variable name to the string in the [Scan to E-Mail] text box.

4. Click [Create].

NOTE
- If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.
- To cancel creating the metadata XML file template and return to the Metadata XML File Templates configuration screen, click [Cancel].

5. If you want to specify a metadata XML file template name that automatically populates the value in the Template to be used drop-down list, select a metadata XML file template name from the Template to be used drop-down list → click [Save].

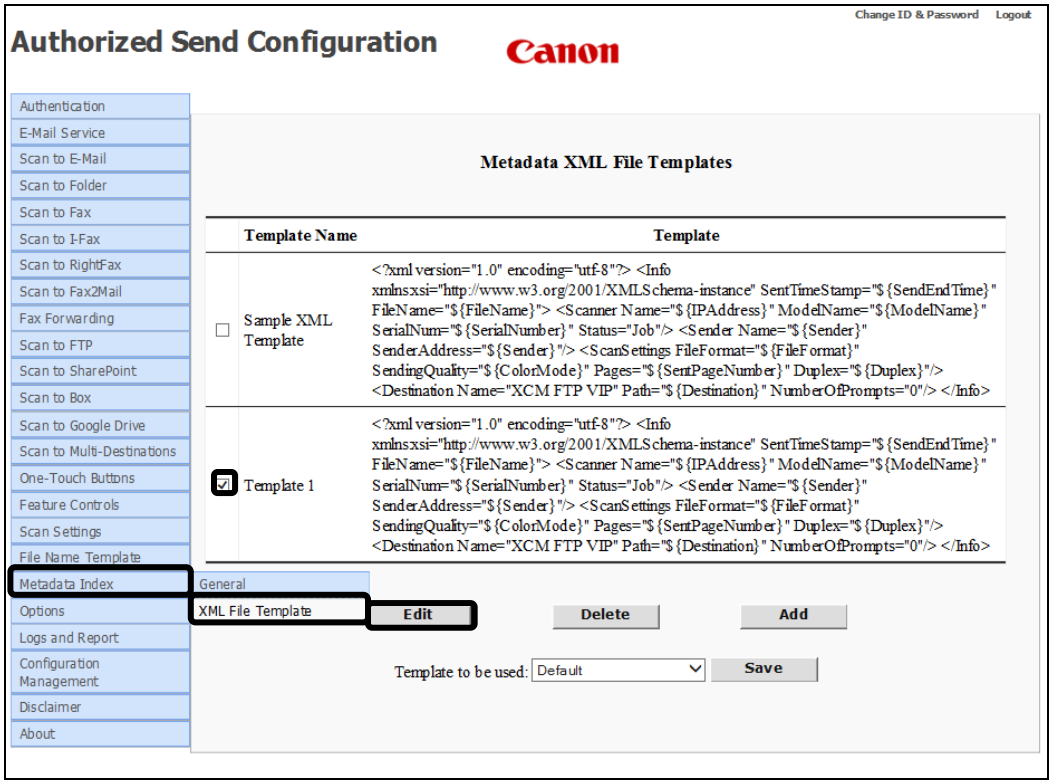


NOTE
The default setting is ‘Default’.

2.23.2 Editing a Metadata XML File Template

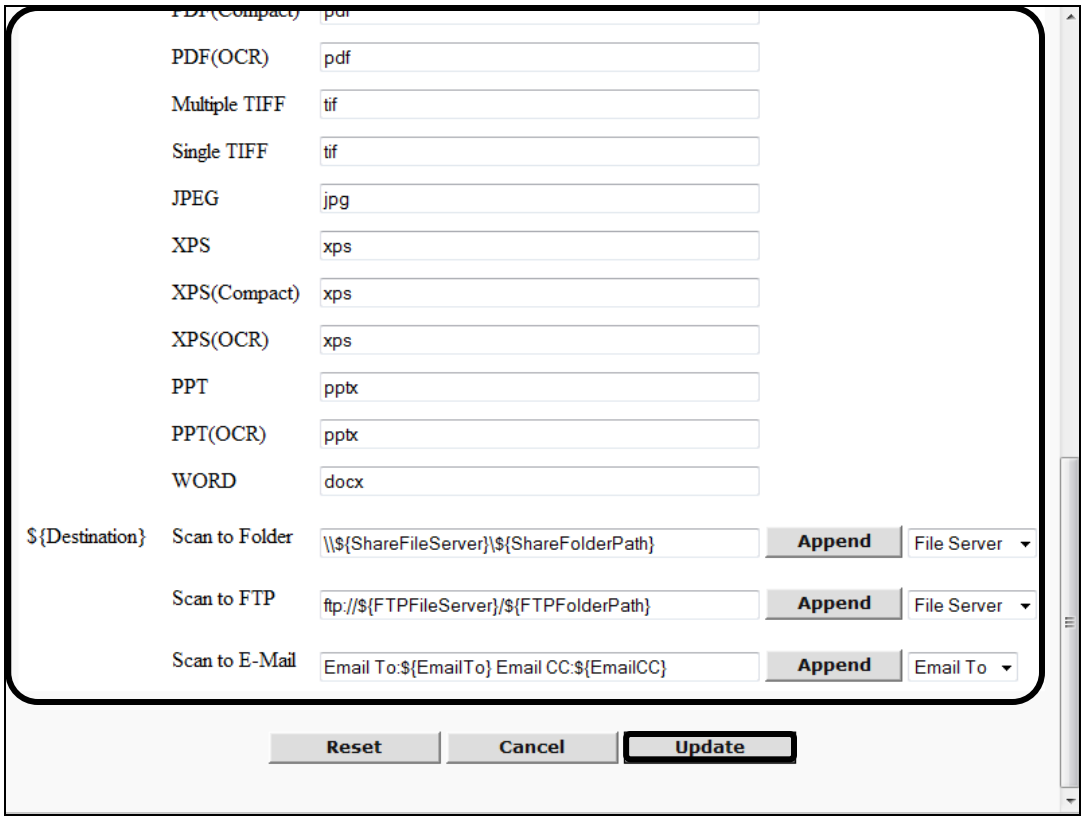
You can edit a previously created metadata XML file template from the Metadata XML File Templates configuration screen.

1. Click [Metadata Index] → [XML File Template] → select the check box next to the template you want to edit → click [Edit].



The Update Metadata XML File Template screen is displayed.

2. Edit the settings for the metadata XML file template, as necessary → click [Update].



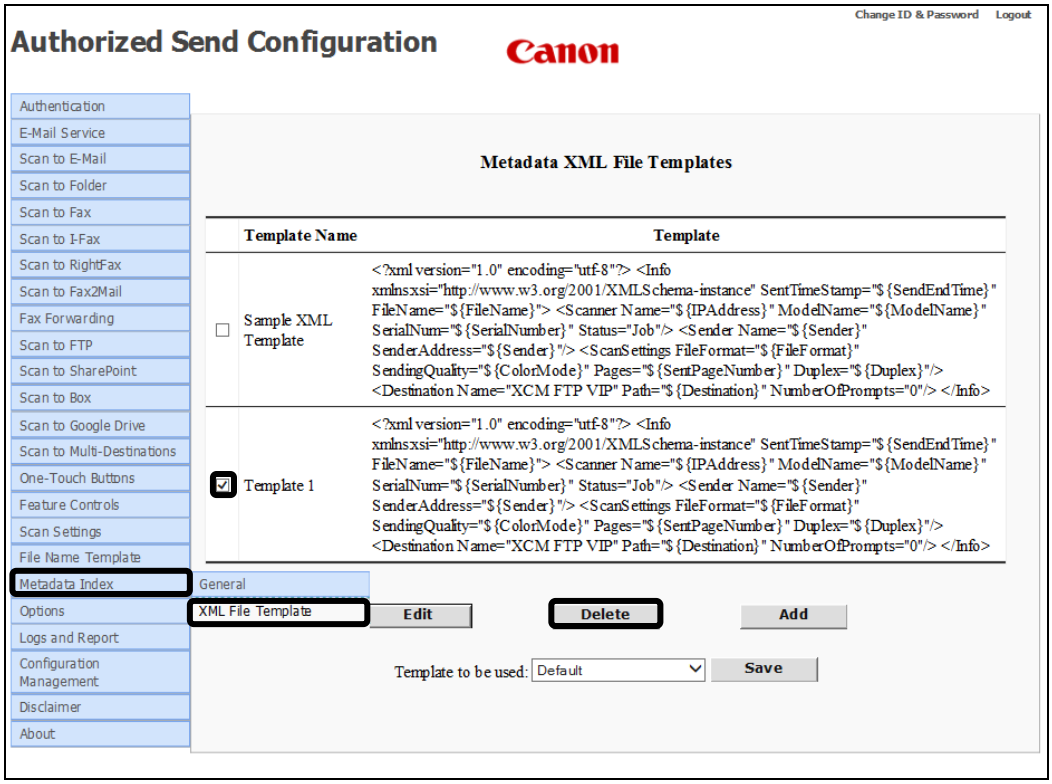
If you make a mistake while editing the settings, click [Reset] to return the settings to their original values.

To cancel editing the metadata XML file template and return to the Metadata XML File Templates configuration screen, click [Cancel].

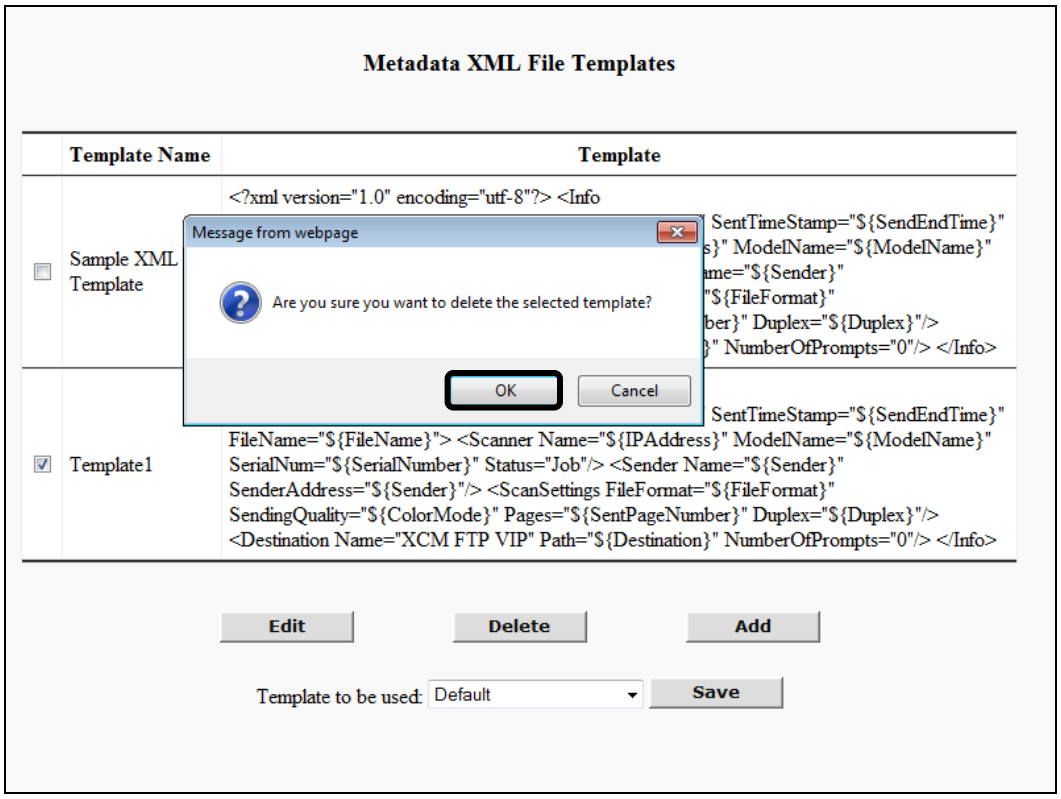
2.23.3 Deleting a Metadata XML File Template

You can delete a previously created metadata XML file template from the Metadata XML File Templates configuration screen.

1. Click [Metadata Index] → [XML File Template] → select the check box next to the template you want to delete → click [Delete].



2. Click [OK] on the confirmation dialog box.



If you do not want to delete the metadata XML file template, click [Cancel].

The metadata XML file template is deleted from the list.

2.24 Configuring the Options Settings

You can configure the Options settings, which includes USB keyboard settings, session and network timeouts, and the application display name.

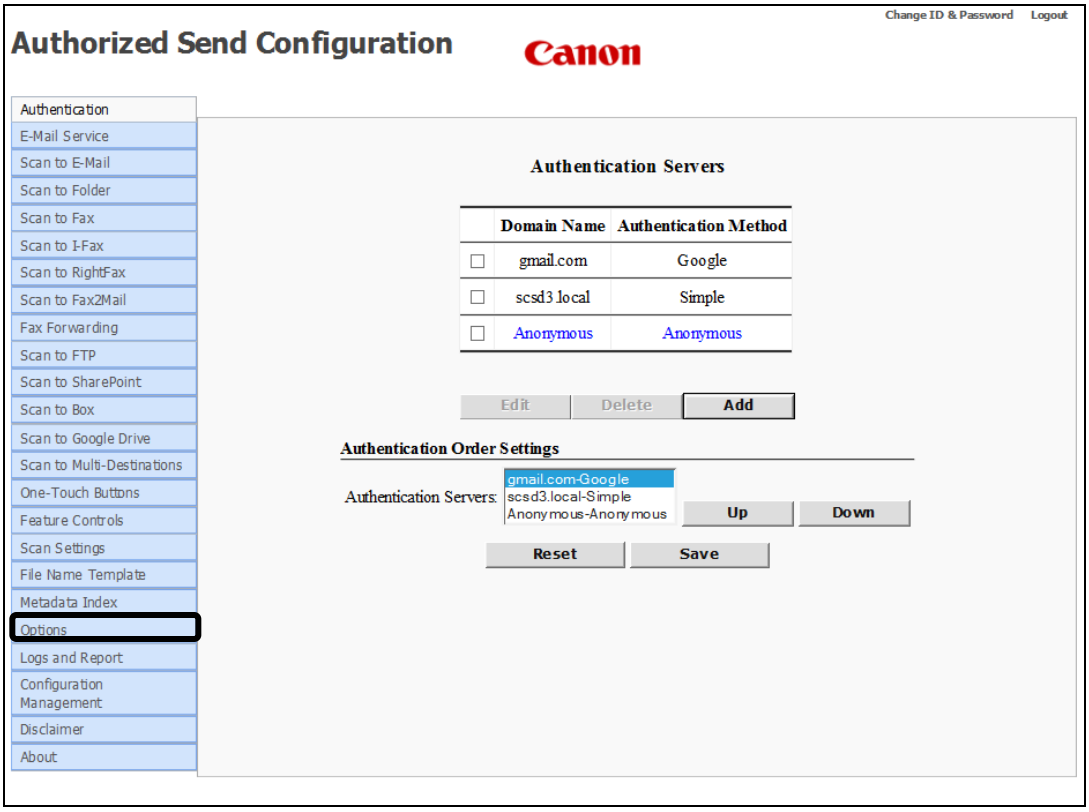
IMPORTANT

- The table below explains the different use-case scenarios if you have a USB keyboard attached to the machine. The use-case scenarios are important for configuring the use of a USB keyboard with Authorized Send for the user.

Scenario	Status of [Enable USB Keyboard input] Check Box	Input Capability (Virtual or USB Keyboard)
The [Use MEAP Driver for USB Input Device] is set to 'Off' in USB Settings in External Interface in Preferences from the Settings/Registration screen on the MEAP device	Not selected.	The virtual and USB keyboards can be used at the same time.
The [Use MEAP Driver for USB Input Device] is set to 'Off' in USB Settings in External Interface in Preferences from the Settings/Registration screen on the MEAP device	Selected.	Only the Cherry G84 keyboard can be used.
The [Use MEAP Driver for USB Input Device] is set to 'On' in USB Settings in External Interface in Preferences from the Settings/Registration screen on the MEAP device	Not selected.	Only the virtual keyboard can be used.
The [Use MEAP Driver for USB Input Device] is set to 'On' in USB Settings in External Interface in Preferences from the Settings/Registration screen on the MEAP device	Selected.	Only the USB keyboard can be used.

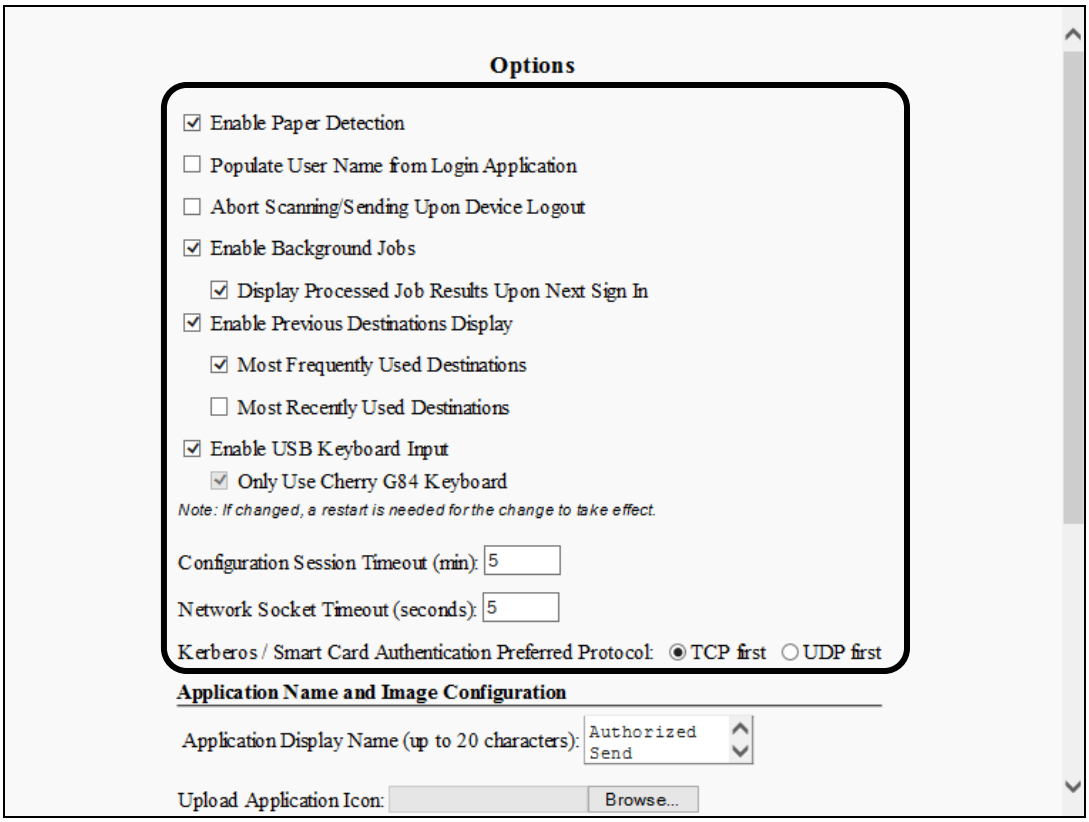
- You can use third-party USB keyboards with Authorized Send. However, only the Cherry G84 keyboard has been tested with this application.

1. Click [Options].



The Options screen is displayed.

2. Configure the settings under Options, as necessary.



Options

Enable Paper Detection:	Select this check box to allow Authorized Send to detect if there is a document on the platen and continue with the send. If this check box is not selected, and Authorized Send does not detect a document in the auto feeder or on the platen, the send job cannot continue. The Send button on the device is deactivated. This is selected by default. NOTE • Paper detection is not available on the following imageRUNNER ADVANCE model series: 2030, C500, C350, C355, C3530, and C356II. • Scanning with the lid open when paper detection is disabled may result in unreliable paper size detection.
Populate User Name from Login Application:	Select this check box to automatically populate the [User Name] text box on the Authorized Send SIGN IN screen on the machine with the user's name from the machine's login Application (if used). If no login application is used, the user must enter their user name manually.

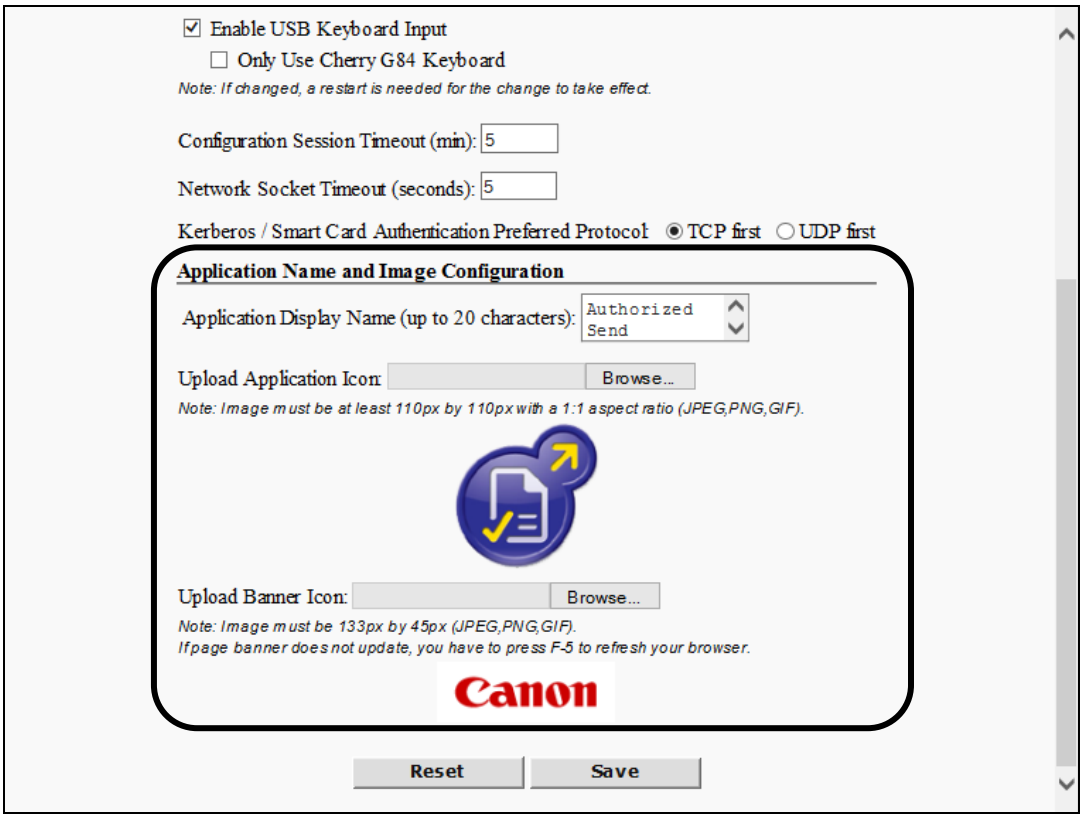
Abort Scanning/ Sending Upon Device Logout:	Select this check box to terminate any scanning or sending when the user logs off the device. If this check box is not selected, and a user starts a scanning job and logs off the device (from a login application), the job completes, and then automatically signs the user out of Authorized Send. By default, this check box is not selected.
Enable Background Jobs:	Select this check box to allow jobs to process in the background, so you don't have to wait for a job to complete sending to start another one. Background jobs can continue to process even after the user logs out.
Display Processed Job Results Upon Next Sign In:	This check box is displayed only if the [Enable Background Jobs] check box is selected. Select this check box to display the results of all background tasks the next time the user logs in. By default, this check box is selected.
Enable Previous Destinations Display:	Select this check box to allow users to select from the five most commonly used or most recently used destinations using a drop-down menu. The maximum number of listed destinations is five (5). If this check box is not selected, users must enter destinations in the text box. The [Enable Previous Destinations Display] check box is not selected by default. NOTE The previous destinations are determined on a per-user basis. A user will not be shown other users' destinations
Most Frequently Used Destinations:	This check box is displayed only if the [Enable Previous Destinations Display] check box is selected. Select this check box to allow users to display a drop-down list of the most frequently used destinations. The [Most Frequently Used Destinations] check box is selected by default.
Most Recently Used Destinations:	This check box is displayed only if the [Enable Previous Destinations Display] check box is selected. Select this check box to allow users to display a drop-down list of the most recently used destinations. The [Most Recently Used Destinations] check box is not selected by default.

Enable USB Keyboard input:	Select this check box to enable your machine to utilize an attached USB keyboard. If this check box is not selected, your machine cannot utilize an attached USB keyboard, and automatically uses the MEAP virtual keyboard instead. If you select the [Enable USB Keyboard input] check box, the [Only Use Cherry G84 Keyboard] check box is selected automatically. The [Enable USB Keyboard input] check box is not selected by default. NOTE • If a USB keyboard is attached to or detached from the machine after Authorized Send has been installed and started, the machine or the Authorized Send application must be restarted. • The machine or the Authorized Send application must be restarted each time you select or clear the [Enable USB Keyboard input] check box for the change to take effect.

Only Use Cherry G84 Keyboard:	This check box is displayed only if the [Enable USB Keyboard input] check box is selected. Select the [Only Use Cherry G84 Keyboard] check box if you want to only use the Cherry G84 keyboard. By default, this check box is selected. NOTE • If you are configuring an imageRUNNER ADVANCE machine, the [Only Use Cherry G84 Keyboard] check box is automatically selected and grayed out when you select the [Enable USB Keyboard input] check box, even after the machine has been restarted. You cannot clear the check mark from the [Only Use Cherry G84 Keyboard] check box. • If a Cherry G84 keyboard and another HID are connected to your machine at the same time, only the Cherry G84 keyboard is functional. • If the [Only Use Cherry G84 Keyboard] check box is not selected and a non-keyboard HID is the only device connected to your machine, you have no way to input text into Authorized Send since the MEAP virtual keyboard is not displayed. • If the [Only Use Cherry G84 Keyboard] check box is not selected and the [Enable USB Keyboard input] check box is selected, any USB keyboard can be used to input text, but only the Cherry G84 keyboard is supported. In this case, to avoid any incompatibility issues between MEAP installed applications and HID card readers, or other HIDs, it is recommended that you select the [Only Use Cherry G84 Keyboard] check box. • The machine or the Authorized Send application must be restarted each time you select or clear the [Only Use Cherry G84 Keyboard] check box for the change to take effect.
Configuration Session Timeout (min):	Enter the time in minutes until the Authorized Send Configuration servlet session times out. You can set the timeout period between ‘1’ and ‘60’ minutes. The default setting is ‘5’ minutes.

Network Socket Timeout (seconds):	Enter the time in seconds until the connection to the authentication server and address book server times out. You can set the timeout period between ‘1’ and ‘30’ seconds. The default setting is ‘5’ seconds.
Kerberos/Smart Card Authentication Preferred Protocol:	Select the [TCP first] radio button to have Kerberos attempt authentication over TCP first, then use UDP only if TCP fails. Select the [UDP first] radio button to have Kerberos attempt authentication over UDP first, then use TCP only if UDP fails. [TCP first] is selected by default.

3. Configure the settings under Application Name and Image Configuration, as necessary.



Application Name and Image Configuration

Application Display Name (up to 20 characters):	Enter the application's display name. You can enter a maximum of 20 characters. Valid characters are the printable ASCII characters and the carriage return. The default setting is 'Authorized Send'. If the application's display name is changed, you do not have to restart the machine for the change to take effect. If you want to return to the default setting, leave this text box blank.

Upload Application Icon:	Enter the name of a graphic file to use as the new Authorized Send icon on the machine's main menu. The graphic file must be 110 pixels x 110 pixels, in a 1-to-1 aspect ratio, and be in the JPEG, GIF, or PNG format. Click in the text box or click the [Browse] button to select the graphic file from your local machine.
Upload Banner Icon:	Enter the name of a graphic file to use as the new banner graphic at the top of the configuration servlet's screen. The graphic must be 133 pixels wide x 45 pixels high, and be in the JPEG, GIF, or PNG format. Click in the text box or click the [Browse] button to select the graphic file from your local machine.

