HP LaserJet 4345 MFP Security Checklist

3/29/2006

Table of Contents

1 Introduction

This document is a security checklist for HP LaserJet 4345 MFPs (hereafter called MFPs) and related peripheral management solutions. This checklist is written for acceptance by the National Institute of Standards and Technology (NIST) and will be available at the NIST website. HP thanks NIST for its support in the process of creating this document.

This checklist is meant for trained network administrators, who use HP Web Jetadmin and the Embedded Web Server (EWS) to configure security settings for normal use in enterprise networks that include access to the internet.

This checklist includes step-by-step instructions to configure MFP security settings using remote access from a network PC. These instructions assume that the network is a TCP/IP network that includes MFPs, Web Jetadmin peripheral management software, DHCP, DNS, LDAP and other components necessary to have a network. Thus, the settings recommended in this checklist are not necessarily applicable to all network environments. You should assess the tools and applications in your network to determine how to they relate to the settings recommended in this checklist.

This checklist assumes that network administrators are familiar with HP Web Jetadmin and use it to configure one or more MFPs. It assumes that network administrators are also familiar with EWS, HP Jetdirect connections, and with firmware upgrades for Jetdirect and MFPs. Refer to the MFP User Guide and the HP Jetdirect Administrator Guide for information on Jetdirect connections. You can find MFP user documents at the following website or by searching for them at hp.com:

HP LaserJet 4345 MFP user guides

Web Jetadmin is a web-based peripheral management tool that uses any standard web browser to access status and settings for MFPs and other peripherals. It is the recommended management tool for all HP network printing products. It handles most settings recommended in this document and much more. HP Web Jetadmin is available free for download and installation at the following location:

http://www.hp.com/go/webjetadmin

You can also find HP Web Jetadmin by searching for it at hp.com. You should install Web Jetadmin and become familiar with its features and functions before attempting to use this checklist.

Some recommended settings are available only using the Embedded Web Server (EWS) on each MFP. These settings are covered in the EWS Settings section. Also, check the Settings List section for a complete list of all recommended settings. The Settings List section includes checkboxes for convenience while making configurations. Print the Settings List section, and mark each configuration as you go.

Keep in mind that Web Jetadmin manages a wide variety of network printers and other peripherals, and it may use terminology that differs slightly from terms in the EWS.

This checklist is a guide to security configurations that allow for reasonable convenience and usability for the MFPs. Some of the recommended settings create extra steps in processes to access and manage MFPs. For instance, once you disable EWS configuration access, the only

way to access the configuration settings in the EWS is to re-enable EWS configuration using Web Jetadmin.

TIP: **You may wish to configure one MFP to the recommended security settings, and use it as a template in Web Jetadmin to configure other MFPs to the same settings.**

You may wish to use higher-level security measures for your network if it is particularly sensitive, for instance, to meet Department of Defense security standards. The instructions address the implications of each setting, and they provide suggestions for higher-level security where applicable. You should consider the impact of each setting on your network, and configure it according to your needs. See the Ramifications section for more information on how these settings can affect various networks.

Much of the information and recommended settings in this checklist are applicable to other HP MFPs and printers especially as they relate to Web Jetadmin configurations. See product guides and Web Jetadmin guides for more information. You can also find detailed information about configuring HP products by searching at hp.com.

This checklist is provided as a complimentary guide to known best practices for increasing security for MFPs in enterprise networks. HP does not claim or warrant that configurations recommended in this document prevent misuse of MFPs or networks or that they prevent malicious attacks on MFPs or networks. Use this document as a reference at your own risk.

1.1 Coverage and Testing

This checklist covers only those parts of HP Web Jetadmin and the EWS that pertain to the recommended settings. The instructions for configuring the settings are presented in the order in which they are the most efficient and effective.

This checklist covers a wide variety of settings that interact with one another and with other network components. These settings are tested in various conditions and in various combinations in test environments. Testing includes setting recommended configurations and trying to use affected features of the network. However, it is impossible to test these configurations in all plausible network environments. You should test these settings in your environment to ensure that you understand the ramifications of them. You may find that some of the recommended settings cause undesirable limitations in your network. See the Ramifications section for further information and cautions.

NIST defines several user environments including environments targeted for HP LaserJet 4345 MFPs; however, this checklist is written to cover enterprise environments. Enterprise environments generally use most all MFP features and capabilities where other environments generally use a subset of them. Thus, this document covers configurations recommended for all types of environments. Consider the impact of each recommended setting on your network environment, and configure the MFP accordingly.

1.2 Assumptions

This checklist makes some assumptions about network administrators and about the enterprise environments:

- Network administrators – This checklist assumes that readers are trained network administrators who are familiar with common networking practices and that they are familiar with the use of Web Jetadmin, EWS, and other network management solutions. Network administrators should understand basic configurations of HP MFPs (or printers) including the use of HP Jetdirect hardware and controls. Administrators should have read the MFP user guide, the MFP administrator guide, the Jetdirect administrator guide, Web Jetadmin user guides, and help files to have a good understanding of the intended usage of MFPs. This checklist relies on user guides to provide necessary information.
- MFP – This checklist covers security settings for one HP LaserJet 4345 MFP only as installed on a network as shipped with factory default settings. The recommendations in this checklist are for an MFP that is already installed and operating correctly in a network. You can configure these settings on multiple MFPs using Web Jetadmin if you are familiar with such techniques.

  While the recommended settings are applicable to some other MFP models, all references and mentions of MFPs in this document are about an HP LaserJet 4345 MFP only.
- Updated firmware – This checklist assumes that each MFP has the latest MFP firmware and the latest Jetdirect firmware. Updated firmware is available for download and installation at the following website:
  http://www.hp.com/go/lj4345mfp_software
  Follow all instructions at the website above to upgrade firmware.
- Web Jetadmin – Much of this checklist is written for use with HP Web Jetadmin. You should install Web Jetadmin, configure it for network security, and become familiar with its use before attempting to configure this checklist. See Web Jetadmin help and user documentation for instructions. Security settings for Web Jetadmin are covered in a white paper at the following location:
  HP Web Jetadmin 7.2 and 7.5 - Password Protection, Profiles, and Other Methods to Make HP Web Jetadmin Secure
- Single MFP – This checklist is written as though only one MFP is configured; however, Web Jetadmin can configure multiple MFPs using the same process.

  TIP: **You may wish to configure one MFP for recommended settings and use it as a template to configure more MFPs using Web Jetadmin. See Web Jetadmin instructions for saving and copying configurations.**
- Environment – This checklist is written for administrators of enterprise networks. However, settings recommended in this checklist apply to most networks. You should consider each recommended setting as it relates to your network, which may include a variety of applications and tools that require access to the MFP.
- Network connection – This checklist assumes that each MFP is connected directly to a local area network via Jetdirect. Other connections, such as direct-connect via parallel cable are not covered in this checklist or tested by HP.
- Suggested settings – All steps in this checklist are only suggestions for best practice security in common enterprise MFP environments. You should make judgments about each recommended setting and configure the MFP to meet your needs. For instance, you would

not disable IPX/SPX protocol if your network uses it with Novell servers. This checklist explains the implications of each recommended setting as much as possible.

Keep in mind that HP LaserJet 4345 MFPs are designed to be flexible and accessible in a wide variety of environments. The configurations recommended in this checklist can limit flexibility and accessibility to promote network security.

- Internet - all HP LaserJet 4345 MFPs should be installed behind network firewalls and other standard tools such as updated virus protection applications. This checklist assumes that the network includes basic security configurations and components.
- Intranet – All networks on which HP LaserJet 4345 MFPs are installed should include standard common network tools such as use of encryption for sensitive data and protection against compromises with physical installations (for instance, wire closets are kept locked).

1.3 Solutions covered

This checklist covers MFP device configurations for HP LaserJet 4345 MFPs as shipped from HP (out of the box). The checklist covers these settings as they appear in remote configuration utilities: Web Jetadmin and EWS. Most of these settings are available only using HP Web Jetadmin management software; some are available only using the MFP EWS. This checklist covers no other solutions or applications.

1.4 Organization

This checklist includes the following sections to organize recommended configuration procedures:

- Threat model – The Threat Model section explains the circumstances around a typical installation of an HP LaserJet 4345 MFP. It follows the Microsoft® STRIDE model to list the types of data that MFPs encounter and the possible threats implied with MFP communications.
- Network Security – The Network Security section provides step-by-step instructions on configuring MFP settings for security. It covers settings in the MFP EWS, and in Web Jetadmin.
- Settings List – The Settings List section is a list of the recommended settings without explanations. A checkbox accompanies each item in the Settings List for convenience as you make the configurations.
- Physical Security – The Physical Security section explains security concerns for the types of information that an MFP would handle while a user is working directly with it, such as picking up print jobs, copying, and scanning. This section includes suggestions for securing or locking removable accessories such as networking cards and hard drives. It also covers security for access to hardware components of an MFP.
- Ramifications – The Ramifications section explains possible limitations that each recommended setting places on the usability and convenience of the MFP. It is reasonable to expect certain compromises in functionality as a trade off to a higher level of security.

2 Threat Model

This section explains the types of security risks involved with operating MFPs in enterprise environments. This is not a comprehensive treatment of these issues. This section is only to alert you of some general examples of the types of threats that can affect MFPs. The remainder of the checklist provides instructions to help protect against these threats.

This section covers the threat model using the Microsoft STRIDE model of threats:

- Spoofing identity
- Tampering with data
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

The following subsections explain how each type of threat relates to MFPs:

2.1 Spoofing Identity

Spoofing identity is masquerading as someone else to fool others or to get unauthorized access. This includes any of the following:

- Placing the address of a known person into the **From address** field of an email message pretending to be that person. Example: Someone could place the address of a co-worker in the **From address** field and send embarrassing or malicious messages others as though the co-worker wrote them.
- Using someone else's email address credentials to log in to the email server to get access to address books
- Using someone else's email address credentials to have free use of an email service
- Using someone else's email credentials to view that person's email messages
- Using someone else's log on privileges for access to MFPs or networks

You can minimize the risks from identity spoofing in the following ways:

- Protect the **from address** field in the Digital Sending and Fax configuration.
- Protect disc access.
- Configure authentication.

2.2 Tampering with Data

Tampering with data can include any method of changing, destroying, or adding to information that is flowing to or from an MFP or stored on it. Here are some examples of tampering with data:

- Canceling someone else's job. The person who sent the job finds that only part or none of the job was printed.
- Intercepting a print job before it reaches the MFP, altering it, and sending it on to the MFP
- Intercepting remote configuration data, such as communications between Web Jetadmin and the MFP, to get passwords and other information

Here are some methods to minimize opportunities of tampering with data:

- Disable **Cancel Job** button.
- Encrypt the data stream to render files unreadable to unauthorized users.
- Prevent unnecessary remote access to files in process, such as closing down all unused ports and protocols.
- Configure SNMPv3 for Web Jetadmin.
- Close down unused ports to prevent unnecessary access to the hard drive.

2.3 Repudiation

Repudiation in the context of MFPs is using the MFP without leaving behind usage information. This includes preventing the MFP from logging data or bypassing security checks such as user authentication. This also includes finding ways to use the MFP for free if job accounting software is used to charge for usage. Here are some examples of repudiation on an MFP:

- Accessing usage logs to remove entries of an individual
- Changing file metadata to remove usage records
- Bypassing user authentication for anonymous use of the MFP
- Finding a way to grant access to the MFP without authenticating

Here are some methods of minimizing opportunities for repudiation on MFPs:

- Encrypt the data stream to include log data and file metadata.
- Prevent unnecessary access to the hard drive by closing unused ports and protocols.
- Save copies of log data at a separate location
- Add further security processes such as swipe-card readers and thumb-print readers.

2.4 Information Disclosure

Information disclosure is gathering information from an MFP and providing it to unauthorized users. This can include job information, authentication information, or information from the contents of a job. Here are some examples of information discloser on an MFP:

- Reading stored print jobs on the MFP hard drive
- Downloading log information

- Intercepting print jobs, copy jobs, fax jobs, or digital send jobs (such as email)

Here are some methods of minimizing opportunities for information disclosure on an MFP:

- Encrypt the data stream.
- Prevent unnecessary access to the MFP hard drive by closing unused ports and protocols.
- Configure all possible password settings.

2.5 Denial of Service

Denial of service is any type of interference with normal use of an MFP. This can include any of the following:

- Canceling or pausing the print jobs of others
- Turning off the MFP
- Disconnecting the MFP from the network
- Causing interference with network communication to the MFP
- Changing the network location of the MFP
- Causing an error state that interrupts service
- Changing access configurations to block usage

Here are some methods of minimizing opportunities for denial of service on an MFP:

- Lock the control panel.
- Lock EWS configuration settings.
- Close unused ports and protocols.
- Disable controls such as the Job Cancel button and the Go button.
- Enable the MFP to resume when possible if an error state stops it from processing.
- Control physical access to the MFP.

2.6 Elevation of Privilege

Elevation of privilege is any method of upgrading authorized access to include unauthorized access. This can be any of the following:

- Non-administrators accessing configuration settings to get administrator privileges for themselves
- Unauthorized use of management software to set configurations to provide access to other unauthorized users
- Using management software to bypass job accounting functions

Here are some methods of minimizing opportunities for elevation of privilege:

- Set the administrator (device) password.
- Lock the control panel.

3 Network Security

The main purpose of this checklist is to provide you a method of configuring MFPs for network security. Each subsection covers one of the remote network tools with which you can configure recommended settings:

- Settings in EWS
- Settings in Web Jetadmin

Some of the recommended settings are available only in the EWS while most are available in Web Jetadmin. You should follow instructions in both sections to complete the checklist. Use the Settings section to check off each configuration to be sure to configure all recommended settings.

3.1 Settings in the EWS

This section covers settings recommended in the EWS: EWS Password, User Authentication, Access Control List, Send to Folder, and Encryption Strength. Some of these settings are also available in Web Jetadmin, but you should configure them in the EWS for best results. Web Jetadmin settings are covered in the next section.

3.1.1 EWS Password

The EWS Password feature requires all users to provide the password for access to the EWS configuration settings. This includes some settings that are also available in Web Jetadmin. Web Jetadmin will prompt for the EWS password whenever a user attempts to change settings that affect the EWS. Setting this password also sets the MFP Device (or Admin) password, which is covered later in this checklist.

Here is how to set the **Embedded Web Server Password**:

1. Open the MFP EWS using secure communication. To do this, open a standard web browser (Microsoft Internet Explorer appears in this checklist), and type https:// followed by the IP address of the MFP. Example:
   https://16.XX.XX.XX
   Using https rather than http ensures that the browser communicates securely with the MFP. After you press ENTER, the EWS default page (Figure 1) will appear.

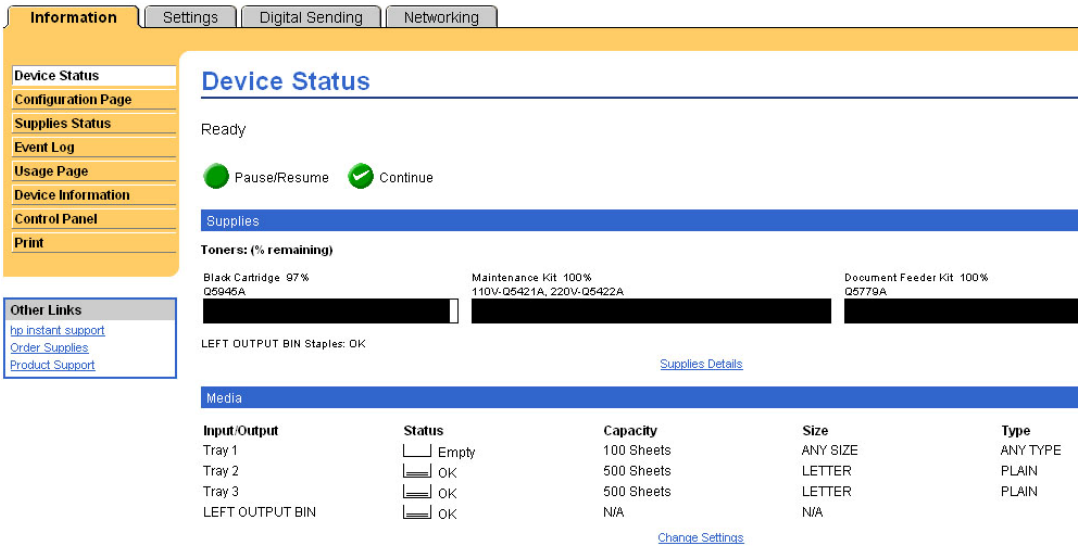

Figure 1: The default EWS page as it appears in Microsoft Internet Explorer.

