Canon

Authorized Send

Installation and Configuration Guide

Version 3.5

meap POWERED BY

08011-35-UD2-004

This page is intentionally left blank.

Contents

Preface

Thank you for purchasing the Authorized Send software application. Please read this manual thoroughly before operating the product on your MEAP-enabled device 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). This manual does not provide instructions for using or operating the Authorized Send application. For instructions on using the Authorized Send application, see the *Authorized Send User's Guide.*

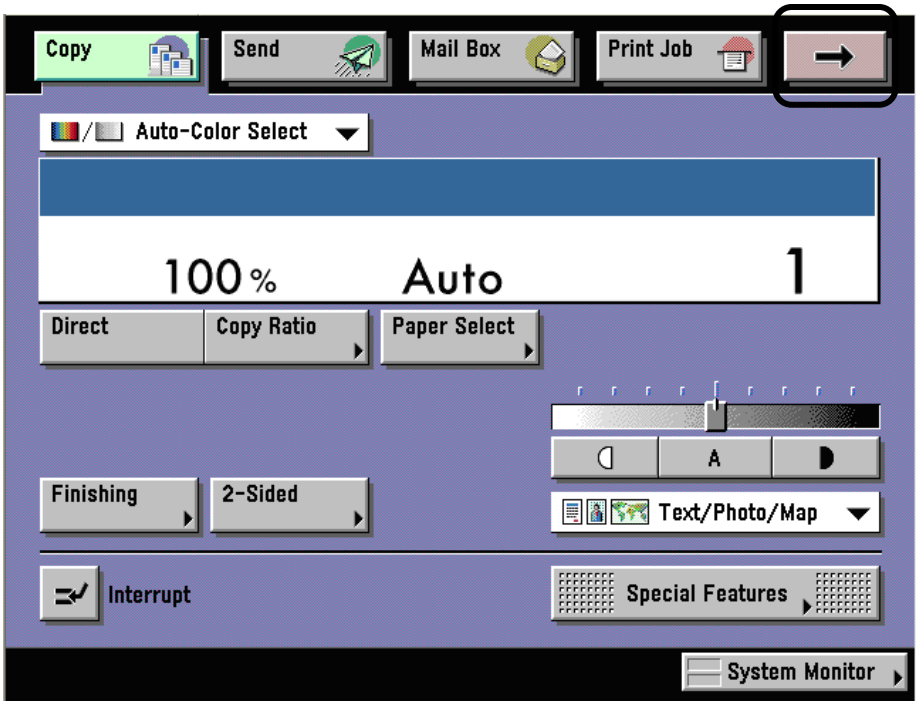
Symbols Used in This Manual

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.

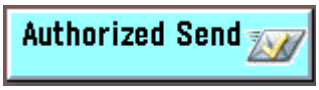
Keys and Buttons Used in This Manual

Keys for using the machine's main functions are located on the top of the touch panel display. To use any of the desired function's features, you must first press the key or application tab for the desired function. Press [→] (arrow key) to access installed MEAP applications.



On the MEAP Application screen, there may be several application tabs that you can select. Select only the proper tab for the application that you want to use.

The application tab for Authorized Send is:



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:	[Key Name]
Examples:	[Install] [OK]

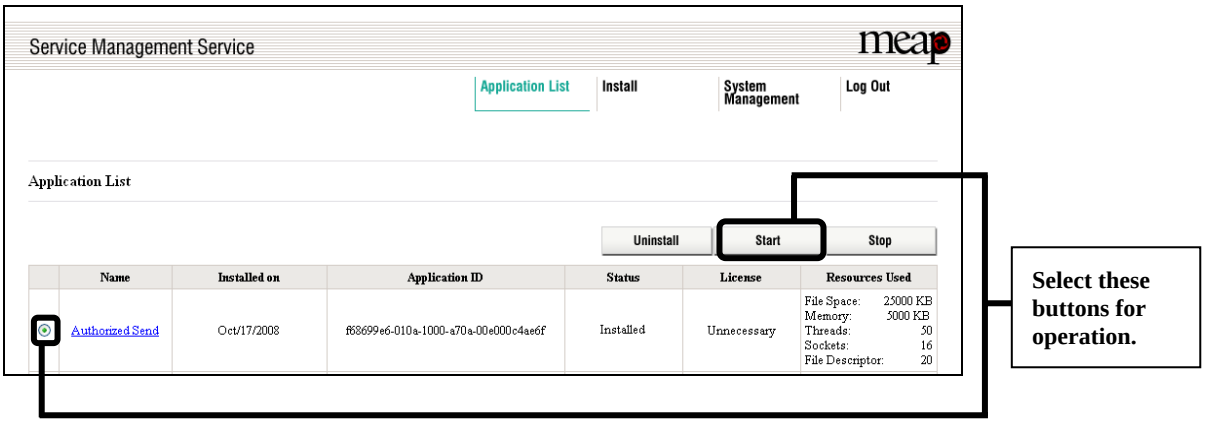
Displays Used in This Manual

Most screen shots used in this manual are those taken when Authorized Send is being installed using MEAP SMS (Service Management Service), or when Authorized Send is running on the Color imageRUNNER 5185, unless otherwise specified.

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. Select the [Authorized Send] radio button → click [Start].



Abbreviations Used in This Manual

The following abbreviations are used in this manual.

Abbreviation	Definition
AD	Active Directory
ADF	Automatic Document Feeder
DFS	Distributed File System
DN	Distinguished Name
FQDN	Fully Qualified Domain Name
KDC	Key Distribution Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MEAP	Multifunctional Embedded Application Platform
MFP	Multifunctional Printer
NTLM	NT LAN Manager
UI	User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
SMTP	Simple Mail Transfer Protocol
SPN	Service Principal Name
SSL	Secure Sockets Layer

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, "Overview," on p. 11.

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

Legal Notices

Trademarks

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

Windows is a registered trademark of Microsoft Corporation in the United States and is a trademark or registered trademark of Microsoft Corporation in other countries.

Java and all Java-based trademarks and logos are the trademarks or registered trademarks of Sun Microsystems, Inc. in the United States or other countries.

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

Copyright

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 OF 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 Overview

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 Canon imageRUNNER machines that enables the development of custom applications, which run alongside native imageRUNNER functions, such as Copy, Print, and Scan.

MEAP, developed by Canon, is based on Sun Microsystems' Java and Java 2 Micro Edition technology.

"MEAP device" is the MEAP-enabled Canon imageRUNNER that is running the Authorized Send application. It may also be referred to as "MEAP imageRUNNER" or "machine."

Authorized Send is designed to perform the following functions once configured from the Authorized Send configuration servlet:

- Authenticate against an LDAP server.
- Authenticate to an Address Book server anonymously.
- Retrieve a user's e-mail address and home directory.
- Search the LDAP address book server for e-mail addresses.
- Browse a network for valid share folders.
- Provide the ability to configure preset shares.
- Scan and send a document to a valid e-mail address, networked folder, or fax server.
- Enables an Administrator to control the features that are available to a user.
- Enables an Administrator to set default values for the Scan to E-Mail function.
- If activated, enables the use of the Searchable PDF, Encrypted PDF, and Compact PDF modes.
- Logs error and debugging information that is generated by the application to your local hard drive and to optional remote Syslog servers.
- Scan in the PDF, TIFF, TIFF (Single), and JPEG file formats.
- Create folders that do not exist dynamically (in particular, using the user's User Name).

- Authenticate to a separate domain when scanning to a folder.
- Provide the ability to use NTLM Authentication for Scan to Folder, regardless of the authentication method used.
- Provide the ability to dynamically locate the closet available domain controller within the domain, and cache that domain controller until it becomes no longer available.
- Provide the ability to populate the User Name field from a login application.
- Authenticate to a separate SMTP Server.

IMPORTANT

- Basic knowledge of networking and imageRUNNER machines is necessary to install and configure the Authorized Send application.
- For instructions on using Authorized Send, see the *Authorized Send User's Guide.*

1.1 System Requirements

Authorized Send requires the proper installation and configuration of all items documented in this guide. Failure to correctly install or configure the application will 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 chapters (including Chapter 5, "Troubleshooting," on p. 123) before contacting Canon U.S.A.'s e-Support.

1.1.1 Hardware Requirements

Authorized Send is designed to operate on the following imageRUNNER or Color imageRUNNER machines using the minimum specified MEAP Contents version.

Device Family	MEAP Contents
imageRUNNER 2270/2870/3570/4570	32.02
imageRUNNER 8070/9070/85+/105+	11.03
imageRUNNER 5570/5070/6570	35.02
imageRUNNER C3170	20.25
imageRUNNER 7105/7095/7086	35.02
imageRUNNER C6870/C5870	11.03
imageRUNNER C5180/C4580/C4080	20.05
imagePRESS C1	1.08
imageRUNNER C3380/C2880	10.02
imageRUNNER 3025/3030/3035/3045	10.05
imageRUNNER 5075/5065/5055	10.04
imageRUNNER C5185/C5180/C4580/C4080 (Version up)	65.13
imageRUNNER C3380/C2880 (Version up)	60.06
imagePRESS C7000VP/C6000VP/C6000	10.07
imageRUNNER C5058/C5068	60.13
imageRUNNER 5055/5065/5075 V2	30.04
imageRUNNER 5050	30.04
imageRUNNER 7086/7086N/7086B/7095/7095P/7105/7105B V2	55.03
imageRUNNER C2550/C3480	75.45
imageRUNNER 3225/3230/3235/3245	21.06

IMPORTANT

- MEAP and Use HTTP settings (from the Additional Functions screen) on the MEAP device must be enabled. (See the *Reference Guide* that came with your machine.)
- Access to System Manager Settings (from the Additional Functions 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.
- Inbox 99 on the MEAP device must be available for use, and without password protection.

1.1.2 Server Requirements

Authorized Send communicates with the following servers:

- Supported authentication servers:
  - Windows 2000/2003 Active Directory
  - Lotus Domino Version 7
  - Novell NetWare 6.5/eDirectory 8.7 SP1
- Supported address book servers:
  - Windows 2000/2003 Active Directory
  - Lotus Domino Version 7
  - Novell NetWare 6.5/eDirectory 8.7 SP1
- Supported name servers:
  - Windows 2000/2003 DNS server
- Supported Scan to E-Mail servers:
  - Microsoft Exchange Server 2000/2003
- Supported Scan to Network Share servers:
  - Windows Vista/XP/2000/2003 Local Share
  - Windows Vista/XP/2000/2003 Domain Share
  - Windows DFS (Distributed File System) Share
    - Windows Vista/XP/2000/2003
- The following fax servers have been tested:
  - Relay Fax 6.7 by ALT-N Technologies

1.1.3 Software Requirements

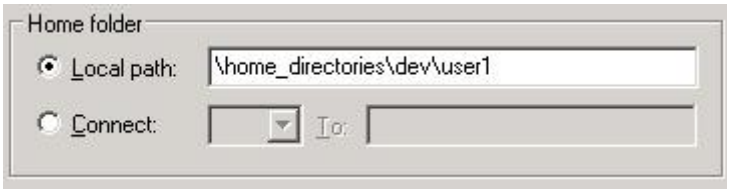
Microsoft Internet Explorer 6.0 or later must be installed and configured prior to installing the Authorized Send application.

1.1.4 Home Directory Requirements

If the Administrator wants to configure the "Create Pre-Set Share to Home Directory (Active Directory only)" feature, the following three types of configurations are supported.

- **Local Share**

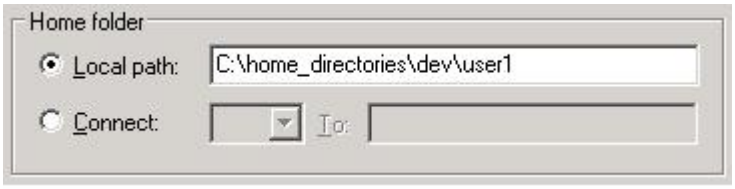
  This configuration illustrates when the home directory exists on the authentication server as a local share. No text manipulation is required, and the value entered is used exactly as is.



Home Directory as a Local Share

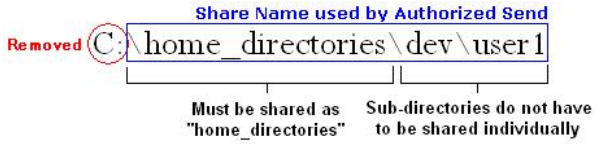
- **Local Path**

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



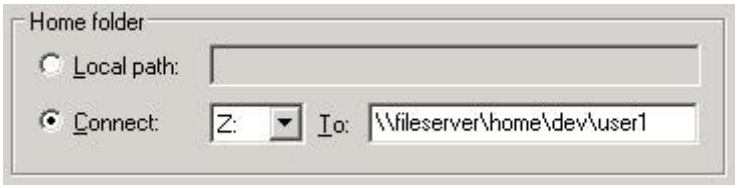
Home Directory as a Local Path

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

1.1.5 Distributed File System Requirements

Authorized Send supports the following two DFS (Distributed File System) roots.

- **Stand-alone 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. End 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 (Fully Qualified Domain Name).

  IMPORTANT
  If the authentication server is configured with a NetBIOS domain name, access is granted to the application; however, you will not be able to access 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 end user will not be able to scan to the DFS root.

1.1.6 Communication Interfaces

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

Communication Interface	Port	Description
NTLM	Determined by AD server	Used for authentication.
Kerberos	TCP Port 88	Used for authentication.
LDAP	TCP Port 389	Used to retrieve e-mail addresses.
SMB	TCP Port 445	Used for the Scan to Folder function.
SMTP	TCP Port 25	Used for the Scan to E-mail function.
HTTP	TCP Port 8000	Used to access the administration Web page.
HTTPS	TCP Port 443	Used to access the secure administration Web page.
SSL	TCP Port 636	Used to communicate with the LDAP server.

1.1.7 Supported Authentication Protocols

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

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 Operating 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.

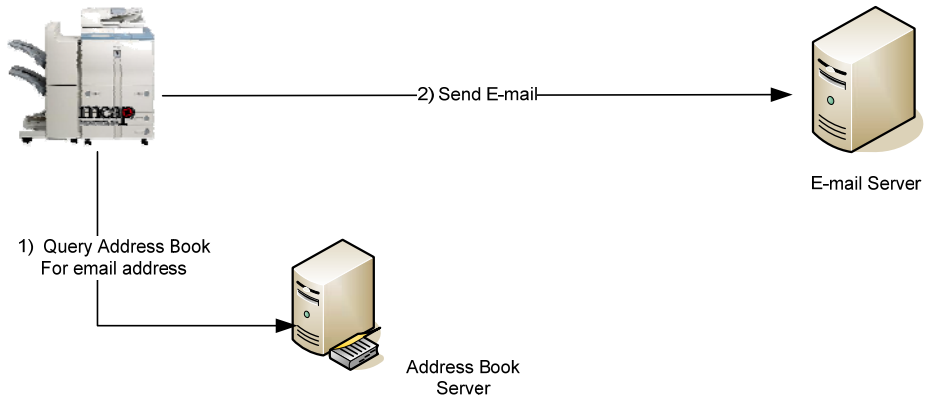
Supported Authentication Servers	Authentication Methods
Windows Active Directory	NTLM, Kerberos (with or without SSL)
Novell NetWare 6.5/eDirectory 8.7 SP1	Simple LDAP (with or without SSL)
Lotus Domino v7	Simple LDAP (with or without SSL)

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 SP1	Simple LDAP (with or without SSL)
Lotus Domino v7	Simple LDAP (with or without SSL)

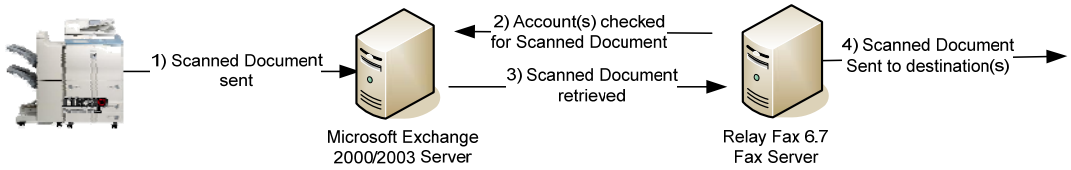
The following illustrations represent a flow of operations for the Scan to E-Mail, Scan to Fax, and Scan to Folder functions of the Authorized Send application.

Scan to E-Mail



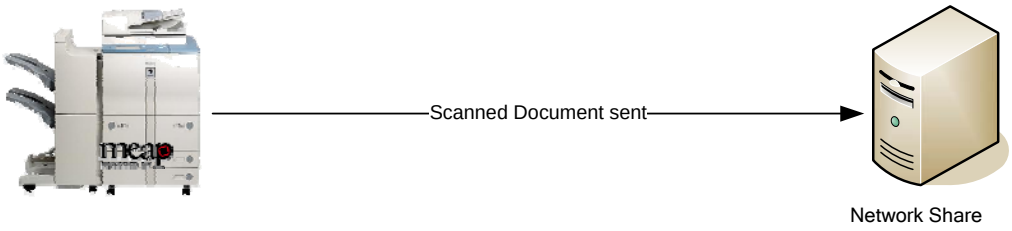
1. The user makes an Address Book query from the Scan to E-mail function on the MEAP machine. The machine sends an LDAP query to the Address Book server to retrieve the desired list of e-mail addresses.
2. Once all e-mail addresses are verified and selected, the machine sends the e-mail message to the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

Scan to Fax



1. The user manually inputs the recipient's fax number.
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

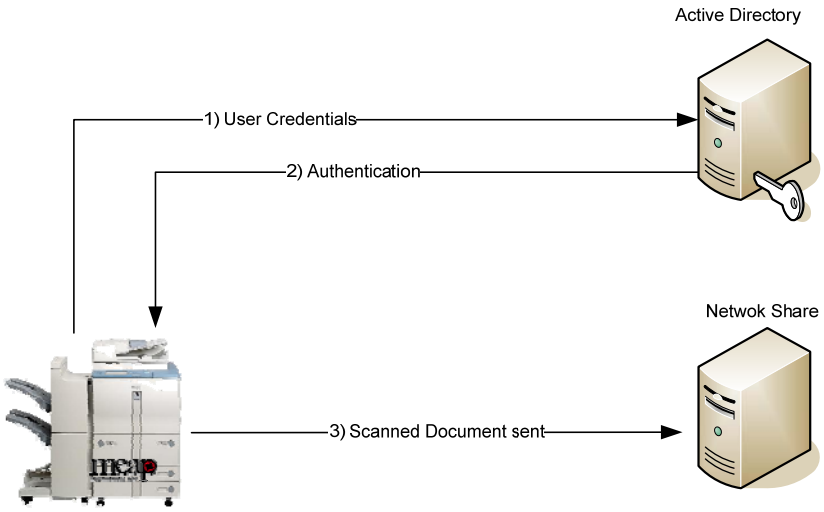


1. The user browses for the desired folder on the file server directly from the machine.
2. Once the directory is found and selected, the machine sends the file to the designated location on the file server.

NOTE

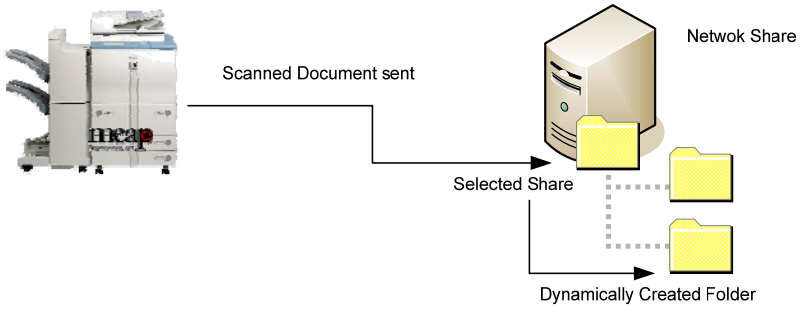
When a user accesses a network share, they are authenticated against that share using their credentials. If they do not have access rights to that share, they will be prompted to enter a user name and password.

Scan to Folder with NTLM Authentication



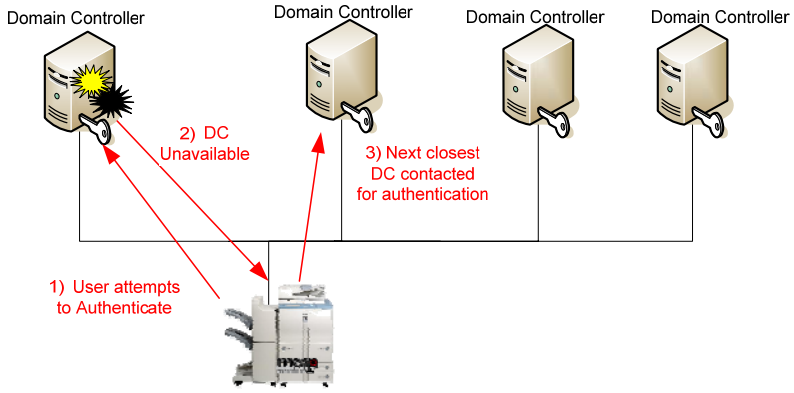
1. The user logs on to the machine using one of the authentication methods.
2. The user browses and enters their credentials to gain access to a network shared folder using NTLM as the authentication method.
3. Once access is granted, the scanned document is stored in the selected folder.

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



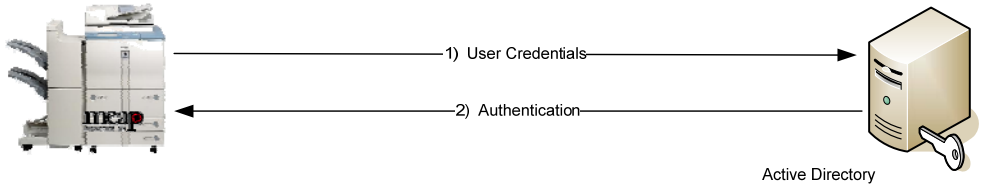
1. The user tries to log on to the machine using one of the authentication methods.
2. The system is unable to contact the authentication server previously cached.
3. The system locates the next closest available domain controller.
4. Authentication or Address Book lookup is performed by the new domain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

1.2.1 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.

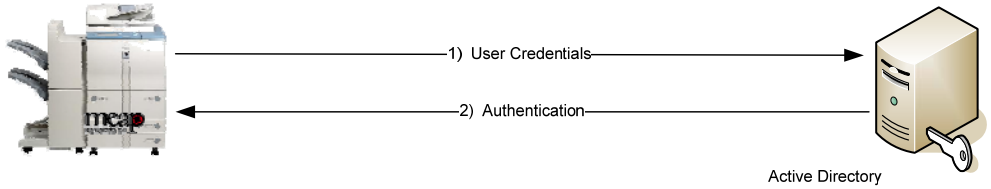
1.2.1.1 Authentication Communication Diagrams

Kerberos Authentication



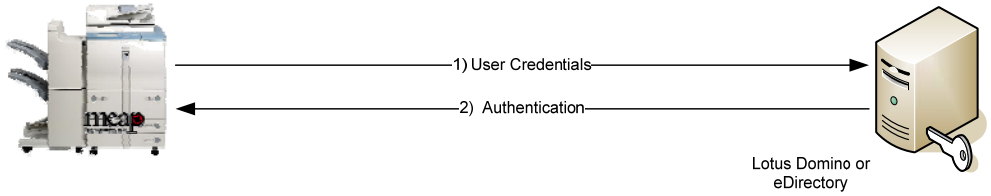
Communication Protocol LDAP/Kerberos

NTLM Authentication



Communication Protocol LDAP/NTLM

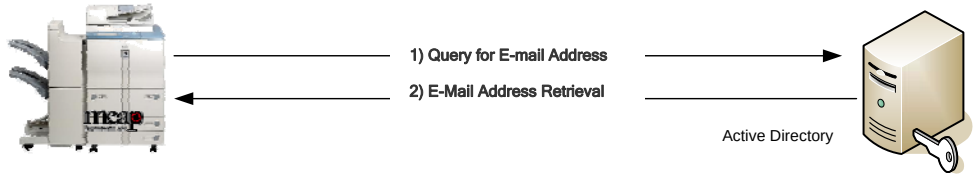
Simple Authentication



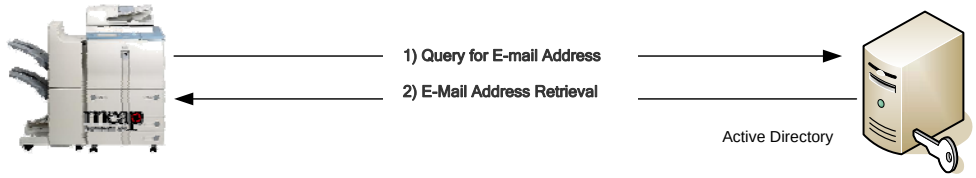
Communication Protocol LDAP/Simple

1.2.1.2 Address Book Communication Diagrams

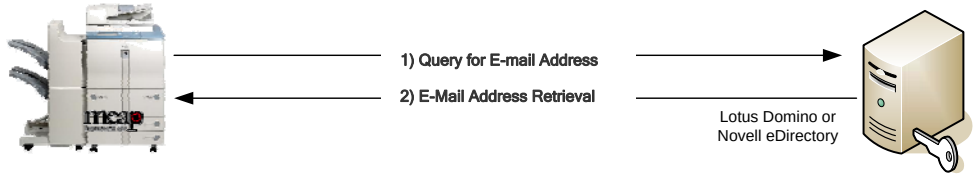
Kerberos Communication with an Address Book Server



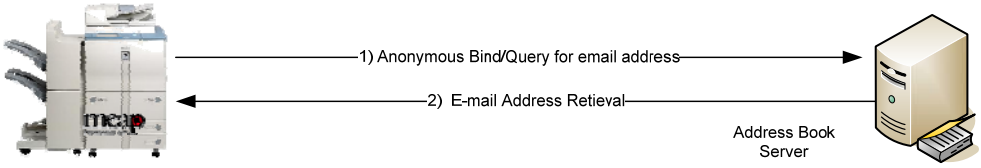
NTLM Communication with an Address Book Server



Simple Communication with an Address Book Server



Anonymous Bind Communication Using LDAP with an Address Book Server



Chapter 2 Installing Authorized Send

This chapter describes how to install Authorized Send on a MEAP-enabled machine using the MEAP SMS (Service Management Service) program.

The System Administrator for the target MEAP device is best suited for installing the Authorized Send application, using a networked computer that is connected to the Internet and the device.

Before installation, you must obtain the license file from www.canon.com/Meap, and have the IP address of the MEAP-enabled device.

IMPORTANT

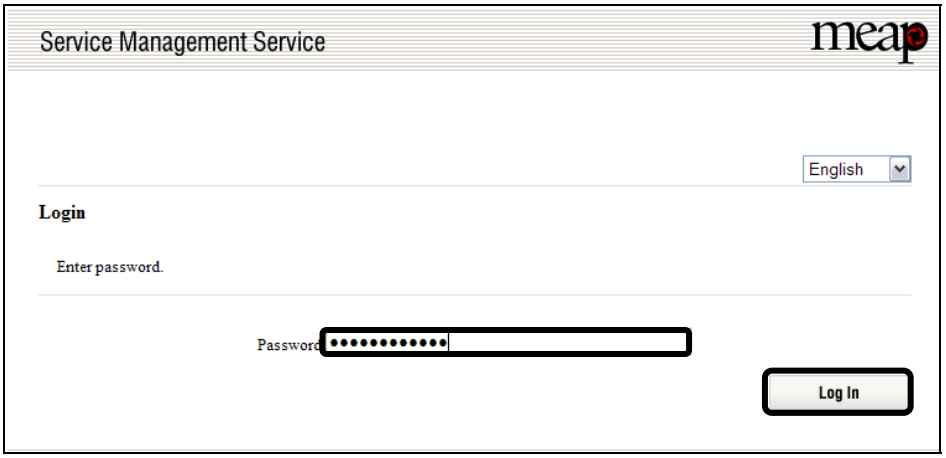
- This chapter describes the procedure for a new installation of Authorized Send Version 3.5. If you want to upgrade from Authorized Send 2.*x*, you must uninstall the application, and then install the new version. However, if you want to upgrade from Authorized Send 3.*x* to Authorized Send 3.5, you only have to stop the previous version, and then install the new version.
- Do not use the browser's [Back] and [Forward] buttons during the installation process. Only use the clickable links in the browser's window.
- For more information on using SMS or uninstalling MEAP applications, see the *MEAP SMS Administrator Guide* that came with your MEAP-enabled device.

---

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

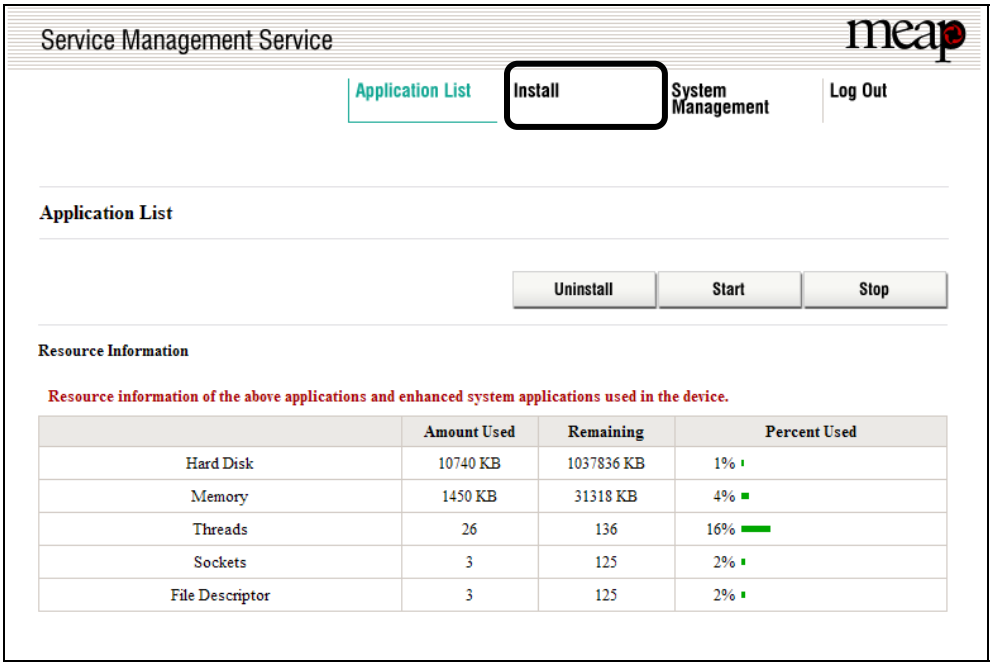
   http://<device IP>:8000/sms
   https://<device IP>:8000/sms (if you are using SSL for communications)
   (Replace <device IP> with the IP address of the MEAP device.)