4. Click [Save].

NOTE

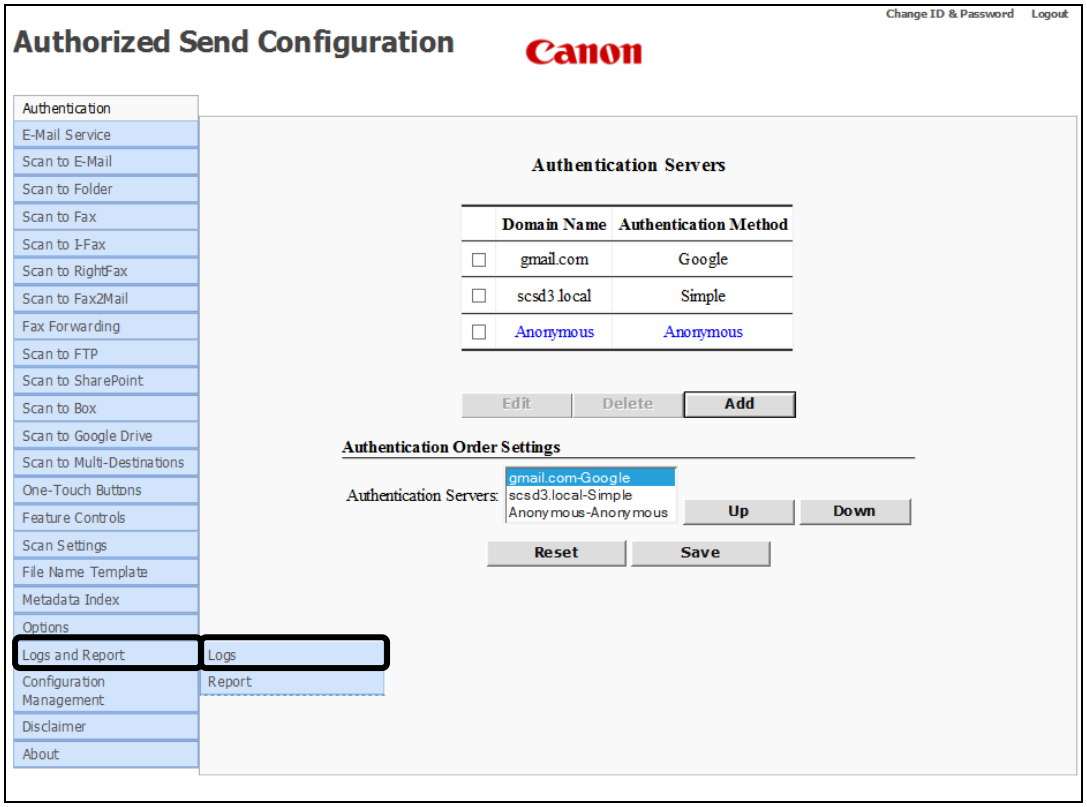
If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

2.25 Configuring the Logs and Reports Settings

2.25.1 Configuring the Logging Settings

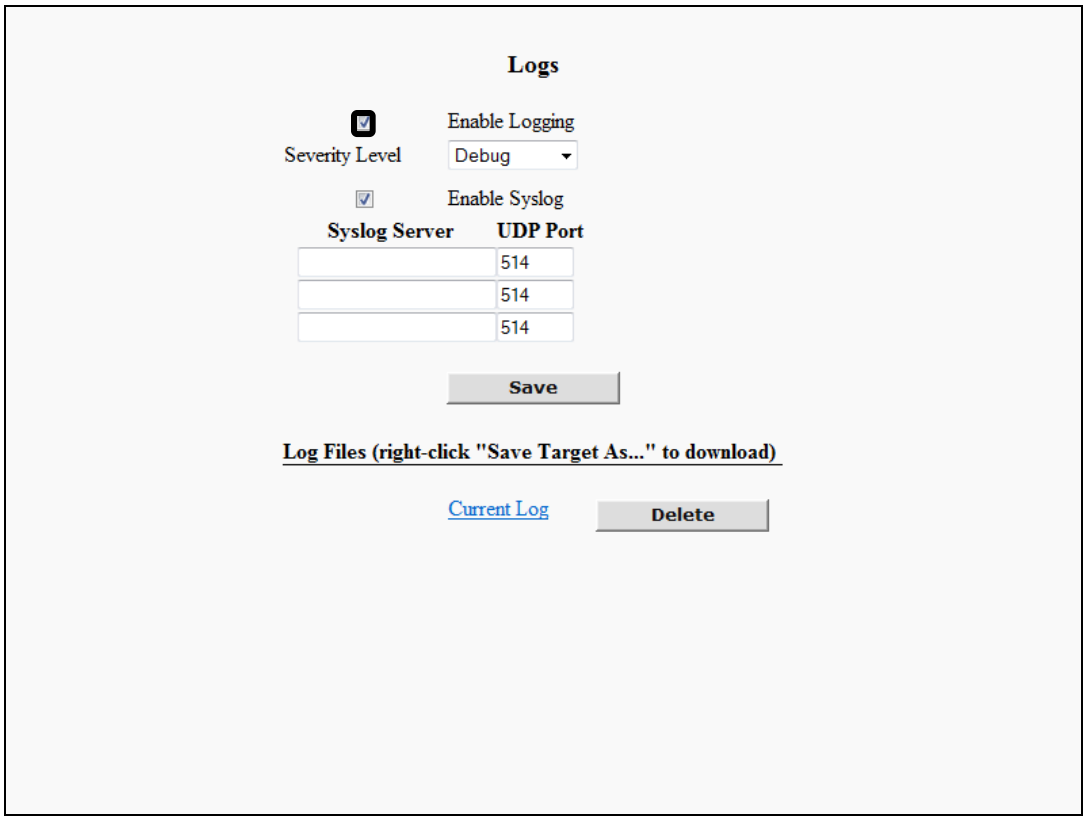
You can configure the Logs function, which includes enabling/disabling log recording, configuring remote syslog servers, and downloading and viewing the logs.

1. Click [Logs and Reports] ➞ [Logs].



The Logs screen is displayed.

2. Click the [Enable Logging] check box, if necessary.



When the [Enable Logging] check box is selected, Authorized Send logs debug and error messages up to a maximum file size of 1 MB (1,024 KB).

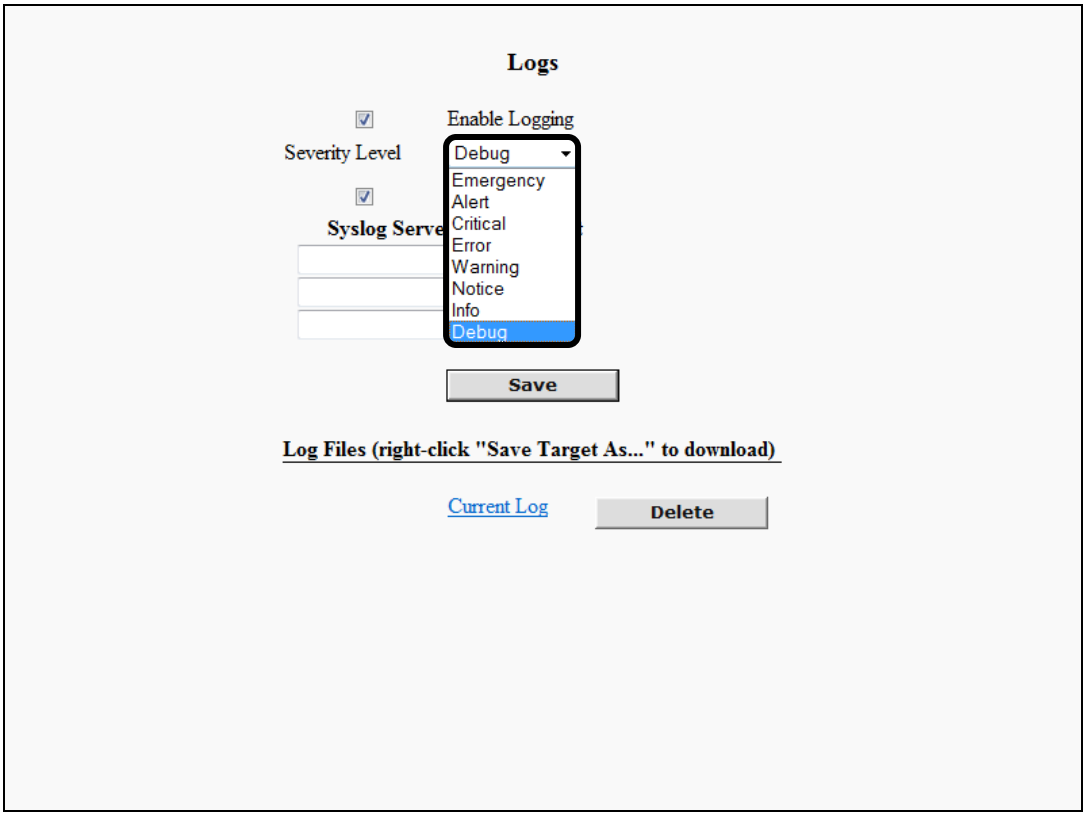
There can be two log files, each with a maximum file size of 512 KB.

Current Log: Contains the most recent logging information. Once the Current Log reaches the maximum file size, it replaces the History Log (if it exists), or it creates a new History Log. The Current Log is then cleared to 0 KB.

History Log: Contains the contents of the last Current Log that reached the maximum file size. The History Log does not exist until the Current Log reaches its maximum size and resets itself.

The [Enable Logging] check box is selected by default.

3. Select the severity level from the Severity Level drop-down list.



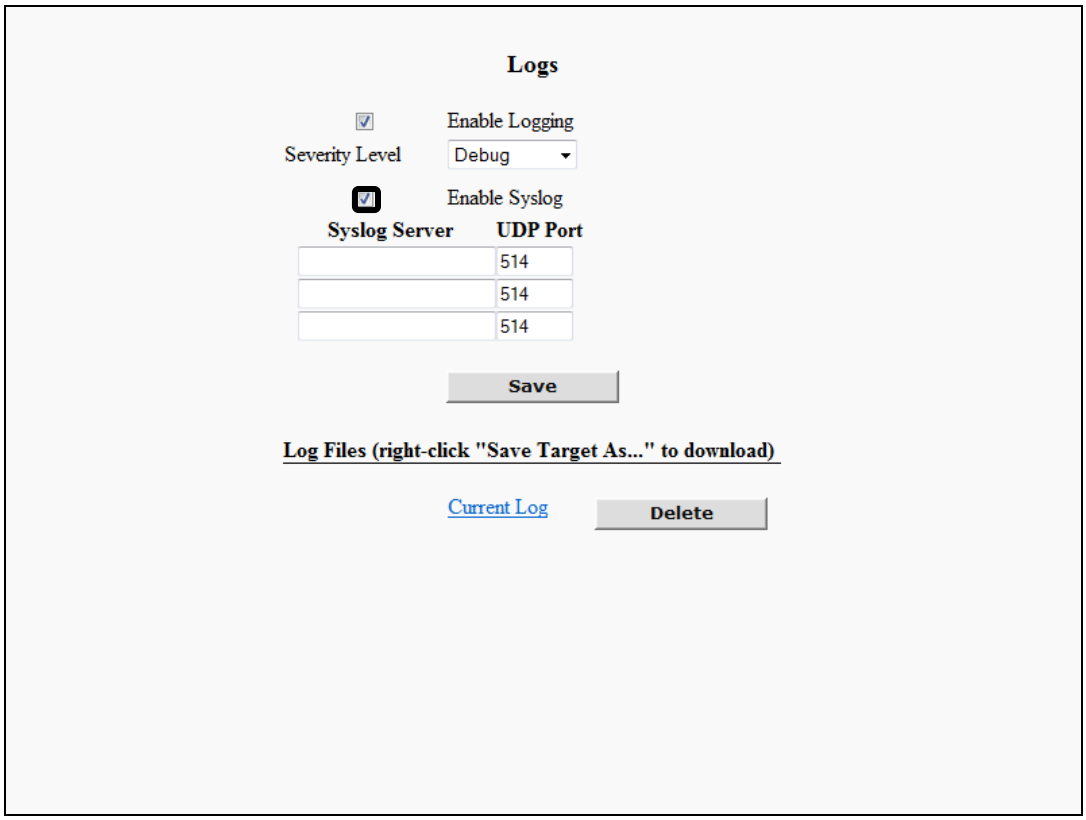
The table below shows the supported levels of increasing severity and their respective numeric codes.

Severity Level	Numeric Code
Emergency	0
Alert	1
Critical	2
Error	3
Warning	4
Notice	5
Info	6
Debug	7

When you select a severity level from the drop-down list, that severity and all severities with a lower numeric value are logged.

The default setting is ‘Debug’. If [Debug] is selected, all severities are logged.

4. Select the [Enable Syslog] check box to send syslog messages to all the configured syslog servers, if necessary.



If you select the [Enable Syslog] check box, at least one syslog server must be configured.

Authorized Send supports only the user-level messages (Numeric Code = 1) and security/authorization messages (Numeric Code = 4). Facilities of the Syslog RFC3164 Protocol.

User-level messages are logged locally within the Authorized Send application. Security/authorization messages are also logged locally, as well as sent to all configured remote syslog servers.

Messages are logged in the following format:
<PRI#> HEADER MSG

PRI = Priority number, depending on the Facility and Severity.
HEADER = Mmm dd hh:mm:ss HostName/IP
MSG = Tag (the application) followed by the message.

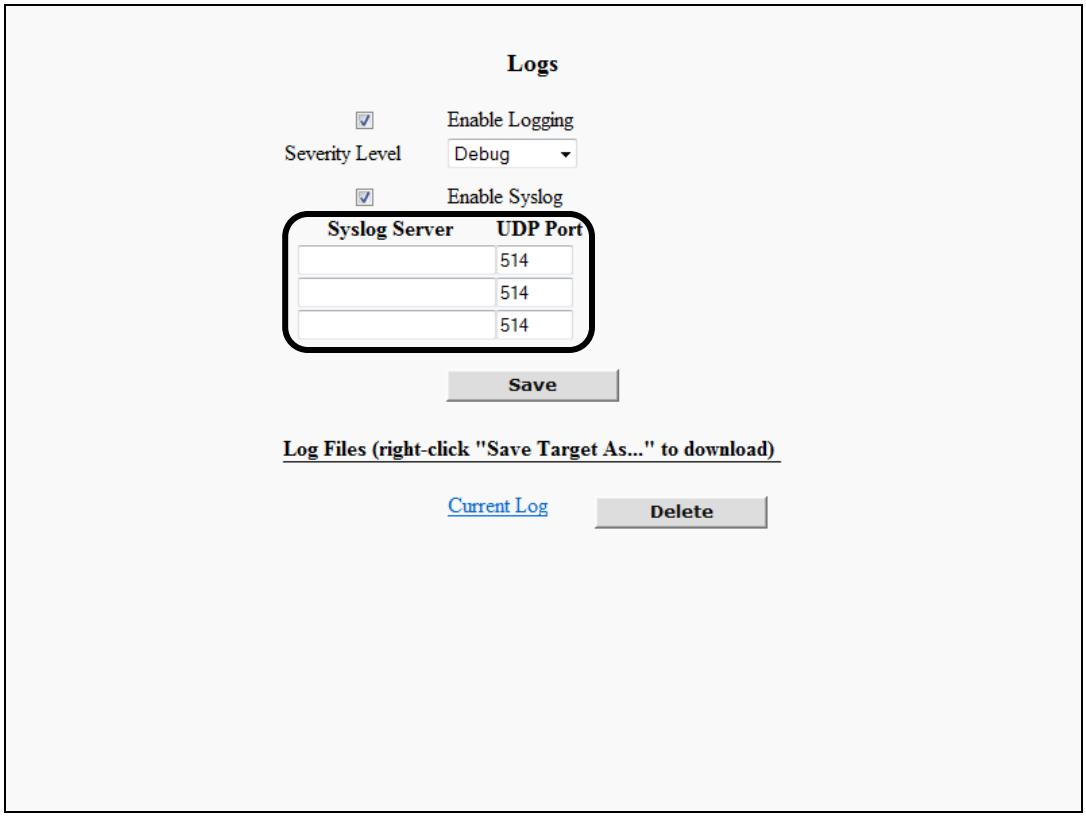
For example: <34>Feb 23 22:14:15 iR-HostName AS sign-in failed.

The [Enable Syslog] check box is not selected by default.

NOTE

The messages sent to a remote syslog server cannot exceed 1,024 bytes. Any messages that exceed 1,024 bytes are split and sent as multiple messages.

5. Enter a syslog server's IP address under <Syslog Server> in the table → enter the corresponding UDP port number for the syslog server under <UDP Port> in the table.



You can configure up to three syslog servers. You can enter a maximum of five numbers for the UDP port.

6. Click [Save].

7. To view the log file, click [Current Log] or [History Log] (if available).

   A browser window opens to display a snapshot of the contents of the log file.

NOTE

- The log file contents displayed are not live. To view the latest contents of the log file, you must close the log window → refresh the Authorized Send Configuration servlet → click [Current Log] to open a new browser window.
- [History Log] only appears after the current log reaches a maximum size of 512 KB. Once the current log reaches the maximum size, it replaces the history log (if it exists), or creates a new history log.

8. To download the log file, right-click [Current Log] or [History Log] ➞ select [Save Target As] ➞ select a location to save the file.

9. To delete the log file, click [Delete].

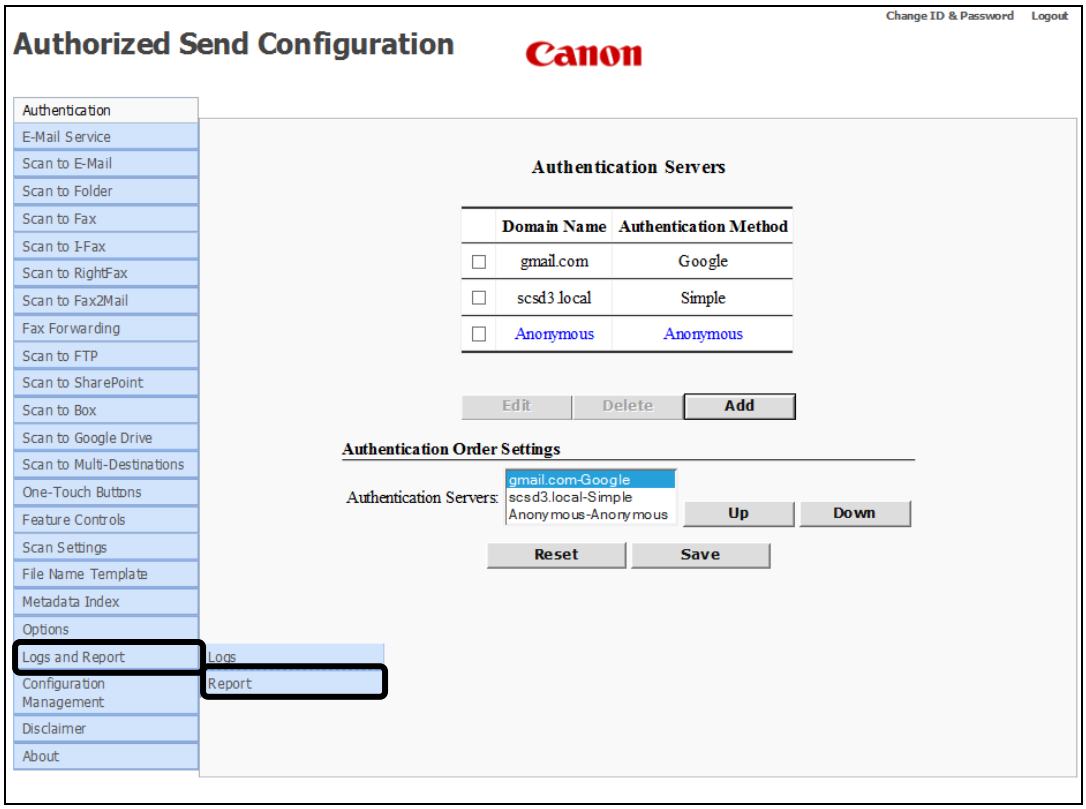
   If you want to disable the Logs function, click the [Enable Logging] check box to clear the check mark ➞ click [Save].

2.25.2 Configuring the Reporting Settings

You can configure the Reports function, which includes sending reports to specified email accounts, and automatically uploading reports to a folder on a file server.

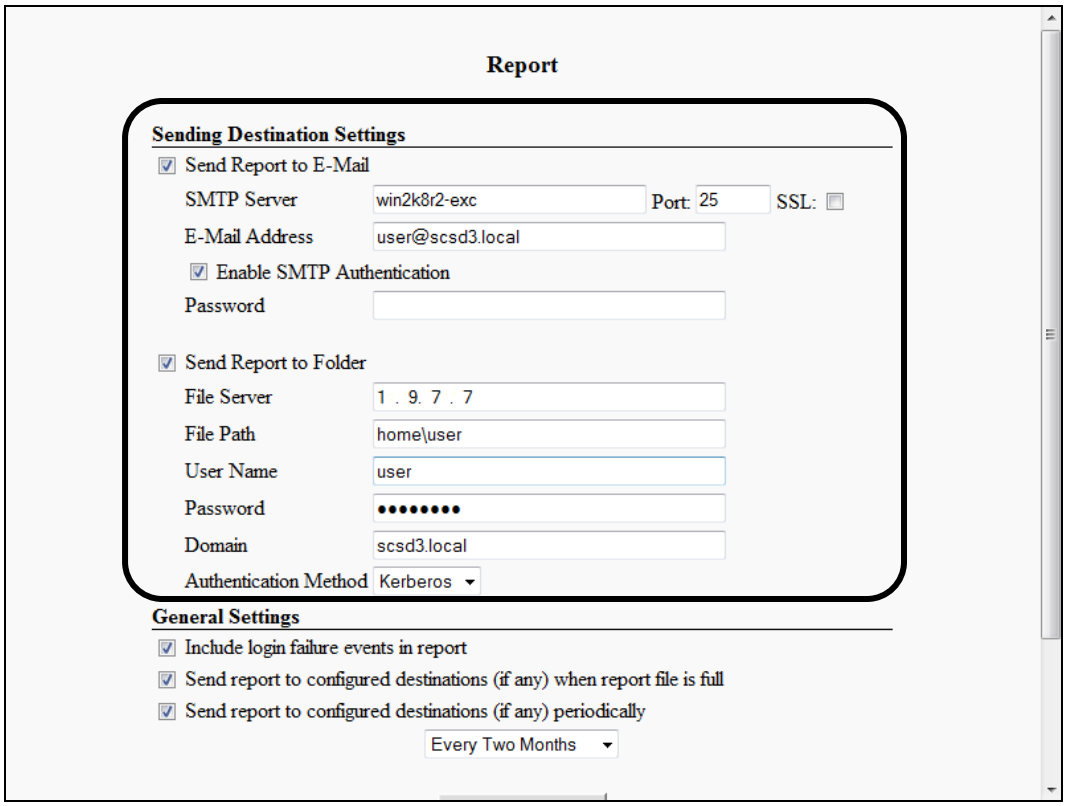
Except where noted, after a report is delivered, the existing report is deleted and a new report is started.

1. Click [Logs and Reports] ➞ [Report].



The Logs screen is displayed.

2. Configure the Sending Destination Settings



Sending Destination Settings

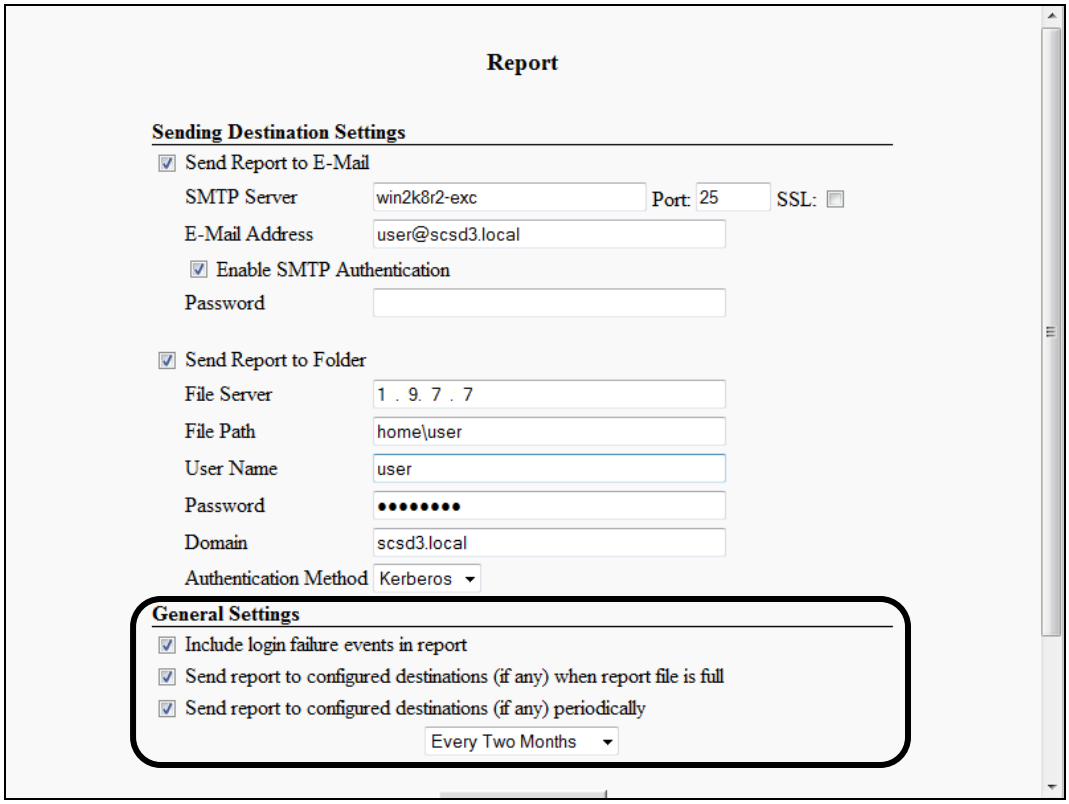
Send Report to E-Mail:	Select this check box to have reports sent to an e-mail address.
SMTP Server:	Enter the IP address or server name of the SMTP server.
Port:	Enter the connecting port number of the SMTP server. You can enter a maximum of five numbers. The default port number is ‘25’
SSL:	Select this check box if you want the SMTP server to use SSL.
E-Mail Address:	Enter the email address to where you want to send the report.
Enable SMTP Authentication:	Select this check box if you want to use SMTP authentication.

Password:	This text box only appears if you check the [Enable SMTP Authentication] check box. Enter the password for the e-mail account in the [E-Mail Address] text box.
Send Report to Folder:	Select this check box to have reports copied to a file folder on a server.
File Server:	Enter the IP address or the server name of the file server.
File Path:	Enter the full pathname of the directory into which the report will be copied.
User Name:	Enter the user name for the account on the file server.
Password:	Enter the user name's password for the account on the file server.
Domain:	Enter the domain name of the file server.
Authentication Method:	Select the authentication method from the drop-down list: [Kerberos] or [NTLM].

NOTE

If the user performs a Scan to E-Mail job and has enabled the [PDF Single] and Sign/Encrypt options, the job is reported as a single PDF instead of multiple individual PDF pages.

3. Configure the General Settings

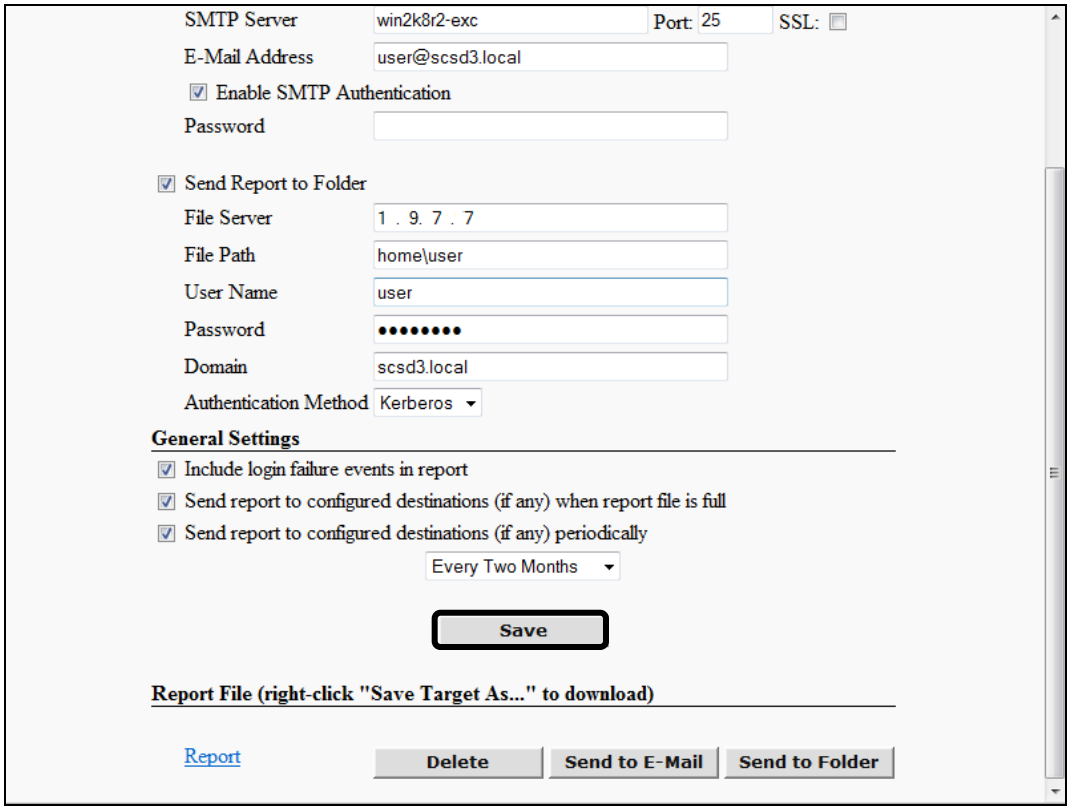


General Settings

Include login failure events in report:	Select this check box to include all instances of failed logins in the report file.
Send report to configured destinations (if any) when report file is full:	Select this check box to automatically send the report file when it has reached it maximum capacity (2 MB). If this check box is not selected and the report file becomes full, the older data is deleted and a new report file is started.