2. Click the **Settings** tab at the top left of the page. The **Settings** page (Figure 2) will appear.

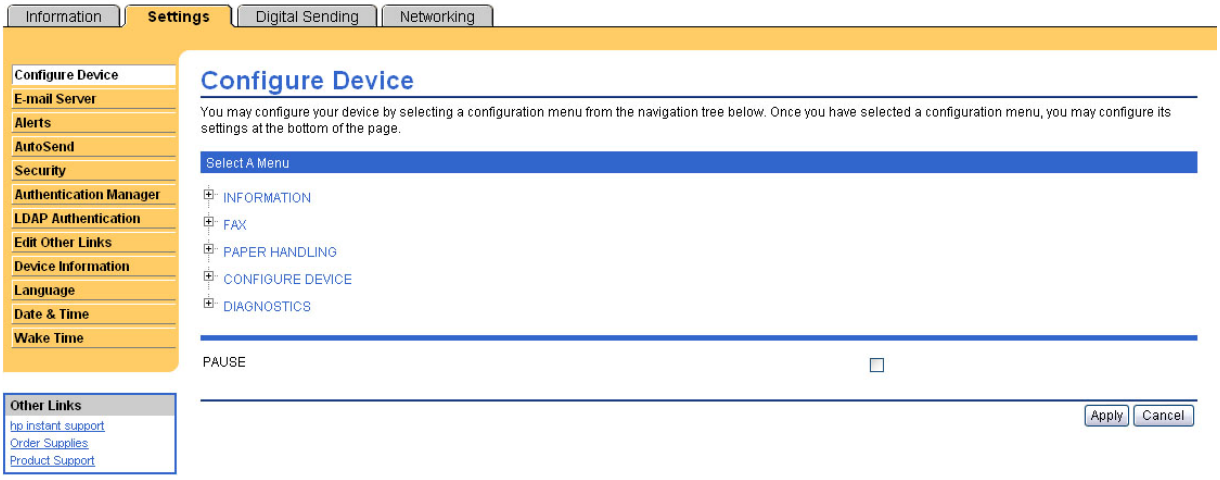

Figure 2: The default settings page of the EWS.

3. Click **Security** in the menu to the left. The Security Setting page (Figure 3) will appear.

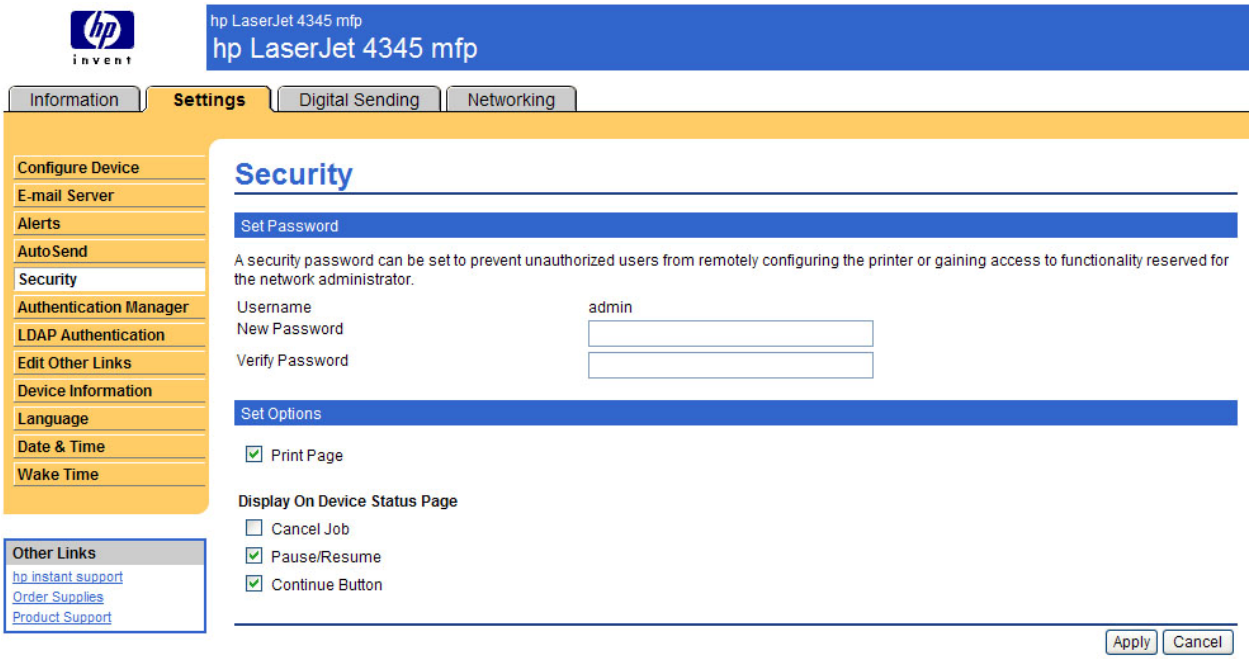

Figure 3: The EWS Settings Security page.

4. Type a password in the **New Password** field, and repeat it exactly in the **Verify Password** field.

   CAUTION: Remember this password, and provide it to authorized users. If this password is forgotten, the only way to restore access to EWS settings is to reset the MFP to factory default settings.

5. Click **Apply** at the bottom of the Security page (see Figure 3, above).

3.1.2 The Access Control List

The Access Control List (ACL) limits administrative access to only those computers or subnets on the list. This, along with the administrative password, can be very useful for controlling who can change settings on the MFP. Follow these instructions to configure the ACL:

CAUTION: Be sure to fill in the Access Control List correctly, or it can cause you to lose all access to configuration settings. See the HP Jetdirect Administrator's Guide for more information. If you lose access to configuration settings, the only way to restore it is by resetting the MFP to factory settings.

1. Click the **Networking** tab in the EWS. The **Networking** page (Figure 4) will appear.

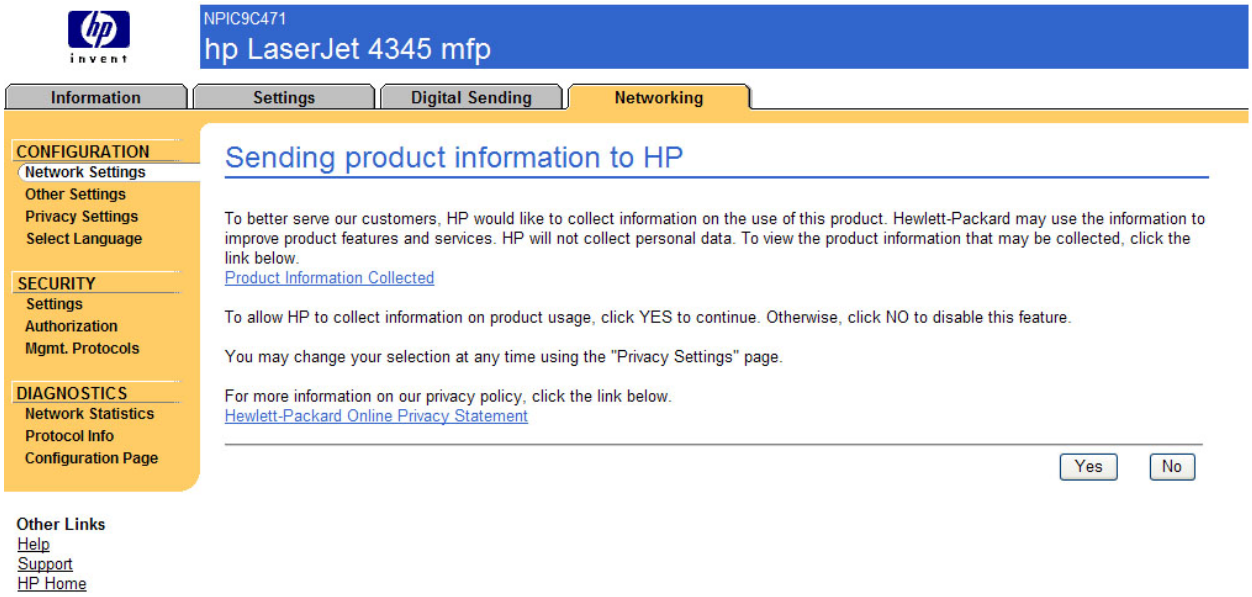

Figure 4: The EWS Network tab.

2. Click **Authorization** under the **Security** heading in the menu to the left. The **Authorization Settings** page (Figure 5) will appear.

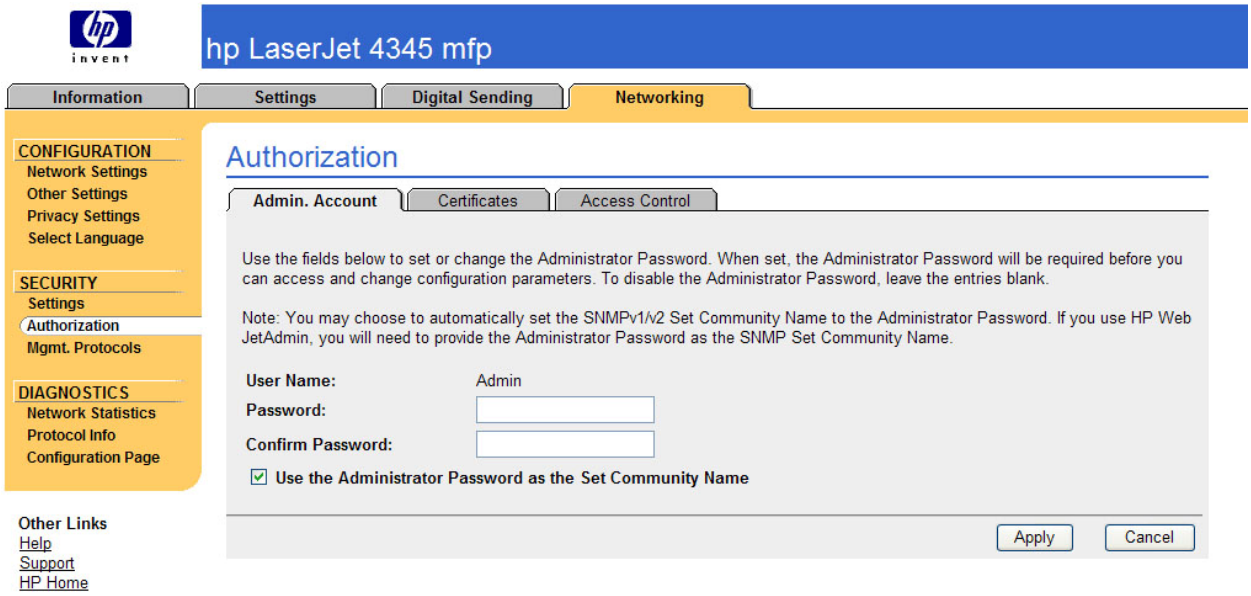

Figure 5: The Networking Authorization page.

3. Click the **Access Control** tab under **Authorization**. The **Access Control** page (Figure 6) will appear.

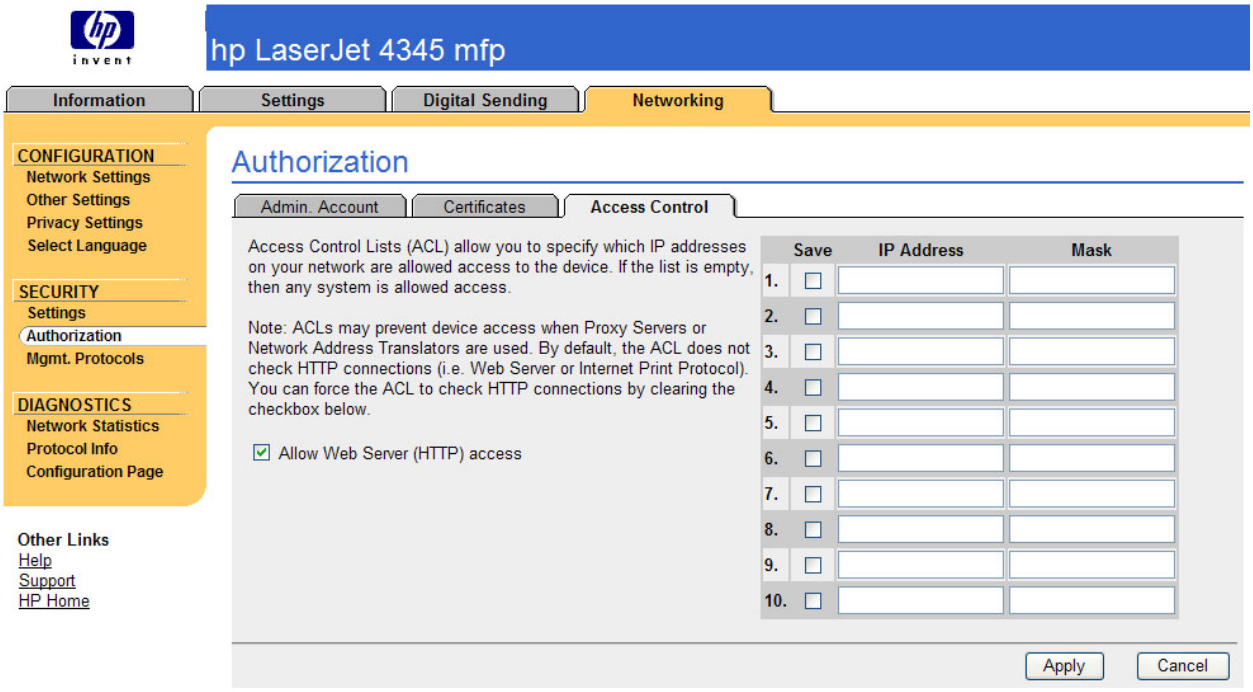

Figure 6: The Access Control page.

4. Fill in the table to provide the desired access controls. The Access Control List provides two types of access controls:

   - Limiting access to one or more computers – Type the IP address of a computer (leaving the Mask field blank) to which you want to grant access. By doing this, the ACL blocks access to all other computers on the network. Specify additional computers on subsequent lines to grant access to them.
   - Limiting access to one or more subnets – Type the IP address and the mask associated with the subnet to which you want to grant access. The ACL will block access to all computers outside that subnet. Specify other subnets to grant access to them. You can also grant access to specific computers (IP addresses) on subsequent lines.

   NOTE: The ACL limits access only when it is filled in.

5. Deselect (disable) the **Allow Web Server (HTTP) access** setting. This setting prevents access from computers, such as proxy servers, that are using HTTP. Disabling web server access ensures that only the computers on the Access Control List can configure the MFP. Configure computers that access the MFP to bypass proxy servers when accessing the MFP IP address.

   CAUTION: With Allow Web Server (HTTP) access disabled, the MFP might deny access to a computer attempting to use a proxy server because the proxy server has an IP address that is not in the Access Control List. Be sure to note the proxy configuration in the computer's browser. You can place the MFP IP address in the browser proxy exception list to ensure that the computer can access the MFP.

   CAUTION: If the Access Control List is filled in incorrectly, and the Allow Web Sever (HTTP) access setting is disabled, you can lose all remote access

to the MFP. At this point, the only way to restore access is to reset the MFP to factory settings. Be sure the Access Control List contains correct addresses before you disable web server access.

6. Click **Apply** at the bottom of the EWS page. If a confirmation page appears informing you of the success of the configuration, click **OK** or **Continue** to return to the EWS page.

3.1.3 Authentication

One of the most important security features of the MFP is user authentication. This feature requires users to login with usernames and passwords before they can use features of the MFP. In order to configure authentication, the MFP requires access to a network LDAP address server. This section does not cover setup and configuration of LDAP servers. It assumes that an LDAP server is already configured correctly and available.

Follow these instructions to configure an MFP for authentication:

1. Click the **Settings** tab in the EWS.
2. Click **Authentication Manager** in the menu to the left. The **Authentication Manager** page (Figure 7) will appear.

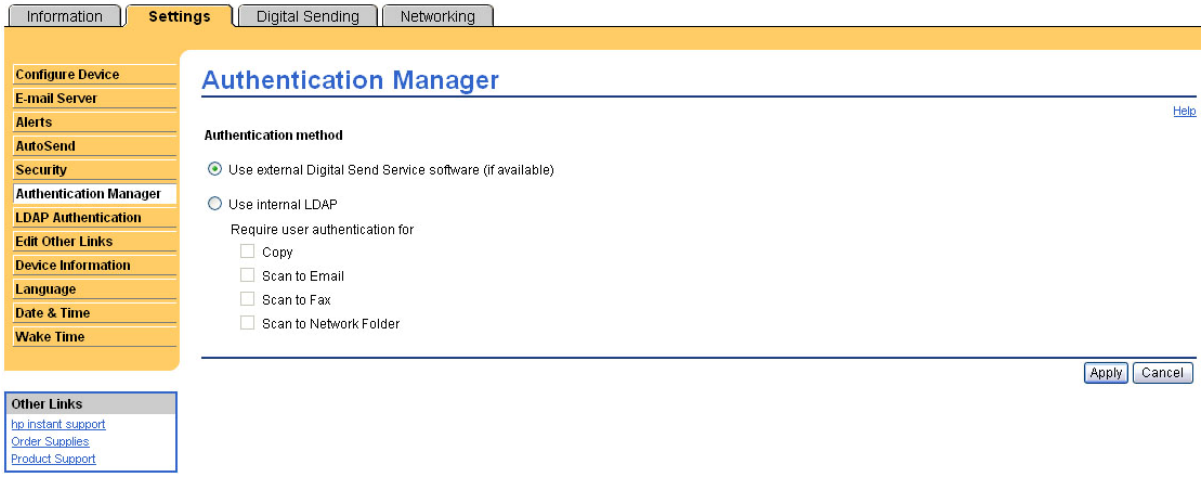

Figure 7: The EWS Authentication Manager Page.