2. Enter **MeapSmsLogin** in [Password] → click [Log In].



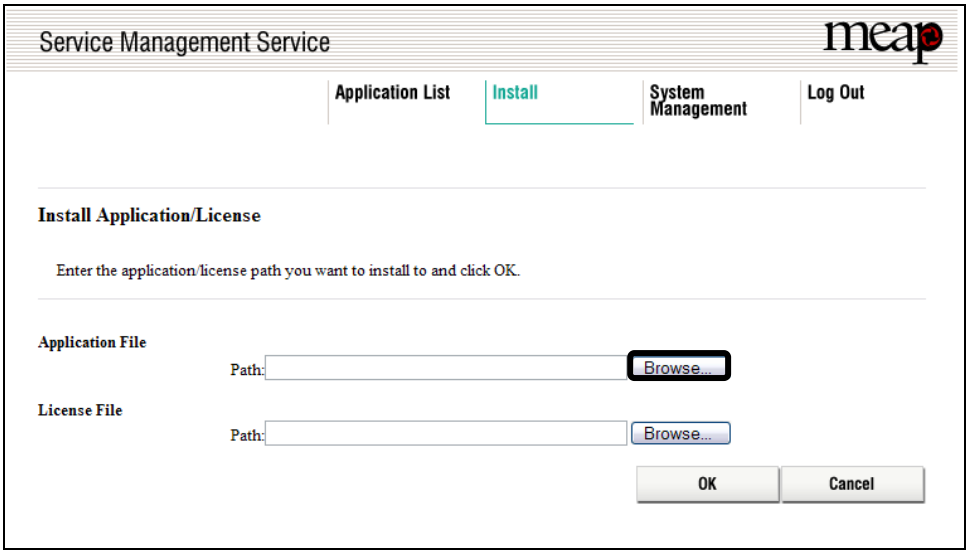
The SMS Application List screen is displayed.

3. Click the [Install] tab.



The SMS Install Application/License screen is displayed.

4. Under <Application File>, click [Browse] to the right of Path.

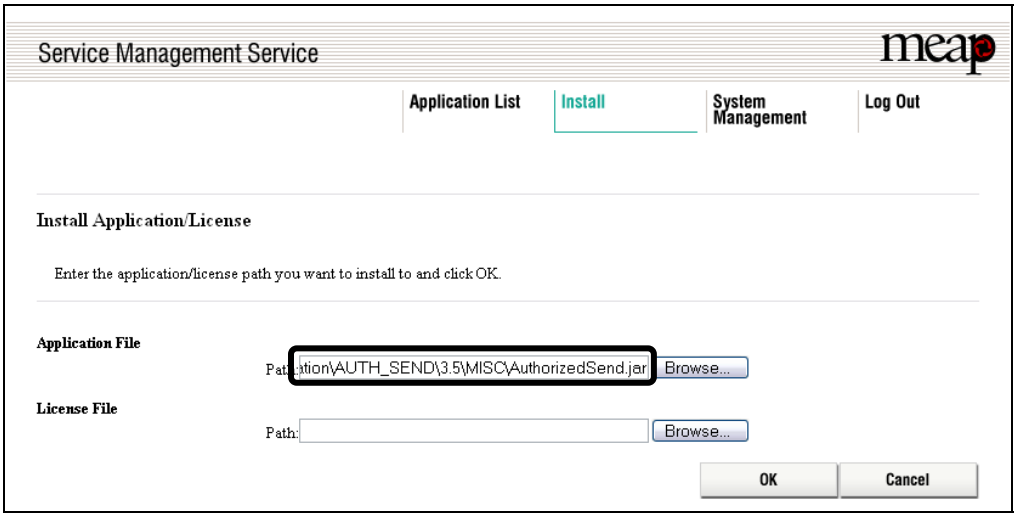


5. Navigate to the drive or directory containing the Authorized Send .jar file → select the file → click [Open].

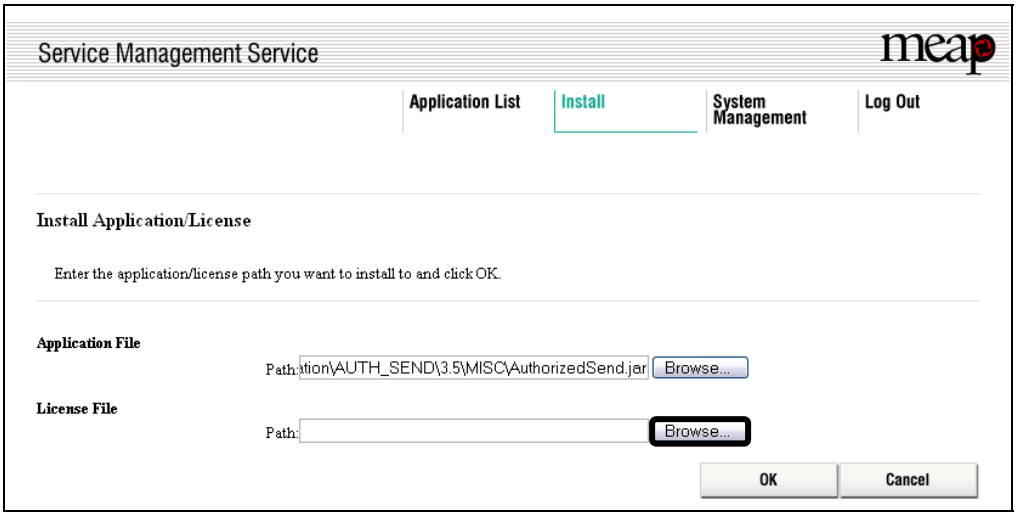
IMPORTANT

Make sure that you select the file that ends with the .jar extension for the application file.

6. Verify that the correct file was selected.



7. Under <License File>, click [Browse] to the right of Path.



IMPORTANT

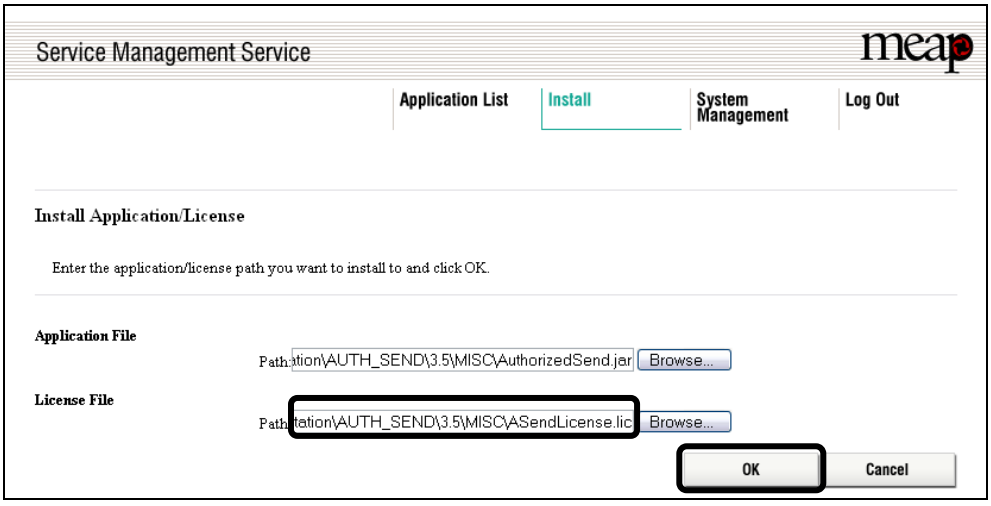
The license file must be downloaded from the LMS (License Management System) beforehand. For more information, contact your local authorized Canon dealer.

8. Navigate to the drive or directory containing the .lic file → select the file → click [Open].

IMPORTANT

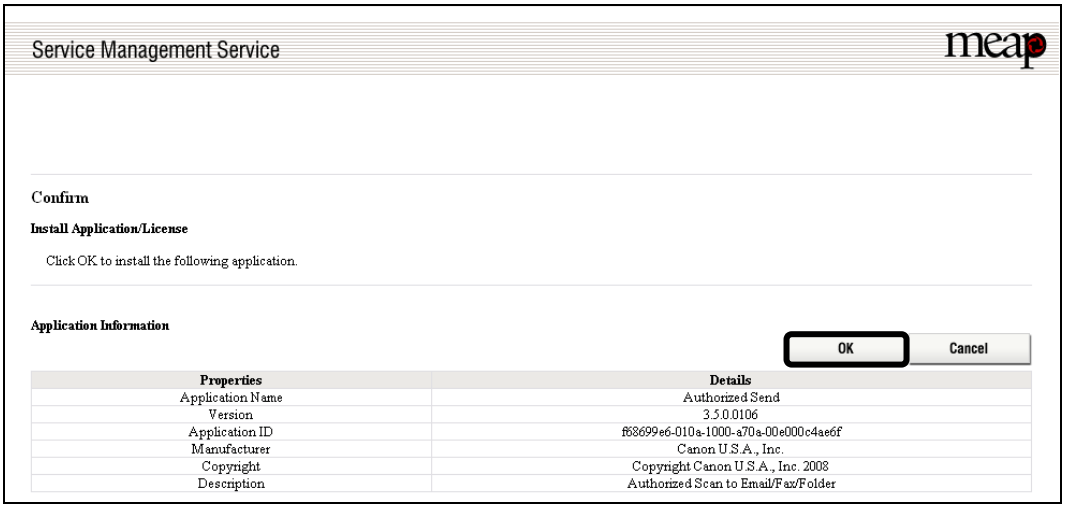
Make sure that you select the file that ends with the .lic extension for the license file.

9. Verify that the correct file was selected → click [OK].



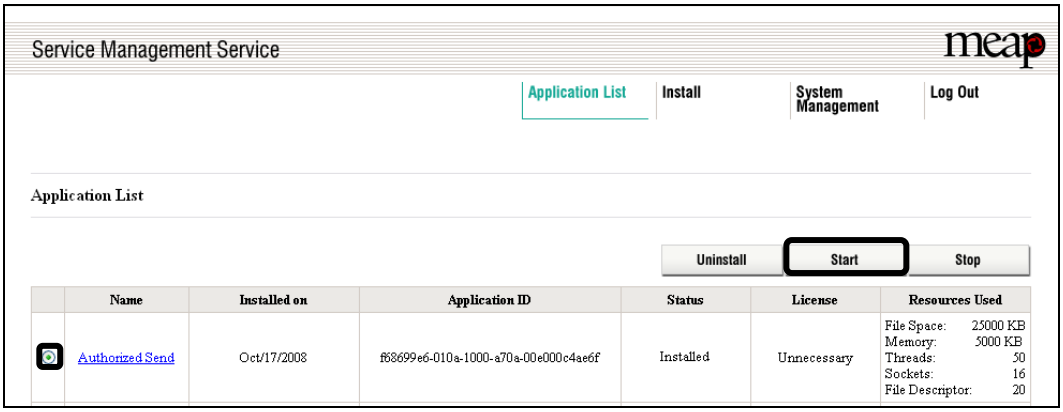
The SMS Confirm Install Application/License screen is displayed.

10. Click [OK].



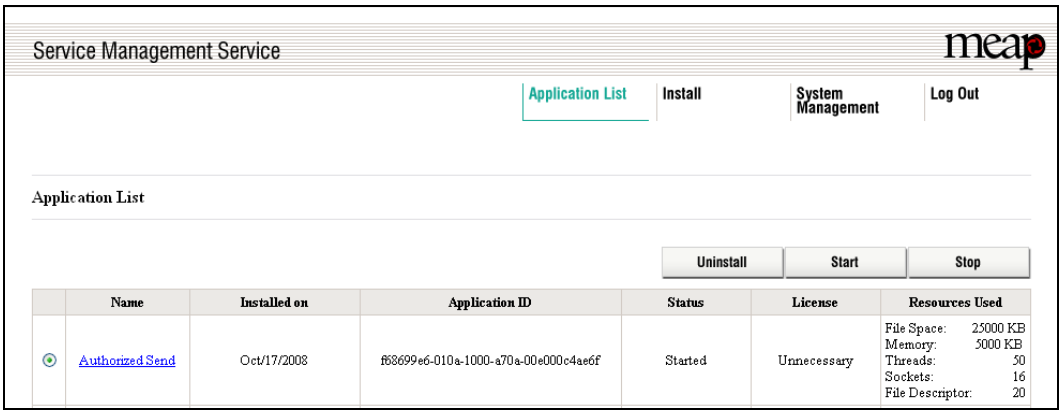
During installation, the message <Installing…Please wait a moment.> is displayed.

11. Click the [Authorized Send] radio button → click [Start].



Note that the status of the Authorized Send application is <Installed> before clicking [Start].

The status will change to <Started> if successful.



Installation is complete.

12. Click [Log Out] to exit SMS.

Chapter 3 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:	
General:	Configure an SMTP server.
Address Book:	Configure 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 Folder:	
General:	Configure the Scan to Folder settings.
Preset Shares:	Create preset folders for users to scan to.
Options:	Configure the optional settings.
Logs:	Configure the log settings, remote syslog servers, and download and view the logs.
About:	Display the Authorized Send version information.

3.1 Flow of Configuration Operations

From the Authorized Send Configuration screen, you can configure the settings necessary to use the Authorized Send application.

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

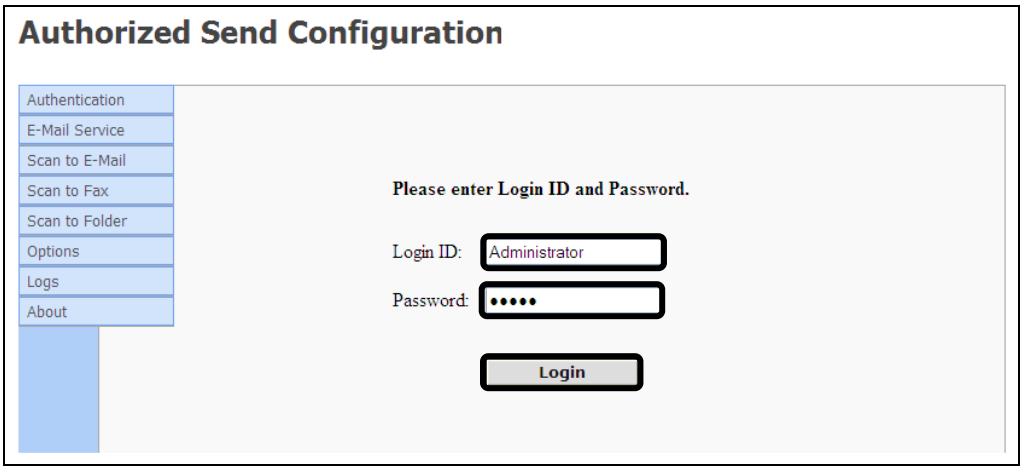
   http://<device IP>:8000/AuthSendConfiguration
   (Replace <device IP> with the IP address of the MEAP device.)

   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’.

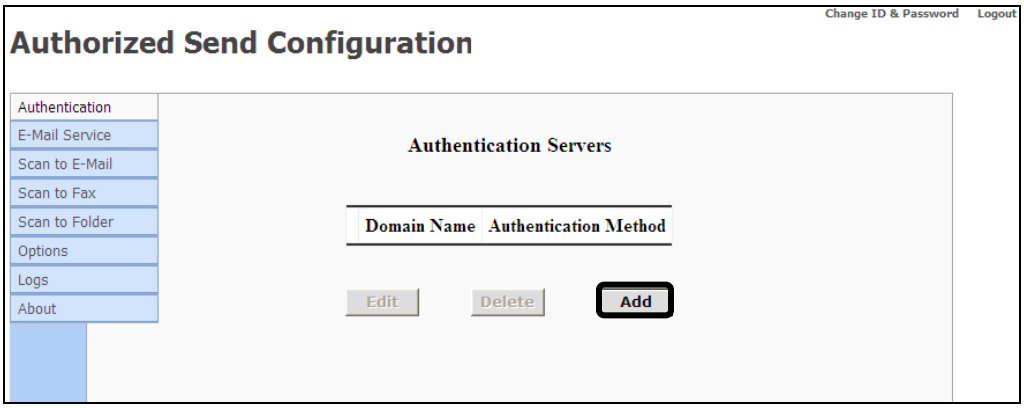


   The Authentication Servers screen is displayed.

IMPORTANT

   If you are using a temporary license and the license has expired, the message <The Authorized Send license has expired. Please contact your Canon dealer.> will be displayed. You must update your license file, or you will not be able to access the configuration servlet.

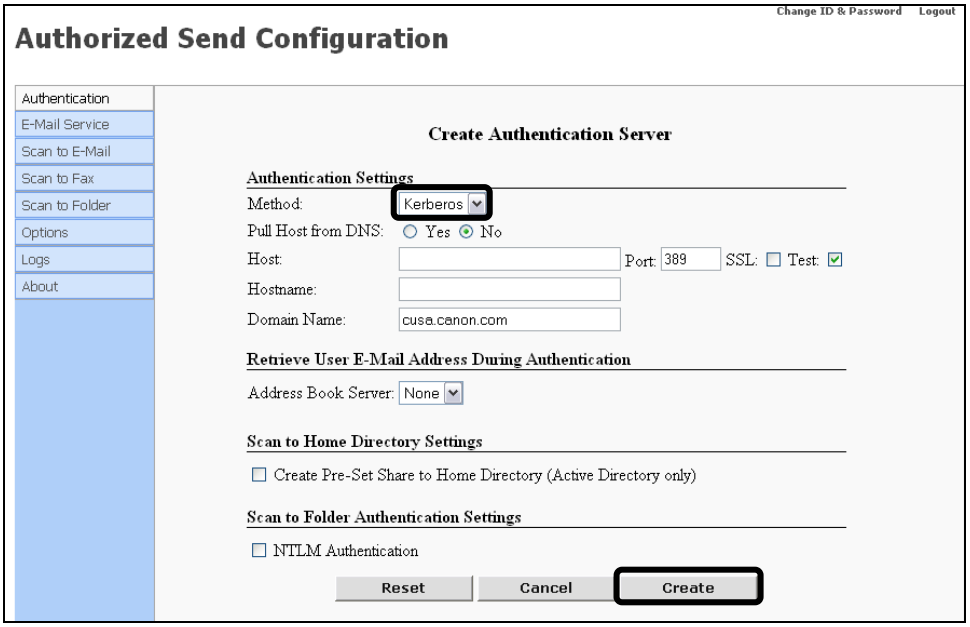
3. Click [Add].



   The Create Authentication Server screen is displayed.

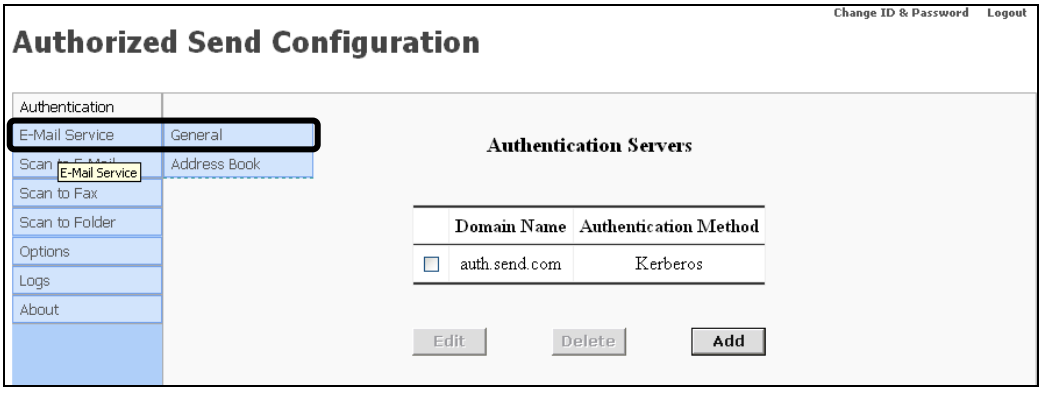
4. Select the authentication method → configure the settings based on the selected authentication method → click [Create]. (See "Creating an Authentication Server," on p. 44.)

   The available settings vary, depending on the selected authentication method.



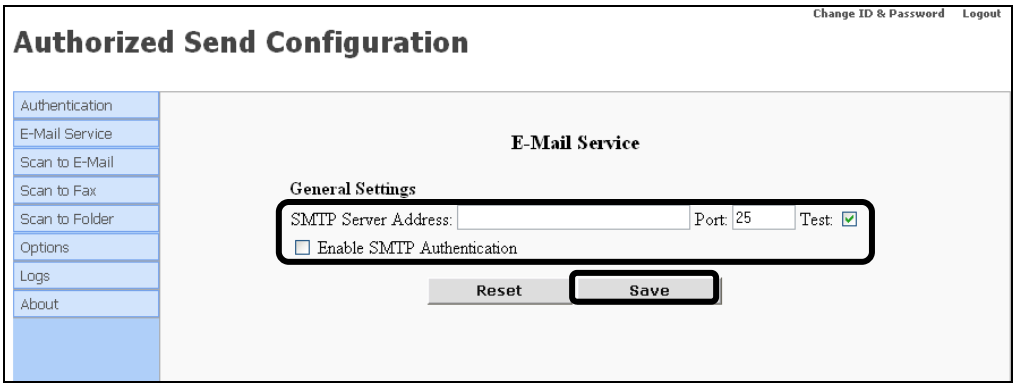
   The Authentication Server is created, and is added to the list on the Authentication Servers screen.

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



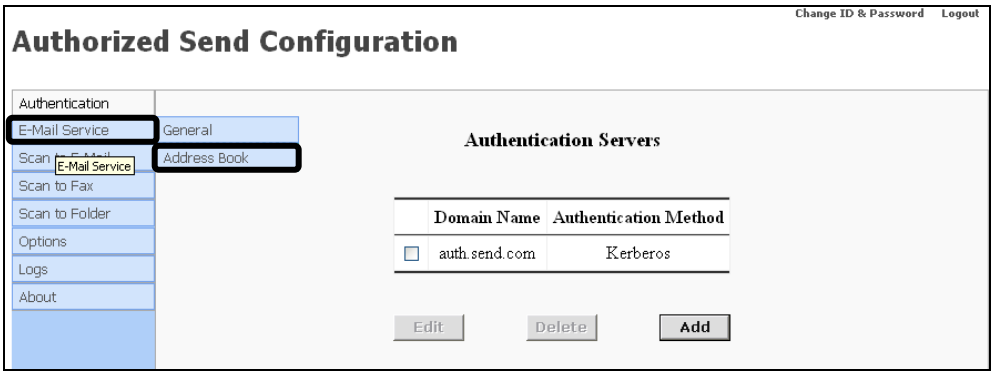
   The E-Mail Service screen appears.

6. Configure the settings under General Settings → click [Save]. (See "Configuring E-Mail Service Settings," on p. 55.)



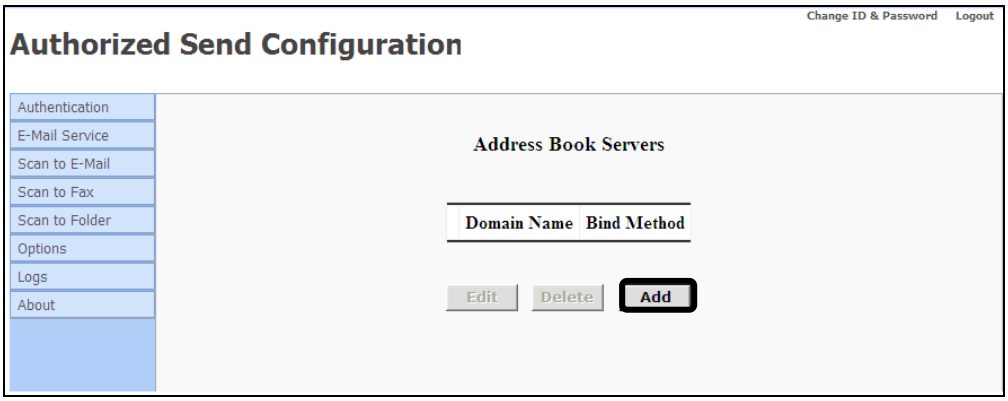
The Authentication Servers screen appears.

7. Click [E-Mail Service] → [Address Book].



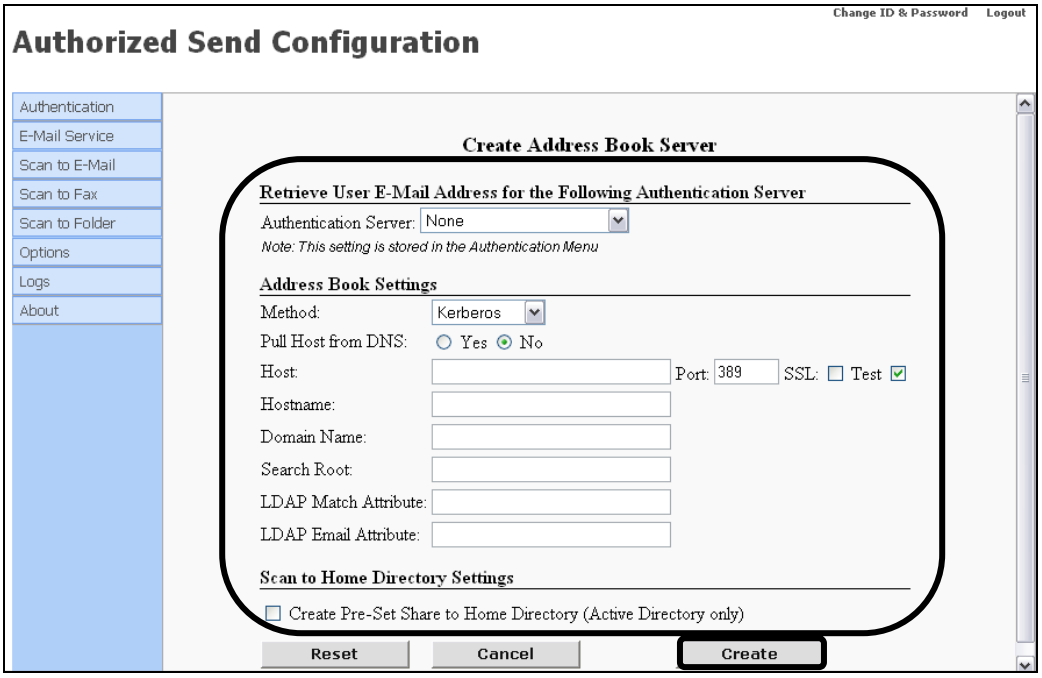
The Address Book Servers screen appears.

8. Click [Add].



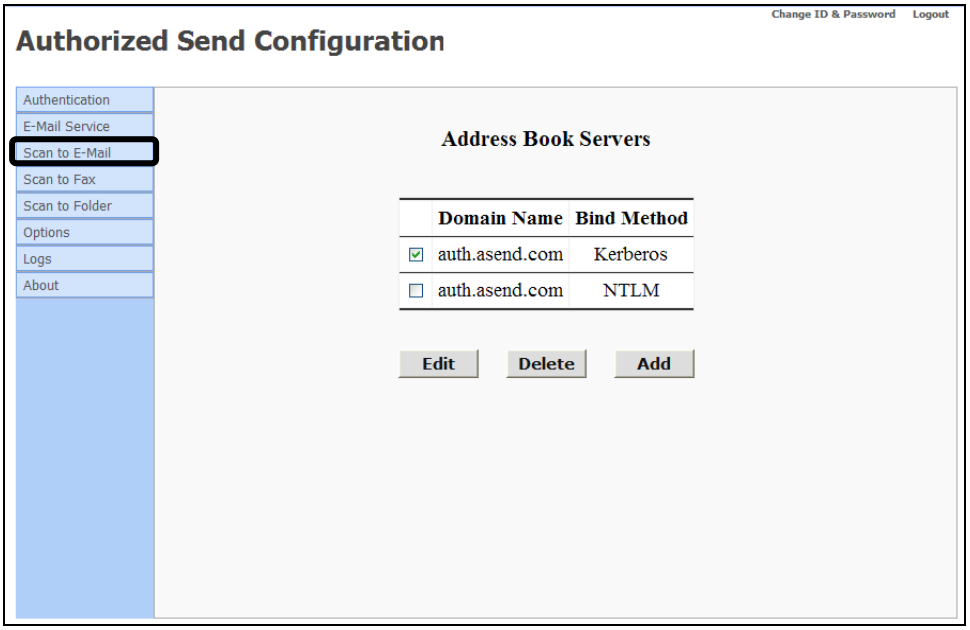
The Create Address Book Server screen appears.

9. Configure the settings on the Create Address Book Server screen → click [Create].



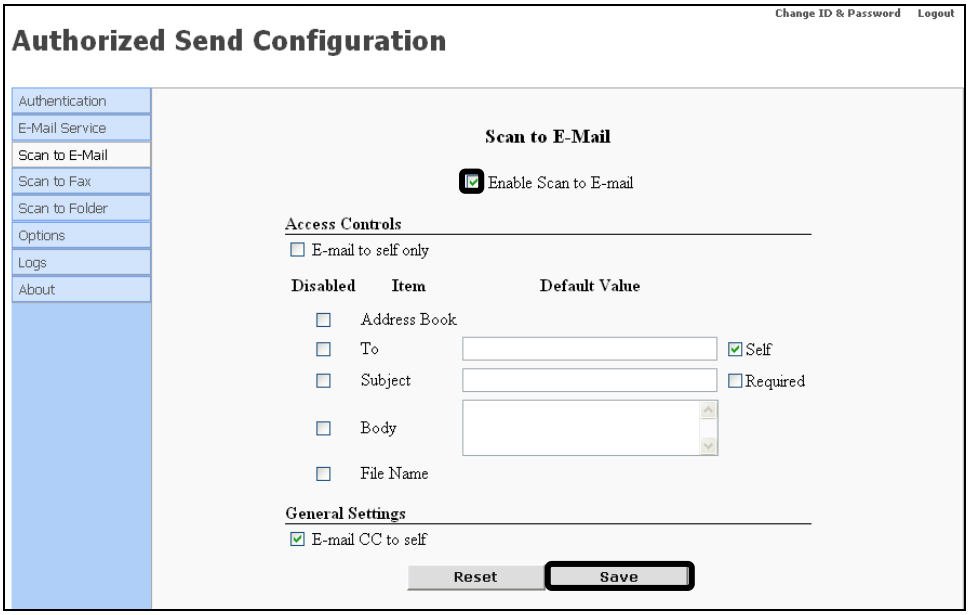
The Address Book Server is created, and is added to the list on the Address Book Servers screen.

10. Click [Scan to E-Mail].



The Scan to E-Mail screen appears.

11. Click the [Enable Scan to E-mail] check box → click [Save].



If you want to restrict the user to only send e-mail messages to themselves, select the [E-mail to self only] check box.

