Technical white paper

HP Printing Security Best Practices for HP FutureSmart Products

Configuring a Printer Securely in HP Web Jetadmin 10.4

Version 2.6

Table of Contents

Introduction

This document is a security checklist for the HP FutureSmart products (see Appendix 2 for full list of products).

This checklist is written for acceptance by the National Institute of Standards and Technology (NIST).

This checklist is meant for trained network administrators who use HP Web Jetadmin version 10.4 or above in enterprise networks. It includes step-by-step instructions to configure one or more printing products 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 Embedded Web Server (EWS), HP Jetdirect, and firmware upgrades for Jetdirect and printing products. Refer to the User Guides and the HP Jetdirect Administrator Guide for more information. You can find these documents and more information by searching at 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.

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

- An ordinary TCP/IP network
- HP Web Jetadmin Version 10.4 installed on one of the follow OS:
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2008 R2 SP1
  - Microsoft Windows 7 SP1 (64-bit edition only)
- Client management PC using one of the following OS with Microsoft Internet Explorer 8, 9, 10, or 11:
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2008 R2 SP1
  - Microsoft Windows 8.1
  - Microsoft Windows 8
  - Microsoft Windows 7 SP1
- One of each supported HP Enterprise product with the latest updated firmware found at hp.com

We developed the process for configuring this checklist using HP Web Jetadmin to manage all the printing products 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 printing security in your workplace. HP has tested this checklist to ensure that printers continue to provide the best possible performance while averting possible security threats; however, some of these settings can cause unexpected problems in your environment especially if you are using custom print solutions. 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 Enterprise printers 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 HP Enterprise Printers. 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 Enterprise products 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 Enterprise product security. HP does not claim or warrant that these configurations prevent misuse of Enterprise products or networks or that they prevent malicious attacks on Enterprise products 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 Enterprise products. However, this checklist applies for HP devices in an enterprise environment or a small to medium business environment. These environments use most of the network features available with HP products. Configuration of the NIST checklist in this document primarily uses HP Web Jetadmin unless a security feature can only be configured using the EWS. 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 HP product User Guide, the 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.

- Enterprise products: This checklist covers security settings for specific HP devices outlined at the beginning of this document. It is meant to enable you to configure multiple devices simultaneously. It assumes that the devices 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 printers and devices; however, this checklist is tested and known to be successful only with the specified device models.

- Updated firmware: This checklist assumes that each device has updated system firmware and Jetdirect firmware (if a Jetdirect product is in use). 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.
- Web Jetadmin Version 10.4: This checklist is written for use with HP Web Jetadmin Version 10.4 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 device is connected directly to a local area network via Jetdirect or Jetdirect inside (JDI) internal network port. Other connections, such as direct-connect 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 Enterprise products.
- 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:

- **Threat Model**: The Threat Model chapter explains the security circumstances relating to MFPs. It follows the Microsoft® STRIDE model.
- **Basic Network Security for Multiple HP Devices**: The Network Security for Multiple MFPs chapter provides step-by-step instructions for configuring MFP security settings.
- **Advanced Security for Multiple HP Devices**: The Advanced Security for Multiple HP Devices provides some limited information on where to find configuration settings in WJA for advanced network configurations.
- **Settings List**: The Settings List chapter provides a bulleted list of the recommended settings with checkboxes. It does not include instructions or explanations.
- **Default Settings**: The Default Settings chapter lists each recommended setting with its corresponding default setting.
- **Ramifications:** The Ramifications chapter explains the possible limitations implied with each recommended setting.
- **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.
- **Appendix 1**: Glossary and Acronyms
- **Appendix 2**: HP FutureSmart products

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 a device 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 device, altering it, and sending it on to the device.
- Intercepting remote configuration data, such as communications between Web Jetadmin and the device, 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.
- Set the PJL and File System password.
- 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:

- Enable embedded IPsec to encrypt the data stream to include log data and file metadata
- 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.
- 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 or contact your HP product supplier).
- Close unused ports and protocols.
- Configure all possible password settings.
- Configure authentication.
- Configure SNMPv3 for Web Jetadmin.
- Disable viewing of job information on the EWS information tab

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 by configuring Access Controls.
- 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 the PJL password.
- Configure SNMPv3 and HTTPS.
- Lock available control panel menus by configuring user access

Basic Network Security for Multiple HP Devices

This chapter explains how to configure security settings for one or more printers 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 ACL, Kerberos, PIN authentication, LDAP, or Solutions please refer to the chapter on Advanced Security before continuing.

Notes on the Process of Configuration

This checklist covers all relevant security settings available for both printers and 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 Printer 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 printer or MFP. When you attempt to make changes to configurations, the printers and 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.

Here is a list of the passwords you should configure:

- Web Jetadmin password (required during installation of Web Jetadmin)
- SNMPv3 credentials
- EWS Password (applies to the EWS, JetDirect networking, and FTP)
- PJL 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, numeric and special 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

This section provides instructions for configuring HP printers for best-practice security. All of these settings are presented for HP Web Jetadmin Version 10.4 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 10.4 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 10.4 or later with the latest upgrades available from HP. See the HP Web Jetadmin Update page in the **Product Update**, **Install** menu.

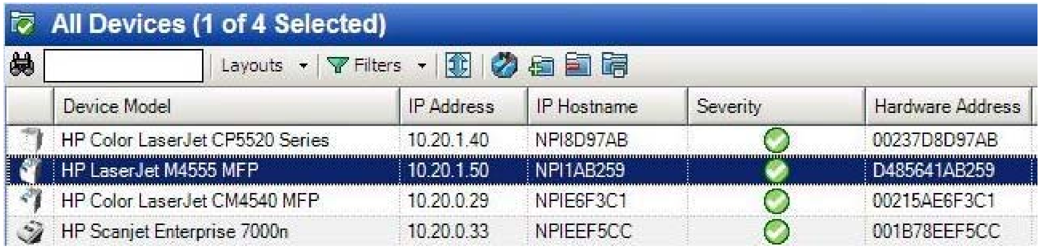
Note:

This checklist was written using screenshots from Web Jetadmin 10.4

Setting up HP Web Jetadmin

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

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



	Device Model	IP Address	IP Hostname	Severity	Hardware Address
	HP Color LaserJet CP5520 Series	10.20.1.40	NPI8D97AB	✓	00237D8D97AB
	HP LaserJet M4555 MFP	10.20.1.50	NPI1AB259	✓	D485641AB259
	HP Color LaserJet CM4540 MFP	10.20.0.29	NPIE6F3C1	✓	00215AE6F3C1
	HP Scanjet Enterprise 7000n	10.20.0.33	NPIEEF5CC	✓	001B78EEF5CC

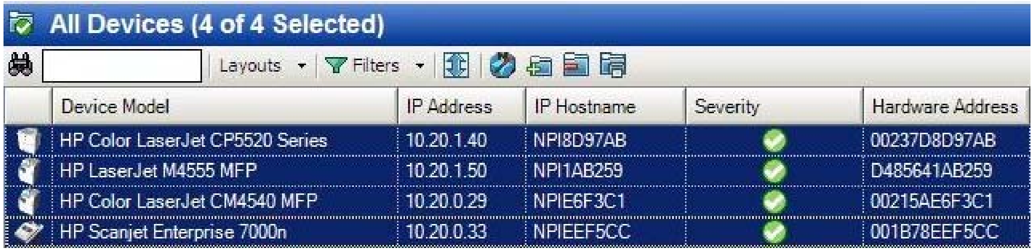
Figure 1: Web Jetadmin showing the device list on the default view.

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

Note:

This checklist does not include details on print device discovery. See Web Jetadmin user guidance for more information. In most cases, the devices will already appear in the default view of Web Jetadmin. It is possible for Web Jetadmin to lose contact temporarily with a device that is configured for DHCP. Use the Discovery options to restore contact or configure the devices with static IP addresses.

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



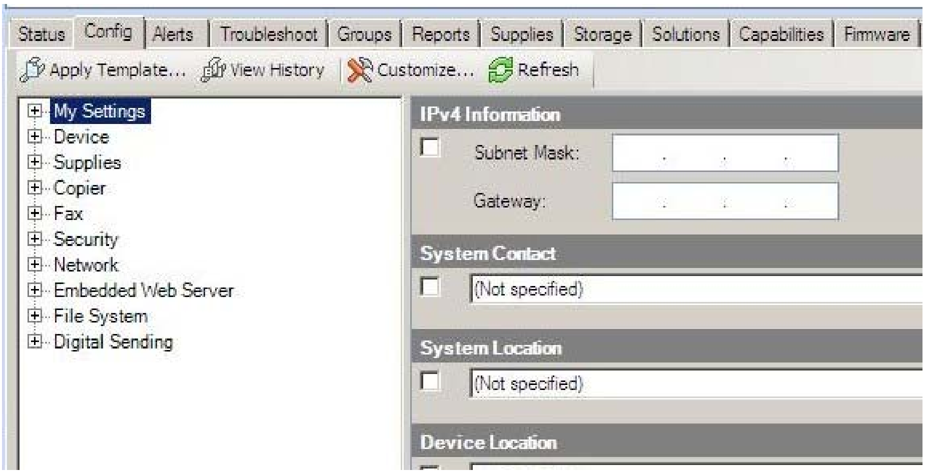
	Device Model	IP Address	IP Hostname	Severity	Hardware Address
	HP Color LaserJet CP5520 Series	10.20.1.40	NPI8D97AB	✓	00237D8D97AB
	HP LaserJet M4555 MFP	10.20.1.50	NPI1AB259	✓	D485641AB259
	HP Color LaserJet CM4540 MFP	10.20.0.29	NPIE6F3C1	✓	00215AE6F3C1
	HP Scanjet Enterprise 7000n	10.20.0.33	NPIEEF5CC	✓	001B78EEF5CC

Figure 2: The Device List showing multiple devices selected.

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.

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



IPv4 Information

□ Subnet Mask:

Gateway:

System Contact

□ (Not specified)

System Location

□ (Not specified)

Device Location

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

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 device.

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

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

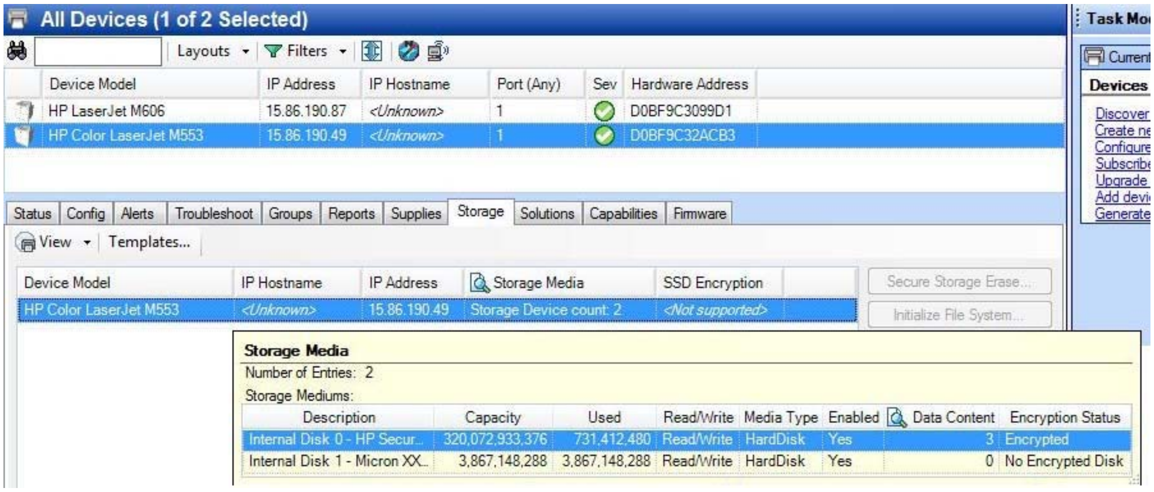
Configuring HP Secure Hard Disk

If you have an HP Secure Hard Disk installed, you need to verify data encryption is enabled. Encryption is enabled by default for products and hard drive accessories.

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. Select the device you want to verify has an encrypted disk and select the Storage tab. Select the device in the device list and mouse over the Storage Media Column.
2. Examine the storage media data available in the pop-up it should show that the hard drive is enabled, and the encryption status should be "Encrypted."



	Device Model	IP Address	IP Hostname	Port (Any)	Sev	Hardware Address
	HP LaserJet M606	15.86.190.87	<Unknown>	1	✓	D0BF9C3099D1
	HP Color LaserJet M553	15.86.190.49	<Unknown>	1	✓	D0BF9C32ACB3

Device Model	IP Hostname	IP Address	Storage Media	SSD Encryption
HP Color LaserJet M553	<Unknown>	15.86.190.49	Storage Device count: 2	<Not supported>

Storage Media

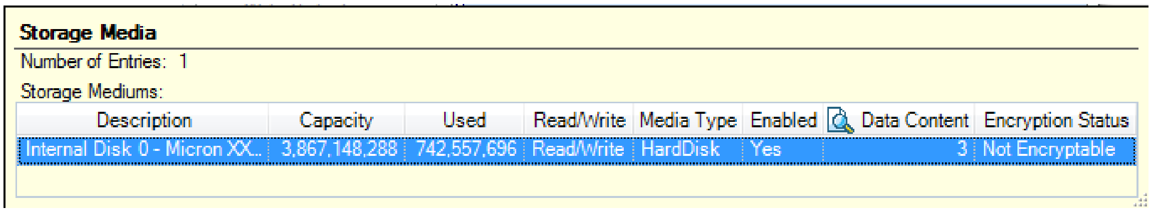
Number of Entries: 2

Storage Mediums:

Description	Capacity	Used	Read/Write	Media Type	Enabled	Data Content	Encryption Status
Internal Disk 0 - HP Secur...	320,072,933,376	731,412,480	Read/Write	HardDisk	Yes	3	Encrypted
Internal Disk 1 - Micron XX...	3,867,148,288	3,867,148,288	Read/Write	HardDisk	Yes	0	No Encrypted Disk

Figure 4: Shows the Storage Media pop-up details.

Figure 4 is an example of a disk that has not the Secure Hard Disk Accessory installed. The Highlighted line is the hard disk. The other listed disk is the original memory module which is no longer being used for customer data. As such it is listed as No Encrypted Disk. If the product does not have an accessory, the memory will show as shown in Figure 5.



Storage Media

Number of Entries: 1

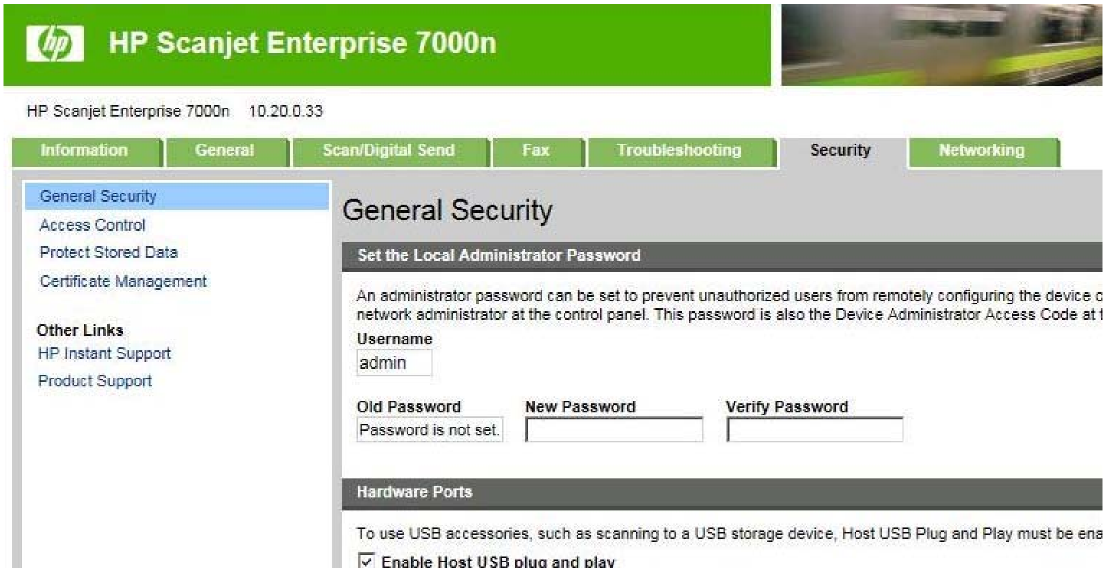
Storage Mediums:

Description	Capacity	Used	Read/Write	Media Type	Enabled	Data Content	Encryption Status
Internal Disk 0 - Micron XX...	3,867,148,288	742,557,696	Read/Write	HardDisk	Yes	3	Not Encryptable

Figure 5: Shows the memory of a printer without a hard drive showing status of **Not Encryptable**

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

1. Go to the EWS for each print device and select the Security tab. (Figure 6).



HP Scanjet Enterprise 7000n 10.20.0.33

General Security

Set the Local Administrator Password

An administrator password can be set to prevent unauthorized users from remotely configuring the device c network administrator at the control panel. This password is also the Device Administrator Access Code at t

Username: admin

Old Password: Password is not set.

New Password:

Verify Password:

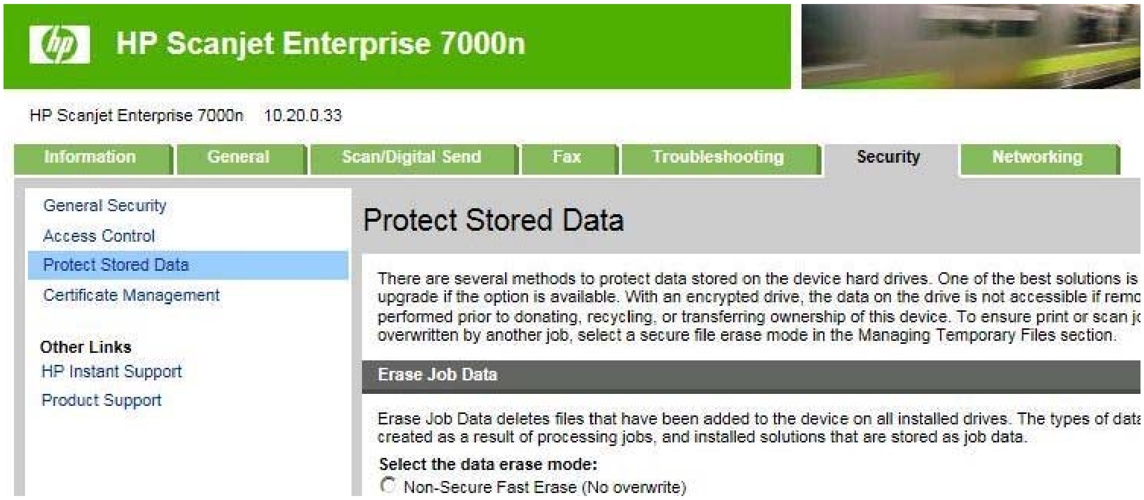
Hardware Ports

To use USB accessories, such as scanning to a USB storage device, Host USB Plug and Play must be ena

☑ Enable Host USB plug and play

Figure 6: Shows the content of the Security tab of your devices EWS.