Send report to configured destinations (if any) periodically:	Select this check box to automatically send the report file at a pre-determined interval.
Periodic interval drop-down list:	This list only appears if you select the [Send report to configured destinations (if any) periodically] check box. Select the interval based on the last time the machine sent a report: • Every Month • Every Two Months • Every Three Months • Every Six Months

4. Click [Save].



5. To download the report file, right-click [Report] → select [Save Target As] → select a location to save the file. Click on[Report] to bring up a separate browser window with a copy of the current report file.

6. To delete the report file, click [Delete]. After deleting the report, the [Report] link becomes inactive until more report data is generated and a new report file is created.

7. To immediately send a copy of the report file to the configured email address, click [Send to E-Mail]. Existing report data is not deleted and a new report is not started.

8. To immediately send a copy of the report file to the configured folder, click [Send to Folder]. Existing report data is not deleted and a new report is not started.

If you want to disable the Report function, click the [Send Report to E-Mail] and [Send Report to Folder] check boxes to clear the check marks → click [Save].

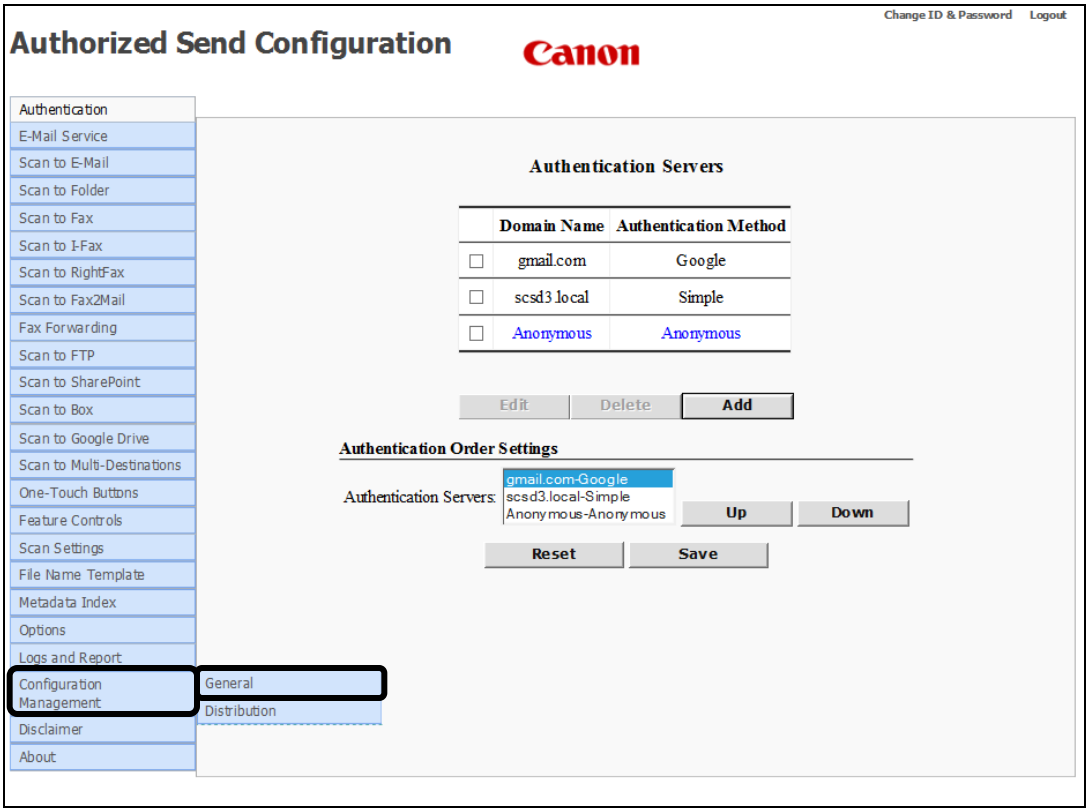
2.26 Configuring the Configuration Management Settings

You can configure the Configuration Distribution function, which distributes the saved Authorized Send configuration settings to target devices.

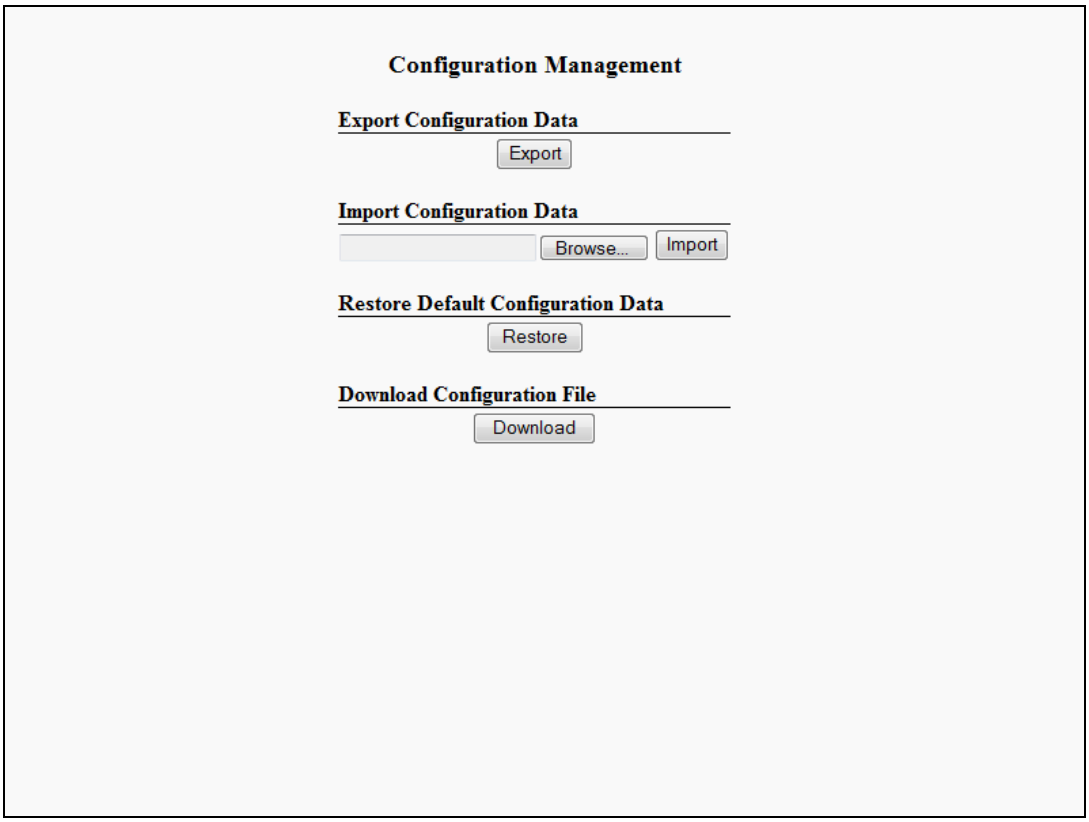
IMPORTANT

It is recommended to always push the configuration settings from an imageRUNNER ADVANCE machine.

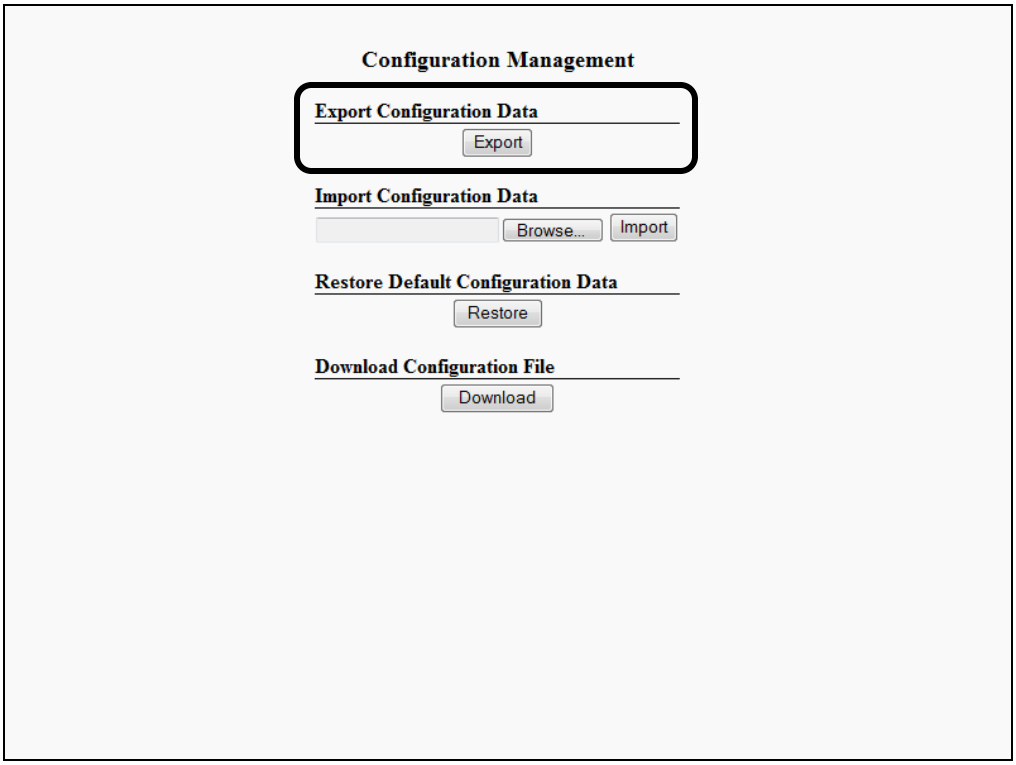
1. To manage the configuration of the device, click [Configuration Management] → [General].



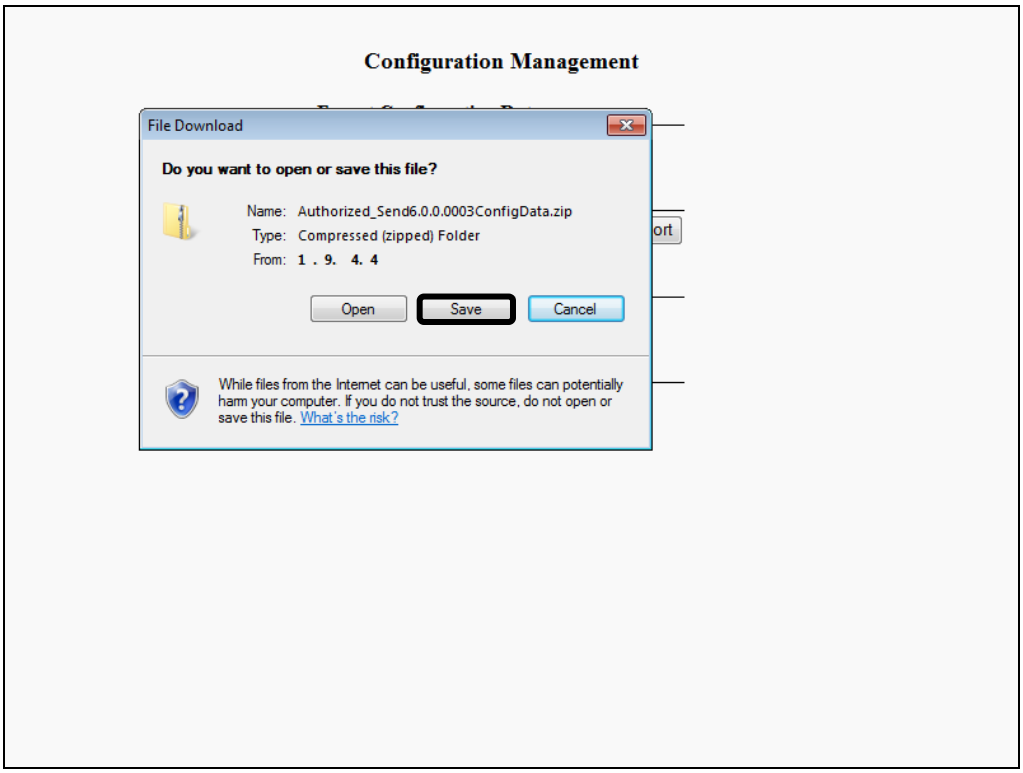
The Configuration Management screen appears.



1.1 If you have a common configuration to be used by multiple machines, you can configure one machine and export the configuration to be used by all others. Use the Export Configuration Data function.



To save the current Authorized Send configuration, click [Export] to export the current Authorized Send configuration into a file → click [Save].



Click [Open] to open the file.

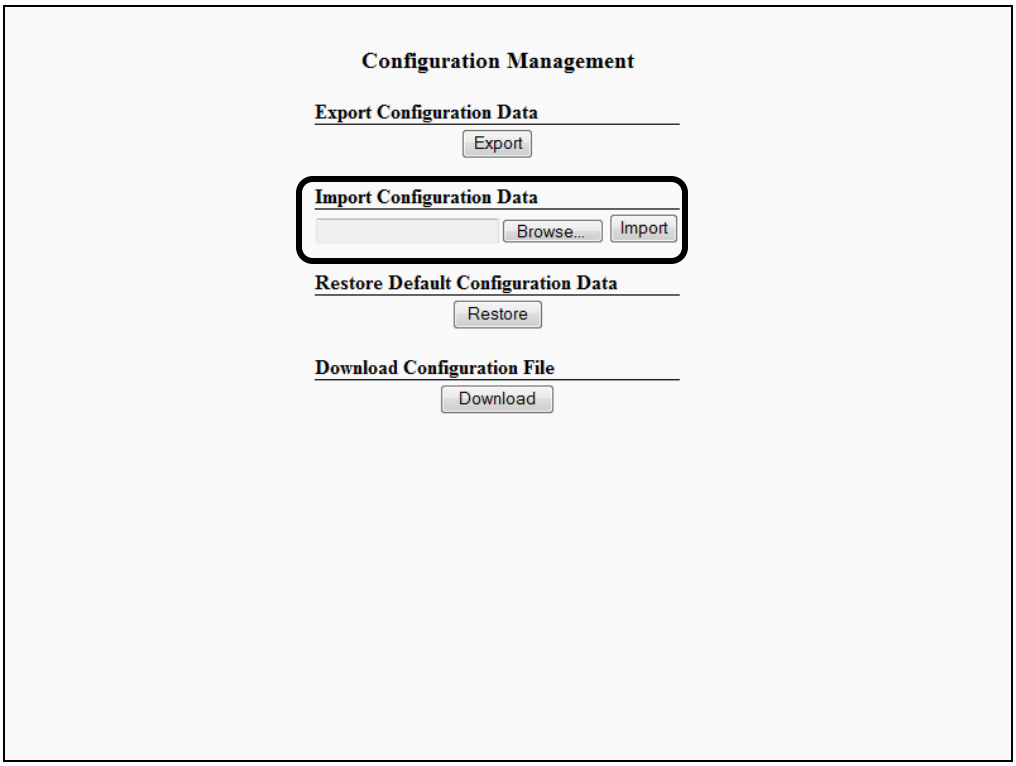
Click [Cancel] to stop the download operation and return to the Configuration Management screen.

The file is in .zip format, and contains two text files:

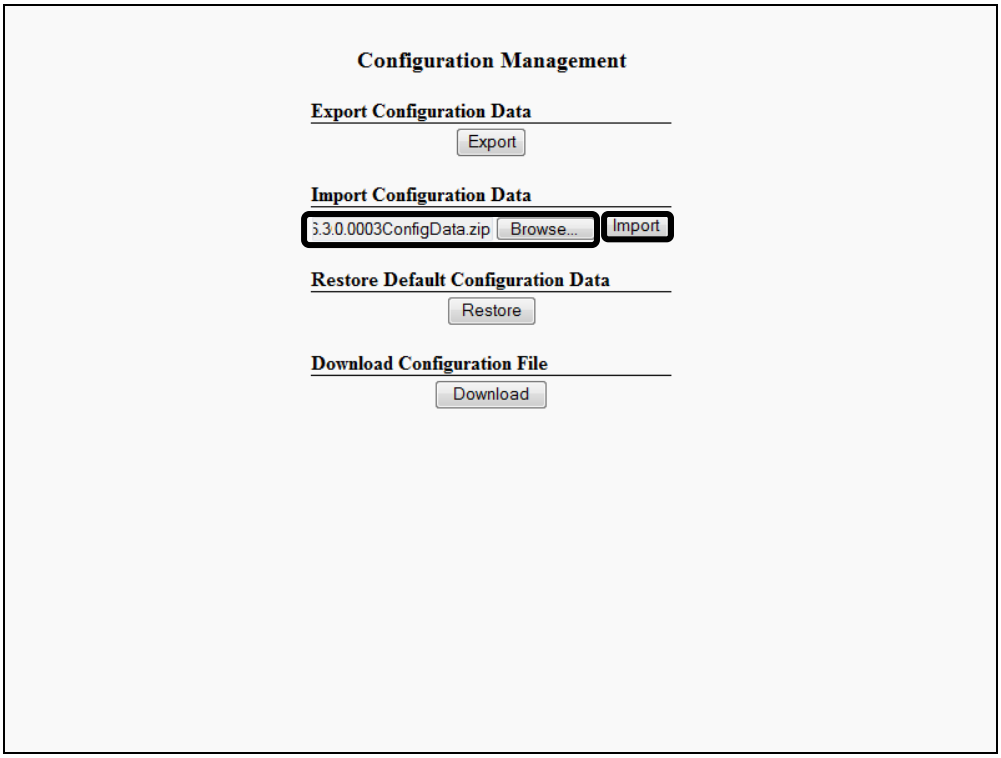
- configData.txt: contains the configuration data
- dataInfo.txt: contains information about the local machine

The configuration archive can then be imported to other systems.

1.2 If you want to import a configuration file that has already been created, use the Import Configuration Data function.



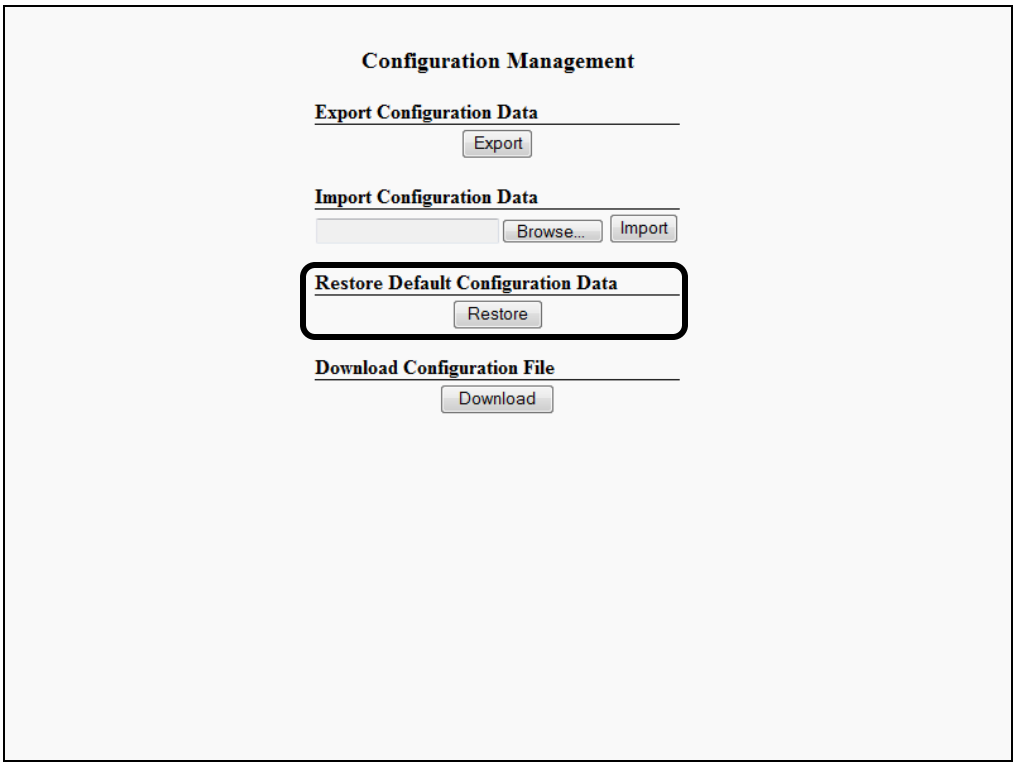
1.3 Click [Browse] to select the file to import → click [Import]



NOTE

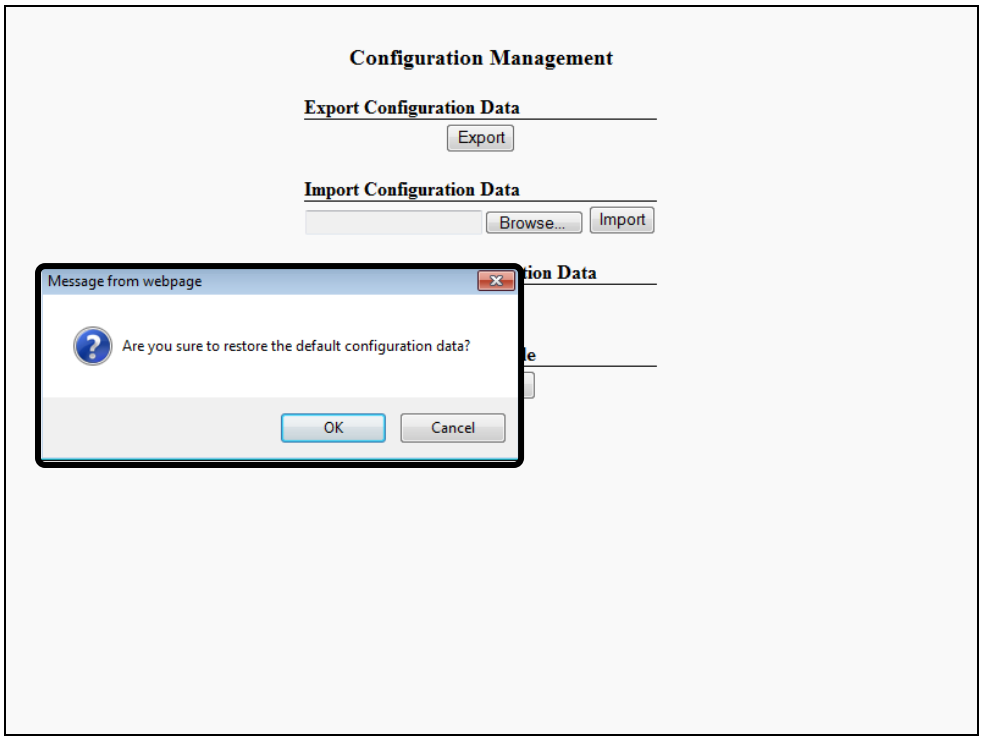
Imported settings take effect immediately after the import operation completes. However, the machine will need to be rebooted if the [Enable USB Keyboard Input] check box in the Options configuration screen is selected.

1.4 If you want to restore Authorized Send to the default configuration, click [Restore].

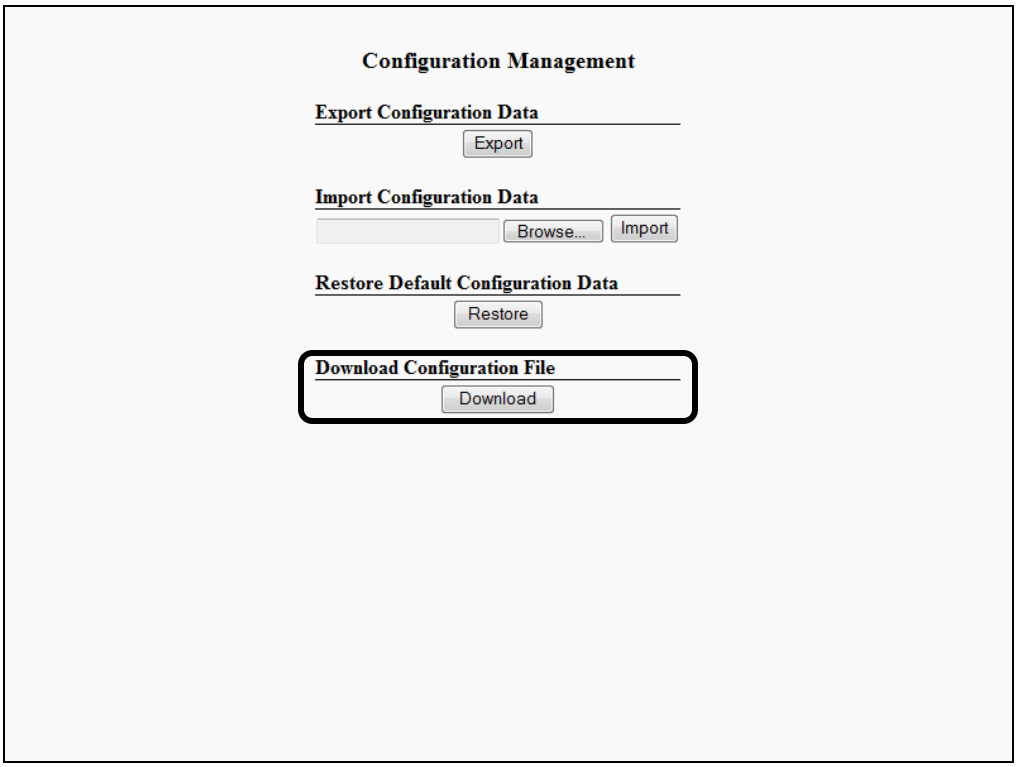


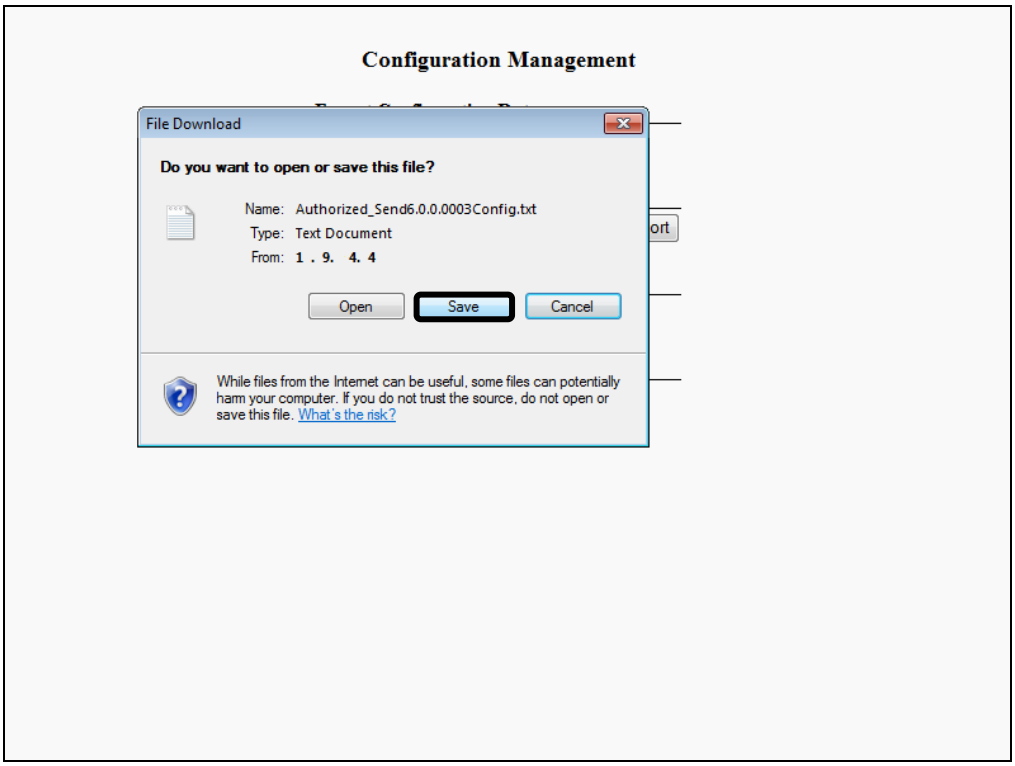
NOTE

A confirmation dialog box appears after you click [Restore]. Click [OK] to restore the settings or click [Cancel] to cancel the restore and return to the Configuration Management screen.

