



# HP Imaging and Printing Security Best Practices

Configuring Security for Multiple LaserJet MFPs and Color LaserJet MFPs

Version 5.0 for HP Web Jetadmin 10.1 or above

- HP LaserJet M3027 MFP
- HP LaserJet M3035 MFP
- HP LaserJet 4345 MFP
- HP LaserJet M4345 MFP
- HP LaserJet M5025 MFP
- HP LaserJet M5035 MFP
- HP LaserJet 9040 MFP
- HP LaserJet 9050 MFP
- HP Color LaserJet 4730 MFP
- HP Color LaserJet CM4730 MFP
- HP Color LaserJet 9500 MFP
- HP Color LaserJet CM3530 MFP
- HP Color LaserJet CM6030 MFP
- HP Color LaserJet CM6040 MFP

# Table of Contents

|   |    |
|---|----|
| Table of Contents .....                                 | i  |
| Chapter 1: Introduction.....                            | 1  |
| Cautions.....   | 2  |
| Follow the Checklist in Order.....                      | 2  |
| Understand the Ramifications.....                       | 2  |
| Continue to be Vigilant.....                            | 2  |
| MFP Environment.....                                    | 3  |
| Assumptions.....  | 3  |
| Solutions covered .....                                 | 4  |
| Organization .....                                      | 4  |
| Chapter 2: Threat Model .....                           | 5  |
| Spoofing Identity .....                                 | 5  |
| Tampering with Data.....                                | 6  |
| Repudiation .....                                       | 6  |
| Information Disclosure .....                            | 7  |
| Denial of Service .....                                 | 7  |
| Elevation of Privilege.....                             | 8  |
| Chapter 3: Basic Security for Multiple MFPs .....       | 9  |
| Notes on the Process of Configuration .....             | 9  |
| Using Web Jetadmin and MFP Passwords .....              | 9  |
| Getting started configuring MFP Security Settings ..... | 11 |
| Setting up HP Web Jetadmin .....                        | 11 |
| Configuring HP Secure Hard Disk .....                   | 13 |
| Configuring SNMPv3 .....                                | 16 |
| Configuring MFP Device Settings .....                   | 22 |
| I/O Timeout to End Print Job.....                       | 22 |
| Job Hold Timeout.....                                   | 22 |
| Job Retention.....                                      | 23 |
| Apply the Changes .....                                 | 23 |
| Configuring MFP Network Settings.....                   | 25 |
| Enable Features .....                                   | 25 |
| Encrypt all Web Communication.....                      | 29 |
| Encryption Strength .....                               | 30 |
| Error Handling .....                                    | 31 |
| IPX RCFG Support.....                                   | 31 |
| Job Timeout.....  | 32 |
| Privacy Setting.....                                    | 32 |
| Protocol Stacks .....                                   | 33 |
| Web Services Print.....                                 | 35 |
| Apply your Changes .....                                | 36 |
| Configuring MFP Security Settings.....                  | 37 |
| Bootloader Password.....                                | 37 |
| Color Access Control.....                               | 38 |
| Control Panel Access.....                               | 38 |
| Embedded Web Password .....                             | 39 |
| PJI Password .....                                      | 40 |

|  |    |
|--|----|
| Printer Firmware Update .....                        | 41 |
| Secure Disk Encryption Mode .....                    | 41 |
| Apply the Changes .....                              | 42 |
| Configuring MFP Fax Settings.....                    | 44 |
| Configuring Fax Printing .....                       | 44 |
| Apply the Changes .....                              | 45 |
| Additional Fax Configuration.....                    | 46 |
| Configuring MFP Embedded Web Server Settings .....   | 48 |
| Embedded Web Server Configuration Options .....      | 48 |
| Apply the Changes .....                              | 50 |
| Configuring MFP File System Settings .....           | 51 |
| File System External Access .....                    | 51 |
| File System Password .....                           | 52 |
| Secure File Erase Mode .....                         | 53 |
| Apply the Changes .....                              | 54 |
| Configuring MFP Digital Sending Settings .....       | 56 |
| Auto Reset Send Settings.....                        | 56 |
| Default From Address .....                           | 57 |
| Apply the Changes .....                              | 57 |
| Configuring Final Settings .....                     | 58 |
| Disabling Direct Ports .....                         | 58 |
| Disabling EWS Config.....                            | 59 |
| Chapter 4: Advanced Security for Multiple MFPs ..... | 61 |
| Access Control List (ACL).....                       | 61 |
| Authentication Manager .....                         | 63 |
| Group 1 PIN and Group 2 PIN.....                     | 64 |
| LDAP.....  | 66 |
| User Pin Authentication .....                        | 67 |
| Chapter 5: Settings List .....                       | 68 |
| Recommended Settings.....                            | 68 |
| Initial settings .....                               | 68 |
| Device Page Settings .....                           | 68 |
| Fax Page Options .....                               | 68 |
| Fax Page Options .....                               | 70 |
| Digital Sending Page Options.....                    | 70 |
| Embedded Web Server Page Options .....               | 70 |
| File System Page Options.....                        | 70 |
| Network Page Options .....                           | 68 |
| Security Page Options .....                          | 69 |
| Final configurations.....                            | 70 |
| Chapter 6: Default Settings: .....                   | 71 |
| Chapter 7: Ramifications .....                       | 75 |
| Device Page Settings .....                           | 76 |
| Fax Page Options .....                               | 76 |
| Additional Fax Configuration.....                    | 81 |
| Digital Sending Page Options.....                    | 81 |
| Embedded Web Server Page Options .....               | 81 |
| File System Page Options.....                        | 82 |

|   |    |
|---|----|
| Network Page Options .....                                  | 76 |
| Security Page Options .....                                 | 79 |
| Final Configurations .....                                  | 84 |
| Overall Limitations .....                                   | 85 |
| Chapter 8: Physical Security.....                           | 86 |
| Chapter 9: Appendix 1: Glossary of Terms and Acronyms ..... | 87 |

# Chapter 1: Introduction

This document is a security checklist for the following HP MFP models:

- HP LaserJet M3027 MFP
- HP LaserJet M3035 MFP
- HP LaserJet 4345 MFP
- HP LaserJet M4345 MFP
- HP LaserJet M5025 MFP
- HP LaserJet M5035 MFP
- HP LaserJet 9040 MFP
- HP LaserJet 9050 MFP
- HP Color LaserJet 4730 MFP
- HP Color LaserJet CM4730 MFP
- HP Color LaserJet 9500 MFP
- HP Color LaserJet CM3530 MFP
- HP Color LaserJet CM6030 MFP
- HP Color LaserJet CM6040 MFP

All of these models are called MFPs hereafter. This checklist is written for acceptance by the National Institute of Standards and Technology (NIST), and it will be available at the NIST Checklist 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 version 10.1 or above in enterprise networks. It includes step-by-step instructions to configure one or more MFPs on a network.

This checklist assumes that network administrators are familiar with HP Web Jetadmin and management of HP MFPs and printers. Network administrators should be familiar with the MFP Embedded Web Server (EWS), HP Jetdirect, and firmware upgrades for Jetdirect and MFPs. Refer to the MFP User Guides and the HP Jetdirect Administrator Guide for more information. You can find these documents and more information by searching for it at [hp.com](http://hp.com).

HP Web Jetadmin is the recommended management tool for all HP network printing and digital sending products. It handles all settings recommended for best security in this document and much more. It 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](http://hp.com).

This checklist applies to most types of networks; however, it is developed and tested in the following environment:

- An ordinary TCP/IP network
- Microsoft Internet Explorer version 6.0 with SP2

- HP Web Jetadmin Version 10.2 installed on a Windows XP or Windows Vista PC
- One of each supported MFP with the latest updated firmware found at [hp.com](http://hp.com)

The process for configuring this checklist is developed using HP Web Jetadmin to manage all of the MFPs at the same time.

This checklist covers only those parts of HP Web Jetadmin that pertain to appropriate security settings. See the user guides, admin guides, and help files for information on other configurations.

## **Cautions**

HP is dedicated to providing the best and latest security information available for MFPs. This checklist is meant to help you to improve MFP security in your workplace. HP has tested this checklist to ensure that MFPs continue to provide the best possible performance while averting possible security threats; however, some of these settings can cause unexpected problems in your environment. Please be aware of the following cautions before you begin:

### **Follow the Checklist in Order**

The settings in this checklist are presented in a specific order to ensure success. Many of these security settings can be configured successfully only in the correct order. You should follow the instructions in this checklist exactly and avoid making additional configurations during this process. Other settings can disrupt the order and cause unexpected results.

### **Understand the Ramifications**

HP Web Jetadmin and MFPs include a wide variety of useful settings designed to make work easier and more productive. However, raising the level of security may require sacrifices in these areas. Be aware that applying this checklist will limit or even eliminate some of these features. See the Ramifications chapter for more information.

HP provides this checklist as a guide to best-practice security configurations that allow for reasonable convenience and usability. Some of the recommended settings create extra steps when accessing and managing MFPs. For instance, once you disable EWS configuration, you cannot access it again until you re-enable EWS configuration from HP Web Jetadmin.

These settings are tested in a variety of conditions and using various combinations of simulated customer environments. Testing includes configuring all of the MFPs at the same time and verifying that the affected features continue to function. However, it is impossible to test these configurations in all possible network environments. You should test these settings in your environment to ensure that you understand their effects. You may find that some of the settings cause undesirable limitations. See the Ramifications section for further information and cautions.

### **Continue to be Vigilant**

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

## MFP Environment

NIST defines several types of user environments, many of which are compatible with HP LaserJet and Color LaserJet MFPs. However, this checklist is written for MFPs in an enterprise environment or a small to medium business environment. These environments use most of the network features available with MFPs. This entire checklist can be configured using HP Web Jetadmin. You should configure as much of this checklist as possible while adapting the settings to your specific situation.

## Assumptions

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

- **Network administrators:** This checklist assumes that readers are trained network administrators who are familiar with common networking practices such as configuring HP Jetdirect connections and using HP Web Jetadmin. Administrators should have read the MFP user guide, the MFP administrator guide, the Jetdirect administrator guide, Web Jetadmin user guides, and help files. This checklist relies on these materials for necessary information. All of these guides are available by searching for them at [hp.com](http://hp.com).
- **MFPs:** This checklist covers security settings for specific HP LaserJet MFPs and HP Color LaserJet MFPs. It is meant to enable you to configure multiple MFPs simultaneously. It assumes that the MFPs are turned on, connected to the network, and in the factory default state.

Most of the settings recommended in this checklist apply to other HP MFPs and printers; however, this checklist is tested and known to be successful only with the specified MFP models.

- **Updated firmware:** This checklist assumes that each MFP has updated system firmware and Jetdirect firmware. You should use the latest firmware available, but realize that updated firmware may have new features not covered in this checklist. Updated firmware is available for download and installation at [hp.com](http://hp.com).
- **Web Jetadmin Version 10.x:** This checklist is written for use with HP Web Jetadmin Version 10.1 and above.
- **Enterprise environment:** This checklist is created and tested in a TCP/IP enterprise environment. However, most of the settings are applicable to any network.
- **Network connection:** This checklist assumes that each MFP is connected directly to a local area network via Jetdirect or Jetdirect Inside (JDI). Other connections, such as direct-connect via parallel cable or via USB are not covered in this checklist (this checklist recommends disabling direct-connect ports).
- **Settings are only suggested:** All settings in this checklist are meant only as suggestions for best-practice security in common enterprise environments. Use it as a reference, and make judgments about each recommended setting before configuring your MFPs.
- **Internet and intranet security:** This checklist assumes that your network includes basic security configurations and components. All MFPs should be installed behind network firewalls and other standard tools such as updated virus protection applications.

## Solutions covered

This checklist covers MFP security settings found in HP Web Jetadmin. This checklist covers no other solutions or applications.

## Organization

This checklist includes the following chapters:

- Chapter 2: Threat Model: The Threat Model chapter explains the security circumstances relating to MFPs. It follows the Microsoft® STRIDE model.
- Chapter 3: Network Security for Multiple MFPs: The Network Security for Multiple MFPs chapter provides step-by-step instructions for configuring MFP security settings.
- Chapter 5: Settings List: The Settings List chapter provides a bulleted list of the recommended settings with checkboxes. It does not include instructions or explanations.
- Chapter 6: Default Settings: The Default Settings chapter lists each recommended setting with its corresponding default setting.
- Chapter 1: Ramifications: The Ramifications chapter explains the possible limitations implied with each recommended setting.
- Chapter 8: Physical Security: The Physical Security chapter explains security concerns in workplaces where MFPs are installed. It covers security for picking up print jobs, copying, and scanning. This section includes suggestions for securing the locations where MFPs are installed and for securing MFP internal hardware.
- Chapter 9: Appendix 1, Glossary and Acronyms.



## Chapter 2: Threat Model

This section explains the types of security risks involved with operating MFPs in enterprise environments.

As technology improves, malicious people (hackers) continue to find new ways to exploit networks. They are beginning to target MFPs and other network peripherals to misuse resources or to gain access to networks or the internet. Predicting the actions of a hacker is difficult, but HP is dedicated to research in this area. This checklist represents some of HP's efforts to ensure that you can use HP MFPs with confidence; however, you should continue to be ware and always remain vigilant. Use other techniques with this checklist to help ensure that your network is resistant to compromise.

---

### NOTE:

This is not a comprehensive treatment of these issues. This chapter is only an introduction to the types of threats known to affect network MFPs.

---

The Microsoft STRIDE model provides a valuable outline to categorize these known types of threats:

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

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

### Spoofing Identity

Spoofing identity is masquerading as someone else to fool others or to get unauthorized access. Here are some ways spoofing identity can relate to MFPs:

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

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

- Protect the **from address** field in the MFP Digital Sending and Fax configurations.
- Protect MFP disk access.
- Configure authentication.
- Configure the administrator password.
- Configure SNMPv3.

## 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 ways tampering with data can relate to MFPs:

- Canceling another person's job. Someone could use a remote access tool to cancel pending jobs. The person who sent a cancelled job gets no warning; only part or none of the job is 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

You can minimize the risks from data tampering in the following ways:

- Disable **Cancel Job** button.
- Disable **Go** (Pause) button.
- Configure SNMPv3.
- Prevent unnecessary remote access: close down all unused ports and protocols.
- Configure HTTPS for EWS access.

## Repudiation

Repudiation is using an MFP without leaving 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 an MFP without paying by bypassing job accounting software. Here are some ways repudiation can relate to MFPs:

- Accessing usage logs to delete entries
- Removing origination information from file metadata
- Bypassing user authentication
- Using remote management software to access the MFP

You can minimize the risks of repudiation in the following ways:

- Install Jetdirect 635n Print Servers or enable embedded IPSec to encrypt the data stream to include log data and file metadata (look for this product at [hp.com](http://hp.com) or contact your hp product supplier).
- Close unused ports and protocols.
- Save copies of log data at a separate location
- Add security solutions such as smartcard, swipe-card and thumbprint readers

## Information Disclosure

Information disclosure is gathering information from an MFP and providing it to unauthorized users. This can include authentication information, usage log information, or information from the contents of a job. Such data stored on your hard drive is considered 'at rest' while data being transmitted by your MFP device is considered 'in transit'. Here are some ways information disclosure can relate to an MFP:

- Reading stored print jobs on the MFP hard drive.
- Downloading log information
- Downloading address books
- Intercepting print jobs, copy jobs, fax jobs, or digital send jobs (such as email).

You can minimize the risks of information disclosure in the following ways:

- Enable IPSec to protect data in transit. Although some devices include this feature embedded, you may need to install an HP Jetdirect 635n (wired) or HP Jetdirect 690n (wireless) Print Server accessory. (Look for this product at [hp.com](http://hp.com) or contact your HP product supplier).
- Use hardware encryption to protect data at rest. Some devices may include an encrypted disk. If not, you can add an HP Secure Hard Disk accessory to protect data stored on your MFP. (Look for this product at [hp.com](http://hp.com) or contact your HP product supplier).
- Close unused ports and protocols.
- Configure all possible password settings.
- Configure authentication.
- Configure SNMPv3 for Web Jetadmin.

## 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 remotely
- Disconnecting power to the MFP
- Removing the MFP formatter board
- 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

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 resume feature to allow the MFP to resume operations after an error state.
- Configure Job Timeout.
- Control physical access to the MFP.
- Lock physical access to removable hardware.

## **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 changing settings to get administrator privileges
- Unauthorized use of management software to provide access for other unauthorized users
- Using management software to bypass job accounting functions

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

- Configure the administrator (device) password.
- Configure SNMPv3 and HTTPS.
- Lock the control panel.

## Chapter 3: Basic Security for Multiple MFPs

This chapter explains how to configure security settings for one or more MFPs using HP Web Jetadmin. It assumes that you have taken or plan to take reasonable steps to secure the network environment in which your MFPs are operating. This includes configuring network firewalls and providing up-to-date virus controls. If you need help doing this or are looking for information on Jetdirect Firewall, ACL, Kerberos, PIN authentication, HP Digital Send Service, IPSec, IPv6, or Full Hard Disk Encryption please refer to the chapter on Advanced Security.

### Notes on the Process of Configuration

This checklist covers all relevant security settings available for MFPs. Testing shows that this combination of settings is successful in the most common network environments as long as the settings are executed in the correct order.

After each setting in the checklist is applied, it is important that you verify configuration to ensure this order is maintained. If a setting was not applied, attempt to set that setting again. If you have further issues with a particular configuration item, you can try using the individual configuration pages, or setting that item through the EWS if available.

Keep in mind that every network is different. Configuring an MFP for your network may require adjustments to this configuration. Be aware of your network environment and consider the right configurations for your situation.

Also, keep in mind that each model of MFP may have unique sets of available settings. For instance, LaserJet (black and white only) MFPs do not provide settings to restrict color printing. However, Web Jetadmin lists the aggregate of all possible settings for all MFPs you are managing. You can select settings for all MFPs, and each individual MFP will accept configurations according to its capabilities and ignore settings that do not apply.

All of the settings in this chapter are found in HP Web Jetadmin, and you should use Web Jetadmin to complete them. If possible, try to complete all of the steps in the correct order.

---

**Tip:**

Use a printout of the Settings List chapter to check off each item as you go along.

---

### 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 the ability to configure a wide variety of features and services on the network. Without proper security, Web Jetadmin allows malicious users the same conveniences for attacking your network. Thus, configuring security features and passwords and updating them regularly for Web Jetadmin and MFPs is important to network security.

This involves several passwords that limit access to important areas of the MFP. When you attempt to make changes to configurations, the MFPs will require all applicable passwords. Web Jetadmin keeps an encrypted cache of all of these passwords for each MFP whenever they are configured or used. However, sometimes the cache can lose track of some credentials. Thus, you should keep a

log of the passwords in a safe place. Web Jetadmin will prompt for passwords during the configuration process if they are missing from the cache.

---

**CAUTION:**

Losing passwords can block access to an MFP. Be careful to record them in a safe place. It is most important to remember the Bootloader password. With it, it is possible to restore the MFPs to factory default settings. Without it, the only way to restore the MFPs is to involve an HP-authorized service technician to reset the entire MFP. 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 configure:

- Web Jetadmin password (required during installation of Web Jetadmin)
- SNMPv3 credentials
- Bootloader Password
- EWS Password
- Device Password
- File system password
- Fax PIN
- Device PIN (for MFP functions)
- User PIN (for individual user accounts)
- PJI password

Use good practices for setting and updating passwords (some of the password settings have limitations on what and how many characters may be used):

- Use alpha and numeric characters whenever possible.
- For numeric only passwords use passwords with at least nine digits.
- Use a different password for each password setting. Many of the latest password cracking tools can follow patterns to make guessing easier.
- Avoid using a pattern for passwords.
- Change the passwords often with the exception of your HP Secure Hard Disk password. Changing your HP Secure Hard Disk password (Drive Lock Key) causes a loss of all data on your disk and system security settings
- Use the maximum number of possible characters. Many of the password settings will accept as few as one character, but one character is easy to guess. Current data shows that nine characters or more are extremely difficult or almost impossible to guess using the latest password cracking tools.
- Use complicated passwords. Use a variety of character types. Some of the passwords allow only numeric digits, but others can accept 96 or more different characters (upper case, lower case, numeric, special characters, and punctuation marks).

- Use meaningless random passwords. Passwords that are real words or phrases are easier to guess. The latest password cracking tools follow dictionaries to narrow down the possibilities.
- Record the passwords in a safe but hidden place. The passwords are designed to restrict access to management options on the MFPs. Losing a password can eliminate your access to settings. This is most important for the Bootloader Password. The Bootloader Password is a permanent setting that can never be changed or reset without the correct password.

## Getting started configuring MFP Security Settings

This section provides instructions for configuring the MFPs for best-practice security. All of these settings are presented for HP Web Jetadmin Version 10.1 or later.

---

### Note:

If you are setting this checklist for a group of several printers at once, Web Jetadmin will display all supported settings for all the MFPs it is managing, even though some of the MFPs may not support all of these settings. Each MFP ignores settings that do not apply to it and continues without issues. For instance, color settings are ignored for a non-color MFP.

For the same reason, some of the settings may not appear in HP Web Jetadmin if none of your MFPs supports them. Web Jetadmin displays only the options that apply to the MFPs you are managing. For instance, color settings will not appear if none of your MFPs has color. Ignore recommendations in this checklist if they do not appear on your Web Jetadmin screen.

---

Before you begin, be sure to install HP Web Jetadmin Version 10.1 or later, and have it working in your network environment. You can find Web Jetadmin free for download and installation at the following location on hp.com:

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

Be sure to update Web Jetadmin Version 10.1 or later with the latest upgrades available from HP. See the HP Web Jetadmin Update page in the **Product Update, Install** menu.

---

### Note:

This checklist was written using screenshots from Web Jetadmin 10.2

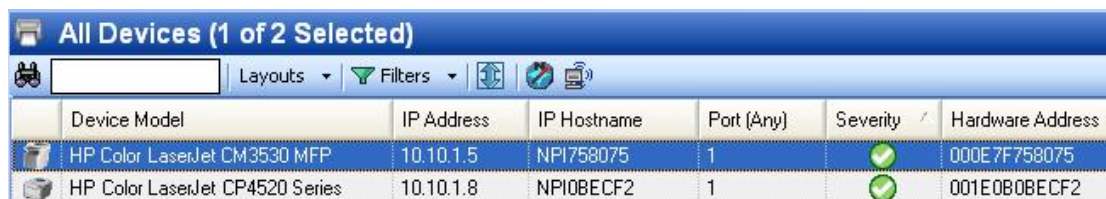
---





## Setting up HP Web Jetadmin

Follow these instructions to prepare Web Jetadmin for configuring the MFPs:

1. Open Web Jetadmin to view the device list (Figure 1) that appears by default.

Figure 1: Web Jetadmin showing the device list on the default view.



| All Devices (1 of 2 Selected)   |                                 |            |             |            |   |                  |
|---|---------------------------------|------------|-------------|------------|---|------------------|
|   | Device Model                    | IP Address | IP Hostname | Port (Any) | Severity  | Hardware Address |
|  | HP Color LaserJet CM3530 MFP    | 10.10.1.5  | NPI758075   | 1          |  | 000E7F758075     |
|  | HP Color LaserJet CP4520 Series | 10.10.1.8  | NPI0BECF2   | 1          |  | 001E0B0BECF2     |

2. Check to see that the MFPs you wish to configure appear in the **Device Model List**. If they are not in the list, use the Discovery options to find the MFPs on your network.

**Note:**

This checklist does not include details on MFP discovery. See Web Jetadmin user guidance for more information. In most cases, the MFPs will already appear in the default view of Web Jetadmin.

