HP DIGITAL SENDING SOFTWARE 5.0

System Administrator Guide

HP Digital Sending Software 5.01

System Administrator Guide

Copyright

The information contained herein is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Edition 3, 5/2013

Trademarks

Table of contents

1 Introduction to Digital Sending

This chapter contains the following topics:

Digital sending overview

HP Digital Sending technology offers a fast, simple, and reliable way to capture valuable information from paper-based documents and convert it to a digital format, which can be further processed and routed to a number of different destinations.

Routing destinations include, but are not limited to, the following:

- Network folders
- E-mail
- FTP sites
- Fax
- Microsoft SharePoint®

The digital file types available include, but are not limited to, the following:

- JPEG
- TIFF
- PDF
- Searchable PDF/A

Optical Character Recognition and Compression are also available offering a wide range of digital file types of varying sizes and quality that the user can select to meet their needs.

Additional data, or metadata, can also be specified and routed along with the scanned images as a method for enabling more complex workflows.

Digital Sending is available from most HP Multifunction devices, the Digital Sender line of products, and some HP Enterprise Scanners. These products offer a wide range of digital sending capability "out of box" via the product firmware. This out of box functionality is referred to as embedded digital sending. The functions available via embedded digital sending varies by product. See Table 1-1 Feature comparison on page 6 for more information.

The digital sending functionality which is provided in the device firmware can be extended with the server based HP Digital Sending Software (DSS). Some features DSS adds to embedded digital sending are shared address books, secure e-mail, a single point for e-mail routing, and Optical Character Recognition (OCR).

Introduction to DSS

This section contains the following topics:

- Advantages of DSS
- Features overview
- Supported devices

Advantages of DSS

The HP Digital Sending Software (DSS) extends the embedded Digital Sending functionality of supported devices by adding the following capabilities:

- Routing e-mail through a central point (the DSS server), which simplifies SMTP security management in environments with Access Control List security.
- Multiple SMTP gateways for redundancy in delivering e-mail jobs.
- Encrypted e-mail channel with SMTP over SSL.
- Sending fax through LAN Fax and Internet Fax servers.
- Public- and Personal Address Books.
- Access to Microsoft® Exchange Contacts from the front panel of the device with the Exchange Contacts feature.
- The LDAP Replication feature allows access to the company directory while off-loading the LDAP servers.
- The Workflow feature allows easy and consistent scanning into company workflow processes. Metadata can be collected for each job from users using configurable prompts or from internal device system information, allowing integration with third-party applications.
- OCR processing of jobs through the I.R.I.S OCR engine to create searchable output.
- Easy and intuitive interface to manage Digital Sending features through the Configuration Utility.
- Central logging of document sending activity for tracking, auditing, and troubleshooting purposes.

DSS runs as a software service on a networked server. Supported devices are "DSS aware," which means they have components built into the firmware that allow them to make use of the services/ features offered by DSS. Once a device is added into DSS, all of the Digital Sending features are managed through the Configuration Utility.

Features overview

This section gives a basic overview of the various features of the DSS.

- **E-mail**
  - **Route e-mail jobs from multiple devices through a single point.** DSS makes it possible to route e-mail jobs either through DSS or directly from the device to the SMTP gateway.

Routing e-mail through the DSS server simplifies SMTP security management in environments with Access Control List security on the SMTP gateways.

  - **SMTP gateway redundancy.** Multiple SMTP gateways for redundancy in delivering e-mail jobs.

  - **Encrypted e-mail channel.** DSS can provide a secure e-mail channel using SMTP over SSL.

- Fax

  - **Manage analog fax settings.** The DSS Configuration Utility provides an intuitive interface for managing fax settings on devices that have an analog fax accessory installed.

  - **Electronic faxing.** Integrates with LAN Fax servers via a shared folder interface and integrates with Internet Fax servers via an e-mail interface.

- **Address Books.** Devices attached to DSS have access to the DSS address books, which provide the following functionality:

  - **Public Address Book.** Allows the administrator to create an address book which is accessible from all attached devices.

  - **Personal Address Book.** Each user can create, use and manage a personal address book from any attached device.

  - **Exchange Contacts.** Each user can access their Microsoft Exchange® Contacts from the front panel of any attached device.

  - **LDAP Replication.** DSS can be configured to replicate addresses from an LDAP server at a regular interval so devices can obtain addresses from the DSS server rather than by querying the LDAP server in real time. This feature allows access to the company directory while off-loading the LDAP servers.

  - **Address Book Management.** Allows the administrator to manage all DSS address books.

- Workflow

  - **Integration with third-party applications.** The Workflow feature allows easy and consistent scanning into company workflow processes, through a shared folder, Microsoft Sharepoint, or an FTP site. Metadata can be collected either directly from the system or by prompting users for input. The metadata is stored in a file that will be sent to the destinations along with the scanned image file.

- Optical Character Recognition (OCR)

  - **Searchable documents.** OCR can process jobs through the I.R.I.S OCR engine to create searchable output in file formats such as PDF, PDF/A, XPS, HTML, RTF, etc.

- Digital Sending management

  - Easy and intuitive interface to manage Digital Sending features through the Configuration Utility.

- Logging

  - Central logging of document sending activity for tracking, auditing and troubleshooting purposes.

Supported devices

DSS supports most recent high-end HP multifunction devices, Digital Senders, and some ScanJet products. This document refers to these devices as *DSS-enabled devices*. For a list of all compatible products currently available, see Table 3-4 Device firmware requirements on page 28. For an up to date list of supported devices, go to www.hp.com/support/dss.

Embedded Digital Sending vs DSS

There are two ways to implement Digital Sending:

1. **Embedded Digital Sending.** Embedded Digital Sending indicates device-specific Digital Sending capabilities. These Digital Sending capabilities are embedded in the firmware of the DSS enabled device. Embedded Digital Sending includes capabilities such as e-mail and fax.

2. **Digital Sending Software (DSS).** DSS is a software service running on a network that expands the existing embedded capabilities of DSS enabled devices. DSS includes capabilities such as Send to E-mail (encrypted e-mail), Send to Fax, Send to Workflow, and Send to Network Folder.

Differences

The following product groups are represented in the Features Comparison table below.

- Pre-FutureSmart

- FutureSmart

Table 1-1 **Feature comparison**

Area	Feature	Pre-FutureSmart	FutureSmart
Authentication	LDAP	✓	✓
	LDAP over SSL	✓	✓
	Microsoft Windows	✓	✓
Send to	E-mail	✓	✓
	Folder	✓	✓
	LAN Fax	DSS	✓
	Internet Fax	DSS	✓
	Analog Fax	E	E**
Printer	DSS	✓**	DSS

Table 1-1 Feature comparison (continued)

Area	Feature	Pre-FutureSmart	FutureSmart
Addressing	Direct LDAP	✓	✓
	Replicated LDAP	DSS	DSS
	Public Address Book	DSS	DSS
	Personal Address Books	DSS	✓
	Exchange Contacts	DSS	✓
	Local Address Book	E	E
Other	Optical Character Recognition (OCR)	DSS	DSS***
	Workflow	DSS	DSS
	Metadata support	✓	✓
	Configurable metadata	DSS	DSS
	FileNet integration	DSS	DSS
	Single point for e-mail routing	DSS	DSS
	SMTP gateway redundancy	DSS	DSS
	SMTP over SSL	DSS	✓
	Quick Sets	NA	✓
	Compact PDF	DSS	✓
	Signed e-mail	E	✓
	Encrypted e-mail (message)	E	✓

Legend

- DSS — Requires DSS
- ✓ — Available both embedded and when managed by DSS
- E — Available only in embedded Digital Sending

- ** — Not available on the HP ScanJet Enterprise 7000n Document Capture Workstation.
- *** — Enterprise ScanJet products and MFP workflow products have this feature available both embedded in the product firmware and when managed by DSS.

DSS vs Web Jetadmin

HP Digital Sending Software and HP Web Jetadmin are two different software products available from HP with very different value propositions. However, while the products are different there is still some overlap in functionality. The purpose of this section is to provide a basic understanding of the differences between DSS and HP Web Jetadmin.

HP Web Jetadmin is a fleet management tool designed to manage printers, including DSS-enabled, multifunction devices, on a network. Features include device configuration, firmware installation, remote diagnostics, alerting, and reporting. For instance, system administrators can use this tool to get alerts for specific error conditions, update firmware on the entire fleet of devices, and create usage reports.

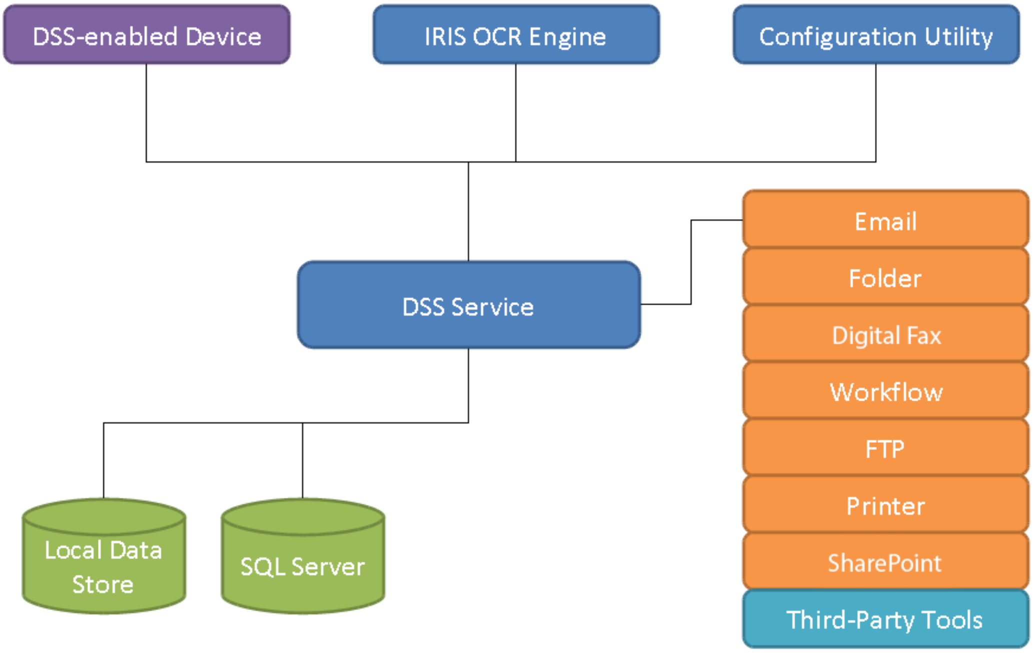
HP Digital Sending Software extends the embedded Digital Sending features of supported devices with features such as LAN Fax, OCR, Workflows, and Personal Address Books. DSS and Web Jetadmin functionality overlap in that both can be used to configure digital sending settings on DSS enabled devices. When a device is connected to DSS its digital sending settings can only be managed by DSS. Web Jetadmin can still be used to manage all other settings on the device. For more information on the values and capabilities of DSS, please refer to other sections of this document.

2 Theory of operations

This chapter contains the following topics:

Components

Figure 2-1 DSS Components



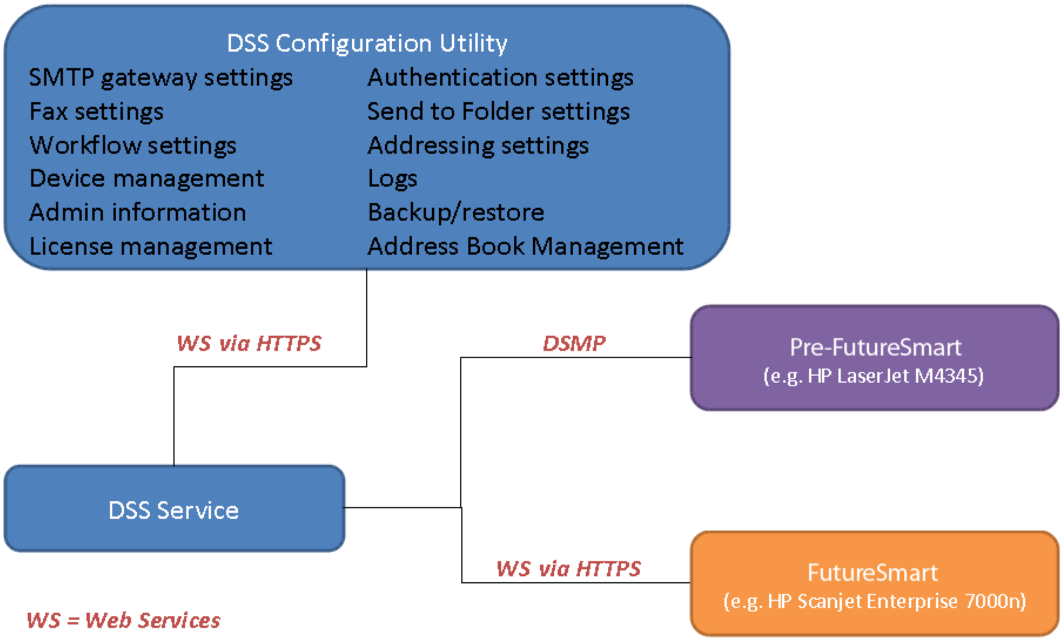
DSS can be viewed as a system that consists of a number of components, where each component provides a specific set of features that allows the system to function as a whole. The above diagram shows the DSS components and how they are connected. The following covers each of these in detail.

Configuration Utility

The role of the Configuration Utility is to act as a management console for DSS. It provides a user friendly interface to manage all settings for DSS functions as well as devices.

The Configuration Utility is always installed with DSS, but can also be installed separately on a different computer on the network. When installed separately it is typically referred to as the "Remote Configuration Utility", since in this mode it is used to manage a remote DSS server. The address of the server to be managed is entered in the startup dialog.

Figure 2-2 Configuration Utility



Remote Configuration Utility

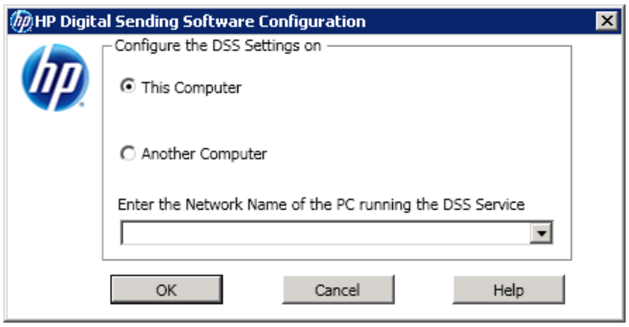
The Remote Configuration Utility is a version of the Configuration Utility that is designed to install and operate on a remote computer.

Using the Remote Configuration Utility allows DSS configuration across the network.

1. Launch the Configuration Utility.

2. Click **Another Computer**.

   Figure 2-3 Remote Configuration Utility

   HP Digital Sending Software Configuration

   Configure the DSS Settings on

   ● This Computer

   ○ Another Computer

   Enter the Network Name of the PC running the DSS Service

3. Type in the network name of the DSS server.

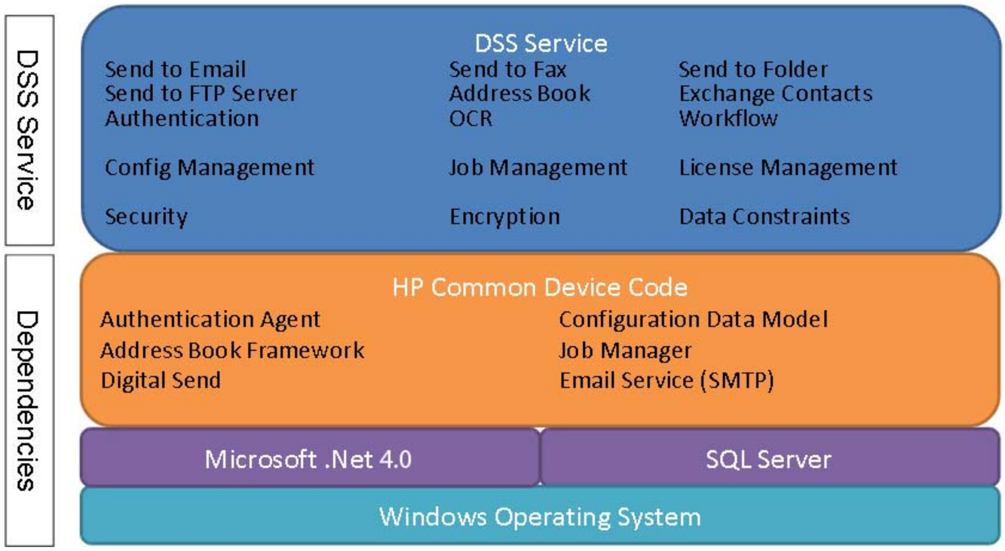
4. Click **OK**.

DSS Service

The core component of the HP Digital Sending Software system of the HP Digital Sending Software is the service named "HP Digital Sending Software", typically called the "DSS service". This is the key component of the software that ties together all other components and enables the DSS system to function. The DSS service is implemented as a Windows System Service.

Internally, the DSS service is divided into several subcomponents and has dependencies. The below figure shows this at a high level:

Figure 2-4 DSS Service Architecture



DSS-enabled device

DSS-enabled devices are the HP MFPs, Digital Senders, or ScanJet products that support DSS. These devices allow end-users to make use of DSS functionality by scanning to the various destination types, using the address book etc. For a complete list of supported devices, see Supported devices on page 5.

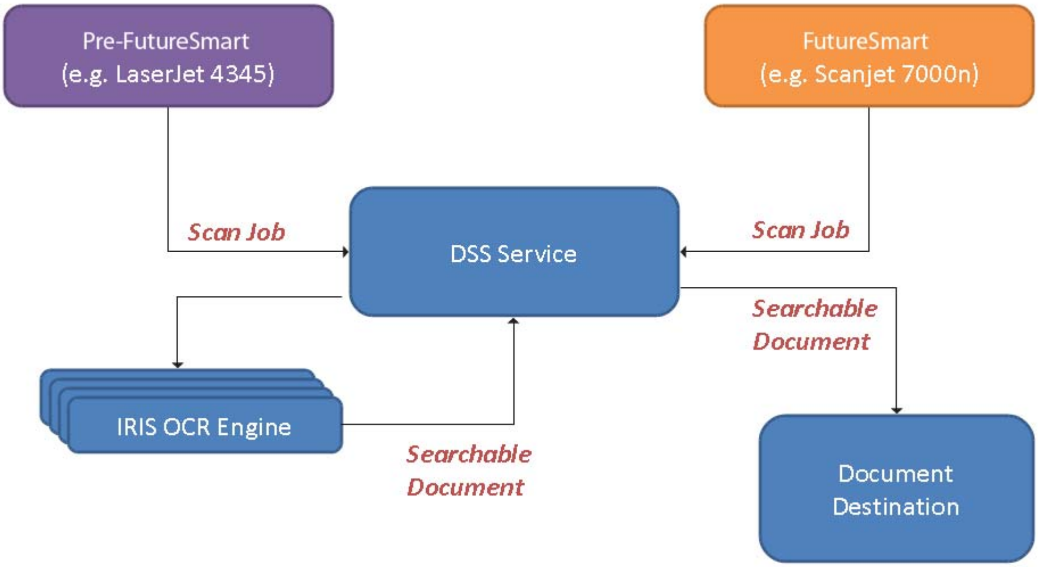
The firmware in these devices has a component built-in which enables use of DSS functionality. In Pre-FutureSmart products this is enabled through DSMP (Digital Sending Management Protocol). In HP's FutureSmart products this component has been replaced by a WS-* (Web Services Star) based interface.

Since all DSS features must be supported by the device firmware, DSS 5.0 has a minimum firmware version requirement, which can be found here Table 3-4 Device firmware requirements on page 28. Over time, as new features become available in DSS, it might be necessary to update the device firmware for compatibility. These changes will be documented in detail in the DSS release notes.

I.R.I.S. OCR engine

DSS uses I.R.I.S. OCR engine version 12 to provide Optical Character Recognition (OCR) and High Compression PDF functionality. The engine features Intelligent High Quality Compression (iHQC) technology™. The engine features Intelligent High Quality Compression (iHQC) technology™, and the ability to create searchable PDF/A documents.

Figure 2-5 OCR engine



The figure above shows the process flow for OCR processing in DSS. When DSS receives a job that requires OCR processing, it invokes the I.R.I.S. OCR engine using COM (Component Object Model). The image data/document is transferred together with control parameters, such as the required output file type. Once OCR processing is completed, the searchable document is passed back to DSS which delivers the document to the destination.

DSS is a multi-threaded application and will launch multiple instances of the OCR engine when there are multiple jobs in the queue that require OCR processing. We refer to this as ‘parallel processing of OCR jobs’. This makes the OCR feature scalable, which means that average job processing times will be improved if the server's resources are improved. For instance, adding additional CPUs and more memory to the server will improve the average processing time of each OCR job when the server is processing multiple jobs simultaneously. This is a significant improvement over previous versions of DSS, where OCR processing was serial.

Database

DSS uses Microsoft SQL Server 2008 SP3 Express Edition to host the DSS database. The database is used to hold job logs, address books, event logs, and some configuration data.

Microsoft SQL Server 2008 is a database management system (DBMS). Within the DBMS, DSS creates two databases for specific use by DSS, named as follows:

- DSS_Customer
- DSS_Machine

The SQL Server 2008 database instance name is “HPDSS2008.”

It is possible to configure DSS to use a DBMS other than Microsoft SQL Server 2008 SP3 Express Edition. If a different DBMS is specified during installation, DSS will not install SQL server on the local server. Even if the local database that DSS installs is used at first, the system can be configured later to use a different DBMS, but some data will be lost during the switch.

Local Data Store

The Local Data Store is the series of files located in the DSS installation directory, which is used to store the DSS configuration data, device information, and debug logs. This is also where the job queue resides.

Table 2-1 Local Data Store – Technical Detail

Technical detail	
Default installation folder:	C:\Program Files (x86)\Hewlett-Packard\HP Digital Sending Software 5.0
Default temporary jobs folder:	<Install folder>\CustomerData\DSS\Jobs
Configuration folder:	<Install folder>\Product\DSS\Configuration

NOTE: The temporary jobs folder can be configured to reside somewhere other than the default location. For information on changing the location of the temporary jobs folder, see Changing the location of the Jobs Folder on page 25.

Third-party tools

As the name indicates, third party tools are not a part of the DSS system. However, they are mentioned here because third party tools are required to deliver some of the DSS functionality as listed here:

- **LAN Fax.** This feature requires a compatible LAN Fax product. DSS enables the functionality by providing a Fax interface at the Digital Sending-device and then passing the fax job along with an HPF file (metadata) to a watched folder.

- **Internet Fax.** This feature requires an Internet Fax server. DSS enables the functionality by providing a Fax interface at the Digital Sending-device and then sending out an e-mail with the fax job attached.

- **Workflow.** One of the main ideas behind the Workflow feature is the ability to capture metadata at the Digital Sending-device and pass it on to a folder that is watched by a third party application. This application is then able to read the metadata and further process and route the job.

- **Personal Address Book.** This feature requires a Microsoft Exchange Server that supports HTTP connections.

Understand DSS data structures

The following describes the different types of data that makes up the DSS system and where they are stored.

Table 2-2 DSS data

Component	Location	Description
Job logs	Database	Job logs for all devices are stored in the DSS database.
Error logs	Database and Windows Event Log	The error logs show system events for information, warning and error conditions such as service stop and security audit.
Debug logs	[Install Path]\FileSystems\MachineData \Logs	DSS maintains a set of debug log files. These files are designed to help HP support debug issues with the DSS service, such as crashes, hangs etc.
DSS configuration settings	[Install Path]\FileSystems\Product\DSS \Configuration	Configuration data used by DSS is stored in a series of files found in the Configuration folder. This data includes things like SMTP gateway settings, LDAP addressing settings, Workflow settings etc.
Managed device Information		DSS maintains a list of all the devices it manages in a binary configuration file. This file also contains some basic information about the device, such as the hostname, device model etc.
Device configuration settings	Stored on the device	All the device-specific configuration data is stored on the device itself. When required DSS will read back the data from the device, manipulate it and send it back.
Configuration Utility UI ‘convenience’ data	Windows Registry	For usability the DSS Configuration Utility will remember entries made into selected list boxes, as well as the state of the Configuration Utility window when closed.
Job data temporary storage	<Install Path>\FileSystems \CustomerData\DSS	Location for the temporary storage of job data. This location can be configured to a location other than the default location. See Temporary jobs folder on page 25.

Understand licensing

This section contains the following topics:

- Licensing requirements
- Trial license
- Auto-generate licenses

- License activation and rehosting

Licensing requirements

DSS server software does not require a license to operate. A license seat is required for each device which is managed by DSS. Licenses can come in bundles of 1, 5, 10, 50, and 250 seats. Licenses can be combined in a DSS server in any combination up to 1000 seats.

Trial license

When DSS is first installed on a new server it comes with a sixty day, fifty seat trial license. If a purchased license is installed in DSS during the trial period, the trial license becomes invalid and only purchased licenses will work on that instance of DSS.

When the trial period ends, if no purchased licenses have been added to DSS, the software is unable to manage or process any jobs from devices.

Auto-generate licenses

The HP 9200C Digital Sender and HP 9250C Digital Sender devices auto-generate licenses after being added to a DSS server. These are the only two DSS-enabled devices that auto-generate licenses.

License activation and rehosting

Purchase DSS licenses from HP or HP authorized resellers. Once purchased, the customer will receive documentation which includes the Entitlement Order Number (EON). Activate the DSS license in order to use it by locking the license to a server. DSS licenses are locked to servers by the server MAC address. The output from locking a license is a license key code which users type into the DSS user interface to enable DSS to use the license. The EON and the server MAC address are required to activate a license.

From time to time it may be necessary for a customer to use a license on a server to which it is not currently locked. The process of changing the server to which a license is locked is called “rehosting.”

Conduct DSS license activation and rehosting via the licensing website: www.hp.com/software/licensing.

For more details on the license activation and rehosting sequence of steps, see the white paper “DSS License Activation and Rehosting”. Access the white paper on the DSS support web site www.hp.com/support/dss5. Once at the website home page, click the “Documentation” link on the left hand side to find this white paper.

Understanding DSS Address Books

DSS can maintain several different address books to make available to the devices maintained by DSS. This section will explain the different types of address books and when the addresses from each are available to users at a device control panel.

Address Book Manager

The Address Book Manager, or ABM, is a feature within DSS that allows for the management of several of the DSS address books. It is started from the **Addressing** tab of the Configuration Utility.

DSS Address Books

Public Address Book

Entries

- When a device is added to DSS, the device's local address book entries are added.
- Entries can be made via the Address Book Manager

Modify/Delete

- The Public address book can only be modified via the ABM

Private Address Books

Private address books are kept for specific users depending on the user's signed-in status at the device. The "Private MFP Guest" address book is for user's that are not signed-in, while "Private MFP User" address books are kept for each user that is signed-in.

Entries

- When user's at the device control panel type in new addresses and choose to save them, they are saved in the appropriate Private address book depending on their sign-in status.
- Entries can be made via the Address Book Manager

Modify/Delete

- Entries can be made to Private address books via the ABM

Personal Address Books

Personal Address Books hold a signed-in user's MicroSoft Outlook contacts. These are temporary address books only available while the signed-in user is accessing addresses, and then only when the system has been configured to collect the Outlook contacts.

Entries

- From the Outlook contacts of a signed in user.

Modify/Delete

- Personal address books are temporary and only maintained while a signed-in user is using the address book at the device control panel.

Replicated LDAP Address Book

DSS is capable of replicating address information from an LDAP server into the DSS database. This allows users to access these addresses via the DSS server instead of directly from the LDAP server at job creation time, offloading some load from the LDAP server to DSS. A replication schedule can be configured to collect addresses at regular intervals to keep the replicated data synchronized with the LDAP server data.

Entries

- Only via the replication mechanism that can be configured and run from the **Addressing** tab in the Configuration Utility.

Modify/Delete

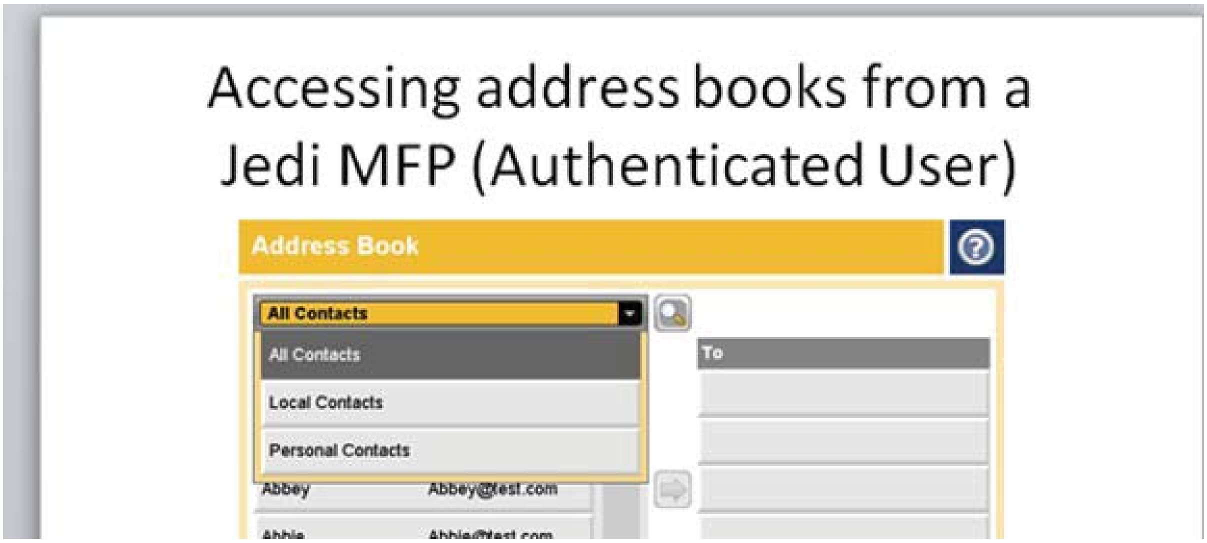
- The LDAP addresses can be cleared from the DSS database using the **Clear LDAP Cache** button on the **Addressing** tab of the Configuration Utility.

Accessing the Address Books from the device control panel

Addresses become available to a user at the device control panel when they click the address book icon while creating e-mail or fax jobs. Which DSS address book are available to a user at the device control panel depend on the user's signed-in status, the device type (FutureSmart versus pre-FutureSmart), and the address book view selection made by the user.

When using address books from the device, the user has the option of selecting an address book view. An example of the selections is shown below:

Figure 2-6 Address book view example



Accessing address books from a Jedi MFP (Authenticated User)

The tables below show which DSS address books are available based on View, sign-in status, and device type.

Table 2-3 Accessing Address Books form a FutureSmart MFP

View	Non Signed-In user	Signed-in User
All View	Public + LDAP + Private MFP Guest	Public + LDAP + Private MFP User + Personal (when configured) + Private MFP Guest

Table 2-3 Accessing Address Books form a FutureSmart MFP (continued)

View	Non Signed-In user	Signed-in User
Local View	Private MFP Guest	Private MFP Guest
Personal View		Private MFP User + Personal MFP User

Table 2-4 Accessing Address Books from a pre-FutureSmart MFP

View	Non Signed-In user	Signed-in User
All View	Public + LDAP + Private MFP Guest	Public + LDAP + Private MFP User + Personal (when configured) + Private MFP Guest
Local View	Private MFP Guest	
Personal View		Private MFP User + Personal MFP User

3 Installation and configuration

This chapter contains the following topics:

- Planning the DSS deployment
- Installation
- Configuration

Planning the DSS deployment

This section contains the following topics:

- System and environment requirements
- System security requirements for using DSS

System and environment requirements

This section contains the following topics:

- Software requirements
- Temporary jobs folder
- Hardware requirements
- Device firmware requirements
- Multiple DSS servers
- Port requirements

Software requirements

The following table shows the server software requirements.