2. Select **Protect Stored Data** from the left-hand menu list to view the Protect Stored Data Page (Figure 7).



Protect Stored Data

There are several methods to protect data stored on the device hard drives. One of the best solutions is upgrade if the option is available. With an encrypted drive, the data on the drive is not accessible if remo performed prior to donating, recycling, or transferring ownership of this device. To ensure print or scan jo overwritten by another job, select a secure file erase mode in the Managing Temporary Files section.

Erase Job Data

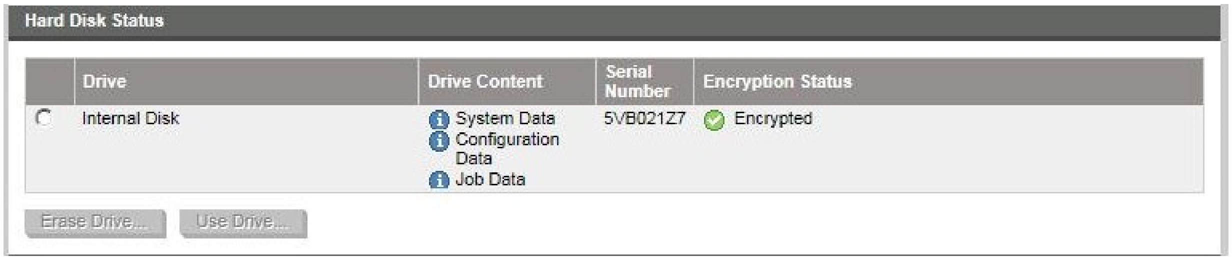
Erase Job Data deletes files that have been added to the device on all installed drives. The types of data created as a result of processing jobs, and installed solutions that are stored as job data.

Select the data erase mode:

○ Non-Secure Fast Erase (No overwrite)

Figure 7: Shows the Protect Stored Data settings page in the EWS.

3. In the Hard Disk Status section of the Protect Stored Data page, you can see the Encryption Status for that device. If you see a green checkmark, the device is encrypting your data properly (Figure 8).



Hard Disk Status

	Drive	Drive Content	Serial Number	Encryption Status
○	Internal Disk	System Data Configuration Data Job Data	5VB021Z7	✓ Encrypted

Figure 8: Shows the Hard Disk Status a green check means an encrypted disk is Installed and 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.

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

Configuring SNMPv3

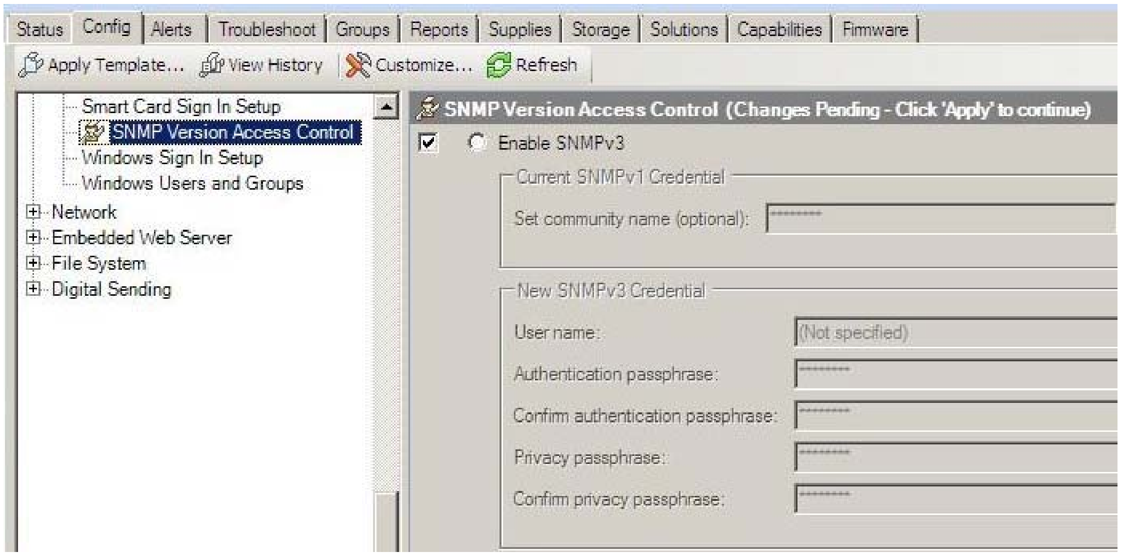
SNMPv3 provides encryption for communication between Web Jetadmin and MFPs. It helps to ensure that only authorized and authenticated administrators have access to the configuration settings of the MFPs. It also helps to ensure that no one can gather sensitive information, such as passwords, usernames,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

Click **Security** in the Configuration Categories menu (Figure 9) to view the options for configuration. From the Security Options select **SNMP Version Access Control**.



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

☑ ○ Enable SNMPv3

Current SNMPv1 Credential

Set community name (optional): *********

New SNMPv3 Credential

User name: (Not specified)

Authentication passphrase: *********

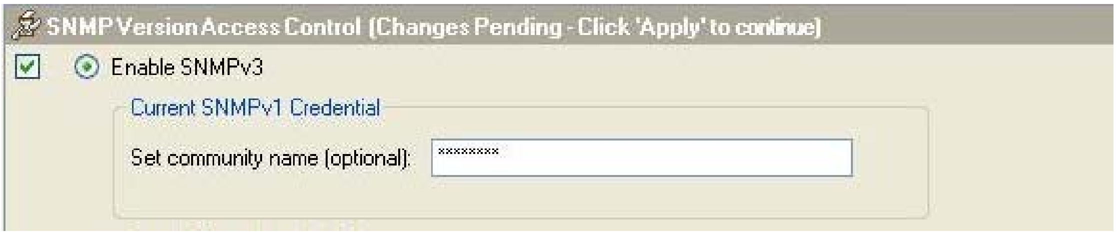
Confirm authentication passphrase: *********

Privacy passphrase: *********

Confirm privacy passphrase: *********

Figure 9: The Security category and SNMP Version Access Control settings.

On the **SNMP Version Access Control** menu and select the **Enable SNMPv3** checkbox (Figure 10).



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

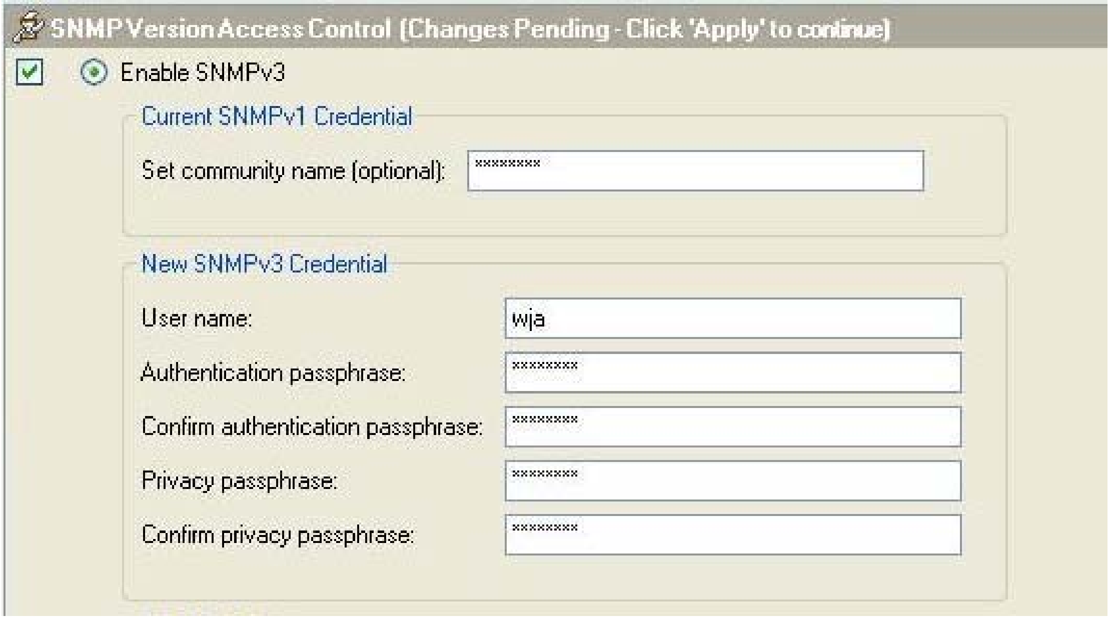
☑ ● Enable SNMPv3

Current SNMPv1 Credential

Set community name (optional): *********

Figure 10: Shows Enable SNMPv3 selected.

Once **Enable SNMPv3** has been selected, and fill in the **New User**, the **New Authentication Passphrase**, and the **New Privacy Passphrase** fields (Figure 11) in the New **SNMPv3 Credential section**. See below for details.



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

☑ ● Enable SNMPv3

Current SNMPv1 Credential

Set community name (optional): ********

New SNMPv3 Credential

User name: wja

Authentication passphrase: ********

Confirm authentication passphrase: ********

Privacy passphrase: ********

Confirm privacy passphrase: ********

Figure 11: The Enable SNMPv3 option has been selected and the New SNMPv3 Credential section is complete.

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 9 alphanumeric characters.

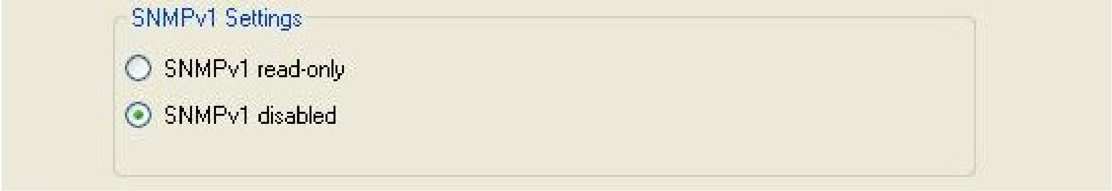
The **New Privacy Passphrase** field can be any word or phrase that is at least 9 alphanumeric characters.

CAUTION:

These instructions are for the initial configuration of SNMPv3. Once you finish this configuration, your devices 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 print devices is to restore them to factory default settings.

Web Jetadmin retains the SNMPv3 credentials for each device, 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.

Scroll down to the SNMPv1 Settings section, and select **SNMPv1 disabled** (Figure 12).



SNMPv1 Settings

○ SNMPv1 read-only

● SNMPv1 disabled

Figure 12: The SNMP Version 3 Only setting.

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

Choose Apply at the bottom of the SNMP Version Access Control configuration to apply the settings to the selected devices. 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 or other device will check for the SNMPv3 credentials.

Note:

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

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

Configuring Device Settings

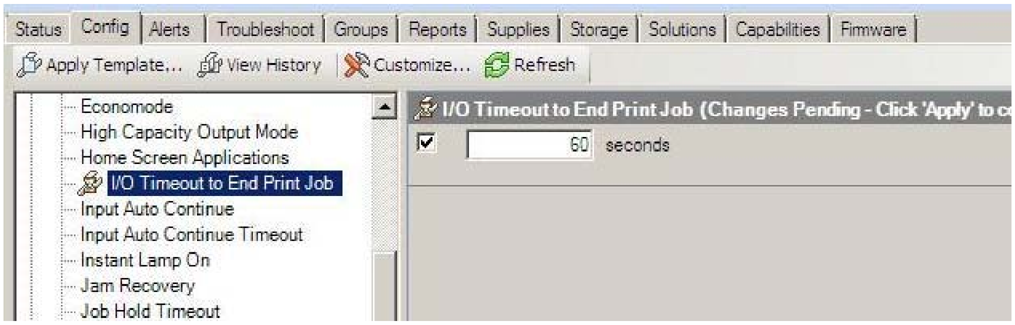
The **Device** category includes settings that affect some of the normal use of the print device. The following settings affect how jobs are stored, and how long your print device will wait before a job times out in a particular way.

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.

From the **Device** category select the **I/O Timeout to End Print Job** menu (Figure 13).
Click checkbox to enable the **I/O Timeout to End Print Job** setting and select a reasonable time the print device should wait between data packets.



I/O Timeout to End Print Job (Changes Pending - Click 'Apply' to c

☑ 60 seconds

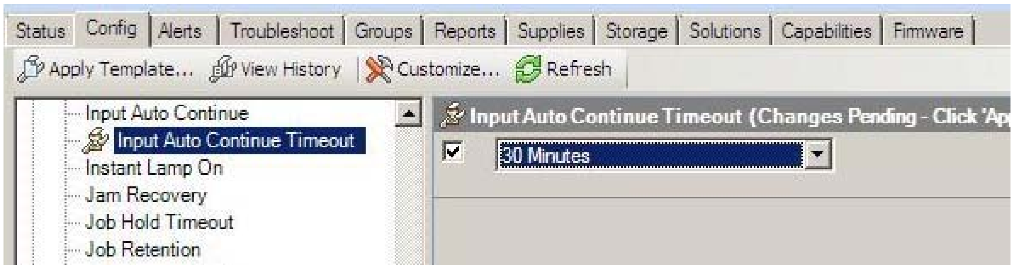
Figure 13: The I/O Timeout to End Print Job options.

Input Auto Continue Timeout

The Input Auto Continue Timeout allows you to specify the amount of time a device should wait before performing the default action when the specified media size for a job is not available. Setting this timeout will help prevent jobs sent with improper paper or media selections from tying up a print resource. To set this timeout follow the instructions below.

From the **Device** category, select the **Input Auto Continue Timeout** menu.

Click checkbox to enable the **Input Auto Continue Timeout** setting and select a reasonable time the print device should wait between data packets.



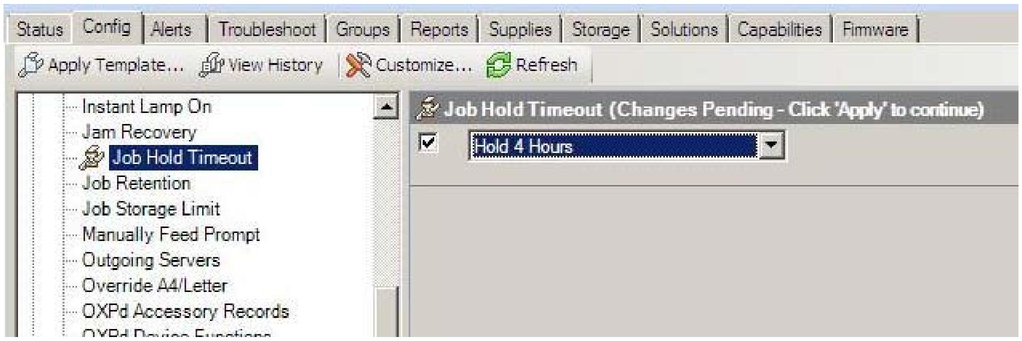
Input Auto Continue Timeout (Changes Pending - Click 'Ap

☑ 30 Minutes

Figure 14: The Input Auto Continue Timeout options.

Job Hold Timeout

From the **Device** category select the **Job Hold Timeout** menu (Figure 15).
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.



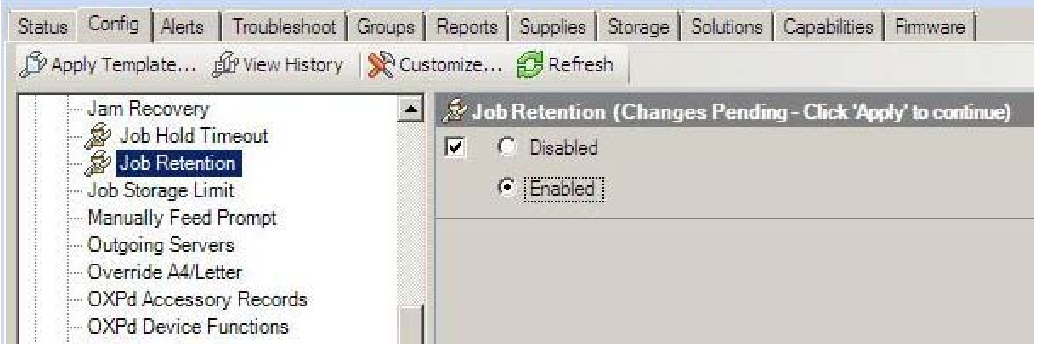
Job Hold Timeout (Changes Pending - Click 'Apply' to continue)

☑ Hold 4 Hours

Figure 15: The Job Hold Timeout options.

Job Retention

From the **Device** category select **Job Retention** (Figure 16).
Click checkbox to select **Job Retention** and select **Enabled**.



Job Retention (Changes Pending - Click 'Apply' to continue)

☑ ○ Disabled

● Enabled

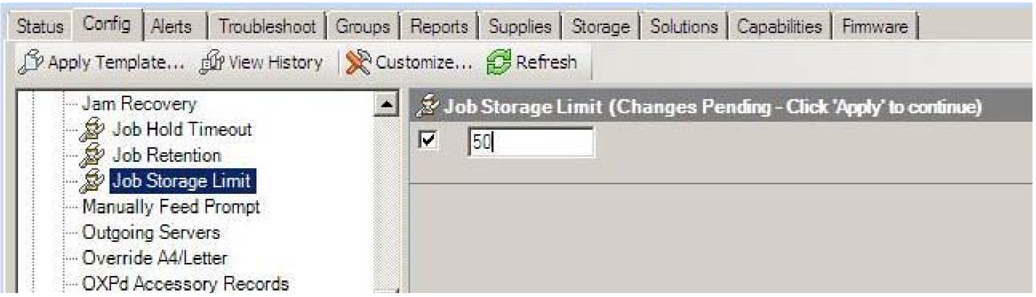
Figure 16: The Job Retention options.

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

Job Storage Limit

The Job Storage Limit allows you to specify the maximum number of stored jobs allowed on the printer. You will want to choose a number of jobs that is appropriate for your print devices and print usage in your environment. This setting can protect your printer from accepting more print jobs than it can effectively store.

From the **Device** category select the **Job Storage Limit** menu (Figure 17).
Click checkbox to enable the **Job Storage Limit** setting and select the number of allowable Stored Jobs.