It is possible for Web Jetadmin to lose contact temporarily with an MFP that is configured for DHCP. Use the Discovery options to restore contact, or configure the MFPs with static IP addresses.

3. Hold down the CTRL key and click to select the MFPs to configure in the Device List view (Figure 2).

Figure 2: The Device List showing multiple devices selected.



| All Devices (2 of 2 Selected)   |                                 |            |             |            |   |                  |
|---|---------------------------------|------------|-------------|------------|---|------------------|
|   | Device Model                    | IP Address | IP Hostname | Port (Any) | Severity  | Hardware Address |
|  | HP Color LaserJet CM3530 MFP    | 10.10.1.5  | NPI758075   | 1          |  | 000E7F758075     |
|  | HP Color LaserJet CP4520 Series | 10.10.1.8  | NPI0BECF2   | 1          |  | 001E0B0BECF2     |

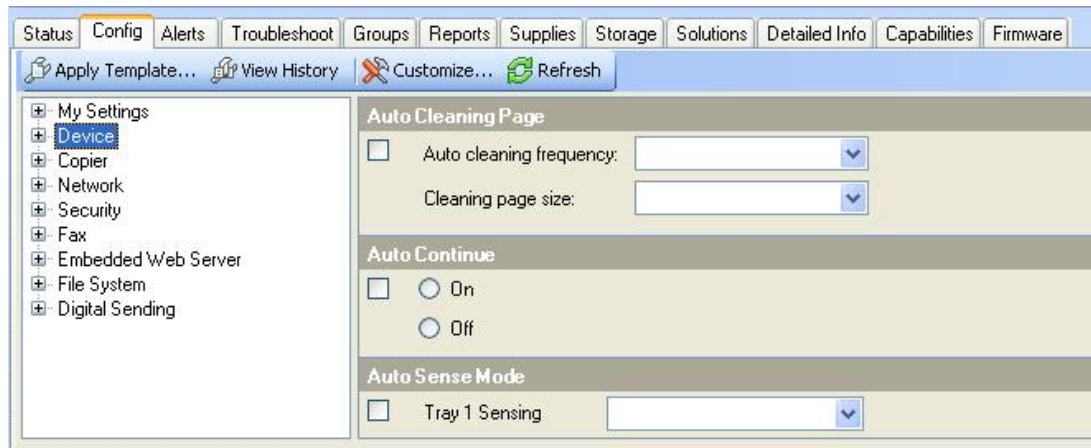
**Note:**

Remember that the steps in this checklist are for the specified HP LaserJet and Color LaserJet MFPs. Other devices may appear in the Device Model list, and it may be possible to configure them using this process, but the results may vary.



4. Click the **Config** tab in the lower half of the Device List view to show settings available for configuration (Figure 3).

Figure 3: The Config tab displays settings available for configuration.



The **Config** tab contains all of the settings recommended in this checklist.

**Tip:**

If you are having a problem configuring a setting, try configuring it using the individual device's configuration page. You can also attempt to configure the setting using the EWS of the MFP.

Sometimes Web Jetadmin can lose track of MFP credentials. If this happens, some settings might fail. Clear the Web Jetadmin Device Cache (see Web Jetadmin Help) and re-enter the MFP credentials.

The next step is to ensure that any installed HP Secure Hard Disks are configured:

### Configuring HP Secure Hard Disk

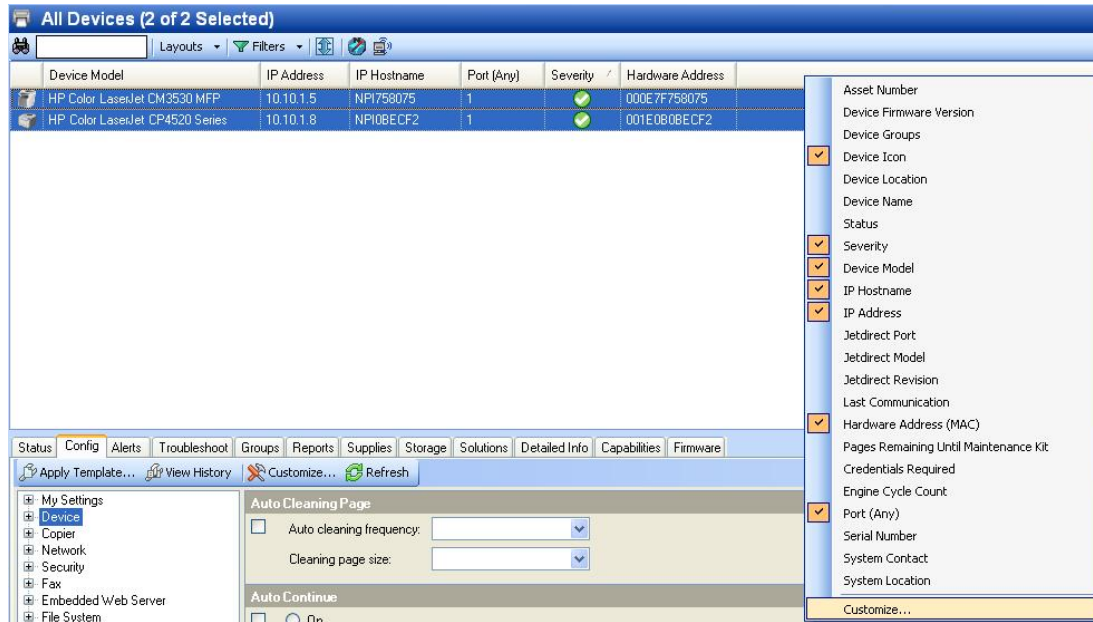
If you have an HP Secure Hard Disk installed you need to verify data encryption is enabled (this should happen by default after initial hard drive installation).

**WARNING:** If your HP Secure Hard Disk is not already configured to encrypt your data, consult your documentation to resolve this issue. Failing to configure your HP Secure Hard Disk before starting this checklist will reset all security settings to factory defaults and require you to repeat this checklist again when you configure the drive.

Follow these steps to use Web Jetadmin to verify your HP Secure Hard Disk is installed and configured:

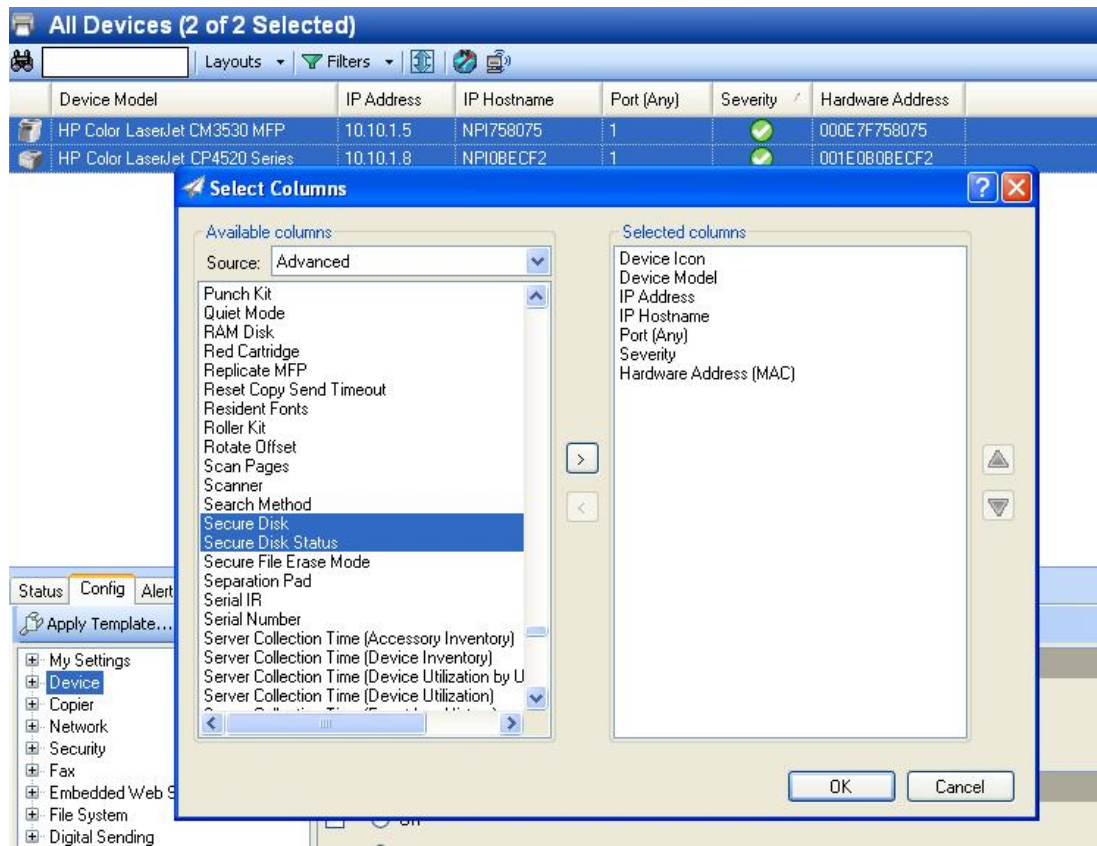
1. In the device list view, add the columns for Secure Disk and Secure Disk Status if they are not visible. First, right click on the column area to the right of the existing columns. Then select customize... from the drop down list (Figure 4).

Figure 4: Shows where how to reach the column customization menu.



2. In the next menu, you need to select the **Secure Disk** and **Secure Disk Status** columns and transfer them to the **Selected Columns** list (Figure 5).

Figure 5: Shows how to add the Secure Disk and Secure Disk Status columns to the columns selected for display.



3. In the listing of printers, check the **Secure Disk** and **Secure Disk Status** columns. The **Secure Disk** column should indicate "Installed". The **Secure Disk Status** column should indicate "Encrypted" (Figure 6).

Figure 6: Shows the Secure Disk and Secure Disk Status columns as Installed and Encrypted.

| All Devices (2 of 2 Selected)   |            |             |            |          |                  |               |                    |
|---------------------------------|------------|-------------|------------|----------|------------------|---------------|--------------------|
| Device Model                    | IP Address | IP Hostname | Port (Any) | Severity | Hardware Address | Secure Disk   | Secure Disk Status |
| HP Color LaserJet CM3530 MFP    | 10.10.1.5  | NPI758075   | 1          | ✓        | 000E7F758075     | Not Installed | No Encrypted Disk  |
| HP Color LaserJet CP4520 Series | 10.10.1.8  | NPI0BECF2   | 1          | ✓        | 001E0B0BECF2     | Installed     | Encrypted          |

---


**Note:**

If your MFP is reporting an installed HP Secure Disk but its status is anything other than Encrypted it is recommended you resolve the issues with your HP Secure Disk before continuing this checklist. If you do not you may need to re-apply the entire checklist to the MFP. An example of an MFP with a HP Secure Disk Installed that is not configured properly is shown below (Figure 7).

---

---

Figure 7: Shows a HP Secure Disk with a status of Not Encrypted indicating an issue with the Disk that needs resolution.



| All Devices (2 of 2 Selected)   |            |             |            |          |                  |               |                    |
|---------------------------------|------------|-------------|------------|----------|------------------|---------------|--------------------|
| Device Model                    | IP Address | IP Hostname | Port (Any) | Severity | Hardware Address | Secure Disk   | Secure Disk Status |
| HP Color LaserJet CM3530 MFP    | 10.10.1.5  | NPI758075   | 1          | ✓        | 000E7F758075     | Not Installed | No Encrypted Disk  |
| HP Color LaserJet CP4520 Series | 10.10.1.8  | NPI0BECF2   | 1          | ✓        | 001E0B0BECF2     | Installed     | Not Encrypted      |

The next step is to configure secure communications between HP Web Jetadmin and the MFPs:

## Configuring SNMPv3

SNMPv3 provides encryption for communication between Web Jetadmin and MFPs. It helps to ensure that only authorized and authenticated administrators have access to the configuration settings of the MFPs. It also helps to ensure that no one can gather sensitive information, such as passwords, usernames, and other codes, over the network while you are configuring the MFPs.

---

**Note:**

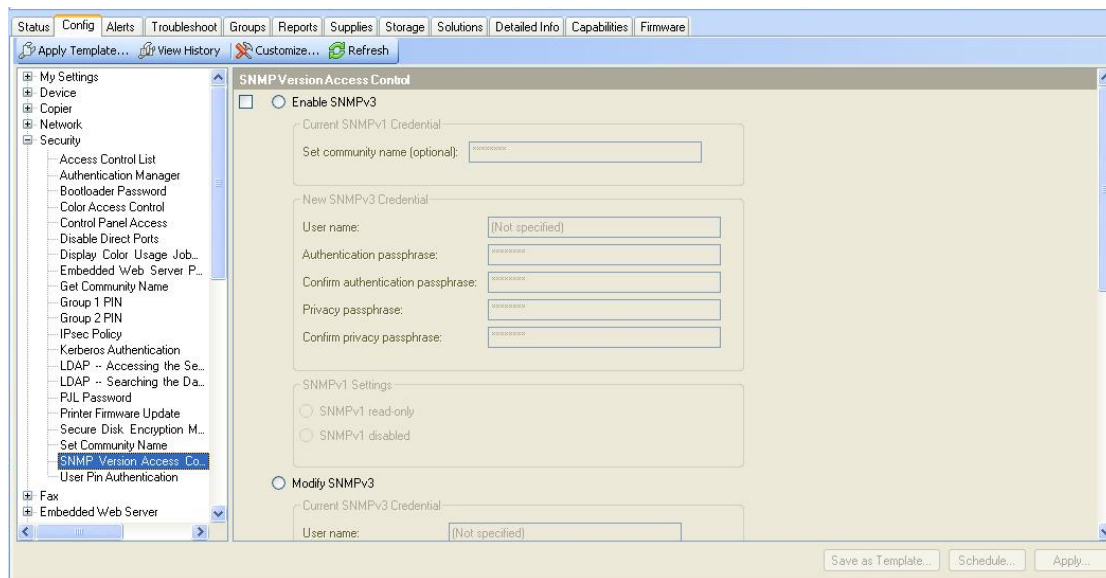
It is best to configure SNMPv3 by itself to ensure that the settings save properly.

---

Follow these steps:

1. Click **Security** in the Configuration Categories menu (Figure 8) to view the options for configuration. From the Security Options select **SNMP Version Access Control**.

Figure 8: The Security category and SNMP Version Access Control settings.



2. On the **SNMP Version Access Control** menu, and select the **Enable SNMPv3** checkbox (Figure 9).

Figure 9: Shows Enable SNMPv3 selected.



3. Once **Enable SNMPv3** has been selected, and fills in the **New User**, the **New Authentication Passphrase**, and the **New Privacy Passphrase** fields (Figure 10) in the New **SNMPv3 Credential** section. See below for details.

Figure 10: The Enable SNMPv3 option has been selected and the New SNMPv3 Credential section is complete.

SNMP Version Access Control (Changes Pending - Click 'Apply' to continue)

☒ ☐ Enable SNMPv3

Current SNMPv1 Credential

Set community name (optional): xxxxxxx

New SNMPv3 Credential

User name: wja

Authentication passphrase: xxxxxxx

Confirm authentication passphrase: xxxxxxx

Privacy passphrase: xxxxxxx

Confirm privacy passphrase: xxxxxxx

The **New User Name** field can be any name you choose.

The **New Authentication Passphrase** field can be any word or phrase that is at least 8 characters.

The **New Privacy Passphrase** field can be any word or phrase that is at least 8 characters.

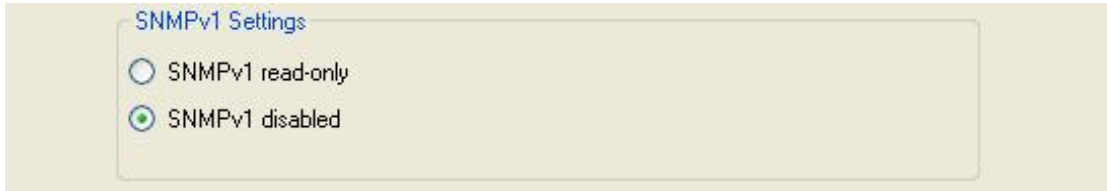
**CAUTION:**

These instructions are for the initial configuration of SNMPv3. Once you finish this configuration, the MFPs will require these credentials whenever anyone attempts to access settings over the network. Be sure to remember these credentials and provide them only to authorized users. If these credentials are forgotten, the only way to restore communication between HP Web Jetadmin and the MFPs is to restore the MFPs to factory default settings.

Web Jetadmin retains the SNMPv3 credentials for each MFP, and it will not prompt for them as long as the settings remain the same. You can clear the Web Jetadmin Device Cache to cause Web Jetadmin to require the credentials again. Web Jetadmin stores the SNMPv3 credentials in an encrypted form.

4. Scroll down to the SNMPv1 Settings section, and select **SNMPv1 disabled** (Figure 11).

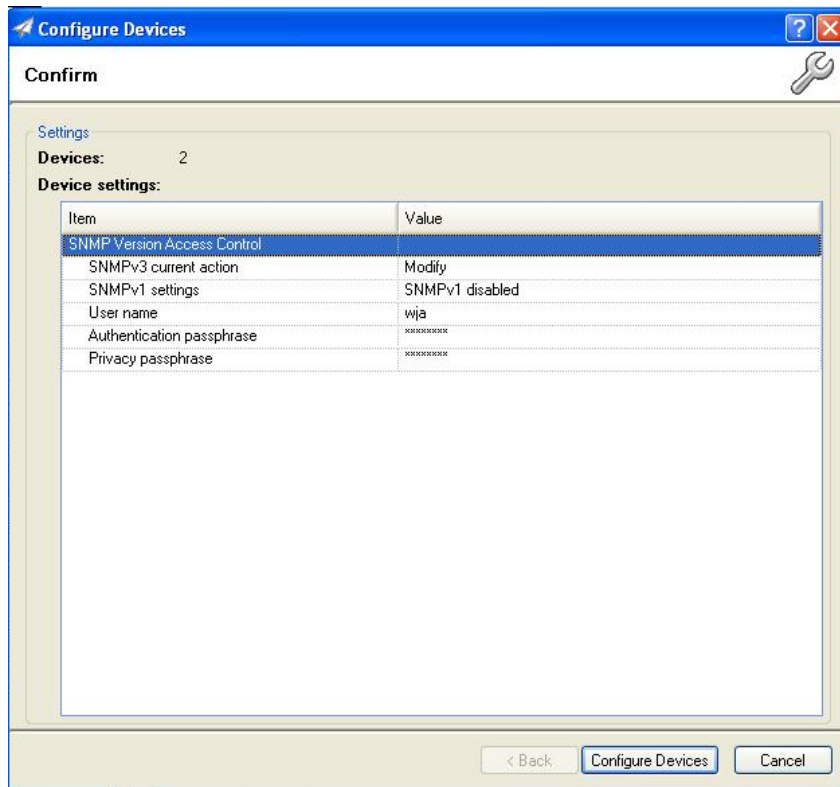
Figure 11: The SNMP Version 3 Only setting.



This setting limits all SNMP configuration communication to only SNMPv 3. Once applied your MFPs will not allow SNMPv1 SET and SNMPv2 GET.

5. Choose Apply at the bottom of the SNMP Version Access Control configuration to apply the settings to the selected devices. This will open the configure devices dialogue box (Figure 12).

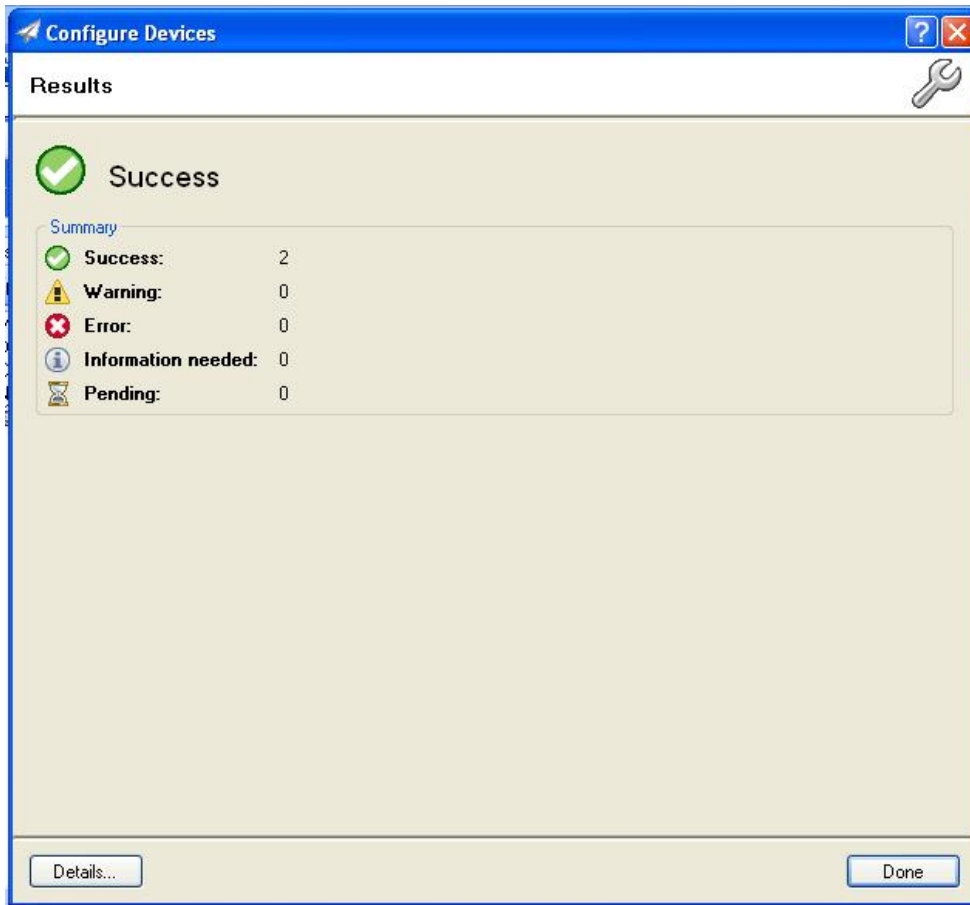
Figure 12: The Configure Devices dialogue box.





6. Click the **Configure Devices** button to execute the configuration. The result of your configuration will be displayed when the configuration is complete (Figure 13).

Figure 13: Shows a successful configuration result.



If your configuration is not successful, you can click the **Details** button for more information on why the configuration failed.

Now, whenever you click **Apply** to configure settings, the MFP will check for the SNMPv3 credentials.

**Note:**

For convenience, Web Jetadmin stores the credentials for each MFP in an encrypted format. However, Web Jetadmin may still prompt you for credentials on occasion so remember the passwords you set.

7. Click **Done** to exit the **Configure Devices** dialogue, and continue with this checklist.

## Configuring MFP Device Settings

The **Device** category includes settings that affect some of the normal use of the MFPs. The following settings affect how jobs are stored, and how long your MFP will wait before a job times out in a particular way.