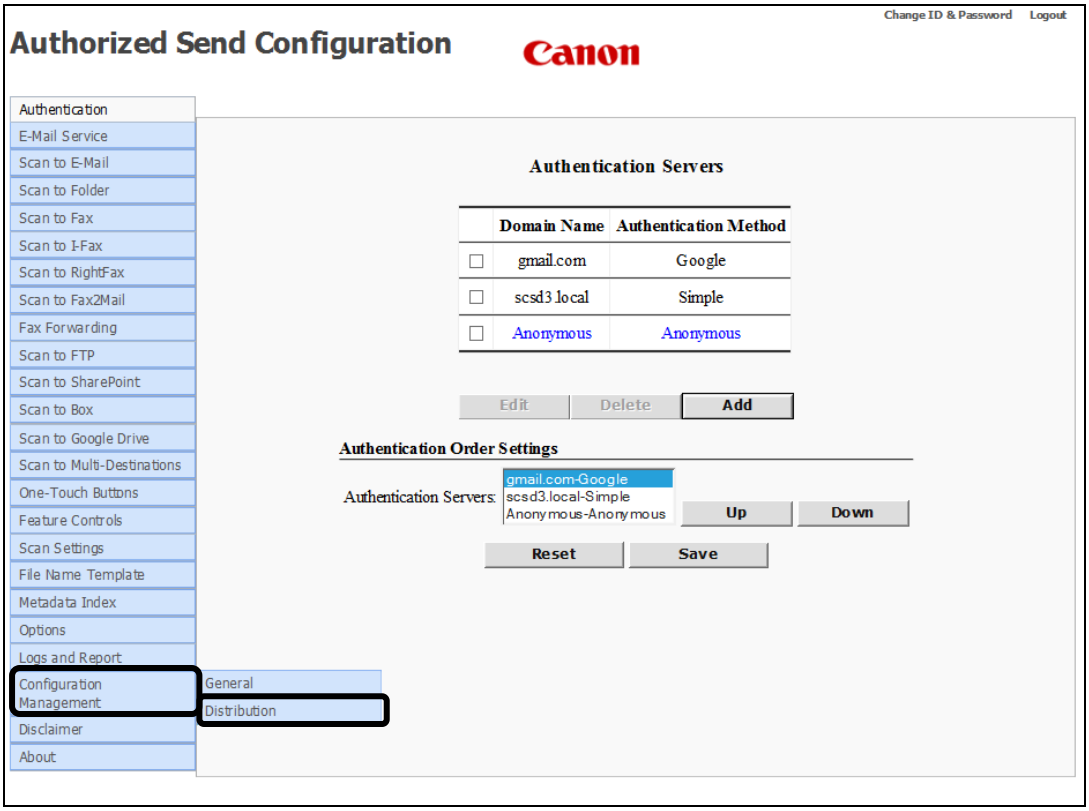


1.5 If you want to create a text file which lists the Authorized Send configuration parameters and their current values, click [Download]





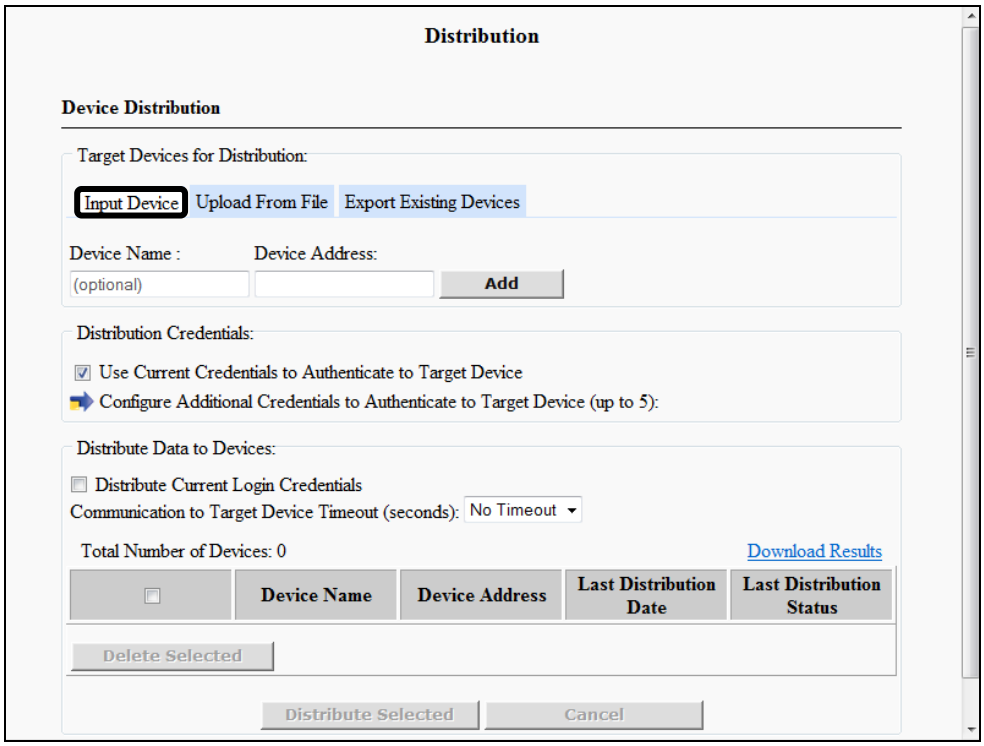
2. To configure the distribution, click [Configuration Management] → [Distribution].



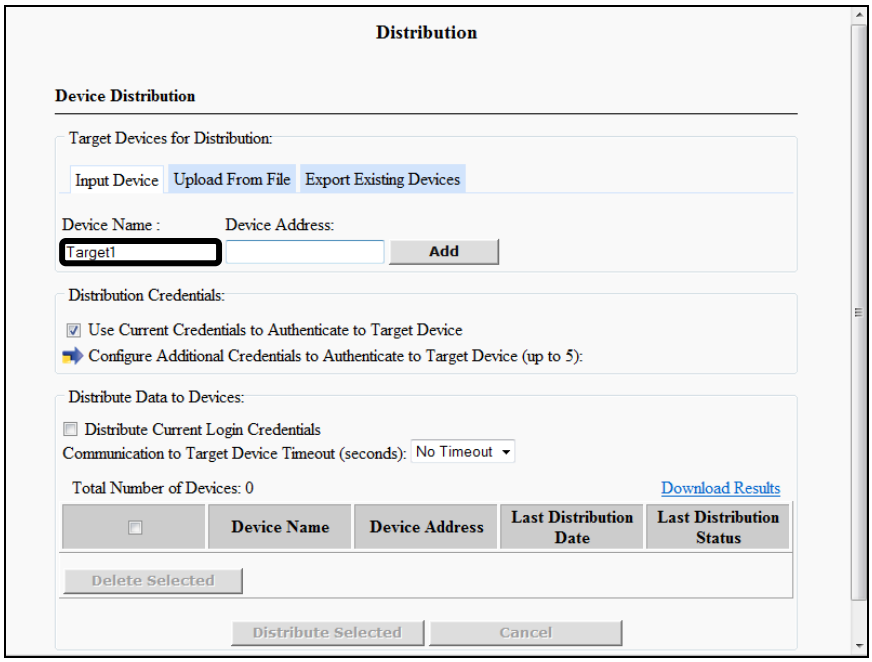
The Configuration Management Distribution screen is displayed.

3. Input a target device individually or by upload it from a file. You can also export saved devices to a text file.

   3.1 To input a target device individually, click the [Input Device] tab.

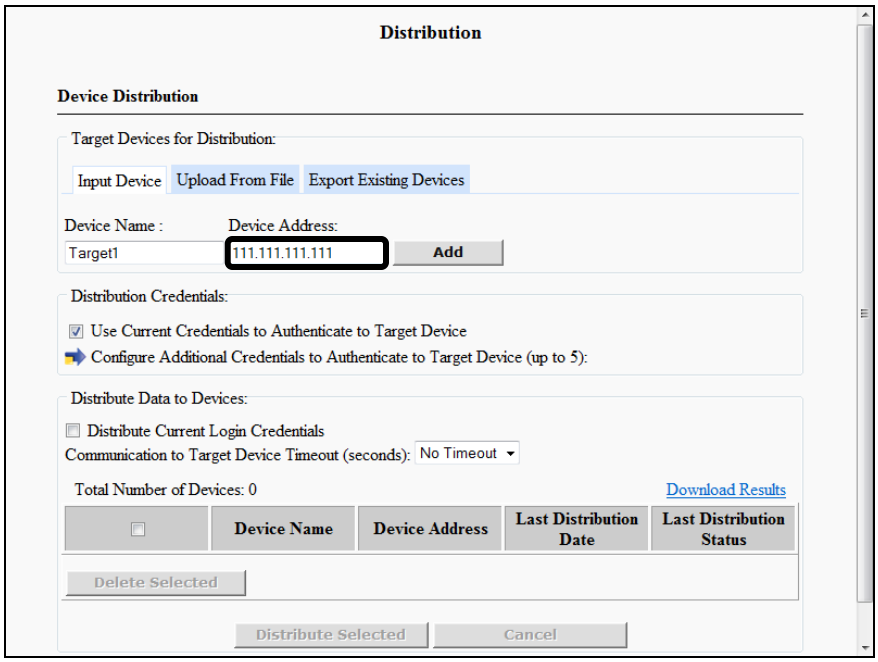


3.1.1 Enter a device name in the [Device Name] text box.



You can enter a maximum of 32 alphanumeric characters for the device name. Entering a device name is used as a convenience to associate it with the device address; however, the device name is optional, and is not used for configuration distribution.

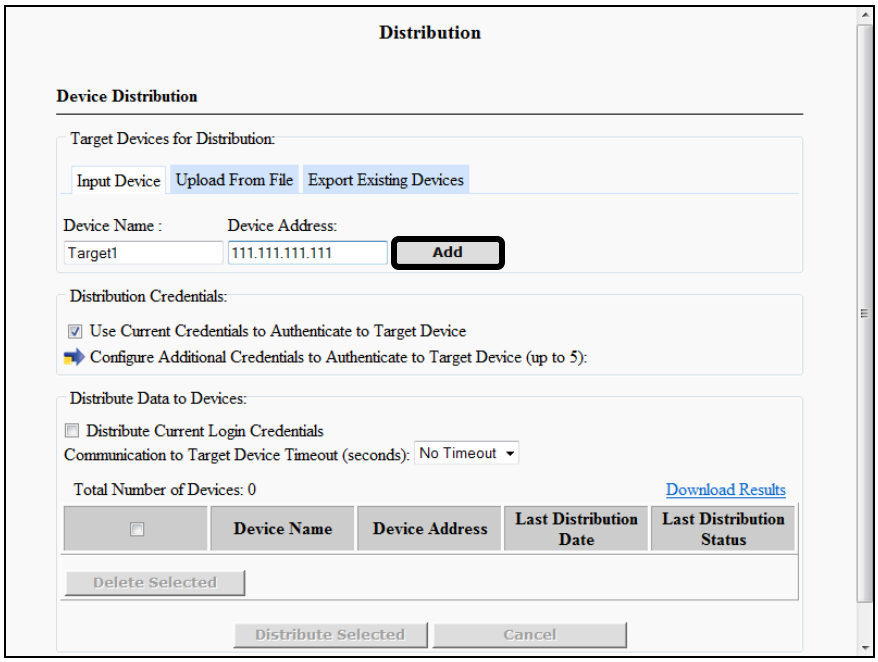
3.1.2 Enter the device address in the [Device Address] text box.



You can enter an unlimited number of any characters in the format of an IP address, or the fully qualified domain name of the device.

The default device address is a blank field.

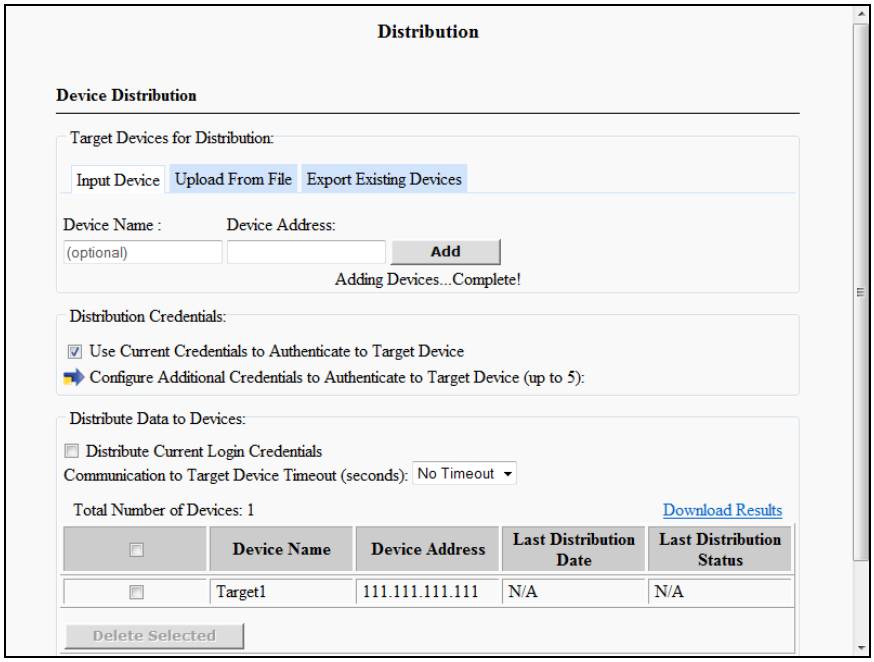
3.1.3 Click [Add] to start the validation process.



Validation is performed to make sure that:

- The device name, if used, does not exceed the maximum number of characters.
- The IP address format is correct, or the FQDN can be resolved.
- The IP address or the FQDN does not already exist.

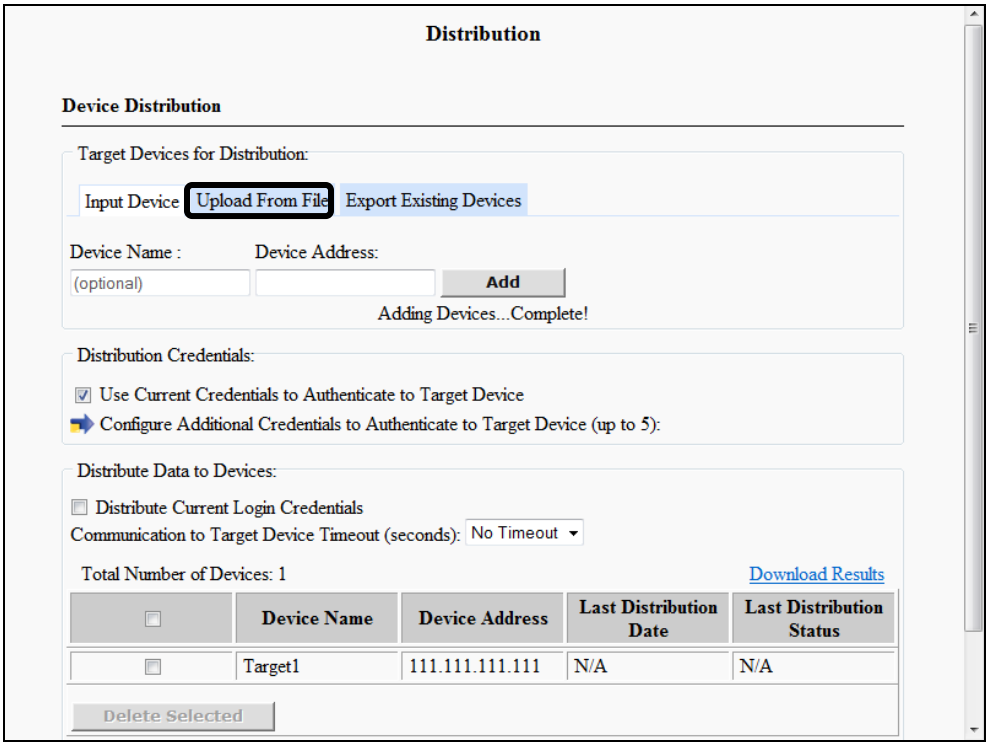
If the validation process is successful, the added device appears in the Distribute Data to Devices table. If it fails, an error message is displayed in red.



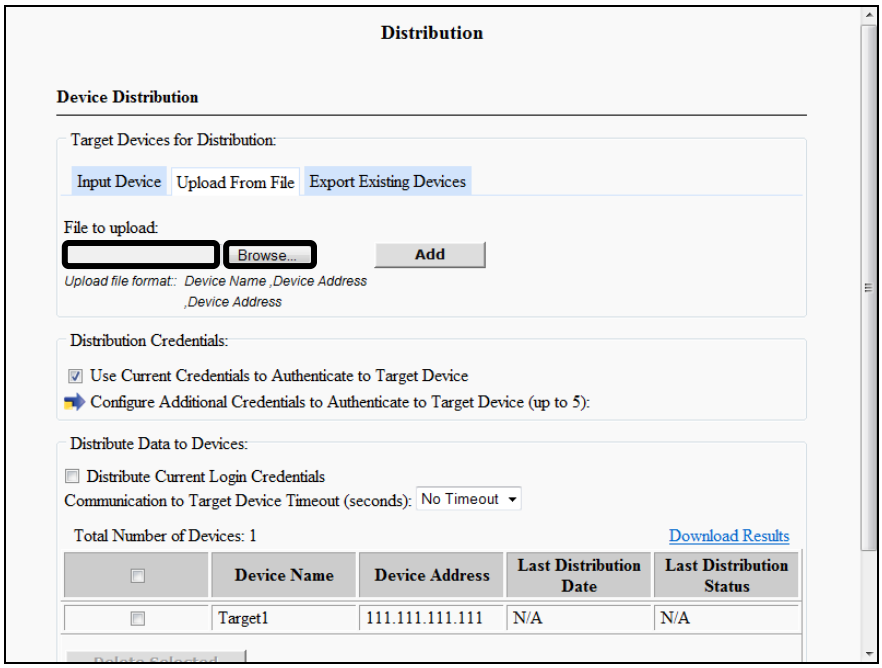
NOTE

- <Total Number of Devices:> displays the number of target devices that are in the Distribute Data to Devices table. This number varies, as target devices are added to, or deleted from, the Distribute Data to Devices table.
- If the maximum number of target devices (50) is reached, the number appears in red.
- [Add] is disabled when the maximum number of target devices (50) is reached.
- The Distribute Data to Devices table is sorted alphabetically under <Device Name>.

3.2 To upload a target device from a file, click the [Upload From File] tab.



3.2.1 Enter a file in the [File to upload] text box, or click [Browse] under <File to upload>.

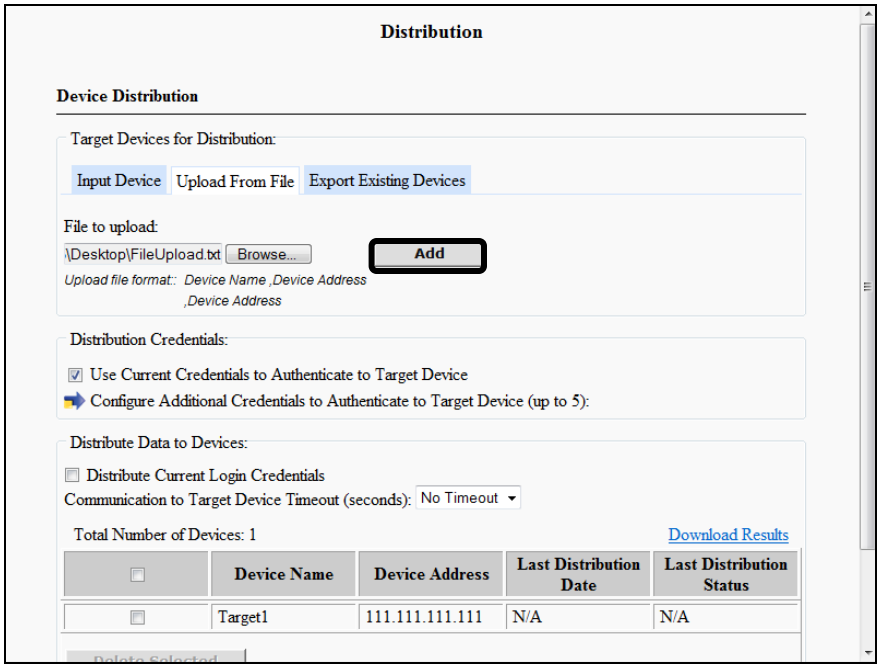


NOTE

The uploaded file extension must be ".txt" or ".csv", is not case-sensitive, and the file size must be less than or equal to 200 KB.

3.2.2 If you clicked [Browse], navigate to the drive or directory containing the file to upload → select the file → click [Open].

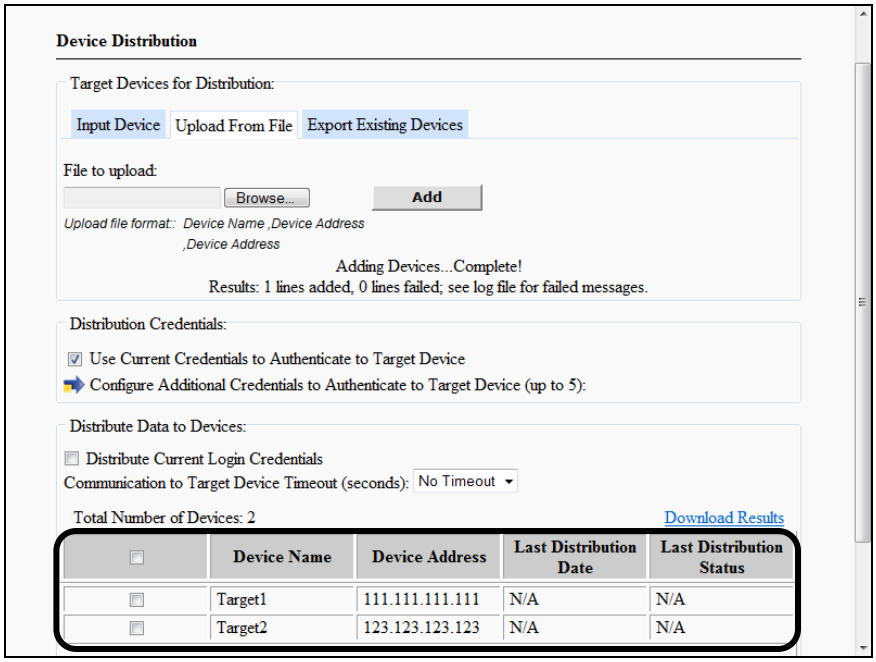
3.2.3 Click [Add] to start the validation process.



Validation is performed to make sure that:

- The uploaded file is a text file with the following format requirements:
  - Each device entry is on a separate line.
  - Each device entry contains a device name and device address separated by a comma (“device_name,device_address”).
  - The device address is in the format of an IP address.
  - Each device name does not contain spaces.
  - Since the device name is optional, the format “,device_address” is also acceptable.
- The device name, if used, does not exceed the maximum of 32 characters. If the device name exceeds 32 characters, it is truncated.
- The IP address format is correct, or the FQDN can be resolved.
- The IP address or the FQDN does not already exist.

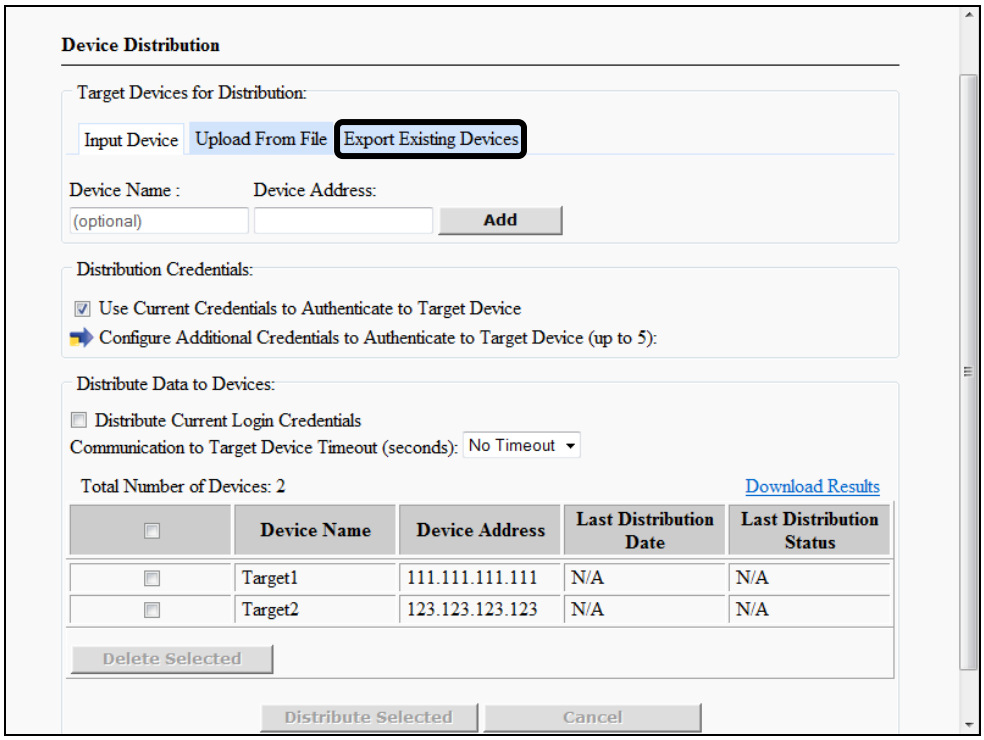
If the validation process is successful, the added device appears in the Distribute Data to Devices table. If it fails, an error message is displayed in red.



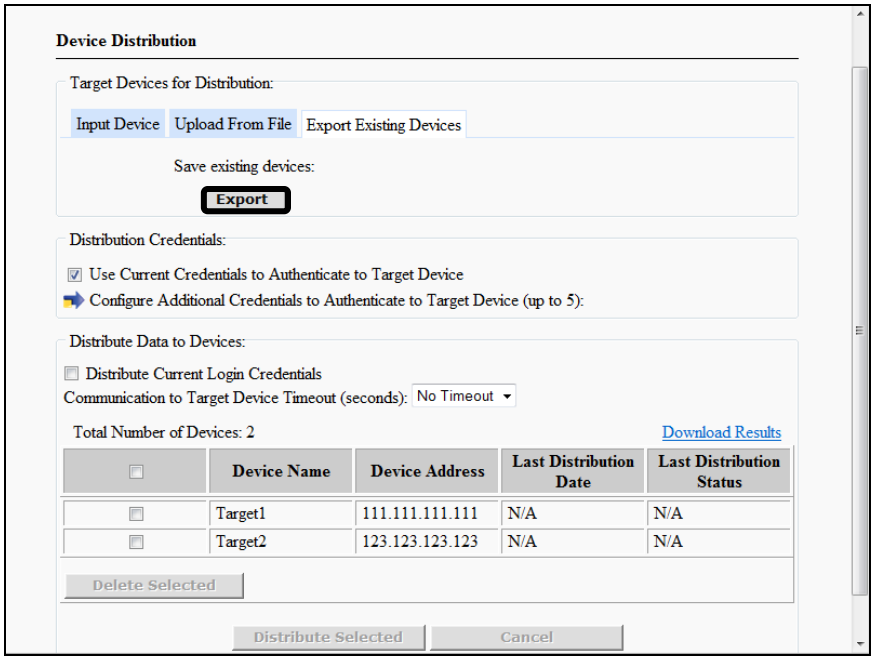
NOTE

- Any line entry in the uploaded file that consists of an invalid format is reported as a failure with the line number. That line is skipped, and uploading continues with the next line.
- Any device address in the uploaded file that has already been saved is ignored, and reported as a duplicate. Only the number of duplicates found in the file is reported, not the exact line number.
- [Add] is disabled when the maximum number of target devices (50) is reached.

3.3 To export the existing target devices to a text file, click the [Export Existing Devices] tab.



3.3.1 Click [Export].



The existing target devices can be exported to a text file.

