



HP Printing Security Best Practices for HP PageWide Pro Printers and HP Web Jetadmin

Configuring a Printer Securely in HP Web Jetadmin 10.4 Version 1.0

HP PageWide Pro 477dn MFP

HP PageWide Pro 477dw MFP

HP PageWide Pro 577dw MFP

HP PageWide Pro 577z MFP

HP PageWide Pro 452dn Printer

HP PageWide Pro 452dw Printer

HP PageWide Pro 552dw Printer

Table of Contents

Introduction	1
Cautions	2
Follow the Checklist in Order	2
Understand the Ramifications.....	2
Continue to be Vigilant.....	2
MFP Environment	2
Assumptions.....	3
Solutions covered.....	3
Organization	3
Chapter 1: Threat Model	5
Spoofing Identity.....	5
Tampering with Data	6
Repudiation.....	6
Information Disclosure	7
Denial of Service	7
Elevation of Privilege	8
Chapter 2: Basic Network Security for Multiple HP Devices	9
Notes on the Process of Configuration.....	9
Using Web Jetadmin and Printer Passwords	9
Getting Started.....	10
Setting up HP Web Jetadmin	11
Configuring SNMPv3.....	13
Configuring Device Settings	15
I/O Timeout to End Print Job.....	15
Input Auto Continue Timeout	16
Job Hold Timeout.....	16
Job Retention.....	17
Job Storage Limit	17
Configuring Network Settings.....	19
ePrint and HP Web Services Settings	19
Enable WINS Port	20
Web Services Print	20
Google Cloud Print.....	21
Network Enable Features.....	21

Configuring Security Settings.....	24
Embedded Web Server Password.....	24
Enable Host USB.....	25
Encrypt all Web Communication.....	26
Encryption Strength.....	26
Printer Firmware Update.....	27
Restrict Color.....	27
Configuring Fax Settings.....	28
Blocked Fax List Settings.....	28
Fax Header Settings.....	28
Configuring MFP File System Settings.....	30
Secure File Erase Mode.....	30
Configuring MFP Digital Sending Settings.....	30
Email Address/Message Settings - Default From Address.....	31
Chapter 3: Advanced Security for Multiple HP Devices.....	32
Access Control for Device Functions.....	32
LDAP.....	34
Disable Wireless.....	34
Configure Firewall.....	35
Security Features Available in the Embedded Web Server.....	36
Disable Job Log on EWS Tools tab.....	37
HP and 3 rd Party Solutions.....	37
Chapter 4: Settings List.....	38
Recommended Basic Settings.....	38
Chapter 5: Default Settings.....	40
Chapter 6: Ramifications.....	41
Initial Settings.....	41
Device Page Settings.....	41
Network Options.....	42
Security Options.....	43
Embedded Web Server Options.....	43
Digital Sending Options.....	44
Overall Limitations.....	45
Chapter 7: Physical Security.....	46
Appendix: Glossary of Terms and Acronyms.....	47

Introduction

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

- HP PageWide Pro 452dn Printer
- HP PageWide Pro 452dw Printer
- HP PageWide Pro 552dw Printer
- HP PageWide Pro 477dn MFP
- HP PageWide Pro 477dw MFP
- HP PageWide Pro 577dw MFP
- HP PageWide Pro 577z MFP

This checklist is written for acceptance by the National Institute of Standards and Technology (NIST). It will be available on the NIST Checklist website at the conclusion of the review process.

The information in this checklist was created for trained network administrators who use HP Web Jetadmin version 10.4 or later in enterprise networks. It includes instructions to configure one or more MFPs on a network.

This checklist assumes that network administrators are familiar with HP Web Jetadmin and management of HP MFPs and printers. Network administrators should be familiar with the MFP Embedded Web Server (EWS), and firmware upgrades for MFPs. Refer to the MFP User Guides 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 for free and can be downloaded from <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 environments:

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

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

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

Cautions

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

Follow the Checklist in Order

To ensure success, follow the checklist items in the order that they are presented. If you do not follow the specific order, some of the security settings will not configure correctly. Avoid making additional configurations during this process. Other settings can disrupt the order and cause unexpected results.

Understand the Ramifications

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

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

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

Continue to be Vigilant

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

MFP Environment

NIST defines several types of user environments, many of which are compatible with HP PageWide Pro MFPs. However, this checklist applies for HP devices and MFPs in an enterprise environment or a small to medium business environment. These environments use most of the network features available with MFPs. 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 MFP user guide and the MFP 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.
- MFPs: This checklist covers security settings for specific HP devices outlined at the beginning of this document. Use the information herein to configure multiple devices simultaneously. The devices you are configuring must be turned-on, connected to the network, and in the factory-default state.
- Most of the settings recommended in this checklist apply to other HP MFPs and 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 MFP firmware. You should use the latest firmware available, but realize that updated firmware may have new features not covered in this checklist. Updated firmware is available for download and installation at hp.com.
- Web Jetadmin version 10.4: The information in this checklist pertains to HP Web Jetadmin version 10.4 and later.
- Enterprise environment: This checklist was created and tested in a TCP/IP enterprise environment. However, most of the settings are applicable to any TCP/IP network.
- Network connection: This checklist assumes that each device is connected directly to a local area network. Direct connection via USB is not covered in this checklist (this checklist recommends disabling direct-connect USB ports).
- Settings are only suggested: All settings in this checklist are meant only as suggestions for best-practice security in common enterprise environments. Use it as a reference, and make judgments about each recommended setting before configuring your MFPs.
- Internet and intranet security: This checklist assumes that your network includes basic security configurations and components. All MFPs should be installed behind network firewalls and other standard tools such as updated virus protection applications.

Solutions covered

This checklist covers MFP security settings found in HP Web Jetadmin. This checklist does not cover any other solutions or applications.

Organization

This checklist includes the following chapters:

- Chapter 1: Threat Model: The Threat Model chapter explains the security circumstances relating to MFPs. It follows the Microsoft® STRIDE model.
- Chapter 2: Basic Network Security for Multiple HP Devices: The Network Security for Multiple MFPs chapter provides step-by-step instructions for configuring MFP security settings.

- Chapter 3: 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.
- Chapter 4: Settings List: The Settings List chapter provides a bulleted list of the recommended settings with checkboxes. It does not include instructions or explanations.
- Chapter 5: Default Settings: The Default Settings chapter lists each recommended setting with its corresponding default setting.
- Chapter 6: Ramifications: The Ramifications chapter explains the possible limitations implied with each recommended setting.
- Chapter 7: 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: Glossary and Acronyms

Chapter 1: 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 beware 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 (e.g. Someone could enter the address of a co-worker in the **From** address field and send embarrassing or malicious messages to others as though the co-worker sent them)
- Using another person's email credentials to login 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 logon credentials for access to use MFPs or networks
- Using another person's logon 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 storage 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:

- 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 proximity cards

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:

- Close unused ports and protocols.
- Configure all possible password settings.
- Configure access control and authentication for device functions.
- Configure SNMPv3 for Web Jetadmin, including disabling SNMPv1/2.

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
- 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
- Protect EWS configuration settings by setting an Admin Password
- Close unused ports and protocols
- Enable the resume feature to allow the MFP to resume operations after an error state
- Configure Job Timeout
- Control physical access to the MFP
- Lock physical access to removable hardware

Elevation of Privilege

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

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

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

- Configure the administrator (device) password
- Configure SNMPv3 and HTTPS
- Lock available control panel menus and configure user access

Chapter 2: 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 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, try configuring the setting again. If you have further issues with a particular configuration item, 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, a mono only MFP does 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 steps 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 order presented.

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 printers. 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 passwords that are configured or used on each HP product. However, sometimes the cache can lose track of 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

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

- Use alpha and numeric characters whenever possible.
- For numeric only passwords use passwords with at least nine digits.
- Use a different password for each password setting. Many of the latest password cracking tools can follow patterns to make guessing easier.
- Avoid using a pattern for passwords.
- Change the passwords often.
- 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.

Getting Started

This section provides instructions for configuring HP printers for best-practice security. All of these settings pertain to 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. To download and install Web Jetadmin, click the following link:

<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:

All screenshots are from Web Jetadmin version 10.4.

Setting up HP Web Jetadmin

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

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

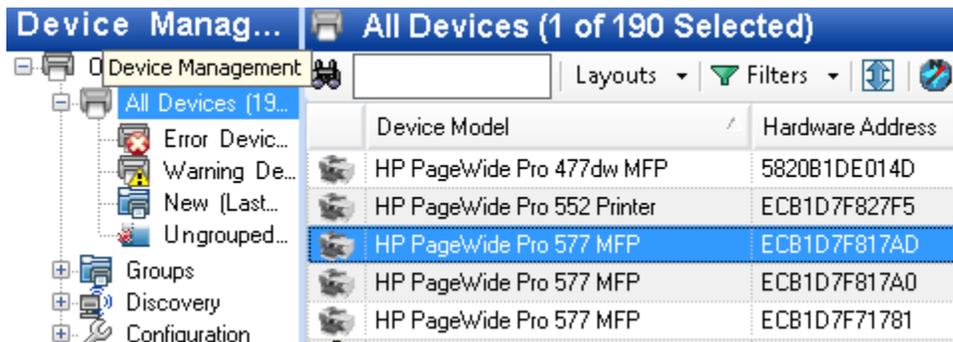


Figure 1: Web Jetadmin showing the device list on the default view

2. Verify 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 printing devices on your network.
-

Note:

This checklist does not include details on print device discovery. See the Web Jetadmin user guide 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.

3. Hold down the **CTRL** key and click to select the printers or MFPs from the Device List (Figure 2) that you would like to configure.