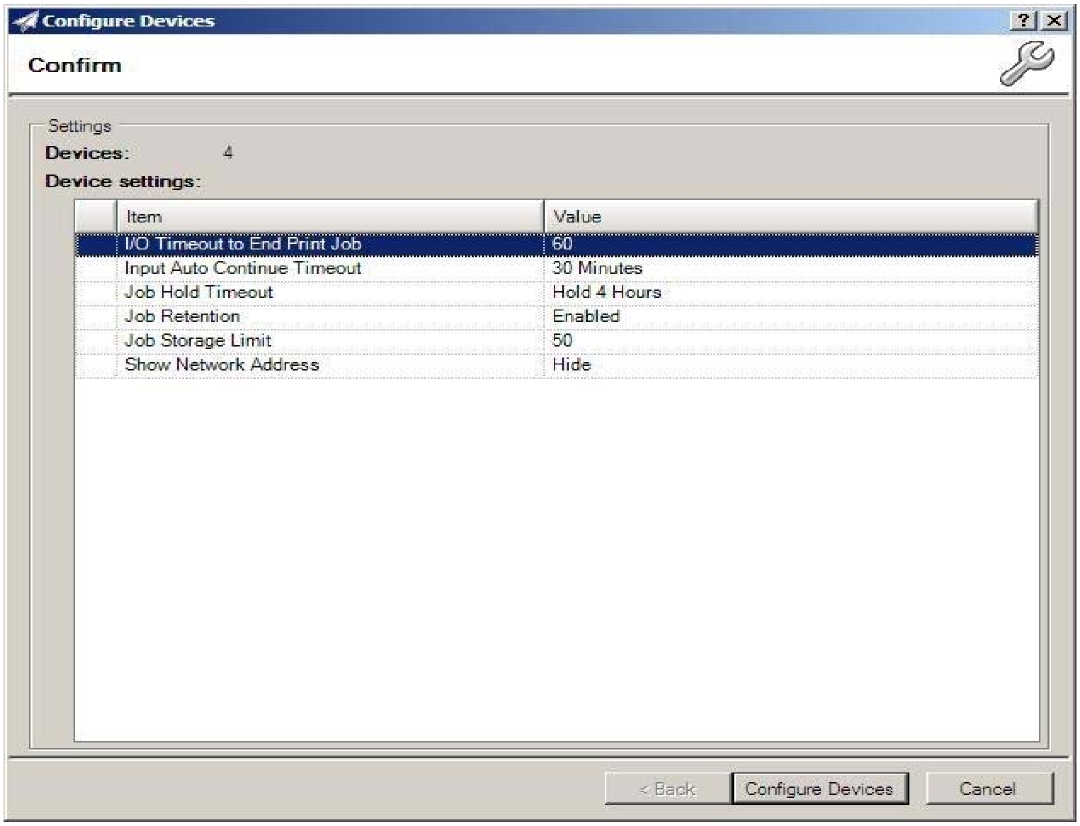
Job Storage Limit (Changes Pending - Click 'Apply' to continue)

☑ 50

Figure 17: The Job Storage Limit options.

Apply the Changes

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 18).



Devices: 4

Device settings:

Item	Value
I/O Timeout to End Print Job	60
Input Auto Continue Timeout	30 Minutes
Job Hold Timeout	Hold 4 Hours
Job Retention	Enabled
Job Storage Limit	50
Show Network Address	Hide

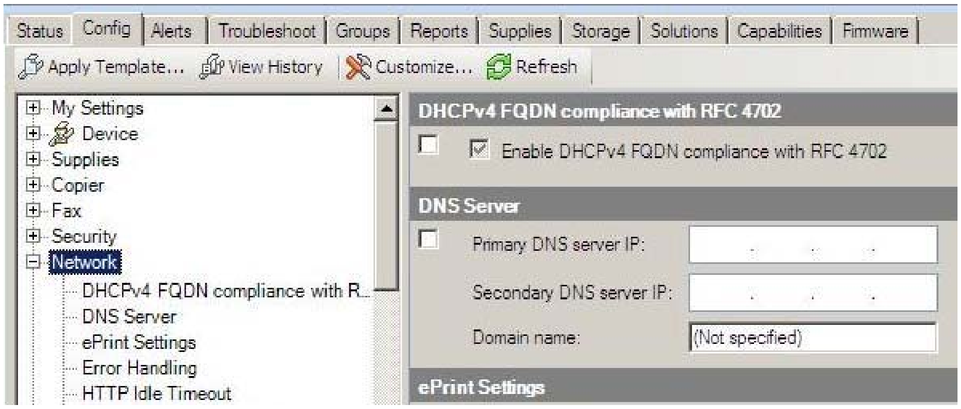
Figure 18: The Configure Devices dialogue box.

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

Configuring 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.

Click the **Network** category on the **Config** tab to expand the configuration options (Figure 19).



DHCPv4 FQDN compliance with RFC 4702

☐ ☑ Enable DHCPv4 FQDN compliance with RFC 4702

DNS Server

☐ Primary DNS server IP: . . .

Secondary DNS server IP: . . .

Domain name: (Not specified)

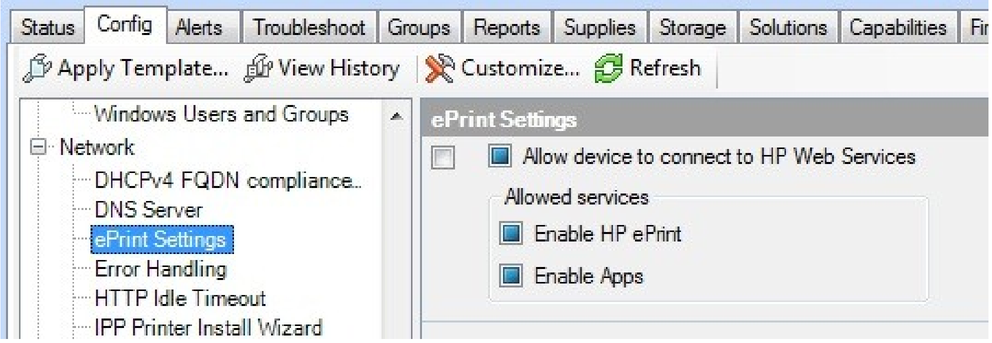
ePrint Settings

Figure 19: The Network Category.

e-Print and HP Web Services Settings

This option enables, disables or configures the ePrint feature on a device. It also allows you to enable, disable or configure HP Web Services and applications on your device. You can allow ePrint via Email or Simple Internet Printing. Unless e-Print, HP Web Services, or other applications are a critical part of your print environment we recommend disabling these features. If you are using the e-print enterprise server and not the HP cloud for e-print, you should refer to your administrators guide for any special settings that may be required to secure your solution.

Click to select **e-Print Settings** (Figure 19), and clear the checkboxes to **Disable**.



ePrint Settings

☐ ■ Allow device to connect to HP Web Services

Allowed services

■ Enable HP ePrint

■ Enable Apps

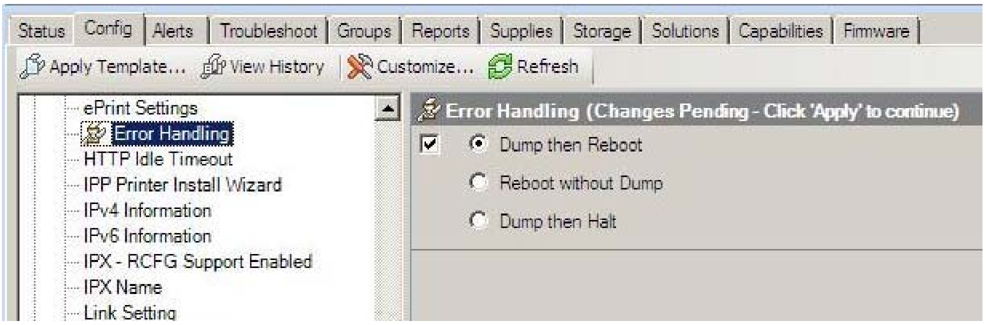
Figure 20: Disable HP ePrint, HP Web Services, and Apps

Error Handling

The Error Handling option (Figure 21) specifies how the Jetdirect Print Server handles error conditions. The settings are:

- **Dump then Reboot** does a memory dump them 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.



Error Handling (Changes Pending - Click 'Apply' to continue)

☑ ● Dump then Reboot

○ Reboot without Dump

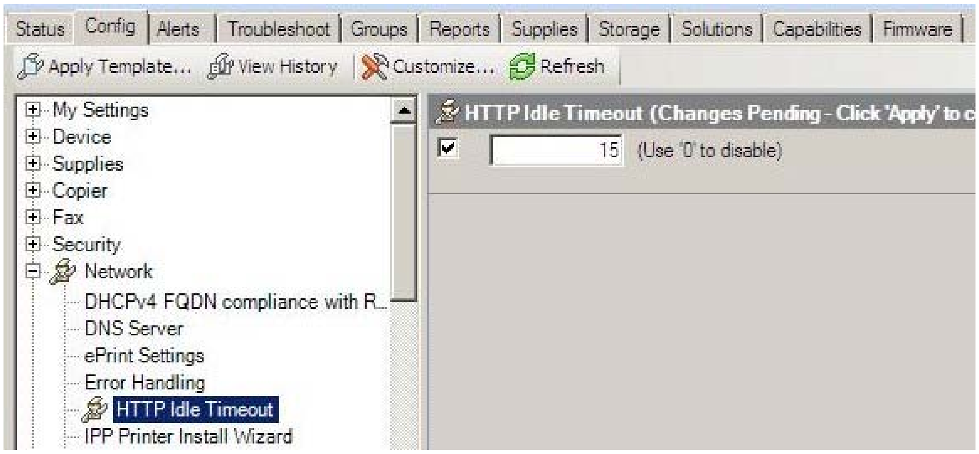
○ Dump then Halt

Figure 21: The Error Handling option.

HTTP Idle Timeout

The HTTP Idle Timeout option configures the amount of time an HTTP connection to the device remains open. This can prevent the need to physically go to the device when you have problem jobs that lack proper end of job signals or other hung connections. After the HTTP Idle Timeout has expired, the idle connection will be closed to allow for a new connection to your device. All devices covered in this document support the **HTTP Idle Timeout** option. To set the HTTP Idle Timeout option:

Click **HTTP Idle Timeout** (Figure 22).



HTTP Idle Timeout (Changes Pending - Click 'Apply' to c

☑ 15 (Use '0' to disable)

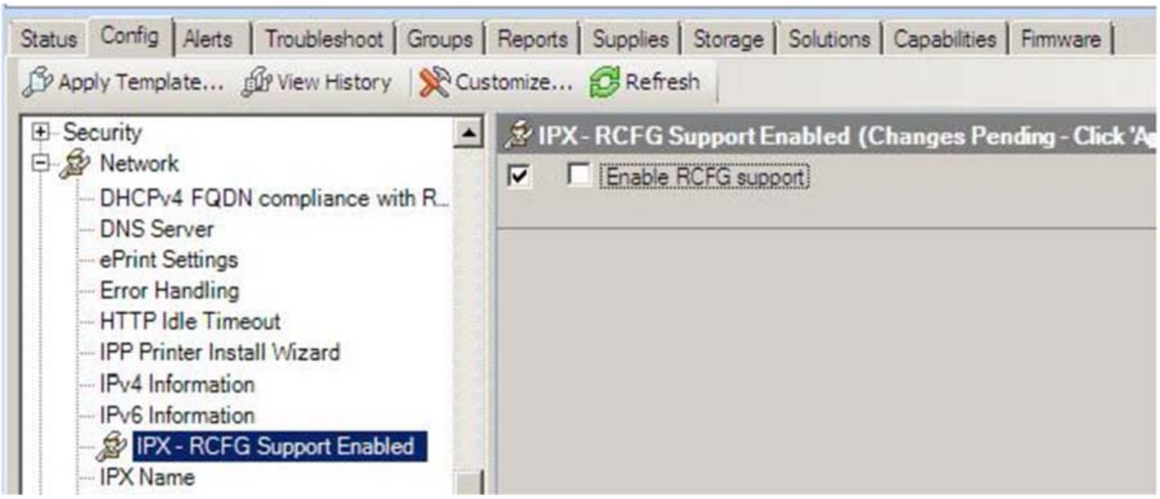
Figure 22: The HTTP Idle Timeout option.

In the input field, type a reasonable number of seconds (5 to 60) for the device to wait on an idle connection before moving on. If you spool large documents on a regular basis you will want to set this on the higher end. The default setting is 15.

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.

Click **IPX -- RCFG Support Enabled** (Figure 22) and leave **Enable RCFG Support** blank to disable it.



IPX - RCFG Support Enabled (Changes Pending - Click 'A

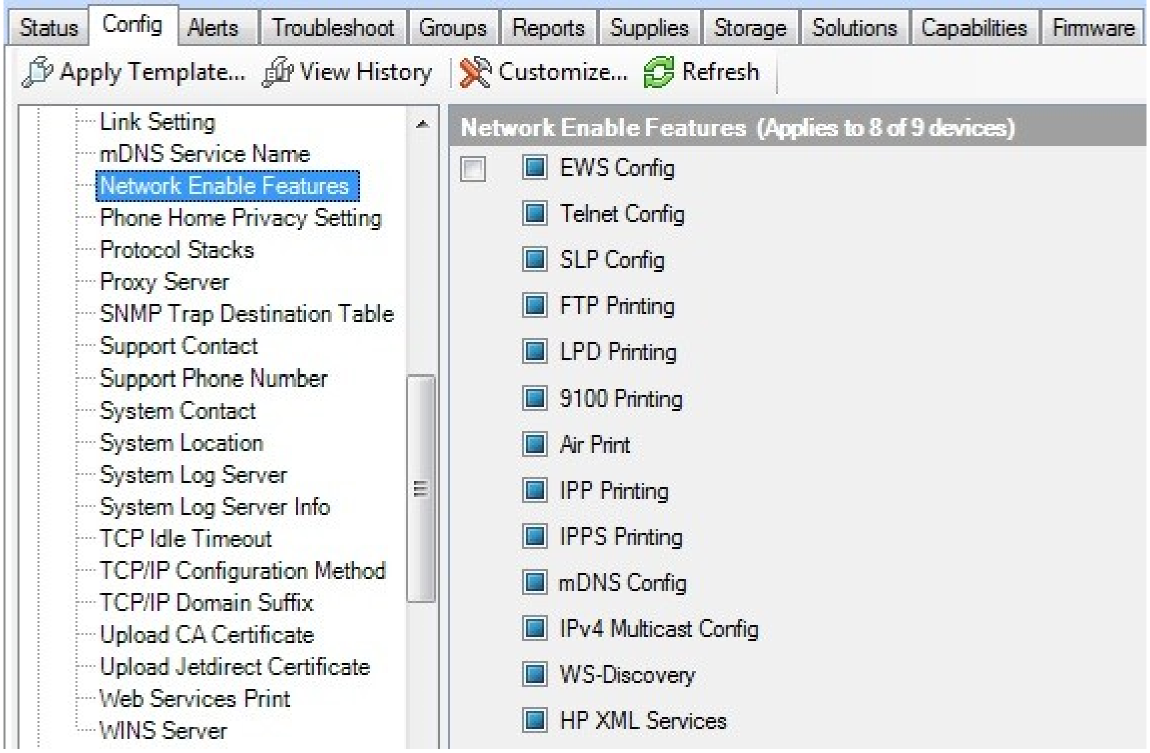
☑ ☐ Enable RCFG support

Figure 23 The RCFG Setting option.

Network Enable Features

To enable or disable print features on your MFP you:

Click **Enable Features** from the configuration options in the Network category (Figure 23).



Network Enable Features (Applies to 8 of 9 devices)

☐ ▣ EWS Config
▣ Telnet Config
▣ SLP Config
▣ FTP Printing
▣ LPD Printing
▣ 9100 Printing
▣ Air Print
▣ IPP Printing
▣ IPPS Printing
▣ mDNS Config
▣ IPv4 Multicast Config
▣ WS-Discovery
▣ HP XML Services

Figure 24: The Enable Features option.

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*** ***NOTE: The recommendation is to disable **EWS Config**, 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 **Telnet Config** prevents access to configuration settings and other features through Telnet.
SLP Config	Disabled	Disabling **SLP Config** prevents access to configuration settings and other features through SLP.
FTP Printing	Disabled	Disabling **FTP Printing** prevents access to configuration settings and other features through FTP. It also prevents printing through FTP.
LPD Printing	Disabled	Disabling **LPD Printing** prevents access to configuration settings and other features through LPD. It also prevents printing through LPD.
9100 Printing	Enabled	**9100 Printing** is the access point for normal printing through standard HP print drivers.
Air Print	Disabled	Disabling **Air Print** prevents also prevents printing via Air Print. If you do not operate in an environment that supports this feature, we recommend disabling this feature.
IPP Printing	Disabled	Disabling **IPP Printing** prevents access to configuration settings and other features through the IPP. It also prevents printing through IPP. If your require IPP to be enabled. We highly recommend enabling IPPS.

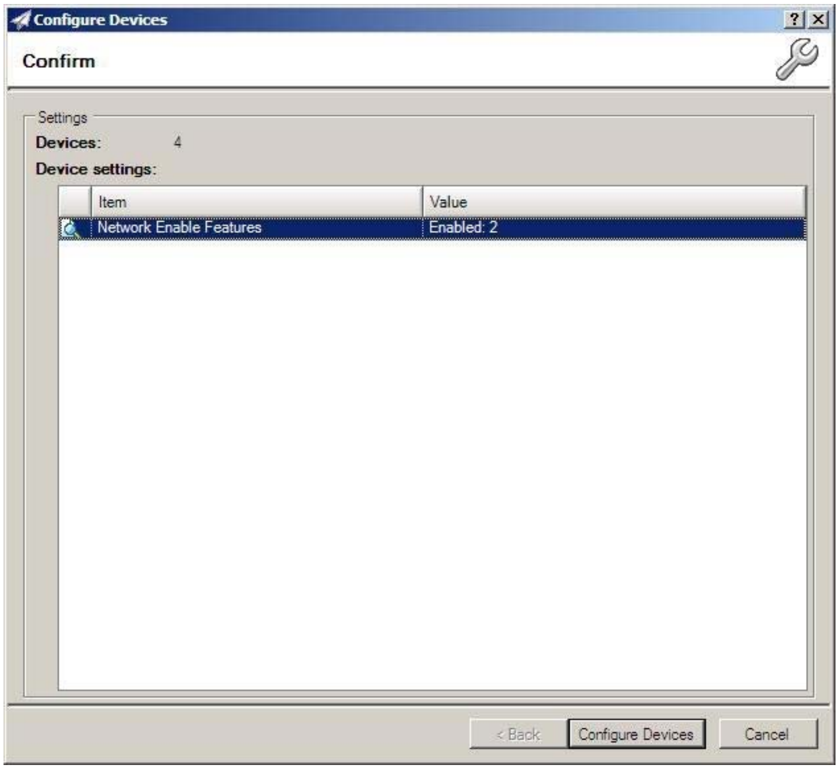
IPPS Printing	Disabled	Disabling **IPPS** when IPP is not in use is your only option. When IPP is enabled, the IPPS Printing setting enables the Internet Printing Protocol over SSL. IPPS provides a secure method for sending print jobs to the device over the Internet or intranet.
MDNS Config	Disabled	Disabling **MDNS Config** prevents access to configuration settings and other features through **MDNS**.
IPv4 Multicast Config	Disabled	Disabling **IPv4 Multicast Config** prevents access to configuration settings and other features through IPv4 Multicast.
WS-Discovery	Disabled	Disabling **WS-Discovery** prevents systems from using WS-Discovery for discovering or browsing printers on the network.
HP XML Services	Disabled	Disabling **HP XML Services** prevents HP Web services from accessing XML-based data on an HP print server.