3. Click **Use Internal LDAP**. The Internal LDAP option enables the MFP to authenticate users via a network LDAP server (it is called Internal LDAP because it is a new feature of the MFP that allows for authentication without external solutions). The **Use external Digital Send Service Software…** option is for networks that include HP Digital Sending Service (DSS) Software, which is a workflow management solution. If you are using DSS, select the DSS option. This checklist does not cover configurations that involve DSS).
4. Click to require user authentication for Copy, Scan to Email, Scan to Fax, and Scan to Network Folder. This enables authentication for all use of the MFP (except for printing).
5. Click **Apply** at the bottom of the EWS page. If a confirmation page appears informing you of the success of the configuration, click **OK** or **Continue** to return to the EWS page.
6. Click **LDAP Authentication** in the menu to the left. The LDAP Authentication page (Figure 8) will appear.

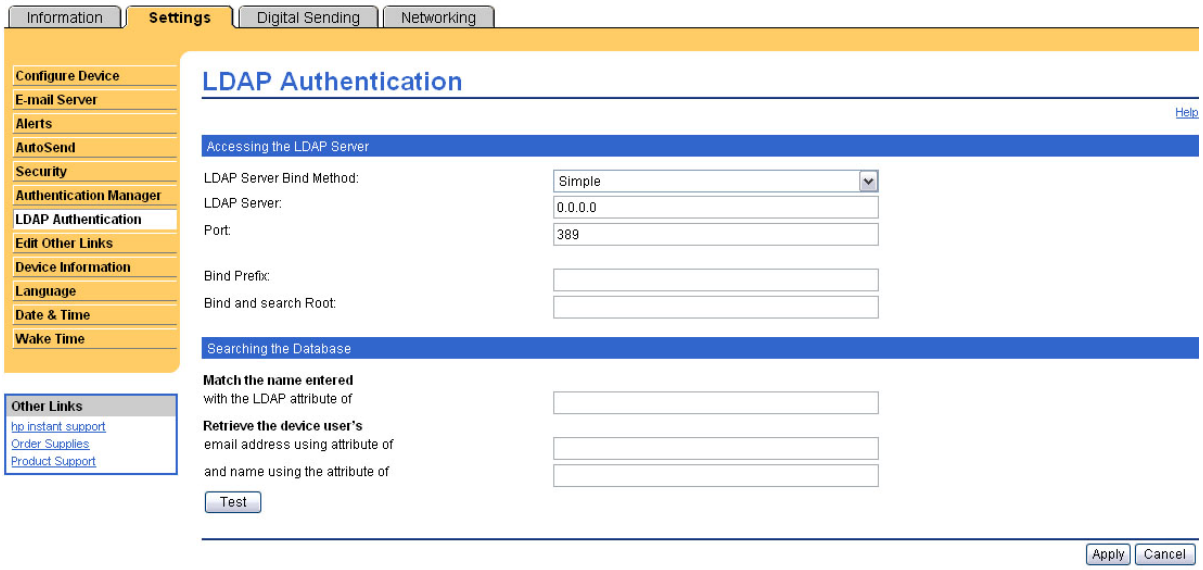

Figure 8: The EWS LDAP Authentication page.

7. Select an **LDAP Server Bind Method**. If your browser is capable of using Secure Socket Layer (SSL) (recommended), select **Simple over SSL**. Otherwise, communication between the MFP and the LDAP server is transferred in clear text. If your browser is capable of using SSL, and you choose the **Simple over SSL** option, go to the EWS Networking Tab (Figure 9) to install the certificate.

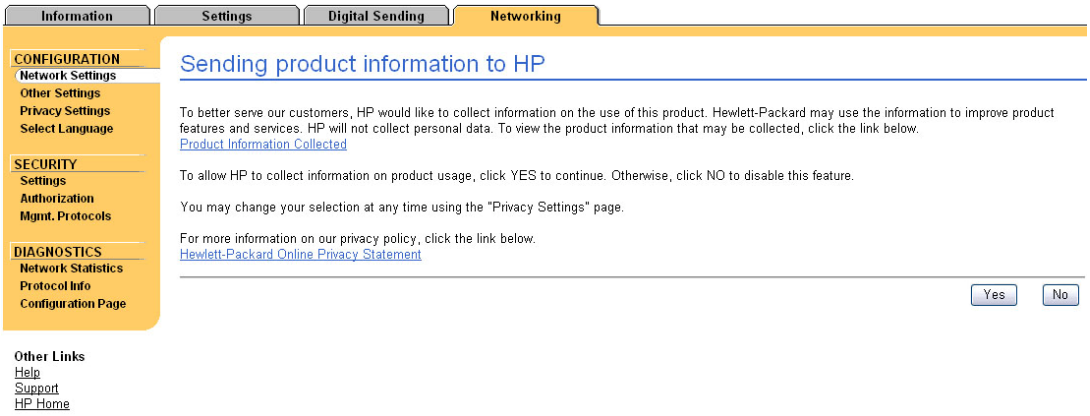

Figure 9: The EWS Networking Tab.

a. Click **Authorization** under the **Security** menu heading to the left. The **Authorization** page (Figure 10) will appear.

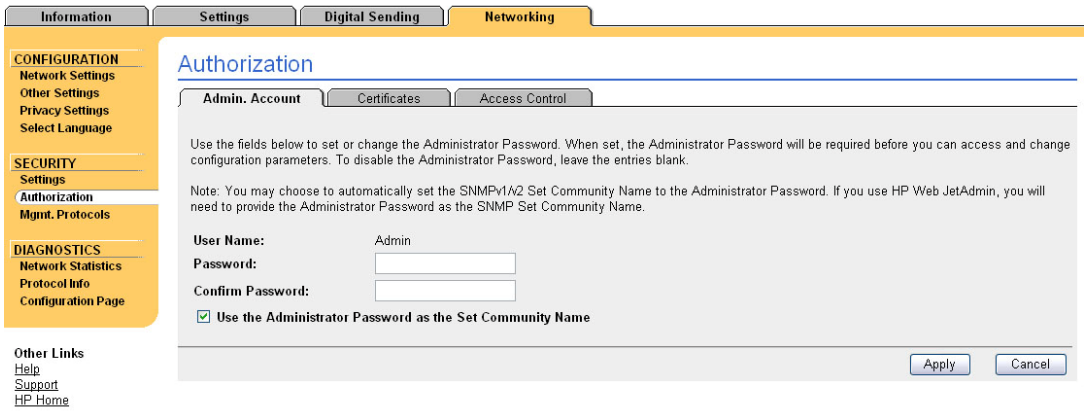

Figure 10: The Networking Authorization Page.

b. Click the **Certificates** tab in the gray area at the upper part of the **Networking** tab. The **Certificates** page (Figure 11) will appear.

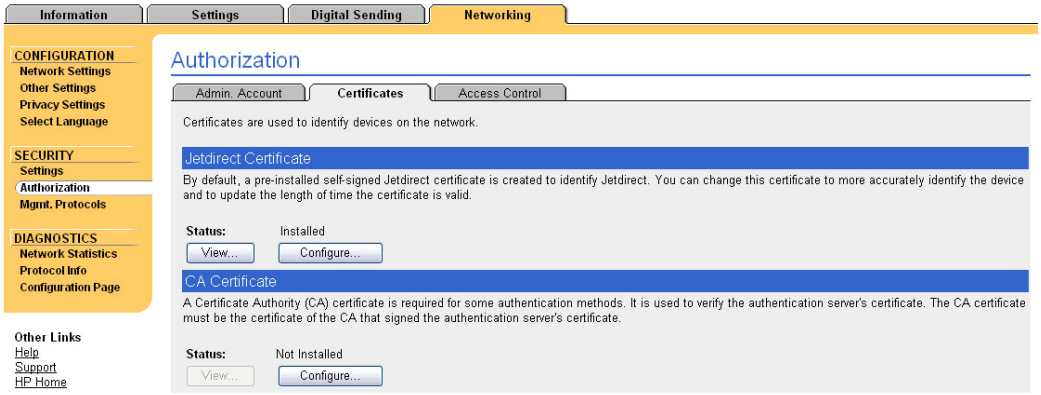

Figure 11: The Certificates page of the Networking Authorization tab.

c. Click **Configure** under **CA Certificate** at the bottom of the **Certificates** page. The **Certificates Options** page (Figure 12) will appear.

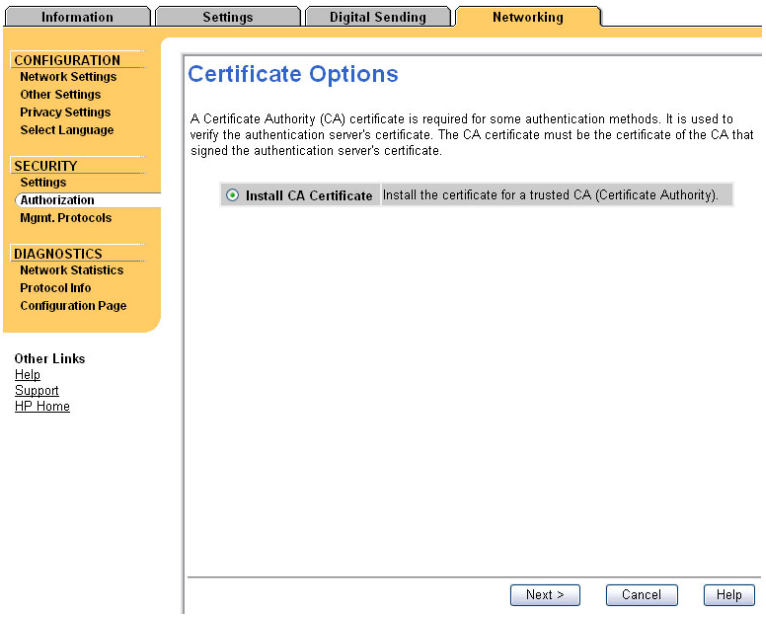

Figure 12: The Networking Certification Options page.

d. Click **Next**. The **Install CA Certificate** page (Figure 13) will appear.

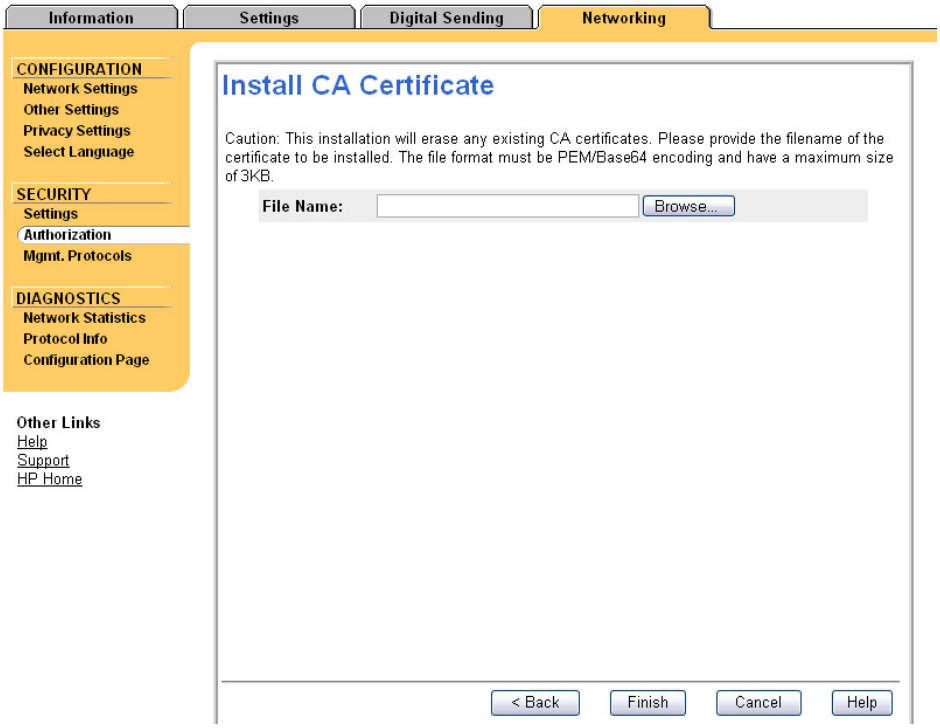

Figure 13: The Networking Install CA Certificate page.

e. Click **Browse**, and locate the certificate.

f. Click **Finish**. The EWS will confirm successful installation of the certificate.

8. Fill out the **LDAP Authentication** page (see Figure 8 above) according to your network configuration.

9. Click **Test** at the bottom of the **LDAP Authentication** page to ensure that the settings are correct.
10. Click **Apply** at the bottom of the EWS page. If a confirmation page appears informing you of the success of the configuration, click **OK** or **Continue** to return to the EWS page.

At this point, the MFP will require users to provide authorization credentials (according to the LDAP configuration) to use the MFP.

3.1.4 Send to Folder

The MFP can send scanned documents to network folders securely when the network and the EWS are configured as such. If you are using Send to Folder, you should configure network folders for limited access by authenticated users. The MFP can accommodate folder access requirements according to settings configured in the EWS:

1. Click the **Digital Sending** Tab on the EWS. The **Digital Sending General Settings** page (Figure 14) will appear.

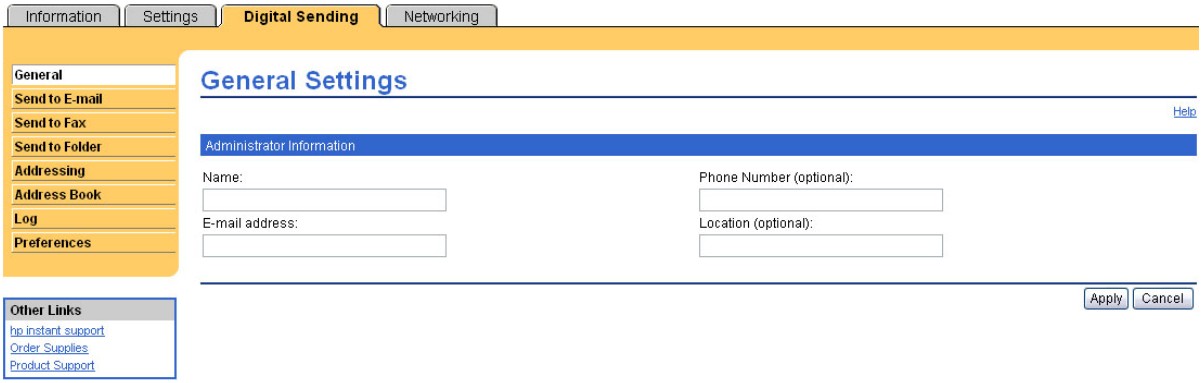

Figure 14: The Digital Sending General Settings page.

2. Click **Send to Folder**. The **Send to Folder** page (Figure 15) will appear.

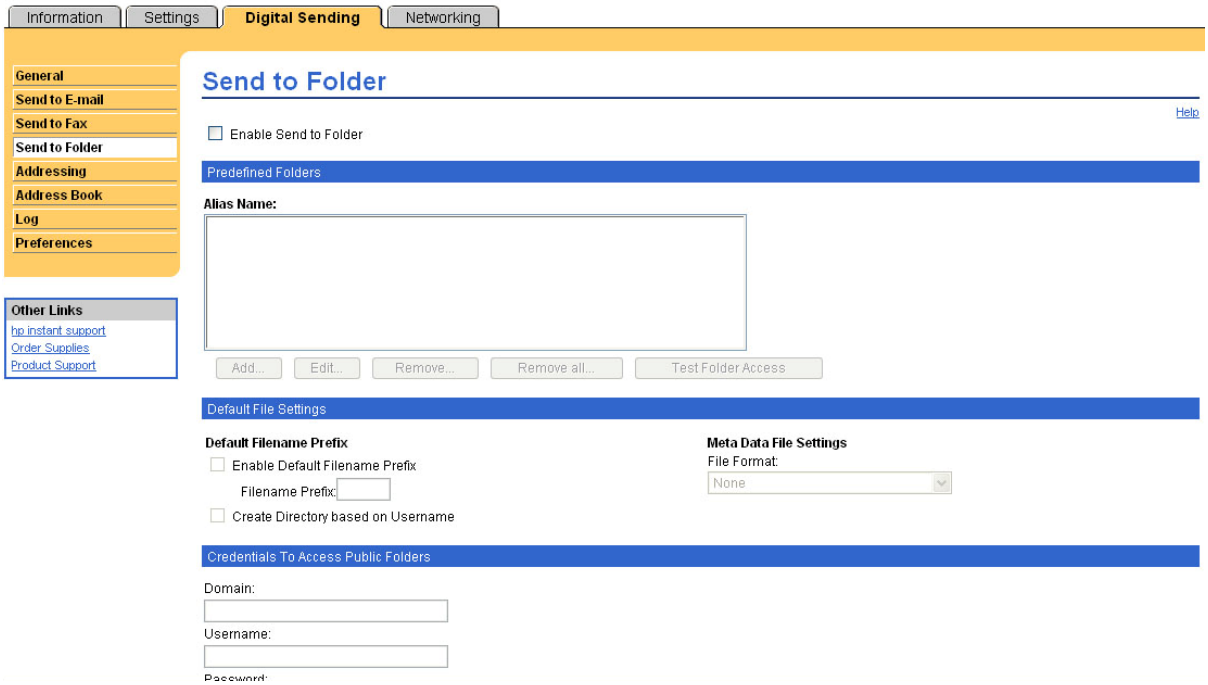

Figure 15: The EWS Send to Folder page.