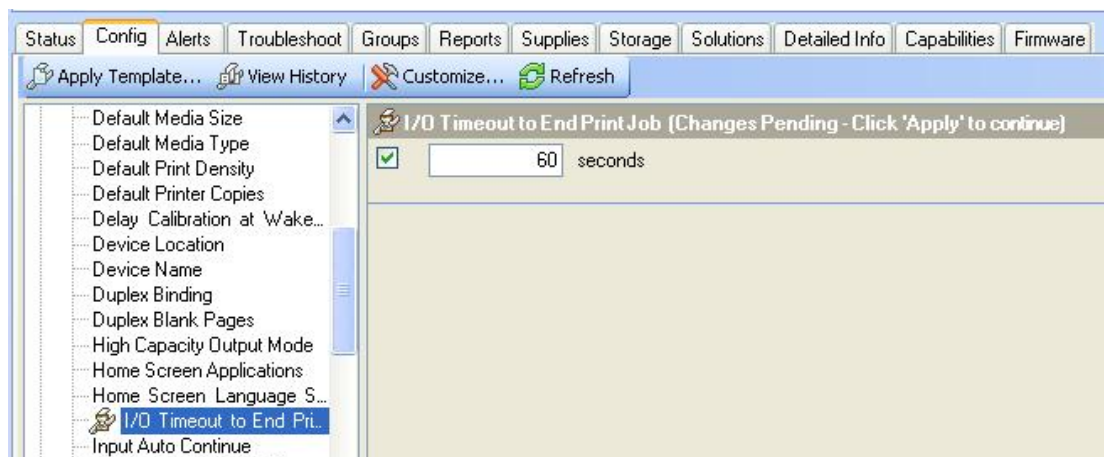
1. Click the **Device** category on the **Config** tab, to view the following configuration options:

### I/O Timeout to End Print Job

The I/O Timeout to End Print Job allows you to specify the amount of time a device should wait between packets before canceling a job. Setting this timeout will help prevent jobs formed or sent incorrectly from tying up a print resource. To set this timeout follow the instructions below.

1. From the **Device** category, select the **I/O Timeout to End Print Job** menu (Figure 14).
2. Click checkbox to enable the **I/O Timeout to End Print Job** setting, and select a reasonable time the MFP should wait between data packets.

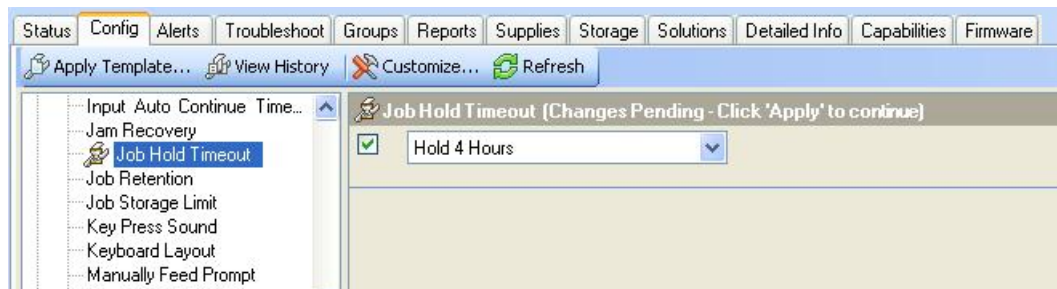
Figure 14: The I/O Timeout to End Print Job options.



### Job Hold Timeout

1. From the **Device** category, select the **Job Hold Timeout** menu (Figure 15).
2. Click checkbox to enable the **Job Hold Timeout** (Figure 15) setting, and select a reasonable time for printing. This ensures that stored copy and print jobs on the MFP are erased after a reasonable time.

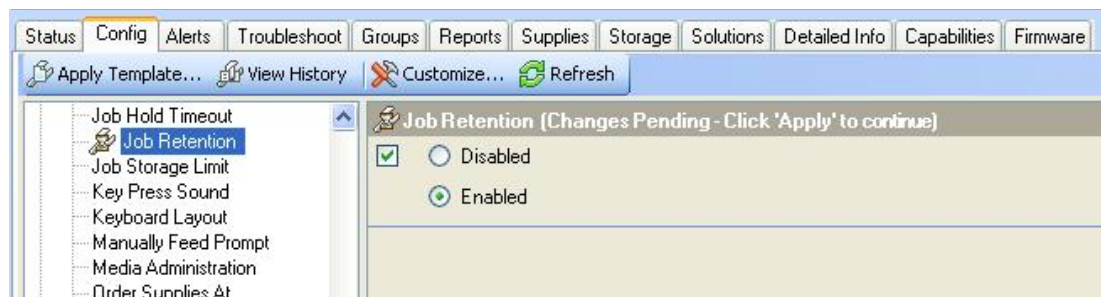
Figure 15: The Job Hold Timeout options.



## Job Retention

1. From the **Device** category, select **Job Retention** (Figure 16).
2. Click checkbox to select **Job Retention (Error! Reference source not found.)**, and select **Enabled**.

Figure 16: The Job Retention options.



This allows users to store print jobs and fax jobs for printing at their discretion (when they can be present to control the printouts and keep them from view).

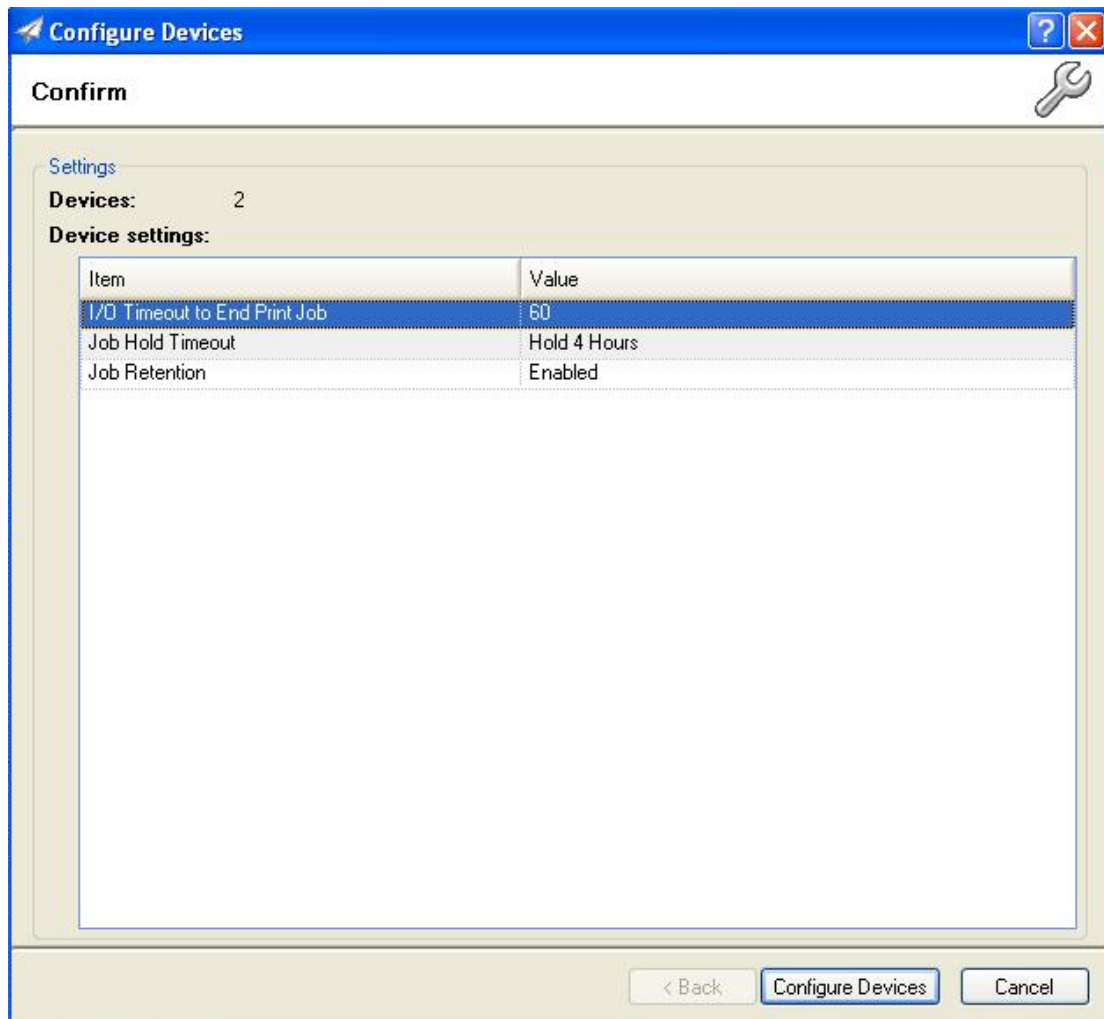
### Note:

Job Hold Timeout does not apply to fax jobs.

## Apply the Changes

1. Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices. This will open the configure devices dialogue box (Figure 17).

Figure 17: The Configure Devices dialogue box.



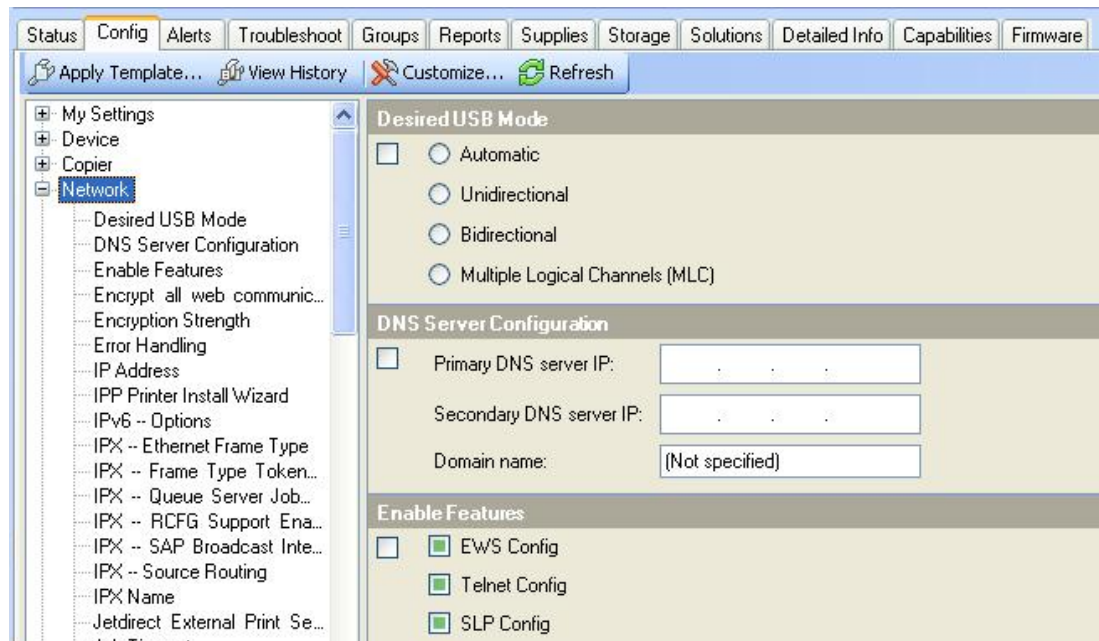
2. Review your settings and then click the **Configure Devices** button to execute the configuration.

## Configuring MFP Network Settings

The **Network** category on the Device tab provides options that relate to Jetdirect Print Servers. The security features you will be configuring restrict what methods are available for communication with your MFP over the network. Follow the instructions below to view and configure these options.

1. Click the **Network** category on the **Config** tab to expand the configuration options (Figure 18).

Figure 18: The Network Category.

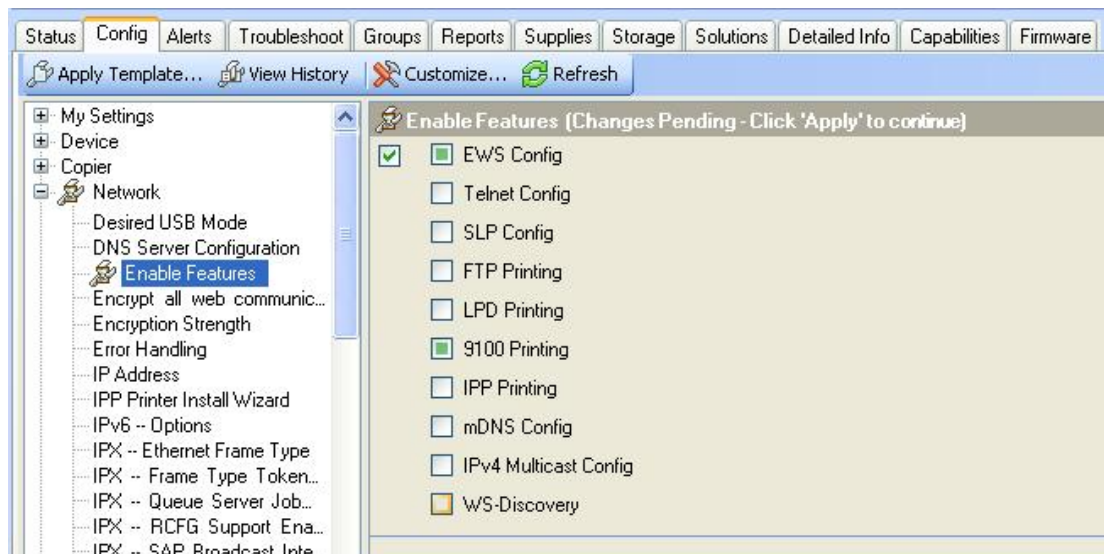


### Enable Features

To enable or disable print features on your MFP you:

1. Click **Enable Features** from the configuration options in the Network category (Figure 19).

Figure 19: The Enable Features option.



2. Next, select the print features you would like to enable or disable. The following table lists and explains the recommended settings for the **Enable Features** option:

| Feature       | Recommended Setting  | Explanation   |
|---------------|--|---|
| EWS Config    | Disabled***<br>***NOTE:<br>The recommendation is to disable <b>EWS Config</b> , but you should leave it enabled until you are finished configuring this checklist. Otherwise, it will prevent you from configuring some of the remaining settings. | Disabling EWS Config closes down the EWS and it eliminates the configuration settings that are controlled by the EWS. It also removes the affected settings from Web Jetadmin menus. This includes settings for email, send to folder, and fax. You should disable EWS Config while the MFPs are in use, and enable it only to make changes to the affected configurations. |
| Telnet Config | Disabled   | Disabling <b>Telnet Config</b> prevents access to configuration settings and other features through Telnet.   |

|                       |          |  |
|-----------------------|----------|--|
| SLP Config            | Disabled | Disabling <b>SLP Config</b> prevents access to configuration settings and other features through SLP.  |
| FTP Printing          | Disabled | Disabling <b>FTP Printing</b> prevents access to configuration settings and other features through FTP. It also prevents printing through FTP.     |
| LPD Printing          | Disabled | Disabling <b>LPD Printing</b> prevents access to configuration settings and other features through LPD. It also prevents printing through LPD.     |
| 9100 Printing         | Enabled  | <b>9100 Printing</b> is the access point for normal printing through standard HP print drivers.  |
| IPP Printing          | Disabled | Disabling <b>IPP Printing</b> prevents access to configuration settings and other features through the IPP. It also prevents printing through IPP. |
| MDNS Config           | Disabled | Disabling <b>MDNS Config</b> prevents access to configuration settings and other features through <b>MDNS</b> .                                    |
| IPv4 Multicast Config | Disabled | Disabling <b>IPv4 Multicast Config</b> prevents access to configuration settings and other features through IPv4 Multicast.                        |
| WS-Discovery          | Disabled | Disabling <b>WS-Discovery</b> prevents systems from using WS-Discovery for discovering or browsing printers on the network.                        |

---

**WARNING:** You will want to enable WS-Discovery on this printer if the following apply: You are using an IPv6 only network, you use WS-Print to discover your devices, or operate in a Windows Vista/ Windows 7 centric environment. If you are unsure of this setting, we highly recommend testing its implications with a single device before applying it to your whole fleet.

---

---

Note:

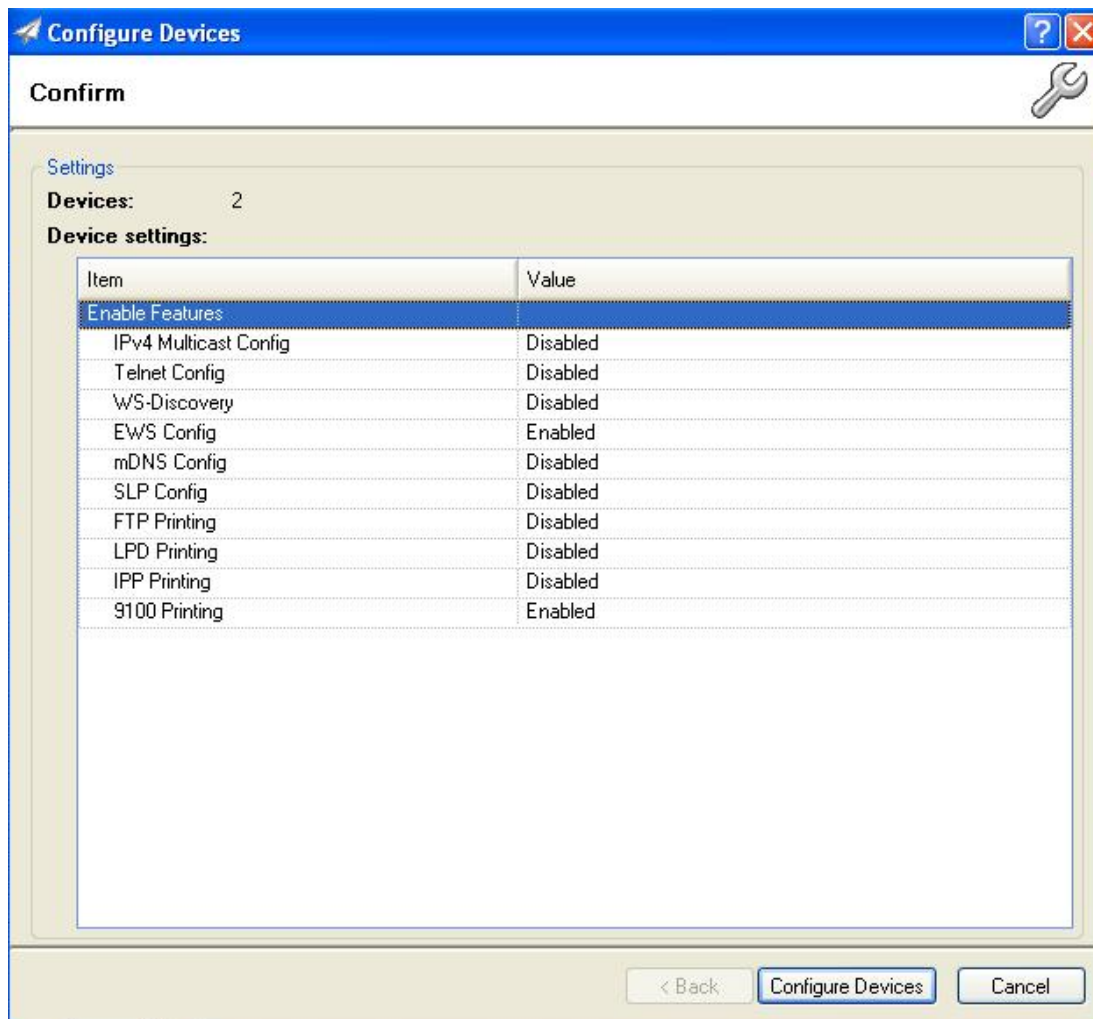
If you are using third party solutions recommendations may be different. Please see the Advanced Security chapter. As a rule, you should close down any MFP network features that are not in use.

---

3. Click **Apply** in the lower right hand corner to view the Configure Devices dialogue box. (Figure 20). Review your selections carefully before clicking on the **Configure Devices** button.



Figure 20: Review your Enable Features Configuration selections before configuring your devices.

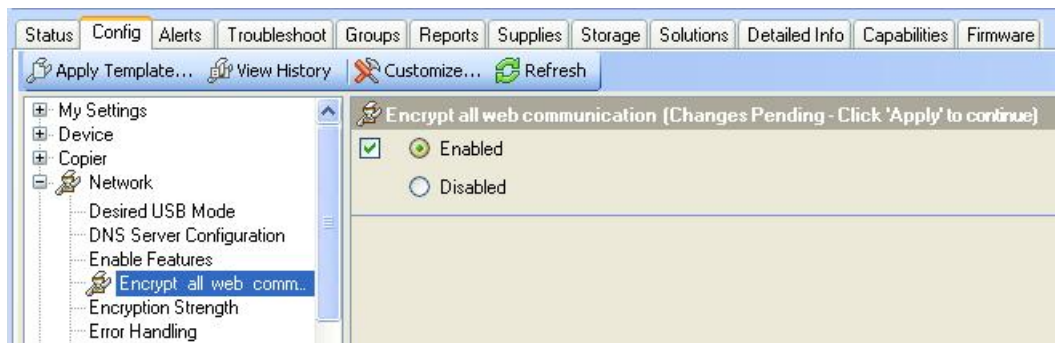


## Encrypt all Web Communication

This setting requires web browsers to use HTTPS when contacting the MFPs. This ensures secure communications with the MFP EWS. To enable this feature:

1. Click **Encrypt all web communication**, and then select **Enabled** to enable HTTPS communication between the Jetdirect Print Server and any web browser (Figure 21).

Figure 21: Enabling HTTPS web communication.



## Encryption Strength

The Encryption Strength setting allows you to choose the strength of the encryption algorithm used for communication between the MFP EWS and the web browsers connecting to it (this is related to the **HTTPS Setting** option above). To configure the Encryption Strength setting:

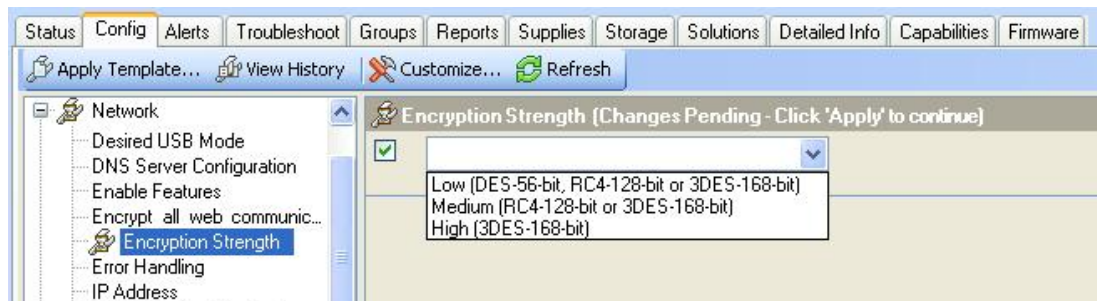
1. Click **Encryption Strength** in the **Network** category (Figure 22).

Figure 22: The Encryption Strength option.



2. Click the **Encryption Strength** dropdown menu, and select the highest setting that your browser supports (Figure 23).

Figure 23: The Encryption Strength dropdown menu.



## Error Handling

The Error Handling option (Figure 24) specifies how the Jetdirect Print Server handles error conditions. The settings are:

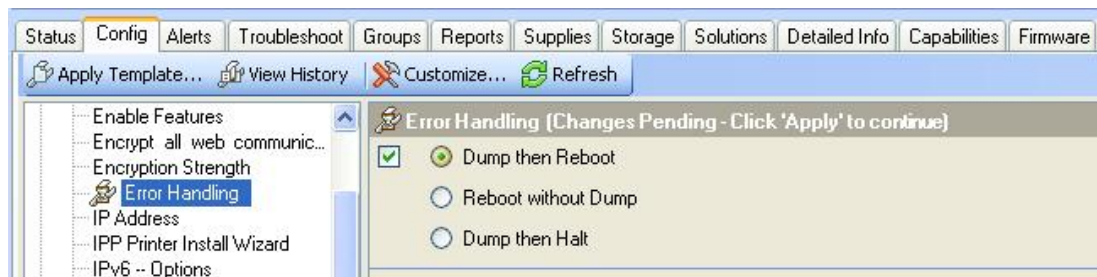
**Dump then Reboot** does a memory dump then reboots.

**Reboot Without Dump** reboots without dumping memory.

**Dump then Halt** does a memory dump but does not do a reboot; operations are halted.

Choose the setting that best fits your security needs.

Figure 24: The Error Handling option.