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.

Click **Apply** in the lower right-hand corner to view the Configure Devices dialogue box. (Figure 25). Review your selections carefully before clicking on the **Configure Devices** button.



Confirm

Settings

Devices: 4

Device settings:

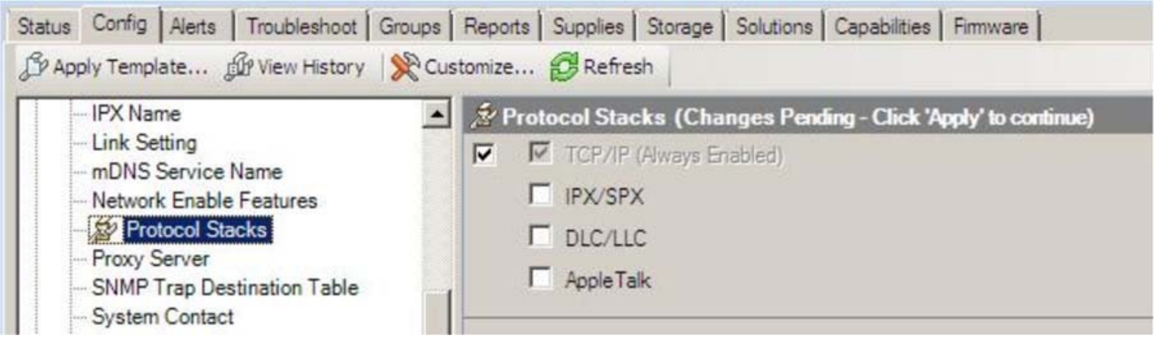
Item	Value
Network Enable Features	Enabled: 2

Figure 25: Review your Enable Features Configuration selections before configuring your devices.

Protocol Stacks

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

Click to select **Protocol Stacks** (Figure 25) and deselect all unused protocol stacks as applicable to your network. See the table below.



Protocol Stacks (Changes Pending - Click 'Apply' to continue)

☑ ☑ TCP/IP (Always Enabled)

☐ IPX/SPX

☐ DLC/LLC

☐ AppleTalk

Figure 26: The Protocol Stacks options.

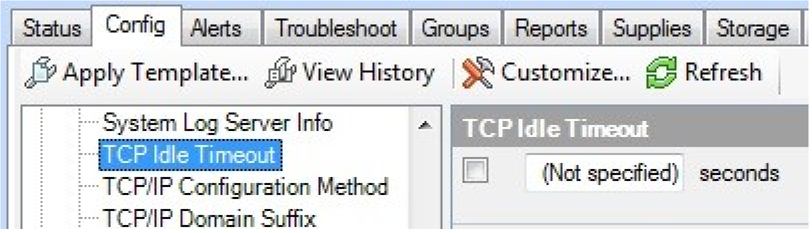
The following table lists each protocol with the recommended setting and an explanation:

Protocol Stack	Recommended Setting	Explanation
TCP/IP	Always enabled	This is the normal operating protocol for the MFPs.
IPX/SPX	Leave blank to disable	This setting disables access for Novell servers.
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.

TCP Idle Timeout

The TCP Idle Timeout option configures the amount of time a TCP/IP connection to the device remains open. This can prevent the need to physically go to the device when you have problem jobs or other hung connections. After the TCP Idle Timeout has expired, the idle connection will be closed to allow for a new connection to your device. All devices covered in this document support the **TCP Idle Timeout** option. To set the HTTP Idle Timeout option:

Click **TCP Idle Timeout** (Figure 26).



TCP Idle Timeout

□ (Not specified) seconds

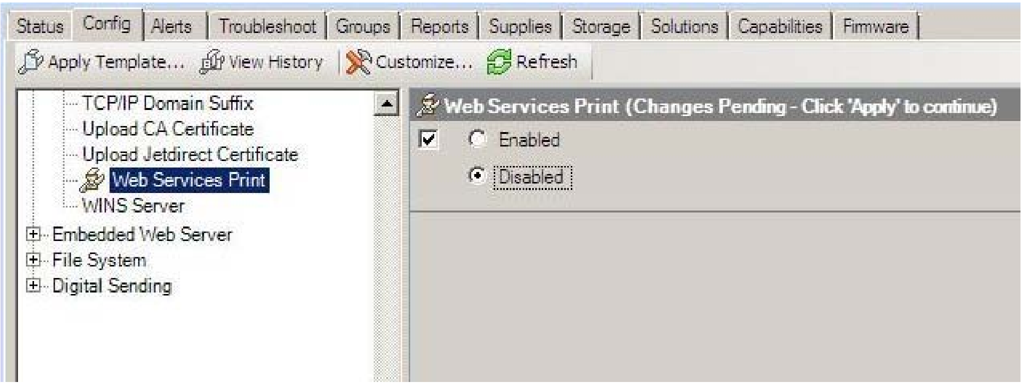
Figure 27: The TCP Idle Timeout option.

In the input field, type a reasonable number of seconds (5 to 60) for the device to wait on an idle connection before moving on. If you spool large documents on a regular basis you will want to set this on the higher end. The default setting is 15.

Web Services Print

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

Click to select **Web Services Print** (Figure 28) and select **Disabled**.



Web Services Print (Changes Pending - Click 'Apply' to continue)

☑ ○ Enabled

● Disabled

Figure 28: Disabling Web Services Print.

Apply your Changes

Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices.

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

Configuring 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

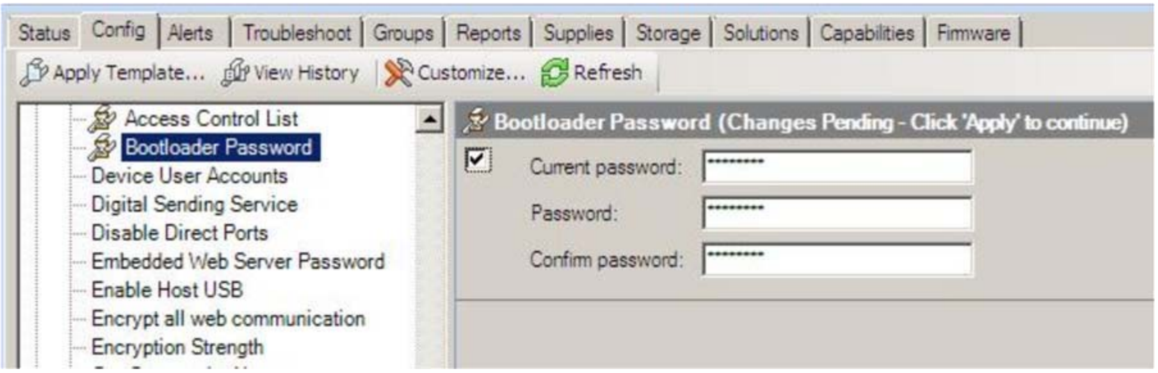
The Bootloader password protects features, such as the MFP reset options that are available on the MFP control panel. These features are not commonly known, but they can severely affect the MFPs if they are executed improperly. The Bootloader password is not configured by default.

CAUTION:

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.

Be very careful to remember the configured bootloader password. A hardware replacement may be required to recover from a forgotten Bootloader Password.

On the Config tab under the **Security** category page, select the **Bootloader Password** option (Figure 28).



Bootloader Password (Changes Pending - Click 'Apply' to continue)

☑ Current password: *********

Password: *********

Confirm password: *********

Figure 29: The Bootloader Password option.

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

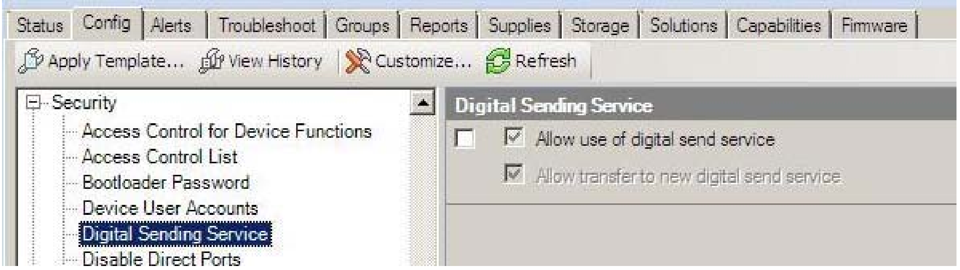
Note:

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.

Digital Sending Service

The Digital Sending Service is used when your print infrastructure utilizes a DSS server or other HP print solutions. If you have a print infrastructure, keep Allow use of digital send service checked. Otherwise, deselect this checkbox to prevent from unauthorized use of this service.

On the Config tab under the **Security** category page, select the **Digital Sending Service** option (Figure 30).



Digital Sending Service

□ ☑ Allow use of digital send service

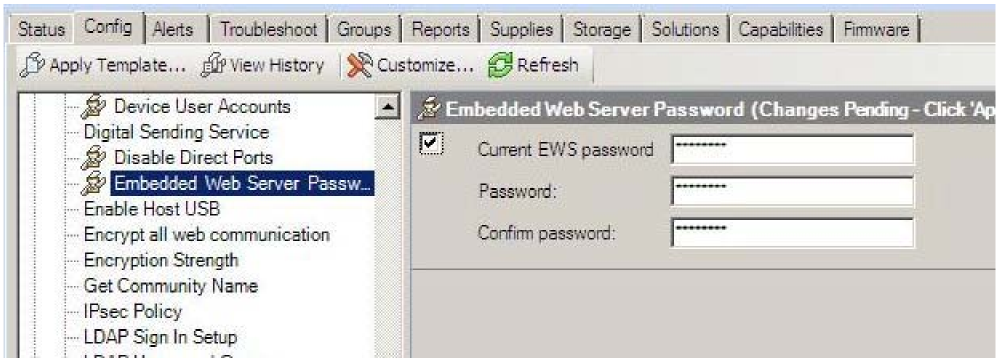
☑ Allow transfer to new digital send service

Figure 30: The Digital Sending Service option.

Embedded Web Server 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.

Click **Embedded Web Server Password** under the **Security** category (Figure 31).



Embedded Web Server Password (Changes Pending - Click 'Ap

☑

Current EWS password: *********

Password: *********

Confirm password: *********

Figure 31: The Embedded Web Server Password options.

Type a password of 9 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. Repeat the password exactly in the **Repeat Password** field.

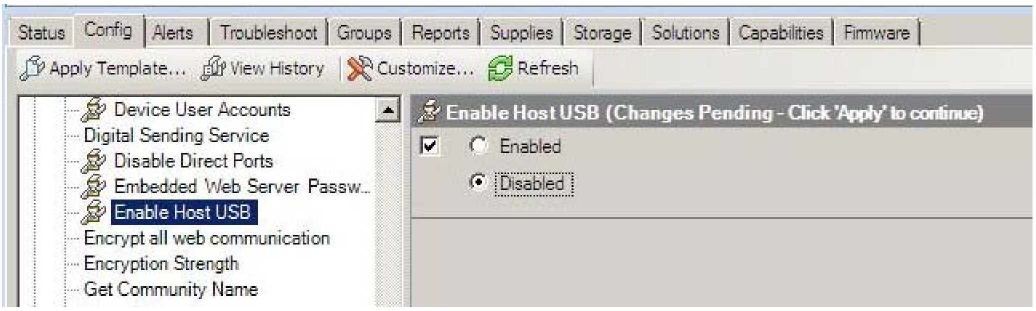
Note:

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.

Enable Host USB

The Enable Host USB Feature allows you to enable or disable use of USB accessories. An Example of this would be scanning to a USB storage device. If you disable this feature, applications which require host USB plug and play (such as the save to USB application) will automatically be disabled. If you are not using this functionality in your environment, we recommend that this feature be **Disabled**. Disabling this feature will not affect your smart card solution or print from USB. To set Enable Host USB:

Click to select the **Enable Host USB** (Figure 31) and click to select **Disabled**.



Enable Host USB (Changes Pending - Click 'Apply' to continue)

☑ ○ Enabled

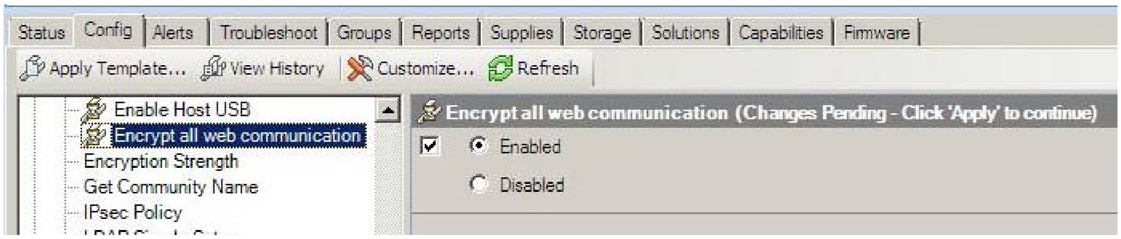
● Disabled

Figure 32: The Enable Host USB option.

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:

Click **Encrypt all web communication**, and then select **Enabled** to enable HTTPS communication between the Jetdirect Print Server and any web browser (Figure 33).



Encrypt all web communication (Changes Pending - Click 'Apply' to continue)

☑ ● Enabled

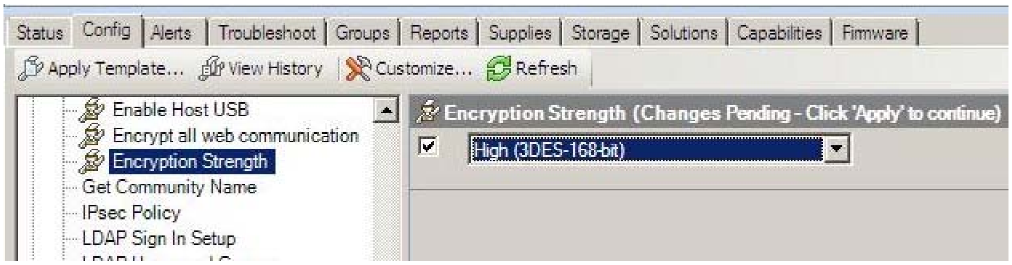
○ Disabled

Figure 33: 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:

Click **Encryption Strength** in the **Security** category (Figure 34).
Click the **Encryption Strength** dropdown menu, and select the highest setting that your browser supports.



Encryption Strength (Changes Pending - Click 'Apply' to continue)

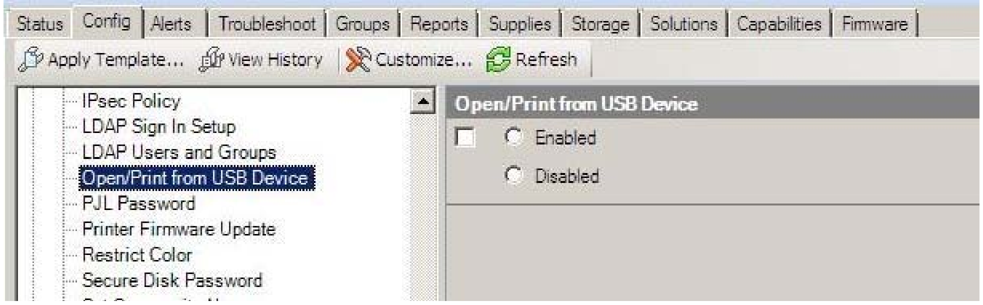
☑ High (3DES-168-bit)

Figure 34: The Encryption Strength option.

Open/Print from USB Device

The Open/Print from USB Device feature allows you to print documents stored on a USB device. Leaving this option enabled could allow people without access to your network print documents from your devices at walk up. We recommend that this feature be **Disabled**. Disabling this feature will not affect your smart card solution or Host USB functionality. To set Enable Host USB:

Click to select the **Open/Print from USB** (Figure 34) and click to select **Disabled**.



Open/Print from USB Device

☐ ○ Enabled

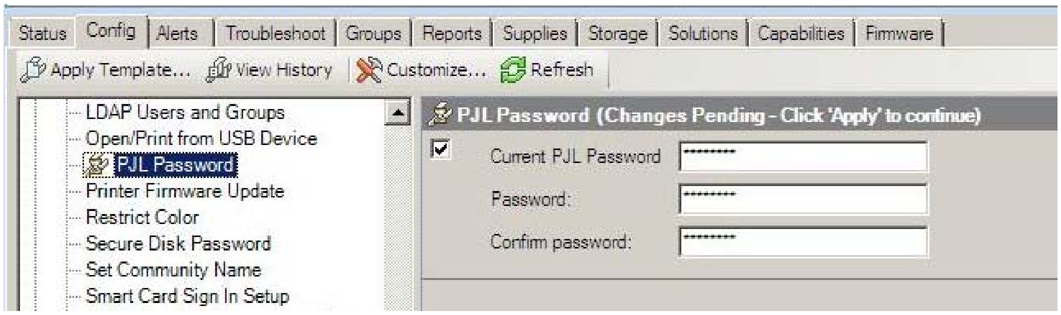
○ Disabled

Figure 35: The Open/Print from USB option.

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. If you do not set this password, you are vulnerable to having your device settings including your control panel display altered. To set the PJL Password:

Click **PJL Password** under the **Security** category (Figure 36).



PJL Password (Changes Pending - Click 'Apply' to continue)

☑ Current PJL Password *********

Password: *********

Confirm password: *********

Figure 36: The PJL Password option.

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. Do not use the same PJL password for all of your print devices as this can significantly increase the risk of having your PJL password guessed by an attacker.

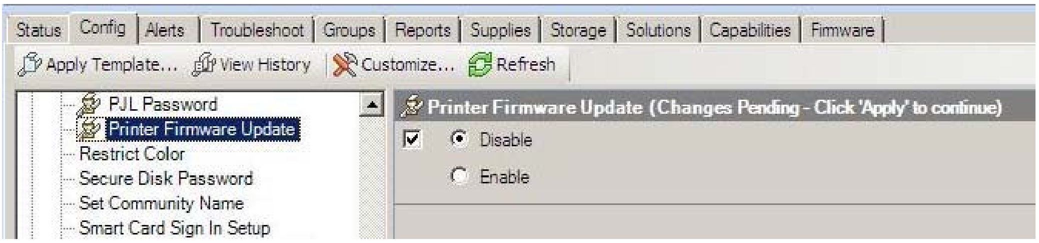
Note:

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:

Click to select **Printer Firmware Update** (Figure 37) and select **Disable**.