3. Fill in the **Credentials to Access Public Folders** fields to match the configurations of the network folders.

The EWS Send to Folder menu also provides an **NTLM Authentication** option, which allows you to transmit network folder access credentials encrypted. This setting and its security depends on the configurations of the network and on the network folders to which the MFP is sending. HP recommends that you configure your network to allow for this option. Here are instructions for configuring this option for the MFP:

4. Scroll to the bottom of the **EWS Send to Folder** page (Figure 15, above) to view the **Send to Folder Network Settings** area.
5. Set the **NTLM Authentication** option to one of the encrypted options according to your network configuration.

   NOTE: The **Send to Folder** page contains other security options that you should have already configured above. See the Authorization Section above for these redundant EWS settings.
6. Click **Apply** at the bottom of the EWS page. If a confirmation page appears informing you of the success of the configuration, click **OK** or **Continue** to return to the EWS page.

3.1.5 Encryption Strength

Encryption Strength is another setting that appears only in the EWS. This setting prescribes the level of encryption for HTTPS (SSL) communications with the MFP. Here is how to set Encryption Strength:

1. Click the **Networking** tab (Figure 16) in the MFP EWS. The **Networking** page will appear.

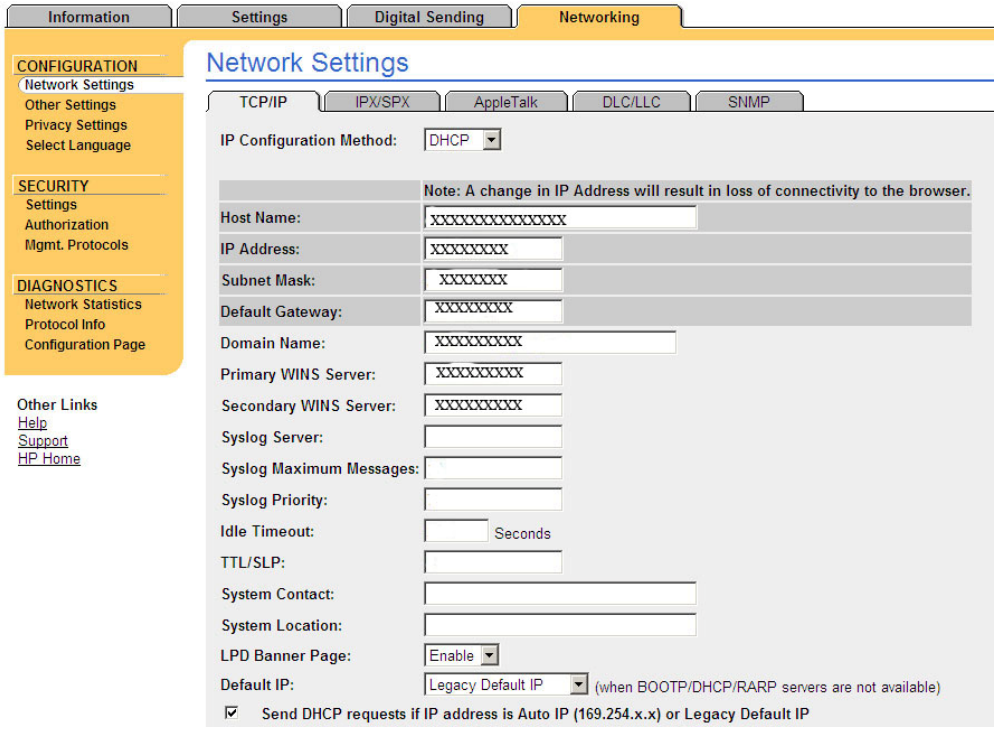

Figure 16: The EWS showing the Networking Tab page.

2. Click **Mgmnt. Protocols** under **Security** in the menu to the left. The **Mgmnt. Protocols** page (Figure 17) will appear.

Figure 17: The Mgmnt. Protocols page.

3. Set **Encryption Strength** to at least **Medium**. Click the dropdown menu next to **Encryption Strength**, and select the setting for medium.

   NOTE: All other settings on this page are covered in the Web Jetadmin section below.

4. Click **Apply** at the bottom of the EWS page. If a confirmation page appears informing you of the success of the configuration, click **OK** or **Continue** to return to the EWS page.

This sets the level of encryption for HTTPS configuration communication between the PC and the EWS. The medium setting provides for relatively fast communication with a reasonable level of encryption for most networks. If your network requires higher-level security for sensitive data, set **Encryption Strength** to **High**.

3.2 Settings in Web Jetadmin

This section explains how to make security settings using Web Jetadmin. The steps in this section follow the Web Jetadmin menus and dialogs in the order in which they are the most secure. This section covers only security-related configuration settings.

See the Setting List section later for a complete list of the recommended settings.

This section makes the following assumptions about the network and the administrator:

- Web Jetadmin is installed and working normally in a network environment. You can find Web Jetadmin for download and installation free at the following hp.com location:
  http://www.hp.com/go/webjetadmin
  Follow all instructions for download and installation at the website above, and configure Web Jetadmin to manage the MFPs.
- MFPs are installed and working normally on the network.
- Networks are configured with reasonable and standard security techniques.
- Administrators are familiar with industry-standard network management conventions.
- Administrators are familiar with Web Jetadmin, Jetdirect, and EWS.

CAUTION: This checklist covers a wide variety of configuration settings that can react with one another and with other components of your network. This checklist is tested in the environment explained in the Assumptions section above. However, your network may react differently. If the MFP or other components of your network show unexpected errors, hangs, or malfunctions, contact HP Customer Care. You can find HP Customer Care contact information by searching for it at hp.com.

Once Web Jetadmin is ready to manage the MFP, you can begin with the instructions below:

5. Open Web Jetadmin, and find the HP LaserJet 4345 MFP that you wish to configure. One easy way to find the MFP is to place the MFP IP address in the **Quick Device Find** field and click **Go**. A page for the device will appear (usually the device status page). The remaining steps in this checklist cover recommended security settings for a single MFP, but you can configure the settings on multiple MFPs.
6. Click the Categories dropdown menu at the top of the page (Figure 18), and click **Configuration**. This will open the configuration page (Figure 19, below).

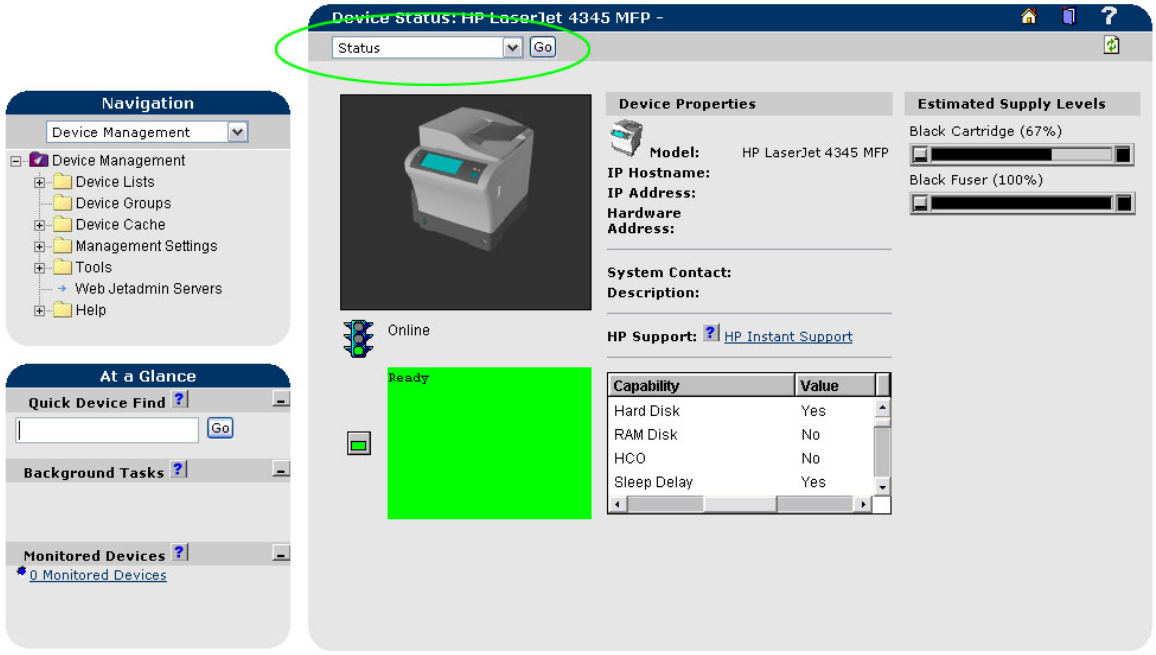

Figure 18: The default page for an HP LaserJet 4345 MFP showing the Categories dropdown menu circled in green.

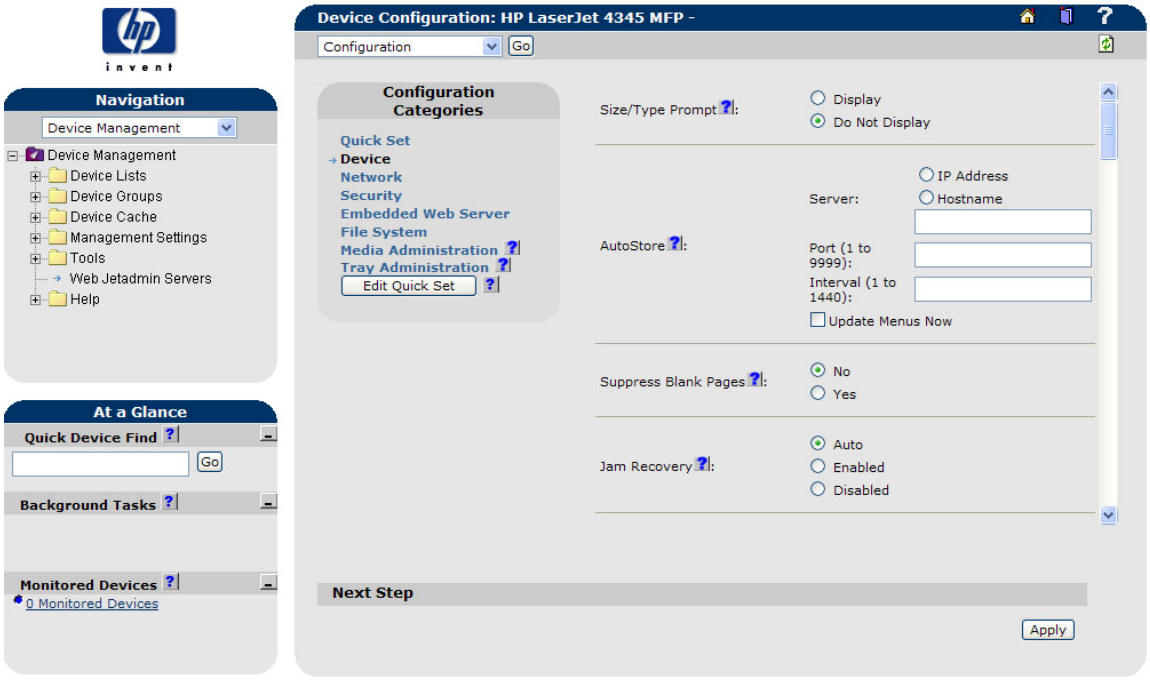

Figure 19: The Configuration Categories page showing the default Device Configuration page.

CAUTION: You must click Apply at the bottom of each configuration page before you move to the next configuration page. Otherwise, the settings you configure will not be applied to the MFP.

The next step is to set up SNMPv3 communication for configuration settings. Setting up SNMPv3 first provides secure communication while you are configuring the remaining

recommended settings. You should configure SNMPv3 by itself because it requires several steps that you should complete in the order explained below. This process requires you to create a username and two passwords and then to provide them in a dialog window to complete the configuration. Once the configuration is complete, the MFP will require these credentials every time a user attempts to make changes to configurations using Web Jetadmin (or any other SNMP tool).

7. Click **Security** in the **Configuration Categories** box (Figure 20). The **Security Configuration** page will appear (Figure 21).

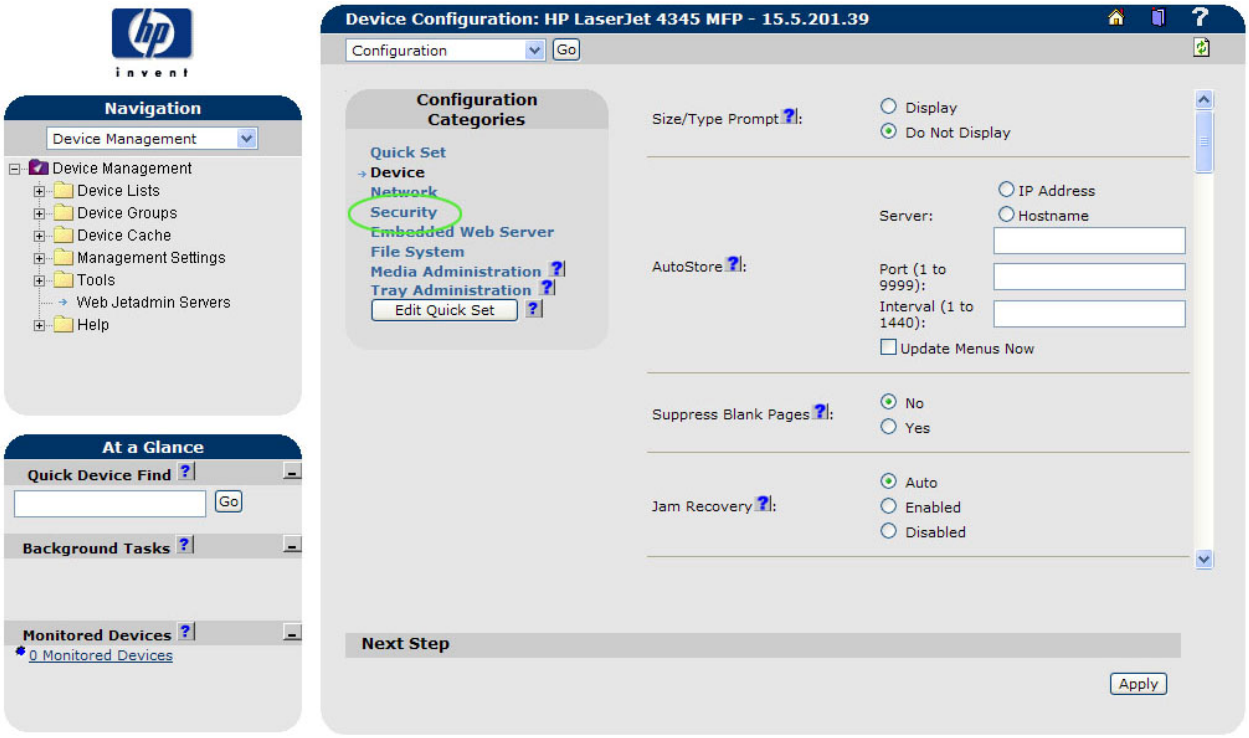

Figure 20: The Device Configuration page showing the Security Configuration Category circled in green.