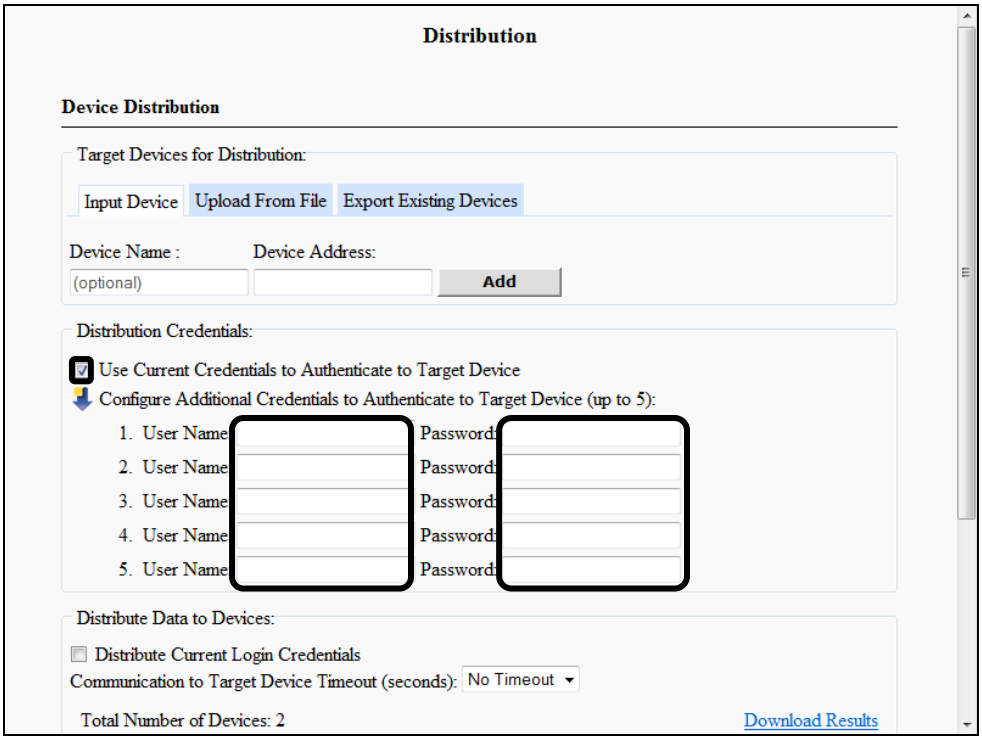
The exported text file is formatted, as described below:

- Each device entry is on a separate line.
- Each device entry contains a device name and device address separated by a comma (“device_name,device_address”).
- The device address is in the format of an IP address or FQDN.
- Since the device name is optional, the format “,device_address” is also acceptable.

3.3.2 Click [File] → [Save As] → navigate to the drive or directory where you want to save the file → click [Save].

4. If you do not want the System Administrator's credentials to be used as one of the configuration distribution credentials that are tried when you authenticate to the target devices, select the [Use Current Credentials to Authenticate to Target Device] check box to clear the check mark → enter at least one user name in a [User Name] text box → enter the password in the [Password] text box.

   You can enter a maximum of 50 characters in each [User Name] and [Password] text box, and up to five user names and passwords.

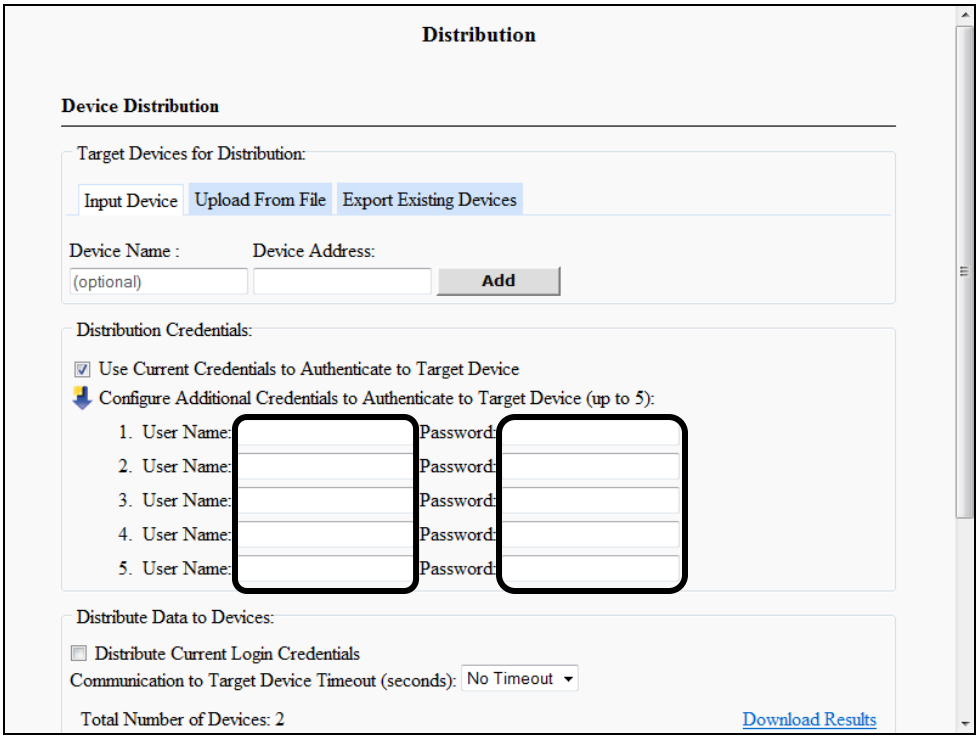


NOTE

- The [Use Current Credentials to Authenticate to Target Device] check box selection is used only when you click [Distribute Selected].
- The [Use Current Credentials to Authenticate to Target Device] check box is selected by default, which is the state to which it returns after you click [Distribute Selected].
- If the check mark is cleared from the [Use Current Credentials to Authenticate to Target Device] check box, at least one additional credential must be configured.
- The user names and passwords entered are only used when you click [Distribute Selected], and the credentials are not saved.

5. If you want to configure additional credentials to be used as one of the configuration distribution credentials that are tried when you authenticate to the target devices, enter a user name in a [User Name] text box → enter the password in the [Password] text box.

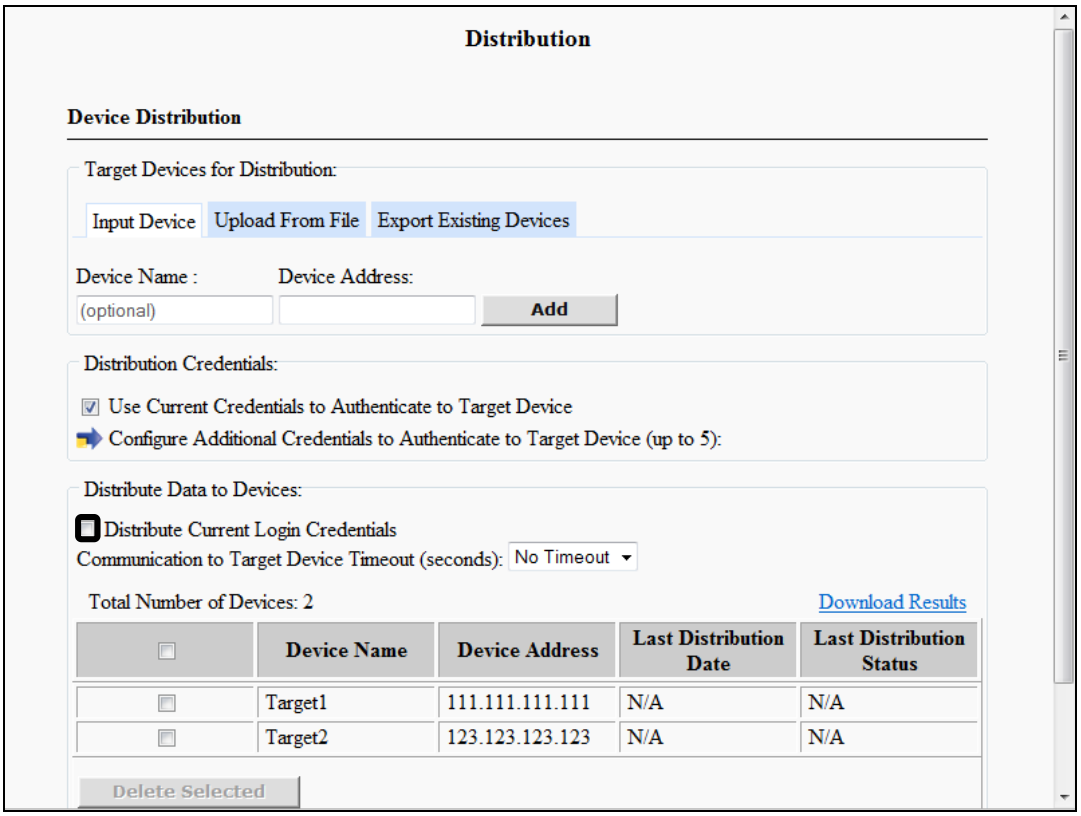
   You can enter a maximum of 50 characters into each [User Name] and [Password] text box, and up to five user names and passwords.



NOTE

- The user names and passwords entered are used only when you click [Distribute Selected], and the credentials are not saved.
- The User Name and Password text boxes are blank by default, which is the state to which they return after you click [Distribute Selected].
- Click the [ ] (down-pointing arrow) icon to hide the additional credentials list, and change the icon to the [ ] (right-pointing arrow).
- Click the [ ] (right-pointing arrow) icon to show the additional credentials list, and change the icon to the [ ] (down-pointing arrow).
- You can toggle between showing and hiding the additional credentials list.
- The default setting' is ' ', which shows the additional credentials list.

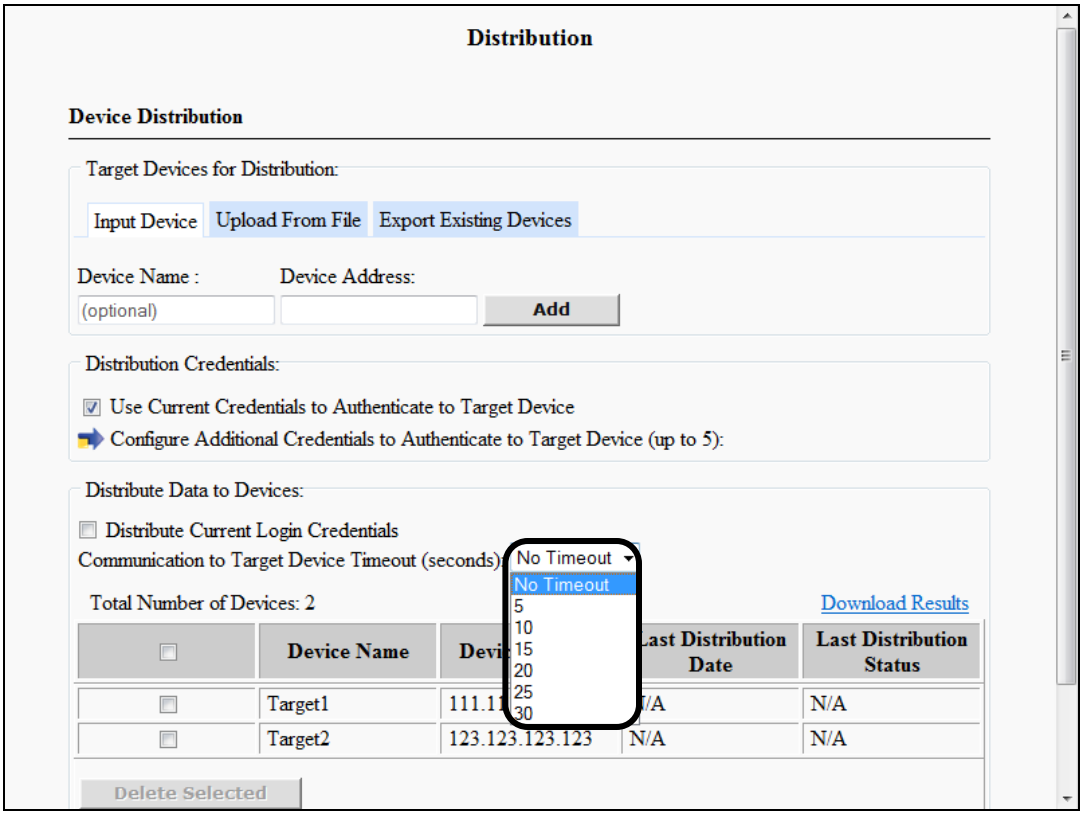
6. Select the [Distribute Current Login Credentials] check box if you want to overwrite the current login credentials of all the target devices with the System Administrator's user name and password that is used to authenticate to the configuration servlet.



NOTE

- The [Distribute Current Login Credentials] check box selection is used only when [Distribute Selected] is clicked, and the current login credentials are not saved.
- The Distribute Current Login Credentials check box is clear by default, which is the state to which it returns after you click [Distribute Selected].

7. From the Communication to Target Device Timeout (seconds) drop-down list, select [No Timeout], [5], [10], [15], [20], [25], or [30] for the communication timeout time.

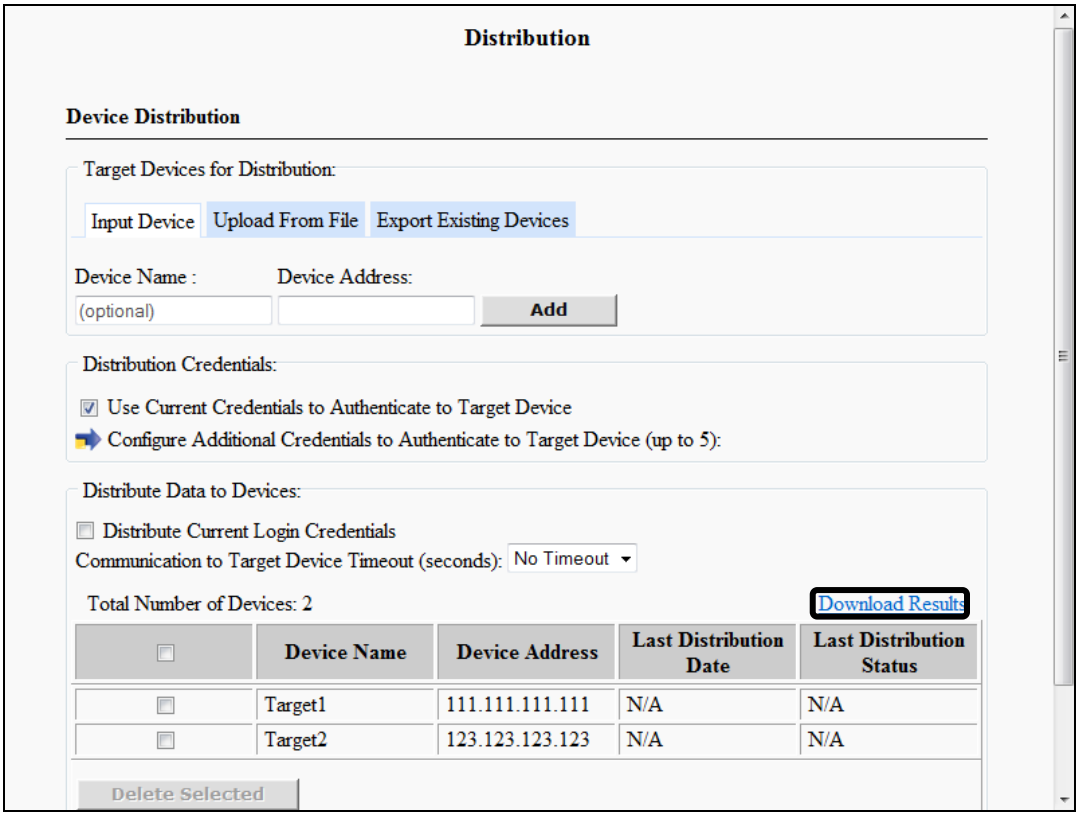


The Communication to Target Device Timeout (seconds) setting is used to specify the amount of time it takes for the source device's configuration distribution module to communicate with the target device's configuration distribution module.

NOTE

- The Communication to Target Devices Timeout (seconds) drop-down list selection is used only after you click [Distribute Selected], and the time out time is not saved.
- The default setting for the Communication to Target Devices Timeout (seconds) drop-down list is 'No Timeout'.

8. If you want to save the Distribute Data to Devices table, click [Download Results].

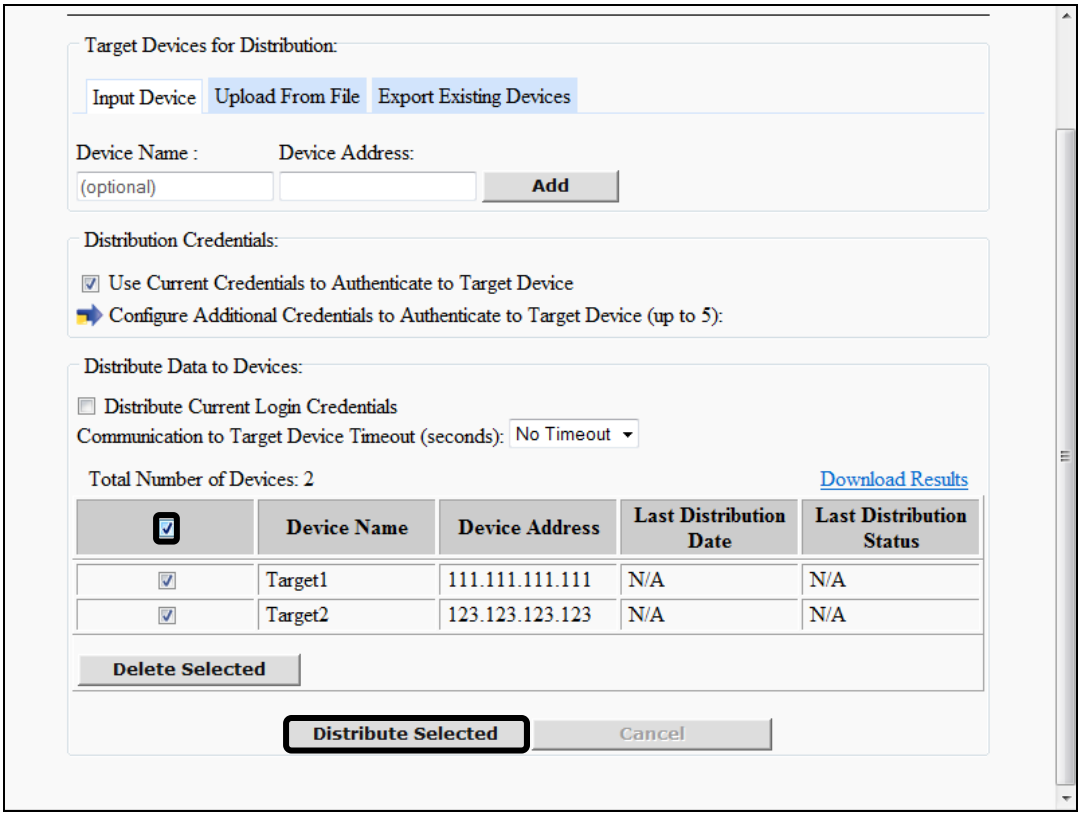


8.1 Click [File] ➞ [Save As] ➞ navigate to the drive or directory where you want to save the file ➞ click [Save].

The downloaded file is rendered as a text file that consists of rows. The maximum number of rows is 50. Each row consists of the following five fields separated by commas:

- The first field is labeled “Application Name.” It is the name of the application that is running.
- The second field is labeled “Device Name.” It is the name of the target device. A blank is displayed if there is no name.
- The third field is labeled “Device Address.” It is the IP address or FQDN of the target device.
- The fourth field is labeled “Last Distribution Date.” It is the date and time of the last distribution to the specific target device. If there has never been a distribution to this target device, <N/A> is displayed.
- The fifth field is labeled “Last Distribution Status.” It is the status of the last distribution to this target device.
  - If there has never been a distribution to this target device, <N/A> is displayed.
  - If there has been a distribution and it was successful, <Successful> is displayed.
  - If there has been a distribution and it failed, <Fail: *Reason*.> is displayed, where *Reason* is replaced with the cause of the failure.

9. To distribute the Authorized Send configuration settings to all of the target devices, click the check box to the left of <Device Name> to select all of the devices → click [Distribute Selected] to start the validation and distribution processes.



Validation is performed to make sure the [Use Current Credentials to Authenticate to Target Device] check box is selected, or at least one additional configuration distribution credential is configured.

The maximum number of target devices that you can distribute to is 50.

Authorized Send can distribute to a maximum of three target devices at one time. Target devices may be distributed out of order, as the network connectivity or speed of each receiving device can be different.

The distribution process attempts to distribute the current Authorized Send configuration data to all of the selected target device IP addresses.

The message <Distribution in progress…> is displayed during the distribution process. If an error occurs, an error message is displayed in red.

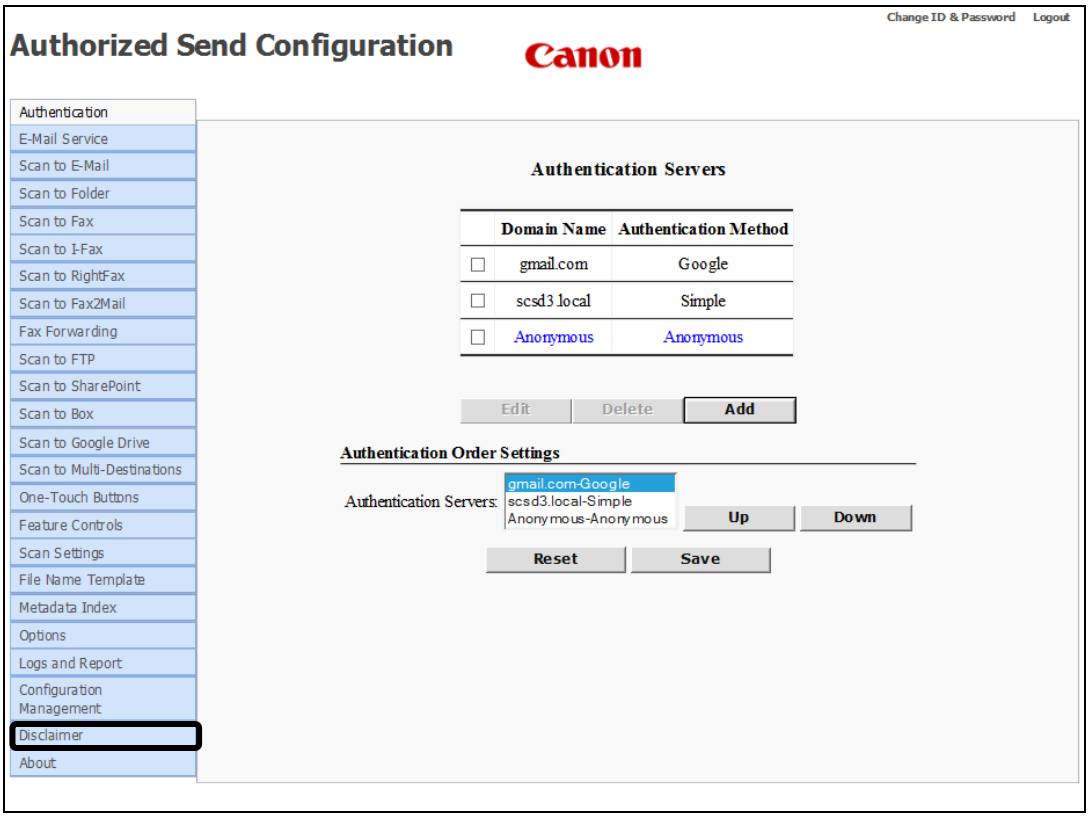
NOTE

- [Add] is disabled during the distribution process.
- The check box that appears before <Device Name> acts as a toggle switch to select or clear all of the check boxes beneath it.
- The check box that appears before each row is used to select or clear that particular row.
- To delete a target device, click [Delete Selected] → [OK]. Only those target devices that have been selected are deleted.
- [Delete Selected] is enabled only when at least one target device is selected.
- Click [Cancel] to cancel the distribution process. Only distribution processes that have not yet started are canceled.
- [Cancel] is enabled only when the distribution process starts.

2.27 Configuring the Disclaimer

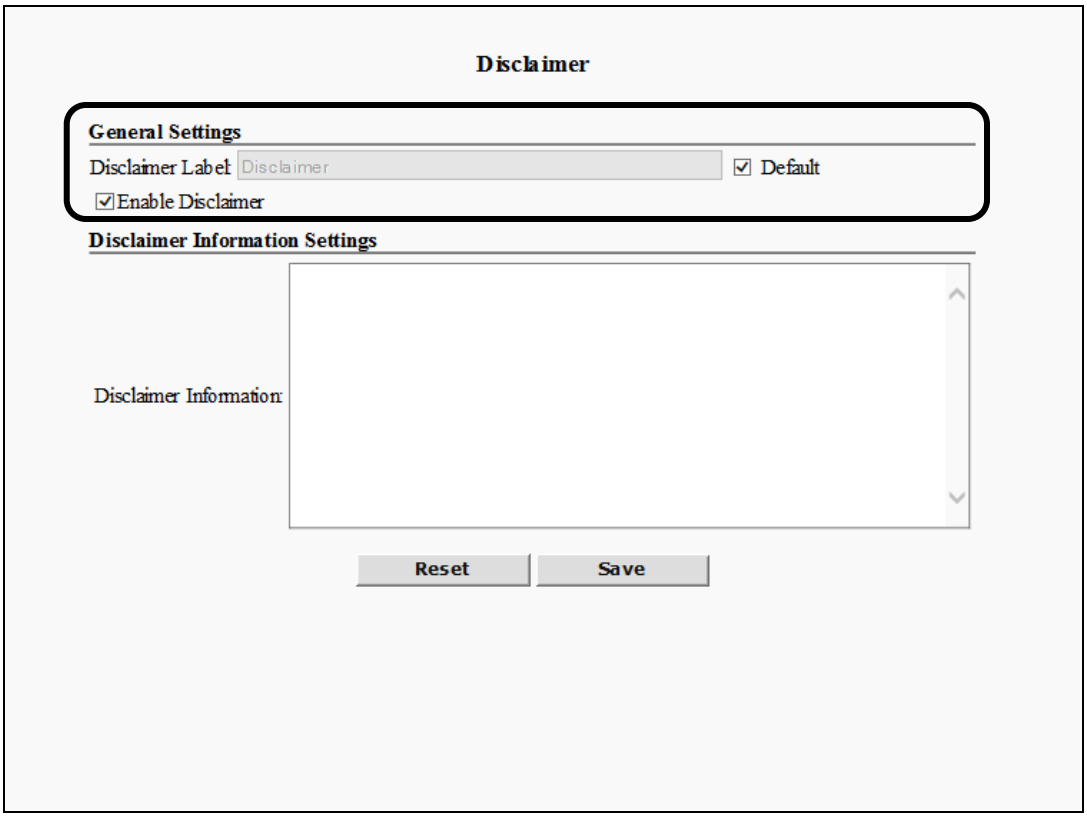
You can configure the Disclaimer function, which enables or disables display of a disclaimer screen when Authorized Send starts and after the user logs off of Authorized Send.

1. Click [Disclaimer].



The Disclaimer screen is displayed.

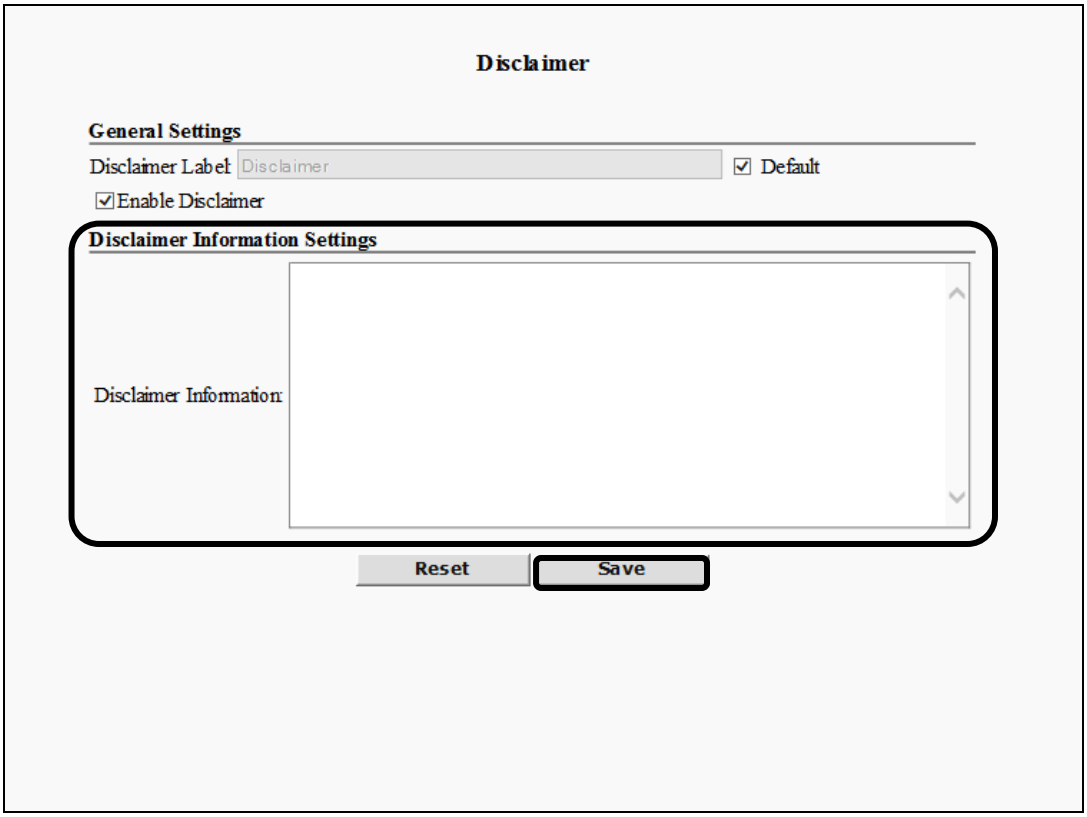
2. Configure the settings under <General Settings>.