Printer Firmware Update (Changes Pending - Click 'Apply' to continue)

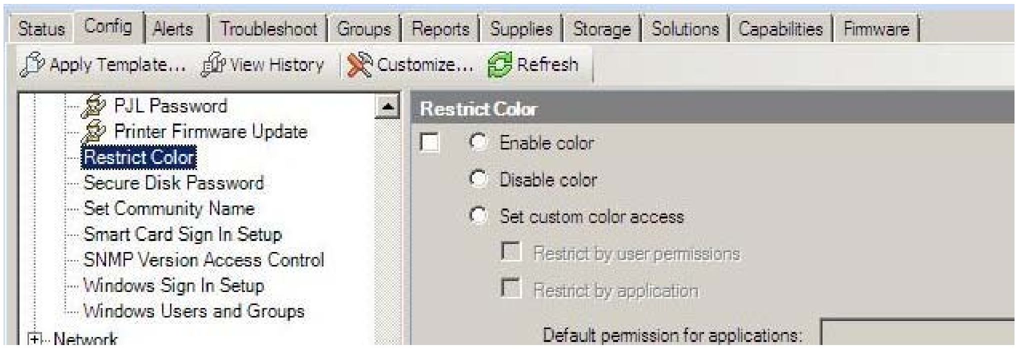
☑ ● Disable

○ Enable

Figure 37: The Printer Firmware Update option.

Restrict Color

The Restrict Color options (Figure 38) 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.



Restrict Color

□ ○ Enable color
○ Disable color
○ Set custom color access
□ Restrict by user permissions
□ Restrict by application
Default permission for applications:

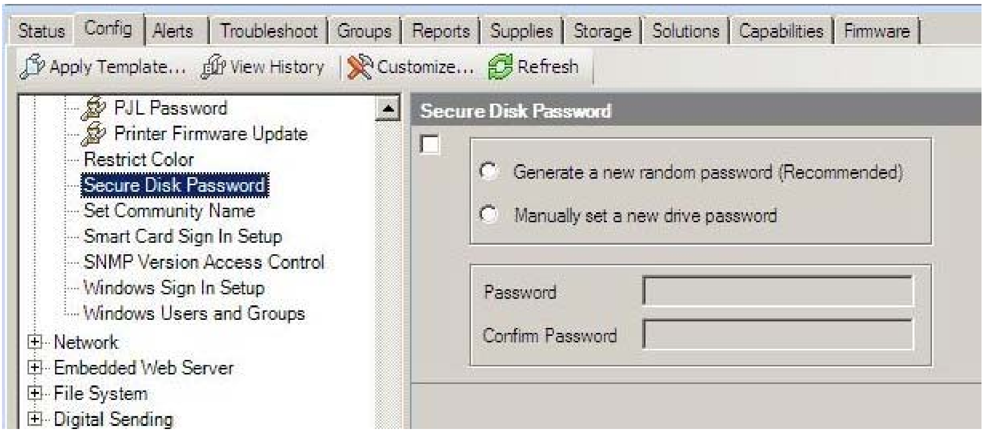
Figure 38: The Color Access Control options.

Secure Disk Password

The Secure Disk Password option (Figure 39) allows you to configure the password for a secure disk. If you change the password, no data on the secure disk is lost.

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.



Secure Disk Password

□
○ Generate a new random password (Recommended)
○ Manually set a new drive password

Password
Confirm Password

Figure 39: The Secure Disk Encryption Mode option.

Apply the Changes

Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices

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

Configuring 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.

Blocked Fax List Settings

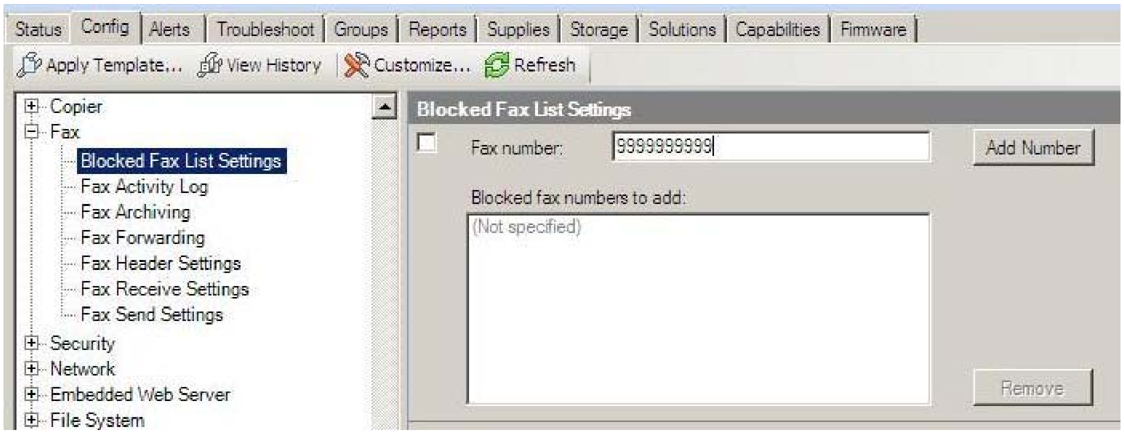
The **Blocked Fax List** option (Figure 39) allows you to maintain the list of fax numbers that are blocked by the fax device. Your organization can prevent unwanted solicitation by adding the fax number to the blocked fax list.

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.

Click Fax on the Config tab and select Blocked Fax List Settings.



Blocked Fax List Settings

□ Fax number: 9999999999

Blocked fax numbers to add:

(Not specified)

Figure 40: The Blocked Fax List settings.

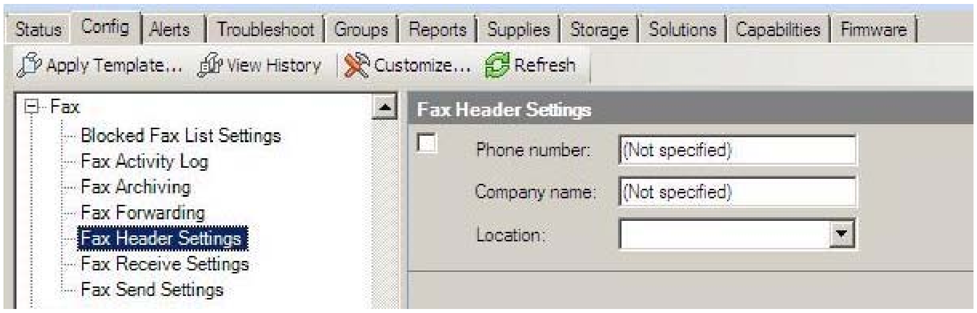
Enter a Fax number you wish to block and clock the Add Number button. To remove a blocked fax number, highlight that number and click the Remove button.

Fax Header Settings

The Fax Header Settings option (Figure 40) allows you to set the phone number company name and location for all your faxes. We recommend setting these options.

Follow these instructions to configure Fax Printing:

Click **Fax** on the **Config** tab, and select **Fax Header Settings**



Fax Header Settings

□ Phone number: (Not specified)

Company name: (Not specified)

Location:

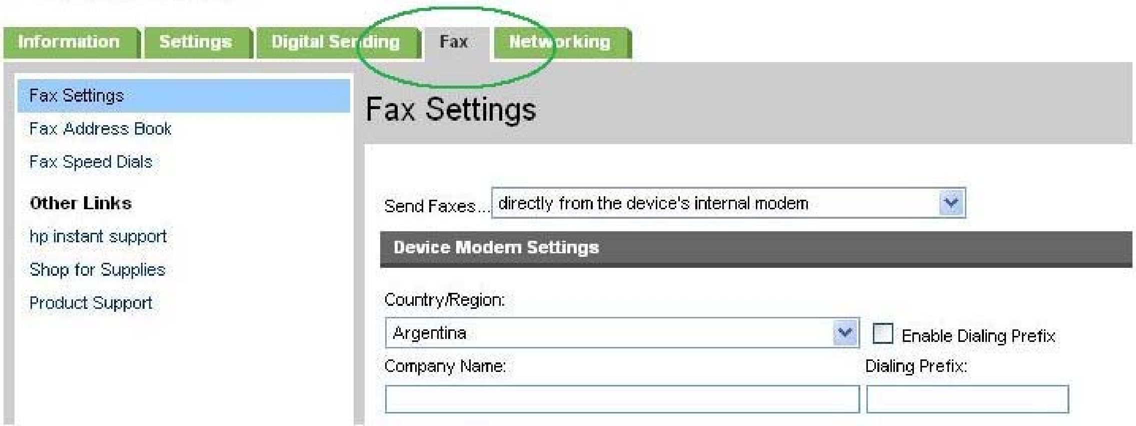
Figure 41: Fax Header settings.

Enter the Phone number, Company name, and location you wish to send with your faxes.

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. 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 42).



Fax Settings

Send Faxes... directly from the device's internal modem

Country/Region: Argentina

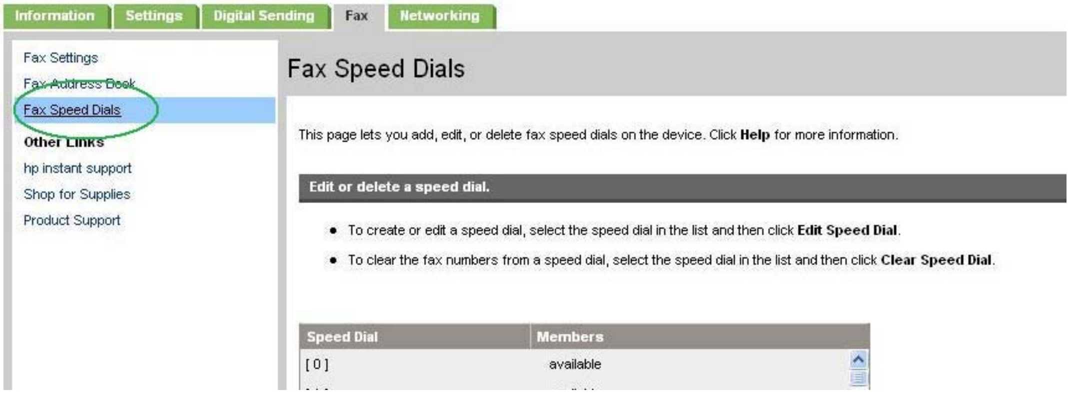
□ Enable Dialing Prefix

Company Name:

Dialing Prefix:

Figure 42: The Fax Settings Page.

2. Click to select Fax Speed Dials on the left-hand menu (Figure 43).



Fax Speed Dials

This page lets you add, edit, or delete fax speed dials on the device. Click **Help** for more information.

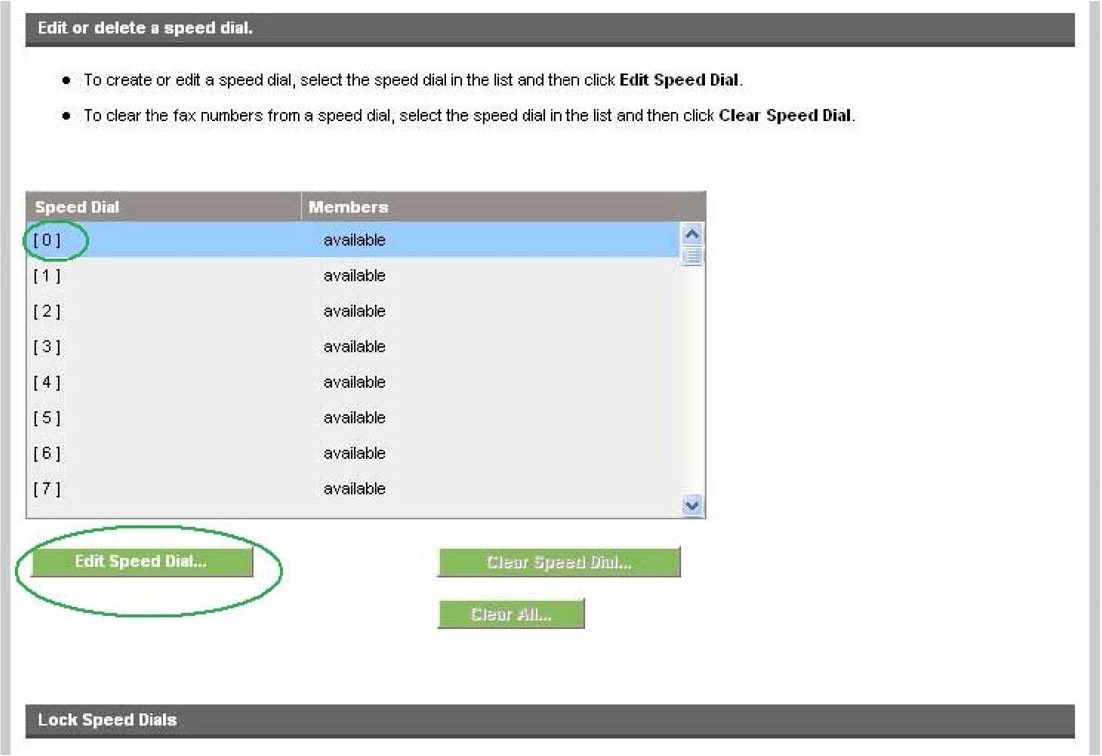
Edit or delete a speed dial.

- 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

Figure 43: Fax Speed Dials selection and page.

3. Set any speed-dials you wish to have by selecting the speed-dial number and clicking the Edit Speed Dial button (Figure 44).



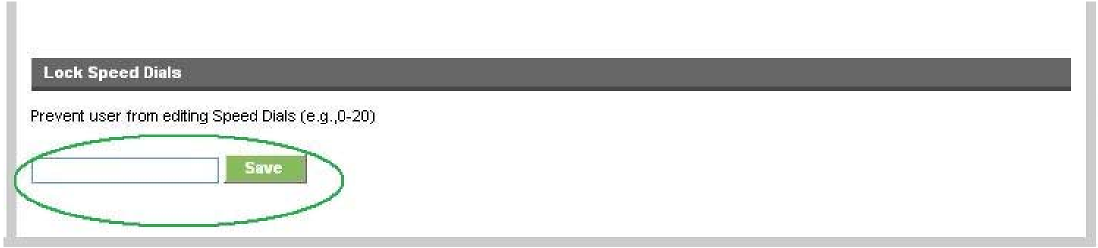
Edit or delete a speed dial.

- 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

Figure 44: The Fax Speed Dials configuration button.

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 45).



Lock Speed Dials

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

Figure 45: The Fax Speed Dials lockdown box

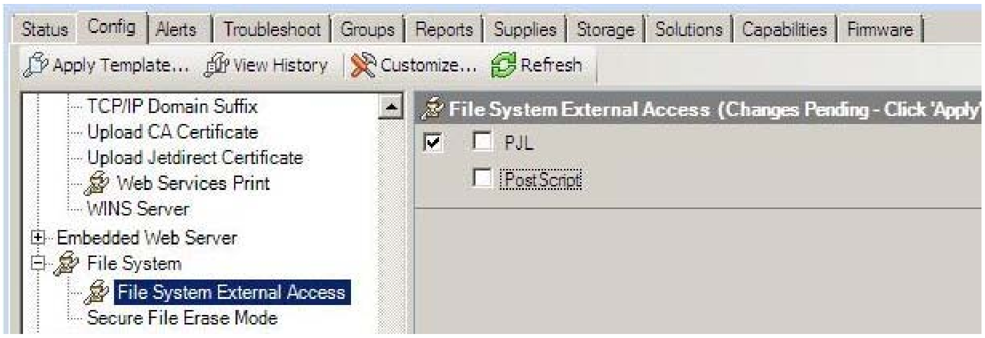
Configuring MFP File System Settings

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:

Click the **File System** category to select **File System External Access** (Figure 46).



File System External Access (Changes Pending - Click 'Apply'

☑ ☐ PJL

☐ PostScript

Figure 46: The File System External Access options.

Disable all options (see the table below).

The following table lists and explains the recommended settings:

File system Access Option	Recommended Setting	Explanation
PJL	Disabled	Prevents access to the file system through this protocol
PostScript	Disabled	Prevents access to the file system through this protocol. NOTE: Disabling PostScript may affect interactions with third party applications.

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.

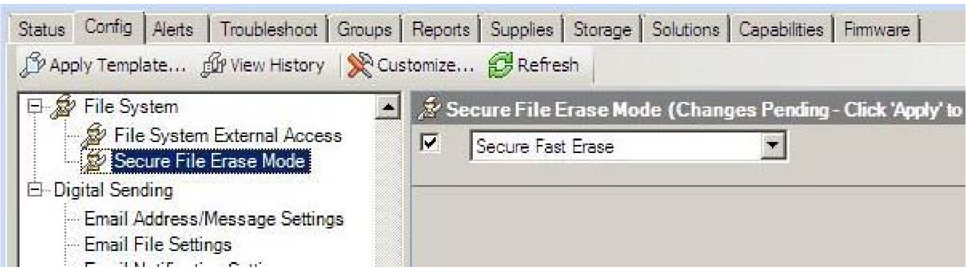
Use **Secure Sanitizing Erase** to meet stringent security requirements such as Department of Defense standards.

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:

Click to select **Secure File Erase Mode** (Figure 47) and view the options in the dropdown menu.



Secure File Erase Mode (Changes Pending - Click 'Apply' to

☑ Secure Fast Erase

Figure 47: The Secure File Erase Mode setting.

Select **Secure Fast Erase** or **Secure Sanitizing Erase** if you require maximum security.

Apply the Changes

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.

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.

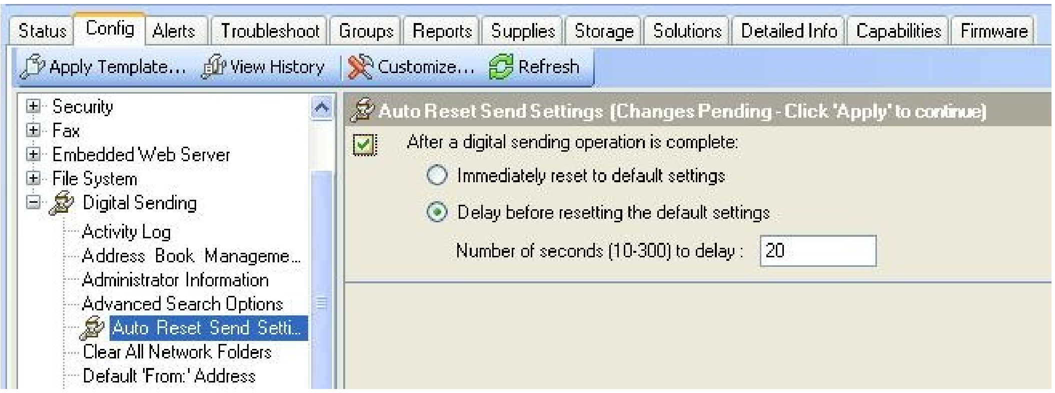
Note:

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 additional 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:

Click to select **Auto Reset Send Setting** from the **Digital Sending** category (Figure 48).