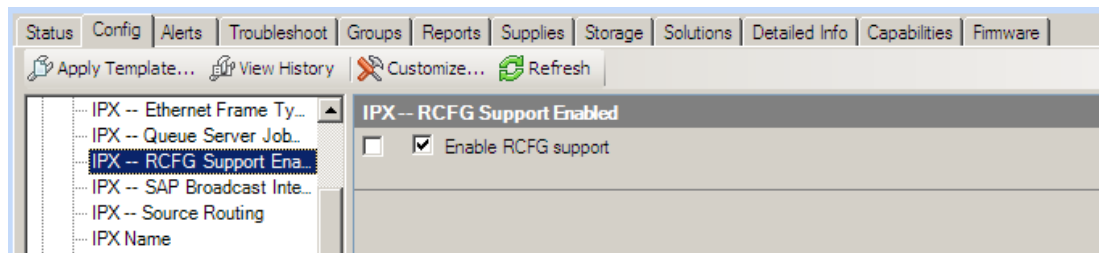


## IPX RCFG Support

This setting prevents access to configuration settings through Novell NetWare linkages; however, you should enable it if your network uses these linkages.

1. Click **IPX -- RCFG Support Enabled** (Figure 25), and leave **Enable RCFG Support** blank to disable it.

Figure 25: The RCFG Setting option.

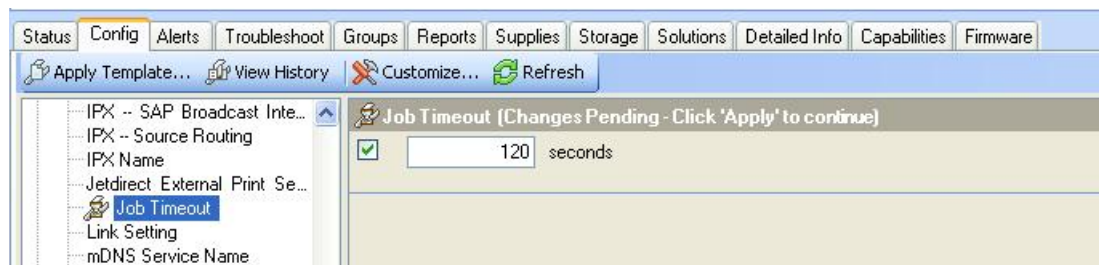


## Job Timeout

The Job Timeout option enables the MFPs to move on from jobs that lack proper end of job signals. The MFPs will be able to switch protocols to continue with other jobs. Not all MFPs support the **Job Timeout** option, so it will not appear for all models. To set the Job Timeout option:

1. Click **Job Timeout** (Figure 26).

Figure 26: The Job Timeout option.



2. In the input field, type a reasonable number of seconds for the MFPs to wait for an end of job before moving on.

## Privacy Setting

The Privacy Setting option is not considered a security-related setting. It is explained here to assure you that it does not compromise your network security. It 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 HP 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:

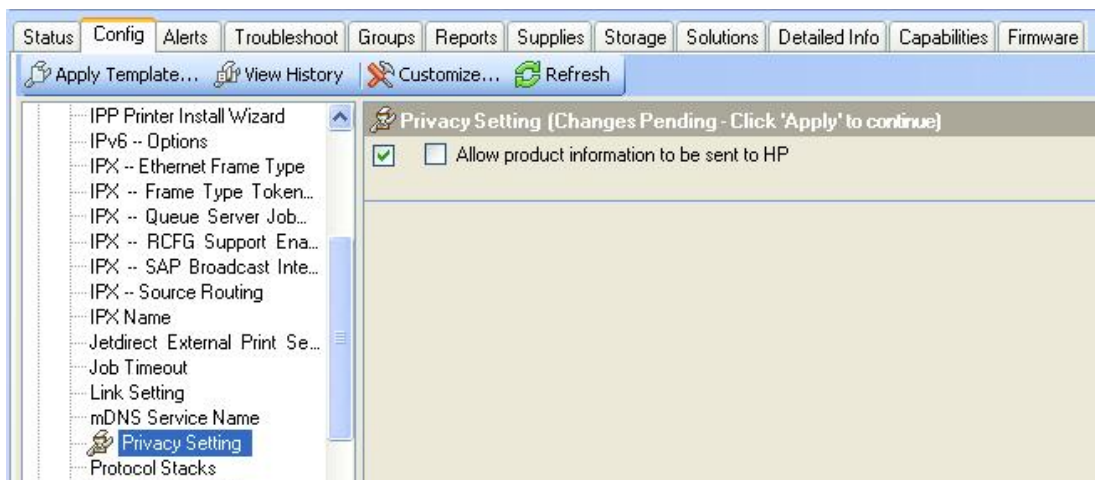
- HP Jetdirect product number, firmware version, and manufacturing date
- Model number of the MFP
- Web browser and operating system detected

- 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. To disable the Privacy Setting option:

1. Click **Privacy Setting** and uncheck the Allow product information to be sent to HP box (Figure 27).

Figure 27: Disabling the Privacy Setting option.

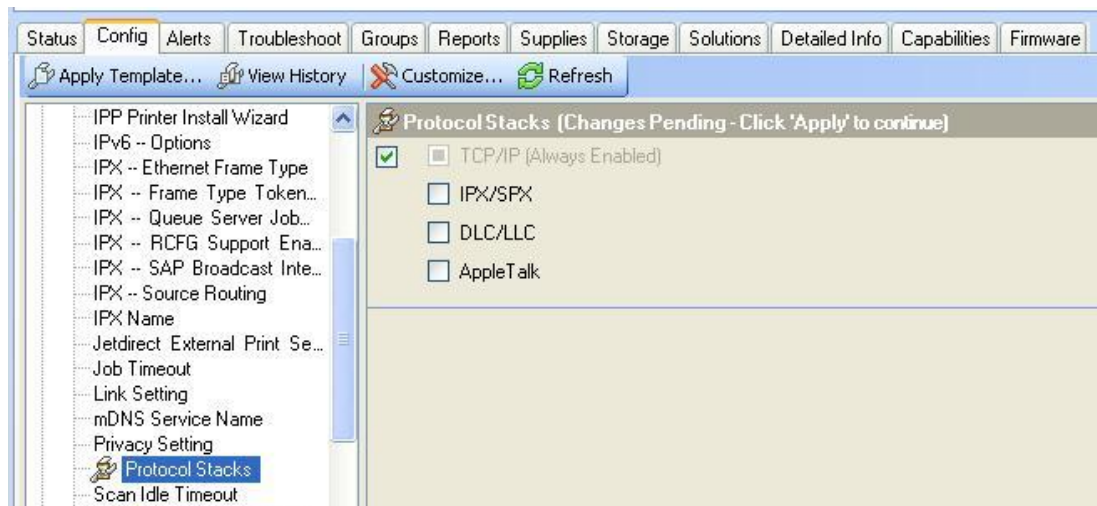


## Protocol Stacks

The Protocol Stacks option allows you to enable or disable certain print protocols used in your environment. To set your configuration:

1. Click to select **Protocol Stacks** (Figure 28), and deselect all unused protocol stacks as applicable to your network. See the table below.

Figure 28: The Protocol Stacks options.



The following table lists each protocol with the recommended setting and an explanation:

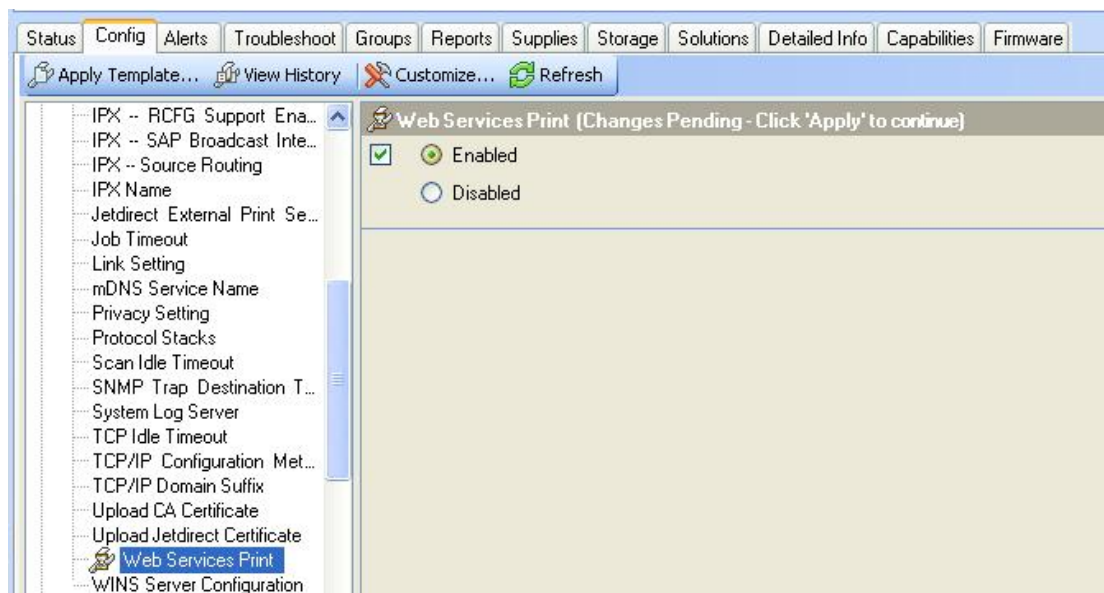
| Protocol Stack | Recommended Setting    | Explanation  |
|----------------|------------------------|--|
| IPX/SPX        | Leave blank to disable | This setting disables access for Novell servers.   |
| TCP/IP         | Always Enabled.        | This is the normal operating protocol for the MFPs.  |
| DLC/LLC        | Leave blank to disable | This setting enables the MFP to communicate at basic levels on the network. It should be disabled if not in use. |
| AppleTalk      | Leave blank to disable | This protocol provides access to older Apple and Macintosh computers. It should be disabled if not in use.       |

## Web Services Print

This option enables or disables the Microsoft Services for Devices WSD Print services supported on the HP Jetdirect Print Server.

1. Click to select **Web Services Print** (Figure 29), and select **Disabled**.

Figure 29: Enabling Web Services Print.

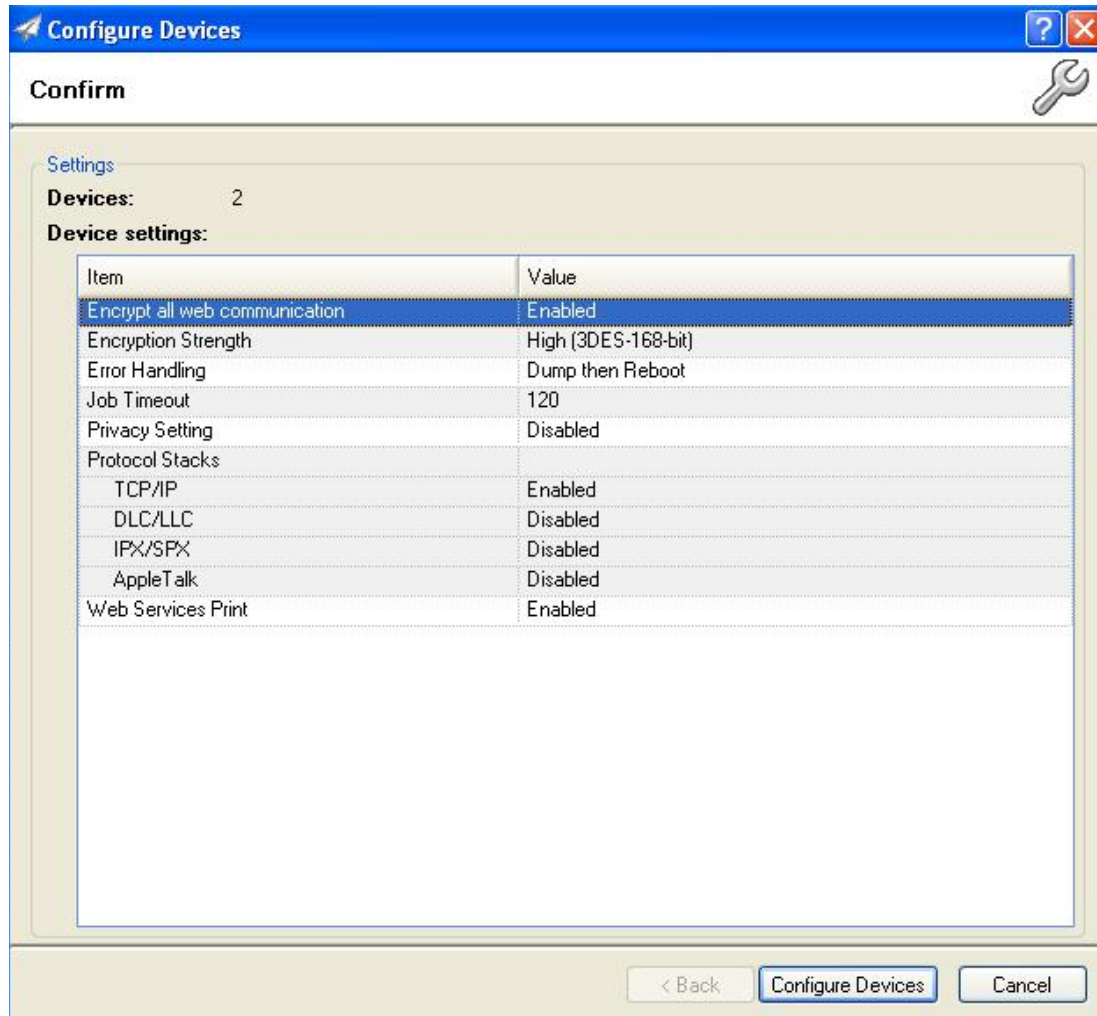




## Apply your Changes

1. Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices. This will open the configure devices dialogue box (Figure 30).

Figure 30: The Configure Devices dialogue box.



2. Review your settings and then click the **Configure Devices** button to execute the configuration.



## Configuring MFP Security Settings

The **Security** category includes many advanced security settings and password settings. If you are attempting to configure a setting that is in the Security category and not listed in this section, you should check the chapter on Advanced Security for multiple MFPs. To set the basic required settings in this category follow the steps in the sections below.

### Bootloader Password

The Bootloader password protects features, such as the MFP reset options that are available on the MFP control panel. These features are not commonly known, but they can severely affect the MFPs if they are executed improperly. The Bootloader password is not configured by default.

---

#### CAUTION:

Be very careful to remember the bootloader password that you provide. Once you configure the bootloader password, the bootloader features will be inaccessible permanently without it. The only way to restore the default setting and clear the password is to provide the correct password and set it with a blank password.

---

1. On the Config tab under the **Security** category page, select the **Bootloader Password** option (Figure 31)

Figure 31: The Bootloader Password option.



2. Type a password of 9 to 16 numeric digits in the **New Password** field, and repeat it exactly in the **Repeat Password** field.

---

#### Note:

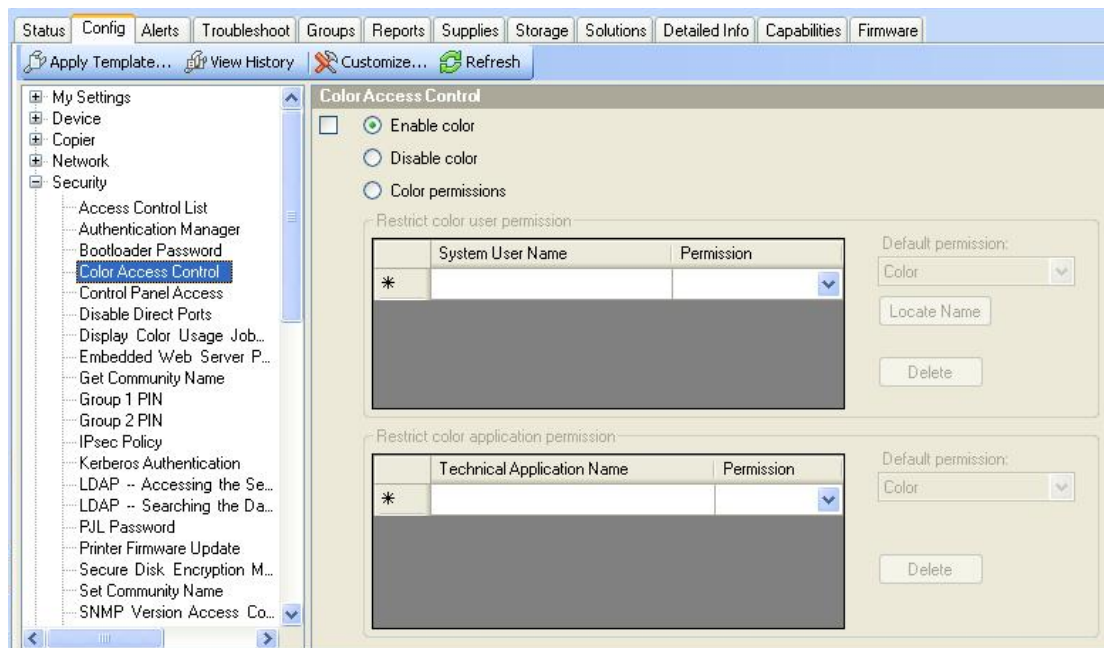
To reset (clear) this password, click to select Bootloader Password, type the correct current password, and leave the New Password and Repeat Password fields blank. Then click Configure, and the bootloader password will be cleared in the MFPs.

---

## Color Access Control

The Color Access Control options (Figure 32) allow you to manage the usage of color printing supplies within your organization. If you wish to restrict access to color printing you can configure these settings to match your policy.

Figure 32: The Color Access Control options.

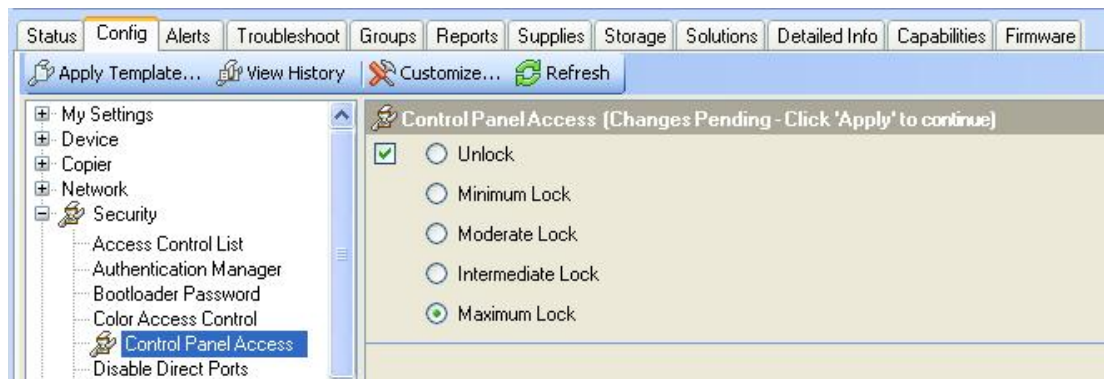


## Control Panel Access

The Control Panel Access Feature allows you to set the level of security on the physical control panel of your MFPs. **Maximum Lock** ensures that no one can access configuration settings in the control panel. To set Control Panel Access:

1. Click to select the **Control Panel Access** (Figure 33), and click to select **Maximum Lock**.

Figure 33: The Control Panel Access option.



**Note:**

This setting prevents access to configuration settings in the control panel, including digital send and fax settings. If you wish to make changes to settings in the control panel, unlock access using Web Jetadmin, make the changes, and then lock access again. See the Ramifications chapter for more information.

## Embedded Web Password

You can configure many of the settings in this checklist using the Embedded Web Server. To protect your MFP while configuring this checklist using Web Jetadmin it is important to set the Embedded Web Password. To do this, follow these instructions.

1. Click **Embedded Web Server Password** under the **Security** category (Figure 34).

Figure 34: The Embedded Web Server Password options.



2. Type a password of 8 to 16 characters in the **Embedded Web Server Password** field (you should always type the maximum number of characters for best security). This setting requires users to log on for parts of the EWS that provide configuration options.
3. Repeat the password exactly in the **Repeat Password** field.

---

**Note:**

The Embedded Web Server Password is synchronized with the Device Password (appears later in this checklist). If you change either the Embedded Web Server password or the Device Password, the MFP will configure both to be the same.

---

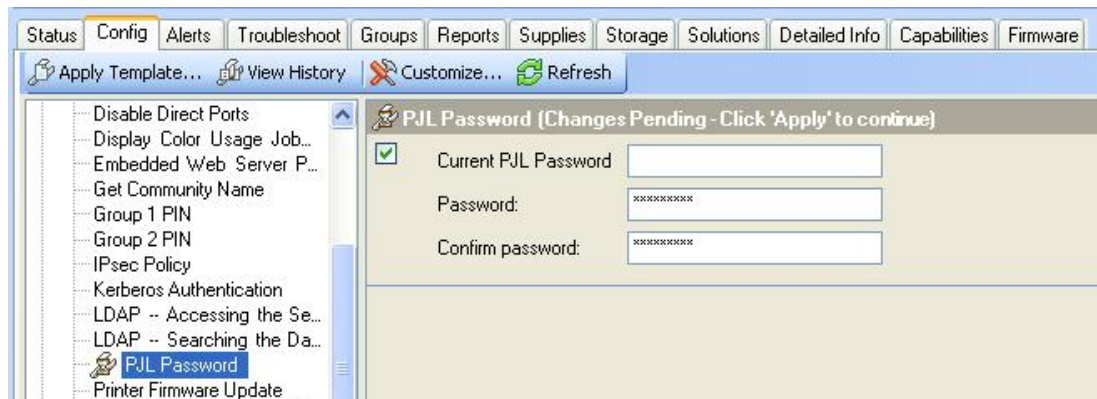
## PJL Password

The PJL password protects the default features on the MFP that can be changed by sending PJL commands to the MFP. The PJL password is required for administrative PJL commands that are used to modify feature settings. To set the PJL Password:

1. Click **PJL Password** under the **Security** category (Figure 35).

---

Figure 35: The PJL Password option.



2. Type a password that is any number between 1 and 2147483647 that is at least nine digits in length, and repeat it in the **Repeat PJL Password** field.

---

**Note:**

If you have problems configuring this password try configuring it through the EWS.

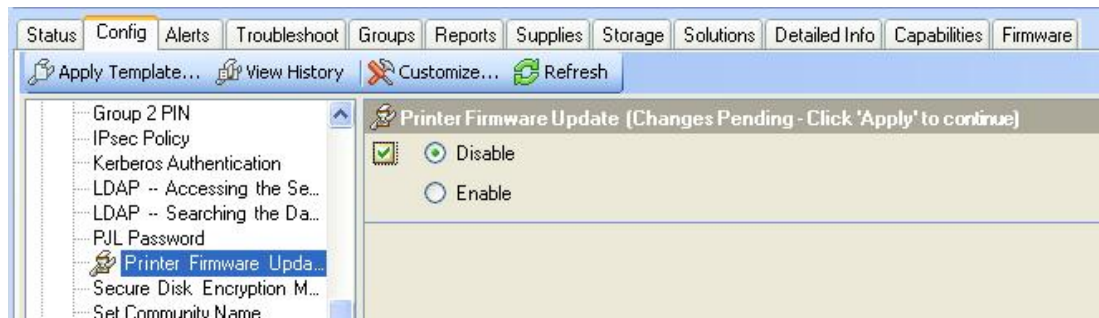
---

## Printer Firmware Update

HP recommends updating firmware whenever new firmware is available, but you should keep Printer Firmware Update disabled until you plan to use it. To disable Printer Firmware Update:

1. Click to select **Printer Firmware Update** (Figure 36), and select **Disable**.

Figure 36: The Printer Firmware Update option.