General Settings

Disclaimer Label:	Enter the title of the disclaimer screen on the machine console. This text box is not active unless you uncheck the [Default] check box. The default is “Disclaimer”.
Default:	Select this check box to set the Disclaimer title to “Disclaimer”. This check box is selected by default.
Enable Disclaimer:	Select this check box to display a disclaimer text screen before a user logs in to Authorized Send and after a user logs out of Authorized Send. This check box is unselected by default.

3. Configure the settings under <Disclaimer Information Settings> → click [Save].



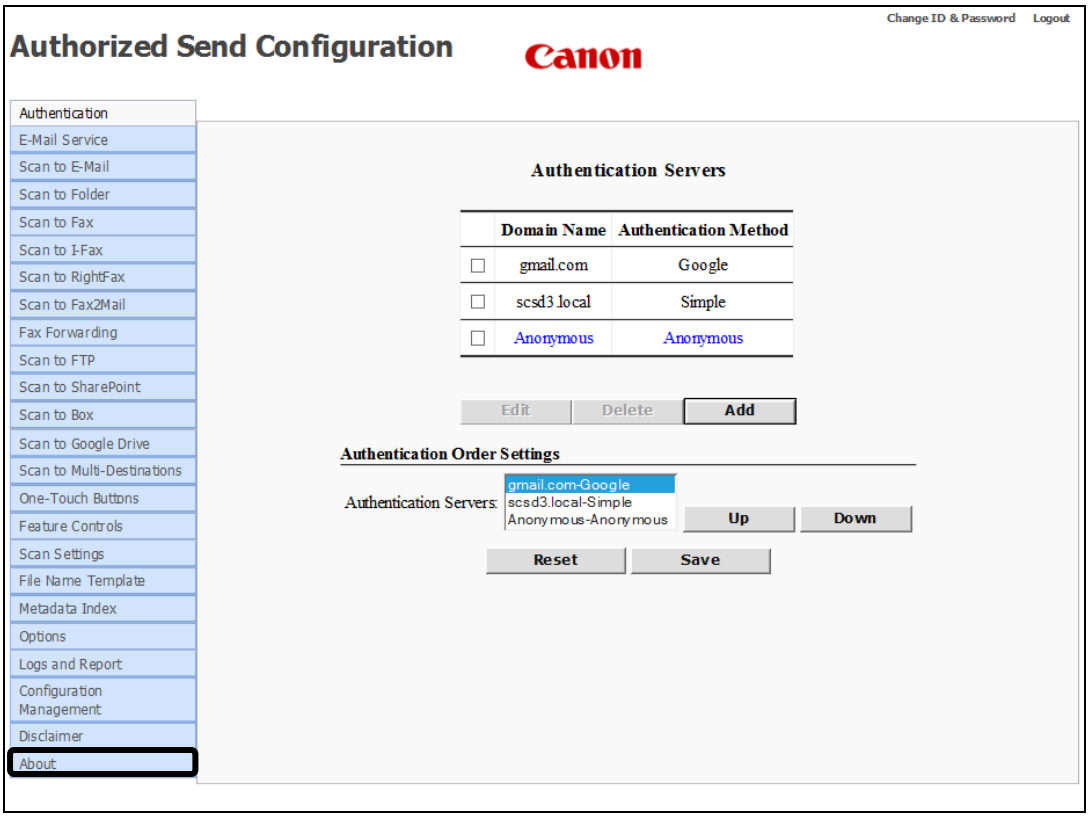
Disclaimer Information Settings

Enter the text to display on the disclaimer screen in the [Disclaimer Information] text box. The text box must have at least one character and no more than 5,000 characters. The [Disclaimer Information] text box appears only if the [Enable Disclaimer] check box is enabled.

2.28 Viewing the Version Number

You can display the version number of Authorized Send.

1. Click [About].

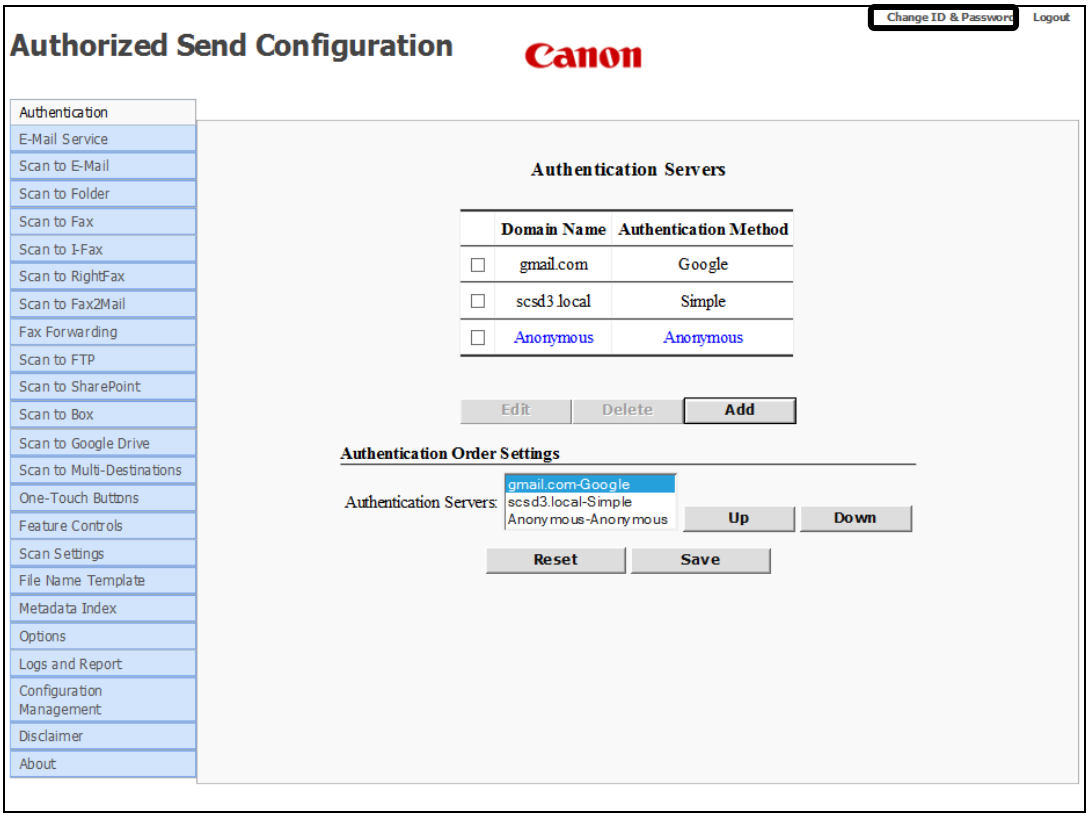


The About screen is displayed with the version number of Authorized Send.

2.29 Changing the Login ID and Password

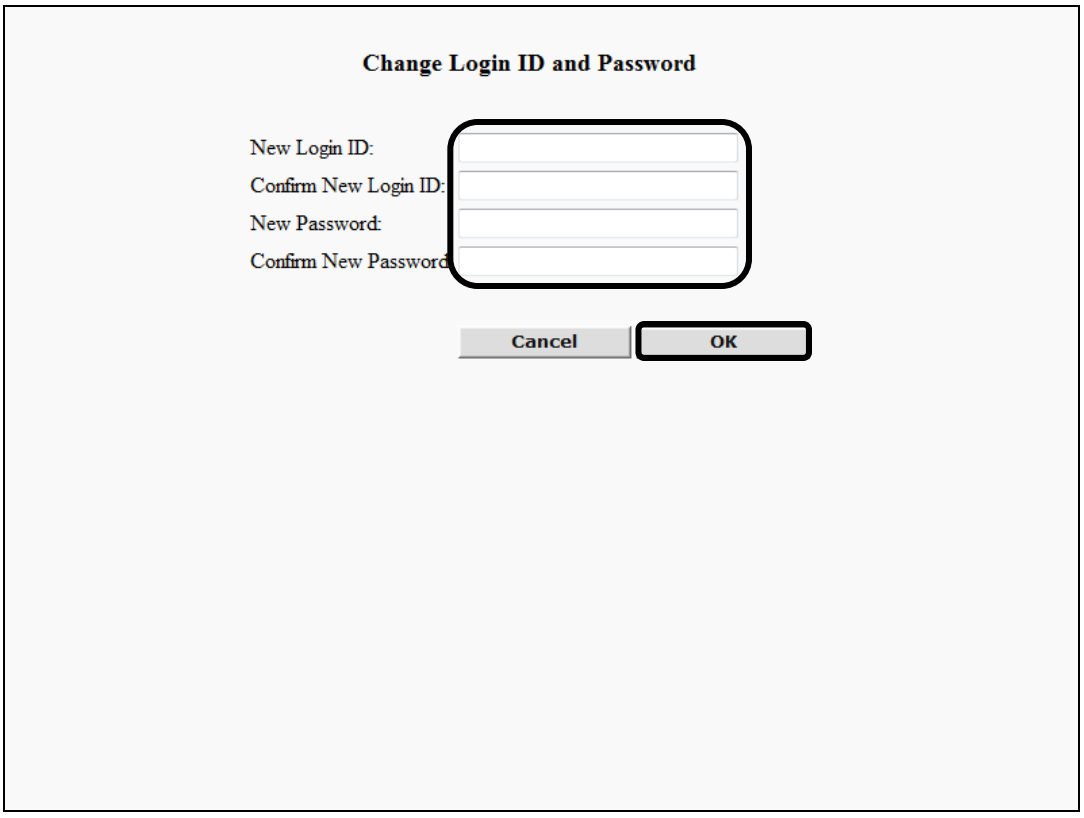
You can change your Login ID and password that is used to log on to the Authorized Send Configuration servlet.

1. Click [Change ID & Password].



The Change Login ID and Password screen is displayed.

2. Enter the new login ID in the [New Login ID] text box → confirm the ID in the [Confirm New Login ID] text box → enter the new password in the [New Password] text box → confirm the password in the [Confirm New Password] text box → click [OK].



If you do not want to change the login ID and password, click [Cancel].

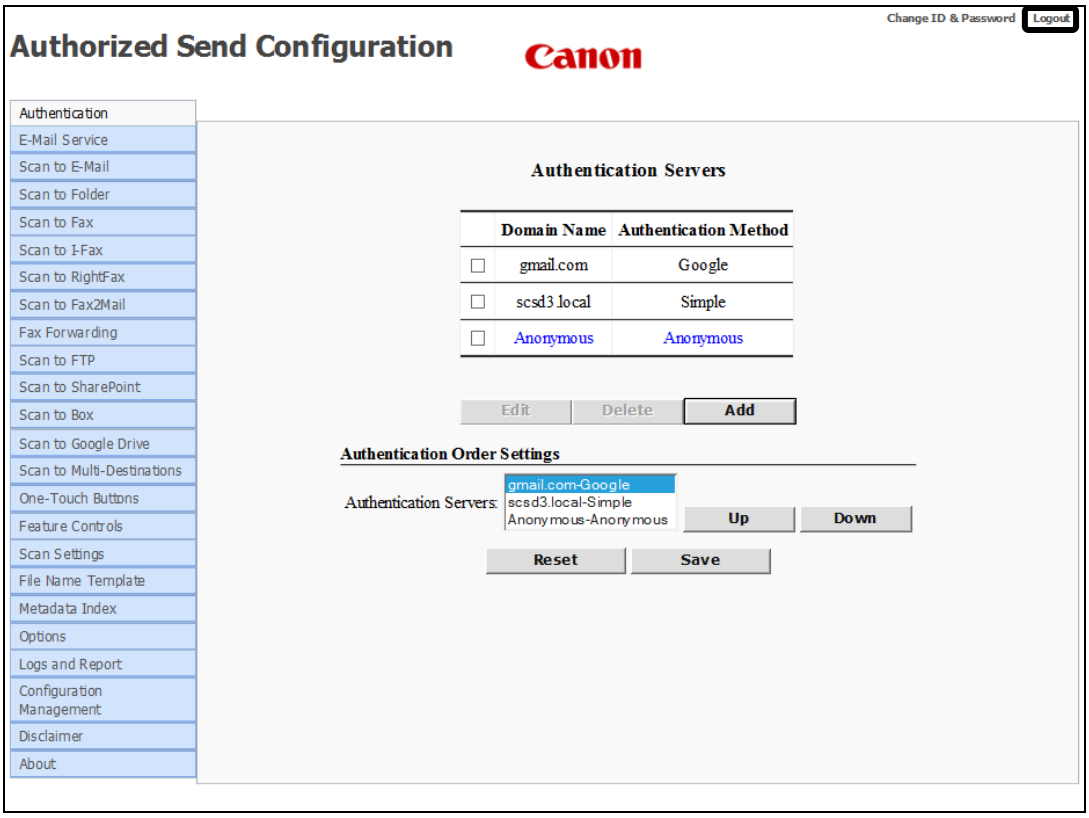
NOTE

You can enter a maximum of 50 alphanumeric characters and spaces for the new login ID and new password.

2.30 Logging Off Authorized Send

Follow the procedure below to log off the Authorized Send Configuration servlet.

1. Click [Logout] from any Authorized Send Configuration screen.



The Please Enter Login ID And Password screen is displayed.

NOTE

You are automatically logged off the Authorized Send Configuration servlet if the time specified in the Options screen elapses. For information on specifying the session timeout setting, see "Configuring the Options Settings," on p. 442.

2.31 Using the Brand Configuration Tool (Optional)

This section describes how to dynamically modify the appearance of the user's interface screens using the optional Brand Configuration tool. You can customize the application's banner image and colors, portal service logo, screen colors, button colors, and special button colors.

NOTE

- If you are upgrading from a previous version of Authorized Send that uses the default brand configuration, the new brand configuration takes effect when Authorized Send is installed.
- If you are upgrading from a previous version of Authorized Send that uses a customized brand configuration, the new brand configuration does not take effect when Authorized Send is installed (the brand configuration is left as is).

---

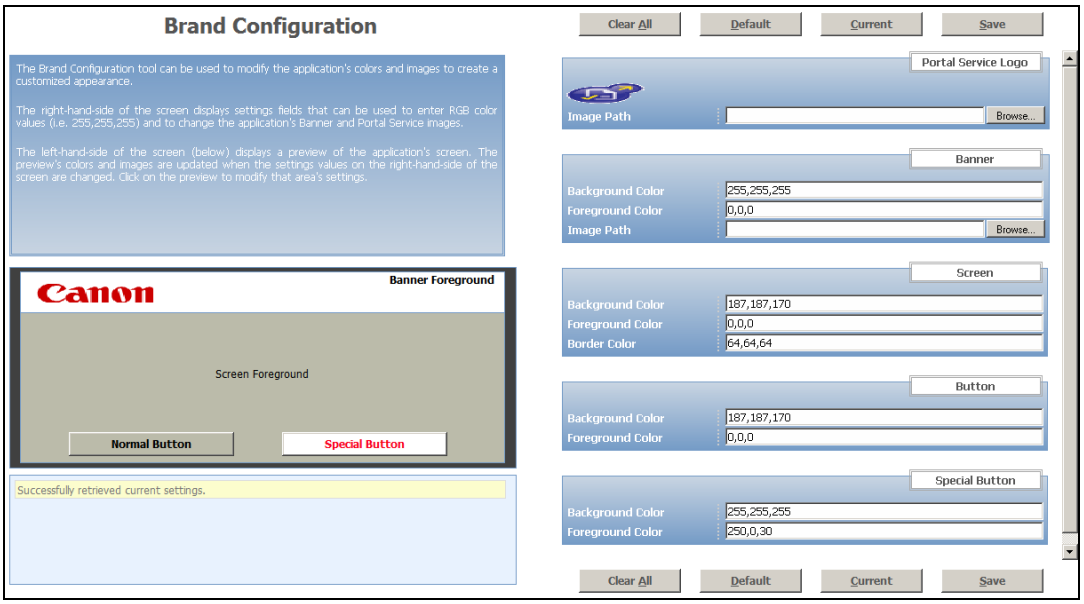
1. Open a browser window → enter the following URL:

   http://<device IP>:8000/AuthSendConfiguration/branding
   (Replace <device IP> with the IP address of the MEAP device.)

IMPORTANT

Enter **AuthSendConfiguration/branding** exactly as shown, as it is case-sensitive.

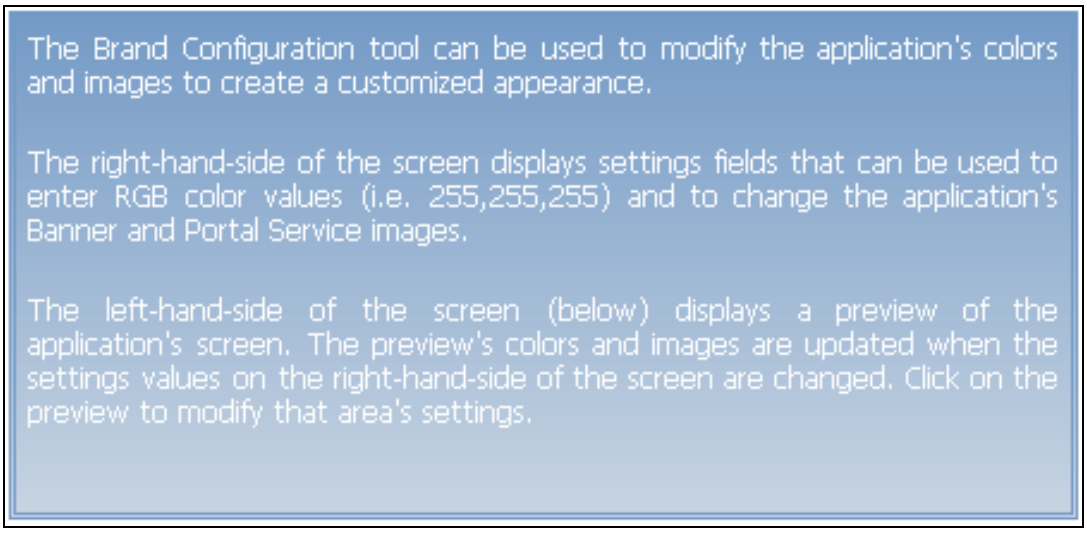
The Brand Configuration tool screen is displayed.



The following section describes the different areas that make up the Brand Configuration tool screen.

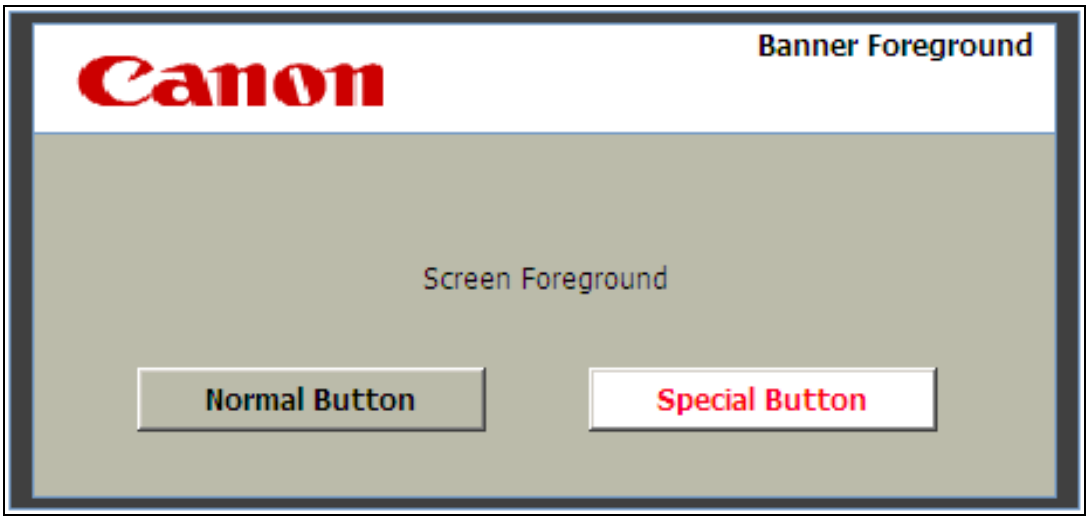
Description Area:

The description area displays an explanation of the Brand Configuration tool's purpose.



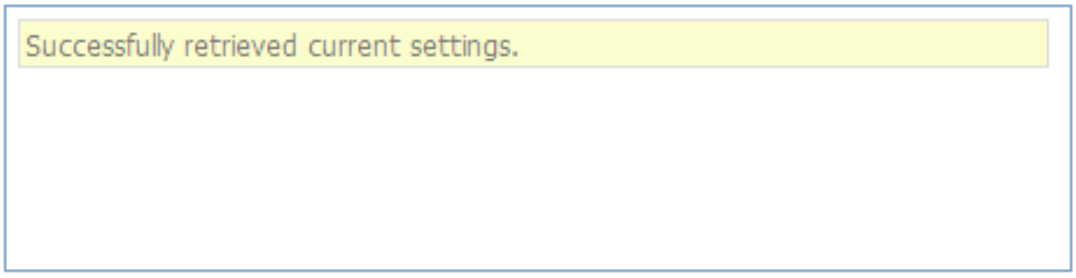
Preview Area:

The preview area displays a preview of how the user's interface screens appear after changing the selected images and colors. This area displays a Banner Foreground, Screen Foreground, Normal Button, Special Button, and all of the images and colors relevant to each.



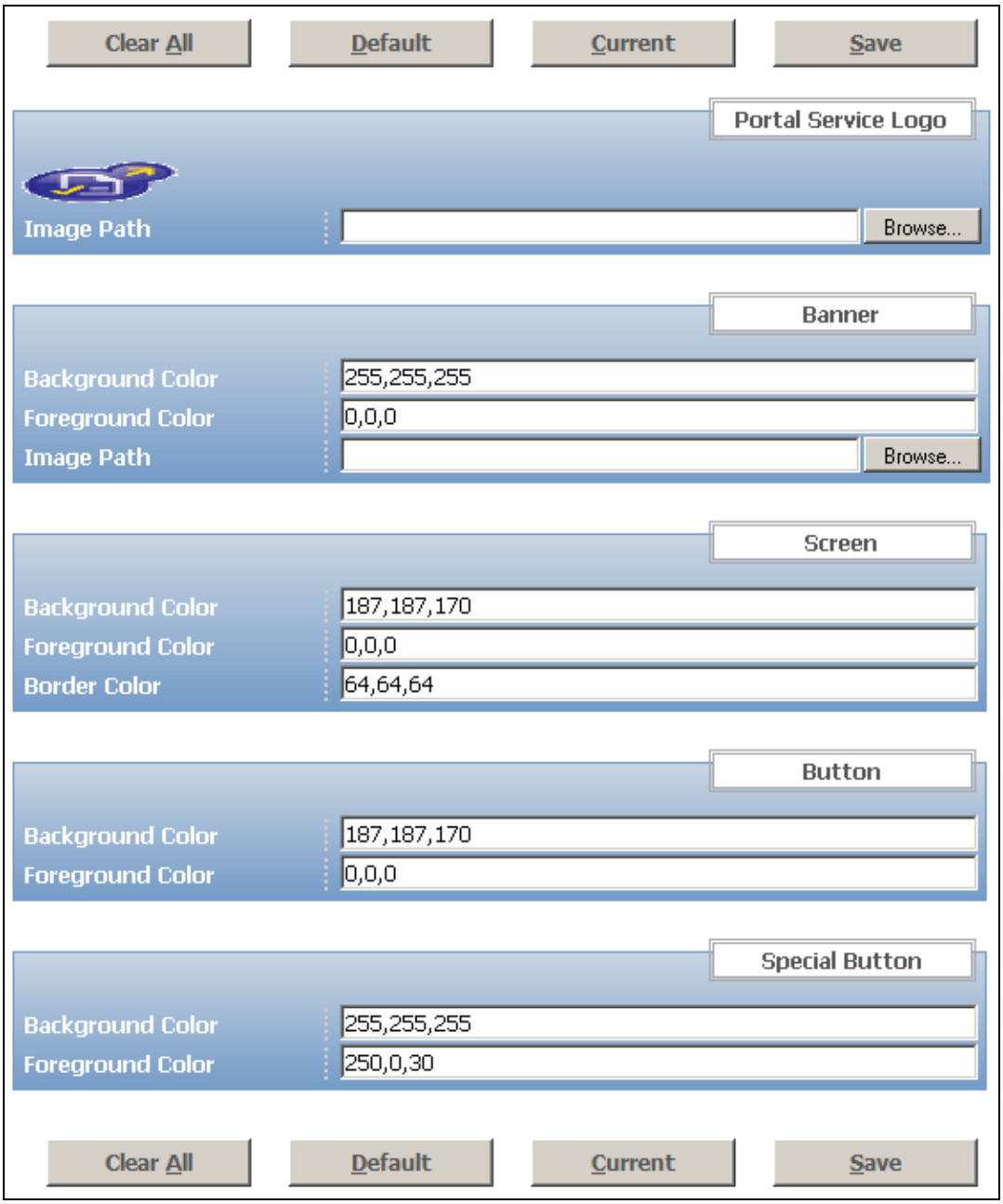
Status Area:

The status area displays messages as various brand configuration operations are performed. It also displays informative messages whenever errors occur. If a message is larger than the display area, a scroll bar appears to enable you to view the entire message.



Settings Area:

The settings area displays the text boxes used for modifying image and color settings seen in the preview area. The settings area is made up of the Portal Service Logo, Banner, Screen, Button, and Special Button.



Portal Service Logo:

The Portal Service Logo provides a text box for entering the location of the application logo, and provides a preview of the selected image.

Banner:

The Banner area provides text boxes for specifying the background and foreground colors, and entering the location of the banner.

Screen:

The Screen area provides text boxes for specifying the background, foreground, and border colors.

Button:

The Button area provides text boxes for specifying the background and foreground colors for normal buttons. A normal button is any button except for the [Sign In] and [Sign Out] buttons.

Special Button:

The Special Button area provides text boxes for specifying the background and foreground colors for special buttons. Special buttons are the [Sign In] and [Sign Out] buttons.

NOTE

- The default values for the Portal Service Logo and Banner Image screens are:

Item	Value
Portal Service Logo for imageRUNNER ADVANCE Devices	
Banner Image	

- The default values for the Background Color, Foreground Color, Border Color, Banner, Screen, Button, and Special Button screens are:

Default Color	Banner	Screen	Button	Special Button
Background Color	255,255,255	187,187,170	187,187,170	255,255,255
Foreground Color	0,0,0	0,0,0	0,0,0	250,0,30
Border Color	N/A	64,64,64	N/A	N/A

2. Select [Clear All], [Default], or [Current].

Clear All: Clears all of the settings.

Default: Loads the default values for each setting and populates the corresponding text boxes in the settings area.

Current: Loads the currently saved values for each setting and populates the corresponding text boxes in the settings area.

3. If you want to specify the user's interface portal service logo:

3.1 Click the [Image Path] text box under <Portal Service Logo> → enter the path to the image file you want to display, or click [Browse] → navigate to the drive or directory containing the path to the image file you want to display.

3.2 Click [Save] to save the settings currently displayed in the settings area, and to update the user's interface portal service logo to use the new settings.

The preview area displays the updated image.

IMPORTANT
The supported file formats are jpg, jpeg, gif, and png.

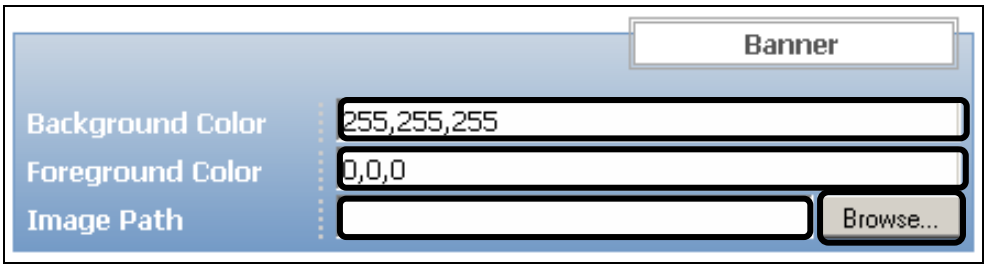
NOTE
The recommended image size is 80 pixels (W) x 23 pixels (H) with 96 dpi.

4. If you want to specify the background and foreground colors, and select the image to be displayed in the user's interface banner area:

   4.1 Click the [Background Color] text box under <Banner> ➞ enter three comma-separated digits representing the desired RGB color.

   4.2 Click the [Foreground Color] text box under <Banner> ➞ enter three comma-separated digits representing the desired RGB color.

   4.3 Click the [Image Path] text box under <Banner> ➞ enter the path to the image file you want to display, or click [Browse] ➞ navigate to the drive or directory containing the path to the image file you want to display.



   4.4 Click [Save] to save the settings currently displayed in the settings area, and to update the user's interface banner to use the new settings.