If you want to restrict access to the Address Book or the [To], [Subject], [Body], or [File Name] text boxes on the SCAN TO EMAIL screen, select the respective check boxes in the <Disabled> column.

If you want to restrict the [To] field to only show the user's e-mail address, select the [Self] check box.

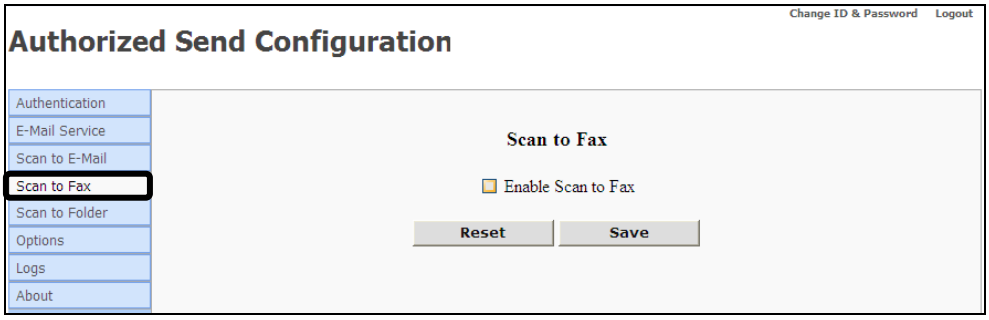
If you require that the [Subject] field is always populated, select the [Required] check box.

You can set up default recipients, subjects, and body text by entering their default values in the [To], [Subject], and [Body] text boxes in the <Default Value> column.

If you want to send a copy of the scanned document to the e-mail address registered to your user account, select the [E-mail CC to self] check box.

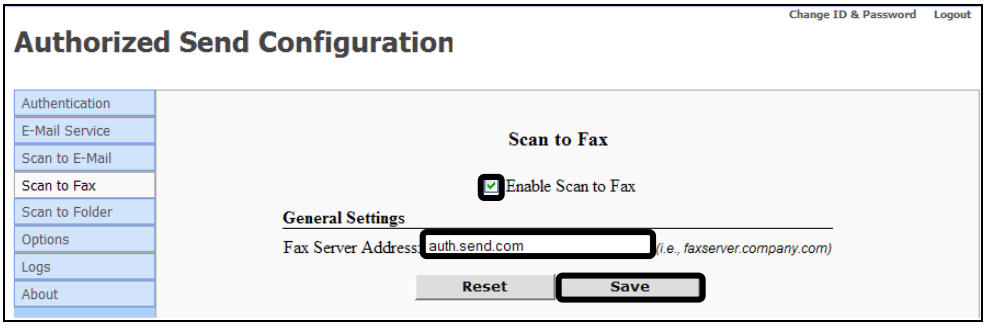
A message appears, informing you that the settings have been saved.

12. Click [Scan to Fax].



The Scan to Fax screen appears.

13. Click the [Enable Scan to Fax] check box → enter the fully qualified domain name of the e-mail server for faxing in [Fax Server Address] → click [Save].

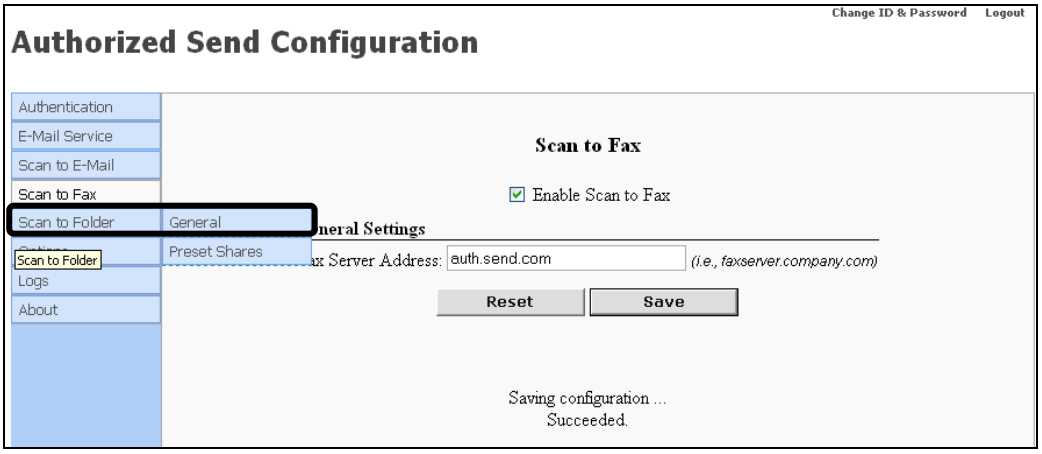


A message appears, informing you that the settings have been saved.

NOTE

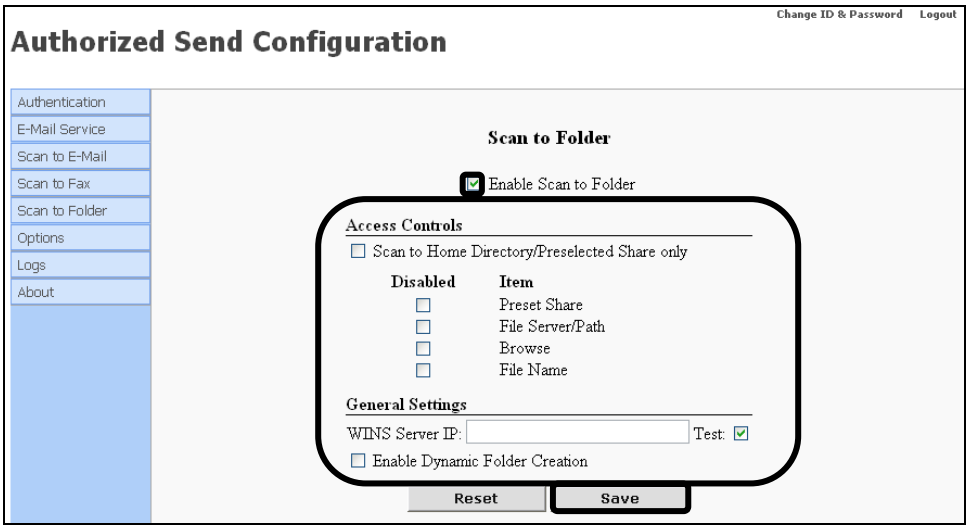
The Scan to Fax function is disabled by default.

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



The Scan to Folder screen appears.

15. Select the [Enable Scan to Folder] check box → configure the Scan to Folder Access Controls → enter the IP address of the NetBIOS name server in [WINS Server IP] → click [Save].



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

If you want to manually restrict user access to the Preset Share drop-down list, File Server and File Path text boxes, the Browse button, or File Name text box on the SCAN TO FOLDER screen, select the [Preset Share], [File Server/Path], [Browse], or [File Name] check boxes in the <Disabled> column.

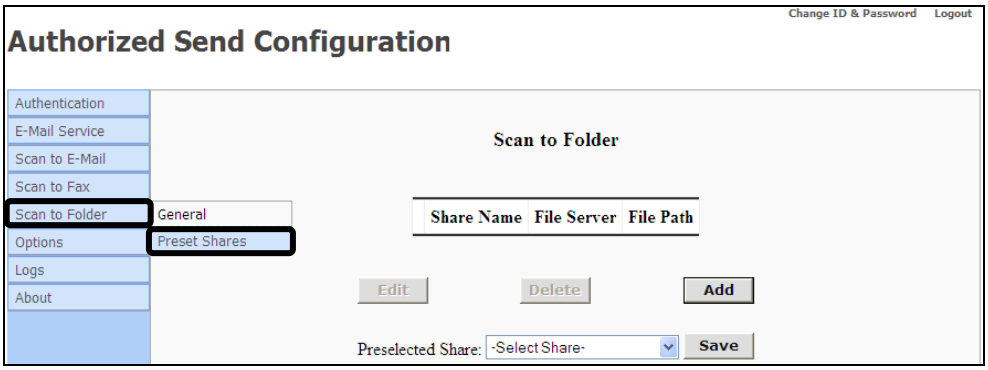
Select the [Test] check box if you want the connection to the WINS server to be verified before you save the settings.

Select the [Enable Dynamic Folder Creation] check box if you want a sub-folder to be automatically created when a user tries to scan to a folder that does not exist.

Select the [Only for Preset Shares] check box to restrict a user to only scan to a dynamic folder that was created as a preset share by the Administrator beforehand. When this option is selected, the user must enter a valid file server/file path manually.

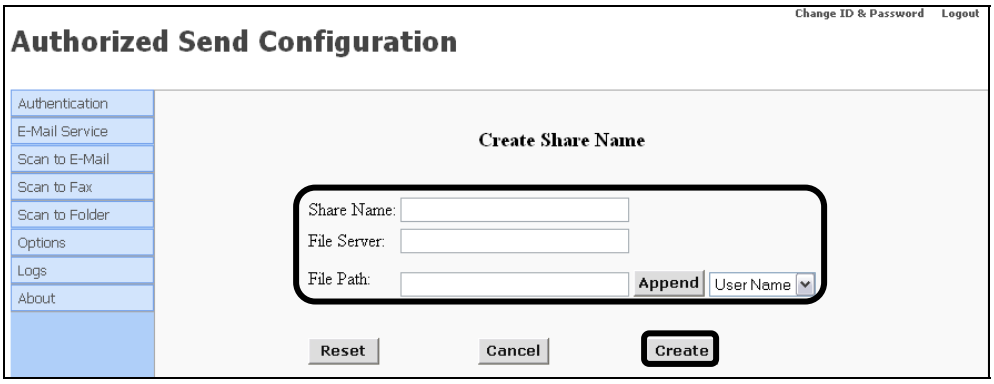
A message appears, informing you that the settings have been saved.

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



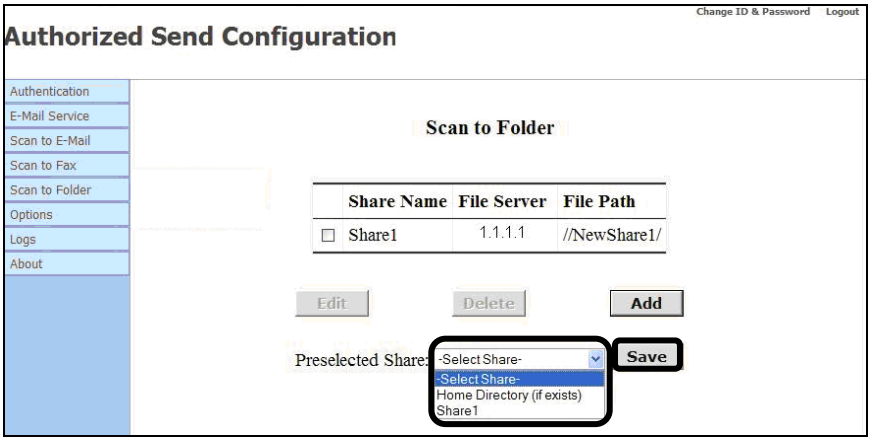
The Preset Shares screen appears.

17. Click [Add] ➞ specify the Share Name settings ➞ click [Create]. (See "Creating a Preset Share," on p. 91.)



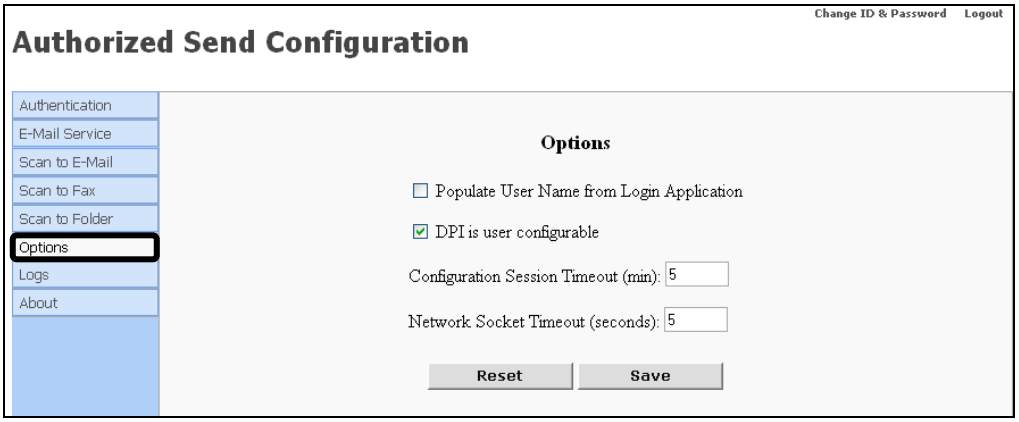
The new preset share is added to the list on the Preset Shares screen.

17.1 If you want to specify your home directory as a preselected share that will automatically appear in the Preset Share drop-down list on the SCAN TO FOLDER screen, select [Home Directory (if exists)] from the Preselected Share drop-down list ➞ click [Save]. (See "Creating a Preset Share," on p. 91.)



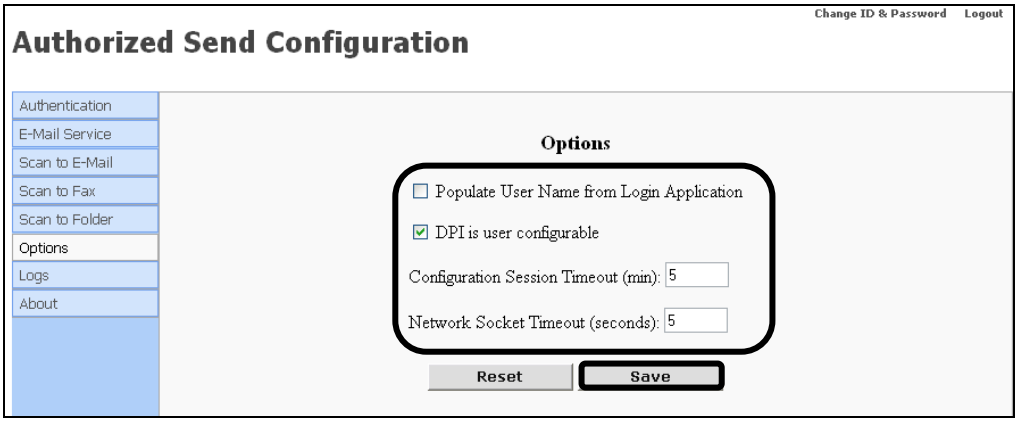
A message appears, informing you that the settings have been saved.

18. Click [Options].



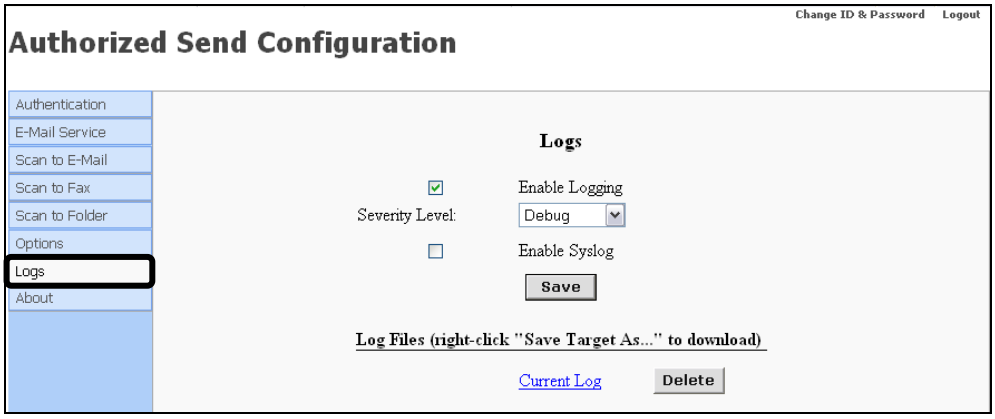
The Options screen appears.

19. Specify the optional settings, as necessary → click [Save]. (See "Configuring Optional Settings," on p. 95.)



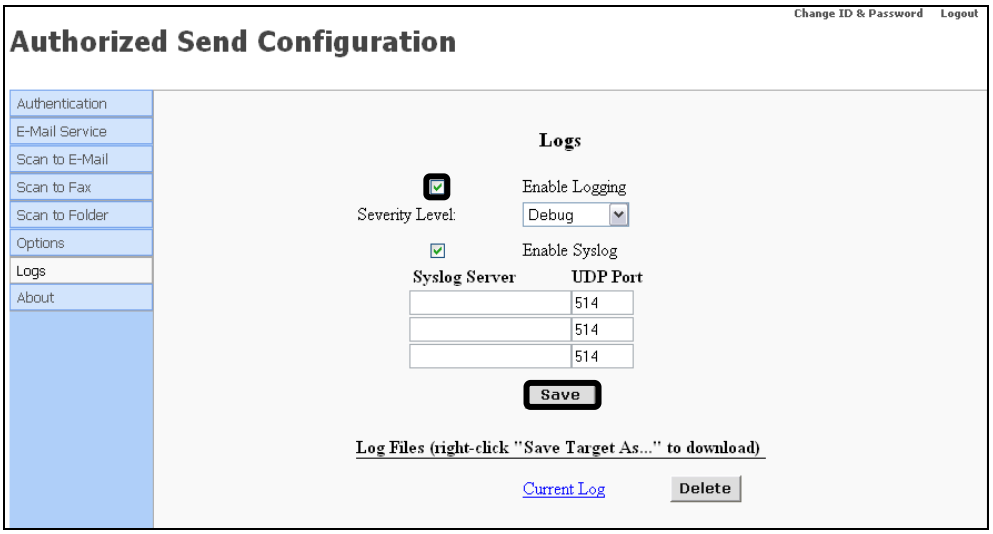
A message appears, informing you that the settings have been saved.

20. Click [Logs].



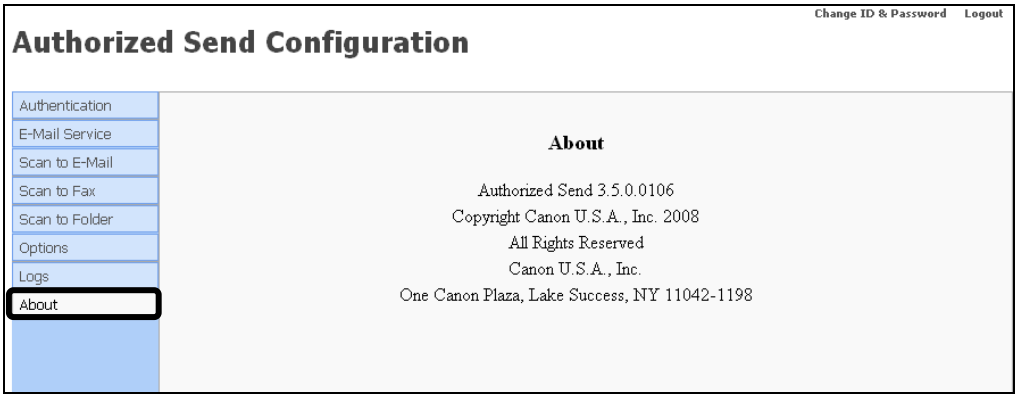
The Logs screen appears.

21. Click the [Enable Logging] check box → specify the Severity Level → configure the syslog servers → click [Save]. (See "Configuring Log Settings," on p. 97.)

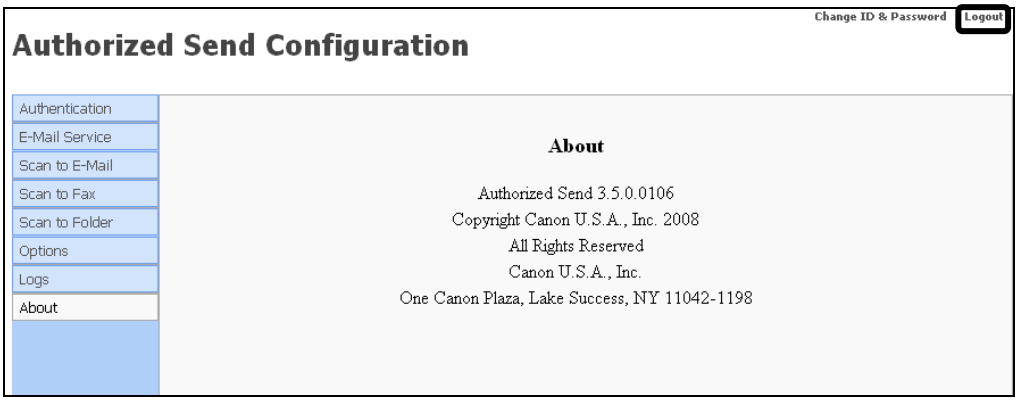


You can also view, download, or delete the current log file. For more information, see "Configuring Log Settings," on p. 97.)

22. If you want to verify the version number of Authorized Send, click [About].



23. Click [Logout].



3.2 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. 117.

1. Display the Authorized Send Configuration screen.

NOTE

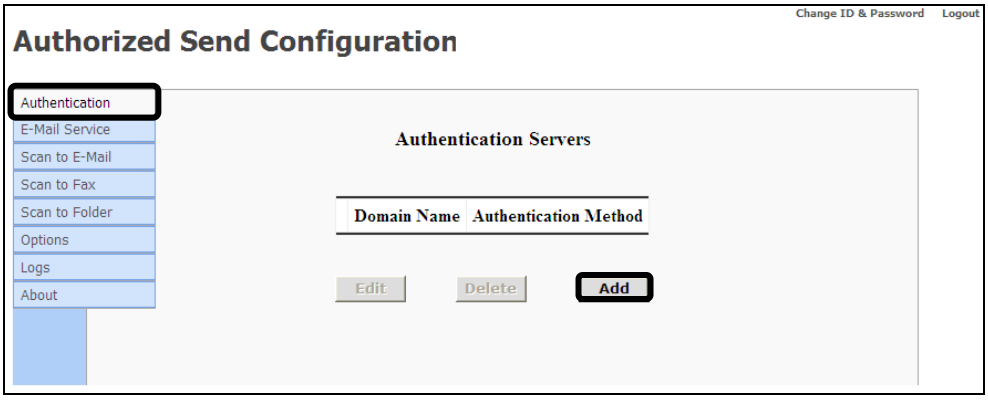
For instructions on displaying the Authorized Send Configuration screen, see "Flow of Configuration Operations," on p. 31.

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

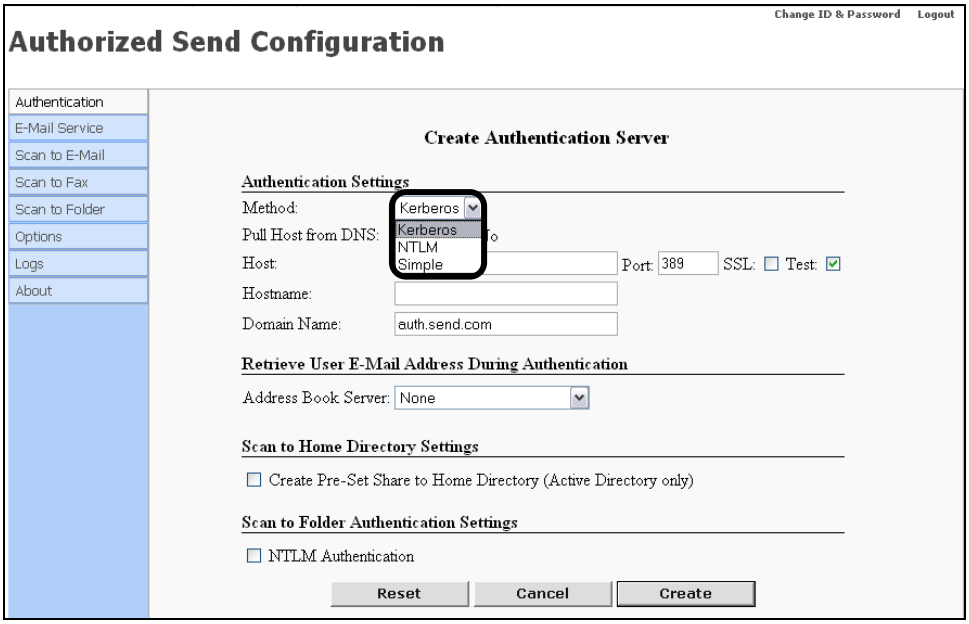
NOTE

For more details on logging on to the Authorized Send Configuration screen, see "Flow of Configuration Operations," on p. 31.

3. Click [Authentication] → [Add].



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



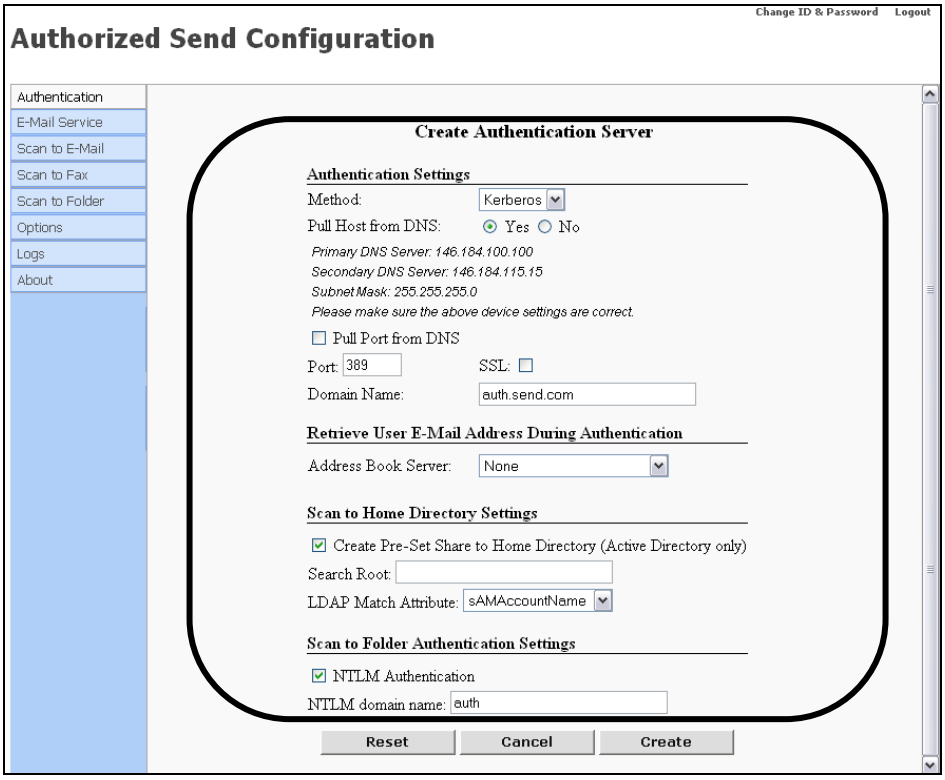
[Kerberos]: The MEAP device communicates directly to Active Directory.

[NTLM]: The MEAP device communicates directly to Active Directory.

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

5. Specify the settings for the selected authentication method.

   5.1 If you select [Kerberos] or [NTLM] as the authentication method, specify the Authentication Settings, Retrieve User E-Mail Address During Authentication, Scan to Home Directory Settings, and Scan to Folder Authentication Settings.



Authentication Settings

Method:	Kerberos or 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. If you select the [Yes] radio button, the first "live" domain controller is used as the authentication server after you click [Create].
Host:	This field is only displayed if Pull Host from DNS is set to 'No'. Enter the DNS name or IP address of the authentication server.

Port:	This field is only displayed 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. The default port number is ‘389’.
SSL:	This check box is only displayed 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 only displayed 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.
Hostname:	This field is only displayed if Pull Host from DNS is set to ‘No’. Enter the host name of the authentication server.
Domain Name:	Enter the domain name of the authentication server.
Pull Port from DNS:	This check box is only displayed if Pull Host from DNS is set to ‘Yes’. Select the [Pull Port from DNS] check box if you want the Port field to be dynamically populated from the DNS.

Retrieve User E-Mail Address During Authentication

Address Book Server:	If you have already configured an address book server, select the address book server from which your e-mail address will be retrieved from the drop-down list.

Scan to Home Directory Settings

Create Pre-Set Share to 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 will create 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, as well as the [Create Pre-Set Share to Home Directory] check box on the Create Address Book Server screen is 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. *If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.* [Search Root] only appears if the [Create Pre-Set Share to Home Directory (Active Directory only)] check box is selected.
LDAP Match Attribute:	Select [sAMAccountName] or [userPrincipalName] from the drop-down list. This enables you to search for the user's Home Directory.

Scan to Folder Authentication Settings

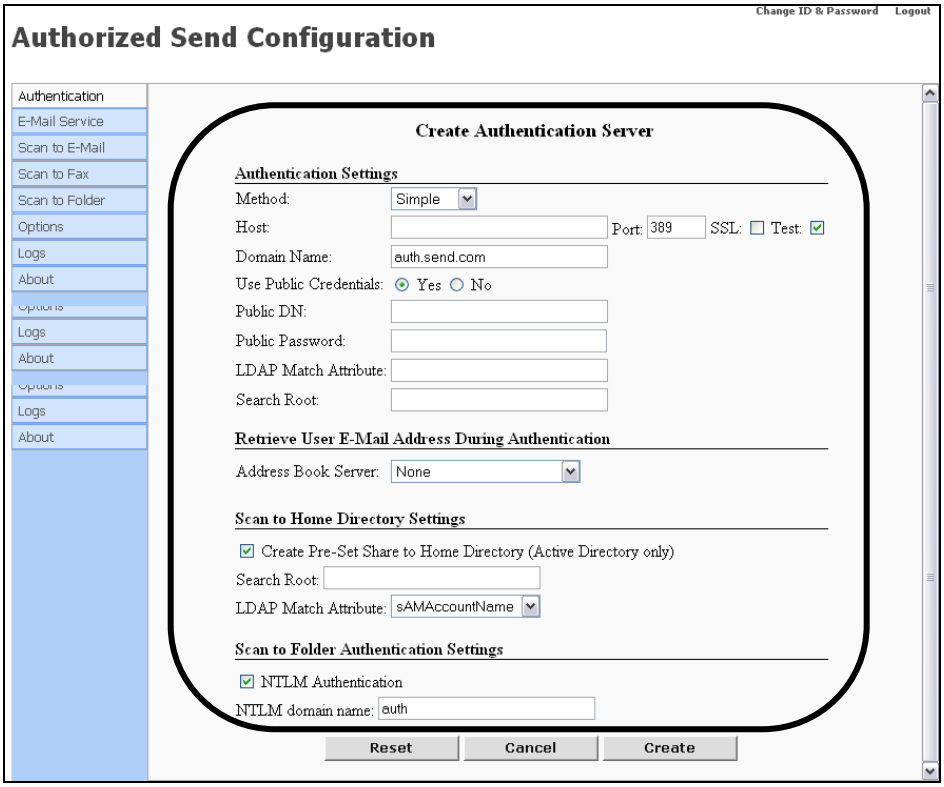
NTLM Authentication: Select this check box to use NTLM as the authentication method for the Scan to Folder feature, regardless of the authentication method you selected for the authentication server.