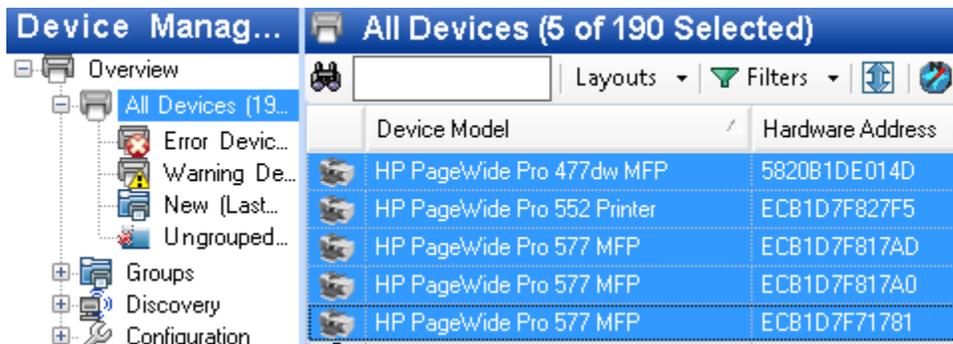


Figure 2: The Device List showing multiple devices selected

Note:

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

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

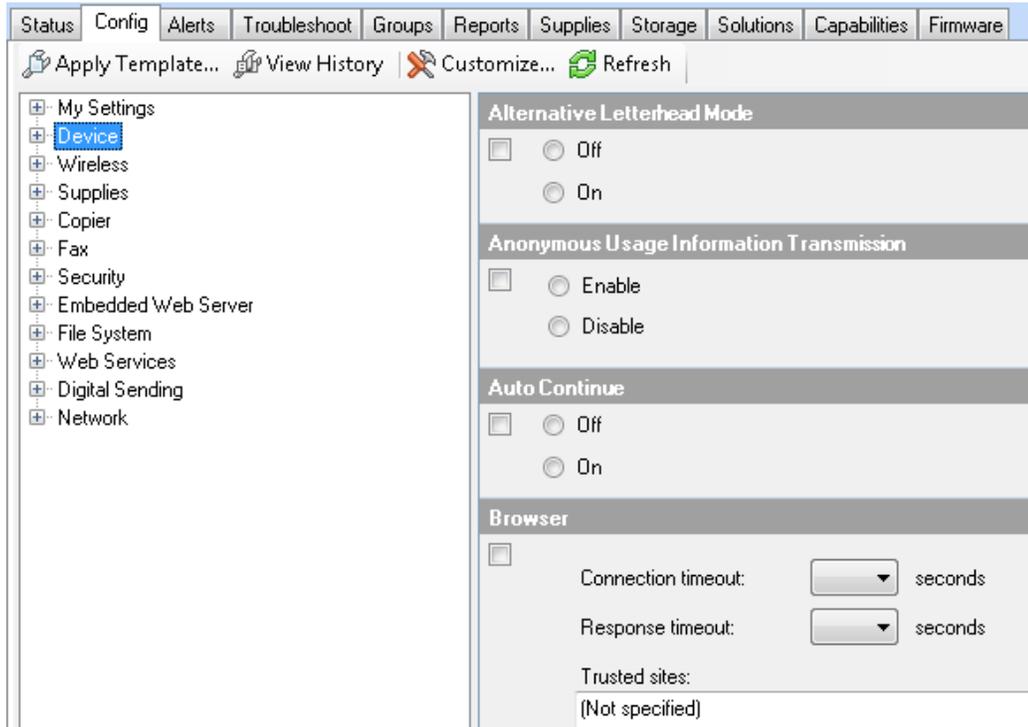


Figure 3: The Config tab displays settings available for configuration

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.

5. Continue to the next step 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 ensures that no one can gather sensitive information (i.e. passwords, usernames, and other codes) over the network while you are configuring the MFPs.

Note:

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

Follow these steps:

1. Click **Security** in the Configuration Categories menu (Figure 4) to view the options for configuration. From the Security Options select **SNMP Version Access Control**.

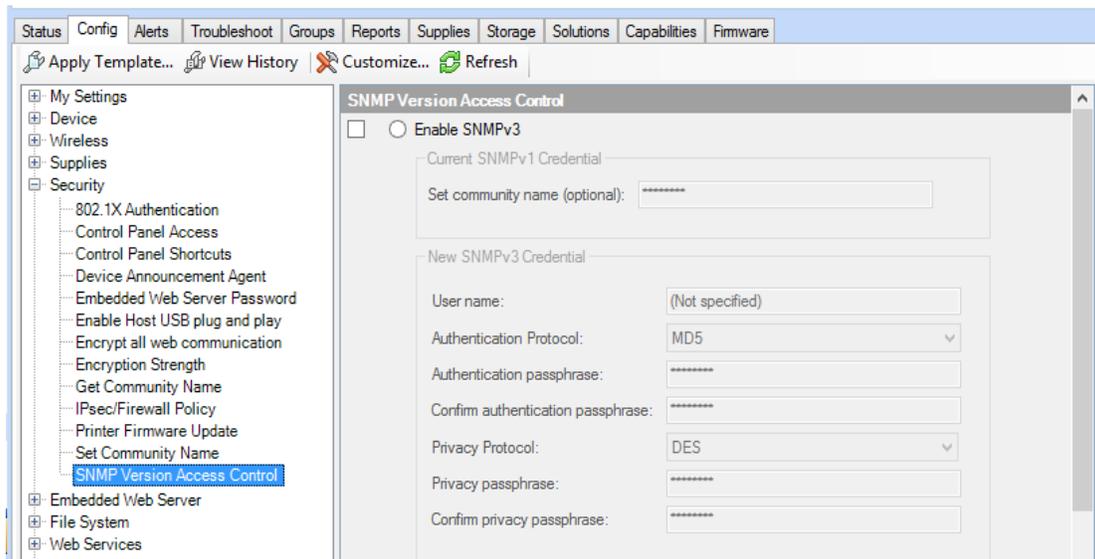


Figure 4: The Security category and SNMP Version Access Control settings

2. On the SNMP Version Access Control menu, select the **Enable SNMPv3** checkbox (Figure 5).

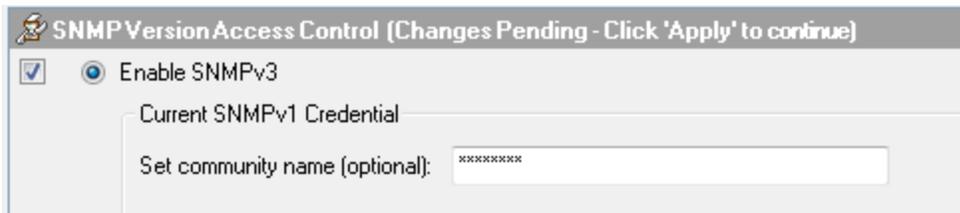


Figure 5: The Enable SNMPv3 checkbox is selected

3. In the New SNMPv3 Credential section, enter a **User Name**, **Authentication passphrase**, and **Privacy passphrase** in the text-fields (Figure 6).

Note:

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

The **Authentication passphrase** and **Privacy passphrase** must be at least nine (9) characters and contain both numbers and letters.

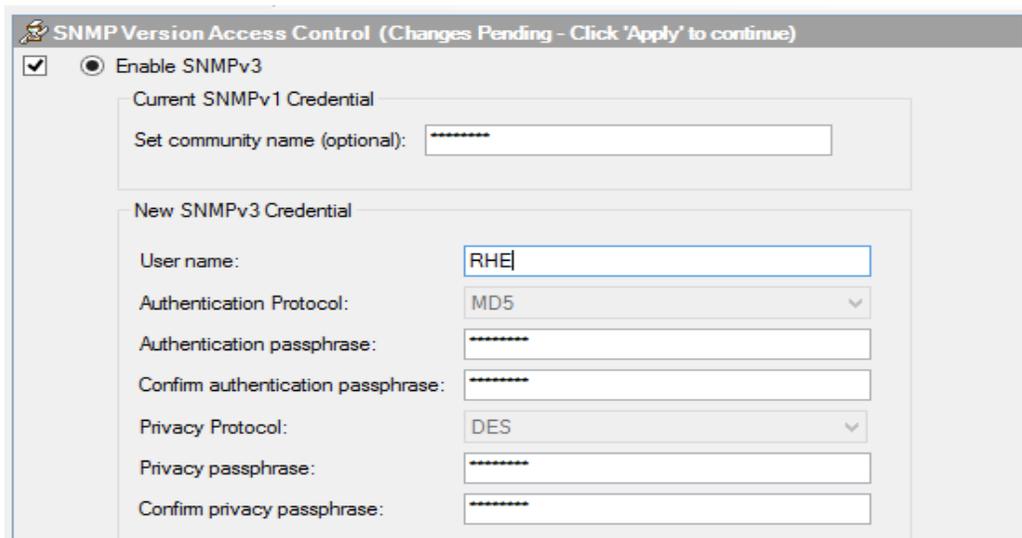


Figure 6: Information entered into text-fields in the SNMP Version Access Control dialog box

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 you forgot these credentials, the only way to restore communication between HP Web Jetadmin and the print devices is to restore the 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.

4. Scroll down to the SNMPv1 Settings section, and select **SNMPv1 disabled** (Figure 7).

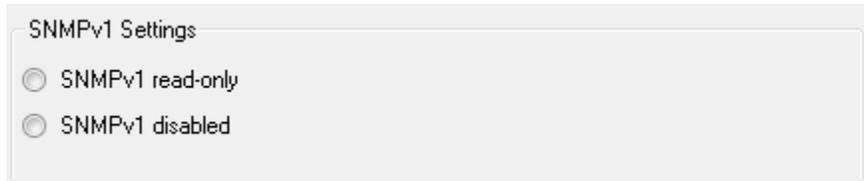


Figure 7: The SNMP Version 3 Only setting

Note:

This setting limits all SNMP configuration communication to only SNMPv3. Once applied, your devices will not allow SNMPv1 SET or SNMPv2 GET.

5. Click **Apply** to save the configuration settings to the selected devices.

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

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.

6. Click **Done** to exit the Configure Devices dialog box, and continue with this checklist.

Configuring Device Settings

The **Device** category includes settings that affect normal usage of the printing device. The following settings affect how jobs are stored, and how long the device will wait before a job times-out.

To configure the device settings, click **Device** in the left-side menu on the **Config** tab.

The following sections contain information about the configuration options.

I/O Timeout to End Print Job

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

1. From the Device category, select the **I/O Timeout to End Print Job** option (Figure 8).

2. Click the checkbox to enable the I/O Timeout to End Print Job setting, and enter a reasonable time for the print device to wait between data packets.

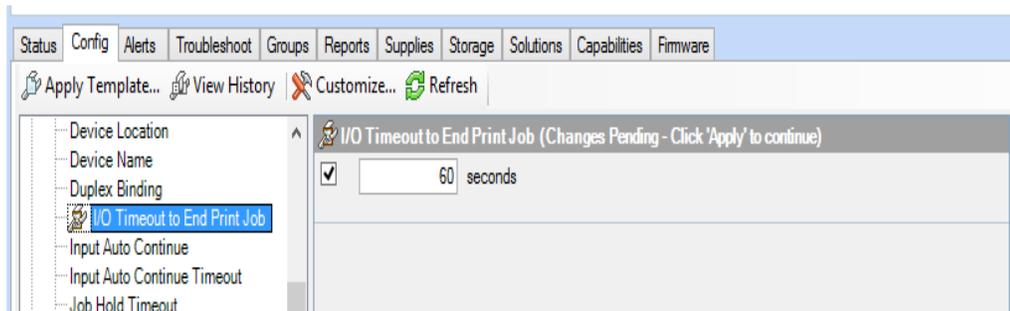


Figure 8: The I/O Timeout to End Print Job options

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.

1. From the Device category, select the **Input Auto Continue Timeout** menu.
2. Click the checkbox to enable the **Input Auto Continue Timeout** setting, and then select a reasonable time the print device should wait between data packets.