   The preview area displays the updated colors and image.

   IMPORTANT
   The supported file formats are jpg, jpeg, gif, and png.

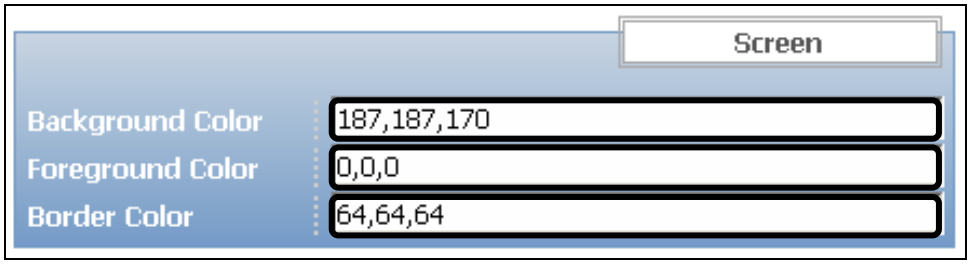
   NOTE
   The recommended image size is 133 pixels (W) x 45 pixels (H) with 96 dpi.

5. If you want to specify the background, foreground, and border colors to be displayed in the user's interface screen area:

   5.1 Click the [Background Color] text box under <Screen> → enter three comma-separated digits representing the desired RGB color.

   5.2 Click the [Foreground Color] text box under <Screen> → enter three comma-separated digits representing the desired RGB color.

   5.3 Click the [Border Color] text box under <Screen> → enter three comma-separated digits representing the desired RGB color.



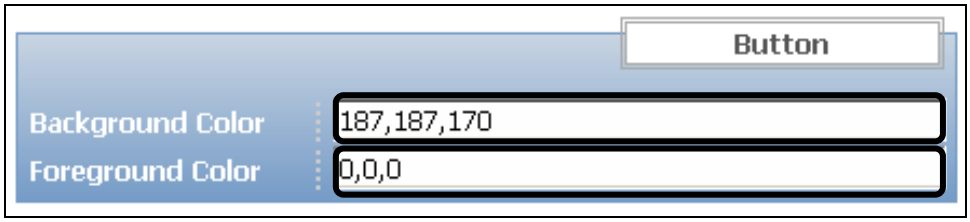
   5.4 Click [Save] to save the settings currently displayed in the settings area, and to update the user's interface screen to use the new settings.

   The preview area displays the updated colors.

6. If you want to specify the user's interface background and foreground colors for the normal buttons:

   6.1 Click the [Background Color] text box under <Button> ➞ enter three comma-separated digits representing the desired RGB color.

   6.2 Click the [Foreground Color] text box under <Button> ➞ enter three comma-separated digits representing the desired RGB color.



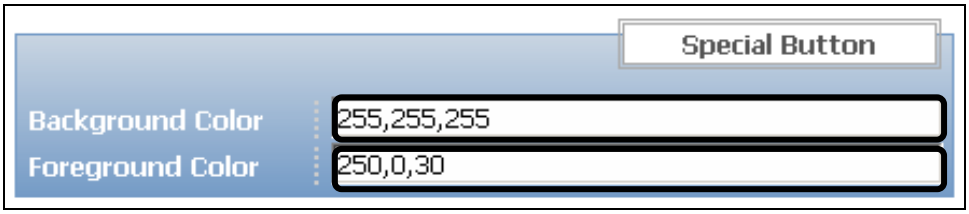
   6.3 Click [Save] to save the settings currently displayed in the settings area, and to update the user's interface normal buttons to use the new settings.

   The preview area displays the updated colors.

7. If you want to specify the user's interface background and foreground colors for the special buttons:

   7.1 Click the [Background Color] text box under <Special Button> → enter three comma-separated digits representing the desired RGB color.

   7.2 Click the [Foreground Color] text box under <Special Button> → enter three comma-separated digits representing the desired RGB color.



   7.3 Click [Save] to save the settings currently displayed in the settings area, and to update the user's interface special buttons to use the new settings.

   The preview area displays the updated colors.

Chapter 3 Configuring the MEAP Device

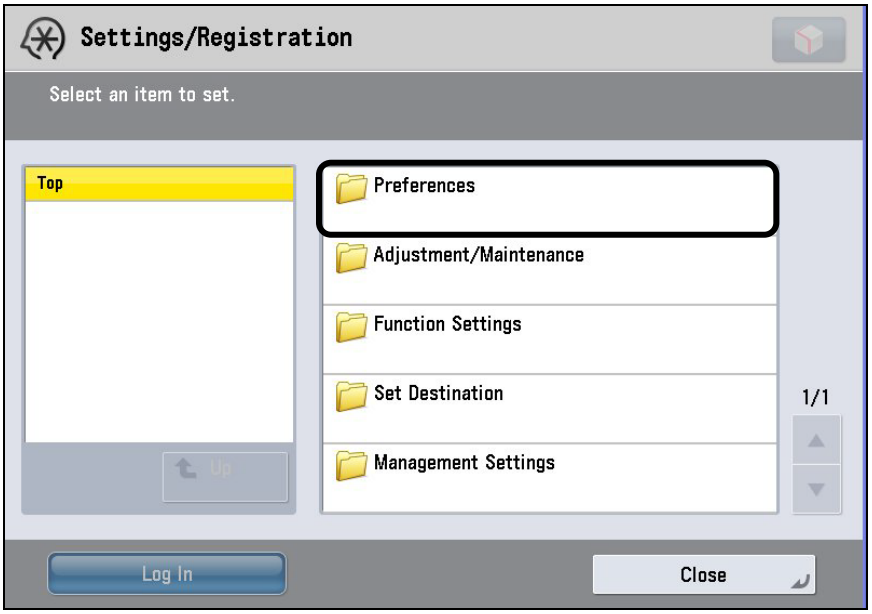
This chapter describes how to configure your MEAP-enabled device so that you can use it with the Authorized Send application.

3.1 DNS Server Settings

After the servers and operating environment is set up, and Authorized Send is installed and configured properly, you must configure your MEAP-enabled device. Follow the procedure below to configure the MEAP device for Authorized Send.

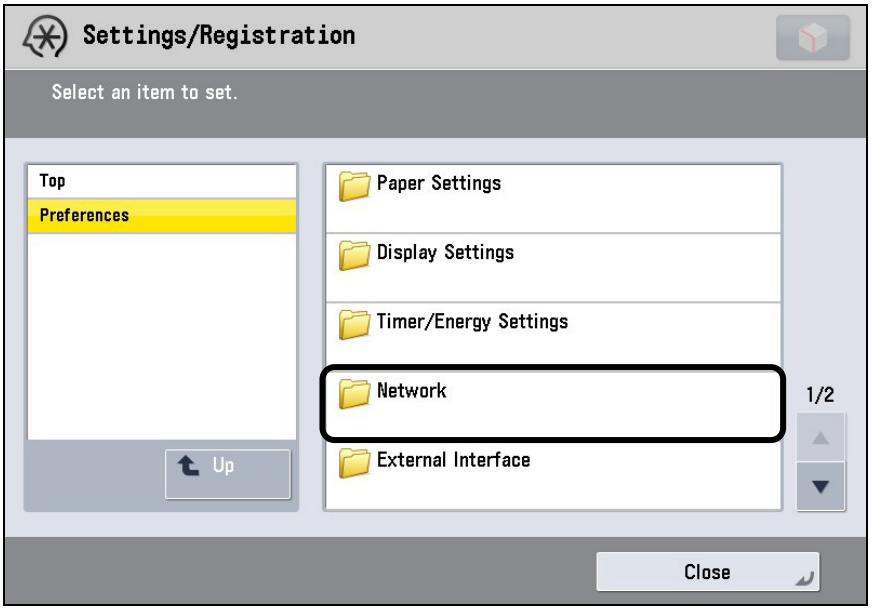
1. On the machine's control panel, press (Settings/Registration).

2. Press [Preferences].

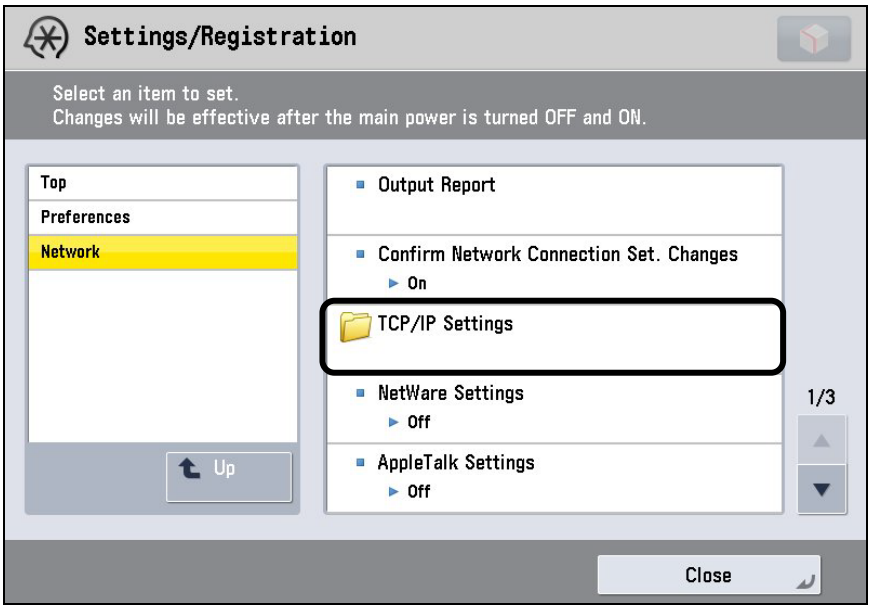


If the System Manager ID and System Password have been set, press [Log In] → enter the System Manager ID and System PIN using ⓪ – ⑨ (numeric keys) → press [Log in].

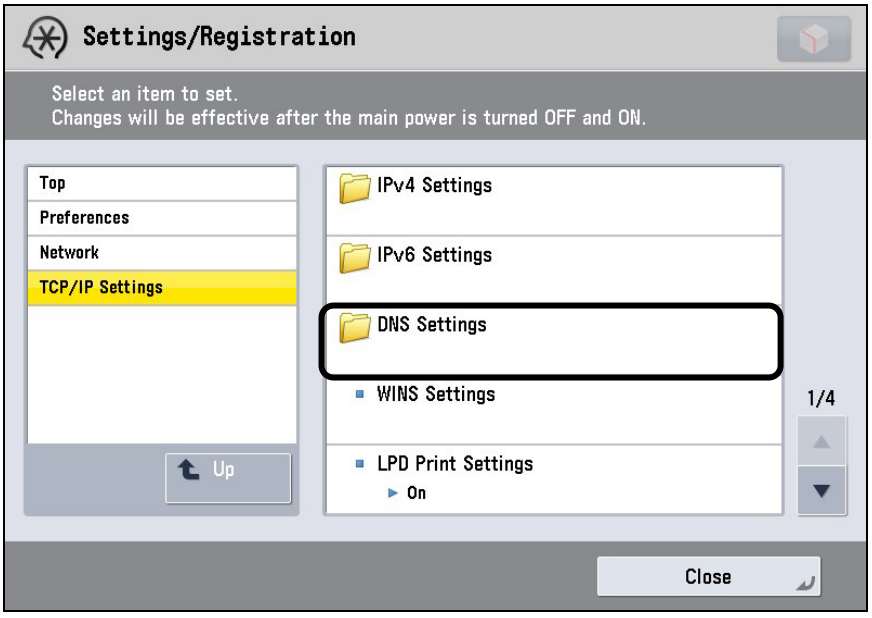
3. Press [Network].



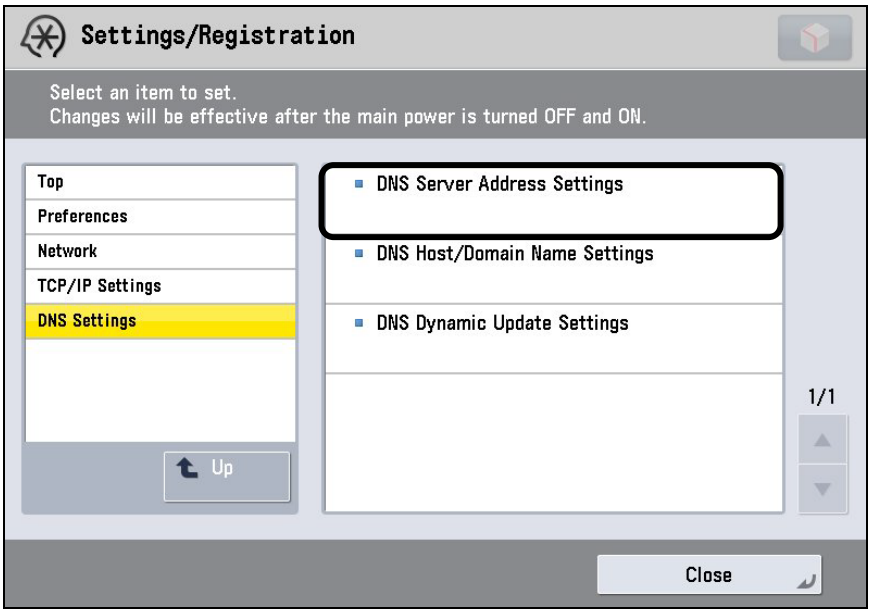
4. Press [TCP/IP Settings].



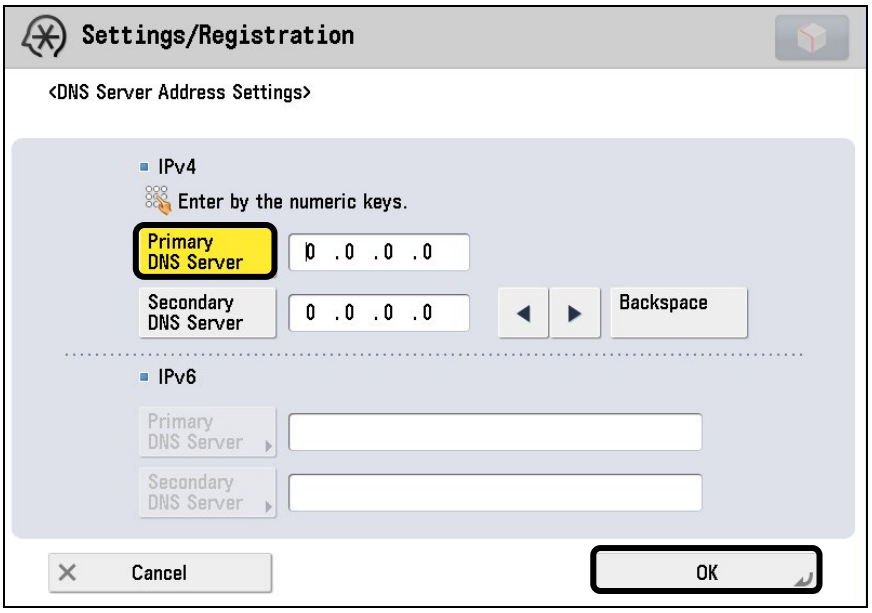
5. Press [DNS Settings].



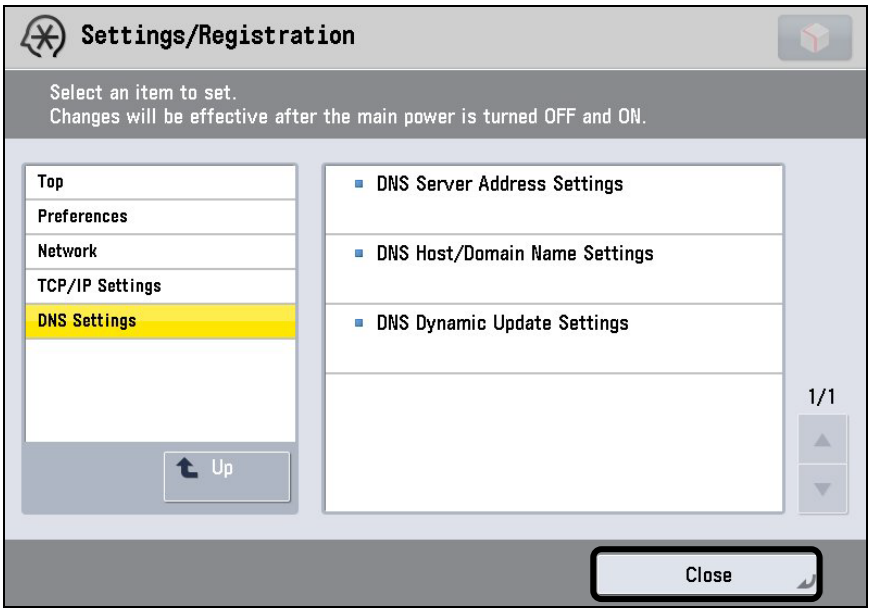
6. Press [DNS Server Address Settings].



7. Press [Primary DNS Server] ➞ enter the IP address using ⓪ – ⑨ (numeric keys) ➞ press [OK].



8. Press [Close].



The Main Menu screen is displayed.

9. Restart the machine.

IMPORTANT

The MEAP device must be restarted before the settings can take effect.

3.2 Automatically Logging Off

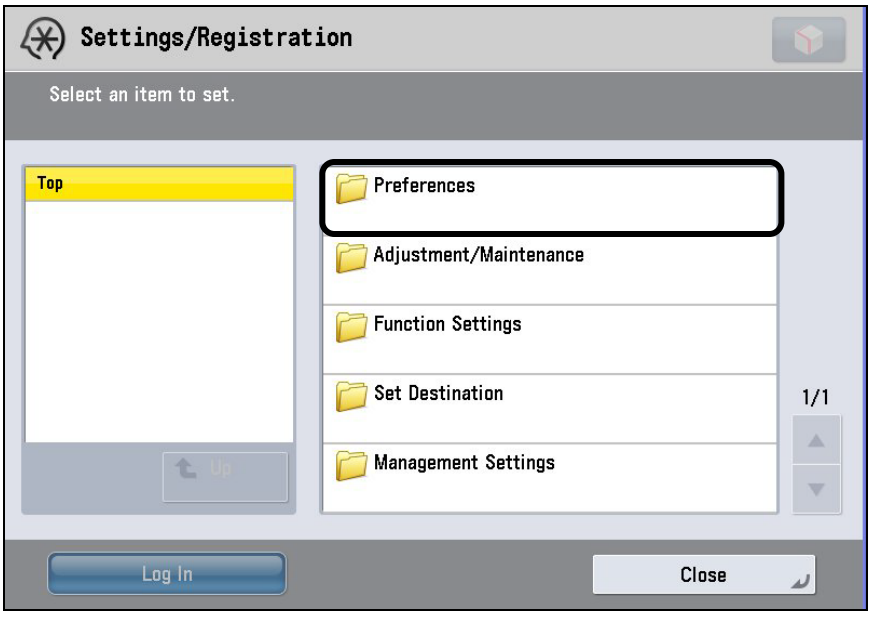
If the machine is idle for a certain period of time (after a scan to e-mail, scan to fax, or scan to folder key operation or job), you are automatically logged off Authorized Send. This period of time is called the “Auto Reset Time”. The Auto Reset Time mode can be set from ‘10’ to ‘50’ seconds in 10 second increments, ‘0’ to ‘9’ minutes in 1 minute increments, and can also be set to ‘Off’.

NOTE
- If [0] is selected, the Auto Reset Time mode is not set.
- The default setting is ‘2’ minutes.

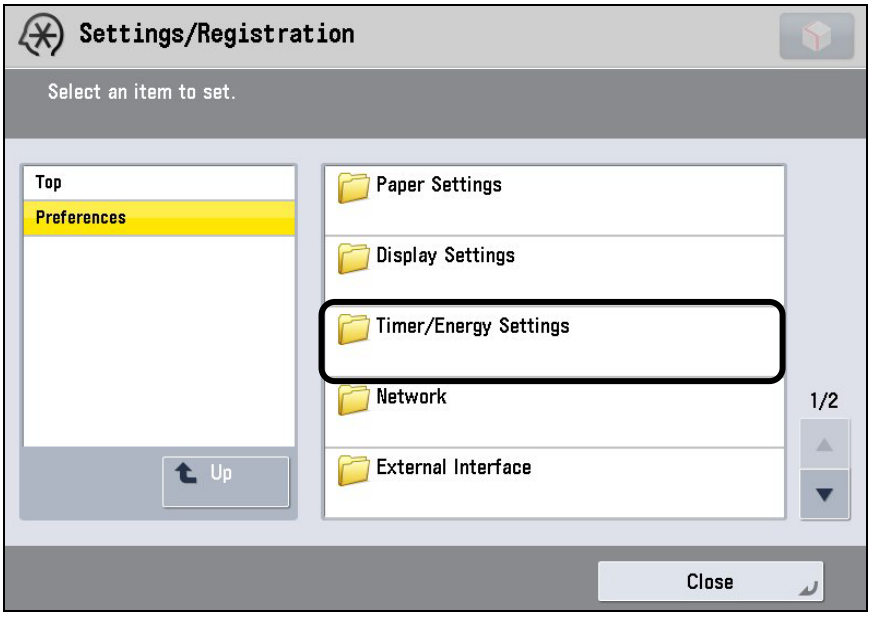
---

1. On the machine’s control panel, press (Settings/Registration).

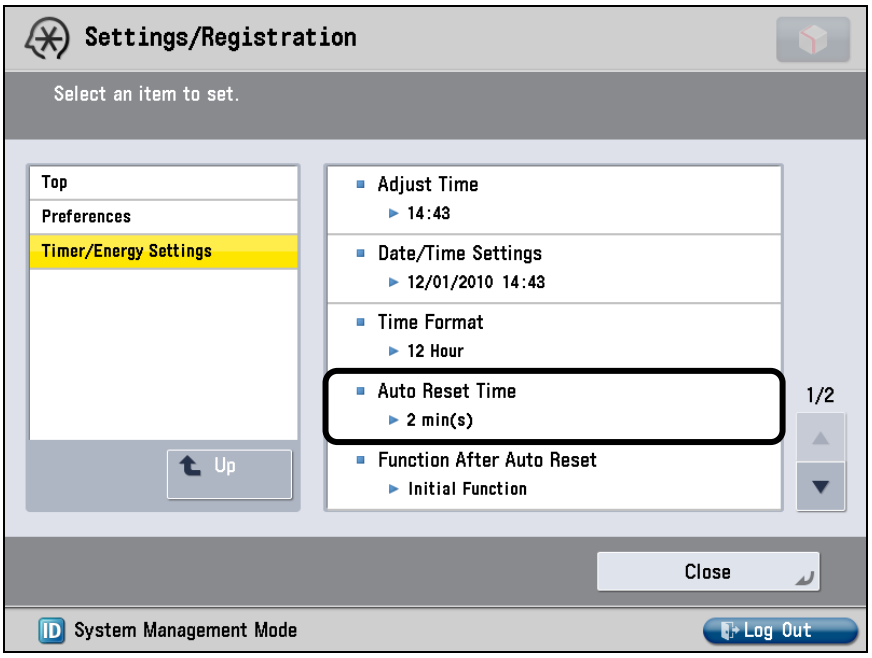
2. Press [Preferences].



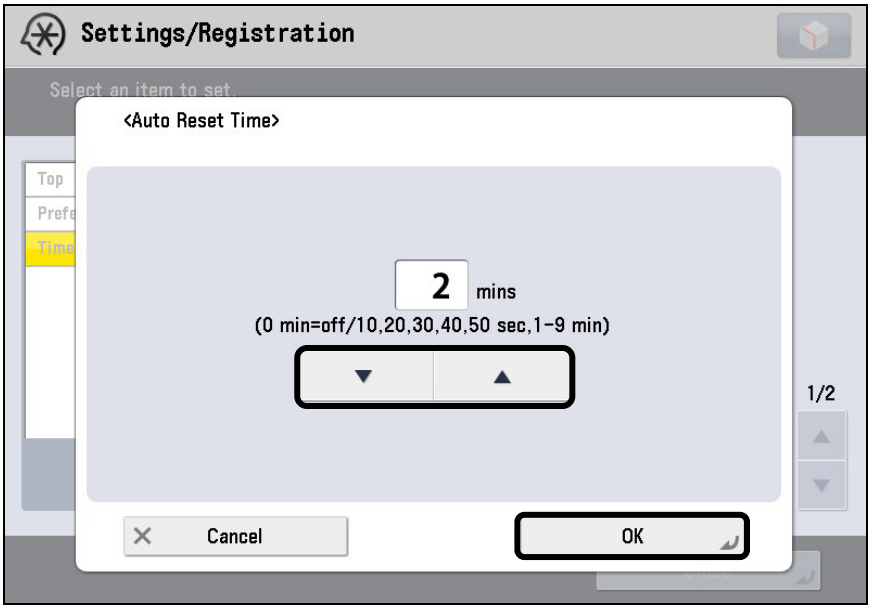
3. Press [Timer/Energy Settings].



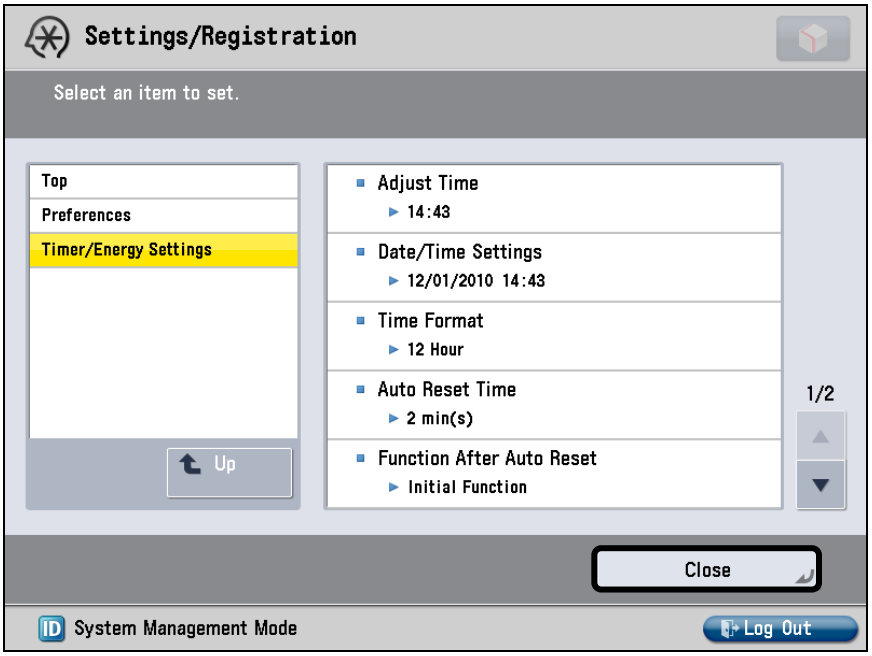
4. Press [Auto Reset Time].



5. Press [▼] or [▲] to specify the desired Auto Reset Time → press [OK].



6. Press [Close].



The Main Menu screen is displayed.

3.3 Synchronizing the Device and Server Time

If you configure an authentication server or address book server for Kerberos authentication, you must ensure that the device clock and server clock are synchronized within the maximum server specified clock skew tolerance of '5' minutes. When you authenticate using Kerberos, if there is more than a 5-minute time difference between the device clock and server clock, an error message is displayed.

You can manually adjust the device time to synchronize with the server time, or you can set to automatically synchronize the device clock with the server clock.

3.3.1 Automatic Time Synchronization

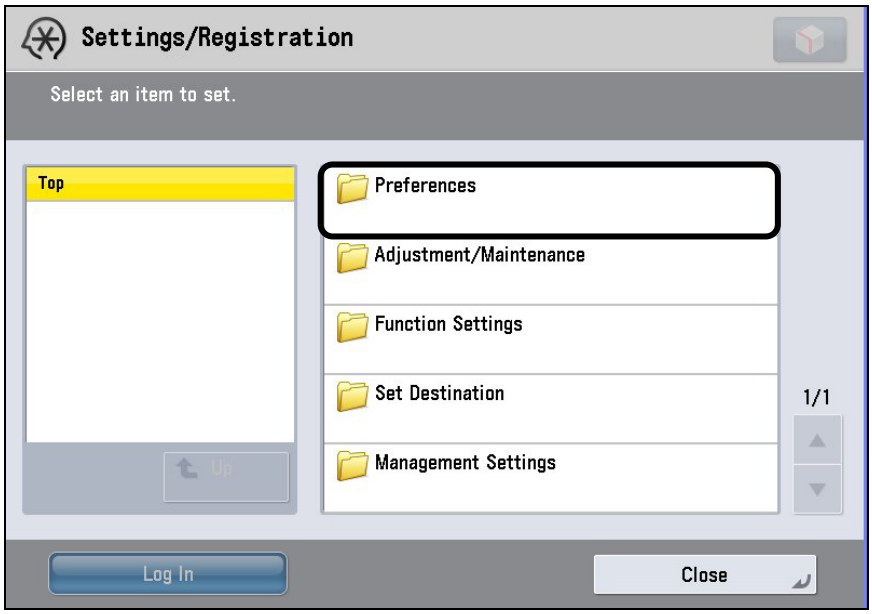
You can set the SNTP (Simple Network Time Protocol) settings to enable imageRUNNER ADVANCE machines to automatically synchronize their system time with a public time server.