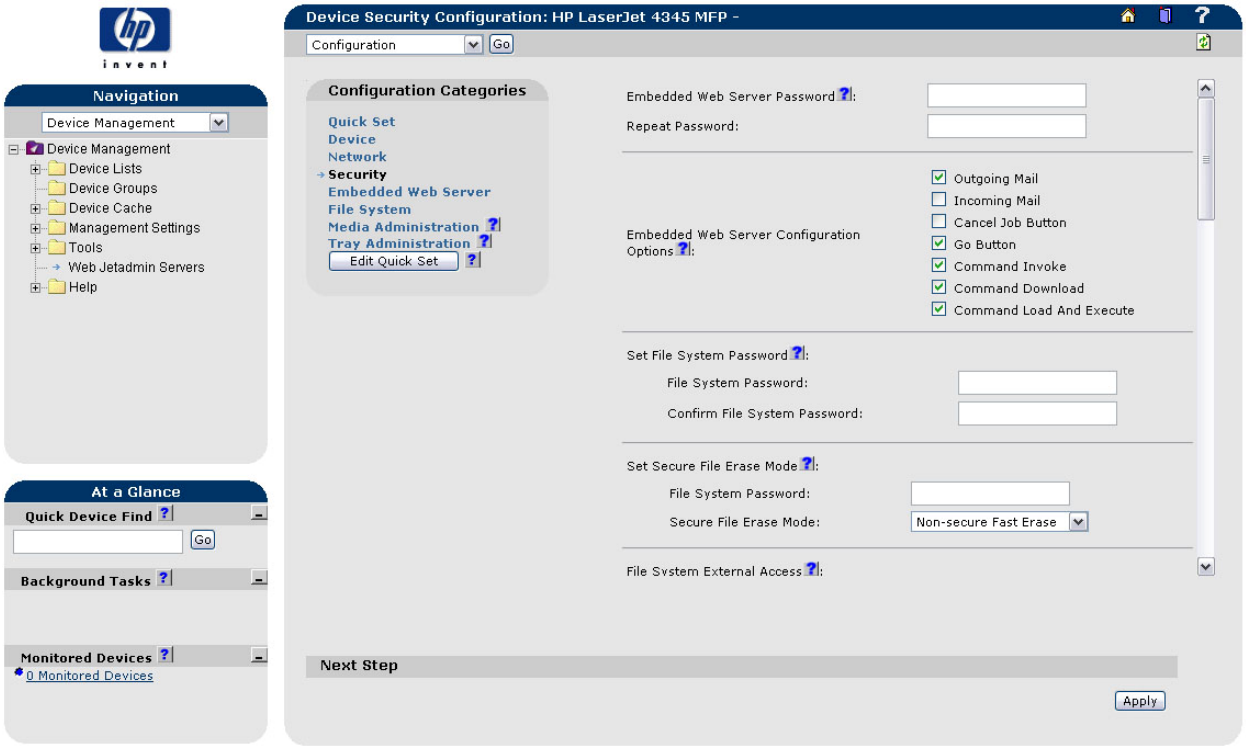

Figure 21: The Security Configuration page.

g. Scroll down to the **SNMPv3** setting, and enable it by clicking to select **Enabled**.

h. Click **Apply** at the bottom of the **Security Configuration** page. The **Device Information** page (Figure 22) will appear asking for SNMPv3 credentials.

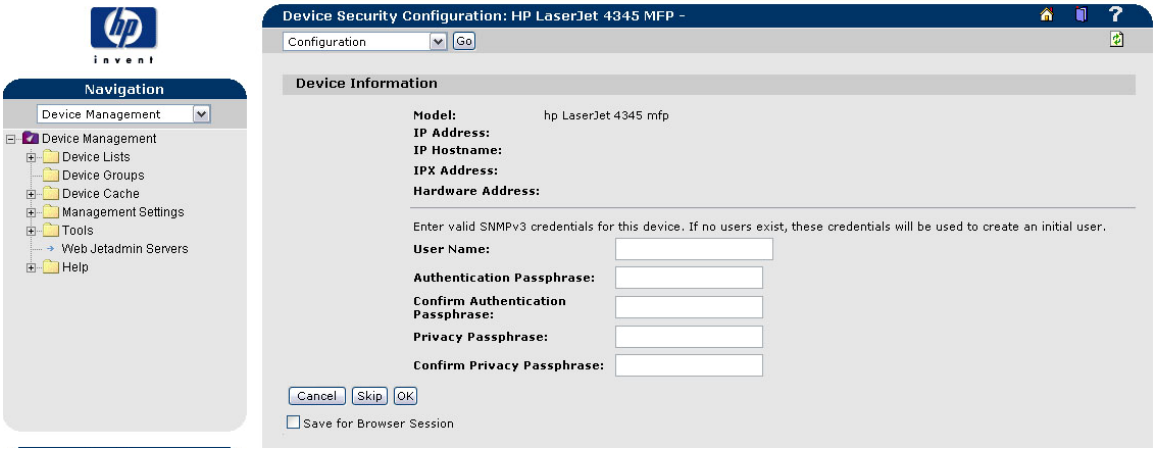

Figure 22: The Device Information page that appears for SNMPv3 user credentials.

NOTE: This page states, "If no users exist, these credentials will be used to create an initial user." This means that SNMPv3 has not been configured (It can also mean that SNMPv3 has been configured but disabled. In this case, you would have to provide the original credentials in order to re-enable SNMPv3. However, this checklist assumes that SNMPv3 has never been configured).

You are providing a new user name, a new passphrase, and a new privacy phrase here for the initial configuration of SNMPv3. Once you finish this configuration, the MFP will require these credentials whenever anyone attempts to change settings.

i. Type a name in the **User Name** field. This can be any name you choose.

j. Type a phrase in the **Authentication Passphrase** field. This can be any word or phrase that is at least 8 characters.

k. Retype the authentication passphrase exactly in the **Confirm Authentication Passphrase** field.

l. Type another phrase in the **Privacy Passphrase** field. This can be any word or phrase that is at least 8 characters.

CAUTION: **Be sure to remember these credentials and provide them to authorized users. If these credentials are forgotten, the only way to restore Web Jetadmin access to the MFP is to restore the MFP to factory default settings.**

NOTE: **The Device Information page has a Save for browser Session option. This option keeps the SNMPv3 credentials available as long as you keep Web Jetadmin open. If you use this setting, configuring the remainder of the settings in this checklist will be easier, but you may be risking the possibility of unauthorized users finding the credentials. HP recommends that you do not use this feature.**

m. Click **OK**. A **View Log** page (Figure 23) will appear confirming that the configuration was successful.

Figure 23: The View Log page that appears showing that the SNMPv3 configuration is successful.

Now, any time you click **Apply** to configure settings in Web Jetadmin (or in any other SNMP tool), the MFP will require the SNMPv3 credentials you created above.

At this point, you can continue configuring the recommended settings in the checklist. The remaining steps are in the order they would normally appear in the Web Jetadmin menus.

If Web Jetadmin is still showing the **View Log** page (Figure 23, above), click **Go Back** to view the **Security Configuration** page.

8. Click **Device** in the **Configuration Categories** box. The **Device Configuration** page (Figure 24) will appear.

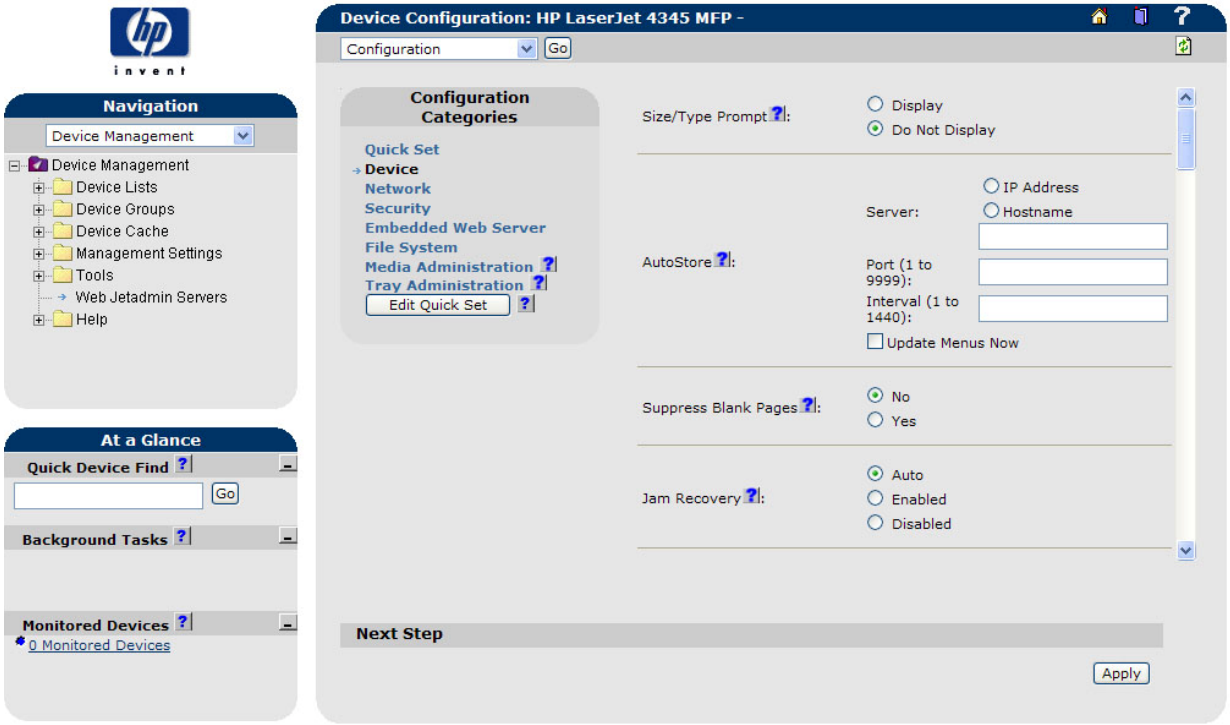

Figure 24: The Device Configuration page.

The **Device Configuration** page normally appears by default. It shows a few options for general behavior of the MFP.

Follow these instructions to configure the recommended settings on the **Device Configuration** page:

a. Enable **Job Retention** (already enabled by default). This allows users to use job retention options such as private job and hold job. Users will be able to ensure that they are present during printing to provide privacy for documents in the MFP output bins.

b. Enable **Job Hold Timeout** by selecting a reasonable timeout value for jobs held. Allow enough time for a user to walk to the MFP to print a job, or allow more time to allow jobs to print in line at the queue.

NOTE: **Job Hold Timeout does not apply to fax jobs (see settings for fax later in this section).**

c. Click **Apply** at the bottom of the **Device Configurations** page. The **Device Information** page will appear prompting for SNMPv3 credentials. These are the credentials you should have created earlier while setting up SNMPv3.

d. Fill in the credentials exactly as you created them, and click **OK**. The **View Log** page (see Figure 23, above) will appear showing the success of the configurations.

9. Click **Network** in the **Configuration Categories** menu in the top left corner of the Device Configuration page. The **Network** configuration page (Figure 25) will appear.

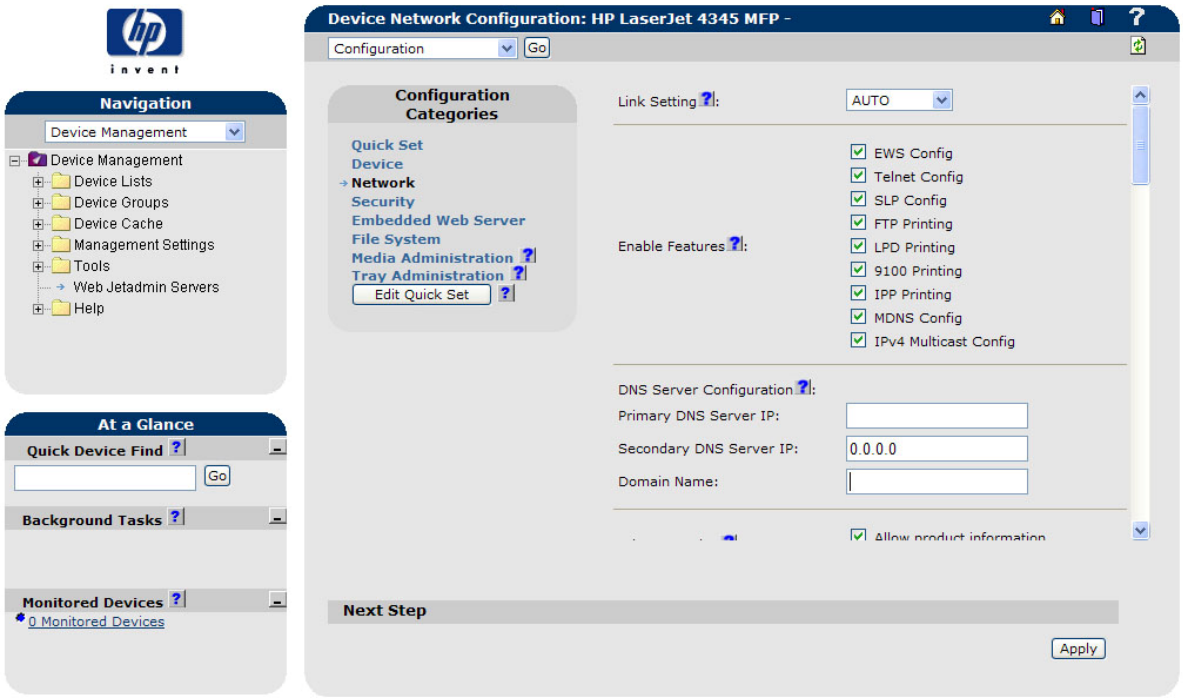

Figure 25: The Network Configuration page (actual page will show the network addresses).

Many of the security settings on the **Network Configuration** page are enabled by default but should be disabled if not in use. However, you should consider each recommended setting in terms of your network to avoid disabling functions that you may be using.

The next few steps explain recommended settings on the **Network Configuration** page. Scroll down on the page as you select the options.

a. Deselect (disable) all features on the features list (see Figure 25, above) except for **9100 Printing**.

   Disabling all but **9100 Printing** prevents users from accessing configuration settings and other features through the network, but it allows users to send and manipulate their own print jobs through 9100 printing. Remember that this recommendation is for common enterprise networks. Your network may use some of the configuration methods on the features list. If you choose to enable these methods, be sure to consider their security on the network. See the Ramifications section for more information on these features.

   NOTE: **Disabling EWS Config prevents all access to the EWS configuration settings including access to these settings through Web Jetadmin. This includes EWS configuration settings for email, send to folder, and fax. You should disable EWS Config, and enable it whenever you wish to make changes to these settings.**

b. Set the privacy option as desired. This setting allows HP to collect statistical data about the MFP. HP will not collect network-specific or personal data. For information on HP privacy policies, read the Hewlett-Packard Online Privacy Statement available by

clicking privacy statement at http://www.hp.com. If you enable this feature, information collected by HP will be limited to the following items:

- HP Jetdirect product number, firmware version, and manufacturing date
- Model number of the MFP
- Web browser and operating system detected
- Local language selections used for viewing Web pages
- Network communications protocols enabled
- Network management interfaces enabled
- Device discovery protocols enabled
- Printing protocols enabled
- TCP/IP configuration methods enabled
- SNMP control methods enabled
- Wireless configuration methods enabled

The MFP must have internet access to allow HP to collect information.

c. Deselect (disable) **RCFG Setting** unless the network includes Novell NetWare linkages for printer management.

NOTE: When you click Apply to disable RCFG Setting, a warning message will appear explaining that you are disabling access for Novell. When this warning appears, click OK to continue with the configuration.

d. Select (enable) **HTTPS Setting** to **Encrypt all web communication**. This setting requires that browsers use HTTPS to ensure secure communications. This setting is related to the SSL certificate and the **Simple Over SSL** settings covered in the EWS section, above.

e. Deselect all unused protocol stacks (as applicable to your network):

i. Deselect (disable) **IPX/SPX** unless your network includes Novell servers that interact with the MFP.
ii. Select (enable) **TCP/IP** (if it is not already selected). TCP/IP protocol enables normal network communication with the MFP.
iii. Select (enable) **DLC/LLC** (if it is not already selected). DLC/LLC protocol enables the MFP to communicate at basic levels on the network.
iv. Deselect (disable) **AppleTalk** unless the network includes Apple computers that interact with the MFP.

f. Click **Apply** at the bottom of the **Device Configuration** page once you are finished with the settings. The **Device Information** page will appear for SNMPv3 credentials (you should have created these credentials earlier in this checklist). Provide the credentials, and click **OK**. The **View Log** page will appear reporting the success of the configuration. Click **Go Back** to continue with this checklist.

10. Click **Security** in the **Configuration Categories** menu. This opens the **Security** configuration page (Figure 26).