Auto Reset Send Settings (Changes Pending - Click 'Apply' to continue)

☑ After a digital sending operation is complete:

○ Immediately reset to default settings

● Delay before resetting the default settings

Number of seconds (10-300) to delay : 20

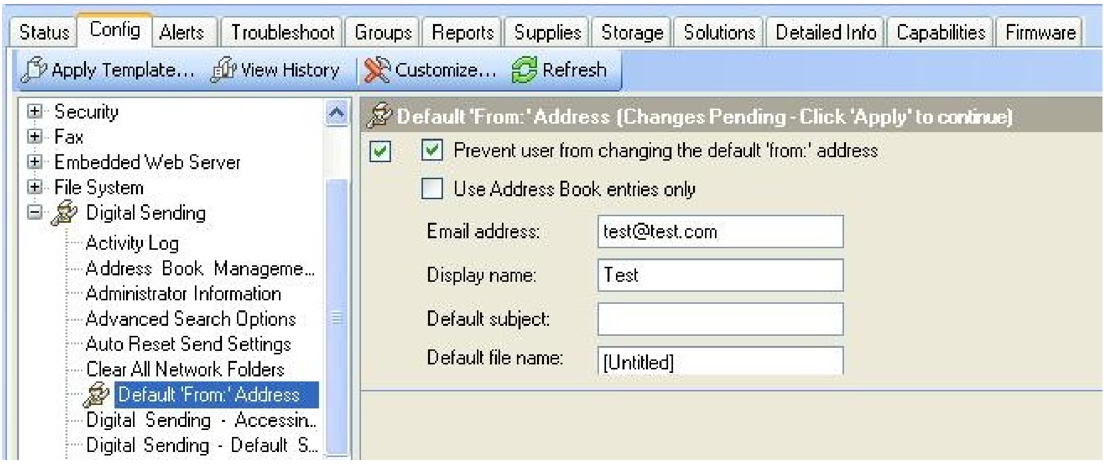
Figure 48: The Time-outs options.

Select Delay before resetting the default settings.
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.
Select **Immediately reset to default settings** to immediately logoff the current session.

Email Address/Message Settings - 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**:

Scroll down and click to select **Default 'From:' Address** (Figure 49).



Default 'From:' Address (Changes Pending - Click 'Apply' to continue)

☑ ☑ Prevent user from changing the default 'from:' address

□ Use Address Book entries only

Email address: test@test.com

Display name: Test

Default subject:

Default file name: [Untitled]

Figure 49: The Default 'From:' Address options.

Click to select Prevent user from changing the Default 'From:' Address.
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.

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

Apply the Changes

Click the **Apply** button located in the bottom right hand corner to apply the settings to the selected devices.

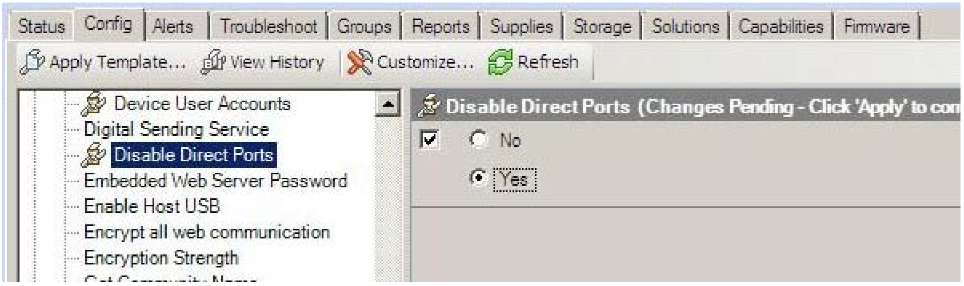
Configuring Final Settings

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:

Go to the **Security** page and click to select **Disable Direct Ports** (Figure 50).



Disable Direct Ports (Changes Pending - Click 'Apply' to con

☑ ○ No

● Yes

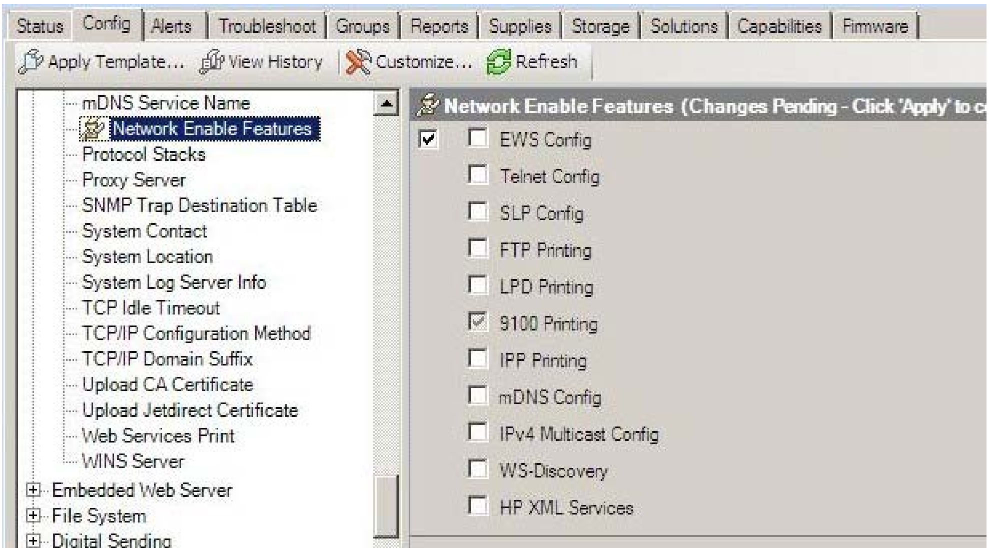
Figure 50: The Disable Direct Ports option.

Click to select the **Disable Direct Ports** option to the right.
Select **Yes**.
Click **Apply** at the bottom of the page.
Wait for a few minutes to allow the products 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:

Go to the **Network** category and click to select **Enable Features** (Figure 51).



Network Enable Features (Changes Pending - Click 'Apply' to c

☑

☐ EWS Config

☐ Telnet Config

☐ SLP Config

☐ FTP Printing

☐ LPD Printing

☑ 9100 Printing

☐ IPP Printing

☐ mDNS Config

☐ IPv4 Multicast Config

☐ WS-Discovery

☐ HP XML Services

Figure 51: The Enable Features option.

Click to disable EWS Config**.**

Advanced Security for Multiple HP Devices

This chapter will provide some tips for configuring HP security features that require network specific information to operate correctly using HP Web Jetadmin. This chapter will also provide some special recommendations for those using customized HP solutions. These features should be installed before locking down your MFPs using the settings in the next 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.

Access Control for Device Functions

Access Control for Device Functions replaces control panel lock and authentication manager configuration options. It allows you to restrict access to a device by permission set and require specific types of authentication by device function. For example, you could configure this feature to allow guest walk up users to an MFP access to only the copy feature while scan to folder or scan to email are available to authenticated users.

You can configure Access Control for Device Functions by:

On the **Config** tab click **Access Control for Device Functions** (Figure 55) under the **Security** Category.

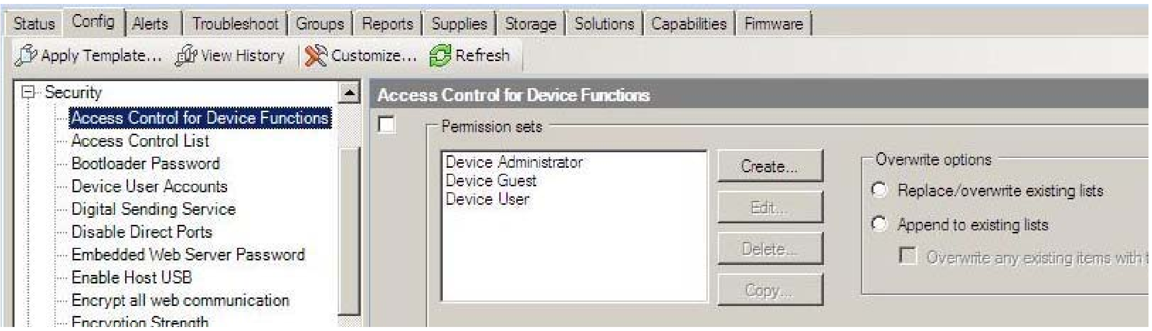


Figure 52: The Access for Device Functions option.

In the right-hand pane you will see the default permission sets, you can also create custom permission sets for advanced configurations. If would like new accounts to be created with a default set of permissions, you will need to set this under the **Device User Accounts** option.

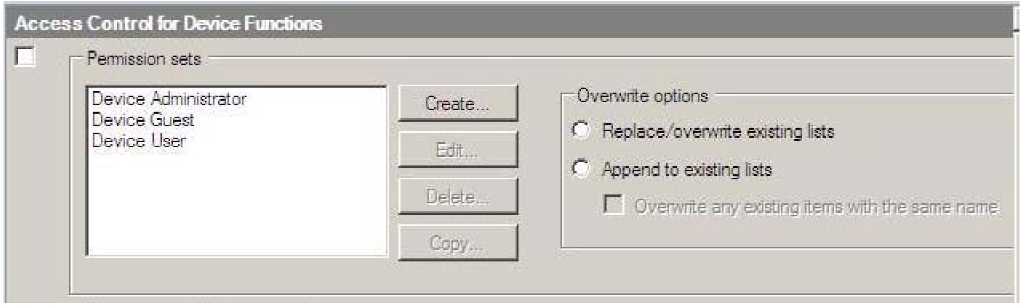
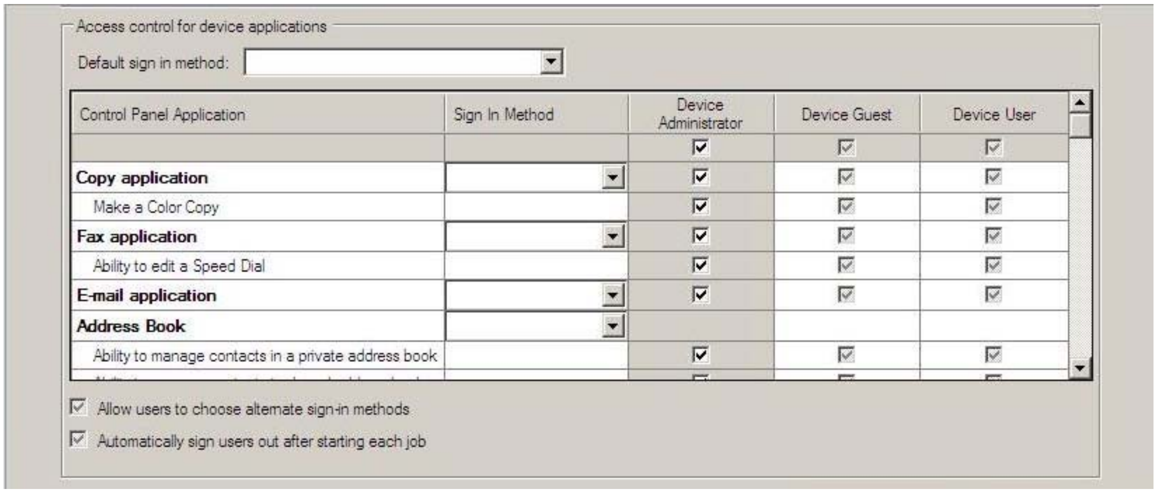


Figure 53: The Access for Device Functions option.

To set access control for each of these permission sets check or un-check the box in that permission set column for access to that function. If you would like a special kind of authentication you can also set the sign in method for that device function.



Access control for device applications

Default sign in method:

Control Panel Application	Sign In Method	Device Administrator	Device Guest	Device User
		☑	☑	☑
Copy application		☑	☑	☑
Make a Color Copy		☑	☑	☑
Fax application		☑	☑	☑
Ability to edit a Speed Dial		☑	☑	☑
E-mail application		☑	☑	☑
Address Book				
Ability to manage contacts in a private address book		☑	☑	☑

☑ Allow users to choose alternate sign-in methods

☑ Automatically sign users out after starting each job

Figure 54: The Access for Device Functions option.

Choosing a default authentication (Local Device, Windows, LDAP, DSS, Smartcard) method causes the MFP to require everyone to log in for access to the control panel menus. You can choose to require further authentication from a user 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:

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.

For more information on Access Control configuration, please refer to the user or administration guide for your device. For more information on Access Control Solutions please refer to the Access Control Printing Solutions Overview located here:

HP Access Control Printing Solutions

Access Control List (ACL)

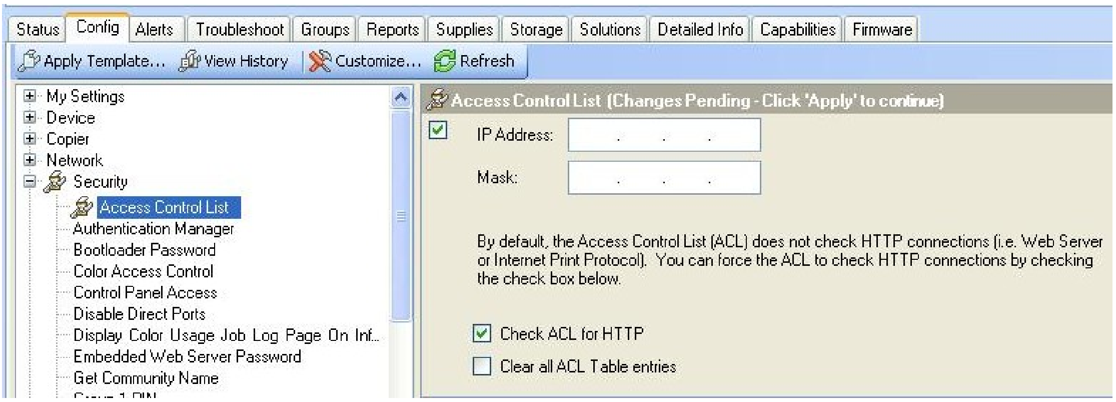
The ACL limits network access to the MFPs to only the IP addresses or subnets that you specify. This includes printing and all other access. Thus, to access the device an administrator must use a computer that is on the list, have the correct Web Jetadmin password, and then have the correct SNMPv3 credentials to manage the MFPs. You may also wish to secure your device by using IPsec/Firewall rules to limit specific traffic.

Note:

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

Follow these steps to configure the ACL:

On the **Config** tab click **Access Control List** (Figure 55) under the **Security** Category.



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

☑ IP Address: . . .

Mask: . . .

By default, the Access Control List (ACL) does not check HTTP connections (i.e. Web Server or Internet Print Protocol). You can force the ACL to check HTTP connections by checking the check box below.

☑ Check ACL for HTTP

□ Clear all ACL Table entries

Figure 55: The Access Control List Settings under the Security Category.

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.

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.

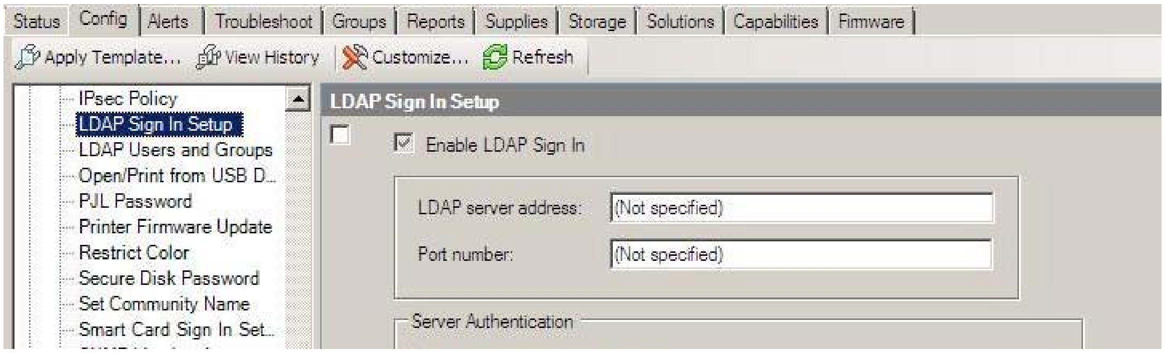
Check the checkbox for **Check ACL for HTTP access** to ensure that the ACL restricts access to the MFP EWS through HTTP.

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.

LDAP

If your network includes LDAP, configure the **LDAP Sign In Setup** and the **LDAP Users and Groups** options (Figure 56 and 56).



LDAP Sign In Setup

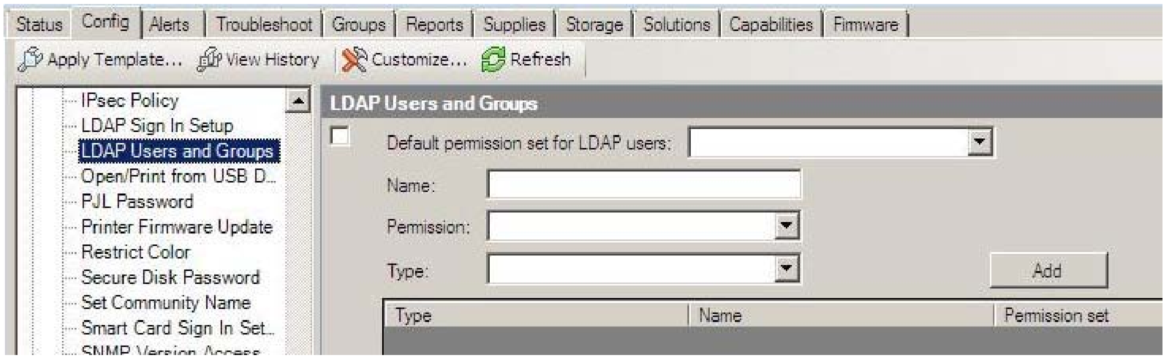
□ ☑ Enable LDAP Sign In

LDAP server address: (Not specified)

Port number: (Not specified)

Server Authentication

Figure 56: The LDAP Sign In Setup options.



LDAP Users and Groups

□ Default permission set for LDAP users:

Name:

Permission:

Type:

Type	Name	Permission set

Figure 57: The LDAP Users and Groups 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.

Note:

Uploading a certificate for use with SSL can be done under the Device Certificates Option in the Device category. This applies to any certificates including those created by the Certificate Authority server on your network.