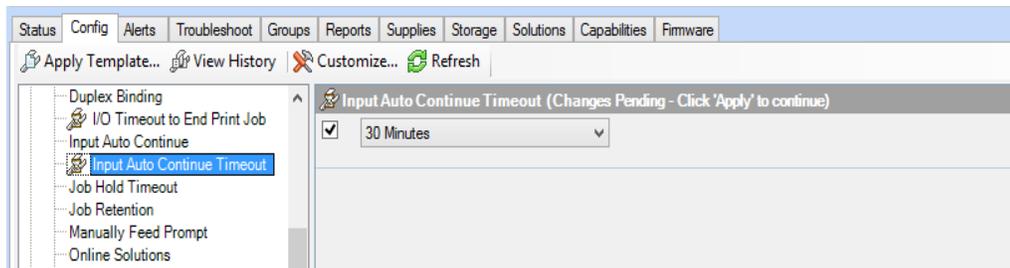


Figure 9: The Input Auto Continue Timeout options

Job Hold Timeout

1. From the Device category select the **Job Hold Timeout** menu (Figure 10).
2. Click the checkbox to enable the Job Hold Timeout (Figure 10) setting, and then enter a reasonable time for printing. This ensures that stored copy jobs and print jobs on the MFP are erased after a reasonable time.

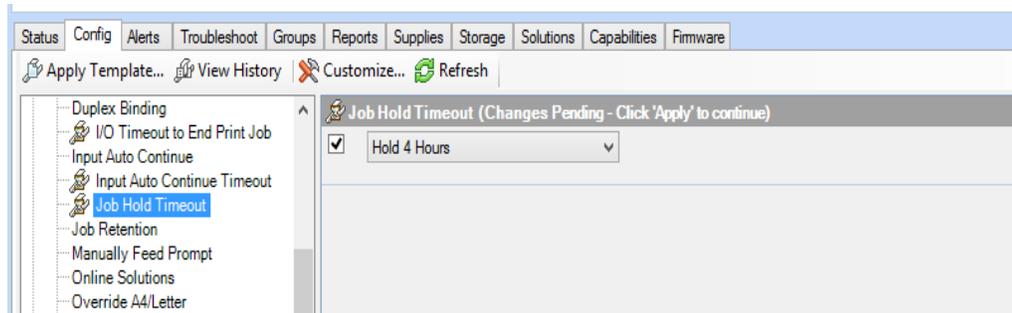


Figure 10: The Job Hold Timeout options

Job Retention

1. From the Device category select **Job Retention** (Figure 11).
2. Click the checkbox to select Job Retention, and then select **Enabled** (Figure 11).

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).

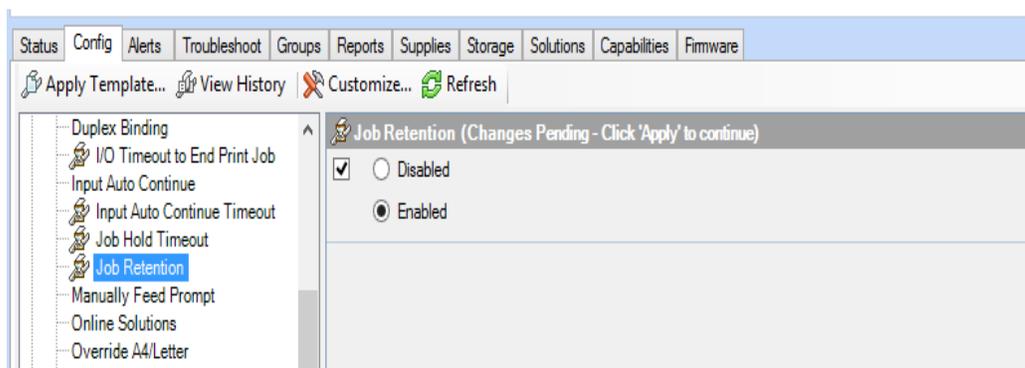


Figure 11: The Job Retention options

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.

1. From the Device category, select the **Job Storage Limit** menu (Figure 12).
2. Click the checkbox to enable the Job Storage Limit setting, and then enter a number of allowable Stored Jobs (Figure 12).

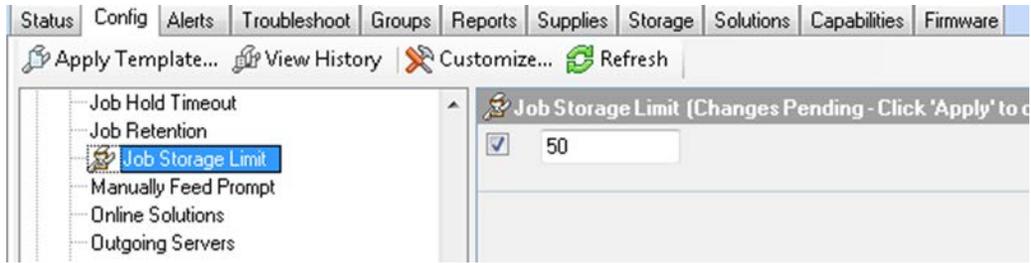


Figure 12: The Job Storage Limit options

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

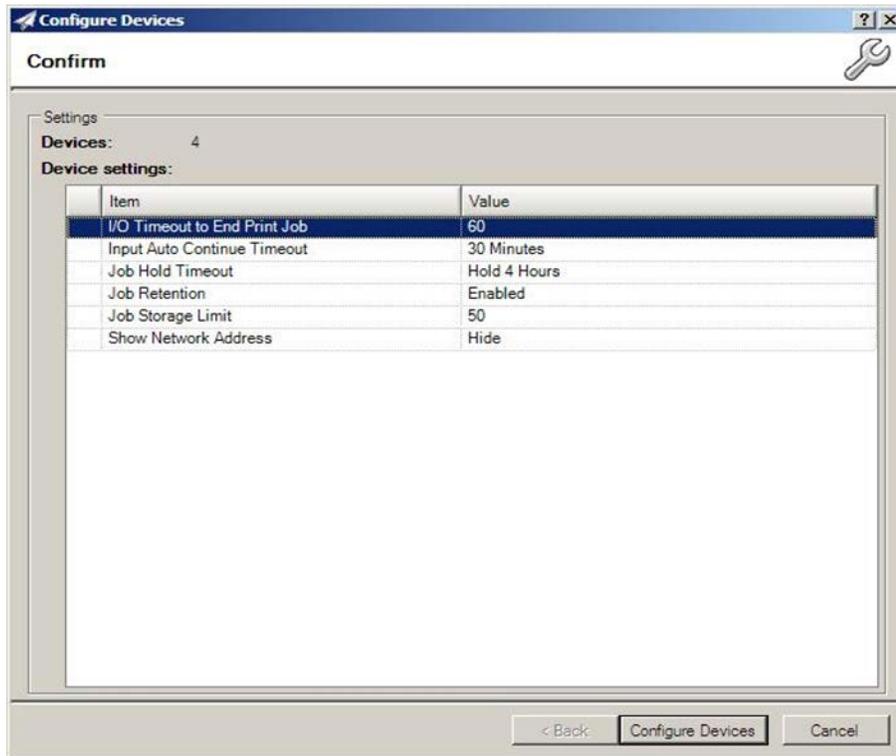


Figure 13: The Configure Devices dialog box

4. 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 network configurations. 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 14).

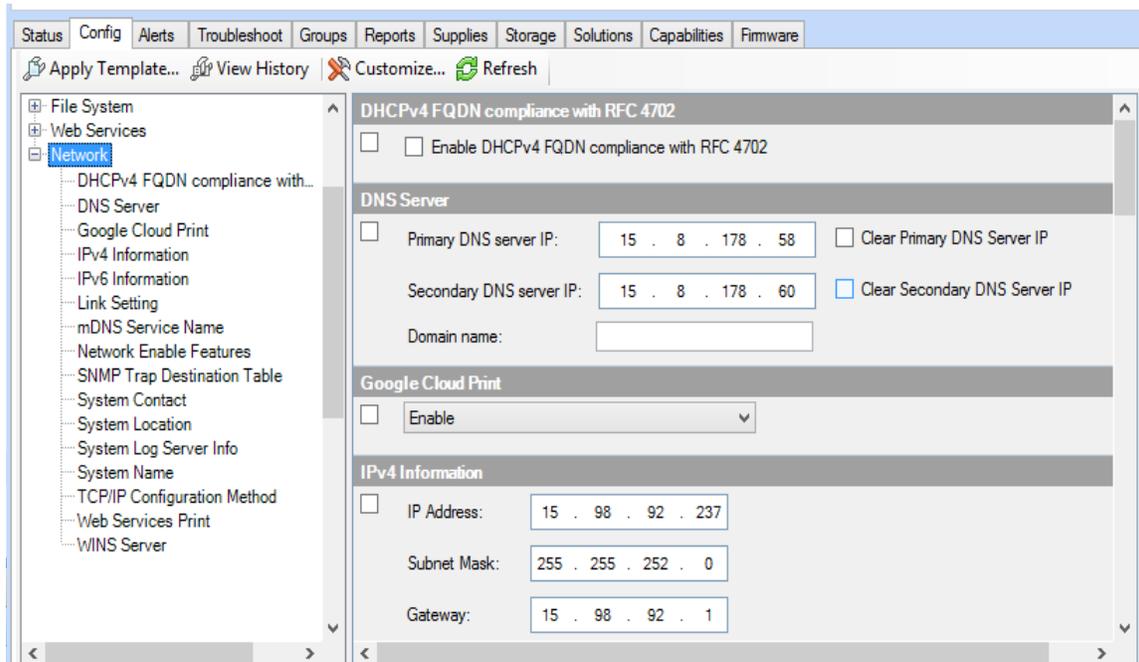


Figure 14: The Network Category

ePrint 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 Apps. Unless ePrint, HP Web Services, or other applications are part of your print environment we recommend disabling these features. If you are using the ePrint enterprise server instead of the HP cloud, you should refer to your administrators guide for any special settings that may be required to secure your solution.

Click to select the **ePrint Settings** checkbox (Figure 15). Do not select the Enable HP ePrint checkbox unless you wish to enable that service.

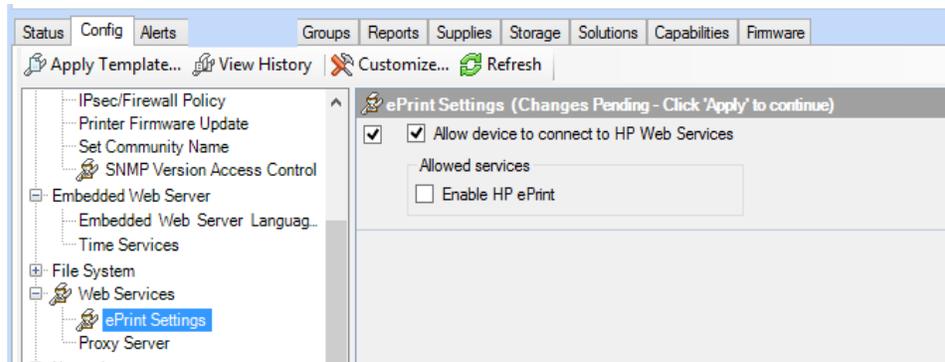


Figure 15: Disable HP ePrint, HP Web Services, and Apps

Enable WINS Port

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

To enable the WINS Port, click **WINS Server** under **Network**, and then check the **Enable WINS server** checkbox (Figure 16).