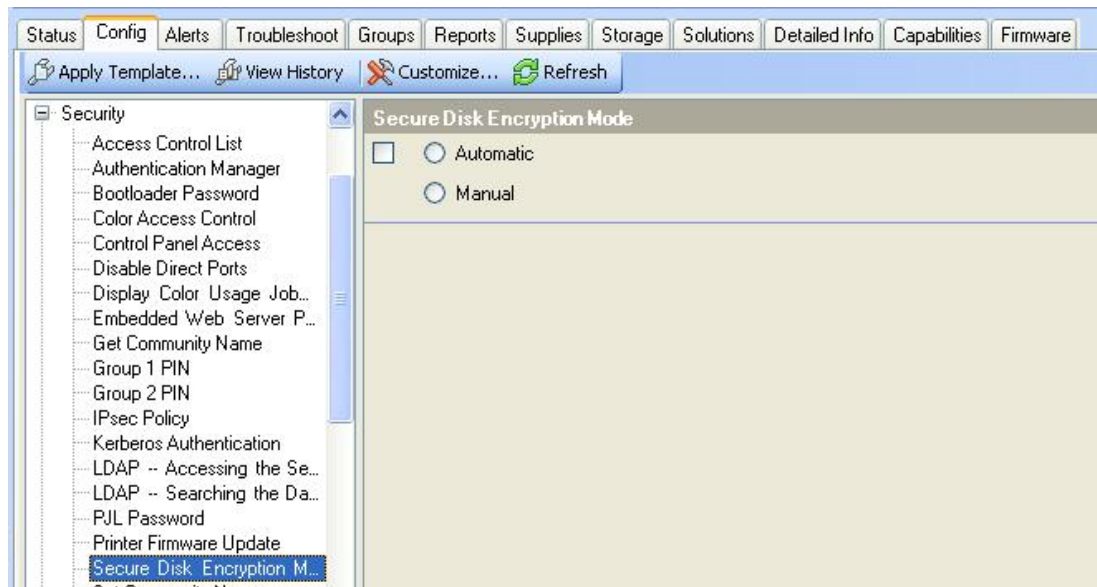
## Secure Disk Encryption Mode

The Secure Disk Encryption Mode option (Figure 37) determines whether encryption is automatically enabled when an HP Secure Hard Disk is installed. Automatic is the default and recommended mode.

### Note:

If you are configuring multiple devices and are not sure whether a manual password has been set on any of those devices it is recommended you skip this step in the configuration.

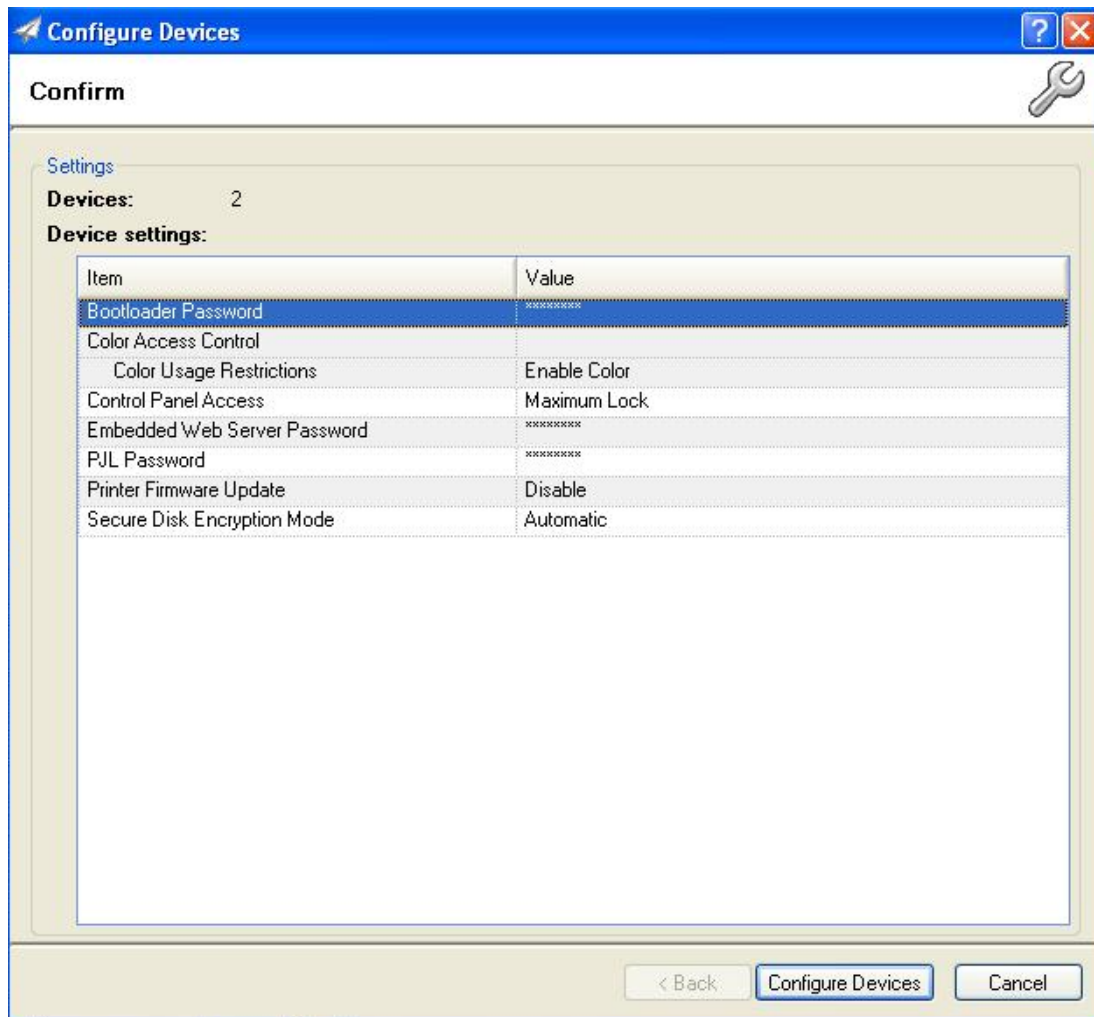
Figure 37: The Secure Disk Encryption Mode option.



### Apply the Changes

1. Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices. This will open the configure devices dialogue box (Figure 38).

Figure 38: The Configure Devices dialogue box.



2. Review your settings and then click the **Configure Devices** button to execute the configuration.



## Configuring MFP Fax Settings

The **Fax** Category provides options for the analog fax functions. This includes settings to allow for printing fax jobs when the recipient is present and for restricting access to fax print jobs.

### Configuring Fax Printing

Follow these instructions to configure Fax Printing:

#### Note:

Be sure to configure the MFPs for fax capabilities before continuing with the instructions below. At the minimum, configure the modem settings for the country, the company, and the phone number.

1. Click **Fax** on the **Config** tab, and select **Fax Printing** (Figure 39).

Figure 39: The Fax Printing options.

The screenshot shows the HP MFP configuration interface. The top navigation bar includes tabs: Status, Config, Alerts, Troubleshoot, Groups, Reports, Supplies, Storage, Solutions, Detailed Info, Capabilities, and Firmware. The 'Config' tab is active. Below the navigation bar are buttons: Apply Template..., View History, Customize..., and Refresh. The left sidebar shows a tree view with 'Fax' expanded and 'Fax Printing' selected. The main area is titled 'Fax Printing (Changes Pending - Click 'Apply' to continue)'. It contains the following settings:

- ☒ PIN number: [text field with 'xxxx']
- Confirm PIN number: [text field with 'xxxx']
- ☐ Print All Received Faxes
- ☒ Store All Received Faxes
- ☐ Use Fax Printing Schedule

|                                     | Week day  | Start printing faxes | Stop printing faxes |
|-------------------------------------|-----------|----------------------|---------------------|
| <input type="checkbox"/>            | Sunday    | 8:00 AM              | 5:00 PM             |
| <input checked="" type="checkbox"/> | Monday    | 8:00 AM              | 5:00 PM             |
| <input checked="" type="checkbox"/> | Tuesday   | 8:00 AM              | 5:00 PM             |
| <input checked="" type="checkbox"/> | Wednesday | 8:00 AM              | 5:00 PM             |
| <input checked="" type="checkbox"/> | Thursday  | 8:00 AM              | 5:00 PM             |
| <input checked="" type="checkbox"/> | Friday    | 8:00 AM              | 5:00 PM             |
| <input type="checkbox"/>            | Saturday  | 8:00 AM              | 5:00 PM             |

2. Enter a four-digit number in the **PIN Number** field, and repeat it in the **Confirm PIN Number** field. This setting requires users to provide the PIN number to print stored Fax jobs.



---

**Note:**

This setting also enables PIN printing.

---

### 3. **Select Store all Received** Faxes.

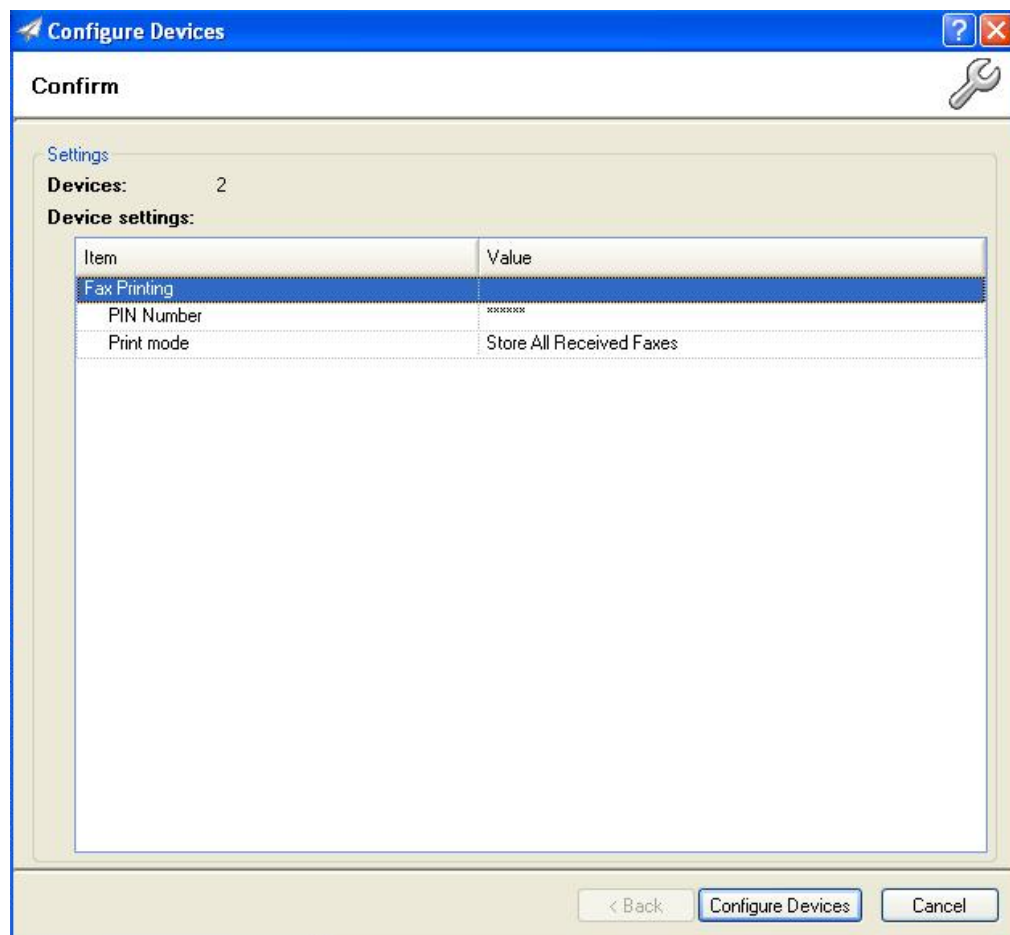
The Store all Received Faxes option holds incoming faxes for printing until someone enters the correct PIN number and selects the menu options at the control panel. This is considered the most secure mode of fax printing. You may wish to use the fax scheduling options to print all faxes at a time when security is optimal.

## Apply the Changes

1. Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices. This will open the configure devices dialogue box (Figure 40).

---

Figure 40: The Configure Devices dialogue box.



2. Review your settings and then click the **Configure Devices** button to execute the configuration.

## Additional Fax Configuration

Some of the newer MFPs or recently upgraded MFPs may contain options for setting and locking down the Fax speed-dial feature. This Fax feature is not yet accessible via Web Jetadmin 10.2. To set your MFP speed-dial options follow the steps below.

1. Open the Embedded Web server for your MFP by entering the IP address of the printer into address field of your web browser and click the fax tab (Figure 41).

Figure 41: The Fax Settings Page.

The screenshot shows the 'Fax Settings' page. The top navigation bar has tabs for 'Information', 'Settings', 'Digital Sending', 'Fax', and 'Networking'. The 'Fax' tab is selected. The left sidebar has a menu with 'Fax Settings' (highlighted), 'Fax Address Book', 'Fax Speed Dials', 'Other Links', 'hp instant support', 'Shop for Supplies', and 'Product Support'. The main content area is titled 'Fax Settings'. It contains a 'Send Faxes...' dropdown menu set to 'directly from the device's internal modem'. Below this is a section titled 'Device Modem Settings' with the following fields: 'Country/Region:' (dropdown set to 'Argentina'), 'Company Name:' (text input), 'Dialing Prefix:' (text input), and an 'Enable Dialing Prefix' checkbox.

2. Click to select Fax Speed Dials on the left hand menu (Figure 42).

Figure 42: Fax Speed Dials selection and page.

The screenshot shows the 'Fax Speed Dials' page. The top navigation bar has tabs for 'Information', 'Settings', 'Digital Sending', 'Fax', and 'Networking'. The 'Fax' tab is selected. The left sidebar has a menu with 'Fax Settings', 'Fax Address Book', 'Fax Speed Dials' (highlighted), 'Other Links', 'hp instant support', 'Shop for Supplies', and 'Product Support'. The main content area is titled 'Fax Speed Dials'. It contains the text: 'This page lets you add, edit, or delete fax speed dials on the device. Click **Help** for more information.' Below this is a section titled 'Edit or delete a speed dial.' with two bullet points: 'To create or edit a speed dial, select the speed dial in the list and then click **Edit Speed Dial**.' and 'To clear the fax numbers from a speed dial, select the speed dial in the list and then click **Clear Speed Dial**.' At the bottom, there is a table with two columns: 'Speed Dial' and 'Members'. The table shows one entry with 'Speed Dial' set to '[0]' and 'Members' set to 'available'.

3. Set any speed-dials you wish to have by selecting the speed-dial number and clicking the Edit Speed Dial button (Figure 43).

Figure 43: The Fax Speed Dials configuration button.

**Edit or delete a speed dial.**

- To create or edit a speed dial, select the speed dial in the list and then click **Edit Speed Dial**.
- To clear the fax numbers from a speed dial, select the speed dial in the list and then click **Clear Speed Dial**.

| Speed Dial | Members   |
|------------|-----------|
| [ 0 ]      | available |
| [ 1 ]      | available |
| [ 2 ]      | available |
| [ 3 ]      | available |
| [ 4 ]      | available |
| [ 5 ]      | available |
| [ 6 ]      | available |
| [ 7 ]      | available |

**Edit Speed Dial...** **Clear Speed Dial...** **Clear All...**

**Lock Speed Dials**

4. To keep speed-dial entries from being added or edited via the control panel input the number of the specific speed-dials you wish to lock. We recommend locking all speed-dial entries from modification. To do this, enter 0-99 in the box and select Save (Figure 44).

Figure 44: The Fax Speed Dials lockdown box

**Lock Speed Dials**

Prevent user from editing Speed Dials (e.g., 0-20)

**Save**

# Configuring MFP Embedded Web Server Settings

## Embedded Web Server Configuration Options

Each MFP has an Embedded Web Server that provides network access to view MFP status, to set preferences, and to configure the MFP. You can view an MFP Embedded Web Server by typing the MFP IP address into a web browser. This section covers settings that Web Jetadmin access through the EWS.

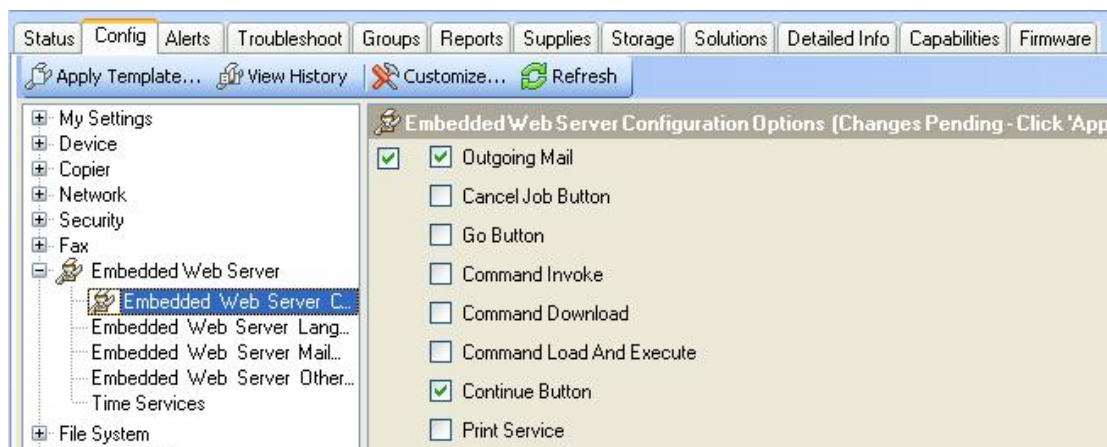
### Note:

Later, at the end of this checklist, you will disable EWS Config, which disables all of the functions of EWS including those managed in Web Jetadmin. Now, however, you should configure the settings below for security while EWS Config is enabled.

Follow these instructions:

1. Click the **Embedded Web Server** category to select **Embedded Web Server Configuration Options** (Figure 45).

Figure 45: The Embedded Web Server Configuration Options.



2. Click to enable **Continue Button** and **Outgoing Mail**, and leave the remaining options blank. See below for more information:

The **Embedded Web Server Configuration Options** are either enabled or disabled in this menu. They will be reconfigured regardless of their current state (which is not displayed). If you select an option, you are enabling it; if you leave an option blank, you are disabling it.

The following table lists the recommended setting for each item in this list:

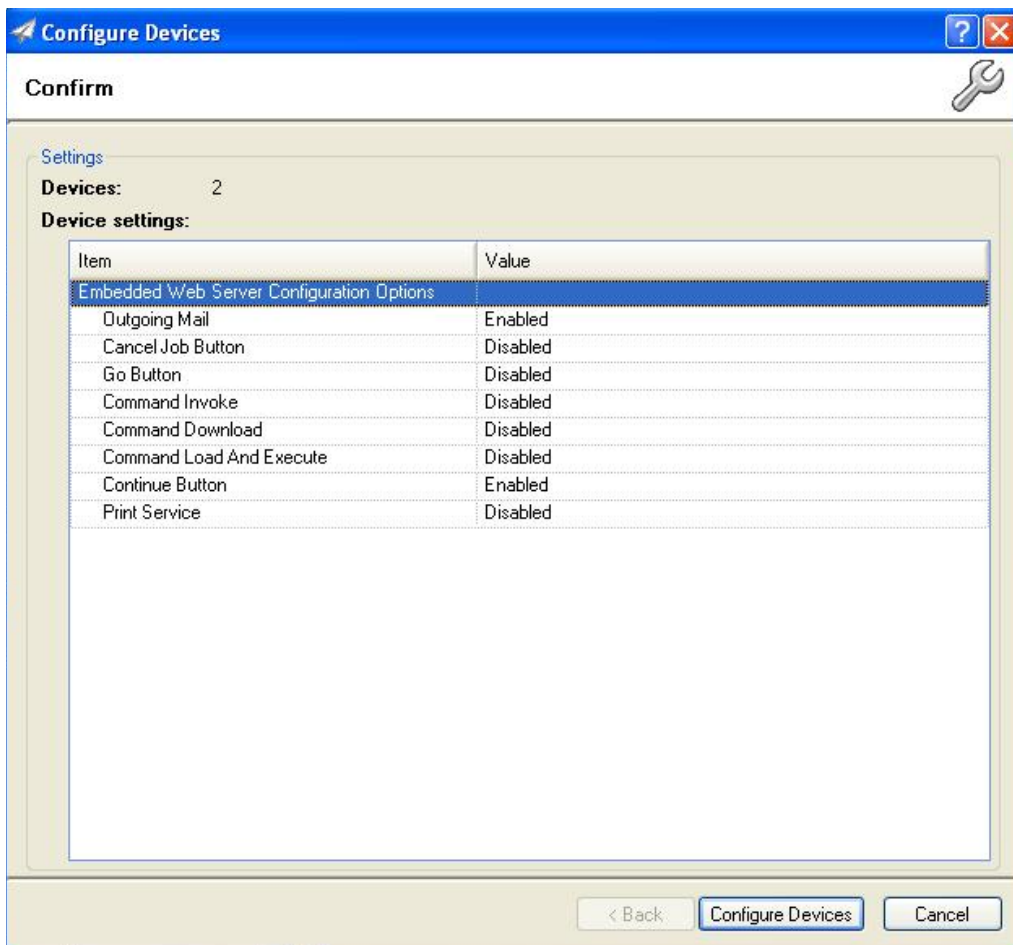
| <b>Embedded Web Server Configuration Option</b> | <b>Recommended setting</b> | <b>Explanation</b>   |
|---|----------------------------|--|
| Outgoing Mail (enabled by default)              | Enable as desired          | <b>Outgoing Mail</b> enables the MFP to send alerts and AutoSend messages to a designated recipient. This is not necessarily a security-related feature. Use it as you see fit.<br><br>This setting does not affect the MFP Send to Email feature. |
| Incoming Mail (disabled by default)             | Leave blank to disable     | Normally, the MFP does not receive incoming mail; however, some legitimate network solutions might use it for certain communications. Unless your network is using it, you should disable <b>Incoming Mail</b> .                                   |
| Cancel Job Button (disabled by default)         | Leave blank to disable     | Disabling <b>Cancel Job Button</b> prevents users from remotely cancelling the jobs of others.   |
| Go Button (enabled by default)                  | Leave blank to disable     | Disabling <b>Go Button</b> prevents users from delaying or stopping the jobs of others. It is the Pause/Resume button in the MFP EWS.  |
| Command Invoke (enabled by default)             | Leave blank to disable     | <b>Command Invoke</b> does not apply to the MFPs. Disabling it is only a best practice.  |
| Command Download (enabled by default)           | Leave blank to disable     | <b>Command Download</b> does not apply to MFPs. Disabling it is only a best practice.  |
| Command Load and Execute (enabled by default)   | Leave blank to disable     | <b>Command Load and Execute</b> enables the MFPs to install and run Chai services, such as workflow applications and job accounting solutions. You should disable it unless you are using installed applications on your MFPs.                     |

|                                      |                        |   |
|--------------------------------------|------------------------|---|
| Continue Button (enabled by default) | Select to enable       | <b>Continue Button</b> allows the MFPs to resume after an error has been cleared.   |
| Print Service (enabled by default)   | Leave blank to disable | <b>Print Service</b> enables users to send print-ready files directly to an MFP without having the MFP installed on a computer. |

## Apply the Changes

1. Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices. This will open the configure devices dialogue box (Figure 46).

Figure 46: The Configure Devices dialogue box.