Security Features Available Through the Embedded Web

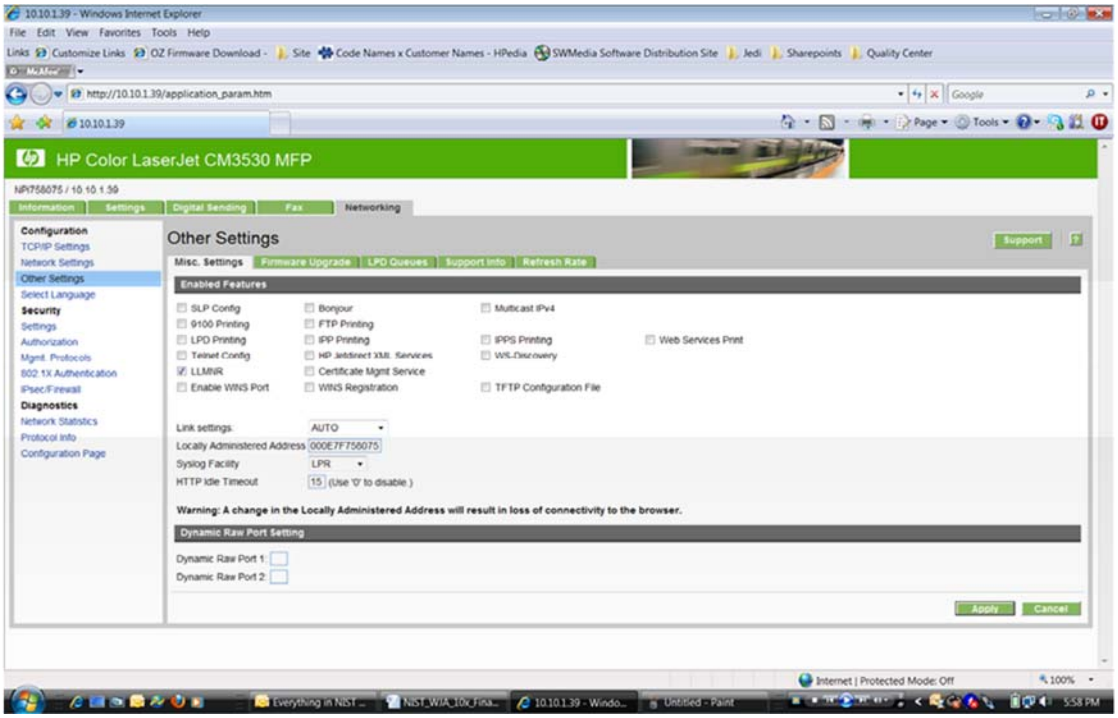
These features are either only partially offered in Web Jetadmin or are only available for configuration through the MFPs embedded web interface.

To configure the following settings:

1. Browse to the Embedded Web Server for the target device.
2. Select the **Networking** tab.
3. Choosing **Other Settings** from the left-hand menu.

LLMNR

Link-Local Multicast Name Resolution (LLMNR) is a protocol that provides a method for resolving host names on the same local link. It is useful in networks that do not have a DNS server. It does not require any configuration or administration in order to work, and it supports IPv4 and IPv6. A host on the network that needs to resolve a host name sends a query to a multicast address. Other hosts on the network who support LLMNR listen to this multicast address and respond to the query.



Other Settings

Enabled Features

☐ SLP Config	☐ Bonjour	☐ Multicast IPv4	
☐ 9100 Printing	☐ FTP Printing		
☐ LPD Printing	☐ IPP Printing	☐ IPPS Printing	☐ Web Services Print
☐ Telnet Config	☐ HP Jetdirect XML Services	☐ WS-Discovery	
☑ LLMNR	☐ Certificate Mgmt Service		
☐ Enable WINS Port	☐ WINS Registration	☐ TFTP Configuration File	

Link settings: AUTO

Locally Administered Address 000E7F758075

Syslog Facility LPR

HTTP Idle Timeout 15 (Use '0' to disable.)

Warning: A change in the Locally Administered Address will result in loss of connectivity to the browser.

Dynamic Raw Port Setting

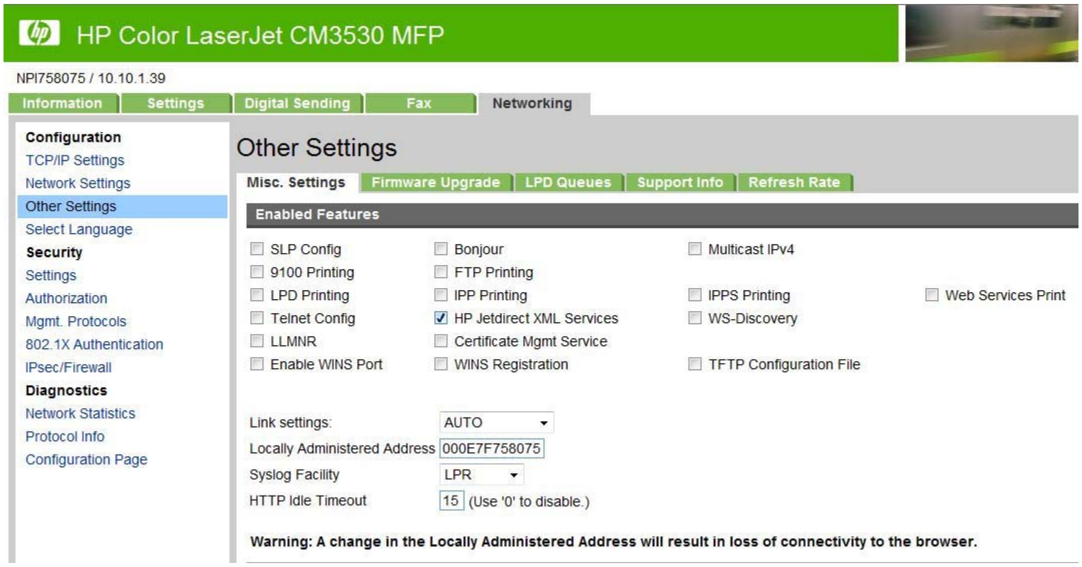
Dynamic Raw Port 1:

Dynamic Raw Port 2:

Figure 58: The Configuration Categories Menu Network option.

HP Jetdirect XML Server

The HP Jetdirect XML Services setting is used to enable/disable the IXDM Access Interface (IXA). XML Device Model (XDM) provides a method for collecting or configuring complex data where SNMP is impractical. One such example is IPsec. Web Jetadmin 10.4 supports configuring IPsec on a device through XDM. To configure IPsec, WJA constructs an XML document and sends it to the IXA interface on the device. When the HP Jetdirect XML services setting is disabled, the IXA interface is disabled and configuration through XDM cannot take place.



Other Settings

Enabled Features

□ SLP Config
□ 9100 Printing
□ LPD Printing
□ Telnet Config
□ LLMNR
□ Enable WINS Port
□ Bonjour
□ FTP Printing
□ IPP Printing
☑ HP Jetdirect XML Services
□ Certificate Mgmt Service
□ WINS Registration
□ Multicast IPv4
□ IPPS Printing
□ WS-Discovery
□ TFTP Configuration File
□ Web Services Print

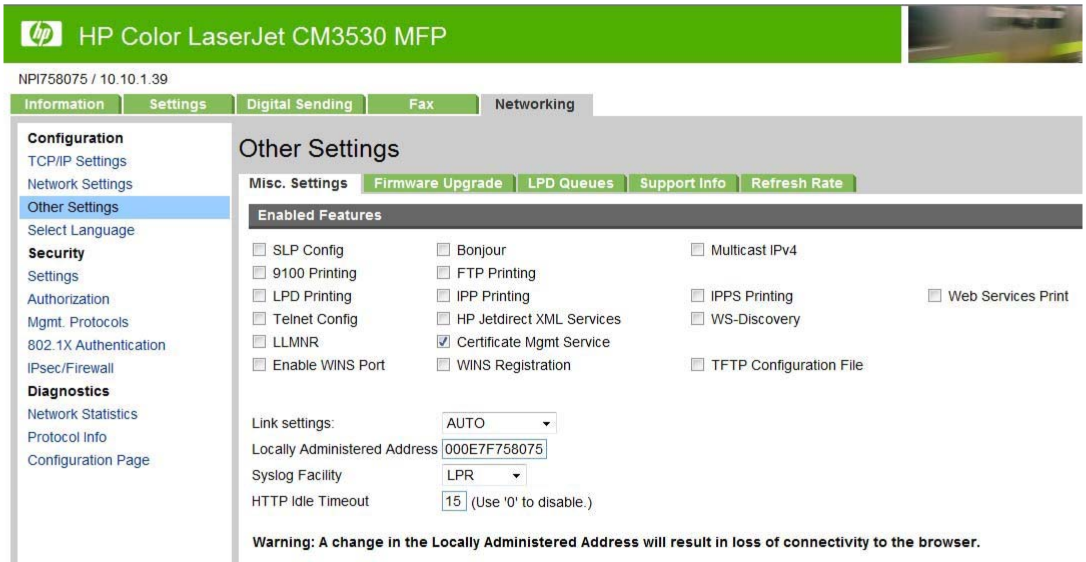
Link settings: AUTO
Locally Administered Address 000E7F758075
Syslog Facility LPR
HTTP Idle Timeout 15 (Use '0' to disable.)

Warning: A change in the Locally Administered Address will result in loss of connectivity to the browser.

Figure 59: The Configuration Categories Menu Network option.

Certificate Management Service

The Certificate Mgmt Service setting enables/disables batch certificate management. Using the Certificate Batch plug-in, WJA 10.x can batch manage and configure certificates on devices that support the Certificate Mgmt Service.



Other Settings

Enabled Features

□ SLP Config
□ 9100 Printing
□ LPD Printing
□ Telnet Config
□ LLMNR
□ Enable WINS Port
□ Bonjour
□ FTP Printing
□ IPP Printing
□ HP Jetdirect XML Services
☑ Certificate Mgmt Service
□ WINS Registration
□ Multicast IPv4
□ IPPS Printing
□ WS-Discovery
□ TFTP Configuration File
□ Web Services Print

Link settings: AUTO
Locally Administered Address 000E7F758075
Syslog Facility LPR
HTTP Idle Timeout 15 (Use '0' to disable.)

Warning: A change in the Locally Administered Address will result in loss of connectivity to the browser.

Figure 60: The Configuration Categories Menu Network option.

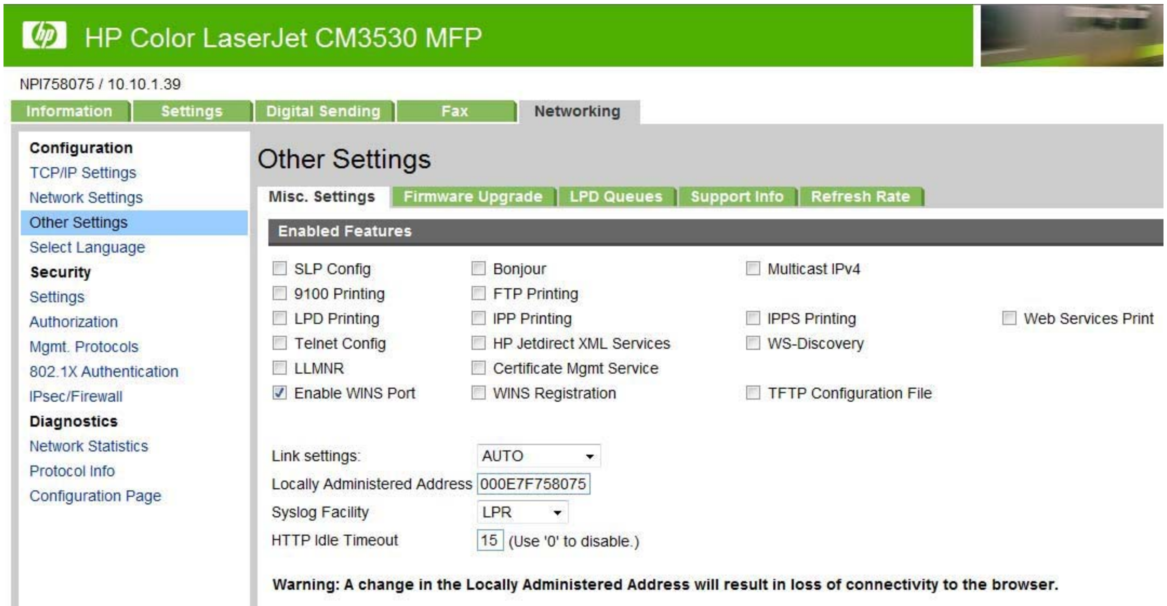
Enable WINS Port

The Enable WINS Port setting enables/disables the port used for WINS name resolution.

To enable the **WINS Port**:

1. Browse to the Embedded Web Server for the target device.
2. Select the **Networking** tab.

3. Choosing **Other Settings** from the left-hand menu.
4. Checking the box for **Enable WINS Port** (Figure 61).



Other Settings

Enabled Features

□ SLP Config □ Bonjour □ Multicast IPv4
□ 9100 Printing □ FTP Printing
□ LPD Printing □ IPP Printing □ IPPS Printing □ Web Services Print
□ Telnet Config □ HP Jetdirect XML Services □ WS-Discovery
□ LLMNR □ Certificate Mgmt Service
☑ Enable WINS Port □ WINS Registration □ TFTP Configuration File

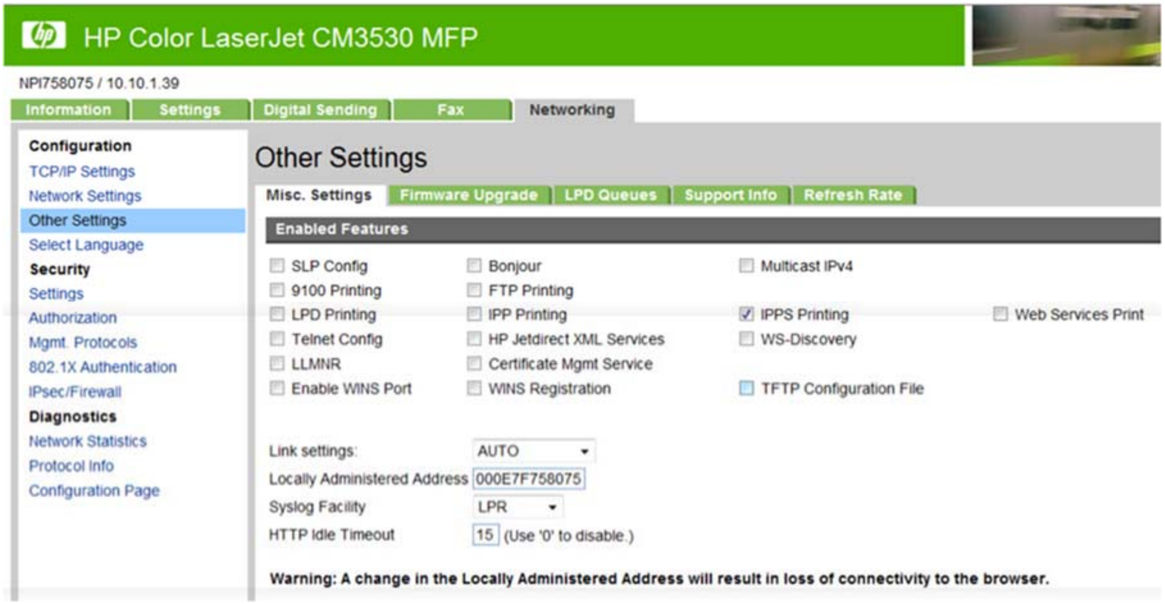
Link settings: AUTO
Locally Administered Address 000E7F758075
Syslog Facility LPR
HTTP Idle Timeout 15 (Use '0' to disable.)

Warning: A change in the Locally Administered Address will result in loss of connectivity to the browser.

Figure 61: Enable WINS Port by selecting check box.

IPPS

The IPPS Printing setting enables/disabled the Internet Printing Protocol over SSL. IPPS provides a secure method for sending print jobs to the device over the Internet or intranet.



Other Settings

Enabled Features

□ SLP Config □ Bonjour □ Multicast IPv4
□ 9100 Printing □ FTP Printing
□ LPD Printing □ IPP Printing ☑ IPPS Printing □ Web Services Print
□ Telnet Config □ HP Jetdirect XML Services □ WS-Discovery
□ LLMNR □ Certificate Mgmt Service
□ Enable WINS Port □ WINS Registration □ TFTP Configuration File

Link settings: AUTO
Locally Administered Address 000E7F758075
Syslog Facility LPR
HTTP Idle Timeout 15 (Use '0' to disable.)

Warning: A change in the Locally Administered Address will result in loss of connectivity to the browser.

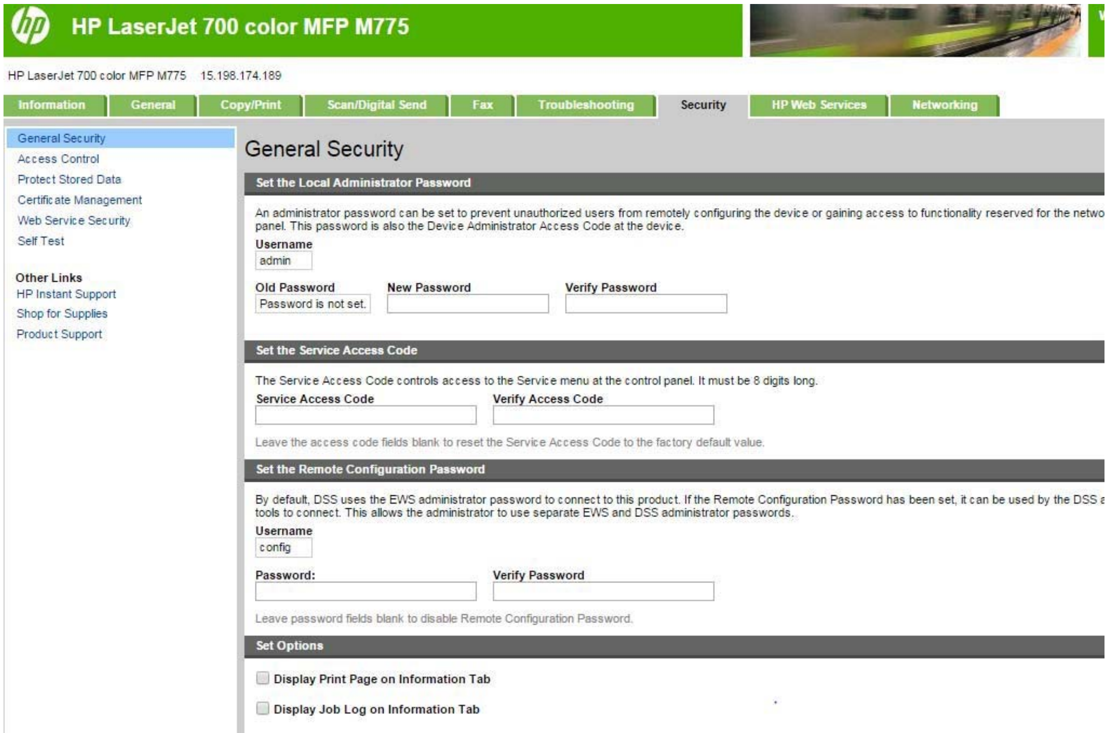
Figure 62 The Configuration Categories Menu Network option.