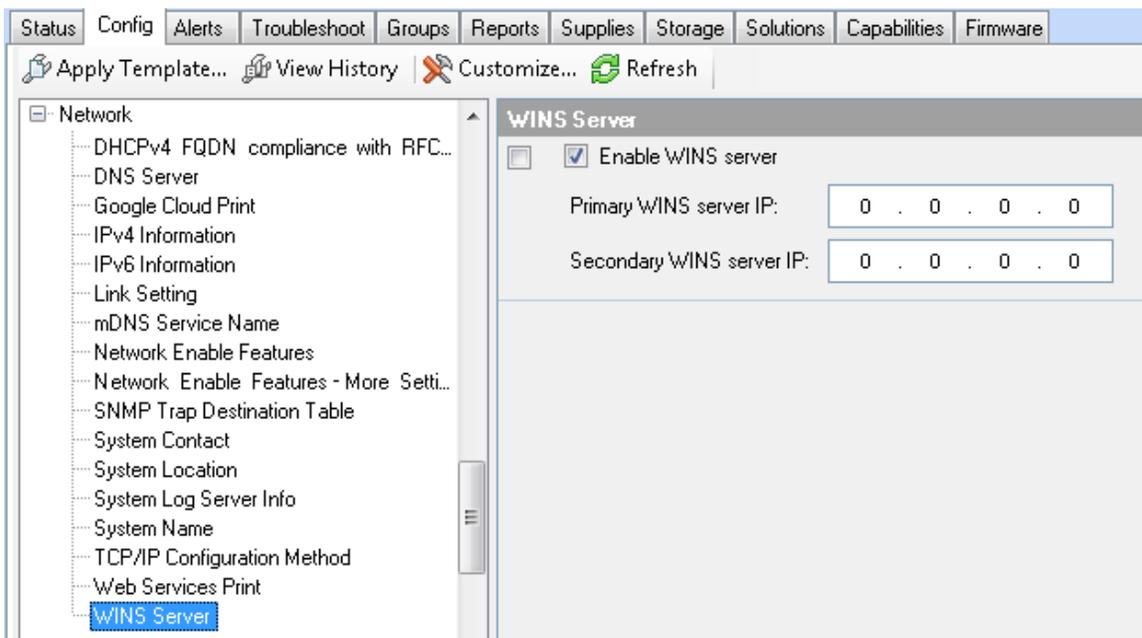


Figure 16: Enable WINS Port by selecting check box

Web Services Print

This option enables or disables the Microsoft Services for WSD Print services.

Click to select **Web Services Print** (Figure 17), and select **Disabled**.

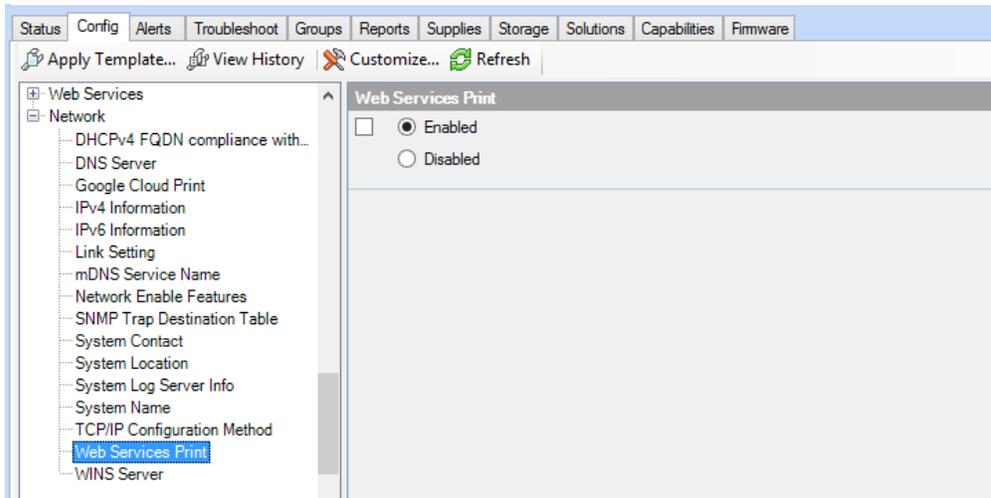


Figure 17: Disabling Web Services Print

Google Cloud Print

This option enables or disables the Google Cloud Print for Devices.

Click to select **Google Cloud Print** (Figure 18), and select **Disable**.

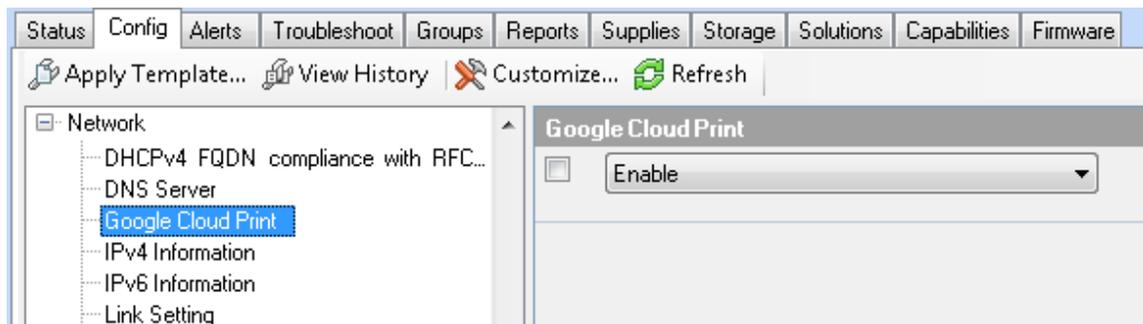


Figure 18: Google Cloud Print setting

Network Enable Features

To enable or disable print features on your MFP, follow these steps:

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

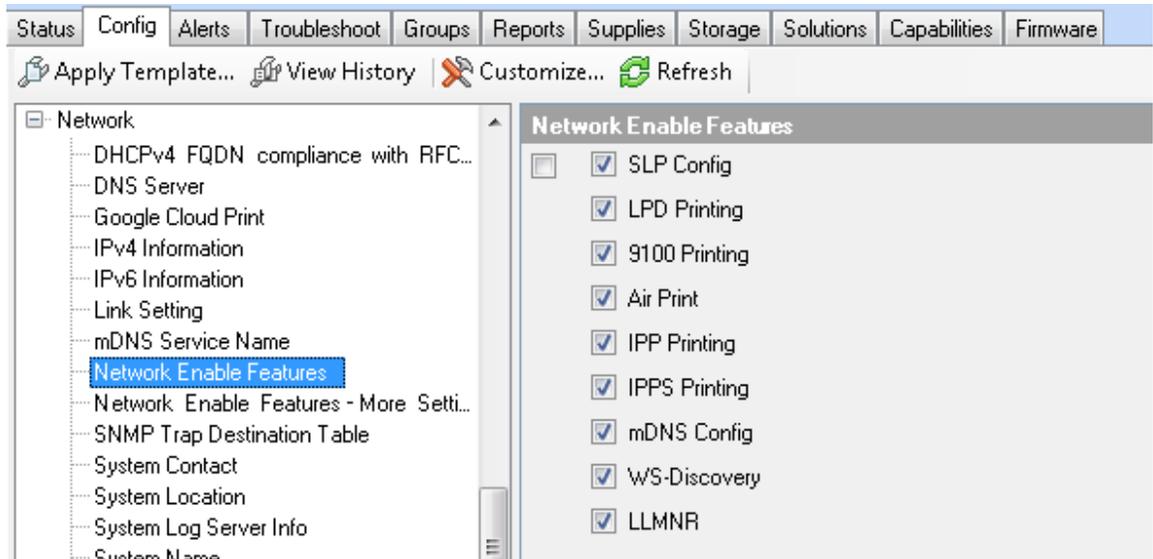


Figure 19: The Enable Features option

2. Select the print features that you would like to enable or disable. The following table contains information about the recommended settings for the **Enable Features** option:

Feature	Recommended Setting	Explanation
SLP Config	Disabled	Disabling SLP Config prevents access to configuration settings and other features through SLP.
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.
AirPrint	Disabled	Disabling AirPrint prevents printing via AirPrint. If you do not operate in an environment that supports this feature, we recommend disabling this feature.
IPP FAX Out	Disabled	Disabling IPP FAX Out prevents faxing via AirPrint. If you do not operate in an environment that supports

		this feature, we recommend disabling this feature.
eSCL Scan	Disabled	Disabling eSCL Scan prevents scanning via eSCL, a REST protocol. 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 you 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 .
WS-Discovery	Disabled	Disabling WS-Discovery prevents systems from using WS-Discovery for discovering or browsing printers on the network.

WARNING: You should enable WS-Discovery on this printer if any of the following apply: 1) You are using an IPv6 only network, 2) you use WS-Print to discover your devices, or 3) you operate in a Windows Vista/ Windows 7 centric-environment.

If you are unsure of this setting, we highly recommend testing its implications with a single device before applying it to your whole fleet.

Note:

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

3. Click **Apply** in the lower right hand corner to view the Configure Devices dialog box. (Figure 24). Review your selections carefully before clicking on the Configure Devices button.

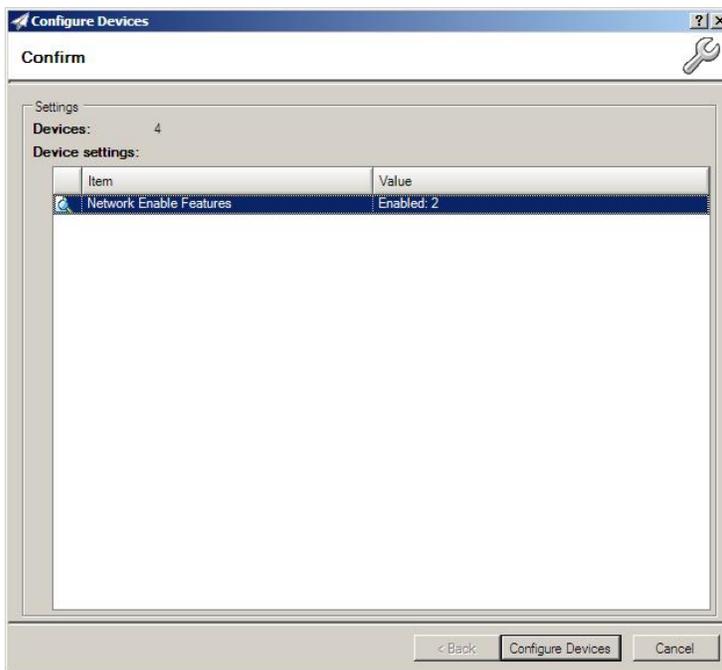


Figure 20: Confirm you configurations

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.