NTLM Domain Name: Enter the domain name to be used for NTLM authentication of a share for the Scan to Folder feature.

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. 117.

5.2 If you select [Simple] as the authentication method, specify the Authentication Settings, Retrieve User E-Mail Address During Authentication, Scan to Home Directory Settings, and Scan to Folder Authentication 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. 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.
Domain Name:	Enter the domain name of the authentication server.
Use Public Credentials:	Select [Yes] to configure the public credentials (Public Domain Name, Public Password), or select [No] to use anonymous binding.
Public DN:	Enter the user's login Distinguished Name to use when performing the first bind of the Simple Binding process. Only displayed if [Yes] is selected for Use Public Credentials.
Public Password:	Enter the password to use when performing the first bind of the Simple Binding process. Only displayed if [Yes] is selected for Use Public Credentials.
LDAP Match Attribute:	Enter the user name's LDAP attribute to be matched with the user name when performing the first bind of the Simple Binding process.
Search Root:	Enter the root to search for the authenticating user's Domain Name. *If the directory server is authenticating against eDirectory or Domino and the organization is, for example, Canon, then the search root is o=canon.*

Retrieve User E-Mail Address During Authentication

Address Book Server:	If you have already configured an address book server, select the address book server from which your e-mail address will be retrieved from the drop-down list.

Scan to Home Directory Settings

Create Pre-Set Share to 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 will create 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, as well as the [Create Pre-Set Share to Home Directory] check box on the Create Address Book Server screen is 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. [Search Root] only appears if the [Create Pre-Set Share to Home Directory (Active Directory only)] check box is selected.
LDAP Match Attribute:	Select [sAMAccountName] or [userPrincipalName] from the drop-down list. This enables you to search for the user's Home Directory.

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.

6. Click [Create].

   If you make a mistake while configuring the authentication server 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 appears informing you that the configuration has been saved, and the screen returns to the Authentication Servers screen.

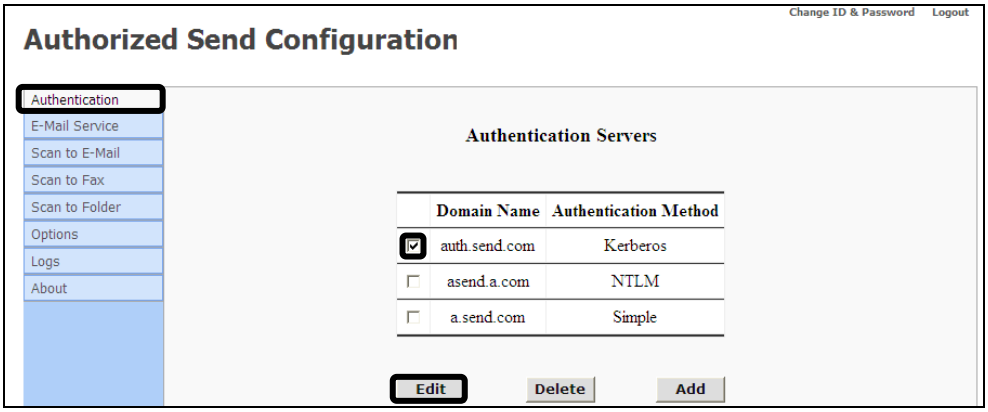
IMPORTANT

- Click 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 will be displayed. Enter the correct information → click [Save].

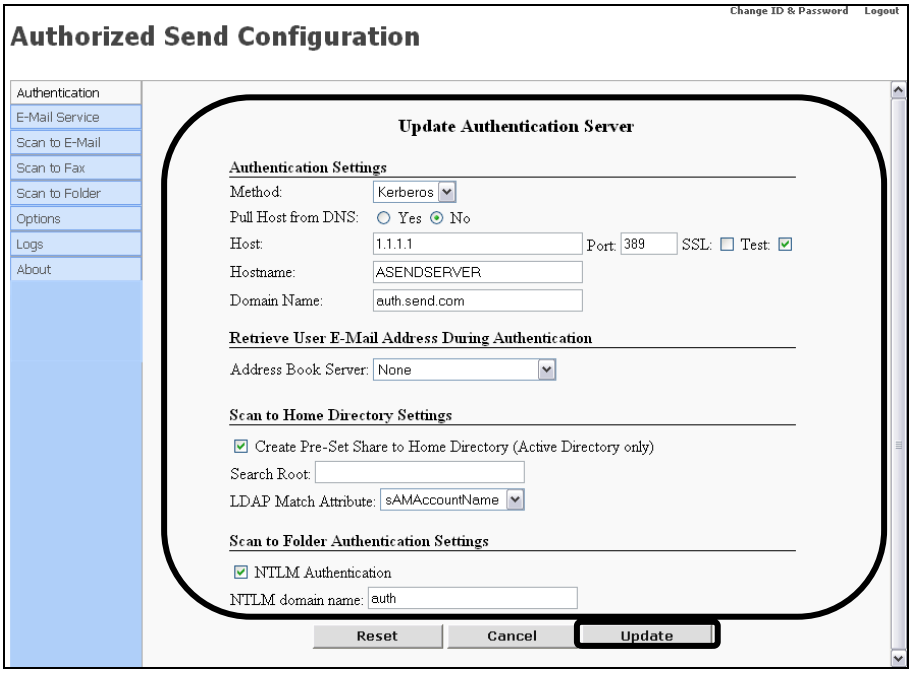
3.3 Editing an Authentication Server

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].



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



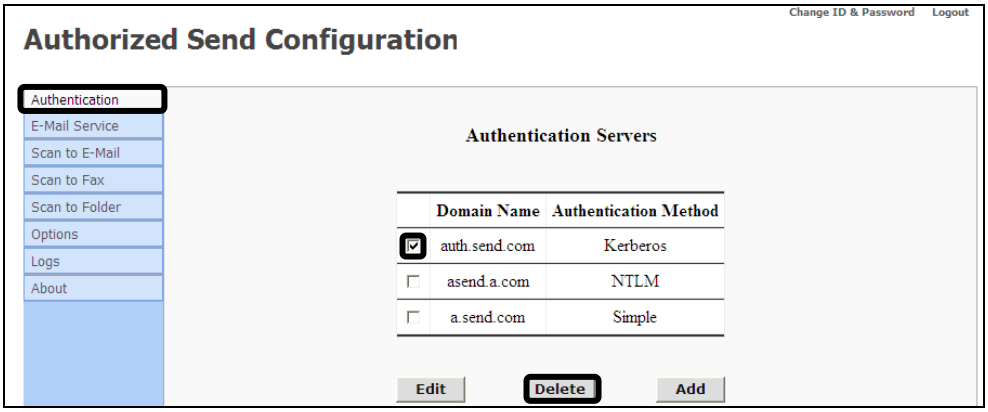
If you make a mistake, click [Reset] to return the settings to their original values.

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

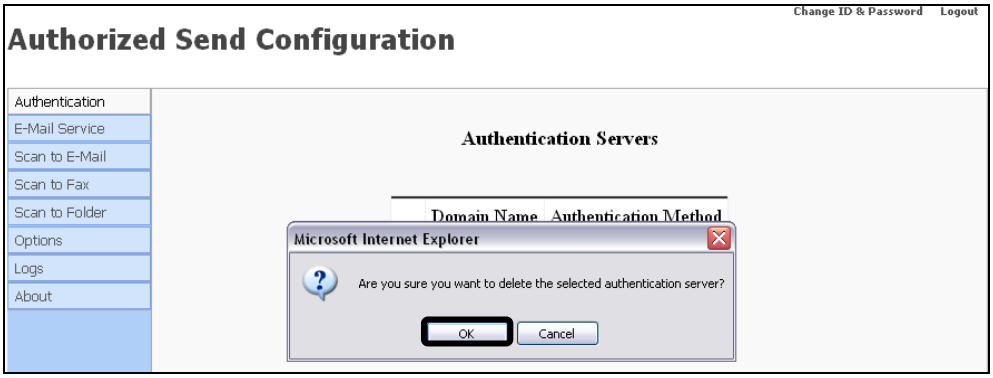
3.4 Deleting an Authentication Server

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.

3.5 Configuring the E-Mail Service Settings

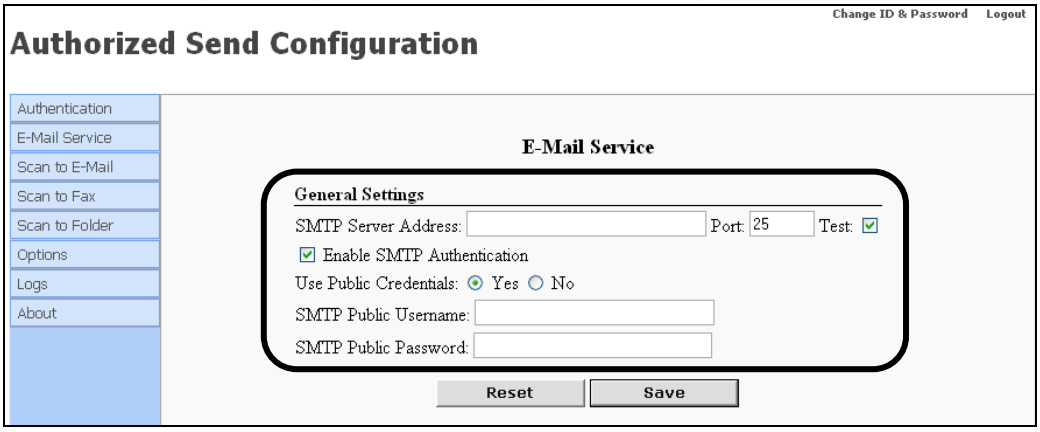
You can configure the settings for the SMTP server.

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

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

   If necessary, see the screen shot in step 5 of "Flow of Configuration Operations," on p. 31.

2. Configure the settings as necessary.



General Settings

SMTP Server Address:	Enter the IP Address or DNS name of the SMTP server.
Port:	Enter the connecting port number of the SMTP server. The default port number is '25'.
Test:	Select this check box if you want the connection to the SMTP server to be verified before you save the settings.
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.

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 login credentials are used.
SMTP Public Username:	If [Yes] is selected for Use Public Credentials, you must enter the user name for SMTP authentication.
SMTP Public Password:	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 appears informing you that the configuration has been saved.

IMPORTANT

- Click 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 will be 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.

3.6 Creating an Address Book Server

You can create up to 10 Address Book Servers. There are two methods for which to create an Address Book Server: with an association to an Authentication Server or without an association to an Authentication Server.

IMPORTANT

- You must configure an address book for an authentication server to retrieve an e-mail address for the end 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. 117.

3.6.1 Creating an Address Book Server with an Association to an Authentication Server

When you create an address book server, you can associate it with an authentication server, which has been previously created.

NOTE

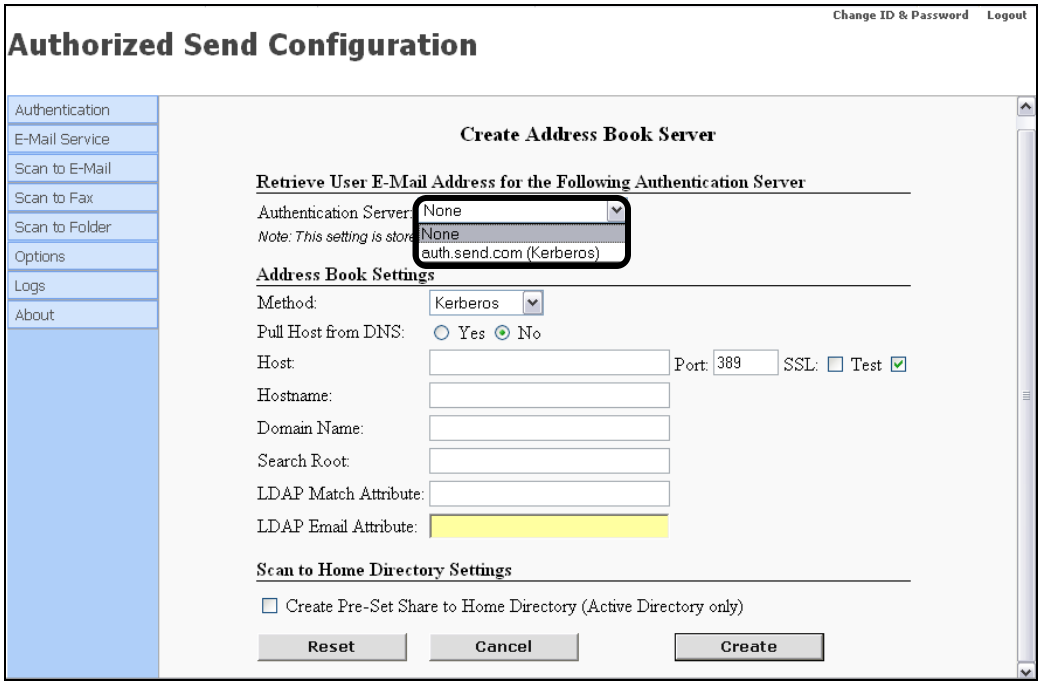
- To associate an address book with an authentication server, you must first create an authentication server for Authorized Send. For instructions on creating an authentication server, see “Creating an Authentication Server,” on p. 44.
- This option may be initially set on this screen, as well as configured and edited on the Create Authentication Server screen.

---

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

   If necessary, see the screen shots in steps 7 and 8 of "Flow of Configuration Operations," on p. 31.

2. Select an authentication server to associate with the address book you are creating from the Authentication Server drop-down list under Retrieve User E-Mail Address for the Following Authentication Server.

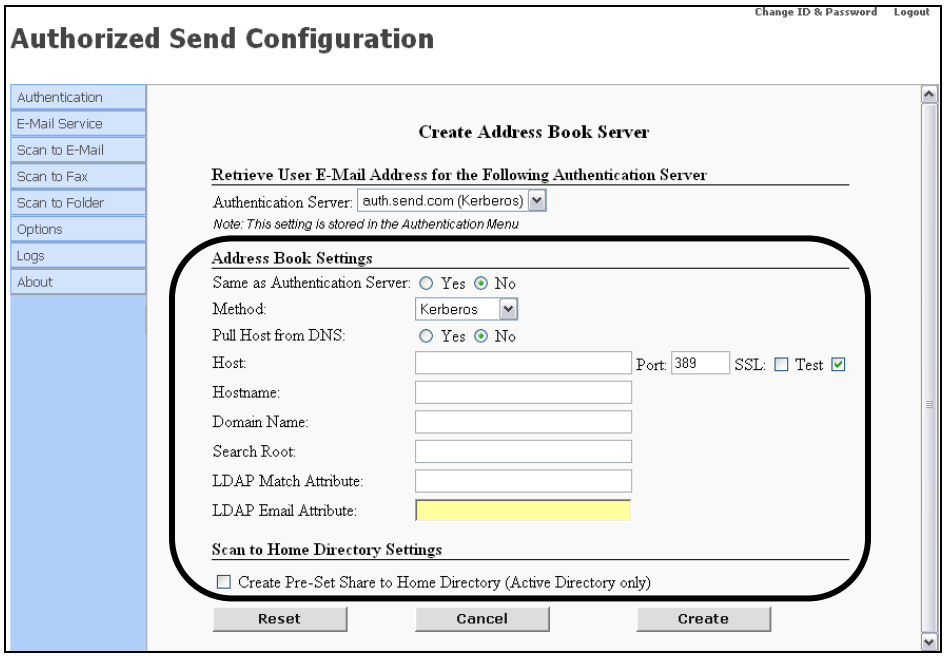


NOTE

- 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 will not be associated with an authentication server and will 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.

3. Specify the Address Book Settings.

   3.1 If you select a Kerberos or NTLM authentication server, specify the Address Book Settings and Scan to Home Directory Settings, as described below.



Address Book Settings

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

Method:	This drop-down list only appears when Same as Authentication Server is set to ‘No’. Select [Kerberos], [NTLM], [Simple], or [Anonymous] to authenticate to the address book host. If [Kerberos] or [NTLM] is selected, the user’s login credentials (user name and password) are used. If [Simple] is selected, the user’s login credentials or public credentials (if configured) are used. If [Anonymous] is selected, no credentials are used to search the address book server for e-mail addresses.
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.
Host:	This field is only displayed if Pull Host from DNS is set to ‘No’. Enter the DNS name or IP address of the address book server.
Port:	This field is only displayed 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. The default port number is ‘389’.
SSL:	This check box is only displayed 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 only displayed 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.
Hostname:	This field is only displayed if Pull Host from DNS is set to 'No'. Enter the host name of the address book server.
Domain Name:	Enter the domain name of the address book server. The [Domain Name] text box only appears if Same as Authentication Server is set to 'No'.
Pull Port from DNS:	This check box is only displayed if Pull Host from DNS is set to 'Yes'. Select the [Pull Port from DNS] check box if you want the Port field to be dynamically populated from the DNS.
Search Root:	Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. *If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.*
LDAP Match Attribute:	Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Create Pre-Set Share to Home Directory] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval. An example for Active Directory is 'sAMAccountName' or 'userPrincipalName'.
LDAP Email Attribute:	Enter the e-mail LDAP attribute to pull the user's e-mail address. An example for Active Directory is 'mail'.

Scan to Home Directory Settings

Create Pre-Set Share to 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 will create a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

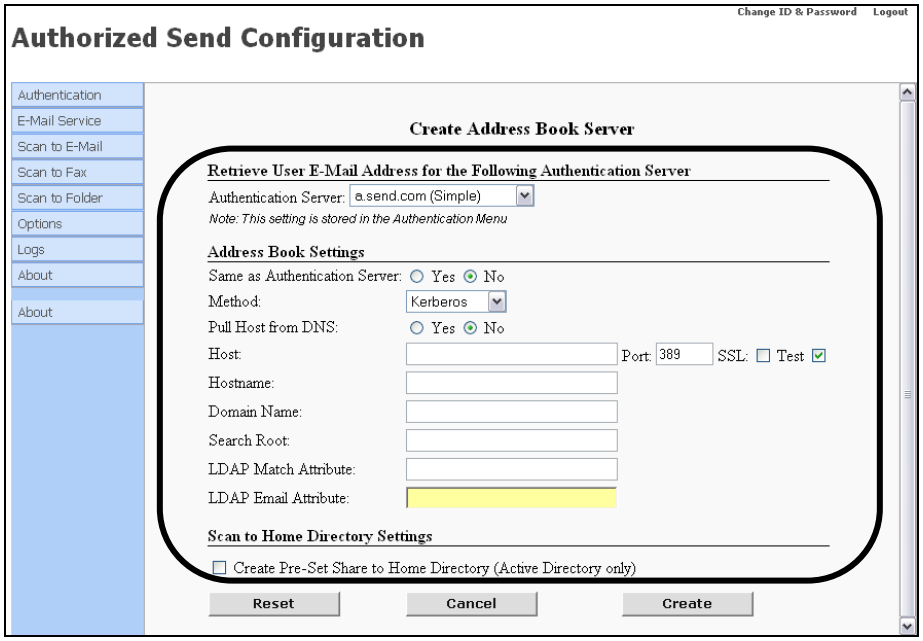
IMPORTANT

If this check box is selected, as well as the [Create Pre-Set Share to Home Directory] check box on the Create Authentication Server screen is 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. 117.

3.2 If you select a Simple authentication server, specify the Address Book Settings and Scan to Home Directory Settings, as described below.



Address Book Settings

Same as Authentication Server:	Select [Yes] to create the address book with the same credentials as the selected authentication server. If you select [No], you must enter the configuration information for the authentication method.
Method:	This drop-down list only appears when Same as Authentication Server is set to 'No'. Select [Kerberos], [NTLM], [Simple], or [Anonymous] to authenticate to the address book host. If [Kerberos] or [NTLM] is selected, the user's login credentials (user name and password) are used. If [Simple] is selected, the user's login credentials or public credentials (if configured) are used. If [Anonymous] is selected, no credentials are used to search the address book server for e-mail addresses.
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.
Host:	This field is only displayed if Pull Host from DNS is set to 'No'. Enter the DNS name or IP address of the address book server.
Port:	This field is only displayed 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. The default port number is '389'.

SSL:	This check box is only displayed 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 only displayed 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.
Hostname:	This field is only displayed if Pull Host from DNS is set to ‘No’. Enter the host name of the address book server.
Domain Name:	Enter the domain name of the address book server. The [Domain Name] text box only appears if Same as Authentication Server is set to ‘No’.
Pull Port from DNS:	This check box is only displayed if Pull Host from DNS is set to ‘Yes’. Select the [Pull Port from DNS] check box if you want the Port field to be dynamically populated from the DNS.
Search Root:	Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. *If the directory server is authenticating against eDirectory or Domino and the organization is, for example, Canon, then the search root is o=canon.*

LDAP Match Attribute:	Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Create Pre-Set Share to Home Directory] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval. An example for eDirectory and Domino is 'uid'.
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'.

Scan to Home Directory Settings

Create Pre-Set Share to 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 will create 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, as well as the [Create Pre-Set Share to Home Directory] check box on the Create Authentication Server screen is 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.

4. Click [Create].

   If you make a mistake while configuring the address book server 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.

3.6.2 Creating an Address Book Server without an Association to an Authentication Server

You can create a standalone address book server with no association to an authentication server.

NOTE

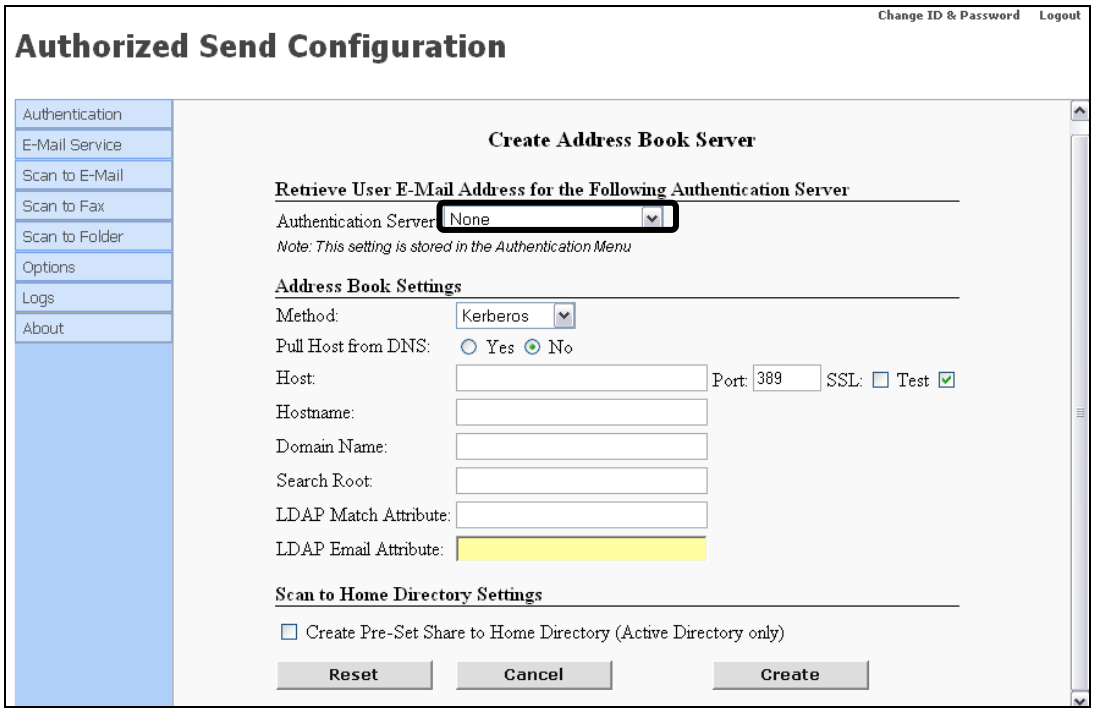
If you select [None] from the Authentication Server drop-down list when creating an address book server, the address book server will not be associated with an authentication server and will not interact with any other features of Authorized Send. Select [None] if you want to create an address book server that can be configured at a later time.

---

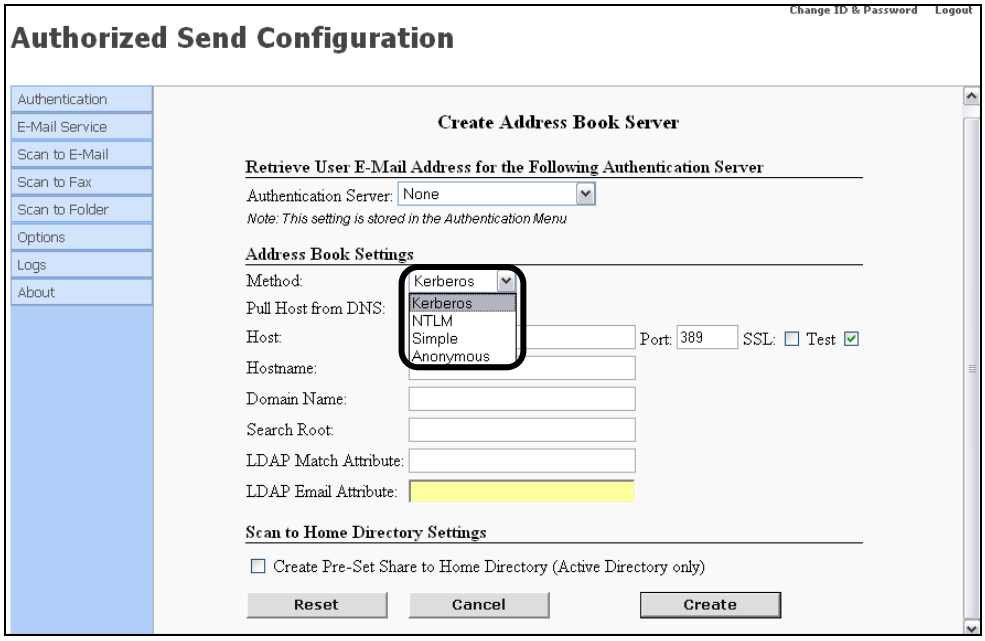
1. Click [E-Mail Service] ➞ [Address Book] ➞ [Add] under Address Book Servers.

   If necessary, see the screen shots in steps 7 and 8 of "Flow of Configuration Operations," on p. 31.

2. Select [None] from the Authentication Server drop-down list under Retrieve User E-Mail Address for the Following Authentication Server.



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



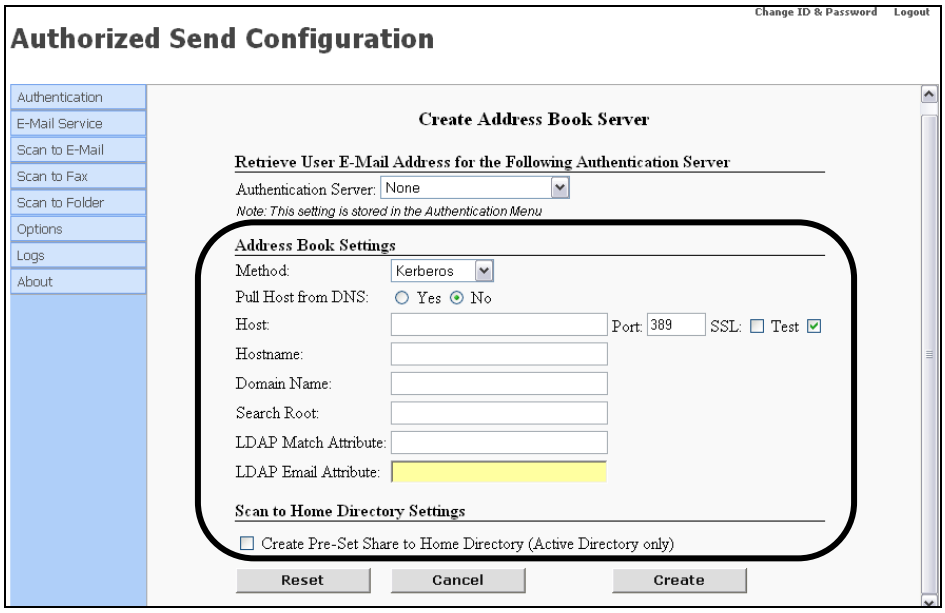
[Kerberos]: The MEAP device communicates directly to Active Directory.

[NTLM]: The MEAP device communicates directly to Active Directory.

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

[Anonymous]: Authorized Send will not use any user login credentials to search the address book for e-mail addresses.

3.1 If you select [Kerberos] as the authentication method, specify 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.
Host:	This field is only displayed if Pull Host from DNS is set to 'No'. Enter the DNS name or IP address of the address book server.
Port:	This field is only displayed 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. The default port number is '389'.
SSL:	This check box is only displayed 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 only displayed 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.
Hostname:	This field is only displayed if Pull Host from DNS is set to 'No'. Enter the host name of the address book server.
Domain Name:	Enter the domain name of the address book server.
Pull Port from DNS:	This check box is only displayed if Pull Host from DNS is set to 'Yes'. Select the [Pull Port from DNS] check box if you want the Port field to be dynamically populated from the DNS.
Search Root:	Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. *If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.*
LDAP Match Attribute:	Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Create Pre-Set Share to Home Directory] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval. An example for Active Directory is 'sAMAccountName' or 'userPrincipalName'.
LDAP Email Attribute:	Enter the e-mail LDAP attribute to pull the user's e-mail address. An example for Active Directory is 'mail'.

Scan to Home Directory Settings

Create Pre-Set Share to 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 will create 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, as well as the [Create Pre-Set Share to Home Directory] check box on the Create Authentication Server screen is 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.

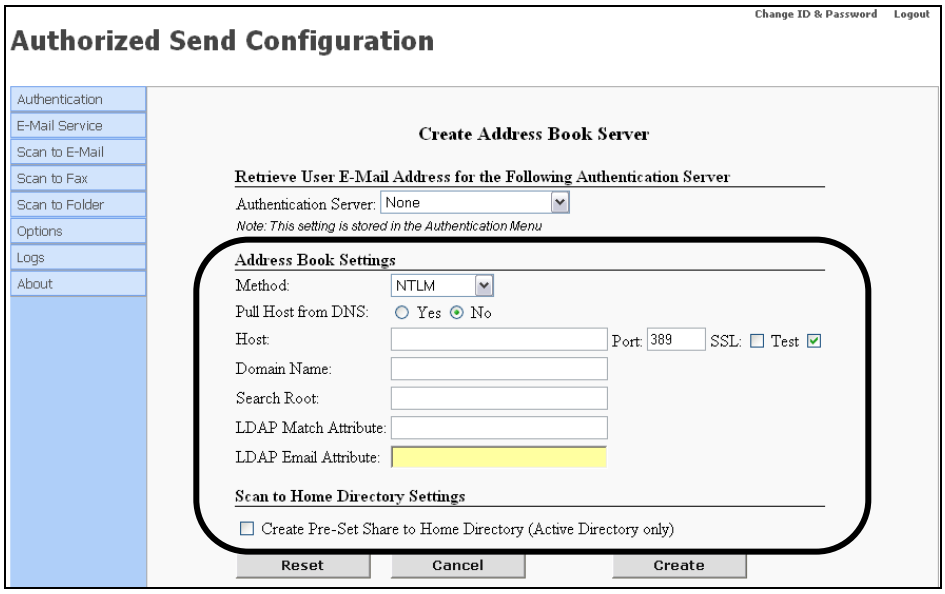
IMPORTANT

- 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. 117.
- Click 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 will be 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.