2. Review your settings and then click the **Configure Devices** button to execute the configuration.

## Configuring MFP File System Settings

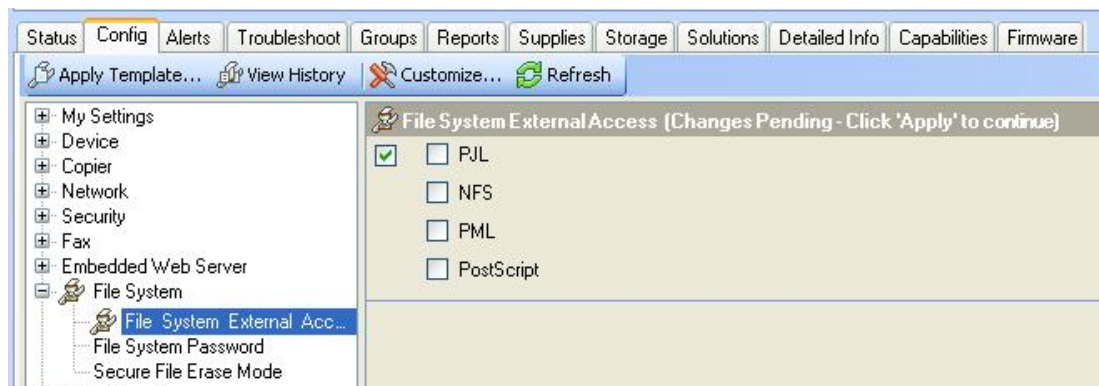
The **File system** category provides settings for access to the MFP hard drive, the Compact Flash card, and optional data storage devices. Several security settings are available that can help prevent unauthorized access to data.

### File System External Access

It is recommended that all external access to the file systems on your MFPs be disabled. To do so, follow these instructions:

1. Click the **File System** category to select **File System External Access** (Figure 47).

Figure 47: The File System External Access options.



2. Disable all options (see the table below).  
The following table lists and explains the recommended settings:

| File system Access Option | Recommended Setting | Explanation  |
|---------------------------|---------------------|--|
| P/L                       | Disabled            | Prevents access to the file system through this protocol   |
| PML                       | Disabled            | Prevents access to the file system through this protocol   |
| NFS                       | Disabled            | Prevents access to the file system through this protocol<br><br>NOTE: Disabling the NFS option disables the entire |

|            |          |  |
|------------|----------|--|
|            |          | protocol for the MFPs.   |
| PostScript | Disabled | Prevents access to the file system through this protocol.<br><br>NOTE: Disabling PostScript may affect interactions with third party applications. |

## File System Password

When a File System Password is set, the MFPs will require the password whenever anyone or any device requests access to the storage devices. To set the File System password follow the instructions below:

1. Click to select **File system Password** (Figure 48).

Figure 48: The File system Password option.



2. Type an 8 character password in the **File System Password** field, and repeat it exactly in the **Confirm Password** field.

### Note:

When Web Jetadmin is used to configure MFPs, it saves all of the passwords, including credentials for SNMPv3, in an encrypted device cache. As long as an authorized administrator is logged into Web Jetadmin, it will supply the passwords automatically without prompting.

3. Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices. This will open the configure devices dialogue box.
4. Review your settings and then click the **Configure Devices** button to execute the configuration.



## Secure File Erase Mode

This setting determines the level of overwriting applied to delete files during routine functions. This includes removal of files for the Secure Storage Erase function. The settings are:

**Non-secure Fast Erase** does a standard erase with no additional security.

**Secure Fast Erase** overwrites files using one pass. This takes some extra time, but it provides reasonable security.

**Secure Sanitizing Erase** overwrites files with three passes. It noticeably slows the MFP, but it ensures that files are completely unrecoverable.

Use **Secure Sanitizing Erase** to meet stringent security requirements such as Department of Defense standards.

---

### Note:

Secure File Erase requires that the File System Password be configured. If you are following this checklist in order this should not be an issue.

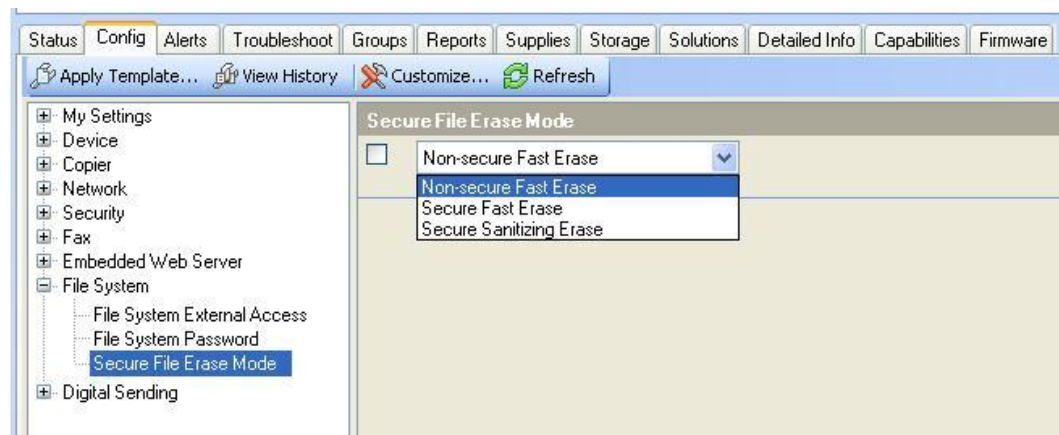
---

To set the Secure File Erase Mode follow these instructions:

1. Click to select **Secure File Erase Mode** (Figure 49), and view the options in the dropdown menu.

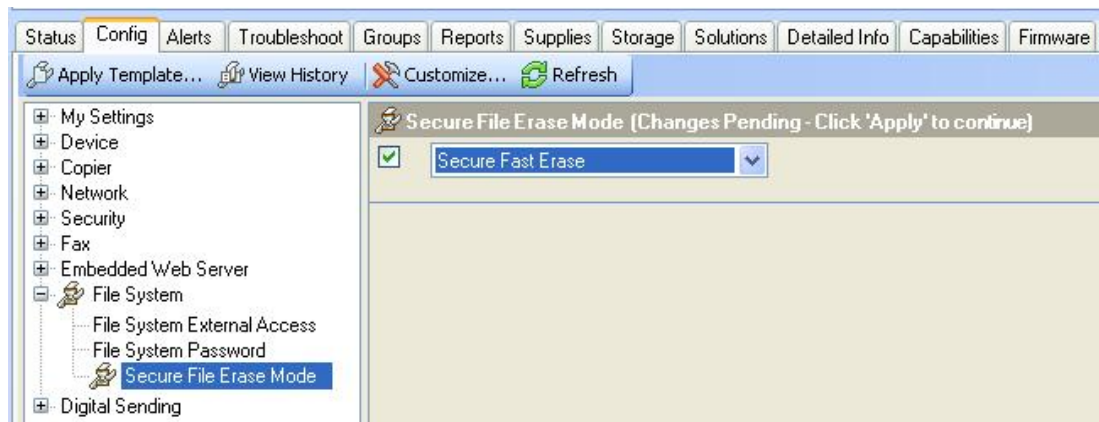
---

Figure 49: The Secure File Erase Mode setting.



2. Select **Secure Fast Erase** (Figure 50) or **Secure Sanitizing Erase** if you require maximum security.

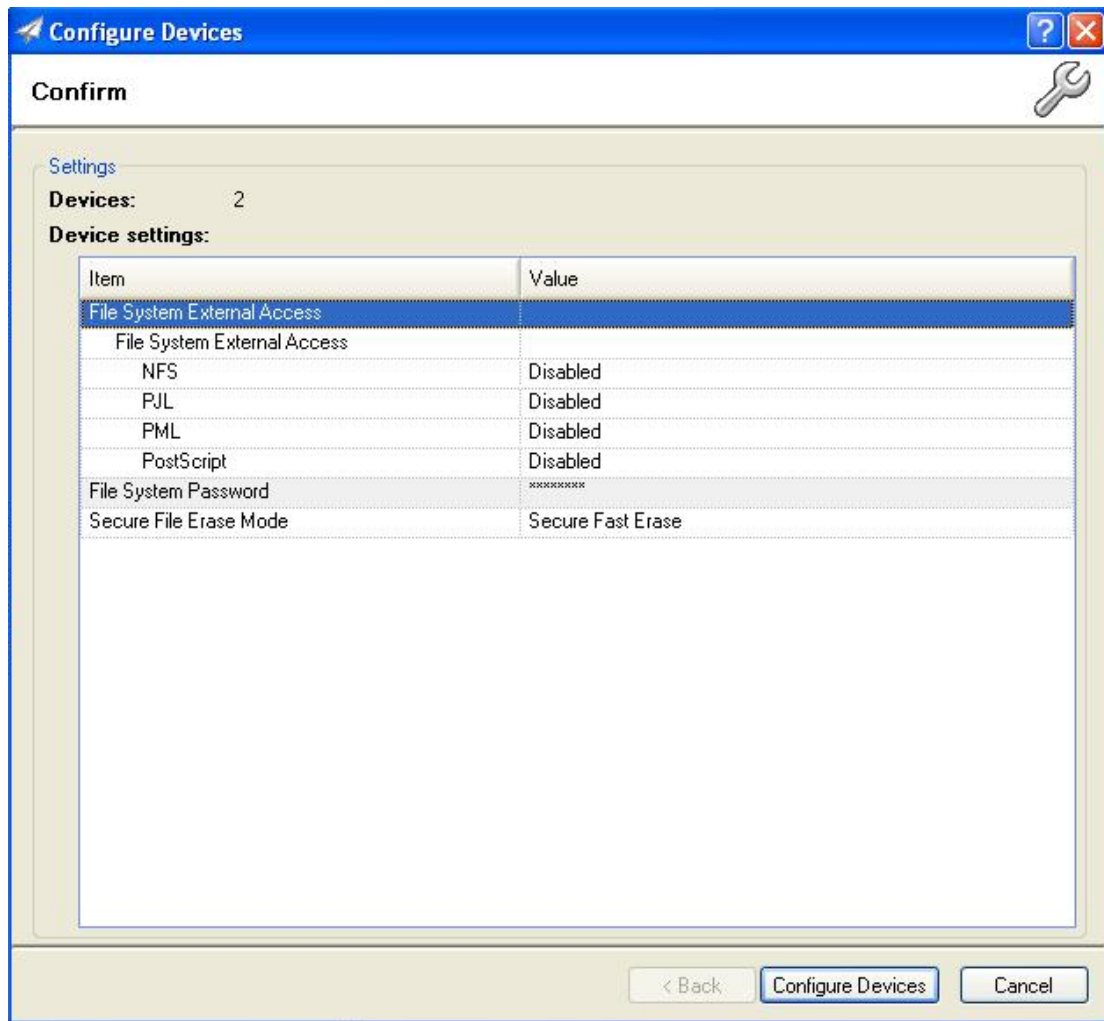
Figure 50: The Secure File Erase Mode setting.



### Apply the Changes

5. Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices. This will open the configure devices dialogue box (Figure 51).

Figure 51: The Configure Devices dialogue box.



6. Review your settings and then click the **Configure Devices** button to execute the configuration.

## Configuring MFP Digital Sending Settings

The **Digital Sending** category includes options for email and for send to network folder. This includes settings for protecting the sender identification fields.

---

### Note:

Some security-related settings that do not apply to LaserJet and Color LaserJet MFPs might appear on the Digital Sending page. These settings are for other types of HP MFPs. You should configure the settings that appear in the instructions below. You may wish to configure the other settings as a safeguard, but they are ignored on devices that do not support them.

---

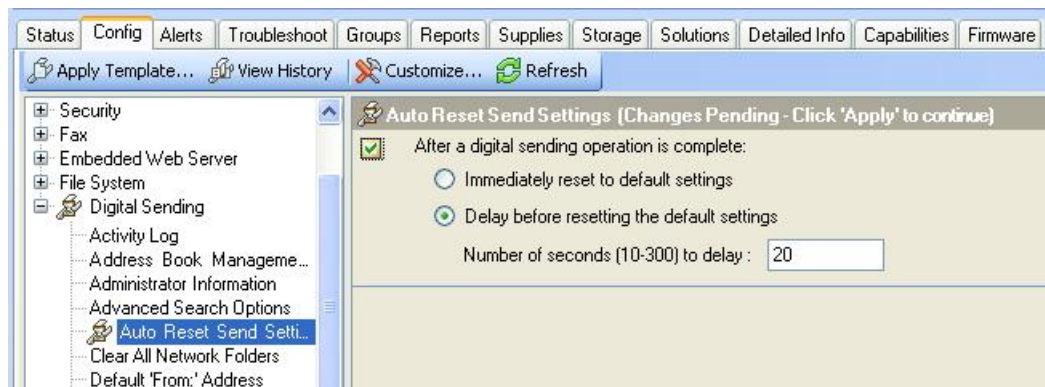
### Auto Reset Send Settings

This setting governs how long after sending a job the device waits to log off the current user and reset the control panel. Selecting **delay before resetting the default settings** allows users to send multiple digital send jobs (email, send to folder, & fax) to a location without having to retype all of the information in the control panel. It ensures that the information displayed on the control panel resets automatically when a user walks away without clearing the menu. The setting only applies to digital send jobs. To configure this setting:

1. Click to select **Auto Reset Send Setting** from the **Digital Sending** category (Figure 52).

---

Figure 52: The Time-outs options.



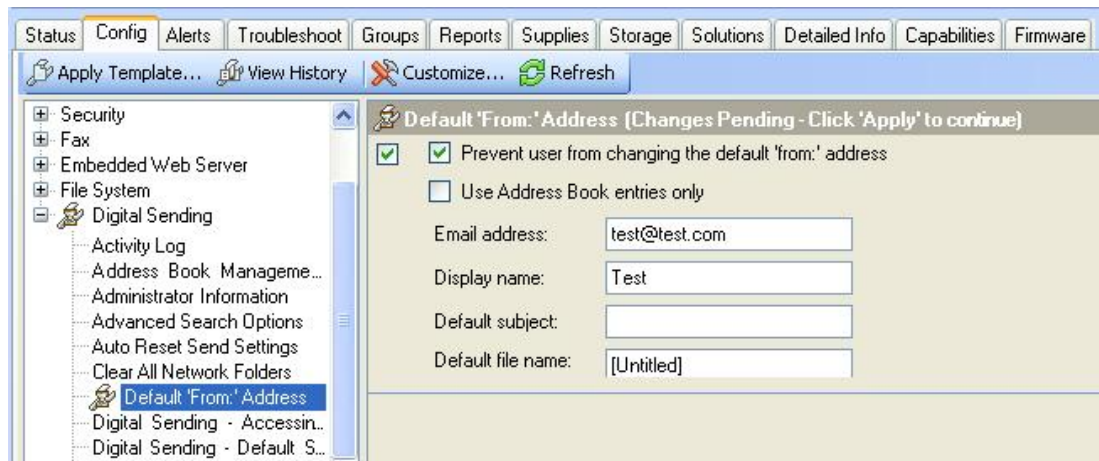
2. Select Delay before resetting the default settings.
3. Choose a reasonable time to allow users to send multiple jobs, but also to ensure that the information will not be left on the control panel for too long after the user walks away.

## Default From Address

HP recommends configuring the default from address to ensure that no one can send email using false or misleading identification. If you are using LDAP Authentication, the MFP will use the email address of the authenticated user to replace the default from address. To configure the **Default 'From:' Address**:

1. Scroll down, and click to select **Default 'From:' Address** (Figure 53).

Figure 53: The Default From Address options.



2. Click to select Prevent user from changing the Default 'From:' Address.
3. Fill in the **Email Address** field with any address that includes the ampersand (@).

### Tip:

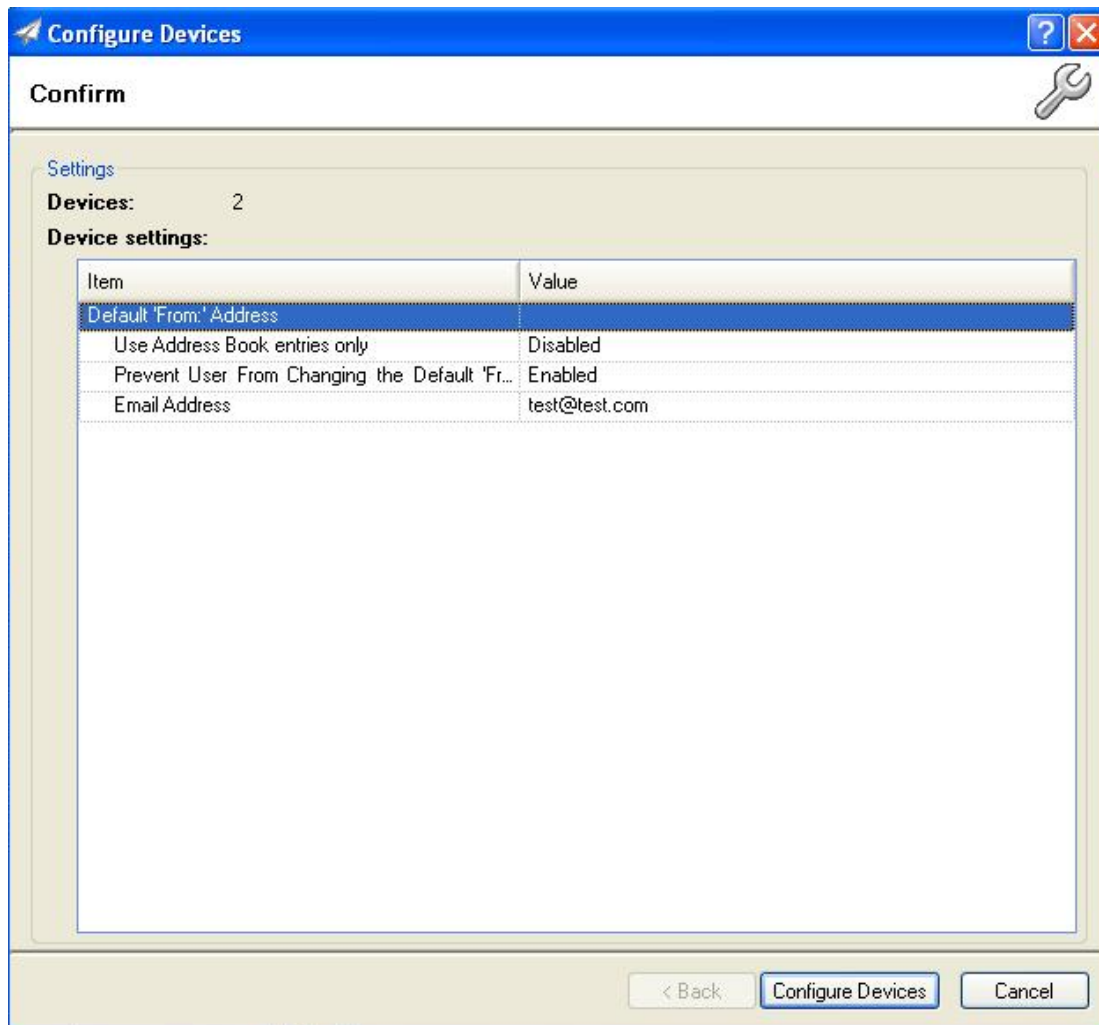
You may wish to use the email address of an administrator who can receive responses such as e-mail and send notices and failures.

4. Fill in the **Display Name** and the **Default Subject** fields as desired.

## Apply the Changes

1. Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices. This will open the configure devices dialogue box (Figure 54).

Figure 54: The Configure Devices dialogue box.



2. Review your settings and then click the **Configure Devices** button to execute the configuration.

## Configuring Final Settings

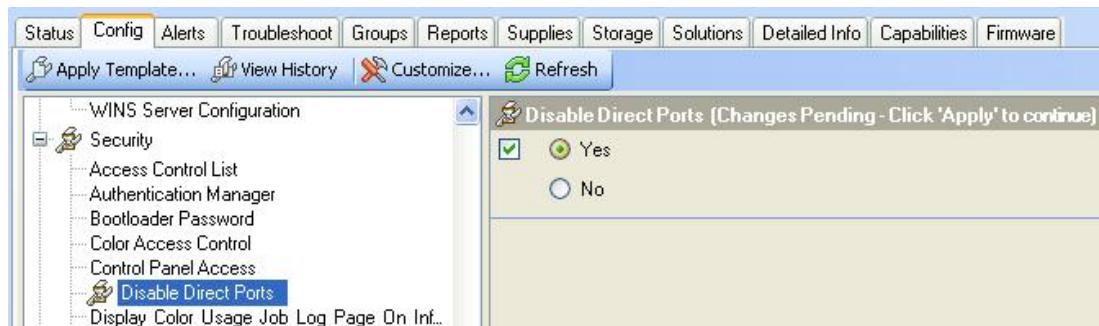
Some of the MFP settings should be configured independently from other settings and only at the end of this checklist. Follow these instructions for the final settings:

### Disabling Direct Ports

The Disable Direct Ports feature disables the USB and Parallel ports on the MFPs. It ensures that only network-connected computers can access the MFPs. In order to configure this feature, each MFP will turn off and turn on automatically. To disable these ports:

1. Go to the **Security** page, and click to select **Disable Direct Ports** (Figure 55).

Figure 55: The Disable Direct Ports option.



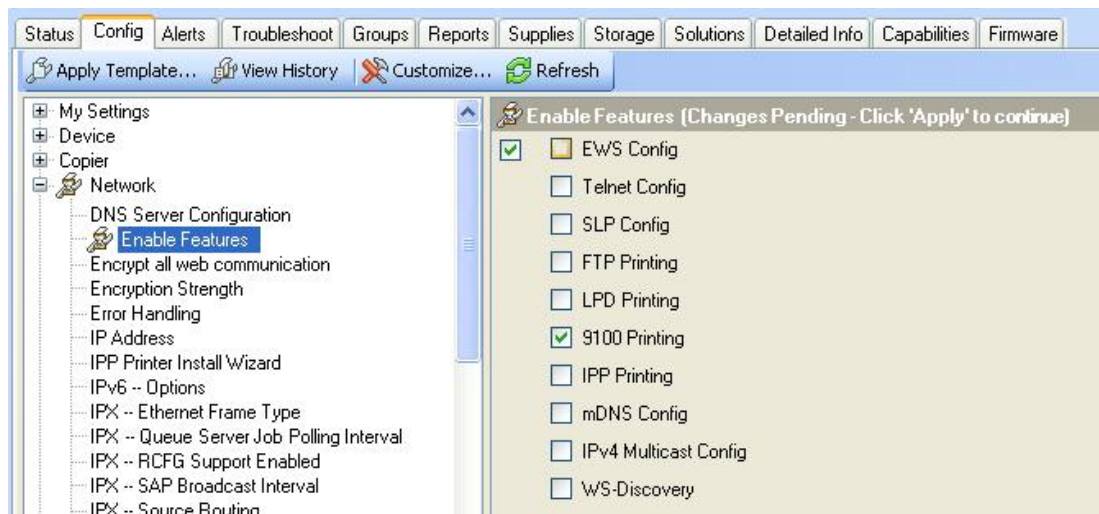
2. Click to select the **Disable Direct Ports** option to the right.
3. Select **Yes**.
4. Click **Apply** at the bottom of the page.
5. Wait for a few minutes to allow all of the MFPs to restart. Do not continue until all of them are at the READY state.

## Disabling EWS Config

EWS Config was required for configuring this checklist, but it should be disabled during normal use of the MFPs. To disable EWS Config:

1. Go to the **Network** category, and click to select **Enable Features** (Figure 56).

Figure 56: The Enable Features option.



2. Click to disable **EWS Config**.

---

**Note:**

This setting disables configuration from the MFP EWS. It also disables all EWS-related settings from Web Jetadmin (they will disappear from Web Jetadmin menus). With this setting configured, the only way to make changes to the EWS settings again is to re-enable them using Web Jetadmin. Always remember to disable EWS Config after making changes.

---

Your MFPs are now securely configured.