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.

1. Click **Embedded Web Server Password** under the Security category (Figure 21).

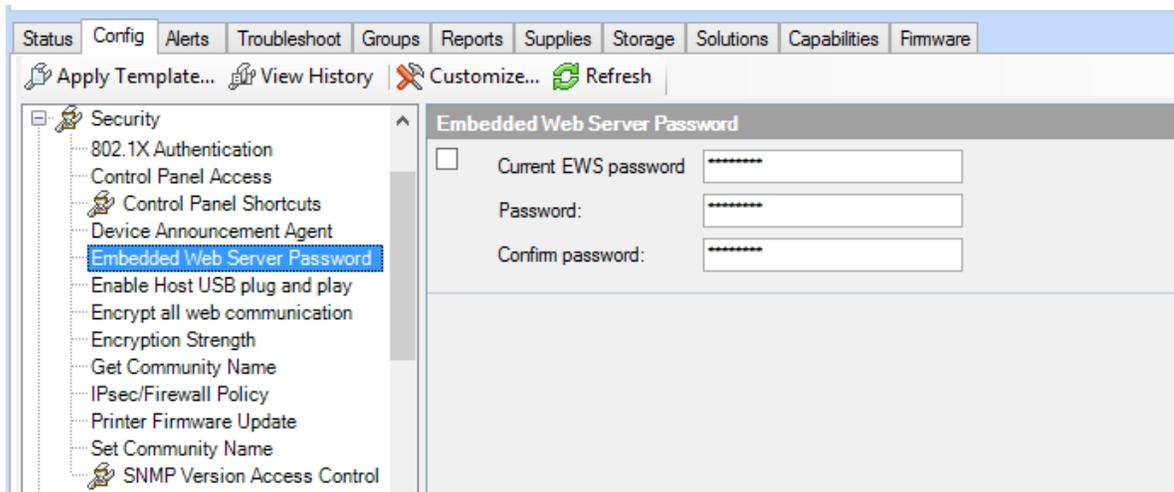


Figure 21: The Embedded Web Server Password options

2. Type a password of 9 to 16 characters in the **Password** field (you should always type the maximum number of characters for best security). This setting requires users to log on for parts of the EWS that provide configuration options.
3. Repeat the password exactly in the **Confirm 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 proximity card solution, or print from USB.

To set Enable Host USB:

Click to select the **Enable Host USB** (Figure 22) and click to select **Disabled**.

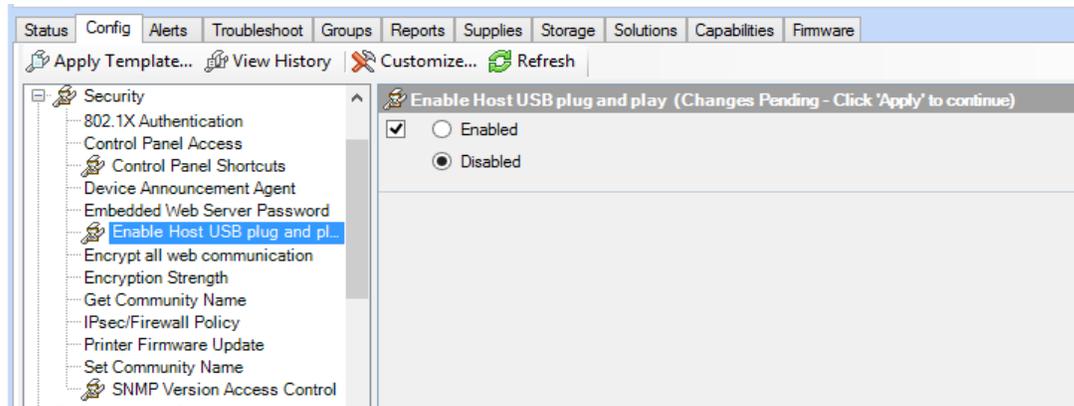


Figure 22: The Enable Host USB option

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 23).



Figure 23: Enabling HTTPS web communication

Encryption Strength

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

To configure the Encryption Strength setting:

1. Click **Encryption Strength** in the Security category (Figure 24).
2. Click the **Encryption Strength** dropdown menu, and select the highest setting that your browser supports.

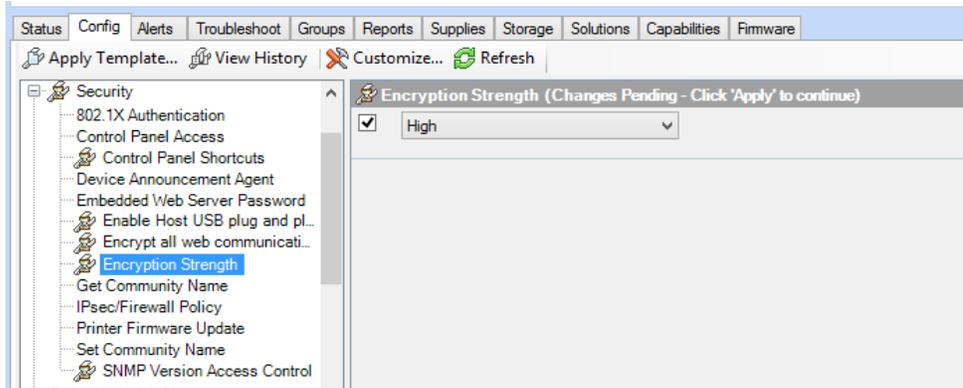


Figure 24: The Encryption Strength option

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 25), and select **Disable**.

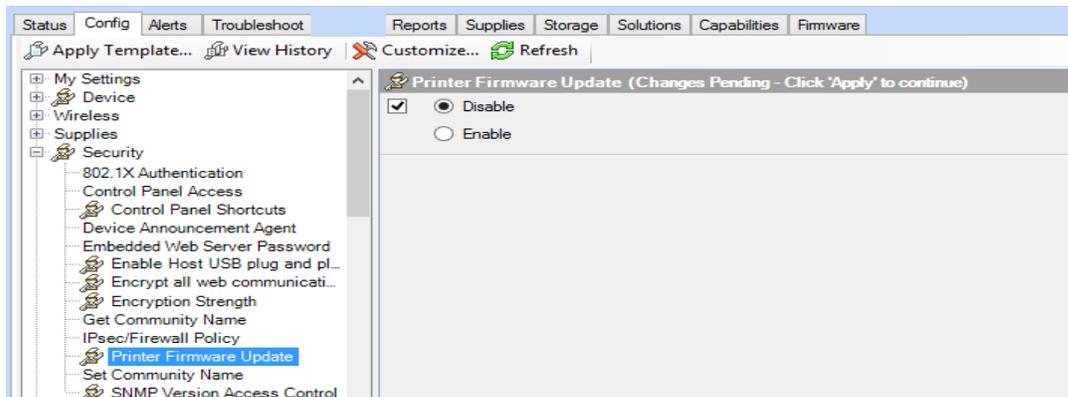


Figure 25: The Printer Firmware Update option

Restrict Color

The Restrict Color options (Figure 26) allow you to manage the usage of color printing supplies within your organization. If you wish to restrict access to color printing you can configure these settings to match your policy.

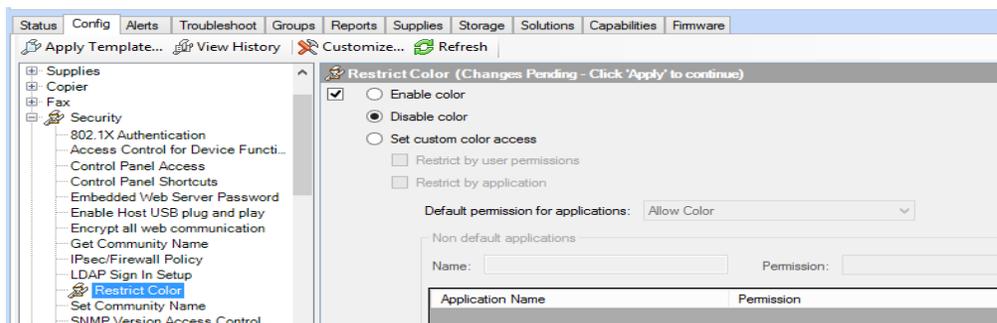


Figure 26: The Color Access Control options

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 27) 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.

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

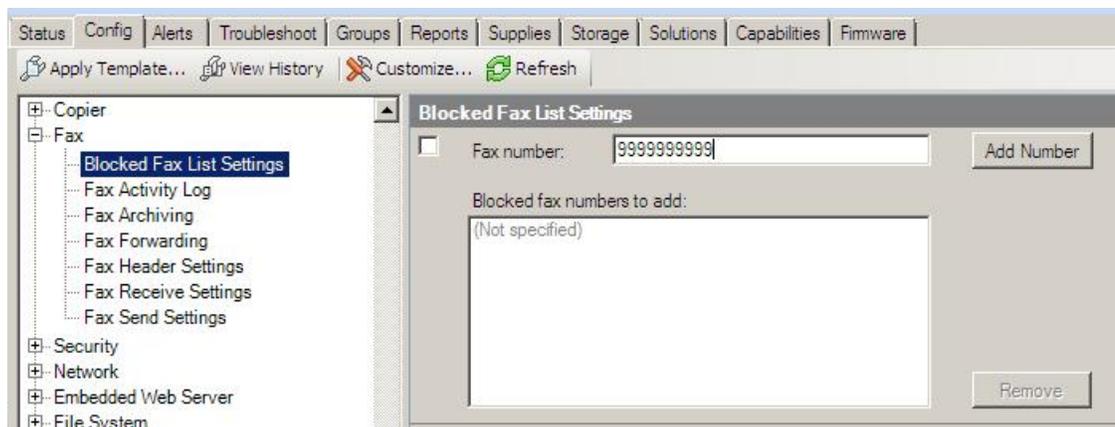


Figure 27: The Blocked Fax List settings

2. Enter a Fax number that you wish to block and click 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 28) allows you to set the phone number and company name for all of your faxes. We recommend setting these options.