3.2 If you select [NTLM] as the authentication method, specify 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.
Host:	This field is only displayed if Pull Host from DNS is set to 'No'. Enter the DNS name or IP address of the address book server.
Port:	This field is only displayed 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. The default port number is '389'.
SSL:	This check box is only displayed 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 only displayed 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.
Domain Name:	Enter the domain name of the address book server.
Pull Port from DNS:	This check box is only displayed if Pull Host from DNS is set to 'Yes'. Select the [Pull Port from DNS] check box if you want the Port field to be dynamically populated from the DNS.
Search Root:	Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. *If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.*
LDAP Match Attribute:	Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Create Pre-Set Share to Home Directory] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval. An example for Active Directory is 'sAMAccountName' or 'userPrincipalName'.
LDAP Email Attribute:	Enter the e-mail LDAP attribute to pull the user's e-mail address. An example for Active Directory is 'mail'.

Scan to Home Directory Settings

Create Pre-Set Share to 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 will create 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, as well as the [Create Pre-Set Share to Home Directory] check box on the Create Authentication Server screen is 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.

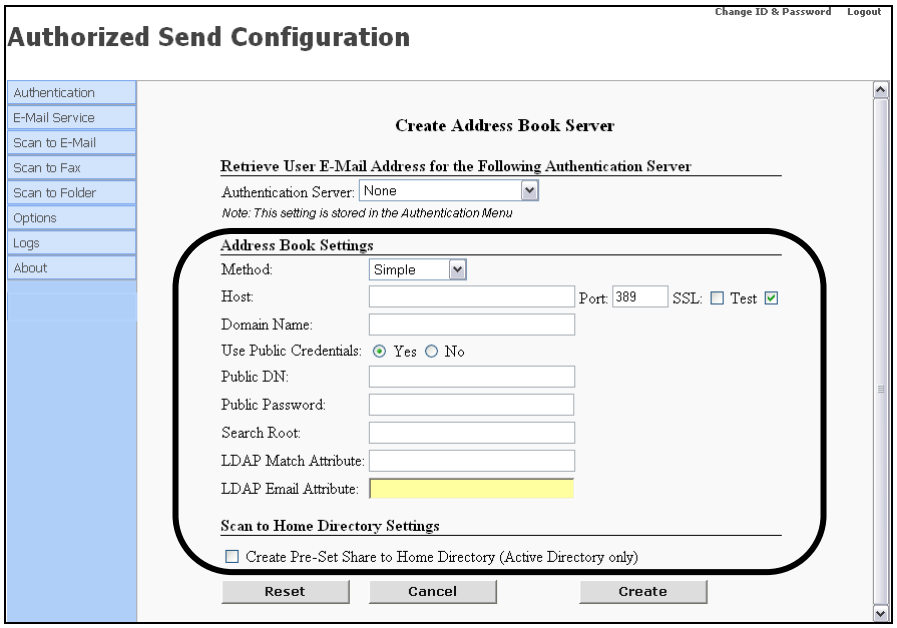
IMPORTANT

- Click 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 will be 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.

3.3 If you select [Simple] as the authentication method, specify 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. 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.
Domain Name:	Enter the domain name of the address book server.

Use Public Credentials:	Select [Yes] to configure the public credentials (Public Domain Name, Public Password), or select [No] to use anonymous binding.
Public DN:	Enter the user's login Distinguished Name to use when performing the first bind of the Simple Binding process. Only displayed if [Yes] is selected for Use Public Credentials.
Public Password:	Enter the password to use when performing the first bind of the Simple Binding process. Only displayed if [Yes] is selected for Use Public Credentials.
Search Root:	Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. *If the directory server is authenticating against eDirectory or Domino and the organization is, for example, Canon, then the search root is o=canon.*
LDAP Match Attribute:	Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Create Pre-Set Share to Home Directory] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval. An example for eDirectory and Domino is 'uid'.
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'.

Scan to Home Directory Settings

Create Pre-Set Share to 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 will create 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, as well as the [Create Pre-Set Share to Home Directory] check box on the Create Authentication Server screen is 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.

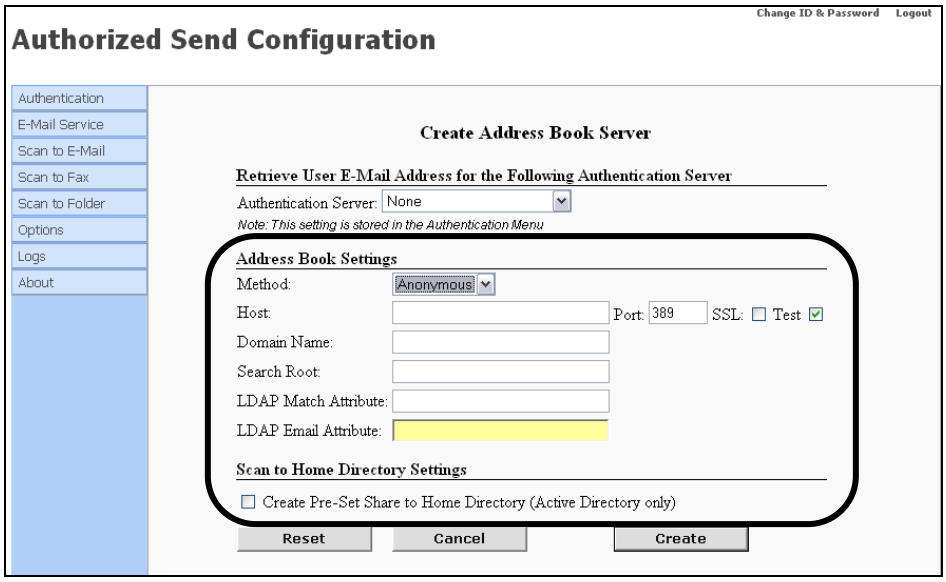

IMPORTANT

- Click 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 will be 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.

3.4 If you select [Anonymous] as the authentication method, specify 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. 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.
Domain Name:	Enter the domain name of the address book server.

Search Root:	Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts. *If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.* *If the directory server is authenticating against eDirectory or Domino and the organization is, for example, Canon, then the search root is o=canon.*
LDAP Match Attribute:	Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Create Pre-Set Share to Home Directory] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval. An example for Active Directory is 'sAMAccountName' or 'userPrincipalName'. An example for eDirectory and Domino is 'uid'.
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'.

Scan to Home Directory Settings

Create Pre-Set Share to 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 will create 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, as well as the [Create Pre-Set Share to Home Directory] check box on the Create Authentication Server screen is 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

- Click 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 will be 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. Click [Create].

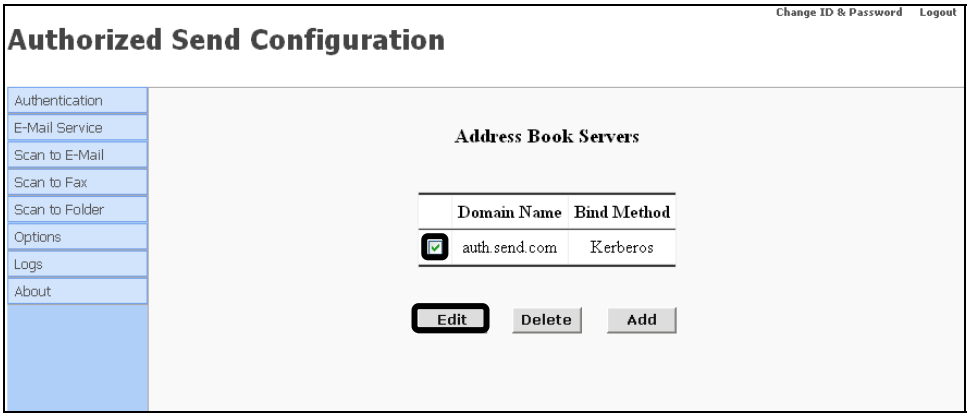
   If you make a mistake while configuring the address book server settings, click [Reset] to return the settings to their original values.

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

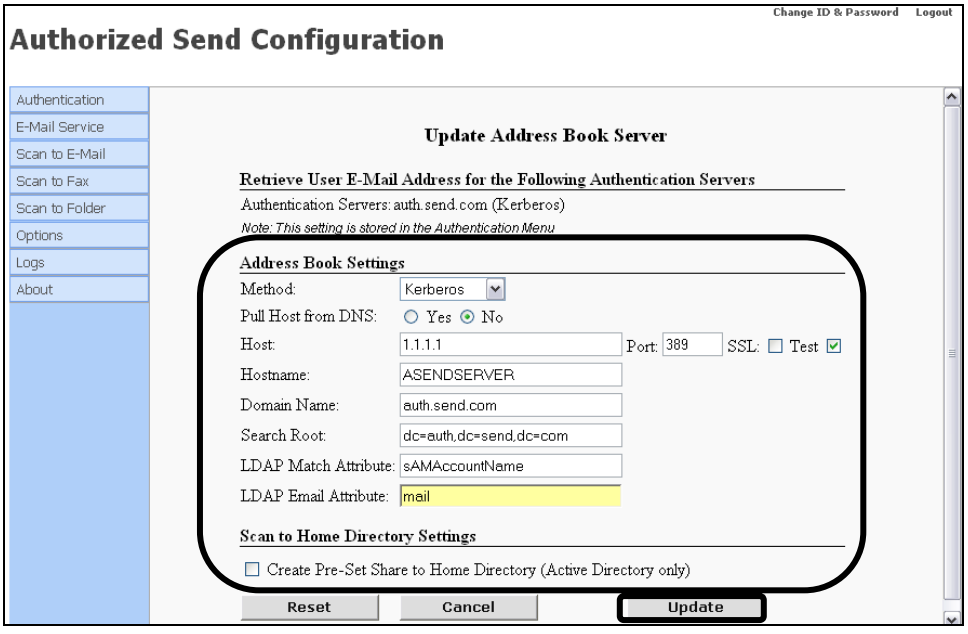
3.7 Editing an Address Book Server

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].



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



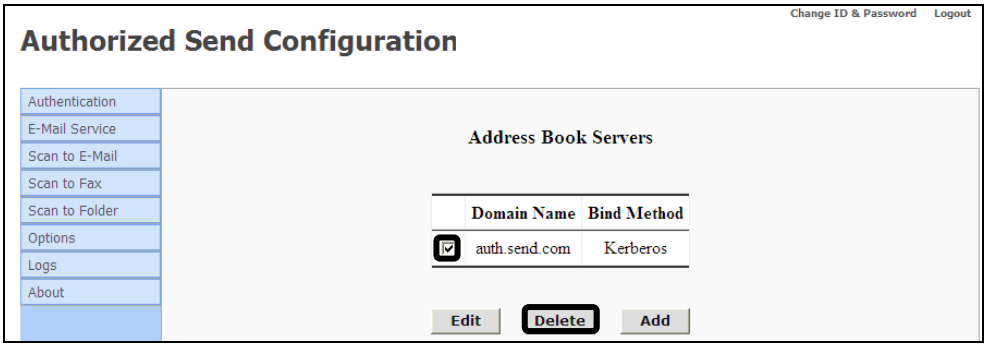
If you make a mistake while editing the address book server settings, click [Reset] to return the settings to their original values.

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

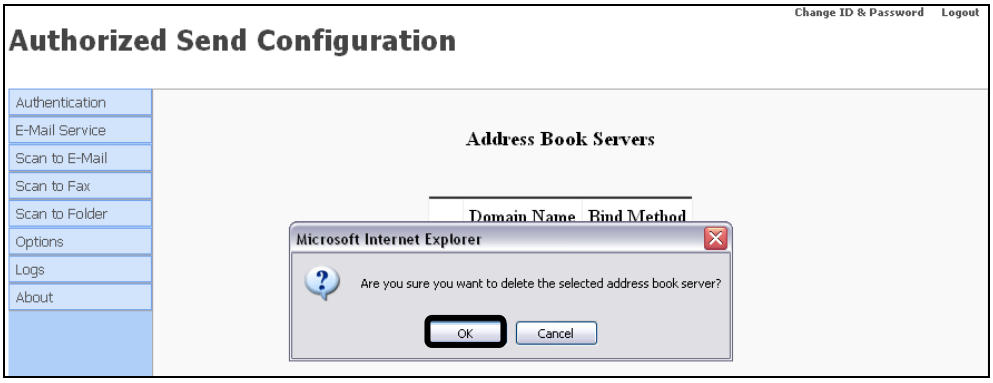
3.8 Deleting an Address Book Server

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.

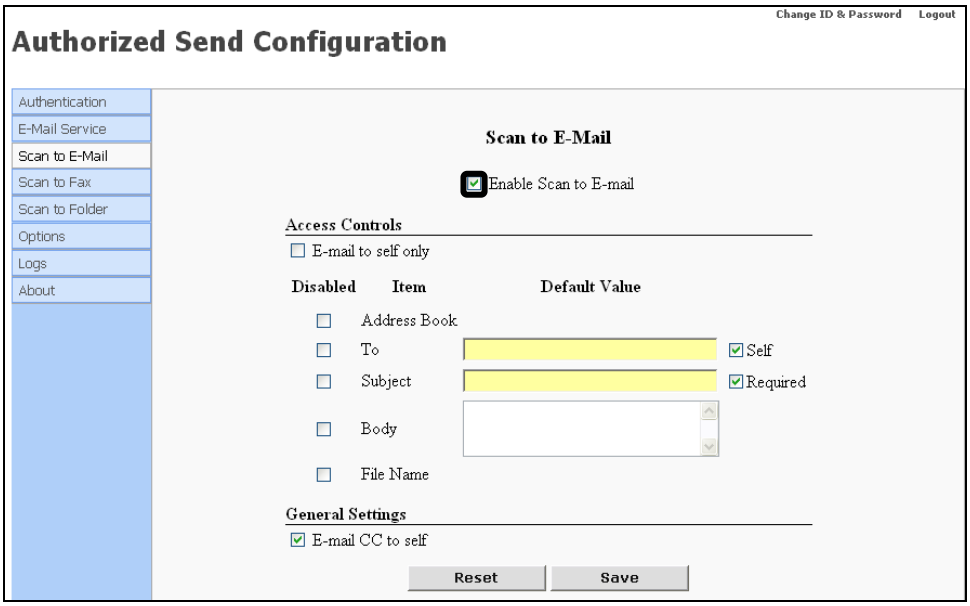
3.9 Configuring Scan to E-Mail Settings

You can enable the Scan to E-Mail function, restrict user access to the Address Book and [To], [Subject], [Body], and [File Name] text boxes on the SCAN TO EMAIL screen, as well as enable E-mail CC to self.

1. Click [Scan to E-Mail].

   If necessary, see the screenshot in step 10 of "Flow of Configuration Operations," on p. 31.

2. Click the [Enable Scan to E-mail] check box.

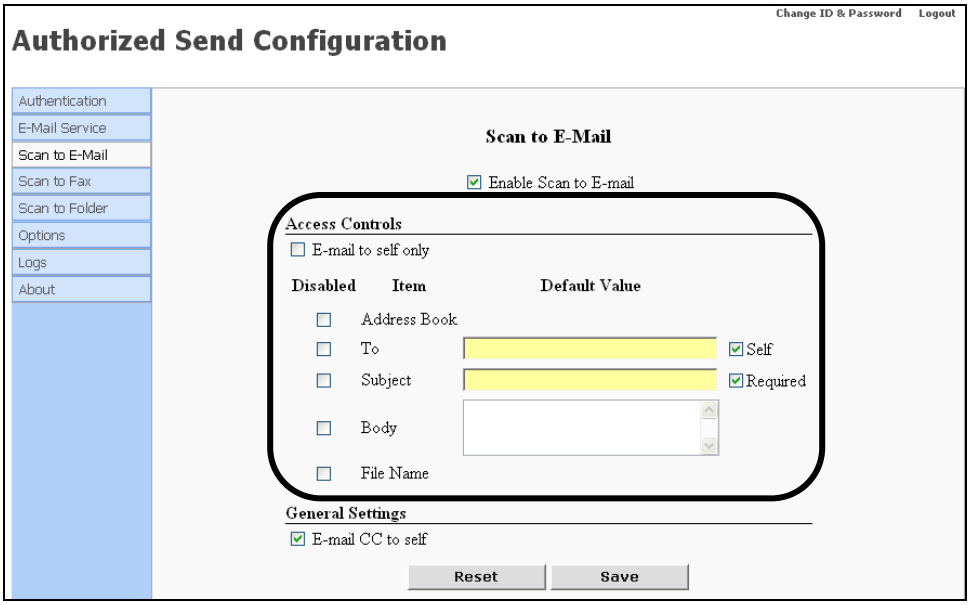


   If you want to disable the Scan to E-Mail function, click the [Enable Scan to E-mail] check box to clear the check mark.

NOTE

You can only disable the Scan to E-Mail function if there is at least one other Authorized Send function enabled.

3. Configure the settings under <Access Controls>.



Access Controls

E-mail to self only: Select this check box if you want to restrict the user to only send e-mail messages to themselves, and to automatically disable the Address Book and the [To] text field.

Disabled Column

Address Book: Select this check box if you want to restrict user access to the Address Book on the SCAN TO EMAIL screen on the machine. If you select this check box, the [Address Book] button will not appear on the SCAN TO EMAIL screen. 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 SCAN TO EMAIL screen on the machine is grayed out. The user can select an e-mail address from the Address Book, but cannot manually specify an address.

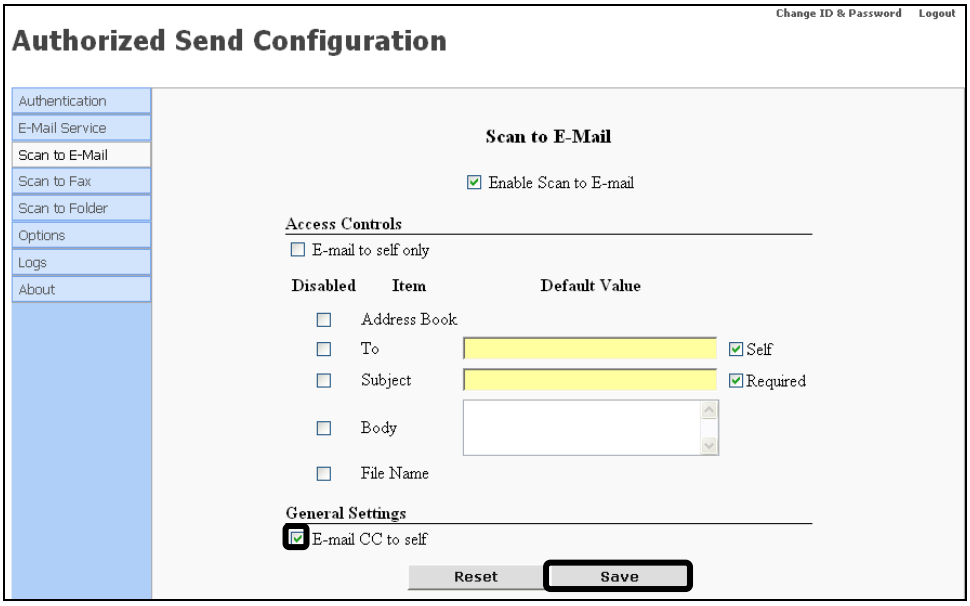
Self This check box is only displayed when the [E-mail to self only] check box is not selected. When the [Self] check box is selected, the e-mail address of the user logged on to Authorized Send is displayed in the [To] field on the SCAN TO E-MAIL screen.

Subject:	Select this check box to disable the [Subject] field on the SCAN TO E-MAIL screen.
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] field on the SCAN TO E-MAIL screen.
File Name:	Select this check box to disable the [File Name] field on the SCAN TO E-MAIL screen.

Default Value Column

To:	Enter the default e-mail address to be displayed in the [To] field on the SCAN TO E-MAIL screen.
Subject:	Enter a default subject to be displayed in the [Subject] field on the SCAN TO E-MAIL screen.
Body:	Enter a default e-mail message to be displayed in the [Body] field on the SCAN TO E-MAIL screen.

4. If necessary, click the [E-mail CC to self] check box → click [Save].



If you select [E-mail CC to self], a copy of each e-mail message sent via Scan to E-Mail will be sent to the currently logged on user's e-mail address.

IMPORTANT

You must select the [Self] check box next to the [To] text box if you selected to disable the [Address Book] and [To] check boxes in the <Disabled> column at the same time and the default value for the [To] text box is blank.

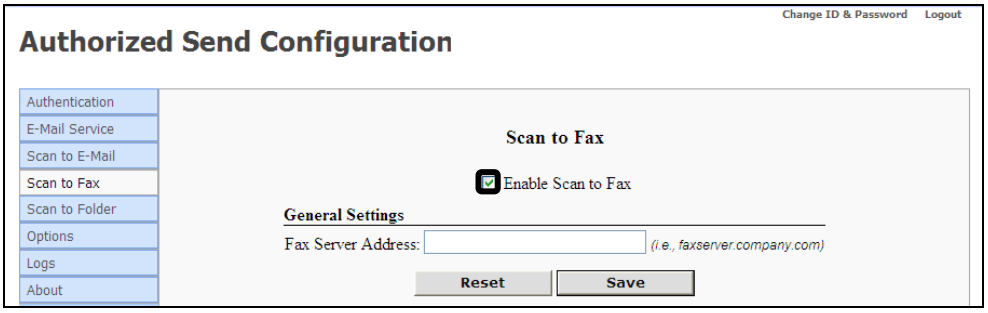
3.10 Configuring Scan to Fax Settings

You can enable the Scan to Fax function and configure the General Settings.

1. Click [Scan to Fax].

   If necessary, see the screen shot in step 12 of "Flow of Configuration Operations," on p. 31.

2. Click the [Enable Scan to Fax] check box.

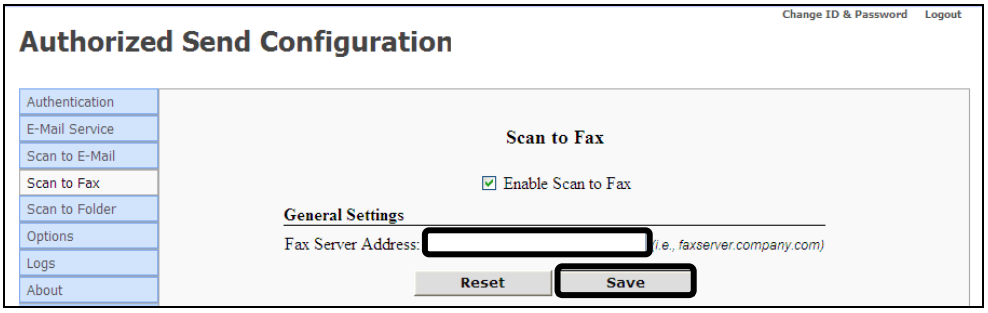


   If you want to disable the Scan to Fax function, click the [Enable Scan to Fax] check box to clear the check mark.

NOTE

- The Scan to Fax function is disabled by default.
- You can only disable the Scan to Fax function if there is at least one other Authorized Send function enabled.

3. Specify the General Settings → click [Save].



General Settings

Fax Server Address: Enter the fully qualified domain name of the e-mail server for faxing.

For example, if you enter 1234 as the fax number when sending from the Scan to Fax screen and the Fax Server Address is faxserver.company.com, the SMTP server will send the e-mail message to 1234@faxserver.company.com.

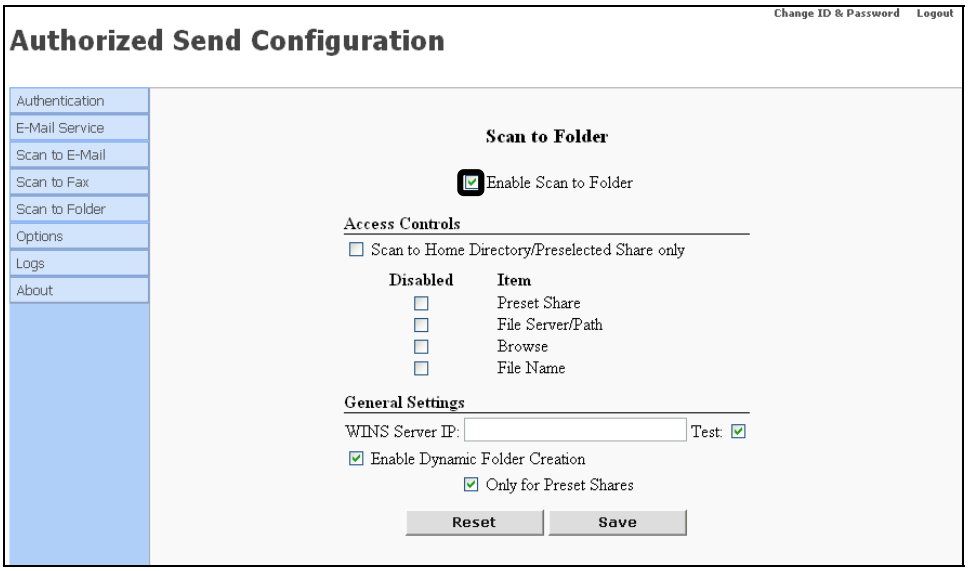
3.11 Configuring Scan to Folder Settings

You can enable the Scan to Folder function and configure the Access Controls and General Settings.

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

   If necessary, see the screen shot in step 14 of "Flow of Configuration Operations," on p. 31.

2. Click the [Enable Scan to Folder] check box.

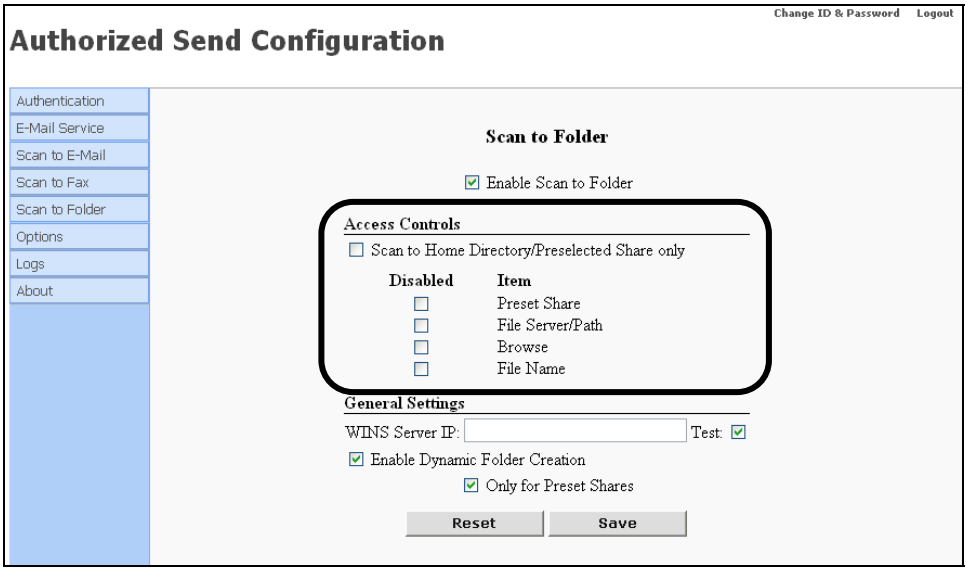


   If you want to disable the Scan to Folder function, click the [Enable Scan to Folder] check box to clear the check mark.

NOTE

You can only disable the Scan to Folder function if there is at least one other Authorized Send function enabled.

3. Configure the settings under Access Controls.



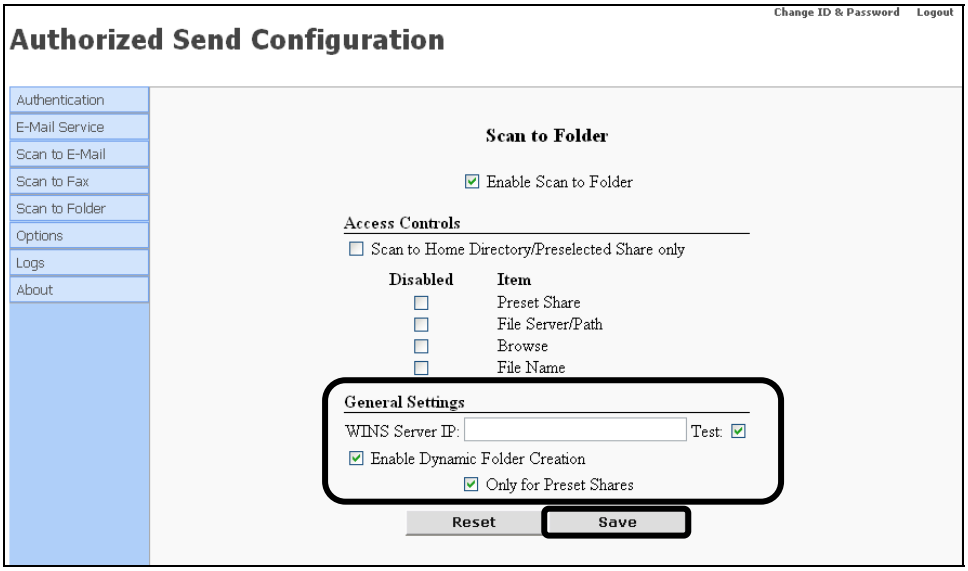
Access Controls

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 in a one-click action.

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 SCAN TO FOLDER screen. If you select this check box, the Preset Share drop-down list is grayed out.
File Server/Path:	Select this check box if you want to disable the [File Server] and [File Path] text boxes on the SCAN TO FOLDER screen. If you select this check box, the [File Server] and [File Path] text boxes are grayed out.
Browse:	Select this check box if you want to disable the [Browse] button on the SCAN TO FOLDER screen. If you select this check box, the [Browse] button does not appear on the SCAN TO FOLDER screen.
File Name:	Select this check box if you want to prevent the user from using the [File Name] text box on the SCAN TO FOLDER screen. If you select this check box, the [File Name] text box is grayed out.