Table 3-1 DSS software requirements

Area	Requirements
Operating systems	• Microsoft Windows 7, 32 and 64–bit • Microsoft Windows Server 2008, including R2, 32 and 64–bit • Microsoft Windows Server 2012 NOTE: 64-bit operating systems are supported, but DSS runs in 32-bit mode
Virtual servers	• VMware ESX 3.5 and later • Microsoft HyperV

Table 3-1 DSS software requirements (continued)

Area	Requirements
External database	Compatible databases which can be used if you choose not to install the default DSS database: ● Microsoft SQL Server 2005 (full or express versions) ● Microsoft SQL Server 2008 (full or express versions) ● Microsoft SQL Server 2012 (full or express versions)
Miscellaneous	.NET Framework 3.5 and 4.0 NOTE: If the .NET Framework 4.0 is not present on the system where DSS is being installed, the installer will install .the .NET Framework 4.0 during the installation process. If the .NET Framework 3.5 is not installed on Windows 7 or Windows Server 2008 systems where DSS is being installed, the installer will install the .NET Framework 3.5 during the installation process. For Windows Server 2012 systems where DSS is being installed, the .NET Framework 3.5 must either be installed *before* running the DSS installer, or the DSS installer must be able to access the internet to download the .NET Framework 3.5 for installation.

Temporary jobs folder

DSS 5.0 temporarily stores job files on disk while processing jobs. All job files are deleted after the job has finished processing. By default, this jobs folder for temporary storage is located within the installation folder sub-folders. Some customers might choose to change the location of this jobs folder. In DSS 5.0, this change is made by editing a configuration file.

Changing the location of the Jobs Folder

The file that controls the location of the temporary jobs folder is:

- `<InstallFolder>\filesystems\core\bin\xp-x86\release\nvram.csv`

Within the nvram.csv file find the line that reads:

- `FE966859-E2D0-48e6-8467-BF6F5A417643,CustomerDataPartition,str,..\..\..\..\CustomerData\Dss`

To change the location where temporary job files are stored, replace the part of the line that reads “..\..\..\..\CustomerData\DSS” with the path of the folder where you want the temporary files to be stored.

For example, to store the files on the d: drive in a folder named dsstemp, change the line to the following:

- `FE966859-E2D0-48e6-8467-BF6F5A417643,CustomerDataPartition,str,d:\dsstemp.`

After editing the file and saving the changes, the DSS service must be stopped and restarted for the change to take effect.

Hardware requirements

DSS hardware requirements vary with the load put upon the system. The primary load is due to processing of jobs that come in from devices.

It is strongly recommended that DSS run on its own server with no other server applications running. If other applications do run, they will also use system resources, and the resources used for those applications must be added to the consideration for resource usage by DSS when deciding what hardware is needed by the DSS server.

The primary factors that affect load are:

- Peak job requests per unit time
- Size of the job being transferred from devices
- Server based operations such as OCR and LAN fax with Notification support

Jobs that are not configured to be processed by the DSS OCR engine are created in the devices in their final format and transferred to DSS for routing to their destinations. Jobs that are to use the DSS OCR engine are sent to DSS as 300 dpi color JPEG images. There are many factors that affect the size of jobs that are created in the devices including, but not limited to:

- Number of pages
- File format
- Resolution
- Compression
- File content

There are so many factors that affect the load on the DSS server that not all variations can be tested. Below are tables of three different load scenarios and the recommended hardware for each load. But given the variables, it is highly recommended that administrators use tools, such as Microsoft Performance Monitor, to monitor their DSS servers' critical resources of processor bandwidth, memory usage, free disk space, and network bandwidth for any usage or performance bottlenecks.

The load scenarios tested are below. An equal percentage of e-mail, folder and workflow jobs were used during the testing.

Table 3-2 **Load scenarios**

Load Scenario	Job frequency (peak)	Average Job Size	% OCR
Minimum	<4	2.3 MB	10%
Medium	8 jobs/min	2.3 MB	10%
High	15 jobs/min	2.3 MB	10%

Table 3-3 **Recommended hardware configurations for load scenario**

Load scenario	Processor	Memory	Free disk space for Installation	Free disk space for temporary job files	Network bandwidth
Minimum	1 core x2 GHz	2 GB	1 GB	100 MB	100 Mb/s

Table 3-3 Recommended hardware configurations for load scenario (continued)

Load scenario	Processor	Memory	Free disk space for Installation	Free disk space for temporary job files	Network bandwidth
Medium	2 core x2 GHz	2 GB	1 GB	100 MB	100 Mb/s
High	4 core x2 GHz	2 GB	1 GB	100 MB	100 Mb/s

Device firmware requirements

To support DSS features, some devices require a minimum revision of firmware. Over time, as new features become available in DSS, it may be required to update the device firmware for compatibility. These changes will be documented in detail in the DSS release notes.

Table 3-4 Device firmware requirements

	Model number	Minimum firmware revision	Firmware date	Firmware version
pre-FutureSmart devices				
MFPs	HP LaserJet 4345MFP	09.220.7	12/8/2010	N/A
	HP LaserJet 4730MFP	46.300.3	11/24/2010	N/A
	HP LaserJet 9040MFP	08.210.5	11/27/2010	N/A
	HP LaserJet 9050MFP	08.210.5	11/27/2010	N/A
	HP LaserJet 9500MFP	08.210.6	11/29/2010	N/A
	HP LaserJet M3035MFP	48.171.5	11/29/2010	N/A
	HP LaserJet CM3530MFP	53.101.5	12/6/2010	N/A
	HP LaserJet M4345MFP	48.171.5	11/29/2010	N/A
	HP LaserJet CM4730MFP	50.151.0	12/6/2010	N/A
	HP LaserJet M5035	48.171.5	11/29/2010	N/A
	HP LaserJet CM6030MFP	52.121.2	12/6/2010	N/A
	HP LaserJet CM6040MFP	52.121.2	12/6/2010	N/A
	HP LaserJet M9040MFP	51.121.2	12/6/2010	N/A
	HP LaserJet M9050MFP	51.121.2	12/6/2010	N/A
Digital senders	HP 9200C	09.220.1	11/13/2010	N/A
	HP 9250C	48.160.3	11/18/2010	N/A
FutureSmart Devices				
MFPs	HP Color LaserJet Enterprise CM4540 MFP	2200643_228337	6/23/2012	FutureSmart 2 SP1
	HP LaserJet Enterprise M4555 MFP	2200643_228339	6/23/2012	FutureSmart 2 SP1
	HP LaserJet Enterprise 500 MFP M525	2200643_228344	6/23/2012	FutureSmart 2 SP1
	HP LaserJet Enterprise flow MFP M525	Any	Any	Any
	HP LaserJet 500 Enterprise color MFP M575	2200643_228345	6/23/2012	FutureSmart 2 SP1
	HP LaserJet Enterprise color flow MFP M575	Any	Any	Any
	HP LaserJet 700 Enterprise color MFP M775	Any	Any	Any
Scanjet Enterprise	HP ScanJet Enterprise 7000n	2200643_228343	6/23/2012	FutureSmart 2 SP1
	HP ScanJet Enterprise 8500	2200643_228339	6/23/2012	FutureSmart 2 SP1

Multiple DSS servers

There are several reasons for considering using multiple DSS servers:

- If there are more than 1000 products to be managed, then more than one server is necessary.
- If the load on any one server is too great for its hardware capability. This can happen if many devices are regularly sending very large jobs, if OCR is used frequently, or if network bandwidth is limited.
- For highly distributed systems of devices (depending on the available network infrastructure), multiple, distributed DSS servers help to ensure network reliability and bandwidth between the DSS servers and the products they manage.

DSS servers function independently of any other DSS server and do not, by themselves, form any type of clustering for enhanced functionality. This means that DSS servers will not share licenses. Each server must have the appropriate number of license seats to support its attached devices. Separate DSS servers also do not share address books or job logs.

DSS servers can be installed into a Microsoft Windows Server 2008 cluster for enhanced failover functionality. For detailed instructions on how to install DSS into an MS Server 2008 clustered environment, please see the white paper on this subject that is available at www.hp.com/support/dss.

Port requirements

DSS 5.0 uses a number of industry standard network protocols and their corresponding TCP and UDP ports in order to facilitate its Digital Sending functionality, such as Send to E-mail, Send To Folder, Authentication, and LDAP Replication. This section gives an overview of which ports are used in different configurations.

In its most basic configuration, DSS 5.0 requires ports 1783, 5213, 7627, and 161 to function. Administrators can refer to the table in this section to determine which ports are required for their specific configuration of DSS 5.0.

Ports used

DSS uses the TCP/IP protocol to communicate on the network. Which TCP or UDP ports are used depends on which features are enabled in DSS 5.0 and which underlying protocols facilitate these features. Also, note that for each protocol DSS acts as a server or client, or both. The following table provides an overview. Administrators should ensure that the required ports are open at appropriate points in the network, for example, desktop firewall, switches, and routers.

Table 3-5 Ports used by DSS 5.0

Feature	Type	Protocol	Port	Role of DSS	Can it be changed?
Device communication with pre-FutureSmart devices	Required	DSMP (HP Proprietary)	1783 (TCP)	Server & client	No
WS-* (WS-STAR), used for device communication with FutureSmart devices and for communication between DSS and the Configuration Utility	Required	HTTPS	7627 (TCP)	Server & client	No
DSS Address Book access for FutureSmart devices	Required	Secure SQL	5213	Server	No
Device data collection [3]	Optional	SNMP	161 (UDP)	Client	No
E-mail notifications, e-mail via service	Optional[1]	SMTP	25 (TCP)	Client	Yes
Send to Folder (Network UNC path)[2]	Optional	CIFS / SMB	445 (TCP)	Client	No
Send to FTP	Optional	FTP	21 (TCP)	Client	No
LDAP Replication & Authentication, simple bind	Optional	LDAP	389 (TCP)	Client	Yes

Table 3-5 Ports used by DSS 5.0 (continued)

Feature	Type	Protocol	Port	Role of DSS	Can it be changed?
LDAP Replication & Authentication, simple over SSL bind	Optional	LDAP	636 (TCP)	Client	Yes
LDAP Replication & Authentication SPNEGO	Optional	Kerberos	88 (TCP)	Client	No
LDAP Replication & Authentication, Global Catalog	Optional	LDAP	3268 (TCP)	Client	Yes
DNS hostname resolution	Optional	DNS	53 (TCP)	Client	No
WINS hostname resolution	Optional	NetBIOS/WINS	137,138,139	Client	No
SMTP and LDAP server discovery – when an MFP sends out a broadcast packet looking for SMTP or LDAP servers DSS will respond with any servers it knows about	Optional	Broadcast	22986	Server	No
SMTP and LDAP server discovery – DSS will broadcast this packet when asked to search for LDAP or SMTP servers	Optional	Broadcast	22986	Client	No

[1] If a mail gateway is not required, enter a dummy address (0.0.0.0) in the Configuration Utility.

[2] Does not apply to local folders, for example. c:\myfolder.

[3] SNMP is only required to get and set paper sizes in pre-FutureSmart devices and to get the firmware version from pre-FutureSmart devices for use in LanFax job logs. We are working to remove these last uses of SNMP in future versions of DSS

DSS Address Book access for FutureSmart devices

HP's FutureSmart devices now access the DSS Address Book by connecting directly to the SQL database on port 5213. Therefore, port 5213 must be open between FutureSmart devices and the SQL database server. The database server is the DSS server by default, but can optionally be configured to be a database on a different server.

Pre-FutureSmart devices continue to make address book requests of the DSS service, not directly to the SQL database, via port 1783. The DSS service accesses the database and returns address information to the device, also via port 1783.

Summary

In its most basic configuration, DSS 5.0 requires ports 1783, 7627, and 5213 to function. At installation, DSS will register itself with the desktop firewall to ensure connections are allowed on these ports. Administrators can refer to the matrix in this document to determine which ports are required for their specific configuration of DSS 5.0.

System security requirements for using DSS

Security to start the Configuration Utility

The DSS Configuration Utility uses Windows security to determine which users are allowed to start and run the Configuration Utility. When the Configuration Utility is first started, the user is prompted to enter the address of the server on which the DSS service is running that they want to control with this Configuration Utility session. Users are allowed to run the Configuration Utility under any of the following conditions:

- The user is a member of the local or global administrators group on the server running the DSS service
- The user is a member of a group on the server running the DSS service that has been configured to allow Configuration Utility access. By default, DSS is configured to use a group named "DSSAdmins" for this purpose. If you want to use a group by that name you must create it on the system. The name of the group can be configured, or multiple groups configured, to allow DSS access. This configuration is contained in the file “<Install path>\FileSystems\Product\DSS\Configuration\HP.Dss.App.Service.Config.xml.”
- If a user attempts to run the Configuration Utility without being a member of the administrators group or the configured group, they will be prompted for the credentials of a user that is a member of one of those groups.

When changing the configuration of the group(s) that allow non-administrators to access the Configuration Utility, the DSS service should be stopped, the configuration file edited, and then the DSS service restarted.

Permissions needed to run DSS with full functionality

Administrators have all the permissions necessary to run DSS. But if the DSS server has Windows User Account Control (UAC) enabled, the administrator might have to use the “Run as Administrator” command to have the necessary permissions.

Non-administrators can start the Configuration Utility if they are members of the proper Windows group, but this does not give them the necessary OS permissions to execute the tasks the Configuration Utility performs. In order for proper Configuration Utility operation, the user must have the following OS permissions on both the remote server (if they are running the Configuration Utility from one system to control the DSS service on another server) and the sever which is running the DSS service.

- Read/write access to the following area of the file system:
  - <Install path> \Hewlett-Packard\HP Digital Sending Software 5.00
- Read/write access to the following areas of the registry:

    - HKEY_CURRENT_USER\Software\Hewlett-Packard\HP Digital Sending Software
    - HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HP Digital Sending Software 5.00
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters \SslBindinginfo

- Users must also have permission to host a service on port 7627. The following command can be used to give this permission to a Windows group. The group should be given permission and non-administrator users should be made members of this group. This command must be run by an administrator on the system.

  In the example below, “DSS_Server” is the server where DSS is installed and “DSSAdmins” is the name of the group to give permissions. If a group was already created to give non-admins permissions to start the Configuration Utility, then it makes sense to give port 7627 permissions to that same group.

    - >netsh http add urlacl url=https://+:7627/ user=DSS_Server\DSSAdmins

  This command can only be used to give permissions to a single group. If permission has been given to one group and you wish to give permissions to a different group instead the following command must be run first:

    - >netsh http delete urlacl url=https://+:7627/

Device credentials for FutureSmart devices

HP Digital Sending Software communicates with FutureSmart devices for many purposes, including adding and removing devices, getting status from devices, configuring devices and processing jobs from devices. When a FutureSmart device has a password set, the device's security model requires that DSS know and use that password to enable device communication.

This section describes the various device passwords that can be set. It also describes how DSS uses the credentials it has stored for device communication and how to configure those credentials within DSS.

FutureSmart device accounts and credentials

HP LaserJet printers have for many years had an Embedded Web Server (EWS) interface. This can be accessed by using a web browser and typing in the IP address of the device. Within the devices is the concept of an Admin User that has access to all of the capabilities available via the EWS. The Admin User also has access to all the applications on the device such as the Copy application, Send to Network Folder application, etc.

As a factory default, the Admin User’s password is blank which means that anyone that accesses the EWS has permissions to all the capabilities provided by the EWS. Within the EWS there is a place where the Administrator User’s password can be set. Once the password is set then a user connecting to the EWS must sign in with the password to have Administrator level permissions.

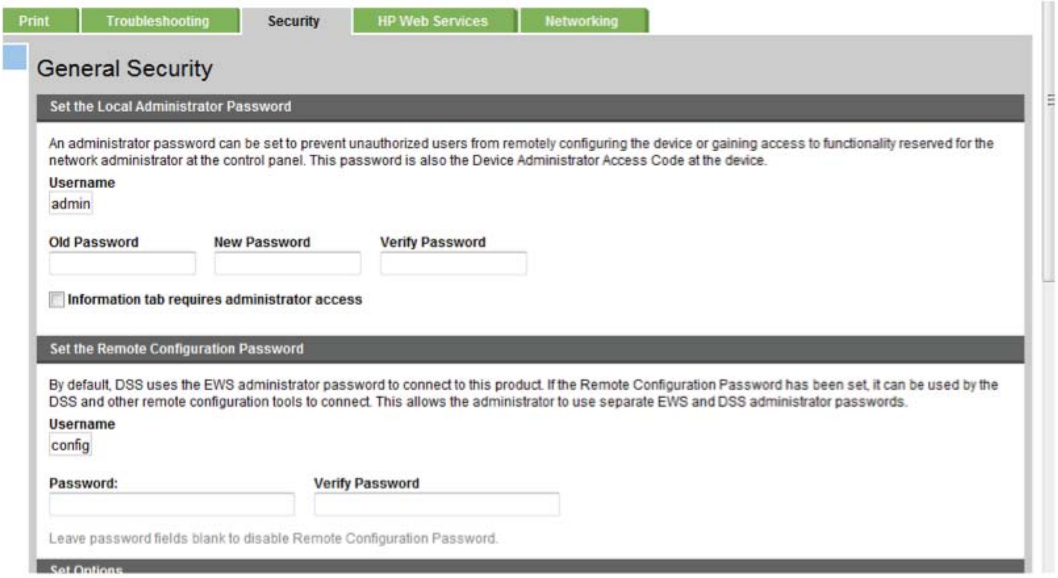
If the Administrator password is set, DSS must also know and use that password for any of the communication tasks (add/remove, get status, configure, process job) it wants to accomplish with the device.

Starting with the spring 2012 release of FutureSmart firmware, a new factory defined user will be available in the devices. This is the Config User. For devices with this spring 2012 firmware (or newer) DSS can communicate if it has either the Admin User or the Config User’s password. The Config User can not be used by users connecting to the EWS with a web browser; it is only available for use by remote applications such as DSS and HP Web Jetadmin.

Like the Admin User, the Config User’s password ships as blank as a factory default. The password can be set within the EWS in the same location as the Admin User’s password. These are set on the Security Tab in the General Security section. Unlike the Admin user however, the Config user is inactive if the password blank. This user is only activated when the password is configured within the EWS. See the screenshot below.

The Config User has been added so that companies can change the Admin password, if their company security policies require, without changing the Config User password. This means that DSS can be given the Config User’s password, instead of the Admin password, and continue to operate properly when the Admin password is changed.

Figure 3-1 DSS General Security screen



General Security

Set the Local Administrator Password

An administrator password can be set to prevent unauthorized users from remotely configuring the device or gaining access to functionality reserved for the network administrator at the control panel. This password is also the Device Administrator Access Code at the device.

Username

admin

Old Password   New Password   Verify Password

□ Information tab requires administrator access

Set the Remote Configuration Password

By default, DSS uses the EWS administrator password to connect to this product. If the Remote Configuration Password has been set, it can be used by the DSS and other remote configuration tools to connect. This allows the administrator to use separate EWS and DSS administrator passwords.

Username

config

Password: Verify Password

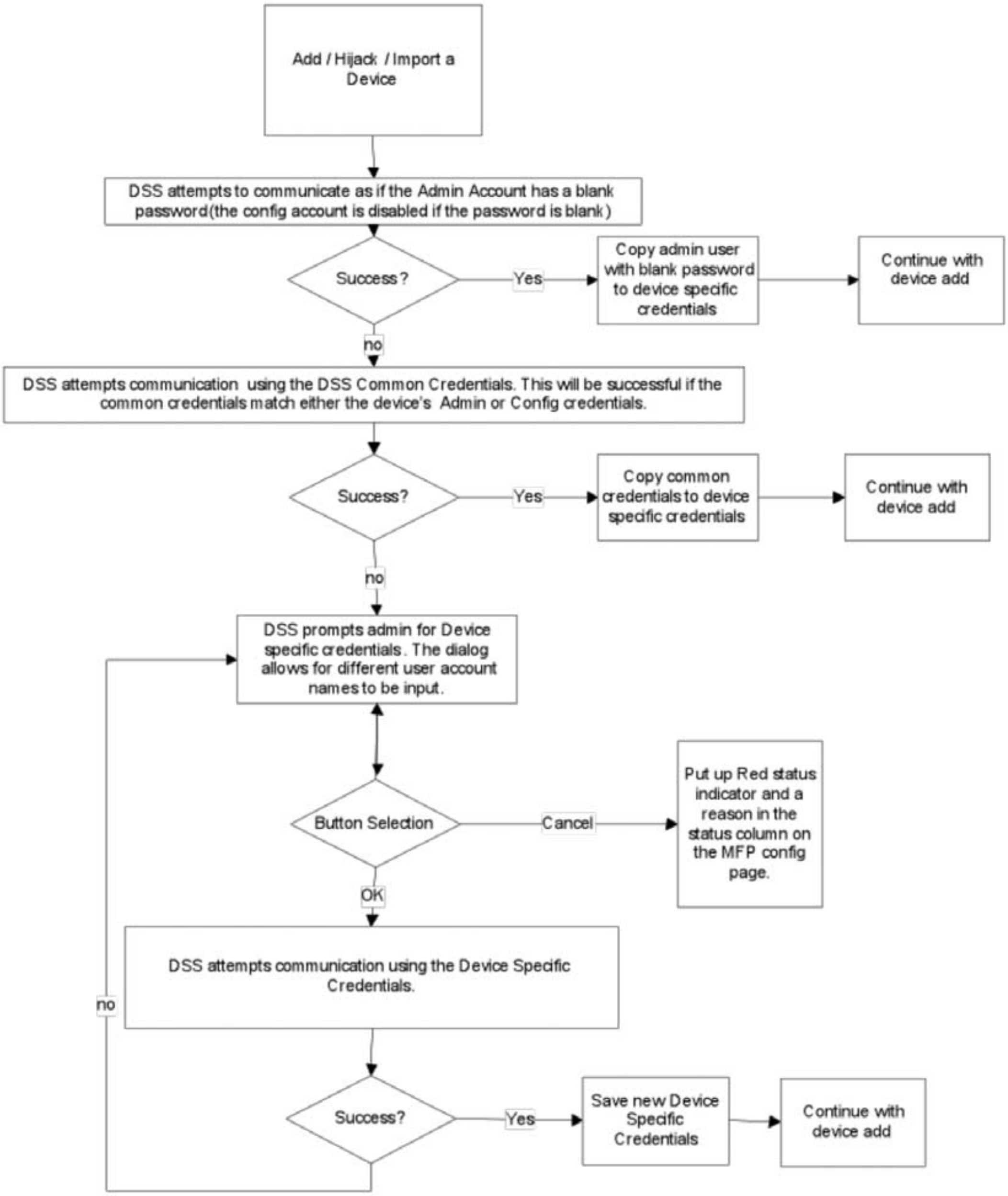
Leave password fields blank to disable Remote Configuration Password.

Set Options

DSS configuration and use of FutureSmart device credentials

DSS stores a single set of device-specific credentials for each device, and is also capable of storing one set of common credentials it can use for communication with FutureSmart devices. See Set the DSS common credentials on page 35 for instructions of how to set these credentials. If DSS tries to use the common credentials with a device and they work, then those common credentials will be copied to the device-specific credentials for that device. See Figure 3-2 DSS common and device-specific credentials flow on page 35 for the logic of how DSS uses the common credentials and device-specific credentials when adding a FutureSmart device.

Figure 3-2 DSS common and device-specific credentials flow

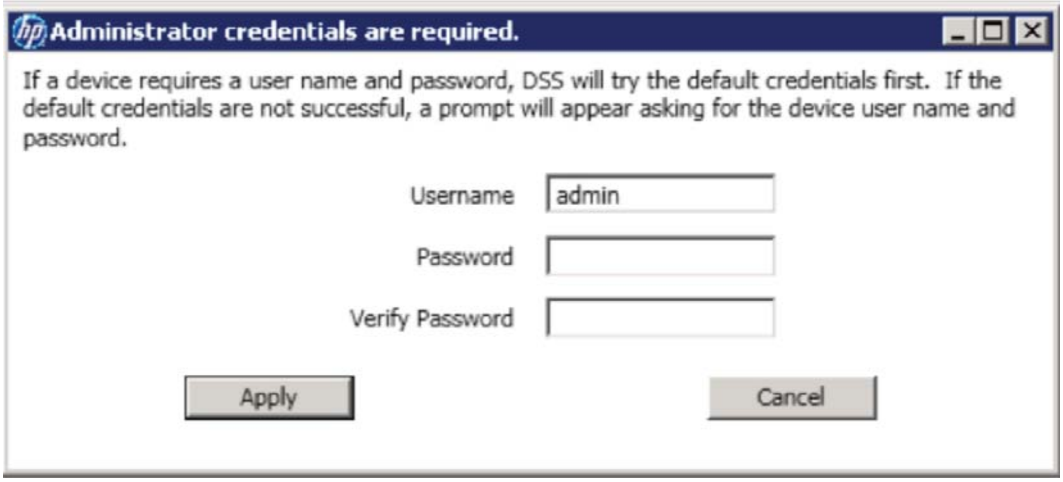

Add / Hijack / Import a Device
DSS attempts to communicate as if the Admin Account has a blank password(the config account is disabled if the password is blank)
Success ?
Yes
Copy admin user with blank password to device specific credentials
Continue with device add
no
DSS attempts communication using the DSS Common Credentials. This will be successful if the common credentials match either the device's Admin or Config credentials.
Success?
Yes
Copy common credentials to device specific credentials
Continue with device add
no
DSS prompts admin for Device specific credentials. The dialog allows for different user account names to be input.
Button Selection
Cancel
Put up Red status indicator and a reason in the status column on the MFP config page.
OK
DSS attempts communication using the Device Specific Credentials.
no
Success?
Yes
Save new Device Specific Credentials
Continue with device add

Set the DSS common credentials

1. Click the **Device Sign In** button in the Configuration Utility.

2. In the **Administrator credentials are required dialog**, use “admin” or “config” for the **Username** field, and then enter and verify a password in the **Password** and **Verify Password** fields.

Figure 3-3 Set the DSS common credentials



Administrator credentials are required.

If a device requires a user name and password, DSS will try the default credentials first. If the default credentials are not successful, a prompt will appear asking for the device user name and password.

Username: admin

Password:

Verify Password:

3. Click the **Apply** button to set the common credentials.

Installation

This section contains the following topics:

- Pre-installation checklist
- Installer screens and options

Pre-installation checklist

1. Review the hardware and software requirements for the DSS server. See System and environment requirements on page 24 for more information.
2. Verify that devices planned for connection to DSS have the minimum required firmware.
3. If you are upgrading from a previous version of DSS, make a backup of the existing configuration.

Installer screens and options

Follow these steps to install the HP Digital Sending Software 5.0.

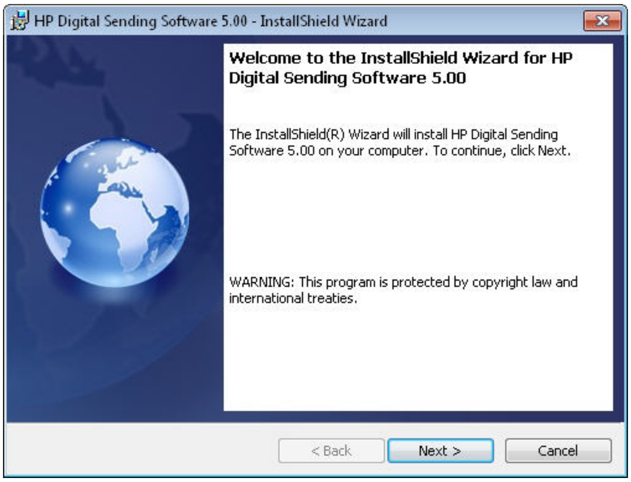
1. After downloading the software to your computer or network, close all programs that are open on the computer.
2. Navigate to the location on the computer or network where you downloaded the HP Digital Sending Software 5.0 software, and double-click the **setup.exe** file.

NOTE: If the downloaded software is in a compressed format, uncompress the installer files before running the setup.exe file.

NOTE: Windows administrator rights are required for installing DSS. However, if User Account Control (UAC) is turned on it may prevent the installation program from completing some tasks successfully, such as installing SQL Server. If UAC is turned on, you might have to right click the DSS installer setup.exe file and select **Run as administrator** from the menu to install DSS.

3. The **Welcome** screen appears. Click **Next** to continue.

Figure 3-4 Software Installation – Welcome screen (1 of 11)



HP Digital Sending Software 5.00 - InstallShield Wizard

Welcome to the InstallShield Wizard for HP Digital Sending Software 5.00

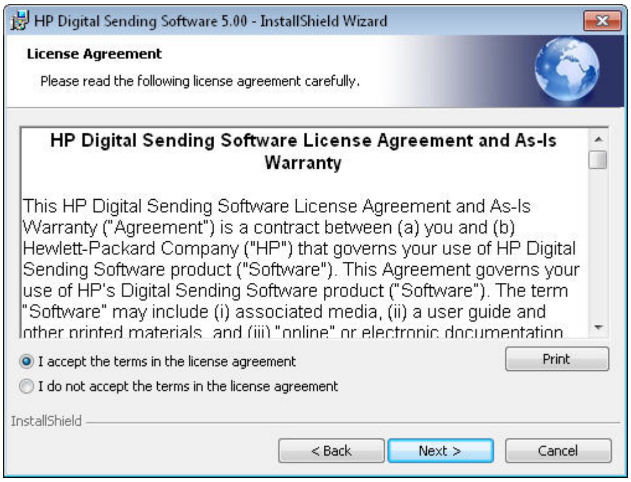
The InstallShield(R) Wizard will install HP Digital Sending Software 5.00 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

4. The **License Agreement** screen appears. Click **Print** to print a copy of the license agreement. Click **I do not accept the terms in the license agreement**, and then click **Next** to cancel the installation.

   After reading the license agreement, click to select **I accept the terms in the license agreement**, and then click **Next** to continue the installation.

   Figure 3-5 Software Installation – license agreement (2 of 11)

   HP Digital Sending Software 5.00 - InstallShield Wizard

   License Agreement

   Please read the following license agreement carefully.

   HP Digital Sending Software License Agreement and As-Is Warranty

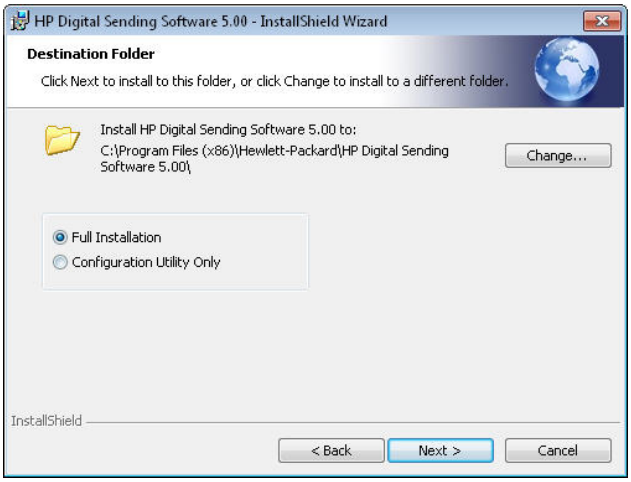
   This HP Digital Sending Software License Agreement and As-Is Warranty ("Agreement") is a contract between (a) you and (b) Hewlett-Packard Company ("HP") that governs your use of HP Digital Sending Software product ("Software"). This Agreement governs your use of HP's Digital Sending Software product ("Software"). The term "Software" may include (i) associated media, (ii) a user guide and other printed materials, and (iii) "online" or electronic documentation

   ● I accept the terms in the license agreement

   ○ I do not accept the terms in the license agreement

5. The **Destination Folder** screen appears. Accept the default installation folder or click the **Change** button to select a different folder. Select the **Full Installation** check box or the **Configuration Utility Only** check box, depending on the type of installation you need. Click the **Next** button.

   Figure 3-6 Software Installation – installation location (3 of 11)

   HP Digital Sending Software 5.00 - InstallShield Wizard

   Destination Folder

   Click Next to install to this folder, or click Change to install to a different folder.