Follow these instructions to configure Fax Printing:

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

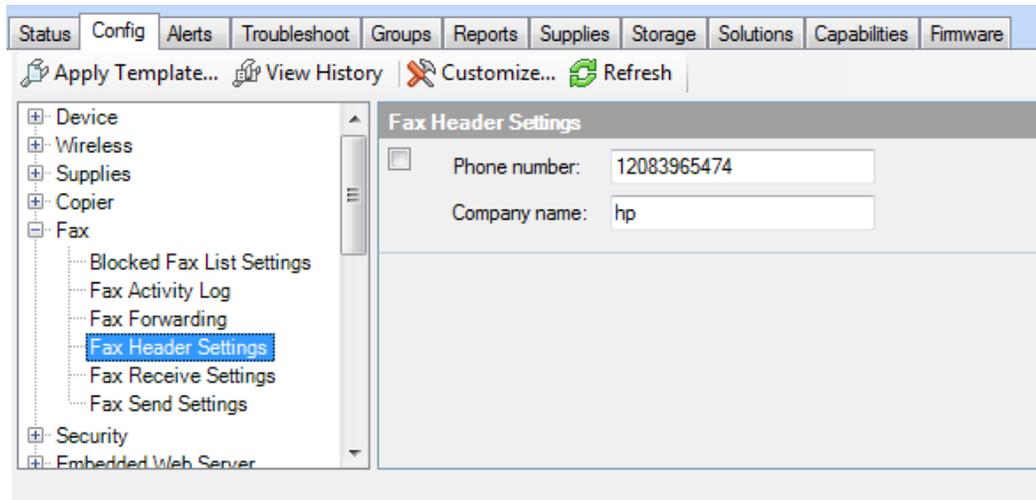


Figure 28: Fax Header settings

2. Enter the Phone number and Company name that you would like to appear on faxes.

Configuring MFP File System Settings

The **File system** category provides settings for access to the embedded and optional data storage devices.

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

To set the Secure File Erase Mode follow these instructions:

1. Click to select **Secure File Erase Mode** (Figure 29), and view the option in the dropdown menu.

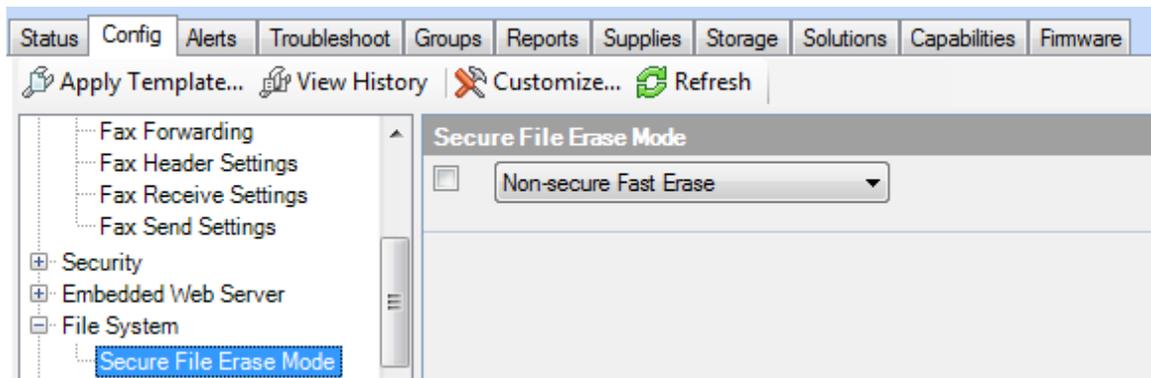


Figure 29: The Secure File Erase Mode setting

2. Select **Non-Secure Fast Erase**.
3. Click the **Apply** button located at the bottom right hand corner to apply the settings to the selected devices. The Configure Devices dialog box will open.
4. 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.

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, follow these steps:

1. Scroll down, and click to select **Email Address/Message Settings** (Figure 30).

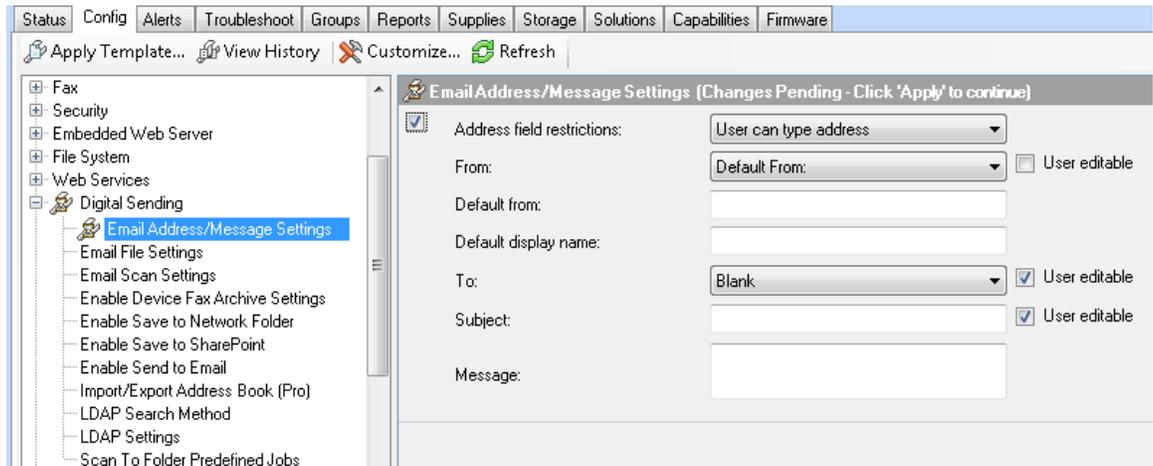


Figure 30: The Email Address/Message Settings

2. Click to select the **Address field restrictions** checkbox.
3. Select options from the dropdown lists.
4. In the **Default From** text box, enter any address that includes an ampersand (@).
5. Click to uncheck the **User editable** box to prevent a user from changing the **Default From:** address.

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.

6. Fill in the **Display Name** and the **Default Subject** fields as desired.
7. Click the **Apply** button located at the bottom right hand corner to apply the settings to the selected devices.

Chapter 3: Advanced Security for Multiple HP Devices

This chapter will provide some tips for configuring HP MFP 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 Embedded Web Server Administrator Guide for more information. You can find these documents and more information at hp.com.

Access Control for Device Functions

Access Control for Device Functions 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.

To configure Access Control for Device Functions, follow these steps:

1. On the **Config** tab click **Access Control for Device Functions** (Figure 31) under the **Security** Category.

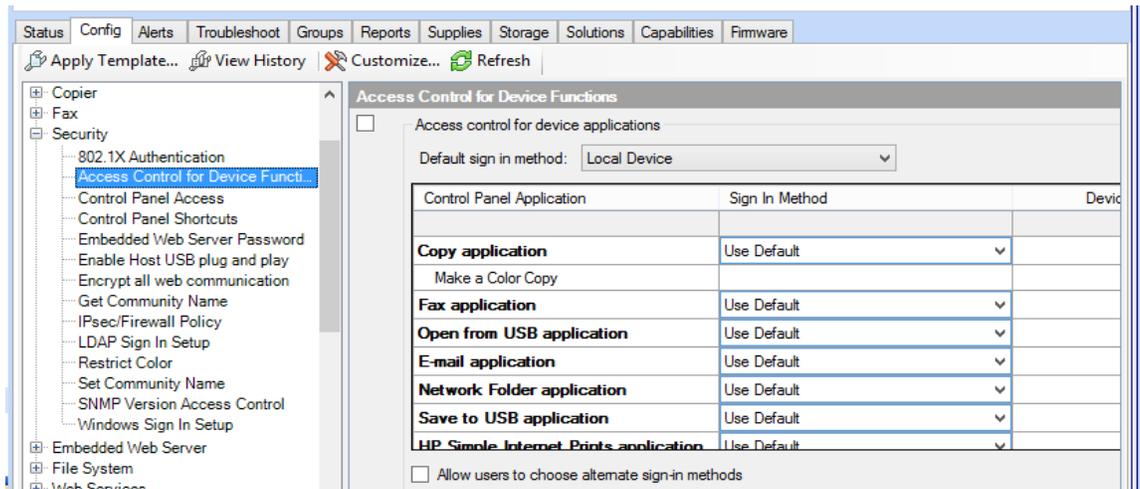


Figure 31: The Access for Device Functions option

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

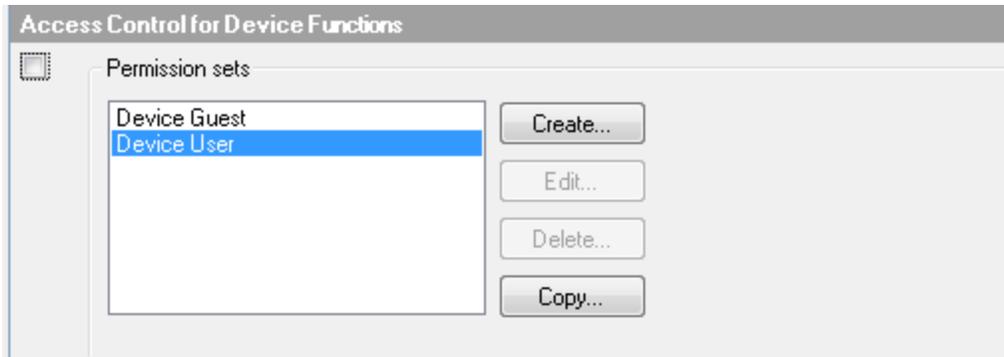


Figure 32: The Device User Option

- 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.

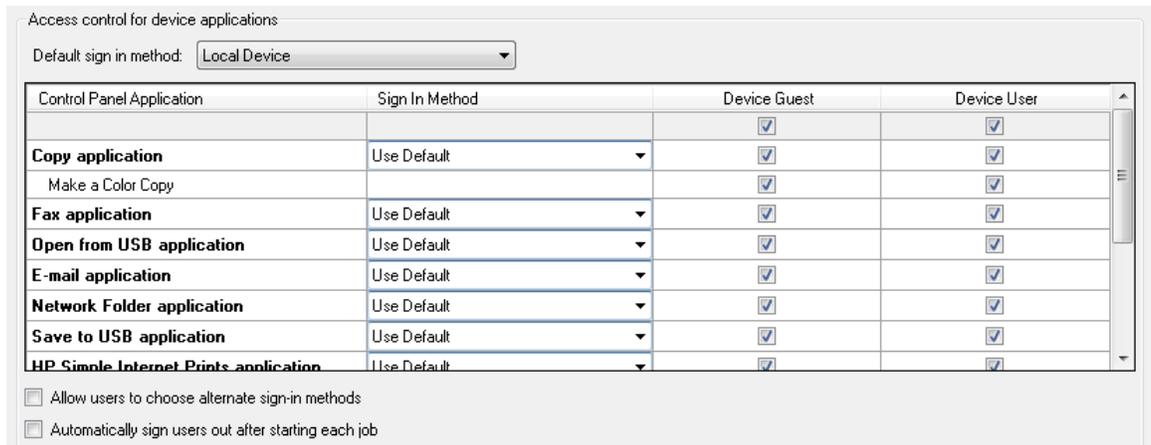


Figure 33: Access control for device applications options

If you choose a default authentication (Local Device, Windows, LDAP) method, then anyone who uses the MFP will be required to login to 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 and Kerberos) require additional solutions on the network for support.

For more information on Access Control configuration, please refer to the user or EWS Administration guide for your device.

LDAP

If your network includes LDAP, configure the **LDAP Sign In Setup** and the **LDAP Users and Groups** options (Figure 34 and 35).