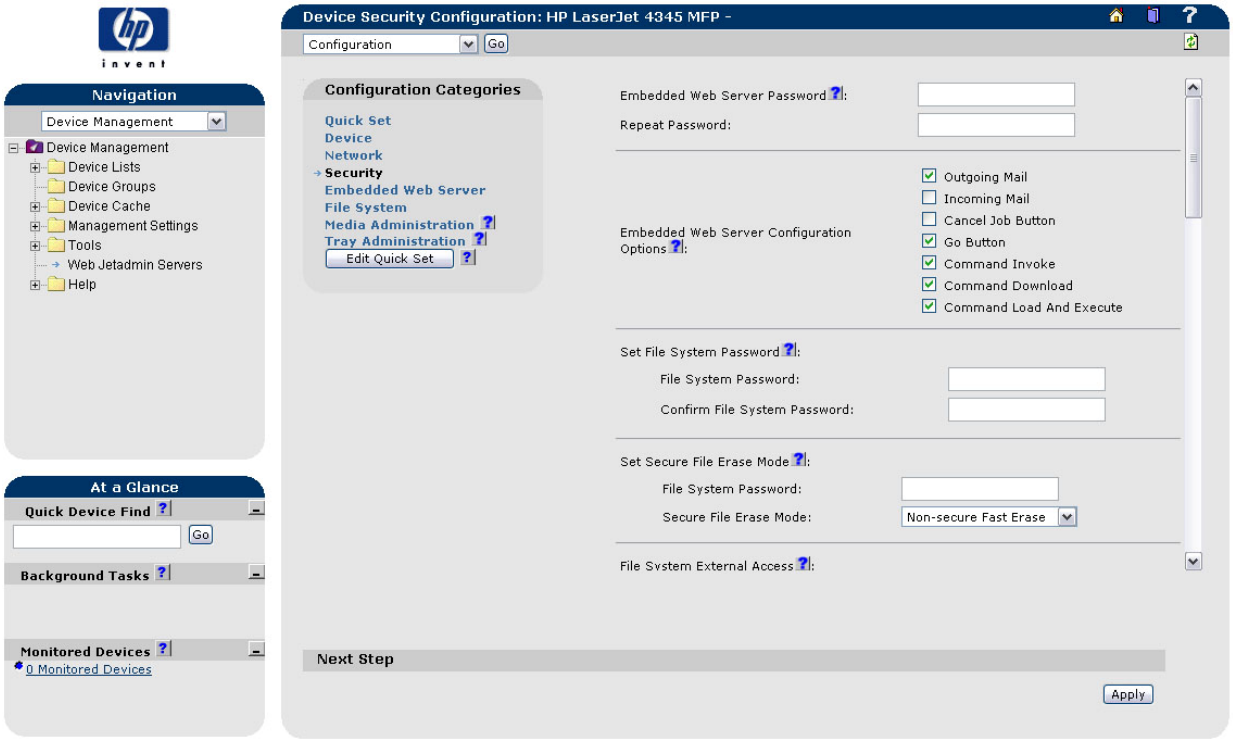

Figure 27: The Security Configuration page.

The **Security Configuration** page lists options that are specific to MFP security. The next few steps suggest and explain recommended settings that increase the level security for the MFP. Scroll down on the Security Configuration page as you select the options:

a. Select **Embedded Web Server Configuration Options**. These options determine which EWS configuration settings are available to users. Select the options as follows:

- Enable **Outgoing Mail**. The outgoing mail feature allows the MFP to send alerts and AutoSend messages. Disable it if you do not wish to use these features.
- Disable **Incoming Mail**. Enable this feature only if you have installed a solution that requires it.
- Disable **Cancel Job Button**. This setting removes the Cancel Job button from the EWS. Disabling it removes the capability of remotely canceling jobs sent by other users.
- Disable **Go Button**. This ensures that a remote user is unable to interfere with some conditions on the MFP. The Go Button is called Pause/Resume in the EWS.
- Disable **Command Invoke**. This function is not applicable to the MFP. Disabling it is a best practice to ensure control over access to the MFP.
- Disable **Command Download**. This function is not applicable to the MFP. Disabling it is a best practice to ensure control over access to the MFP.
- Disable **Command Load and Execute**. This function allows Chai services such as workflow applications and job accounting applications to be installed and run on the MFP. If your network uses such applications, be sure to enable **Command Load and Execute**, otherwise, disable it to ensure that no one can install programs on the MFP.

b. Set the **File System Password**. Type a password in the **File System Password** field and repeat it exactly in the **Confirm File System Password** field. This setting requires all

users to log in to configure the file system. This includes access to disc erase features and other features that affect information on the hard drive.

NOTE: **With this password and SNMPv3 configured, the MFP will require it along with SNMPv3 credentials and any other applicable passwords. You may see the Device Information page several times for some configurations.**

CAUTION: **Remember this password, and provide it to authorized users. If this password is forgotten, the only way to restore access to configure the file system features is to reset the MFP to factory default settings.**

c. Set the **Secure File Erase Mode** to **Secure Fast Erase**. Type the correct password in the File System Password field (as configured in the previous step), click the dropdown menu, and select **Secure Fast Erase**. **Secure Fast Erase** will appear in the **Secure File Erase** field. This setting determines the level of overwriting applied as files are deleted during routine functions.

The **Secure Fast Erase** option deletes files by overwriting them with one pass. It can slow down performance slightly, but it provides a reasonable level of file security.

Use the **Secure Sanitizing Erase** option to meet stringent security requirements such as Department of Defense standards. The **Secure Sanitize Erase** option overwrites files with three passes. It also takes significantly more time and can noticeably slow down performance of the MFP.

d. Disable **PJL**, **PML**, and **NFS** in the **File System External Access** section if your network is not using them. Type the File System password as configured above, and click to select **Disabled**, for each one. Disabling file access through these protocols prevents anyone from using them to access the hard drive. Disabling the NFS option disables the entire protocol. If your network includes tools, such as disk management applications, that interact with the MFP, you should enable the appropriate protocols – otherwise, disable them.

e. Enable the **PostScript** protocol in the **File System External Access** section. Click to select **Enabled** next to it. If you disable PostScript protocol, some types of print jobs will not work properly.

f. Set the **Device Password**. This password should be already set if you are following the checklist in order. When you set the EWS password in the first step of the EWS Settings section, the MFP synchronized it with the Device password. Thus, you should be able to use the EWS password for this feature. If it is not set for some reason, type a password in the **Set Device Password** field, and type it again exactly in the **Repeat Password** field. This password requires all users to login before remotely changing configuration settings. This password is required for all access to the MFP via Web Jetadmin, the MFP EWS, or any other management software.

NOTE: **If you reset the Device Password, the EWS password will also be reset to be the same as the Device Password.**

NOTE: With this password and SNMPv3 configured, the MFP will require it along with SNMPv3 credentials and any other applicable passwords. You may see the Device Information page several times for some configurations.

CAUTION: Remember this password, and provide it to authorized users. If this password is forgotten, the only way to restore remote access to MFP configuration settings is to reset the MFP to factory default settings.

g. Lock **Control Panel Access**. Click to select one of the lock options in the **Control Panel Access** menu. HP recommends selecting at least **Moderate Lock** to ensure that no one can access configuration settings in the control panel.

NOTE: This setting prevents everyone from accessing configuration settings in the control panel, including digital send and fax settings. If you have made the recommended settings up to this point, no one will have access to control panel configuration settings for the MFP unless an authorized administrator unlocks access via Web Jetadmin. If you wish to make changes to configuration settings in the control panel, unlock access in Web Jetadmin, make the changes, and then lock access again.

h. Click **Apply** at the bottom of the **Security Configuration** page once you are finished with the settings. The **Device Information** page will appear for SNMPv3 credentials (you should have created these credentials in the first step of this checklist). Provide the credentials, and click **OK**. The **View Log** page will appear reporting the success of the configuration. Click **Go Back** to continue with this checklist.

Other pages in the **Configuration Categories** menu include security-related settings. Many of them are redundant for your convenience, and they are already covered above. The next few steps cover security settings that are not covered so far:

NOTE: The steps below cover only settings recommended for security in an enterprise network environment. You may wish to make other settings during this process, but they are not covered in this checklist.

11. Click **Secure Storage Erase** in the dropdown menu (Figure 29) at the top of the Web Jetadmin device page.

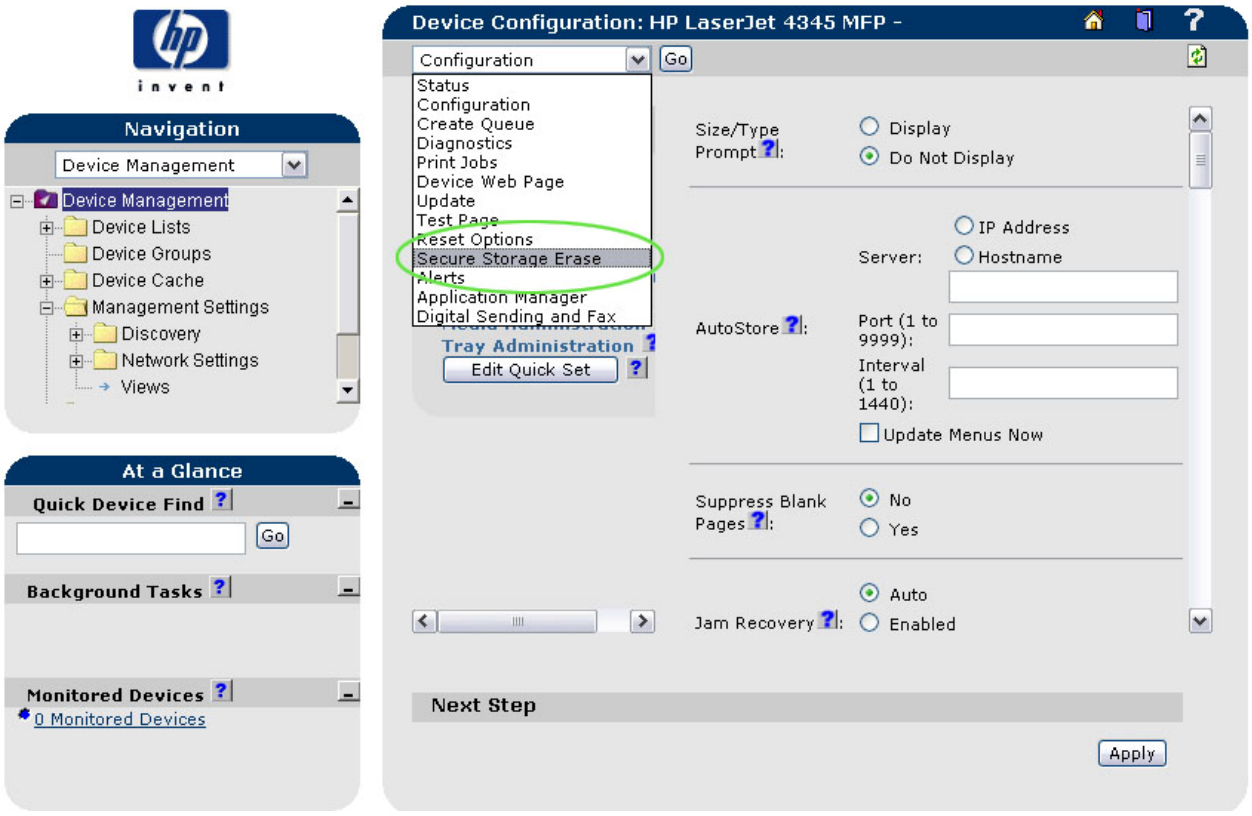

Figure 29: The Device Configuration page showing the Secure Storage Erase menu item circled in green.

The **Secure Storage Erase** page (Figure 30) will appear.

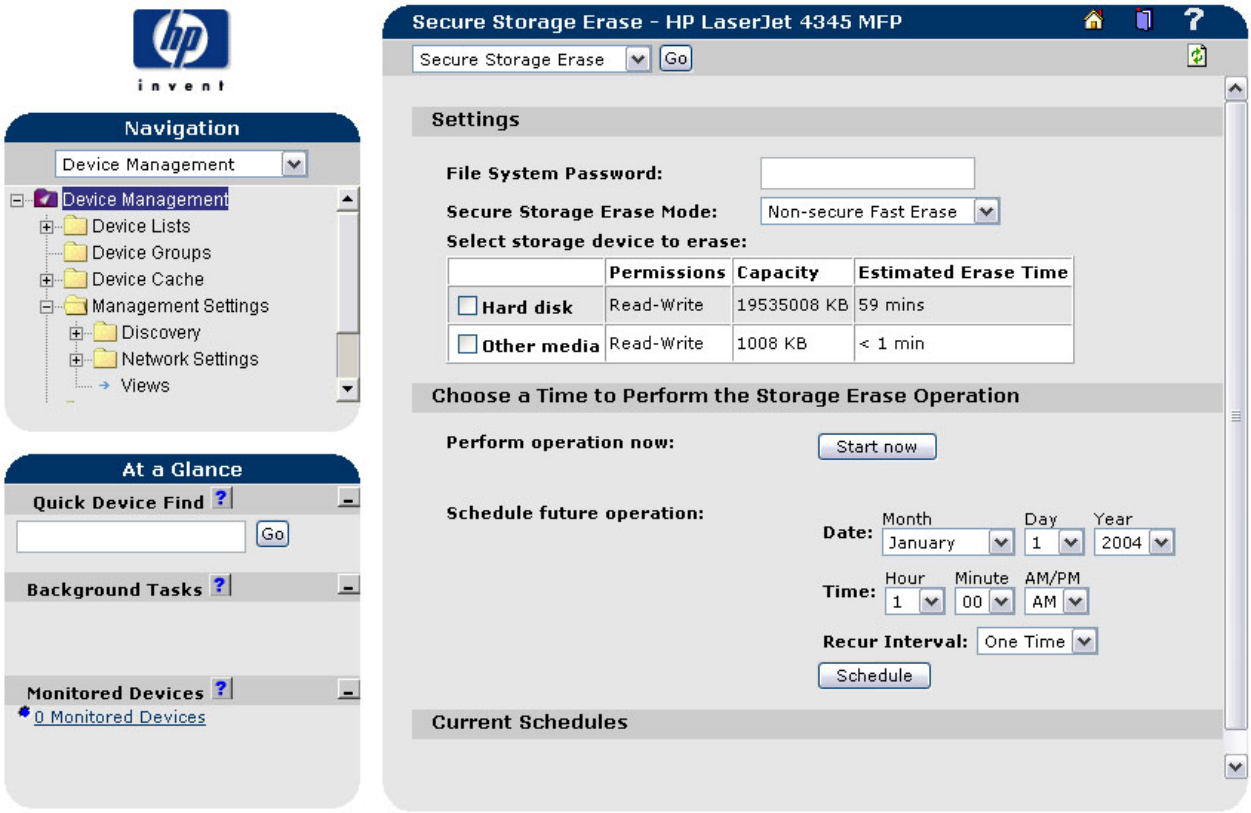

Figure 30: The Secure Storage Erase page.

The **Secure Storage Erase** page provides options for erasing all stored files on demand or as scheduled. Keep in mind that this feature erases everything permanently from storage. This includes stored jobs, downloaded fonts, and logs.

a. Type the File System Password (as configured in steps above) in the **File System Password** field to enable the settings on the page.

b. Select **Secure (Fast) Erase** or **Secure Sanitizing Erase** in the **Secure Storage Erase Mode** dropdown menu. You may have selected the secure storage erase mode in steps above, but this page allows you to erase the entire contents of storage on demand. You can also schedule this operation on this page. You may wish to use **Secure Sanitizing Erase** for this operation and reset the secure erase mode to **Secure Fast Erase** when finished. This will allow you to use the higher security mode periodically, but use the faster erase mode for better performance while the MFP is operating normally.

c. Click to select the storage devices you wish to erase. This feature can erase the hard drive or the Compact Flash (this feature erases Partition 2 of the Compact Flash card. It does not erase the vital system data that resides on Partition 1, which is not accessible to these settings).

d. Click **Start now** if you wish to erase storage now.

e. Select options for scheduling if you wish to erase storage on a regular schedule.