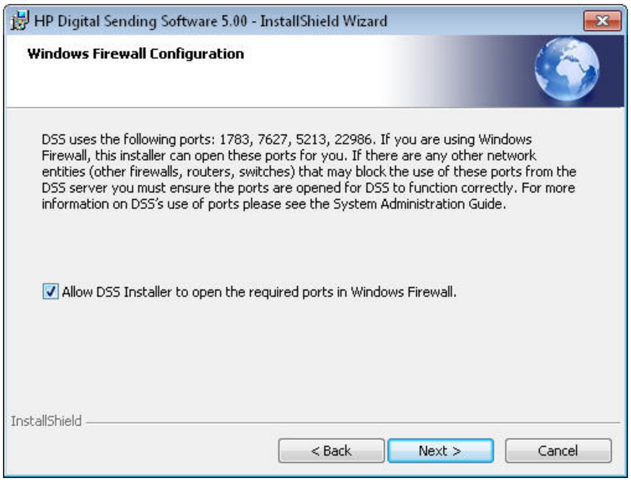
   Install HP Digital Sending Software 5.00 to:
   C:\Program Files (x86)\Hewlett-Packard\HP Digital Sending Software 5.00\

   ● Full Installation

   ○ Configuration Utility Only

6. The **Windows Firewall Configuration** screen appears. Click to select the **Allow DSS Installer to open the required ports in Windows Firewall.** check box, and then click **Next** to continue.

Figure 3-7 Software Installation – firewall configuration (4 of 11)



Windows Firewall Configuration

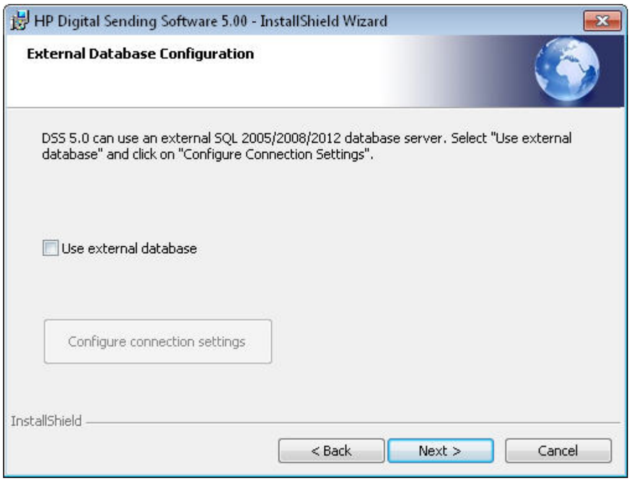
DSS uses the following ports: 1783, 7627, 5213, 22986. If you are using Windows Firewall, this installer can open these ports for you. If there are any other network entities (other firewalls, routers, switches) that may block the use of these ports from the DSS server you must ensure the ports are opened for DSS to function correctly. For more information on DSS's use of ports please see the System Administration Guide.

☑ Allow DSS Installer to open the required ports in Windows Firewall.

7. The **External Database Configuration** screen appears. This screen allows for a database other than the default Microsoft SQL Server database installed by DSS to be used with DSS. When this feature is used, the DSS installer does not install the default MS SQL Server database.

   The DSS installer creates two separate, uniquely-named databases within a single SQL Server instance; one database for customer data and one database for machine data.

Figure 3-8 Software Installation – external database configuration (5 of 11)



HP Digital Sending Software 5.00 - InstallShield Wizard

External Database Configuration

DSS 5.0 can use an external SQL 2005/2008/2012 database server. Select "Use external database" and click on "Configure Connection Settings".

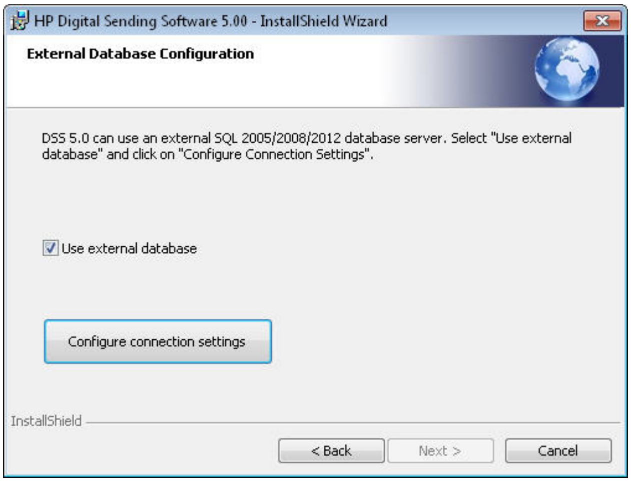
□ Use external database

Configure connection settings
InstallShield
< Back
Next >
Cancel

Use the following steps to configure an external database for use with DSS

a. Select the **Use external database** check box, and then click the **Configure connection settings** button.

Figure 3-9 Software Installation – external database configuration (6 of 11)


HP Digital Sending Software 5.00 - InstallShield Wizard
InstallShield
< Back
Next >
Cancel
Configure connection settings

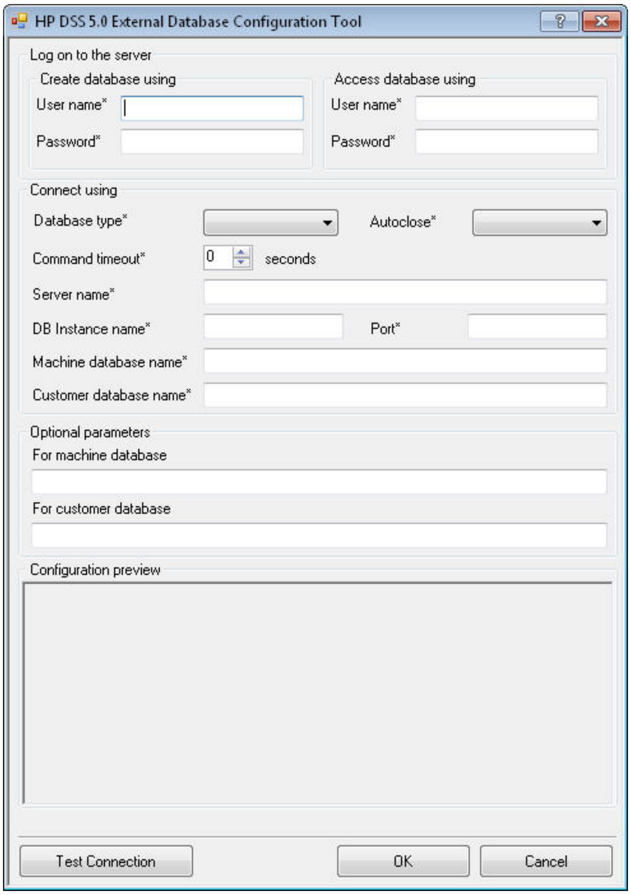
External Database Configuration

DSS 5.0 can use an external SQL 2005/2008/2012 database server. Select "Use external database" and click on "Configure Connection Settings".

☑ Use external database

b. The **HP DSS 5.0 External Database Configuration Tool** screen appears.

Figure 3-10 Software Installation – external database configuration (7 of 11)



Command timeout* 0 seconds

The following settings are required for configuring an external database:

- **Create database using** area: Enter values for the **User name** and **Password** fields. These credentials are used by DSS to configure databases for DSS use. DSS will not do the initial creation of these databases, but DSS will configure the databases with the structure they need such as tables, keys, etc. These credentials are used only for initial database configuration. Enter the credentials for a SQL-authorized user account, not a Windows-authorized user account.

The “Create database using” user must have, as a minimum, the following roles in SQL Server:

  - Server role: public
  - Database roles for the two DSS databases: db_owner

- The **Access database using** area: Enter values for the **User name** and **Password** fields. DSS uses these credentials for all database operations, except the database initialization process

  The “Access database using” user must have, as a minimum, the following roles in SQL Server:

  - Server role: public
  - Database roles for the two DSS databases: db_datareader, db_datawriter

- The **Connect using** area:

  - **Database type**: Select one of the three SQL Server versions:

    - SQL Server 2005
    - SQL Server 2008
    - SQL Server 2012

  - **Autoclose**: When set to **On**, the SQL Server instance and its databases are closed and their resources are freed when the last associated DSS instance is closed. The SQL server instance and its databases are opened automatically when a DSS user requires them. When set to **Off**, the SQL Server instance and its databases remain open even when the last associated DSS instance is closed.

  - **Command timeout**: The amount of time DSS waits for a connection to the SQL Server before terminating the connection attempt.

  - **Server name**: The name of the server where the DSS SQL server is installed.

  - **DB instance name**: The name of the SQL Server instance.

  - **Machine database name**: The name to use for the machine data database. This database must exist within the SQL Server instance before DSS can be configured to use it. DSS will fill out the structure of the database but will not do the initial creation.

  - **Customer database name**: The name to use for the customer data database. This database must exist within the SQL Server instance before DSS can be configured to use it. DSS will fill out the structure of the database but will not do the initial creation.

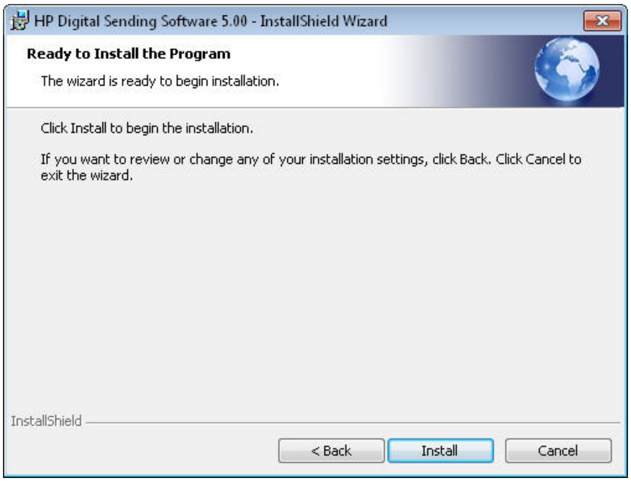
- The **Optional parameters** area: Use the **For machine database** and **For customer database** fields to enter additional connection strings parameters appended to the connection string when connecting to these databases. The syntax of these additional connection string parameters must adhere to the SQL Server connection string format.

The **Configuration preview** field displays the connection strings for the machine and customer databases as the connections strings are being entered. When the HP DSS 5.0 External Database Configuration Tool is opened after the initial configuration, the **Configuration preview** field displays the saved connection string settings.

- Click the **Test Connection** button to test the following configuration settings:
  - The SQL Server instance exists
  - The “create database” credentials are valid
  - The “access database” credentials are valid
- Click the **OK** button to test, and then save the following configuration settings:
  - The SQL Server instance exists
  - The “create database” credentials are valid
  - The “access database” credentials are valid
- Click the **Cancel** button to close the HP DSS 5.0 External Database Configuration Tool without saving any changes.

8. The **Ready to Install the Program** screen appears. Click **Back** to go back to change installation options. Click **Install** to start the installation.

Figure 3-11 Software Installation – ready to install screen (8 of 11)



HP Digital Sending Software 5.00 - InstallShield Wizard

Ready to Install the Program

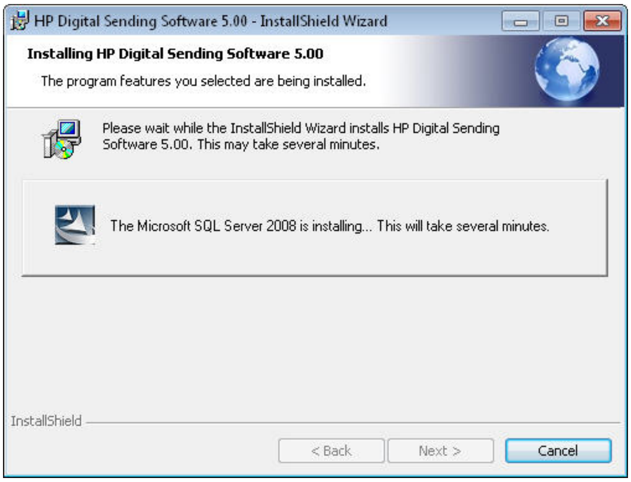
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

9. The **Microsoft SQL Server 2008 Setup Progress** screen displays the installation progress for the SQL server. The DSS install program will install the IRIS OCR engine, an instance of SQL Server (unless an external database is to be used), and then the DSS software itself. If the install program detects that some necessary OS components are missing, such as .NET 3.5, it will also install those components.

   Figure 3-12 Software Installation – SQL Server setup progress screen (9 of 11)

   HP Digital Sending Software 5.00 - InstallShield Wizard

   Installing HP Digital Sending Software 5.00

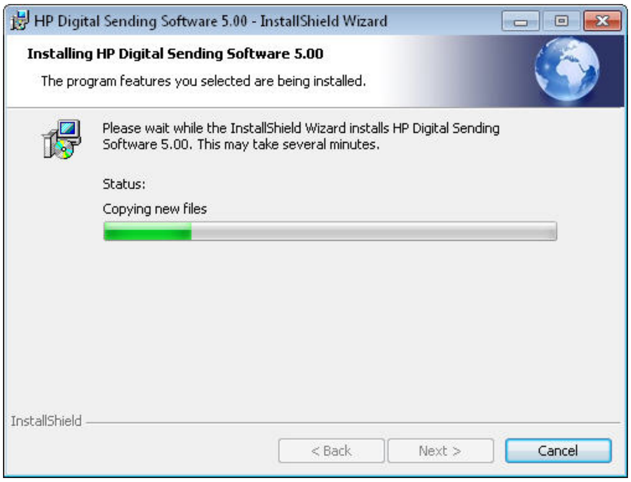
   The program features you selected are being installed.

   Please wait while the InstallShield Wizard installs HP Digital Sending Software 5.00. This may take several minutes.

   The Microsoft SQL Server 2008 is installing... This will take several minutes.

10. The **Installing HP Digital Sending Software 5.0** screen shows the progress of the software installation.

   Figure 3-13 Software Installation – installation progress screen (10 of 11)

   HP Digital Sending Software 5.00 - InstallShield Wizard

   Installing HP Digital Sending Software 5.00

   The program features you selected are being installed.

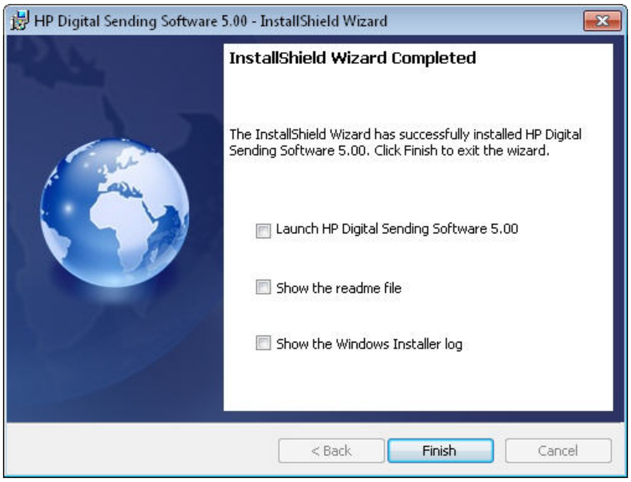
   Please wait while the InstallShield Wizard installs HP Digital Sending Software 5.00. This may take several minutes.

   Status:

   Copying new files

11. When the installation completes, the **InstallShield Wizard Completed** screen appears. Based on your configuration and the options installed, a reboot of the DSS server might be required. Click the **Launch HP Digital Sending Software 5.0** check box to launch the software when the installer closes. Click the **Show me the readme file** check box if you want to see the product readme file when the installer closes. Click the **Show the Windows Installer log** check box to view the Windows log file for the installation. Click **Finish** to complete the installation.

Figure 3-14 Software Installation – installation complete screen (11 of 11)



HP Digital Sending Software 5.00 - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed HP Digital Sending Software 5.00. Click Finish to exit the wizard.

□ Launch HP Digital Sending Software 5.00

□ Show the readme file

□ Show the Windows Installer log

Configuration

The HP Digital Sending Software (DSS) executes as a Windows service and allows users to scan documents at DSS-enabled devices, and send the scanned images to various types of destinations (such as e-mail, fax and folder). This software package includes a Configuration Utility that allows you to set up DSS features in a way that works best in your environment. Each DSS feature must be configured before it is available for use on DSS-enabled devices.

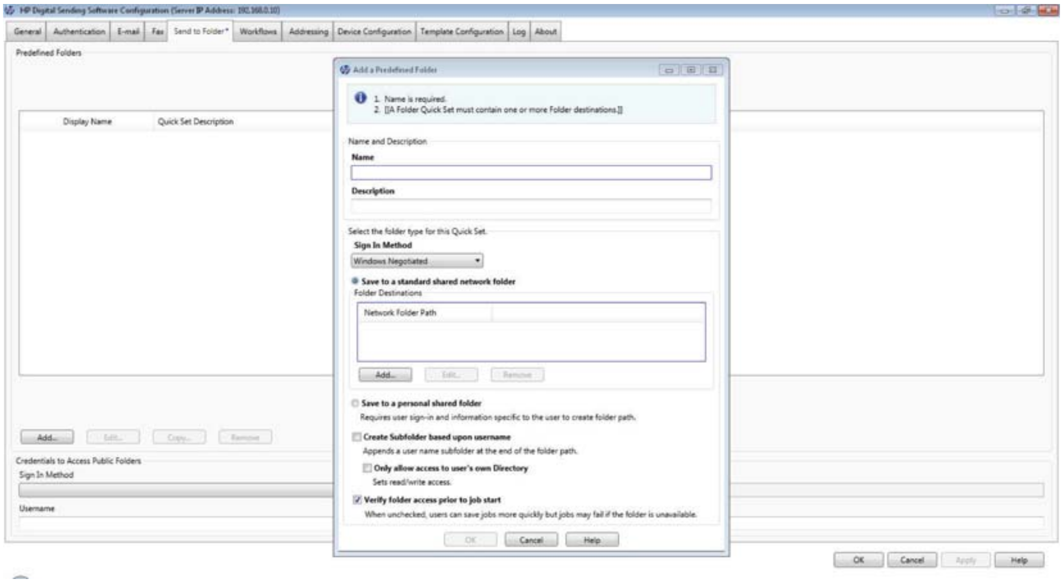
Most DSS functions require some configuration of settings within the DSS service as well as settings within devices managed by DSS to operate as desired. The Configuration utility is used to configure both service settings and device settings. If you have groups of devices that will share settings, using templates can help with configuration of device settings.

This section contains the following topics:

Configuration Utility

The Configuration Utility manages settings that apply across all DSS-enabled devices, such as an e-mail server and Authentication method, and also settings that apply to specific devices. The Configuration Utility has several display elements to assist you in knowing what data is required to make DSS features available on devices.

Figure 3-15 Configuration Utility elements



HP Digital Sending Software Configuration (Server IP Address: 192.168.0.10)

Predefined Folders

Add a Predefined Folder

1. Name is required.
2. [[A Folder Quick Set must contain one or more Folder destinations.]]

Name and Description

Name

Description

Select the folder type for this Quick Set.

Sign In Method: Windows Negotiated

● Save to a standard shared network folder

Folder Destinations

○ Save to a personal shared folder

Requires user sign-in and information specific to the user to create folder path.

□ Create Subfolder based upon username

Appends a user name subfolder at the end of the folder path.

□ Only allow access to user's own Directory

Sets read/write access.

☑ Verify folder access prior to job start

When unchecked, users can save jobs more quickly but jobs may fail if the folder is unavailable.

Credentials to Access Public Folders

Sign In Method

Username

Table 3-6 Configuration Utility elements

Callout	Component	Description
1	**Exclamation point**	An exclamation point (!) next to the name of a tab indicates that required data for that feature has not been supplied, or that some data is invalid. If an exclamation point exists on any tab you must navigate to that tab and change the settings so that the exclamation point is removed. There will be a blue field at the top of the dialog explaining what needs to be changed, and the fields that require change in the dialog will be surrounded with a blue border. DO NOT try to apply settings until all exclamation points are removed.
2	**Asterisk**	An asterisk (*) next to the name of a tab indicates that data has been entered, but not yet applied. The **Apply** button must be clicked in order to save the settings.
3	**Outline**	Required data is highlighted with an outline around the necessary setting. In this diagram the Name and UNC Folder Path settings are highlighted to indicate that those are required.

Licensing

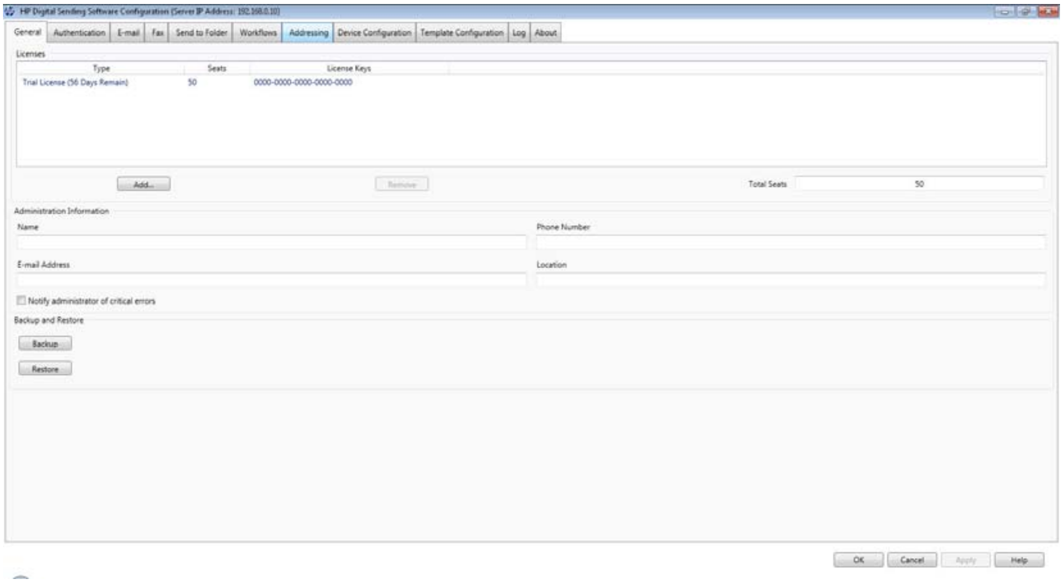
This section contains the following topics:

- Add licenses
- Remove licenses
- Auto-generated licenses

Add licenses

1. In the DSS Configuration Utility, click the **General** tab.

Figure 3-16 **General** tab – DSS Configuration Utility



HP Digital Sending Software Configuration (Server IP Address: 192.168.0.10)

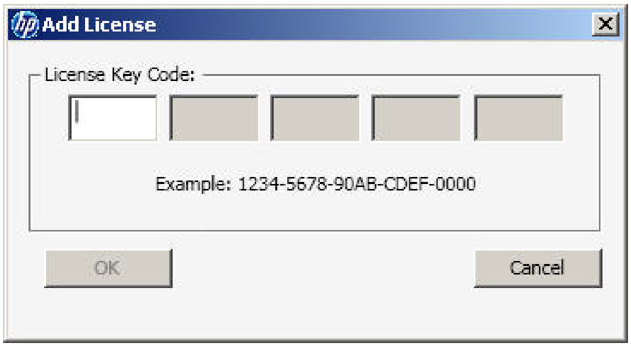
Type	Seats	License Keys
Trial License (56 Days Remain)	50	0000-0000-0000-0000-0000

Total Seats 50

□ Notify administrator of critical errors

2. In the **Licenses** section, click **Add...**. The **Add License** dialog box appears.

Figure 3-17 **Add License** dialog box



Example: 1234-5678-90AB-CDEF-0000

3. Type in the 20-digit license key code for the license you are installing, and then click **OK.**

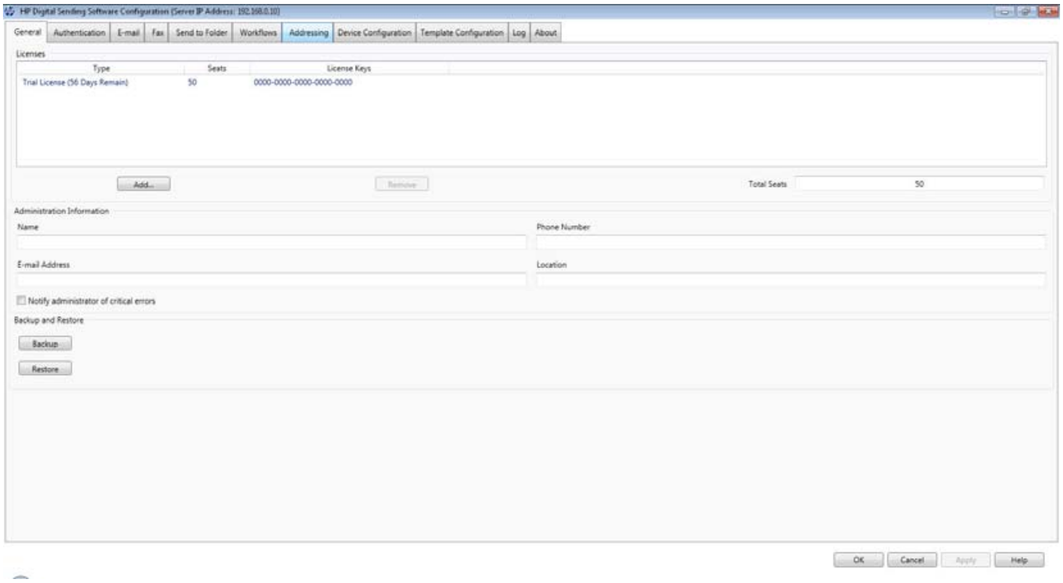
4. The new license appears in the **Licenses** list and the **Seats** field updates to reflect the additional seats provided by this license.

Remove licenses

In rare instances it is necessary to remove licenses from the DSS server. One condition that would prompt license removal from a DSS server would be to install those licenses on a new DSS server.

1. In the DSS Configuration Utility, click the **General** tab.

Figure 3-18 **General** tab – DSS Configuration Utility



HP Digital Sending Software Configuration (Server IP Address: 192.168.0.10)

Licenses

Type	Seats	License Keys
Trial License (56 Days Remain)	50	0000-0000-0000-0000-0000

Total Seats 50

2. In the **Licenses** section, click the license you want to remove, and then click **Remove**.

3. The license is removed from the **Licenses** list and the **Seats** field updates to reflect the current number of seats provided by any remaining licenses.

NOTE: If by removing a license, your total number of seats falls below the number of devices you currently have configured for Digital Sending features, you will be required to remove devices from the **Device List** on the **Device Configuration** tab to match the number of remaining sets available.

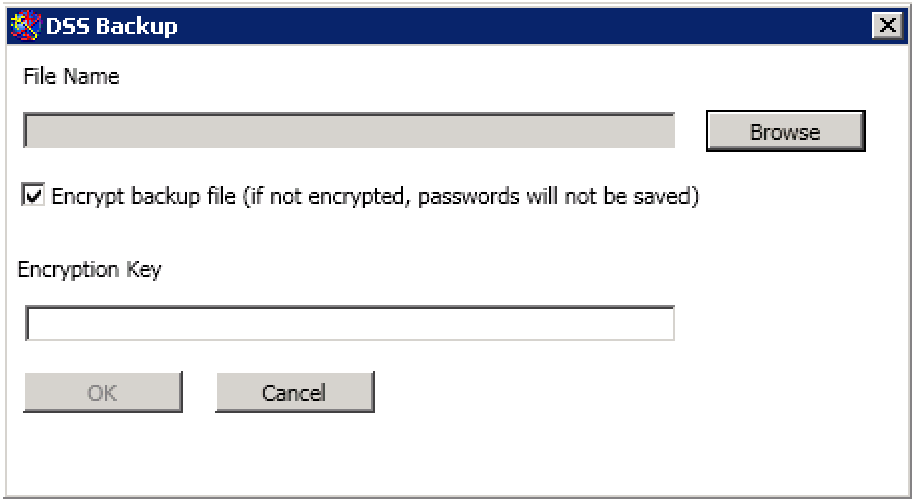
Auto-generated licenses

The HP LaserJet 9200c and 9250c devices auto-generate a license for use in DSS. This means that no additional license seat is required for these devices. Once these devices are managed by DSS, they will automatically generate a license that shows up in the DSS Configuration Utility.

Backup and Restore

Backup

Figure 3-19 DSS Backup



☑ Encrypt backup file (if not encrypted, passwords will not be saved)

Click the Backup button on the **General** tab of the Configuration Utility to reveal the DSS backup dialog box. The DSS Backup backs up DSS data stored on the DSS server. The DSS Backup does not include data which is stored on the devices themselves. When a device is opened for configuration via the Device Configuration tab of the CU, DSS displays device data that is not backed up.

When performing a DSS backup, all of the server data is collected; users cannot back up a portion of the DSS data. However, when restoring data from a backup file, an administrator can select which data to restore. Restoring all of the data at the same time is not a requirement.

By default, DSS assumes backup files will be encrypted. Encrypted backup files contain passwords that are stored in DSS. Passwords can exist in many places in DSS including (but not limited to):

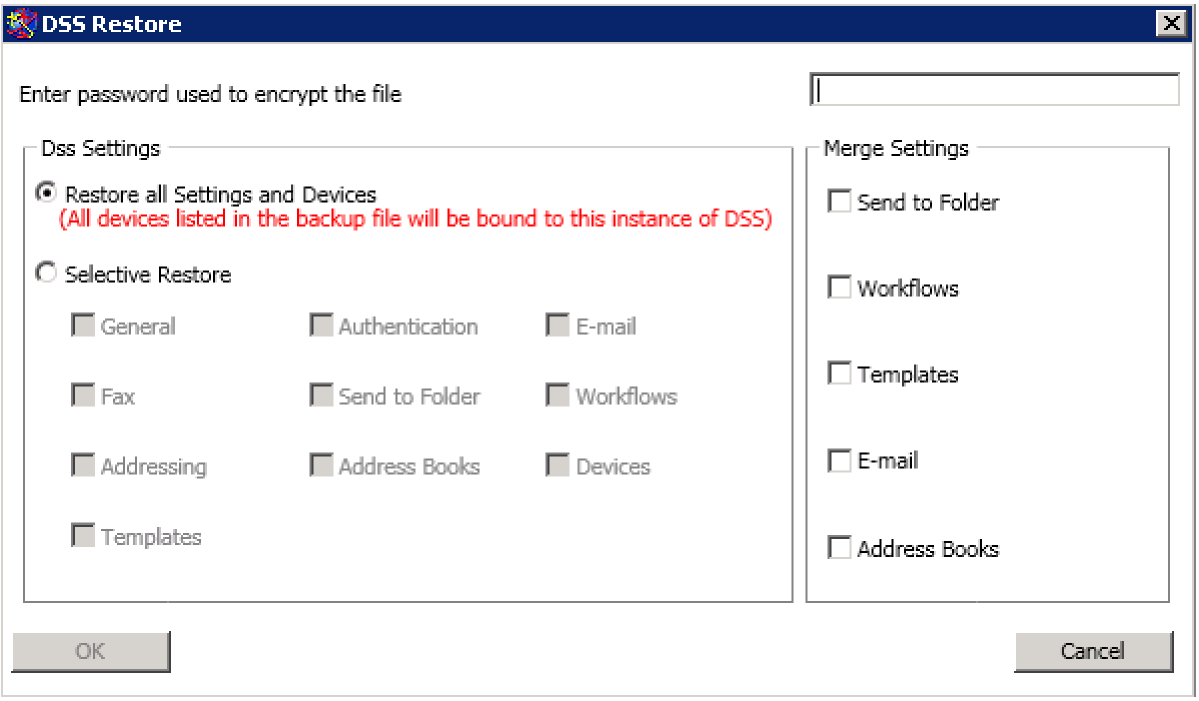
- Credentials for SMTP server authentication
- Credentials for LDAP server access for authentication or addressing
- Credentials for folder access in Send to Folder, Send to Workflow, or Send to LanFax

Administrators must provide an encryption key for encrypted backup files. Administrators must remember this key. DSS prompts administrators for it when attempting a Restore from this backup file.

If the backup is not encrypted, the file will not contain passwords and will be stored in an xml format. This may be useful in some circumstances (for example, when debugging some error conditions). In general, HP strongly suggests encrypting back up files. Encryption strengthens security and saves the administrator from having to remember and re-enter passwords after a Restore.