4. Specify the General Settings → click [Save].



General Settings

WINS Server IP:	Enter the IP address of the NetBIOS name server.
Test:	Select this check box if you want the connection to the WINS server to be verified before you save the settings.
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.
Only for Preset Shares:	Select this check box to only enable dynamic folder creation for preset shares created by an Administrator. If a user enters a share path manually that does not exist, the share is not dynamically created when a user scans a document.

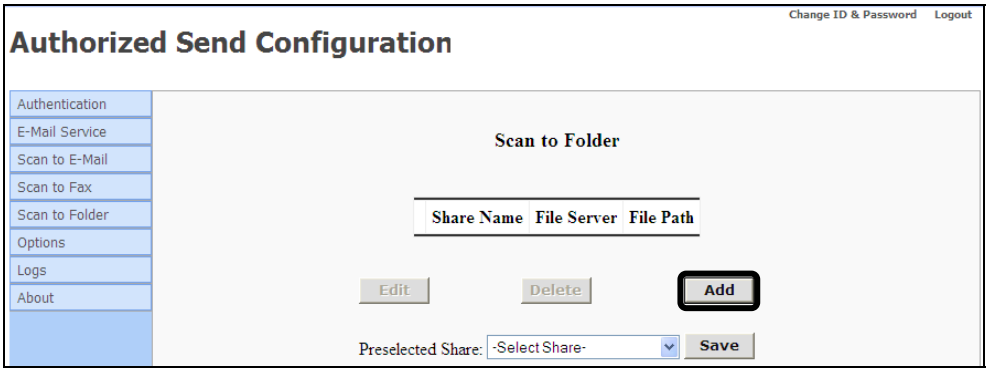
3.12 Creating a Preset Share

You can create a maximum of 10 preset shares.

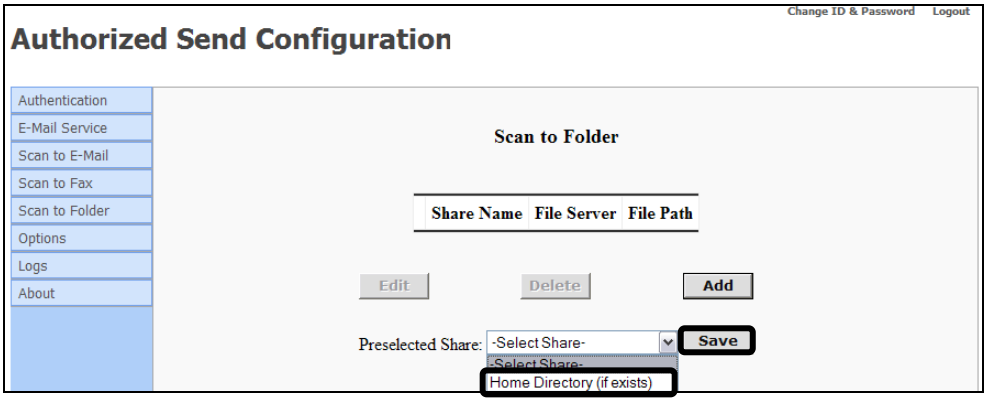
1. Click [Scan to Folder] ➞ [Preset Shares].

   If necessary, see the screen shot in step 16 of "Flow of Configuration Operations," on p. 31.

2. Click [Add].



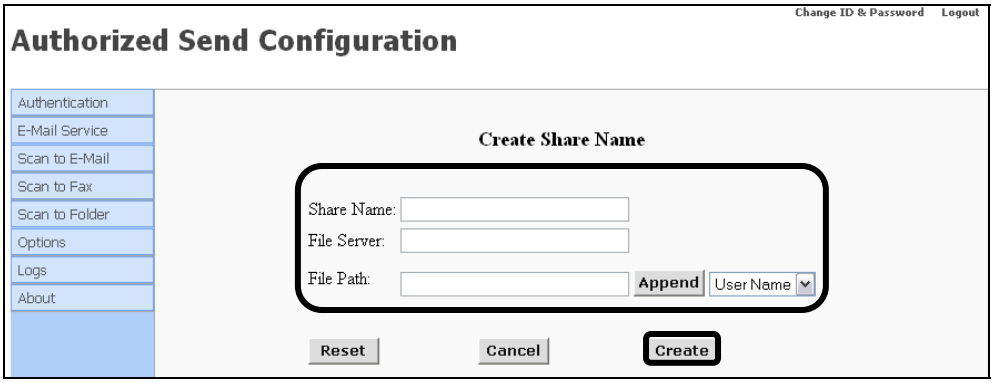
If you want to specify your home directory as a preselected share that will automatically appear in the Preset Share drop-down list on the SCAN TO FOLDER screen, select [Home Directory (if exists)] from the Preselected Share drop-down list ➞ click [Save].



NOTE

If you do not have a Home Directory, or if you do not select [Home Directory (if exists)] from the Preselected Share drop-down list, no share will appear on the SCAN TO FOLDER screen.

3. Specify the Share Name settings → click [Create].



Create Share Name

Share Name: Enter a name for the preset share.

File Server: Enter the DNS name or IP Address to send documents.

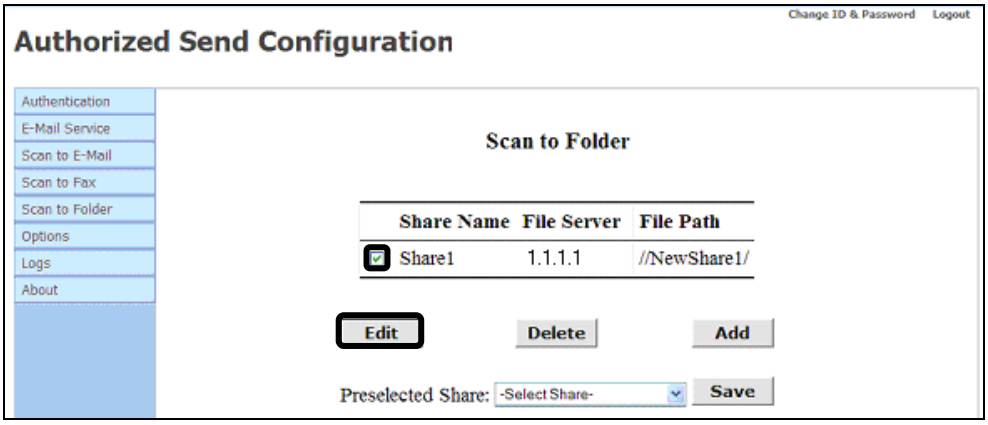
File Path: Enter the path of the folder to send documents.

Append: Click [Append] to add a user's name to the string in the [Share Path] text box.

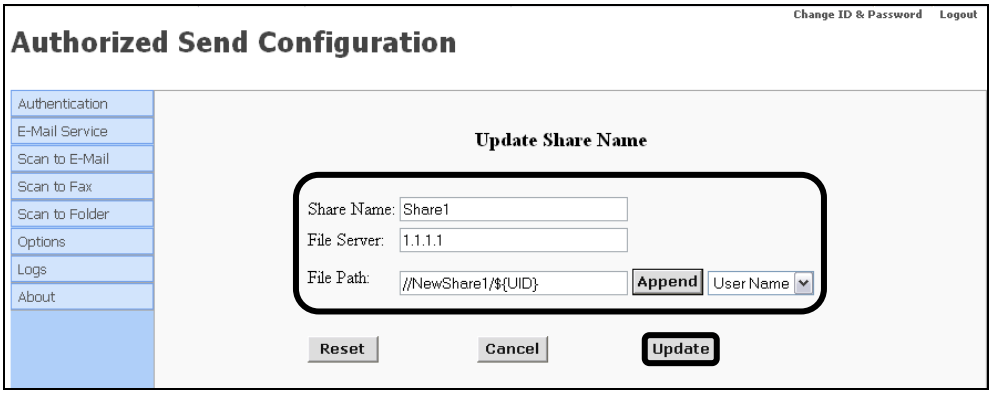
3.13 Editing a Preset Share

You can edit a previously created preset share from the Scan to Folder configuration screen.

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



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



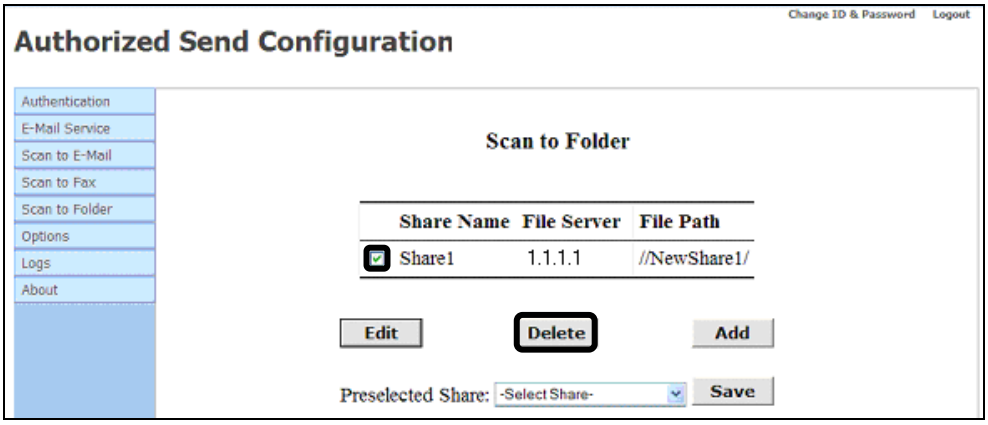
If you make a mistake, click [Reset] to return the settings to their original values.

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

3.14 Deleting a Preset Share

You can delete a previously created preset share from the Scan to Folder 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.

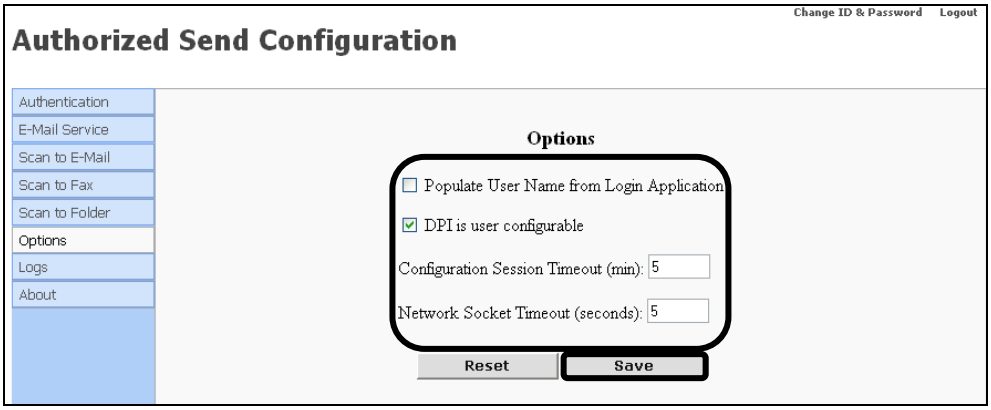
3.15 Configuring Optional Settings

You can configure the timeout settings, decide whether to populate the User Name text field on the Authorized Send Login screen, and set to enable the Resolution drop-down list on the Scan Settings screen of the Authorized Send UI.

1. Click [Options].

   If necessary, see the screen shot in step 18 of "Flow of Configuration Operations," on p. 31.

2. Specify the settings under Options as necessary → click [Save].



Options

Populate User Name from Login Application:	Select this check box to have the [User Name] text box on the Authorized Send Login screen automatically populated with the user's name from the MEAP device's login application (if used). If no login application is used, the user must enter their log on name manually.
DPI is user configurable:	Select this check box to enable the Resolution drop-down list on the Scan Settings screen of the Authorized Send UI. If this check box is selected, users can change the send resolution from the Resolution drop-down list. If this check box is not selected, the send resolution is set to '200 x 200 dpi', and users cannot change it.

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.
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.

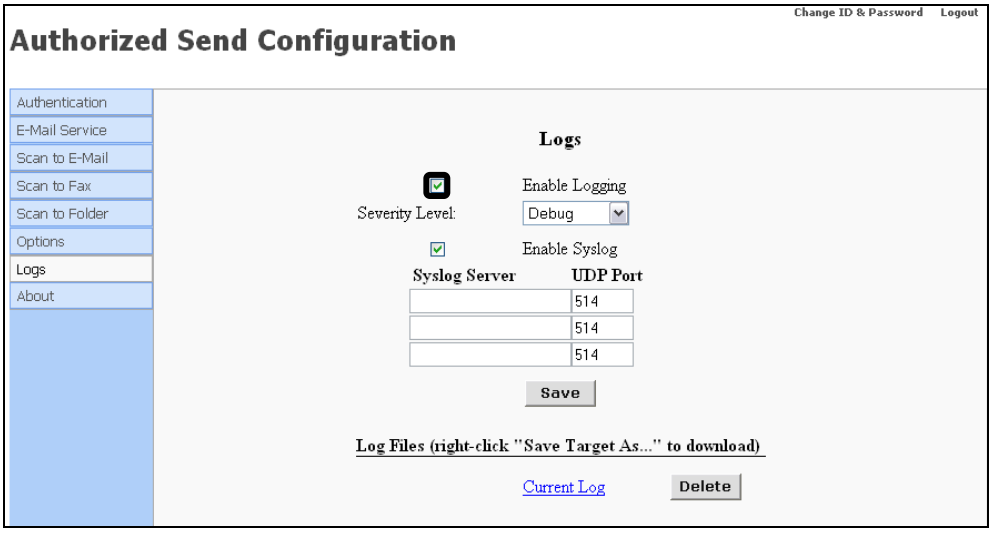
3.16 Configuring Log Settings

You can enable the Log function and view or delete the current log file.

1. Click [Logs].

   If necessary, see the screen shot in step 20 of "Flow of Configuration Operations," on p. 31.

2. Click the [Enable Logging] check box.



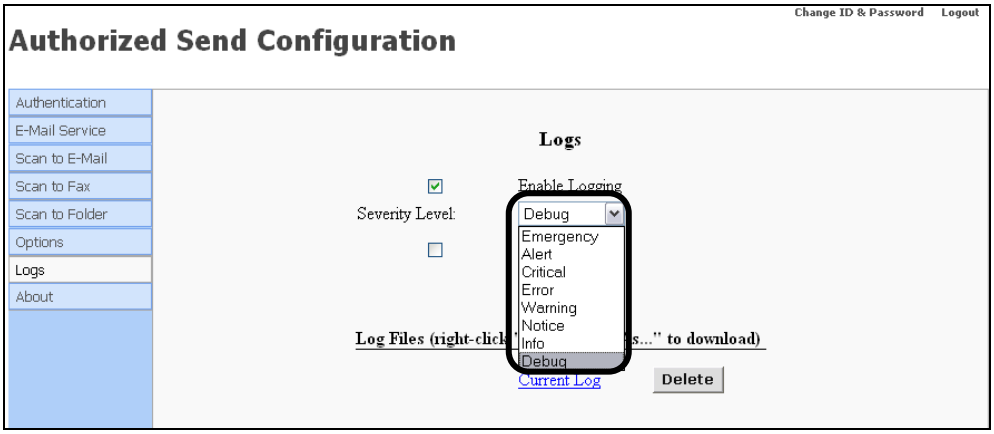
When the [Enable Logging] check box is selected, Authorized Send will log debug and error messages up to a maximum file size of 1 MB (1,024 KB).

There are 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.

3. Select the severity level from the Severity Level drop-down list.



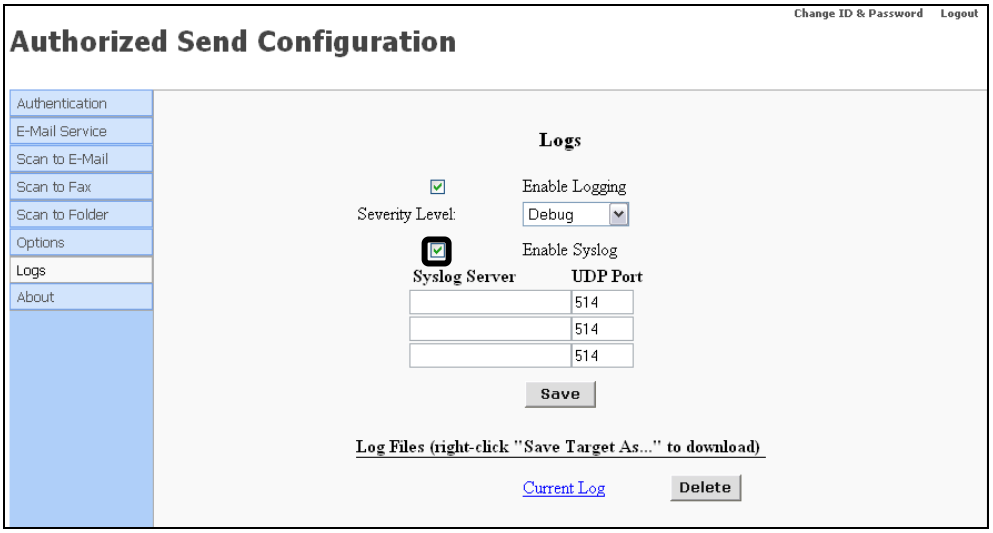
The table below shows the supported levels of severity and their respective numerical codes.

Severity Level	Numerical Code
Emergency	0
Alert	1
Critical	2
Error	3
Warning	4
Notice	5
Informational	6
Debug	7

When you select a severity from the drop-down list, that severity and all severities with a lower numerical value are logged.

The default value is ‘Debug’. If [Debug] is selected, all severities are logged.

4. Select the [Enable Syslog] check box.



If you select the [Enable Syslog] check box, at least one syslog server must be configured.

Authorized Send supports only the user-level messages (Numerical Code = 1) and security/authorization messages (Numerical 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.

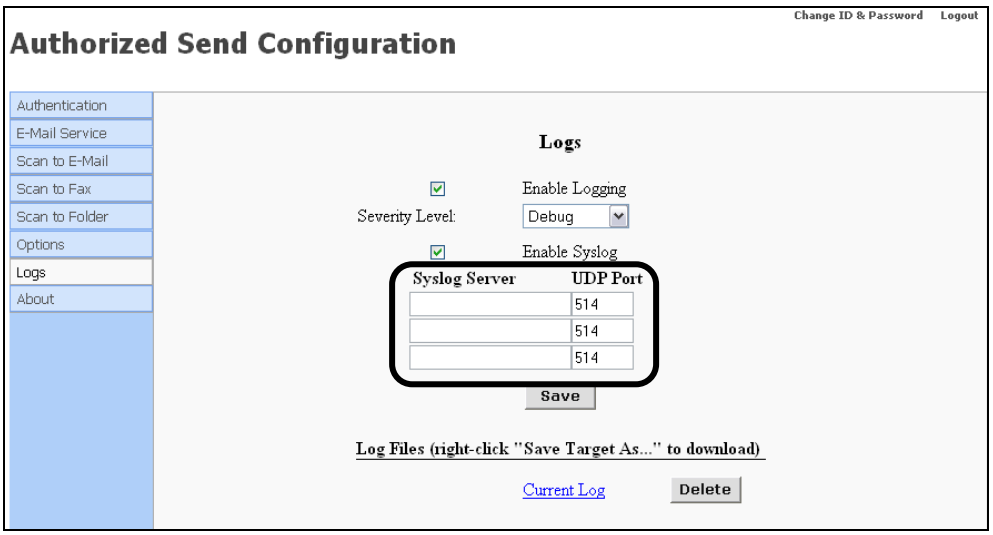
Messages are logged in the following format:
<PRI#> HEADER MSG

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 login failed.

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 in the <Syslog Server> column in the table → enter the corresponding UDP (User Datagram Protocol) port number for the syslog server in the <UDP Port> column in the table.



You can configure up to three syslog servers.

6. Click [Save].

7. To view the log file, click [Current Log] or [History Log].

   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 Log function, click the [Enable Logging] check box to clear the check mark → click [Save].

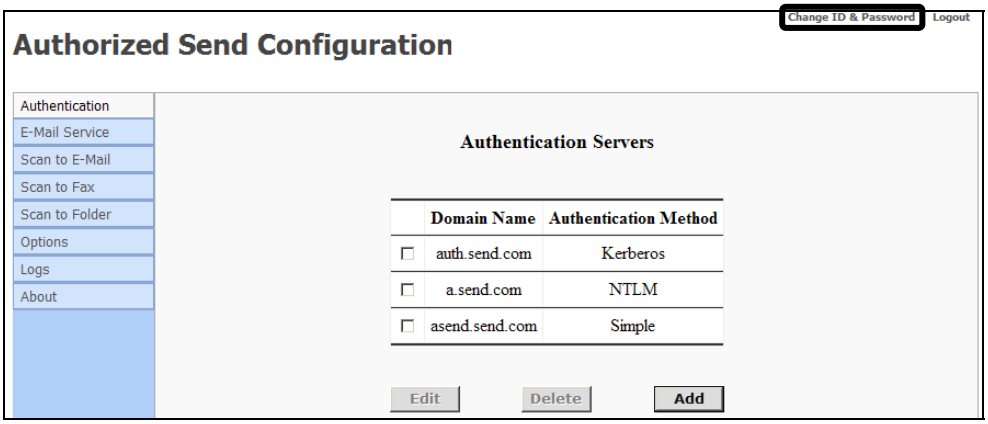
3.17 Changing the Login ID and Password

You can change your Login ID and password to log on to the Authorized Send Configuration servlet.

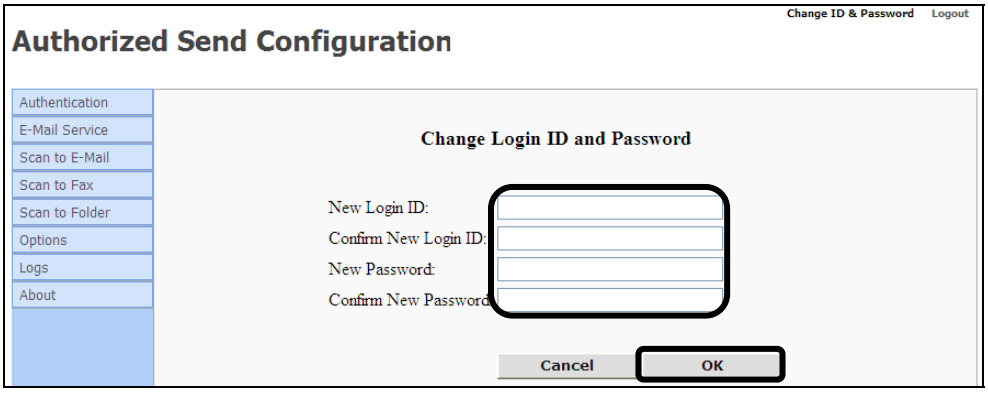
1. Display the Authorized Send Configuration screen and log on to the Authorized Send Configuration servlet.

   If necessary, see steps 1 and 2 of "Flow of Configuration Operations," on p. 31.

2. Click [Change ID & Password].



3. Enter the new login ID → confirm the ID → enter the new password → confirm the password → click [OK].



If you want to cancel changing the login ID and password, press [Cancel].

3.18 Brand Configuration Tool (Optional)

This section describes how to dynamically modify the appearance of the end 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.

3.18.1 Using the Brand Configuration Tool

This section describes how to use the Brand Configuration tool.

---

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

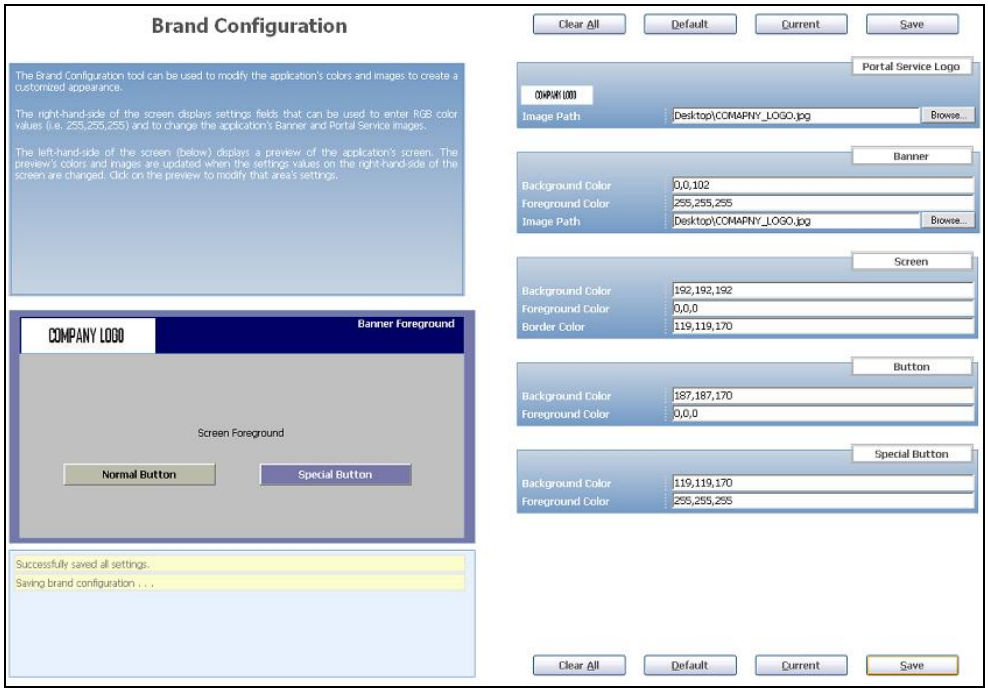
   http://<device IP>:8000/AuthSendConfiguration/branding

   (Replace <device IP> with the IP address of the MEAP device.)

IMPORTANT

Enter **AuthSendConfiguration/branding** exactly as shown, as it is case-sensitive.

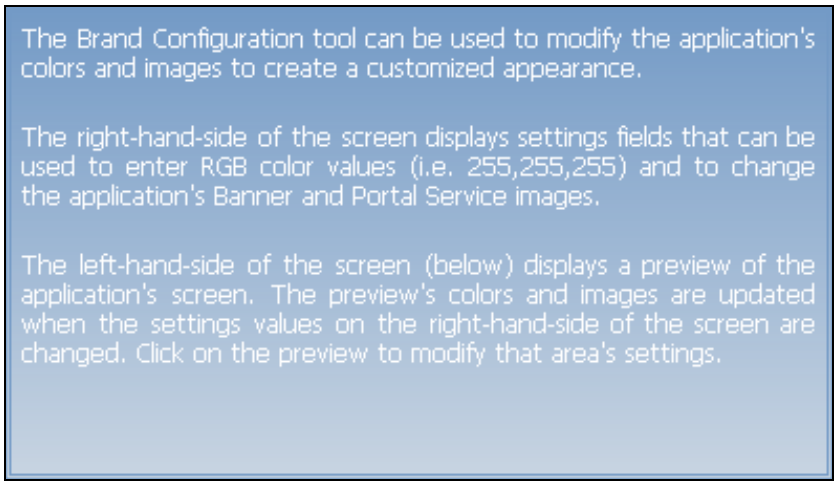
The Brand Configuration tool screen appears.



The following section describes the different areas that make up the Brand Configuration tool screen.

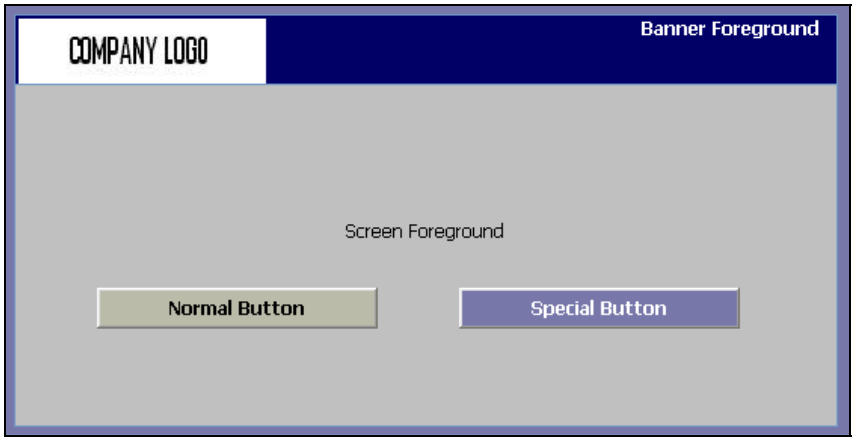
Description Area:

The description area displays an explanation of the Brand Configuration tool's purpose.



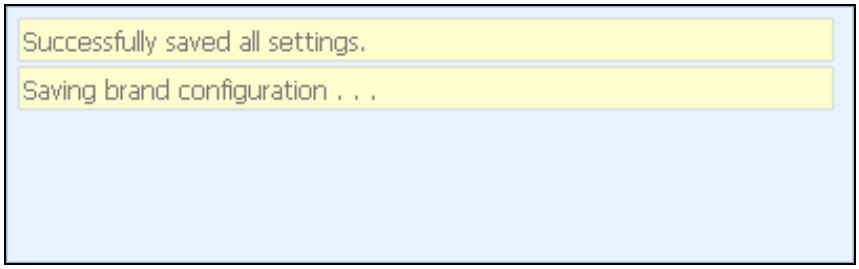
Preview Area:

The preview area displays a preview of how the end 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.



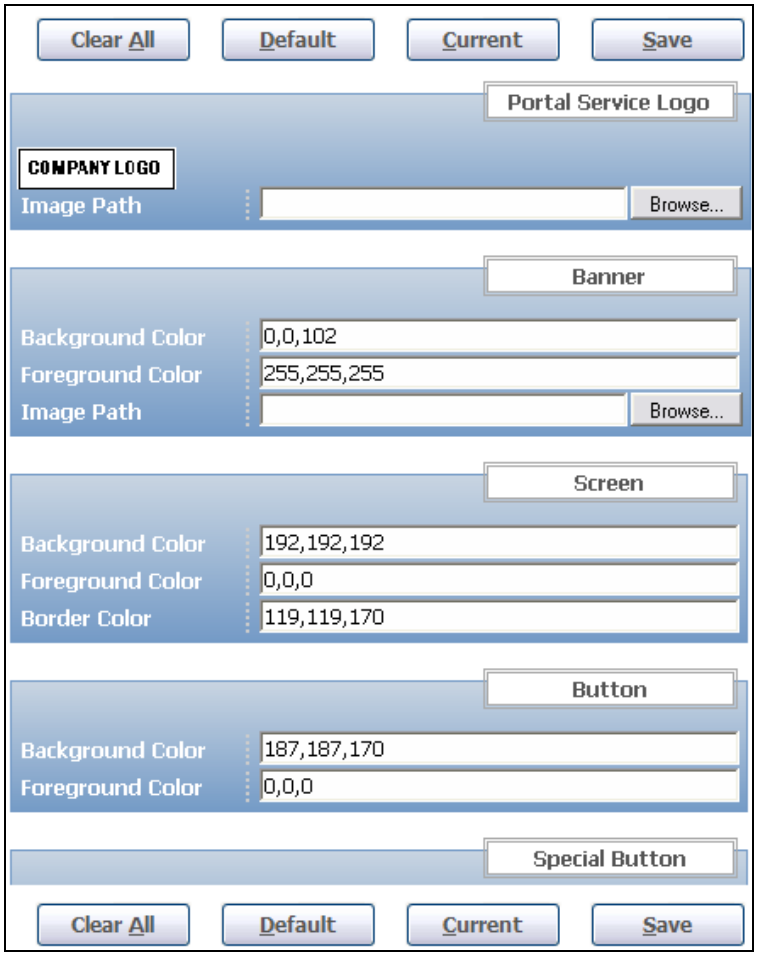
Status Area:

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 scrollbar appears to enable you to view the entire message.