12. Click **Digital Send and Fax** in the dropdown menu at the top of the configuration page (Figure 31).

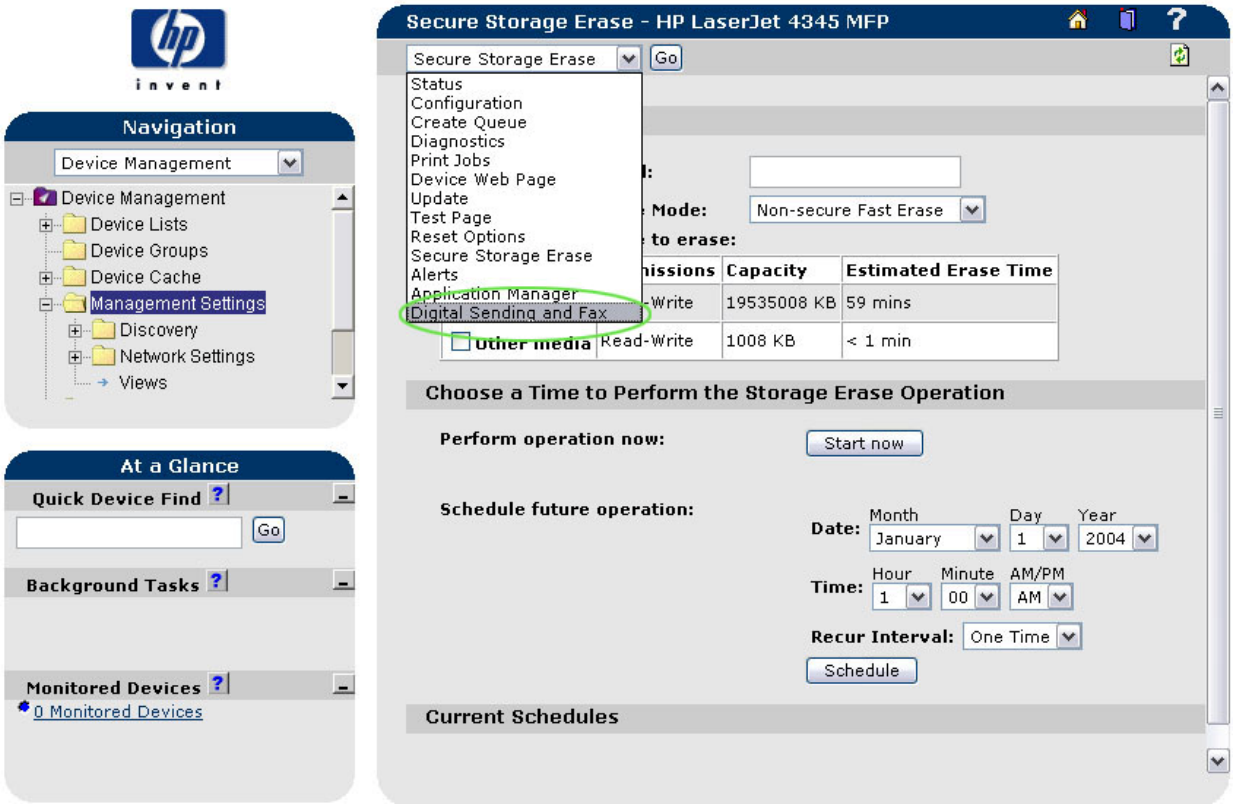

Figure 31: The Configuration page showing the Digital Send and Fax option circled in green.

The **Digital Sending and Fax** configuration page (Figure 32) will appear.

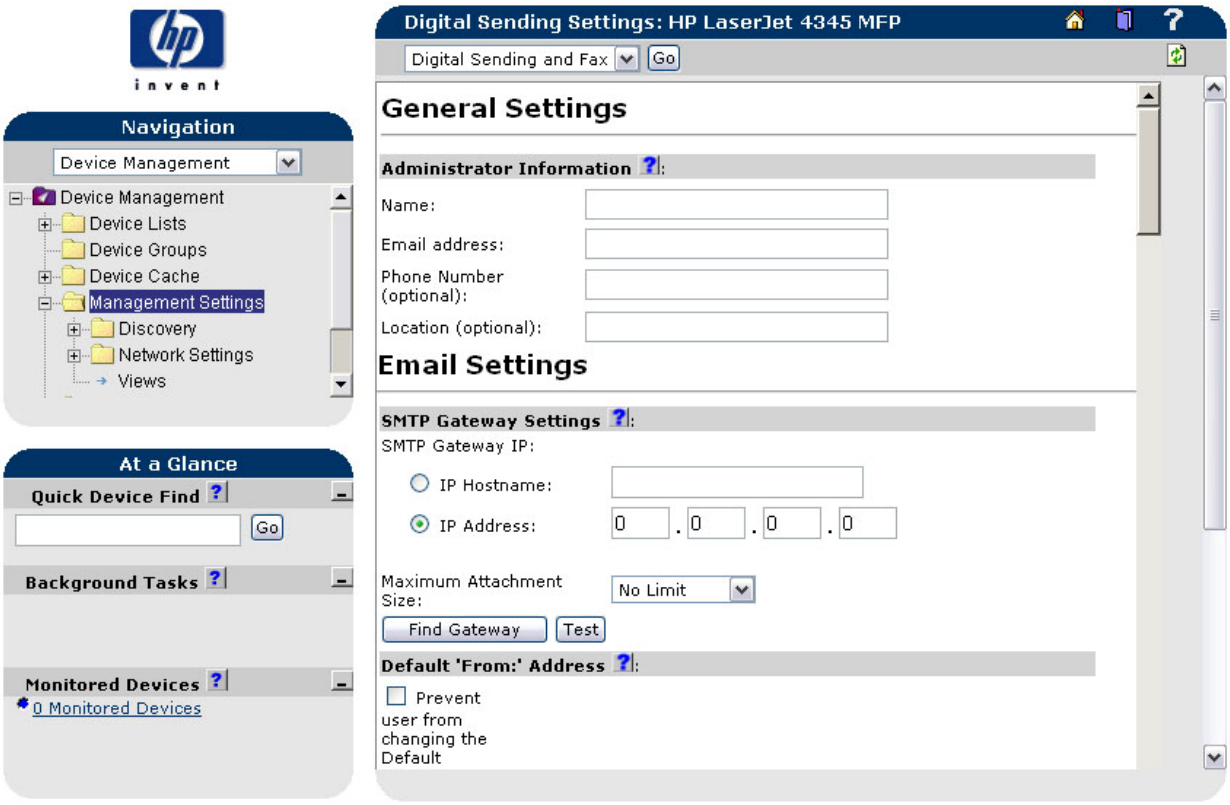

Figure 32: The Digital Send and Fax page.

The **Digital Send and Fax** page provides options for built-in email and fax capabilities. Many of these settings affect security. The next few steps cover settings on this page. Scroll down as you make the selections.

13. Fill in the **Default From Address**, and select **Prevent users from changing the Default From Address**. This ensures that users are unable to send email with incorrect or inappropriate from addresses. Keep in mind some properties of the default from address as you consider what to have in this field:

    - The email sent from the MFP will show the default from address regardless of who sends it.
    - Some networks allow email sent only with a valid from address. This may mean that the from address must be formatted correctly, but not necessarily that it is an actual email address. You may wish to have a description of the MFP in a properly-formatted address. Example: 4345.MFP.in.hallway@popserver.com.
    - You may wish to use an actual email address if you wish to receive replies to messages sent from the MFP. The MFP will not receive email, but you can configure a from address that leads to an email account that is monitored elsewhere.

    Note: **You may also consider setting up the MFP for authentication, which is configured only in the Embedded Web Server (see the EWS section above). The MFP Authentication feature requires users to login using a user name and password (depending on LDAP or address book configurations). With the email option included in the authentication**

configuration, the MFP will place the user's email address in the From field, and it will not allow the user to change it.

14. Set the PIN number under **Establish PIN Number** in the **Special Features** section. This feature requires users to have the PIN number for fax printing, fax forwarding, and fax blocking.
15. Click **Apply** at the bottom of the **Digital Send and Fax** page once you are finished with the settings. The **Device Information** page will appear for SNMPv3 credentials (you should have created these credentials in the first step of this checklist). Once the MFP has authenticated the SNMPv3 credentials, the **Device Information** page will reappear for other applicable passwords (that should be configured in steps above). Provide the credentials required each time the **Device Information** page appears, and click **OK**. The **View Log** page will appear reporting the success of the configuration.

3.2.1 Using Web Jetadmin and MFP Passwords

Web Jetadmin is a powerful tool that allows you to manage any number of MFPs and printers. It provides a wide variety of features and services on the network. Without proper security, Web Jetadmin can enable malicious users the same conveniences for attacking your network. Thus, setting Web Jetadmin and MFP passwords and updating them is important to network security. This involves a large number of passwords that limit access to important areas of the MFP. When you make changes to configurations of the MFP, the MFP will require all applicable passwords. Thus, you may see several prompts for passwords when applying one or more changes to settings.

Losing passwords can eliminate access to the MFP. The only way to restore access to many of these areas without the password is to restore the MFP to factory default setting and completely reconfigure it. You may wish to use a password vault program to organize and store all of the passwords. Here is a list of the passwords you should set:

- EWS Password
- Web Jetadmin password
- SNMPv3 credentials
- Device password
- File system password

Use good practices for setting and updating passwords:

- Use alpha and numeric characters.
- Use passwords with at least six digits.
- Avoid using the same password for more than one setting (however, some passwords are synchronized in the MFP).
- Avoid using a pattern for passwords.
- Change the passwords often.

4 Settings List

This section is a complete list of the settings recommended in this checklist. This section does not include explanations of the settings or the implications of them on the MFP and on the network. Use this section as a reference to check off each setting to help ensure that you configure all of the recommended settings. See the Network Security section (above) and the Ramifications section (below) for information on each setting.

This section lists recommended settings for reasonable security on the most common networks that include HP LaserJet 4345 MFPs. Networks configured according to this list are considered reasonably secure, but HP does not warrant or guarantee that this configuration prevents or limits networks from malicious attacks.

CAUTION: Remember that these settings are recommended for the most common types of networks that do not include management tools other than Web Jetadmin. Your network likely requires some configurations that are not recommended in this section. Consider each setting for your unique network.

4.1 EWS Settings

- ☐ Set the **Embedded Web Server Password**.
- ☐ Configure the Access Control List.
- ☐ Disable **Allow Web Server (HTTP) access**.
- ☐ Configure Authentication.
- ☐ Configure secure options on Send to Folder.
- ☐ Set Encryption Strength to at least medium.

4.2 Web Jetadmin Settings

- ☐ Enable **SNMPv3** (Security page).

4.2.1 Device Page Settings

- ☐ Set the **Device Password**.
- ☐ Enable **Job Retention**.
- ☐ Enable **Job Hold Timeout**.
- ☐ Select a timeout value for jobs held.

4.2.2 Networking Page Options

- ☐ Disable all features on the features list except for **9100 Printing**.
- ☐ Set the privacy setting as desired.
- ☐ Disable **RCFG Setting**.
- ☐ Enable **HTTPS**.

4.2.3 Protocol Stacks (Networking Page)

- ☐ Disable **IPX/SPX** protocol stack.
- ☐ Enable **TCP/IP** protocol stack.
- ☐ Enable **DLC/LLC** protocol stack.
- ☐ Disable **AppleTalk** protocol stack.

4.2.4 Security Page Options

- ☐ Enable **Outgoing Mail**.
- ☐ Disable **Incoming Mail**.
- ☐ Disable **Cancel Job Button**.
- ☐ Disable **Go Button**.
- ☐ Disable **Command Invoke**.
- ☐ Disable **Command Download**.
- ☐ Disable **Command Load and Execute**.
- ☐ Set the **File System password**.
- ☐ Set the **Secure File Erase Mode** to **Secure Fast Erase**.
- ☐ Disable **PJL**, **PML**, and **NFS** protocols in File System External Access.
- ☐ Enable the **PostScript** protocol in the **File System External Access**.
- ☐ Set **Control Panel Access Lock** to **Moderate Lock**.

4.2.5 Secure Erase Options

- ☐ Set **Secure File Erase** to **Secure (Fast) Erase**.
- ☐ Use **Secure Storage Erase** often, and configure options for scheduling.

4.2.6 Digital Sending and Fax Options

- ☐ Fill in the **Default From Address**, and select **Prevent users from changing the Default From Address**.
- ☐ Configure the PIN number for fax printing, on demand fax printing, fax forwarding, and fax blocking.

5 Ramifications

Raising the level of security on a system usually requires giving up some conveniences and usability. This section explains some of the compromises that can occur from using the settings and configurations recommended in this checklist. However, keep in mind that this is not a comprehensive list. You should test your system to know how it reacts to these settings and configurations. You should also note the order of the settings recommended in the instructions. Your network may require some changes to the order in which these settings are configured to complete the checklist.

The following explains some of the known ramifications of each recommended setting:

5.1 EWS settings

- Set the **Embedded Web Server Password**. The EWS password is added security for configuration settings. With it configured, the MFP prompts for the password whenever a user attempts to access certain configuration settings. This is true even when SNMPv3 is enabled. The MFP will prompt for the SNMPv3 credentials and for the EWS password. It will also prompt for other passwords such as the device password if they are configured. Thus, you may see several prompts for authorization credentials when you click Apply to change settings in Web Jetadmin.
- Fill in the **Access Control List**. The Access Control List is a table that lists the IP addresses of PCs that are allowed to send configuration data to the MFP. This can be helpful toward a highly secure configuration; however, if the Access Control List is filled in at all, it limits all configuration communication with the MFP to the IP addresses (or subnets) in the list. Thus if the IP address of a PC is not in the Access Control List, the PC will not be able to configure the MFP.

  CAUTION: If the Access Control List is filled out incorrectly, it can cause complete loss of communication with the MFP. Thus, make sure to fill in all fields with the correct information. It is possible to restore communication with the MFP by resetting the MFP to factory default settings, which it takes more time and effort to start over configuring the MFP.
- Disable **Allow Web Server (HTTP) access**. This adds more assurance that unauthorized users will be prevented from using web browsers to access configuration settings on the MFP. You already should have enabled HTTPS, which requires secure communication, and you should have limited access to only authorized users by filling in the Access Control List and by setting EWS and device passwords. This setting also adds more assurance that the MFP will not allow IPP Printing (see an explanation of IPP Printing later in this section).
- Configure Authentication. Authentication provides two benefits to improve security: it requires users to log on using usernames and passwords for use of the MFP, and it places the user's email address in the From address of email messages. It also does not permit users to change the From addresses. The Authentication feature overrides other settings for the default From address. Authentication requires an LDAP server accessible on the network. This feature supports no other address servers.
- Set Encryption Strength to at least medium. The encryption strength setting covers only communication between a PC and the Embedded Web Server. When HTTPS is configured (as recommended in this checklist), communication with the Embedded Web Server is encrypted according to the Encryption Strength setting. With HTTPS enabled, the browser used to configure the MFP must accommodate HTTPS.

5.2 Web Jetadmin Settings

- Enable **SNMPv3** (Security Page). SNMPv3 is a secure protocol that encrypts information over network lines. Web Jetadmin accesses many of the MFP configuration settings through

the MFP SNMP port.

Setting up SNMPv3 can be tricky. Be sure to follow the instructions exactly. If the SMNPv3 setup process fails, try it again. If failure continues, power cycle the MFP, and try it again.

Once SNMPv3 is configured, the MFP will prompt for the credentials every time anyone tries to configure settings using Web Jetadmin or any other tool. Thus, an MFP configured according to this checklist may prompt several times for various passwords and credentials to make certain configuration changes.

If you enter the SNMPv3 credentials incorrectly while attempting to make a configuration change, the SNMPv3 credentials window will refresh with blank fields. It does not alert you that the credentials you provided are incorrect.

5.2.1 Device Page Settings

- Set the **Device Password**. The device password helps to prevent unauthorized users from using management software such as Web Jetadmin to change configurations on the MFP. The MFP will not allow network access to configuration settings without the password. Web Jetadmin will always prompt for this password before accessing the configuration settings, but other management software may not. The MFP will not allow them access without it.

  The MFP will require the device password even if SNMPv3 is enabled and configured. When you make configuration changes an MFP with this configuration, the MFP will require SNMPv3 credentials and the device password in separate steps.

- Enable **Job Retention**. Job Retention is a feature of the MFP that saves fax or print jobs on the hard drive for printing at the convenience of the user. The security implication is that a user can be sure to be present at the time of printing. Thus, the user can be sure that others do not have access to the printed documents. Security for Job Retention in printing requires that the user configure a PIN number at the time of sending the print job. The MFP will require the PIN number at the control panel before it will print the job. Security for Job Retention in fax printing requires that the fax PIN number is configured using Web Jetadmin (see the Network Security section).

  Job Retention security also requires that access to the MFP hard drive is limited to authorized users. You should disable access to the hard drive and enable secure file erase as recommended in the Network Security section to ensure that stored jobs are kept from unauthorized users.

- Enable **Job Hold Timeout**. Job Hold Timeout is enabled when you select a timeout value for jobs held. Job Hold Timeout is related to Job Retention. Job Hold Timeout is a limit on the time a job is held for printing on the hard drive. Once the Job Hold Timeout expires, the MFP erases the job on the hard drive. The MFP will use the **Secure File Erase** mode to erase the file securely. Job Hold Timeout is meant to ensure that files are not left on the hard drive long enough to allow unauthorized access. The ramification of using the Job Hold Timeout is that jobs removed after the timeout expires are gone permanently.

5.2.2 Networking Page Options

- Disable all features on the features list except for **9100 Printing**. The features list provides options to enable or disable various supported features for the MFP. These features are designed for access and convenience on the network, but they should be disabled when not in use (sometimes only for best-practice control of the networking capabilities). The following list explains the ramifications of each feature supported for the MFP:
  - **EWS Config** – EWS Config enables access to configuration settings via the MFP Embedded Web Server. The Embedded Web Server is the main access point to configuration settings for an MFP out of the box. Without Web Jetadmin, it is the only access point available for many important configuration settings such as email and fax settings. Thus, you should disable EWS Config only after you have configured settings in the Embedded Web Server. If you wish to change these settings, enable EWS Config using Web Jetadmin, make the changes, and disable EWS Config again.
  - **Telnet Config** – Telnet Config is an access point for some older (legacy) printer management tools. It is also an access point to make configurations in Jetdirect using ordinary Telnet commands (if the user knows which commands are compatible). Thus, unless your network uses legacy printer management software, you should disable Telnet Config. Enabling Telnet Config also transmits data across network lines in clear text. HP recommends using only Web Jetadmin to manage all network peripherals to ensure that you can make the configurations securely.
  - **SLP Config –** SLP Config accommodates network service discovery features of Novell (depending on how Novell is configured). Disabling it disables these features. Thus if your network uses these features of Novell, you should enable SLP Config.