Restore

Figure 3-20 DSS Restore



DSS Restore

Enter password used to encrypt the file

Dss Settings

● Restore all Settings and Devices
(All devices listed in the backup file will be bound to this instance of DSS)

○ Selective Restore

□ General	□ Authentication	□ E-mail
□ Fax	□ Send to Folder	□ Workflows
□ Addressing	□ Address Books	□ Devices
□ Templates		

Merge Settings

□ Send to Folder

□ Workflows

□ Templates

□ E-mail

□ Address Books

Administrators may access the Restore functionality in the CU by selecting the **Restore** button in the General tab. The Restore function first prompts the administrator to select a DSS backup file from the file system. The DSS Restore dialog box appears when the administrator selects a backup file.

Administrators must provide an encryption key for encrypted backup files. This is the same encryption key provided at the time the backup file was created.

By default, the Restore feature assumes that all data in the backup file will be restored. However, administrators can restore selected portions of data by clicking the **Selective Restore** radio button, then selecting the check boxes beside the desired data items.

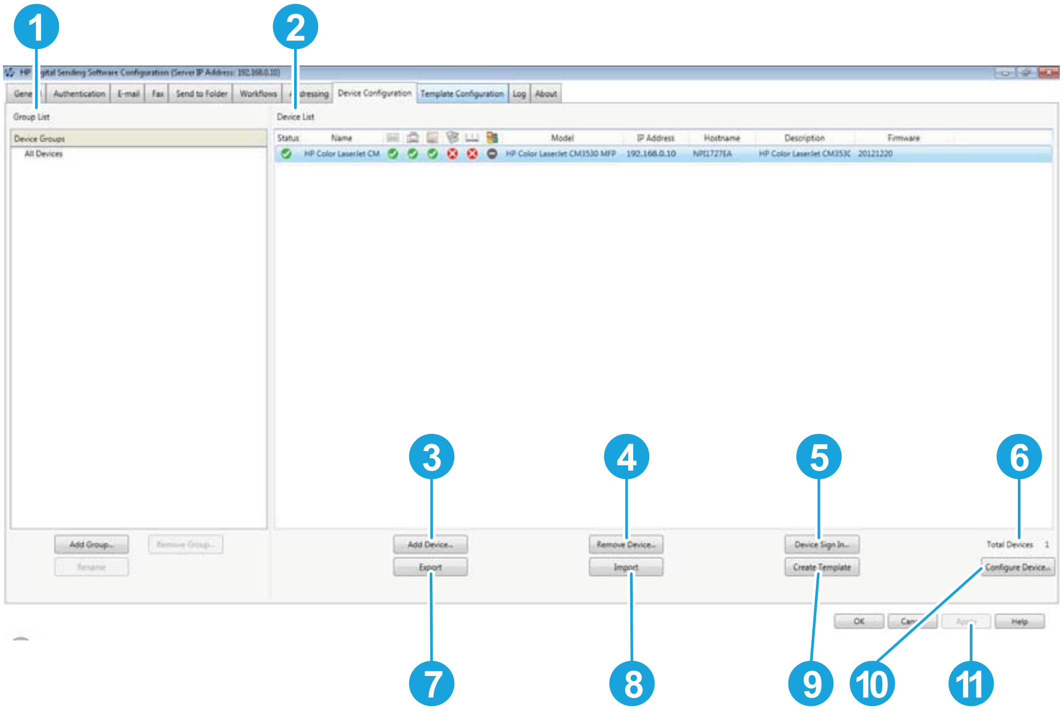
By default, the Restore function replaces the data currently on the DSS server with the data from the backup file. For some types of data, those for which there are lists of items, administrators can configure Restore to merge the data currently on the system with data from the backup file. Select the checkbox next to the desired data type to merge data in the **Merge Settings** area of the Restore dialog box.

Restore resolves duplicates by renaming one of them when merging settings. For example: if the current DSS server and the DSS backup file each contain a folder named FOLDER X, then the item from the backup file will be renamed FOLDER X(2) when it is restored.

Device management

The **Device Configuration** tab on the Configuration Utility specifies which devices are using the DSS service and also provides an interface for customizing DSS features for specific devices.

Figure 3-21 **Device Configuration** tab



HP Digital Sending Software Configuration (Server IP Address: 192.168.0.10)

Group List

Device Groups
All Devices

Device List

Status	Name							Model	IP Address	Hostname	Description	Firmware
✓	HP Color LaserJet CM	✓	✓	✓	✗	✗	⊖	HP Color LaserJet CM3530 MFP	192.168.0.10	NPI1727EA	HP Color LaserJet CM353C	20121220

Total Devices 1

The **Device Configuration** tab contains the following elements.

Table 3-7 **Device Configuration** tab

Callout	Component	Description
1	**Group List**	Use this list to organize the devices using the DSS service. ● **Add Group.** Click to create a new group. ● **Remove Group.** Click to remove a group. ● **Rename.** Click to change a group name.

Table 3-7 Device Configuration tab (continued)

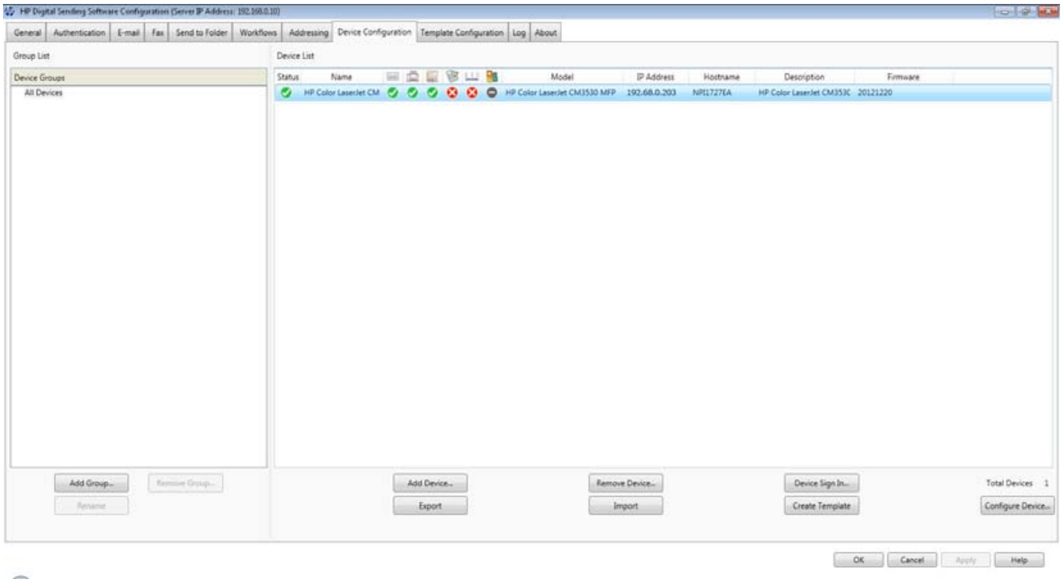
Callout	Component	Description
2	**Device List**	This list shows the individual devices using the DSS service as well as the features that are enabled or not enabled on each device. The **Device List** contains the following headings: ● **Status** ● **Name** ● **Send to E-mail icon** ● **Send to Fax icon** ● **Send to folder icon** ● **Workflow icon** ● **Authentication icon** ● **Addressing icon** ● **Model** ● **IP Address** ● **Hostname (will be blank if the device has been added by IP address)** ● **Description** ● Firmware
3	**Add Device**	Click to connect a new device to the DSS service. Once added, the device will appear in the Device List.
4	**Remove Device**	Click to select a device from the list, then click this button to remove the device.
5	**Device Sign-in**	Click this button to enter in a default set of credentials that can be used for communicating with FutureSmart devices that have their EWS password enabled.
6	**Total Devices**	Displays the total number of devices in the **Device List**.
7	**Export**	Saves, to a .csv file, the list of devices managed by DSS.
8	**Import**	Imports, from a .csv file, a list of devices that will be added to any devices currently in the device list.
9	**Create Template**	Select a device in the list and then click the **Create Template** button to create a template of device settings that match the settings in the selected device.
10	**Configure Device**	Click to select the device you want to configure, then use the sub-tabs to configure DSS features for the selected device.
11	**Apply**	Click this button to save changes made on this tab.

Add and remove devices

Add a device

1. On the DSS server, open the Configuration Utility, and then click the **Device Configuration** tab.

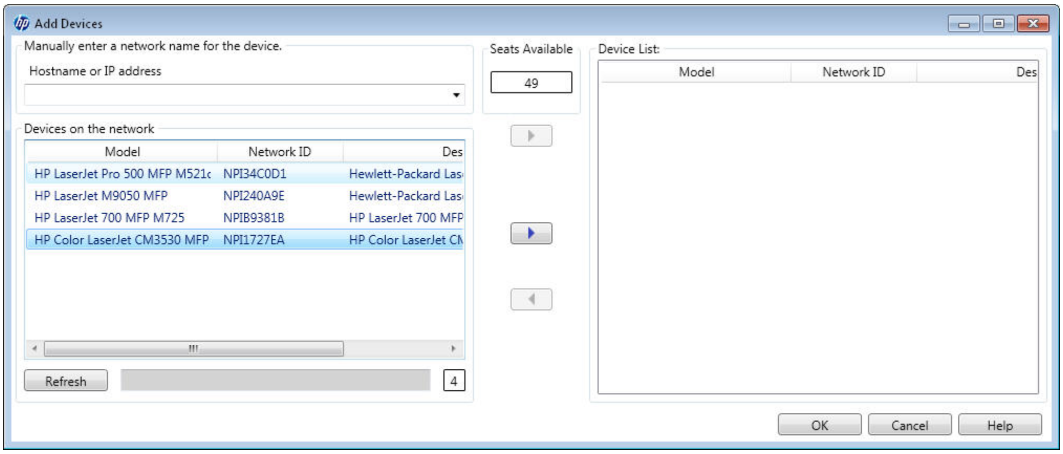
Figure 3-22 **Device Configuration** tab



Status	Name							Model	IP Address	Hostname	Description	Firmware
✓	HP Color LaserJet CM	✓	✓	✓	☒	☒	●	HP Color LaserJet CM3530 MFP	192.68.0.203	NPI1727EA	HP Color LaserJet CM353C	20121220

2. Click **Add Device...**. The **Add Devices** dialog box appears.

Figure 3-23 **Add Devices** dialog box



Model	Network ID	Des
HP LaserJet Pro 500 MFP M521c	NPI34C0D1	Hewlett-Packard Las
HP LaserJet M9050 MFP	NPI240A9E	Hewlett-Packard Las
HP LaserJet 700 MFP M725	NPIB9381B	HP LaserJet 700 MFP
HP Color LaserJet CM3530 MFP	NPI1727EA	HP Color LaserJet CN

3. If you know the hostname or TCP/IP address of the device, you can type it in the **Hostname or IP Address** text box under **Manually enter a device's network name** heading. Click the right-arrow **>** or press the Enter key to add the device to the **Device List**.

   -or-

   Select a device from the **Devices on the network** list, and then click the right-arrow **>** or press the Enter key to add the device to the **Device List**.

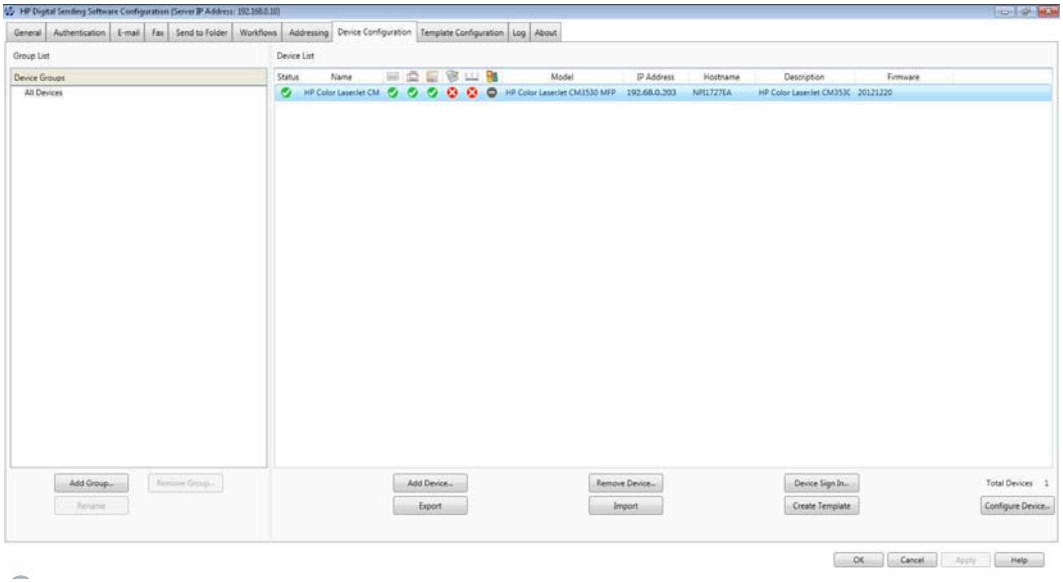
4. Click the **OK** button to close the **Add Devices** dialog box.

NOTE: You can add only as many DSS-enabled devices as there are seats available in the DSS license. The number of seats available appears near the top of the **Add Devices** dialog box.

Remove a device

1. On the DSS server, open the Configuration Utility, and then click the **Device Configuration** tab.

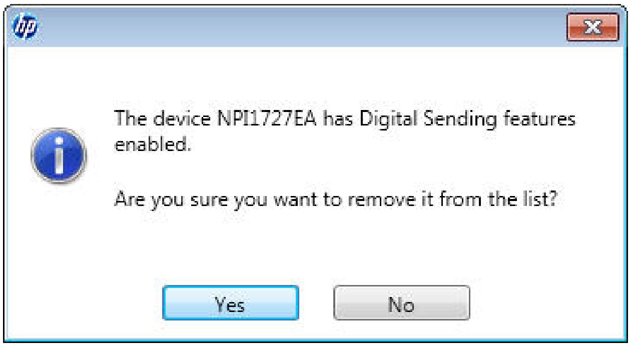
Figure 3-24 **Device Configuration** tab



Status	Name							Model	IP Address	Hostname	Description	Firmware
✓	HP Color LaserJet CM	✓	✓	✓	✗	✗	●	HP Color LaserJet CM3530 MFP	192.68.0.203	NPI1727EA	HP Color LaserJet CM353C	20121220

2. In the **Device List**, click to select the device you want to remove, and then click **Remove Device**. The **Remove Device** dialog box appears.

Figure 3-25 **Remove Device** dialog box


The device NPI1727EA has Digital Sending features enabled.

Are you sure you want to remove it from the list?

3. Click **Yes** to remove DSS-enabled devices.

Device configuration

After adding a new device (or group of devices), use the following procedure to configure the Digital Sending features for the device or group.

1. On the DSS server, open the Configuration Utility and click the **Device Configuration** tab.

2. Select a device from the **Device List**.

3. Click **Configure Device**. The dialog box that appears looks similar to the main Configuration program interface. Use this interface to customize the specific Digital Sending settings for this device.

NOTE: Use this interface to enable the Digital Sending features for the individual devices. Even if a feature is enabled on the DSS configuration tabs, it is not available on the device until it has been enabled in the **Configure Device** interface.

4. On the **General** tab, server administrators name, phone number, e-mail address, and optional location.

5. On the **Authentication** tab, click to select the check box for the authentication method you want to use to enable authentication for the selected device. Select the check boxes next to the features that are being enabled. Enabling authentication requires the user to log in before using the selected features. Select the network domain from the **Default Domain** drop-down menu.

6. On the **Send to E-mail** tab, select the **Enable Send to E-mail** check box, and then select either **Directly from the device** or **via the Digital Sender service** in the **Send E-mail** drop-down list.

   When sending e-mail directly from the device, specify the SMTP server, port number, and server usage settings to use.

   Then use the controls in the **Address and Message Field Control** and **File Settings** sections to customize the Send to E-mail settings for the selected device.

7. On the **Fax** tab, select the **Enable Fax Send** check box to enable the fax feature. Select the desired fax method in the drop-down menu.

8. On the **Send to Folder** tab, select the **Enable Send to Folder** check box to enable this feature.

9. On the **Send to Workflows** tab, select the **Enable Send to Workflows** check box to enable workflows and configure settings.

10. On the **Addressing** tab, select the **Enable Network Contacts (use LDAP server)** check box if DSS should retrieve e-mail addresses directly from an LDAP server. Enter the LDAP server Hostname or IP address, or click the "Auto Find" button. Then enter the LDAP port number (usually 389).

11. The **Log** tab will show a list of job logs for jobs that have been sent from that device.

12. On the **Preferences** tab, set the default scanner settings and the timeout settings for digital sending operations. The Preferences tab is only available for pre-FutureSmart devices.

13. Click **Apply** to save all of the changes.

NOTE: The settings are not propagated to the device until **Apply** is selected.

Understanding the Device List icons

The **Device List** on the **Device Configuration** tab shows the DSS-enabled devices that are currently being served by DSS. The icon to the left of the device name indicates the status of the device.

Table 3-8 **Device List icons**

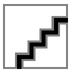
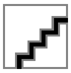
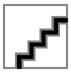
Icon	Description
	Communication with the device is established and the configuration settings are known.
	The device configuration has not been retrieved since the Configuration Utility was loaded.
	DSS can communicate with the device but the device is no longer configured to be managed by DSS. It is possible that device settings have been reset by an administrator or service technician from the control panel or using the Embedded Web Server.

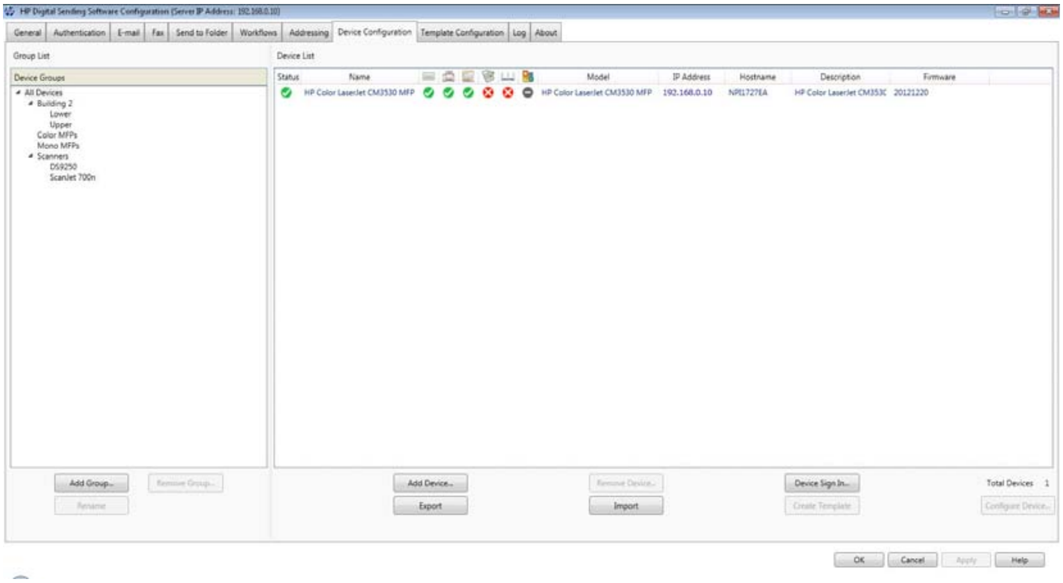
Table 3-8 Device List icons (continued)

Icon	Description
	The device was seized by another computer that is running the Configuration Utility. The TCP/IP address of the other computer is available under the **Status** heading on the **Device List**. To reclaim ownership of a seized device, right-click the crossbones icon and click **OK** in the two dialog boxes that appear.
	DSS is unable to establish communication with the device and the settings are unknown.

Device grouping

Device grouping provides the ability to organize devices for more efficient configuration and management.

Figure 3-26 Device grouping



Status	Name							Model	IP Address	Hostname	Description	Firmware
✓	HP Color LaserJet CM3530 MFP	✓	✓	✓	✗	✗	⊖	HP Color LaserJet CM3530 MFP	192.168.0.10	NPI1727EA	HP Color LaserJet CM353C	20121220

Create a device group

1. Open the Configuration Utility, and then click the **Device Configuration** tab.

2. Select the group in which you want to add a new group or select **All Devices**. Device groups can be nested within other groups.

3. Click **Add group**.

4. Type a name for the new group.

Add devices to a group

1. Right-click on a device and select **Add to Group**.

2. Click the desired group for this device.

Remove devices from a group

1. Right-click on a device and select **Remove**.
2. Click **Remove from Group**.

Authentication

Authentication is a security feature that requires users to provide a network username and password before using Digital Sending features. Authentication can be turned on or off for individual features within each device that DSS supports.

NOTE: At no time are the credentials that are used to authenticate at the device written to either the DSS server or the device hard disk. In addition, although the credentials that the DSS administrator uses to configure authentication or LDAP addressing are written to the DSS server hard disk, encryption is incorporated to ensure that these credentials cannot be recovered.

Configure DSS

This section contains the following topics:

- Authentication methods

Authentication methods

This section describes the two methods of authentication:

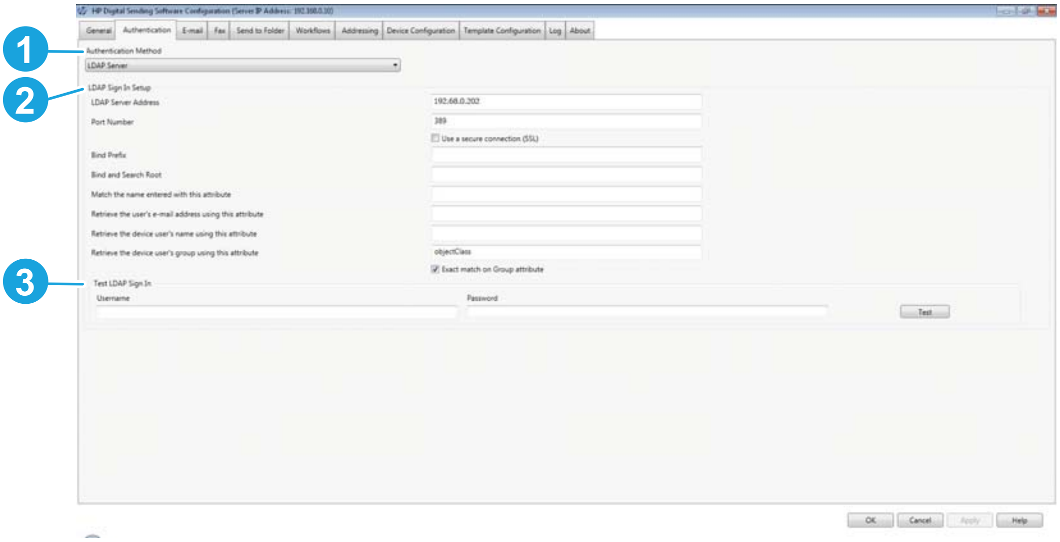
- LDAP authentication
- Windows Active Directory

LDAP Server

Many modern computer systems store and organize data in Directories. A Directory is a set of data where the data for a particular entity is kept in a container and all the containers are organized in a tree structure. Microsoft's Active Directory, the database associated with Windows Domain Controllers, is a Directory based database, but there are many implementations of Directories from different vendors. Directories not only store data but provide other services such as security and the ability to authenticate users for Directory access.

LDAP, or Lightweight Directory Access Protocol, is an industry standard protocol for interacting with Directories. Servers that host a directory which supports the LDAP protocol are called LDAP servers. The LDAP configuration tab is where DSS is configured with all of the information it needs to interact with an LDAP server in order to authenticate a user that has entered LDAP credentials at the device control panel.

Figure 3-27 **Authentication** tab – LDAP Server



Authentication Method: LDAP Server

LDAP Sign In Setup

LDAP Server Address	192.68.0.202
Port Number	389
	□ Use a secure connection (SSL)
Bind Prefix	
Bind and Search Root	
Match the name entered with this attribute	
Retrieve the user's e-mail address using this attribute	
Retrieve the device user's name using this attribute	
Retrieve the device user's group using this attribute	objectClass
	☑ Exact match on Group attribute

Test LDAP Sign In

Username

Password

The LDAP Server option on the **Authentication** tab contains the following elements.

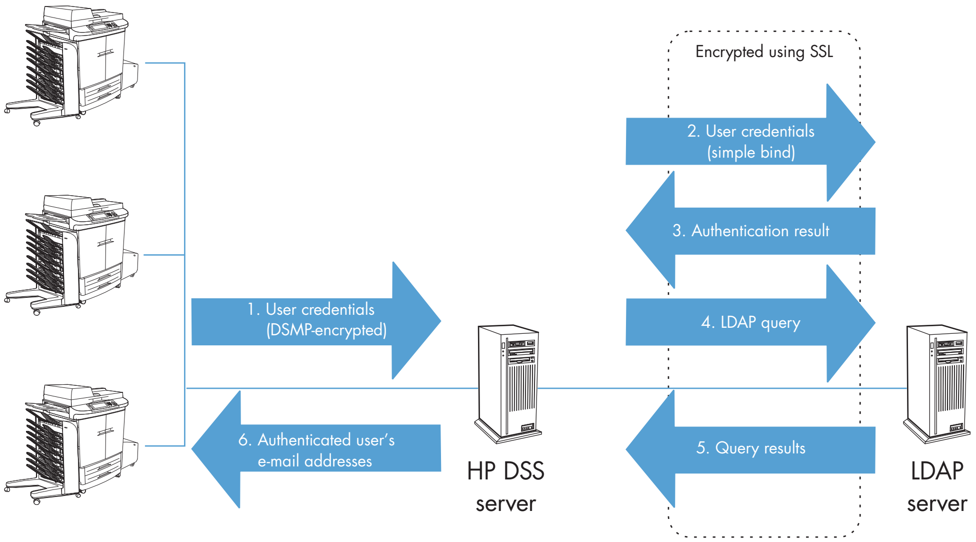
Table 3-9 **Authentication tab – LDAP Server**

Callout	Component	Description
1	**Authentication method**	Select **LDAP Server** from the drop-down menu.

Table 3-9 Authentication tab – LDAP Server (continued)

Callout	Component	Description
2	LDAP Sign In Setup	Use the following fields to set up the sign-in method. Provide the appropriate LDAP attribute name for your environment. ● **LDAP Server address** ● **Port number** NOTE: Select **Use a secure connection (SSL)** to enable an SSL (Secure Sockets Layer) connection. ● **Bind prefix**: This is the attribute that guarantees uniqueness between any container in the Directory and other containers at the same level in the directory tree. The is commonly the attribute 'cn', but can be configured by the LDAP administrator to be any attribute. ● **Bind and Search Root**: The search root is the distinguished name (DN) of the entry in the LDAP directory where the search is to begin. A DN is made up of '*attribute=value*' pairs separated by commas. In Windows Active Directory Services, the search root normally takes the form: `CN=Users,DC=domain_name,DC=domain_suffix`. To limit the address search even more, for example, to a single organizational unit (OU), add components to the search root. For example, to search for users in the "accounting" OU, add "`OU=accounting`" to the search root (`OU=accounting,CN=Users,DC=domain_name,DC=domain_suffix`). By using these methods to configure the search root that is used in authentication, access to Digital Sending features can be limited to a subset of users in an organization. Several methods can be used to determine the search root. NOTE: On some LDAP servers, the search root can remain blank. In this case, the root node is assumed to be the starting place. ● **Match the name entered with this attribute** ● **Retrieve the user's e-mail address using this attribute** ● **Retrieve the device user's name using this attribute** ● **Retrieve the device user's group using this attribute** To allow an exact match only, click to select the **Exact match on Group attribute** check box.
3	Test LDAP Sign in	Type information into the following fields, and then click **Test** to test the LDAP Server sign-in setup. ● **Username** ● **Password**

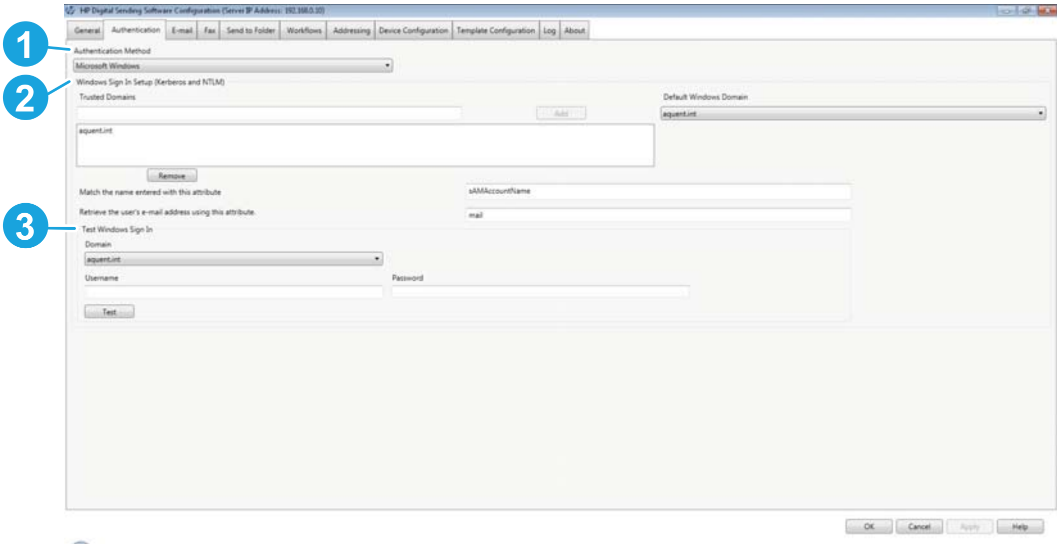
Figure 3-28 LDAP authentication


Encrypted using SSL
2. User credentials (simple bind)
3. Authentication result
4. LDAP query
5. Query results
1. User credentials (DSMP-encrypted)
6. Authenticated user's e-mail addresses
HP DSS server
LDAP server

Microsoft Windows

When a user signs-in for Windows authentication, they provide a domain, user name, and password. DSS communicates with the domain controller associated with the domain provided by the user to authenticate the user. In addition to domain controller authentication, DSS also retrieves some data items about the user, such as e-mail address, from an LDAP database. By default, the LDAP database that DSS gathers user information from is the Active Directory database associated with the domain controller being used to authenticate the user.

Figure 3-29 **Authentication** tab – Microsoft Windows



Authentication Method: Microsoft Windows

Windows Sign In Setup (Kerberos and NTLM)

Trusted Domains: aquent.int

Default Windows Domain: aquent.int

Match the name entered with this attribute: sAMAccountName

Retrieve the user's e-mail address using this attribute: mail

Test Windows Sign In

Domain: aquent.int

Username

Password

The Microsoft Windows option on the **Authentication** tab contains the following elements.

Table 3-10 Authentication tab – Microsoft Windows

Callout	Component	Description
1	**Authentication method**	Select **Microsoft Windows** from the drop-down menu.

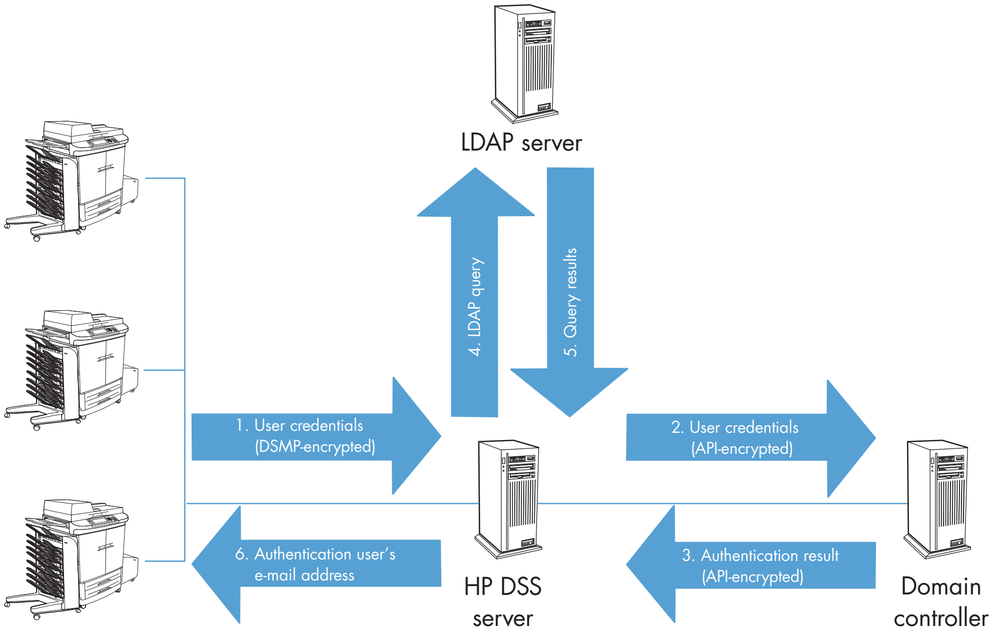
Table 3-10 Authentication tab – Microsoft Windows (continued)

Callout	Component	Description
2	Windows Sign in Setup (Kerberos and NTLM)	Click **Add** to add domains to the **Trusted Domains** list. Click **Remove** to remove domains from the list. Select the **Default Windows Domain** from the drop-down menu. Use the following fields to set up the sign-in method. ● **Match the name entered with this attribute** ● **Retrieve the user's e-mail address using this attribute**
3	Test Windows Sign In	Type information into the following fields, and then click **Test** to test the Microsoft Windows sign-in setup. ● **Domain** ● **Username** ● **Password**

As shown in Figure 3-30 Windows Active Directory authentication on page 62, the following steps occur during Windows authentication:

1. The user types his or her username and password at the device. This information is securely transmitted to the DSS server.
2. The DSS program authenticates to the domain through the Windows API to validate the user's credentials.
3. If the user's credentials are correct, the Domain Controller returns either the security identifier (SID) or the BSID (Binary SID).
4. Using the LDAP interface, DSS queries the LDAP directory for the authenticated user's e-mail address.
5. The LDAP directory returns the authenticated user's e-mail address.
6. DSS inserts the authenticated user's e-mail address in the **From:** text box of the e-mail and prohibits the user from changing the field.