Settings Area:

The settings area displays the fields 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 field for entering the location of the application logo you want, and provides a preview of the selected image.

Banner:

The Banner area provides text fields for specifying the background and foreground colors, and entering the location of the banner you want.

Screen:

The Screen area provides text fields for specifying the background, foreground, and border colors.

Button:

The Button area provides text fields for specifying the background and foreground colors for normal buttons. A normal button is any button except for the Login and Logout buttons.

Special Button:

The Special Button area provides text fields for specifying the background and foreground colors for special buttons. The special buttons are the Login and Logout buttons.

2. Select [Clear All], [Default], or [Current].

[Clear All]: Click to clear all of the settings.

[Default]: Click to load the default values for each setting and populate the corresponding fields in the settings area.

[Current]: Click to load the currently saved values for each setting and populate the corresponding fields in the settings area.

2.1 If you want to specify the end user's interface portal service logo:

Click the [Image Path] text field 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.

2.2 Click [Save] to save the settings currently displayed in the settings area, and to update the end 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.

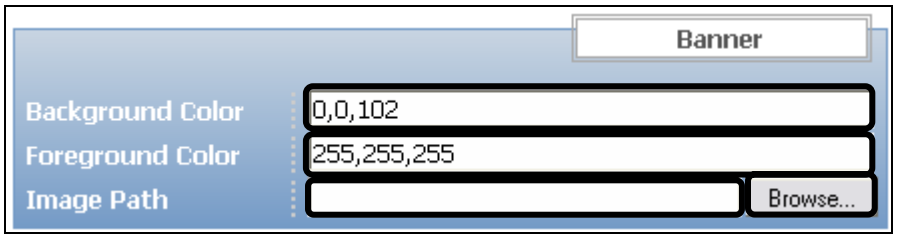
NOTE
The recommended image size is 88 pixels (W) x 23 pixels (H).

3. If you want to specify the background and foreground colors, and select the image to be displayed in the end user's interface banner area:

   3.1 Click the [Background Color] text field under <Banner> ➞ enter three comma-separated digits representing the desired RGB color.

   3.2 Click the [Foreground Color] text field under <Banner> ➞ enter three comma-separated digits representing the desired RGB color.

   3.3 Click the [Image Path] text field 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.



   3.4 Click [Save] to save the settings currently displayed in the settings area, and to update the end 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.

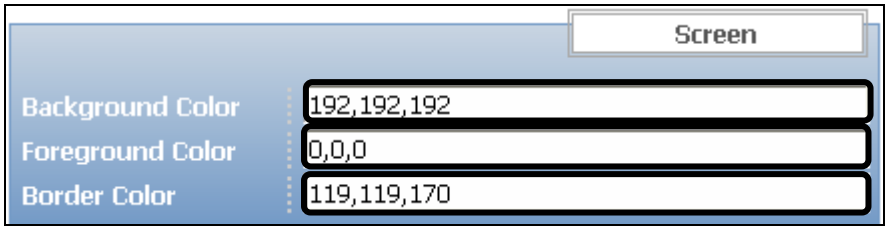
NOTE
The recommended image size is 164 pixels (W) x 43 pixels (H).

4. If you want to specify the background, foreground, and border colors to be displayed in the end user's interface screen area:

   4.1 Click the [Background Color] text field under Screen → enter three comma-separated digits representing the desired RGB color.

   4.2 Click the [Foreground Color] text field under Screen → enter three comma-separated digits representing the desired RGB color.

   4.3 Click the [Border Color] text field under Screen → enter three comma-separated digits representing the desired RGB color.



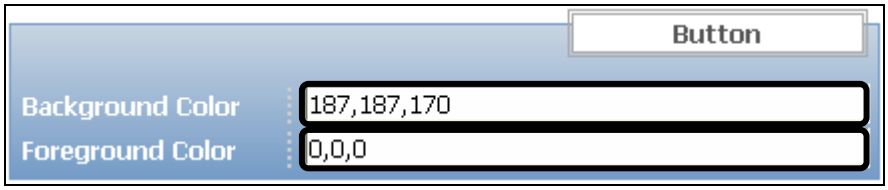
   4.4 Click [Save] to save the settings currently displayed in the settings area, and to update the end user's interface screen to use the new settings.

   The preview area displays the updated colors.

5. If you want to specify the end user's interface background and foreground colors for the normal buttons:

   5.1 Click the [Background Color] text field under Button → enter three comma-separated digits representing the desired RGB color.

   5.2 Click the [Foreground Color] text field under Button → enter three comma-separated digits representing the desired RGB color.



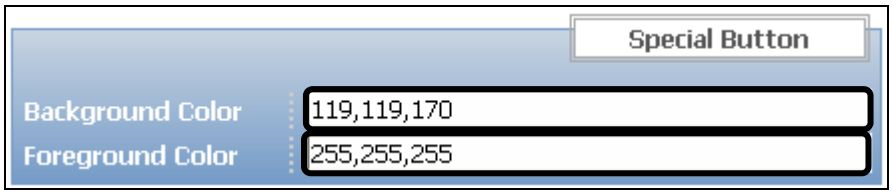
   5.3 Click [Save] to save the settings currently displayed in the settings area, and to update the end user's interface normal buttons to use the new settings.

   The preview area displays the updated colors.

6. If you want to specify the end user's interface background and foreground colors for the special buttons:

   6.1 Click the [Background Color] text field under Special Button → enter three comma-separated digits representing the desired RGB color.

   6.2 Click the [Foreground Color] text field under Special 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 end user's interface special buttons to use the new settings.

   The preview area displays the updated colors.

Chapter 4 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.

4.1 Device Configuration

This section describes how to set up your MEAP device for use with Authorized Send.

IMPORTANT

Inbox 99 must be available for use on the MEAP device (i.e., no documents stored), and with no password protection. Authorized Send temporarily stores scanned images in this inbox, and therefore, it is important that Inbox 99 have sufficient space available for these images to be stored. The images are automatically erased from Inbox 99 after scanning is complete.

4.1.1 Setting Up DNS Server Settings

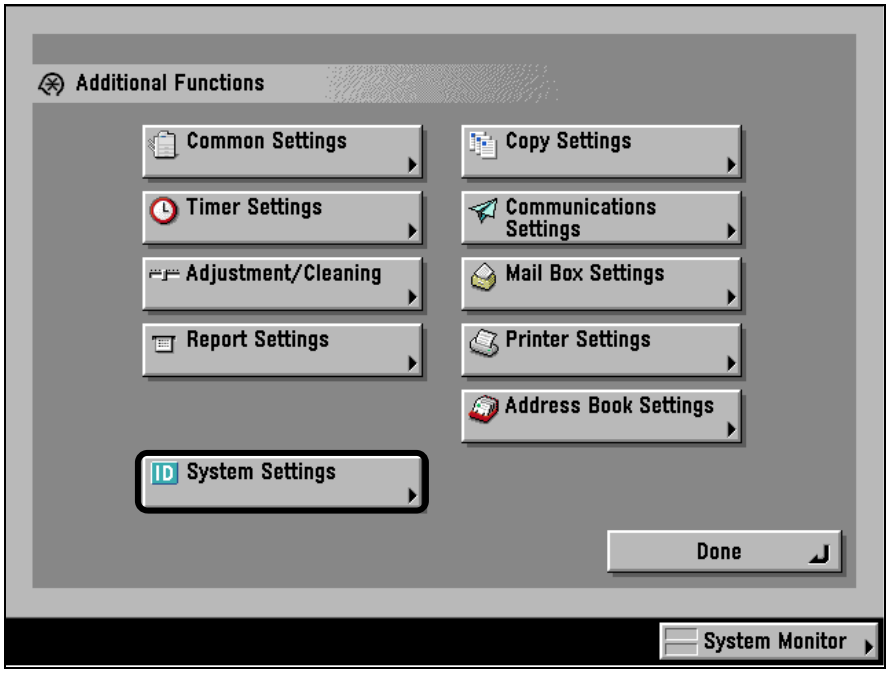
After the servers and operating environment is set up, and Authorized Send is installed and configured properly, you must configure your MEAP-enabled device.

Follow the procedure below to configure the MEAP device for Authorized Send.

---

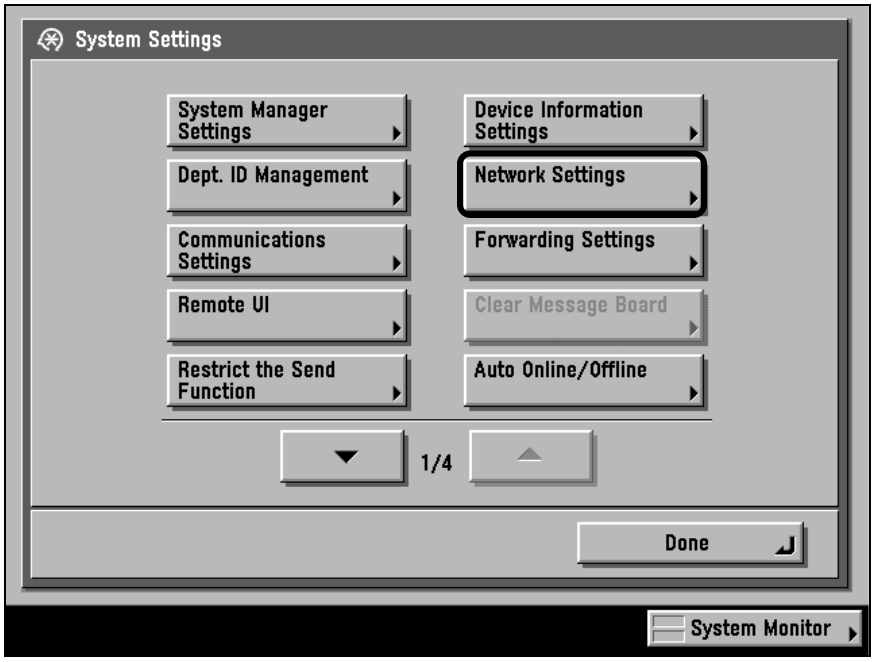
1. On the machine's control panel, press (Additional Functions).

2. Press [System Settings].



If the System Manager ID and System Password have been set, enter the System Manager ID and System Password using ⓪ – ⑨ (numeric keys) → press ⓘⓓ (Log In/Out).

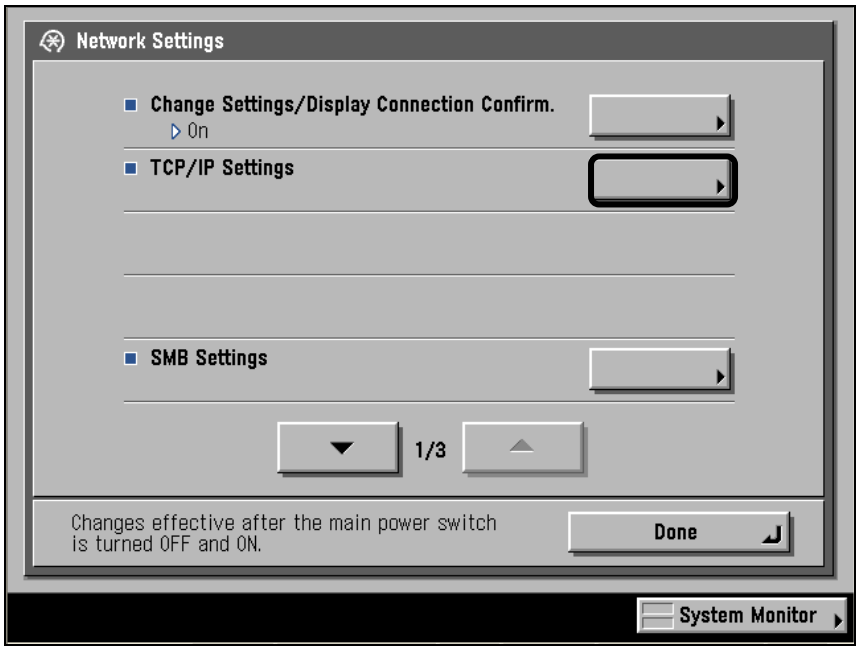
3. Press [Network Settings].



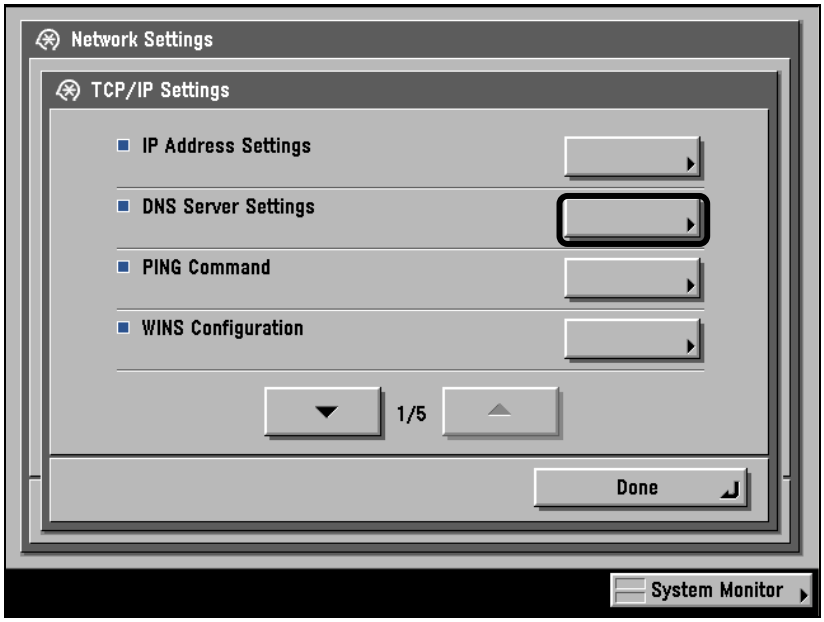
NOTE

If the desired setting is not displayed, press [▼] or [▲] to scroll to the desired setting.

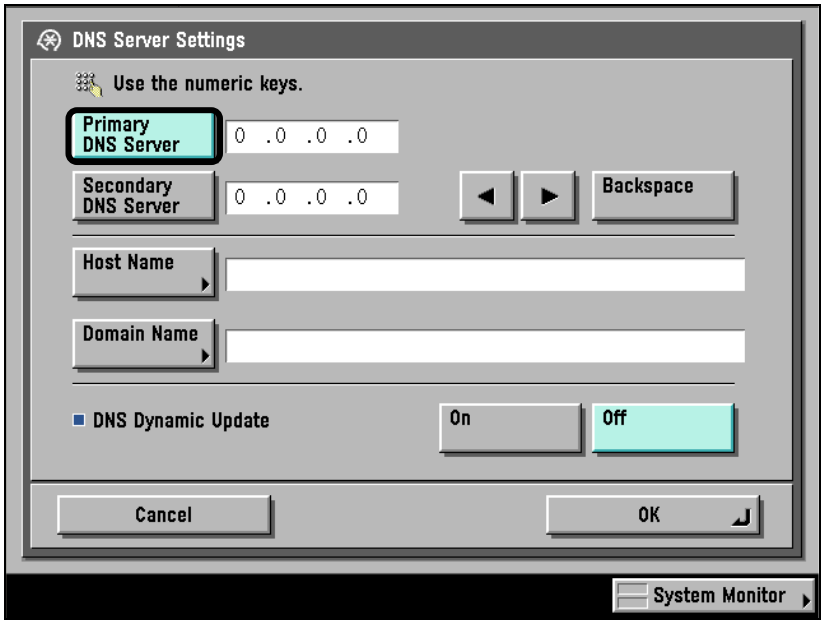
4. Press [TCP/IP Settings].



5. Press [DNS Server Settings].



6. Press [Primary DNS Server] → enter the IP address using ⓪ – ⑨ (numeric keys).



IMPORTANT

- It is not necessary to enter a [Secondary DNS Server] or [Host Name]; however, you must enter a [Domain Name].
- If you are using SMTP Authentication, make sure that the host name does not contain spaces (including trailing spaces) or trailing periods.

7. Press [Domain Name] → enter the domain name → press [OK].

8. Press [OK].

9. Press [Done] repeatedly until the Basic Features screen appears.

10. Restart the machine.

IMPORTANT
The MEAP device must be restarted before the settings can take effect.

4.1.2 Specifying the Auto Clear Mode for Auto Log Out

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 will be logged out of Authorized Send. This period of time is called the "Auto Clear Time."

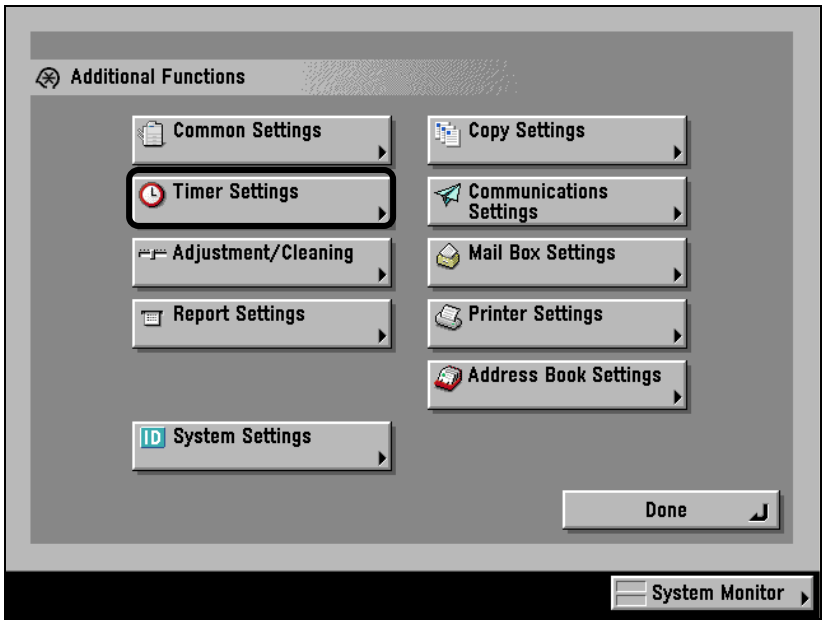
The Auto Clear Time mode can be set from ‘0’ to ‘9’ minutes in 1 minute increments, and can also be set to 'Off'.

NOTE
- If '0' is selected, the Auto Clear Time mode is not set.
- The default setting is '2' minutes.

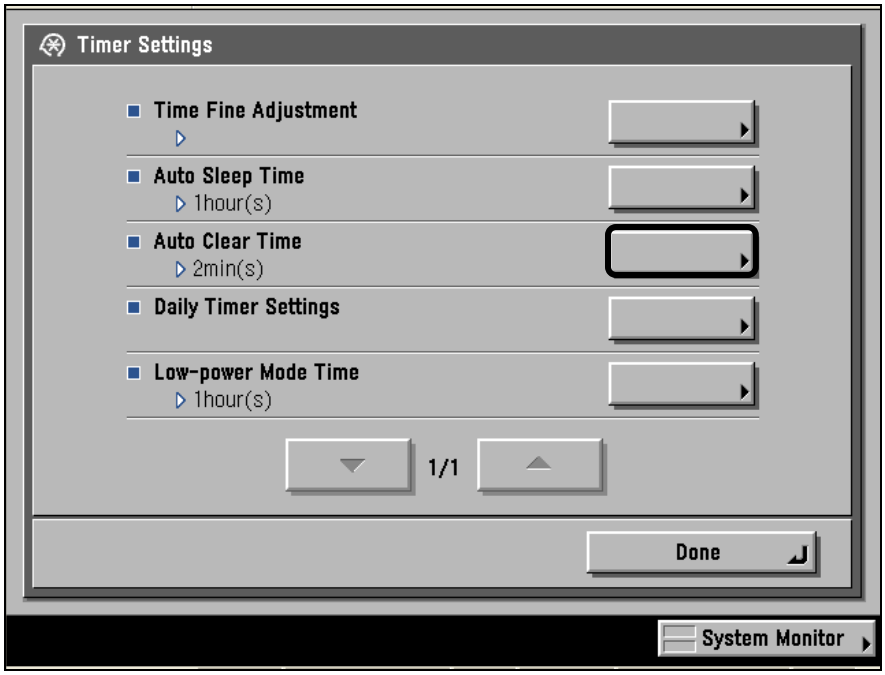
---

1. On the machine’s control panel, press (Additional Functions).

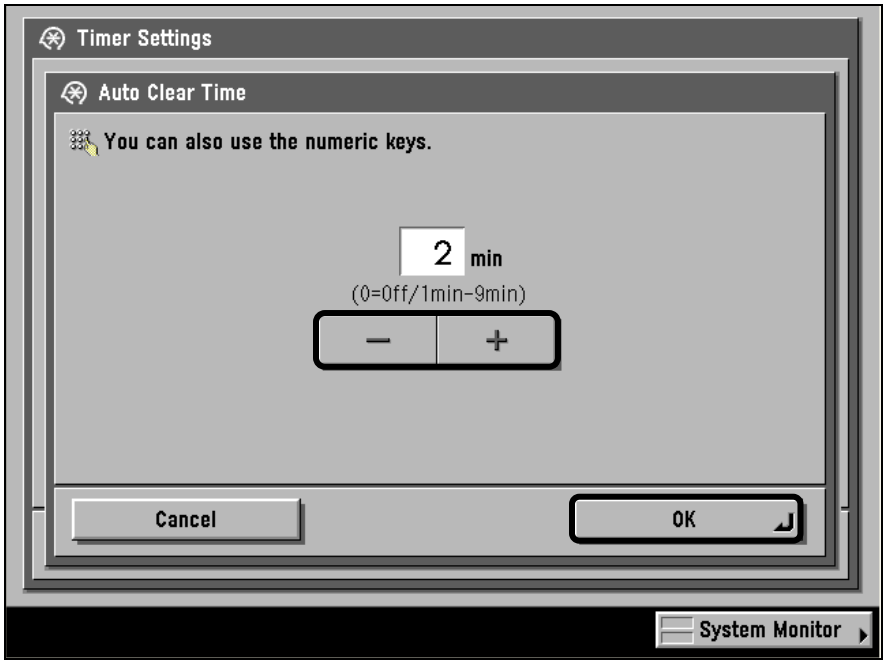
2. Press [Timer Settings].



3. Press [Auto Clear Time].



4. Press [-] or [+] to specify the desired Auto Clear Time → press [OK].



You can also enter values using ⓪ – ⑨ (numeric keys).

5. Press [Done] repeatedly until the Basic Features screen appears.

4.1.3 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.

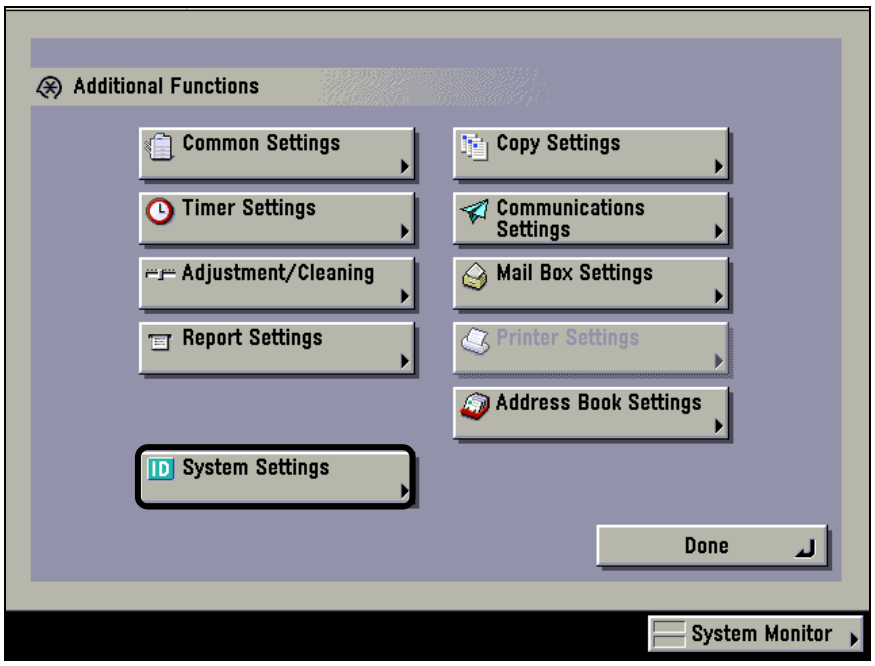
4.1.3.1 Specifying Automatic Time Synchronization

You can set the SNTP (Simple Network Time Protocol) settings to enable the device to automatically synchronize its system time with a public time server.

---

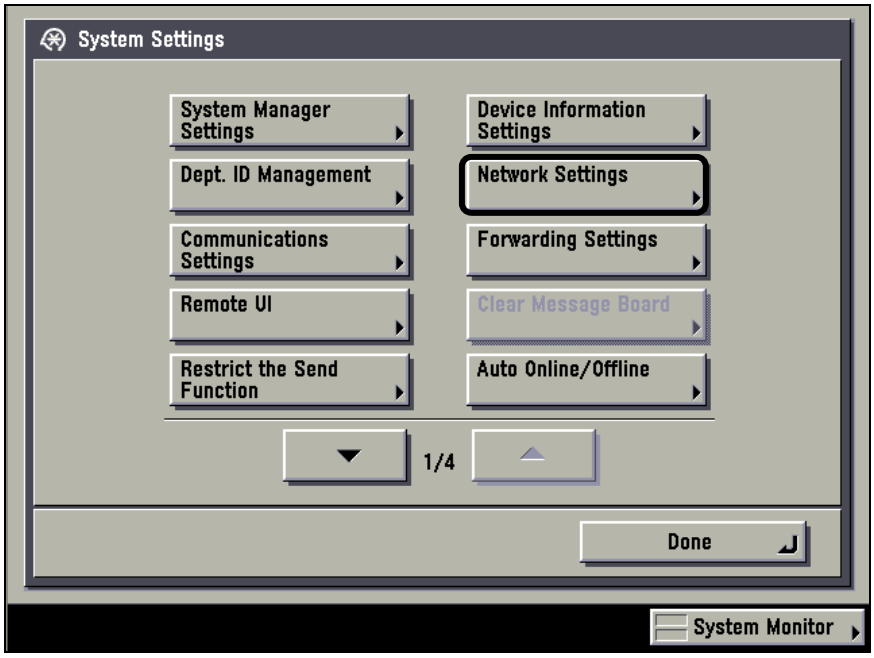
1. On the machine's control panel, press ⚙ (Additional Functions).

2. Press [System Settings].

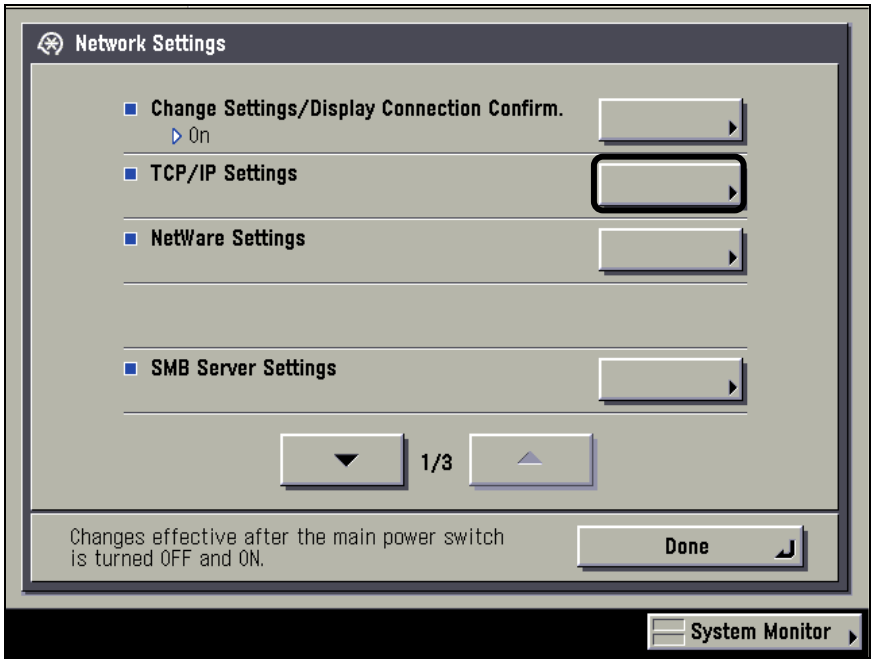


If the System Manager ID and System Password have been set, enter the System Manager ID and System Password using ⓪ – ⑨ (numeric keys) → press ID (Log In/Out).

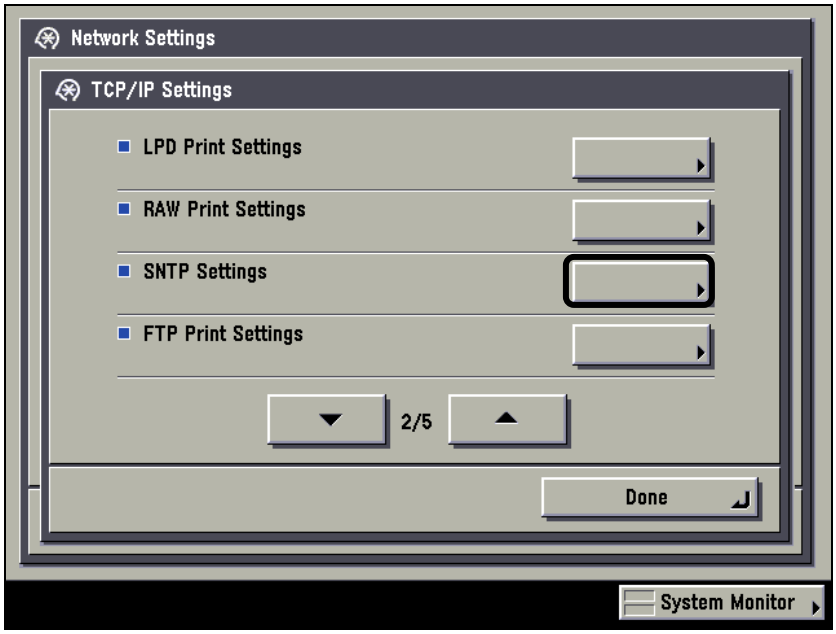
3. Press [Network Settings].