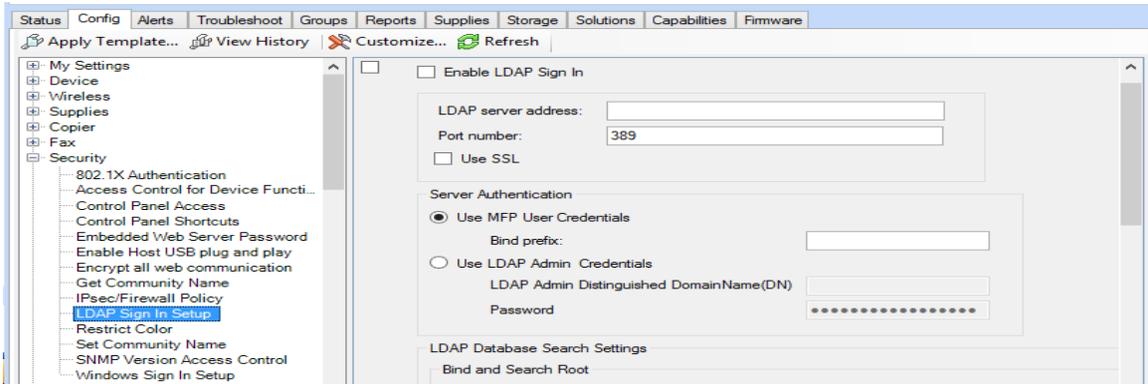


Figure 34: The LDAP Sign In Setup options

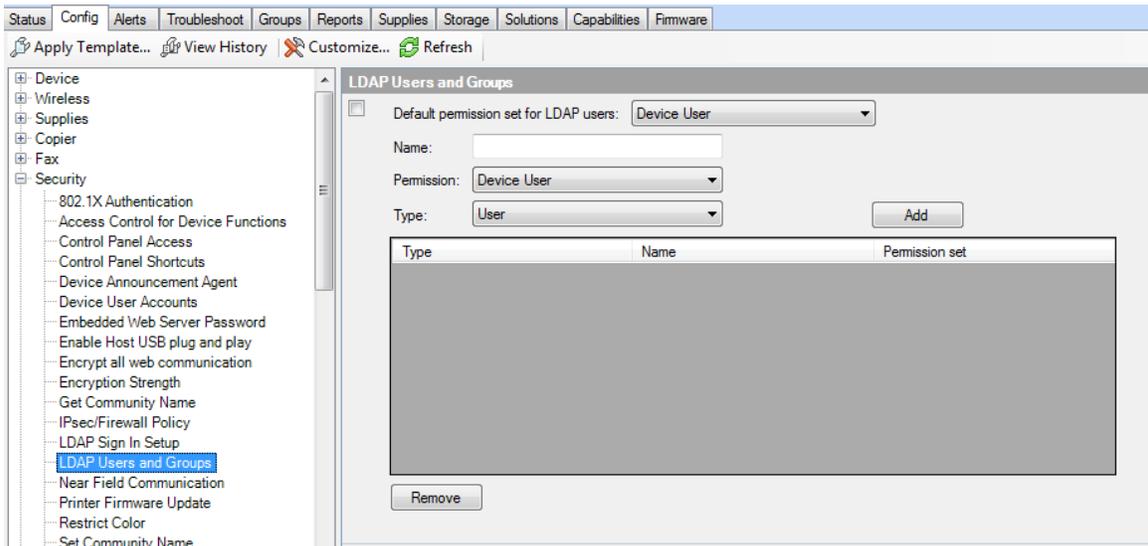


Figure 35: The LDAP Users and Groups options

Once these settings are configured, users will be required to enter login credentials to use the MFPs.

Disable Wireless

Unless your environment requires wireless printing, we recommend disabling these features.

There are three types of wireless features on these devices, as follows:

- 802.11 b/g/n
- Enable Wireless Station
- Wi-Fi Direct

Each of these features can be disabled separately.

In Web Jetadmin select the **Config** tab to see these options under **Wireless** (Figure 36).

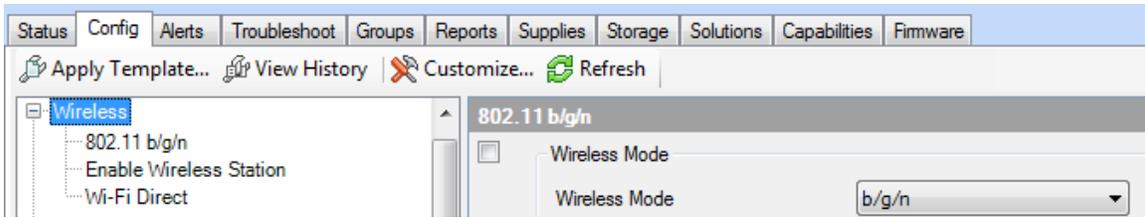


Figure 36: Wireless options on the Config tab

Configure Firewall

Firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. HP PageWide printers provide this feature to ensure that printing is secure.

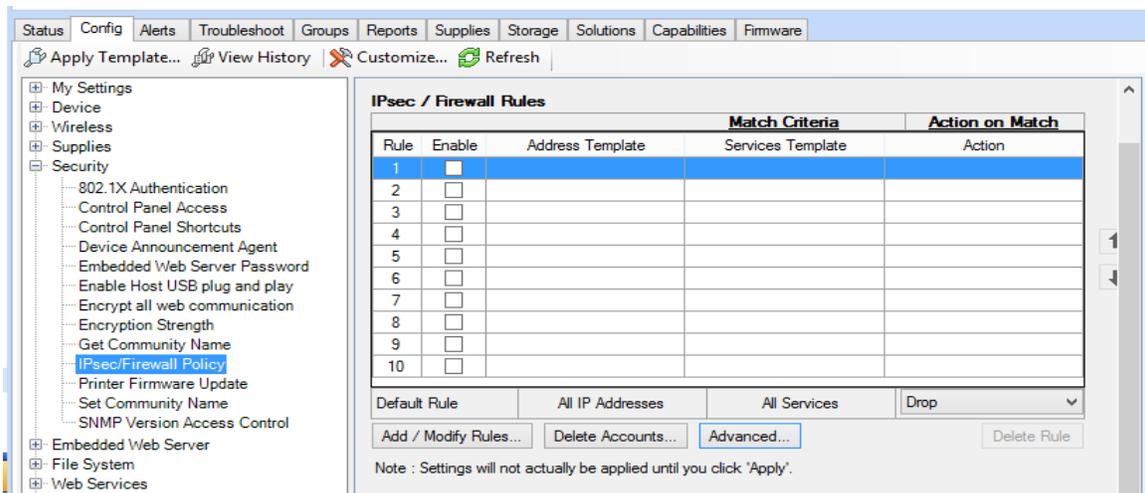


Figure 37: The Firewall Setup options

The **Failsafe** option (Figure 38) ensures that HTTPS remains accessible even if it is blocked by the Firewall policy. This allows the administrator to test the policy without inadvertently locking themselves out of the device. It is recommended that the Failsafe Option be disabled once the policy has been successfully tested.

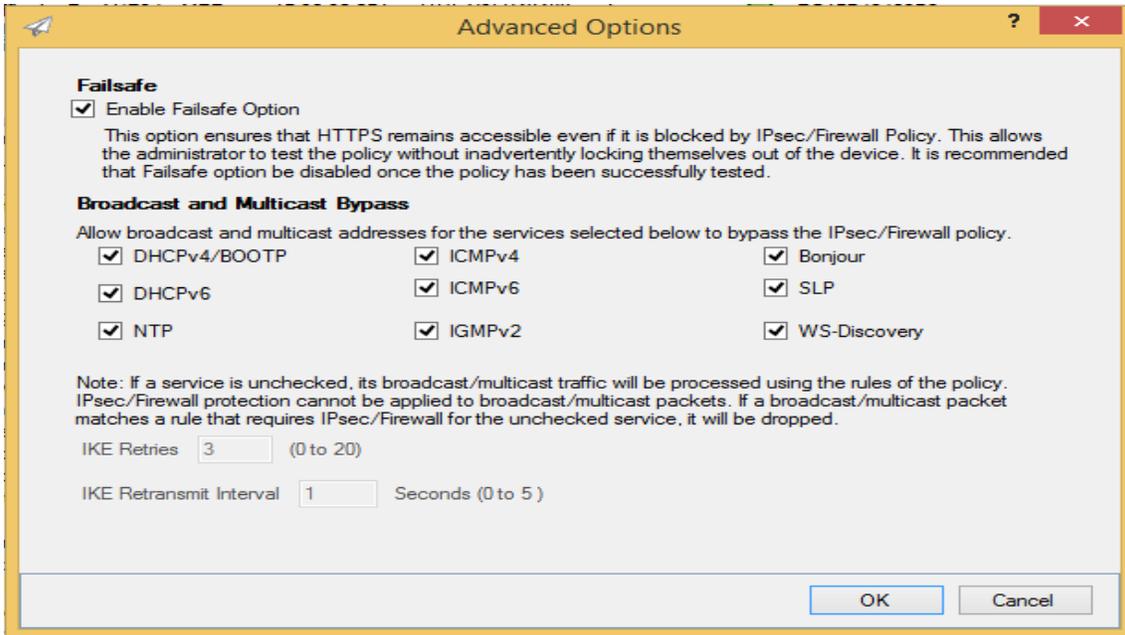


Figure 38: The HTTPS Setup options

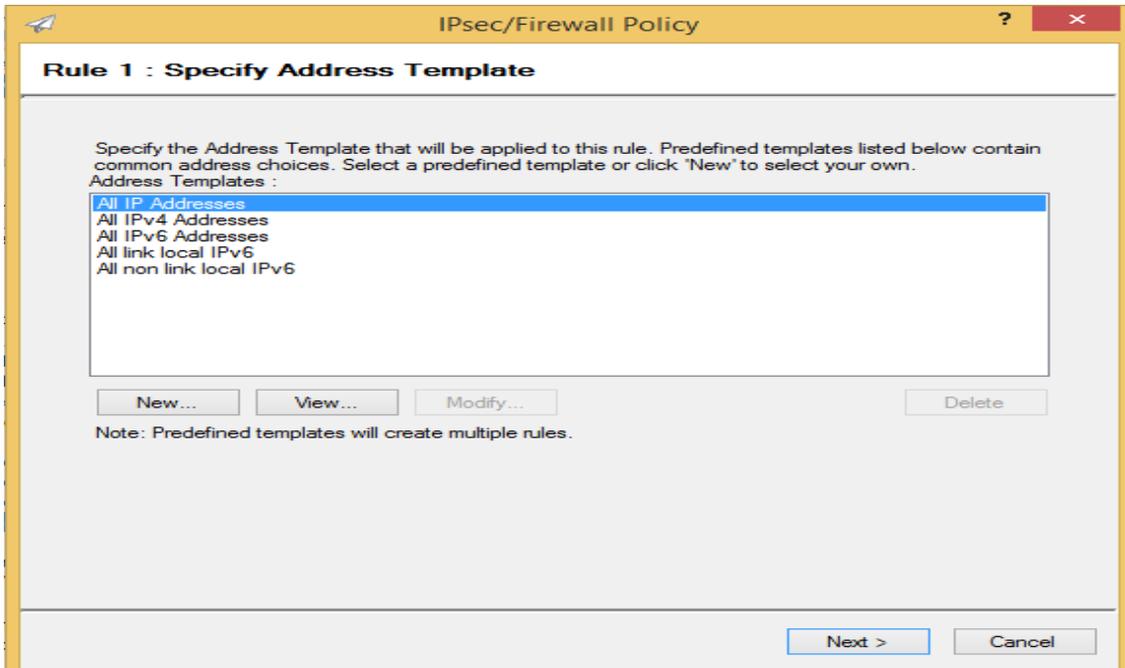


Figure 39: The IPsec Setup options

Security Features Available in the Embedded Web Server

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

To configure these settings, follow these steps:

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.