Figure 3-30 Windows Active Directory authentication


LDAP server
4. LDAP query
5. Query results
1. User credentials (DSMP-encrypted)
2. User credentials (API-encrypted)
6. Authentication user's e-mail address
3. Authentication result (API-encrypted)
HP DSS server
Domain controller

Windows Two Server authentication

DSS can be configured to use an LDAP database other than the Active Directory database for user data retrieval. The configuration for Two Server authentication is partially done using the Windows authentication user interface and partially done using a configuration file.

All of the fields in the user interface are still used except for the **Match the name entered with this attribute** and **Retrieve the user's e-mail address using this attribute** fields. The **Trusted Domains** and **Windows default domain** settings from the user interface are still required.

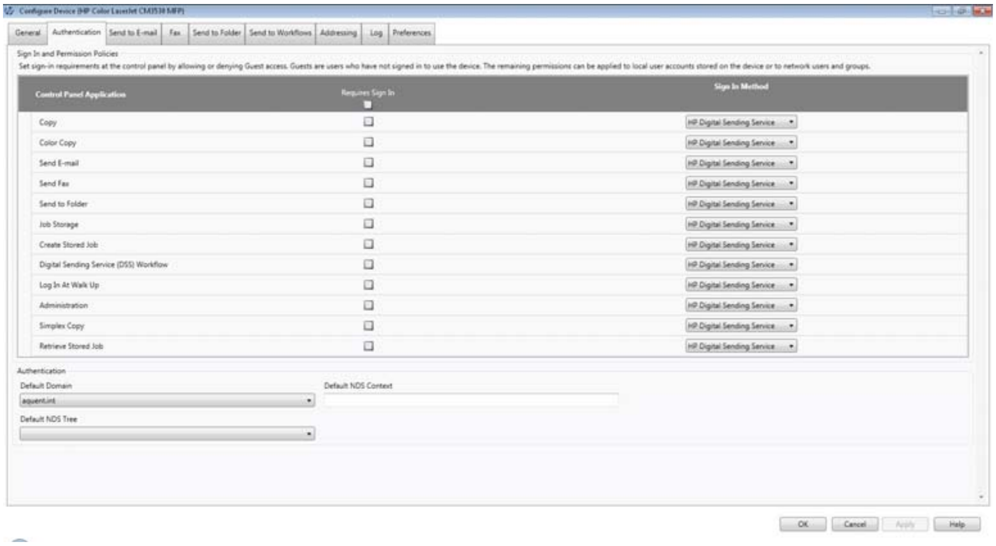
The configuration used for Windows Two Server authentication is:

```
<install folder>\FileSystems\Product\Dss\Configuration
\HP.Dss.App.Utilities.TwoServerAuthentication.xml
```

Use this file to configure information DSS needs to find and access the LDAP database and which attributes to retrieve. See the documentation in the file for further configuration information.

Configure the Device

Figure 3-31 **Authentication** subtab – Configure Devices tab set



Sign In and Permission Policies

Set sign-in requirements at the control panel by allowing or denying Guest access. Guests are users who have not signed in to use the device. The remaining permissions can be applied to local user accounts stored on the device or to network users and groups.

Control Panel Application	Requires Sign In □	Sign In Method
Copy	□	HP Digital Sending Service
Color Copy	□	HP Digital Sending Service
Send E-mail	□	HP Digital Sending Service
Send Fax	□	HP Digital Sending Service
Send to Folder	□	HP Digital Sending Service
Job Storage	□	HP Digital Sending Service
Create Stored Job	□	HP Digital Sending Service
Digital Sending Service (DSS) Workflow	□	HP Digital Sending Service
Log In At Walk Up	□	HP Digital Sending Service
Administration	□	HP Digital Sending Service
Simplex Copy	□	HP Digital Sending Service
Retrieve Stored Job	□	HP Digital Sending Service

Authentication

Default Domain: aquent.int

Default NDS Context:

Default NDS Tree:

The **Authentication** subtab on the Configure Devices tab set contains the following elements.

Table 3-11 Authentication subtab — Configure Devices tab set

Callout	Component	Description
1	Sign In and Permission Policies	Requires Sign-In: To require that a user must sign-in to use a feature in the device, check the **Requires Sign In** checkbox in that feature's row. Sign In method: In the **Sign-In Method** drop down list, select the authentication agent to use for sign-in for that feature. Authentication agents are software that collect the user's sign-in credentials and authenticate those credentials against the appropriate authority. The device firmware has built into it two different possible authentication agents to choose from, one for Windows authentication and the second for LDAP authentication. DSS can also act as an authentication agent (if it was configured to work that way when configuring the **Authentication** tab in the DSS service) and can be chosen from the drop down menu as one of the selections when a device is managed by DSS. It is also possible that other, 3rd party, authentication agents will be available to choose from if they have been installed on this device. Some popular 3rd party agents are HP Access Control and Safecom.
2	Authentication	Add the following information to enable authentication. ● **Default domain**

General Device configuration

This section contains information about some of the more general sub-tabs available on the **Configure Devices** tab set in the Configuration Utility. Use this tab set to configure individual DSS-enabled devices. The following tabs are included in this section:

- General subtab
- Addressing subtab

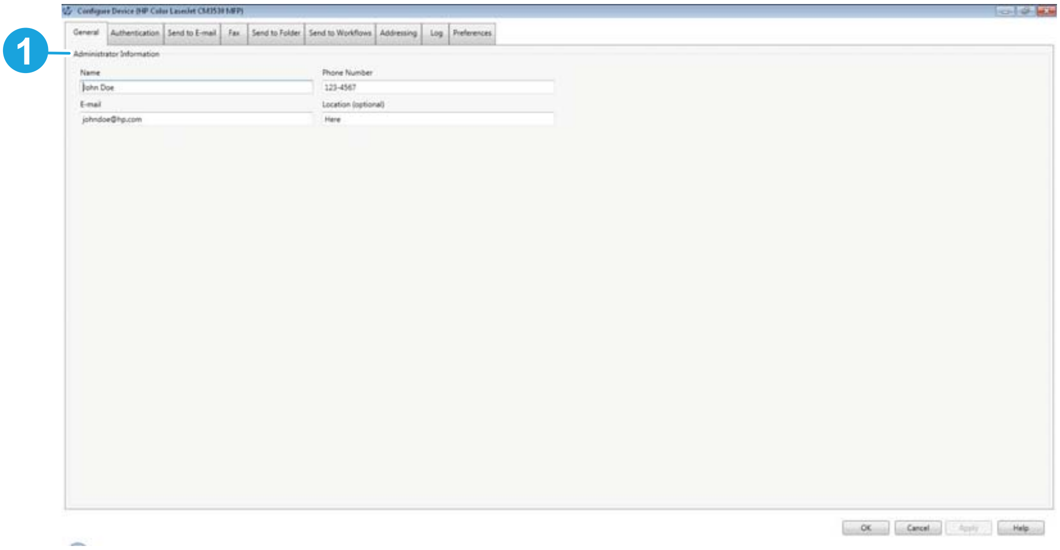
- Log subtab
- Preferences subtab

For information about the remaining tabs, see the following topics:

- Table 3-11 Authentication subtab — Configure Devices tab set on page 63
- Fax subtab — Configure the Device on page 78
- Table 3-18 Send to Workflows subtab – Configure Devices tab set on page 89

General subtab

Figure 3-32 **General** subtab in the Configure Devices tab set



Administrator Information

Name: John Doe

Phone Number: 123-4567

E-mail: johndoe@hp.com

Location (optional): Here

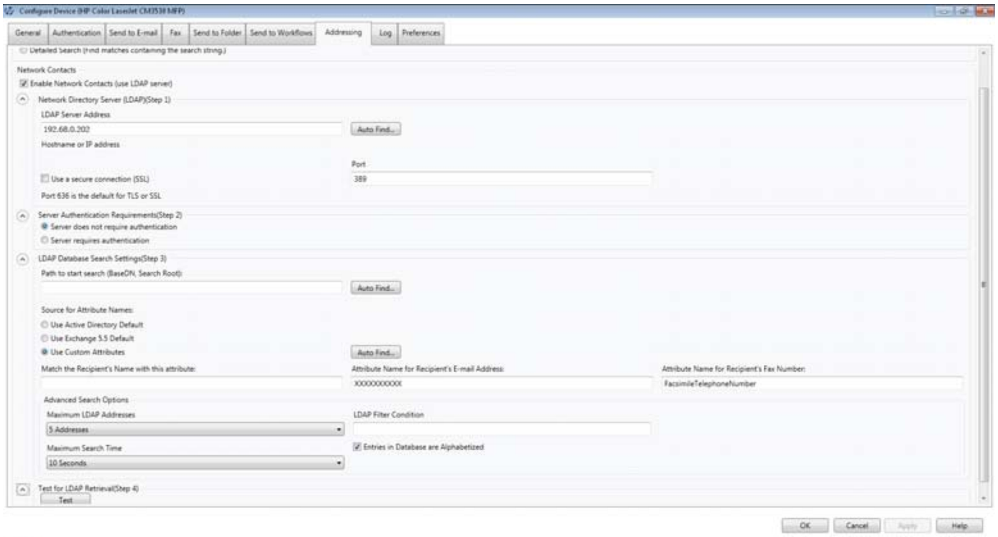
The **General** subtab in the Configure Devices tab set contains the following elements.

Table 3-12 **General subtab on the Configure Devices tab set**

Callout	Component	Description
1	**Administrator Information**	The General tab allows you to configure settings common to all the Digital Sending features supported on the device. The device displays the Administrator Contact Information when an error occurs that requires administrator intervention. ● In the Name edit box, enter the name of the person responsible for maintaining the Digital Sending features of this device. ● In the E-mail Address edit box, enter the e-mail address of the person responsible for maintaining the Digital Sending features of this device. ● In the Phone Number (optional) edit box, optionally enter the phone number of the person responsible for maintaining the Digital Sending features of this device. ● In the Location (optional) edit box, optionally enter the physical location of the person responsible for maintaining the Digital Sending features of this device.

Addressing subtab

Figure 3-33 **Addressing** subtab on the **Device Configuration** tab set



○ Detailed Search (Find matches containing the search string.)

Network Contacts

☑ Enable Network Contacts (use LDAP server)

Network Directory Server (LDAP)(Step 1)

LDAP Server Address: 192.68.0.202

Hostname or IP address

☐ Use a secure connection (SSL)

Port: 389

Port 636 is the default for TLS or SSL

Server Authentication Requirements(Step 2)

● Server does not require authentication

○ Server requires authentication

LDAP Database Search Settings(Step 3)

Path to start search (BaseDN, Search Root):

Source for Attribute Names:

○ Use Active Directory Default

○ Use Exchange 5.5 Default

● Use Custom Attributes

Match the Recipient's Name with this attribute:

Attribute Name for Recipient's E-mail Address: XXXXXXXXXX

Attribute Name for Recipient's Fax Number: FacsimileTelephoneNumber

Advanced Search Options

Maximum LDAP Addresses: 5 Addresses

LDAP Filter Condition:

Maximum Search Time: 10 Seconds

☑ Entries in Database are Alphabetized

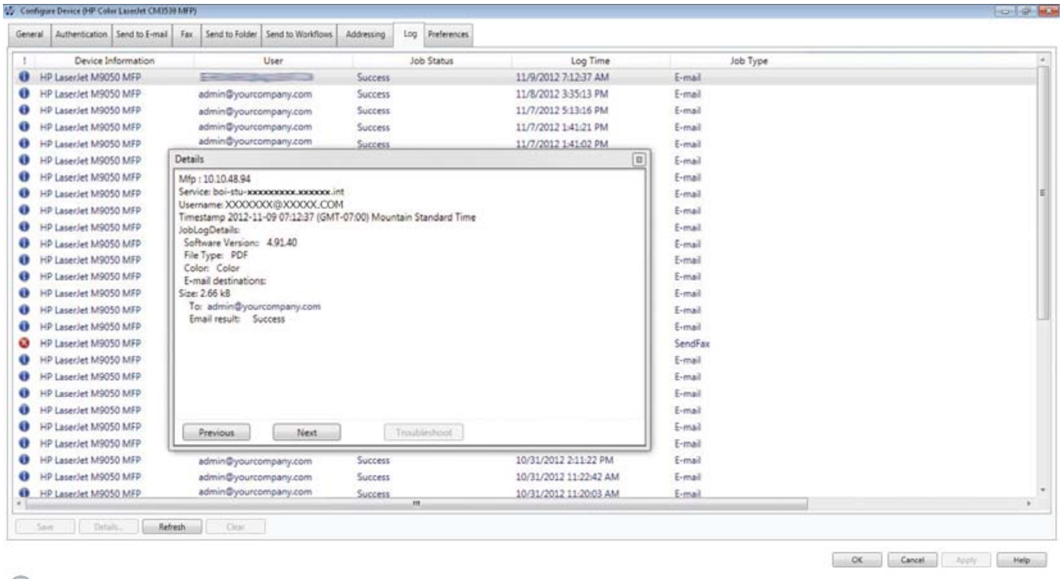
Test for LDAP Retrieval(Step 4)

The **Addressing** tab is used to configure a device's ability to get address information directly from an LDAP server, without the use of DSS. This direct device addressing can be used whether or not DSS LDAP replication is enabled. Any addresses collected directly by the device will be merged with addresses from DSS address books for the user to select from at the control panel.

Log subtab

The **Log** subtab on the **Configure Device** tab set displays the job log information for jobs sent from that device.

Figure 3-34 **Log** subtab in the Configure Devices tab set



!	Device Information	User	Job Status	Log Time	Job Type
ℹ	HP LaserJet M9050 MFP	[redacted]	Success	11/9/2012 7:12:37 AM	E-mail
ℹ	HP LaserJet M9050 MFP	admin@yourcompany.com	Success	11/8/2012 3:35:13 PM	E-mail
ℹ	HP LaserJet M9050 MFP	admin@yourcompany.com	Success	11/7/2012 5:13:16 PM	E-mail
ℹ	HP LaserJet M9050 MFP	admin@yourcompany.com	Success	11/7/2012 1:41:21 PM	E-mail
ℹ	HP LaserJet M9050 MFP	admin@yourcompany.com	Success	11/7/2012 1:41:02 PM	E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
✖	HP LaserJet M9050 MFP				SendFax
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP				E-mail
ℹ	HP LaserJet M9050 MFP	admin@yourcompany.com	Success	10/31/2012 2:11:22 PM	E-mail
ℹ	HP LaserJet M9050 MFP	admin@yourcompany.com	Success	10/31/2012 11:22:42 AM	E-mail
ℹ	HP LaserJet M9050 MFP	admin@yourcompany.com	Success	10/31/2012 11:20:03 AM	E-mail

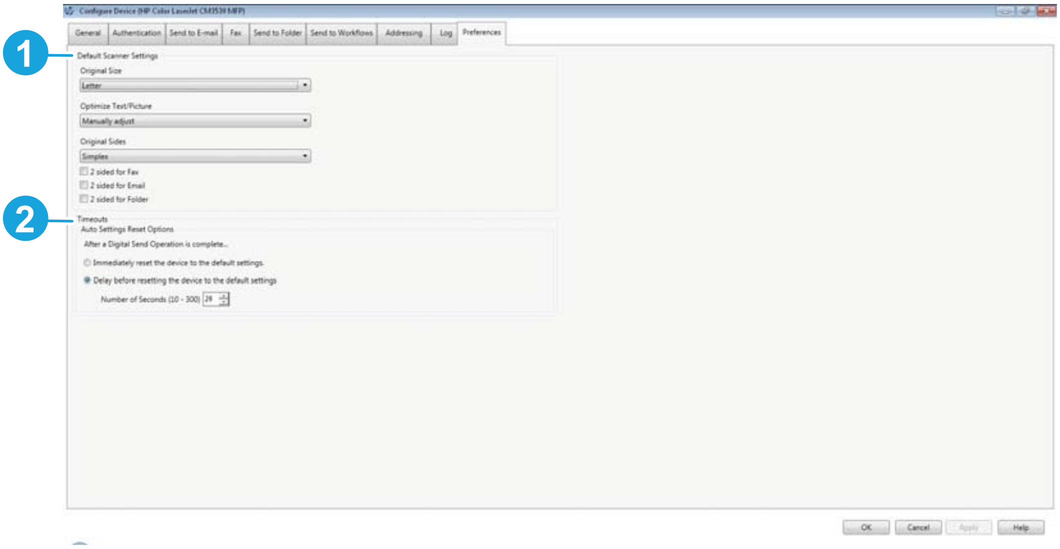
Details

```
Mfp : 10.10.48.94
Service: boi-stu-xxxxxxxxxx.xxxxxxx.int
Username: XXXXXXX@XXXXX.COM
Timestamp 2012-11-09 07:12:37 (GMT-07:00) Mountain Standard Time
JobLogDetails:
  Software Version:   4.91.40
  File Type:   PDF
  Color:   Color
  E-mail destinations:
Size: 2.66 kB
    To:  admin@yourcompany.com
    Email result:     Success
```

Preferences subtab

The **Preferences** subtab is only available on pre-FutureSmart devices.

Figure 3-35 **Preferences** subtab in the Configure Devices tab set



Default Scanner Settings

Original Size: Letter

Optimize Text/Picture: Manually adjust

Original Sides: Simplex

☐ 2 sided for Fax

☐ 2 sided for Email

☐ 2 sided for Folder

Timeouts

Auto Settings Reset Options

After a Digital Send Operation is complete...

○ Immediately reset the device to the default settings.

● Delay before resetting the device to the default settings

Number of Seconds (10 - 300) 20

The **Preferences** subtab contains the following controls.

Table 3-13 Preferences subtab on the Configure Devices tab set

Callout	Component	Description
1	**Default Scanner Settings**	Use **Default Scanner Settings** to set the default settings for document size, expected page content, and duplexing: ● **Original Size** ● **Optimize Text/Picture** ● **Original Sides** NOTE: On FutureSmart devices these settings are set individually for each send feature – e-mail, fax, folder, and workflow. On pre-FutureSmart devices these settings are set once and apply globally to *all* the send features.
2	**Timeouts**	Use the controls in the **Time-outs** group box to control the delay before the device returns to its default digital-send settings. The following options are available to control the auto settings resets: NOTE: These specific time-outs do not exist for FutureSmart devices. ● **Immediate reset to defaults** ● **Delay reset to defaults** ● **Number of seconds** combo box – choose from 1 to 30 seconds.

Send to Folder

The Digital Sending features of the device can send scanned documents directly to a network folder, transforming paper-based information into digital images that can be shared, stored, or edited.

Configure DSS

Use the Configuration Utility **Send to Folder** tab to set up the Send to Folder feature and select network folders to send to.

Figure 3-36 The **Send to Folder** tab

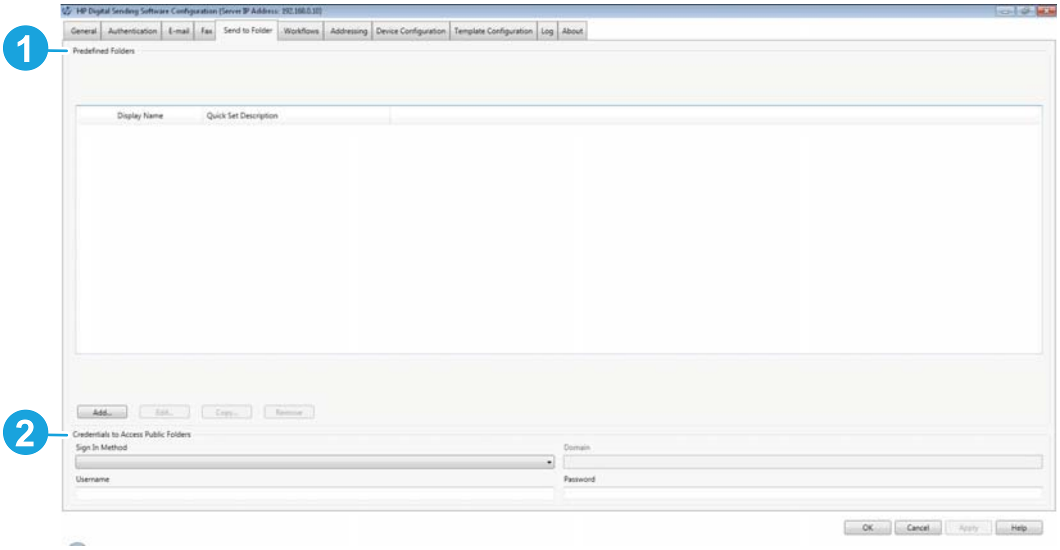


Table 3-14 Send to Folder tab

Callout	Component	Description
1	**Predefined folders**	The **Predefined folders** list shows the folders as they are added to the DSS service. These folders are available at the device. The **Display name**, **UNC Folder path**, and **Credentials** for each folder are listed here. The following controls are also available for configuring the folders. ● **Add**. Click to add a new folder ● **Edit**. Click to edit settings for the selected folder. ● **Copy**. Click to copy a folder. ● **Remove**. Click to remove a folder from the list of available folders. ● **Test**. Click to test folder settings.
2	**Credentials to Access Public Folders**	Use the **Credentials to Access Public Folders** to define a common set of service credentials that can be used for Windows folder access. When defining a folder destination, then these credentials can be configured to be what DSS uses for folder access rights. ● **Username**. Type in the username. ● **Password**. Type in the password. ● **Domain**. Type in the domain.

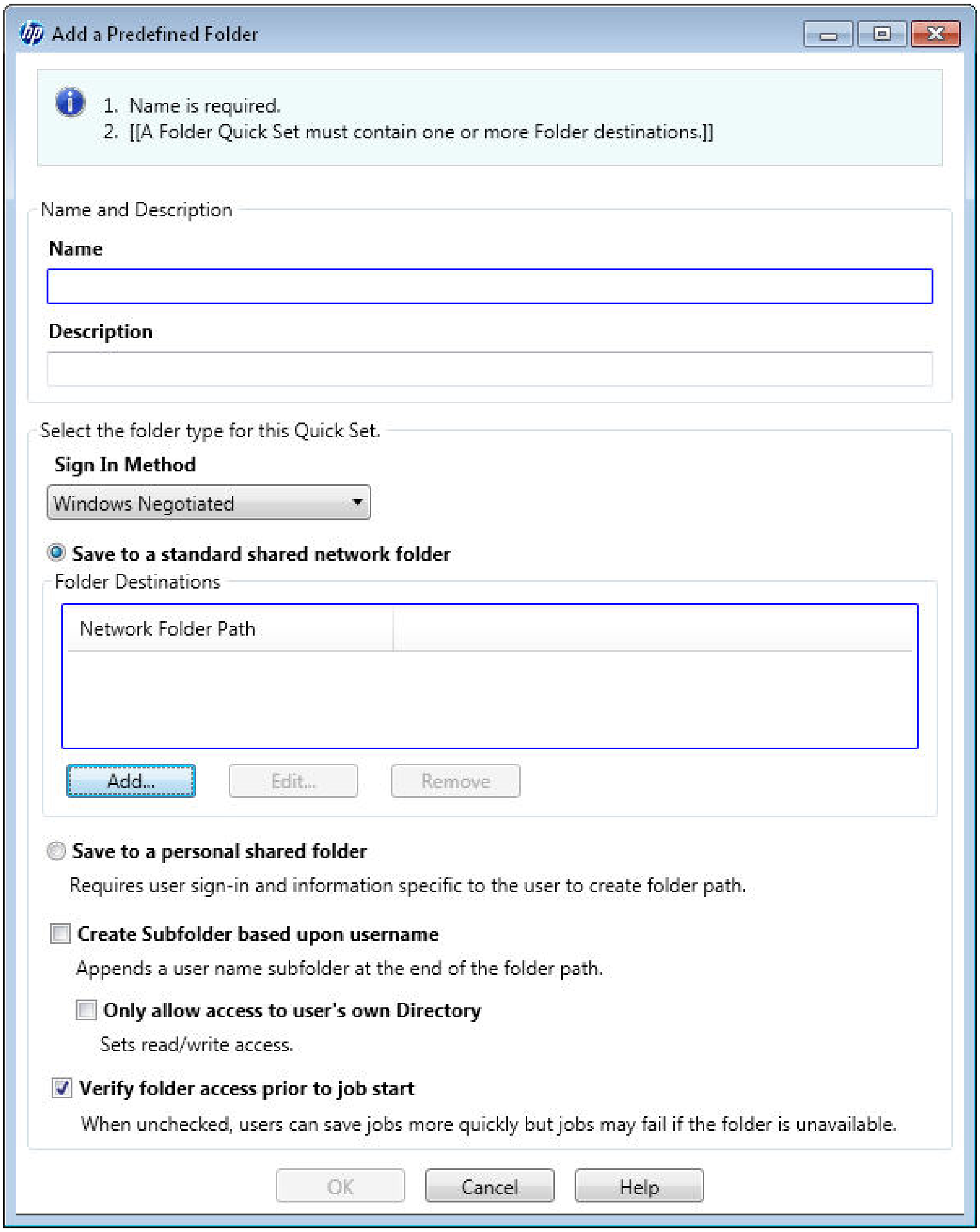
To configure the Send to Folder feature

1. On the DSS server, open the Configuration Utility, and then click the **Send to Folder** tab.
2. Select the **Enable Send to Folder** check box.
3. Click **Add…** to add a new folder. The **Predefined Folder** dialog box appears.
4. Type a name and description for the folder into the **Name** and **Description** text boxes. The name and description appear on the device control-panel interface.
5. Click to select one of the following folder types:

NOTE: Supported operating systems for folder destinations are CIFS/SMB-compliant file systems.

- **Save to a standard shared network folder..**

Figure 3-37 Add a Predefined Folder screen



Add a Predefined Folder

1. Name is required.
2. [[A Folder Quick Set must contain one or more Folder destinations.]]

Name and Description

Name

Description

Select the folder type for this Quick Set.

Sign In Method

Windows Negotiated

● **Save to a standard shared network folder**

Folder Destinations

Network Folder Path

○ **Save to a personal shared folder**

Requires user sign-in and information specific to the user to create folder path.

□ **Create Subfolder based upon username**

Appends a user name subfolder at the end of the folder path.

□ **Only allow access to user's own Directory**

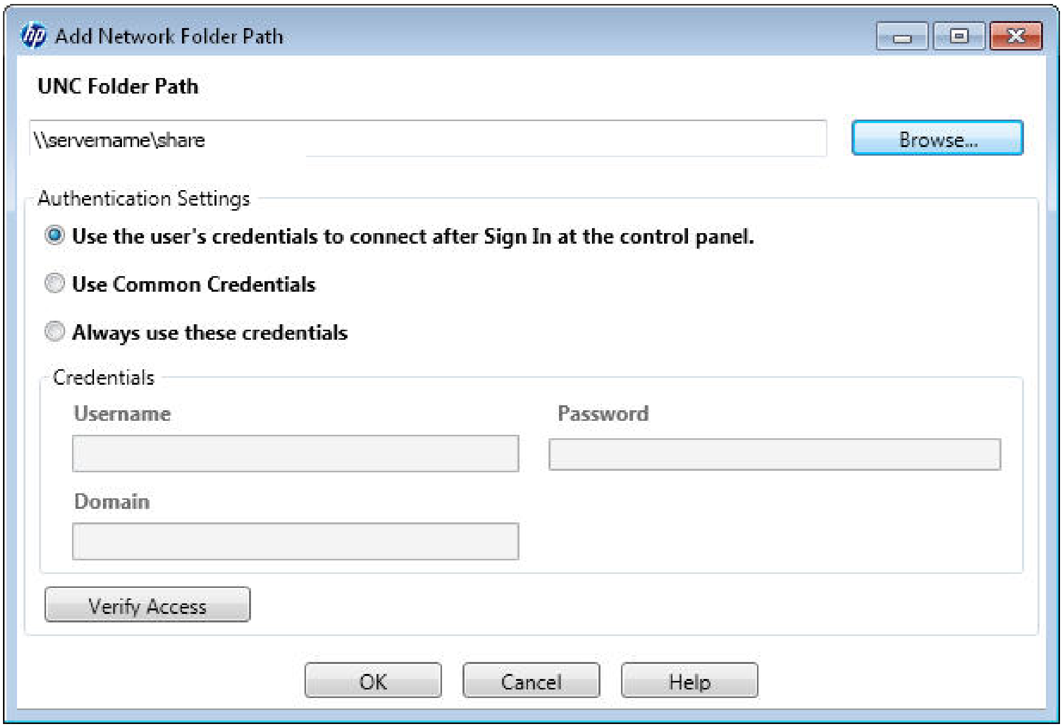
Sets read/write access.

☑ **Verify folder access prior to job start**

When unchecked, users can save jobs more quickly but jobs may fail if the folder is unavailable.

1. Click the **Add** button to open the **Add Network Folder Path** screen.

Figure 3-38 Add Network Folder Path screen



Add Network Folder Path

UNC Folder Path

\\servername\share

Authentication Settings

● Use the user's credentials to connect after Sign In at the control panel.

○ Use Common Credentials

○ Always use these credentials

Credentials

Username:

Password:

Domain:

2. Click the **Browse** button to select a folder path.

3. Select the credentials that should be used to gain access to the folder in the **Authentication Settings** section. Click to select **Use credentials of user to connect after Sign-in at the control panel** to use the credentials of the user when logged into the device. Or click to select **Use common credentials** to use the credentials designated in the **Credentials to Access Public Folders** section on the **Send to Folder** tab. Click **Verify Access** to test authentication.

4. Click the **OK** button to save the settings. The new folder(s) is added to the **Folder Destinations** list.

- **Save to a personal shared folder.** This feature will save to a folder path that is stored in an LDAP attribute. The LDAP attribute is associated with the user name of a signed-in user, so this feature can only be used when user sign-in is enabled. Type in the name of the LDAP attribute in which to find the UNC path to the user's folder.

- **Create subfolder based upon user name.** This feature customizes the path in which data is stored by appending the signed-in user's name to the provided UNC path for the final destination path. User sign-is required for send to folder for this feature to be used. If the **Only allow access to user's own Directory** checkbox is not checked then the destination folder will inherit the permissions of its parent. If the **Only allow access to user's own Directory** is checked then DSS will modify the folder permissions so that only the user and administrators will have access.

6. Click the **Verify folder access prior to job start** check box to ensure the target folder is accessible before each job.

7. Click **OK** to save the settings. The new folder is added to the **Predefined Folders** list.

8. Repeat steps 1 through 7 to add more folders.

9. Click the **OK** button to save the folder settings.

Configure the Device

In the Configuration Utility, use the **Send to Folder** subtab on the **Device Configuration** tab set to set up the Send to Folder feature on the device.