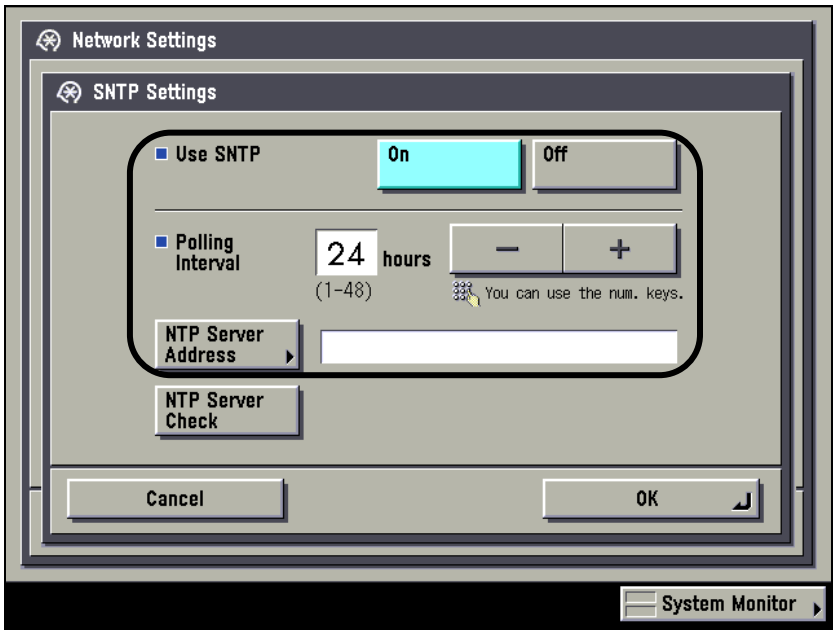
4. Press [TCP/IP Settings].



5. Press [SNTP Settings].



6. Specify the SNTP settings.

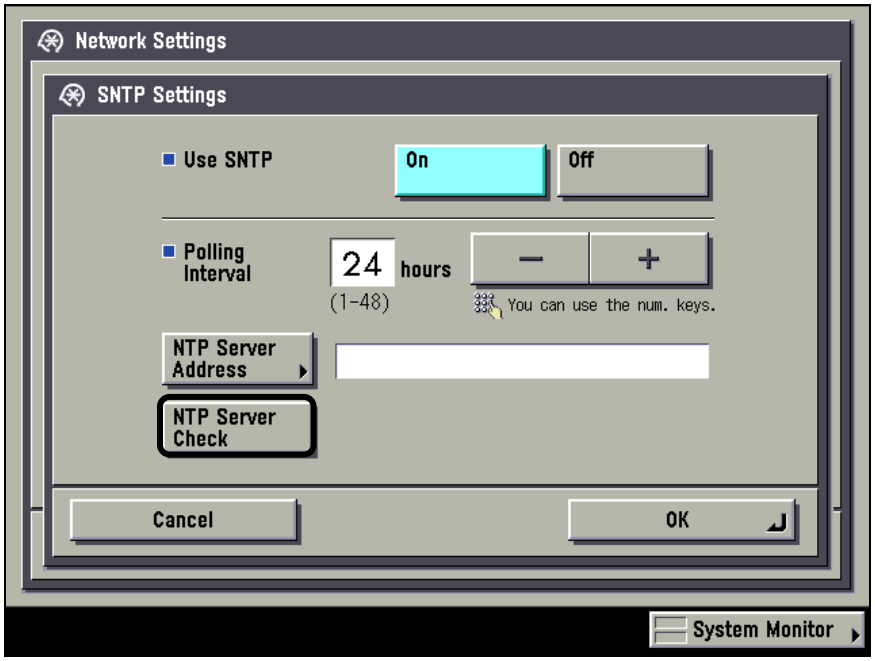


<Use SNTP>: Select [On] to perform time synchronization using SNTP.

<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 [NTP Server Check] to check the status of the NTP server.



If <OK> is displayed next to [NTP Server Check], time synchronization is working correctly via SNTP.

If <Error> is displayed next to [NTP Server Check], check the settings for [NTP Server Address] set in step 6.

8. Press [OK].

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 *Reference Guide* that came with your machine.

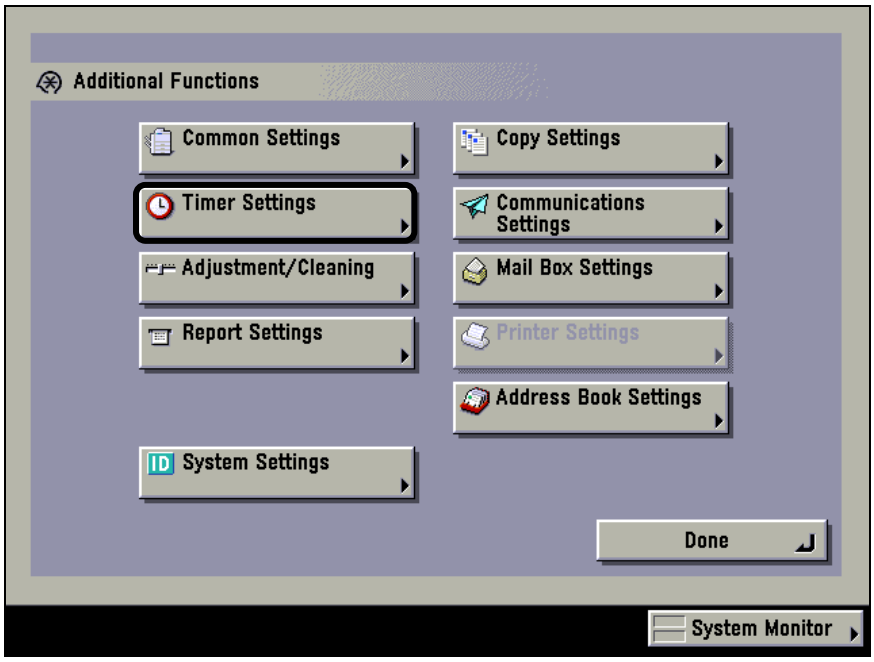
9. Press [Done] repeatedly until the Basic Features screen appears.

4.1.3.2 Manually Adjusting the Device Time

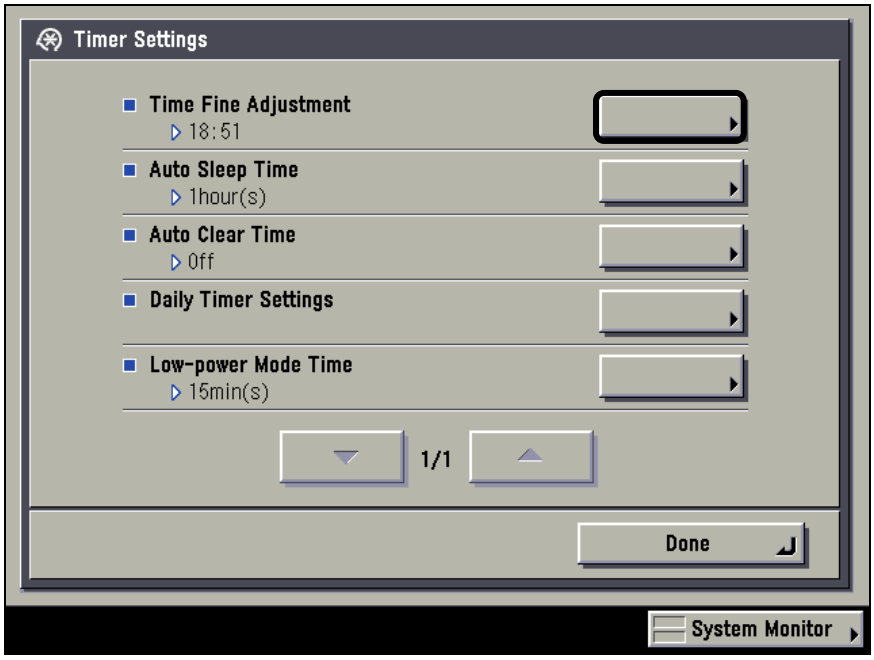
You can manually adjust the device time to match the Kerberos authentication server or address book server time.

1. On the machine's control panel, press (Additional Functions).

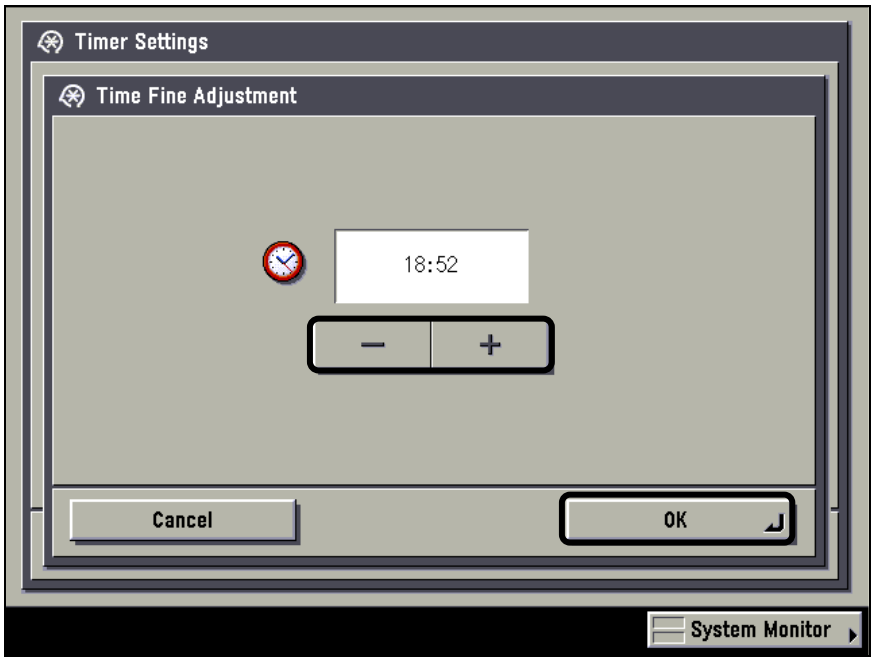
2. Press [Timer Settings].



3. Press [Time Fine Adjustment].



4. Press [-] or [+] to adjust the time as necessary → press [OK].



5. Press [Done] repeatedly until the Basic Features screen appears.

Chapter 5 Troubleshooting

This chapter explains the various issues that may arise when installing and configuring the necessary components of the Authorized Send application, along with possible causes and remedies.

Problem You cannot connect to the network.

Remedy Make sure that:

- The IP addresses of the MEAP device and server PCs are correct, and that you can ping the device.
- The server PC is on the network.
- You are not using a proxy server.

Problem The Authorized Send application is not functioning properly.

Remedy Verify that the supported MEAP contents and system software versions are installed on the MEAP device. Please see the Readme.doc file for supported versions.

Problem When creating a share name on the Authorized Send Configuration screen, the message <Connection failed. Could not resolve host name: xxx.> appears.

Remedy Make sure that the MEAP device is on the same domain as your domain controller. (See "Setting Up DNS Server Settings," on p. 111.)

Problem Cannot access SMS.

Remedy Two people cannot be logged on to SMS at the same time. Make sure that you are the only one logged on to SMS, and that you have the correct IP address and port number (:8000).

Problem The Authorized Send application cannot be installed or started.

Remedy Check to make sure that:

- Another application is not using resources.
- An authorized copy of the software is being used.

Problem The [Scan to E-Mail] button is disabled.

Remedy Check to make sure that:

- An e-mail address is specified in the user's Address Book account.
- An SMTP server address is configured for Authorized Send.
- For more information, see "LDAP Failure Notification Messages," on p. 130.

IMPORTANT

It is necessary for the user to logout, and then log back in after the changes mentioned above have been made to activate the [Scan to E-Mail] key.

Problem The Browse feature in the Scan to Folder function only displays non-hidden and non-system shares (i.e., the first level directory under the root is not displayed in the Browse window).

Remedy Specify the first level directory share in the path field, and then you can browse from this directory.

Problem The Address Book feature in the Scan to E-mail function does not work.

Remedy Make sure that the correct Base DN (Distinguished Name) is entered in the [E-Mail Service] → [Address Book] tab in the Authorized Send Configuration servlet. (See "Creating an Address Book Server," on p.57.)

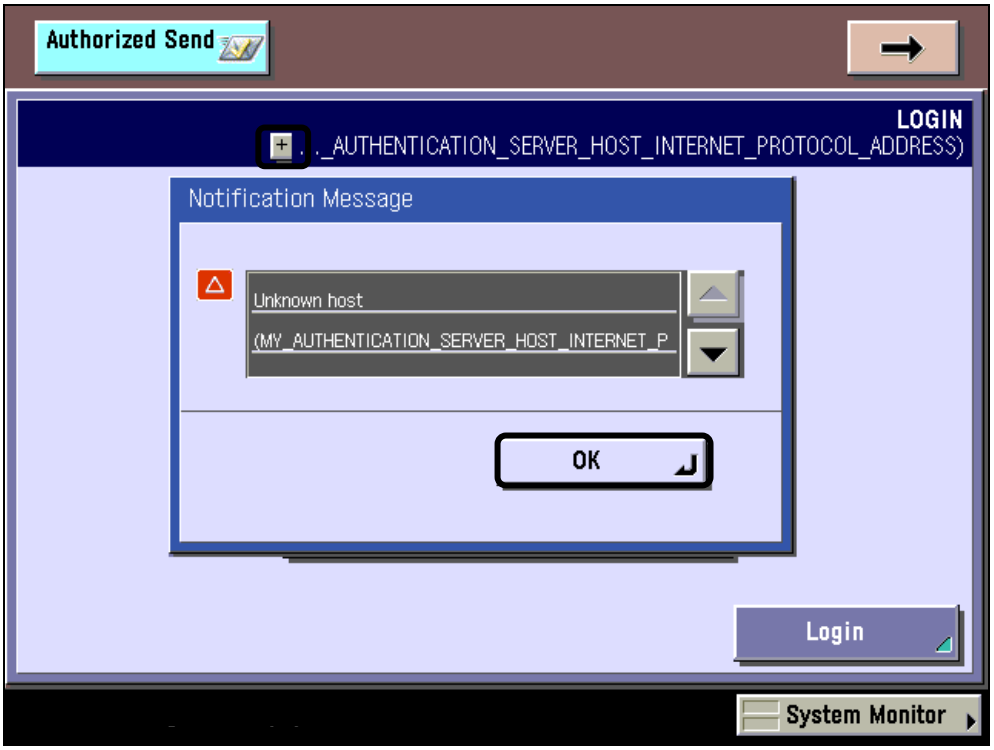
Chapter 6 List of Error Messages

This chapter explains the various messages that appear on the touch panel display of the MEAP device, along with possible causes and remedies.

Any words that appear italicized are variables, and will be replaced with their corresponding values on the actual application screen.

NOTE

If an error message is too long to display in full in the Message Notification Section, click [⊞] next to the message to display a pop-up dialog box containing the full text of the error message → click [OK] to close the dialog box.



6.1 Login Screen Notification Messages

The Login screen notification messages are displayed on the Login screen in the upper right hand portion. You will remain at the Login screen until they are resolved.

6.1.1 General Authentication Notification Messages

This section explains the general authentication notification messages, along with possible causes and remedies.

Message	Cause	Remedy
User name and password fields cannot be empty	The user name field or password field is blank.	Enter values for the user name and password fields, and do not leave them blank.
Please contact administrator to configure this device	You are attempting to log on to a MEAP device that has not been configured by an administrator.	Authorized Send has not been configured (configuration servlet). Configure the settings on the configuration servlet.
Server connect error, connection timed out *(host)*	The log on authentication process exceeds the specified Network Socket Timeout on the Options tab of the configuration servlet. The default setting is '5' seconds.	• Check that the configured servers are active. • Try to PING the servers from the MEAP device. • Increase the Network Socket Timeout on the configuration servlet.
User Name cannot be longer than 20 characters	The user name field exceeds 20 characters.	Make sure your user name is no longer than 20 characters.
Check User Name and Password and try again	The entered user name or password is incorrect.	Enter the correct user name or password.

6.1.2 Kerberos Authentication Notification Messages

This section explains the Kerberos authentication notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Kerberos requires username, password, host and domain	The entered user name or password is blank, or the configuration servlet's host or domain value is blank.	Verify and reconfigure the authentication server settings for the appropriate authentication server on the configuration servlet, and try to log on again.
Kerberos bind failed, no connection to (*host*)	A Kerberos bind is attempted, and an LDAP connection has not established.	Check your Kerberos configuration.
Kerberos bind failed, LDAP ticket to (*host name*)	A Kerberos session could not be established.	• Check your Kerberos configuration. • Ensure that the configured server's host name is correct.
Kerberos bind failed to host *(host)* hostname (*host name*)	A Kerberos bind is unsuccessful to the specified host and host name.	Check your Kerberos configuration.
Unable to get LDAP ticket to (*host name*)	An LDAP ticket to the host name could not be acquired.	• Check your Kerberos configuration. • Ensure that the configured server's host name is correct.
Clock skew exceeds maximum tolerance at host (*host*)	The MEAP device clock and KDC server clock are not within the server specified maximum clock skew tolerance. The default setting for a Windows 2000 or Windows 2003 server is '5' minutes.	Verify that the MEAP device clock and configured server clock are in sync within the server maximum clock skew tolerance. For more information, see "Synchronizing the Device and Server Time," on p. 117.
Unable to connect to KDC at host (*host*)	A connection to the KDC at the specified host cannot be reached.	• Check your Kerberos configuration. • Ensure that the configured server is active.
Unable to connect to KDC at domain (*domain*)	Insufficient cross realm privileges are configured for the MEAP device's domain.	• Check your Kerberos configuration. • Verify the Kerberos cross-realm configuration.

Message	Cause	Remedy
Unknown host (*host*)	The host cannot be resolved.	• Check your Kerberos configuration. • Ensure that the configured server is active.
An unknown Kerberos error has occurred	Any other Kerberos error message that has not been defined as caught has occurred.	Check your Kerberos configuration.

6.1.3 NTLM Authentication Notification Messages

This section explains the NTLM authentication notification messages, along with possible causes and remedies.

Message	Cause	Remedy
NTLM requires username, password and domain	The entered user name, password, or domain is blank.	Verify and reconfigure the authentication server settings for the appropriate authentication server on the configuration servlet, and try to log on again.
NTLM bind failed, no connection to (*host*)	A NTLM bind is attempted, and an LDAP connection has not been established.	Check your NTLM configuration.
NTLM bind failed to host (*host*) domain (*domain*)	A NTLM bind is unsuccessful to the specified host and host name.	Check your NTLM configuration.
An unknown NTLM error has occurred.	Any other NTLM error message that has not been defined as caught has occurred.	Check your NTLM configuration.

6.1.4 Simple Authentication Notification Messages

This section explains the Simple authentication notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Check Public DN and Public Password and try again	The public DN and public password have been configured on the configuration servlet, however they are incorrect.	Verify the public DN and public password.
Anonymous binding not accepted by host (*host*)	The server does not allow anonymous binding, and the public DN and public password are not configured on the configuration servlet.	• Verify that anonymous connections are enabled on the server. • If anonymous connections are required to be disabled, configure the public DN and public password credentials.
Confidentiality Required	The authentication server you are using has a "Require TLS/SSL" option enabled, and Authorized Send is not using SSL for authentication.	• Disable any "Require TLS/SSL" options on the authentication server. • Enable SSL for authentication in Authorized Send. See "Creating an Authentication Server," on p. 44.

6.2 Main Screen Notification Messages

The Main screen notification messages are displayed on the Main screen in the upper right hand portion of the MEAP device's UI. If an error has occurred during the authentication process, it will be displayed here.

6.2.1 LDAP Failure Notification Messages

This section explains the LDAP failure notification messages, along with possible causes and remedies.

These errors will not prevent you from authenticating into Authorized Send. However, the Scan to E-mail and Scan to Fax keys will be disabled, and you will only be allowed to use the Scan to Folder function.

Message	Cause	Remedy
Your E-mail was not found, admin limit exceeded.	An LDAP server limit set by an admin authority has been exceeded.	Check your LDAP configuration.
Your E-mail was not found, ambiguous response.	An ambiguous response from the server was received by the client.	Check your LDAP configuration.
Your E-mail was not found, authentication not supported.	The client authentication method is not supported by the server.	• Check your LDAP configuration. • Use a different authentication method.
Your E-mail was not found, server busy.	There are too many connections to the server, and the client must wait.	• Check your LDAP configuration. • Increase the amount of connections allowed by the server. • Try authenticating later.
Your E-mail was not found, confidentiality required.	The session is not protected by a protocol, such as TLS.	• Check your LDAP configuration. • Configure Authorized Send with SSL.
Your E-mail was not found, inappropriate authentication.	During a bind operation, the client is attempting to use an authentication method that the client cannot use correctly.	Check your LDAP configuration.
Your E-mail was not found, insufficient access rights.	The client does not have sufficient rights to perform the requested operation.	Check your LDAP configuration.
Your E-mail was not found, bad attribute.	A bad LDAP object has been specified.	Check your LDAP configuration.

Message	Cause	Remedy
Your E-mail was not found, invalid credentials.	Invalid credentials have been supplied by the client.	Check your LDAP configuration.
Your E-mail was not found, invalid DN syntax.	Invalid DN syntax has been supplied by the client (for example, an invalid search root is entered for the authentication server settings on the configuration servlet).	• Check your LDAP configuration. • Ensure that the configured search root in the authentication server settings on the configuration servlet is correct.
Your E-mail was not found, LDAP not supported.	LDAP is not a supported protocol on the server.	Check your LDAP configuration.
Your E-mail was not found, searched partial results.	An LDAP referral was received, but was not followed.	Check your LDAP configuration.
Your E-mail was not found, LDAP timed out.	The LDAP server has timed out.	Check your LDAP configuration.
Your E-mail was not found, no results.	No results were returned by the LDAP server.	Check your LDAP configuration.
Your E-mail was not found, bad object class.	The target object cannot be found.	Check your LDAP configuration.
Your E-mail was not found, could not handle referral.	An LDAP referral was received; however it could not be followed.	Check your LDAP configuration.
Your E-mail was not found, time limit exceeded.	The client has exceeded its operation time limit.	Check your LDAP configuration.
Your E-mail was not found, size limit exceeded.	The client has exceeded its operation size limit	Check your LDAP configuration.
Your E-mail was not found, unknown error (*resultCode*).	An unknown LDAP error was received.	Check your LDAP configuration.

6.2.2 Configuration Notification Messages

This section explains the configuration notification messages, along with possible causes and remedies.

Message	Cause	Remedy
The E-mail server has not been configured.	Bad configuration.	Configure a valid SMTP server for the appropriate address book server on the configuration servlet.

6.2.3 Warning Notification Messages

This section explains the warning notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Usernames over 20 characters may cause issues with AD.	User names that are longer than 20 characters may cause problems with Active Directory.	Make sure your user name is no longer than 20 characters.

6.3 SCAN TO E-MAIL Screen Notification Messages

The SCAN TO E-MAIL screen notification messages are displayed on the SCAN TO E-MAIL screen in the upper-right hand portion of the MEAP devices UI. As you interact with the application, different types of messages are displayed to notify you of an event.

6.3.1 Scan to E-Mail Warning Messages

This section explains the Scan to E-Mail warning messages, along with possible causes and remedies.

Message	Cause	Remedy
Scanning is disabled because the device is not ready.	The MEAP device is still in the process of sending an e-mail message, and you are attempting to start another scan.	• Wait until the MEAP device has completed the operation in progress. • Reboot the device.

6.3.2 Scan to E-Mail Input Request Messages

This section explains the Scan to E-Mail input request messages, along with possible causes and remedies.

Message	Cause	Remedy
Please specify at least one recipient.	You tried to scan a document to e-mail, but you have not specified an e-mail address.	• Specify an e-mail address. • Enable the [E-mail CC to Self] option from the [Scan to E-Mail] tab in the Configuration servlet. See "Configuring Scan to E-Mail Settings," on p.82.
Place a document in the ADF or on the Platen then close the lid.	You have not placed a document in the automatic document feeder or on the platen glass.	Place your document in the automatic document feeder or on the platen glass.
Please input subject. It is required.	The device is ready to scan a document to be e-mailed, and you did not specify a subject in the [Subject] text box.	The [Subject] text box is configured as 'Required', and you must enter a subject before the device scans and sends your document.

6.3.3 Scan to E-Mail Notification Messages

This section explains the Scan to E-Mail notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Checking SMTP Connection.	You are attempting to scan and send a document via SMTP.	If the connection is OK, your document is sent to the specified destination.
Checking SMTP Authentication.	You are attempting to scan and send a document via SMTP, and SMTP Authentication is enabled.	You must enter the correct User Name and Password to gain access to the SMTP server.

6.3.4 Scan to E-Mail Error Messages

This section explains the Scan to E-Mail error messages, along with possible causes and remedies.

Message	Cause	Remedy
Cannot connect to the SMTP Server.	• Connection to the SMTP server cannot be established. • The Network Socket Timeout option is configured.	Make sure that the SMTP server is connected to the network properly, and is accepting connections.
Cannot Authenticate to SMTP Server; Invalid Credentials.	SMTP Authentication is enabled, and the SMTP authentication credentials used are invalid.	• If you are not using public credentials, make sure that you enter the correct SMTP authentication credentials on the SMTP Authentication Password pop-up screen. • If you are using public credentials, verify the public credentials configured in the Configuration Servlet. See "Configuring the E-Mail Service Settings," on p. 55.

6.4 SCAN TO FAX Screen Notification Messages

The SCAN TO FAX screen notification messages are displayed on the SCAN TO FAX screen in the upper-right hand portion of the MEAP device's UI. As you interact with the application, different types of messages are displayed notifying you of an event.

6.4.1 Scan to Fax Warning Messages

This section explains the Scan to Fax warning messages, along with possible causes and remedies.

Message	Cause	Remedy
Scanning is disabled because the device is not ready.	The MEAP device is still in the process of sending a fax, and you are attempting to start another scan.	• Wait until the MEAP device has completed the operation in progress. • Reboot the device.

6.4.2 Scan to Fax Input Request Messages

This section explains the Scan to Fax input request messages, along with possible causes and remedies.

Message	Cause	Remedy
Please specify at least one fax number.	You tried to scan a fax document, but you have not specified a fax number.	Specify fax number.
Place a document in the ADF or on the Platen then close the lid.	You have not placed a document in the automatic document feeder or on the platen glass.	Place your document in the automatic document feeder or on the platen glass.

6.4.3 Scan to Fax Notification Messages

This section explains the Scan to Fax notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Checking SMTP Connection.	You are attempting to scan and send a document via SMTP.	If the connection is OK, your document is sent to the specified destination.
Checking SMTP Authentication.	You are attempting to scan and send a document via SMTP, and SMTP Authentication is enabled.	You must enter the correct User Name and Password to gain access to the SMTP server.

6.4.4 Scan to Fax Error Messages

This section explains the Scan to Fax error messages, along with possible causes and remedies.

Message	Cause	Remedy
Cannot connect to the SMTP Server.	• Connection to the SMTP server cannot be established. • The Network Socket Timeout option is configured.	Make sure that the SMTP server is connected to the network properly, and is accepting connections.
Cannot Authenticate to SMTP Server; Invalid Credentials.	SMTP Authentication is enabled, and the SMTP authentication credentials used are invalid.	• If you are not using public credentials, make sure that you enter the correct SMTP authentication credentials on the SMTP Authentication Password pop-up screen. • If you are using public credentials, verify the public credentials configured in the Configuration Servlet. See "Configuring Scan to Fax Settings," on p. 86.

6.5 SCAN TO FOLDER Screen Notification Messages

The SCAN TO FOLDER screen notification messages are displayed on the SCAN TO FOLDER screen in the upper-right hand portion of the MEAP device's UI. As you interact with the application, different types of messages are displayed notifying you of an event.

6.5.1 Scan to Folder Warning Messages

This section explains the Scan to Folder warning messages, along with possible causes and remedies.

Message	Cause	Remedy
Scanning is disabled because the device is not ready.	The MEAP device is still in the process of sending a document to a shared folder, and you are attempting to start another scan.	• Wait until the MEAP device has completed the operation in progress. • Reboot the device.

6.5.2 Scan to Folder Input Request Messages

This section explains the Scan to Folder input request messages, along with possible causes and remedies.

Message	Cause	Remedy
Select a Preset Share or enter a File Server and File Path.	You have a document in the automatic document feeder or on the platen glass, and you have not selected a preset share or entered a file server and file path.	Select a preset share, or enter a file server and file path.
Place a document in the ADF or on the Platen then close the lid.	You have not placed a document in the automatic document feeder or on the platen glass.	Place your document in the automatic document feeder or on the platen glass.
Press the [Scan] button or <Start> key to begin scanning.	The MEAP device is ready to scan the document to the share.	Press [Scan] or ⊙ (Start).

6.5.3 Scan to Folder Notification Messages

This section explains the Scan to Folder notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Checking access to [*share*] share…	The MEAP device is attempting to acquire sufficient read privileges.	Not applicable.
Validating File Server and File Path…	The MEAP device is validating correct formatting of the file server and file path.	Not applicable.

6.5.4 Scan to Folder Error Messages

This section explains the Scan to Folder error messages, along with possible causes and remedies.

Message	Cause	Remedy
Specified share is inaccessible. Please enter or select another.	The MEAP device cannot acquire sufficient read privileges to the specified file path on the specified file server.	Verify that the share exists and that sufficient privileges have been configured.
Home Directory is not configured. Contact Administrator.	In the Configuration Servlet, the [Scan to Home Directory/Preselected Share only] check box is selected, and the user has no Home Directory configured in Active Directory.	• Verify that the user has a Home Directory configured in Active Directory. • Clear the check mark from the [Scan to Home Directory/Preselected Share only] check box.
No share is pre-selected. Contact Administrator.	In the Configuration Servlet, the [Scan to Home Directory/Preselected Share only] check box is selected, and no preselected share is selected from the Preselected Share drop-down list.	• Select or configure a preselected share in the Configuration Servlet. • Clear the check mark from the [Scan to Home Directory/Preselected Share only] check box.
No share can be selected. Contact Administrator.	In the Configuration Servlet, the [File Server/Path] and [Browse] check boxes in the <Disabled> column are selected, and there are no preset shares configured.	• Add a preset share via the Configuration Servlet. • Clear the check marks from the [File Server/Path] and [Browse] check boxes in the <Disabled> column. See "Configuring Scan to Folder Settings," on p. 88.