## Chapter 4: Advanced Security for Multiple MFPs

This chapter gives some tips for configuring more advanced security settings for one or more MFPs using HP Web Jetadmin. These features should be set up before locking down your MFPs using the settings in the previous chapter. This allows adequate testing of your security solution to be completed while you still have open access to your devices. If you are looking for information in this section that is not contained in this document you can refer to the MFP User Guides and the HP Jetdirect Administrator Guide for more information. You can find these documents and more information by searching for it at [hp.com](http://hp.com).

### Access Control List (ACL)

The ACL limits network access to the MFPs to only the IP addresses or subnets that you specify. This includes printing and all other access. Thus, to access the device an administrator must use a computer that is on the list, have the correct Web Jetadmin password, and then have the correct SNMPv3 credentials to manage the MFPs.

The following MFP models also have a Jetdirect Firewall feature along with the Access Control List:

- HP LaserJet M3027 MFP
- HP LaserJet M3035 MFP
- HP LaserJet M4345 MFP
- HP LaserJet M5025 MFP
- HP LaserJet M5035 MFP
- HP LaserJet M9040 MFP
- HP LaserJet M9050 MFP
- HP Color LaserJet CM3530 MFP
- HP Color LaserJet CM6030 MFP
- HP Color LaserJet CM6040 MFP

HP Web Jetadmin may not provide options to configure the Jetdirect Firewall settings. Look for them in the MFP EWS.

---

#### Note:

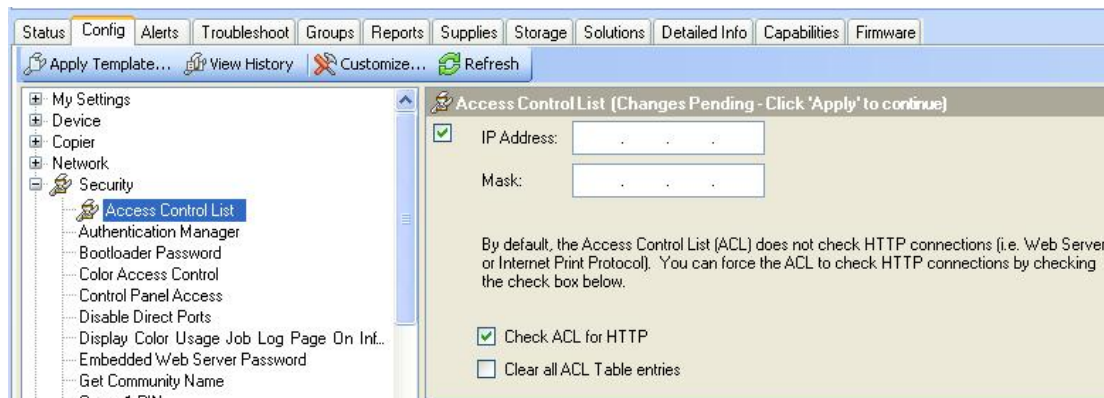
Keep in mind that the ACL is not configured until at least one computer is in the list. When it is configured, no computer outside the list will have access to the MFP including printing.

---

Follow these steps to configure the ACL:

1. On the **Config** tab click **Access Control List** (Figure 57) under the **Security** Category.

Figure 57: The Configuration Categories Menu Network option.



2. Add an IP address or a net mask by filling in the **IP Address** or **Mask** fields.

**CAUTION:**

Be sure to include the IP address of the computer that is running Web Jetadmin (it can be a computer other than the one you are using). Otherwise, the ACL will block your access, and you will not be able to continue.

The Mask option requires an entry in the IP address field to determine the subnet for which to grant access. If you set a mask be sure it is correct before moving on.

3. To make sure all of the MFPs are configured with your new listings, click **Clear all ACL Table entries** the first time you add a listing.

**Note:**

To find out which IPs are configured in the ACL of a single MFP, open the device in Web Jetadmin and navigate to the ACL options (all of the MFPs should be the same if you are configuring them all at once). It will list the IP addresses or subnets that are already configured.

4. Check the checkbox for **Check ACL for HTTP access** to ensure that the ACL restricts access to the MFP EWS through HTTP.

**Note:**

These ACL options allow you to add one IP address or one mask at a time. To add more IPs or masks, repeat these steps. Remember to deselect Allow Web Server (HTTP) access each time.

## Authentication Manager

The Authentication Manager allows you to customize access to functions of the MFP. You can use these options to provide varying services to different groups of people.

1. Click to select **Authentication Manager** (Figure 58).

Figure 58: The Authentication Manager options.

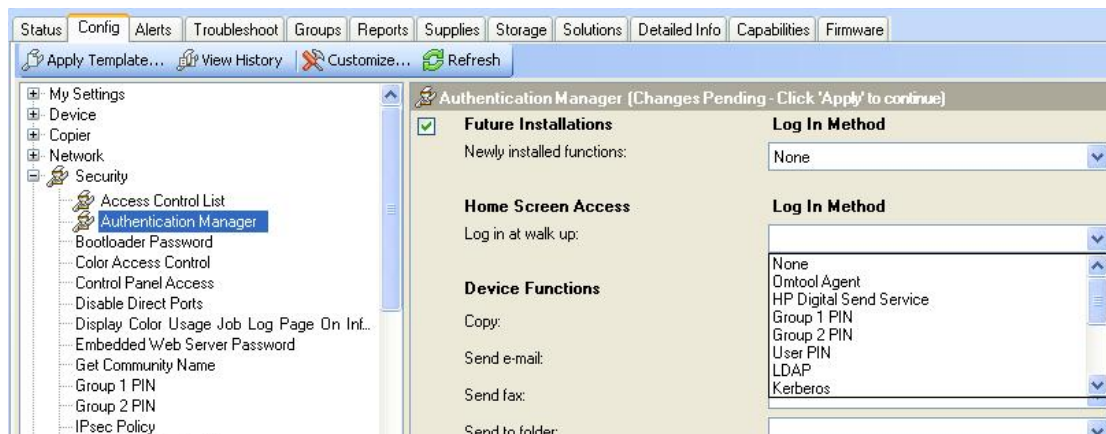


### Note:

Be sure to select only the authentication features that you plan to configure for the MFPs selected. Many of the options available (such as LDAP, Kerberos, and Digital Send Service) require additional solutions on the network for support.

2. Click the dropdown menu next to **Log in at Walk Up**, and select from the list (Figure 59).

Figure 59: The drop down menu for Log in at Walk Up.



Choosing an authentication method for **Log in at Walk Up** causes the MFP to require everyone to log in for access to the control panel menus. You can choose to require further authentication for specific functions of the MFP.

Choose an authentication method for each device function as desired. If you choose to use different log in methods for each device function, the MFP will require authentication as needed. The MFP automatically allows authenticated users to continue whenever they are allowed to use a feature.

**Note:**

The DSS Secondary E-mail function and the DSS Workflow function require HP Digital Send Service to be installed on the Network. Digital Send Service is an additional solution offered at [hp.com](http://hp.com).

Choose an authentication method for **Future Installations** as desired. This automatically requires authentication for new solutions that may be installed on the MFP. You should choose a method for this option as a best practice for security even if you do not expect to add solutions to the MFPs.

### Group 1 PIN and Group 2 PIN

You can use PIN Authentication with other authentication features to restrict use of the MFPs further. For instance, you can require all users to login at walk up using the LDAP system and then require group 1 PIN for access to the copy function and group 2 PIN for access to the fax function.

Configure **PIN Authentication** as desired (Figure 60).

Figure 60: The Group 1 PIN and Group 2 PIN Authentication options.

The figure consists of two screenshots of the HP MFP Security Checklist configuration interface. Both screenshots show the 'Config' tab selected in the top navigation bar. The left sidebar contains a tree view with 'My Settings', 'Device', 'Copier', 'Network', 'Security', 'Access Control List', and 'Authentication Manager'. The right pane shows the 'Group 1 PIN' configuration screen. The title bar of the right pane reads 'Group 1 PIN (Changes Pending - Click 'Apply' to continue)'. Below the title bar, there is a green checkmark icon and two input fields: 'Enter PIN:' and 'Confirm PIN:'. Both fields contain a series of asterisks (XXXXXXXXXX). The top navigation bar includes tabs for Status, Config, Alerts, Troubleshoot, Groups, Reports, Supplies, Storage, Solutions, Detailed Info, Capabilities, and Firmware. Below the navigation bar, there are buttons for 'Apply Template...', 'View History', 'Customize...', and 'Refresh'.

Click to select **PIN Authentication**, and enter PINs as desired. Be sure to repeat the PINs exactly in the **Confirm PIN** fields.

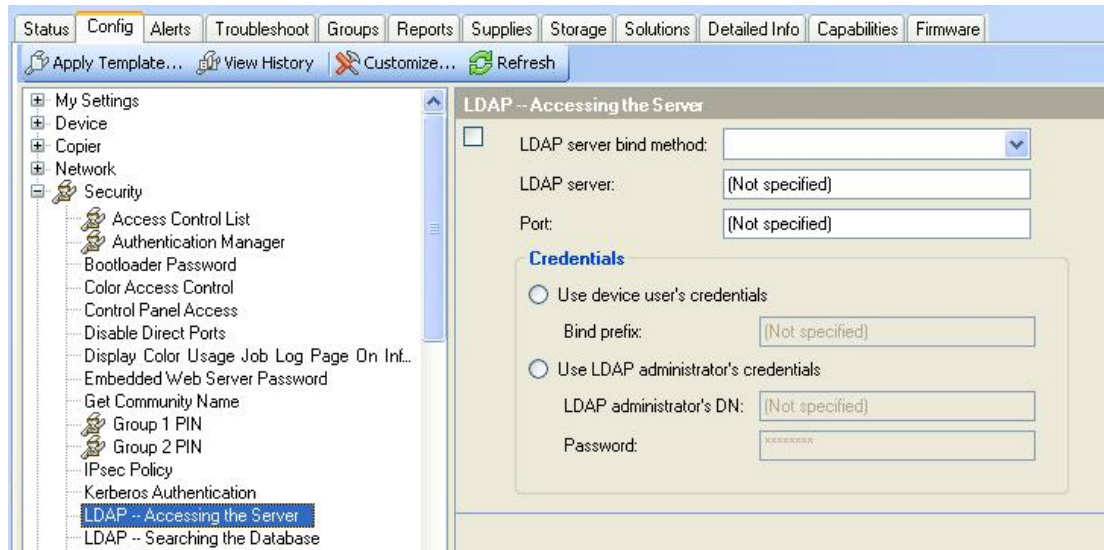
**Note:**

If your network includes NTLM service, configure NTLM. This option specifies the authentication method to use when your MFP executes a send to folder job. We recommend using the highest authentication available.

## LDAP

If your network includes LDAP, configure the **LDAP Authentication** options (Figure 61).

Figure 61: The Accessing the LDAP Server options.



These settings enable the MFPs to require a user's logon credentials for use of the MFPs. This is related to the LDAP access options in the Digital Sending category, which enable the MFP to use the LDAP address book; however, the SSL certificate options for both configurations appear on the Digital Sending page.

### Note:

These instructions assume that the LDAP server is configured for SSL. If you have this feature available, you should go to the Digital Send page (see the Digital Send section, above) to upload a certificate created by the Certificate Authority server on your network.

Select Simple over SSL in the LDAP Server Bind Method: dropdown menu.

### Note:

If possible, you should choose Simple over SSL for the bind method and configure the LDAP server for communication over a secure SSL channel. This also requires that you generate SSL certificates and upload them to the MFPs using the LDAP Access options in the Digital Sending page (explained earlier).

If you choose Simple for the bind method, usernames, email addresses, passwords, and other data will be sent over the LDAP protocol in clear text.

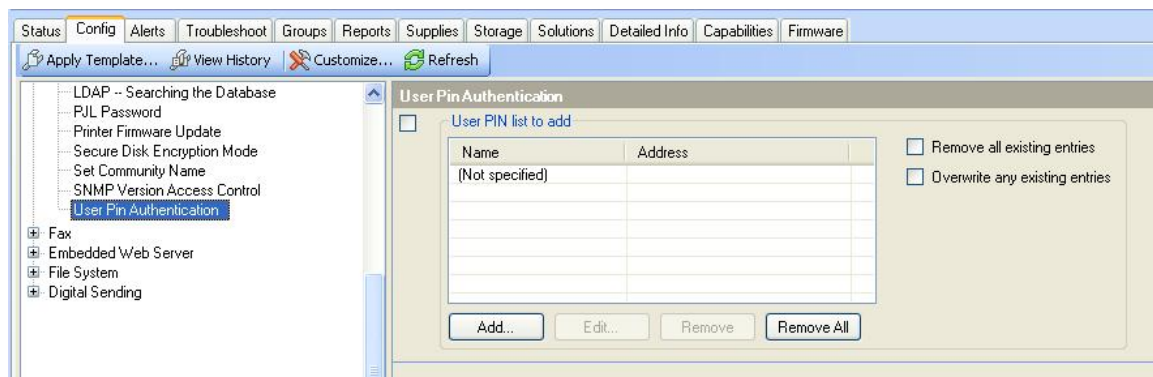
Fill in the remaining fields according to your network configuration.  
If your network has Kerberos authentication capabilities, configure the Kerberos Authentication options.

## User Pin Authentication

User PIN Authentication allows you to restrict access to MFP functions by specific users. A user will be required to log in by PIN in order to use a restricted function on the MFP (see the **Authentication Manager** section above). This feature also provides a way to add user email addresses to the MFP address book. You can configure up to 2000 users in this feature.

Configure User PIN Authentication (Figure 62) as desired.

Figure 62: The User Pin Authentication options.



## Chapter 5: Settings List

This section is a complete list of the settings recommended in this checklist. This section does not include instructions or explanations. It is intended to be used as a check-off list of the recommended settings to help ensure that you complete the entire configuration. See the Network Security section (above) and the Ramifications section (below) for information on each setting.

---

### NOTE:

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

Remember that these settings are recommended for the most common types of network environment. Your environment may require configurations not recommended in this checklist. Consider each setting in the context of your network environment needs and constraints.

---

## Recommended Settings

### Initial Settings

- ☐ Configure Advanced Security Settings (ACL, Firewall, LDAP, Kerberos, etc.)
- ☐ Verify your HP Secure Hard Disk is functioning correctly.
- ☐ Configure **SNMPv3** (Security page).

### Device Category Settings

- ☐ Configure **I/O Timeout to End Print Job**
- ☐ Configure **Job Hold Timeout**.
- ☐ Enable **Job Retention**.

### Network Category Options

- ☐ Configure **Enable Features** options.
  - ☐ Enable **EWS Config**.
  - ☐ Disable **Telnet Config**.
  - ☐ Disable **SLP Config**.
  - ☐ Disable **FTP Printing**.
  - ☐ Disable **LPD Printing**.
  - ☐ Enable **9100 Printing**.
  - ☐ Disable **IPP Printing**.



- ☐ Disable **mDNS Config**.
- ☐ Disable **IPV4 Multicast Config**.
- ☐ Disable **WS-Discovery**.
- ☐ Enable **HTTPS Setting** to **Encrypt all web communication**.
- ☐ Configure **Encryption Strength** to **High**.
- ☐ Configure **Error Handling**
- ☐ Disable **IPX RCFG Support**.
- ☐ Configure **Job Timeout**.
- ☐ Set the **Privacy Setting** as desired.
- ☐ Configure **Protocol Stacks**.
  - ☐ Disable **IPX/SPX**.
  - ☐ Enable **TCP/IP**.
  - ☐ Disable **DLC/LLC**.
  - ☐ Disable **AppleTalk**.
- ☐ Disable **Web Services Print**.

### Security Category Options

- ☐ Configure **Bootloader Password**.
- ☐ Configure **Color Access Control** as desired.
- ☐ Configure **Control Panel Access** to **Maximum Lock**.
- ☐ Configure **Embedded Web Server Password**.
- ☐ Configure the **PJL Password**.
- ☐ Disable **Printer Firmware Update**.
- ☐ Configure **Secure Disk Encryption Mode**

### Fax Category Options

- ☐ Configure **Fax Printing**.
  - ☐ Establish PIN Number.
  - ☐ Select **Store All Received Faxes**.

### Additional Fax Configuration

- ☐ Configure **Fax Speed Dials**.
  - ☐ Lock Speed Dials.

## Embedded Web Server Page Options

- ☐ Configure **Embedded Web Server Configuration** 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.
  - ☐ Enable Continue Button.
  - ☐ Disable Print Service.

## File System Page Options

- ☐ Configure **File System External Access**.
  - ☐ Disable **PJL**.
  - ☐ Disable **PML**.
  - ☐ Disable **NFS**.
  - ☐ Disable **PostScript**.
- ☐ Configure **File System Password**.
- ☐ Configure **Secure File Erase Mode** to **Secure Fast Erase** or **Secure Sanitize Erase**.

## Digital Sending Page Options

- ☐ Configure **Auto Reset Send Setting** to **Delay before resetting the default settings**, and type a number of seconds to delay.
- ☐ Configure **Default From Address**.
  - ☐ Select Prevent user from changing the Default From Address.

## Final configurations

- ☐ Disable **Direct Ports** (wait for MFPs to restart).
- ☐ Disable **EWS Config**.

## Chapter 6: Default Settings:

This chapter lists the default setting for each configuration in the checklist:

| Setting  | Default Setting       |
|--|-----------------------|
| Configure HP Secure Hard Disk  | Installed and Enabled |
| Configure <b>SNMPv3</b> (Security page).   | Not configured        |
| I/O Timeout to End Print Job   | Not configured        |
| Configure Job Hold Timeout.  | Never Delete          |
| Enable Job Retention.  | Enabled               |
| Configure <b>Enable Features</b> options (do not disable <b>EWS Config</b> at this point). | (See below)           |
| Disable Telnet Config.   | Enabled               |
| Disable SLP Config.  | Enabled               |
| Disable FTP Printing.  | Enabled               |
| Disable LPD Printing.  | Enabled               |
| Enable 9100 Printing.  | Enabled               |
| Disable IPP Printing.  | Enabled               |
| Disable MDNS Config.   | Enabled               |
| Disable IPV Multicast Config.  | Enabled               |
| Disable WS-Discovery.  | ?                     |
| Enable Encrypt all Web Communication.  | Enabled               |
| Configure Encryption Strength to High.   | Low                   |
| Error Handling   | Dump then Reboot      |

|  |                          |
|--|--------------------------|
| IPX RCFG Support.                                    | Enabled                  |
| Configure <b>Job Timeout</b> .                       | Not Configured           |
| Set the privacy setting as desired.                  | Not configured           |
| Configure Protocol Stacks.                           | (See below)              |
| Disable <b>IPX/SPX</b> .                             | Enabled                  |
| Enable <b>TCP/IP</b> .                               | Enabled                  |
| Disable <b>DLC/LLC</b> .                             | Enabled                  |
| Disable <b>AppleTalk</b> .                           | Enabled                  |
| Web Services Print.                                  | Enabled                  |
| Configure Bootloader password.                       | Not configured           |
| Configure Color Access Control                       | Not configured           |
| Configure Control Panel Access to Maximum Lock.      | Unlock                   |
| Configure Embedded Web Server Password.              | Not configured           |
| Configure the <b>PJL Password</b> .                  | Not configured           |
| Disable Printer Firmware Update.                     | Enabled                  |
| Configure Secure Disk Encryption Mode                | Not configured           |
| Configure Fax Printing.                              | Not configured           |
| Establish PIN Number.                                | Not configured           |
| Configure Enable Mode to Store All Received Faxes.   | Print All Received Faxes |
| Configure Fax Speed Dials                            | Not configured           |
| Configure Embedded Web Server Configuration options. | (See below)              |
| Enable Outgoing Mail.                                | Enabled                  |

|   |                       |
|---|-----------------------|
| Disable Incoming Mail.  | Disabled              |
| Disable Cancel Job Button.  | Disabled              |
| Disable Go Button.  | Enabled               |
| Disable Command Invoke.   | Enabled               |
| Disable Command Download.   | Enabled               |
| Disable Command Load and Execute.   | Enabled               |
| Enable Continue Button.   | Enabled               |
| Disable Print Service.  | Enabled               |
| Configure File System External Access.  | (See below)           |
| Disable <b>PJL</b> .  | Enabled               |
| Disable <b>PML</b> .  | Enabled               |
| Disable <b>NFS</b> .  | Enabled               |
| Enable PostScript.  | Enabled               |
| Configure File System Password.   | Not Configured        |
| Configure Secure File Erase Mode to Secure Fast Erase or Secure Sanitize Erase. | Non-Secure Fast Erase |

|  |   |
|--|---|
| Configure <b>Auto Reset Send Settings</b> to <b>Delay before resetting the default settings</b> , and type a number of seconds to delay. | Not configured, Delay default: 20 seconds |
| Configure Default From Address.  | Not configured                            |
| Select Prevent user from changing the Default From Address.  | Not selected                              |
| Disable <b>Direct Ports</b> (wait for MFPs to restart).  | Enabled                                   |
| Disable EWS Config.  | Enabled                                   |

## Chapter 7: Ramifications

Raising the level of security on HP MFPs requires giving up some conveniences and usability. This section explains some of the compromises you can expect from configuring the settings recommended in this checklist. Keep in mind that this is not a comprehensive list. You should test each MFP in your network environment to understand the implications of these settings and configurations.

The following sections explain some of the known ramifications of each recommended setting:

### Initial Settings

- Configuring Advanced Security Settings (ACL, Firewall, LDAP, Kerberos, etc.)  
There are many advanced security settings that you may be using as part of your infrastructure or print solution. These settings should be configured and tested before locking down your devices with this checklist. If you are unsure how a setting may affect an advanced security configuration see the advanced security section, or test the setting on a single device before applying it to your fleet.

- Configure HP Secure Hard Disk.

HP Secure Hard Disk is a disk that encrypts all data stored on your hard drive.

Failure to set up this device before setting the NIST checklist or other MFP settings will result in a loss of all previous settings when the HP Secure Hard Disk is installed and set to encrypt data.

Once the HP Secure Hard Disk is installed, the hardware encryption is transparent to the device. It should have no impact on subsequent configurations unless you:

- Remove the HP Secure Hard Disk and install a new one
- Use the "reinitialize" feature which will result in cryptographically erasing your entire disk, or
- Change the password, which will also result in reinitializing the encrypted disk

- Enable **SNMPv3**

SNMPv3 is a secure protocol that encrypts configuration data transmitted over the network. Web Jetadmin accesses most of the MFP configuration settings through the MFP SNMP ports.

Once SNMPv3 is configured, the MFPs will prompt for the credentials every time anyone tries to configure settings using Web Jetadmin or any other tool. However, Web Jetadmin includes a convenient device cache feature that stores all of the passwords and credentials for each MFP. Whenever an authorized Web Jetadmin administrator makes a change, Web Jetadmin automatically provides the credentials without prompting. Thus, the administrator is required to remember the credentials only when the device cache credentials are outdated. The device cache is secured by encryption, and Web Jetadmin allows only the authenticated administrator to log in and manage the MFPs. Be sure to configure a robust password for Web Jetadmin.

With SNMPv3 configured, an unauthorized user attempting to access the MFP configuration settings will observe a prompt for the SNMPv3 credentials. The MFP will not disclose which credentials are incorrect; it will only revert to the prompt for credentials.

SNMPv3 causes some slowing of the configuration process due to the additional time taken to encrypt the data.

Disabling SNMPv1 disables SNMPv1 GET and SNMPv2 SET commands. Any solution or software that requires SNMPv1 or SNMPv2 will not function. If you require these to be enabled be sure to set the community name to something that would be difficult to guess.

## Device Page Settings

- Set **I/O Timeout to End Print Job**. The I/O Timeout to End Print Job allows you to specify the amount of time a device should wait between packets before canceling a job. Setting this timeout will help prevent jobs formed or sent incorrectly from tying up a print resource. If you are on a busy network or spool large jobs real time that may cause packet gap set this setting high enough to accommodate your environment.
- Enable **Job Hold Timeout**. Job Hold Timeout is related to the **Job Retention** setting below. It permanently deletes stored jobs (except fax) that are held past the allowed time. This ensures that the stored jobs are not accessible after a time, and it ensures that the hard drive is cleared periodically.