Configure the device to use Send To Folder

1. Click to select the **Enable Send to Folder** check box on the **Send To Folder** subtab on the **Configure Devices** tab set.

2. To enable options for OCR processing the scanned documents, select an OCR file type from the Default File Type drop-down menu.

3. For pre-FutureSmart devices managed by DSS, send to folder jobs always flow through DSS. For FutureSmart devices, the jobs can be configured to flow through DSS or to be sent directly from the device.

Send to E-mail

This section contains the following topics:

- Configuration overview
- Configure DSS
- Configure the Device

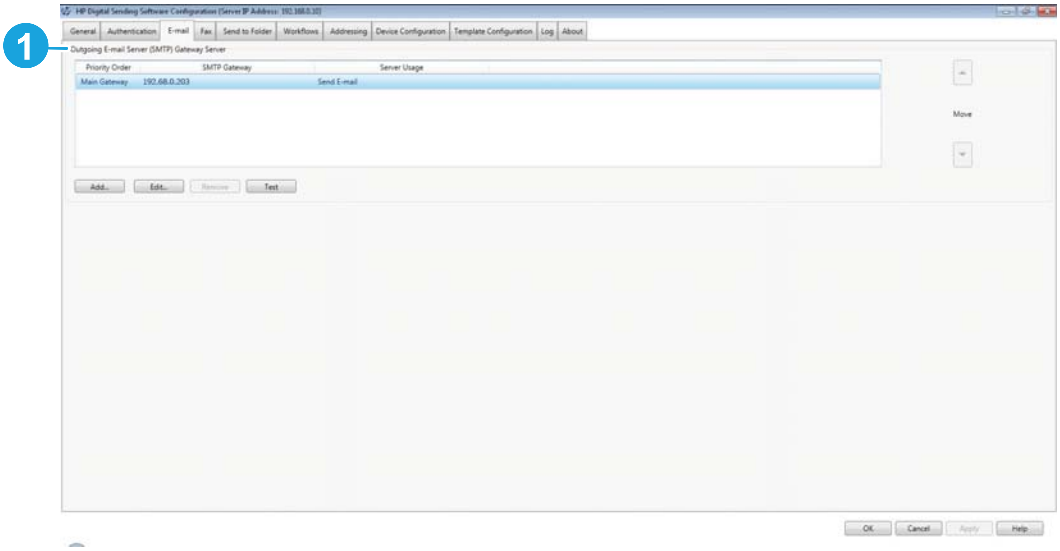
Configuration overview

The Digital Sending features of the device can send scanned documents directly to e-mail, transforming paper-based information into digital images that can be shared, stored, or edited. This saves the device user from having to first create and save an electronic copy of a hard-copy document, and then send it via their mail application. This can now all be done in one step at the device.

Configure DSS

Use the **E-mail** tab of the Configuration Utility to configure and organize the SMTP e-mail servers that DSS uses to send e-mail messages.

Figure 3-39 **E-mail** tab



Priority Order	SMTP Gateway	Server Usage
Main Gateway	192.68.0.203	Send E-mail

The **E-mail** tab contains the following elements.

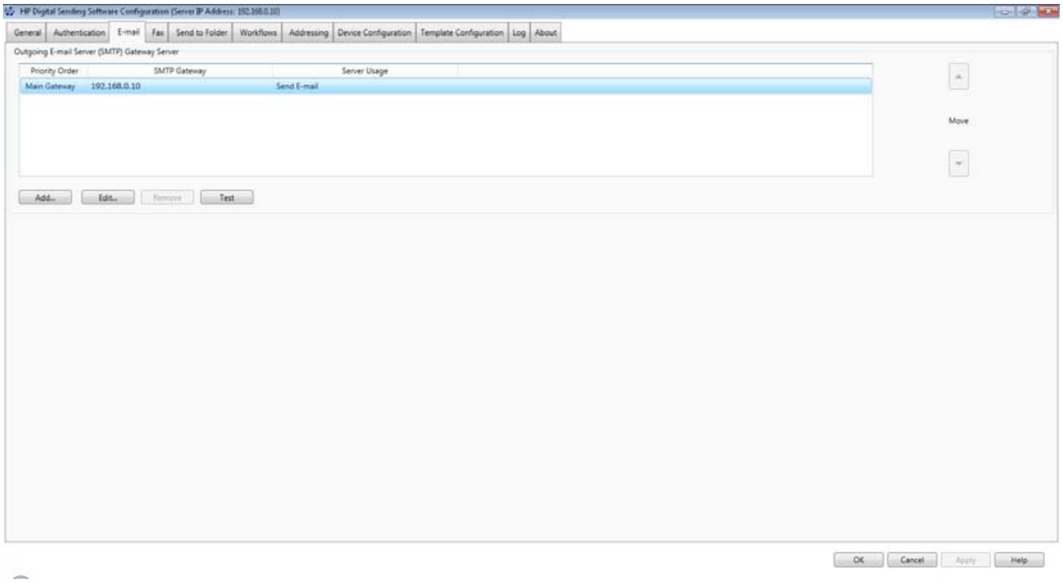
Table 3-15 **E-mail tab**

Callout	Component	Description
1	**Outgoing E-mail Server (SMTP) Gateway Server**	Use the **Outgoing E-mail Server (SMTP) Gateway Server** to manage e-mail servers for the DSS server. The e-mail servers are listed here by priority. Use the up and down arrows to move e-mail servers up or down in the list. The following controls are available for configuring the e-mail servers. ● **Add**. Click to add a new e-mail server. ● **Edit**. Click to edit the settings for an e-mail server. ● **Remove**. Click to remove an e-mail server from the list. ● **Test**. Click to test an e-mail server.

Configure the e-mail feature on DSS

1. On the DSS server, open the Configuration Utility, and then click the **E-mail** tab.

Figure 3-40 The **E-mail** tab



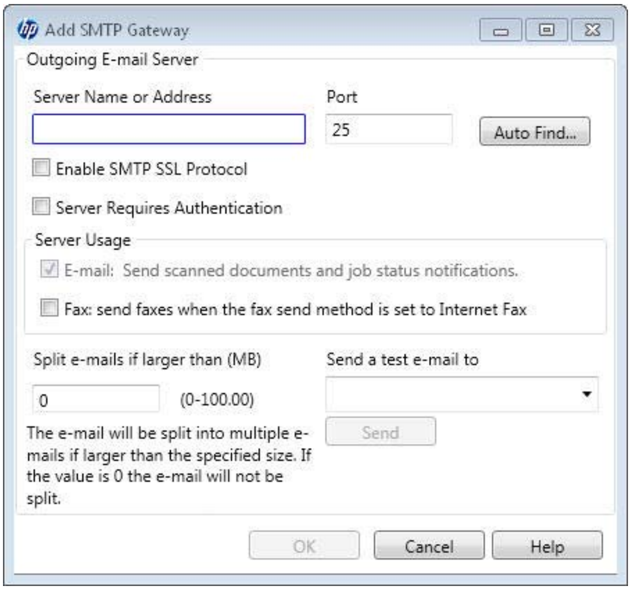
HP Digital Sending Software Configuration (Server IP Address: 192.168.0.10)

Outgoing E-mail Server (SMTP) Gateway Server

Priority Order	SMTP Gateway	Server Usage
Main Gateway	192.168.0.10	Send E-mail

2. Click **Add**. The **Add SMTP Gateway** dialog box appears.

   Figure 3-41 Add SMTP Gateway dialog box



Add SMTP Gateway

Outgoing E-mail Server

Server Name or Address:

Port: 25

□ Enable SMTP SSL Protocol

□ Server Requires Authentication

Server Usage

☑ E-mail: Send scanned documents and job status notifications.

□ Fax: send faxes when the fax send method is set to Internet Fax

Split e-mails if larger than (MB): 0 (0-100.00)

The e-mail will be split into multiple e-mails if larger than the specified size. If the value is 0 the e-mail will not be split.

Send a test e-mail to:

3. Type the host name or TCP/IP address of the SMTP server in the **Server Name or Address** field.

   -or-

   Or click **Auto Find** to find all of the SMTP servers on the network. A list of SMTP servers appears. Select one or more SMTP servers and click **OK**.

4. Select any of the following additional SMTP gateway options:

   - **Enable SMTP SSL Protocol**
   - **Server Requires Authentication**
   - **E-mail: Send scanned documents and job status notifications.**

- **Fax: send faxes when the fax send method is set to Internet Fax.** Since the Send to Fax feature also uses an e-mail interface, checking this box indicates the SMTP server being configured can be used for both Send to e-mail and Send to Fax.

- **Split e-mails if larger than (MB).** Use this control to set a maximum file size for the specified SMTP gateway. If an e-mail attachment exceeds the specified file size, the attachment is divided into two or more smaller attachments.

- **Send a test e-mail to.** Type an e-mail address, and then click **Send** to verify the presence of the SMTP gateway.

NOTE: If the test fails, double-check the gateway address, and then contact the network administrator to see if the SMTP server is functioning.

5. Click **OK** to add the server to the SMTP Gateway Server list.

6. If there is more than one SMTP server, use the **Move** arrow buttons to move SMTP servers to a different position on the list. DSS attempts to use the first SMTP server when processing an e-mail transmission. If the first server is unavailable for use, DSS attempts to use the next server on the list. DSS continues this process until it finds an available SMTP server.

Configure the Device

1. On the DSS server, open the Configuration Utility, and then select a device from the list on the **Device Configuration** tab.

2. Click the **Configure Device...** button, and then select the **Send to E-mail** tab.

3. Select the **Enable Send to E-mail** check box.

4. In the **Send E-mail** drop-down menu box, select **via the Digital Sending Service** if you want e-mail jobs routed via DSS, or select **Directly from the device** if you want jobs to be sent from the device.

5. Configure the rest of the settings as needed.

Send to Fax

This section contains the following topics:

- Configuration overview
- Configure DSS
- Configure the Device

Configuration overview

This section contains the following topics:

- Analog fax
- Digital fax

Analog fax

DSS can be used to configure the settings for the embedded analog fax modem in a device. Use the **Send to Fax** tab in the Device Configuration interface to configure these settings on individual devices.

Digital fax

Digital Fax is the name for a process where the original file is scanned and digitized before it is sent to its destination via a fax modem. In the DSS digital fax process the original files are scanned on the device, sent to DSS, and then routed via DSS to a third party software application. The third party software application processes the digital file and manages the sending of the file over a fax modem. DSS does not fax the scanned image, it just routes the image to the third party software.

There are two types of digital fax: LAN Fax and Internet Fax. They are differentiated by the method DSS uses to interact with the fax software. For LAN Fax, DSS delivers the scanned image to the fax software using a shared folder interface. With Internet Fax, DSS delivers the scanned image via an e-mail interface. For all digital fax jobs, DSS delivers a metadata file with the scanned image file. The metadata file contains information the fax software needs to send the fax including things like destination phone number, modem speed to use, etc.

Configure DSS

The Configuration Utility **Fax** tab controls all of the DSS fax settings. To configure the fax option, first select the fax delivery method from the **Fax Send Method** drop-down list. The following options are available:

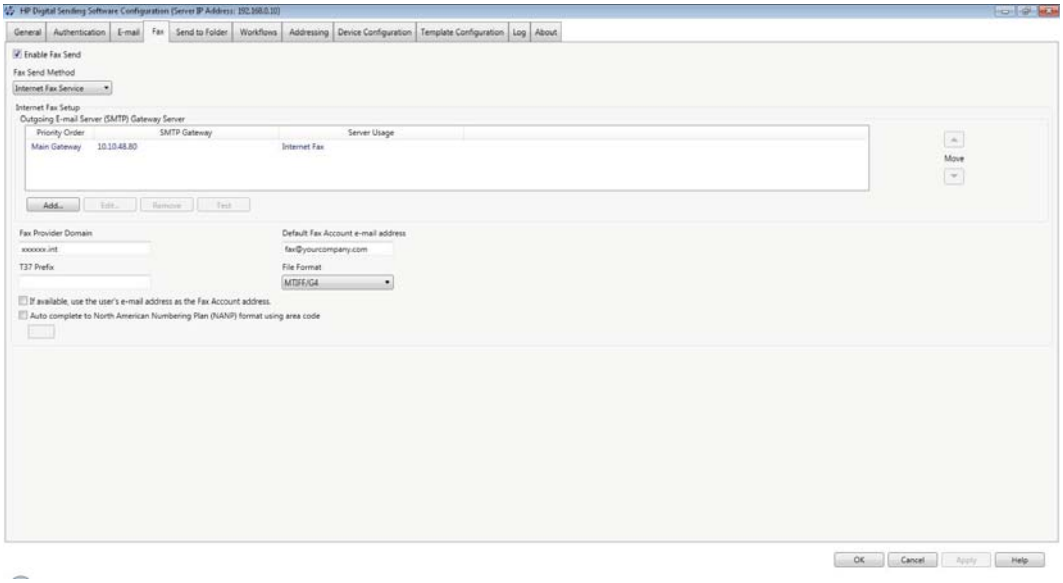
- None
- LAN Fax
- Internet Fax

Depending on which method is selected, the applicable settings appear on the **Fax** tab. Fill in these settings to complete the fax configuration process.

Internet fax

DSS uses an e-mail interface to communicate with a third party internet fax vendor.

Figure 3-42 **Fax** tab – Internet fax option



☑ Enable Fax Send

Fax Send Method: Internet Fax Service

Internet Fax Setup

Outgoing E-mail Server (SMTP) Gateway Server

Priority Order	SMTP Gateway	Server Usage
Main Gateway	10.10.48.80	Internet Fax

Fax Provider Domain: xxxxxx.int

Default Fax Account e-mail address: fax@yourcompany.com

T37 Prefix:

File Format: MTIFF/G4

□ If available, use the user's e-mail address as the Fax Account address.

□ Auto complete to North American Numbering Plan (NANP) format using area code

To configure Internet fax

With an Internet fax service, faxes are sent in e-mail. When using DSS, the user specifies a fax number at the device, and then the software creates and sends the e-mail behind the scenes.

1. On the DSS server, open the Configuration Utility and click the **Fax** tab.

2. Select **Internet Fax** from the **Fax Send Method** drop-down list.

3. Set up the **Outgoing E-mail Server (SMTP) Gateway Server**. Click the **Add...** button to open the **Add SMTP Gateway dialog** and add the outgoing e-mail server address manually or click the **Auto Find...** button to search for servers.

   If, when configuring an SMTP server for send to e-mail, the checkbox labeled **Fax: send faxes when the fax send method is set to Internet Fax** was checked, then those SMTP servers will already be shown in the list of servers available for use with Internet Fax.

4. Type the domain name for the Internet fax provider into the **Fax Provider Domain** text box (for example, efax.com). DSS takes the phone number that is typed at the device and then uses this domain name to create the e-mail (for example, [phone number]@efax.com).

5. Type a valid e-mail address into the **Default Fax Account E-mail Address** text box. The Fax Account E-mail Address is used by third party fax service for billing purposes or as a return address for notifications. This address is used if the check box labeled **If available, use the user's e-mail address as the Fax Account Address** is not checked, or if user sign-in is not enabled for fax. The Fax Account E-mail address is used as the "from:" address in the e-mail sent to the fax software.

6. Enter the T37 prefix. The T37 prefix is an optional data item that may be required by some third party fax software applications.

7. Select the default **File Format** from the drop-down menu.

8. Select the check box to use the authenticated user's e-mail address as the return e-mail address. If the device user's e-mail address is not available, the **Default Fax Account E-mail Address** e-mail address is used.

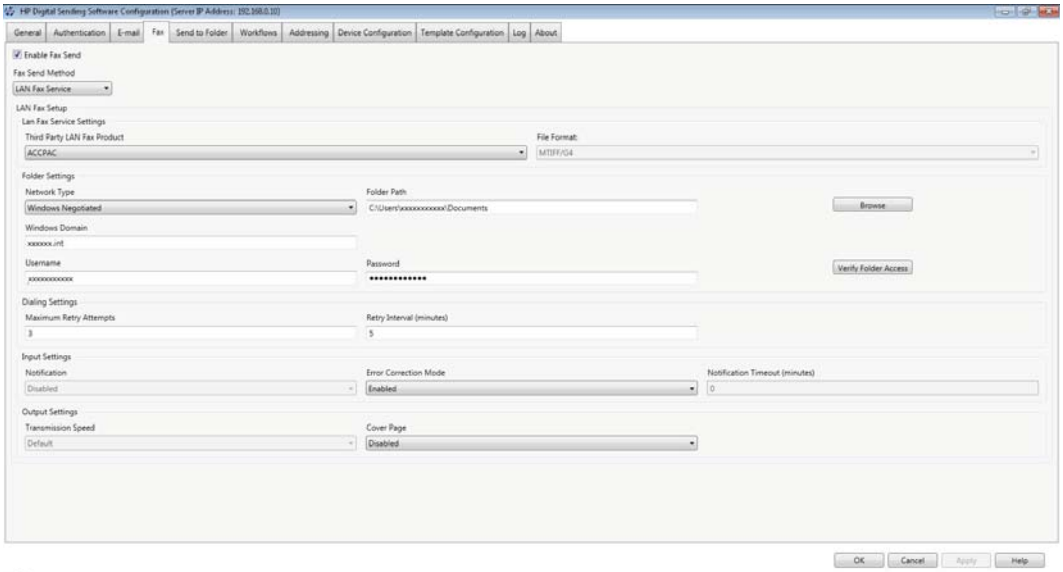
> NOTE: If you select this option, the user's e-mail address must be registered with the Internet fax service provider in order to fax successfully.

9. Click **Apply** to save the Internet fax settings.

LAN fax

DSS uses a shared folder interface to communicate with a third party LAN Fax vendor.

Figure 3-43 **Fax** tab – LAN fax option



☑ Enable Fax Send

Fax Send Method: LAN Fax Service

LAN Fax Setup

Lan Fax Service Settings

Third Party LAN Fax Product: ACCPAC

File Format: MTIFF/G4

Folder Settings

Network Type: Windows Negotiated

Folder Path: C:\Users\xxxxxxxxxxx\Documents

Windows Domain: xxxxxx.int

Username: xxxxxxxxxxx

Password: ••••••••••••

Dialing Settings

Maximum Retry Attempts: 3

Retry Interval (minutes): 5

Input Settings

Notification: Disabled

Error Correction Mode: Enabled

Notification Timeout (minutes): 0

Output Settings

Transmission Speed: Default

Cover Page: Disabled

To configure LAN fax

Follow these instructions to set up faxing from the device by using the network LAN fax service.

1. On the DSS server, open the Configuration Utility and click the **Fax** tab.

2. Select **LAN fax** from the **Fax Send Method** drop-down list.

3. Select the LAN fax software product name from the **Third Party LAN Fax Product** drop-down menu.

> NOTE: If you are unsure about whether the product supports notification, select the **Generic LAN fax product without notification support** option from the drop-down menu.

4. Select the **Network Type** from the drop-down menu.

5. Type in the network path in the **Folder Path**, or click **Browse** to select the network folder that the fax software uses.

6. Enter the Windows credentials of domain, user name, and password that DSS will use for access rights to the shared folder. Click **Verify Folder Access** to test the credentials and verify access to the folder.

7. Complete the **Dialing Settings** section by typing in the values you want to use in the **Maximum Retry Attempts** and **Retry Interval (minutes)** text boxes.

8. Complete the **Input Settings** section by selecting the values you want to use in the **Notification** and **Error Correction Mode** drop-down menus. Type in the value you want to use in the **Notification Timeout (minutes)** text box.

9. Complete the **Output Settings** section by selecting the values you want to use in the **Transmission Speed** and **Cover Page** drop-down menus.

10. Click **Apply** to save the LAN fax settings.

Configure the Device

Use the **Fax** tab to configure the send-to-fax features for the selected device. Depending on the device type and hardware configuration, some of these options might not be available.

To configure the fax option, first select the fax delivery method from the **Fax Send Method** drop-down list. A device can only be configured to use a single fax delivery method at any one time. The following options are available:

- Internet Fax Service: When this is selected, configuration is done for the device firmware's ability to send digital fax to internet fax vendors. DSS is not involved.
- Lan Fax Service: When this is selected, configuration is done for the device firmware's ability to send digital fax to LAN fax vendors. DSS is not involved.
- Internal Modem: When this is selected, the device is configured to send fax via its internal modem. DSS is not involved.
- via the Digital Send Service: When this is selected, the device is configured to send faxes via DSS. This will be either Internet Fax or LAN fax depending on how the DSS service is configured.

Once the **Enable Fax Send** check box has been checked and the **Fax Send Method** is set to **via the Digital Sending Service**, configure other settings on the tab as appropriate for your environment.

Send to Workflows

This section contains the following topics:

- Configuration overview
- Configure DSS
- Configure the Device

Configuration overview

Workflows give device users the ability to send additional information along with the scanned document to a specified location. The additional information is in a file called a metadata file. Metadata files can be configured by DSS administrators and contain a collection of data items referred to as prompts. Prompts can be either system generated information or information provided by the end user after being prompted for input at the control panel when using the workflow.

Third party applications, or in-house applications developed by customers, can be used to monitor for new scanned image files being delivered to a destination and can subsequently use the metadata files to decide how to further process the scanned image file.

The available destinations for workflow are:

- Folders
- FTP sites
- SharePoint®
- Printers

Metadata files are not created and printed for send to printer workflows. Some reasons to use send to printer are:

- When printing a file scanned at a scanner only device
- When printing a file to a color printer that was scanned at a device with a color scanner but only a mono printer

Workflow organizational structures

Workflows are arranged in an hierarchical fashion. The top-most level is Groups. The default group is called the Common Device Group and cannot be deleted. Devices are configured to show only one Workflow group. If multiple groups are configured, a device will only show a subset of all the workflows. This can be used to manage large numbers of workflows so users at a device do not have to navigate through them all to find the one they want. For example, if you wanted the device in the marketing department to present only marketing specific workflows, you might create a Marketing Workflow Group that contained a subset of the workflows (the marketing specific ones). You would then configure the marketing department's device to use the Marketing Workflow Group (see the Send to Workflow settings in Device Configuration). All your other devices would then be configured to use the Common Device Group.

The next Workflow level is Menus. Menus are the first level that is viewable at the device's control panel. Typically, Menus are used to categorize workflows. Within a Menu, you can create another Menu (up to 30 levels deep) or forms

Forms are workflows. Each form contains information about the workflow destination and file settings for the scanned file image. Also included in each form is the definition of the metadata file associated with that workflow, including the metadata file format and which prompts are included.

Configure DSS

The Configuration Utility **Workflows** tab can also be used to view workflow entries or to set up workflow processes.

Figure 3-44 The **Workflows** tab

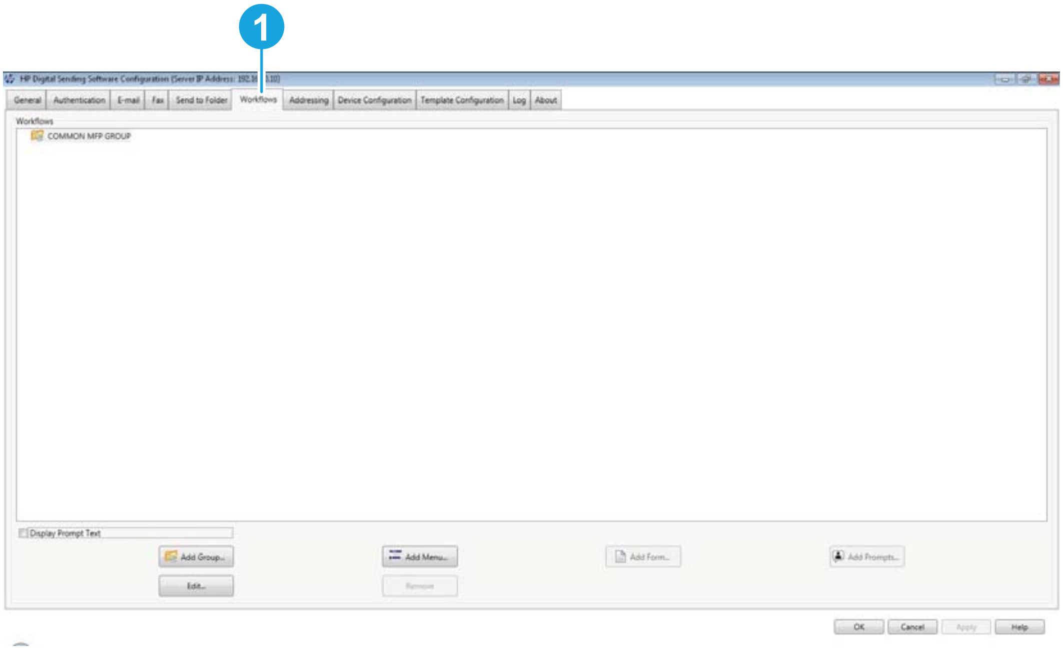


Table 3-16 Workflows tab

Callout	Component	Description
1	**Workflows**	This list shows the workflows that are set up and available for use to any of the devices connected to the DSS server. Click to select the **Display Prompt Text** check box to show the prompt text for each workflow in the list. The following controls are available to help configure workflows. • **Add Group**. Click to add a group to a workflow. • **Add Menu**. Click to add a menu to a workflow. • **Add Form**. Click to add a form to a workflow. • **Add Prompts**. Click to add prompts to a workflow. • **Edit**. Click to change workflow settings. • **Remove**. Click to remove a workflow from the list.

Configure the menu structure (groups, menus, and forms)

The workflow configuration process comprises three steps:

- Creating the workflow group, which defines which workflow menus and forms are available on the device control panel.
- Creating the workflow menu, which creates logical groups of workflow forms.
- Creating the workflow form, which accumulates information that the user specifies at the control panel before initiating a send-to-workflow job.

Groups

The first step in creating a workflow process is to create a workflow group.

NOTE: Rather than creating a new group, the default group, called the **Common Device Group** can also be used. This group cannot be deleted. Custom groups are optional and provide a way to associate different workflows with different devices or groups of devices.

1. On the DSS server, open the Configuration Utility and click the **Workflows** tab.

2. Click **Add Group**. The **Workflow Group** dialog box appears.

3. Type the name of the new group. The name must be unique.

4. Click to select either the **This group does not contain the devices mentioned below** option or the **This group contains workflows that will be used on LJ9065, LJ90** option.

5. Click **OK** to save the new group.

Menus

The second step in creating a workflow process is to create a workflow menu.

1. In the workflow tree, click a group to select it.

2. Click **Add Menu**. The **Workflow Menu** dialog box appears.

3. Type the name of the new menu. This name must be unique within the workflow group.

4. Click **OK** to save the new workflow menu.

Forms

The final step in creating a workflow process is to create a workflow form. Forms are destination-specific. Four destination types are available:

- Folder

- FTP site

- Printer

- SharePoint

The following sections describe how to create a workflow form for each of these destination types.

Configuring metadata files

Metadata files are configured within the forms for folder, FTP, and SharePoint® destinations. Each form has its own metadata file, but all the metadata files share the same configuration user interface. This section will describe the metadata configuration sub-section of form configuration.

1. From the **Meta Data File Settings** section of a workflow form, select the file type for the metadata file from the **File Format** drop-down menu. The options are **None**, **HPS**, **XML**, or **FNA**. The metadata file contains the data that is collected by the workflow prompts. If no prompts are being created, select **None**.

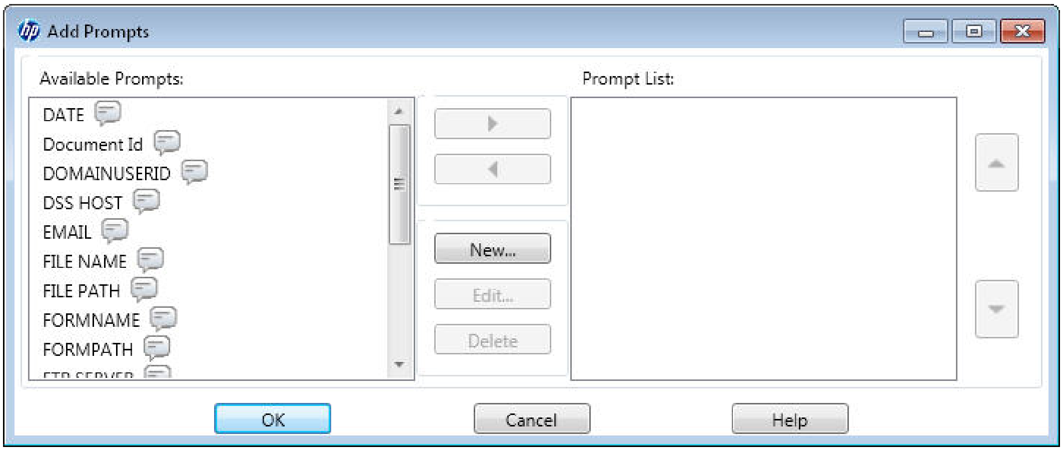
2. In the **Prompts** area, define any appropriate prompts and expected responses for the user of the workflow form. The prompts appear on the device control panel. The responses to the prompts

are saved in the metadata file, which is stored with the document image for use by the third-party workflow software program.

Follow these instructions to add prompts.

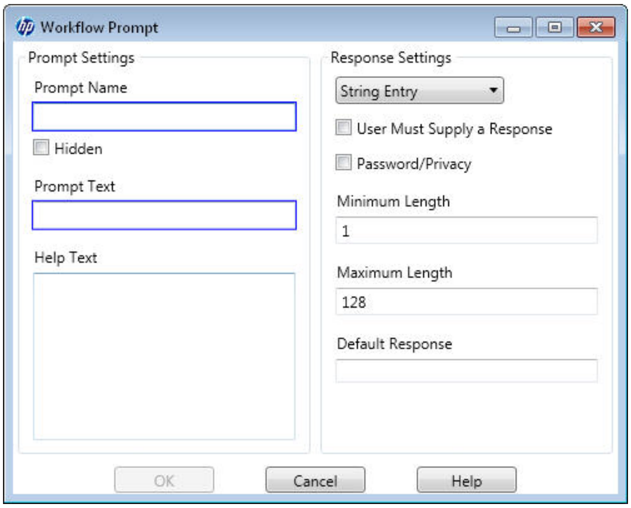
a. Click **Add**. The **Add Prompts** dialog box appears.

Figure 3-45 **Add Prompts** dialog box



b. Prompts that are already available are listed on the left hand side of the dialog. To create new prompts, click the **New...** button. This opens the Workflow Prompt dialog box.

Figure 3-46 **Workflow Prompt** dialog box



String Entry

Minimum Length
1

Maximum Length
128

i. Under **Prompt Settings** in the **Workflow Prompt** dialog box, type the **Prompt Name**. This name is used internally and is not visible to the user. It must be unique within the workflow form.

ii. Select the **Hidden** check box if the prompt is not to be shown to the user. Hidden prompts are typically used to send specific unaltered information to the third-party programs in the metadata file. When the **Hidden** check box is selected, a **Prompt Information** text box appears. Type the information for the hidden prompt in the **Prompt Information** text box.

iii. In the **Prompt Text** text box, type the text that you want to appear on the device control panel.

iv. In the **Help Text** text box, type the help text for the prompt. The help text appears if the user touches HELP on the device control panel while the prompt is on the screen.

v. Select a setting from the **Response Settings** drop-down menu. The following table provides a description of each option.

Table 3-17 Response format options

Format	Attributes
String Entry	● The user can type any alphanumeric string. ● Minimum length: 1 ● Maximum length: 127
Number Entry	● The user is limited to typing numbers only. ● Decimal places range from 0 to 15 ● Minimum Value: 0 ● Maximum Value: 4294967295
Selection List	● The user can select from a list of options.
Date	● The user is limited to typing a date value in the form of HH/DD/YYYY. The date format cannot be changed.
Time	● The user is limited to typing a time value in the form of HH:MM:SS using the 24-hour clock. The time format cannot be changed.

vi. Click to select the **User must supply a response** check box to require a response to the prompt.

vii. Click to select the **Password Privacy** check box to have passwords displayed as asterisks.

viii. As appropriate, type a default response in the **Default Response** text box. The program uses the default response if the user does not provide a response to the prompt. Specify the **Minimum Length** and **Maximum Length** by typing values in the text boxes.

ix. Click **OK** to save the prompt settings. The new prompt is added to the **Prompts List** in the **Add Prompts** dialog box.

x. Repeat steps as needed to create more prompts.

c. After creating the new prompts, move any of the available prompts you want in this metadata file by selecting the prompt and then clicking the right arrow to move it to the **Prompt List.** You can change the order the prompt data will appear in the file by using the up and down arrows to the right of the prompt list.

d. Click **OK** to accept the new set of prompts. The new prompts appear in the **Prompts** area of the **Workflow Form** dialog box.