IMPORTANT

To perform time synchronization via SNTP, it is necessary to set the time zone of the region in which you are using the machine in advance. For instructions on how to set the time zone, see the appropriate e-Manual that came with your machine.

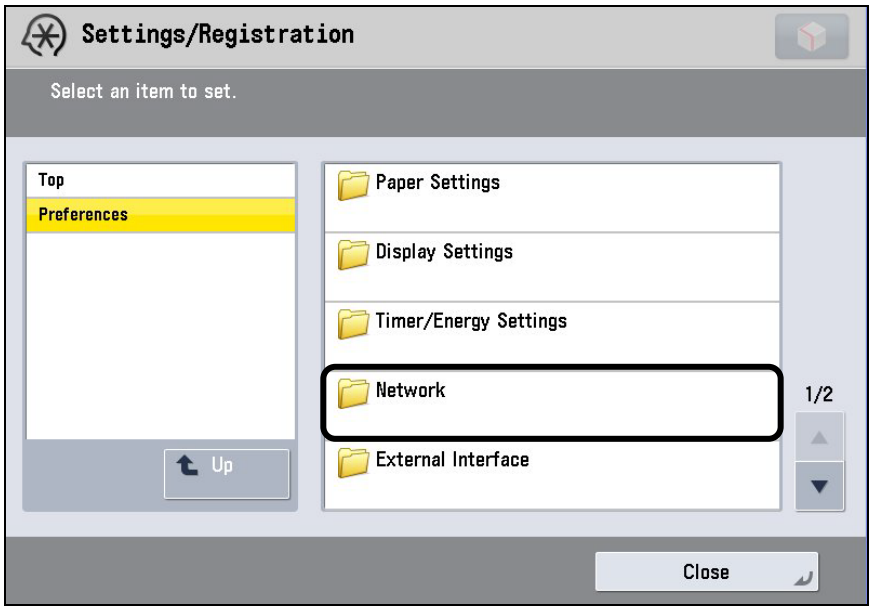
1. On the machine's control panel, press (Settings/Registration).

2. Press [Preferences].

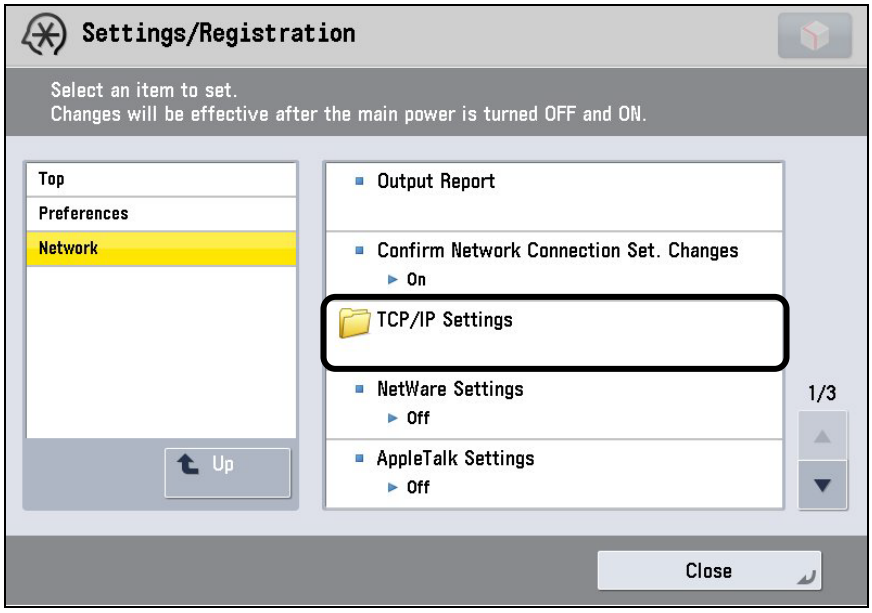


If the System Manager ID and System Password have been set, press [Log In] → enter the System Manager ID and System PIN using ⓪ – ⑨ (numeric keys) → press [Log in].

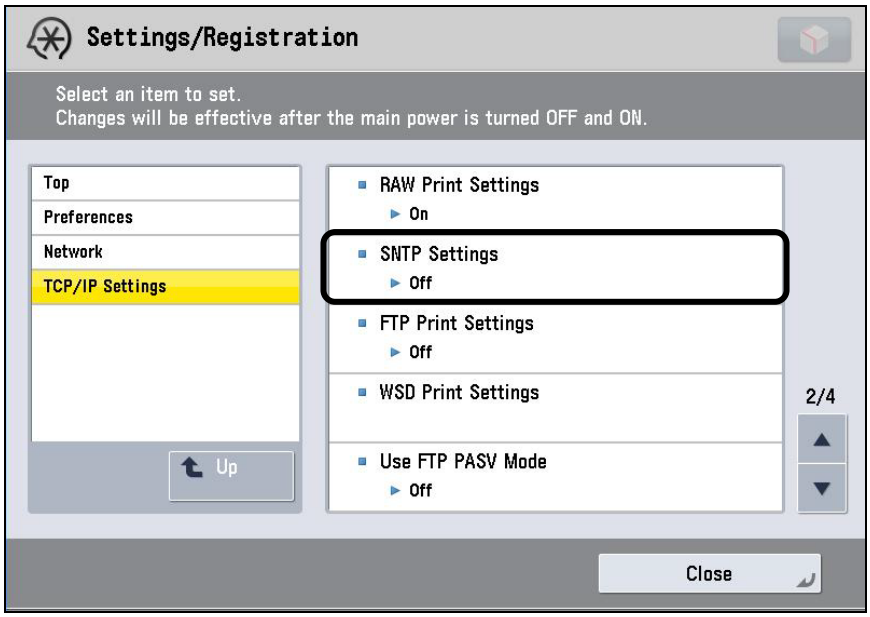
3. Press [Network].



4. Press [TCP/IP Settings].



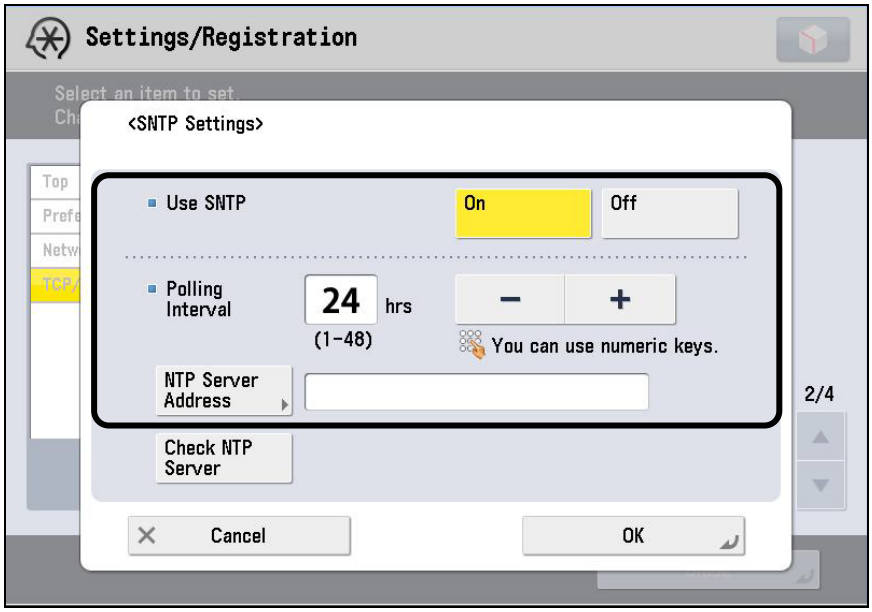
5. Press [SNTP Settings].



NOTE

If the desired setting is not displayed, press [▼] or [▲] to scroll to the desired setting.

6. Specify the SNTP settings.

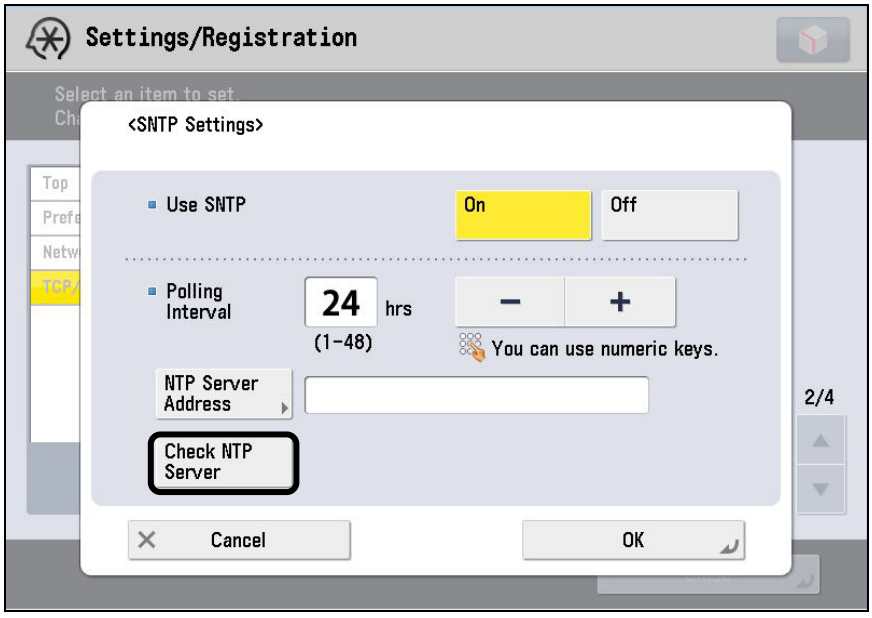


Use SNTP: Select [On] to perform time synchronization using SNTP.

Polling Interval: Select the interval for performing time synchronization from ‘1’ to ‘48’ hours.

NTP Server Address: Enter the NTP server address or host name.

7. Press [Check NTP Server] to check the status of the NTP server.



If <OK> is displayed next to [Check NTP Server], time synchronization is working correctly via SNTP.

If <Error> is displayed next to [Check NTP Server], check the settings for the NTP Server Address set in step 6.

8. Press [OK].

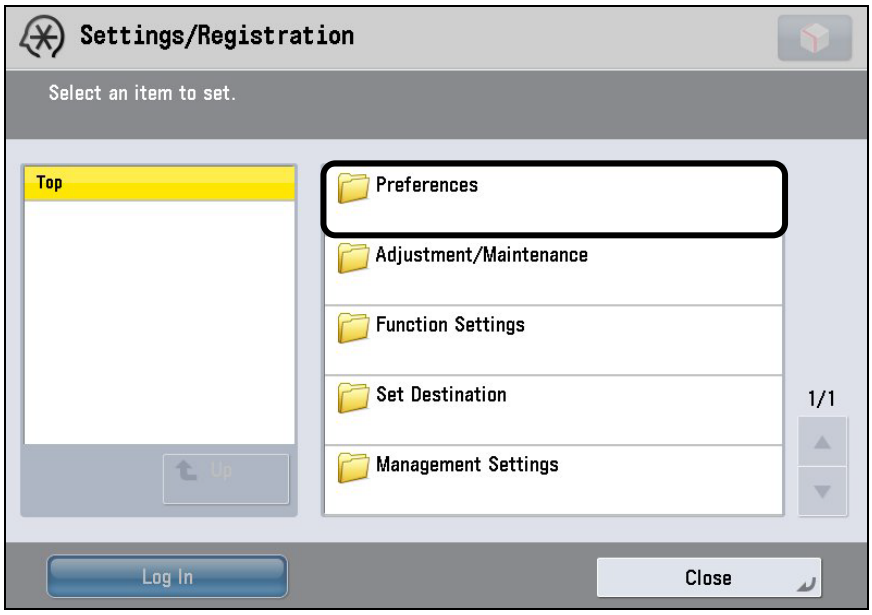
9. Press [Close].

The Main Menu screen is displayed.

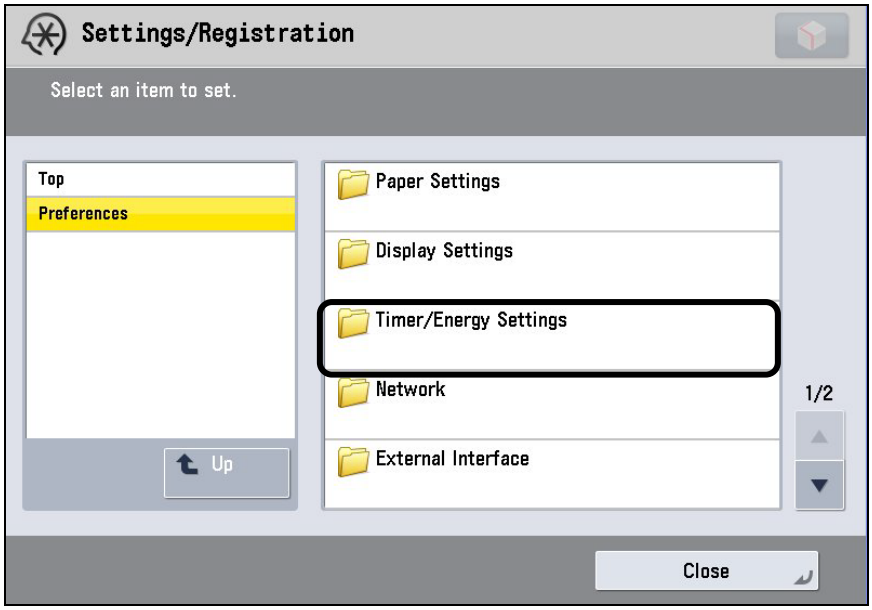
3.3.2 Adjusting the Device Time

You can manually adjust the device time to match the Kerberos authentication server or address book server time.

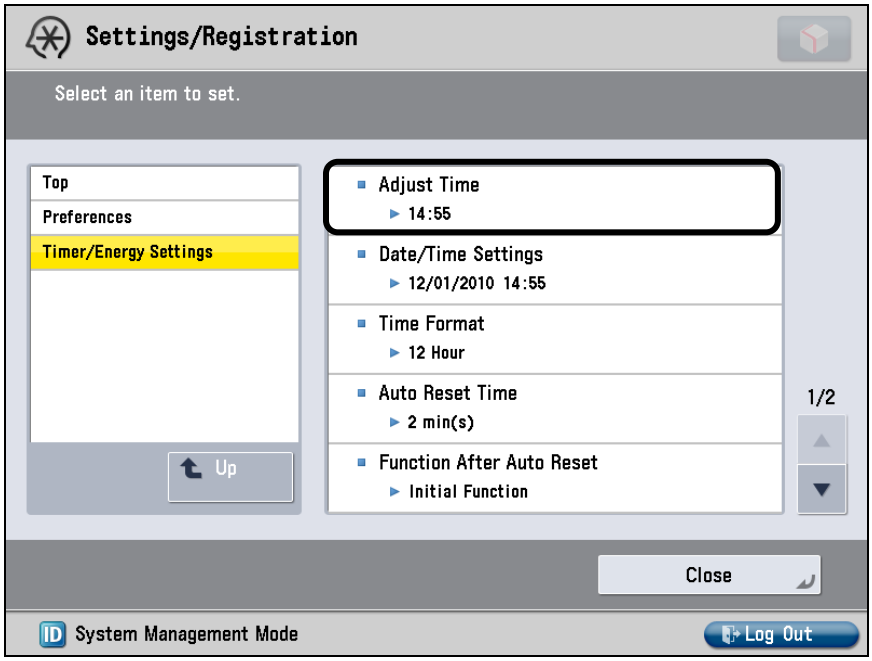
1. On the machine's control panel, press (Settings/Registration).
2. Press [Preferences].



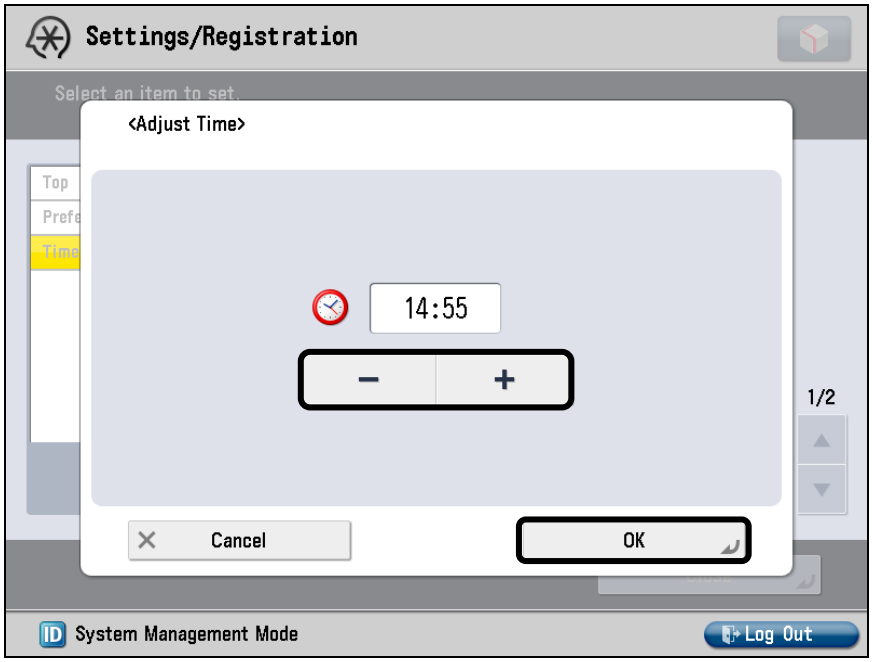
3. Press [Timer/Energy Settings].



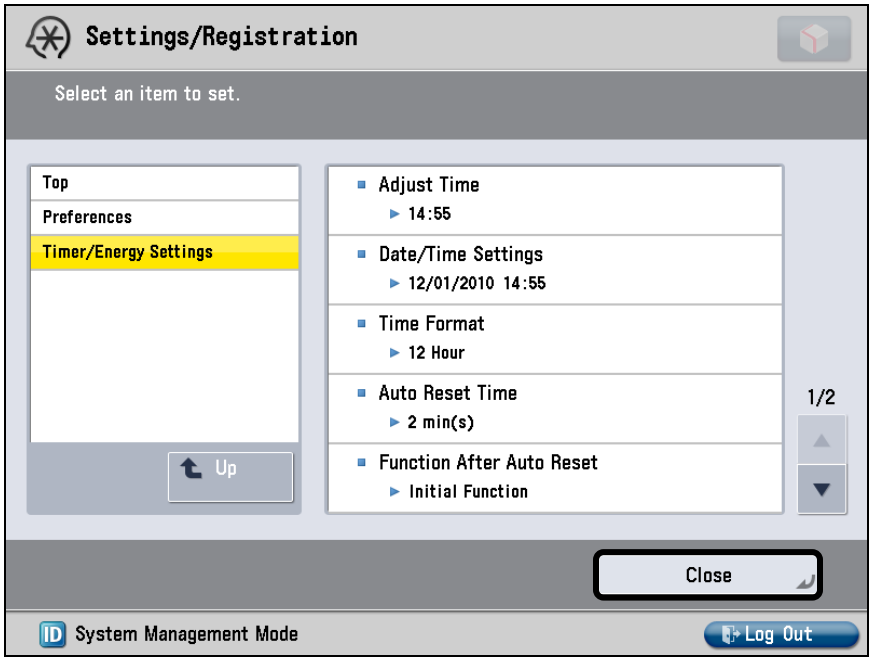
4. Press [Adjust Time].



5. Press [-] or [+] to adjust the time → press [OK].



6. Press [Close].



The Main Menu screen is displayed.

This page is intentionally left blank.

Chapter 4 Appendix: Configuring Authorized Send with Trusted Login Managers

This Appendix contains additional information for configuring Authorized Send to use Single Sign On with separate machine login managers.

4.1 Universal Login Manager

Single Sign On with ULM (Universal Login Manager) requires software installation, configuration, and credential verification to occur in a specific order. Follow the procedure below to enable ULM Single Sign On with Authorized Send.

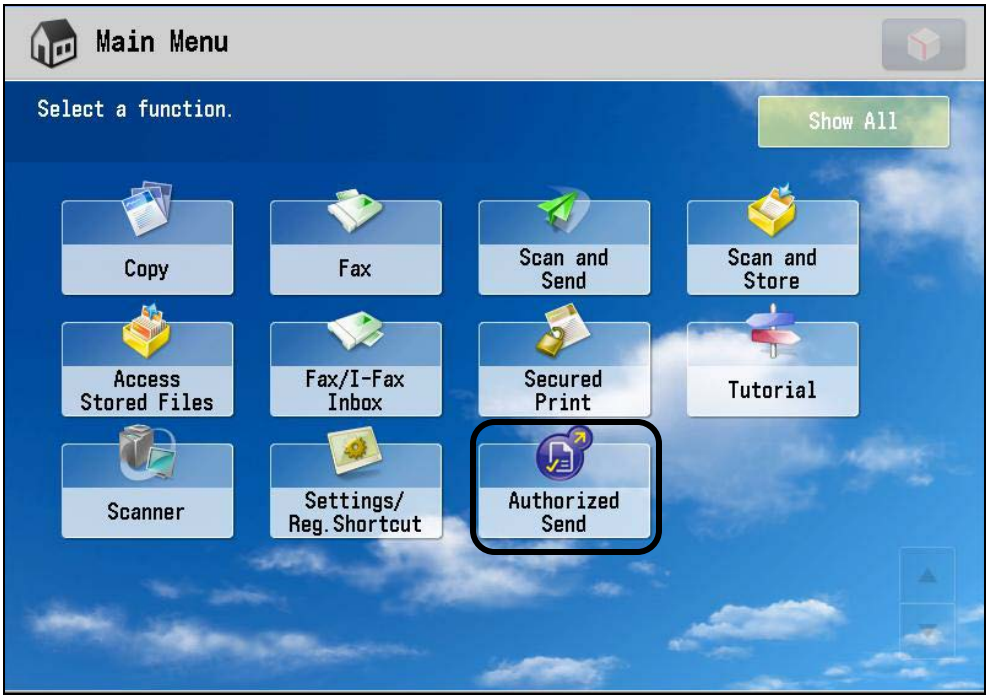
1. Install and configure ULM on the device. Refer to the ULM documentation for installation and configuration instructions.

2. Log in to the device via ULM to verify ULM allows access with valid credentials. Log out once you have verified ULM works properly. Refer to the ULM documentation for log in and log out instructions.

3. Install and configure Authorized Send. For Authorized Send installation instructions, refer to the *Authorized Send 6.4 Installation Guide*. For Authorized Send configuration instructions, refer to "Configuring Authorized Send".

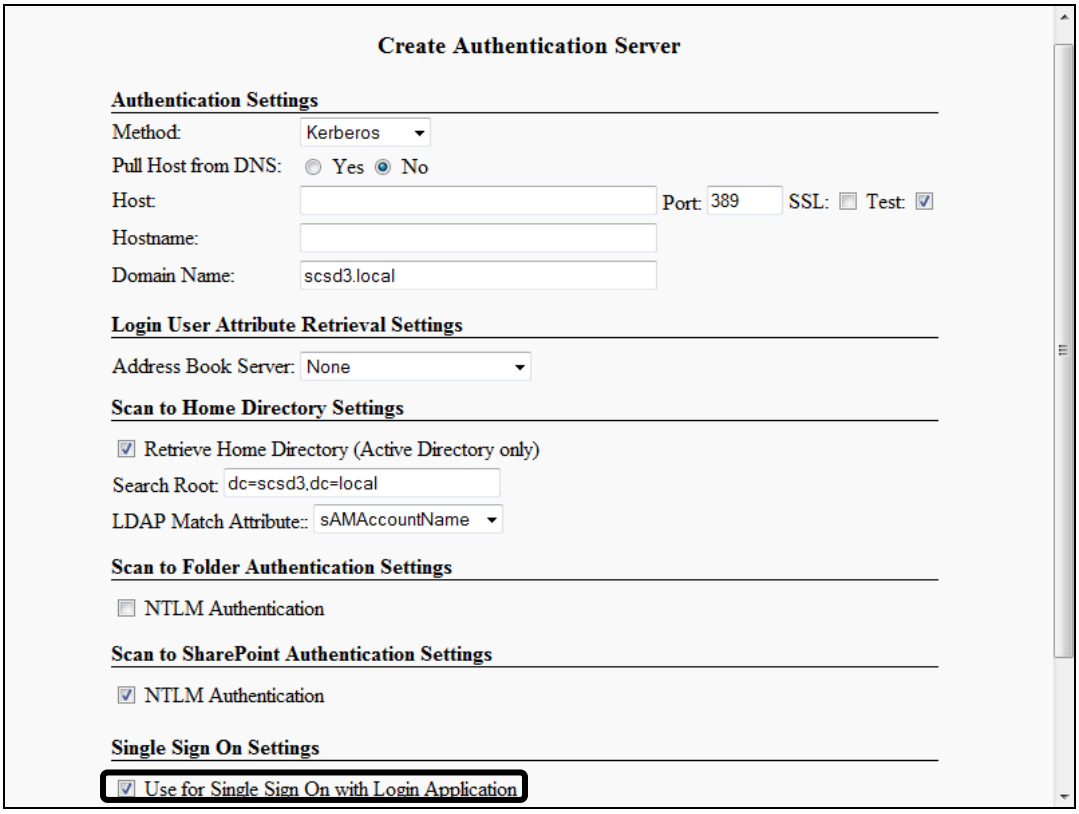
   Authorized Send should automatically retrieve the authentication domain and DNS information during installation. If Authorized Send did not retrieve the correct authentication information, refer to "Creating an Authentication Server," and "Editing an Authentication Server," for Authentication Server configuration instructions.

4. Log in to the device → start and sign in to Authorized Send to verify Authorized Send allows access with valid credentials. For Authorized Send start and sign in procedures, refer to the *Authorized Send 6.4 User's Guide*.



5. On a separate computer with local network access, access the Authorized Send configuration servlet → edit the current Authentication Server profile. For information on accessing the configuration servlet, refer to "Logging On to Authorized Send," on page 32. For information on editing the Authentication Server profile, refer to "Editing an Authentication Server," on page 59.

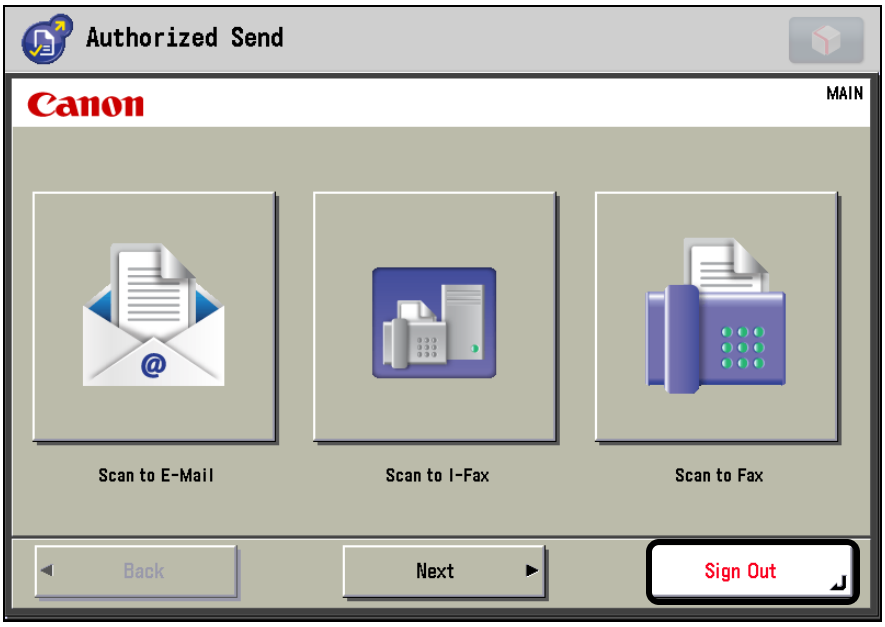
6. Enable the [Use for Single Sign On with Login Application] option in the servlet and click [Update] if you updated an existing server profile, or [Create] if you created a new server profile. The Authorized Send servlet automatically signs you out of the Authorized Send application on the device.



7. Log out of ULM on the device.

8. Log in to ULM on the device → sign in to Authorized Send.

9. Sign out of Authorized Send → log out of ULM. For Authorized Send sign out procedures, refer to the *Authorized Send 6.4 User's Guide*.



10. Log in to ULM on the device → start the Authorized Send application.

    Authorized Send now uses the ULM credentials for Single Sign On. No Authorized Send sign in screen appears for future Authorized Send sessions when you log in to the machine using the ULM credentials.