Disable Display Print Page and Job Log on EWS information tab

Viewing of job log and print page information on the EWS information tab is enabled on default. To restrict access to this data, disable the feature.

To disable **Print Page** and **Job Log:**

1. Browse to the Embedded Web Server for the target device.
2. Select the **Security** tab.
3. Select **General Settings** from the left-hand menu.
4. Uncheck the boxes for **Display Print Page on Information tab** and **Display Job Log in Information Tab (**Figure 63**).**
5. Click **Apply.**



HP LaserJet 700 color MFP M775 15.198.174.189

General Security

Set the Local Administrator Password

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

Username: admin

Old Password: Password is not set.
New Password:
Verify Password:

Set the Service Access Code

The Service Access Code controls access to the Service menu at the control panel. It must be 8 digits long.

Service Access Code:
Verify Access Code:

Leave the access code fields blank to reset the Service Access Code to the factory default value.

Set the Remote Configuration Password

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

Username: config

Password:
Verify Password:

Leave password fields blank to disable Remote Configuration Password.

Set Options

☐ Display Print Page on Information Tab

☐ Display Job Log on Information Tab

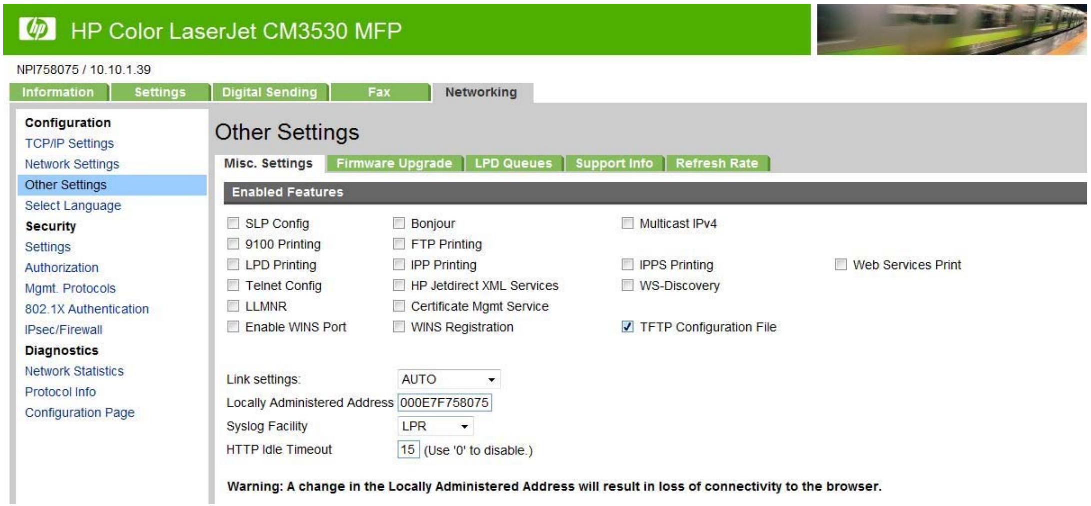
Figure 63 Disable Display Print Page and Job Log on EWS information tab

TFTP Configuration File

BOOTP is a protocol that provides a method for a network host to obtain an IP address and configuration information from a BOOTP server. Jetdirect supports the BOOTP protocol. When enabled, Jetdirect sends a BOOTP message onto the network. A properly configured BOOTP server responds to the message with an IP address that Jetdirect can use. In addition to providing an IP address, the BOOTP server can also provide the location of a TFTP configuration file for automatic configuration of Jetdirect. When the TFTP Configuration File setting is enabled, Jetdirect attempts to retrieve the TFTP configuration file from the server containing the file through the TFTP protocol.

To enable the use of the **TFTP Configuration File**:

1. Browse to the Embedded Web Server for the target device.
2. Select the **Networking** tab.
3. Choosing **Other Settings** from the left-hand menu.
4. Checking the box for **TFTP Configuration File** (Figure 64).



HP Color LaserJet CM3530 MFP

NPI758075 / 10.10.1.39

Information | Settings | Digital Sending | Fax | Networking

Configuration
TCP/IP Settings
Network Settings
Other Settings
Select Language
Security
Settings
Authorization
Mgmt. Protocols
802.1X Authentication
IPsec/Firewall
Diagnostics
Network Statistics
Protocol Info
Configuration Page

Other Settings

Misc. Settings | Firmware Upgrade | LPD Queues | Support Info | Refresh Rate

Enabled Features

□ SLP Config　□ Bonjour　□ Multicast IPv4
□ 9100 Printing　□ FTP Printing
□ LPD Printing　□ IPP Printing　□ IPPS Printing　□ Web Services Print
□ Telnet Config　□ HP Jetdirect XML Services　□ WS-Discovery
□ LLMNR　□ Certificate Mgmt Service
□ Enable WINS Port　□ WINS Registration　☑ TFTP Configuration File

Link settings: AUTO
Locally Administered Address 000E7F758075
Syslog Facility LPR
HTTP Idle Timeout 15 (Use '0' to disable.)

Warning: A change in the Locally Administered Address will result in loss of connectivity to the browser.

Figure 64: Enable TFTP Configuration File use by selecting check box.

HP & 3rd Party Solutions

Most of the recommendations in the next chapter of this checklist can be implemented without having a negative impact on HP & 3rd party solutions you may utilize in your environment without causing them to fail. However, there are some settings that have been known to cause problems. When setting up a solution in your environment you want to test the following:

- Disabling EWS remote access (port 80, port 443 etc.)
- Disabling Command load and execute

If your previously working solution no longer works revert to your original settings, or if you are unable to get your solution working enable them if disabled by default. The reason for this is many solutions require specific ports to communicate with the printer and may need to load a piece of their solution on boot of the print device.

Also, be sure you do not implement a Secure Storage Erase as a disk cleaning practice. This type of erase will wipe everything off your existing hard drive including any HP or 3rd party solution you have installed.

There are two suggestions in the next chapter that should only be implemented after a solution has been installed. They are:

- Configure a PJL password
- Disable PJL file system access

Once installed, you can test whether implementing these recommendation impacts your solution. If your solution is impacted, skip these recommendations in the next chapter. If you choose to implement these recommendations a solution needs to be updated, you will need to re-enable PJL file system access and set the PJL password to blank to install the solution. After the upgrade you will need to test if the new version of the solution is adversely affected.

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.

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 Basic Settings

Initial Settings

- □ 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 **Input Auto Continue Timeout**
- □ Configure **Job Hold Timeout**.
- □ Enable **Job Retention**.
- □ Configure **Job Storage Limit**

Network Category Options

- □ Disable **e-Print Settings**
- □ Configure **Error Handling**
- □ Configure **HTTP Idle Timeout.**
- □ Configure **Network Enable Features** options.
  - □ Enable **EWS Config**.
  - □ Disable **Telnet Config**.
  - □ Disable **SLP Config**.
  - □ Disable **FTP Printing**.
  - □ Disable **LPD Printing**.
  - □ Enable **9100 Printing**.
  - □ Disable **Air Print.**
  - □ Disable **IPP Printing**.
  - □ Disable **IPPS**.
  - □ Disable **mDNS Config**.
  - □ Disable **IPV4 Multicast Config**.
  - □ Disable **WS-Discovery**.
  - □ Disable **HP XML Services**
- □ Configure **TCP Idle Timeout**.
- □ Disable **Web Services Print**.

Security Category Options

- □ Disable **Digital Sending Service**.
- □ Configure **Embedded Web Server Password**.
- □ Disable **Enable Host USB**.
- □ Enable **HTTPS Setting** to **Encrypt all web communication**.
- □ Configure **Encryption Strength** to **High**.
- □ Configure **Open/Print from USB Device**.
- □ Configure the **PJL Password**.
- □ Disable **Printer Firmware Update**.
- □ Configure **Restrict Color** as desired.
- □ Configure the **Secure Disk Password.**

Fax Category Options

- □ Configure **Fax Printing**.
  - □ Blocked Fax List Settings.
  - □ Fax Header Settings.

Additional Fax Configuration

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

MFP File System Options

- □ Configure **File System External Access**.
  - □ Disable **PJL**.
  - □ Disable **PostScript**.
- □ Configure **Secure File Erase Mode** to **Secure Fast Erase** or **Secure Sanitize Erase**.

Digital Sending Settings 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**. (Optional)

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 **SNMPv3** (Security page).	Not configured
I/O Timeout to End Print Job	Not configured
Configure Job Hold Timeout.	Never Delete
Enable Job Retention.	Enabled
Job Storage Limit	Enabled
e-Print Settings	Disabled and Not Configured
Error Handling	Dump then Reboot
HTTP Idle Timeout	Enabled
Configure **Enable Features** options (do not disable **EWS Config** 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 Air Print	Enabled
Disable IPP Printing.	Enabled
Disable IPPS.	Enabled
Disable MDNS Config.	Enabled
Disable IPV Multicast Config.	Enabled
Disable WS-Discovery.	Disabled
TCP Idle Timeout	Enabled
Web Services Print	Enabled
Digital Sending Service	Disabled
Embedded Web Server Password	Disabled
Enable Host USB	Disabled
Enable Encrypt all Web Communication.	Enabled
Configure Encryption Strength to High.	Low
Open/Print from USB Device	Disabled
Configure the **PJL Password**.	Not configured
Disable Printer Firmware Update.	Enabled

Setting	**Default Setting**
Restrict Color	Not configured
Secure Disk Password	Automatic
Configure Fax Printing.	Not configured
Blocked Fax List Settings	Not Configured
Fax Header Settings	Not Configured
Configure Fax Speed Dials	Not Configured
Lock Speed Dials	Not Configured
Configure File System External Access.	(See below)
Disable **PJL**.	Enabled
Disable 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 **Auto Reset Send Settings** to **Delay before resetting the default settings** 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 **Direct Ports** (wait for MFPs to restart).	Enabled
Disable EWS Config.	Enabled
HP XML Services	Enabled

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, PIN Authentication, LDAP, Solutions, 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.

- **Input Auto Continue Timeout.** Configure Auto Continue Timeout to setting of your choice.
- 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.
- Enable **Job Storage Limit**. Job Storage Limit when enables is set to a default of 32. Adjust accordingly to your print job needs.

NOTE:

Stored faxes are not affected by the Job Hold Timeout.

Network Options

- Disable **e-Print.** Unless e-Print, HP Web Services, or other applications are a critical part of your print environment we recommend disabling these features. If you are using the e-print enterprise server and not the HP cloud for e-Print you should refer to your administrators guide for any special settings that may be required to secure your solution.
- Configure **Error Handling.** Choose the setting that best fits your security need.
- Configure **HTTP Idle Timeout.** The HTTP Idle Timeout option configures the amount of time an HTTP connection to the device remains open. This can prevent the need to physically go to the device when you have problem jobs that lack proper end of job signals or other hung connections. Enabled on default and set to a 15 second timeout.

- 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 effect 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, HPUX, 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.

- o 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.
- o Disable **Air Print. Air Print Printing** is a protocol for printing from apple devices. Unless your network environment supports Air Print, we recommend keeping this feature disabled.
- o 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.
- o Disable **IPPS** when IPP is not in use is your only option. When IPP is enabled, the IPPS Printing setting enables the Internet Printing Protocol over SSL. IPPS provides a secure method for sending print jobs to the device over the Internet or intranet. If you have chosen to enable IPP then we recommend Enabling IPPS as well.
- o 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.
- o 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.
- o Disable **WS-Discovery. WS-Discovery** enables network hosts which 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.
- o Disable **HP XML Services.** The HP Jetdirect XML Services setting is used to enable/disable the IXDM Access Interface (IXA) which provides a method for collecting or configuring complex data where SNMP is impractical. When the HP Jetdirect XML services setting is disabled, the IXA interface is disabled and configuration through XDM cannot take place.
- o Configure **TCP Idle Timeout (previously called Job Timeout)**. The **TCP Idle 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.
- o 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 Options

- 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.
- 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. 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.

Embedded Web Server 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, which will include any solution that is required to load at boot.

  If a solution stops working after disabling Command Load and Execute we recommend re-enabling this setting followed by a power cycle of your MFP.

- 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.

- 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.
- Disable **Enable Host USB** Leaving this option enabled could allow people without access to your network print documents from your devices at walk up. We recommend that this feature be **Disabled**. Disabling this feature will not affect your smart card solution or Host USB functionality.

- **Encrypt all web communication** by Enabling **HTTPS**. 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 below.
- 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.

  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 **Open/Print from USB Device.** The **Open/Print** from USB Device feature allows you to print documents stored on a USB device. Leaving this option enabled could allow people without access to your network to print documents from your devices at walk up.
- 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 (PJL) commands.

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

  If you are using an HP or 3rd party solution this setting may interfere with upgrades to an existing solution, or installation of a new solution.

- 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. 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 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.

Fax 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.

File System 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 PJL and PML only affects file system access, but disabling NFS shuts down the protocol for the entire MFP.

  - Disable **PJL** access. PJL (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 PJL 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 **PJL** access disabled, the MFPs will ignore PJL commands that attempt to access the file system.

    PJL access needs to be enabled for some solutions to be installed correctly. After a solution is installed it is usually safe to disable PJL access till the next upgrade or installation.

  - 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.

- 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 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.

  Keep in mind 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 effects 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.
- 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.
- 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.

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.

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.
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 hp.com. 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 hp.com. This checklist assumes that each MFP is upgraded with the latest firmware.
Formatter	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. Since the formatter is removable (using common tools), it includes the capability to be locked using devices such as Kensington locks.
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 in a numeric password. MFPs use PINs for secure printing and secure fax printing. They can also use PINs for authentication.

Term	Description
Scanner, ADF, or flatbed scanner	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. 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. 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.
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	A storage device is a component that stores data. The MFP includes two types of storage devices: hard drive and Compact Flash cards. 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.
WJA	HP Web Jetadmin: HP Web Jetadmin is a peripheral management tool that provides access to multiple devices for status and configuration. It can configure multiple MFPs simultaneously. Web Jetadmin is the recommended tool for configuring all settings in this checklist.

Appendix 2: Products supported by this checklist

HP Color LaserJet CM4540 MFP

HP Color LaserJet CP5525xh

HP LaserJet Enterprise M4555 MFP

HP LaserJet Enterprise M406/M407 series

HP LaserJet Enterprise MFP M430/M431 series

HP Color LaserJet Enterprise M455series

HP Color LaserJet Enterprise MFP M480 series

HP LaserJet Enterprise M506 series

HP LaserJet Enterprise M507 series

HP LaserJet Enterprise MFP M525 series

HP LaserJet Enterprise MFP M527 series

HP LaserJet Enterprise MFP M528 series

HP LaserJet Enterprise 500 Color M551xh

HP Color LaserJet Enterprise M553 series

HP Color LaserJet Managed M553 series

HP Color LaserJet Managed M555 series

HP Color LaserJet Managed MFP M575 series

HP LaserJet Enterprise 500 color MFP M575 series

HP Color LaserJet Enterprise MFP M577 series

HP Color LaserJet Managed MFP M577

HP Color LaserJet Enterprise MFP M578 series

HP LaserJet Enterprise 600 M603xh

HP LaserJet Enterprise M604, 605, 606 series

HP LaserJet Enterprise M607, M608, M609 series

HP LaserJet Enterprise M610, M611, M612 series

HP LaserJet Enterprise MFP M630 series

HP LaserJet Managed MFP M630 series

HP LaserJet Enterprise MFP M631/M632/M633 series

HP LaserJet Enterprise MFP M634/M635/M636 series

HP LaserJet Enterprise MFP M651xh

HP Color LaserJet Managed M651xhm

HP Color LaserJet Enterprise M652/M653 series

HP LaserJet Enterprise MFP M680 series

HP Color LaserJet Managed MFP M680 series

HP Color LaserJet Enterprise MFP M681/M682 series

HP LaserJet Enterprise 700 M712xh

HP LaserJet Enterprise MFP M725 series

HP LaserJet Enterprise M750 series

HP Color LaserJet Enterprise M751 Printer series

HP LaserJet Enterprise 700 color M775 series

HP Color LaserJet MFP M776 series

HP LaserJet Enterprise M806

HP LaserJet Enterprise Flow MFP M830 series

HP LaserJet Enterprise M855

HP Color LaserJet Enterprise M856 series

HP LaserJet Enterprise Flow MFP M880 series

HP LaserJet Managed E40040 series

HP LaserJet Managed MFP E42540 series

HP Color LaserJet Managed E45028 series

HP LaserJet Managed MFP E42540 series

HP Color LaserJet Managed MFP E47528 series

HP LaserJet Managed E50045 series

HP LaserJet Managed E50145 series

HP LaserJet Managed MFP E52545 series

HP LaserJet Managed MFP E52645 series

HP Color LaserJet Managed MFP E57540 series

HP LaserJet Managed E60055/65/75 series

HP LaserJet Managed E60155/65/75 series

HP LaserJet Managed MFP E62555/65/75 series

HP LaserJet Managed MFP E62655/65/75 series

HP Color LaserJet Managed E65050/60 series

HP Color LaserJet Managed E65150/60 series

HP Color LaserJet Managed MFP E67550dh

HP Color LaserJet Managed MFP E67650/60 series

HP Color LaserJet Managed Flow MFP E67560z

HP LaserJet Managed MFP E72425/30 series

HP LaserJet Managed MFP E72525/30/35 series

HP Color LaserJet Managed E75245 Printer series

HP Color LaserJet Managed MFP E77422/28 series

HP Color LaserJet Managed MFP E77822/25/30 series

HP LaserJet Managed MFP E78223/28 series

HP LaserJet Managed MFP E78323/30 series

HP LaserJet Managed MFP E82540/50/60du series

HP Color LaserJet Managed E85055 series

HP Color LaserJet Managed MFP E87640/50/60du series

HP OfficeJet Enterprise X555 series

HP OfficeJet Enterprise X585 series

HP PageWide Enterprise Color MFP 586 series

HP PageWide Color 755 Printer series

HP PageWide Enterprise Color 765 series

HP PageWide Enterprise Color 774/779 series

HP PageWide Enterprise Color MFP 780/785 series

HP PageWide Managed Color MFP E58650 series HP

PageWide Managed Color E75160 series

HP PageWide Managed Color MFP E77650/60 series HP

PageWide Managed Color MFP P77940/50/60 series

HP Digital Sender Flow 8500 fn2

HP ScanJet Enterprise Flow N9120 fn2 Document Scanner

Get connected

hp.com/go/getconnected

Current HP driver, support, and security alerts
delivered directly to your desktop

Created November 2021