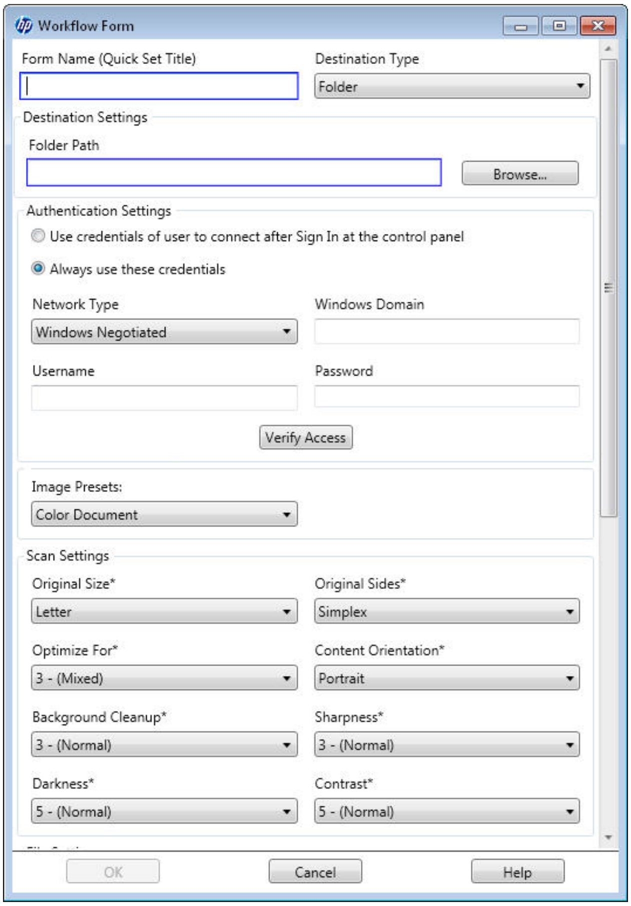
Folder

To create a workflow form for a folder destination

1. Click a workflow menu to select it.

2. Click **Add Form**. The **Workflow Form** dialog box appears.

Figure 3-47 **Workflow Form** dialog box



Form Name (Quick Set Title)

Destination Type: Folder

Destination Settings

Folder Path

Authentication Settings

○ Use credentials of user to connect after Sign In at the control panel

● Always use these credentials

Network Type: Windows Negotiated

Windows Domain

Username

Password

Image Presets: Color Document

Scan Settings

Original Size*: Letter

Original Sides*: Simplex

Optimize For*: 3 - (Mixed)

Content Orientation*: Portrait

Background Cleanup*: 3 - (Normal)

Sharpness*: 3 - (Normal)

Darkness*: 5 - (Normal)

Contrast*: 5 - (Normal)

3. In the **Form Name** text box, type a name for the new form. The name must be unique within the workflow menu.

4. Select **Folder** from the **Destination Type** drop-down list.

NOTE: Based on the option selected, the options on the **Workflow Form** dialog box change. This procedure applies to the **Folder** option. See the following sections for instructions for creating a workflow form for an FTP site or a printer.

5. In the **Authentication Settings** section, click to select the **Use credentials of user to connect after Sign In at the control panel** option to have DSS use the credentials of the user that is logged into the device. Or click to select the **Always use these credentials** option.

6. Select the **Network Type** from the drop-down menu. Type the path for the destination folder in the **Folder Path** text box, or browse to select a path. Type in the **Windows Domain**, **Username**, and **Password**. Click **Verify Access** to test the credentials.

7. Select a setting from the **Image Presets** drop-down menu, if needed.

8. Under **Scan Settings** and **File Settings**, select the settings for the scanned file. These should be the settings that the third-party software program that processes the file requires.

9. Configure the metadata settings. See Configuring metadata files on page 81.

10. Click **OK** to accept all of the settings on the **Workflow Form** dialog box. The new form appears in the workflows list on the **Workflows** tab.

NOTE: A workflow form can be edited at any time by selecting it, and then clicking **Edit**.

11. Click **Apply** to save the new workflow settings.

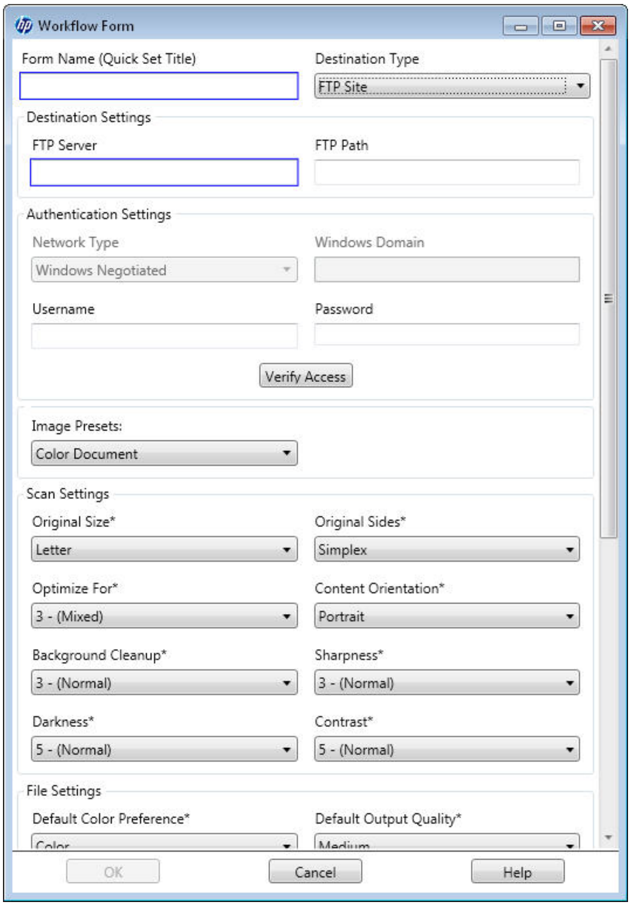
FTP site

The following instructions describe how to send a workflow document to an FTP site rather than a network folder.

1. Click a workflow menu to select it.

2. Click **Add Form**. The **Workflow Form** dialog box appears.

Figure 3-48 Workflow form for an FTP site



Workflow Form

Form Name (Quick Set Title):

Destination Type: FTP Site

Destination Settings

FTP Server:

FTP Path:

Authentication Settings

Network Type: Windows Negotiated

Windows Domain:

Username:

Password:

Image Presets: Color Document

Scan Settings

Original Size*: Letter

Original Sides*: Simplex

Optimize For*: 3 - (Mixed)

Content Orientation*: Portrait

Background Cleanup*: 3 - (Normal)

Sharpness*: 3 - (Normal)

Darkness*: 5 - (Normal)

Contrast*: 5 - (Normal)

File Settings

Default Color Preference*: Color

Default Output Quality*: Medium

3. In the **Form Name** text box, type a name for the new form. The name must be unique within the workflow menu.

4. Select **FTP Site** in the **Destination Type** drop-down menu.

5. In the **FTP Server** text box, type the host name or TCP/IP address of the FTP server.

6. In the **FTP Path** text box, type in the path to the directory on the FTP server that will hold the scanned documents.

7. In the **Authentication Settings** section, type in the username and password that are required for the FTP server.

8. Select a setting from the **Image Presets** drop-down menu, if needed.

9. Under **Scan Settings** and **File Settings**, select the settings for the scanned file. These should be the settings that the third-party software program that processes the file requires.

10. Configure the metadata settings. See Configuring metadata files on page 81.

11. Click **OK** to accept all of the settings on the **Workflow Form** dialog box. The new form appears in the workflows list on the **Workflows** tab.

NOTE: A workflow form can be edited at any time by selecting it and then clicking **Edit**.

12. Click **Apply** to save the new workflow settings.

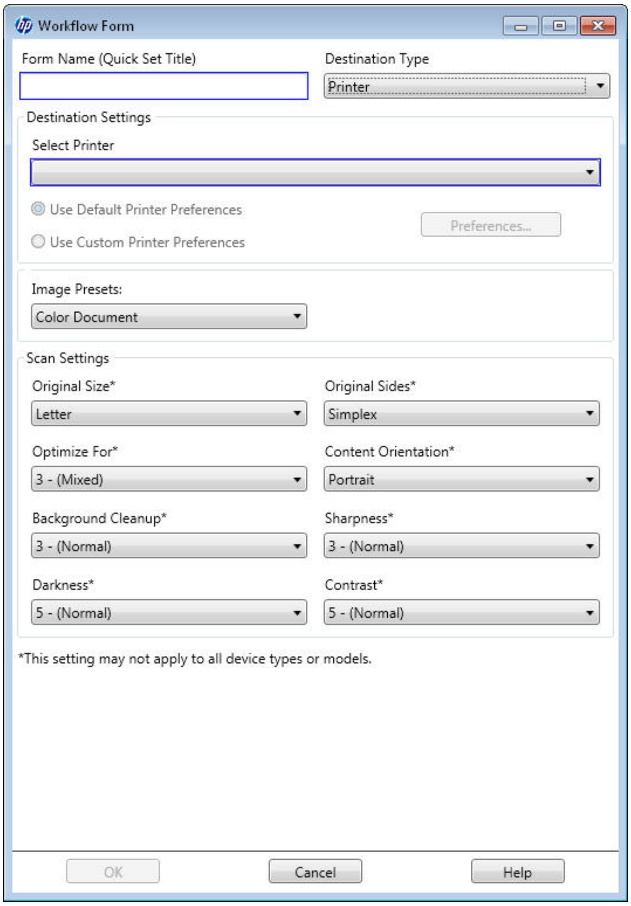
Printer

The following instructions describe how a workflow form can also be used to send a scanned document to a network printer to be printed.

1. Click a workflow menu to select it.

2. Click **Add Form**. The **Workflow Form** dialog box appears.

Figure 3-49 Workflow form for a printer



Workflow Form

Form Name (Quick Set Title):

Destination Type: Printer

Destination Settings

Select Printer:

○ Use Default Printer Preferences

○ Use Custom Printer Preferences

Image Presets: Color Document

Scan Settings

Original Size*: Letter

Original Sides*: Simplex

Optimize For*: 3 - (Mixed)

Content Orientation*: Portrait

Background Cleanup*: 3 - (Normal)

Sharpness*: 3 - (Normal)

Darkness*: 5 - (Normal)

Contrast*: 5 - (Normal)

*This setting may not apply to all device types or models.

3. In the **Form Name** text box, type a name for the new form. The name must be unique within the workflow menu.

4. Select **Printer** in the **Destination Type** drop-down menu.

5. In the **Select Printer** drop-down menu, select a printer from the list of available network printers. DSS can only print to printers that are installed and available on the DSS server as seen in the Windows control panel's printers section.

6. Select one of the option buttons to use the default or custom printer preferences. If custom printer preferences are selected, click **Preferences** to set them up.

   NOTE: The device user cannot change any of these print settings from the device control panel.

7. Select a setting from the **Image Presets** drop-down menu, if needed. Options include **Color Document** and **Photo**.

8. Under **Scan Settings**, select the settings for the scanned file. These should be the settings that the third-party software program that processes the file requires.

9. Click **OK** to save the workflow form.

10. Click **Apply** to save the settings on the **Workflow** tab.

NOTE: Metadata files are not available for printer destinations.

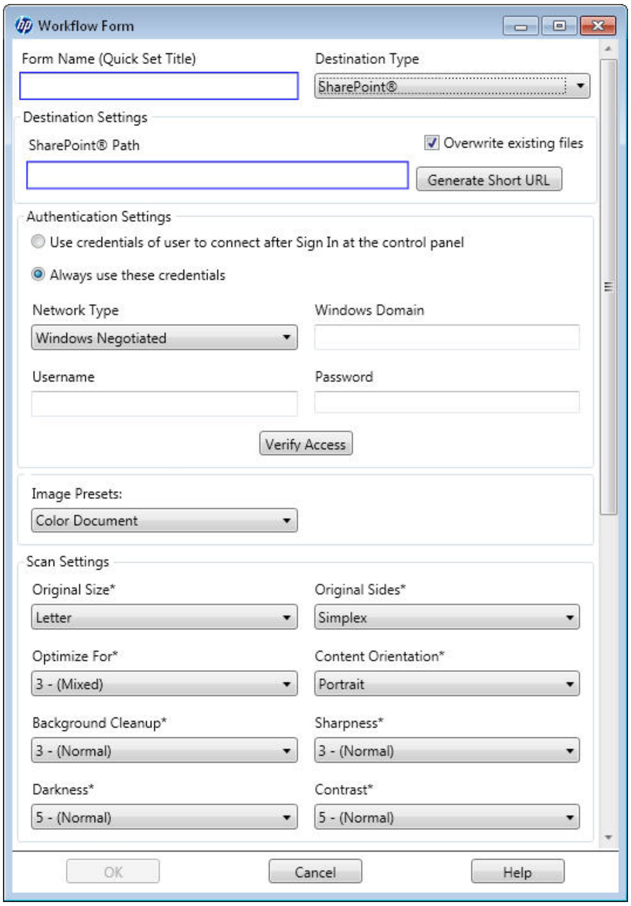
Sharepoint®

The following instructions describe how to send a workflow document to a Sharepoint® site rather than a network folder.

1. Click a workflow menu to select it.

2. Click **Add Form**. The **Workflow Form** dialog box appears.

Figure 3-50 **Workflow Form** dialog box



Workflow Form

Form Name (Quick Set Title):

Destination Type: SharePoint®

Destination Settings

SharePoint® Path:

☑ Overwrite existing files

Authentication Settings

○ Use credentials of user to connect after Sign In at the control panel

● Always use these credentials

Network Type: Windows Negotiated

Windows Domain:

Username:

Password:

Image Presets: Color Document

Scan Settings

Original Size*: Letter

Original Sides*: Simplex

Optimize For*: 3 - (Mixed)

Content Orientation*: Portrait

Background Cleanup*: 3 - (Normal)

Sharpness*: 3 - (Normal)

Darkness*: 5 - (Normal)

Contrast*: 5 - (Normal)

3. In the **Form Name** text box, type a name for the new form. The name must be unique within the workflow menu.

4. Select **Sharepoint®** in the **Destination Type** drop-down menu.

5. In the **Sharepoint® Path** field, type the URL path to the Sharepoint® server.

   It is typical to get a Sharepoint® destination path by navigating to the Sharepoint® location in a web browser, and then copying the path. When this is done, the path information is in the form of a URL that may contain some ASCII equivalents for characters instead of the characters themselves. A common example is to see "%20" instead of a space character. For example:

   ```
   http://sharepointname.company.com/folderlevel1%20name1/folderlevel2
   ```

   URL's must be converted to a form that has the characters in them, not their ASCII equivalents. Click the **Generate Short URL** button to perform this conversion. For the example above the URL will be converted to:

   ```
   http://sharepointname.company.com/folderlevel1 name1/folderlevel2
   ```

6. In the **Authentication Settings** section, type in the username and password that are required for the Sharepoint® server.

7. In the **Authentication Settings** section, click to select the **Use credentials of user to connect after Sign In at the control panel** option to have DSS use the credentials of the user that is logged into

the device. Or click to select the **Always use these credentials** option and then type in the **Windows Domain**, **Username**, and **Password**. Click **Verify Access** to test the credentials.

8. Select a setting from the **Image Presets** drop-down menu, if needed.

9. Under **Scan Settings** and **File Settings**, select the settings for the scanned file.

10. Configure the metadata settings. See Configuring metadata files on page 81.

11. Click **OK** to accept all of the settings on the **Workflow Form** dialog box. The new form appears in the workflows list on the **Workflows** tab.

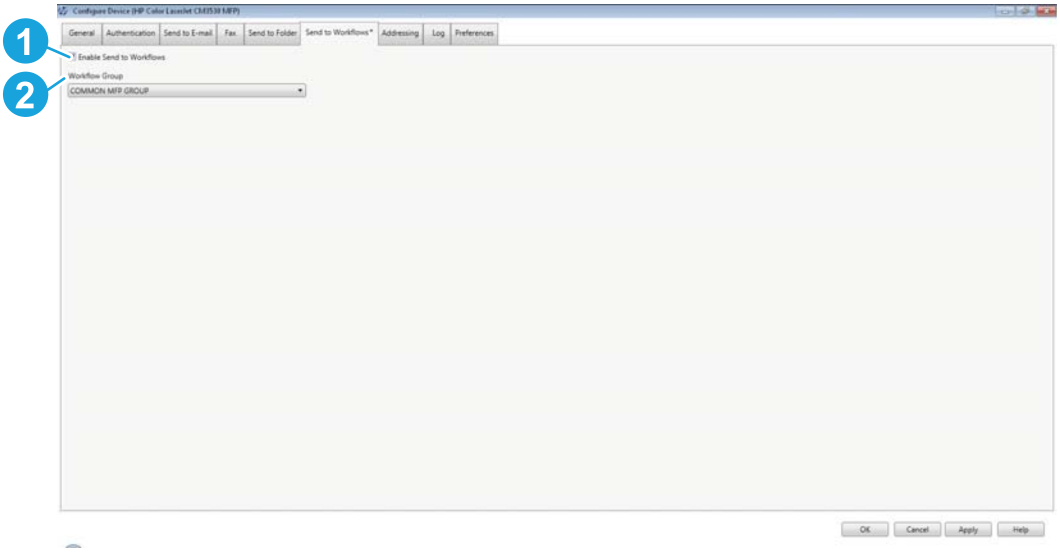
NOTE: A workflow form can be edited at any time by selecting it and then clicking **Edit**.

12. Click **Apply** to save the new workflow settings.

Configure the Device

The **Send to Workflows** subtab is shown in the following illustration.

Figure 3-51 **Send to Workflows** subtab in the Configure Devices tab set



Enable Send to Workflows

Workflow Group: COMMON MFP GROUP

Table 3-18 Send to Workflows subtab – Configure Devices tab set

Callout	Component	Description
1	Enable Send to Workflows	Click to select the **Enable Send to Workflows** check box.
2	Workflow Group	Select a workflow group from the drop-down menu.

Configure the device to use Send To Workflows

1. Click to select the **Enable Send to Workflows** check box on the **Send To Workflows** tab on the **Device Configuration** tab set.

2. Select a workflow from the **Workflow Group** drop-down menu.

3. Click **Apply**.

Addressing

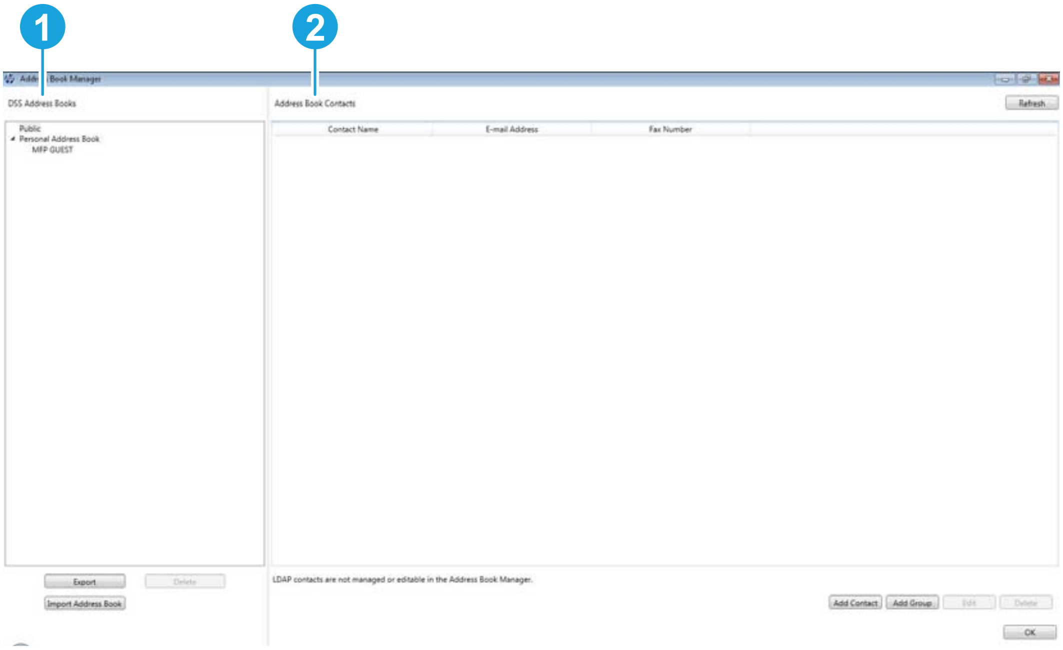
This section contains the following topics:

- Address Book Manager
- Personal address books
- Exchange contacts
- Guest address book
- Public address book
- LDAP replication
- LDAP filters
- Configure DSS for Windows Active Directory Services

Address Book Manager

Use the **Address Book Manager** on the **Addressing** tab to manage the address books for the DSS service.

Figure 3-52 Address Book Manager



LDAP contacts are not managed or editable in the Address Book Manager.

Table 3-19 Address Book Manager

Callout	Component	Description
1	**DSS Address Books**	The DSS Address Books list shows the address books available to the devices connected to the DSS server. Click an address book to see the address book contacts appear in the window to the right. Use the following controls to configure the address books ● **Export**. Click to export an address book. ● **Delete**. Click to delete an address book from the list. ● **Import Address Book**. Click to import an address book.
2	**Address Book Contacts**	The address book contacts appear in this part of the window. Use the following controls to manage contacts. ● **Refresh**. Click to update the contacts list. ● **Add Contact**. Click to add a contact. ● **Add Group**. Click to add a group. ● **Edit**. Click to edit a contact. ● **Delete**. Click to delete a contact. ● **Finish**. Click to close the Address Book Manager.

Importing addresses using the Address Book Manager

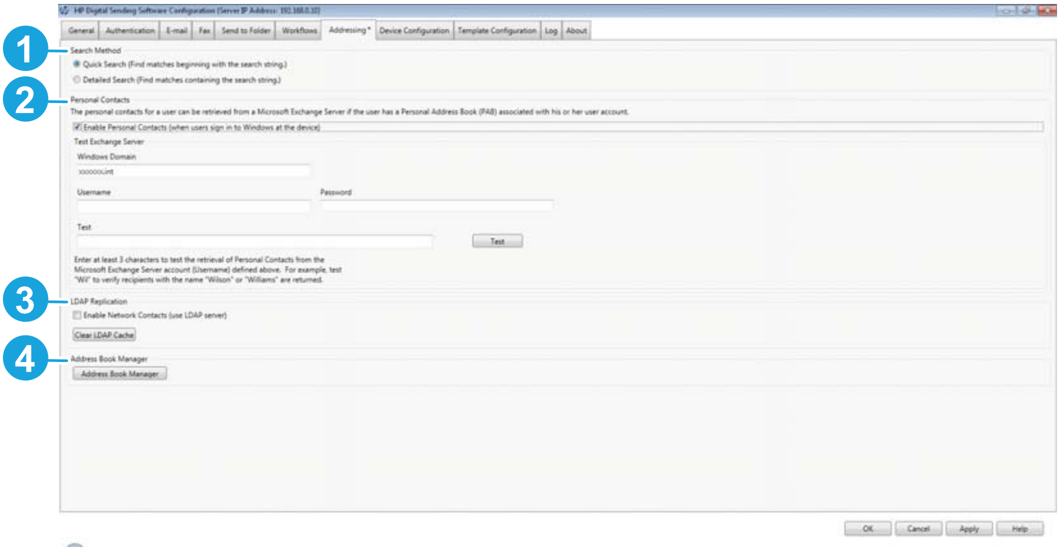
E-mail addresses can be imported from the Address Book Manager so that they can be made available to devices served by DSS. Four types of e-mail address lists can be imported:

- .CSV
- .HPB
- .LDIF
- Microsoft Exchange

Configuring address books on the Addressing tab

Use the Configuration Utility **Addressing** tab to configure DSS to make centralized address books available to digital-sender users.

Figure 3-53 The **Addressing** tab



HP Digital Sending Software Configuration (Server IP Address: 192.168.0.10)

Search Method

● Quick Search (Find matches beginning with the search string.)

○ Detailed Search (Find matches containing the search string.)

Personal Contacts

The personal contacts for a user can be retrieved from a Microsoft Exchange Server if the user has a Personal Address Book (PAB) associated with his or her user account.

☑ Enable Personal Contacts (when users sign in to Windows at the device)

Test Exchange Server

Windows Domain: xxxxxx.int

Username:

Password:

Test:

Enter at least 3 characters to test the retrieval of Personal Contacts from the Microsoft Exchange Server account (Username) defined above. For example, test "Wil" to verify recipients with the name "Wilson" or "Williams" are returned.

LDAP Replication

□ Enable Network Contacts (use LDAP server)

Address Book Manager

Table 3-20 Addressing tab

Callout	Component	Description
1	**Search Method**	Click to select **Quick Search** to find matches beginning with the search string. Click to select **Detailed Search** to find matches containing the search string.
2	**Personal Contacts**	The personal contacts for a user can be retrieved from a Microsoft Exchange Server if the user has a personal address book (PAB) associated with his or her user account. Click to select the **Enable Personal Contacts (when users sign into Windows at the device)** check box to enable this feature. Then type in the **Windows Domain**, **Username**, and **Password**. To test the credentials, type at least 3 characters into the **Test** text box, and then click **Test**.
3	**LDAP Replication**	Click to select the **Enable Network Contacts (use LDAP server)** check box, and then follow the steps below. ● **Network Directory Server (LDAP) (Step 1)**. Use the following controls to designate the LDAP server. ◦ Type the hostname or IP address in the **LDAP Server Address** text box or click **AutoFind** to have DSS find the LDAP server address. ◦ Click to select the **Use a secure connection (SSL)** check box. ◦ Type the port number in the **Port** text box. ● **Server Authentication Requirements (Step 2)**. Click to select one of the following options. ◦ **Server does not require authentication.** ◦ **Server requires authentication.** ● **LDAP Database Search Settings (Step 3)**. Use the following controls to configure the search settings.

Table 3-20 Addressing tab (continued)

Callout	Component	Description
		◦ Type in the **Path to Start Search (BaseDN, Search Root)** or click **Auto Find** to have DSS find the path. ◦ Select a **Source for Attribute Names** or click **Auto Find** to have DSS find the source. ◦ Type in the attribute to match the recipient's name, e-mail address, and fax number. ◦ In the **Advanced Search Options** section, Select the **Maximum LDAP Addresses** and the **Maximum Search Time** from the drop-down menus, and then type in the **LDAP Filter Condition** in the text box. ● **Test for LDAP Retrieval (Step 4)**. Type in at least 3 characters to test the retrieval of address book entries using the LDAP setup, and then click **Test**. ● **Sync Schedule (Step 5)**. Select a sync schedule from the drop-down menu, or click **Sync now**. The last replication shows in the text box.
4	Address Book Manager	Click this button to launch the Address Book Manager. For more information, see Address Book Manager on page 90.

Configuring Personal Contacts feature

When the **Enable Personal Contacts** check box on the **Addressing** tab is selected, users can gain access to their personal Outlook contacts address books at the device. Exchange Contacts support is only available if authentication is enabled and the authentication method is set to Microsoft Windows. See Authentication on page 57 for more information.

Configuring DSS address books

DSS uses address books to store e-mail addresses that a user types at the device. If user authentication is enabled on the device, addresses are stored in a user's personal DSS address book. Otherwise, the addresses are stored in a public DSS address book. These DSS address books are available to every digital sender or device that DSS supports. If the addresses that are contained in these address books are no longer needed, they can be deleted by clicking **Clear** in the **DSS Address Books** section of the **Addressing** tab. This lists all existing address books, so that one or more of them can be selected.

Configuring LDAP directory replication

The e-mail addresses and fax numbers in the address book come from several sources:

- The LDAP server on the network
- Destinations that users have previously specified at the control panel
- E-mail and fax address books that have been created by using the HP Address Book Manager

One of two methods can be used to synchronize the digital-sender address books with the LDAP server. Table 3-21 Address book synchronization on page 94 contains descriptions of these methods.

Table 3-21 Address book synchronization

Method	Description	Effect at the control panel
Using a replicated LDAP address book	DSS takes a snapshot of the LDAP server database and populates the device address book with the addresses that it finds. The Configuration Utility can be used to either initiate the task manually or schedule it to run automatically at a certain time.	As the user types the initial characters in a name, the device attempts to complete the name from the names in the address book. The user types more characters until a match is found. When the user selects a name, the associated e-mail address is automatically selected.
Using an LDAP address book directly	Firmware in the device initiates and resolves name queries directly with the LDAP server. The administrator does not need to synchronize the address book with the LDAP server, either manually or according to a schedule.	The user types a partial name. The device shows the list of resulting names from the LDAP server. When the user selects a name, the associated e-mail address is automatically selected.

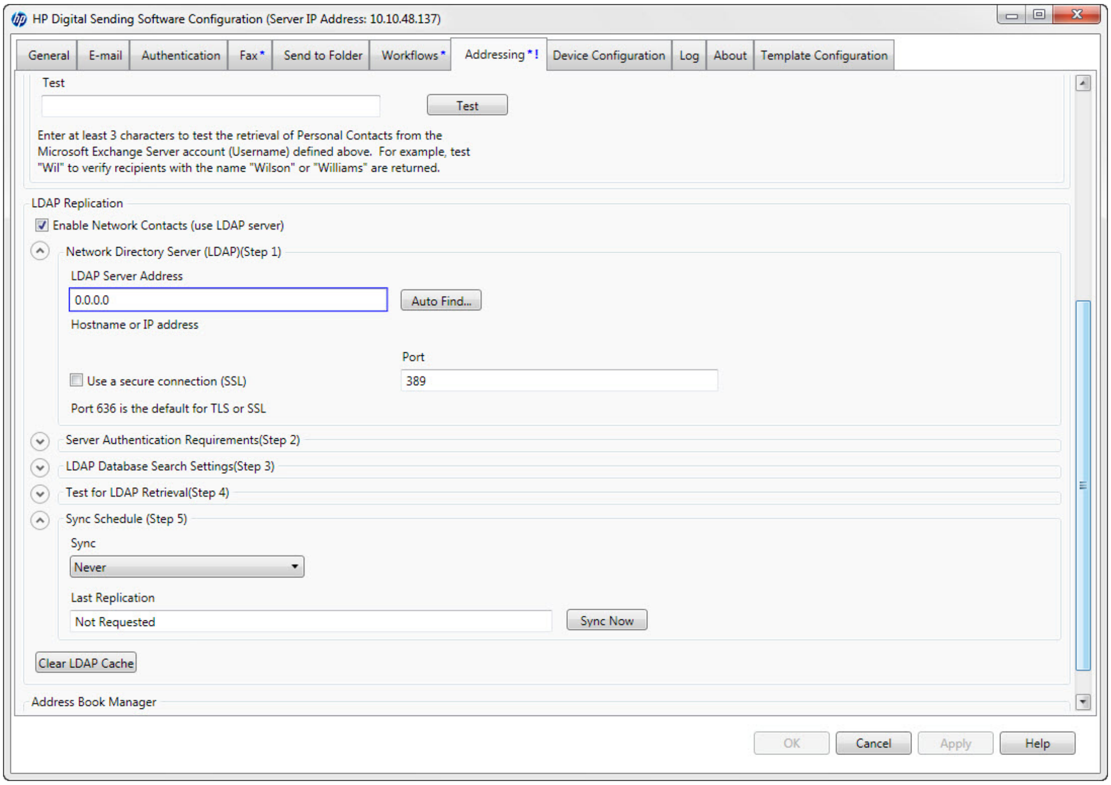
NOTE: If the device is configured to use an LDAP address book directly, it cannot gain access to the replicated address book. If replication is used, only the display names and e-mail addresses are replicated.

To set up automatic replication of the LDAP address book

1. On the DSS server, open the Configuration Utility, and then click the **Addressing** tab.

2. Click to select the **Enable Network Contacts** check box. The screen expands to show the steps for configuring the LDAP server.