  - **FTP Printing –** FTP Printing enables firmware upgrades using certain tools; however, it also allows anyone to upload files onto the MFP hard drive with the potential of filling up the hard drive. HP recommends disabling FTP printing and using Web Jetadmin to upgrade firmware.

  - **LPD Printing –** LPD Printing is the protocol necessary for printing in UNIX, HPUX, or Linux environments. You should enable LPD Printing if your network includes any of these workstations that might print using the MFP.

  - **9100 Printing –** 9100 Printing should always be enabled. It is the printing protocol used by the HP LaserJet 4345 MFP print driver. Disabling 9100 Printing would disable all printing for most users.

  - **IPP Printing –** IPP Printing is a protocol for printing directly from the Internet. It is not secure, and it should not be used. You can print images from the Internet using other methods.

  - **MDNS Config –** MDNS Config is a method of resolving host names with IP addresses in small networks that have no DNS servers. Most enterprise networks include DNS servers and do not require this service. If your network does not include a DNS server, enable MDNS Config.

- **IPv4 Multicast Config** – IPv4 Config is a method of configuring multiple devices simultaneously over the network. Some networks may include tools that use this method; however, HP recommends using Web Jetadmin to manage multiple devices securely.

- Set the Privacy setting as desired. The Privacy setting is included in this checklist to inform you that enabling it allows HP to collect statistical data on the use of MFPs. HP uses such information to help improve the design and development of MFPs. HP will not collect network-specific or personal data. For information on HP privacy policies, read the Hewlett-Packard Online Privacy Statement available by clicking privacy statement at http://www.hp.com viewed in your language.

  If you enable this feature, information collected by HP will be limited to the following items:
  - HP Jetdirect product number, firmware version, and manufacturing date
  - Model number of the attached printer or device
  - Web browser and operating system detected
  - Local language selections used for viewing Web pages
  - Network communications protocols enabled
  - Network management interfaces enabled
  - Device discovery protocols enabled
  - Printing protocols enabled
  - TCP/IP configuration methods enabled
  - SNMP control methods enabled
  - Wireless configuration methods enabled

  For HP to collect any information, Internet access must be available.

- Disable **RCFG Setting**. The RCFG setting (sometimes called RCONFIG) allows remote configuration of the MFP on an IPX/SPX network. Web Jetadmin may use RCFG to configure Novell NetWare queue-server linkages on older Jetdirect print servers. You should disable RCFG Setting unless your network has Novell and older Jetdirect print servers.

  When you disable the RCFG setting and click Apply, a caution message will appear to alert you that you are disabling certain types of Novell access. Click **OK** to go ahead with disabling it.

- Enable **HTTPS**. This setting enables secure Internet protocol that provides encryption for configuration data as it is transferred between the PC and the MFP. You should enable HTTPS to configure the MFP via Web Jetadmin or via EWS. If HTTPS is disabled, configuration communication with the MFP, including passwords, is transferred in clear text. This setting is related to the EWS **Encryption Strength** setting explained later in this section.

5.2.3 Protocol Stacks (Networking Page)

- Disable **IPX/SPX** protocol stack. IPX/SPX protocol is the network protocol for Novell. Disabling it prevents printing and other communication between the MFP and other points if they are using Novell. Thus, you should enable IPX/SPX protocol if your network includes Novell components.

- Enable **TCP/IP** protocol stack. TCP/IP protocol is the standard network protocol for the MFP. It provides the necessary network communication for printing and for configuration. If you disable the TCP/IP protocol stack, the MFP will most likely be unable to provide services over the network.
- Enable **DLC/LLC** protocol stack. DLC/LLC is a networking protocol used in small networks in which routing is not required. HP includes it in MFPs because it is used on older products. Unless the network is using the DLC/LLC for communication, disabling it has no affect the MFP.
- Disable **AppleTalk** protocol stack. AppleTalk is a protocol used with Apple computers. If your network includes Apple or Macintosh computers, enable AppleTalk. Otherwise, disable it as a best practice to maintain control over network communications.

5.2.4 Security Page Options

- Enable **Outgoing Mail**. The MFP sends some email, such as automatic fax notifications and consumables alerts, depending on configurations. This Outgoing Mail feature does not affect the MFP send to email functions. It also is not known to affect network security. If you use fax notification or other automatic email alerts, you should enable outgoing email.
- Disable **Incoming Mail**. Some network solutions can send commands to the MFP via email. If your network uses any of these solutions, you should enable Incoming mail. Otherwise, disable it.
- Disable **Cancel Job Button**. The EWS provides a Cancel Job button that allows users to cancel jobs that are pending in the queue. This includes canceling jobs sent by other users. Thus, disabling the Cancel Job button removes the ability to remotely (and anonymously) cancel jobs; however, users will be able to cancel their own jobs from the printer driver or from the control panel.
- Disable **Go Button**. The Go button is the EWS **Pause/Resume** button, which enables users to pause operations, such as print jobs, indefinitely. Disabling the Go button prevents users from delaying or even preventing other users from using the MFP; however, users will be able to pause or resume their own jobs from the print driver or from the control panel.
- Disable **Command Invoke**. Command Invoke is a legacy feature that is not available on the MFP. Disabling it is good security practice to ensure that access to it is closed.
- Disable **Command Download**. Command Download is a legacy feature that is not available on the MFP. Disabling it is good security practice to ensure that access to it is closed
- Disable **Command Load and Execute**. Command Load and Execute accommodates add-on applications (Chailets), such as workflow programs and job accounting programs. This function is called Load Services in the EWS. If your network uses such MFP add-on software, you should enable Command Load and Execute. If not, you should disable it to prevent users from installing these types of applications.

  You may wish to power cycle (turn off power and turn it on) the MFP after disabling Command Load and execute. The MFP will run add-on applications that are already loaded until it reboots.

- Set the **File System** password. The File System password feature prevents unauthorized users from making changes to the contents or to the settings of the MFP hard drive. This includes changing secure erase settings (see the next step). The File System password setting provides and extra layer of protection for certain settings of the MFP. This is true even when SNMPv3 is enabled. The MFP will prompt for the SNMPv3 credentials and for the File System password. It will also prompt for other passwords such as the device password if they are configured. Thus, you may see several prompts for authorization credentials when you click Apply to change certain settings in Web Jetadmin.
- Set the **Secure File Erase Mode** to **Secure Fast Erase**. Secure Fast Erase mode overwrites files with arbitrary characters one time to render the files unreadable whenever the MFP deletes files. This process requires considerably more time than the default Non-Secure Fast Erase mode does. You should consider the impact of this configuration on normal use of the MFP. If the MFP might store sensitive data on the hard drive, you should use Secure Fast Erase. If your network is required to meet stringent security requirements such as DOD regulations, you should use Secure Sanitize Erase. Secure Sanitize Erase overwrites files three times with arbitrary characters. It requires significantly more time than Secure Fast Erase does, and it noticeably slows down MFP performance.
- Disable **PJL**, **PML**, and **NFS** protocols in **File System External Access**. The File System External Access settings limits read and write access to the MFP data storage file system. Some data storage applications, such as the Web Jetadmin Device Storage Manager (available by installing the Device Storage Manager plug-in using the Product Update navigation mode), use these protocols to access the MFP file system. If your network uses any of these applications, you can disable these protocols, enable them to use the applications, and then disable the protocols when you are finished. Disabling PJL and PML in this feature disables these protocols only for MFP disc access. Disabling NFS in this feature disables the entire protocol for all access to the MFP.

- Enable the **PostScript** protocol in the **File System External Access** area. The PostScript protocol enables programs such as Adobe ® products to access the MFP directly for printing and for access to fonts. This feature is convenient and useful, and it is not known to pose a significant risk to security. If you never use PostScript® drivers or print PDF files, you may wish to disable **PostScript** protocol.
- Set **Control Panel Access Lock** to Moderate Lock. The Control Panel Access Lock setting removes configuration settings from the MFP control panel. HP recommends using the Moderate Lock option to allow users to operate the MFP on their own jobs but to prevent them from making configuration changes that affect default settings on the MFP.

  The Control Panel Access Lock prevents everyone from accessing settings on the control panel. There is no way to give access to authorized users. The MFP does not include functionality to setup authorization for control panel controls. Thus, you should lock the control panel and use Web Jetadmin to unlock it whenever you wish to changes to control panel configurations. However, most of the locked control panel settings are available remotely using Web Jetadmin.

  Control Panel Access Lock closes all access to the fax menu. This includes the options to

Cancel All Pending Transmissions and 'Cancel Current Transmission. Thus, Control Panel Access Lock prevents all users from canceling faxes.

5.2.5 Secure Erase Options

- Set **Secure File Erase** to **Secure (Fast) Erase**. Secure File Erase the mode the MFP uses whenever it deletes files. The default mode, **Non-Secure**, is the fastest, but it provides no security for the data that remains on the hard drive. It only removes the file references to the data, but does not actually alter the data.

  The recommended mode, **Secure (Fast) Erase**, overwrites file data with a single pass of arbitrary characters. This renders the data virtually unrecoverable while taking a reasonable amount of time. Secure (Fast) Erase mode takes more time than the default mode does, but considerably less time than **Secure Sanitize Erase** does.

  Secure Sanitize Erase overwrites files with three passes to ensure that the data is completely unrecoverable. It uses a method that meets stringent DOD requirements to render the data destroyed. Secure Sanitize Erase slows down MFP performance considerably. You should use Secure Sanitize Erase only for circumstance where the data is extremely sensitive or where the network is required to meet DOD standards.

- Use **Secure Storage Erase** often, and configure options for scheduling. **Secure Storage Erase** is a feature that uses the **Secure File Erase** mode to delete files from MFP storage on a schedule or on demand. It guarantees that nothing is left behind during routine MFP operations. You may wish to use the **Secure (Fast) Erase** for normal MFP operation, and configure **Secure Sanitize Erase** for Secure Storage Erase on demand. This will allow better performance during normal use and better security when you can choose a time that is convenient for lower performance.

  You should also configure scheduled Secure Storage Erase to be sure that all data is removed regularly.

5.2.6 Digital Sending and Fax Options

- Fill in the **Default From Address**, and select **Prevent users from changing the Default From Address**. The **Default From Address** setting allows you to place a standard and consistent address in the From field of emails sent from the MFP. Selecting **Prevent users from changing the default from address** ensures that users are unable to tamper with the address in the From field. These features ensure that nobody can use the MFP to spoof identity or provide erroneous addresses. Consider using a From address that describes the location or the type of MFP, or use a real From address for a location that can monitor reply messages.

  With the Default From Address configured, no one can change the From address in email messages sent by the MFP. The address you create is the only address anyone can use. Keep this in mind as you choose an address for this setting.

  You may wish to consider using email address authentication, which authenticates the user’s

own email address at the LDAP server and places it in the From address. This configuration does not allow users to change the From address.

- Configure the Fax PIN number. With this feature configured, the MFP requires a code at the control panel before it will release fax jobs for printing. This ensures that authorized users are present at the time of printing. Unauthorized people are less likely to see printed faxes.

  With the fax PIN configured, the MFP will not release a fax job to anyone without the PIN. The MFP will hold a fax job on the MFP hard drive until someone prints it (according to fax job settings). However, Secure Storage Erase removes all non-system files including fax jobs. Thus, if someone is not available to print a fax, the fax job could be lost to Secure Storage Erase before the fax can be printed. Be sure to plan for this as you configure these settings.

  NOTE: Stored faxes are not affected by Job Storage settings such as Job Hold Timeout.

6 Physical Security

Many of the most notable features of a HP LaserJet 4345 MFP involve hard copy documents. The MFP can print them, scan them, send them to email, send them to network folders, send them to other printers, and fax them. Handling hardcopy documents can involve a variety of activities that can lead to compromise of data security:

- Leaving documents in the print output trays exposed to possible unauthorized viewers.
- Leaving documents in Automatic Document Feeder (ADF) or on the flatbed scanner exposed to possible unauthorized view.

Physical security also involves access to the location where an MFP is installed. Limiting physical access to an MFP can easily prevent many security risks from unauthorized users. Such risks include the following:

- Access to configurations in the control panel
- Access to power cycle the MFP, to initiate cold resets, and to change other configurations
- Access to removable storage devices such as hard drives and memory cards
- Access to input trays, output trays, and automatic document feeder trays where hardcopy documents may be left after processing
- Access to network cables connected to the MFP
- Access to digital sending services and features
- Access to stored print jobs (depending on settings)
- Access to copy features (unauthorized overuse of resources such as toner and paper)

You can help minimize all of these risks by placing the MFP in an access-controlled location. HP LaserJet 4345MFPs also accommodate locks to protect access to removable storage devices. Use a lock, such as a Kensington Lock, as recommended in the HP LaserJet 4345 MFP User Guide.

7 Appendix 1: Glossary of Terms and Acronyms

The following table lists terms and acronyms found in this checklist:

Term	Description
MFP	Multi-Functional Peripheral – An MFP is a device that includes multiple capabilities such as print, copy, fax, and email (digital sending). This checklist covers the HP LaserJet 4345 MFP, which includes all of these functions. The HP LaserJet 4345 MFP provides monochrome printing, color scanning, fax, and email. It can perform other functions with additional solutions: digitally sending documents to network folders, LAN fax, or work flows. However, this checklist covers the HP LaserJet 4345 MFP only as it comes shipped and installed on a network. Thus, in this context, digital sending refers to the send to email capability, and fax refers to analog fax (fax via telephone lines). This context also assumes that the MFP is connected to a LAN via Ethernet cables.
EWS	Embedded Web Server – The embedded web server is a web page built into the MFP to provide status and configuration settings. The EWS is accessible over network lines using any Web browser connecting to the MFP network IP address.
WJA	HP Web Jetadmin – HP Web Jetadmin is a peripheral management tool that provides access to multiple devices for status and configuration. It is capable of configuring multiple MFPs simultaneously. Web Jetadmin is the recommended tool for configuring all settings in this checklist.
Digital sending	Digital sending is a function of the MFP that sends scanned documents to email destinations. Digital sending can also be upgraded to send scanned documents to network destinations on networks with Digital Sending Service software installed. This checklist assumes that the MFP is installed and used as shipped without upgraded solutions, and thus in this context, digital sending refers only to send to email functions.
Analog fax	Analog fax is fax functions via telephone lines. HP LaserJet 4345 MFPs are available with analog fax functions with a fax module installed. The fax module is available in most HP LaserJet 4345 MFP bundles and it is covered in this checklist. HP LaserJet 4345 MFPs are also capable of sending fax via LAN fax or internet fax using additional solutions on the network. LAN fax and Internet fax are not covered in this checklist.
Firmware	Firmware is the program that operates the MFP. It controls all functions of the MFP. Firmware is upgraded as HP improves it. New firmware is available searching for it by product at hp.com. This checklist assumes that the MFP is upgraded with the latest firmware.

Term	Description
Storage device	A storage device is a component that stores data. The MFP includes two types of storage devices: hard drive, and Compact Flash cards. The MFP hard drive stores two types of data: system data, such as configurations, that is part of the firmware and user data such as print jobs and address books. The MFP compact flash cards store system information such as firmware data and fonts.
Formatter	The formatter is the main circuit board of the MFP. It is similar to the motherboard of a PC. The formatter of HP LaserJet 4345 MFPs accommodates the MFP hard drive, the Compact Flash cards, the Jetdirect card, the CPU, the analog fax accessory card, and the DC Controller, which is the power supply for the MFP. The formatter also accommodates accessories such as wireless cards for the MFP. Since the formatter of an HP LaserJet 4345 MFP is removable (using common tools), it includes the capability to be locked using devices such as Kensington locks.
Scanner , ADF, or flatbed scanner	The top of the MFP is a scanner that converts paper documents into digital images for copy, fax, or digital sending. The scanner can scan a document in two ways: Automatic Document Feeder (ADF) or flatbed. The ADF is the top of the MFP. It is the cover of the flatbed scanner (see below). The ADF draws sheets into a paper path from an input tray similar to the input paper tray on a printer. It runs each sheet past the scanner and places it in an output tray. The flatbed scanner is a flat pane of glass under a cover (the ADF) that opens to allow placement of one sheet for scanning. The flatbed scanner is for documents such as folded paper or books that will not go through the ADF.
SNMPv3	SNMPv3 is a secure network protocol that encrypts network traffic. It is available with Web Jetadmin, but it requires configuration at Web Jetadmin and at the MFP.