**Job Hold Timeout** requires that users are mindful of their print jobs. They will not be able to recover jobs that are deleted after the timeout period. Jobs are deleted securely according to the **Secure File Erase** setting (appears later in this checklist).

- Enable **Job Retention**. Job Retention is a feature of the MFP that saves fax or print jobs on the hard drive for printing when the user is present. The security implication is that a user can be sure others will not be able to see the printed documents. For printing, a user sets the PIN at the time of sending the print job to the MFP. For fax printing, the PIN is configured for all incoming jobs using Web Jetadmin. The MFP will require the PIN number at the control panel before it will print the job.

Configuring Job Retention enables more efficient use of the MFP hard drive. Thus, you should configure **Job Hold Timeout** and other related settings.

---

### NOTE:

Stored faxes are not affected by the Job Hold Timeout.

---

## Network Page Options

- Configure **Enable Features** options (do not disable **EWS Config** at this point). These options 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:
  - Disable **Telnet Config**. **Telnet Config** is an access point used by some older (legacy) printer management tools. Jetdirect also supports some Telnet commands. Telnet Config transmits data in clear text, and it should not be used. With it disabled, MFPs will deny access to Telnet sessions.

Web Jetadmin does not use **Telnet Config**; thus disabling it has no affect on it. It disables other tools, but Web Jetadmin is the only solution recommended for managing HP MFPs.



- Disable **SLP Config**. **SLP Config** accommodates software using SLP as a discovery mechanism. For example disabling **SLP Config** on some Novell networks (depending on how Novell is configured) would cause Novell to not recognize the MFPs on the network. Thus, if your network uses these features of Novell, you should enable SLP Config. If you use software other than HP Web Jetadmin with your HP MFPs please test this feature before disabling it. HP Web Jetadmin is not affected by this setting,
- Disable **FTP Printing**. **FTP Printing** enables files to be sent to the printer via FTP for printing on the MFP, enabling FTP Printing also allows you to upgrade your printer firmware by sending the firmware via FTP. HP recommends disabling it and using Web Jetadmin to upgrade firmware. MFPs will deny access to FTP sessions.
- Disable **LPD Printing**. **LPD Printing** is the protocol necessary for printing in UNIX, HP-UX, or Linux environments. You should disable LPD Printing unless your network includes UNIX workstations that might print using the MFPs. With this option disabled, MFPs will deny access to UNIX machines.
- Enable **9100 Printing**. **9100 Printing** should always be enabled. It is the standard printing protocol used by MFP print drivers. Disabling **9100 Printing** would disable all printing for most users.
- Disable **IPP Printing**. **IPP Printing** is a protocol for printing over the internet or locally. Unless you have a requirement for IPP printing it should be disabled. With it disabled, the MFPs will deny access to direct printing from the Internet. Print jobs generated from web browsers using the installed print driver are not affected.
- Disable **MDNS Config**. **MDNS Config** resolves host names with IP addresses in small networks without DNS servers. Most enterprise networks include DNS servers and do not require this service. With this option disabled, a non-DNS network will not recognize the MFPs. If your network does not include a DNS server, you should enable MDNS Config.
- Disable **IPv4 Multicast Config**. **IPv4 Multicast Config** configures multiple devices simultaneously over the network. You should always disable **IPv4 Multicast Config**, and use Web Jetadmin for managing MFPs.
- Disable **WS-Discovery**. **WS-Discovery** enables network hosts that support WS-Discovery to discover printers and devices on the network. Unless you are in an IPv6 or Windows Vista/Windows 7 only environment there are other protocols you can use to discover your printers.
- Configure **Encryption Strength** to **High**. The encryption strength setting covers communication between a PC and the Embedded Web Server. When HTTPS is configured (as recommended in this checklist), communication is encrypted according to this Encryption Strength setting.

With **Encryption Strength** set to **High**, users will find that the EWS are accessible only from web browsers that support that level of HTTPS communications.

This checklist recommends disabling EWS Config during normal use of MFPs. This removes all access to the EWS; however, you should configure this setting for times when you temporarily enable EWS Config to make changes to configurations.

- Enable **HTTPS**, and configure the setting to **Encrypt all web communication**. This setting enables encryption for configuration data between the PC and the MFP EWS. It prevents sensitive data such as usernames and passwords from passing over the network in clear text. This setting is related to the EWS **Encryption Strength** setting explained earlier.

Web browsers that do not support SSL and high encryption strength will not be able to access the MFP EWS.

This checklist recommends disabling EWS Config during normal MFP operations and enabling it temporarily for changes to configurations. This setting ensures that the network traffic is secure during those configurations.

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

With **IPX RCFG Support** disabled, MFPs will deny access to Novell.

When you click **Apply** for this setting, 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.

- Configure **Job Timeout**. The **Job Timeout** option enables the MFPs to move on from jobs that lack proper end of job signals. The MFPs will be able to switch protocols to continue with other jobs rather than waiting indefinitely for improperly formatted jobs to finish.
- Set the **Privacy** setting as desired. The Privacy setting is included in this checklist to inform you of its purpose: 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 HP 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 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 unused Protocol Stacks. These options provide for the various types of network communication to the MFPs. Closing down unused protocol stacks is effective toward better network security. See the ramifications of each option below:
  - Disable **IPX/SPX**. IPX/SPX is the network protocol for Novell. Disabling it prevents printing and all other communications with Novell non-TCP/IP components. With it disabled, Novell non-TCP/IP components will not recognize the MFPs on the network.
  - Enable **TCP/IP**. TCP/IP is the standard network protocol for MFP operations. It provides the necessary network communication for printing and for configuration. It should be enabled during normal use of MFPs.
  - Disable **DLC/LLC**. DLC/LLC is used in small networks in which routing is not required. The MFPs include it for compatibility with older HP products.
  - Disable **AppleTalk**. **AppleTalk** is used with older Apple computers. You should disable it unless your network includes older Apple or Macintosh computers. With it disabled MFPs will not appear on the network for these computers.

Disable Web Services Print. This disables the Microsoft WSD Print services supported on the HP Jetdirect Print Server. If this feature is enabled someone with a host that supports Web Services Print can discover IP Addresses and other information about the printers in your environment.

## Security Page Options

- Configure **Bootloader Password**.  
The Bootloader Password protects against accidental or unauthorized intentional access to the MFP Bootloader settings. These settings are similar to the BIOS settings on a PC. They affect the services that are loaded when the MFP is turned on. The Bootloader Password setting is permanent. There is no way to reset it or to change it without providing the correct password. Thus, it is extremely important to use a password that can be remembered and to record the password in a safe place.
- Configure color restriction settings. If your network includes Color LaserJet MFPs, you can configure settings to restrict the use of color printing by users and by applications.

With color restriction settings configured, an MFP will print only in black and white for restricted users or applications.

- Configure **Control Panel Access Lock** to **Maximum Lock**. Control Panel Access Lock denies access to configuration settings from the MFP control panel. This ensures that no one will be able to change configuration settings from the control panel.

This setting places a lock icon on the affected settings on the control panel. If a user selects a locked setting, the control panel states that access is denied. Access can be restored only by changing the **Control Panel Access Lock** configuration using Web Jetadmin (assuming that you are following all of the recommendations in this checklist).

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.

The maximum Control Panel Access Lock closes all access to the fax menu. This includes the options to **Cancel All Pending Transmissions** and **Cancel Current Transmission**. If you wish to provide these options, use **Intermediate Lock**.

- Configure the **Embedded Web Server Password**. The EWS password restricts access to the configuration settings in the EWS. When configured, the MFP requires the password whenever anyone or any application attempts to make changes to the EWS settings. Keep in mind that the settings provided in the EWS are also accessed by Web Jetadmin. Thus, the MFPs will require the EWS password from Web Jetadmin whenever it attempts to access these settings.

Web Jetadmin keeps all passwords and credentials in the encrypted device cache. It will automatically provide the EWS password to the MFPs whenever they MFPs prompt for it.

The EWS password is synchronized with the device password, which is recommended later in this checklist. Whenever you change either password, the MFP will change the other one to be the same.

- Configure the **PJL Password**. The PJL password prevents unauthorized users from configuring certain features of the MFP. It requires the password to change these settings via Print Job Language (PJM) commands.

With the PJL Password configured, the MFPs will deny access to commands that attempt to change default settings without the correct password.

- Disable **Printer Firmware Update**. **Printer Firmware Update** enables the MFPs to accept printer firmware updates from various sources. Disabling it ensures that no one can send firmware updates to the MFPs. If this feature is disabled it may still be possible to update the firmware manually through the boot loader if you have not safeguarded this option.

HP recommends updating firmware whenever it becomes available at [hp.com](http://hp.com). You should enable **Printer Firmware Update** to perform the upgrades and then disable it again during normal use of the MFPs.

With **Printer Firmware Update** disabled, the MFPs will deny access whenever anyone attempts to upgrade the firmware.

- Configure Authentication (LDAP, Kerberos, Device PIN, or User PIN). Authentication requires users to log on for use of the MFPs.
- Configure **Authentication Manager**. The Authentication Manager provides the settings to require log in for use of the MFP. It is important to be sure to configure the authentication methods (LDAP, Kerberos, Device PIN, or User PIN) you wish to enforce in the authentication manager. With authentication enabled, MFPs will deny access to users who cannot supply the correct credentials.
- Set the **Device Password**. The **Device Password** helps prevent unauthorized users from changing configurations in the MFPs. The MFPs will deny access to configuration settings without the password.

Web Jetadmin keeps MFP credentials in its encrypted device cache. It will not prompt for the device password of an MFP that it manages.

The **Device Password** is synchronized with the EWS password. If you change either of them, the MFP will change the other one to be the same.

- Disable **Allow Use of Digital Send Service**. HP Digital Sending Software is a useful tool for managing MFP digital sending. It is available for purchase at [hp.com](http://hp.com). HP recommends using Digital Send Service, but it is not covered in this checklist. Thus, this checklist recommends disabling it unless you are using it.

With **Allow Use of Digital Send Service** disabled, no one can manage the MFPs with an installation of Digital Send Service. The MFPs will deny access.

- Disable **Allow Transfer to New Digital Send Service**. This setting is related to the previous setting. If you allow use of Digital Send Service, it is possible for any installation of Digital Send Service to take over management of an MFP. Disabling this setting ensures that the MFPs will allow only one Digital Send Service computer to manage the MFPs.

With this setting disabled, the MFPs will deny access to a second Digital Send Service attempting to take over management.

## Fax Page Options

- Configure the Fax PIN. With the fax PIN configured, the MFP requires the Fax PIN be provided before access to held fax jobs is gained at the control panel. This improves security by ensuring that printed faxes are not left in the output trays where unauthorized personnel might see them.

---

### NOTE:

Stored faxes are not affected by the Job Hold Timeout.

---

The **Fax Printing** options limit access to timely faxes. You may wish to provide the PIN to a number of people to ensure that someone can print a fax on demand. You can also configure fax alerts to ensure that personnel will know when a fax arrives even though it is not printed upon arrival.

## Additional Fax Configuration

Configure the number of Fax Speed Dials with the Embedded Web server. With the number of fax speed-dials configured and access to these locked down no one can tamper with you speed-dial settings from the front panel of the MFP.

## Embedded Web Server Page Options

- Configure **Embedded Web Server Configuration Options**. These options limit some of the EWS features that can be misused:
  - 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 as a best practice. This setting does not affect any other use of the MFP. With this setting configured, the MFPs will ignore all incoming emails.
- 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 cancel jobs remotely (and anonymously); 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 removes it from the EWS preventing users from delaying jobs or even denying service to other users; 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 does not apply to the MFPs. Disabling it is good security practice to ensure that all possible access to it is closed.
- Disable **Command Download**. Command Download is a legacy feature that does not apply to the MFPs. Disabling it is good security practice to ensure that all possible 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. Disabling it stops the MFPs from running Chailets when it starts up. This function is called Service Loading in the EWS. If your network uses Chailets, you should enable Command Load and Execute. If not, you should disable it to prevent users from installing this type of application.

You may wish to (turn off the MFPs and turn them on again (power cycle) after disabling Command Load and execute. This will stop applications that may be already loaded and running.

With this setting configured, the MFPs will ignore all add-on applications.

- Disable **Print Service**. Print service allows users to send print-ready files such as PDF files directly to MFPs for immediate printing. This feature is available to anyone who has access to the EWS. Disabling it ensures that only users with the MFP Print driver installed can send print jobs to the MFPs.

With **Print Service** disabled, the print options do not appear on the EWS.

## File System Page Options

- Configure **File System External Access**. The File System External Access settings shuts down access to the MFP file system (storage devices and configuration settings) through protocols and ports. They eliminate access from various types of management tools. HP recommends shutting down all unused access to the file system. See the ramifications for each protocol below.

---

**NOTE:**

Some storage management tools, such as the Web Jetadmin Device Storage Manager (a Web Jetadmin add-on available in the Product Update navigation mode), use some of these protocols to access the file system. You might consider enabling these protocols only to update configurations and then disable them during normal MFP operation.

Also, note that disabling PJJ and PML only affects file system access, but disabling NFS shuts down the protocol for the entire MFP.

---

- Disable **PJJ** access. PJJ (Printer Job Language) includes capabilities to manage configurations in the form of commands inside print jobs. Some of these commands can access MFP storage devices. Disabling PJJ access to the file system disables only the commands that affect the file system. This will not affect the preferences available for normal print jobs.

With **PJJ** access disabled, the MFPs will ignore PJJ commands that attempt to access the file system.

- Disable PostScript access. The PostScript protocol enables programs such as Adobe® products to access the MFPs directly for printing and for access to fonts. Some of the commands it uses can access MFP storage devices. Disabling PostScript access to the file system disables only the commands that affect the file system. This will not affect the preferences available for normal print jobs, but could affect interoperability with third party products.
- Disable **PML** access. PML (Printer Management Language) is an HP proprietary protocol that manages MFPs. Web Jetadmin uses PML for many of its configuration settings. Disabling this PML access eliminates the PML commands that affect access to the storage devices even for Web Jetadmin. If you wish to make changes to the file system, enable PML access to make the changes, and disable it again. With this setting, MFPs will ignore PML commands that attempt to access the file system.
- Disable **NFS** access. The NFS protocol is used by UNIX, and Linux, and Norton systems. Disabling it disables the entire protocol for the MFPs. With this setting, MFPs will ignore all NFS requests. If your network uses these protocols, you should enable NFS.
- Configure the **File System Password**. The File System password feature restricts access to the Secure File Erase Mode, Secure Storage Erase, and External File System Access Settings. This setting is important because it helps protect data stored on the MFPs. It does not affect normal use of the MFPs such as job storage.

Users attempting to make changes to the file system settings or attempting to access data through network ports will be required to provide this password. Without the password, the MFP denies access to the File System and to File System configurations.

Web Jetadmin stores the file system password in its encrypted device cache. It automatically provides the password when the MFPs request it.

- Set the **Secure File Erase Mode** to **Secure Fast Erase** or to **Secure Sanitizing Erase**. Secure File Erase enables the MFPs to overwrite storage space whenever files are deleted. This

ensures that the original data is destroyed.

Secure Fast Erase mode overwrites files one time. It slows MFP performance a bit, but it provides reasonable security for most situations.

Secure Sanitizing Erase overwrites files 3 times. It slows MFP performance considerably, but it provides even more assurance that the data is not recoverable. If your network is required to meet stringent security requirements such as DOD regulations, you should use Secure Sanitizing Erase.

## Digital Sending Page Options

- Configure **Auto Reset Send Settings** to **Delay before resetting the default settings**, and type a number of seconds to delay. This setting enables the MFPs to remove email addresses or fax information from the control panel if a user forgets to reset it. The authenticated user performing a digital send job is also automatically logged off.

With the timeouts configured, an MFP control panel will revert to the default screen, and a user will not be able to reuse addresses and other destination data beyond the timeout period.

- Configure 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, and that it is automatically populated with the default or the authenticated users email address. 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 address to monitor reply messages.

With the Default From Address configured, no one can change the From address in email messages. The address you configure is the only address anyone can use.

## Final Configurations

- Disable **Direct Ports**. This setting shuts down the MFP parallel ports. It restricts access to only network connections.

Shutting down the parallel ports ensures that no one can configure the MFPs or print using these connections. Thus, users will not be able to bypass job accounting or restricted access, such as color printing, by using alternative connections.

This setting causes the MFPs to turn off and turn on. They will be out of service during this time. This is also the reason this setting should be configured independently of other setting configurations. If you attempt to configure this setting with other settings, the other settings will likely fail. This is because Web Jetadmin temporarily loses contact with each MFP while the MFP is restarting. Be sure to wait a few minutes until all of the MFPs are online and ready before executing another configuration.

With Direct Ports disabled, the parallel and USB ports are turned off, and the MFPs behave as if the ports do not exist.



- Disable **EWS Config**. Disabling EWS Config removes the EWS from the network. They become unavailable to everyone. This eliminates many risks to security.

Since all of the EWS configuration settings are available in Web Jetadmin, there is no need to have them available anywhere else. Keep in mind, though, that disabling EWS Config also eliminates the affected settings from Web Jetadmin. Thus, you will have to enable EWS Config temporarily to make changes to the configurations, and then disable it again.

With **EWS Config** disabled, the MFPs will not provide the EWS on the network. Web browsers will return with no such web site found. This removes some conveniences that EWS provide, but all of the functions that you would want to provide to users are available using the MFP drivers or the control panels.

## Overall Limitations

This overall configuration provides a high level of network security for HP MFPs. At the same time, it introduces some limitations to the conveniences designed into the MFPs. Here are some known affects of this overall configuration:

- Extra steps to use MFPs: Users will be required to provide usernames and passwords at the control panels before they can use the MFPs.
- No access to control panel configuration menus: The control panels block access to configuration settings for anyone. Configuration settings will be available only on Web Jetadmin. Some settings will have to be enabled using Web Jetadmin before they can be accessed.
- No way to cancel print jobs from the control panel: The MFPs will not allow a user to cancel the print jobs of other users. The user would have to go to the person who submitted the job and ask that person to cancel it.
- No way to cancel a fax job: The maximum lock setting on the control panel includes removing the fax job cancelling options. Once a user selects Send, there is no way to stop an outgoing fax (other than disconnecting the phone line). You can enable fax cancelling by configured Control Panel Access Lock to **Intermediate Lock**.
- Extra steps for printing faxes: A user will be required to provide a fax PIN before printing a fax.
- No Embedded Web Servers: Disabling EWS Config disables the entire EWS feature.

No way to change the From Address on email send jobs: Depending on the capabilities of your network, the MFPs will place either a default from address or the user's email address of the user who logged into the MFP. It will provide no method to change it.

## Chapter 8: Physical Security

Many of the most notable features of HP MFPs involve hard copy documents. MFPs 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 printer output trays exposed to possible unauthorized viewers.
- Leaving documents in Automatic Document Feeder (ADF) or on the flatbed scanner exposed to possible unauthorized view.

These are common-sense security risks. Use PIN printing and PIN fax printing to ensure that authorized users are present during printing. Stay with the MFP while using the ADF or the flat bed scanners. Keep the MFP in an enclosed room to allow for controlled access for sensitive printing or scanning.

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 on 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 and phone lines 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 MFPs in access-controlled locations.

You can control access to the MFP internal hardware (hard drives, Compact Flash cards, and formatter board) using hardware locks. Use a lock, such as a Kensington Lock, as recommended in the MFP User Guide.

If you have purchased the EIO version of the HP Secure Hard Disk (J8019A), you can also use a Kensington style lock (cabled or cable-less) to protect the disk from being unscrewed and removed from the device. If you use a cabled Kensington lock, you can even secure the device to a stationary object to avoid someone from stealing the MFP.

## Chapter 9: Appendix 1: Glossary of Terms and Acronyms

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

| Term            | Description  |
|-----------------|--|
| ACL             | Access Control List. The ACL restricts network access to the MFP by allowing only those IP addresses or subnets that are listed in it.   |
| Analog fax      | Analog fax is fax functions via telephone lines. The fax module is available in most HP MFP bundles and it is covered in this checklist. 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.   |
| Bootloader      | The bootloader is the program that starts up an MFP when the power is turned on. It loads the MFP operating systems and the configurations. The bootloader includes settings, such as cold resetting, that are accessible via special codes (not covered in this checklist). These settings are protected by the bootloader password.  |
| Control Panel   | The control panel is the display and the buttons on the front of an MFP.   |
| Digital sending | Digital sending is a function of the MFP that sends scanned documents to email destinations or to network destinations. Faxing is also considered digital sending, but it is separate from the network functions.  |
| DSS             | Digital Send Service. DSS is an HP solution to enhance MFP digital sending functionality and security. For instance, it can encrypt the contents of digital send jobs. It can be purchased and downloaded at <a href="http://hp.com">hp.com</a> . DSS is useful and recommended, but it is not covered in this checklist.  |
| EWS             | Embedded Web Server. The EWS is a web page built into an 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.  |
| Firmware        | Firmware is the program that operates the MFP. It controls all functions of the MFP. Firmware can be upgraded as new versions become available. New firmware is available by searching for it by product at <a href="http://hp.com">hp.com</a> . This checklist assumes that each MFP is upgraded with the latest firmware.  |
| Formatter       | <p>The formatter is the main circuit board of the MFP. It is similar to the motherboard of a PC. The formatter 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.</p> <p>Since the formatter is removable (using common tools), it includes the capability to be locked using devices such as Kensington locks.</p> |

| Term                              | Description   |
|-----------------------------------|---|
| JDI                               | Jetdirect Inside. Many of the MFPs include internal Jetdirect hardware as standard equipment. Other MFPs, such as HP Color LaserJet 9500 MFPs require EIO Jetdirect cards for network connectivity.   |
| Job Retention                     | Job Retention is the MFP capability of storing print jobs or fax jobs for printing on demand at the control panel. PIN printing and PIN fax printing are functions of Job Retention.  |
| MFP                               | Multi-Functional Peripheral – An MFP is a device that includes multiple capabilities such as print, copy, fax, and digital sending (email and send to network folder).  |
| PIN                               | Personal Identification Number. A PIN is a numeric password. MFPs use PINs for secure printing and secure fax printing. They can also use PINs for authentication.  |
| Scanner , ADF, or flatbed scanner | <p>The top of the MFP is a scanner that converts paper documents into digital images for copying, fax, or digital sending. The scanner can scan a document in two ways: Automatic Document Feeder (ADF) or flatbed.</p> <p>The ADF is the top of the MFP. It is the cover of the flatbed scanner. 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.</p> <p>The flatbed scanner is a flat pane of glass under a cover (the ADF) that opens to allow placement of one surface for scanning. The flatbed scanner is for documents such as folded paper or books that will not go through the ADF.</p> |
| SNMPv3                            | SNMPv3 is a secure network protocol that encrypts network traffic. It is available with Web Jetadmin.   |
| SSL                               | Secure Socket Layer. SSL is the encryption capability of the internet. It is the system used for web communication via HTTPS.   |
| Storage device                    | <p>A storage device is a component that stores data. The MFP includes two types of storage devices: hard drive and Compact Flash cards.</p> <p>MFP storage devices store two types of data: system data, such as configurations, and user data, such as print jobs, address books, and installed applications.</p>  |
| 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.   |

Microsoft® is a U.S. registered trademark of Microsoft Corporation.  
Adobe and PostScript are trademarks of Adobe Systems Incorporated.  
© 2016 Copyright HP Development Company, L.P.