   Figure 3-54 **Enable Network Contacts** section



HP Digital Sending Software Configuration (Server IP Address: 10.10.48.137)

Test

Enter at least 3 characters to test the retrieval of Personal Contacts from the Microsoft Exchange Server account (Username) defined above. For example, test "Wil" to verify recipients with the name "Wilson" or "Williams" are returned.

LDAP Replication

☑ Enable Network Contacts (use LDAP server)

Network Directory Server (LDAP)(Step 1)

LDAP Server Address: 0.0.0.0

Hostname or IP address

☐ Use a secure connection (SSL)

Port: 389

Port 636 is the default for TLS or SSL

Server Authentication Requirements(Step 2)

LDAP Database Search Settings(Step 3)

Test for LDAP Retrieval(Step 4)

Sync Schedule (Step 5)

Sync: Never

Last Replication: Not Requested

Address Book Manager

3. Click the arrow next to **Sync schedule**. The screen expands to show sync options.

4. Select a replication schedule from the **Sync** drop-down menu. Click **Sync Now** to replicate now. The **Last Replication** text box displays the last time the LDAP address book was replicated.

Personal address books

The Personal address book feature is automatically activated when users are authenticated at the device. The feature allows users to access and maintain a Personal address book from the front panel of any devices connected to the same DSS server.

An administrator can manage the contents of the Personal address books using the **Address Book Management** tab in the Configuration Utility.

Exchange contacts

The Exchange Contacts feature allows users to access their Microsoft Exchange Contacts from the front panel of devices. The feature must be activated in the DSS Configuration Utility. Users have read only access to the Exchange Contacts – entries added from the front panel of the device go into the Personal address book.

Guest address book

The Guest address book is always available to all devices and cannot be disabled. This address book is used to store addresses added by un-authenticated users ("guests") from the front panel of devices.

Public address book

The Public address book is always available to all devices and cannot be disabled. An administrator can use the Address Book Management tab in the Configuration Utility to manage the contents of the address book.

When enabled any address book entries added from the front panel of devices by un-authenticated users will be put into the Public address book – and thereby be available to all other devices connected to the same DSS server.

Use the Public Address Book when certain e-mail addresses and/or fax numbers need to be available to all devices.

LDAP replication

The LDAP Replication feature is designed to off-load LDAP servers by replicating the information into the DSS address book at a schedule set by the administrator. The address book information replicated from LDAP is stored in a dedicated, read-only and hidden address book.

The configuration settings for LDAP Replication are very similar to those for LDAP Addressing. The administrator needs to supply the address/name of the LDAP server, which port to connect to, the "bind" method and credentials, as well as the "search root" (search context) and attribute settings.

LDAP filters

When doing an LDAP search, users and groups will appear in the result found.

To be able to filter the LDAP search, follow these steps.

1. Open the Configuration Utility, and then click the **Device Configuration** tab

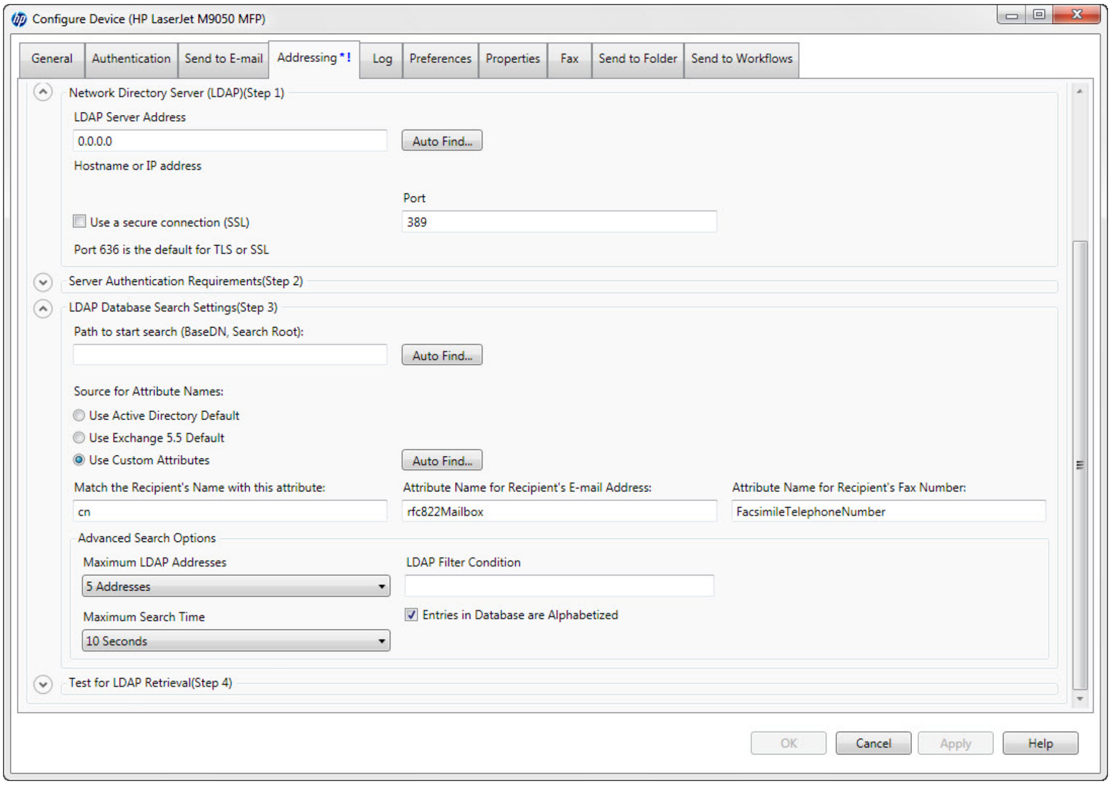
2. Click to select the device that you would like to filter. Click **Configure Devices**.

   NOTE: If all the devices need this filter, configure one and then copy the configuration to the other devices.

3. The **Configure Devices** dialog box appears. Click the **Addressing** subtab.

4. Click to select the **Enable Network Contacts (use LDAP server)** check box, and then click the arrow next to **LDAP Database Search Settings (Step 3)**.

Figure 3-55 The **LDAP Database Search Settings** section



Configure Device (HP LaserJet M9050 MFP)

Network Directory Server (LDAP)(Step 1)

LDAP Server Address: 0.0.0.0

Hostname or IP address

Port: 389

□ Use a secure connection (SSL)

Port 636 is the default for TLS or SSL

Server Authentication Requirements(Step 2)

LDAP Database Search Settings(Step 3)

Path to start search (BaseDN, Search Root):

Source for Attribute Names:

○ Use Active Directory Default

○ Use Exchange 5.5 Default

● Use Custom Attributes

Match the Recipient's Name with this attribute: cn

Attribute Name for Recipient's E-mail Address: rfc822Mailbox

Attribute Name for Recipient's Fax Number: FacsimileTelephoneNumber

Advanced Search Options

Maximum LDAP Addresses: 5 Addresses

LDAP Filter Condition:

Maximum Search Time: 10 Seconds

☑ Entries in Database are Alphabetized

Test for LDAP Retrieval(Step 4)

5. In the **LDAP Filter condition** text box, type in the syntax to filter the LDAP search.

   To exclude the groups setting for Exchange 5.5, the filter would be (!(objectclass=groupofnames)).

   Other e-mail settings could include but not limited to the following:

   - iPlanet: (!(objectclass=groupofuniquenames))
   - Active Directory: (!(objectclass=group))

6. Click **Apply**.

Configure DSS for Windows Active Directory Services

You must install the Digital Sending Software and ensure that the Digital Sending Service is running before you can configure the software for the Windows Active Directory environment.

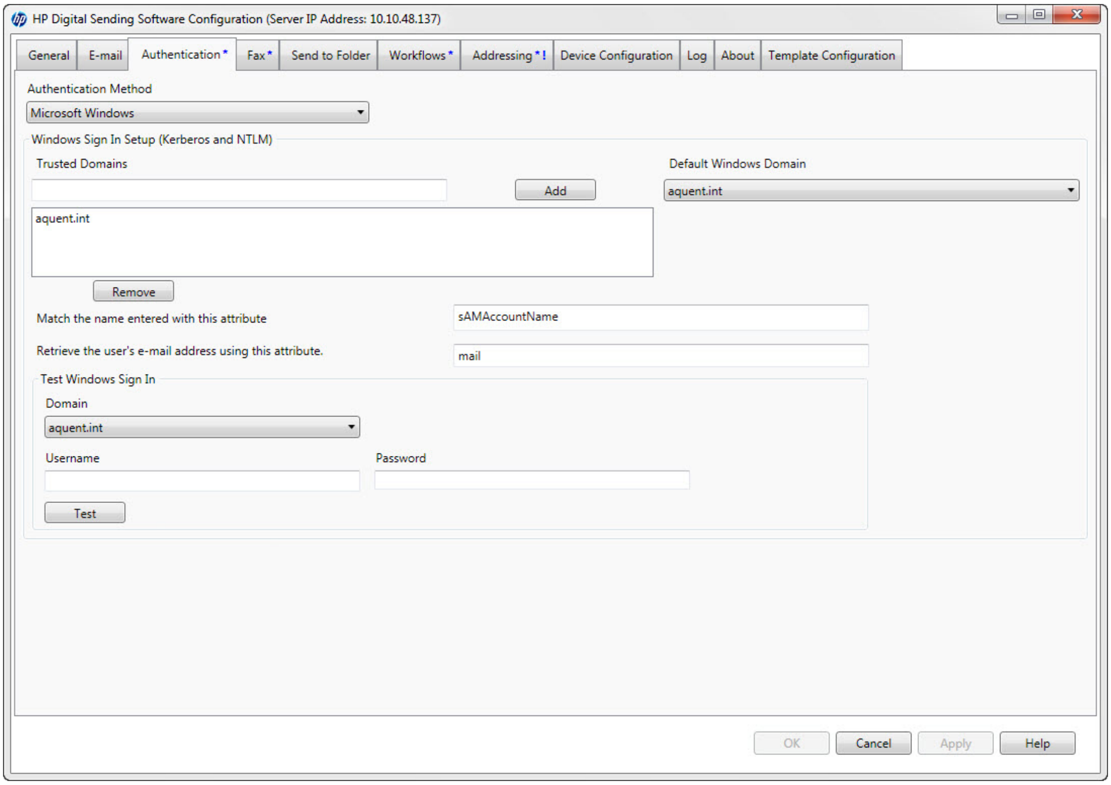
Configure Authentication

Follow these steps to configure Authentication for the Windows Active Directory environment.

1. Open the DSS Configuration Utility and click on the **Authentication** tab.

2. Click to select the **Enable Authentication** check box, and then select **Microsoft Windows** from the **Authentication Method** drop-down menu.

Figure 3-56 Authentication tab



HP Digital Sending Software Configuration (Server IP Address: 10.10.48.137)

Authentication Method: Microsoft Windows

Windows Sign In Setup (Kerberos and NTLM)

Trusted Domains: aquent.int

Default Windows Domain: aquent.int

Match the name entered with this attribute: sAMAccountName

Retrieve the user's e-mail address using this attribute.: mail

Test Windows Sign In

Domain: aquent.int

Username:

Password:

3. Type in the domain name in the **Trusted Domains** text box, and then click **Add**.

4. In the **Test Windows Sign In** section, select the domain from the **Domain** drop-down menu, and then type in the username and password for an authenticated user in the **Username** and **Password** text boxes. Click **Test** to test the credentials.

5. Click **Apply**.

Configure Addressing

Devices configured to use the Digital Sending Software can be configured to use one of two different types of address books: (1) an address book that resides on the server on which the Digital Sending Software is installed, and (2) the Global Address List (GAL) that exists as data in Active Directory. You can only configure a device to use one of these addressing methods at a time.

In option one, the Digital Sending Software can be configured to periodically export data from the Global Address List to the service-based address book. Or, by using the Address Book Manager (an optional component of the Digital Sending Software) administrators can create recipients by entering names and e-mail addresses or can import lists of recipients in several popular formats. In either case, devices perform queries of the service-based address book as users enter a recipient's e-mail address at the control panel of the device. Option one has the advantage that NTLM can be used to "bind" (authenticate) to the Active Directory server. Option two only provides Simple authentication.

NOTE: NTLM authentication can be used as the bind method for option one. Option two only provides Simple authentication. If Simple is chosen, the username and password are transmitted over the network as ‘cleartext.’ This means that this information can be read by anyone with access to the data on the network.

Configure the Service-Based Address Book

Follow these steps to configure the service-based address book.

1. Open the DSS Configuration Utility and click the **Addressing** tab.
2. Click to select the **Enable Network Contacts (use LDAP server)** check box.
3. In the **Network Directory Server (LDAP) Step 1** section, type in the IP address or Hostname of the Domain Controller or Global Catalog Server in the **LDAP Server Address** text box.

   NOTE: If the Global Catalog Server is used, the default LDAP port must be changed to 3268.

4. In the **Server Authentication Requirements (Step 2)** section, click to select the **Server requires authentication** option, and then select **NTLM** from the drop-down menu.
5. Type the credentials of an authenticated user into the **Username**, **Password**, and **Domain** text boxes.
6. In the **Sync Schedule** section, select the replication frequency.
7. Click **Apply**.

Configure individual devices to connect to the LDAP interface of Active Directory

1. Open the DSS Configuration Utility, and then click the **Device Configuration** tab.
2. Click to select the device you want to configure, and then click **Configure Device**.
3. Click the **Authentication** subtab. Set the **Authentication Method** to **Microsoft Windows**.
4. Set the **Login Method** to **Simple**.
5. Type in the credentials of an authenticated user into the **Username**, **Password**, and **Domain** text boxes.
6. Type the IP Address or Hostname of the Domain Controller or Global Catalog Server.
7. Make sure the **LDAP Database is Alphabetized** check box is not selected. When configuring for Active Directory Services, in most cases, having this check box selected will cause names shown in the list of matching names to **not** appear in alphabetical order.
8. Click **Apply**.

DSS templates

DSS templates are collections of device configuration settings that can be applied to individual products or groups of products. Templates configure a product’s settings at the time that they are applied to the product. There is no automated mechanism to maintain a product’s settings to match a template. A product’s settings can change after a template has been applied due to manual editing or the application of different template(s).

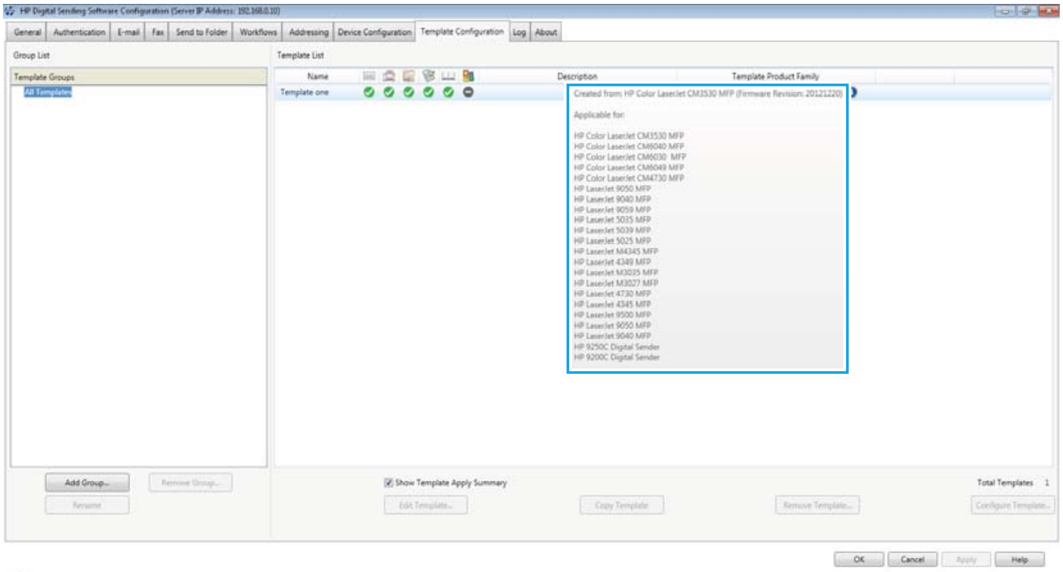
DSS template types are divided into the two following product-family classes:

- Pre-FutureSmart
- FutureSmart

Pre-FutureSmart templates are derived from the configuration settings of pre-FutureSmart products. FutureSmart templates are derived from the configuration settings of FutureSmart products. For more information on creating templates, see Create a template on page 100.

The **Template Product Family** column in the **Template List** area of the **Template Configuration** tab lists the product-family class for each template. Move your cursor over the 'i' icon to view the firmware version of the product used to create the template and the products supported by the template family.

Figure 3-57 DSS template family firmware and supported products view



☑ Show Template Apply Summary

Total Templates 1

Created from: HP Color LaserJet CM3530 MFP (Firmware Revision: 20121220)

Applicable for:

HP Color LaserJet CM3530 MFP
HP Color LaserJet CM6040 MFP
HP Color LaserJet CM6030 MFP
HP Color LaserJet CM6049 MFP
HP Color LaserJet CM4730 MFP
HP LaserJet 9050 MFP
HP LaserJet 9040 MFP
HP LaserJet 9059 MFP
HP LaserJet 5035 MFP
HP LaserJet 5039 MFP
HP LaserJet 5025 MFP
HP LaserJet M4345 MFP
HP LaserJet 4349 MFP
HP LaserJet M3035 MFP
HP LaserJet M3027 MFP
HP LaserJet 4730 MFP
HP LaserJet 4345 MFP
HP LaserJet 9500 MFP
HP LaserJet 9050 MFP
HP LaserJet 9040 MFP
HP 9250C Digital Sender
HP 9200C Digital Sender

This section contains the following topics:

- Create a template
- Use the Template Configuration tab to manage templates
- Apply a template

Create a template

Create a DSS template:

1. Click the **Device Configuration** tab.
2. Select a product from the **Device List** area.
3. Right-click the selected product, and then click **Create Template** from the menu.
4. Type a name for the template in the **Name** field.
5. Type a description for the template in the **Description** field.

NOTE: The **Configurable Features** section of this dialog window is read-only when creating a template.

6. Click the **OK** button to complete the creation of the template.

7. Check the template to be sure there are no issues. To check for issues, configure the template and make sure none of the tabs within the template show an exclamation mark (!) next to the tab name. If an exclamation mark is present, go to that tab and fix the problem, and then save the changes. See Configure a template on page 105 for information on configuring templates.

NOTE: New templates can have issues if the settings copied from the device are incomplete or conflict with other settings. For example, if a device is configured to send faxes via its internal modem but no Country/Region is configured.

A second source of template issues can occur because, due to security controls, passwords cannot be retrieved from FutureSmart devices. For example, if a device has a quickset that requires a password, then when the template is first created it will need a password for that quickset but no password will be present. FutureSmart templates require that passwords that exist on the device when a template is created be re-entered into the template after the template is created.

Failure to correct template issues such as these will result in errors when trying to apply the template to devices.

After a template is created, it becomes available for editing on the **Template Configuration** tab and can be applied to products present on the **Device Configuration** tab. For more information on applying templates, see Apply a template on page 105.

Use the Template Configuration tab to manage templates

Use the **Template Configuration** tab to view and edit DSS templates and template groups.

Figure 3-58 DSS Template Configuration tab

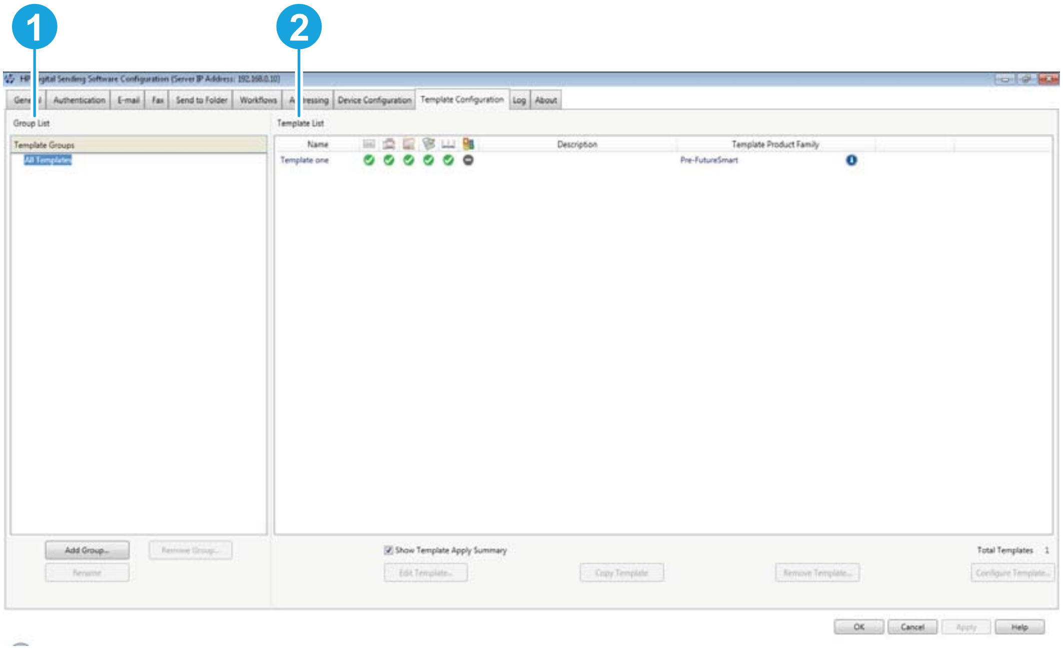


Table 3-22 DSS Template Configuration tab

Callout	Component	Description
1	**Template Groups**	A list of the template groups defined on the DSS server.
2	**Template List**	A list of the templates defined on the DSS server.

Template groups

The **Template Groups** area of the **Template Configuration** tab allows you to create, organize, and group templates for application to products.

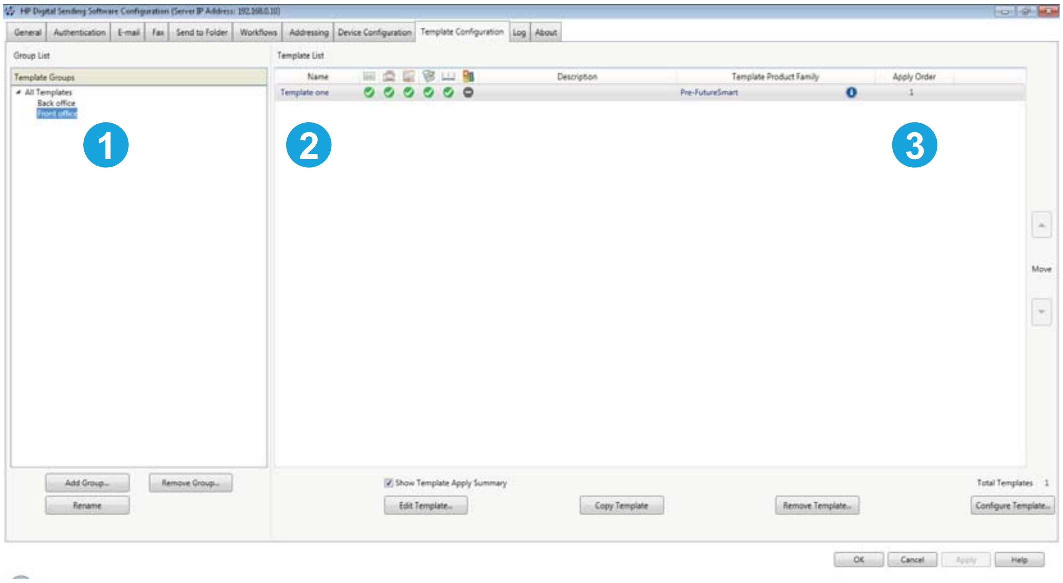
Create a template group

Use the following steps to create a template group:

1. Click the **Add Group...** button in the **Template Groups** area.
2. Type a name for the group in the **Group Name** field.
3. Click the **OK** button to save the group.

Template groups can be nested beneath other template groups. To nest an existing template group, drag and drop the group onto another group. To create a nested template group, select an existing group before creating the new group. The new template group will be created beneath the selected existing group.

Figure 3-59 DSS template groups



Name							Description	Template Product Family		Apply Order
Template one	✓	✓	✓	✓	✓	⊖		Pre-FutureSmart	ⓘ	1

☑ Show Template Apply Summary

Total Templates 1

Table 3-23 DSS template groups

Callout	Component	Description
1	Nested template groups	A list of the nested template groups defined on the DSS server.
2	Templates contained in the nested group	A list of the templates defined in a nested template group on the DSS server.
3	**Apply Order**	Lists the order of application of templates in a group.

Add a template to a group

▲ Select one or more templates from the **Template List** area.

Right-click the selected template(s), select **Add to Group**, and then click the group to add the template(s).

-or-

Drag and drop the template(s) onto the group in the **Template Groups** area.

The templates in a group are given an order of application for when they are applied to a product. This order of application is listed in the group's **Apply Order** column.

The apply order for a template group designates the order in which templates in the group, and their associated device settings, are applied to a product. The template with the greatest numerical apply order value is applied last.

For example, if two templates in the same group both have send to folder settings defined, the send to folder settings defined in the template with the higher numerical apply order value will take precedence. However, a template with a lower numerical apply order value may have a group of settings not defined in templates with higher apply order values. In this case, that group of settings would be part of the overall settings applied to the selected product.

The following table is a scaled down example of template application ordering and settings precedence.

Table 3-24 Template groups apply order example

Template example	Apply order	Settings
Template A	1	Send to folder ● Default Color Preference: Black/Gray ● Default Resolution: 600 dpi General ● Name: Admin
Template B	2	Send to folder ● Default Color Preference: Color ● Default Resolution: 200 dpi
Final net settings	Template A + Template B Template B takes precedence for common settings. Settings in Template A, but not in Template B, are included.	Send to folder ● Default Color Preference: Color ● Default Resolution: 200 dpi General ● Name: Admin

Use the **Remove Group...** and **Rename** buttons to remove or rename groups in the Template Groups area.

Template list

The **Template List** area of the **Template Configuration** tab lists all the available templates on the DSS server. DSS templates can be edited, copied, removed, and configured in this area.

Edit a template

Use the following steps to edit a template:

1. Select a template from the **Template List** area.
2. Click the **Edit Template...** button.
3. Change the **Name**, **Description**, or **Configurable Features** settings for the template.
4. Click the **OK** button to save your changes.

Copy a template

The copy template functionality allows you to create a new template, with a unique name, based on an existing template. When creating a copy of a template, the **Configurable Features** defined in the source template may be changed for the new template.

NOTE: The model number and firmware version of the product used to create the original template are available on the Information tab of the copied template.

1. Select a template from the **Template List** area to copy.
2. Click the **Copy Template...** button.
3. Enter a unique name for the copied template in the **Name** field.

   NOTE: Copied templates cannot be saved with the name of an existing template.

4. Enter a description for the template in the **Description** field.
5. Select, or de-select, any features in the **Configurable Features** area.
6. Click the **OK** button to save the copied template.

Remove a template

Use the following steps to remove a template from the DSS server:

1. Select a template from the **Template List** area.
2. Click the **Remove Template...** button.
3. Click the **Yes** button in the dialog window to confirm the removal of the template.

NOTE: The template is also removed from any groups it has been associated with.

Configure a template

The configure template option allows specific changes to be made to a template's settings. Clicking the **Configure Template** button opens a set of tabs containing tabs for each configurable feature specified in the template settings.

For example, if the **Send to Folder** feature has been checked in the **Configurable Features** area of the template, the **Send to Folder** settings tab will be available for editing in the **Configure Template** sub-tab set.

Use the following steps to configure a template:

1. Select a template from the **Template List** area.
2. Click the **Configure Template...** button.
3. Edit the template settings.
4. Click the **Apply** button.
5. Click the **OK** button.

Apply a template

A DSS-enabled product can have either individual templates or template groups applied to it. Templates and template groups can also be applied to device groups.

Use the following steps to apply templates to a product:

1. Click the **Device Configuration** tab.

2. Select a device from the **Device List**.

3. Right-click the selected device.

4. Choose **Apply Template** to apply a single template to the device, or choose **Apply Template Group** to apply a template group to the device.

The **Template Apply Summary** window displays, listing the specific details of the template application process. The **Description** column lists whether the template or template group was successfully applied.

Template settings can be overridden by changes to the product settings made at the product control-panel. If the settings in a template are not being applied as expected, it might be necessary to reapply the template to the product.

External Database Configuration

The primary means for configuring DSS to use an external database, which is any database other than the one DSS installs by default, is during installation. It is also possible to change the database that DSS uses, either from the default database to an external database, or from one external database to another, after software installation. This is done by running a utility that allows the administrator to change the connection string that DSS uses to connect to its database. **This must only be done with CAREFUL CONSIDERATION of the following point**:

- **Data that exists in the database which DSS is currently using will be lost and not transferred to the new database. This includes, but is not limited to, DSS address books and job logs.**

To change the database connection string after installation:

1. Run the utility

   ```
   <install folder>\scripts\ExternalDbConfigurationUtility
   \Hp.Dss.Utility.ExternalDbConfiguration.exe
   ```

   This utility provides the same UI for setting the database connection string as seen during installation. See step seven of Installer screens and options on page 37 for instructions.

2. Stop and then re-start the DSS service

3. Remove all the FutureSmart devices from DSS, and then add them back to DSS.

4 Support and troubleshooting

This chapter contains the following topics:

Obtaining support

This section contains the following topics:

- HP Customer Care service and support
- Finding documentation and other supporting information
- Using Internet support

HP Customer Care service and support

HP provides free phone support for Digital Sending Software. The support is provided by the HP LaserJet support organization. For contact numbers, please visit www.hp.com/support.

Finding documentation and other supporting information

The following table outlines the source for, and description of, the information that is available about issues that can arise when using HP DSS.

Table 4-1 Sources of information

Source	Description
Device online Help system	DSS-enabled devices feature an online Help system that provides instructions for resolving common problems. To use Help, press **?** on the control panel.
DSS event log	The event log is a list of major events that DSS encounters. It can be accessed by navigating to the **Log** tab of the DSS Configuration Utility. Two logs can be viewed: ● The Configuration Utility **Log** tab shows general log messages for DSS. ● In the Device Configuration section of the Configuration Utility, a second **Log** tab shows log messages that are specific to the selected device. See the Help file for the Configuration Utility for a list of messages and recommended actions.
Windows Event Viewer messages	The Windows Application Event log and System Event log can provide significant information for issue resolution. Both logs may contain some information logged by DSS, as well as information logged by other applications, that can point to the causes of DSS behavior
Control-panel messages	Messages appear on the device control panel to report Digital Sending problems.
Configuration Utility messages	Messages appear in the Configuration Utility when problems occur.
Alert notifications	E-mail alert notifications can be sent when Digital Sending problems occur. Administrators can configure DSS to send alert e-mails on the **General** tab of the Configuration Utility.

Using Internet support

Information about the software and all documentation can be found at the following Website:

www.hp.com/support/dss

DSS error messages

Select the **Notify administrator of critical error** check box on the **General** tab of the Configuration Utility to receive e-mail messages when critical errors occur. The subject line of these e-mail messages reads: **Digital Sending Software – Critical Error Notification**. The e-mail message body reads as follows: "The Digital Sending Software server [server TCP/IP] incurred a critical error [error message]. This error might require administrative action."

This section lists some of the critical-error messages that might be sent.

Table 4-2 **Critical error messages**

Error Message	Suggested Actions
Insufficient disk space to allow job	Check available disk space on the DSS server. In some high-usage environments where numerous devices are configured in DSS, several gigabytes of free disk space might be required during peak usage periods.
A notification message was not printed on the [device TCP/IP] printer	Verify that DSS can communicate with the device that is indicated in the message.
Address Book checking terminated with a severe corruption indication	Call HP Support or an authorized service provider. The Address Book might need to be rebuilt.
The SMTP server didn't accept the e-mail message because it was too big	Reduce the e-mail size limit in DSS to a number less than the limit that is configured at the SMTP server.
A disk file was not downloaded to the [device IP] printer	Remove the device (indicated by the TCP/IP address) and add the device back again to DSS.

Index

www.hp.com