Disable Job Log on EWS Tools tab

Job log on the EWS tools tab is disabled by default. To ensure that access to this data remains restricted, this feature should remain disabled.

To enable/disable **Job Log**, follow these steps:

1. Browse to the Embedded Web Server for the target device.
2. Select the **Tools** tab.
3. Select **Reports** from the left hand menu.
4. Select the **Enable Job Log** checkbox to enable the setting, or deselect the checkbox to disable the setting.

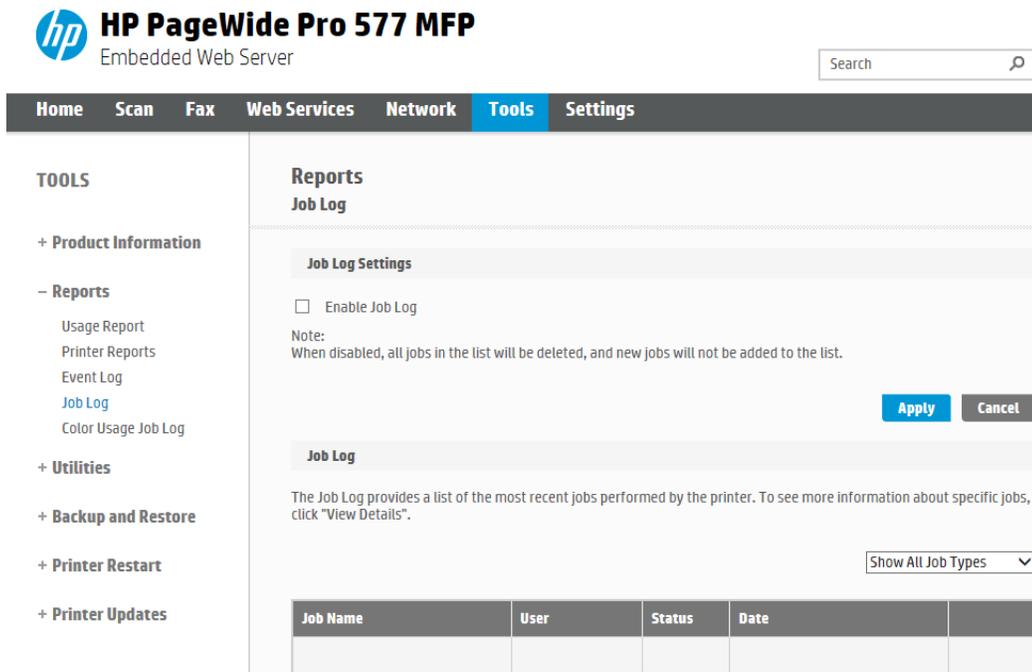


Figure 40: Disable Job Log on EWS information tab

HP and 3rd Party Solutions

Most of the recommendations in the next chapter can be implemented without having a negative impact on HP and 3rd party solutions, however HP and 3rd party solutions should be tested with any settings changes to ensure that there are not any negative impacts. If a previously working solution no longer works, revert to your original settings.

Chapter 4: Settings List

This section is a complete list of the settings recommended in this checklist. This section does not include instructions or explanations. This list provides the recommended settings to 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

- 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 **ePrint Settings**
- Configure **Network Enable Features** options
 - Disable **SLP Config**
 - Enable **9100 Printing**
 - Disable **AirPrint**
 - Disable **IPP Printing**
 - Disable **IPPS**
 - Disable **mDNS Config**
 - Disable **WS-Discovery**

- Disable **Web Services Print**

Security Category Options

- Configure **Embedded Web Server Password**
- Disable **Enable Host USB**
- Enable **HTTPS Setting to Encrypt all web communication**
- Configure **Encryption Strength to High**
- Disable **Printer Firmware Update**
- Configure **Restrict Color** as desired

Fax Category Options

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

MFP File System Options

- Configure **Secure File Erase Mode to Non Secure Fast Erase**

Digital Sending Settings Options

- Configure **Default From Address**
 - Select Prevent user from changing the Default From Address

Chapter 5: Default Settings

The table below lists the default setting for each configuration in the checklist.

Setting	Default Setting
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
ePrint Settings	Disabled and Not Configured
Configure Enable Features options	(See below)
Disable SLP Config	Enabled
Disable LPD Printing	Enabled
Enable 9100 Printing	Enabled
Disable AirPrint	Enabled
Disable IPP Printing	Enabled
Disable IPPS	Enabled
Disable MDNS Config	Enabled
Disable WS-Discovery	Disabled
Web Services Print	Enabled
Embedded Web Server Password	Disabled
Enable Host USB	Disabled
Enable Encrypt all Web Communication	Enabled
Configure Encryption Strength to High	High
Disable Printer Firmware Update	Enabled
Restrict Color	Not configured
Configure Fax Printing	Not configured
Blocked Fax List Settings	Not Configured
Fax Header Settings	Not Configured
Configure File System External Access	(See below)
Configure Secure File Erase Mode to Non-Secure Fast Erase	Non-Secure Fast Erase
Configure Default From Address	Not configured
Select Prevent user from changing the Default From Address	Not selected

Chapter 6: 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 Firewall, 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.

- **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 faxes) 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 memory. Thus, you should configure Job Hold Timeout and other related settings.
- **Enable Job Storage Limit.** Job Storage Limit when enabled 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 ePrint.** Unless ePrint, HP Web Services, or other applications are a critical part of your print environment we recommend disabling these features. If you are using the ePrint enterprise server and not the HP cloud for ePrint you should refer to your administrators guide for any special settings that may be required to secure your solution.
- **Configure Enable Features options.** 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 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 LPD Printing.** LPD Printing is the protocol necessary for printing in UNIX, HP-UX, or Linux environments. You should disable LPD Printing unless your network includes UNIX workstations that might print using the MFPs. With this option disabled, MFPs will deny access to UNIX machines.
 - **Enable 9100 Printing.** 9100 Printing should always be enabled. It is the standard printing protocol used by MFP print drivers. Disabling 9100 Printing would disable all printing for most users.
 - **Disable AirPrint.** AirPrint Printing is a protocol for printing from Apple devices. Unless your network environment supports AirPrint, we recommend keeping this feature disabled.
 - **Disable IPP Printing.** IPP Printing is a protocol for printing over the Internet or locally. Unless you have a requirement for IPP printing it should be disabled. With it disabled, the MFPs will deny access to direct printing from the Internet. Print jobs generated from web browsers using the installed print driver are not affected.

- **Disable IPPS when IPP 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.
- **Disable MDNS Config.** MDNS Config resolves host names with IP addresses in small networks without DNS servers. Most enterprise networks include DNS servers and do not require this service. With this option disabled, a non-DNS network will not recognize the MFPs. If your network does not include a DNS server, you should enable MDNS Config.
- **Disable 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.
- **Disable Web Services Print.** This disables the Microsoft WSD Print services supported. 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 Access Control.** The Access Control 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 Access Control. With Access Control enabled, MFPs will deny access to users who cannot supply the correct credentials.

Embedded Web Server Options

- **Configure Embedded Web Server Configuration Options.** These options limit some of the EWS features that can be misused:
- **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 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.

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

It is recommended that you disable 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.
- **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.

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.

- **Set the Secure File Erase Mode to Non-Secure Fast Erase.** Non-Secure Fast Erase marks the print job data as deleted, and allows the MFP to reclaim and subsequently overwrite the data when needed.

Digital Sending Options

- **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.

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. Following is a list of 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.

Chapter 7: 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, such as the following:

- Leaving documents in the printer output trays exposed to possible unauthorized viewers
- Leaving documents in the 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 flatbed scanner. Keep the MFP in an enclosed room to allow for controlled access when printing or scanning sensitive documents.

Physical security also involves access to the location where an MFP is installed. Limiting physical access to an MFP can help prevent security risks. 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.

Appendix: Glossary of Terms and Acronyms

The table below lists terms and acronyms that are used in this document.

Term	Description
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.
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.
Job Retention	Job Retention is the MFP capability of storing print jobs or fax jobs for printing on demand at the control panel. PIN printing and PIN fax printing are functions of Job Retention.
MFP	Multi-Functional Peripheral – An MFP is a device that includes multiple capabilities such as print, copy, fax, and digital sending (email and send to network folder).
PIN	Personal Identification Number. A PIN is a numeric password. MFPs use PINs for secure printing and secure fax printing. They can also use PINs for authentication.
Scanner , ADF, or flatbed scanner	<p>The top of the MFP is a scanner that converts paper documents into digital images for copying, fax, or digital sending. The scanner can scan a document in two ways: Automatic Document Feeder (ADF) or flatbed.</p> <p>The ADF is the top of the MFP. It is the cover of the flatbed scanner. The ADF draws sheets into a paper path from an input tray similar to the input paper tray on a printer. It runs each sheet past the scanner and places it in an output tray.</p> <p>The flatbed scanner is a flat pane of glass under a cover (the ADF) that opens to allow placement of one surface for scanning. The flatbed scanner is for documents such as folded paper or books that will not go through the ADF.</p>
SNMPv3	SNMPv3 is a secure network protocol that encrypts network traffic. It is available with Web Jetadmin.
SSL	Secure Socket Layer. SSL is the encryption capability of the Internet. It is the system used for web communication via HTTPS.

Term	Description
Storage device	<p>A storage device is a component that stores data. The MFP includes two types of storage devices: hard drive and Compact Flash cards.</p> <p>MFP storage devices store two types of data: system data, such as configurations, and user data, such as print jobs, address books, and installed applications.</p>
WJA	<p>HP Web Jetadmin: HP Web Jetadmin is a peripheral management tool that provides access to multiple devices for status and configuration. It is capable of configuring multiple MFPs simultaneously. Web Jetadmin is the recommended tool for configuring all settings in this checklist.</p>

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Adobe and PostScript are trademarks of Adobe Systems Incorporated.

© Copyright 2016 Hewlett-Packard Development Company, L.P.